

Configuratie van 802.1x eigenschappen op SX500 Series Stackable-switches

Doel

IEEE 802.1x is een standaard die toegangscontrole tussen een client en een server vergemakkelijkt. Voordat er diensten aan een client kunnen worden geleverd door een LAN of de client die is aangesloten op de switchpoort, moet deze client geauthentiseerd zijn door de verificatieserver die in dit geval de Radio-In User Service (RADIUS) op afstand uitvoert. Om 802.1x op poort gebaseerde authenticatie mogelijk te maken, moet 802.1x wereldwijd op de switch ingeschakeld zijn.

Om 802.1x volledig te configureren dienen de volgende configuraties te worden uitgevoerd:

1. Maak een VLAN en klik [hier](#).
2. Pas Port aan VLAN toe, ga verder met het bovenstaande artikel. Klik [hier](#) om in de CLI te configureren.
3. Het configureren van poortverificatie klikt [hier](#).

Dit artikel legt uit hoe te om 802.1x eigenschappen te configureren, die verificatie en de eigenschappen van gast VLAN omvatten. Zie de bovenstaande artikelen voor andere configuraties. Gast VLAN verleent toegang tot services die niet vereisen dat de abonneeapparaten of -poorten worden geauthentiseerd en geautoriseerd via 802.1x of MAC-gebaseerde verificatie.

Toepasselijke apparaten

- SX500 Series Stackable-switches

Softwareversie

- 1.3.0.62

Port-gebaseerde verificatie en training voor VLAN's in 802.1x-eigenschappen inschakelen

Stap 1. Meld u aan bij het web configuratie hulpprogramma om **security > 802.1X > Eigenschappen** te kiezen. De pagina *Eigenschappen* wordt geopend:

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID: 1 ▾

☀ Guest VLAN Timeout: Immediate
 User Defined 36 sec. (Range: 30 - 180)

Apply Cancel

Stap 2. Controleer de optie in het veld Port-gebaseerde verificatie om op poorten gebaseerde 802.1x-verificatie mogelijk te maken.

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID: 1 ▾

☀ Guest VLAN Timeout: Immediate
 User Defined 36 sec. (Range: 30 - 180)

Apply Cancel

Stap 3. Klik het gewenste keuzerondje aan in het veld Verificatiemethode. De RADIUS-server voert de verificatie van de client uit. Deze server bevestigt of de gebruiker al dan niet geauthentiseerd is en waarschuwt de switch of de client toegang tot de LAN en andere switchservices is toegestaan. De switch werkt als een proxy en de server is transparant voor de client.

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID: 1 ▾

☀ Guest VLAN Timeout: Immediate
 User Defined 36 sec. (Range: 30 - 180)

Apply Cancel

- RADIUS, geen — Dit voert eerst de poortverificatie uit met behulp van de RADIUS-server. Als er geen reactie is van de server zoals wanneer de server is ingedrukt, wordt er geen verificatie uitgevoerd en wordt de sessie toegestaan. Als de server beschikbaar is en de gebruikersreferenties niet correct zijn, wordt de toegang geweigerd en wordt de sessie beëindigd.
- RADIUS — Dit voert de poortverificatie uit op basis van de RADIUS-server. Als er geen verificatie wordt uitgevoerd, wordt de sessie beëindigd.
- Geen — hiermee wordt de gebruiker niet gewaarmerkt en wordt de sessie toegestaan.

Stap 4. (Optioneel) Controleer Schakel in om het gebruik van een gastVLAN voor onbevoegde poorten in het veld Guest VLAN in te schakelen. Als een VLAN van de Gast wordt geactiveerd, zullen alle onbevoegde poorten automatisch zich bij het VLAN aansluiten dat in het veld ID van Gast VLAN is geselecteerd. Als een poort later is geautoriseerd, wordt deze verwijderd uit het VLAN van de Gast.

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

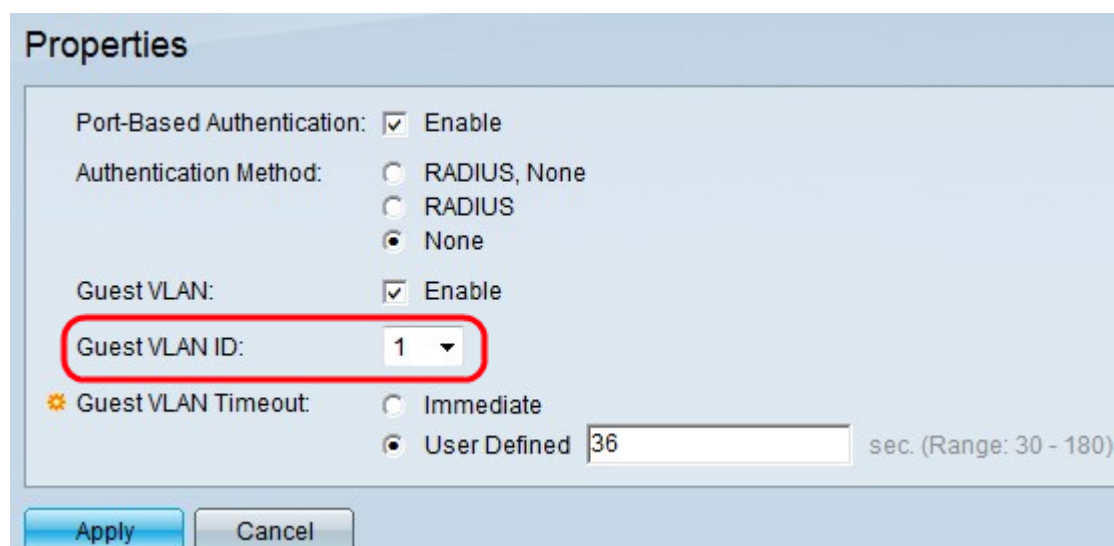
Een West-VLAN-modus moet worden geconfigureerd voordat u de MAC-verificatie-modus kunt gebruiken. Het 802.1x kader stelt een apparaat (de aanvrager) in staat om poorttoegang te vragen van een ver apparaat (authenticator) waarmee het is verbonden. Alleen wanneer de aanvrager die om toegang tot de haven verzoekt, gewaarmerkt en geautoriseerd is, mag hij gegevens naar de haven sturen. Anders gooit de authenticator de leveringsgegevens weg tenzij de gegevens naar een Gast VLAN worden verzonden en/of niet-echt bevonden VLAN's.

Opmerking: Het Guest VLAN is, indien geconfigureerd, een statisch VLAN met de volgende kenmerken:

- Moet handmatig worden gedefinieerd vanuit een bestaand statisch VLAN.
- Is automatisch beschikbaar alleen voor onbevoegde apparaten of poorten van apparaten die zijn aangesloten en Guest-VLAN-enabled.
- Als een poort is geactiveerd Guest-VLAN, voegt de switch automatisch de poort toe als een niet-gelabeld lid van het Guest VLAN wanneer de poort niet is geautoriseerd, en verwijdert u de poort uit het Guest VLAN wanneer de eerste applicatie van de poort is toegestaan.
- Het VLAN van de Gast kan niet als zowel spraak VLAN als niet-echt VLAN worden gebruikt.

Timesaver: Als Guest VLAN is uitgeschakeld, sla dan over naar Stap 7.

Stap 5. Kies de gast VLAN-id uit de lijst met VLAN's in de vervolgkeuzelijst Guest VLAN-id.



Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID: 1

Guest VLAN Timeout: Immediate
 User Defined 36 sec. (Range: 30 - 180)

Apply Cancel

Stap 6. Klik het gewenste keuzerondje aan in het veld Time-out voor Guest VLAN. De beschikbare opties zijn:

- Onmiddellijk — Het gastVLAN verloopt na een periode van 10 seconden.
- Gebruikershandleiding - Voer de tijdsperiode handmatig in in in het veld Gebruikershandleiding.

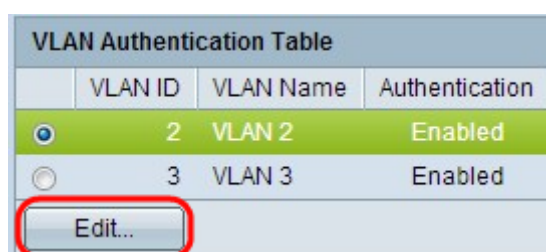
Opmerking: Na verbinding, als de software geen 802.1x smeekbede detecteert of als de poortverificatie heeft gefaald, wordt de poort alleen aan het gastVLAN toegevoegd nadat de Time-outperiode van Gast VLAN is verlopen. Als de poort van Authorized om niet geautoriseerd verandert, wordt de haven aan het VLAN van de Gast toegevoegd slechts nadat de de time-out van West VLAN verstrijkt. De tabel met VLAN-verificatie toont alle VLAN's en toont aan of de verificatie op deze VLAN's is ingeschakeld.

Stap 7. Klik op **Toepassen** om de instellingen op te slaan.

Configuratie onecht VLAN

Wanneer 802.1x wordt geactiveerd, mogen niet-geautoriseerde poorten of apparaten geen toegang tot het VLAN hebben, tenzij ze deel uitmaken van het Gast VLAN of een niet-echt gemaakt VLAN. poorten moeten handmatig aan VLAN's worden toegevoegd met behulp van de *poort op VLAN*-pagina.

Stap 1. Meld u aan bij het programma voor webconfiguratie om **Beveiliging > 802.1X > Eigenschappen** te kiezen. De pagina *Eigenschappen* wordt geopend.



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

Edit...

Stap 2. Scrollt de pagina naar de tabel met VLAN-verificatie, klik op de radioknop van het VLAN waarop u verificatie wilt uitschakelen en klik op **Bewerken**. De pagina *VLAN-verificatie bewerken* wordt geopend.

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

Apply Close

Stap 3. (Optioneel) Kies een VLAN-id in de vervolgkeuzelijst VLAN-id.

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

Apply Close

Stap 4. Schakel de **optie** uit om verificatie uit te schakelen en om het VLAN als niet-echt VLAN uit te schakelen.

Stap 5. Klik op **Toepassen** om de instellingen toe te passen. De wijzigingen worden aangebracht in de VLAN-verificatietabel:

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

Edit..