# Inundação de Unicast em Redes de Campus Comutadas

## Contents



## Introduction

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

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

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

### Conventions

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

## Definição do problema

Os Switches de LAN usam tabelas de encaminhamento (tabelas Camada 2 (L2), tabelas CAM (Content Addressable Memory) para direcionar o tráfego em portas específicas com base no número do VLAN e no endereço MAC de destino da estrutura. 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.

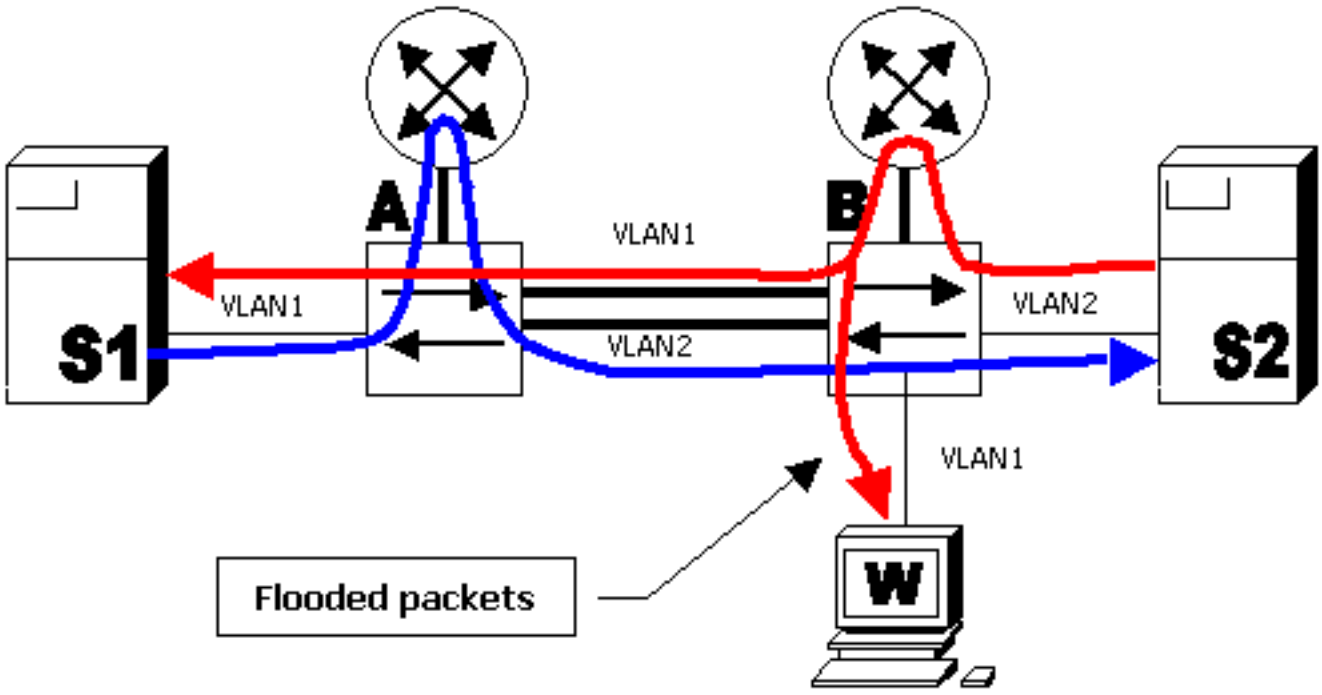
Note that most modern Switches including the Catalyst 2900 XL, 3500 XL, 2940, 2950, 2970, 3550, 3750, 4500/4000, 5000, and 6500/6000 series Switches maintain L2 forwarding tables per VLAN.

# Causas de inundação

A própria causa da inundação é que o endereço MAC de destino do pacote não está na tabela de encaminhamento L2 do switch. Nesse caso, o pacote será inundado de todas as portas de encaminhamento em sua VLAN (exceto a porta em que foi recebido). Os estudos de caso a seguir mostram as razões mais comuns para o endereço MAC de destino não ser conhecido pelo switch.

## 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 servidor S1 no VLAN 1 está executando o backup (transferência de dados de grande escala) para o servidor S2 no VLAN 2. O servidor S1 tem seu gateway padrão apontando para a interface VLAN 1 do roteador A. O servidor S2 tem seu gateway padrão apontando para a interface VLAN 2 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 para VLAN 1—S1 (linha vermelha)

Observe que, com tal disposição, o Switch A não visualizará tráfego do endereço MAC S2 na VLAN 2 (porque o endereço MAC de origem será gravado novamente pelo roteador B, e o pacote chegará apenas na VLAN 1). Isso significa que toda vez que o switch A precisar enviar o pacote para o endereço MAC do S2, o pacote será inundado para a VLAN 2. A mesma situação ocorrerá com o endereço MAC do S1 no switch B.

Esse comportamento é chamado de 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

Voltando ao exemplo acima, o resultado é que os pacotes de transferência de dados entre S1 e S2 serão inundados principalmente para a VLAN 2 no switch A e para a VLAN 1 no switch B. Isso significa que cada porta conectada (estação de trabalho W neste exemplo) na VLAN 1 no switch B receberá todos os pacotes de conversação entre S1 e S2. Suponha que o backup do servidor ocupe 50 Mbps da largura de banda. Essa quantidade de tráfego saturará os links de 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 esse pacote na VLAN 1 e o Switch B receberá e identificará o endereço MAC do S1. Como o switch não está recebendo tráfego constantemente, essa entrada de encaminhamento eventualmente envelhecerá e a inundação continuará. O mesmo processo se aplica 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)

Geralmente, o método é definir o timeout ARP do roteador e o tempo de envelhecimento da tabela de encaminhamento dos Switches com valores próximos. Isso fará com que os pacotes ARP sejam transmitidos. A liberação deve ocorrer antes que a entrada da tabela de encaminhamento L2 expire.

Um cenário típico em que esse tipo de problema pode ser observado é quando há switches redundantes de Camada 3 (L3) (como um Catalyst 6000 com MSFC (Multilayer Switch Feature Card) configurados para balanceamento de carga com HSRP (Hot Standby Router Protocol). Nesse caso, um Switch estará ativo para VLANs pares e outro para VLANs 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 é projetado para corrigir tabelas de

encaminhamento após a alteração da topologia de encaminhamento. Isso é necessário para evitar uma interrupção de conectividade, pois após uma alteração de topologia alguns destinos anteriormente acessíveis através de portas específicas podem se tornar acessíveis através de 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. Os Switches estarão constantemente executando rapidamente as tabelas de encaminhamento, portanto a inundação será quase constante.

Normalmente, um TCN é raro em uma rede bem configurada. Quando a porta de um Switch é ativada e desativada, pode haver um TCN, uma vez que o estado STP da porta está sendo alterado em relação ao encaminhamento. Quando a porta está oscilando, ocorrem TCNs repetitivos e inundação.

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. Consulte este documento para obter mais informações sobre TCNs:

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

**Observação:** no MSFC IOS, há uma otimização que ativará as interfaces VLAN para repovoar suas tabelas ARP quando houver um TCN na respectiva VLAN. 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

Outra causa possível de inundação é o excesso da tabela de encaminhamento do Switch. 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. This is possible but rare, since most modern Switches have large enough forwarding tables to accommodate MAC addresses for most designs.

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. Isso vinculará todos os recursos da tabela de encaminhamento. Quando as tabelas de encaminhamento ficarem saturadas, outro tráfego será inundados porque não é possível ocorrer nova aprendizagem. This kind of attack can be detected by examining the Switch forwarding table. A maioria dos endereços MAC apontará para a mesma porta ou grupo de portas. Esses ataques podem ser evitados limitando o número de endereços MAC aprendidos em portas não confiáveis usando o recurso de segurança de porta.

Os Guias de Configuração para Catalyst Switches com Cisco IOS® ou CatOS Software têm uma seção chamada Configuração de Segurança de Porta ou Configuração de Controle de Tráfego Baseado em Porta. Consulte a Documentação Técnica do seu switch nas páginas de produtos Cisco Switches para obter mais informações.

**Observação:** se a inundação unicast ocorrer em uma porta de switch configurada para Segurança de porta com a condição de "Restringir" para deter a inundação, uma violação de segurança será acionada.

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

**Observação:** quando ocorre tal violação de segurança, as portas afetadas configuradas para o modo "restringir" devem descartar pacotes com endereços de origem desconhecidos até que você remova um número suficiente de endereços MAC seguros para cair abaixo do valor máximo. Isso faz com que o contador SecurityViolation aumente.

**Observação:** em vez desse comportamento, se a porta do switch se mover para o estado "Desligar", você precisará configurar `Router(config-if)#switchport block unicast` para que a porta do switch específica seja desabilitada para inundação unicast.

# Como detectar a inundação excessiva

Most Switches implement no special command to detect flooding. Os Catalyst 6500/6000 Supervisor Engine 2 e os switches da série superior executando o software Cisco IOS System (Native) versão 12.1(14)E e versões superiores ou o software do sistema Cisco CatOS versão 7.5 ou superior implementam o recurso de **proteção contra inundação unicast**. Resumindo, esse recurso permite que o switch monitore a quantidade de inundação de unicast por VLAN e tome a ação especificada se a inundação exceder a quantidade especificada. As ações podem ser syslog, limit ou shutdown VLAN - o syslog é o mais útil para a detecção de inundação. Quando a inundação exceder a taxa configurada e a ação configurada for syslog, uma mensagem semelhante à seguinte será impressa:

```
%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 endereço MAC indicado é o MAC de origem do qual os pacotes são inundados nesse switch. É frequentemente necessário saber os endereços MAC de destino para os quais o switch está inundando (porque o switch está encaminhando observando o endereço MAC de destino). O Cisco IOS (Nativo) versões 12.1(20)E para o mecanismo supervisor Catalyst 6500/6000 2 e outros implementará a capacidade de exibir os endereços MAC aos quais 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
```

Uma investigação mais detalhada pode ser realizada para ver se o endereço MAC 0000.2222.0000 deve estar enviando tráfego para os endereços MAC listados na seção de endereço MAC de destino. Se o tráfego for legítimo, então será necessário estabelecer por que os endereços MAC de destino não são conhecidos pelo switch.

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