Routage inter-VLAN sur un routeur RV34x avec restrictions de liste de contrôle d'accès ciblée

Objectif

Cet article explique comment configurer le routage VLAN sur un routeur de la gamme RV34x avec une liste de contrôle d'accès (ACL) ciblée pour restreindre certains trafics. Le trafic peut être limité par une adresse IP, un groupe d'adresses ou par type de protocole.

Introduction

Les réseaux locaux virtuels (VLAN) sont excellents, ils définissent les domaines de diffusion dans un réseau de couche 2. Les domaines de diffusion sont généralement limités par les routeurs, car ils ne transmettent pas de trames de diffusion. Les commutateurs de couche 2 créent des domaines de diffusion en fonction de la configuration du commutateur. Le trafic ne peut pas passer directement à un autre VLAN (entre domaines de diffusion) au sein du commutateur ou entre deux commutateurs. Les VLAN vous permettent de garder différents services indépendants les uns des autres. Par exemple, vous pouvez ne pas vouloir que le service des ventes soit impliqué dans le service de comptabilité.

L'indépendance est fantastique, mais que se passe-t-il si vous voulez que les utilisateurs finaux des VLAN puissent se router entre eux ? Le service des ventes peut avoir besoin d'envoyer des enregistrements ou des feuilles de temps au service comptable. Le service de comptabilité peut souhaiter envoyer des notifications à l'équipe de vente sur leurs chèques de paie ou numéros de vente. C'est à ce moment que le routage entre VLAN sauve la journée !

Pour les communications entre VLAN, un périphérique OSI (Open Systems Interconnections) de couche 3, généralement un routeur, est nécessaire. Ce périphérique de couche 3 doit avoir une adresse IP (Internet Protocol) dans chaque interface VLAN et avoir une route connectée à chacun de ces sous-réseaux IP. Les hôtes de chaque sous-réseau IP peuvent ensuite être configurés pour utiliser les adresses IP de l'interface VLAN respective comme passerelle par défaut. Une fois configuré, les utilisateurs finaux peuvent envoyer un message à un utilisateur final de l’autre VLAN. Ça a l'air parfait, non ?

Mais qu'en est-il du serveur en comptabilité ? Il existe des informations sensibles sur ce serveur qui doivent rester protégées. N'ayez pas peur, il ya une solution à cela aussi! Les règles d'accès ou les politiques sur les routeurs de la gamme RV34x permettent de configurer des règles pour accroître la sécurité du réseau. Les listes de contrôle d’accès sont des listes qui bloquent ou autorisent l’envoi du trafic à destination et en provenance de certains utilisateurs. Les règles d'accès peuvent être configurées pour être en vigueur à tout moment ou en fonction de calendriers définis.

Cet article décrit les étapes de configuration d’un deuxième VLAN, du routage entre VLAN et d’une liste de contrôle d’accès.

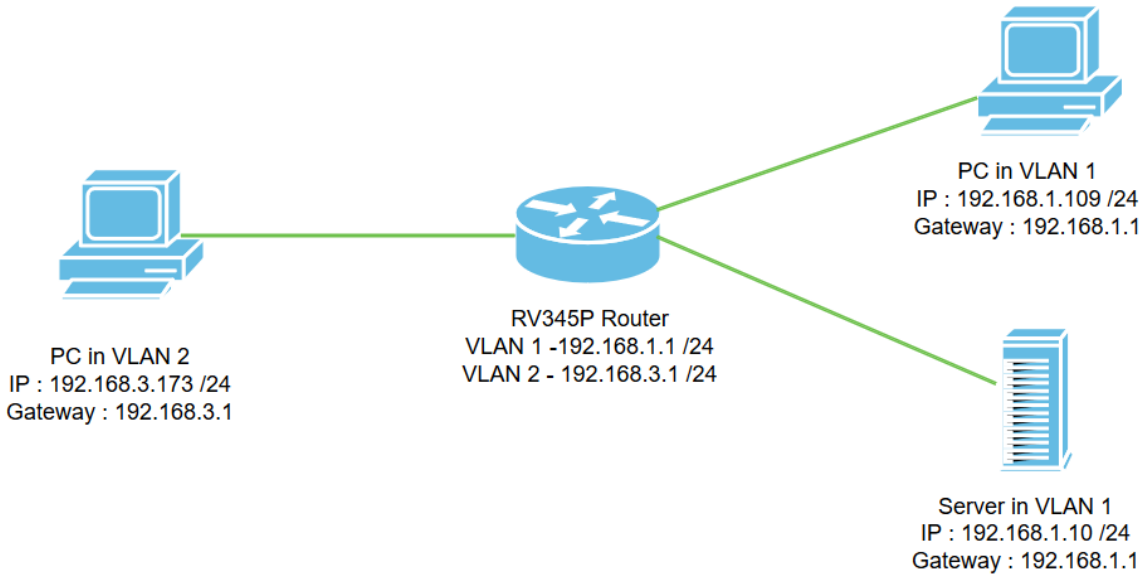
Périphériques pertinents

- RV340
- RV340W
- RV345
- RV345P

Version du logiciel

- 1.0.03.16

Topologie



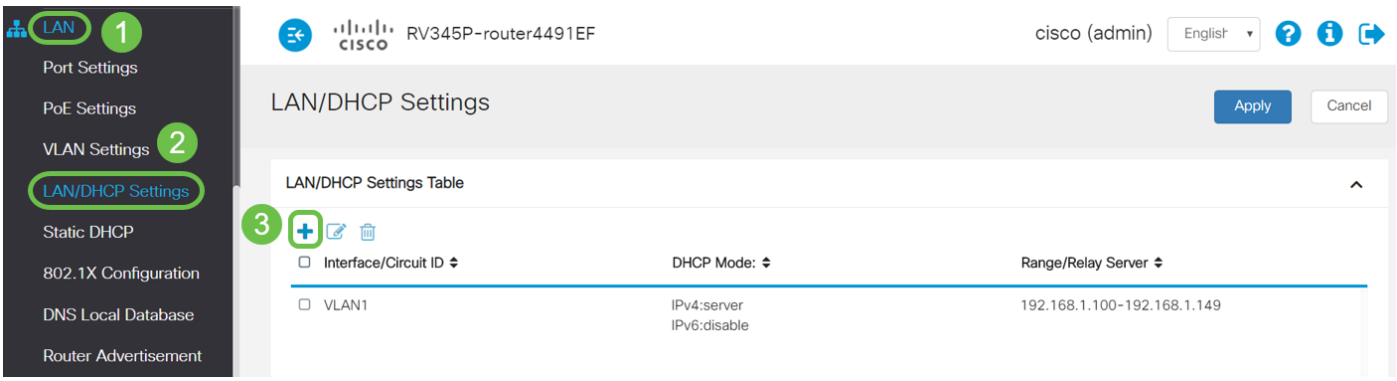
Dans ce scénario, le routage entre VLAN sera activé pour VLAN1 et VLAN2 afin que les utilisateurs de ces VLAN puissent communiquer entre eux. Par mesure de sécurité, nous empêcherons les utilisateurs de VLAN2 d'accéder au serveur VLAN1 [IPv4 (Internet Protocol version 4)] : 192.168.1.10 /24].

Ports de routeur utilisés :

- L'ordinateur personnel (PC) de VLAN1 est connecté au port *LAN1*.
- L'ordinateur personnel (PC) dans VLAN2 est connecté au port *LAN2*.
- Le serveur de VLAN1 est connecté au port *LAN3*.

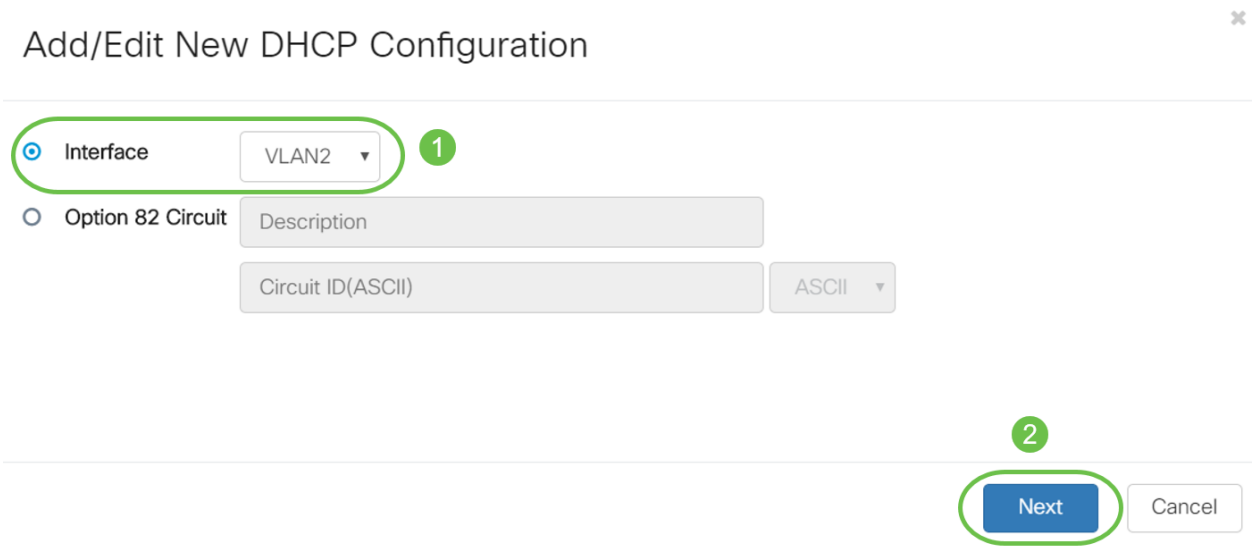
Configuration

Étape 1. Connectez-vous à l'utilitaire de configuration Web du routeur. Pour ajouter une nouvelle interface VLAN sur le routeur, accédez à **LAN > LAN/DHCP Settings** et cliquez sur l'**icône plus** sous la *table LAN/DHCP Settings*.

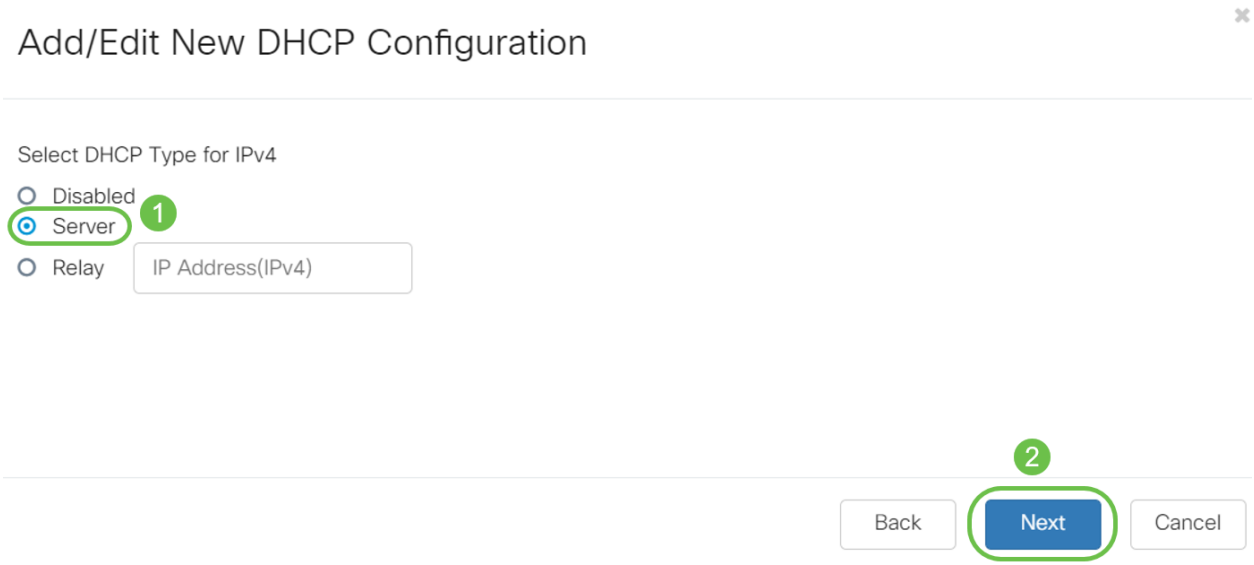


Note: L'interface VLAN1 est créée par défaut sur le routeur RV34x et le serveur DHCP (Dynamic Host Configuration Protocol) pour IPv4 est activé sur ce routeur.

Étape 2. Une nouvelle fenêtre contextuelle s'ouvre avec l'**interface** *VLAN2* sélectionnée, cliquez sur **Suivant**.



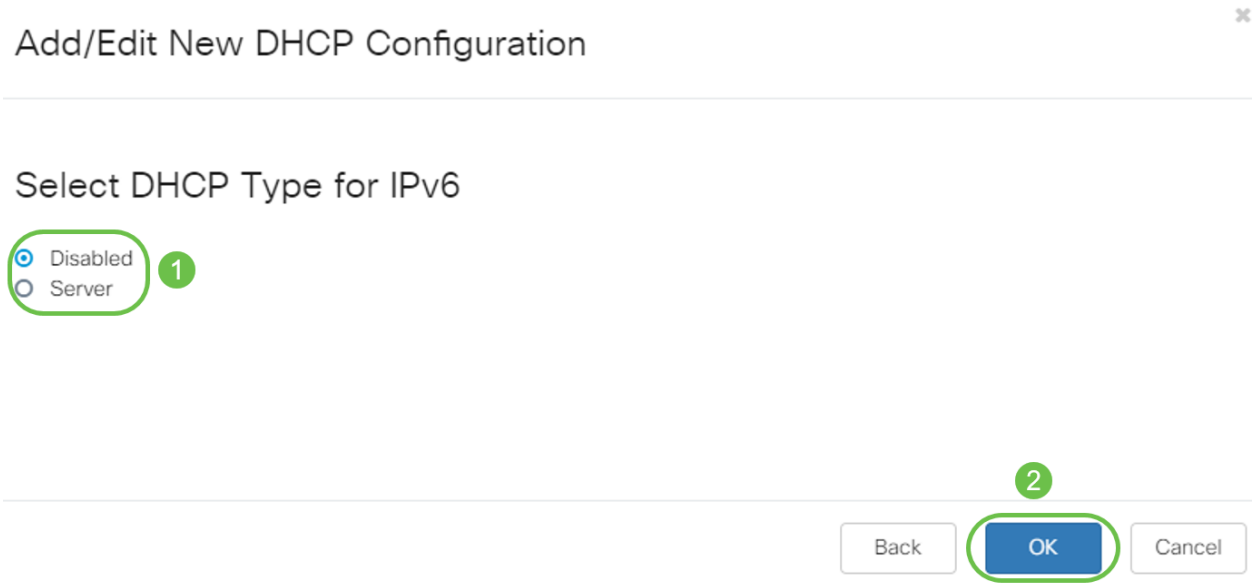
Étape 3. Pour activer le serveur DHCP sur l'interface VLAN2, sous *Sélectionner le type DHCP pour IPv4,* sélectionnez **Serveur**. Cliquez sur **Next** (Suivant).



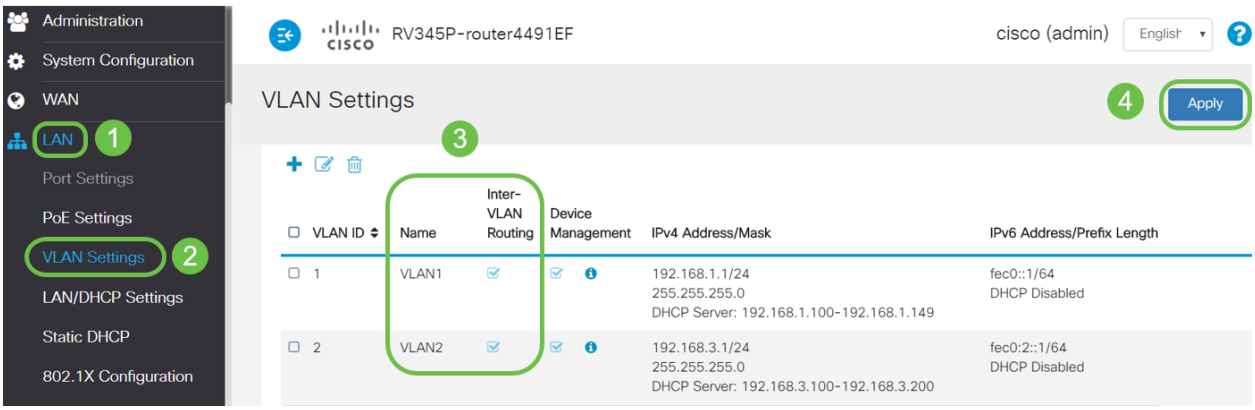
Étape 4. Entrez les paramètres de configuration du serveur DHCP, notamment *Client Lease Time, Range Start, Range End* et *DNS Server.* Cliquez sur **Next** (Suivant).

Étape 5. (Facultatif) Vous pouvez désactiver le *type DHCP pour IPv6* en cochant la case **Désactivé** car cet exemple est basé sur IPv4. Click OK. La configuration du serveur DHCP est terminée.

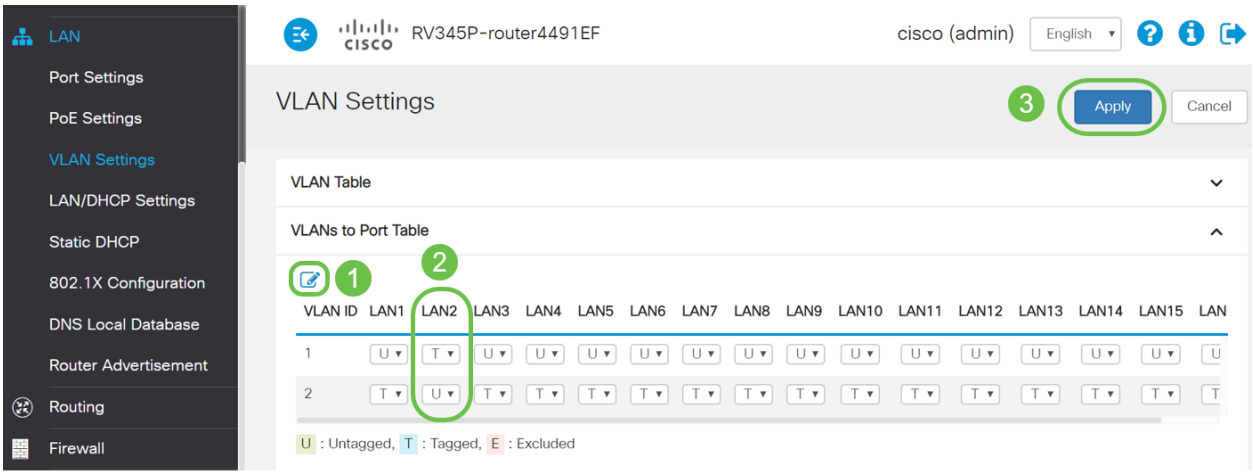
Note: Vous pouvez utiliser IPv6.



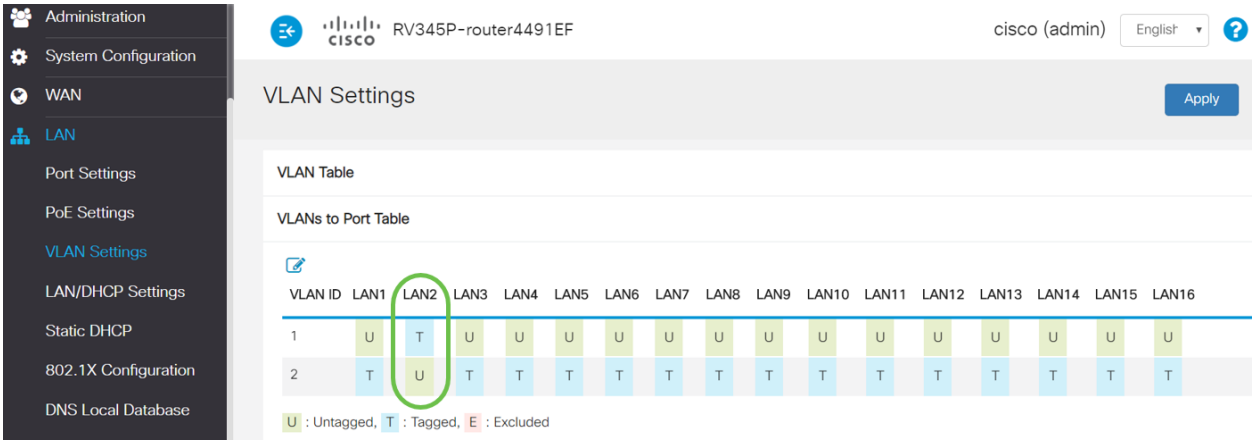
Étape 6. Accédez à **LAN > VLAN Settings** et vérifiez que le *routage inter-VLAN* est activé pour les VLAN, VLAN1 et VLAN2. Cette configuration active les communications entre les deux VLAN. Cliquez sur Apply.



Étape 7. Pour affecter le trafic non étiqueté pour VLAN2 sur le port *LAN2*, cliquez sur le bouton Edit sous l'option *VLAN to Port Table*. Maintenant, sous le port LAN2, sélectionnez l'option **T** (étiqueté) pour *VLAN1* et **U** (non étiqueté) pour *VLAN2* dans le menu déroulant. Cliquez sur **Apply** pour enregistrer la configuration. Cette configuration transfère le trafic non étiqueté pour VLAN2 sur le port LAN2 de sorte que la carte réseau (NIC) de l'ordinateur, normalement non capable de l'étiquetage VLAN, puisse obtenir l'IP DHCP de VLAN2 et faire partie de VLAN2.

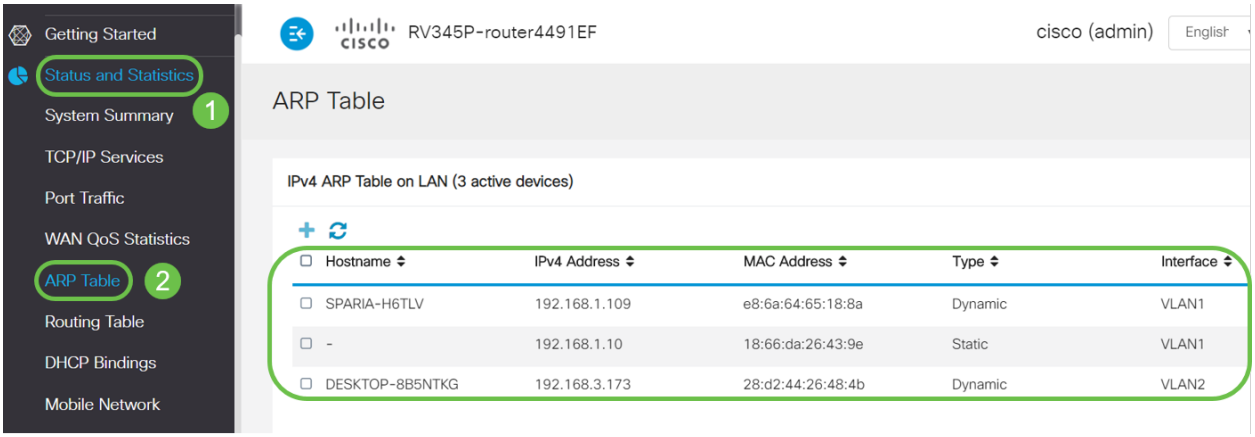


Étape 8. Vérifiez que les paramètres VLAN2 pour le port *LAN2* s'affichent sous la forme U *(non balisé)*. Pour les ports LAN restants, les paramètres VLAN2 sont *T (étiquetés)* et le trafic VLAN1 est *U (non étiqueté)*.

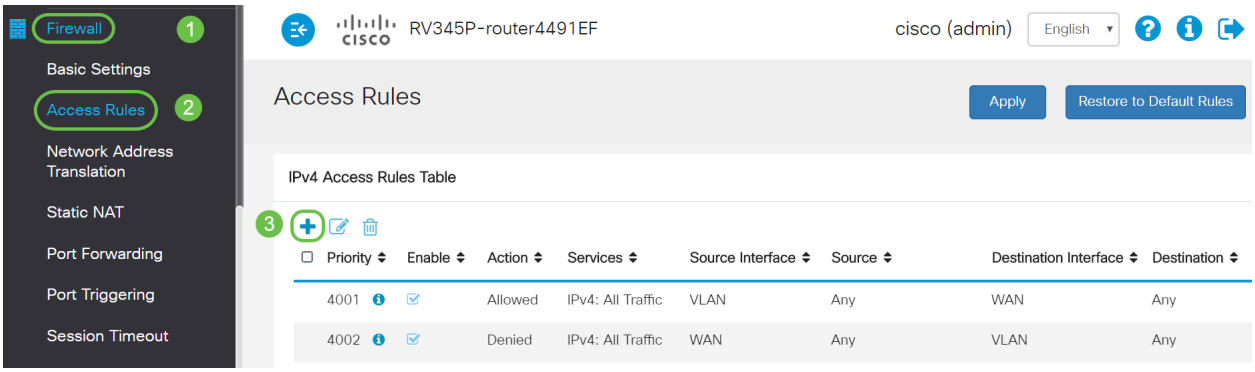


Étape 9. Accédez à **Status and Statistics > ARP Table** et vérifiez que l'*adresse IPv4* dynamique des PC se trouve sur différents VLAN.

Note: L'adresse IP du serveur sur VLAN1 a été attribuée de manière statique.



Étape 10. Appliquer une liste de contrôle d'accès pour restreindre le serveur (IPv4 : 192.168.1.10/24) accès des utilisateurs de VLAN2. Pour configurer la liste de contrôle d'accès, accédez à **Firewall > Access Rules** et cliquez sur l'**icône plus** pour ajouter une nouvelle règle.



Étape 11. Configurez les paramètres *des règles d'accès*. Pour ce scénario, les paramètres seront les suivants :

État de la règle : Activer

Action : Refuser

Services : Tout le trafic

Journal : Vrai

Interface source : VLAN2

Adresse source: tous les modèles

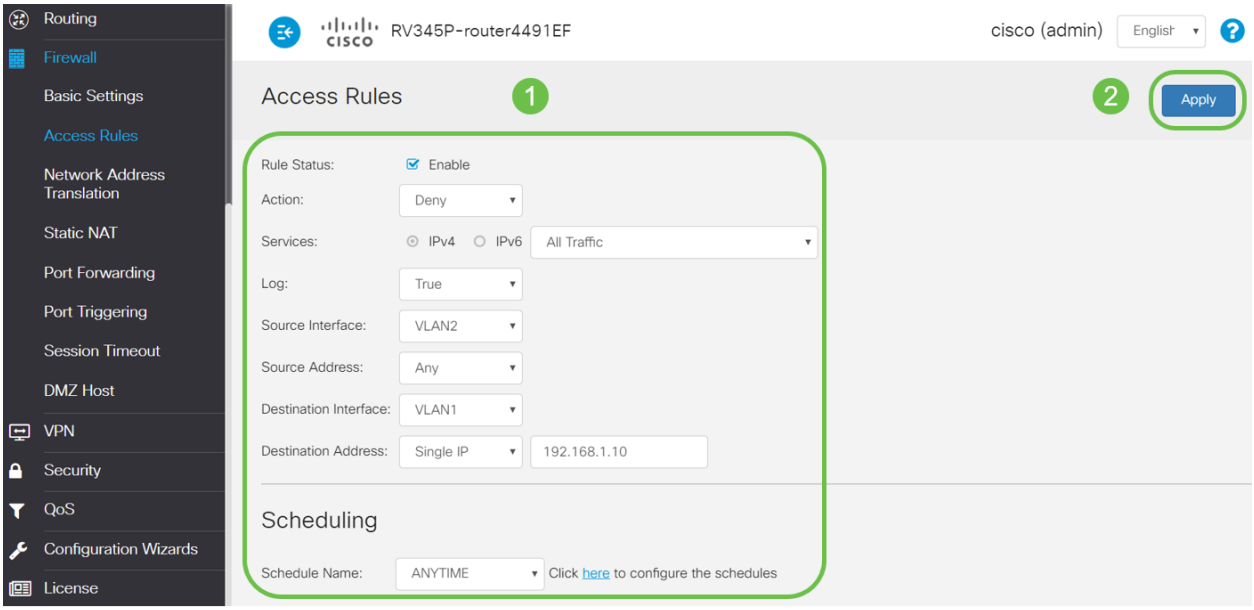
Interface de destination : VLAN1

Adresse de destination: Adresse IP unique 192.168.1.10

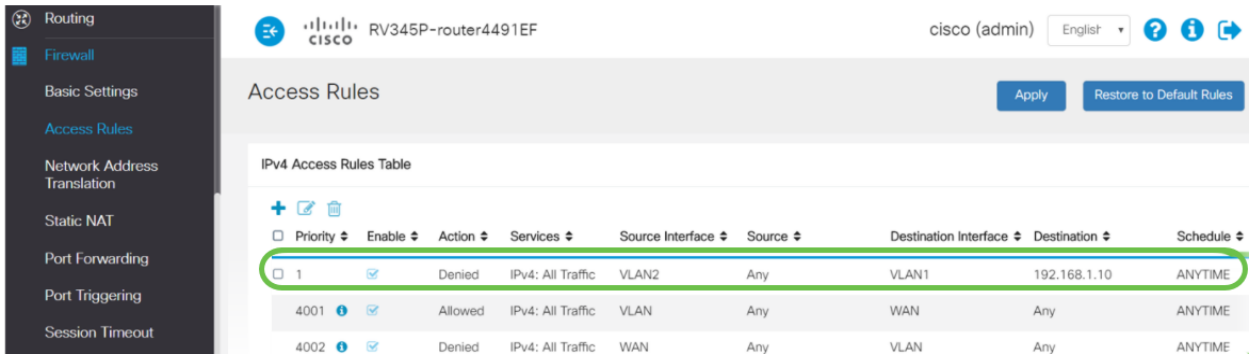
Nom de la planification : À tout moment

Cliquez sur Apply.

Note: Dans cet exemple, nous avons refusé l'accès de n'importe quel périphérique de VLAN2 au serveur, puis nous avons autorisé l'accès aux autres périphériques de VLAN1. Vos besoins peuvent varier.



Étape 12. La liste *Règles d'accès* s'affiche comme suit :



La règle d'accès est définie explicitement pour restreindre l'accès au serveur, 192.168.1.10, à partir des utilisateurs de VLAN2.

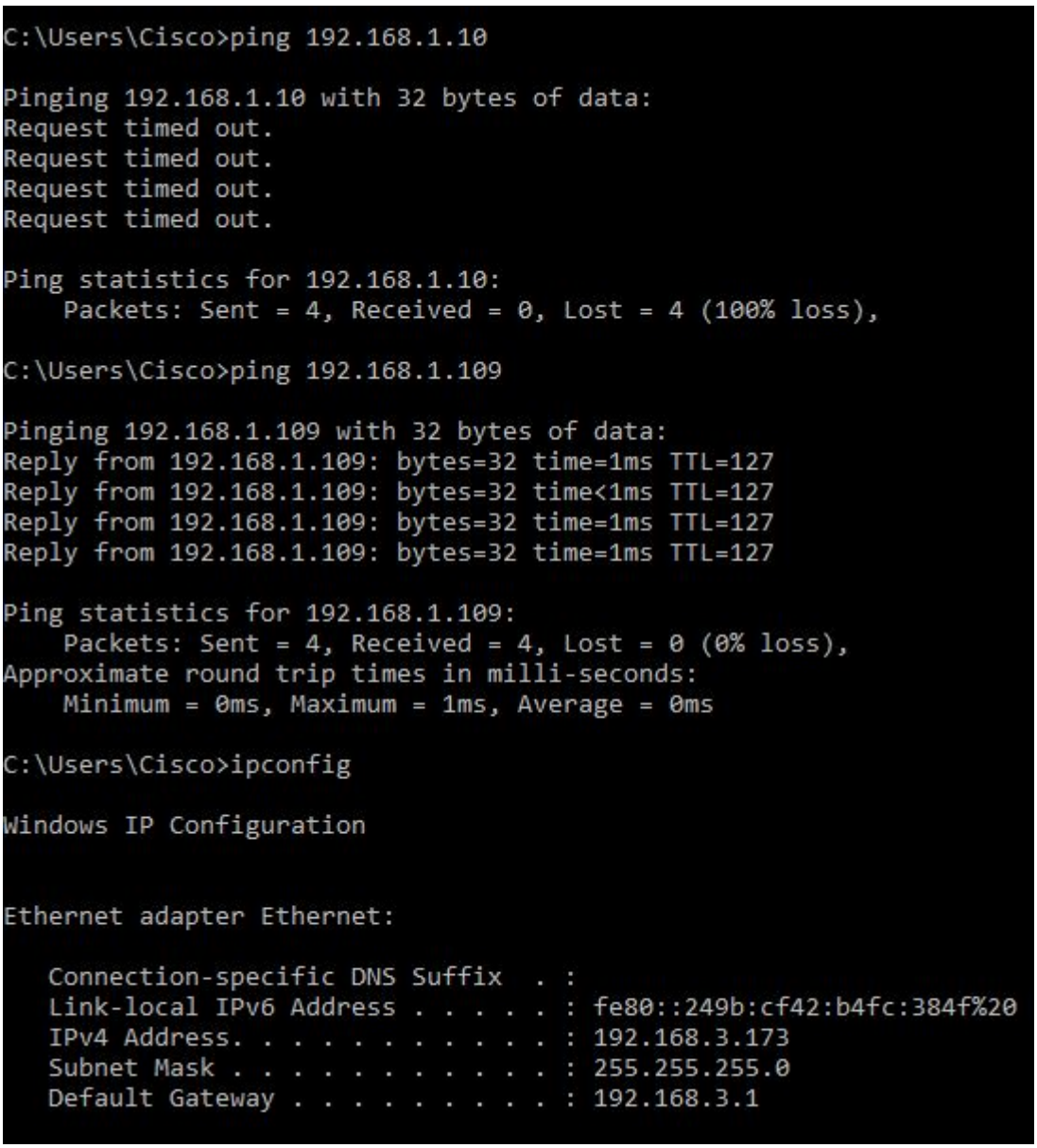
Vérification

Pour vérifier le service, ouvrez l'invite de commandes. Sur les plates-formes Windows, cela peut être réalisé en cliquant sur le bouton Windows, puis en tapant **cmd** dans la zone de recherche

inférieure gauche de l'ordinateur et en sélectionnant **Invite de commandes** dans le menu.

Entrez les commandes suivantes :

- Sur le PC (192.168.3.173) dans VLAN2, envoyez une requête ping au serveur (IP : 192.168.1.10). Vous recevrez une notification de *délai d'attente de la demande*, ce qui signifie que la communication n'est pas autorisée.
- Sur le PC (192.168.3.173) dans VLAN2, envoyez une requête ping à l'autre PC (192.168.1.109) dans VLAN1. Vous obtiendrez une réponse réussie.



Conclusion

Vous avez vu les étapes nécessaires pour configurer le routage entre VLAN sur un routeur de la gamme RV34x et comment effectuer une restriction de liste de contrôle d'accès ciblée. Maintenant, vous pouvez utiliser toutes ces connaissances pour créer des VLAN dans votre réseau qui répondent à vos besoins !