

Configurazione delle proprietà 802.1x sugli switch impilabili serie Sx500

Obiettivo

IEEE 802.1x è uno standard che facilita il controllo dell'accesso tra un client e un server. Prima che i servizi possano essere forniti a un client da una LAN o da uno switch, il client connesso alla porta dello switch deve essere autenticato dal server di autenticazione che in questo caso esegue RADIUS (Remote Authentication Dial-In User Service). Per abilitare l'autenticazione basata sulla porta 802.1x, è necessario abilitare 802.1x a livello globale sullo switch.

Per configurare completamente 802.1x, è necessario eseguire le seguenti configurazioni:

1. Creare una VLAN, fare clic [qui](#).
2. Assegnare la porta alla VLAN, continuare con l'articolo di cui sopra. Per configurare nella CLI, fare clic [qui](#).
3. Configurare l'autenticazione della porta, fare clic [qui](#).

In questo articolo viene spiegato come configurare le proprietà 802.1x, che includono l'autenticazione e le proprietà della VLAN guest. Fare riferimento agli articoli precedenti per altre configurazioni. La VLAN guest consente di accedere a servizi che non richiedono che le porte o i dispositivi in abbonamento siano autenticati e autorizzati tramite l'autenticazione 802.1x o basata sull'indirizzo MAC.

Dispositivi interessati

·Switch Stack Serie Sx500

Versione del software

•1.3.0.62

Abilita autenticazione basata sulla porta e VLAN guest nelle proprietà 802.1x

Passaggio 1. Accedere all'utilità di configurazione Web per scegliere **Protezione > 802.1X > Proprietà**. Viene visualizzata la pagina *Proprietà*:

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID:

☀ Guest VLAN Timeout: Immediate
 User Defined sec. (Range: 30 - 180)

Passaggio 2. Selezionare **Abilita** nel campo Autenticazione basata sulla porta per abilitare l'autenticazione 802.1x basata sulla porta.

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID:

☀ Guest VLAN Timeout: Immediate
 User Defined sec. (Range: 30 - 180)

Passaggio 3. Fare clic sul pulsante di opzione desiderato nel campo Metodo di autenticazione. Il server RADIUS esegue l'autenticazione del client. Questo server convalida se l'utente è autenticato o meno e notifica allo switch se al client è consentito accedere alla LAN e ad altri servizi dello switch. Lo switch funge da proxy e il server è trasparente per il client.

Properties

Port-Based Authentication: Enable

**Authentication Method: RADIUS, None
 RADIUS
 None**

Guest VLAN: Enable

Guest VLAN ID:

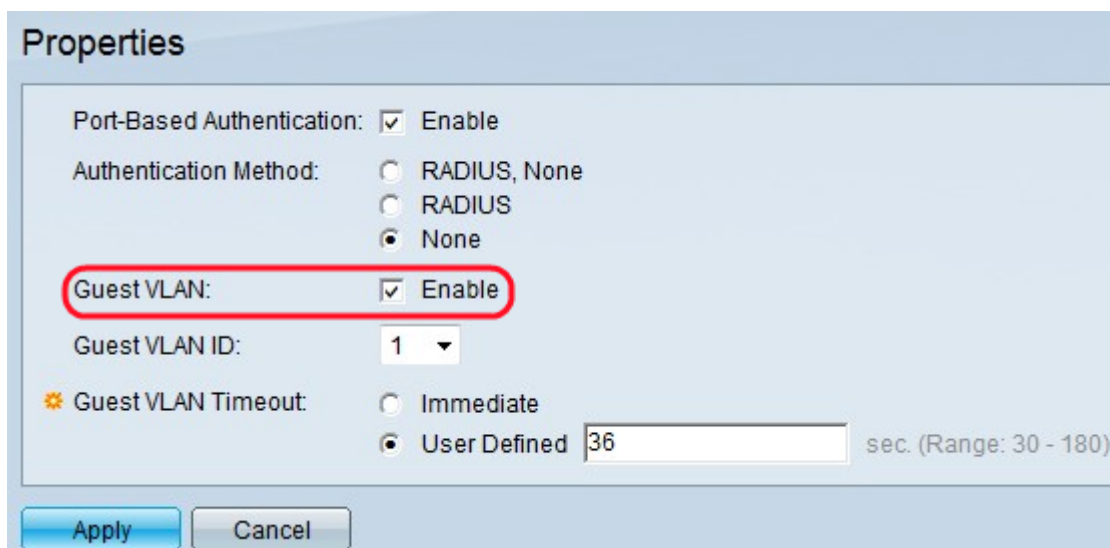
☀ Guest VLAN Timeout: Immediate
 User Defined sec. (Range: 30 - 180)

·RADIUS, None: esegue prima l'autenticazione della porta con l'aiuto del server RADIUS. Se il server non risponde, ad esempio quando è inattivo, non viene eseguita alcuna autenticazione e la sessione è consentita. Se il server è disponibile e le credenziali utente non sono corrette, l'accesso viene negato e la sessione viene terminata.

·RADIUS: esegue l'autenticazione della porta in base al server RADIUS. Se non viene eseguita alcuna autenticazione, la sessione viene terminata.

·Nessuno - Non autentica l'utente e consente la sessione.

Passaggio 4. (Facoltativo) Selezionare **Enable** per abilitare l'uso di una VLAN guest per le porte non autorizzate nel campo Guest VLAN. Se è abilitata una VLAN guest, tutte le porte non autorizzate si uniscono automaticamente alla VLAN scelta nel campo ID VLAN guest. Se una porta viene successivamente autorizzata, viene rimossa dalla VLAN guest.



The screenshot shows a 'Properties' dialog box with the following settings:

- Port-Based Authentication: Enable
- Authentication Method: RADIUS, None; RADIUS; None
- Guest VLAN: Enable (highlighted with a red circle)
- Guest VLAN ID: 1 (dropdown menu)
- Guest VLAN Timeout: Immediate; User Defined 36 sec. (Range: 30 - 180)

Buttons: Apply, Cancel

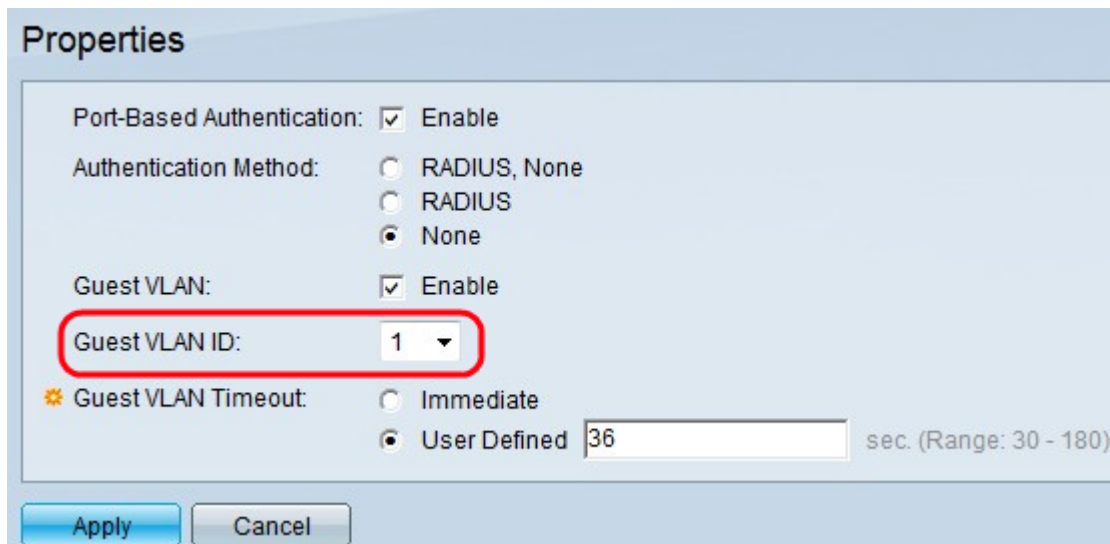
Prima di poter usare la modalità di autenticazione MAC, è necessario configurare una modalità VLAN guest. Il framework 802.1x consente a un dispositivo (il richiedente) di richiedere l'accesso alla porta da un dispositivo remoto (autenticatore) al quale è connesso. Solo quando il richiedente che richiede l'accesso alla porta viene autenticato e autorizzato è autorizzato a inviare dati alla porta. In caso contrario, l'autenticatore elimina i dati supplicant a meno che i dati non vengano inviati a una VLAN guest e/o a VLAN non autenticate.

Nota: La VLAN guest, se configurata, è una VLAN statica con le seguenti caratteristiche:

- Deve essere definita manualmente da una VLAN statica esistente.
- Disponibile automaticamente solo per dispositivi non autorizzati o porte di dispositivi connessi e abilitati per le VLAN guest.
- Se una porta è abilitata per la VLAN guest, lo switch aggiunge automaticamente la porta come membro senza tag della VLAN guest quando la porta non è autorizzata e rimuove la porta dalla VLAN guest quando il primo richiedente della porta è autorizzato.
- La VLAN guest non può essere utilizzata sia come VLAN voce che come VLAN non autenticata.

Timesaver: se la VLAN guest è disabilitata, andare al passaggio 7.

Passaggio 5. Selezionare l'ID della VLAN guest dall'elenco di VLAN nell'elenco a discesa ID VLAN guest.



Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID:

Guest VLAN Timeout: Immediate
 User Defined sec. (Range: 30 - 180)

Passaggio 6. Fare clic sul pulsante di opzione desiderato nel campo Timeout VLAN guest. Le opzioni disponibili sono:

- Immediato: la VLAN guest scade dopo un periodo di tempo di 10 secondi.
- Definito da utente: immettere manualmente il periodo di tempo nel campo Definito da utente.

Nota: Dopo il collegamento, se il software non rileva un supplicante 802.1x o l'autenticazione della porta non è riuscita, la porta viene aggiunta alla VLAN guest solo dopo la scadenza del periodo di timeout della VLAN guest. Se la porta viene modificata da Autorizzata a Non autorizzata, viene aggiunta alla VLAN guest solo dopo la scadenza del periodo di timeout della VLAN guest. Nella tabella Autenticazione VLAN vengono visualizzate tutte le VLAN e viene indicato se l'autenticazione è abilitata o meno per queste VLAN.

Passaggio 7. Fare clic su **Apply** per salvare le impostazioni.

Configurazione VLAN non autenticata

Quando lo standard 802.1x è abilitato, le porte o i dispositivi non autorizzati non sono autorizzati ad accedere alla VLAN a meno che non facciano parte della VLAN guest o non siano autenticati. Le porte devono essere aggiunte manualmente alle VLAN nella pagina *Port to VLAN (Porta sulla VLAN)*.

Passaggio 1. Accedere all'utilità di configurazione Web per scegliere **Protezione > 802.1X > Proprietà**. Viene visualizzata la pagina *Proprietà*.

VLAN Authentication Table			
	VLAN ID	VLAN Name	Authentication
<input checked="" type="radio"/>	2	VLAN 2	Enabled
<input type="radio"/>	3	VLAN 3	Enabled

Passaggio 2. Scorrere la pagina fino alla tabella di autenticazione VLAN, fare clic sul pulsante di opzione della VLAN su cui si desidera disabilitare l'autenticazione e fare clic su **Modifica**. Viene visualizzata la pagina *Modifica autenticazione VLAN*.

VLAN ID: 2 ▼
VLAN Name: VLAN 2
Authentication: Enable

Apply Close

Passaggio 3. (Facoltativo) Selezionare un ID VLAN dall'elenco a discesa VLAN ID.

VLAN ID: 2 ▼
VLAN Name: VLAN 2
Authentication: Enable

Apply Close

Passaggio 4. Deselezionare **Enable** per disabilitare l'autenticazione e rendere la VLAN una VLAN non autenticata.

Passaggio 5. Fare clic su **Apply** per applicare le impostazioni. Le modifiche vengono apportate alla tabella di autenticazione VLAN:

VLAN Authentication Table			
	VLAN ID	VLAN Name	Authentication
<input checked="" type="radio"/>	2	VLAN 2	Disabled
<input type="radio"/>	3	VLAN 3	Enabled

Edit..