Configurazione degli elenchi degli accessi basati su IPv4 sugli switch gestiti serie 200/300

Obiettivo

Gli elenchi di accesso sono regole che è possibile applicare per consentire o negare un flusso di traffico specifico sulla rete, aumentando in questo modo la sicurezza e le prestazioni complessive della rete.

L'obiettivo di questo documento è mostrare come configurare gli elenchi degli accessi basati su IPv4 sugli switch gestiti serie 200/300.

Dispositivi interessati

·SF/SG serie 200 e SF/SG serie 300 Managed Switch

Versione del software

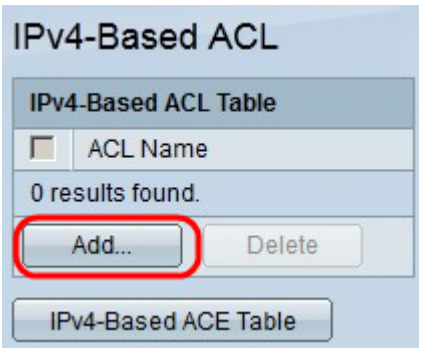
•1.3.0.62

Configurazione di ACL e ACE basati su IPv4

ACL basati su IPv4

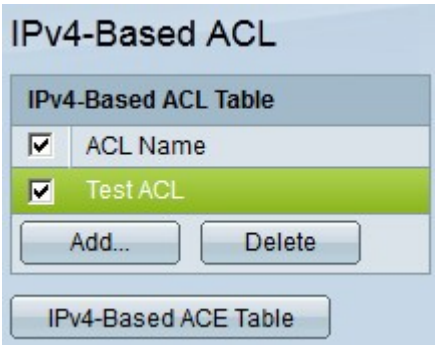
Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Controllo dell'accesso > ACL basato su IPv4**. Viene visualizzata la pagina *ACL basato su IPv4*.

Passaggio 2. Fare clic su **Add** per aggiungere un nuovo elenco degli accessi.



Passaggio 3. Nel campo *Nome ACL*, immettere un nome per il nuovo elenco degli accessi.

Passaggio 4. Fare clic su **Apply** (Applica) per salvare l'elenco degli accessi.



Passaggio 5. (Facoltativo) Per eliminare un elenco degli accessi, selezionare la casella di controllo dell'elenco degli accessi che si desidera eliminare e fare clic su **Elimina**.

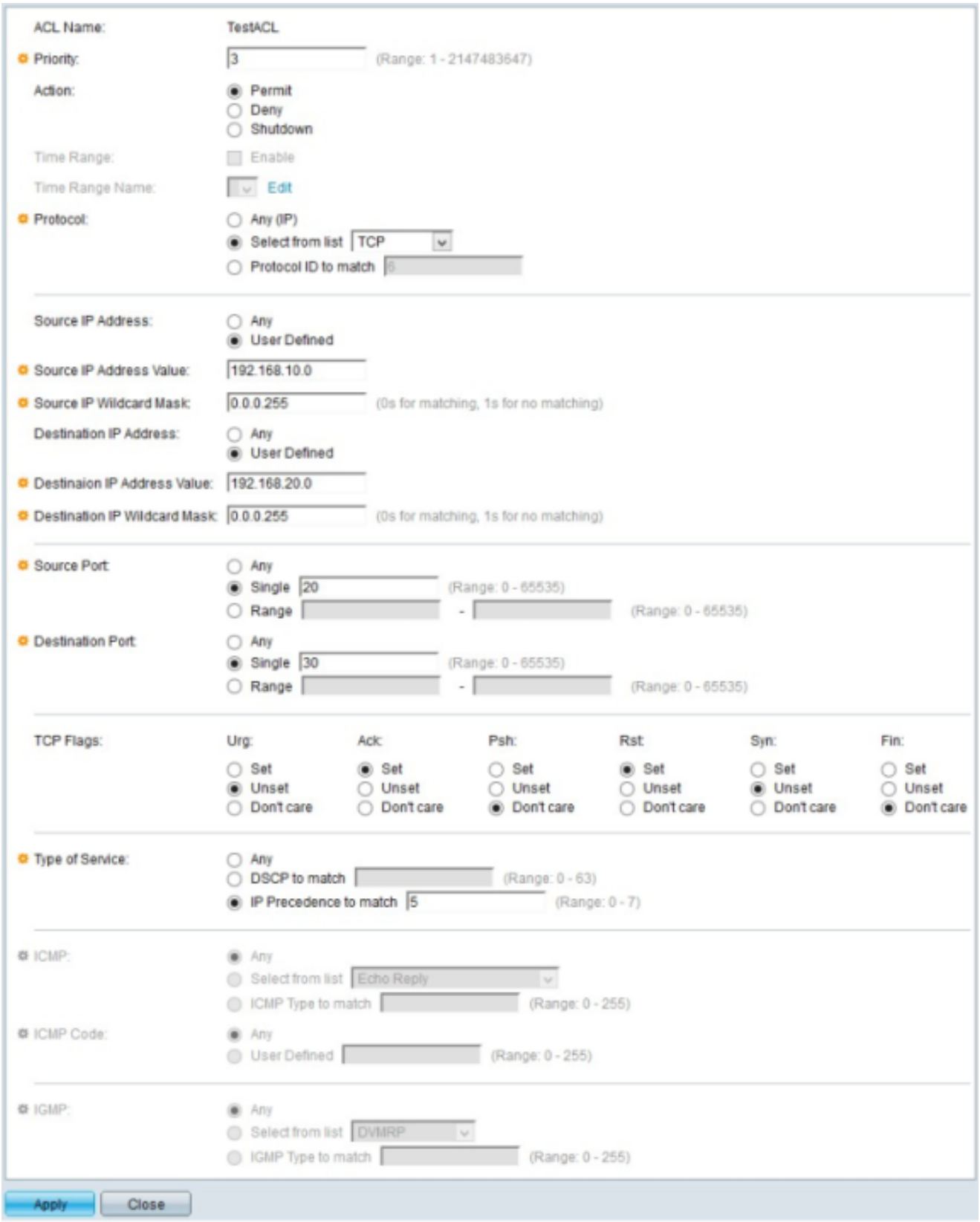
ACE basati su IPv4

Per gestire una voce ACE in un ACL, è necessario eseguire i passaggi successivi.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Controllo accesso > ACE basati su IPv4**. Viene visualizzata la pagina *ACE basata su IPv4*.

Passaggio 2. Nell'elenco a discesa *Filtro: nome ACL uguale a* scegliere l'elenco degli accessi a cui si desidera assegnare una regola di accesso.

Passaggio 3. Fare clic su **Add**. Viene visualizzata la finestra *Add IP-Based ACE*.



Passaggio 4. Immettere la priorità dell'ACE nel campo *Priorità*. La voce ACE con la priorità più alta viene elaborata per prima. La priorità più alta è 1. L'intervallo è compreso tra 1 e 2147483647.

Passaggio 5. Nel campo *Azione* fare clic sul pulsante di opzione dell'azione che si desidera venga eseguita dalla regola di accesso. Le opzioni disponibili sono:

·Permit: inoltra i pacchetti filtrati dall'ACE corrente.

·Deny - Elimina i pacchetti filtrati in base all'ACE corrente.

·Shutdown — Elimina i pacchetti filtrati dall'ACE corrente e disabilita la porta da cui sono stati ricevuti.

Passaggio 6. Nel campo *Protocol* (Protocollo), fare clic sul pulsante di opzione del protocollo che si desidera aggiungere alla voce ACE. L'ACE è configurata per tutti i protocolli di rete indirizzati in modo da filtrare i pacchetti quando passano attraverso un router. Le opzioni disponibili sono:

· Qualsiasi: consente di scegliere uno dei protocolli ACE basati su IPv4.

·Selezionare dall'elenco: scegliere il protocollo desiderato dall'elenco a discesa.

·ID protocollo corrispondente - Questa opzione consente di immettere l'ID protocollo che si desidera utilizzare.

Passaggio 7. Nel campo *Source IP Address* (Indirizzo IP di origine), selezionare una delle opzioni disponibili come indirizzo IP di origine:

·Qualsiasi - Questa opzione applica la regola di accesso a qualsiasi indirizzo IP disponibile in un segmento di rete specifico.

·Definito dall'utente - Questa opzione consente di immettere un indirizzo IP specifico.

- Valore indirizzo IP di origine — In questo campo, immettere l'indirizzo IP di origine.

- Source IP Wildcard Mask: in questo campo, immettere la maschera con caratteri jolly dell'indirizzo IP di origine. La wildcard mask consente di specificare a quale host dell'indirizzo IP di origine viene applicato questo elenco degli accessi.

Passaggio 8. Nel campo *Destination IP Address* (Indirizzo IP di destinazione), selezionare una delle opzioni disponibili come indirizzo IP di destinazione:

·Qualsiasi - Questa opzione applica la regola di accesso a qualsiasi indirizzo IP disponibile in un segmento di rete specifico.

·Definito dall'utente: questa opzione consente di immettere un indirizzo IP specifico per applicare la regola di accesso:

- Valore indirizzo IP di destinazione - In questo campo, immettere l'indirizzo IP di destinazione.

- Destination IP Wildcard Mask (Maschera jolly IP di destinazione): in questo campo, immettere la maschera con caratteri jolly dell'indirizzo IP di destinazione. La wildcard mask consente di specificare a quali host dell'indirizzo IP di destinazione viene applicato questo elenco degli accessi.

Passaggio 9. Il campo *Source Port* (Porta di origine) viene abilitato solo quando si sceglie TCP o UDP nel passaggio 5. Fare clic sul pulsante di opzione di una delle opzioni disponibili per scegliere la porta di origine:

·Qualsiasi - Questa opzione accetta qualsiasi porta di origine.

·Singolo - Questa opzione consente di immettere un singolo valore della porta di origine.

·Intervallo - Questa opzione consente di immettere un intervallo di porte di origine disponibili.

Passaggio 10. Il campo *Porta di destinazione* viene abilitato solo quando si sceglie TCP o UDP nel passo 5. Fare clic sul pulsante di opzione di una delle opzioni disponibili per scegliere la porta di destinazione:

·Qualsiasi - Questa opzione accetta tutte le porte di destinazione.

·Singolo - Questa opzione consente di immettere un valore di porta di destinazione singolo.

·Intervallo - Questa opzione consente di immettere un intervallo di porte di destinazione disponibili.

Passaggio 11. Il campo *Contrassegni TCP* viene abilitato solo se si sceglie TCP dal punto 5. Fare clic su uno dei pulsanti di opzione per ogni flag per scegliere lo stato da attivare per la regola di accesso:

·Urg: questo flag identifica i dati in arrivo come urgenti.

·Ack: questo flag viene utilizzato per confermare la ricezione dei pacchetti.

·Psh: questo flag viene utilizzato per assicurare che ai dati venga assegnata la priorità corretta e che vengano elaborati all'estremità di invio o di ricezione.

·Rst - Questo flag viene utilizzato quando una connessione riceve un segmento errato.

·Syn: questo flag viene utilizzato per le comunicazioni TCP.

·Fin - Questo flag viene utilizzato al termine della comunicazione o del trasferimento dei dati.

Passaggio 12. Nel campo *Type of Service* (Tipo di servizio), fare clic su uno dei pulsanti di opzione disponibili per scegliere un tipo di servizio per il pacchetto IP:

·Qualsiasi - Questa opzione consente di scegliere qualsiasi tipo di servizio.

·DSCP corrispondente - Scegliere questa opzione per implementare DSCP (Differentiated Service Code Point) come tipo di servizio. DSCP è un meccanismo per classificare e gestire il traffico di rete. Immettere il valore DSCP da applicare alla regola di accesso.

·IP Precedence to match: questo tipo di servizio viene utilizzato dalla rete corrente per fornire il corretto QoS (Quality of Service). Immettere il valore da applicare alla regola di accesso.

Passaggio 13. Il campo *ICMP (Internet Control Message Protocol)* è abilitato solo quando si sceglie ICMP nel passaggio 5. ICMP viene utilizzato per inviare messaggi di errore quando un servizio non è disponibile o per verificare la connettività. Fare clic su uno dei pulsanti di opzione disponibili per filtrare i tipi di messaggi ICMP:

·Qualsiasi - Può trattarsi di uno qualsiasi dei messaggi di errore o di query.

·Selezionare dall'elenco: scegliere uno dei messaggi di controllo consentiti dall'elenco a discesa.

·Tipo ICMP corrispondente - Questa opzione consente di immettere il numero di tipi ICMP che si desidera filtrare.

Passaggio 14. Il campo *ICMP Code* (Codice ICMP) viene abilitato solo quando si sceglie ICMP dal passaggio 5. I codici ICMP vengono utilizzati per fornire informazioni più specifiche sui messaggi di controllo. Fare clic su una delle opzioni disponibili:

·Qualsiasi - Può essere qualsiasi valore che corrisponda al messaggio di controllo.

·Definito dall'utente: immettere il codice ICMP da filtrare.

Passaggio 15. Il campo *IGMP (Internet Group Management Protocol)* è abilitato solo quando si sceglie IGMP dal passo 5. IGMP gestisce l'appartenenza dell'host ai gruppi multicast IP su un segmento di rete. Fare clic su uno dei pulsanti di opzione disponibili per filtrare i tipi di messaggi IGMP:

·Qualsiasi - Questa opzione accetta tutti i tipi di messaggi IGMP.

·Seleziona dall'elenco — Scegliere una delle opzioni disponibili dall'elenco a discesa per filtrare:

- DVMRP: utilizza una tecnica di flooding del percorso inverso, che invia 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

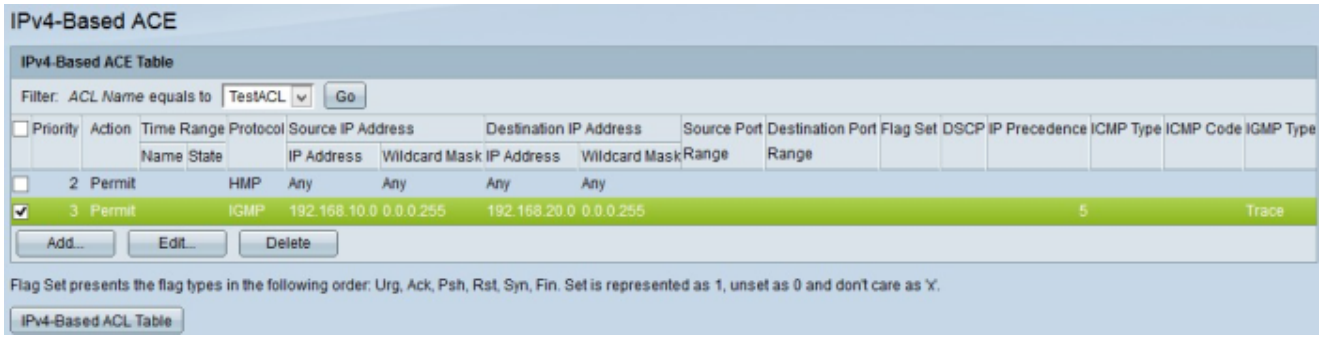
- Host-Reply — Risponde alla query .

- PIM: viene utilizzato tra i router multicast locali e remoti per indirizzare il traffico multicast dal server multicast a molti client multicast.

- Trace - Fornisce informazioni per unirsi e uscire da un gruppo multicast IGMP.

·Tipo di corrispondenza IGMP — questa opzione consente di immettere il numero di tipi IGMP che si desidera filtrare.

Passaggio 16. Fare clic su **Apply** (Applica) per salvare la configurazione.



Passaggio 17. (Facoltativo) Per modificare una regola di accesso corrente, selezionare la casella di controllo della regola di accesso che si desidera modificare e fare clic su **Modifica**.

Passaggio 18. (Facoltativo) Per eliminare una regola di accesso corrente, selezionare la casella di controllo della regola di accesso che si desidera eliminare e fare clic su **Elimina**.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).