

# Nexus 7000: Funktion "Hardware-IP-Glean-Throttle" verstehen

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Labortest](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie die **Hardware-Funktion ip glean throttle** mit Beispielen funktioniert und wie diese Funktion beabsichtigt ist.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse der Konfiguration von Nexus Switches der Serie 7000 verfügen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Nexus 7000 mit Version 6.2.x und höher
- F2e-Line Card

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Hintergrundinformationen

Wenn Sie ein eingehendes IP-Paket in einer Linecard weiterleiten und die ARP-Anforderung (Address Resolution Protocol) für den nächsten Hop nicht aufgelöst wird, leitet die Linecard die Pakete an den Supervisor weiter, um eine ARP-Anforderung zu generieren. Wenn die ARP-Anforderung an den Supervisor antwortet, löst sie die MAC-Adresse für den nächsten Hop auf und programmiert die Hardware.

Wenn der Supervisor den ARP-Eintrag nicht auflösen kann, sendet die Linecard alle an diese Adresse gerichteten Pakete an den Supervisor. Der Supervisor generiert ARP-Anfragen auf unbestimmte Zeit, bis der ARP-Eintrag aufgelöst ist. Es gibt einen Hardware-Ratenlimiter namens "Glean", der platziert wurde, um den Prozessor (CPU) des Supervisors vor übermäßigem Datenverkehr zu schützen.

Ein Problem, das auftreten kann, ist, dass eine einzelne Ziel-IP aufgrund von Wartungsarbeiten oder Hardwareproblemen aus dem Netzwerk fällt und plötzlich der gesamte für sie bestimmte Datenverkehr an die CPU gesendet wird. Da der Durchsatzbegrenzer vorhanden ist, wird die CPU nicht erhöht, aber diese eine Ziel-IP-Adresse kann den gesamten Durchsatzbegrenzer nutzen und anderen legitimen IP-Adressen keinen Zugriff auf die CPU gewähren. Für dieses Szenario wurde **Hardware-IP-Glean-Throttle** erstellt.

Bei der Konfiguration der **Hardware-IP-Glean-Throttle** erreicht der geroutete Datenverkehr für jede unbekannte Ziel-IP die Aktion des Hardware Rate Limiter (HWRL) für die ARP-Auflösung nach dem Start der CPU. Nicht erreichbares Ziel führt zu einer /32-Drop-Adjacency, die in der Hardware erstellt wird. Dadurch wird verhindert, dass zusätzliche Pakete an dieselbe Next-Hop-IP-Adresse an den Supervisor weitergeleitet werden. Beim Hinzufügen dieser Drop-Adjacency werden die nachfolgenden Pakete verworfen, aber der Supervisor generiert weiterhin ARP-Anforderungen, bis der nächste Hop aufgelöst ist. Die Drop-Adjacency wird für einen kurzen Zeitraum installiert, der konfigurierbar ist. Sobald der Timer abläuft, wird ein Paket erneut an die CPU gesendet, und der Vorgang wiederholt sich. Die Anzahl der auf diese Weise installierten Einträge ist standardmäßig auf 1000 beschränkt, kann jedoch auf eine größere Anzahl gewünschter Einträge konfiguriert werden. Dadurch sollen die Auswirkungen auf die Größe der RIB-Tabelle (Routing Information Base) begrenzt werden.

## Labortest

In diesem Fall haben Sie einen Server, 172.28.191.200, der aufgrund eines Hardwarefehlers ausgefallen ist und derzeit für den Dienstverkehr nicht verfügbar ist.

**Anmerkung:** Es gibt keinen ARP-Eintrag für den Host, und es wird keine Adjacency erstellt.

```
N7K# show ip route vrf VRF_ABC 172.28.191.200
IP Route Table for VRF "VRF_ABC"
 '*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>

172.28.191.192/28, ubest/mbest: 1/0, attached >>> There is no /32 entry
  *via 172.28.191.195, Vlan1601, [0/0], 02:01:17, direct
```

Der Datenverkehr wird an den Supervisor gesendet, um eine ARP-Anforderung zu generieren:

```
N7K# show system internal forwarding vrf VRF_ABC ipv4 route 172.28.191.200 detail
slot 1
=====
RPF Flags legend:
  S - Directly attached route (S_Star)
```

```

V - RPF valid
M - SMAC IP check enabled
G - SGT valid
E - RPF External table valid
172.28.191.192/28 , sup-eth2
Dev: 0 , Idx: 0x65fb , Prio: 0x8487 , RPF Flags: VS , DGT: 0 , VPN: 9
RPF_Intf_5: Vlan1601 (0x19 )
AdjIdx: 0x5a , LIFB: 0 , LIF: sup-eth2 (0x1fe1 ), DI: 0xc01
DMAC: 0000.0000.0000 SMAC: 0000.0000.0000
172.28.191.192/28 , sup-eth2
Dev: 1 , Idx: 0x65fb , Prio: 0x8487 , RPF Flags: VS , DGT: 0 , VPN: 9
RPF_Intf_5: Vlan1601 (0x19 )
AdjIdx: 0x5a , LIFB: 0 , LIF: sup-eth2 (0x1fe1 ), DI: 0xc01
DMAC: 0000.0000.0000 SMAC: 0000.0000.0000
172.28.191.192/28 , sup-eth2
Dev: 2 , Idx: 0x65fb , Prio: 0x8487 , RPF Flags: VS , DGT: 0 , VPN: 9
RPF_Intf_5: Vlan1601 (0x19 )
AdjIdx: 0x5a , LIFB: 0 , LIF: sup-eth2 (0x1fe1 ), DI: 0xc01
DMAC: 0000.0000.0000 SMAC: 0000.0000.0000
172.28.191.192/28 , sup-eth2
Dev: 5 , Idx: 0x65f1 , Prio: 0x84f2 , RPF Flags: VS , DGT: 0 , VPN: 9
RPF_Intf_5: Vlan1601 (0x19 )
AdjIdx: 0x5a , LIFB: 0 , LIF: sup-eth2 (0x1fe1 ), DI: 0xc01
DMAC: 0000.0000.0000 SMAC: 0000.0000.0000

```

Der Durchsatzbegrenzer "Glean" für das jeweilige Modul drosselt den Datenverkehr auf 100 Pakete pro Sekunde pro Modul. Sie können sehen, dass einige Pakete verworfen werden.

```

N7K# show hardware rate-limiter
Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters
rl-1: STP and Fabricpath-ISIS
rl-2: L3-ISIS and OTV-ISIS
rl-3: UDLD, LACP, CDP and LLDP
rl-4: Q-in-Q and ARP request
rl-5: IGMP, NTP, DHCP-Snoop, Port-Security, Mgmt and Copy traffic

```

```

Module: 1

```

R-L Class	Config	Allowed	Dropped	Total
L3 mtu	500	0	0	0
L3 ttl	500	0	0	0
L3 control	10000	0	0	0
<b>L3 glean</b>	<b>100</b>	<b>3326</b>	<b>3190</b>	<b>6516</b>
L3 mcast dirconn	3000	0	0	0
L3 mcast loc-grp	3000	0	0	0
L3 mcast rpf-leak	500	0	0	0
L2 storm-ctrl	Disable			
access-list-log	100	0	0	0
copy	30000	1877	0	1877
receive	30000	318	0	318

Wenn der Befehl `hardware ip glean throttle` konfiguriert ist:

```
N7K(config)#hardware ip glean throttle
```

Eine Adjacency wird in der RIB installiert:

```

N7K# show ip route 172.28.191.200 vrf VRF-ABC
IP Route Table for VRF "VRF-ABC"
'*' denotes best ucast next-hop

```

'\*\*' denotes best mcast next-hop  
'[x/y]' denotes [preference/metric]  
'%<string>' in via output denotes VRF <string>

172.28.191.200/32, ubest/mbest: 1/0, attached  
\*via 172.28.191.200, Vlan1601, [250/0], 00:01:37, am

Wenn Sie sich die Hardwareprogrammierung ansehen, wird ein Dropindex installiert:

N7K# show system internal forwarding vrf VRF\_ABC ipv4 route 172.28.191.200 detail

slot 1  
=====

RPF Flags legend:

S - Directly attached route (S\_Star)  
V - RPF valid  
M - SMAC IP check enabled  
G - SGT valid  
E - RPF External table valid

172.28.191.200/32 , Drop

Dev: 0 , Idx: 0x1a5 , Prio: 0x8b61 , RPF Flags: VS , DGT: 0 , VPN: 9

RPF\_Intf\_5: Vlan1601 (0x19 )

AdjIdx: 0x8913 , LIFB: 0 , **LIF: Drop** (0x0 ) , DI: 0x0

DMAC: 0000.0000.0000 SMAC: 0000.0000.0000

172.28.191.200/32 , Drop

Dev: 1 , Idx: 0x1a5 , Prio: 0x8b61 , RPF Flags: VS , DGT: 0 , VPN: 9

RPF\_Intf\_5: Vlan1601 (0x19 )

AdjIdx: 0x8913 , LIFB: 0 , **LIF: Drop** (0x0 ) , DI: 0x0

DMAC: 0000.0000.0000 SMAC: 0000.0000.0000

172.28.191.200/32 , Drop

Dev: 2 , Idx: 0x1a5 , Prio: 0x8b61 , RPF Flags: VS , DGT: 0 , VPN: 9

RPF\_Intf\_5: Vlan1601 (0x19 )

AdjIdx: 0x8913 , LIFB: 0 , **LIF: Drop** (0x0 ) , DI: 0x0

DMAC: 0000.0000.0000 SMAC: 0000.0000.0000

172.28.191.200/32 , Drop

Dev: 5 , Idx: 0x1e1 , Prio: 0x88ee , RPF Flags: VS , DGT: 0 , VPN: 9

RPF\_Intf\_5: Vlan1601 (0x19 )

AdjIdx: 0x8914 , LIFB: 0 , **LIF: Drop** (0x0 ) , DI: 0x0

DMAC: 0000.0000.0000 SMAC: 0000.0000.0000

Sie können nun sehen, dass der Hardware-Ratenlimiter keine Heruntergefallenen erkennt.

N7K# show hardware rate-limiter

Units for Config: packets per second

Allowed, Dropped & Total: aggregated since last clear counters

rl-1: STP and Fabricpath-ISIS

rl-2: L3-ISIS and OTV-ISIS

rl-3: UDLD, LACP, CDP and LLDP

rl-4: Q-in-Q and ARP request

rl-5: IGMP, NTP, DHCP-Snoop, Port-Security, Mgmt and Copy traffic

Module: 1

R-L Class	Config	Allowed	Dropped	Total
L3 mtu	500	0	0	0
L3 ttl	500	0	0	0
L3 control	10000	0	0	0
<b>L3 glean</b>	<b>100</b>	<b>0</b>	<b>0</b>	<b>0</b>
L3 mcast dirconn	3000	0	0	0

L3 mcast loc-grp	3000	0	0	0
L3 mcast rpf-leak	500	0	0	0
L2 storm-ctrl	Disable			
access-list-log	100	0	0	0
copy	30000	1877	0	1877
receive	30000	318	0	318

## Zugehörige Informationen

- [Konfigurieren der IP-Glean-Einschränkung](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.