Compreender informações importantes sobre comandos debug

Contents

Introdução

Este documento descreve as diretrizes gerais sobre o uso de debug comandos, incluindo o debug ip packet comando disponível nas plataformas Cisco IOS®.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conexão com o roteador usando o console, as portas aux e vty

- Problemas gerais de configuração do Cisco IOS
- Interpretação das saídas de depuração do Cisco IOS

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

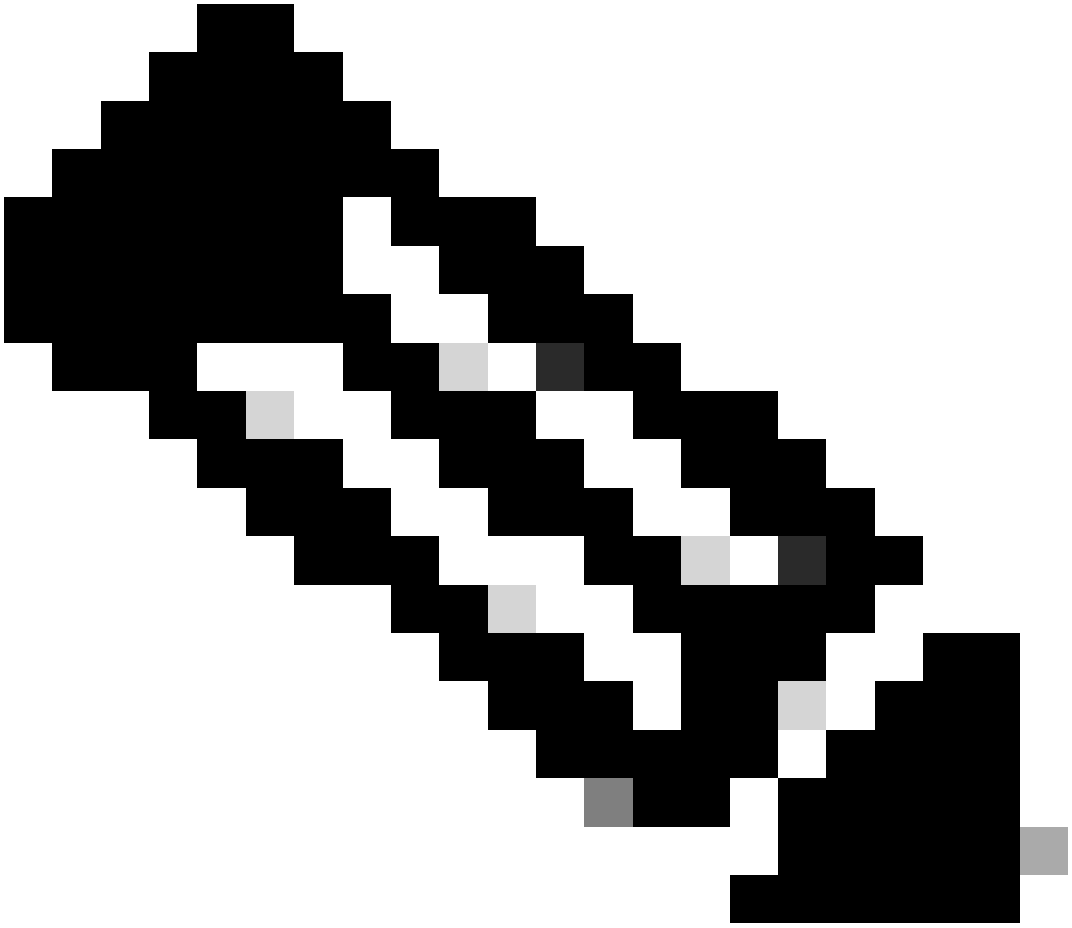
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Esta página fornece algumas diretrizes gerais sobre o uso das depurações disponíveis nas plataformas Cisco IOS, bem como exemplos para o uso adequado **debug ip packet** do comando e da depuração condicional.



Observação: este documento não explica como usar e interpretar comandos e saídas de depuração específicos. Consulte a documentação de referência de comando de depuração da Cisco apropriada, para obter informações sobre comandos debug específicos.

A saída **debug** dos comandos EXEC privilegiados fornece informações de diagnóstico que incluem uma variedade de eventos de internetworking relacionados ao status do protocolo e à atividade da rede em geral.

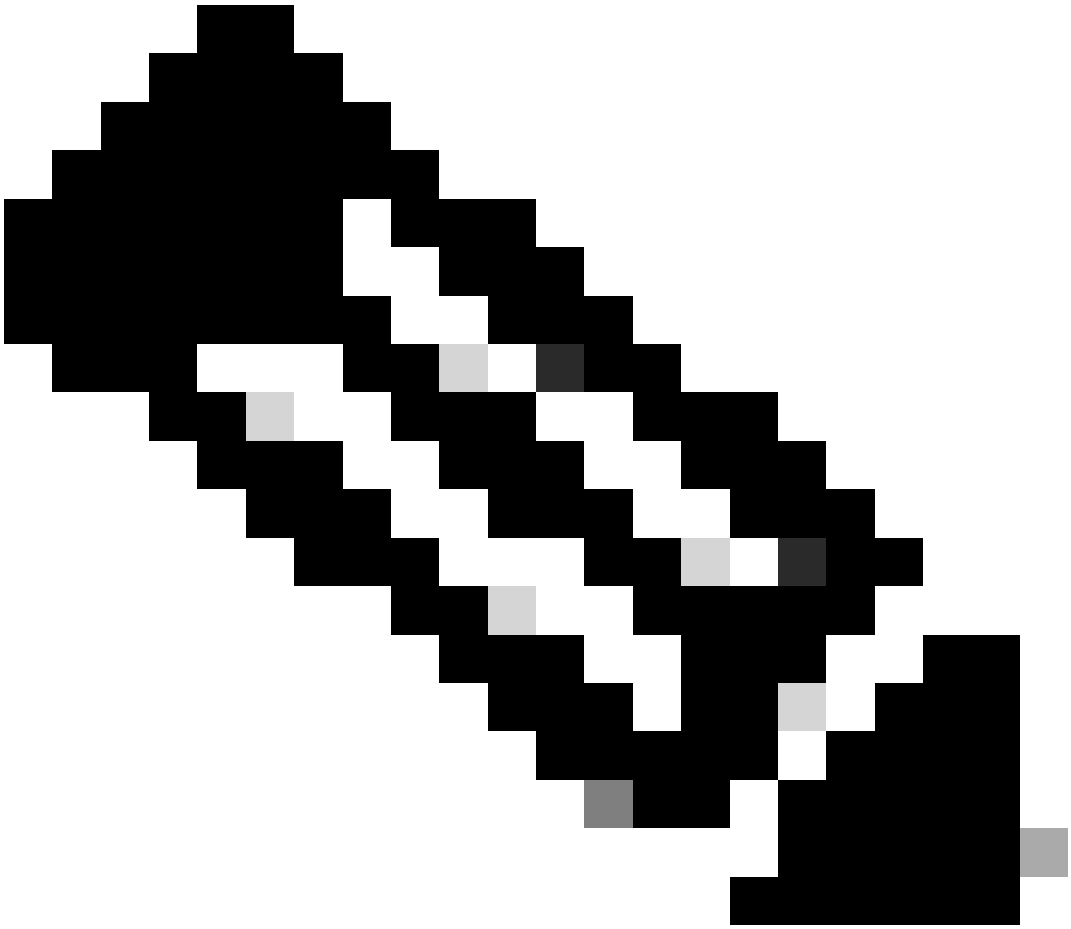
Avisos

debug Use os comandos com cuidado. Geralmente, recomenda-se que esses comandos sejam somente utilizados sob a coordenação do representante de suporte técnico do roteador quando Troubleshooting problemas específicos.

Habilitar a depuração pode interromper a operação do roteador quando as inter-redes estiverem com condição de carga elevada. Portanto, se o log estiver ativado, o servidor de acesso poderá congelar intermitentemente assim que a porta do console for sobrecarregada com mensagens de log.

Antes de iniciar um **debug** comando, sempre considere a saída que esse comando pode gerar e a quantidade de tempo que isso pode levar. Por exemplo, se você tiver um roteador com uma interface de taxa básica (BRI, basic rate interface), **debug isdn q931** provavelmente não danificará o sistema. Mas, fazer a mesma depuração em um AS5800 com configuração E1 completa provavelmente pode gerar tanta entrada que ele pode travar e parar de responder.

Antes de depurar, examine a carga da CPU com **show processes cpu** ocomando. Verifique se você tem CPU suficiente disponível antes de iniciar as depurações. Consulte Solução de problemas de alta utilização da CPU nos roteadores Cisco, para obter mais informações sobre como lidar com altas cargas de CPU. Por exemplo, se você tiver um roteador Cisco 7200 com uma interface ATM fazendo bridging, então, dependendo da quantidade de subinterfaces configuradas, reiniciar o roteador pode usar muito de sua CPU. A razão aqui é que, para cada VC (Circuito virtual), um pacote de BPDU (Unidade de dados do protocolo de ponte) precisa ser gerado. Iniciar depurações durante esse tempo crítico pode fazer com que a utilização da CPU aumente drasticamente e resultar em uma suspensão ou perda de conectividade da rede.



Observação: quando as depurações estão em execução, você normalmente não vê o prompt do roteador, especialmente quando a depuração é intensiva. Mas, na maioria dos casos, você pode usar os comandos no debug all ou undebug all para interromper as depurações. Consulte a seção Obter saídas de depuração para obter mais informações sobre o uso seguro de depurações.

Antes da depuração

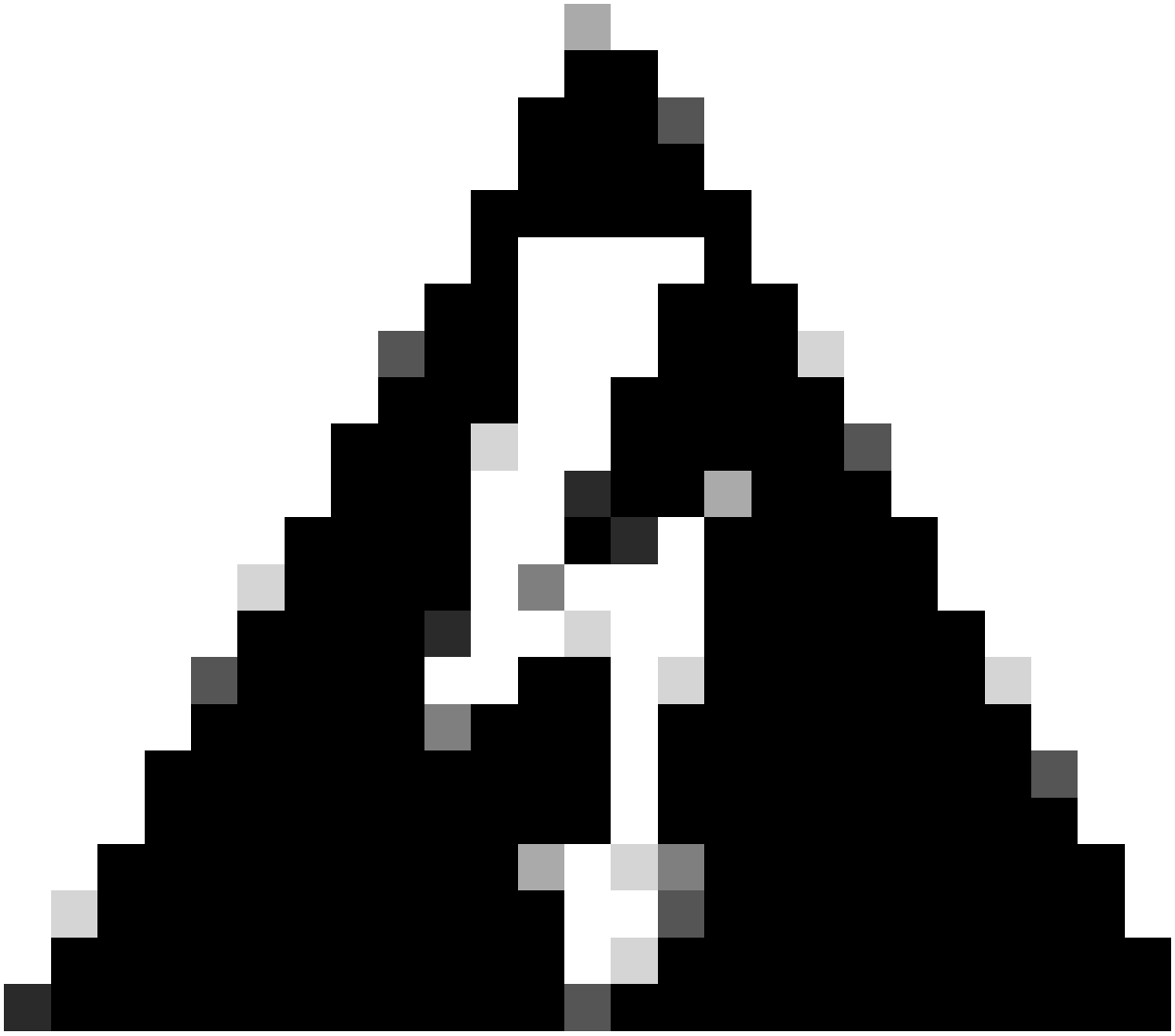
Além dos pontos mencionados acima, verifique se você entendeu o impacto das depurações na estabilidade da plataforma. Você também deve considerar a que interface do roteador você deve se conectar. Esta seção tem algumas diretrizes.

Obtendo saídas de depuração

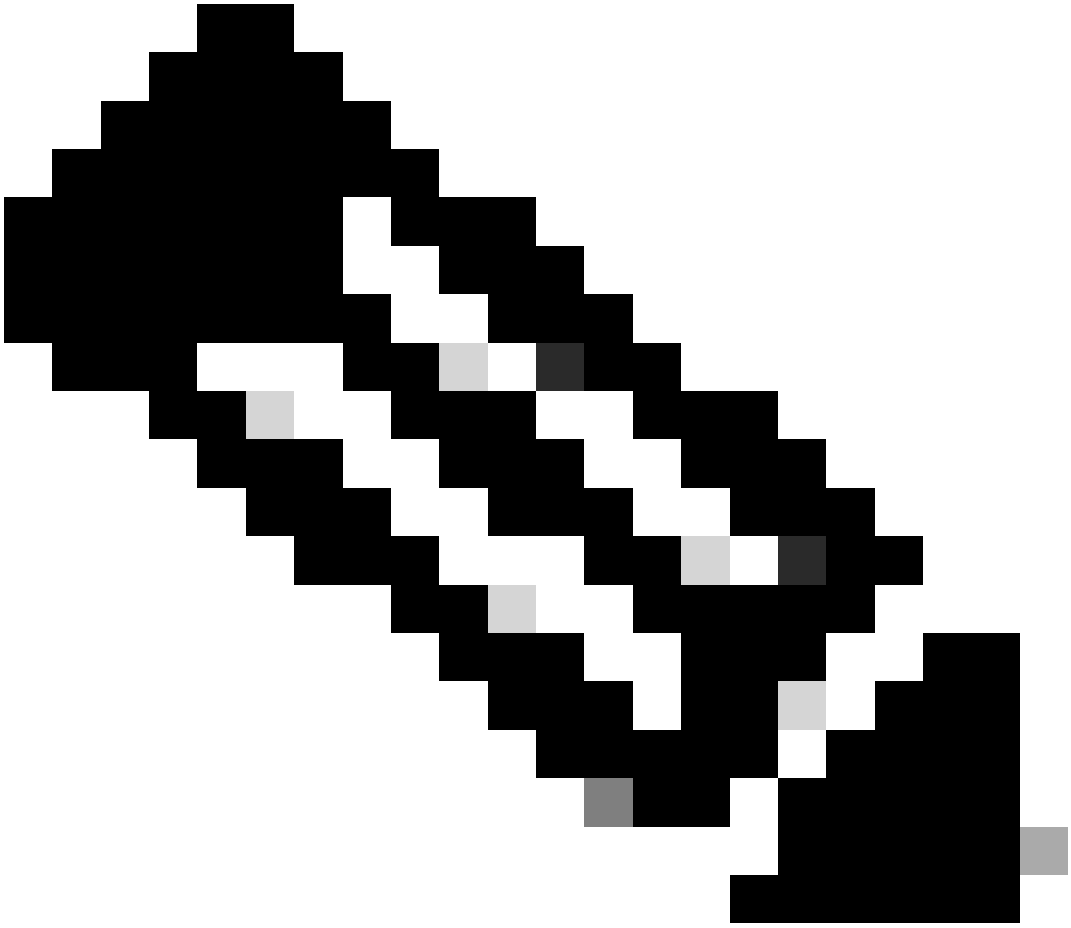
Os roteadores podem exibir saídas de depuração para várias interfaces, incluindo as portas de console, aux e vty. Os roteadores também registram mensagens em um buffer interno de um servidor syslog unix externo. As instruções e advertências para cada método são discutidas a seguir:

Porta de Console

Se você estiver conectado ao console, em configurações normais, nenhum trabalho extra precisará ser feito. A saída da depuração deve ser exibida automaticamente. Mas certifique-se de que **logging console level** ele esteja definido como desejado e que o registro não tenha sido desativado com **no logging console** o comando.



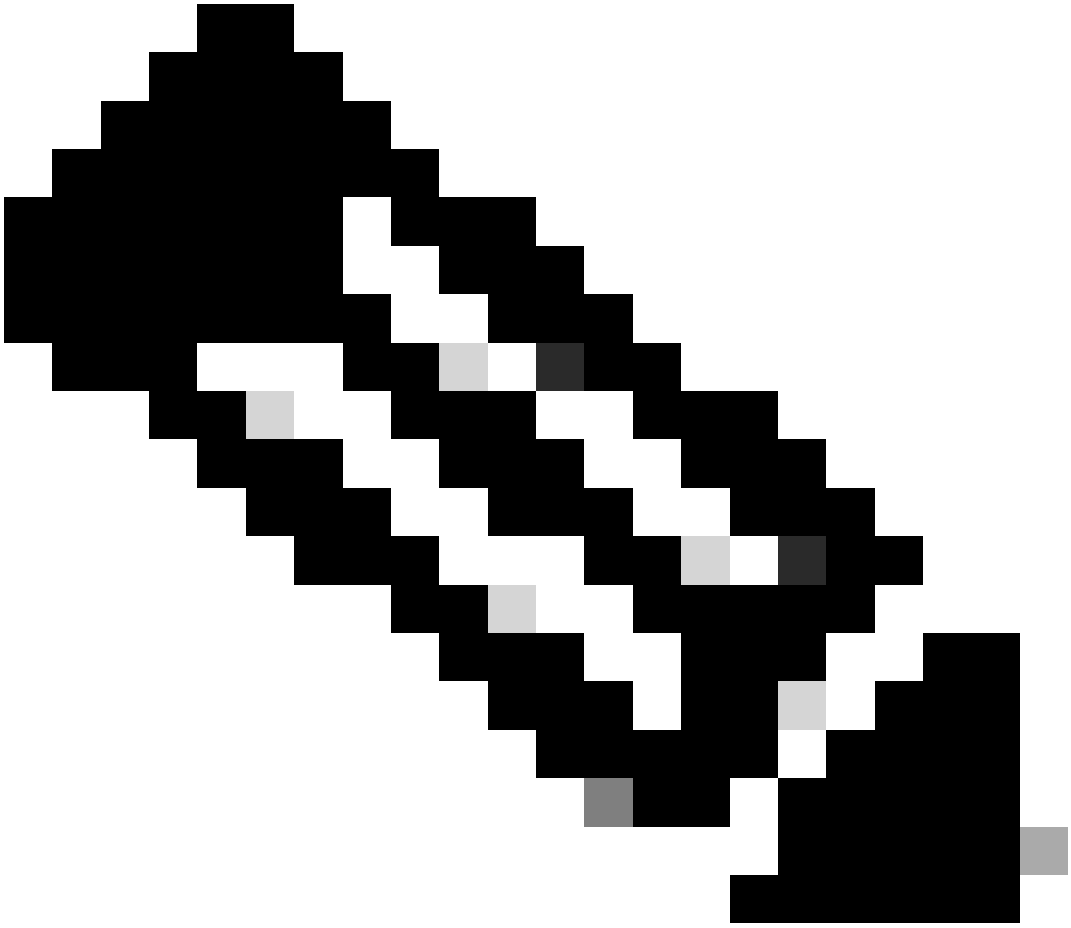
Aviso: depurações excessivas na porta de console de um roteador podem causar travamento. Isso é porque o roteador prioriza automaticamente a saída do console a frente de outras funções do roteador. Portanto, se o roteador estiver processando uma grande saída de depuração para a porta de console, ele poderá travar. Portanto, se a saída de depurações for excessiva, use as portas vty (telnet) ou os buffers de registro para obter depurações. Mais informações são fornecidas a seguir.



Observação: por padrão, o registro está habilitado na porta de console. Dessa forma, a porta do console sempre processará a saída de depurações, mesmo que você esteja usando na prática outro método ou porta (como Aux, vty ou buffer) para capturar a saída. Portanto, a Cisco recomenda que, em condições operacionais normais, você tenha o comando no logging console ativado o tempo todo e use outros métodos para capturar depurações. Nas situações em que é necessário o uso de console, ative temporariamente o console de logon.

Porta Aux

Se estiver conectado por uma porta Auxiliar, digite **terminal monitor** o comando. Verifique também se **no logging on** o comando não foi ativado no roteador.



Observação: se você usar a porta Aux para monitorar o roteador, lembre-se de que, quando o roteador for reinicializado, a porta Aux não exibirá a saída da sequência de inicialização. Conecte-se à porta do console para visualizar a sequência de inicialização.

Portas VTY

Se você estiver conectado por uma porta auxiliar ou via telnet, digite **terminal monitor** o comando. Verifique também se **no logging on** o comando não foi usado.

Registrando as mensagens em um buffer interno

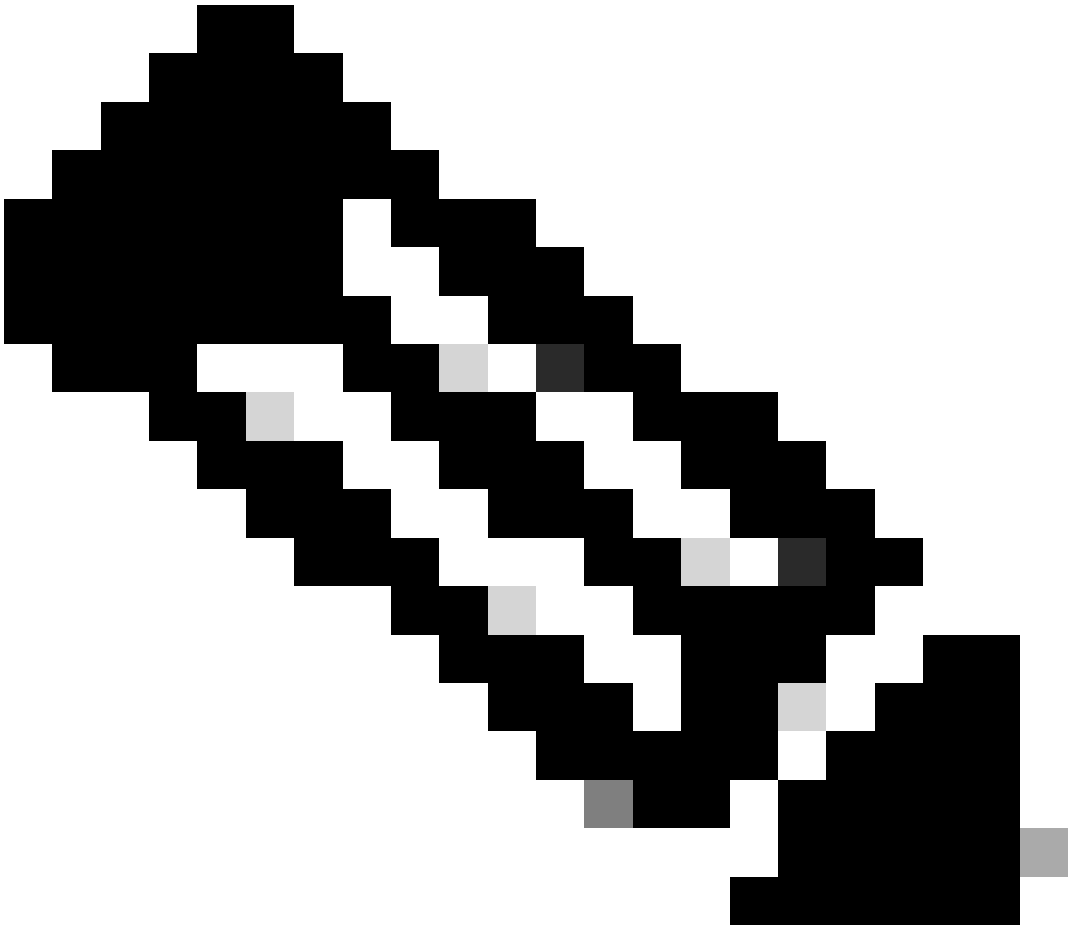
O dispositivo de registro padrão é o console; todas as mensagens são exibidas no console, a menos que especificado de outra forma.

Para registrar mensagens em um buffer interno, use o comando de configuração **logging buffered** do roteador. Esta é a sintaxe completa deste comando:

<#root>

logging buffered no logging buffered

logging buffered O comando copia as mensagens de log para um buffer interno em vez de gravá-las no console. O buffer é circular por natureza; portanto, as mensagens mais recentes substituem as novas mais antigas. Para exibir as mensagens registradas no buffer, use o comando **show logging** EXEC privilegiado. A primeira mensagem exibida é a mensagem mais antiga no buffer. Você pode especificar o tamanho do buffer e também o nível de gravidade das mensagens a serem registradas.



Observação: verifique se há memória suficiente disponível na caixa antes de inserir o tamanho do buffer. Use o comando Cisco IOS show proc mem para ver a memória disponível.

---

no logging buffered O comando cancela o uso do buffer e grava mensagens no console (o padrão).

Registrando mensagens para um UNIX Syslog Server

Para registrar mensagens no host do servidor syslog, use o comando logging router configuration. A sintaxe completa deste comando é:

<#root>

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

loggingO comando identifica um host do servidor syslog para receber mensagens de registro. O argumento < ip-address > é o endereço IP do host. Ao emitir esse comando mais de uma vez, você cria uma lista de servidores syslog que recebem mensagens de registro.

no logging O comando exclui o Servidor syslog com o endereço especificado da lista de syslogs.

Outras tarefas de pré-depuração

- Configure o software emulador de terminal (por exemplo, HyperTerminal) para que ele possa capturar a saída de depuração em um arquivo. Por exemplo, no HyperTerminal, clique**Transfer** em e, em seguida, clique **Capture Text** em e escolha as opções apropriadas. Para obter mais informações, consulte Captura de saída de texto do HyperTerminal. Para outro software de emulador de terminal, consulte a documentação do software.

- Habilite os timestamps de milissegundos (ms) usando **service timestamps** o comando:

<#root>

```
router(config)#
```

```
service timestamps debug datetime msec
```

```
router(config)#
```

```
service timestamps log datetime msec
```

Esses comandos adicionam carimbos de hora às depurações no formato MMM DD HH:MM:SS, indicando a data e a hora de acordo com o relógio do sistema. Se o relógio do sistema não tiver sido definido, a data e a hora serão precedidos por um asterisco (*) de forma a indicar que a data e a hora provavelmente não estão corretas.

Geralmente, é aconselhável configurar os timbres de hora em milisegundos, visto que isso fornece um alto nível de clareza quando se observa saídas de depuração. Os carimbos de hora em milissegundos fornecem uma indicação melhor do tempo dos vários eventos de depuração em relação um ao outro. No entanto, observe que, quando a porta de console envia muitas mensagens, elas não podem se correlacionar com a temporização real do evento. Por exemplo, se você **debug x25** habilitar tudo em uma caixa que tenha 200 VCs e a saída estiver registrada no buffer (usando **no logging console logging buffered** os comandos andcomando), o carimbo de data/hora exibido na saída de depuração (dentro do buffer) não poderá ser o horário exato em que o pacote passa pela interface. Portanto, não use timbres de tempo em ms para provar questões de desempenho, mas para obter informações relativas sobre quando os eventos ocorrem.

Para interromper a depuração

Para parar uma depuração, use **no debug allundebug all**teorcomandos. Verifique se as depurações foram desativadas usando o comando**show debug**.

Lembre-se de que os **no logging console terminal no monitor** comandos apenas impedem que a saída seja gerada no console, Aux ou vty, respectivamente. Ele não interrompe a depuração e, portanto, consome os recursos do roteador.

Usando o comando debug ip packet

debug ip packet O comando produz informações sobre pacotes que não são comutados rapidamente pelo roteador. Todavia, como ele gera uma saída para cada pacote, a saída pode ser extensiva e, por isso, causar a suspensão do roteador. Por esse motivo, **debug ip packet** use somente sob os controles mais rigorosos descritos nesta seção.

A melhor maneira de limitar a saída **debug ip packet** do é criar uma lista de acesso vinculada à depuração. Somente pacotes que correspondam aos critérios da lista de acesso podem estar sujeitos **debug ip packet** . Essa lista de acesso não precisa ser aplicada a nenhuma interface, mas sim à operação de depuração.

Antes de usar **debugging ip packet** , observe que o roteador está fazendo a switching rápida por padrão ou pode estar fazendo a switching CEF se configurado para isso. Isso significa que, após aquelas técnicas serem implementadas, o pacote não é fornecido ao processador e, portanto, a

depuração não mostra nada. Para que isso funcione, você precisa desativar a switching rápida no roteador com **no ip route-cache** (para pacotes unicast) ou **no ip mroute-cache** (para pacotes multicast). Isso deve ser aplicado nas interfaces onde o tráfego deve fluir. Verifique isso com **show ip route** o comando.

Avisos

- A desabilitação da switching rápida em um roteador que lida com um grande número de pacotes pode fazer com que a utilização de CPU aumente, de modo que a caixa trava ou perde sua conexão com os peers.

- Não desabilite a comutação rápida em um roteador que executa o Multi Protocol Label Switching (MPLS). O MPLS é usado com o CEF. Portanto, a desativação da switching rápida na interface por ter um efeito desastroso.

Considere este exemplo de cenário:

A lista de acesso configurada no roteador_122 é:

<#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

Essa lista de acesso permite qualquer pacote ICMP (Internet Control Message Protocol) do host router_121 (com endereço IP 10.10.10.2) para o host router_123 (com endereço IP 10.1.1.1), bem como na outra direção. É importante que você permita os pacotes em qualquer direção, caso contrário o roteador poderá descartar o pacote ICMP de retorno.

Remova o fast-switching em apenas uma interface no router_122. Isso significa que você só pode ver as depurações para os pacotes destinados a essa interface, como visto da perspectiva do Cisco IOS que intercepta o pacote. Nas depurações, esses pacotes aparecem com "d =". Como você ainda não desativou a comutação rápida na outra interface, o pacote de retorno não está sujeito **debug ip packet** a. Esta saída mostra como você pode desativar o fast-switching:

<#root>

router_122(config)#

interface virtual-template 1

router_122(config-if)#

no ip route-cache

router_122(config-if)#

end

Agora você deve **debug ip packet** ativarcom a lista de acesso 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

Agora, remova a switching rápida na outra interface (no roteador_122). Isso significa que todos os pacotes nessas duas interfaces agora são comutados por pacotes (o que é um 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 o debug ip packet output não mostra nenhum pacote que não corresponda aos critérios da lista de acesso. Para obter mais informações sobre este procedimento, consulte Noções básicas sobre os comandos Ping e Traceroute.

Para obter mais informações sobre como criar listas de acesso, consulte Registro de lista de acesso de IP padrão.

Depurações disparadas condicionalmente

Quando o recurso de depuração disparada condicionalmente está habilitado, o roteador gera mensagens de depuração para pacotes que entram ou saem do roteador em uma interface especificada; o roteador não gera saída de depuração para pacotes que entram ou saem por uma interface diferente.

Observe uma implementação simples de depurações condicionais. Considere este cenário: o roteador mostrado a seguir (trabol) tem duas interfaces (serial 0 e serial 3) executando o encapsulamento HDLC.

Você pode usar o comando **debug serial interface** normalpara observar os keepalives HDLC recebidos em todas as interfaces. Você pode observar os keepalives em ambas as 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 a depuração condicional da interface serial 3. Isso significa que somente as depurações para a interface serial 3 são exibidas. Use **debug interface <interface_type interface_number** >o comando.

<#root>

traxbol#

debug interface serial 3

```
 Condition 1 set
```

Use **show debug condition** o comando para verificar se a depuração condicional está ativa. Observe que uma condição para o serial de interface 3 está ativa.

<#root>

traxbol#

show debug condition

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

Observe que agora, somente as depurações da interface serial 3 são exibidas

<#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
```

Use **undebug interface <interface_type interface_number>** o comando para remover a depuração condicional. É recomendável que você desligue as depurações (por exemplo, usando undebug all) antes de remover o acionador condicional. Isso é para evitar a inundação de saídas de depuração quando a condição for removida.

<#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
```

Agora, você pode observar que a depuração para a interface serial 0 e a serial 3 são exibidas.

<#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
```

Aviso: algumas operações de depuração são condicionais por si só. Um exemplo é a depuração de atm. Com a depuração ATM, você deve especificar explicitamente a interface para a qual as depurações devem ser habilitadas, em vez de habilitar depurações em todas as interfaces ATM e especificar uma condição.

Esta seção mostra a maneira correta de limitar a depuração de pacotes ATM a uma subinterface:

<#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

Se você tentar **atm debugging** ativar em todas as interfaces (com uma condição aplicada), o roteador poderá travar se tiver um grande número de subinterfaces ATM. Um exemplo do método incorreto para depuração ATM é fornecido.

Nesse caso, você pode ver que uma condição foi aplicada, mas também ver que isso não tem efeito. Você ainda pode ver o pacote de outra interface. Neste cenário de laboratório, você tem apenas duas interfaces e muito pouco tráfego. Se o número de interfaces for alto, a saída de depuração para todas as interfaces será extremamente alta e poderá causar a interrupção do roteador.

<#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

Informações Relacionadas

- **Suporte à tecnologia de discagem e acesso**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.