Información importante sobre los comandos de depuración

Contenido

Introducción

Este documento describe las pautas generales sobre el uso de debug comandos, incluido el debug ip packet comando disponible en las plataformas Cisco IOS®.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conexión al router utilizando los puertos de consola, auxiliares y vty

- Problemas generales de configuración de Cisco IOS
- Interpretación de resultados de depuración de Cisco IOS

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

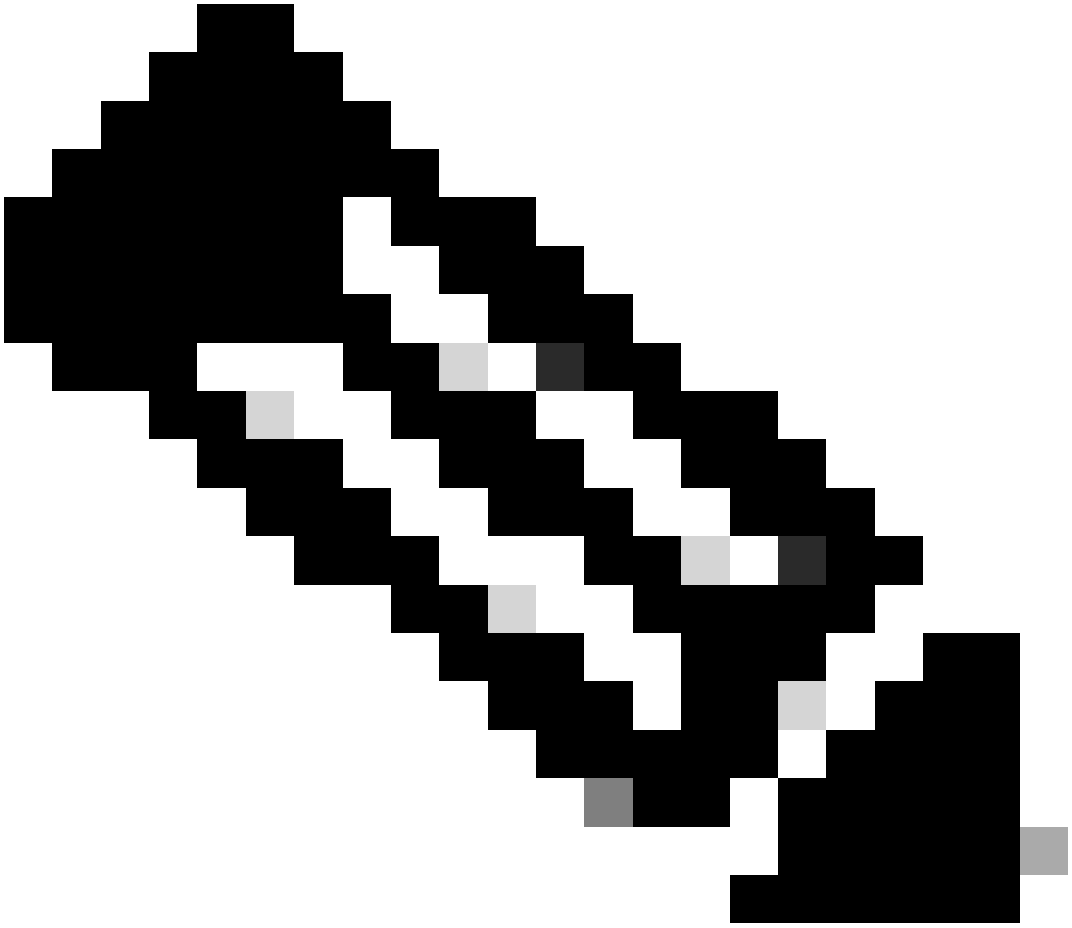
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Esta página proporciona algunas pautas generales sobre el uso de los debugs disponibles en las plataformas del IOS de Cisco, así como ejemplos para el uso correcto **debug ip packet** del comando y la depuración condicional.



Nota: Este documento no explica cómo utilizar e interpretar comandos y salidas de debug específicos. Refiérase a la documentación apropiada de Referencia de Comandos Debug de Cisco para obtener información sobre los comandos debug específicos.

El resultado **debug** de los comandos EXEC privilegiados proporciona información de diagnóstico que incluye una variedad de eventos de interconexión de redes relacionados con el estado del protocolo y la actividad de la red en general.

Advertencias

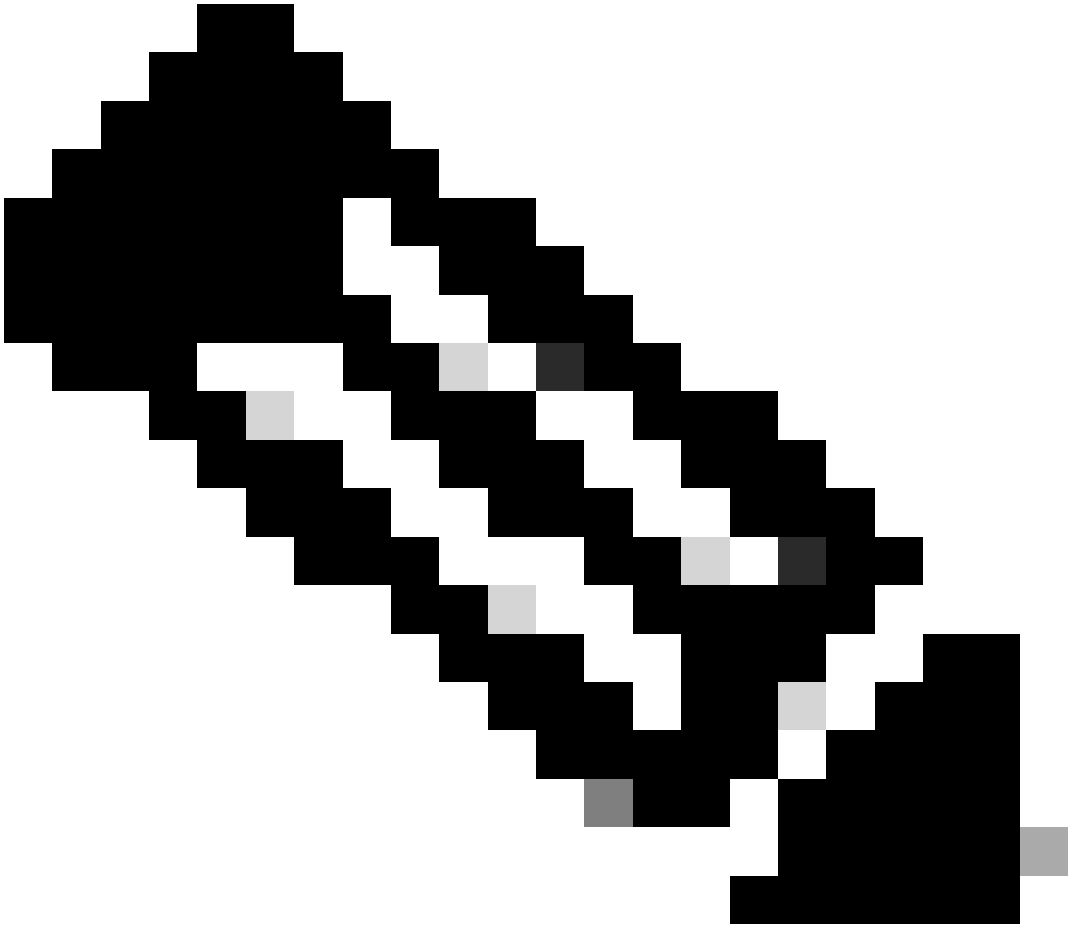
debug Usecomands con precaución. En general, se recomienda que estos comandos se utilicen sólo bajo la dirección del representante de soporte técnico de su router cuando se intenta resolver problemas específicos.

La habilitación de la depuración puede interrumpir el funcionamiento del router cuando las redes interconectadas experimentan condiciones de

carga elevadas. Por lo tanto, si el registro está activado, el servidor de acceso puede congelarse intermitentemente tan pronto como el puerto de la consola se sobrecargue con mensajes de registro.

Antes de iniciar un **debug** comando, tenga siempre en cuenta el resultado que este comando puede generar y el tiempo que puede tardar. Por ejemplo, si tiene un router con una interfaz de velocidad básica (BRI), **debug isdn q931** probablemente no dañe el sistema. Sin embargo, hacer la misma depuración en un AS5800 con configuración E1 completa probablemente puede generar tanta entrada que puede bloquearse y dejar de responder.

Antes de depurar, observe la carga de la CPU con **show processes cpu** el comando. Verifique que tenga suficiente CPU disponible antes de comenzar las depuraciones. Consulte Resolución de problemas por uso excesivo de CPU en routers de Cisco para obtener más información. Por ejemplo, si tiene un router Cisco 7200 con una interfaz ATM haciendo bridging, entonces, dependiendo de la cantidad de subinterfaces configuradas, reiniciar el router puede utilizar gran parte de su CPU. La causa aquí es que, para cada circuito virtual (VC),se necesita generar un paquete de unidad de datos del protocolo de puente (BPDU). Iniciar depuraciones durante un tiempo tan crítico puede hacer que la utilización de la CPU aumente drásticamente y resulte en un bloqueo o en una pérdida de conectividad de red.



Nota: Cuando se ejecutan los debugs, generalmente no ve el mensaje del router, especialmente cuando el debug es intensivo. Pero, en la mayoría de los casos, puede utilizar los comandos no debug all o undebug all para detener las depuraciones. Consulte la sección Obtención de resultados de depuración para obtener más información sobre el uso seguro de las depuraciones.

Antes de la depuración

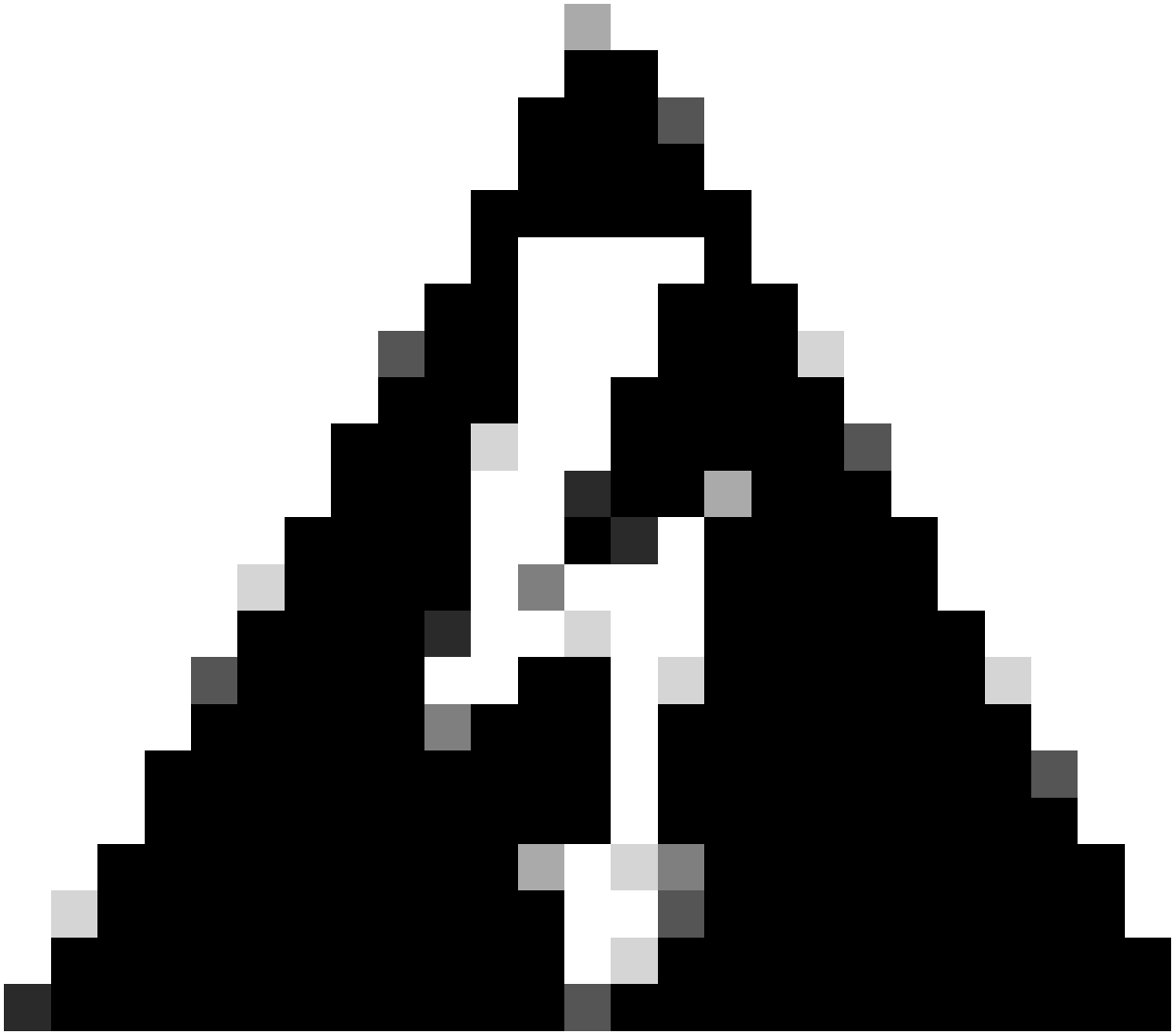
Además de los puntos mencionados arriba, asegúrese de comprender el impacto de las depuraciones en la estabilidad de la plataforma. También debe considerar a qué interfaz del router debe conectarse. Esta sección incluye algunas pautas.

Cómo obtener las salidas de los depuradores

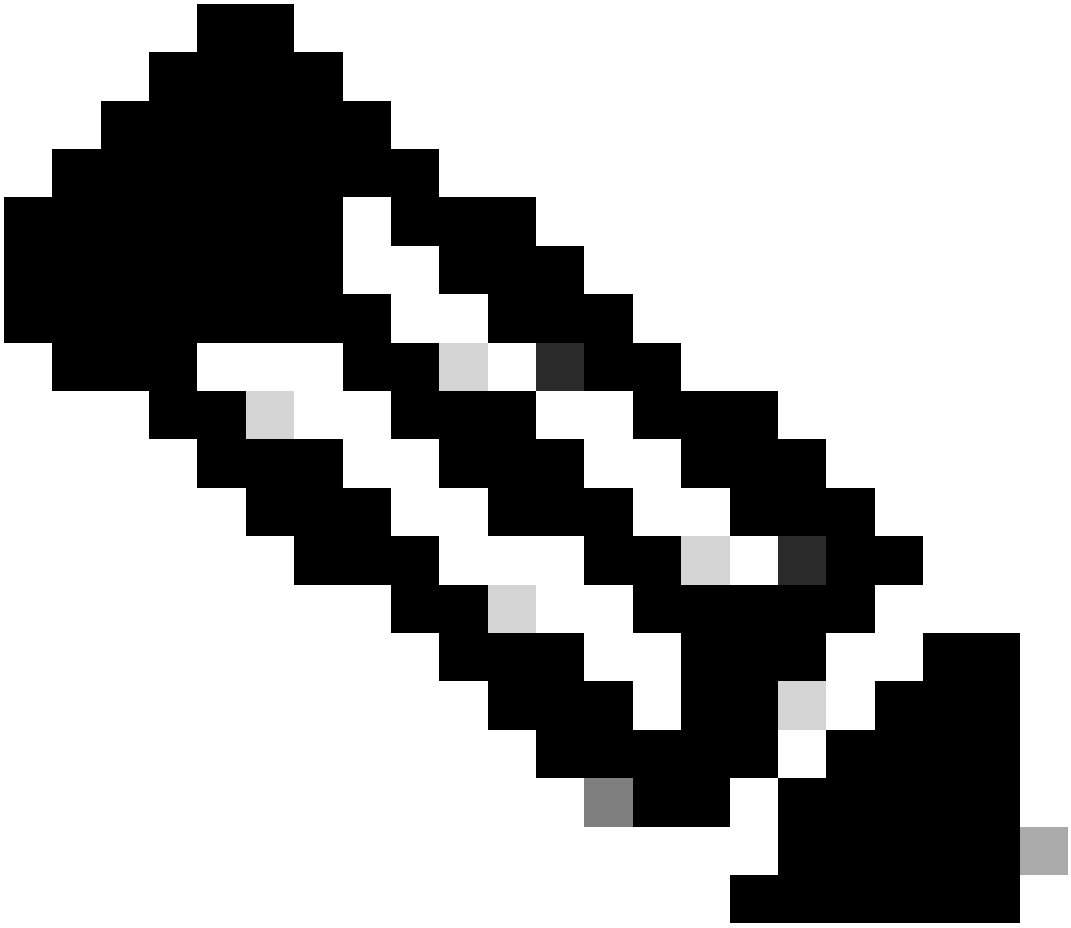
Los routers pueden mostrar resultados de depuración para diversas interfaces, dentro de los cuales se encuentran los puertos de consola, auxiliares y vty. Los routers también pueden registrar mensajes a un búfer interno, a un servidor syslog unix externo. A continuación se explican las instrucciones y advertencias de cada método:

Puerto de consola

Si está conectado a la consola, en configuraciones normales, no es necesario realizar ningún trabajo adicional. El resultado de la depuración debe mostrarse automáticamente. Sin embargo, asegúrese de **logging console level** que esté configurado como desee y de que el registro no se haya deshabilitado con **no logging console** el comando.



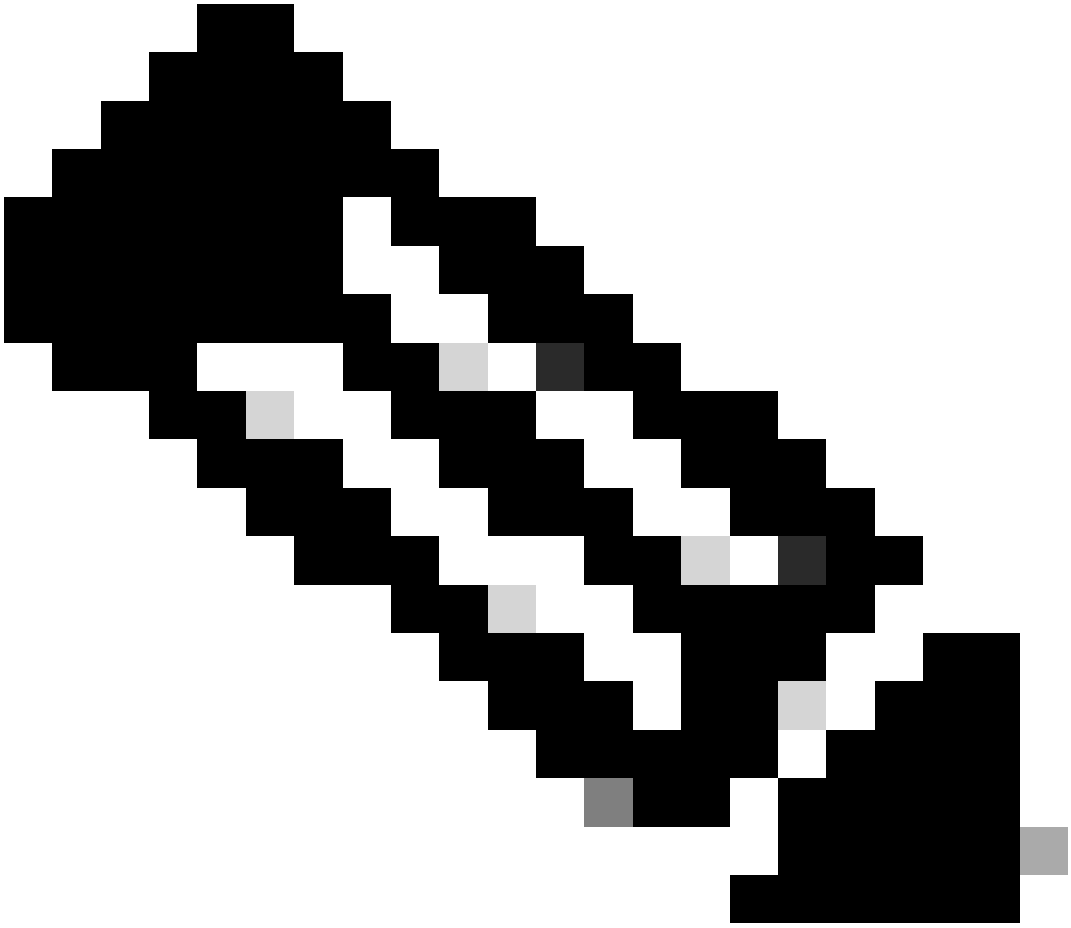
Advertencia: Las depuraciones excesivas en el puerto de consola de un router pueden hacer que se bloquee. Esto se debe a que el router da prioridad automáticamente a la salida de la consola por encima de otras funciones del router. Por lo tanto, si el router está procesando una salida de depuración grande al puerto de la consola, puede bloquearse. Por lo tanto, si el resultado de la depuración es excesivo, utilice los puertos vty (telnet) o las memorias intermedias de registro para obtener sus depuraciones. A continuación se proporciona más información.



Nota: de forma predeterminada, el registro está habilitado en el puerto de la consola. Por lo tanto, el puerto de la consola siempre procesa el resultado de la depuración aunque se estuviese utilizando otro puerto u método (como Aux, vty o búfer) para capturar el resultado. Es por ello que Cisco recomienda que, bajo condiciones normales de funcionamiento, tenga habilitado el comando no logging console en todo momento y use otros métodos para capturar depuraciones. En situaciones en las que necesite usar la consola, vuelva a activar temporalmente el registro de consola.

Puerto auxiliar

Si está conectado a través de un puerto auxiliar, escriba **terminal monitor** el comando. Verifique también que **no logging on** el comando no se haya activado en el router.



Nota: Si utiliza el puerto auxiliar para monitorear el router, tenga en cuenta que, cuando el router se reinicia, el puerto auxiliar no muestra la salida de la secuencia de inicio. Conéctese al puerto de la consola para ver la secuencia de arranque.

Puertos VTY

Si está conectado a través de un puerto auxiliar o de telnet, escriba **terminal monitor** el comando. Compruebe también que **no logging on** no se ha utilizado el comando.

Registro de mensajes en una memoria intermedia interna

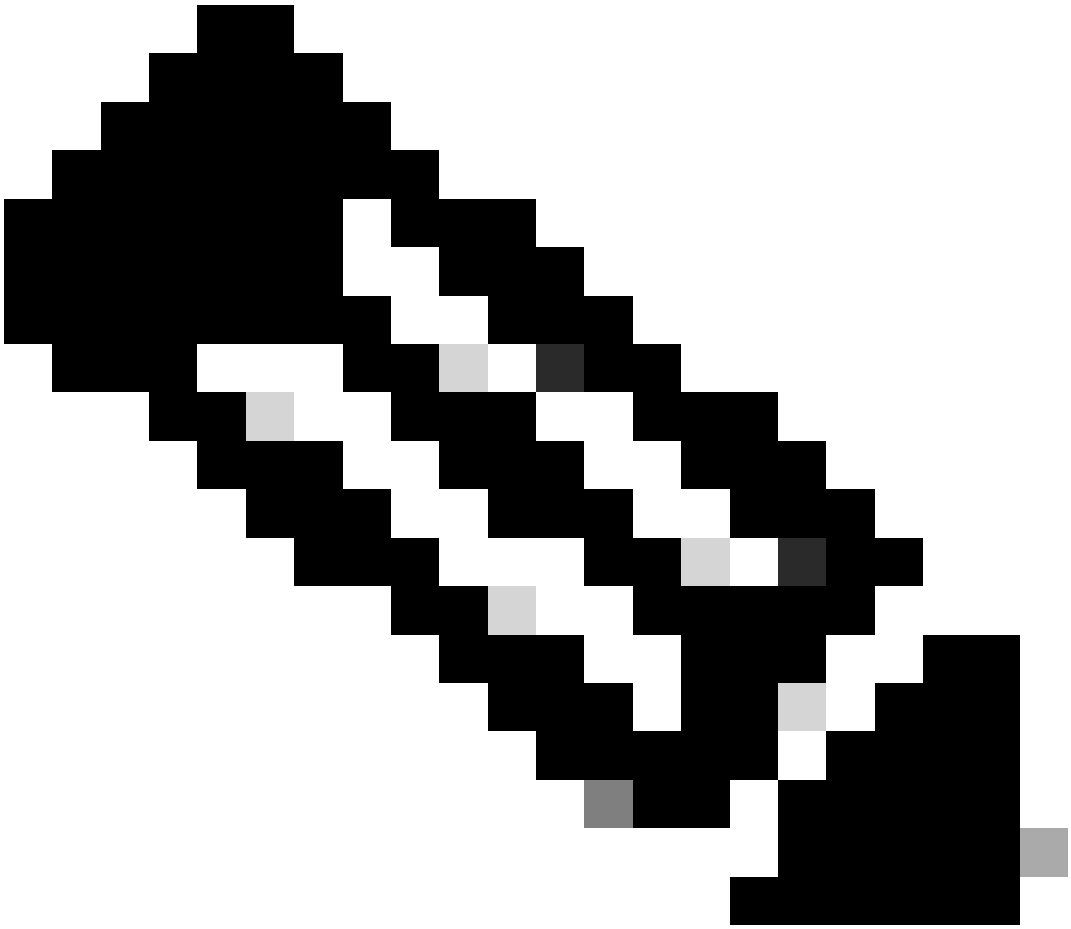
El dispositivo de registro predeterminado es la consola; todos los mensajes se muestran en la consola a menos que se especifique lo contrario.

Para registrar mensajes en un búfer interno, utilice el **logging buffered** comando de configuración outer. Esta es la sintaxis completa de este comando:

<#root>

logging buffered no logging buffered

logging buffered El comando copia los mensajes de registro en un búfer interno en lugar de escribirlos en la consola. El búfer es originalmente circular, por lo que los mensajes nuevos sobrescriben a los anteriores. Para mostrar los mensajes que se registran en el búfer, utilice el comando **show logging** EXEC privilegiado. El primer mensaje mostrado es el más antiguo del buffer. Puede especificar el tamaño del búfer así como el nivel de gravedad de los mensajes que ingresarán al registro.



Nota: Asegúrese de que hay suficiente memoria disponible en el cuadro antes de introducir el tamaño del búfer. Utilice el comando Cisco IOS show proc mem para ver la memoria disponible.

---

no logging buffered El comando cancela el uso del búfer y escribe mensajes en la consola (valor predeterminado).

Mensajes de registro a un servidor UNIX Syslog.

Para registrar mensajes en el host del servidor Syslog, utilice el comando logging router configuration. La sintaxis completa de este comando es la siguiente:

<#root>

```
logging <ip-address> no logging <ip-address>
```

loggingEl comando identifica un host del servidor syslog para recibir mensajes de registro. El argumento < ip-address> es la dirección IP del host. Si se ejecuta este comando más de una vez, se crea una lista de servidores Syslog que reciben los mensajes de registro.

no logging El comando elimina el servidor syslog con la dirección especificada de la lista de syslogs.

Otras tareas previas a la depuración

- Configure su software de emulador de terminal (por ejemplo, HyperTerminal) de modo que pueda capturar la salida de debug a un archivo. Por ejemplo, en HyperTerminal, haga clic**Transfer** en, a continuación, haga clic **Capture Text** en y elija las opciones adecuadas. Para obtener más información, refiérase a Captura de la Salida de Texto desde Hyper Terminal. Para otro software de emulador de terminal, refiérase a la documentación del software.

- Habilite las marcas de hora en milisegundos (mseg) mediante **service timestamps** el comando:

<#root>

```
router(config)#
```

```
service timestamps debug datetime msec
```

```
router(config)#
```

```
service timestamps log datetime msec
```

Estos comandos agregan marcas de tiempo a las depuraciones con el formato MMM DD HH:MM:SS, lo que indica la fecha y la hora según el reloj del sistema. Si el reloj del sistema no ha sido configurado, un asterisco (*) precede la fecha y hora para indicar que es probable que estos datos no sean correctos.

Por lo general, es aconsejable configurar sellos de hora en milisegundos, ya que esto brinda un nivel alto de claridad al analizar los resultados de la depuración. Los sellos de fecha y hora en milisegundos proporcionan una mejor indicación de la sincronización de los diversos eventos de debug entre sí. Sin embargo, tenga en cuenta que, cuando el puerto de la consola emite muchos mensajes, no pueden correlacionarse con la temporización real del evento. Por ejemplo, si **debug x25** habilita all en un cuadro que tiene 200 VC y la salida se registra en el buffer (mediante **no logging console logging buffered** los comandos theandy), la marca de tiempo que se muestra en la salida de debug (dentro del buffer) no puede ser la hora exacta en que el paquete pasa a través de la interfaz. Por lo tanto, no utilice sellos de hora mseg para demostrar problemas de rendimiento sino para obtener información relativa acerca de cuándo tienen lugar los eventos.

Para detener la depuración

Para detener una depuración, utilice **no debug allundebug all**theorcommands. Verifique que las depuraciones se hayan desactivado mediante el comando**show debug**.

Recuerde que los **no logging console terminal no monitor** comandos sólo evitan que la salida se emita en la consola, Aux o vty respectivamente. No detienen la depuración y por lo tanto agotan los recursos de router.

Uso del comando debug ip packet

debug ip packet El comando produce información sobre los paquetes que no son conmutados rápidamente por el router. Sin embargo, como genera un resultado para cada paquete, el resultado puede ser amplio y, por lo tanto, ocasionar el bloqueo del router. Por este motivo, utilice **debug ip packet** únicamente bajo los controles más estrictos descritos en esta sección.

La mejor manera de limitar la salida **debug ip packet** ofis es crear una lista de acceso que se vincule a la depuración. Sólo los paquetes que coinciden con los criterios de la lista de acceso pueden estar sujetos **debug ip packet** a. Esta lista de acceso no necesita aplicarse en ninguna interfaz, sino que se aplica a la operación de debugging.

Antes de utilizar **debugging ip packet** , tenga en cuenta que el router está realizando la conmutación rápida de forma predeterminada o puede estar realizando la conmutación CEF si está configurado para ello. Esto quiere decir que, una vez que esas técnicas están en su lugar, no se envía

el paquete al procesador y, por lo tanto, la depuración no muestra nada. Para que esto funcione, debe inhabilitar la conmutación rápida en el router con **no ip route-cache** (para paquetes de unidifusión) o **no ip mroute-cache** (para paquetes de multidifusión). Esto debe aplicarse en las interfaces donde se supone que fluye el tráfico. Verifique esto con **show ip route** el comando.

Advertencias

- La inhabilitación de la conmutación rápida en un router que administra una gran cantidad de paquetes puede causar picos de uso de la CPU de modo que el equipo se cuelgue o pierda la conexión con sus pares.

- No inhabilite la opción de conmutación rápida en un router que esté ejecutando la Conmutación de protocolo de identificación múltiple (MPLS). MPLS se utiliza junto con CEF. Por lo tanto, desactivar la conmutación rápida en la interfaz puede tener efectos desastrosos.

Considere este ejemplo de escenario:

La Lista de acceso configurada en el router_122 es:

<#root>

access-list 105 permit icmp host 10.10.10.2 host 10.1.1.1 access-list 105 permit icmp host 10.1.1.1 host

Esta lista de acceso permite cualquier paquete Internet Control Message Protocol (ICMP) del router del host_121 (con la dirección IP 10.10.10.2) al router del host_123 (con la dirección IP 10.1.1.1), así como en la dirección contraria. Es importante que permita los paquetes en cualquier dirección; de lo contrario, el router puede descartar el paquete ICMP de retorno.

Retire la conmutación rápida en una sola interfaz en el router 122. Esto significa que sólo puede ver las depuraciones de los paquetes destinados a esa interfaz, como se ve desde la perspectiva del IOS de Cisco que intercepta el paquete. De las depuraciones, estos paquetes aparecen con "d=". Dado que aún no ha desactivado el fast switching en la otra interfaz, el paquete de retorno no está sujeto **debug ip packet** a. Este resultado muestra la manera de deshabilitar el switching rápido:

<#root>

router_122(config)#

interface virtual-template 1

router_122(config-if)#

no ip route-cache

router_122(config-if)#

end

Ahora debe activarla **debug ip packet** con la lista de acceso definida anteriormente (access-list 105).

<#root>

router_122#

debug ip packet

detail 105 IP packet debugging is on (detailed) for access list 105 router_122# 00:10:01: IP: s=10.1.1

Ahora quite el fast-switching en la otra interfaz (en router_122). Esto significa que todos los paquetes a través de esas dos interfaces ahora son conmutados por paquetes (lo cual es un requisito para **debug ip packet**

<#root>

router_122(config)#

interface serial 3/0

router_122(config-if)#

no ip route-cache

router_122(config-if)#

end

router_122# 00:11:57: IP:

s=10.10.10.2

(Virtual-Access1),

d=10.1.1.1

(Serial3/0), g=172.16.1.6, len 100, forward 00:11:57:

ICMP type=8

, code=0 *! -- ICMP packet (echo) from 10.10.10.2 to 10.1.1.1* 00:11:57: IP:

s=10.1.1.1

(Serial3/0),

d=10.10.10.2

(Virtual-Access1), g=10.10.10.2, len 100, forward 00:11:57:

ICMP type=0

, code=0 *! -- ICMP return packet (echo-reply) from 10.1.1.1 to 10.10.10.2* 00:11:57: IP: s=10.10.10.2

Observe que la salida de debug ip packet no muestra ningún paquete que no coincida con los criterios de la lista de acceso. Para obtener más información sobre este procedimiento, refiérase a Comprensión de los Comandos Ping y Traceroute.

Para obtener más información sobre cómo crear listas de acceso, refiérase a Registro de Lista de Acceso IP Estándar.

Depuraciones accionadas de manera condicional

Cuando la función Conditionally Triggered Debugging está habilitada, el router genera mensajes de depuración para los paquetes que entran o salen del router en una interfaz especificada; el router no genera resultados de depuración para los paquetes que entran o salen a través de una interfaz diferente.

Observe una implementación simple de depuraciones condicionales. Considere este escenario: el router que se muestra a continuación (trabol) tiene dos interfaces (serial 0 y serial 3) que ejecutan encapsulación HDLC.

Puede utilizar el comando **debug serial interface** normal para observar los keepalives HDLC recibidos en todas las interfaces. Puede observar las señales de mantenimiento en ambas interfaces.

<#root>

traxbol#

debug serial interface

Serial network interface debugging is on traxbol# *Mar 8 09:42:34.851:

Serial0: HDLC

myseq 28, mineseen 28*, yourseen 41, line up *! -- HDLC keeplaive on interface Serial 0* *Mar 8 09:42:

Serial3: HDLC

myseq 26, mineseen 26*, yourseen 27, line up *! -- HDLC keeplaive on interface Serial 3* *Mar 8 09:42:

Habilite las depuraciones condicionales para la interfaz serial 3. Esto significa que solamente se muestran los debugs para la interfaz serial 3. Utilice **debug interface <interface_type interface_number >**el comando.

<#root>

traxbol#

debug interface serial 3

```
 Condition 1 set
```

Utilice **show debug condition** el comando para verificar que el debug condicional está activo. Tome en cuenta que está activa una condición para la interfaz serial.

<#root>

traxbol#

show debug condition

```
 Condition 1: interface Se3 (1 flags triggered) Flags: Se3 traxbol#
```

Tenga en cuenta que sólo se muestran las depuraciones para la interfaz de serie 3.

<#root>

*Mar 8 09:43:04.855:

Serial3: HDLC

```
 myseq 29, mineseen 29*, yourseen 30, line up *Mar 8 09:43:14.855:
```

Serial3: HDLC

```
 myseq 30, mineseen 30*, yourseen 31, line up
```

Utilice **undebug interface <interface_type interface_number>** el comando para quitar la depuración condicional. Se recomienda desactivar las depuraciones (por ejemplo, con undebug all) antes de eliminar el activador condicional. Esto es así para evitar un aluvión de salidas de depuración cuando se elimina la condición.

<#root>

traxbol#

undebug interface serial 3

```
 This condition is the last interface condition set. Removing all conditions can cause a flood of debug
```

y

```
 Condition 1 has been removed traxbol
```

Ahora puede observar que se muestra la depuración de las interfaces serial 0 y serial 3.

<#root>

*Mar 8 09:43:34.927:

```
Serial3: HDLC
 myseq 32, mineseen 32*, yourseen 33, line up *Mar 8 09:43:44.923:
Serial0: HDLC
 myseq 35, mineseen 35*, yourseen 48, line up
```

Advertencia: Algunas operaciones de depuración son condicionales por sí mismas. Un ejemplo es debugging atm. Con la depuración ATM debe especificar explícitamente la interfaz para la que se deben habilitar los debugs en lugar de habilitar los debugs en todas las interfaces atm y especificar una condición.

Esta sección muestra la forma correcta de limitar la depuración de paquetes de ATM a una subinterfaz:

<#root>

arielle-nrp2#

debug atm packet interface atm 0/0/0.1

!--- Note that you explicitly specify the sub-interface to be used for debugging ATM packets debuggi

Displaying packets on interface ATM0/0/0.1 only

arielle-nrp2# *Dec 21 10:16:51.891: ATM0/0/0.1(O): VCD:0x1 VPI:0x1 VCI:0x21 DM:0x100 SAP:AAAA CTL:03 O

Si intenta **atm debugging** habilitar en todas las interfaces (con una condición aplicada), el router puede bloquearse si tiene un gran número de subinterfaces ATM. Se muestra un ejemplo del método incorrecto para depurar el atm.

En este caso, puede ver que se aplica una condición, pero también que ésta no tiene ningún efecto. Aún puede ver el paquete desde la otra interfaz. En este escenario de laboratorio, solo tiene dos interfaces y muy poco tráfico. Si el número de interfaces es elevado, el resultado de la depuración de todas las interfaces es extremadamente alto y puede provocar el bloqueo del router.

<#root>

arielle-nrp2#

show debugging condition

Condition 1: interface AT0/0/0.1

(1 flags triggered) Flags: AT0/0/0.1 *! -- A condition for a specific interface.* arielle-nrp2#

debug atm packet

ATM packets debugging is on Displaying all ATM packets arielle-nrp2# *Dec 21 10:22:06.727:

ATM0/0/0.2

(O): *! -- You see debugs from interface ATM0/0/0/.2, even though the condition ! -- specified ONLY AT0*

ATM0/0/0.1

(O): *!--- You also see debugs for interface ATM0/0/0.1 as you wanted.* VCD:0x1 VPI:0x1 VCI:0x21 DM:0x1

Información Relacionada

- **Soporte de Tecnología de Discado y Acceso**
- **Soporte técnico y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).