Gestion de la qualité de service IP dans Oracle® Solaris 11.2

Référence: E53874
juillet 2014

ORACLE

Table des matières

Utilisation de la présente documentation

- **Présentation** : décrit comment configurer le le service IPQoS
- **Public visé** : les techniciens, aux administrateurs système et les fournisseurs de services agréés
- **Connaissances requises** : de l'expérience dans l'utilisation d'Oracle Solaris est utile

Bibliothèque de documentation du produit

Les informations de dernière minute et les problèmes connus pour ce produit sont inclus dans la bibliothèque de documentation accessible à l'adresse : http://www.oracle.com/pls/topic/lookup?ctx=E56338.

Accès aux services de support Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs si vous êtes malentendant.

Commentaires en retour

Faites part de vos commentaires sur cette documentation à la page suivante : http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPITRE 1

Présentation d'IPQoS

La qualité de service IP (IPQoS) permet de hiérarchiser, de contrôler et de recueillir les statistiques comptables. A l'aide d'IPQoS, vous pouvez fournir des niveaux de service homogènes aux utilisateurs de votre réseau. Cela permet également de gérer le trafic pour éviter la congestion du réseau.

Ce chapitre comprend les sections suivantes :

Remarque - La fonction IPQoS risque d'être supprimée dans une version ultérieure. Les utilisateurs sont invités à utiliser à sa place les commandes `dladm` et `flowadm` ainsi que les commandes associées, qui assurent des fonctions de contrôle des ressources de bande passante similaires. Pour plus d'informations, reportez-vous au manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Principes de base d'IPQoS

IPQoS active l'architecture de services différenciés (Diffserv) qui est défini par le groupe de travail de l'IETF, The Differentiated Services Working Group. Dans Oracle Solaris, IPQoS est implémenté au niveau de la pile de protocole TCP/IP.

Quels sont les services différenciés ?

En activant IPQoS, vous pouvez fournir des niveaux de service différents pour les clients et les applications sélectionnés. Les différents niveaux de service sont collectivement désignés sous l'appellation de *services différenciés*. Les services différenciés fournis aux clients peuvent

se baser sur la structure des niveaux de service offerts par l'entreprise à ses clients. Vous pouvez également fournir des services différenciés en fonction des priorités définies pour les applications ou les utilisateurs de votre réseau.

Assurer la qualité de service (QoS) implique de réaliser les activités suivantes :

- Déléguer des niveaux de service à différents groupes (clients ou services d'une entreprise, par exemple)
- Définir la priorité des services réseau attribuée à certains groupes ou applications
- Discerner et éliminer les goulets d'étranglement ou toute autre forme de congestion
- Contrôler les performances réseau et fournir des statistiques sur les performances
- Réguler la bande passante au vu des ressources réseau

Fonctions IPQoS

IPQoS comprend les fonctions suivantes :

- Classificateur sélectionnant les actions, selon les filtres configurant la stratégie QoS de votre organisation
- Module de mesure du trafic réseau conformé au modèle Diffserv
- Différenciation des services basée sur la possibilité de marquer un en-tête IP de paquet avec des informations de transmission
- Module de comptabilisation des flux rassemblant les statistiques des flux de trafic
- Statistiques sur les classes de trafic, via la commande UNIX `kstat`
- Prise en charge des architectures SPARC et x86
- Prise en charge des adresses IPv4 et IPv6
- Interopérabilité avec l'architecture de sécurité IP (IPsec)
- Prise en charge des marquages de priorité utilisateur 802.1D dans les réseaux locaux virtuels (VLAN)

Sources d'informations

Vous trouverez des informations sur les services différenciés et la qualité de service dans la documentation papier ou en ligne.

IPQoS est conforme aux spécifications qui sont décrites dans les documents RFC suivants :

- Le document RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (http://www.ietf.org/rfc/rfc2474.txt?number=2474) (en anglais) décrit une amélioration du champ de type de service (ToS) ou champ DS des en-têtes de paquet IPv4 et IPv6 pour la prise en charge des services différenciés

- Le document RFC 2475, An Architecture for Differentiated Services (http://www.ietf.org/rfc/rfc2475.txt?number=2475) (en anglais) décrit en détail l'organisation et les modules de l'architecture Diffserv

La documentation d'IPQoS comprend les pages de manuel suivantes :

- `ipqosconf`(1M) - Décrit la commande permettant de paramétrer le fichier de configuration IPQoS
- `ipqos`(7ipp) – Décrit l'implémentation IPQoS du modèle d'architecture Diffserv
- `ipgpc`(7ipp) – Décrit l'implémentation IPQoS d'un classificateur Diffserv
- `tokenmt`(7ipp) – Décrit le module de mesure IPQoS `tokenmt`
- `tswtclmt`(7ipp) – Décrit le module de mesure IPQoS `tswtclmt`
- `dscpmk`(7ipp) – Décrit le module de marquage DSCP
- `dlcosmk`(7ipp) – Décrit le module de marquage de priorité utilisateur IPQoS 802.1D
- `flowacct`(7ipp)– Décrit le module de comptabilisation de flux IPQoS
- `acctadm`(1M) – Décrit la commande permettant de configurer les fonctions de comptabilité étendues d'Oracle Solaris et inclut des extensions IPQoS.

Livraison d'une qualité de service avec IPQoS

Les fonctions IPQoS permettent aux fournisseurs d'accès Internet (FAI) ainsi qu'aux fournisseurs de services d'applications (ASP) d'offrir différents niveaux de service réseau à leurs clients. Ces fonctions permettent à des sociétés et à des organismes d'éducation ou de formation de hiérarchiser les services pour des organisations internes ou pour les applications principales.

Implémentation des accords de niveau de service

Si votre organisation est un FAI ou un fournisseur de services d'applications, vous pouvez baser votre configuration IPQoS sur le *contrat de niveau de service* que votre entreprise propose à ses clients. Dans le cadre d'un contrat de niveau de service, un fournisseur de service garantit à un client un certain niveau de service réseau basé sur une hiérarchie de prix. Par exemple, un accord de type premium implique que le client reçoive la plus haute priorité pour tous les types de trafic réseau 24 h/24h 7j/7. Inversement, un accord facturé à un prix moyen indique que le client bénéficie d'une haute priorité pour la transmission des messages électroniques uniquement pendant les heures d'ouverture de bureau. Tout autre trafic se voit appliquer une priorité moyenne 24 h/24h.

Garantie d'une qualité de service pour une organisation

Si votre organisation est une entreprise ou une institution, vous pouvez également utiliser différentes fonctions liées à la qualité de service pour votre réseau. Ainsi, il est possible d'appliquer un degré de service plus ou moins élevé au trafic d'un groupe ou d'une application spécifique.

Introduction à la stratégie de qualité de service

Pour implémenter la qualité de service, vous devez définir une *stratégie de qualité de service (QoS)*. La stratégie de qualité de service spécifie plusieurs attributs de réseau comme la priorité des clients ou des applications et les actions pour le traitement de différentes catégories de trafic. Vous implémentez la stratégie de qualité de service de votre organisation dans un fichier de configuration IPQoS. Ce fichier configure les modules IPQoS se trouvant dans le noyau Oracle Solaris. Un hôte auquel une stratégie IPQoS est appliquée est considéré comme un *système IPQoS*.

Votre stratégie QoS définit les éléments suivants :

- Des groupes discrets de trafic réseau appelés *classes de service*.
- Des mesures de régulation du volume du trafic réseau de chaque classe. Elles régissent le processus de contrôle du trafic appelé *mesure*.
- Une action qu'un système IPQoS et un routeur Diffserv doivent appliquer à un flux de paquets. Ce type d'action est désigné comme le *PHB* (per-hop behavior ou comportement par saut).
- Toute collecte de statistiques dont votre organisation a besoin sur une classe de service. Par exemple, le trafic généré par un client ou une application spécifique.

Lorsque les paquets arrivent sur le réseau, le système IPQoS évalue les en-têtes de paquets. L'action que le système IPQoS réalise est déterminée par votre stratégie QoS.

Les tâches pour élaborer la conception de la stratégie QoS sont décrites dans la section “Planification de la stratégie de qualité de service” à la page 29.

Amélioration de l'efficacité du réseau dans IPQoS

IPQoS contient des fonctions qui contribuent à augmenter l'efficacité des performances réseau lors de l'implémentation de la qualité de service. Par exemple, dans le cadre d'une entreprise ou d'une institution, il est indispensable de maintenir un réseau performant afin d'éviter les goulets d'étranglement. Vous devez également veiller à ce qu'un groupe ou une application ne

consomme pas plus de bande passante que le volume alloué. Pour un FAI ou un ASP, vous devez gérer les performances du réseau pour assurer que les clients reçoivent le service réseau correspondant à l'abonnement souscrit.

Les pertes de données et la congestion du trafic peuvent être des symptômes d'un réseau surexploité. Ces signes se traduisent par des délais de réponse très lents. Dans le passé, les administrateurs système géraient les problèmes de trafic réseau, c'est - à - dire la bande passante volume maximal de données qu'une liaison réseau ou un périphérique intégralement exploité peut transmettre. Cependant, souvent le niveau du trafic des liaisons variait considérablement. Grâce à IPQoS, il est possible de gérer le trafic sur le réseau existant et d'évaluer si une extension s'avère nécessaire et, le cas échéant, les zones visées.

Impact de la bande passante sur le trafic réseau

Votre stratégie QoS doit déterminer la priorité de l'utilisation de la bande passante afin de fournir la qualité de service aux clients ou utilisateurs. Les modules de mesure IPQoS permettent de mesurer et de contrôler l'allocation de la bande passante aux classes de trafic sur un hôte IPQoS.

Examinez les questions suivantes afin de déterminer le mode de gérer efficacement le trafic sur un réseau, procédez comme suit :

- Quelles sont les zones de votre réseau local associées à un problème de trafic ?
- Que devez vous faire pour atteindre l'utilisation optimale de la bande passante disponible ?
- Quelles sont les applications critiques de votre site auxquelles une priorité élevée doit être attribuée ?
- Quelles sont les applications sensibles à une éventuelle congestion ?
- Quelles sont, parmi vos applications, les applications les moins critiques compatibles avec une priorité la plus faible ?

Utilisation des classes de service pour hiérarchiser le trafic

Pour implémenter la qualité de service, vous analysez le trafic du réseau afin de déterminer les groupes globaux dans lesquels le trafic peut être réparti. Organisez ensuite les groupes en classes de service dotées de caractéristiques et de priorités spécifiques. Classes de service forment les catégories fondamentales sur lesquelles vous basez la stratégie QoS de votre organisation et représentent les groupes de trafic à contrôler.

Lorsque vous analysez les détails du trafic réseau, tenez compte des consignes suivantes :

- **L'entreprise offre-t-elle des accords de niveau de service à ses clients ?**

Si oui, évaluez les niveaux de priorité relatifs définis pour les contrats de niveau de service qu'offre l'entreprise. Les clients peuvent se voir proposer une même application assortie de niveaux de priorité différents.

Par exemple, l'entreprise peut offrir un hébergement de site Web à chacun de ses clients ce qui signifie qu'il est nécessaire de définir une classe pour chaque site Web client. Un contrat de niveau de service peut fournir un site Web Premium au titre d'un niveau de service. Un autre contrat de niveau de service peut consister en un site Web personnel utilisable "au mieux" à l'usage de clients bénéficiant de remises. Ce facteur signale non seulement différentes classes de sites Web, mais également des comportements (PHB) potentiellement différents, assignés aux classes de sites Web.

- **Le système IPQoS offre-t-il des applications courantes nécessitant éventuellement un contrôle des flux ?**

  Vous pouvez améliorer les performances réseau en activant IPQoS sur les serveurs proposant des applications courantes qui génèrent un trafic important. Les exemples les plus courants sont les applications de messagerie électronique, de discussion réseau et FTP. Envisagez de créer des classes indépendantes pour le trafic entrant et sortant de chaque type de service, si besoin est. Par exemple, il est possible de créer une classe `courrier entrant` et une classe `courrier sortant` pour la stratégie QoS d'un serveur de courrier.

- **Le réseau exécute-t-il des applications qui impliquent une transmission en haute priorité ?**

  Toute application critique nécessitant un transfert en priorité haute doit être prioritaire dans la file d'attente du routeur. C'est le cas, par exemple, des flux de données vidéo et audio.

  Définissez les classes entrantes et sortantes pour ces applications à haute priorité. Ensuite, insérez les classes dans les stratégies QoS du routeur Diffserv et du système IPQoS fournissant les applications.

- **Le réseau fait-il l'objet de flux de trafic à contrôler en raison de la consommation importante de bande passante ?**

  Exécutez `netstat` , `snoop` et d'autres utilitaires de contrôle réseau pour détecter les types de trafic à l'origine des problèmes survenant sur le réseau. Etudiez les classes que vous avez créées jusqu'ici, puis générez de nouvelles classes pour les catégories de problèmes de trafic non définis. Si vous avez déjà défini des classes pour une catégorie de problèmes, définissez les débits du compteur chargé de contrôler le trafic problématique.

  Créez des classes pour le trafic posant problème dans chaque système IPQoS situé sur le réseau. Chaque système IPQoS peut alors gérer un trafic problématique en réduisant le débit du flux arrivant sur le réseau. Assurez-vous également de spécifier ces classes dans la stratégie QoS sur le routeur Diffserv. Le routeur peut ainsi mettre en attente et planifier les flux problématiques conformément à la configuration de la stratégie QoS.

- **Avez-vous besoin de connaître les statistiques sur certains types de trafic ?**

  L'examen rapide d'un contrat de niveau de service peut révéler les types des trafics client devant être comptabilisés. Si votre site offre des contrats de niveau de service, vous avez sans doute déjà créé des classes relatives au trafic impliquant des données de comptabilisation. Vous pouvez également être amené à définir des classes en vue de la

collecte de statistiques concernant les flux de trafic que vous contrôlez. Il est possible de définir des classes pour le trafic soumis à des restrictions d'accès pour des raisons de sécurité.

Par exemple, un fournisseur peut offre des accords de niveau de service platinum, gold, silver et bronze disponibles selon une échelle de prix. Un contrat de niveau de service platinum accorde la priorité la plus haute au trafic entrant d'un site Web que le FAI héberge au nom du client.

Dans le cadre d'une entreprise, vous pouvez créer des classes de service, par exemple les exemples suivants :

- Les applications courantes comme la messagerie électronique et le trafic FTP sortant vers un serveur particulier peuvent constituer l'un ou l'autre une classe. Puisque les employés font constamment appel à ces applications, votre stratégie QoS garantit aux courriers électroniques et au trafic FTP sortant une petite partie de la bande passante et une priorité plus faible.
- Une base de données d'entrées correspondant à des commandes devant fonctionner 24 h/24. Selon l'importance de l'application de la base de données pour l'entreprise, il est possible d'accorder à la base de données une grande partie de la bande passante et une priorité élevée.
- Un service qui réalise des tâches importantes ou confidentielle, comme le service de paie. L'importance du service pour l'organisation détermine la priorité et la largeur de bande passante accordée à un tel service.
- Appels entrants vers le site web externe d'une entreprise. Vous pouvez donner à cette classe une largeur de bande passante moyenne qui s'exécute à basse priorité.

Modèle de services différenciés

IPQoS comprend les modules suivants, lesquels font partie de l'architecture Diffserv définie dans le document RFC 2475 :

- Classificateur
- Compteur
- Marqueur

IPQoS apporte les améliorations suivantes au modèle Diffserv :

- Module de comptabilisation des flux
- Marqueur de datagramme 802.1D

Cette section présente les modules Diffserv tel qu'ils sont utilisés par IPQoS. Pour plus d'informations détaillées sur chaque module, reportez-vous à la section “Architecture IPQoS et modèle Diffserv” à la page 87.

Présentation du classificateur (`ipgpc`)

Dans le modèle Diffserv, le *classificateur* sélectionne des paquets à partir d'un flux de trafic réseau. Un *flux de trafic* consiste en un groupe de paquets avec des informations identiques dans les champs d'en-tête IP suivants :

- Adresse source
- Adresse de destination
- Port source
- Port de destination
- Numéro de protocole

Dans IPQoS, ces champs sont désignés *5-uplet*.

Le classificateur IPQoS `ipgpc` organise les flux de trafic en classes selon les caractéristiques configurées dans le fichier de configuration IPQoS.

Pour des informations détaillées sur `ipgpc`, reportez-vous à la section “Module de classification” à la page 88.

Classes IPQoS

L'organisation du trafic en classes constitue une partie primordiale de la planification de votre stratégie QoS. Lorsque vous créez des classes à l'aide de l'utilitaire `ipqosconf`, vous configurez de fait le module de classification `ipgpc`.

Pour obtenir des informations sur la définition des classes, reportez-vous à la section “Définition des classes de votre stratégie QoS” à la page 31.

Filtres IPQoS

Les *filtres* sont des jeux de règles qui contiennent des paramètres appelés *sélecteurs*. Chaque filtre doit désigner une classe. IPQoS fait correspondre aux paquets les sélecteurs de chaque filtre afin de déterminer si le paquet appartient à la classe du filtre. Toute une gamme de sélecteurs permet de filtrer un paquet, par exemple, l'uplet à 5 attributs d'IPQoS et d'autres paramètres courants :

- Adresses source et de destination
- Port source et port de destination
- Numéros de protocole
- ID utilisateur

- ID de projet
- Point de code de services différenciés (DSCP)
- Indice d'interface

Par exemple, un filtre simple peut comporter le port de destination avec la valeur 80. Le classificateur `ipgpc` sélectionne ensuite tous les paquets liés au port de destination 80 (HTTP) et traite les paquets comme indiqué dans la stratégie QoS.

Pour plus d'informations sur la création de filtres, reportez-vous à la section “Définition de filtres dans la stratégie QoS” à la page 33.

Présentation des compteurs (`tokenmt` et `tswtclmt`)

Dans le modèle Diffserv model, le *compteur* étudie le taux de transmission des flux de trafic par classe. Le compteur évalue dans quelle proportion le débit réel du flux se conforme aux débits configurés et définit le résultat qui convient. Le trafic du flux en fonction du résultat, le compteur sélectionne l'action qui s'ensuit, telles que la transmission du paquet vers une autre action ou le retour du paquet vers le réseau sans traitement supplémentaire.

Les compteurs IPQoS déterminent si un flux de réseau est conforme au débit de transmission défini pour sa classe dans la stratégie QoS. IPQoS comporte deux modules de mesure :

- `tokenmt` – Utilise un plan de mesure de seau à deux jetons
- `tswtclmt` – Utilise un plan de mesure à fenêtre glissante

Les deux modules de mesure aboutissent aux trois résultats rouge, orange et vert. Définissez les actions à réaliser en fonction de chaque résultat dans les paramètres `red_action_name`, `yellow_action_name` et `green_action_name` .

Vous pouvez, en outre, configurer `tokenmt` pour la reconnaissance des couleurs. Une instance de mesure couleur utilise la taille du paquet, le DSCP, le débit du trafic et le paramètres configurés pour déterminer le résultat. Le compteur utilise le DSCP de manière à traduire le résultat du paquet en vert, orange ou rouge.

Pour plus d'informations sur la définition des paramètres pour les compteurs IPQoS, reportez-vous à la section “Planification du contrôle de flux” à la page 34.

Présentation des marqueurs (`dscpmk` et `dlcosmk`)

Dans le modèle Diffserv, le *marqueur* donne une valeur au paquet reflétant un comportement de transmission. Le *marquage* est le processus consistant à placer une valeur dans l'en-tête du paquet de façon à signaler le mode de transmission du paquet vers le réseau.

IPQoS contient deux modules de marquage :

- `dscpmk` – Attribue au champ DS de l'en-tête du paquet IP une valeur numérique appelée *point de code de services différenciés*, ou *DSCP*. Un routeur Diffserv est alors en mesure d'utiliser le point de code DS pour appliquer le comportement de transmission au paquet.
- `dlcosmk` – Spécifie l'étiquette du réseau local virtuel (VLAN) d'un entête de trame Ethernet. Pour cela, il lui attribue une valeur numérique appelée *priorité utilisateur*. La priorité utilisateur indique la *classe de service (CoS)*, définissant le comportement à appliquer au datagramme.

  `dlcosmk` est un extension d'IPQoS qui ne fait pas partie du modèle Diffserv IETF.

Pour plus d'informations sur l'implémentation d'une approche utilisant un marqueur dans le cadre de la stratégie QoS, reportez-vous à la section “Planification du comportement de transfert” à la page 36.

Présentation de la comptabilisation des flux (`flowacct`)

IPQoS ajoute le module de comptabilisation `flowacct` au modèle Diffserv. Vous pouvez utiliser `flowacct` pour collecter des statistiques sur les flux de trafic et facturer les clients en conséquence conformément au contrat de niveau de service souscrit. La comptabilisation des flux présente également un intérêt dans l'optique de la planification de la capacité et du contrôle du système.

Le module `flowacct` fonctionne avec la commande `acctadm` pour créer un fichier journal de comptabilisation. Un journal standard inclut l'uplet à 5 attributs IPQoS, ainsi que deux autres attributs, procédez comme suit :

- Adresse source
- Port source
- Adresse de destination
- Port de destination
- Numéro du protocole
- Nombre de paquets
- Nombre d'octets

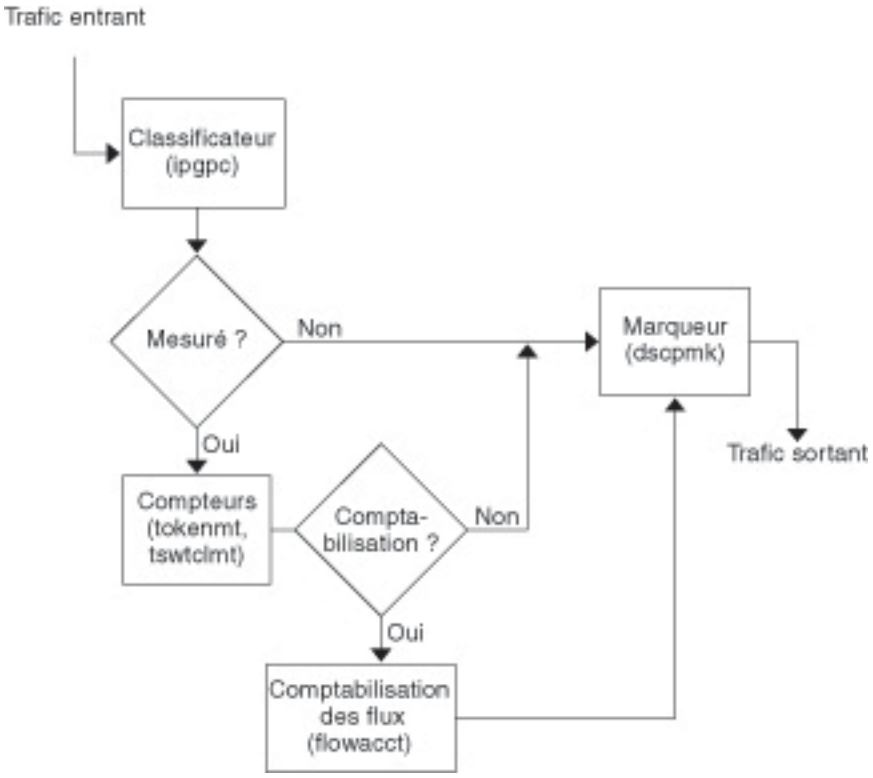
Vous pouvez recueillir les statistiques sur d'autres attributs, comme indiqué à la section “Enregistrement des informations sur les flux de trafic” à la page 81 et dans les pages de manuel `flowacct`(7ipp) et `acctadm`(1M).

Pour plus d'informations sur la planification d'une stratégie de comptabilisation des flux, reportez-vous à la section “Planification de la comptabilisation du flux” à la page 38.

Transit du trafic par les modules IPQoS

La figure suivante présente un itinéraire que le trafic entrant peut suivre en passant par certains modules IPQoS.

FIGURE 1-1 Flux de trafic et implémentation IPQoS du modèle Diffserv



Cette figure illustre une séquence de flux courante sur un ordinateur compatible IPQoS :

1. Le classificateur sélectionne les paquets qui correspondent aux critères de filtre définis pour la stratégie QoS du système dans le flux de paquets.
2. Les paquets sélectionnés sont ensuite évalués en vue de l'action suivante à réaliser.
3. Le classificateur envoie au marqueur le trafic ne nécessitant aucun contrôle de flux.
4. Le trafic à contrôler est transmis au module de mesure.
5. Ce module applique le taux configuré. Il assigne ensuite une valeur de conformité du trafic aux paquets contrôlés.

6. Les paquets dont les flux ont été contrôlés sont ensuite analysés afin de déterminer si des paquets doivent être comptabilisés.
7. Le compteur transmet au marqueur le trafic qui n'exige pas de comptabilisation des flux.
8. Le flux de comptabilisation collecte les statistiques sur les paquets reçus. Le module transmet ensuite les paquets au marqueur.
9. Le marqueur introduit un point de code DS dans l'en-tête du paquet. Ce DSCP signale le traitement, ou PHB, qu'un système Diffserv doit appliquer au paquet.

Trafic sur un réseau compatible IPQoS

Cette section présente les éléments impliqués dans la transmission des paquets sur un réseau IPQoS. Un système IPQoS traite les paquets du réseau en fonction de l'adresse IP du système faisant office de destination. Ce système applique ensuite la stratégie QoS aux paquets afin de fournir des services différenciés.

Point de code DS

Le point de code DS (DSCP) définit, dans l'en-tête du paquet, l'action que le système Diffserv doit appliquer au paquet marqué. L'architecture Diffserv définit un ensemble de points de code DS pour le système IPQoS et le routeur Diffserv à utiliser. L'architecture Diffserv définit également *les comportements de transmission*, qui correspondent aux DSCP. Le système IPQoS marque, à l'aide du DSCP, les bits définissant le niveau de priorité du champ DS dans l'en-tête de paquet. Lorsqu'un routeur reçoit un paquet comportant une valeur DSCP, il applique le comportement associé à ce DSCP. Le paquet est ensuite libéré sur le réseau.

Remarque - Le marqueur `dlcosmk` ne fait pas appel aux valeurs DSCP. A la place, `dlcosmk` marque les en-têtes de trames Ethernet par une valeur CoS (classe de service). Si vous envisagez de configurer IPQoS sur un réseau utilisant des périphériques VLAN, reportez-vous à la section “Module de marquage” à la page 93.

PHB (Per-Hop Behaviors)

Dans la terminologie Diffserv, le comportement assigné à un DSCP est désigné comme le *per-hop behavior (PHB, comportement par saut)*. Le PHB définit le niveau de priorité dont bénéficie un paquet marqué par rapport à tout autre trafic sur le système Diffserv. C'est ce niveau de priorité qui détermine si le système IPQoS ou le routeur Diffserv transmet ou rejette le paquet marqué. Pour un paquet s'effectue sans erreur, tous les routeurs Diffserv rencontrés retransmis que le paquet rencontre trajet vers sa destination finale appliquent le même PHB, à moins qu'un autre système a fait passer le DSCP Diffserv. Pour plus d'informations sur les

PHB, reportez-vous à la section “Utilisation du marqueur `dscpmk` pour la transmission des paquets” à la page 93.

L'objectif d'un PHB consiste à fournir le volume de ressources réseau spécifié à une classe de trafic sur le réseau contigu. Définissez dans la stratégie QoS les DSCP chargés de signaler le niveau de priorité des classes de trafic lorsque les flux de trafic quittent le système IPQoS. Les niveaux de priorités varient entre une haute priorité/faible probabilité de rejet et une priorité faible/haute probabilité de rejet.

Par exemple, votre stratégie QoS peut assigner à une classe de trafic un DSCP garantissant un PHB de faible probabilité de rejet par à partir de n'importe quel les routeurs Diffserv qui réservent la bande passante pour les paquets de cette classe. Vous pouvez associer d'autres DSCP à la stratégie QoS, assignant des niveaux variables de priorité à d'autres classes de trafic. La bande passante accordée aux paquets dont le niveau de priorité est le plus faible dépend des priorités spécifiées par les DSCP des paquets.

IPQoS prend en charge deux types de comportements, définis dans l'architecture Diffserv, le transfert accéléré (EF, Expedited Forwarding) et le transfert garanti (AF, Assured Forwarding).

- EF (Expedited Forwarding)

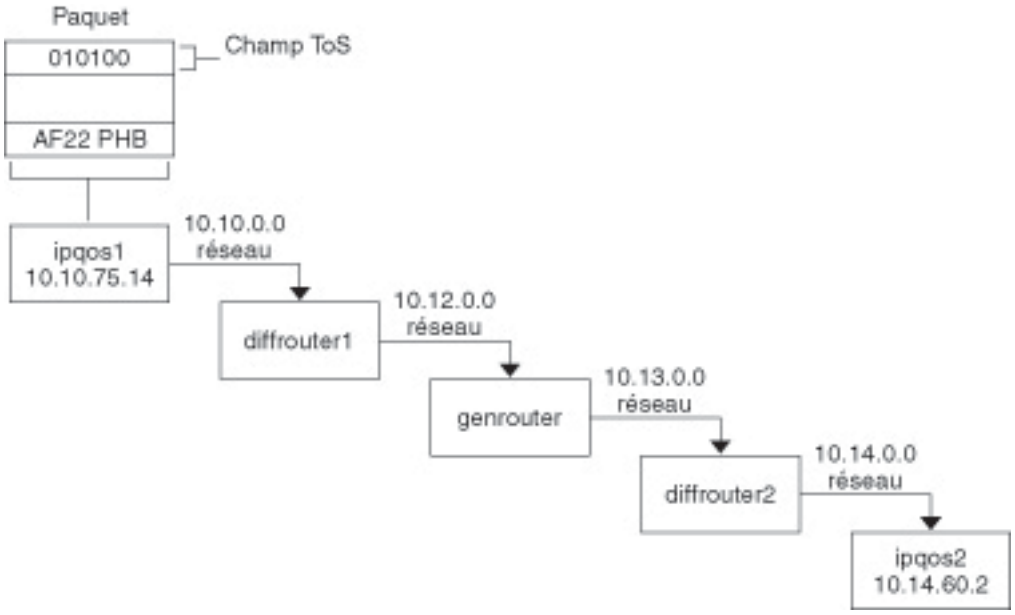
  Ce PHB garantit à toute classe de trafic avec un DSCP EF la priorité la plus élevée. Le trafic doté d'un DSCP EF n'est pas placé dans la file d'attente. EF assure des taux de perte, de délai et de gigue faibles. Le code DSCP recommandé pour EF est 101110. Un paquet ainsi marqué se voit garantir une faible probabilité de rejet alors qu'il transite par les réseaux Diffserv pour parvenir à sa destination. Utilisez le DSCP EF lorsque vous définissez la priorité des clients ou des applications bénéficiant d'un contrat de niveau de service de type premium.
- AF (Assured Forwarding)

  Ce PHB comporte quatre classes de transmission différentes susceptibles d'être appliquées à un paquet.. Chaque classe fournit, à trois niveaux de priorité : taux de perte faible, à son tour un taux de perte moyen et haut de la suppression d'objets. Pour obtenir des informations plus détaillées, reportez-vous au Tableau 6-2, “Points de code Assured Forwarding” Les points de codes AF offrent la possibilité d'assigner différents niveaux de service aux clients et aux applications.

Transmission des paquets dans un environnement Diffserv

La figure suivante illustre une partie de l'intranet d'une entreprise dont l'environnement est partiellement soumis aux règles des services différenciés. Dans cet exemple, tous les hôtes des réseaux `10.10.0.0` et `10.14.0.0` sont compatibles IPQoS et les routeurs locaux sur les deux réseaux reconnaissent Diffserv. Cependant, des réseaux intermédiaires ne sont pas configurés pour prendre en charge les services du modèle Diffserv.

FIGURE 1-2 Transmission des paquets via les noeuds du réseau Diffserv



Le flux du paquet illustré dans cette figure commence par le paquet provenant de l'hôte `ipqos1`. Elles se poursuivent par le passage par plusieurs noeuds afin d'atteindre l'hôte `ipqos2`.

1. L'utilisateur au niveau de l'hôte `ipqos1` exécute la commande `ftp` pour accéder à l'hôte `ipqos2`, situé à trois sauts de là.
2. `ipqos1` applique sa stratégie QoS au flux de paquet. `ipqos1` établit la classification du trafic `ftp`.

   L'administrateur système a créé une classe pour tout le trafic `ftp` sortant issu du réseau local 10.10.0.0. Le trafic de la classe `ftp` est affecté au comportement AF22 : priorité de classe 2, niveau de perte moyen. Un débit de 2 Mbits/sec est défini pour la classe `ftp`.
3. `ipqos-1` mesure le flux `ftp` pour déterminer si le flux dépasse le débit garanti de 2 Mbits/sec.
4. Le marqueur sur l'hôte `ipqos1` définit les champs DS des paquets `ftp` sortant à l'aide du DSCP 010100, correspondant au PHB AF22.
5. Le routeur `diffrouter1` reçoit les paquets `ftp`. `diffrouter1` prend ensuite connaissance du DSCP. Si `diffrouter1` est surchargé, les paquets marqués AF22 sont rejetés.
6. Le trafic `ftp` est transmis au noeud suivant conformément au PHB défini pour AF22 dans les fichiers de `diffrouter1`.

7. Le trafic `ftp` transite par le réseau `10.12.0.0` pour rejoindre le routeur `genrouter` qui ne reconnaît pas les services différenciés. Un traitement "au mieux" est alors appliqué au trafic.
8. `genrouter` transmet le trafic `ftp` au réseau `10.13.0.0` au sein duquel le trafic est reçu par le routeur `diffrouter2`.
9. `diffrouter2` reconnaît l'architecture Diffserv. Par conséquent, le routeur envoie les paquets `ftp` sur le réseau conformément au PHB défini dans la stratégie du routeur pour les paquets AF22.
10. `ipqos2` reçoit le trafic `ftp`. `ipqos2` demande à l'utilisateur au niveau de l'hôte `ipqos1` son nom d'utilisateur et son mot de passe.

♦ ♦ ♦ CHAPITRE 2

Planification d'un réseau compatible IPQoS

Vous pouvez configurer une architecture IPQoS sur un système qui exécute Oracle Solaris Le système IPQoS fonctionne alors avec des routeurs Diffserv chargés de fournir des services différenciés et une gestion du trafic sur un intranet.

Ce chapitre contient des informations de planification visant à ajouter des systèmes IPQoS sur un réseau compatible avec Diffserv.

Remarque - La fonction IPQoS risque d'être supprimée dans une version ultérieure. Les utilisateurs sont invités à utiliser à sa place les commandes `dladm` et `flowadm` ainsi que les commandes associées, qui assurent des fonctions de contrôle des ressources de bande passante similaires. Pour plus d'informations, reportez-vous au manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Planification générale de la configuration IPQoS (liste de tâches)

L'implémentation de services différenciés, dont IPQoS, sur un réseau demande une planification approfondie. Vous devez tenir compte de l'emplacement et de la fonction de chaque système IPQoS, mais également de la relation que chaque système entretient avec le routeur ou le réseau local. La liste des tâches suivante répertorie les principales tâches de planification pour l'implémentation d'une architecture IPQoS sur votre réseau et renvoie vers les procédures permettant d'effectuer ces tâches.

Tâche	Description	Pour obtenir des instructions
1. Planification d'une topologie de réseau Diffserv qui intègre les systèmes IPQoS.	Choisissez parmi les différentes topologies de réseau Diffserv pour déterminer la solution la plus adaptée à votre site.	“Planification de la topologie de réseau Diffserv” à la page 26.
2. Planification des différents types de service qui seront offerts par les systèmes IPQoS.	Organisez les types de service que le réseau fournit dans les contrats de niveau de service.	“Planification de la stratégie de qualité de service” à la page 29.
3. Planification de la stratégie QoS pour chaque système IPQoS.	Identifiez les classes, les fonctions de mesure et de comptabilité nécessaires à l'implémentation de chaque contrat de niveau de service.	“Planification de la stratégie de qualité de service” à la page 29.
4. Si nécessaire, planification de la stratégie du routeur Diffserv.	Elaborez d'éventuelles stratégies de programmation et de mise en file d'attente pour le routeur Diffserv utilisé avec les systèmes IPQoS.	Pour plus d'informations sur ces stratégies, reportez-vous à la documentation du routeur.

Planification de la topologie de réseau Diffserv

Pour faire bénéficier votre réseau de services différenciés, vous devez disposer d'au moins un système IPQoS et d'un routeur compatible Diffserv. Vous pouvez intégrer ce scénario de base à une multitude de variantes, comme expliqué dans cette section.

Stratégies matérielles pour le réseau Diffserv

En général, les clients exécutent IPQoS sur les serveurs et les consolidations de serveurs. Inversement, vous pouvez également exécuter IPQoS sur des ordinateurs de bureau, en fonction des besoins du réseau utilisé.

La liste suivante décrit les systèmes possibles pour une configuration IPQoS :

- Systèmes Oracle Solaris offrant des services variés (serveurs Web et serveurs de base de données)
- Serveurs d'application proposant des applications de messagerie électronique, FTP ou d'autres applications réseau courantes
- Serveurs de cache Web ou serveurs proxy
- Réseau de batteries de serveurs IPQoS gérées par des équilibreurs de charge compatibles Diffserv
- Pare-feux gérant le trafic d'un seul réseau hétérogène
- Systèmes IPQoS faisant partie d'un réseau local virtuel

Vous pouvez insérer des systèmes IPQoS dans une topologie de réseau comportant des routeurs compatibles Diffserv. Si le routeur local n'implémente pas Diffserv, le routeur transmet les paquets marqués au noeud suivant sans analyser les marques.

Topologies de réseau IPQoS

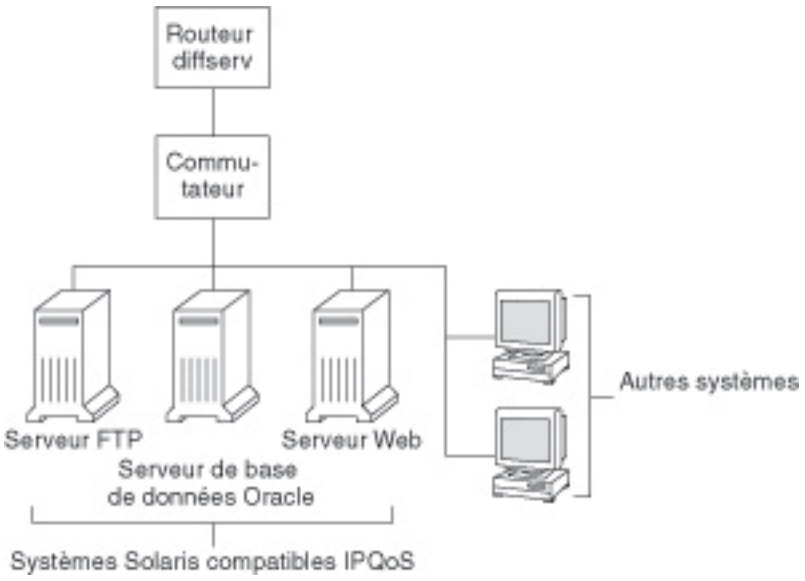
Cette section illustre les stratégies IPQoS qui répondent à différentes exigences de réseau.

IPQoS sur des hôtes indépendants

La figure suivante présente un réseau unique composé de systèmes IPQoS. Ce réseau ne représente qu'un seul segment d'un intranet d'entreprise. En activant IPQoS sur les serveurs d'application et les serveurs Web, vous pouvez contrôler le débit auquel chaque système IPQoS libère le trafic sortant. Si le routeur Diffserv est compatible, vous pouvez contrôler davantage le trafic entrant et sortant.

Les exemples du présent guide font appel ce scénario.

FIGURE 2-1 Systèmes IPQoS sur un segment de réseau

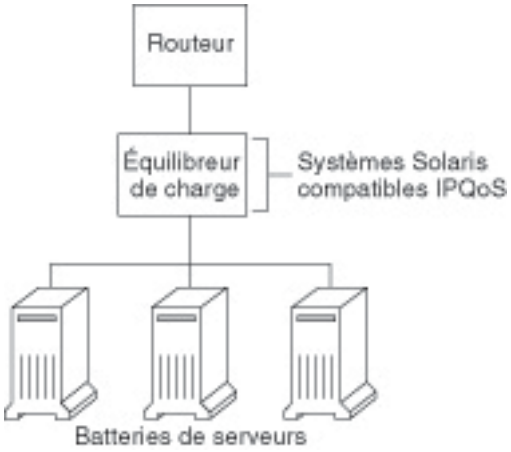


IPQoS sur une batterie de serveurs réseau

La figure suivante présente un réseau avec des batteries de serveurs hétérogènes. Dans cette configuration, le routeur est compatible avec Diffserv et peut, à ce titre, mettre en attente et

adapter le débit du trafic entrant et sortant. L'équilibreur de charge est également compatible avec Diffserv tandis que les batteries de serveurs reconnaissent le système IPQoS. L'équilibreur de charge peut fournir des fonctions de filtrage supplémentaires au-delà du routeur grâce à des sélecteurs de type ID utilisateur et ID projet. Ces sélecteurs sont inclus dans les données d'application

FIGURE 2-2 Réseau de batteries de serveurs compatibles IPQoS

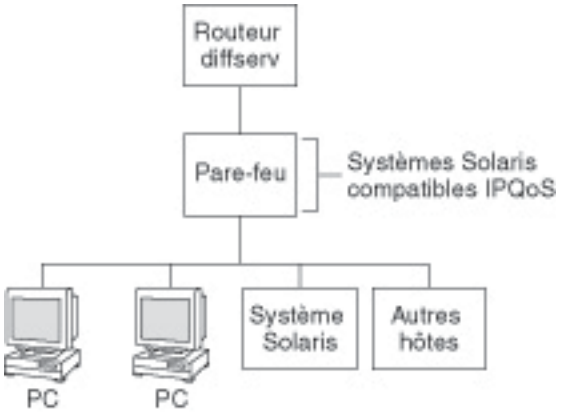


Ce scénario illustre un contrôle des flux et une transmission du trafic en mesure de gérer une éventuelle congestion du réseau local. Il interdit également au trafic sortant des batteries des serveurs d'encombrer d'autres sections du réseau intranet.

IPQoS sur un pare-feu

La figure suivante montre un segment d'un réseau d'entreprise protégé contre les autres segments au moyen d'un pare-feu. Dans l'exemple illustré, le trafic passe par le routeur compatible Diffserv où les paquets sont filtrés et mis en attente. Tout le trafic entrant, transmis par le routeur, transite alors par le pare-feu IPQoS. Pour utiliser IPQoS, le pare-feu ne doit pas passer outre la pile de transmission IP.

FIGURE 2-3 Réseau protégé par un pare-feu compatible IPQoS



La stratégie de sécurité du pare-feu détermine si le trafic entrant est autorisé à entrer ou à sortir du réseau interne. La stratégie QoS contrôle les niveaux de service applicables au trafic entrant ayant traversé le pare-feu. Selon la stratégie QoS retenue, le trafic sortant peut également être associé à un comportement de transmission particulier.

Planification de la stratégie de qualité de service

Lorsque vous planifiez une stratégie de qualité de service (QoS), vous devez examiner et classer les services que le réseau fournit, puis leur donner un ordre de priorité. Vous devez également évaluer la quantité de bande passante disponible de manière à déterminer le débit de chaque classe de trafic arrivant sur le réseau.

Aides à la planification de la stratégie QoS

Rassemblez les informations pour la planification de la stratégie dans un format prenant en compte les informations nécessaires pour le fichier de configuration IPQoS. Par exemple, servez-vous du modèle suivant pour énumérer les catégories principales d'information à intégrer au fichier de configuration IPQoS.

TABLEAU 2-1 Modèle de planification QoS

Class (Classe)	PRIORITY	Filtrer	Sélecteur	Débit	Retransmission	Comptabilisation
Classe 1	1	Filtre1	Sélecteur 1	Débits de l'indicateur	Niveau de priorité du marqueur	Requiert des statistiques

Class (Classe)	PRIORITY	Filtrer	Sélecteur	Débit	Retransmission	Comptabilisation
		Filtre 3	Sélecteur 2	selon le type de mesure		de comptabilisation des flux
Classe 1	1	Filtre 2	Sélecteur 1 Sélecteur 2	SO	SO	SO
Classe 2	2	Filtre1	Sélecteur 1 Sélecteur 2	Débits de l'indicateur selon le type de mesure	Niveau de priorité du marqueur	Requiert des statistiques de comptabilisation des flux
Classe 2	2	Filtre 2	Sélecteur 1 Sélecteur 2	SO	SO	SO

Il est possible de diviser chaque catégorie principale pour définir encore plus précisément la stratégie QoS. Les sections suivantes indiquent comment obtenir des informations sur les catégories du modèle.

Liste de tâches pour la planification de la stratégie QoS

Cette liste de tâches répertorie les principales tâches de planification d'une stratégie QoS et renvoie vers les procédures permettant d'effectuer chaque tâche.

Tâche	Description	Pour obtenir des instructions
1. Etablissement de la topologie du réseau pour qu'il prenne en charge IPQoS.	Identifiez les hôtes et les routeurs du réseau de manière à fournir des services différenciés.	“Préparation d'un réseau pour IPQOS” à la page 31
2. Définition des classes dans lesquelles les services du réseau doivent être répartis.	Examinez les types de service et les niveaux de service offerts par votre site et déterminez à quelles classes de trafic discret les services appartiennent.	“Définition des classes de votre stratégie QoS” à la page 31
3. Définition des filtres pour les classes.	Déterminez les méthodes les plus adaptées pour isoler le trafic d'une classe particulière par rapport au flux du trafic réseau.	“Définition de filtres dans la stratégie QoS” à la page 33
4. Définition des débits de contrôle de flux visant à mesurer le trafic	Déterminez les débits acceptables pour chaque classe de trafic.	“Planification du contrôle de flux” à la page 34

Tâche	Description	Pour obtenir des instructions
lorsque les paquets quittent le système IPQoS.		
5. Définition des valeurs DSCP ou les valeurs dont la priorité est définie par l'utilisateur à appliquer à la stratégie QoS.	Mettez en place un plan et déterminez le comportement de transmission assigné à un flux de trafic si le flux est géré par le routeur ou le commutateur.	“Planification du comportement de transfert” à la page 36
6. Le cas échéant, définition d'un plan de contrôle statistique concernant les flux de trafic sur le réseau.	Analysez les classes de trafic pour identifier les flux à contrôler à des fins comptables ou statistiques.	“Planification de la comptabilisation du flux” à la page 38

Remarque - Cette section décrit la planification de la stratégie QoS d'un système IPQoS. Pour planifier la stratégie QoS d'un routeur Diffserv, consultez la documentation du routeur ainsi que le site Web du fabricant.

Préparation d'un réseau pour IPQOS

La liste des tâches générales de planification à effectuer avant de créer la stratégie QoS sont les suivantes :

1. Examinez la topologie du réseau. Elaborez ensuite une stratégie associant les systèmes IPQoS et les routeurs Diffserv. Pour consulter des exemples de topologie, reportez-vous à la section “Planification de la topologie de réseau Diffserv” à la page 26.
2. Identifiez les hôtes de la topologie qui nécessitent IPQoS ou qui sont susceptibles d'être intéressés par le service IPQoS.
3. Définissez parmi les systèmes compatibles IPQoS ceux qui peuvent recourir à la même stratégie QoS.

   Si, par exemple, vous envisagez d'activer IPQoS sur tous les hôtes du réseau, identifiez ceux qui peuvent utiliser une même stratégie QoS. Chaque système IPQoS doit posséder une stratégie QoS locale. Celle-ci est implémentée dans le fichier de configuration IPQoS associé. Cependant, il est possible de créer un fichier de configuration IPQoS exploitable par une large gamme de systèmes. Il suffit alors de copier le fichier de configuration dans chaque système partageant les mêmes exigences en matière de stratégie QoS.
4. Evaluez et effectuez toutes les tâches de planification requises par le routeur Diffserv sur votre réseau. Reportez-vous à la documentation du routeur et au site Web du fabricant pour plus de détails.

Définition des classes de votre stratégie QoS

La première étape de la définition de la stratégie QoS consiste à organiser les flux de trafic en plusieurs classes. Vous n'avez pas besoin de créer des classes pour chaque type de trafic

sur un réseau Diffserv. De plus, selon la topologie du réseau, vous pouvez être amené à créer une stratégie QoS différente pour chaque système compatible IPQoS. Pour des informations générales sur les classes, reportez-vous à la section “Classes IPQoS” à la page 16.

Avant la définition des classes, vous devez déterminer les systèmes de votre réseau qui sont compatibles IPQoS comme indiqué dans la section “Préparation d'un réseau pour IPQOS” à la page 31.

1. Créez un tableau de planification QoS pour organiser les informations de la stratégie QoS, tel qu'indiqué dans le Tableau 2-1, “Modèle de planification QoS”
2. Effectuez les étapes restantes pour chaque stratégie QoS figurant sur le réseau.
3. Définissez les classes à utiliser dans la stratégie QoS.

   Pour des directives sur l'analyse du trafic réseau en vue d'éventuelles définitions de classe, reportez-vous à la section “Utilisation des classes de service pour hiérarchiser le trafic” à la page 13.
4. Dressez la liste des classes dans la planification QoS.
5. Attribuez un niveau de priorité à chacune des classes.

   Par exemple, le niveau de priorité 1 représente la classe dotée de la priorité la plus élevée. Définissez les priorités suivantes en ordre décroissant pour les autres classes. Ce niveau de priorité est utilisé à des fins organisationnelles uniquement. Vous pouvez attribuer une même priorité à plusieurs classes si cela convient à la stratégie QoS.

   Outre l'attribution d'un tel comportement à une classe, il est également possible de définir, pour la classe, un sélecteur de priorité dans un filtre. Le sélecteur de priorité est actif sur l'hôte IPQoS seulement. Considérons plusieurs classes avec des débits et des valeurs DSCP (Differentiated Services Code Point) identiques qui se font concurrence au niveau de la bande passante lorsqu'ils sortent du système IPQoS. Le sélecteur de priorité de chaque classe permet de classer le niveau de service attribué aux classes dont les valeurs sont identiques.

   Lorsque vous avez terminé la définition des classes, vous pouvez passer à la définition des filtres pour chaque classe, comme expliqué à la section “Définition de filtres dans la stratégie QoS” à la page 33.

Définition de filtres

Les filtres créés permettent d'identifier les flux de paquets appartenant à une classe particulière. Chaque filtre contient des sélecteurs définissant les critères qui contribuent à l'évaluation d'un flux de paquet. Le système IPQoS utilise les critères des sélecteurs pour extraire les paquets à partir d'un flux de trafic. Le système IPQoS associe ensuite les paquets à une classe. Pour obtenir une présentation des filtres, reportez-vous à la section “Filtres IPQoS” à la page 16 à la page 16.

Veillez à ne pas utiliser plus de sélecteurs que nécessaire pour extraire les paquets d'une classe. En effet plus le nombre de sélecteurs est important, plus cela aura d'impact sur les performances IPQoS.

Le tableau suivant répertorie les sélecteurs les plus répandus. Les cinq premiers sélecteurs représentent l'uplet à 5 attributs IPQoS dont le système IPQoS se sert pour identifier les paquets sous forme de membres d'un flux. Pour obtenir la liste complète des sélecteurs, reportez-vous au Tableau 6-1, “Sélecteurs de filtre pour le classificateur IPQoS”.

TABLEAU 2-2 Sélecteurs IPQoS communs

Name ;	Définition
`saddr`	Adresse source.
`daddr`	Adresse de destination.
`sport`	Numéro de port source. Vous pouvez utiliser un numéro de port connu comme indiqué dans `/etc/services` ou un numéro de port défini par l'utilisateur.
`dport`	Numéro de port de destination.
`protocol`	Numéro de protocole IP ou nom du protocol attribué au type de flux de trafic dans le fichier `/etc/protocols`.
`ip_version`	L'adressage style à utiliser. il s'agit d'IPv4 (valeur par défaut) ou IPv6.
`dsfield`	Contenu du champ DS, c'est-à-dire la valeur DSCP. Servez-vous de ce sélecteur pour extraire les paquets entrants déjà signalés par une valeur DSCP.
`priority`	Niveau de priorité attribué à la classe. Pour plus d'informations, reportez-vous à la section “Définition des classes de votre stratégie QoS” à la page 31.
`user`	Identifiant utilisateur UNIX ou nom de l'utilisateur à l'exécution de l'application de niveau supérieur.
`projid`	ID de projet utilisé à l'exécution de l'application de niveau supérieur.
`direction`	Direction du flux de trafic. Les valeurs acceptables sont `LOCAL_IN`,`LOCAL_OUT`, `FWD_IN` ou `FWD_OUT`.

▼ Définition de filtres dans la stratégie QoS

Avant de commencer

Avant de pouvoir définir des filtres, vous devez définir les classes de votre stratégie QoS. Pour plus d'informations, reportez-vous à la section “Définition des classes de votre stratégie QoS” à la page 31 à la page 29.

1. **Créez au moins un filtre pour chaque classe dans le tableau de planification QoS.**

   Envisagez de créer des filtres indépendants pour le trafic entrant et le trafic sortant de chaque classe, si besoin est. Par exemple, intégrez un filtre `ftp-in` et un filtre `ftp-out` à la stratégie QoS d'un serveur FTP compatible IPQoS. Vous pouvez ensuite définir le sélecteur `direction` qui convient en plus des sélecteurs de base.

2. **Définissez au moins un sélecteur pour chaque filtre au sein d'une classe.**

   Utilisez le tableau de planification QoS pour assurer le suivi de la les filtres des classes définies.

Exemple 2-1 Définition des filtres pour le trafic FTP

L'exemple ci-dessous illustre comment définir un filtre pour le trafic FTP sortant.

Class (Classe)	PRIORITY	Filtres	Sélecteurs

`ftp-traffic`	4	`ftp-out`	`saddr 10.190.17.44`
			`daddr 10.100.10.53`
			`sport 21`
			`direction LOCAL_OUT`

Planification du contrôle des flux

Le contrôle de flux implique de mesurer les flux de trafic pour une classe, puis de libérer les paquets sur le réseau à un débit défini. Lorsque vous planifiez le contrôle de flux, vous définissez les paramètres à appliquer aux modules de mesure IPQoS. Les compteurs déterminent le débit auquel le trafic est diffusé sur le réseau. Pour une présentation des modules de mesure, reportez-vous à la section “Présentation des compteurs (`tokenmt` et `tswtclmt`)” à la page 17.

Le trafic est généralement mesuré pour les raisons suivantes :

- Un accord de niveau de service garantit aux paquets de cette classe un service supérieur ou inférieur lorsque le réseau est fortement sollicité.
- Une classe dotée d'une priorité moindre aura tendance à submerger le réseau.

Les fonctions de marquage et de mesure permettent de fournir à ces classes des services différenciés et une gestion de la bande passante.

▼ Planification du contrôle de flux

Avant de commencer Avant de planifier le contrôle de flux, vous devez avoir défini les filtres et les sélecteurs comme décrit dans la section “Définition de filtres dans la stratégie QoS” à la page 33

1. **Déterminez la bande passante maximum pour votre réseau.**
2. **Passer en revue les contrats de niveau de service gérés par votre réseau et d'identifier les clients et le type de service assuré.**
   Pour garantir un niveau de service donné, il peut être indispensable de contrôler certaines classes de trafic générées par le client.
3. **Examinez la liste des classes pour déterminer si d'autres classes, outre celles qui sont associées aux contrats de niveau de service, doivent faire l'objet de mesures.**

Supposons par exemple que le système IPQoS exécute une application générant un niveau de trafic élevé. Après avoir établi une classification du trafic de l'application, évaluez les flux de manière à vérifier le débit auquel les paquets du flux arrivent sur le réseau.

Remarque - Il n'est pas utile de quantifier toutes les classes.

---

4. **Dans chaque classe, déterminez les filtres en rapport avec un trafic devant faire l'objet d'un contrôle de flux. Affinez ensuite la liste des classes nécessitant des opérations de mesure.**
   Lorsque les classes sont dotées de plusieurs filtres, il se peut que seul un filtre exige d'être contrôlé. Par exemple, si vous définissez des filtres pour le trafic entrant et le trafic sortant d'une classe donnée, vous pouvez établir que seul trafic d'une direction exige un contrôle de flux.

5. **Choisissez un module de mesure pour chaque classe à traiter et ajoutez le nom du module à la colonne de mesure dans le tableau de planification de qualité de service (QoS).**

6. **Ajoutez les débits des classes à mesurer dans la table de planification.**

   Si vous utilisez le module `tokenmt`, définissez les débits en bits par seconde suivants :

   - Débit garanti
   - Débit de pointe

   Si ces débits suffisent à mesurer une classe donnée, contentez-vous de spécifier le débit garanti et la taille de rafale garantie pour le module `tokenmt`.

   Si nécessaire, vous pouvez également définir les débits suivants :

   - Taille de rafale garantie
   - Taille de rafale de pointe

   Pour la définition complète des débits `tokenmt`, reportez-vous à la section “Configuration du `tokenmt` en tant que compteur à débit double” à la page 91. Vous trouverez également plus d'informations dans la page de manuel `tokenmt`(7ipp).
   Si vous recourez au module `tswtclmt`, il est nécessaire de définir les débits (en bits par seconde) suivants.

   - Débit garanti
   - Débit de pointe

   Vous pouvez aussi paramétrer la taille de la fenêtre en millisecondes. Ces débits sont définis à la section “Module de mesure `tswtclmt`” à la page 92 et à la page de manuel `tswtclmt`(7ipp).

7. **Ajoutez les résultats de conformité du trafic vers le tableau de planification avec compteur.**

Les résultats des deux modules de mesure s'affichent en vert, en rouge et en orange. Les résultats des opérations de mesure sont expliqués en détail dans la section “Module de mesure” à la page 89.

Vous devez préciser l'action à entreprendre lorsque le trafic se conforme ou ne se conforme pas au débit garanti. La plupart du temps, cette action consiste à marquer l'en-tête du paquet par un comportement appelé PHB (per-hop behavior). Lorsque le trafic est vert, l'action autorisée peut être de continuer le traitement des flux de trafic tant que ces derniers ne dépassent pas le contrat de trafic. Une autre action possible peut être de rejeter les paquets de la classe si les flux sont supérieurs au débit de pointe.

Exemple 2-2 Définition des compteurs

L'exemple suivant affiche les entrées d'une classe de trafic de messagerie électronique. Le réseau sur lequel se trouve le système IPQoS dispose d'une bande passante totale de 100 Mbits/sec, soit 10 millions de bits par seconde. La stratégie QoS assigne une priorité basse à la classe du courrier électronique. Cette classe obtient également le traitement « au mieux ».

Class (Classe)	PRIORITY	Filtrer	Sélecteur	Débit
email	8	mail_in	daddr10.50.50.5 dport imap direction LOCAL_IN	
email	8	mail_out	saddr10.50.50.5 sport imap direction LOCAL_OUT	mesure=tokenmt débit garanti=5000000 taille de rafale garantie =5000000 débit de pointe =10000000 taille de rafale de pointe=1000000 niveau de priorité vert=poursuivre le traitement niveau de priorité orange=signaliser par un PHB orange niveau de priorité rouge=rejeter

Planification du comportement de transfert

Le comportement de transmission détermine la priorité ainsi que le niveau de priorité des flux de trafic qui vont être transmis au réseau. Vous avez le choix entre deux comportements principaux : hiérarchiser les flux d'une classe par rapport à d'autres classes de trafic ou rejeter l'intégralité des flux.

Le modèle Diffserv utilise un marqueur pour assigner le comportement de transmission choisi aux flux de trafic. IPQoS comporte les deux modules de marquage suivants.

Notez que les suggestions de cette section se rapportent spécifiquement aux paquets IP. Si votre système IPQoS comprend un dispositif VLAN, vous pouvez utiliser le marqueur `dlcosmk` pour identifier certains comportements de transmission associés aux datagrammes. Pour plus d'informations, reportez-vous à la section “Utilisation du marqueur `dlcosmk` avec les périphériques VLAN” à la page 95.

Pour définir la priorité d'un trafic IP, vous devez attribuer un DSCP à chaque paquet. Le marqueur `dscpmk` code le champ DS du paquet à l'aide d'un DSCP. Vous choisissez le DSCP pour une classe dans un groupe de points de codes connus associés au type de comportement. Ces points de codes correspondent à 46 (101110) pour le PHB de classe EF et une plage de points de codes pour le PHB de classe AF. Pour des informations générales sur le DSCP et la transmission, reportez-vous à la section “Trafic sur un réseau compatible IPQoS” à la page 20.

▼ Planification du comportement de transmission

Avant de commencer

Avant de déterminer le comportement de transmission, vous devez avoir défini les classes et les filtres de la stratégie QoS. Même si vous combinez généralement les opérations de mesure et de marquage du trafic à contrôler, le marquage seul permet de définir un comportement de transmission.

1. **Vérifiez les classes créées jusqu'à présent, ainsi que les priorités assignées à chacune d'entre elles.**

   Il n'est pas utile de marquer toutes les classes de trafic.

2. **Attribuez le PHB EF (expedited forwarding, traitement accéléré) à la classe avec la priorité la plus élevée.**

   Le PHB EF garantit que les paquets marqués EF DSCP 46 (101110) sont diffusés sur le réseau avant les paquets de classe AF. Réservez le PHB EF pour le trafic prioritaire. Pour plus d'informations sur EF, reportez-vous à la section “PHB Expedited Forwarding (EF) (traitement accéléré)” à la page 94.

3. **Attribuez des comportements de routeurs aux classes dont le trafic doit être mesuré.**

4. **Définissez des points de codes DS pour les autres classes conformément aux priorités associées aux classes.**

Exemple 2-3 Stratégie QoS pour une application de jeu

Le tableau suivant présente une partie d'une stratégie QoS. Cette stratégie définit une classe pour un jeu populaire générant un niveau important de trafic.

Class (Classe)	PRIORITY	Filtrer	Sélecteur	Débit	Transmission ?
`games_app`	9	`games_in`	`sport 6080`	SO	SO
`games_app`	9	`games_out`	`dport 6081`	mesure=`tokenmt` débit garanti= 5000000 taille de rafale garantie =5000000 débit de pointe = 10000000 taille de rafale de pointe=15 000 000 niveau de priorité vert=poursuivre le traitement niveau de priorité orange=signaliser par un PHB orange niveau de priorité rouge=rejeter	vert = AF31 jaune = AF42 rouge = rejeter

Les comportements assignent des DSCP de priorité basse au trafic `games_app` conforme au débit garanti ou inférieur au débit de pointe. Si le trafic `games_app` dépasse le débit de pointe, la stratégie QoS indique que les paquets issus du trafic `games_app` doivent être ignorés. Le Tableau 6-2, “Points de code Assured Forwarding” dresse la liste de tous les points de codes AF.

Planification de la comptabilisation du flux

Faites appel au module `flowacct` IPQoS pour effectuer le suivi des flux de trafic à des fins de facturation et de gestion du réseau. Votre stratégie QoS doit inclure une comptabilisation des flux dans les circonstances suivantes :

- Votre entreprise offre des accords de niveaux de services à ses clients.

  Examinez les contrats de niveau de service pour déterminer les types de trafic réseau que l'entreprise veut facturer à ces clients. Passez ensuite en revue votre stratégie QoS pour identifier les classes de trafic à facturer.
- Vous disposez d'applications devant faire l'objet d'une surveillance ou d'un test pour pallier des éventuels problèmes liés au réseau.

  Vous pouvez envisager d'utiliser la comptabilisation des flux de manière à observer le comportement de ces applications. Examinez la stratégie QoS pour identifier les classes assignées au trafic et qui nécessitent un contrôle.

Signalez par la lettre O, dans la colonne de comptabilisation des flux, chaque classe nécessitant une comptabilisation dans la table de planification QoS.

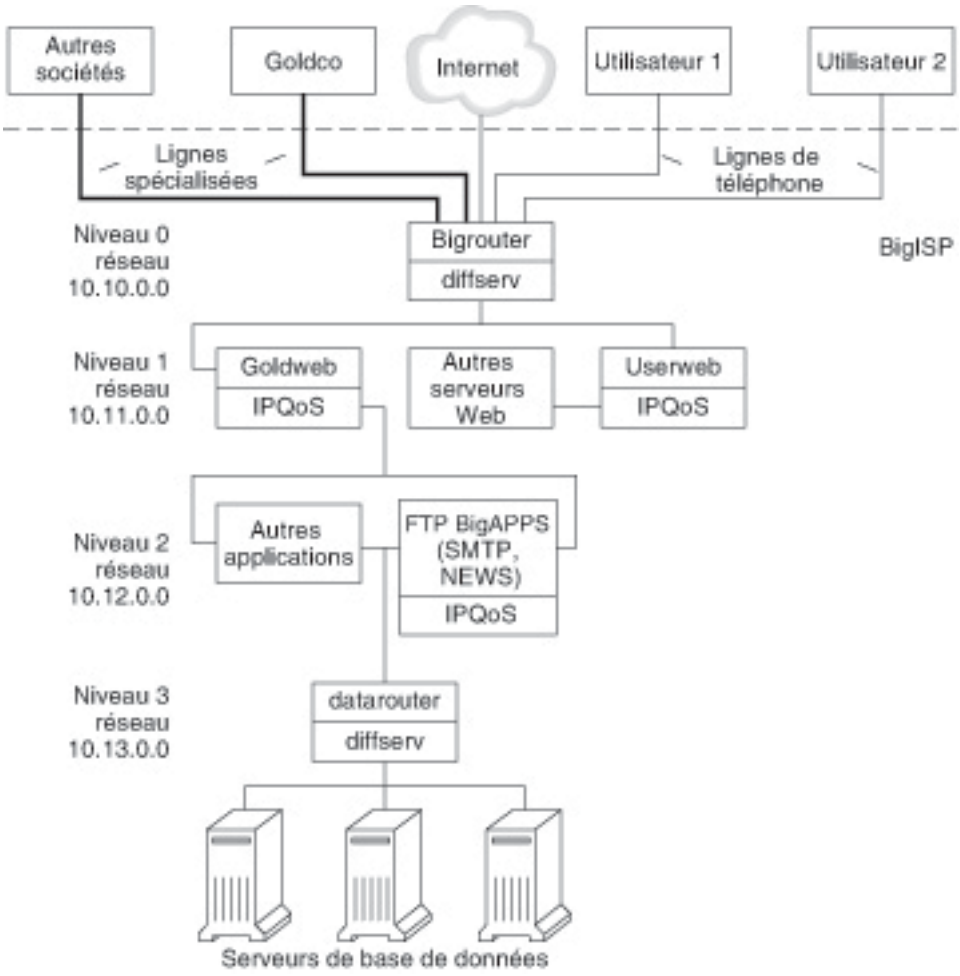
Présentation d'un exemple de configuration IPQoS

IPQOS cette section présente l'exemple qui est utilisée dans la configuration les tâches des autres chapitres de ce guide. L'exemple fait état d'une solution de services différenciés mise en place pour l'intranet public de BigISP, fournisseur de services fictif. BigISP offre des services à des grandes entreprises qui ont accès à BigISP par le biais de lignes spécialisées. Les utilisateurs qui se connectent via des modems peuvent également acheter des services auprès de BigISP.

Topologie IPQoS

La figure suivante illustre la topologie du réseau exploitée par l'intranet public de BigISP.

FIGURE 2-4 Exemple de topologie IPQoS



BigISP a les quatre niveaux suivants dans son intranet public :

- **Niveau 0** : le réseau`10.10.0.0` inclut un routeur Diffserv étendu appelé `Bigrouter` possédant des interfaces externes et internes. Plusieurs sociétés, notamment une grande organisation dénommée Goldco, a loué des services à lignes spécialisées aboutissant au `Bigrouter`. Le niveau 0 gère également des particuliers qui communiquent via les lignes téléphoniques ou le réseau RNIS.
- **Niveau 1** : le réseau `10.11.0.0` fournit des services Web. Le serveur `Goldweb` héberge le site Web de Goldco que ce dernier a acquis auprès de BigISP dans le cadre du service

premium. Le serveur `Userweb` héberge des sites Web de taille réduite achetés par des particuliers. Les sites `Goldweb` et `Userweb` sont compatibles IPQoS.

- **Niveau 2** : le réseau `10.12.0.0` met des applications à la disposition de l'ensemble de ses clients. Le serveur d'applications `BigAPPS` est compatible IPQoS. `BigAPPS` fournit des services de type SMTP, actualités et FTP.
- **Niveau 3** : le réseau `10.13.0.0` héberge des serveurs de bases de données de grande taille. L'accès au niveau 3 est contrôlé par `datarouter` (routeur Diffserv).

♦ ♦ ♦ CHAPITRE 3

Tâches pour la création du fichier de configuration IPQoS

Ce chapitre décrit la procédure de création du fichier de configuration IPQoS, `/etc/inet/ipqosinit.conf`. Les thèmes ci-dessous sont abordés :

- “Définition d'une stratégie QoS liste des tâches” à la page 43
- “Outils de création d'une stratégie QoS” à la page 44
- “Création de fichiers de configuration IPQoS pour les serveurs Web” à la page 45
- “Création d'un fichier de configuration pour un serveur d'application” à la page 61
- “Fourniture de services différenciés sur un routeur” à la page 71

Ce chapitre suppose que vous ayez préalablement défini une stratégie QoS complète et que vous soyez prêt à l'appliquer comme base du fichier de configuration IPQoS. Pour obtenir des instructions sur la planification de la stratégie QoS, reportez-vous à la section “Planification de la stratégie de qualité de service” à la page 29.

Remarque - La fonction IPQoS risque d'être supprimée dans une version ultérieure. Utilisez à sa place les commandes `dladm`, `flowadm` ainsi que les commandes associées, qui assurent des fonctions de contrôle des ressources de bande passante similaires. Pour plus d'informations, reportez-vous au manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Définition d'une stratégie QoS liste des tâches

Cette liste répertorie les tâches IPQoS d'ordre général nécessaires à la création d'un fichier de configuration et les liens vers les sections décrivant les étapes à suivre pour effectuer ces tâches.

Tâche	Description	Pour obtenir des instructions
1. Planification de la configuration de votre réseau IPQoS.	Déterminez les systèmes sur le réseau local qui doivent être activés pour IPQoS.	“Préparation d'un réseau pour IPQOS” à la page 31

Tâche	Description	Pour obtenir des instructions
2. Planification de la stratégie QoS pour les systèmes IPQoS sur votre réseau.	Déterminez les différentes classes de service pour les flux de trafic. Déterminez ensuite les flux nécessitant une gestion du trafic.	“Planification de la stratégie de qualité de service” à la page 29
3. Création du fichier de configuration IPQoS et définition son action initiale.	Créez le fichier IPQoS, appelez le classificateur IP et définissez une classe de traitement.	“Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 47
4. Ajoutez les filtres qui définissent le trafic sélectionné et organisé en une classe.	Créez les filtres d'une classe.	“Définition des filtres dans le fichier de configuration IPQoS” à la page 50
5. Créez des classes et des filtres supplémentaires pour le traitement par le classificateur IP.	Ajoutez d'autres classes et filtres au fichier de configuration IPQoS.	“Création d'un fichier de configuration IPQoS pour un serveur Web au mieux” à la page 58
6. Si la stratégie QoS fait appel au contrôle de flux, spécifiez les débits de contrôle de flux ainsi que les niveaux de conformité par rapport au compteur.	Ajoutez une instruction `action` avec des paramètres visant à configurer les modules de mesure.	“Configuration du contrôle de flux dans le fichier de configuration IPQoS” à la page 68
7. Si la stratégie QoS fait intervenir des comportements différenciés, définissez le mode de transmission des différentes classes de service.	Ajoutez une instruction `action` avec des paramètres visant à configurer le marqueur.	“Définition de la transmission du trafic dans le fichier de configuration IPQoS” à la page 52
8. Si la stratégie QoS implique la collecte de statistiques relatives aux flux de trafic, définissez la manière dont les données sont rassemblées.	Ajoutez une instruction `action` aux paramètres visant à configurer le module de comptabilisation de flux.	“Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS” à la page 56
9. Ajoutez le contenu d'un fichier de configuration IPQoS spécifié dans le module du noyau qui convient.	Appliquez le fichier de configuration IPQoS.	“Démarrage du service `ipqos`” à la page 74
10. Si les fichiers de configuration IPQoS du réseau définissent les comportements de transfert, ajoutez les DSCP obtenus dans les fichiers d'ordonnancement appropriés sur le routeur.	Configurez les comportements de transfert dans les fichiers du routeur.	“Fourniture de services différenciés sur un routeur” à la page 71

Outils de création d'une stratégie QoS

La stratégie QoS de votre réseau se trouve dans le fichier de configuration IPQoS, `/etc/inet/ipqosinit.conf`. Vous créez ce fichier de configuration dans un éditeur de texte. Ensuite, vous démarrez le service `svc:/network/ipqos` qui exécute la commande `ipqosconf`. La stratégie est ensuite écrite dans le système IPQoS du noyau. Pour des informations détaillées sur la commande `ipqosconf`, reportez-vous à la page de manuel `ipqosconf`(1M). L'Exemple 6-3, “Syntaxe du fichier de configuration IPQoS” indique la syntaxe complète du fichier de configuration IPQoS.

Fichier de configuration IPQoS standard

Le fichie rde IPQoS consiste en une arborescence d'instructions `action` chargée d'implémenter la stratégie QoS, définie à la section “Planification de la stratégie de qualité de service” à la page 29. Le fichier de configuration IPQoS permet de configurer les modules IPQoS. Chaque instruction d'action contient un jeu de *classes*, de *filtres* ou de *paramètres* à traiter par le module appelé dans l'instruction d'action.

Les tâches décrites dans ce chapitre expliquent comment créer un fichier de configuration IPQoS pour trois systèmes compatibles IPQoS. Ces systèmes font partie de la topologie du réseau de l'entreprise BigISP, présentée à la Figure 2-4, “Exemple de topologie IPQoS”.

- `Goldweb` : serveur Web hébergeant les sites Web de clients ayant acquis des contrats de niveau de service de type premium
- `Userweb` : serveur Web moins puissant hébergeant des sites web personnels pour des usagers domestiques qui ont souscrit à des contrats de niveau de service "au mieux"
- `BigAPPS` – Serveur d'application délivrant des messages électroniques, des actualités sur le réseau et un service FTP aux clients des services Premium et au mieux

Ces trois fichiers de configuration illustrent les configurations IPQoS les plus courantes. Il est possible d'utiliser les fichiers d'exemple présentés à la section suivante comme modèle de votre propre implémentation IPQoS.

Création de fichiers de configuration IPQoS pour les serveurs Web

Cette section présente le fichier de configuration IPQoS et la procédure destinée à créer un fichier de configuration pour un serveur Web de type premium. Elle explique ensuite comment configurer un niveau de service complètement différent dans un autre fichier de configuration pour un serveur hébergeant des sites Web personnels. Les deux serveurs appartiennent au réseau illustré à la Figure 2-4, “Exemple de topologie IPQoS”.

Le fichier de configuration suivant définit les activités IPQoS du serveur `Goldweb`. Ce serveur héberge le site Web de Goldco, l'entreprise qui a acquis un contrat de niveau de service de niveau premium.

EXEMPLE 3-1 Fichier de configuration IPQoS pour un serveur Web premium

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
```

```
        global_stats TRUE
    }
    class {
        name goldweb
        next_action markAF11
        enable_stats FALSE
    }
    class {
        name video
        next_action markEF
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class goldweb
    }
    filter {
        name videoout
        sport videosrv
        direction LOCAL_OUT
        class video
    }
}
action {
    module dscpmk
    name markAF11
    params {
        global_stats FALSE
        dscp_map{0-63:10}
        next_action continue
    }
}
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
action {
    module flowacct
    name acct
    params {
        enable_stats TRUE
        timer 10000
        timeout 10000
        max_limit 2048
    }
}
```

Le fichier de configuration suivant définit les activités IPQoS sur `Userweb`. Ce serveur héberge des sites Web pour les accords de niveau de service à bas prix ou "au mieux". Ce niveau de service garantit le meilleur service susceptible d'être fourni après la gestion, par le système IPQoS, du trafic correspondant aux clients bénéficiant d'contrats de niveau de service plus onéreux.

EXEMPLE 3-2 Exemple de configuration pour un serveur Web "au mieux"

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name Userweb
        next_action markAF12
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class Userweb
   }
}
action {
    module dscpmk
    name markAF12
    params {
        global_stats FALSE
        dscp_map{0-63:12}
        next_action continue
    }
}
```

▼ Création du fichier de configuration IPQoS et définition des classes de trafic

Le fichier de configuration IPQoS doit être copié dans `/etc/inet/ipqosinit.conf` lorsque vous êtes prêt à l'utiliser. Si vous démarrez avec une nouvelle installation il est plus simple fichier de configuration pour modifier votre document provisoire à l'endroit qu'il serve à visualiser. Cette procédure génère le segment initial du fichier de configuration IPQoS présenté dans l'Exemple 3-1, “Fichier de configuration IPQoS pour un serveur Web premium”.

Remarque - Lors de la création du fichier de configuration IPQoS, veillez à commencer et à terminer chaque instruction `action` et chaque clause par des accolades ({ }). Pour plus de détails sur l'utilisation des accolades, reportez-vous à l'Exemple 3-1, “Fichier de configuration IPQoS pour un serveur Web premium”.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Connectez-vous au serveur Web premium.**

3. **Modifiez `/etc/inet/ipqosinit.conf`.**

4. **En tant que première ligne non commentée, insérez le numéro de version `fmt_version 1.0`.**

   Chaque fichier de configuration IPQoS doit commencer par cette ligne.

5. **Inérez l'instruction `action` initiale, qui configure le classificateur IP générique `ipgpc`.**

   L'action initiale marque le début de l'arborescence des instructions `action` composant le fichier de configuration IPQoS. Par exemple, le fichier de configuration commence par l'instruction `action` initiale destinée à appeler le classificateur `ipgpc`.

   ```
   fmt_version 1.0

   action {
       module ipgpc
       name ipgpc.classify
   ```

`fmt_version 1.0`	Marque le début du fichier de configuration IPQoS.
`action {`	Marque le début de l'instruction d'action.
`module ipgpc`	Configure le classificateur `ipgpc` en tant qu'action initiale du fichier de configuration.
`name ipgpc.classify`	Définit le nom de l'instruction `action` du classificateur qui doit toujours correspondre à `ipgpc.classify`.

   Pour plus d'informations sur les détails de la syntaxe des instructions `action`, reportez-vous à la section “Instruction `action`” à la page 101 et à la page de manuel `ipqosconf`(1M).

6. **Ajoutez une clause `params` avec le paramètre statistique `global_stats`.**

```
params {
          global_stats TRUE
   }
```

Le paramètre `global_stats TRUE` dans l'instruction `ipgpc.classify` permet de collecter les statistiques liées à cette action. `global_stats TRUE` permet de recueillir des statistiques par classe dès qu'une définition de clause de classe a la valeur `enable_stats TRUE`.

L'activation des statistiques a un impact sur les performances. Il est possible de recueillir des statistiques sur un nouveau fichier de configuration IPQoS pour vérifier qu'IPQoS fonctionne correctement. Par la suite, vous pouvez désactiver la collecte de statistiques en attribuant à l'argument `global_stats` la valeur `FALSE`.

Les statistiques générales ne représentent qu'un seul type de paramètre que vous pouvez définir dans une clause `params`. Pour plus d'informations sur la syntaxe et sur d'autres détails relatifs aux clauses `params`, reportez-vous à la section “Clause `params`” à la page 103 et à la page de manuel `ipqosconf`(1M).

7. Définissez une classe destinée à identifier le trafic lié au serveur premium.

```
class {
        name goldweb
        next_action markAF11
        enable_stats FALSE
    }
```

Cette instruction est appelée une *clause class*. Le contenu de la clause `class` est le suivant.

`name goldweb`	Crée la classe `goldweb` pour identifier le trafic rattaché au serveur `Goldweb`.
next_action markAF11	Donne l'instruction au module `ipgpc` de transmettre les paquets de la classe `goldweb` à l'instruction d'action `markAF11`. Cette instruction `markAF11` appelle le marqueur `dscpmk`.
enable_stats FALSE	Active le recueil de statistiques pour la classe `goldweb`. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques de cette classe sont désactivées.

Pour des informations détaillées sur la syntaxe de la clause `class`, reportez-vous à la section “Clause `class`” à la page 102 et à la page de manuel `ipqosconf`(1M).

8. Définissez une classe identifiant une application devant bénéficier de la priorité de transmission la plus haute.

```
class {
        name video
```

```
        next_action markEF
        enable_stats FALSE
    }
```

`name video`	Crée la classe `vidéo` destinée à identifier le trafic du flux vidéo sortant du serveur `Goldweb`.
`next_action markEF`	Donne l'instruction au module `ipgpc` de transmettre les paquets de la classe `video` à l'instruction `markEF` après traitement par `ipgpc`. L'instruction `markEF` appelle le marqueur `dscpmk`.
`enable_stats FALSE`	Active le recueil de statistiques pour la classe `video`. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, la collecte de statistiques pour cette classe est désactivée.

9. **Enregistrez les modifications apportées au fichier `/etc/inet/ipqosinit.conf`.**

   - **Si vous avez terminé d'apporter des modifications, démarrez le service `ipqos`.**

     Reportez-vous à “Démarrage du service `ipqos`” à la page 74 pour des instructions spécifiques sur le démarrage ou redémarrage du service.

   - **Si vous souhaitez continuer à apporter des modifications dans le fichier de configuration IPQoS, choisissez une autre tâche.**

     Reportez-vous à “Planification générale de la configuration IPQoS (liste de tâches)” à la page 25 pour une liste des autres modifications qui peuvent être nécessaires.

▼ Définition des filtres dans le fichier de configuration IPQoS

Avant de commencer

La procédure suppose que vous ayez déjà lancé la création du fichier et défini des classes. Elle poursuit la génération du fichier de configuration IPQoS créé à la section “Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 47.

Remarque - Lors de la création du fichier de configuration IPQoS, veillez à commencer et à terminer chaque clause `class` et chaque clause `filter` par des accolades ({ }). Pour plus de détails sur l'utilisation des accolades, reportez-vous à l'Exemple 3-1, “Fichier de configuration IPQoS pour un serveur Web premium”.

---

1. **Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Si le fichier de configuration IPQoS n'est pas ouvert, ouvrez-le .**

3. **Recherchez la fin de la dernière classe que vous avez définis.**

   Par exemple, sur le serveur IPQoS `Goldweb`, vous devez débuter après la clause `class` suivante :

```
class {
        name video
        next_action markEF
        enable_stats FALSE
    }
```

4. **Définissez une clause `filter` pour sélectionner le trafic sortant depuis le système IPQoS.**

```
filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class goldweb
}
```

`name webout`	Attribue le nom `webout` au filtre.
`sport 80`	Sélectionne le trafic par le port source 80, port habituel du trafic (Web) HTTP.
`direction LOCAL_OUT`	Affine la sélection du trafic sortant provenant du système local.
`class goldweb`	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `goldweb`.

   Pour des informations sur la syntaxe et d'autres détails sur la clause `filter` figurant dans le fichier de configuration IPQoS, reportez-vous à la section "Clause `filter`" à la page 103.

5. **Définissez une clause `filter` pour sélectionner le trafic de flux vidéo dans le système IPQoS.**

```
filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
}
```

`name videoout`	Attribue le nom `videoout` au filtre.
`sport videosrv`	Sélectionne le trafic par le port source `videosrv`, port précédemment défini pour les applications de flux vidéo du système.
`direction LOCAL_OUT`	Affine la sélection du trafic sortant provenant du système local.
`class video`	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `video`.

6. **Enregistrez les modifications apportées au fichier `/etc/inet/ipqosinit.conf`.**

   - **Si vous avez terminé d'apporter des modifications, démarrez le service `ipqos`.**

     Reportez-vous à “Démarrage du service `ipqos`” à la page 74 pour des instructions spécifiques sur le démarrage ou redémarrage du service.

   - **Si vous souhaitez continuer à apporter des modifications dans le fichier de configuration IPQoS, choisissez une autre tâche.**

     Reportez-vous à “Planification générale de la configuration IPQoS (liste de tâches)” à la page 25 pour une liste des autres modifications qui peuvent être nécessaires.

▼ Définition de la transmission du trafic dans le fichier de configuration IPQoS

Cette procédure indique comment définir le transfert du trafic en ajoutant des comportements par saut à une classe dans le fichier de configuration IPQoS.

Remarque - La procédure montre comment configurer la transmission du trafic à l'aide du module de marquage `dscpmk`. Pour plus d'informations sur la transmission du trafic sur des systèmes VLAN à l'aide du marqueur `dlclosmk`, reportez-vous à la section “Utilisation du marqueur `dlcosmk` avec les périphériques VLAN” à la page 95.

Avant de commencer

Cette procédure suppose que vous disposiez d'un fichier de configuration IPSQoS assorti de classes et de filtres définis. Elle poursuit la génération du fichier de configuration IPQoS de l'Exemple 3-1, “Fichier de configuration IPQoS pour un serveur Web premium”.

1. **Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Si le fichier de configuration IPQoS n'est pas déjà ouvert, ouvrez-le .**

3. **Recherchez la fin du dernier filtre défini.**

   Par exemple, sur le serveur IPQoS `Goldweb`, vous devez débuter après la clause `filtre` suivante dans le fichier de configuration :

```
filter {
        name videoout
        sport videosrv
        direction LOCAL_OUT
        class video
    }
}
```

   Etant donné que cette `clause` filter se trouve à la fin de l'instruction `action` du classificateur `ipgpc`, vous devez insérer deux accolades : une pour la fin du filtre et la deuxième pour la fin de l'instruction `action`.

4. **Appelez le marqueur à l'aide d'une instruction `action`.**

```
action {
    module dscpmk
    name markAF11
```

   `module dscpmk` — Appelle le module de marquage `dscpmk`.

   `name markAF11` — Attribue le nom `markAF11` à l'instruction `action`.

   La classe précédemment définie `goldweb` inclut une instruction `next_action markAF11`. Cette instruction envoie les flux de trafic vers l'instruction d'action `markAF11` à l'issue du traitement par le classificateur.

5. **Définit les actions du marqueur sur le flux de trafic.**

```
    params {
        global_stats FALSE
        dscp_map{0-63:10}
        next_action continue
    }
}
```

   `global_stats FALSE` — Active la collecte de statistiques pour l'instruction `action` du marqueur `markAF11`. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques ne sont pas recueillies.

`dscp_map{0–63:10}`	Attribue un DSCP égal à `10` aux en-têtes de paquets de la classe de trafic `goldweb` actuellement traitée par le marqueur.
`next_action continue`	Indique qu'aucun traitement supplémentaire n'est requis sur les paquets de la classe de trafic `goldweb` et que ces paquets peuvent revenir dans le flux réseau.

Un DSCP `10` donne pour instruction au marqueur d'attribuer la valeur décimale 10 (binaire 001010) à toutes les entrées de la structure `dscp`. Ce point de code signale que les paquets de la classe de trafic `goldweb` sont soumis au comportement AF11. AF11 garantit à tous les paquets de DSCP `10` un service haute priorité avec un taux de perte faible. Ainsi, le trafic sortant des client premium sur `Goldweb` bénéficie de la priorité la plus haute disponible pour le PHB Assured Forwarding (AF). Pour consulter le tableau des DSCP possibles pour AF, reportez-vous au Tableau 6-2, “Points de code Assured Forwarding”.

6. Démarrez une nouvelle instruction `action` de marqueur.

```
action {
    module dscpmk
    name markEF
```

`module dscpmk`	Appelle le module de marquage `dscpmk`.
`name markEF`	Attribue le nom `markEF` à l'instruction `action`.

7. Définissez les actions que le marqueur doit appliquer au flux de trafic.

```
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

`global_stats TRUE`	Active la collecte des statistiques sur une classe `video`, chargée de sélectionner les paquets de flux vidéo.
`dscp_map{0–63:46}`	Attribue un DSCP égal à `46` aux en-têtes de paquets de la classe de trafic `video` actuellement traitée par le marqueur.
`next_action acct`	Donne l'instruction au module `dscpmk` de transmettre les paquets de la classe `video` à l'instruction `action acct` après traitement par `dscpmk`. L'instruction `acct action` appelle le module `flowacct`.

Le DSCP `46` demande au module `dscpmk` d'attribuer la valeur décimale 46 (binaire 101110) à toutes les entrées de structure `dscp`, dans le champ DS. Ce point de code signale que les paquets de la classe de trafic `video` sont soumis au comportement EF.

Remarque - Le point de code recommandé est 46 (binaire 101110). D'autres DSCP assignent des PHB AF à un paquet.

Le PHB EF garantit aux paquets de DSCP `46` un traitement prioritaire par les systèmes compatibles IPQoS et Diffserv. Définir des flux pour les applications nécessite un service de priorité élevée conduisant logiquement à l'attribution de PHB de type EF dans la stratégie QoS. Pour plus de détails sur le PHB EF, reportez-vous à la section “PHB Expedited Forwarding (EF) (traitement accéléré)” à la page 94.

8. **Ajoutez les DSCP que vous venez de créer dans les fichiers appropriés sur le routeur Diffserv.**

   Pour plus d'informations, reportez-vous à la section “Fourniture de services différenciés sur un routeur” à la page 71.

9. **Enregistrez les modifications apportées au fichier `/etc/inet/ipqosinit.conf`.**

   - **Si vous avez terminé d'apporter des modifications, démarrez le service `ipqos`.**

     Reportez-vous à “Démarrage du service `ipqos`” à la page 74 pour des instructions spécifiques sur le démarrage ou redémarrage du service.

   - **Si vous souhaitez continuer à apporter des modifications dans le fichier de configuration IPQoS, choisissez une autre tâche.**

     Reportez-vous à “Planification générale de la configuration IPQoS (liste de tâches)” à la page 25 pour une liste des autres modifications qui peuvent être nécessaires.

Étapes suivantes

- Pour lancer la collecte de statistiques de comptabilisation des flux de trafic, reportez-vous à la section “Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS” à la page 56.
- Pour définir les comportements au niveau des modules de marquage, reportez-vous à la section “Définition de la transmission du trafic dans le fichier de configuration IPQoS” à la page 52.
- Pour définir les paramètres de contrôle des flux au niveau des modules de mesure, reportez-vous à la section “Configuration du contrôle de flux dans le fichier de configuration IPQoS” à la page 68.
- Pour activer le fichier de configuration IPQoS, reportez-vous à la section “Démarrage du service `ipqos`” à la page 74

- Pour définir des filtres supplémentaires, reportez-vous à la section “Définition des filtres dans le fichier de configuration IPQoS” à la page 50.
- Pour créer des classes pour les flux de trafic provenant d'applications, reportez-vous à la section “Configuration d'un fichier de configuration IPQoS pour un serveur d'application” à la page 63.

▼ Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS

Cette procédure indique la manière d'activer la comptabilisation pour une classe de trafic dans le fichier de configuration IPQoS. Elle précise comment définir la comptabilisation des flux pour la classe `video`, présentée à la section “Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 47. Cette classe sélectionne le trafic vidéo qui doit être facturé au client premium au titre du contrat de niveau de service contracté.

Avant de commencer La procédure suppose que vous possédiez un fichier de configuration IPQoS comportant des classes, des filtres, des actions de mesure, le cas échéant, et d'éventuelles actions de marquage. Elle poursuit la génération du fichier de configuration IPQoS de l'Exemple 3-1, “Fichier de configuration IPQoS pour un serveur Web premium”.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Si le fichier de configuration IPQoS n'est pas déjà ouvert, ouvrez-le .**

3. **Recherchez la fin de la dernière instruction `action` définie.**

   Par exemple, sur le serveur IPQoS `Goldweb`, vous devez débuter après l'instruction `markEF action` suivante dans le fichier de configuration, `/etc/inet/ipqosinit.conf`.

```
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

4. **Spécifiez une instruction `action` qui appelle la comptabilisation des flux.**

```
action {
```

```
    module flowacct
    name acct
```

`module flowacct` Invoque le module de comptabilisation des flux `flowacct`.

`name acct` Attribue le nom `acct` à l'instruction `action`.

5. **Définissez une clause `params` contrôler la comptabilisation de la classe de trafic.**

```
params {
        global_stats TRUE
        timer 10000
        timeout 10000
        max_limit 2048
        next_action continue
    }
}
```

`global_stats TRUE` Active la collecte des statistiques sur la classe `video`, chargée de sélectionner les paquets de flux vidéo.

`timer 10000` Spécifie la durée de l'intervalle, exprimé en millisecondes, lors de l'analyse de la table des flux afin de vérifier les flux dont le délai d'attente a expiré. Pour ce paramètre, l'intervalle correspond à 10 000 millisecondes.

`timeout 10000` Valeur du délai d'attente précise la taille minimale d'intervalle. Un flux arrive à expiration lorsque les paquets du flux n'apparaissent pas à l'issue de l'intervalle défini. Pour ce paramètre, les paquets parviennent à expiration au bout de 10 000 millisecondes.

`max_limit 2048` Définit le nombre maximum d'enregistrements de flux actifs dans la table des flux pour cette instance d'action.

`next_action continue` Indique qu'aucun traitement supplémentaire n'est requis sur les paquets de la classe de trafic `video` et que ces paquets peuvent revenir dans le flux réseau.

Le module `flowacct` collecte les informations statistiques sur les flux de paquet d'une classe particulière tant que la valeur `timeout` spécifiée n'est pas atteinte.

6. **Enregistrez les modifications apportées au fichier `/etc/inet/ipqosinit.conf`.**

- **Si vous avez terminé d'apporter des modifications, démarrez le service `ipqos`.**

  Reportez-vous à "Démarrage du service `ipqos`" à la page 74 pour des instructions spécifiques sur le démarrage ou redémarrage du service.

- **Si vous souhaitez continuer à apporter des modifications dans le fichier de configuration IPQoS, choisissez une autre tâche.**

  Reportez-vous à “Planification générale de la configuration IPQoS (liste de tâches)” à la page 25 pour une liste des autres modifications qui peuvent être nécessaires.

Création d'un fichier de configuration IPQoS pour un serveur Web au mieux

Le fichier de configuration IPQoS d'un serveur Web au mieux diffère légèrement du fichier de configuration IPQoS utilisé par un serveur Web de niveau premium. Cette procédure utilise le fichier de configuration de l'Exemple 3-2, “Exemple de configuration pour un serveur Web "au mieux"”.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Connectez-vous au serveur Web au mieux.**

3. **Produisez un nouveau fichier de configuration IPQoS suivi de l'extension `.qos`.**

```
fmt_version 1.0
action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
   }
```

   Le fichier doit commencer par l'instruction partielle `action` visant à appeler le classificateur `ipgpc`. En outre, l'instruction `action` possède une clause `params` pour activer le recueil de statistiques. Pour obtenir une explication de l'instruction `action`, reportez-vous à la section “Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 47.

4. **Définissez une classe identifiant le trafic en direction du serveur web au mieux.**

```
class {
        name userweb
        next_action markAF12
        enable_stats FALSE
    }
```

`name userweb`	Crée une classe appelée `userweb` pour la transmission du trafic Web émanant des utilisateurs.
`next_action markAF1`	Demande au module `ipgpc` de transmettre les paquets de la classe `userweb` à l'instruction `action markAF12` après traitement par `ipgpc`. L'instruction `action markAF12` appelle le module `dscpmk`.
`enable_stats FALSE`	Active le recueil de statistiques pour la classe `userweb`. Néanmoins, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, la collecte de statistiques ne se produit pas.

Pour obtenir une explication de la tâche de la clause `class`, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 47.

5. Définissez une clause `filter` pour sélectionner les flux de trafic pour la classe `userweb`.

```
    filter {
       name webout
       sport 80
       direction LOCAL_OUT
       class userweb
   }
}
```

`name webout`	Attribue le nom `webout` au filtre.
`sport 80`	Sélectionne le trafic par le port source 80, port habituel du trafic (Web) HTTP.
`direction LOCAL_OUT`	Affine la sélection du trafic sortant provenant du système local.
class userweb	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `userweb`.

Pour obtenir une explication de la tâche liée à la clause `filter`, reportez-vous à la section "Définition des filtres dans le fichier de configuration IPQoS" à la page 50.

6. Commencez l'instruction `action` en appelant le marqueur `dscpmk`.

```
action {
    module dscpmk
    name markAF12
```

`module dscpmk`	Appelle le module de marquage `dscpmk`.

`name markAF12` Attribue le nom `markAF12` à l'instruction `action`.

La classe précédemment définie `userweb` inclut une instruction `next_action markAF12`. Cette instruction envoie les flux de trafic vers l'instruction `action markAF12` à l'issue du traitement par le classificateur.

7. **Définissez les paramètres du marqueur pour le traitement du flux de trafic.**

```
    params {
        global_stats FALSE
        dscp_map{0-63:12}
        next_action continue
    }
}
```

`global_stats FALSE` Active la collecte de statistiques pour l'instruction `action` du marqueur `markAF12`. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques ne sont pas recueillies.

`dscp_map{0–63:12}` Attribue un DSCP égal à `12` aux en-têtes de paquets de la classe de trafic `userweb` actuellement traitée par le marqueur.

`next_action continue` Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic `userweb` et que ces paquets peuvent revenir dans le flux réseau.

Un DSCP `12` donne pour instruction au marqueur d'attribuer la valeur décimale 12 (binaire 001100) à toutes les entrées de la structure `dscp`. Ce point de code signale que les paquets de la classe de trafic `userweb` sont soumis au comportement AF12. AF12 garantit à tous les paquets de DSCP `12` un service haute priorité avec un taux de perte moyen.

8. **Enregistrez les modifications apportées au fichier `/etc/inet/ipqosinit.conf`.**

   - **Si vous avez terminé d'apporter des modifications, démarrez le service `ipqos`.**

     Reportez-vous à "Démarrage du service `ipqos`" à la page 74 pour des instructions spécifiques sur le démarrage ou redémarrage du service.

   - **Si vous souhaitez continuer à apporter des modifications dans le fichier de configuration IPQoS, choisissez une autre tâche.**

     Reportez-vous à "Planification générale de la configuration IPQoS (liste de tâches)" à la page 25 pour une liste des autres modifications qui peuvent être nécessaires.

Création d'un fichier de configuration pour un serveur d'application

Cette section décrit comment créer un fichier de configuration pour un serveur d'application délivrant des applications importantes aux clients. La procédure utilise le serveur `BigAPPS` de la Figure 2-4, “Exemple de topologie IPQoS” en guise d'exemple.

Le fichier de configuration suivant définit les activités IPQoS du serveur `BigAPPS`. Ce serveur héberge, à l'usage des clients, des données FTP, des messages électroniques (SMTP) ainsi que des informations sur le réseau (NNTP).

EXEMPLE 3-3 Exemple de fichier de configuration pour un serveur d'application

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        next_action meterftp
    }
    filter {
        name smtpout
        sport smtp
        class smtp
    }
    filter {
        name newsout
        sport nntp
        class news
    }
    filter {
        name ftpout
        sport ftp
        class ftp
    }
   filter {
```

```
        name ftpdata
        sport ftp-data
        class ftp
    }
}
action {
    module dscpmk
    name markAF13
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
action {
    module tokenmt
    name meterftp
    params {
        committed_rate 50000000
        committed_burst 50000000
        red_action_name AF31
        green_action_name markAF22
        global_stats TRUE
    }
}
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

▼ Configuration d'un fichier de configuration IPQoS pour un serveur d'application

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Connectez - vous au serveur d'applications IPQoS.**

3. **Produisez un nouveau fichier de configuration IPQoS suivi de l'extension `.qos`.**

4. **Insérez les phrases suivantes pour lancer l'instruction `action` visant à appeler le classificateur `ipgpc` :**

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
```

   Pour obtenir une explication de l'instruction `action` d'ouverture, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 47.

5. **Créez des classes pour sélectionner le trafic de trois applications situées sur le serveur BigAPPS.**

```
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        enable_stats TRUE
        next_action meterftp
    }
```

`name smtp` Crée une classe nommée `smtp` qui intègre les flux de trafic de messagerie électronique à gérer par l'application SMTP.

`enable_stats FALSE`	Active le recueil de statistiques pour la classe `smtp`. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques de cette classe ne sont pas recueillies.
`next_action markAF13`	Demande au module `ipgpc` de transmettre les paquets de la classe `smtp` à l'instruction `action markAF13` après traitement par `ipgpc`.
`name news`	Crée une classe nommée `news` qui intègre les flux d'informations sur le réseau à gérer par l'application NNTP.
`next_action markAF21`	Donne l'instruction au module `ipgpc` de transmettre les paquets de la classe `news` à l'instruction `markAF21` après traitement par `ipgpc`.
`name ftp`	Crée une classe nommée `ftp` qui traite le trafic sortant géré par l'application FTP.
`enable_stats TRUE`	Active le recueil de statistiques pour la classe `ftp`.
`next_action meterftp`	Demande au module `ipgpc` de transmettre les paquets de la classe `ftp` à l'instruction `action meterftp` après traitement par `ipgpc`.

Pour plus d'informations sur la définition des classes, reportez-vous à la section “Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 47.

6. **Définisse des clauses `filter` fin de sélectionner le trafic des classes définies à l'étape 2.**

```
filter {
    name smtpout
    sport smtp
    class smtp
}
filter {
    name newsout
    sport nntp
    class news
}
    filter {
    name ftpout
    sport ftp
    class ftp
}
    filter {
    name ftpdata
    sport ftp-data
    class ftp
```

```
    }
}
```

`name smtpout`	Attribue le nom `smtpout` au filtre.
`sport smtp`	Sélectionne le trafic transitant par le port source 25 représentant le port consacré à l'application `sendmail` (SMTP).
`class smtp`	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `smtp`.
`name newsout`	Attribue le nom `newsout` au filtre.
`sport nntp`	Sélectionne le trafic transitant par le port source `nntp`, couramment utilisé pour l'application d'informations réseau (NNTP).
`class news`	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `news`.
`name ftpout`	Attribue le nom `ftpout` au filtre.
`sport ftp`	Sélectionne les données de contrôle passant par le port source 21, port réservé au trafic FTP.
`name ftpdata`	Attribue le nom `ftpdata` au filtre.
`sport ftp-data`	Sélectionne les données de contrôle passant par le port source 20, port réservé au trafic de données FTP.
`class ftp`	Identifie la classe à laquelle les filtres `ftpout` et `ftpdata` appartiennent. Dans cet exemple, il s'agit de `ftp`.

7. **Enregistrez les modifications apportées au fichier `/etc/inet/ipqosinit.conf`.**

   - **Si vous avez terminé d'apporter des modifications, démarrez le service `ipqos`.**

     Reportez-vous à “Démarrage du service `ipqos`” à la page 74 pour des instructions spécifiques sur le démarrage ou redémarrage du service.

   - **Si vous souhaitez continuer à apporter des modifications dans le fichier de configuration IPQoS, choisissez une autre tâche.**

     Reportez-vous à “Planification générale de la configuration IPQoS (liste de tâches)” à la page 25 pour une liste des autres modifications qui peuvent être nécessaires.

Configuration de la transmission du trafic d'une application dans le fichier de configuration IPQoS

La procédure suivante indique comment configurer la transmission du trafic d'une application. Dans la procédure, vous définissez les comportements par saut pour les classes de trafic de l'application qui sont susceptibles d'avoir des niveaux de priorité inférieurs à ceux d'autres flux de trafic sur un réseau. La procédure poursuit la génération du fichier de configuration IPQoS de l'Exemple 3-3, “Exemple de fichier de configuration pour un serveur d'application”.

Avant de commencer Cette procédure suppose que vous disposiez d'un fichier de configuration IPSQoS assorti de classes et de filtres définis pour les applications à marquer.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Ouvrez `/etc/inet/ipqosinit.conf` et recherchez la fin de la dernière clause `filter`.**

   Dans `/etc/inet/ipqosinit.conf`, le filtre final est le suivant :

   ```
    filter {
           name ftpdata
           sport ftp-data
           class ftp
       }
   }
   ```

3. **Appelez le marqueur.**

   ```
   action {
       module dscpmk
       name markAF13
   ```

   `module dscpmk` Appelle le module de marquage `dscpmk`.

   `name markAF13` Attribue le nom `markAF13` à l'instruction `action`.

4. **Définissez le comportement par saut à signaler au niveau des flux de trafic de courriers électroniques.**

   ```
       params {
           global_stats FALSE
           dscp_map{0-63:14}
           next_action continue
       }
   }
   ```

`global_stats FALSE`	Active la collecte de statistiques pour l'instruction `action` `markAF13` du marqueur. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques ne sont pas recueillies.
`dscp_map{0–63:14}`	Attribue un DSCP égal à `14` aux en-têtes de paquets de la classe de trafic `smtp` actuellement traitée par le marqueur.
`next_action continue`	Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic `smtp`. Ces paquets peuvent alors revenir dans le flux du réseau.

Un DSCP `14` donne pour instruction au marqueur d'attribuer la valeur décimale 14 (binaire 001110) à toutes les entrées de la structure `dscp`. Le DSCP `14` définit le comportement AF13. Le marqueur signale les paquets de la classe de trafic `smtp` par le DSCP `14` dans le champ DS.

AF13 assigne à l'ensemble des paquets marqués d'un DSCP `14` un niveau de priorité élevé. Cependant, étant donné que AF13 garantit une priorité de classe 1, le routeur garantit une priorité élevée au trafic sortant des courriers électroniques dans la file d'attente. Pour une liste de points de code AF possibles, consultez le Tableau 6-2, “Points de code Assured Forwarding”.

5. Ajoutez une instruction `action` de marqueur pour définir un comportement pour le trafic des informations réseau :

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

`name markAF21`	Attribue le nom `markAF21` à l'instruction `action`.
`dscp_map{0–63:18}`	Attribue un DSCP égal à `18` aux en-têtes de paquets de la classe de trafic `nntp` actuellement traitée par le marqueur.

Le DSCP `18` donne pour instruction au marqueur d'attribuer la valeur décimale 18 (binaire 010010) à toutes les entrées de la structure `dscp`. Le DSCP `18` définit le comportement AF21. Le marqueur signale les paquets de la classe de trafic `news` par le DSCP `18` dans le champ DS.

AF21 garantit que tous les paquets avec un DSCP égal à `18` se voient attribuer un niveau de perte faible assorti d'une priorité de classe 2. Ainsi, les probabilités de perdre les données de trafic d'informations sur le réseau sont faibles.

6. **Enregistrez les modifications apportées au fichier `/etc/inet/ipqosinit.conf`.**

   - **Si vous avez terminé d'apporter des modifications, démarrez le service `ipqos`.**
     Reportez-vous à “Démarrage du service `ipqos`” à la page 74 pour des instructions spécifiques sur le démarrage ou redémarrage du service.

   - **Si vous souhaitez continuer à apporter des modifications dans le fichier de configuration IPQoS, choisissez une autre tâche.**
     Reportez-vous à “Planification générale de la configuration IPQoS (liste de tâches)” à la page 25 pour une liste des autres modifications qui peuvent être nécessaires.

Configuration du contrôle de flux dans le fichier de configuration IPQoS

Pour contrôler le débit selon lequel un flux de trafic est libéré sur le réseau, vous devez définir des paramètres de mesure. Vous pouvez utiliser un des deux modules de mesure, `tokenmt` ou `tswtclmt`, dans le fichier de configuration IPQoS.

La procédure suivante poursuit la génération du fichier de configuration IPQoS pour le serveur d'application de l'Exemple 3-3, “Exemple de fichier de configuration pour un serveur d'application”. Dans la procédure, vous pouvez configurer le compteur ainsi que deux actions du marqueur appelées par l'instruction `action` du module de mesure.

Avant de commencer La procédure suppose que vous ayez déjà défini une classe et un filtre pour l'application dont vous voulez contrôler le flux.

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Ouvrez `/etc/inet/ipqosinit.conf`-**
   Commencer à apporter des modifications après l'action du marqueur suivante :

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

3. **Créez une instruction `action` pour le compteur pour contrôler le flux de trafic de la classe `ftp`.**

```
action {
    module tokenmt
    name meterftp
```

`module tokenmt`	Appelle le module de mesure `tokenmt`.
`name meterftp`	Attribue le nom `meterftp` à l'instruction `action`.

4. **Ajoutez des paramètres pour configurer le débit du module de mesure.**

```
params {
       committed_rate 50000000
       committed_burst 50000000
```

`committed_rate 50000000`	Assigne une vitesse de transmission de 50 000 000 bps au trafic de la classe `ftp`.
`committed_burst 50000000`	Valide une taille de rafale de 50 000 000 bits pour le trafic de la classe `ftp`.

Pour une explication des paramètres `tokenmt`, reportez-vous à la section “Configuration du `tokenmt` en tant que compteur à débit double” à la page 91.

5. **Ajoutez des paramètres pour configurer les niveaux de priorité de conformité de trafic :**

```
    red_action markAF31
    green_action_name markAF22
    global_stats TRUE
    }
}
```

`red_action_name markAF31`	Indique que lorsque le flux de trafic de la classe `ftp` dépasse le débit garanti, les paquets sont envoyés vers l'instruction de marquage `action markAF31`.
`green_action_name markAF22`	Indique que le flux de trafic de la classe `ftp` est conforme au débit garanti, les paquets sont envoyés à l'instruction de l'action `markAF22`.
`global_stats TRUE`	Active le recueil de statistiques pour la classe `ftp`.

Pour plus d'informations sur la conformité du trafic, reportez-vous à la section “Module de mesure” à la page 89.

6. **Aoutez une instruction `action` au marqueur pour attribuer un comportement par saut aux flux de trafic non conformes de classe `ftp`.**

```
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
```

`module dscpmk`	Appelle le module de marquage `dscpmk`.
`name markAF31`	Attribue le nom `markAF31` à l'instruction `action`.
`global_stats TRUE`	Active le recueil de statistiques pour la classe `ftp`.
`dscp_map{0–63:26}`	Assigne un DSCP `26` aux en-têtes de paquets de la classe de trafic `ftp` lorsque ce trafic dépasse le débit garanti.
`next_action continue`	Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic `ftp` et que ces paquets peuvent revenir dans le flux réseau.

Un DSCP `26` donne pour instruction au marqueur d'attribuer la valeur décimale 26 (binaire 011010) à toutes les entrées de la structure `dscp`. Le DSCP `26` définit le comportement AF31. Le marqueur signale les paquets de la classe de trafic `ftp` par le DSCP `26` dans le champ DS.

AF31 garantit que tous les paquets avec un DSCP égal à `26` se voient attribuer un niveau de perte faible assorti d'une priorité de classe 3. En d'autres termes, la probabilité de rejeter un trafic FTP non conforme est faible. Le Tableau 6-2, “Points de code Assured Forwarding” répertorie les points de code AF possibles.

7. **Ajoutez une instruction `action` au marqueur pour attribuer un comportement par saut aux flux `ftp` conformes au débit garanti.**

```
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

`name markAF22`	Attribue le nom `markAF22` à l'instruction `action`.
`dscp_map{0–63:20}`	Assigne un DSCP `20` aux en-têtes de paquets de la classe de trafic `ftp` lorsque le trafic `ftp` dépasse le débit configuré.

Un DSCP égal à 20 donne pour instruction au marqueur d'attribuer la valeur décimale 20 (binaire 010100) à toutes les entrées de la structure `dscp`. Le DSCP `20` définit le comportement AF22. Le marqueur signale les paquets de la classe de trafic `ftp` par le DSCP `20` dans le champ DS.

AF22 garantit que tous les paquets avec un DSCP égal à `20` se voient attribuer un niveau de perte moyen assorti d'une priorité de classe 2. En conséquence, le trafic FTP respectant ces conditions peut compter sur un niveau de priorité moyen parmi les flux libérés simultanément par le système IPQoS. Toutefois, le routeur assigne une plus grande priorité aux classes de trafic dotées d'un niveau de priorité identique de classe 1 ou supérieur. Le Tableau 6-2, “Points de code Assured Forwarding” répertorie les points de code AF possibles.

8. **Insérez les DSCP créés pour le serveur d'application dans les fichiers correspondants sur le routeur Diffserv.**

9. **Enregistrez les modifications apportées au fichier `/etc/inet/ipqosinit.conf`.**

   - **Si vous avez terminé d'apporter des modifications, démarrez le service `ipqos`.**

     Reportez-vous à “Démarrage du service `ipqos`” à la page 74 pour des instructions spécifiques sur le démarrage ou redémarrage du service.

   - **Si vous souhaitez continuer à apporter des modifications dans le fichier de configuration IPQoS, choisissez une autre tâche.**

     Reportez-vous à “Planification générale de la configuration IPQoS (liste de tâches)” à la page 25 pour une liste des autres modifications qui peuvent être nécessaires.

Fourniture de services différenciés sur un routeur

Pour fournir des services réellement différenciés, vous devez inclure un routeur Diffserv dans la topologie de votre réseau comme décrit dans la section “Stratégies matérielles pour le réseau Diffserv” à la page 26. Les étapes véritables de la configuration Diffserv sur un routeur ainsi que la mise à jour des fichiers du routeur dépassent le cadre de ce guide.

Cette section donne des indications générales sur la procédure de coordination des informations de transmission entre les différents systèmes IPQoS sur le réseau et le routeur Diffserv.

Tout d'abord, examinez les fichiers de configuration pour tous les systèmes IPQoS sur votre réseau pour les points de code fournis la qualité de service (QoS) sont des stratégies utilisées dans les différents.

Dressez la liste des points de code ainsi que celle des systèmes et des classes auxquels font référence les points de code. Si l'utilisation d'un même point de code pour différentes zones est acceptable, vous devez fournir d'autres critères dans le fichier de configuration IPQoS, tel qu'un sélecteur `precedence`, pour déterminer la priorité de deux classes marquées de manière identique.

Par exemple, dans le cadre du réseau illustré dans les procédures de ce chapitre, il est possible d'élaborer le tableau de points de codes suivants.

système	Class (Classe)	PHB	Point de code DS
`Goldweb`	`video`	EF	46 (101110)
`Goldweb`	`goldweb`	AF11	10 (001010)
`Userweb`	`webout`	AF12	12 (001100)
`BigAPPS`	`smtp`	AF13	14 (001110)
`BigAPPS`	`news`	AF18	18 (010010)
`BigAPPS`	Trafic `ftp` conforme	AF22	20 (010100)
`BigAPPS`	Trafic `ftp` non conforme	AF31	26 (011010)

Après avoir identifié les points de code provenant des fichiers de configuration IPQoS de votre réseau, ajoutez-les aux fichiers qui conviennent sur le routeur Diffserv. Les points de code fournis contribuent à configurer le mécanisme d'ordonnancement Diffserv du routeur. Reportez-vous à la documentation du fabricant du routeur ainsi qu'à son site Web pour obtenir des instructions.

♦ ♦ ♦ CHAPITRE 4

Tâches pour le démarrage et la maintenance d'IPQoS

Ce chapitre inclut les tâches destinées à activer un fichier de configuration IPQoS et à consigner les événements en rapport avec IPQoS. Les thèmes ci-dessous sont abordés :

- “Administration d'IPQoS” à la page 73
- “Dépannage des messages d'erreur IPQoS” à la page 76

Remarque - La fonction IPQoS risque d'être supprimée dans une version ultérieure. Utilisez à sa place les commandes `dladm`, `flowadm` ainsi que les commandes associées, qui assurent des fonctions de contrôle des ressources de bande passante similaires. Pour plus d'informations, reportez-vous au manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Administration d'IPQoS

Cette section décrit comment démarrer et gérer IPQoS sur un système Oracle Solaris. Avant de commencer ces tâches, vous devez disposer d'un fichier de configuration IPQoS complet comme décrit dans la section “Définition d'une stratégie QoS liste des tâches” à la page 43. Cette section couvre les tâches suivantes :

- “Ajout du package `ipqos`” à la page 73
- “Démarrage du service `ipqos`” à la page 74
- “Activation de la journalisation des messages IPQoS au cours de l'initialisation” à la page 75

▼ Ajout du package `ipqos`

Le package `ipqos` n'est pas ajouté par défaut dans toutes les configurations. Cette procédure explique comment ajouter ce package.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Vérifiez que le package n'est installée IPQoS.**

```
# pkg list ipqos
pkg list: no packages matching 'ipqos' installed
```

3. **Vérifiez que votre AI référentiel de packages IPS contient le package.**

```
# pkg list -a ipqos
NAME (PUBLISHER)                        VERSION                    IFO
system/network/ipqos                    0.5.11-0.175.2.0.0.26.2    i--
```

4. **Installez le package AI.**

```
# pkg install system/network/ipqos
           Packages to install:  1
       Create boot environment: No
Create backup boot environment: No
            Services to change:  1

DOWNLOAD                      PKGS       FILES    XFER (MB)   SPEED
Completed                      1/1       32/32      0.1/0.1  546k/s
```

Démarrage du service ipqos

Une fois que vous avez apporté des modifications dans le fichier de configuration IPQoS, vous devez démarrer ou redémarrer le service SMF ipqos.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Assurez-vous que les modifications correctes se trouvent dans le fichier /etc/inet/ipqosinit.conf.**

3. **Déterminez si le service ipqos est en cours d'exécution.**

```
# svcs svc:/network/ipqos
STATE          STIME    FMRI
disabled       Mar_11   svc:/network/ipqos:default
```

4. **Activez ou redémarrez le service ipqos.**

- **Si le service `ipqos` est désactivé, démarrez-le.**

  ```
  # svcadm enable svc:/network/ipqos
  ```

- **Si le service `ipqos` est activé, désactivez-le puis réactivez-le.**

  Les étapes ci-dessous utiliseront le nouveau fichier de configuration au démarrage du service.

  ```
  # svcadm disable svc:/network/ipqos
  # svcadm enable svc:/network/ipqos
  ```

5. **Testez et déboguez la nouvelle configuration IPQoS.**

   Les utilitaires UNIX permettent d'effectuer le suivi du comportement d'IPQoS et de recueillir des statistiques sur votre mise en oeuvre IPQoS. Ces informations vous aident à déterminer si la configuration fonctionne comme prévu.

Voir aussi

- Pour étudier les statistiques concernant le fonctionnement des modules IPQoS, reportez-vous à la section “Collecte des informations statistiques” à la page 84.
- Pour journaliser les messages `ipqosconf`, reportez-vous à la section “Activation de la journalisation des messages IPQoS au cours de l'initialisation” à la page 75.

▼ Activation de la journalisation des messages IPQoS au cours de l'initialisation

Pour enregistrer les messages d'initialisation d'IPQoS, vous devez modifier le fichier `/etc/syslog.conf`.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Ajoutez le texte suivant comme ultime entrée du fichier `/etc/syslog.conf`.**

   ```
   user.info                  /var/adm/messages
   ```

   Insérez des tabulations plutôt que des espaces entre les colonnes.

   Cette entrée permet de journaliser tous les messages générés par IPQoS dans le fichier `/var/adm/messages`, lors de l'initialisation.

3. **Réinitialisez le système pour appliquer les messages.**

Exemple 4-1 Sortie d'IPQoS du fichier `/var/adm/messages`

Lorsque vous affichez `/var/adm/messages` après la réinitialisation du système, la sortie peut contenir des messages de journalisation IPQoS similaires aux exemples suivants.

```
May 14 10:44:33 ipqos-14 ipqosconf: [ID 815575 user.info]
 New configuration applied.
May 14 10:44:46 ipqos-14 ipqosconf: [ID 469457 user.info]
Current configuration saved to init file.
May 14 10:44:55 ipqos-14 ipqosconf: [ID 435810 user.info]
Configuration flushed.
```

Vous pouvez également afficher des messages d'erreur IPQoS, identiques aux exemples suivants.

```
May 14 10:56:47 ipqos-14 ipqosconf: [ID 123217 user.error]
 Missing/Invalid config file fmt_version.
May 14 10:58:19 ipqos-14 ipqosconf: [ID 671991 user.error]
No ipgpc action defined.
```

Pour obtenir la description de ces messages d'erreur, reportez-vous au Tableau 4-1, “Messages d'erreur IPQoS”.

Dépannage des messages d'erreur IPQoS

Le tableau suivant répertorie les messages d'erreur générés par IPQoS ainsi que leurs solutions possibles.

TABLEAU 4-1 Messages d'erreur IPQoS

Message d'erreur	Description	Solution
`Undefined action in parameter` *parameter-name's* `action` *action-name*	Dans le fichier de configuration IPQoS, le nom de l'action spécifiée pour *nom-paramètre* n'existe pas dans le fichier de configuration.	Créez l'action ou faites appel à une action différente existante dans le paramètre.
`Action` *action-name* `involved in cycle`	Dans le fichier de configuration IPQoS, *nom-action* fait partie du cycle d'actions, ce qui n'est pas autorisé par IPQoS.	Déterminez le cycle d'actions. Supprimez ensuite une des références cycliques du fichier de configuration IPQoS.
`action` *nom-action* `isn't referenced by any other actions`	Une définition d'action non `ipgpc` n'est pas référencée par d'autres actions définies dans le fichier de configuration IPQoS, ce qui n'est pas autorisé par IPQoS.	Supprimez l'action non référencée. Vous pouvez aussi faire en sorte qu'une action fasse référence à l'action actuellement sans référence.
`Missing/Invalid config file fmt_version`	Le format du fichier du configuration n'est pas spécifié en tant que première entrée du fichier, ce qui est requis par IPQoS.	Ajoutez la version du format comme indiqué dans la section “Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 47.

Message d'erreur	Description	Solution
`Unsupported config file format version`	La version de format spécifiée dans le fichier de configuration n'est pas prise en charge par IPQoS.	Remplacez la version du format par `fmt_version 1.0`, nécessaire pour utiliser la version Solaris 9 9/02 d'IPQoS.
`No ipgpc action defined.`	Vous n'avez pas défini une action pour la classification `ipgpc` dans le fichier de configuration alors que cela est une exigence d'IPQoS.	Définissez une action pour `ipgpc` comme indiqué dans la section “Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 47.
`Can't commit a null configuration`	`ipqosconf -c`a été exécuté pour valider une configuration vide, ce qui n'est pas autorisé dans IPQoS.	Assurez-vous d'avoir appliqué un fichier de configuration avant de valider une configuration. Pour obtenir des instructions, reportez-vous à “Démarrage du service `ipqos`” à la page 74.
`Invalid CIDR mask on line` *numéro de la ligne*	Dans le fichier de configuration, un masque CIDR est utilisé en tant que partie de l'adresse IP qui se trouve hors de la plage des adresses IP valides.	Changez la valeur du masque pour qu'elle soit comprise dans la page 1–32 pour IPv4 et 1–128 pour IPv6.
`Address masks aren't allowed for host names line` *numéro-ligne*	Dans le fichier de configuration, vous avez défini un masque CIDR en guise de nom d'hôte ce qui n'est pas autorisé dans IPQoS.	Supprimez le masque ou remplacez le nom d'hôte par une adresse IP.
`Invalid module name line` *numéro de la ligne*	Le nom du module spécifié dans une instruction d'action au sein du fichier de configuration est incorrect.	Vérifiez l'orthographe du nom de module. Pour obtenir la liste des modules IPQoS, reportez-vous au Tableau 6-5, “Modules IPQoS”.
`ipgpc action has incorrect name line` *line-number*	Le nom de l'action `ipgpc` dans le fichier de configuration n'est pas le nom `ipgpc.classify` demandé.	Renommez l'action `ipgpc.classify`.
`Second parameter clause not supported line` *line-number*	Dans le fichier de configuration, vous avez spécifié deux clauses de paramètres pour une seule action, ce qui n'est pas autorisé dans IPQoS.	Combinez tous les paramètres faisant référence à l'action en une seule clause de paramètres.
`Duplicate named action`	Dans le fichier de configuration, deux actions porter le même nom.	Renommez ou supprimez une des actions.
`Duplicate named filter/class in action` *action-name*	Deux filtres ou à deux classes ont le même nom de la même action, qui n'est pas autorisé dans le fichier de configuration IPQoS.	Renommez ou supprimez une des classes.
`Undefined class in filter` *filter-name* `in action` *action-name*	Dans le fichier de configuration, le filtre fait référence à une classe qui n'est pas définie dans l'action.	Créez la classe ou remplacez la référence de filtre par une classe déjà existante.
`Undefined action in class` *class-name* `action` *action-name*	Le classe fait référence à une action non définie dans le fichier de configuration.	Créez l'action ou remplacez la référence par une action déjà existante.
`Invalid parameters for action` *action-name*	Dans le fichier de configuration, un des paramètres est incorrect.	Pour plus d'informations sur le module appelé par l'action nommée, reportez-vous à l'entrée du module figurant dans la section “Architecture IPQoS et modèle Diffserv” à la page 87. Vous pouvez

Message d'erreur	Description	Solution
		également vous reporter à la page de manuel `ipqosconf`(1M).
`Mandatory parameter missing for action` *action-name*	Un paramètre obligatoire n'est pas défini pour une action dans le fichier de configuration.	Pour plus d'informations sur le module appelé par l'action nommée, reportez-vous à l'entrée du module figurant dans la section “Architecture IPQoS et modèle Diffserv” à la page 87. Vous pouvez également vous reporter à la page de manuel `ipqosconf`(1M).
`Max number of classes reached in ipgpc`	Vous avez spécifié plus de classes qu'il n'est permis de le faire dans l'action `ipgpc` du fichier de configuration IPQoS. Le nombre maximum est 10007.	Vérifiez le fichier de configuration et supprimez les classes inutiles. Une autre solution consiste à augmenter le nombre maximum de classes en ajoutant l'entrée`ipgpc_max_classes` *class-number* au fichier `/etc/system`.
`Max number of filters reached in action ipgpc`	Vous avez spécifié plus de filtres qu'il n'est permis de le faire dans l'action `ipgpc` du fichier de configuration IPQoS. Le nombre maximum est 10007.	Vérifiez le fichier de configuration et supprimez les filtres inutiles. Vous pouvez aussi élever le nombre maximum de filtres en ajoutant l'entrée `ipgpc_max_filters` *filter-number* au fichier `/etc/system`.
`Invalid/missing parameters for filter` *filter-name* `in action ipgpc`	Dans le fichier de configuration, le filtre *nom-filtre* comporte un paramètre non valide ou un paramètre est manquant.	Reportez-vous à la page de manuel `ipqosconf`(1M) pour la liste des paramètres valides.
`Name not allowed to start with '!', line` *line-number*	Un nom d'action, de filtre ou de classe commence par un point d'exclamation (!), ce qui n'est pas autorisé dans le fichier IPQoS.	Supprimez le point d'exclamation ou changez le nom de l'action, de la classe ou du filtre.
`Name exceeds the maximum name length line` *line-number*	Une action, une classe ou un nom dans le fichier de configuration filtre dépasse la longueur maximum de 23 caractères.	Attribuez un nom d'action, de classe ou de filtre plus court.
`Array declaration line` *line-number* `is invalid`	Dans le fichier de configuration, la déclaration de tableau pour le paramètre sur la ligne *numéro-ligne* n'est pas valide.	Pour définir correctement la syntaxe de déclaration de tableau appelée par l'instruction `action` avec le tableau non valide, reportez-vous à la section “Architecture IPQoS et modèle Diffserv” à la page 87. Vous pouvez également vous reporter à la page de manuel `ipqosconf`(1M).
`Quoted string exceeds line,` *numéro de la ligne*	La chaîne n'inclut pas les guillemets de fermeture sur la même ligne, ce qui est obligatoire dans le fichier de configuration.	Assurez-vous que la chaîne comprise entre les guillemets commence et finit sur la même ligne dans le fichier de configuration.
`Invalid value, line` *numéro-ligne*	La valeur attribuée à la ligne *numéro-ligne* du fichier de configuration n'est pas prise en charge par le paramètre.	Pour connaître les valeurs autorisées pour le module appelé par l'instruction `action`, reportez-vous à la description du module dans la section “Architecture IPQoS et modèle Diffserv” à la page 87. Vous pouvez également vous reporter à la page de manuel `ipqosconf`(1M).

Message d'erreur	Description	Solution
`Unrecognized value, line` *numéro de la ligne*	La valeur du *numéro-ligne* du fichier de configuration n'est pas une valeur d'énumération prise en charge par le paramètre.	Vérifiez la validité de la valeur d'énumération choisie pour le paramètre. Pour obtenir une description du module appelé par l'instruction `action` avec le numéro de ligne non reconnu, reportez-vous à la section “Architecture IPQoS et modèle Diffserv” à la page 87. Vous pouvez également vous reporter à la page de manuel `ipqosconf`(1M).
`Malformed value list line` *numéro de la ligne*	L'énumération spécifiée à la ligne *numéro-ligne* du fichier de configuration n'est pas conforme à la syntaxe de spécification.	Pour en savoir plus sur la syntaxe correcte du module appelé par l'instruction `action` avec la liste de valeurs non conforme, reportez-vous à la description du module figurant à la section “Architecture IPQoS et modèle Diffserv” à la page 87 Vous pouvez également vous reporter à la page de manuel `ipqosconf`(1M).
`Duplicate parameter line` *numéro de la ligne*	Un paramètre en double a été spécifié à la ligne *numéro-ligne* qui n'est pas autorisé dans le fichier de configuration.	Supprimez les paramètres en double.
`Invalid action name line` *numéro de la ligne*	Le nom de l'action à *line-number* du fichier de configuration utilise un nom correspondant à un des noms prédéfinis (continue" ou "drop").	Renommez l'action de sorte que son nom diffère des noms prédéfinis.
`Failed to resolve src/dst host name for filter at line` *line-number*`, ignoring filter`	`ipqosconf` n'a pas pu résoudre l'adresse d'origine ou de destination définie pour le filtre concerné dans le fichier de configuration. En conséquence, le filtre n'est pas pris en compte.	Si le filtre est important, réessayez d'appliquer la configuration plus tard.
`Incompatible address version line` *line-number*	La version IP de l'adresse à la ligne *numéro-ligne* est incompatible avec la version d'une adresse IP ou d'un paramètre `version_ip` déjà spécifié.	Modifiez les deux entrées en conflit de manière à ce qu'elles soient compatibles.
`Action at line` *numéro de la ligne* `has the same name as currently installed action, but is for a different module`	Une action a essayé de modifier le module d'une action qui existe déjà dans la configuration IPQoS du système, mais ce n'est pas autorisé.	Videz la configuration actuelle avant d'appliquer la nouvelle configuration.

♦ ♦ ♦ CHAPITRE 5

Tâches pour l'utilisation de la comptabilisation des flux et de la collecte statistique

Ce chapitre décrit comment obtenir des informations comptables et statistiques sur le trafic géré par un système IPQoS. Les thèmes ci-dessous sont abordés :

Remarque - La fonction IPQoS risque d'être supprimée dans une version ultérieure. Utilisez à sa place les commandes `dladm`, `flowadm` ainsi que les commandes associées, qui assurent des fonctions de contrôle des ressources de bande passante similaires. Pour plus d'informations, reportez-vous au manuel " Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ".

Enregistrement des informations sur les flux de trafic

Vous utilisez le module IPQoS `flowacct` pour collecter des informations sur les flux de trafic, par exemple les adresses source et de destination, le nombre de kits dans un flux, et d'autres données similaires. Le processus consistant à accumuler et à enregistrer des informations relatifs aux flux s'appelle la *comptabilisation de flux*.

Les résultats de la comptabilisation de flux sur le trafic d'une classe donnée sont enregistrés dans la table des *enregistrements de flux*. Chaque enregistrement de flux se décompose en une série d'attributs. Ces attributs contiennent des données sur les flux de trafic de la classe en question sur une période de temps. Pour connaître la liste des attributs de `flowacct`, reportez-vous au Tableau 6-4, "Attributs d'un enregistrement `flowacct`".

La comptabilisation des flux est un outil pratique pour la facturation des clients telle qu'elle est définie dans leur accord de niveau de service. Vous pouvez également faire appel à la comptabilisation des flux pour obtenir des statistiques sur les flux en rapport avec des applications critiques. Cette section récapitule les tâches au cours desquelles le module

`flowacct` est associé à l'utilitaire de comptabilité étendue d'Oracle Solaris afin d'obtenir les données des flux de trafic.

Pour plus d'informations, reportez-vous aux sources suivantes :

- Pour obtenir des instructions sur la façon d'assigner les paramètres `flowacct` dans les fichiers de configuration IPQoS, reportez-vous à “Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS” à la page 56.
- Pour connaître la procédure permettant de créer une instruction `flowacct` dans le fichier de configuration IPQoS, reportez-vous à la section “Configuration du contrôle de flux dans le fichier de configuration IPQoS” à la page 68.
- Pour en savoir plus sur le fonctionnement de `flowacct`, reportez-vous à la section “Module de classification” à la page 88.
- Pour des informations techniques, reportez-vous à la page de manuel `flowacct`(7ipp).

▼ Création d'un fichier contenant les données de comptabilisation des flux

Avant d'ajouter une action `flowacct` au fichier de configuration IPQoS, vous devez créer un fichier d'enregistrement des flux du module `flowacct`. `acctadm` peut enregistrer les attributs de base ou les attributs étendus dans le fichier. Tous les attributs `flowacct` sont répertoriés dans le Tableau 6-4, “Attributs d'un enregistrement `flowacct`”. Pour plus d'informations, reportez-vous à la page de manuel `acctadm`(1M).

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Créez un fichier standard de comptabilisation de flux.**

   Voici comment créer un fichier standard de comptabilisation de flux pour le serveur Web Premium tel qu'il est configuré dans l'Exemple 3-1, “Fichier de configuration IPQoS pour un serveur Web premium”.

   ```
   # /usr/sbin/acctadm -e basic -f /var/ipqos/goldweb/account.info flow
   ```

   `acctadm -e` — Appelle la commande `acctadm` assortie de l'option `-e`. L'option `-e` active les arguments qui suivent.

   `basic` — Déclare que seules les données des huit attributs `flowacct` standard doivent être enregistrées dans le fichier.

`/var/ipqos/goldweb/account.info`	Spécifie le nom du chemin complet du fichier contenant les enregistrements de flux émanant de `flowacct`.
`flow`	Demande à `acctadm` d'activer la comptabilisation des flux.

3. **Examinez les information sur la comptabilisation des flux concernant le système IPQoS en tapant `acctadm` sans arguments.**

   La sortie`acctadm` est similaire à celle présentée ci-dessous :

```
Task accounting: inactive
       Task accounting file: none
     Tracked task resources: none
   Untracked task resources: extended
         Process accounting: inactive
    Process accounting file: none
  Tracked process resources: none
Untracked process resources: extended,host,mstate
            Flow accounting: active
       Flow accounting file: /var/ipqos/goldweb/account.info
     Tracked flow resources: basic
   Untracked flow resources: dsfield,ctime,lseen,projid,uid
```

   Toutes les entrées hormis les quatre dernières sont destinées à la fonction du gestionnaire de ressources d'Oracle Solaris. Les entrées spécifiques à IPQoS sont les suivantes :

`Flow accounting: active`	Indique que la comptabilisation est activée.
`Flow accounting file: /var/ipqos/goldweb/account.info`	Indique le nom du fichier de comptabilisation des flux actuel.
`Tracked flow resources: basic`	Spécifie que seuls les attributs de flux standard sont suivis.
`Untracked flow resources: dsfield,ctime,lseen,projid,uid`	Spécifie que seuls les attributs de flux standard sont suivis.

4. **(Facultatif) Ajoutez des attributs étendus au fichier de comptabilisation.**

```
# acctadm -e extended -f /var/ipqos/goldweb/account.info flow
```

5. **(Facultatif) Revenez au seul enregistrement des attributs standard dans le fichier de comptabilisation.**

```
# acctadm -d extended -e basic -f /var/ipqos/goldweb/account.info
```

L'option `-d` désactive la comptabilité étendue.

6. **Affichez le contenu du fichier de comptabilisation des flux.**

   Pour obtenir des instructions sur l'affichage du contenu d'un fichier de comptabilisation des flux, reportez-vous à la section " Interface Perl pour libexacct " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ".

Voir aussi Pour obtenir des informations détaillées sur la fonction de comptabilisation étendue, reportez-vous au Chapitre 4, " A propos de la comptabilisation étendue " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ".

Étapes suivantes

- Pour définir les paramètres de `flowacct` dans le fichier de configuration IPQoS, reportez-vous à la section "Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS" à la page 56.
- Pour imprimer les données du fichier créé avec la commande `acctadm`, reportez-vous à la section " Interface Perl pour libexacct " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ".

Collecte des informations statistiques

La commande `kstat` permet de générer des informations statistiques à partir des modules IPQoS.

`/bin/kstat -m` *ipqos-module-name*

Spécifiez un nom de module IPQoS valide comme illustré dans le Tableau 6-5, "Modules IPQoS". Ainsi, pour afficher les statistiques générées par le marqueur `dscpmk`, utilisez la commande suivante :

```
/bin/kstat -m dscpmk
```

Pour des détails techniques, reportez-vous à la page de manuel `kstat`(1M).

EXEMPLE 5-1 Statistiques `kstat` pour IPQoS

L'exemple suivant présente les résultats qu'il est possible d'obtenir suite à l'exécution de la commande `kstat` afin d'obtenir des statistiques sur le module `flowacct`.

```
# kstat -m flowacct
module: flowacct                        instance: 3
name:   Flowacct statistics             class:    flacct
        bytes_in_tbl                    84
```

```
        crtime                  345728.504106363
        epackets                0
        flows_in_tbl            1
        nbytes                  84
        npackets                1
        snaptime                345774.031843301
        usedmem                 256
```

`class: flacct` Indique le nom de la classe à laquelle les flux de trafic appartiennent. Dans l'exemple illustré, il s'agit de `flacct`.

`bytes_in_tbl` Nombre total d'octets dans la table des flux. Le nombre total d'octets constitue la somme, exprimée en octets, de tous les enregistrements de flux actuellement consignés dans la table des flux. Le nombre total d'octets de cette table des flux est 84. Si aucun flux ne se trouve dans la table, la valeur de `bytes_in_tbl` est 0.

`crtime` Heure à laquelle la sortie `kstat` a été générée.

`epackets` Nombre de paquets ayant entraîné une erreur au cours du traitement. Dans l'exemple, cette valeur est nulle.

`flows_in_tbl` Nombre d'enregistrements de flux dans la table des flux qui, dans cet exemple, est 1. Si aucun enregistrement ne se trouve dans la table, la valeur de `flows_in_tbl` est 0.

`nbytes` Nombre total d'octets signalés pour cette instance d'action `flowacct`. Il est de 84 dans l'exemple. La valeur inclut les octets qui se trouvent actuellement dans la table des flux. La valeur inclut également des octets dont le délai est dépassé et qui ne figurent plus dans la table des flux.

`npackets` Nombre total de paquets signalés pour cette instance d'action `flowacct`. Il est de 1 dans l'exemple. `npackets` inclut les paquets qui se trouvent actuellement dans la table de flux. `npackets` inclut les paquets dont le délai est dépassé et ne figurant plus dans la table des flux.

`usedmem` Mémoire, exprimée en nombre d'octets, utilisée par la table des flux qui est gérée par cette instance de `flowacct.` La valeur `usedmem` est de 256 dans l'exemple. La valeur de `usedmem` est de 0 si la table des flux n'affiche aucun enregistrement de flux.

♦ ♦ ♦ CHAPITRE 6

Référence IPQoS en détails

Ce chapitre fournit des informations approfondies sur les sujets IPQoS suivants :

- “Architecture IPQoS et modèle Diffserv” à la page 87
- “Fichier de configuration IPQoS” à la page 100

Pour plus d'informations, reportez-vous aux références suivantes :

- Pour obtenir une présentation générale, reportez-vous au Chapitre 1, Présentation d'IPQoS.
- Pour obtenir des informations sur la planification, reportez-vous au Chapitre 2, Planification d'un réseau compatible IPQoS.
- Pour consulter les procédures de configuration d'IPQoS, reportez-vous au Chapitre 3, Tâches pour la création du fichier de configuration IPQoS.

Remarque - La fonction IPQoS risque d'être supprimée dans une version ultérieure. Utilisez à sa place les commandes `dladm`, `flowadm` ainsi que les commandes associées, qui assurent des fonctions de contrôle des ressources de bande passante similaires. Pour plus d'informations, reportez-vous au manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Architecture IPQoS et modèle Diffserv

Cette section décrit l'architecture IPQoS et la manière dont IPQoS implémente le modèle de services différenciés (Diffserv) défini par le document RFC 2475, An Architecture for Differentiated Services (http://www.ietf.org/rfc/rfc2475.txt?number=2475) (en anglais). Les éléments suivants du modèle Diffserv sont inclus dans IPQoS :

- Classificateur
- Compteur
- Marqueur

Par ailleurs, IPQoS inclut le module de comptabilisation des flux et le marqueur `dlcosmk` utilisé avec les périphériques VLAN (réseau local virtuel).

Module de classification

Dans le modèle Diffserv, le *classificateur* est chargé d'organiser les flux de trafic sélectionnés en groupes auxquels s'appliquent différents niveaux de service. Les classificateurs définis dans le document RFC 2475 ont été initialement conçus pour les routeurs de bordure. En revanche, le classificateur IPQoS `ipgpc` est destiné à traiter les flux de trafic pour les hôtes internes au réseau local. En conséquence, un réseau doté de systèmes IPQoS et d'un routeur Diffserv peut fournir un niveau supérieur de services différenciés. Pour une description technique, reportez-vous à la page de manuel `ipgpc`(7ipp).

Le classificateur `ipgpc` effectue les opérations suivantes :

1. Sélection des flux de trafic répondant aux critères spécifiés dans le fichier de configuration IPQoS sur le système IPQoS

   La stratégie QoS définit les différents critères obligatoirement présents dans les en-têtes de paquets. Ces critères sont appelés *sélecteurs*. Le classificateur `ipgpc` compare ces sélecteurs aux en-têtes de paquets reçus par le système IPQoS. `ipgpc` sélectionne ensuite tous les paquets correspondants.
2. Séparation des flux de paquets en *classes* : trafic réseau dont les caractéristiques sont identiques comme indiqué dans le fichier de configuration IPQoS
3. Examen de la valeur du champ de services différenciés (DS) du paquet grâce à la présence d'un point de code de services différenciés ou DSCP

   La présence du DSCP indique si l'expéditeur a prévu un comportement de transmission pour le trafic entrant.
4. Définition de l'action supplémentaire spécifiée dans le fichier de configuration IPQoS pour les paquets d'une classe particulière
5. Transmission des paquets au module IPQoS suivant indiqué dans le fichier de configuration IPQoS ou renvoi des paquets dans le trafic réseau

Pour obtenir des informations générales sur le classificateur, reportez-vous à la section “Présentation du classificateur (`ipgpc`)” à la page 16. Pour plus d'informations sur l'appel du classificateur dans le fichier de configuration IPQoS, reportez-vous à la section “Fichier de configuration IPQoS” à la page 100.

Sélecteurs IPQoS

Le classificateur `ipgpc` prend en charge un grand nombre de sélecteurs que vous pouvez utiliser dans la clause `filter` du fichier de configuration IPQoS. Lorsque vous définissez un filtre, veillez à n'utiliser que le minimum de sélecteurs nécessaire à la récupération du trafic d'une classe particulière. Le nombre de filtres défini peut avoir des conséquences sur les performances du protocole IPQoS.

Le tableau suivant répertorie les sélecteurs disponibles pour `ipgpc`.

TABLEAU 6-1 Sélecteurs de filtre pour le classificateur IPQoS

Sélecteur	Argument	Informations sélectionnées
`saddr`	Numéro d'adresse IP.	Adresse source.
`daddr`	Numéro d'adresse IP.	Adresse de destination.
`sport`	Numéro du port ou nom du service comme indiqué dans le fichier `/etc/services`.	Port source à partir duquel provient une classe de trafic.
`dport`	Numéro du port ou nom du service comme indiqué dans le fichier `/etc/services`.	Port de destination auquel une classe de trafic est liée.
`protocol`	Numéro ou nom de protocole comme indiqué dans le fichier `/etc/protocols`.	Protocole à utiliser par cette classe de trafic.
`dsfield`	Point de code DS (DSCP) d'une valeur comprise dans l'intervalle 0–63.	DSCP définissant un comportement de transmission à appliquer au paquet. Si ce paramètre est spécifié, le paramètre `dsfield_mask` doit également être spécifié.
`dsfield_mask`	Masque de bits d'une valeur comprise entre 0 et 255.	Utilisé conjointement avec le sélecteur `dsfield`. `dsfield_mask` est appliqué au sélecteur `dsfield` pour déterminer les bits qu'il faut faire correspondre.
`if_name`	Nom de l'interface.	Interface à utiliser pour le trafic entrant et le trafic sortant d'une classe particulière.
`user`	Numéro de l'identifiant utilisateur UNIX ou nom d'utilisateur à sélectionner. Si aucun identifiant utilisateur ou nom d'utilisateur ne se trouve dans le paquet, le paramètre par défaut –1 est appliqué.	ID utilisateur fourni à une application.
`projid`	Numéro de l'ID du projet à sélectionner.	ID du projet fourni à une application.
`priority`	Numéro de la priorité. La priorité la plus basse est de 0.	Priorité attribuée aux paquets de cette classe. La priorité sert à classer les filtres selon leur importance dans une même classe.
`direction`	Les valeurs possibles sont les suivantes :	Direction du flux du paquet de la machine IPQo S.
	`LOCAL_IN`	Trafic local d'entrée au système IPQoS.
	`LOCAL_OUT`	Trafic local de sortie au système IPQoS.
	`FWD_IN`	Trafic d'entrée à transmettre.
	`FWD_OUT`	Trafic de sortie à transmettre.
`precedence`	Valeur du niveau de priorité. Le niveau de priorité le plus élevé est de 0.	Utilisé pour classer les filtres de même priorité.
`ip_version`	`V4` ou `V6`	Schéma d'adressage utilisé par les paquets. Il s'agit d'IPv4 ou d'IPv6.

Module de mesure

Le *compteur* permet de suivre le taux de transmission des flux exprimé en nombre de paquets. Le compteur détermine si le paquet est conforme aux paramètres configurés. Le module de

mesure détermine l'action suivante à entreprendre pour un paquet provenant d'un jeu d'actions en fonction de la taille du paquet, des paramètres configurés et du débit du flux.

Le compteur comprend deux modules de mesure, `tokenmt` et `tswtclmt`, que vous définissez dans le fichier de configuration IPQoS. Vous pouvez configurer l'un des deux modules ou les deux modules pour une classe donnée.

Lorsque vous configurez un module de mesure, vous pouvez définir deux paramètres pour une même vitesse de tranfert :

- `committed-rate` : définit le taux de transmission acceptable en bits par seconde pour les paquets d'une classe particulière.
- `peak-rate` : définit le taux de transmission maximal en bits par seconde autorisé pour les paquets d'une classe particulière.

Une action de mesure d'un paquet peut aboutir à l'un des trois résultats suivants :

- `green` : le paquet contraint le flux à rester dans les limites du débit garanti.
- `yellow` : le paquet contraint le flux à dépasser le débit garanti, mais pas le débit de pointe.
- `red` : le paquet contraint le flux à dépasser le débit de pointe.

Vous pouvez associer chaque résultat à différentes actions dans le fichier de configuration IPQoS.

Module de mesure `tokenmt`

Le module `tokenmt` fait appel à des *seaux de jetons* pour mesurer le taux de transmission d'un flux. Vous pouvez configurer `tokenmt` pour fonctionner comme un compteur à débit simple ou à débit double. Une instance d'action `tokenmt` gère deux seaux de jetons qui déterminent si le flux de trafic est conforme aux paramètres configurés.

La page de manuel `tokenmt`(7ipp) explique comment IPQoS implémente le paradigme du contrôle de jetons.

Les paramètres de configuration pour `tokenmt` sont les suivants :

- `committed_rate` : spécifie le débit garanti du flux en bits par seconde.
- `committed_burst` : spécifie la taille maximale de rafale garantie en bits. Le paramètre `committed_burst` définit le nombre de paquets sortants d'une classe spécifique pouvant arriver sur le réseau à un débit garanti.
- `peak_rate` : spécifie le débit de pointe en bits par seconde.
- `peak_burst` : spécifie la taille maximale de rafale ou de pointe en bits. Le paramètre `peak_burst` accorde à une classe de trafic une taille peak-burst qui dépasse le débit garanti.

- `color_aware` – Active le mode de reconnaissance de couleurs pour `tokenmt`.
- `color_map` : définit un tableau d'entiers faisant correspondre les valeurs DSCP au vert, à l'orange et au rouge.

Configuration du `tokenmt` en tant que compteur à débit simple

Pour configurer `tokenmt` en tant que compteur à débit simple, ne spécifiez pas le paramètre `peak_rate` pour `tokenmt` dans le fichier de configuration IPQoS. Pour configurer une instance `tokenmt` à débit simple afin d'obtenir un résultat rouge, vert ou orange, vous devez spécifier le paramètre `peak_burst` . Si vous n'utilisez pas le paramètre `peak_burst`, vous pouvez configurer `tokenmt` de sorte qu'il aboutisse seulement à un résultat rouge ou vert. Pour consulter un exemple de `tokenmt` à débit simple donnant lieu à deux résultats, reportez-vous à l'Exemple 3-3, “Exemple de fichier de configuration pour un serveur d'application”.

Lorsque `tokenmt` fonctionne comme un compteur à débit simple, le paramètre `peak_burst` définit, en fait, la taille de rafale excessive. Les paramètres `committed_rate` et `committed_burst` ou `peak_burst` doivent désigner des entiers positifs non nuls.

Configuration du `tokenmt` en tant que compteur à débit double

Pour configurer `tokenmt` en tant que compteur à débit double, spécifiez le paramètre `peak_rate` pour l'action `tokenmt` dans le fichier de configuration IPQoS. Un module `tokenmt` à débit double a toujours trois résultats : vert, rouge et orange. Les paramètres `committed_rate` , `committed_burst` et `peak_burst` doivent désigner des entiers positifs non nuls.

Configuration du module `tokenmt` en mode de reconnaissance des couleurs

Pour configurer un mode de reconnaissance des couleurs pour le module `tokenmt` à débit double, yvous devez prévoir des paramètres supplémentaires pour ajouter la fonction d'interprétation des couleurs. Vous trouverez ci-dessous un exemple d'instruction action qui permet de configurer la reconnaissance des couleurs pour `tokenmt`.

EXEMPLE 6-1 Action `tokenmt` de prise en compte des couleurs dans le fichier de configuration IPQoS

```
action {
    module tokenmt
    name meter1
    params {
       committed_rate 4000000
       peak_rate 8000000
       committed_burst 4000000
```

```
        peak_burst 8000000
        global_stats true
        red_action_name continue
        yellow_action_name continue
        green_action_name continue
        color_aware true
        color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
    }
}
```

Vous pouvez activer la fonction de reconnaissance des couleurs en définissant le paramètre `color_aware` sur `true`. En tant que module d'interprétation des couleurs, `tokenmt` suppose que le paquet est déjà marqué en rouge, orange ou vert par une action `tokenmt` précédente. Le module d'interprétation des couleurs `tokenmt` évalue un paquet à l'aide du DSCP figurant dans l'en-tête du paquet en plus des paramètres de compteur à débit double.

Le paramètre `color_map` contient un tableau auquel le DSCP de l'en-tête du paquet est lié. Considérez le tableau `color_map` suivant :

```
color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
```

Les paquets avec un DSCP compris entre 0 et 20 ou équivalent à 22 correspondent au vert. Les paquets avec un DSCP équivalent à 21 ou compris entre 23 et 42 correspondent au rouge. Les paquets avec un DSCP compris entre 43 et 63 sont associés à l'orange. Par défaut, `tokenmt` conserve une table de correspondance de couleurs. Cependant, il est possible de modifier au besoin les valeurs par défaut à l'aide des paramètres `color_map`.

Pour les paramètres *couleur*`_action_name`, vous pouvez spécifier `continue` de manière à terminer le traitement du paquet. Vous pouvez aussi ajouter un argument pour soumettre le paquet à une action de marquage, par exemple, `yellow_action_name mark22`.

Module de mesure `tswtclmt`

Le module `tswtclmt` évalue la bande passante moyenne pour une classe de trafic en procédant à l'*estimation du débit* en fonction du temps. `tswtclmt` fonctionne toujours comme un contrôle à trois résultats. La fonction d'estimation du débit fournit une indication du taux d'arrivée du flux. Ce taux doit correspondre à la bande passante moyenne applicable à un flux de trafic sur une période de temps donnée appelée *fenêtre*.

Utilisez les paramètres suivants pour configurer `tswtclmt` :

- `committed_rate` : spécifie le taux garanti en bits par seconde.
- `peak_rate` : spécifie le débit de pointe en bits par seconde.
- `window` : définit la fenêtre de temps, exprimée en millisecondes, pendant laquelle l'historique de la bande passante moyenne est conservé.

Pour des informations techniques sur `tswtclmt`, reportez-vous à la page de manuel `tswtclmt`(7ipp).

Module de marquage

IPQoS comprend deux modules de marquage, `dscpmk` et `dlcosmk`. Cette section contient des informations sur l'utilisation des deux marqueurs. En théorie, vous devez utiliser `dscpmk`, car `dlcosmk` n'est disponible que pour les systèmes IPQoS et les périphériques VLAN.

Pour obtenir des informations techniques sur ces modules, reportez-vous aux pages de manuel `dscpmk`(7ipp) et `dlcosmk`(7ipp).

Utilisation du marqueur `dscpmk` pour la transmission des paquets

Le marqueur reçoit les flux de trafic après leur traitement par les modules de classification ou de mesure. Le marqueur associe un comportement de transmission au trafic. Ce comportement indique l'action à appliquer aux flux lorsque ces flux quittent le système IPQoS. Le comportement de transmission d'une classe de trafic est défini par le *comportement par saut ou PHB*. Le PHB affecte une priorité à une classe de trafic précisant les flux prioritaires de cette classe par rapport aux autres classes de trafic. Les PHB régissent uniquement les comportements de transfert sur le réseau contigu du système IPQoS. Pour plus d'informations sur les PHB, reportez-vous à la section “PHB (Per-Hop Behaviors)” à la page 20.

La *transmission de paquet* est le processus consistant à envoyer le trafic d'une classe particulière vers sa prochaine destination sur un réseau. Pour un hôte tel qu'un système IPQoS, un paquet est transmis de l'hôte vers le flux de réseau local. Lorsqu'il s'agit d'un routeur Diffserv, un paquet est transmis du réseau local vers le saut suivant du routeur.

Le marqueur signale dans le champ DS de l'en-tête du paquet un comportement de transfert bien connu défini dans le fichier de configuration IPQoS. Par la suite, le système IPQoS et les systèmes Diffserv suivants transmettent le trafic comme indiqué dans le champ DS jusqu'à ce que le marquage change. Pour attribuer un PHB, le système IPQoS inscrit une valeur dans le champ DS de l'en-tête du paquet. Cette valeur est appelée le point de code de services différenciés (DSCP). L'architecture Diffserv définit deux types de comportement de transmission, EF et AF, utilisant des DSCP différents. Pour plus d'informations sur les DSCP, reportez-vous à la section “Point de code DS” à la page 20.

Le système IPQoS lit le DSCP et évalue le niveau de priorité par rapport à d'autres flux de trafic sortants. Le système IPQoS établit la priorité des flux de trafic simultanés et libère chaque flux sur le réseau en fonction de sa priorité.

Le routeur Diffserv reçoit les flux de trafic sortants et lit le champ DS dans les en-têtes de paquets. Le DSCP permet au routeur de classifier et d'ordonnancer les flux de trafic simultanés. Le routeur transmet chaque flux en fonction de la priorité indiquée par le PHB. Notez que le PHB ne peut pas être appliqué au-delà de la limite du routeur du réseau à moins que les systèmes Diffserv des pas suivants reconnaissent le même PHB.

PHB Expedited Forwarding (EF) (traitement accéléré)

Le *transfert accéléré* (EF, Expedited Forwarding) garantit que les paquets dotés du point de code EF recommandé 46 (101110) bénéficient du meilleur traitement disponible sur le réseau. Le service Expedited Forwarding est souvent comparé à une ligne spécialisée. Les routeurs Diffserv garantissent un traitement préférentiel aux paquets accompagnés du point de code 46 (101110) pour l'acheminement vers leur destination.

PHB Assured Forwarding (AF) (traitement assuré)

Le *transfert garanti* (AF, Assured Forwarding) offre quatre classes de comportements de transfert applicables au marqueur. Le tableau suivant présente les classes, les trois « drop precedences » (niveaux de priorité) de chaque classe et les DSCP recommandés associés à chaque priorité. Chaque DSCP est représenté par sa valeur AF, sa valeur en notation décimale et en notation binaire.

TABLEAU 6-2 Points de code Assured Forwarding

	Classe 1	Classe 2	Classe 3	Classe 4
Faible niveau de priorité	AF11 = 10 (001010)	AF21 = 18 (010010)	AF31 = 26 (011010)	AF41 = 34 (100010)
Niveau de priorité intermédiaire	AF12 = 12 (001100)	AF22 = 20 (010100)	AF32 = 28 (011100)	AF42 = 36 (100100)
Niveau de priorité élevé	AF13 = 14 (001110)	AF23 = 22 (010110)	AF33 = 30 (011110)	AF43 = 38 (100110)

Tout système Diffserv peut faire appel au point de code AF afin de l'utiliser en tant que guide lors de la fourniture de services différenciés à différentes classes de trafic.

Lorsque ces paquets atteignent un routeur Diffserv, celui-ci évalue les points de code des paquets ainsi que les DSCP d'autres flux de trafic placés dans la file d'attente. Le routeur transmet ou rejette les paquets, selon la bande passante disponible et les priorités définies par les DSCP des paquets. Notez que l'accès à la bande passante est garanti en priorité aux paquets marqués par un PHB EF par rapport aux paquets marqués par un PHB AF (quelle que soit leur classe).

Coordonnez le marquage des paquets entre les différents systèmes IPQoS de votre réseau et le routeur Diffserv pour veiller à ce que les paquets soient transférés comme prévu. Par exemple, supposons que les systèmes IPQoS de votre réseau marquent les paquets à l'aide des points de code AF21 (010010), AF13 (001110), AF43 (100110) et EF (101110). Vous devez ensuite ajouter les DSCP AF21, AF13, AF43 et EF au fichier approprié sur le routeur Diffserv.

Reportez - vous à la documentation du fabricant du routeur pour plus d'informations sur la modification et des instructions sur la définition de PHB AF des points de code DS sur votre équipement.

Fourniture d'un DSCP au marqueur

Le DSCP a une longueur de 6 bits. Le champ DS a une longueur d'1 octet. Lorsque vous définissez un DSCP, le marquer marque les 6 premiers bits significatifs de l'en-tête du paquet avec le code de point DS. Les deux bits restants (les moins significatifs) ne sont pas utilisés.

Pour définir un DSCP, servez-vous du paramètre suivant au sein d'une instruction d'action du marqueur :

```
dscp_map{0-63:DS-name tcodepoint}
```

Le paramètre `dscp_map` est un tableau à 64 éléments que vous remplissez à l'aide de la valeur (DSCP). Le paramètre `dscp_map` sert à faire correspondre les DSCP entrants aux DSCP sortants appliqués par le marqueur `dscpmk`.

Vous devez spécifier la valeur DSCP pour le paramètre `dscp_map` en notation décimale. Par exemple, vous devez traduire le point de code EF de 101110 en valeur décimale 46 ce qui équivaut à `dscp_map{0-63:46}`. Pour les points de code AF, vous devez exprimer les différents points de code présentés dans le Tableau 6-2, “Points de code Assured Forwarding” en notation décimale spécialement pour le paramètre `dscp_map`.

Utilisation du marqueur `dlcosmk` avec les périphériques VLAN

Le module de marquage `dlcosmk` inscrit le comportement de transmission dans l'en-tête MAC d'un datagramme. Vous ne pouvez utiliser le paramètre `dlcosmk` que dans un système IPQoS avec une interface VLAN.

`dlcosmk` ajoute quatre octets, désignés sous l'appellation d'*étiquette VLAN*, à l'en-tête MAC. L'étiquette VLAN inclut une valeur de priorité utilisateur de 3 bits, définie par la norme IEEE 801.D. Les commutateurs Diffserv en mesure de reconnaître VLAN peuvent lire le champ de priorité utilisateur dans un datagramme. Valeurs de priorité utilisateur la mettre en oeuvre les 801.D de classe de service (CoS), ou encore à l'aide de compatible avec les commutateurs du marché.

Vous pouvez utiliser les valeurs de priorité utilisateur dans l'action du marqueur `dlcosmk` en définissant les indices de classes de service répertoriés dans le tableau suivant.

TABLEAU 6-3 Valeurs de priorité utilisateur 801.D

Classe de service	Définition
0	Au mieux (Best effort)
1	Arrière-plan
2	Disjoncteur de secours
3	Effort excellent (Excellent effort)
4	Charge contrôlée (Controlled load)
5	Vidéo inférieure à une latence de 100ms (Video less than 100ms latency)
6	Vidéo inférieure à une latence de 10ms (Video less than 10ms latency)
7	Contrôle du réseau (Network control)

Pour plus d'informations, reportez-vous à la page de manuel `dlcosmk`(7ipp).

Configuration IPQoS pour les systèmes comportant des périphériques VLAN

Cette section illustre un scénario de réseau simple montrant comment implémenter IPQoS sur les systèmes avec des périphériques VLAN. Le scénario prend en compte deux systèmes IPQoS, `ordinateur1` et `ordinateur2`, reliés par un commutateur. Le périphérique VLAN sur `ordinateur1` a l'adresse IP `10.10.8.1`. Le périphérique VLAN sur `machine2` a l'adresse IP `10.10.8.3`.

Le fichier de configuration IPQoS suivant de l'`ordinateur1` décrit une solution simple pour marquer le trafic allant du commutateur à l'`ordinateur2`.

EXEMPLE 6-2 Fichier de configuration IPQoS pour un système avec un périphérique VLAN

```
fmt_version 1.0
action {
        module ipgpc
       name ipgpc.classify

        filter {
                name myfilter2
                daddr 10.10.8.3
                class myclass
        }

        class {
```

```
                name myclass
                next_action mark4
        }
}

action {
        name mark4
        module dlcosmk
        params {
                cos 4
                next_action continue
  global_stats true
        }
}
```

Dans cette configuration, tout le trafic de l'`ordinateur1` destiné au périphérique VLAN sur l'`ordinateur2` est transmis sur le marqueur `dlcosmk`. L'action de marqueur `marque4` indique à `dlcosmk` d'ajouter une marque VLAN aux datagrammes de la classe `maclasse` possédant une classe de service de 4. La valeur de priorité utilisateur 4 indique que le commutateur reliant les deux machines doit donner la transmission de charge contrôlée aux flux de trafic `maclasse` de l'`ordinateur1`.

Module `flowacct`

Le module `flowacct` d'IPQoS enregistre les informations sur les flux de trafic, un processus connu sous le nom de *comptabilisation des flux*. La comptabilisation des flux produit des données qui peuvent servir à la facturation des clients ou à l'évaluation du trafic d'une classe particulière.

La comptabilisation des flux est facultative. Le module `flowacct` est généralement le dernier module par lequel passent les flux de trafic mesurés ou marqués avant d'être libérés sur le réseau. Pour voir la position de `flowacct` dans le modèle Diffserv, reportez-vous à la Figure 1-1, “Flux de trafic et implémentation IPQoS du modèle Diffserv”. Pour obtenir des informations techniques précises, reportez-vous à la page de manuel `flowacct`(7ipp).

Pour activer la comptabilisation des flux, vous devez utiliser la fonction de comptabilisation d'Oracle Solaris, `exacct` et la commande `acctadm`, ainsi que `flowacct`. Pour plus d'informations sur la comptabilisation des flux, reportez-vous au Chapitre 5, Tâches pour l'utilisation de la comptabilisation des flux et de la collecte statistique.

Paramètres `flowacct`

Le module `flowacct` rassemble des informations sur les flux dans une *table des flux* composée d'*enregistrements de flux*. Chaque entrée de la table contient un enregistrement de flux. Vous ne pouvez pas afficher une table des flux.

Dans le fichier de configuration IPQoS, vous définissez les paramètres `flowacct` suivants pour mesurer les enregistrements de flux et consigner les enregistrements dans la table :

- `timer` : définit un intervalle, en millisecondes, lorsque les flux dont le délai a expiré sont supprimés de la table des flux et consignés dans le fichier créé par `acctadm`.
- `timeout` : définit un intervalle, en millisecondes, spécifiant la durée d'inactivité d'un flux de paquet avant que ce dernier ne soit considéré comme ayant expiré.

Remarque - Vous pouvez configurer `timer` et `timeout` de sorte qu'ils aient des valeurs différentes.

- `max_limit` : définit la limite supérieure du nombre d'enregistrements de flux pouvant être stockés dans la table des flux.

Pour obtenir un exemple d'utilisation des paramètres `flowacct` dans le fichier de configuration IPQoS, reportez-vous à la section “Configuration du contrôle de flux dans le fichier de configuration IPQoS” à la page 68.

Table des flux

Le module `flowacct` gère une table des flux dans laquelle sont enregistrés tous les flux de paquets rencontrés par une instance de `flowacct`.

Un flux est identifié par les paramètres suivants qui incluent l'uplet à 8 attributs de `flowacct` :

- Adresse source
- Adresse de destination
- Port source
- Port de destination
- DSCP
- USER ID
- ID de projet
- Numéro du protocole

Si tous les paramètres de l'uplet à 8 attributs concernant un même flux sont identiques, la table de flux ne contient qu'une seule entrée. Le paramètre `max_limit` détermine le nombre d'entrées que peut inclure une table des flux.

La table des flux est numérisée à l'intervalle spécifié dans le fichier de configuration IPQoS grâce au paramètre `timer`. Le paramètre par défaut est de 15 secondes. Un flux "arrive à expiration" lorsque ses paquets ne sont pas visibles par le système IPQoS à la fin du `délai d'attente` (au moins) indiqué dans le fichier de configuration IPQoS. La période de

temporisation par défaut est de 30 secondes. Les entrées dont le délai d'attente a été dépassé sont ensuite enregistrées dans le fichier de comptabilisation créé par la commande `acctadm`.

Enregistrements `flowacct`

Un enregistrement `flowacct` inclut les attributs décrits dans le tableau suivant.

TABLEAU 6-4 Attributs d'un enregistrement `flowacct`

Nom de l'attribut	Contenu des attributs	type
`src-addr-`*address-type*	Adresse source de l'expéditeur. *type-adresse* équivaut à `v4` pour IPv4 ou `v6` pour IPv6, comme indiqué dans le fichier de configuration IPQo S.	Standard
`dest-addr-`*address-type*	Adresse de destination des paquets. *type-adresse* équivaut à `v4` pour IPv4 ou `v6` pour IPv6, comme indiqué dans le fichier de configuration IPQoS.	Standard
`src-port`	Port source d'où provient le flux.	Standard
`dest-port`	Numéro du port de destination vers lequel le flux est dirigé.	Standard
`protocol`	Numéro du protocole du flux.	Standard
`total-packets`	Nombre de paquets dans le flux.	Standard
`total-bytes`	Nombre d'octets dans le flux.	Standard
action-name	Nom de l'action `flowacct` ayant enregistré le flux.	Standard
`creation-time`	Première fois qu'un paquet est vu par `flowacct`.	Etendu uniquement
`last-seen`	Dernière fois qu'un paquet du flux a été vu.	Etendu uniquement
`diffserv-field`	DSCP dans les en-têtes de paquets sortants du flux.	Etendu uniquement
`user`	ID utilisateur ou nom d'utilisateur UNIX obtenu par l'application.	Etendu uniquement
`projid`	ID du projet obtenu par l'application.	Etendu uniquement

Utilisation d'`acctadm` avec le module `flowacct`

Vous exécutez la commande `acctadm` pour créer un fichier réservé aux enregistrements de flux générés par `flowacct`. `acctadm` s'utilise en parallèle avec la fonction de comptabilisation étendue. Pour des informations techniques, reportez-vous à la page de manuel `acctadm`(1M).

Le module `flowacct` observe les flux et inscrit les enregistrements de flux dans la table des flux. `flowacct` évalue ensuite ses paramètres et attributs dans l'intervalle spécifié par `timer`. Un paquet expire s'il n'est pas visible pendant la durée équivalent aux valeurs `last_seen` et

`timeout`. Toutes les entrées ayant dépassé le délai d'expiration sont supprimées de la table des flux. Elles sont alors consignées dans le fichier de comptabilisation à l'issue de l'intervalle spécifié par le paramètre `timer`.

Pour appliquer `acctadm` au module `flowacct`, respectez la syntaxe suivante :

`acctadm -e` *file-type* `-f` *filename* `flow`

`acctadm -e`	Appelle la commande `acctadm` assortie de l'option `-e`. La valeur -e indique la présence d'une liste de ressources.
file-type	Spécifie les attributs à collecter, soit `basic` ou `extended`. Pour connaître la liste des attributs de chaque type de fichier, reportez-vous au Tableau 6-4, “Attributs d'un enregistrement `flowacct`”.
`-f` *file-name*	Crée le fichier *file-name* dans lequel sont consignés les enregistrements de flux.
`flow`	Implique l'exécution de la commande `acctadm` avec IPQoS.

Fichier de configuration IPQoS

Cette section décrit en détail les différentes parties du fichier de configuration IPQoS. La stratégie activée au démarrage d'IPQoS est stockée dans le fichier `/etc/inet/ipqosinit.conf`. Bien qu'il soit possible de modifier ce fichier, dans le cas d'un nouveau système IPQoS, il est préférable de créer un fichier de configuration sous un autre nom. Les tâches à réaliser pour appliquer et déboguer une configuration IPQoS sont présentées dans le Chapitre 3, Tâches pour la création du fichier de configuration IPQoS.

La syntaxe du fichier de configuration IPQoS est présentée dans l'Exemple 6-3, “Syntaxe du fichier de configuration IPQoS”.

EXEMPLE 6-3 Syntaxe du fichier de configuration IPQoS

```
file_format_version ::= fmt_version version

action_clause ::= action {
     name action-name
     module module-name
     params-clause |  ""
     cf-clauses
}
action_name ::= string
module_name ::= ipgpc | dlcosmk | dscpmk | tswtclmt | tokenmt | flowacct
```

```
params_clause ::= params {
     parameters
     params-stats |    ""
     }
parameters ::=     prm-name-value parameters |   ""
prm_name_value ::= param-name param-value

params_stats ::= global-stats Boolean

cf_clauses ::= class-clause cf-clauses |
               filter-clause cf-clauses | ""

class_clause ::= class {
     name class-name
     next_action next-action-name
     class-stats | ""
                  }
class_name  ::= string
next_action_name  ::= string
class_stats ::= enable_stats Boolean
boolean ::= TRUE | FALSE

filter_clause ::= filter {
                  name filter-name
                  class class–name
                  parameters
                  }
filter_name ::= string
```

Instruction `action`

Les instructions `action` servent à appeler les différents modules IPQoS décrits à la section “Architecture IPQoS et modèle Diffserv” à la page 87.

Lorsque vous créez le fichier de configuration IPQoS, vous devez toujours commencer par indiquer le numéro de version. Vous devez ensuite ajouter l'instruction `action` suivante pour appeler le classificateur :

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
}
```

Faites suivre l'instruction `action` du classificateur par une clause `params` ou une clause `class`.

Respectez la syntaxe suivante pour toutes les autres instructions `action` :

```
action {
```

```
name action-name
module module-name
params-clause | ""
cf-clauses
}
```

`name` *action-name*	Attribue un nom à l'action.
`module` *module-name*	Identifie le module IPQoS à appeler (il doit s'agir de l'un des modules présentés dans le Tableau 6-5, “Modules IPQoS”).
params-clause	Il peut s'agir des paramètres à traiter par le classificateur (statistiques globales ou prochaine action à effectuer, par exemple).
cf-clauses	Ensemble constitué d'aucune ou de plusieurs clauses `class` ou `filter`

Définitions des modules

La définition du module désigne le module chargé de traiter les paramètres dans l'instruction `action`. Le fichier de configuration IPQoS peut inclure les clients répertoriés dans le tableau ci-dessous .

TABLEAU 6-5 Modules IPQoS

Nom de module	Définition
`ipgpc`	Classificateur IP
`dscpmk`	Marqueur servant à créer des DSCP dans des paquets IP
`dlcosmk`	Marqueur à utiliser avec les périphériques VLAN
`tokenmt`	Compteur de seau à jetons
`tswtclmt`	Compteur de fenêtre de temps
`flowacct`	Module de comptabilisation des flux

Clause `class`

Vous définissez une clause `class` pour chaque classe de trafic.

La syntaxe pour définir les classes restantes dans le fichier de configuration IPQoS soit comme suit :

```
class {

      name class-name
      next_action next-action-name
```

```
}
```

Pour collecter des statistiques au sujet d'une classe particulière, vous devez d'abord activer les statistiques globales dans l'instruction `ipgpc.classify action.` Pour plus d'informations, reportez-vous à la section “Instruction `action`” à la page 101.

Utilisez l'instruction `enable_stats TRUE` lorsque vous souhaitez activer la collecte de statistiques pour une classe. Si vous n'avez pas besoin de connaître les statistiques d'une classe, il suffit de spécifier `enable_stats FALSE` ou de supprimer l'instruction `enable_stats`.

Le trafic sur un réseau IPQoS non défini de façon explicite est relégué vers la *classe par défaut*.

Clause `filter`

Les *filtres* sont constitués de sélecteurs qui regroupent les flux de trafic en classes. Ces sélecteurs définissent plus précisément les critères à appliquer au trafic de la classe créée dans la clause class. Si un paquet répond à tous les critères des sélecteurs du filtre de priorité supérieur, il est considéré comme un membre de la classe du filtre. Pour obtenir la liste complète des sélecteurs applicables au classificateur `ipgpc`, reportez-vous au Tableau 6-1, “Sélecteurs de filtre pour le classificateur IPQoS”.

Vous définissez les filtres dans le fichier de configuration IPQoS à l'aide d'une *clause filter* correspondant à la syntaxe suivante :

```
filter {
       name filter-name
       class class-name
       parameters (selectors)
       }
```

Clause `params`

La clause `params` contient les instructions de traitement pour le module défini dans l'instruction action. Respectez la syntaxe suivante pour la clause `params` :

```
params {
           parameters
           params-stats | ""
       }
```

Dans la clause `params`, vous utilisez les paramètres qui se rapportent au module.

La valeur *params-stats* définie dans la clause `params` est soit `global_stats TRUE`, soit `global_stats FALSE`. L'instruction `global_stats TRUE` a pour effet d'activer les statistiques de type UNIX pour l'instruction `action` à partir de laquelle les statistiques globales sont

demandées. Pour afficher les statistiques, exécutez la commande `kstat`. Vous devez activer les statistiques de l'instruction `action` avant d'activer les statistiques par classe.

Index

P

Q

R

S

T

V