

Konfiguration von 802.1x-Eigenschaften auf stapelbaren Switches der Serie Sx500

Ziel

IEEE 802.1x ist ein Standard, der die Zugriffskontrolle zwischen Client und Server vereinfacht. Bevor einem Client Services über ein LAN oder einen Switch bereitgestellt werden können, muss der mit dem Switch-Port verbundene Client vom Authentifizierungsserver authentifiziert werden, der in diesem Fall RADIUS (Remote Authentication Dial-In User Service) ausführt. Um die 802.1x-Port-basierte Authentifizierung zu aktivieren, sollte 802.1x global auf dem Switch aktiviert werden.

Um 802.1x vollständig zu konfigurieren, müssen die folgenden Konfigurationen durchgeführt werden:

1. Erstellen Sie ein VLAN, klicken Sie [hier](#).
2. Weisen Sie dem VLAN Port zu, fahren Sie mit dem oben genannten Artikel fort. Klicken Sie [hier](#), um die Konfiguration in der CLI vorzunehmen.
3. Konfigurieren Sie die Portauthentifizierung. Klicken Sie [hier](#).

In diesem Artikel wird erläutert, wie Sie 802.1x-Eigenschaften konfigurieren, die Authentifizierung und Gast-VLAN-Eigenschaften enthalten. Weitere Konfigurationen finden Sie in den obigen Artikeln. Gast-VLAN bietet Zugriff auf Services, für die die Abonnementgeräte oder -ports nicht authentifiziert und über 802.1x- oder MAC-basierte Authentifizierung autorisiert werden müssen.

Anwendbare Geräte

·Stackable Switches der Serie Sx500

Softwareversion

·1.3.0.62

Aktivieren von Port-basierter Authentifizierung und Gast-VLAN in 802.1x-Eigenschaften

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, um **Security > 802.1X > Properties** auszuwählen. Die Seite *Eigenschaften* wird geöffnet:

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

Schritt 2: Aktivieren Sie **Aktivieren** im Feld Port-Based Authentication (Port-basierte Authentifizierung), um die Port-basierte 802.1x-Authentifizierung zu aktivieren.

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

Schritt 3: Klicken Sie im Feld Authentifizierungsmethode auf das gewünschte Optionsfeld. Der RADIUS-Server führt die Authentifizierung des Clients durch. Dieser Server überprüft, ob der Benutzer authentifiziert wird oder nicht, und informiert den Switch darüber, ob dem Client der Zugriff auf das LAN und andere Switch-Services gestattet ist. Der Switch fungiert als Proxy, und der Server ist für den Client transparent.

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, None (RADIUS, Keine): Dies führt zuerst mithilfe des RADIUS-Servers die Port-Authentifizierung durch. Wenn der Server nicht reagiert, z. B. wenn der Server ausgefallen ist, wird keine Authentifizierung durchgeführt, und die Sitzung ist zulässig. Wenn der Server verfügbar ist und die Anmeldeinformationen des Benutzers falsch sind, wird der Zugriff verweigert und die Sitzung beendet.

·RADIUS (RADIUS) - Diese Funktion führt die Port-Authentifizierung auf Basis des RADIUS-Servers aus. Wenn keine Authentifizierung durchgeführt wird, wird die Sitzung beendet.

·Keine: Der Benutzer wird nicht authentifiziert, und die Sitzung wird zugelassen.

Schritt 4: (Optional) Aktivieren Sie **Aktivieren**, um die Verwendung eines Gast-VLAN für nicht autorisierte Ports im Feld Gast-VLAN zu aktivieren. Wenn ein Gast-VLAN aktiviert ist, werden alle nicht autorisierten Ports automatisch dem im Feld Gast-VLAN-ID ausgewählten VLAN hinzugefügt. Wenn ein Port später autorisiert wird, wird er aus dem Gast-VLAN entfernt.

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

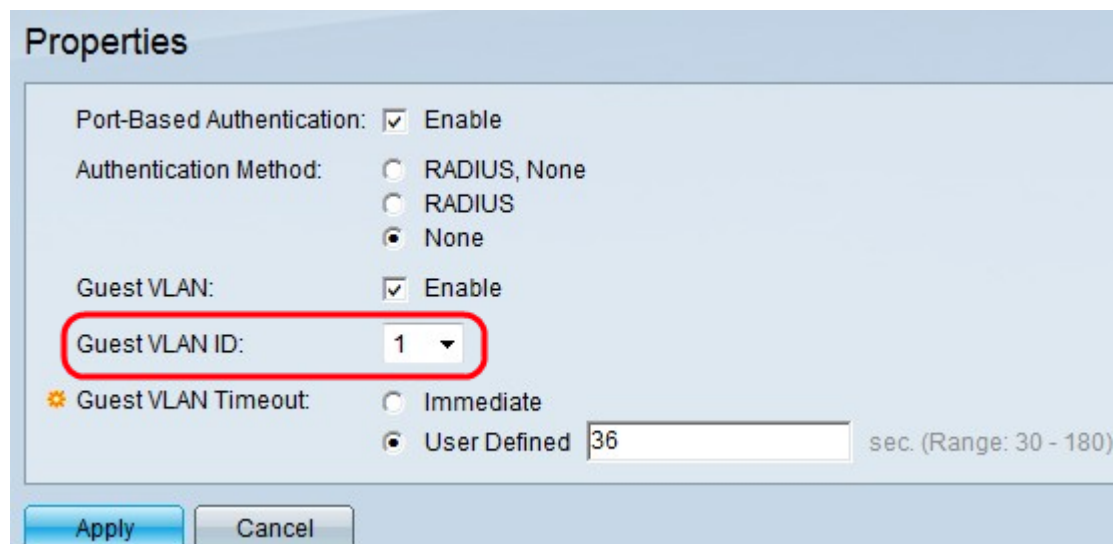
Bevor Sie den MAC-Authentifizierungsmodus verwenden können, muss ein Gast-VLAN-Modus konfiguriert werden. Das 802.1x-Framework ermöglicht es einem Gerät (dem Supplicant), Port-Zugriff von einem Remote-Gerät (Authentifizierer) anzufordern, mit dem es verbunden ist. Nur wenn der Supplicant, der den Port-Zugriff anfordert, authentifiziert und autorisiert ist, darf er Daten an den Port senden. Andernfalls verwirft der Authentifizierer die Zusatzdaten, es sei denn, die Daten werden an ein Gast-VLAN und/oder nicht authentifizierte VLANs gesendet.

Hinweis: Das Gast-VLAN ist, sofern konfiguriert, ein statisches VLAN mit den folgenden Eigenschaften:

- Muss manuell aus einem vorhandenen statischen VLAN definiert werden.
- Ist automatisch nur für nicht autorisierte Geräte oder Ports von Geräten verfügbar, die angeschlossen sind und das Gast-VLAN aktivieren.
- Wenn ein Port Gast-VLAN-aktiviert ist, fügt der Switch den Port automatisch als nicht markiertes Mitglied des Gast-VLAN hinzu, wenn der Port nicht autorisiert ist, und entfernt den Port aus dem Gast-VLAN, wenn die erste Komponente des Ports autorisiert ist.
- Das Gast-VLAN kann nicht sowohl als Sprach-VLAN als auch als nicht authentifiziertes VLAN verwendet werden.

Timesaver: Wenn das Gast-VLAN deaktiviert ist, fahren Sie mit Schritt 7 fort.

Schritt 5: Wählen Sie die Gast-VLAN-ID aus der Liste der VLANs in der Dropdown-Liste Guest VLAN ID (Gast-VLAN-ID) aus.



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

Schritt 6: Klicken Sie im Feld Guest VLAN Timeout auf das gewünschte Optionsfeld. Folgende Optionen stehen zur Verfügung:

- Immediate (Sofort): Das Gast-VLAN läuft nach einem Zeitraum von 10 Sekunden ab.
- Benutzerdefiniert - Geben Sie den Zeitraum manuell im Feld Benutzerdefiniert ein.

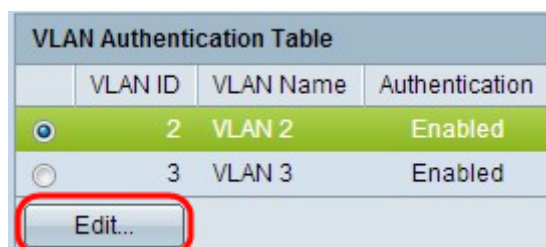
Hinweis: Wenn die Software nach dem Verbindungsaufbau keine 802.1x-Komponente erkennt oder die Port-Authentifizierung fehlgeschlagen ist, wird der Port dem Gast-VLAN erst nach Ablauf der Gast-VLAN-Zeitüberschreitungsfrist hinzugefügt. Wenn sich der Port von Authorized (Autorisiert) zu Not Authorized (Nicht autorisiert) ändert, wird der Port dem Gast-VLAN erst nach Ablauf der Timeout-Zeit für das Gast-VLAN hinzugefügt. Die VLAN-Authentifizierungstabelle zeigt alle VLANs und ob die Authentifizierung für diese aktiviert ist.

Schritt 7: Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Nicht authentifizierte VLAN-Konfiguration

Wenn 802.1x aktiviert ist, dürfen nicht autorisierte Ports oder Geräte nur dann auf das VLAN zugreifen, wenn sie Teil des Gast-VLAN oder eines nicht authentifzierten VLAN sind. Ports müssen VLANs mithilfe der Seite *Port to VLAN* manuell hinzugefügt werden.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, um **Security > 802.1X > Properties** auszuwählen. Die Seite *Eigenschaften* wird geöffnet.



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

Edit..

Schritt 2: Blättern Sie auf der Seite nach unten zur Tabelle für die VLAN-Authentifizierung, klicken Sie auf das Optionsfeld des VLAN, für das Sie die Authentifizierung deaktivieren möchten, und klicken Sie auf **Bearbeiten**. Die Seite *VLAN-Authentifizierung bearbeiten* wird geöffnet.

VLAN ID: 2 ▾
VLAN Name: VLAN 2
Authentication: Enable
Apply Close

Schritt 3: (Optional) Wählen Sie in der Dropdown-Liste VLAN ID (VLAN-ID) eine VLAN-ID aus.

VLAN ID: 2 ▾
VLAN Name: VLAN 2
Authentication: Enable
Apply Close

Schritt 4: Deaktivieren Sie **Enable**, um die Authentifizierung zu deaktivieren und das VLAN als nicht authentifiziertes VLAN einzurichten.

Schritt 5: Klicken Sie auf **Übernehmen**, um die Einstellungen zu übernehmen. Änderungen werden an der VLAN-Authentifizierungstabelle vorgenommen:

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

Edit..