Nexus 7000 Storm Control: Auswählen der geeigneten Unterdrückungswerte

Inhalt

Einführung

Ein Datenverkehrssturm tritt auf, wenn Pakete das LAN überfluten. Dies führt zu einem übermäßigen Datenverkehr und beeinträchtigt die Netzwerkleistung. Sie können die Traffic Storm Control-Funktion verwenden, um Unterbrechungen an Layer-2-Ports durch einen Broadcast-, Multicast- oder Unicast-Datenverkehrssturm an physischen Schnittstellen zu verhindern.

Die Traffic Storm Control (auch als Verkehrsunterdrückung bezeichnet) ermöglicht die Überwachung des Datenverkehrs von eingehenden Broadcast-, Multicast- und Unicast-Datenverkehr in einem Intervall von 10 Millisekunden. In diesem Intervall wird die Datenverkehrsstufe, die einen Prozentsatz der gesamten verfügbaren Bandbreite des Ports ausmacht, mit der von Ihnen konfigurierten Kontrollstufe für Datenverkehrsenstürme verglichen. Wenn der eingehende Datenverkehr die auf dem Port konfigurierte Sturmkontrollebene erreicht, wird der Datenverkehr durch die Datenverkehrsüberwachung unterbrochen, bis das Intervall endet.

Die Grenzwerte für die Sturmkontrolle und das Zeitintervall ermöglichen es dem Algorithmus zur Steuerung des Datenverkehrs, mit unterschiedlichen Detaillierungsgraden zu arbeiten. Ein höherer Grenzwert ermöglicht die Übertragung von mehr Paketen.

Standardmäßig ergreift die Cisco Nexus Operating System (NX-OS)-Software keine Korrekturmaßnahmen, wenn der Datenverkehr das konfigurierte Niveau überschreitet. Sie können jedoch eine EEM-Aktion (Embedded Event Management) konfigurieren, mit der eine Schnittstelle deaktiviert wird, wenn der Datenverkehr innerhalb eines bestimmten Zeitraums nicht nachlässt (unter den Schwellenwert fällt).

Richtlinien und Einschränkungen für die Steuerung von Datenverkehrsströmen

Beachten Sie bei der Konfiguration der Kontrollebene für Datenverkehrsenstürme die folgenden Richtlinien und Einschränkungen:

- Sie können die Datenverkehrsensturmkontrolle auf einer Port-Channel-Schnittstelle konfigurieren.
- Konfigurieren Sie keine Datenverkehrsensturm-Steuerung an Schnittstellen, die zu einer Port-Channel-Schnittstelle gehören. Durch die Konfiguration der Traffic Storm Control für Schnittstellen, die als Member eines Port-Channels konfiguriert sind, werden die Ports in einen ausgesetzten Zustand versetzt.
- Geben Sie die Ebene als Prozentsatz der gesamten Schnittstellenbandbreite an: Die Stufe kann zwischen 0 und 100 liegen.Der optionale Teil einer Ebene kann zwischen 0 und 99 liegen.100 Prozent bedeutet keine Sturmkontrolle.0 % unterdrückt den gesamten Datenverkehr.

Aufgrund von Hardware-Einschränkungen und der Methode, mit der Pakete unterschiedlicher Größen gezählt werden, ist der Prozentanteil der Stufe eine Annäherung. Je nach Größe der Frames, aus denen der eingehende Datenverkehr besteht, kann die tatsächliche Durchsetzungsebene um mehrere Prozentpunkte von der konfigurierten Ebene abweichen.

Standardeinstellungen für Traffic Storm Control

Parameter	Standard
Sturmkontrolle	Deaktiviert
Grenzwert in Prozent	100

Konfigurieren der Traffic Storm Control

Sie können den Prozentsatz der gesamten verfügbaren Bandbreite festlegen, die der kontrollierte Datenverkehr verwenden kann.

1. Terminal konfigurieren
2. Schnittstelle {Ethernet Steckplatz/Port | Port-Channel Nummer}
3. Sturmkontrolle {Broadcast | Multicast | Unicast} Ebene Prozentsatz[.Bruchteil]

Hinweis: Bei der Datenverkehrsflusskontrolle wird ein Intervall von 10 Millisekunden verwendet, das das Verhalten der Sturmkontrolle beeinflussen kann.

Überprüfen der Konfiguration der Traffic Storm Control

So zeigen Sie Konfigurationsinformationen für die Datenverkehrsensturmsteuerung an:

Befehl	Zweck
Anzeigeschnittstelle [Ethernet Steckplatz/Port | Port-Channel Nummer] Sturmkontrolle	Zeigt die Konfiguration der Traffic Storm Con für die Schnittstellen an.
show running-config interface	Zeigt die Konfiguration der Traffic Storm Con an.

Überwachung von Datenverkehrs-Sturm-Kontrollzählern

Sie können die Zähler, die das Cisco NX-OS-Gerät verwaltet, auf Aktivitäten zur Steuerung von Datenverkehrsströmen überwachen.

```
switch# show interface counters storm-control
```

Nexus 7000 Storm Control: Auswählen der geeigneten Unterdrückungswerte

Um Kunden bei der Auswahl des geeigneten Schwellenwerts zu unterstützen, bietet dieser Abschnitt Einblicke in die Logik, die hinter der Verwendung der Schwellenwerte steckt.

Hinweis: Die hier dargestellten Informationen stellen keine Best Practice-Nummern bereit, der Kunde kann jedoch nach dem Durchlaufen der Informationen zu einer logischen Entscheidung gelangen.

Verwendete Komponenten

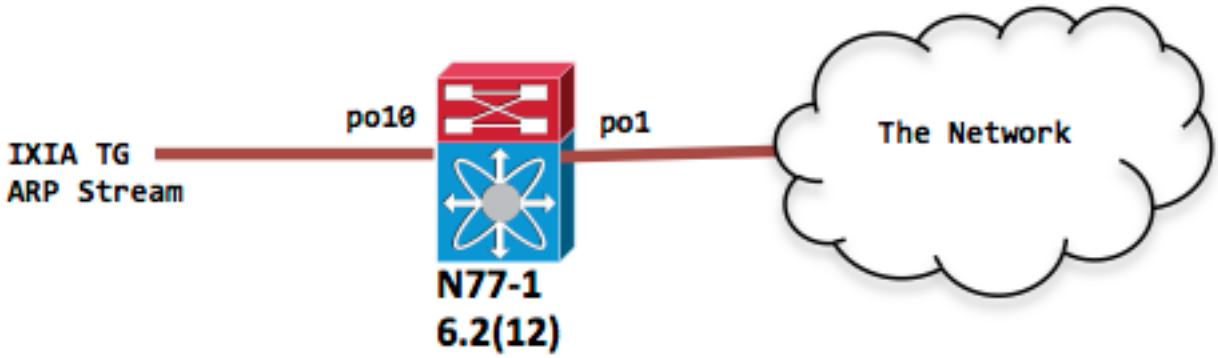
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Nexus 7700 mit Version 6.2.12 und höher
- Line Card der F3-Serie

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Labortests

Die Sturmkontrolle ist ein Mechanismus zur Unterdrückung des Datenverkehrs, der auf den eingehenden Datenverkehr an einem bestimmten Port angewendet wird.




```
N77-1(config-if)# sh port-c sum
1     Po1(SU)     Eth     LACP     Eth2/4(P)
10    Po10(SU)    Eth     LACP     Eth1/1(P)

interface port-channel1
switchport

interface port-channel10
switchport
```

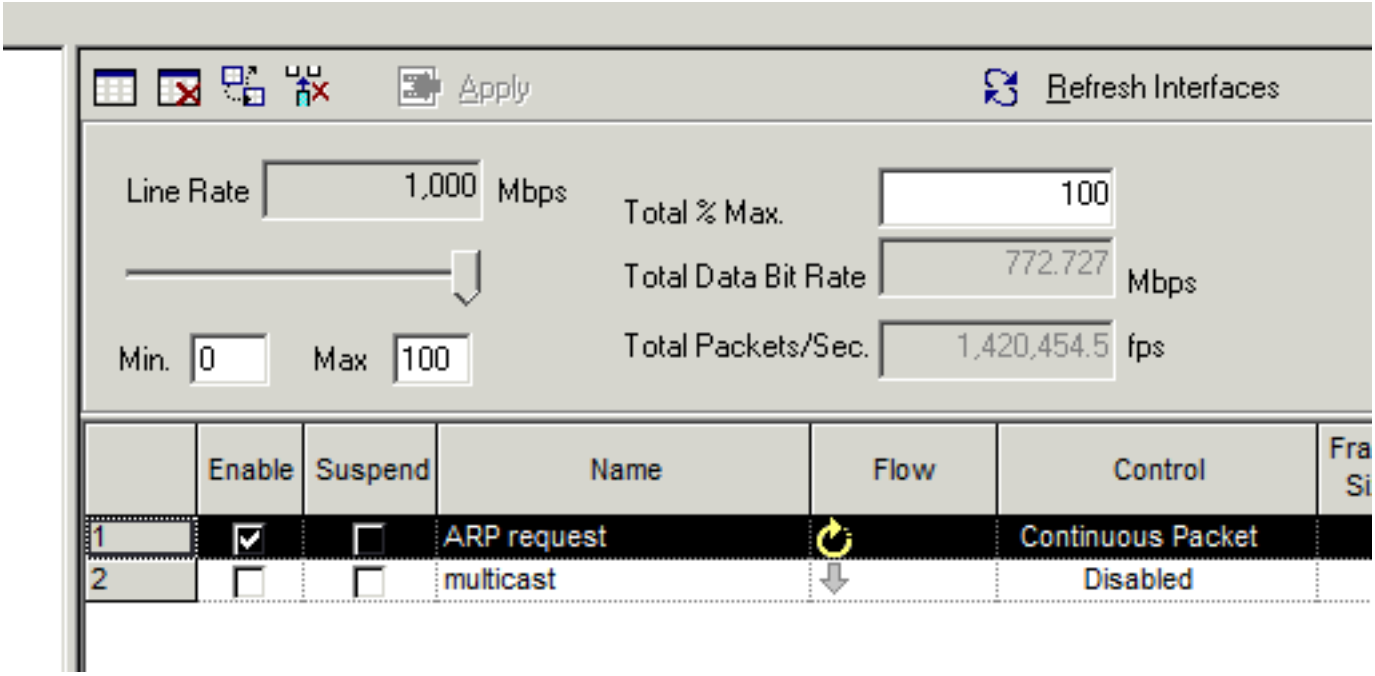
Szenerio 1: Die Unterdrückungsrate beträgt 0,01 %.

Die Eingangsverkehrsrate wird auf 1 Gbit/s für den ARP-Anfrageverkehr festgelegt.

Konfiguration

interface port-channel10
Storm-Control Broadcast Level 0,01

IXIA-Snapshot für Referenz




```
N77-1(config-if)# sh int po10 | in rate | in "30 sec"
   30 seconds input rate 954649416 bits/sec, 1420607 packets/sec
   30 seconds output rate 1856 bits/sec, 0 packets/sec
input rate 954.82 Mbps, 1.42 Mpps; output rate 1.97 Kbps, 0 pps

N77-1(config-if)# sh int po1 | in rate | in "30 sec"
   30 seconds input rate 8656 bits/sec, 8 packets/sec
   30 seconds output rate 853632 bits/sec, 1225 packets/sec >>>> Output rate is ~ 1200 pps
input rate 8.74 Kbps, 8 pps; output rate 875.32 Kbps, 1.22 Kpps

N77-1# sh int po10 counters storm-control
--------------------------------------------------------------------------------
Port        UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Po10             100.00          100.00            0.01           67993069388
```

Die Sturmkontrolle wird als Referenz angezeigt.

Szenerio 2: Die Unterdrückungsrate beträgt 0,1 %.

Die Eingangsverkehrsrate wird auf 1 Gbit/s für den ARP-Anfrageverkehr festgelegt.

Konfiguration

interface port-channel10
Storm-Control Broadcast Level 0,10

Nur die Ausgangsschnittstelle wird angezeigt, da die Eingangsschnittstelle po10 dieselbe eingehende Datenverkehrsrate von 1 Gbit/s aufweist.

```
N77-1(config-if)# sh int po1 | in rate | in "30 sec"
  30 seconds input rate 8840 bits/sec, 8 packets/sec
  30 seconds output rate 8253392 bits/sec, 12271 packets/sec >>>> Output rate is ~ 12k pps
```

Szenerio 3: Die Unterdrückungsrate beträgt 1 %.

Die Eingangsverkehrsrate wird auf 1 Gbit/s für den ARP-Anfrageverkehr festgelegt.

Konfiguration

interface port-channel10

Sturmkontrolle Broadcast Level 1

Nur die Ausgangsschnittstelle wird angezeigt, da die Eingangsschnittstelle po10 dieselbe eingehende Datenverkehrsrate von 1 Gbit/s aufweist.

```
N77-1(config-if)# sh int po1 | in rate
  30 seconds input rate 8784 bits/sec, 7 packets/sec
  30 seconds output rate 86601056 bits/sec, 129293 packets/sec >>>> Output rate is ~ 120k pps
  input rate 8.78 Kbps, 7 pps; output rate 86.60 Mbps, 129.29 Kpps
```

Szenerio 4: Die Unterdrückungsrate beträgt 10 %.

Die Eingangsverkehrsrate wird auf 1 Gbit/s für den ARP-Anfrageverkehr festgelegt.

Konfiguration

interface port-channel10

Storm-Control Broadcast Level 10,00

```
 N77-1(config-if)# sh int po1 | in rate
  30 seconds input rate 8496 bits/sec, 7 packets/sec
  30 seconds output rate 839570968 bits/sec, 1249761 packets/sec >>>> Output rate is ~ 1.2mil
pps
  input rate 8.50 Kbps, 7 pps; output rate 839.57 Mbps, 1.25 Mpps
```

Zusammenfassung:

Alle oben genannten Szenarien behandeln einen dauerhaften Datenverkehrsstrom, der möglicherweise durch eine Schleife oder eine fehlerhafte NIC verursacht wird. Die Sturmkontrolle ermöglicht in diesem Szenario eine Ratenbegrenzung, bevor der Datenverkehr in das Netzwerk eingespeist wird. Die verschiedenen Unterdrückungsstufen geben an, wie viel Datenverkehr Sie in Ihr Netzwerk einspeisen werden.

Würde es bei einer Sturmkontrolle dazu führen, dass der normale ARP fallen würde, wenn der Grenzwert aggressiv bleibt?

Es gibt einige Punkte, die beachtet werden sollten

1. In erster Linie, wenn ARP beim ersten Abbruch immer wieder von der Anwendungsschicht initiiert wird, erhöht sich die Wahrscheinlichkeit, dass ARP bei nachfolgenden Wiederholungen aufgelöst wird und eine erfolgreiche IP-zu-MAC-Auflösung erreicht wird.

2. Die Sturmkontrolle ist eine Eingangsüberwachung, die so nahe wie möglich am Edge angewendet werden sollte. Es kann also sein, dass Sie es mit einem physischen Host oder einem VM-Cluster zu tun haben. Bei einem Host stellt die Anzahl der ARPs in einem normalen Arbeitsszenario kein wirkliches Problem dar. Wenn es sich um einen VM-Cluster handelt, kann eine bestimmte Anzahl von Hosts vorhanden sein, aber wiederum keine Angabe einer vollständigen Layer-2-Domäne hinter einem Edge-Port.
3. Wenn Sie die Konfiguration der Sturmkontrolle auf Core-Ports anwenden, sollten Sie wissen, wie der Broadcast-Datenverkehr aggregiert werden kann, bevor er den Core-Layer erreicht.

Kehren wir zu unseren Tests zurück. Hier sind einige der Tests für Burst-ARP-Datenverkehr:

Test 1: 5.000 Pakete Burst bei 5.000 pps Einmaliges Burst

Unterdrückungsstufe 0,01 %

Konfiguration

interface port-channel10

Storm-Control Broadcast Level 0,01

```
N77-1# sh int po10
port-channel10 is up
admin state is up
RX
  12985158 unicast packets 27 multicast packets 5000 broadcast packets
   12990674 input packets 1091154042 bytes
  0 jumbo packets 2560 storm suppression packets

N77-1#Sh int po1
port-channel1 is up
admin state is up
TX
  0 unicast packets 507 multicast packets 2440 broadcast packets

N77-1(config-if)# sh int po10 counters storm-control
--------------------------------------------------------------------------------
Port       UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Po10             100.00         100.00            0.01                 2560
```

Die obige Abbildung zeigt 2560 verworfene ARP-Pakete. Wenn Sie 5000 Hosts hinter einer Schnittstelle haben, dann durchläuft die Hälfte dieser Hosts die erste Iteration und die zweite Hälfte wird in der nächsten oder so weiter gehen. Wenn Ihre Anwendung nur eine ARP-Anforderung sendet, um die IP-to-MAC-Auflösung zu erhalten, muss die Anwendung möglicherweise geändert werden, um ARP-Anfragen erneut zu übertragen, wenn keine Antwort erfolgt. Wenden Sie sich in diesem Fall an den Anwendungsanbieter, um Unterstützung bei der Änderung dieses Verhaltens zu erhalten.

Test 2: 5000 Pakete Burst bei 50000pps Einmaliges Burst

Unterdrückungsstufe 0,01 %

Konfiguration

interface port-channel10

Storm-Control Broadcast Level 0,01

```
N77-1(config-if)# sh int po10
port-channel10 is up
admin state is up
RX
  0 unicast packets 19 multicast packets 5000 broadcast packets
  5019 input packets 435550 bytes
  0 jumbo packets 3771 storm suppression packets

N77-1(config-if)# sh int po1
port-channel1 is up
admin state is up
TX
  0 unicast packets 712 multicast packets 1229 broadcast packets

N77-1(config-if)# sh int po10 counters storm-control
--------------------------------------------------------------------------------
Port       UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Po10             100.00         100.00           0.01                  3771
```

In der obigen Ausgabe gibt es aufgrund der höheren Geschwindigkeit des Paket-Bursts eine höhere Anzahl an Verwerfungen.

Ähnliche Ergebnisse werden angezeigt, wenn die pps-Rate für 5.000 Paket-Burst bei 100 Kpps bis zu einer Paketrate von 1 Gbit/s erhöht wird.

Zur Erkennung des Sturmzustands stehen folgende Optionen zur Verfügung:

Warnmeldungen auf Datenebene:

- Durch die Konfiguration der Sturmkontrolle wird eine Syslog-Meldung für Warnungen generiert, und Sie können EEM einbinden, um Simple Network Management Protocol (SNMP)-Traps zu generieren, oder den Port als vorbeugende Maßnahme herunterfahren.

Warnmeldungen auf Kontrollebene:

- Option "logging drop threshold" konfigurieren:

Auf Nexus 7000 gibt es eine standardmäßige Richtlinienzuweisung - Kontrollebene:

Diese Richtlinienzuordnung regelt, welcher Datenverkehr an die CPU weitergeleitet wird. In dieser Richtlinienzuordnung wird eine Klasse angezeigt, die reguliert, wie viel ARP an die CPU geht.

Durch die Konfiguration des 'logging drop threshold' unter dieser Klasse werden alle Verletzungen im Syslog gemeldet. Sie können EEM auch zur Generierung von SNMP-Traps verwenden.

- Control Plane Policing (CoPP) MIB-Polling

Ab NX-OS 6.2(2) unterstützt CoPP die Cisco Class-Based QoS MIB (cbQoSMIB). Alle Elemente können mithilfe von SNMP überwacht werden.

Schlussfolgerung

Storm Control ist die nützliche Funktion, die Unterbrechungen an Layer-2-Ports durch einen Broadcast-, Multicast- oder Unicast-Datenverkehrssturm an physischen Schnittstellen verhindert. Diese Funktion steuert den Sturm auf der Datenebene, bevor er sich auf die Kontrollebene und das CoPP auswirkt.