Entender mensagens de redirecionamento ICMP

Contents

Introduction

Este documento descreve a funcionalidade de redirecionamento de pacotes do Internet Control Message Protocol (ICMP).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Arquitetura da plataforma Nexus 7000
- Configuração do software Cisco NX-OS
- Internet Control Message Protocol conforme documentado em Request for Comments (RFC) 792

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Nexus 7000
- Software Cisco NX-OS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento discute a funcionalidade de redirecionamento de pacotes fornecida pelo Internet Control Message Protocol (ICMP). O documento explica o que a presença de mensagens de redirecionamento ICMP na rede geralmente indica e o que pode ser feito para minimizar os efeitos colaterais negativos associados às condições de rede que causam a geração de mensagens de redirecionamento ICMP.

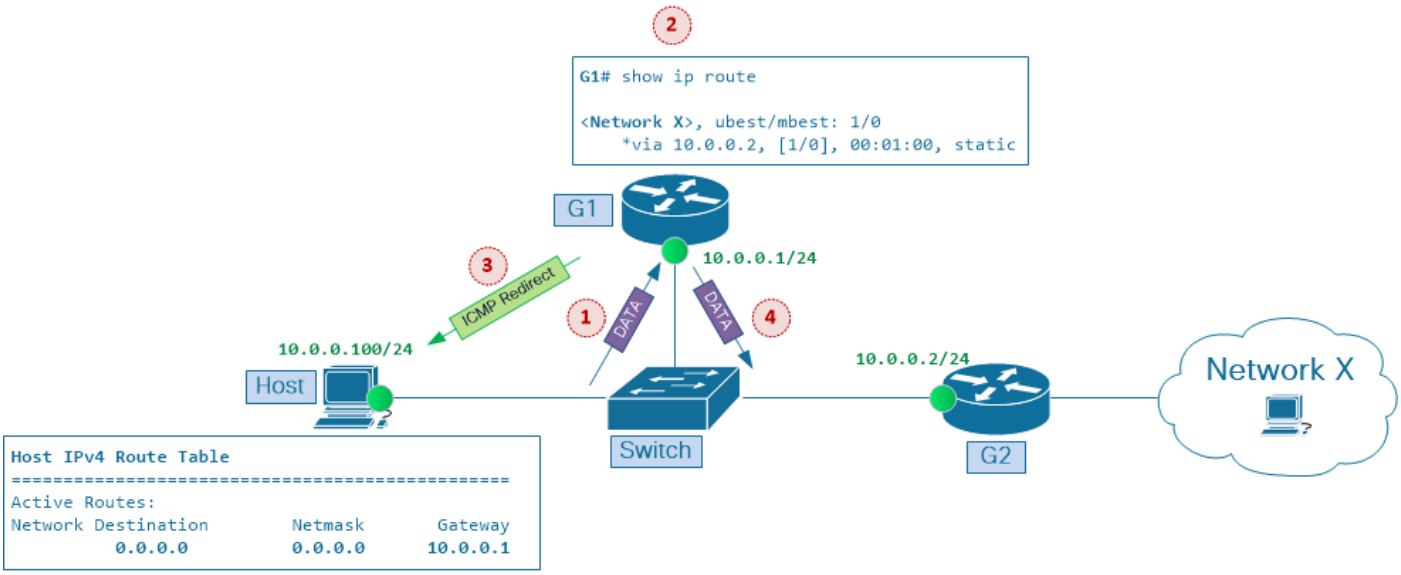
Mensagens de redirecionamento ICMP

A funcionalidade de redirecionamento de ICMP é explicada no RFC 792 Internet Control Message Protocol com este exemplo:

> O gateway envia uma mensagem de redirecionamento a um host nessa situação.
>
> Um gateway, G1, recebe um datagrama de Internet de um host em uma rede à qual o gateway está conectado. O gateway, G1, verifica sua tabela de roteamento e obtém o endereço do próximo gateway, G2, na rota para a rede de destino de Internet do datagrama, X
>
> Se o G2 e o host identificado pelo endereço de origem na Internet do datagrama estiverem na mesma rede, uma mensagem de redirecionamento será enviada ao host. A mensagem de redirecionamento aconselha o host a enviar seu tráfego para a rede X diretamente para o gateway G2, pois esse é um caminho mais curto para o destino.
>
> O gateway encaminha os dados do datagrama original para seu destino na Internet.

Esse cenário é mostrado na Figura 1. O host e dois roteadores, G1 e G2, estão conectados ao segmento Ethernet compartilhado e têm endereços IP na mesma rede 10.0.0.0/24

Figura 1 Redirecionamentos de ICMP em redes Ethernet multiponto



Redirecionamentos de ICMP em Redes Ethernet Multiponto

O host tem o endereço IP 10.0.0.100. A tabela de roteamento do host tem uma entrada de rota padrão que aponta para o endereço IP 10.0.0.1 do roteador G1 como o gateway padrão. O roteador G1 usa o endereço IP 10.0.0.2 do roteador G2 como seu próximo salto ao encaminhar o tráfego para a rede de destino X.

Isso é o que acontece quando o Host envia um pacote à rede destino X:

1. Gateway G1 com endereço IP 10.0.0.1 recebe pacote de dados do host 10.0.0.100 em uma rede à qual está conectado.

2. O gateway, G1, verifica sua tabela de roteamento e obtém o endereço IP 10.0.0.2 do próximo gateway, G2, na rota para a rede destino do pacote de dados, X.

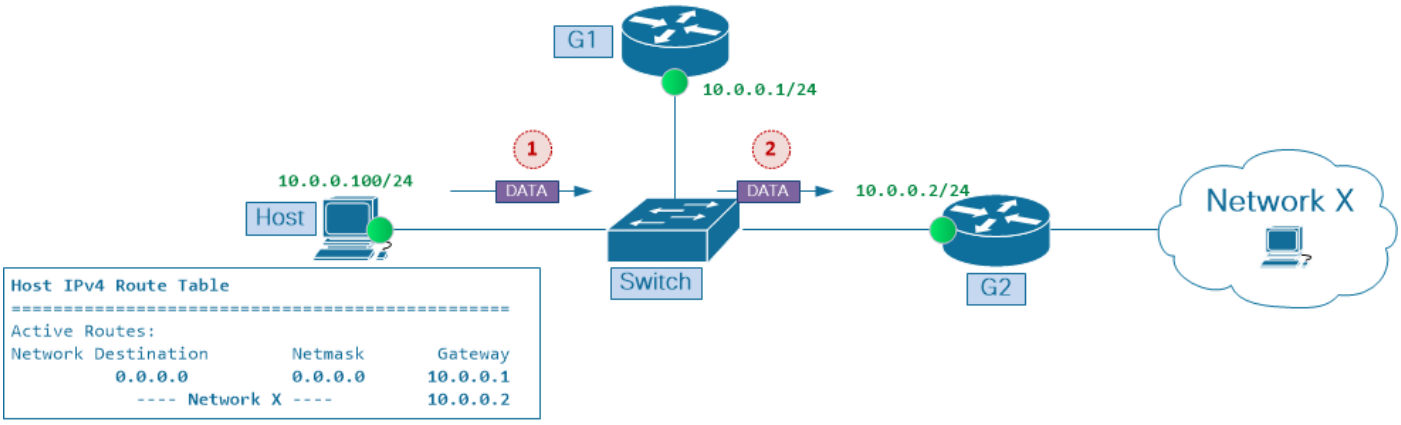
3. Se o G2 e o host identificado pelo endereço de origem do pacote IP estiverem na mesma rede, a mensagem de Redirecionamento ICMP será enviada ao host. A mensagem de Redirecionamento ICMP aconselha o host a enviar seu tráfego para a rede X diretamente ao gateway G2, pois esse é um caminho mais curto para o destino.

4. O gateway G1 encaminha o pacote de dados original ao seu destino.

Dependendo da configuração do host, ele pode optar por ignorar as mensagens de redirecionamento ICMP que o G1 envia para ele. No entanto, se o host usar mensagens de redirecionamento ICMP para ajustar seu cache de roteamento e começar a enviar pacotes de dados subsequentes diretamente para G2, esses benefícios serão obtidos nesse cenário

- Otimização do caminho de encaminhamento de dados através da rede; o tráfego chega ao seu destino mais rapidamente
- Redução da utilização de recursos da rede, como largura de banda e carga da CPU do roteador

Figura 2 Próximo Salto G2 Instalado no Cache de Roteamento do Host



Próximo salto G2 instalado no cache de roteamento do host

Como mostrado na Figura 2, depois que o host criou a entrada de cache de rota para a Rede X com G2 como seu próximo salto, esses benefícios são vistos na rede:

- A utilização da largura de banda no link entre o Switch e o roteador G1 diminui em ambas as direções.
- A utilização da CPU no roteador G1 é reduzida, pois o fluxo de tráfego do Host para a Rede X

não atravessa mais esse nó.

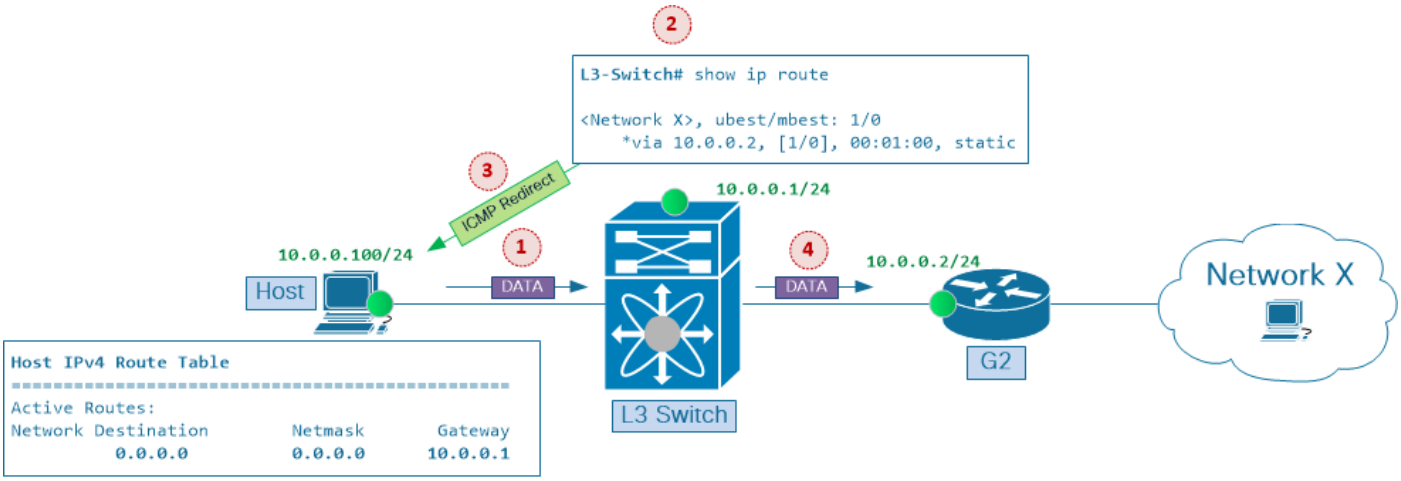
- O atraso de rede de ponta a ponta entre o Host e a Rede X melhora.

Para entender a importância do mecanismo de redirecionamento ICMP, lembre-se de que as primeiras implementações de roteadores da Internet dependiam principalmente dos recursos da CPU para processar o tráfego de dados. Portanto, era desejável reduzir o volume de tráfego que tinha de ser tratado por qualquer roteador e também minimizar o número de saltos de roteador que um fluxo de tráfego específico tinha de atravessar a caminho do destino. Ao mesmo tempo, o encaminhamento de Camada 2 (também conhecido como comutação) foi implementado principalmente em Circuitos Integrados Específicos de Aplicação (ASIC - Application-Specific Integrated Circuits) personalizados, e da perspectiva de desempenho de encaminhamento era relativamente "barato" em comparação com o encaminhamento de Camada 3 (também chamado de roteamento), que, novamente, foi feito em processadores de uso geral.

As gerações ASIC mais recentes podem fazer o encaminhamento de pacotes de Camada 2 e Camada 3. A consulta na tabela da Camada 3 realizada no hardware ajuda a reduzir o custo de desempenho associado ao tratamento de pacotes pelos roteadores. Além disso, quando a funcionalidade de encaminhamento de Camada 3 em switches de Camada 2 foi integrada (que agora são chamados de switches de Camada 3) tornou a operação de encaminhamento de pacotes mais eficiente, isso eliminou a necessidade de opções de design de **roteador com um braço** (também conhecido como **roteador em um bastão**) e evita limitações associadas a essas configurações de rede.

A Figura 3 baseia-se no cenário da Figura 1. Agora, as funções de Camada 2 e Camada 3, fornecidas originalmente por dois nós separados, Switch e roteador G1, são consolidadas em um único Switch de Camada 3, como a plataforma Nexus 7000 Series.

Figura 3 Switch de Camada 3 Substitui a Configuração de "Um Roteador Armado"



Switch de Camada 3 Substitui a Configuração de "Um Roteador Armado"

Isso é o que acontece quando o Host envia um pacote à Rede X de destino:

1. Switch L3 Gateway com endereço IP 10.0.0.1 recebe pacote de dados de um host 10.0.0.100 em uma rede à qual está conectado.

2. O gateway, Switch L3, verifica sua tabela de roteamento e obtém o endereço 10.0.0.2 do próximo gateway, G2, na rota para a rede de destino do pacote de dados, X.

3. Se o G2 e o host identificado pelo endereço de origem do pacote IP estiverem na mesma rede, a mensagem de Redirecionamento ICMP será enviada ao host. A mensagem de

Redirecionamento ICMP aconselha o host a enviar seu tráfego para a Rede X diretamente ao gateway G2, pois esse é um caminho mais curto para o destino.

4. O gateway encaminha o pacote de dados original ao seu destino.

Com os switches de Camada 3 agora capazes de executar encaminhamento de pacotes de Camada 2 e Camada 3 no nível ASIC, pode-se concluir que ambos os benefícios da funcionalidade Redirecionamento ICMP, (a) melhoria do atraso através da rede e (b) redução da utilização de recursos de rede, são alcançados, e não há mais necessidade de se ter muita atenção às técnicas de otimização de caminho em segmentos Ethernet multiponto.

No entanto, com a funcionalidade de redirecionamento ICMP habilitada nas interfaces de Camada 3, o encaminhamento não otimizado através de segmentos Ethernet multiponto continua a apresentar gargalos de desempenho em potencial, mesmo que por um motivo diferente, como explicado na seção Considerações sobre a plataforma Nexus, mais adiante neste documento.

> **Note**: Os redirecionamentos de ICMP são ativados por padrão nas interfaces de Camada 3 no software Cisco IOS e Cisco NX-OS.

> **Note**: Resumo das condições quando mensagens de redirecionamento ICMP são geradas: O switch de Camada 3 gera a mensagem de redirecionamento ICMP de volta à origem do pacote de dados, se o pacote de dados tiver que ser encaminhado através da interface de Camada 3 na qual esse pacote é recebido.

Caminhos sub-ideais através de redes Ethernet

Os Interior Gateway Protocols (IGP), como o Open Shortest Path First (OSFP) e o Cisco Enhanced Interior Gateway Routing Protocol (EIGRP), são projetados para sincronizar as informações de roteamento entre os roteadores e para fornecer um comportamento consistente e previsível de encaminhamento de pacotes em todos os nós de rede que honrem essas informações. Por exemplo, com redes Ethernet multiponto, se todos os nós de Camada 3 em um segmento usarem as mesmas informações de roteamento e concordarem com o mesmo ponto de saída para o destino, o encaminhamento abaixo do ideal através dessas redes raramente é o caso.

Para entender o que causa caminhos de encaminhamento abaixo do ideal, lembre-se de que os nós da camada 3 tomam decisões de encaminhamento de pacotes independentemente uns dos outros. Ou seja, a decisão de encaminhamento de pacotes tomada pelo Roteador B não depende da decisão de encaminhamento de pacotes tomada pelo Roteador A. Esse é um dos princípios-chave a serem lembrados ao solucionar problemas de encaminhamento de pacotes através de redes IP e é importante ter em mente quando você investiga caminhos de encaminhamento não ideais em redes Ethernet multiponto.

Como mencionado anteriormente, em redes onde todos os roteadores dependem de um único protocolo de roteamento dinâmico para fornecer tráfego entre pontos finais, o encaminhamento abaixo do ideal através de segmentos Ethernet multiponto não deve acontecer. No entanto, em redes reais é muito comum encontrar combinações de vários mecanismos de roteamento e encaminhamento de pacotes. Exemplos desses mecanismos são vários IGPs, Roteamento Estático e Roteamento Baseado em Política. Esses recursos são normalmente usados em

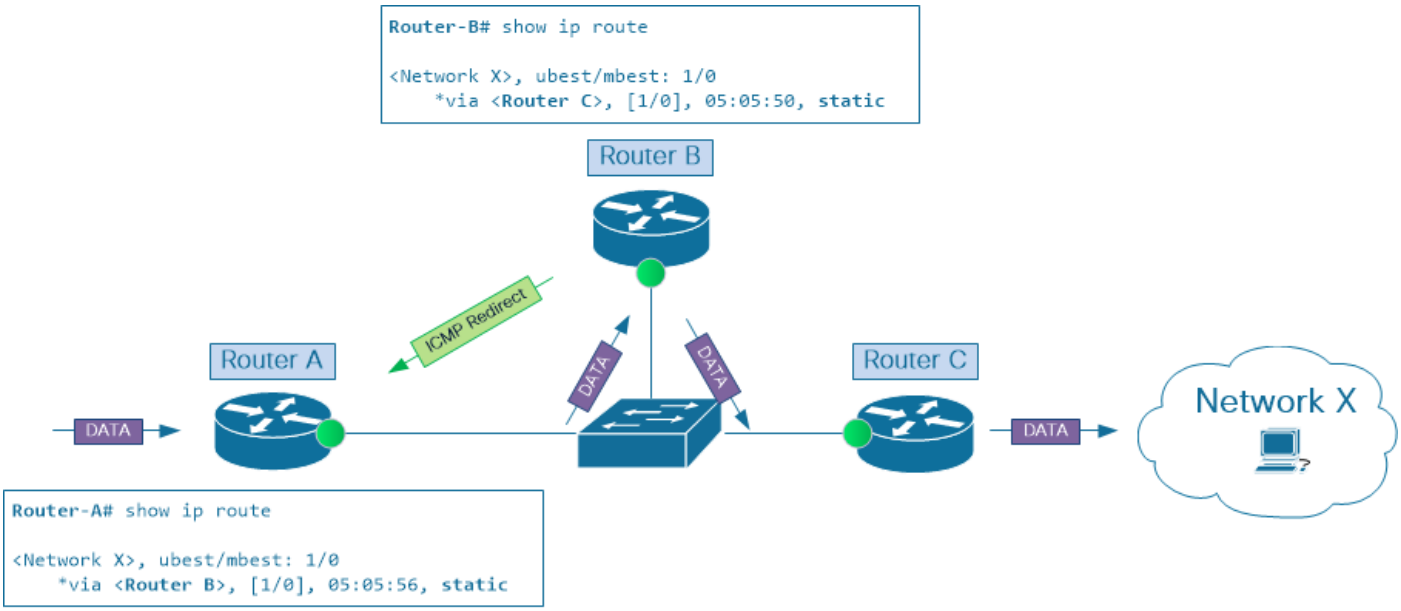
conjunto para obter o encaminhamento de tráfego desejado através da rede.

Embora o uso combinado desses mecanismos possa ajudar a ajustar o fluxo de tráfego e atender aos requisitos de um projeto de rede específico, eles ignoram os efeitos colaterais que essas ferramentas juntas podem causar em redes Ethernet multiponto que podem resultar em um desempenho geral de rede ruim.

Roteamento estático

Para ilustrar isso, considere o cenário na Figura 4. O Roteador A tem uma rota estática para a Rede X com o Roteador B como seu próximo salto. Ao mesmo tempo, o Roteador B usa o Roteador C como seu próximo salto na rota estática para a Rede X.

Figura 4 Caminho abaixo do ideal com roteamento estático



Caminho abaixo do ideal com roteamento estático

Enquanto o tráfego entra nessa rede no Roteador A, sai dele através do Roteador C e, por fim, é entregue à Rede X de destino, os pacotes têm que atravessar essa rede IP duas vezes a caminho do destino. Esse não é um uso eficiente dos recursos da rede. Em vez disso, enviar pacotes do Roteador A diretamente para o Roteador C alcançaria os mesmos resultados, enquanto consumiria menos recursos de rede.

> **Note**: Embora neste cenário os Roteadores A e C sejam usados como nós de Camada 3 de entrada e saída para este segmento de rede IP, ambos os nós podem ser substituídos por dispositivos de rede (como Balanceadores de Carga ou Firewalls) se estes últimos tiverem uma configuração de roteamento que resulte no mesmo comportamento de encaminhamento de pacotes.

Roteamento baseado em políticas

O Roteamento Baseado em Políticas (PBR - Policy Based Routing) é outro mecanismo que pode causar um caminho abaixo do ideal através de redes Ethernet. No entanto, ao contrário do Roteamento Estático ou Dinâmico, o PBR não opera no nível da tabela de roteamento. Em vez disso, ele programa o tráfego para redirecionar a ACL (Lista de Controle de Acesso) diretamente

no hardware do switch. Como resultado, para fluxos de tráfego selecionados, a consulta de encaminhamento de pacotes na placa de linha de entrada ignora as informações de roteamento obtidas por meio do Roteamento Estático ou Dinâmico.

Na Figura 4, os Roteadores A e B trocam informações de roteamento sobre a Rede X de destino com um dos protocolos de roteamento dinâmico. Ambos concordam que o Roteador B é o melhor próximo salto para essa rede.

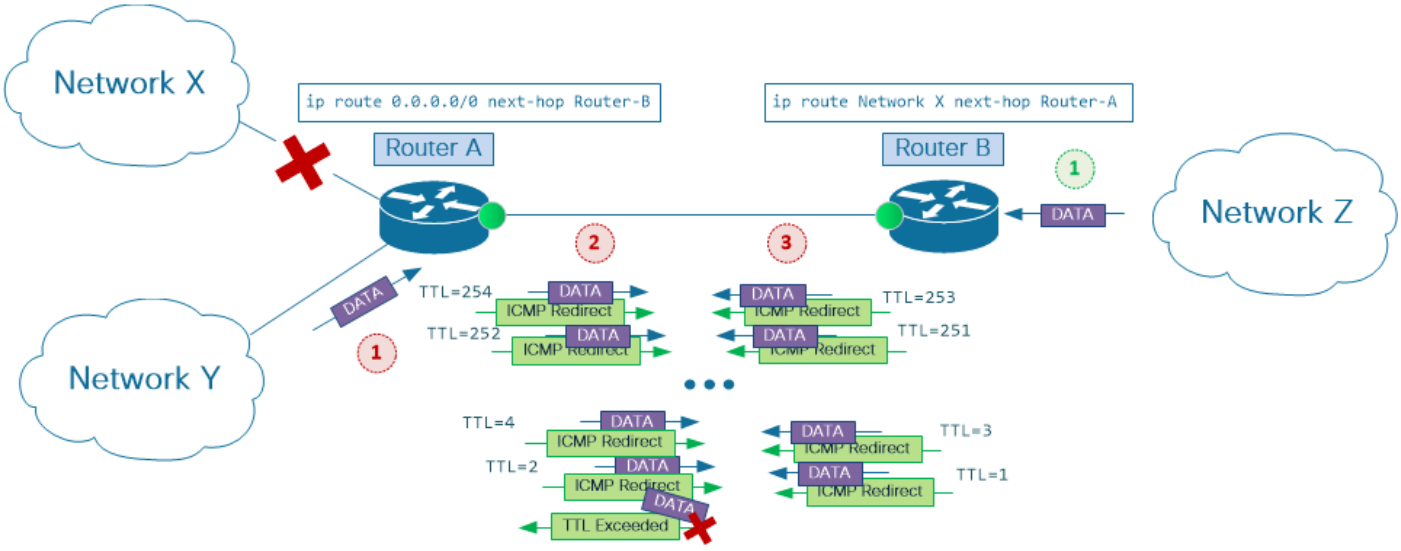
No entanto, com uma configuração de PBR no Roteador B que substitui as informações de roteamento recebidas do protocolo de roteamento e define o Roteador C como o próximo salto para a rede X, a condição para acionar a função de Redirecionamento ICMP é atendida e o pacote é enviado para a CPU do Roteador B para processá-lo ainda mais.

Redirecionamentos de ICMP em links ponto a ponto

Até agora, este documento referia-se a redes Ethernet que têm três (ou mais) nós de Camada 3 conectados, daí o nome redes Ethernet multiponto. Entretanto, lembre-se de que as mensagens de redirecionamento ICMP também podem ser geradas em links Ethernet ponto a ponto.

Considere o cenário na Figura 5. O Roteador A usa uma rota padrão estática para enviar tráfego ao Roteador B, enquanto o Roteador B tem uma rota estática para a rede X que aponta para o Roteador A.

Figura 5 Redirecionamentos de ICMP em Links Ponto a Ponto



Caminho abaixo do ideal com roteamento estático

Essa opção de design, também conhecida como conexão single-homed, é uma escolha popular quando você conecta ambientes de usuários pequenos a redes de provedores de serviços. Aqui o Roteador B é um dispositivo PE (Provider Edge) e o Roteador A é um dispositivo CE (User Edge).

Observe que a configuração típica do CE inclui rotas estáticas agregadas para blocos de endereço IP do usuário que apontam para a interface Null0. Essa configuração é uma prática recomendada para a opção de conectividade CE-PE single-homed com roteamento estático. No entanto, para os fins deste exemplo, suponha que tal configuração não esteja presente.

Suponha que o Roteador A perca conectividade com a Rede X, como mostrado na figura.

Quando os pacotes do usuário Network Y ou da Rede Z remota tentam acessar a Rede X, os Roteadores A e B podem devolver o tráfego entre si e diminuir o campo IP Time-To-Live em cada pacote até que seu valor atinja 1, momento em que o roteamento adicional do pacote não é possível.

Enquanto o tráfego para a Rede X é devolvido entre os roteadores PE e CE, aumenta drasticamente (e desnecessariamente) a utilização da largura de banda do link CE-PE, o problema se torna pior se os redirecionamentos ICMP são ativados em um ou nos dois lados da conexão PE-CE ponto a ponto. Nesse caso, cada pacote no fluxo direcionado à Rede X é processado na CPU em cada roteador várias vezes para ajudar a gerar as mensagens de redirecionamento ICMP.

Considerações sobre a plataforma Nexus

Quando os redirecionamentos de ICMP são ativados na interface da Camada 3 e um pacote de dados de entrada usa essa interface para entrar e sair de um switch da Camada 3, uma mensagem de redirecionamento de ICMP é gerada. Embora o encaminhamento de pacotes da Camada 3 seja feito em hardware na plataforma Cisco Nexus 7000, ainda é responsabilidade da CPU do switch criar mensagens de redirecionamento de ICMP. Para fazer isso, a CPU no módulo Supervisor do Nexus 7000 precisa obter informações de endereço IP do fluxo cujo caminho pelo segmento de rede pode ser otimizado. Essa é a razão por trás do pacote de dados enviado pela placa de linha de entrada para o módulo Supervisor.

Se os destinatários da mensagem de redirecionamento de ICMP a ignorarem e continuarem encaminhando o tráfego de dados para a interface de Camada 3 do switch Nexus na qual os redirecionamentos de ICMP estão ativados, o processo de geração de redirecionamento de ICMP será acionado para cada pacote de dados.

No nível da placa de linha, o processo começa na forma de exceção de encaminhamento de hardware. São geradas exceções em ASICs quando a operação de encaminhamento de pacotes não pode ser concluída com êxito pelo módulo de placa de linha. Nesse caso, o pacote de dados precisa ser enviado ao módulo Supervisor para o manuseio correto do pacote.

> Note: A CPU no módulo Supervisor, além de gerar mensagens de redirecionamento ICMP, trata de muitas outras exceções de encaminhamento de pacotes, como pacotes IP com valor Time To Live (TTL) definido como 1 ou pacotes IP que precisam ser fragmentados antes de serem enviados para o próximo salto.

Depois que a CPU no módulo Supervisor enviou uma mensagem de redirecionamento ICMP à origem, ela conclui o tratamento de exceções encaminhando o pacote de dados ao próximo salto através do módulo da placa de linha de saída.

Enquanto os módulos Supervisor do Nexus 7000 usam poderosos processadores de CPU que podem processar grandes volumes de tráfego, a plataforma é projetada para lidar com a maioria do tráfego de dados no nível da placa de linha sem a necessidade de envolver o processador de CPU do Supervisor no processo de encaminhamento de pacotes. Isso permite que a CPU se concentre em suas tarefas principais e deixa a operação de encaminhamento de pacotes para mecanismos de hardware dedicados em placas de linha.

Em redes estáveis, espera-se que as exceções de encaminhamento de pacotes, se ocorrerem, ocorram a taxas razoavelmente baixas. Com essa suposição, elas podem ser tratadas pelo

Supervisor CPU sem impacto significativo em seu desempenho. Por outro lado, com uma CPU que lida com exceções de encaminhamento de pacotes que ocorrem em uma taxa muito alta pode ter um efeito negativo na estabilidade e capacidade de resposta geral do sistema.

O design da plataforma Nexus 7000 fornece vários mecanismos para proteger a CPU do switch de quantidades significativas de tráfego. Esses mecanismos são implementados em diferentes pontos do sistema. No nível da placa de linha, há limitadores de taxa de hardware e plano de controle Policing (CoPP). Ambos definem limiares de taxa de tráfego, que controlam efetivamente a quantidade de tráfego a ser encaminhada ao Supervisor a partir de cada módulo de placa de linha.

Esses mecanismos de proteção dão preferência ao tráfego de vários protocolos de controle que são críticos para a estabilidade da rede e gerenciabilidade do switch, como OSPF, BGP ou SSH, e ao mesmo tempo filtram agressivamente tipos de tráfego que não são críticos para controlar a funcionalidade do plano do switch. A maior parte do tráfego de dados, se encaminhado para a CPU como resultado de exceções de encaminhamento de pacotes, é fortemente vigiado por esses mecanismos.

Embora os limitadores de taxa de hardware e CoPP policing os mecanismos fornecem estabilidade do plano de controle do switch e é altamente recomendável que estejam sempre ativados; eles podem ser um dos principais motivos de quedas de pacotes de dados, atrasos de transferência e desempenho geral ruim de aplicativos na rede. É por isso que é importante entender os caminhos que os fluxos de tráfego percorrem na rede e o uso de ferramentas para monitorar o equipamento de rede que pode e/ou deve usar a funcionalidade Redirecionamento ICMP.

Ferramentas para monitorar e diagnosticar tráfego

show ip traffic

Os softwares Cisco IOS e Cisco NX-OS oferecem uma maneira de verificar as estatísticas do tráfego que é processado pela CPU. Isso é feito com **show ip traffic** comando. Esse comando pode ser usado para verificar o recebimento e/ou a geração de mensagens de redirecionamento ICMP pelo switch ou roteador de Camada 3.

```
Nexus7000#show ip traffic | begin ICMP

ICMP Software Processed Traffic Statistics
----------------------------------------
Transmission:
Redirect: 1000, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

ICMP originate Req: 0, Redirects Originate Req: 1000
Originate deny - Resource fail: 0, short ip: 0, icmp: 0, others: 0
Reception:
Redirect: 0, unreachable: 0, echo request: 0, echo reply: 0,
```

```
<output omitted for brevity>

Nexus7000#
```

Executar show ip traffic algumas vezes e verifique se os contadores de redirecionamento ICMP são incrementados.

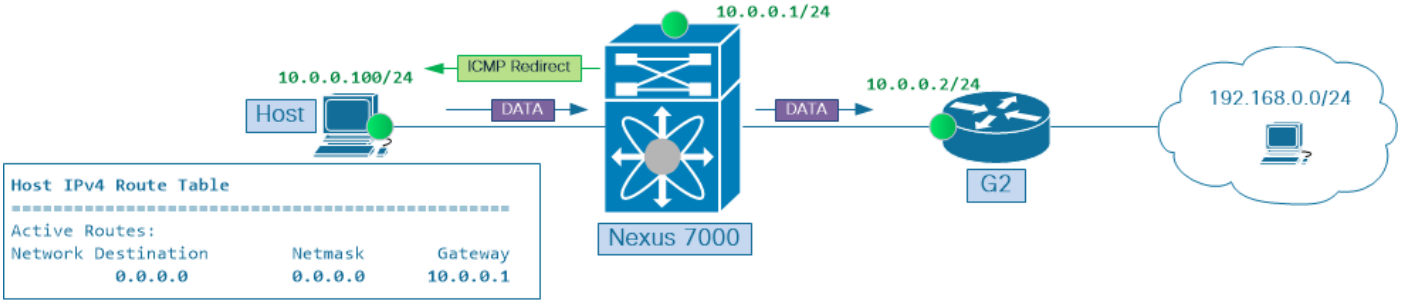
Ethanalyzer

O software Cisco NX-OS tem uma ferramenta integrada para capturar o tráfego flowing de e para a CPU do switch, conhecida como Ethanalyzer.

> **Note**: Para obter mais informações sobre o Ethanalyzer, consulte Ethanalyzer on Nexus 7000 Troubleshooting Guide.

A Figura 6 mostra um cenário semelhante ao da Figura 3. Aqui, a Rede X é substituída pela rede 192.168.0.0/24.

Figura 6 - Executar captura do Ethanalyzer



Executar captura do Ethanalyzer

O Host 10.0.0.100 envia um fluxo contínuo de Solicitações de Eco ICMP para o endereço IP destino 192.168.0.1. O Host usa o Switch Virtual Interface (SVI) 10 do switch Nexus 7000 como seu próximo salto para a rede remota 192.168.0.0/24. Para fins de demonstração, o Host é configurado para ignorar mensagens de Redirecionamento ICMP.

Use este próximo comando para capturar o tráfego ICMP recebido e enviado pela CPU do Nexus 7000:

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000

Capturing on inband
2018-09-15 23:45:40.124077   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.124477     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.124533   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126344   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.126655   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128348   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128611     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
    2018-09-15 23:45:40.128659   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130362   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130621     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
```

```
2018-09-15 23:45:40.130669   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132392   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132652     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.132700   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134612     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.134660   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136598     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.136645   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138351   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.138656   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request

...
```

Os timestamps na saída anterior sugerem que três pacotes destacados neste exemplo foram capturados ao mesmo tempo, 2018-09-15 23:45:40.128. O próximo é uma divisão por pacote deste grupo de pacotes

- O primeiro pacote é o pacote de dados de entrada, que neste exemplo é uma solicitação de eco ICMP.

  2018-09-15 23:45:40.128348 10.0.0.100 -> 192.168.0.1 Solicitação de eco (ping) ICMP

- O segundo pacote é um pacote de redirecionamento ICMP, gerado pelo gateway. Esse pacote é enviado de volta ao host.

  2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 Redirecionamento ICMP (Redirecionamento para host)

- O terceiro pacote é o pacote de dados capturado na direção de saída, depois de ter sido roteado pela CPU. Embora não mostrado anteriormente, esse pacote tem seu TTL IP diminuído e o checksum recalculado.

  2018-09-15 23:45:40.128659 10.0.0.100 -> 192.168.0.1 Solicitação de eco (ping) ICMP

Enquanto você navega por grandes capturas do Ethanalyzer que têm muitos pacotes de diferentes tipos e fluxos, pode ser difícil correlacionar as mensagens de redirecionamento ICMP com o tráfego de dados que corresponde a elas.

Nessas situações, concentre-se nas mensagens de redirecionamento ICMP para recuperar informações sobre fluxos de tráfego encaminhados de forma não ideal. As mensagens de Redirecionamento ICMP incluem o cabeçalho da Internet mais os primeiros 64 bits dos dados do datagrama original. Esses dados são usados pela origem do datagrama para corresponder a mensagem ao processo apropriado.

Use a ferramenta de captura de pacotes do Ethanalyzer com a palavra-chave **detail** para exibir o conteúdo das mensagens de redirecionamento do ICMP e encontrar informações de endereço IP do fluxo de dados que está sendo encaminhado de forma não ideal

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000
detail

...
Frame 2 (70 bytes on wire, 70 bytes captured)
Arrival Time: Sep 15, 2018 23:54:04.388577000
[Time delta from previous captured frame: 0.000426000 seconds]
```

[Time delta from previous displayed frame: 0.000426000 seconds]
[Time since reference or first frame: 0.000426000 seconds]
Frame Number: 2
Frame Length: 70 bytes
Capture Length: 70 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:ip:icmp:data]
Ethernet II, Src: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf), Dst: 00:0a:00:0a:00:0a
(00:0a:00:0a:00:0a)
Destination: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
Address: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
Source: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
Address: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.100 (10.0.0.100)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 56
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0xadd9 [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.1 (10.0.0.1)
Destination: 10.0.0.100 (10.0.0.100)
Internet Control Message Protocol
Type: 5 (Redirect)
Code: 1 (Redirect for host)
Checksum: 0xb8e5 [correct]
Gateway address: 10.0.0.2 (10.0.0.2)
Internet Protocol, Src: 10.0.0.100 (10.0.0.100), Dst: 192.168.0.1 (192.168.0.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 84
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 254
Protocol: ICMP (0x01)
Header checksum: 0xa8ae [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.100 (10.0.0.100)

```
Destination: 192.168.0.1 (192.168.0.1)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x02f9 [incorrect, should be 0xcae1]
Identifier: 0xa01d
Sequence number: 36096 (0x8d00)

...
```

Desabilite o redirecionamentos de ICMP

Se o projeto de rede exigir que o fluxo de tráfego seja roteado para fora da mesma interface de Camada 3 na qual ele entrou no switch ou roteador, é possível impedir que o fluxo seja roteado através da CPU se você desativar a funcionalidade de redirecionamento ICMP na interface de Camada 3 que corresponde a ele.

Na verdade, para a maioria das redes, é uma boa prática desativar proativamente os redirecionamentos ICMP em todas as interfaces de Camada 3, tanto físicas, como a interface Ethernet, quanto virtuais, como as interfaces de canal de porta e SVI. Use o no ip redirects Comando no nível da interface do Cisco NX-OS para desativar os redirecionamentos ICMP em uma interface de Camada 3. Para verificar se a funcionalidade de redirecionamento ICMP está desativada:

- Garantir**no ip redirects** é adicionado à configuração de interface.

```
Nexus7000#show run interface vlan 10

interface Vlan10
no shutdown no ip redirects
  ip address 10.0.0.1/24
```

- Certifique-se de que o status dos redirecionamentos ICMP na interface mostre "desativado".

```
Nexus7000#show ip interface vlan 10 | include redirects
  IP icmp redirects: disabled
```

- Certifique-se de que o indicador de ativação/desativação do redirecionamento ICMP esteja definido como **0** pelo componente de software do Cisco NX-OS que envia a configuração da interface do Supervisor do switch para uma ou mais placas de linha.

```
Nexus7000#show system internal eltm info interface vlan 10 | i icmp_redirect
  per_pkt_ls_en = 0, icmp_redirect = 0, v4_same_if_check = 0
```

- Certifique-se de que o indicador de ativação/desativação de redirecionamento ICMP para uma interface de Camada 3 específica esteja definido como **0** em uma ou mais placas de linha.

```
Nexus7000#attach module 7
Attaching to module 7 ...
To exit type 'exit', to abort type '$.'
Last login: Wed Sep 15 23:56:25 UTC 2018 from 127.1.1.1 on pts/0
module-7#
```

```
!--- Optionally, jump to non-admin Virtual Device Context (VDC) if verification needs to be done
in one of the custom VDCs
module-7#vdc 6

module-7#show system internal iftmc info interface vlan 10 | include icmp_redirect
icmp_redirect : 0x0 ipv6_redirect : 0x1
```

Summary

O mecanismo de redirecionamento ICMP, conforme descrito no RFC 792, foi projetado para otimizar o caminho de encaminhamento através de segmentos de rede multiponto. No início da Internet, essa otimização ajudou a proteger recursos de rede caros, como a largura de banda do link e os ciclos de CPU dos roteadores. À medida que a largura de banda da rede se tornou mais acessível e o roteamento de pacotes baseado em CPU relativamente lento evoluiu para um encaminhamento mais rápido de pacotes de Camada 3 em ASICs de hardware dedicados, a importância do trânsito ideal de dados através de segmentos de rede de vários pontos diminuiu. Por padrão, a funcionalidade Redirecionamento ICMP é habilitada em cada interface de Camada 3. No entanto, suas tentativas de notificar nós de rede em segmentos Ethernet multiponto sobre caminhos de encaminhamento ideais nem sempre são entendidas e tomadas medidas pelo pessoal de rede. Em redes com o uso combinado de vários mecanismos de encaminhamento, como Roteamento Estático, Roteamento Dinâmico e Roteamento Baseado em Política, se você deixar a funcionalidade Redirecionamento ICMP habilitada e não monitorá-la corretamente, isso poderá resultar no uso indesejado da CPU do(s) nó(s) de trânsito para tratar do tráfego de produção. Isso, por sua vez, pode causar um impacto significativo nos fluxos de tráfego de produção e na estabilidade do plano de controle da infraestrutura de rede.

Para a maioria das redes, considera-se uma boa prática desativar proativamente a funcionalidade Redirecionamento ICMP em todas as interfaces de Camada 3 na infraestrutura de rede. Isso ajuda a evitar cenários de tráfego de dados de produção que são manipulados na CPU de switches e roteadores de Camada 3 quando há um caminho de encaminhamento melhor através de segmentos de rede multiponto.

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.