

Creazione di un ACL basato su MAC su SG350XG e SG550XG

Obiettivo

Un elenco di controllo di accesso (ACL, Access Control List) è un insieme di regole che possono essere create per manipolare i pacchetti a seconda che soddisfino o meno determinati criteri. Tali criteri possono essere gli indirizzi di origine o di destinazione, i campi di intestazione e altri componenti di un pacchetto. Se un pacchetto soddisfa i criteri specificati da un ACL, viene scartato o autorizzato a continuare. Un ACL basato su MAC usa le regole che analizzano l'intestazione di layer 2 di un pacchetto per questi criteri, come gli indirizzi MAC, gli ID VLAN e i valori Ethertype. L'implementazione di un ACL basato su MAC permette di controllare i pacchetti che viaggiano attraverso lo switch al livello 2.

Lo scopo di questo documento è mostrare come creare e configurare un ACL basato su MAC sugli switch SG350XG e SG550XG.

Dispositivi interessati

- SG350XG
- SG550XG

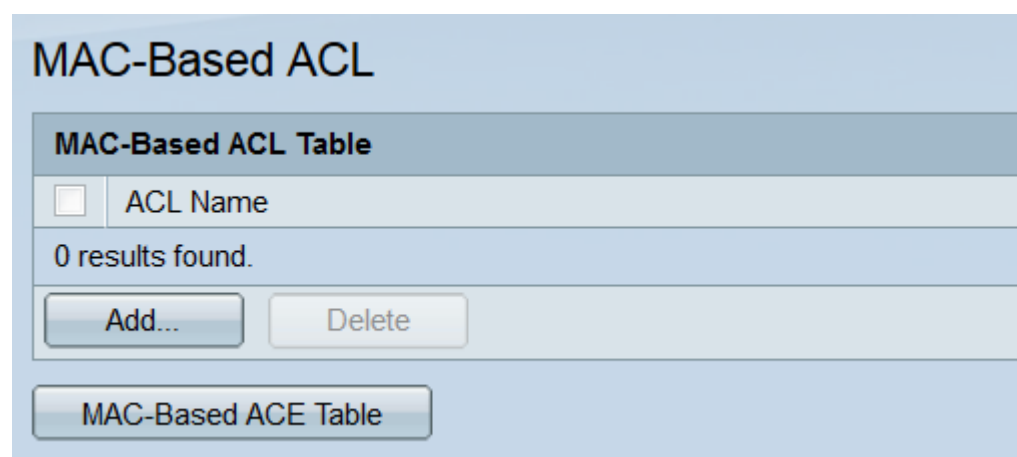
Versione del software

- v2.0.0.73

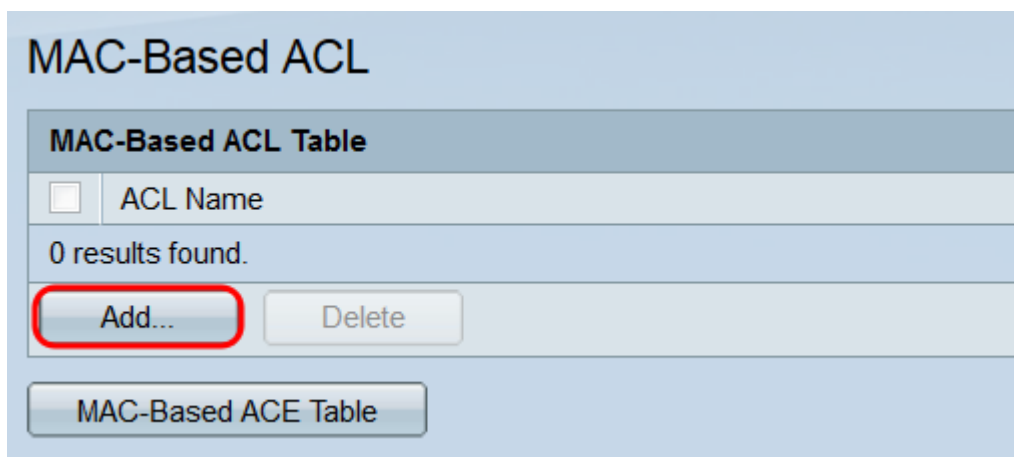
Configurazione ACL basati su MAC

Creazione un ACL e le regole

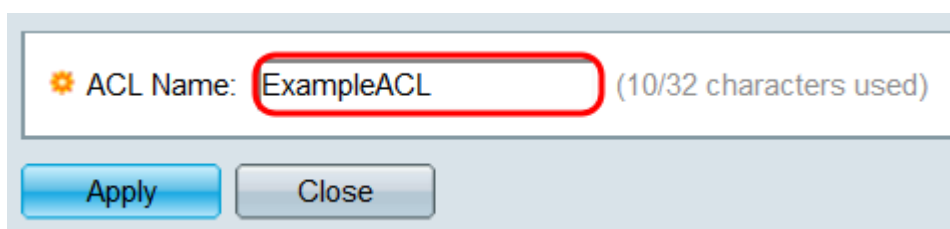
Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Access Control > ACL basato su MAC**. Viene visualizzata la pagina *ACL basato su MAC*.



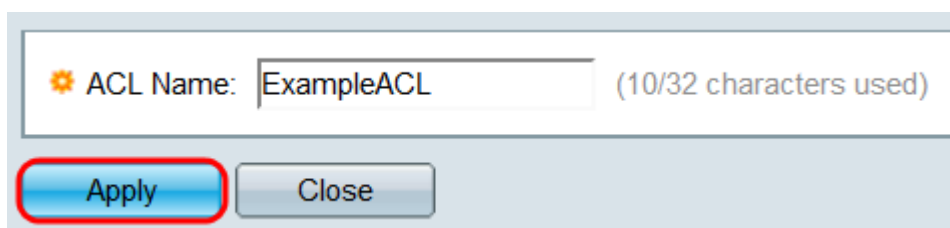
Passaggio 2. La *tabella degli ACL basati sull'indirizzo MAC* visualizzerà tutti gli ACL basati sull'indirizzo MAC presenti sullo switch. Per creare un nuovo ACL, fare clic sul pulsante **Add...**. Si apre la finestra *Add MAC-Based ACL*.



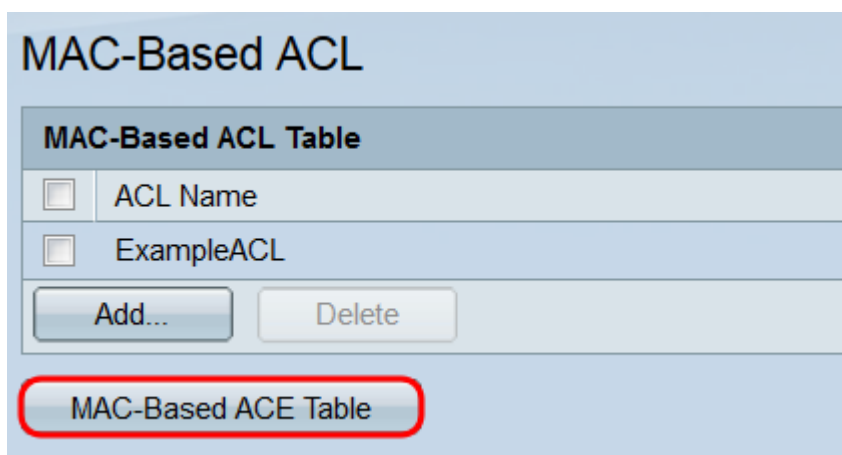
Passaggio 3. Nel campo *ACL Name* (Nome ACL), immettere il nome del nuovo ACL. Questo nome non influisce sulla funzione dell'ACL e serve solo a scopi di identificazione.



Passaggio 4. Fare clic su **Applica**. Il nuovo ACL verrà aggiunto alla *tabella degli ACL basati sull'indirizzo MAC*. Fare clic su **Chiudi** (Chiudi) per tornare alla pagina *MAC-Based ACL* o creare un altro ACL ripetendo il passaggio precedente.



Passaggio 5. Ogni ACL appena creato sarà vuoto; ovvero, non contiene regole per bloccare o consentire i pacchetti basati su indirizzi MAC. Per creare queste regole, è necessario aggiungere una voce di controllo di accesso (ACE) all'ACL. A tale scopo, fare clic sul pulsante **Tabella ACE basata su MAC** per andare alla pagina *ACE basata su MAC*.



Passaggio 6. Nella pagina *MAC-Based ACE*, selezionare l'ACL a cui si desidera aggiungere una voce ACE dall'elenco a discesa nella parte superiore della *tabella ACE basata su MAC*, quindi fare clic su **Vai**. Nella tabella vengono visualizzate le voci ACE attualmente associate

all'ACL selezionato. Per aggiungere una voce di controllo di accesso, fare clic sul pulsante **Aggiungi**. Viene visualizzata la finestra *Add MAC-Based ACE*.

Priority	Action	Logging	Destination		Source		VLAN ID	802.1p	802.1p Mask	Ethertype
			MAC Address	Wildcard Mask	MAC Address	Wildcard Mask				
0 results found.										

Passaggio 7. Nel campo *ACL Name* (Nome ACL) viene visualizzato il nome dell'ACL a cui si sta aggiungendo una voce ACE. Nel campo *Priorità*, immettere un numero di priorità per la voce ACE. Maggiore è la priorità di un ACE, prima verrà elaborato. L'intervallo è compreso tra 1 e 2147483647, dove 1 rappresenta la priorità più alta.

ACL Name: ExampleACL

Priority: 1 (Range: 1 - 2147483647)

Action: Permit Deny Shutdown

Logging: Enable

Time Range: Enable

Time Range Name: Edit

Destination MAC Address: Any User Defined

Destination MAC Address Value: [Input Field]

Destination MAC Wildcard Mask: [Input Field] (0s for matching, 1s for no matching)

Source MAC Address: Any User Defined

Source MAC Address Value: [Input Field]

Source MAC Wildcard Mask: [Input Field] (0s for matching, 1s for no matching)

VLAN ID: [Input Field] (Range: 1 - 4094)

802.1p: Include

802.1p Value: [Input Field] (Range: 0 - 7)

802.1p Mask: [Input Field] (Range: 0 - 7)

Ethertype: [Input Field] (Range: 5DD - FFFF)

Apply Close

Passaggio 8. Nel campo *Azione* selezionare un pulsante di opzione per determinare l'azione che verrà eseguita quando vengono soddisfatti i criteri della voce ACE.

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input type="checkbox"/> Enable	
Time Range:	<input type="checkbox"/> Enable	
Time Range Name:	▼ Edit	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
* Destination MAC Address Value:	<input type="text"/>	
* Destination MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
* Source MAC Address Value:	<input type="text"/>	
* Source MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
VLAN ID:	<input type="text"/> (Range: 1 - 4094)	
802.1p:	<input type="checkbox"/> Include	
* 802.1p Value:	<input type="text"/> (Range: 0 - 7)	
* 802.1p Mask:	<input type="text"/> (Range: 0 - 7)	
Ethertype:	<input type="text"/> (Range: 5DD - FFFF)	
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

Le opzioni sono:

- Permit: inoltra i pacchetti che soddisfano i criteri.
- Rifiuta - Elimina i pacchetti che soddisfano i criteri.
- Shutdown - Elimina i pacchetti che soddisfano i criteri, quindi disabilita la porta.

Passaggio 9. Nel campo *Registrazione*, selezionare la casella di controllo **Abilita** per abilitare la registrazione dei flussi ACL che corrispondono alla regola ACE. Se si utilizza la modalità di visualizzazione di base, andare al [punto 12](#). La modalità di visualizzazione può essere modificata mediante l'elenco a discesa nell'angolo superiore destro dell'utilità Web.

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="Edit"/>	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Source MAC Address Value:	<input type="text"/>	
Source MAC Wildcard Mask:	<input type="text"/> (0s for matching, 1s for no matching)	
VLAN ID:	<input type="text"/> (Range: 1 - 4094)	
802.1p:	<input type="checkbox"/> Include	
802.1p Value:	<input type="text"/> (Range: 0 - 7)	
802.1p Mask:	<input type="text"/> (Range: 0 - 7)	
Ethertype:	<input type="text"/> (Range: 5DD - FFFF)	

Passaggio 10. Nel campo *Intervallo di tempo*, selezionare la casella di controllo **Abilita** per fare in modo che la voce ACE sia attiva solo per un intervallo di tempo specificato. Se sullo switch non sono configurati intervalli di tempo, questo campo non è disponibile.

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input checked="" type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="ExampleRange"/> <input type="button" value="Edit"/>	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Source MAC Address Value:	<input type="text"/>	
Source MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
VLAN ID:	<input type="text"/>	(Range: 1 - 4094)
802.1p:	<input type="checkbox"/> Include	
802.1p Value:	<input type="text"/>	(Range: 0 - 7)
802.1p Mask:	<input type="text"/>	(Range: 0 - 7)
Ethertype:	<input type="text"/>	(Range: 5DD - FFFF)

Passaggio 11. Se è stato abilitato un intervallo di tempo per la voce di controllo di accesso, il campo *Nome intervallo di tempo* sarà disponibile. Utilizzare l'elenco a discesa per selezionare un intervallo di tempo già configurato sullo switch da applicare all'ACE. Se lo switch non dispone di intervalli di tempo, questo campo non è disponibile; fare clic sul collegamento **Modifica** per accedere alla pagina *Intervallo di tempo* e creare o modificare gli intervalli. Per ulteriori informazioni, fare riferimento all'articolo [Setting Up a Time Range sui modelli SG350XG e SG550XG](#).

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input checked="" type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="ExampleRange"/> <input type="button" value="Edit"/>	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Source MAC Address Value:	<input type="text"/>	
Source MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
VLAN ID:	<input type="text"/>	(Range: 1 - 4094)
802.1p:	<input type="checkbox"/> Include	
802.1p Value:	<input type="text"/>	(Range: 0 - 7)
802.1p Mask:	<input type="text"/>	(Range: 0 - 7)
Ethertype:	<input type="text"/>	(Range: 5DD - FFFF)

Passaggio 12. Nel campo *Indirizzo MAC di destinazione*, selezionare un pulsante di opzione per determinare gli indirizzi MAC di destinazione che costituiranno una corrispondenza. Selezionare **Qualsiasi** per far corrispondere l'indirizzo di destinazione oppure **Definito dall'utente** per specificare un indirizzo o un intervallo di indirizzi.

Destination MAC Address:	<input type="radio"/> Any <input checked="" type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text" value="00:12:34:56:78:90"/>	
Destination MAC Wildcard Mask:	<input type="text" value="00:00:00:00:00:00"/>	(0s for matching, 1s for no matching)

Se è stata selezionata l'opzione **Definito da utente**, compilare i campi riportati di seguito.

- Valore indirizzo MAC di destinazione: immettere l'indirizzo MAC di destinazione. Se un pacchetto contiene questo indirizzo di destinazione, l'ACE lo considererà una corrispondenza.
- Maschera jolly MAC di destinazione: immettere una maschera per definire un intervallo di indirizzi. Se si imposta un bit come 1, il bit corrispondente nell'indirizzo MAC verrà ignorato e i

bit corrispondenti saranno 0.

Nota: Data una maschera di 0000 000 000 000 000 000 000 000 000 000 000 000 000 000 111 1111 (il che significa che si cerca una corrispondenza nei bit in cui c'è 0 e non quella nei bit in cui c'è 1). È necessario convertire gli 1 in un valore esadecimale e scrivere 0 ogni quattro zeri. In questo esempio, poiché 1111 111 = FF, la maschera verrebbe scritta: come 00:00:00:00:00:FF.

Passaggio 13. Nel campo *Source MAC Address* (Indirizzo MAC di origine), selezionare un pulsante di opzione per determinare gli indirizzi MAC di origine che costituiranno una corrispondenza. Selezionare **Qualsiasi** per far corrispondere l'indirizzo di origine o **Definito dall'utente** per specificare un indirizzo o un intervallo di indirizzi.

Source MAC Address: Any User Defined

✱ Source MAC Address Value:

✱ Source MAC Wildcard Mask: (0s for matching, 1s for no matching)

Se è stata selezionata l'opzione **Definito da utente**, compilare i campi riportati di seguito.

- Valore indirizzo MAC di origine: immettere l'indirizzo MAC di origine. Se un pacchetto contiene questo indirizzo di origine, l'ACE lo considererà una corrispondenza.
- Maschera con caratteri jolly MAC di origine: immettere una maschera per definire un intervallo di indirizzi. Se si imposta un bit come 1, il bit corrispondente nell'indirizzo MAC verrà ignorato e i bit corrispondenti saranno 0 (ad esempio 00:00:00:00:00:11).

Nota: Data una maschera di 0000 000 000 000 000 000 000 000 000 000 000 000 000 000 111 1111 (il che significa che si cerca una corrispondenza nei bit in cui c'è 0 e non quella nei bit in cui c'è 1). È necessario convertire gli 1 in un valore esadecimale e scrivere 0 ogni quattro zeri. In questo esempio, poiché 1111 111 = FF, la maschera verrebbe scritta: come 00:00:00:00:00:FF.

Passaggio 14. Nel campo *VLAN ID*, immettere un ID VLAN compreso tra 1 e 4094. Se un pacchetto contiene questo ID VLAN, l'ACE lo considererà una corrispondenza. Questo campo non è obbligatorio; se la voce viene lasciata vuota, l'ACE non terrà conto degli ID VLAN quando esaminerà i pacchetti.

VLAN ID: (Range: 1 - 4094)

Passaggio 15. Nel campo *802.1p*, selezionare la casella di controllo **Includi** per includere i criteri 802.1p in ACE. Se sono stati inclusi i criteri 802.1p, immettere un valore 802.1p e una maschera rispettivamente nei campi *Valore 802.1p* e *Maschera 802.1p*. L'intervallo per entrambi i campi è compreso tra 0 e 7. Se un pacchetto contiene il valore 802.1p corrispondente e rientra nella maschera, la voce ACE lo considererà una corrispondenza.

802.1p:

Include

⚙️ 802.1p Value:

5

(Range: 0 - 7)

⚙️ 802.1p Mask:

0

(Range: 0 - 7)

Passaggio 16. Nel campo *Ethertype*, immettere un valore Ethertype da confrontare con i pacchetti in arrivo. Ethertype è un campo a due ottetti in un frame che indica il protocollo incapsulato nel pacchetto. L'intervallo è 5DD- FFFF. Se un pacchetto contiene il valore Ethertype specificato, l'ACE lo considererà una corrispondenza. Un elenco di valori Ethertype è disponibile in questa [pagina degli standard IEEE](#).

Ethertype:

5DD

(Range: 5DD - FFFF)

Passaggio 17. Fare clic su **Applica**. La voce di controllo di accesso verrà aggiunta all'ACL specificato. Fare clic su **Chiudi** per tornare alla pagina *ACE basata su MAC*.

ACL Name:	ExampleACL	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Destination MAC Address:	<input type="radio"/> Any <input checked="" type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text" value="00:12:34:56:78:90"/>	
Destination MAC Wildcard Mask:	<input type="text" value="00:00:00:00:00:00"/>	(0s for matching, 1s for no matching)
Source MAC Address:	<input type="radio"/> Any <input checked="" type="radio"/> User Defined	
Source MAC Address Value:	<input type="text" value="00:98:76:54:32:10"/>	
Source MAC Wildcard Mask:	<input type="text" value="00:00:00:00:FF:FF"/>	(0s for matching, 1s for no matching)
VLAN ID:	<input type="text" value="10"/>	(Range: 1 - 4094)
802.1p:	<input checked="" type="checkbox"/> Include	
802.1p Value:	<input type="text" value="5"/>	(Range: 0 - 7)
802.1p Mask:	<input type="text" value="0"/>	(Range: 0 - 7)
Ethertype:	<input type="text" value="5DD"/>	(Range: 5DD - FFFF)

Mappatura di un ACL basato su MAC alle porte

Passaggio 1. È possibile mappare un ACL a porte o VLAN. Per mappare un ACL basato su MAC a una o più porte, selezionare **Controllo di accesso > Binding ACL (porta)**. Si apre la pagina *Binding ACL (porta)*.

ACL Binding (Port)

A port can be bound with either a [policy](#) or an ACL, but not both.
The default action is to discard (Deny Any) all the packets that do not meet the rules in an ACL. You can override the default action of an ACL to forward those packets by configuring Permit Any on the desired ports.

ACL Binding Table Showing 1-10 of 48 per page

Filter: Interface Type equals to

<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input type="checkbox"/>	1	XG1				
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

[\[1-10\]](#) [\[11-20\]](#) [\[21-30\]](#) [\[31-40\]](#) [\[41-48\]](#)

Passaggio 2. Nell'elenco a discesa nella parte superiore della *tabella di associazione* degli ACL, selezionare porte o LAG (link aggregation group) come tipo di interfaccia. Se lo switch fa parte di uno stack, è possibile selezionare le porte di altre unità. Fare clic su **Go** per visualizzare un elenco del tipo di interfaccia specificato.

ACL Binding (Port)

A port can be bound with either a [policy](#) or an ACL, but not both.
The default action is to discard (Deny Any) all the packets that do not meet the rules in an ACL. You can override the default action of an ACL to forward those packets by configuring Permit Any on the desired ports.

ACL Binding Table

Filter: Interface Type equals to

<input type="checkbox"/>	Entry No.	Interface	MA	IPv6 ACL	Default Action
<input type="checkbox"/>	1	XG1			
<input type="checkbox"/>	2	XG2			
<input type="checkbox"/>	3	XG3			
<input type="checkbox"/>	4	XG4			
<input type="checkbox"/>	5	XG5			
<input type="checkbox"/>	6	XG6			
<input type="checkbox"/>	7	XG7			
<input type="checkbox"/>	8	XG8			
<input type="checkbox"/>	9	XG9			
<input type="checkbox"/>	10	XG10			

Passaggio 3. Selezionare la casella di controllo di un'interfaccia, quindi fare clic sul pulsante **Modifica**. Viene visualizzata la finestra *Modifica binding ACL*.

ACL Binding (Port)

A port can be bound with either a [policy](#) or an ACL, but not both.

The default action is to discard (Deny Any) all the packets that do not meet the rules in an ACL. You can override the default action of an ACL to forward those packets by configuring Permit Any on the desired ports.

ACL Binding Table						
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1"/> <input type="button" value="Go"/>						
<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input checked="" type="checkbox"/>	1	XG1				
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

Passaggio 4. Il campo *Interface* visualizza la porta o il LAG attualmente in fase di configurazione. L'interfaccia selezionata nella *tabella di binding ACL* verrà visualizzata automaticamente. Questo campo può essere usato per passare rapidamente da un'interfaccia all'altra senza tornare alla pagina *Binding ACL (porta)*.

Interface: Unit Port LAG

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action: Deny Any Permit Any

Passaggio 5. Selezionare la casella di controllo **Select MAC-Based ACL**, quindi usare l'elenco a discesa per selezionare un ACL da mappare all'interfaccia specificata.

Interface: Unit Port LAG

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action: Deny Any Permit Any

Passaggio 6. Nel campo *Azione predefinita*, selezionare un pulsante di opzione per determinare come verranno gestiti i pacchetti che non corrispondono ai criteri dell'ACL. Il valore predefinito è **Deny Any**, che elimina tutti i pacchetti che non corrispondono ai criteri dell'ACL; **Permit Any** inoltrerà invece i pacchetti non corrispondenti.

Interface: Unit Port LAG

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action: Deny Any Permit Any

Passaggio 7. Fare clic su **Applica**. L'ACL è mappato all'interfaccia specificata. È possibile usare il campo *Interfaccia* per selezionare un'interfaccia diversa da configurare oppure fare clic su **Close** per tornare alla pagina *ACL Binding (Porta)*.

Interface: Unit Port LAG

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action: Deny Any Permit Any

Passaggio 8. Per copiare rapidamente le impostazioni di un'interfaccia su altre interfacce, selezionare la casella di controllo dell'interfaccia che si desidera copiare, quindi fare clic sul

pulsante **Copia impostazioni...**. Viene visualizzata la finestra *Copia impostazioni*.

ACL Binding (Port)

A port can be bound with either a [policy](#) or an ACL, but not both.
The default action is to discard (Deny Any) all the packets that do not meet the rules in an ACL. You can override the default action of an ACL to forward those packets by configuring Permit Any on the desired ports.

ACL Binding Table

Filter: *Interface Type* equals to

<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input checked="" type="checkbox"/>	1	XG1	ExampleACL			Deny Any
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

Passaggio 9. Nel campo di testo, immettere l'interfaccia o le interfacce in cui si desidera copiare le impostazioni. Le interfacce possono essere separate da virgole oppure è possibile specificare un intervallo.

Copy configuration from entry 1 (XG1)

to: (Example: 1,3,5-10 or: XG1,XG3-XG5)

Passaggio 10. Fare clic su **Applica**. Le impostazioni vengono copiate.

Copy configuration from entry 1 (XG1)

to: (Example: 1,3,5-10 or: XG1,XG3-XG5)

Passaggio 11. Per cancellare le impostazioni di un'interfaccia, selezionare la relativa casella di controllo e fare clic su **Cancella**. Si noti che è possibile selezionare e deselezionare contemporaneamente più interfacce.

ACL Binding (Port)

A port can be bound with either a [policy](#) or an ACL, but not both.

The default action is to discard (Deny Any) all the packets that do not meet the rules in an ACL. You can override the default action of an ACL to forward those packets by configuring Permit Any on the desired ports.

ACL Binding Table						
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1"/> <input type="button" value="Go"/>						
<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input checked="" type="checkbox"/>	1	XG1	ExampleACL			Deny Any
<input type="checkbox"/>	2	XG2				
<input type="checkbox"/>	3	XG3				
<input type="checkbox"/>	4	XG4				
<input type="checkbox"/>	5	XG5				
<input type="checkbox"/>	6	XG6				
<input type="checkbox"/>	7	XG7				
<input type="checkbox"/>	8	XG8				
<input type="checkbox"/>	9	XG9				
<input type="checkbox"/>	10	XG10				

Mappatura di un ACL basato su MAC sulle VLAN

Passaggio 1. È possibile mappare un ACL a porte o VLAN. Per mappare un ACL basato su MAC a una VLAN, selezionare **Controllo di accesso > Binding ACL (VLAN)**. Si apre la pagina *ACL Binding (VLAN)*.

ACL Binding Table					
<input type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
0 results found.					

Passaggio 2. La *tabella di binding degli ACL* visualizza tutti gli ACL attualmente mappati alle VLAN. Se non è stato mappato alcun ACL, la tabella è vuota. Per mappare un ACL a una VLAN, fare clic sul pulsante **Add...** Viene visualizzata la finestra *Add ACL Binding* (Aggiungi associazione ACL).

ACL Binding Table					
<input type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
0 results found.					

Passaggio 3. Selezionare una VLAN a cui mappare un ACL usando l'elenco a discesa nel campo *VLAN ID*. Questo campo può essere usato anche per passare rapidamente da una VLAN all'altra senza tornare alla pagina *Binding ACL (VLAN)*.

VLAN ID: 1

Select MAC-Based ACL: ExampleACL

Select IPv4-Based ACL: [dropdown]

Select IPv6-Based ACL: [dropdown]

Default Action: Deny Any Permit Any

Apply Close

Passaggio 4. Selezionare la casella di controllo **Select MAC-Based ACL** e usare l'elenco a discesa per selezionare un ACL da mappare alla VLAN specificata.

VLAN ID: 1

Select MAC-Based ACL: ExampleACL

Select IPv4-Based ACL: [dropdown]

Select IPv6-Based ACL: [dropdown]

Default Action: Deny Any Permit Any

Apply Close

Nota: Non è possibile associare un ACL basato su MAC che usa un ID VLAN come parte dei suoi criteri a una VLAN. Inoltre, un ACL con un intervallo di tempo non può essere associato a una VLAN.

Passaggio 5. Nel campo *Default Action* (Azione predefinita), selezionare un pulsante di opzione per determinare come verranno gestiti i pacchetti che non corrispondono ai criteri dell'ACL. Il valore predefinito è **Deny Any**, che elimina tutti i pacchetti che non corrispondono ai criteri dell'ACL; **Permit Any** inoltrerà invece i pacchetti non corrispondenti.

VLAN ID:

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action: Deny Any Permit Any

Passaggio 6. Fare clic su **Applica**. L'ACL è mappato alla VLAN specificata. È possibile usare il campo *VLAN ID* per selezionare una VLAN diversa da configurare oppure fare clic su **Close** per tornare alla pagina *VLAN (Associazione ACL)*.

VLAN ID:

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Default Action: Deny Any Permit Any

Passaggio 7. Per copiare rapidamente le impostazioni di una VLAN su altre VLAN, selezionare la casella di controllo della configurazione VLAN da copiare, quindi fare clic sul pulsante **Copy Settings....** Viene visualizzata la finestra *Copia impostazioni*.

ACL Binding (VLAN)

ACL Binding Table					
<input checked="" type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input checked="" type="checkbox"/>	1	ExampleACL			Deny Any

Passaggio 8. Nel campo di testo, immettere l'ID VLAN o gli ID VLAN in cui copiare le impostazioni. Gli ID possono essere separati da virgole oppure è possibile specificare un intervallo.

Copy configuration from VLAN1
to VLAN(s): (Example: 1,3,5-10)

Passaggio 9. Fare clic su **Applica**. Le impostazioni vengono copiate.

Copy configuration from VLAN1
to VLAN(s): (Example: 1,3,5-10)

Passaggio 10. Per cancellare le impostazioni di una VLAN, selezionare la relativa casella di controllo e fare clic su **Elimina**. È possibile selezionare e cancellare contemporaneamente più VLAN.

ACL Binding (VLAN)

ACL Binding Table						
<input checked="" type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action	
<input checked="" type="checkbox"/>	1	ExampleACL			Deny Any	