交換式園區網中的單點傳播泛濫

目錄

簡介

本文討論交換網路中單點傳播封包泛濫的可能原因和影響。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題定義

LAN交換機使用轉發表(第2層(L2)表、內容可定址儲存器(CAM)表)根據幀的VLAN編號和目標MAC地址將流量定向到特定埠。當傳入VLAN中沒有與幀的目的MAC地址對應的條目時，（單播）幀將傳送到相應VLAN中的所有轉發埠，這會導致泛洪。

有限泛洪是正常交換過程的一部分。但是，有時連續泛洪會對網路效能造成負面影響。本檔案將說明洪災可能會引起哪些問題，以及某些流量可能會持續遭到洪災的最常見原因。

請注意，大多數現代交換器（包括Catalyst 2900 XL、3500 XL、2940、2950、2970、3550、

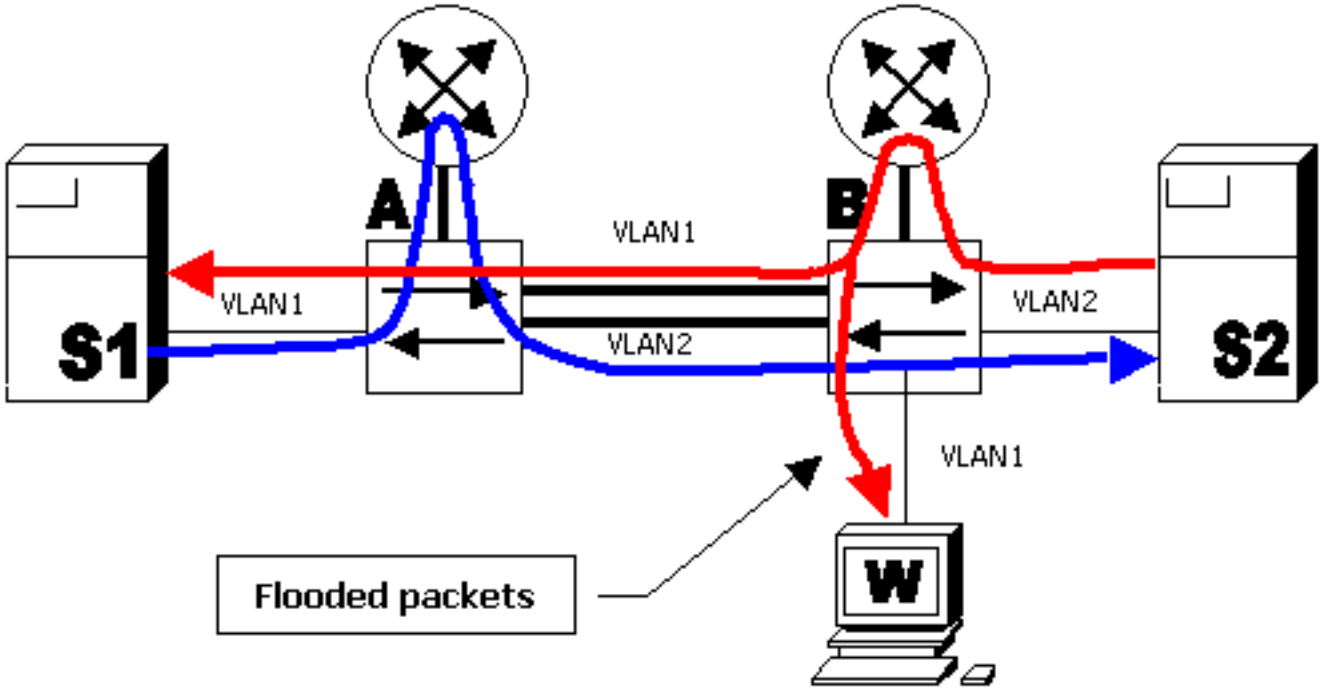
3750、4500/4000、5000和6500/6000系列交換器）會維持每個VLAN的L2轉送表。

泛濫的原因

泛洪的根本原因是資料包的目的MAC地址不在交換機的L2轉發表中。在這種情況下，封包將從其VLAN中的所有轉送連線埠上湧出（接收它的連線埠除外）。 下面的案例分析顯示了交換機不知道目的MAC地址的最常見原因。

原因1:非對稱路由

大量泛洪流量可能會使低頻寬鏈路飽和，從而導致網路效能問題或連線此類低頻寬鏈路的裝置完全連線中斷。請考慮以下圖表：



在上圖中，VLAN 1中的伺服器S1正在向VLAN 2中的伺服器S2運行備份（批次資料傳輸）。伺服器S1的預設網關指向路由器A的VLAN 1介面。伺服器S2的預設網關指向路由器B的VLAN 2介面。從S1到S2的資料包將遵循以下路徑：

- S1 - VLAN 1 — 交換機A — 路由器A - VLAN 2 — 交換機B - VLAN 2 - S2（藍線）

從S2到S1的資料包沿以下路徑傳輸：

- S2 — VLAN 2 — 交換機B — 路由器B — VLAN 1 — 交換機A — 泛洪到VLAN 1 — S1（紅線）

請注意，透過這種安排，交換器A不會「看到」來自VLAN 2中S2 MAC位址的流量（因為來源MAC位址將由路由器B重新寫入，而封包只會到達VLAN 1）。 這表示每次交換器A需要將封包傳送到S2 MAC位址時，封包都會湧向VLAN 2。交換器B上的S1 MAC位址也會發生相同的情況。

這種行為稱為非對稱路由。封包遵循不同的路徑（視方向而定）。非對稱路由是泛濫的兩個最常見原因之一。

單點傳播泛濫的影響

返回上例，結果是S1和S2之間資料傳輸的資料包大部分將泛洪到交換機A的VLAN 2和交換機B的

VLAN 1。這意味著交換機B的VLAN 1中的每個連線埠（本例中是工作站W）都將接收S1和S2之間的所有會話資料包。假設伺服器備份佔用50 Mbps的頻寬。此流量將使10 Mbps鏈路飽和。這將導致與PC的完全連線中斷或顯著降低連線速度。

此泛洪是由於非對稱路由引起的，並可能在伺服器S1傳送廣播資料包(例如地址解析協定(ARP))時停止。 交換機A會將此資料包泛洪到VLAN 1，交換機B將接收並獲知S1的MAC地址。由於交換機不會持續接收流量，因此此轉發條目最終會過期，並且泛洪將會繼續。同樣的過程也適用於S2。

有多種方法可以限制非對稱路由導致的泛洪。請參閱以下文件以瞭解更多資訊：

- Catalyst 2948G-L3和4908G-L3交換機上帶有網橋組的非對稱路由
- 非對稱路由和HSRP（運行HSRP的路由器在網路中泛洪過多單播流量）

通常的方法是使路由器的ARP超時和交換機的轉發表老化時間彼此接近。這將導致ARP資料包被廣播。重新學習必須在L2轉發表項過期之前進行。

可能會發生此類問題的典型場景是，存在配置為使用熱待命路由器協定(HSRP)進行負載均衡的冗餘第3層(L3)交換機(例如具有多層交換機功能卡(MSFC)的Catalyst 6000)。 在這種情況下，一台交換機對於偶數VLAN將處於活動狀態，另一台交換機對於奇數VLAN將處於活動狀態。

原因二：生成樹協定拓撲更改

泛洪引起的另一個常見問題是生成樹協定(STP)拓撲更改通知(TCN)。TCN設計用於在轉發拓撲更改後更正轉發表。這是避免連線中斷所必需的，因為拓撲更改後，以前可通過特定埠訪問的某些目標可能可通過不同的埠訪問。TCN的運行方式是縮短轉發表老化時間，以便如果不重新學習地址，地址將老化並發生泛洪。

TCN由轉換到轉發狀態或從轉發狀態轉換的埠觸發。在TCN之後，即使特定目的MAC地址已過期，由於將重新獲取地址，在大多數情況下也不會發生很長的泛洪。當TCN以短時間間隔重複發生時，可能會出現此問題。交換機將不斷快速老化其轉發表，因此泛洪幾乎會一直持續。

通常，在配置良好的網路中很少使用TCN。當交換器上的連線埠開啟或關閉時，一旦連線埠的STP狀態變為轉送或從轉送，最終就會有TCN。當連線埠擺動時，會發生重複的TCN和泛洪。

啟用STP portfast功能的埠在進入或離開轉發狀態時不會引起TCN。在所有終端裝置埠（如印表機、PC、伺服器等）上配置portfast應將TCN限制在低數量。如需有關TCN的詳細資訊，請參閱以下檔案：

- 瞭解擴充樹通訊協定拓撲變更

注意：在MSFC IOS中，當各個VLAN中有一個TCN時，會觸發VLAN介面重新填充其ARP表的最佳化。這樣可限制在TCN情況下的泛洪，因為將會出現ARP廣播，並且主機在回覆ARP時將重新獲取主機MAC地址。

原因三：轉發表溢位

泛洪的另一個可能原因是交換機轉發表溢位。在這種情況下，無法獲知新地址，而且發往這些地址的資料包會被泛洪，直到轉發表中有一些空間可用。然後會學習新的地址。這是有可能的，但非常罕見，因為大多數現代交換機都有足夠大的轉發表，能夠容納大多數設計中的MAC地址。

轉發表耗盡也可能是由於網路受到攻擊，一台主機開始生成每個來自不同MAC地址的幀。這將佔用所有轉發表資源。一旦轉發表飽和，其他流量將會泛洪，因為新的學習無法進行。通過檢查交換機轉發表可以檢測到此類攻擊。大多數MAC地址將指向同一埠或埠組。通過使用埠安全功能，可以限

制在不可信埠上學習的MAC地址數量，從而防止此類攻擊。

執行Cisco IOS®或CatOS軟體的Catalyst交換器的設定指南中有一個稱為設定連線埠安全或設定連線埠型流量控制的部分。如需詳細資訊，請參閱思科交換器產品頁面上您交換器的技術檔案。

註：如果為埠安全配置的交換機埠發生單播泛洪，且條件為「限制」以阻止泛洪，則會觸發安全違規。

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

註：發生此類安全違規時，配置為「restrict」模式的受影響埠應丟棄具有未知源地址的資料包，直到刪除足夠數量的安全MAC地址以丟棄低於最大值。這會導致SecurityViolation計數器增加。

註意：如果交換器連線埠移至「關閉」狀態，而不是此行為，則需要設定`Router(config-if)#switchport block unicast`

如何檢測過度泛洪

大多數交換器不實作特殊指令來偵測泛濫。執行Cisco IOS系統軟體（原生）版本12.1(14)E和更高版本或Cisco CatOS系統軟體版本7.5或更高版本的Catalyst 6500/6000 Supervisor Engine 2和更高系列交換器實作「**unicast flood protection**」功能。簡而言之，此功能允許交換器監控每個VLAN的單點傳播泛洪量，並在泛洪超過指定量時執行指定的動作。操作可以是syslog 、 limit或shutdown VLAN — 系統日誌對於泛洪檢測最有用。當泛洪超過配置的速率並且配置的操作為syslog時，將列印類似以下內容的消息：

```
%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
```

指示的MAC地址是此交換機上資料包泛洪的源MAC。通常需要知道交換機正在泛洪到的目的MAC地址（因為交換機通過檢視目的MAC地址進行轉發）。 適用於Catalyst 6500/6000 Supervisor engine 2及更高版本的Cisco IOS（原生）版本12.1(20)E將實作顯示發生泛洪的MAC位址的功能：

```
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
```

進一步調查後，可以檢視MAC地址0000.2222.0000是否應該將流量傳送到目標MAC地址部分列出的MAC地址。如果流量是合法的，則需要確定交換機不知道目的MAC地址的原因。

您可能會通過捕獲在速度減慢或中斷期間在工作站上看到的資料包跟蹤來檢測是否發生泛濫。通常，埠上不應重複出現不涉及工作站的單點傳播資料包。如果發生這種情況，可能會發生洪災。當出現各種泛洪原因時，資料包跟蹤可能看起來不同。

使用非對稱路由時，可能會有封包到達特定的MAC位址，且即使在目的地回覆之後也不會停止泛濫。使用TCN時，泛洪將包括許多不同地址，但最終應停止然後重新啟動。

使用L2轉發表溢位時，您可能會看到與非對稱路由相同的泛洪。不同之處在於，可能會有大量的異常資料包，或具有不同源MAC地址的正常資料包數量異常。

相關資訊

- 交換器產品支援
- LAN 交換技術支援
- 技術支援 - Cisco Systems