Controleer besturingsplane voor schendingen op Nexus-platforms

Inhoud

Inleiding

Dit document beschrijft details over Control Plane Policing (CoPP) op Cisco Nexus switches en de relevante invloed ervan op niet-standaard class schendingen.

Voorwaarden

Cisco raadt u aan basisinformatie over CoPP-controle (Control Plane Policing), de richtlijnen en beperkingen ervan en de algemene configuratie te begrijpen. Naast Quality-of-Service (QoS) (Quality-of-Service) toezicht- (CIR) functionaliteit. Raadpleeg voor meer informatie over deze functie de toepasbare documenten:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het controlevliegtuigverkeer wordt naar de controlemodule omgeleid door toegangscontrolelijsten (ACL's) te heroriënteren die geprogrammeerd zijn om het gematchte verkeer op te geven dat door twee lagen bescherming passeert, de hardwaresnelheidslimiters en CoPP. Elke ontwrichting of aanval op de toezichthouder module kan, indien deze niet wordt gecontroleerd, leiden tot ernstige netwerkstoringen; CoPP moet dus als beschermingsmechanisme dienen. Als er sprake is van instabiliteit op het niveau van het besturingsplane, is het belangrijk om CoPP te controleren, omdat abnormale verkeerspatronen die zijn ontstaan door lussen of overstromingen, of schurkenapparatuur de supervisor kunnen belasten en verhinderen dat hij het legitieme verkeer verwerkt. Dergelijke aanvallen, die ofwel onopzettelijk door schurkenmachines of opzettelijk door aanvallers kunnen worden uitgevoerd, hebben doorgaans betrekking op hoge verkeerstarieven die bestemd zijn voor de toezichthouder of de CPU.

Controle van besturingsplane (CoPP) is een functie die het besturingsplane beschermt door alle ontvangen pakketten over de in-band (voorpaneel) poorten die bestemd zijn voor de routeradressen te segregeren en classificeren, of die een mate van toezicht vereisen en ze controleren op basis van een geëngageerd invoertarief (CIR). Met deze functie kan een beleidskaart op het bedieningspaneel worden toegepast. Deze beleidskaart lijkt op een beleid van normale kwaliteit van de service en wordt toegepast op al het verkeer dat de switch binnenkomt vanuit een niet-beheerpoort. Bescherming van de Supervisor module door middel van toezicht stelt de switch in staat om overstromingen van verkeer te verzachten die verder gaan dan de vastgelegde ingangswaarden voor elke klasse door het weggooien van de pakketten en te voorkomen dat de switch overweldigd wordt en de prestaties beïnvloeden.

Het is van belang de CoP-tellers voortdurend te volgen en te rechtvaardigen, hetgeen het doel van dit document is. CoP-schendingen kunnen, als ze niet worden gecontroleerd, verhinderen dat het besturingsplane echt verkeer op de corresponderende getroffen klasse verwerkt. De CoP-configuratie is een evoluerend en doorlopend proces dat moet inspelen op de netwerk- en infrastructurele vereisten. Er zijn drie standaardinstellingen voor CoPP. Standaard raadt Cisco het gebruik van het standaardbeleid '**strikte**' aan als het beginpunt en wordt de basis voor dit document gebruikt.

CoPP is alleen van toepassing op in-band verkeer dat door de voorpaneelpoorten wordt

ontvangen. De out-of-band beheerpoort (GMT0) is niet aan CoPP onderworpen. De hardware van het apparaat van Cisco NX-OS voert CoPP op een per-expediteur-motor basis uit. Kies daarom tarieven zodat het geaggregeerde verkeer niet overweldigend is voor de supervisor module. Dit is vooral belangrijk voor end-of-row/modulaire switches, aangezien de CIR van toepassing is op het geaggregeerde verkeer van het aan CPU gebonden verkeer van alle modules.

Toepasselijke hardware

De component die in dit document wordt besproken, is van toepassing op alle switches van Cisco Nexus-datacenter.

Interpretatie van de controle van het besturingsplane

De focus van dit document is om de meest voorkomende en kritieke niet standaard class-schendingen die te zien zijn op Nexus switches aan te pakken.

Standaard CoPP-profiel

Om te begrijpen hoe CoPP moet worden geïnterpreteerd, moet de eerste verificatie zijn om te verzekeren dat een profiel wordt toegepast en om te begrijpen of een standaardprofiel of een aangepaste profiel op de switch wordt toegepast.

> **Opmerking:** Als best practice moeten alle Nexus switches CoPP ingeschakeld hebben. Als deze optie niet is ingeschakeld kan dit instabiliteit veroorzaken voor al het verkeer van het besturingsplane omdat verschillende platforms Supervisor (SUP) gebonden verkeer beperken. Als CoPP bijvoorbeeld niet is ingeschakeld op een Nexus 9000, is het voor de SUP bestemde verkeer beperkt tot 50 pps, waardoor de switch bijna onwerkbaar is. CoPP wordt beschouwd als een vereiste voor Nexus 3000- en Nexus 9000-platforms.

Als CoPP niet is ingeschakeld, kan deze op de switch opnieuw worden ingeschakeld of ingesteld door de opdracht '**Setup**' uit te voeren of door een van de standaardbeleidslijnen toe te passen onder de optie Configuration: **profiel van het copp [dense|lenient|gematigd|strak]**.

Een onbeschermd apparaat classificeert en scheidt verkeer niet naar klassen en zo is elke weigering van dienstgedrag voor een bepaalde functie of protocol niet in dat toepassingsgebied opgenomen en kan het gehele regelvlak beïnvloeden.

> **Opmerking:** CoPP-beleid wordt uitgevoerd door Ternary Content-Adresseerbare Memory (TCAM) classificatie-omleidingen, en kan rechtstreeks worden gezien onder '**show system interne access-list invoerstatistieken module X | b CoPP"** of '**toon details voor toegang tot hardware-ingangslijsten**'.

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

Toezichtklassen van besturingsplane

CoPP classificeert verkeer op basis van de overeenkomsten die overeenkomen met IP- of MAC-ACL's. Daarom is het belangrijk te begrijpen wat verkeer onder welke klasse is ingedeeld.

De klassen, die afhankelijk zijn van het platform, kunnen verschillen. Het is dus belangrijk om te begrijpen hoe je de lessen kunt verifiëren.

Bijvoorbeeld, op **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 dit voorbeeld, **omvat** de class-map **copp-system-p-class-criet**, verkeer gerelateerd aan routing protocollen, zoals Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Protocol (DHCP) en andere protocollen, zoals vPC.

De IP- of MAC-ACL's-naamgevingsconventie is meestal een zelfverklaring voor het protocol of de functie in kwestie, met het prefix **copp-acl-[protocol|optie]**.

Om een specifieke klasse te bekijken, kan het direct worden gespecificeerd terwijl de show opdracht wordt uitgevoerd. Voorbeeld:

```
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
```

Terwijl de CoPP standaardprofielen normaal verborgen zijn als deel van de standaardconfiguratie, kunt u de configuratie zien met '**show run-conf copp all**':

```
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)
...
```

De class-map **copp-system-p-class-criet**, gezien vóór, verwijzingen meerdere overeenkomende verklaringen die op systeem ACL**'s roepen**, die standaard verborgen zijn, en verwijzen naar de classificatie die op gecompenseerd wordt. Bijvoorbeeld voor 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)
```

Dit betekent dat elk BGP-verkeer met deze klasse overeenkomt en is geclassificeerd onder **kritiek van het copp-systeem-p-klasse**, samen met alle andere protocollen op dezelfde klasse.

De **Nexus 7000** heeft een sterk vergelijkbare CoPP-structuur als de 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
```

Het is belangrijk om op te merken dat op een Nexus 7000, aangezien het hier modulaire switches zijn, de klasse wordt gedeeld door module; Het CIR geldt echter voor het totaal van alle modules en CoPP geldt voor het gehele chassis. De CoP-verificatie en -uitvoer kunnen alleen worden gezien vanuit de standaard- of admin Virtual Devices Context (VDC).
Het is met name belangrijk om CoPP op een Nexus 7000 te controleren als er problemen zijn met het besturingsplane, omdat instabiliteit op een VDC met overmatig CPU-gebonden verkeer dat CoPP-schendingen veroorzaakt, de stabiliteit van andere VDC's kan beïnvloeden.

Op een **Nexus 5600** verschillen de klassen. Voor BGP is het dus zijn eigen aparte 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)
```

Op een **Nexus 3100** zijn er 3 routingprotocol klassen, zodat u kunt controleren tot welke klasse BGP behoort, referentie de 4 CoPP ACL die gerefereerd is aan:
DHCP wordt behandeld door zijn eigen klasse op Nexus 3100.

```
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 dit geval, wordt BGP door het ACL **copp-systeem-acl-routingproto1** gematcht, en zo valt de CoPP klasse BGP in zijn **copp-s-RoutingProto1**.

Toezichtstatistieken en -tellers van het besturingsplane

CoPP ondersteunt QoS statistieken om de geaggregeerde tellers van verkeer te volgen die de vastgelegde invoersnelheid (CIR) voor een bepaalde klasse bevestigen of overtreden, voor elke module.
Elke class-map categoriseert CPU-gebonden verkeer, op basis van de klasse waarin het overeenkomt met, en voegt een CIR toe voor alle pakketten die onder die classificatie vallen. Als voorbeeld wordt de klasse die op **BGP**-verkeer betrekking heeft gebruikt als referentie:

Op een Nexus 9000 top-of-rack (TOR) voor **kritiek op het copp-systeem-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
```

In het gedeelte van de class-map, na de wedstrijdverklaringen, zien we de acties die betrekking hebben op al het verkeer binnen de klas. Al het verkeer dat binnen **copp-system-p-class-kritiek** is ingedeeld, is ingesteld met een serviceklasse (CoS) van 7, dat het hoogste prioriteitsverkeer is, en deze klasse wordt gecontroleerd met een CIR van 36000 kbps en een geëngageerd-burst-rate van 128000 bytes. Verkeersverkeer dat met dit beleid overeenkomt, wordt naar de SUP verzonden om te worden verwerkt en alle schendingen worden ingetrokken.

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

In de volgende paragraaf worden de statistische gegevens betreffende de module, voor switches boven-rek (TOR), met één module, en in module 1 wordt verwezen naar de 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
```

De statistieken die op de output worden gezien, zijn historisch, zodat dit een momentopname biedt van de huidige statistieken op het moment dat de opdracht wordt uitgevoerd.

Hier zijn twee onderdelen te interpreteren: de **uitgezonden** en **uitgebrachte** delen:
De verzonden datapoint volgt alle verzonden pakketten die met het beleid in overeenstemming zijn. Deze sectie is belangrijk aangezien het inzicht in het type verkeer verschaft dat de supervisor verwerkt.

De aangeboden waarde van 5 minuten geeft inzicht in het huidige tarief.
Het conformeerde piektarief en de datum, voorzien in een breuk van het hoogste piektarief per seconden dat nog steeds in het beleid en het tijdstip dat het plaatsvond.
Als er een nieuwe piek wordt gezien, dan vervangt deze deze waarde en datum.

Het belangrijkste deel van de statistieken is de ingetrokken datapoint. Net zoals de verzonden statistieken, volgt de ingetrokken sectie de cumulatieve bytes die zijn gevallen als gevolg van schendingen van het politiecijfer.
Het voorziet ook in de schending van de afgelopen 5 minuten, de overtreden piek, en als er een piek is, de tijdstempel van die piekbreuk. En nogmaals, als er een nieuwe piek wordt gezien, dan vervangt hij deze waarde en datum. Op andere platforms varieert de output, maar de logica is zeer gelijkend.

Nexus 7000 volgt een identieke structuur en de verificatie is hetzelfde, hoewel sommige klassen enigszins verschillen van de ACL's waarnaar wordt verwezen:

```
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
```

Op een 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;
```

Hoewel het geen informatie geeft over de snelheid of pieken, geeft het nog steeds de

geaggregeerde bytes die zijn gevormd en zijn overtreden.

Op een **Nexus 3100**, toont de uitvoer van het controlevliegtuig, OutPackets en DropPackets

```
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 verwijzen naar gecodeerde pakketten, terwijl DropPackets naar schendingen aan de CIR verwijzen. In dit scenario zien we geen druppels op de corresponderende klasse.

Op een **Nexus 3500** wordt in de uitvoer het volgende aangegeven:

```
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
```

De HW Aangepaste pakketten verwijzen naar de pakketten die in HW door ACL worden aangepast. Net zoals bij de politie zijn de pakjes met de politie. Elk verschil tussen de HW en SW overeenkomende pakketten impliceert een schending.
In dit geval, zijn er geen druppels gezien bij het verzenden van protocol-1 klassenpakketten (die BGP omvatten), als de waarden overeenkomend.

Controle op actieve Drop Violations

Gezien het feit dat de politiestatistieken van het besturingsplane historisch zijn, is het belangrijk vast te stellen of er sprake is van actieve overtredingen die toenemen. De standaardmanier om deze taak uit te voeren is om twee volledige outputs te vergelijken en eventuele verschillen te verifiëren.
Deze taak kan handmatig worden uitgevoerd, of de Nexus-switches bieden het 'diff'-gereedschap dat kan helpen om de output te vergelijken.
Hoewel de gehele productie kan worden vergeleken, is deze niet nodig omdat de nadruk alleen op de ingetrokken statistieken ligt. De CoPP-productie kan dus worden gefilterd zodat deze alleen op de schendingen is gericht.

Deze opdracht is: **Beleids- en -kaartbesturingsplane voor de interface tonen | Nierklassen |module|overtreden |gevallen | diff-y**

> **Opmerking:** De opdracht moet twee keer worden uitgevoerd zodat de diff de stroom kan vergelijken met de vorige uitvoer.

```
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;
```

Met de vorige opdracht kunt u de delta tussen twee klassen zien en overschrijvingsverhogingen vinden.

> **Opmerking:** Aangezien de CoPP-statistieken historisch zijn, is een andere aanbeveling om de statistieken na de uitvoering van de opdracht vrij te geven, om na te gaan of er actieve stijgingen zijn. U verwijdert de CoPP-statistieken als volgt: " **duidelijke copp - statistieken** "

Typen CoPP-druppels

CoPP is een eenvoudige controlestructuur, aangezien elk CPU-gebonden verkeer dat de CIR schendt, wordt ingetrokken. De gevolgen zijn echter aanzienlijk afhankelijk van het soort druppels. Hoewel de logica hetzelfde is, is het niet hetzelfde om verkeer te laten vallen dat is bestemd voor **kritiek op het copp-systeem-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
```

in vergelijking met het druppelverkeer dat bestemd is voor class-map **copp-system-p-class-**

monitoring.

```
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
```

Het eerste gaat over de meest routingprotocollen, het tweede over het Internet Control Message Protocol (ICMP), dat een van de laagste prioriteiten en CIR heeft. Het verschil op CIR is honderd keer zo groot. Daarom is het belangrijk de klassen, de effecten, de gemeenschappelijke controles/verificaties en de aanbevelingen te begrijpen.

CoP-klassen

Class Monitoring - copp-system-p-class-monitoring

Deze klasse omvat, ICMP voor IPv4 en IPv6 en traceroute van verkeer dat op de switch in kwestie wordt gericht.

```
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
```

Impact

- Een veel voorkomend misverstand wanneer u pakketverlies of vertragingen bij het oplossen van problemen wilt oplossen, veroorzaakt dat de switch door zijn in-band poorten, die door CoPP aan snelheid zijn beperkt. Aangezien CoPP zwaar toezicht houdt op ICMP, zelfs met een laag verkeer of congestie, kan het pakketverlies worden gezien wanneer u in-band interfaces direct indrukt als zij de CIR overtreden.

Bijvoorbeeld, door direct aangesloten interfaces op routed havens te pingelen, met een pakketlading van 500, kunnen de dalingen periodiek worden gezien.

```
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
```

Op de Nexus, waar de ICMP-pakketten bedoeld waren, zien we dat CoPP ze liet vallen toen de schending werd gedetecteerd en de CPU werd beschermd:

```
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
```

Als u problemen wilt oplossen bij latentie of pakketverlies, wordt het aanbevolen om hosts die door de switch bereikbaar zijn, te gebruiken in het gegevensvliegtuig, dat niet bestemd is voor de switch zelf, maar het luchtverkeer moet controleren. Het dataverkeer wordt doorgestuurd/routeerd op hardwareniveau zonder SUP-interventie en dus niet gecontroleerd door CoPP, en heeft doorgaans geen druppels.

Aanbevelingen

- Controleer valse positieve resultaten voor pakketverlies door een ping over de switch door het gegevensvliegtuig te verzenden, niet naar de switch

-Limit Network Monitoring System (NMS) of tools die op agressieve wijze gebruik maken van ICMP in de switch om een uitbarsting te voorkomen via de vastgelegde invoersnelheid voor de klasse. Denk eraan dat CoPP van toepassing is op al het geaggregeerde verkeer dat in de klas valt.

Class Management - copp-system-p-class-beheer

Zoals hier te zien is, omvat deze klasse verschillende beheerprotocollen die kunnen worden gebruikt voor communicatie (SSH, telnet), overdrachten (SCP, FTP, SFTP, TFTP), kloktijd (NTP), AAA (Radius/TACACS) en controle (SNMP), voor IPv4 en IPv6 communicatie.

```
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
```

Impact

De meest voorkomende gedragingen of vallen die bij deze klasse horen, zijn:

- Veronderstelde CLI-vertraging bij aansluiting door SSH/telnet. Als er actieve vallen op de klas staan, kunnen communicatiesessies langzaam zijn en lijden aan druppels.
-Bestanden overzetten met FTP, SCP, SFTP, TFTP-protocollen op de switch. Het meest voorkomende gedrag dat we zien is een poging om systeemafbeeldingen over te brengen/te starten door in-band beheerpoorten. Dit kan leiden tot hogere overdrachtstijden en gesloten/afgesloten transmissiesessies bepaald door de totale bandbreedte voor de klasse.
- NTP-synchronisatieproblemen, is deze klasse ook belangrijk omdat het scheurende NTP-agents of aanvallen verzacht.
- De diensten van AAA Radius en TACACS vallen ook onder deze categorie. Als het effect op deze klasse wordt waargenomen, kan het de autorisatie- en authenticatiediensten beïnvloeden op de switch voor gebruikersrekeningen, die ook kunnen bijdragen tot vertraging op de opdrachten van de CLI.
-SNMP wordt ook onder deze klasse gecontroleerd. Het meest voorkomende gedrag dat gezien wordt als gevolg van vallen vanwege de SNMP-klasse, is op NMS-servers, die lopen, bulkcollecties of netwerkscans uitvoeren. Wanneer periodieke instabiliteit optreedt, is deze meestal gecorreleerd aan het NMS-verzamelingsschema.

Aanbevelingen

- Als CLI traagheid gezien wordt, samen met druppels in deze klasse, gebruik console toegang, of management out-of-band toegang (gmt0).

-Als systeembeelden naar de switch moeten worden geüpload, gebruik dan de out-of-band beheerpoort (GMT0) of gebruik de USB-poorten voor de snelste overdracht.

- Als NTP-pakketten verloren gaan, controleer dan 'show ntp peer-status' en controleer de bereikbaarheidskolom, geen druppels vertalen zich naar 377.

- Als er problemen worden gezien met de AAA-services, gebruik dan alleen lokale gebruikers om problemen op te lossen, totdat het gedrag is verzacht

- Beperken voor SNMP-problemen zijn minder agressief gedrag, doelgerichte verzameling of minimalisering van netwerkscanners. Onderzoek periodieke tijden van scanners tot gebeurtenissen op het niveau van de CPU.

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

Deze class gaat specifiek in op pakketten die leunen. Dit type pakket wordt ook verwerkt door de Hardware Rate Limiter (WHRL).
Als het ARP-verzoek (Admission Protocol) voor de volgende hop niet wordt opgelost wanneer inkomende IP-pakketten in een lijnkaart worden verzonden, stuurt de lijnkaart de pakketten naar de supervisor module door.

De toezichthouder lost het MAC adres voor de volgende hop op en programma's de hardware.

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

Dit gebeurt normaal wanneer statische routes worden gebruikt en de volgende hop onbereikbaar of onopgelost is.

Wanneer een ARP-verzoek wordt verstuurd, voegt de software een /32-druppelnabijheid in de hardware toe om te voorkomen dat de pakketten op hetzelfde IP-adres worden verzonden naar de supervisor. Wanneer het ARP wordt opgelost, wordt de hardware-invoer bijgewerkt met het juiste MAC-adres. Als het ARP-nummer niet is opgelost voor een tijdelijke periode, wordt de ingang van de hardware verwijderd.

> **Opmerking:** CoPP en HWRL werken tegelijkertijd om ervoor te zorgen dat de CPU wordt beschermd. Terwijl zij schijnen soortgelijke functies uit te voeren, treedt eerst HWRL op. De implementatie is gebaseerd op de plaats waar de specifieke functie wordt toegepast op de verzendingsmotoren op de ASIC. Deze seriële benadering maakt granulariteit en meerlaagse bescherming mogelijk die alle CPU-gebonden pakketten bespoedigen.

De HWRL wordt uitgevoerd per instantie/verzendmotor op de module en kan worden bekeken met de opdracht '**show hardware rate-limiter**'. HWRL valt buiten het toepassingsgebied van dit technische document.

```
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
```

Impact

- Het vliegtuigverkeer wordt naar de toezichthouder gestraft als een schending, aangezien het niet in hardware kan worden verwerkt en op die manier druk op de CPU uitoefent.

Aanbevelingen

- De gezamenlijke resolutie voor deze kwestie om de gleaanse vallen te minimaliseren is om te verzekeren dat de volgende hop bereikbaar is en om glein-trotling door de configuratieopdracht mogelijk te maken: '**hardware ip gleb throttle** '

Raadpleeg: 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

-Bij Nexus 7000, 8.4(2), werd ook ondersteuning van het vloeibaar filter geïntroduceerd voor makreelnabijheid voor M3- en F4-modules. Raadpleeg: 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

- Bekijk alle statische routeconfiguraties die onbereikbare next-hop adressen gebruiken of dynamische routingprotocollen gebruiken die dergelijke routes uit de RIB dynamisch kunnen verwijderen

Class Critical - class-map copp-system-p-class-kritiek

Deze klasse verwijst naar de meest kritische controlevliegtuigprotocollen vanuit een L3-perspectief, die routingprotocollen voor IPv4 en IPv6 omvatten (RIP, OSPF, DHCP, BGP), auto-RP, virtueel poortkanaal (vPC), en l2pt en 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
```

Impact

Droogt op **copp-system-p-class-kritische** overdrachtinstabiliteit aan het routeren van protocollen, die nabijheid kunnen omvatten druppelend of convergentiemislukkingen, of update/NLRI propagatie.
De meest voorkomende beleidsdruppels op deze klasse kunnen betrekking hebben op schurkenapparatuur op het netwerk die abnormaal werkt (door een foutieve configuratie of storing) of schaalbaarheid.

Aanbevelingen

- Als er geen anomalieën worden gedetecteerd, zoals een schurkenapparaat of L2 instabiliteit die een voortdurende convergentie van bovenlaagprotocollen veroorzaakt, dan kan een aangepaste configuratie van CoPP of een meer lenientere klasse vereist zijn om de schaal aan te passen.
- Raadpleeg de CoPP-configuratiehandleiding voor hoe u een aangepast CoPP-profiel kunt configureren vanuit een standaardprofiel dat momenteel bestaat.
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

Belangrijk van klasse - copp-system-p-klasse

Deze klasse heeft betrekking op de first-hop redundantie protocollen (FHRP), inclusief HSRP, VRRP en ook 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
```

Impact

Het meest voorkomende gedrag dat hier wordt gezien en tot druppels leidt, zijn problemen met Layer 2 instabiliteit, wat leidt tot apparaten die zich aan het transitioneren in actieve (gesplitste brein) scenario's, agressieve timers, misconfiguraties of schaalbaarheid aanpassen.

Aanbevelingen

- Zorg ervoor dat voor FHRP groepen goed zijn geconfigureerd en dat er goed wordt onderhandeld over de rollen active/stand-by of primair/secundair, en dat er geen sprake is van flaps op de staat.

-Controleer op convergentiekwesties bij L2 of problemen met multicast propagatie voor het L2-domein.

Klasse L2 Niet-opgeleid - copp-system-p-class-l2 zonder toezicht

De L2 niet-gepolitieerde klasse verwijst naar alle kritische Layer 2-protocollen die de basis zijn voor alle bovenlaagprotocollen en die dus worden beschouwd als bijna niet gepoligeerd met de hoogste CIR en prioriteit.
Effectief, deze klasse behandelt, 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
```

Deze klasse heeft een CIR van de politie van 50 Mbps, het hoogste van alle klassen, samen met de hoogste absorptie van burst.

Impact

vallen op deze klasse kan leiden tot mondiale instabiliteit, aangezien alle bovenlaagprotocollen en communicatie over gegevens, controle, en beheervliegtuigen afhankelijk zijn van een onderliggende Layer 2 stabiliteit.

Problemen met STP-schendingen kunnen GN's en STP-convergentiekwesties veroorzaken, waaronder STP-geschillen, MAC-flushes, -bewegingen en het leren van gehandicapte gedragingen. Dit veroorzaakt bereikbaarheidsproblemen en kan verkeersmaten veroorzaken die het netwerk destabiliseren.

Deze klasse verwijst ook naar LACP, en behandelt dus alle EtherType-pakketten geassocieerd met 0x8809, die alle LACPDUs omvatten die worden gebruikt om de staat van de haven-kanaalobligaties te bewaren. Instabiliteit op deze class kan de oorzaak zijn dat de poortkanalen stilvallen als de LACPDU's worden ingetrokken.

Cisco Fabric Service over Ethernet (CSFoE) valt binnen deze klasse en wordt gebruikt om kritieke toepassingscontrolestatus tussen Nexus-switches te communiceren en is daarom imperatief voor stabiliteit.

Het zelfde is van toepassing op andere protocollen binnen deze klasse, die CDP, UDLD, en VTP omvat.

Aanbevelingen

- Het meest algemene gedrag heeft betrekking op L2 Ethernet instabiliteit. Zorg ervoor dat STP op een deterministische manier correct is ontworpen met de relevante functieverbeteringen in het spel om de impact van convergentie- of scheerapparaten in het netwerk te minimaliseren. Zorg ervoor dat het juiste STP poorttype is geconfigureerd voor alle end-host apparaten die niet deelnemen aan de L2-extensie, zijn geconfigureerd als rand/rand boomstampoorten om TCN's te minimaliseren.

Gebruik verbeteringen van STP, zoals BPDUGuard, LoopGuard, BPDUfilter, RootGuard waar nodig om het bereik van een storing of problemen met verkeerde configuratie of schurkenapparaten op het netwerk te beperken.

Raadpleeg: 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

-Controleer op MAC-bewegingsgedrag dat kan leiden tot MAC-leren dat uitgeschakeld en opvliegt. Raadpleeg: 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

Deze klasse verwijst naar besturingsplane-protocol onafhankelijke multicast (PIM) pakketten die gebruikt worden voor het instellen en beheersen van routed multicast-gedeelde bomen door alle PIM-enabled-apparaten in het dataplatform, inclusief First-Hop-router (FHR), Last-Hop-router (LHR), Intermediate-Hoprouters (IHR) en Rendezvouz Point (RPs). Packets die binnen deze klasse zijn ingedeeld, omvatten PIM-registratie voor bronnen, PIM-verbindingen voor ontvangers voor zowel IPv4 als IPv6, in het algemeen elk verkeer dat bestemd is voor PIM (224.0.13), en Multicast Source Discovery Protocol (MSDP). Let erop dat er meerdere extra klassen zijn die betrekking hebben op zeer specifieke delen van de multicast- of RP-functionaliteit die door verschillende klassen worden verwerkt.

```
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
```

Impact

De belangrijkste impact op druppels die op deze klasse betrekking hebben wordt geassocieerd met kwesties die naar multicastbronnen communiceren door PIM registratie naar de RP's of PIM voegen zich bij niet juist verwerkt, wat de gedeelde of kortste padbomen naar de bronnen van de multicaststroom of naar de RP's zou destabiliseren. Gedrag kan uitgaande interface-lijst (OIL) omvatten die niet goed gevuld is door het ontbreken van grappen, of (S, G), of (*, G) die niet consistent in het hele milieu is gezien. Problemen kunnen ook ontstaan tussen multicast routing domeinen die op MSDP vertrouwen voor interconnectie.

Aanbevelingen

- Het meest voorkomende gedrag bij PIM controle-gerelateerde kwesties heeft betrekking op schaalproblemen of schurkengedrag. Een van de meest voorkomende gedragingen wordt gezien door de implementatie op UPnP, die ook problemen kan opleveren met de uitputting van het geheugen. Dit kan worden aangepakt door filters en het beperkte bereik van schurkenmachines. Voor meer informatie over hoe de multicast-besturingspakketten voor het beperken en filteren, afhankelijk van de netwerkrol van het apparaat, raadpleegt u:

Multicastfiltering op Nexus 7K/N9K - Cisco configureren

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

Deze klasse verwijst naar Multicast Luistener Discovery (MLD), specifiek MLD query, rapport, reductie en MLDv2 pakkettypes. MLD is een IPv6-protocol dat een host gebruikt om multicast gegevens voor een bepaalde groep aan te vragen. Met de informatie die via MLD wordt verkregen, houdt de software een lijst bij van multicast groepslidmaatschap of kanaallidmaatschap per interface. De apparaten die MLD-pakketten ontvangen verzenden de multicast gegevens die ze voor gevraagde groepen ontvangen of kanalen uit het netwerksegment van de bekende

ontvangers. MLDv1 is afgeleid van IGMPv2 en MLDv2 is afgeleid van IGMPv3. IGMP gebruikt IP Protocol 2 berichttypes, terwijl MLD IP Protocol 58 berichttypes gebruikt, wat een subset is van de ICMPv6 berichten.

```
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
```

Impact

De dalingen op deze klasse vertalen naar kwesties op link-lokale IPv6 multicast communicatie, die luisterrapporten van ontvangers of reacties op algemene vragen kunnen veroorzaken om te worden gedropt, wat die ontdekking van multicast groepen voorkomt de gastheren willen ontvangen. Dit kan invloed hebben op het snooping mechanisme en niet op de juiste manier door te sturen verkeer door verwachte interfaces die om het verkeer vroegen.

Aanbevelingen

- Aangezien MLD-verkeer op een link-lokaal niveau aanzienlijk is voor IPv6, als er druppels in deze klasse worden gezien, hebben de meest voorkomende gedragsoorzaken te maken met schaal, L2 instabiliteit of schurkenapparatuur.

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

Deze klassen verwijzen naar verkeer dat bij een multicast uitzondering op omleiding naar SUP aansluit. In dit geval zijn er twee voorwaarden die door deze klassen worden verwerkt. De eerste is fout in het doorsturen van de route (RPF) en de tweede is misser van de bestemming. Miss-bestemming verwijst naar multicast pakketten waar de raadpleging in hardware voor de Layer 3 multicast-verzendtabel mislukt, en dus wordt het gegevenspakket naar de CPU geleid. Deze pakketten worden soms gebruikt om het multicast controlevliegtuig te activeren/te installeren en de ingangen van de hardware die tabellen moeten verzenden toe te voegen, op basis van het gegevensverkeer. Data plane multicast pakketten die de RPF overtreden, zouden ook met deze uitzondering overeenkomen en als een schending worden geclassificeerd.

```
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
```

Impact

Fouten van RPF en de Misselijkheid van de Bestemming impliceren een ontwerp of een configuratiekwestie met betrekking tot hoe het verkeer door de multicast router stroomt. DoelMisses zijn gebruikelijk bij het creëren van de staat, vallen kunnen leiden tot het

programmeren en creëren van (*, G), (S, G) falend.

Aanbevelingen

- Veranderingen in het ontwerp van het uniek project uitvoeren, of statische route toevoegen om verkeer door een bepaalde interface te sturen in het geval van een defect van het RPF-bestand.

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

Class IGMP - Comp-system-p-class-igmp

Deze klasse verwijst naar alle IGMP-berichten, voor alle versies die worden gebruikt om multicast gegevens voor een bepaalde groep aan te vragen en door de IGMP-snooping functionaliteit worden gebruikt om de groepen en relevante uitgaande interface-lijst (OIL) te behouden die het verkeer doorsturen naar de geïnteresseerde ontvangers op Layer 2. De IGMP-berichten zijn lokaal belangrijk omdat ze geen Layer 3-grens overschrijden, omdat hun tijd om te leven (TTL) 1 moet zijn, zoals gedocumenteerd onder RFC2236 (https://datatracker.ietf.org/doc/html/rfc2236). De IGMP-pakketten die door deze klasse worden verwerkt omvatten alle lidmaatschapsvragen (algemeen of bron/groep specifiek), samen met het lidmaatschap en verlaten rapporten van de ontvangers.

```
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
```

Impact

Als u op deze class valt, vertaalt u zich naar problemen op alle niveaus van een multicast communicatie tussen bron en ontvanger, afhankelijk van het type IGMP-bericht dat als gevolg van de schending is achtergelaten. Als de lidmaatschapsrapporten van ontvangers verloren zijn, dan is de router niet op de hoogte van apparaten die op het verkeer geïnteresseerd zijn en omvat het dus niet de interface/VLAN op zijn relevante vertrekinterfacelijst. Als dit apparaat ook de kwader of aangewezen router is, roept het niet de relevante PIM bij berichten naar de RP aan als de bron voorbij het lokale Layer 2 domein is, en stelt het dus nooit het gegevensvliegtuig over de multicast boom helemaal tot aan de ontvanger of RP vast. Als het verlofrapport verloren is, kan de ontvanger ongewenst verkeer blijven ontvangen. Dit kan ook alle relevante IGMP vragen beïnvloeden die door de kwader en de communicatie tussen de multicast routers in een domein worden veroorzaakt.

Aanbevelingen

- De meest voorkomende gedragingen die geassocieerd worden met IGMP-druppels hebben te maken met L2-instabiliteit, problemen met timers of schaal.

Klasse Normaal - copp-systeem-p-klasse-normaal

Deze klasse verwijst naar verkeer dat standaard ARP verkeer aanpast en omvat ook verkeer verbonden met 802.1X, gebruikt voor op poort gebaseerde controle van de netwerktoegang. Dit is een van de meest algemene klassen die schendingen als ARP verzoeken tegenkomt, Gratouve

ARP, Omgekeerde ARP pakketten worden uitgezonden en door het volledige Layer 2 domein verspreid. Het is belangrijk om te onthouden dat ARP-pakketten geen IP-pakketten zijn, deze pakketten geen L3-header bevatten, en dus wordt de beslissing alleen genomen met behulp van de L2-headers. Als een router met een IP interface verbonden met die ubnet, zoals een Virtuele Interface van de Switch (SVI) wordt gevormd, bepaalt de router de ARP pakketten aan SUP die moeten worden verwerkt, aangezien zij aan het adres van de hardware uitzending bestemd zijn. Elke uitzending storm, Layer 2 loop (door STP of flaps), of een routeapparaat in het netwerk kan tot een ARP storm leiden die schendingen veroorzaakt om aanzienlijk te verhogen.

```
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
```

Impact

De gevolgen van de schendingen in deze klasse zijn sterk afhankelijk van de duur van de gebeurtenissen en de rol van de switch op het milieu. Drops in deze klasse impliceert dat ARP-pakketten worden weggegooid en dus niet worden verwerkt door de SUP-motor, wat kan leiden tot twee belangrijke gedragingen veroorzaakt door onvolledige ARP-resoluties.

Vanuit het perspectief van de eindgastheer, kunnen de apparaten in het netwerk de adresresolutie met de switch niet oplossen of voltooien. Als dit apparaat als standaardgateway voor het segment fungeert, kan het tot apparaten leiden die niet hun gateway kunnen oplossen en dus niet kunnen leiden om buiten hun L2 Ethernet-segment (VLAN) te bewegen. Apparaten kunnen nog op het lokale segment communiceren als ze de ARP-resolutie voor andere eindhosts op het lokale segment kunnen voltooien.

Vanuit het gezichtspunt van de switch, als de storm en de schendingen overheersen, kan dit er ook toe leiden dat de switch het proces voor ARP-aanvragen niet kan voltooien. Deze verzoeken worden normaal gegenereerd voor de volgende-hop of direct verbonden subnetresoluties. Hoewel de ARP-antwoorden van unieke aard zijn, aangezien ze gericht zijn op de MAC van de switch, worden ze ingedeeld onder dezelfde klasse, aangezien het nog steeds ARP-pakketten zijn. Dit vertaalt zich in bereikbaarheidskwesties omdat de switch verkeer niet correct kan verwerken als de volgende hop niet wordt opgelost en kan leiden tot kwesties met Layer 2 header herschrijven als de Nabency Manager geen entry voor de host heeft.

Het effect hangt ook af van de reikwijdte van het fundamentele probleem dat tot de ARP-schending heeft geleid. Bijvoorbeeld, in een uitzendstorm, blijven de hosts en de switch tot ARP doorgaan om te proberen de nabijheid op te lossen, wat kan leiden tot extra uitzending op het netwerk, en aangezien ARP pakketten Layer 2 zijn, is er geen Layer 3 tijd om een L2 lus te breken (TTL) om een L2 lus te breken en zullen zij exponentieel door het netwerk groeien tot de lus wordt gebroken.

Aanbevelingen

- Los elke fundamentele L2 instabiliteit op die ARP stormen op het milieu kan veroorzaken, zoals STP, kranen, of scheerapparaten. Breek indien nodig die lopen door een gewenste methode om het link pad te openen.

-Storm-control kan ook gebruikt worden om een ARP storm te verzachten. Als stormcontrole niet is ingeschakeld, verifieer dan de tegenstatistieken over interfaces om het percentage uitgezonden

verkeer dat op de interfaces wordt gezien te verifiëren in verhouding tot het totale verkeer dat door de interface passeert.

- Als er geen storm is, maar er nog steeds constante druppels in het milieu worden gezien, controleer het SUP verkeer om enige schurkenapparaten te identificeren, constant ARP pakketten op het netwerk te verzenden, die het legitieme verkeer kunnen beïnvloeden.

- De stijgingen kunnen worden gezien afhankelijk van het aantal hosts op het netwerk en de rol van de switch op het milieu, het ARP is ontworpen om items te herproberen, op te lossen en te verfrissen en daarom wordt verwacht dat het ARP-verkeer te allen tijde zal zien. Als er slechts sporadische druppels zichtbaar zijn, kunnen ze van voorbijgaande aard zijn, afhankelijk van de netwerkbelasting, en er wordt geen impact waargenomen. Maar het is belangrijk om het netwerk te controleren en te weten om een verwachte en verwachte abnormale situatie goed te identificeren en te differentiëren.

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

Deze klasse verwijst naar verkeer verbonden met IPv6 buurontdekking/advertentie en routersolicatie en advertentiepakketten die ICMP-berichten gebruiken om lokale Link-laagadressen van buren te bepalen, en het wordt gebruikt voor bereikbaarheid en spoor van buurapparaten.

```
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
```

Impact

Schendingen op deze klasse kunnen IPv6 communicatie tussen buurapparaten verhinderen, aangezien deze pakketten worden gebruikt om de dynamische ontdekking of de verbinding-laag/lokale informatie tussen hosts en routers op de lokale link te vergemakkelijken. Een onderbreking van deze mededeling kan ook kwesties met bereikbaarheid buiten of door de verbonden lokale verbinding veroorzaken. Als er communicatieproblemen zijn tussen de IPv6-buren, zorg er dan voor dat er geen druppels op deze class zitten.

Aanbevelingen

-Bekijk alle abnormale ICMP-gedragingen van buurapparaten, in het bijzonder die welke betrekking hebben op de ontdekking van de buur en/of ontdekking van de router

- Zorg ervoor dat alle verwachte timer en intervalwaarden voor de periodieke berichten consistent zijn over het milieu en worden nageleefd, bijvoorbeeld voor berichten van routeradvertenties (RA-berichten).

Class Normal DHCP - Comp-systeem-p-klasse normaal-dhcp

Deze klasse verwijst naar verkeer dat gekoppeld is aan de Bootstrap Protocol (BOOTP client/server), dat bekend staat als Dynamic Host Control Protocol (DHCP)-pakketten op hetzelfde lokale Ethernet-segment voor zowel IPv4 als IPv6. Dit heeft specifiek betrekking op de verkeerscommunicatie die afkomstig is van een willekeurige IP-client of bestemd is voor een

BOOTP-server, door de volledige ontdekking, aanbieding, aanvraag en herkenning (DORA) van pakketverkeer. v6 client/server transactie via UDP-poorten 546/547.

```
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
```

Impact

Overtredingen op deze klasse kunnen leiden tot eindhosts die niet in staat zijn een IP van de DHCP-server te verwerven, en kunnen dus terugvallen op hun automatische privé IP-adresbereik (APIPA), 169.254.0.0/16. Zulke schendingen kunnen voorkomen in omgevingen waar apparaten tegelijkertijd proberen te beginnen en dus verder gaan dan de CIR die met de klasse is geassocieerd.

Aanbevelingen

- Controleer met opnamen, op hosts en DHCP-server aan de gehele DORA-transactie. Als de switch deel uitmaakt van deze communicatie, is het ook belangrijk om de verwerkte pakketten of die op de CPU zijn gestraft te controleren en om de statistische gegevens over de switch te controleren: ' toon ip dhcp global statistics ' en aanwijzingen : 'toon systeem interne toegangslijst sup-redirect-stats module 1 | grep -i dhcp".

Class Normal DHCP Relay Response - copp-systeem-p-class-normaal-dhcp-relais-respons

Deze klasse verwijst naar verkeer dat gekoppeld is aan de DHCP-relais voor zowel IPv4 als IPv6, gericht op de geconfigureerde DHCP-servers die onder het relais zijn ingesteld. Dit heeft uitsluitend betrekking op de verkeerscommunicatie die afkomstig is van een BOTP-server of die bestemd is voor een BOTP-client via de volledige DORA-pakketuitwisseling, en omvat ook DHCPv6-client/server-transactie via UDP-poorten 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
```

Impact

Schendingen voor deze klasse hebben dezelfde impact als de schendingen voor de klasse-copp-system-p-klasse-normaal-dhcp, omdat ze beide delen van dezelfde transactie zijn. Deze klasse richt zich voornamelijk op responscommunicatie van de relaismakelaars servers. De Nexus fungeert niet als de DHCP-server, maar is uitsluitend ontworpen om als relais-agent te fungeren.

Aanbevelingen

Dezelfde aanbevelingen als klasse normale DHCP zijn hier van toepassing. Aangezien de functie van Nexus enkel als relais agent moet fungeren, verwacht u op de SUP de gehele transactie tussen de host en de switch die als relais optreedt, en de switch en de servers te zien vormen.

Zorg ervoor dat er geen schurkenapparaten zijn, zoals onverwachte DHCP-servers die op het netwerk actief zijn, die op de scope kunnen reageren of dat apparaten die in een lus overlopen op het netwerk met DHCP-ontdekkingspakketten aanwezig zijn. De opdrachten kunnen extra controles uitvoeren: " **show ip dhcp relais** " en " **show ip dhcp relaisstatistieken** " .

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

Deze klasse verwijst naar software switch NAT flow traffic. Wanneer u een nieuwe dynamische vertaling maakt, wordt de stroom met software doorgestuurd totdat de vertaling geprogrammeerd is in hardware. Vervolgens wordt de vertaling door CoPP gecontroleerd om het verkeer te beperken dat aan de toezichthouder wordt gestraft terwijl de invoer in hardware is geïnstalleerd.

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

Impact

Een druppel op deze class treedt doorgaans op als er een hoog tempo nieuwe dynamische vertalingen en stromen in de hardware worden geïnstalleerd. De impact heeft op software geschakelde pakketten die weggegooid worden en niet aan de eindhost worden geleverd, wat tot verlies en terugzending kan leiden. Zodra de invoer in hardware is geïnstalleerd, wordt geen verder verkeer gestraft naar de toezichthouder.

Aanbevelingen

-Controleer de richtlijnen en beperkingen van dynamische NAT op het betreffende platform. Er zijn bekende beperkingen die gedocumenteerd zijn op platforms zoals de 3548, waarin de vertaling een paar seconden kan duren. Raadpleeg: 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

Uitzondering van klasse - copp-system-p-klasse

Deze klasse verwijst naar uitzonderingspakketten verbonden aan IP optie en IP ICMP onbereikbare pakketten. Als een doeladres niet op de verzendende informatiebasis (FIB) aanwezig is en het resultaat in een mis is, stuurt SUP een onbereikbaar ICMP-pakket terug naar de afzender. Packets met IP-opties die ook binnen deze klasse vallen. Raadpleeg het IANA-document voor meer informatie over IP-opties: 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
```

Impact

Deze klasse is zwaar gecontroleerd, en de dalingen op deze klasse zijn niet indicatief van een mislukking maar eerder van een beschermingsmechanisme om het bereik van ICMP onbereikbaar en IP opties pakketten te beperken.

Aanbevelingen

-Controleer of er verkeersstromen zichtbaar of gepunteerd zijn op de CPU's voor bestemmingen die niet op het FIB liggen.

Klasse Redirect - copp-system-p-class-redirect

Deze klasse verwijst naar verkeer dat gekoppeld is aan Precision Time Protocol (PTP), dat gebruikt wordt voor tijdsynchronisatie. Dit omvat multicast verkeer voor het gereserveerde bereik 224.0.1.129/32, eenastverkeer op UDP-poort 319/320 en Ethernet 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
```

Impact

Als u deze klasse laat vallen, kan dit leiden tot problemen bij apparaten die niet goed zijn gesynchroon of die niet de juiste hiërarchie hebben ingesteld.

Aanbevelingen

- Zorg voor stabiliteit van klokken en zorg ervoor dat deze correct zijn geconfigureerd. Zorg ervoor dat het PTP-apparaat is geconfigureerd voor multicast of unicast PTP-modus, maar niet beide tegelijk. Dit wordt ook gedocumenteerd onder de richtsnoeren en de beperking, en kan het verkeer verder doen dan het vastgelegde invoertarief.

- Bekijk het ontwerp en de configuratie van de grenskloktijd en alle PTP-apparaten in de omgeving. Zorg ervoor dat alle richtlijnen en beperkingen per platform worden gevolgd, omdat ze verschillen.

Klasse OpenFlow-copp-systeem-p-klasse

Deze klasse verwijst naar verkeer dat gekoppeld is aan OpenFlow-agent-operaties en de corresponderende TCP-verbinding tussen de controller en de agent.

```
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
```

Impact

Als u op deze klasse valt, kan dit leiden tot problemen met agents die de instructies van de

controller niet goed ontvangen en verwerken om het verzendingsvlak van het netwerk te beheren

Aanbevelingen

- Zorg ervoor dat er geen dubbel verkeer op het netwerk is gezien of dat er een apparaat is dat de communicatie tussen de controller en de agents belemmert.

- Controleer dat het L2-netwerk geen instabiliteit heeft (STP, loops).

CoPP-reducties voor probleemoplossing

De eerste stappen om CoP-schendingen van de probleemoplossing te melden zijn om te bepalen:

Gevolgen en reikwijdte van de kwestie

- begrijpen de verkeersstroom door het milieu en de rol van de switch in de getroffen communicatie

- Bepaal of er sprake is van schending van de betreffende klasse en onderbreek indien nodig.

Het vermelde gedrag is bijvoorbeeld gedetecteerd:

- De apparaten kunnen niet op andere apparaten buiten hun netwerk communiceren maar kunnen lokaal communiceren.

-Impact is geïsoleerd om communicatie buiten het VLAN te verplaatsen, en de switch fungeert als de standaardgateway.

- Een controle van de gastheren, wijst erop dat zij de gateway niet kunnen pingelen, na een controle van hun ARP tabel, blijft de ingang voor de gateway als Onvolledig.

- Alle andere hosts die de oplossing van de gateway hebben, hebben geen communicatieproblemen. Een controle van CoPP op de switch die als de gateway dienst doet wijst op schendingen op copp-systeem-p-klasse-normaal.

```
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;
```

- Bovendien, meerdere commando controles, laten zien dat de druppels actief toenemen.

-Deze schendingen kunnen ervoor zorgen dat het legitieme ARP-verkeer wordt verbroken, wat leidt tot een ontkenning van het servicetechnicus.

Opmerking: Het is belangrijk om te benadrukken dat CoPP de impact op het verkeer dat met de specifieke klasse verbonden is, isoleert, wat in dit voorbeeld ARP en copp-class-normaalwaarde zijn. Verkeersverkeer dat gerelateerd is aan andere klassen, zoals OSPF, BGP wordt niet door CoPP laten vallen, omdat ze volledig binnen een andere klasse vallen. Als er niets aan wordt

gedaan, kunnen ARP kwesties in andere problemen veroorzaken, die protocollen kunnen beïnvloeden die ervan afhankelijk zijn om mee te beginnen. Bijvoorbeeld, als een ARP cache tijden uit zijn en niet wordt ververst door excessieve schendingen kan een TCP sessie zoals BGP beëindigen.

Aanbevolen wordt om controles op besturingsplane uit te voeren, zoals Ethanalyzer, CPU-mac in-band stats en CPU-proces om de zaak verder te isoleren.

Ethanalizer

Aangezien verkeer dat door CoPP wordt gecontroleerd uitsluitend met CPU-gebonden verkeer is verbonden, is een van de belangrijkste instrumenten de ethanalyzer. Dit gereedschap is een Nexus-implementatie van Thark en maakt het mogelijk dat verkeer dat door de toezichthouder wordt verstuurd en ontvangen, wordt opgenomen en gedecodeerd. Het kan ook filters gebruiken die zijn gebaseerd op verschillende criteria, zoals protocollen of veldnameninformatie, en zo een onschatbaar gereedschap worden om verkeer te bepalen dat door de CPU wordt verzonden en ontvangen.

De aanbeveling is om eerst het ARP verkeer te onderzoeken dat door de toezichthouder wordt gezien wanneer het ethanalyzer-gereedschap direct op de eindsessie wordt uitgevoerd of naar een bestand wordt gestuurd voor analyse. Filters en limieten kunnen worden gedefinieerd om de opname in een specifiek patroon of gedrag te concentreren. Om dit te doen, voegt u flexibele weergavefilters toe.

Een veel voorkomend misverstand is dat de ethanalyzer al het verkeer dat door de switch reist, fotografeert. Het gegevensverkeer tussen hosts wordt door de hardware-ASIC's tussen gegevenspoorten geschakeld of verstuurd zonder betrokkenheid van de CPU's en wordt derhalve normaal gezien door de etanzer-opname. Om het gegevensverkeer in te voeren, is het raadzaam andere hulpmiddelen zoals ELAM of SPAN te gebruiken. Om ARP bijvoorbeeld te filteren, gebruikt u de opdracht:

ethanalyzer lokale interface-unit voor weergave-filter limiet-opgenomen pijp-frames 0 autostop duur 60 > arpcpu

Belangrijke configureerbare velden:

- "interface inband" - verwijst naar verkeer dat gericht is op SUP

-'display-filter' - verwijst naar het gebruikte haaienfilter, waarbij de meeste Wireshark-filters worden geaccepteerd

- 'limiet-opgenomen frames 0' - verwijst naar de limiet, 0 is gelijk aan onbeperkt, totdat deze wordt gestopt door een andere parameter of handmatig wordt gestopt door Ctrl+C

-"autostop-duur 60" - verwijst naar het ethanalyzer-einde na 60 seconden, waardoor een momentopname van 60 seconden ARP-verkeer op de CPU wordt gecreëerd

De ethanalyzer-uitvoer wordt opnieuw naar een bestand op de flitser met '> arpcpu' gericht, dat handmatig moet worden verwerkt. Na 60 seconden wordt de opname voltooid en wordt de ethanalyzer dynamisch beëindigd. Het bestandsindeling wordt uitgevoerd in de flitser van de switch, die vervolgens kan worden verwerkt om de bovenste talk te extraheren. Voorbeeld:

```
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
```

Dit filter wordt gesorteerd op: De bron- en doelkolommen, dan de unieke gevonden overeenkomsten (maar negeert de datumkolom), telt de instanties en voegt het nummer toe, en sorteert tenslotte top-to-bottom, op basis van telling, en toont de eerste 50 resultaten.

In dit voorbeeld werden in 60 seconden meer dan 600 ARP-pakketten ontvangen van drie apparaten, die geïdentificeerd zijn als de apparatuur waarvan vermoed wordt dat ze de dader zijn. In de eerste kolom op het filter wordt het aantal gevallen voor deze gebeurtenis in de opgegeven tijdsduur weergegeven in het opnamebestand.

Het is belangrijk te begrijpen dat het ethanalisatiegereedschap werkt op de in-band-bestuurder, wat in wezen de communicatie naar de ASIC is. In theorie, moet het pakket door de knel en de pakketmanager gaan om aan het bijbehorende proces zelf te worden afgegeven. CoPP en HWRL werken voordat het verkeer wordt gezien op de analyseapparatuur. Zelfs als de schendingen actief blijven toenemen, gaat nog wat verkeer door en wordt binnen de politie conformerend gewerkt, wat helpt inzicht te verschaffen in de verkeersstromen die naar de CPU worden gestraft. Dit is een belangrijk onderscheid, aangezien het verkeer dat op de ethanalyzer wordt gezien NIET het verkeer is dat de CIR heeft geschonden en is geschrapt.

De ethanalyzer kan ook op een open manier worden gebruikt, zonder een weergavefilter of opnamefilter die wordt gespecificeerd om al het relevante SUP-verkeer te vangen. Dit kan als een isolatiemaatregel worden gebruikt als deel van de probleemoplossing.

Raadpleeg voor meer informatie over en gebruik van de ethanalyzer de Technische opmerking:

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

Opmerking: Nexus 7000, voorafgaand aan de 8.X code release, kan alleen ethanalyzer opnamen via de admin VDC, die SUP-gebonden verkeer van alle VDC's omvat. VDC-specifieke ethanalyzer is aanwezig in 8.X-codes.

CPU-MAC-inband-statussen

De in-band status die bij CPU-gebonden verkeer is gekoppeld, houdt relevante statistieken van in-band TX/RX CPU-verkeer bij. Deze statistieken kunnen met de opdracht worden gecontroleerd: **'toon hardware interne cpu-mac inband stats'**., die inzicht geven in de actuele statistieken over de tarieven en de piektarieven.

```
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 beste praktijk wordt geadviseerd een basislijn te creëren en te traceren, omdat afhankelijk van de rol van de switch en de infrastructurele output van de "show hardware interne cpu-mac inband stats" aanzienlijk verschilt. In dit lab zijn de normale waarden en historische pieken gewoonlijk niet hoger dan een paar honderd pps, en dus is dit abnormaal. De opdracht '**show hardware interne cpu-mac inband events**' is ook nuttig als historische referentie, omdat het gegevens bevat over het piekgebruik en de tijd dat het werd gedetecteerd.

ProcesCPU

De Nexus-switches zijn op Linux gebaseerde systemen, en het Nexus Operating System (NXOS) maakt gebruik van CPU's, preventieve planner, multitasking en multithreading van de cores-architectuur, om eerlijke toegang tot alle processen te bieden, en dus zijn spikes niet altijd kenmerkend voor een probleem. Als er echter sprake is van aanhoudende verkeersovertredingen, is het waarschijnlijk dat het bijbehorende proces ook veel wordt gebruikt en als een topbron onder de CPU-uitgangen wordt weergegeven. Maak meerdere momentopnamen van de CPU-processen om het hoge gebruik van een bepaald proces te verifiëren door gebruik te maken van: **tonen processen cpu - soort | 0,0** of **show processen cpu-type uitsluiten | groen <proces>**.

De processen CPU's, in-band stats en verificaties in ethiek bieden inzicht in de processen en het verkeer dat momenteel door de toezichthouder wordt verwerkt en helpen de aanhoudende instabiliteit van het controlevliegtuigverkeer te isoleren, dat kan worden omgezet in problemen met het gegevensverkeer. Het is belangrijk te begrijpen dat CoPP een beschermingsmechanisme is. Het is reactionair omdat het alleen maar werkt op het verkeer dat naar de SUP wordt gestraft. Het is ontworpen om de integriteit van de toezichthouder te waarborgen door de teruggooi van verkeerstarieven, die de verwachte marges overschrijden, te beperken. Niet alle druppels wijzen op een probleem of vereisen interventie, aangezien het belang ervan betrekking heeft op de specifieke CoPP-klasse en de geverifieerde impact, gebaseerd op de infrastructuur en het netwerkontwerp. Droogvallen als gevolg van sporadische uitbarstingen vertaalt zich niet in een inslag, omdat protocollen ingebouwde mechanismen hebben, zoals het in stand houden en het opnieuw proberen van voorbijgaande gebeurtenissen. Bewaar de focus op aanhoudende gebeurtenissen of abnormale gebeurtenissen buiten de gevestigde basislijnen. Denk eraan dat CoPP zich moet houden aan de protocollen en functies die specifiek zijn voor het milieu en dat de producten moeten worden gemonitord en continu op elkaar afgestemd om ze te verfijnen, afhankelijk van de schaalbaarheidsbehoeften tijdens de ontwikkeling. Stel, als er druppels optreden, vast of CoPP onbedoeld verkeer liet vallen of in reactie op een defect of aanval. In beide gevallen moet de situatie worden geanalyseerd en moet worden nagegaan of er moet worden ingegrepen door middel van een analyse van de impact en corrigerende maatregelen op het milieu, die buiten het toepassingsgebied van de switch zelf kunnen vallen.

Aanvullende informatie

Recente platforms/codes kunnen de mogelijkheid hebben om een SPAN-to-CPU uit te voeren door de spiegel van een poort en het punt van het gegevensverkeer naar de CPU. Normaal gesproken is dit een zeer tariefbeperking voor de hardware en CoPP. Voorzichtig gebruik van de SPAN naar CPU is aanbevolen, en is buiten het bereik van dit document. Raadpleeg de technische opmerking die bij deze optie is vermeld voor meer informatie:

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