Überprüfen von Verstößen gegen das Control Plane Policing auf Nexus-Plattformen

Inhalt

Einleitung

In diesem Dokument werden Details zum Control Plane Policing (CoPP) für Cisco Nexus-Switches und deren relevante Auswirkungen auf nicht standardmäßige Klassenverletzungen beschrieben.

Voraussetzungen

Cisco empfiehlt, grundlegende Informationen über CoPP (Control Plane Policing), Richtlinien und Einschränkungen sowie die allgemeine Konfiguration zu verstehen. sowie Funktionen für die Quality of Service (QoS)-Richtlinienvergabe (CIR). Weitere Informationen zu dieser Funktion finden Sie in den entsprechenden Dokumenten:

https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/Security/cisco-nexus-9000-nx-os-security-configuration-guide-102x/m-configuring-copp.html

https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/116043-copp-nexus7000-tshoot-00.html

https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/qos/cisco-nexus-9000-nx-os-quality-of-service-configuration-guide-102x/m-configuring-policing.html

Verwendete Komponenten

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 Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Der Datenverkehr auf Kontrollebene wird an das Supervisor-Modul umgeleitet, indem Zugriffskontrolllisten (ACLs) umgeleitet werden, die so programmiert sind, dass der entsprechende Datenverkehr, der durch zwei Schutzebenen geleitet wird, die Hardware-Ratenlimitierungen und CoPP. Störungen oder Angriffe auf das Supervisor-Modul können, wenn sie nicht kontrolliert werden, zu schwerwiegenden Netzwerkausfällen führen. CoPP dient somit als Schutzmechanismus. Bei Instabilität auf Kontrollebene ist es wichtig, CoPP zu überprüfen, da anormale Datenverkehrsmuster, die durch Schleifen oder Überschwemmungen erzeugt werden, oder nicht autorisierte Geräte den Supervisor an der Verarbeitung von legitimem Datenverkehr hindern können. Solche Angriffe, die entweder versehentlich von unberechtigten Geräten oder böswillig von Angreifern verübt werden können, führen in der Regel zu einer hohen Datenverkehrsrate, die für das Supervisor-Modul oder die CPU bestimmt ist.

Control Plane Policing (CoPP) ist eine Funktion, die die Kontrollebene schützt, indem alle über die In-Band (Vorderseite)-Ports empfangenen Pakete, die für die Router-Adressen bestimmt sind oder die eine Einbeziehung des Supervisors erfordern, isoliert und klassifiziert werden. Diese Pakete werden auf der Grundlage einer bestätigten Eingangsrate (CIR) überwacht. Mit dieser Funktion kann eine Richtlinienzuordnung auf die Kontrollebene angewendet werden. Diese Richtlinienzuordnung ähnelt einer normalen Quality of Service (QoS)-Richtlinie und wird auf den gesamten Datenverkehr angewendet, der von einem Nicht-Management-Port in den Switch gelangt. Der Schutz des Supervisor-Moduls durch Richtlinienvergabe ermöglicht dem Switch die Eindämmung von Datenverkehrsspitzen, die über die für jede Klasse festgelegten Eingangsraten hinausgehen, indem die Pakete verworfen werden und verhindert wird, dass der Switch überlastet wird und die Leistung beeinträchtigt.

Es ist wichtig, die CoPP-Zähler fortlaufend zu überwachen und zu rechtfertigen. Dies ist der Zweck dieses Dokuments. Wenn CoPP-Verletzungen nicht aktiviert sind, kann die Kontrollebene verhindern, dass echter Datenverkehr in der entsprechenden betroffenen Klasse verarbeitet wird. Die CoPP-Konfiguration ist ein dynamischer und fortlaufender Prozess, der auf die Netzwerk- und Infrastrukturanforderungen reagieren muss. Es gibt drei Standardsystemrichtlinien für CoPP. Cisco empfiehlt standardmäßig die Verwendung der Standardrichtlinie "**strict**" als Ausgangspunkt und wird als Grundlage für dieses Dokument verwendet.

CoPP gilt nur für In-Band-Datenverkehr, der über die Ports an der Vorderseite eingeht. Der Out-of-Band-Management-Port (mgmt0) unterliegt nicht CoPP. Die Cisco NX-OS-Gerätehardware führt CoPP pro Weiterleitungs-Engine durch. Wählen Sie deshalb Übertragungsraten aus, damit der aggregierte Datenverkehr das Supervisor-Modul nicht überlastet. Dies ist besonders wichtig für End-of-Row/Modular Switches, da die CIR für den gesamten Datenverkehr des CPU-gebundenen Datenverkehrs aller Module gilt.

Anwendbare Hardware

Die in diesem Dokument behandelte Komponente gilt für alle Cisco Nexus-Switches für Rechenzentren.

Interpretation von Control Plane Policing

Der Schwerpunkt dieses Dokuments liegt auf den häufigsten und kritischsten nicht standardmäßigen Klassenverletzungen, die auf Nexus-Switches aufgetreten sind.

Standard-CoPP-Standardprofil

Um zu verstehen, wie CoPP interpretiert werden kann, muss zuerst überprüft werden, ob ein Profil angewendet wird und ob ein Standardprofil oder ein benutzerdefiniertes Profil auf den Switch angewendet wird.

> **Anmerkung:** Als Best Practice muss für alle Nexus-Switches CoPP aktiviert sein. Wenn diese Funktion nicht aktiviert ist, kann sie Instabilität für den gesamten Datenverkehr auf Kontrollebene verursachen, da verschiedene Plattformen den SUP-gebundenen Datenverkehr (Supervisor) einschränken können. Wenn CoPP beispielsweise auf einem Nexus 9000 nicht aktiviert ist, ist die Datenverkehrsrate für SUP auf 50 pps beschränkt, wodurch der Switch nahezu funktionsunfähig wird. CoPP gilt als Voraussetzung für Nexus 3000- und Nexus 9000-Plattformen.

Wenn CoPP nicht aktiviert ist, kann es auf dem Switch erneut aktiviert oder konfiguriert werden, indem der Befehl **"setup"** ausgeführt wird oder eine der Standardrichtlinien unter der Konfigurationsoption angewendet wird: **copp-Profil [dense|lenient|moderate|strict]**.

Ein ungeschütztes Gerät klassifiziert und trennt Datenverkehr nicht ordnungsgemäß in Klassen. Daher ist jedes Diensteverweigerungsverhalten für eine bestimmte Funktion oder ein bestimmtes Protokoll nicht in diesem Bereich enthalten und kann sich auf die gesamte Kontrollebene auswirken.

> **Anmerkung:** CoPP-Richtlinien werden durch Umleitungen der Ternary Content-Addressable Memory (TCAM)-Klassifizierung implementiert. Sie sind direkt unter dem **internen Eingabestatistik-Modul X** des **Systems** zu sehen. **| b CoPP'** oder '**show hardware access-list input entries detail**'.

N9K1# show copp status Last Config Operation: None Last Config Operation Timestamp: None Last Config Operation Status: None Policy-map attached to the control-plane: copp-system-p-policy-strict copp-system-p-policy-strict is one of the system default

profiles, in particular the strict profile. N9K1# show running-config copp !Command: show running-config copp !Running configuration last done at: Tue Apr 26 16:34:10 2022 !Time: Sun May 1 16:30:57 2022 version 10.2(1) Bios:version 05.45 copp profile strict

Control Plane Policing-Klassen

CoPP klassifiziert Datenverkehr anhand der Übereinstimmungen, die den IP- oder MAC-ACLs entsprechen. Daher ist es wichtig zu verstehen, welcher Datenverkehr unter welcher Klasse klassifiziert wird.

Die plattformabhängigen Klassen können variieren. Daher ist es wichtig zu verstehen, wie die Klassen überprüft werden.

Beispiel für **Nexus 9000** Top-of-Rack (TOR):

```
N9K1# show policy-map interface control-plane
Control Plane

Service-policy input: copp-system-p-policy-strict
...
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
...
```

In diesem Beispiel umfasst die Klassenzuordnung **copp-system-p-class-critical** Datenverkehr im Zusammenhang mit Routing-Protokollen wie Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Router Protocol (EIGRP) und weitere Protokolle wie vPC.

Die Namenskonvention für IP- oder MAC-ACLs ist größtenteils selbsterklärend für das verwendete Protokoll oder die zugehörige Funktion, mit dem Präfix **copp-system-p-acl-[protocol|feature]**.

Um eine bestimmte Klasse anzuzeigen, kann sie direkt angegeben werden, während der Befehl show ausgeführt wird. Beispiele:

```
N9K-4# show policy-map interface control-plane class copp-system-p-class-management
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes
module 1 :
transmitted 0 bytes;
5-minute offered rate 0 bytes/sec
conformed 0 peak-rate bytes/sec

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

Während die CoPP-Standardprofile normalerweise als Teil der Standardkonfiguration ausgeblendet werden, wird die Konfiguration mit "**show running-conf copp all**" angezeigt:

```
N9K1# show running-config copp all

!Command: show running-config copp all
!Running configuration last done at: Tue Apr 26 16:34:10 2022
!Time: Sun May 1 16:41:55 2022

version 10.2(1) Bios:version 05.45
control-plane
scale-factor 1.00 module 1
class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
```

```
match access-group name copp-system-p-acl-mac-l3-isis
(snip)
...
```

Die Klasse-Map **copp-system-p-class-critical**, wie oben beschrieben, bezieht sich auf mehrere Übereinstimmungsanweisungen, die System-ACLs aufrufen, die standardmäßig ausgeblendet sind, und verweist auf die Übereinstimmungsklassifizierung, die zugeordnet ist. Beispiel für BGP:

```
N9K1# show running-config aclmgr all | b copp-system-p-acl-bgp
ip access-list copp-system-p-acl-bgp
10 permit tcp any gt 1023 any eq bgp
20 permit tcp any eq bgp any gt 1023
(snip)
```

Dies bedeutet, dass jeder BGP-Datenverkehr dieser Klasse entspricht und unter **copp-system-p-class-critical**, zusammen mit allen anderen Protokollen derselben Klasse klassifiziert wird.

Der **Nexus 7000** folgt einer sehr ähnlichen CoPP-Funktionsstruktur wie der Nexus 9000:

```
N77-A-Admin# show policy-map interface control-plane
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
set cos 7
police cir 36000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
```

```
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
```

Beachten Sie, dass auf einem Nexus 7000, da es sich um modulare Switches handelt, die Klasse nach Modul aufgeteilt ist. Der CIR gilt jedoch für die Aggregation aller Module, und CoPP gilt für das gesamte Chassis. Die CoPP-Verifizierung und -Ausgaben können nur vom Standard- oder Admin Virtual Device Context (VDC) aus gesehen werden.
Besonders wichtig ist die Überprüfung von CoPP auf einem Nexus 7000, wenn Probleme auf der Kontrollebene auftreten, da Instabilität auf einem VDC mit übermäßigem CPU-gebundenen Datenverkehr, der zu CoPP-Verletzungen führt, die Stabilität anderer VDCs beeinträchtigen kann.

Auf einem **Nexus 5600** variieren die Klassen. Für BGP ist es daher eine eigene separate Klasse:

```
N5K# show policy-map interface control-plane
Control Plane
(snip)
class-map copp-system-class-bgp (match-any)
match protocol bgp
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
(snip)
```

Auf einem **Nexus 3100** gibt es drei Routing-Protokollklassen. Um zu überprüfen, zu welcher Klasse das BGP gehört, verweisen Sie auf die 4 CoPP-ACL, auf die verwiesen wird:
EIGRP wird von einer eigenen Klasse auf dem Nexus 3100 behandelt.

```
N3K-C3172# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy

class-map copp-s-routingProto2 (match-any)
match access-group name copp-system-acl-routingproto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-v6routingProto2 (match-any)
match access-group name copp-system-acl-v6routingProto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-eigrp (match-any)
match access-group name copp-system-acl-eigrp
match access-group name copp-system-acl-eigrp6
police pps 200
OutPackets 0
DropPackets 0
class-map copp-s-routingProto1 (match-any)
```

```
match access-group name copp-system-acl-routingproto1
match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 0
DropPackets 0

N3K-C3172# show running-config aclmgr

!Command: show running-config aclmgr
!No configuration change since last restart
!Time: Sun May 1 18:14:16 2022

version 9.3(9) Bios:version 5.3.1
ip access-list copp-system-acl-eigrp
10 permit eigrp any 224.0.0.10/32
ipv6 access-list copp-system-acl-eigrp6
10 permit eigrp any ff02::a/128
ip access-list copp-system-acl-routingproto1
10 permit tcp any gt 1024 any eq bgp
20 permit tcp any eq bgp any gt 1024
30 permit udp any 224.0.0.0/24 eq rip
40 permit tcp any gt 1024 any eq 639
50 permit tcp any eq 639 any gt 1024
70 permit ospf any any
80 permit ospf any 224.0.0.5/32
90 permit ospf any 224.0.0.6/32
ip access-list copp-system-acl-routingproto2
10 permit udp any 224.0.0.0/24 eq 1985
20 permit 112 any 224.0.0.0/24
ipv6 access-list copp-system-acl-v6routingProto2
10 permit udp any ff02::66/128 eq 2029
20 permit udp any ff02::fb/128 eq 5353
30 permit 112 any ff02::12/128
ipv6 access-list copp-system-acl-v6routingproto1
10 permit 89 any ff02::5/128
20 permit 89 any ff02::6/128
30 permit udp any ff02::9/128 eq 521
```

In diesem Fall wird BGP vom ACL **copp-system-acl-routing proto1** abgeglichen, und die CoPP-Klasse BGP fällt daher in **copp-s-routingProto1**.

Statistiken und Zähler zum Control Plane Policing

CoPP unterstützt QoS-Statistiken, um die aggregierten Zähler des Datenverkehrs zu verfolgen, der die bestätigte oder die bestätigte Eingangsrate (CIR) für eine bestimmte Klasse für jedes Modul bestätigt.
Jede Klassenzuordnung klassifiziert CPU-gebundenen Datenverkehr, basierend auf der Klasse, der er entspricht, und fügt eine CIR für alle Pakete an, die unter diese Klassifizierung fallen. Als Beispiel wird die Klasse, die sich auf **BGP-**Datenverkehr bezieht, als Referenz verwendet:

Auf einem Nexus 9000 Top-of-Rack (TOR) für **geschäftskritische CP-System-p-Klasse**:

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
```

```
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

Im Abschnitt der Klassenzuordnung werden nach den Match-Anweisungen die Aktionen angezeigt, die sich auf den gesamten Datenverkehr innerhalb der Klasse beziehen. Der gesamte innerhalb von **copp-system-p-class-critical** klassifizierte Datenverkehr wird mit einer Class of Service (CoS) von 7 festgelegt, bei der es sich um Datenverkehr mit der höchsten Priorität handelt. Diese Klasse wird mit einer CIR von 36000 Kbit/s und einer Burst-Rate von 128000 Byte geregelt. Datenverkehr, der dieser Richtlinie entspricht, wird zur Verarbeitung an den SUP weitergeleitet, und alle Verstöße werden verworfen.

```
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

Der nächste Abschnitt enthält die Statistiken zum Modul für Top-of-Rack (TOR)-Switches mit einem einzigen Modul. Modul 1 bezieht sich auf den Switch.

```
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

Die auf der Ausgabe angezeigten Statistiken sind historisch. Dies bietet einen Snapshot der aktuellen Statistiken zum Zeitpunkt der Ausführung des Befehls.

Hier sind zwei Abschnitte zu interpretieren: die **übertragenen** und **verworfenen** Abschnitte:
Der übertragene Datenpunkt verfolgt alle Pakete, die mit der Richtlinie übertragen wurden. Dieser Abschnitt ist wichtig, da er einen Einblick in die Art des Datenverkehrs bietet, den der Supervisor verarbeitet.

Der angebotene Preis von 5 Minuten bietet Einblicke in den aktuellen Zinssatz.
Die konforme Spitzengeschwindigkeit und das konforme Datum ermöglichen einen Schnappschuss der höchsten Spitzengeschwindigkeit pro Sekunde, die noch innerhalb der Richtlinie und der Zeit, die sie auftrat, konform ist.
Wenn ein neuer Peak angezeigt wird, ersetzt er diesen Wert und das Datum.

Der wichtigste Teil der Statistiken ist der verworfene Datenpunkt. Genau wie die übertragenen Statistiken verfolgt der verworfene Abschnitt die kumulativen Bytes, die aufgrund von Verstößen

gegen die Polizeirate verworfen wurden.
Außerdem wird die Verletzungsrate für die letzten 5 Minuten, der verletzte Peak und, falls ein Peak vorhanden ist, der Zeitstempel für diesen Peak-Verstoß angegeben. Wenn ein neuer Peak sichtbar ist, ersetzt er diesen Wert und das Datum. Auf anderen Plattformen variieren die Ausgaben, aber die Logik ist sehr ähnlich.

Der Nexus 7000 folgt einer identischen Struktur und die Überprüfung ist dieselbe, obwohl einige Klassen in den angegebenen ACLs leicht unterschiedlich sind:

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
set cos 7
police cir 36000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
```

Auf einem Nexus 5600:

```
class-map copp-system-class-bgp (match-any)
```

```
match protocol bgp
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
```

Obwohl keine Informationen zur Rate oder zu Spitzenwerten bereitgestellt werden, werden trotzdem die aggregierten Bytes konform und verletzt bereitgestellt.

Auf einem **Nexus 3100** werden die Ausgabe auf der Kontrollebene, OutPackets und DropPackets angezeigt.

```
class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 8732060
DropPackets 0
```

OutPackets beziehen sich auf konforme Pakete, während DropPackets auf Verletzungen des CIRs verweisen. In diesem Szenario wird keine Dropdownliste der zugeordneten Klasse angezeigt.

Auf einem **Nexus 3500** wird in der Ausgabe Folgendes angezeigt:

```
class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
police pps 900
HW Matched Packets 471425
SW Matched Packets 471425
```

Die übereinstimmenden Pakete in der Hardware beziehen sich auf die Pakete, die von der ACL in der HW abgeglichen werden. Bei den SW-kompatiblen Paketen handelt es sich um Pakete, die der Richtlinie entsprechen. Jegliche Unterschiede zwischen den per HW und SW abgeglichenen Paketen implizieren eine Verletzung.
In diesem Fall gibt es keine Verwerfungen bei Routing-Protokoll-1-Class-Paketen (die BGP enthalten), da die Werte übereinstimmen.

Überprüfen auf Active Drop-Verstöße

Da die Statistiken über die Überwachung auf Kontrollebene historisch sind, ist es wichtig zu ermitteln, ob die Anzahl der aktiven Verstöße zunimmt. Die Standardmethode zur Durchführung dieser Aufgabe besteht darin, zwei vollständige Ausgaben zu vergleichen und etwaige Unterschiede zu überprüfen.
Diese Aufgabe kann manuell durchgeführt werden, oder die Nexus Switches stellen das "diff"-Tool zur Verfügung, mit dem die Ergebnisse verglichen werden können.
Obwohl die gesamte Ausgabe verglichen werden kann, ist sie nicht erforderlich, da der Fokus nur auf den verworfenen Statistiken liegt. So kann die CoPP-Ausgabe so gefiltert werden, dass sie sich nur auf die Verstöße konzentriert.

Der Befehl lautet: **show policy-map interface control plane | egrep class|module|violett|drop | diff -y**

> **Anmerkung:** Der Befehl muss zweimal ausgeführt werden, damit der Diff den Strom mit der vorherigen Ausgabe vergleichen kann.

```
N9K-3# show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y
    class-map copp-system-p-class-l3uc-data (match-any)             class-map copp-system-p-class-l3uc-data (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-critical (match-any)              class-map copp-system-p-class-critical (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-important (match-any)             class-map copp-system-p-class-important (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-openflow (match-any)              class-map copp-system-p-class-openflow (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-router (match-any       class-map copp-system-p-class-multicast-router (match-any
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-host (match-any)        class-map copp-system-p-class-multicast-host (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-l3mc-data (match-any)             class-map copp-system-p-class-l3mc-data (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal (match-any)                class-map copp-system-p-class-normal (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-ndp (match-any)                   class-map copp-system-p-class-ndp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp (match-any)           class-map copp-system-p-class-normal-dhcp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp-relay-response        class-map copp-system-p-class-normal-dhcp-relay-response
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-igmp (match-any)           class-map copp-system-p-class-normal-igmp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
```

Mit dem vorherigen Befehl können Sie das Delta zwischen zwei Klassen anzeigen und die Anzahl der Verstöße ermitteln.

> **Anmerkung:** Da die CoPP-Statistiken historisch sind, wird empfohlen, die Statistiken nach der Ausführung des Befehls zu löschen und zu überprüfen, ob aktive Erhöhungen vorliegen. Führen Sie zum Löschen der CoPP-Statistiken den folgenden Befehl aus: '**klare Kopplungs-Statistiken**'

Arten von CoPP-Drops

CoPP ist eine einfache Richtlinienstruktur, da jeder CPU-gebundene Datenverkehr, der den CIR verletzt, verworfen wird. Die Auswirkungen variieren jedoch erheblich je nach Art der Verwerfen. Obwohl die Logik identisch ist, ist es nicht dasselbe, Datenverkehr zu verwerfen, der für **copp-system-p-class-critical** bestimmt ist

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

im Vergleich zu verworfenem Datenverkehr, der zur **Überwachung** nach Klasse-Maps**-copp-system-p-class** bestimmt ist.

```
class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
```

Das erste befasst sich hauptsächlich mit Routing-Protokollen, das zweite mit Internet Control Message Protocol (ICMP), das eine der niedrigsten Prioritäten und CIR hat. Der Unterschied in der CIR beträgt das Hundertfache. Aus diesem Grund ist es wichtig, die Klassen, Auswirkungen, allgemeinen Kontrollen/Überprüfungen und Empfehlungen zu verstehen.

CoPP-Klassen

Klassenüberwachung - copp-system-p-class-monitoring

Diese Klasse umfasst ICMP für IPv4 und IPv6 sowie Traceroute des an den betreffenden Switch gerichteten Datenverkehrs.

```
class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
```

Auswirkungen

- Ein häufiges Missverständnis bei der Fehlerbehebung bei Paketverlusten oder Latenzen besteht darin, den Switch über seine In-Band-Ports zu pingen, die durch CoPP eingeschränkt sind. Da CoPP ICMP selbst bei geringem Datenverkehr oder Überlastung stark überwacht, kann der Paketverlust beim direkten Pingen von In-Band-Schnittstellen beobachtet werden, wenn diese die CIR verletzen.

So können beispielsweise bei einem Ping für direkt verbundene Schnittstellen an gerouteten Ports mit einer Paketnutzlast von 500 regelmäßig Verwerfungen auftreten.

```
N9K-3# ping 192.168.1.1 count 1000 packet-size 500
...
--- 192.168.1.1 ping statistics ---
1000 packets transmitted, 995 packets received, 0.50% packet loss
round-trip min/avg/max = 0.597/0.693/2.056 ms
```

Auf dem Nexus, auf dem die ICMP-Pakete bestimmt wurden, wurden sie vom CoPP verworfen, da die Verletzung erkannt und die CPU geschützt wurde:

```
N9K-4# show policy-map interface control-plane class copp-system-p-class-monitoring
Control Plane

Service-policy input: copp-system-p-policy-strict
```

```
class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
module 1 :
transmitted 750902 bytes;
5-minute offered rate 13606 bytes/sec
conformed 13606 peak-rate bytes/sec
at Sun May 01 22:49:24 2022

dropped 2950 bytes;
5-min violate rate 53 byte/sec
violated 53 peak-rate byte/sec at Sun May 01 22:49:24 2022
```

Bei der Fehlerbehebung bei Latenz oder Paketverlusten wird empfohlen, Hosts zu verwenden, die über den Switch über die Datenebene erreichbar sind und nicht für den eigentlichen Switch bestimmt sind, d. h. Datenverkehr auf Kontrollebene. Der Datenverkehr auf der Datenebene wird ohne SUP-Eingriff auf Hardwareebene weitergeleitet/weitergeleitet und wird daher nicht durch CoPP geregelt. In der Regel kommt es zu keinerlei Verlusten.

Empfehlungen

- Überprüfen Sie falsch positive Ergebnisse für Paketverluste, indem Sie einen Ping über den Switch und nicht an den Switch senden.

- Limit Network Monitoring System (NMS) oder Tools, die ICMP auf dem Switch aggressiv verwenden, um einen Burst über die zugesicherte Eingangsrate für die Klasse zu vermeiden. Beachten Sie, dass CoPP für den gesamten aggregierten Datenverkehr gilt, der in die Klasse fällt.

Klassenmanagement - copp-system-p-class-management

Wie hier gezeigt, umfasst diese Klasse verschiedene Verwaltungsprotokolle, die für Kommunikation (SSH, Telnet), Übertragungen (SCP, FTP, HTTP, SFTP, TFTP), Takt (NTP), AAA (Radius/TACACS) und Überwachung (SNMP) für IPv4- und IPv6-Kommunikation verwendet werden können.

```
class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
```

```
set cos 2
police cir 36000 kbps , bc 512000 bytes
```

Auswirkungen

Zu den häufigsten Verhaltensweisen oder Verwerfungen, die dieser Klasse zugeordnet sind, gehören:

- Verlangsamung der CLI bei Verbindung über SSH/Telnet Wenn die Klasse aktiv verworfen wird, können die Kommunikationssitzungen langsam verlaufen und fallen.
-Dateien mit FTP-, SCP-, SFTP- und TFTP-Protokollen auf den Switch übertragen. Das häufigste Verhalten ist der Versuch, System-/Kickstart-Boot-Images über In-Band-Verwaltungsports zu übertragen. Dies kann zu höheren Übertragungszeiten und geschlossenen/beendeten Übertragungssitzungen führen, die durch die aggregierte Bandbreite der Klasse bestimmt werden.
-NTP-Synchronisierungsprobleme, ist diese Klasse ebenfalls wichtig, da sie nicht autorisierte NTP-Agenten oder Angriffe abwehrt.
-AAA Radius- und TACACS-Dienste gehören ebenfalls zu dieser Klasse. Wenn die Auswirkungen auf diese Klasse wahrgenommen werden, kann dies Autorisierungs- und Authentifizierungsdienste auf dem Switch für Benutzerkonten beeinträchtigen, was auch zur Verzögerung der CLI-Befehle beitragen kann.
-SNMP wird auch unter dieser Klasse geregelt. Das häufigste Verhalten, das aufgrund von Verwerfen der SNMP-Klasse beobachtet wurde, sind NMS-Server, die Spaziergänge, Sammelauflistungen oder Netzwerkscans durchführen. Bei periodischer Instabilität wird diese normalerweise mit dem NMS-Erfassungszeitplan korreliert.

Empfehlungen

- Wenn die Verlangsamung der CLI wahrgenommen wird, zusammen mit Verwerfungen in dieser Klasse, den Konsolenzugriff oder den Out-of-Band-Zugriff für die Verwaltung verwenden (mgmt0).

- Wenn System-Images auf den Switch hochgeladen werden müssen, verwenden Sie entweder den Out-of-Band-Verwaltungsport (mgmt0) oder verwenden Sie die USB-Ports für den schnellsten Transfer.

- Wenn NTP-Pakete verloren gehen, aktivieren Sie die Option "show ntp peer-status" (ntp Peer-Status anzeigen), und überprüfen Sie die Erreichbarkeit in der Spalte. Keine Drops übersetzen in 377.

- Wenn Probleme mit AAA-Services auftreten, sollten Sie zur Fehlerbehebung lokale Benutzer verwenden, bis das Verhalten gemindert wird.

- Die Fehlerbehebung bei SNMP-Problemen umfasst weniger aggressives Verhalten, zielgerichtete Erfassung oder Minimierung von Netzwerkscannern. Überprüfen Sie die periodischen Zeiten von Scannern bis hin zu Ereignissen auf CPU-Ebene.

Class L3 Unicast Data - copp-system-p-class-l3uc-data

Diese Klasse behandelt speziell leere Pakete. Dieser Pakettyp wird auch vom Hardware Rate Limiter (WHRL) behandelt.
Wenn die ARP-Anfrage (Address Resolution Protocol) für den nächsten Hop nicht aufgelöst wird, wenn eingehende IP-Pakete in einer Linecard weitergeleitet werden, leitet die Linecard die Pakete an das Supervisor-Modul weiter.

Der Supervisor löst die MAC-Adresse für den nächsten Hop auf und programmiert die Hardware.

```
class-map copp-system-p-class-l3uc-data (match-any)
match exception glean
set cos 1
```

Dies geschieht normalerweise, wenn statische Routen verwendet werden und der nächste Hop nicht erreichbar oder nicht aufgelöst werden kann.

Wenn eine ARP-Anfrage gesendet wird, fügt die Software der Hardware eine /32-Drop-Adjacency hinzu, um zu verhindern, dass Pakete an dieselbe Next-Hop-IP-Adresse an den Supervisor weitergeleitet werden. Wenn der ARP aufgelöst wird, wird der Hardwareeintrag mit der richtigen MAC-Adresse aktualisiert. Wenn der ARP-Eintrag nicht vor einem Timeout aufgelöst wird, wird der Eintrag aus der Hardware entfernt.

> **Anmerkung:** CoPP und HWRL arbeiten zusammen, um den Schutz der CPU zu gewährleisten. Obwohl sie scheinbar ähnliche Funktionen ausführen, tritt zuerst HWRL auf. Die Implementierung basiert darauf, wo die spezifische Funktion auf den Forwarding-Engines des ASIC implementiert wird. Dieser serielle Ansatz ermöglicht Granularität und mehrschichtigen Schutz, bei dem alle CPU-gebundenen Pakete bewertet werden.

Der HWRL wird pro Instanz/Weiterleitungs-Engine auf dem Modul ausgeführt und kann mit dem Befehl "**show hardware rate-limiter**" angezeigt werden. HWRL ist nicht Bestandteil dieses technischen Dokuments.

```
show hardware rate-limiter

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters


Module: 1
R-L Class Config Allowed Dropped Total
+---------------+----------+--------------------+--------------------+--------------------+
L3 glean 100 0 0 0
L3 mcast loc-grp 3000 0 0 0
access-list-log 100 0 0 0
bfd 10000 0 0 0
fex 12000 0 0 0
span 50 0 0 0
sflow 40000 0 0 0
vxlan-oam 1000 0 0 0
100M-ethports 10000 0 0 0
span-egress disabled 0 0 0
dot1x 3000 0 0 0
mpls-oam 300 0 0 0
netflow 120000 0 0 0
ucs-mgmt 12000 0 0 0
```

Auswirkungen

- Datenverkehr auf der Datenebene wird als Verletzung an den Supervisor gesendet, da er nicht in der Hardware verarbeitet werden kann und somit Druck auf die CPU ausübt.

Empfehlungen

-Die gemeinsame Lösung zur Minimierung der Glean-Drops besteht darin, sicherzustellen, dass der nächste Hop erreichbar ist, und die Glean-Throttling über den Konfigurationsbefehl zu aktivieren: '**Hardware ip glean throttle**'

Siehe: https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/Unicast-routing/cisco-nexus-9000-series-nx-os-unicast-configuration-guide-release-102x/m-n9k-configuring-ipv4-93x.html#concept_A6E56C2E174440BBA33F829C23897807

-Auf dem Nexus 7000 wurde mit 8.4(2) auch die Unterstützung von Blockfiltern für Glean-Adjacencies für M3- und F4-Module eingeführt. Siehe: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/unicast/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Unicast-Routing-Configuration-Guide-Release/n7k_unicast_config_ipv4.html#concept_4B4BF5FE17DE443EAAD710690FE670EB

- Überprüfen Sie alle statischen Routenkonfigurationen, die nicht erreichbare Next-Hop-Adressen verwenden, oder verwenden Sie dynamische Routing-Protokolle, die solche Routen dynamisch aus der RIB entfernen würden.

Klassenkritisch - class-map copp-system-p-class-critical

Diese Klasse verweist aus L3-Sicht auf die wichtigsten Kontrollebenenprotokolle, darunter Routing-Protokolle für IPv4 und IPv6, (RIP, OSPF, EIGRP, BGP), Auto-RP, Virtual Port Channel (vPC) sowie l2pt und IS-IS.

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

Auswirkungen

Löscht bei **copp-system-p-class-critical** Transfer Instabilität zu Routing-Protokollen, wozu auch Adjacencies fallen oder Konvergenzfehler auftreten können, oder Update/NLRI-Weitergabe.
Die gängigsten Richtlinien, die bei dieser Klasse verworfen werden, können sich auf nicht autorisierte Geräte im Netzwerk beziehen, die ungewöhnlich (aufgrund von Fehlkonfiguration oder -ausfall) oder skalierbar agieren.

Empfehlungen

- Wenn keine Anomalien erkannt werden, wie z. B. ein nicht autorisiertes Gerät oder eine L2-Instabilität, die eine kontinuierliche Rekonvergenz von Protokollen der oberen Ebene verursacht, kann eine benutzerdefinierte Konfiguration von CoPP oder eine lockere Klasse erforderlich sein, um die Skalierung zu unterstützen.
-Informationen zum Konfigurieren eines benutzerdefinierten CoPP-Profils aus einem derzeit vorhandenen Standardprofil finden Sie im CoPP-Konfigurationsleitfaden.
https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/Security/cisco-nexus-9000-nx-os-security-configuration-guide-102x/m-configuring-copp.html#task_E3D04369F59F471885BC5E8CD24337CA

Wichtige Klasse - copp-system-p-class-important

Diese Klasse bezieht sich auf die First-Hop Redundancy Protocols (FHRP), einschließlich HSRP, VRRP und LLDP

```
class-map copp-system-p-class-important (match-any)
match access-group name copp-system-p-acl-hsrp
match access-group name copp-system-p-acl-vrrp
match access-group name copp-system-p-acl-hsrp6
match access-group name copp-system-p-acl-vrrp6
match access-group name copp-system-p-acl-mac-lldp
set cos 6
police cir 2500 kbps , bc 1280000 bytes
```

Auswirkungen

Das häufigste Verhalten, das zu Verwerfungen führt, sind Probleme mit Layer-2-Instabilität, die dazu führt, dass Geräte in den aktiven Zustand (Split-Hirn), aggressive Timer, Fehlkonfigurationen oder Skalierbarkeit übergehen.

Empfehlungen

- Stellen Sie sicher, dass für FHRP Gruppen korrekt konfiguriert sind und die Rollen entweder aktiv/Standby oder primär/sekundär korrekt verhandelt werden und dass keine Flaps vorhanden sind.

- Auf Konvergenzprobleme bei L2 oder Probleme mit der Multicast-Übertragung für die L2-Domäne prüfen.

Klasse L2 Unpoliced - copp-system-p-class-l2-unpoliced

Die nicht überwachte L2-Klasse bezieht sich auf alle kritischen Layer-2-Protokolle, die die Grundlage für alle Protokolle der oberen Schicht bilden und daher als nahezu unbeschränkt mit der höchsten CIR- und Prioritätsstufe gelten.
Diese Klasse verarbeitet effektiv Spanning-Tree Protocol (STP), Link Aggregation Control Protocol (LACP), Cisco Fabric Service over Ethernet (CFSoE).

```
class-map copp-system-p-class-l2-unpoliced (match-any)
match access-group name copp-system-p-acl-mac-stp
match access-group name copp-system-p-acl-mac-lacp
match access-group name copp-system-p-acl-mac-cfsoe
match access-group name copp-system-p-acl-mac-sdp-srp
match access-group name copp-system-p-acl-mac-l2-tunnel
match access-group name copp-system-p-acl-mac-cdp-udld-vtp
set cos 7
police cir 50 mbps , bc 8192000 bytes
```

Diese Klasse hat einen CIR von 50 Mbit/s, den höchsten unter allen Klassen, zusammen mit der höchsten Absorption bei Spitzengeschwindigkeit.

Auswirkungen

Wenn diese Klasse verworfen wird, kann dies zu globaler Instabilität führen, da alle Protokolle der oberen Schichten und die Kommunikation auf Daten-, Kontroll- und Verwaltungsebenen auf einer zugrunde liegenden Layer-2-Stabilität beruhen.

Probleme mit STP-Verletzungen können TCNs und STP-Konvergenz-Probleme verursachen, darunter STP-Streitigkeiten, MAC-Flushes, -Verschiebungen und lernbehinderte Verhaltensweisen, die Probleme mit der Erreichbarkeit verursachen und Datenverkehrsschleifen verursachen können, die das Netzwerk destabilisieren.

Diese Klasse verweist auch auf LACP und behandelt daher alle EtherType-Pakete, die 0x8809 zugeordnet sind, einschließlich aller LACPDUs, die zum Beibehalten des Zustands der Port-Channel-Anleihen verwendet werden. Instabilität bei dieser Klasse kann dazu führen, dass die Port-Channels das Timeout verursachen, wenn die LACPDUs verworfen werden.

Cisco Fabric Service over Ethernet (CSFoE) gehört zu dieser Klasse und dient zur Kommunikation wichtiger Anwendungssteuerungszustände zwischen Nexus-Switches und ist daher für die Stabilität unerlässlich.

Dasselbe gilt für andere Protokolle innerhalb dieser Klasse, zu denen CDP, UDLD und VTP gehören.

Empfehlungen

- Das häufigste Verhalten bezieht sich auf L2-Ethernet-Instabilität. Stellen Sie sicher, dass STP deterministisch konzipiert ist und die relevanten Funktionsverbesserungen umfasst, um die Auswirkungen von Rekonvergenz oder nicht autorisierten Geräten im Netzwerk zu minimieren. Stellen Sie sicher, dass der richtige STP-Port-Typ für alle End-Host-Geräte konfiguriert ist, die nicht an der L2-Erweiterung teilnehmen, und als Edge-/Edge-Trunk-Ports konfiguriert sind, um TCNs zu minimieren.

- Verwenden Sie ggf. STP-Erweiterungen wie BPDUguard, Loopguard, BPDUfilter oder RootGuard, um den Umfang eines Fehlers oder Probleme mit fehlerhaften Geräten oder nicht autorisierten Geräten im Netzwerk zu begrenzen.

Siehe: https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/layer-2-switching/cisco-nexus-9000-nx-os-layer-2-switching-configuration-guide-102x/m-configuring-stp-extensions.html

- Überprüfen Sie, ob MAC-Bewegungsverhalten aktiviert sind, die dazu führen können, dass das

MAC-Lernen deaktiviert wird und geleert wird. Weitere Informationen finden Sie unter: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/nx-os-software/213906-nexus-9000-mac-move-troubleshooting-and.html

Class Multicast-Router - class-map copp-system-p-class-multicast-router

Diese Klasse bezieht sich auf PIM-Pakete (Control Plane Protocol Independent Multicast), die zum Einrichten und Steuern von gerouteten Multicast-Shared Trees über alle PIM-fähigen Geräte im Datenebenenpfad verwendet werden, einschließlich First-Hop Router (FHR), Last-Hop Router (LHR), Intermediate-Hop Router (IHR) und Rendezvouz Points (RPs). Zu den in dieser Klasse klassifizierten Paketen gehören die PIM-Registrierung für Quellen, PIM-Joins für Empfänger sowohl für IPv4 als auch für IPv6, im Allgemeinen für den PIM-Verkehr (224.0.0.13) und das Multicast Source Discovery Protocol (MSDP). Beachten Sie, dass es mehrere zusätzliche Klassen gibt, die sehr spezifische Teile von Multicast- oder RP-Funktionen behandeln, die von verschiedenen Klassen behandelt werden.

```
class-map copp-system-p-class-multicast-router (match-any)
match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp
match access-group name copp-system-p-acl-pim6
match access-group name copp-system-p-acl-pim-reg
match access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
match exception mvpn
set cos 6
police cir 2600 kbps , bc 128000 bytes
```

Auswirkungen

Die Hauptauswirkungen auf Verwerfen, die sich auf diese Klasse beziehen, sind mit Problemen verbunden, die durch die PIM-Registrierung mit Multicast-Quellen an die RPs oder PIM-Verbindungen kommunizieren, die nicht ordnungsgemäß verarbeitet wurden. Dies würde die Shared oder Shortest Path Trees zu den Quellen des Multicast-Streams oder zu den RPs destabilisieren. Das Verhalten kann ausgehende Schnittstellenlisten (OIL) einschließen, die aufgrund fehlender Joins nicht korrekt ausgefüllt wurden, oder (S, G) oder (*, G), die in der Umgebung nicht einheitlich angezeigt werden. Es können auch Probleme zwischen Multicast-Routing-Domänen auftreten, die für die Verbindung auf MSDP angewiesen sind.

Empfehlungen

- Das häufigste Verhalten bei PIM-Steuerungsproblemen bezieht sich auf Probleme bei der Skalierung oder unberechtigtes Verhalten. Eines der häufigsten Verhaltensweisen wird durch die Implementierung auf UPnP beobachtet, was auch zu Speichererschöpfungsproblemen führen kann. Dies kann durch Filter und einen geringeren Umfang der nicht autorisierten Geräte behoben werden. Weitere Einzelheiten dazu, wie Multicast-Kontrollpakete je nach Netzwerkrolle des Geräts reduziert und gefiltert werden, finden Sie unter:

Konfigurieren der Multicast-Filterung auf Nexus 7K/N9K - Cisco

Class Multicast Host - copp-system-p-class-multicast-host

Diese Klasse bezieht sich auf die Multicast Listener Discovery (MLD), insbesondere MLD-Abfrage,

-Bericht, -Reduzierung und MLDv2-Pakettypen. MLD ist ein IPv6-Protokoll, das ein Host verwendet, um Multicast-Daten für eine bestimmte Gruppe anzufordern. Mithilfe der über MLD erhaltenen Informationen verwaltet die Software eine Liste der Multicast-Gruppen- oder Channel-Mitgliedschaften auf Schnittstellenbasis. Die Geräte, die MLD-Pakete empfangen, senden die Multicast-Daten, die sie für angeforderte Gruppen oder Kanäle empfangen, aus dem Netzwerksegment der bekannten Empfänger. MLDv1 wird von IGMPv2 abgeleitet, und MLDv2 wird von IGMPv3 abgeleitet. IGMP verwendet den Meldungstyp IP Protocol 2, während MLD den Meldungstyp IP Protocol 58 verwendet. Dies ist eine Teilmenge der ICMPv6-Nachrichten.

```
class-map copp-system-p-class-multicast-host (match-any)
match access-group name copp-system-p-acl-mld
set cos 1
police cir 1000 kbps , bc 128000 bytes
```

Auswirkungen

Drops für diese Klasse führen zu Problemen bei der standortübergreifenden IPv6-Multicast-Kommunikation, die dazu führen können, dass Listenerberichte von Empfängern oder Antworten auf allgemeine Abfragen verworfen werden, wodurch die Erkennung von Multicast-Gruppen verhindert wird, die die Hosts empfangen möchten. Dies kann sich auf den Snooping-Mechanismus auswirken und Datenverkehr nicht ordnungsgemäß über erwartete Schnittstellen weiterleiten, die den Datenverkehr angefordert haben.

Empfehlungen

- Da der MLD-Datenverkehr für IPv6 auf der lokalen Verbindungsebene von Bedeutung ist, beziehen sich die häufigsten Ursachen für Verwerfungen bei dieser Klasse auf Skalierung, L2-Instabilität oder nicht autorisierte Geräte.

Class Layer 3 Multicast Data - copp-system-p-class-l3mc-data und Class Layer 3 Multicast IPv6 Data - copp-system-p-class-l3mcv6-data

Diese Klassen beziehen sich auf Datenverkehr, der mit einer Multicast-Ausnahmeumleitung zum SUP übereinstimmt. In diesem Fall gibt es zwei Bedingungen, die von diesen Klassen behandelt werden. Der erste ist Reverse-Path Forwarding (RPF) Failure, der zweite ist Destination Miss. Ziel Miss bezieht sich auf Multicast-Pakete, bei denen die Suche in der Hardware für die Multicast-Weiterleitungstabelle auf Layer 3 fehlschlägt und das Datenpaket somit auf die CPU beschränkt wird. Diese Pakete werden manchmal verwendet, um die Multicast-Kontrollebene auszulösen/zu installieren und die Einträge der Hardware-Weiterleitungstabellen auf Basis des Datenverkehrs auf der Datenebene hinzuzufügen. Multicast-Pakete auf Datenebene, die gegen RPF verstoßen, stimmen ebenfalls mit dieser Ausnahme überein und werden als Verletzung klassifiziert.

```
class-map copp-system-p-class-l3mc-data (match-any)
match exception multicast rpf-failure
match exception multicast dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes

class-map copp-system-p-class-l3mcv6-data (match-any)
match exception multicast ipv6-rpf-failure
match exception multicast ipv6-dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes
```

Auswirkungen

Bei RPF-Ausfällen und Ziel-Fehlern liegt ein Design- oder Konfigurationsproblem vor, der sich auf den Datenverkehr durch den Multicast-Router bezieht. Zielfehler sind bei der Zustandserstellung üblich, Verwerfen kann dazu führen, dass die Programmierung und Erstellung von (*, G), (S, G) fehlschlägt.

Empfehlungen

- Durchführung von Änderungen am grundlegenden Unicast-RIB-Design oder Hinzufügen einer statischen Route zur Steuerung des Datenverkehrs über eine bestimmte Schnittstelle, falls RPF-Fehler auftreten.

- Siehe https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/16450-mcastguide0.html#anc5

Klasse IGMP - copp-system-p-class-igmp

Diese Klasse bezieht sich auf alle IGMP-Nachrichten für alle Versionen, die zum Anfordern von Multicast-Daten für eine bestimmte Gruppe verwendet werden und von der IGMP-Snooping-Funktion verwendet werden, um die Gruppen und die relevante OIL-Liste (Outgoing Interface List) beizubehalten, die den Datenverkehr an die interessierten Empfänger auf Layer 2 weiterleitet. Die IGMP-Meldungen sind lokal von Bedeutung, da sie keine Layer-3-Grenze überschreiten, da ihre "Time to Live" (TTL) 1 sein muss (siehe RFC 2236 (https://datatracker.ietf.org/doc/html/rfc2236)). Die IGMP-Pakete, die von dieser Klasse behandelt werden, beinhalten alle Mitgliedschaftsabfragen (allgemeine oder Quell-/Gruppenspezifische) sowie die Mitgliedschaftsabfragen und die Berichte von den Empfängern.

```
class-map copp-system-p-class-normal-igmp (match-any)
match access-group name copp-system-p-acl-igmp
set cos 3
police cir 3000 kbps , bc 64000 bytes
```

Auswirkungen

Drops für diese Klasse führen zu Problemen auf allen Ebenen der Multicast-Kommunikation zwischen Quelle und Empfänger, abhängig vom Typ der IGMP-Nachricht, die aufgrund der Verletzung verworfen wurde. Wenn Mitgliedschaftsberichte von Empfängern verloren gehen, sind dem Router keine Geräte bekannt, die an dem Datenverkehr interessiert sind. Daher wird die Schnittstelle/das VLAN nicht in die entsprechende Liste der ausgehenden Schnittstellen aufgenommen. Wenn es sich bei diesem Gerät auch um den Querier oder den designierten Router handelt, werden die relevanten PIM-Join-Nachrichten nicht zum RP ausgelöst, wenn die Quelle außerhalb der lokalen Layer-2-Domäne liegt. Auf diese Weise wird die Datenebene über den Multicast Tree bis zum Empfänger oder RP nie vollständig erstellt. Wenn der Urlaubsbericht verloren geht, kann der Empfänger weiterhin unerwünschten Datenverkehr empfangen. Dies kann sich auch auf alle relevanten IGMP-Abfragen auswirken, die vom Abfrager ausgelöst werden, sowie auf die Kommunikation zwischen den Multicast-Routern in einer Domäne.

Empfehlungen

- Die häufigsten Verhaltensweisen, die mit IGMP-Drops verbunden sind, beziehen sich auf L2-Instabilität, Timer-Probleme oder Skalierbarkeit.

Klasse Normal - copp-system-p-class-normal

Diese Klasse bezieht sich auf Datenverkehr, der mit standardmäßigem ARP-Datenverkehr übereinstimmt. Sie umfasst auch Datenverkehr, der mit 802.1X verknüpft ist und für die Port-basierte Netzwerkzugriffskontrolle verwendet wird. Dies ist eine der gängigsten Klassen, bei der es zu Verletzungen kommt, da ARP-Anfragen, Gratuitous ARP- und Reverse ARP-Pakete gesendet und über die gesamte Layer-2-Domäne verteilt werden. Es ist wichtig zu beachten, dass ARP-Pakete keine IP-Pakete sind, diese Pakete keinen L3-Header enthalten. Daher wird die Entscheidung ausschließlich über den Bereich der L2-Header getroffen. Wenn ein Router mit einer IP-Schnittstelle konfiguriert ist, die diesem Subnetz zugeordnet ist, z. B. eine Switch Virtual Interface (SVI), überträgt der Router die ARP-Pakete an die SUP, die verarbeitet werden sollen, da sie zur Broadcast-Adresse der Hardware bestimmt sind. Ein Broadcast-Sturm, eine Layer-2-Schleife (aufgrund von STP oder Flaps) oder ein Routing-Gerät im Netzwerk können zu einem ARP-Sturm führen, der zu einem deutlichen Anstieg der Verletzungen führt.

```
class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
```

Auswirkungen

Die Auswirkungen von Verletzungen in dieser Klasse hängen stark von der Dauer der Ereignisse und der Rolle des Switches in der Umgebung ab. Drops in dieser Klasse implizieren, dass ARP-Pakete verworfen und daher nicht von der SUP-Engine verarbeitet werden, was zu zwei Hauptverhaltensweisen führen kann, die durch unvollständige ARP-Auflösungen verursacht werden.

Aus Sicht des End-Hosts können Geräte im Netzwerk die Auflösung der Adresse nicht mit dem Switch auflösen oder abschließen. Wenn dieses Gerät als Standard-Gateway für das Segment fungiert, können Geräte sein Gateway nicht auflösen können und daher nicht außerhalb des L2-Ethernet-Segments (VLAN) routen können. Geräte können weiterhin im lokalen Segment kommunizieren, wenn sie die ARP-Auflösung für andere Endhosts im lokalen Segment abschließen können.

Wenn der Sturm und die Verletzungen vorkommen, kann der Switch aus Sicht des Switches auch nicht in der Lage sein, den Prozess für die von ihm generierte ARP-Anfrage abzuschließen. Diese Anforderungen werden normalerweise für Next-Hop- oder direkt verbundene Subnetzauflösungen generiert. Die ARP-Antworten sind zwar Unicast-Natur, da sie an die MAC-Adresse des Switches adressiert werden, werden jedoch derselben Klasse zugeordnet, da es sich bei ihnen immer noch um ARP-Pakete handelt. Dies führt zu Problemen bei der Erreichbarkeit, da der Switch Datenverkehr nicht ordnungsgemäß verarbeiten kann, wenn der nächste Hop nicht behoben wird. Dies kann zu Problemen beim Umschreiben des Layer-2-Headers führen, wenn der Adjacency Manager keinen Eintrag für den Host hat.

Die Auswirkungen hängen auch vom Umfang des grundlegenden Problems ab, das die ARP-Verletzung ausgelöst hat. In einem Broadcast-Sturm versuchen Hosts und der Switch beispielsweise weiterhin ARP, die Adjacency aufzulösen, was zu zusätzlichem Broadcast-Datenverkehr im Netzwerk führen kann. Da ARP-Pakete Layer 2 sind, gibt es keine Layer 3 Time to Live (TTL), um eine L2-Schleife zu unterbrechen, sodass sie weiter schleifen und exponentiell durch das Netzwerk wachsen, bis die Schleife unterbrochen wird.

Empfehlungen

- Beheben Sie alle grundlegenden L2-Instabilitäten, die in der Umgebung ARP-Stürme verursachen können, z. B. STP, Flaps oder nicht autorisierte Geräte. Brechen Sie diese Schleifen nach Bedarf, indem Sie eine beliebige Methode zum Öffnen des Verbindungspfads verwenden.

-Storm-Control kann auch verwendet werden, um einen ARP-Sturm zu mildern. Wenn die Sturmkontrolle nicht aktiviert ist, überprüfen Sie Zählerstatistiken für Schnittstellen, um den Anteil des Broadcast-Datenverkehrs an den Schnittstellen im Verhältnis zum gesamten Datenverkehr, der über die Schnittstelle geleitet wird, zu überprüfen.

- Wenn es keinen Sturm gibt, aber in der Umgebung immer noch konstante Verwerfungen auftreten, überprüfen Sie den SUP-Datenverkehr, um unautorisierte Geräte zu identifizieren. Senden Sie laufend ARP-Pakete im Netzwerk, was den legitimen Datenverkehr beeinträchtigen kann.

- Erhöhungen sind abhängig von der Anzahl der Hosts im Netzwerk und der Rolle des Switches in der Umgebung erkennbar. Das ARP ist so konzipiert, dass Einträge wiederholt, aufgelöst und aktualisiert werden können. Daher wird erwartet, dass der ARP-Datenverkehr jederzeit angezeigt wird. Wenn nur sporadische Verwerfungen zu beobachten sind, können diese je nach Netzwerkauslastung vorübergehend sein, und es werden keine Auswirkungen wahrgenommen. Es ist jedoch wichtig, das Netzwerk zu überwachen und zu kennen, um eine erwartete Situation richtig zu erkennen und von einer ungewöhnlichen Situation abzuheben.

Klasse NDP - copp-system-p-acl-ndp

Diese Klasse bezieht sich auf Datenverkehr im Zusammenhang mit IPv6-Netznachbarenerkennung/-anzeige sowie Routeranfragen und -anzeigenpaketen, die mithilfe von ICMP-Nachrichten lokale Link-Layer-Adressen von Nachbarn ermitteln, und wird für die Erreichbarkeit und Nachverfolgung benachbarter Geräte verwendet.

```
class-map copp-system-p-class-ndp (match-any)
match access-group name copp-system-p-acl-ndp
set cos 6
police cir 1400 kbps , bc 32000 bytes
```

Auswirkungen

Verstöße gegen diese Klasse können die IPv6-Kommunikation zwischen benachbarten Geräten behindern, da diese Pakete verwendet werden, um die dynamische Erkennung oder Link-Layer/lokale Informationen zwischen Hosts und Routern auf der lokalen Verbindung zu erleichtern. Eine Unterbrechung dieser Kommunikation kann auch Probleme mit der Erreichbarkeit verursachen, die über die zugeordnete lokale Verbindung hinausgehen oder auftreten. Wenn Kommunikationsprobleme zwischen IPv6-Nachbarn auftreten, stellen Sie sicher, dass diese Klasse nicht ausgeblendet wird.

Empfehlungen

- Überprüfen Sie alle ungewöhnlichen ICMP-Verhaltensweisen von benachbarten Geräten, insbesondere solche, die sich auf die Erkennung von Nachbarn und/oder Routern beziehen.

-Stellen Sie sicher, dass alle erwarteten Timer- und Intervallwerte für die periodischen Meldungen

in der Umgebung konsistent sind und eingehalten werden, z. B. bei Router Advertisement Messages (RA Messages).

Class Normal DHCP - copp-system-p-class-normal-dhcp

Diese Klasse bezieht sich auf Datenverkehr, der mit dem Bootstrap Protocol (BOOTP-Client/Server) verbunden ist, gemeinhin als Dynamic Host Control Protocol (DHCP)-Pakete im gleichen lokalen Ethernet-Segment für IPv4 und IPv6 bezeichnet. Dies bezieht sich speziell nur auf die Datenverkehrskommunikation, die von einem Bootp-Client stammt oder für einen beliebigen BOOTP-Server bestimmt ist. Dies geschieht über den gesamten Austausch von Entdeckungs-, Angebots-, Anforderungs- und Bestätigungs-Paketen (DORA) und schließt auch DHCPv6-Client-/Servertransaktionen über die UDP-Ports 546/547 ein.

```
class-map copp-system-p-class-normal-dhcp (match-any)
match access-group name copp-system-p-acl-dhcp
match access-group name copp-system-p-acl-dhcp6
set cos 1
police cir 1300 kbps , bc 32000 bytes
```

Auswirkungen

Verstöße gegen diese Klasse können dazu führen, dass Endhosts nicht in der Lage sind, eine IP-Adresse vom DHCP-Server korrekt abzurufen, sodass sie auf ihren automatischen privaten IP-Adressbereich (APIPA), 169.254.0.0/16, zurückgreifen können. Solche Verletzungen können in Umgebungen auftreten, in denen Geräte versuchen, gleichzeitig zu booten und damit über die CIR-Schnittstelle der Klasse hinausgehen.

Empfehlungen

- Überprüfen Sie bei der Erfassung, auf Hosts und auf DHCP-Servern die gesamte DORA-Transaktion. Wenn der Switch Teil dieser Kommunikation ist, ist es auch wichtig, die verarbeiteten oder an die CPU gestrafften Pakete zu überprüfen und Statistiken über den Switch zu überprüfen: 'show ip dhcp global statistics' und Umleitungen: 'show system internal access list sup-redirect-stats module 1 | grep -i dhcp'.

Class Normal DHCP Relay Response - copp-system-p-class-normal-dhcp-relais-response

Diese Klasse bezieht sich auf Datenverkehr, der mit der DHCP-Relay-Funktion für IPv4 und IPv6 verknüpft ist und an die konfigurierten DHCP-Server weitergeleitet wird, die unter dem Relay konfiguriert wurden. Dies bezieht sich speziell auf die Datenverkehrskommunikation, die von einem BOOTP-Server ausgeht oder für BOOTP-Clients über den gesamten DORA-Paketaustausch bestimmt ist, und umfasst auch DHCPv6-Client-/Servertransaktionen über die UDP-Ports 546/547.

```
class-map copp-system-p-class-normal-dhcp-relay-response (match-any)
match access-group name copp-system-p-acl-dhcp-relay-response
match access-group name copp-system-p-acl-dhcp6-relay-response
set cos 1
police cir 1500 kbps , bc 64000 bytes
```

Auswirkungen

Verstöße gegen diese Klasse haben dieselben Auswirkungen wie die Verletzungen für die Klasse copp-system-p-class-normal-dhcp, da sie beide Teile derselben Transaktion sind. Diese Klasse konzentriert sich hauptsächlich auf die Antwortkommunikation der Relay-Agent-Server. Der Nexus fungiert nicht als DHCP-Server, sondern dient lediglich als Relay-Agent.

Empfehlungen

Hier gelten die gleichen Empfehlungen wie für die normale DHCP-Klasse. Da der Nexus nur als Relay-Agent fungieren soll, erwarten Sie auf dem SUP, dass die gesamte Transaktion zwischen Host und Switch als Relay fungiert und der Switch und die Server konfiguriert werden.

Stellen Sie sicher, dass keine unberechtigten Geräte wie unerwartete DHCP-Server im Netzwerk ausgeführt werden, die auf den Bereich reagieren können, oder dass Geräte in einer Schleife stecken, die das Netzwerk mit DHCP Discover-Paketen überflutet. Zusätzliche Prüfungen können mithilfe der folgenden Befehle durchgeführt werden: '**show ip dhcp relais**' und '**show ip dhcp relay statistics**'.

Class NAT Flow - copp-system-p-class-nat-flow

Diese Klasse bezieht sich auf den NAT-Datenfluss des Software-Switches. Beim Erstellen einer neuen dynamischen Übersetzung wird der Datenfluss per Software weitergeleitet, bis die Übersetzung in der Hardware programmiert ist. Anschließend wird der Datenverkehr, der an den Supervisor geleitet wird, durch CoPP geregelt, während der Eintrag in der Hardware installiert ist.

```
class-map copp-system-p-class-nat-flow (match-any)
match exception nat-flow
set cos 7
police cir 800 kbps , bc 64000 bytes
```

Auswirkungen

Diese Klasse fällt normalerweise aus, wenn eine hohe Rate neuer dynamischer Übersetzungen und Datenflüsse in der Hardware installiert wird. Die Auswirkungen beziehen sich auf Software-Switched-Pakete, die verworfen und nicht an den End-Host geliefert werden, was zu Verlusten und Neuübertragungen führen kann. Nachdem der Eintrag in der Hardware installiert wurde, wird kein weiterer Datenverkehr an den Supervisor geleitet.

Empfehlungen

- Richtlinien und Einschränkungen dynamischer NAT auf der entsprechenden Plattform überprüfen. Es gibt bekannte Einschränkungen, die auf Plattformen dokumentiert werden, wie zum Beispiel der 3548, in dem die Übersetzung einige Sekunden dauern kann. Siehe: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/93x/interfaces/configuration/guide/b-cisco-nexus-3500-nx-os-interfaces-configuration-guide-93x/b-cisco-nexus-3500-nx-os-interfaces-configuration-guide-93x_chapter_0110.html#id_35947

Klassenausnahme - copp-system-p-class-exception

Diese Klasse bezieht sich auf Ausnahmepakete, die mit der IP-Option und IP-ICMP-Paketen verknüpft sind, die nicht erreichbar sind. Wenn in der FIB keine Zieladresse angegeben ist und ein Fehler auftritt, sendet der SUP ein nicht erreichbares ICMP-Paket zurück an den Absender.

Pakete mit aktivierten IP-Optionen gehören ebenfalls zu dieser Klasse. Einzelheiten zu IP-Optionen finden Sie im IANA-Dokument: https://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml#ip-parameters-1

```
 class-map copp-system-p-class-exception (match-any)
match exception ip option
match exception ip icmp unreachable
match exception ipv6 option
match exception ipv6 icmp unreachable
set cos 1
police cir 150 kbps , bc 32000 bytes
```

Auswirkungen

Diese Klasse wird streng überwacht, und Verwerfen dieser Klasse sind kein Anzeichen für einen Ausfall, sondern ein Schutzmechanismus, der den Umfang der Pakete mit nicht erreichbaren ICMP-Dateien und IP-Optionen begrenzt.

Empfehlungen

- Überprüfen Sie, ob Datenverkehrsflüsse an die CPU gesendet oder an Ziele gesendet werden, die sich nicht auf der FIB befinden.

Klassenumleitung - copp-system-p-class-redirect

Diese Klasse bezieht sich auf Datenverkehr, der mit dem Precision Time Protocol (PTP) verknüpft ist und für die Zeitsynchronisierung verwendet wird. Dies umfasst Multicast-Datenverkehr für den reservierten Bereich 224.0.1.129/32, Unicast-Datenverkehr auf dem UDP-Port 319/320 und Ethernet-Typ 0X88F7.

```
class-map copp-system-p-class-redirect (match-any)
match access-group name copp-system-p-acl-ptp
match access-group name copp-system-p-acl-ptp-l2
match access-group name copp-system-p-acl-ptp-uc
set cos 1
police cir 280 kbps , bc 32000 bytes
```

Auswirkungen

Wenn diese Klasse nicht verfügbar ist, können Probleme bei Geräten auftreten, die nicht richtig synchronisiert wurden oder noch nicht die entsprechende Hierarchie eingerichtet haben.

Empfehlungen

-Stellen Sie die Stabilität der Uhren sicher und stellen Sie sicher, dass sie korrekt konfiguriert sind. Stellen Sie sicher, dass das PTP-Gerät für den Multicast- oder Unicast-PTP-Modus konfiguriert ist, jedoch nicht für beide gleichzeitig. Dies ist auch in den Richtlinien und Einschränkungen dokumentiert und kann den Datenverkehr über die zugesicherte Eingangsrate hinaus bewegen.

- Überprüfung des Designs und der Konfiguration der Grenzwertuhr und aller PTP-Geräte in der Umgebung Stellen Sie sicher, dass alle Richtlinien und Einschränkungen pro Plattform befolgt werden, da sie variieren.

Klasse OpenFlow- copp-system-p-class-openflow

Diese Klasse bezieht sich auf Datenverkehr, der mit OpenFlow-Agent-Vorgängen verknüpft ist, und die entsprechende TCP-Verbindung zwischen dem Controller und dem Agenten.

```
class-map copp-system-p-class-openflow (match-any)
match access-group name copp-system-p-acl-openflow
set cos 5
police cir 1000 kbps , bc 32000 bytes
```

Auswirkungen

Bei einer Unterlassung dieser Klasse können Probleme auftreten, wenn Agenten die Anweisungen des Controllers zur Verwaltung der Weiterleitungsebene im Netzwerk nicht ordnungsgemäß erhalten und verarbeiten.

Empfehlungen

- Stellen Sie sicher, dass im Netzwerk kein doppelter Datenverkehr erkannt wird oder dass ein Gerät die Kommunikation zwischen dem Controller und den Agenten behindert.

- Überprüfen Sie, ob das L2-Netzwerk nicht instabil ist (STP, Schleifen).

Fehlerbehebung bei CoPP-Verlusten

Die ersten Schritte zur Fehlerbehebung bei CoPP-Verletzungen sind:

- Auswirkungen und Umfang des Problems

- Verständnis des Datenverkehrsflusses durch die Umgebung und der Rolle des Switches bei der betroffenen Kommunikation

-Bestimmen Sie, ob Verstöße gegen die zugeordnete Klasse vermutet werden, und durchlaufen Sie diese ggf...

Das aufgelistete Verhalten wurde z. B. erkannt:

- Geräte können nicht mit anderen Geräten außerhalb ihres Netzwerks kommunizieren, sondern lokal kommunizieren.

-Der Impact wurde isoliert für die geroutete Kommunikation außerhalb des VLAN, und der Switch fungiert als Standard-Gateway.

- Eine Prüfung der Hosts zeigt an, dass sie das Gateway nicht pingen können. Nach einer Überprüfung der ARP-Tabelle bleibt der Eintrag für das Gateway unvollständig.

- Bei allen anderen Hosts, die das Gateway auflösen, treten keine Kommunikationsprobleme auf. Eine Überprüfung von CoPP auf dem Switch, der als Gateway fungiert, weist darauf hin, dass Verstöße gegen das CoPP-System-p-class-normal vorliegen.

```
class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
module 1 :
transmitted 3292445628 bytes;
dropped 522023852 bytes;
```

- Außerdem werden bei mehreren Befehlsprüfungen die Verluste aktiv erhöht.

- Diese Verletzungen können dazu führen, dass legitimer ARP-Datenverkehr verworfen wird, was zu einem Denial of Service-Verhalten führt.

Anmerkung: Es ist wichtig, zu betonen, dass CoPP die Auswirkungen auf den Datenverkehr isoliert, der der jeweiligen Klasse zugeordnet ist, die in diesem Beispiel ARP und copp-system-p-class-normal sind. Datenverkehr, der sich auf andere Klassen bezieht, z. B. OSPF, BGP wird von CoPP nicht verworfen, da sie vollständig in eine andere Klasse fallen. Wenn ARP-Probleme nicht markiert sind, können sie in andere Probleme übergehen, die sich auf Protokolle auswirken können, die von Anfang an darauf angewiesen sind. Wenn beispielsweise ein ARP-Cache das Zeitlimit überschreitet und aufgrund übermäßiger Verletzungen nicht aktualisiert wird, kann eine TCP-Sitzung wie BGP beendet werden.

- Es wird empfohlen, Prüfungen der Kontrollebene durchzuführen, z. B. Ethanalyzer, CPU-MAC-In-Band-Statistiken und CPU-Prozess, um die Angelegenheit weiter zu isolieren.

Ethanalyzer

Da der von CoPP geregelte Datenverkehr nur mit CPU-gebundenem Datenverkehr verknüpft ist, ist einer der wichtigsten Tools der Ethanalyzer. Dieses Tool ist eine Nexus-Implementierung von TShark und ermöglicht die Erfassung und Dekodierung des vom Supervisor gesendeten und empfangenen Datenverkehrs. Es kann auch Filter verwenden, die auf unterschiedlichen Kriterien basieren, z. B. Protokolle oder Header-Informationen. Dadurch wird es zu einem wertvollen Tool, um den von der CPU gesendeten und empfangenen Datenverkehr zu bestimmen.

Es wird empfohlen, zuerst den ARP-Datenverkehr zu untersuchen, der vom Supervisor erkannt wird, wenn das Ethanalyzer-Tool direkt auf der Terminal-Sitzung ausgeführt oder zur Analyse an eine Datei gesendet wird. Filter und Limits können definiert werden, um die Erfassung auf ein bestimmtes Muster oder Verhalten zu konzentrieren. Fügen Sie dazu flexible Anzeigefilter hinzu.

Ein häufiges Missverständnis ist, dass der Ethanalyzer den gesamten Datenverkehr erfasst, der den Switch durchläuft. Der Datenverkehr zwischen Hosts wird von den Hardware-ASICs zwischen den Datenports geschaltet oder geroutet und erfordert keine CPU-Beteiligung. Daher wird er normalerweise nicht von der Ethanalyzer-Erfassung erkannt. Zur Erfassung des Datenverkehrs auf Datenebene werden weitere Tools wie ELAM oder SPAN empfohlen. Um beispielsweise ARP zu filtern, verwenden Sie den folgenden Befehl:

Ethanalyzer Local Interface In-Band Display-Filter arp limit-captured-frames 0 autostop Dauer 60 > arpcpu

Wichtige konfigurierbare Felder:

-'interface inband' - bezieht sich auf Datenverkehr, der an SUP weitergeleitet wird.

-'display-filter arp' - bezieht sich auf den angewendeten tshark-Filter, die meisten Wireshark-Filter

werden akzeptiert.

-'limit-captured-frames 0' - bezieht sich auf das Limit, 0 entspricht unbegrenzt, bis durch einen anderen Parameter angehalten oder manuell durch Strg+C beendet wird

-'autostop duration 60' (automatische Stoppdauer 60'): bezieht sich auf den Stopp des Ethanalyzers nach 60 Sekunden, erstellt also einen Snapshot von 60 Sekunden ARP-Datenverkehr, der auf der CPU sichtbar ist

Die Ethanalyzer-Ausgabe wird zu einer Datei im Bootflash mit '> arpcpu' umgeleitet, die manuell verarbeitet werden kann. Nach 60 Sekunden wird die Erfassung abgeschlossen, und der Ethanalyzer wird dynamisch beendet, und die Datei arpcpu befindet sich im Bootflash des Switches, der dann verarbeitet werden kann, um die Top Talkers zu extrahieren. Beispiele:

```
show file bootflash:arpcpu | sort -k 3,5 | uniq -f 2 -c | sort -r -n | head lines 50

669 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:47 -> ff:ff:ff:ff:ff:ff ARP Who has 10.1.1.1? Tell
10.1.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:43 -> ff:ff:ff:ff:ff:ff ARP Who has 10.2.1.1? Tell
10.2.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:41 -> ff:ff:ff:ff:ff:ff ARP Who has 10.3.1.1? Tell
10.3.1.2
```

Dieser Filter ist nach folgenden Kriterien sortiert: die Quell- und die Zielspalten, dann die eindeutigen Übereinstimmungen, die gefunden wurden (jedoch die Spalte Datum ignoriert), zählen die Instanzen und fügen die angezeigte Zahl hinzu, und sortieren schließlich die Ergebnisse von oben nach unten, basierend auf der Anzahl, und zeigen die ersten 50 Ergebnisse an.

In diesem Beispiel wurden in 60 Sekunden mehr als 600 ARP-Pakete von drei Geräten empfangen, die als Geräte identifiziert wurden, bei denen ein Verstoß vermutet wurde. In der ersten Spalte des Filters wird die Anzahl der Instanzen für dieses Ereignis angegeben, die in der Erfassungsdatei im angegebenen Zeitraum angezeigt wurden.

Es ist wichtig, zu verstehen, dass das Ethanalyzer-Tool auf den In-Band-Treiber wirkt, was im Wesentlichen die Kommunikation in die ASIC ist. Theoretisch muss das Paket den Kernel und den Paketmanager durchlaufen, um an den zugehörigen Prozess selbst übergeben zu werden. CoPP und HWRL handeln, bevor der Datenverkehr im Ethanalyzer erkannt wird. Auch wenn die Anzahl der Verstöße aktiv zunimmt, durchläuft ein Teil des Datenverkehrs noch immer die Polizeirate und wird entsprechend angepasst, was einen Einblick in die an die CPU gesendeten Datenverkehrsflüsse ermöglicht. Dies ist eine wichtige Unterscheidung, da der Datenverkehr im Ethanalyzer NICHT den Datenverkehr darstellt, der die CIR verletzt und verworfen wurde.

Der Ethanalyzer kann auch offen eingesetzt werden, ohne dass ein Display-Filter oder ein Erfassungsfilter zum Abfangen des gesamten relevanten SUP-Datenverkehrs spezifiziert sind. Dies kann als Isoliermaßnahme im Rahmen der Fehlerbehebung verwendet werden.

Weitere Einzelheiten und die Verwendung des Ethanalysators finden Sie im technischen Hinweis:

https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/116136-trouble-ethanalyzer-nexus7000-00.html

https://community.cisco.com/t5/networking-documents/using-ethanalyzer-on-nexus-platform-for-control-plane-and-data/ta-p/3142665

Anmerkung: Der Nexus 7000 kann vor der 8.x-Codeversion nur Ethanalyzer-Erfassungen über den Admin-VDC durchführen, der SUP-gebundenen Datenverkehr von allen VDCs umfasst. VDC-spezifischer Ethanalyzer ist in 8.X-Codes enthalten.

CPU-MAC In-Band-Statistiken

Die In-Band-Statistiken für CPU-gebundenen Datenverkehr enthalten relevante Statistiken des In-Band-TX/RX-CPU-Datenverkehrs. Diese Statistiken können mit dem folgenden Befehl überprüft werden: '**show hardware internal cpu-mac inband stats**'. Diese Statistiken liefern Einblicke in die aktuelle Rate und die Spitzenrate.

```
show hardware internal cpu-mac inband stats`
================ Packet Statistics =====================
Packets received: 363598837
Bytes received: 74156192058
Packets sent: 389466025
Bytes sent: 42501379591
Rx packet rate (current/peak): 35095 / 47577 pps
Peak rx rate time: 2022-05-10 12:56:18
Tx packet rate (current/peak): 949 / 2106 pps
Peak tx rate time: 2022-05-10 12:57:00
```

Als Best Practice wird empfohlen, eine Baseline zu erstellen und zu verfolgen, da abhängig von der Rolle des Switches und der Infrastrukturausgabe der "show hardware internal cpu-mac inband stats" erheblich variiert. In dieser Laborumgebung sind die üblichen Werte und historischen Höchstwerte in der Regel nicht größer als ein paar hundert pps, und dies ist daher ungewöhnlich. Der Befehl "**show hardware internal cpu-mac inband events**" ist ebenfalls als historische Referenz nützlich, da er Daten zur Spitzenauslastung und zum Zeitpunkt der Erkennung enthält.

Prozess-CPU

Die Nexus-Switches sind Linux-basierte Systeme, und das Nexus-Betriebssystem (NXOS) nutzt CPU-Preemptive Scheduler, Multitasking und Multithreading seiner jeweiligen Kernarchitektur, um einen fairen Zugriff auf alle Prozesse zu ermöglichen. Daher sind Spitzenwerte nicht immer ein Anzeichen für ein Problem. Werden jedoch anhaltende Datenverkehrsverletzungen beobachtet, ist es wahrscheinlich, dass der zugehörige Prozess auch stark genutzt wird und unter den CPU-Ausgaben als wichtigste Ressource erscheint. Erstellen Sie mehrere Snapshots der CPU-Prozesse, um die hohe Auslastung eines bestimmten Prozesses zu überprüfen, indem Sie: **show process cpsort | 0.0 ausschließen** oder **Prozess-CPU-Sortierung anzeigen | grep <process>**.

Die Prozess-CPU-, In-Band-Statistiken und Ethanalyzer-Verifizierungen bieten Einblicke in die Prozesse und den Datenverkehr, der derzeit vom Supervisor verarbeitet wird. Sie helfen, die laufende Instabilität des Kontrollebenen-Datenverkehrs zu isolieren, die zu Problemen auf der Datenebene führen kann. Es ist wichtig zu verstehen, dass CoPP ein Schutzmechanismus ist. Sie ist reaktionär, da sie nur auf Datenverkehr reagiert, der an die SUP geleitet wird. Sie soll die Integrität des Supervisors durch die Rücknahme von Datenverkehrsraten schützen, die die erwarteten Bereiche überschreiten. Nicht alle Verwerfen weisen auf ein Problem hin oder erfordern Eingriffe, da ihre Bedeutung sich auf die spezifische CoPP-Klasse und die geprüften Auswirkungen bezieht, die auf der Infrastruktur und dem Netzwerkdesign basieren. Drops aufgrund von sporadischen Burst-Ereignissen führen nicht zu Auswirkungen, da Protokolle integrierte Mechanismen wie Keepalive und Neuversuche aufweisen, die mit vorübergehenden Ereignissen umgehen können. Konzentrieren Sie sich weiterhin auf anhaltende Ereignisse oder anormale Ereignisse, die über die festgelegten Basiswerte hinausgehen. Denken Sie daran, dass CoPP die für die Umgebung spezifischen Protokolle und Funktionen einhalten und kontinuierlich

überwacht und durchlaufen werden muss, um sie auf Basis der Skalierbarkeitsanforderungen im Zuge der Weiterentwicklung zu optimieren. Wenn es zu Unterbrechungen kommt, stellen Sie fest, ob CoPP den Datenverkehr unbeabsichtigt oder als Reaktion auf eine Fehlfunktion oder einen Angriff verworfen hat. In beiden Fällen ist die Situation zu analysieren und die Notwendigkeit der Eingriffe durch Analyse der Auswirkungen und Abhilfemaßnahmen auf die Umwelt zu bewerten, die außerhalb des Anwendungsbereichs des Switches liegen können.

Zusätzliche Informationen

Aktuelle Plattformen und Codes können eine SPAN-zu-CPU mithilfe eines Ports und eines Postens des Datenverkehrs auf der Datenebene zur CPU ausführen. Dies wird normalerweise durch die Hardware-Ratenbegrenzung und CoPP stark eingeschränkt. Es wird empfohlen, SPAN-CPU sorgfältig zu verwenden und wird nicht in diesem Dokument behandelt. Weitere Informationen zu dieser Funktion finden Sie in der aufgelisteten technischen Anmerkung:

https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/215329-nexus-9000-cloud-scale-asic-nx-os-span-t.html