Inondazioni unicast nelle reti a campus commutati

Sommario

Introduzione

In questo documento vengono descritte le possibili cause e implicazioni del flooding di pacchetti unicast nelle reti a commutazione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Descrizione del problema

Gli switch LAN utilizzano tabelle di inoltro (tabelle di layer 2 (L2), tabelle CAM (Content Addressable Memory) per indirizzare il traffico a porte specifiche in base al numero VLAN e all'indirizzo MAC di destinazione del frame. Quando non vi è alcuna voce corrispondente all'indirizzo MAC di destinazione del frame nella VLAN in arrivo, il frame (unicast) viene inviato a

tutte le porte di inoltro all'interno della VLAN corrispondente, causando un flooding.

Un allagamento limitato fa parte del normale processo di commutazione. Esistono tuttavia situazioni in cui un allagamento continuo può causare effetti negativi sulle prestazioni della rete. Questo documento spiega quali problemi possono sorgere a causa delle inondazioni, e le ragioni più comuni per cui certi traffici potrebbero essere costantemente inondati.

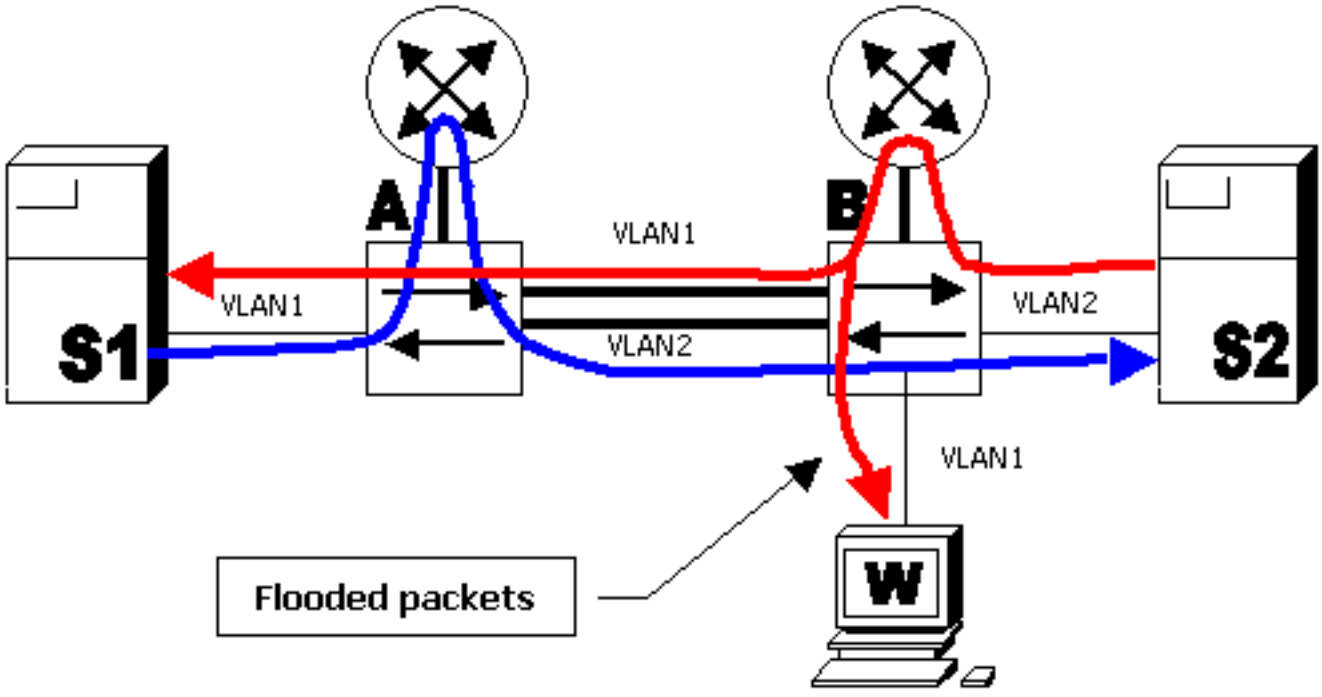
La maggior parte degli switch moderni, inclusi gli switch Catalyst serie 2900 XL, 3500 XL, 2940, 2950, 2970, 3550, 3750, 4500/4000, 5000 e 6500/6000, conserva tabelle di inoltro L2 per VLAN.

Cause delle inondazioni

La causa vera e propria del problema è che l'indirizzo MAC di destinazione del pacchetto non è presente nella tabella di inoltro L2 dello switch. In questo caso, il pacchetto verrà scaricato da tutte le porte di inoltro della VLAN (ad eccezione della porta su cui è stato ricevuto). Di seguito vengono riportati i motivi più comuni per cui l'indirizzo MAC di destinazione non è noto allo switch.

Causa 1: Routing asimmetrico

Grandi quantità di traffico alluvionato potrebbero saturare i collegamenti a bassa larghezza di banda causando problemi di prestazioni della rete o interruzioni complete della connettività ai dispositivi connessi tramite tali collegamenti a bassa larghezza di banda. Si consideri il diagramma seguente:



Nel diagramma precedente, sul server S1 della VLAN 1 è in esecuzione il backup (trasferimento di dati in blocco) sul server S2 della VLAN 2. Il gateway predefinito del server S1 fa riferimento all'interfaccia VLAN 1 del router A. Il server S2 ha il gateway predefinito che punta all'interfaccia VLAN 2 del router B. I pacchetti da S1 a S2 seguiranno questo percorso:

- S1—VLAN 1—switch A—router A—VLAN 2—switch B—VLAN 2—S2 (linea blu)

I pacchetti da S2 a S1 seguono il seguente percorso:

- S2—VLAN 2—switch B—router B—VLAN 1—switch A—allagato alla VLAN 1—S1 (linea rossa)

Tenere presente che con una tale disposizione, lo switch A non "vede" il traffico proveniente dall'indirizzo MAC S2 nella VLAN 2 (poiché l'indirizzo MAC di origine verrà riscritto dal router B e il pacchetto arriverà solo nella VLAN 1). Ciò significa che ogni volta che lo switch A deve inviare il pacchetto all'indirizzo MAC S2, il pacchetto verrà inondato alla VLAN 2. La stessa situazione si verificherà con l'indirizzo MAC S1 sullo switch B.

Questo comportamento è noto come routing asimmetrico. I pacchetti seguono percorsi diversi a seconda della direzione. Il routing asimmetrico è una delle due cause più comuni delle inondazioni.

Impatto delle inondazioni unicast

Tornando all'esempio precedente, il risultato è che i pacchetti del trasferimento di dati tra S1 e S2 verranno per la maggior parte trasmessi alla VLAN 2 sullo switch A e alla VLAN 1 sullo switch B. Ciò significa che ogni porta connessa (la workstation W in questo esempio) nella VLAN 1 sullo switch B riceverà tutti i pacchetti della conversazione tra S1 e S2. Si supponga che il backup del server richieda 50 Mbps di larghezza di banda. Questa quantità di traffico saturerà i collegamenti a 10 Mbps. Ciò causerà un'interruzione completa della connettività ai PC o li rallenterà notevolmente.

Questo flooding è dovuto al routing asimmetrico e può interrompersi quando il server S1 invia un pacchetto di trasmissione (ad esempio, Address Resolution Protocol (ARP)). Lo switch A invia il pacchetto alla VLAN 1 e lo switch B riceve e conosce l'indirizzo MAC di S1. Poiché lo switch non riceve costantemente il traffico, questa voce di inoltro alla fine scadrà e l'inondazione riprenderà. Lo stesso processo si applica a S2.

Ci sono diversi approcci per limitare le inondazioni causate dal routing asimmetrico. Per ulteriori informazioni, fare riferimento a questi documenti:

- Routing asimmetrico con gruppi di bridge sugli switch Catalyst 2948G-L3 e 4908G-L3
- Routing asimmetrico e HSRP (sovraccarico del traffico unicast nella rete con router che eseguono HSRP)

In genere, l'approccio è quello di avvicinare il timeout ARP del router e il tempo di aging della tabella di inoltro degli switch. In questo modo, i pacchetti ARP verranno trasmessi. La riprogrammazione deve essere eseguita prima della scadenza della voce della tabella di inoltro L2.

Uno scenario tipico in cui questo tipo di problema può essere osservato è quando vi sono switch di layer 3 (L3) ridondanti (ad esempio, Catalyst 6000 con Multilayer Switch Feature Card (MSFC)) configurati per il bilanciamento del carico con il protocollo HSRP (Hot Standby Router Protocol). In questo caso, uno switch sarà attivo per le VLAN pari e l'altro sarà attivo per le VLAN dispari.

Causa 2: Modifiche alla topologia dello Spanning-Tree Protocol

Un altro problema comune causato dall'inondazione è la Notifica di modifica della topologia STP (Spanning-Tree Protocol). Il TCN è progettato per correggere le tabelle di inoltro dopo la modifica della topologia di inoltro. Ciò è necessario per evitare interruzioni della connettività, in quanto dopo una modifica della topologia alcune destinazioni precedentemente accessibili tramite porte particolari potrebbero diventare accessibili tramite porte diverse. Il TCN opera riducendo i tempi di aging della tabella di inoltro, in modo che se l'indirizzo non viene riguadagnato, si verificherà un

timeout e un allagamento.

I TCN vengono attivati da una porta in transizione da o verso lo stato di inoltro. Dopo il TCN, anche se l'indirizzo MAC di destinazione è scaduto, nella maggior parte dei casi l'inondazione non dovrebbe protrarsi a lungo poiché l'indirizzo verrà riguadagnato. Il problema potrebbe sorgere quando i cittadini di paesi terzi si verificano ripetutamente a intervalli brevi. Gli switch invecchieranno continuamente nelle loro tabelle di inoltro, quindi l'inondazione sarà quasi costante.

Normalmente, un TCN è raro in una rete ben configurata. Quando la porta di uno switch si solleva o si abbassa, alla fine si verifica un TCN quando lo stato STP della porta viene modificato in o da inoltro. Quando la porta sfalda, si verificano ripetitivi TCN e allagamenti.

Le porte con la funzione portfast STP abilitata non causano TCN quando si passa allo stato di inoltro o lo si rimuove. La configurazione di portfast su tutte le porte dei dispositivi finali (ad esempio stampanti, PC, server e così via) dovrebbe limitare i TCN a una quantità ridotta. Per ulteriori informazioni sui TCN, consultare il documento:

- Descrizione delle modifiche alla topologia nel protocollo SPT (Spanning Tree Protocol)

Nota: nell'MSFC IOS, è disponibile un'ottimizzazione che attiverà le interfacce VLAN per ripopolare le tabelle ARP quando è presente un TCN nella VLAN corrispondente. Ciò limita l'inondazione nel caso di TCN, in quanto ci sarà una trasmissione ARP e l'indirizzo MAC dell'host verrà riguadagnato quando gli host risponderanno ad ARP.

Causa 3: Overflow tabella di inoltro

Un'altra possibile causa di allagamento può essere l'overflow della tabella di inoltro dello switch. In questo caso, non è possibile apprendere nuovi indirizzi e i pacchetti destinati a tali indirizzi vengono trasmessi fino a quando non viene liberato spazio nella tabella di inoltro. Verranno quindi appresi nuovi indirizzi. Questo è possibile, ma raro, dal momento che la maggior parte degli switch moderni dispone di tabelle di inoltro abbastanza grandi da contenere gli indirizzi MAC per la maggior parte delle progettazioni.

L'esaurimento della tabella di inoltro può essere causato anche da un attacco alla rete in cui un host inizia a generare frame ciascuno originati con indirizzi MAC diversi. Tutte le risorse della tabella di inoltro verranno bloccate. Quando le tabelle di inoltro diventano sature, il traffico di altro tipo viene inondato perché non è possibile eseguire nuove attività di apprendimento. Questo tipo di attacco può essere rilevato esaminando la tabella di inoltro dello switch. La maggior parte degli indirizzi MAC fa riferimento alla stessa porta o allo stesso gruppo di porte. È possibile prevenire tali attacchi limitando il numero di indirizzi MAC appresi sulle porte non attendibili tramite la funzione di sicurezza delle porte.

Le guide alla configurazione per gli switch Catalyst con software Cisco IOS® o CatOS includono una sezione chiamata Configurazione della sicurezza delle porte o Configurazione del controllo del traffico basato sulle porte. Per ulteriori informazioni, consultare la documentazione tecnica dello switch nelle pagine dei prodotti Cisco Switch.

Nota: se in una porta dello switch configurata per la sicurezza delle porte con la condizione "Restrict" (Limita) si verifica un allagamento unicast, viene attivata una violazione della sicurezza.

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

Nota: quando si verifica una violazione di sicurezza di questo tipo, le porte interessate configurate per la modalità "limita" devono eliminare i pacchetti con indirizzi di origine sconosciuti finché non si rimuove un numero di indirizzi MAC sicuri sufficiente per scendere al di sotto del valore massimo. In questo modo il contatore SecurityViolation verrà incrementato.

Nota: al contrario, se la porta dello switch viene impostata sullo stato "Shutdown", è necessario configurare il `blocco unicast Router(config-if)#switchport in` modo che la porta dello switch in questione sia disabilitata per il flooding unicast.

Come rilevare le inondazioni eccessive

La maggior parte degli switch non implementa comandi speciali per rilevare le allagamenti. Gli switch Catalyst serie 6500/6000 Supervisor Engine 2 e superiori con software Cisco IOS (nativo) versione 12.1(14)E e successive o il software Cisco CatOS versione 7.5 o successive implementano la funzionalità di **'protezione da inondazioni unicast'**. In breve, questa funzione consente allo switch di monitorare la quantità di allagamento unicast per VLAN e di intraprendere un'azione specifica se l'allagamento supera la quantità specificata. Le azioni possono essere eseguite sul syslog, sul limite o sulla VLAN di arresto - il syslog è il più utile per il rilevamento delle inondazioni. Quando il flooding supera la velocità configurata e l'azione configurata è syslog, viene visualizzato un messaggio simile al seguente:

```
%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
```

L'indirizzo MAC indicato è l'indirizzo MAC di origine da cui i pacchetti vengono trasmessi sullo switch. Spesso è necessario conoscere gli indirizzi MAC di destinazione a cui lo switch sta inviando (perché lo switch sta inoltrando guardando l'indirizzo MAC di destinazione). Cisco IOS (Native) versioni 12.1(20)E per Catalyst 6500/6000 Supervisor Engine 2 e successivi implementerà la funzionalità di visualizzazione degli indirizzi MAC in cui si verifica il flooding:

```
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
```

Èquindi possibile eseguire ulteriori indagini per verificare se l'indirizzo MAC 0000.222.0000 deve inviare il traffico agli indirizzi MAC elencati nella sezione degli indirizzi MAC di destinazione. Se il traffico è legittimo, è necessario stabilire perché gli indirizzi MAC di destinazione non sono noti allo switch.

Èpossibile rilevare se si verifica un allagamento catturando una traccia dei pacchetti rilevati su una workstation durante il rallentamento o l'interruzione. In genere, i pacchetti unicast che non interessano la workstation non devono essere visualizzati ripetutamente sulla porta. Se questo sta accadendo, è probabile che ci siano inondazioni. Le tracce dei pacchetti possono avere un aspetto diverso quando vi sono diverse cause di inondazione.

Con il routing asimmetrico, è probabile che i pacchetti indirizzati a un indirizzo MAC specifico non terminino il flooding anche dopo la risposta della destinazione. Con i cittadini di paesi terzi, l'inondazione includerà molti indirizzi diversi, ma alla fine dovrebbe fermarsi e poi ripartire.

Con l'overflow della tabella di inoltro L2, è probabile che venga visualizzato lo stesso tipo di flooding di quello del routing asimmetrico. La differenza è che ci sarà probabilmente una grande quantità di pacchetti strani, o pacchetti normali in quantità anormali con un indirizzo MAC di origine diverso.

Informazioni correlate

- Switch - Supporto dei prodotti
- Supporto della tecnologia di switching LAN
- Supporto tecnico – Cisco Systems