Configuration de la qualité de service de réseau local pour la téléphonie IP Cisco

Lorsque le nombre de périphériques et le trafic LAN augmentent, la segmentation du trafic, le contrôle d'accès et la hiérarchisation du trafic deviennent des éléments clés. Les commutateurs administrables Cisco Small Business incluent une gestion réseau avancée ainsi que d'autres fonctionnalités qui prennent en charge la croissance de l'entreprise en offrant un plus grand contrôle du trafic réseau.

Produits proposés

Ce document décrit l'utilisation d'un commutateur administrable de la gamme Cisco Small Business série 300 (modèle SF 300-48P) avec divers ports PoE (Power over Ethernet) et non-PoE. Pour plus de détails sur d'autres commutateurs administrables de la gamme Cisco série 300, consultez : http://www.cisco.com/cisco/go/300switches.

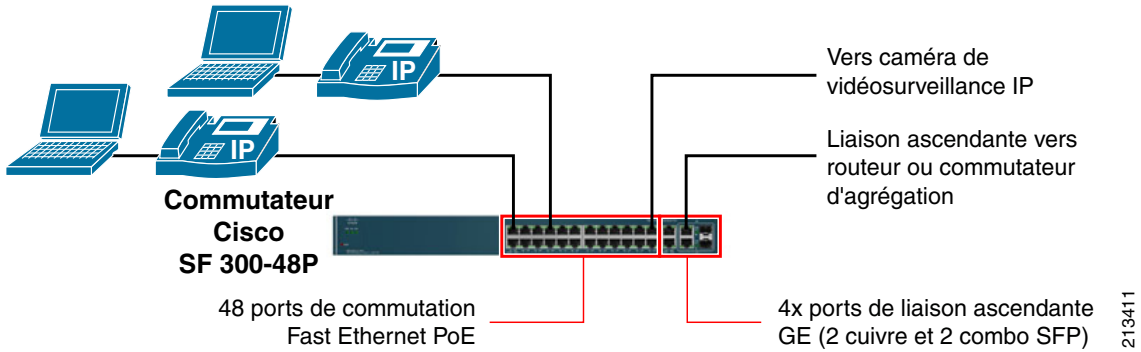
La Figure 1 présente un exemple de l'utilisation du commutateur Cisco SF 300-48P dans une installation de réseau local de PME.

Pourquoi utiliser la qualité de service (QoS)?

La qualité de service (QoS, quality of service) dans un périphérique réseau aide les applications telles que la voix, le flux vidéo et d'autres applications liées au temps à attribuer une priorité appropriée et une bande passante adéquate au trafic en cas de congestion du réseau. Les appels voix et le flux vidéo peuvent devenir instables et perturbés si le trafic global dépasse la capacité du réseau, voilà pourquoi le trafic voix et vidéo doit bénéficier d'un traitement prioritaire assuré par la classification QoS. En outre, QoS peut fournir des niveaux configurés de bande passante au trafic d'autres importantes applications lors d'une congestion du réseau, garantissant ainsi la continuité des activités lors de tels événements. Bien que QoS ait une importance critique dans un routeur WAN, un commutateur de réseau local peut lui aussi être encombré, bien que moins fréquemment ; par conséquent, un commutateur nécessite également une configuration QoS pour éviter toute dégradation potentielle de la qualité de la voix ou de la vidéo.

Ce document décrit la procédure de configuration d'un commutateur Cisco SF 300-48P avec la qualité de service (QoS) pour prendre en charge la voix, le flux vidéo (tel que la vidéosurveillance), et d'autres types de trafic fréquemment présents dans un réseau de PME. Reportez-vous à la Figure 1.

Figure 1 Réseau local avec qualité de service



Conseils de conception

Classification du trafic

Dans les solutions de conception Cisco Smart Design, la qualité de service répartit le trafic en plusieurs classes où chaque classe est configurée de manière à obtenir le type de traitement QoS qu'elle nécessite. Dans les solutions de conception Smart Designs, la classe de trafic d'un paquet est identifiée par le point DSCP (Differentiated Services Code Point, point de code de services différenciés) ou la valeur CoS (class of service, classe de service) du paquet. DSCP est un champ de 6 bits dans l'en-tête de paquet IP auquel une valeur spécifique peut être affectée pour représenter le type de traitement QoS que nécessite le trafic. Vous pouvez configurer QoS pour traiter tous les paquets présentant une valeur DSCP spécifique (ou plusieurs valeurs DSCP spécifiques) comme une classe de trafic unique, distincte des autres classes de trafic. Les classes de trafic courantes, telles que définies dans les guides Smart Designs, sont présentées dans les deux premières colonnes du Tableau 1.

Bien que les commutateurs transfèrent le trafic en fonction de l'en-tête Ethernet et non pas de l'en-tête IP d'un paquet, les commutateurs administrables de la gamme Cisco Small Business série 300 lisent l'en-tête IP pour classer le trafic selon le code DSCP transporté par les paquets IP.

Un commutateur peut également classer les paquets en fonction d'une valeur spécifique du champ CoS de 3 bits se trouvant dans l'en-tête Ethernet des paquets 802.1q.

Remarque Pour certains types d'actions QoS, les commutateurs de la gamme Cisco série 300 utilisent également des classes de trafic basées sur une liste de contrôle d'accès (ACL, access control list) correspondante.

Le code DSCP *EF* désigne l'acheminement expédié (Expedited Forwarding), qui impose que les paquets de cette classe soient acheminés avec le moins de délai, de gigue ou de perte de paquets possible. Ce DSCP est donc applicable à la classe de trafic voix ou vidéo en temps réel.

En général, les codes DSCP commençant par *AF* (Assured Forwarding, acheminement assuré) peuvent être compris dans les plages AF11–AF13, AF21–AF23, AF31-AF33 ou AF41–AF43. L'acheminement assuré impose que le trafic de ces classes soit assuré d'être acheminé tant qu'il ne dépasse pas une certaine limite de bande passante configurable. Les deux chiffres suivant le préfixe *AF* représentent la classe AF et la préséance de rejet (élevée, faible ou moyenne). Par exemple, dans AF31, la classe AF est 3 et la préséance de rejet est 1 (préséance de rejet 1= faible rejet, 2= rejet moyen, 3 = rejet élevé).

En cas d'encombrement entre classes de trafic présentant différentes classes AF (AF1x, AF2x, AF3x et AF4x), le trafic de classe AF plus élevé bénéficie d'une préférence d'acheminement. Cependant, si un encombrement se produit entre classes de trafic de même classe AF (par exemple entre AF11, AF12, AF13), le trafic présentant une préséance de rejet élevé est rejeté en premier.

Les codes DSCP commençant par *CS* (Class Selector, sélecteur de classe) sont compris entre CS0 et CS7, et ont été créés de manière à être rétrocompatibles avec les systèmes QoS qui utilisent la préséance IP (et non DSCP) pour la classification du trafic. Cependant, en pratique, une combinaison de marquages de trafic CS- et AF- a tendance à prévaloir. Les code CS n'ont pas de préséance de rejet.

Marquage du trafic

Le marquage est le processus visant à définir ou à changer le code DSCP ou la valeur CoS d'un paquet en fonction du type de trafic. Les solutions de conception Cisco Smart Designs marquent le trafic de la façon suivante :

- Le trafic issu d'équipements raccordés tels que serveurs, stockage en réseau (NAS, network-attached storage), ou caméras de vidéosurveillance est marqué pour se conformer à la classification de trafic décrite dans la section précédente, si la source de trafic marque le trafic différemment, sinon il n'est pas approuvé.
- Le trafic entrant avec des codes DSCP autres que ceux répertoriés dans le Tableau 1 est marqué DSCP CS0 (service au mieux).

Tableau 1 Noms de classes de trafic, DSCP et valeurs CoS

Description du trafic	Nom de la classe de trafic	Code DSCP (valeur décimale)	CoS
Trafic support voix	Voix	EF (46)	5
Trafic de flux vidéo ; par exemple, à partir d'une caméra de vidéosurveillance (en option)	Flux vidéo	CS4 (32)	4
Trafic de signalisation pour voix/vidéo, etc.	Signalisation	CS3 (24), AF31 (26)	3
Trafic de contrôle interréseau ; paquets de contrôle, par exemple acheminement dynamique généré par des équipements de réseau	Contrôle interréseau	CS6 (48)	6
Trafic d'importantes applications métiers (transactionnelles) (en option)	Transactionnel	CS2 (16), AF21 (18)	2
Paquets BPDU (Bridge Protocol Data Unit) échangés entre des commutateurs (uniquement sur les commutateurs)	BPDU	N/A	7
Le reste du trafic	Trafic au mieux	CS0 (0)	0

Mise en file d'attente du trafic

La mise en file d'attente est employée pour permettre à diverses classes de trafic de partager de la bande passante, et à certains types de trafic (tels que la voix et la vidéo) d'obtenir un traitement prioritaire sur d'autres types de trafic. Le commutateur de la gamme Cisco série 300 a quatre files d'attente matérielles. Chacune de ces files d'attentes peut être définie comme une file d'attente prioritaire pour l'acheminement expédié du trafic placé dans la file d'attente, ou comme une file d'attente WRR (weighted round robin, circuit cyclique pondéré) pouvant partager de la bande passante avec d'autres files d'attente WRR dans une proportion configurée. En outre, chaque file d'attente peut être individuellement mise en forme à un débit maximal ; le trafic excédentaire supérieur au débit mis en forme est rejeté. Notez qu'un port de commutateur peut également être configuré pour contrôler le trafic ; dans ce cas, il peut également rejeter le trafic allant au-delà de son débit configuré. Chaque file d'attente WRR est configurée avec une pondération (ou un pourcentage de bande passante). Le commutateur achemine le trafic provenant de ces files d'attente proportionnellement à leur pondération, garantissant ainsi un pourcentage minimal de bande passante disponible pour chaque file d'attente WRR après le traitement des files d'attente prioritaires.

Cette conception affecte le trafic aux quatre files d'attente matérielles des commutateurs Cisco Sx 300 comme le montre le Tableau 1 (ces valeurs peuvent être modifiées dans un déploiement si nécessaire)

Tableau 1 Affectation de files d'attente de trafic

Nom de la classe de trafic	DSCP	N° de file d'attente	Type de file d'attente	Pondération WRR.	Remarques
Voix	EF	4	Prioritaire		Mis en forme à 10 % du débit de ligne
Flux vidéo	CS4	3	Prioritaire		Mis en forme à 40 % du débit de ligne
Signalisation	CS3, AF31				
Contrôle interréseau	CS6				
BPDU	CS7				
Transactionnel	CS2, AF21	2	WRR	1 (33,33 %)	Équivalant à 33,33 % de la bande passante restante après traitement des deux files d'attentes prioritaires
Trafic au mieux	CS0	1	WRR	2 (66,67 %)	66,67 % de la bande passante restante

Dans la conception décrite au Tableau 1, le trafic de la file d'attente 4 (file d'attente prioritaire avec la priorité la plus élevée) est traité en premier. Lorsque la file d'attente 4 est vide, le trafic de la file d'attente 3 (la file d'attente prioritaire avec la plus basse priorité) est traité. C'est uniquement lorsque ces files d'attente sont vides que le reste de la bande passante disponible est partagé entre les files d'attente WRR en proportion de leurs pondérations. Les pondérations indiquées ci-dessus fournissent 33,67 % du reste de la bande passante à la file d'attente 1 et 66,67 % à la file d'attente 2.

Contrôle/mise en forme des files d'attente prioritaires

Les files d'attente prioritaires n'ont pas de limite de bande passante dans leur configuration par défaut ; elles peuvent donc potentiellement utiliser trop de bande passante, défavorisant ainsi d'autres files d'attente. Par conséquent, cette conception impose une limite de débit sur chaque file d'attente prioritaire. Bien que les débits de contrôle des files d'attente prioritaires individuelles puissent varier selon le déploiement, une recommandation générale consiste à limiter le trafic prioritaire total sur toute interface à pas plus de 50 % de la bande passante de l'interface. Cette conception met en forme le trafic voix et vidéo à 10 % et 40 % de la bande passante de l'interface, en partant du principe que le trafic voix et vidéo réel attendu sera bien en dessous de ces débits mis en forme.

Suppression d'encombrement TCP (en option)

La fonction de suppression d'encombrement TCP atténue l'effet de la synchronisation TCP qui entraîne une sous-utilisation du réseau. Cette focntion contribue à améliorer les performances du trafic TCP en rejetant des paquets de façon aléatoire avant qu'une congestion du réseau ne se produise.

Sans suppression d'encombrement TCP, lorsqu'une file d'attente se remplit, tous les autres paquets entrants sont rejetés. Cette soudaine augmentation des rejets de paquets peut affecter un grand nombre d'applications TCP. Toutes ces applications seront simultanément forcées de réduire considérablement leur débit d'envoi, puis de l'augmenter de nouveau progressivement. Lorsque que le débit d'envoi croissant dépasse une certaine limite de remplissage des files d'attente, la file d'attente rejette de nouveau tous les paquets entrants. Cela entraîne une séquence répétitive de surcharge et de sous-utilisation du réseau.

La suppression d'encombrement TCP atténue ce problème en rejetant de façon aléatoire des paquets des files d'attente avant que celles-ci ne soient saturées. Cette solution est préférable au rejet de tout le trafic entrant après saturation de la file d'attente. La suppression d'encombrement TCP étale dans le temps les rejets de paquets, évitant ainsi le rejet simultané de paquets pour un grand nombre de flux TCP.

Dans les conceptions Cisco Smart Designs, cette fonction est essentielle pour le routeur WAN, mais est facultative sur les commutateurs de réseau local, car sa configuration sur le routeur WAN couvre également le trafic acheminé sur le réseau local. Cependant, si le routeur WAN ne prend pas en charge la suppression d'encombrement TCP, cette fonction peut être activée sur les commutateurs de réseau local.

Conseils de configuration

La configuration décrite dans cette section concerne chaque port d'un commutateur de la gamme Cisco série 300 (déployé en tant que commutateur d'accès ou commutateur d'agrégation dans une topologie de conception Cisco Smart Designs) avec des fonctionnalités de mise en file d'attente permettant de prendre en charge les classes de trafic définies ci-dessus. En outre, cette configuration illustre comment configurer un port pour contrôler et marquer le trafic entrant provenant d'un appareil raccordé au commutateur.

Comme les configurations non enregistrées sont perdues lors du redémarrage du commutateur, il convient de les enregistrer fréquemment dans le fichier de configuration de démarrage en procédant comme suit :

Étape 1 Cliquez sur **Administration > File Management (gestion de fichiers) > Copy (Copier)/Save Configuration (Enregistrer la configuration)**.

La page Copy/Save Auto Configuration s'ouvre.

Étape 2 Sélectionnez le nom du fichier source (Source File Name) à copier comme *Running configuration (configuration active)*.

Étape 3 Sélectionnez le nom de fichier de destination (Destination File Name) comme *Startup configuration (Configuration de démarrage)*.

Étape 4 Cliquez sur **Apply (appliquer)**. Le fichier de configuration est alors enregistré.

Modes QoS de base et avancé

Les commutateurs Cisco Sx300 peuvent être configurés en mode QoS de base ou avancé. Le mode QoS de base prend en charge la fonctionnalité de mise en file d'attente requise (mise en file d'attente prioritaire et WRR) et la mise en forme des files d'attente prioritaires. Cependant, cette conception utilise le mode QoS avancé, car ce mode est requis pour contrôler/marquer le trafic provenant de ports de commutateur spécifiques. Il est courant de marquer tout le trafic provenant de sources de trafic telles que serveurs, NAS et caméras vidéo, si elles ne marquent pas le trafic, ou si elles ne sont approuvées (pas sous le contrôle administratif de l'administrateur réseau, ou peuvent être potentiellement exploitées par un attaquant). Le mode QoS avancé permet de spécifier le trafic pour un tel contrôle/marquage avec une grande granularité ; vous pouvez spécifier les adresses IP/sous-réseaux source/destination, leurs protocoles TCP/UDP et leurs ports. Si un tel contrôle/marquage des flux de trafic n'est pas requis dans un déploiement, le mode QoS de base est adéquat.

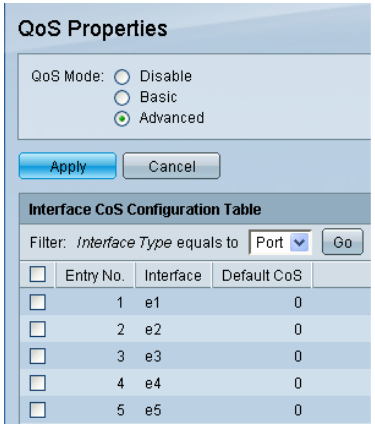
La procédure de configuration suivante part du principe que vous pouvez accéder à l'écran d'administration Web du commutateur Cisco SF 300-48P. Elle suppose également que le VLAN de données et le VLAN voix ont été créés sur le commutateur et ailleurs dans le réseau si nécessaire, et que le commutateur est connecté au routeur WAN, comme dans la Figure 1.

Pour configurer la qualité de service LAN, procédez comme suit :

Étape 1 Sélectionnez **Quality of Service (qualité de service) > General > QoS Properties (propriétés de qualité de service)**.

L'écran QoS Properties s'affiche, comme dans la Figure 2.

Figure 2 Écran QoS Properties



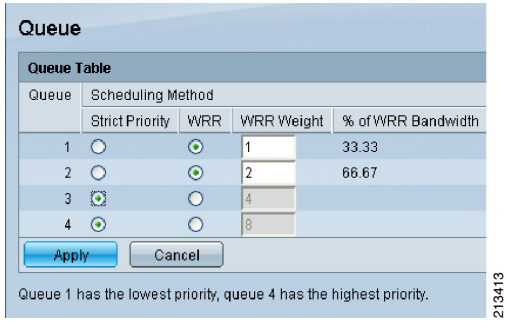
Étape 2 Sélectionnez *Advanced (avancé)* dans le champ QoS Mode (mode QoS), et cliquez sur **Apply (appliquer)**.

Dans le tableau Interface CoS Configuration Table (tableau de configuration CoS de l'interface), vérifiez que la classe de service (CoS) par défaut pour tous les ports du commutateur est 0.

Étape 3 Sélectionnez **Quality of Service > General > QoS Properties > Queue (file d'attente)**.

L'écran Queue s'affiche, comme dans la Figure 3.

Figure 3 Écran Queue



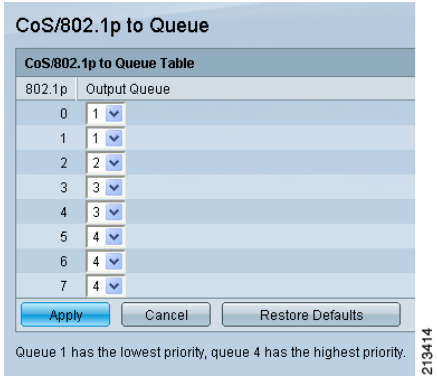
Étape 4 Dans l'écran Queue, configurez les files d'attente 1 et 2 comme files d'attente WRR avec des pondérations 1 et 2 ; configurez les files d'attente 3 et 4 comme files d'attentes prioritaires ; puis, cliquez sur **Apply (appliquer)**.

La file d'attente 4 est dédiée à la voix, la file d'attente 3 au flux vidéo (si déployé). En outre, la file d'attente 3 transporte également du trafic de signalisation. Notez que la configuration de ces files d'attentes prioritaires pour la voix et la vidéo est correcte même lorsque la voix et la vidéo ne sont pas déployées, car les files d'attente prioritaires ne réservent pas de bande passante ; tout le trafic inutilisé est employé par les autres classes de trafic.

Étape 5 Sélectionnez **Quality of Service > General > QoS Properties > QoS/802.1p to Queue (QoS/802.1p vers file d'attente)**.

L'écran CoS/802.1P to Queue s'affiche, comme dans la Figure 4.

Figure 4 Écran CoS/802.1P to Queue

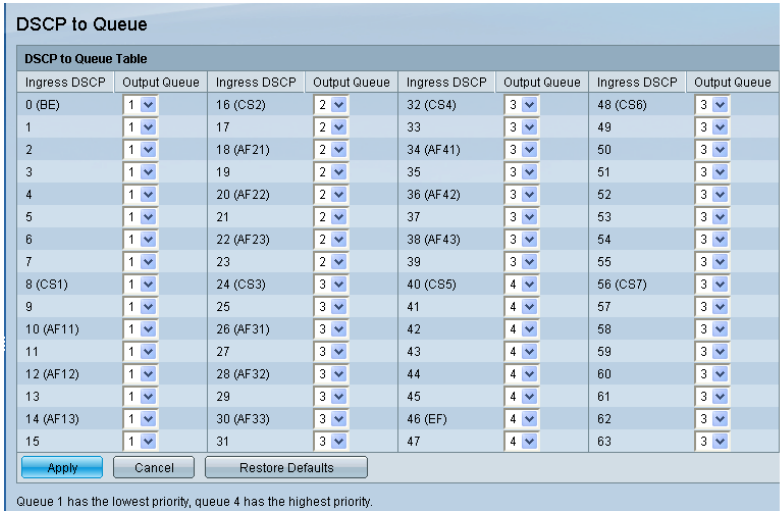


Étape 6 Vérifiez que les valeurs CoS sont mappées comme dans la Figure 4, ou changez le mappage en conséquence, et cliquez sur **Apply (Appliquer)**.

Étape 7 Sélectionnez **Quality of Service > General > QoS Properties > DSCP to Queue (DSCP vers file d'attente)**.

L'écran DSCP to Queue s'affiche, comme dans la Figure 5.

Figure 5 Écran DSCP to Queue

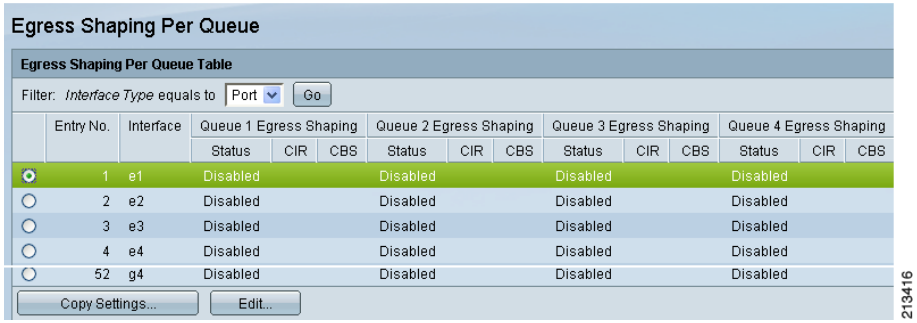


Étape 8 Vérifiez que les DSCP sont mappés aux files d'attente comme dans la Figure 5, ou changez le mappage en conséquence, et cliquez sur **Apply**.

Étape 9 Sélectionnez **Quality of Service > General > QoS Properties > Egress Shaping per Queue (mise en forme de sortie par file d'attente)**.

L'écran Egress Shaping per Queue s'affiche, comme dans la Figure 6.

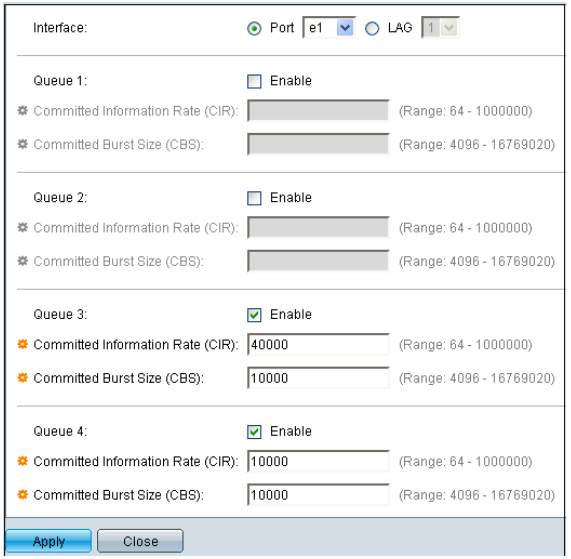
Figure 6 Écran Egress Shaping per Queue



Étape 10 Dans l'écran Egress Shaping Per Queue, sélectionnez le premier port E1 comme dans la Figure 6, et cliquez sur **Edit (modifier)**.

L'écran contextuel présenté dans la Figure 7 s'affiche.

Figure 7 Écran contextuel



Étape 11 Dans l'écran contextuel présenté dans la Figure 7, procédez comme suit :

a. Cliquez sur les boutons de sélection pour activer la mise en forme sur les files d'attente 3 et 4.

b. Saisissez les valeurs indiquées dans la Figure 7 pour mettre en forme la file d'attente 3 avec les valeurs CIR 40 000 Kbit/s et CBS 10000.

c. Mettez en forme la file d'attente 4 avec les valeurs CIR 10000 Kbit/s et CBS 10000.

d. Cliquez sur **Apply**.

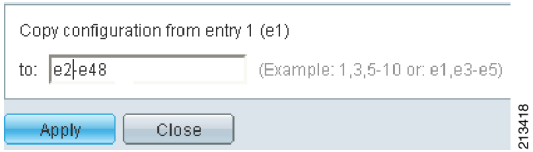
e. Lorsque « Success » (réussite) s'affiche, cliquez sur **Close (fermer)**.

L'écran contextuel se ferme, puis l'écran Egress Shaping Per Queue s'ouvre. Vérifiez que le port E1 a maintenant les valeurs de mise en forme saisies dans l'écran Egress Shaping per Queue.

Étape 12 Dans l'écran Egress Setting per Queue (configuration de sortie par file d'attente), cliquez sur **Copy Settings (copier les paramètres)** pour copier la configuration de mise en forme du port E1 sur tous les autres ports du commutateur.

Dans l'écran contextuel, saisissez la plage de ports Fast Ethernet du commutateur, comme dans la Figure 8, puis cliquez sur **Apply**.

Figure 8 Écran Copy Configuration (copier la configuration)



L'écran contextuel Copy Configuration se ferme. Vérifiez que l'écran Egress Shaping Per Queue affiche maintenant les valeurs de mise en forme de tous les ports du commutateur.

Répétez cette étape pour les ports Gigabit Ethernet (G1 à G4). Utilisez CIR=400000 et CBS=100000 pour la file d'attente 3 ; et CIR=100000 et CBS=100000 pour la file d'attente 4.

Facultatif : cette étape et les suivantes sont requises si vous souhaitez contrôler et/ou marquer le trafic entrant d'un équipement connecté au commutateur. Cet exemple contrôle le trafic d'une caméra de vidéosurveillance (adresse IP 10.1.20.5) à 500 Kbit/s. Le trafic dépassant les 500 Kbit/s est rejeté, tandis que le le trafic respectant le débit de contrôle est marqué avec DSCP CS4.

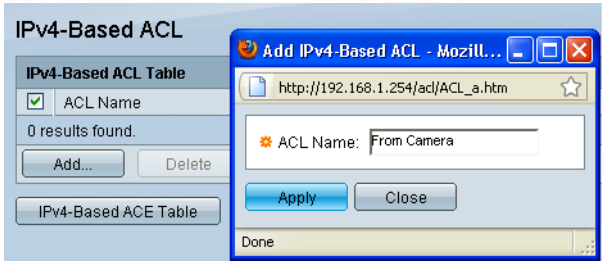
Cette procédure inclut les étapes principales suivantes :

- Création d'une classe de trafic utilisant une liste de contrôle d'accès (ACL) qui correspond à l'adresse IP de la caméra vidéo
- Création d'une table de politiques QoS qui contient un ou plusieurs mappages de classes de politiques
- Création d'un mappage de classes de politiques qui spécifie les actions de contrôle/marquage à effectuer pour la classe de trafic spécifique
- Association du mappage de classes de politiques au port du commutateur qui est connecté à la caméra vidéo

Étape 13 Pour créer une liste ACL qui identifie le trafic provenant de la caméra, sélectionnez **Access Control (contrôle d'accès) > IPv4 based ACL (ACL basée sur IPv4)**.

L'écran IPv4-Based ACL s'affiche, comme dans la Figure 9.

Figure 9 Écran IPv4-Based ACL



Étape 14 Cliquez sur la zone de sélection **ACL Name (nom d'ACL)**, puis cliquez sur **Add (ajouter)**.

L'écran contextuel Add IPv4-Based ACL (ajouter une liste de contrôle d'accès basée sur IPv4) s'affiche, comme dans la Figure 9.

Étape 15 Saisissez le nom de l'ACL (par exemple, *From Camera*), et cliquez sur **Apply**.

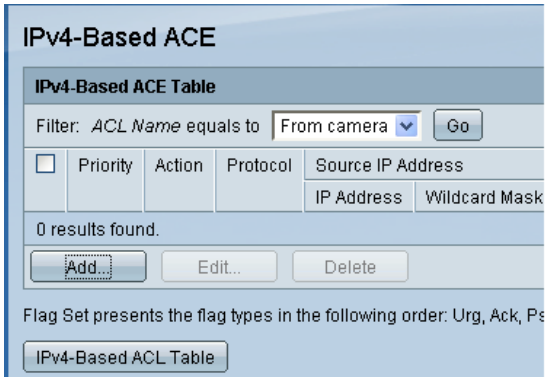
L'écran de saisie des données se ferme, et les données saisies sur l'écran IPv4-Based ACL s'affichent.

Étape 16 Cliquez sur le bouton **IPv4-Based ACE Table (tableau des listes de contrôle d'accès IPv4)**.

L'écran IPv4-Base ACE s'affiche (partiellement illustré dans la Figure 10).

Remarque Une ACL est composée d'une ou plusieurs ACE (access control expressions, expressions de contrôle d'accès).

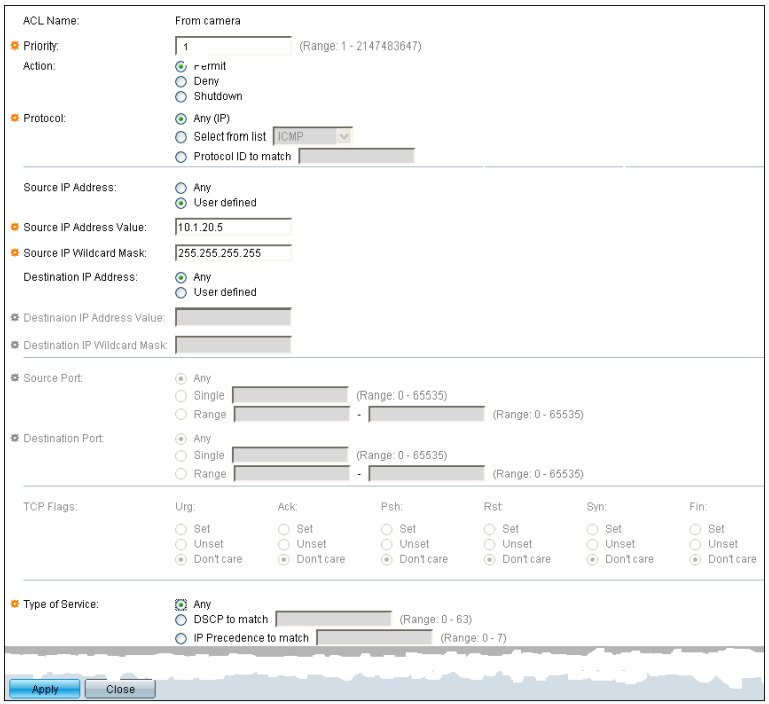
Figure 10 Écran Add IPv4-Based ACE



Étape 17 Cliquez sur **Add (ajouter)**.

L'écran partiellement illustré dans la Figure 11 s'affiche pour saisir les détails des entrées de contrôle d'accès (ACE) à inclure dans l'ACL *From Camera*. Plusieurs ACE peuvent être incluses si nécessaire.

Figure 11 Saisie des détails ACE



Étape 18 Saisissez les données ACE comme suit :

a. Priorité 1 (la priorité détermine l'ordre dans lequel plusieurs ACE, le cas échéant, d'une ACL sont évaluées)

b. Adresse IP source, celle de la caméra, 10.1.20.5

c. Masque générique IP source, 255.255.255.255

Étape 19 Cliquez sur **Apply (appliquer)**.

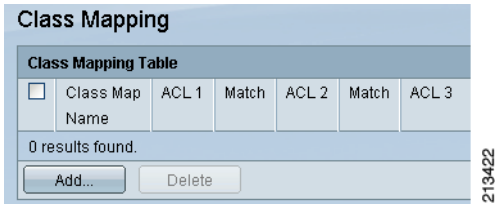
L'ACL avec l'ACE que vous venez de saisir est alors créée.

Remarque Vous pouvez également spécifier l'adresse IP/sous réseau, le protocole et le port TCP/UCP de destination dans l'entrée ACE si applicable pour une ACE.

Étape 20 Sélectionnez **Quality of Service > QoS Advanced Mode > Class Mapping (mappage de classe)**.

L'écran Class Mapping s'affiche, comme dans la Figure 12. Un mappage de classe définit la règle pour identifier la classe de trafic (dans ce cas, il utilise une ACL prédéfinie à associer au trafic provenant de la caméra vidéo, tel qu'illustré ci-dessous).

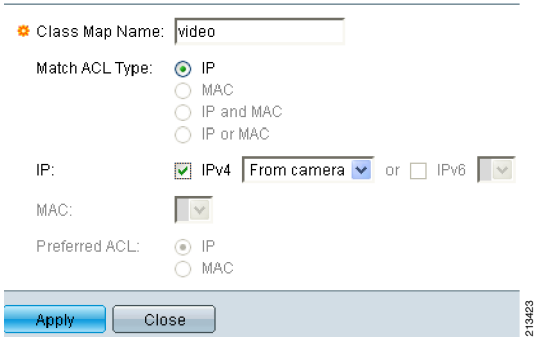
Figure 12 Écran Class Mapping



Étape 21 Cliquez sur **Add** pour ajouter un nouveau mappage de classe utilisant l'ACL que vous venez de créer.

L'écran contextuel servant à créer un nouveau mappage de classe apparaît, comme dans la Figure 13.

Figure 13 Création d'un nouveau mappage de classe



Étape 22 Dans l'écran contextuel, procédez comme suit :

a. Dans le champ Class Map Name (Nom du mappage de classe), saisissez *video*.

b. Dans le champ Match ACL Type (type d'ACL correspondant), cochez **IP**.

c. Dans le champ IP, cochez **IPv4**.

d. Sélectionnez l'ACL **From Camera** dans la liste déroulante.

e. Cliquez sur **Apply**, et vérifiez que l'opération a réussi.

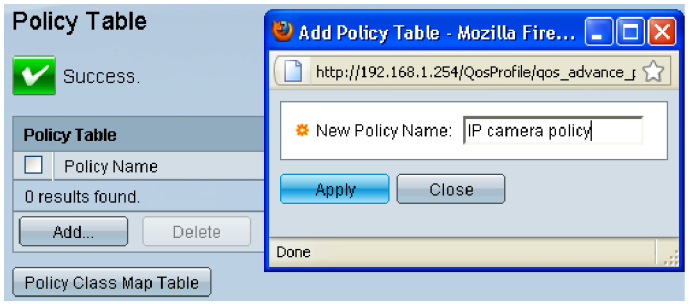
Étape 23 Sélectionnez **Quality of Service > QoS Advanced Mode > Policy Table (tableau de politiques)**.

L'écran Policy Table s'affiche.

Étape 24 Cliquez sur **Add** pour ajouter une nouvelle politique.

L'écran contextuel présenté dans la Figure 14 s'affiche.

Figure 14 Écran Policy Table



Étape 25 Saisissez le nom du tableau de politique (*IP camera policy* dans cet exemple).

Étape 26 Cliquez sur **Apply**.

L'écran contextuel se ferme et le message « Success » (réussite) s'affiche sur l'écran Policy Table, avec le nom de la politique venant d'être créée.

Étape 27 Pour ajouter la politique du trafic réel (contrôle, marquage, etc.) à inclure dans le tableau de politiques venant d'être créé, sélectionnez **Quality of Service > QoS Advanced Mode > Policy Class Map (mappage de classe de politique)**.

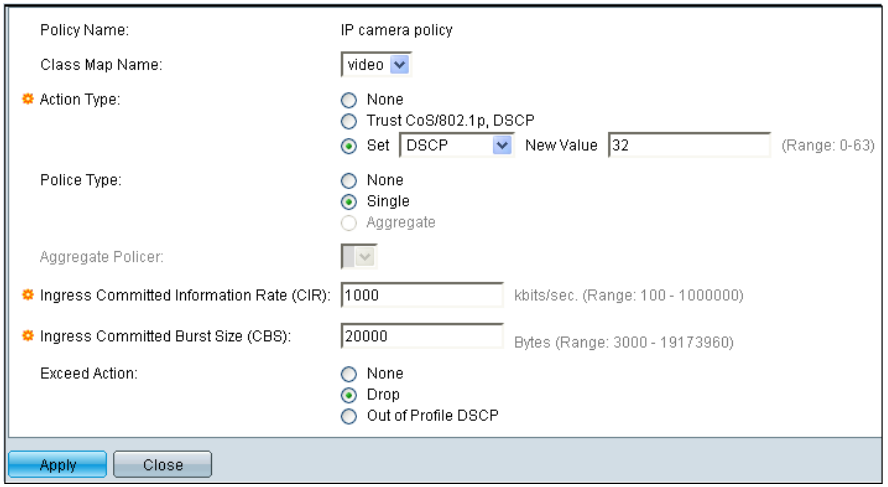
L'écran Policy Class Maps (mappages de classe de politique) apparaît, comme dans la Figure 15.

Figure 15 Écran Policy Class Maps

Étape 28 Sélectionnez le nom de la politique (*IP camera policy*) dans le menu déroulant et cliquez sur **Add**.

L'écran présenté dans la Figure 16 s'affiche pour ajouter les actions de contrôle/marquage à effectuer pour le trafic correspondant à cette politique.

Figure 16 Ajout d'actions de contrôle/marquage



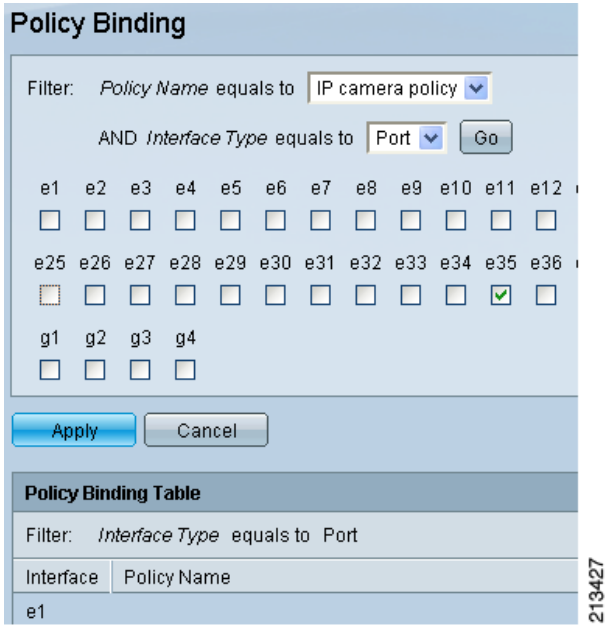
Étape 29 Dans l'écran présenté dans la Figure 16, procédez comme suit :

a. Sélectionnez le mappage de classe **video** dans la liste déroulante.
b. Cliquez sur la case d'option pour sélectionner l'opération Set (définir), et sélectionnez **DSCP** dans la liste déroulante correspondante.
c. Saisissez *32* (c'est-à-dire, DSCP CS4) dans le champ New Value (nouvelle valeur). DSCP est alors défini à CS4 pour tout le trafic correspondant au mappage de classe *video*.
d. En partant du principe que vous souhaitez contrôler le trafic de la caméra IP à 1 Mbit/s, et rejeter le trafic excédentaire, saisissez les valeurs *1000 Kbit/s* dans le champ Committed Information Rate (débit d'informations validées d'entrée), puis *20000* dans le champ Ingress Committed Burst Size (taille de rafale validée d'entrée).
e. Dans le champ Exceed Action (action pour trafic excédentaire), cochez **Drop (rejeter)**.
f. Cliquez sur **Apply**.
g. Vérifiez que « Success » s'affiche pour confirmer la réussite de l'opération.
h. Cliquez sur **Close** pour fermer l'écran contextuel.

Étape 30 Cliquez sur **Quality of Service** > Advanced Mode > Policy Binding (liaison de politique).

L'écran Policy Binding s'affiche, comme dans la Figure 17.

Figure 17 Écran Policy Binding



Cet écran sert à appliquer la politique que vous venez de créer au port de commutateur connecté à la caméra de vidéosurveillance IP (port de commutateur *E35* dans cet exemple).

Étape 31 Dans l'écran Policy Binding (liaison de politique), procédez comme suit :

a. Sélectionnez le nom de la politique (*IP camera policy*) dans la liste déroulante des politiques à appliquer.

b. Sélectionnez le type d'interface *port* dans la liste déroulante.

c. Cliquez sur la case de sélection indiquant le port du commutateur (*E 35* dans cet exemple) où la politique *IP camera policy* doit être appliquée (vous pouvez également appliquer une politique spécifique sur plusieurs ports du commutateur, si nécessaire).

d. Cliquez sur **Apply**.

Une fois l'opération effectuée, le message « Success » s'affiche à l'écran, et le nom de la politique (*IP camera policy*) s'affiche en regard du port E35 dans la section Policy Binding Table (tableau de liaison de politiques).

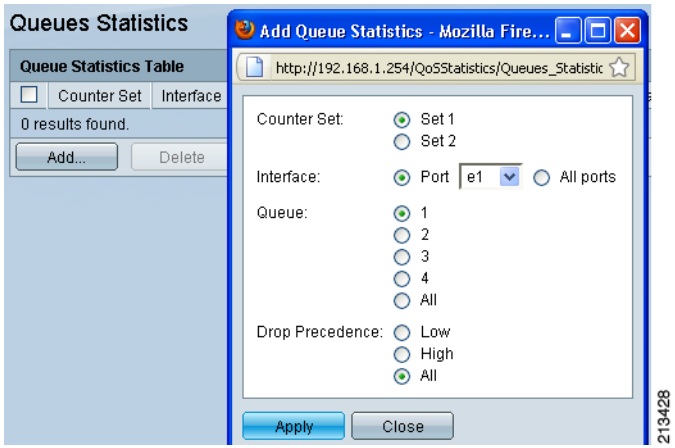
La configuration de la qualité de service sur le commutateur est maintenant terminée.

Vérification

Étape 1 Cliquez sur **Quality of Service > QoS Statistics (statistiques de qualité de service) > Queues Statistics (statistiques des files d'attente)**.

L'écran Queues Statistics s'affiche, ce qui vous permet de configurer jusqu'à deux jeux de compteurs de paquets, comme le montre la Figure 18.

Figure 18 Écran Queues Statistics



Étape 2 Cliquez sur **Add** pour ajouter le premier jeu de compteurs.

L'écran contextuel Add Queue Statistics (ajouter des statistiques de file d'attente) s'affiche, comme dans la Figure 18.

Étape 3 Dans l'écran contextuel Add Queue Statistics, procédez comme suit :

a. Saisissez les valeurs pour choisir le port de commutateur, la file d'attente et les valeurs de préséance de rejet pour les statistiques.

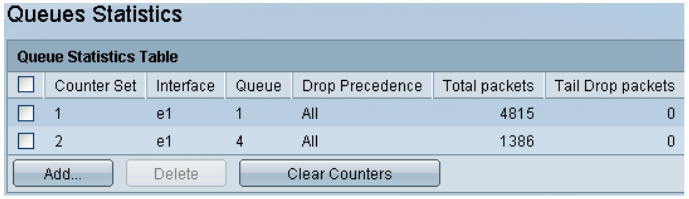
b. Cliquez sur **Apply (appliquer)**.

c. Vérifiez que « Success » s'affiche pour confirmer la réussite de l'opération.

d. Cliquez sur **Close** (Fermer).

Le nombre réel de paquets s'affiche, comme dans la Figure 19.

Figure 19 Vérification des nombres de paquets réels



Vous pouvez réinitialiser les compteurs en cliquant sur le bouton **Clear Counters (réinitialiser les compteurs)**. Vérifiez périodiquement que le nombre de paquets augmente dans les diverses files d'attente conformément à la configuration de la qualité de service.

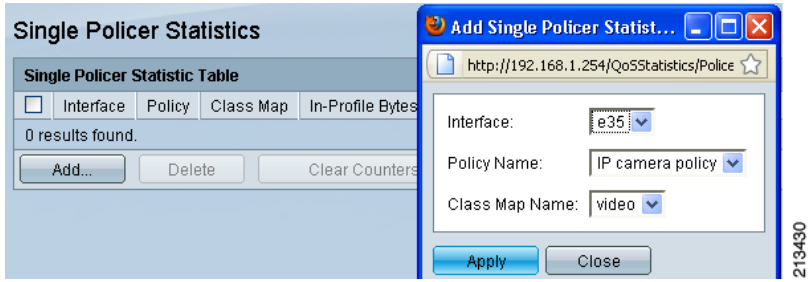
Étape 4 Sélectionnez **Quality of Service > QoS Statistics > Single Policer Statistics (statistiques d'un contrôleur spécifique)**.

L'écran Single Policer Statistics s'affiche, qui vous permet de spécifier le port, le nom de la politique, etc., pour lesquels les statistiques sont requises.

Étape 5 Cliquez sur **Add (ajouter)**.

L'écran contextuel Add Single Policer (ajouter un contrôleur individuel) s'affiche comme dans la Figure 20.

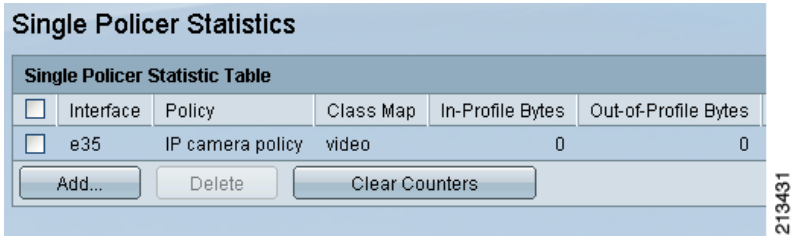
Figure 20 Écran contextuel Add Single Policer



Étape 6 Entrez le nom du port du commutateur (*E35*), le nom de la politique et le nom du mappage de classes concernés, puis cliquez sur **Apply**.

Les statistiques de contrôle s'affichent comme dans la Figure 21.

Figure 21 Écran Single Policer Statistics



Pour tester le bon fonctionnement du contrôle, réglez temporairement le débit de contrôle à une faible valeur et vérifiez que le trafic excédentaire supérieur au débit de contrôle est comptabilisé comme octets hors profil (Out-of-Profile).

Résumé

Ce document définit les divers types de fonctionnalités QoS pouvant être utilisées dans un réseau, plus particulièrement sur le réseau local. Lorsqu'une qualité de service est configurée dans les commutateurs de la gamme Cisco Small Business série 300, ces derniers peuvent fournir le traitement QoS approprié pour les classes de trafic de la conception Cisco Smart Designs. Le commutateur administrable de la gamme Cisco série 300 prend en charge des fonctionnalités QoS supplémentaires pouvant être utilisées si nécessaire.

Pour plus d'informations sur la configuration des commutateurs administrables de la gamme Cisco série 300, consultez le guide de l'administrateur à l'adresse URL suivante : http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf.