

Configuration des propriétés 802.1x sur les commutateurs empilables de la gamme Sx500

Objectif

IEEE 802.1x est une norme qui facilite le contrôle d'accès entre un client et un serveur. Pour que les services puissent être fournis à un client par un réseau local ou un commutateur, le client connecté au port du commutateur doit être authentifié par le serveur d'authentification qui exécute le service RADIUS (Remote Authentication Dial-In User Service) dans ce cas. Pour activer l'authentification 802.1x basée sur les ports, 802.1x doit être activé globalement sur le commutateur.

Pour configurer entièrement 802.1x, vous devez effectuer les configurations suivantes :

1. Créez un VLAN, cliquez [ici](#).
2. Attribuez le port au VLAN, continuez l'article mentionné ci-dessus. Pour configurer dans l'interface de ligne de commande, cliquez [ici](#).
3. Configurez l'authentification de port, cliquez [ici](#).

Cet article explique comment configurer les propriétés 802.1x, qui incluent l'authentification et les propriétés VLAN invité. Reportez-vous aux articles ci-dessus pour d'autres configurations. Le VLAN invité fournit un accès aux services qui ne nécessitent pas que les périphériques ou ports d'abonnement soient authentifiés et autorisés via l'authentification 802.1x ou MAC.

Périphériques pertinents

Commutateurs Empilables · Sx500

Version du logiciel

•1.3.0.62

Activer l'authentification basée sur les ports et le VLAN invité dans les propriétés 802.1x

Étape 1. Connectez-vous à l'utilitaire de configuration Web pour sélectionner **Security > 802.1X > Properties**. La page *Propriétés* s'ouvre :

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

Étape 2. Cochez **Enable** dans le champ Port-Based Authentication pour activer l'authentification 802.1x basée sur les ports.

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

Étape 3. Sélectionnez la case d'option souhaitée dans le champ Authentication Method. Le serveur RADIUS effectue l'authentification du client. Ce serveur vérifie si l'utilisateur est authentifié ou non et indique au commutateur si le client est autorisé ou non à accéder au réseau local et aux autres services du commutateur. Le commutateur agit comme un proxy et le serveur est transparent pour le 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)

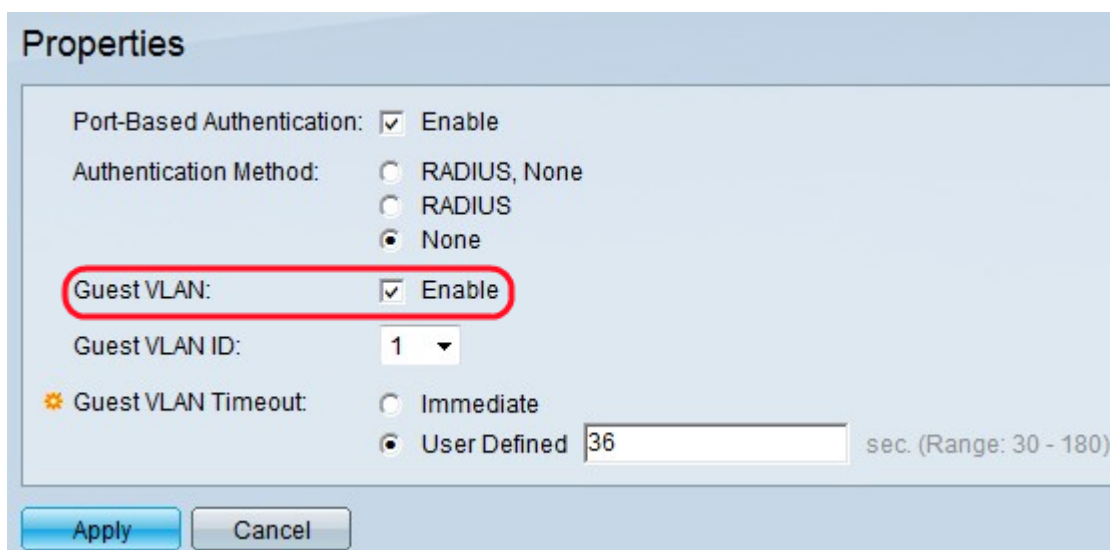
Apply Cancel

·RADIUS, None : cette opération effectuée d'abord l'authentification du port à l'aide du serveur RADIUS. Si le serveur ne répond pas, par exemple lorsque le serveur est en panne, aucune authentification n'est effectuée et la session est autorisée. Si le serveur est disponible et que les informations d'identification de l'utilisateur sont incorrectes, l'accès est refusé et la session est terminée.

·RADIUS : effectuée l'authentification du port en fonction du serveur RADIUS. Si aucune authentification n'est effectuée, la session est interrompue.

·Aucun : ne authentifie pas l'utilisateur et autorise la session.

Étape 4. (Facultatif) Cochez **Enable** pour activer l'utilisation d'un VLAN invité pour les ports non autorisés dans le champ Guest VLAN. Si un VLAN invité est activé, tous les ports non autorisés se joignent automatiquement au VLAN sélectionné dans le champ Guest VLAN ID. Si un port est autorisé ultérieurement, il est supprimé du VLAN invité.



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

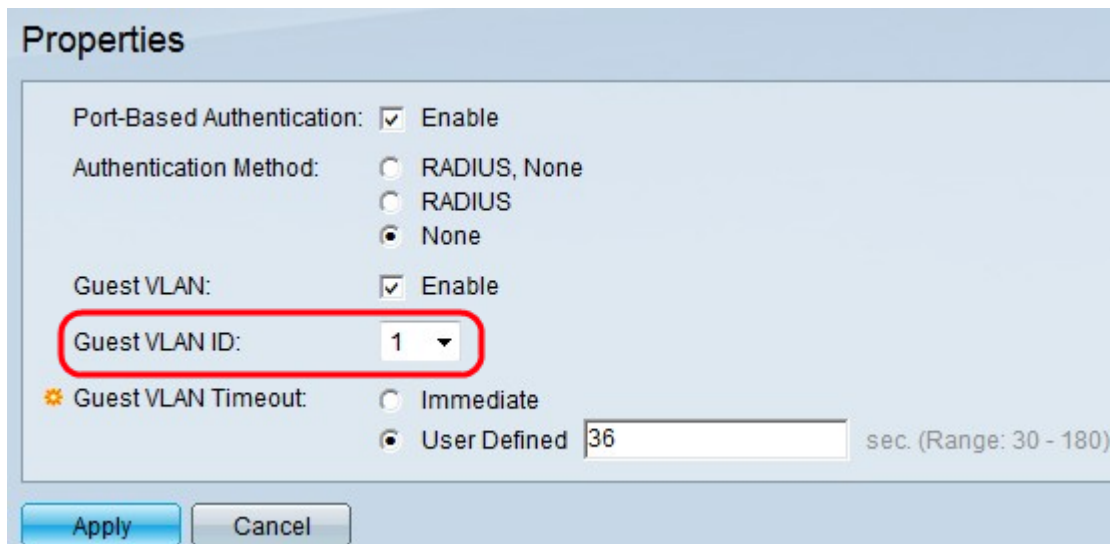
Un mode VLAN invité doit être configuré avant de pouvoir utiliser le mode d'authentification MAC. La structure 802.1x permet à un périphérique (le demandeur) de demander l'accès au port à partir d'un périphérique distant (authentificateur) auquel il est connecté. Ce n'est que lorsque le demandeur qui demande l'accès au port est authentifié et autorisé qu'il est autorisé à envoyer des données au port. Sinon, l'authentificateur rejette les données du demandeur à moins que les données ne soient envoyées à un VLAN invité et/ou à des VLAN non authentifiés.

Note: Le VLAN invité, s'il est configuré, est un VLAN statique présentant les caractéristiques suivantes :

- Doit être défini manuellement à partir d'un VLAN statique existant.
- est automatiquement disponible uniquement pour les périphériques ou ports non autorisés des périphériques connectés et activés par le VLAN invité.
- Si un port est activé par le VLAN invité, le commutateur ajoute automatiquement le port en tant que membre non balisé du VLAN invité lorsque le port n'est pas autorisé et supprime le port du VLAN invité lorsque le premier demandeur du port est autorisé.
- Le VLAN invité ne peut pas être utilisé à la fois comme VLAN voix et comme VLAN non authentifié.

Économie de temps : si le VLAN invité est désactivé, passez à l'étape 7.

Étape 5. Sélectionnez l'ID de VLAN invité dans la liste déroulante ID de VLAN invité.



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)

Étape 6. Cliquez sur la case d'option souhaitée dans le champ Guest VLAN Timeout. Les options disponibles sont les suivantes :

- Immédiat : le VLAN invité expire après une période de 10 secondes.
- défini par l'utilisateur : saisissez la période manuellement dans le champ défini par l'utilisateur.

Note: Après la liaison, si le logiciel ne détecte pas un demandeur 802.1x ou si l'authentification du port a échoué, le port est ajouté au VLAN invité uniquement après l'expiration du délai d'expiration du VLAN invité. Si le port passe de Authorized à Not Authorized, le port est ajouté au VLAN invité uniquement après l'expiration du délai d'expiration du VLAN invité. La table d'authentification VLAN affiche tous les VLAN et indique si l'authentification est activée sur eux ou non.

Étape 7. Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration VLAN non authentifiée

Lorsque 802.1x est activé, les ports ou périphériques non autorisés ne sont pas autorisés à accéder au VLAN, sauf s'ils font partie du VLAN invité ou d'un VLAN non authentifié. Les ports doivent être ajoutés manuellement aux VLAN à l'aide de la page *Port to VLAN*.

Étape 1. Connectez-vous à l'utilitaire de configuration Web pour sélectionner **Security > 802.1X > Properties**. La page *Propriétés* s'affiche.

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

Étape 2. Faites défiler la page jusqu'à la table d'authentification VLAN, cliquez sur la case d'option du VLAN sur lequel vous voulez désactiver l'authentification, puis cliquez sur **Modifier**. La page *Edit VLAN Authentication* s'affiche.

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

Apply Close

Étape 3. (Facultatif) Choisissez un ID de VLAN dans la liste déroulante ID de VLAN.

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

Apply Close

Étape 4. Décochez **Enable** pour désactiver l'authentification et faire du VLAN un VLAN non authentifié.

Étape 5. Cliquez sur **Apply** pour appliquer les paramètres. Les modifications sont apportées à la table d'authentification 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..