Inundação de Unicast em Redes de Campus Comutadas

Índice

Introdução

Este documento discute causas possíveis e implicações da inundação de pacotes do unicast em redes comutadas.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Definição do problema

Tabelas do forwarding do uso dos switch LAN (tabelas da camada 2 (L2), tabelas do Content Addressable Memory (CAM)) ao tráfego direto às portas específicas baseadas no número de VLAN e no endereço MAC de destino do quadro. Quando, no VLAN de entrada, não há nenhuma entrada correspondente ao endereço MAC de destino do quadro, o quadro (unicast) é enviado

para todas as portas de encaminhamento dentro do respectivo VLAN, o que causa inundação.

Inundação limitada faz parte do processo de switching normal. No entanto, há situações em que inundação contínua pode provocar efeitos adversos no desempenho da rede. Este documento explica quais as questões que podem surgir devido à inundação e as causas mais comuns de certos tráficos serem constantemente inundados.

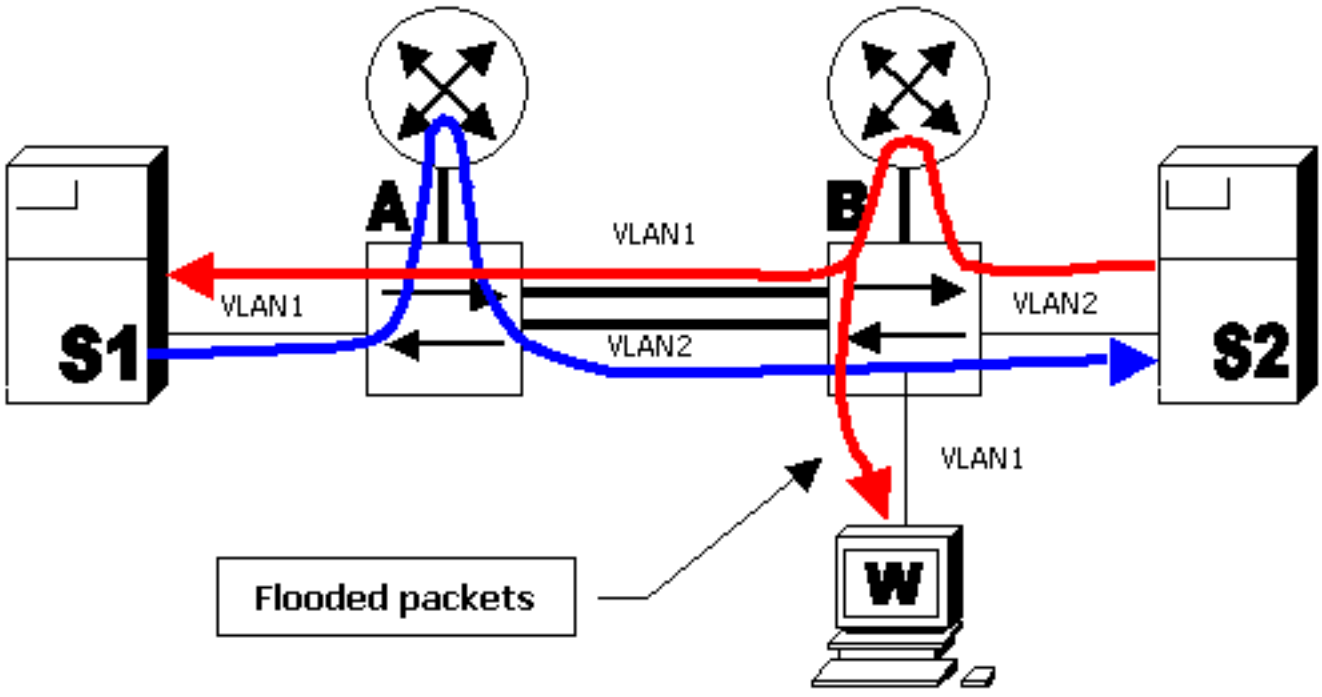
Note que a maioria de Switches moderno que inclui o Catalyst 2900 XL, os 3500 XL, os 2940, a 2950, 2970, 3550, 3750, 4500/4000, 5000, e Switches do 6500/6000 Series mantém as tabelas do forwarding L2 pelo VLAN.

Causas de inundação

A causa de inundação mesma é que o endereço MAC de destino do pacote não está na tabela do forwarding L2 do interruptor. O pacote será inundado neste caso fora de todas as portas da transmissão em seu VLAN (a não ser que a porta ele foi recebida sobre). Abaixo dos Casos Práticos indique a maioria de motivos comuns para o endereço MAC de destino que não está sendo sabido ao interruptor.

Causa 1: Roteamento assimétrico

Grandes quantidades de tráfego inundado podem saturar os enlaces de largura de banda baixa, causando problemas de desempenho de rede ou parada total de conectividade com dispositivos conectados através de tais enlaces de baixa largura de banda. Considere o seguinte diagrama:



No diagrama acima, o server S1 no VLAN1 é backup running (transferência de dados de grande escala) ao server S2 no server VLAN 2. S1 tem seu gateway padrão que aponta à relação VLAN1 do roteador a. O server S2 tem seu gateway padrão que aponta à relação VLAN2 do roteador b. Os pacotes de S1 a S2 seguirão este caminho:

- S1--VLAN 1--switch A--roteador A--VLAN 2--switch B--VLAN 2--S2 (linha azul)

Os pacotes de S2 a S1 seguem o seguinte caminho:

- S2--VLAN 2--switch B--roteador B--VLAN 1--switch A--inundado a VLAN 1--S1 (linha vermelha)

Note que com tal arranjo, comute A “não verá” o tráfego do MAC address S2 no VLAN2 (desde que o endereço MAC de origem será reescrito pelo roteador B e o pacote chegará somente no VLAN1). Isto significa que cada vez que o interruptor A precisa de enviar o pacote ao MAC address S2, o pacote estará inundado ao VLAN2. A mesma situação ocorrerá com o MAC address S1 no switch B.

Este comportamento é chamado roteamento assimétrico. Os pacotes seguem caminhos diferentes dependendo da direção. O roteamento assimétrico é uma das duas causas mais comuns da inundação.

Impacto de inundação de unicast

Retornando ao exemplo acima, o resultado é que os pacotes de transferência de dados entre o S1 e o S2 estarão inundados na maior parte ao VLAN2 no interruptor A e ao VLAN1 no switch B. Isto significa que cada porta conectada (estação de trabalho W neste exemplo) no VLAN1 no switch B receberá todos os pacotes de conversação entre o S1 e o S2. Suponha que o backup do servidor ocupe 50 Mbps da largura de banda. Esta quantidade de tráfego saturará os links do 10 Mbps. Isso causará uma falha completa da conectividade com os PCs ou uma considerável redução na velocidade.

Essa inundação se deve ao roteamento assimétrico e pode parar quando o servidor S1 enviar um pacote de broadcast (por exemplo Protocolo de Resolução de Endereço (ARP)). O Switch A inundará este pacote ao VLAN1 e ao switch B receberá e aprenderá o MAC address do S1. Desde que o interruptor não está recebendo o tráfego constantemente, esta entrada de encaminhamento envelhecerá eventualmente para fora e inundar recomeçará. O mesmo processo aplica-se ao S2.

Há diferentes abordagens para limitar a inundação causada pelo roteamento assimétrico. Consulte estes documentos para obter outras informações:

- Roteamento assimétrico com grupos de ligação em Switches Catalyst 2948G-L3 e 4908G-L3
- Roteamento Assimétrico e HSRP (Inundação Excessiva de Tráfego de Unicast em Rede com Roteadores Executando HSRP)

A aproximação é normalmente trazer o arp timeout do roteador e o tempo do tabela-envelhecimento da transmissão do Switches perto de se. Isto causará os pacotes ARP ser transmissão. Relearning deve ocorrer antes das idades da entrada de tabela da transmissão L2 para fora.

Um cenário típico onde este tipo da edição possa ser observado está quando há um Switches da camada redundante 3 (L3) (tal como um Catalyst 6000 com Mutilayer Switch Feature Card (o MSFC)) configurado ao balanceamento de carga com Hot Standby Router Protocol (HSRP). Neste caso, um interruptor será ativo para mesmo VLAN e outro será ativo para vlan ímpares.

Causa 2: Alterações na topologia do protocolo de extensão de árvore

Outro problema comum causado pela inundação é a TCN (Notificação de alteração de topologia) no STP (Protocolo de árvore de abrangência). O TCN está projetado corrigir tabelas do forwarding depois que a topologia da transmissão mudou. Isto é necessário para evitar uma

interrupção de conectividade, como depois que uma alteração de topologia alguns destinos previamente acessíveis através das portas particular pôde se tornar acessível através das portas diferentes. O TCN opera diminuindo o tempo de envelhecimento da tabela de encaminhamento, como se o endereço não fosse reaprendido, ele envelhecerá e uma inundação ocorrerá.

Os TCNs são acionados por uma porta fazendo a transição de ou para o estado de encaminhamento. Após o TCN, ainda que o endereço MAC de destino particular tenha envelhecido, não deverá ocorrer inundação por muito tempo na maioria dos casos, já que o endereço será reaprendido. O problema pode aparecer quando os TCNs estão ocorrendo repetidamente em intervalos curtos. O Switches será constantemente fast aging suas tabelas do forwarding assim que a inundação será quase constante.

Normalmente, um TCN é raro em uma rede bem-configurada. Quando a porta em um interruptor vai para cima ou para baixo, há eventualmente um TCN uma vez que o estado STP da porta está mudando a ou da transmissão. Quando a porta está batendo, os TCN repetitivos e a inundação ocorrem.

As portas com o recurso portfast de STP ativadas não provocarão os TCNs quando forem ou vierem de um estado de encaminhamento. A configuração de portfast em todas as portas de dispositivo final (como impressoras, PCs, servidores e assim por diante) deve limitar o TCNs a uma quantidade baixa. Refira este documento para obter mais informações sobre dos TCN:

- Entendendo as alterações de topologia de protocolo de árvore de abrangência

Nota: Em MSFC IO, há uma otimização que provoque interfaces de VLAN para preencher novamente suas tabelas ARP quando há um TCN no VLAN respectivo. Isso limita a inundação no caso de TCNs, pois haverá uma difusão de ARP e o endereço MAC do host ser reaprendido como resposta dos hosts para ARP.

Causa 3: Excesso da tabela de encaminhamento

Uma outra causa possível da inundação pode ser excesso da tabela do forwarding do interruptor. Nesse caso, não é possível conhecer novos endereços, e os pacotes destinados a esses endereços são inundados até que haja espaço disponível na tabela de encaminhamento. Depois disso, novos endereços serão aprendidos. Isto é possível mas raro, desde que a maioria de Switches moderno tem as grandes bastante tabelas do forwarding para acomodar endereços MAC para a maioria de projetos.

A exaustão da tabela de encaminhamento também pode ser causada por um ataque na rede, no qual um host começa a gerar quadros, cada um tendo como origem um endereço MAC diferente. Isto amarrará acima todos os recursos da tabela do forwarding. Quando as tabelas de encaminhamento ficarem saturadas, outro tráfego será inundados porque não é possível ocorrer nova aprendizagem. Este tipo do ataque pode ser detectado examinando a tabela do forwarding do interruptor. A maioria dos endereços MAC apontará para a mesma porta ou grupo de portas. Tais ataques podem ser impedidos limitando o número de endereços MAC aprendidos em portas não-confiável usando os recursos de segurança de porta.

Os manuais de configuração para os Catalyst Switches que dirigem Cisco IOS® ou Cactos Software têm uma seção chamada configurar a Segurança de portas ou configurar o controle de tráfego com base na porta. Refira a documentação técnica para seu interruptor nas páginas de produto dos switch Cisco para mais informação.

Nota: Se a inundação unicast ocorre em uma porta de switch de que esteja configurado para a

Segurança de portas com a condição “restrinja” para prender a inundação, uma violação de segurança trigerred.

```
Router(config-if)#switchport port-security violation restrict
```

Nota: Quando tal violação de segurança ocorre, as portas afetadas configuradas para “restringem” o modo devem deixar cair pacotes com endereços de origem desconhecida até que você remova um número suficiente de endereços MAC seguros para deixar cair abaixo do valor máximo. Isto causa o SecurityViolation ao contrário do incremento.

Nota: Em vez deste comportamento, se a porta de switch o move para o estado de " interrupção " então necessidade de configurar o `unicast do bloco do #switchport do roteador (config-if)` de modo que a porta do switch particular esteja desabilitada para a inundação unicast.

Como detectar a inundação excessiva

A maioria de Switches não executa nenhum comando especial detectar a inundação. Supervisor Engine 2 do Catalyst 6500/6000 e Series Switch mais altos que executam a versão 12.1(14)E e mais recente do software do sistema do Cisco IOS ou versão de software do sistema 7.5 de Cisco Cactos ou característica (nativa) da **proteção de inundação do unicast dos** implementares mais altos”. Em curto, esta característica permite que o interruptor monitore a quantidade de inundação unicast pelo VLAN e tome a ação especificada se inundar excede a quantidade especificada. As ações podem ser ao Syslog, ao limite ou à parada programada VLAN - o Syslog que é as mais úteis para a detecção da inundação. Quando inundar excede a taxa configurada e a ação configurada é Syslog, uma mensagem similar ao seguinte estará imprimida:

```
%UNICAST_FLOOD-4-DETECTED: Host 0000.0000.2100 on vlan 1 is flooding
to an unknown unicast destination at a rate greater than/equal to 1 Kfps
```

O MAC address indicado é o MAC de origem de que os pacotes são inundados neste interruptor. É precisado frequentemente de conhecer os endereços MAC de destino a que o interruptor está inundando (porque o interruptor está enviando olhando o endereço MAC de destino). As versões 12.1(20)E (nativas) do Cisco IOS para o Supervisor Engine 2 do Catalyst 6500/6000 e sobre executarão a capacidade de indicar os endereços MAC a que a inundação está ocorrendo:

```
cat6000#sh mac-address-table unicast-flood
Unicast Flood Protection status: enabled

Configuration:
 vlan      Kfps         action       timeout
------+----------+-----------------+----------
   55          1             alert      none

Mac filters:
 No.   vlan   souce mac addr.           installed on           time left (mm:ss)
-----+------+-----------------+------------------------------+------------------

Flood details:
 Vlan   souce mac addr.              destination mac addr.
------+----------------+-------------------------------------------------
   55   0000.2222.0000    0000.1111.0029, 0000.1111.0040, 0000.1111.0063
                          0000.1111.0018, 0000.1111.0090, 0000.1111.0046
                          0000.1111.006d
```

As investigações adicionais podem então ser realizadas para considerar se o MAC address 0000.2222.0000 é suposto enviar o tráfego aos endereços MAC alistados na seção de endereço MAC de destino. Se o tráfego é legítimo, a seguir um precisaria de estabelecer porque os endereços MAC de destino não são sabidos ao interruptor.

Épossível detectar se a inundação está ocorrendo capturando um rastreamento de pacotes vistos em uma estação de trabalho durante o período de redução ou parada. Normalmente, pacotes unicast que não envolvem a estação de trabalho não devem ser vistos repetidamente na porta. Se isso estiver acontecendo, há probabilidade de estar ocorrendo inundação. Rastreamentos de pacotes podem ter uma aparência diferente quando existem várias causas de inundação.

Com o roteamento assimétrico, é provável que pacotes específicos para MAC Addresses não parem de se inundar mesmo após a resposta do destino. Com TCNs, a inundação incluirá muitos endereços diferentes, mas deve parar e, em seguida, reiniciar.

Com o excesso da camada de encaminhamento da L2, provavelmente você observará algum tipo de inundação com roteamento assimétrico. A diferença é que haverá provavelmente uma grande quantidade de pacotes estranhos ou pacotes normais em quantidade anormal com um endereço MAC de origem diferente.

Informações Relacionadas

- Suporte ao Produto - Switches
- Suporte de tecnologia de switching de LAN
- Suporte Técnico - Cisco Systems