# Configurazione di ACL (Access Control List) e ACE (Access Control Entry) basati su IPv4 su uno switch

## Obiettivo

Un elenco di controllo di accesso (ACL, Access Control List) è un elenco di filtri del traffico di rete e di azioni correlate utilizzato per migliorare la sicurezza. Blocca o consente agli utenti di accedere a risorse specifiche. Un ACL contiene gli host a cui è consentito o negato l'accesso al dispositivo di rete.

L'ACL basato su IPv4 è un elenco di indirizzi IPv4 di origine che usano le informazioni di layer 3 per autorizzare o negare l'accesso al traffico. Gli ACL IPv4 limitano il traffico connesso all'IP in base ai filtri IP configurati. Un filtro contiene le regole per trovare una corrispondenza con un pacchetto IP e, se il pacchetto corrisponde, la regola stabilisce anche se il pacchetto deve essere autorizzato o rifiutato.

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.

Èconsigliabile utilizzare gli elenchi degli accessi per fornire un livello di protezione di base per l'accesso alla rete. Se non si configurano gli elenchi degli accessi sui dispositivi di rete, tutti i pacchetti che passano attraverso lo switch o il router potrebbero essere autorizzati su tutte le parti della rete.

In questo documento viene spiegato come configurare gli ACL e gli ACE basati su IPv4 sullo switch gestito.

## Dispositivi interessati

- Serie Sx350
- Serie SG350X
- Serie Sx500
- Serie Sx550X

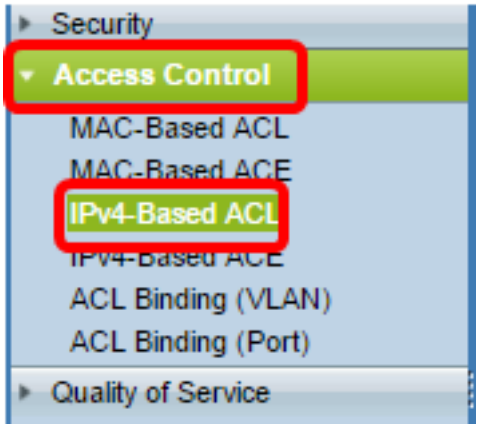
## Versione del software

- 1.4.5.02 - Serie Sx500
- 2.2.5.68 - Serie Sx350, Serie SG350X, Serie Sx550X

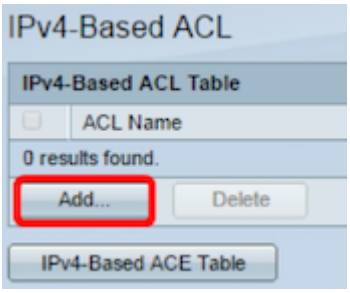
## Configurazione di ACL e ACE basati su IPv4

### Configurazione di ACL basati su IPv4

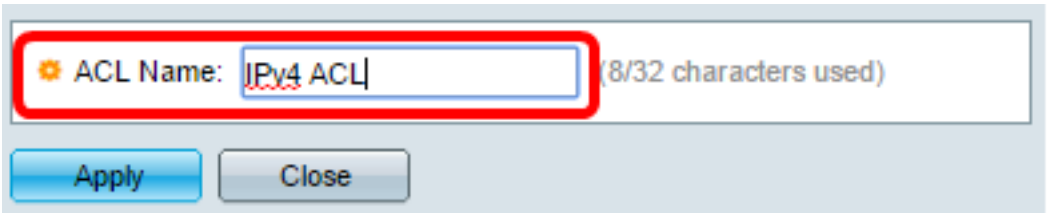
Passaggio 1. Accedere all'utility basata sul Web, quindi selezionare **Controllo dell'accesso > ACL basato su IPv4**.




Passaggio 2. Fare clic sul pulsante **Aggiungi**.

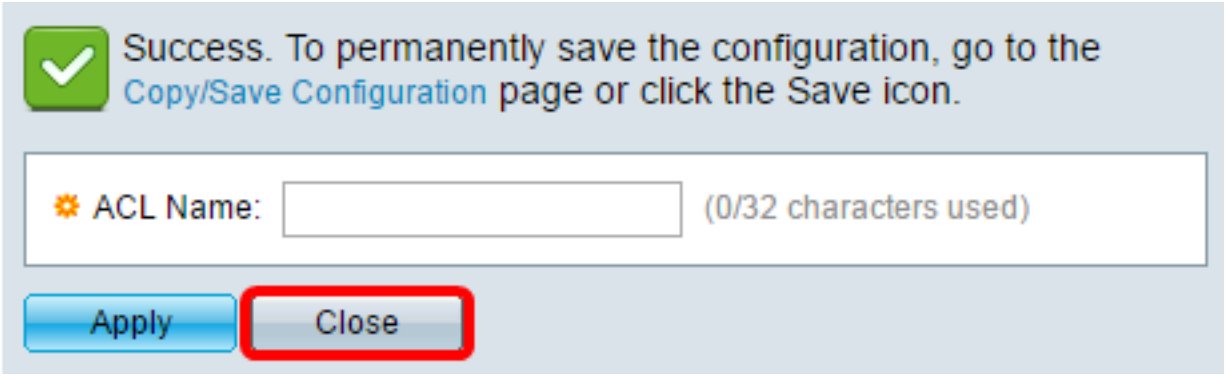



Passaggio 3. Inserire il nome del nuovo ACL nel campo *Nome ACL*.




**Nota:** Nell'esempio, viene usato un ACL IPv4.

Passaggio 4. Fare clic su **Apply** (Applica), quindi su **Close** (Chiudi).




Passaggio 5. (Facoltativo) Fare clic su **Save** (Salva) per salvare le impostazioni nel file della configurazione di avvio.


A questo punto, è necessario configurare un ACL basato su IPv4 sullo switch.

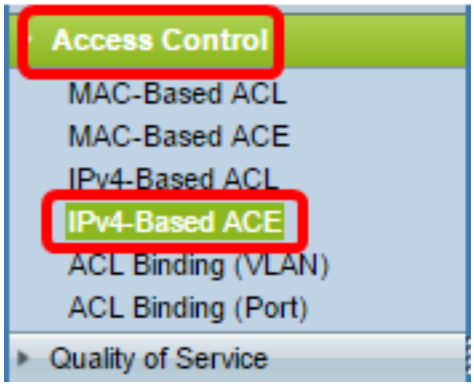
## Configurare la voce ACE basata su IPv4

Quando si riceve un pacchetto su una porta, lo switch lo elabora tramite il primo ACL. Se il pacchetto corrisponde a un filtro ACE del primo ACL, viene eseguita l'azione ACE. Se il pacchetto 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 pacchetto viene scartato per impostazione predefinita.

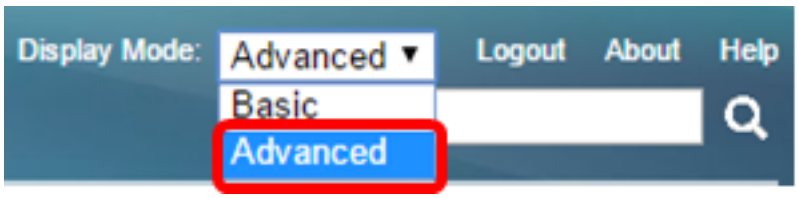
In questo scenario, verrà creata una voce ACE per impedire il traffico inviato da un indirizzo IPv4 di origine definito dall'utente a qualsiasi indirizzo di destinazione.

**Nota:** Per evitare questa azione predefinita, è possibile creare una voce ACE a bassa priorità che autorizzi tutto il traffico.

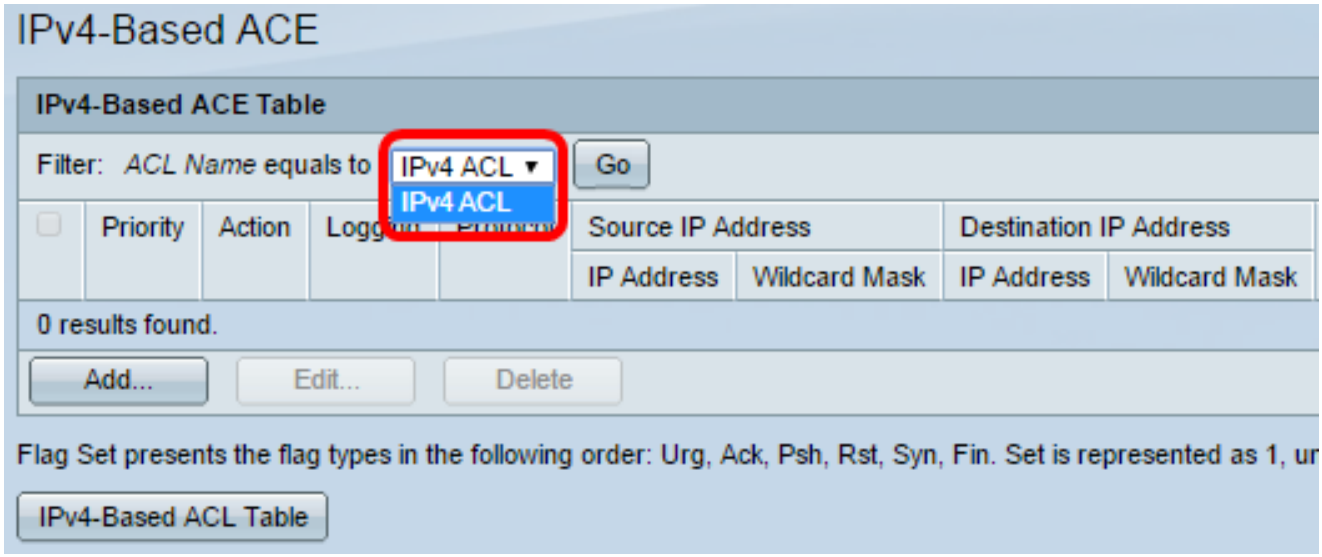
Passaggio 1. Nell'utility basata sul Web, selezionare **Controllo dell'accesso > ACE basata su IPv4**.




**Importante:** Per usare al meglio le funzioni e le caratteristiche dello switch, passare alla modalità Avanzata scegliendo **Avanzate** dall'elenco a discesa Display Mode (Modalità di visualizzazione) nell'angolo superiore destro della pagina.




Passaggio 2. Scegliere un ACL dall'elenco a discesa Nome ACL, quindi fare clic su **Vai**.

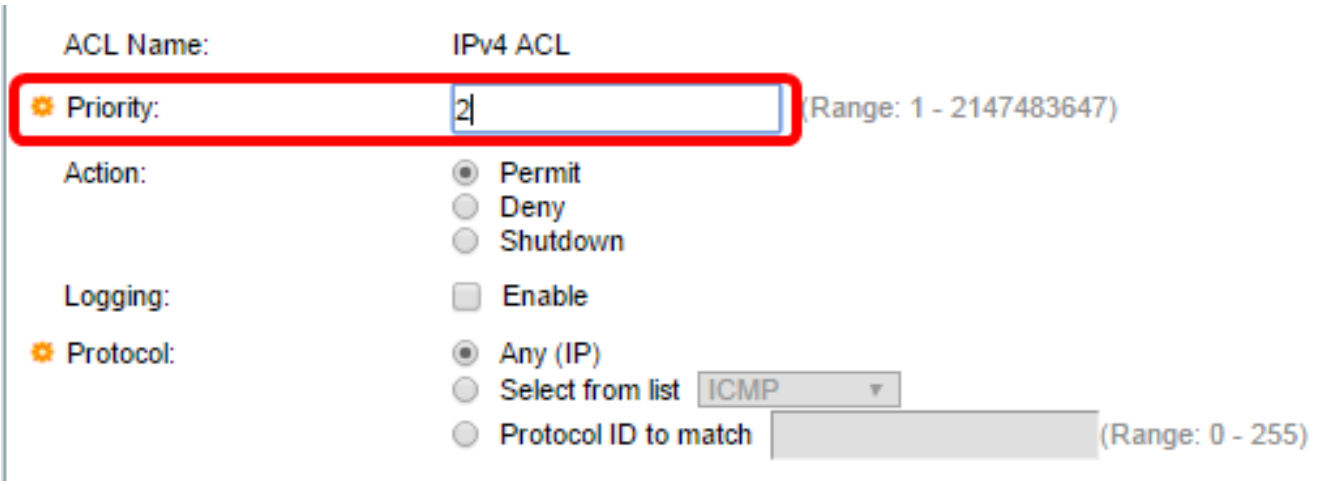



**Nota:** Le voci ACE già configurate per l'ACL verranno visualizzate nella tabella.

Passaggio 3. Fare clic sul pulsante **Add** per aggiungere una nuova regola all'ACL.

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

Passaggio 4. 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. L'intervallo è compreso tra 1 e 2147483647.




**Nota:** Nell'esempio viene utilizzato 2.

Passaggio 5. Fare clic sul pulsante di opzione corrispondente all'azione desiderata eseguita quando un frame soddisfa i criteri richiesti dell'ACE.

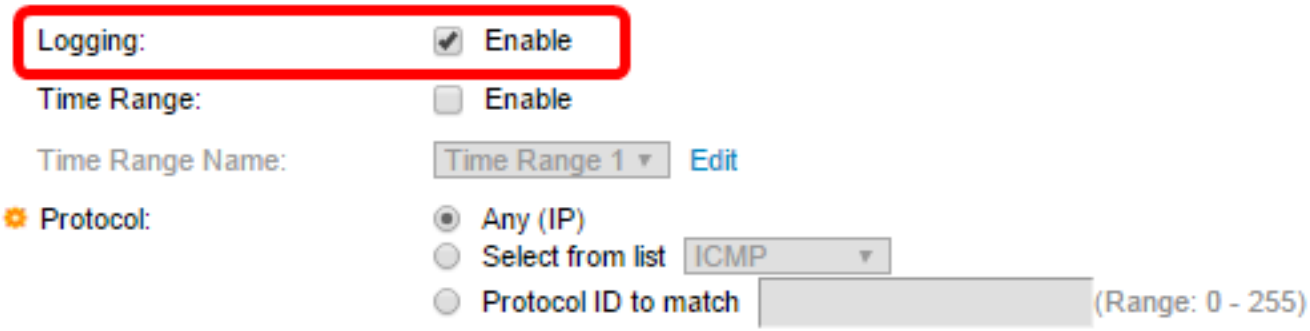
**Nota:** Nell'esempio riportato di seguito, viene selezionato Permit.

- Permit: lo switch inoltra i pacchetti che soddisfano i criteri richiesti dall'ACE.

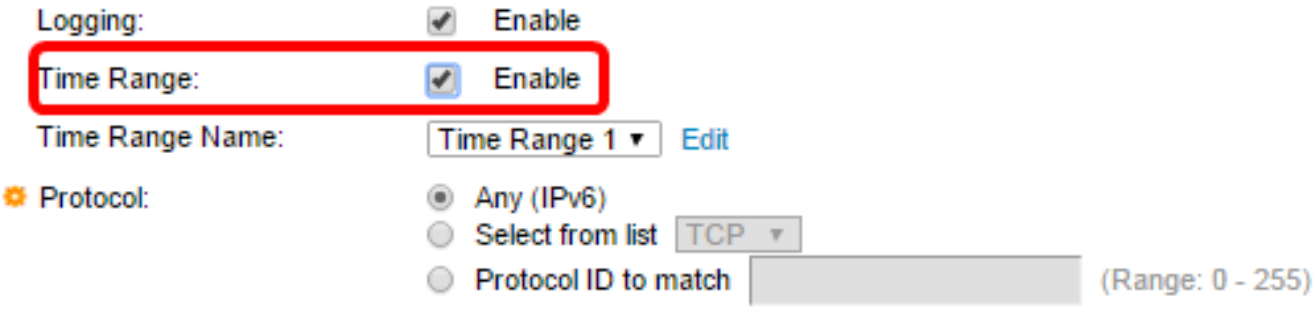
- Nega: lo switch scarta i pacchetti che soddisfano i criteri richiesti dell'ACE.
- Shutdown: lo switch scarta i pacchetti che non soddisfano i criteri richiesti dall'ACE e disabilita la porta a cui sono stati ricevuti.

**Nota:** Le porte disabilitate possono essere riattivate nella pagina Impostazioni porta.

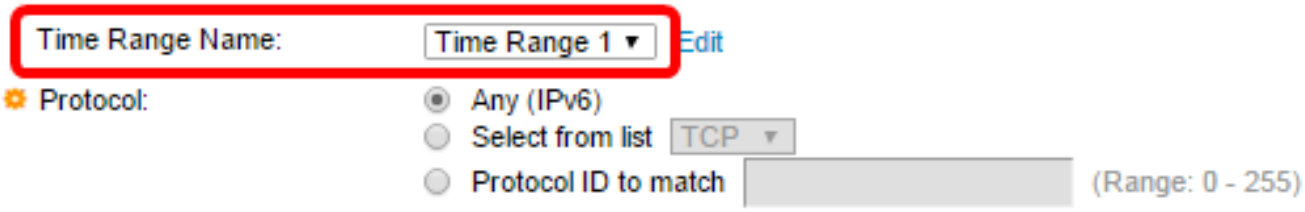
Passaggio 6. (Facoltativo) Selezionare la casella di controllo **Abilita** registrazione per abilitare la registrazione dei flussi ACL che corrispondono alla regola ACL.



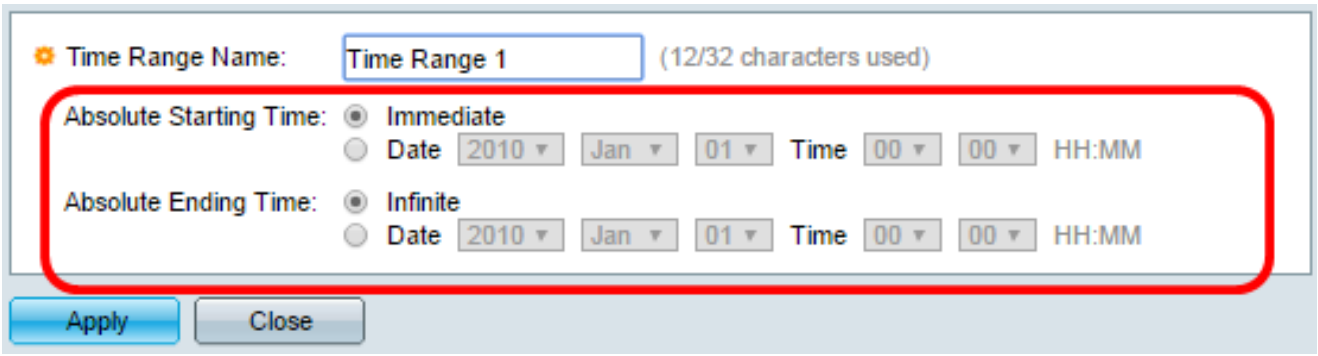

Passaggio 7. (Facoltativo) Selezionare la casella di controllo **Abilita** intervallo di tempo per consentire la configurazione di un intervallo di tempo per l'ACE. Gli intervalli di tempo vengono utilizzati per limitare il periodo di validità di un ACE.



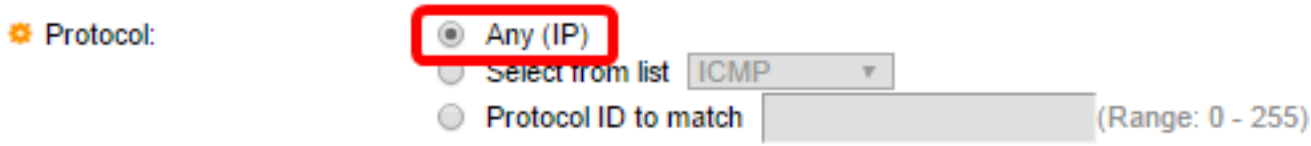

Passaggio 8. (Facoltativo) Dall'elenco a discesa Nome intervallo di tempo, scegliere un intervallo di tempo da applicare alla voce ACE.




**Nota:** È possibile fare clic su **Modifica** per spostarsi all'interno della pagina Intervallo di tempo e creare un intervallo di tempo.




Passaggio 9. Scegliere un tipo di protocollo nell'area Protocollo. La voce ACE verrà creata in base a un protocollo o a un ID di protocollo specifico.

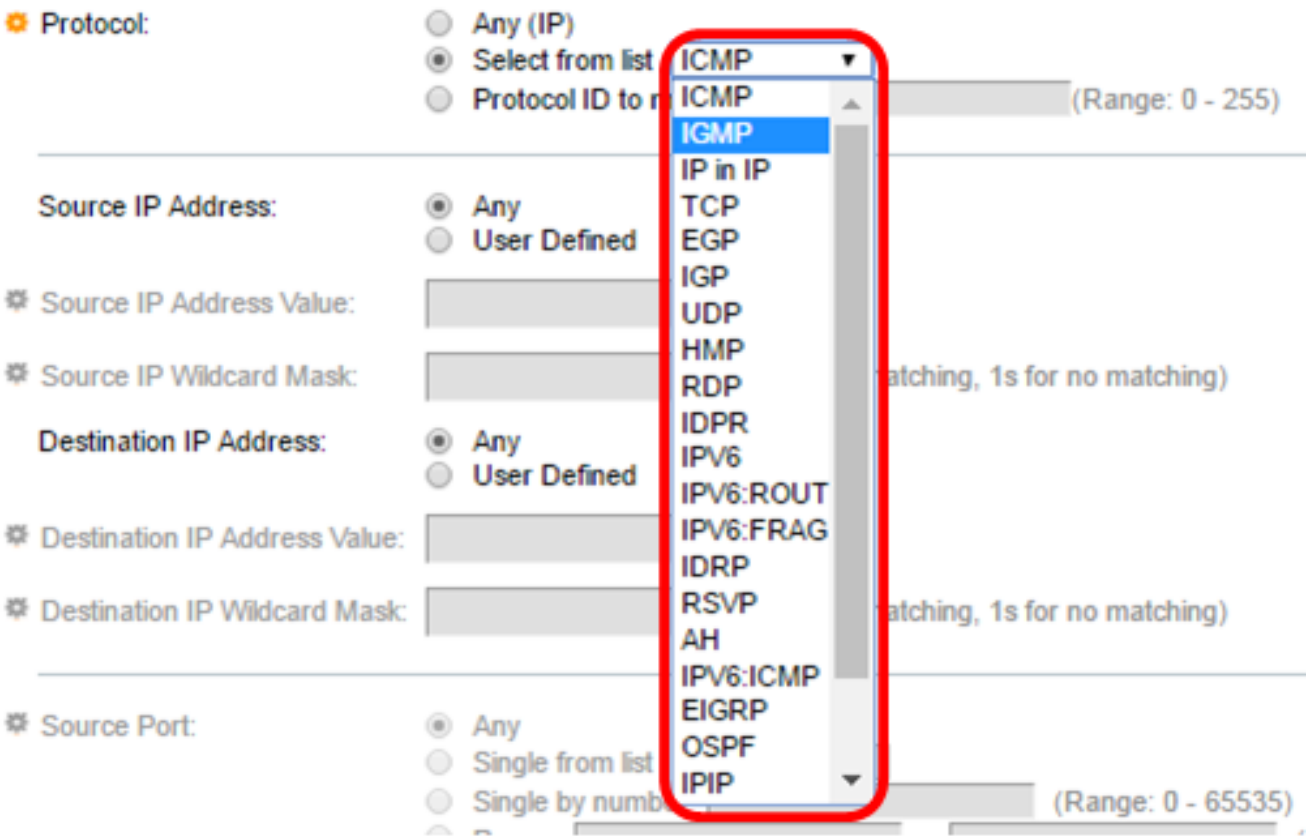



Le opzioni sono:

- Any (IP) — Questa opzione consente di configurare l'ACE in modo che accetti tutti i protocolli IP.
- Select from list: questa opzione consente di scegliere un protocollo dall'elenco a discesa. Se si preferisce questa opzione, andare al passaggio 10.
- ID protocollo corrispondente - questa opzione consente di immettere un ID protocollo. Se si preferisce questa opzione, andare al passaggio 11.

**Nota:** Nell'esempio, viene scelto Any (IP).

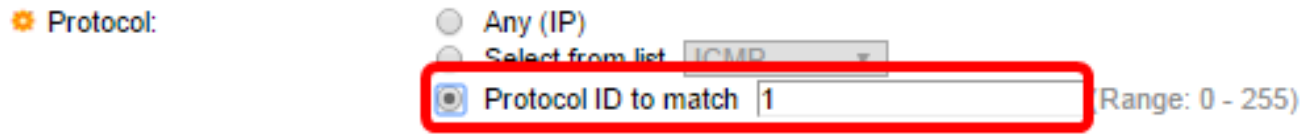
Passaggio 10. (Facoltativo) Se si sceglie Seleziona da elenco nel passaggio 9, scegliere un protocollo dall'elenco a discesa.




Le opzioni sono:

- ICMP — Internet Control Message Protocol
- IP in IP — IP in IP encapsulation
- TCP — Transmission Control Protocol
- EGP — Exterior Gateway Protocol
- IGP — Interior Gateway Protocol
- UDP — User Datagram Protocol
- HMP — Host Mapping Protocol
- RDP — Reliable Datagram Protocol
- IDPR — Routing delle policy tra domini
- IPV6 — Tunneling IPv6 su IPv4
- IPV6:ROUTER — Corrisponde ai pacchetti appartenenti alla route IPv6 su IPv4 tramite un gateway
- IPV6:FRAG — Corrisponde ai pacchetti appartenenti all'intestazione di frammento IPv6 su IPv4
- IDRP — Protocollo di routing tra domini IS-IS
- RSVP — Protocollo ReSerVation
- AH — Authentication Header
- IPV6:ICMP — ICMP per IPv6
- EIGRP — Enhanced Interior Gateway Routing Protocol
- OSPF: Open Shortest Path First
- IPIP — IP in IP
- PIM — Protocol Independent Multicast
- L2TP: protocollo di tunneling di livello 2

Passaggio 11. (Facoltativo) Se nel passaggio 9 è stata scelta la corrispondenza per ID protocollo, immettere l'ID protocollo nel campo *ID protocollo da associare*.



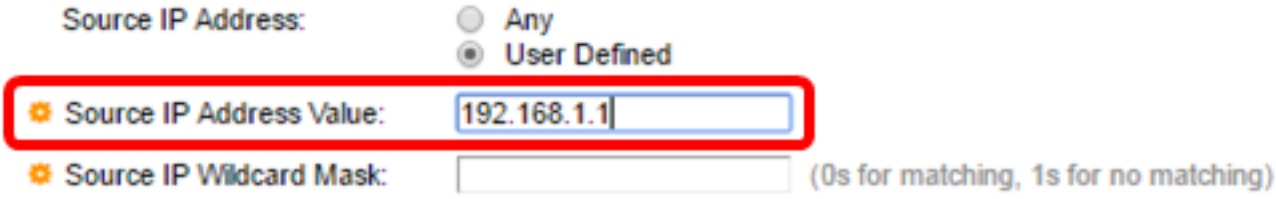

Passaggio 12. Fare clic sul pulsante di opzione corrispondente ai criteri desiderati per l'ACE nell'area Source IP Address (Indirizzo IP di origine).


Le opzioni sono:

- Qualsiasi: tutti gli indirizzi IPv4 di origine vengono applicati all'ACE.
- Definito dall'utente: immettere un indirizzo IP e una maschera con caratteri jolly IP da applicare alla voce ACE nei campi *Valore indirizzo IP di origine* e *Maschera con caratteri jolly IP di origine*. Le maschere con caratteri jolly vengono utilizzate per definire un intervallo di indirizzi IP.

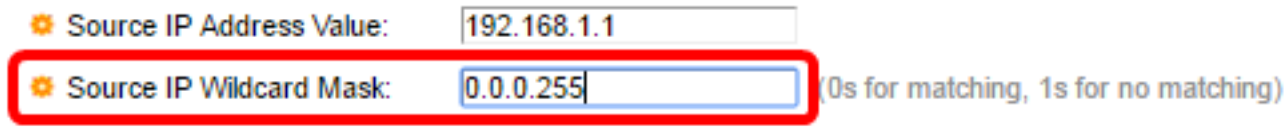
**Nota:** In questo esempio, viene scelto Definito dall'utente. Se si sceglie Qualsiasi, andare al passo 15.

Passaggio 13. Immettere l'indirizzo IP di origine nel campo *Valore indirizzo IP di origine*.



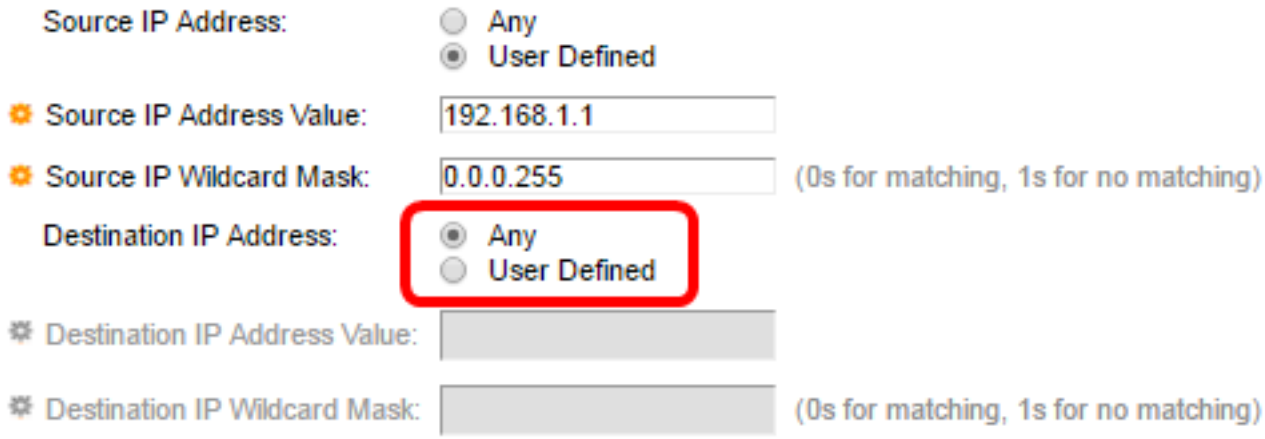

**Nota:** nell'esempio viene usato 192.168.1.1.

Passaggio 14. Immettere la maschera con caratteri jolly di origine nel campo *Maschera con caratteri jolly IP di origine*.




**Nota:** Nell'esempio viene utilizzato 0.0.0.255.

Passaggio 15. Fare clic sul pulsante di opzione corrispondente ai criteri desiderati per l'ACE nell'area Indirizzo IP di destinazione.

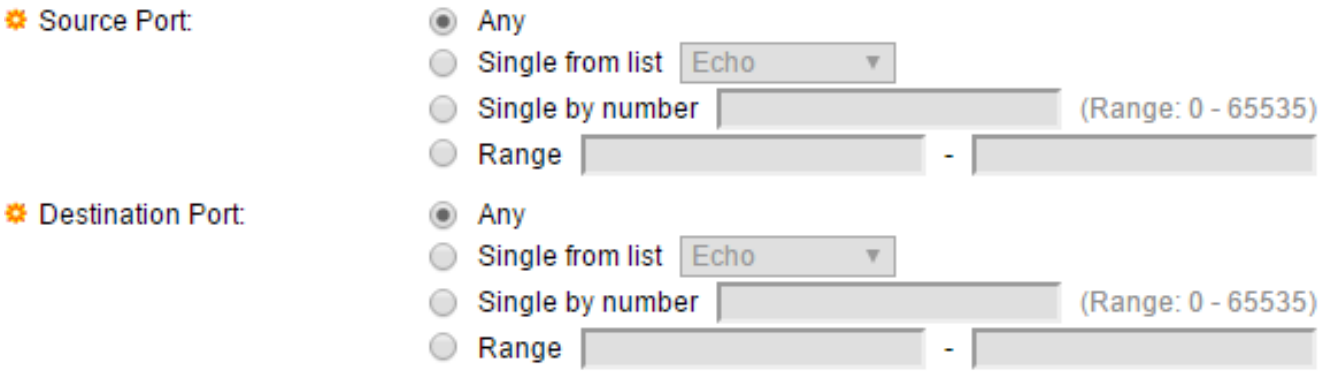



Le opzioni sono:

- Qualsiasi: tutti gli indirizzi IPv4 di destinazione vengono applicati all'ACE.
- Definito dall'utente: immettere un indirizzo IP e una maschera con caratteri jolly IP da applicare alla voce di controllo di accesso nei campi *Valore indirizzo IP di destinazione* e *Maschera con caratteri jolly IP di destinazione*. Le maschere con caratteri jolly vengono utilizzate per definire un intervallo di indirizzi IP.

**Nota:** Nell'esempio, viene scelto Qualsiasi. Scegliendo questa opzione, la voce ACE da creare consentirà il traffico ACE proveniente dall'indirizzo IPv4 specificato e diretto a qualsiasi destinazione.

Passaggio 16. (Facoltativo) Fare clic su un pulsante di opzione nell'area Porta di origine. Il valore predefinito è Any.




- Any — corrisponde a tutte le porte di origine.
- Single from list: è possibile scegliere una singola porta di origine TCP/UDP a cui far corrispondere i pacchetti. Questo campo è attivo solo se si sceglie 800/6-TCP o 800/17-UDP dal menu a discesa Select from List (Scegli dall'elenco).
- Singola in base al numero: è possibile scegliere una singola porta di origine TCP/UDP a cui associare i pacchetti. Questo campo è attivo solo se si sceglie 800/6-TCP o 800/17-UDP dal menu a discesa Select from List (Scegli dall'elenco).
- Intervallo: è possibile scegliere un intervallo di porte di origine TCP/UDP a cui associare il pacchetto. È possibile configurare otto intervalli di porte diversi (condivisi tra le porte di origine e di destinazione). I protocolli TCP e UDP hanno ciascuno otto intervalli di porte.

Passaggio 17. (Facoltativo) Fare clic su un pulsante di opzione nell'area Porta di destinazione. Il valore predefinito è Any.

- Any — Corrisponde a tutte le porte di origine

- Single from list: è possibile scegliere una singola porta di origine TCP/UDP a cui far corrispondere i pacchetti. Questo campo è attivo solo se si sceglie 800/6-TCP o 800/17-UDP dal menu a discesa Select from List (Scegli dall'elenco).
- Singola in base al numero: è possibile scegliere una singola porta di origine TCP/UDP a cui associare i pacchetti. Questo campo è attivo solo se si sceglie 800/6-TCP o 800/17-UDP dal menu a discesa Select from List (Scegli dall'elenco).
- Intervallo: è possibile scegliere un intervallo di porte di origine TCP/UDP a cui associare il pacchetto. È possibile configurare otto intervalli di porte diversi (condivisi tra le porte di origine e di destinazione). I protocolli TCP e UDP hanno ciascuno otto intervalli di porte.

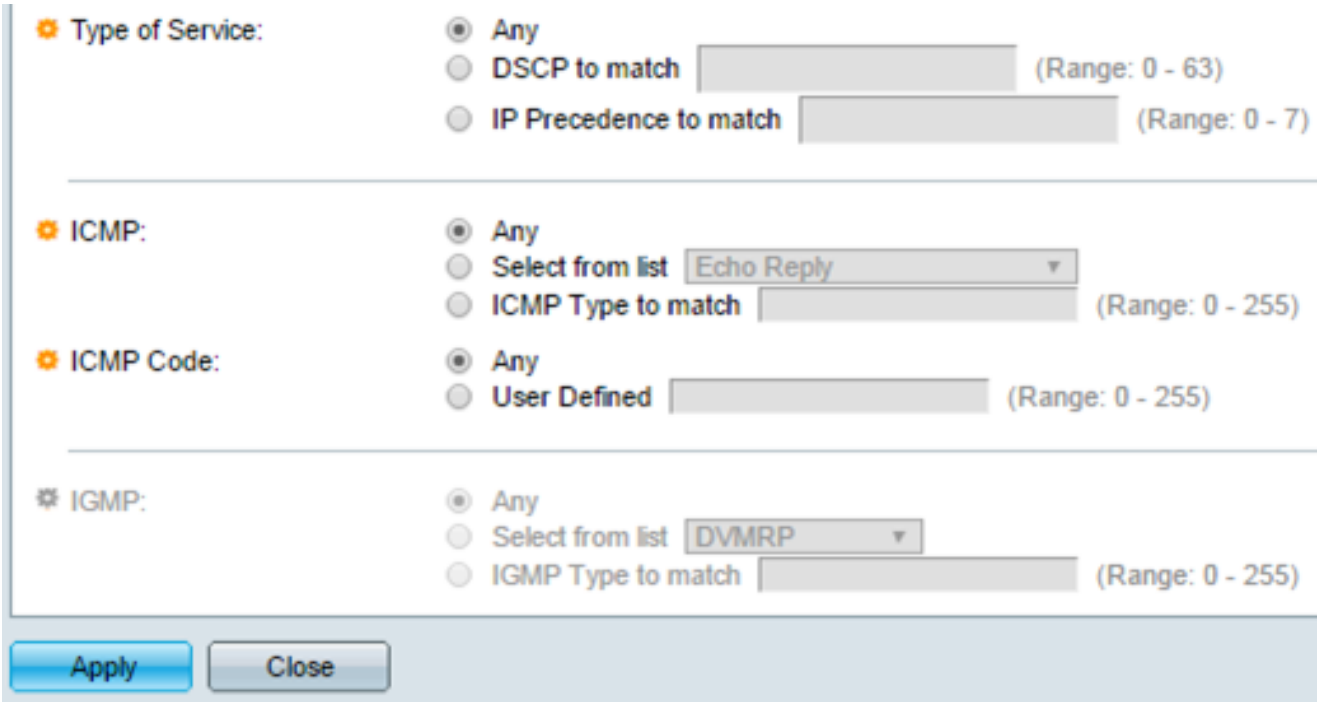
Passaggio 18. (Facoltativo) Nell'area Flag TCP, scegliere uno o più flag TCP con cui filtrare i pacchetti. I pacchetti filtrati vengono inoltrati o scartati. Il filtraggio dei pacchetti tramite flag TCP aumenta il controllo dei pacchetti, aumentando la sicurezza della rete.

- Imposta - Corrisponde se è impostato il flag.
- Annulla impostazione - Corrisponde se il flag non è impostato.
- Non importa — ignora il flag TCP.

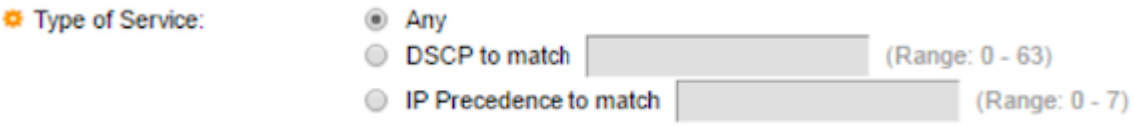

I flag TCP sono:

- Urg: questo flag viene utilizzato per identificare i dati in arrivo come urgenti.
- Ack - Questo flag viene utilizzato per confermare la ricezione dei pacchetti.
- Psh: questo flag viene utilizzato per garantire che ai dati venga assegnata la priorità (dovuta) e che vengano elaborati all'estremità di invio o di ricezione.
- Rst - Questo flag viene utilizzato quando arriva un segmento non destinato alla connessione corrente.
- Syn: questo flag viene utilizzato per le comunicazioni TCP.
- Fin - Questo flag viene utilizzato al termine della comunicazione o del trasferimento dei dati.

Passaggio 19. (Facoltativo) Fare clic sul tipo di servizio del pacchetto IP nell'area Tipo di servizio.




Le opzioni sono:




- Any — Può essere un servizio di qualsiasi tipo per la congestione del traffico.
- DSCP to match: DSCP è un meccanismo per la classificazione e la gestione del traffico di rete. Vengono usati sei bit (0-63) per selezionare il comportamento per hop di un pacchetto su ciascun nodo.
- Precedenza IP da abbinare: la precedenza IP è un modello di TOS (Type of Service) utilizzato dalla rete per garantire gli impegni QoS (Quality of Service) appropriati. Questo modello utilizza i tre bit più significativi del byte del tipo di servizio nell'intestazione IP, come descritto nella RFC 791 e nella RFC 1349. La parola chiave con il valore della preferenza IP è la seguente:

  - 0 — per usi ordinari

  - 1 — per priorità

  - 2 — da immediato

  - 3 — per flash

  - 4 — per flash-override

  - 5 — per i sistemi critici

  - 6 — per Internet

  - 7 — per reti

Passaggio 20. (Facoltativo) Se il protocollo IP dell'ACL è ICMP, fare clic sul tipo di messaggio ICMP usato per il filtro. Scegliere il tipo di messaggio in base al nome o

immettere il numero del tipo di messaggio:

- Qualsiasi - Vengono accettati tutti i tipi di messaggi.
- Seleziona dall'elenco: è possibile scegliere il tipo di messaggio in base al nome.
- Tipo ICMP da associare - il numero di tipi di messaggi da utilizzare per il filtro. L'intervallo è compreso tra 0 e 255.

Passaggio 21. (Facoltativo) I messaggi ICMP possono contenere un campo di codice che indica come gestire il messaggio. Fare clic su una delle opzioni seguenti per configurare se filtrare in base a questo codice:

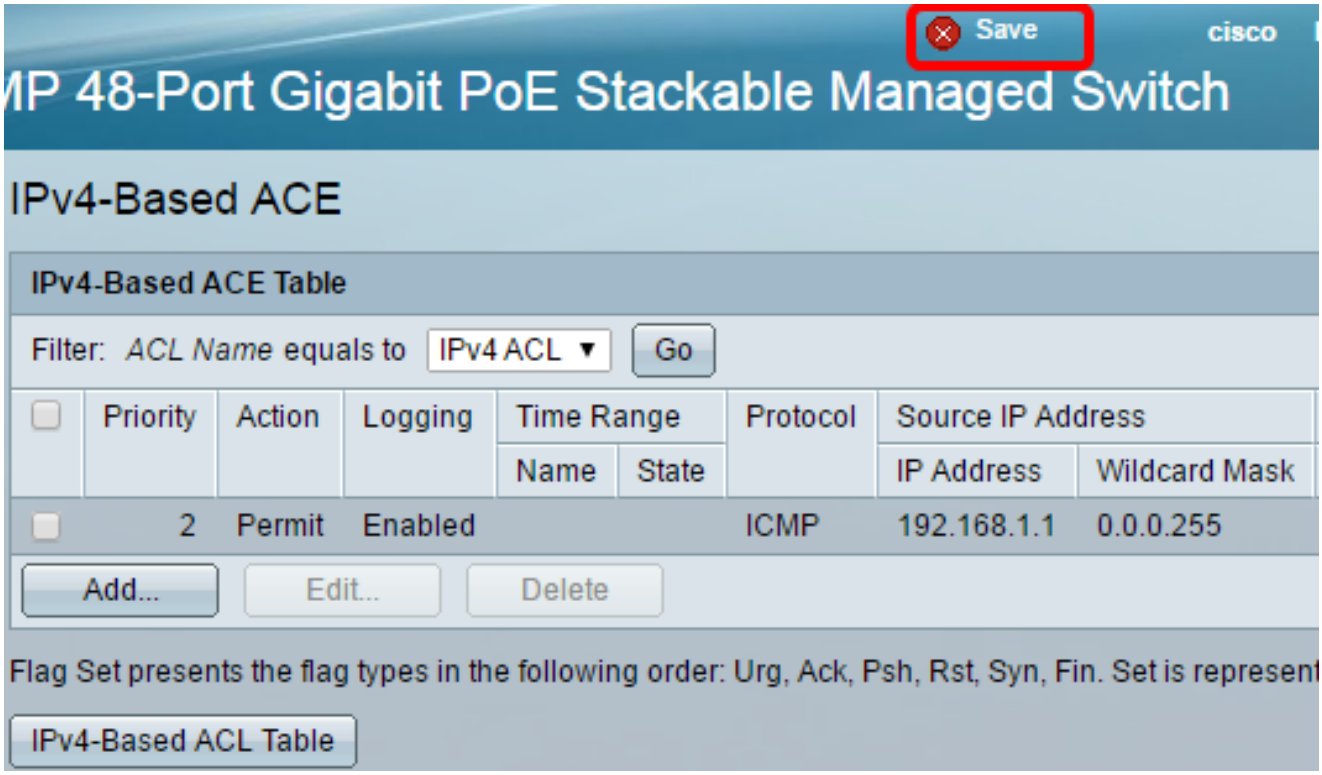
- Qualsiasi - Accetta tutti i codici.
- Definito dall'utente: è possibile immettere un codice ICMP a scopo di filtro. L'intervallo è compreso tra 0 e 255.

Passaggio 22. (Facoltativo) Se l'ACL è basato su IGMP, fare clic sul tipo di messaggio IGMP da usare ai fini del filtro. Scegliere il tipo di messaggio in base al nome o immettere il numero del tipo di messaggio:

- Qualsiasi - Vengono accettati tutti i tipi di messaggi.
- Seleziona dall'elenco: è possibile scegliere una delle opzioni seguenti dall'elenco a discesa:
- DVMRP: utilizza una tecnica di flooding del percorso inverso, inviando una copia di un pacchetto ricevuto attraverso ciascuna interfaccia ad eccezione di quella in cui il pacchetto è arrivato.
- Host-Query: invia periodicamente messaggi generici di query host su ciascuna rete collegata per ottenere informazioni.
- Host-Reply - Risponde alla query.
- PIM: Protocol Independent Multicast (PIM) viene utilizzato tra i router multicast locali e remoti per indirizzare il traffico multicast dal server multicast a molti client multicast.
- Traccia - fornisce informazioni sull'unione e l'uscita dai gruppi multicast IGMP.
- Tipo IGMP da abbinare — il numero di tipi di messaggi da utilizzare per il filtraggio. L'intervallo è compreso tra 0 e 255.

Passaggio 23. Fare clic su **Apply (Applica)**, quindi su **Close** (Chiudi). La voce di controllo di accesso viene creata e associata al nome dell'ACL.

Passaggio 24. Fare clic su **Save** per salvare le impostazioni nel file della configurazione di avvio.




A questo punto, è necessario configurare una voce ACE basata su IPv4 sullo switch.