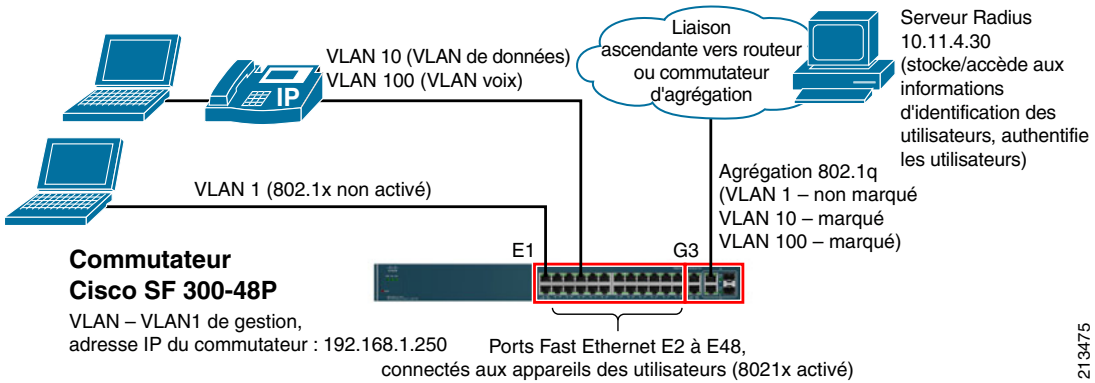

# Accès réseau authentifié et basé sur l'heure avec l'authentification 802.1x

802.1x est une norme IEEE pour le contrôle d'accès à un réseau au niveau de chaque port. Les commutateurs de la gamme Cisco Small Business 300 prennent en charge la norme 802.1x pour garantir une meilleure sécurité du réseau. Dans un réseau compatible 802.1x, un appareil d'utilisateur tel qu'un ordinateur portable ou un téléphone IP demande à son commutateur directement connecté l'acccès à un port. Le commutateur obtient l'identifiant et le mot de passe de l'utilisateur (ou de l'appareil) et les transfère à un serveur RADIUS pour authentification. Le commutateur autorise l'accès au port uniquement si l'authentification de l'utilisateur réussit. Un tel accès authentifié à un réseau local améliore la sécurité du réseau.

# Produits proposés

Ce document décrit l'utilisation de l'authentification 802.1x sur un commutateur administrable de la gamme Cisco Small Business 300 (modèle SF300-48P) avec divers ports PoE (Power over Ethernet) et non-PoE. Pour plus de détails sur d'autres commutateurs administrables de la gamme Cisco 300, visitez : http://www.cisco.com/go/300switches.

**Figure 1 Accès réseau authentifié à l'aide de l'authentification 802.1x**




# Conception réseau 802.1x

Les principaux composants d'un réseau utilisant l'authentification 802.1x, tel qu'illustré dans la Figure 1, sont indiqués ci-dessous :

- Ordinateurs portables/téléphones IP (ou autres appareils d'utilisateur final similaires pouvant demander un accès 802.1x à un réseau)
- Un commutateur qui authentifie l'utilisateur à l'aide d'un serveur RADIUS et qui permet l'accès au réseau uniquement lorsque l'authentification aboutit.
- Un serveur RADIUS pour authentifier l'utilisateur.

Lorsque l'authentification 802.1x est activée sur un réseau local, elle est généralement activée sur tous les ports du commutateur destinés à être connectés à des appareils d'utilisateur final ou autres appareils nécessitant un tel accès authentifié aux ports.

# Authentification

Pour authentifier un utilisateur, le serveur RADIUS accède à une base de données d'utilisateurs qui contient des informations telles que l'identifiant et le mot de passe des utilisateurs, et autres informations en option qu'il fournit au commutateur lorsque l'authentification réussit. La base de données peut être intégrée dans le serveur RADIUS ou être une base externe, par exemple une base Active Directory.

## Quels ports convient-il d'authentifier ?

L'authentification 802.1x est principalement destinée aux appareils d'utilisateurs finaux tels que des ordinateurs portables ou des téléphones IP qui sont des appareils non approuvés du point de vue de la sécurité. Par conséquent, l'authentification 802.1x n'est pas configurée sur les ports connectés à des équipements réseau tels que des routeurs, des commutateurs ou des serveurs, ou de tels équipements approuvés. Elles est configurée sur les ports destinés à la connexion d'appareils d'utilisateurs sur un commutateur d'accès, et également sur un commutateur d'agrégation si des appareils d'utilisateurs peuvent lui être connectés directement.

## Politique d'authentification par port

Le port du commutateur Cisco Small Business 300 peut être configuré avec l'une des trois politiques suivantes qui déterminent comment l'authentification 802.1x affecte l'accès au port lorsque plusieurs appareils peuvent être potentiellement connectés à un port unique :

- Unique - permet à un seul hôte autorisé d'accéder au port.
- Hôtes multiples (802.1x) - le port prend en charge plusieurs hôtes. Seul le premier hôte doit faire l'objet d'une autorisation 802.1x. Si l'autorisation réussit, non seulement l'appareil authentifié peut accéder au port, mais tous les autres appareils connectés peuvent y accéder sans autre authentification. Tant qu'au moins un appareil connecté n'a pas été authentifié, aucun appareil ne peut accéder au port. Cela est utile pour le déploiement d'appareils qui ne prennent pas en charge l'authentification 802.1x.
- Sessions multiples - permet à plusieurs hôtes d'accéder au port, mais chacun doit être individuellement et séparément authentifié.

**Remarque** La politique à sessions multiples est recommandée dans les guides Cisco SMART Designs pour garantir plus de souplesse et une meilleure sécurité. La politique à hôtes multiples peut être utilisée pour prendre en charge les appareils sur un port qui ne prend pas en charge l'authentification 802.1 x.

**Remarque** Le commutateur de la gamme Cisco Small Business 300 peut être configuré pour placer un utilisateur dans le VLAN Invité lorsque l'authentification 802.1x échoue pour l'utilisateur.

## Précisions sur le serveur RADIUS

Le commutateur de la gamme Cisco Small Business 300 accède au serveur RADIUS sur le VLAN de gestion, en utilisant l'adresse IP de gestion spécifique affectée au commutateur (en tant que commutateur compatible de couche 3, le commutateur peut également prendre en charge plusieurs interfaces IP). Cela implique que le commutateur puisse utiliser son VLAN de gestion pour atteindre le serveur RADIUS. Si le serveur RADIUS se trouve sur un autre VLAN (comme dans la Figure 1), le routeur WAN effectue généralement le routage inter-VLAN nécessaire.

Le routeur WAN termine le VLAN de gestion. Si le VLAN de gestion par défaut (VLAN 1) est employé, les commutateurs du réseau local doivent être configurés pour acheminer le VLAN 1 non marqué avec les éventuels autres VLAN par leurs ports d'agrégation au routeur WAN.

## Authentification des téléphones IP

À l'instar des PC et des ordinateurs portables, les téléphones IP peuvent aussi faire l'objet d'une authentification 802.1x. Les téléphones IP Cisco sont compatibles 802.1x. Pour plus de détails sur l'activation de l'authentification 802.1x sur le téléphone IP et pour créer un identifiant d'utilisateur approprié pour le téléphone IP dans le serveur RADIUS, consultez le guide de l'administrateur du téléphone IP spécifique.

## Authentification basée sur l'heure

Le commutateur de la gamme Cisco Small Business 300 permet de restreindre l'accès aux ports 802.1x à un intervalle de temps spécifié correspondant à un intervalle de temps absolu tel que 9 h 00, 22 février, 2010 à 17 h 00, 30 avril, 2023. Dans ce cas, les utilisateurs bénéficient d'un accès authentifié à toute heure pendant la période spécifiée. En dehors de cette période, les ports sont dans un état d'« interdiction forcée », ce qui signifie qu'ils ne sont pas accessibles et qu'aucune authentification 802.1x n'est initialisée.

Après avoir défini un intervalle de temps absolu, vous pouvez facultativement lui adjoindre un intervalle de temps récurrent. Un intervalle de temps récurrent définit une restriction d'accès supplémentaire avec une heure de début et une heure de fin spécifiques de chaque jour de la semaine (vous pouvez définir des périodes distinctes pour chaque jour de la semaine).

Les ports peuvent être affectés à différents intervalles de temps. Cette possibilité peut être pratique si les heures ouvrables (où les heures d'accès au réseau) des employés sont variables.

## Affectation de VLAN dynamique

L'affectation de VLAN dynamique (DVA, Dynamic VLAN Assignment) affecte dynamiquement un VLAN spécifique d'un utilisateur à un port après une authentification 802.1x réussie. Le VLAN correspondant à l'utilisateur doit être défini dans le profil RADIUS de l'utilisateur. Lorsque l'utilisateur est authentifié, le serveur RADIUS fournit les informations VLAN de l'utilisateur au commutateur dans le cadre de la procédure d'authentification. Le commutateur ajoute ensuite le port en tant que membre non marqué de ce VLAN. Cela favorise la mobilité des utilisateurs lorsque différents utilisateurs appartiennent à des VLAN de données distincts en fonction de leurs services, ou d'autres critères.

Bien que le commutateur de la gamme Cisco Small Business série 300 prenne en charge DVA, ce document ne couvre pas la configuration de cette fonction. Pour plus d'informations, consultez le guide d'administration à l'adresse URL suivante : http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf.

# Conseils de configuration

Cette section fournit un exemple de configuration de l'authentification 802.1x pour un commutateur de la gamme Cisco Small Business série 300. Plus spécifiquement, l'exemple configure les ports Fast Ethernet e2 à e48 d'un commutateur Cisco SF 300-48P pour activer un accès authentifié aux ports à l'aide de 802.1x.

Cette section se réfère à la configuration d'un commutateur d'accès dans une topologie Cisco SMART Design telle qu'illustrée dans la Figure 1.

## Conditions prérequises du réseau pour cette configuration

### Conditions prérequises du réseau local

1. Tous les ports d'un commutateur de la gamme Cisco Small Business série 300 sont associés au VLAN 1 natif par défaut. En pratique, il est souvent nécessaire de créer d'autres VLAN séparés pour les données et la voix. Cet exemple de configuration utilise VLAN 10 comme VLAN de données et VLAN 100 comme VLAN voix.

   Par exemple, un port unique (e1) est affecté à VLAN 1 et est destiné à être utilisé comme port de gestion dédié. Cependant, notez que dans la pratique, VLAN 10 (VLAN de données) peut également être utilisé comme VLAN de gestion. En outre, l'utilisation de ports de gestion dédiés est facultative.
2. Tous ces VLAN (VLAN 10, 100 et 1) se terminent sur le routeur WAN.
3. Le commutateur de la gamme Cisco série 300 peut configurer un port de trois manières :
   - Port d'accès - le port peut être associé à un VLAN spécifique, le PVID (Port VLAN ID, identifiant de VLAN de port). Un port d'accès place tous les paquets entrants par le port dans le PVID. Il ne peut prendre en charge qu'un seul VLAN, et n'est donc pas adapté si des VLAN voix et de données séparés sont employés.
   - Port d'agrégation - le port peut prendre en charge un PVID spécifique et un ou plusieurs VLAN 802.1q encapsulés (marqués) . Comme illustré dans le Tableau 1, cette conception utilise des ports d'agrégation.
   - Port général - ce type de port peut prendre en charge plusieurs VLAN non marqués et marqués, où le trafic non marqué est placé dans des VLAN en fonction des adresses MAC source.

Cette configuration part du principe que le commutateur d'accès est configuré de la manière indiquée dans le Tableau 1. Les numéros et ports VLAN réels utilisés peuvent varier dans un déploiement en fonction de conditions spécifiques (voir la Figure 1).

**Tableau 1 Configurations des ports pour cet exemple**

| | N° de port | Type de port | Port VLAN (PVID) | VLAN marqués | VLAN exclus |
|---|---|---|---|---|---|
| Interface de gestion de commutateur spécifique, (en option) | e1 | Agrégation | VLAN 1 | | 10, 100 |
| Ports connectés aux ordinateurs portables/téléphones IP des utilisateurs | e2 à e48 | Agrégation | VLAN 10 (VLAN de données) | VLAN 100 (VLAN voix) | 1 |
| Port en amont | G3 (aussi G1, G2, G4) | Agrégation | VLAN 1 | VLAN 10, 100 | 1 |

4. Le protocole RSTP (Rapid Spanning Tree Protocol) est activé sur le commutateur, et celui-ci peut acheminer du trafic sur le réseau local en utilisant ses VLAN.

### Configuration d'un commutateur d'agrégation

Cette configuration part du principe que le commutateur d'agrégation est configuré de la manière indiquée dans le Tableau 2.

**Tableau 2 Configuration d'un commutateur d'agrégation**

| | Port raccordé au commutateur de la gamme Cisco série 300 | Port raccordé au routeur WAN |
|---|---|---|
| VLAN 1 | Non marqué (PVID) | Non marqué (PVID) |
| VLAN 10 | Marqué | Marqué |
| VLAN 100 | Marqué | Marqué |

**Remarque** Spécifiquement, vérifiez que le commutateur d'agrégation est configuré pour acheminer le VLAN 1 non marqué (par exemple, si un commutateur Cisco Catalyst est employé, le VLAN non marqué doit être inclus dans les VLAN devant être autorisés par le port d'agrégation au moyen d'une commande telle que **switchport trunk allowed vlan 1,10,100**).

## Configuration requise du routeur WAN

Cette documentation part du principe que le routeur WAN termine les VLAN de la manière indiquée dans le Tableau 3.

**Tableau 3 Terminaison VLAN du routeur WAN**

| | Port du routeur raccordé au commutateur de la gamme Cisco série 300 | |
|---|---|---|
| | Type d'interface VLAN | Adresse IP (passerelle par défaut pour le sous-réseau) |
| VLAN 1 | VLAN natif (non marqué) | 192.168.1.1 |
| VLAN 10 | Marqué | 10.1.20.1 |
| VLAN 100 | Marqué | 10.1.100.1 |

## Configuration requise du serveur RADIUS

1. Vérifiez que le serveur RADIUS est configuré pour accepter les demandes d'authentification RADIUS pour le commutateur spécifique ; c'est-à-dire que l'adresse IP et la clé d'authenrification (mot de passe partagé) du commutateur sont spécifiées dans le serveur RADIUS. Les informations suivantes doivent donc être configurées sur le serveur RADIUS :
   - Les ports UDP utilisés par le serveur RADIUS pour écouter les demandes d'authentification RADIUS et les autorisations RADIUS ; généralement, ce sont 1812/1813 ou 1645/1646. Ils doivent correspondre entre le serveur RADIUS et tous les commutateurs compatibles 802.1x.
   - Adresse IP du serveur d'accès réseau (NAS). Un NAS est le client qui envoie des demandes d'authentification RADIUS au serveur RADIUS. Dans ce cas, le commutateur envoie les demandes d'authentification des utilisateurs au serveur RADIUS, et est donc le NAS. Par conséquent, le serveur RADIUS doit être configuré avec l'adresse IP de chaque commutateur qui effectue des authentifications 802.1x dans le réseau.
   - Clé d'authentification - chaîne alphanumérique utilisée par le serveur RADIUS pour authentifier le NAS spécifique. La même clé d'authentification doit également être configurée dans le commutateur correspondant lors de la configuration du commutateur (voir ci-dessous).
2. Vérifiez que le commutateur peut atteindre (requête ping) le serveur RADIUS. Le commutateur dialogue avec le serveur RADIUS sur le VLAN de gestion (VLAN 1, dans cet exemple) en utilisant l'adresse IP de gestion comme adresse IP source.
3. Vérifiez que le serveur RADIUS contient au moins un profil d'utilisateur (identifiant d'utilisateur et mot de passe) à des fins de test (d'autres utilisateurs peuvent être ajoutés ultérieurement). Généralement, les informations minimales configurées pour un utilisateur sur un serveur RADIUS tel que Cisco ACS sont les suivantes :
   - Identifiant d'utilisateur
   - Groupe d'utilisateurs - groupes créés par un administrateur et incluant des employés, des administrateurs de réseau, des gestionnaires, le personnel comptable, etc.
   - Mot de passe d'utilisateur
   - Le type d'authentification (PAP/CHAP, etc.) associé au groupe d'utilisateurs
   - La liste d'attributs RADIUS (dictionnaire RADIUS) prise en charge par le groupe d'utilisateurs, si plusieurs listes sont prises en charge par le serveur RADIUS

**Remarque** Les champs requis par le profil d'utilisateur peuvent varier selon le serveur RADIUS. En option, un groupe d'utilisateurs dans un serveur RADIUS peut être configuré avec des informations supplémentaires utilisées lors de l'établissement de la connexion de l'utilisateur. Par exemple, le groupe d'utilisateurs peut spécifier un VLAN à utiliser comme PVID du port du commutateur, après authentification de l'utilisateur.

# Configuration du commutateur pour l'utilisation d'un serveur RADIUS

Cette configuration active une authentification RADIUS sur le commutateur et configure l'authentification 802.1x sur les ports e2 à e48 du commutateur.

Lors de la configuration du commutateur, enregistrez la configuration fréquemment dans le fichier de configuration de démarrage, car les configurations non enregistrées sont perdues lors du redémarrage du commutateur. Pour enregistrer la configuration, procédez comme suit :

Étape 1 Sélectionnez **Administration > File Management (Gestion de fichiers) > Copy/Save Configuration (Copier/Enregistrer la configuration)**.

La page Copy/Save Configuration (Copier/Enregistrer la configuration) s'ouvre.

Étape 2 Sélectionnez le nom du fichier source (Source File Name) à copier comme *Running configuration (Configuration active)*.

Étape 3 Sélectionnez le nom de fichier de destination (Destination File Name) comme *Startup configuration (Configuration de démarrage)*.

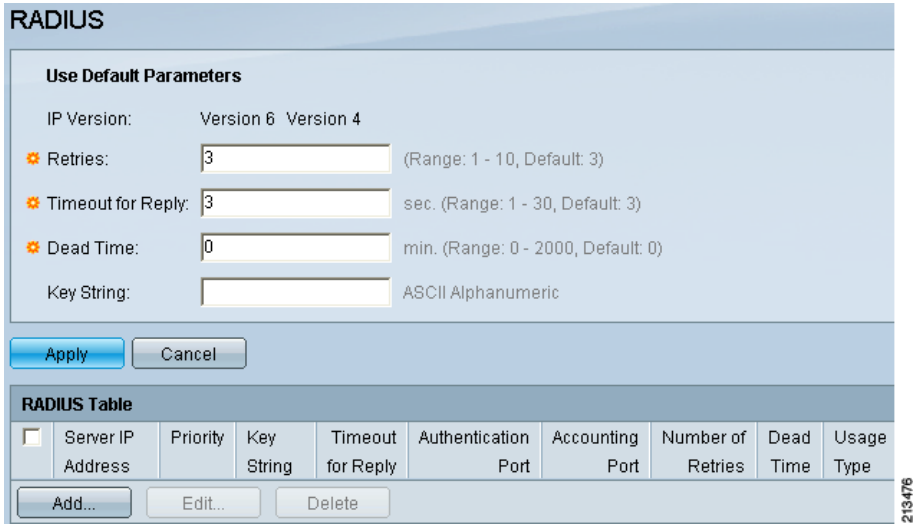
Étape 4 Cliquez sur **Apply (appliquer)**. Le fichier de configuration est alors enregistré.

Pour configurer le commutateur de manière à utiliser un serveur RADIUS, procédez comme suit.

Étape 1 **Étape 1** Sélectionnez **Security (sécurité) > RADIUS**.

L'écran RADIUS (Figure 2) s'affiche.

**Figure 2 Écran RADIUS**

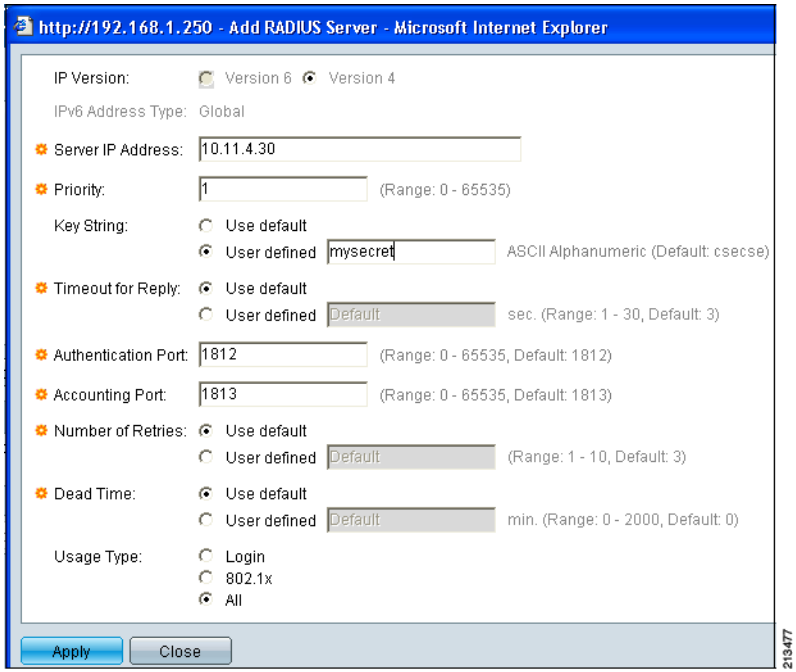



Cette étape spécifie les détails du serveur RADIUS (adresse IP et clé d'authentification) au commutateur, afin que ce dernier puisse communiquer avec ce serveur. Vérifiez que les informations détaillées du serveur RADIUS ne sont pas déjà configurées sur le commutateur, c'est-à-dire qu'aucun détail du serveur RADIUS n'apparaît sous le tableau RADIUS (si elles sont déjà configurées, vous pouvez utiliser le serveur RADIUS existant).

Étape 2 Pour ajouter les informations d'un nouveau serveur RADIUS au commutateur, cliquez sur **Add (ajouter)**.

L'écran contextuel de la Figure 3 s'affiche.

**Figure 3 Ajout des informations d'un nouveau serveur RADIUS**




Étape 3 Saisissez les informations suivantes :

**a.** Server IP address (adresse IP du serveur) - adresse IP du serveur RADIUS.

**b.** Priority (priorité) - (le premier serveur RADIUS à contacter).

**c.** Key string (clé d'authentification) - le mot de passe partagé configuré dans le serveur RADIUS pour ce commutateur. Le serveur RADIUS authentifie le commutateur en utilisant ce mot de passe avant d'effectuer toute authentification d'utilisateur.

**d.** Ports d'authentification et d'accès - changez ces valeurs par défaut si le serveur RADIUS est configuré pour communiquer en utilisant d'autres ports UDP.

**e.** Usage type (type d'utilisation) - sélectionnez **All (tous)**, ce qui signifie que RADIUS sera utilisé pour l'authentification basée sur 802.1x mais aussi pour l'authentification basée sur une ouverture de session.

Étape 4 Cliquez sur **Close (fermer)** pour fermer l'écran contextuel.

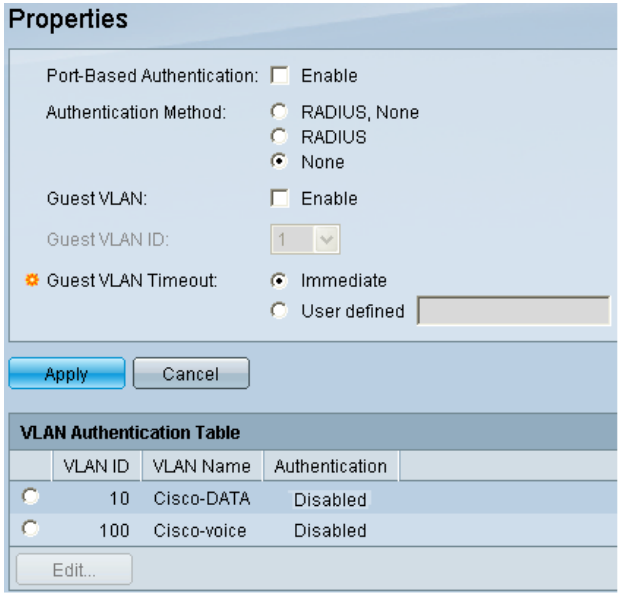
Le tableau RADIUS dans l'écran RADIUS affiche maintenant les nouvelles informations du serveur RADIUS.

# Configuration du commutateur pour un accès authentifié aux ports basé sur 802.1x

Étape 1 Sélectionnez **Security (sécurité) > 802.1x >Properties (propriétés)**.

L'écran Properties (Figure 4) s'affiche.

**Figure 4 Écran Properties**




Les étapes suivantes activent 802.1x sur les VLAN sélectionnés, et spécifient RADIUS comme politique d'authentification pour 802.1x.

Étape 2 Dans l'écran Properties (propriétés), procédez comme suit :

**a.** Port-based Authentication (authentification basée sur un port) - cliquez sur **Enable (activer)**.

**b.** Authentication Method (méthode d'authentification) - sélectionnez **RADIUS** pour indiquer une authentification RADIUS obligatoire. Si le serveur RADIUS refuse l'authentification, ou s'il est hors service, la session n'est pas autorisée.

Le choix de l'option « RADIUS, None » donne le même résultat si un refus d'authentification termine la session. Cependant, si l'authentification RADIUS ne peut pas être exécutée (serveur/réseau hors service), la session est autorisée.

**c.** Guest VLAN (VLAN invité) - non utilisé dans cet exemple.

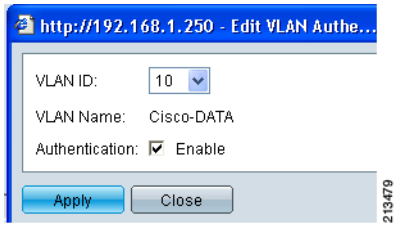
Étape 3 Cliquez sur **Apply (appliquer)**, et vérifiez que l'opération a abouti.

Le tableau VLAN Authentication Table (en bas de l'écran Properties) montre les VLAN et indique si l'authentification 802.1x est activée sur chaque VLAN (par défaut, elle pourrait être activée).

Étape 4 Dans l'écran Properties (propriétés), sélectionnez **VLAN 10** et cliquez sur **Edit (modifier)**.

L'écran contextuel présenté dans la Figure 5 s'affiche.

**Figure 5 Écran Edit VLAN (modifier VLAN)**




Étape 5 Procédez comme suit :

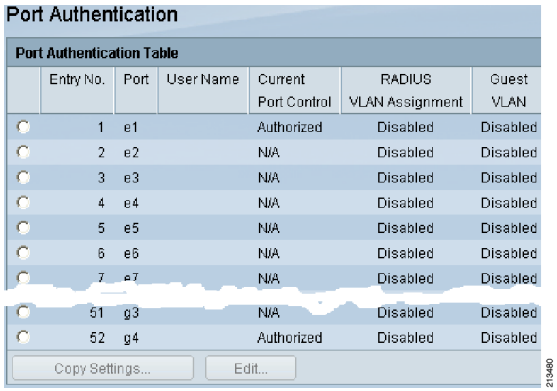
- Si le champ Authentication (authentification) indique que l'authentification 802.1x est désactivée sur VLAN 10, cliquez sur **Enable (activer)** pour activer l'authentification 802.1x sur VLAN 10, et cliquez sur **Apply (appliquer)** et vérifiez que l'opération a réussi.
- Si l'authentification 802.1x doit être activée pour les téléphones IP, activez également l'authentification 802.1x sur VLAN 100. Pour cela, sélectionnez **VLAN 100** dans cet écran, cliquez sur **Enable**, puis cliquez sur **Apply**.

Dans l'écran Properties, vérifiez que l'authentification 802.1x a été activée sur les VLAN appropriés.

Étape 6 Sélectionnez **Security (sécurité) > 802.1x >Port Authentication (authentification par port)**.

L'écran Port Authentication présenté dans la Figure 6 s'affiche.

**Figure 6 Écran Port Authentication**



Bien que l'authentification 802.1x a été activée sur le ou les VLAN, cet écran vous permet de la configurer également au niveau des ports. Chaque port peut être configuré avec l'une des options suivantes :

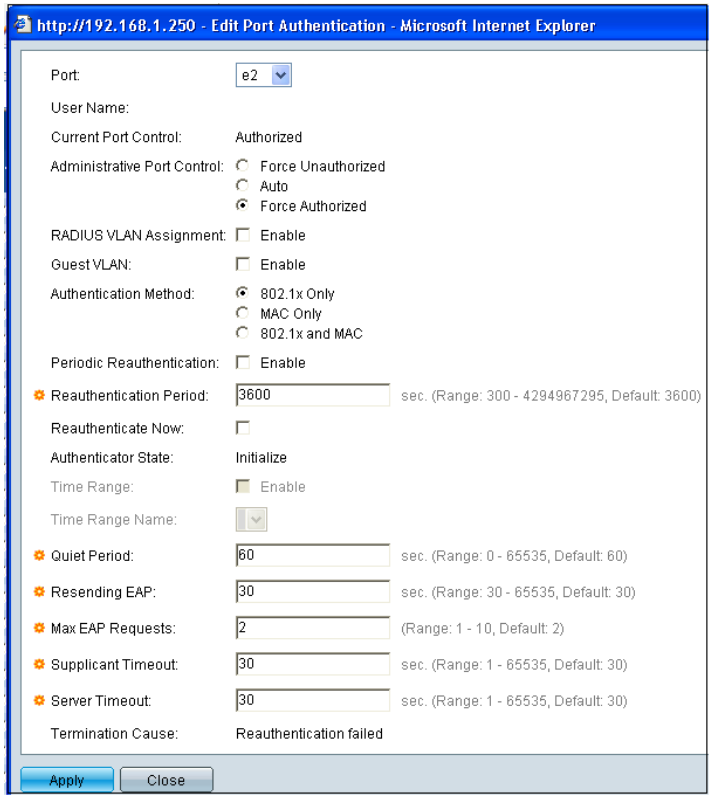
- Force Authorized (autorisation forcée) - l'accès au port est toujours autorisé (désactiver l'authentification 802.1x sur ce port)
- Force Unauthorized (interdiction forcée) - aucun accès n'est autorisé par le port
- Auto - permet un accès par le port uniquement si l'authentification 802.1x réussit

Bien que le port doive être en mode Auto pour appliquer l'authentification 802.1x, avant d'activer le mode sur la plage de ports, vous devez configurer les paramètres supplémentaires sur les ports devant être en mode « autorisation forcée ». Par conséquent, avant de continuer, vous devez vous assurer que tous les ports de la plage sont en mode « autorisation forcée ».

Étape 7 Sélectionnez le port **e2**, et cliquez sur **Edit (modifier)**.

L'écran Edit Port Authentication (modifier l'authentification des ports) s'affiche comme dans la Figure 7.

**Figure 7 Écran Edit Port Authentication**




Étape 8 Entrez les valeurs suivantes pour les différents champs, tel qu'indiqué à la Figure 7:

- Administrative Port Control (contrôle administratif des ports) - sélectionnez Force Authorized (autorisation forcée).
- Authentication Method (méthode d'authentification) - sélectionnez 802.1x Only (802.1x seulement).
- Si nécessaire, vous pouvez activer une réauthentification périodique. Laissez les valeurs par défaut inchangées, comme dans la Figure 7.

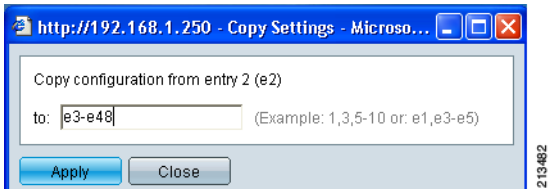
Étape 9 Cliquez sur **Apply (appliquer).** Vérifiez que « Success » (réussite) est affiché à l'écran.

Étape 10 Cliquez sur **Close (fermer)** pour fermer l'écran contextuel et afficher l'écran Port Authentication (authentification par port) sous-jacent.

Étape 11 Dans l'écran Port Authentication, sélectionnez le port **e2**, et cliquez sur **Copy Settings (copier les paramètres)**.

L'écran contextuel Copy Settings présenté à la Figure 8 s'affiche.

**Figure 8 Écran contextuel Copy Settings**




Étape 12 Entrez la plage de ports (par exemple, **e3–e48**) pour copier la configuration de e2.

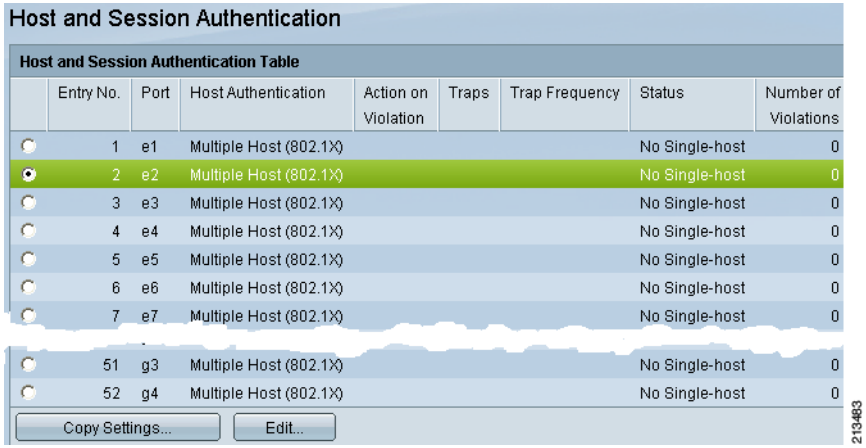
Étape 13 Cliquez sur **Apply**, et vérifiez que l'écran Port Authentication affiche « Success » (réussite).

Cela permet de placer les ports de la plage de port en mode « Forced Authorized » (autorisation forcée).

Étape 14 Sélectionnez **Security (sécurité) > 802.1x >Hosts and Session Authentication (authentification des hôtes et de la session)**.

L'écran Host and Session Authentication (Figure 9) s'affiche, ce qui vous permet de spécifier les politiques d'accès à utiliser lorsque plusieurs appareils sont connectés au port.

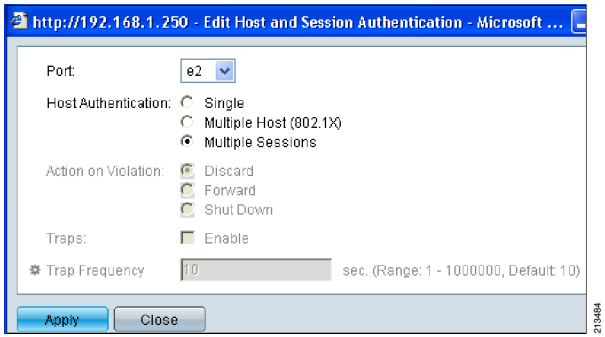
**Figure 9 Écran Host and Session Authentication**




Étape 15 Pour changer la politique sur le port **e2**, sélectionnez le port **e2**, comme dans la Figure 9, et cliquez sur **Edit (modifier)**.

L'écran contextuel Edit Hosts and Session Authentication (modifier l'authentification des hôtes et de la session) présenté dans la Figure 10 s'affiche.

**Figure 10 Écran contextuel Edit Hosts and Session Authentication**




Étape 16 Dans le champ Host Authentication (authentification des hôtes), sélectionnez **Multiple Sessions (sessions multiples)** et cliquez sur **Apply**.

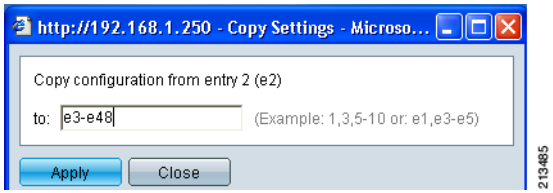
Vérifiez que « Success » (réussite) s'affiche.

Si l'opération est refusée, revenez à l'étape 7, changez la valeur du champ Administrative Port Control (contrôle administratif des ports) à **Force Authorized (autorisation forcée)** et recommencez.

Étape 17 Dans l'écran Host and Session Authentication, sélectionnez le port **e2** et cliquez sur **Copy Settings (copier les paramètres)**.

L'écran contextuel Copy Settings présenté à la Figure 11 s'affiche.

**Figure 11 Écran contextuel Copy Settings**




Étape 18 Entrez la plage de ports (par exemple **e3–e48**) pour copier la configuration de e2 sur les ports spécifiés, et cliquez sur **Apply**.

Vérifiez que l'écran Host and Session Authentication affiche "Success".

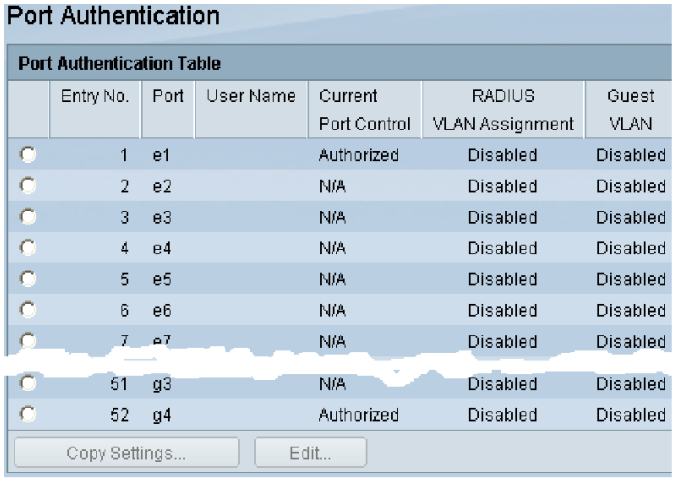
Cela permet de placer les ports dans la plage de ports en mode « Multiple Session » (sessions multiples) d'authentification d'hôte.

L'étape suivante active l'authentification 802.1x sur un port unique (e2) à des fins de vérification. Après vérification de son fonctionnement, l'authentification 802.1.x est activée sur les autres ports.

Étape 19 Pour activer l'authentification 802.1x sur le port e2, sélectionnez **Security (sécurité) > 802.1x >Port Authentication (authentification par port)**.

L'écran Port Authentication s'affiche, comme dans la Figure 12.

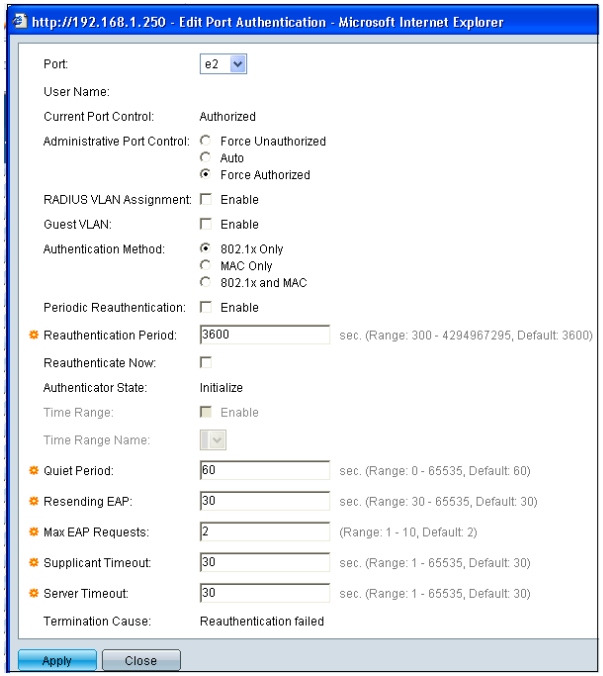
**Figure 12 Écran Port Authentication**



Étape 20 Sélectionnez le port **e2**, et cliquez sur **Edit (modifier)**.

L'écran Edit Port Authentication (modifier l'authentification des ports) s'affiche comme dans la Figure 13.

**Figure 13 Écran Edit Port Authentication**




Étape 21 Entrez les valeurs suivantes pour les champs :

- Administrative Port Control (contrôle administratif des ports) : sélectionnez **Auto**.
- Authentication Method (méthode d'authentification) : sélectionnez **802.1x Only (802.1x seulement)**
- Si nécessaire, vous pouvez activer une réauthentification périodique. Conservez les valeurs par défaut des délais d'attente comme indiqué dans la Figure 13.

Étape 22 Cliquez sur **Apply** et vérifiez que « Success » (réussite) est affiché à l'écran.

Étape 23 Cliquez sur **Close (fermer)** pour fermer l'écran contextuel et afficher l'écran Port Authentication (authentification par port) sous-jacent.

Cela termine la configuration de l'authentification 802.1x sur le port e2.

Étape 24 Pour vérifier que l'authentification 802.1x fonctionne sur le port e2, connectez un ordinateur portable au port e2 et configurez la connexion Ethernet de l'ordinateur portable avec les paramètres suivants :

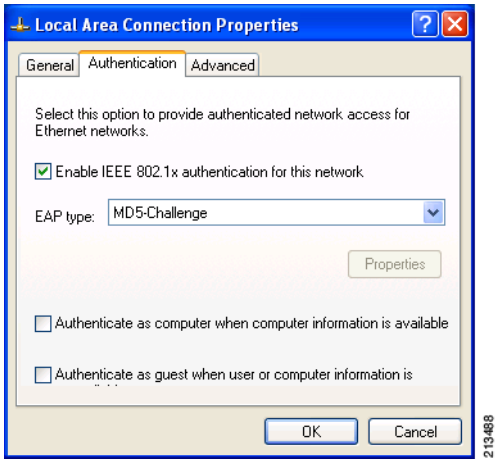
- Accepter une adresse IP et DNS via DHCP
- Effectuer une authentification 802.1x

Les écrans affichés varient selon la version spécifique du système d'exploitation de l'ordinateur portable. Windows XP est utilisé dans l'exemple.

Étape 25 Selectionnez **Propriétés de la connexion au réseau local > Général > Authentification**.

L'écran présenté dans la Figure 14 s'affiche.

**Figure 14 Propriété de la connexion au réseau local - onglet Authentification**




Étape 26 Cochez **Authentification IEEE 802.1x**.

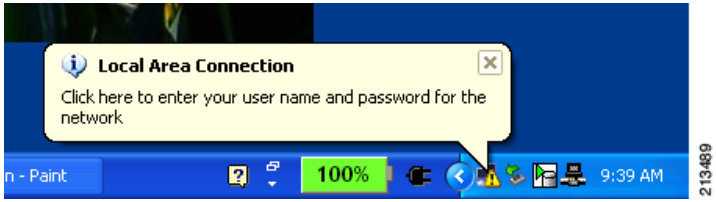
Étape 27 Sélectionnez le type EAP **MD5-Challenge** ou **PEAP** selon les besoins.

Ce choix doit correspondre au type d'authentification du groupe d'utilisateurs configuré dans le serveur RADIUS.

Étape 28 Cliquez sur **OK** pour enregistrer le changement de configuration.

Pendant quelques secondes après la connexion de l'ordinateur portable, ce dernier peut indiquer que la connexion est établie, bien que l'accès ne soit pas attribué à l'utilisateur. Après quelques secondes, un message doit apparaître invitant à entrer le nom de l'utilisateur et le mot de passe, comme dans la Figure 15.

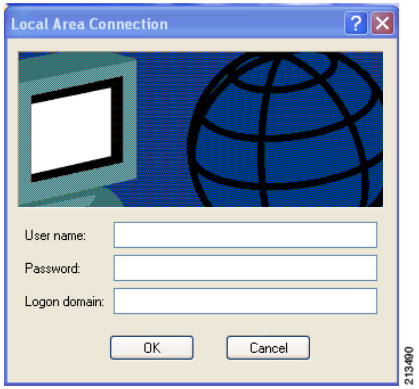
**Figure 15 Entrée du nom de l'utilisateur et du mot de passe**



Étape 29 Cliquez sur l'icône indiquée.

L'écran présenté dans la Figure 16 s'affiche et permet d'entrer le nom d'utilisateur et le mot de passe pour l'authentification.

**Figure 16 Écran User Authentication (authentification de l'utilisateur)**




Étape 30 Entrez le nom de l'utilisateur et le mot de passe, puis cliquez sur **OK**.

L'authentification 802.1x se termine et l'icône de connexion de l'ordinateur portable dans la barre des tâches confirme l'établissement d'une connexion.

Étape 31 Sélectionnez **Security (sécurité) > 802.1x > Port Authentication (authentification par port)**.

L'écran Port Authentication (Figure 12) s'affiche avec un tableau qui présente l'état d'authentification des ports. Vérifiez que le port e2 est maintenant indiqué dans l'état « Authorized » (autorisé) sous la colonne Current Port Control (contrôle du port actuel).

Étape 32 Sélectionnez **Security (sécurité) > 802.1x > Authenticated Hosts (hôtes authentifiés)**.

L'écran Authenticated Hosts s'affiche, présentant chaque port se trouvant actuellement dans l'état authentifié 802.1x. Pour chaque port authentifié, il indique l'identifiant de l'utilisateur, l'adresse MAC de l'appareil de l'utilisateur (par exemple un ordinateur portable) et la durée de session correspondants. Vérifiez que les informations affichées ici pour le port e2 sont correctes.

Vous pouvez maintenant interroger (requête ping) les adresses IP dans le réseau pour vérifier que le port autorise un trafic utilisateur.

La vérification de l'authentification 802.1x sur le port e2 est maintenant terminée.

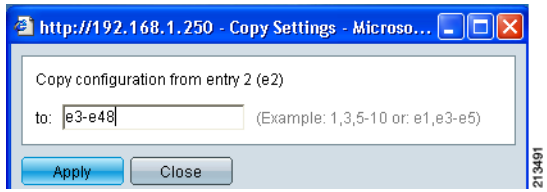
Étape 33 Pour activer l'authentification 802.1x sur d'autres ports (ports e2 à e48, dans cet exemple), sélectionnez **Security (sécurité) > 802.1x >Port Authentication (authentification par port)**.

L'écran Port Authentication s'affiche.

Étape 34 Sélectionnez port **e2**, et cliquez sur **Copy Settings (copier les paramètres)**.

L'écran contextuel Copy Settings présenté à la Figure 17 s'affiche.

**Figure 17 Écran contextuel Copy Settings**




Étape 35 Saisissez la plage de ports (par exemple, **e3–e48**) pour copier la configuration de e2 sur les ports spécifiés, et cliquez sur **Apply (appliquer)**.

Vérifiez que l'écran Port Authentication (authentification par port) affiche « Success » (réussite).

L'authentification 802.1x est maintenant activée sur la plage de ports spécifiée.

## Configuration de l'accès aux ports basé sur l'heure (en option)

Cette configuration définit un intervalle de temps absolu allant du 17 août 2010 au 1er janvier 2020. Elle restreint également l'accès utilisateur à des périodes spécifiques chaque jour de la semaine (par exemple de 9 h 00 à 17 h 00 le lundi).

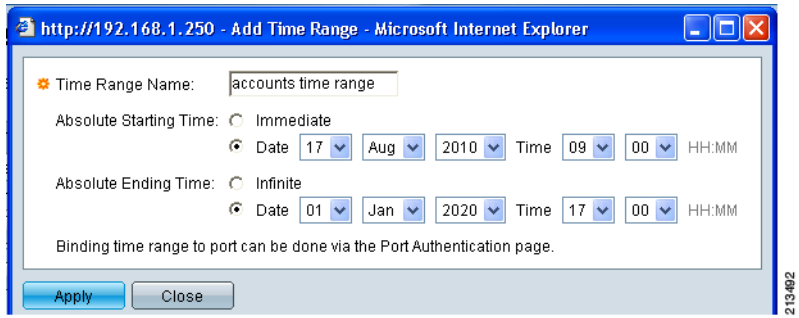
Step 1 Sélectionnez **Security (sécurité) > 802.1x > Time Range (intervalle de temps)**.

L'écran Time Range s'affiche pour ajouter un intervalle de temps absolu.

Étape 2 Cliquez sur **Add (ajouter)**.

L'écran contextuel présenté dans la Figure 18 s'affiche.

**Figure 18 Ajout d'un intervalle de temps**



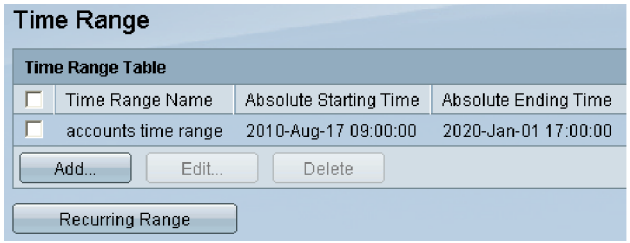

Étape 3 Saisissez un nom pour l'intervalle de temps absolu (**accounts time range**), l'heure et la date de début, l'heure et la date de fin de la période, comme dans la Figure 18.

Vous pouvez spécifier l'heure de début comme immédiate, et l'heure de fin comme infinie, si vous le souhaitez.

Étape 4 Cliquez sur **Apply** et vérifiez que « Success » (réussite) s'affiche.

L'écran présenté dans la Figure 19 s'affiche, indiquant le nouvel intervalle de temps entré.

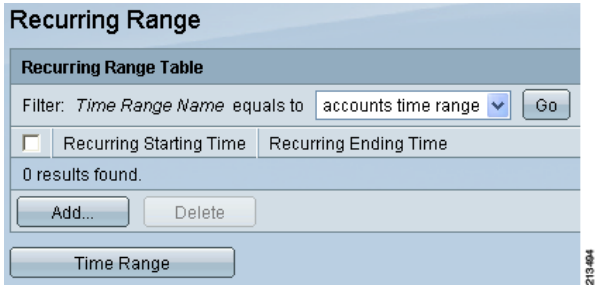
**Figure 19 Écran Time Range (intervalle de temps)**




Étape 5 Cliquez sur **Recurring Range (intervalle récurrent)**.

L'écran Recurring Time Range (intervalle de temps récurrent) présenté dans la Figure 20 s'affiche.

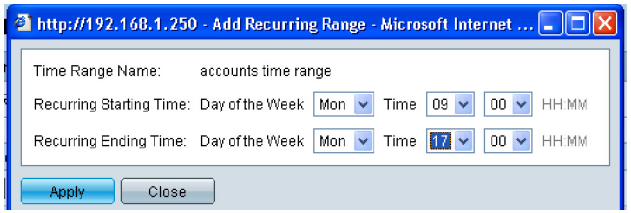
**Figure 20 Écran Recurring Range**




Étape 6 Cliquez sur **Add...**

L'écran Add Recurring Range (ajouter un intervalle récurrent) s'affiche, comme dans la Figure 21, qui est utilisé pour ajouter un ou plusieurs intervalles de temps récurrents à l'intervalle de temps absolu sélectionné (accounts time range, dans cet exemple).

**Figure 21 Figure 23**




Étape 7 Saisissez les valeurs Recurring Starting time (Heure de début récurrente) et Recurring Ending Time (Heure de fin récurrente) pour chaque jour de la semaine tel qu'indiqué dans la Figure 21, et cliquez sur **Apply (appliquer)**.

Vérifiez que « Success » (réussite) s'affiche.

Comme le montre la Figure 21, cela crée un intervalle de temps récurrent pour lundi de 9 h 00 à 17 h 00, qui permet un accès réseau uniquement pendant cette période, à condition que l'authentification 802.1x réussisse.

Répétez les étapes 5 et 6 pour ajouter d'autres intervalles de temps récurrents pour les autres jours de la semaine.

Ainsi se termine la création de l'intervalle de temps. Vous devez maintenant l'appliquer aux ports.

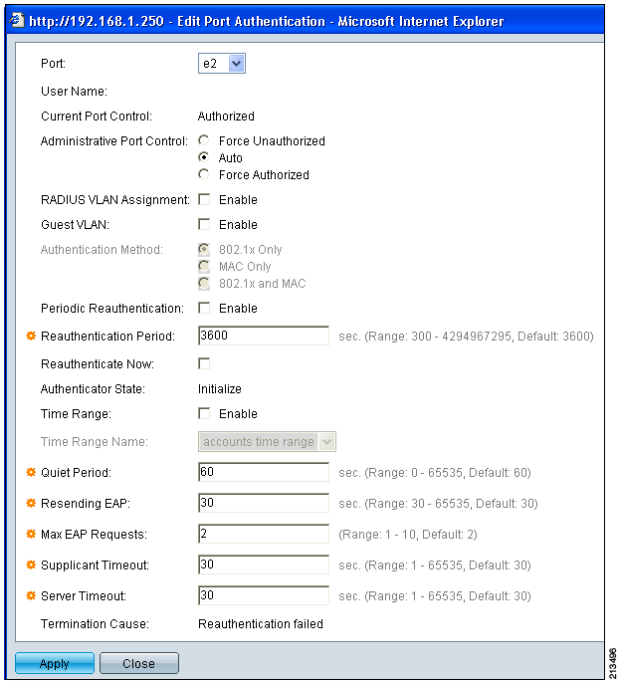
Étape 8 Sélectionnez **Security (sécurité) > 802.1x > Port Authentication (authentification par port)**.

L'écran Port Authentication (authentification par port) s'affiche répertoriant chaque port et ses informations détaillées.

Étape 9 Sélectionnez un port (**e2**, dans cet exemple) où l'intervalle de temps doit être appliqué, et cliquez sur **Edit (modifier)**.

L'écran présenté dans la Figure 22 s'affiche avec les détails du port. Notez que le champ Time Range (intervalle de temps) n'est pas activé sur cet écran par défaut.

**Figure 22 Écran Edit Port Authentication (modifier l'authentification des ports)**



Étape 10 Pour ajouter l'intervalle de temps au port e2, procédez comme suit :

**a.** Cliquez pour activer le champ Time Range.

**b.** Dans le champ Time Range Name (nom de l'interavalle de temps), sélectionnez un intervalle de temps dans la liste déroulante (dans ce cas, accounts time range).

Étape 11 Cliquez sur **Apply (appliquer).**

Vérifiez que l'écran Edit Port Authentication affiche « Success » (réussite).

Étape 12 Cliquez sur **Close (fermer)**, pour fermer l'écran Edit Port Authentication.

Le port e2 est maintenant configuré avec l'intervalle de temps.

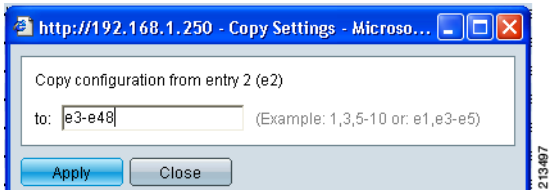
Étape 13 Sélectionnez **Security (sécurité) > 802.1x > Port Authentication (authentification par port)**.

L'écran Port Authentication (authentification par port) s'affiche répertoriant chaque port et ses informations détaillées. Cela permet de copier la configuration du port e2 sur d'autres ports similaires.

Étape 14 Sélectionnez un port (e2, dans cet exemple) où l'intervalle de temps a été appliqué, et cliquez sur **Copy Settings (copier les paramètres)**.

L'écran présenté dans la Figure 23 s'affiche pour entrer la plage de ports où la configuration du port e2 sera copiée.

**Figure 23 Copie de l'écran de configuration**




Étape 15 Entrez la plage (par exemple, e2 à e48), puis cliquez sur **Apply**.

Cet écran disparaît, et l'écran Port Authentication (authentification par port) s'actualise.

Étape 16 Vérifiez que « Success » (réussite) est affiché sur l'écran Port Authentication.

La configuration de l'authentification 802.1x pour les ports e2 à e48 est maintenant terminée.

# Résumé

Ce document décrit l'utilisation de l'authentification 802.1x et sa configuration sur un commutateur de la gamme Cisco Small Business série 300. Cette authentication permet un accès authentifié aux ports du réseau local, améliorant ainsi la sécurité du réseau. Pour accroître la sécurité, elle prend en charge un accès basé sur l'heure qui restreint l'accès au port à des heures spécifiques d'une journée. En outre, l'affectation de VLAN dynamique peut être utilisée pour affecter automatiquement le VLAN à un utilisateur, de sorte que les ports n'ont pas besoin d'être préconfigurés avec des VLAN. Cette procédure simplifie le déploiement de réseaux locaux avec une plus grande sécurité et une meilleure souplesse.

Pour plus d'informations sur la configuration des commutateurs administrables de la gamme Cisco série 300, consultez le guide de l'administrateur à l'adresse URL suivante :

http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf