

Configurazione delle proprietà di ispezione Address Resolution Protocol (ARP) sugli switch gestiti serie 300

Obiettivo

Il protocollo ARP (Address Resolution Protocol) viene utilizzato per mappare gli indirizzi IP agli indirizzi MAC. L'ispezione ARP è utilizzata per proteggere una rete dagli attacchi ARP. L'ispezione ARP aumenta la sicurezza del traffico ispezionando i pacchetti che si trovano su interfacce definite non attendibili nella pagina *Impostazioni interfaccia*. Quando un pacchetto arriva su un'interfaccia non attendibile, il controllo ARP controlla l'indirizzo IP di origine e l'indirizzo MAC del pacchetto. Se corrispondono all'indirizzo IP e all'indirizzo MAC specificati nelle regole di controllo d'accesso ARP, il pacchetto viene inoltrato, altrimenti viene scartato.

In questo documento viene spiegato come configurare l'ispezione ARP sugli switch gestiti serie 300.

Dispositivi interessati

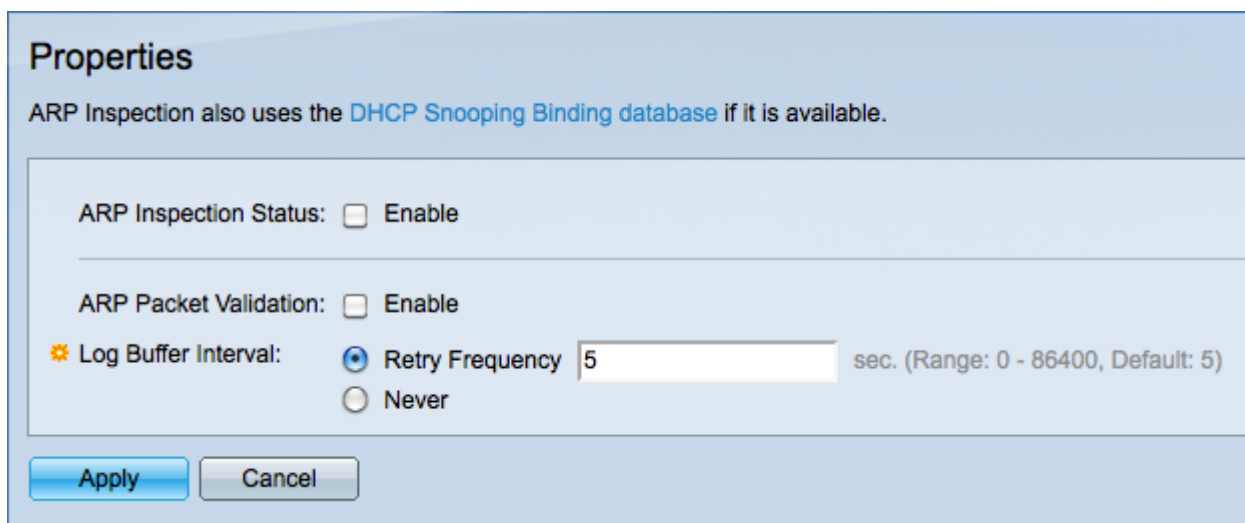
•SF/SG serie 300 Managed Switch

Versione del software

•1.3.0.62

Proprietà

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Protezione > Ispezione ARP > Proprietà**. Viene visualizzata la pagina *Proprietà*:



The screenshot shows the 'Properties' configuration window for ARP Inspection. At the top, it states: 'ARP Inspection also uses the DHCP Snooping Binding database if it is available.' Below this, there are three main settings:

- ARP Inspection Status:** A checkbox labeled 'Enable' is currently unchecked.
- ARP Packet Validation:** A checkbox labeled 'Enable' is currently unchecked.
- Log Buffer Interval:** A radio button labeled 'Retry Frequency' is selected, with a text input field containing the value '5'. To the right of the input field, it says 'sec. (Range: 0 - 86400, Default: 5)'. A radio button labeled 'Never' is also present but unselected.

At the bottom of the window, there are two buttons: 'Apply' and 'Cancel'.

Passaggio 2. Selezionare la casella di controllo **Abilita** nel campo Stato ispezione ARP per abilitare l'ispezione ARP.

Passaggio 3. (Facoltativo) Selezionare la casella di controllo **Abilita** nel campo Convalida

pacchetto ARP per abilitare le seguenti convalide. I pacchetti considerati non validi dalla verifica ARP vengono registrati e scartati.

- MAC di origine: confronta l'indirizzo MAC di origine del pacchetto con l'indirizzo MAC del mittente nella richiesta ARP. Questo controllo viene eseguito sia per le richieste ARP che per le risposte ARP.

- MAC di destinazione: confronta l'indirizzo MAC di destinazione del pacchetto con l'indirizzo MAC di destinazione dell'interfaccia. Questo controllo viene eseguito solo per le risposte ARP.

- Indirizzi IP — confronta il corpo ARP con indirizzi IP non validi. Questi indirizzi includono 0.0.0.0, 255.255.255.255 e tutti gli indirizzi multicast IP.

Passaggio 4. Fare clic sul pulsante di opzione corrispondente all'opzione desiderata nel campo Intervallo buffer di log. Se l'indirizzo IP di origine del pacchetto in arrivo non viene trovato dalla ispezione ARP, il pacchetto viene scartato e viene inviato un messaggio SYSLOG. L'intervallo del buffer di registro è l'intervallo di tempo tra i messaggi SYSLOG.

- Frequenza tentativi: immettere il valore che definisce la frequenza (in secondi) con cui vengono inviati i messaggi dei pacchetti ignorati da SYSLOG.

- Mai — disabilita i messaggi di pacchetto ignorati da SYSLOG.

Passaggio 5. Fare clic su **Applica** per salvare le modifiche o su **Annulla** per annullarle.