Controle de tempestade de mensagens do Nexus 7000: Seleção de valores de supressão apropriados

Contents

Introduction

Uma tempestade de tráfego ocorre quando os pacotes inundam a LAN, criando tráfego excessivo e degradando o desempenho da rede. Você pode usar o recurso de controle de tempestade de tráfego para evitar interrupções nas portas da Camada 2 por uma tempestade de tráfego de broadcast, multicast ou unicast em interfaces físicas.

O controle de tempestade de tráfego (também chamado de supressão de tráfego) permite monitorar os níveis do tráfego de entrada broadcast, multicast e unicast em um intervalo de 10 milissegundos. Durante esse intervalo, o nível de tráfego, que é uma porcentagem da largura de banda total disponível da porta, é comparado ao nível de controle de tempestade de tráfego que você configurou. Quando o tráfego de entrada atinge o nível de controle de tempestade de tráfego

configurado na porta, o controle de tempestade de tráfego descarta o tráfego até que o intervalo termine.

Os números de limite de controle de tempestade de tráfego e o intervalo de tempo permitem que o algoritmo de controle de tempestade de tráfego funcione com diferentes níveis de granularidade. Um limiar mais alto permite que mais pacotes passem.

Por padrão, o software Cisco Nexus Operating System (NX-OS) não executa nenhuma ação corretiva quando o tráfego excede o nível configurado. No entanto, você pode configurar uma ação do Embedded Event Management (EEM) para desativar um erro em uma interface se o tráfego não subtrair (cair abaixo do limite) em um determinado período de tempo

Diretrizes e limitações para controle de tempestade de tráfego

Ao configurar o nível de controle de tempestade de tráfego, observe as seguintes diretrizes e limitações:

- Você pode configurar o controle de tempestade de tráfego em uma interface de canal de porta.
- Não configure o controle de tempestade de tráfego em interfaces que sejam membros de uma interface de canal de porta. Configurar o controle de tempestade de tráfego em interfaces configuradas como membros de um canal de porta coloca as portas em um estado suspenso.
- Especifique o nível como uma porcentagem da largura de banda total da interface: O nível pode ser de 0 a 100.A fração opcional de um nível pode ser de 0 a 99.100% significa que não há controle de tempestade de tráfego.0% suprime todo o tráfego.

Devido às limitações de hardware e ao método pelo qual os pacotes de tamanhos diferentes são contados, a porcentagem de nível é uma aproximação. Dependendo dos tamanhos dos quadros que compõem o tráfego de entrada, o nível de execução real pode diferir do nível configurado por vários pontos percentuais.

Configurações padrão para controle de tempestade de tráfego

Parâmetros	Padrão
Controle de tempestade de tráfego	Desabilitado
Porcentagem de limite	100

Configurando o Controle de Tempestade de Tráfego

Você pode definir a porcentagem da largura de banda total disponível que o tráfego controlado pode usar.

1. configure terminal
2. interface {ethernet slot/porta | Canal de porta número}
3. controle de tempestade {broadcast | multicast | unicast} nível porcentagem[.fração]

Note: O controle de tempestade de tráfego usa um intervalo de 10 milissegundos que pode afetar o comportamento do controle de tempestade de tráfego.

Verificando a Configuração do Controle de Tempestade de Mensagens de Tráfego

Para exibir informações de configuração do controle de tempestade de tráfego, execute uma das seguintes tarefas:

Comando	Propósito
show interface [ethernet slot/porta | Canal de porta número] contadores de controle de tempestade	Exibe a configuração do controle de tempe de tráfego para as interfaces.
show running-config interface	Exibe a configuração do controle de tempe de tráfego.

Monitorando contadores de controle de tempestade de tráfego

Você pode monitorar os contadores que o dispositivo Cisco NX-OS mantém para a atividade de controle de tempestade de tráfego.

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

Controle de tempestade de mensagens do Nexus 7000: Seleção de valores de supressão apropriados

Para ajudar o cliente a selecionar o valor de limite apropriado, esta seção fornece informações sobre a lógica por trás do uso dos valores de limite.

Note: as informações apresentadas aqui não fornecem nenhum número de melhores práticas, mas o cliente pode chegar a uma decisão lógica após analisar as informações.

Componentes Utilizados

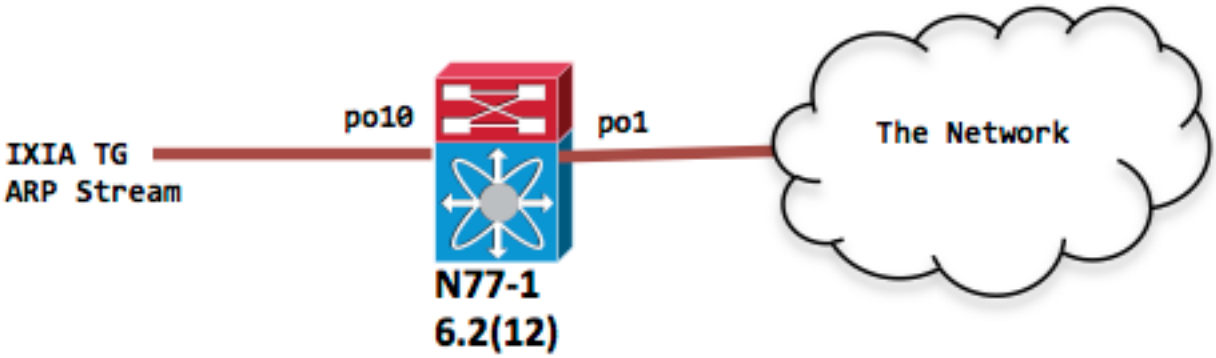
As informações neste documento são baseadas nestas versões de software e hardware:

- Nexus 7700 com versão 6.2.12 e posterior.
- Placa de linha F3 Series.

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.

Teste de laboratório

O controle de tempestade de mensagens é um mecanismo de supressão de tráfego que é aplicado ao tráfego de entrada em uma porta específica.




```
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
```

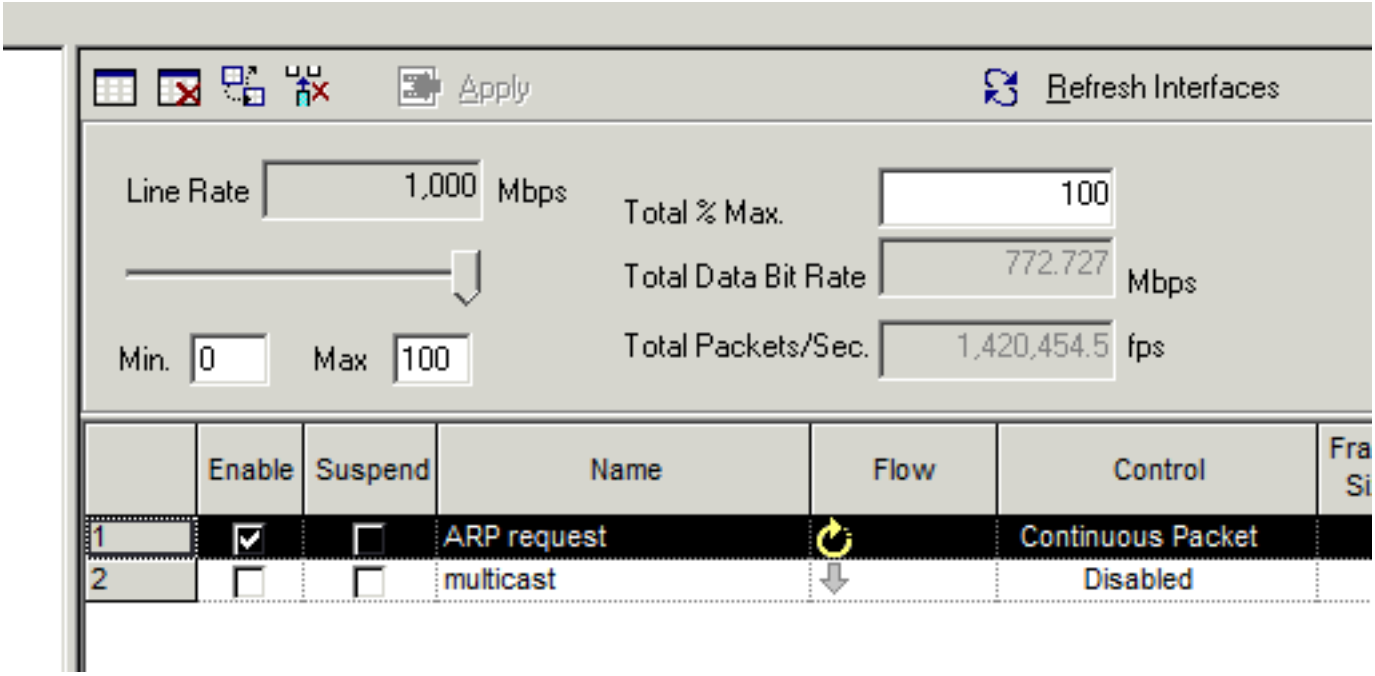
Cenário 1: A taxa de supressão é 0,01%

A taxa de tráfego de entrada está definida como 1 Gbps de tráfego de solicitação ARP

Config

interface port-channel10
nível de transmissão de controle de tempestade 0,01

Instantâneo IXIA para referência




```
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
```

As quedas de controle de tempestade são mostradas para referência.

Cenário 2: A taxa de supressão é 0,1%

A taxa de tráfego de entrada está definida como 1 Gbps de tráfego de solicitação ARP

Config

interface port-channel10
nível de transmissão de controle de tempestade 0,10

Somente mostrando a interface de saída, pois a interface de entrada po10 tem a mesma taxa de tráfego de entrada de 1 gbps

```
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
```

Cenário 3: A taxa de supressão é de 1%

A taxa de tráfego de entrada está definida como 1 Gbps de tráfego de solicitação ARP

Config

interface port-channel10

nível 1 de transmissão de controle de tempestade

Somente mostrando a interface de saída, pois a interface de entrada po10 tem a mesma taxa de tráfego de entrada de 1 gbps

```
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
```

Cenário 4: A taxa de supressão é de 10%

A taxa de tráfego de entrada está definida como 1 Gbps de tráfego de solicitação ARP

Config

interface port-channel10

nível de transmissão de controle de tempestade 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
```

Resumo:

Todos os cenários acima lidam com o fluxo de tráfego sustentado possivelmente causado por um loop ou uma placa de rede defeituosa. O controle de tempestade de mensagens é eficaz neste cenário na taxa de limitação do tráfego antes de ele ser injetado na rede. Os diferentes níveis de supressão indicam a quantidade de tráfego que você vai injetar na sua rede.

Quando o controle de tempestade estiver ativo, o ARP normal será descartado se você manter o limite em um nível agressivo?

Há algumas coisas a considerar

1. Em primeiro lugar, se o ARP for descartado pela primeira vez, sempre haverá novas tentativas iniciadas pela camada de aplicação, de modo que as chances de o ARP ser resolvido durante as novas tentativas subsequentes sejam maiores e levarão a uma resolução de IP para MAC bem-sucedida.

2. O controle de tempestades é um vigilante de ingresso e deve ser aplicado o mais próximo possível da borda. Então, você pode lidar com um host físico ou um cluster de VM. Se um host, o número de ARPs não é realmente um problema durante um cenário de trabalho normal. Se for um cluster de VM, você pode ter um certo número de hosts, mas, novamente, nada que indique um domínio inteiro de camada 2 atrás de uma porta de borda.
3. Se você aplicar a configuração de controle de tempestade em portas centrais, saiba como o tráfego de broadcast pode ser agregado antes de chegar à camada central.

Voltando aos nossos testes - para tráfego ARP em surtos aqui estão alguns dos testes-

Teste 1: rajada de 5.000 pacotes em burst único de 5.000 pps

Nível de depressão 0,01%

Config

interface port-channel10

nível de transmissão de controle de tempestade 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
```

O acima mostra 2560 pacotes ARP descartados. Claro, se você tem 5.000 hosts atrás de uma interface, metade deles passa pela primeira iteração e a segunda metade passa pela próxima. Se seu aplicativo estiver enviando apenas uma solicitação ARP para obter a resolução de IP para MAC, o aplicativo poderá precisar ser modificado para retransmitir solicitações ARP se não houver resposta. Nesse caso, consulte o fornecedor do aplicativo para obter assistência para alterar esse comportamento.

Teste 2: rajada de 5.000 pacotes em burst único de 5.000 pps

Nível de depressão 0,01%

Config

interface port-channel10

nível de transmissão de controle de tempestade 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
```

Na saída acima, há um número maior de descartes devido à taxa mais alta de burst de pacote.

Resultados semelhantes são vistos à medida que a taxa de pps é aumentada para a intermitência de pacote de 5.000 a 100 kpps até uma taxa de pacote de 1 gbps

As seguintes opções estão disponíveis para a detecção da condição de tempestade.

Alerta no plano de dados:

- Configurar o controle de tempestade gera mensagens de syslog para alertas e você pode ligar o EEM para gerar interceptações SNMP (Simple Network Management Protocol) ou desligar a porta como uma ação preventiva.

Alertas no plano de controle:

- Configure a opção 'logging drop threshold':

No Nexus 7k há um mapa de política padrão - plano de controle:

Esse mapa de política está regulando qual tráfego está passando para a CPU. Neste mapa de política, você pode ver uma classe que regula a quantidade de ARP que vai para a CPU.

A configuração do 'limite de queda de registro' nesta classe reportará quaisquer violações no syslog. Você pode ainda usar o EEM para gerar armadilha SNMP.

- Polling MIB de plano de controle (CoPP)

A partir do NX-OS 6.2(2), o CoPP suporta o MIB de QoS baseado em classe da Cisco (cbQoSMIB) e todos os seus elementos podem ser monitorados usando SNMP

Conclusão

O Controle de Tempestade de Mensagens é o recurso útil que evita interrupções nas portas da

Camada 2 por uma tempestade de tráfego de broadcast, multicast ou unicast em interfaces físicas. Esse recurso controla a tempestade no plano de dados antes que afete o plano de controle e o CoPP.