

Configurazione di ACL (Access Control List) e ACE (Access Control Entry) basati su IPv6 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.

La funzionalità tipica degli ACL in IPv6 è simile a quella degli ACL in IPv4. Gli ACL determinano il traffico da bloccare e il traffico da inoltrare alle interfacce dello switch. Gli ACL permettono di filtrare i dati in base agli indirizzi di origine e di destinazione, in entrata e in uscita, su interfacce specifiche. Alla fine di ogni ACL è presente un'istruzione di rifiuto implicita. Le regole per gli ACL sono configurate nelle voci di controllo di accesso (ACE).

È consigliabile 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 ACL e ACE basati su IPv6 su uno switch.

Dispositivi interessati

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

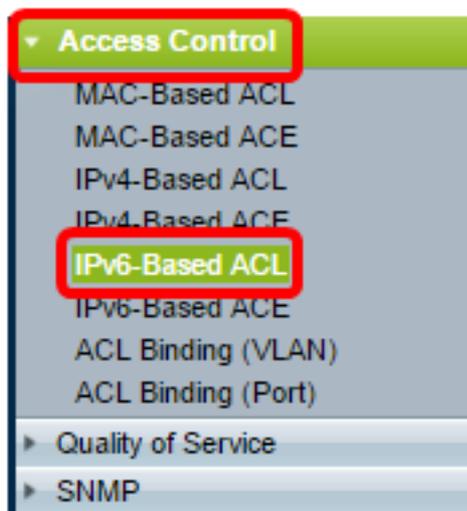
Versione del software

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

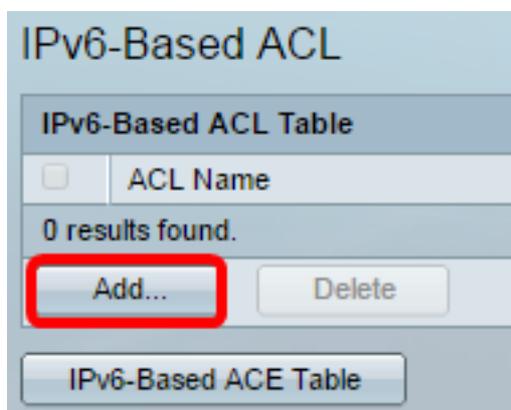
Configurare ACL e ACE basati su IPv6

Configurazione di ACL basati su IPv6

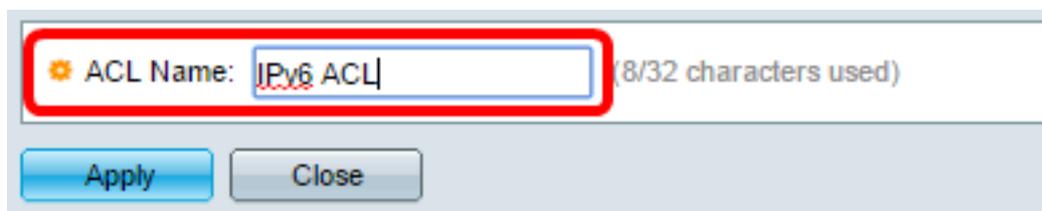
Passaggio 1. Accedere all'utility basata sul Web, quindi selezionare **Access Control > IPv6-Based ACL**.



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

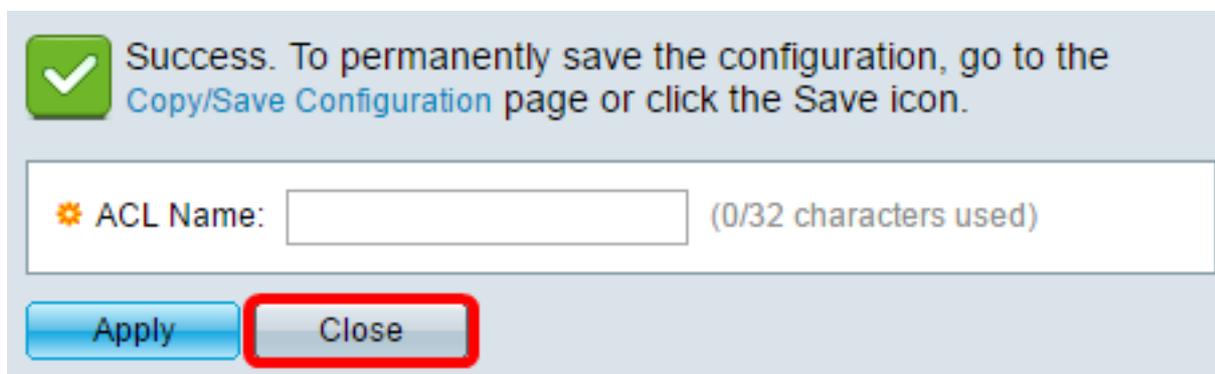


Passaggio 3. Inserire il nome del nuovo ACL nel campo *Nome ACL*.



Nota: Nell'esempio viene utilizzato un ACL IPv6.

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 IPv6 sullo switch.

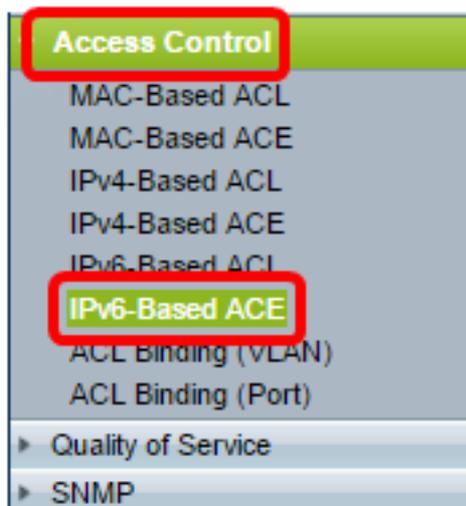
Configura ACE basata su IPv6

Quando si riceve un pacchetto su una porta, lo switch elabora il frame 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.

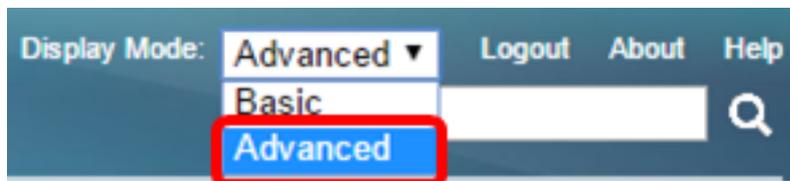
In questo scenario verrà creata una voce ACE per impedire il traffico inviato da un indirizzo IPv6 di origine definito dall'utente a qualsiasi indirizzo di destinazione.

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

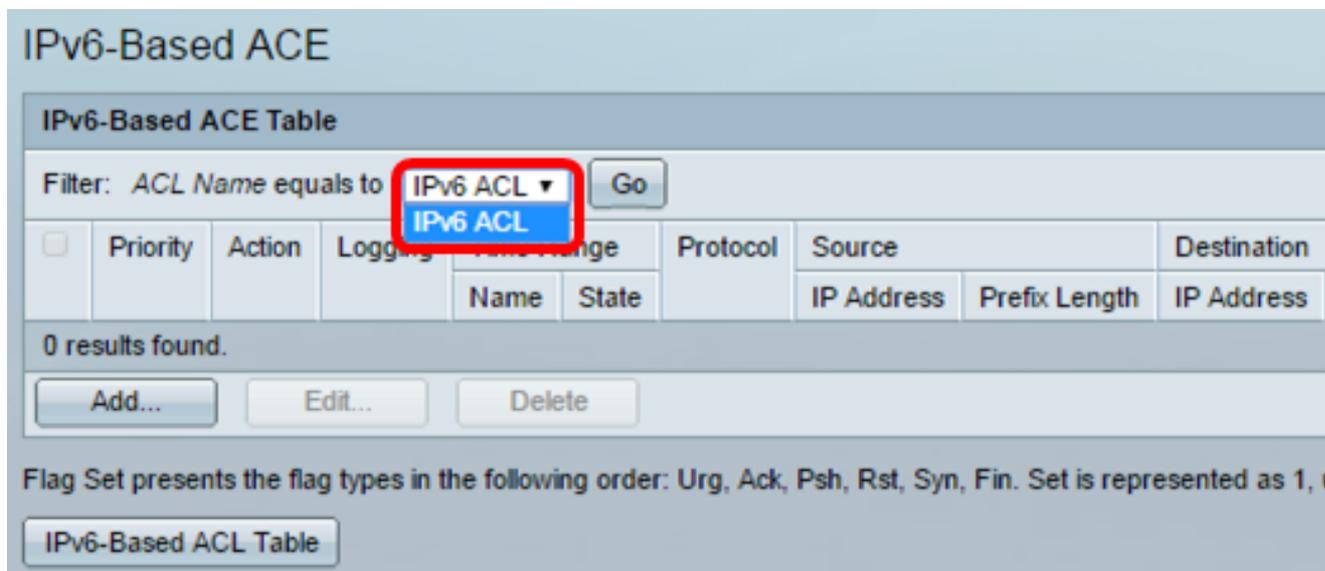
Passaggio 1. Nell'utilità basata sul Web, passare a **Controllo accesso > ACE basata su IPv6**.



Importante: Se si dispone di uno switch Sx350, SG350X, Sx550X, passare alla modalità avanzata scegliendo **Avanzate** dall'elenco a discesa Modalità di visualizzazione nell'angolo superiore destro della pagina.

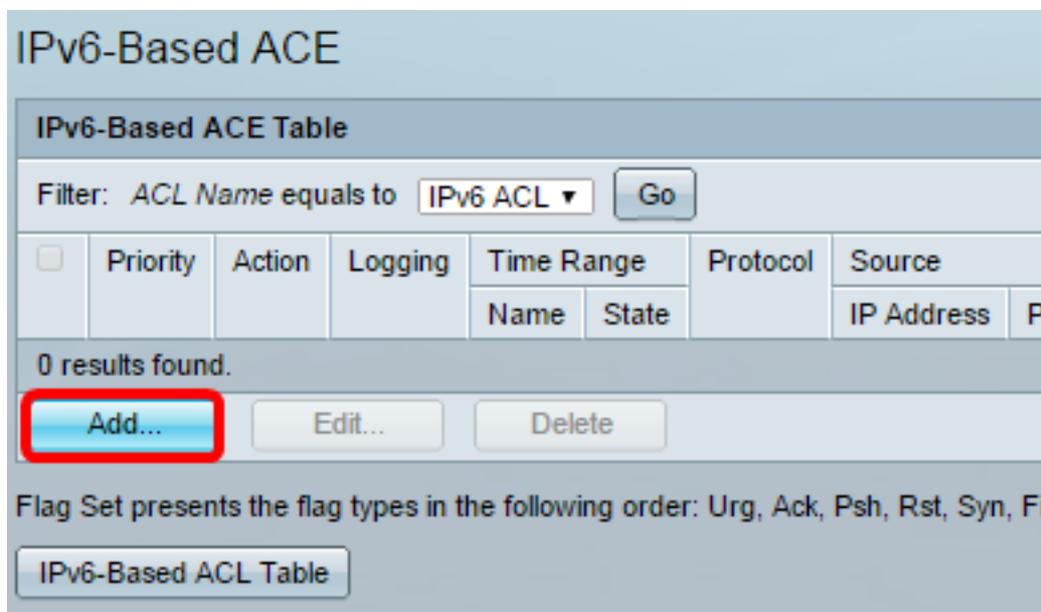


Passaggio 2. Scegliere un ACL dall'elenco a discesa Nome ACL, quindi fare clic su **Vai**.



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.

ACL Name: IPv6 ACL

Priority: (Range: 1 - 2147483647)

Action:
 Permit
 Deny
 Shutdown

Logging: Enable

Time Range: Enable

Time Range Name: [Edit](#)

Protocol:
 Any (IPv6)
 Select from list
 Protocol ID to match (Range: 0 - 255)

Nota: Nell'esempio viene utilizzato 3.

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.
- Negate: 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. Le porte disabilite 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.

Logging: Enable

Time Range: Enable

Time Range Name: [Edit](#)

Protocol:
 Any (IP)
 Select from list
 Protocol ID to match (Range: 0 - 255)

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. Se questa opzione viene lasciata disattivata, l'ACE funzionerà in qualsiasi momento.

Logging: Enable

Time Range: **Enable**

Time Range Name: Time Range 1 [Edit](#)

Protocol: Any (IPv6)

Select from list TCP

Protocol ID to match (Range: 0 - 255)

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

Time Range Name: Time Range 1 [Edit](#)

Protocol: Any (IPv6)

Select from list TCP

Protocol ID to match (Range: 0 - 255)

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

Time Range Name: Time Range 1 (12/32 characters used)

Absolute Starting Time: Immediate

Date 2010 Jan 01 Time 00 00 HH:MM

Absolute Ending Time: Infinite

Date 2010 Jan 01 Time 00 00 HH:MM

[Apply](#) [Close](#)

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.

Protocol: Any (IPv6)

Select from list ICMP

Protocol ID to match 58 (Range: 0 - 255)

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: In questo esempio, viene scelto Seleziona da elenco.

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

Protocol:
 Any (IPv6)
 Select from list
 Protocol ID to match
 (Range: 0 - 255)

TCP
 TCP
 UDP
 ICMP

Le opzioni sono:

- TCP: il protocollo TCP (Transmission Control Protocol) consente a due host di comunicare e scambiare flussi di dati. Il protocollo TCP garantisce la consegna dei pacchetti e la trasmissione e la ricezione dei pacchetti nell'ordine in cui sono stati inviati.
- UDP — User Datagram Protocol (UDP) trasmette i pacchetti ma non ne garantisce la consegna.
- ICMP: confronta i pacchetti con il protocollo ICMP (Internet Control Message Protocol).

Nota: nell'esempio viene usato il protocollo TCP.

[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*.

Protocol:
 Any (IP)
 Select from list

 Protocol ID to match
 (Range: 0 - 255)

Nota: Nell'esempio viene utilizzato 1.

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

Source IP Address:
 Any
 User Defined

Le opzioni sono:

- Qualsiasi - Tutti gli indirizzi IPv6 di origine 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 *Source IP Address Value* (Valore indirizzo IP di origine) e *Source IP Prefix Length* (Lunghezza prefisso IP di origine).

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*.

Source IP Address:
 Any
 User Defined

Source IP Address Value:

Nota: Nell'esempio viene utilizzato fe80::d0ba:7021:37f7:d68d.

Passaggio 14. Immettere la lunghezza del prefisso IP di origine nel campo *Lunghezza*

prefisso IP di origine.

Source IP Address: Any
 User Defined

Source IP Address Value:

Source IP Prefix Length: (Range: 0 - 128)

Nota: nell'esempio viene utilizzato 128.

[Passaggio 15](#). Fare clic sul pulsante di opzione corrispondente ai criteri desiderati per l'ACE nell'area Destination IP Address.

Source IP Address: Any
 User Defined

Source IP Address Value:

Source IP Prefix Length: (Range: 0 - 128)

Destination IP Address: Any
 User Defined

Destination IP Address Value:

Destination IP Prefix Length: (Range: 0 - 128)

Le opzioni sono:

- Qualsiasi - Tutti gli indirizzi IPv6 di destinazione vengono applicati all'ACE.
- Definito dall'utente: immettere un indirizzo IP e una maschera con caratteri jolly IP da applicare all'ACE nei campi *Valore indirizzo IP di destinazione* e *Lunghezza prefisso IP di destinazione*.

Nota: Nell'esempio, viene scelto Qualsiasi. Se si sceglie questa opzione, la voce ACE da creare consentirà il traffico ACE proveniente dall'indirizzo IPv6 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.

Source Port: Any
 Single from list
 Single by number (Range: 0 - 65535)
 Range -

Destination Port: Any
 Single from list
 Single by number (Range: 0 - 65535)
 Range -

- 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.

Urg:	Ack:	Psh:	Rst:	Syn:	Fin:
<input type="radio"/> Set	<input type="radio"/> Set	<input checked="" type="radio"/> Set	<input type="radio"/> Set	<input type="radio"/> Set	<input type="radio"/> Set
<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset
<input checked="" type="radio"/> Don't care	<input checked="" type="radio"/> Don't care	<input type="radio"/> Don't care	<input checked="" type="radio"/> Don't care	<input checked="" type="radio"/> Don't care	<input checked="" type="radio"/> Don't care

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.

Type of Service:
 Any
 DSCP to match (Range: 0 - 63)
 IP Precedence to match (Range: 0 - 7)

Le opzioni sono:

- Any — Può essere un servizio di qualsiasi tipo per la congestione del traffico.
- DSCP to match: Differentiated Services Code Point 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 i valori delle preferenze 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

Nota: Nell'esempio, viene scelto Qualsiasi.

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:

ICMP:
 Any
 Select from list
 ICMP Type to match (Range: 0 - 255)

ICMP Code:
 Any
 User Defined (Range: 0 - 255)

- 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.

Nota: In questo esempio, viene scelto Seleziona da elenco.

Passaggio 21. (Facoltativo) Se nel passaggio 20 si sceglie Seleziona da elenco, scegliere i messaggi di controllo da filtrare dalle opzioni disponibili nell'elenco a discesa:

The screenshot shows a configuration window for ICMP messages. It has three main sections: 'TCP Flags', 'Type of Service', and 'ICMP'. The 'ICMP' section is active, showing a dropdown menu for 'Select from list'. The dropdown menu is open, displaying a list of ICMP message types with their respective codes in parentheses. The 'Destination Unreachable (1)' option is selected and highlighted with a red border. Other options include 'Packet Too Big (2)', 'Time Exceeded (3)', 'Parameter Problem (4)', 'Echo Request (128)', 'Echo Reply (129)', 'MLD Query (130)', 'MLD Report (131)', 'MLDv2 Report (143)', 'MLD Done (132)', 'Router Solicitation (133)', 'Router Advertisement (134)', 'ND NS (135)', and 'ND NA (136)'. The 'Destination Unreachable (1)' option is also highlighted with a blue bar at the top of the dropdown.

- Destination Unreachable (1): viene generato dall'host o dal relativo gateway per informare il client che, per qualche motivo, la destinazione non è raggiungibile (esempio: Errore di rete o host non raggiungibile).
- Pacchetto troppo grande (2): le dimensioni del datagramma superano l'MTU specificata.
- Tempo scaduto (3): viene generato da un gateway per informare l'origine di un datagramma scartato a causa del valore zero del campo Time to Live.
- Parametro Problem (4) - Viene generato come risposta a qualsiasi errore non specificamente coperto da un altro messaggio ICMP.
- Richiesta echo (128) - Si tratta di un ping, i cui dati devono essere ricevuti nuovamente in una risposta echo.
- Risposta echo (129) — Viene generata in risposta a una richiesta echo.
- Query MLD (130) - Consente di individuare gli indirizzi multicast a cui sono associati listener su un collegamento. Digitare 130 in decimale.
- Report MLD (131) — Viene generato quando l'indirizzo multicast IPv6 a cui è in ascolto il mittente del messaggio.
- Report MLD v2 (143). Equivale a Report MLD con versione 2.
- MLD Done (132) - Quando l'host lascia un gruppo, invia un messaggio multicast di completamento ascolto ai router multicast della rete.
- Richiesta router (133) - È un messaggio di rilevamento router. Gli host scoprono gli indirizzi dei router adiacenti semplicemente quando ascoltano le pubblicità. L'impostazione predefinita per il multicast è 224.0.0.2, altrimenti è 255.255.255.255.
- Router Advertisement (134): il router multicast periodicamente un annuncio router da ciascuna delle proprie interfacce multicast e annuncia gli indirizzi IP di tale interfaccia.
- ND NS (135): i messaggi vengono generati dai nodi per richiedere l'indirizzo del livello di collegamento di un altro nodo e anche per funzioni quali il rilevamento degli indirizzi duplicati e il rilevamento dell'irraggiungibilità dei nodi adiacenti.
- ND NA (136) — I messaggi vengono inviati in risposta ai messaggi NS. Se un nodo modifica il proprio indirizzo del livello di collegamento, può inviare un NA non richiesto per annunciare il nuovo indirizzo.

Passaggio 22. (Facoltativo) I messaggi ICMP possono contenere un campo di codice che

indica come gestire il messaggio. Questa opzione è abilitata se si sceglie il protocollo ICMP nel passaggio 10. Fare clic su una delle opzioni seguenti per configurare se filtrare in base a questo codice:

ICMP: Any
 Select from list ICMP Type to match (Range: 0 - 255)

ICMP Code: Any User Defined (Range: 0 - 255)

- Qualsiasi - Accetta tutti i codici.
- Definito dall'utente: è possibile immettere un codice ICMP a scopo di filtro.

Nota: Nell'esempio, viene scelto Qualsiasi.

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.



MP 48-Port Gigabit PoE Stackable Managed Switch

IPv6-Based ACE

IPv6-Based ACE Table

Filter: ACL Name equals to

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Protocol	Source
				Name	State		IP Address
<input type="checkbox"/>	3	Deny	Enabled			ICMP	fe80::d0ba:7021:37f7:d68d

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represe

È ora necessario configurare una voce ACE basata su IPv6 sullo switch.