

# Nexus 7000風暴控制：選擇適當的抑制值

## 目錄

### [簡介](#)

### [交通風暴控制的准則和限制](#)

### [流量風暴控制的預設設定](#)

### [配置流量風暴控制](#)

### [驗證流量風暴控制配置](#)

### [監控流量風暴控制計數器](#)

### [Nexus 7000風暴控制：選擇適當的抑制值](#)

### [採用元件](#)

### [實驗室測試](#)

### [案例1:抑制率為0.01%](#)

### [設定](#)

### [案例2:抑制率為0.1%](#)

### [設定](#)

### [案例3:抑制率為1%](#)

### [設定](#)

### [案例4:抑制率為10%](#)

### [設定](#)

### [摘要:](#)

### [測試1:5000 packets burst @ 5000pps single burst](#)

### [設定](#)

### [測試2:5000 packets burst @ 50000pps single burst](#)

### [設定](#)

### [結論](#)

### [相關思科支援社群討論](#)

## 簡介

當資料包泛洪LAN時，就會發生流量風暴，從而產生過多的流量並降低網路效能。您可以使用流量風暴控制功能防止物理介面上的廣播、組播或單播流量風暴對第2層埠造成中斷。

流量風暴控制（也稱為流量抑制）允許您監控以10毫秒時間間隔傳入的廣播、組播和單播流量的級別。在此間隔期間，將流量級別（即埠總可用頻寬的百分比）與配置的流量風暴控制級別進行比較。當輸入流量達到在連線埠上設定的流量風暴控制層級時，流量風暴控制會捨棄流量，直到時間間隔結束。

交通風暴控制閾值編號和時間間隔允許交通風暴控制演算法在不同粒度級別上工作。更高的閾值允許更多資料包通過。

預設情況下，Cisco Nexus Operating System(NX-OS)軟體在流量超過配置級別時不會採取糾正措施。但是，您可以配置嵌入式事件管理(EEM)操作，以便在流量在某一時間段內未減少（低於閾值）時錯誤禁用介面

# 交通風暴控制的准則和限制

配置流量風暴控制級別時，請注意以下准則和限制：

- 您可以在埠通道介面上配置流量風暴控制。
- 請勿在屬於埠通道介面的介面上配置流量風暴控制。在配置為埠通道成員的介面上配置流量風暴控制，可使埠進入暫停狀態。
- 以總介面頻寬的百分比指定級別：級別可以是0到100。級別的可選部分可以是0到99。100%意味著無法控制交通風暴。0%抑制所有流量。

由於硬體限制以及計數不同大小資料包的方法，級別百分比是一個近似值。根據組成傳入流量的幀大小，實際強制級別可能與配置的級別有數個百分點的差異。

## 流量風暴控制的預設設定

引數	預設
交通風暴控制	已禁用
閾值百分比	100

## 配置流量風暴控制

您可以設定受控流量可以使用的總可用頻寬的百分比。

1. configure terminal
2. 介面 {乙太網路 插槽/連接埠 | port-channel 編號}
3. 風暴控制 {廣播 | 多點傳播 | 單點傳播} 級別 百分比[.分數]

附註：交通風暴控制使用10毫秒的時間間隔，該時間間隔會影響交通風暴控制的行為。

## 驗證流量風暴控制配置

要顯示流量風暴控制配置資訊，請執行以下任務之一：

指令	目的
顯示介面 [乙太網路 插槽/連接埠   port-channel 編號] 計數器風暴控制	顯示介面的流量風暴控制配置。
show running-config interface	顯示流量風暴控制配置。

## 監控流量風暴控制計數器

您可以監控Cisco NX-OS裝置維護的流量風暴控制活動計數器。

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

## Nexus 7000風暴控制：選擇適當的抑制值

為了幫助客戶選擇合適的閾值，本節提供了有關使用閾值背後的邏輯的見解。

附註：此處提供的資訊並不提供任何最佳實踐編號，但客戶可以在瀏覽完資訊後做出合理的決策。

# 採用元件

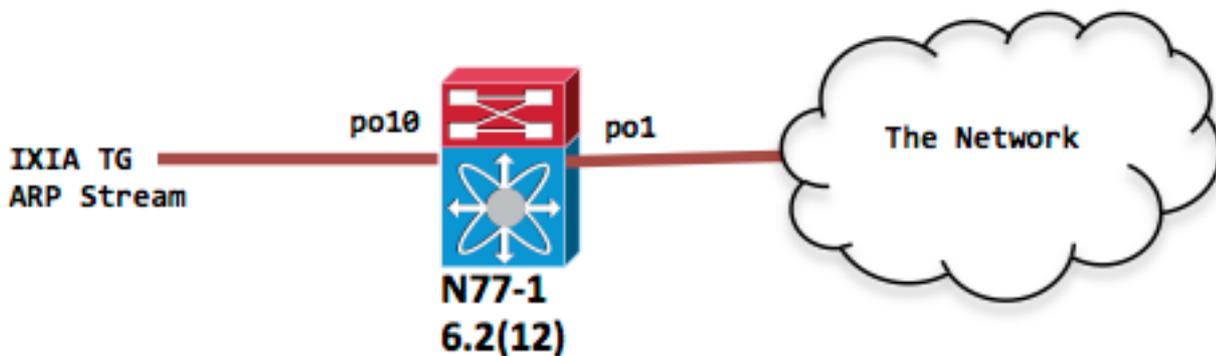
本文中的資訊係根據以下軟體和硬體版本：

- Nexus 7700 ( 6.2.12及更新版本 )。
- F3系列線路卡。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 實驗室測試

風暴控制是一種流量抑制機制，應用於特定連線埠上的輸入流量。



```
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
```

## 案例1:抑制率為0.01%

入口流量速率設定為1Gbps ARP請求流量

### 設定

```
interface port-channel10
風暴控制廣播級別0.01
```

IXIA快照以供參考

Apply Refresh Interfaces

Line Rate  Mbps

Total % Max.

Total Data Bit Rate  Mbps

Min.  Max

Total Packets/Sec.  fps

	Enable	Suspend	Name	Flow	Control	Fra Si
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ARP request		Continuous Packet	
2	<input type="checkbox"/>	<input type="checkbox"/>	multicast		Disabled	

```
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
```

顯示風暴控制點以供參考。

## 案例2:抑制率為0.1%

入口流量速率設定為1Gbps ARP請求流量

### 設定

```
interface port-channel10
風暴控制廣播級別0.10
```

由於輸入介面po10具有相同1gbps的傳入流量速率，因此只顯示輸出介面

```
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
```

## 案例3:抑制率為1%

入口流量速率設定為1Gbps ARP請求流量

### 設定

```
interface port-channel10
```

```
風暴控制廣播級別1
```

由於輸入介面po10具有相同1gbps的傳入流量速率，因此只顯示輸出介面

```
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
```

## 案例4:抑制率為10%

入口流量速率設定為1Gbps ARP請求流量

### 設定

```
interface port-channel10
```

```
風暴控制廣播級別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
```

### 摘要:

上述所有場景都處理可能由環路或NIC故障引起的持續流量流。在此案例中，風暴控制可有效限制流量注入網路之前的速率。不同的抑制級別會告訴您將向網路注入多少流量。

實施風暴控制後，如果將閾值保持在主動級別，是否會造成正常ARP丟棄？

有幾個事情需要考慮

1. 首先也是最重要的是，如果ARP確實在第一次被丟棄，那麼應用層總是會發起重試，因此在隨後的重試中，ARP被解析的可能性會更高，並且會導致IP到MAC解析的成功。
  2. 風暴控制是輸入管制器，應儘可能靠近邊緣應用。因此，您可能要處理一台物理主機或一個VM群集。如果是一台主機，那麼ARP的數量在正常工作場景中實際上不是問題。如果這是VM群集，則您可能具有特定數量的主機，但同樣沒有表示邊緣埠後整個第2層域的主機。
  3. 如果在核心埠上應用風暴控制配置，則請注意廣播流量在到達核心層之前如何聚集。
- 回到我們的測試 — 此處是一些針對突發ARP流量的測試。

# 測試1:5000 packets burst @ 5000pps single burst

抑制水準0.01%

## 設定

```
interface port-channel10
```

風暴控制廣播級別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-channel11 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	<b>2560</b>

上面顯示2560個丟棄的ARP資料包。當然，如果一個介面後有5000台主機，那麼其中一半主機在第一次迭代中通過，而另一半主機在下一次迭代中通過等等。如果您的應用程式只傳送一個ARP請求來獲得IP到MAC的解析，則可能需要修改該應用程式來重新傳輸ARP請求（如果沒有響應）。在這種情況下，請與應用程式供應商聯絡，以獲得更改此行為的幫助。

# 測試2:5000 packets burst @ 50000pps single burst

抑制水準0.01%

## 設定

```
interface port-channel10
```

風暴控制廣播級別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
```

在以上輸出中，由於較高分組突發速率，有較高的丟棄數量。

在100kpps時的5000個資料包突發的pps速率增加至1 gbps資料包速率時，也會看到類似的結果

下列選項可用於檢測風暴狀況。

資料平面上的警報：

- 配置風暴控制會生成警報的系統日誌消息，您可以連線EEM以生成簡單網路管理協定 (SNMP)陷阱或作為預防措施關閉埠。

控制平面上的警報：

- 配置「logging drop threshold」選項：

在Nexus 7k上有一個預設策略對映 — 控制平面：

此策略對映正在調節哪些流量正在傳遞到CPU。在此策略對映中，您可以看到一個類，它規範了向CPU傳遞的ARP數量。

在此類下配置「logging drop threshold」將報告系統日誌中的任何違規，您可以進一步使用EEM生成SNMP陷阱。

- 控制階段管制(CoPP)MIB輪詢

從NX-OS 6.2(2)開始，CoPP支援Cisco基於類別的QoS MIB(cbQoS MIB)，其所有元素均可使用SNMP進行監控

## 結論

風暴控制是一項有用的功能，可防止物理介面上的廣播、組播或單播流量風暴對第2層埠造成中斷。此功能在影響控制平面和CoPP之前控制資料平面上的風暴。