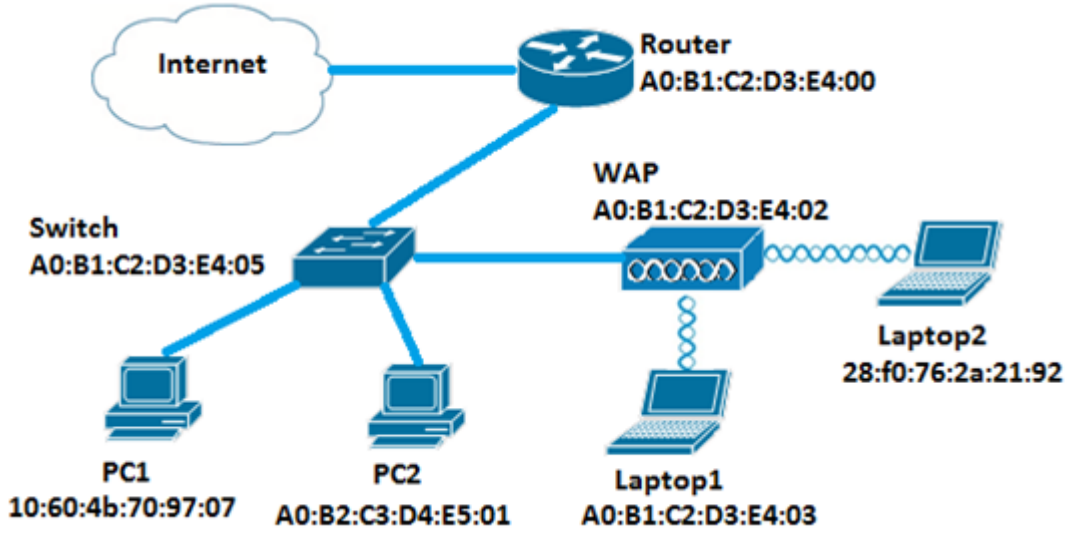
Configurazione di un ACL MAC su un WAP125 e WAP581

Introduzione

Gli ACL (Access Control List) MAC (Media Access Control) sono ACL di layer 2. Ogni ACL è un insieme di regole applicate al traffico ricevuto dal Wireless Access Point (WAP). La regola specifica se il contenuto di un determinato campo deve essere utilizzato per consentire o negare l'accesso alla rete. Gli ACL possono essere configurati per ispezionare i campi di un frame, ad esempio l'indirizzo MAC di origine o di destinazione, l'ID (ID) della VLAN (Virtual Local Area Network) o la classe di servizio (CoS). Quando un frame entra nella porta del dispositivo WAP, controlla il frame e confronta le regole ACL con il contenuto del frame. Se una delle regole corrisponde al contenuto, viene eseguita un'azione di autorizzazione o rifiuto sul frame. La configurazione degli ACL MAC viene in genere utilizzata per autorizzare l'accesso alle risorse di rete per selezionare i dispositivi della rete.

Nota: Alla fine di ogni regola creata è presente un rifiuto implicito.



In questo scenario, a tutti i dispositivi della rete sarà consentito l'accesso al notebook 2 dietro il WAP, ad eccezione di PC1.

Obiettivo

Questo articolo ha lo scopo di mostrare come configurare un ACL basato su MAC su un Access Point WAP125 o WAP581 in modo da impedire a PC1 di accedere al Laptop2 dietro il WAP.

Dispositivi interessati

- WAP125
- WAP581

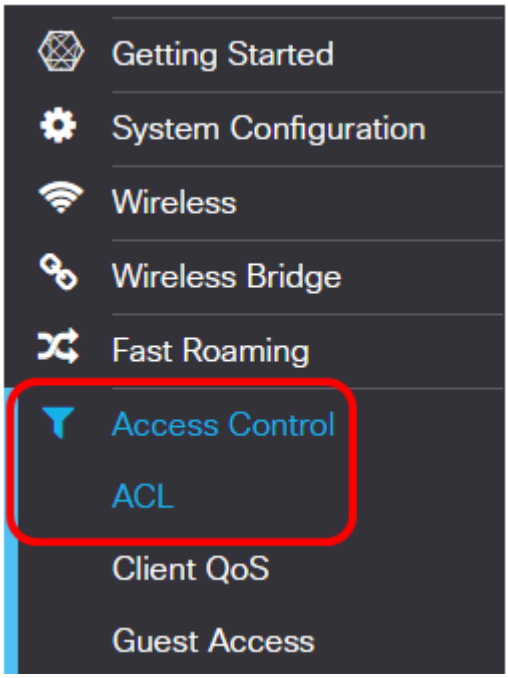
Versione del software

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

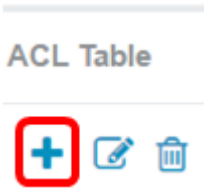
Configurare un elenco di filtri client

Nota: Le opzioni di menu possono variare a seconda del modello di WAP in uso. Le immagini seguenti sono tratte da WAP125.

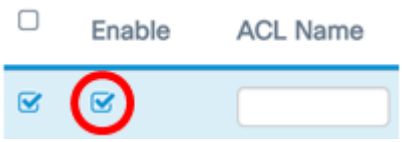
Passaggio 1. Accedere all'utility basata sul Web di WAP e scegliere **Controllo accesso > ACL**.



Passaggio 2. Fare clic sul pulsante.



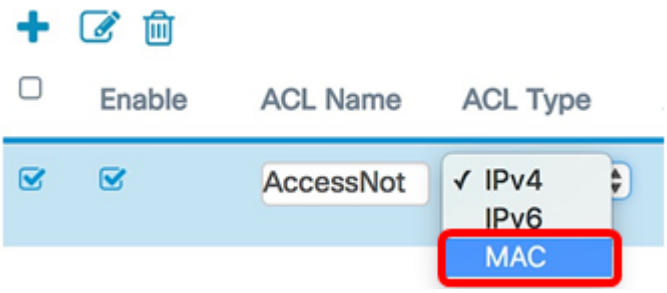
Passaggio 3. Verificare che la casella di controllo **Abilita** sia selezionata per accertarsi che l'ACL sia attivo. Questa opzione è selezionata per default.



Passaggio 4. Per identificare l'ACL, immettere un nome per l'ACL nel campo *Nome ACL*.

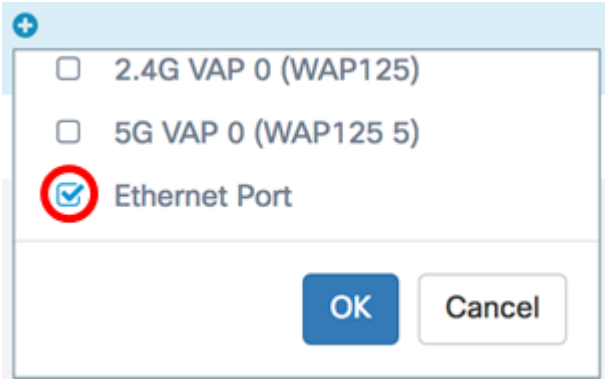
Nota: Nell'esempio, viene immesso AccessNot.

Passaggio 5. Selezionare **MAC** dall'elenco a discesa Tipo ACL.



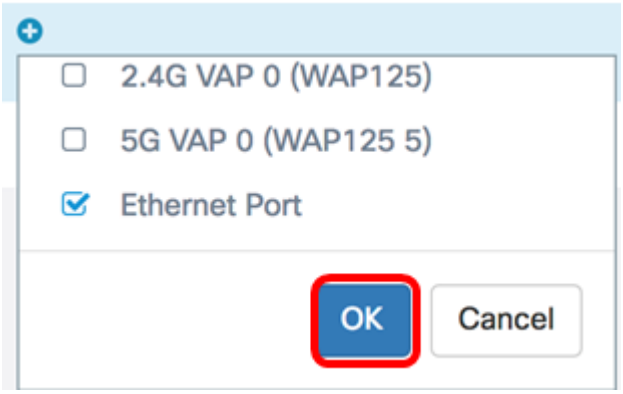
Passaggio 6. Fare clic sul pulsante e scegliere un'interfaccia dall'elenco a discesa Interfaccia associata. Le opzioni sono:

- 2.4G VAP 0 (nome SSID): questa opzione applica l'ACL MAC al VAP (Virtual Access Point) a 2,4 GHz. La sezione Nome SSID può variare a seconda del nome SSID configurato nel punto di accesso WAP.
- 5G VAP0 (nome SSID) - Questa opzione applica l'ACL MAC al VAP da 5 GHz.
- Ethernet Port: questa opzione applica l'ACL MAC all'interfaccia Ethernet del WAP.

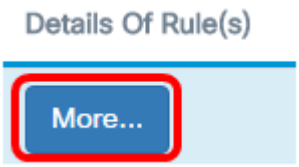


Nota: Ad un ACL possono essere associate più interfacce. Selezionare la casella di controllo dell'interfaccia corrispondente per associare l'interfaccia all'ACL. Deselezionare la casella per dissociare l'interfaccia dall'ACL. Nell'esempio, la porta Ethernet è associata all'ACL.

Passaggio 7. Fare clic su **OK**.



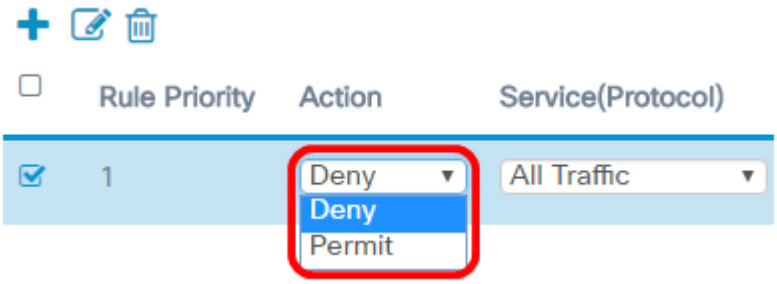
Passaggio 8. Fare clic sul pulsante **More...** per configurare i parametri dell'ACL.



Passaggio 9. Fare clic sul pulsante per aggiungere una nuova regola.

Passaggio 10. Scegliere un'azione dall'elenco a discesa Azione. Le opzioni sono:

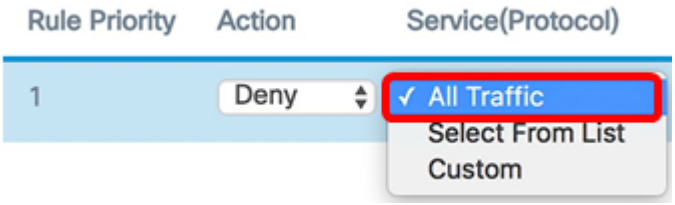
- Permit: questa opzione consente la connessione alla rete dei pacchetti che soddisfano i criteri ACL.
- Nega — questa opzione impedisce ai pacchetti che soddisfano i criteri ACL di connettersi alla rete.



Nota: Nell'esempio, viene scelto Nega.

Passaggio 11. Scegliere un servizio o un protocollo da filtrare dall'elenco a discesa Servizio (protocollo). Le opzioni sono:

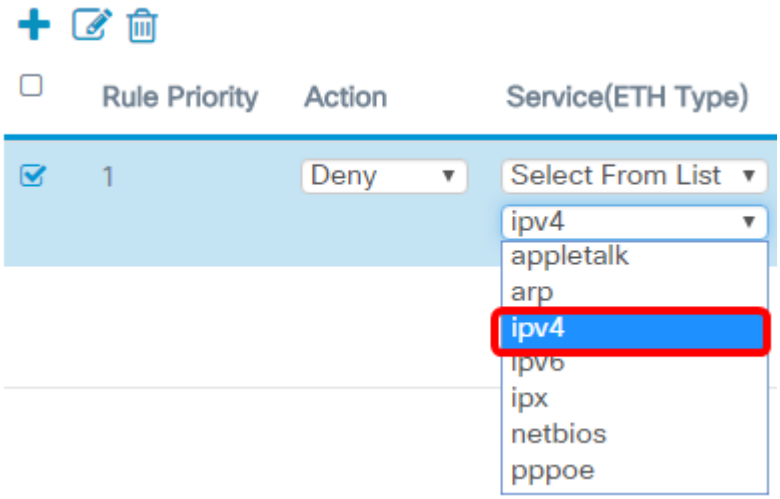
- All Traffic: questa opzione considera tutti i pacchetti come una corrispondenza con il filtro ACL.
- Select From List: questa opzione permette di scegliere appletalk, arp, ipv4, ipv6, ipx, netbios e pppoe come filtri per l'ACL. Se si sceglie questa opzione, andare al passaggio 12.
- Personalizzato — questa opzione consente di immettere un identificativo di protocollo personalizzato come filtro per i pacchetti. Il valore è un numero esadecimale a quattro cifre. L'intervallo è compreso tra 0600 e FFFF.



Nota: Nell'esempio, viene scelto **All Traffic** (Tutto il traffico).

Passaggio 12. (Facoltativo) Se si sceglie Seleziona da elenco, scegliere una delle seguenti opzioni:

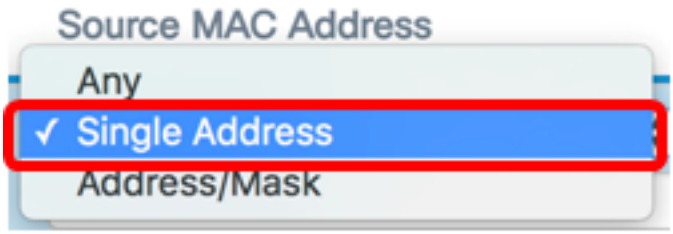
- appletalk — questa opzione filtra i pacchetti appletalk in base all'istruzione dell'ACL. Appletalk è un insieme di protocolli di rete sviluppati da Apple per i loro computer Mac. Una delle funzionalità consente di connettere le LAN (Local Area Network) senza la necessità di un router o di un server centrale.
- arp - questa opzione filtra i pacchetti Address Resolution Protocol (ARP) in base all'istruzione dell'ACL. ARP gestisce una tabella in cui gli indirizzi MAC vengono mappati agli indirizzi IP.
- ipv4: questa opzione filtra i pacchetti ipv4 in base all'istruzione dell'ACL.
- ipv6 — questa opzione filtra i pacchetti ipv6 in base all'istruzione dell'ACL. IPv6 è il successore di IPv6 nell'indirizzamento di rete.
- ipx: questa opzione filtra i pacchetti IPX (Internetwork Packet Exchange) in base all'istruzione dell'ACL. Come appletalk, IPX è anche un protocollo di rete proprietario. Collega le reti che utilizzano client e server Novell.
- netbios: questa opzione filtra i pacchetti NetBIOS (Network Basic Input and Output System) in base all'istruzione dell'ACL. NetBIOS consente alle applicazioni su computer separati di comunicare fornendo loro i servizi per la comunicazione.
- pppoe: questa opzione filtra i pacchetti PPPoE (Point-to-Point Protocol over Ethernet) in base all'istruzione dell'ACL. È utilizzata principalmente nei servizi DSL (Digital Subscriber Line).



Nota: nell'esempio, viene scelto ipv4.

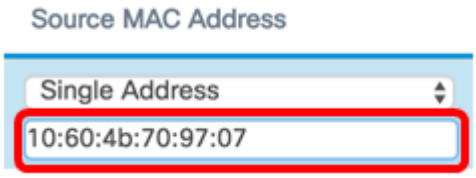
Passaggio 13. Definire l'indirizzo MAC di origine dall'elenco a discesa Indirizzo MAC di origine. Le opzioni sono:

- Any — questa opzione consente al WAP di applicare il filtro ai pacchetti provenienti da qualsiasi indirizzo MAC.
- Indirizzo singolo — questa opzione consente al WAP di applicare il filtro ai pacchetti provenienti da un indirizzo MAC specificato.
- Indirizzo/maschera — questa opzione consente al punto di accesso Windows di applicare il filtro ai pacchetti a un indirizzo MAC e alla maschera del punto di accesso Windows.



Nota: Nell'esempio viene scelto Indirizzo singolo.

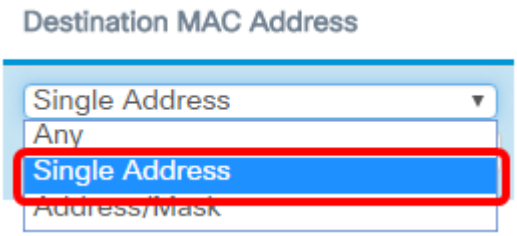
Passaggio 14. Immettere l'indirizzo MAC di origine nel campo *Indirizzo MAC di origine*.



Nota: Nell'esempio, viene immesso 10:60:4b:70:97:07. Questo è l'indirizzo MAC di PC1.

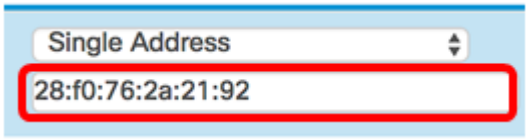
Passaggio 15. Definire l'indirizzo MAC di destinazione dall'elenco a discesa Indirizzo MAC di destinazione. Le opzioni sono:

- Any — questa opzione consente al WAP di applicare il filtro ai pacchetti provenienti da qualsiasi indirizzo MAC.
- Indirizzo singolo — questa opzione consente al WAP di applicare il filtro ai pacchetti provenienti da un indirizzo MAC specificato.
- Indirizzo/maschera — questa opzione consente al punto di accesso Windows di applicare il filtro ai pacchetti a un indirizzo MAC e alla maschera del punto di accesso Windows.



Nota: Nell'esempio viene scelto Indirizzo singolo.

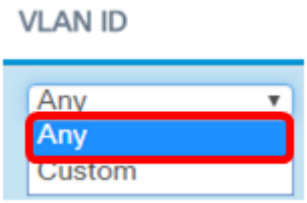
Passaggio 16. Immettere l'indirizzo MAC di destinazione nel campo **Indirizzo MAC di destinazione**.



Nota: Nell'esempio, viene immesso 28:f0:76:2a:21:92. Questo è l'indirizzo MAC del notebook2.

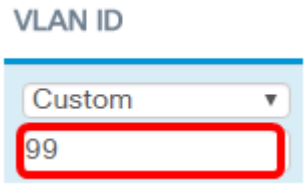
Passaggio 17. Selezionare un ID VLAN dall'elenco a discesa.

- Any: questa opzione consente di usare qualsiasi ID VLAN attraverso la rete.
- Personalizzata: questa opzione consente di immettere un ID VLAN specifico. Se si sceglie questa opzione, andare al passaggio 18.



Nota: Nell'esempio, viene scelto Qualsiasi.

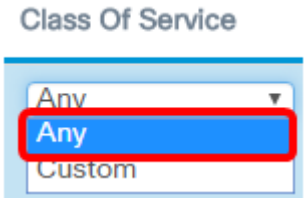
Passaggio 18. (Facoltativo) Se si sceglie Personalizzata, immettere l'ID VLAN nel campo *ID VLAN*.



Nota: Nell'esempio, viene immesso 99.

Passaggio 19. (Facoltativo) Scegliere una classe di servizio dall'elenco a discesa. Le opzioni sono:

- Any - Questa opzione consente di connettere alla rete un pacchetto con qualsiasi livello di priorità.
- Personalizzata - questa opzione consente di filtrare i pacchetti a un livello di priorità specifico.

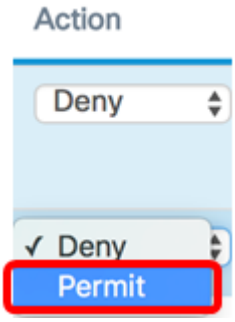


Nota: Nell'esempio, viene scelto Qualsiasi. Se si sceglie Personalizzata, immettere la priorità nel campo *Classe di servizio*.

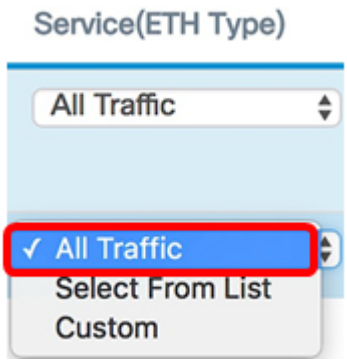
Passaggio 20. Fare di nuovo clic sul pulsante per aggiungere una regola di autorizzazione.

Nota: Poiché alla fine di ciascuna regola creata viene visualizzato un rifiuto implicito, si consiglia di aggiungere una regola di autorizzazione all'ACL per consentire il traffico proveniente da altri dispositivi nella rete.

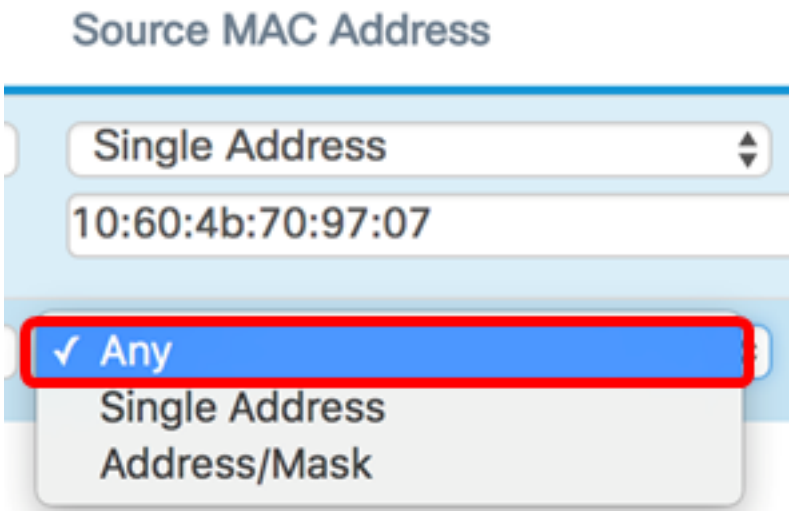
Passaggio 21. Fare clic sulla freccia dell'elenco a discesa Azione e scegliere **Autorizza**.



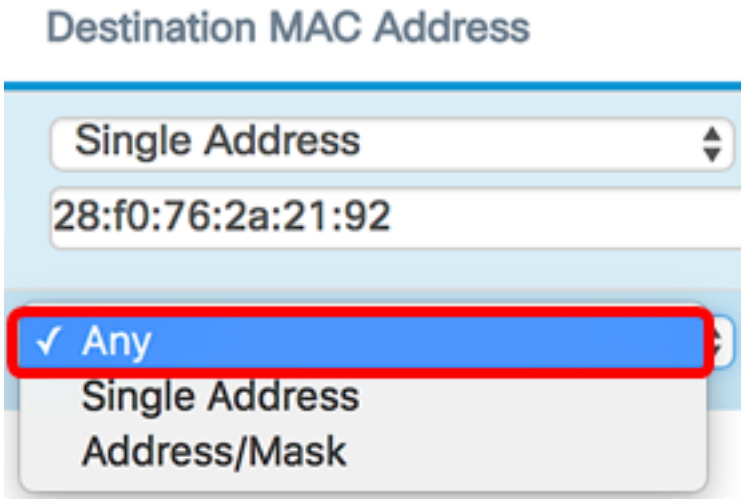
Passaggio 2. Fare clic sulla freccia a discesa Service(ETH Type) (Tipo ETH) e scegliere **All Traffic** (Tutto il traffico).



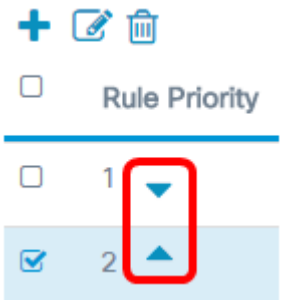
Passaggio 23. Fare clic sul menu a discesa Source MAC Address (Indirizzo MAC di origine) e scegliere **Any (Qualsiasi)**. In questo modo, verrà consentito il traffico proveniente da qualsiasi altro indirizzo MAC della rete, ad eccezione dell'indirizzo MAC PC1 indicato nella prima regola.



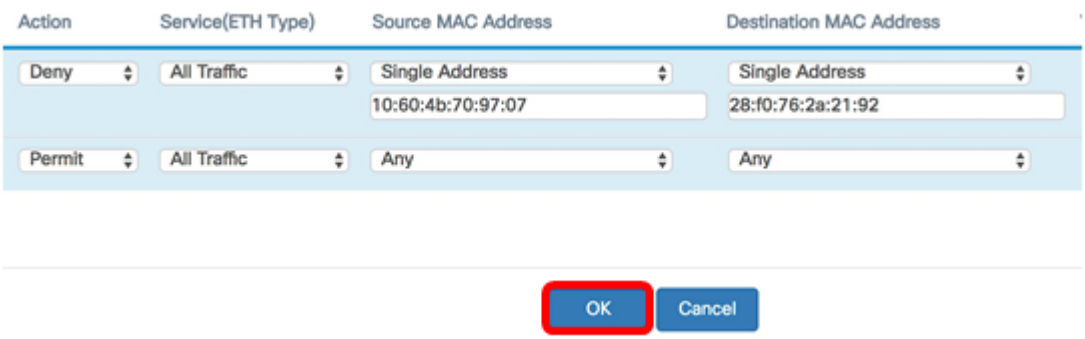
Passaggio 24. Fare clic sul menu a discesa Indirizzo MAC di destinazione e scegliere **Qualsiasi**. In questo modo, il traffico potrebbe raggiungere qualsiasi indirizzo MAC della rete.



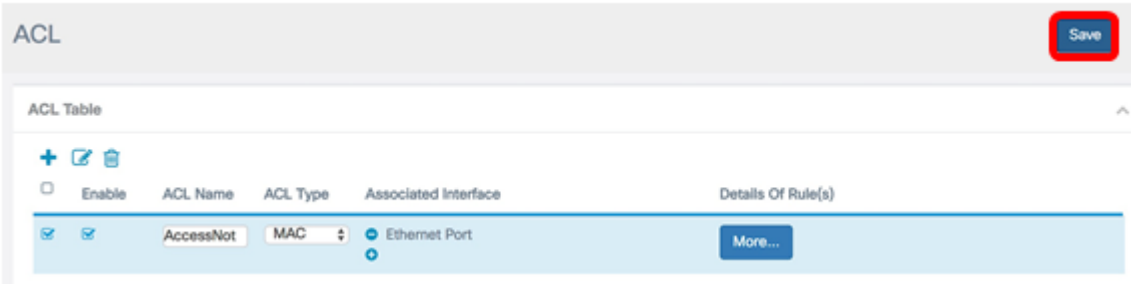
Passaggio 25. (Facoltativo) Modificare la priorità della regola facendo clic sulle frecce su e giù fino a quando la regola non è stata impostata.



Passaggio 26. Fare clic su **OK**.



Passaggio 27. Fare clic su **Salva**.



A questo punto, è necessario configurare l'ACL MAC sul punto di accesso WAP125 o WAP581.

Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco]