Traducido del inglés al español - www.onlinedoctranslator.com

Vigilancia Dahua DH-S7600

Serie de interruptores de enrutamiento

Gestión y monitoreo de redes

Guía de configuración

Dahua Tecnología Co., Ltd.

Versión de software: DH-S7600_SYSTEM_V7.1.45-R7184P02
Versión del documento: 6W100-20161115

Copyright © 2016, Dahua Technology Co., Ltd. Todos los derechos reservados.

Ninguna parte de este manual puede reproducirse ni transmitirse de ninguna forma ni por ningún medio sin el consentimiento previo por escrito de Dahua Technology Co., Ltd.

Marcas registradas

, , y son marcas comerciales de Dahua Technology Co., Ltd.

Todas las demás marcas comerciales que puedan mencionarse en este manual son propiedad de sus respectivos dueños.

Aviso

La información contenida en este documento está sujeta a cambios sin previo aviso. Se han hecho todos los esfuerzos posibles en la preparación de este documento para garantizar la exactitud del contenido, pero todas las declaraciones, información y recomendaciones contenidas en este documento no constituyen garantía de ningún tipo, expresa o implícita.

Prefacio

Esta guía de configuración describe los fundamentos y la configuración de administración y monitoreo de la red. Describe cómo ver la información del sistema, evaluar el rendimiento de la red, sincronizar la hora de los dispositivos con los relojes de su red y utilizar la**silbido**y**tracert**Comandos para verificar y depurar la conectividad de red actual.

Este prefacio incluye los siguientes temas sobre la documentación:

- Audiencia.
- Convenciones.

Audiencia

Esta documentación está destinada a:

- Planificadores de redes.
- Ingenieros de servicio y soporte técnico de campo.
- Administradores de red que trabajan con la serie de conmutadores DH-S7600.

Convenciones

Esta sección describe las convenciones utilizadas en la documentación.

Numeración de puertos en ejemplos

Los números de puerto en la documentación son solo para ilustración y es posible que no estén disponibles en su dispositivo.

Convenciones de comando

Convención	Descripción
Negrita	**Atrevido**El texto representa comandos y palabras clave que ingresa literalmente como se muestra.
Itálico	*Itálico*El texto representa argumentos que se reemplazan con valores reales.
[ ]	Los corchetes encierran opciones de sintaxis (palabras clave o argumentos) que son opcionales.
{ x | y | ... }	Las llaves encierran un conjunto de opciones de sintaxis requeridas separadas por barras verticales, entre las cuales usted selecciona una.
[x | y | ...]	Los corchetes encierran un conjunto de opciones de sintaxis opcionales separadas por barras verticales,

Convención	Descripción
	del cual seleccionas uno o ninguno.
{ x | y | ... } *	Las llaves marcadas con asteriscos encierran un conjunto de opciones de sintaxis requeridas separadas por barras verticales, de las cuales puede seleccionar al menos una.
[x | y | ...] *	Los corchetes marcados con asteriscos encierran opciones de sintaxis opcionales separadas por barras verticales, entre las cuales puede seleccionar una opción, varias opciones o ninguna.
&<1-n>	El argumento o la combinación de palabra clave y argumento antes del signo comercial (&) se puede ingresar de 1 a n veces.
#	Una línea que comienza con un signo de almohadilla (#) son comentarios.

Convenciones GUI

Convención	Descripción
Negrita	Los nombres de ventanas, botones, campos y elementos de menú están en negrita. Por ejemplo, el**Nuevo Usuario**aparece la ventana; hacer clic**DE ACUERDO**.
>	Los menús de varios niveles están separados por corchetes angulares. Por ejemplo,**Archivo**>**Crear**> **Carpeta**.

Símbolos

Convención	Descripción
¡ADVERTENCIA!	Una alerta que llama la atención sobre información importante que, si no se comprende o se sigue, puede provocar lesiones personales.
PRECAUCIÓN:	Una alerta que llama la atención sobre información importante que, si no se comprende o se sigue, puede provocar pérdida o corrupción de datos o daños al hardware o software.
IMPORTANTE:	Una alerta que llama la atención sobre información esencial.
NOTA:	Una alerta que contiene información adicional o complementaria.
CONSEJO:	Una alerta que proporciona información útil.

Iconos de topología de red

Convención	Descripción
	Representa un dispositivo de red genérico, como un enrutador, conmutador o firewall.
	Representa un dispositivo con capacidad de enrutamiento, como un enrutador o un conmutador de capa 3.
	Representa un conmutador genérico, como un conmutador de Capa 2 o Capa 3, o un enrutador que admite el reenvío de Capa 2 y otras funciones de Capa 2.
	Representa un controlador de acceso, un módulo WLAN por cable unificado o el motor del controlador de acceso en un conmutador WLAN por cable unificado.
	Representa un punto de acceso.
	Unidad terminadora inalámbrica.

Convención	Descripción
	Terminador inalámbrico.
	Representa un punto de acceso de malla.
	Representa señales omnidireccionales.
	Representa señales direccionales.
	Representa un producto de seguridad, como un firewall, UTM, una puerta de enlace de seguridad multiservicio o un dispositivo de equilibrio de carga.
	Representa una tarjeta de seguridad, como un firewall, equilibrio de carga, NetStream, SSL VPN, IPS o tarjeta ACG.

contenido

Configuración de NQA

Descripción general

El analizador de calidad de red (NQA) le permite medir el rendimiento de la red, verificar los niveles de servicio para servicios y aplicaciones IP y solucionar problemas de red. Proporciona los siguientes tipos de operaciones:

- Eco ICMP.
- DHCP.
- DNS.
- FTP.
- HTTP.
- Fluctuación UDP.
- SNMP.
- TCP.
- Eco UDP.
- Tracert UDP.
- Voz.
- Nerviosismo en el camino.
- DLSw.

Como se muestra enFigura 1, el dispositivo de origen NQA (cliente NQA) envía datos al dispositivo de destino NQA simulando servicios y aplicaciones IP para medir el rendimiento de la red. Las métricas de rendimiento obtenidas incluyen latencia unidireccional, fluctuación, pérdida de paquetes, calidad de voz, rendimiento de la aplicación y tiempo de respuesta del servidor.

Todos los tipos de operaciones NQA requieren el cliente NQA, pero sólo las operaciones TCP, eco UDP, fluctuación UDP y voz requieren el servidor NQA. Las operaciones NQA para servicios que ya proporciona el dispositivo de destino, como FTP, no necesitan el servidor NQA.

Puede configurar el servidor NQA para escuchar y responder a direcciones IP y puertos específicos para satisfacer diversas necesidades de prueba.

Figura 1 Diagrama de red

Operación NQA

A continuación se describe cómo NQA realiza diferentes tipos de operaciones:

- Una operación TCP o DLSw establece una conexión.
- Una fluctuación UDP o una operación de voz envía varios paquetes de sonda. El número de paquetes de sonda se establece utilizando el**número de paquete de sonda**dominio.
- Una operación FTP carga o descarga un archivo. Una
- operación HTTP obtiene una página web.
- Una operación DHCP obtiene una dirección IP a través de DHCP.

- Una operación DNS traduce un nombre de dominio a una dirección IP.
- Una operación de eco ICMP envía una solicitud de eco ICMP.
- Una operación de eco UDP envía un paquete UDP.
- Una operación SNMP envía un paquete SNMPv1, un paquete SNMPv2c y un paquete SNMPv3.
- Una operación de fluctuación de ruta se logra en los siguientes pasos:

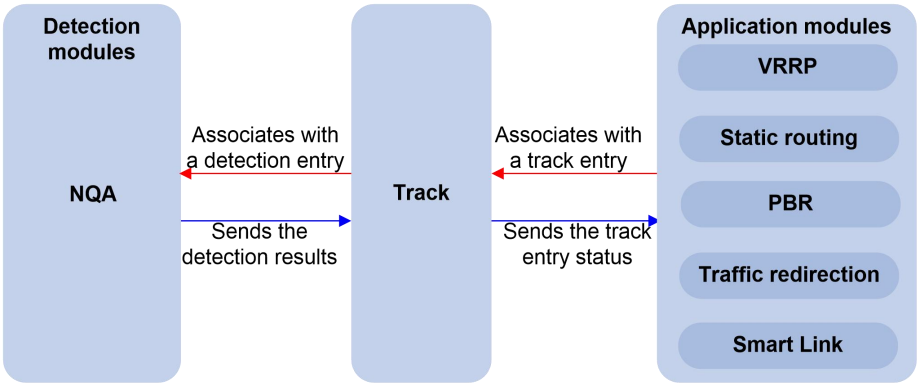
  a.La operación utiliza tracert para obtener la ruta desde el cliente NQA hasta el destino. Se pueden detectar un máximo de 64 saltos.

  b.El cliente NQA envía solicitudes de eco ICMP a cada salto a lo largo de la ruta. El número de solicitudes de eco ICMP se establece utilizando el**número de paquete de sonda**dominio.
- Una operación de tracert UDP determina la ruta de enrutamiento desde el origen hasta el destino. El número de sondas para cada salto se establece utilizando el**recuento de sondas**dominio.

Colaboración

NQA puede colaborar con el módulo Track para notificar a los módulos de la aplicación cambios de estado o rendimiento para que los módulos de la aplicación puedan realizar acciones predefinidas.

Figura 2 Colaboración



A continuación se describe cómo se monitorea mediante colaboración una ruta estática destinada a 192.168.0.88:

1. NQA supervisa la accesibilidad a 192.168.0.88.
2. Cuando 192.168.0.88 deja de ser accesible, NQA notifica el cambio al módulo Track.
3. El módulo Track notifica al módulo de enrutamiento estático del cambio de estado.
4. El módulo de enrutamiento estático establece la ruta estática como no válida según una acción predefinida.

Para obtener más información sobre la colaboración, consulte*Guía de configuración de alta disponibilidad*.

Monitoreo de umbral

La supervisión de umbral permite al cliente NQA realizar una acción predefinida cuando las métricas de rendimiento de la operación NQA violan los umbrales especificados.

tabla 1describe las relaciones entre las métricas de desempeño y los tipos de operaciones NQA.

Tabla 2 Métricas de desempeño y tipos de operaciones NQA

Métrica de rendimiento	Tipos de operaciones NQA que pueden recopilar la métrica
Duración de la sonda	Todos los tipos de operación NQA excepto UDP jitter, UDP tracert, path jitter y voz
Número de fallos de sonda	Todos los tipos de operación NQA excepto UDP jitter, UDP tracert, path jitter y voz
Tiempo de viaje	Jitter y voz UDP
Número de paquetes descartados	Jitter y voz UDP
Jitter unidireccional (fuente a destino o destino a fuente)	Jitter y voz UDP
Retraso unidireccional (fuente a destino o destino a fuente)	Jitter y voz UDP
Factor de deterioro de planificación calculado (ICPIF) (ver "Configurar la operación por voz")	Voz
Puntuaciones medias de opinión (MOS) (ver "Configurar la operación por voz")	Voz

Lista de tareas de configuración de NQA

Tareas de un vistazo	Observaciones
Configurar el servidor NQA	Requerido para TCP, eco UDP, fluctuación UDP y operaciones de voz.
(Requerido.)Habilitando el cliente NQA	N / A
(Obligatorio.) Realice al menos una de las siguientes tareas: - Configuración de operaciones NQA en el cliente NQA - Configuración de plantillas NQA en el cliente NQA	Cuando configura una plantilla NQA para analizar el rendimiento de la red, la función que utiliza la plantilla realiza la operación NQA.

Configurar el servidor NQA

Para realizar operaciones TCP, eco UDP, fluctuación UDP y voz, debe habilitar el servidor NQA en el dispositivo de destino. El servidor NQA escucha y responde a las solicitudes en las direcciones IP y puertos especificados.

Puede configurar varios servicios de escucha TCP o UDP en un servidor NQA, donde cada uno corresponde a una dirección IP y un número de puerto específicos. La dirección IP y el número de puerto para un servicio de escucha deben ser únicos en el servidor NQA y coincidir con la configuración en el cliente NQA.

Para configurar el servidor NQA:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite el servidor NQA.	**habilitar el servidor nqa**	De forma predeterminada, el servidor NQA está deshabilitado.

Paso	Dominio	Observaciones
3. Configure un servicio de escucha TCP o UDP.	- Servicio de escucha TCP: **conexión tcp del servidor nqa***dirección-ip número-puerto*[**instancia-vpn** *nombre-instancia-vpn*] [**tos***tos*] - Servicio de escucha UDP: **servidor nqa udp-echo***dirección-ip número-puerto*[**instancia-vpn** *nombre-instancia-vpn*] [**tos***tos*]	Puede configurar el valor ToS en el encabezado IP de los paquetes de respuesta enviados por el servidor NQA. El valor ToS predeterminado es 0.

Habilitando el cliente NQA

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite el cliente NQA.	**agente nqa habilitado**	De forma predeterminada, el cliente NQA está habilitado.

Configuración de operaciones NQA en el cliente NQA

Lista de tareas de configuración de operaciones de NQA

Tareas de un vistazo

(Obligatorio.) Realice al menos una de las siguientes tareas: - Configurar la operación de eco ICMP - Configurar la operación DHCP - Configurar la operación DNS Configurar - la operación FTP Configurar la - operación HTTP Configurar la operación - jitter UDP Configurar la operación SNMP - Configurar la operación TCP Configurar - la operación eco UDP Configurar la - operación tracert UDP Configurar la - operación de voz Configurar el - Operación DLSw Configuración de la - operación de fluctuación de ruta -
(Opcional.)Configuración de parámetros opcionales para la operación NQA
(Opcional.)Configurar la función de colaboración
(Opcional.)Configuración de la supervisión de umbrales
(Opcional.)Configuración de la función de recopilación de estadísticas de NQA
(Opcional.)Configurar el guardado de registros históricos de NQA
(Requerido.)Programación de la operación NQA en el cliente NQA

Configuración de la operación de eco ICMP

La operación de eco ICMP mide la accesibilidad de un dispositivo de destino. Tiene la misma función que el **silbido** comando, pero proporciona más información de salida. Además, si existen varias rutas entre los dispositivos de origen y de destino, puede especificar el siguiente salto para la operación de eco ICMP.

La operación de eco ICMP no es compatible con redes IPv6. Para probar la accesibilidad de una dirección IPv6, utilice el**hacer ping a ipv6**dominio. Para obtener más información sobre el comando, consulte*Referencia de comandos de monitoreo y administración de redes.*

Para configurar la operación de eco ICMP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de eco ICMP e ingrese su vista.	**escriba icmp-echo**	N / A
4. Especifique la dirección IP de destino de las solicitudes de eco ICMP.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino.
5. (Opcional). Especifique el tamaño de la carga útil en cada solicitud de eco ICMP.	**tamaño de datos***tamaño*	La configuración predeterminada es 100 bytes.
6. (Opcional). Especifique la cadena de relleno de carga útil para las solicitudes de eco ICMP.	**relleno de datos***cadena*	La cadena predeterminada es el número hexadecimal. 00010203040506070809.
7. (Opcional). Especifique la interfaz de salida para las solicitudes de eco ICMP.	**interfaz de salida***tipo de interfaz número de interfaz*	De forma predeterminada, la interfaz de salida para solicitudes de eco ICMP no es especificado. El cliente NQA determina la interfaz de salida en función de la búsqueda en la tabla de enrutamiento.
8. (Opcional). Especifique la dirección IP de origen de las solicitudes de eco ICMP.	- Especifique la dirección IP de la interfaz especificada como dirección IP de origen: **interfaz fuente** *Tipo de interfaz número de interfaz* - Especifique la dirección IP de origen: **IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. Las solicitudes toman la dirección IP principal de la interfaz de salida como su IP de origen. DIRECCIÓN. Si configura tanto el**IP de origen** y **interfaz fuente**comandos, la configuración más reciente entra en vigor. La interfaz de origen especificada debe estar activa. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.
9. (Opcional.) Especifique el siguiente salto para el eco ICMP peticiones.	**siguiente salto***dirección IP*	De forma predeterminada, no se configura ningún siguiente salto.

Configurar la operación DHCP

La operación DHCP mide si el servidor DHCP puede responder a las solicitudes del cliente. DHCP también mide la cantidad de tiempo que le toma al cliente NQA obtener una dirección IP de un servidor DHCP.

El cliente NQA simula el agente de retransmisión DHCP para reenviar solicitudes DHCP para la adquisición de direcciones IP desde el servidor DHCP. La interfaz que realiza la operación DHCP no cambia su dirección IP. Cuando se completa la operación DHCP, el cliente NQA envía un paquete para liberar la dirección IP obtenida.

Para configurar la operación DHCP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de DHCP e ingrese su vista.	**escribe dhcp**	N / A
4. Especifique la dirección IP del servidor DHCP como dirección IP de destino de los paquetes DHCP.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino.
5. (Opcional). Especifique la interfaz de salida para los paquetes de solicitud DHCP.	**interfaz de salida** *Tipo de interfaz número de interfaz*	De forma predeterminada, no se especifica la interfaz de salida para solicitudes DHCP. El cliente NQA determina la interfaz de salida en función de la búsqueda en la tabla de enrutamiento.
6. (Opcional). Especifique la dirección IP de origen de los paquetes de solicitud DHCP.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen para los paquetes de solicitud. Las solicitudes toman la dirección IP de la interfaz de salida como dirección IP de origen. La dirección IP de origen especificada debe ser la dirección IP de una interfaz local y la interfaz local debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda. El cliente NQA agrega la dirección IP de origen al **giaddr**campo en las solicitudes DHCP que se enviarán al servidor DHCP. Para más información sobre el**giaddr**campo, ver *Capa 3: Guía de configuración de servicios IP*.

Configurar la operación DNS

La operación DNS mide el tiempo que tarda el cliente NQA en traducir un nombre de dominio en una dirección IP a través de un servidor DNS.

Una operación DNS simula la resolución de nombres de dominio y no guarda la entrada DNS obtenida.

Para configurar la operación DNS:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.

Paso	Dominio	Observaciones
3. Especifique el tipo de DNS e ingrese su vista.	**escribe dns**	N / A
4. Especifique la dirección IP del servidor DNS como dirección IP de destino de los paquetes DNS.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino.
5. Especifique el nombre de dominio que se traducirá.	**resolver-objetivo***nombre de dominio*	De forma predeterminada, no se especifica ningún nombre de dominio.

Configurar la operación FTP

La operación FTP mide el tiempo que tarda el cliente NQA en transferir o descargar un archivo desde un servidor FTP.

Cuando configure la operación FTP, siga estas restricciones y pautas:

- Cuando realizas el**poner**operación con el**Nombre del archivo**comando configurado, asegúrese de que el archivo exista en el cliente NQA.
- Si obtiene un archivo del servidor FTP, asegúrese de que el archivo especificado en la URL exista en el servidor FTP.
- El cliente NQA no guarda el archivo obtenido del servidor FTP.
- Utilice un archivo pequeño para la operación FTP. Un archivo grande puede provocar un error en la transferencia debido al tiempo de espera o puede afectar a otros servicios por ocupar mucho ancho de banda de la red.

Para configurar la operación FTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de FTP e ingrese su vista.	**escriba ftp**	N / A
4. Especifique la URL del servidor FTP de destino.	**URL***URL*	De forma predeterminada, no se especifica ninguna URL para el servidor FTP de destino. Ingrese la URL en uno de los siguientes formatos: - ftp://*anfitrión*/*Nombre del archivo*. ftp:// - *Puerto host*/*Nombre del archivo*. Cuando realizas el**conseguir**operación, se requiere el nombre del archivo.
5. (Opcional). Especifique la dirección IP de origen de los paquetes de solicitud FTP.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar solicitudes FTP.
6. Especifique el tipo de operación FTP.	**operación**{**conseguir**|**poner**}	De forma predeterminada, el tipo de operación FTP es **conseguir**, lo que significa obtener archivos del servidor FTP.

Paso	Dominio	Observaciones
7. Especifique un nombre de usuario de inicio de sesión FTP.	**nombre de usuario***nombre de usuario*	De forma predeterminada, no se configura ningún nombre de usuario de inicio de sesión FTP.
8. Especifique una contraseña de inicio de sesión FTP.	**contraseña**{**cifrar**|**simple**}*contraseña*	De forma predeterminada, no se configura ninguna contraseña de inicio de sesión FTP.
9. (Opcional). Especifique el nombre de un archivo que se transferirá.	**Nombre del archivo***Nombre del archivo*	De forma predeterminada, no se especifica ningún archivo. Este paso es necesario si realiza la **poner** operación.
10. Configure el modo de transmisión de datos.	**modo**{**activo**|**pasivo**}	El modo predeterminado es**activo**.

Configurar la operación HTTP

Una operación HTTP mide el tiempo que tarda el cliente NQA en obtener datos de un servidor HTTP. Para configurar una operación HTTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo HTTP e ingrese su vista.	**escribe http**	N / A
4. Especifique la URL del servidor HTTP de destino.	**URL***URL*	De forma predeterminada, no se especifica ninguna URL para el servidor HTTP de destino. Ingrese la URL en uno de los siguientes formatos: - http://*anfitrión*/*recurso.* - http://*host: puerto/recurso.*
5. Especifique un nombre de usuario de inicio de sesión HTTP.	**nombre de usuario***nombre de usuario*	De forma predeterminada, no se especifica ningún nombre de usuario de inicio de sesión HTTP.
6. Especifique una contraseña de inicio de sesión HTTP.	**contraseña**{**cifrar**|**simple**}*contraseña*	De forma predeterminada, no se especifica ninguna contraseña de inicio de sesión HTTP.
7. (Opcional). Especifique la dirección IP de origen de los paquetes de solicitud.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de solicitud.
8. Especifique el tipo de operación HTTP.	**operación**{**conseguir**|**correo**|**crudo**}	De forma predeterminada, el tipo de operación HTTP es **conseguir**, lo que significa obtener datos del servidor HTTP.
9. Especifique la versión HTTP.	**versión**{**v1.0**|**v1.1**}	De forma predeterminada, se utiliza HTTP 1.0.
10.(Opcional.) Ingrese a la vista de solicitud sin formato.	**solicitud sin procesar**	Cada vez que ingresa a la vista de solicitud sin formato, se elimina el contenido previamente configurado de la solicitud HTTP.

Paso	Dominio	Observaciones
11.(Opcional.) Especifique el contenido de una solicitud GET para la operación HTTP.	Ingrese o pegue el contenido.	De forma predeterminada, no se especifica ningún contenido. Este paso es necesario para el**crudo** operación.
12. Guarde la entrada y salga a la vista de operación HTTP.	**abandonar**	N / A

Configuración de la operación de fluctuación UDP

PRECAUCIÓN:

Para garantizar operaciones de fluctuación UDP exitosas y evitar afectar los servicios existentes, no realice operaciones en puertos conocidos del 1 al 1023.

Jitter significa variación de retardo entre paquetes. La operación de jitter AUDIP mide jitters unidireccionales y bidireccionales. Puede verificar si la red puede transportar servicios sensibles a la fluctuación, como servicios de voz y vídeo en tiempo real, mediante la operación de fluctuación UDP.

La operación de fluctuación UDP funciona de la siguiente manera:

1. El cliente NQA envía paquetes UDP al puerto de destino con regularidad.
2. El dispositivo de destino toma una marca de tiempo para cada paquete que recibe y luego envía el paquete de regreso al cliente NQA.
3. Al recibir las respuestas, el cliente NQA calcula el jitter según las marcas de tiempo.

La operación de fluctuación UDP requiere tanto el servidor NQA como el cliente NQA. Antes de realizar la operación de fluctuación UDP, configure el servicio de escucha UDP en el servidor NQA. Para obtener más información sobre la configuración del servicio de escucha UDP, consulte "Configurar el servidor NQA".

Para configurar una operación de fluctuación UDP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de fluctuación UDP e ingrese su vista.	**tipo udp-jitter**	N / A
4. Especifique la dirección IP de destino de los paquetes UDP.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino. La dirección IP de destino debe ser la misma que la dirección IP del servicio de escucha en el servidor NQA.
5. Especifique el puerto de destino de los paquetes UDP.	**Puerto de destino***número de puerto*	De forma predeterminada, no se especifica ningún número de puerto de destino. El número de puerto de destino debe ser el mismo que el número de puerto del servicio de escucha en el servidor NQA.
6. (Opcional). Especifique el número de puerto de origen de los paquetes UDP.	**Puerto de origen***número de puerto*	De forma predeterminada, no se especifica ningún número de puerto de origen.

Paso	Dominio	Observaciones
7. (Opcional). Especifique el tamaño de la carga útil en cada paquete UDP.	**tamaño de datos***tamaño*	La configuración predeterminada es 100 bytes.
8. (Opcional). Especifique la cadena de relleno de carga útil para paquetes UDP.	**relleno de datos***cadena*	La cadena predeterminada es el número hexadecimal. 00010203040506070809.
9. (Opcional). Especifique la cantidad de paquetes UDP enviados en una operación de fluctuación UDP.	**número de paquete de sonda** *número de paquete*	La configuración predeterminada es 10.
10.(Opcional.) Configure el intervalo para enviar paquetes UDP.	**intervalo de paquete de sonda** *intervalo de paquetes*	La configuración predeterminada es 20 milisegundos.
11.(Opcional.) Especifique cuánto tiempo espera el cliente NQA por una respuesta del servidor antes de que se considere que se agota el tiempo de respuesta.	**tiempo de espera del paquete de sonda** *tiempo de espera del paquete*	La configuración predeterminada es 3000 milisegundos.
12.(Opcional.) Especifique la dirección IP de origen para los paquetes UDP.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes UDP.

NOTA:

Utilizar el**mostrar resultado nqa**o**mostrar estadísticas de nqa**comando para verificar la operación de fluctuación UDP. El**mostrar el historial de nqa**El comando no muestra los resultados ni las estadísticas de la operación de fluctuación UDP.

Configurar la operación SNMP

La operación SNMP mide el tiempo que tarda el cliente NQA en recibir un paquete de respuesta de un agente SNMP. Para configurar la operación SNMP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de SNMP e ingrese a su vista.	**tipo snmp**	N / A
4. Especifique la dirección IP de destino de los paquetes SNMP.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino.
5. (Opcional). Especifique el puerto de origen de los paquetes SNMP.	**Puerto de origen***número de puerto*	De forma predeterminada, no se especifica ningún número de puerto de origen.

Paso	Dominio	Observaciones
6. (Opcional). Especifique la dirección IP de origen de los paquetes SNMP.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes SNMP.

Configurar la operación TCP

La operación TCP mide el tiempo que tarda el cliente NQA en establecer una conexión TCP a un puerto en el servidor NQA.

La operación TCP requiere tanto el servidor NQA como el cliente NQA. Antes de realizar una operación TCP, configure un servicio de escucha TCP en el servidor NQA. Para obtener más información sobre la configuración del servicio de escucha TCP, consulte "Configurar el servidor NQA".

Para configurar la operación TCP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de TCP e ingrese su vista.	**escribe tcp**	N / A
4. Especifique la dirección IP de destino de los paquetes TCP.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino. La dirección IP de destino debe ser la misma que la dirección IP del servicio de escucha configurado en el servidor NQA.
5. Especifique el puerto de destino de los paquetes TCP.	**Puerto de destino***número de puerto*	De forma predeterminada, no se configura ningún número de puerto de destino. El número de puerto de destino debe ser el mismo que el número de puerto del servicio de escucha en el servidor NQA.
6. (Opcional). Especifique la dirección IP de origen de los paquetes TCP.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes TCP.

Configurar la operación de eco UDP

La operación de eco UDP mide el tiempo de ida y vuelta entre el cliente y un puerto UDP en el servidor NQA.

La operación de eco UDP requiere tanto el servidor NQA como el cliente NQA. Antes de realizar una operación de eco UDP, configure un servicio de escucha UDP en el servidor NQA. Para obtener más información sobre la configuración del servicio de escucha UDP, consulte "Configurar el servidor NQA".

Para configurar la operación de eco UDP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de eco UDP e ingrese su vista.	**escriba udp-echo**	N / A
4. Especifique la dirección IP de destino de los paquetes UDP.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino. La dirección IP de destino debe ser la misma que la dirección IP del servicio de escucha configurado en el servidor NQA.
5. Especifique el puerto de destino de los paquetes UDP.	**Puerto de destino***número de puerto*	De forma predeterminada, no se especifica ningún número de puerto de destino. El número de puerto de destino debe ser el mismo que el número de puerto del servicio de escucha en el servidor NQA.
6. (Opcional). Especifique el tamaño de la carga útil en cada paquete UDP.	**tamaño de datos***tamaño*	La configuración predeterminada es 100 bytes.
7. (Opcional). Especifique la cadena de relleno de carga útil para paquetes UDP.	**relleno de datos***cadena*	La cadena predeterminada es el número hexadecimal. 00010203040506070809.
8. (Opcional). Especifique el puerto de origen de los paquetes UDP.	**Puerto de origen***número de puerto*	De forma predeterminada, no se especifica ningún número de puerto de origen.
9. (Opcional). Especifique la dirección IP de origen de los paquetes UDP.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes UDP.

Configuración de la operación de tracert UDP

La operación UDP tracert determina la ruta de enrutamiento desde el dispositivo de origen al dispositivo de destino. Antes de configurar la operación UDP tracert, realice las siguientes tareas:

- Habilite el envío de mensajes de tiempo excedido ICMP en los dispositivos intermedios entre los dispositivos de origen y de destino. Si los dispositivos intermedios son dispositivos Dahua, utilice el**ip ttl-expires habilitar**dominio.
- Habilite el envío de mensajes ICMP de destino inalcanzable en el dispositivo de destino. Si el dispositivo de destino es un dispositivo Dahua, utilice el**ip inalcanzables habilitar**dominio.

Para más información sobre el**ip ttl-expires habilitar**y**ip inalcanzables habilitar**comandos, ver*Capa 3: referencia de comandos de servicios IP*.

La operación UDP tracert no es compatible con redes IPv6. Para determinar la ruta de enrutamiento que atraviesan los paquetes IPv6 desde el origen hasta el destino, utilice el**tracert ipv6**dominio. Para obtener más información sobre el comando, consulte*Referencia de comandos de monitoreo y administración de redes.*

Para configurar la operación de tracert UDP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de operación de tracert UDP e ingrese su vista.	**escriba udp-tracert**	N / A
4. Especifique la dirección IP de destino de los paquetes UDP.	**IP de destino***dirección IP*	De forma predeterminada, no se configura ninguna dirección IP de destino.
5. (Opcional). Especifique el puerto de destino de los paquetes UDP.	**Puerto de destino***número de puerto*	De forma predeterminada, el número de puerto de destino es 33434. Este número de puerto debe ser un número no utilizado en el dispositivo de destino, para que el dispositivo de destino pueda responder con mensajes de puerto ICMP inalcanzable.
6. (Opcional). Establezca el tamaño de carga útil para cada paquete UDP.	**tamaño de datos***tamaño*	La configuración predeterminada es 100 bytes.
7. (Opcional). Habilite el característica sin fragmentación.	**habilitación sin fragmentos**	De forma predeterminada, la función de no fragmentación está deshabilitada.
8. (Opcional). Configure el número máximo de fallos consecutivos de la sonda.	**fracaso máximo***valor*	La configuración predeterminada es 5.
9. (Opcional). Establezca el valor TTL para los paquetes UDP en la ronda inicial de la operación de seguimiento UDP.	**init-ttl***valor*	La configuración predeterminada es 1.
10.(Opcional.) Especifique una interfaz de salida para paquetes UDP.	**interfaz de salida***tipo de interfaz número de interfaz*	De forma predeterminada, no se especifica la interfaz de salida para paquetes UDP. El cliente NQA determina la interfaz de salida en función de la búsqueda en la tabla de enrutamiento.
11.(Opcional.) Especifique el puerto de origen de UDP. paquetes.	**Puerto de origen***número de puerto*	De forma predeterminada, no se especifica ningún número de puerto de origen.
12.(Opcional.) Especifique la dirección IP de origen de los paquetes UDP.	- Especifique la dirección IP de la interfaz especificada como dirección IP de origen: **interfaz fuente** *Tipo de interfaz número de interfaz* - Especifique la dirección IP de origen: **IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. Los paquetes toman la dirección IP principal de la interfaz de salida como dirección IP de origen. Si configura tanto el**IP de origen** y **interfaz fuente**comandos, la configuración más reciente entra en vigor. La interfaz de origen especificada debe estar activa. La dirección IP de origen debe ser la dirección IP de un local interfaz y la interfaz local debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.

Configurar la operación por voz

PRECAUCIÓN:

Para garantizar operaciones de voz exitosas y evitar afectar los servicios existentes, no realice operaciones en puertos conocidos del 1 al 1023.

La operación de voz mide el rendimiento de la red VoIP.

La operación por voz funciona de la siguiente manera:

1. El cliente NQA envía paquetes de voz a intervalos de envío al dispositivo de destino (servidor NQA).

   Los paquetes de voz son de uno de los siguientes tipos de códec:

   - G.711 Ley A.
   - G.711 ley μ.
   - G.729 Ley A.
2. El dispositivo de destino toma una marca de tiempo para cada paquete de voz que recibe y lo envía de regreso al origen.
3. Al recibir el paquete, el dispositivo de origen calcula la fluctuación y el retraso unidireccional en función de la marca de tiempo.

Los siguientes parámetros que reflejan el rendimiento de la red VoIP se pueden calcular utilizando las métricas recopiladas por la operación de voz:

- **Factor de deterioro de planificación calculado (ICPIF)**—Mide el deterioro de la calidad de la voz en una red VoIP. Se decide por la pérdida y el retraso de paquetes. Un valor más alto representa una calidad de servicio más baja.
- **Puntuaciones medias de opinión (MOS)**—El valor AMOS se puede evaluar utilizando el valor ICPIF, en el rango de 1 a 5. Un valor más alto representa una mayor calidad de servicio.

La evaluación de la calidad de la voz depende de la tolerancia de los usuarios hacia la calidad de la voz. Para usuarios con mayor tolerancia a la calidad de la voz, utilice el**factor de ventaja**comando para configurar el factor de ventaja. Cuando el sistema calcula el valor ICPIF, resta el factor de ventaja para modificar los valores ICPIF y MOS para la evaluación de la calidad de la voz.

La operación de voz requiere tanto el servidor NQA como el cliente NQA. Antes de realizar una operación de voz, configure un servicio de escucha UDP en el servidor NQA. Para obtener más información sobre la configuración del servicio de escucha UDP, consulte "Configurar el servidor NQA".

La operación de voz no se puede repetir.

Para configurar la operación por voz:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de voz y acceda a su vista.	**tipo de voz**	N / A
4. Especifique la dirección IP de destino de los paquetes de voz.	**IP de destino***dirección IP*	De forma predeterminada, no se configura ninguna dirección IP de destino. La dirección IP de destino debe ser la misma que la dirección IP del servicio de escucha en el servidor NQA.

Paso	Dominio	Observaciones
5. Especifique el puerto de destino de los paquetes de voz.	**Puerto de destino***número de puerto*	De forma predeterminada, no se configura ningún número de puerto de destino. El número de puerto de destino debe ser el mismo que el número de puerto del servicio de escucha en el servidor NQA.
6. (Opcional). Especifique el tipo de códec.	**tipo códec**{**g711a**|**g711u**|**g729a**}	De forma predeterminada, el tipo de códec es ley A G.711.
7. (Opcional). Especifique el factor de ventaja para calcular los valores MOS e ICPIF.	**factor de ventaja***factor*	Por defecto, el factor de ventaja es 0.
8. (Opcional). Especifique la dirección IP de origen de los paquetes de voz.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de voz.
9. (Opcional). Especifique el número de puerto de origen de los paquetes de voz.	**Puerto de origen***número de puerto*	De forma predeterminada, no se especifica ningún número de puerto de origen.
10.(Opcional.) Especifique el tamaño de la carga útil en cada paquete de voz.	**tamaño de datos***tamaño*	De forma predeterminada, el tamaño del paquete de voz varía según el tipo de códec. El tamaño de paquete predeterminado es 172 bytes para el tipo de códec de ley G.711A y ley μ G.711, y 32 bytes para el tipo de códec de ley A G.729.
11.(Opcional.) Especifique la cadena de relleno de carga útil para paquetes de voz.	**relleno de datos***cadena*	La cadena predeterminada es el número hexadecimal. 00010203040506070809.
12.(Opcional.) Especifique la cantidad de paquetes de voz que se enviarán en una sonda de voz.	**número de paquete de sonda** *número de paquete*	La configuración predeterminada es 1000.
13.(Opcional.) Especifique el intervalo para enviar paquetes de voz.	**intervalo de paquete de sonda** *intervalo de paquetes*	La configuración predeterminada es 20 milisegundos.
14.(Opcional.) Especifique cuánto tiempo espera el cliente NQA por una respuesta del servidor antes de que se considere que se agota el tiempo de respuesta.	**tiempo de espera del paquete de sonda** *tiempo de espera del paquete*	La configuración predeterminada es 5000 milisegundos.

NOTA:

Utilizar el**mostrar resultado nqa**o**mostrar estadísticas de nqa**Comando para verificar la operación de voz. El **mostrar el historial de nqa**El comando no muestra los resultados ni las estadísticas de la operación de voz.

Configurar la operación DLSw

La operación DLSw mide el tiempo de respuesta de un dispositivo DLSw.

Para configurar la operación DLSw:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo DLSw e ingrese su vista.	**tipo dlsw**	N / A
4. Especifique la dirección IP de destino de los paquetes de sonda.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino.
5. (Opcional). Especifique la dirección IP de origen de los paquetes de sonda.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.

Configuración de la operación de fluctuación de ruta

La operación de fluctuación de ruta mide la fluctuación, la fluctuación negativa y la fluctuación positiva del cliente NQA en cada salto en la ruta hacia el destino.

Antes de configurar la operación de fluctuación de ruta, realice las siguientes tareas:

- Habilite el envío de mensajes de tiempo excedido ICMP en los dispositivos intermedios entre los dispositivos de origen y de destino. Si los dispositivos intermedios son dispositivos Dahua, utilice el**ip ttl-expires habilitar**dominio.
- Habilite el envío de mensajes ICMP de destino inalcanzable en el dispositivo de destino. Si el dispositivo de destino es un dispositivo Dahua, utilice el**ip inalcanzables habilitar**dominio.

Para más información sobre el**ip ttl-expires habilitar**y**ip inalcanzables habilitar**comandos, ver*Capa 3: referencia de comandos de servicios IP*.

Para configurar la operación de fluctuación de ruta:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique el tipo de fluctuación de ruta e ingrese su vista.	**tipo de fluctuación de ruta**	N / A
4. Especifique la dirección IP de destino de las solicitudes de eco ICMP.	**IP de destino***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de destino.
5. (Opcional). Especifique el tamaño de la carga útil en cada eco ICMP. pedido.	**tamaño de datos***tamaño*	La configuración predeterminada es 100 bytes.
6. (Opcional). Especifique la cadena de relleno de carga útil para el eco ICMP. peticiones.	**relleno de datos***cadena*	La cadena predeterminada es el número hexadecimal. 00010203040506070809.

Paso	Dominio	Observaciones
7. Especifique la dirección IP de origen de las solicitudes de eco ICMP.	**IP de origen***dirección IP*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar solicitudes de eco ICMP.
8. (Opcional). Especifique la cantidad de solicitudes de eco ICMP que se enviarán en una operación de fluctuación de ruta.	**número de paquete de sonda** *número de paquete*	La configuración predeterminada es 10.
9. (Opcional.) Especifique el intervalo para enviar eco ICMP peticiones.	**intervalo de paquete de sonda** *intervalo de paquetes*	La configuración predeterminada es 20 milisegundos.
10.(Opcional.) Especifique cuánto tiempo espera el cliente NQA por una respuesta del servidor antes de que se considere que se agota el tiempo de respuesta.	**tiempo de espera del paquete de sonda** *tiempo de espera del paquete*	La configuración predeterminada es 3000 milisegundos.
11.(Opcional.) Especifique una ruta LSR.	**ruta-lsr***dirección IP*&<1-8>	De forma predeterminada, no se especifica ninguna ruta LSR. La operación de fluctuación de ruta utiliza el tracert para detectar la ruta LSR al destino y envía solicitudes de eco ICMP a cada salto en el LSR.
12.(Opcional.) Realice la operación de fluctuación de ruta sólo en el dirección de destino.	**solo objetivo**	De forma predeterminada, la operación de fluctuación de ruta se realiza en cada salto en la ruta hacia el destino.

Configuración de parámetros opcionales para la operación NQA

A menos que se especifique lo contrario, los siguientes parámetros opcionales se aplican a todos los tipos de operaciones NQA. Para configurar parámetros opcionales para una operación NQA:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especificar una NQA tipo de operación e ingrese a su vista.	**tipo**{**DHCP**|**dlsw**|**DNS**|**ftp**| **http**| **eco-icmp**|**nerviosismo en el camino** |**SNMP**|**TCP**|**udp-eco**| **jitter udp**|**udp-tracert**| **voz**}	N / A
4. Configurar una descripción.	**descripción***texto*	De forma predeterminada, no se configura ninguna descripción.
5. Especifique el intervalo en el que se repite la operación NQA.	**frecuencia***intervalo*	Para una operación de voz o fluctuación de ruta, la configuración predeterminada es 60000 milisegundos. Para otras operaciones, la configuración predeterminada es 0 milisegundos. Sólo se realiza una operación. Si la operación no se completa cuando expira el intervalo, la siguiente operación no comienza.

Paso	Dominio	Observaciones
6. Especifique los tiempos de sonda.	**recuento de sondas***veces*	Por defecto: - En una operación de tracert UDP, el cliente NQA realiza tres sondeos en cada salto al destino. - En otros tipos de operaciones, el cliente NQA realiza un sondeo al destino por operación. Este comando no está disponible para las operaciones de voz y fluctuación de ruta. Cada una de estas operaciones realiza solo una sonda.
7. Especificar la sonda tiempo de espera.	**tiempo de espera de la sonda***se acabó el tiempo*	La configuración predeterminada es 3000 milisegundos. Este comando no está disponible para las operaciones de fluctuación de ruta, fluctuación de UDP y voz.
8. Especifique el máximo número de saltos que los paquetes de sonda pueden atravesar.	**ttl***valor*	La configuración predeterminada es 30 para paquetes de sonda de la operación de tracert UDP y es 20 para paquetes de sonda de otros tipos de operaciones. Este comando no está disponible para las operaciones de DHCP y jitter de ruta.
9. Especifique el valor ToS en el encabezado IP de los paquetes de sonda.	**tos***valor*	La configuración predeterminada es 0.
10. Habilite la función de omisión de la tabla de enrutamiento.	**opción de ruta ruta-bypass**	De forma predeterminada, la función de omisión de la tabla de enrutamiento está deshabilitada. Este comando no está disponible para las operaciones de DHCP y jitter de ruta.
11. Especifica la VPN donde está la operación realizado.	**instancia-vpn** *nombre-instancia-vpn*	Por defecto, la operación se realiza en la red pública.

Configurar la función de colaboración

La colaboración se implementa asociando una entrada de reacción de una operación NQA con una entrada de seguimiento. La entrada de reacción monitorea la operación NQA. Si el número de errores de operación alcanza el umbral especificado, se activa la acción configurada.

Para configurar la función de colaboración:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique un tipo de operación NQA e ingrese su vista.	**tipo**{**DHCP**|**dlsw**|**DNS**|**ftp**|**http**|**eco-icmp**|**SNMP**|**TCP**|**udp-eco**}	La función de colaboración no está disponible para las operaciones de fluctuación de ruta, fluctuación de UDP, tracert UDP y voz.

Paso		Dominio	Observaciones
4.	Configure una entrada de reacción.	**reacción***número de artículo* **elemento comprobado tipo de umbral de falla de sonda consecutivo** *ocurrencias consecutivas* **solo disparador de tipo acción**	De forma predeterminada, no se configura ninguna entrada de reacción. No puede modificar el contenido de una entrada de reacción existente.
5.	Salir a la vista del sistema.	**abandonar**	N / A
6.	Pista asociada con NQA.	Ver*Alta disponibilidad Guía de configuración*.	N / A
7.	Asociar Track con un módulo de aplicación.	Ver*Alta disponibilidad Guía de configuración*.	N / A

Configuración de la supervisión de umbrales

Esta función le permite monitorear el estado de ejecución de la operación NQA.

Tipos de umbral

Una operación NQA admite los siguientes tipos de umbral:

- **promedio**—Si el valor promedio de la métrica de rendimiento monitoreada excede el umbral superior o cae por debajo del umbral inferior, se produce una infracción del umbral.
- **acumular**—Si el número total de veces que la métrica de rendimiento supervisada está fuera del rango de valores especificado alcanza o supera el umbral especificado, se produce una infracción del umbral.
- **consecutivo**—Si el número de veces consecutivas que la métrica de rendimiento supervisada está fuera del rango de valores especificado alcanza o supera el umbral especificado, se produce una infracción del umbral.

Las infracciones de umbral para el tipo de umbral promedio o acumulado se determinan por operación de NQA. Las violaciones de umbral para el tipo consecutivo se determinan desde el momento en que comienza la operación NQA.

Acciones desencadenadas

Se podrían desencadenar las siguientes acciones:

- **ninguno**—NQA muestra los resultados sólo en la pantalla del terminal. No envía trampas al NMS.
- **solo trampa**—NQA muestra los resultados en la pantalla del terminal y, mientras tanto, envía trampas al NMS.
- **solo disparador**—NQA muestra los resultados en la pantalla del terminal y, mientras tanto, activa otros módulos para la colaboración.

La operación DNS no admite la acción de enviar mensajes de captura.

Entrada de reacción

En una entrada de reacción, configure un elemento monitoreado, un tipo de umbral y una acción que se activará para implementar la monitorización de umbral.

El estado de una entrada de reacción puede ser no válido, estar por encima del umbral o por debajo del umbral.

- Antes de que comience una operación NQA, la entrada de reacción está en estado no válido.
- Si se viola el umbral, el estado de la entrada se establece por encima del umbral. De lo contrario, el estado de la entrada se establece por debajo del umbral.

Si la acción está configurada como**solo trampa**para una entrada de reacción, se envía un mensaje de captura al NMS cuando cambia el estado de la entrada.

Procedimiento de configuración

Antes de configurar la supervisión de umbral, configure la dirección de destino de los mensajes de captura mediante el comando**host-destino del agente snmp**dominio. Para obtener más información sobre el comando, consulte*Referencia de comandos de monitoreo y administración de red*.

Para configurar la supervisión de umbral:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Crear una NQA operación y entrar NQA vista de operación.	**entrada nqa***nombre-administrador etiqueta-operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Introduzca NQA vista de operación.	**tipo**{**DHCP**|**dlsw**|**DNS**|**ftp**|**http**|**eco-icmp** | **SNMP**|**TCP**|**udp-eco**|**jitter udp** |**udp-tracert**| **voz**}	La fluctuación de ruta no admite la supervisión de umbrales.
4. Habilitar envío trampas al NMS cuando son específicas las condiciones son reunió.	**trampa de reacción**{**cambio de ruta**|**fallo de la sonda** *fallos-de-sonda-secutivos*|**prueba completa**| **fracaso de la prueba**[*fallos-de-sondeo-acumulados*] }	De forma predeterminada, no se envían capturas al NMS. Las operaciones de voz y fluctuación UDP solo admiten la **prueba completa**palabra clave. La operación UDP tracert admite la**cambio de ruta**, **prueba completa**, y **fracaso de la prueba**palabras clave.

Paso	Dominio	Observaciones
5. Configurar límite supervisión.	- Supervise la duración de la operación (no compatible con las operaciones de voz y fluctuación UDP): **reacción***número de artículo***elemento-marcado duración-sonda-tipo-umbral** {**acumular***ocurrencias acumuladas*| **promedio**|**consecutivo** *ocurrencias consecutivas*}**valor umbral** *umbral superior umbral inferior* [**tipo de acción**{**ninguno**|**solo trampa**}] - Supervise los tiempos de falla (no admitido en las operaciones de voz y fluctuación UDP): **reacción***número de artículo***tipo de umbral de fallo de sonda de elemento comprobado**{ **acumular** *ocurrencias acumuladas*|**consecutivo** *ocurrencias consecutivas*} [**tipo de acción** { **ninguno**|**solo trampa**}] - Supervise el tiempo de ida y vuelta (solo para operaciones de voz y fluctuación en UDP): **reacción***número de artículo***tipo de umbral rtt de elemento marcado**{**acumular** *ocurrencias acumuladas*|**promedio**} **valor umbral***umbral superior umbral inferior*[**tipo de acción**{**ninguno**| **solo trampa**}] - Supervise la pérdida de paquetes (solo para operaciones de voz y fluctuación UDP): **reacción***número de artículo***elemento-marcado-pérdida-de-paquetes-tipo-umbral-acumular** *ocurrencias acumuladas*[**tipo de acción** {**ninguno** |**solo trampa**}] - Supervise la fluctuación unidireccional (solo para las operaciones de voz y fluctuación UDP): **reacción***número de artículo***elemento comprobado** {**nerviosismo**|**jitter-sd**}**tipo de umbral** {**acumular***ocurrencias acumuladas*| **promedio**}**valor umbral***umbral superior umbral inferior*[**tipo de acción**{**ninguno**| **solo trampa**}] - Supervise el retraso unidireccional (solo para las operaciones de voz y fluctuación UDP): **reacción***número de artículo***elemento comprobado** {**owd-ds**|**owd-sd**}**valor umbral** *umbral superior umbral inferior* - Monitoree el valor ICPIF (solo para la operación por voz): **reacción***número de artículo***valor umbral icpif de elemento comprobado***umbral superior umbral** *inferior*[**tipo de acción**{**ninguno**| **solo trampa**}] - Monitoree el valor MOS (solo para la operación por voz): **reacción***número de artículo***valor umbral mos del elemento marcado***umbral superior umbral** *inferior*[**tipo de acción**{**ninguno**| **solo trampa**}]	N / A

Configuración de la función de recopilación de estadísticas de NQA

NQA forma estadísticas dentro del mismo intervalo de recopilación que un grupo de estadísticas. Para mostrar información sobre los grupos de estadísticas, utilice el**mostrar estadísticas de nqa**dominio.

NQA no genera ningún grupo de estadísticas para la operación que se ejecuta una vez. Para configurar la operación NQA para que se ejecute solo una vez, use el**frecuencia**comando para establecer el intervalo en 0 milisegundos.

Para configurar la función de recopilación de estadísticas de NQA:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una operación NQA e ingrese a la vista de operaciones NQA.	**entrada nqa***nombre-administrador etiqueta de operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Especifique un tipo de operación NQA e ingrese su vista.	**tipo**{**DHCP**|**dlsw**|**DNS**|**ftp**| **http**| **eco-icmp**|**nerviosismo en el camino**| **SNMP**|**TCP**|**udp-eco**| **jitter udp**|**voz**}	La operación UDP tracert no admite la función de recopilación de estadísticas de NQA.
4. (Opcional). Especifique el intervalo para recopilar las estadísticas.	**intervalo de estadísticas***intervalo*	La configuración predeterminada es 60 minutos.
5. (Opcional). Especifique el número máximo de grupos de estadísticas que se pueden guardar.	**grupo máximo de estadísticas***número*	La configuración predeterminada es dos grupos. Para desactivar la recopilación de estadísticas NQA, establezca el número máximo en 0. Cuando se alcanza el número máximo de grupos de estadísticas, para guardar un nuevo grupo de estadísticas, se elimina el grupo de estadísticas más antiguo.
6. (Opcional). Especifique el tiempo de espera de los grupos de estadísticas.	**tiempo de espera de estadísticas***hora de espera*	La configuración predeterminada es 120 minutos. Un grupo de estadísticas se elimina cuando expira su tiempo de retención.

Configurar el guardado de registros históricos de NQA

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Crear una NQA operación y entrar Vista de operación NQA.	**entrada nqa***nombre-administrador etiqueta-operación*	De forma predeterminada, no se crea ninguna operación NQA.
3. Ingrese a la operación NQA tipo vista.	**tipo**{**DHCP**|**dlsw**|**DNS**|**ftp**|**http**| **eco-icmp**|**SNMP**|**TCP**|**udp-eco**| **udp-tracert**}	Las operaciones de fluctuación UDP, fluctuación de ruta y voz no Admite guardar registros históricos.
4. Habilite el guardado de registros históricos para la operación NQA.	**habilitar registro histórico**	De forma predeterminada, esta función está habilitada solo para la operación de tracert UDP.
5. (Opcional). Configure el vida de la historia registros.	**tiempo de mantenimiento del registro histórico***Mantén el tiempo*	La configuración predeterminada es 120 minutos. Un registro se elimina cuando se alcanza su vida útil.

Paso	Dominio	Observaciones
6. (Opcional). Especifique el número máximo de registros históricos que se pueden guardar.	**número de registro histórico***número*	La configuración predeterminada es 50. Si se alcanza el número máximo de registros históricos para una operación NQA, se eliminan los registros históricos más antiguos.
7. (Opcional.) Pantalla Registros históricos de la NQA.	**mostrar el historial de nqa**	N / A

Programación de la operación NQA en el cliente NQA

La operación NQA funciona entre la hora de inicio especificada y la hora de finalización (la hora de inicio más la duración de la operación). Si la hora de inicio especificada está adelantada a la hora del sistema, la operación comienza inmediatamente. Si tanto la hora de inicio como la hora de finalización especificadas están por delante de la hora del sistema, la operación no se inicia. Para mostrar la hora actual del sistema, utilice el**reloj de pantalla**dominio.

Cuando programe una operación NQA, siga estas restricciones y pautas:

- No puede ingresar a la vista de tipo de operación o a la vista de operación de una operación NQA programada.
- Un ajuste de hora del sistema no afecta las operaciones NQA iniciadas o completadas. Afecta únicamente a las operaciones de NQA que no han comenzado.

Para programar la operación NQA en el cliente NQA:

Paso	Dominio
1. Ingrese a la vista del sistema.	**vista del sistema**
2. Especificar la programación parámetros para una operación NQA.	**horario nqa***nombre-administrador etiqueta-operación***hora de inicio**{*hh:mm:ss* [*aaaa/mm/dd*| *dd/mm/aaaa*] |**ahora**}**toda la vida**{*toda la vida*|**para siempre**} [**periódico**]

Configuración de plantillas NQA en el cliente NQA

Una plantilla NQA es un conjunto de parámetros de operación, como la dirección de destino, el número de puerto de destino y la URL del servidor de destino. Puede utilizar una plantilla NQA en equilibrio de carga, supervisión del estado y otros módulos de funciones para proporcionar estadísticas de prueba. Puede crear varias plantillas en un dispositivo y cada plantilla debe tener un nombre exclusivo.

La plantilla NQA admite los tipos de operaciones ICMP, DNS, HTTP, TCP, UDP y FTP.

Algunos parámetros de operación para una plantilla NQA se pueden especificar mediante la configuración de la plantilla o la función que utiliza la plantilla. Cuando se especifican ambos, los parámetros de la configuración de la plantilla entran en vigor. Por ejemplo, el equilibrio de carga del servidor utiliza la plantilla ICMP de NQA para la supervisión del estado. Si la dirección IP de destino en la plantilla es diferente de la dirección del servidor real, la dirección IP de destino en la plantilla entra en vigor.

Lista de tareas de configuración de plantilla NQA

Tareas de un vistazo
(Obligatorio.) Realice al menos una de las siguientes tareas: - Configurar la plantilla ICMP - Configurar la plantilla DNS - Configurar la plantilla TCP - Configurar la plantilla UDP - Configurar la plantilla HTTP - Configurar la plantilla FTP
(Opcional.)Configuración de parámetros opcionales para la plantilla NQA

Configurar la plantilla ICMP

Una función que utiliza la plantilla ICMP realiza la operación ICMP para medir la accesibilidad de un dispositivo de destino. La plantilla ICMP es compatible con redes IPv4 e IPv6.

Para configurar la plantilla ICMP:

Paso	**Dominio**	**Observaciones**
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una plantilla ICMP e ingrese a su vista.	**plantilla nqa icmp***nombre*	N / A
3. (Opcional). Especifique la dirección IP de destino de la operación.	- Dirección IPv4: **IP de destino***dirección IP* - Dirección IPv6: **destino ipv6** *dirección ipv6*	De forma predeterminada, no se configura ninguna dirección IP de destino.
4. (Opcional). Especifique el tamaño de la carga útil en cada solicitud ICMP.	**tamaño de datos***tamaño*	La configuración predeterminada es 100 bytes.
5. (Opcional). Especifique la cadena de relleno de carga útil para las solicitudes.	**relleno de datos***cadena*	La cadena predeterminada es el número hexadecimal. 00010203040506070809.
6. (Opcional). Especifique la dirección IP de la interfaz especificada como la dirección IP de origen de las solicitudes de eco ICMP.	**interfaz fuente***tipo de interfaz número de interfaz*	De forma predeterminada, no se especifica ninguna dirección IP de origen. Las solicitudes utilizan la dirección IP principal de la interfaz de salida como su IP de origen. DIRECCIÓN. Si configura el**interfaz fuente**comando con el **IP de origen**o**fuente ipv6** comando, la configuración más reciente entra en vigor. La interfaz de origen especificada debe estar activa.

Paso	Dominio	Observaciones
7. (Opcional). Especifique la dirección IP de origen de los paquetes de sonda.	- Dirección IPv4: **IP de origen***dirección IP* - Dirección IPv6: **fuente ipv6***dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.

Configurar la plantilla DNS

Una función que utiliza la plantilla DNS realiza la operación DNS para determinar el estado del servidor. Es compatible con redes IPv4 e IPv6.

En la vista de plantilla DNS, puede especificar la dirección que se espera que se devuelva. Si las direcciones IP devueltas incluyen la dirección esperada, el servidor DNS es válido y la operación se realiza correctamente. De lo contrario, la operación falla.

Cree una asignación entre el nombre de dominio y una dirección antes de realizar la operación DNS. Para obtener información sobre la configuración del servidor DNS, consulte*Capa 3: Guía de configuración de servicios IP*.

Para configurar la plantilla DNS:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una plantilla DNS e ingrese a la vista de plantilla DNS.	**plantilla nqa dns***nombre*	N / A
3. (Opcional). Especifique la dirección IP de destino de los paquetes DNS.	- Dirección IPv4: **IP de destino***dirección IP* - Dirección IPv6: **destino ipv6***dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de destino.
4. (Opcional). Configure el número de puerto de destino para la operación.	**Puerto de destino***número de puerto*	De forma predeterminada, el número del puerto de destino es 53.
5. Especifique el nombre de dominio que debe traducirse.	**resolver-objetivo***nombre de dominio*	De forma predeterminada, no se especifica ningún nombre de dominio.
6. Configure el tipo de resolución del nombre de dominio.	**tipo de resolución**{**A**|**AAAA**}	Por defecto, el tipo es el tipo A. Una consulta de tipo A resuelve un nombre de dominio en una dirección IPv4 asignada y una consulta de tipo AAAA en una dirección IPv6 asignada. DIRECCIÓN.
7. (Opcional). Especifique la dirección IP de origen de los paquetes de sonda.	- Dirección IPv4: **IP de origen***dirección IP* - Dirección IPv6: **fuente ipv6***dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de un local interfaz, y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.
8. (Opcional). Configure el puerto de origen para los paquetes de sonda.	**Puerto de origen***número de puerto*	De forma predeterminada, no se configura ningún número de puerto de origen.

Paso	Dominio	Observaciones
9. (Opcional). Especifique la dirección IP que se espera que se devuelva.	- Dirección IPv4: **esperar ip***dirección IP* - Dirección IPv6: **esperar ipv6***dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP esperada.

Configurar la plantilla TCP

Una característica que utiliza la plantilla TCP realiza la operación TCP para probar los siguientes elementos:

- Si el cliente NQA puede establecer una conexión TCP a un puerto específico en el servidor.
- Si el servicio solicitado está disponible en el servidor.

En la vista de plantilla TCP, puede especificar los datos que se espera que se devuelvan. Si no especifica los datos esperados, la operación TCP solo prueba si el cliente puede establecer una conexión TCP con el servidor.

La operación TCP requiere tanto el servidor NQA como el cliente NQA. Antes de realizar una operación TCP, configure un servicio de escucha TCP en el servidor NQA. Para obtener más información sobre la configuración del servicio de escucha TCP, consulte "Configurar el servidor NQA".

Para configurar la plantilla TCP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una plantilla TCP e ingrese a su vista.	**plantilla tcp nqa***nombre*	N / A
3. (Opcional). Especifique la dirección IP de destino de la operación.	- Dirección IPv4: **IP de destino***dirección IP* - Dirección IPv6: **destino ipv6***dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de destino. La dirección IP de destino debe ser la misma que la dirección IP del servicio de escucha configurado en el servidor NQA.
4. (Opcional). Configure el número de puerto de destino para la operación.	**Puerto de destino***número de puerto*	De forma predeterminada, no se configura ningún número de puerto de destino. El número de puerto de destino debe ser el mismo que el número de puerto del servicio de escucha en el servidor NQA.
5. (Opcional). Especifique la cadena de relleno de carga útil para las solicitudes.	**relleno de datos***cadena*	La cadena predeterminada es el número hexadecimal. 00010203040506070809.
6. (Opcional). Especifique la dirección IP de origen de los paquetes de sonda.	- Dirección IPv4: **IP de origen***dirección IP* - Dirección IPv6: **fuente ipv6***dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de un local interfaz, y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.
7. (Opcional). Configure los datos esperados.	**esperar datos***expresión*[**compensar** *número*]	De forma predeterminada, no se configuran datos esperados. Los datos esperados se verifican solo cuando configura tanto el **relleno de datos**y**datos esperados** comandos.

Configurar la plantilla UDP

Una característica que utiliza la plantilla UDP realiza la operación UDP para probar los siguientes elementos:

- Accesibilidad de un puerto específico en el servidor NQA.
- Disponibilidad del servicio solicitado en el servidor de NQA.

En la vista de plantilla UDP, puede especificar los datos que se espera que se devuelvan. Si no especifica los datos esperados, la operación UDP solo prueba si el cliente puede recibir el paquete de respuesta del servidor.

La operación UDP requiere tanto el servidor NQA como el cliente NQA. Antes de realizar una operación UDP, configure un servicio de escucha UDP en el servidor NQA. Para obtener más información sobre la configuración del servicio de escucha UDP, consulte "Configurar el servidor NQA".

Para configurar la plantilla UDP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una plantilla UDP y acceda a su vista.	**plantilla nqa udp***nombre*	N / A
3. (Opcional). Especifique la dirección IP de destino para la operación.	- Dirección IPv4: **IP de destino***dirección IP* - Dirección IPv6: **destino ipv6** *dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de destino. La dirección IP de destino debe ser la misma que la dirección IP del servicio de escucha configurado en el servidor NQA.
4. (Opcional). Configure el número de puerto de destino para la operación.	**Puerto de destino***número de puerto*	De forma predeterminada, no se configura ningún número de puerto de destino. El número de puerto de destino debe ser el mismo que el número de puerto del servicio de escucha en el servidor NQA.
5. (Opcional). Especifique la cadena de relleno de carga útil para los paquetes de sonda.	**relleno de datos***cadena*	La cadena predeterminada es el número hexadecimal 00010203040506070809.
6. (Opcional). Establezca el tamaño de carga útil para los paquetes de sonda.	**tamaño de datos***tamaño*	La configuración predeterminada es 100 bytes.
7. (Opcional). Especifique la dirección IP de origen de los paquetes de sonda.	- Dirección IPv4: **IP de origen***dirección IP* - Dirección IPv6: **fuente ipv6***dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.
8. (Opcional). Configure los datos esperados.	**esperar datos***expresión*[**compensar** *número*]	De forma predeterminada, no se configuran datos esperados. Si desea configurar este comando, asegúrese de que**relleno de datos** El comando ya está ejecutado.

Configurar la plantilla HTTP

Una función que utiliza la plantilla HTTP realiza la operación HTTP para medir el tiempo que le toma al cliente NQA obtener datos de un servidor HTTP.

Los datos esperados se verifican solo cuando están configurados y la respuesta HTTP contiene el campo Longitud del contenido en el encabezado HTTP. El campo Longitud del contenido indica la longitud del cuerpo del paquete y

no incluye la longitud del encabezado. Un paquete HTTP con este campo indica que los datos del paquete no incluyen el tipo multiparte y que el cuerpo del paquete es un tipo de datos.

El código de estado del paquete HTTP es un campo de tres dígitos en notación decimal e incluye la información de estado del servidor HTTP. El primer dígito define la clase de respuesta y los dos últimos dígitos no tienen ninguna función de categorización.

Configure el servidor HTTP antes de realizar la operación HTTP.

Para configurar la plantilla HTTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una plantilla HTTP e ingrese a su vista.	**plantilla nqa http***nombre*	N / A
3. Especifique la URL del servidor HTTP de destino.	**URL***URL*	De forma predeterminada, no se especifica ninguna URL para el servidor HTTP de destino. Ingrese la URL en uno de los siguientes formatos: - http://*anfitrión*/*recurso*. http:// - *anfitrión*:*puerto*/*recurso*.
4. Especifique un nombre de usuario de inicio de sesión HTTP.	**nombre de usuario***nombre de usuario*	De forma predeterminada, no se especifica ningún nombre de usuario de inicio de sesión HTTP.
5. Especifique una contraseña de inicio de sesión HTTP.	**contraseña**{**cifrar**|**simple**}*contraseña*	De forma predeterminada, no se especifica ninguna contraseña de inicio de sesión HTTP.
6. Especifique el tipo de operación HTTP.	**operación**{**conseguir**|**correo**|**crudo**}	De forma predeterminada, el tipo de operación HTTP es **conseguir**, lo que significa obtener datos del servidor HTTP. en el HTTP**crudo**operación, utilice el **solicitud sin procesar**comando para especificar el contenido de la solicitud GET que se enviará al servidor HTTP.
7. (Opcional). Ingrese a la vista de solicitud sin formato.	**solicitud sin procesar**	Este paso es necesario para el**crudo** operación. Cada vez que ingresa a la vista de solicitud sin formato, se elimina el contenido previamente configurado de la solicitud GET.
8. (Opcional). Ingrese o pegue el contenido de la solicitud GET para la operación HTTP.	N / A	Este paso es necesario para el**crudo** operación. De forma predeterminada, no se especifica ningún contenido.
9. (Opcional). Guarde la entrada y salga a la vista de plantilla HTTP.	**abandonar**	N / A
10.(Opcional.) Especifique la dirección IP de origen de la sonda. paquetes.	- Dirección IPv4: **IP de origen***dirección IP* - Dirección IPv6: **fuente ipv6** *dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.
11.(Opcional.) Configure los códigos de estado esperados.	**esperar estado***lista de estado*	De forma predeterminada, no se configura ningún código de estado esperado.
12.(Opcional.) Configure los datos esperados.	**esperar datos***expresión* [**compensar***número*]	De forma predeterminada, no se configuran datos esperados.

Configurar la plantilla FTP

Una función que utiliza la plantilla FTP realiza la operación FTP. La operación mide el tiempo que le toma al cliente NQA transferir un archivo o descargarlo desde un servidor FTP.

Configure el nombre de usuario y la contraseña para que el cliente FTP inicie sesión en el servidor FTP antes de realizar una operación FTP. Para obtener información sobre la configuración del servidor FTP, consulte*Guía de configuración básica*.

Para configurar la plantilla FTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una plantilla FTP y acceda a su vista.	**plantilla ftp nqa***nombre*	N / A
3. Especifique la URL del servidor FTP de destino.	**URL***URL*	De forma predeterminada, no se especifica ninguna URL para el servidor FTP de destino. Ingrese la URL en uno de los siguientes formatos: - ftp://*anfitrión*/*Nombre del archivo*. ftp:// - *anfitrión*:*puerto*/*Nombre del archivo*. Cuando realizas el**conseguir**operación, se requiere el nombre del archivo. Cuando realizas el**poner**operación, el*Nombre del archivo*El argumento no tiene efecto, incluso si se especifica. El nombre del archivo para el**poner**El funcionamiento está determinado por el**Nombre del archivo**dominio.
4. (Opcional). Especifique el tipo de operación FTP.	**operación**{**conseguir**|**poner**}	De forma predeterminada, el tipo de operación FTP es **conseguir**, lo que significa obtener archivos del servidor FTP.
5. Especifique un nombre de usuario de inicio de sesión FTP.	**nombre de usuario***nombre de usuario*	De forma predeterminada, no se especifica ningún nombre de usuario de inicio de sesión FTP.
6. Especifique una contraseña de inicio de sesión FTP.	**contraseña**{**cifrar**|**simple**} *contraseña*	De forma predeterminada, no se especifica ninguna contraseña de inicio de sesión FTP.
7. (Opcional). Especifique el nombre de un archivo que se transferirá.	**Nombre del archivo***Nombre del archivo*	Este paso es necesario si realiza la **poner** operación. Esta configuración no tiene efecto para el **conseguir**operación. De forma predeterminada, no se especifica ningún archivo.
8. Configure el modo de transmisión de datos.	**modo**{**activo**|**pasivo**}	El modo predeterminado es**activo**.
9. (Opcional). Especifique la dirección IP de origen de los paquetes de sonda.	- Dirección IPv4: **IP de origen***dirección IP* - Dirección IPv6: **fuente ipv6***dirección ipv6*	De forma predeterminada, no se especifica ninguna dirección IP de origen. La dirección IP de origen debe ser la dirección IP de una interfaz local y la interfaz debe estar activa. De lo contrario, no se podrán enviar paquetes de sonda.

Configuración de parámetros opcionales para la plantilla NQA

A menos que se especifique lo contrario, los siguientes parámetros opcionales se aplican a todos los tipos de plantillas

NQA. La configuración de los parámetros solo tiene efecto en la plantilla NQA actual.

Para configurar parámetros opcionales para una plantilla NQA:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una plantilla NQA e ingrese a su vista.	**plantilla nqa**{**DNS**|**ftp**| **http**| **ICMP**|**TCP**|**udp**}*nombre*	N / A
3. Configurar una descripción.	**descripción***texto*	De forma predeterminada, no se configura ninguna descripción.
4. Especifique el intervalo en el que se repite la operación NQA.	**frecuencia***intervalo*	La configuración predeterminada es 5000 milisegundos. Si la operación no se completa cuando expira el intervalo, la siguiente operación no comienza.
5. Especificar la sonda tiempo de espera.	**tiempo de espera de la sonda***se acabó el tiempo*	La configuración predeterminada es 3000 milisegundos.
6. Especifique el TTL para los paquetes de sonda.	**ttl***valor*	La configuración predeterminada es 20.
7. Especifique el valor ToS en el encabezado IP de los paquetes de sonda.	**tos***valor*	La configuración predeterminada es 0.
8. Especifica la VPN donde está la operación realizado.	**instancia-vpn** *nombre-instancia-vpn*	Por defecto, la operación se realiza en la red pública.
9. Configurar el número de éxitos consecutivos sondas que conduzcan a una operación exitosa.	**gatillo de reacción-paso de sonda** *contar*	La configuración predeterminada es 3. Si se alcanza el número de sondeos exitosos consecutivos para una operación NQA, el cliente NQA notifica a la función que utiliza la plantilla del evento de operación exitosa.
10. Configurar el número de sondas consecutivas fallas que conducen a una falla en la operación.	**Fallo de sonda de activación de reacción** *contar*	La configuración predeterminada es 3. Si se alcanza el número de errores de sondeo consecutivos para una operación NQA, el cliente NQA notifica el error de la operación a la función que utiliza la plantilla NQA.

Visualización y mantenimiento de NQA

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Muestra registros históricos de operaciones de NQA.	**mostrar el historial de nqa**[*nombre-administrador etiqueta-operación*]
Muestra los resultados de monitoreo actuales de las entradas de reacción.	**mostrar contadores de reacciones nqa**[*nombre-administrador etiqueta-operación* [*número de artículo*]]
Muestra el resultado más reciente de la operación NQA.	**mostrar resultado nqa**[*nombre-administrador etiqueta-operación*]
Mostrar estadísticas de NQA.	**mostrar estadísticas de nqa**[*nombre-administrador etiqueta-operación*]
Muestra el estado del servidor NQA.	**mostrar el estado del servidor nqa**

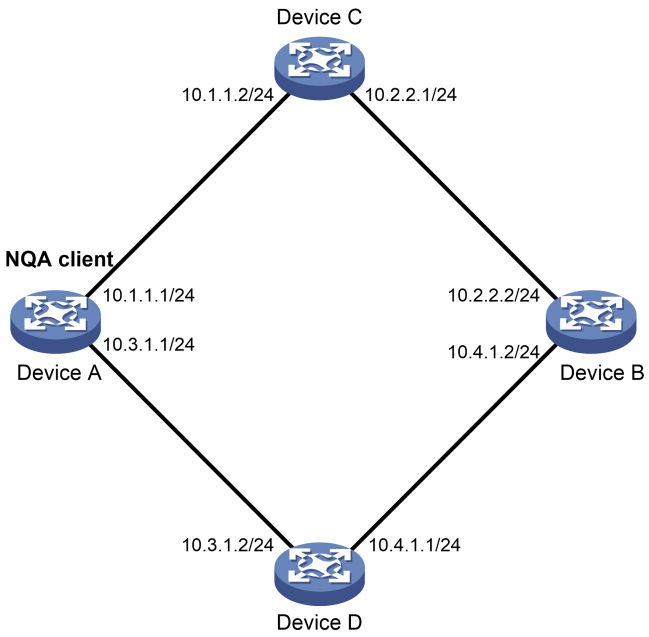
Ejemplos de configuración de NQA

Ejemplo de configuración de operación de eco ICMP

Requisitos de red

Como se muestra enfigura 3, configure una operación de eco ICMP desde el dispositivo A del cliente NQA al dispositivo B para probar el tiempo de ida y vuelta. El siguiente salto del Dispositivo A es el Dispositivo C.

Figura 3 Diagrama de red



Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crea una operación de eco ICMP.

<DispositivoA> vista del sistema

[DispositivoA] prueba de administrador de entrada nqa1

[DispositivoA-nqa-admin-test1] escriba icmp-echo

Especifique la dirección IP de destino de las solicitudes de eco ICMP como 10.2.2.2.

[DeviceA-nqa-admin-test1-icmp-echo] IP de destino 10.2.2.2

Configure 10.1.1.2 como el siguiente salto. Las solicitudes de eco ICMP se envían a través del Dispositivo C al Dispositivo B.

[DeviceA-nqa-admin-test1-icmp-echo] siguiente salto 10.1.1.2

Configure la operación de eco ICMP para realizar 10 sondas.

[DeviceA-nqa-admin-test1-icmp-echo] recuento de sondas 10

Especifique el tiempo de espera de la sonda para la operación de eco ICMP como 500 milisegundos.

[DeviceA-nqa-admin-test1-icmp-echo] Tiempo de espera de sonda 500

Configure la operación de eco ICMP para que se repita cada 5000 milisegundos.

[DeviceA-nqa-admin-test1-icmp-echo] frecuencia 5000

Habilite el guardado de registros del historial.

[DeviceA-nqa-admin-test1-icmp-echo] habilitación de registro histórico

Configure el número máximo de registros del historial que se pueden guardar como 10.

[DeviceA-nqa-admin-test1-icmp-echo] registro histórico número 10 [DeviceA-nqa-admin-test1-icmp-echo] salir

Inicie la operación de eco ICMP.

[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

Después de que la operación de eco ICMP se ejecute durante un período de tiempo, detenga la operación.

[DispositivoA] deshacer la prueba de administrador de programación nqa1

Muestra el resultado más reciente de la operación de eco ICMP.

[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA (admin admin, etiqueta test1) resultados de la prueba:

Enviar tiempos de operación: 10 Recibir tiempos de respuesta: 10

Tiempo mínimo/máximo/promedio de ida y vuelta: 2/5/3

Cuadrado-Suma del tiempo de ida y vuelta: 96

Hora de la última sonda realizada con éxito: 2011-08-23 15:00:01.2

Resultados extendidos:

Ratio de pérdida de paquetes: 0% Fallos por tiempo de espera: 0 Fallos por error interno: 0 Fallos por otros errores: 0

Muestra los registros históricos de la operación de eco ICMP.

[DispositivoA] muestra la prueba de administrador del historial nqa1

Registros del historial de entradas NQA (administrador, prueba de etiquetas):

Índice	Respuesta	Estado	Tiempo	
370	3	Tuvo éxito	2007-08-23	15:00:01.2
369	3	Tuvo éxito	2007-08-23	15:00:01.2
368	3	Tuvo éxito	2007-08-23	15:00:01.2
367	5	Tuvo éxito	2007-08-23	15:00:01.2
366	3	Tuvo éxito	2007-08-23	15:00:01.2
365	3	Tuvo éxito	2007-08-23	15:00:01.2
364	3	Tuvo éxito	2007-08-23	15:00:01.1
363	2	Tuvo éxito	2007-08-23	15:00:01.1
362	3	Tuvo éxito	2007-08-23	15:00:01.1
361	2	Tuvo éxito	2007-08-23	15:00:01.1

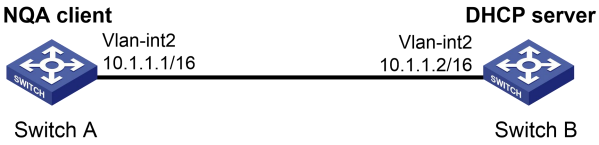
El resultado muestra que los paquetes enviados por el dispositivo A pueden llegar al dispositivo B a través del dispositivo C. No se produce ninguna pérdida de paquetes durante la operación. Los tiempos mínimo, máximo y promedio de ida y vuelta son 2, 5 y 3 milisegundos, respectivamente.

Ejemplo de configuración de operación DHCP

Requisitos de red

Como se muestra enFigura 4, configure una operación DHCP para probar el tiempo necesario para que el conmutador A obtenga una dirección IP del servidor DHCP (conmutador B).

Figura 4 Diagrama de red



Procedimiento de configuración

Crea una operación DHCP.

<SwitchA> vista del sistema

[SwitchA] nqa entrada admin test1 [SwitchA-nqa-admin-test1] tipo dhcp

Especifique la dirección del servidor DHCP 10.1.1.2 como dirección de destino.

[SwitchA-nqa-admin-test1-dhcp] IP de destino 10.1.1.2

Habilite el guardado de registros históricos.

[SwitchA-nqa-admin-test1-dhcp] habilitar registro histórico [SwitchA-nqa-admin-test1-dhcp] salir

Inicie la operación DHCP.

[SwitchA] nqa programar administrador test1 hora de inicio ahora de por vida para siempre

Después de que la operación DHCP se ejecute durante un período de tiempo, detenga la operación.

[SwitchA] deshacer la prueba de administrador de programación nqa1

Muestra el resultado más reciente de la operación DHCP.

```
[SwitchA] muestra el resultado de nqa admin test1 Entrada NQA
(admin admin, etiqueta test1) resultados de la prueba:
    Enviar tiempos de operación: 1                Recibir tiempos de respuesta: 1
    Tiempo mínimo/máximo/promedio de ida y vuelta: 512/512/512
    Cuadrado-Suma del tiempo de ida y vuelta: 262144
    Hora de la última sonda realizada con éxito: 2011-11-22 09:56:03.2
  Resultados extendidos:
    Ratio de pérdida de paquetes: 0% Fallos por
    tiempo de espera: 0 Fallos por error interno:
    0 Fallos por otros errores: 0
```

Muestra los registros históricos de la operación DHCP.

```
[SwitchA] muestra la prueba de administrador del historial de nqa1
Registros del historial de entradas NQA (admin admin, etiqueta test1):
  Índice      Respuesta   Estado          Tiempo
  1           512         Tuvo éxito      2011-11-22 09:56:03.2
```

El resultado muestra que al Switch A le tomó 512 milisegundos obtener una dirección IP del servidor DHCP.

Ejemplo de configuración de operación DNS

Requisitos de red

Como se muestra enFigura 5, configure una operación DNS para probar si el Dispositivo A puede realizar la resolución de direcciones a través del servidor DNS y probar el tiempo de resolución.

Figura 5 Diagrama de red

Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crear una operación DNS.

<DispositivoA> vista del sistema

[DispositivoA] prueba de administrador de entrada

nqa1 [DispositivoA-nqa-admin-test1] tipo dns

Especifique la dirección IP del servidor DNS 10.2.2.2 como dirección de destino.

[DeviceA-nqa-admin-test1-dns] IP de destino 10.2.2.2

Especifique el nombre de dominio que se traducirá como**anfitrión.com**.

[DispositivoA-nqa-admin-test1-dns] resolver-objetivo host.com

Habilite el guardado de registros históricos.

[DispositivoA-nqa-admin-test1-dns] habilitar registro histórico

[DispositivoA-nqa-admin-test1-dns] abandonar

Inicie la operación DNS.

[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

Después de que la operación DNS se ejecute durante un período de tiempo, detenga la operación.

[DispositivoA] deshacer la prueba de administrador de programación nqa1

Muestra el resultado más reciente de la operación DNS.

[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA

(admin admin, etiqueta test1) resultados de la prueba:

Enviar tiempos de operación: 1 Recibir tiempos de respuesta: 1

Tiempo mínimo/máximo/promedio de ida y vuelta: 62/62/62

Cuadrado-Suma del tiempo de ida y vuelta: 3844

Hora de la última sonda realizada con éxito: 2011-11-10 10:49:37.3

Resultados extendidos:

Ratio de pérdida de paquetes: 0% Fallos por

tiempo de espera: 0 Fallos por error interno:

0 Fallos por otros errores: 0

Mostrar los registros históricos de la operación DNS.

[DispositivoA] muestra la prueba de administrador del historial nqa1

Registros del historial de entradas NQA (administrador, prueba de etiquetas):

Índice	Respuesta	Estado	Tiempo
1	62	Tuvo éxito	2011-11-10 10:49:37.3

El resultado muestra que al dispositivo A62 le llevó milisegundos traducir el nombre de dominio.**anfitrión.com**en una dirección IP.

Ejemplo de configuración de operación FTP

Requisitos de red

Como se muestra enFigura 6, configure una operación FTP para probar el tiempo necesario para que el dispositivo A cargue un archivo en el servidor FTP. El nombre de usuario y la contraseña de inicio de sesión son**administración**y**prueba del sistema**, respectivamente. El archivo que se transferirá al servidor FTP es**configuración.txt**.

Figura 6 Diagrama de red

Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crea una operación FTP.

<DispositivoA> vista del sistema

[DispositivoA] prueba de administrador de entrada

nqa1 [DispositivoA-nqa-admin-test1] tipo ftp

Especifique la URL del servidor FTP.

[DeviceA-nqa-admin-test-ftp] URL ftp://10.2.2.2

Especifique 10.1.1.1 como dirección IP de origen.

[DeviceA-nqa-admin-test1-ftp] IP de origen 10.1.1.1

Configurar el dispositivo para cargar archivos**configuración.txt**al servidor FTP.

[DispositivoA-nqa-admin-test1-ftp] operación puesta

[DispositivoA-nqa-admin-test1-ftp] nombre de archivo config.txt

Especifique el nombre de usuario para la operación FTP como**administración**.

[DeviceA-nqa-admin-test1-ftp] nombre de usuario administrador

Especifique la contraseña para la operación FTP como**prueba del sistema**.

[DeviceA-nqa-admin-test1-ftp] prueba de sistema simple de contraseña

Habilite el guardado de registros históricos.

[DeviceA-nqa-admin-test1-ftp] habilitar registro histórico [DeviceA-nqa-admin-test1-ftp] salir

Inicie la operación FTP.

[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

Después de que la operación FTP se ejecute durante un período de tiempo, detenga la operación.

[DispositivoA] deshacer la prueba de administrador de programación nqa1

Muestra el resultado más reciente de la operación FTP.

[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA

(admin admin, etiqueta test1) resultados de la prueba:

Enviar tiempos de operación: 1 Recibir tiempos de respuesta: 1

Tiempo mínimo/máximo/promedio de ida y vuelta: 173/173/173

Cuadrado-Suma del tiempo de ida y vuelta: 29929

Hora de la última sonda realizada con éxito: 2011-11-22 10:07:28.6

Resultados extendidos:

Ratio de pérdida de paquetes: 0% Fallos por tiempo de espera: 0 Fallos por desconexión: 0 Fallos por falta de conexión: 0 Fallos por error interno: 0 Fallos por otros errores: 0

Mostrar los registros históricos de la operación FTP.

[DispositivoA] muestra la prueba de administrador del historial nqa1

Registros del historial de entradas NQA (admin admin, etiqueta test1):

Índice	Respuesta	Estado	Tiempo	
1	173	Tuvo éxito	2011-11-22	10:07:28.6

El resultado muestra que al Dispositivo A le tomó 173 milisegundos cargar un archivo al servidor FTP.

Ejemplo de configuración de operación HTTP

Requisitos de red

Como se muestra enFigura 7, configure una operación HTTP en el cliente NQA para probar el tiempo necesario para obtener datos del servidor HTTP.

Figura 7 Diagrama de red

Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crea una operación HTTP.

<DispositivoA> vista del sistema

[DispositivoA] prueba de administrador de entrada

nqa1 [DispositivoA-nqa-admin-test1] escriba http

Especifique la URL del servidor HTTP.

[DeviceA-nqa-admin-test-http] URL http://10.2.2.2/index.htm

Configure la operación HTTP para obtener datos del servidor HTTP.

Obtención de operación [DeviceA-nqa-admin-test1-http]

Configure la operación para usar HTTP versión 1.0.

[DeviceA-nqa-admin-test1-http] versión v1.0

Habilite el guardado de registros históricos.

[DeviceA-nqa-admin-test1-http] habilitar registro histórico [DeviceA-nqa-admin-test1-http] salir

Inicie la operación HTTP.

[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

Después de que la operación HTTP se ejecute durante un período de tiempo, detenga la operación.

[DispositivoA] deshacer la prueba de administrador de programación nqa1

Muestra el resultado más reciente de la operación HTTP.

[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA

(admin admin, etiqueta test1) resultados de la prueba:

Enviar tiempos de operación: 1 Recibir tiempos de respuesta: 1

Tiempo mínimo/máximo/promedio de ida y vuelta: 64/64/64

Cuadrado-Suma del tiempo de ida y vuelta: 4096

Hora de la última sonda realizada con éxito: 2011-11-22 10:12:47.9

Resultados extendidos:

Ratio de pérdida de paquetes: 0% Fallos por tiempo de espera: 0 Fallos por desconexión: 0 Fallos por falta de conexión: 0 Fallos por error interno: 0 Fallos por otros errores: 0

Mostrar los registros históricos de la operación HTTP.

[DispositivoA] muestra la prueba de administrador del historial nqa1

Registros del historial de entradas NQA (admin admin, etiqueta test1):

Índice	Respuesta	Estado	Tiempo
1	64	Tuvo éxito	2011-11-22 10:12:47.9

El resultado muestra que al Dispositivo A le tomó 64 milisegundos obtener datos del servidor HTTP.

Ejemplo de configuración de operación de fluctuación UDP

Requisitos de red

Como se muestra enFigura 8, configure una operación de fluctuación UDP para probar la fluctuación, el retraso y el tiempo de ida y vuelta entre el dispositivo A y el dispositivo B.

Figura 8 Diagrama de red

Procedimiento de configuración

1. Asigne a cada interfaz una dirección IP. (No se muestran detalles).
2. Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).
3. Configurar el dispositivo B:

   # Habilite el servidor NQA.

   <DispositivoB> vista del sistema

   [DispositivoB] servidor nqa habilitado

   # Configure un servicio de escucha para escuchar en la dirección IP 10.2.2.2 y el puerto UDP 9000.

   [DispositivoB] servidor nqa udp-echo 10.2.2.2 9000
4. Configurar el dispositivo A:

   # Cree una operación de fluctuación UDP.

   <DispositivoA> vista del sistema

[DispositivoA] prueba de administrador de entrada nqa1
[DispositivoA-nqa-admin-test1] tipo udp-jitter
Configure 10.2.2.2 como dirección IP de destino y el puerto 9000 como puerto de destino.
[DeviceA-nqa-admin-test1-udp-jitter] ip destino 10.2.2.2 [DeviceA-nqa-admin-test1-udp-jitter] puerto destino 9000
Configure la operación para que se repita cada 1000 milisegundos.
[DispositivoA-nqa-admin-test1-udp-jitter] frecuencia 1000
[DispositivoA-nqa-admin-test1-udp-jitter] abandonar
Inicie la operación de fluctuación UDP.
[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre
Después de que la operación de fluctuación UDP se ejecute durante un período de tiempo, detenga la operación.
[DispositivoA] deshacer la prueba de administrador de programación nqa1
Muestra el resultado más reciente de la operación de fluctuación UDP.
[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA
(admin admin, etiqueta test1) resultados de la prueba:
Enviar tiempos de operación: 10 Recibir tiempos de respuesta: 10
Tiempo mínimo/máximo/promedio de ida y vuelta: 15/32/17
Cuadrado-Suma del tiempo de ida y vuelta: 3235
Hora del último paquete recibido: 2011-05-29 13:56:17.6
Resultados extendidos:
Ratio de pérdida de paquetes: 0% Fallos por tiempo de espera: 0 Fallos por error interno: 0 Fallos por otros errores: 0 Paquetes fuera de secuencia: 0
Los paquetes llegaron tarde: 0
resultados de fluctuación UDP:
Número RTT: 10
DE positiva mínima: 4 DE positiva máxima: 21 Número de DE positiva: 5 Suma de DE positiva: 52 Promedio de DE positiva: 10 Suma cuadrada de DE positiva: 754 DE negativa mínima: 1
DS positivo mínimo: 1 DS positivo máximo: 28 Número de DS positivo: 4 Suma de DS positivo: 38 Promedio de DS positivo: 10 Suma cuadrada de DS positivo: 460 DS mínimo negativo: 6
DE negativa máxima: 13 Número de DE negativa: 4 Suma de DE negativa: 38 Promedio de DE negativa: 10 Suma de cuadrados de DE negativa: 460
DS negativo máximo: 22 Número de DS negativo: 5 Suma de DS negativo: 52 Promedio de DS negativo: 10 Suma cuadrada de DS negativo: 754
Resultados unidireccionales:
Retardo máximo de SD: 15
Retardo mínimo de SD: 7
Número de retraso de SD: 10 Suma de retraso de SD: 78 Suma cuadrada de retraso de SD: 666 Paquetes perdidos de SD: 0
Retardo máximo de DS: 16
Retardo mínimo de DS: 7
Número de retraso DS: 10 Suma de retraso DS: 85 Suma cuadrada de retraso DS: 787 Paquetes DS perdidos: 0
Paquetes perdidos por motivo desconocido: 0

Muestra las estadísticas de la operación de fluctuación UDP.
[DispositivoA] muestra estadísticas de nqa admin test1 Entrada NQA
(admin admin, etiqueta test1) estadísticas de prueba:
NO. : 1
Hora de inicio: 2011-05-29 13:56:14.0
Duración: 47 segundos
Tiempos de operación de envío: 410 Tiempo mínimo/máximo/Recibir tiempos de respuesta: 410
promedio de ida y vuelta: 1/93/19 Suma cuadrada del tiempo
de ida y vuelta: 206176 Resultados extendidos:

Ratio de pérdida de paquetes: 0% Fallos por
tiempo de espera: 0 Fallos por error interno:
0 Fallos por otros errores: 0 Paquetes fuera
de secuencia: 0

Los paquetes llegaron tarde: 0
resultados de fluctuación UDP:
Número RTT: 410
DE positiva mínima: 3 DE positiva
máxima: 30 Número de DE positiva: 186
Suma de DE positiva: 2602 Promedio de
DE positiva: 13 Suma cuadrada de DE
positiva: 45304 DE negativa mínima: 1

DE negativa máxima: 30 Número de DE
negativa: 181 Suma de DE negativa: 181
Promedio de DE negativa: 13 Suma de
cuadrados de DE negativa: 46994
Resultados unidireccionales:

Retardo SD máximo: 46
Retardo SD mínimo: 7
Número de retraso SD: 410 Suma del
retraso SD: 3705 Suma cuadrada del
retraso SD: 45987 Paquetes perdidos
SD: 0
Paquetes perdidos por motivo desconocido: 0

DS positivo mínimo: 1 DS positivo
máximo: 79 Número de DS positivo:
158 Suma de DS positivo: 1928
Promedio de DS positivo: 12 Suma
cuadrada de DS positivo: 31682 DS
mínimo negativo: 1

DS negativo máximo: 78 Número de
DS negativo: 209 Suma de DS
negativo: 209 Promedio de DS
negativo: 14 Suma cuadrada de DS
negativo: 3030

Retardo máximo de DS: 46
Retardo mínimo de DS: 7
Número de retraso de DS: 410 Suma de
retraso de DS: 3891 Suma cuadrada de
retraso de DS: 49393 Paquetes perdidos
de DS: 0

Ejemplo de configuración de operación SNMP

Requisitos de red

Como se muestra enFigura 9, configure una operación SNMP para probar el tiempo que utiliza el cliente NQA para obtener una respuesta del agente SNMP.

Figura 9 Diagrama de red

Procedimiento de configuración

1. Asigne a cada interfaz una dirección IP. (No se muestran detalles).
2. Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).
3. Configure el agente SNMP (Dispositivo B):

   # Establezca la versión de SNMP en**todo**.

   <DispositivoB> vista del sistema

   [DispositivoB] snmp-agent sys-info versión toda

   # Establece la comunidad de lectura en**público**.

   [DispositivoB] comunidad de agente snmp leída públicamente

   # Establece la comunidad de escritura en**privado**.

   [DispositivoB] comunidad de agente snmp escritura privada
4. Configurar el dispositivo A:

   # Cree una operación SNMP.

   <DispositivoA> vista del sistema

   [DispositivoA] prueba de administrador de entrada nqa1

   [DispositivoA-nqa-admin-test1] escriba snmp

   # Configure 10.2.2.2 como la dirección IP de destino de la operación SNMP.

   [DeviceA-nqa-admin-test1-snmp] IP de destino 10.2.2.2

   # Habilite el guardado de registros históricos.

   [DispositivoA-nqa-admin-test1-snmp] habilitar registro histórico

   [DispositivoA-nqa-admin-test1-snmp] abandonar

   # Inicie la operación SNMP.

   [DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

   # Después de que la operación SNMP se ejecute durante un período de tiempo, detenga la operación.

   [DispositivoA] deshacer la prueba de administrador de programación nqa1

   # Muestra el resultado más reciente de la operación SNMP.

   [DispositivoA] muestra el resultado nqa admin test1 Entrada NQA

   (admin admin, etiqueta test1) resultados de la prueba:

   Enviar tiempos de operación: 1 Recibir tiempos de respuesta: 1

   Tiempo mínimo/máximo/promedio de ida y vuelta: 50/50/50

   Cuadrado-Suma del tiempo de ida y vuelta: 2500

   Hora de la última sonda realizada con éxito: 2011-11-22 10:24:41.1

   Resultados extendidos:

   Ratio de pérdida de paquetes: 0% Fallos por

   tiempo de espera: 0 Fallos por error interno:

   0 Fallos por otros errores: 0

   # Mostrar los registros históricos de la operación SNMP.

   [DispositivoA] muestra la prueba de administrador del historial nqa1

   Registros del historial de entradas NQA (admin admin, etiqueta test1):

Índice	Respuesta	Estado	Tiempo
1	50	Tuvo éxito	2011-11-22 10:24:41.1

El resultado muestra que el dispositivo A tardó 50 milisegundos en recibir una respuesta del agente SNMP.

Ejemplo de configuración de operación TCP

Requisitos de red

Como se muestra enFigura 10, configure una operación TCP para probar el tiempo necesario para que el Dispositivo A y el Dispositivo B establezcan una conexión TCP.

Figura 10 Diagrama de red

Procedimiento de configuración

1. Asigne a cada interfaz una dirección IP. (No se muestran detalles).
2. Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).
3. Configurar el dispositivo B:

   # Habilite el servidor NQA.

   <DispositivoB> vista del sistema

   [DispositivoB] servidor nqa habilitado

   # Configure un servicio de escucha para escuchar en la dirección IP 10.2.2.2 y el puerto TCP 9000.

   [DispositivoB] servidor nqa tcp-connect 10.2.2.2 9000
4. Configurar el dispositivo A:

   # Crea una operación TCP.

   <DispositivoA> vista del sistema

   [DispositivoA] prueba de administrador de entrada

   nqa1 [DispositivoA-nqa-admin-test1] tipo tcp

   # Configure 10.2.2.2 como dirección IP de destino y el puerto 9000 como puerto de destino.

   [DeviceA-nqa-admin-test1-tcp] IP de destino 10.2.2.2 [DeviceA-nqa-

   admin-test1-tcp] Puerto de destino 9000

   # Habilite el guardado de registros históricos.

   [DeviceA-nqa-admin-test1-tcp] habilitar registro histórico [DeviceA-

   nqa-admin-test1-tcp] salir

   # Inicie la operación TCP.

   [DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

   # Después de que la operación TCP se ejecute durante un período de tiempo, detenga la operación.

   [DispositivoA] deshacer la prueba de administrador de programación nqa1

   # Muestra el resultado más reciente de la operación TCP.

   [DispositivoA] muestra el resultado nqa admin test1 Entrada NQA

   (admin admin, etiqueta test1) resultados de la prueba:

   Enviar tiempos de operación: 1 Recibir tiempos de respuesta: 1

   Tiempo mínimo/máximo/promedio de ida y vuelta: 13/13/13

Suma cuadrada del tiempo de ida y vuelta: 169

Hora de la última sonda realizada con éxito: 2011-11-22 10:27:25.1

Resultados extendidos:

Ratio de pérdida de paquetes: 0% Fallos por

tiempo de espera: 0 Fallos por desconexión:

0 Fallos por falta de conexión: 0 Fallos por

error interno: 0 Fallos por otros errores: 0

Mostrar los registros históricos de la operación TCP.

[DispositivoA] muestra la prueba de administrador del historial nqa1

Registros del historial de entradas NQA (admin admin, etiqueta test1):

Índice	Respuesta	Estado	Tiempo
1	13	Tuvo éxito	2011-11-22 10:27:25.1

El resultado muestra que al Dispositivo A le tomó 13 milisegundos establecer una conexión TCP al puerto 9000 en el servidor NQA.

Ejemplo de configuración de operación de eco UDP

Requisitos de red

Como se muestra enFigura 11, configure una operación de eco UDP para probar el tiempo de ida y vuelta entre el Dispositivo A y el Dispositivo B. El número de puerto de destino es 8000.

Figura 11 Diagrama de red

Procedimiento de configuración

1. Asigne a cada interfaz una dirección IP. (No se muestran detalles).
2. Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).
3. Configurar el dispositivo B:

   # Habilite el servidor NQA.

   <DispositivoB> vista del sistema

   [DispositivoB] servidor nqa habilitado

   # Configure un servicio de escucha para escuchar en la dirección IP 10.2.2.2 y el puerto UDP 8000.

   [DispositivoB] servidor nqa udp-echo 10.2.2.2 8000
4. Configurar el dispositivo A:

   # Crea una operación de eco UDP.

   <DispositivoA> vista del sistema

   [DispositivoA] prueba de administrador de entrada nqa1

   [DispositivoA-nqa-admin-test1] tipo udp-echo

   # Configure 10.2.2.2 como dirección IP de destino y el puerto 8000 como puerto de destino.

   [DeviceA-nqa-admin-test1-udp-echo] ip destino 10.2.2.2 [DeviceA-nqa-admin-

   test1-udp-echo] puerto destino 8000

   # Habilite el guardado de registros históricos.

[DeviceA-nqa-admin-test1-udp-echo] habilitar registro histórico [DeviceA-nqa-admin-test1-udp-echo] salir

Inicie la operación de eco UDP.

[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

Después de que la operación de eco UDP se ejecute durante un período de tiempo, detenga la operación.

[DispositivoA] deshacer la prueba de administrador de programación nqa1

Muestra el resultado más reciente de la operación de eco UDP.

[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA

(admin admin, etiqueta test1) resultados de la prueba:

Enviar tiempos de operación: 1 Recibir tiempos de respuesta: 1

Tiempo mínimo/máximo/promedio de ida y vuelta: 25/25/25

Cuadrado-Suma del tiempo de ida y vuelta: 625

Hora de la última sonda realizada con éxito: 2011-11-22 10:36:17.9

Resultados extendidos:

Ratio de pérdida de paquetes: 0% Fallos por tiempo de espera: 0 Fallos por error interno: 0 Fallos por otros errores: 0

Muestra los registros históricos de la operación de eco UDP.

[DispositivoA] muestra la prueba de administrador del historial nqa1

Registros del historial de entradas NQA (admin admin, etiqueta test1):

Índice	Respuesta	Estado	Tiempo
1	25	Tuvo éxito	2011-11-22 10:36:17.9

El resultado muestra que el tiempo de ida y vuelta entre el dispositivo A y el puerto 8000 en el dispositivo B es de 25 milisegundos.

Ejemplo de configuración de operación de tracert UDP

Requisitos de red

Como se muestra enFigura 12, configure una operación de tracert UDP para determinar la ruta de enrutamiento desde el Dispositivo A al Dispositivo B.

Figura 12 Diagrama de red

Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz. (No se muestran detalles).
2. Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).
3. Utilizar el**ip ttl-expires habilitar**comando en el dispositivo intermedio y utilice el**ip inalcanzables habilitar**comando en el dispositivo B.
4. Configurar el dispositivo A:

   # Cree una operación de seguimiento UDP.

   <DispositivoA> vista del sistema

   [DispositivoA] prueba de administrador de entrada nqa1

[DeviceA-nqa-admin-test1] tipo udp-tracert

Especifique 10.2.2.2 como dirección IP de destino.

[DeviceA-nqa-admin-test1-udp-tracert] ip destino 10.2.2.2

Establezca el número de puerto de destino en 33434.

[DeviceA-nqa-admin-test1-udp-tracert] puerto de destino 33434

Configure el dispositivo A para realizar tres sondas en cada salto.

[DeviceA-nqa-admin-test1-udp-tracert] recuento de sondas 3

Establezca el tiempo de espera de la sonda en 500 milisegundos.

[DeviceA-nqa-admin-test1-udp-tracert] tiempo de espera de sonda 500

Configure la operación de tracert UDP para que se repita cada 5000 milisegundos.

[DeviceA-nqa-admin-test1-udp-tracert] frecuencia 5000

Especifique GigabitEthernet 2/0/1 como interfaz de salida para paquetes UDP.

[DeviceA-nqa-admin-test1-udp-tracert] interfaz de salida gigabitethernet 2/0/1

Habilite la función de no fragmentación.

[DeviceA-nqa-admin-test1-udp-tracert] habilitación sin fragmentos

Establezca el número máximo de fallas de sonda consecutivas en 6.

[DeviceA-nqa-admin-test1-udp-tracert] fallo máximo 6

Establezca el valor TTL en 1 para los paquetes UDP en la ronda inicial de la operación de seguimiento UDP.

[DeviceA-nqa-admin-test1-udp-tracert] init-ttl 1

Inicie la operación de tracert UDP.

[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

Después de que la operación UDP tracert se ejecute durante un período de tiempo, detenga la operación.

[DispositivoA] deshacer la prueba de administrador de programación nqa1

Muestra el resultado más reciente de la operación de tracert UDP.

[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA

(admin admin, etiqueta test1) resultados de la prueba:

Enviar tiempos de operación: 6 Recibir tiempos de respuesta: 6

Tiempo mínimo/máximo/promedio de ida y vuelta: 1/1/1

Cuadrado-Suma del tiempo de ida y vuelta: 1

Hora de la última sonda realizada con éxito: 2013-09-09 14:46:06.2

Resultados extendidos:

Pérdida de paquetes en prueba: 0% Fallos

por tiempo de espera: 0 Fallos por error

interno: 0 Fallos por otros errores: 0

Resultados UDP-tracert:

TTL	IP de salto	Tiempo	
1	3.1.1.1	2013-09-09	14:46:03.2
2	10.2.2.2	2013-09-09	14:46:06.2

Mostrar los registros históricos de la operación de tracert UDP.

[DispositivoA] muestra la prueba de administrador del historial nqa1

Registros del historial de entradas NQA (admin admin, etiqueta test1):

Índice	TTL	Respuesta	IP de salto	Estado	Tiempo	
1	2	2	10.2.2.2	Tuvo éxito	2013-09-09	14:46:06.2
1	2	1	10.2.2.2	Tuvo éxito	2013-09-09	14:46:05.2
1	2	2	10.2.2.2	Tuvo éxito	2013-09-09	14:46:04.2
1	1	1	3.1.1.1	Tuvo éxito	2013-09-09	14:46:03.2

1	1	2	3.1.1.1	Tuvo éxito	2013-09-09	14:46:02.2
1	1	1	3.1.1.1	Tuvo éxito	2013-09-09	14:46:01.2

Ejemplo de configuración de operación por voz

Requisitos de red

Como se muestra enFigura 13, configure una operación de voz para probar las fluctuaciones entre el Dispositivo A y el Dispositivo B.

Figura 13 Diagrama de red

Procedimiento de configuración

1. Asigne a cada interfaz una dirección IP. (No se muestran detalles).
2. Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).
3. Configurar el dispositivo B:

   # Habilite el servidor NQA.

   <DispositivoB> vista del sistema

   [DispositivoB] servidor nqa habilitado

   # Configure un servicio de escucha para escuchar en la dirección IP 10.2.2.2 y el puerto UDP 9000.

   [DispositivoB] servidor nqa udp-echo 10.2.2.2 9000
4. Configurar el dispositivo A:

   # Crea una operación de voz.

   <DispositivoA> vista del sistema

   [DispositivoA] prueba de administrador de entrada

   nqa1 [DeviceA-nqa-admin-test1] escriba voz

   # Configure 10.2.2.2 como dirección IP de destino y el puerto 9000 como puerto de destino.

   [DeviceA-nqa-admin-test1-voice] ip de destino 10.2.2.2 [DeviceA-nqa-admin-test1-voice] puerto de destino 9000 [DeviceA-nqa-admin-test1-voice] salir

   # Inicie la operación de voz.

   [DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

   # Después de que la operación de voz se ejecute durante un período de tiempo, detenga la operación.

   [DispositivoA] deshacer la prueba de administrador de programación nqa1

   # Muestra el resultado más reciente de la operación de voz.

   [DispositivoA] muestra el resultado nqa admin test1 Entrada NQA

   (admin admin, etiqueta test1) resultados de la prueba:

   Enviar tiempos de operación: 1000 Recibir tiempos de respuesta: 1000

   Tiempo mínimo/máximo/promedio de ida y vuelta: 31/1328/33

   Cuadrado-Suma del tiempo de ida y vuelta: 2844813

   Hora del último paquete recibido: 2011-06-13 09:49:31.1

   Resultados extendidos:

   Ratio de pérdida de paquetes: 0%

   Fallos por tiempo de espera: 0

Fallos por error interno: 0 Fallos por otros errores: 0 Paquetes fuera de secuencia: 0

Los paquetes llegaron tarde: 0
Resultados de voz:
Número RTT: 1000
DE positiva mínima: 1 DE positiva máxima: 204 Número de DE positiva: 257 Suma de DE positiva: 759 Promedio de DE positiva: 2 Suma cuadrada de DE positiva: 54127 DE negativa mínima: 1
DS positivo mínimo: 1 DS positivo máximo: 1297 Número de DS positivo: 259 Suma de DS positivo: 1797 Promedio de DS positivo: 6 Suma cuadrada de DS positivo: 1691967 DS mínimo negativo: 1

SD negativa máxima: 203 Número de SD negativo: 255 Suma de SD negativa: 759 Promedio de SD negativa: 2 Suma cuadrada de SD negativa: 53655
DS negativo máximo: 1297 Número de DS negativo: 259 Suma de DS negativo: 1796 Promedio de DS negativo: 6 Suma cuadrada de DS negativo: 1691776
Resultados unidireccionales:

Retardo SD máximo: 343 Retardo SD mínimo: 343 Número de retraso SD: 1 Suma del retraso SD: 343 Suma cuadrada del retraso SD: 117649 Paquetes perdidos SD: 0
Retraso máximo de DS: 985 Retraso mínimo de DS: 985 Número de retrasos de DS: 1 Suma de retrasos de DS: 985 Suma cuadrada de retrasos de DS: 970225 Paquetes perdidos de DS: 0

Paquetes perdidos por motivo desconocido: 0
Puntuaciones de voz:
Valor MOS: 4,38
Valor ICPIF: 0

Muestra las estadísticas de la operación de voz.
[DispositivoA] muestra estadísticas de nqa admin test1 Entrada NQA (admin admin, etiqueta test1) estadísticas de prueba:
NO. : 1

Hora de inicio: 2011-06-13 09:45:37.8
Duración: 331 segundos
Tiempos de operación de envío: 4000 Tiempo mínimo/máximo/promedio de ida y vuelta: 15/1328/32 Suma cuadrada del tiempo de ida y vuelta: 7160528
Recibir tiempos de respuesta: 4000
Resultados extendidos:

Ratio de pérdida de paquetes: 0% Fallos por tiempo de espera: 0 Fallos por error interno: 0 Fallos por otros errores: 0 Paquetes fuera de secuencia: 0

Los paquetes llegaron tarde: 0
Resultados de voz:
Número RTT: 4000
DE positiva mínima: 1
DS mínimo positivo: 1

SD positiva máxima: 360 Número de SD positiva: 1030 Suma de SD positiva: 4363 Promedio de SD positiva: 4 Suma cuadrada de SD positiva: 497725 SD negativa mínima: 1

DS positivo máximo: 1297 Número de DS positivo: 1024 Suma de DS positivo: 5423 Promedio de DS positivo: 5 Suma cuadrada de DS positivo: 2254957 DS negativo mínimo: 1

SD negativa máxima: 360 Número de SD negativo: 1028 Suma de SD negativa: 1028 Promedio de SD negativa: 4 Suma cuadrada de SD negativa: 495901 Resultados unidireccionales:

DS negativo máximo: 1297 Número de DS negativo: 1022 Suma de DS negativo: 1022 Promedio de DS negativo: 5 Suma cuadrada de DS negativo: 5419

Retardo máximo de SD: 359

Retardo mínimo de SD: 0

Número de retraso de SD: 4 Suma de retraso de SD: 1390 Suma cuadrada de retraso de SD: 483202 Paquetes perdidos de SD: 0

Retardo máximo de DS: 985

Retardo mínimo de DS: 0

Número de retraso DS: 4 Suma de retraso DS: 1079 Suma cuadrada de retraso DS: 973651 Paquetes DS perdidos: 0

Paquetes perdidos por motivo desconocido: 0

Puntuaciones de voz:

Valor máximo de MOS: 4,38

Valor mínimo de MOS: 4,38

Valor máximo de ICPIF: 0

Valor mínimo de ICPIF: 0

Ejemplo de configuración de operación DLSw

Requisitos de red

Como se muestra enFigura 14, configure una operación DLSw para probar el tiempo de respuesta del dispositivo DLSw.

Figura 14 Diagrama de red

Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crear una operación DLSw.

<DispositivoA> vista del sistema

[DispositivoA] prueba de administrador de entrada

nqa1 [DispositivoA-nqa-admin-test1] tipo dlsw

Configure 10.2.2.2 como la dirección IP de destino.

[DeviceA-nqa-admin-test1-dlsw] IP de destino 10.2.2.2

Habilite el guardado de registros históricos.

[DeviceA-nqa-admin-test1-dlsw] habilitar registro histórico [DeviceA-nqa-admin-test1-dlsw] salir

Inicie la operación DLSw.

```
[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre
```

Después de que la operación DLSw se ejecute durante un período de tiempo, detenga la operación.

```
[DispositivoA] deshacer la prueba de administrador de programación nqa1
```

Muestra el resultado más reciente de la operación DLSw.

```
[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA
(admin admin, etiqueta test1) resultados de la prueba:
    Enviar tiempos de operación: 1                Recibir tiempos de respuesta: 1
    Tiempo mínimo/máximo/promedio de ida y vuelta: 19/19/19
    Cuadrado-Suma del tiempo de ida y vuelta: 361
    Hora de la última sonda realizada con éxito: 2011-11-22 10:40:27.7
  Resultados extendidos:
    Ratio de pérdida de paquetes: 0% Fallos por
    tiempo de espera: 0 Fallos por desconexión:
    0 Fallos por falta de conexión: 0 Fallos por
    error interno: 0 Fallos por otros errores: 0
```

Mostrar los registros históricos de la operación DLSw.

```
[DispositivoA] muestra la prueba de administrador del historial nqa1
Registros del historial de entradas NQA (admin admin, etiqueta test1):
```

Índice	Respuesta	Estado	Tiempo
1	19	Tuvo éxito	2011-11-22 10:40:27.7

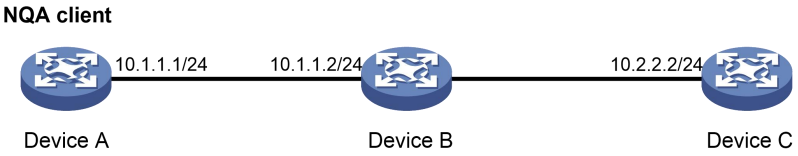
El resultado muestra que el tiempo de respuesta del dispositivo DLSw es de 19 milisegundos.

Ejemplo de configuración de operación de fluctuación de ruta

Requisitos de red

Como se muestra enFigura 15, configure una operación de fluctuación de ruta para probar el tiempo de ida y vuelta y las fluctuaciones desde el Dispositivo A al Dispositivo B y al Dispositivo C.

Figura 15 Diagrama de red



Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Utilizar el**ip ttl-expires habilitar**comando en el dispositivo B y use el**ip inalcanzables habilitar**comando en el dispositivo C.

Crea una operación de fluctuación de ruta.

```
<DispositivoA> vista del sistema
[DispositivoA] prueba de administrador de entrada nqa1
[DeviceA-nqa-admin-test1] tipo path-jitter
```

Especifique 10.2.2.2 como la dirección IP de destino de las solicitudes de eco ICMP.

[DeviceA-nqa-admin-test1-path-jitter] IP de destino 10.2.2.2

Configure la operación de fluctuación de ruta para que se repita cada 10000 milisegundos.

[DeviceA-nqa-admin-test1-path-jitter] [DeviceA-nqa-admin-test1-path-jitter] frecuencia 10000 abandonar

Inicie la operación de fluctuación de ruta.

[DispositivoA] nqa programar administrador prueba1 hora de inicio ahora de por vida para siempre

Después de que la operación de fluctuación de ruta se ejecute durante un período de tiempo, detenga la operación.

[DispositivoA] deshacer la prueba de administrador de programación nqa1

Muestra el resultado más reciente de la operación de fluctuación de ruta.

[DispositivoA] muestra el resultado nqa admin test1 Entrada NQA (admin admin, etiqueta test1) resultados de la prueba:

Salto IP 10.1.1.2

Resultados básicos

Tiempos de operación de envío: 10 Tiempo mínimo/máximo/Recibir tiempos de respuesta: 10 promedio de ida y vuelta: 21/09/14 Suma cuadrada del tiempo de ida y vuelta: 2419 Resultados extendidos

Fallos por tiempo de espera: 0 Fallos por error interno: 0 Fallos por otros errores: 0 Paquetes fuera de secuencia: 0

Los paquetes llegaron tarde: 0

resultados de Path-Jitter

Número de fluctuación: 9

Jitter mínimo/máximo/promedio: 1/10/4

Número de jitter positivo: 6

Jitter positivo mínimo/máximo/promedio: 1/9/4

Jitter positivo suma/suma cuadrada: 25/173

Número de jitter negativo: 3

Jitter negativo mínimo/máximo/promedio: 2/10/6

Jitter positivo suma/suma cuadrada: 19/153

Salto IP 10.2.2.2

Resultados básicos

Tiempos de operación de envío: 10 Min/Max/Tiempo Recibir tiempos de respuesta: 10 promedio de ida y vuelta: 15/40/28 Cuadrado-Suma del tiempo de ida y vuelta: 4493 Resultados extendidos

Fallos por tiempo de espera: 0 Fallos por error interno: 0 Fallos por otros errores: 0 Paquetes fuera de secuencia: 0

Los paquetes llegaron tarde: 0

resultados de Path-Jitter

Número de fluctuación: 9

Jitter mínimo/máximo/promedio: 1/10/4

Número de fluctuación positiva: 6

Jitter positivo mínimo/máximo/promedio: 1/9/4

Jitter positivo suma/suma cuadrada: 25/173

Número de jitter negativo: 3

Jitter negativo mínimo/máximo/promedio: 2/10/6

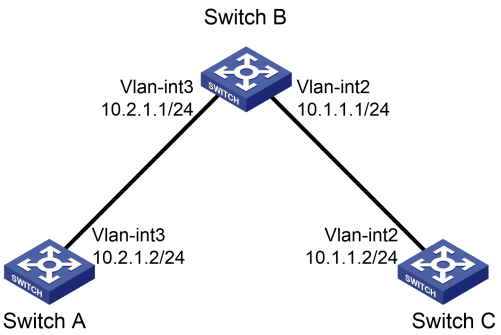
Jitter positivo suma/suma cuadrada: 19/153

Ejemplo de configuración de colaboración NQA

Requisitos de red

Como se muestra enFigura 16, configure una ruta estática al Switch C con el Switch B como el siguiente salto en el Switch A. Asocie la ruta estática, una entrada de seguimiento y una operación de eco ICMP para monitorear el estado de la ruta estática.

Figura 16 Diagrama de red



Procedimiento de configuración

1. Asigne a cada interfaz una dirección IP. (No se muestran detalles).
2. En el conmutador A, configure una ruta estática y asocie la ruta estática con la entrada de pista 1.

   <SwitchA> vista del sistema

   [SwitchA] ip ruta estática 10.1.1.2 24 10.2.1.1 pista 1
3. En el Switch A, configure una operación de eco ICMP:

   # Crear una operación NQA con el nombre del administrador**administración**y etiqueta de operación**prueba1**.

   [SwitchA] prueba de administrador de entrada nqa1

   # Configure el tipo de operación NQA como eco ICMP.

   [SwitchA-nqa-admin-test1] escriba icmp-echo

   # Configure 10.2.1.1 como la dirección IP de destino.

   [SwitchA-nqa-admin-test1-icmp-echo] IP de destino 10.2.1.1

   # Configure la operación para que se repita cada 100 milisegundos.

   [SwitchA-nqa-admin-test1-icmp-echo] frecuencia 100

   # Crear entrada de reacción 1. Si el número de fallas de sonda consecutivas llega a 5, se activa la colaboración.

   [SwitchA-nqa-admin-test1-icmp-echo] reacción 1 elemento comprobado tipo de umbral de falla de sonda consecutiva 5 tipo de acción solo disparador

   [SwitchA-nqa-admin-test1-icmp-echo] salir

   # Inicie la operación ICMP.

   [SwitchA] nqa programar administrador test1 hora de inicio ahora de por vida para siempre
4. En el conmutador A, cree la entrada de seguimiento 1 y asóciela con la entrada de reacción 1 de la operación NQA.

   [SwitchA] pista 1 entrada nqa prueba de administrador 1 reacción 1

Verificando la configuración

Muestra información sobre todas las entradas de pistas en el Switch A.

[SwitchA] muestra todas las pistas ID
de pista: 1
Estado: Positivo
Duración: 0 días 0 horas 0 minutos 0 segundos Retraso de notificación:
Positivo 0, Negativo 0 (en segundos) Objeto rastreado:

Entrada NQA: prueba de
administrador1 Reacción: 1

Mostrar información breve sobre rutas activas en la tabla de enrutamiento en el Switch A.

[SwitchA] muestra la tabla de enrutamiento IP

Destinos : 13 Rutas : 13

Destino/Máscara	Proto	Pre	Costo	Siguiente salto	Interfaz
0.0.0.0/32	directo	0	0	127.0.0.1	en bucle0
10.1.1.0/24	Estático	60	0	10.2.1.1	Vlan3
10.2.1.0/24	directo	0	0	10.2.1.2	Vlan3
10.2.1.0/32	directo	0	0	10.2.1.2	Vlan3
10.2.1.2/32	directo	0	0	127.0.0.1	en bucle0
10.2.1.255/32	directo	0	0	10.2.1.2	Vlan3
127.0.0.0/8	directo	0	0	127.0.0.1	en bucle0
127.0.0.0/32	directo	0	0	127.0.0.1	en bucle0
127.0.0.1/32	directo	0	0	127.0.0.1	en bucle0
127.255.255.255/32	directo	0	0	127.0.0.1	en bucle0
224.0.0.0/4	directo	0	0	0.0.0.0	NULL0
224.0.0.0/24	directo	0	0	0.0.0.0	NULL0
255.255.255.255/32	directo	0	0	127.0.0.1	en bucle0

El resultado muestra que la ruta estática con el siguiente salto 10.2.1.1 está activa y el estado de la entrada de seguimiento es positivo.

Elimine la dirección IP de la interfaz VLAN 3 en el conmutador B.

<SwitchB> vista del sistema
[SwitchB] interfaz vlan-interface 3 [SwitchB-Vlan-
interface3] deshacer dirección IP

Muestra información sobre todas las entradas de pistas en el Switch A.

[SwitchA] muestra todas las pistas ID
de pista: 1
Estado: Negativo
Duración: 0 días 0 horas 0 minutos 0 segundos Retraso de notificación:
Positivo 0, Negativo 0 (en segundos) Objeto rastreado:

Entrada NQA: prueba de
administrador1 Reacción: 1

Mostrar información breve sobre rutas activas en la tabla de enrutamiento en el Switch A.

[SwitchA] muestra la tabla de enrutamiento IP

Destinos : 12 Rutas: 12

Destino/Máscara	Proto Pre	Costo	Siguiente salto	Interfaz
0.0.0.0/32	directo 0	0	127.0.0.1	en bucle0
10.2.1.0/24	directo 0	0	10.2.1.2	Vlan3
10.2.1.0/32	directo 0	0	10.2.1.2	Vlan3
10.2.1.2/32	directo 0	0	127.0.0.1	en bucle0
10.2.1.255/32	directo 0	0	10.2.1.2	Vlan3
127.0.0.0/8	directo 0	0	127.0.0.1	en bucle0
127.0.0.0/32	directo 0	0	127.0.0.1	en bucle0
127.0.0.1/32	directo 0	0	127.0.0.1	en bucle0
127.255.255.255/32	directo 0	0	127.0.0.1	en bucle0
224.0.0.0/4	directo 0	0	0.0.0.0	NULL0
224.0.0.0/24	directo 0	0	0.0.0.0	NULL0
255.255.255.255/32	directo 0	0	127.0.0.1	en bucle0

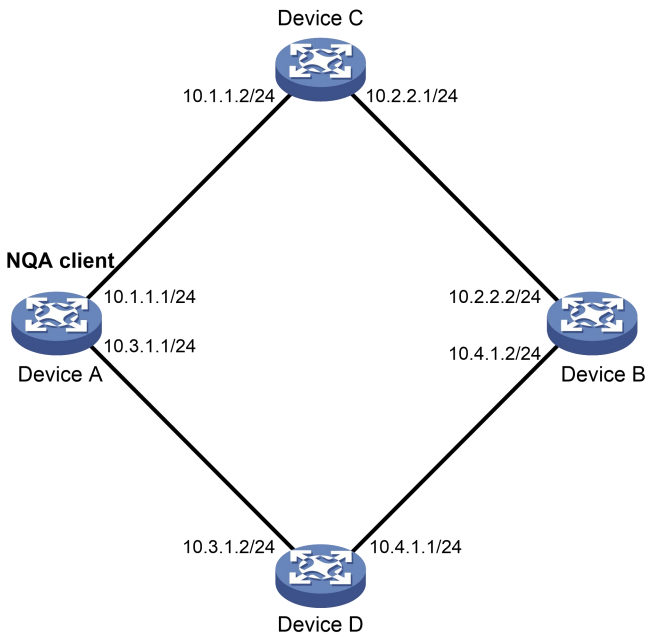
El resultado muestra que la ruta estática no existe y el estado de la entrada de seguimiento es negativo.

Ejemplo de configuración de plantilla ICMP

Requisitos de red

Como se muestra enFigura 17, configure una plantilla ICMP para que una función realice la operación de eco ICMP desde el dispositivo A al dispositivo B.

Figura 17 Diagrama de red



Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crear plantilla ICMP**ICMP**.

<DispositivoA> vista del sistema

[DispositivoA] plantilla nqa icmp icmp

Especifique 10.2.2.2 como la dirección IP de destino de las solicitudes de eco ICMP.

[DeviceA-nqatplt-icmp-icmp] IP de destino 10.2.2.2

Establezca el tiempo de espera de la sonda para la operación de eco ICMP en 500 milisegundos.

[DeviceA-nqatplt-icmp-icmp] tiempo de espera de sonda 500

Configure la operación de eco ICMP para que se repita cada 3000 milisegundos.

[DispositivoA-nqatplt-icmp-icmp] frecuencia 3000

Si el número de sondeos exitosos consecutivos llega a 2, la operación tiene éxito. El cliente NQA notifica a la función del evento de operación exitosa.

[DeviceA-nqatplt-icmp-icmp] sonda de activación de reacción-pase 2

Si el número de fallas de sonda consecutivas llega a 2, la operación falla. El cliente NQA notifica a la característica del error de operación.

[DeviceA-nqatplt-icmp-icmp] sonda de activación de reacción-fallo 2

Ejemplo de configuración de plantilla DNS

Requisitos de red

Como se muestra enFigura 18, configure una plantilla DNS para que una función realice la operación DNS. La operación prueba si el Dispositivo A puede realizar la resolución de direcciones a través del servidor DNS.

Figura 18 Diagrama de red

Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crear plantilla DNS**DNS**.

<DispositivoA> vista del sistema

[DispositivoA] plantilla nqa dns dns

Especifique la dirección IP del servidor DNS 10.2.2.2 como dirección IP de destino.

[DeviceA-nqatplt-dns-dns] IP de destino 10.2.2.2

Especifique el nombre de dominio que se traducirá como**anfitrión.com**.

[DeviceA-nqatplt-dns-dns] resolver-target host.com

Especifique el tipo de resolución del nombre de dominio como tipo A.

[DeviceA-nqatplt-dns-dns] resolver tipo A

Especifique la dirección IP esperada como 3.3.3.3.

[DeviceA-nqatplt-dns-dns] espera ip 3.3.3.3

Si el número de sondeos exitosos consecutivos llega a 2, la operación tiene éxito. El cliente NQA notifica a la función del evento de operación exitosa.

[DeviceA-nqatplt-dns-dns] sonda de activación de reacción-pase 2

Si el número de fallas de sonda consecutivas llega a 2, la operación falla. El cliente NQA notifica a la característica del error de operación.

[DeviceA-nqatplt-dns-dns] sonda de activación de reacción-fallo 2

Ejemplo de configuración de plantilla TCP

Requisitos de red

Como se muestra enFigura 19, configure una plantilla TCP para que una característica realice la operación TCP. La operación prueba si el Dispositivo A puede establecer una conexión TCP con el Dispositivo B.

Figura 19 Diagrama de red

Procedimiento de configuración

1. Asigne a cada interfaz una dirección IP. (No se muestran detalles).
2. Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).
3. Configurar el dispositivo B:

   # Habilite el servidor NQA.

   <DispositivoB> vista del sistema

   [DispositivoB] servidor nqa habilitado

   # Configure un servicio de escucha para escuchar la dirección IP 10.2.2.2 y el puerto TCP 9000.

   [DispositivoB] servidor nqa tcp-connect 10.2.2.2 9000
4. Configurar el dispositivo A:

   # Crear plantilla TCP**TCP**.

   <DispositivoA> vista del sistema

   [DispositivoA] plantilla nqa tcp tcp

   # Configure 10.2.2.2 como dirección IP de destino y el puerto 9000 como puerto de destino.

   [DeviceA-nqatplt-tcp-tcp] IP de destino 10.2.2.2 [DeviceA-nqatplt-

   tcp-tcp] Puerto de destino 9000

   # Si el número de sondeos exitosos consecutivos llega a 2, la operación tiene éxito. El cliente NQA notifica a la función del evento de operación exitosa.

   [DeviceA-nqatplt-tcp-tcp] sonda de activación de reacción-pase 2

   # Si el número de fallas de sonda consecutivas llega a 2, la operación falla. El cliente NQA notifica a la característica del error de operación.

   [DeviceA-nqatplt-tcp-tcp] sonda de activación de reacción-fallo 2

Ejemplo de configuración de plantilla UDP

Requisitos de red

Como se muestra enFigura 20, configure una plantilla UDP para que una función realice la operación UDP. La operación prueba si el Dispositivo A puede recibir una respuesta del Dispositivo B.

Figura 20 Diagrama de red

Procedimiento de configuración

1. Asigne a cada interfaz una dirección IP. (No se muestran detalles).
2. Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).
3. Configurar el dispositivo B:

   # Habilite el servidor NQA.

   <DispositivoB> vista del sistema

   [DispositivoB] servidor nqa habilitado

   # Configure un servicio de escucha para escuchar la dirección IP 10.2.2.2 y el puerto UDP 9000.

   [DispositivoB] servidor nqa udp-echo 10.2.2.2 9000
4. Configurar el dispositivo A:

   # Crear plantilla UDP**udp**.

   <DispositivoA> vista del sistema

   [DispositivoA] plantilla nqa udp udp

   # Especifique 10.2.2.2 como dirección IP de destino.

   [DeviceA-nqatplt-udp-udp] ip de destino 10.2.2.2

   # Establezca el número de puerto de destino en 9000.

   [DeviceA-nqatplt-udp-udp] puerto de destino 9000

   # Si el número de sondeos exitosos consecutivos llega a 2, la operación tiene éxito. El cliente NQA notifica a la función del evento de operación exitosa.

   [DeviceA-nqatplt-udp-udp] sonda de activación de reacción-pase 2

   # Si el número de fallas de sonda consecutivas llega a 2, la operación falla. El cliente NQA notifica a la característica del error de operación.

   [DeviceA-nqatplt-udp-udp] sonda de activación de reacción-fallo 2

Ejemplo de configuración de plantilla HTTP

Requisitos de red

Como se muestra enFigura 21, configure una plantilla HTTP para que una característica realice la operación HTTP. La operación prueba si el cliente NQA puede obtener datos del servidor HTTP.

Figura 21 Diagrama de red

Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crear plantilla HTTP**http**.

<DispositivoA> vista del sistema

[DispositivoA] plantilla nqa http http

Especifique la URL del servidor.

[DispositivoA-nqatplt-http-http] URL http://10.2.2.2/index.htm

Configure la operación HTTP para obtener datos del servidor HTTP.

Obtención de operación [DeviceA-nqatplt-http-http]

Si el número de sondeos exitosos consecutivos llega a 2, la operación tiene éxito. El cliente NQA notifica a la función del evento de operación exitosa.

[DeviceA-nqatplt-http-http] sonda de activación de reacción-pase 2

Si el número de fallas de sonda consecutivas llega a 2, la operación falla. El cliente NQA notifica a la característica del error de operación.

[DeviceA-nqatplt-http-http] sonda de activación de reacción-fallo 2

Ejemplo de configuración de plantilla FTP

Requisitos de red

Como se muestra enFigura 22, configure una plantilla FTP para que una función realice la operación FTP. La operación prueba si el Dispositivo A puede cargar un archivo en el servidor FTP. El nombre de usuario y la contraseña de inicio de sesión son**administración**y **prueba del sistema**, respectivamente. El archivo que se transferirá al servidor FTP es**configuración.txt**.

Figura 22 Diagrama de red

Procedimiento de configuración

Asigne a cada interfaz una dirección IP. (No se muestran detalles).

Configure rutas estáticas o un protocolo de enrutamiento para asegurarse de que los dispositivos puedan comunicarse entre sí. (No se muestran detalles).

Crear plantilla FTP**ftp**.

<DispositivoA> vista del sistema

[DispositivoA] plantilla nqa ftp ftp

Especifique la URL del servidor FTP.

[DispositivoA-nqatplt-ftp-ftp] URL ftp://10.2.2.2

Especifique 10.1.1.1 como dirección IP de origen.

[DispositivoA-nqatplt-ftp-ftp] IP de origen 10.1.1.1

Configurar el dispositivo para cargar archivos**configuración.txt**al servidor FTP.

Operación [DeviceA-nqatplt-ftp-ftp] poner [DeviceA-nqatplt-ftp-ftp] nombre de archivo config.txt

Especifique el nombre de usuario para el inicio de sesión del servidor FTP como**administración**.

[DeviceA-nqatplt-ftp-ftp] nombre de usuario administrador

Especifique la contraseña para iniciar sesión en el servidor FTP como**prueba del sistema**.

[DeviceA-nqatplt-ftp-ftp] prueba de sistema simple de contraseña

Si el número de sondeos exitosos consecutivos llega a 2, la operación tiene éxito. El cliente NQA notifica a la función del evento de operación exitosa.

[DeviceA-nqatplt-ftp-ftp] sonda de activación de reacción-pase 2

Si el número de fallas de sonda consecutivas llega a 2, la operación falla. El cliente NQA notifica a la característica del error de operación.

[DeviceA-nqatplt-ftp-ftp] sonda de activación de reacción-fallo 2

Contenido

Configurando NTP

Sincronice su dispositivo con una fuente horaria confiable utilizando el Protocolo de hora de red (NTP) o cambiando la hora del sistema antes de ejecutarlo en una red activa. Varias tareas, incluida la gestión de red, la carga, la auditoría y la computación distribuida, dependen de una configuración precisa de la hora del sistema, porque las marcas de tiempo de los mensajes y registros del sistema utilizan la hora del sistema.

Descripción general

NTP se utiliza normalmente en redes grandes para sincronizar dinámicamente la hora entre dispositivos de red. Garantiza una mayor precisión del reloj que la configuración manual del reloj del sistema. En una red pequeña que no requiere una alta precisión del reloj, puede mantener la hora sincronizada entre dispositivos cambiando los relojes del sistema uno por uno.

NTP se ejecuta sobre UDP y utiliza el puerto UDP 123.

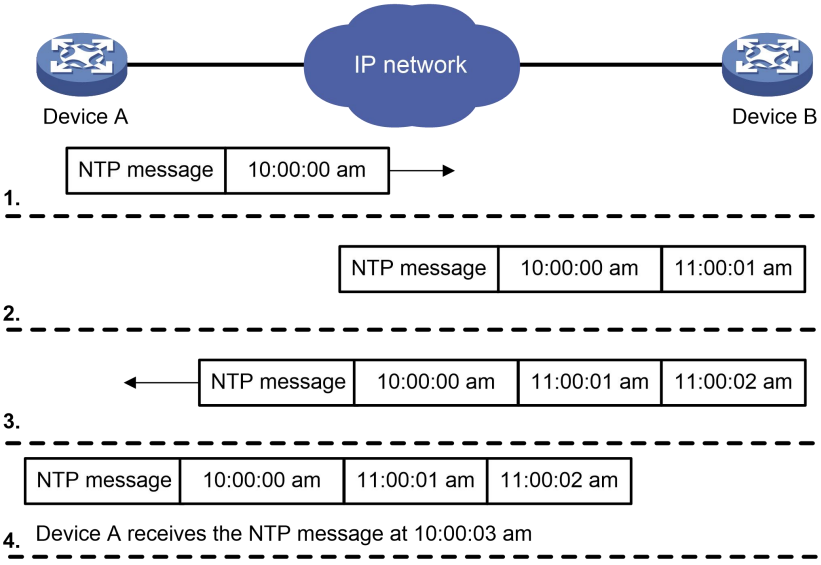
> **NOTA:**
> NTP solo se admite en las siguientes interfaces de Capa 3:
> - Interfaces Ethernet de capa 3.
> - Subinterfaces Ethernet de capa 3.
> - Interfaces agregadas de capa 3.
> - Subinterfaces agregadas de capa 3.
> - Interfaces VLAN e interfaces de túnel.

Cómo funciona NTP

Figura 1muestra cómo NTP sincroniza la hora del sistema entre dos dispositivos (Dispositivo A y Dispositivo B, en este ejemplo). Asumir que:

- Antes de la sincronización horaria, la hora del Dispositivo A y del Dispositivo B se establece en 10:00:00 am y 11:00:00 am, respectivamente.
- El dispositivo B se utiliza como servidor NTP. El dispositivo A debe sincronizarse con el dispositivo B.
- Un mensaje NTP tarda 1 segundo en viajar del dispositivo A al dispositivo B y del dispositivo B al dispositivo A.
- El dispositivo B tarda 1 segundo en procesar el mensaje NTP.

Figura 23 Flujo de trabajo básico



El proceso de sincronización es el siguiente:

1. El dispositivo A envía al dispositivo B un mensaje NTP, que tiene una marca de tiempo cuando sale del dispositivo A. La marca de tiempo es las 10:00:00 am (T1).
2. Cuando este mensaje NTP llega al Dispositivo B, el Dispositivo B agrega una marca de tiempo que muestra la hora en que el mensaje llegó al Dispositivo B. La marca de tiempo es las 11:00:01 am (T2).
3. Cuando el mensaje NTP sale del Dispositivo B, el Dispositivo B agrega una marca de tiempo que muestra la hora en que el mensaje salió del Dispositivo B. La marca de tiempo es las 11:00:02 am (T3).
4. Cuando el dispositivo A recibe el mensaje NTP, la hora local del dispositivo A es las 10:00:03 am (T4).

Hasta ahora, el Dispositivo A puede calcular los siguientes parámetros en función de las marcas de tiempo:

- El retraso de ida y vuelta del mensaje NTP: Retraso = (T4 – T1) – (T3 – T2) = 2 segundos. Diferencia horaria
- entre el Dispositivo A y el Dispositivo B: Compensación = ((T2 – T1) + (T3 – T4)) /2 = 1 hora.

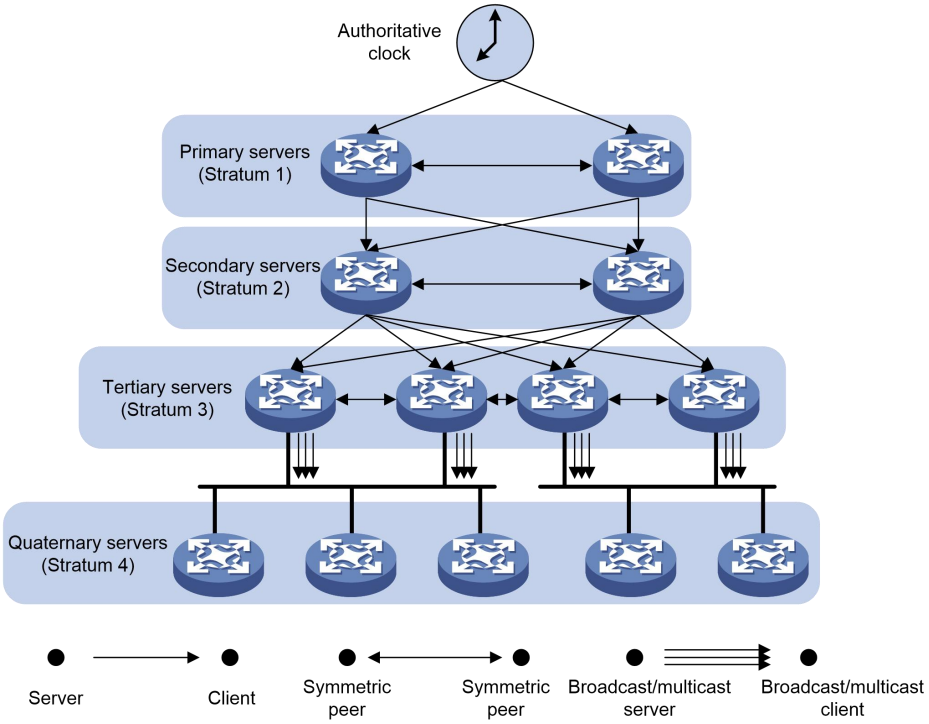
Según estos parámetros, el dispositivo A se puede sincronizar con el dispositivo B.

Esta es sólo una descripción aproximada del mecanismo de trabajo de NTP. Para obtener más información, consulte los protocolos y estándares relacionados.

arquitectura NTP

NTP utiliza los estratos 1 a 16 para definir la precisión del reloj, como se muestra enFigura 2. Un valor de estrato más bajo representa una mayor precisión. Los relojes de los estratos 1 al 15 están en estado sincronizado y los relojes del estrato 16 no están sincronizados.

Figura 24 Arquitectura NTP



Un servidor NTP de estrato 1 obtiene su hora de una fuente de hora autorizada, como un reloj atómico. Proporciona tiempo para otros dispositivos como servidor NTP principal. Un servidor de tiempo de estrato 2 recibe su tiempo de un servidor de tiempo de estrato 1, y así sucesivamente.

Para garantizar la precisión y la disponibilidad de la hora, puede especificar varios servidores NTP para un dispositivo. El dispositivo selecciona un servidor NTP óptimo como fuente de reloj en función de parámetros como el estrato. El reloj que selecciona el dispositivo se llama fuente de referencia. Para obtener más información sobre la selección de reloj, consulte los protocolos y estándares relacionados.

Si los dispositivos de una red no pueden sincronizarse con una fuente horaria autorizada, puede realizar las siguientes tareas:

- Seleccione un dispositivo que tenga un reloj relativamente preciso de la red.
- Utilice el reloj local del dispositivo como reloj de referencia para sincronizar otros dispositivos en la red.

Modos de asociación

NTP admite los siguientes modos de asociación:

- Modo cliente/servidor
- Modo activo/pasivo simétrico Modo
- de transmisión
- Modo de multidifusión

Tabla 3 Modos de asociación NTP

Modo	Proceso de trabajo	Principio	Escenario de aplicación
Servidor de cliente	En el cliente, especifique la dirección IP del servidor NTP. Un cliente envía un mensaje de sincronización de reloj a los servidores NTP. Al recibir el mensaje, los servidores operar automáticamente en modo servidor y enviar una respuesta. Si el cliente se puede sincronizar con varios servidores de hora, selecciona un reloj óptimo y sincroniza su reloj local con la fuente de referencia óptima después de recibir las respuestas de los servidores.	Un cliente puede sincronizarse con un servidor, pero un servidor no puede sincronizarse con un cliente.	ComoFigura 2muestra, este modo está diseñado para configuraciones donde dispositivos de un estrato superior se sincronizan con dispositivos con un estrato inferior.
Simétrico activo pasivo	En el par activo simétrico, especifique la dirección IP del par pasivo simétrico. Un par activo simétrico envía periódicamente mensajes de sincronización de reloj a un par pasivo simétrico. El par pasivo simétrico Opera automáticamente en modo pasivo simétrico y envía una respuesta. Si el par activo simétrico se puede sincronizar con varios servidores de hora, selecciona un reloj óptimo y sincroniza su reloj local con la fuente de referencia óptima después de recibir las respuestas de los servidores.	Un par activo simétrico y un par simétrico El par pasivo se puede sincronizar con cada uno. otro. Si ambos están sincronizados, el par con un estrato superior está sincronizado con el pares de estrato inferior.	ComoFigura 2Como muestra, este modo se usa con mayor frecuencia entre servidores con el mismo estrato para operar como respaldo para uno. otro. Si un servidor no puede comunicarse con todos los servidores de un estrato inferior, el servidor aún puede sincronizar con los servidores del mismo estrato.
Transmisión	Un servidor envía periódicamente mensajes de sincronización de reloj a la dirección de transmisión. 255.255.255.255. Los clientes escuchan los mensajes de difusión de los servidores para sincronizarlos con el servidor de acuerdo con la mensajes de difusión. Cuando un cliente recibe el primer mensaje de difusión, el cliente y el servidor comienzan a intercambiar mensajes para calcular el retraso de la red entre ellos. Entonces, sólo el servidor de transmisión envía mensajes de sincronización de reloj.	Un cliente de transmisión puede sincronizarse con un servidor de difusión, pero un servidor de difusión no puede sincronizarse con un cliente de transmisión.	Un servidor de transmisión envía sincronización de reloj mensajes para sincronizar clientes en el mismo subred. ComoFigura 2 programas, el modo de transmisión está diseñado para configuraciones que involucran uno o varios servidores y una población de clientes potencialmente grande. El modo de transmisión tiene una precisión de tiempo menor que el cliente/servidor y los modos activo/pasivo simétrico porque solo los servidores de transmisión envían sincronización de reloj mensajes.

Modo	Proceso de trabajo	Principio	Escenario de aplicación
Multidifusión	Un servidor de multidifusión envía periódicamente mensajes de sincronización de reloj a la dirección de multidifusión configurada por el usuario. Los clientes escuchan los mensajes de multidifusión de los servidores y se sincronizan con el servidor de acuerdo con los mensajes recibidos.	Un cliente de multidifusión puede sincronizarse con un servidor de multidifusión, pero un servidor de multidifusión no puede sincronizarse con un cliente de multidifusión.	Un servidor de multidifusión puede proporcionar tiempo sincronización para clientes en la misma subred o en diferentes subredes. El modo multicast tiene una precisión de tiempo menor que el modo cliente/servidor y modos simétricos activo/pasivo.

En este documento, un "servidor NTP" o un "servidor" se refiere a un dispositivo que funciona como servidor NTP en modo cliente/servidor. Los servidores de hora se refieren a todos los dispositivos que pueden proporcionar sincronización horaria, incluidos servidores NTP, pares simétricos NTP, servidores de transmisión y servidores de multidifusión.

seguridad NTP

Para mejorar la seguridad de la sincronización horaria, NTP proporciona funciones de autenticación y control de acceso.

control de acceso NTP

Puede controlar el acceso a NTP mediante una ACL. Los derechos de acceso están en el siguiente orden, de menos restrictivos a más restrictivos:

- **Par**—Permite solicitudes de tiempo y consultas de control NTP (como alarmas, estado de autenticación e información del servidor de tiempo) y permite que el dispositivo local se sincronice con un dispositivo par.
- **Servidor**—Permite solicitudes de tiempo y consultas de control NTP, pero no permite que el dispositivo local se sincronice con un dispositivo par.
- **Sincronización**—Permite solo solicitudes de tiempo de un sistema cuya dirección pasa los criterios de la lista de acceso.
- **Consulta**—Permite solo consultas de control NTP desde un dispositivo par al dispositivo local.

El dispositivo procesa una solicitud NTP de la siguiente manera:

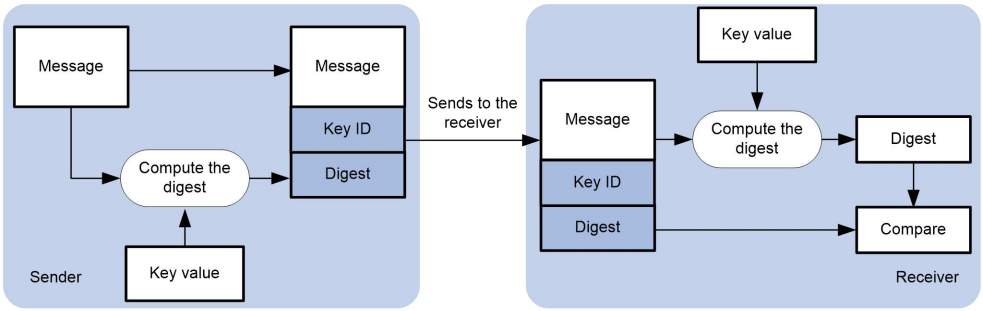
- Si no se configura ningún control de acceso NTP,**par**se otorga al dispositivo local y a los dispositivos pares.
- Si la dirección IP del dispositivo par coincide con una**permiso**declaración en una ACL para más de un derecho de acceso, el derecho de acceso menos restrictivo se otorga al dispositivo par. si un**denegar**declaración o no coincide ninguna ACL, no se concede ningún derecho de acceso.
- Si no se crea ninguna ACL para un derecho de acceso, no se otorga el derecho de acceso asociado. Si no se
- crea ninguna ACL para ningún derecho de acceso,**par**se concede.

Esta característica proporciona una seguridad mínima para un sistema que ejecuta NTP. Un método más seguro es la autenticación NTP.

autenticación NTP

Utilice esta función para autenticar los mensajes NTP por motivos de seguridad. Si un mensaje NTP pasa la autenticación, el dispositivo puede recibirlo y obtener información de sincronización horaria. En caso contrario, el dispositivo descarta el mensaje. Esta función garantiza que el dispositivo no se sincronice con un servidor de hora no autorizado.

Figura 25 Autenticación NTP



Como se muestra enfigura 3, la autenticación NTP funciona de la siguiente manera:

1. El remitente utiliza el algoritmo MD5 para calcular el mensaje NTP según la clave identificada por un ID de clave. Luego, envía el resumen calculado junto con el mensaje NTP y la ID de clave al receptor.
2. Al recibir el mensaje, el receptor realiza las siguientes acciones:

   a.Encuentra la clave según el ID de clave en el mensaje.

   b.Utiliza el algoritmo MD5 para calcular el resumen.

   C.Compara el resumen con el resumen contenido en el mensaje NTP. Si son iguales, el receptor acepta el mensaje. De lo contrario, descarta el mensaje.

NTP para MPLS L3VPN

En una red MPLS L3VPN, el dispositivo admite múltiples instancias de VPN cuando:

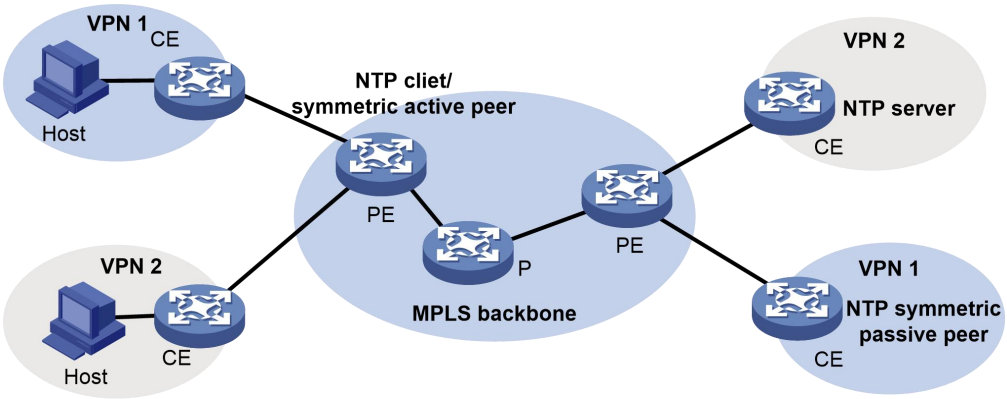
- Funciona como un cliente NTP para sincronizarse con el servidor NTP.
- Funciona como un par activo simétrico para sincronizarse con el par pasivo simétrico.

Solo los modos cliente/servidor y simétrico activo/pasivo admiten instancias de VPN.

Como se muestra enFigura 4, los usuarios de VPN 1 y VPN 2 están conectados a la red troncal MPLS a través de dispositivos de borde de proveedor (PE) y los servicios de las dos VPN están aislados. La sincronización horaria entre los PE y los dispositivos de las dos VPN se puede realizar si realiza las siguientes tareas:

- Configure los PE para que funcionen en cliente NTP o en modo activo simétrico.
- Especifique la VPN a la que pertenece el servidor NTP o el par pasivo simétrico NTP.

Figura 26 Diagrama de red



Protocolos y estándares

- RFC 1305,*Especificación, implementación y análisis del protocolo de tiempo de red (versión 3)* RFC
- 5905,*Protocolo de tiempo de red versión 4: especificación de protocolos y algoritmos*

Restricciones y pautas de configuración

Cuando configure NTP, siga estas restricciones y pautas:

- No puede configurar NTP y SNTP en el mismo dispositivo. No
- configure NTP en un puerto miembro agregado.
- El servicio NTP y el servicio SNTP son mutuamente excluyentes. Sólo puede habilitar el servicio NTP o el servicio SNTP a la vez.
- Para garantizar la precisión de la sincronización horaria, no especifique más de una fuente de referencia. Hacerlo podría provocar cambios de hora frecuentes o incluso fallos de sincronización.
- Asegúrate de utilizar el**protocolo de reloj**comando para especificar el protocolo de tiempo como NTP. Para más información sobre el**protocolo de reloj**comando, ver*Referencia de comandos fundamentales*.

Lista de tareas de configuración

Tareas de un vistazo
(Requerido.)Habilitando el servicio NTP
(Obligatorio.) Realice al menos una de las siguientes tareas: - Configurar el modo de asociación NTP Configurar el - reloj local como fuente de referencia
(Opcional.)Configurar derechos de control de acceso
(Opcional.)Configurar la autenticación NTP
(Opcional.)Configuración de parámetros opcionales de NTP

Habilitando el servicio NTP

Paso	**Dominio**	**Observaciones**
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite el servicio NTP.	**habilitación del servicio ntp**	De forma predeterminada, el servicio NTP no está habilitado.

Configurar el modo de asociación NTP

Esta sección describe cómo configurar los modos de asociación NTP.

Configurar NTP en modo cliente/servidor

Cuando el dispositivo funciona en modo cliente/servidor, especifique la dirección IP del servidor en el cliente. Siga estas pautas cuando configure un cliente NTP:

- Un servidor debe estar sincronizado mediante otros dispositivos o utilizar su reloj local como fuente de referencia antes de sincronizar un cliente NTP. De lo contrario, el cliente no se sincronizará con el servidor NTP.
- Si el nivel de estrato de un servidor es superior o igual al de un cliente, el cliente no se sincronizará con ese servidor.
- Puede configurar varios servidores repitiendo el proceso**servidor-unicast-servicio-ntp**y **servidor-unicast-ipv6-servicio-ntp**comandos.

Para configurar un cliente NTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Especifique un servidor NTP para el dispositivo.	- Especifique un servidor NTP para el dispositivo: **servidor-unicast-servicio-ntp** { *nombre del servidor*| *dirección IP*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*| **prioridad**|**fuente** *Tipo de interfaz* *número de interfaz*|**versión** *número*] * - Especifique un servidor NTP IPv6 para el dispositivo: **servicio ntp ipv6** **servidor de unidifusión**{*nombre del servidor* | *dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*| **prioridad**|**fuente** *Tipo de interfaz* *número de interfaz*] *	De forma predeterminada, no se especifica ningún servidor NTP para el dispositivo.

Configuración de NTP en modo activo/pasivo simétrico

Cuando el dispositivo funciona en modo activo/pasivo simétrico, especifique en un par activo simétrico la dirección IP para un par pasivo simétrico.

Siga estas pautas cuando configure un par activo simétrico:

- Ejecute el**habilitación del servicio ntp**comando en un par pasivo simétrico para habilitar NTP. De lo contrario, el par simétrico-pasivo no procesará mensajes NTP de un par simétrico-activo.
- El par simétrico activo, el par simétrico pasivo o ambos deben estar en estado sincronizado. De lo contrario, su hora no se podrá sincronizar.
- Puede configurar varios pares pasivos simétricos repitiendo el procedimiento**par de unidifusión de servicio ntp**o**servicio-ntp ipv6 par-unicast**dominio.

Para configurar un par simétrico-activo:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A

Paso	Dominio	Observaciones
2. Especifique un par pasivo simétrico para el dispositivo.	- Especifique un par simétrico-pasivo: **par de unidifusión de servicio ntp** {*nombre de compañero*|*dirección IP*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*|**prioridad**|**fuente** *Tipo de interfaz número de interfaz*|**versión** *número*] * - Especificar un IPv6 par simétrico-pasivo: **servicio ntp ipv6 par de unidifusión**{*nombre de compañero*| *dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*|**prioridad**|**fuente** *Tipo de interfaz número de interfaz*] *	De forma predeterminada, no se especifica ningún igual pasivo simétrico.

Configurar NTP en modo transmisión

Un servidor de transmisión debe sincronizarse mediante otros dispositivos o usar su reloj local como fuente de referencia antes de sincronizar un cliente de transmisión. De lo contrario, el cliente de transmisión no se sincronizará con el servidor de transmisión.

Configure NTP en modo de transmisión tanto en el servidor de transmisión como en el cliente.

Configurar un cliente de transmisión

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	Ingrese a la interfaz para recibir mensajes de transmisión NTP.
3. Configure el dispositivo para que funcione en modo de cliente de transmisión.	**cliente de transmisión de servicio ntp**	De forma predeterminada, el dispositivo no funciona en modo cliente de transmisión. Después de ejecutar el comando, el dispositivo recibe NTP transmitir mensajes desde la interfaz especificada.

Configurar el servidor de transmisión

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	Ingrese a la interfaz para enviar mensajes de difusión NTP.

Paso	Dominio	Observaciones
3. Configure el dispositivo para que funcione en modo de servidor de transmisión NTP.	**servidor de transmisión de servicio ntp** [**ID de clave de autenticación***ID de clave*| **versión***número*] *	De forma predeterminada, el dispositivo no funciona en modo de servidor de transmisión. Después de ejecutar el comando, el dispositivo recibe NTP transmitir mensajes desde la interfaz especificada.

Configurar NTP en modo multidifusión

Un servidor de multidifusión debe estar sincronizado por otros dispositivos o utilizar su reloj local como fuente de referencia antes de sincronizar un cliente de multidifusión. De lo contrario, el cliente de multidifusión no se sincronizará con el servidor de multidifusión.

Configure NTP en modo de multidifusión tanto en un servidor como en un cliente de multidifusión.

Configurar un cliente de multidifusión

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	Ingrese a la interfaz para recibir mensajes de multidifusión NTP.
3. Configure el dispositivo para que funcione en modo cliente de multidifusión.	- Configure el dispositivo para que funcione en modo cliente de multidifusión: **cliente-multidifusión-servicio-ntp** [*dirección IP*] - Configure el dispositivo para que funcione en modo cliente de multidifusión IPv6: **servicio ntp ipv6 cliente de multidifusión** *dirección-multidifusión-ipv6*	De forma predeterminada, el dispositivo no funciona en modo cliente de multidifusión. Como práctica recomendada, especifique una dirección IP de multidifusión en el rango de 224.0.1.0 a 224.0.1.255 para el *dirección IP*argumento. Después de ejecutar el comando, el dispositivo recibe mensajes de multidifusión NTP desde la interfaz especificada.

Configurar el servidor de multidifusión

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	Ingrese a la interfaz para enviar mensajes de multidifusión NTP.
3. Configure el dispositivo para que funcione en modo de servidor de multidifusión.	- Configure el dispositivo para que funcione en modo de servidor de multidifusión: **servidor-multidifusión-servicio-ntp** [*dirección IP*] [**ID de clave de autenticación***ID de clave*| **ttl***número-ttl*|**versión** *número*] * - Configure el dispositivo para que funcione en modo de servidor de multidifusión: **servicio ntp ipv6 servidor de multidifusión** *dirección-multidifusión-ipv6* [**ID de clave de autenticación***ID de clave*| **ttl***número-ttl*] *	De forma predeterminada, el dispositivo no funciona en modo de servidor de multidifusión. Como práctica recomendada, especifique una dirección IP de multidifusión en el rango de 224.0.1.0 a 224.0.1.255 para el *dirección IP*argumento. Después de ejecutar el comando, el dispositivo envía mensajes de multidifusión NTP desde la interfaz especificada.

Configurar derechos de control de acceso

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configure el derecho de control de acceso al servicio NTP para que un dispositivo par acceda al dispositivo local.	- Configure el derecho de control de acceso al servicio NTP para que un dispositivo par acceda al dispositivo local **acceso al servicio ntp**{**par**|**consulta**|**servidor**|**sincronización**} *número-acl* - Configure el derecho de control de acceso al servicio IPv6 NTP para que un dispositivo par acceda al dispositivo local **servicio ntp ipv6**{**par**|**consulta**|**servidor**|**sincronización**}**accl** *número-acl*	De forma predeterminada, el derecho de control de acceso al servicio NTP para que un dispositivo par acceda al dispositivo local es par.

Antes de configurar el derecho de control de acceso al servicio NTP para el dispositivo local, cree y configure una ACL asociada con el derecho de control de acceso. Para obtener más información sobre ACL, consulte *Guía de configuración de ACL y QoS*.

Configurar la autenticación NTP

Esta sección proporciona instrucciones para configurar la autenticación NTP.

Configurar la autenticación NTP en modo cliente/servidor

Cuando configura la autenticación NTP en modo cliente/servidor:

- Habilite la autenticación NTP.
- Configure una clave de autenticación.
- Establezca la clave como clave confiable tanto en el cliente como en
- el servidor. Asocie la clave con el servidor NTP en el cliente.

Los ID de clave y los valores de clave configurados en el servidor y el cliente deben ser los mismos. De lo contrario, la autenticación NTP falla.

Para configurar la autenticación NTP para un cliente:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
3. Configurar un NTP clave de autenticación.	**servicio ntp** **ID de clave de autenticación** *ID de clave* **modo de autenticación md5** {**cifrar**|**simple**} *valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
4. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación** *ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Paso	Dominio	Observaciones
5. Asocie la clave especificada con un servidor NTP.	- Asocie la clave especificada con un servidor NTP: **servidor-unicast-servicio-ntp** { *nombre del servidor*| *dirección IP*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave* - Asocie la clave especificada con un servidor NTP IPv6: **servicio ntp ipv6** **servidor de unidifusión**{*nombre del servidor* | *dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave*	N / A

Para configurar la autenticación NTP para un servidor:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
3. Configurar un NTP clave de autenticación.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
4. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Los resultados de la autenticación NTP difieren cuando se realizan diferentes configuraciones en el cliente y el servidor. Para más información, verTabla 2. (N/A en la tabla significa que si se realiza o no la configuración no hace ninguna diferencia).

Tabla 4 Resultados de la autenticación NTP

Cliente			Servidor		
Habilitar NTP autenticación norte	**Configurar cada llave y configurar** es como un **confiable llave**	**Asociar el llave con un servidor NTP**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **clave confiable**	**Autenticación resultado**
Sí	Sí	Sí	Sí	Sí	Tuvo éxito. NTP los mensajes pueden ser enviado y recibido correctamente.
Sí	Sí	Sí	Sí	No	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.

Cliente			Servidor		Autenticación resultado
Habilitar NTP autenticación norte	Configurar cada llave y configurar es como un confiable llave	Asociar el llave con un servidor NTP	Habilitar NTP autenticación norte	Configurar una llave y configurar es como un clave confiable	
Sí	Sí	Sí	No	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	No	Sí	N / A	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	N / A	No	N / A	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.
No	N / A	N / A	N / A	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.

Configuración de la autenticación NTP en modo activo/pasivo simétrico

Cuando configura la autenticación NTP en modo de pares simétricos:

- Habilite la autenticación NTP.
- Configure una clave de autenticación.
- Establezca la clave como clave confiable tanto en el par activo como en el
- par pasivo. Asocie la clave con el par pasivo del par activo.

Los ID de clave y los valores de clave configurados en el par activo y en el par pasivo deben ser los mismos. De lo contrario, la autenticación NTP falla.

Para configurar la autenticación NTP para un par activo:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
3. Configurar un NTP clave de autenticación.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.

Traducido del inglés al español - www.onlinedoctranslator.com

Paso	Dominio	Observaciones
4. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.
5. Asocie la clave especificada con un par pasivo.	- Asocie la clave especificada con un par pasivo: **par de unidifusión de servicio ntp** {*dirección IP*|*nombre de compañero*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave* - Asocie la clave especificada con un par pasivo: **servicio ntp ipv6** **par de unidifusión**{*dirección ipv6*|*nombre de compañero*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave*	N / A

Para configurar la autenticación NTP para un par pasivo:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
3. Configurar un NTP clave de autenticación.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
4. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Los resultados de la autenticación NTP difieren cuando se realizan diferentes configuraciones en el par activo y en el par pasivo. Para más información, verTabla 3. (N/A en la tabla significa que si se realiza o no la configuración no hace ninguna diferencia).

Tabla 5 Resultados de la autenticación NTP

Compañero activo			Par pasivo		
Habilitar NTP autenticación norte	**Configurar una llave y configurar** es como un **clave confiable**	**asociado e la clave con un pasivo par**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **confiable llave**	**Autenticación resultado**
No se considera el nivel de estrato de los pares activos y pasivos.					
Sí	Sí	Sí	Sí	Sí	Tuvo éxito. NTP los mensajes pueden ser enviado y recibido correctamente.
Sí	Sí	Sí	Sí	No	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.

Compañero activo			Par pasivo		
Habilitar NTP autenticación norte	**Configurar una llave y configurar** es como un **clave confiable**	**asociado e la clave con un pasivo par**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **confiable llave**	**Autenticación resultado**
Sí	Sí	Sí	No	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
Sí	N / A	No	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
Sí	N / A	No	No	N / A	Sin autenticacion. Los mensajes NTP pueden ser enviado y recibido correctamente.
No	N / A	N / A	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
No	N / A	N / A	No	N / A	Sin autenticacion. Los mensajes NTP pueden ser enviado y recibido correctamente.
El par activo tiene un estrato más alto que el par pasivo.					
Sí	No	Sí	N / A	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
El par pasivo tiene un estrato más alto que el par activo.					
Sí	No	Sí	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
Sí	No	Sí	No	N / A	Sin autenticacion. Los mensajes NTP pueden ser enviado y recibido correctamente.

Configurar la autenticación NTP en modo transmisión

Cuando configura la autenticación NTP en modo de transmisión:

- Habilite la autenticación NTP.
- Configure una clave de autenticación.
- Establezca la clave como clave confiable tanto en el cliente como en el servidor de
- transmisión. Configure una clave de autenticación NTP en el servidor de transmisión.

Los ID de clave y los valores de clave configurados en el servidor de transmisión y el cliente deben ser los mismos. De lo contrario, la autenticación NTP falla.

Para configurar la autenticación NTP para un cliente de transmisión:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
3. Configurar un NTP clave de autenticación.	**servicio ntp ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
4. Configure la clave como una clave confiable.	**servicio ntp confiable ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Para configurar la autenticación NTP para un servidor de transmisión:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
3. Configurar un NTP clave de autenticación.	**servicio ntp ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
4. Configure la clave como una clave confiable.	**servicio ntp confiable ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.
5. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
6. Asocie la clave especificada con el servidor de transmisión.	**ID de clave de autenticación del servidor de transmisión del servicio ntp***ID de clave*	De forma predeterminada, el servidor de transmisión no está asociado con ninguna clave.

Los resultados de la autenticación NTP difieren cuando se realizan diferentes configuraciones en el cliente y el servidor de transmisión. Para más información, verTabla 4. (N/A en la tabla significa que si se realiza o no la configuración no hace ninguna diferencia).

Tabla 6 Resultados de la autenticación NTP

servidor de transmisión			Cliente de transmisión		Resultado de la autenticación
Habilitar NTP autenticación norte	**Configurar cada llave y configurar** es como un **confiable llave**	**asociado e la clave con un transmisiones servidor t**	**Habilitar NTP autenticación** norte	**Configurar cada llave y configurar** es como un **confiable llave**	**Resultado de la autenticación**
Sí	Sí	Sí	Sí	Sí	Tuvo éxito. NTP Los mensajes se pueden enviar y recibir correctamente.
Sí	Sí	Sí	Sí	No	Fallido. mensajes NTP no se puede enviar y recibir correctamente.

servidor de transmisión			Cliente de transmisión		Resultado de la autenticación
Habilitar NTP autenticación norte	**Configurar cada llave y configurar es como un confiable llave**	**asociado e la clave con un transmisiones servidor t**	**Habilitar NTP autenticación** norte	**Configurar cada llave y configurar es como un confiable llave**	
Sí	Sí	Sí	No	N / A	Fallido. mensajes NTP no se puede enviar y recibir correctamente.
Sí	No	Sí	Sí	N / A	Fallido. mensajes NTP no se puede enviar y recibir correctamente.
Sí	No	Sí	No	N / A	Sin autenticacion. NTP Los mensajes se pueden enviar y recibir correctamente.
Sí	N / A	No	Sí	N / A	Fallido. mensajes NTP no se puede enviar y recibir correctamente.
Sí	N / A	No	No	N / A	Sin autenticacion. NTP Los mensajes se pueden enviar y recibir correctamente.
No	N / A	N / A	Sí	N / A	Fallido. mensajes NTP no se puede enviar y recibir correctamente.
No	N / A	N / A	No	N / A	Sin autenticacion. NTP Los mensajes se pueden enviar y recibir correctamente.

Configurar la autenticación NTP en modo multidifusión

Cuando configura la autenticación NTP en modo multidifusión:

- Habilite la autenticación NTP.
- Configure una clave de autenticación.
- Establezca la clave como clave confiable tanto en el cliente como en el servidor de multidifusión.
- Configure una clave de autenticación NTP en el servidor de multidifusión.

Los ID de clave y los valores de clave configurados en el servidor y el cliente de multidifusión deben ser los mismos. De lo contrario, la autenticación NTP falla.

Para configurar la autenticación NTP para un cliente de multidifusión:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
3. Configurar un NTP clave de autenticación.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.

Paso	Dominio	Observaciones
4. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Para configurar la autenticación NTP para un servidor de multidifusión:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
3. Configurar un NTP clave de autenticación.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
4. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.
5. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
6. Asocie la clave especificada con el servidor de multidifusión.	- Asocie la clave especificada con un servidor de multidifusión: **servidor-multidifusión-servicio-ntp** [*dirección IP*] **ID de clave de autenticación***ID de clave* - Asocie la clave especificada con un servidor de multidifusión IPv6: **servicio ntp ipv6** **servidor de multidifusión** *dirección-multidifusión-ipv6* **ID de clave de autenticación***ID de clave*	De forma predeterminada, no hay ningún servidor de multidifusión asociado con la clave especificada.

Los resultados de la autenticación NTP difieren cuando se realizan diferentes configuraciones en el cliente y el servidor de transmisión. Para más información, verTabla 5. (N/A en la tabla significa que si se realiza o no la configuración no hace ninguna diferencia).

Tabla 7 Resultados de la autenticación NTP

Servidor de multidifusión			Cliente de multidifusión		
Habilitar NTP autenticación norte	**Configurar una llave y configurar** es como un **clave confiable**	**Asociado la llave con** una multidifusión **servidor**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **clave confiable**	**Autenticación** resultado
Sí	Sí	Sí	Sí	Sí	Tuvo éxito. NTP los mensajes pueden ser enviado y recibido correctamente.
Sí	Sí	Sí	Sí	No	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.

Servidor de multidifusión			Cliente de multidifusión		
Habilitar NTP autenticación norte	**Configurar una llave y configurar** es como un **clave confiable**	**Asociado la llave con** una multidifusión **servidor**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **clave confiable**	**Autenticación** resultado
Sí	Sí	Sí	No	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	No	Sí	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	No	Sí	No	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.
Sí	N / A	No	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	N / A	No	No	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.
No	N / A	N / A	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
No	N / A	N / A	No	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.

Configuración de parámetros opcionales de NTP

Las tareas de configuración de esta sección son tareas opcionales. Configúrelos para mejorar la seguridad, el rendimiento o la confiabilidad de NTP.

Especificación de la interfaz de origen para mensajes NTP

Para evitar que los cambios de estado de la interfaz causen fallas en la comunicación NTP, configure el dispositivo para usar la dirección IP de una interfaz que esté siempre activa. Por ejemplo, puede configurar el dispositivo para utilizar una interfaz de bucle invertido como dirección IP de origen para los mensajes NTP que se enviarán.

Cuando el dispositivo responde a una solicitud NTP, la dirección IP de origen de la respuesta NTP es siempre la dirección IP de la interfaz que recibió la solicitud NTP.

Siga estas pautas cuando especifique la interfaz de origen para mensajes NTP:

- Si ha especificado la interfaz de origen para los mensajes NTP en el**servicio ntp**[**ipv6**] **servidor de unidifusión**o**servicio ntp**[**ipv6**]**par de unidifusión**comando, la interfaz especificada en el **servicio ntp**[**ipv6**]**servidor de unidifusión**o**servicio ntp**[**ipv6**]**par de unidifusión**El comando funciona como interfaz de origen para mensajes NTP.
- Si ha configurado el**servidor de transmisión de servicio ntp**o**servicio ntp**[**ipv6**] **servidor de multidifusión**comando, la interfaz de origen para los mensajes NTP de difusión o multidifusión es la interfaz configurada con el comando respectivo.

Para especificar la interfaz de origen para mensajes NTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Especifique la interfaz de origen para los mensajes NTP.	- Especifique la interfaz de origen para los mensajes NTP: **fuente de servicio ntp** *Tipo de interfaz* *número de interfaz* - Especifique la interfaz de origen para los mensajes NTP IPv6: **fuente ipv6 del servicio ntp** *Tipo de interfaz* *número de interfaz*	De forma predeterminada, no se especifica ninguna interfaz de origen para los mensajes NTP.

Deshabilitar una interfaz para que no reciba mensajes NTP

Cuando NTP está habilitado, todas las interfaces de forma predeterminada pueden recibir mensajes NTP. Por motivos de seguridad, puede desactivar algunas de las interfaces para que no reciban mensajes NTP.

Para desactivar una interfaz para que no reciba mensajes NTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz* *número de interfaz*	N / A
3. Deshabilite la interfaz para que no reciba mensajes NTP.	- Para IPv4: **deshacer la habilitación entrante del servicio ntp** - Para IPv6: **deshacer el servicio ntp ipv6 habilitación entrante**	De forma predeterminada, una interfaz recibe mensajes NTP.

Configurar el número máximo de asociaciones dinámicas

NTP tiene los siguientes tipos de asociaciones:

- **Asociación estática**—Una asociación creada manualmente.
- **Asociación dinámica**—Asociación temporal creada por el sistema durante la operación NTP. Una asociación dinámica se elimina si no se intercambian mensajes en aproximadamente 12 minutos.

A continuación se describe cómo se establece una asociación en diferentes modos de asociación:

- **Modo cliente/servidor**—Después de especificar un servidor NTP, el sistema crea una asociación estática en el cliente. El servidor simplemente responde pasivamente al recibir un mensaje, en lugar de crear una asociación (estática o dinámica).
- **Modo activo/pasivo simétrico**—Después de especificar un par simétrico-pasivo en un par simétrico-activo, se crean asociaciones estáticas en el par simétrico-activo y asociaciones dinámicas en el par simétrico-pasivo.
- **Modo de transmisión o multidifusión**—Las asociaciones estáticas se crean en el servidor y las asociaciones dinámicas se crean en el cliente.

Un único dispositivo puede tener un máximo de 128 asociaciones simultáneas, incluidas asociaciones estáticas y asociaciones dinámicas.

Realice esta tarea para restringir el número de asociaciones dinámicas y evitar que ocupen demasiados recursos del sistema.

Para configurar el número máximo de asociaciones dinámicas:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configurar el máximo número de sesiones dinámicas que se permite establecer.	**servicio ntp sesiones-max-dinamicas***número*	Por defecto, el comando puede establecer hasta 100 sesiones dinámicas.

Establecer un valor DSCP para paquetes NTP

El valor DSCP determina la prioridad de envío de un paquete. Para

establecer un valor DSCP para paquetes NTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Establezca un valor DSCP para paquetes NTP.	- Paquetes IPv4: **servicio ntp dscp***valor-dscp* - Paquetes IPv6: **servicio ntp ipv6 dscp** *valor-dscp*	Los valores predeterminados para un valor DSCP: - 48 para paquetes IPv4 NTP. - 56 para paquetes IPv6 NTP.

Configurar el reloj local como fuente de referencia

Siga estas pautas cuando configure el reloj local como fuente de referencia:

- Asegúrese de que el reloj local pueda proporcionar la precisión horaria requerida para la red. Después de configurar el reloj local como fuente de referencia, el reloj local se sincroniza y puede funcionar como servidor de hora para sincronizar otros dispositivos en la red. Si el reloj local es incorrecto, se producen errores de sincronización.
- Antes de configurar esta función, ajuste la hora del sistema local para asegurarse de que sea precisa.
- Los dispositivos se diferencian por el hardware y la precisión del reloj. Para evitar fluctuaciones en la red y fallas en la sincronización del reloj, no configure múltiples fuentes de referencia en la misma red.

Para configurar el reloj local como fuente de referencia:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A

Paso	Dominio	Observaciones
2. Configure el reloj local como fuente de referencia.	**servicio ntp refclock-master** [*dirección IP*] [*estrato*]	De forma predeterminada, el dispositivo no utiliza el reloj local como fuente de referencia.

Visualización y mantenimiento de NTP

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Muestra información sobre asociaciones NTP IPv6.	**mostrar sesiones ipv6 de servicio ntp**[**verboso**]
Muestra información sobre asociaciones NTP IPv4.	**mostrar sesiones de servicio ntp**[**verboso**]
Muestra información sobre el estado del servicio NTP.	**mostrar el estado del servicio ntp**
Muestre información breve sobre los servidores NTP desde el dispositivo local a la fuente de referencia principal.	**mostrar el seguimiento del servicio ntp**

Ejemplos de configuración NTP

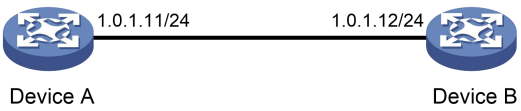
Ejemplo de configuración del modo cliente/servidor NTP

Requisitos de red

Como se muestra enFigura 5, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo B para que funcione en modo cliente y el Dispositivo A para que se utilice como servidor NTP para el Dispositivo B.

Figura 27 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 5. (No se muestran detalles).
2. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2
3. Configurar el dispositivo B:

   # Habilite el servicio NTP.

   <DispositivoB> vista del sistema

   [DispositivoB] habilitación del servicio ntp

Especifique el Dispositivo A como el servidor NTP del Dispositivo B para que el Dispositivo B se sincronice con el Dispositivo A.

[DispositivoB] servidor de unidifusión de servicio ntp 1.0.1.11

4. Verifique la configuración:

Verifique que el dispositivo B se haya sincronizado con el dispositivo A y que el nivel del estrato de reloj sea 3 en el dispositivo B y 2 en el dispositivo A.

[DispositivoB] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 1.0.1.11

Modo local: cliente

ID del reloj de referencia: 1.0.1.11

Indicador de salto: 00

Fluctuación del reloj: 0,000977 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00383 ms Dispersión de raíz: 16,26572 ms Tiempo de referencia: d0c6033f.b9923965 Miércoles 29 de diciembre de 2010 18:58:07.724

Verifique que se haya establecido una asociación NTP IPv4 entre el dispositivo B y el dispositivo A.

[DispositivoB] muestra sesiones de servicio ntp

	fuente	referencia	la encuesta de alcance de Stra ahora compensa el retraso de dispersión
* * [12345]1.0.1.11	127.127.1.0	2	1 64 15 -4,0 0,0038 16,262

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

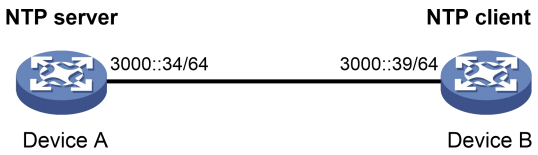
Ejemplo de configuración del modo cliente/servidor IPv6 NTP

Requisitos de red

Como se muestra enFigura 6, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo B para que funcione en modo cliente y el Dispositivo A para que se utilice como servidor NTP IPv6 para el Dispositivo B.

Figura 28 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 6. (No se muestran detalles).
2. Configurar el dispositivo A:

Habilite el servicio NTP.

<DispositivoA> vista del sistema

[DispositivoA] habilitación del servicio ntp

Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

[DispositivoA] ntp-service refclock-master 2

3. Configurar el dispositivo B:

Habilite el servicio NTP.

<DispositivoB> vista del sistema

[DispositivoB] habilitación del servicio ntp

Especifique el Dispositivo A como el servidor NTP IPv6 del Dispositivo B para que el Dispositivo B se sincronice con el Dispositivo A.

[DispositivoB] servicio ntp ipv6 servidor unicast 3000::34

4. Verifique la configuración:

Verifique que el dispositivo B se haya sincronizado con el dispositivo A y que el nivel del estrato de reloj sea 3 en el dispositivo B y 2 en el dispositivo A.

[DispositivoB] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 3000::34

Modo local: cliente

ID de reloj de referencia: 163.29.247.19

Indicador de salto: 00

Fluctuación del reloj: 0,000977 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,02649 ms Dispersión de raíz: 12,24641 ms Tiempo de referencia: d0c60419.9952fb3e Miércoles 29 de diciembre de 2010 19:01:45.598

Verifique que se haya establecido una asociación NTP IPv6 entre el dispositivo B y el dispositivo A.

[DispositivoB] muestra sesiones ipv6 de servicio ntp

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Fuente: [12345]3000::34

Referencia: 127.127.1.0 Estrato de reloj: 2

Accesibilidad: 15 Intervalo de encuesta: 64

Hora de la última recepción: 19 Compensación: 0,0

Retraso de ida y vuelta: 0,0 Dispersión: 0.0

Sesiones totales: 1

Ejemplo de configuración de modo activo/pasivo simétrico NTP

Requisitos de red

Como se muestra enFigura 7, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo A para que funcione en modo activo simétrico y especifique el Dispositivo B como par pasivo del Dispositivo A.

Figura 29 Diagrama de red

Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 7. (No se muestran detalles).
2. Configurar el dispositivo B:

   # Habilite el servicio NTP.

   <DispositivoB> vista del sistema

   [DispositivoB] habilitación del servicio ntp
3. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2

   # Configure el dispositivo B como un par pasivo simétrico.

   [DispositivoA] ntp-service unicast-peer 3.0.1.32
4. Verifique la configuración:

   # Verifique que el dispositivo B se haya sincronizado con el dispositivo A.

   [DispositivoB] muestra el estado del servicio ntp

   Reloj estado: sincronizado

   Reloj estrato: 3

   Sistema par: 3.0.1.3 1

   Local modo: sim_pasivo

   ID del reloj de referencia: 3.0.1.31

   Indicador de salto: 00

   Fluctuación del reloj: 0,000916 s

   Estabilidad: 0,000 pps

   Precisión del reloj: 2^-17

   Retardo de raíz: 0,00609 ms Dispersión de raíz: 1,95859 ms Tiempo de referencia: 83aec681.deb6d3e5 Casarse, Ene 8 2014 14:33:11.081

   # Verifique que se haya establecido una asociación NTP IPv4 entre el dispositivo B y el dispositivo A.

   [DispositivoB] muestra sesiones de servicio ntp

   fuente referencia la encuesta de alcance de Stra ahora compensa el retraso de dispersión

   ****

   [12]3.0.1.31 127.127.1.0 2 62 64 34 0,4251 6,0882 1392,1

   Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

   Sesiones totales: 1

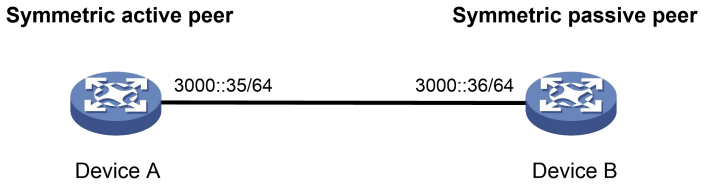
Ejemplo de configuración de modo activo/pasivo simétrico IPv6 NTP

Requisitos de red

Como se muestra enFigura 8, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo A para que funcione en modo activo simétrico y especifique el Dispositivo B como el par pasivo IPv6 del Dispositivo A.

Figura 30 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 8. (No se muestran detalles).
2. Configurar el dispositivo B:

   # Habilite el servicio NTP.

   <DispositivoB> vista del sistema

   [DispositivoB] habilitación del servicio ntp
3. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2

   # Configure el dispositivo B como un par pasivo simétrico IPv6.

   [DispositivoA] ntp-service ipv6 unicast-peer 3000::36
4. Verifique la configuración:

   # Verifique que el dispositivo B se haya sincronizado con el dispositivo A.

   [DispositivoB] muestra el estado del servicio ntp

   Reloj estado: sincronizado

   Reloj estrato: 3

   Sistema par: 3000::35

   Local modo: sim_ pasivo

   ID de reloj de referencia: 251.73.79.32

   Indicador de salto: 11

   Fluctuación del reloj: 0,000977 s

   Estabilidad: 0,000 pps

   Precisión del reloj: 2^-18

   Retardo de raíz: 0,01855 ms Dispersión de raíz: 9,23483 ms Tiempo de referencia: d0c6047c.97199f9f Miércoles 29 de diciembre de 2010 19:03:24.590

Verifique que se haya establecido una asociación NTP IPv6 entre el dispositivo B y el dispositivo A.

[DispositivoB] muestra sesiones ipv6 de servicio ntp

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Fuente: [1234]3000::35

Referencia: 127.127.1.0 Estrato de reloj: 2

Accesibilidad: 15 Intervalo de encuesta: 64

Hora de la última recepción: 19 Compensación: 0,0

Retraso de ida y vuelta: 0,0 Dispersión: 0.0

Sesiones totales: 1

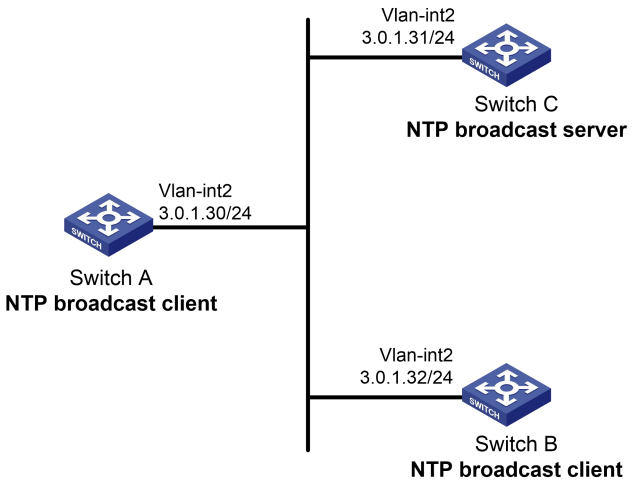
Ejemplo de configuración del modo de transmisión NTP

Requisitos de red

Como se muestra enFigura 9, Switch C funciona como servidor NTP para múltiples dispositivos en un segmento de red y sincroniza la hora entre múltiples dispositivos.

- Configure el reloj local del Switch C como fuente de referencia, con el nivel de estrato 2.
- Configure el Switch C para operar en modo de servidor de transmisión y enviar mensajes de transmisión desde la interfaz VLAN 2.
- Configure el Switch A y el Switch B para operar en modo de cliente de transmisión y escuche los mensajes de transmisión a través de la interfaz VLAN 2.

Figura 31 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el conmutador A, el conmutador B y el conmutador C puedan comunicarse entre sí, como se muestra enFigura 9. (No se muestran detalles).
2. Configurar el interruptor C:

   # Habilite el servicio NTP.

   <SwitchC> vista del sistema

   [SwitchC] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [SwitchC] servicio ntp refclock-master 2

Configure el Switch C para operar en modo de servidor de transmisión y enviar mensajes de transmisión a través de la interfaz VLAN 2.

[SwitchC] interfaz vlan-interface 2 [SwitchC-Vlan-interface2] servidor de

transmisión de servicio ntp

3. Configurar el interruptor A:

Habilite el servicio NTP.

<SwitchA> vista del sistema

[SwitchA] habilitación del servicio ntp

Configure el conmutador A para que funcione en modo de cliente de transmisión y reciba mensajes de transmisión en la interfaz VLAN 2.

[SwitchA] interfaz vlan-interface 2 [SwitchA-Vlan-interface2] cliente de

transmisión de servicio ntp

4. Configurar el interruptor B:

Habilite el servicio NTP.

<SwitchB> vista del sistema

[SwitchB] habilitación del servicio ntp

Configure el Switch B para operar en modo de cliente de transmisión y recibir mensajes de transmisión en la interfaz VLAN 2.

[SwitchB] interfaz vlan-interface 2 [SwitchB-Vlan-interface2] cliente de

transmisión de servicio ntp

5. Verifique la configuración:

Verifique que el Switch A se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch A y 2 en el Switch C.

[SwitchA-Vlan-interface2] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 3.0.1.31

Modo local: bcliente

ID del reloj de referencia: 3.0.1.31

Indicador de salto: 00

Fluctuación del reloj: 0,044281 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00229 ms Dispersión de

raíz: 4,12572 ms Tiempo de referencia:

d0d289fe.ec43c720 Se sentó, Ene 8 2011 7:00:14.922

Verifique que se haya establecido una asociación NTP IPv4 entre el Switch A y el Switch C.

[SwitchA-Vlan-interface2] muestra sesiones de servicio ntp

fuente referencia encuesta de alcance de Stra ahora compensado retraso disper

****

* * [1245]3.0.1.31 127.127.1.0 2 1 64 519 - 0,0 0,0022 4,1257

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

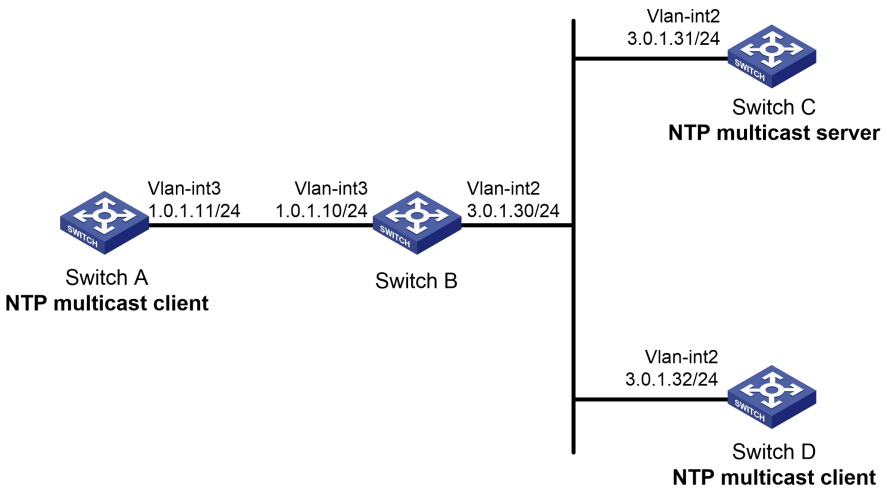
Ejemplo de configuración del modo multidifusión NTP

Requisitos de red

Como se muestra enFigura 10, Switch C funciona como servidor NTP para múltiples dispositivos en diferentes segmentos de red y sincroniza la hora entre múltiples dispositivos.

- Configure el reloj local del Switch C como fuente de referencia, con el nivel de estrato 2.
- Configure el Switch C para operar en modo de servidor de multidifusión y enviar mensajes de multidifusión desde la interfaz VLAN 2.
- Configure el Switch A y el Switch D para operar en modo de cliente de multidifusión y recibir mensajes de multidifusión a través de la interfaz VLAN 3 y la interfaz VLAN 2, respectivamente.

Figura 32 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que los conmutadores puedan comunicarse entre sí, como se muestra enFigura 10. (No se muestran detalles).
2. Configurar el interruptor C:

   # Habilite el servicio NTP.

   <SwitchC> vista del sistema

   [SwitchC] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [SwitchC] servicio ntp refclock-master 2

   # Configure el Switch C para operar en modo de servidor de multidifusión y enviar mensajes de multidifusión a través de la interfaz VLAN 2.

   [SwitchC] interfaz vlan-interface 2 [SwitchC-Vlan-interface2] servicio ntp

   servidor de multidifusión
3. Configurar el interruptor D:

   # Habilite el servicio NTP.

   <SwitchD> vista del sistema

   [SwitchD] habilitación del servicio ntp

   # Configure el Switch D para operar en modo de cliente de multidifusión y recibir mensajes de multidifusión en la interfaz VLAN 2.

   [SwitchD] interfaz vlan-interface 2 [SwitchD-Vlan-interface2] servicio ntp

   cliente de multidifusión

4. Verifique la configuración:

El Switch D y el Switch C están en la misma subred, por lo que el Switch D puede hacer lo siguiente:

- Reciba los mensajes multicast del Switch C sin estar habilitado con las funciones multicast.
- Sincronizar con el interruptor C.

Verifique que el Switch D se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch D y 2 en el Switch C.

[SwitchD-Vlan-interface2] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 3.0.1.31

Modo local: bcliente

ID del reloj de referencia: 3.0.1.31

Indicador de salto: 00

Fluctuación del reloj: 0,044281 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00229 ms Dispersión de

raíz: 4,12572 ms Tiempo de referencia:

d0d289fe.ec43c720 Se sentó, Ene 8 2011 7:00:14.922

Verifique que se haya establecido una asociación NTP IPv4 entre el Switch D y el Switch C.

[SwitchD-Vlan-interface2] muestra sesiones de servicio ntp

	fuente	referencia	encuesta de alcance de Stra	ahora compensado retraso disper
**********				
* * [1245]3.0.1.31	127.127.1.0	2	1 64 519 - 0,0 0,0022 4,1257	

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

5. Configurar el interruptor B:

Debido a que el Switch A y el Switch C están en subredes diferentes, debe habilitar las funciones de multidifusión en el Switch B antes de que el Switch A pueda recibir mensajes de multidifusión desde el Switch C.

Habilite el enrutamiento de multidifusión IP e IGMP.

<SwitchB> vista del sistema

[SwitchB] enrutamiento de

multidifusión [SwitchB-mrib] salir

[SwitchB] interfaz vlan-interface 2 [SwitchB-Vlan-

interface2] pim dm [SwitchB-Vlan-interface2] quit

[SwitchB] vlan 3

[SwitchB-vlan3] puerto gigabitethernet 2/0/1 [SwitchB-

vlan3] salir

[SwitchB] interfaz vlan-interface 3 [SwitchB-Vlan-interface3] igmp enable

[SwitchB-Vlan-interface3] igmp static-group 224.0.1.1 [SwitchB-Vlan-

interface3] salir

[SwitchB] igmp-snooping [SwitchB-igmp-snooping] salir [SwitchB] interfaz gigabitethernet 2/0/1

[SwitchB-GigabitEthernet2/0/1] igmp-snooping static-group 224.0.1.1 vlan 3

6. Configurar el interruptor A:

   # Habilite el servicio NTP.

   <SwitchA> vista del sistema

   [SwitchA] habilitación del servicio ntp

   # Configure el conmutador A para que funcione en modo de cliente de multidifusión y reciba mensajes de multidifusión en la interfaz VLAN 3.

   [SwitchA] interfaz vlan-interface 3 [SwitchA-Vlan-interface3] cliente-

   multidifusión de servicio ntp

7. Verifique la configuración:

   # Verifique que el Switch A se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch A y 2 en el Switch C.

   [SwitchA-Vlan-interface3] muestra el estado del servicio ntp

   Reloj estado: sincronizado

   Reloj estrato: 3

   Par del sistema: 3.0.1.31

   Modo local: bcliente

   ID del reloj de referencia: 3.0.1.31

   Indicador de salto: 00

   Fluctuación del reloj: 0,165741 s

   Estabilidad: 0,000 pps

   Precisión del reloj: 2^-18

   Retardo de raíz: 0,00534 ms Dispersión de

   raíz: 4,51282 ms Tiempo de referencia:

   d0c61289.10b1193f Miércoles 29 de diciembre de 2010 20:03:21.065

   # Verifique que se haya establecido una asociación NTP IPv4 entre el Switch A y el Switch C.

   [SwitchA-Vlan-interface3] muestra sesiones de servicio ntp

   fuente referencia encuesta de alcance de Stra ahora compensado retraso disper

   ****

   * * [1234]3.0.1.31 127.127.1.0 2 247 64 381 - 0,0 0,0053 4,5128

   Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

   Sesiones totales: 1

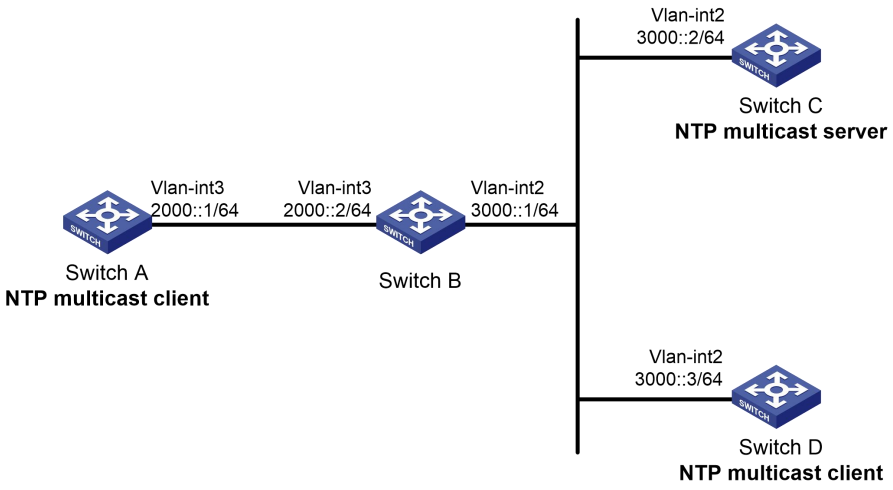
Ejemplo de configuración del modo multidifusión IPv6 NTP

Requisitos de red

Como se muestra enFigura 11, Switch C funciona como servidor NTP para múltiples dispositivos en diferentes segmentos de red y sincroniza la hora entre múltiples dispositivos.

- Configure el reloj local del Switch C como fuente de referencia, con el nivel de estrato 2.
- Configure el Switch C para operar en modo de servidor de multidifusión IPv6 y enviar mensajes de multidifusión IPv6 desde la interfaz VLAN 2.
- Configure el Switch A y el Switch D para operar en modo de cliente de multidifusión IPv6 y recibir mensajes de multidifusión IPv6 a través de la interfaz VLAN 3 y la interfaz VLAN 2, respectivamente.

Figura 33 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que los conmutadores puedan comunicarse entre sí, como se muestra enFigura 11. (No se muestran detalles).
2. Configurar el interruptor C:

   # Habilite el servicio NTP.

   <SwitchC> vista del sistema

   [SwitchC] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [SwitchC] servicio ntp refclock-master 2

   # Configure el Switch C para operar en modo de servidor de multidifusión IPv6 y enviar mensajes de multidifusión a través de la interfaz VLAN 2.

   [SwitchC] interfaz vlan-interfaz 2

   [SwitchC-Vlan-interface2] servidor de multidifusión ipv6 de servicio ntp ff24::1
3. Configurar el interruptor D:

   # Habilite el servicio NTP.

   <SwitchD> vista del sistema

   [SwitchD] habilitación del servicio ntp

   # Configure el Switch D para operar en modo de cliente de multidifusión IPv6 y recibir mensajes de multidifusión en la interfaz VLAN 2.

   [SwitchD] interfaz vlan-interfaz 2

   [SwitchD-Vlan-interface2] servicio ntp ipv6 cliente de multidifusión ff24::1
4. Verifique la configuración:

   El Switch D y el Switch C están en la misma subred, por lo que el Switch D puede hacer lo siguiente:

   - Reciba los mensajes de multidifusión IPv6 desde el Switch C sin estar habilitado con las funciones de multidifusión IPv6.
   - Sincronizar con el interruptor C.

   # Verifique que el Switch D se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch D y 2 en el Switch C.

   [SwitchD-Vlan-interface2] muestra el estado del servicio ntp

   ```
   Reloj estado: sincronizado
   Reloj estrato: 3
   Par del sistema: 3000::2
   ```

Modo local: bcliente
ID de reloj de referencia: 165.84.121.65
Indicador de salto: 00
Fluctuación del reloj: 0,000977 s
Estabilidad: 0,000 pps
Precisión del reloj: 2^-18
Retardo de raíz: 0,00000 ms Dispersión de
raíz: 8,00578 ms Tiempo de referencia:
d0c60680.9754fb17 Miércoles 29 de diciembre de 2010 19:12:00.591

Verifique que se haya establecido una asociación NTP IPv6 entre el Switch D y el Switch C.

[SwitchD-Vlan-interface2] muestra sesiones ipv6 de servicio ntp
Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Fuente: [1234]3000::2
Referencia: 127.127.1.0 Estrato de reloj: 2
Accesibilidad: 111 Intervalo de encuesta: 64
Hora de la última recepción: 23 Compensación: -0,0
Retraso de ida y vuelta: 0,0 Dispersión: 0,0

Sesiones totales: 1

5. Configurar el interruptor B:

Debido a que el Switch A y el Switch C están en subredes diferentes, debe habilitar las funciones de multidifusión IPv6 en el Switch B antes de que el Switch A pueda recibir mensajes de multidifusión IPv6 desde el Switch C.

Habilite las funciones de multidifusión IPv6.

<SwitchB> vista del sistema
[SwitchB] enrutamiento de multidifusión
ipv6 [SwitchB-mrib6] salir
[SwitchB] interfaz vlan-interface 2 [SwitchB-Vlan-
interface2] ipv6 pim dm [SwitchB-Vlan-interface2]
salir [SwitchB] vlan 3

[SwitchB-vlan3] puerto gigabitethernet 2/0/1 [SwitchB-
vlan3] salir
[SwitchB] interfaz vlan-interface 3 [SwitchB-Vlan-interface3] mld
enable [SwitchB-Vlan-interface3] mld static-group ff24::1 [SwitchB-
Vlan-interface3] quit

[SwitchB] espionaje
[SwitchB-mld-espionaje] abandonar
[SwitchB] interfaz gigabitethernet 2/0/1 [SwitchB-GigabitEthernet2/0/1] mld-snooping static-
group ff24::1 vlan 3

6. Configurar el interruptor A:

Habilite el servicio NTP.

<SwitchA> vista del sistema
[SwitchA] habilitación del servicio ntp

Configure el conmutador A para que funcione en modo de cliente de multidifusión IPv6 y reciba mensajes de multidifusión IPv6 en la interfaz VLAN 3.

[SwitchA] interfaz vlan-interfaz 3

[SwitchA-Vlan-interface3] servicio ntp ipv6 cliente de multidifusión ff24::1

7. Verifique la configuración:

Verifique que el Switch A se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch A y 2 en el Switch C.

[SwitchA-Vlan-interface3] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 3000::2

Modo local: bcliente

ID de reloj de referencia: 165.84.121.65

Indicador de salto: 00

Fluctuación del reloj: 0,165741 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00534 ms Dispersión de

raíz: 4,51282 ms Tiempo de referencia:

d0c61289.10b1193f Miércoles 29 de diciembre de 2010 20:03:21.065

Verifique que se haya establecido una asociación NTP IPv6 entre el Switch A y el Switch C.

[SwitchA-Vlan-interface3] muestra sesiones ipv6 de servicio ntp

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Fuente: [124]3000::2

Referencia: 127.127.1.0 Estrato de reloj: 2

Accesibilidad: 2 Intervalo de encuesta: 64

Hora de la última recepción: 71 Compensación: -0,0

Retraso de ida y vuelta: 0,0 Dispersión: 0,0

Sesiones totales: 1

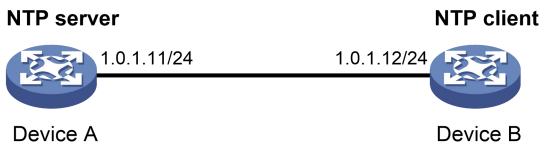
Ejemplo de configuración para modo cliente/servidor NTP con autenticación

Requisitos de red

Como se muestra enFigura 12, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo B para que funcione en modo cliente y especifique el Dispositivo A como el servidor NTP del Dispositivo B.
- Configure la autenticación NTP tanto en el Dispositivo A como en el Dispositivo B.

Figura 34 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 12. (No se muestran detalles).
2. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2
3. Configurar el dispositivo B:

   # Habilite el servicio NTP.

   <DispositivoB> vista del sistema

   [DispositivoB] habilitación del servicio ntp

   # Habilite la autenticación NTP en el dispositivo B.

   [DispositivoB] habilitación de autenticación de servicio ntp

   # Establezca una clave de autenticación e ingrese la clave en texto sin formato.

   [DispositivoB] ID de clave de autenticación de servicio ntp 42 modo de autenticación md5 simple aNiceKey

   # Especifique la clave como clave confiable.

   [DispositivoB] ntp-service autenticación confiable-keyid 42

   # Especifique el Dispositivo A como el servidor NTP del Dispositivo B y asocie el servidor con la clave 42.

   [DispositivoB] ntp-service unicast-server 1.0.1.11 autenticación-keyid 42

   Antes de que el Dispositivo B pueda sincronizar su reloj con el del Dispositivo A, habilite la autenticación NTP para el Dispositivo A.
4. Configure la autenticación NTP en el dispositivo A:

   # Habilite la autenticación NTP.

   [DispositivoA] habilitación de autenticación de servicio ntp

   # Establezca una clave de autenticación e ingrese la clave en texto sin formato.

   [DispositivoA] ID de clave de autenticación de servicio ntp 42 modo de autenticación md5 simple aNiceKey

   # Especifique la clave como clave confiable.

   [DispositivoA] ntp-service-keyid de autenticación confiable 42
5. Verifique la configuración:

   # Verifique que el dispositivo B se haya sincronizado con el dispositivo A y que el nivel del estrato de reloj sea 3 en el dispositivo B y 2 en el dispositivo A.

   [DispositivoB] muestra el estado del servicio ntp

   ```
   Reloj estado: sincronizado
   Reloj estrato: 3
   Par del sistema: 1.0.1.11
   Modo local: cliente
   ID del reloj de referencia: 1.0.1.11
   Indicador de salto: 00
   Fluctuación del reloj: 0,005096 s
   Estabilidad: 0,000 pps
   Precisión del reloj: 2^-18
   Retardo de raíz: 0,00655 ms
   Dispersión de raíz: 1,15869 ms
   ```

Hora de referencia: d0c62687.ab1bba7d miércoles 29 de diciembre de 2010 21:28:39.668

Verifique que se haya establecido una asociación NTP IPv4 entre el dispositivo B y el dispositivo A.

[DispositivoB] muestra sesiones de servicio ntp

	fuente	referencia	la encuesta de alcance de Stra ahora compensa el retraso de dispersión
* * [1245]1.0.1.11	127.127.1.0	2	1 64 519 - 0,0 0,0065 0,0

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

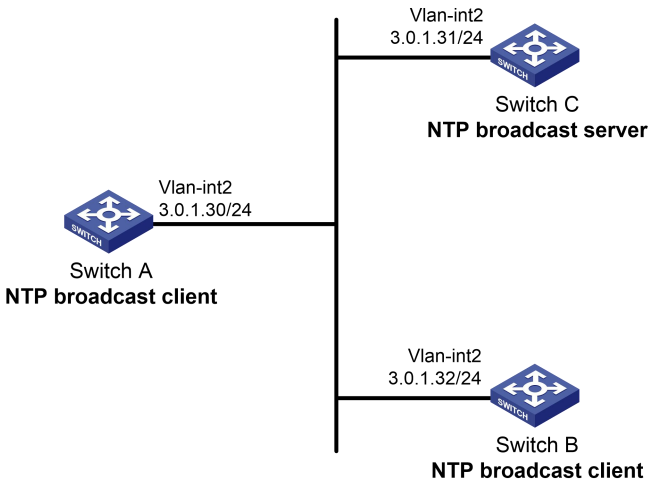
Ejemplo de configuración para modo de transmisión NTP con autenticación

Requisitos de red

Como se muestra enFigura 13, Switch C funciona como servidor NTP para múltiples dispositivos en diferentes segmentos de red y sincroniza la hora entre múltiples dispositivos. El conmutador A y el conmutador B autentican la fuente de referencia.

- Configure el reloj local del Switch C como fuente de referencia, con el nivel de estrato 3.
- Configure el Switch C para operar en modo de servidor de transmisión y enviar mensajes de transmisión desde la interfaz VLAN 2.
- Configure el Switch A y el Switch B para operar en modo de cliente de transmisión y recibir mensajes de transmisión a través de la interfaz VLAN 2.
- Habilite la autenticación NTP en el Switch A, el Switch B y el Switch C.

Figura 35 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el conmutador A, el conmutador B y el conmutador C puedan comunicarse entre sí, como se muestra enFigura 13. (No se muestran detalles).
2. Configurar el interruptor A:

   # Habilite el servicio NTP.

   <SwitchA> vista del sistema

   [SwitchA] habilitación del servicio ntp

   # Habilite la autenticación NTP en el conmutador A. Configure una clave de autenticación NTP, con el ID de clave 88 y el valor de clave 123456. Ingrese la clave en texto sin formato y especifíquela como clave confiable.

[SwitchA] Habilitación de autenticación de servicio ntp

[SwitchA] ntp-service autenticación-keyid 88 modo de autenticación md5 simple 123456 [SwitchA] ntp-service autenticación-keyid confiable 88

Configure el conmutador A para que funcione en modo de cliente de transmisión NTP y reciba mensajes de transmisión NTP en la interfaz VLAN 2.

[SwitchA] interfaz vlan-interface 2 [SwitchA-Vlan-interface2] cliente de

transmisión de servicio ntp

3. Configurar el interruptor B:

Habilite el servicio NTP.

<SwitchB> vista del sistema

[SwitchB] habilitación del servicio ntp

Habilite la autenticación NTP en el Switch B. Configure una clave de autenticación NTP, con el ID de clave 88 y el valor de clave 123456. Ingrese la clave en texto sin formato y especifíquela como clave confiable.

[SwitchB] Habilitación de autenticación de servicio ntp

[SwitchB] ntp-service autenticación-keyid 88 modo de autenticación md5 simple 123456 [SwitchB] ntp-service autenticación-keyid confiable 88

Configure el Switch B para operar en modo de cliente de transmisión y recibir mensajes de transmisión NTP en la interfaz VLAN 2.

[SwitchB] interfaz vlan-interface 2 [SwitchB-Vlan-interface2] cliente de

transmisión de servicio ntp

4. Configurar el interruptor C:

Habilite el servicio NTP.

<SwitchC> vista del sistema

[SwitchC] habilitación del servicio ntp

Especifique el reloj local como fuente de referencia, con el nivel de estrato 3.

[SwitchC] servicio ntp refclock-master 3

Configure el conmutador C para que funcione en modo de servidor de transmisión NTP y use la interfaz VLAN 2 para enviar paquetes de transmisión NTP.

[SwitchC] interfaz vlan-interface 2 [SwitchC-Vlan-interface2] servidor de

transmisión de servicio ntp [SwitchC-Vlan-interface2] salir

5. Verifique la configuración:

La autenticación NTP está habilitada en el Switch A y el Switch B, pero no en el Switch C, por lo que el Switch A y el Switch B no pueden sincronizar sus relojes locales con el Switch C.

Verifique que el Switch B no se haya sincronizado con el Switch C.

[SwitchB-Vlan-interface2] muestra el estado del servicio ntp

Reloj estado: no sincronizado

Reloj estrato: dieciséis

ID del reloj de referencia: ninguno

6. Habilite la autenticación NTP en el Switch C:

Habilite la autenticación NTP en el Switch C. Configure una clave de autenticación NTP, con el ID de clave 88 y el valor de clave 123456. Ingrese la clave en texto sin formato y especifíquela como clave confiable.

[SwitchC] habilitar la autenticación del servicio ntp

[SwitchC] ntp-service autenticación-keyid 88 modo de autenticación md5 simple 123456 [SwitchC] ntp-service autenticación-keyid confiable 88

Especifique el conmutador C como servidor de transmisión NTP y asocie la clave 88 con el conmutador C.

[SwitchC] interfaz vlan-interfaz 2

[SwitchC-Vlan-interface2] ID de clave de autenticación del servidor de transmisión de servicio ntp 88

7. Verifique la configuración:

Verifique que el Switch B se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 4 en el Switch B y 3 en el Switch C.

[SwitchB-Vlan-interface2] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 4

Par del sistema: 3.0.1.31

Modo local: bcliente

ID del reloj de referencia: 3.0.1.31

Indicador de salto: 00

Fluctuación del reloj: 0,006683 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00127 ms Dispersión de

raíz: 2,89877 ms Tiempo de referencia:

d0d287a7.3119666f Se sentó, Ene 8 2011 6:50:15.191

Verifique que se haya establecido una asociación NTP IPv4 entre el Switch B y el Switch C.

[SwitchB-Vlan-interface2] muestra sesiones de servicio ntp

	fuente	referencia	encuesta de alcance de Stra	ahora compensado retraso disper
**********				
* *	[1245]3.0.1.31	127.127.1.0	3	3 64 68 -0,0 0,0000 0,0

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

Configurar SNTP

SNTP es una versión simplificada de NTP solo para cliente especificada en RFC 4330. SNTP solo admite el modo cliente/servidor. Un dispositivo habilitado para SNTP puede recibir hora de servidores NTP, pero no puede proporcionar servicios de hora a otros dispositivos.

SNTP utiliza el mismo formato de paquete y procedimiento de intercambio de paquetes que NTP, pero proporciona una sincronización más rápida a costa de la precisión del tiempo.

Si especifica varios servidores NTP para un cliente SNTP, se selecciona el servidor con el mejor estrato. Si hay varios servidores en el mismo estrato, se selecciona el servidor NTP cuyo paquete de tiempo se recibe por primera vez.

Restricciones y pautas de configuración

Cuando configure SNTP, siga estas restricciones y pautas:

- No puede configurar NTP y SNTP en el mismo dispositivo.
- Asegúrate de utilizar el**protocolo de reloj**comando para especificar el protocolo de tiempo como NTP.

Lista de tareas de configuración

Tareas de un vistazo
(Requerido.)Habilitar el servicio SNTP
(Requerido.)Especificación de un servidor NTP para el dispositivo
(Opcional.)Configurar la autenticación SNTP

Habilitar el servicio SNTP

El servicio NTP y el servicio SNTP son mutuamente excluyentes. Sólo puede habilitar el servicio NTP o el servicio SNTP a la vez.

Para habilitar el servicio SNTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite el servicio SNTP.	**habilitar sntp**	De forma predeterminada, el servicio SNTP no está habilitado.

Especificación de un servidor NTP para el dispositivo

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A

Paso	Dominio	Observaciones
2. Especifique un servidor NTP para el dispositivo.	- Para IPv4: **servidor de unidifusión sntp** {*nombre del servidor*|*dirección IP*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*| **fuente***Tipo de interfaz número de interfaz*|**versión** *número*] * - Para IPv6: **Servidor de unidifusión sntp ipv6** {*nombre del servidor*|*dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*| **fuente***Tipo de interfaz número de interfaz*] *	De forma predeterminada, no se especifica ningún servidor NTP para el dispositivo. Repita este paso para especificar varios servidores NTP. Para utilizar la autenticación, debe especificar el**ID de clave de autenticación** *ID de clave*opción.

Para utilizar un servidor NTP como fuente de hora, asegúrese de que su reloj esté sincronizado. Si el nivel de estrato del servidor NTP es mayor o igual que el del cliente, el cliente no se sincroniza con el servidor NTP.

Configurar la autenticación SNTP

La autenticación SNTP garantiza que un cliente SNTP esté sincronizado únicamente con un servidor NTP confiable y autenticado.

Siga estas pautas cuando configure la autenticación SNTP:

- Habilite la autenticación tanto en el servidor NTP como en el cliente SNTP.
- Configure el cliente SNTP con el mismo ID de clave de autenticación y valor de clave que el servidor NTP, y especifique la clave como clave confiable tanto en el servidor NTP como en el cliente SNTP. Para obtener información sobre cómo configurar la autenticación NTP en un servidor NTP, consulte "Configurando NTP".
- Asocie la clave especificada con un servidor NTP en el cliente SNTP.

Con la autenticación deshabilitada, el cliente SNTP puede sincronizarse con el servidor NTP independientemente de si el servidor NTP está habilitado con autenticación.

Para configurar la autenticación SNTP en el cliente SNTP:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Habilite la autenticación SNTP.	**habilitar la autenticación SNTP**	De forma predeterminada, la autenticación SNTP está deshabilitada.
3. Configurar un SNTP clave de autenticación.	**ID de clave de autenticación SNTP***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación SNTP.
4. Especifique la clave como clave confiable.	**SNTP confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, no se especifica ninguna clave confiable.

Paso	Dominio	Observaciones
5. Asociar el SNTP clave de autenticación con un servidor NTP.	- Para IPv4: **servidor de unidifusión sntp** {*nombre del servidor*| *dirección IP* } [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave* - Para IPv6: **Servidor de unidifusión sntp ipv6** { *nombre del servidor*| *dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave*	De forma predeterminada, no se especifica ningún servidor NTP.

Visualización y mantenimiento de SNTP

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Muestra información sobre todas las asociaciones SNTP IPv6.	**mostrar sesiones sntp ipv6**
Muestra información sobre todas las asociaciones SNTP IPv4.	**mostrar sesiones sntp**

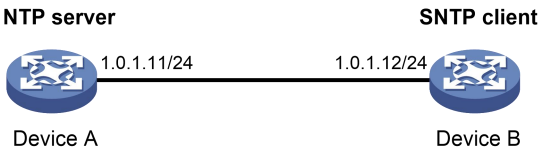
Ejemplo de configuración SNTP

Requisitos de red

Como se muestra enFigura 14, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2. Configure el Dispositivo
- B para que funcione en modo de cliente SNTP y especifique el Dispositivo A como servidor NTP. Configure la
- autenticación NTP en el dispositivo A y la autenticación SNTP en el dispositivo B.

Figura 36 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 14. (No se muestran detalles).
2. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Configurar el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2

   # Habilite la autenticación NTP en el dispositivo A.

   [DispositivoA] habilitación de autenticación de servicio ntp

Configure una clave de autenticación NTP, con el ID de clave de**10**y valor clave de**una buena llave**. Ingrese la clave en texto plano.

[DispositivoA] ID de clave de autenticación de servicio ntp 10 modo de autenticación md5 simple aNiceKey

Especifique la clave como clave confiable.

[DispositivoA] ntp-service autenticación confiable-keyid 10

3. Configurar el dispositivo B:

Habilite el servicio SNTP.

<DispositivoB> vista del sistema

[DispositivoB] sntp habilitado

Habilite la autenticación SNTP en el dispositivo B.

[DispositivoB] habilitación de autenticación SNTP

Configure una clave de autenticación SNTP, con el ID de clave de**10**y valor clave de**una buena llave**. Ingrese la clave en texto plano.

[DispositivoB] ID de clave de autenticación sntp 10 modo de autenticación md5 simple aNiceKey

Especifique la clave como clave confiable.

[DispositivoB] sntp autenticación confiable-keyid 10

Especifique el Dispositivo A como el servidor NTP del Dispositivo B y asocie el servidor con la clave 10.

[DispositivoB] sntp unicast-server 1.0.1.11 ID de clave de autenticación 10

4. Verifique la configuración:

Verifique que se haya establecido una asociación SNTP entre el dispositivo B y el dispositivo A, y que el dispositivo B se haya sincronizado con el dispositivo A.

[DispositivoB] muestra sesiones sntp

servidor NTP	Estrato	Versión	Última hora de recepción
1.0.1.11	2	4	Martes, 17 de mayo de 2011 9:11:20.833 (sincronizado)

Contenido

Configuración de NTP ····· ····· 1

Configurando NTP

Sincronice su dispositivo con una fuente horaria confiable utilizando el Protocolo de hora de red (NTP) o cambiando la hora del sistema antes de ejecutarlo en una red activa. Varias tareas, incluida la gestión de red, la carga, la auditoría y la computación distribuida, dependen de una configuración precisa de la hora del sistema, porque las marcas de tiempo de los mensajes y registros del sistema utilizan la hora del sistema.

Descripción general

NTP se utiliza normalmente en redes grandes para sincronizar dinámicamente la hora entre dispositivos de red. Garantiza una mayor precisión del reloj que la configuración manual del reloj del sistema. En una red pequeña que no requiere una alta precisión del reloj, puede mantener la hora sincronizada entre dispositivos cambiando los relojes del sistema uno por uno.

NTP se ejecuta sobre UDP y utiliza el puerto UDP 123.

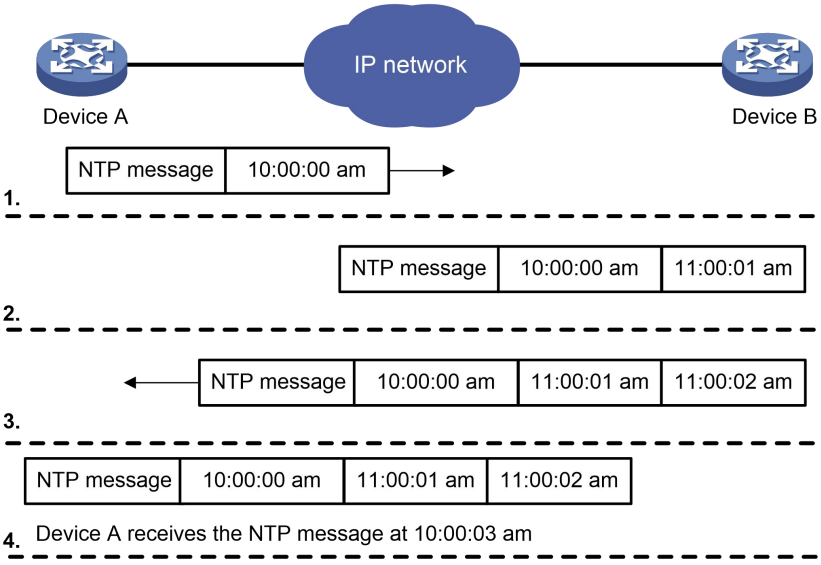
> **NOTA:**
> NTP solo se admite en las siguientes interfaces de Capa 3:
> - Interfaces Ethernet de capa 3.
> - Subinterfaces Ethernet de capa 3.
> - Interfaces agregadas de capa 3.
> - Subinterfaces agregadas de capa 3.
> - Interfaces VLAN e interfaces de túnel.

Cómo funciona NTP

Figura 1muestra cómo NTP sincroniza la hora del sistema entre dos dispositivos (Dispositivo A y Dispositivo B, en este ejemplo). Asumir que:

- Antes de la sincronización horaria, la hora del Dispositivo A y del Dispositivo B se establece en 10:00:00 am y 11:00:00 am, respectivamente.
- El dispositivo B se utiliza como servidor NTP. El dispositivo A debe sincronizarse con el dispositivo B.
- Un mensaje NTP tarda 1 segundo en viajar del dispositivo A al dispositivo B y del dispositivo B al dispositivo A.
- El dispositivo B tarda 1 segundo en procesar el mensaje NTP.

Figura 37 Flujo de trabajo básico



El proceso de sincronización es el siguiente:

1. El dispositivo A envía al dispositivo B un mensaje NTP, que tiene una marca de tiempo cuando sale del dispositivo A. La marca de tiempo es las 10:00:00 am (T1).
2. Cuando este mensaje NTP llega al Dispositivo B, el Dispositivo B agrega una marca de tiempo que muestra la hora en que el mensaje llegó al Dispositivo B. La marca de tiempo es las 11:00:01 am (T2).
3. Cuando el mensaje NTP sale del Dispositivo B, el Dispositivo B agrega una marca de tiempo que muestra la hora en que el mensaje salió del Dispositivo B. La marca de tiempo es las 11:00:02 am (T3).
4. Cuando el dispositivo A recibe el mensaje NTP, la hora local del dispositivo A es las 10:00:03 am (T4).

Hasta ahora, el Dispositivo A puede calcular los siguientes parámetros en función de las marcas de tiempo:

- El retraso de ida y vuelta del mensaje NTP: Retraso = (T4 – T1) – (T3 – T2) = 2 segundos. Diferencia horaria
- entre el Dispositivo A y el Dispositivo B: Compensación = ((T2 – T1) + (T3 – T4)) /2 = 1 hora.

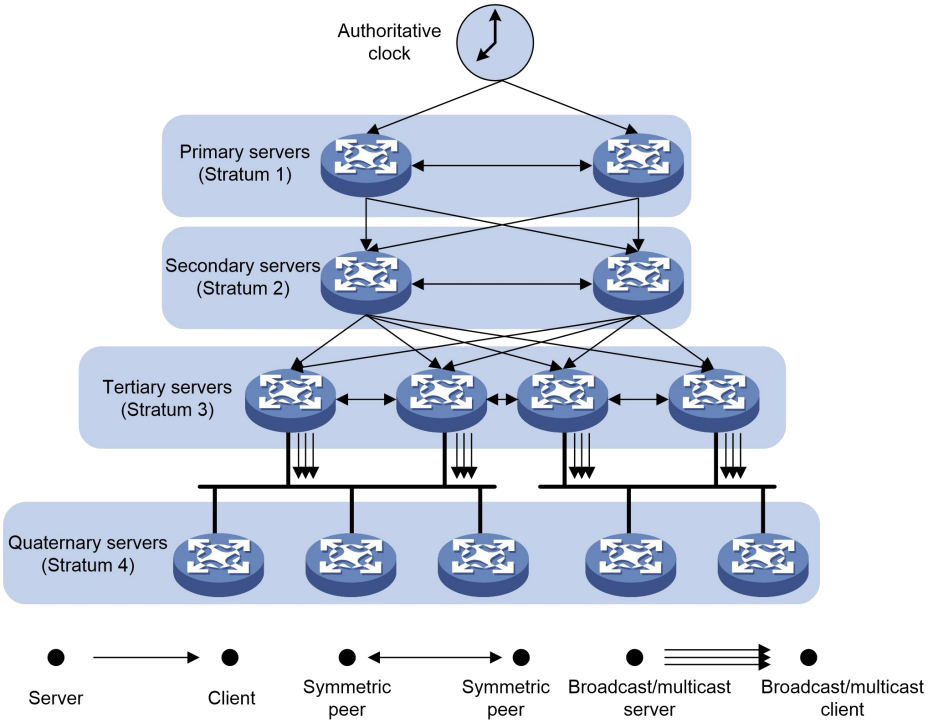
Según estos parámetros, el dispositivo A se puede sincronizar con el dispositivo B.

Esta es sólo una descripción aproximada del mecanismo de trabajo de NTP. Para obtener más información, consulte los protocolos y estándares relacionados.

arquitectura NTP

NTP utiliza los estratos 1 a 16 para definir la precisión del reloj, como se muestra enFigura 2. Un valor de estrato más bajo representa una mayor precisión. Los relojes de los estratos 1 al 15 están en estado sincronizado y los relojes del estrato 16 no están sincronizados.

Figura 38 Arquitectura NTP



Un servidor NTP de estrato 1 obtiene su hora de una fuente de hora autorizada, como un reloj atómico. Proporciona tiempo para otros dispositivos como servidor NTP principal. Un servidor de tiempo de estrato 2 recibe su tiempo de un servidor de tiempo de estrato 1, y así sucesivamente.

Para garantizar la precisión y la disponibilidad de la hora, puede especificar varios servidores NTP para un dispositivo. El dispositivo selecciona un servidor NTP óptimo como fuente de reloj en función de parámetros como el estrato. El reloj que selecciona el dispositivo se llama fuente de referencia. Para obtener más información sobre la selección de reloj, consulte los protocolos y estándares relacionados.

Si los dispositivos de una red no pueden sincronizarse con una fuente horaria autorizada, puede realizar las siguientes tareas:

- Seleccione un dispositivo que tenga un reloj relativamente preciso de la red.
- Utilice el reloj local del dispositivo como reloj de referencia para sincronizar otros dispositivos en la red.

Modos de asociación

NTP admite los siguientes modos de asociación:

- Modo cliente/servidor
- Modo activo/pasivo simétrico Modo
- de transmisión
- Modo de multidifusión

Tabla 8 modos de asociación NTP

Modo	Proceso de trabajo	Principio	Escenario de aplicación
Servidor de cliente	En el cliente, especifique la dirección IP del servidor NTP. Un cliente envía un mensaje de sincronización de reloj a los servidores NTP. Al recibir el mensaje, los servidores operar automáticamente en modo servidor y enviar una respuesta. Si el cliente se puede sincronizar con varios servidores de hora, selecciona un reloj óptimo y sincroniza su reloj local con la fuente de referencia óptima después de recibir las respuestas de los servidores.	Un cliente puede sincronizarse con un servidor, pero un servidor no puede sincronizarse con un cliente.	ComoFigura 2muestra, este modo está diseñado para configuraciones donde dispositivos de un estrato superior se sincronizan con dispositivos con un estrato inferior.
Simétrico activo pasivo	En el par activo simétrico, especifique la dirección IP del par pasivo simétrico. Un par activo simétrico envía periódicamente mensajes de sincronización de reloj a un par pasivo simétrico. El par pasivo simétrico Opera automáticamente en modo pasivo simétrico y envía una respuesta. Si el par activo simétrico se puede sincronizar con varios servidores de hora, selecciona un reloj óptimo y sincroniza su reloj local con la fuente de referencia óptima después de recibir las respuestas de los servidores.	Un par activo simétrico y un par simétrico El par pasivo se puede sincronizar con cada uno. otro. Si ambos están sincronizados, el par con un estrato superior está sincronizado con el pares de estrato inferior.	ComoFigura 2Como muestra, este modo se usa con mayor frecuencia entre servidores con el mismo estrato para operar como respaldo para uno. otro. Si un servidor no puede comunicarse con todos los servidores de un estrato inferior, el servidor aún puede sincronizar con los servidores del mismo estrato.
Transmisión	Un servidor envía periódicamente mensajes de sincronización de reloj a la dirección de transmisión. 255.255.255.255. Los clientes escuchan los mensajes de difusión de los servidores para sincronizarlos con el servidor de acuerdo con la mensajes de difusión. Cuando un cliente recibe el primer mensaje de difusión, el cliente y el servidor comienzan a intercambiar mensajes para calcular el retraso de la red entre ellos. Entonces, sólo el servidor de transmisión envía mensajes de sincronización de reloj.	Un cliente de transmisión puede sincronizarse con un servidor de difusión, pero un servidor de difusión no puede sincronizarse con un cliente de transmisión.	Un servidor de transmisión envía sincronización de reloj mensajes para sincronizar clientes en el mismo subred. ComoFigura 2 programas, el modo de transmisión está diseñado para configuraciones que involucran uno o varios servidores y una población de clientes potencialmente grande. El modo de transmisión tiene una precisión de tiempo menor que el cliente/servidor y los modos activo/pasivo simétrico porque solo los servidores de transmisión envían sincronización de reloj mensajes.

Modo	Proceso de trabajo	Principio	Escenario de aplicación
Multidifusión	Un servidor de multidifusión envía periódicamente mensajes de sincronización de reloj a la dirección de multidifusión configurada por el usuario. Los clientes escuchan los mensajes de multidifusión de los servidores y se sincronizan con el servidor de acuerdo con los mensajes recibidos.	Un cliente de multidifusión puede sincronizarse con un servidor de multidifusión, pero un servidor de multidifusión no puede sincronizarse con un cliente de multidifusión.	Un servidor de multidifusión puede proporcionar tiempo sincronización para clientes en la misma subred o en diferentes subredes. El modo multicast tiene una precisión de tiempo menor que el modo cliente/servidor y modos simétricos activo/pasivo.

En este documento, un "servidor NTP" o un "servidor" se refiere a un dispositivo que funciona como servidor NTP en modo cliente/servidor. Los servidores de hora se refieren a todos los dispositivos que pueden proporcionar sincronización horaria, incluidos servidores NTP, pares simétricos NTP, servidores de transmisión y servidores de multidifusión.

seguridad NTP

Para mejorar la seguridad de la sincronización horaria, NTP proporciona funciones de autenticación y control de acceso.

control de acceso NTP

Puede controlar el acceso a NTP mediante una ACL. Los derechos de acceso están en el siguiente orden, de menos restrictivos a más restrictivos:

- **Par**—Permite solicitudes de tiempo y consultas de control NTP (como alarmas, estado de autenticación e información del servidor de tiempo) y permite que el dispositivo local se sincronice con un dispositivo par.
- **Servidor**—Permite solicitudes de tiempo y consultas de control NTP, pero no permite que el dispositivo local se sincronice con un dispositivo par.
- **Sincronización**—Permite solo solicitudes de tiempo de un sistema cuya dirección pasa los criterios de la lista de acceso.
- **Consulta**—Permite solo consultas de control NTP desde un dispositivo par al dispositivo local.

El dispositivo procesa una solicitud NTP de la siguiente manera:

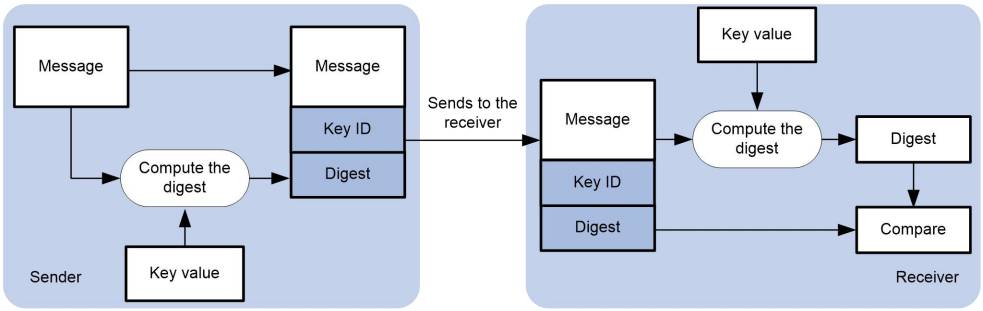
- Si no se configura ningún control de acceso NTP,**par**se otorga al dispositivo local y a los dispositivos pares.
- Si la dirección IP del dispositivo par coincide con una**permiso**declaración en una ACL para más de un derecho de acceso, el derecho de acceso menos restrictivo se otorga al dispositivo par. si un**denegar**declaración o no coincide ninguna ACL, no se concede ningún derecho de acceso.
- Si no se crea ninguna ACL para un derecho de acceso, no se otorga el derecho de acceso asociado. Si no se
- crea ninguna ACL para ningún derecho de acceso,**par**se concede.

Esta característica proporciona una seguridad mínima para un sistema que ejecuta NTP. Un método más seguro es la autenticación NTP.

autenticación NTP

Utilice esta función para autenticar los mensajes NTP por motivos de seguridad. Si un mensaje NTP pasa la autenticación, el dispositivo puede recibirlo y obtener información de sincronización horaria. En caso contrario, el dispositivo descarta el mensaje. Esta función garantiza que el dispositivo no se sincronice con un servidor de hora no autorizado.

Figura 39 Autenticación NTP



Como se muestra enfigura 3, la autenticación NTP funciona de la siguiente manera:

1. El remitente utiliza el algoritmo MD5 para calcular el mensaje NTP según la clave identificada por un ID de clave. Luego, envía el resumen calculado junto con el mensaje NTP y la ID de clave al receptor.
2. Al recibir el mensaje, el receptor realiza las siguientes acciones:

   a.Encuentra la clave según el ID de clave en el mensaje.

   b.Utiliza el algoritmo MD5 para calcular el resumen.

   C.Compara el resumen con el resumen contenido en el mensaje NTP. Si son iguales, el receptor acepta el mensaje. De lo contrario, descarta el mensaje.

NTP para MPLS L3VPN

En una red MPLS L3VPN, el dispositivo admite múltiples instancias de VPN cuando:

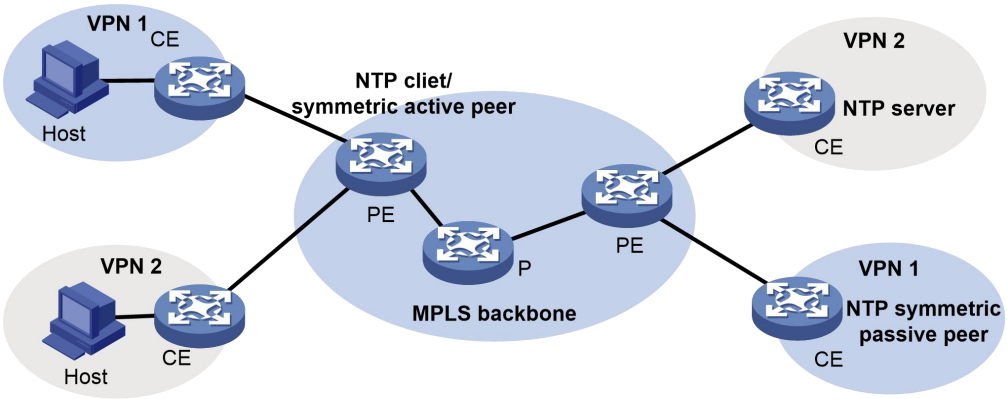
- Funciona como un cliente NTP para sincronizarse con el servidor NTP.
- Funciona como un par activo simétrico para sincronizarse con el par pasivo simétrico.

Solo los modos cliente/servidor y simétrico activo/pasivo admiten instancias de VPN.

Como se muestra enFigura 4, los usuarios de VPN 1 y VPN 2 están conectados a la red troncal MPLS a través de dispositivos de borde de proveedor (PE) y los servicios de las dos VPN están aislados. La sincronización horaria entre los PE y los dispositivos de las dos VPN se puede realizar si realiza las siguientes tareas:

- Configure los PE para que funcionen en cliente NTP o en modo activo simétrico.
- Especifique la VPN a la que pertenece el servidor NTP o el par pasivo simétrico NTP.

Figura 40 Diagrama de red



Protocolos y estándares

- RFC 1305,*Especificación, implementación y análisis del protocolo de tiempo de red (versión 3)* RFC
- 5905,*Protocolo de tiempo de red versión 4: especificación de protocolos y algoritmos*

Restricciones y pautas de configuración

Cuando configure NTP, siga estas restricciones y pautas:

- No puede configurar NTP y SNTP en el mismo dispositivo. No
- configure NTP en un puerto miembro agregado.
- El servicio NTP y el servicio SNTP son mutuamente excluyentes. Sólo puede habilitar el servicio NTP o el servicio SNTP a la vez.
- Para garantizar la precisión de la sincronización horaria, no especifique más de una fuente de referencia. Hacerlo podría provocar cambios de hora frecuentes o incluso fallos de sincronización.
- Asegúrate de utilizar el**protocolo de reloj**comando para especificar el protocolo de tiempo como NTP. Para más información sobre el**protocolo de reloj**comando, ver*Referencia de comandos fundamentales*.

Lista de tareas de configuración

Tareas de un vistazo
(Requerido.)Habilitando el servicio NTP
(Obligatorio.) Realice al menos una de las siguientes tareas: - Configurar el modo de asociación NTP Configurar el - reloj local como fuente de referencia
(Opcional.)Configurar derechos de control de acceso
(Opcional.)Configurar la autenticación NTP
(Opcional.)Configuración de parámetros opcionales de NTP

Habilitando el servicio NTP

Paso	**Dominio**	**Observaciones**
6. Ingrese a la vista del sistema.	**vista del sistema**	N / A
7. Habilite el servicio NTP.	**habilitación del servicio ntp**	De forma predeterminada, el servicio NTP no está habilitado.

Configurar el modo de asociación NTP

Esta sección describe cómo configurar los modos de asociación NTP.

Configurar NTP en modo cliente/servidor

Cuando el dispositivo funciona en modo cliente/servidor, especifique la dirección IP del servidor en el cliente. Siga estas pautas cuando configure un cliente NTP:

- Un servidor debe estar sincronizado mediante otros dispositivos o utilizar su reloj local como fuente de referencia antes de sincronizar un cliente NTP. De lo contrario, el cliente no se sincronizará con el servidor NTP.
- Si el nivel de estrato de un servidor es superior o igual al de un cliente, el cliente no se sincronizará con ese servidor.
- Puede configurar varios servidores repitiendo el proceso**servidor-unicast-servicio-ntp**y **servidor-unicast-ipv6-servicio-ntp**comandos.

Para configurar un cliente NTP:

Paso	Dominio	Observaciones
8. Ingrese a la vista del sistema.	**vista del sistema**	N / A
9. Especifique un servidor NTP para el dispositivo.	- Especifique un servidor NTP para el dispositivo: **servidor-unicast-servicio-ntp** { *nombre del servidor*| *dirección IP*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*| **prioridad**|**fuente** *Tipo de interfaz número de interfaz*|**versión** *número*] * - Especifique un servidor NTP IPv6 para el dispositivo: **servicio ntp ipv6** **servidor de unidifusión**{*nombre del servidor* | *dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*| **prioridad**|**fuente** *Tipo de interfaz número de interfaz*] *	De forma predeterminada, no se especifica ningún servidor NTP para el dispositivo.

Configuración de NTP en modo activo/pasivo simétrico

Cuando el dispositivo funciona en modo activo/pasivo simétrico, especifique en un par activo simétrico la dirección IP para un par pasivo simétrico.

Siga estas pautas cuando configure un par activo simétrico:

- Ejecute el**habilitación del servicio ntp**comando en un par pasivo simétrico para habilitar NTP. De lo contrario, el par simétrico-pasivo no procesará mensajes NTP de un par simétrico-activo.
- El par simétrico activo, el par simétrico pasivo o ambos deben estar en estado sincronizado. De lo contrario, su hora no se podrá sincronizar.
- Puede configurar varios pares pasivos simétricos repitiendo el procedimiento**par de unidifusión de servicio ntp**o**servicio-ntp ipv6 par-unicast**dominio.

Para configurar un par simétrico-activo:

Paso	Dominio	Observaciones
10. Ingrese a la vista del sistema.	**vista del sistema**	N / A

Paso	Dominio	Observaciones
11. Especifique un par pasivo simétrico para el dispositivo.	- Especifique un par simétrico-pasivo: **par de unidifusión de servicio ntp** {*nombre de compañero*|*dirección IP*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*|**prioridad**|**fuente** *Tipo de interfaz número de interfaz*|**versión** *número*] * - Especificar un IPv6 par simétrico-pasivo: **servicio ntp ipv6 par de unidifusión**{*nombre de compañero*| *dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*|**prioridad**|**fuente** *Tipo de interfaz número de interfaz*] *	De forma predeterminada, no se especifica ningún igual pasivo simétrico.

Configurar NTP en modo transmisión

Un servidor de transmisión debe sincronizarse mediante otros dispositivos o usar su reloj local como fuente de referencia antes de sincronizar un cliente de transmisión. De lo contrario, el cliente de transmisión no se sincronizará con el servidor de transmisión.

Configure NTP en modo de transmisión tanto en el servidor de transmisión como en el cliente.

Configurar un cliente de transmisión

Paso	Dominio	Observaciones
12. Ingrese a la vista del sistema.	**vista del sistema**	N / A
13. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	Ingrese a la interfaz para recibir mensajes de transmisión NTP.
14. Configure el dispositivo para que funcione en modo de cliente de transmisión.	**cliente de transmisión de servicio ntp**	De forma predeterminada, el dispositivo no funciona en modo cliente de transmisión. Después de ejecutar el comando, el dispositivo recibe NTP transmitir mensajes desde la interfaz especificada.

Configurar el servidor de transmisión

Paso	Dominio	Observaciones
15. Ingrese a la vista del sistema.	**vista del sistema**	N / A
dieciséis. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	Ingrese a la interfaz para enviar mensajes de difusión NTP.

Paso	Dominio	Observaciones
17. Configure el dispositivo para que funcione en modo de servidor de transmisión NTP.	**servidor de transmisión de servicio ntp** [**ID de clave de autenticación***ID de clave*| **versión***número*] *	De forma predeterminada, el dispositivo no funciona en modo de servidor de transmisión. Después de ejecutar el comando, el dispositivo recibe NTP transmitir mensajes desde la interfaz especificada.

Configurar NTP en modo multidifusión

Un servidor de multidifusión debe estar sincronizado por otros dispositivos o utilizar su reloj local como fuente de referencia antes de sincronizar un cliente de multidifusión. De lo contrario, el cliente de multidifusión no se sincronizará con el servidor de multidifusión.

Configure NTP en modo de multidifusión tanto en un servidor como en un cliente de multidifusión.

Configurar un cliente de multidifusión

Paso	Dominio	Observaciones
18. Ingrese a la vista del sistema.	**vista del sistema**	N / A
19. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	Ingrese a la interfaz para recibir mensajes de multidifusión NTP.
20. Configure el dispositivo para que funcione en modo cliente de multidifusión.	- Configure el dispositivo para que funcione en modo cliente de multidifusión: **cliente-multidifusión-servicio-ntp** [*dirección IP*] - Configure el dispositivo para que funcione en modo cliente de multidifusión IPv6: **servicio ntp ipv6 cliente de multidifusión** *dirección-multidifusión-ipv6*	De forma predeterminada, el dispositivo no funciona en modo cliente de multidifusión. Como práctica recomendada, especifique una dirección IP de multidifusión en el rango de 224.0.1.0 a 224.0.1.255 para el *dirección IP*argumento. Después de ejecutar el comando, el dispositivo recibe mensajes de multidifusión NTP desde la interfaz especificada.

Configurar el servidor de multidifusión

Paso	Dominio	Observaciones
21. Ingrese a la vista del sistema.	**vista del sistema**	N / A
22. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	Ingrese a la interfaz para enviar mensajes de multidifusión NTP.
23. Configure el dispositivo para que funcione en modo de servidor de multidifusión.	- Configure el dispositivo para que funcione en modo de servidor de multidifusión: **servidor-multidifusión-servicio-ntp** [*dirección IP*] [**ID de clave de autenticación***ID de clave*| **ttl***número-ttl*|**versión** *número*] * - Configure el dispositivo para que funcione en modo de servidor de multidifusión: **servicio ntp ipv6 servidor de multidifusión** *dirección-multidifusión-ipv6* [**ID de clave de autenticación***ID de clave*| **ttl***número-ttl*] *	De forma predeterminada, el dispositivo no funciona en modo de servidor de multidifusión. Como práctica recomendada, especifique una dirección IP de multidifusión en el rango de 224.0.1.0 a 224.0.1.255 para el *dirección IP*argumento. Después de ejecutar el comando, el dispositivo envía mensajes de multidifusión NTP desde la interfaz especificada.

Configurar derechos de control de acceso

Paso	Dominio	Observaciones
24. Ingrese a la vista del sistema.	**vista del sistema**	N / A
25. Configurar el derecho de control de acceso al servicio NTP para un dispositivo par para acceder al dispositivo local.	- Configure el derecho de control de acceso al servicio NTP para que un dispositivo par acceda al dispositivo local **acceso al servicio ntp**{**par**|**consulta**|**servidor**|**sincronización**} *número-acl* - Configure el derecho de control de acceso al servicio IPv6 NTP para que un dispositivo par acceda al dispositivo local **servicio ntp ipv6**{**par**|**consulta**|**servidor**|**sincronización**}**accl** *número-acl*	De forma predeterminada, el derecho de control de acceso al servicio NTP para que un dispositivo par acceda al dispositivo local es par.

Antes de configurar el derecho de control de acceso al servicio NTP para el dispositivo local, cree y configure una ACL asociada con el derecho de control de acceso. Para obtener más información sobre ACL, consulte*Guía de configuración de ACL y QoS*.

Configurar la autenticación NTP

Esta sección proporciona instrucciones para configurar la autenticación NTP.

Configurar la autenticación NTP en modo cliente/servidor

Cuando configura la autenticación NTP en modo cliente/servidor:

- Habilite la autenticación NTP.
- Configure una clave de autenticación.
- Establezca la clave como clave confiable tanto en el cliente como en
- el servidor. Asocie la clave con el servidor NTP en el cliente.

Los ID de clave y los valores de clave configurados en el servidor y el cliente deben ser los mismos. De lo contrario, la autenticación NTP falla.

Para configurar la autenticación NTP para un cliente:

Paso	Dominio	Observaciones
26. Ingrese a la vista del sistema.	**vista del sistema**	N / A
27. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
28. Configure una clave de autenticación NTP.	**servicio ntp ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
29. Configure la clave como una clave confiable.	**servicio ntp confiable ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Paso	Dominio	Observaciones
30. Asocie la clave especificada con un servidor NTP.	- Asocie la clave especificada con un servidor NTP: **servidor-unicast-servicio-ntp** { *nombre del servidor*| *dirección IP*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave* - Asocie la clave especificada con un servidor NTP IPv6: **servicio ntp ipv6** **servidor de unidifusión**{*nombre del servidor* | *dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave*	N / A

Para configurar la autenticación NTP para un servidor:

Paso	Dominio	Observaciones
31. Ingrese a la vista del sistema.	**vista del sistema**	N / A
32. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
33. Configure una clave de autenticación NTP.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
34. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Los resultados de la autenticación NTP difieren cuando se realizan diferentes configuraciones en el cliente y el servidor. Para más información, verTabla 2. (N/A en la tabla significa que si se realiza o no la configuración no hace ninguna diferencia).

Tabla 9 Resultados de la autenticación NTP

Cliente			Servidor		
Habilitar NTP autenticación norte	**Configurar cada llave y configurar** es como un **confiable llave**	**Asociar el llave con un servidor NTP**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **clave confiable**	**Autenticación** **resultado**
Sí	Sí	Sí	Sí	Sí	Tuvo éxito. NTP los mensajes pueden ser enviado y recibido correctamente.
Sí	Sí	Sí	Sí	No	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.

Cliente			Servidor		Autenticación resultado
Habilitar NTP autenticación norte	Configurar cada llave y configurar es como un confiable llave	Asociar el llave con un servidor NTP	Habilitar NTP autenticación norte	Configurar una llave y configurar es como un clave confiable	
Sí	Sí	Sí	No	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	No	Sí	N / A	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	N / A	No	N / A	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.
No	N / A	N / A	N / A	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.

Configuración de la autenticación NTP en modo activo/pasivo simétrico

Cuando configura la autenticación NTP en modo de pares simétricos:

- Habilite la autenticación NTP.
- Configure una clave de autenticación.
- Establezca la clave como clave confiable tanto en el par activo como en el
- par pasivo. Asocie la clave con el par pasivo del par activo.

Los ID de clave y los valores de clave configurados en el par activo y en el par pasivo deben ser los mismos. De lo contrario, la autenticación NTP falla.

Para configurar la autenticación NTP para un par activo:

Paso	Dominio	Observaciones
35. Ingrese a la vista del sistema.	**vista del sistema**	N / A
36. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
37. Configure una clave de autenticación NTP.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.

Paso	Dominio	Observaciones
38. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.
39. Asocie la clave especificada con un par pasivo.	- Asocie la clave especificada con un par pasivo: **par de unidifusión de servicio ntp** { *dirección IP*| *nombre de compañero*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave* - Asocie la clave especificada con un par pasivo: **servicio ntp ipv6** **par de unidifusión**{*dirección ipv6*| *nombre de compañero*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave*	N / A

Para configurar la autenticación NTP para un par pasivo:

Paso	Dominio	Observaciones
40. Ingrese a la vista del sistema.	**vista del sistema**	N / A
41. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
42. Configure una clave de autenticación NTP.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
43. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Los resultados de la autenticación NTP difieren cuando se realizan diferentes configuraciones en el par activo y en el par pasivo. Para más información, verTabla 3. (N/A en la tabla significa que si se realiza o no la configuración no hace ninguna diferencia).

Tabla 10 resultados de autenticación NTP

Compañero activo			Par pasivo		
Habilitar NTP autenticación norte	**Configurar una llave y configurar** es como un **clave confiable**	**asociado e la clave con un pasivo par**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **confiable llave**	**Autenticación** **resultado**
No se considera el nivel de estrato de los pares activos y pasivos.					
Sí	Sí	Sí	Sí	Sí	Tuvo éxito. NTP los mensajes pueden ser enviado y recibido correctamente.
Sí	Sí	Sí	Sí	No	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.

Compañero activo			Par pasivo		
Habilitar NTP autenticación norte	**Configurar una llave y configurar** es como un **clave confiable**	**asociado e la clave con un pasivo par**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **confiable llave**	**Autenticación resultado**
Sí	Sí	Sí	No	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
Sí	N / A	No	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
Sí	N / A	No	No	N / A	Sin autenticacion. Los mensajes NTP pueden ser enviado y recibido correctamente.
No	N / A	N / A	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
No	N / A	N / A	No	N / A	Sin autenticacion. Los mensajes NTP pueden ser enviado y recibido correctamente.
El par activo tiene un estrato más alto que el par pasivo.					
Sí	No	Sí	N / A	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
El par pasivo tiene un estrato más alto que el par activo.					
Sí	No	Sí	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibido correctamente.
Sí	No	Sí	No	N / A	Sin autenticacion. Los mensajes NTP pueden ser enviado y recibido correctamente.

Configurar la autenticación NTP en modo transmisión

Cuando configura la autenticación NTP en modo de transmisión:

- Habilite la autenticación NTP.
- Configure una clave de autenticación.
- Establezca la clave como clave confiable tanto en el cliente como en el servidor de
- transmisión. Configure una clave de autenticación NTP en el servidor de transmisión.

Los ID de clave y los valores de clave configurados en el servidor de transmisión y el cliente deben ser los mismos. De lo contrario, la autenticación NTP falla.

Para configurar la autenticación NTP para un cliente de transmisión:

Paso	Dominio	Observaciones
44. Ingrese a la vista del sistema.	**vista del sistema**	N / A
45. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
46. Configure una clave de autenticación NTP.	**servicio ntp ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
47. Configure la clave como una clave confiable.	**servicio ntp confiable ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Para configurar la autenticación NTP para un servidor de transmisión:

Paso	Dominio	Observaciones
48. Ingrese a la vista del sistema.	**vista del sistema**	N / A
49. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
50. Configure una clave de autenticación NTP.	**servicio ntp ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
51. Configure la clave como una clave confiable.	**servicio ntp confiable ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.
52. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
53. Asocie la clave especificada con el servidor de transmisión.	**ID de clave de autenticación del servidor de transmisión del servicio ntp***ID de clave*	De forma predeterminada, el servidor de transmisión no está asociado con ninguna clave.

Los resultados de la autenticación NTP difieren cuando se realizan diferentes configuraciones en el cliente y el servidor de transmisión. Para más información, verTabla 4. (N/A en la tabla significa que si se realiza o no la configuración no hace ninguna diferencia).

Tabla 11 Resultados de la autenticación NTP

servidor de transmisión			Cliente de transmisión		Resultado de la autenticación
Habilitar NTP autenticación norte	**Configurar cada llave y configurar** es como un **confiable llave**	**asociado e la clave con un transmisiones servidor t**	**Habilitar NTP autenticación** norte	**Configurar cada llave y configurar** es como un **confiable llave**	
Sí	Sí	Sí	Sí	Sí	Tuvo éxito. NTP Los mensajes se pueden enviar y recibir correctamente.
Sí	Sí	Sí	Sí	No	Fallido. mensajes NTP no se puede enviar y recibir correctamente.

servidor de transmisión			Cliente de transmisión		Resultado de la autenticación
Habilitar NTP autenticación norte	**Configurar cada llave y configurar es como un confiable llave**	**asociado e la clave con un transmisiones servidor t**	**Habilitar NTP autenticación** norte	**Configurar cada llave y configurar es como un confiable llave**	
Sí	Sí	Sí	No	N / A	Fallido. mensajes NTP no se puede enviar y recibir correctamente.
Sí	No	Sí	Sí	N / A	Fallido. mensajes NTP no se puede enviar y recibir correctamente.
Sí	No	Sí	No	N / A	Sin autenticacion. NTP Los mensajes se pueden enviar y recibir correctamente.
Sí	N / A	No	Sí	N / A	Fallido. mensajes NTP no se puede enviar y recibir correctamente.
Sí	N / A	No	No	N / A	Sin autenticacion. NTP Los mensajes se pueden enviar y recibir correctamente.
No	N / A	N / A	Sí	N / A	Fallido. mensajes NTP no se puede enviar y recibir correctamente.
No	N / A	N / A	No	N / A	Sin autenticacion. NTP Los mensajes se pueden enviar y recibir correctamente.

Configurar la autenticación NTP en modo multidifusión

Cuando configura la autenticación NTP en modo multidifusión:

- Habilite la autenticación NTP.
- Configure una clave de autenticación.
- Establezca la clave como clave confiable tanto en el cliente como en el servidor de multidifusión.
- Configure una clave de autenticación NTP en el servidor de multidifusión.

Los ID de clave y los valores de clave configurados en el servidor y el cliente de multidifusión deben ser los mismos. De lo contrario, la autenticación NTP falla.

Para configurar la autenticación NTP para un cliente de multidifusión:

Paso	Dominio	Observaciones
54. Ingrese a la vista del sistema.	**vista del sistema**	N / A
55. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
56. Configure una clave de autenticación NTP.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.

Paso	Dominio	Observaciones
57. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.

Para configurar la autenticación NTP para un servidor de multidifusión:

Paso	Dominio	Observaciones
58. Ingrese a la vista del sistema.	**vista del sistema**	N / A
59. Habilite la autenticación NTP.	**habilitación de autenticación de servicio ntp**	De forma predeterminada, la autenticación NTP está deshabilitada.
60. Configure una clave de autenticación NTP.	**servicio ntp** **ID de clave de autenticación***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación NTP.
61. Configure la clave como una clave confiable.	**servicio ntp confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, ninguna clave de autenticación está configurada como clave confiable.
62. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
63. Asocie la clave especificada con el servidor de multidifusión.	- Asocie la clave especificada con un servidor de multidifusión: **servidor-multidifusión-servicio-ntp** [*dirección IP*] **ID de clave de autenticación***ID de clave* - Asocie la clave especificada con un servidor de multidifusión IPv6: **servicio ntp ipv6** **servidor de multidifusión** *dirección-multidifusión-ipv6* **ID de clave de autenticación***ID de clave*	De forma predeterminada, no hay ningún servidor de multidifusión asociado con la clave especificada.

Los resultados de la autenticación NTP difieren cuando se realizan diferentes configuraciones en el cliente y el servidor de transmisión. Para más información, verTabla 5. (N/A en la tabla significa que si se realiza o no la configuración no hace ninguna diferencia).

Tabla 12 Resultados de la autenticación NTP

Servidor de multidifusión			Cliente de multidifusión		
Habilitar NTP autenticación norte	**Configurar una llave y configurar** es como un **clave confiable**	**Asociado la llave con** una multidifusión **servidor**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **clave confiable**	**Autenticación** **resultado**
Sí	Sí	Sí	Sí	Sí	Tuvo éxito. NTP los mensajes pueden ser enviado y recibido correctamente.
Sí	Sí	Sí	Sí	No	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.

Servidor de multidifusión			Cliente de multidifusión		
Habilitar NTP autenticación norte	**Configurar una llave y configurar** es como un **clave confiable**	**Asociado la llave con** una multidifusión **servidor**	**Habilitar NTP autenticación** norte	**Configurar una llave y configurar** es como un **clave confiable**	**Autenticación** resultado
Sí	Sí	Sí	No	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	No	Sí	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	No	Sí	No	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.
Sí	N / A	No	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
Sí	N / A	No	No	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.
No	N / A	N / A	Sí	N / A	Fallido. NTP los mensajes no pueden ser enviado y recibió correctamente.
No	N / A	N / A	No	N / A	Sin autenticacion. mensajes NTP se puede enviar y recibió correctamente.

Configuración de parámetros opcionales de NTP

Las tareas de configuración de esta sección son tareas opcionales. Configúrelos para mejorar la seguridad, el rendimiento o la confiabilidad de NTP.

Especificación de la interfaz de origen para mensajes NTP

Para evitar que los cambios de estado de la interfaz causen fallas en la comunicación NTP, configure el dispositivo para usar la dirección IP de una interfaz que esté siempre activa. Por ejemplo, puede configurar el dispositivo para utilizar una interfaz de bucle invertido como dirección IP de origen para los mensajes NTP que se enviarán.

Cuando el dispositivo responde a una solicitud NTP, la dirección IP de origen de la respuesta NTP es siempre la dirección IP de la interfaz que recibió la solicitud NTP.

Siga estas pautas cuando especifique la interfaz de origen para mensajes NTP:

- Si ha especificado la interfaz de origen para los mensajes NTP en el**servicio ntp**[**ipv6**] **servidor de unidifusión**o**servicio ntp**[**ipv6**]**par de unidifusión**comando, la interfaz especificada en el **servicio ntp**[**ipv6**]**servidor de unidifusión**o**servicio ntp**[**ipv6**]**par de unidifusión**El comando funciona como interfaz de origen para mensajes NTP.
- Si ha configurado el**servidor de transmisión de servicio ntp**o**servicio ntp**[**ipv6**] **servidor de multidifusión**comando, la interfaz de origen para los mensajes NTP de difusión o multidifusión es la interfaz configurada con el comando respectivo.

Para especificar la interfaz de origen para mensajes NTP:

Paso	Dominio	Observaciones
64. Ingrese a la vista del sistema.	**vista del sistema**	N / A
sesenta y cinco. Especifique la interfaz de origen para los mensajes NTP.	- Especifique la interfaz de origen para los mensajes NTP: **fuente de servicio ntp** *Tipo de interfaz* *número de interfaz* - Especifique la interfaz de origen para los mensajes NTP IPv6: **fuente ipv6 del servicio ntp** *Tipo de interfaz* *número de interfaz*	De forma predeterminada, no se especifica ninguna interfaz de origen para los mensajes NTP.

Deshabilitar una interfaz para que no reciba mensajes NTP

Cuando NTP está habilitado, todas las interfaces de forma predeterminada pueden recibir mensajes NTP. Por motivos de seguridad, puede desactivar algunas de las interfaces para que no reciban mensajes NTP.

Para desactivar una interfaz para que no reciba mensajes NTP:

Paso	Dominio	Observaciones
66. Ingrese a la vista del sistema.	**vista del sistema**	N / A
67. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz* *número de interfaz*	N / A
68. Deshabilite la interfaz para que no reciba mensajes NTP.	- Para IPv4: **deshacer la habilitación entrante del servicio ntp** - Para IPv6: **deshacer el servicio ntp ipv6 habilitación entrante**	De forma predeterminada, una interfaz recibe mensajes NTP.

Configurar el número máximo de asociaciones dinámicas

NTP tiene los siguientes tipos de asociaciones:

- **Asociación estática**—Una asociación creada manualmente.
- **Asociación dinámica**—Asociación temporal creada por el sistema durante la operación NTP. Una asociación dinámica se elimina si no se intercambian mensajes en aproximadamente 12 minutos.

A continuación se describe cómo se establece una asociación en diferentes modos de asociación:

- **Modo cliente/servidor**—Después de especificar un servidor NTP, el sistema crea una asociación estática en el cliente. El servidor simplemente responde pasivamente al recibir un mensaje, en lugar de crear una asociación (estática o dinámica).
- **Modo activo/pasivo simétrico**—Después de especificar un par simétrico-pasivo en un par simétrico-activo, se crean asociaciones estáticas en el par simétrico-activo y asociaciones dinámicas en el par simétrico-pasivo.
- **Modo de transmisión o multidifusión**—Las asociaciones estáticas se crean en el servidor y las asociaciones dinámicas se crean en el cliente.

Un único dispositivo puede tener un máximo de 128 asociaciones simultáneas, incluidas asociaciones estáticas y asociaciones dinámicas.

Realice esta tarea para restringir el número de asociaciones dinámicas y evitar que ocupen demasiados recursos del sistema.

Para configurar el número máximo de asociaciones dinámicas:

Paso	Dominio	Observaciones
69. Ingrese a la vista del sistema.	**vista del sistema**	N / A
70. Configurar el número máximo de sesiones dinámicas que se pueden establecer.	**servicio ntp sesiones-max-dinamicas***número*	Por defecto, el comando puede establecer hasta 100 sesiones dinámicas.

Establecer un valor DSCP para paquetes NTP

El valor DSCP determina la prioridad de envío de un paquete. Para

establecer un valor DSCP para paquetes NTP:

Paso	Dominio	Observaciones
71. Ingrese a la vista del sistema.	**vista del sistema**	N / A
72. Establezca un valor DSCP para paquetes NTP.	- Paquetes IPv4: **servicio ntp dscp***valor-dscp* - Paquetes IPv6: **servicio ntp ipv6 dscp** *valor-dscp*	Los valores predeterminados para un valor DSCP: - 48 para paquetes IPv4 NTP. - 56 para paquetes IPv6 NTP.

Configurar el reloj local como fuente de referencia

Siga estas pautas cuando configure el reloj local como fuente de referencia:

- Asegúrese de que el reloj local pueda proporcionar la precisión horaria requerida para la red. Después de configurar el reloj local como fuente de referencia, el reloj local se sincroniza y puede funcionar como servidor de hora para sincronizar otros dispositivos en la red. Si el reloj local es incorrecto, se producen errores de sincronización.
- Antes de configurar esta función, ajuste la hora del sistema local para asegurarse de que sea precisa.
- Los dispositivos se diferencian por el hardware y la precisión del reloj. Para evitar fluctuaciones en la red y fallas en la sincronización del reloj, no configure múltiples fuentes de referencia en la misma red.

Para configurar el reloj local como fuente de referencia:

Paso	Dominio	Observaciones
73. Ingrese a la vista del sistema.	**vista del sistema**	N / A

Paso	Dominio	Observaciones
74. Configure el reloj local como fuente de referencia.	**servicio ntp refclock-master** [*dirección IP*] [*estrato*]	De forma predeterminada, el dispositivo no utiliza el reloj local como fuente de referencia.

Visualización y mantenimiento de NTP

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Muestra información sobre asociaciones NTP IPv6.	**mostrar sesiones ipv6 de servicio ntp**[**verboso**]
Muestra información sobre asociaciones NTP IPv4.	**mostrar sesiones de servicio ntp**[**verboso**]
Muestra información sobre el estado del servicio NTP.	**mostrar el estado del servicio ntp**
Muestre información breve sobre los servidores NTP desde el dispositivo local a la fuente de referencia principal.	**mostrar el seguimiento del servicio ntp**

Ejemplos de configuración NTP

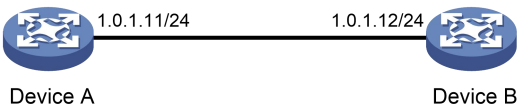
Ejemplo de configuración del modo cliente/servidor NTP

Requisitos de red

Como se muestra enFigura 5, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo B para que funcione en modo cliente y el Dispositivo A para que se utilice como servidor NTP para el Dispositivo B.

Figura 41 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 5. (No se muestran detalles).
2. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2
3. Configurar el dispositivo B:

   # Habilite el servicio NTP.

   <DispositivoB> vista del sistema

   [DispositivoB] habilitación del servicio ntp

Especifique el Dispositivo A como el servidor NTP del Dispositivo B para que el Dispositivo B se sincronice con el Dispositivo A.

[DispositivoB] servidor de unidifusión de servicio ntp 1.0.1.11

4. Verifique la configuración:

Verifique que el dispositivo B se haya sincronizado con el dispositivo A y que el nivel del estrato de reloj sea 3 en el dispositivo B y 2 en el dispositivo A.

[DispositivoB] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 1.0.1.11

Modo local: cliente

ID del reloj de referencia: 1.0.1.11

Indicador de salto: 00

Fluctuación del reloj: 0,000977 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00383 ms Dispersión de raíz: 16,26572 ms Tiempo de referencia: d0c6033f.b9923965 Miércoles 29 de diciembre de 2010 18:58:07.724

Verifique que se haya establecido una asociación NTP IPv4 entre el dispositivo B y el dispositivo A.

[DispositivoB] muestra sesiones de servicio ntp

	fuente	referencia	la encuesta de alcance de Stra ahora compensa el retraso de dispersión
* * [12345]1.0.1.11	127.127.1.0	2	1 64 15 -4,0 0,0038 16,262

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

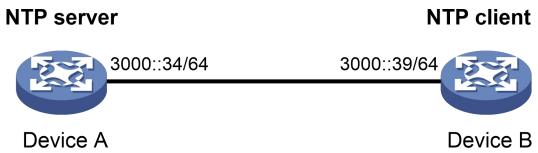
Ejemplo de configuración del modo cliente/servidor IPv6 NTP

Requisitos de red

Como se muestra enFigura 6, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo B para que funcione en modo cliente y el Dispositivo A para que se utilice como servidor NTP IPv6 para el Dispositivo B.

Figura 42 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 6. (No se muestran detalles).
2. Configurar el dispositivo A:

Habilite el servicio NTP.

<DispositivoA> vista del sistema

[DispositivoA] habilitación del servicio ntp

Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

[DispositivoA] ntp-service refclock-master 2

3. Configurar el dispositivo B:

Habilite el servicio NTP.

<DispositivoB> vista del sistema

[DispositivoB] habilitación del servicio ntp

Especifique el Dispositivo A como el servidor NTP IPv6 del Dispositivo B para que el Dispositivo B se sincronice con el Dispositivo A.

[DispositivoB] servicio ntp ipv6 servidor unicast 3000::34

4. Verifique la configuración:

Verifique que el dispositivo B se haya sincronizado con el dispositivo A y que el nivel del estrato de reloj sea 3 en el dispositivo B y 2 en el dispositivo A.

[DispositivoB] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 3000::34

Modo local: cliente

ID de reloj de referencia: 163.29.247.19

Indicador de salto: 00

Fluctuación del reloj: 0,000977 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,02649 ms Dispersión de raíz: 12,24641 ms Tiempo de referencia: d0c60419.9952fb3e Miércoles 29 de diciembre de 2010 19:01:45.598

Verifique que se haya establecido una asociación NTP IPv6 entre el dispositivo B y el dispositivo A.

[DispositivoB] muestra sesiones ipv6 de servicio ntp

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Fuente: [12345]3000::34

Referencia: 127.127.1.0 Estrato de reloj: 2

Accesibilidad: 15 Intervalo de encuesta: 64

Hora de la última recepción: 19 Compensación: 0,0

Retraso de ida y vuelta: 0,0 Dispersión: 0.0

Sesiones totales: 1

Ejemplo de configuración de modo activo/pasivo simétrico NTP

Requisitos de red

Como se muestra enFigura 7, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo A para que funcione en modo activo simétrico y especifique el Dispositivo B como par pasivo del Dispositivo A.

Figura 43 Diagrama de red

Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 7. (No se muestran detalles).
2. Configurar el dispositivo B:

   # Habilite el servicio NTP.

   <DispositivoB> vista del sistema

   [DispositivoB] habilitación del servicio ntp
3. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2

   # Configure el dispositivo B como un par pasivo simétrico.

   [DispositivoA] ntp-service unicast-peer 3.0.1.32
4. Verifique la configuración:

   # Verifique que el dispositivo B se haya sincronizado con el dispositivo A.

   [DispositivoB] muestra el estado del servicio ntp

   Reloj estado: sincronizado

   Reloj estrato: 3

   Sistema par: 3.0.1.3 1

   Local modo: sim_pasivo

   ID del reloj de referencia: 3.0.1.31

   Indicador de salto: 00

   Fluctuación del reloj: 0,000916 s

   Estabilidad: 0,000 pps

   Precisión del reloj: 2^-17

   Retardo de raíz: 0,00609 ms Dispersión de raíz: 1,95859 ms Tiempo de referencia: 83aec681.deb6d3e5 Casarse, Ene 8 2014 14:33:11.081

   # Verifique que se haya establecido una asociación NTP IPv4 entre el dispositivo B y el dispositivo A.

   [DispositivoB] muestra sesiones de servicio ntp

   fuente referencia la encuesta de alcance de Stra ahora compensa el retraso de dispersión

   ****

   [12]3.0.1.31 127.127.1.0 2 62 64 34 0,4251 6,0882 1392,1

   Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

   Sesiones totales: 1

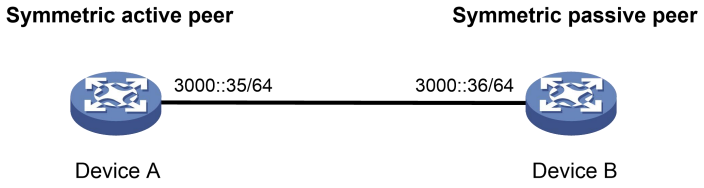
Ejemplo de configuración de modo activo/pasivo simétrico IPv6 NTP

Requisitos de red

Como se muestra enFigura 8, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo A para que funcione en modo activo simétrico y especifique el Dispositivo B como el par pasivo IPv6 del Dispositivo A.

Figura 44 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 8. (No se muestran detalles).
2. Configurar el dispositivo B:

   # Habilite el servicio NTP.

   <DispositivoB> vista del sistema

   [DispositivoB] habilitación del servicio ntp
3. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2

   # Configure el dispositivo B como un par pasivo simétrico IPv6.

   [DispositivoA] ntp-service ipv6 unicast-peer 3000::36
4. Verifique la configuración:

   # Verifique que el dispositivo B se haya sincronizado con el dispositivo A.

   [DispositivoB] muestra el estado del servicio ntp

   Reloj estado: sincronizado

   Reloj estrato: 3

   Sistema par: 3000::35

   Local modo: sim_ pasivo

   ID de reloj de referencia: 251.73.79.32

   Indicador de salto: 11

   Fluctuación del reloj: 0,000977 s

   Estabilidad: 0,000 pps

   Precisión del reloj: 2^-18

   Retardo de raíz: 0,01855 ms Dispersión de raíz: 9,23483 ms Tiempo de referencia: d0c6047c.97199f9f Miércoles 29 de diciembre de 2010 19:03:24.590

Verifique que se haya establecido una asociación NTP IPv6 entre el dispositivo B y el dispositivo A.

[DispositivoB] muestra sesiones ipv6 de servicio ntp

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Fuente: [1234]3000::35

Referencia: 127.127.1.0 Estrato de reloj: 2

Accesibilidad: 15 Intervalo de encuesta: 64

Hora de la última recepción: 19 Compensación: 0,0

Retraso de ida y vuelta: 0,0 Dispersión: 0.0

Sesiones totales: 1

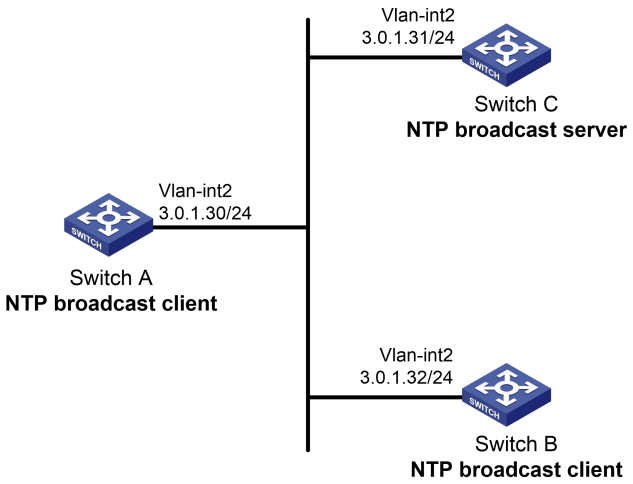
Ejemplo de configuración del modo de transmisión NTP

Requisitos de red

Como se muestra enFigura 9, Switch C funciona como servidor NTP para múltiples dispositivos en un segmento de red y sincroniza la hora entre múltiples dispositivos.

- Configure el reloj local del Switch C como fuente de referencia, con el nivel de estrato 2.
- Configure el Switch C para operar en modo de servidor de transmisión y enviar mensajes de transmisión desde la interfaz VLAN 2.
- Configure el Switch A y el Switch B para operar en modo de cliente de transmisión y escuche los mensajes de transmisión a través de la interfaz VLAN 2.

Figura 45 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el conmutador A, el conmutador B y el conmutador C puedan comunicarse entre sí, como se muestra enFigura 9. (No se muestran detalles).
2. Configurar el interruptor C:

   # Habilite el servicio NTP.

   <SwitchC> vista del sistema

   [SwitchC] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [SwitchC] servicio ntp refclock-master 2

Configure el Switch C para operar en modo de servidor de transmisión y enviar mensajes de transmisión a través de la interfaz VLAN 2.

[SwitchC] interfaz vlan-interface 2 [SwitchC-Vlan-interface2] servidor de

transmisión de servicio ntp

3. Configurar el interruptor A:

Habilite el servicio NTP.

<SwitchA> vista del sistema

[SwitchA] habilitación del servicio ntp

Configure el conmutador A para que funcione en modo de cliente de transmisión y reciba mensajes de transmisión en la interfaz VLAN 2.

[SwitchA] interfaz vlan-interface 2 [SwitchA-Vlan-interface2] cliente de

transmisión de servicio ntp

4. Configurar el interruptor B:

Habilite el servicio NTP.

<SwitchB> vista del sistema

[SwitchB] habilitación del servicio ntp

Configure el Switch B para operar en modo de cliente de transmisión y recibir mensajes de transmisión en la interfaz VLAN 2.

[SwitchB] interfaz vlan-interface 2 [SwitchB-Vlan-interface2] cliente de

transmisión de servicio ntp

5. Verifique la configuración:

Verifique que el Switch A se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch A y 2 en el Switch C.

[SwitchA-Vlan-interface2] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 3.0.1.31

Modo local: bcliente

ID del reloj de referencia: 3.0.1.31

Indicador de salto: 00

Fluctuación del reloj: 0,044281 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00229 ms Dispersión de

raíz: 4,12572 ms Tiempo de referencia:

d0d289fe.ec43c720 Se sentó, Ene 8 2011 7:00:14.922

Verifique que se haya establecido una asociación NTP IPv4 entre el Switch A y el Switch C.

[SwitchA-Vlan-interface2] muestra sesiones de servicio ntp

fuente referencia encuesta de alcance de Stra ahora compensado retraso disper

****

* * [1245]3.0.1.31 127.127.1.0 2 1 64 519 - 0,0 0,0022 4,1257

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

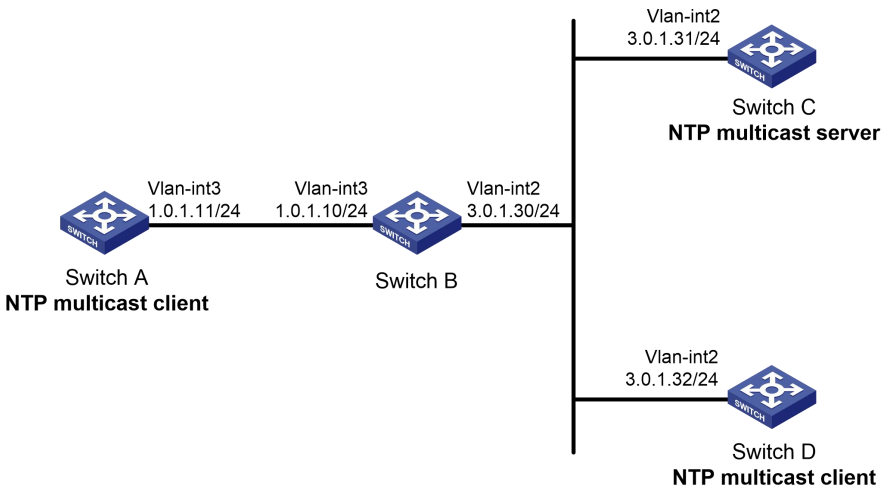
Ejemplo de configuración del modo multidifusión NTP

Requisitos de red

Como se muestra enFigura 10, Switch C funciona como servidor NTP para múltiples dispositivos en diferentes segmentos de red y sincroniza la hora entre múltiples dispositivos.

- Configure el reloj local del Switch C como fuente de referencia, con el nivel de estrato 2.
- Configure el Switch C para operar en modo de servidor de multidifusión y enviar mensajes de multidifusión desde la interfaz VLAN 2.
- Configure el Switch A y el Switch D para operar en modo de cliente de multidifusión y recibir mensajes de multidifusión a través de la interfaz VLAN 3 y la interfaz VLAN 2, respectivamente.

Figura 46 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que los conmutadores puedan comunicarse entre sí, como se muestra enFigura 10. (No se muestran detalles).
2. Configurar el interruptor C:

   # Habilite el servicio NTP.

   <SwitchC> vista del sistema

   [SwitchC] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [SwitchC] servicio ntp refclock-master 2

   # Configure el Switch C para operar en modo de servidor de multidifusión y enviar mensajes de multidifusión a través de la interfaz VLAN 2.

   [SwitchC] interfaz vlan-interface 2 [SwitchC-Vlan-interface2] servicio ntp

   servidor de multidifusión
3. Configurar el interruptor D:

   # Habilite el servicio NTP.

   <SwitchD> vista del sistema

   [SwitchD] habilitación del servicio ntp

   # Configure el Switch D para operar en modo de cliente de multidifusión y recibir mensajes de multidifusión en la interfaz VLAN 2.

   [SwitchD] interfaz vlan-interface 2 [SwitchD-Vlan-interface2] servicio ntp

   cliente de multidifusión

4. Verifique la configuración:

El Switch D y el Switch C están en la misma subred, por lo que el Switch D puede hacer lo siguiente:

- Reciba los mensajes multicast del Switch C sin estar habilitado con las funciones multicast.
- Sincronizar con el interruptor C.

Verifique que el Switch D se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch D y 2 en el Switch C.

[SwitchD-Vlan-interface2] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 3.0.1.31

Modo local: bcliente

ID del reloj de referencia: 3.0.1.31

Indicador de salto: 00

Fluctuación del reloj: 0,044281 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00229 ms Dispersión de

raíz: 4,12572 ms Tiempo de referencia:

d0d289fe.ec43c720 Se sentó, Ene 8 2011 7:00:14.922

Verifique que se haya establecido una asociación NTP IPv4 entre el Switch D y el Switch C.

[SwitchD-Vlan-interface2] muestra sesiones de servicio ntp

	fuente	referencia	encuesta de alcance de Stra	ahora compensado retraso disper
**********				
* * [1245]3.0.1.31	127.127.1.0	2	1 64 519 - 0,0 0,0022 4,1257	

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

5. Configurar el interruptor B:

Debido a que el Switch A y el Switch C están en subredes diferentes, debe habilitar las funciones de multidifusión en el Switch B antes de que el Switch A pueda recibir mensajes de multidifusión desde el Switch C.

Habilite el enrutamiento de multidifusión IP e IGMP.

<SwitchB> vista del sistema

[SwitchB] enrutamiento de

multidifusión [SwitchB-mrib] salir

[SwitchB] interfaz vlan-interface 2 [SwitchB-Vlan-

interface2] pim dm [SwitchB-Vlan-interface2] quit

[SwitchB] vlan 3

[SwitchB-vlan3] puerto gigabitethernet 2/0/1 [SwitchB-

vlan3] salir

[SwitchB] interfaz vlan-interface 3 [SwitchB-Vlan-interface3] igmp enable

[SwitchB-Vlan-interface3] igmp static-group 224.0.1.1 [SwitchB-Vlan-

interface3] salir

[SwitchB] igmp-snooping [SwitchB-igmp-snooping] salir [SwitchB] interfaz gigabitethernet 2/0/1

[SwitchB-GigabitEthernet2/0/1] igmp-snooping static-group 224.0.1.1 vlan 3

6. Configurar el interruptor A:

   # Habilite el servicio NTP.

   <SwitchA> vista del sistema

   [SwitchA] habilitación del servicio ntp

   # Configure el conmutador A para que funcione en modo de cliente de multidifusión y reciba mensajes de multidifusión en la interfaz VLAN 3.

   [SwitchA] interfaz vlan-interface 3 [SwitchA-Vlan-interface3] cliente-

   multidifusión de servicio ntp

7. Verifique la configuración:

   # Verifique que el Switch A se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch A y 2 en el Switch C.

   [SwitchA-Vlan-interface3] muestra el estado del servicio ntp

   Reloj estado: sincronizado

   Reloj estrato: 3

   Par del sistema: 3.0.1.31

   Modo local: bcliente

   ID del reloj de referencia: 3.0.1.31

   Indicador de salto: 00

   Fluctuación del reloj: 0,165741 s

   Estabilidad: 0,000 pps

   Precisión del reloj: 2^-18

   Retardo de raíz: 0,00534 ms Dispersión de

   raíz: 4,51282 ms Tiempo de referencia:

   d0c61289.10b1193f Miércoles 29 de diciembre de 2010 20:03:21.065

   # Verifique que se haya establecido una asociación NTP IPv4 entre el Switch A y el Switch C.

   [SwitchA-Vlan-interface3] muestra sesiones de servicio ntp

   fuente referencia encuesta de alcance de Stra ahora compensado retraso disper

   ****

   * * [1234]3.0.1.31 127.127.1.0 2 247 64 381 - 0,0 0,0053 4,5128

   Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

   Sesiones totales: 1

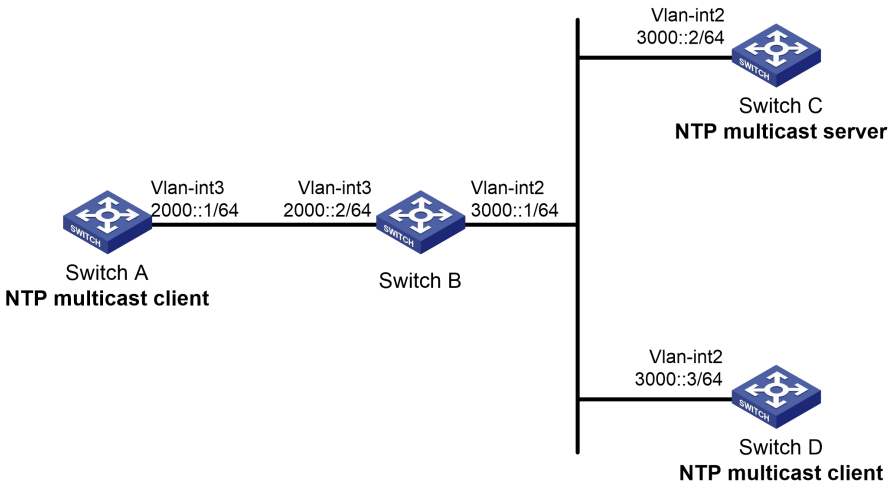
Ejemplo de configuración del modo multidifusión IPv6 NTP

Requisitos de red

Como se muestra enFigura 11, Switch C funciona como servidor NTP para múltiples dispositivos en diferentes segmentos de red y sincroniza la hora entre múltiples dispositivos.

- Configure el reloj local del Switch C como fuente de referencia, con el nivel de estrato 2.
- Configure el Switch C para operar en modo de servidor de multidifusión IPv6 y enviar mensajes de multidifusión IPv6 desde la interfaz VLAN 2.
- Configure el Switch A y el Switch D para operar en modo de cliente de multidifusión IPv6 y recibir mensajes de multidifusión IPv6 a través de la interfaz VLAN 3 y la interfaz VLAN 2, respectivamente.

Figura 47 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que los conmutadores puedan comunicarse entre sí, como se muestra enFigura 11. (No se muestran detalles).
2. Configurar el interruptor C:

   # Habilite el servicio NTP.

   <SwitchC> vista del sistema

   [SwitchC] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [SwitchC] servicio ntp refclock-master 2

   # Configure el Switch C para operar en modo de servidor de multidifusión IPv6 y enviar mensajes de multidifusión a través de la interfaz VLAN 2.

   [SwitchC] interfaz vlan-interfaz 2

   [SwitchC-Vlan-interface2] servidor de multidifusión ipv6 de servicio ntp ff24::1
3. Configurar el interruptor D:

   # Habilite el servicio NTP.

   <SwitchD> vista del sistema

   [SwitchD] habilitación del servicio ntp

   # Configure el Switch D para operar en modo de cliente de multidifusión IPv6 y recibir mensajes de multidifusión en la interfaz VLAN 2.

   [SwitchD] interfaz vlan-interfaz 2

   [SwitchD-Vlan-interface2] servicio ntp ipv6 cliente de multidifusión ff24::1
4. Verifique la configuración:

   El Switch D y el Switch C están en la misma subred, por lo que el Switch D puede hacer lo siguiente:

   - Reciba los mensajes de multidifusión IPv6 desde el Switch C sin estar habilitado con las funciones de multidifusión IPv6.
   - Sincronizar con el interruptor C.

   # Verifique que el Switch D se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch D y 2 en el Switch C.

   [SwitchD-Vlan-interface2] muestra el estado del servicio ntp

   ```
   Reloj estado: sincronizado
   Reloj estrato: 3
   Par del sistema: 3000::2
   ```

Modo local: bcliente
ID de reloj de referencia: 165.84.121.65
Indicador de salto: 00
Fluctuación del reloj: 0,000977 s
Estabilidad: 0,000 pps
Precisión del reloj: 2^-18
Retardo de raíz: 0,00000 ms Dispersión de
raíz: 8,00578 ms Tiempo de referencia:
d0c60680.9754fb17 Miércoles 29 de diciembre de 2010 19:12:00.591

Verifique que se haya establecido una asociación NTP IPv6 entre el Switch D y el Switch C.

[SwitchD-Vlan-interface2] muestra sesiones ipv6 de servicio ntp
Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Fuente: [1234]3000::2
Referencia: 127.127.1.0 Estrato de reloj: 2
Accesibilidad: 111 Intervalo de encuesta: 64
Hora de la última recepción: 23 Compensación: -0,0
Retraso de ida y vuelta: 0,0 Dispersión: 0,0

Sesiones totales: 1

5. Configurar el interruptor B:

Debido a que el Switch A y el Switch C están en subredes diferentes, debe habilitar las funciones de multidifusión IPv6 en el Switch B antes de que el Switch A pueda recibir mensajes de multidifusión IPv6 desde el Switch C.

Habilite las funciones de multidifusión IPv6.

<SwitchB> vista del sistema
[SwitchB] enrutamiento de multidifusión
ipv6 [SwitchB-mrib6] salir
[SwitchB] interfaz vlan-interface 2 [SwitchB-Vlan-
interface2] ipv6 pim dm [SwitchB-Vlan-interface2]
salir [SwitchB] vlan 3

[SwitchB-vlan3] puerto gigabitethernet 2/0/1 [SwitchB-
vlan3] salir
[SwitchB] interfaz vlan-interface 3 [SwitchB-Vlan-interface3] mld
enable [SwitchB-Vlan-interface3] mld static-group ff24::1 [SwitchB-
Vlan-interface3] quit

[SwitchB] espionaje
[SwitchB-mld-espionaje] abandonar
[SwitchB] interfaz gigabitethernet 2/0/1 [SwitchB-GigabitEthernet2/0/1] mld-snooping static-
group ff24::1 vlan 3

6. Configurar el interruptor A:

Habilite el servicio NTP.

<SwitchA> vista del sistema
[SwitchA] habilitación del servicio ntp

Configure el conmutador A para que funcione en modo de cliente de multidifusión IPv6 y reciba mensajes de multidifusión IPv6 en la interfaz VLAN 3.

[SwitchA] interfaz vlan-interfaz 3

[SwitchA-Vlan-interface3] servicio ntp ipv6 cliente de multidifusión ff24::1

7. Verifique la configuración:

Verifique que el Switch A se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 3 en el Switch A y 2 en el Switch C.

[SwitchA-Vlan-interface3] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 3

Par del sistema: 3000::2

Modo local: bcliente

ID de reloj de referencia: 165.84.121.65

Indicador de salto: 00

Fluctuación del reloj: 0,165741 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00534 ms Dispersión de

raíz: 4,51282 ms Tiempo de referencia:

d0c61289.10b1193f Miércoles 29 de diciembre de 2010 20:03:21.065

Verifique que se haya establecido una asociación NTP IPv6 entre el Switch A y el Switch C.

[SwitchA-Vlan-interface3] muestra sesiones ipv6 de servicio ntp

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Fuente: [124]3000::2

Referencia: 127.127.1.0 Estrato de reloj: 2

Accesibilidad: 2 Intervalo de encuesta: 64

Hora de la última recepción: 71 Compensación: -0,0

Retraso de ida y vuelta: 0,0 Dispersión: 0,0

Sesiones totales: 1

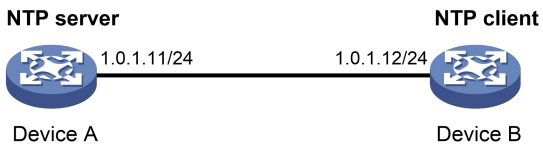
Ejemplo de configuración para modo cliente/servidor NTP con autenticación

Requisitos de red

Como se muestra enFigura 12, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.
- Configure el Dispositivo B para que funcione en modo cliente y especifique el Dispositivo A como el servidor NTP del Dispositivo B.
- Configure la autenticación NTP tanto en el Dispositivo A como en el Dispositivo B.

Figura 48 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 12. (No se muestran detalles).
2. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Especifique el reloj local como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2
3. Configurar el dispositivo B:

   # Habilite el servicio NTP.

   <DispositivoB> vista del sistema

   [DispositivoB] habilitación del servicio ntp

   # Habilite la autenticación NTP en el dispositivo B.

   [DispositivoB] habilitación de autenticación de servicio ntp

   # Establezca una clave de autenticación e ingrese la clave en texto sin formato.

   [DispositivoB] ID de clave de autenticación de servicio ntp 42 modo de autenticación md5 simple aNiceKey

   # Especifique la clave como clave confiable.

   [DispositivoB] ntp-service autenticación confiable-keyid 42

   # Especifique el Dispositivo A como el servidor NTP del Dispositivo B y asocie el servidor con la clave 42.

   [DispositivoB] ntp-service unicast-server 1.0.1.11 autenticación-keyid 42

   Antes de que el Dispositivo B pueda sincronizar su reloj con el del Dispositivo A, habilite la autenticación NTP para el Dispositivo A.
4. Configure la autenticación NTP en el dispositivo A:

   # Habilite la autenticación NTP.

   [DispositivoA] habilitación de autenticación de servicio ntp

   # Establezca una clave de autenticación e ingrese la clave en texto sin formato.

   [DispositivoA] ID de clave de autenticación de servicio ntp 42 modo de autenticación md5 simple aNiceKey

   # Especifique la clave como clave confiable.

   [DispositivoA] ntp-service-keyid de autenticación confiable 42
5. Verifique la configuración:

   # Verifique que el dispositivo B se haya sincronizado con el dispositivo A y que el nivel del estrato de reloj sea 3 en el dispositivo B y 2 en el dispositivo A.

   [DispositivoB] muestra el estado del servicio ntp

   ```
   Reloj estado: sincronizado
   Reloj estrato: 3
   Par del sistema: 1.0.1.11
   Modo local: cliente
   ID del reloj de referencia: 1.0.1.11
   Indicador de salto: 00
   Fluctuación del reloj: 0,005096 s
   Estabilidad: 0,000 pps
   Precisión del reloj: 2^-18
   Retardo de raíz: 0,00655 ms
   Dispersión de raíz: 1,15869 ms
   ```

Hora de referencia: d0c62687.ab1bba7d miércoles 29 de diciembre de 2010 21:28:39.668

Verifique que se haya establecido una asociación NTP IPv4 entre el dispositivo B y el dispositivo A.

[DispositivoB] muestra sesiones de servicio ntp

	fuente	referencia	la encuesta de alcance de Stra ahora compensa el retraso de dispersión
* * [1245]1.0.1.11	127.127.1.0	2	1 64 519 - 0,0 0,0065 0,0

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

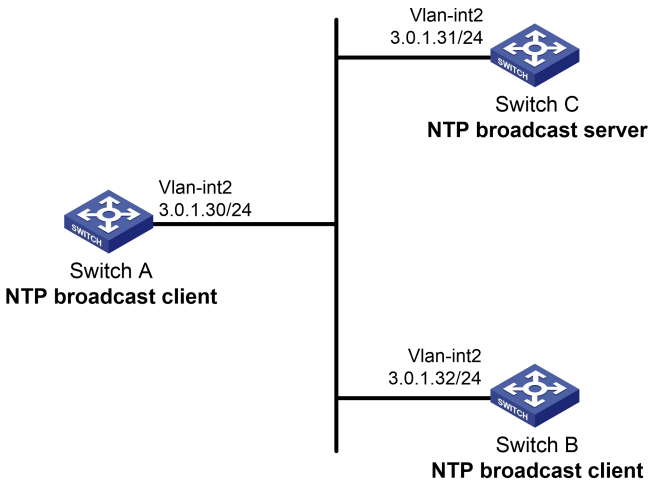
Ejemplo de configuración para modo de transmisión NTP con autenticación

Requisitos de red

Como se muestra enFigura 13, Switch C funciona como servidor NTP para múltiples dispositivos en diferentes segmentos de red y sincroniza la hora entre múltiples dispositivos. El conmutador A y el conmutador B autentican la fuente de referencia.

- Configure el reloj local del Switch C como fuente de referencia, con el nivel de estrato 3.
- Configure el Switch C para operar en modo de servidor de transmisión y enviar mensajes de transmisión desde la interfaz VLAN 2.
- Configure el Switch A y el Switch B para operar en modo de cliente de transmisión y recibir mensajes de transmisión a través de la interfaz VLAN 2.
- Habilite la autenticación NTP en el Switch A, el Switch B y el Switch C.

Figura 49 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el conmutador A, el conmutador B y el conmutador C puedan comunicarse entre sí, como se muestra enFigura 13. (No se muestran detalles).
2. Configurar el interruptor A:

   # Habilite el servicio NTP.

   <SwitchA> vista del sistema

   [SwitchA] habilitación del servicio ntp

   # Habilite la autenticación NTP en el conmutador A. Configure una clave de autenticación NTP, con el ID de clave 88 y el valor de clave 123456. Ingrese la clave en texto sin formato y especifíquela como clave confiable.

[SwitchA] Habilitación de autenticación de servicio ntp

[SwitchA] ntp-service autenticación-keyid 88 modo de autenticación md5 simple 123456 [SwitchA] ntp-service autenticación-keyid confiable 88

Configure el conmutador A para que funcione en modo de cliente de transmisión NTP y reciba mensajes de transmisión NTP en la interfaz VLAN 2.

[SwitchA] interfaz vlan-interface 2 [SwitchA-Vlan-interface2] cliente de

transmisión de servicio ntp

3. Configurar el interruptor B:

Habilite el servicio NTP.

<SwitchB> vista del sistema

[SwitchB] habilitación del servicio ntp

Habilite la autenticación NTP en el Switch B. Configure una clave de autenticación NTP, con el ID de clave 88 y el valor de clave 123456. Ingrese la clave en texto sin formato y especifíquela como clave confiable.

[SwitchB] Habilitación de autenticación de servicio ntp

[SwitchB] ntp-service autenticación-keyid 88 modo de autenticación md5 simple 123456 [SwitchB] ntp-service autenticación-keyid confiable 88

Configure el Switch B para operar en modo de cliente de transmisión y recibir mensajes de transmisión NTP en la interfaz VLAN 2.

[SwitchB] interfaz vlan-interface 2 [SwitchB-Vlan-interface2] cliente de

transmisión de servicio ntp

4. Configurar el interruptor C:

Habilite el servicio NTP.

<SwitchC> vista del sistema

[SwitchC] habilitación del servicio ntp

Especifique el reloj local como fuente de referencia, con el nivel de estrato 3.

[SwitchC] servicio ntp refclock-master 3

Configure el conmutador C para que funcione en modo de servidor de transmisión NTP y use la interfaz VLAN 2 para enviar paquetes de transmisión NTP.

[SwitchC] interfaz vlan-interface 2 [SwitchC-Vlan-interface2] servidor de

transmisión de servicio ntp [SwitchC-Vlan-interface2] salir

5. Verifique la configuración:

La autenticación NTP está habilitada en el Switch A y el Switch B, pero no en el Switch C, por lo que el Switch A y el Switch B no pueden sincronizar sus relojes locales con el Switch C.

Verifique que el Switch B no se haya sincronizado con el Switch C.

[SwitchB-Vlan-interface2] muestra el estado del servicio ntp

Reloj estado: no sincronizado

Reloj estrato: dieciséis

ID del reloj de referencia: ninguno

6. Habilite la autenticación NTP en el Switch C:

Habilite la autenticación NTP en el Switch C. Configure una clave de autenticación NTP, con el ID de clave 88 y el valor de clave 123456. Ingrese la clave en texto sin formato y especifíquela como clave confiable.

[SwitchC] habilitar la autenticación del servicio ntp

[SwitchC] ntp-service autenticación-keyid 88 modo de autenticación md5 simple 123456 [SwitchC] ntp-service autenticación-keyid confiable 88

Especifique el conmutador C como servidor de transmisión NTP y asocie la clave 88 con el conmutador C.

[SwitchC] interfaz vlan-interfaz 2

[SwitchC-Vlan-interface2] ID de clave de autenticación del servidor de transmisión de servicio ntp 88

7. Verifique la configuración:

Verifique que el Switch B se haya sincronizado con el Switch C y que el nivel del estrato del reloj sea 4 en el Switch B y 3 en el Switch C.

[SwitchB-Vlan-interface2] muestra el estado del servicio ntp

Reloj estado: sincronizado

Reloj estrato: 4

Par del sistema: 3.0.1.31

Modo local: bcliente

ID del reloj de referencia: 3.0.1.31

Indicador de salto: 00

Fluctuación del reloj: 0,006683 s

Estabilidad: 0,000 pps

Precisión del reloj: 2^-18

Retardo de raíz: 0,00127 ms Dispersión de

raíz: 2,89877 ms Tiempo de referencia:

d0d287a7.3119666f Se sentó, Ene 8 2011 6:50:15.191

Verifique que se haya establecido una asociación NTP IPv4 entre el Switch B y el Switch C.

[SwitchB-Vlan-interface2] muestra sesiones de servicio ntp

	fuente	referencia	encuesta de alcance de Stra	ahora compensado retraso disper
**********				
* *	[1245]3.0.1.31	127.127.1.0	3	3 64 68 -0,0 0,0000 0,0

Notas: 1 fuente (maestro), 2 fuentes (pares), 3 seleccionadas, 4 candidatas, 5 configuradas.

Sesiones totales: 1

Configurar SNTP

SNTP es una versión simplificada de NTP solo para cliente especificada en RFC 4330. SNTP solo admite el modo cliente/servidor. Un dispositivo habilitado para SNTP puede recibir hora de servidores NTP, pero no puede proporcionar servicios de hora a otros dispositivos.

SNTP utiliza el mismo formato de paquete y procedimiento de intercambio de paquetes que NTP, pero proporciona una sincronización más rápida a costa de la precisión del tiempo.

Si especifica varios servidores NTP para un cliente SNTP, se selecciona el servidor con el mejor estrato. Si hay varios servidores en el mismo estrato, se selecciona el servidor NTP cuyo paquete de tiempo se recibe por primera vez.

Restricciones y pautas de configuración

Cuando configure SNTP, siga estas restricciones y pautas:

- No puede configurar NTP y SNTP en el mismo dispositivo.
- Asegúrate de utilizar el**protocolo de reloj**comando para especificar el protocolo de tiempo como NTP.

Lista de tareas de configuración

Tareas de un vistazo
(Requerido.)Habilitar el servicio SNTP
(Requerido.)Especificación de un servidor NTP para el dispositivo
(Opcional.)Configurar la autenticación SNTP

Habilitar el servicio SNTP

El servicio NTP y el servicio SNTP son mutuamente excluyentes. Sólo puede habilitar el servicio NTP o el servicio SNTP a la vez.

Para habilitar el servicio SNTP:

Paso	Dominio	Observaciones
75. Ingrese a la vista del sistema.	**vista del sistema**	N / A
76. Habilite el servicio SNTP.	**habilitar sntp**	De forma predeterminada, el servicio SNTP no está habilitado.

Especificación de un servidor NTP para el dispositivo

Paso	Dominio	Observaciones
77. Ingrese a la vista del sistema.	**vista del sistema**	N / A

Paso	Dominio	Observaciones
78. Especifique un servidor NTP para el dispositivo.	- Para IPv4: **servidor de unidifusión sntp** {*nombre del servidor*|*dirección IP*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*| **fuente***Tipo de interfaz número de interfaz*|**versión** *número*] * - Para IPv6: **Servidor de unidifusión sntp ipv6** {*nombre del servidor*|*dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] [**ID de clave de autenticación***ID de clave*| **fuente***Tipo de interfaz número de interfaz*] *	De forma predeterminada, no se especifica ningún servidor NTP para el dispositivo. Repita este paso para especificar varios servidores NTP. Para utilizar la autenticación, debe especificar el**ID de clave de autenticación** *ID de clave*opción.

Para utilizar un servidor NTP como fuente de hora, asegúrese de que su reloj esté sincronizado. Si el nivel de estrato del servidor NTP es mayor o igual que el del cliente, el cliente no se sincroniza con el servidor NTP.

Configurar la autenticación SNTP

La autenticación SNTP garantiza que un cliente SNTP esté sincronizado únicamente con un servidor NTP confiable y autenticado.

Siga estas pautas cuando configure la autenticación SNTP:

- Habilite la autenticación tanto en el servidor NTP como en el cliente SNTP.
- Configure el cliente SNTP con el mismo ID de clave de autenticación y valor de clave que el servidor NTP, y especifique la clave como clave confiable tanto en el servidor NTP como en el cliente SNTP. Para obtener información sobre cómo configurar la autenticación NTP en un servidor NTP, consulte "Configurando NTP".
- Asocie la clave especificada con un servidor NTP en el cliente SNTP.

Con la autenticación deshabilitada, el cliente SNTP puede sincronizarse con el servidor NTP independientemente de si el servidor NTP está habilitado con autenticación.

Para configurar la autenticación SNTP en el cliente SNTP:

Paso	Dominio	Observaciones
79. Ingrese a la vista del sistema.	**vista del sistema**	N / A
80. Habilite la autenticación SNTP.	**habilitar la autenticación SNTP**	De forma predeterminada, la autenticación SNTP está deshabilitada.
81. Configure una clave de autenticación SNTP.	**ID de clave de autenticación SNTP***ID de clave* **modo de autenticación md5** {**cifrar**|**simple**}*valor*	De forma predeterminada, no se configura ninguna clave de autenticación SNTP.
82. Especifique la clave como clave confiable.	**SNTP confiable** **ID de clave de autenticación***ID de clave*	De forma predeterminada, no se especifica ninguna clave confiable.

Paso	Dominio	Observaciones
83. Asocie la clave de autenticación SNTP con un servidor NTP.	- Para IPv4: **servidor de unidifusión sntp** {*nombre del servidor*| *dirección IP* } [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave* - Para IPv6: **Servidor de unidifusión sntp ipv6** { *nombre del servidor*| *dirección ipv6*} [**instancia-vpn** *nombre-instancia-vpn*] **ID de clave de autenticación***ID de clave*	De forma predeterminada, no se especifica ningún servidor NTP.

Visualización y mantenimiento de SNTP

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Muestra información sobre todas las asociaciones SNTP IPv6.	**mostrar sesiones sntp ipv6**
Muestra información sobre todas las asociaciones SNTP IPv4.	**mostrar sesiones sntp**

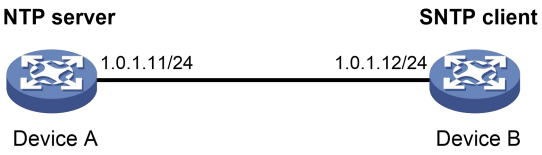
Ejemplo de configuración SNTP

Requisitos de red

Como se muestra enFigura 14, realice las siguientes tareas:

- Configure el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2. Configure el Dispositivo
- B para que funcione en modo de cliente SNTP y especifique el Dispositivo A como servidor NTP. Configure la
- autenticación NTP en el dispositivo A y la autenticación SNTP en el dispositivo B.

Figura 50 Diagrama de red



Procedimiento de configuración

1. Asigne una dirección IP a cada interfaz y asegúrese de que el dispositivo A y el dispositivo B puedan comunicarse entre sí, como se muestra enFigura 14. (No se muestran detalles).
2. Configurar el dispositivo A:

   # Habilite el servicio NTP.

   <DispositivoA> vista del sistema

   [DispositivoA] habilitación del servicio ntp

   # Configurar el reloj local del Dispositivo A como fuente de referencia, con el nivel de estrato 2.

   [DispositivoA] ntp-service refclock-master 2

   # Habilite la autenticación NTP en el dispositivo A.

   [DispositivoA] habilitación de autenticación de servicio ntp

Configure una clave de autenticación NTP, con el ID de clave de**10**y valor clave de**una buena llave**. Ingrese la clave en texto plano.

[DispositivoA] ID de clave de autenticación de servicio ntp 10 modo de autenticación md5 simple aNiceKey

Especifique la clave como clave confiable.

[DispositivoA] ntp-service autenticación confiable-keyid 10

3. Configurar el dispositivo B:

Habilite el servicio SNTP.

<DispositivoB> vista del sistema

[DispositivoB] sntp habilitado

Habilite la autenticación SNTP en el dispositivo B.

[DispositivoB] habilitación de autenticación SNTP

Configure una clave de autenticación SNTP, con el ID de clave de**10**y valor clave de**una buena llave**. Ingrese la clave en texto plano.

[DispositivoB] ID de clave de autenticación sntp 10 modo de autenticación md5 simple aNiceKey

Especifique la clave como clave confiable.

[DispositivoB] sntp autenticación confiable-keyid 10

Especifique el Dispositivo A como el servidor NTP del Dispositivo B y asocie el servidor con la clave 10.

[DispositivoB] sntp unicast-server 1.0.1.11 ID de clave de autenticación 10

4. Verifique la configuración:

Verifique que se haya establecido una asociación SNTP entre el dispositivo B y el dispositivo A, y que el dispositivo B se haya sincronizado con el dispositivo A.

[DispositivoB] muestra sesiones sntp

servidor NTP	Estrato	Versión	Última hora de recepción
1.0.1.11	2	4	Martes, 17 de mayo de 2011 9:11:20.833 (sincronizado)

contenido

Configurando RMON

Descripción general

La supervisión remota de red (RMON) es una mejora de SNMP. Permite la supervisión y gestión remota proactiva de dispositivos y subredes de red. Un monitor RMON recopila periódica o continuamente estadísticas de tráfico para la red conectada a un puerto en el dispositivo administrado. El dispositivo administrado puede enviar automáticamente una notificación cuando una estadística cruza un umbral de alarma, por lo que el NMS no necesita sondear constantemente las variables MIB y comparar los resultados.

RMON utiliza notificaciones SNMP para notificar a los NMS sobre diversas condiciones de alarma, como la superación del umbral de tráfico de transmisión. Por el contrario, SNMP informa cambios en el estado operativo de la función y la interfaz, como enlace activo, enlace inactivo y falla del módulo. Para obtener más información sobre las notificaciones SNMP, consulte "Configuración de SNMP".

Los dispositivos Dahua proporcionan un agente RMON integrado como monitor RMON. Un NMS puede realizar operaciones SNMP básicas para acceder a la MIB RMON.

Grupos RMON

Entre los grupos RMON estándar, Dahua implementa el grupo de estadísticas, el grupo de historial, el grupo de eventos, el grupo de alarmas, el grupo de configuración de sondas y el grupo de historial de usuarios. Dahua también implementa un grupo de alarma privado, que mejora el grupo de alarma estándar. El grupo de configuración de la sonda y el grupo de historial de usuario no se pueden configurar desde la CLI. Para configurar estos dos grupos, debe acceder a la MIB. Para obtener más información sobre la configuración de MIB para RMON, consulte*Compañero MIB de la plataforma Comware 7*.

Grupo de estadísticas

El grupo de estadísticas muestra estadísticas de tráfico para interfaces Ethernet monitoreadas y almacena las estadísticas en la tabla de estadísticas de Ethernet (ethernetStatsTable). Las estadísticas incluyen:

- Número de colisiones.
- Errores de alineación del CRC.
- Número de paquetes de tamaño insuficiente o excesivo.
- Número de transmisiones.
- Número de multidifusiones.
- Número de bytes recibidos.
- Número de paquetes recibidos.

Las estadísticas de la tabla de estadísticas de Ethernet son sumas acumulativas.

grupo de historia

El grupo de historial toma muestras periódicamente de las estadísticas de tráfico en las interfaces y guarda las muestras del historial en la tabla de historial (etherHistoryTable). Las estadísticas incluyen:

- Utilización del ancho de banda.
- Número de paquetes de error.
- Número total de paquetes.

La tabla de historial almacena las estadísticas de tráfico recopiladas para cada intervalo de muestreo.

grupo de eventos

El grupo de eventos controla la generación y notificaciones de eventos activados por las alarmas definidas en el grupo de alarmas y en el grupo de alarmas privadas. Los siguientes son métodos de manejo de eventos de alarma RMON:

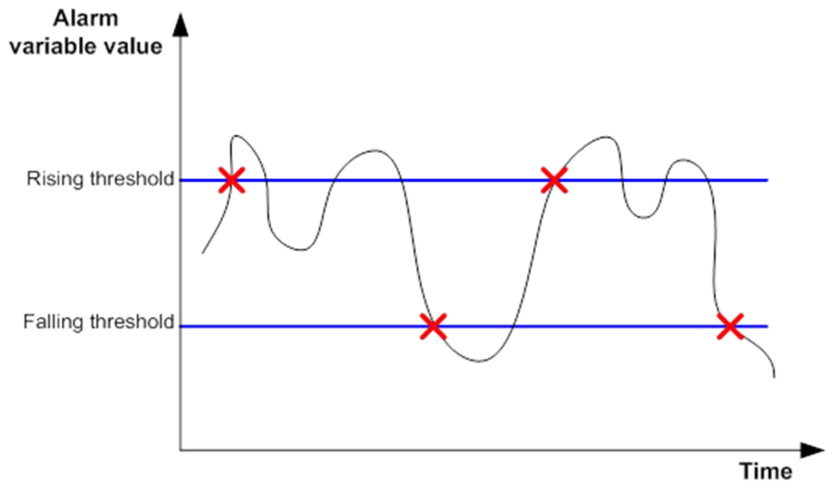
- **Registro**: registra información del evento (incluida la hora y la descripción del evento) en la tabla de registro de eventos para que el dispositivo de administración pueda obtener los registros a través de SNMP.
- **Trampa**—Envía una notificación SNMP cuando ocurre el evento.
- **Trampa de troncos**: registra información del evento en la tabla de registro de eventos y envía una notificación SNMP cuando ocurre el evento.
- **Ninguno**—No realiza ninguna acción.

grupo de alarma

El grupo de alarmas RMON monitorea variables de alarma, como el recuento de paquetes entrantes (etherStatsPkts) en una interfaz. Después de crear una entrada de alarma, el agente RMON toma muestras del valor de la variable de alarma monitoreada periódicamente. Si el valor de la variable monitoreada es mayor o igual que el umbral ascendente, se activa un evento de alarma ascendente. Si el valor de la variable monitoreada es menor o igual que el umbral de caída, se activa un evento de alarma de caída. El grupo de eventos define la acción a tomar ante el evento de alarma.

Si una entrada de alarma cruza un umbral varias veces seguidas, el agente RMON genera un evento de alarma solo para el primer cruce. Por ejemplo, si el valor de una variable de alarma muestreada cruza el umbral ascendente varias veces antes de cruzar el umbral descendente, solo el primer cruce desencadena un evento de alarma ascendente, como se muestra enFigura 1.

Figura 51 Eventos de alarma ascendentes y descendentes



grupo de alarma privado

El grupo de alarma privado le permite realizar operaciones matemáticas básicas en múltiples variables y comparar el resultado del cálculo con los umbrales ascendentes y descendentes.

El agente RMON toma muestras de variables y realiza una acción de alarma basada en una entrada de alarma privada de la siguiente manera:

1. Muestra las variables de alarma privadas en la fórmula definida por el usuario.
2. Procesa los valores muestreados con la fórmula.
3. Compara el resultado del cálculo con los umbrales predefinidos y luego realiza una de las siguientes acciones:
   - Activa el evento asociado al evento de alarma ascendente si el resultado es igual o mayor que el umbral ascendente.
   - Activa el evento asociado al evento de alarma de caída si el resultado es igual o menor que el umbral de caída.

Si una entrada de alarma privada cruza un umbral varias veces seguidas, el agente RMON genera un evento de alarma solo para el primer cruce. Por ejemplo, si el valor de una variable de alarma muestreada cruza el umbral ascendente varias veces antes de cruzar el umbral descendente, solo el primer cruce desencadena un evento de alarma ascendente.

Tipos de muestra para el grupo de alarma y el grupo de alarma privado

El agente RMON admite los siguientes tipos de muestra:

- **absoluto**—RMON compara el valor de la variable monitoreada con los umbrales ascendentes y descendentes al final del intervalo de muestreo.
- **delta**—RMON resta el valor de la variable monitoreada en la muestra anterior del valor actual y luego compara la diferencia con los umbrales ascendentes y descendentes.

Protocolos y estándares

- RFC 4502,*Base de información de gestión de monitoreo remoto de red versión 2*
- RFC 2819,*Base de Información de Gestión de Monitoreo Remoto de Red Estado de este Memo*

Configuración de la función de estadísticas RMON

RMON implementa la función de estadísticas a través del grupo de estadísticas de Ethernet y el grupo de historial. La función de estadísticas está disponible solo para interfaces Ethernet de Capa 2 y Capa 3.

El grupo de estadísticas de Ethernet proporciona la estadística acumulativa de una variable desde el momento en que se crea la entrada de estadísticas hasta el momento actual. Para obtener más información sobre la configuración, consulte "Creación de una entrada de estadísticas de Ethernet RMON".

El grupo de historial proporciona estadísticas que se muestrean para una variable para cada intervalo de muestreo. El grupo de historial utiliza la tabla de control de historial para controlar el muestreo y almacena muestras en la tabla de historial. Para obtener más información sobre la configuración, consulte "Crear una entrada de control de historial RMON".

Creación de una entrada de estadísticas de Ethernet RMON

Paso	Dominio	Observaciones
84. Ingresar al sistema vista.	**vista del sistema**	N / A
85. Ingrese a Ethernet vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
86. Cree una entrada para la interfaz en el RMON estadísticas mesa.	**estadísticas de rmon***entrada-número* [**dueño***texto*]	De forma predeterminada, la tabla de estadísticas de RMON no contiene entradas. Puede crear una entrada de estadísticas para cada interfaz Ethernet y un máximo de 100 entradas de estadísticas en el dispositivo. Una vez alcanzado el límite de entradas, no podrá agregar nuevas entradas.

Crear una entrada de control de historial RMON

Puede configurar varias entradas de control de historial para una interfaz, pero debe asegurarse de que sus números de entrada e intervalos de muestreo sean diferentes.

Puede crear una entrada de control de historial correctamente incluso si el tamaño del depósito especificado excede el tamaño de la tabla de historial disponible. RMON establecerá el tamaño del depósito lo más cerca posible del tamaño esperado del depósito.

Para crear una entrada de control de historial RMON:

Traducido del inglés al español - www.onlinedoctranslator.com

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a Ethernet vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
3. Cree una entrada para la interfaz en el historial de RMON mesa de control.	**historia humana***entrada-número* **cubos***número***intervalo** *muestreo-intervalo*[**dueño***texto*]	De forma predeterminada, la tabla de control del historial de RMON no contiene entradas. Puede crear un máximo de 100 entradas de control de historial.

Configuración de la función de alarma RMON

Cuando configure la función de alarma RMON, siga estas pautas:

- Antes de poder crear entradas de alarma RMON, debe habilitar el agente SNMP.
- Para enviar notificaciones al NMS cuando se activa una alarma, configure el agente SNMP como se describe en "Configuración de SNMP" antes de configurar la función de alarma RMON.
- Para crear un nuevo evento, alarma o entrada de alarma privada:
  - La entrada no debe tener el mismo conjunto de parámetros que una entrada
  - existente. No se alcanza el número máximo de entradas.

tabla 1muestra los parámetros que se compararán para la duplicación y los límites de entrada.

Tabla 13 Restricciones de configuración de RMON

Entrada	Parámetros a comparar	Máximo número de entradas
Evento	- Descripción del evento (**descripción***cadena*) Tipo de evento (- **registro**,**trampa**,**trampa de troncos**, o**ninguno**) Nombre de - la comunidad (*cadena de seguridad*)	60
Alarma	- Variable de alarma (*variable de alarma*) - Intervalo de muestreo (*intervalo de* - *muestreo*) Tipo de ejemplo (**absoluto**o**delta**) - Umbral ascendente (*valor umbral1*) Umbral - descendente (*valor-umbral2*)	60
alarma privada	- Fórmula de variable de alarma (*fórmula-prialarma* -) Intervalo de muestreo (*intervalo de muestreo*) - Tipo de ejemplo (**absoluto**o**delta**) Umbral - ascendente (*valor umbral1*) Umbral descendente (- *valor-umbral2*)	50

Para configurar la función de alarma RMON:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. (Opcional). Cree un entrada de evento en la tabla de eventos.	**evento común***entrada-número*[**descripción***cadena*] {**registro** | **trampa de troncos***cadena de seguridad*| **ninguno**| **trampa** *cadena de seguridad*} [**dueño***texto*]	De forma predeterminada, la tabla de eventos RMON no contiene entradas.

Paso	Dominio	Observaciones
3. Cree una entrada en la tabla de alarmas o tabla de alarmas privada.	- Cree una entrada en la tabla de alarmas: **alarma común** *número-de-entrada variable-alarma intervalo-muestreo*{ **absoluto**|**delta**} [**alarma de inicio**{**descendente**| **creciente**| **aumento de la caída**}]**umbral ascendente** *valor-umbral1 entrada-evento1***umbral descendente** *valor-umbral2 entrada-evento2*[**dueño***texto*] - Cree una entrada en la tabla de alarmas privadas: **alarma primaria rmon***número de entrada fórmula-prialarm prialarm-des intervalo-muestreo*{**absoluto**| **delta**} [**alarma de inicio**{ **cayendo | en aumento | aumento de la caída**}]**umbral ascendente** *valor-umbral1 entrada-evento1***umbral descendente** *valor-umbral2 entrada-evento2***tipo de entrada** { **para siempre**|**ciclo***período de ciclo*} [**dueño***texto*]	De forma predeterminada, la tabla de alarmas RMON y la tabla de alarmas privadas no contienen entradas. Puede asociar una alarma a un evento que aún no se ha creado. El La alarma activará el evento solo después de que se cree el evento.

Visualización y mantenimiento de la configuración de RMON

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Mostrar estadísticas de RMON.	**mostrar estadísticas comunes**[*tipo de interfaz número de interfaz*]
Muestra entradas de control de historial de RMON y muestras de historial.	**mostrar el historial de rmon**[*tipo de interfaz número de interfaz*]
Muestra las entradas de alarma RMON.	**mostrar alarma común**[*número de entrada*]
Muestra las entradas de alarmas privadas RMON.	**mostrar alarma primaria rmon**[*número de entrada*]
Mostrar entradas de eventos RMON.	**mostrar evento común**[*número de entrada*]
Muestra información de registro para entradas de eventos.	**mostrar registro de eventos rmon**[*número de entrada*]

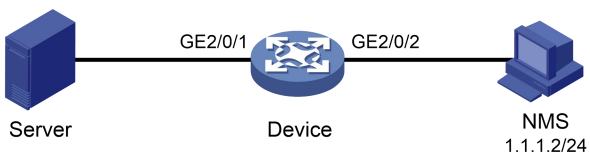
Ejemplos de configuración de RMON

Ejemplo de configuración del grupo de estadísticas de Ethernet

Requisitos de red

Como se muestra enFigura 2, cree una entrada de estadísticas de Ethernet RMON en el dispositivo para recopilar estadísticas de tráfico acumuladas para GigabitEthernet 2/0/1.

Figura 52 Diagrama de red



Procedimiento de configuración

Cree una entrada de estadísticas de Ethernet RMON para GigabitEthernet 2/0/1.

<nombre del sistema> vista del sistema

[Nombre del sistema] interfaz gigabitethernet 2/0/1 [Nombre del sistema-GigabitEthernet2/0/1] estadísticas rmon 1 propietario usuario1

Mostrar estadísticas recopiladas para GigabitEthernet 2/0/1.

<Nombre del sistema> muestra estadísticas de rmon gigabitethernet 2/0/1

EtherStatsEntry 1 propiedad del usuario1 es VÁLIDA.

Interfaz: GigabitEthernet2/0/1<ifIndex.3> etherStatsOctets : 21657 , etherStatsPkts : 307

etherStatsBroadcastPkts : 56 , etherStatsMulticastPkts : 34

etherStatsUndersizePkts : 0 , etherStatsOversizePkts : 0

etherStatsFragmentos : 0 , etherStatsJabbers : 0

etherStatsCRCAlignErrors: 0 etherStatsDropEvents, (eth : 0 etherStatsColisiones : 0

insuficientes): 0 Paquetes entrantes por tamaño:

64 : 235 , 65-127: 67 , 128-255 : 4

256-511: 1 , 512-1023: 0 , 1024-1518: 0

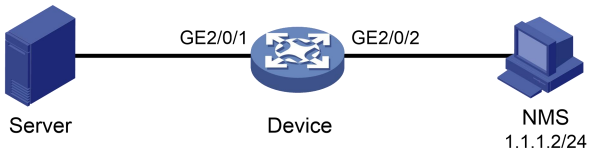
Obtener las estadísticas de tráfico del NMS a través de SNMP. (No se muestran detalles).

Ejemplo de configuración del grupo de historial

Requisitos de red

Como se muestra enfigura 3, cree una entrada de control de historial RMON en el dispositivo para muestrear las estadísticas de tráfico de GigabitEthernet 2/0/1 cada minuto.

Figura 53 Diagrama de red



Procedimiento de configuración

Cree una entrada de control del historial RMON para muestrear las estadísticas de tráfico cada minuto para GigabitEthernet 2/0/1. Conserve un máximo de ocho muestras para la interfaz en la tabla de estadísticas del historial.

<nombre del sistema> vista del sistema

[Nombre del sistema] interfaz gigabitethernet 2/0/1

[Sysname-GigabitEthernet2/0/1] historial de rmon 1 depósitos 8 intervalo 60 propietario usuario1

Muestra las estadísticas del historial recopiladas para GigabitEthernet 2/0/1.

[Sysname-GigabitEthernet2/0/1] muestra el historial de rmon

HistoryControlEntry 1 propiedad del usuario1 es VÁLIDO

Interfaz muestreada : GigabitEthernet2/0/1<ifIndex.3> : 60(seg)

Intervalo de muestreo con 8 depósitos como máximo

Registro de muestreo 1:

eventos de caída : 0 , octetos : 834

paquetes : 8 , transmisión paquetes : 1

paquetes de multidifusión: 6 , errores de alineación CRC: 0

paquetes de tamaño , paquetes de gran tamaño : 0

insuficiente: 0 fragmentos : 0 , parloteos : 0

colisiones : 0 , utilización : 0

Registro de muestreo 2:

eventos de caída : 0 , octetos : 962

paquetes : 10 , paquetes de difusión : 3

paquetes de multidifusión: 6 , errores de alineación CRC: 0

paquetes de tamaño , paquetes de gran tamaño : 0

insuficiente: 0 fragmentos : 0 , parloteos : 0

colisiones : 0 , utilización : 0

Registro de muestreo 3:

eventos de caída : 0 , octetos : 830

paquetes : 8 , paquetes de difusión : 0

paquetes de multidifusión: 6 , errores de alineación CRC: 0

paquetes de tamaño , paquetes de gran tamaño : 0

insuficiente: 0 fragmentos : 0 , parloteos : 0

colisiones : 0 , utilización : 0

Registro de muestreo 4:

eventos de caída : 0 , octetos : 933

paquetes : 8 , paquetes de difusión : 0

paquetes de multidifusión: 7 , errores de alineación CRC: 0

paquetes de tamaño , paquetes de gran tamaño : 0

insuficiente: 0 fragmentos : 0 , parloteos : 0

colisiones : 0 , utilización : 0

Registro de muestreo 5:

eventos de caída : 0 , octetos : 898

paquetes : 9 , paquetes de difusión : 2

paquetes de multidifusión: 6 , errores de alineación CRC: 0

paquetes de tamaño , paquetes de gran tamaño : 0

insuficiente: 0 fragmentos : 0 , parloteos : 0

colisiones : 0 , utilización : 0

Registro de muestreo 6:

eventos de caída : 0 , octetos : 898

paquetes : 9 , paquetes de difusión : 2

paquetes de multidifusión: 6 , errores de alineación CRC: 0

paquetes de tamaño , paquetes de gran tamaño : 0

insuficiente: 0 fragmentos : 0 , parloteos : 0

colisiones : 0 , utilización : 0

Registro de muestreo 7:

eventos de caída : 0 , octetos : 766

paquetes : 7 , paquetes de difusión : 0

paquetes de multidifusión: 6 , errores de alineación CRC: 0

paquetes de tamaño , paquetes de gran tamaño : 0

insuficiente: 0 fragmentos : 0 , parloteos : 0

colisiones : 0 , utilización : 0

Registro de muestreo 8:

eventos de caída : 0 , octetos : 1154

paquetes : 13 , paquetes de difusión : 1

paquetes de multidifusión: 6 , errores de alineación CRC: 0

paquetes de tamaño insuficiente: 0 , paquetes de gran tamaño : 0

fragmentos	: 0	, parloteos	: 0
colisiones	: 0	, utilización	: 0

Obtener las estadísticas de tráfico del NMS a través de SNMP. (No se muestran detalles).

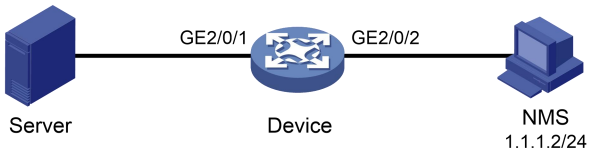
Ejemplo de configuración de la función de alarma

Requisitos de red

Como se muestra enFigura 4, configure el dispositivo para monitorear las estadísticas de tráfico entrante en GigabitEthernet 2/0/1 y envíe alarmas RMON cuando ocurran los siguientes eventos:

- La muestra delta de 5 segundos para la estadística de tráfico cruza el umbral ascendente (100). La muestra
- delta de 5 segundos para la estadística de tráfico cae por debajo del umbral de caída (50).

Figura 54 Diagrama de red



Procedimiento de configuración

Configure el agente SNMP (el dispositivo) con la misma configuración SNMP que el NMS en 1.1.1.2. Este ejemplo utiliza SNMPv1, comunidad de lectura**público**y escribe comunidad**privado**.

```
<nombre del sistema> vista del sistema
[Nombre del sistema] agente-snmp
[Nombre del sistema] comunidad snmp-agent lectura pública [Nombre
del sistema] comunidad de agente snmp escritura privada [Nombre del
sistema] snmp-agent sys-info versión v1 [Nombre del sistema]
habilitación de trampa de agente snmp
[Nombre del sistema] registro de captura del agente snmp
[Nombre del sistema] agente snmp dirección de captura de host-destino dominio-udp 1.1.1.2 parámetros nombre de seguridad
público
```

Cree una entrada de estadísticas de Ethernet RMON para GigabitEthernet 2/0/1.

```
[Nombre del sistema] interfaz gigabitethernet 2/0/1 [Nombre del sistema-
GigabitEthernet2/0/1] estadísticas rmon 1 propietario usuario1 [Nombre del sistema-
GigabitEthernet2/0/1] salir
```

Cree una entrada de evento RMON y una entrada de alarma RMON para enviar notificaciones SNMP cuando la muestra delta para 1.3.6.1.2.1.16.1.1.1.4.1 exceda 100 o caiga por debajo de 50.

```
[Nombre del sistema] rmon evento 1 trampa propietario público usuario1
[Nombre del sistema] alarma rmon 1 1.3.6.1.2.1.16.1.1.1.4.1 5 umbral ascendente delta 100 1 umbral
descendente 50 1 usuario propietario1
```

NOTA:

La cadena 1.3.6.1.2.1.16.1.1.1.4.1 es la instancia del objeto para GigabitEthernet 2/0/1. Los dígitos antes del último dígito (1.3.6.1.2.1.16.1.1.1.4) representan el objeto de las estadísticas de tráfico entrante total. El último dígito (1) es el índice de entrada de estadísticas de Ethernet RMON para GigabitEthernet 2/0/1.

Muestra la entrada de alarma RMON.

```
<Nombre del sistema> muestra la alarma rmon 1 La entrada
de alarma 1 propiedad del usuario1 es VÁLIDA.
```

Tipo de ejemplo : delta
variable muestreada : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
Intervalo de muestreo (en segundos) : 5
Umbral ascendente : 100 (asociado con el evento 1) : 50
Umbral descendente (asociado con el evento 1)
Alarma enviada al iniciar la entrada : alarma en ascenso o en descenso
Último valor : 0

Mostrar estadísticas para GigabitEthernet 2/0/1.

<Nombre del sistema> muestra estadísticas de rmon gigabitethernet 2/0/1
EtherStatsEntry 1 propiedad del usuario1 es VÁLIDA.
Interfaz: GigabitEthernet2/0/1<ifIndex.3> etherStatsOctets
: 57329 , etherStatsPkts : 455
etherStatsBroadcastPkts : 53 , etherStatsMulticastPkts : 353
etherStatsUndersizePkts : 0 , etherStatsOversizePkts : 0
etherStatsFragmentos : 0 , etherStatsJabbers : 0
etherStatsCRCAlignErrors: 0 etherStatsDropEvents, (etherStatsColisiones : 0
insuficientes): 0 Paquetes entrantes por tamaño:

64 : 7 , 65-127: 413 , 128-255 : 35
256-511: 0 , 512-1023: 0 , 1024-1518: 0

Consultar eventos de alarma en el NMS. (No se muestran detalles).

En el dispositivo, los mensajes de eventos de alarma se muestran cuando ocurren eventos. El siguiente es un mensaje de evento de alarma de ejemplo:

[Nombre del sistema] % 6 de abril 09:23:53:357 2013 nombre del sistema SNMP/6/SNMP_NOTIFY: Notificación cayendo Una alarma (1.3.6.1.2.1.16.0.2) con índice de alarma (1.3.6.1.2.1.16.3.1.1.1.1) =1;alarmVariable(1.3.6.1.2.1.16.3.1.1.3.1)=1.3.6.1.2.1.16.1.1.1.4.1;alarmSampleType(1.3.6.1.2. 1.16.3.1.1.4.1)=2; alarmValue(1.3.6.1.2.1.16.3.1.1.5.1)=0;alarmFallingThreshold(1 . 3.6.1.2.1.16.3.1.1.8.1)=50.

Contenido

Configuración de EEA

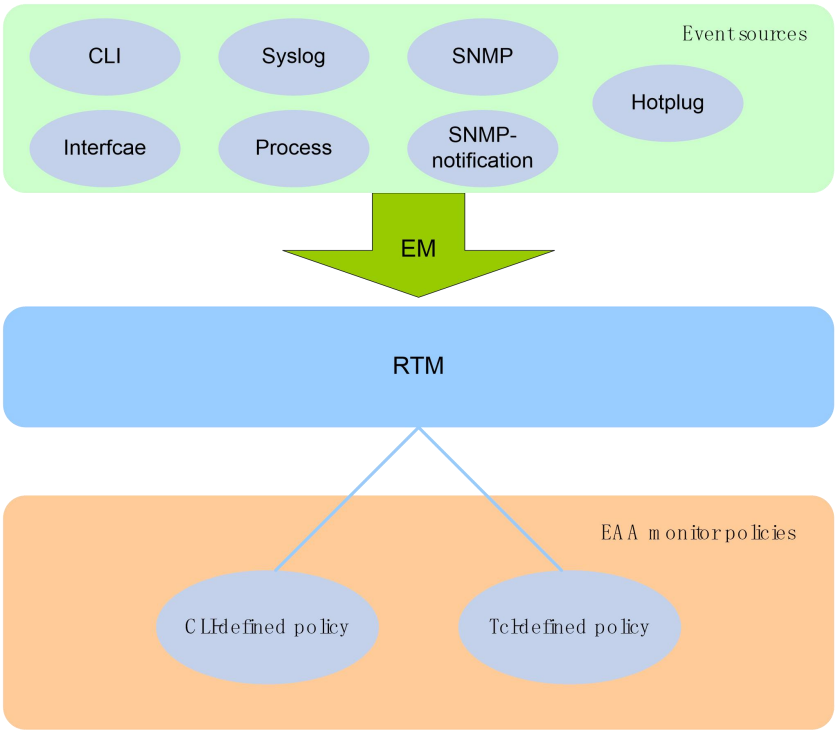
Descripción general

La arquitectura de automatización integrada (EAA) es un marco de monitoreo que le permite autodefinir eventos monitoreados y acciones a tomar en respuesta a un evento. Le permite crear políticas de monitorización mediante el uso de scripts CLI o Tcl.

Marco del EEA

El marco EAA incluye un conjunto de fuentes de eventos, un conjunto de monitores de eventos, un administrador de eventos en tiempo real (RTM) y un conjunto de políticas de monitorización definidas por el usuario, como se muestra enFigura 1.

Figura 55 Marco EAA



Fuentes de eventos

Las fuentes de eventos son módulos de software o hardware que activan eventos (consulteFigura 1).

Por ejemplo, el módulo CLI desencadena un evento cuando ingresa un comando. El módulo Syslog (el centro de información) desencadena un evento cuando recibe un mensaje de registro.

Monitores de eventos

EAA crea un monitor de eventos para una política de monitorización para monitorear el sistema en busca del evento especificado en cada política. Un monitor de eventos notifica al RTM que ejecute la política de monitor cuando ocurre el evento monitoreado.

RTM

RTM gestiona la creación, la máquina de estado y la ejecución de políticas de monitorización.

Políticas de seguimiento de la EAA

Una política de monitor especifica el evento a monitorear y las acciones a tomar cuando ocurre el evento.

Puede configurar las políticas de monitorización de EAA mediante CLI o Tcl.

Una política de monitor contiene los siguientes elementos:

- Un evento.
- Un mínimo de una acción. Un mínimo
- de un rol de usuario. Una
- configuración de tiempo de ejecución.

Para obtener más información sobre estos elementos, consulte "Elementos de una política de monitorización".

Elementos de una política de monitorización

Evento

tabla 1muestra los tipos de eventos que EAA puede monitorear.

Tabla 14 Eventos monitoreados

Tipo de evento	Descripción
CLI	El evento CLI ocurre en respuesta a operaciones monitoreadas realizadas en la CLI. Por ejemplo, se ingresa un comando, se ingresa un signo de interrogación (?) o el**Pestaña**Se presiona la tecla para completar un comando.
registro del sistema	El evento Syslog ocurre cuando el centro de información recibe el registro monitoreado dentro de un período específico. NOTA: El registro generado por EAA RTM no activa la ejecución de la política de monitor.
Proceso	El evento del proceso ocurre en respuesta a un cambio de estado del proceso monitoreado (como una excepción, apagado, inicio o reinicio). Tanto los cambios de estado manuales como los automáticos pueden provocar que se produzca el evento.
Conexión en caliente	El evento Hotplug ocurre cuando la tarjeta monitoreada se inserta o retira mientras el dispositivo está en funcionamiento.
Interfaz	Cada evento de interfaz está asociado con dos umbrales definidos por el usuario: inicio y reinicio. Se produce un evento de interfaz cuando la estadística de tráfico de interfaz supervisada cruza el umbral de inicio en las siguientes situaciones: - La estadística cruza por primera vez el umbral de salida. - La estadística cruza el umbral de inicio cada vez que cruza el umbral de reinicio.
SNMP	Cada evento SNMP está asociado con dos umbrales definidos por el usuario: inicio y reinicio. El evento SNMP ocurre cuando el valor de la variable MIB monitoreada cruza el umbral de inicio en las siguientes situaciones: - El valor de la variable monitorizada cruza el umbral inicial por primera vez. - El valor de la variable supervisada cruza el umbral de inicio cada vez que cruza el umbral de reinicio.
Notificación SNMP	El evento de notificación SNMP ocurre cuando el valor de la variable MIB monitoreada en una notificación SNMP coincide con la condición especificada. Por ejemplo, la tasa de tráfico de transmisión en una interfaz Ethernet alcanza o supera el 30%.

Acción

Puede crear una serie de acciones dependientes del orden para realizar en respuesta al evento especificado en la política del monitor.

Las siguientes son acciones disponibles:

- Ejecutando un comando.

- Envío de un registro.
- Habilitación de una conmutación activa/en espera.
- Ejecutar un reinicio sin guardar la configuración en ejecución.

Rol del usuario

Para que EAA ejecute una acción en una política de monitor, debe asignar a la política el rol de usuario que tiene acceso a los comandos y recursos específicos de la acción. Si EAA carece de acceso a un comando o recurso específico de una acción, EAA no realiza la acción ni todas las acciones posteriores.

Por ejemplo, una política de monitor tiene cuatro acciones numeradas del 1 al 4. La política tiene roles de usuario necesarios para realizar las acciones 1, 3 y 4. Sin embargo, no tiene el rol de usuario requerido para realizar la acción 2. Cuando la Se activa la política, EAA ejecuta solo la acción 1.

Para obtener más información sobre los roles de usuario, consulte RBAC en*Guía de configuración básica*.

Tiempo de ejecución

El tiempo de ejecución de la política limita la cantidad de tiempo que la política del monitor puede ejecutarse desde el momento en que se activa. Esta configuración evita que los recursos del sistema sean ocupados por políticas definidas incorrectamente.

Variables de entorno EAA

Las variables de entorno de EAA desacoplan la configuración de los argumentos de acción de la política del monitor para que pueda modificar una política fácilmente.

Una variable de entorno EAA se define como <*variable nombre_variable_valor*> par y se puede utilizar en diferentes pólizas. Cuando define una acción, puede ingresar un nombre de variable con un signo de dólar inicial (**ps***nombre de la variable*). EAA reemplazará el nombre de la variable con el valor de la variable cuando realice la acción.

Para cambiar el valor de un argumento de acción, modifique el valor especificado en el par de variables en lugar de editar cada política de monitor afectada.

Las variables de entorno EAA incluyen variables definidas por el sistema y variables definidas por el usuario.

Variables definidas por el sistema

Las variables definidas por el sistema se proporcionan de forma predeterminada y los usuarios no pueden crearlas, eliminarlas ni modificarlas. Los nombres de variables definidas por el sistema comienzan con un signo de subrayado (_). Los valores de las variables se establecen automáticamente según la configuración del evento en la política que utiliza las variables.

Las variables definidas por el sistema incluyen los siguientes tipos:

- **Variable pública**—Disponible para cualquier evento. **Variable específica**
- **del evento**—Disponible solo para un tipo de evento.

Tabla 2muestra todas las variables definidas por el sistema.

Tabla 15 Variables de entorno EAA definidas por el sistema por tipo de evento

Nombre de la variable	Descripción
Cualquier evento:	
_id_evento	Identificación del evento.
_tipo de evento	Tipo de evento.
_cadena_tipo_evento	Descripción del tipo de evento.
_hora del evento	Hora en que ocurre el evento.
_evento_severidad	Nivel de gravedad de un evento.
CLI:	
_cmd	Comandos que coinciden.

Nombre de la variable	Descripción
Registro del sistema:	
_syslog_pattern	Registrar el contenido del mensaje.
Conexión en caliente:	
_ranura	ID de la ranura donde se produce un evento de intercambio en caliente.
_subranura	ID de la subranura donde se produce un evento de intercambio en caliente. En la versión actual del software, el dispositivo no admite esta variable.
Interfaz:	
_ifnombre	Nombre de la interfaz.
SNMP:	
_oid	OID de la variable MIB donde se realiza una operación SNMP.
_valor_oid	Valor de la variable MIB.
Notificación SNMP:	
_oid	OID que se incluye en la notificación SNMP.
Proceso:	
_nombre del proceso	Nombre del proceso.

Variables definidas por el usuario

Puede utilizar variables definidas por el usuario para todo tipo de eventos.

Los nombres de variables definidas por el usuario pueden contener dígitos, caracteres y el signo de subrayado (_), excepto que el signo de subrayado no puede ser el carácter inicial.

Configuración de una variable de entorno EAA definida por el usuario

Configure una variable de entorno EAA definida por el usuario antes de usarla en una acción. Para

configurar una variable de entorno EAA definida por el usuario:

Paso	Dominio	Observaciones
4. Ingresar al sistema vista.	**vista del sistema**	N / A
5. Configurar un EAA definido por el usuario ambiente variable.	**entorno rtm***nombre-var valor-var*	De forma predeterminada, no se configuran variables de entorno definidas por el usuario. El sistema proporciona las variables definidas por el sistema en Tabla 2.

Configurar una política de monitorización

Puede configurar una política de monitor utilizando la CLI o Tcl.

Restricciones y pautas de configuración

Cuando configure políticas de monitor, siga estas restricciones y pautas:

- Asegúrese de que las acciones de diferentes políticas no entren en conflicto. El resultado de la ejecución de políticas será impredecible si las políticas que entran en conflicto en acciones se ejecutan simultáneamente.
- Puede asignar el mismo nombre de política a una política definida por CLI y a una política definida por Tcl. Sin embargo, no puede asignar el mismo nombre a políticas que sean del mismo tipo.
- El sistema ejecuta las acciones de una política en orden ascendente de ID de acción. Cuando agrega acciones a una política, debe asegurarse de que el orden de ejecución sea correcto.

Configuración de una política de monitor desde la CLI

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese definido por CLI vista de política.	**política cli rtm** *Nombre de directiva*	Si la política no existe, este comando crea la política primero.
3. Configure un evento en la política.	- Configure un evento CLI: **evento cli**{**asíncrono**[**saltar**] |**sincronizar**} **modo**{**ejecutar**|**ayuda**|**pestaña**}**patrón** *exp regular* - Configure un evento de conexión en caliente (en modo independiente): **ranura de conexión en caliente para eventos** *número de ranura* [**subranura** *número de subranura*] - Configure un evento hotplug (en modo IRF): **chasis de conexión en caliente para eventos** *número de chasis***ranura** *número de ranura* [**subranura** *número de subranura*] - Configurar un evento de interfaz: **interfaz de eventos** *tipo de interfaz número de interfaz***objeto-monitor** *objeto-monitor***inicio de operación** *inicio de operación* **valor-inicio** *valor-inicio***operación de reinicio** *operación de reinicio* **reiniciar-val** *reiniciar-val*[**intervalo** *intervalo*] - Configurar un evento de proceso (en modo independiente): **proceso de evento**{**excepción**|**Reanudar**|**cerrar**|**comenzar**} [**nombre** *nombre del proceso* [**instancia** *ID de instancia*]] [**ranura** *número de ranura*] - Configurar un evento de proceso (en modo IRF): **proceso de evento**{**excepción**|**Reanudar**|**cerrar**|**comenzar**} [**nombre** *nombre del proceso*[**instancia** *ID de instancia*]] [**chasis** *número de chasis*[**ranura** *número de ranura*]] - Configure un evento SNMP: **evento snmp oid** *oid***objeto-monitor**{**conseguir** |**próximo**} **inicio de operación** *inicio de operación***valor-inicio** *valor-inicio***operación de reinicio** *operación de reinicio* **reiniciar-val** *reiniciar-val*[**intervalo** *intervalo*] - Configure un evento de notificación SNMP: **SNMP de evento**-**notificación oid** *oid* **oid-val** *oid-val***op** *op*[**gota**] - Configure un evento Syslog: **prioridad de syslog de eventos** *nivel***mensaje** *mensaje* **ocurre** *veces***período** *período*	De forma predeterminada, una política de monitor no contiene ningún evento. Puede configurar solo un evento en una política de monitor. Si la política de monitor ya contiene un evento, el nuevo evento anula el evento anterior. En la versión actual del software, el dispositivo no es compatible con **subranura** *número de subranura* opción.

Paso	Dominio	Observaciones
4. Configurar las acciones tomar cuando ocurra el evento.	- Configure la acción para ejecutar un comando: **acción***número***cli***línea de comando* - Configure una acción de reinicio (en modo independiente): **acción***número***reiniciar**[**ranura** *número de ranura*[**subranura** *número de subranura*]] - Configure una acción de reinicio (en modo IRF): **acción***número***reiniciar**[**chasis** *número de chasis*[**ranura***número de ranura* [**subranura***número de subranura*]]] - Configure una acción de registro: **prioridad de syslog de acción***nivel***instalación** *Número local* **mensaje***cuerpo del mensaje* - Configure una acción de conmutación activa/en espera: **acción***número***pasar a otra cosa**	De forma predeterminada, una política de monitor no contiene ninguna acción. Repita este paso para agregar un máximo de 232 acciones a la política. Cuando define una acción, puede optar por especificar un valor o especificar un nombre de variable en **ps***nombre de la variable*formato para un argumento. En la versión actual del software, el dispositivo no es compatible con **subranura***número de subranura*opción.
5. (Opcional). Asigne un rol de usuario a la política.	**rol del usuario***nombre de rol*	De forma predeterminada, una política de supervisión contiene roles de usuario que tenía su creador en el momento de la creación de la política. Una política de monitor admite un máximo de 64 roles de usuario válidos. Los roles de usuario agregados después de alcanzar este límite no surten efecto. Una póliza EAA no puede tener al mismo tiempo **auditoría de seguridad**rol de usuario y cualquier otro rol de usuario. Cualquier Los roles de usuario previamente asignados se eliminan automáticamente cuando asigna el**auditoría de seguridad** rol de usuario a la política. Los previamente asignados **auditoría de seguridad**La función de usuario se elimina automáticamente cuando asigna otras funciones de usuario a la política.
6. (Opcional). Configurar el tiempo de ejecución de la política.	**tiempo de ejecución***tiempo*	El tiempo de ejecución predeterminado es de 20 segundos.
7. Habilite la política.	**comprometerse**	De forma predeterminada, las políticas definidas por CLI no están habilitadas. Una política definida por CLI puede entrar en vigor solo después de realizar este paso.

Configuración de una política de monitor mediante Tcl

Paso	Dominio	Observaciones
1. Edite un archivo de script Tcl (consulteTabla 3).	N / A	La versión de Tcl compatible es 8.5.8.
2. Descargue el archivo al dispositivo mediante FTP o TFTP.	N / A	Para obtener más información sobre el uso de FTP y TFTP, consulte*Guía de configuración básica*.

Paso	Dominio	Observaciones
3. Ingrese a la vista del sistema.	**vista del sistema**	N / A
4. Crear un definido por Tcl política y vincularla al archivo de script Tcl.	**política-rtm tcl***nombre-política nombre-archivo-tcl*	Por defecto, el sistema no cuenta con políticas Tcl. Este paso habilita la política definida por Tcl. Para revisar el script Tcl de una política, primero debe suspender todas las políticas de monitor y luego reanudar las políticas una vez que termine de revisar el script. El sistema no puede ejecutar una política definida por Tcl si edita su script Tcl sin suspender las políticas.

Escriba un script Tcl en dos líneas para una política de monitor, como se muestra enTabla 3.

Tabla 16 Requisitos del script Tcl

Línea	Contenido	Requisitos
Línea 1	Eventos, roles de usuario y tiempo de ejecución de políticas	Esta línea debe utilizar el siguiente formato: **::comware::rtm::event_register***nombre de evento arg1 arg2 arg3*...**rol del usuario***nombre de rol1*| [**rol del usuario***nombre de rol2*| [ ]][**tiempo de ejecución** *tiempo de ejecución*]
Línea 2	Comportamiento	Puede hacer referencia a un nombre de variable en el **ps** *nombre de la variable*formato en lugar de especificar un valor para un argumento cuando define una acción. Están disponibles las siguientes acciones: - Comandos Tcl estándar. - Comandos Tcl específicos de EAA. Comandos - soportados por el dispositivo.

Suspensión de políticas de monitorización

Esta tarea suspende todas las políticas de monitor definidas por CLI y Tcl, excepto las políticas que se están ejecutando. Para suspender las políticas de supervisión:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Suspender las políticas de seguimiento.	**suspensión del programador rtm**	Para reanudar las políticas de monitorización, utilice el**deshacer la suspensión del programador rtm**dominio.

Visualización y mantenimiento de la configuración de EAA

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Muestra variables de entorno EAA definidas por el usuario.	**mostrar entorno rtm**[*nombre-var*]

Tarea	Dominio
Mostrar políticas de monitorización de EAA.	**mostrar política rtm**{**activo**|**registrado**[**verboso**] } [*Nombre de directiva*]

Ejemplos de configuración de EAA

Ejemplo de configuración de política definida por CLI

Requisitos de red

Configure una política desde la CLI para monitorear el evento que ocurre cuando se ingresa un signo de interrogación (?) en la línea de comando que contiene letras y dígitos.

Cuando ocurre el evento, el sistema ejecuta el comando y envía el mensaje de registro "hola mundo" al centro de información.

Procedimiento de configuración

Crear política definida por CLI**prueba**y entrar en su vista.

<nombre del sistema> vista del sistema

[Nombre del sistema] prueba de política de cli rtm

Agregue un evento CLI que ocurre cuando se ingresa un signo de interrogación (?) en cualquier línea de comando que contenga letras y dígitos.

[Sysname-rtm-test] evento cli patrón de ayuda del modo asíncrono [a-zA-Z0-9]

Agregar una acción que envíe el mensaje "hola mundo" con una prioridad de 4 desde la función de registro**local3**cuando ocurre el evento.

[Sysname-rtm-test] acción 0 prioridad de syslog 4 instalación local3 mensaje “hola mundo”

Agregue una acción que ingrese a la vista del sistema cuando ocurra el evento.

[Sysname-rtm-test] acción 2 cli vista del sistema

Agregue una acción que cree la VLAN 2 cuando ocurra el evento.

[Sysname-rtm-test] acción 3 cli vlan 2

Establezca el tiempo de ejecución de la política en 2000 segundos. El sistema deja de ejecutar la política y muestra un mensaje de error de ejecución si no completa la ejecución de la política en 2000 segundos.

[Nombre del sistema-rtm-test] tiempo de ejecución 2000

Especifica el**administrador de red**rol de usuario para ejecutar la política.

[Nombre del sistema-rtm-test] rol de usuario administrador de red

Habilite la política.

Confirmación de [nombre del sistema-rtm-test]

Verificando la configuración

Mostrar información sobre la política.

[Sysname-rtm-test] muestra la política rtm registrada Total

numero 1

Tipo	Evento	Hora de registro	Nombre de directiva
CLI	CLI	29 de agosto 14:56:50 prueba de 2013	

Habilite el centro de información para enviar mensajes de registro al terminal de monitoreo actual.

[Sysname-rtm-test] devuelve el

monitor de terminal <Sysname>

Ingrese un signo de interrogación (?) en una línea de comando que contenga una letra**d**. Verifique que el sistema muestre el mensaje "hola mundo" y un mensaje de política ejecutada exitosamente en la pantalla del terminal.

```
<Nombre del sistema> d?
  depuración
  borrar
  archivo de registro de diagnóstico
  directorio
  mostrar

<Nombre del sistema>d%Mayo 7 02:10:03:218 2013 nombre del sistema RTM/4/RTM_ACCIÓN: "Hola mundo"
%Puede 7 02:10:04:176 2013 nombre del sistema RTM/6/RTM_POLICY: CLI política prueba es correr exitosamente.
```

Ejemplo de configuración de política definida por CLI con variables de entorno EAA

Requisitos de red

Defina una variable de entorno para que coincida con la dirección IP 1.1.1.1.

Configure una política desde la CLI para monitorear el evento que ocurre cuando una línea de comando que contiene **bucle invertido0**es ejecutado. En la política, utilice la variable de entorno para la asignación de direcciones IP.

Cuando ocurre el evento, el sistema realiza las siguientes tareas:

- Crea la interfaz Loopback 0. Asigna
- 1.1.1.1/24 a la interfaz.
- Envía la línea de comando coincidente al centro de información.

Procedimiento de configuración

Configure una variable de entorno EAA para la asignación de direcciones IP. El nombre de la variable es**bucle invertido0IP**, y el valor de la variable es**1.1.1.1**.

```
<nombre del sistema> vista del sistema
[Nombre del sistema] entorno rtm loopback0IP 1.1.1.1
```

Crear la política definida por CLI**prueba**y entrar en su vista.

```
<nombre del sistema> vista del sistema
[Nombre del sistema] prueba de política de cli rtm
```

Agregar un evento CLI que ocurre cuando una línea de comando que contiene**bucle invertido0**es ejecutado.

```
[Sysname-rtm-test] evento cli modo asíncrono ejecutar patrón loopback0
```

Agregue una acción que ingrese a la vista del sistema cuando ocurra el evento.

```
[Sysname-rtm-test] acción 0 cli vista del sistema
```

Agregue una acción que cree la interfaz Loopback 0 e ingrese a la vista de interfaz de loopback.

```
[Sysname-rtm-test] acción 1 interfaz cli loopback 0
```

Agregue una acción que asigne la dirección IP 1.1.1.1 a Loopback 0. El**bucle invertido0IP**La variable se utiliza en la acción para la asignación de dirección IP.

```
[Sysname-rtm-test] acción 2 dirección IP del clip $loopback0IP 24
```

Agrega una acción que envía la correspondencia**bucle invertido0**comando con una prioridad de 0 desde la función de registro **local7**cuando ocurre el evento.

```
[Sysname-rtm-test] acción 3 prioridad syslog 0 instalación local7 mensaje $_cmd
```

Especifica el**administrador de red**rol de usuario para ejecutar la política.

[Nombre del sistema-rtm-test] rol de usuario administrador de red

Habilite la política.

[Sysname-rtm-test] confirmar

[Sysname-rtm-test] devolver

<Sysname>

Verificando la configuración

Habilite el centro de información para enviar mensajes de registro al terminal de monitoreo actual.

Monitor de terminal <nombre del sistema>

Ejecutar el**bucle invertido0**dominio. Verifique que el sistema muestre el**bucle invertido0**mensaje y un mensaje de política ejecutada exitosamente en la pantalla del terminal.

<Nombre del sistema> bucle invertido0

<Nombre del sistema>

%Ene 3 09:46:10:592 2014 Dispositivo001 RTM/0/RTM_ACTION: -MDC=1; bucle invertido0

%Ene 3 09:46:10:613 2014 Dispositivo001 RTM/6/RTM_POLICY: -MDC=1; La prueba de política CLI se está ejecutando exitosamente.

Verifique que se haya creado Loopback 0 y se le haya asignado la dirección IP 1.1.1.1.

Monitor de terminal <nombre del sistema>

<Sysname> muestra breve interfaz de bucle invertido Información

breve sobre las interfaces en modo de ruta: Enlace: ADM -

administrativamente inactivo; Stby - Protocolo de espera: (s) -

suplantación de identidad

Interfaz	Protocolo de enlace IP	Descripción
Bucle0	principal UP UP(s) 1.1.1.1	

<Nombre del sistema>

Ejemplo de configuración de política definida por Tcl

Requisitos de red

Como se muestra enFigura 2, utilice Tcl para crear una política de monitorización en el dispositivo. Esta póliza debe cumplir con los siguientes requisitos:

- EAA envía el mensaje de registro "rtm_tcl_test se está ejecutando" cuando un comando que contiene el **mostrar esto**se ingresa la cadena.
- El sistema ejecuta el comando solo después de ejecutar la política con éxito.

Figura 56 Diagrama de red

Procedimiento de configuración

Edite un archivo de script Tcl (rtm_tcl_test.tcl, en este ejemplo) para que EAA envíe el mensaje "rtm_tcl_test se está ejecutando" cuando se ejecuta un comando que contiene el**mostrar esto**Se ejecuta la cadena.

::comware::rtm::event_register modo de sincronización cli ejecutar patrón mostrar este rol de usuario administrador de red

::comware::rtm::action syslog prioridad 1 instalación local4 msg rtm_tcl_test se está ejecutando

Descargue el archivo de script Tcl del servidor TFTP en**1.2.1.1**.

<Nombre del sistema> tftp 1.2.1.1 obtenga rtm_tcl_test.tcl

Crear política definida por Tcl**prueba**y vincúlelo al archivo de script Tcl.

<nombre del sistema> vista del sistema

[Nombre del sistema] rtm tcl-policy test rtm_tcl_test.tcl [Nombre

del sistema] salir

Verificando la configuración

Mostrar información sobre la política.

<Sysname> muestra la política rtm registrada Total

numero 1

Tipo	Evento	Hora de registro	Nombre de directiva
TCL	TCL	29 de agosto 14:54:50 prueba de 2013	

Habilite el centro de información para enviar mensajes de registro al terminal de monitoreo actual.

Monitor de terminal <nombre del sistema>

Ejecutar el**mostrar esto**dominio. Verifique que el sistema muestre el**rtm_tcl_test se está ejecutando**mensaje y un mensaje de que la política se está ejecutando correctamente.

<Nombre del sistema> muestra esto

#

devolver

<Nombre del sistema>% 4 de junio 15:02:30:354 2013 Nombre del sistema RTM/1/RTM_ACTION: -MDC=1; rtm_tcl_test se está ejecutando

% 4 de junio 15:02:30:382 2013 Nombre del sistema RTM/6/RTM_POLICY: -MDC=1; La prueba de política TCL se está ejecutando correctamente.

Contenido

Configurar la duplicación de puertos

Descripción general

La duplicación de puertos copia los paquetes que pasan a través de un puerto o CPU a un puerto que se conecta a un dispositivo de monitoreo de datos para el análisis de paquetes.

Terminología

Los siguientes términos se utilizan en la configuración de duplicación de puertos.

Fuente de duplicación

Las fuentes de duplicación pueden ser uno o más puertos o CPU monitoreados. Los puertos y CPU monitoreados se denominan puertos de origen y CPU de origen, respectivamente.

Los paquetes que pasan a través de fuentes de duplicación se copian a un puerto que se conecta a un dispositivo de monitoreo de datos para el análisis de paquetes. Las copias se denominan paquetes reflejados.

Dispositivo fuente

El dispositivo donde residen las fuentes de duplicación se denomina dispositivo fuente.

Destino de duplicación

El destino de la duplicación es el puerto de destino (también conocido como puerto de monitoreo) de los paquetes duplicados y se conecta a un dispositivo de monitoreo de datos. Los paquetes reflejados se envían desde el puerto del monitor al dispositivo de monitoreo de datos.

Un puerto de monitor puede recibir varias copias de un paquete cuando monitorea varias fuentes de duplicación. Por ejemplo, se reciben dos copias de un paquete en el puerto 1 cuando existen las siguientes condiciones:

- El puerto 1 monitorea el tráfico bidireccional del puerto 2 y el puerto 3 en el mismo
- dispositivo. El paquete viaja del Puerto 2 al Puerto 3.

Dispositivo de destino

El dispositivo donde reside el puerto del monitor se denomina dispositivo de destino.

Dirección de espejo

La dirección de duplicación especifica la dirección del tráfico que se copia en una fuente de duplicación.

- **Entrante**—Paquetes de copias recibidos. **saliente**—
- Paquetes de copias enviados. **Bidireccional**—Copias de
- paquetes recibidos y enviados.

Grupo de duplicación

La duplicación de puertos se implementa a través de grupos de duplicación, que incluyen grupos locales, de origen remoto y de destino remoto. Para obtener más información sobre los grupos de duplicación, consulte "Clasificación e implementación de duplicación de puertos.".

Puerto reflector, puerto de salida y VLAN de sonda remota

Los puertos reflectores, las VLAN de sonda remota y los puertos de salida se utilizan para la duplicación de puertos remotos de Capa 2. La VLAN de sonda remota es una VLAN dedicada para transmitir paquetes reflejados al dispositivo de destino. Tanto el puerto reflector como el puerto de salida residen en un dispositivo de origen y envían paquetes reflejados a la VLAN de la sonda remota. Para obtener más información sobre el puerto reflector, el puerto de salida, la VLAN de sonda remota y la duplicación del puerto remoto de capa 2, consulte "Clasificación e implementación de duplicación de puertos.".

NOTA:

En los dispositivos de duplicación de puertos, todos los puertos excepto los de origen, destino, reflector y salida se denominan puertos comunes.

Clasificación e implementación de duplicación de puertos.

La duplicación de puertos incluye la duplicación de puertos local y la duplicación de puertos remota.

- **Duplicación de puertos locales**—Las fuentes de duplicación y el destino de duplicación están en el mismo dispositivo.
- **Duplicación remota de puertos**—Las fuentes de duplicación y el destino de la duplicación se encuentran en dispositivos diferentes.

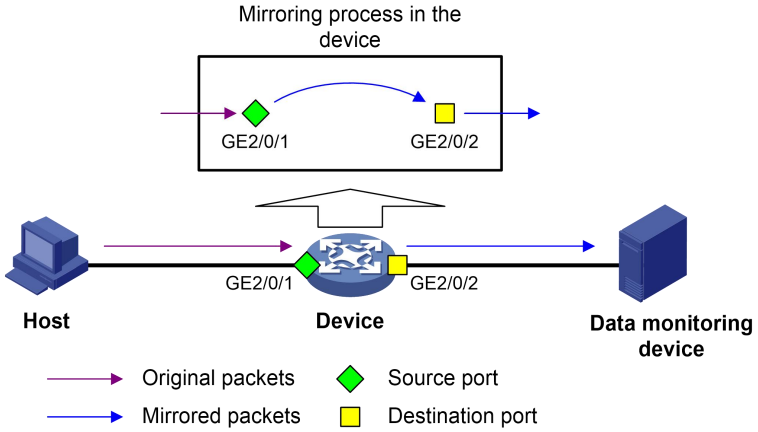
Duplicación de puertos locales

En la duplicación de puertos local, existen las siguientes condiciones:

- El dispositivo fuente está conectado directamente a un dispositivo de monitoreo de datos.
- El dispositivo de origen actúa como dispositivo de destino para reenviar paquetes reflejados al dispositivo de monitoreo de datos.

Un grupo de duplicación local es un grupo de duplicación que contiene los orígenes y el destino de la duplicación en el mismo dispositivo. Las fuentes de duplicación y el destino de duplicación se pueden ubicar en diferentes tarjetas del conmutador.

Figura 57 Implementación de duplicación de puerto local



Como se muestra enFigura 1, el puerto de origen GigabitEthernet 2/0/1 y el puerto de monitor GigabitEthernet 2/0/2 residen en el mismo dispositivo. Los paquetes recibidos en GigabitEthernet 2/0/1 se copian a GigabitEthernet 2/0/2. Luego, GigabitEthernet 2/0/2 reenvía los paquetes al dispositivo de monitoreo de datos para su análisis.

Duplicación remota de puertos

En la duplicación de puertos remotos, existen las siguientes condiciones:

- El dispositivo fuente no está conectado directamente a un dispositivo de monitoreo de datos.
- El dispositivo de origen copia los paquetes reflejados al dispositivo de destino, que los reenvía al dispositivo de monitoreo de datos.
- Los orígenes y el destino de la duplicación residen en diferentes dispositivos y están en diferentes grupos de duplicación.

Un grupo de origen remoto es un grupo de duplicación que contiene las fuentes de duplicación. Un grupo de destino remoto es un grupo de duplicación que contiene el destino de duplicación. Los dispositivos intermedios son los dispositivos entre el dispositivo de origen y el dispositivo de destino.

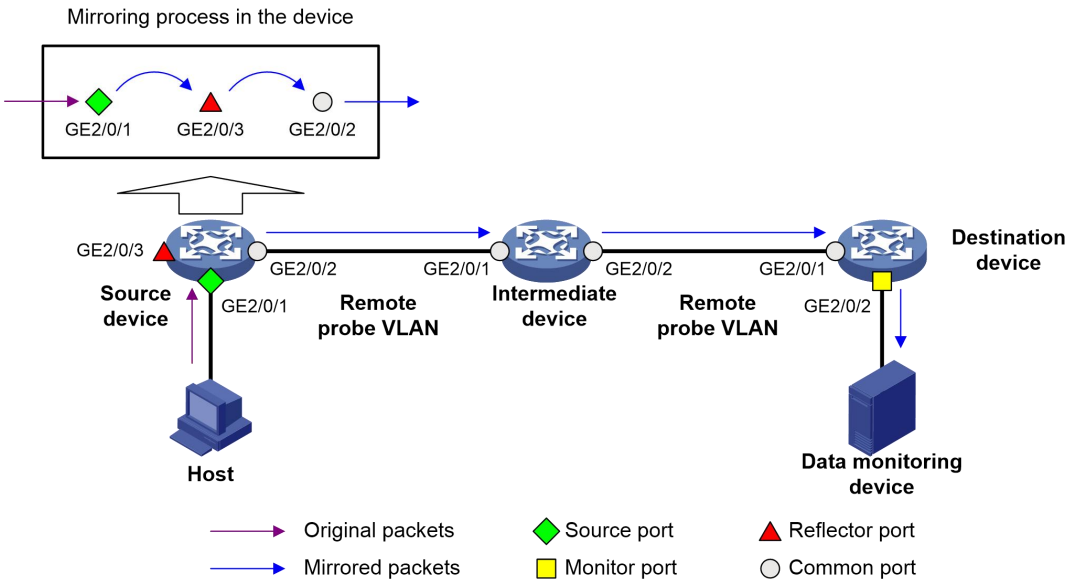
En la duplicación de puertos remotos, los orígenes y el destino de la duplicación se encuentran en diferentes dispositivos en la misma red de Capa 2.

La duplicación de puertos remotos de capa 2 se puede implementar cuando un puerto reflector o un puerto de salida está disponible en el dispositivo de origen. El método para utilizar el puerto reflector y el método para utilizar el puerto de salida se denominan método del puerto reflector y método del puerto de salida, respectivamente.

- **Método del puerto reflector**—Los paquetes se reflejan de la siguiente manera:
  - El dispositivo fuente copia los paquetes recibidos en las fuentes reflejadas al puerto reflector. El
  - puerto reflector transmite los paquetes reflejados en la VLAN de la sonda remota.
  - Los dispositivos intermedios transmiten los paquetes reflejados al dispositivo de destino a través de la VLAN de sonda remota.
  - Al recibir los paquetes reflejados, el dispositivo de destino determina si el ID de los paquetes reflejados es el mismo que el ID de VLAN de la sonda remota. Si las dos ID de VLAN son iguales, el dispositivo de destino reenvía los paquetes reflejados al dispositivo de monitoreo de datos a través del puerto del monitor.

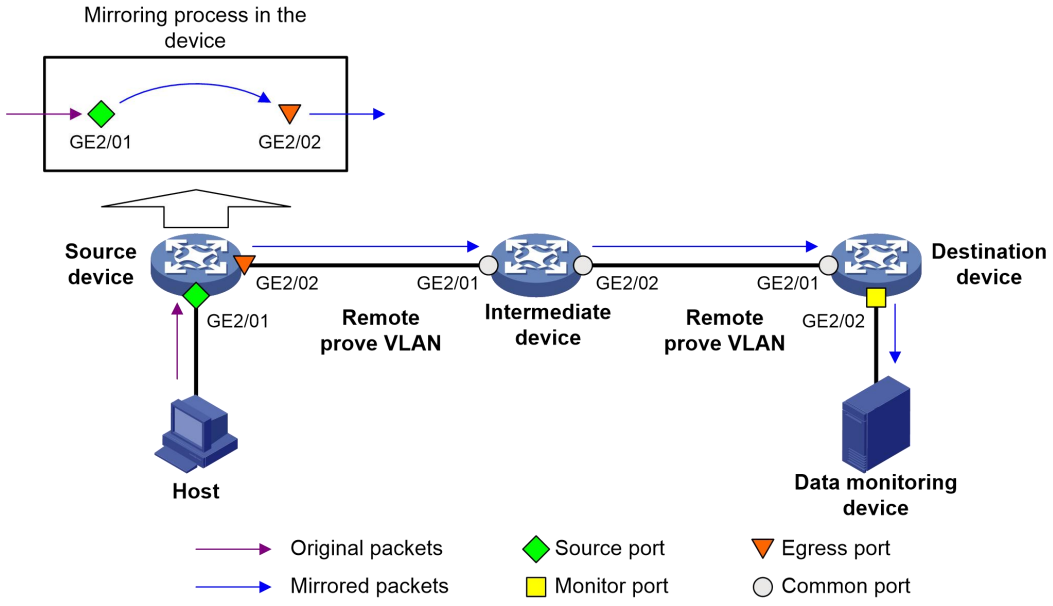
  Un puerto reflector puede ser fijo o configurable. El conmutador solo admite el puerto reflector configurable.

Figura 58 Implementación de duplicación de puerto remoto de capa 2 mediante el método del puerto reflector



- **Método del puerto de salida**—Los paquetes se reflejan de la siguiente manera:
  - El dispositivo de origen copia los paquetes recibidos en las fuentes de duplicación al puerto de salida.
  - El puerto de salida reenvía los paquetes reflejados a los dispositivos intermedios.
  - Los dispositivos intermedios inundan los paquetes reflejados en la VLAN de sonda remota y transmiten los paquetes reflejados al dispositivo de destino.
  - Al recibir los paquetes reflejados, el dispositivo de destino determina si el ID de los paquetes reflejados es el mismo que el ID de VLAN de la sonda remota. Si las dos ID de VLAN son iguales, el dispositivo de destino reenvía los paquetes reflejados al dispositivo de monitoreo de datos a través del puerto del monitor.

Figura 59 Implementación de duplicación de puerto remoto de capa 2 mediante el método del puerto de salida



En el método del puerto reflector, el puerto reflector transmite paquetes reflejados en la VLAN de sonda remota. Al asignar un puerto que no es de origen en el dispositivo de origen a la VLAN de la sonda remota, puede utilizar el método del puerto reflector para implementar la duplicación de puertos local. El método del puerto de salida no puede implementar la duplicación del puerto local de esta manera.

Para garantizar el reenvío de Capa 2 de los paquetes reflejados, asigne los puertos que conectan los dispositivos intermedios a los dispositivos de origen y de destino a la VLAN de sonda remota.

Para monitorear el tráfico bidireccional de un puerto de origen, deshabilite el aprendizaje de la dirección MAC para la VLAN de sonda remota en los dispositivos de origen, intermedio y de destino. Para obtener más información sobre el aprendizaje de direcciones MAC, consulte*Capa 2: Guía de configuración de conmutación LAN*.

Configurar la duplicación de puertos locales

Un grupo de duplicación local entra en vigor solo cuando configura el puerto del monitor y los puertos de origen o las CPU de origen para el grupo de duplicación local.

Lista de tareas de configuración de duplicación de puertos locales

Tareas de un vistazo
3. (Requerido.)Crear un grupo de duplicación local
4. (Obligatorio.) Realice al menos una de las siguientes tareas: - Configuración de puertos de origen para el grupo de duplicación local - Configuración de CPU de origen para el grupo de duplicación local
5. (Requerido.)Configuración del puerto del monitor para el grupo de duplicación local

Crear un grupo de duplicación local

Paso	**Dominio**	**Observaciones**
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A

Paso	Dominio	Observaciones
2. Cree un grupo de duplicación local.	**grupo de duplicación***Identificación del grupo***local**	De forma predeterminada, no existe ningún grupo de duplicación local.

Configuración de puertos de origen para el grupo de duplicación local

Para configurar puertos de origen para un grupo de duplicación local, utilice uno de los siguientes métodos:

- Asigne una lista de puertos de origen al grupo de duplicación en la vista del sistema. Asigne
- un puerto al grupo de duplicación como puerto de origen en la vista de interfaz.

  Para asignar varios puertos al grupo de duplicación como puertos de origen en la vista de interfaz, repita la operación.

Restricciones y pautas de configuración

Cuando configure puertos de origen para un grupo de duplicación local, siga estas restricciones y pautas:

- Un grupo de duplicación puede contener varios puertos de origen.
- Las interfaces agregadas de Capa 2 o Capa 3 no se pueden configurar como puertos de origen para grupos de duplicación.
- Normalmente, un puerto puede actuar como puerto de origen para un solo grupo de duplicación. En el conmutador, un puerto puede ser un puerto de origen para varios grupos de duplicación que tienen diferentes puertos de monitor.
- Un puerto de origen no se puede configurar como puerto reflector, puerto de salida o puerto de monitor.

Configurar puertos de origen en la vista del sistema

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configure los puertos de origen para un grupo de duplicación local.	**grupo de duplicación***Identificación del grupo* **puerto de duplicación***lista de interfaces* {**ambos**|**entrante**|**saliente**}	De forma predeterminada, no se configura ningún puerto de origen para un grupo de duplicación local.

Configurar puertos de origen en la vista de interfaz

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
3. Configure el puerto como puerto de origen para un grupo de duplicación local.	**grupo de duplicación***Identificación del grupo* **puerto de duplicación**{**ambos**|**entrante**|**saliente**}	De forma predeterminada, un puerto no actúa como puerto de origen para ningún puerto local. grupos espejo.

Configuración de CPU de origen para el grupo de duplicación local

Las CPU de las siguientes MPU no se pueden configurar como CPU de origen:

- S7602-MPU.
- S7606-MPU.

Un grupo de duplicación puede contener varias CPU de origen.

Para configurar CPU de origen para un grupo de duplicación local:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configurar fuente CPU para un grupo de duplicación local.	- En modo independiente: **grupo de duplicación***Identificación del grupo***ranura de duplicación de CPU***lista de números de ranura*{**ambos**|**entrante**|**saliente**} - En modo IRF: **grupo de duplicación***Identificación del grupo***chasis de CPU reflejada***número de chasis***ranura** *lista de números de ranura*{**ambos**|**entrante**|**saliente**}	De forma predeterminada, no se configura ninguna CPU de origen para un grupo de duplicación local.

Configuración del puerto del monitor para el grupo de duplicación local

Para configurar el puerto del monitor para un grupo de duplicación, utilice uno de los siguientes métodos:

- Configure el puerto del monitor para el grupo de duplicación en la vista del sistema. Asigne un
- puerto al grupo de duplicación como puerto del monitor en la vista de interfaz.

Restricciones y pautas de configuración

Cuando configure el puerto del monitor para un grupo de duplicación local, siga estas restricciones y pautas:

- No habilite la función de árbol de expansión en el puerto del monitor.
- Para una interfaz agregada de Capa 2 configurada como puerto de monitor de un grupo de creación de reflejo, no configure sus puertos miembros como puertos de origen del grupo de creación de reflejo.
- Un grupo de duplicación contiene solo un puerto de monitor.
- Utilice un puerto de monitor solo para la duplicación de puertos, de modo que el dispositivo de monitoreo de datos reciba solo el tráfico duplicado.

Configurar el puerto del monitor en la vista del sistema

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configure el puerto del monitor para un grupo de duplicación local.	**grupo de duplicación***Identificación del grupo* **puerto de monitor***tipo de interfaz número de interfaz*	De forma predeterminada, no se configura ningún puerto de monitor para un grupo de duplicación local.

Configurar el puerto del monitor en la vista de interfaz

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
3. Configure el puerto como puerto de monitor para un grupo de duplicación.	**grupo de duplicación***Identificación del grupo* **puerto de monitor**	De forma predeterminada, un puerto no actúa como puerto de monitor para ningún grupo de duplicación local.

Configuración de la duplicación de puertos remotos de capa 2

Para configurar la duplicación de puertos remotos de Capa 2, realice las siguientes tareas:

- Configure un grupo de origen remoto en el dispositivo de origen.

- Configure un grupo de destino remoto cooperante en el dispositivo de destino.
- Si existen dispositivos intermedios, configure los siguientes dispositivos y puertos para permitir el paso de la VLAN de la sonda remota.
  - Dispositivos intermedios.
  - Puertos conectados a los dispositivos intermedios en los dispositivos de origen y destino.

Cuando configure la duplicación de puertos remotos de Capa 2, siga estas restricciones y pautas:

- El puerto de salida debe asignarse a la VLAN de la sonda remota. El puerto del reflector configurable no está necesariamente asignado a la VLAN de la sonda remota.
- Para que un paquete reflejado llegue exitosamente al dispositivo de destino remoto, asegúrese de que su ID de VLAN no se elimine ni cambie.
- No configure la duplicación de puertos remotos MVRP y Capa 2. De lo contrario, MVRP podría registrar la VLAN de la sonda remota con puertos incorrectos, lo que provocaría que el puerto del monitor recibiera copias no deseadas. Para obtener más información sobre MVRP, consulte*Capa 2: Guía de configuración de conmutación LAN*.
- Como práctica recomendada, configure los dispositivos en el orden de dispositivo de destino, dispositivos intermedios y dispositivo de origen.

Duplicación de puertos remotos de capa 2 con lista de tareas de configuración de puertos reflectores configurables

Tareas de un vistazo

(Requerido.)Configurar un grupo de destino remoto en el dispositivo de destino:

1. Crear un grupo de destino remoto
2. Configuración del puerto del monitor para un grupo de destino remoto
3. Configuración de la VLAN de sonda remota para un grupo de destino remoto
4. Asignación del puerto del monitor a la VLAN de la sonda remota

(Requerido.)Configurar un grupo de origen remoto en el dispositivo de origen:

1. Crear un grupo de origen remoto
2. Realice al menos una de las siguientes tareas:
   - Configuración de puertos de origen para un grupo de origen remoto
   - Configuración de CPU de origen para un grupo de origen remoto
3. Configuración del puerto reflector para un grupo de origen remoto
4. Configuración de la VLAN de sonda remota para un grupo de origen remoto

Duplicación de puerto remoto de capa 2 con lista de tareas de configuración del puerto de salida

Tareas de un vistazo

(Requerido.)Configurar un grupo de destino remoto en el dispositivo de destino:

1. Crear un grupo de destino remoto
2. Configuración del puerto del monitor para un grupo de destino remoto
3. Configuración de la VLAN de sonda remota para un grupo de destino remoto
4. Asignación del puerto del monitor a la VLAN de la sonda remota

Tareas de un vistazo

(Requerido.)Configurar un grupo de origen remoto en el dispositivo de origen:

1. Crear un grupo de origen remoto
2. Realice al menos una de las siguientes tareas:
   - Configuración de puertos de origen para un grupo de origen remoto
   - Configuración de CPU de origen para un grupo de origen remoto
3. Configurar el puerto de salida para un grupo de origen remoto
4. Configuración de la VLAN de sonda remota para un grupo de origen remoto

Configurar un grupo de destino remoto en el dispositivo de destino

Crear un grupo de destino remoto

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree un grupo de destino remoto.	**grupo de duplicación***Identificación del grupo* **destino-remoto**	De forma predeterminada, no existe ningún grupo de destino remoto en un dispositivo.

Configuración del puerto del monitor para un grupo de destino remoto

Para configurar el puerto del monitor para un grupo de duplicación, utilice uno de los siguientes métodos:

- Configure el puerto del monitor para el grupo de duplicación en la vista del sistema. Asigne un
- puerto al grupo de duplicación como puerto del monitor en la vista de interfaz.

Cuando configure el puerto del monitor para un grupo de destino remoto, siga estas restricciones y pautas:

- No habilite la función de árbol de expansión en el puerto del monitor.
- Para una interfaz agregada de Capa 2 configurada como puerto de monitor de un grupo de creación de reflejo, no configure sus puertos miembros como puertos de origen del grupo de creación de reflejo.
- Utilice un puerto de monitor solo para la duplicación de puertos, de modo que el dispositivo de monitoreo de datos reciba solo el tráfico duplicado.
- Un grupo de duplicación debe contener solo un puerto de monitor. Un
- puerto de monitor sólo puede pertenecer a un grupo de duplicación.

Configuración del puerto del monitor para un grupo de destino remoto en la vista del sistema

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configure el puerto del monitor para un grupo de destino remoto.	**grupo de duplicación***Identificación del grupo* **puerto de monitor***tipo de interfaz número de interfaz*	De forma predeterminada, no se configura ningún puerto de monitor para un grupo de destino remoto.

Configurar el puerto del monitor para un grupo de destino remoto en la vista de interfaz

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A

Paso	Dominio	Observaciones
3. Configure el puerto como puerto de monitor para un grupo de destino remoto.	**grupo de duplicación***Identificación del grupo* **puerto de monitor**	De forma predeterminada, un puerto no actúa como puerto de monitor para ningún grupo de destino remoto.

Configuración de la VLAN de sonda remota para un grupo de destino remoto

Cuando configure la VLAN de la sonda remota para un grupo de destino remoto, siga estas restricciones y pautas:

- Solo una VLAN estática existente se puede configurar como VLAN de sonda remota.
- Cuando una VLAN está configurada como una VLAN de sonda remota, utilice la VLAN de sonda remota para la duplicación de puertos exclusivamente.
- Configure la misma VLAN de sonda remota para los grupos remotos en los dispositivos de origen y de destino.

Para configurar la VLAN de sonda remota para un grupo de destino remoto:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configure la VLAN de la sonda remota para un control remoto grupo de destino.	**grupo de duplicación***Identificación del grupo* **VLAN de sonda remota***id-vlan*	De forma predeterminada, no se configura ninguna VLAN de sonda remota para un grupo de destino.

Asignación del puerto del monitor a la VLAN de la sonda remota

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz del puerto del monitor.	**interfaz***tipo de interfaz número de interfaz*	N / A
3. Asigne el puerto a la VLAN de la sonda remota.	- Para un puerto de acceso: **VLAN de acceso al puerto***id-vlan* - Para un puerto troncal: **vlan de permiso troncal de puerto***id-vlan* - Para un puerto híbrido: **VLAN híbrida de puerto***id-vlan*{**etiquetado** | **sin etiquetar**}	Para más información sobre el **VLAN de acceso al puerto**,**vlan de permiso troncal de puerto**, y**VLAN híbrida de puerto**comandos, ver*Capa 2: referencia de comandos de conmutación de LAN*.

Configurar un grupo de origen remoto en el dispositivo de origen

Crear un grupo de origen remoto

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree un grupo de origen remoto.	**grupo de duplicación***Identificación del grupo* **fuente remota**	De forma predeterminada, no existe ningún grupo de origen remoto en un dispositivo.

Configuración de puertos de origen para un grupo de origen remoto

Para configurar puertos de origen para un grupo de duplicación, utilice uno de los siguientes métodos:

- Asigne una lista de puertos de origen al grupo de duplicación en la vista del sistema. Asigne
- un puerto al grupo de duplicación como puerto de origen en la vista de interfaz.

Para asignar varios puertos al grupo de duplicación como puertos de origen en la vista de interfaz, repita la operación.

Cuando configure puertos de origen para un grupo de origen remoto, siga estas restricciones y pautas:

- No asigne un puerto de origen de un grupo de duplicación a la VLAN de sonda remota del grupo de duplicación.
- Un grupo de duplicación puede contener varios puertos de origen.
- Las interfaces agregadas de Capa 2 o Capa 3 no se pueden configurar como puertos de origen para grupos de duplicación.
- Normalmente, un puerto puede actuar como puerto de origen para un solo grupo de duplicación. En el conmutador, un puerto puede ser un puerto de origen para varios grupos de duplicación que tienen diferentes puertos de monitor.
- Un puerto de origen no se puede configurar como puerto reflector, puerto de monitor o puerto de salida.

Para configurar puertos de origen para un grupo de origen remoto en la vista del sistema:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configure puertos de origen para un grupo de origen remoto.	**grupo de duplicación***Identificación del grupo* **puerto de duplicación***lista de interfaces* {**ambos**|**entrante**|**saliente**}	De forma predeterminada, no se configura ningún puerto de origen para un grupo de origen remoto.

Para configurar un puerto de origen para un grupo de origen remoto en la vista de interfaz:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
3. Configure el puerto como puerto de origen para un grupo de origen remoto.	**grupo de duplicación***Identificación del grupo* **puerto de duplicación**{**ambos**|**entrante**|**saliente**}	De forma predeterminada, un puerto no actúa como puerto de origen para ningún grupo de origen remoto.

Configuración de CPU de origen para un grupo de origen remoto

Las CPU de las siguientes MPU no se pueden configurar como CPU de origen:

- S7602-MPU.
- S7606-MPU.

Un grupo de duplicación puede contener varias CPU de origen.

Para configurar CPU de origen para un grupo de origen remoto:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configurar CPU de origen para un grupo de origen remoto.	- En modo independiente: **grupo de duplicación***Identificación del grupo* **ranura de duplicación de CPU***lista de números de ranura*{**ambos**|**entrante**| **saliente**} - En modo IRF: **grupo de duplicación***Identificación del grupo* **chasis de CPU reflejada***número de chasis* **ranura***lista de números de ranura* { **ambos**|**entrante**|**saliente**}	De forma predeterminada, no se configura ninguna CPU de origen para un grupo de origen remoto.

Configuración del puerto reflector para un grupo de origen remoto

Para configurar el puerto reflector para un grupo de origen remoto, utilice uno de los siguientes métodos:

- Configure el puerto reflector para el grupo de fuentes remotas en la vista del sistema. Asigne un
- puerto al grupo de origen remoto como puerto reflector en la vista de interfaz.

Cuando configure el puerto reflector para un grupo de origen remoto, siga estas restricciones y pautas:

- El puerto que se configurará como puerto reflector debe ser un puerto que no esté en uso. No conecte un cable de red a un puerto reflector.
- Cuando un puerto se configura como puerto reflector, se borran todas las configuraciones existentes del puerto. No puede configurar otras funciones en el puerto reflector.
- Un grupo de duplicación contiene solo un puerto reflector.
- Puede configurar un puerto como puerto reflector solo cuando el puerto esté funcionando con el modo dúplex, la velocidad y la configuración MDI predeterminados. No puede cambiar esta configuración para un puerto reflector.

Para configurar el puerto reflector para un grupo de origen remoto en la vista del sistema:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configure el puerto reflector para un grupo de origen remoto.	**grupo de duplicación***Identificación del grupo* **puerto reflector***tipo de interfaz número de interfaz*	De forma predeterminada, no se configura ningún puerto reflector para un grupo de origen remoto.

Para configurar el puerto reflector para un grupo de origen remoto en la vista de interfaz:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
3. Configure el puerto como puerto reflector para un grupo de origen remoto.	**grupo de duplicación***Identificación del grupo* **puerto reflector**	De forma predeterminada, un puerto no actúa como puerto reflector para ningún grupo de origen remoto.

Configurar el puerto de salida para un grupo de origen remoto

Para configurar el puerto de salida para un grupo de origen remoto, utilice uno de los siguientes métodos:

- Configure el puerto de salida para el grupo de origen remoto en la vista del sistema. Asigne un
- puerto al grupo de origen remoto como puerto de salida en la vista de interfaz.

Cuando configure el puerto de salida para un grupo de origen remoto, siga estas restricciones y pautas:

- Deshabilite las siguientes funciones en el puerto de salida:
  - Árbol de expansión.
  - 802.1X.
  - Espionaje IGMP.
  - ARP estático.
  - Aprendizaje de direcciones MAC.
- Un grupo de duplicación contiene solo un puerto de salida.
- Un puerto de un grupo de duplicación existente no se puede configurar como puerto de salida.

Para configurar el puerto de salida para un grupo de origen remoto en la vista del sistema:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A

Paso	Dominio	Observaciones
2. Configure el puerto de salida para un grupo de origen remoto.	**grupo de duplicación***Identificación del grupo* **salida del monitor***tipo de interfaz número de interfaz*	De forma predeterminada, no se configura ningún puerto de salida para un grupo de origen remoto.

Para configurar el puerto de salida para un grupo de origen remoto en la vista de interfaz:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*	N / A
3. Configure el puerto como puerto de salida para un grupo de origen remoto.	**grupo de duplicación***Identificación del grupo* **salida del monitor**	De forma predeterminada, un puerto no actúa como puerto de salida para ningún grupo de origen remoto.

Configuración de la VLAN de sonda remota para un grupo de origen remoto

Cuando configure la VLAN de la sonda remota para un grupo de origen remoto, siga estas restricciones y pautas:

- Solo una VLAN estática existente se puede configurar como VLAN de sonda remota.
- Cuando una VLAN está configurada como una VLAN de sonda remota, utilice la VLAN de sonda remota para la duplicación de puertos exclusivamente.
- Los grupos de duplicación remota en el dispositivo de origen y el dispositivo de destino deben usar la misma VLAN de sonda remota.

Para configurar la VLAN de sonda remota para un grupo de origen remoto:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Configure la VLAN de la sonda remota para un grupo de origen remoto.	**grupo de duplicación***Identificación del grupo* **VLAN de sonda remota***id-vlan*	De forma predeterminada, no se configura ninguna VLAN de sonda remota para un grupo de origen remoto.

Visualización y mantenimiento de la duplicación de puertos

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Muestra información del grupo de duplicación.	**mostrar grupo de duplicación**{*Identificación del grupo*| **todo**|**local**| **destino-remoto**|**fuente remota**}

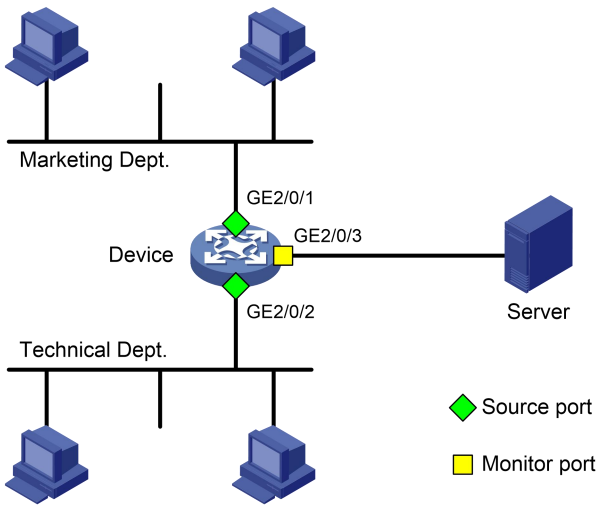
Ejemplos de configuración de duplicación de puertos

Ejemplo de configuración de duplicación de puerto local (en modo de puerto de origen)

Requisitos de red

Como se muestra enFigura 4, configure la duplicación del puerto local en el modo de puerto de origen para permitir que el servidor monitoree el tráfico bidireccional del departamento de marketing y el departamento técnico.

Figura 60 Diagrama de red



Procedimiento de configuración

Crear grupo de duplicación local 1.

<Dispositivo> vista del sistema

[Dispositivo] duplicación-grupo 1 local

Configure GigabitEthernet 2/0/1 y GigabitEthernet 2/0/2 como puertos de origen para el grupo de duplicación local 1.

[Dispositivo] grupo de duplicación 1 puerto de duplicación gigabitethernet 2/0/1 gigabitethernet 2/0/2 ambos

Configure GigabitEthernet 2/0/3 como puerto de monitor para el grupo de duplicación local 1.

[Dispositivo] grupo de duplicación 1 puerto de monitor gigabitethernet 2/0/3

Deshabilite la función de árbol de expansión en el puerto del monitor (GigabitEthernet 2/0/3).

[Dispositivo] interfaz gigabitethernet 2/0/3 [Dispositivo-GigabitEthernet2/0/3] deshacer stp enable [Dispositivo-GigabitEthernet2/0/3] salir

Verificando la configuración

Verifique la configuración del grupo de duplicación.

[Dispositivo] mostrar duplicación: agrupar todas las duplicaciones grupo 1:

Tipo: Local

Estado: Activo

Duplicación puerto:

GigabitEthernet2/0/1 Ambos

GigabitEthernet2/0/2 Ambos puertos de
monitor: GigabitEthernet2/0/3

Ejemplo de configuración de duplicación de puerto local (en modo CPU de origen)

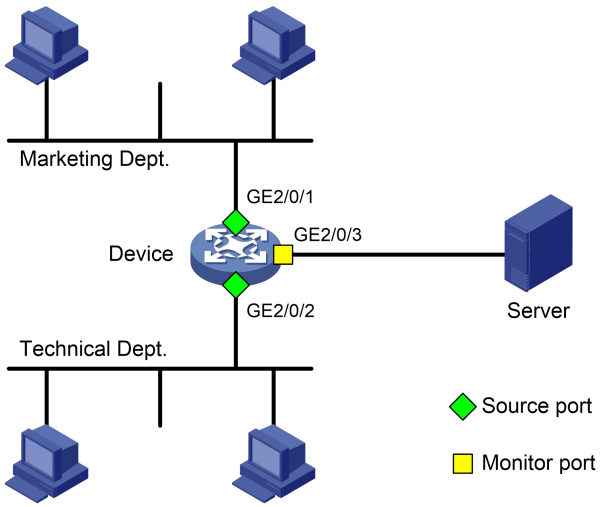
Requisitos de red

Como se muestra enFigura 5, GigabitEthernet 2/0/1 y GigabitEthernet 2/0/2 se encuentran en la tarjeta en la ranura 1.

Configure la duplicación del puerto local en el modo de CPU de origen para permitir que el servidor supervise todos los paquetes que coincidan con los siguientes criterios:

- Recibido y enviado por el departamento de Marketing y el departamento Técnico.
- Procesado por la CPU de la tarjeta en la ranura 1 del dispositivo.

Figura 61 Diagrama de red



Procedimiento de configuración

Crear grupo de duplicación local 1.

<Dispositivo> vista del sistema
[Dispositivo] duplicación-grupo 1 local

Configure la CPU de la tarjeta en la ranura 1 del dispositivo como CPU de origen para el grupo de duplicación local 1.

[Dispositivo] grupo de duplicación 1 ranura de CPU de duplicación 1 ambos

Configure GigabitEthernet 2/0/3 como puerto de monitor para el grupo de duplicación local 1.

[Dispositivo] grupo de duplicación 1 puerto de monitor gigabitethernet 2/0/3

Deshabilite la función de árbol de expansión en el puerto del monitor (GigabitEthernet 2/0/3).

[Dispositivo] interfaz gigabitethernet 2/0/3 [Dispositivo-
GigabitEthernet2/0/3] deshacer stp enable [Dispositivo-
GigabitEthernet2/0/3] salir

Verificando la configuración

Verifique la configuración del grupo de duplicación.

[Dispositivo] mostrar duplicación: agrupar todas las
duplicaciones grupo 1:
Tipo: Local

Estado: Activo

Duplicación UPC:

Ranura 1 Ambos

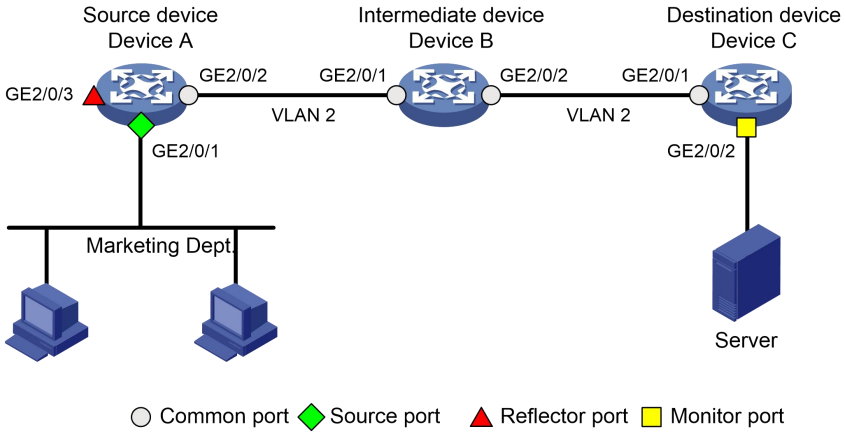
Puerto de monitorización: GigabitEthernet2/0/3

Ejemplo de configuración de duplicación de puerto remoto de capa 2 (puerto reflector configurable)

Requisitos de red

Como se muestra enFigura 6, configure la duplicación de puertos remotos de Capa 2 para permitir que el servidor supervise el tráfico bidireccional del departamento de marketing.

Figura 62 Diagrama de red



Procedimiento de configuración

1. Configure el dispositivo C (el dispositivo de destino):

   # Configure GigabitEthernet 2/0/1 como puerto troncal y asigne el puerto a VLAN 2.

   <DispositivoC> vista del sistema

   [DeviceC] interfaz gigabitethernet 2/0/1 [DeviceC-GigabitEthernet2/0/1]

   puerto tipo enlace troncal [DeviceC-GigabitEthernet2/0/1] puerto troncal

   permiso vlan 2 [DeviceC-GigabitEthernet2/0/1] salir

   # Cree un grupo de destino remoto.

   [DeviceC] duplicación-grupo 2 destino-remoto

   # Crear VLAN 2.

   [DispositivoC] vlan 2

   # Deshabilite el aprendizaje de direcciones MAC para VLAN 2.

   [DeviceC-vlan2] deshacer dirección mac mac-learning habilitar

   [DeviceC-vlan2] salir

   # Configure la VLAN 2 como la VLAN de sonda remota para el grupo de duplicación.

   [DeviceC] grupo de duplicación 2 sonda remota vlan 2

   # Configure GigabitEthernet 2/0/2 como puerto de monitor para el grupo de duplicación.

   [DeviceC] interfaz gigabitethernet 2/0/2 [DeviceC-GigabitEthernet2/0/2] puerto de monitor del grupo 2 de duplicación

   # Deshabilite la función de árbol de expansión en GigabitEthernet 2/0/2.

[DeviceC-GigabitEthernet2/0/2] deshacer la habilitación de stp

Asigne GigabitEthernet 2/0/2 a VLAN 2.

[DeviceC-GigabitEthernet2/0/2] acceso al puerto vlan 2 [DeviceC-GigabitEthernet2/0/2] salir

2. Configure el dispositivo B (el dispositivo intermedio):

Crear VLAN 2.

<DispositivoB> vista del sistema

[DispositivoB] vlan 2

Deshabilite el aprendizaje de direcciones MAC para VLAN 2.

[DeviceB-vlan2] deshacer dirección mac mac-learning habilitar

[DeviceB-vlan2] salir

Configure GigabitEthernet 2/0/1 como puerto troncal y asigne el puerto a VLAN 2.

[DeviceB] interfaz gigabitethernet 2/0/1 [DeviceB-GigabitEthernet2/0/1]

puerto tipo enlace troncal [DeviceB-GigabitEthernet2/0/1] puerto troncal

permiso vlan 2 [DeviceB-GigabitEthernet2/0/1] salir

Configure GigabitEthernet 2/0/2 como puerto troncal y asigne el puerto a VLAN 2.

[DeviceB] interfaz gigabitethernet 2/0/2 [DeviceB-GigabitEthernet2/0/2]

puerto tipo enlace troncal [DeviceB-GigabitEthernet2/0/2] puerto troncal

permiso vlan 2 [DeviceB-GigabitEthernet2/0/2] salir

3. Configure el dispositivo A (el dispositivo de origen):

Cree un grupo de origen remoto.

<DispositivoA> vista del sistema

[DispositivoA] fuente remota del grupo 1 de duplicación

Crear VLAN 2.

[DispositivoA] vlan 2

Deshabilite el aprendizaje de direcciones MAC para VLAN 2.

[DeviceA-vlan2] deshacer dirección mac habilitar aprendizaje de mac

[DeviceA-vlan2] salir

Configure la VLAN 2 como la VLAN de sonda remota para el grupo de duplicación.

[DispositivoA] grupo de duplicación 1 vlan de sonda remota 2

Configure GigabitEthernet 2/0/1 como puerto de origen para el grupo de duplicación.

[DispositivoA] grupo de duplicación 1 puerto de duplicación gigabitethernet 2/0/1 ambos

Configure GigabitEthernet 2/0/3 como el puerto reflector para el grupo de duplicación.

[DispositivoA] grupo de duplicación 1 puerto reflector gigabitethernet 2/0/3

Esta operación puede eliminar todas las configuraciones realizadas en la interfaz. ¿Continuar? [T/N]: sí

Configure GigabitEthernet 2/0/2 como puerto troncal y asigne el puerto a VLAN 2.

[DeviceA] interfaz gigabitethernet 2/0/2 [DeviceA-GigabitEthernet2/0/2]

puerto tipo enlace troncal [DeviceA-GigabitEthernet2/0/2] puerto troncal

permiso vlan 2 [DeviceA-GigabitEthernet2/0/2] salir

Verificando la configuración

Verifique la configuración del grupo de duplicación en el dispositivo C.

[DispositivoC] muestra el grupo de duplicación todo

el grupo de duplicación 2:

Tipo: Destino remoto Estado:
Activo
Monitor puerto: GigabitEthernet2/0/2
VLAN de sonda remota: 2

Verifique la configuración del grupo de duplicación en el dispositivo A.

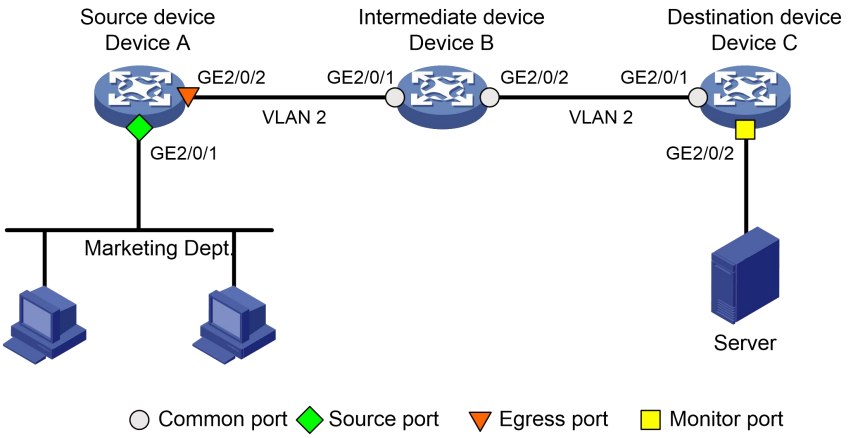
[DispositivoA] muestra el grupo de duplicación de todos los duplicados grupo 1:
Tipo: fuente remota
Estado: Activo
Duplicación puerto:
GigabitEthernet2/0/1 Ambos
Puerto reflector: GigabitEthernet2/0/3 Sonda remota VLAN: 2

Ejemplo de configuración de duplicación de puerto remoto de capa 2 (con puerto de salida)

Requisitos de red

En la red de Capa 2 que se muestra enFigura 7, configure la duplicación de puertos remotos de Capa 2 para permitir que el servidor supervise el tráfico bidireccional del departamento de marketing.

Figura 63 Diagrama de red



Procedimiento de configuración

1. Configure el dispositivo C (el dispositivo de destino):

   # Configure GigabitEthernet 2/0/1 como puerto troncal y asigne el puerto a VLAN 2.

   <DispositivoC> vista del sistema
   [DeviceC] interfaz gigabitethernet 2/0/1 [DeviceC-GigabitEthernet2/0/1]
   puerto tipo enlace troncal [DeviceC-GigabitEthernet2/0/1] puerto troncal
   permiso vlan 2 [DeviceC-GigabitEthernet2/0/1] salir

   # Cree un grupo de destino remoto.

   [DeviceC] duplicación-grupo 2 destino-remoto

   # Crear VLAN 2.

   [DispositivoC] vlan 2

Deshabilite el aprendizaje de direcciones MAC para VLAN 2.

[DeviceC-vlan2] deshacer dirección mac mac-learning habilitar

[DeviceC-vlan2] salir

Configure la VLAN 2 como la VLAN de sonda remota para el grupo de duplicación.

[DeviceC] grupo de duplicación 2 sonda remota vlan 2

Configure GigabitEthernet 2/0/2 como puerto de monitor para el grupo de duplicación.

[DeviceC] interfaz gigabitethernet 2/0/2 [DeviceC-GigabitEthernet2/0/2] puerto de monitor del grupo 2 de duplicación

Deshabilite la función de árbol de expansión en GigabitEthernet 2/0/2.

[DeviceC-GigabitEthernet2/0/2] deshacer la habilitación de stp

Asigne GigabitEthernet 2/0/2 a VLAN 2 como puerto de acceso.

[DeviceC-GigabitEthernet2/0/2] acceso al puerto vlan 2 [DeviceC-GigabitEthernet2/0/2] salir

2. Configure el dispositivo B (el dispositivo intermedio):

Crear VLAN 2.

<DispositivoB> vista del sistema

[DispositivoB] vlan 2

Deshabilite el aprendizaje de direcciones MAC para VLAN 2.

[DeviceB-vlan2] deshacer dirección mac mac-learning habilitar

[DeviceB-vlan2] salir

Configure GigabitEthernet 2/0/1 como puerto troncal y asigne el puerto a VLAN 2.

[DeviceB] interfaz gigabitethernet 2/0/1 [DeviceB-GigabitEthernet2/0/1] puerto tipo enlace troncal [DeviceB-GigabitEthernet2/0/1] puerto troncal permiso vlan 2 [DeviceB-GigabitEthernet2/0/1] salir

Configure GigabitEthernet 2/0/2 como puerto troncal y asigne el puerto a VLAN 2.

[DeviceB] interfaz gigabitethernet 2/0/2 [DeviceB-GigabitEthernet2/0/2] puerto tipo enlace troncal [DeviceB-GigabitEthernet2/0/2] puerto troncal permiso vlan 2 [DeviceB-GigabitEthernet2/0/2] salir

3. Configure el dispositivo A (el dispositivo de origen):

Cree un grupo de origen remoto.

<DispositivoA> vista del sistema

[DispositivoA] fuente remota del grupo 1 de duplicación

Crear VLAN 2.

[DispositivoA] vlan 2

Deshabilite el aprendizaje de direcciones MAC para VLAN 2.

[DeviceA-vlan2] deshacer dirección mac habilitar aprendizaje de mac

[DeviceA-vlan2] salir

Configure la VLAN 2 como la VLAN de sonda remota del grupo de duplicación.

[DispositivoA] grupo de duplicación 1 vlan de sonda remota 2

Configure GigabitEthernet 2/0/1 como puerto de origen para el grupo de duplicación.

[DispositivoA] grupo de duplicación 1 puerto de duplicación gigabitethernet 2/0/1 ambos

Configure GigabitEthernet 2/0/2 como puerto de salida para el grupo de duplicación.

[DispositivoA] duplicación-grupo 1 monitor-salida gigabitethernet 2/0/2

Configure el puerto GigabitEthernet 2/0/2 como puerto troncal y asigne el puerto a VLAN 2.

[DispositivoA] interfaz gigabitethernet 2/0/2

[DeviceA-GigabitEthernet2/0/2] puerto troncal de tipo enlace [DeviceA-GigabitEthernet2/0/2] puerto troncal permiso vlan 2

Deshabilite la función de árbol de expansión en el puerto.

[DeviceA-GigabitEthernet2/0/2] deshacer stp enable [DeviceA-GigabitEthernet2/0/2] salir

Verificando la configuración

Verifique la configuración del grupo de duplicación en el dispositivo C.

[DeviceC] muestra el grupo de duplicación de todos los duplicados Grupo 2:

Tipo: Destino remoto

Estado: Activo

Monitor puerto: GigabitEthernet2/0/2

VLAN de sonda remota: 2

Verifique la configuración del grupo de duplicación en el dispositivo A.

[DispositivoA] muestra el grupo de duplicación de todos los duplicados grupo 1:

Tipo: fuente remota

Estado: Activo

Duplicación puerto:

GigabitEthernet2/0/1 Ambos

Puerto de salida del monitor: GigabitEthernet2/0/2

VLAN de sonda remota: 2

Configurar la duplicación de flujo

La función de duplicación de flujo está disponible en interfaces Ethernet de Capa 2 y Capa 3. El término "interfaz" en este capítulo se refiere colectivamente a estos dos tipos de interfaces. Puedes usar el**modo de enlace de puerto**comando para configurar un puerto Ethernet como una interfaz de Capa 2 o Capa 3 (consulte*Capa 2: Guía de configuración de conmutación LAN*).

La duplicación de flujo copia paquetes que coinciden con una clase en un destino para analizar y monitorear paquetes. Se implementa a través de políticas de QoS.

Para configurar la duplicación de flujo, realice las siguientes tareas:

- Defina clases de tráfico y configure criterios de coincidencia para clasificar los paquetes que se van a reflejar. La duplicación de flujo le permite clasificar de manera flexible los paquetes que se analizarán definiendo criterios de coincidencia.
- Configure los comportamientos del tráfico para reflejar los paquetes coincidentes en el destino especificado.

Puede configurar una acción para reflejar los paquetes coincidentes en uno de los siguientes destinos:

- **Interfaz**—Los paquetes coincidentes se copian a una interfaz que se conecta a un dispositivo de monitoreo de datos. El dispositivo de seguimiento de datos analiza los paquetes recibidos en la interfaz.
- **UPC**—Los paquetes coincidentes se copian a la CPU de la tarjeta donde se reciben. La CPU analiza los paquetes o los entrega a las capas superiores.

Para obtener más información sobre políticas de QoS, clases de tráfico y comportamientos del tráfico, consulte*Guía de configuración de ACL y QoS*.

Lista de tareas de configuración de duplicación de flujo

Tareas de un vistazo
(Requerido.)Configurar criterios de coincidencia
(Requerido.)Configurar un comportamiento de tráfico
(Requerido.)Configurar una política de QoS
(Obligatorio). Aplicación de una política de QoS: - Aplicar una política de QoS a una interfaz Aplicar - una política de QoS a una VLAN Aplicar una política - de QoS globalmente Aplicar una política de QoS al - plano de control

Para obtener más información sobre los siguientes comandos, excepto el**espejo a**comando, ver*Referencia de comandos de ACL y QoS*.

Configurar criterios de coincidencia

Paso	**Dominio**	**Observaciones**
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una clase y acceda a la vista de clase.	**clasificador de trafico** *nombre-tcl* [**operador**{**y**|**o**}]	De forma predeterminada, no existe ninguna clase de tráfico.
3. Configurar criterios de coincidencia.	**si coincide***criterios de coincidencia*	De forma predeterminada, no se configura ningún criterio de coincidencia en una clase de tráfico.

Configurar un comportamiento de tráfico

Para configurar un comportamiento de tráfico:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree un comportamiento de tráfico e ingrese a la vista de comportamiento de tráfico.	**comportamiento del tráfico***nombre-comportamiento*	De forma predeterminada, no existe ningún comportamiento de tráfico.
3. Configure una acción de duplicación para el comportamiento del tráfico.	- Reflejar el tráfico en una interfaz: **interfaz espejo a** *Tipo de interfaz número de interfaz* - Tráfico reflejado a la CPU: **espejo a CPU**	De forma predeterminada, no se configura ninguna acción de duplicación para un comportamiento de tráfico.
4. (Opcional). Muestra la configuración del comportamiento del tráfico.	**mostrar el comportamiento del tráfico**	Disponible en cualquier vista.

Configurar una política de QoS

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Cree una política de QoS e ingrese a la vista de política de QoS.	**política de qos***Nombre de directiva*	De forma predeterminada, no existe ninguna política de QoS.
3. Asocie una clase con un comportamiento de tráfico en la política de QoS.	**clasificador***nombre-tc***comportamiento** *nombre-comportamiento*	De forma predeterminada, no hay ningún comportamiento de tráfico asociado con una clase.
4. (Opcional). Muestra la configuración de la política de QoS.	**mostrar política qos**	Disponible en cualquier vista.

Aplicar una política de QoS

Aplicar una política de QoS a una interfaz

Al aplicar una política de QoS a una interfaz, puede reflejar el tráfico en la dirección especificada de la interfaz. Se puede aplicar una política a múltiples interfaces. En una dirección (entrante o saliente) de una interfaz, sólo se puede aplicar una política.

Para aplicar una política de QoS a una interfaz:

Paso	Dominio
1. Ingrese a la vista del sistema.	**vista del sistema**
2. Ingrese a la vista de interfaz.	**interfaz***tipo de interfaz número de interfaz*
3. Aplicar una política a la interfaz.	**política de aplicación de qos***Nombre de directiva*{**entrante**|**saliente**}

Aplicar una política de QoS a una VLAN

Puede aplicar una política de QoS a una VLAN para reflejar el tráfico en la dirección especificada en todos los puertos de la VLAN.

Para aplicar la política de QoS a una VLAN:

Paso		Dominio
1.	Ingrese a la vista del sistema.	**vista del sistema**
2.	Aplicar una política de QoS a una VLAN.	**política qos vlan***Nombre de directiva***vlan***lista-id-vlan*{ **entrante** |**saliente**}

Aplicar una política de QoS a nivel global

Puede aplicar una política de QoS globalmente para reflejar el tráfico en la dirección especificada en todos los puertos. Para aplicar

una política de QoS globalmente:

Paso		Dominio
1.	Ingrese a la vista del sistema.	**vista del sistema**
2.	Aplicar una política de QoS a nivel global.	**política de aplicación de qos***Nombre de directiva***global**{ **entrante**| **saliente**}

Aplicar una política de QoS al plano de control

Puede aplicar una política de QoS al plano de control para reflejar el tráfico en la dirección especificada de todos los puertos en el plano de control.

Para aplicar una política de QoS al plano de control:

Paso		Dominio
1.	Ingrese a la vista del sistema.	**vista del sistema**
2.	Ingrese a la vista del plano de control.	- En modo independiente: **ranura del plano de control***número de ranura* - En modo IRF: **chasis del plano de control***número de chasis***ranura***número de ranura*
3.	Aplicar una política de QoS al plano de control.	**política de aplicación de qos***Nombre de directiva*{**entrante**|**saliente**}

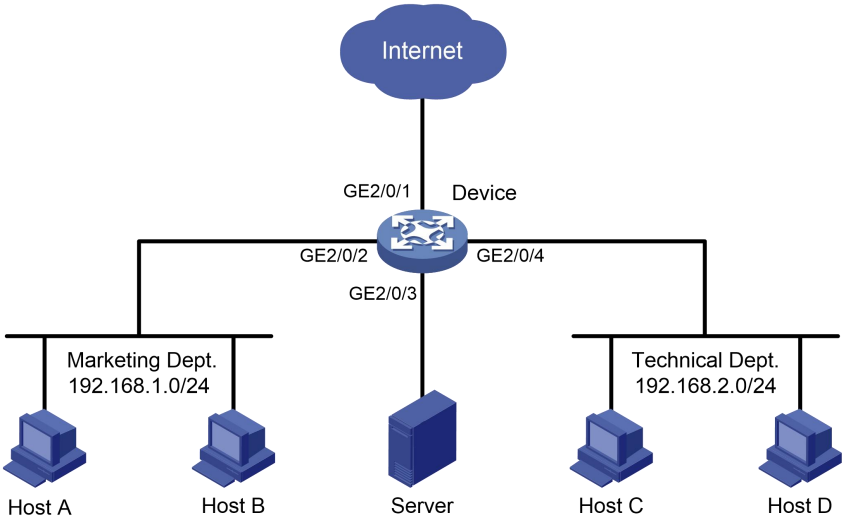
Ejemplo de configuración de duplicación de flujo

Requisitos de red

Como se muestra enFigura 8, configure la duplicación de flujo para que el servidor pueda monitorear el siguiente tráfico:

- Todo el tráfico que envía el departamento Técnico para acceder a Internet.
- Tráfico IP que el departamento Técnico envía al departamento de Marketing en horario laboral (8:00 a 18:00) de lunes a viernes.

Figura 64 Diagrama de red



Procedimiento de configuración

Crear rango de horas de trabajo**trabajar**, en el que el horario laboral es de 8:00 a 18:00 horas los días laborables.

<DispositivoA> vista del sistema

[DispositivoA] rango de tiempo de trabajo de 8:00 a 18:00 días laborables

Crear ACL 3000 para permitir que los paquetes del departamento técnico accedan a Internet y al departamento de marketing durante el horario laboral.

[DispositivoA] número de acl 3000

[DeviceA-acl-adv-3000] regla permite fuente tcp 192.168.2.0 0.0.0.255 puerto-destino eq www

[DeviceA-acl-adv-3000] regla permite ip fuente 192.168.2.0 0.0.0.255 destino 192.168.1.0 0.0.0.255 trabajo de rango de tiempo

[DeviceA-acl-adv-3000] salir

Crear clase de tráfico**tecnología_c**y configure el criterio de coincidencia como ACL 3000.

[DispositivoA] clasificador de tráfico tech_c [DeviceA-classifier-tech_c] if-match acl 3000 [DeviceA-classifier-tech_c]

salir

Crear comportamiento de tráfico**tecnología_b**, configure la acción de duplicar el tráfico al puerto GigabitEthernet 2/0/3.

[DispositivoA] comportamiento del tráfico tech_b

[DeviceA-behavior-tech_b] espejo a interfaz gigabitethernet 2/0/3 [DeviceA-behavior-tech_b] salir

Crear política de QoS**tecnología_p**y clase de tráfico asociada**tecnología_c**con el comportamiento del tráfico**tecnología_b**en la política de QoS.

[DispositivoA] política qos tech_p

[DeviceA-qospolicy-tech_p] clasificador tech_c comportamiento tech_b [DeviceA-qospolicy-tech_p] salir

Aplicar política de QoS**tecnología_p**a los paquetes entrantes de GigabitEthernet 2/0/4.

[DeviceA] interfaz gigabitethernet 2/0/4 [DeviceA-GigabitEthernet2/0/4] qos aplicar política tech_p entrante [DeviceA-GigabitEthernet2/0/4] salir

Verificando la configuración

Verifique que el servidor pueda monitorear el siguiente tráfico:

- Todo el tráfico enviado por el departamento Técnico para acceder a Internet.
- Tráfico IP que el departamento Técnico envía al departamento de Marketing en horario laboral entre semana.

(No se muestran detalles).

Contenido

Configurando sFlow

sFlow es una tecnología de monitoreo de tráfico.

Como se muestra enFigura 1, el sistema sFlow implica un agente sFlow integrado en un dispositivo y un recolector de sFlow remoto. El agente sFlow recopila información del contador de la interfaz y de paquetes y encapsula la información muestreada en paquetes sFlow. Cuando el búfer de paquetes de sFlow está lleno o el temporizador de vencimiento (fijado en 1 segundo) expira, el agente de sFlow realiza las siguientes acciones:

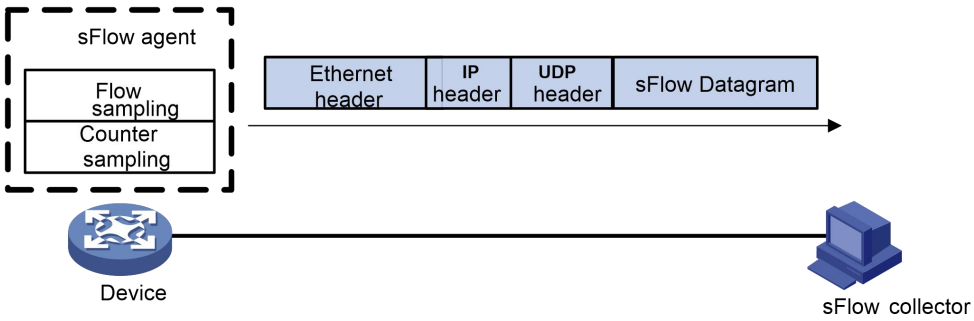
- Encapsula los paquetes sFlow en los datagramas UDP. Envía
- los datagramas UDP al recopilador sFlow especificado.

El recopilador sFlow analiza la información y muestra los resultados. Un recopilador de sFlow puede monitorear varios agentes de sFlow.

sFlow proporciona los siguientes mecanismos de muestreo:

- **Muestreo de flujo**: obtiene información del paquete. **Contramuestreo**—
- Obtiene información del contador de la interfaz.

Figura 65 Sistema de flujo



Protocolos y estándares

- RFC 3176,*sFlow de InMon Corporation: un método para monitorear el tráfico en redes conmutadas y enrutadas*
- sFlow.org,*sFlow Versión 5*

Restricciones y pautas de configuración

El dispositivo no admite el uso de un puerto Ethernet de administración para conectarse a un recopilador sFlow.

Lista de tareas de configuración de sFlow

Tareas de un vistazo
(Requerido.)Configuración de la información del agente sFlow y del recopilador sFlow
Realice al menos una de las siguientes tareas: - Configuración del muestreo de flujo - Configuración del muestreo del contador

Configuración de la información del agente sFlow y del recopilador sFlow

Paso	Dominio	Observaciones
4. Ingrese a la vista del sistema.	**vista del sistema**	N / A
5. (Opcional.) Configurar una IP dirección para el Agente de flujo.	**agente de flujo**{**IP***dirección IP*|**ipv6***dirección ipv6*}	De forma predeterminada, no se configura ninguna dirección IP para el agente sFlow. El conmutador comprueba periódicamente si el agente sFlow tiene una dirección IP. De lo contrario, el conmutador selecciona automáticamente una dirección IPv4 para el agente sFlow pero no guarda la dirección IPv4 en el archivo de configuración. **NOTA:** - Como práctica recomendada, configure manualmente una dirección IP para el agente sFlow. - Solo se puede configurar una dirección IP para el agente sFlow en el conmutador y una dirección IP recién configurada sobrescribe la existente.
6. Configurar el Colector de flujo información.	**colector de flujo***ID de coleccionista* [**instancia-vpn** *nombre-instancia-vpn*] {**IP** *dirección IP*|**ipv6** *dirección ipv6*} [**puerto** *número de puerto*|**tamaño de datagrama** *tamaño*|**tiempo-afuera***segundos*| **descripción** *texto*] *	De forma predeterminada, no se configura ninguna información del recopilador de sFlow. El rango de valores para el*ID de coleccionista*El argumento es de 1 a 10.
7. (Opcional). Especificar la IP de origen dirección de sFlow paquetes.	**fuente de flujo**{**IP***dirección IP* |**ipv6***dirección ipv6*} *	De forma predeterminada, la dirección IP de origen se determina mediante el enrutamiento.

Configurar el muestreo de flujo

Realice esta tarea para configurar el muestreo de flujo en una interfaz Ethernet. El agente sFlow realiza las siguientes tareas:

1. Muestra paquetes en esa interfaz según los parámetros configurados.
2. Encapsula los paquetes en paquetes sFlow.
3. Encapsula los paquetes sFlow en los paquetes UDP y envía los paquetes UDP al recopilador sFlow especificado.

Para configurar el muestreo de flujo:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz Ethernet de capa 2 o a la vista de interfaz Ethernet de capa 3.	**interfaz***tipo de interfaz número de interfaz*	N / A

Paso	Dominio	Observaciones
3. (Opcional). Configure el modo de muestreo de flujo.	**modo de muestreo de flujo** {**determinar**|**aleatorio**}	De forma predeterminada, se utiliza el muestreo aleatorio. El**determinar**La palabra clave no es compatible con la versión actual del software. La palabra clave está reservada para soporte futuro.
4. Habilite el muestreo de flujo y especifique la cantidad de paquetes de los cuales el muestreo de flujo muestrea un paquete en la interfaz.	**tasa de muestreo de flujo de flujo***tasa*	De forma predeterminada, el muestreo de flujo está deshabilitado.
5. (Opcional). Establezca el número máximo de bytes (a partir del encabezado del paquete) que el muestreo de flujo puede copiar por paquete.	**encabezado máximo de flujo de flujo***longitud*	La configuración predeterminada es 128 bytes. Como práctica recomendada, utilice la configuración predeterminada.
6. Especifique el recopilador sFlow para el muestreo de flujo.	**colector de flujo***ID de coleccionista*	De forma predeterminada, no se especifica ningún recopilador sFlow para el muestreo de flujo.

Configurar el muestreo del contador

Realice esta tarea para configurar el contador de muestreo en una interfaz Ethernet. El agente sFlow realiza las siguientes tareas:

1. Recopila periódicamente la información del contador en esa interfaz.
2. Encapsula la información del contador en paquetes sFlow.
3. Encapsula los paquetes sFlow en los paquetes UDP y envía los paquetes UDP al recopilador sFlow especificado.

Para configurar el contador de muestreo:

Paso	Dominio	Observaciones
1. Ingrese a la vista del sistema.	**vista del sistema**	N / A
2. Ingrese a la vista de interfaz Ethernet de capa 2 o a la vista de interfaz Ethernet de capa 3.	**interfaz***tipo de interfaz número de interfaz*	N / A
3. Habilite el muestreo del contador y establezca el intervalo de muestreo del contador.	**intervalo del contador de flujo** *tiempo de intervalo*	De forma predeterminada, el contramuestreo está deshabilitado.
4. Especifique el recopilador sFlow para el contramuestreo.	**colector contador de flujo** *ID de coleccionista*	De forma predeterminada, no se especifica ningún recopilador sFlow para el contramuestreo.

Visualización y mantenimiento de sFlow

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Mostrar la configuración de sFlow.	**mostrar flujo**

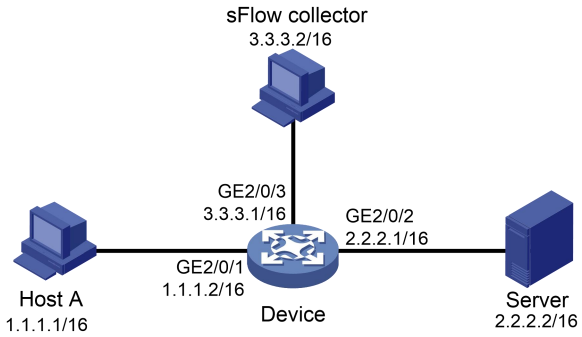
Ejemplo de configuración de sFlow

Requisitos de red

Como se muestra enFigura 2, realice las siguientes tareas:

- Configure el muestreo de flujo en modo aleatorio y el contramuestreo en GigabitEthernet 2/0/1 del dispositivo para monitorear el tráfico en el puerto.
- Configure el dispositivo para enviar información de muestra en paquetes sFlow a través de GigabitEthernet 2/0/3 al recopilador de sFlow.

Figura 66 Diagrama de red



Procedimiento de configuración

1. Configure las direcciones IP y máscaras de subred para las interfaces, como se muestra enFigura 2. (No se muestran detalles).

2. Configure el agente sFlow y configure la información sobre el recopilador sFlow:

   # Configure la dirección IP para el agente sFlow.

   <Dispositivo> vista del sistema

   [Dispositivo] ip del agente sflow 3.3.3.1

   # Configurar información sobre el recopilador sFlow. Especifique el ID del recopilador de sFlow como 1, la dirección IP como 3.3.3.2, el número de puerto como 6343 (predeterminado) y la descripción como**servidor de red**.

   [Dispositivo] sflow recopilador 1 ip 3.3.3.2 descripción netserver

3. Configurar el muestreo del contador:

   # Habilite el muestreo del contador y establezca el intervalo de muestreo del contador en 120 segundos en GigabitEthernet 2/0/1.

   [Dispositivo] interfaz gigabitethernet 2/0/1 [Dispositivo-GigabitEthernet2/0/1] intervalo de contador de flujo 120

   # Especifique el colector sFlow 1 para el contramuestreo.

   [Device-GigabitEthernet2/0/1] recopilador de contador de flujo 1

4. Configurar el muestreo de flujo:

   # Habilite el muestreo de flujo y establezca el modo de muestreo de flujo en aleatorio y el intervalo de muestreo en 4000.

   [Device-GigabitEthernet2/0/1] modo de muestreo de flujo aleatorio [Device-GigabitEthernet2/0/1] frecuencia de muestreo de flujo 4000

   # Especifique el colector sFlow 1 para el muestreo de flujo.

   [Device-GigabitEthernet2/0/1] colector de flujo 1

Verificando las configuraciones

Verifique los siguientes elementos:

- GigabitEthernet 2/0/1 habilitado con sFlow está activo. El
- intervalo de muestreo del contador es de 120 segundos.
- El intervalo de muestreo de flujo es 4000 (se muestrea un paquete de cada 4000 paquetes).

[Device-GigabitEthernet2/0/1] Versión mostrar fluir
del datagrama sFlow: 5 Información
global:
IP del agente: 3.3.3.1(CLI)
Dirección de la fuente:
Coleccionista información:

IDENTIFICACIÓN	IP	Puerto	Envejecimiento	Tamaño	Descripción de la instancia VPN
1	3.3.3.2	6343	N / A	1400	servidor de red

Información del puerto:

Interfaz	CID	Intervalo(s)	FID	Tasa	MaxHLen	Modo	Estado
GE2/0/1	1	120	1	128	4000	Aleatorio	Activo

Solución de problemas de configuración de sFlow

El recopilador de sFlow remoto no puede recibir paquetes de sFlow

Síntoma

El recopilador de sFlow remoto no puede recibir paquetes de sFlow.

Análisis

Las posibles razones incluyen:

- El recopilador sFlow no está especificado. sFlow
- no está configurado en la interfaz.
- La dirección IP del recopilador de sFlow especificado en el agente de sFlow es diferente de la del recopilador de sFlow remoto.
- No se configura ninguna dirección IP para la interfaz de Capa 3 que envía paquetes sFlow.
- Se configura una dirección IP para la interfaz de Capa 3 que envía paquetes sFlow. Sin embargo, los datagramas UDP con esta dirección IP de origen no pueden llegar al recopilador sFlow.
- El vínculo físico entre el dispositivo y el recopilador de sFlow falla. El
- recopilador sFlow está vinculado a una VPN inexistente.
- La longitud de un paquete sFlow es menor que la suma de los dos valores siguientes:
  - La longitud del encabezado del paquete sFlow.
  - El número de bytes que el muestreo de flujo puede copiar por paquete.

Solución

Para resolver el problema:

1. Utilizar el**mostrar flujo**comando para verificar que sFlow esté configurado correctamente.
2. Verifique que esté configurada una dirección IP correcta para que el dispositivo se comunique con el recopilador sFlow.
3. Verifique que el enlace físico entre el dispositivo y el recopilador sFlow esté activo.

4. Verifique que la VPN vinculada al recopilador sFlow ya exista.
5. Verifique que la longitud de un paquete sFlow sea mayor que la suma de los dos valores siguientes:
   - La longitud del encabezado del paquete sFlow.
   - La cantidad de bytes (como práctica recomendada, use el valor predeterminado) que el muestreo de flujo puede copiar por paquete.

Contenido

Configurando sFlow

sFlow es una tecnología de monitoreo de tráfico.

Como se muestra enFigura 1, el sistema sFlow implica un agente sFlow integrado en un dispositivo y un recolector de sFlow remoto. El agente sFlow recopila información del contador de la interfaz y de paquetes y encapsula la información muestreada en paquetes sFlow. Cuando el búfer de paquetes de sFlow está lleno o el temporizador de vencimiento (fijado en 1 segundo) expira, el agente de sFlow realiza las siguientes acciones:

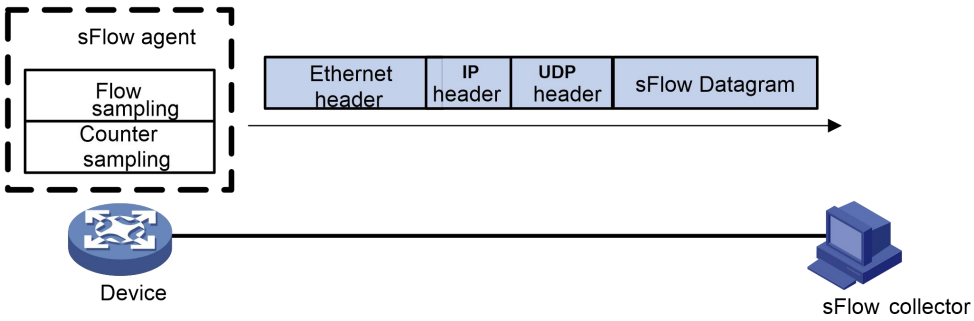
- Encapsula los paquetes sFlow en los datagramas UDP. Envía
- los datagramas UDP al recopilador sFlow especificado.

El recopilador sFlow analiza la información y muestra los resultados. Un recopilador de sFlow puede monitorear varios agentes de sFlow.

sFlow proporciona los siguientes mecanismos de muestreo:

- **Muestreo de flujo**: obtiene información del paquete. **Contramuestreo**—
- Obtiene información del contador de la interfaz.

Figura 67 Sistema de flujo



Protocolos y estándares

- RFC 3176,*sFlow de InMon Corporation: un método para monitorear el tráfico en redes conmutadas y enrutadas*
- sFlow.org,*sFlow Versión 5*

Restricciones y pautas de configuración

El dispositivo no admite el uso de un puerto Ethernet de administración para conectarse a un recopilador sFlow.

Lista de tareas de configuración de sFlow

Tareas de un vistazo
(Requerido.)Configuración de la información del agente sFlow y del recopilador sFlow
Realice al menos una de las siguientes tareas: - Configuración del muestreo de flujo - Configuración del muestreo del contador

Configuración de la información del agente sFlow y del recopilador sFlow

Paso	Dominio	Observaciones
5. Ingrese a la vista del sistema.	**vista del sistema**	N / A
6. (Opcional.) Configurar una IP dirección para el Agente de flujo.	**agente de flujo**{**IP***dirección IP*| **ipv6***dirección ipv6*}	De forma predeterminada, no se configura ninguna dirección IP para el agente sFlow. El conmutador comprueba periódicamente si el agente sFlow tiene una dirección IP. De lo contrario, el conmutador selecciona automáticamente una dirección IPv4 para el agente sFlow pero no guarda la dirección IPv4 en el archivo de configuración. **NOTA:** - Como práctica recomendada, configure manualmente una dirección IP para el agente sFlow. - Solo se puede configurar una dirección IP para el agente sFlow en el conmutador y una dirección IP recién configurada sobrescribe la existente.
7. Configurar el Colector de flujo información.	**colector de flujo***ID de coleccionista* [**instancia-vpn** *nombre-instancia-vpn*] {**IP** *dirección IP*| **ipv6** *dirección ipv6*} [**puerto** *número de puerto*| **tamaño de datagrama** *tamaño*| **tiempo-afuera***segundos*| **descripción** *texto*] *	De forma predeterminada, no se configura ninguna información del recopilador de sFlow. El rango de valores para el*ID de coleccionista*El argumento es de 1 a 10.
8. (Opcional). Especificar la IP de origen dirección de sFlow paquetes.	**fuente de flujo**{**IP***dirección IP* | **ipv6***dirección ipv6*} *	De forma predeterminada, la dirección IP de origen se determina mediante el enrutamiento.

Configurar el muestreo de flujo

Realice esta tarea para configurar el muestreo de flujo en una interfaz Ethernet. El agente sFlow realiza las siguientes tareas:

1. Muestra paquetes en esa interfaz según los parámetros configurados.
2. Encapsula los paquetes en paquetes sFlow.
3. Encapsula los paquetes sFlow en los paquetes UDP y envía los paquetes UDP al recopilador sFlow especificado.

Para configurar el muestreo de flujo:

Paso	Dominio	Observaciones
9. Ingrese a la vista del sistema.	**vista del sistema**	N / A
10. Ingrese a la vista de interfaz Ethernet de capa 2 o a la vista de interfaz Ethernet de capa 3.	**interfaz***tipo de interfaz número de interfaz*	N / A

Paso	Dominio	Observaciones
11.(Opcional.) Configure el modo de muestreo de flujo.	**modo de muestreo de flujo** {**determinar**|**aleatorio**}	De forma predeterminada, se utiliza el muestreo aleatorio. El**determinar**La palabra clave no es compatible con la versión actual del software. La palabra clave está reservada para soporte futuro.
12. Habilite el muestreo de flujo y especifique el número de paquetes de los cuales el muestreo de flujo toma muestras de un paquete en la interfaz.	**tasa de muestreo de flujo de flujo***tasa*	De forma predeterminada, el muestreo de flujo está deshabilitado.
13.(Opcional.) Establezca el número máximo de bytes (a partir del encabezado del paquete) que el muestreo de flujo puede copiar por paquete.	**encabezado máximo de flujo de flujo***longitud*	La configuración predeterminada es 128 bytes. Como práctica recomendada, utilice la configuración predeterminada.
14. Especifique el recopilador sFlow para el muestreo de flujo.	**colector de flujo***ID de coleccionista*	De forma predeterminada, no se especifica ningún recopilador sFlow para el muestreo de flujo.

Configurar el muestreo del contador

Realice esta tarea para configurar el contador de muestreo en una interfaz Ethernet. El agente sFlow realiza las siguientes tareas:

1. Recopila periódicamente la información del contador en esa interfaz.
2. Encapsula la información del contador en paquetes sFlow.
3. Encapsula los paquetes sFlow en los paquetes UDP y envía los paquetes UDP al recopilador sFlow especificado.

Para configurar el contador de muestreo:

Paso	Dominio	Observaciones
15. Ingrese a la vista del sistema.	**vista del sistema**	N / A
dieciséis. Ingrese a la vista de interfaz Ethernet de capa 2 o a la vista de interfaz Ethernet de capa 3.	**interfaz***tipo de interfaz número de interfaz*	N / A
17. Habilite el muestreo del contador y establezca el intervalo de muestreo del contador.	**intervalo del contador de flujo** *tiempo de intervalo*	De forma predeterminada, el contramuestreo está deshabilitado.
18. Especifique el recopilador sFlow para el contramuestreo.	**colector contador de flujo** *ID de coleccionista*	De forma predeterminada, no se especifica ningún recopilador sFlow para el contramuestreo.

Visualización y mantenimiento de sFlow

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Mostrar la configuración de sFlow.	**mostrar flujo**

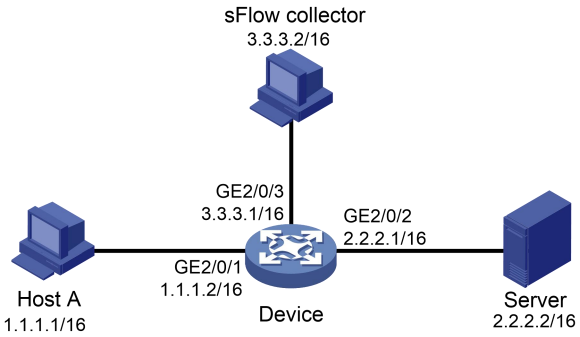
Ejemplo de configuración de sFlow

Requisitos de red

Como se muestra enFigura 2, realice las siguientes tareas:

- Configure el muestreo de flujo en modo aleatorio y el contramuestreo en GigabitEthernet 2/0/1 del dispositivo para monitorear el tráfico en el puerto.
- Configure el dispositivo para enviar información de muestra en paquetes sFlow a través de GigabitEthernet 2/0/3 al recopilador de sFlow.

Figura 68 Diagrama de red



Procedimiento de configuración

1. Configure las direcciones IP y máscaras de subred para las interfaces, como se muestra enFigura 2. (No se muestran detalles).

2. Configure el agente sFlow y configure la información sobre el recopilador sFlow:

   # Configure la dirección IP para el agente sFlow.

   <Dispositivo> vista del sistema

   [Dispositivo] ip del agente sflow 3.3.3.1

   # Configurar información sobre el recopilador sFlow. Especifique el ID del recopilador de sFlow como 1, la dirección IP como 3.3.3.2, el número de puerto como 6343 (predeterminado) y la descripción como**servidor de red**.

   [Dispositivo] sflow recopilador 1 ip 3.3.3.2 descripción netserver

3. Configurar el muestreo del contador:

   # Habilite el muestreo del contador y establezca el intervalo de muestreo del contador en 120 segundos en GigabitEthernet 2/0/1.

   [Dispositivo] interfaz gigabitethernet 2/0/1 [Dispositivo-GigabitEthernet2/0/1] intervalo de contador de flujo 120

   # Especifique el colector sFlow 1 para el contramuestreo.

   [Device-GigabitEthernet2/0/1] recopilador de contador de flujo 1

4. Configurar el muestreo de flujo:

   # Habilite el muestreo de flujo y establezca el modo de muestreo de flujo en aleatorio y el intervalo de muestreo en 4000.

   [Device-GigabitEthernet2/0/1] modo de muestreo de flujo aleatorio [Device-GigabitEthernet2/0/1] frecuencia de muestreo de flujo 4000

   # Especifique el colector sFlow 1 para el muestreo de flujo.

   [Device-GigabitEthernet2/0/1] colector de flujo 1

Verificando las configuraciones

Verifique los siguientes elementos:

- GigabitEthernet 2/0/1 habilitado con sFlow está activo. El
- intervalo de muestreo del contador es de 120 segundos.
- El intervalo de muestreo de flujo es 4000 (se muestrea un paquete de cada 4000 paquetes).

[Device-GigabitEthernet2/0/1] Versión mostrar fluir
del datagrama sFlow: 5 Información
global:
IP del agente: 3.3.3.1(CLI)
Dirección de la fuente:
Coleccionista información:

IDENTIFICACIÓN	IP	Puerto	Envejecimiento	Tamaño	Descripción de la instancia VPN
1	3.3.3.2	6343	N / A	1400	servidor de red

Información del puerto:

Interfaz	CID	Intervalo(s)	FID	Tasa	MaxHLen	Modo	Estado
GE2/0/1	1	120	1	128	4000	Aleatorio	Activo

Solución de problemas de configuración de sFlow

El recopilador de sFlow remoto no puede recibir paquetes de sFlow

Síntoma

El recopilador de sFlow remoto no puede recibir paquetes de sFlow.

Análisis

Las posibles razones incluyen:

- El recopilador sFlow no está especificado. sFlow
- no está configurado en la interfaz.
- La dirección IP del recopilador de sFlow especificado en el agente de sFlow es diferente de la del recopilador de sFlow remoto.
- No se configura ninguna dirección IP para la interfaz de Capa 3 que envía paquetes sFlow.
- Se configura una dirección IP para la interfaz de Capa 3 que envía paquetes sFlow. Sin embargo, los datagramas UDP con esta dirección IP de origen no pueden llegar al recopilador sFlow.
- El vínculo físico entre el dispositivo y el recopilador de sFlow falla. El
- recopilador sFlow está vinculado a una VPN inexistente.
- La longitud de un paquete sFlow es menor que la suma de los dos valores siguientes:
  - La longitud del encabezado del paquete sFlow.
  - El número de bytes que el muestreo de flujo puede copiar por paquete.

Solución

Para resolver el problema:

1. Utilizar el**mostrar flujo**comando para verificar que sFlow esté configurado correctamente.
2. Verifique que esté configurada una dirección IP correcta para que el dispositivo se comunique con el recopilador sFlow.
3. Verifique que el enlace físico entre el dispositivo y el recopilador sFlow esté activo.

4. Verifique que la VPN vinculada al recopilador sFlow ya exista.
5. Verifique que la longitud de un paquete sFlow sea mayor que la suma de los dos valores siguientes:
   - La longitud del encabezado del paquete sFlow.
   - La cantidad de bytes (como práctica recomendada, use el valor predeterminado) que el muestreo de flujo puede copiar por paquete.

Contenido

Configurando sFlow

sFlow es una tecnología de monitoreo de tráfico.

Como se muestra enFigura 1, el sistema sFlow implica un agente sFlow integrado en un dispositivo y un recolector de sFlow remoto. El agente sFlow recopila información del contador de la interfaz y de paquetes y encapsula la información muestreada en paquetes sFlow. Cuando el búfer de paquetes de sFlow está lleno o el temporizador de vencimiento (fijado en 1 segundo) expira, el agente de sFlow realiza las siguientes acciones:

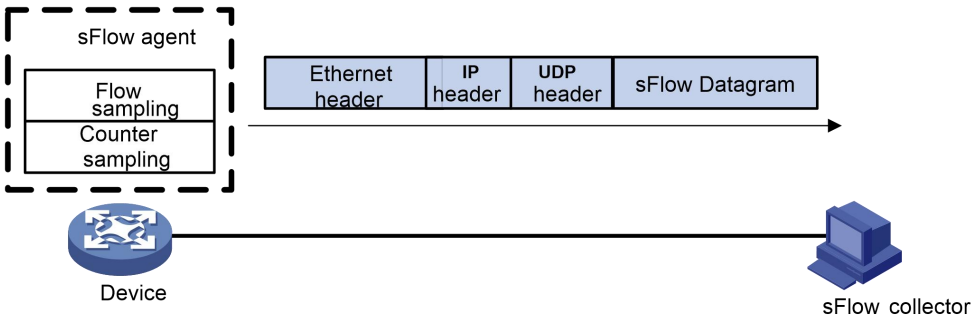
- Encapsula los paquetes sFlow en los datagramas UDP. Envía
- los datagramas UDP al recopilador sFlow especificado.

El recopilador sFlow analiza la información y muestra los resultados. Un recopilador de sFlow puede monitorear varios agentes de sFlow.

sFlow proporciona los siguientes mecanismos de muestreo:

- **Muestreo de flujo**: obtiene información del paquete. **Contramuestreo**—
- Obtiene información del contador de la interfaz.

Figura 69 Sistema de flujo



Protocolos y estándares

- RFC 3176,*sFlow de InMon Corporation: un método para monitorear el tráfico en redes conmutadas y enrutadas*
- sFlow.org,*sFlow Versión 5*

Restricciones y pautas de configuración

El dispositivo no admite el uso de un puerto Ethernet de administración para conectarse a un recopilador sFlow.

Lista de tareas de configuración de sFlow

Tareas de un vistazo
(Requerido.)Configuración de la información del agente sFlow y del recopilador sFlow
Realice al menos una de las siguientes tareas: - Configuración del muestreo de flujo - Configuración del muestreo del contador

Configuración de la información del agente sFlow y del recopilador sFlow

Paso	Dominio	Observaciones
19. Ingrese a la vista del sistema.	**vista del sistema**	N / A
20.(Opcional.) Configurar una IP dirección para el Agente de flujo.	**agente de flujo**{**IP***dirección IP*|**ipv6***dirección ipv6*}	De forma predeterminada, no se configura ninguna dirección IP para el agente sFlow. El conmutador comprueba periódicamente si el agente sFlow tiene una dirección IP. De lo contrario, el conmutador selecciona automáticamente una dirección IPv4 para el agente sFlow pero no guarda la dirección IPv4 en el archivo de configuración. **NOTA:** - Como práctica recomendada, configure manualmente una dirección IP para el agente sFlow. - Solo se puede configurar una dirección IP para el agente sFlow en el conmutador y una dirección IP recién configurada sobrescribe la existente.
21. Configurar el Colector de flujo información.	**colector de flujo***ID de coleccionista* [**instancia-vpn** *nombre-instancia-vpn*] {**IP** *dirección IP*|**ipv6** *dirección ipv6*} [**puerto** *número de puerto*|**tamaño de datagrama** *tamaño*|**tiempo-afuera***segundos*| **descripción** *texto*] *	De forma predeterminada, no se configura ninguna información del recopilador de sFlow. El rango de valores para el*ID de coleccionista*El argumento es de 1 a 10.
22.(Opcional.) Especifique la IP de origen. dirección de sFlow paquetes.	**fuente de flujo**{**IP***dirección IP*|**ipv6***dirección ipv6*} *	De forma predeterminada, la dirección IP de origen se determina mediante el enrutamiento.

Configurar el muestreo de flujo

Realice esta tarea para configurar el muestreo de flujo en una interfaz Ethernet. El agente sFlow realiza las siguientes tareas:

1. Muestra paquetes en esa interfaz según los parámetros configurados.
2. Encapsula los paquetes en paquetes sFlow.
3. Encapsula los paquetes sFlow en los paquetes UDP y envía los paquetes UDP al recopilador sFlow especificado.

Para configurar el muestreo de flujo:

Paso	Dominio	Observaciones
23. Ingrese a la vista del sistema.	**vista del sistema**	N / A
24. Ingrese a la vista de interfaz Ethernet de capa 2 o a la vista de interfaz Ethernet de capa 3.	**interfaz***tipo de interfaz número de interfaz*	N / A

Paso	Dominio	Observaciones
25.(Opcional.) Configure el modo de muestreo de flujo.	**modo de muestreo de flujo** {**determinar**|**aleatorio**}	De forma predeterminada, se utiliza el muestreo aleatorio. El**determinar**La palabra clave no es compatible con la versión actual del software. La palabra clave está reservada para soporte futuro.
26. Habilite el muestreo de flujo y especifique el número de paquetes de los cuales el muestreo de flujo toma muestras de un paquete en la interfaz.	**tasa de muestreo de flujo de flujo***tasa*	De forma predeterminada, el muestreo de flujo está deshabilitado.
27.(Opcional.) Establezca el número máximo de bytes (a partir del encabezado del paquete) que el muestreo de flujo puede copiar por paquete.	**encabezado máximo de flujo de flujo***longitud*	La configuración predeterminada es 128 bytes. Como práctica recomendada, utilice la configuración predeterminada.
28. Especifique el recopilador sFlow para el muestreo de flujo.	**colector de flujo***ID de coleccionista*	De forma predeterminada, no se especifica ningún recopilador sFlow para el muestreo de flujo.

Configurar el muestreo del contador

Realice esta tarea para configurar el contador de muestreo en una interfaz Ethernet. El agente sFlow realiza las siguientes tareas:

1. Recopila periódicamente la información del contador en esa interfaz.
2. Encapsula la información del contador en paquetes sFlow.
3. Encapsula los paquetes sFlow en los paquetes UDP y envía los paquetes UDP al recopilador sFlow especificado.

Para configurar el contador de muestreo:

Paso	Dominio	Observaciones
29. Ingrese a la vista del sistema.	**vista del sistema**	N / A
30. Ingrese a la vista de interfaz Ethernet de capa 2 o a la vista de interfaz Ethernet de capa 3.	**interfaz***tipo de interfaz número de interfaz*	N / A
31. Habilite el muestreo del contador y establezca el intervalo de muestreo del contador.	**intervalo del contador de flujo** *tiempo de intervalo*	De forma predeterminada, el contramuestreo está deshabilitado.
32. Especifique el recopilador sFlow para el contramuestreo.	**colector contador de flujo** *ID de coleccionista*	De forma predeterminada, no se especifica ningún recopilador sFlow para el contramuestreo.

Visualización y mantenimiento de sFlow

Ejecutar**mostrar**comandos en cualquier vista.

Tarea	Dominio
Mostrar la configuración de sFlow.	**mostrar flujo**

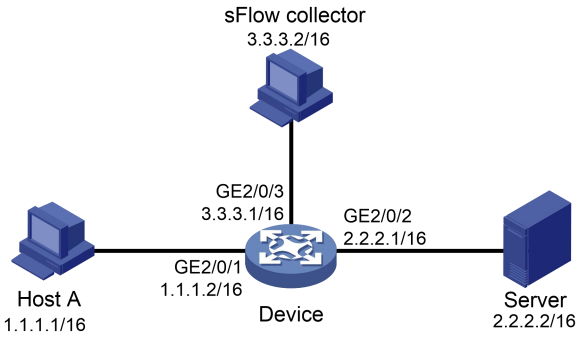
Ejemplo de configuración de sFlow

Requisitos de red

Como se muestra enFigura 2, realice las siguientes tareas:

- Configure el muestreo de flujo en modo aleatorio y el contramuestreo en GigabitEthernet 2/0/1 del dispositivo para monitorear el tráfico en el puerto.
- Configure el dispositivo para enviar información de muestra en paquetes sFlow a través de GigabitEthernet 2/0/3 al recopilador de sFlow.

Figura 70 Diagrama de red



Procedimiento de configuración

1. Configure las direcciones IP y máscaras de subred para las interfaces, como se muestra enFigura 2. (No se muestran detalles).

2. Configure el agente sFlow y configure la información sobre el recopilador sFlow:

   # Configure la dirección IP para el agente sFlow.

   <Dispositivo> vista del sistema

   [Dispositivo] ip del agente sflow 3.3.3.1

   # Configurar información sobre el recopilador sFlow. Especifique el ID del recopilador de sFlow como 1, la dirección IP como 3.3.3.2, el número de puerto como 6343 (predeterminado) y la descripción como**servidor de red**.

   [Dispositivo] sflow recopilador 1 ip 3.3.3.2 descripción netserver

3. Configurar el muestreo del contador:

   # Habilite el muestreo del contador y establezca el intervalo de muestreo del contador en 120 segundos en GigabitEthernet 2/0/1.

   [Dispositivo] interfaz gigabitethernet 2/0/1 [Dispositivo-GigabitEthernet2/0/1] intervalo de contador de flujo 120

   # Especifique el colector sFlow 1 para el contramuestreo.

   [Device-GigabitEthernet2/0/1] recopilador de contador de flujo 1

4. Configurar el muestreo de flujo:

   # Habilite el muestreo de flujo y establezca el modo de muestreo de flujo en aleatorio y el intervalo de muestreo en 4000.

   [Device-GigabitEthernet2/0/1] modo de muestreo de flujo aleatorio [Device-GigabitEthernet2/0/1] frecuencia de muestreo de flujo 4000

   # Especifique el colector sFlow 1 para el muestreo de flujo.

   [Device-GigabitEthernet2/0/1] colector de flujo 1

Verificando las configuraciones

Verifique los siguientes elementos:

- GigabitEthernet 2/0/1 habilitado con sFlow está activo. El
- intervalo de muestreo del contador es de 120 segundos.
- El intervalo de muestreo de flujo es 4000 (se muestrea un paquete de cada 4000 paquetes).

[Device-GigabitEthernet2/0/1] Versión mostrar fluir
del datagrama sFlow: 5 Información
global:
IP del agente: 3.3.3.1(CLI)
Dirección de la fuente:
Coleccionista información:

IDENTIFICACIÓN	IP	Puerto	Envejecimiento	Tamaño	Descripción de la instancia VPN
1	3.3.3.2	6343	N / A	1400	servidor de red

Información del puerto:

Interfaz	CID	Intervalo(s)	FID	Tasa	MaxHLen	Modo	Estado
GE2/0/1	1	120	1	128	4000	Aleatorio	Activo

Solución de problemas de configuración de sFlow

El recopilador de sFlow remoto no puede recibir paquetes de sFlow

Síntoma

El recopilador de sFlow remoto no puede recibir paquetes de sFlow.

Análisis

Las posibles razones incluyen:

- El recopilador sFlow no está especificado. sFlow
- no está configurado en la interfaz.
- La dirección IP del recopilador de sFlow especificado en el agente de sFlow es diferente de la del recopilador de sFlow remoto.
- No se configura ninguna dirección IP para la interfaz de Capa 3 que envía paquetes sFlow.
- Se configura una dirección IP para la interfaz de Capa 3 que envía paquetes sFlow. Sin embargo, los datagramas UDP con esta dirección IP de origen no pueden llegar al recopilador sFlow.
- El vínculo físico entre el dispositivo y el recopilador de sFlow falla. El
- recopilador sFlow está vinculado a una VPN inexistente.
- La longitud de un paquete sFlow es menor que la suma de los dos valores siguientes:
  - La longitud del encabezado del paquete sFlow.
  - El número de bytes que el muestreo de flujo puede copiar por paquete.

Solución

Para resolver el problema:

1. Utilizar el**mostrar flujo**comando para verificar que sFlow esté configurado correctamente.
2. Verifique que esté configurada una dirección IP correcta para que el dispositivo se comunique con el recopilador sFlow.
3. Verifique que el enlace físico entre el dispositivo y el recopilador sFlow esté activo.

4. Verifique que la VPN vinculada al recopilador sFlow ya exista.
5. Verifique que la longitud de un paquete sFlow sea mayor que la suma de los dos valores siguientes:
   - La longitud del encabezado del paquete sFlow.
   - La cantidad de bytes (como práctica recomendada, use el valor predeterminado) que el muestreo de flujo puede copiar por paquete.

Contenido

Configurar la captura de paquetes

Descripción general

La función de captura de paquetes captura los paquetes entrantes que se reenviarán a la CPU. La función muestra los paquetes capturados en tiempo real y le permite guardarlos en un archivo .pcap para análisis futuros.

La captura de paquetes admite filtros de captura y filtros de visualización. Puede utilizar expresiones para hacer coincidir paquetes para capturar o mostrar.

Elementos filtrantes

Un filtro de captura o visualización contiene una cadena de palabras clave o varias cadenas de palabras clave conectadas por operadores.

Las palabras clave incluyen los siguientes tipos:

- **Clasificatorios**—Cadenas de palabras clave fijas. Por ejemplo, debes utilizar el**IP**calificador para especificar el protocolo IPv4.
- **variables**—Valores suministrados por los usuarios en el formato requerido. Por ejemplo, puede configurar una dirección IP en 2.2.2.2 o cualquier otro valor válido.

Una variable debe ser modificada por uno o varios calificadores. Por ejemplo, para capturar cualquier paquete enviado desde el host en 2.2.2.2, use el filtro**host src 2.2.2.2**.

Los operadores incluyen los siguientes tipos:

- **Operadores logicos**—Realizar operaciones lógicas, como la operación AND. **Operadores**
- **aritméticos**—Realizar operaciones aritméticas, como la operación SUMA.
- **Operadores relacionales**—Indicar la relación entre cadenas de palabras clave. Por ejemplo, el**=** El operador indica igualdad.

Este documento proporciona información básica sobre estos elementos. Para obtener más información sobre los filtros de captura y visualización, visite los siguientes sitios web:

- http://wiki.wireshark.org/CaptureFilters .
- http://wiki.wireshark.org/DisplayFilters .

Capturar palabras clave de filtro

tabla 1yTabla 2Describe los calificadores y variables para los filtros de captura, respectivamente.

Tabla 17 Calificadores para filtros de captura

Categoría	Descripción	Ejemplos
Protocolo	Coincide con un protocolo. Si no especifica un calificador de protocolo, el filtro coincide con cualquier protocolo admitido.	- **arpía**—Coincide con ARP. - **ICMP**—Coincide con ICMP. - **IP**—Coincide con IPv4. - **ip6**—Coincide con IPv6. - **TCP**—Coincide con TCP. - **udp**—Coincide con la UDP.

Categoría	Descripción	Ejemplos
Dirección	Compara paquetes según su ubicación de origen o destino (una dirección IP o número de puerto). Si no especifica un calificador de dirección, el**src o dst**Se aplica el calificativo.	- **src**: coincide con el campo de dirección IP de origen. - **horario de verano**: coincide con el campo de dirección IP de destino. - **src o dst**: coincide con el campo de dirección IP de origen o destino. **NOTA:** El**src o dst**El calificador se aplica si no especifica un calificador de dirección. Por ejemplo, **puerto 23**es equivalente a**puerto src o dst 23**.
Tipo	Especifica el tipo de dirección.	- **anfitrión**: coincide con la dirección IP de un host. - **neto**: coincide con una subred IP. - **puerto**: coincide con un número de puerto de servicio. - **rango de puertos**: coincide con un rango de puertos de servicio. **NOTA:** El**anfitrión**El calificador se aplica si no especifica ningún tipo de calificador. Por ejemplo,**fuente 2.2.2.2**es equivalente a**host src 2.2.2.2**. Para especificar una subred IPv6, debe especificar el **neto**Calificatorio.
Otros	Cualquier otro calificador distinto a los calificados anteriormente descritos.	- **transmisión**—Coincide con paquetes de difusión. - **multidifusión**—Coincide con paquetes de multidifusión y difusión. - **menos**: coincide con paquetes que son menores o iguales a un tamaño específico. - **mayor que**: coincide con paquetes que son mayores o iguales a un tamaño específico. - **len**: coincide con la longitud del paquete. - **vlan**—Coincide con los paquetes VLAN.

NOTA:

El**transmisión**,**multidifusión**y todos los calificadores de protocolo no pueden modificar las variables.

Tabla 18 Tipos de variables para filtros de captura

Tipo de variable	Descripción	Ejemplos
Entero	Representado en notación binaria, octal, decimal o hexadecimal.	El**puerto 23**La expresión coincide con el tráfico enviado hacia o desde el puerto número 23.
rango de enteros	Representado por números enteros separados por guiones.	El**portrange 100-200**La expresión coincide con el tráfico enviado hacia o desde cualquier puerto en el rango de 100 a 200.
dirección IPv4	Representado en notación decimal con puntos.	El**fuente 1.1.1.1**La expresión coincide con el tráfico enviado desde el host IPv4 en 1.1.1.1.
dirección IPv6	Representado en notación hexadecimal de dos puntos.	El**horario de host 1::1**La expresión coincide con el tráfico enviado al host IPv6 en 1::1.
subred IPv4	Representado por un ID de red IPv4 o una dirección IPv4 con una máscara.	Las dos expresiones siguientes coinciden con el tráfico enviado hacia o desde la subred IPv4 1.1.1.0/24: - **fuente 1.1.1**. - **src neto 1.1.1.0/24**.

Tipo de variable	Descripción	Ejemplos
red IPv6 segmento	Representado por una dirección IPv6 con una longitud de prefijo.	El**horario de verano neto 1::/64**La expresión coincide con el tráfico enviado a la red IPv6 1::/64.

Operadores de filtro de captura

Los filtros de captura admiten operadores lógicos (Tabla 3), operadores aritméticos (Tabla 4) y operadores relacionales (Tabla 5). Los operadores lógicos pueden utilizar símbolos alfanuméricos y no alfanuméricos. Los operadores aritméticos y relacionales sólo pueden utilizar símbolos no alfanuméricos.

Los operadores lógicos son asociativos por izquierda. Se agrupan de izquierda a derecha. El**no**El operador tiene la máxima prioridad. El**y**y**o**los operadores tienen la misma prioridad.

Tabla 19 Operadores lógicos para filtros de captura

No alfanumérico símbolo ic	Alfanumérico símbolo	Descripción
!	no	Invierte el resultado de una condición. Utilice este operador para capturar el tráfico que coincida con el valor opuesto de una condición. Por ejemplo, para capturar tráfico que no sea HTTP, utilice**no el puerto 80**.
&&	y	Une dos condiciones. Utilice este operador para capturar el tráfico que coincida con ambas condiciones. Por ejemplo, para capturar tráfico no HTTP que se envía hacia o desde 1.1.1.1, utilice**host 1.1.1.1 y no el puerto 80**.
||	o	Une dos condiciones. Utilice este operador para capturar el tráfico que coincida con cualquiera de las condiciones. Por ejemplo, para capturar el tráfico que se envía hacia o desde 1.1.1.1 o 2.2.2.2, utilice**anfitrión 1.1.1.1 o anfitrión 2.2.2.2**.

Tabla 20 Operadores aritméticos para filtros de captura

No alfanumérico símbolo	Descripción
+	Agrega dos valores.
-	Resta un valor de otro.
*	Multiplica un valor por otro.
/	Divide un valor por otro.
&	Devuelve el resultado de la operación AND bit a bit sobre dos valores integrales en forma binaria.
|	Devuelve el resultado de la operación OR bit a bit en dos valores integrales en forma binaria.
<<	Realiza la operación de desplazamiento bit a izquierda en el operando a la izquierda del operador. El operando de la derecha especifica el número de bits a desplazar.
> >	Realiza la operación de desplazamiento bit a derecha en el operando a la izquierda del operador. El operando de la derecha especifica el número de bits a desplazar.
[ ]	Especifica un desplazamiento de bytes relativo a una capa de protocolo. Este desplazamiento indica el byte donde comienza la coincidencia. Debe incluir el valor de compensación entre corchetes y especificar un calificador de protocolo. Por ejemplo,**IP[6]**coincide con el séptimo byte de la carga útil en los paquetes IPv4 (el byte que está a seis bytes del comienzo de la carga útil IPv4).

Tabla 21 Operadores relacionales para filtros de captura

No alfanumérico símbolo	Descripción
=	Igual a. Por ejemplo,**ip[6]=0x1c**coincide con un paquete IPv4 si su séptimo byte de carga útil es igual a 0x1c.
!=	No igual a. Por ejemplo,**longitud!=60**coincide con un paquete si su longitud no es igual a 60 bytes.
>	Mas grande que. Por ejemplo,**longitud>100**coincide con un paquete si su longitud es superior a 100 bytes.
<	Menos que. Por ejemplo,**longitud<100**coincide con un paquete si su longitud es inferior a 100 bytes.
> =	Mayor qué o igual a. Por ejemplo,**longitud>=100**coincide con un paquete si su longitud es mayor o igual a 100 bytes.
<=	Menos que o igual a. Por ejemplo,**longitud<=100**coincide con un paquete si su longitud es menor o igual a 100 bytes.

Mostrar palabras clave de filtro

Tabla 6yTabla 7Describe los calificadores y variables para los filtros de visualización, respectivamente.

Tabla 22 Calificadores para filtros de visualización

Categoría	Descripción	Ejemplos
Protocolo	Coincide con un protocolo.	- **ética**—Coincide con Ethernet. - **ftp**—Coincide con FTP. - **http**—Coincide con HTTP. - **ICMP**—Coincide con ICMP. - **IP**—Coincide con IPv4. - **ipv6**—Coincide con IPv6. - **TCP**—Coincide con TCP. - **Telnet**—Coincide con Telnet. - **udp**—Coincide con la UDP.
campo de paquete	Coincide con un campo en paquetes usando una cadena de puntos en el *protocolo.campo[.subcampo nivel1]...[.subcampo nivelado]*formato.	- **tcp.flags.syn**—Coincide con el bit SYN en el campo de banderas de TCP. - **puerto.tcp**: coincide con el campo del puerto de origen o de destino.

NOTA:

Los calificadores de protocolo no pueden modificar variables.

Tabla 23 Tipos de variables para filtros de visualización

Variable tipo	Descripción
Entero	Representado en notación binaria, octal, decimal o hexadecimal. Por ejemplo, para mostrar paquetes IP de 1500 bytes o menos, utilice una de las siguientes expresiones: - **ip.len le 1500**. - **ip.len le 02734**. - **ip.len le 0x436**.
Booleano	Este tipo de variable tiene dos valores: verdadero o falso. Este tipo de variable se aplica si utiliza solo una cadena de campo de paquete para identificar la presencia de un campo en un paquete. - Si el campo está presente, el resultado del partido es verdadero. El filtro muestra el paquete. - Si el campo no está presente, el resultado de la coincidencia es falso. El filtro no muestra el paquete. Por ejemplo, para mostrar paquetes TCP que contienen el campo SYN, utilice**tcp.flags.syn**.
MAC dirección (seis bytes)	Utiliza dos puntos (:), puntos (.) o guiones (-) para dividir la dirección MAC en dos o cuatro segmentos. Por ejemplo, para mostrar paquetes que contienen una dirección MAC de destino ffff.ffff.ffff, utilice una de las siguientes expresiones: - **eth.dst==ff:ff:ff:ff:ff:ff**. - **eth.dst==ff-ff-ff-ff-ff-ff**. - **eth.dst ==ffff.ffff.ffff**.
IPv4 DIRECCIÓN	Representado en notación decimal con puntos. Por ejemplo: - Para mostrar paquetes IPv4 que se envían hacia o desde 192.168.0.1, utilice**dirección.ip==192.168.0.1**. - Para mostrar paquetes IPv4 que se envían hacia o desde 129.111.0.0/16, use **dirección.ip==129.111.0.0/16**.
IPv6 DIRECCIÓN	Representado en notación hexadecimal de dos puntos. Por ejemplo: - Para mostrar paquetes IPv6 que se envían hacia o desde 1::1, utilice**ipv6.dirección==1::1**. Para - mostrar paquetes IPv6 que se envían hacia o desde 1::/64, utilice**ipv6.dirección==1::/64**.
Cadena	Cadena de caracteres. Por ejemplo, para mostrar paquetes HTTP que contienen la cadena**HTTP/1.1**para el campo de versión de solicitud, utilice**http.request.version=="HTTP/1.1"**.

Operadores de filtro de visualización

Los filtros de visualización admiten operadores lógicos (Tabla 8) y operadores relacionales (Tabla 9). Ambos tipos de operadores pueden utilizar símbolos alfanuméricos y no alfanuméricos.

Los operadores lógicos son asociativos por izquierda. Se agrupan de izquierda a derecha.Tabla 8muestra los operadores lógicos por prioridad, de mayor a menor. El**y**y**o**los operadores tienen la misma prioridad:

Tabla 24 Operadores lógicos para filtros de visualización

No alfanuméricos C símbolo	Alfanumérico símbolo	Descripción
[ ]	Sin alfanuméricos el símbolo es disponible.	Se utiliza con calificadores de protocolo. Para más información, ver "La expresión proto[...]".

No alfanuméricos C símbolo	Alfanumérico símbolo	Descripción
!	no	Muestra paquetes que no coinciden con la condición conectada a este operador.
&&	y	Une dos condiciones. Utilice este operador para mostrar el tráfico que coincida con ambas condiciones.
||	o	Une dos condiciones. Utilice este operador para mostrar el tráfico que coincida con cualquiera de las condiciones.

Tabla 25 Operadores relacionales para filtros de visualización

No alfanumérico símbolo	Alfanumérico símbolo	Descripción
==	ecuación	Igual a. Por ejemplo,**ip.src==10.0.0.5**muestra paquetes con la dirección IP de origen como 10.0.0.5.
!=	nordeste	No igual a. Por ejemplo,**ip.src!=10.0.0.5**muestra paquetes cuya dirección IP de origen no es 10.0.0.5.
>	gt	Mas grande que. Por ejemplo,**marco.len>100**muestra fotogramas con una longitud superior a 100 bytes.
<	es	Menos que. Por ejemplo,**marco.len<100**muestra fotogramas con una longitud inferior a 100 bytes.
> =	ge	Mayor qué o igual a. Por ejemplo,**frame.len ge 0x100**muestra fotogramas con una longitud mayor o igual a 256 bytes.
<=	le	Menos que o igual a. Por ejemplo,**frame.len le 0x100**muestra fotogramas con una longitud inferior o igual a 256 bytes.

Construyendo un filtro de captura

Esta sección proporciona los tipos de expresión más utilizados para filtros de captura.

expresión lógica

Utilice este tipo de expresión para capturar paquetes que coincidan con el resultado de operaciones lógicas.

Las expresiones lógicas contienen palabras clave y operadores lógicos. Por ejemplo:

- **ni el puerto 23 ni el puerto 22**—Captura paquetes con un número de puerto que no es 23 o 22. **puerto**
- **23 o icmp**—Captura paquetes con un número de puerto 23 o paquetes ICMP.

En una expresión lógica, un calificador puede modificar más de una variable conectada por su operador lógico más cercano. Por ejemplo, para capturar paquetes procedentes de la dirección IPv4 192.168.56.1 o la red IPv4 192.168.27, utilice cualquiera de las siguientes expresiones:

- **fuente 192.168.56.1 o 192.168.27**.

- **fuente 192.168.56.1 o fuente 192.168.27**.

El*expr relop expr*expresión

Utilice este tipo de expresión para capturar paquetes que coincidan con el resultado de operaciones aritméticas.

Esta expresión contiene palabras clave, operadores aritméticos (*exprés*) y operadores relacionales (*relop*). Por ejemplo, **longitud+100>=200**captura paquetes que son mayores o iguales a 100 bytes.

El*prototipo*[*exprés*:*tamaño*]expresión

Utilice este tipo de expresión para capturar paquetes que coincidan con el resultado de operaciones aritméticas en una cantidad de bytes en relación con una capa de protocolo.

Este tipo de expresión contiene los siguientes elementos:

- *proto*—Especifica una capa de protocolo.
- []: realiza operaciones aritméticas en una cantidad de bytes relacionados con la capa de protocolo.
- *exprés*: especifica la expresión aritmética.
- *tamaño*: especifica el desplazamiento de bytes. Este desplazamiento indica el número de bytes relativos a la capa de protocolo. La operación se realiza en los bytes especificados. El desplazamiento se establece en 1 byte si no especifica un desplazamiento.

Por ejemplo,**ip[0]&0xf !=5**captura un paquete IP si el resultado de aplicar AND al primer byte con 0x0f no es 5.

Para hacer coincidir un campo, puede especificar un nombre de campo para*exprés*:*tamaño*. Por ejemplo,**icmp[tipo icmp]=0x08**captura paquetes ICMP que contienen un valor de 0x08 en el campo Tipo.

la vlan*vlan_id*expresión

Utilice este tipo de expresión para capturar el tráfico VLAN etiquetado 802.1Q.

Este tipo de expresión contiene la**vlan***vlan_id*palabras clave y operadores lógicos. El*vlan_id*La variable es un número entero que especifica una ID de VLAN. Por ejemplo,**vlan 1 e ip6**Captura paquetes IPv6 en la VLAN 1.

Para capturar el tráfico etiquetado 802.1Q, debe utilizar el**vlan***vlan_id*expresión antes que cualquier otra expresión. Una expresión coincide con paquetes sin etiquetar si no sigue una**vlan***vlan_id*expresión. Por ejemplo:

- **vlan 1 y !tcp—Captura paquetes no TCP etiquetados con VLAN 1.**
- **icmp y vlan 1**—Captura paquetes ICMP sin etiquetar que están etiquetados con VLAN 1. Esta expresión no captura ningún paquete porque ningún paquete se puede etiquetar y desetiquetar al mismo tiempo.

Construyendo un filtro de visualización

Esta sección proporciona los tipos de expresión más utilizados para los filtros de visualización.

expresión lógica

Utilice este tipo de expresión para mostrar paquetes que coincidan con el resultado de operaciones lógicas.

Las expresiones lógicas contienen palabras clave y operadores lógicos. Por ejemplo,**ftp o icmp**muestra todos los paquetes FTP y paquetes ICMP.

expresión relacional

Utilice este tipo de expresión para mostrar paquetes que coincidan con el resultado de las operaciones de comparación.

Las expresiones relacionales contienen palabras clave y operadores relacionales. Por ejemplo,**ip.len<=28**muestra paquetes IP que contienen un valor de 28 bytes o menos en el campo de longitud.

Expresión de campo de paquete

Utilice este tipo de expresión para mostrar paquetes que contengan un campo específico.

Las expresiones de campos de paquetes contienen sólo cadenas de campos de paquetes. Por ejemplo,**tcp.flags.syn**muestra todos los paquetes TCP que contienen el campo de bits SYN.

El*prototipo*[...] expresión

Utilice este tipo de expresión para mostrar paquetes que contienen valores de campo

específicos. Este tipo de expresión contiene los siguientes elementos:

- *proto*—Especifica una capa de protocolo o campo de paquete.
- [...]: coincide con una cantidad de bytes relacionados con una capa de protocolo o campo de paquete. Los valores de los bytes que deben coincidir deben ser una cadena entera hexadecimal. La expresión entre paréntesis puede utilizar los siguientes formatos:
  - [*norte*:*metro*]—Coincide con un total de*metro*bytes después de un desplazamiento de*norte*bytes desde el principio de la capa o campo de protocolo especificado. Para hacer coincidir solo 1 byte, puede utilizar los formatos [n] y [n:1]. Por ejemplo,**eth.src[0:3]==00:00:83**coincide con una trama Ethernet si los primeros tres bytes de su dirección MAC de origen son 0x00, 0x00 y 0x83. El**eth.src[2] == 83**La expresión coincide con una trama Ethernet si el tercer byte de su dirección MAC de origen es 0x83.
  - [*norte-metro*]: coincide con un total de (*m-n+1*) bytes, comenzando desde (*norte+1*)º byte relativo al comienzo de la capa de protocolo o campo de paquete especificado. Por ejemplo,**eth.src[1-2]==00:83** coincide con una trama Ethernet si el segundo y tercer byte de su dirección MAC de origen son 0x00 y 0x83, respectivamente.

Restricciones y pautas de configuración

Cuando configure la captura de paquetes, siga estas restricciones y pautas:

- Para utilizar la función de captura de paquetes, debe instalar la imagen de la función utilizando el**cargador de arranque** o**instalar**dominio. El archivo de imagen característica utiliza S7500E-CMW710-PACKET-CAPTURE-*versión* Formato .bin, por ejemplo, S7500E-CMW710-PACKET-CAPTURE-A7145.bin. Para obtener información sobre la versión de la imagen de función que coincide con su dispositivo, consulte las notas de la versión. Para obtener más información sobre los comandos, consulte*Referencia de comandos fundamentales*.

Lista de tareas de configuración de captura de paquetes

Tareas de un vistazo	Observaciones
(Requerido.)Capturando paquetes	N / A
(Opcional.)Mostrar el contenido de un archivo de paquete	Esta tarea solo está disponible si configura la captura para guardar paquetes en un archivo.

Capturando paquetes

IMPORTANTE:

Para capturar o mostrar los paquetes deseados, asegúrese de que las expresiones del filtro no entren en conflicto. El sistema no busca errores lógicos.

La captura de paquetes captura solo los paquetes que se reenvían a través de la CPU. Para capturar paquetes que se reenvían a través de chips, debe configurar la duplicación de flujo para reflejar los paquetes en la CPU. Para obtener más información sobre la duplicación de flujo, consulte "Configuración de la duplicación de flujo".

La captura muestra los paquetes capturados en tiempo real. Puede configurar la captura para guardar los paquetes capturados en un archivo o filtrar los paquetes para mostrarlos.

No puede configurar el dispositivo desde la CLI mientras la captura está en funcionamiento. Para detener la captura mientras captura paquetes, presione**Ctrl+C**. Es posible que haya un retraso hasta que se detenga la captura debido al tráfico intenso.

Para capturar paquetes:

Tarea	Dominio
Capture paquetes entrantes en una interfaz.	- Guarde los paquetes capturados en un archivo: **interfaz de captura de paquetes***tipo de interfaz número de interfaz* [**filtro de captura***expresión-capt* |**límite-de-fotogramas-capturados***límite*| **límite-tamaño-del-marco***bytes*|**tamaño de archivo de parada automática***kilobytes*|**duración de la parada automática** *segundos*|**archivos de parada automática***números*|**tamaño de archivo del búfer de anillo de captura** *kilobytes*|**duración del buffer de anillo de captura***segundos*|**archivos de búfer de anillo de captura***números*] ***escribir** *ruta de archivo*[**crudo**| {**breve**|**verboso**}] * - Filtrar paquetes para mostrar: **interfaz de captura de paquetes***tipo de interfaz número de interfaz* [**filtro de captura***expresión-capt*|**filtro de visualización***expresión-disp*| **límite-de-fotogramas-capturados***límite*|**límite-tamaño-del-marco***bytes*|**duración de la parada automática***segundos*] * [**crudo**| {**breve**|**verboso**}] *

Mostrar el contenido de un archivo de paquete

Tarea	Dominio	Observaciones
Muestra el contenido de un archivo de paquete.	**lectura de captura de paquetes***ruta de archivo*[**verboso**] [**filtro de visualización***expresión-disp*] [**crudo**| {**breve**|**verboso**}] *	Un archivo de paquete debe usar la extensión .pcap o .pcapng.

Ejemplos de configuración de captura de paquetes

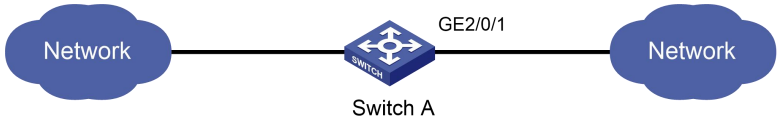
Ejemplo de configuración básica de captura de paquetes

Requisitos de red

Como se muestra enFigura 1, capture los siguientes paquetes IP entrantes en GigabitEthernet 2/0/1:

- Paquetes reenviados a través de la CPU.
- Paquetes que provienen de 192.168.56.1 0 y se reenvían a través de chips.

Figura 71 Diagrama de red



Procedimiento de configuración

Cree una ACL avanzada de IPv4 para hacer coincidir los paquetes que provienen de 192.168.56.1 0.

<SwitchA> vista del sistema

[SwitchA] número de lista 3000

La regla [SwitchA-acl-adv-3000] permite la fuente de IP 192.168.56.1 0 [SwitchA-acl-adv-3000] sale

Configure un comportamiento de tráfico para reflejar el tráfico en la CPU.

[SwitchA] comportamiento del tráfico comportamiento1

[SwitchA-behavior-behavior1] duplicar a la CPU [SwitchA-behavior-behavior1] salir

Configure una clase de tráfico para usar la ACL para hacer coincidir el tráfico.

[CambiarA] clasificador de tráfico clasificador1 [Cambiar-clasificador-clasificador1] if-match acl 3000 [Cambiar-clasificador-clasificador1] salir

Asociar la clase de tráfico con el comportamiento del tráfico en una política de QoS.

[CambiarA] política qos usuario1
[SwitchA-qospolicy-user1] clasificador clasificador1 comportamiento comportamiento1
[SwitchA-qospolicy-user1] salir

Aplicar la política de QoS al tráfico entrante de GigabitEthernet 2/0/1.

[SwitchA] interfaz gigabitethernet 2/0/1 [SwitchA-GigabitEthernet2/0/1] qos aplicar política usuario1 entrante [SwitchA-GigabitEthernet2/0/1] salir

[Cambiar A] salir

Capture el tráfico entrante en GigabitEthernet 2/0/1.

<SwitchA> interfaz de captura de paquetes gigabitethernet 2/0/1
Capturando en 'Gigabitethernet2/0/1'
1 0.000000 192.168.56.1 -> 192.168.56.2 TCP 62 6325 > telnet [SYN] Seq=0 Win =65535 Len=0 MSS=1460 SACK_PERM=1
2 0.000061 192.168.56.1 -> 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=1 Ack =1 Win=65535 Len=0

3 0.024370 192.168.56.1 -> 192.168.56.2 TELNET 60 Datos Telnet ... 0.024449 192.168.56.1 ->
4 192.168.56.2 TELNET 78 Datos Telnet ... 0.025766 192.168.56.1 -> 192 .168.56.2 TELNET 65 Datos
5 Telnet... 0.035096 192.168 .56.1 -> 192.168.56.2 TELNET 60 Datos Telnet ... 0.047317 192.168.56.1 ->
6 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=42 Ac Win=65102 Len=0
7
k=434
8 0.050994 192.168.56.1 -> 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=42 Ac Win=65100 Len=0
k=436
9 0.052401 192.168.56.1 -> 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=42 Ac Win=65098 Len=0
k=438
10 0.057736 192.168.56.1 -> 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=42 Ac Win=65096 Len=0
k=440
10 paquetes capturados

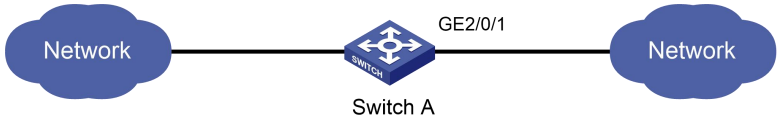
Ejemplo de configuración de visualización de archivos de paquetes

Requisitos de red

Como se muestra enFigura 2:

- Capture 10 paquetes entrantes en GigabitEthernet 2/0/1 y guárdelos en un archivo de paquetes. Mostrar el
- contenido del archivo.

Figura 72 Diagrama de red



Procedimiento de configuración

Capturar paquetes en GigabitEthernet 2/0/1. Establezca el número máximo de paquetes capturados en 10. Guarde los paquetes en el archivo**flash:/a.pcap**.

<SwitchA> interfaz de captura de paquetes gigabitethernet 2/0/1 límite de fotogramas capturados 10 escritura flash:/a.pcap

Capturando en 'Gigabitethernet2/0/1'

Muestra el contenido del archivo del paquete.

<SwitchA> lectura de captura de paquetes flash:/a.pcap

1 0.000000 192.168.56.1 -> 192.168.56.2 TCP 62 6325 > telnet [SYN] Seq=0 Win =65535 Len=0 MSS=1460 SACK_PERM=1

2 0.000061 192.168.56.1 -> 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=1 Ack =1 Win=65535 Len=0

3 0.024370 192.168.56.1 -> 192.168.56.2 TELNET 60 Datos Telnet ... 0.024449 192.168.56.1 ->

4 192.168.56.2 TELNET 78 Datos Telnet ... 0.025766 192.168.56.1 -> 192 .168.56.2 TELNET 65 Datos

5 Telnet... 0.035096 192.168 .56.1 -> 192.168.56.2 TELNET 60 Datos Telnet ... 0.047317 192.168.56.1 ->

6 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=42 Ac Win=65102 Len=0

7

k=434

8 0.050994 192.168.56.1 -> 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=42 Ac Win=65100 Len=0

k=436

9 0.052401 192.168.56.1 -> 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=42 Ac Win=65098 Len=0

k=438

10 0.057736 192.168.56.1 -> 192.168.56.2 TCP 60 6325 > telnet [ACK] Seq=42 Ac Win=65096 Len=0

k=440