Contrôle des tempêtes du Nexus 7000 : Sélection des valeurs de suppression appropriées

Contenu

Introduction

Une tempête de trafic se produit lorsque des paquets inondent le réseau local, créant un trafic excessif et dégradant les performances du réseau. Vous pouvez utiliser la fonctionnalité de contrôle des tempêtes de trafic pour empêcher les interruptions sur les ports de couche 2 par une tempête de trafic de diffusion, de multidiffusion ou de monodiffusion sur les interfaces physiques.

Le contrôle des tempêtes de trafic (également appelé suppression du trafic) vous permet de surveiller les niveaux du trafic entrant de diffusion, de multidiffusion et de monodiffusion sur un intervalle de 10 millisecondes. Au cours de cet intervalle, le niveau de trafic, qui est un pourcentage de la bande passante totale disponible du port, est comparé au niveau de contrôle de tempête de trafic que vous avez configuré. Lorsque le trafic d'entrée atteint le niveau de contrôle des tempêtes de trafic configuré sur le port, le contrôle des tempêtes de trafic abandonne le trafic

jusqu'à la fin de l'intervalle.

Les numéros de seuil de contrôle des tempêtes de trafic et l'intervalle de temps permettent à l'algorithme de contrôle des tempêtes de trafic de fonctionner avec différents niveaux de granularité. Un seuil plus élevé permet à plus de paquets de passer.

Par défaut, le logiciel Cisco Nexus Operating System (NX-OS) ne prend aucune mesure corrective lorsque le trafic dépasse le niveau configuré. Cependant, vous pouvez configurer une action EEM (Embedded Event Management) pour désactiver une interface par erreur si le trafic ne subside pas (tombe sous le seuil) dans un délai donné

Directives et limitations pour le contrôle des tempêtes de trafic

Lors de la configuration du niveau de contrôle des tempêtes de trafic, prenez note des consignes et des limitations suivantes :

- Vous pouvez configurer le contrôle des tempêtes de trafic sur une interface port-channel.
- Ne configurez pas le contrôle des tempêtes de trafic sur les interfaces qui sont membres d'une interface port-channel. La configuration du contrôle des tempêtes de trafic sur les interfaces configurées en tant que membres d'un canal de port met les ports en état de suspension.
- Spécifiez le niveau en pourcentage de la bande passante totale de l'interface : Le niveau peut être compris entre 0 et 100.La fraction facultative d'un niveau peut être comprise entre 0 et 99.100 % signifie qu'aucun contrôle de tempête de trafic n'est effectué.0 % supprime tout le trafic.

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

Paramètres par défaut pour le contrôle des tempêtes de trafic

Paramètres	Par défaut
Contrôle des tempêtes de trafic	Désactivé
Pourcentage de seuil	100

Configuration du contrôle des tempêtes de trafic

Vous pouvez définir le pourcentage de bande passante disponible totale que le trafic contrôlé peut utiliser.

1. configurer le terminal
2. interface {ethernet emplacement/port | port-channel nombre}
3. contrôle des tempêtes {diffusion | multidiffusion | monodiffusion} niveau pourcentage[.fraction]

Note: Le contrôle des tempêtes de trafic utilise un intervalle de 10 millisecondes qui peut affecter le comportement du contrôle des tempêtes de trafic.

Vérification de la configuration du contrôle des tempêtes de trafic

Pour afficher les informations de configuration du contrôle de tempête de trafic, effectuez l'une des tâches suivantes :

Commande	Objectif
show interface [ethernet emplacement/port | port-channel nombre] compteur tempête-control	Affiche la configuration du contrôle de temp de trafic pour les interfaces.
show running-config interface	Affiche la configuration du contrôle de temp de trafic.

Surveillance des compteurs de contrôle des tempêtes de trafic

Vous pouvez surveiller les compteurs gérés par le périphérique Cisco NX-OS pour contrôler les tempêtes de trafic.

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

Contrôle des tempêtes du Nexus 7000 : Sélection des valeurs de suppression appropriées

Pour aider le client à sélectionner la valeur de seuil appropriée, cette section fournit des informations sur la logique derrière l'utilisation des valeurs de seuil.

Note: les informations présentées ici ne fournissent aucun numéro de meilleure pratique, mais le client peut prendre une décision logique après avoir examiné les informations.

Components Used

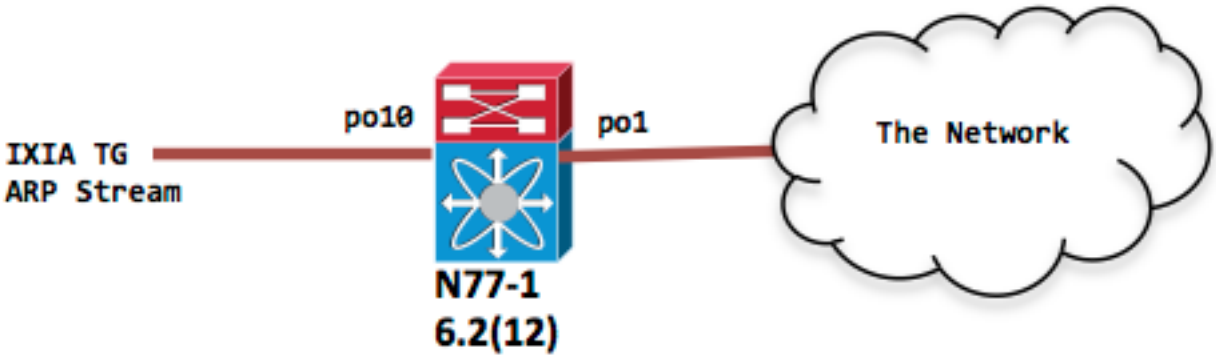
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Nexus 7700 avec les versions 6.2.12 et ultérieures.
- Carte de ligne de la gamme F3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Tests en laboratoire

Le contrôle des tempêtes est un mécanisme de suppression du trafic qui est appliqué au trafic d'entrée sur un port particulier.




```
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
```

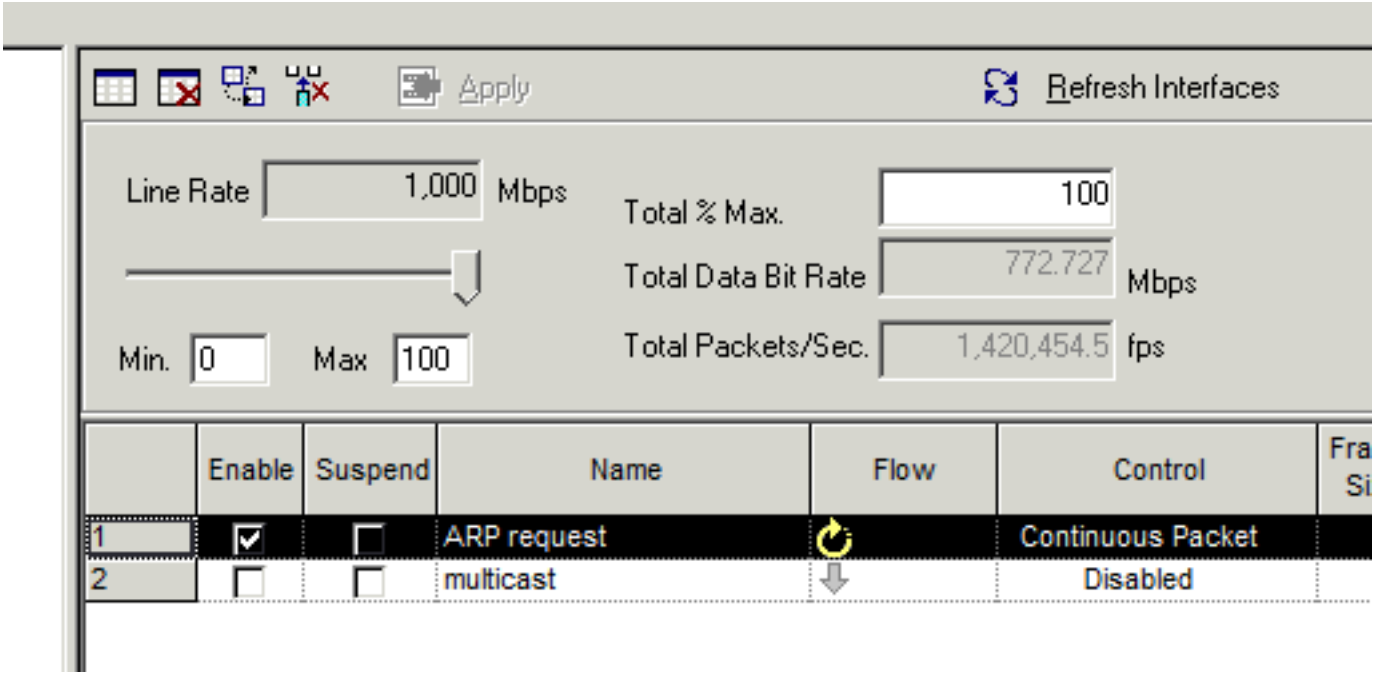
Scenerio 1 : Taux de compression de 0,01 %

Le débit de trafic entrant est défini sur 1 Gbit/s du trafic de requête ARP

configuration

interface port-channel10
niveau de diffusion de contrôle de tempête 0,01

Instantané IXIA de référence




```
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
```

Les chutes de contrôle de tempête sont indiquées à titre de référence.

Scenerio 2 : Taux de compression : 0,1 %

Le débit de trafic entrant est défini sur 1 Gbit/s du trafic de requête ARP

configuration

interface port-channel10
niveau de diffusion de contrôle de tempête 0,10

Uniquement pour afficher l'interface de sortie puisque l'interface d'entrée po10 a le même débit de trafic entrant de 1 Gbit/s

```
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 : Taux de compression de 1 %

Le débit de trafic entrant est défini sur 1 Gbit/s du trafic de requête ARP

configuration

interface port-channel10

niveau de diffusion de contrôle de tempête 1

Uniquement pour afficher l'interface de sortie puisque l'interface d'entrée po10 a le même débit de trafic entrant de 1 Gbit/s

```
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 : Taux de compression de 10 %

Le débit de trafic entrant est défini sur 1 Gbit/s du trafic de requête ARP

configuration

interface port-channel10

niveau de diffusion de contrôle de tempête 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
```

Résumé:

Tous les paysages ci-dessus traitent d'un flux de trafic soutenu qui peut être causé par une boucle ou une carte réseau défectueuse. Le contrôle des tempêtes est efficace dans ce scénario pour limiter le débit du trafic avant son injection dans le réseau. Les différents niveaux de suppression indiquent la quantité de trafic que vous injecterez dans votre réseau.

Lorsque le contrôle des tempêtes est en place, le protocole ARP normal est-il abandonné si vous maintenez le seuil à un niveau agressif ?

Il y a quelques points à considérer

1. Tout d'abord, si ARP est abandonné la première fois, il y a toujours des tentatives initiées par la couche application, de sorte que les chances de résolution ARP lors des tentatives ultérieures sont plus élevées et conduiront à une résolution IP/MAC réussie.
2. Le contrôle des tempêtes est un régulateur d'entrée et il doit être appliqué aussi près que

possible du bord. Vous avez peut-être affaire à un hôte physique ou à un cluster de machines virtuelles. Si un hôte est présent, le nombre d'ARP n'est pas vraiment un problème dans un scénario de travail normal. S'il s'agit d'un cluster de machines virtuelles, il se peut que vous ayez un certain nombre d'hôtes, mais à nouveau rien qui indique un domaine de couche 2 entier derrière un port de périphérie.

3. Si vous appliquez la configuration de contrôle de tempête sur les ports principaux, sachez comment le trafic de diffusion peut être agrégé avant d'atteindre la couche coeur de réseau.

Revenons à nos tests - pour le trafic ARP par salves, voici quelques-uns des tests...

Test 1 : 5 000 paquets ont éclaté à une rafale unique de 5 000 pps

Niveau de compression 0,01 %

configuration

interface port-channel10

niveau de diffusion de contrôle de tempête 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
```

La figure ci-dessus montre 2 560 paquets ARP abandonnés. Bien sûr, si vous avez 5000 hôtes derrière une interface alors la moitié d'entre eux passe par la première itération et la seconde moitié passe par la suivante ou ainsi de suite. Si votre application n'envoie qu'une seule requête ARP pour obtenir la résolution IP vers MAC, il se peut que l'application doive être modifiée pour retransmettre les requêtes ARP en l'absence de réponse. Dans ce cas, demandez de l'aide au fournisseur de l'application pour modifier ce comportement.

Test 2 : 5 000 paquets ont éclaté à une rafale unique de 5 000 pps

Niveau de compression 0,01 %

configuration

interface port-channel10

niveau de diffusion de contrôle de tempête 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
```

Dans le résultat ci-dessus, il y a un nombre plus élevé de pertes en raison du taux plus élevé de rafale de paquets.

Des résultats similaires sont observés lorsque le débit pps est augmenté pour une rafale de paquets de 5 000 à 100 kpps jusqu'à un débit de paquets de 1 gbit/s

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

Alerte au niveau du plan de données :

- La configuration du contrôle de tempête génère un message syslog pour les alertes et vous pouvez lier EEM pour générer des interruptions SNMP (Simple Network Management Protocol) ou arrêter le port en tant qu'action préventive.

Alerte au niveau du plan de contrôle :

- Configurer l'option 'logging drop threshold' :

Sur Nexus 7k, il existe une carte de stratégie par défaut - plan de contrôle :

Cette carte de stratégie régit le trafic qui passe au CPU. Dans cette carte-politique, vous pouvez voir une classe qui régit la quantité d'ARP qui va au CPU.

La configuration de 'logging drop threshold' sous cette classe signalera toute violation dans syslog. Vous pouvez également utiliser EEM pour générer un déroutement SNMP.

- Contrôle de la base MIB (CoPP)

Àpartir de NX-OS 6.2(2), CoPP prend en charge la MIB QoS basée sur les classes Cisco

(cbQoSMIB) et tous ses éléments peuvent être surveillés à l'aide de SNMP

Conclusion

Le contrôle des tempêtes est la fonctionnalité utile qui empêche les interruptions sur les ports de couche 2 par une tempête de trafic de diffusion, de multidiffusion ou de monodiffusion sur les interfaces physiques. Cette fonctionnalité contrôle la tempête au niveau du plan de données avant qu'elle n'affecte le plan de contrôle et CoPP.