Pratiques exemplaires relatives au VLAN et conseils de sécurité pour les routeurs Cisco Business

Objectif

L'objectif de cet article est d'expliquer les concepts et les étapes de mise en œuvre des pratiques exemplaires et des conseils de sécurité lors de la configuration des réseaux VLAN sur les équipements Cisco Business.

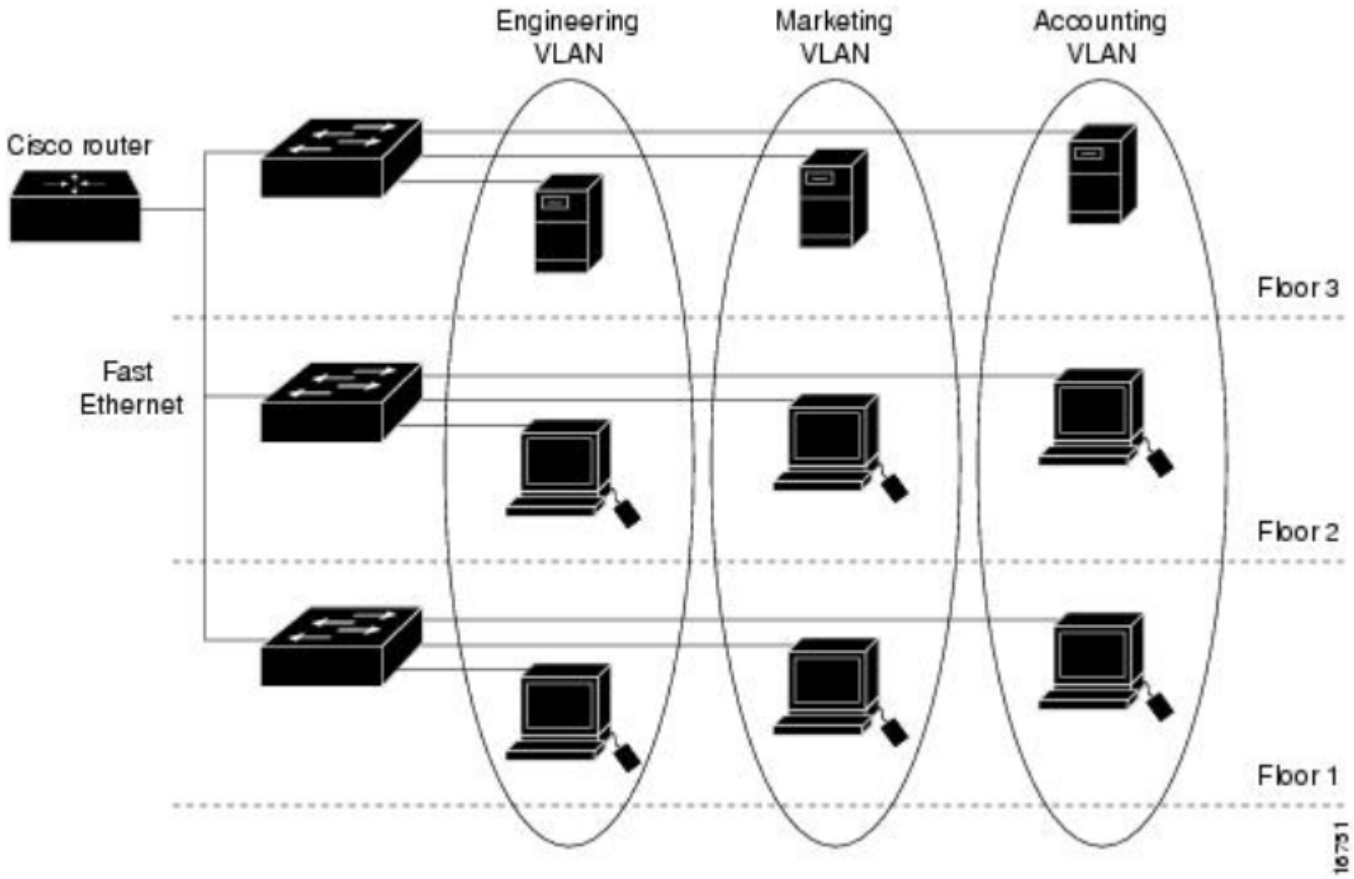
Table des matières

Introduction

Vous souhaitez rendre votre réseau d'entreprise plus efficace tout en le maintenant sécurisé ? Pour ce faire, vous pouvez notamment configurer correctement les réseaux locaux virtuels (VLAN).

Un VLAN est un groupe logique de stations de travail, de serveurs et de périphériques réseau qui semblent se trouver sur le même réseau local (LAN) malgré leur répartition géographique. En bref, le matériel des mêmes VLAN permet de séparer et de sécuriser le trafic entre les équipements.

Par exemple, vous pouvez avoir un service d'ingénierie, de marketing et de comptabilité. Chaque service a des employés à différents étages de l'immeuble, mais ils ont toujours besoin d'accéder aux informations et de les communiquer au sein de leur propre service. Il est essentiel au partage de documents et de services Web.



Les réseaux locaux virtuels doivent être configurés selon les meilleures pratiques afin de garantir la sécurité de votre réseau. Effectuez les choix intelligents suivants lors de la configuration des VLAN. Vous ne le regretterez pas !

Périphériques pertinents

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

Vous serez peut-être intéressé de savoir que les routeurs de la gamme RV160 ou RV260 peuvent transporter jusqu'à 16 VLAN, tandis que les routeurs de la gamme RV34x peuvent transporter jusqu'à 32 VLAN. Le RV320 prend en charge jusqu'à 7 VLAN. Si vous souhaitez connaître le nombre de VLAN que votre routeur peut transporter, consultez la fiche technique de votre modèle spécifique sur le site Web de Cisco. Sélectionnez **Support** et entrez votre numéro de modèle ou

effectuez simplement une recherche pour la fiche technique et le numéro de modèle.

Un vocabulaire rapide pour les débutants

Port d'accès: Un port d'accès transporte le trafic pour un seul VLAN. Les ports d'accès sont souvent appelés ports non balisés, car il n'y a qu'un seul VLAN sur ce port et le trafic peut être transmis sans balises.

Port trunk : Port d'un commutateur qui transporte le trafic de plusieurs VLAN. Les ports agrégés sont souvent appelés ports balisés car il y a plus d'un VLAN sur ce port et le trafic pour tous les VLAN sauf un doit être balisé.

VLAN natif: Le seul VLAN dans un port trunk qui ne reçoit pas de balise. Tout trafic qui n'a pas de balise sera envoyé au VLAN natif. C'est pourquoi les deux côtés d'une agrégation doivent s'assurer qu'ils ont le même VLAN natif ou que le trafic n'ira pas au bon endroit.

Meilleure pratique #1 - Attribution de ports VLAN

Notions de base sur les affectations de ports

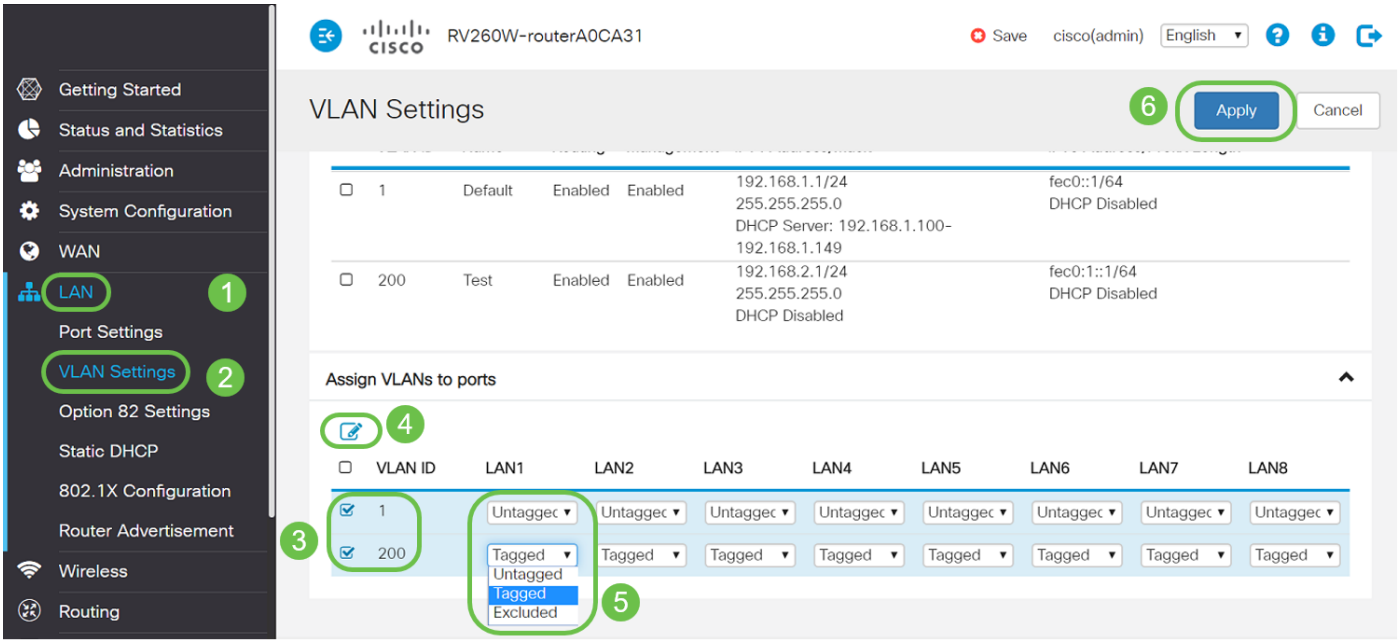
- Chaque port LAN peut être configuré comme port d'accès ou port agrégé.
- Les VLAN dont vous ne voulez pas sur l'agrégation doivent être exclus.
- Un VLAN peut être placé dans plusieurs ports.

Configuration des ports d'accès

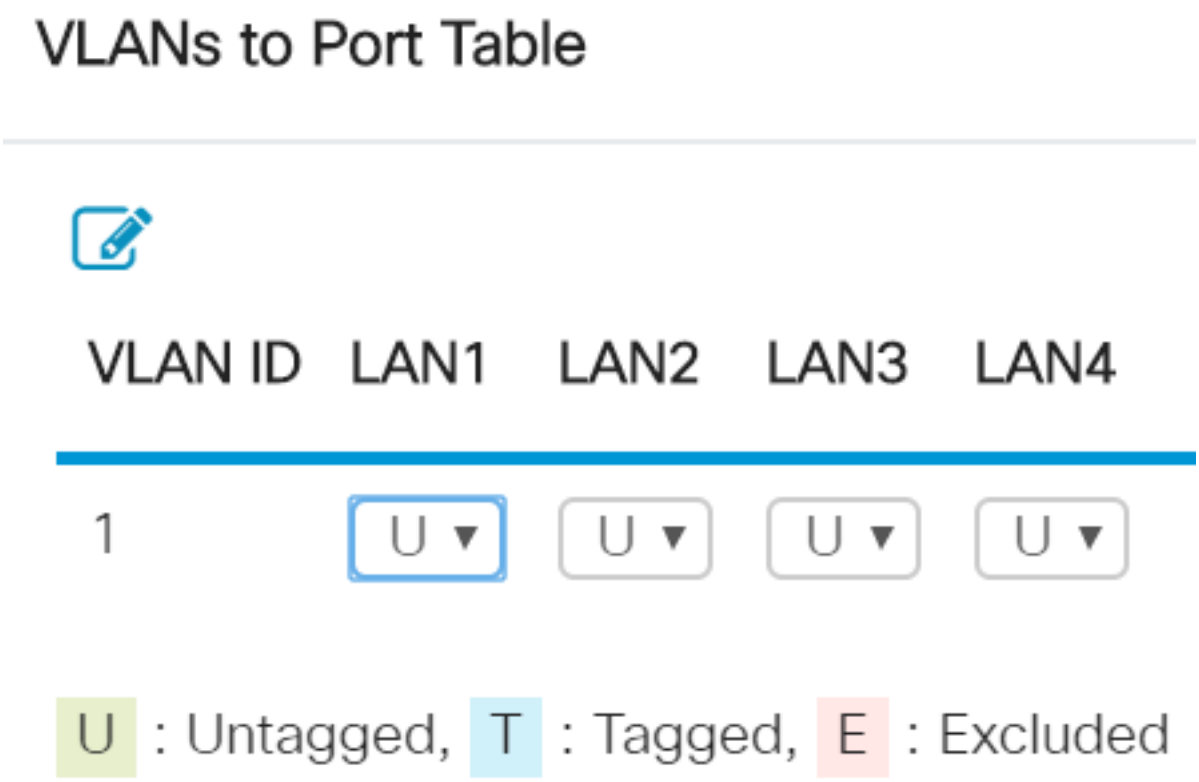
- Un VLAN attribué sur un port LAN
- Le VLAN qui est assigné à ce port doit être étiqueté *Untagged*
- Tous les autres VLAN doivent être étiquetés *Excluded* pour ce port

Pour les définir correctement, accédez à **LAN > VLAN Settings**. Sélectionnez les *ID* de *VLAN* et **cliquez** sur l'icône de *modification*. Sélectionnez le menu déroulant de l'une des interfaces LAN des VLAN répertoriés pour modifier l'étiquetage VLAN. Cliquez sur Apply.

Découvrez cet exemple de chaque VLAN auquel est affecté son propre port LAN :



Cette image de l'interface graphique utilisateur a été prise à partir d'un routeur RV260W. Vos options peuvent être légèrement différentes. Par exemple, sur la série RV34x, les étiquettes *Untagged*, *Excluded*, et *Tagged* sont abrégées à la première lettre seulement. Le processus est toujours le même.

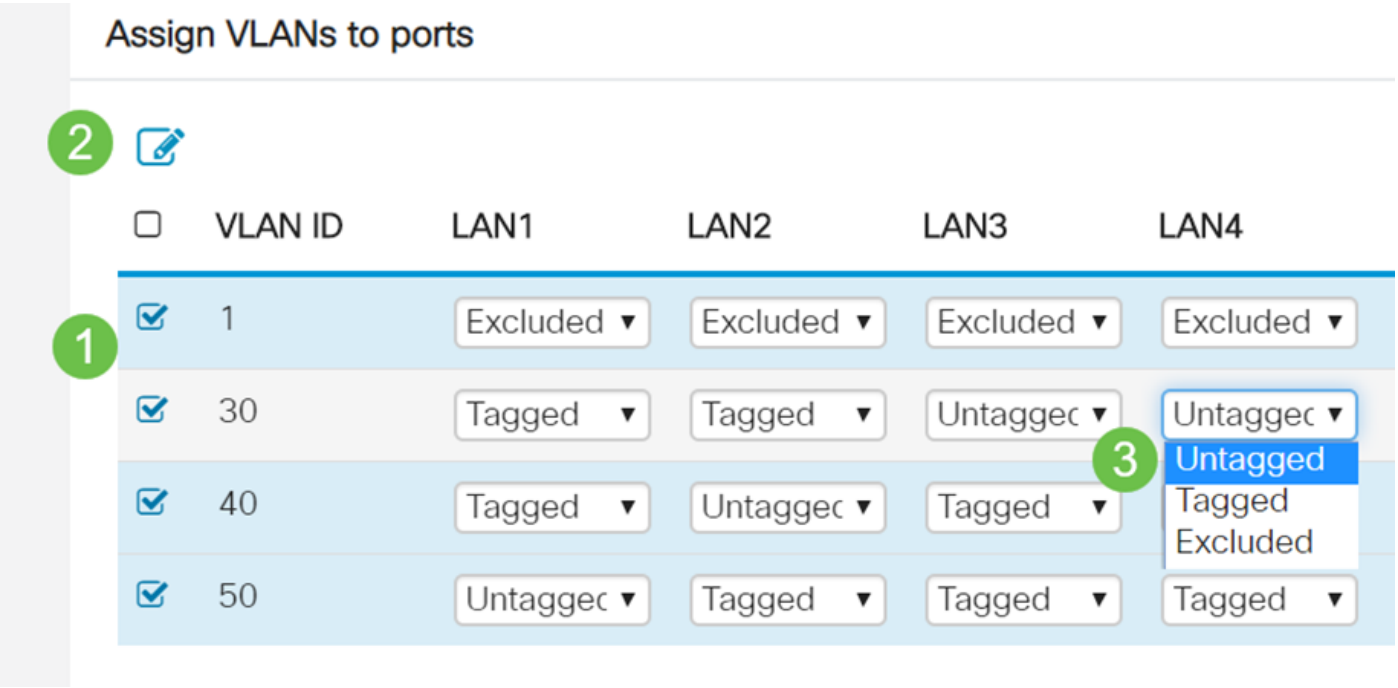


Configuration des ports agrégés

- Au moins deux VLAN partagent un port LAN
- L'un des VLAN peut être étiqueté *Untagged*.
- Le reste des VLAN qui font partie du port trunk doit être étiqueté *Tagged*.
- Les VLAN qui ne font pas partie du port trunk doivent être étiquetés *Excluded* pour ce port.

Examinez cet exemple de différents VLAN qui se trouvent tous sur des ports agrégés. Pour les définir correctement, sélectionnez les *ID de VLAN* qui doivent être modifiés. **Cliquez** sur l'icône *Modifier*. Modifiez-les en fonction de vos besoins, en suivant les recommandations ci-dessus. Au

fait, avez-vous remarqué que VLAN 1 est exclu de chaque port LAN ? Cela sera expliqué dans la section Meilleure pratique pour le VLAN 1 par défaut.



Forum aux questions

Pourquoi un VLAN est-il laissé non balisé alors qu'il est le seul VLAN sur ce port ?

Comme un seul VLAN est affecté à un port d'accès, le trafic sortant du port est envoyé sans étiquette VLAN sur les trames. Lorsque la trame atteint le port du commutateur (trafic entrant), le commutateur ajoute l'étiquette VLAN.

Pourquoi les VLAN sont-ils balisés lorsqu'ils font partie d'une agrégation ?

Ceci est fait pour que le trafic qui passe ne soit pas envoyé au mauvais VLAN sur ce port. Les VLAN partagent ce port. Semblable aux numéros d'appartement ajoutés à une adresse pour s'assurer que le courrier va au bon appartement dans ce bâtiment partagé.

Pourquoi le trafic n'est-il pas étiqueté lorsqu'il fait partie du VLAN natif ?

Un VLAN natif est un moyen de transporter le trafic non étiqueté sur un ou plusieurs commutateurs. Le commutateur attribue au VLAN natif toute trame non étiquetée qui arrive sur un port étiqueté. Si une trame sur le VLAN natif quitte un port trunk (étiqueté), le commutateur supprime l'étiquette VLAN.

Pourquoi les VLAN sont-ils exclus alors qu'ils ne sont pas sur ce port ?

Cela permet de conserver le trafic sur cette agrégation uniquement pour les VLAN que l'utilisateur souhaite spécifiquement. Elle est considérée comme une meilleure pratique.

Meilleure pratique #2 - VLAN 1 par défaut et ports inutilisés

Tous les ports doivent être affectés à un ou plusieurs VLAN, y compris le VLAN natif. Les routeurs Cisco Business sont fournis avec le VLAN 1 affecté à tous les ports par défaut.

Un VLAN de gestion est le VLAN utilisé pour gérer, contrôler et surveiller à distance les périphériques de votre réseau à l'aide de Telnet, SSH, SNMP, syslog ou FindIT de Cisco. Par

défaut, il s'agit également du VLAN 1. Une bonne pratique de sécurité consiste à séparer le trafic de gestion et le trafic de données utilisateur. Par conséquent, il est recommandé d'utiliser VLAN 1 uniquement à des fins de gestion lorsque vous configurez des VLAN.

Pour communiquer à distance avec un commutateur Cisco à des fins de gestion, le commutateur doit avoir une adresse IP configurée sur le VLAN de gestion. Les utilisateurs d'autres VLAN ne peuvent pas établir de sessions d'accès à distance au commutateur, sauf s'ils sont routés vers le VLAN de gestion, ce qui fournit une couche de sécurité supplémentaire. En outre, le commutateur doit être configuré pour accepter uniquement les sessions SSH chiffrées pour la gestion à distance. Pour lire certaines discussions sur ce sujet, cliquez sur les liens suivants sur le site Web de la communauté Cisco :

- Gestion VLAN Discussion #1
- Gestion VLAN Discussion #2

Forum aux questions

Pourquoi le VLAN 1 par défaut n'est-il pas recommandé pour segmenter virtuellement votre réseau ?

La raison principale est que les acteurs hostiles savent que VLAN 1 est le VLAN par défaut et souvent utilisé. Ils peuvent l'utiliser pour accéder à d'autres VLAN via le « saut de VLAN ». Comme son nom l'indique, l'acteur hostile peut envoyer du trafic usurpé se présentant comme VLAN 1, ce qui permet d'accéder aux ports trunk et donc aux autres VLAN.

Puis-je laisser un port inutilisé affecté au VLAN 1 par défaut ?

Pour préserver la sécurité de votre réseau, vous ne devriez vraiment pas. Il est recommandé de configurer tous ces ports pour qu'ils soient associés à des VLAN autres que le VLAN 1 par défaut.

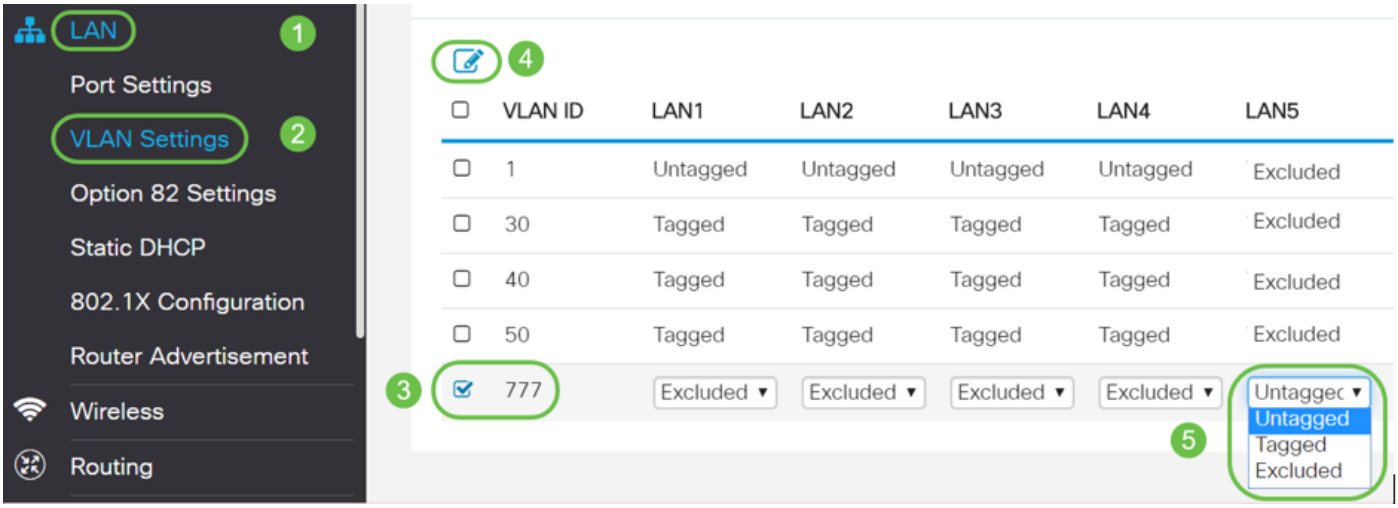
Je ne veux pas attribuer un de mes VLAN de production à un port inutilisé. Que puis-je faire ?

Il est recommandé de créer un VLAN « sans issue » en suivant les instructions de la section suivante de cet article.

Meilleure pratique #3 - Créer un VLAN « sans issue » pour les ports inutilisés

Étape 1. Accédez à **LAN > VLAN Settings**.

Choisissez un nombre aléatoire pour le VLAN. Assurez-vous que DHCP, le routage inter-VLAN ou la gestion des périphériques ne sont pas activés pour ce VLAN. Cela permet de sécuriser les autres VLAN. Placez tout port LAN inutilisé sur ce VLAN. Dans l'exemple ci-dessous, le *VLAN 777* a été créé et attribué au *LAN5*. Cela doit être fait avec tous les ports LAN inutilisés.



Notez que les autres VLAN sont exclus de ce port LAN.

Étape 2. **Cliquez** sur le bouton *Apply* pour enregistrer les modifications de configuration effectuées.

Meilleure pratique #4 - Téléphones IP sur un VLAN

Le trafic vocal est soumis à des exigences strictes en matière de qualité de service (QoS). Si votre entreprise a des ordinateurs et des téléphones IP sur le même VLAN, chacun essaie d'utiliser la bande passante disponible sans tenir compte de l'autre périphérique. Pour éviter ce conflit, il est recommandé d'utiliser des VLAN distincts pour le trafic voix et le trafic données de téléphonie IP. Pour en savoir plus sur cette configuration, consultez les articles et vidéos suivants :

- Cisco Tech Talk : Configuration et configuration de VLAN voix à l'aide de produits Cisco Small Business (vidéo)
- Configuration du VLAN voix automatique avec QoS sur le commutateur de la gamme SG500
- Configuration du VLAN voix sur les commutateurs gérés de la gamme 200/300
- Cisco Tech Talk : Configuration du VLAN voix automatique sur les commutateurs des gammes SG350 et SG550 (vidéo)

Meilleure pratique #5 - Routage inter-VLAN

Les VLAN sont configurés de sorte que le trafic puisse être séparé, mais parfois, vous avez besoin de VLAN pour pouvoir effectuer le routage entre eux. Il s'agit d'un routage inter-VLAN qui n'est généralement pas recommandé. Si votre entreprise en a besoin, configurez-la de manière aussi sécurisée que possible. Lorsque vous utilisez le routage inter-VLAN, veillez à limiter le trafic à l'aide des listes de contrôle d'accès (ACL) aux serveurs qui contiennent des informations confidentielles.

Les listes de contrôle d'accès filtrent les paquets pour contrôler leur déplacement sur un réseau. Le filtrage des paquets assure la sécurité en limitant l'accès du trafic au réseau, en limitant l'accès des utilisateurs et des périphériques au réseau et en empêchant le trafic de quitter le réseau. Les listes d'accès IP réduisent les risques d'usurpation et de déni de service et permettent un accès utilisateur dynamique et temporaire via un pare-feu.

- Routage inter-VLAN sur un routeur RV34x avec restrictions ACL ciblées
- Cisco Tech Talk : Configuration du routage inter-VLAN sur les commutateurs de la gamme SG250 (vidéo)

- Cisco Tech Talk : Configuration inter-VLAN sur RV180 et RV180W (vidéo)
- Limitation d'accès inter-VLAN RV34x (correction du bogue CSCvo92300)

Conclusion

Voilà, vous connaissez maintenant quelques bonnes pratiques pour configurer des VLAN sécurisés. Gardez ces conseils à l'esprit lorsque vous configurez des VLAN pour votre réseau. Vous trouverez ci-dessous quelques articles qui contiennent des instructions détaillées. Ces solutions vous permettront d'évoluer vers un réseau productif et efficace, parfaitement adapté à votre entreprise.

- Configuration des paramètres VLAN sur les routeurs RV160 et RV260
- Configuration des paramètres de réseau local virtuel (VLAN) sur un routeur de la gamme RV34x
- Configurer l'appartenance VLAN sur les routeurs VPN RV320 et RV325
- Configurer l'appartenance à un réseau local virtuel (VLAN) sur un routeur de la gamme RV
- Configurer l'adresse IPv4 de l'interface VLAN sur un commutateur Sx350 ou SG350X via l'interface de ligne de commande

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.