Controllo Nexus 7000 Storm: Selezione dei valori di soppressione appropriati

Sommario

Introduzione

Quando i pacchetti inondano la LAN, si verifica una tempesta di traffico che provoca traffico eccessivo e prestazioni di rete ridotte. È possibile utilizzare la funzione di controllo della tempesta di traffico per impedire interruzioni sulle porte di livello 2 da parte di una tempesta di traffico broadcast, multicast o unicast su interfacce fisiche.

Il controllo dell'urto del traffico (detto anche soppressione del traffico) consente di monitorare i livelli del traffico in ingresso, broadcast, multicast e unicast su un intervallo di 10 millisecondi. Durante questo intervallo, il livello del traffico, che è una percentuale della larghezza di banda totale disponibile della porta, viene confrontato con il livello di controllo della tempesta di traffico configurato. Quando il traffico in entrata raggiunge il livello di controllo della tempesta di traffico configurato sulla porta, il controllo della tempesta di traffico scarta il traffico fino al termine dell'intervallo.

I numeri di soglia di controllo della tempesta di traffico e l'intervallo di tempo consentono all'algoritmo di controllo della tempesta di traffico di funzionare con diversi livelli di granularità. Una soglia più alta consente il passaggio di un numero maggiore di pacchetti.

Per impostazione predefinita, il software Cisco Nexus Operating System (NX-OS) non esegue alcuna azione correttiva quando il traffico supera il livello configurato. Tuttavia, è possibile configurare un'azione EEM (Embedded Event Management) per disabilitare a causa di un errore un'interfaccia se il traffico non si interrompe (scende al di sotto della soglia) entro un determinato periodo di tempo

Linee guida e limitazioni per il controllo delle tempeste di traffico

Quando si configura il livello di controllo della tempesta di traffico, tenere presenti le linee guida e le limitazioni riportate di seguito.

- Èpossibile configurare il controllo della tempesta di traffico su un'interfaccia di canale porta.
- Non configurare il controllo della tempesta di traffico sulle interfacce che sono membri di un'interfaccia porta-canale. Configurando il controllo della tempesta di traffico sulle interfacce configurate come membri di un canale di porta, le porte vengono messe in stato sospeso.
- Specificare il livello come percentuale della larghezza di banda totale dell'interfaccia: Il livello può essere compreso tra 0 e 100.La frazione facoltativa di un livello può essere compresa tra 0 e 99.Il 100% significa nessun controllo della tempesta di traffico.0% elimina tutto il traffico.

A causa delle limitazioni hardware e del metodo con cui vengono conteggiati i pacchetti di dimensioni diverse, la percentuale del livello è un'approssimazione. A seconda delle dimensioni dei frame che costituiscono il traffico in entrata, il livello effettivo imposto potrebbe differire dal livello configurato di diversi punti percentuali.

Impostazioni predefinite per il controllo Traffic Storm

Parametri	Predefinito
Controllo della tempesta	Disattivato
Percentuale soglia	100

Configurazione di Traffic Storm Control

Èpossibile impostare la percentuale della larghezza di banda totale disponibile che può essere utilizzata dal traffico controllato.

1. configurare il terminale
2. interfaccia {ethernet slot/port | port-channel numero}
3. controllo temporale {trasmissione | multicast | unicast} livello percentuale[.frazione]

Nota: Il controllo Traffic Storm utilizza un intervallo di 10 millisecondi che può influire sul comportamento del controllo Traffic Storm.

Verifica della configurazione di Traffic Storm Control

Per visualizzare le informazioni di configurazione del controllo Traffic Storm, eseguire una delle attività seguenti:

Comando	Scopo
show interface [ethernet slot/port | port-channel numero] contatori controllo tempesta	Visualizza la configurazione di controllo della tempesta di traffico per le interfacce.
show running-config interface	Visualizza la configurazione di controllo della tempesta di traffico.

Monitoraggio dei contatori di controllo Traffic Storm

Èpossibile monitorare i contatori gestiti dal dispositivo Cisco NX-OS per l'attività di controllo della tempesta di traffico.

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

Controllo Nexus 7000 Storm: Selezione dei valori di soppressione appropriati

Per aiutare il cliente a selezionare il valore di soglia appropriato, questa sezione fornisce informazioni dettagliate sulla logica alla base dell'utilizzo dei valori di soglia.

Nota: le informazioni presentate non forniscono alcun numero di best practice, ma il cliente può arrivare a una decisione logica dopo aver esaminato le informazioni.

Componenti usati

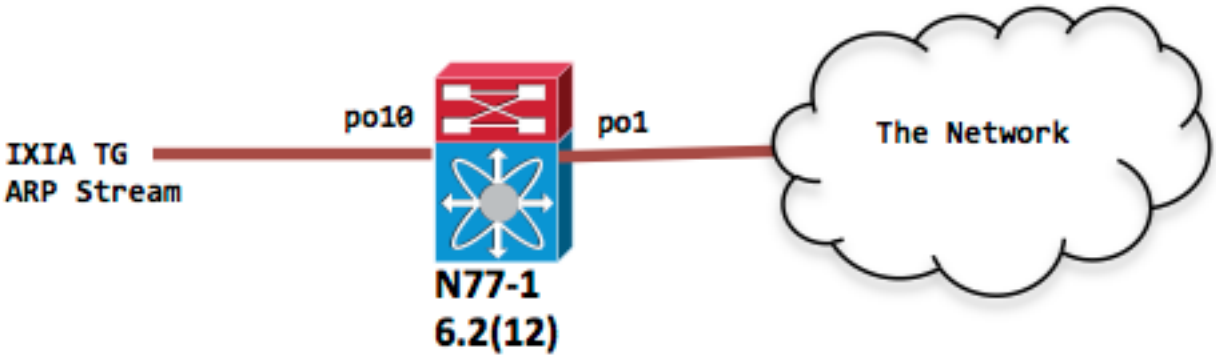
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Nexus 7700 con versione 6.2.12 e successive.
- Scheda di linea serie F3.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Test di laboratorio

Il controllo delle tempeste è un meccanismo di soppressione del traffico che viene applicato al traffico in entrata su una particolare porta.




```
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
```

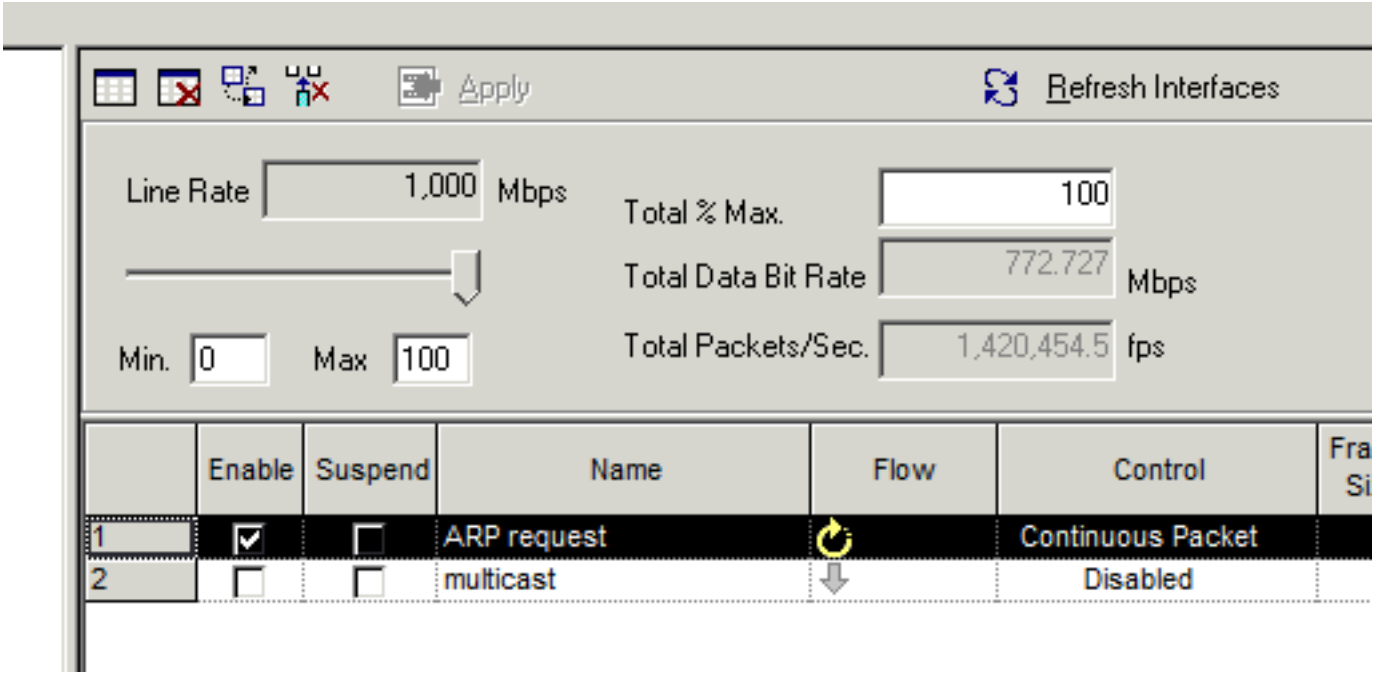
Scenario 1: Il tasso di soppressione è 0,01%

La velocità del traffico in entrata è impostata su 1 Gbps di traffico di richiesta ARP

Config

interface port-channel 10
controllo temporale livello broadcast 0,01

Snapshot IXIA per riferimento




```
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
```

Le gocce di controllo della tempesta vengono mostrate come riferimento.

Scenario 2: Il tasso di soppressione è 0,1%

La velocità del traffico in entrata è impostata su 1 Gbps di traffico di richiesta ARP

Config

interface port-channel 10
controllo temporale livello broadcast 0.10

Verrà mostrata solo l'interfaccia in uscita poiché l'interfaccia in entrata po10 ha la stessa velocità di traffico in entrata di 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
```

Scenario 3: Tasso di soppressione è 1%

La velocità del traffico in entrata è impostata su 1 Gbps di traffico di richiesta ARP

Config

interface port-channel 10

controllo temporale broadcast livello 1

Verrà mostrata solo l'interfaccia in uscita poiché l'interfaccia in entrata po10 ha la stessa velocità di traffico in entrata di 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
```

Scenario 4: Tasso di soppressione: 10%

La velocità del traffico in entrata è impostata su 1 Gbps di traffico di richiesta ARP

Config

interface port-channel 10

controllo temporale broadcast level 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
```

Riepilogo:

In tutti gli scenari sopra riportati il flusso di traffico sostenuto potrebbe essere causato da un loop o da una scheda NIC non funzionante. Il controllo delle tempeste è efficace in questo scenario in quanto limita la velocità del traffico prima che venga iniettato nella rete. I diversi livelli di eliminazione indicano la quantità di traffico che verrà iniettata nella rete.

Quando il controllo della tempesta è in posizione, causerebbe la caduta del normale ARP se si mantiene la soglia a un livello aggressivo?

Ci sono alcune cose da considerare

1. In primo luogo, se ARP viene eliminato per la prima volta, ci sono sempre tentativi avviati dal livello dell'applicazione, quindi le probabilità che ARP venga risolto durante i tentativi successivi sono maggiori e porteranno ad una risoluzione IP-MAC corretta.
2. Il controllo della tempesta è un sistema di controllo in entrata che deve essere applicato il più

vicino possibile al bordo. È quindi possibile gestire un host fisico o un cluster di VM. Se si utilizza un solo host, il numero di ARP non costituisce un problema in uno scenario di lavoro normale. Se si tratta di un cluster di VM, è possibile che sia presente un certo numero di host, ma anche in questo caso nulla che indichi un intero dominio di livello 2 dietro una porta edge.

3. Se si applica la configurazione del controllo di temporizzazione alle porte principali, è necessario essere consapevoli di come il traffico di trasmissione possa essere aggregato prima che raggiunga il livello principale.

Tornando ai nostri test - per traffico ARP bursty qui sono alcuni dei test-

Test 1: burst di 5000 pacchetti a 5000 p/s (single burst)

Livello di soppressione 0,01%

Config

interface port-channel 10

controllo temporale livello broadcast 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
```

Quanto sopra mostra 2560 pacchetti ARP scartati. Naturalmente, se si hanno 5000 host dietro un'interfaccia, la metà di essi passerà durante la prima iterazione e la seconda metà durante la successiva. Se l'applicazione invia una sola richiesta ARP per ottenere la risoluzione IP-MAC, potrebbe essere necessario modificare l'applicazione per ritrasmettere le richieste ARP in assenza di risposta. In questo caso, richiedere assistenza al fornitore dell'applicazione per modificare questo comportamento.

Test 2: burst di 5000 pacchetti a 50000 p/s (single burst)

Livello di soppressione 0,01%

Config

interface port-channel 10

controllo temporale livello broadcast 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
```

Nell'output di cui sopra è presente un numero maggiore di perdite dovute alla maggiore velocità di burst dei pacchetti.

Risultati simili si vedono come la velocità in pps viene aumentata per burst di pacchetti 5000 a 100 kpps fino a una velocità in pacchetti di 1 gbps

Per il rilevamento della condizione di tempesta sono disponibili le opzioni seguenti.

Avvisi al piano dati:

- La configurazione del controllo della temporizzazione genera un messaggio syslog per gli allarmi ed è possibile collegare EEM per generare trap SNMP (Simple Network Management Protocol) o chiudere la porta come misura preventiva.

Avvisi al piano di controllo:

- Configurare l'opzione 'soglia di rilascio log':

Su Nexus 7k è disponibile una mappa-politica - control-plane predefinita:

Questa mappa dei criteri regola il traffico che passa alla CPU. All'interno di questa mappa delle policy è possibile vedere una classe che regola quanto ARP va alla CPU.

Configurando 'logging drop threshold' sotto questa classe verranno segnalate eventuali violazioni in syslog. È possibile utilizzare EEM per generare trap SNMP.

- Polling MIB Control Plane Policing (CoPP)

A partire da NX-OS 6.2(2), CoPP supporta Cisco Class-Based QoS MIB (cbQoSMIB) e tutti i suoi elementi possono essere monitorati tramite SNMP

Conclusioni

Il controllo delle tempeste è una funzione utile che previene le interruzioni sulle porte di layer 2 causate da un traffico broadcast, multicast o unicast su interfacce fisiche. Questa funzione controlla la tempesta sul piano dati prima che impatti sul piano di controllo e sul CoPP.