Ferramentas de Troubleshooting de Multicast Básico

Índice

Introdução

Este documento explica diferentes ferramentas e técnicas para solucionar problemas de redes

multicast. Se você compreende as várias ferramentas da interface de linha de comando e os campos de informações-chave em suas saídas, isso o ajudará a solucionar problemas de redes multicast.

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Estratégias de Troubleshooting

Quando você soluciona problemas de redes multicast, é bom considerar o protocolo de sinalização utilizado na rede e no fluxo de pacotes. O protocolo de sinalização é utilizado para configurar e destruir sessões multicast (como o modo denso de PIM, o modo escasso de PIM, e o DVMRP), e o fluxo de pacotes corresponde ao envio real, duplicando e recebendo de pacotes multicast entre a fonte e o receptor, com base na tabela de encaminhamentos criada pelo processo de sinalização.

Esta tabela ajuda a verificar cada parte das informações de troubleshooting ao verificar que cada seção da tabela está funcionando corretamente:

	Fonte	Rede	Receptores
Sinalização	NA	Verifique a sinalização da rede	Verificar a sinalização do receptor
Fluxo de pacote	Verificação do Fluxo de Pacotes de Origem	Verificar fluxo de pacote de rede	Verificar fluxo de pacote do receptor

As subseções a seguir detalham as ferramentas de troubleshooting que você pode utilizar para verificar e corrigir problemas comuns.

Verificação do Fluxo de Pacotes de Origem

Conclua estes passos para determinar se a origem está realmente fornecendo os pacotes e os inserindo nos campos de pacote corretos:

1. Verifique os contadores de interface no host. Primeiro, verifique os contadores de interface (se você está em um sistema Unix, use o **comando netstat**) no host de origem para verificar se ele está enviando pacotes. Se não estiver, verifique se há erros de configuração ou bugs no aplicativo e na pilha do host.
2. Use o ***comando show ip igmp groups nome-interface*** para verificar se o roteador upstream recebeu um relatório de ingressos na interface diretamente conectada à origem.
3. Verifique o valor TTL nos pacotes de origem de aplicativo; ele deve ser maior que 1. Se o aplicativo enviar pacotes com um valor TTL menor que 1, você deverá verificar o tráfego descartado no primeiro roteador upstream. Para verificar, use o **comando show ip traffic** e procure um aumento no valor do contador "contagem de saltos incorretos". Qualquer pacote com um valor TTL igual a 1, ou menor que o limite de TTL definido pela interface com o **comando ip multicast ttl-threshold**, é descartado e o contador "contagem de saltos incorretos" é incrementado em um. Use o ***comando show ip igmp interface interface-name*** para ver o valor do limite de TTL da interface.
4. Use os comandos show ip mroute count e show ip mroute active para verificar o primeiro roteador upstream ou switch de forma a verificar se ele vê pacotes multicast da origem. A saída do comando mostra as estatísticas do fluxo de tráfego para cada par (S, G). Se você não observar tráfego, verifique a sinalização do receptor.
5. Use o comando debug ip mpacket no roteador upstream mais próximo com o argumento ***detail*** ou ***acl*** para granularidade. Use este comando com cuidado quando houver um tráfego multicast pesado na rede. Somente se for necessário, use o comando debug ip mpacket na rota. Use o argumento ***detail*** para mostrar cabeçalhos de pacote na **saída da depuração** e em listas de acessos para procurar tráfego de fontes específicas. Lembre-se que este comando pode causar um sério impacto no desempenho de outro tráfego. Portanto, use-o com cuidado.

Verifique a sinalização da rede

Esta é a parte mais complexa e importante do troubleshooting em qualquer rede. Depende do protocolo de sinalização da rede utilizado, como o modo escasso de PIM, o modo denso de PIM, e o DVMRP. Nós recomendamos a abordagem multipassos descrita nesta seção.

Troubleshooting com o PIM Sparse Mode

Conclua estes passos para solucionar problemas do modo escasso de PIM:

1. Verifique se o roteamento IP multicast está habilitado em todos os roteadores multicast.
2. Use o comando show ip pim neighbor para verificar o modo e o temporizador de expiração de forma a garantir o estabelecimento bem-sucedido de vizinhos PIM e procurar quaisquer possíveis problemas de conectividade e temporizador que possam inibir o estabelecimento de vizinhos PIM. Se necessário, use o subcomando **ip pim [versão] [modo denso] [modo escasso] [modo denso escasso] nível da interface** para definir o modo e a versão corretos para um estabelecimento bem-sucedido de vizinhos PIM.

3. Use o comando show ip pim rp mapping para garantir o mapeamento correto de grupo RP e verificar o temporizador de expiração se o RP automático estiver configurado. Use o **comando debug ip pim auto-rp** para ajudar a desvendar quaisquer falhas do RP automático. Se nenhum dos mapeamentos PIM Grupo para RP for exibido, verifique a configuração de RP automático ou configure mapeamentos Grupo-RP estáticos com o **comando ip pim rp-address ip address of RP [access-list] [named-accesslist] [override] command**. A configuração do RP automático pode ser feita com os comandos **ip pim send-rp-announce** *interface-id* **scope** *TTL value* e **ip pim send-rp-discovery** *interface-id* **scope** *TTL value*. Esses comandos deverão ser configurados somente se houver configurações de RP automático.
4. Use o *comando show ip rpf ip address of source* para verificar a falha de RPF para o endereço de origem. O modo denso de PIM e o modo escasso de PIM enviarão mensagens de remoção de volta à origem se o tráfego chegar em uma interface ponto a ponto não RPF. As ajudas do comando debug ip pim identificam razões possíveis para uma falha em uma rede PIM — compara as saídas típicas com o que você vê. Use esta saída para identificar as três fases discretas no modo escasso de PIM: ingressar, registrar e switchover de SPT. O comando show ip mroute permite que você monitore entradas nulas nas listas da Interface de Saída e entradas removidas na tabela mroute.

Verificar fluxo de pacote de rede

Use estes comandos para verificar o fluxo dos pacotes multicast através da rede:

- multicast trace salto a salto usando o comando mtrace
- mstat
- ping
- show ip mroute count
- show ip mroute active
- debug ip mpacket

Verificar a sinalização do receptor

Conclua estes passos para verificar a sinalização do receptor:

1. Use o comando show ip igmp groups no primeiro roteador upstream conectado ao receptor para verificar se a interface ingressou no grupo.
2. Use o comando ping para verificar a acessibilidade do host e o primeiro roteador upstream.
3. Use o comando show ip igmp interface para verificar a versão IGMP da interface.**Nota:** Lembre-se que um roteador configurado com IGMP versão 1 considera pacotes IGMP version 2 recebidos do host como inválidos. Estes pacotes IGMP não ingressarão no grupo até que o roteador receba um pacote IGMP versão 1 do host.
4. Use o comando debug ip igmp para fazer o troubleshooting adicional da sinalização do receptor.

Verificar fluxo de pacote do receptor

Conclua estes passos para verificar o fluxo de pacotes do receptor:

1. Use o **comando netstat em um** sistema Unix para verificar as estatísticas da interface do

receptor.
2. Verifique se a pilha TCP/IP foi instalada e configurada adequadamente.
3. Verifique se o aplicativo cliente do receptor Multicast foi instalado e configurado apropriadamente.
4. Verifique pacotes multicast duplicados em um segmento de vários acessos.

Ferramentas para alimentação

Os comandos nesta seção também podem ser úteis ao solucionar problemas, especialmente quando você testa o fluxo de pacotes da rede e encontra os pontos de falha na rede multicast. Para obter informações mais abrangentes sobre comandos de ferramentas de multicast, consulte Comandos de Ferramentas de Multicast IP.

mstat

Este comando mostra o caminho multicast no formato gráfico ASCII. Ele rastreia o caminho entre dois pontos na rede, mostra descartes e duplicatas, TTLs e atrasos em cada nó na rede. É muito útil quando você precisa localizar pontos de congestão na rede, ou o foco em um roteador com altos índices de descartes/duplicatas. As duplicatas são indicadas na saída como descartes "negativos".

```
Router# mstat lwei-home-ss2 171.69.58.88 224.0.255.255 Type escape sequence to abort Mtrace from
171.69.143.27 to 171.69.58.88 via group 224.0.255.255 >From source (lwei-home-ss2.cisco.com) to
destination (lwei-ss20.cisco.com) Waiting to accumulate statistics...... Results after 10
seconds: Source Response Dest Packet Statistics For Only For Traffic 171.69.143.27 171.69.62.144
All Multicast Traffic From 171.69.143.27 | __/ rtt 48 ms Lost/Sent = Pct Rate To 224.0.255.255 v
/ hop 48 ms ---------- ---------- 171.69.143.25 lwei-cisco-isdn.cisco.com |
^ ttl 1 v | hop 31 ms 0/12 = 0% 1 pps 0/1 = --% 0 pps 171.69.121.84 171.69.121.45 eng-frmt12-
pri.cisco.com | ^ ttl 2 v | hop -17 ms -735/12 = --% 1 pps 0/1 = --% 0 pps 171.69.121.4
171.69.5.27 eng-cc-4.cisco.com | ^ ttl 3 v | hop -21 ms -678/23 = --% 2 pps 0/1 = --% 0 pps
171.69.5.21 171.69.62.130 eng-ios-2.cisco.com | ^ ttl 4 v | hop 5 ms 605/639 = 95% 63 pps 1/1 =
--% 0 pps 171.69.62.144 171.69.58.65 eng-ios-f-5.cisco.com | \__ ttl 5 v \ hop 0 ms 4 0 pps 0 0
pps 171.69.58.88 171.69.62.144 Receiver Query Source
```

mrinfo

Este comando mostra as informações do roteador de vizinhos multicast, os recursos do roteador e a versão de código, as informações da interface multicast, os limites de TTL, as métricas, o protocolo, e o status. É útil quando você precisa verificar vizinhos multicast, confirmar que há uma adjacência de vizinhos bidirecional, e verificar que os túneis estão ativos em ambas as direções.

```
Router# mrinfo 192.1.7.37 (b.cisco.com) [version cisco 11.1] [flags: PMSA]: 192.1.7.37 ->
192.1.7.34 (s.cisco.com) [1/0/pim] 192.1.7.37 -> 192.1.7.47 (d.cisco.com) [1/0/pim] 192.1.7.37 -
> 192.1.7.44 (d2.cisco.com) [1/0/pim] 131.9.26.10 -> 131.9.26.9 (su.bbnplanet.net) [1/32/pim]
```

Os sinalizadores na saída indicam:

- P = capaz de remoção
- M = habilitado para mtrace
- S = capacidade de SNMP
- A = Capaz de RP automático

mtrace

Este comando mostra o caminho multicast da origem ao receptor, e rastreia o caminho entre pontos nas redes, que mostra limites de TTL e atraso em cada nó. Ao fazer o troubleshooting, use o **comando mtrace** para localizar onde o fluxo do tráfego multicast é interrompido, verificar o caminho do tráfego multicast e identificar caminhos não necessariamente ideais.

```
Router# mtrace 171.69.215.41 171.69.215.67 239.254.254.254 Type escape sequence to abort. Mtrace
from 171.69.215.41 to 171.69.215.67 via group 239.254.254.254 From source (?) to destination (?)
Querying full reverse path... 0 171.69.215.67 -1 171.69.215.67 PIM thresh^ 0 0 ms -2
171.69.215.74 PIM thresh^ 0 2 ms -3 171.69.215.57 PIM thresh^ 0 894 ms -4 171.69.215.41 PIM
thresh^ 0 893 ms -5 171.69.215.12 PIM thresh^ 0 894 ms -6 171.69.215.98 PIM thresh^ 0 893 ms
```

ping

Durante o troubleshooting, o **comando ping** é a maneira mais fácil de gerar tráfego multicast no laboratório para testar a árvore multicast porque ele consulta todos os membros do grupo e todos os membros respondem.

```
R3# ping 239.255.0.1 Type escape sequence to abort. Sending 1, 100-byte ICMP Echos to
239.255.0.1, timeout is 2 seconds: Reply to request 0 from 172.16.12.2, 16 ms Reply to request 0
from 172.16.7.2, 20 ms
```

comandos show

Os comandos nesta seção o ajudam a obter informações úteis ao solucionar um problema de multicast. Consulte o Guia de Referência de Comandos de Multicast IP para obter informações mais detalhadas sobre estes **comandos show**.

Dica: Se suas respostas do **comando show** forem lentas, o motivo mais provável é que o roteador executa atualmente uma consulta de domínio IP para endereços IP no **comando show**. Você pode desabilitar a consulta de domínios IP. Você pode utilizar o **comando no ip domain-lookup**, no modo de configuração global do roteador, para desabilitar a consulta de domínios IP. Isso interrompe a consulta de domínio e aumenta a velocidade da **saída do comando show**.

show ip igmp groups

Este comando mostra quais grupos multicast estão conectados diretamente ao roteador, e quais são aprendidos através do Internet Group Management Protocol (IGMP). Você pode utilizar este comando para verificar se uma origem ou um receptor ingressaram no grupo de destino na interface do roteador. A coluna "Último Repórter" mostra somente um host IGMP, que indica que ele enviou um pedido de Ingresso IGMP não solicitado ou Relatório IGMP em resposta a uma Consulta IGMP do roteador PIM para este grupo específico. Somente um "Último Repórter" pode ser exibido por Endereço de Grupo.

```
R1# show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires
Last Reporter 239.255.0.1 Ethernet1 00:10:54 00:01:10 192.168.9.1 224.0.1.40 Ethernet0 01:36:27
00:02:45 192.168.10.2 224.0.1.40 Ethernet1 01:48:15 never 192.168.9.3
```

show ip igmp interface

Use este comando para exibir informações relacionadas a multicast sobre uma interface, e para verificar se o IGMP está habilitado, se a versão correta está em execução e se as opções de temporizadores, Time To Live (TTL) valor de limite e roteador gerador de consultas IGMP estão definidas corretamente. O IGMP não precisa de ser configurado em uma interface. Ele é habilitado por padrão quando você configura o ***modo denso do*** **pim IP|***modo escasso*|***modo denso escasso***.

```
R1# show ip igmp interface Ethernet1 is up, line protocol is up Internet address is
192.168.9.3/24 IGMP is enabled on interface Current IGMP version is 2 CGMP is disabled on
interface IGMP query interval is 60 seconds IGMP querier timeout is 120 seconds IGMP max query
response time is 10 seconds Last member query response interval is 1000 ms Inbound IGMP access
group is not set IGMP activity: 22 joins, 18 leaves Multicast routing is enabled on interface
Multicast TTL threshold is 0 Multicast designated router (DR) is 192.168.9.5 IGMP querying
router is 192.168.9.3 (this system) Multicast groups joined (number of users): 224.0.1.40(1)
```

show ip pim neighbor

Use este comando para listar os vizinhos de Multicast Independente de Protocolo (PIM) descobertos pelo software Cisco IOS®.

```
R1# show ip pim neighbor PIM Neighbor Table Neighbor Interface Uptime/Expires Ver DR Address
Prio/Mode 10.10.10.1 Ethernet0/0 02:19:41/00:01:38 v2 1 / DR B S
```

Os detalhes de cada campo são explicados aqui:

- **Neighbor Address** - Especifica o endereço IP de um vizinho PIM
- **Interface** - Uma interface onde um vizinho PIM foi descoberto
- **Uptime** - O tempo total de atividade do vizinho
- **Expires** - O tempo antes de um vizinho expirar e até que a próxima saudação PIM seja recebida
- **Ver** - A versão do PIM na interface do vizinho
- **DR Prio** - Os valores possíveis são 0 a 4294967294 ou "N"Esta é uma coluna nova que controla a prioridade de uma interface PIM para a eleição do DR. O recurso para configurar um DR baseado na prioridade mais alta versus o maior endereço IP foi introduzido nos Cisco IOS Software Releases 12.1(2)T e 12.2 e nas imagens do Cisco IOS com Bidir-PIM. Você pode utilizar o comando de interface **ip pim dr-priority <0-4294967294>** para definir a prioridade do DR. A prioridade padrão do DR é 1. Para interoperabilidade, se um vizinho PIM estiver executando uma versão do Cisco IOS que não ofereça suporte ao recurso de prioridade do DR, a coluna "DR Prior" exibirá "N". Se o vizinho for o único roteador que exibir "N" para a interface, ele se tornará DR independentemente de qual roteador possuir o maior endereço IP. Se houver vários vizinhos PIM com "N" listado sob esta coluna, o disjuntor da conexão será o maior endereço IP entre eles.
- **Mode - Informações** sobre o DR e outros recursos PIM.Esta coluna lista o DR além dos recursos com suporte pelo vizinho PIM:**DR** - O vizinho de PIM é roteador designado**B** - Habilitado para PIM bidirecional (Bidir-PIM)**S** - Habilitado para atualização de estado (aplica-se somente ao modo denso)

Ao solucionar problemas, use este comando para verificar se todos os vizinhos estão ativos e se estão usando o modo, a versão, e o temporizador de expiração corretos. Você também pode verificar a configuração do roteador, ou utilizar o comando show ip pim interface para verificar o modo (PIM escasso ou modo denso). Use o comando debug ip pim para observar a troca de mensagens de consulta do PIM.

show ip pim interface

Use este comando para exibir informações sobre as interfaces configuradas para o PIM. Além disso, você pode utilizar este comando para verificar se o modo PIM correto (denso ou escasso) está configurado na interface, a contagem de vizinhos está correta e o Roteador Designado (DR) está correto (crítico para o modo escasso de PIM). Os segmentos de multiacesso (tais como Ethernet, Token Ring, FDDI) elegem um DR baseado no maior endereço IP. Os links Point-to-Point não exibem informações do DR.

```
R1# show ip pim interface Address Interface Version/Mode Nbr Query DR Count Intvl 192.168.10.1
Ethernet0 v2/Sparse-Dense 1 30 192.168.10.2 192.168.9.3 Ethernet1 v2/Sparse-Dense 1 30
192.168.9.5
```

show ip mroute summary

Use este comando para exibir o conteúdo resumido da tabela de roteamento IP Multicast. Você também pode usá-la para verificar o grupo multicast ativo e quais remetentes multicast estão ativos olhando os temporizadores e os sinalizadores.

```
R1## show ip mroute summary IP Multicast Routing Table Flags: D - Dense, S - Sparse, C -
Connected, L - Local, P - Pruned R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join
SPT M - MSDP created entry, X - Proxy Join Timer Running A - Advertised via MSDP Outgoing
interface flags: H - Hardware switched Timers: Uptime/Expires Interface state: Interface, Next-
Hop or VCD, State/Mode (*, 239.255.0.1), 01:57:07/00:02:59, RP 192.168.7.2, flags: SJCF
(133.33.33.32, 239.255.0.1), 01:56:23/00:02:59, flags: CJT (192.168.9.1, 239.255.0.1),
01:57:07/00:03:27, flags: CFT (*, 224.0.1.40), 1d00h/00:00:00, RP 192.168.7.2, flags: SJPCL
```

show ip mroute

Use este comando para exibir o conteúdo completo da tabela de roteamento IP Multicast. Ao solucionar problemas, use este comando para verificar:

- As entradas de estado (S,G) e (*,G) dos indicadores.
- A interface de entrada está correta. Se não estiver, verifique a tabela de roteamento unicast.
- A interface de saída está correta. Se ela for removida incorretamente, verifique o estado no roteador downstream.

```
R1# show ip mroute IP Multicast Routing Table Flags: D - Dense, S - Sparse, C - Connected, L -
Local, P - Pruned R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT M - MSDP
created entry, X - Proxy Join Timer Running A - Advertised via MSDP Outgoing interface flags: H
- Hardware switched Timers: Uptime/Expires Interface state: Interface, Next-Hop or VCD,
State/Mode (*, 239.255.0.1), 01:55:27/00:02:59, RP 192.168.7.2, flags: SJCF Incoming interface:
Ethernet0, RPF nbr 192.168.10.2 Outgoing interface list: Ethernet1, Forward/Sparse,
01:55:27/00:02:52 (133.33.33.32, 239.255.0.1), 01:54:43/00:02:59, flags: CJT Incoming interface:
Ethernet0, RPF nbr 192.168.10.2 Outgoing interface list: Ethernet1, Forward/Sparse,
01:54:43/00:02:52 (192.168.9.1, 239.255.0.1), 01:55:30/00:03:26, flags: CFT Incoming interface:
Ethernet1, RPF nbr 0.0.0.0 Outgoing interface list: Ethernet0, Forward/Sparse, 01:55:30/00:03:12
(*, 224.0.1.40), 1d00h/00:00:00, RP 192.168.7.2, flags: SJPCL Incoming interface: Ethernet0, RPF
nbr 192.168.10.2 Outgoing interface list: Null
```

show ip mroute active

Use este comando para exibir as origens do tráfego ativo e os grupos acima do limite. Ao solucionar problemas, use-o para verificar os grupos de origem ativos, a taxa do tráfego para cada par de grupo de origem (S,G) pair (você deverá ter alternado para Shortest Path Tree (SPT)), e para verificar se o tráfego multicast do grupo de destino está sendo recebido. Se o tráfego não estiver sendo recebido, procure o tráfego ativo que parte da fonte para o receptor.

```
R1# show ip mroute active Active IP Multicast Sources - sending >= 4 kbps Group: 239.255.0.1,
(?) Source: 133.33.33.32 (?) Rate: 10 pps/115 kbps(1sec), 235 kbps(last 23 secs), 87 kbps(life
avg)
```

show ip rpf

Use este comando para exibir como o roteamento IP Multicast executa o Encaminhamento de Caminho Reverso (RPF). Ao solucionar problemas, use-o para verificar se as informações de RPF estão corretas. Se não estiverem, verifique a tabela de roteamento unicast para identificar o

endereço de origem. Use também os comandos **ping** e **trace** no endereço de origem para verificar se o roteamento unicast funciona. Talvez você precise utilizar rotas ou mroutes estáticas Distance Vector Multicast Routing Protocol (DVMRP) para corrigir inconsistências unicast-multicast.

```
R1# show ip rpf 133.33.33.32 RPF information for ? (133.33.33.32) RPF interface: Ethernet0 RPF
neighbor: ? (192.168.10.2) RPF route/mask: 133.33.0.0/16 RPF type: unicast (eigrp 1) RPF
recursion count: 0 Doing distance-preferred lookups across tables
```

show ip mcache

Este comando pode verificar o cache de switching IP Multicast rapidamente e depurar bugs de switching rápido.

```
R1# show ip mcache IP Multicast Fast-Switching Cache (133.33.33.32/32, 239.255.0.1), Ethernet0,
Last used: 00:00:00 Ethernet1 MAC Header: 01005E7F000100000C13DBA90800 (192.168.9.1/32,
239.255.0.1), Ethernet1, Last used: 00:00:00 Ethernet0 MAC Header: 01005E7F000100000C13DBA80800
```

show ip mroute count

Use este comando para verificar se o tráfego multicast é recebido e verificar suas taxas de fluxo e descartes. Se nenhum tráfego for recebido, trabalhe da origem para o receptor até encontrar a interrupção do tráfego. Você também pode utilizar este comando para verificar se o tráfego está sendo encaminhado. Se não estiver, use o comando show ip mroute para procurar a "lista de interfaces de saída nula" e falhas de RPF.

```
R1# show ip mroute count IP Multicast Statistics routes using 2406 bytes of memory 2 groups,
1.00 average sources per group Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt
Size/Kilobits per second Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 239.255.0.1, Source count: 2, Group pkt count: 11709 RP-tree: Forwarding: 3/0/431/0,
Other: 3/0/0 Source: 133.33.33.32/32, Forwarding: 11225/6/1401/62, Other: 11225/0/0 Source:
192.168.9.1/32, Forwarding: 481/0/85/0, Other: 490/0/9 Group: 224.0.1.40, Source count: 0, Group
pkt count:
```

show ip route

Use este comando para verificar a tabela de roteamento unicast e corrigir as falhas de RPF na tabela mroute.

```
R2# show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set D 192.168.9.0/24 [90/307200] via 192.168.10.1, 00:59:45, Ethernet0 C 192.168.10.0/24 is
directly connected, Ethernet0 D 192.168.4.0/24 [90/11040000] via 192.168.7.1, 23:21:00, Serial0
D 192.168.5.0/24 [90/11023872] via 192.168.7.1, 23:21:02, Serial0 C 192.168.7.0/24 is directly
connected, Serial0 D 133.33.0.0/16 [90/2195456] via 192.168.7.1, 1d23h, Serial0 D 192.168.1.0/24
[90/11552000] via 192.168.7.1, 22:41:27, Serial0
```

show ip pim rp mapping

Use este comando para verificar a atribuição de RP pelo intervalo de grupos multicast e se a origem do aprendizado RP (estático ou RP automático) e o mapeamento estão corretos. Se você encontrar um erro, verifique a configuração de roteador local ou a configuração de RP automático.

```
R1# show ip pim rp mapping PIM Group-to-RP Mappings Group(s) 224.0.1.40/32 RP 192.168.7.2 (?),
v1 Info source: local, via Auto-RP Uptime: 2d00h, expires: never Group(s): 224.0.0.0/4, Static
RP: 192.168.7.2 (?)
```

Comandos debug

Esta seção foi criada para mostrar como determinadas **saídas do comando debug** devem ser em uma rede em funcionamento. Fazer o troubleshooting, você pode distinguir entre uma **saída de depuração** "correta" e uma que aponta para um problema em sua rede. Para obter mais informações sobre estes **comandos debug**, consulte a Referência de Comandos Debug do Cisco IOS.

debug ip igmp

Use o **comando debug ip igmp** para exibir os pacotes IGMP recebidos e transmitidos, bem como eventos relacionados do host IGMP. A forma **no** deste comando desabilita a saída de depuração.

Esta saída o ajuda a descobrir se o IGMP processa a função. Geralmente, se o IGMP não funcionar, o processo do roteador nunca descobrirá outro host na rede configurado para receber pacotes multicast. No modo denso de PIM, isso significa que os pacotes são entregues intermitentemente (alguns a cada três minutos). No modo escasso de PIM, eles nunca são entregues.

```
R1# debug ip igmp 12:32:51.065: IGMP: Send v2 Query on Ethernet1 to 224.0.0.1 12:32:51.069:
IGMP: Set report delay time to 9.4 seconds for 224.0.1.40 on Ethernet1 12:32:56.909: IGMP:
Received v1 Report from 192.168.9.1 (Ethernet1) for 239.255.0.1 12:32:56.917: IGMP: Starting old
host present timer for 239.255.0.1 on Ethernet1 12:33:01.065: IGMP: Send v2 Report for
224.0.1.40 on Ethernet1 12:33:01.069: IGMP: Received v2 Report from 192.168.9.4 (Ethernet1) for
224.0.1.40 12:33:51.065: IGMP: Send v2 Query on Ethernet1 to 224.0.0.1
```

A saída acima mostra que o roteador envia uma consulta IGMP versão 2 através da Ethernet 1 da interface no endereço multicast 224.0.0.1 (todos os sistemas multicast nesta sub-rede). A Ethernet 1 da Interface em si é um membro do grupo 224.0.1.40 (você pode utilizar o comando show ip igmp interface para determinar isso), que define um tempo de retardo de 9,4 segundos (determinados aleatoriamente). Como ela não receberá nenhum relatório de outro sistema para o grupo multicast 224.0.1.40 pelos próximos 9,4 segundos, ela enviará um relatório versão 2 de sua associação que será recebido pelo roteador em si na Ethernet 1. Ela também receberá um relatório IGMP versão 1 do host 192.168.9.1, que está conectado diretamente à Ethernet 1 da interface para o grupo 239.255.0.1.

Esta **saída de depuração** é útil quando você verifica que a interface do roteador envia consultas e para determinar o intervalo das consultas (no caso acima, em 60 segundos). Você também pode utilizar o comando para determinar a versão do IGMP utilizada pelos clientes.

debug ip mpacket

Use o **comando debug ip mpacket** para exibir todos os pacotes recebidos e transmitidos via IP Multicast. A forma **no** deste comando desabilita a saída de depuração.

```
R1# debug ip mpacket 239.255.0.1 detail 13:09:55.973: IP: MAC sa=0000.0c70.d41e (Ethernet0), IP
last-hop=192.168.10.2 13:09:55.977: IP: IP tos=0x0, len=892, id=0xD3C1, ttl=12, prot=17
13:09:55.981: IP: s=133.33.33.32 (Ethernet0) d=239.255.0.1 (Ethernet1) len 906, mforward
```

Este comando decodifica o pacote multicast e mostra se ele é encaminhado (mforward) ou descartado. Ele é útil quando você depura problemas do fluxo de pacotes na rede para verificar o valor de TTL e o motivo de um pacote ser descartado.

Cuidado: Tenha cuidado ao ativar a saída de depuração no nível de pacotes, especialmente

quando o roteador estiver atendendo a altas cargas de pacotes multicast.

debug ip mrouting

Este comando é útil para fins de manutenção da tabela de roteamento. Use-o para verificar se (S, G) mroute está instalado na tabela mrouting, e se não estiver, o motivo. As principais informações nesta saída são a interface RPF. Se houver uma falha da verificação RPF, (S, G) mroute não será instalado na tabela mrouting.

```
R1# debug ip mrouting 239.255.0.1 13:17:27.821: MRT: Create (*, 239.255.0.1), RPF Null, PC
0x34F16CE 13:17:27.825: MRT: Create (133.33.33.32/32, 239.255.0.1), RPF Ethernet0/192.168.10.2,
PC 0x34F181A 13:17:30.481: MRT: Create (192.168.9.1/32, 239.255.0.1), RPF Ethernet1/0.0.0.0, PC
0x34F18
```

debug ip pim

Use o **comando debug ip pim** para exibir os pacotes PIM recebidos e transmitidos, bem como eventos relacionados ao PIM. A forma **no** deste comando desabilita a saída de depuração.

Esta seção usa um exemplo para ajudá-lo a compreender a saída de depuração do modo escasso de PIM, e mostra uma saída de depuração típica.

Esta é a saída de **debug ip pim** em R1:

```
R1# debug ip pim PIM: Send v2 Hello on Ethernet0 PIM: Send v2 Hello on Ethernet1 PIM: Received
v2 Hello on Ethernet0 from 192.168.10.2 PIM: Send v2 Hello on Ethernet0 PIM: Send v2 Hello on
Ethernet1 PIM: Building Join/Prune message for 239.255.0.1 PIM: v2, for RP, Join-list:
192.168.7.2/32, RP-bit, WC-bit, S-bit PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2
(Ethernet0) PIM: Received RP-Reachable on Ethernet0 from 192.168.7.2 for group 239.255.0.1 PIM:
Update RP expiration timer (270 sec) for 239.255.0.1
```

Aqui está o que cada linha representa: R1 e R2 estabelecem vizinhos PIM trocando mensagens de saudação. Estas mensagens de saudação periódicas, trocadas durante os segundos do "Intervalo de Consulta" entre R1 (E0) e R2 (E0), acompanham os vizinhos PIM.

R1 envia uma mensagem Join/Prune ao endereço 192.168.7.2 RP. RP (R2) responde com uma mensagem RP acessível retornada a R1 para o grupo 239.255.0.1. Isso ativa atualizações no temporizador de expiração RP em R1. O temporizador de expiração define um ponto de verificação para certificar-se de que o RP ainda existe; caso contrário, um novo RP deverá ser descoberto. Use o **comando show ip pim rp** para observar o tempo de expiração de RP.

Agora, observe a **saída de depuração** entre R1 e R2 quando um receptor multicast para o grupo 239.255.0.1 ingressa em R1.

Primeiro, veja a saída em R1:

```
1 PIM: Check RP 192.168.7.2 into the (*, 239.255.0.1) entry 2 PIM: Send v2 Join on Ethernet0 to
192.168.10.2 for (192.16.8.7.2/32, 239.255.0.1), WC-bit, RPT-bit, S-bit 3 PIM: Building batch
join message for 239.255.0.1 4 PIM: Building Join/Prune message for 239.255.0.1 5 PIM: v2, for
RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit, S-bit 6 PIM: Send v2 periodic Join/Prune to RP
via 192.168.10.2 (Ethernet0) 7 PIM: Received RP-Reachable on Ethernet0 from 192.168.7.2 : for
group 239.255.0.1 8 PIM: Update RP expiration timer (270 sec) for 239.255.0.1 9 PIM: Building
Join/Prune message for 239.255.0.1 10 PIM: v2, for RP, Join-list: 192.168.7.2/32, RP-bit, WC-
bit, S-bit 11 PIM: Send v2 periodic Join/Prune to RP via 192.168.10.2 (Ethernet0)
```

Agora, olhe a saída em R2:

```
12 PIM: Received v2 Join/Prune on Ethernet0 from 192.168.10.1, to us 13 PIM: Join-list: (*,
239.255.0.1) RP 192.168.7.2 14 PIM: Check RP 192.168.7.2 into the (*, 239.255.0.1) entry, RPT-
bit set, WC-bit set, S-bit set 15 PIM: Add Ethernet0/192.168.10.1 to (*, 239.255.0.1), Forward
state 16 PIM: Building Join/Prune message for 239.255.0.1 17 PIM: Received v2 Join/Prune on
Ethernet0 from 192.168.10.1, to us 18 PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2, RPT-bit
set, WC-bit set, S-bit set 19 PIM: Add Ethernet0/192.168.10.1 to (*, 239.255.0.1), Forward state
20 PIM: Building Join/Prune message for 239.255.0.1 21 PIM: Send RP-reachability for 239.255.0.1
on Ethernet0 22 PIM: Received v2 Join/Prune on Ethernet0 from 192.168.10.1, to us 23 PIM: Join-
list: (*, 239.255.0.1) RP 192.168.7.2, RPT-bit set, WC-bit set, S-bit set 24 PIM: Add
Ethernet0/192.168.10.1 to (*, 239.255.0.1), Forward state 25 PIM: Building Join/Prune message
for 239.255.0.1
```

Na linha 1 acima, o receptor multicast para o grupo 239.255.0.1 ingressa em R1. Isto instala uma entrada (*, 239.255.0.1) na tabela mroute. Em seguida, na linha 2, o receptor multicast envia um Join IGMP para R2 (RP) para ingressar na árvore compartilhada.

Quando o join IGMP chega em R2, R2 instala um mroute a (*, 239.255.0.1), como mostrado nas linhas 12 a 15 da saída R2.

Como R2 instala (*, 239.255.0.1) em sua tabela mrouting, ele adiciona a interface da qual recebeu a mensagem Join/Prune à sua lista de interfaces de saída no estado de encaminhamento. Em seguida, ele devolve uma mensagem de acessibilidade RP para a interface na qual ele recebeu a mensagem Join/Prune. Esta transação é mostrada nas linhas 15 a 21 da saída de R2.

R1 recebe a mensagem de acessibilidade de RP para o grupo 239.255.0.1 e atualiza seu temporizador de expiração para RP. Esta troca é repetida uma vez por minuto por padrão e atualiza seu estado de encaminhamento multicast como mostrado nas linhas 7 e 8 da saída de R1.

Nas próximas linhas, a **saída de depuração** entre R2 (RP) e R3 são exibidas. A origem (conectada diretamente a R3) começou a enviar pacotes para o grupo 239.255.0.1.

Primeiro, olhe a saída em R3:

```
1 PIM: Check RP 192.168.7.2 into the (*, 239.255.0.1) entry 2 PIM: Building Join/Prune message
for 239.255.0.1 3 PIM: For RP, Join-list: 192.168.7.2/32, RP-bit, WC-bit 4 PIM: Send periodic
Join/Prune to RP via 192.168.7.2 (Serial4/0) 5 PIM: Received RP-Reachable on Serial4/0 from
192.168.7.2 6 PIM: Update RP expiration timer (270 sec) for 239.255.0.1 7 PIM: Send Register to
192.168.7.2 for 133.33.33.32, group 239.255.0.1 8 PIM: Send Register to 192.168.7.2 for
133.33.33.32, group 239.255.0.1 9 PIM: Received Join/Prune on Serial4/0 from 192.168.7.2 10 PIM:
Join-list: (133.33.33.32/32, 239.255.0.1), S-bit set 11 PIM: Add Serial4/0/192.168.7.2 to
(133.33.33.32/32, 239.255.0.1), Forward state 12 PIM: Received Register-Stop on Serial4/0 from
192.168.7.2 13 PIM: Clear register flag to 192.168.7.2 for (133.33.33.32/32, 239.255.0.1) 14
PIM: Received Register-Stop on Serial4/0 from 192.168.7.2 15 PIM: Clear register flag to
192.168.7.2 for (133.33.33.32/32, 239.255.0.1)
```

Esta é a saída de R2, o RP:

```
16 PIM: Received Join/Prune on Serial0 from 192.168.7.1, to us 17 PIM: Send RP-reachability for
239.255.0.1 on Serial0 18 PIM: Received Register on Serial0 from 192.168.7.1 for 133.33.33.32,
group 239.255.0.1 19 PIM: Forward decapsulated data packet for 239.255.0.1 on Ethernet0 10 PIM:
Forward decapsulated data packet for 239.255.0.1 on Serial0 21 PIM: Send Join on Serial0 to
192.168.7.1 for (133.33.33.32/32, 239.255.0.1), S-bit 22 PIM: Send Join on Serial0 to
192.168.7.1 for (133.33.33.32/32, 239.255.0.1), S-bit 23 PIM: Send Register-Stop to 192.168.7.1
for 133.33.33.32, group 239.255.0.1 24 PIM: Received Join/Prune on Serial0 from 192.168.7.1, to
us 25 PIM: Prune-list: (133.33.33.32/32, 239.255.0.1) 26 PIM: Received v2 Join/Prune on
Ethernet0 from 192.168.10.1, to us 27 PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2, RPT-bit
set, WC-bit set, S-bit set 28 PIM: Add Ethernet0/192.168.10.1 to (*, 239.255.0.1), Forward state
```

```
29 PIM: Add Ethernet0/192.168.10.1 to (133.33.33.32/32, 239.255.0.1) 30 PIM: Join-list:
(133.33.33.32/32, 239.255.0.1), S-bit set 31 PIM: Add Ethernet0/192.168.10.1 to
(133.33.33.32/32, 239.255.0.1), Forward state 32 PIM: Building Join/Prune message for
239.255.0.1 33 PIM: For 192.168.7.1, Join-list: 133.33.33.32/32 34 PIM: For 192.168.10.1, Join-
list: 192.168.9.1/32 35 PIM: Send v2 periodic Join/Prune to 192.168.10.1 (Ethernet0) 36 PIM:
Send periodic Join/Prune to 192.168.7.1 (Serial0) 37 PIM: Received Join/Prune on Serial0 from
192.168.7.1, to us 38 PIM: Join-list: (*, 239.255.0.1) RP 192.168.7.2, RP-bit set, WC-bit set,
S-bit set 39 PIM: Add Serial0/192.168.7.1 to (*, 239.255.0.1), Forward state 40 PIM: Add
Serial0/192.168.7.1 to (133.33.33.32/32, 239.255.0.1) 41 PIM: Add Serial0/192.168.7.1 to
(192.168.9.1/32, 239.255.0.1) 42 PIM: Join-list: (192.168.9.1/32, 239.255.0.1), S-bit set 43
PIM: Add Serial0/192.168.7.1 to (192.168.9.1/32, 239.255.0.1), Forward state 44 PIM: Join-list:
(*, 239.255.0.1) RP 192.168.7.2, RP-bit set, WC-bit set, S-bit set 45 PIM: Add
Serial0/192.168.7.1 to (*, 239.255.0.1), Forward state
```

A linha 1 acima mostra esse R3, que está conectado diretamente à origem via Ethernet0/0, recebe tráfego multicast para o grupo 239.255.0.1. Ela cria uma entrada (*, 239.255.0.1) e envia uma mensagem Join ao RP.

As linhas 16 e 17 mostram que R2, que é o RP, também recebe a mensagem Join/Prune e devolve informações de acessibilidade do RP ao R3.

Nas linhas 5 e 6, R3 atualiza seu temporizador de expiração RP após receber as informações de acessibilidade do RP. As linhas 7 e 8 acima mostram que R3 usa sua entrada (*, G) para enviar os dados ao RP encapsulado em um pacote de registrador com a fonte que inicia a transmissão para agrupar 239.255.0.1.

As linhas 18 a 20 mostram que R2 recebeu o pacote do registrador, desencapsulado e o encaminhou para baixo na árvore com uma entrada (*, 239.255.0.1) preexistente na tabela de roteamento.

As linhas 21 e 29 mostram que R2 envia uma mensagem de União em direção a R3 e instala uma entrada (S,G) (133.33.33.32, 239.255.0.1) na tabela mroute.

As linhas 9 a 11 mostram que R3 recebe a mensagem Join de R2, instala a entrada (S, G) (133.33.33.32,239.255.0.1) na tabela mroute, e aciona o modo de encaminhamento na interface conectada ao RP, que cria a árvore SPT (S,G) multicast voltada para a origem.

Na linha 23, R2 começa a receber SPT de tráfego para baixo (S,G) e envia uma mensagem de interrupção de registro (e uma mensagem Join) para a origem.

As linhas 12 a 15 mostram que R3 recebe a mensagem de interrupção de registro, remove o sinalizador do registro, e interrompe o tráfego (S,G) de encapsulamento.

Mensagens periódicas de Join/Prune (Juntar/Reduzir) são trocadas entre o RP e o R3 para manter a árvore de multicast.

Informações Relacionadas

- Manual de Troubleshooting de IP Multicast
- Manual de configuração de Multicast Quick Start
- Página de Suporte ao Multicast IP
- Página de suporte dos protocolos roteados de IP
- Página de Suporte do IP Routing
- IP3R: Referência de Comandos IP do Cisco IOS, Volume 3 de 3: Multicast, Release 12.2

- Suporte Técnico - Cisco Systems