Konfiguration der 802.1X-Eigenschaften auf den Managed Switches der Serien 200 und 300

Ziel

Die Seite *Properties* des 802.1X IEEE-Standards im Abschnitt Security der Managed Switches der Serien 200 und 300 bietet verschiedene Authentifizierungsoptionen. Der 802.1X IEEE-Standard ermöglicht die portbasierte Authentifizierung von Benutzern. Ein Benutzer in einem bestimmten Netzwerk, in dem 802.1X aktiviert ist, muss auf die vollständige Authentifizierung warten, um Daten über das Netzwerk zu senden. Sie können 802.1X aktivieren und die Authentifizierungsmethode für Ports festlegen. In diesem Artikel wird erläutert, wie Sie die 802.1X-Eigenschaften der Managed Switches der Serien 200 und 300 konfigurieren.

Unterstützte Geräte

ã*ƒ*» Managed Switches der Serien SF/SG 200 und SF/SG 300

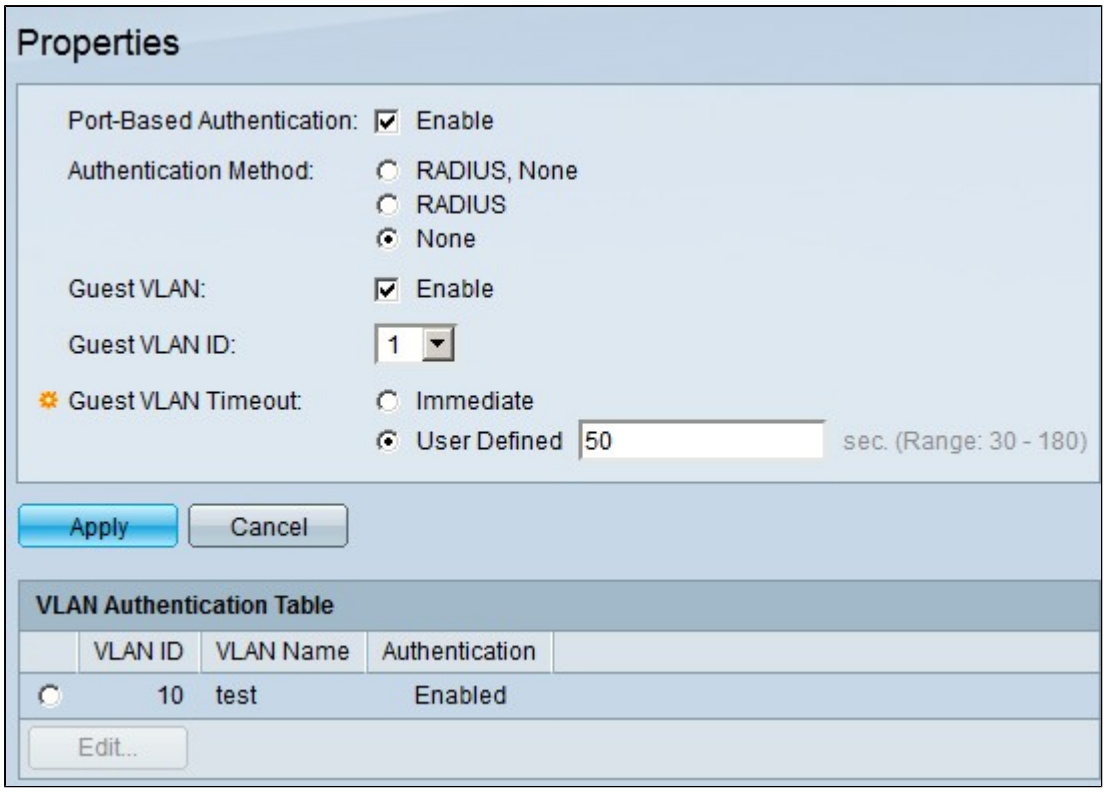
Software-Version

â€¢3.1.0.62

Konfiguration der 802.1x-Eigenschaften

Parameter für 802.1X-Eigenschaften definieren

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



Schritt 2: Um eine portbasierte 802.1x-Authentifizierung zu aktivieren, aktivieren Sie im Feld "Port-Based Authentication" das Kontrollkästchen **Enable**.

Schritt 3: Klicken Sie im Feld Authentifizierungsmethode auf das Optionsfeld für die gewünschte Authentifizierungsmethode. Folgende Optionen sind verfügbar:

ãƒ» RADIUS, None - Erstmalige Authentifizierung über RADIUS-Server. Wenn der RADIUS-Server nicht reagiert, werden die verbundenen Geräte ohne Authentifizierung zugelassen.

ãƒ» RADIUS - Authentifizierung von Benutzern nur über einen RADIUS-Server. Wenn der RADIUS-Server nicht reagiert, werden die Dienste von Benutzern abgelehnt.

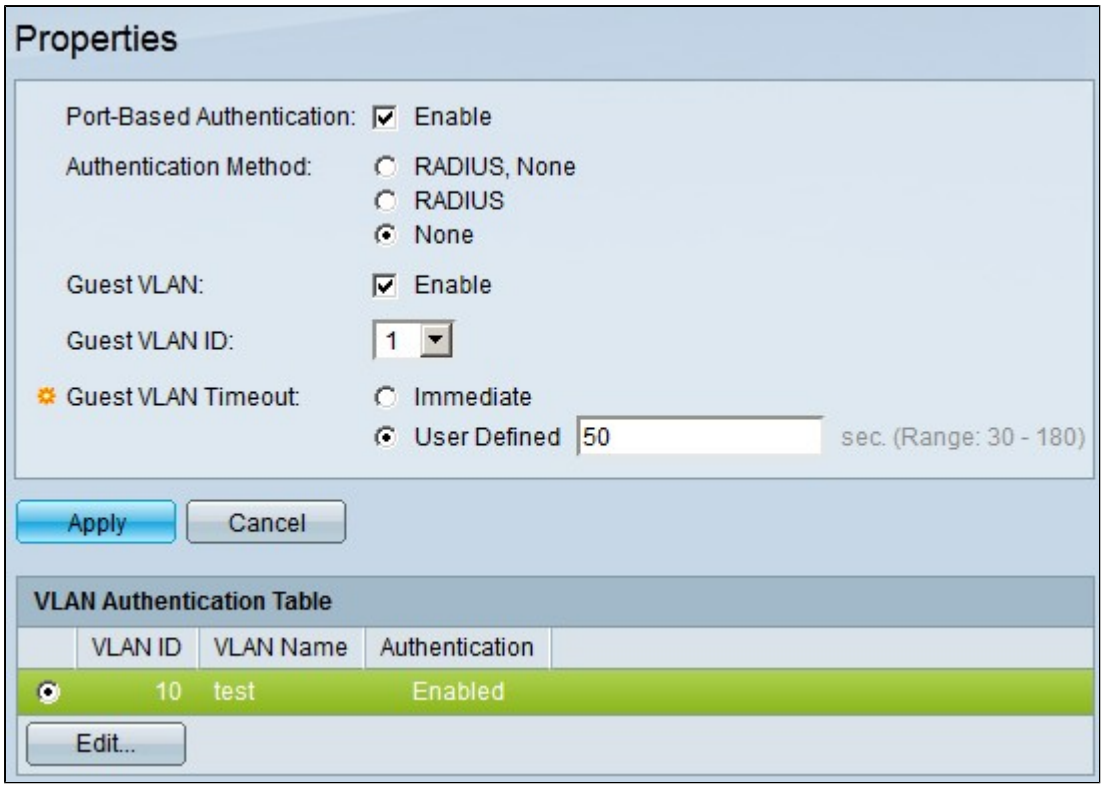
ãƒ» Keine â€" Keine Authentifizierung für Benutzer erforderlich, alle Benutzer sind erlaubt.

Schritt 3: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

Nicht authentifizierte VLAN-Konfiguration

Ein nicht autorisierter Port kann nur dann auf ein VLAN zugreifen, wenn es sich bei diesem VLAN um das Gast-VLAN handelt. Sie können diese VLANs authentifizieren. In diesem Abschnitt wird erläutert, wie Sie VLANs auf den Managed Switches der Serien 200 und 300 authentifizieren.

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



Schritt 2: Klicken Sie in der VLAN Authentication Table auf das Optionsfeld des VLAN, das Sie für die Authentifizierung aktivieren möchten.

Schritt 3: Klicken Sie auf **Bearbeiten**. Das Fenster *Bearbeiten* wird angezeigt:

Schritt 4: Aktivieren Sie im Authentifizierungsfeld das Kontrollkästchen **Aktivieren**, um die Authentifizierung für das ausgewählte VLAN zu aktivieren.

Schritt 5: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.