目录

[简介](#)
[指南和限制流量风暴控制的](#)
[流量风暴控制的默认设置](#)
[配置流量风暴控制](#)
[正在验证的流量风暴控制配置](#)
[监控流量风暴控制计数器](#)
[连结7000风暴控制：选择适当的抑制值](#)
[使用的组件](#)
[实验室测试](#)
[案例1 ：Supression速率是0.01%](#)
[设置](#)
[案例2 ：Supression速率是0.1%](#)
[设置](#)
[案例3 ：Supression速率是1%](#)
[设置](#)
[案例4 ：Supression速率是10%](#)
[设置](#)
[摘要：](#)
[测试 1：5000个信息包突发@ 5000pps单个突发流量](#)
[设置](#)
[测试 2：5000个信息包突发@ 50000pps单个突发流量](#)
[设置](#)
[结论](#)
[相关的思科支持社区讨论](#)

简介

当数据包充斥LAN，创建额外数据流和降低网络性能，流量风暴发生。您能使用流量风暴控制功能由广播，组播防止在Layer2端口的中断或者在物理接口的单播流量风暴。

流量风暴控制(也呼叫流量抑制)允许您监控流入广播，组播的级别和单播流量10毫秒间隔。在此间隔期间，数据流级别，是端口的百分比总可用的带宽，与该流量风暴的控制层比较您配置。当入口流量到达在端口配置的流量风暴控制层时，流量风暴控制降低流量，直到间隔结束。

流量风暴控制阈值数字和时间间隔允许流量风暴控制算法与不同的级别粒度一起使用。高限阈值准许更多数据包通过通过。

默认情况下，思科连结操作系统的(NX-OS)软件不采取纠正措施，当流量超出已配置的级别时。然而，您能配置一嵌入式事件管理(EEM)操作使错误停止接口，如果流量不在某一时间消退(丢弃在阈值之下)

指南和限制流量风暴控制的

当配置流量风暴控制层时，请注释以下指南和限制：

- 您能配置在端口信道接口的流量风暴控制。
- 请勿配置在是端口信道接口的成员的接口的流量风暴控制。配置在配置作为端口信道的成员的接口的流量风暴控制放端口到中止状态。
- 指定级别作为百分比总接口带宽： 级别可以是从0到100。级别的可选部分可以是从0到99。100百分比不含义流量风暴控制。0百分比抑制所有流量。

由于数据包不同的大小计数的硬件限制和方法，级别百分比是近似值。根据组成流入的数据流帧的大小，实际被强制执行的级别也许与已配置的级别有所不同由几个百分点。

流量风暴控制的默认设置

参数	默认
流量风暴控制	已禁用
门限值百分比	100

配置流量风暴控制

您能设置控制流量能使用总可用的带宽的百分比。

1. configure terminal
2. 接口{以太网插槽/端口|Port-Channel编号}
3. storm-control {广播|组播|单播}级别百分比[.fraction]

注意：流量风暴控制使用能影响流量风暴控制行为的10毫秒间隔。

正在验证的流量风暴控制配置

要显示流量风暴控制配置信息，请执行以下任务之一：

命令	目的
show interface [以太网插槽/端口|Port-Channel编号]计数器storm-control	显示接口的流量风暴控制配置。
show running-config interface	显示流量风暴控制配置。

监控流量风暴控制计数器

您能监控Cisco NX-OS设备为流量风暴控制活动维护的计数器。

连结7000风暴控制：选择适当的抑制值

要帮助客户挑选适当的阈值，此部分在使用阈值后的逻辑提供见解。

注意：被提交的信息此处不提供任何最佳实践编号，但是客户能做出逻辑判定在通过信息以后。

使用的组件

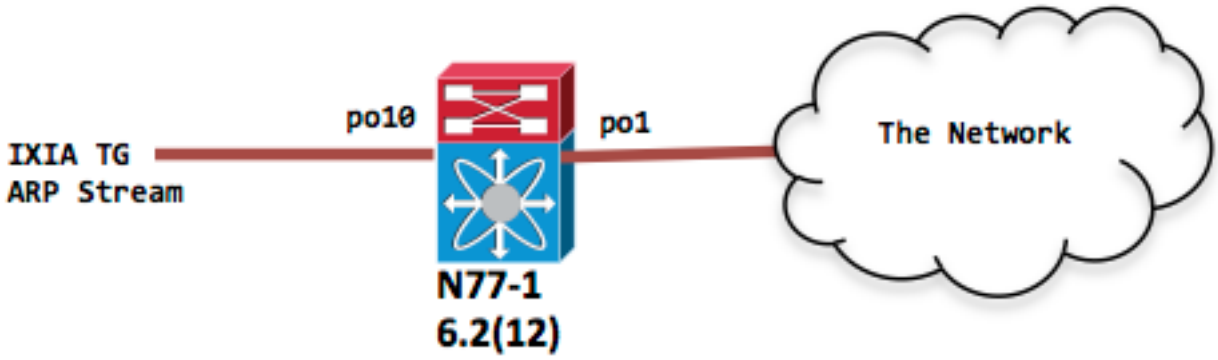
本文档中的信息基于以下软件和硬件版本：

- 连结7700用版本6.2.12及以后。
- F3系列线卡。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

实验室测试

风暴控制是应用对在特定端口的入口流量的流量抑制mechnicm。



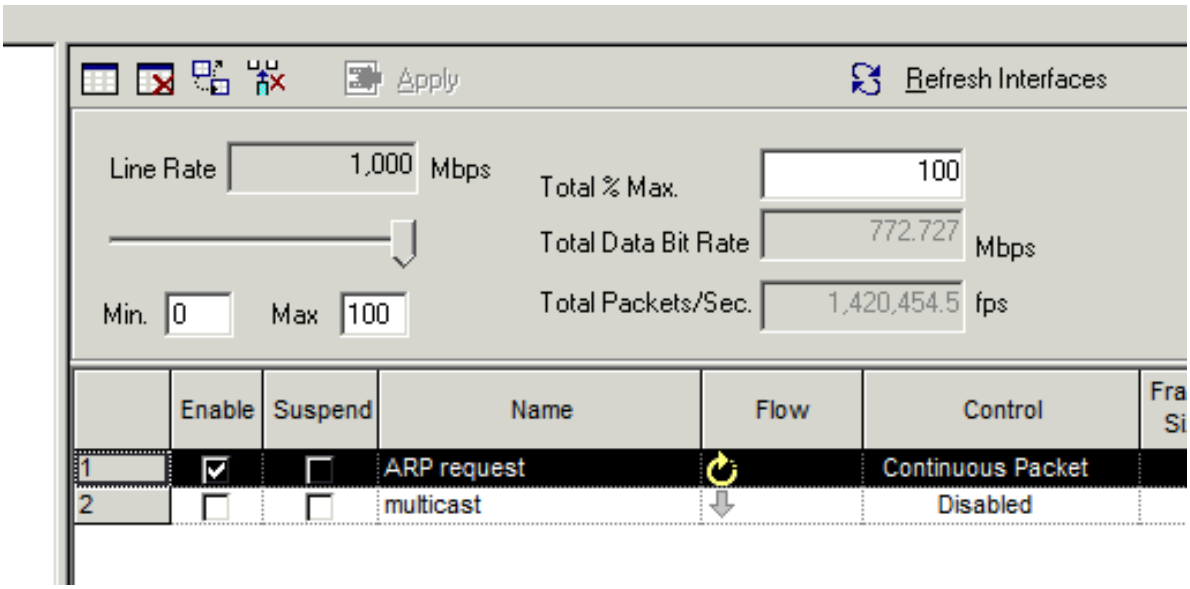
案例1 ：Supression速率是0.01%

入口流量速率设置为ARP请求流量1Gbps

设置

接口port-channel10
storm-control广播级别0.01

鸢尾属快照供参考




```
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/secinput 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 ppsinput 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
```

风暴控制丢包显示供参考。

案例2 ：Supression速率是0.1%

入口流量速率设置为ARP请求流量1Gbps

设置

接口port-channel10
storm-control广播级别0.10

只去显示出口接口，因为入口接口po10有同一流入的数据流速率1gbps

```
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 ：Supression速率是1%

入口流量速率设置为ARP请求流量1Gbps

设置

接口port-channel10

storm-control广播1级

只去显示出口接口，因为入口接口po10有同一流入的数据流速率1gbps

```
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 ：Supression速率是10%

入口流量速率设置为ARP请求流量1Gbps

设置

接口port-channel10

storm-control广播级别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：

所有上述案例涉及持续的数据流可能导致的由于环路或发生故障的NIC。在被注入网络前，风暴控制是有效在限制流量的速率的此方案。不同的抑制级别如何告诉多少流量您注入您的网络。

当风暴控制到位时，是否将造成正常ARP被撤销，如果保持阈值在一个积极的级别？

有要考虑的一些工作

1. 首要，如果ARP被撤销第一次总是有应用层启动的重试次数，因此获得ARP的机会被解决在随后的重试次数期间更大，并且请导致成功的IP MAC解决方法。
2. 风暴控制是入口策略，并且它应该是作为应用的close到边缘尽可能。因此可能交易与一物理主机或VM集群的您。在一个正常工作的方案期间，如果一台主机然后ARPs编号确实不是问题。如果这是VM集群，则您可以有将指示一个整个第2层域在边缘端口背后主机，但是再没什么的某一编号。
3. 如果运用在核心端口的风暴控制设置那么请注意广播数据流如何能获得聚集，在到达核心层前。

对我们的测验的去的上一步？对于此处突变性ARP流量是某些测试

测试 1：5000个信息包突发@ 5000pps单个突发流量

Supression级别0.01%

设置

接口port-channel10

storm-control广播级别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
```

以上显示2560丢弃的ARP数据包。当然，如果有在一个接口后的5000台主机然后半他们在第一迭代时通过和第二半将通过在下期间或那么。如果您的应用程序只发送一个ARP请求有IP MAC解决方法那么应用程序是否可能需要被修改重新传输ARP请求无响应。 在这种情况下，与应用供应商的检查在更改此行为的协助的。

测试 2：5000个信息包突发@ 50000pps单个突发流量

Supression级别0.01%

设置

接口port-channel10

storm-control广播级别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
```

在上述输出中有丢包较高的值由于信息包突发更高的速率。

当pps速率为5000信息包突发@直到1 gbps数据包速率的100kpps增加相同的结果被看到

以下选项为风暴情况的检测是可用的。

警告在数据层面：

- 配置风暴控制生成警报的系统消息，并且您在EEM能附加形成简单网络管理协议(SNMP)陷阱或关闭端口作为一预防操作。

警告在控制层面：

- 配置‘记录日志丢弃阈值’选项：

在连结7k有默认策略映射-控制面板：

流量通过对CPU的此策略映射调控。在此策略映射内您能看到调控的类多少ARP去CPU。

配置‘记录日志丢弃阈值’在此类下将报告在Syslog的所有侵害，您能进一步使用EEM形成SNMP陷阱。

- 控制平面策略(CoPP) MIB轮询

开始在NX-OS 6.2(2)， CoPP支持思科基于类的QoS MIB (cbQoSMIB)使用SNMP，并且所有其元素可以监控

结论

风暴控制是由广播，组播防止在Layer2端口的中断的有用的功能，或者在物理接口的单播流量风暴。在影响控制面板和CoPP前，此功能控制风暴在数据层面。