Configurazione di ACL (Access Control List) e ACE (Access Control Entry) basati su MAC su uno switch gestito

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'elenco di controllo di accesso (ACL) basato su MAC (Media Access Control) è un elenco di indirizzi MAC di origine che utilizzano informazioni di layer 2 per autorizzare o negare l'accesso al traffico. Se un pacchetto proviene da un punto di accesso wireless a una porta LAN (Local Area Network) o viceversa, il dispositivo controllerà se l'indirizzo MAC di origine del pacchetto corrisponde a una voce dell'elenco e controllerà le regole ACL in base al contenuto del frame. Utilizza quindi i risultati corrispondenti per autorizzare o negare il pacchetto. Tuttavia, i pacchetti da LAN a porta LAN non verranno controllati. 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. 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 gli ACL e gli ACE basati sull'indirizzo MAC sullo switch gestito.

Dispositivi interessati | Versione software

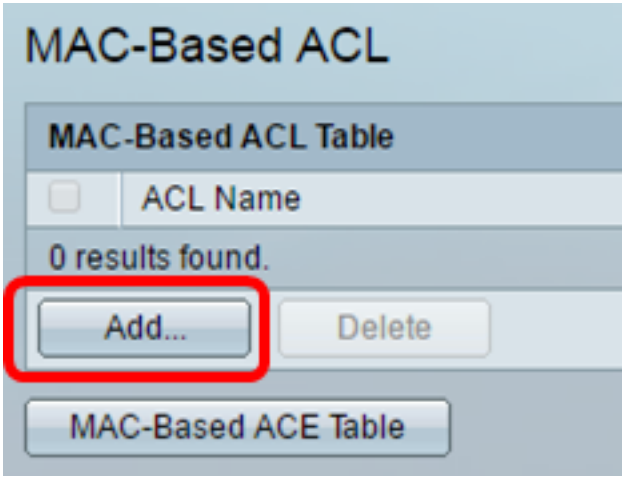
- Serie Sx350 | 2.2.0.66 (scarica la versione più recente)
- Serie SG350X | 2.2.0.66 (scarica la versione più recente)
- Serie Sx500 | 1.4.5.02 (scarica la versione più recente)
- Serie Sx550X | 2.2.0.66 (scarica la versione più recente)

Configurazione di ACL e ACE basati su MAC

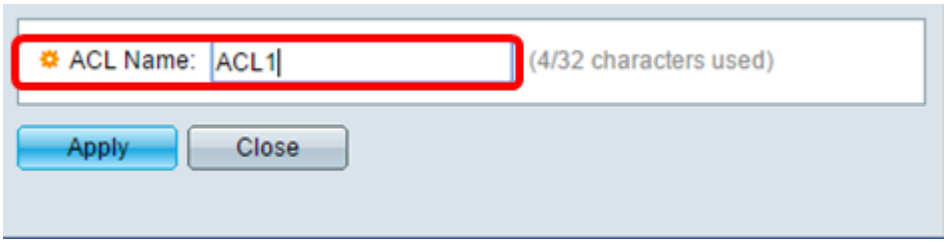
Configurazione di ACL basati su MAC

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

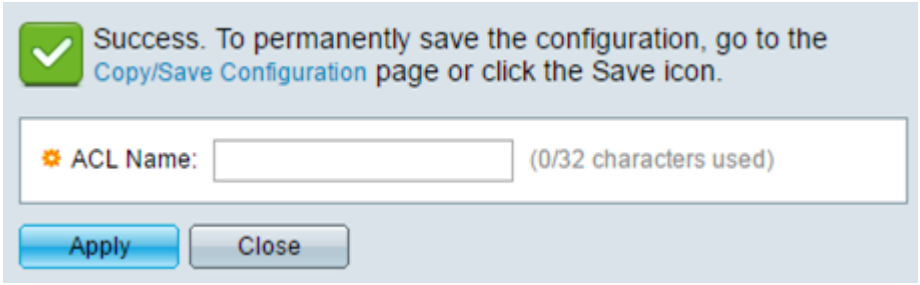
Passaggio 2. Fare clic sul pulsante **Aggiungi**.



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



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 MAC sullo switch.

Configura ACE basata su MAC

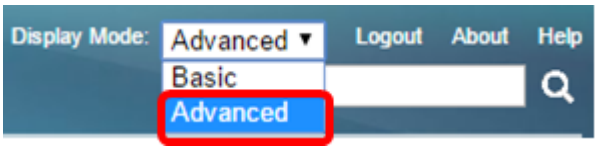
Quando si riceve un frame su una porta, lo switch lo elabora tramite il primo ACL. Se il frame corrisponde a un filtro ACE del primo ACL, viene eseguita l'azione ACE. Se il frame non corrisponde a nessuno dei filtri ACE, viene elaborato l'ACL successivo. Se non viene trovata alcuna corrispondenza con nessuna voce ACE in tutti gli ACL rilevanti, il frame viene scartato per impostazione predefinita.

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

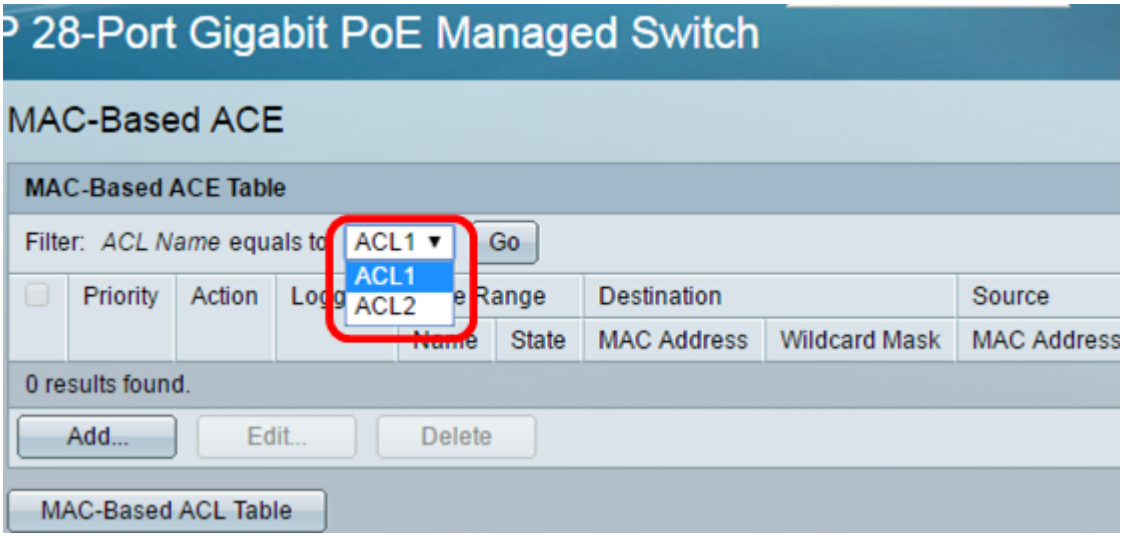
Nota: Per evitare questa azione predefinita, è possibile creare una voce ACE a bassa priorità che autorizzi tutto il traffico.

Passaggio 1. Nell'utility basata sul Web, andare a **Controllo accesso > ACE basata su MAC**.

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**.

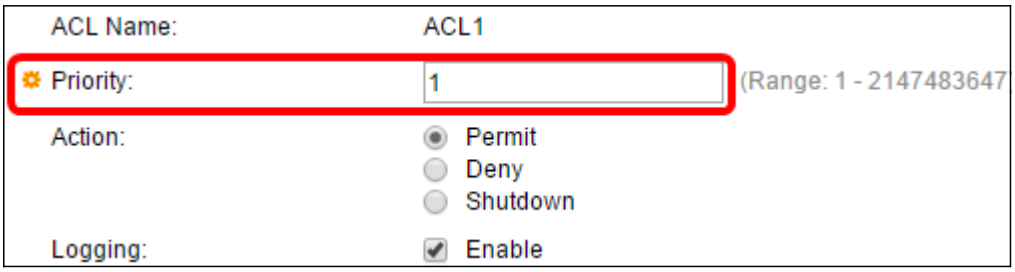


Nota: Le voci ACE già configurate per l'ACL verranno visualizzate nella tabella.

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.

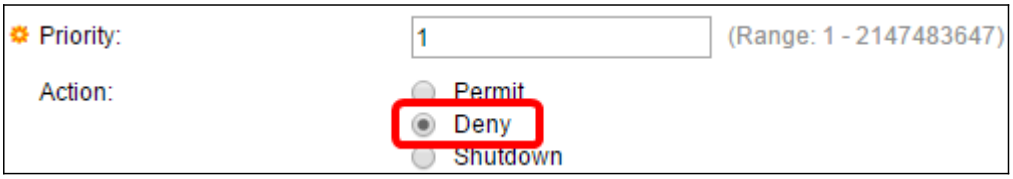
Passaggio 4. Inserire il valore di priorità per la voce ACE nel campo *Priorità*. Le voci di controllo di accesso con priorità più alta vengono elaborate per prime. Il valore 1 rappresenta la priorità più alta.



Passaggio 5. (Facoltativo) Selezionare la casella di controllo Abilita registrazione per abilitare la registrazione dei flussi ACL che corrispondono alla regola ACL.

Passaggio 6. Fare clic sul pulsante di opzione corrispondente all'azione desiderata eseguita quando un frame soddisfa i criteri richiesti dell'ACE.

Nota: Nell'esempio, viene scelto Nega.



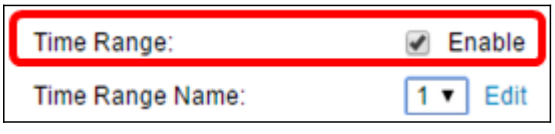
Permit: lo switch inoltra i pacchetti che soddisfano i criteri richiesti dall'ACE.

Nega: lo switch scarta i pacchetti che soddisfano i criteri richiesti dell'ACE.

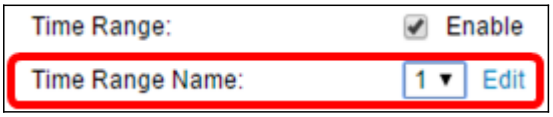
Shutdown: lo switch scarta i pacchetti che non soddisfano i criteri richiesti dall'ACE e disabilita la porta a cui sono stati ricevuti.

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

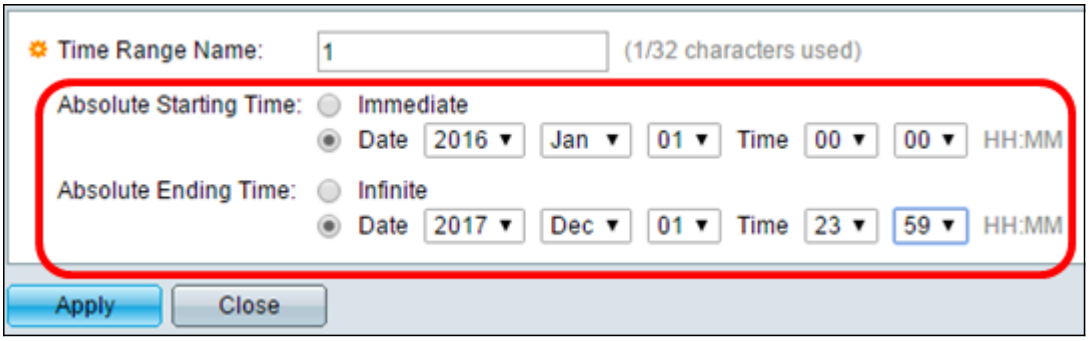
Passaggio 7. (Facoltativo) Selezionare la casella di controllo **Abilita** intervallo di tempo per consentire la configurazione di un intervallo di tempo per l'ACE. Gli intervalli di tempo vengono utilizzati per limitare il periodo di validità di un ACE.



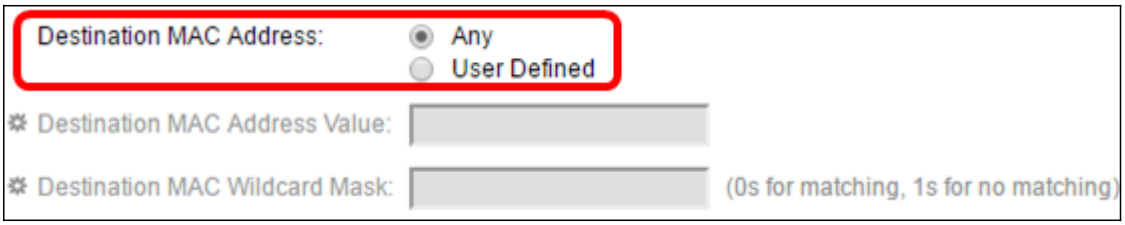
Passaggio 8. (Facoltativo) Dall'elenco a discesa Nome intervallo di tempo, scegliere un intervallo di tempo da applicare alla voce ACE.



Nota: È possibile fare clic su **Modifica** per passare a un intervallo di tempo e crearlo nella pagina Intervallo di tempo.



Passaggio 9. Fare clic sul pulsante di opzione corrispondente ai criteri desiderati per l'ACE nell'area Indirizzo MAC di destinazione.



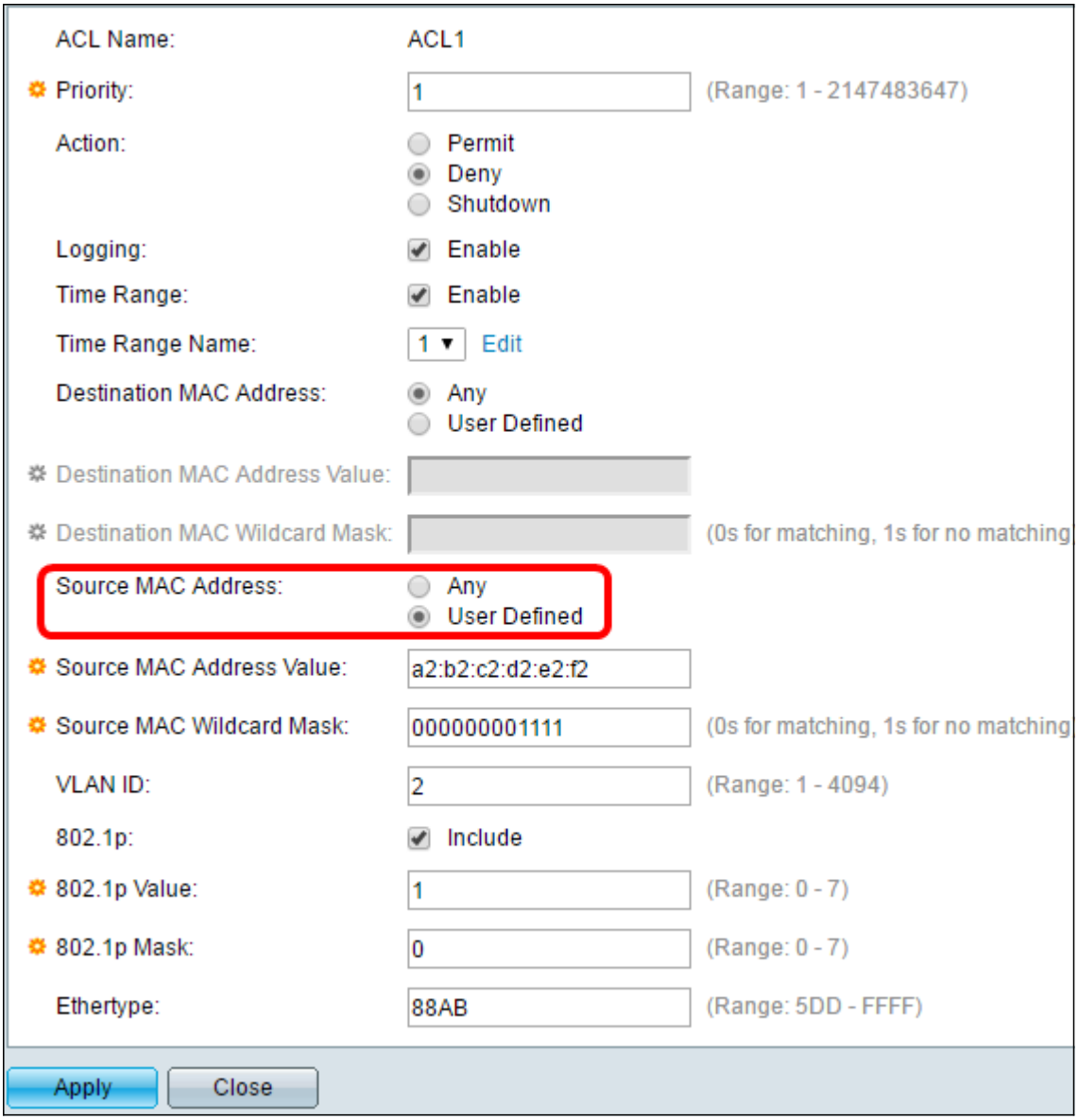
Le opzioni sono:

Qualsiasi - Tutti gli indirizzi MAC di destinazione vengono applicati all'ACE.

Definito dall'utente: immettere un indirizzo MAC e una maschera jolly MAC da applicare all'ACE nei campi *Valore indirizzo MAC destinazione* e *Maschera jolly MAC destinazione*. Le maschere con caratteri jolly vengono utilizzate per definire un intervallo di indirizzi MAC.

Nota: Nell'esempio, viene scelto Qualsiasi. Scegliendo questa opzione, la voce ACE da creare negherà il traffico ACE.

Passaggio 10. Fare clic sul pulsante di opzione corrispondente ai criteri desiderati per l'ACE nell'area Indirizzo MAC di origine.



Le opzioni sono:

Qualsiasi - Tutti gli indirizzi MAC di origine vengono applicati all'ACE.

Definito dall'utente: immettere un indirizzo MAC e una maschera con caratteri jolly MAC da applicare all'ACE nei campi *Valore indirizzo MAC di origine* e *Maschera con caratteri jolly MAC di origine*. Le maschere con caratteri jolly vengono utilizzate per definire un intervallo di indirizzi MAC.

Nota: In questo esempio, viene scelto Definito dall'utente.

Passaggio 11. (Facoltativo) Nel campo *VLAN ID* (ID VLAN), immettere un ID VLAN che verrà associato al tag VLAN del frame.

Passaggio 12. (Facoltativo) Per includere i valori 802.1p nei criteri ACE, selezionare **Includi** nella casella di controllo 802.1p. Lo standard 802.1p riguarda la tecnologia Class of Service (CoS). CoS è un campo a 3 bit in un frame Ethernet utilizzato per differenziare il traffico.

Passaggio 13. Se sono inclusi valori 802.1p, immettere i seguenti campi:

Valore 802.1p - Immettere il valore 802.1p da associare. 802.1p è una specifica che offre agli switch di layer 2 la possibilità di assegnare priorità al traffico e di eseguire un filtro multicast dinamico. I valori sono i seguenti:

- 0 — Contesto. I dati con la priorità più bassa, ad esempio trasferimenti in blocco, giochi e così via.

- 1 — Massimo sforzo. I dati che richiedono la distribuzione nel miglior modo possibile sulla normale priorità LAN. La rete non fornisce alcuna garanzia sulla consegna, ma i dati ottengono una velocità in bit e un tempo di consegna non specificati in base al traffico.

- 2 — Ottimo sforzo. Dati che richiedono la massima attenzione da parte degli utenti importanti.

- 3 — Applicazioni critiche come il protocollo SIP (Phone Session Initiation Protocol) LVS (Linux Virtual Server).

- 4 — Video latenza e jitter inferiore a 100 ms.

- 5 — Voce Cisco IP phone predefinito. latenza e jitter inferiore a 10 ms.

- 6 — Protocollo RTP (Real-time Transport Protocol) LVS di controllo della rete interna.

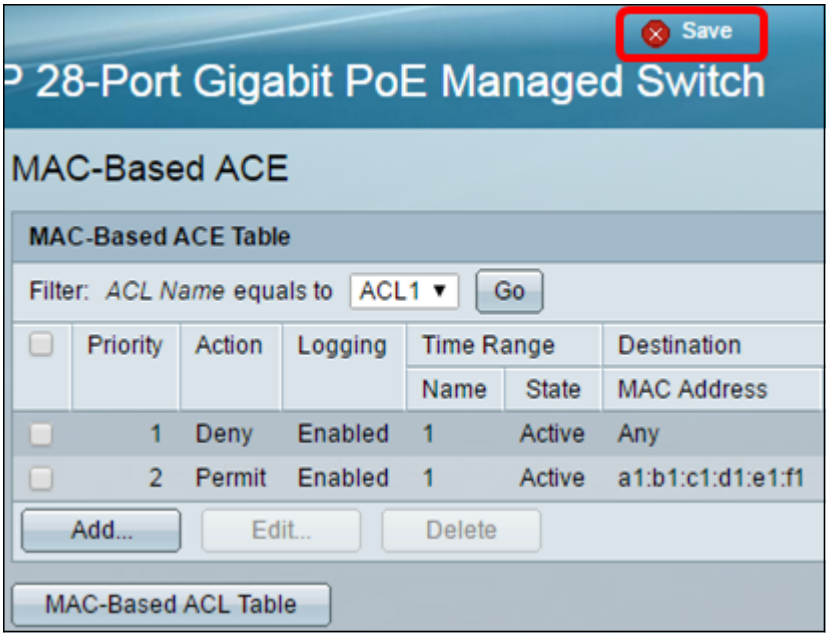
- 7 — Controllo della rete. Requisiti elevati per la manutenzione e il supporto dell'infrastruttura di rete.

Maschera 802.1p — immettere la maschera con caratteri jolly dei valori 802.1p. Questa maschera con caratteri jolly viene utilizzata per definire l'intervallo di valori 802.1p.

Passaggio 14. (Facoltativo) Immettere il tipo Ethernet del frame da abbinare. Ethertype è un campo a 2 ottetti in un frame Ethernet utilizzato per indicare il protocollo utilizzato per il payload del frame.

Passaggio 14. Fare clic su **Apply (Applica)**, quindi su **Close** (Chiudi). La voce di controllo di accesso viene creata e associata al nome dell'ACL.

Passaggio 15. Fare clic su **Save** per salvare le impostazioni nel file della configurazione di avvio.



A questo punto, è necessario configurare un ACE basato su MAC sullo switch.

Altri link utili:

- Switch serie 350 - Pagina del prodotto
- Switch serie 3500X - Pagina del prodotto
- Switch serie 550 - Pagina del prodotto
- Switch serie 550X - Pagina del prodotto

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

Fare clic qui per visualizzare altre Tech Talks di Cisco