交换式园区网络中的单播泛洪

目录

简介

本文档讨论交换网络中单播数据包泛洪的可能的原因和影响。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题定义

依据VLAN号和帧的目的MAC地址，LAN交换机使用转发表（第2层表、内容可寻址存储器(CAM)表）可以将数据流直接传输到特定端口。当流入 VLAN 中的帧目标 MAC 地址没有条目响应时，（单播）帧将在各自的 VLAN 中被发送到所有转发端口，引起泛滥。

有限泛洪是正常交换过程的一部分。但是也会出现一些情况，持续泛滥可能在网络上对性能产生影响。本文说明了泛滥可能引起什么问题，以及某个数据流经常泛滥的最常见原因。

注意大多数现代交换机（包括 Catalyst 2900 XL、3500 XL、2940、2950、2970、3550、3750、

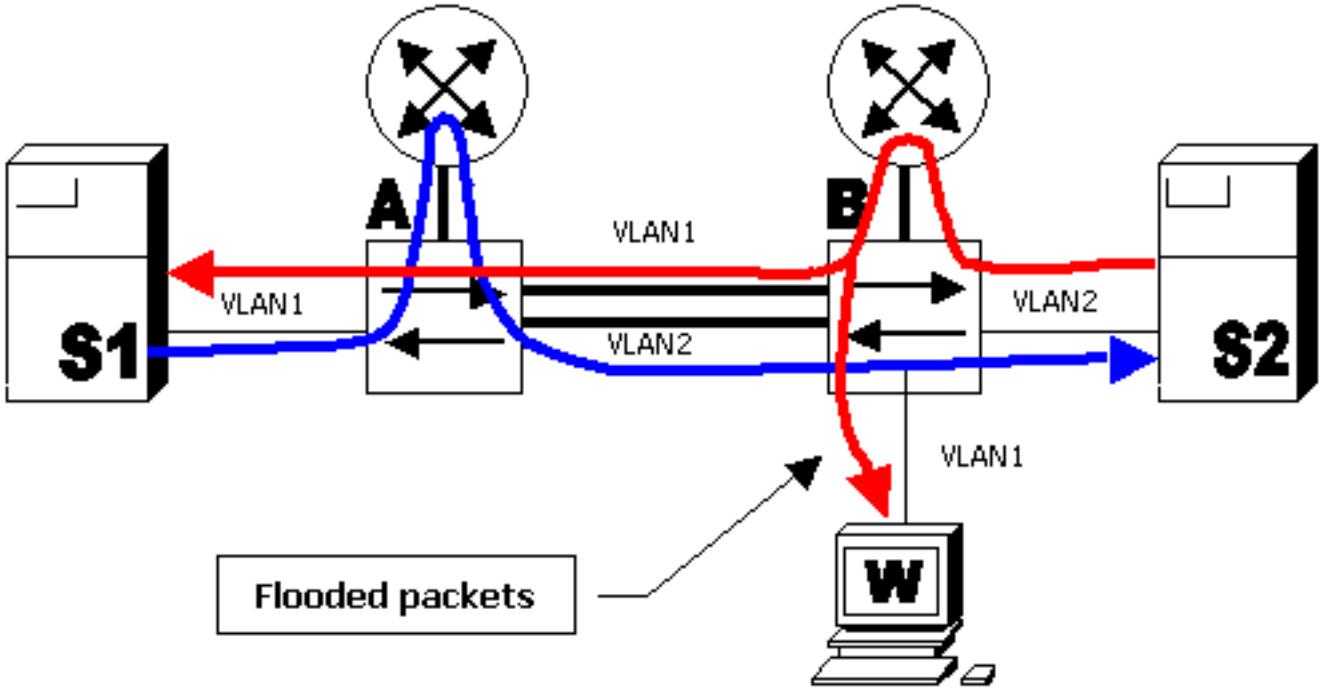
4500/4000、5000 和 6500/6000 系列交换机）能够维护每个 VLAN 的第 2 层转发表。

泛洪的原因

泛洪的原因正是数据包的目标 MAC 地址不在交换机的 L2 转发表中。在这种情况下，数据包将被充斥在 VLAN 的所有转发端口之外（除接收端口以外）。以下案例分析显示交换机未知目标 MAC 地址的常见原因。

原因 1：非对称路由

数据流大量泛滥，可能使连接到这种低带宽链路的设备出现导致网络性能问题或连接完全中断的低带宽链路饱和。请观察下图：



在上图中，VLAN 1 中的服务器 S1 正在运行备份（批量数据传输）到 VLAN 2 中的服务器 S2。服务器 S1 的默认网关指向路由器 A 的 VLAN 1 接口。服务器 S2 的默认网关指向路由器 B 的 VLAN 2 接口。从 S1 到 S2 的数据包将按以下路径传输：

- S1--VLAN 1交换机A--路由器 A--VLAN 2交换机B--VLAN 2--S2 (蓝线)

从 S2 到 S1 的数据包按以下路径传输：

- S2--VLAN 2交换机B--路由器 B--VLAN 1交换机A--充斥对VLAN 1--S1 (红线)

注意采用这种安排，交换机 A 不会看到 VLAN 2 的 S2 MAC 地址发出的数据流（因为源 MAC 地址将被路由器 B 重写，数据包只能到达 VLAN 1）。这意味着交换机 A 每次需要发送数据包到 S2 MAC 地址时，数据包将泛滥到 VLAN 2。对于交换机 B 上的 S1 MAC 地址，将发生相同的情况。

此行为称为非对称路由。数据包根据方向按不同路径传输。非对称路由是泛洪的两个最常见的原因之一。

单播泛洪的影响

返回以上示例，结果是 S1 和 S2 之间的数据传输数据包将主要泛洪到 交换机 A 上的 VLAN 2 和交

换机 B 上的 VLAN 1。这意味着交换机 B 上 VLAN 1 中的每个已连接端口（在本例中是工作站 W）将收到 S1 和 S2 之间对话的所有数据包。假定服务器备份占用 50 Mbps 的带宽。此数据流量将导致 10 Mbps 链路饱和。这将导致到 PC 的连接完全中断，或者使它们的连接速度明显降低。

此泛滥归结于不对称路由，当服务器S1发送广播包时(例如地址解析协议(ARP))，可能终止此泛滥。交换机 A 把此数据包充斥到 VLAN 1，而交换机B将收到和获取 S1 的 MAC 地址。由于交换机并非经常收到数据流，因此此转发条目最终会超龄，数据流溢出重新开始。相同的过程也适用于 S2。

有几种不同的方法可用于限制由非对称路由造成的泛洪。有关详细信息，请参阅以下文档：

- Catalyst 2948G-L3与4908G-L3交换机上使用网桥组的不对称路由
- 非对称路由和 HSRP（采用运行 HSRP 的路由器的网络中的单播流量过度泛洪）

此方法通常会导致路由器的 ARP 超时，交换机的转发表过期时间接近彼此。这将导致 ARP 数据包成为广播。必须在 L2 转发表条目过期之前进行重新获知。

通常情况是，配有冗余第3层(L3)交换机时(例如配有多层交换机功能卡(MSFC)的Catalyst 6000)，可以查看到这种问题。配置负载平衡与热备份路由协议(HSRP)。在这种情况下，一台交换机主要用于偶数 VLAN，另一台交换机主要用于奇数 VLAN。

原因 2：生成树协议拓扑发生变化

充斥导致的另一个常见问题是生成树协议拓扑变化通知(TCN)。TCN 设计用于在转发拓扑发生变化后更正转发表。该操作对于避免连接中断很有必要，因为拓扑更改以后，原来可以通过特定端口访问的某些目的地可能通过不同端口进行访问。TCN 的运行方式是缩短转发表过期时间，这样如果地址没有重新获取，TCN 会超龄，并发生泛滥。

TCN 由正在进入或离开转发状态的端口触发。在 TCN 以后，即使特定目的地 MAC 地址超龄，在大多情况下应当不会出现长时间泛滥，因为地址将重新被学习。当 TCN 以较短的间隔重复发生时，可能会出现此问题。交换机经常让它们的转发表快速过期，这样溢出现象也几乎经常发生。

通常情况下，配置良好的网络中极少出现 TCN。当交换机上的端口接通或断开时，一旦端口的 STP 状态转变为转发或非转发状态时，最终会有 TCN。当端口抖动时，会发生重复性 TCN 和泛洪。

支持 STP portfast 功能的端口转为/转出转发状态时，将不会导致 TCN。所有终端设备端口（例如打印机、PC、服务器等等）的 portfast 配置应当将 TCN 限制到一个低数值。有关 TCN 的更多信息，请参阅以下文档：

- 了解生成树协议拓扑变化

注意： 在 MSFC IOS 中，当各自的 VLAN 中配有 TCN 时，有一种优化机制会触发 VLAN 接口重新填充它们的 ARP 表。这将限制 TCN 的泛滥，当主机回复 ARP 时，将重新获取 ARP 广播和主机 MAC 地址。

原因 3：转发表溢出

泛洪的另一个可能的原因是交换机转发表溢出。在这种情况下，不能获取新地址，指定到新地址的数据包会泛滥，直到某些空间在转发表中变得可用。随后将获知新的地址。因为大多数现代交换机有足够大的转发表来容纳大多数设计的 MAC 地址，因此这种情况可能出现但很少见。

转发表耗尽也可能由网络攻击引起，其中一台主机开始生成生帧，每台主机配置带有不同的 MAC 地址。这将占用所有转发表资源。一旦转发表饱和，因为新了解不能发生，所以其他数据流将溢出。通过检查交换机转发表可以检测到这种攻击。大部分 MAC 地址将指向相同的端口或端口组。通

过使用端口安全功能，限制不可信端口上获取的 MAC 地址的数量，可以防止这样的攻击。

运行 Cisco IOS® 或 CATOS 软件的 Catalyst 交换机配置指南，包括名为“配置端口安全或配置基于端口的数据流控制”的部分。有关详细信息，请参阅 Cisco 交换机产品网页的交换机技术文档。

注意： 如果单播泛洪在为端口安全配置以情况“的交换机端口发生请限制”拘捕泛滥，安全侵害trigerred。

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

注意： 当这样安全侵害发生时，受影响的端口配置为“限制”模式应该丢弃数据包和未知源源点地址一起，直到您删除安全MAC地址足够的数目下降在最大值下面。与增量相反，这导致SecurityViolation。

注意： 而不是此行为，如果交换机端口移动向"shutdown"状态然后您需要配置`(config-if)#switchport`以便特定交换机端口为单播泛洪禁用。

如何检测过度泛洪

大部分交换机不执行特殊命令以检测泛洪。运行 Cisco IOS 系统软件（本地）12.1(14)E 版和更高版本或 Cisco CatOS 系统软件 7.5 版或更高版本的Catalyst 6500/6000 Supervisor 引擎 2 和更高系列的交换机实现了**“单播泛滥保护”**功能。简而言之，此功能允许交换机监控每个VLAN的单播泛泛洪数量，如果泛洪超出指定数量，交换机会采取相应的措施。操作可以记入 syslog，限制或关闭 VLAN — syslog 对于泛滥检测最有用。当泛滥超出配置速率并且配置的操作是 syslog 时，类似于以下的消息将被打印：

```
%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
```

所显示的 MAC 地址是这台交换机上溢出数据包的源 MAC。经常需要了解正在泛洪的交换机目地 MAC 地址（因为交换机的转发是通过查看目目的 MAC 地址）。用于 Catalyst 6500/6000 Supervisor 引擎 2 的 Cisco IOS (Native) 12.1(20)E 版能够显示泛滥发生指向的 MAC 地址：

```
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
```

然后执行进一步调查，查看 MAC 地址 0000.2222.0000 是否应该把数据流发送到目的 MAC 地址部分列出的MAC地址。如果数据流合法，您将需要了解交换机不知道目的 MAC 地址的原因。

通过在减速或中断时，从工作站上看到的数据包追踪，您可以检测到是否发生泛滥。通常情况下，端口不应重复出现与工作站无关的单播数据包。如果发生这种情况，则可能是出现了泛洪。存在多种泛洪原因时，数据包踪迹可能有所不同。

使用不对称路由，到特定 MAC 地址的数据包很可能停止泛滥，即使在目的地进行回复之后。使用 TCN，溢出将包括许多不同地址，但最终应该终止，然后重新启动。

使用第 2 层转发表溢出，您可能会发现与不对称路由相同类型的溢出。区别在于可能有大量的奇怪数据包，或者数量异常的正常数据包带有不同源 MAC 地址。

相关信息

- 交换机产品支持
- LAN 交换技术支持
- 技术支持 - Cisco Systems