

Contenu

[Introduction](#)

[Instructions et limites pour le contrôle de tempête du trafic](#)

[Valeurs par défaut pour le contrôle de tempête du trafic](#)

[Configurer le contrôle de tempête du trafic](#)

[Vérifier la configuration de contrôle de tempête du trafic](#)

[Surveillance des compteurs d'instruction de tempête du trafic](#)

[Contrôle de tempête de Nexus 7000 : Sélectionner des valeurs appropriées de suppression](#)

[Composants utilisés](#)

[Essai en laboratoire](#)

[Scenerio 1 : Le débit de Supression est 0.01%](#)

[Config](#)

[Scenerio 2 : Le débit de Supression est 0.1%](#)

[Config](#)

[Scenerio 3 : Le débit de Supression est 1%](#)

[Config](#)

[Scenerio 4 : Le débit de Supression est 10%](#)

[Config](#)

[Résumé :](#)

[Test 1 : 5000 @ 5000pps éclatés par paquets choisissent la rafale](#)

[Config](#)

[Test 2 : 5000 @ 50000pps éclatés par paquets choisissent la rafale](#)

[Config](#)

[Conclusion](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Une tempête du trafic se produit quand les paquets inondent le RÉSEAU LOCAL, créant le trafic excessif et dégradant des performances du réseau. Vous pouvez employer la caractéristique de contrôle de tempête du trafic pour empêcher des interruptions sur des ports de la couche 2 par une émission, une Multidiffusion, ou une tempête du trafic unicast sur des interfaces physiques.

Le contrôle de tempête du trafic (également appelé la suppression du trafic) te permet pour surveiller les niveaux de l'émission, de la Multidiffusion, et du trafic unicast entrants pendant un intervalle 10-millisecond. Pendant cet intervalle, le niveau du trafic, qui est un pourcentage de toute la bande passante disponible du port, est comparé au niveau de contrôle de tempête du trafic que vous avez configuré. Quand le trafic entrant atteint le niveau de contrôle de tempête du trafic qui est configuré sur le port, trafiquez le contrôle de tempête relâche le trafic jusqu'à ce que l'intervalle finisse.

Les nombres de seuil de contrôle de tempête du trafic et l'intervalle de temps permettent à l'algorithme de contrôle de tempête du trafic pour fonctionner avec des différents niveaux de finesse. Un seuil plus élevé laisse plus de paquets pour traverser.

Par défaut, le logiciel du système d'exploitation de Cisco Nexus (NX-OS) ne prend aucune action corrective quand le trafic dépasse le niveau configuré. Cependant, vous pouvez configurer un erreur-débranchement inclus d'action de la gestion d'événement (EEM) une interface si le trafic ne s'abaisse pas (baisse au-dessous du seuil) au cours d'un certain délai prévu

Instructions et limites pour le contrôle de tempête du trafic

En configurant le niveau de contrôle de tempête du trafic, notez les instructions et les limites suivantes :

- Vous pouvez configurer le contrôle de tempête du trafic sur une interface de canal de port.
- Ne configurez pas le contrôle de tempête du trafic sur les interfaces qui sont des membres d'une interface de canal de port. En configurant le trafic fulminez le contrôle sur les interfaces qui sont configurées pendant que les membres d'un Port canalisé met les ports dans un état interrompu.
- Spécifiez le niveau comme pourcentage de la bande passante totale de l'interface : Le niveau peut être de 0 à 100. La fraction facultative d'un niveau peut être de 0 à 99. 100 pour cent ne signifient aucun contrôle de tempête du trafic. 0 pour cent suppriment tout le trafic.

En raison des limitations matérielles et de la méthode par lesquelles des paquets de différentes tailles sont comptés, le pourcentage de niveau est une approximation. Selon les tailles des trames qui composent le trafic entrant, l'effectif imposé de niveau pourrait différer du niveau configuré par plusieurs points.

Valeurs par défaut pour le contrôle de tempête du trafic

Paramètres	Par défaut
Contrôle de tempête du trafic	Handicapé
Threshold percentage	100

Configurer le contrôle de tempête du trafic

Vous pouvez placer le pourcentage de la bande passante disponible totale que le trafic commandé peut utiliser.

1. configure terminal
2. interface {emplacement/port d'Ethernets | nombre de Port canalisé}
3. storm-control {émission | Multidiffusion | pourcentage de niveau d'unicast} [.fraction]

Remarque: Le contrôle de tempête du trafic utilise un intervalle 10-millisecond qui peut affecter le comportement du contrôle de tempête du trafic.

Vérifier la configuration de contrôle de tempête du trafic

Pour afficher la tempête du trafic contrôlez les informations de configuration, effectuent une des tâches suivantes :

Commande	But
affichez l'interface [emplacement/port d'Ethernets storm-control de compteurs de nombre de Port canalisé]	Affiche la configuration de contrôle de tempête du trafic pour les interfaces.

interface de show running-config

Affiche la configuration de contrôle de tempête du trafic.

Surveillance des compteurs d'instruction de tempête du trafic

Vous pouvez surveiller les compteurs que le périphérique de Cisco NX-OS met à jour pour l'activité de contrôle de tempête du trafic.

Contrôle de tempête de Nexus 7000 : Sélectionner des valeurs appropriées de suppression

Pour aider la valeur seuil appropriée choisie de client, cette section fournit la vue sur la logique derrière utiliser les valeurs seuil.

Remarque: les informations présentées ici ne fournissent aucun nombre de pratique recommandée mais le client peut arriver à une décision logique après être allé par les informations.

Composants utilisés

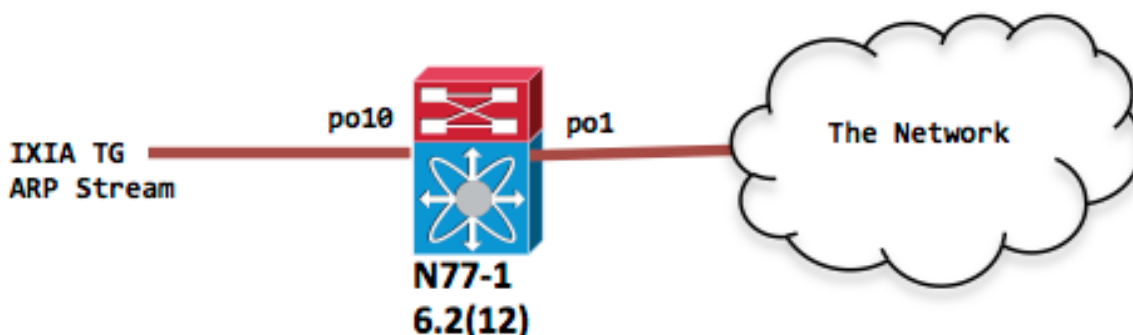
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Nexus 7700 avec la version 6.2.12 et ultérieures.
- Linecard de gamme F3.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Essai en laboratoire

Le contrôle de tempête est un mechnicm de suppression du trafic qui est appliqué au trafic entrant sur un port particulier.



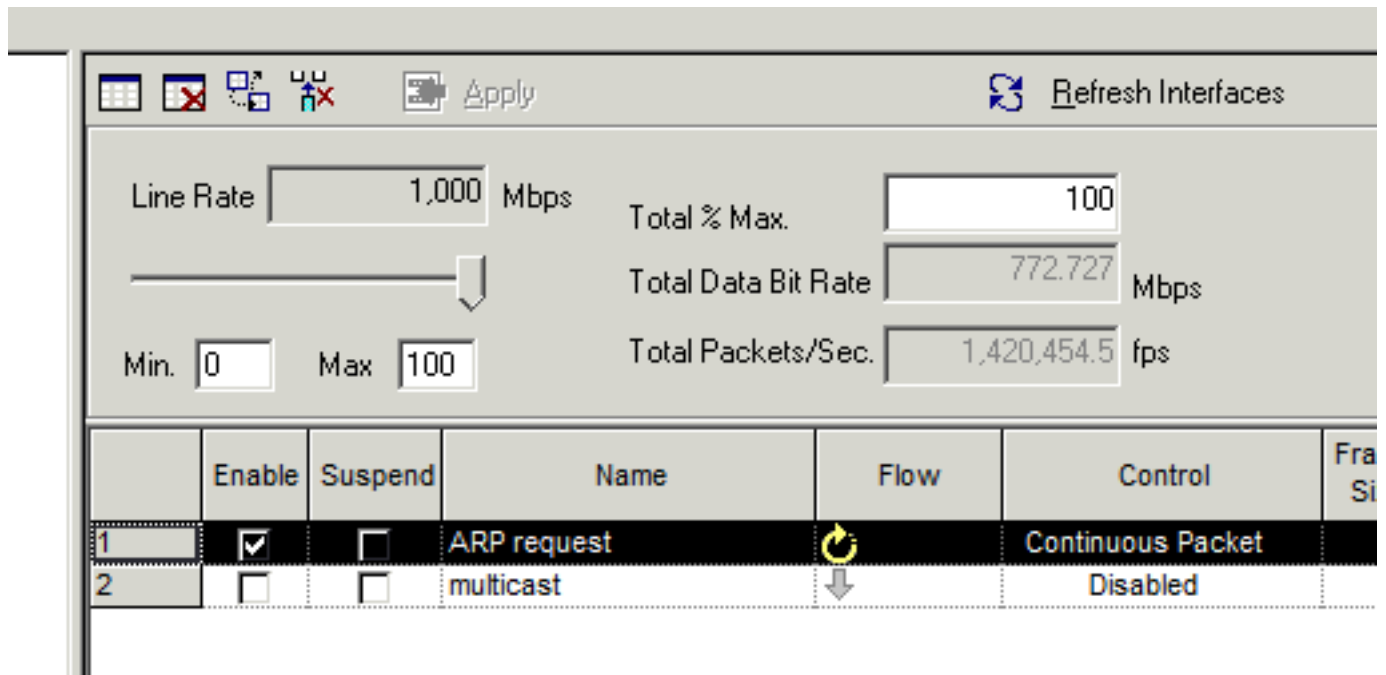
Scenerio 1 : Le débit de Supression est 0.01%



Le débit du trafic entrant est placé à 1Gbps du trafic de demande d'ARP

Config

interface port-channel10
niveau 0.01 d'émission de storm-control

Instantané d'IXIA pour la référence



	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/secinput rate
954.82 Mbps, 1.42 Mpps; output rate 1.97 Kbps, 0 pps N77-1(config-if)# sh int po1 | 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
```

Les baisses de contrôle de tempête sont affichées pour la référence.

Scenerio 2 : Le débit de Supression est 0.1%

Le débit du trafic entrant est placé à 1Gbps du trafic de demande d'ARP

Config

interface port-channel10
niveau 0.10 d'émission de storm-control

Seulement allant afficher l'interface de sortie puisque l'interface d'entrée po10 a le même débit du

trafic entrant de 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
```

Scenerio 3 : Le débit de Supression est 1%

Le débit du trafic entrant est placé à 1Gbps du trafic de demande d'ARP

Config

```
interface port-channel10
```

```
niveau 1 d'émission de storm-control
```

Seulement allant afficher l'interface de sortie puisque l'interface d'entrée po10 a le même débit du trafic entrant de 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
```

Scenerio 4 : Le débit de Supression est 10%

Le débit du trafic entrant est placé à 1Gbps du trafic de demande d'ARP

Config

```
interface port-channel10
```

```
niveau 10.00 d'émission de storm-control
```

```
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
```

Résumé :

Tous les scenerios ci-dessus traitent en raison probablement entraîné soutenu de flux de trafic d'une boucle ou d'un NIC de défaut de fonctionnement. Le contrôle de tempête est efficace dans ce scénario dans la limitation de débit le trafic avant qu'il soit injecté dans le réseau. Les différents niveaux de suppression indiquent que combien de trafic vous injecterez dans votre réseau.

Quand contrôle de tempête est-il en place, ferait-il obtenir l'ARP normal relâché si vous gardez le seuil à un niveau agressif ?

Il y a quelques choses à considérer

1. En premier lieu, si l'ARP obtient la première fois relâchée il y a toujours des relances initiées

par la couche application ainsi la probabilité de l'ARP obtenant résolue pendant des relances ultérieures est plus grande et mènera à l'IP réussi à la résolution de MAC.

2. Le contrôle de tempête est un régulateur d'entrée et il devrait être appliqué aussi étroitement à la périphérie comme possible. Ainsi vous traitant peut-être des hôtes d'un examen médical ou une batterie VM. Si un hôte alors le nombre d'ARPs n'est pas vraiment un problème pendant un scénario fonctionnant normal. Si c'est une batterie VM, alors vous pouvez avoir certain nombre d'hôtes mais de nouveau de rien qui indiquera un domaine entier de la couche 2 derrière un port de périphérie.
3. Si vous appliquez le config de contrôle de tempête sur de principaux ports puis rendez-vous compte de la façon dont le trafic d'émission peut obtenir agrégé avant qu'il atteigne la principale couche.

Aller de retour à nos tests ? pour le trafic ARP bursty ici sont certains des essais

Test 1 : 5000 @ 5000pps éclatés par paquets choisissent la rafale

Niveau 0.01% de Supression

Config

interface port-channel10

niveau 0.01 d'émission de storm-control

```
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-channell1 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

Les expositions ci-dessus 2560 paquets goutte d'ARP. Naturellement, si vous avez 5000 hôtes derrière une interface puis la moitié de eux obtenir pendant la première itération et la deuxième moitié obtiendront pendant le prochain ou ainsi de suite. Si votre application envoie seulement une demande d'ARP d'obtenir l'IP à la résolution de MAC puis l'application peut devoir être modifiée pour retransmettre des demandes d'ARP si aucune réponse. Dans ce cas, contrôle avec le fournisseur d'applications pour l'assistance en changeant ce comportement.

Test 2 : 5000 @ 50000pps éclatés par paquets choisissent la

rafale

Niveau 0.01% de Supression

Config

interface port-channel10

niveau 0.01 d'émission de storm-control

```
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

Dans la sortie ci-dessus il y a un nombre supérieur de baisses dues au débit supérieur de la rafale de paquet.

Des résultats similaires sont vus à mesure que le débit PPS est augmenté pour 5000 @ 100kpps éclatés par paquet jusqu'à un 1 débit de paquets GBP

Les options suivantes sont disponibles pour la détection de l'état de tempête.

Alerte au plan de données :

- En configurant la tempête contrôlez génère le message de Syslog pour des alertes et vous pouvez attacher dans EEM pour générer des déroutements ou l'arrêt de Protocole SNMP (Simple Network Management Protocol) le port comme action préventive.

Alerte à l'avion de contrôle :

- Configurez l'option « en se connectant de baisse seuil » :

Sur le Nexus 7k il y a un policy-map par défaut - contrôle-avion :

Cette carte de stratégie règle que le trafic passe à la CPU. Dans ce policy-map vous pouvez voir une classe qui règle combien d'ARP va à la CPU.

Configurant « se connectant le seuil de baisse » sous cette classe signalera toutes les violations dans le Syslog, vous peut plus loin employer EEM pour générer le déroutement SNMP.

- Interrogation MIB de Réglementation du plan de commande (CoPP)

Commençant dans NX-OS 6.2(2), CoPP prend en charge le MIB basé sur classe de Cisco QoS (cbQoS MIB) et tous ses éléments peuvent être surveillés utilisant le SNMP

Conclusion

Le contrôle de tempête est la fonctionnalité utile qui empêche des interruptions sur des ports de la couche 2 par une émission, une Multidiffusion, ou une tempête du trafic unicast sur des interfaces physiques. Cette caractéristique contrôle la tempête au plan de données avant qu'elle affecte le contrôle-avion et le CoPP.