Routing inter-VLAN su un router RV34x con restrizioni ACL di destinazione

Obiettivo

In questo documento viene spiegato come configurare il routing tra VLAN (Virtual Local Area Network) su un router della serie RV34x con un elenco di controllo di accesso (ACL) di destinazione per limitare determinati traffici. Il traffico può essere limitato da un indirizzo IP, un gruppo di indirizzi o un tipo di protocollo.

Introduzione

Le VLAN sono fantastiche, definiscono i domini di broadcast in una rete di layer 2. I domini di trasmissione sono in genere delimitati da router perché i router non inoltrano i frame di trasmissione. Gli switch di layer 2 creano domini di trasmissione basati sulla configurazione dello switch. Il traffico non può passare direttamente a un'altra VLAN (tra domini di broadcast) all'interno dello switch o tra due switch. Le VLAN consentono di mantenere diversi reparti indipendenti l'uno dall'altro. Ad esempio, si potrebbe desiderare che l'ufficio vendite non sia in alcun modo coinvolto con l'ufficio contabilità.

L'indipendenza è fantastica, ma cosa succede se si desidera che gli utenti finali nelle VLAN siano in grado di comunicare tra loro? Il reparto vendite potrebbe dover inviare record o schede attività al reparto contabilità. Il reparto contabilità potrebbe voler inviare al team vendite notifiche relative ai propri assegni paga o ai numeri di vendita. In questo modo, il routing tra VLAN risparmia una giornata!

Per la comunicazione tra VLAN, è necessario un dispositivo OSI (Open Systems Interconnect) di livello 3, generalmente un router. Questo dispositivo di layer 3 deve avere un indirizzo IP (Internet Protocol) in ciascuna interfaccia VLAN e un percorso connesso a ciascuna subnet IP. Gli host di ciascuna subnet IP possono quindi essere configurati in modo da usare gli indirizzi IP dell'interfaccia VLAN come gateway predefinito. Una volta configurati, gli utenti finali possono inviare un messaggio a un utente finale sull'altra VLAN. Sembra perfetto, vero?

Ma aspettate, cosa dire del server in accounting? Il server contiene informazioni riservate che devono essere protette. Non abbiate paura, c'è una soluzione anche a questo! Le regole o le policy di accesso sul router serie RV34x consentono di configurare le regole per aumentare la sicurezza della rete. Gli ACL sono elenchi che bloccano o consentono l'invio di traffico da e verso determinati utenti. È possibile configurare le regole di accesso in modo che siano sempre attive o basate su pianificazioni definite.

In questo documento viene descritto come configurare una seconda VLAN, il routing tra VLAN e un ACL.

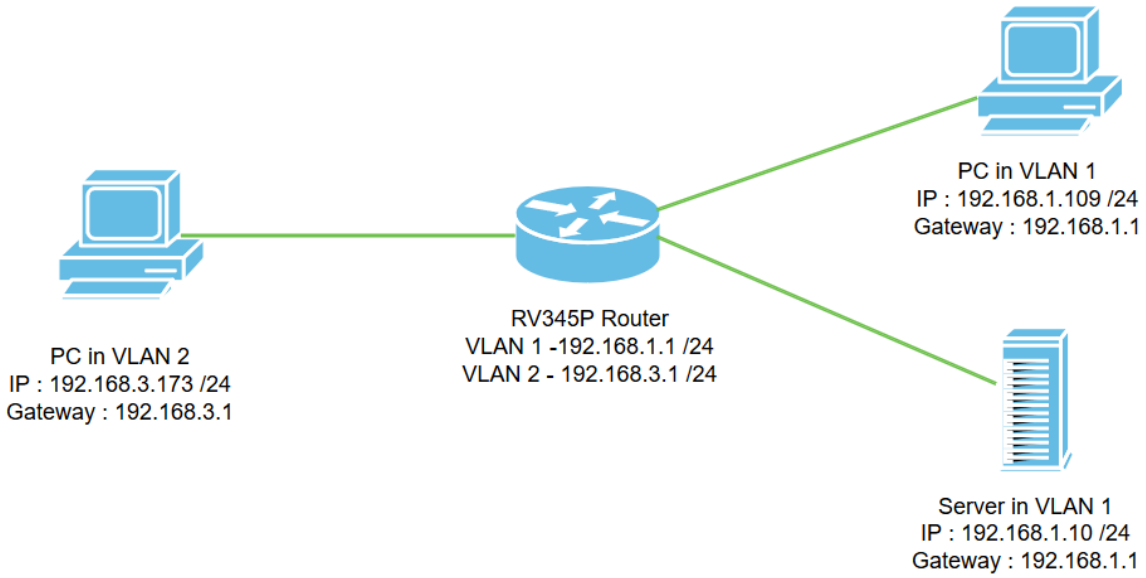
Dispositivi interessati

- RV340
- RV340W
- RV345
- RV345P

Versione del software

- 1.0.03.16

Topologia



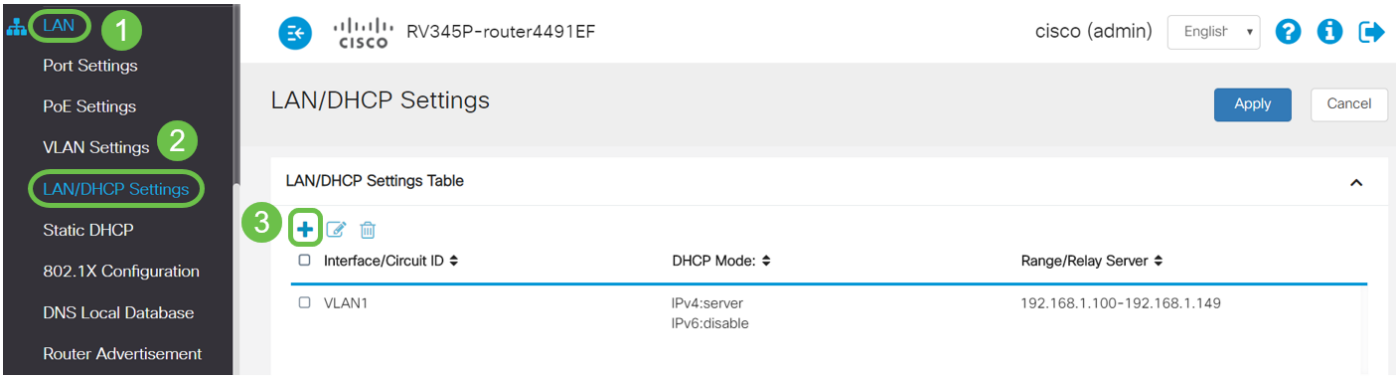
In questo scenario, il routing tra VLAN sarà abilitato sia per la VLAN1 che per la VLAN2 in modo che gli utenti di queste VLAN possano comunicare tra loro. Come misura di sicurezza, gli utenti VLAN2 non saranno in grado di accedere al server VLAN1 [IPv4 (Internet Protocol versione 4)]: 192.168.1.10 /24].

Porte router utilizzate:

- Il PC nella VLAN1 è collegato alla porta *LAN1*.
- Il PC nella VLAN2 è collegato alla porta *LAN2*.
- Il server nella VLAN1 è collegato alla porta *LAN3*.

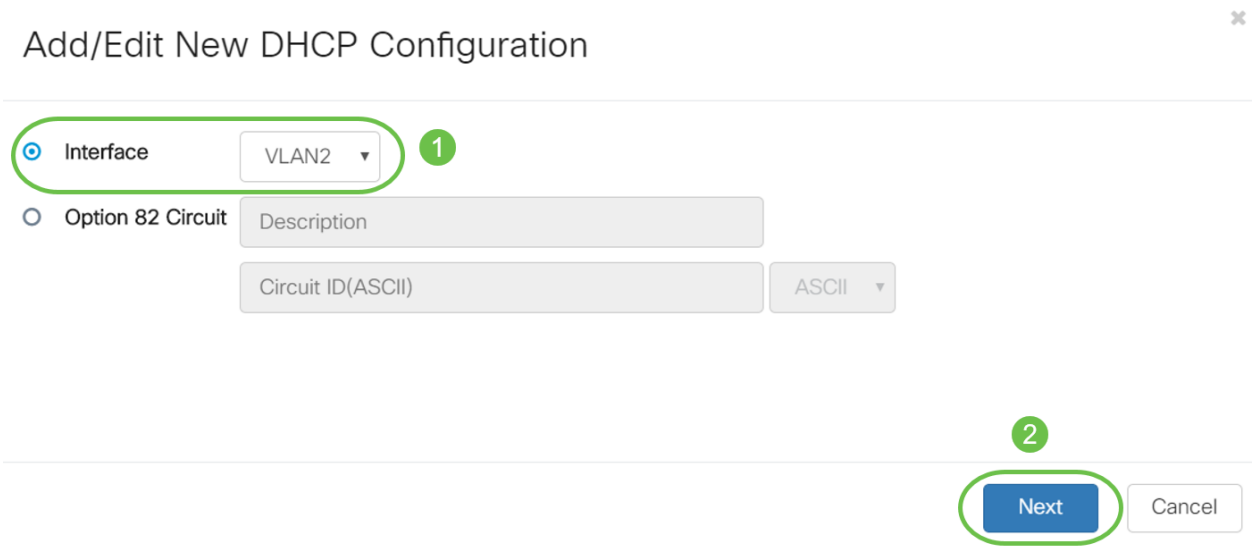
Configurazione

Passaggio 1. Accedere all'utility di configurazione Web del router. Per aggiungere una nuova interfaccia VLAN sul router, selezionare **LAN > Impostazioni LAN/DHCP**, quindi fare clic sul **segno più** nella *tabella Impostazioni LAN/DHCP*.

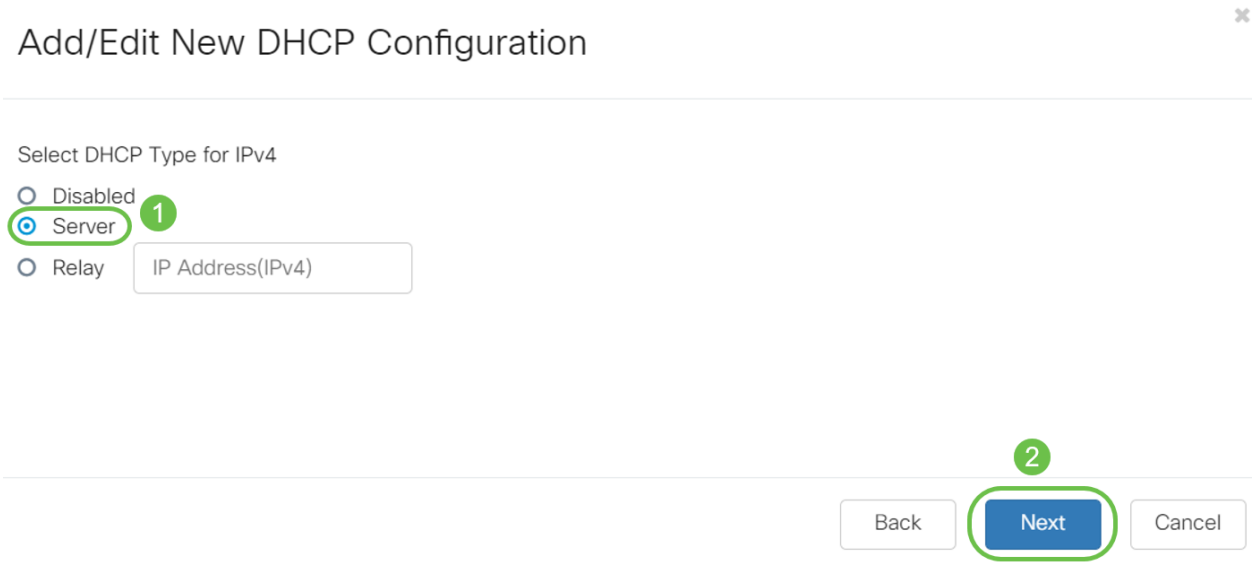


Nota: Per impostazione predefinita, l'interfaccia VLAN1 viene creata sul router RV34x su cui è abilitato il server DHCP (Dynamic Host Configuration Protocol) per IPv4.

Passaggio 2. Viene visualizzata una nuova finestra popup con l'**interfaccia** *VLAN2* selezionata, fare clic su **Next**.



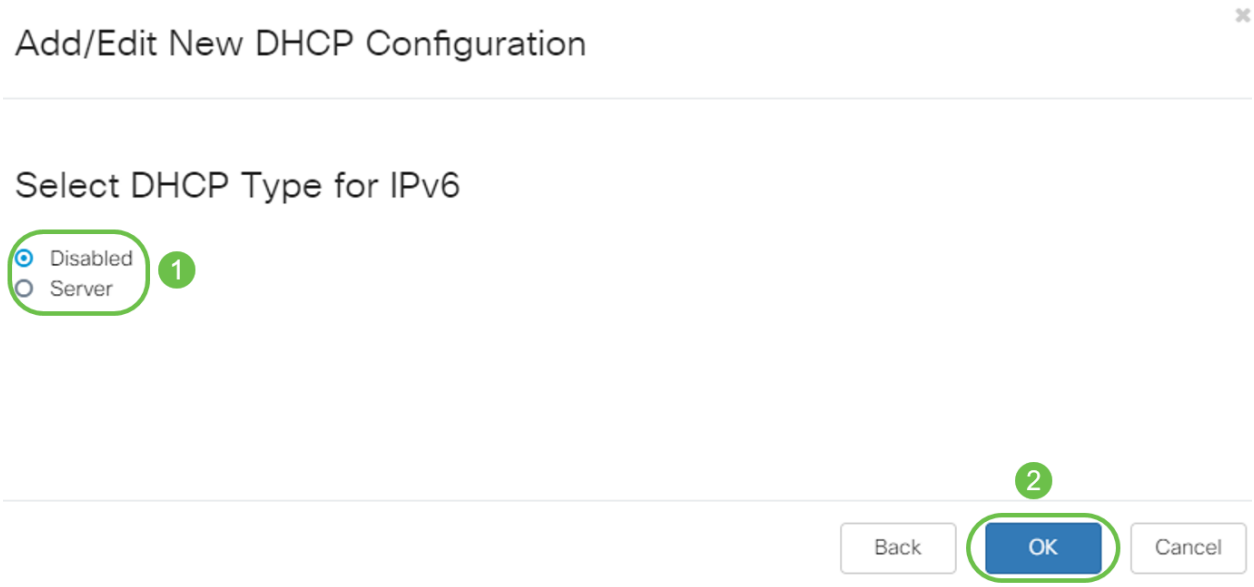
Passaggio 3. Per abilitare il server DHCP sull'interfaccia VLAN2, in *Select DHCP Type for IPv4* selezionare **Server**. Fare clic su **Next** (Avanti).



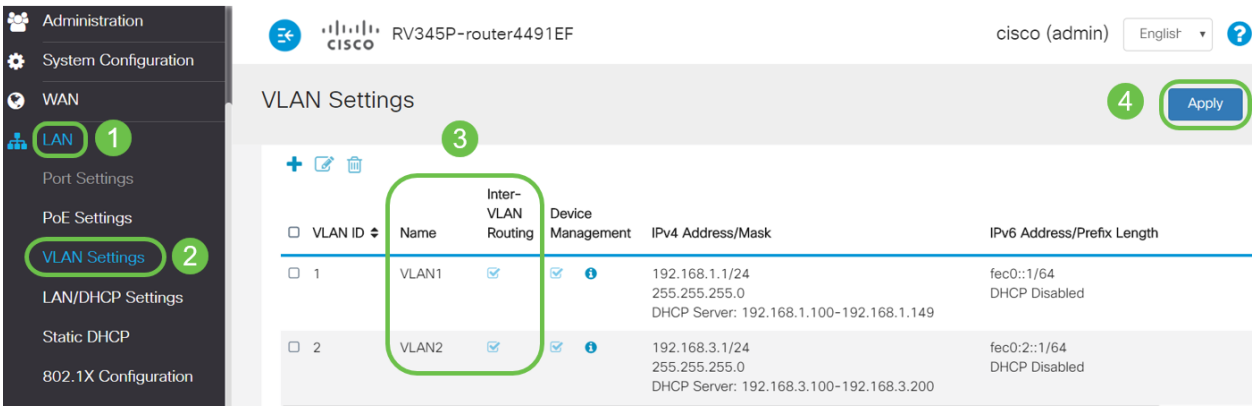
Passaggio 4. Immettere i parametri di configurazione del server DHCP, tra cui *Lease time client, Range Start*, *Range End* e *DNS Server.* Fare clic su **Next** (Avanti).

Passaggio 5. (Facoltativo) È possibile disabilitare il *tipo DHCP per IPv6* selezionando la casella di controllo **Disabilitato** poiché questo esempio è basato su IPv4. Fare clic su **OK**. Configurazione del server DHCP completata.

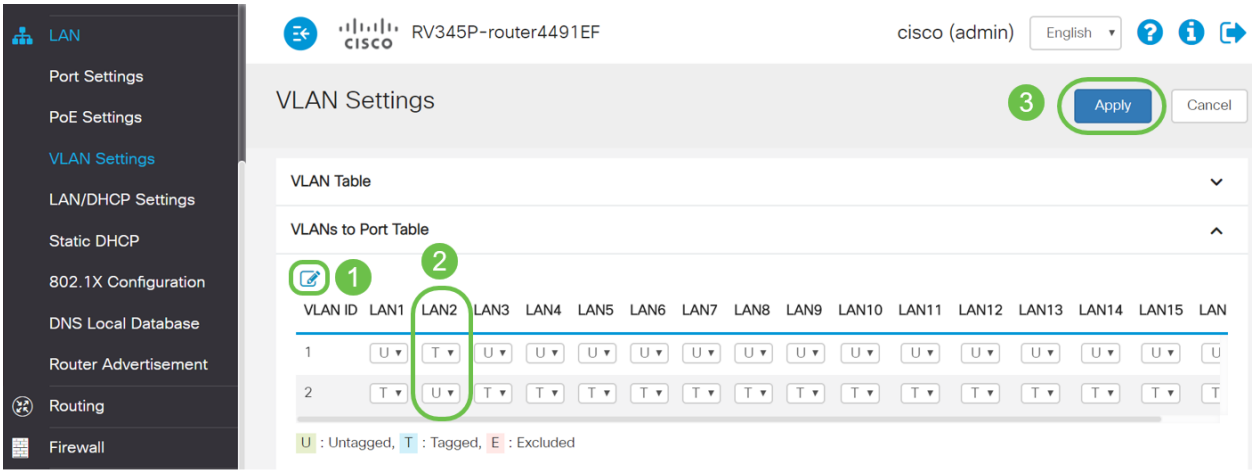
Nota: È possibile utilizzare IPv6.



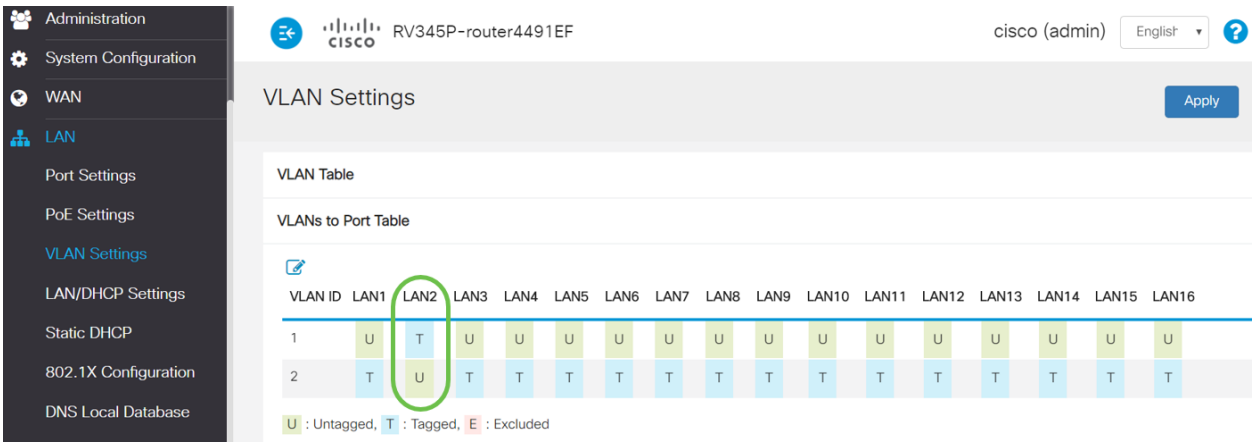
Passaggio 6. Passare a **LAN > Impostazioni VLAN** e verificare che il *routing tra VLAN* sia abilitato per entrambe le VLAN, VLAN1 e VLAN2. Questa configurazione abiliterà le comunicazioni tra le VLAN. Fare clic su **Apply** (Applica).



Passaggio 7. Per assegnare il traffico senza tag per la VLAN2 sulla porta *LAN2*, fare clic sul pulsante edit in *VLAN to Port Table* option. A questo punto, sotto la porta LAN2 selezionare l'opzione **T** (con tag) per *VLAN1* e **U** (senza tag) per *VLAN2* dal menu a discesa. Fare clic su **Apply** (Applica) per salvare la configurazione. Questa configurazione inoltrerà il traffico non codificato per la VLAN2 sulla porta LAN2 in modo che la scheda di interfaccia di rete (NIC, Network Interface Card) del PC, normalmente non in grado di associare il tag VLAN, possa ottenere l'IP DHCP dalla VLAN2 e far parte della VLAN2.

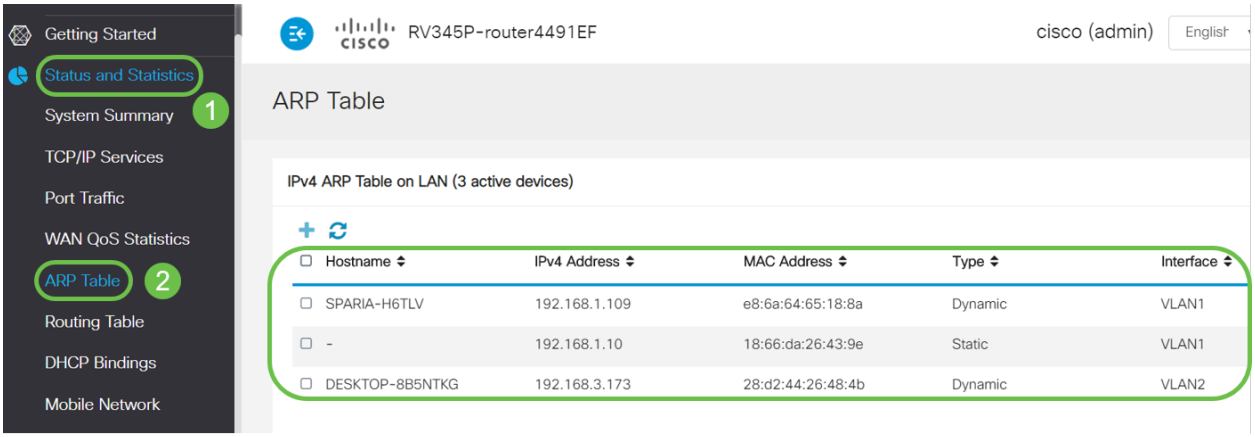


Passaggio 8. Verificare che le impostazioni della VLAN2 per la porta *LAN2* siano visualizzate come U *(Senza tag)*. Per le restanti porte LAN, le impostazioni VLAN2 saranno *T (con tag)* e il traffico VLAN1 *U (senza tag)*.

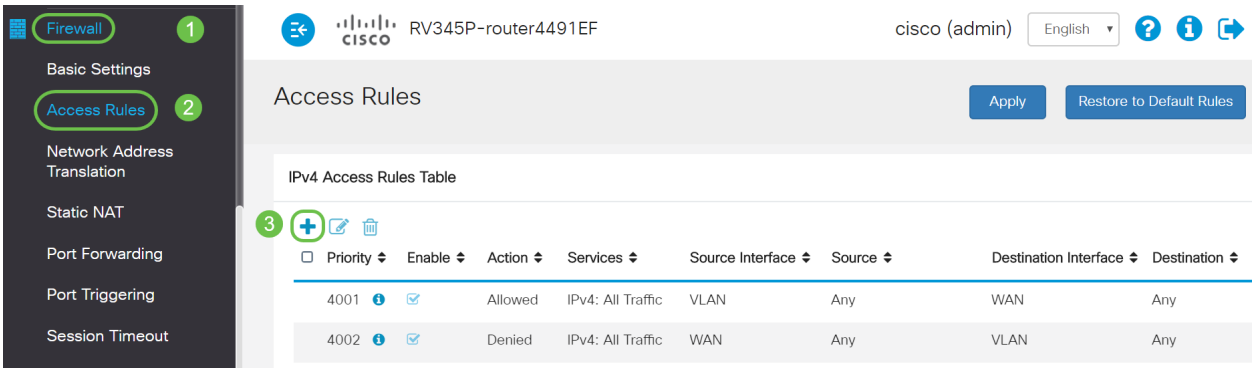


Passaggio 9. Selezionare **Status and Statistics > ARP Table** e verificare che l'*indirizzo IPv4* dinamico per i PC si trovi su VLAN diverse.

Nota: L'IP del server sulla VLAN1 è stato assegnato in modo statico.



Passaggio 10. Applicazione dell'ACL per limitare il server (IPv4: 192.168.1.10/24) da parte degli utenti VLAN2. Per configurare l'ACL, selezionare **Firewall > Regole di accesso** e fare clic sull' **icona con il segno più** per aggiungere una nuova regola.



Passaggio 11. Configurare i parametri *delle regole di accesso*. Per questo scenario i parametri saranno i seguenti:

Stato regola: Attiva

Azione: Nega

Servizi Tutto il traffico

Registro: Vero

Interfaccia di origine: VLAN2

Source address: Qualsiasi

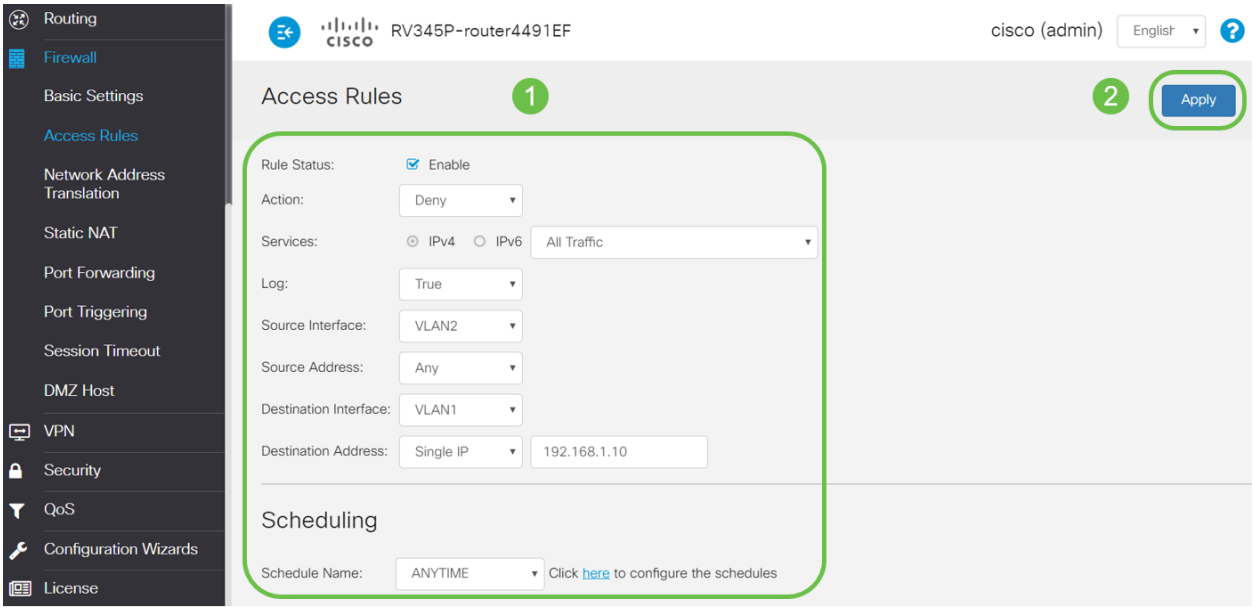
Interfaccia di destinazione: VLAN1

Indirizzo di destinazione: IP 192.168.1.10 singolo

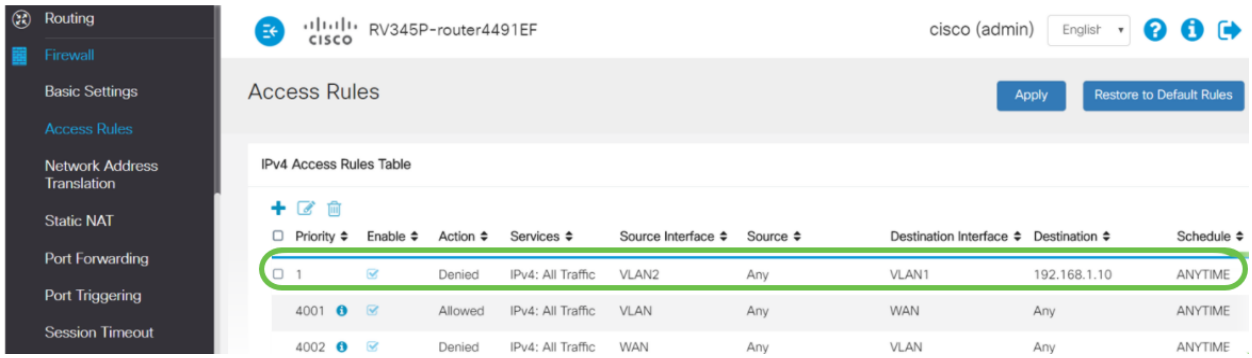
Nome pianificazione: In qualsiasi momento

Fare clic su **Apply** (Applica).

Nota: Nell'esempio, è stato negato l'accesso di qualsiasi dispositivo dalla VLAN2 al server e quindi è stato consentito l'accesso agli altri dispositivi collegati nella VLAN1. Le esigenze dell'utente potrebbero variare.



Passaggio 12. Nell'elenco *Regole di accesso* verrà visualizzato quanto segue:



La regola di accesso viene definita in modo esplicito per limitare l'accesso del server, 192.168.1.10, agli utenti VLAN2.

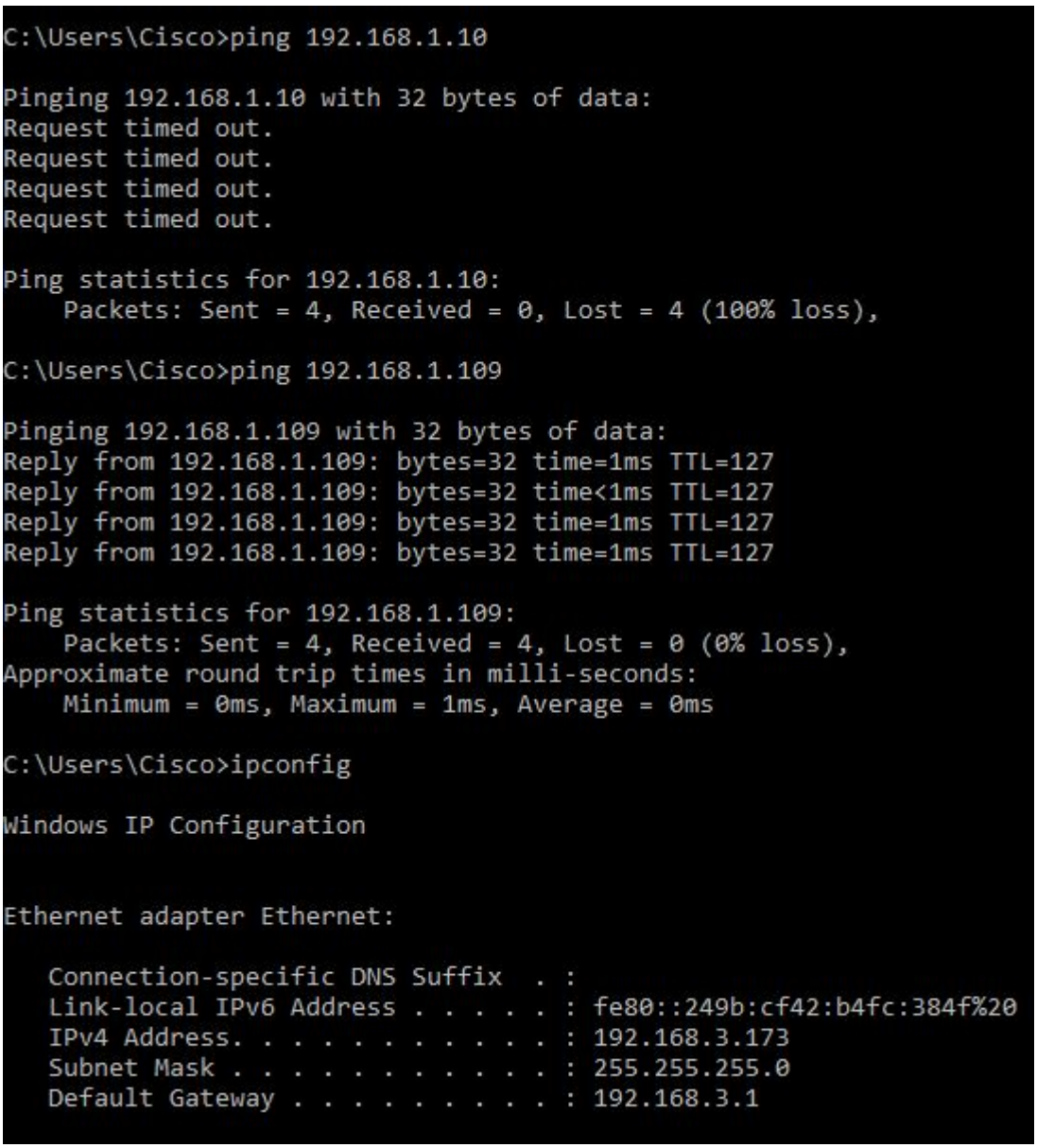
Verifica

Per verificare il servizio, aprire il prompt dei comandi. Per ottenere questo risultato sulle piattaforme Windows, fare clic sul pulsante Windows, digitare **cmd** nella casella di ricerca in basso

a sinistra del computer e selezionare **Prompt dei comandi** dal menu.

Immettere i seguenti comandi:

- Sul PC (192.168.3.173) nella VLAN2, eseguire il ping del server (IP: 192.168.1.10). Si riceverà una notifica di *timeout della richiesta* che indica che la comunicazione non è consentita.
- Sul PC (192.168.3.173) della VLAN2, eseguire il ping sull'altro PC (192.168.1.109) della VLAN1. La risposta verrà accettata.



Conclusioni

Dopo aver eseguito le operazioni necessarie per configurare il routing tra VLAN su un router serie RV34x, è possibile istruzioni su come eseguire una restrizione ACL di destinazione. Ora è possibile acquisire tutte queste conoscenze e utilizzarle per creare VLAN nella rete in grado di soddisfare le proprie esigenze.