Catalyst 6500/6000 QoS FAQ-module

Inhoud

Inleiding

Dit document behandelt vaak gestelde vragen (FAQ's) over de Quality of Service (QoS) optie van Catalyst 6500/6000 met supervisor 1 (Sup1), supervisor 1A (Sup1A), supervisor 2 (Sup2) en supervisor 720 (Sup720) die Catalyst OS (CatOS) uitvoeren. In dit document worden deze switches Catalyst 6500 (Cat6K) Switches genoemd die CatOS uitvoeren. Raadpleeg PFC QoS configureren voor QoS-functies op Catalyst 6500/6000 Switches die Cisco IOS®-software uitvoeren.

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Q. Is QoS standaard ingeschakeld voor Catalyst 6500 Switches?

A. QoS is standaard niet ingeschakeld. Geef de **ingestelde QoS uit om** opdracht te geven om QoS in te schakelen.

Q. Wat is de standaard gedifferentieerde service code point (DSCP) waarde die aan pakketten wordt toegewezen?

A. Al het verkeer dat een onvertrouwde poort ingaat wordt gemarkeerd met een DSCP van 0. In het bijzonder wordt DSCP door de poort op 0 gezet.

Q. Kan ik op VLAN gebaseerde QoS opzetten op een 6500?

A. De standaardinstelling is gebaseerd op poorten. U kunt dat wijzigen als u de **ingestelde poort qos** *mod*/*port* **op VLAN gebaseerde** opdracht geeft.

Q. Wat zijn de havenmogelijkheden voor elke lijnkaart en hoe kan ik de rijmogelijkheden interpreteren?

A. Raadpleeg de tabel met poortfuncties in de modus voor Wachtrij van een poortgedeelte van QoS-uitvoerplanning op Catalyst 6500/6000 Series Switches die CatOS-systeemsoftware uitvoeren.

Q. Wat zijn de standaard QoS-configuraties op een 6500 wanneer QoS aanvankelijk is ingeschakeld?

A. Raadpleeg de standaardconfiguratie voor QoS in het gedeelte Catalyst 6000 van QoS-uitvoerplanning op Catalyst 6500/6000 Series Switches die CatOS-systeemsoftware uitvoeren.

V. Waar worden de QoS-processen in Catalyst 6000 uitgevoerd?

A. Invoerplanning—Door PINNACLE/COIL poort op applicatie-specifieke geïntegreerde schakelingen (ASIC's). Layer 2 alleen, met of zonder beleidsfunctiekaart (PFC).

Classificatie—Door supervisor of door PFC via de ACL-motor (toegangscontrolelijst). Alleen Layer 2, zonder PFC; Layer 2 of Layer 3 met een PFC.

Toezicht-door PFC via Layer 3 verzendmotor. Layer 2 of Layer 3 met een PFC (vereist).

Packet herschrijven-door PINNACLE/COIL poort ASICs. Layer 2 of Layer 3 gebaseerd op eerder uitgevoerde classificatie.

Uitloop planning-door PINNACLE/COIL poort ASICs. Layer 2 of Layer 3 gebaseerd op eerder uitgevoerde classificatie.

Q. Kan ik QoS-functies implementeren zonder een beleidsfunctiekaart (PFC)?

A. In Catalyst 6000 Series Switches ligt het hart van de QoS-functionaliteit op de PFC en is een vereiste voor Layer 3 of Layer 4 QoS-verwerking. Een supervisor zonder een PFC kan echter worden gebruikt voor Layer 2 QoS-classificatie en -markering.

Q. Wat is het verschil in QoS-functionaliteit tussen de Policy functiekaart 1 (PFC1) en PFC2?

A. PFC2 stelt u in staat het QoS-beleid omlaag te brengen naar een Distributed Forwarding Card (DFC). PFC2 voegt ook steun toe voor een te hoge rente, wat een tweede niveau van toezicht aangeeft waarop beleidsmaatregelen kunnen worden genomen. Raadpleeg de hardwareondersteuning voor QoS in het gedeelte Catalyst 6000 Series van Understanding Quality of Service op Catalyst 6000 Series Switches voor meer informatie.

Q. Wat is de standaardklasse van de dienst (CoS) om configuratie van het rijontwerp te verzenden wanneer auto-qos wordt toegelaten?

A. set qos map 2q2t tx wachtrij 2 cos 5,6,7

set qos map 2q2t tx wachtrij 2 1 cos 1,2,3,4

set qs kaart 2q2t vaste wachtrij 1 nos 0

Q. Wat is de standaard gedifferentieerde services code point (DSCP) naar CoS-classificatie (serviceklasse)?

A. 8 tot 1 (verdeel DSCP met 8 om CoS te krijgen).

Q. In de wachtrij voor stress, als de rij voor prioriteit verzadigd is, wordt het verkeer uiteindelijk bediend in de wachtrijen (WRR)?

A. Nee, de WRR wachtrijen worden niet geserveerd tot de prioriteitswachtrij volledig leeg is.

Q. bepaalt gewogen round-robin (WRR) de bandbreedte toewijzing gebaseerd op aantal pakketten of op een bepaald aantal bytes?

A. Gebaseerd op een bepaald aantal bytes, die meer dan één pakket kunnen vertegenwoordigen. Het laatste pakket dat de toegewezen bytes overschrijdt, wordt niet verzonden. Bij een extreme gewichtsconfiguratie, zoals 1% voor rij 1 en 99% voor rij 2, wordt het exacte gewicht mogelijk niet bereikt. De switch gebruikt een WRR algoritme om frames uit één rij tegelijk over te brengen.

WRR gebruikt een gewichtswaarde om te beslissen hoeveel van één rij te verzenden voordat het naar de andere rij switch. Hoe hoger het gewicht dat aan een rij wordt toegewezen, hoe meer bandbreedte wordt toegewezen.

Opmerking: Het werkelijk overgedragen aantal bytes komt niet overeen met de berekening, omdat de hele frames worden doorgegeven voordat deze naar de andere wachtrij wordt switch.

Q. Mijn nieuwe 65xx lijnkaartdocumentatie zegt dat ze ondersteuning biedt voor een begrotinggewogen round robin (DWRR). Wat is DWRR en wat betekent dat?

A. DWRR geeft wachtrijen door zonder de wachtrij met een lage prioriteit te verlaten, omdat de wachtrij tijdens de volgende ronde wordt onderverdeeld en gecompenseerd. Als een wachtrij een pakket niet kan verzenden, omdat de pakketgrootte groter is dan de beschikbare bytes, worden de ongebruikte bytes aan de volgende ronde gecrediteerd.

Q. Wat zijn de standaardgewichten op een 2q2t poort en hoe stel ik ze aan?

A. Geef de opdracht **set qos wrr 2q2t** *q1_weight q2_weight* uit om de standaardgewichten voor Wachtrij 1 (de rij met lage prioriteit diende 5/260ste van de tijd) en rij 2 (de rij met hoge prioriteit diende 255/260ste van de tijd) aan te passen.

Q. Ik zou Simple Network Management Protocol (SNMP) willen gebruiken om het aantal pakketten te verzamelen door de afzonderlijke politieagent. Is dit mogelijk? Zo ja, welke MIB wordt gebruikt?

A. Ja, SNMP ondersteunt CISCO-QOS-PIB-MIB en CISCO-CAR-MIB.

Q. is er een show opdracht die het aantal geworpen pakketten door politieagent weergeeft?

A. De **show qos statistieken verzamelen-politier** en **tonen qos statistiek l3stats** opdrachten tonen het aantal geworpen pakketten door politieagent.

Q. Ik zou Simple Network Management Protocol (SNMP) willen gebruiken om een politieman aan te passen zodat de parameters voor snelheid en doorslag dynamisch kunnen worden gewijzigd. Bijvoorbeeld op het tijdstip van de dag. Is dit mogelijk? Zo ja, welke MIB wordt gebruikt?

A. Ja, SNMP ondersteunt CISCO-QOS-PIB-MIB en CISCO-CAR-MIB.

Q. Is het mogelijk om tijd-van-dag-gebaseerde QoS te implementeren - specifiek, om het maximum aan te passen en tarieven te barsten - door Cisco IOS software op de Multilayer Switch functiekaart (MSFC) in hybride modus? Indien mogelijk, wordt deze QoS uitgevoerd in hardware en niet door de MSFC processor?

A. Nee, dat kan niet. In de hybride modus (CatOS) wordt alle QoS-toezicht uitgevoerd door de toezichthouder.

Q. Ik zag geen beschrijving van hoe het rentetarief van de politie en de barstwaarden van de politie worden geïmplementeerd. Ik wil daar technische documentatie over afronden, zodat ik kan begrijpen welke invloed ze op mijn netwerk hebben.

A. De barstwaarden van de politieagent en de politieagent worden op deze wijze ten uitvoer gelegd:

```
burst = sustained rate bps × 0.00025 (the leaky bucket rate) + MTU kbps
```

Bijvoorbeeld, als u een 20 Mbps politieagent en een maximum transmissie eenheid (MTU) (op Ethernet) van 1500 bytes wilt, dan is dit hoe de burst wordt berekend:

```
burst = (20,000,000 bps × 0.00025) + (1500 × 0.008 kbps)
      = 5000 bps + 12 kbps
      = 17 kbps
```

Maar door de granulariteit van de hardware van de politieagent met Sup1 en Sup2 moet u dit tot 32 kbps, wat het minimum is, afronden.

Raadpleeg deze documenten voor meer informatie over de implementatie van de politiekoersen en barstwaarden:

- QoS O-planning bij Catalyst 6500/6000 Series Switches die CatOS-systeemsoftware uitvoeren
- QoS configureren

Ik wil mijn Sup1A Supervisors vervangen door Sup2s. Verandert de techniek van QoS, zoals de barstsnelheid, tussen Sup1A en Sup2?

A. Ja, er is verschil tussen twee supervisors wanneer een Catalyst 6500 Switch SUP2/PFC2 heeft. Als het Cisco Express Forwarding (CEF) in werking stelt is het gedrag iets anders wanneer u de netflow in SUP2 configureren.

Q. Welke opdrachten kan ik gebruiken om mijn QoS-instellingen te controleren?

A. Raadpleeg het gedeelte Monitoring and Verification a Configuration of QoS Classifier en Marking op Catalyst 6500/6000 Series Switches die CatOS-software uitvoeren.

Q. Wanneer ik de code van het besturingssysteem van Catalyst (CatOS) op een 6500 en Cisco IOS software in de functiekaart van de Multilayer Switch (MSFC) in werking stel, geef ik de opdrachten QoS op de MSFC of op de supervisor uit?

A. Wanneer u hybride code (CatOS) gebruikt, geeft u de QoS-opdrachten uit op de Supervisor/Policy functiekaart (PFC). De 6500 voert QoS uit op drie plaatsen:

- Op software gebaseerd in de MSFC
- Op hardware gebaseerde (meerlaagse switching-gebaseerd) in de PFC
- Op software gebaseerd op sommige lijnkaarten

Dit probleem doet zich voor wanneer u met hybride IOS werkt (CatOS + IOS voor MSFC). CatOS

en IOS hebben twee reeksen van configuratieopdrachten. Wanneer u QoS echter configureren onder native IOS-naam, bijvoorbeeld met de nieuwere Sup32- of Sup720-motoren, bent u verder verwijderd van de hardware en is het lijnkaartgedeelte onzichtbaar voor de gebruiker. Dit is belangrijk omdat het meeste verkeer meerdere lagen geschakeld is (hardware geschakeld). Daarom wordt het behandeld door de PFC-logica. De MSFC ziet dat verkeer nooit. Als u geen op PFC gebaseerde QoS instelt, wordt het grootste deel van het verkeer verloren.

Q. Wat gebeurt er als de set port qos trust opdracht niet wordt ondersteund door mijn lijnkaart?

A. U kunt een QoS-toegangscontrolelijst (ACL) maken om de DSCP-waarde (gedifferentieerde servicescode) van het inkomende pakket te vertrouwen. Geef bijvoorbeeld de **set qos acl ip test trust-dscp om het even welke** opdracht uit.

Wat is het verschil tussen politie-eenheden met aggregaten en microflow?

A. Raadpleeg de classificatie en controle met de PFC-sectie van Understanding Quality of Service op Catalyst 6000 familieSwitches.

Q. Welke opdrachten staan me toe statistieken te bekijken voor politie-eenheden met aggregaten of microflow?

A. Met Supervisor Engine 1 en 1A is het niet mogelijk om politiestatistieken te hebben voor individuele geaggregeerde politieagenten. Geef de **show qos statistics l3stats** opdracht uit om de politiestatistieken per systeem te bekijken.

Met Supervisor Engine 2 kun je geaggregeerde politiestatistieken bekijken op een per-politiestatus basis met de opdracht **tonen qos statistieken geaggregeerd-politieagent**. Geef de **show mls entry qos short** opdracht uit om de microflow politiestatistieken te controleren.

Q. wordt traffic shaping ondersteund op Catalyst 6500 (Cat6K)-Switch?

A. Traffic Shaping wordt alleen ondersteund op bepaalde WAN-modules voor Catalyst 6500/7600 Series, zoals de optische servicesmodules (OSM's) en FlexWAN-modules. Raadpleeg Class-Based Traffic Shaping en Traffic Shaping voor meer informatie.

Q. Hoeveel bewakers van aggregaten of microflow worden ondersteund op de Catalyst 6500 (Cat6K)-Switch?

A. Catalyst 6500/6000 ondersteunt tot 63 microflow-politiers en tot 1023 geaggregeerde politiers.

Q. Welk Catalyst besturingssysteem (CatOS) of functiekaart voor meerlaagse Switch (MSFC) is Cisco IOS-afbeelding vereist om toezicht te ondersteunen?

A. The Supervisor Engine 1A ondersteunt inbraaktoezicht in CatOS versie 5.3(1) en hoger, en Cisco IOS-softwarerelease 12.0(7)XE en later.

Supervisor Engine 2 ondersteunt inbraaktoezicht in CatOS versie 6.1(1) en hoger, en Cisco IOS-softwarerelease 12.1(5c)EX en hoger. Microflow-toezicht wordt echter alleen ondersteund in Cisco

IOS-software.

Q. Ik heb een upgrade uitgevoerd van een Sup2 naar een Sup720 en mijn statistieken over verkeerssnelheden vertonen een andere lijn met hetzelfde verkeer. Waarom?

A. Een belangrijke verandering in het toezicht op Supervisor Engine 720 is dat het verkeer met Layer 2 lengte van het frame kan tellen. Dit verschilt van Supervisor Engine 1 en Supervisor Engine 2, die IP en IPX frames telt door hun Layer 3 lengte. Bij sommige toepassingen zijn Layer 2 en Layer 3 lengte mogelijk niet consistent. Een voorbeeld is een klein Layer 3-pakket binnen een groot Layer 2-kader. In dit geval, zou Supervisor Engine 720 een enigszins verschillend verkeerstarief kunnen tonen vergeleken met Supervisor Engine 1 en Supervisor Engine 2.

Vraag. Hoe weet ik welke waarden ik moet gebruiken voor de snelheid en de barst als ik een politieagent stel?

A. Deze parameters regelen de werking van de penning:

- **Rate**-definieert hoeveel tokens elk interval worden verwijderd. Dit stelt in feite de politiekoers in. Alle verkeer onder de snelheid wordt in profiel beschouwd.
- **Interval**-definieert hoe vaak penningen uit de emmer worden verwijderd. De interval is vastgesteld op 0,00025 seconden, dus worden penningen uit een emmer van 4,000 keer per seconde verwijderd. Het interval kan niet worden gewijzigd.
- **Burst**—definieert het maximale aantal penningen dat de emmer op ieder moment kan bevatten. Om de opgegeven verkeerssnelheid te kunnen handhaven, moet de barst niet minder zijn dan de snelheidstijden van het interval. Een andere overweging is dat het pakje met een maximale grootte in de emmer moet passen.

Gebruik deze vergelijking om de burst parameter te bepalen:

```
Burst = (rate bps * 0.00025 sec/interval) or (maximum packet size bits) [whichever is greater]
```

Bijvoorbeeld, als u de minimum burst waarde wilt berekenen nodig om een tarief van 1 Mbps op een netwerk Ethernet te handhaven, wordt het tarief gedefinieerd als 1 Mbps en de maximum Ethernet pakketgrootte is 1518 bytes. Dit is de vergelijking:

```
Burst = (1,000,000 bps * 0.00025) or (1518 bytes * 8 bits/byte) = 250 or 12144
```

Het grotere resultaat is 12144, wat je tot 13 kbps doet.

Opmerking: In Cisco IOS-software is de mate van toezicht gedefinieerd in bits per seconde (bps). In Catalyst besturingssysteem (CatOS) wordt het gedefinieerd in kbps. Ook, in Cisco IOS software, wordt de burst rate gedefinieerd in bytes, maar in CatOS, wordt het gedefinieerd in kilobits.

Opmerking: Vanwege de granulariteit van het hardware-toezicht worden de exacte snelheid en uitbarsting tot de dichtstbijzijnde ondersteunde waarde afgerond. Verzeker dat de burst waarde niet minder is dan het maximum groote pakje. Anders worden alle pakketten die groter zijn dan de barstgrootte, verbroken.

Als u bijvoorbeeld probeert de burst in Cisco IOS-software op 1518 in te stellen, wordt deze

afgerond op 1000. Hierdoor worden alle frames die groter zijn dan 1000 bytes gevallen. De oplossing is de burst in 2000 te configureren.

Wanneer u de burst rate configureren houdt u er rekening mee dat sommige protocollen, zoals TCP, een flow-control mechanisme implementeren dat op pakketverlies reageert. TCP bijvoorbeeld verlaagt het venster met de helft voor elk verloren pakket. Als de controle in een bepaald tempo wordt uitgevoerd, is de effectieve benutting van de link dus lager dan het geconfigureerde percentage. Je kan de barst verhogen om beter gebruik te maken. Een goede start voor dit soort verkeer is het verdubbelen van de barstgrootte. In dit voorbeeld, wordt de burst grootte verhoogd van 13 kbps tot 26 kbps. Daarna moet u de prestaties controleren en indien nodig verdere aanpassingen uitvoeren.

Om dezelfde reden wordt het niet aanbevolen om de politietoezicht te benchmarken met op verbindingen gericht verkeer. Dit laat over het algemeen een lagere prestatie zien dan de politieagent toestaat.

Q. Ik configureren QoS via een poortkanaal. Zijn er beperkingen die ik moet weten?

A. Wanneer u QoS vormt op poorten die deel uitmaken van een poortkanaal op Catalyst besturingssysteem (CatOS), moet u dezelfde configuratie toepassen op alle fysieke poorten in het poortkanaal. Deze parameters moeten overeenkomen voor alle havens in het havenkanaal:

- Poorttrust type
- Ontvang poorttype (2q2t of 1p2q2t)
- Type transmissiepoort (1q4t of 1p1q4t)
- Standaard poortklasse van de service (CoS)
- Op poorten gebaseerde QoS voor VLAN-gebaseerde QoS
- Toegangscontrolelijst (ACL) of protocolpaar dat door de poort wordt vervoerd

Q. Waarom kan ik de drempelwaarde niet aanpassen?

A. Met CatOS-versies (Catalyst.ar-zonder) eerder dan 6.2 wordt de maximale waarde van de WRED-drempelwaarde (gewogen willekeurige vroegtijdige detectie) ingesteld, terwijl de minimale drempelwaarde moeilijk gecodeerd is tot 0%. Dit wordt gecorrigeerd in CatOS 6.2 en later, wat de configuratie van de min-drempelwaarde mogelijk maakt.De standaard min-drempel is afhankelijk van de voorrang. De minimum-drempel voor IP voorrang 0 correspondeert met de helft van de max-drempel. De waarden voor de nog resterende prioriteitsgebieden dalen tussen de helft van de max-drempel en de max-drempel met gelijkmatige tussenpozen.

Q. Ik heb moeite om de buffers van de verzendwachtrij aan te passen. Zijn er beperkingen?

A. Als u drie wachtrijen hebt (1p2q2t), moeten de hoge prioriteit gewogen round-robin (WRR) wachtrij en de strikte prioriteitswachtrij op hetzelfde niveau worden ingesteld.

Ik heb een 62xx/63xx lijnkaart. Ik kan het ingestelde commando niet toepassen dat vertrouwen heeft in een gedifferentieerd services code point (DSCP) op een poort. Is er een beperking op deze lijnkaart voor QoS-functies?

A. Ja, omdat u de opdrachten WS-X6248-xx, WS-X6224-xx en WS-X6348-xx niet kunt uitvoeren

op de opdrachten trust-ipprec of trust-cosxx. De makkelijkste methode in deze situatie is om alle poorten onbetrouwbaar te laten en de standaard toegangscontrolelijst (ACL) te wijzigen in de opdracht trust-dscp:

```
set qos enable

set port qos 2/1-16 trust untrusted

set qos acl default-action ip trust-dscp
```

Raadpleeg de limieten van de WS-X6248-xx, WS-X624-xx en WS-X6348-xx lijnkaarten in het gedeelte QoS-classificatie en markering op Catalyst 6500/6000 Series Switches die CatOS uitvoeren Software voor extra lijnkaartspecifieke beperkingen.

Q. Welke Catalyst besturingssystemen (CatOS) versies en toezichthouders zijn vereist om toezicht te ondersteunen?

A. De Supervisor Engine 1A ondersteunt inbraaktoezicht in CatOS versie 5.3(1) en later, en in Cisco IOS-softwarerelease 12.0(7)XE en later.

Opmerking: Voor toezicht met Supervisor Engine 1A is een dochterkaart van de beleidsfunctiekaart (PFC) vereist.

Supervisor Engine 2 ondersteunt inbraaktoezicht in CatOS versie 6.1(1) en later, en in Cisco IOS-softwarerelease 12.1(5c)EX en hoger. De Supervisor Engine 2 ondersteunt de overtollige snelheidsparameter.

De supervisor 720 ondersteunt inbraaktoezicht op het poort- en VLAN-interfaceniveau. Raadpleeg de Update over functies voor Supervisor Engine 720 in het gedeelte van QoS-toezicht op Catalyst 6500/6000 Series Switches voor meer informatie over de functies die Sup720 biedt op politieel.

Wat moet ik weten over de configuratie van QoS via EtherChannel?

A. Wanneer u QoS op een poort vormt die deel uitmaakt van een EtherChannel op CatOS, moet u deze altijd op een per-poorts basis configureren. Bovendien moet u ervoor zorgen dat u dezelfde QoS-configuratie op alle poorten toepast, omdat EtherChannel alleen poorten met dezelfde QoS-configuraties kunt bundelen. Dit betekent dat u deze parameters hetzelfde moet configureren:

- Poorttrust type
- Ontvang poorttype (2q2t of 1p2q2t)
- Type transmissiepoort (1q4t of 1p1q4t)
- Standaard poortklasse van de service (CoS)
- Op poorten gebaseerde QoS voor VLAN-gebaseerde QoS
- Toegangscontrolelijst (ACL) of protocolpaar dat door de poort wordt vervoerd

Q. Waar kan ik voorbeelden vinden van het gebruik van QoS toegangscontrolelijsten (ACL's) om het verkeer te markeren of te controleren?

A. Zie zaak 1: Markeren op het gedeelte Edge van de QoS-classificatie en markering op Catalyst

6500/6000 Series Switches die CatOS-software uitvoeren, bijvoorbeeld bij het markeren van verkeer.

Raadpleeg het gedeelte Toezicht instellen en bewaken in het gedeelte CatOS-software van de QoS-controle op Catalyst 6500/6000 Series Switches voor een voorbeeld van hoe verkeer wordt gemonitord.

Q. Wat is het verschil tussen op poort gebaseerde en op VLAN gebaseerde QoS toegangscontrolelijsten (ACL's)?

A. Elke QoS ACL kan of op een poort of op een VLAN worden toegepast, maar er is een extra configuratieparameter om rekening te houden met: het ACL-poorttype. Een poort kan worden ingesteld om VLAN-gebaseerd of op poort gebaseerd te zijn. Dit zijn de twee soorten configuraties:

1. Als een op VLAN gebaseerde poort met een toegepaste ACL aan een VLAN wordt toegewezen dat ook toegepaste ACL heeft, dan krijgt VLAN-gebaseerde ACL prioriteit boven op haven-gebaseerde ACL.
2. Als een op poort gebaseerde poort met een toegepaste ACL wordt toegewezen aan een VLAN dat ook toegepaste ACL heeft, dan krijgt de op poort gebaseerde ACL voorrang boven VLAN-gebaseerde ACL.

Raadpleeg Welke van de vier mogelijke bronnen voor interne DSCP zal worden gebruikt? sectie van QoS-classificatie en markering op Catalyst 6500/6000 Series Switches die CatOS-software uitvoeren voor meer informatie.

Q. Wat is de typische waarde van de barstgrootte die moet worden gebruikt voor snelheidsbeperking op Layer 3-switches?

A. Layer 3 switches implementeren een benadering van het algoritme van één token in firmware. Een redelijke burst size voor het bereik van verkeerssnelheden is ongeveer 64000 bytes. De barstgrootte moet zodanig gekozen worden dat er zich minimaal één pakje met een maximale grootte bevindt. Met elk aankomend pakket, bepaalt het controle algoritme de tijd tussen dit pakket en het laatste pakket, en berekent het aantal penningen die tijdens de verlopen tijd gegenereerd zijn. Dan voegt het dit aantal penningen aan de emmer toe en bepaalt of het aankomende pakket met, of de gespecificeerde parameters in overeenstemming is.

Q. Waarom krijg ik een lagere prestatie voor TCP verkeer met snelheidsbeperking?

A. TCP toepassingen gedragen zich slecht wanneer pakketten als resultaat van snelheidsbeperking worden gedropt. Dit is het gevolg van het inherente raamschema dat bij de stroomregeling wordt gebruikt. U kunt de parameter burst size of de parameter rate aanpassen om de vereiste doorvoersnelheid te verkrijgen.

Q. Wat is het voordeel van gewogen willekeurige vroege detectie (WRED), en hoe weet ik of mijn lijnkaart WRED kan ondersteunen?

A. Voor congestievermijding bij uitvoerschema's ondersteunt de Catalyst 6500 (Cat6K)-Switch WRED op sommige tegenslagen. Elke rij heeft een configureerbare grootte en drempel. Sommigen hebben WRED. WRED is een congestievermijdingsmechanisme dat op willekeurige wijze pakketten met een bepaalde IP-voorrang laat vallen wanneer de buffers een bepaalde

drempelvulling bereiken. WRED is een combinatie van twee functies: staartdruppels en willekeurige vroegtijdige detectie (RED). De vroege implementatie van het besturingssysteem van Catalyst (CatOS) van WRED stelde alleen de max-drempel in, terwijl de min-drempel hard werd gecodeerd tot 0%. Merk op dat de vervolgkeuzemogelijkheid voor een pakje altijd niet ongeldig is, omdat ze altijd boven de min-drempel liggen. Dit gedrag wordt gecorrigeerd in CatOS 6.2 en later. WRED is een zeer nuttig mechanisme om congestie te vermijden voor wanneer het verkeerstype op TCP gebaseerd is. Voor andere types van verkeer, is ROOD niet zeer efficiënt omdat ROOD gebruik maakt van het raammechanisme dat door TCP wordt gebruikt om congestie te beheren.

Raadpleeg het gedeelte Inzicht op de wachtrij van een poortdeel van QoS-uitvoerplanning op Catalyst 6500/6000 Series Switches die CatOS-systeemsoftware uitvoeren om te bepalen of een lijnkaart of wachtrijstructuur WRED kan ondersteunen. U kunt ook de opdracht **Show port mogelijkheden** uitgeven om de rijstructuur van uw lijnkaart te zien.

Q. Wat is het "internal fied services code point" (DSCP)?

A. Elk frame heeft een interne serviceklasse (CoS) die is toegewezen, ofwel de ontvangen CoS of de standaardpoort CoS. Dit omvat niet-gelabelde frames die geen echte CoS dragen. Deze interne CoS en de ontvangen DSCP worden geschreven in een speciale pakketheader (een gegevensbus-header genaamd) en verzonden over de Data Bus naar de switchingmachine. Dit gebeurt op de ingangslijnkaart. Op dit moment is het nog niet bekend of deze interne CoS naar het egress Application-specifieke geïntegreerde circuit (ASIC) wordt overgebracht en in het uitgaande frame wordt ingebracht. Zodra de header de switchingmachine bereikt, kent de switchingmachine Encoded Address Recognition Logic (EARL) elk frame en interne DSCP toe. Deze interne DSCP is een interne prioriteit die aan het frame is toegewezen door de Policy functiekaart (PFC) wanneer deze de switch doorvoert. Dit is niet de DSCP in de IPv4 header. Het is afgeleid van een bestaande CoS of een type service (ToS) instelling en wordt gebruikt om de CoS of ToS te resetten terwijl het frame de switch verlaat. Deze interne DSCP wordt toegewezen aan alle frames die door de PFC zijn geschakeld of routeerd, zelfs niet-IP frames.

V. Wat zijn de mogelijke bronnen voor het "internal gedifferentieerde services code point" (DSCP)?

A. Raadpleeg de vier mogelijke bronnen voor interne DSCP-sectie van QoS-classificatie en markering op Catalyst 6500/6000 Series Switches die CatOS-software uitvoeren.

V. Hoe wordt het interne gedifferentieerde servicecepunt (DSCP) gekozen?

A. De interne DSCP is afhankelijk van deze factoren:

- Havenvertrouwensstaat
- Toegangscontrolelijst (ACL) gekoppeld aan de poort
- Standaard ACL
- VLAN-gebaseerd of op havens gebaseerd, wat betreft de ACL

Dit stroomschema vat samen hoe de interne DSCP op basis van de configuratie wordt geselecteerd:

Q. Wordt op klasse gebaseerde gewogen fair lange wachtrijen (CBWFQ) of lage latentie wachtrijen (LLQ) ondersteund in de Catalyst 6500 (Cat6K) Switch?

A. Ja, CBWFQ staat u toe om een klasse van verkeer te definiëren en het een minimum bandbreedtegarantie toe te wijzen. Het algoritme achter dit mechanisme is gewogen fair wachtrij (WFQ), wat de naam verklaart. U definieert specifieke klassen in map-class statements om CBWFQ te configureren. Dan geef je een beleid aan elke klasse toe in een beleids-kaart. Deze beleidskaart wordt dan verbonden aan het in/uit van een interface.

Q. Is Layer 2 class of Service (CoS) waarde behouden voor Routed Packets?

A. Ja, het interne gedifferentieerde servicescodenummer (DSCP) wordt gebruikt om de CoS op noodopdrachten te resetten.

Q. Past QoS de identieke configuratie toe op alle LAN poort die door dezelfde ASIC wordt gecontroleerd?

A. Ja, wanneer deze opdrachten worden geconfigureerd, past QoS identieke configuratie toe op alle LAN/routed poorten die gecontroleerd worden door dezelfde Application Specific Integrated Circuit (ASIC). De QoS-instellingen worden verspreid naar andere havens die tot dezelfde ASIC behoren, ongeacht of de haven een toegangshaven, boomhaven of een routehaven is.

- rcv-wachtrij met willekeurige detectie
- rijbeperkingen in de rij-rij

- **wachtrijlimiet**
- **bandbreedte in de wachtrij** (behalve Gigabit Ethernet LAN-poorten)
- **prioriteitswachtrij voor cos-map**
- **rcv-wachtrij voor cos-map**
- **warenrij rapport**
- **drempelwaarde voor wachtrijen**
- **grenswaarde voor rcv-wachtrij**
- **rij-op-rij willekeurig detecteren**
- **rij-willekeurig detecteren ondergrens**
- **rij-willekeurig detecteren max-drempel**

Wanneer het **standaard *interface* commando** op een van de poorten wordt uitgevoerd, dan stelt ASIC die de poort controleert de QoS configuratie opnieuw in voor alle poorten die door het besturen worden.

Q. Waarom toont de opdracht Statistieken van de show geen positief resultaat, zelfs niet wanneer het verkeer wordt geschuild?

```
Router#show traffic-shape statistics
          Access Queue     Packets   Bytes     Packets   Bytes     Shaping
I/F       List   Depth                        Delayed   Delayed   Active
Et0       101    0         2         180       0         0         no
Et1              0         0         0         0         0         no
```

A. De eigenschap Shaping Active heeft **`ja`** **wanneer timers aangeven dat traffic shaping plaatsvindt en `niet` indien traffic shaping niet plaatsvindt.**

U kunt de opdracht **Show beleid-map** gebruiken om te controleren of het geconfigureerde verkeer werkt.

```
Router#show policy-map
  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)
  Policy Map MQC-SHAPE-LLQ1
    Class class-default
      Traffic Shaping
         Average Rate Traffic Shaping
                 CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
                 Adapt to 8000 (bps)
                 Voice Adapt Deactivation Timer 30 Sec
      service-policy VSD1
```

Q. steunt Catalyst 6500 PFC alle standaard QoS opdrachten?

A. Cisco Catalyst 6500 PFC QoS heeft bepaalde beperkingen en ondersteunt geen bepaalde opdrachten die betrekking hebben op QoS. Raadpleeg deze documenten voor de volledige lijst met opdrachten die niet worden ondersteund.

- Beperkingen van klasse-kaartopdracht
- Beperkingen in beleidsmap
- Beperkingen van klasse van beleidskaarten

Q. Waarom zijn de software CoP tellers groter dan de hardware CoP tellers?

A. Tellers van CoPP-softwarecontrole (Software Control Plane Policing) zijn de som van pakketten waarin hardware-CoPP wordt getransporteerd en de hardwaresnelheidsbeperking wordt toegepast. Pakketten worden eerst verwerkt door hardwaresnelheidslimiters en als ze niet overeenkomen, wordt hardware-CoPP op een foto gezet. Als de hardwaresnelheidsbeperking voor de pakketten toestaat, gaat dit pakket naar software waar het door software CoPP wordt verwerkt. Dankzij deze software kan CoPP groter zijn dan hardware CoP tellers.

Er zijn ook enkele beperkingen waaraan CoPP niet in hardware wordt ondersteund. Onder hen:

- CoPP wordt niet in hardware ondersteund voor multicast pakketten. De combinatie van ACL's, multicast CPU-snelheidslimiters en CoPP-softwarebeveiliging biedt bescherming tegen multicast DoS-aanvallen.
- CoPP wordt niet in hardware ondersteund voor broadcast-pakketten. De combinatie van ACL's, verkeersonweerscontrole en CoPP-softwarebescherming biedt bescherming tegen DoS-aanvallen door uitzending.
- Klassen die overeenkomen met multicast worden niet toegepast in hardware maar worden in software toegepast.
- CoPP is niet ingeschakeld in hardware tenzij MMLS QoS wereldwijd is ingeschakeld met de opdracht **mls qos**. Als de opdracht **mls qos** niet wordt ingevoerd, werkt CoPP alleen in software en levert CoPP geen voordeel op aan de hardware.

Raadpleeg Config Control Plane Monitoring (CoPP) voor meer informatie.

Q. Werkt de standaard (interface) opdracht QoS-configuratie op andere interfaces/poorten?

A. Wanneer het **standaard *interface*** bevel wordt uitgegeven, wordt de niet standaard configuratie verzameld, wat gelijk is aan wat in **show in werking stellen-configuratie interface *x/y*** wordt weergegeven, en elk van deze wordt ingesteld op hun standaardwaarden. Dit kan ook een simpele negatie van een opdracht zijn.

Als er een QoS of andere functies zijn die op die interface zijn geconfigureerd en die opdrachten worden verwaarloosd, kunnen ze naar andere interfaces van de lijnkaart propageren.

Het wordt aanbevolen om de uitvoer van de opdracht **Show interface *x/y* mogelijkheden** te controleren, voordat u verdergaat met het standaardiseren van een interface. Raadpleeg Is QoS van toepassing op alle LAN poort die door dezelfde ASIC wordt bestuurd? voor meer informatie .

De output van het **standaard *interface* bevel** toont ook (als enig) andere interfaces die beïnvloed worden voor QoS en andere eigenschappen die in die haven ASIC worden geïmplementeerd.

Kan ik QoS configureren in een interface met een secundaire IP?

A. Ja. U kunt QoS op een secundair IP configureren.

Gerelateerde informatie

- QoS O-planning bij Catalyst 6500/6000 Series Switches die CatOS-systeemsoftware uitvoeren
- QoS-classificatie en markering op Catalyst 6500/6000 Series Switches die CatOS-software uitvoeren
- QoS-toezicht op Catalyst 6500/6000 Series Switches
- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems