

Quality-of-Service uitvoeren

Inhoud

[Inleiding](#)

[Welke toepassingen hebben QoS nodig?](#)

[De eigenschappen van de toepassingen begrijpen](#)

[De netwerktopologie kennen](#)

[Link Layer Header Sizes](#)

[Klassen creëren op basis van de criteria](#)

[Een beleid maken om elke klasse te markeren](#)

[Vanaf de rand naar de kern werken](#)

[Het bouwen van een beleid om het verkeer te behandelen](#)

[Het beleid toepassen](#)

[Het gebruik van QoS Policy Manager \(QPM\) om de effecten van het beleid te bewaken](#)

[Algemene doelstellingen QoS - aanbevelingen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document bevat enige richtlijnen op hoog niveau voor het implementeren van Quality of Service (QoS) in een netwerk dat fungeert als transport voor meerdere toepassingen, inclusief vertraginggevoelige en bandbreedte-intensieve toepassingen. Deze toepassingen kunnen bedrijfsprocessen verbeteren, maar strekken netwerkbronnen uit. QoS kan veilige, voorspelbare, meetbare en gegarandeerde services aan deze toepassingen leveren door vertraging, vertragingen (jitter), bandbreedte en pakketverlies in een netwerk te beheren.

Welke toepassingen hebben QoS nodig?

Bepaal eerst welke toepassingen van bedrijfskritiek belang zijn en bescherming vereisen. Het kan zijn dat je alle toepassingen moet bekijken die concurreren om netwerkbronnen. Als dit probleem zich voordoet, gebruikt u [NetFlow Accounting](#), [Network-Based Application Recognition \(NBAR\)](#), of [QoS Devices Manager \(QDM\)](#) om de verkeerspatronen in het netwerk te analyseren.

NetFlow-accounting biedt details over netwerkverkeer en kan worden gebruikt om de verkeersclassificatie of voorrang te geven die bij elke stroom hoort.

NBAR is een classificatiehulpmiddel dat verkeer tot de toepassingslaag kan identificeren. Het voorziet per interface, per-protocol, en bi-directionele statistieken voor elke verkeersstroom die een interface overschrijdt. NBAR heeft ook een subpoortclassificatie; kijken naar en identificeren van havens buiten de toepassingsgebieden .

QDM is een op internet gebaseerde toepassing voor netwerkbeheer die een gebruiksvriendelijke grafische gebruikersinterface biedt voor het configureren en bewaken van geavanceerde IP-

gebaseerde QoS-functies in routers.

De eigenschappen van de toepassingen begrijpen

Het is belangrijk de kenmerken van de toepassingen te begrijpen die bescherming behoeven. Sommige toepassingen zijn gevoelig voor latentie of pakketverlies, terwijl anderen als "agressief" worden beschouwd omdat ze last hebben of veel bandbreedte consumeren. Als de applicatie barst, controleer dan of er een constante uitbarsting of een kleine uitbarsting is. Is de pakketgrootte van de toepassing groot of klein? Is de toepassing TCP of UDP gebaseerd?

karakteristiek	Richtsnoer
Toepassing die vertraging- of verliesgevoelig is. (spraak- en realtime-video)	Gebruik <i>geen</i> gewogen willekeurige vroegtijdige detectie (WRED), traffic shaping, fragmentation (FRF-12) of toezicht. Voor dit soort verkeer dient u Low Latency Queuing (LLQ) te implementeren en een prioriteitswachtrij voor het vertraginggevoelige verkeer te gebruiken.
Een toepassing die constant bursty is of een bandbreedteschoen is. (FTP en HTTP)	Gebruik WRED, toezicht, traffic shaping of class-Based Wachten (CBWFQ) om bandbreedte te garanderen.
Toepassing die op TCP gebaseerd is.	Gebruik WRED sinds verloren pakketten TCP terugkeren en dan opnieuw opvoeren met de langzaam-start algoritme. Als het verkeer op UDP gebaseerd is en zijn gedrag niet verandert wanneer pakketten worden ingetrokken, gebruik dan geen WRED. Gebruik controle als u de toepassing wilt beperken; laat de pakketten anders gewoon achter.

De netwerktopologie kennen

Sommige apparaten kunnen een IOS upgrade nodig hebben om voordeel te halen uit de QoS-functies die u wilt implementeren. De diagrammen van de netwerktopologie, de routerconfiguraties, en de softwareversie op elk apparaat helpen u het aantal apparaten schatten dat een IOS upgrade vereist. Raadpleeg de [Cisco ICON Library](#) voor pictogrammen die u kunnen helpen netwerkdiagrammen te maken.

- Evalueer het CPU-gebruik op elke router tijdens drukke perioden om te helpen beslissen hoe u QoS-functies onder apparaten distribueert om de lading te delen.
- Classificeer zakelijk-kritieke verkeerstypen de interfaces die dit verkeer zal oversteken. Bepaal welke prioriteitsgroepen of -klassen u wilt maken om de QoS-doelstellingen voor uw netwerk te realiseren.
- Bepaal de maximale vertraging die de meest kritische toepassingen kunnen verwerken en aanpassen van de barstparameters binnen traffic conditioners (traffic shapers of politiers) om deze vertraging op te vangen.
- Zoek uit welke snelheden op elke interface worden ondersteund: PVC's of subinterfaces en configureren de bandbreedte die moet worden aangepast.
- Langzame koppelingen identificeren om te helpen bepalen waar de knelpunten in het netwerk zich bevinden en beslissen hoe de mechanismen voor koppelingsefficiëntie op de juiste interfaces worden toegepast.
- Bereken Layer 2 en Layer 3 overhead voor elk mediatype dat het bedrijfs kritieke verkeer zal transporteren. Dit zal helpen de correcte hoeveelheid bandbreedte voor elke klasse te berekenen nodig.
- Een ander belangrijk stuk informatie is of u verkeer wilt beschermen op basis van toepassing, IP bron en bestemming, of beiden.

[Link Layer Header Sizes](#)

Type media	Kop voor koppelingslaag
Ethernet	14 Bytes
PPP	6 Bytes
Frame Relay	4 Bytes
ATM	5 bytes/cel

[Klassen creëren op basis van de criteria](#)

Zodra u hebt bepaald welke toepassingen QoS nodig hebben en welke classificatiecriteria moeten worden gebruikt (op basis van de kenmerken van de toepassingen), bent u klaar om klassen op basis van deze informatie te creëren.

[Een beleid maken om elke klasse te markeren](#)

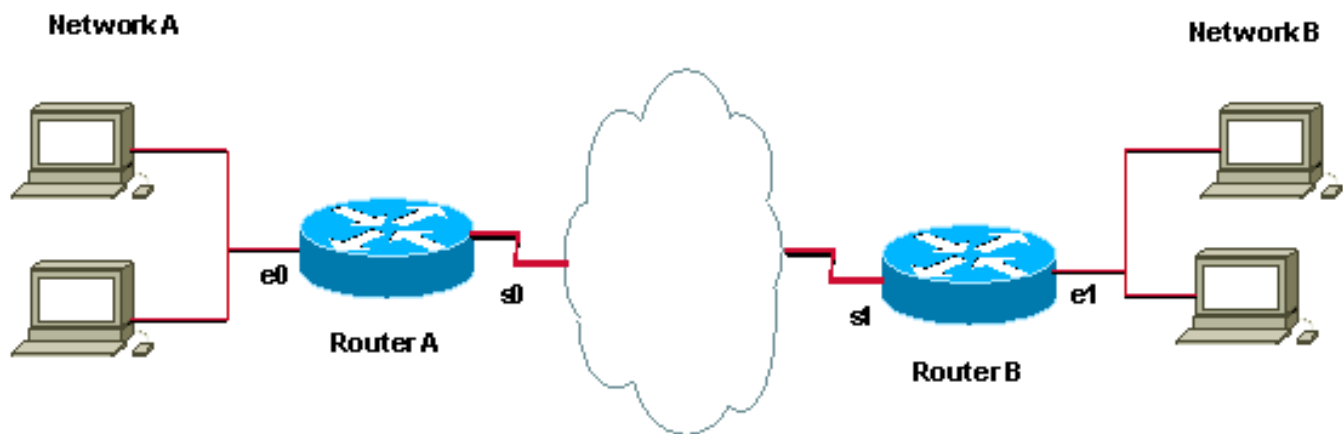
Maak een beleid om elke verkeersklasse te markeren met de juiste prioritaire waarden (gebruik gedifferentieerd servicecontract (DSCP) of IP-voorrang). Het verkeer zal worden gemarkeerd aangezien het in de router op de ingangside interface komt. De markeringen zullen worden gebruikt om het verkeer te behandelen aangezien het de router op de spanning interface verlaat.

[Vanaf de rand naar de kern werken](#)

Werk vanuit de router die het dichtst bij het verkeer naar de kern ligt. Pas uw markering toe op de ingangside interface van de router. In de topologie hieronder, is router A de voor de hand liggende plaats om verkeer te markeren en beleid toe te passen voor gegevens die van Netwerk A zijn gekomen en voor router B bestemd zijn. Het verkeer zal worden gemerkt aangezien het in de

interface van de router A Ethernet0 komt, en het QoS beleid zal op de interface van de router A's seriële0 worden toegepast aangezien het de router verlaat. Als hetzelfde beleid in beide richtingen moet worden toegepast (zodat het verkeer dat afkomstig is van Network B en bestemd is voor Network A dezelfde behandeling krijgt), moet het verkeer dat afkomstig is van Network B worden gemarkeerd als het in de Ethernet1-interface van de router B komt en behandeld worden zoals het de router op de Serial1 interface laat.

Zodra het verkeer op de ingangsiinterface op één router wordt gemarkeerd, behoudt het dezelfde markeringen als het meerdere hop overbrengt (tenzij het opnieuw wordt gemarkeerd). Gewoonlijk hoeft het verkeer slechts eenmaal te zijn gemarkeerd. Het QoS-beleid kan worden toegepast op extra hop op basis van deze markeringen. U hoeft alleen opnieuw te markeren als het verkeer afkomstig is van een onbetrouwbaar domein.



Het bouwen van een beleid om het verkeer te behandelen

Nu u het verkeer hebt gemarkeerd, kunt u de markeringen gebruiken om een beleid te bouwen en verkeersclassificatie op de rest van de netwerksegmenten te doen. We raden aan om het beleid eenvoudig te houden door niet meer dan vier klassen te gebruiken.

Indien mogelijk moet u een QoS-implementatie implementeren in een labomgeving implementeren en testen. Stel deze in het bewegende netwerk in nadat u tevreden bent met de resultaten.

Het beleid toepassen

Pas het beleid in de juiste richting toe. Beslissen of het beleid in één richting of in beide richtingen moet worden toegepast. Merk altijd verkeer zo dicht bij de bron als mogelijk, zoals beschreven in het [Maken van een Beleid om Elke](#) sectie van [Klasse](#) van dit document [te markeren](#).

We raden u aan hetzelfde beleid in beide richtingen toe te passen om verkeer te filteren dat aankomt van en bestemd is voor beide zijden van de locatie. Dit betekent dat u hetzelfde beleid moet toepassen uitgaande op de seriële interface van RouterA en de seriële interface van RouterB.

Het gebruik van QoS Policy Manager (QPM) om de effecten van het beleid te bewaken

Gebruik [QPM](#) als een compleet systeem voor gecentraliseerde beleidscontrole en geautomatiseerde, betrouwbare beleidsimplementatie.

Algemene doelstellingen QoS - aanbevelingen

Hieronder staat een lijst met QoS-categorieën en een aantal van de meer algemeen gebruikte QoS-functies die bij elke categorie horen.

Categorie	Verbonden QoS-functies
QoS-servicemodule	Voorziene (DiffServ) QoS indien mogelijk of indien nodig gemarkeerd (RSVP).
Classificatie/markering	DiffServ-codepunten of qos-groep-ID.
congestiebeheer	LLQ of CBWFQ.
congestievermijding	DiffServ-conforme WRED .
koppelingsefficiëntie	MLPPP, LFI, FRF.11, FRF.12, CRTP
Signalering	RSVP, QPPB
Verkeersconditioners/toezicht	Class Based Policer en Generic Traffic Shaping (GTS) of Frame-Relay Traffic Shaping (FRTS).
Configuratie/bewaking	QPM, modulaire QoS-opdrachtregel (CLI), QDM

Gerelateerde informatie

- [QoS-ondersteuningspagina](#)
- [Ondersteuningspagina voor IP-routeringsprotocollen](#)
- [Ondersteuningspagina voor IP-routing](#)
- [IS-IS ondersteuningspagina](#)
- [Technische ondersteuning - Cisco-systemen](#)