Unicast overstromingen in Switched Campus Networks

Inhoud

Inleiding

In dit document worden mogelijke oorzaken en implicaties van overstroming van pakketten in geschakelde netwerken besproken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Probleemdefinitie

LAN-switches gebruiken verzendtabellen (Layer 2 (L2) tabellen, Content Adresseerbare Geheugen (CAM) tabellen) om verkeer naar specifieke poorten te richten, gebaseerd op het VLAN-nummer en het doeladres van het frame. Wanneer er geen ingang is die aan het doel van MAC van het kader overeenkomt in het inkomende VLAN, zal het (unicast) kader naar alle verzendende poorten binnen het respectieve VLAN worden verzonden, wat overstromingen

veroorzaakt.

Beperkte overstromingen maken deel uit van het normale switchproces. Er zijn echter situaties waarin een voortdurende overstroming schadelijke effecten op het netwerk kan hebben. In dit document wordt uitgelegd welke problemen overstromingen kunnen veroorzaken, en welke de meest voorkomende redenen zijn dat bepaalde bezoekers voortdurend overstromen.

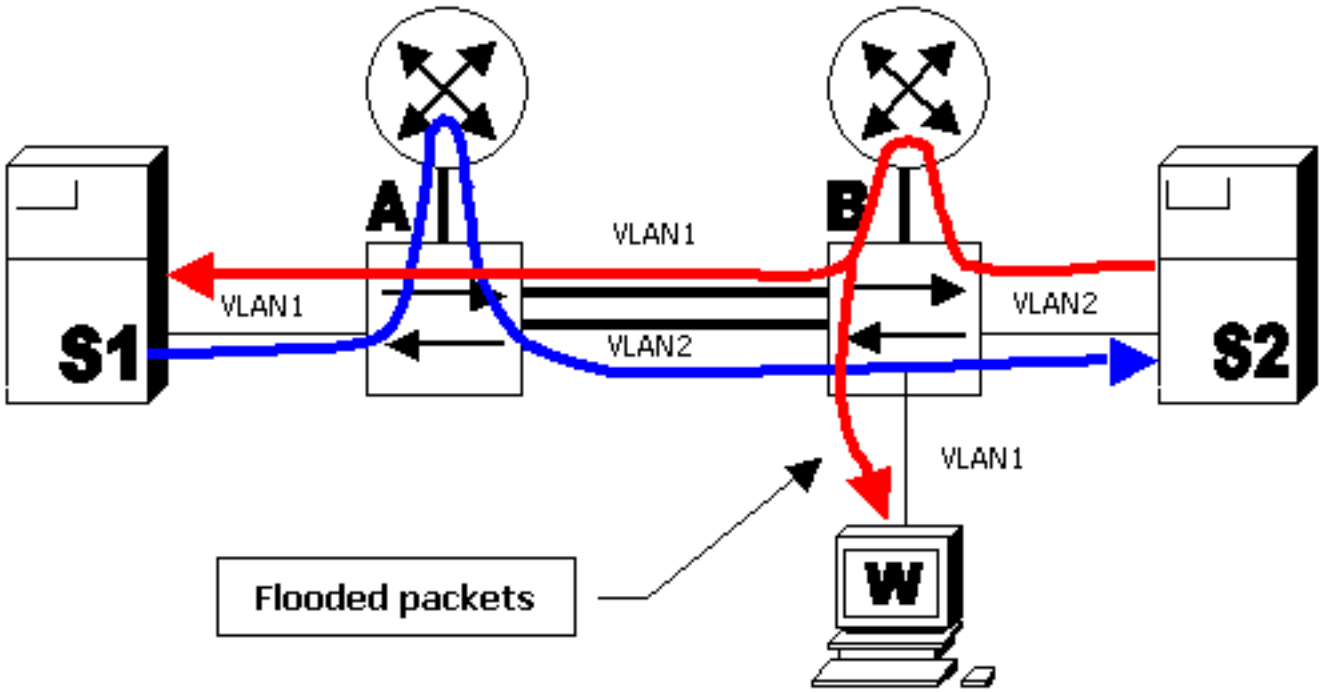
Merk op dat de meeste moderne switches waaronder Catalyst 2900 XL, 3500 XL, 2940, 2950, 2970, 3550, 3750, 4500/4000, 5000 en 6500 1600/6000 Series-switches houden L2-verzendtabellen per VLAN bij.

Oorzaken van overstromingen

De oorzaak van overstroming is dat het doel-MAC-adres van het pakket niet in de L2-verzendtabel van de switch is. In dit geval zal het pakket uit alle verzendende poorten in zijn VLAN worden overstroomd (behalve de poort waarop het is ontvangen). Hieronder staan casestudy's die de meeste gebruikelijke redenen voor het MAC-adres van de bestemming hebben en die niet bekend zijn met de switch.

Oorzaak 1: Asymmetric routing

Grote hoeveelheden overstroomd verkeer kunnen lage bandbreedte-links verzachten die problemen met netwerkprestaties veroorzaken of een volledige aansluitingsachterstand op apparaten die over dergelijke lage bandbreedte-links zijn verbonden. Bekijk het volgende schema:



In het bovenstaande diagram voert server S1 in VLAN 1 back-up (bulkgegevensoverdracht) naar server S2 in VLAN 2 uit. Server S1 heeft zijn standaardgateway naar router A's VLAN 1 interface. Server S2 heeft zijn standaardgateway gericht aan VLAN 2 van router B. Pakketten van S1 tot S2 volgen dit pad:

- S1-VLAN 1-schakelaar A-router A-VLAN 2-schakelaar B-VLAN 2-S2 (blauwe lijn)

Packets van S2 naar S1 gaan het volgende pad in:

- S2-VLAN 2-schakelaar B-router B-VLAN 1-schakelaar A-overstroomd naar VLAN 1-S1 (rode lijn)

Let op dat met zo een overeenkomst, schakelaar A geen "zie" verkeer van het S2 MAC-adres in VLAN 2 (aangezien het bron-MAC-adres door router B zal worden herschreven en het pakket alleen in VLAN 1 zal arriveren). Dit betekent dat elke keer dat schakelaar A het pakket naar het S2 MAC-adres moet verzenden, het pakket overstroomd zal worden naar VLAN 2. Dezelfde situatie zal voorkomen met het S1 MAC-adres op schakelaar B.

Dit gedrag wordt asymmetrische routing genoemd. Pakketten volgen verschillende paden, afhankelijk van de richting. Asymmetrische routing is een van de twee meest voorkomende oorzaken van overstromingen.

Gevolgen van overstroming in de ramp

Teruggrijpend op het bovenstaande voorbeeld, is het resultaat dat pakketten van de gegevensoverdracht tussen S1 en S2 meestal overstroomd zullen worden naar VLAN 2 op switch A en naar VLAN 1 op switch B. Dit betekent elke aangesloten poort (werkstation W in dit voorbeeld) in VLAN 1 op switch B alle gesprekspakketten tussen S1 en S2 zal ontvangen. Stel dat de back-up van de server 50 Mbps van bandbreedte vergt. Deze hoeveelheid verkeer zal 10 Mbps verbindingen verzadigen. Dit zal een complete aansluitingsachterstand op de PC's veroorzaken of deze aanzienlijk vertragen.

Deze overstroming is te wijten aan asymmetrische routing en kan stoppen wanneer server S1 een uitzendingspakket versturen (bijvoorbeeld Adreventie Protocol (ARP)). Switch A zal dit pakket overspoelen naar VLAN 1 en switch B zal het MAC-adres van S1 ontvangen en leren. Aangezien de switch geen verkeer constant ontvangt, zal deze verzendingsingang uiteindelijk verouderd worden en zullen de overstromingen hervat worden. Hetzelfde proces geldt voor S2.

Er zijn verschillende benaderingen om de overstromingen te beperken veroorzaakt door asymmetrische routing. Raadpleeg deze documenten voor meer informatie:

- Asymmetrische routing met Bridge Group op Catalyst 2948G-L3 en 4908G-L3-switches
- Asymmetrische routing en HSRP (buitensporige overstromingen van Unicast-verkeer in netwerk met routers die HSRP uitvoeren)

De benadering is normaal om de ARP timeout van de router en de door te sturen tijd van de switches dicht bij elkaar te brengen. Dit zal veroorzaken dat de ARP pakketten worden uitgezonden. Relearning moet plaatsvinden voordat de L2-verzendingstabel uit de tabel komt.

Een typisch scenario waar dit soort kwestie geobserveerd zou kunnen worden is wanneer er overtollige Layer 3 (L3) switches (zoals een Catalyst 6000 met Multilayer Switch functiekaart (MSFC)) zijn geconfigureerd om in balans te zijn met Hot Standby Router Protocol (HSRP). In dit geval, zal één switch actief zijn voor zelfs VLAN's en de andere actief voor oneven VLAN's.

Oorzaak 2: Wijzigingen in Spanning-Tree Protocol

Een ander veelvoorkomend probleem dat door overstromingen wordt veroorzaakt, is Spanning-Tree Protocol (STP) meldingen over wijziging van topologie (TCN). TCN is ontworpen om verzendingstabellen te corrigeren nadat de verzendende topologie is gewijzigd. Dit is nodig om een aansluitingsbreuk te vermijden, aangezien na een topologie sommige bestemmingen die eerder toegankelijk waren via bepaalde havens toegankelijk zouden kunnen worden via

verschillende havens. De TCN werkt door de verouderingstijd van de tabel te verkorten, zodat, indien het adres niet wordt vrijgegeven, deze veroudert en er overstromingen zullen plaatsvinden.

TCN's worden geactiveerd door een poort die overschakelt naar of van de verzendende staat. Na de GN, zelfs als het specifieke MAC-adres van de bestemming is verouderd, zou er in de meeste gevallen geen overstroming moeten plaatsvinden, aangezien het adres zal worden vrijgegeven. De kwestie zou zich kunnen voordoen wanneer TCN's met korte tussenpozen herhaaldelijk worden toegepast. De veranderingen zullen constant snel verouderd zijn hun verrijkingstafels zodat de overstroming bijna constant zal zijn.

Normaal gesproken is een TCN zeldzaam in een goed geconfigureerd netwerk. Wanneer de haven op een schakelaar omhoog of omlaag gaat is er uiteindelijk een TCN wanneer de staat van de haven in of van het vervoer verandert. Wanneer de haven vlakt, komen er repetitieve TCN's en overstromingen voor.

Poorten met de STP portfast optie zullen geen GNs veroorzaken wanneer het gaan naar of van de verzendstaat. De configuratie van portfast op alle eindapparaten poorten (zoals printers, PC's, servers, enz.) zou de TCN's tot een lage hoeveelheid moeten beperken. Raadpleeg dit document voor meer informatie over GN's:

- Understanding Spanning-Tree Protocol Topology Changes (Inzicht in wijzigingen in topologie van Spanning Tree Protocol)

Opmerking: In MSFC IOS is er een optimalisatie die VLAN-interfaces zal activeren om hun ARP-tabellen te herbevolken wanneer er een TCN in het betreffende VLAN is. Dit beperkt overstromingen in het geval van GN's, aangezien er een ARP-uitzending zal zijn en het MAC-adres van de host wordt vrijgegeven als de hosts antwoord op ARP.

Oorzaak 3: Overflow doorsturen

Een andere mogelijke oorzaak van overstroming kan overflow van de switch die tabel wordt verzonden zijn. In dit geval, kunnen de nieuwe adressen niet worden geleerd en de pakketten die aan dergelijke adressen worden gedoopt worden overstroomd tot enige ruimte in de het door:sturen tabel beschikbaar wordt. Nieuwe adressen zullen dan worden geleerd. Dit is mogelijk maar zeldzaam, aangezien de meeste moderne switches grote genoeg verzendtabellen hebben om MAC-adressen voor de meeste ontwerpen aan te passen.

Het doorsturen van de tabeluitputting kan ook door een aanval op het netwerk worden veroorzaakt waar één host begint met het genereren van frames die elke bron met een ander MAC-adres hebben. Hierdoor zullen alle verzendingstabelmiddelen worden gebonden. Zodra de verzendtabellen verzadigd zijn, zal er ander verkeer overstroomd raken omdat er geen nieuw leren kan plaatsvinden. Dit soort aanval kan worden gedetecteerd door de switch-expedentiatietabel te onderzoeken. Het merendeel van de MAC-adressen wijst naar dezelfde poort of groep poorten. Zulke aanvallen kunnen worden voorkomen door het aantal MAC-adressen te beperken dat op onvertrouwde poorten is geleerd door gebruik te maken van de havenveiligheidsfunctie.

Configuratiehandleidingen voor Catalyst-switches die Cisco IOS® of CatOS-software gebruiken, hebben een sectie genaamd Poortbeveiliging configureren of poortgebaseerde verkeerscontrole configureren. Raadpleeg de Technische documentatie voor uw schakelaar op de productpagina's van Cisco-switches voor meer informatie.

Opmerking: Als er een overstroming van eenmalig water optreedt in een switchpoort die is

ingesteld voor Port Security met de voorwaarde "Beperken" om de overstroming te arresteren, is er een overwinning voor de beveiliging.

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

Opmerking: Als zo'n schending van de beveiliging optreedt, moeten de getroffen poorten die zijn geconfigureerd voor "beperken"-modus pakketten met onbekende bronadressen laten vallen totdat u een voldoende aantal beveiligde MAC-adressen verwijdert om onder de maximale waarde te vallen. Dit veroorzaakt de SecurityViolation teller van de toename.

Opmerking: In plaats van dit gedrag, als de switchpoort zich naar "Shutdown" status beweegt, dan moet u `Router (configuratie-als) #`Switch`-blokkeerunicast` configureren zodat de specifieke switchpoort wordt uitgeschakeld voor overstroming op het net.

Hoe te veel overstromingen worden gedetecteerd

De meeste switches voeren geen speciale opdracht uit om overstromingen te detecteren. Catalyst 6500/6000 Supervisor Engine 2 en hogere Series switches met Cisco IOS-systeemsoftware (Native) versie 12.1(14)E en hoger of Cisco CatOS systeemsoftwareversie 7.5 of hoger implementeert '**unicast flood protection**'-functie. In het kort, deze functie staat de schakelaar toe om de hoeveelheid unicast overstroming per VLAN te controleren en gespecificeerde actie te ondernemen als de overstroming bepaalde hoeveelheid overschrijdt. Handelingen kunnen zijn om VLAN te syslog, beperken of af te sluiten - de slang is het meest handig voor het detecteren van overstromingen. Wanneer het overspoelen hoger is dan de ingestelde snelheid en de ingestelde actie syslog is, wordt een bericht zoals het volgende afgedrukt:

```
%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
```

Het aangegeven MAC-adres is de bron-MAC waarvan de pakketten op deze schakelaar zijn overstroomd. Het is vaak nodig om de bestemming MAC adressen te kennen waaraan de schakelaar overstroomt (omdat de schakelaar door het doel MAC adres te bekijken). Cisco IOS (Native) versies 12.1(20)E voor Catalyst 6500/6000 Supervisor Engine 2 en on zal mogelijkheid implementeren om de MAC-adressen weer te geven waar overstromingen plaatsvinden:

```
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
```

Vervolgens kan verder onderzoek worden verricht om na te gaan of MAC-adres 000.2222.0000 geacht wordt verkeer naar de MAC-adressen te verzenden die zijn opgenomen in de MAC-adressectie van het doel. Als verkeer legitiem is, zou men moeten vaststellen waarom de adressen van bestemming MAC niet aan de schakelaar bekend zijn.

U kunt zien of er overstromingen plaatsvinden door tijdens de groeivertraging of de stroomonderbreking een aantal pakketten in te voeren die op een werkstation zijn gezien. Normaal gesproken moeten eenastpakketten waarin het werkstation niet is meegeleverd, niet herhaaldelijk in de haven worden gezien. Als dit gebeurt, zijn er kans dat er overstromingen plaatsvinden. Packet-sporen kunnen er anders uitzien wanneer er verschillende oorzaken van overstroming zijn.

Met asymmetrische routing zijn er waarschijnlijk pakketten naar een specifiek MAC-adres die niet stoppen met overstromen, zelfs na de doelantwoorden. Met GN's zal de overstroming veel verschillende adressen omvatten, maar uiteindelijk zou ze moeten stoppen en dan opnieuw beginnen.

Met L2 het door:sturen van een tabel overflow, zult u waarschijnlijk hetzelfde soort overstroming zien zoals met asymmetrische routing. Het verschil is dat er waarschijnlijk een hoge hoeveelheid vreemde pakketten zijn, of normale pakketten in abnormale hoeveelheden met een ander bron-MAC-adres.

Gerelateerde informatie

- Productondersteuning voor switches
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning - Cisco-systemen