Identificar e Solucionar Problemas de HSRP em Redes de Switch Catalyst

Contents

Introdução

Este documento descreve problemas comuns e maneiras de resolver problemas do Hot Standby Router Protocol (HSRP).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

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.

Entender o HSRP

Informações de Apoio

Este documento contempla esses problemas mais comuns relacionados ao HSRP:

- Relatório do roteador de um endereço IP standby do HSRP duplicado
- Alterações de estado constantes do HSRP(ativo, standby, falar)
- Peers HSRP ausentes
- Mensagens de erro do switch relacionadas ao HSRP
- Inundação excessiva de unicast da rede para a configuração do HSRP

Observação: este documento detalha como solucionar problemas de HSRP em ambientes de switch Catalyst. O documento contém muitas referências às versões de software e ao projeto de topologia de rede. No entanto, a única finalidade deste documento é facilitar e orientar os engenheiros a respeito de quem solucionará os problemas do HSRP. Este documento não é indicado para ser um guia de design, um documento de recomendação de software ou um documento de melhores práticas.

As empresas e os consumidores que dependem dos serviços de intranet e Internet para comunicações de missão crítica exigem e esperam que as redes e as aplicações estejam continuamente disponíveis. Os clientes poderão atender às demandas de disponibilidade da rede em quase 100% se utilizarem o HSRP no software Cisco IOS®. O HSRP, exclusivo das plataformas Cisco, fornece redundância de rede para redes IP de maneira a garantir que o tráfego do usuário se recupere de forma imediata e transparente de falhas no primeiro salto, em dispositivos de borda de rede ou circuitos de acesso.

Dois ou mais roteadores podem atuar como um único roteador virtual se compartilham um endereço IP e um endereço MAC (Camada 2 [L2]) O endereço é necessário para a redundância de gateway padrão do local de trabalho do host. A maioria do locais de trabalho do host não contém tabelas de roteamento e usa apenas um único endereço IP e MAC de próximo salto. Esse endereço é conhecido como gateway padrão. Com o HSRP, os membros do grupo de roteador virtual trocam continuamente mensagens de status. Um roteador pode assumir a responsabilidade de roteamento de outro, se um roteador para de funcionar, por motivos

planejados ou não. Os hosts são configurados com um único gateway padrão e continuam a encaminhar pacotes IP para um endereço IP e MAC confiável. A transição de dispositivos que fazem o roteamento é transparente para os locais de trabalho finais.

Observação: você pode configurar as estações de trabalho do host que executam o sistema operacional Microsoft para vários gateways padrão. Mas os vários gateways padrão não são dinâmicos. O OS somente usa um único gateway padrão de cada vez. O sistema seleciona apenas um gateway padrão configurado adicional, no momento da inicialização, se o primeiro gateway padrão configurado for considerado inatingível pelo protocolo ICMP (Internet Control Management Protocol).

Operação básica

Um conjunto de roteadores que executa o HRSP trabalha simultaneamente para dar a sensação de um único roteador do gateway padrão para os hosts na LAN. Esse conjunto de roteadores é conhecido como um grupo de HSRP ou um grupo standby. Um único roteador eleito do grupo é responsável por encaminhar os pacotes que os hosts enviam ao roteador virtual. Esse roteador é conhecido como o roteador ativo. Outro roteador está eleito como roteador em standby. Se ocorrer uma falha no roteador ativo, o standby assumirá as tarefas de encaminhamento de pacotes. Embora um número arbitrário de roteadores possa executar o HSRP, somente o roteador ativo encaminha os pacotes que são enviados ao endereço IP do roteador virtual.

Para minimizar o tráfego de rede, somente os roteadores ativo e standby enviam mensagens do HSRP periódicas, depois que o protocolo conclui o processo de eleição. Os roteadores adicionais no grupo do HSRP permanecem no estado `Ouvir`. Se o roteador ativo falhar, o roteador em standby assume como o roteador ativo. Se o roteador standby falhar ou se tornar o roteador ativo, outro roteador será eleito como o roteador standby.

Cada grupo standby simula um único roteador virtual (gateway padrão). Para cada grupo, um único endereço IP e MAC bem conhecido é alocado para esse grupo. Vários grupos standby podem coexistir e se sobrepor em uma LAN, e os roteadores individuais podem participar de vários grupos. Nesse caso, o roteador mantém um estado separado e temporizadores para cada grupo.

Termos de HSRP

Termo	Definição
Roteador ativo	O roteador que atualmente encaminha pacotes para o roteador virtual
Roteador de standby	O roteador de backup primário
Grupo standby	O conjunto de roteadores que participam do HSRP e simulam um roteador virtual em conjunto
Hello time	O intervalo entre sucessivas mensagens Hello do HSRP de determinado roteador
Tempo de espera	O intervalo entre o recebimento de uma mensagem Hello e a suposição de que o roteador de envio falhou

Endereçamento de HSRP

Comunicação do roteador HSRP

Os roteadores que executam o HSRP comunicam as informações do HSRP entre si através dos pacotes Hello do HSRP. Esses pacotes são enviados para o endereço IP multicast de destino 224.0.0.2 na porta 1985 UDP (User Datagram Protocol). O endereço IP multicast 224.0.0.2 é um endereço multicast reservado usado para se comunicar com todos os roteadores. O roteador ativo origina os pacotes Hello pelo endereço IP configurado e pelo endereço MAC virtual do HSRP. O roteador standby origina pacotes Hello pelo endereço IP configurado e pelo endereço MAC (BIA) gravado. Esse uso do endereçamento de origem é necessário para que os roteadores do HSRP possam se identificar corretamente.

Na maioria dos casos, quando os roteadores são configurados para fazer parte de um grupo de HSRP, os roteadores ouvem o endereço MAC do HSRP para esse grupo, bem como o próprio BIA. A única exceção para esse comportamento é nos roteadores Cisco 2500, 4000 e 4500. Esses roteadores têm hardware Ethernet que reconhece apenas um único endereço MAC. Portanto, esses roteadores usam o endereço MAC do HSRP quando atuam como roteador ativo. Os roteadores usam o BIA quando atuam como roteador standby.

Comunicação de endereço IP standby do HSRP em todas as mídias, exceto token ring

Como os locais de trabalho do host são configurados com o gateway padrão como o endereço IP standby do HSRP, os hosts devem se comunicar com o endereço MAC associado ao endereço IP standby do HSRP. Esse endereço MAC é um endereço MAC virtual composto de 0000.0c07.ac**. O ** é o número de grupo do HSRP em hexadecimal, com base na respectiva interface. Por exemplo, o grupo do HSRP 1 usa o endereço MAC virtual do HSRP de 0000.0c07.ac01. Os hosts no segmento de LAN adjacente usam o processo normal de ARP (Address Resolution Protocol) para resolver os endereços MAC associados.

Redirecionamentos de ICMP

Os roteadores pares do HSRP que protegem uma sub-rede são capazes de fornecer acesso a todas as outras sub-redes na rede. Essa é a base do HSRP. Portanto, o roteador que se torna o roteador ativo do HSRP é irrelevante. Nas versões anteriores ao software Cisco IOS versão 12.1(3)T, os redirecionamentos de ICMP são automaticamente desativados em uma interface quando o HSRP é usado nessa interface. Sem essa configuração, os hosts podem ser redirecionados para fora do endereço IP virtual do HSRP e para um endereço IP e MAC de interface de um único roteador. A redundância é perdida.

O Cisco IOS Software apresenta um método para permitir redirecionamentos ICMP com HSRP. Esse método filtra as mensagens de redirecionamento de ICMP de saída por meio do HSRP. O endereço IP do próximo salto é alterado para um endereço virtual do HSRP. O endereço IP do gateway na mensagem de redirecionamento de ICMP de saída é comparado a uma lista de roteadores ativos do HSRP presentes nessa rede. Se o roteador correspondente ao endereço IP do gateway for um roteador ativo para um grupo de HSRP, o endereço IP do gateway será

substituído por esse endereço IP virtual do grupo. Essa solução permite que os hosts aprendam as rotas ideais para redes remotas e, ao mesmo tempo, mantenham a resiliência oferecida pelo HSRP.

Matriz de funcionalidade de HSRP

Consulte a seção Matriz de funcionalidade do HSRP e versão do Cisco IOS em Recursos e funcionalidades do Hot Standby Router Protocol para saber mais sobre os recursos e as versões do software Cisco IOS que são compatíveis com o HSRP.

Recursos de HSRP

Consulte Recursos e funcionalidade do Hot Standby Router Protocol para obter informações sobre a maioria dos recursos do HSRP. Este documento fornece informações sobre estes recursos do HSRP:

- Preempção
- Rastreamento de interface
- Uso de um BIA
- Vários grupos de HSRP
- Endereços MAC configuráveis
- Suporte de syslog
- Depuração HSRP
- depuração de HSRP aprimorada
- Autenticação
- Redundância de IP
- MIB SNMP (Simple Network Management Protocol)
- HSRP para Multiprotocol Label Switching (MPLS)

Observação: você pode usar o recurso Localizar do navegador para localizar essas seções no documento.

Formato de pacote

Esta tabela mostra o formato da parte de dados no quadro de HSRP do UDP:

Versão	Código Op	Estado	Hellotime
Tempo de suspensão	Prioridade	Grupo	Reservado

Dados de autenticação
Dados de autenticação
Endereço IP virtual:

Esta tabela descreve cada um dos campos no pacote de HSRP:

Campo de Pacote	Descrição
Op Code (1 octeto)	O código Op descreve o tipo de mensagem do pacote. Os valores possíveis são: 0 - olá, 1 - golpe e 2 - demitir. As mensagens Hello são enviadas para indicar que um roteador executa o HSRP e pode se tornar o roteador ativo. Mensagens de vitória são enviadas quando um roteador deseja se tornar o roteador ativo. Mensagens de despedida são enviadas quando um roteador não quer mais ser o roteador ativo.
Estado (1 octeto)	Cada roteador no grupo de standby implementa uma máquina de estado. O campo de estado descreve o estado atual do roteador que envia a mensagem. Estes são detalhes sobre os estados individuais: 0 - inicial, 1 - aprender, 2 - escutar, 4 - falar, 8 - standby e 16 - ativo.
Tempo de saudação (1 octeto)	Esse campo é significativo somente em mensagens de saudação. Ele contém o período aproximado entre as mensagens de saudação enviadas pelo roteador. O tempo é fornecido em segundos.
Tempo de espera (1 octeto)	Esse campo é significativo somente em mensagens de saudação. Ele contém a quantidade de tempo que os roteadores esperam por uma mensagem Hello, antes de iniciarem uma alteração de estado.
Prioridade (octeto 1)	Esse campo é usado para escolher os roteadores ativo e standby. Em uma comparação das prioridades de dois roteadores, o roteador com o valor mais alto se torna o roteador ativo. O infrator de vínculo é o roteador com o maior endereço IP.
Grupo (1 octeto)	Esse campo identifica o grupo de espera.
Data de autenticação (8 octetos)	Esse campo contém uma senha de oito caracteres em texto não criptografado.
Endereço IP virtual (4 octetos)	Se o endereço IP virtual não estiver configurado em um roteador, o endereço pode ser aprendido a partir da mensagem Hello no roteador ativo. Um endereço será aprendido somente se um endereço IP standby do HSRP não for configurado e se a mensagem Hello for autenticada (se a autenticação estiver configurada).

Estados de HSRP

Estado	Definição
`Initial`	Esse é o estado no início. Esse estado indica que o HSRP não foi executado. Esse estado é inserido por meio de uma alteração de configuração ou quando uma interface se torna disponível pela primeira vez.
`Saiba`	O roteador não determinou o endereço IP virtual e ainda não recebeu uma mensagem

	Hello autenticada do roteador ativo. Nesse estado, o roteador ainda aguarda o recebimento de uma mensagem do roteador ativo.
`Ouvir`	O roteador conhece o endereço IP virtual, mas não é o roteador ativo nem em standby. Ele escuta mensagens de saudação daqueles roteadores.
`Falar`	O roteador envia mensagens de aviso periódicas e participa ativamente da eleição do roteador ativo e/ou do roteador em standby. Um roteador não pode entrar no estado `Falar, a menos que o roteador tenha o endereço IP virtual.`
`Standby`	O roteador é candidato a se tornar o próximo roteador ativo e envia mensagens de aviso periódicas. Com a exclusão de condições transitórias, há, no máximo, um roteador do grupo no estado `standby`.
`Ativo`	O roteador desvia pacotes enviados para o endereço MAC virtual do grupo. O roteador envia mensagens de aviso periódicas. Com a exclusão de condições transitórias, deve haver, no máximo, um roteador do grupo no estado `ativo`.

Cronômetros HSRP

Cada roteador usa apenas três temporizadores no HSRP. Os temporizadores cronometram as mensagens Hello. Os convergências do HSRP, quando ocorre uma falha, dependem de como os temporizadores Hello e Hold do HSRP são configurados. Por padrão, esses temporizadores são definidos como 3 e 10 segundos, respectivamente, o que significa que um pacote Hello é enviado entre os dispositivos de grupo standby do HSRP a cada 3 segundos e o dispositivo standby se torna ativo quando um pacote Hello não foi recebido por 10 segundos. Você pode reduzir essas configurações de temporizador para acelerar o failover ou a apropriação, mas, para evitar o aumento do uso da CPU e a oscilação desnecessária do estado de espera, não defina o temporizador de Hello com menos de um (1) segundo ou o temporizador de espera com menos de 4 segundos. Observe que, se você usar o mecanismo de rastreamento do HSRP e ocorrer uma falha no link rastreado, o failover ou a preempção ocorrerá de imediato, independentemente dos temporizadores Hello e Hold. Quando um temporizador expira, o roteador faz transição para um novo estado do HSRP. Os temporizadores podem ser alterados com este comando: standby [group-number] timers hellotime holdtime. Por exemplo, standby 1 timers 5 15.

Esta tabela fornece mais informações sobre esses temporizadores:

Cronômetro	Descrição
Temporizador ativo	Esse temporizador é usado para monitorar o roteador ativo. Esse temporizador começa sempre que um roteador ativo recebe um pacote Hello. Esse temporizador expira de acordo com o valor do tempo de espera definido no campo relacionado da mensagem de Hello do HSRP.
Temporizador de standby	Esse temporizador é usado para monitorar o roteador standby. O temporizador começa sempre que o roteador standby recebe um pacote Hello. Esse temporizador expira de acordo com o valor do tempo de espera definido no respectivo pacote Hello.
Temporizador de saudação	Esse temporizador é usado para registrar os pacotes Hello. Todos os roteadores do HSRP em qualquer estado do HSRP geram um pacote Hello quando esse temporizador Hello expira.

Eventos de HSRP

Esta tabela fornece os eventos na máquina de estado finito do HSRP:

Chave	Events
1	O HSRP é configurado em uma interface ativada.
2	O HSRP está desativado em uma interface ou a interface está desativada.
3	Expiração do temporizador ativo O temporizador ativo é definido como o tempo de espera, quando a última mensagem Hello é vista no roteador ativo.
4	Expiração do temporizador standby O temporizador standby é definido como o tempo de espera, quando a última mensagem Hello é vista no roteador standby.
5	Expiração do temporizador Hello O temporizador periódico para o envio de mensagens Hello expirou.
6	Recebimento de uma mensagem Hello de maior prioridade de um roteador no estado `falar`
7	Recebimento de uma mensagem Hello de maior prioridade de um roteador ativo
8	Recebimento de uma mensagem Hello de menor prioridade de um roteador ativo
9	Recebimento de uma mensagem Resign do roteador ativo
10	Recebimento de uma mensagem Coup de um roteador de maior prioridade
11	Recebimento de uma mensagem Hello de maior prioridade do roteador standby
12	Recebimento de uma mensagem Hello de menor prioridade do roteador standby

Ações HSRP

Esta tabela especifica as ações a serem tomadas como parte da máquina de estado:

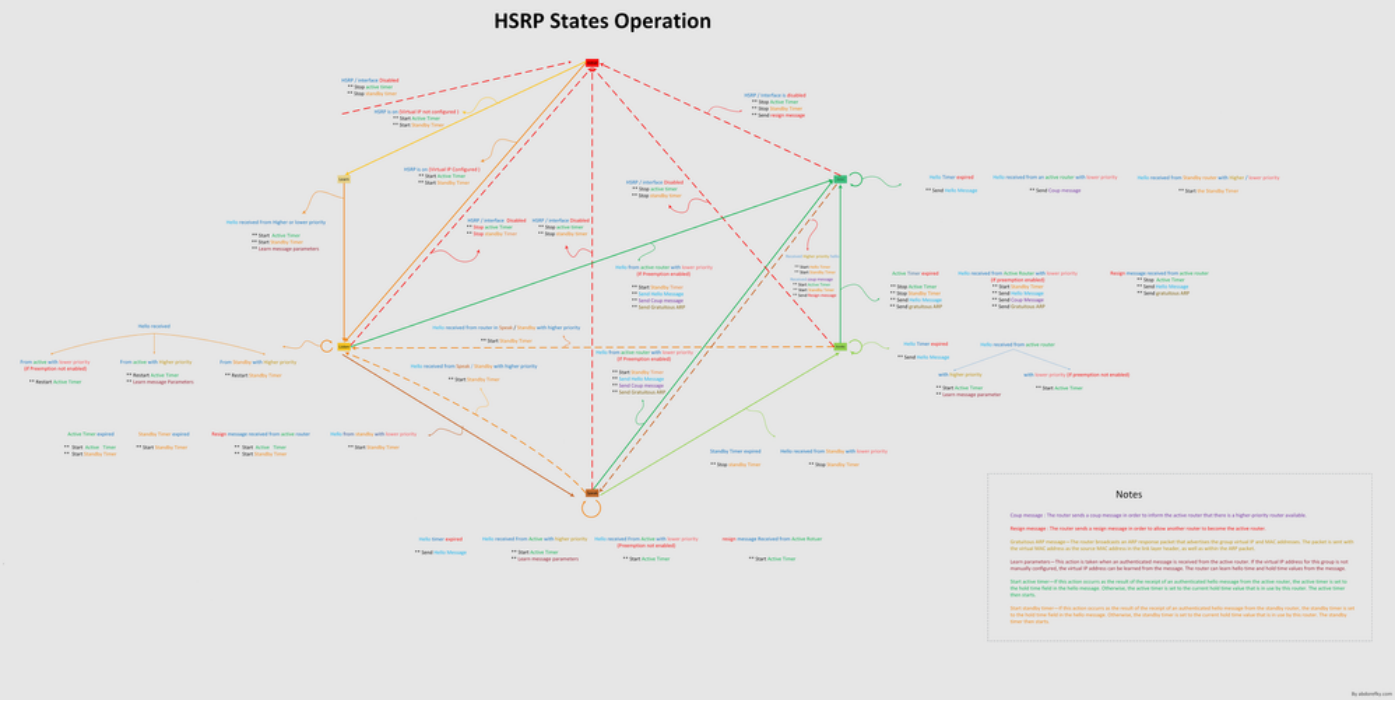
Letra	Ação
R	Iniciar temporizador ativo — Se essa ação ocorrer como resultado do recebimento de uma mensagem de saudação autenticada do roteador ativo, o temporizador ativo será definido para o campo de tempo de espera na mensagem de saudação. Caso contrário, o temporizador ativo será definido como o valor do tempo de espera atual que está sendo usado por este roteador. Em seguida, o temporizador ativo é iniciado.
B	Iniciar temporizador de standby — Se essa ação ocorrer como resultado do recebimento de uma mensagem de saudação autenticada do roteador em standby, o temporizador de standby será definido para o campo de tempo de espera na mensagem de saudação. Caso contrário, o temporizador standby será definido como o valor do tempo de espera atual que está sendo usado por este roteador. Em seguida, o temporizador standby é iniciado.
C	Parar temporizador ativo — o temporizador ativo é interrompido.
D	Parar temporizador standby — o temporizador standby é interrompido.
E	Aprender parâmetros—Esta ação é executada quando uma mensagem autenticada é recebida do roteador ativo. Se o endereço IP virtual desse grupo não for configurado manualmente, o endereço IP virtual poderá ser aprendido na mensagem. O roteador pode conhecer os valores do tempo Hello e do tempo de espera na mensagem.
F	Enviar mensagem Hello — o roteador envia uma mensagem Hello com o estado atual,

	tempo Hello e tempo de espera.
G	Enviar mensagem Coup — o roteador envia uma mensagem Coup para informar ao roteador ativo que há um roteador de maior prioridade disponível.
H	Enviar mensagem Resign — o roteador envia uma mensagem Resign para permitir que outro roteador se torne o roteador ativo.
I	Enviar mensagem do ARP gratuito — o roteador transmite um pacote de resposta do ARP que anuncia os endereços IP e MAC virtuais do grupo. O pacote é enviado com o endereço MAC virtual como o endereço MAC de origem no cabeçalho da camada de link, bem como no pacote do ARP.

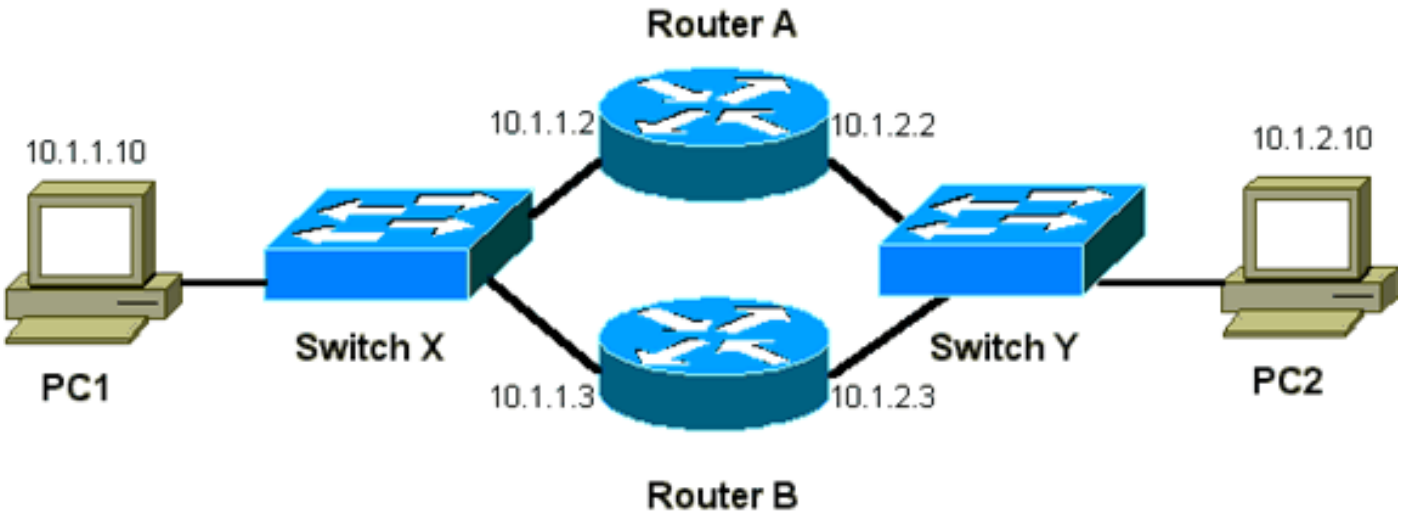
Tabela de estado de HSRP

O diagrama nesta seção mostra as transições de estado da máquina de estado do HSRP. Toda vez que um evento ocorre, os resultados da ação associada e o roteador fazem transição para o próximo estado do HSRP. No diagrama, os números designam os eventos e as letras designam a ação associada. A tabela na seção Eventos do HSRP define os números e a tabela na seção Ações do HSRP define as letras. Use este diagrama somente como referência. O diagrama é detalhado e não é necessário para fins gerais de solução de problemas.

Para obter uma imagem de alta resolução do diagrama, consulte Operação dos estados do HSRP.



Fluxo de pacote



Dispositivo	Endereço MAC	IP Address	Máscara de sub-rede	Gateway padrão
PC1	0000.0c00.0001	10.1.1.10	255.255.255.0	10.1.1.1
PC2	0000.0 c 00.1110	10.1.2.10	255.255.255.0	10.1.2.1

Configuração do roteador A (roteador ativo)

```
interface GigabitEthernet 0/0
 ip address 10.1.1.2 255.255.255.0
 mac-address 4000.0000.0010
 standby 1 ip 10.1.1.1
 standby 1 priority 200

interface GigabitEthernet 0/1
 ip address 10.1.2.2 255.255.255.0
 mac-address 4000.0000.0011
 standby 1 ip 10.1.2.1
 standby 1 priority 200
```

Configuração do roteador B (roteador standby)

```
interface GigabitEthernet 0/0
    ip address 10.1.1.3 255.255.225.0
    mac-address 4000.0000.0020
    standby 1 ip 10.1.1.1

interface GigabitEthernet 0/1
     ip address 10.1.2.3 255.255.255.0
     mac-address 4000.0000.0021
     standby 1 ip 10.1.2.1
```

Observação: esses exemplos configuram endereços MAC estáticos apenas para fins de ilustração. Não configure endereços MAC estáticos, a menos que seja necessário.

Você deve entender o conceito por trás do fluxo de pacotes quando obtém farejadores de rastreamento para solucionar problemas de HSRP. O roteador A usa a prioridade de 200 e se torna o roteador ativo em ambas as interfaces. No exemplo desta seção, os pacotes do roteador destinados a um local de trabalho do host têm o endereço MAC de origem do endereço MAC físico do roteador (BIA). Os pacotes das máquinas de host destinados ao endereço IP do HSRP têm o endereço MAC de destino do endereço MAC virtual do HSRP. Observe que os endereços MAC não são os mesmos para cada fluxo entre o roteador e o host.

Esta tabela mostra as informações do endereço IP e MAC correspondentes por fluxo com base em um rastreamento de sniffer que é obtido do switch X.

Fluxo de pacote	MAC de Origem	MAC de destino	IP origem	IP de Destino
Pacotes do PC1 destinados ao PC2	PC1 (0000.0c00.0001)	Endereço MAC virtual do HSRP da interface Ethernet 0 do Roteador A (0000.0c07.ac01)	10.1.1.10	10.1.2.10
Pacotes que retornam pelo Roteador A do PC2 e são destinados ao PC1	BIA Ethernet 0 do Roteador A (4000.0000.0010)	PC1 (0000.0c00.0001)	10.1.2.10	10.1.1.10
Pacotes do PC1 são destinados ao endereço IP standby do HSRP (ICMP, Telnet)	PC1 (0000.0c00.0001)	Endereço MAC virtual do HSRP da interface Ethernet 0 do Roteador A (0000.0c07.ac01)	10.1.1.10	10.1.1.1
Pacotes destinados ao endereço IP real do roteador ativo (ICMP, Telnet)	PC1 (0000.0c00.0001)	BIA Ethernet 0 do Roteador A (4000.0000.0010)	10.1.1.10	10.1.1.2
Pacotes destinados ao endereço IP real do roteador standby (ICMP, Telnet)	PC1 (0000.0c00.0001)	BIA Ethernet 0 do Roteador B (4000.0000.0020)	10.1.1.10	10.1.1.3

Solucionar os problemas dos estudos de caso do HSRP

Estudo de caso #1: o endereço IP em standby do HSRP é relatado como um endereço IP duplicado

Estas mensagens de erro podem ser exibidas:

```
Oct 12 13:15:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 13 16:25:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:31:02: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:41:01: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
```

Essas mensagens de erro não indicam necessariamente um problema no HSRP. Em vez disso, as mensagens de erro indicam um possível loop do Spanning Tree Protocol (STP) ou um problema de configuração do roteador/switch. As mensagens de erros são apenas sintomas de um outro problema.

Além disso, essas mensagens de erro não impedem a operação adequada do HSRP. O pacote do HSRP duplicado é ignorado. Essas mensagens de erro são limitadas em intervalos de 30 segundos. Mas o desempenho lento da rede e a perda de pacotes podem resultar da instabilidade da rede que causa as mensagens de erro `STANDBY-3-DUPADDR do endereço do HSRP.`

Essas mensagens indicam especificamente que o roteador recebeu um pacote de dados originado pelo endereço IP do HSRP na VLAN 25 com os endereços MAC 0000.0c07.ac19. Como o endereço MAC do HSRP é 0000.0c07.ac19, o roteador em questão recebeu seu próprio pacote de volta ou ambos os roteadores no grupo HSRP entraram no estado ativo. Como o roteador recebeu o próprio pacote, o problema mais provável é com a rede, e não com o roteador. Diversos problemas podem causar esse comportamento. Veja a seguir os possíveis problemas de rede que causam as mensagens de erro:

- Loops de STP momentâneos
- Problemas de configuração do EtherChannel
- Quadros duplicados

Ao solucionar problemas dessas mensagens de erro, consulte as etapas para solucionar problemas na seção Troubleshooting de HSRP em Catalyst Switches deste documento. Todos os módulos de solução de problemas são aplicáveis a esta seção, que inclui módulos na configuração. Além disso, observe todos os erros no log do switch e faça referência a estudos de caso adicionais, conforme necessário.

Você pode usar uma lista de acesso para impedir que o roteador ativo receba o próprio pacote Hello multicast. Mas essa é apenas uma solução alternativa para as mensagens de erro e, na verdade, oculta o sintoma do problema. A solução alternativa é aplicar uma lista de acesso de entrada estendida às interfaces do HSRP. A lista de acesso bloqueia todo o tráfego originado do endereço IP físico e que é destinado a todos os roteadores do endereço multicast 224.0.0.2.

```
access-list 101 deny ip host 172.16.12.3 host 224.0.0.2
access-list 101 permit ip any any

interface GigabitEthernet 0/0
```

```
 ip address 172.16.12.3 255.255.255.0
 standby 1 ip 172.16.12.1
 ip access-group 101 in
```

Estudo de caso #2: alterações contínuas do estado do HSRP (ativo, em espera, falar) ou %HSRP-6-STATECHANGE

Estas mensagens de erro podem ser exibidas:

```
Jan 9 08:00:42.623: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:00:56.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:03.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
Jan 9 08:01:29.427: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:01:36.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:43.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
```

Jul 29 14:03:19.441: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active
Jul 29 16:27:04.133: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak
Jul 29 16:31:49.035: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Speak -> Standby

Essas mensagens de erro descrevem uma situação em que um roteador do HSRP standby não recebeu três pacotes Hello do HSRP sucessivos do par do HSRP. A saída mostra que o roteador standby passa do estado `standby para o estado ativo`. Logo em seguida, o roteador volta ao estado de espera. A menos que essa mensagem de erro ocorra durante a instalação inicial, provavelmente um problema do HSRP não causa a mensagem de erro. As mensagens de erro significam a perda de Hellos do HSRP entre os pares. Ao solucionar esse problema, você deve verificar a comunicação entre os pares do HSRP. Uma perda de dados aleatória e momentânea entre os peers é o problema mais comum que resulta nestas mensagens. Muitas vezes, as alterações de estado do HSRP ocorrem devido à alta utilização da CPU. Se a mensagem de erro for devido à alta utilização da CPU, insira um sniffer na rede e rastreie o sistema que causa a alta utilização da CPU.

Há várias causas possíveis para a perda de pacotes do HSRP entre os pares. Os problemas mais comuns são problemas de camada física, tráfego de rede excessivo causado por problemas de Spanning Tree ou tráfego excessivo causado em cada VLAN. Como no Estudo de caso nº 1, todos os módulos de solução de problemas são aplicáveis à resolução de alterações de estado do HSRP, particularmente a Depuração HSRP da Camada 3.

Se a perda de pacotes do HSRP entre os pares for devido ao tráfego excessivo causado em cada

VLAN, conforme mencionado, você poderá ajustar ou aumentar o SPD e manter o tamanho da fila para superar o problema de queda da fila de entrada.

Para aumentar o tamanho do SPD (Selective Packet Discard), vá para o modo de configuração e execute estes comandos nos switches Cat6500:

```
(config)#ip spd queue max-threshold 600

!--- Hidden Command

(config)#ip spd queue min-threshold 500

!--- Hidden Command
```

Para aumentar o tamanho da fila de espera, vá para o modo de interface da VLAN e execute este comando:

```
(config-if)#hold-queue 500 in
```

Depois de aumentar o SPD e manter o tamanho da fila, você pode limpar os contadores da interface se executar o comando **`clear counter`** interface.

Estudo de caso #3: o HSRP não reconhece o peer

A saída do roteador nesta seção mostra um roteador configurado para HSRP, mas não reconhece os pares do HSRP. Para que isso ocorra, o roteador não deve receber Hello do HSRP no roteador vizinho. Ao solucionar esse problema, consulte a seção Verificar a conectividade da camada física e a seção Verificar a configuração do roteador do HSRP deste documento. Se a conectividade da camada física estiver correta, verifique os modos de VTP incompatíveis.

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

Estudo de caso #4: Alterações de estado de HSRP e relatórios de switch SYS-4-P2_WARN: 1/Host <mac_address> está oscilando entre a porta <port_1> e a porta

<port_2> no Syslog

Estas mensagens de erro podem ser exibidas:

```
2001 Jan 03 14:18:43 %SYS-4-P2_WARN: 1/Host 00:00:0c:14:9d:08
  is flapping between port 2/4 and port 2/3
```

Feb 4 07:17:44 AST: %SW_MATM-4-MACFLAP_NOTIF: Host 0050.56a9.1f28 in vlan 1027 is flapping between port Te1/0/7 and port Te2/0/2

Nos Switches Catalyst, o switch relata um endereço MAC do host que se move se o endereço MAC do host se move duas vezes dentro de 15 segundos. Uma causa possível é um loop de STP. O switch descarta pacotes desse host por cerca de 15 segundos, tentando minimizar o impacto de um loop de STP. Se o endereço MAC reportado que se move entre duas portas for o endereço MAC virtual do HSRP, provavelmente o problema será que os dois roteadores do HSRP entram no estado `ativo`.

Se o endereço MAC relatado não for o endereço MAC virtual do HSRP, o problema poderá indicar o loop, a duplicação ou a reflexão dos pacotes na rede. Esses tipos de condições podem contribuir com os problemas do HSRP. As causas mais comuns para a movimentação dos endereços MAC são problemas no Spanning Tree ou problemas na camada física.

Ao solucionar os problemas dessa mensagem de erro, execute estas etapas:

Observação: além disso, conclua as etapas da seção Troubleshooting de HSRP em Catalyst Switches deste documento.

---

1. Determine a origem correta (porta) do endereço MAC do host.
2. Desconecte a porta que não deve originar o endereço MAC do host.
3. Documente a topologia do STP de acordo com a VLAN e verifique se há falha de STP.
4. Verifique a configuração do canal da porta.
    1. Uma configuração incorreta no canal da porta pode resultar na oscilação das mensagens de erro pelo endereço MAC do host. Isso ocorre devido à natureza de balanceamento de carga do canal da porta.

Estudo de caso #5: roteamento assimétrico e HSRP (inundação excessiva de tráfego unicast em rede com roteadores que executam o HSRP)

Com o roteamento assimétrico, os pacotes de transmissão e recepção usam caminhos diferentes entre um host e o peer com o qual se comunicam. Esse fluxo de pacotes é resultado da

configuração do balanceamento de carga entre roteadores HSRP, com base na prioridade HSRP, que define o HSRP como ativo ou em espera. Esse tipo de fluxo de pacotes em um ambiente de switching pode resultar em excesso de inundação unicast desconhecido. Além disso, as entradas de MLS (Multilayer Switching, Switching multicamadas) podem estar ausentes. A inundação unicast desconhecida ocorre quando o switch inunda um pacote unicast em todas as portas. O switch inunda o pacote porque não há entrada para o endereço MAC de destino. Esse comportamento não interrompe a conectividade porque os pacotes ainda são encaminhados. Mas o comportamento é responsável pelo fluxo de pacotes extras nas portas do host. Esse caso estuda o comportamento do roteamento assimétrico e por que a inundação unicast ocorre.

Os sintomas do roteamento assimétrico incluem:

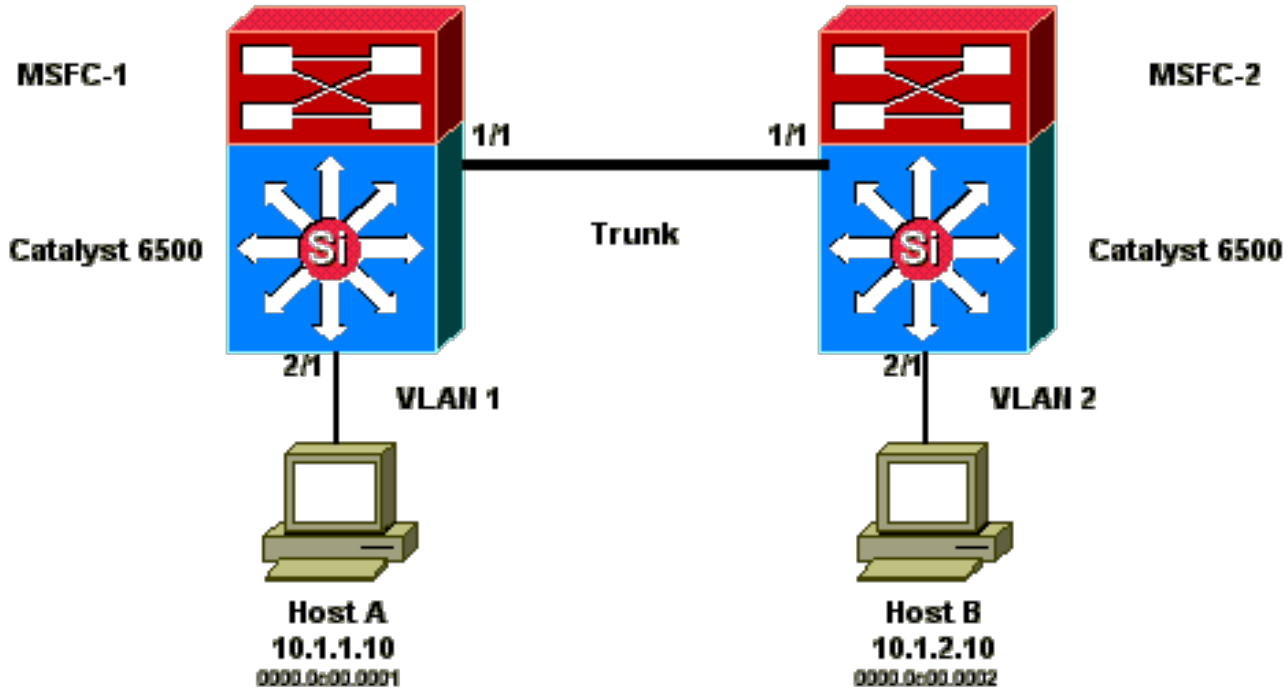
- Inundação excessiva de pacotes unicast
- Entrada de MLS ausente para fluxos
- Rastreamento de sniffer que mostra que os pacotes na porta do host não são destinados ao host
- Maior latência de rede com mecanismos de regravação de pacotes baseados em L2, como balanceadores de carga do servidor, dispositivos de Web cache e dispositivos de rede

  Os exemplos incluem o Cisco LocalDirector e o Cisco Cache Engine.
- Pacotes descartados nos hosts conectados e locais de trabalho que não podem lidar com a carga de tráfego de inundação unicast adicional

---

Observação: o tempo de envelhecimento do cache ARP padrão em um roteador é de quatro horas. O tempo de envelhecimento padrão da entrada de CAM (content-addressable memory, memória endereçável de conteúdo) do switch é de cinco minutos. O tempo de envelhecimento ARP das estações de trabalho do host não é significativo para esta discussão. Mas o exemplo define o tempo de envelhecimento ARP para quatro horas.

Este diagrama ilustra esse problema. Esse exemplo de topologia inclui Catalyst 6500s com MSFCs (Multilayer Switch Feature Cards, Placas de recursos de switch multicamadas) em cada switch. Embora esse exemplo use MSFCs, você pode usar qualquer roteador em vez de MSFC. Os exemplo de roteadores que você pode usar incluem o RSM (Route Switch Module, Módulo de switch de rota), o GSR (Gigabit Switch Router, Roteador de switch gigabit) e o Cisco 7500. Os hosts estão diretamente conectados às portas no switch. Os switches são interconectados por meio de um tronco que transporta o tráfego para a VLAN 1 e para a VLAN 2.



Essas saídas são extraídas da configuração do comando show standby de cada MSF.

MSFC1

```
interface Vlan 1
 mac-address 0003.6bf1.2a01
 ip address 10.1.1.2 255.255.255.0
 no ip redirects
 standby 1 ip 10.1.1.1
 standby 1 priority 110

interface Vlan 2
 mac-address 0003.6bf1.2a01
 ip address 10.1.2.2 255.255.255.0
 no ip redirects
 standby 2 ip 10.1.2.1

MSFC1#show standby
Vlan1 - Group 1
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.696
Hot standby IP address is 10.1.1.1 configured
Active router is local
Standby router is 10.1.1.3 expires in 00:00:07
Standby virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:20:40
Vlan2 - Group 2
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.776
Hot standby IP address is 10.1.2.1 configured
Active router is 10.1.2.3 expires in 00:00:09, priority 110
Standby router is local
4 state changes, last state change 00:00:51
```

```
MSFC1#exit
Console> (enable)
```

MSFC2

```
interface Vlan 1
 mac-address 0003.6bf1.2a02
 ip address 10.1.1.3 255.255.255.0
 no ip redirects
 standby 1 ip 10.1.1.1

interface Vlan 2
 mac-address 0003.6bf1.2a02
 ip address 10.1.2.3 255.255.255.0
 no ip redirects
 standby 2 ip 10.1.2.1
 standby 2 priority 110

MSFC2#show standby
Vlan1 - Group 1
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.242
Hot standby IP address is 10.1.1.1 configured
Active router is 10.1.1.2 expires in 00:00:09, priority 110
Standby router is local
7 state changes, last state change 00:01:17
Vlan2 - Group 2
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.924
Hot standby IP address is 10.1.2.1 configured
Active router is local
Standby router is 10.1.2.2 expires in 00:00:09
Standby virtual mac address is 0000.0c07.ac02
2 state changes, last state change 00:40:08
MSFC2#exit
```

Observação: no MSFC1, a VLAN 1 está no `estado ativo` do HSRP e a VLAN 2 está no estado de `standby` do HSRP. Em MSFC2, a VLAN 2 está no estado `ativo do HSRP e a VLAN 1 está no estado` standby do HSRP. O gateway padrão de cada host é o respectivo endereço IP em standby.

---

1. Inicialmente, todos os caches estão vazios. O host A usa MSFC1 como gateway padrão. O host B usa MSFC2.

   Tabelas de endereços ARP e MAC antes de iniciar o ping

Tabela ARP do Host A	Porta de VLAN MAC da tabela de endereços MAC do switch 1	Tabela MSFC1 ARP	Tabela MSFC2 ARP	Porta de VLAN MAC da tabela de endereços MAC do switch 2	Tabela ARP do Host B

	0003.6bf1.2a01 1 15/1			0003.6bf1.2a02 1 15/1	
	0003.6bf1.2a01 2 15/1			0003.6bf1.2a02 2 15/1	
	0000.0c07.ac01 1 15/1			0000.0c07.ac01 1 1/1	
	0000.0c07.ac02 2 1/1			0000.0c07.ac02 2 15/1	
	0003.6bf1.2a02 1 1/1			0003.6bf1.2a01 1 1/1	
	0003.6bf1.2a02 2 1/1			0003.6bf1.2a01 2 1/1	

Observação: resumindo, o endereço MAC do Switch 1 para o roteador HSRP e o endereço MAC não estão incluídos nas outras tabelas que aparecem nesta seção.

2. O host A executa o ping no host B, o que significa que o host A envia um pacote de ICMP Echo. Como cada host reside em uma VLAN separada, o host A encaminha os pacotes destinados ao host B para o gateway padrão. Para que esse processo ocorra, o host A deve enviar um ARP para resolver o endereço MAC de gateway padrão, 10.1.1.1.

   Tabelas de endereços ARP e MAC depois que o host A envia o ARP para o gateway padrão

Tabela ARP do Host A	Porta de VLAN MAC da tabela de endereços MAC do switch 1	Tabela MSFC1 ARP	Tabela MSFC2 ARP	Porta de VLAN MAC da tabela de endereços MAC do switch 2	Tabela ARP do Host B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001			

3. O MSFC1 recebe o pacote, regrava o pacote e encaminha o pacote para o host B. Para regravar o pacote, o MSFC1 envia uma solicitação ARP para o host B porque o host reside fora de uma interface diretamente conectada. O MSFC2 ainda precisa receber os pacotes nesse fluxo. Quando o MSFC1 recebe a resposta de ARP do host B, ambos os switches aprendem a porta de origem associada ao host B.

   Tabelas de ARP e endereço MAC depois que o host A envia um pacote ao gateway padrão e o MSFC1 envia o ARP para o host B

Tabela ARP do Host A	Porta de VLAN MAC da tabela de endereços MAC do switch 1	Tabela MSFC1 ARP	Tabela MSFC2 ARP	Porta de VLAN MAC da tabela de endereços MAC do switch 2	Tabela ARP do Host B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001		0000.0c00.0002 2 2/1	10.1.2.2 : 003.6bf1.2a01
	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0002			

4. O host B recebe o pacote de echo do host A, por meio do MSFC1. Agora o host B deve enviar uma resposta de echo para o host A. Como o host A reside em uma VLAN diferente, o host B encaminha a resposta por meio de gateway padrão, MSFC2. Para encaminhar o pacote por meio do MSFC2, o host B deve enviar um ARP para o endereço IP de gateway

padrão, 10.1.2.1.

Tabelas de endereços ARP e MAC depois que o host B envia o ARP para o gateway padrão

Tabela ARP do Host A	Porta de VLAN MAC da tabela de endereços MAC do switch 1	Tabela MSFC1 ARP	Tabela MSFC2 ARP	Porta de VLAN MAC da tabela de endereços MAC do switch 2	Tabela ARP do Host B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2 (0003.6bf1.2a01
	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0001			10.1.2.1 (0000.0c07.ac02

5. Agora o host B encaminha o pacote de resposta de echo para o MSFC2. O MSFC2 envia uma solicitação ARP para o host A porque está conectado diretamente à VLAN 1. O Switch 2 preenche a sua tabela de endereços MAC com o endereço MAC do host B.

Tabelas de endereços ARP e MAC após o pacote de echo ter sido recebido pelo host A

Tabela ARP do Host A	Porta de VLAN MAC da tabela de endereços MAC do switch 1	Tabela MSFC1 ARP	Tabela MSFC2 ARP	Porta de VLAN MAC da tabela de endereços MAC do switch 2	Tabela ARP d Host B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2 (0003.6bf1.2a0
10.1.1.3 : 0003.6bf1.2a0	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0001	10.1.1.10 0000.0c00.0001	0000.0c00.00001 1 1/1	10.1.2.1 (0000.0c07.ac0

6. A resposta de echo chega ao host A e o fluxo é concluído.

Consequências do roteamento assimétrico

Considere o caso do ping contínuo do host B pelo host A. Lembre-se de que o host A envia o pacote de echo para o MSFC1 e o host B envia a resposta de echo para o MSFC2, que está em um estado de roteamento assimétrico. A única vez que o switch 1 aprende o MAC de origem do host B é quando o host B responde a uma solicitação de ARP do MSFC1. Isso ocorre porque o host B usa o MSFC2 como gateway padrão e não envia os pacotes para o MSFC1 e, consequentemente, para o switch 1. Como o limite de tempo do ARP é de quatro horas por padrão, o switch 1 expira o endereço MAC do host B após cinco minutos por padrão. O switch 2 expira o host A após cinco minutos. Como resultado, o switch 1 deve tratar qualquer pacote com um MAC de destino do host B como unicast desconhecido. O switch inunda o pacote proveniente do host A e é destinado ao host B de todas as portas. Além disso, como não há entrada de endereço MAC do host B no switch 1, também não há entradas de MLS.

Tabelas de endereços ARP e MAC após 5 minutos de ping contínuo do host B pelo host A

Tabela ARP do	Porta de VLAN	Tabela MSFC1	Tabela MSFC2	Porta de VLAN	Tabela ARP do

Host A	MAC da tabela de endereços MAC do switch 1	ARP	ARP	MAC da tabela de endereços MAC do switch 2	Host B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2 : 003.6bf1.2a01
10.1.1.3 : 0003.6bf1.2a0		10.1.2.10 : 0000.0c00.0001	10.1.1.10 0000.0c00.0001		10.1.2.1 : 0000.0c07.ac01

Os pacotes de resposta de eco que vêm do host B experimentam o mesmo problema depois que a entrada do endereço MAC para o host A expira no Switch 2. O host B encaminha a resposta de eco para o MSFC2, que, por sua vez, roteia o pacote e o envia na VLAN 1. O switch não tem um host de entrada A na tabela de endereços MAC e deve inundar o pacote em todas as portas na VLAN 1.

Os problemas de roteamento assimétrico não interrompem a conectividade. Mas o roteamento assimétrico pode causar inundação unicast excessiva e entradas de MLS ausentes. Existem três alterações de configuração que podem remediar essa situação:

- Ajuste o tempo de envelhecimento MAC nos respectivos switches para 14.400 segundos (quatro horas) ou mais.
- Altere o limite de tempo do ARP nos roteadores para cinco minutos (300 segundos).
- Altere o tempo de envelhecimento MAC e o limite de tempo do ARP para o mesmo valor do limite de tempo.

O método preferencial é alterar o tempo de envelhecimento MAC para 14.400 segundos. Estas são as instruções de configuração:

- Cisco IOS Software:

  mac address-table aging-time <seconds> vlan <vlan_id>

Estudo de caso #6: o endereço IP virtual do HSRP é relatado como um endereço IP diferente

A mensagem de erro `STANDBY-3-DIFFVIP1 ocorre quando há vazamento entre VLANs devido a loops de ponte no switch.`

Se você receber essa mensagem de erro e houver um vazamento entre VLANs devido a loops de ponte no switch, siga estas etapas para resolver o erro:

1. Identificar o caminho que os pacotes seguem entre os nós finais.

   Se houver um roteador nesse caminho, execute estas etapas:

   a. Solucione os problemas do caminho do primeiro switch para o roteador.

b. Solucione os problemas do caminho do roteador para o segundo switch.

2. Conecte-se a cada switch no caminho e verifique o status das portas usadas no caminho entre os nós finais.

Estudo de caso #7: HSRP causa violação de MAC em uma porta segura

Quando a segurança de porta é configurada nas portas do switch que são conectadas aos roteadores habilitados para HSRP, isso causa uma violação de MAC, pois não é possível ter o mesmo endereço MAC seguro em mais de uma interface. Uma violação de segurança ocorre em uma porta segura em uma das situações a seguir:

- O número máximo de endereços MAC seguros é adicionado à tabela de endereços e uma estação cujo endereço MAC não está na tabela de endereços tenta acessar a interface.
- Um endereço aprendido ou configurado em uma interface segura é visualizado em outra interface segura na mesma VLAN.

Por padrão, uma violação de segurança da porta faz com que a interface do switch seja desativada por erro e desligada imediatamente, o que bloqueia as mensagens de status do HSRP entre os roteadores.

Solução

- Execute o comando standby use-bia nos roteadores. Isso força os roteadores a usarem um burned-in address para o HSRP, em vez do endereço MAC virtual.
- Desative a segurança das portas do switch conectadas aos roteadores habilitados para HSRP.

Estudo De Caso #9: %Interface Hardware Não Pode Suportar Vários Grupos

Se vários grupos de HSRP forem criados na interface, essa mensagem de erro será recebida:

```
%Interface hardware cannot support multiple groups
```

Essa mensagem de erro é recebida devido à limitação de hardware em alguns roteadores ou switches. Não é possível superar a limitação por nenhum método de software. O problema é que cada grupo de HSRP usa um endereço MAC adicional na interface, portanto, o chip MAC Ethernet deve respaldar vários endereços MAC programáveis para ativar diversos grupos de HSRP.

A solução alternativa é usar o comando de configuração de interface standby use-bia, que utiliza o Burned-In Address (BIA) da interface como endereço MAC virtual, em vez do endereço MAC pré-atribuído.

Identificar e Solucionar Problemas de HSRP em Switches Catalyst

A. Verifique a configuração do roteador HSRP

1. Verificar o Endereço IP Exclusivo da Interface do Roteador

Verifique se cada roteador do HSRP tem um endereço IP exclusivo para cada sub-rede de acordo com cada interface. Além disso, verifique se cada interface tem o protocolo de linha `ativo`. Para verificar rapidamente o estado atual de cada interface, execute o comando show ip interface brief. Aqui está um exemplo:

```
Router_1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.1     YES manual up                    up
Vlan10                 192.168.10.1    YES manual up                    up
Vlan11                 192.168.11.1    YES manual up                    up

Router_2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.2     YES manual up                    up
Vlan10                 192.168.10.2    YES manual up                    up
Vlan11                 192.168.11.2    YES manual up                    up
```

2. Verificar Endereços IP de Standby (HSRP) e Números de Grupos de Standby

Verifique se os endereços IP (HSRP) standby configurados e os números de grupo standby correspondem a cada roteador participante do HSRP. Uma incompatibilidade dos grupos standby ou dos endereços standby do HSRP pode causar problemas de HSRP. O comando show standby detalha o grupo standby e a configuração do endereço IP standby de cada interface. Aqui está um exemplo:

```
Router_1#show standby
Vlan10 - Group 110
  State is Active
    2 state changes, last state change 00:01:34
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.144 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-110" (default)
```

```
  FLAGS: 0/1
Vlan11 - Group 111
  State is Active
    2 state changes, last state change 00:00:27
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.096 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1

Router_2#show standby
Vlan10 - Group 110
  State is Standby
    1 state change, last state change 00:03:15
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.088 secs
  Preemption disabled
  Active router is 192.168.10.1, priority 110 (expires in 11.584 sec)
  Standby router is local
  Priority 109 (configured 109)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Standby
    1 state change, last state change 00:02:53
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.352 secs
  Preemption disabled
  Active router is 192.168.11.1, priority 110 (expires in 9.120 sec)
  Standby router is local
  Priority 109 (configured 109)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1
```

3. Verifique se o endereço IP de standby (HSRP) é diferente por interface

Verifique se o endereço IP (HSRP) standby é exclusivo no endereço IP configurado em cada interface. O comando show standby é uma referência rápida para exibir essas informações. Aqui está um exemplo:

```
Router_1#show standby
```

```
Vlan10 - Group 110
  State is Active
    2 state changes, last state change 00:01:34
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.144 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Active
    2 state changes, last state change 00:00:27
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.096 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1

Router_2#show standby
Vlan10 - Group 110
  State is Standby
    1 state change, last state change 00:03:15
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.088 secs
  Preemption disabled
  Active router is 192.168.10.1, priority 110 (expires in 11.584 sec)
  Standby router is local
  Priority 109 (configured 109)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Standby
    1 state change, last state change 00:02:53
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.352 secs
  Preemption disabled
  Active router is 192.168.11.1, priority 110 (expires in 9.120 sec)
  Standby router is local
  Priority 109 (configured 109)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1
```

4. Quando usar o comando standy use-bia

A menos que o HSRP esteja configurado em uma interface de Token Ting, use o comando standby use-bia somente em circunstâncias especiais. Esse comando instrui o roteador a usar o BIA, em vez do endereço MAC do HSRP virtual para o grupo de HSRP. Em uma rede de Token Ring, se a SRB (source-route bridging, ponte da rota de origem) estiver em uso, o comando standby use-bia permite que o novo roteador ativo atualize o cache do RIF (Routing Information Field, Campo de informações de roteamento) do host com um ARP gratuito. Mas nem todas as implementações de host processam o ARP gratuito corretamente. Outra advertência para o comando standby use-bia envolve o ARP de proxy. Um roteador de standby não pode cobrir o banco de dados de ARP de proxy perdido do roteador ativo que falhou.

5. Verificar a Configuração da Lista de Acesso

Verifique se as listas de acesso configuradas em todos os pares do HSRP não filtram os endereços de HSRP configurados nas interfaces. Especificamente, verifique o endereço multicast usado para enviar o tráfego para todos os roteadores em uma sub-rede (224.0.0.2). Além disso, verifique se o tráfego de UDP destinado à porta de HSRP 1985 não está filtrado. O HSRP usa esse endereço e a porta para enviar pacotes Hello entre os pares. Execute o comando show access-lists como uma referência rápida para anotar as listas de acesso configuradas no roteador. Aqui está um exemplo:

```
Router_1#show access-lists
Standard IP access list 77
    deny 10.19.0.0, wildcard bits 0.0.255.255
    permit any
Extended IP access list 144
    deny pim 238.0.10.0 0.0.0.255 any
    permit ip any any (58 matches)
```

B. Verificar a Configuração do Catalyst Fast EtherChannel e do Entroncamento

1. Verificar a Configuração do Entroncamento

Se um tronco for usado para conectar os roteadores do HSRP, verifique as configurações de entroncamento nos roteadores e switches. Há cinco modos de entroncamento possíveis:

- ligado
- desirable
- automático

- desligado
- sem negociação

Verifique se os modos de entroncamento configurados fornecem o método de entroncamento desejado.

Use a `configuração desejada para conexões switch a switch ao solucionar os problemas de HSRP.` Essa configuração pode isolar os problemas em que as portas do switch não conseguem estabelecer troncos corretamente. Defina uma configuração de roteador a switch como nonegotiate, pois a maioria dos roteadores Cisco IOS não é compatível com a negociação de um tronco.

Para o modo trunking IEEE 802.1Q (dot1q), verifique se ambos os lados do tronco estão configurados para usar a mesma VLAN nativa e encapsulamento. Como os produtos Cisco não marcam a VLAN nativa por padrão, uma incompatibilidade nas configurações de VLAN nativa resulta em nenhuma conectividade nas VLANs incompatíveis. Por fim, verifique se o tronco está configurado para transportar as VLANs configuradas no roteador e verifique se as VLANs não foram removidas e estão no estado do STP para as portas conectadas ao roteador. Emita o comando show interfaces <interface> trunk para obter uma referência rápida que mostre essas informações. Aqui está um exemplo:

```
L2Switch_1#show interfaces gigabitEthernet1/0/13 trunk Port Mode Encapsulation Status Native vlan Gi1/0/13 on 802.1q trunking 1 Port Vlans allowed o
Router_1#show interfaces gigabitEthernet1/0/1 trunk Port Mode Encapsulation Status Native vlan Gi1/0/1 on 802.1q trunking 1 Port Vlans allowed on trun
```

2. Verificar a Configuração do Fast EtherChannel (Port Channeling)

Se um canal da porta for usado para conectar os roteadores do HSRP, verifique a configuração EtherChannel nos roteadores e switches. Configure um canal da porta switch a switch como desejado em pelo menos um lado. O outro lado pode estar em qualquer um destes modos:

- ligado
- desirable
- automático

No entanto, neste exemplo, as interfaces não são membros de um canal de porta:

```
Router_1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
```

```
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 0
Number of aggregators:           0

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

Router_1#

Router_2#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 0
Number of aggregators:           0

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

Router_2#
```

3. Investigar a Tabela de Encaminhamento de Endereços MAC do Switch

Verifique se existem entradas da tabela de endereços MAC no switch para os roteadores do HSRP para o endereço MAC virtual do HSRP e o BIA físico. O comando show standby no roteador fornece o endereço MAC virtual. O comando show interface fornece o Bia físico. Veja a seguir exemplos de saídas:

```
Router_1#show standby
Vlan10 - Group 110
  State is Active
    2 state changes, last state change 00:37:03
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
```

```
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.768 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.2, priority 109 (expires in 10.368 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Active
    2 state changes, last state change 00:35:56
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.472 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.11.2, priority 109 (expires in 8.336 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1

Router_1#show interfaces vlan 10
Vlan10 is up, line protocol is up , Autostate Enabled
  Hardware is Ethernet SVI, address is d4e8.801f.4846 (bia d4e8.801f.4846)
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     9258 packets input, 803066 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     3034 packets output, 368908 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 2 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out

L2Switch_1#show mac address-table address 0000.0c07.ac6e
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0000.0c07.ac6e    DYNAMIC     Gi1/0/13
Total Mac Addresses for this criterion: 1

L2Switch_1#show mac address-table address 0000.0c07.ac6f
```

```
        Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  11    0000.0c07.ac6f    DYNAMIC     Gi1/0/13
Total Mac Addresses for this criterion: 1
```

Verifique o tempo de envelhecimento de CAM para determinar a rapidez com que as entradas expiram. Se o tempo for igual ao valor configurado para o atraso de encaminhamento do STP, que é de 15 segundos por padrão, há uma grande possibilidade de haver um loop de STP na rede. Este é um exemplo da saída do comando:

```
L2Switch_1#show mac address-table aging-time  vlan 10
Global Aging Time:  300
Vlan    Aging Time
----    ----------
  10     300

L2Switch_1#show mac address-table aging-time  vlan 11
Global Aging Time:  300
Vlan    Aging Time
----    ----------
  11     300
```

C. Verificar a conectividade da camada física

Se mais de um roteador em um grupo de HSRP se tornar ativo, esses roteadores não receberão de forma contínua os pacotes Hello dos pares do HSRP. Os problemas da camada física podem impedir a passagem contínua de tráfego entre os pares e causar esse cenário. Verifique a conectividade física e a conectividade IP entre os pares do HSRP ao solucionar os problemas do HSRP. Execute o comando show standby para verificar a conectividade. Aqui está um exemplo:

```
Router_1#show standby
Vlan10 - Group 110
  State is Active
    2 state changes, last state change 00:54:03
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.848 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
```

```
Vlan11 - Group 111
  State is Active
    2 state changes, last state change 00:52:56
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.512 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1

Router_2#show standby
Vlan10 - Group 110
  State is Init (interface down)
    2 state changes, last state change 00:00:42
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is unknown (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 109 (configured 109)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Init (interface down)
    2 state changes, last state change 00:00:36
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is unknown (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 109 (configured 109)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1
```

1. Verificar o Status da Interface

Verifique as interfaces. Verifique se todas as interfaces configuradas para HSRP estão `ativas/ativas`, como mostra este exemplo:

```
Router_1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.1     YES manual up                    up
Vlan10                 192.168.10.1    YES manual up                    up
Vlan11                 192.168.11.1    YES manual up                    up
```

```
Router_2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.2     YES manual up                    up
Vlan10                 192.168.10.2    YES manual administratively down down
Vlan11                 192.168.11.2    YES manual administratively down down
```

Se alguma interface estiver administrativamente `inativa/inativa`, entre no modo de configuração no roteador e execute o comando específico da interface no shutdown. Aqui está um exemplo:

```
Router_2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_2(config)#interface vlan 10
Router_2(config-if)#no shutdown
Router_2(config-if)#end
```

```
Router_2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_2(config)#interface vlan 11
Router_2(config-if)#no shutdown
Router_2(config-if)#end

Router_2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.2     YES manual up                    up
Vlan10                 192.168.10.2    YES manual up                    down
Vlan11                 192.168.11.2    YES manual up                    up
```

Se alguma interface estiver `inativa/inativa ou ativa/inativa`, analise o log quanto a notificações de alteração da interface. Para os switches baseados no software Cisco IOS, essas mensagens aparecem para `situações de link ativo/inativo:`

```
%LINK-3-UPDOWN: Interface "interface", changed state to up
%LINK-3-UPDOWN: Interface "interface", changed state to down

Router_1#show log
3d04h: %STANDBY-6-STATECHANGE: Standby: 0: Vlan10 state Active-> Speak
3d04h: %LINK-5-CHANGED: Interface Vlan10, changed state to down
3d04h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
```

Inspecione as portas, os cabos e quaisquer transceptores ou outros dispositivos entre os pares do HSRP. Alguém removeu ou flexibilizou as conexões? Existem interfaces que perdem um link repetidamente? Os tipos de cabo apropriados são usados? Verifique se há erros nas interfaces, conforme mostrado neste exemplo:

```
Router_2#show interface vlan 10
Vlan10 is down, line protocol is down , Autostate Enabled
```

```
  Hardware is Ethernet SVI, address is 1880.90d8.5946 (bia 1880.90d8.5946)
  Internet address is 192.168.10.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:10, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1243 packets input, 87214 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     23 packets output, 1628 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 2 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

2. Alteração de Link e Erros de Porta

Verifique as alterações de link das portas do switch e outros erros. Execute esses comandos e analise a saída:

- show logging
- show interfaces <interface> counters
- show interfaces <interface> status

Esses comandos ajudam a determinar se existe um problema na conectividade entre os switches e outros dispositivos.

Essas mensagens são normais para situações de link `ativo/inativo`:

```
L2Switch_1#show logging
Syslog logging: enabled (0 messages dropped, 5 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level informational, 319 messages logged, xml disabled,
                     filtering disabled
```

```
   Monitor logging: level debugging, 0 messages logged, xml disabled,
                    filtering disabled
   Buffer logging:  level debugging, 467 messages logged, xml disabled,
                    filtering disabled
   Exception Logging: size (4096 bytes)
   Count and timestamp logging messages: disabled
   File logging: disabled
   Persistent logging: disabled

No active filter modules.

   Trap logging: level informational, 327 message lines logged
      Logging Source-Interface:       VRF Name:

Log Buffer (10000 bytes):
*Jul 26 17:52:07.526: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up
*Jul 26 17:52:09.747: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down
*Jul 26 17:57:11.716: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307.
*Jul 26 17:57:11.716: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type.
*Jul 26 17:57:13.583: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up
*Jul 26 17:57:16.237: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down
*Jul 26 18:02:16.481: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307.
*Jul 26 18:02:16.481: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type.
*Jul 26 18:02:18.367: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up
*Jul 26 18:02:20.561: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down
```

`Execute o comando` show interfaces <interface> status para determinar a integridade geral de uma porta. Aqui está um exemplo:

```
L2Switch_1#show interfaces gigabitEthernet 1/0/13 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/13                     connected    trunk      a-full a-1000 10/100/1000BaseTX
```

O status da interface é `connected`, `notconnect` ou `errdisable`? Se o status for `não conectado`, verifique se o cabo está conectado nos dois lados. Verifique se o cabo apropriado está sendo usado. Se o status for errdisable, verifique os contadores quanto a excesso de erros. Consulte Recuperar o Estado da Porta Errdisable nas Plataformas Cisco IOS para obter mais informações.

Para qual VLAN esta porta está configurada? Verifique se o outro lado da conexão está configurado para a mesma VLAN. Se o link estiver configurado para ser um tronco, verifique se ambos os lados do tronco transportam as mesmas VLANs.

Qual é a configuração de velocidade e de duplex? Se a configuração for precedida por a-, a porta está configurada para negociar automaticamente a velocidade e o duplex. Caso contrário, o administrador de rede predeterminou essa configuração. Para a configuração de velocidade e de duplex de um link, as definições em ambos os lados do link devem corresponder. Se uma porta do switch estiver configurada para negociação automática, o outro lado do link também deverá estar configurado para negociação automática. Se um lado está codificado por hardware para

uma velocidade e um dúplex específicos, o outro lado também deve estar codificado por hardware. Se você deixar um lado como negociação automática, enquanto o outro lado estiver codificado, você interromperá o processo de negociação automática.

<#root>

L2Switch_1#show interfaces gi1/0/13 counters errors Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards Gi1/0/13

```
 0 0 0 0 0 0

 Port Single-Col Multi-Col Late-Col Excess-Col Carri-Sen Runs Gi1/0/13

0 0 0 0 0 0
```

Existem muitos Align-Err, FCS-Err ou Runts? Indicam uma incompatibilidade de velocidade ou do dúplex entre a porta e o dispositivo de conexão. Altere as configurações de velocidade e de duplex dessa porta para ajudar a corrigir esses erros.

Execute o comando show mac para verificar se a porta está transmitindo o tráfego. As colunas `In` e `Out` indicam o número de pacotes unicast, multicast e broadcast que são recebidos e transmitidos em uma porta específica. Os contadores inferiores revelam quantos pacotes são descartados ou perdidos e se esses pacotes fazem parte do tráfego de entrada ou saída. `Lrn-Discrd`, `In-Lost` e `Out-Lost` contam o número de pacotes enviados por engano ou descartados devido a buffers insuficientes.

L2Switch_1#show interfaces gi1/0/13 counters

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi1/0/13	304933333	1180453	1082538	14978

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
Gi1/0/13	282752538	276716	824562	588960

3. Verificar a Conectividade IP

Verifique a conectividade IP. Emita um ping IP do roteador associado para o dispositivo HSRP remoto. Isso ajuda a expor as perdas momentâneas de conectividade. Um ping estendido está disponível somente no modo Enable. Este é um exemplo da saída do comando:

```
Router_1#show run interface vlan 10
Building configuration...

Current configuration : 141 bytes
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
```

```
 standby 110 ip 192.168.10.100
 standby 110 priority 110
 standby 110 preempt
end

Router_2#show run interface vlan 10
Building configuration...

Current configuration : 120 bytes
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby 110 ip 192.168.10.100
 standby 110 priority 109
end

Router_1#ping 192.168.10.2 repeat 1500
Type escape sequence to abort.
Sending 1500, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/2/9 ms
```

Execute o ping de cada roteador do HSRP para os pares a fim de determinar o local da falha na conectividade.

4. Verificar Link Unidirecional

Verifique o switch quanto a links unidirecionais entre os pares do HSRP. Um link unidirecional ocorre sempre que o tráfego sobre o qual um dispositivo local transmite um link é recebido pelo vizinho, mas o tráfego sobre o qual o vizinho transmite não é recebido pelo dispositivo local. Esse recurso é conhecido como modo agressivo de UDLD (UniDirectional Link Detection, Detecção de link unidirecional). O uso do UDLD só será possível se os dois lados da conexão respaldarem o recurso. O modo agressivo de UDLD opera na L2 para determinar se um link está conectado

corretamente e se o tráfego flui bidirecionalmente entre os vizinhos corretos. Veja a seguir exemplos de saídas de comando:

Observação: navegue até o próximo link para Compreender e configurar o recurso UDLD depende de qual plataforma é usada.

Outra opção que pode ajudar a verificar um link unidirecional se o UDLD não estiver disponível é com o uso do Cisco Discovery Protocol (CDP). A ativação do CDP é outra forma de detectar se existe um link unidirecional. Se apenas um lado de um link puder ver o dispositivo vizinho, substitua o cabo entre os dispositivos e verifique se há interfaces defeituosas.

```
Router_1#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is  enabled

Router_1#show cdp neighbors gi1/0/1 detail
-------------------------
Device ID: L2Switch_1.cisco.com
Entry address(es):
  IP address: 192.168.70.1
  IPv6 address: 2001:420:140E:2101::1  (global unicast)
  IPv6 address: FE80::2FE:C8FF:FED3:86C7  (link-local)
Platform: cisco WS-C3650-12X48UR,  Capabilities: Router Switch IGMP
Interface: GigabitEthernet1/0/1,  Port ID (outgoing port): GigabitEthernet1/0/13
Holdtime : 173 sec

Version :
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.8, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Wed 13-Feb-19 03:00 by mcpre

advertisement version: 2
VTP Management Domain: 'CALOnet'
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 192.168.70.1
Spare Pair PoE: Yes, Spare Pair Detection Required: No
Spare Pair PD Config: Disable, Spare Pair PSE Operational: No


Total cdp entries displayed : 1
```

5. Referências Adicionais de Identificação e Solução de Problemas da Camada Física

Consulte estes documentos:

- Configuração e Troubleshooting da Negociação Automática de Ethernet 10/100/1000 Mb Half/Full-Duplex
- Recuperar estado de porta errdisable nas plataformas Cisco IOS
- Troubleshooting de Compatibilidade entre Catalyst Switches e NIC Compatibility Issues
- A seção Noções básicas sobre erros de link de dados da Solução de problemas dos Switches Cisco Catalyst para questões de compatibilidade de NIC
- Troubleshooting de Portas de Switches e Interfaces

D. Depuração de HSRP de camada 3

Se as alterações de estado do HSRP forem frequentes, use os comandos debug do HSRP (no modo de ativação) no roteador para observar a atividade do HSRP. Essas informações ajudam a determinar os pacotes HSRP recebidos e enviados pelo roteador. Reúna essas informações se você criar uma solicitação de serviço com o Suporte técnico da Cisco. A saída de depuração também mostra as informações de estado do HSRP, juntamente com as contas detalhadas do pacote Hello do HSRP.

1. Depuração HSRP Padrão

No Cisco IOS, habilite o recurso de depuração HSRP com o comando debug standby. Essas informações são úteis quando os problemas são intermitentes e afetam apenas algumas interfaces. A depuração permite determinar se o roteador do HSRP em questão recebe e transmite os pacotes Hello do HSRP em intervalos específicos. Se o roteador não receber pacotes Hello, você pode inferir que o par não transmite os pacotes Hello ou a rede descarta os pacotes.

Comando	Propósito
debug standby	Ativa a depuração do HSRP

Este é um exemplo da saída do comando:

```
Router_1#debug standby
HSRP debugging is on
Jul 29 16:12:16.889: HSRP: Vl10 Grp 110 Hello  out 192.168.10.1 Active  pri 110 vIP 192.168.10.100
Jul 29 16:12:16.996: HSRP: Vl11 Grp 111 Hello  in  192.168.11.2 Standby pri 109 vIP 192.168.11.100
Jul 29 16:12:17.183: HSRP: Vl10 Grp 110 Hello  in  192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:12:17.366: HSRP: Vl11 Grp 111 Hello  out 192.168.11.1 Active  pri 110 vIP 192.168.11.100
Jul 29 16:12:18.736: HSRP: Vl10 Interface adv in, Passive, active 0, passive 1, from 192.168.10.2
Jul 29 16:12:19.622: HSRP: Vl10 Grp 110 Hello  out 192.168.10.1 Active  pri 110 vIP 192.168.10.100
```

2. Depuração Condicional de HSRP (Limitando a Saída com Base no Grupo em Standby e/ou VLAN)

O Software Cisco IOS versão 12.0(3) apresentou uma condição de depuração para permitir que a saída do comando debug standby seja filtrada com base na interface e no número do grupo. O comando utiliza o paradigma da condição de depuração apresentado no Software Cisco IOS versão 12.0.

Comando	Propósito
debug condition standby <interface> <group>	Habilita a depuração condicional de HSRP do grupo (0-255)

A interface deve ser uma interface válida que possa respaldar o HSRP. O grupo pode ser qualquer grupo, de 0 a 255. Uma condição de depuração pode ser definida para os grupos que não existem. Isso permite a captura de depurações durante a inicialização de um novo grupo. O debug standby deve ser ativado para produzir qualquer saída de depuração. Se não existir condições de depuração standby, a saída de depuração será produzida para todos os grupos em todas as interfaces. Se existir pelo menos uma condição de depuração standby, a saída de depuração standby será filtrada com base em todas as condições de depuração standby. Este é um exemplo da saída do comando:

```
Router_1#debug condition standby vlan 10 110
Condition 1 set
Router_1#
Jul 29 16:16:20.284: Vl10 HSRP110 Debug: Condition 1, hsrp Vl10 HSRP110 triggered, count 1
Router_1#debug standby
HSRP debugging is on
Router_1#
Jul 29 16:16:44.797: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:45.381: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:16:47.231: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:48.248: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
```

3. Depuração de HSRP aprimorada

O software Cisco IOS versão 12.1(1) adicionou a depuração aprimorada de HSRP. Para ajudar a localizar informações úteis, a depuração aprimorada de HSRP limita o ruído das mensagens Hello periódicas e inclui informações adicionais de estado. Essas informações são particularmente úteis quando você trabalha com um engenheiro do Suporte técnico da Cisco, se criar uma solicitação de serviço.

Comando	Propósito
debug standby	Exibe todos os erros, eventos e pacotes do HSRP
debug standby errors	Exibe os erros do HSRP
debug standby events [[all] | [hsrp | redundância | track]] [detail]	Exibe os eventos do HSRP
debug standby packets [[all | terse] | [advertise | coup | olá | resign]] [detail]	Exibe os pacotes do HSRP

debug standby terse	Exibir uma faixa limitada de erros, eventos e pacotes do HSRP

Este é um exemplo da saída do comando:

```
Router_2#debug standby terse
HSRP:
  HSRP Errors debugging is on
  HSRP Events debugging is on
    (protocol, neighbor, redundancy, track, ha, arp, interface)
  HSRP Packets debugging is on
    (Coup, Resign)
Router_2#
*Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Resign in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Standby: i/Resign rcvd (110/192.168.10.1)
*Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Active router is local, was 192.168.10.1
*Jul 29 16:49:35.416: HSRP: Vl10 Nbr 192.168.10.1 no longer active for group 110 (Standby)
*Jul 29 16:49:35.417: HSRP: Vl10 Nbr 192.168.10.1 Was active or standby - start passive holddown
*Jul 29 16:49:35.417: HSRP: Vl10 Grp 110 Standby router is unknown, was local
*Jul 29 16:49:35.417: HSRP: Vl10 Grp 110 Standby -> Active
*Jul 29 16:49:35.418: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active
*Jul 29 16:49:35.418: HSRP: Peer not present
*Jul 29 16:49:35.418: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Standby -> Active
*Jul 29 16:49:35.419: HSRP: Vl10 Grp 110 Added 192.168.10.100 to ARP (0000.0c07.ac6e)
*Jul 29 16:49:35.420: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" standby, local -> unknown
*Jul 29 16:49:35.421: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" update, Standby -> Active
*Jul 29 16:49:38.422: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" update, Active -> Active
```

Você pode usar a depuração condicional de interface e/ou grupo de HSRP para filtrar essa saída de depuração.

Comando	Propósito
debug condition interface interface	Ativa a depuração condicional da interface
debug condition standby <interface> <group>	Ativa a depuração condicional do HSRP

Neste exemplo, o roteador entra em um grupo de HSRP preexistente:

```
Rotuer_2#debug condition standby vlan 10 110
Condition 1 set
Router_2#debug condition interface gigabitEthernet 1/0/1 vlan-id 10
Condition 2 set
Router_2#debug standby
HSRP debugging is on
Router_2#
*Jul 29 16:54:12.496: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Active  pri 109 vIP 192.168.10.100
*Jul 29 16:54:15.122: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Active  pri 109 vIP 192.168.10.100
*Jul 29 16:54:17.737: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Active  pri 109 vIP 192.168.10.100
*Jul 29 16:54:18.880: HSRP: Vl10 Nbr 192.168.10.1 is passive
*Jul 29 16:54:20.316: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Active  pri 109 vIP 192.168.10.100
*Jul 29 16:54:20.322: HSRP: Vl10 Grp 110 Coup   in  192.168.10.1 Listen  pri 110 vIP 192.168.10.100
*Jul 29 16:54:20.323: HSRP: Vl10 Grp 110 Active: j/Coup rcvd from higher pri router (110/192.168.10.1)
```

```
*Jul 29 16:54:20.323: HSRP: Vl10 Grp 110 Active router is 192.168.10.1, was local
*Jul 29 16:54:20.323: HSRP: Vl10 Nbr 192.168.10.1 is no longer passive
*Jul 29 16:54:20.324: HSRP: Vl10 Nbr 192.168.10.1 active for group 110
*Jul 29 16:54:20.324: HSRP: Vl10 Grp 110 Active -> Speak
*Jul 29 16:54:20.325: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak
*Jul 29 16:54:20.325: HSRP: Peer not present
*Jul 29 16:54:20.325: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Active -> Speak
*Jul 29 16:54:20.326: HSRP: Vl10 Grp 110 Removed 192.168.10.100 from ARP
*Jul 29 16:54:20.326: HSRP: Vl10 Grp 110 Deactivating MAC 0000.0c07.ac6e
*Jul 29 16:54:20.327: HSRP: Vl10 Grp 110 Removing 0000.0c07.ac6e from MAC address filter
*Jul 29 16:54:20.328: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Speak   pri 109 vIP 192.168.10.100
*Jul 29 16:54:20.328: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:23.104: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Speak   pri 109 vIP 192.168.10.100
*Jul 29 16:54:23.226: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:25.825: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:25.952: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Speak   pri 109 vIP 192.168.10.100
*Jul 29 16:54:28.427: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:28.772: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Speak   pri 109 vIP 192.168.10.100
*Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Speak: d/Standby timer expired (unknown)
*Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Standby router is local
*Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Speak -> Standby
*Jul 29 16:54:30.727: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Speak -> Standby
*Jul 29 16:54:30.728: HSRP: Peer not present
*Jul 29 16:54:30.728: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Speak -> Standby
*Jul 29 16:54:30.728: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:31.082: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:33.459: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:33.811: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:36.344: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:36.378: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:38.856: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:38.876: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:41.688: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:41.717: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
```

E. Troubleshooting de Spanning Tree

As condições de loop do STP ou instabilidade em uma rede podem impedir a comunicação adequada dos pares do HSRP. Devido a essa comunicação inadequada, cada par se torna um roteador ativo. Os loops do STP podem causar congestionamento de transmissões, quadros duplicados e inconsistência na tabela MAC. Todos esses problemas afetam toda a rede e, especialmente, o HSRP. As mensagens de erro do HSRP podem ser a primeira indicação de um problema de STP.

Ao solucionar os problemas do STP, você deve entender a topologia do STP da rede em cada VLAN. Você deve determinar qual switch é a ponte de origem e quais portas no switch estão no bloqueio e no encaminhamento. Como cada VLAN tem sua própria topologia de STP, essas informações são muito importantes em cada VLAN.

1. Verificar a Configuração do Spanning Tree

Verifique se o STP está configurado em cada switch e dispositivo de ponte na rede. Anote onde

cada switch acredita que a ponte de origem está localizada. Além disso, observe os valores desses temporizadores:

- idade máxima da raiz
- hello time
- retardo de encaminhamento

Execute o comando show spanning-tree para ver todas essas informações. Por padrão, o comando mostra essas informações para todas as VLANs. Mas você também pode filtrar outras informações de VLAN se fornecer o número da VLAN com o comando. Essas informações são muito úteis ao solucionar os problemas do STP.

Esses três temporizadores que você observa na saída de show spanning-tree são aprendidos da bridge raiz. Esses temporizadores não precisam corresponder aos temporizadores definidos nessa ponte específica. Mas verifique se os temporizadores correspondam à ponte de origem, caso esse switch se torne a ponte de origem a qualquer momento. Essa correspondência dos temporizadores com a ponte de origem ajuda a manter uma administração contínua e fácil. A correspondência também impede que um switch com temporizadores incorretos prejudiquem a rede.

Observação: habilite o STP para todas as VLANs o tempo todo, independentemente de haver ou não links redundantes na rede. Se ativar o STP em redes não redundantes, você evitará um rompimento. Um rompimento pode ocorrer se alguém fizer uma ponte entre switches e hubs ou outros switches e criar acidentalmente um loop físico. O STP também é muito útil no isolamento de problemas específicos. Se a ativação do STP afetar a operação de algo na rede, pode existir um problema que você precisa isolar.

Aqui está um exemplo de saída do comando show spanning-tree:

```
L2Switch_1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
             Address     00fe.c8d3.8680
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00fe.c8d3.8680
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/3            Desg FWD 4         128.3    P2p
Gi1/0/10           Desg FWD 4         128.10   P2p Edge
Gi1/0/11           Desg FWD 4         128.11   P2p
```

```
Gi1/0/13         Desg FWD 4        128.13   P2p
Gi1/0/14         Desg FWD 4        128.14   P2p
Gi1/0/15         Desg FWD 4        128.15   P2p
Gi1/0/16         Desg FWD 4        128.16   P2p
Gi1/0/35         Desg FWD 4        128.35   P2p


L2Switch_1#show spanning-tree vlan 11

VLAN0011
  Spanning tree enabled protocol rstp
  Root ID    Priority    32779
             Address     00fe.c8d3.8680
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32779  (priority 32768 sys-id-ext 11)
             Address     00fe.c8d3.8680
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/3            Desg FWD 4         128.3    P2p
Gi1/0/10           Desg FWD 4         128.10   P2p Edge
Gi1/0/11           Desg FWD 4         128.11   P2p
Gi1/0/13           Desg FWD 4         128.13   P2p
Gi1/0/14           Desg FWD 4         128.14   P2p
Gi1/0/15           Desg FWD 4         128.15   P2p
Gi1/0/16           Desg FWD 4         128.16   P2p
Gi1/0/35           Desg FWD 4         128.35   P2p
```

O switch L2Switch_1 é a raiz da VLAN 10 e da VLAN 11.

2. Condições de Loop do Spanning Tree

Para que um loop de STP ocorra, deve haver redundância física L2 na rede. Um STP não ocorre se não houver possibilidade de uma condição de loop físico. Os sintomas de uma condição de loop de STP são os seguintes:

- Interrupção total da rede
- Perda de conectividade
- O relatório por equipamento de rede de alta utilização do processo e do sistema

Uma única VLAN que experimenta uma condição de loop de STP pode congestionar um link e privar as outras VLANs da largura de banda. O comando show interfaces <interface> controller observa quais portas transmitem ou recebem um número excessivo de pacotes. O excesso de broadcast e multicast pode indicar as portas que fazem parte de um loop de STP. Como regra geral, suspeite de um link de uma condição de loop de STP a qualquer momento, se o multicast ou broadcast exceder o número de pacotes unicast.

> Observação: o switch também conta as unidades de dados de protocolo de ponte (BPDUs) do STP que são recebidas e transmitidas como quadros multicast. Uma porta que está no estado de bloqueio do STP ainda transmite e recebe as BPDUs do STP.

```
Router_2#show interfaces gi1/0/1 controller
GigabitEthernet1/0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 1880.90d8.5901 (bia 1880.90d8.5901)
  Description: PNP STARTUP VLAN
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is on, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 33000 bits/sec, 31 packets/sec
  5 minute output rate 116000 bits/sec, 33 packets/sec
     9641686 packets input, 1477317083 bytes, 0 no buffer
     Received 1913802 broadcasts (1151766 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 1151766 multicast, 0 pause input
     0 input packets with dribble condition detected
     10702696 packets output, 4241534645 bytes, 0 underruns
     Output 3432 broadcasts (0 multicasts)
     0 output errors, 0 collisions, 2 interface resets
     9582 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Transmit                GigabitEthernet1/0/1          Receive
   4241534645 Total bytes                1477317083 Total bytes
     10562003 Unicast frames                7727884 Unicast frames
   4229489212 Unicast bytes              1291270617 Unicast bytes
      137261 Multicast frames              1151766 Multicast frames
     11812065 Multicast bytes              91096867 Multicast bytes
        3432 Broadcast frames              762036 Broadcast frames
      233368 Broadcast bytes              94949599 Broadcast bytes
           0 System FCS error frames             0 IpgViolation frames
           0 MacUnderrun frames                  0 MacOverrun frames
           0 Pause frames                  0 Pause frames
           0 Cos 0 Pause frames                  0 Cos 0 Pause frames
           0 Cos 1 Pause frames                  0 Cos 1 Pause frames
           0 Cos 2 Pause frames                  0 Cos 2 Pause frames
           0 Cos 3 Pause frames                  0 Cos 3 Pause frames
           0 Cos 4 Pause frames                  0 Cos 4 Pause frames
           0 Cos 5 Pause frames                  0 Cos 5 Pause frames
           0 Cos 6 Pause frames                  0 Cos 6 Pause frames
           0 Cos 7 Pause frames                  0 Cos 7 Pause frames
           0 Oam frames                  0 OamProcessed frames
```

0 Oam frames	0 OamDropped frames
38144 Minimum size frames	4165201 Minimum size frames
4910833 65 to 127 byte frames	3126489 65 to 127 byte frames
1237675 128 to 255 byte frames	750243 128 to 255 byte frames
1029126 256 to 511 byte frames	1279281 256 to 511 byte frames
2205966 512 to 1023 byte frames	103668 512 to 1023 byte frames
1280952 1024 to 1518 byte frames	205229 1024 to 1518 byte frames
0 1519 to 2047 byte frames	11575 1519 to 2047 byte frames
0 2048 to 4095 byte frames	0 2048 to 4095 byte frames
0 4096 to 8191 byte frames	0 4096 to 8191 byte frames
0 8192 to 16383 byte frames	0 8192 to 16383 byte frames
0 16384 to 32767 byte frame	0 16384 to 32767 byte frame
0 > 32768 byte frames	0 > 32768 byte frames
0 Late collision frames	0 SymbolErr frames
0 Excess Defer frames	0 Collision fragments
0 Good (1 coll) frames	0 ValidUnderSize frames
0 Good (>1 coll) frames	0 InvalidOverSize frames
0 Deferred frames	0 ValidOverSize frames
0 Gold frames dropped	0 FcsErr frames
0 Gold frames truncated	
0 Gold frames successful	
0 1 collision frames	
0 2 collision frames	
0 3 collision frames	
0 4 collision frames	
0 5 collision frames	
0 6 collision frames	
0 7 collision frames	
0 8 collision frames	
0 9 collision frames	
0 10 collision frames	
0 11 collision frames	
0 12 collision frames	
0 13 collision frames	
0 14 collision frames	
0 15 collision frames	
0 Excess collision frames	

LAST UPDATE 2384 msecs AGO

3. Notificação de Alteração de Topologia

Outro comando vital para o diagnóstico de problemas de STP é o comando show spanning-tree detail. Esse comando rastreia as mensagens de TCN (Topology Change Notification, Notificação de alteração de topologia) até o originador. Essas mensagens, enviadas como BPDUs especiais entre switches, indicam que houve uma alteração de topologia em um switch. Esse switch envia uma TCN para a porta de origem. A TCN é enviada para a ponte de origem. A ponte de origem envia outra BPDU especial, uma TCA (Topology Change Acknowledgement, Confirmação de alteração de topologia) para todas as portas. A ponte de origem define o bit de TCN na BPDU de configuração. Isso faz com que todas as pontes que não são de origem definam o temporizador de envelhecimento da tabela de endereços MAC como o atraso de encaminhamento do STP de configuração.

Para isolar esse problema, acesse a bridge raiz de cada VLAN e emita o comando show spanning-tree <interface> detail para as portas conectadas ao switch. A entrada `Ocorreu a última alteração` fornece a hora em que o último TCN foi recebido. Nessa situação, é tarde demais para ver quem emitiu as TCNs que podem ter causado o possível loop de STP. A entrada `Number of topology changes` dá uma ideia sobre o número de TCNs que ocorrem. Durante um loop de STP, esse contador pode ser aumentado a cada minuto. Consulte Problemas do Protocolo Spanning Tree e considerações sobre o projeto relacionado para obter mais informações.

Outras informações úteis incluem:

- Porta da última TCN
- Hora da última TCN
- Contagem atual de TCNs

Este é um exemplo da saída do comando:

```
L2Switch_1#show spanning-tree vlan 10 detail

 VLAN0010 is executing the rstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 10, address 00fe.c8d3.8680
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 8 last change occurred 03:21:48 ago
        from GigabitEthernet1/0/35
  Times:  hold 1, topology change 35, notification 2
        hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 3 (GigabitEthernet1/0/3) of VLAN0010 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.3.
   Designated root has priority 32778, address 00fe.c8d3.8680
   Designated bridge has priority 32778, address 00fe.c8d3.8680
   Designated port id is 128.3, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 6066, received 0

 Port 10 (GigabitEthernet1/0/10) of VLAN0010 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.10.
   Designated root has priority 32778, address 00fe.c8d3.8680
   Designated bridge has priority 32778, address 00fe.c8d3.8680
   Designated port id is 128.10, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode by portfast trunk configuration
   Link type is point-to-point by default
   BPDU: sent 6063, received 0

 Port 11 (GigabitEthernet1/0/11) of VLAN0010 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.11.
```

Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.11, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6066, received 0

Port 13 (GigabitEthernet1/0/13) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.13.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.13, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6066, received 3

Port 14 (GigabitEthernet1/0/14) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.14.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.14, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6066, received 3

Port 15 (GigabitEthernet1/0/15) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.15.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.15, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6067, received 0

Port 16 (GigabitEthernet1/0/16) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.16.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.16, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6067, received 0

Port 35 (GigabitEthernet1/0/35) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.35.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.35, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6067, received 0

Esta saída mostra que a última alteração de topologia ocorreu de um dispositivo conectado fora da interface GigabitEthernet1/0/35. Em seguida, execute o mesmo comando show spanning-tree detail neste dispositivo para tentar rastrear o problema. Se esse switch que gera os TCNs estiver conectado apenas ao PC ou a endpoints, certifique-se de que o STP PortFast esteja habilitado nessas portas. O STP PortFast suprime as TCNs do STP quando uma porta faz transição entre os estados.

Consulte esses documentos para obter informações sobre o STP e como solucionar os problemas de transições de link que estão associadas às placas de interface de rede (NICs):

- Utilização de Portfast e outros comandos para reparar retardos de conectividade da inicialização de estação de trabalho
- Entender o Rapid Spanning Tree Protocol (802.1w)
- Problemas de STP e considerações de projeto relacionadas

4. Portas Bloqueadas Desconectadas

Devido à natureza do balanceamento de carga do Fast EtherChannel (FEC) (canal da porta), os problemas de FEC podem contribuir com os problemas do HSRP e do STP. Ao solucionar problemas de STP ou HSRP, você pode remover a configuração de qualquer conexão FEC. Depois que as alterações de configuração estiverem em vigor, emita o comando show spanning-tree blockedports em ambos os switches. Verifique se pelo menos uma das portas começa a bloquear em ambos os lados da conexão.

Consulte estes documentos para obter informações sobre Fast EtherChannel:

- Entender o Balanceamento de Carga e a Redundância do EtherChannel em Switches Catalyst
- Configuração dos EtherChannels

5. Supressão de Broadcast

Ative a supressão de transmissão para ajudar a reduzir o impacto de um congestionamento de transmissões. Um congestionamento de transmissões é um dos principais efeitos de um loop de STP. Este é um exemplo da saída do comando:

```
L2Switch_1#show run interface TenGigabitEthernet1/1/5
Building configuration...

Current configuration : 279 bytes
!
interface TenGigabitEthernet1/1/5
 switchport trunk allowed vlan 300-309
 switchport mode trunk
 storm-control broadcast level 30.00
 storm-control multicast level 30.00
```

```
 storm-control unicast level 30.00
 spanning-tree guard root
end

L2Switch_1#show storm-control broadcast
Key: U - Unicast, B - Broadcast, M - Multicast
Interface  Filter State   Upper      Lower      Current    Action    Type
---------  -------------  ---------- ---------- ---------- --------- ----
Te1/1/5    Forwarding       30.00%     30.00%     0.00%  None      B
Te1/1/7    Link Down        30.00%     30.00%     0.00%  None      B
Te1/1/8    Forwarding       10.00%     10.00%     0.00%  None      B

L2Switch_1#show storm-control multicast
Key: U - Unicast, B - Broadcast, M - Multicast
Interface  Filter State   Upper      Lower      Current    Action    Type
---------  -------------  ---------- ---------- ---------- --------- ----
Te1/1/5    Forwarding       30.00%     30.00%     0.00%  None      M
Te1/1/7    Link Down        30.00%     30.00%     0.00%  None      M
```

6. Console e Acesso Telnet

O tráfego do Console ou do Telnet para o switch geralmente fica lento para rastrear adequadamente um dispositivo incorreto durante um loop de STP. Para forçar a recuperação instantânea da rede, remova todos os links físicos redundantes. Depois que o STP tiver permissão para se reconvergir na nova topologia não redundante, reconecte um link redundante de cada vez. Se o loop de STP retornar após adicionar um segmento específico, você identificou os dispositivos incorretos.

7. Recursos do Spanning Tree: Portfast, UplinkFast e BackboneFast

Verifique se o PortFast, o UplinkFast e o BackboneFast estão configurados corretamente. Ao solucionar os problemas de STP, desative todos os STP avançados (UplinkFast e BackboneFast). Além disso, verifique se o STP PortFast está ativado apenas nas portas conectadas diretamente aos hosts que não são de ponte. Os hosts que não são de ponte incluem os locais de trabalho do usuário e os roteadores sem grupos de ponte. Não ative o PortFast nas portas conectadas a hubs ou outros switches. Aqui estão alguns documentos para ajudar a entender e configurar esses recursos:

Configurar o Spanning Tree PortFast, BPDU Guard, Filtro de BPDU, UplinkFast, BackboneFast e Loop Guard

Entender e configurar o recurso Cisco UplinkFast

8. Proteção de BPDU

Quando você ativa a proteção de BPDU do PortFast, uma porta de não entroncamento habilitada para PortFast muda para um estado errdisable ao receber uma BPDU nessa porta. Este recurso

ajuda a localizar as portas que estão configuradas incorretamente para PortFast. O recurso também detecta onde os dispositivos refletem pacotes ou injetam STP BPDUs na rede. Ao solucionar problemas de STP, você pode habilitar esse recurso para ajudar a isolar o problema de STP.

```
L2Switch_1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
L2Switch_1(config)#spanning-tree portfast bpduguard
L2Switch_1(config)#end
```

9. Poda de VTP

Quando a remoção de VTP está ativada na rede, ela pode fazer com que os dispositivos de um grupo de HSRP fiquem ativos. Isso resulta em conflitos de IP entre os gateways e causa problemas de tráfego. Assegure que a VLAN de qualquer grupo de HSRP não seja removida pelo VTP na rede.

F. Dividir e conquistar

Se todas as outras tentativas de isolar ou resolver o HSRP falharem, o método "dividir e conquistar" será a próxima abordagem. Esse método ajuda a isolar a rede e os componentes. Dividir e conquistar envolve qualquer uma das diretrizes nesta lista:

Observação: esta lista repete algumas diretrizes de outras seções deste documento.

- Crie uma VLAN de teste para HSRP e a VLAN isolada para switch com os roteadores do HSRP.
- Desconecte todas as portas redundantes.
- Divida as portas FEC em portas conectadas simples.
- Reduza os membros do grupo de HSRP para apenas dois.
- Remova as portas de tronco de modo que apenas as VLANs necessárias sejam propagadas por essas portas.
- Desconecte os switches conectados na rede até que não haja problemas.

Problemas conhecidos

Estado de HSRP oscilante/instável ao usar Cisco 2620/2621, Cisco 3600 com Fast Ethernet

Esse problema pode ocorrer com as interfaces Fast Ethernet na interrupção da conectividade de rede ou na adição de um roteador do HSRP com prioridade mais alta para uma rede. Quando o estado do HSRP muda de ativo para fala, o roteador redefine a interface para remover o endereço MAC do HSRP do filtro de endereços MAC das interfaces. Somente o hardware específico usado nas interfaces Fast Ethernet para Cisco 2600s, 3600s e 7500s tem esse problema. A redefinição da interface do roteador causa uma alteração no estado do link nas interfaces Fast Ethernet e o switch detecta a alteração. Se o switch executar o STP, a alteração causará uma transição de STP. O STP leva 30 segundos para fazer a transição da porta para o estado de encaminhamento. Esse tempo é o dobro do tempo de atraso de encaminhamento padrão de 15 segundos. Ao mesmo tempo, o roteador de fala faz transição para o estado `standby após 10 segundos, que é o tempo de espera do HSRP`. O STP ainda não está encaminhando, portanto, nenhuma mensagem Hello do HSRP é enviada pelo roteador ativo. Isso faz com que o roteador standby se torne ativo após cerca de 10 segundos. Agora os dois roteadores estão `ativos`. Quando as portas de STP se tornam encaminhamento, o roteador de prioridade mais baixa muda de ativo para fala e todo o processo é repetido.

Platform	Descrição	ID de bug da Cisco	Reparar	Solução
Cisco 2620/2621	A interface Fast Ethernet começa a oscilar quando o HSRP é configurado e o cabo é desconectado.		Uma atualização de software; consulte o bug para obter detalhes de revisão.	Ativa o Spanning Tree PortFast na porta do switch conectado.
Cisco 2620/2621	O estado do HSRP está oscilando no 2600 com Fast Ethernet.		Software Cisco IOS versão 12.1.3	Ativa o Spanning Tree PortFast na porta do switch conectado.
Cisco 3600 com NM-1FE-TX[1]	O estado do HSRP está oscilando no 2600 e no 3600 com Fast Ethernet.		Software Cisco IOS versão 12.1.3	Ativa o Spanning Tree PortFast na porta do switch conectado.
Cisco 4500 com interface Fast Ethernet	O estado do HSRP está oscilando no 4500 com Fast Ethernet.	ID de bug da Cisco CSCds16055	Software Cisco IOS versão 12.1.5	Ativa o Spanning Tree PortFast na porta do switch conectado.

1NM-1FE-TX = módulo de rede Fast Ethernet (interface 10/100BASE-TX) de uma porta.

Uma solução alternativa é ajustar os temporizadores do HSRP para que o atraso de encaminhamento do STP seja menor que metade do tempo de espera do HSRP padrão. O atraso de encaminhamento do STP padrão é de 15 segundos e o tempo de espera do HSRP padrão é de 10 segundos.

Quando você usa o comando track no processo de HSRP, a Cisco recomenda que o uso de determinado valor de decréscimo para evitar a oscilação do HSRP.

Este é um exemplo de configuração em um roteador ativo do HSRP ao usar o comando track:

```
standby 1 ip 10.0.0.1
standby 1 priority 105
standby 1 preempt delay minimum 60
standby 1 name TEST
standby 1 track <object> decrement 15
```

Onde 15 é o valor de decremento quando o objeto oscila. Para saber mais sobre o comando track, navegue para o documento Opção Track no Exemplo de Configuração do HSRPv2.

Informações Relacionadas

- Switches Catalyst para LAN de campus - Acesso
- LAN Switching
- Suporte Técnico e Documentação - Cisco Systems

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.