

Configurazione di ACL (Access Control List) e ACE (Access Control Entry) basati su MAC sugli switch gestiti serie 300

Obiettivo

Un elenco di controllo di accesso (ACL, Access Control List) è una tecnologia di sicurezza utilizzata per autorizzare o negare il flusso del traffico di rete. Gli ACL basati sull'indirizzo MAC utilizzano le informazioni di layer 2 per autorizzare o negare l'accesso al traffico. Una voce di controllo di accesso (ACE, Access Control Entry) contiene i criteri della regola di accesso effettiva. Una volta creata, la voce ACE viene applicata a un ACL. Gli switch gestiti serie 300 supportano un massimo di 512 ACL e 512 ACE.

In questo documento viene spiegato come creare gli ACL basati sull'indirizzo MAC e come applicare gli ACE agli ACL sugli switch gestiti serie 300.

Dispositivi interessati

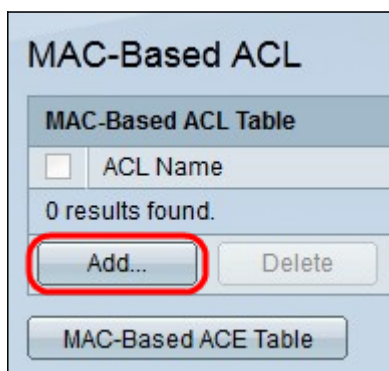
- SG/SF serie 300 Managed Switch

Versione del software

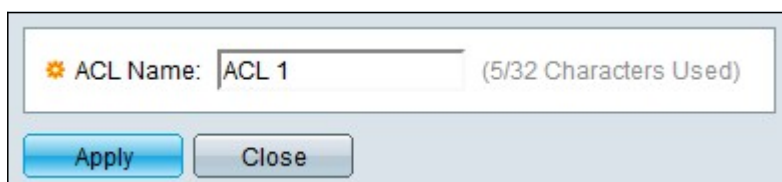
- 1.3.0.62

ACL basato su MAC

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Controllo accesso > ACL basato su MAC**. Viene visualizzata la pagina *ACL basato su MAC*:

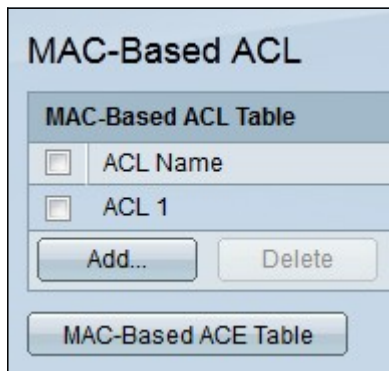


Passaggio 2. Fare clic su **Add**. Viene visualizzata la finestra *Add MAC-Based ACL*.



Passaggio 3. Inserire un nome per l'ACL nel campo Nome ACL.

Passaggio 4. Fare clic su **Applica**. Viene creato l'ACL.



ACE basato su MAC

Quando si riceve un frame su una porta, lo switch lo elabora tramite il primo ACL. Se il frame corrisponde a un filtro ACE del primo ACL, viene eseguita l'azione ACE. Se il frame non corrisponde a nessuno dei filtri ACE, viene elaborato l'ACL successivo. Se non viene trovata alcuna corrispondenza con nessuna voce ACE in tutti gli ACL rilevanti, il frame viene scartato per impostazione predefinita.

Nota: questa azione predefinita può essere evitata creando una voce ACE a bassa priorità che autorizzi tutto il traffico.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Controllo accesso > MAC Based ACE**. Viene visualizzata la pagina *MAC Based ACE*:

Passaggio 2. Dall'elenco a discesa Nome ACL, scegliere un ACL a cui applicare una regola.

Passaggio 3. Fare clic su **Vai**. Vengono visualizzate le voci ACE già configurate per l'ACL.

Passaggio 4. Fare clic su **Add** per aggiungere una nuova regola all'ACL. Viene visualizzata la finestra *Aggiungi ACE basata su MAC*.

Nel campo Name (Nome ACL) viene visualizzato il nome dell'ACL.

Passaggio 5. Inserire il valore di priorità per la voce ACE nel campo Priorità. Le voci di controllo di accesso con priorità più alta vengono elaborate per prime. Il valore 1 rappresenta la priorità più alta.

Passaggio 6. Fare clic sul pulsante di opzione corrispondente all'azione desiderata eseguita quando un frame soddisfa i criteri richiesti dell'ACE.

- Permit: lo switch inoltra i pacchetti che soddisfano i criteri richiesti dall'ACE.
- Nega: lo switch scarta i pacchetti che non soddisfano i criteri richiesti dall'ACE.
- Shutdown: lo switch scarta i pacchetti che non soddisfano i criteri richiesti dall'ACE e disabilita la porta a cui sono stati ricevuti.

Nota: le porte disabilite possono essere riattivate nella pagina *Impostazioni porta*.

Passaggio 7. Selezionare la casella di controllo **Abilita** nel campo Intervallo di tempo per consentire la configurazione di un intervallo di tempo per la voce ACE. Gli intervalli di tempo vengono utilizzati per limitare il periodo di validità di un ACE.

Passaggio 8. Dall'elenco a discesa Nome intervallo di tempo, scegliere un intervallo di tempo da applicare all'ACE.

Nota: fare clic su **Modifica** per passare a un intervallo di tempo e crearlo nella pagina

Intervallo di tempo.

Passaggio 9. Fare clic sul pulsante di opzione corrispondente ai criteri desiderati per l'ACE nel campo Indirizzo MAC di destinazione.

Passaggio 10. Fare clic sul pulsante di opzione corrispondente ai criteri desiderati per l'ACE nel campo Indirizzo MAC di origine.

- Qualsiasi - Tutti gli indirizzi MAC di destinazione vengono applicati all'ACE.
- Definito dall'utente: immettere un indirizzo MAC e una maschera jolly MAC da applicare all'ACE nei campi Valore indirizzo MAC destinazione e Maschera jolly MAC destinazione. Le maschere con caratteri jolly vengono utilizzate per definire un intervallo di indirizzi MAC.
- Qualsiasi - Tutti gli indirizzi MAC di origine vengono applicati all'ACE.
- Definito dall'utente: immettere un indirizzo MAC e una maschera jolly MAC da applicare all'ACE nei campi Valore indirizzo MAC destinazione e Maschera jolly MAC destinazione. Le maschere con caratteri jolly vengono utilizzate per definire un intervallo di indirizzi MAC.

Passaggio 11. Immettere un ID VLAN che verrà associato al tag VLAN del frame.

Passaggio 12. (Facoltativo) Per includere i valori 802.1p nei criteri ACE, selezionare **Includi** nel campo 802.1p. 802.1p coinvolge la tecnologia Class of Service (CoS). CoS è un campo a 3 bit in un frame Ethernet utilizzato per differenziare il traffico.

Passaggio 13. Se sono inclusi valori 802.1p, immettere i campi riportati di seguito.

- Valore 802.1p: immettere il valore 802.1p da associare. 802.1p è una specifica che consente agli switch di layer 2 di assegnare le priorità al traffico e di eseguire il filtro multicast dinamico.
- Maschera 802.1p — immettere la maschera con caratteri jolly dei valori 802.1p. Questa maschera con caratteri jolly viene utilizzata per definire l'intervallo di valori 802.1p.

Passaggio 14. Inserire l'Ethertype del frame da abbinare. Ethertype è un campo a due ottetti in un frame Ethernet utilizzato per indicare il protocollo utilizzato per il payload del frame.

Passaggio 15. Fare clic su **Applica**. Viene creata la voce ACE. In questo esempio, la voce ACE creata impedisce il traffico inviato dagli indirizzi MAC di origine definiti a tutti gli indirizzi di destinazione.