Unicast Flooding in Switched Campus-Netzwerken

Inhalt

Einführung

In diesem Dokument werden mögliche Ursachen und Auswirkungen von Unicast-Paketflutungen in Switched-Netzwerken erläutert.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

Problemdefinition

LAN-Switches verwenden Forwarding-Tabellen (Layer 2 (L2)-Tabellen, Content Addressable Memory (CAM)-Tabellen), um Datenverkehr an bestimmte Ports basierend auf der VLAN-Nummer und der MAC-Zieladresse des Frames weiterzuleiten. Wenn im eingehenden VLAN kein Eintrag vorhanden ist, der der MAC-Zieladresse des Frames entspricht, wird der (Unicast-) Frame an alle

Weiterleitungsports innerhalb des entsprechenden VLAN gesendet, was eine Überflutung verursacht.

Eingeschränkte Überflutung ist Teil des normalen Switching-Prozesses. Es gibt jedoch Situationen, in denen eine ständige Überflutung das Netzwerk beeinträchtigen kann. In diesem Dokument wird erläutert, welche Probleme durch Überschwemmungen auftreten können. Außerdem werden die häufigsten Gründe erläutert, aus denen der Datenverkehr ständig überflutet werden kann.

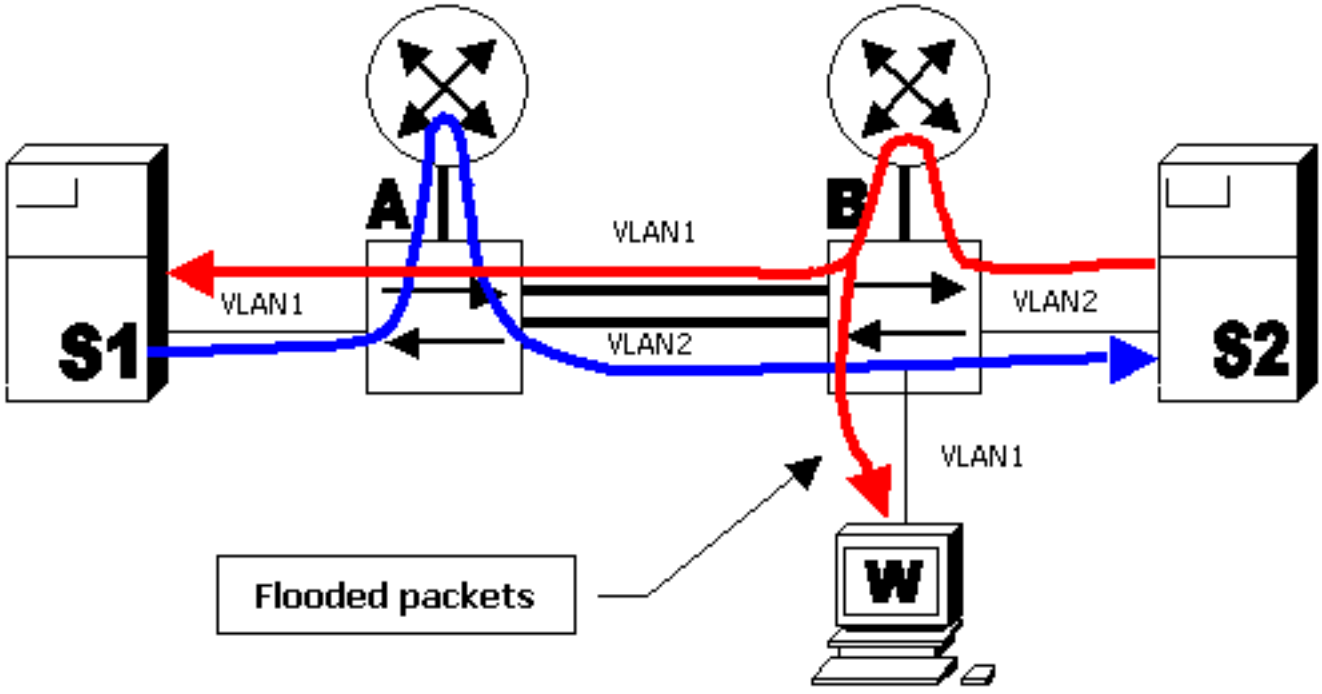
Beachten Sie, dass die meisten modernen Switches, einschließlich Catalyst 2900 XL, 3500 XL, 2940, 2950, 2970, 3550, 3750, 4500/4000, 500 und 6500 Switches der Serien 600/00 halten L2-Weiterleitungstabellen pro VLAN.

Hochwasserursachen

Die eigentliche Ursache für die Überflutung ist, dass sich die MAC-Zieladresse des Pakets nicht in der L2-Weiterleitungstabelle des Switches befindet. In diesem Fall wird das Paket von allen Weiterleitungsports im VLAN (mit Ausnahme des Ports, an dem es empfangen wurde) überflutet. Die folgenden Fallstudien zeigen die häufigsten Gründe dafür, dass die MAC-Zieladresse für den Switch nicht bekannt ist.

Ursache 1: Asymmetrisches Routing

Bei großen Mengen an Datenflut können Links mit niedriger Bandbreite zu Problemen bei der Netzwerkleistung führen oder die Verbindung zu Geräten, die über Links mit niedriger Bandbreite verbunden sind, komplett ausfallen. Betrachten Sie das folgende Diagramm:



Im obigen Diagramm wird auf dem Server S1 in VLAN 1 die Sicherung (Massenübertragung von Daten) zum Server S2 in VLAN 2 ausgeführt. Das Standard-Gateway des Servers S1 verweist auf die VLAN 1-Schnittstelle des Routers A. Das Standard-Gateway des Servers S2 verweist auf die VLAN 2-Schnittstelle des Routers B. Pakete von S1 bis S2 folgen diesem Pfad:

- S1 - VLAN 1 - Switch A - Router A - VLAN 2 - Switch B - VLAN 2 - S2 (blaue Leitung)

Pakete von S2 bis S1 folgen dem folgenden Pfad:

- S2 - VLAN 2 - Switch B - Router B - VLAN 1 - Switch A - überflutet in VLAN 1 - S1 (rote Leitung)

Beachten Sie, dass Switch A bei einer solchen Anordnung keinen Datenverkehr von der S2-MAC-Adresse in VLAN 2 "sieht" (da die Quell-MAC-Adresse von Router B umgeschrieben wird und das Paket nur in VLAN 1 eintrifft). Das bedeutet, dass jedes Mal, wenn Switch A das Paket an die MAC-Adresse S2 senden muss, das Paket an VLAN 2 geflutet wird. Die gleiche Situation tritt bei der S1-MAC-Adresse auf Switch B auf.

Dieses Verhalten wird als asymmetrisches Routing bezeichnet. Pakete folgen je nach Richtung unterschiedlichen Pfaden. Asymmetrisches Routing ist eine der beiden häufigsten Ursachen für Überschwemmungen.

Auswirkungen von Unicast Flooding

Um auf das obige Beispiel zurückzukommen, ist das Ergebnis, dass Pakete der Datenübertragung zwischen S1 und S2 größtenteils zu VLAN 2 auf Switch A und zu VLAN 1 auf Switch B geflutet werden. Dies bedeutet, dass jeder verbundene Port (Workstation W in diesem Beispiel) in VLAN 1 auf Switch B alle Datenpakete für die Kommunikation zwischen S1 und S2 empfängt. Angenommen, die Server-Datensicherung benötigt 50 Mbit/s Bandbreite. Dieser Datenverkehr überlastet 10-Mbit/s-Verbindungen. Dies führt zu einem kompletten Ausfall der Verbindungen zu den PCs oder zu einer erheblichen Verlangsamung dieser Verbindungen.

Diese Überflutung ist auf asymmetrisches Routing zurückzuführen und kann gestoppt werden, wenn der Server S1 ein Broadcast-Paket sendet (z. B. Address Resolution Protocol (ARP)). Switch A überflutet dieses Paket in VLAN 1, und Switch B empfängt und lernt die MAC-Adresse von S1. Da der Switch nicht ständig Datenverkehr empfängt, verfällt dieser Weiterleitungseintrag, und die Überflutung wird wieder aufgenommen. Das gleiche Verfahren gilt für S2.

Es gibt verschiedene Ansätze, um die Überflutung durch asymmetrisches Routing zu begrenzen. Weitere Informationen finden Sie in diesen Dokumenten:

- Asymmetrisches Routing mit Bridge-Gruppen auf Catalyst Switches der Serien 2948G-L3 und 4908G-L3
- Asymmetric Routing und HSRP (übermäßige Flooding des Unicast-Datenverkehrs im Netzwerk mit Routern, die HSRP ausführen)

Der Ansatz besteht in der Regel darin, die ARP-Timeout-Einstellung des Routers und die Weiterleitungstabelle-Alterungszeit der Switches einander nahe zu bringen. Dadurch werden die ARP-Pakete übertragen. Die Relevanz muss erfolgen, bevor die L2-Weiterleitungstabelle das Zeitlimit erreicht.

Ein typisches Szenario, in dem ein solches Problem auftreten kann, ist die Tatsache, dass es redundante Layer-3-Switches (z. B. Catalyst 6000 mit Multilayer Switch Feature Card (MSFC)) gibt, die für den Lastenausgleich mit Hot Standby Router Protocol (HSRP) konfiguriert sind. In diesem Fall ist ein Switch für selbst VLANs aktiv, der andere für ungerade VLANs.

Ursache 2: Topologieänderungen für Spanning Tree Protocol

Ein weiteres häufiges Problem, das durch Flooding verursacht wird, ist Spanning Tree Protocol

(STP) Topology Change Notification (TCN). TCN wurde entwickelt, um Weiterleitungstabellen zu korrigieren, nachdem die Weiterleitungstopologie geändert wurde. Dies ist erforderlich, um einen Verbindungsausfall zu vermeiden, da nach einer Topologieänderung einige Ziele, auf die zuvor über bestimmte Ports zugegriffen werden konnte, über verschiedene Ports zugänglich sein können. TCN beschleunigt die Alterung der Weiterleitungstabelle. Wenn die Adresse also nicht erneut abgerufen wird, wird sie veraltet und es kommt zu Überflutungen.

TCNs werden von einem Port ausgelöst, der zum oder vom Weiterleitungsstatus wechselt. Auch wenn die MAC-Zieladresse nach dem TCN abgelaufen ist, sollte es in den meisten Fällen zu Überflutungen kommen, da die Adresse erneut abgerufen wird. Das Problem kann auftreten, wenn TCNs wiederholt in kurzen Intervallen auftreten. Die Switches werden ihre Weiterleitungstabellen ständig schnell altern, sodass die Überflutung nahezu konstant bleibt.

Normalerweise ist eine TCN in einem gut konfigurierten Netzwerk selten. Wenn der Port eines Switches aktiv oder inaktiv ist, wird schließlich eine TCN aktiviert, sobald der STP-Status des Ports an die oder von der Weiterleitung geändert wird. Beim Flapping des Ports entstehen wiederholte TCNs und Flooding.

Ports mit aktivierter STP-Portfast-Funktion verursachen keine TCNs beim Wechsel vom oder zum Weiterleitungsstatus. Die Konfiguration des Portfast an allen Endgeräte-Ports (z. B. Drucker, PCs, Server usw.) sollte die Anzahl der TCNs auf ein Minimum beschränken. Weitere Informationen zu TCNs finden Sie in diesem Dokument:

- Verstehen von Änderungen der Spanning Tree Protocol-Topologie

Hinweis: In MSFC IOS gibt es eine Optimierung, die VLAN-Schnittstellen auslöst, um ihre ARP-Tabellen zu replizieren, wenn sich im jeweiligen VLAN eine TCN befindet. Dadurch wird die Überflutung bei TCNs begrenzt, da ein ARP-Broadcast stattfinden wird und die MAC-Adresse des Hosts erneut abgerufen wird, wenn die Hosts auf ARP antworten.

Ursache 3: Überlauf der Weiterleitungstabelle

Eine weitere mögliche Ursache für eine Überflutung kann der Überlauf der Switch-Weiterleitungstabelle sein. In diesem Fall können keine neuen Adressen abgerufen werden, und die Pakete, die für diese Adressen bestimmt sind, werden überflutet, bis in der Weiterleitungstabelle Speicherplatz verfügbar wird. Anschließend werden neue Adressen gelernt. Dies ist möglich, aber selten, da die meisten modernen Switches über ausreichend große Weiterleitungstabellen verfügen, um MAC-Adressen für die meisten Designs unterzubringen.

Die Erschöpfung der Weiterleitungstabelle kann auch durch einen Angriff auf das Netzwerk verursacht werden, bei dem ein Host beginnt, Frames zu generieren, die jeweils mit unterschiedlichen MAC-Adressen stammen. Dadurch werden alle Ressourcen der Weiterleitungstabelle zusammengefasst. Sobald die Weiterleitungstabellen ausgelastet sind, wird anderer Datenverkehr überflutet, da keine neue Lernfunktion möglich ist. Diese Art von Angriff kann erkannt werden, indem die Switch-Weiterleitungstabelle geprüft wird. Die meisten MAC-Adressen verweisen auf denselben Port oder dieselbe Portgruppe. Solche Angriffe können verhindert werden, indem die Anzahl der MAC-Adressen, die an nicht vertrauenswürdigen Ports abgefragt werden, mithilfe der Port-Sicherheitsfunktion beschränkt wird.

Konfigurationsanleitungen für Catalyst Switches mit Cisco IOS®- oder CatOS-Software enthalten den Abschnitt Konfigurieren der Port-Sicherheit oder Konfigurieren der Port-basierten Datenverkehrskontrolle. Weitere Informationen finden Sie in der technischen Dokumentation für Ihren Switch auf den Produktseiten für Cisco Switches.

Hinweis: Wenn Unicast-Flooding in einem Switch-Port auftritt, der für die Port-Sicherheit konfiguriert ist, unter der Bedingung "Restrict" (Einschränken), um die Flutung zu stoppen, wird eine Sicherheitsverletzung trigeriert.

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

Hinweis: Wenn eine solche Sicherheitsverletzung auftritt, sollten die betroffenen Ports, die für den Modus "Einschränken" konfiguriert sind, Pakete mit unbekannten Quelladressen verwerfen, bis eine ausreichende Anzahl sicherer MAC-Adressen entfernt wird, um unter den maximalen Wert zu fallen. Dadurch erhöht sich der SecurityViolation-Zähler.

Hinweis: Wenn der Switch-Port in den "Shutdown"-Status wechselt, müssen Sie `Router(config-if)#switchport block unicast` konfigurieren, damit der jeweilige Switch-Port für Unicast-Flooding deaktiviert wird.

Erkennen übermäßiger Überflutung

Die meisten Switches implementieren keinen speziellen Befehl zum Erkennen von Flooding. Catalyst Switches der Serie 6500/6000 Supervisor Engine 2 und höher mit Cisco IOS System Software (Native) Version 12.1(14)E und höher oder Cisco CatOS-Systemsoftware Version 7.5 oder höher implementiert die Funktion zum **Schutz vor Unicast-Überflutung**. Kurz gesagt ermöglicht diese Funktion dem Switch die Überwachung der Unicast-Flooding pro VLAN und die Durchführung bestimmter Aktionen, wenn die Flutung die angegebene Menge überschreitet. Die Aktionen können in Syslog, Einschränkung oder Herunterfahren des VLANs erfolgen - das Syslog ist das nützlichste bei der Erkennung von Überschwemmungen. Wenn das Hochfahren die konfigurierte Rate überschreitet und die konfigurierte Aktion Syslog lautet, wird eine Meldung ausgegeben, die der folgenden ähnelt:

```
%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
```

Die angegebene MAC-Adresse ist die Quell-MAC-Adresse, von der die Pakete auf diesem Switch geflutet werden. Häufig müssen die MAC-Zieladressen bekannt sein, an die der Switch überflutet wird (da der Switch die Weiterleitung anhand der MAC-Zieladresse durchführt). Cisco IOS (nativ) Version 12.1(20)E für Catalyst 6500/6000 Supervisor Engine 2 und höher implementiert Funktionen zur Anzeige der MAC-Adressen, auf die überflutet wird:

```
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
```

Anschließend können weitere Untersuchungen durchgeführt werden, um festzustellen, ob die MAC-Adresse 0000.2222.000 Datenverkehr an die MAC-Adressen sendet, die im Abschnitt "MAC-Zieladresse" aufgeführt sind. Wenn Datenverkehr legitim ist, muss ermittelt werden, warum die MAC-Zieladressen für den Switch nicht bekannt sind.

Sie können feststellen, ob eine Flutung auftritt, indem Sie während einer Verlangsamung oder eines Ausfalls eine Spur von Paketen auf einer Workstation erfassen. In der Regel sollten Unicast-Pakete, die keine Workstation enthalten, nicht wiederholt auf dem Port angezeigt werden. Wenn dies geschieht, besteht die Gefahr, dass es zu Überschwemmungen kommt. Paketspuren können bei verschiedenen Hochwasserursachen anders aussehen.

Bei asymmetrischem Routing gibt es wahrscheinlich Pakete an eine bestimmte MAC-Adresse, die die Überflutung auch nach den Zielantworten nicht stoppen. Bei TCNs umfasst die Flooding viele verschiedene Adressen, sollte aber irgendwann anhalten und dann neu starten.

Bei einem Überlauf der L2-Weiterleitungstabelle wird wahrscheinlich die gleiche Flutung wie beim asymmetrischen Routing auftreten. Der Unterschied besteht darin, dass es wahrscheinlich eine hohe Anzahl seltsamer Pakete oder normale Pakete in ungewöhnlichen Mengen mit einer anderen Quell-MAC-Adresse geben wird.

Zugehörige Informationen

- Produkt-Support für Switches
- Support für LAN-Switching-Technologie
- Technischer Support – Cisco Systems