

Configuration et optimisation du trafic multicast

Les commutateurs Cisco Small Business série 300/200 offrent des solutions multicast puissantes et faciles à gérer aux PME qui font attention à leurs dépenses. Ce document explique comment une solution de commutation économique peut être mise en œuvre pour optimiser le trafic multicast dans un seul bureau ou réseau local (LAN) avec un ou plusieurs commutateurs Cisco série 300/200. Il fournit des conseils de conception pour l'optimisation du trafic multicast dans des environnements LAN ou de couche 2 à l'aide de commutateurs Cisco série 300/200, ainsi que des exemples de configuration.

Pourquoi le multicast ?

Le multicast permet qu'un seul flux de trafic IP d'une source soit répliqué sur un réseau vers plusieurs destinations ou récepteurs. La source n'a ainsi pas besoin d'envoyer différentes copies du même flux à différents récepteurs. Cela permet également d'optimiser la bande passante du réseau : à la place d'un flux par destination, le réseau transmet un flux unique et le réplique uniquement lorsque cela est nécessaire pour atteindre les destinations, optimisant ainsi l'utilisation de la bande passante. La technologie multicast est largement utilisée aujourd'hui avec l'explosion des périphériques audio/vidéo IP, des téléphones portables, etc. Elle était couramment utilisée dans les grands réseaux ; à présent, les chaînes de télévision commencent à utiliser les réseaux IP pour transmettre leurs émissions, le multicast devient de plus en plus important. Plusieurs autres applications tirent profit du multicast, dont la vidéoconférence, l'apprentissage en ligne, les cours de bourse, les actualités et la vidéosurveillance. Ce document explique comment configurer et optimiser le multicast sur les commutateurs Cisco série 300/200, par exemple à l'aide de la vidéosurveillance. Pour en savoir plus sur la technologie multicast, accédez à l'adresse URL suivante : <http://www.cisco.com/go/300switches>.

Produits proposés

Ce document décrit l'utilisation d'un commutateur Cisco Small Business Managed Switch série 300/200 avec différents ports de commutation PoE (Power over Ethernet) et non PoE. Pour obtenir des détails sur d'autres commutateurs Cisco Managed Switch série 300/200, visitez le site Web <http://www.cisco.com/go/smallbusiness>, cliquez sur le lien **Routers and Switches**, et recherchez le nom du commutateur approprié.

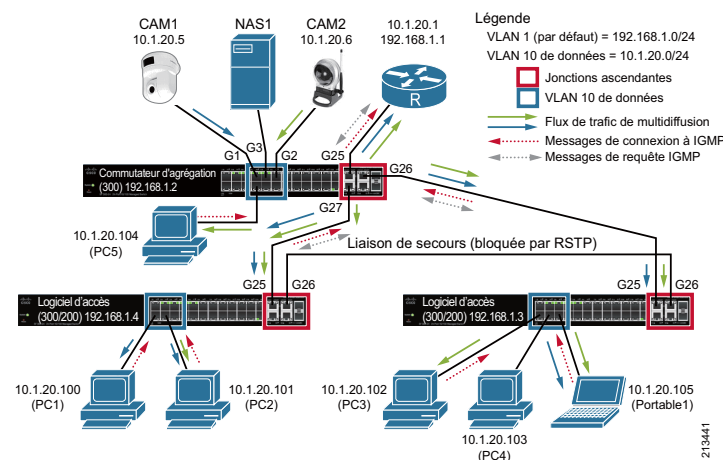
Conception d'un réseau multicast

Topologie du réseau

Les descriptions contenues dans ce document reposent sur la topologie de réseau illustrée dans la Figure 1, avec des commutateurs Cisco Small Business série 300/200 connectés à un routeur générique de PME. La Figure 1 montre comment les données d'une source, la caméra de surveillance IP, sont remises à plusieurs destinataires intéressés à l'aide du multicast IP.

La disposition de cette topologie comprend un routeur de PME, trois commutateurs Cisco série 300/200, une ou plusieurs caméras vidéo et plusieurs ordinateurs (de bureau et portables) connectés aux commutateurs. Bien que cette topologie ne les représente pas, d'autres périphériques réseau tels que des points d'accès sans fil, des périphériques de stockage NAS et des serveurs de fichiers peuvent également être connectés au réseau ou aux commutateurs d'agrégation. Cependant, ce document s'intéresse principalement à l'optimisation du multicast des commutateurs Cisco série 300/200 dans un environnement LAN. La caméra de vidéosurveillance IP est un exemple de périphérique qui utilise le multicast pour envoyer des images vidéo uniquement aux destinataires ou clients qui les ont demandées.

Figure 1 Topologie multicast pour PME



219441



Remarque Cisco recommande d'utiliser un commutateur Cisco série 300 plutôt que série 200 comme commutateur d'agrégation. Le commutateur série 300 dispose de la fonctionnalité « demandeur » qui interroge régulièrement le réseau local pour déterminer si les membres du groupe multicast sont toujours actifs. Si plusieurs commutateurs série 300 proposent le multicast IP sur le réseau local, l'un de ces commutateurs est désigné comme « demandeur » et est chargé d'interroger le réseau local pour obtenir des informations sur les membres du groupe. En fonction des informations de groupe apprises à l'aide du protocole IGMP (Internet Group Management Protocol), un commutateur série 300 est capable de déterminer quel trafic multicast (le cas échéant) doit être transféré à chacun de ses commutateurs « terminaux ». Le commutateur série 200 ne prend pas en charge la fonctionnalité « demandeur » et est, par conséquent, recommandé comme commutateur « terminal » ou de couche d'accès ; c'est-à-dire qu'il est connecté uniquement à un commutateur d'agrégation série 300 (commutation entre lui-même et le routeur), ou un routeur pour un réseau multicast.

Détails de la conception réseau

Dans la topologie illustrée dans la [Figure 1](#), un port Gigabit Ethernet des ports de commutation intégrés du routeur est connecté au port de liaison ascendante *G25* du commutateur d'agrégation Cisco série 300. Les ports de liaison ascendante *G26* et *G27* du commutateur d'agrégation sont à leur tour connectés à chacun des ports de liaison ascendante *G25* des deux commutateurs Cisco série 300/200 « terminaux » ou de couche d'accès, respectivement. Éventuellement, une liaison de secours peut être créée en connectant le port de liaison ascendante *G26* des deux commutateurs d'accès. La liaison de secours permet, en cas d'échec accidentel entre le commutateur d'agrégation et l'un des commutateurs, de réacheminer le trafic.



Remarque Les protocoles STP (Spanning Tree Protocol) ou RSTP (Rapid STP) doivent être configurés sur tous les commutateurs pour empêcher qu'une boucle de couche 2 ne se crée entre les trois commutateurs. Le protocole RSTP est recommandé pour une meilleure convergence. Notez également que le protocole RSTP est configuré par défaut pour les commutateurs Cisco série 300/200.

Le VLAN 1 et une adresse IP sont généralement préconfigurés sur les routeurs Cisco Small Business. Un seul VLAN est généralement approprié pour une mise en œuvre simple. Si le déploiement IP doit être pris en compte, Cisco recommande d'isoler le trafic de téléphonie sur IP du trafic utilisateur de données en créant des VLAN supplémentaires pour la voix. Cette démonstration n'utilise qu'un VLAN 10 de données en plus du VLAN 1. Ce guide utilise les VLAN et adresses réseau répertoriés dans le [Tableau 1](#) uniquement à des fins de démonstration ; vous pouvez utiliser votre propre système d'adressage IP.

Tableau 1 Système d'adressage IP possible

VLAN par défaut	1
Adresse IP/passerelle par défaut/routeur WAN	192.168.1.1
Pool DHCP pour VLAN 1 par défaut (périphériques réseau)	192.168.1.100–254
Commutateur d'agrégation	192.168.1.2
Commutateur d'accès 1	192.168.1.3
Commutateur d'accès 2	192.168.1.4
VLAN de données	10
Passerelle par défaut du VLAN de données	10.1.20.1
Pool DHCP pour les clients DHCP du VLAN de données (ordinateurs de bureau, ordinateurs portables, etc.)	10.1.20.100–254
Caméra IP 1 (CAM1)/adresse de groupe multicast	10.1.20.5 / 239.10.10.5
Caméra IP 2 (CAM2)/adresse de groupe multicast	10.1.20.6 / 239.10.10.6

Par défaut, un commutateur transfère le trafic multicast par tous les ports sur le VLAN (comme la diffusion). Les ports qui ne sont pas intéressés par le flux multicast le transfèrent tout de même aux périphériques connectés. Néanmoins, cela gaspille la bande passante du commutateur, et cause des congestions sur les liaisons qui n'ont pas besoin de recevoir le flux. La configuration de la surveillance IGMP sur le commutateur permet de réduire ces problèmes. En activant la surveillance IGMP sur tous les commutateurs, les flux multicast vidéo ne sont acheminés qu'aux clients multicast qui souhaitent les recevoir, et n'inondent pas les autres ports.

Principales caractéristiques multicast des commutateurs Cisco série 300/200

Protocole IGMP (Internet Group Management Protocol) V2 et V3

Le protocole IGMP permet d'inscrire de manière dynamique des hôtes individuels dans un groupe multicast sur un réseau local spécifique. Les hôtes identifient les appartenances aux groupes en envoyant des messages IGMP à leur routeur multicast local. Avec le protocole IGMP, les routeurs écoutent les messages IGMP et envoient régulièrement des requêtes pour détecter les groupes actifs ou inactifs sur un sous-réseau spécifique. Il existe trois versions du protocole IGMP : 1, 2 et 3. Les commutateurs Cisco série 300/200 prennent en charge les versions 2 et 3, et peuvent également envoyer des messages de requête, comme un routeur.

Surveillance IGMP

La surveillance IGMP requiert que le commutateur du réseau local examine, ou surveille, certaines informations de couche 3 dans les paquets IGMP envoyés entre les hôtes et le routeur. Lorsque le commutateur entend le rapport d'hôte IGMP d'un hôte d'un groupe multicast spécifique, le commutateur ajoute le numéro de port hôte à l'entrée de table multicast associée. Lorsque le commutateur entend le message de groupe de départ IGMP d'un hôte, il supprime le port d'hôte de l'entrée de table. Un commutateur Cisco série 300/200 effectue la surveillance IGMP si celle-ci et le filtrage multicast par pont sont tous les deux activés.

Utilisation du commutateur Cisco série 300 en tant que demandeur IGMP (non pris en charge pour le commutateur série 200)

Un demandeur IGMP est requis pour la mise en œuvre du protocole IGMP sur le réseau. En général, un routeur multicast est également demandeur IGMP. Dans une PME, où le routeur peut ne pas prendre en charge le transfert multicast, le commutateur Cisco série 300 peut éventuellement être utilisé comme demandeur IGMP, en dernier recours. Un seul demandeur IGMP doit être présent sur un réseau. Le commutateur Cisco série 300 prend en charge la sélection du demandeur IGMP basée sur des normes. La fonctionnalité de demandeur peut être configurée manuellement, ou dynamiquement, à l'aide d'une procédure de sélection.



Remarque Dans une topologie plus importante avec des commutateurs d'agrégation et de couche d'accès, comme dans la [Figure 1](#), le commutateur de couche d'agrégation doit être configuré manuellement comme demandeur IGMP.

Utilisation d'adresses de groupe MAC

Le commutateur prend en charge le transfert du trafic multicast entrant en fonction des informations de groupe multicast. Ces informations sont dérivées des paquets IGMP reçus, ou résultant d'une configuration manuelle, et stockées dans la base de données de transfert multicast.

Lorsqu'une trame est reçue d'un VLAN configuré pour transférer les flux multicast basés sur des adresses de groupe MAC alors que son adresse de destination est une adresse multicast de couche 2, la trame est transférée à tous les ports membres de l'adresse de groupe MAC.



Remarque Une ou plusieurs adresses de groupe multicast IP peuvent être mappées en une adresse de groupe MAC. Le transfert basé sur les adresses de groupe MAC peut entraîner le transfert d'un flux multicast IP vers des ports ne disposant d'aucun récepteur pour le flux.

Utilisation de l'adresse de groupe de multicast IP

La fonctionnalité d'adresse de groupe multicast IP est similaire à la fonctionnalité d'adresse de groupe MAC, sauf que les groupes multicast sont identifiés par les adresses IP. Les trames multicast sont transférées en fonction de l'adresse IP de destination du paquet IP.

Utilisation d'un port de routeur multicast

Un port de routeur multicast (Mrouter) est un port qui se connecte à un routeur multicast. Le commutateur inclut les ports de routeur multicast lorsqu'il transfère les flux multicast et les messages d'enregistrement IGMP. Cela est requis pour que tous les routeurs multicast puissent à leur tour transférer les flux multicast et distribuer les messages d'enregistrement aux autres sous-réseaux. Sur les commutateurs Cisco série 300/200, vous pouvez configurer de manière statique ou détecter de manière dynamique les ports connectés aux Mrouters.

Utilisation du transfert de tous les multicast

La fonctionnalité Forward All Multicast active et affiche la configuration des ports et/ou groupes d'agrégation de liaisons (LAG) qui doivent recevoir tous les flux multicast provenant d'un VLAN spécifique. Cette fonctionnalité requiert que le filtrage multicast par pont de l'écran Properties du commutateur Cisco série 300/200 soit activé. Si le filtrage multicast par pont est désactivé, tout le trafic multicast inonde tous les ports du commutateur.

Un port des commutateurs Cisco série 300/200 peut être configuré de manière statique pour transférer tous les multicast, si les périphériques qui se connectent au port ne prennent pas en charge le protocole IGMP. La configuration affecte uniquement les ports membres du VLAN sélectionné.

Utilisation des paramètres multicast non enregistrés

Si la surveillance IGMP est activée, le commutateur détecte la présence de groupes multicast et contrôle quels ports rejoignent quel groupe multicast. Les groupes multicast peuvent également être configurés de manière statique. Les groupes multicast qui ont été détectés de manière dynamique ou configurés de manière statique sont considérés comme enregistrés. Ainsi, le commutateur peut transmettre les trames multicast (à partir d'un groupe multicast enregistré) uniquement aux ports associés au groupe en question.



Remarque Vous pouvez sélectionner un port qui reçoit ou filtre les flux multicast non enregistrés. La configuration est valide pour tous les VLAN dont il est (ou sera) membre. Cette fonctionnalité permet de s'assurer que le client reçoit uniquement les groupes multicast demandés et pas les autres groupes qui pourraient être transmis sur le réseau.

Liste de vérification de préconfiguration

Cette configuration repose sur un réseau existant conforme à la topologie illustrée dans la [Figure 1](#), avec les caractéristiques suivantes :

- Le VLAN de données (VLAN 10) est défini sur le réseau, comme requis.
- Des VLAN voix ou autres peuvent être déployés (facultatif).
- Les caméras vidéo sont configurées pour fournir des flux vidéo multicast par le VLAN de données.
- Le protocole RSTP (Rapid Spanning Tree) est configuré sur tous les commutateurs du réseau.
- La fonctionnalité QoS est configurée sur les commutateurs pour fournir une file d'attente prioritaire au trafic multicast.
- Les flux multicast ont un DSCP CS4 ; si la caméra marque le trafic différemment, le commutateur doit remarquer le trafic pour CS4.

Conseils de configuration

Ces étapes de configuration activent les fonctions suivantes :

- Le réseau local diffuse en multicast les flux vidéo du [Tableau 2](#) vers les ordinateurs de bureau connectés à l'ordinateur portable.

Tableau 2 Adresses IP et multicast

Nom de la caméra de vidéosurveillance IP	Adresse IP de la caméra	Adresse multicast de flux vidéo
CAM1	10.1.20.5	239.10.10.5
CAM2	10.1.20.6	239.10.10.6

- Cette configuration n'inclut aucune configuration de routeur qui active le routeur pour le transfert ou l'acheminement des flux multicast (bien que cela soit possible, le cas échéant, si le routeur prend en charge le multicast).
- Cette configuration utilise le protocole IGMP v2, et les ordinateurs exécutent le client VLC 1.1.2 pour afficher les flux multicast ; vous pouvez utiliser d'autres clients si vous le souhaitez.
- Cette configuration utilise l'« adresse de groupe IP » comme « mode de transfert pour IPv4 », au lieu de l'« adresse de groupe MAC ».
- Cette configuration utilise le commutateur d'agrégation comme routeur demandeur de multicast.
- Les ports connectés au routeur ainsi que les ports connectés aux autres commutateurs sont configurés comme des ports Mrouter.
- La configuration doit être enregistrée à la fin de la procédure. Les modifications apportées au commutateur sont enregistrées dans la configuration en cours après avoir cliqué sur **Apply**. La configuration en cours doit être enregistrée pour conserver les modifications. Pour conserver les modifications après le redémarrage, la configuration en cours doit être enregistrée dans le fichier de configuration initiale.

Configuration multicast sur les commutateurs Cisco série 300/200

La première étape de configuration multicast sur les commutateurs est l'utilisation de l'écran **Propriétés** pour activer le filtrage multicast par pont.

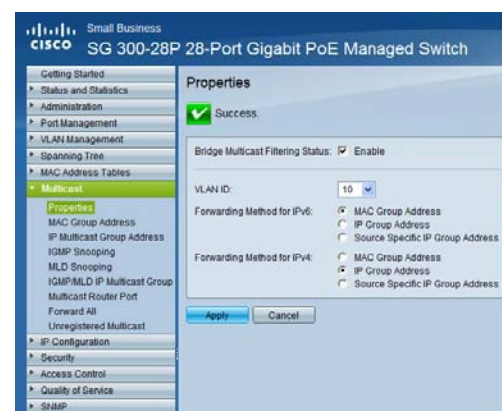
Définition des propriétés du multicast

Pour activer le filtrage multicast par pont et sélectionner l'adresse de groupe IP comme mode de transfert pour IPv4, procédez comme suit :

Étape 1 Cliquez sur **Multicast> Propriétés**.

L'écran **Propriétés** s'affiche, comme l'illustre la [Figure 2](#).

Figure 2 Écran Propriétés



Étape 2 Saisissez les paramètres comme indiqué dans la [Figure 2](#).

Étape 3 Cliquez sur **Apply**.

Le commutateur est mis à jour.

Affichage et ajout d'adresses de groupe multicast IP

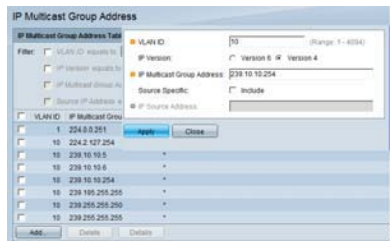
Une fois le filtrage multicast activé, l'écran **IP Multicast Group Address** est similaire à l'écran **MAC Group Address**, sauf que les groupes multicast sont identifiés par des adresses IP.

Pour afficher et ajouter des groupes multicast dans la base de données de transfert multicast, procédez comme suit :

Étape 1 Cliquez sur **Multicast> IP Multicast Group Address**.

L'écran **IP Multicast Group Address** s'affiche, comme l'illustre la [Figure 3](#).

Figure 3 Écran IP Multicast Group Address



Étape 2 Saisissez les paramètres requis pour le filtrage, comme l'illustre la Figure 3.

Étape 3 Cliquez sur **Add** pour ajouter une adresse de groupe multicast IP statique.

L'écran Add IP Multicast Group Address s'affiche.

Étape 4 Saisissez les paramètres indiqués dans la Figure 3 pour ajouter un groupe multicast statique.

Étape 5 Cliquez sur **Apply**.

Le groupe multicast IP est ajouté et le périphérique mis à jour. La Figure 3 montre l'ajout et l'affichage du groupe statique 239.10.10.254 dans le tableau. Ce tableau comprend l'intégralité de la base de données de transfert multicast, y compris tous les VLAN actifs.

Activation de la surveillance IGMP

Pour activer la surveillance IGMP sur le commutateur d'agrégation et identifier le commutateur comme demandeur de surveillance IGMP sur le VLAN 10, procédez comme suit :

Étape 1 Cliquez sur **Multicast > IGMP Snooping**.

L'écran IGMP Snooping s'affiche, comme l'illustre la Figure 4.

Figure 4 Écran IGMP Snooping



213444

Le tableau de la surveillance IGMP affiche les informations de surveillance IGMP pour les VLAN sur le commutateur.

Étape 2 Pour l'option IGMP Snooping Status, sélectionnez **Enable**.

Étape 3 Sélectionnez VLAN 10, puis cliquez sur **Edit**.

L'écran Edit IGMP Snooping s'affiche.

Étape 4 Saisissez les paramètres comme indiqué dans la Figure 4.

Étape 5 Cliquez sur **Apply**.

Le commutateur est mis à jour.

 **Remarque**

Le commutateur d'agrégation est représenté comme demandeur, avec l'adresse IP *192.168.1.2*. Comme mentionné ci-dessus, un réseau ne peut comporter qu'un seul demandeur IGMP.

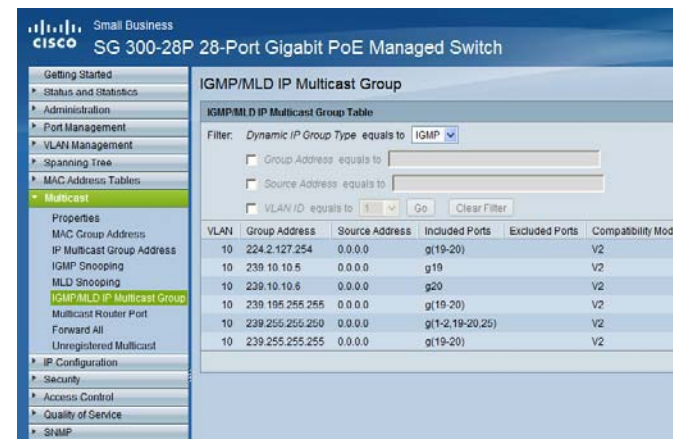
Utilisation de l'écran IGMP IP Multicast Group

Pour interroger un groupe multicast IP et afficher les groupes multicast surveillés sur le commutateur, procédez comme suit :

Étape 1 Cliquez sur **Multicast> IGMP IP Multicast Group**.

L'écran IGMP IP Multicast Group s'affiche, comme l'illustre la Figure 5.

Figure 5 Écran IGMP/MLD IP Multicast Group



213445

Étape 2 Définissez le type de groupe de surveillance à rechercher : *IGMP*.

Étape 3 Saisissez les critères de filtre d'interrogation, comme l'illustre la Figure 5.

Étape 4 Cliquez sur **Go**.

Les champs de la Figure 5 sont affichés pour tous les groupes multicast.



Remarque Notez que les groupes multicast surveillés sur le commutateur pour le VLAN 10 pour 239.10.10.5 et 239.10.10.6 de CAM1 et CAM2 respectivement.

Définition d'un port de routeur multicast (facultatif)

Cette opération n'est pertinente que si le routeur prend en charge le transfert multicast et achemine le trafic multicast vers les autres routeurs ou Internet. Pour obtenir les étapes de configuration, consultez le guide d'administration ou la page d'aide.

Définition du transfert de tous les multicast (facultatif)

Cette opération est requise si les périphériques qui se connectent au port ne prennent pas en charge les protocoles IGMP et/ou MLD (Multicast Listener Discovery). Pour obtenir les étapes de configuration, consultez le guide d'administration ou la page d'aide.

Définition de paramètres multicast non enregistrés (facultatif)

Cette fonctionnalité permet de s'assurer que le client reçoit uniquement les groupes multicast demandés et pas les autres groupes qui pourraient être transmis sur le réseau. Pour obtenir les étapes de configuration, consultez le guide d'administration ou la page d'aide.

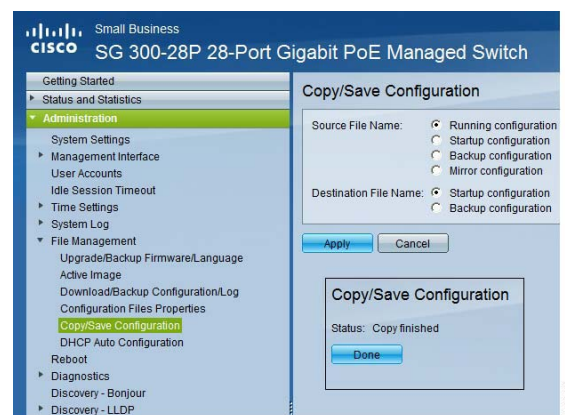
Copie et enregistrement de la configuration

Pour copier une configuration d'un type de fichier vers un autre type de fichier :

Étape 1 Cliquez sur **Administration > File Management > Copy/Save Configuration**.

L'écran Copy/Save Configuration s'affiche, comme l'illustre la Figure 6.

Figure 6 Écran Copy/Save Configuration



Étape 2 Sélectionnez le nom du fichier source à copier.

Seuls les types de fichiers valides sont affichés ; les types de fichiers sont décrits à la section Fichiers et types de fichiers.

Étape 3 Sélectionnez le nom du fichier de destination à remplacer par le fichier source.

Étape 4 Cliquez sur **Apply**.

Le fichier est copié et le commutateur est mis à jour.

Configuration de la caméra IP Cisco pour le multicast

Pour configurer la caméra IP Cisco, reportez-vous au document *IP Video Surveillance Solution Smart Setup Guide*.

Pour configurer la caméra IP pour le multicast, procédez comme suit :

Étape 1 Cliquez sur **Advance Setup**, comme l'illustre la Figure 7.

Figure 7 Configuration de la caméra IP Cisco pour le multicast



Étape 2 Cochez **Enable Multicast**.

Étape 3 Saisissez les informations multicast avec une adresse de groupe distincte pour chaque caméra.

Étape 4 Cochez **Enable QoS Mode** et saisissez **32** dans le champ DSCP (conformément au document *Configuration de la qualité de service LAN pour la téléphonie IP Cisco*).

Étape 5 Cliquez sur **Save** pour enregistrer vos paramètres.

Configuration de VLC pour afficher le flux multicast d'une caméra de vidéosurveillance IP

Pour télécharger, installer et configurer le lecteur multimédia VLC, reportez-vous au guide de configuration VLC disponible sur le site Web VLC à l'adresse suivante : <http://www.videolan.org/>.

Une fois VLC téléchargé et correctement installé et configuré sur l'ordinateur, il est prêt à recevoir le trafic multicast du réseau local ou d'Internet. À l'aide de l'icône de raccourci VLC sur le Bureau ou du menu Démarrer > Tous les Programmes sur l'ordinateur, lancez le lecteur multimédia VLC.

Les flux multicast peuvent être reçus manuellement ou à l'aide du service SAP (Session Announcement Protocol). Pour obtenir plus d'informations sur le service SAP avec VLC, consultez le site Web suivant : <http://wiki.videolan.org/SAP>.

Pour utiliser VLC comme client multicast pour recevoir les flux multicast de la caméra de vidéosurveillance IP Cisco à l'aide du service SAP, procédez comme suit :

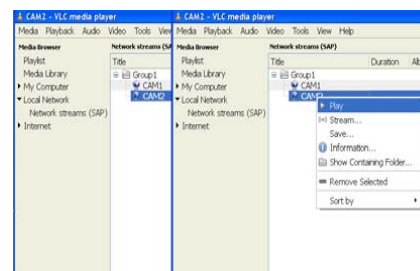
Étape 1 À l'aide du service SAP, définissez la liste de lecture dans VLC en sélectionnant **Vue > Liste de lecture**.

Étape 2 Dans le Navigateur de médias VLC, sélectionnez **Réseau local**, puis **Network Streams (SAP)** pour afficher les flux disponibles à la lecture.

Au début, la liste est vide ; pour remplir la liste, un demandeur IGMP peut être nécessaire.

Étape 3 Pour afficher la vidéo, double-cliquez sur la caméra répertoriée dans la liste de lecture illustrée dans la Figure 8, ou cliquez avec le bouton droit sur les caméras et sélectionnez **Lire** dans le menu.

Figure 8 Saisie de l'adresse URL pour le flux multicast



Remarque

L'image de VLC ne peut pas être enregistrée dans les applications telles que MS Word ou MS Paint. Elle s'affiche généralement sous forme d'image dynamique dans ces applications.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, le logo Cisco, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband et Welcome to the Human Network sont des marques commerciales ; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card et One Million Acts of Green sont des marques de services et Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, le logo IronPort, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx et le logo WebEx sont des marques déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1002R)

Les adresses de protocole Internet (IP) utilisées dans ce document ne sont pas supposées être des adresses réelles. Tous les exemples, résultats d'affichage de commandes et chiffres auxquels il est fait référence dans ce document sont donnés à titre indicatif uniquement. L'utilisation de toute adresse IP réelle à titre d'exemple est non intentionnelle et fortuite.

