



GUIDE D'ADMINISTRATION

Cisco Small Business Pro

Point d'accès à radio unique bi-bande AP 541N

OL-23754-01

Préface	9
Public visé	9
Conventions utilisées dans le présent document	9
Aide en ligne, navigateurs pris en charge et restrictions	11
Chapitre 1 : Mise en route	13
Configuration requise de l'ordinateur de l'administrateur	14
Adresse IP de l'ordinateur d'administration	15
Connexion du point d'accès à un ordinateur	16
Connecter le point d'accès à un ordinateur d'administration	16
Connexion du point d'accès à l'ordinateur à l'aide d'une connexion par câble directe	16
Connexion du point d'accès à l'ordinateur via une connexion réseau	17
Lancement de l'utilitaire de configuration du point d'accès	18
Afficher l'utilitaire de configuration en utilisant l'adresse IP par défaut	18
Afficher l'utilitaire de configuration en utilisant Cisco Configuration Assistant 2.1 ou version ultérieure	21
Afficher l'utilitaire de configuration en utilisant une autre adresse IP	23
Dépannage de votre connexion	25
Utilisation de la commande ping pour tester la connexion	25
Cause possible de l'échec	26
Réinitialisation du périphérique à l'aide du bouton Reset	26
Configuration du point d'accès à l'aide de la page Getting Started	27
Configuration du point d'accès	27
Page Access Point Management	28
Page Wireless Configuration	28
Configuration requise du client	29
Vérification de l'installation	30
Configuration de la sécurité sur le point d'accès sans fil	31

Table des matières

Chapitre 2 : État	33
Informations périphérique	33
Interfaces réseau	35
Wired Settings	35
Wireless Settings	36
Statistiques de trafic	36
Clients associés	39
Surveillance de l'intégrité de la liaison	41
Détection des points d'accès indésirables	41
Enregistrer ou importer la liste des points d'accès connus	46
Chapitre 3 : Configuration	47
Paramètres LAN	47
Configuration de l'authentification 802.1X	51
Activation du protocole Network Time	53
Chapitre 4 : Sans fil	59
Modification des paramètres radio sans fil	59
Modification des paramètres de point d'accès virtuel	63
Security (mode)	71
Contrôle de la connexion des clients	85
Configuration d'un filtre MAC et d'une liste de stations sur le point d'accès	86
Configuration de l'authentification MAC sur le serveur RADIUS	89
Modification des paramètres avancés	89
Configuration du système de distribution sans fil (WDS)	100
Cryptage WEP sur les liens WDS	103
Cryptage WPA/PSK sur les liens WDS	104
Utilisation de la bande passante	106
Configuration de la qualité de service (QoS)	107

Chapitre 5 : SNMP	113
Configuration du SNMP sur le point d'accès	113
Configuration des vues SNMP	118
Configuration des groupes SNMP	121
Configuration des utilisateurs SNMP	124
Cibles SNMP	126
 Chapitre 6 : Administration	 129
Administrateur	129
Configuration du point d'accès	131
Réinitialisation de la configuration par défaut du point d'accès	132
Enregistrement de la configuration actuelle dans un fichier de sauvegarde	132
Enregistrement de la configuration actuelle via TFTP	132
Enregistrement de la configuration actuelle via HTTP	133
Restauration de la configuration à partir d'un fichier enregistré	133
Restauration de la configuration actuelle via TFTP	133
Restauration de la configuration actuelle via HTTP	134
Redémarrage du point d'accès	135
Mise à niveau du logiciel	135
Mise à niveau du logiciel via TFTP	136
Mise à niveau du logiciel via HTTP	137
Journaux d'événements	138
Configuration des options de consignation persistante	139
Configuration de l'hôte de relais de consignation pour les messages de noyau	142
Activation ou désactivation de l'hôte de relais de consignation dans la page Events	142
Configuration des paramètres du serveur Web	144
Création d'une liste de contrôle d'accès d'administration	146

Chapitre 7 : Mise en grappe de plusieurs points d'accès	149
Gestion des points d'accès de la grappe	149
Mise en grappe de points d'accès à un ou deux modules radio	150
Affichage et configuration des membres d'une grappe	150
Suppression d'un point d'accès de la grappe	153
Ajout d'un point d'accès à une grappe	153
Navigation jusqu'aux informations de configuration d'un point d'accès spécifique	154
Navigation jusqu'à un point d'accès à l'aide de son adresse IP dans une URL	154
Gestion des sessions de grappe	155
Tri des informations de session	157
Configuration et affichage des paramètres de gestion des canaux	158
Démarrage/arrêt de l'affectation automatique des canaux	159
Affichage des affectations de canaux et définition de verrous	160
Affichage du dernier ensemble de modifications proposé	161
Configuration des paramètres avancés	162
Affichage des informations sur le voisinage réseau sans fil	163
Affichage des détails relatifs à un membre de la grappe	167
Chapitre 8 : Des exemples de configuration	169
Configuration d'un point d'accès virtuel (VAP)	170
Configuration du VAP à partir de l'interface Web	171
Configuration du VAP à partir du SNMP	172
Configuration des paramètres de la radio sans fil	173
Configuration de la radio sans fil à partir de l'interface Web	173
Configuration de la radio sans fil à l'aide du SNMP	175
Configuration du système de distribution sans fil	175
Configuration du WDS à partir de l'interface Web	176
Configuration du WDS à partir du SNMP	177
Mise en grappe des points d'accès	178
Mise en grappe des points d'accès à l'aide de l'interface Web	178
Mise en grappe des points d'accès à l'aide du SNMP	180

Annexe A : Paramètres par défaut	181
Annexe B : Pour en savoir plus	185

Table des matières

Préface

Ce guide décrit le réglage, la configuration, l'administration et la maintenance du Cisco® Point d'accès à radio unique bi-bande AP 541N sur un réseau sans fil.

Public visé

Ce guide s'adresse aux administrateurs système responsables de la configuration et de l'exploitation du réseau à l'aide du logiciel Cisco.

Pour profiter au maximum de ce guide, vous devez avoir une connaissance de base de la mise en réseau Ethernet et sans fil.

Conventions utilisées dans le présent document

Cette section décrit les conventions utilisées dans le présent document.



REMARQUE Une remarque fournit des informations supplémentaires sur une fonctionnalité ou une technologie et fait référence aux rubriques connexes.



AVERTISSEMENT Un avertissement fournit des informations sur les aspects cruciaux de la configuration du point d'accès, la combinaison des paramètres, les événements et les procédures susceptibles d'avoir une incidence négative sur la connectivité du réseau, la sécurité du réseau, etc.

Tableau 1 décrit les conventions typographiques utilisées dans ce guide.

Tableau 1 Conventions typographiques

Symbole	Exemple	Description
Gras	Cliquez sur Apply pour enregistrer vos paramètres.	Titres de menus, noms de pages et noms de boutons
Texte bleu	Reportez-vous à Conventions utilisées dans le présent document, page 9.	Lien hypertexte.
police courier	WLAN-AP# show network	Texte affiché à l'écran, noms de fichiers, commandes, lignes de commande utilisateur
<i>police courier italique</i>	<i>valeur</i>	Paramètre de la commande, qui peut correspondre à une variable ou une valeur fixe.
<> Crochets en chevron	<valeur>	Indique que le paramètre est une variable. Vous devez saisir une valeur à la place des crochets et saisir du texte à l'intérieur.
[] Crochets	[valeur]	Indique un paramètre fixe en option.
[<>] Crochets en chevron entre crochets	[<valeur>]	Indique une variable en option.
{ } Accolades	{choix1 choix2}	Indique que vous devez sélectionner un paramètre dans une liste de choix.
Barres verticales	choix1 choix2	Séparent les choix qui s'excluent mutuellement.
[{}] Accolades entre crochets	[{choix1 choix2}]	Indique un choix dans un élément en option.

Aide en ligne, navigateurs pris en charge et restrictions

L'aide en ligne des pages *Utilitaire de configuration du point d'accès* fournit des informations sur tous les champs et toutes les fonctionnalités disponibles pour *Utilitaire de configuration du point d'accès*. Les informations de l'aide en ligne constituent un sous-élément des informations disponibles dans le *Guide d'administration du point d'accès à radio unique bi-bande Cisco AP 541N*.

Les informations de l'aide en ligne correspondent à chaque page du point d'accès Utilitaire de configuration.

Pour obtenir des informations sur les paramètres de la page actuelle, cliquez sur le lien **Help** situé à droite de la page.

Préface

Mise en route

Le point d'accès Cisco fournit un accès haut débit continu entre les périphériques sans fil et Ethernet. Il s'agit d'une solution avancée et conforme aux normes de mise en réseau sans fil destinée aux entreprises de toute taille. Le point d'accès permet le déploiement d'un réseau local sans fil (WLAN) tout en offrant des fonctionnalités de mise en réseau sans fil de pointe.

Le point d'accès fonctionne en mode autonome. En mode autonome, le point d'accès agit en tant que point d'accès individuel dans le réseau. Vous pouvez le gérer à l'aide de l'*Utilitaire de configuration du point d'accès* ou le protocole SNMP.

Ce document décrit la procédure à suivre pour effectuer la configuration, la gestion et la maintenance du point d'accès en mode autonome. Avant de mettre sous tension un nouveau le point d'accès, consultez les sections suivantes pour connaître les composants matériels et logiciels requis, les configurations client et les problèmes de compatibilité. Veillez à disposer de tout ce dont vous avez besoin pour réussir le lancement et le test de votre nouveau réseau sans fil ou de votre réseau sans fil étendu.

Ce chapitre contient les rubriques suivantes :

- **Configuration requise de l'ordinateur de l'administrateur**
- **Connexion du point d'accès à un ordinateur**
- **Dépannage de votre connexion**
- **Configuration du point d'accès à l'aide de la page Getting Started**
- **Vérification de l'installation**
- **Configuration de la sécurité sur le point d'accès sans fil**

Pour gérer le point d'accès à l'aide de l'interface Web , le point d'accès nécessite une adresse IP. Si vous utilisez des VLAN ou l'authentification IEEE 802.1X (sécurité des ports) sur votre réseau, vous devrez peut-être configurer des paramètres supplémentaires sur le point d'accès avant qu'il puisse se connecter au réseau.



REMARQUE Le point d'accès WLAN n'est pas conçu pour fonctionner en tant que passerelle vers Internet. Pour connecter votre WLAN à d'autres LAN ou à Internet, vous avez besoin d'un périphérique passerelle.

Configuration requise de l'ordinateur de l'administrateur

Le **Tableau 1** décrit la configuration minimale requise de votre ordinateur personnel pour la configuration et l'administration initiales du point d'accès via un *Utilitaire de configuration du point d'accès*.

Tableau 1 Configuration requise

Logiciel ou composant requis	Description
Connexion Ethernet au point d'accès	L'ordinateur utilisé pour configurer le point d'accès doit être connecté à ce dernier via un câble Ethernet. L'adresse IP doit être sur le même sous-réseau que le point d'accès. Le masque de sous-réseau doit correspondre à celui du point d'accès. La section Adresse IP de l'ordinateur d'administration décrit la procédure à suivre pour modifier ces paramètres sur un ordinateur exécutant Windows.
Navigateur Web et système d'exploitation	<p>Les navigateurs Web suivants peuvent être utilisés pour afficher les pages Web de l'Utilitaire de configuration du point d'accès :</p> <ul style="list-style-type: none"> Microsoft® Internet Explorer® version 6.x ou 7.x (avec niveau de correctifs actualisé pour l'une ou l'autre de ces versions majeures) et Mozilla Firefox 3.x sous Microsoft Windows® XP ou Microsoft Windows 2000 Mozilla Firefox 3.x sous Redhat® Linux® 2.4 ou version ultérieure <p>JavaScript™ doit être activé dans le navigateur Web pour prendre en charge les fonctionnalités interactives de l'interface de l'Utilitaire de configuration.</p>

Tableau 1 Configuration requise (suite)

Logiciel ou composant requis	Description
Paramètres de sécurité	Assurez-vous de la désactivation de la sécurité sur le client sans fil initialement utilisé pour configurer le point d'accès. Une fois la configuration du périphérique effectuée, la sécurité peut être activée.

Adresse IP de l'ordinateur d'administration

Si vous utilisez la configuration par défaut ou si le périphérique est configuré pour la première fois, nous vous recommandons de le configurer avant de le déployer dans le réseau en utilisant l'adresse IP statique du point d'accès par défaut (192.168.10.10). Pour ce faire, l'adresse IP de l'ordinateur doit être sur le même sous-réseau que le point d'accès.

Assurez-vous que l'adresse IP de votre ordinateur est définie sur une adresse située sur le même sous-réseau que le point d'accès :

-
- ÉTAPE 1** Dans le menu **Démarrer** de Windows, sélectionnez **Paramètres > Panneau de configuration**.
- ÉTAPE 2** Dans la boîte de dialogue du panneau de configuration, cliquez sur **Network**.
- ÉTAPE 3** Dans la boîte de dialogue Network, sélectionnez **TCP/IP** pour la carte Ethernet de votre ordinateur, puis cliquez sur **Properties**.
- ÉTAPE 4** Dans la fenêtre IP Address, cliquez sur **Specify an IP address**.
- ÉTAPE 5** Dans le champ IP Address, entrez une adresse IP située dans le même sous-réseau que l'adresse IP du point d'accès. (L'adresse IP du point d'accès par défaut est 192.168.10.10. Le masque de sous-réseau par défaut est 255.255.255.0.) Par exemple, vous pouvez définir les éléments suivants :
- Adresse IP de l'ordinateur : 192.168.10.250
Masque de sous-réseau IP de l'ordinateur : 255.255.255.0
- ÉTAPE 6** Dans le champ Subnet Mask, saisissez 255.255.255.0.
- ÉTAPE 7** Cliquez sur **OK**.
- ÉTAPE 8** Si vous êtes invité à redémarrer votre ordinateur, cliquez sur **Yes**.
-

Connexion du point d'accès à un ordinateur

Pour configurer le point d'accès, vous pouvez connecter le point d'accès à un ordinateur d'administration directement ou via le réseau.

Si vous n'utilisez pas l'assistant CCA pour configurer le point d'accès, nous vous recommandons de configurer le périphérique avant de le déployer dans le réseau en suivant les instructions de la section « **Connecter le point d'accès à un ordinateur d'administration** ». Sinon, suivez les instructions de la section « **Connexion du point d'accès à l'ordinateur via une connexion réseau** ».

Connecter le point d'accès à un ordinateur d'administration

Vous pouvez connecter le point d'accès à un ordinateur d'administration directement ou via le réseau. Nous vous recommandons de connecter le point d'accès directement à l'ordinateur, sauf si vous utilisez l'assistant CCA pour configurer le point d'accès.

Connexion du point d'accès à l'ordinateur à l'aide d'une connexion par câble directe

Pour connecter le point d'accès à un ordinateur d'administration, utilisez une connexion par câble directe :

- ÉTAPE 1** Connectez l'une des extrémités d'un câble Ethernet direct ou croisé au port réseau sur le point d'accès, comme illustré dans la **Figure 1**.
- ÉTAPE 2** Connectez l'autre extrémité du câble au port Ethernet de votre ordinateur.

Figure 1 Connexion du point d'accès à l'aide d'une connexion par câble directe



Si vous utilisez cette méthode, vous devrez reconfigurer le câblage lors des prochains démarrages et déploiements du point d'accès, de sorte que ce dernier ne soit plus directement connecté à l'ordinateur, mais connecté au LAN (grâce à un hub ou un commutateur).

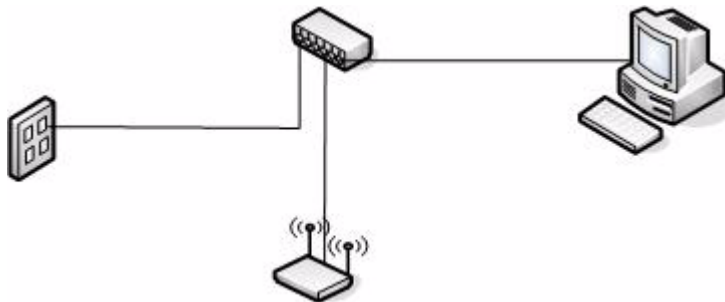
- ÉTAPE 3** Branchez l'adaptateur secteur sur le port d'alimentation situé à l'arrière du point d'accès.
- ÉTAPE 4** Branchez l'autre extrémité du cordon d'alimentation sur une prise de courant.
- ÉTAPE 5** Configurez le point d'accès en suivant les instructions de la section « **Afficher l'utilitaire de configuration en utilisant l'adresse IP par défaut** ».

Connexion du point d'accès à l'ordinateur via une connexion réseau

Pour connecter le point d'accès à un ordinateur d'administration via le réseau, procédez comme suit :

- ÉTAPE 1** Connectez l'une des extrémités d'un câble Ethernet direct ou croisé au port réseau sur le point d'accès, comme illustré dans la **Figure 2**.
- ÉTAPE 2** Connectez l'autre extrémité au même hub ou commutateur auquel votre ordinateur est connecté.

Figure 2 Connexion du point d'accès à l'aide d'une connexion LAN



Le hub ou le commutateur que vous utilisez doit permettre aux signaux de diffusion du point d'accès d'atteindre les autres périphériques du réseau.

- ÉTAPE 3** Si vous n'utilisez pas PoE, connectez l'adaptateur secteur au port d'alimentation situé à l'arrière du point d'accès, puis branchez l'autre extrémité du cordon d'alimentation sur une prise de courant.

Lancement de l'utilitaire de configuration du point d'accès

Cette section contient des informations concernant le lancement de l'*Utilitaire de configuration du point d'accès* :

- Utilisation de l'adresse IP statique par défaut du commutateur. Suivez les instructions de la section « **Afficher l'utilitaire de configuration en utilisant l'adresse IP par défaut** ».
- Utilisation du programme Cisco Configuration Assistant (CCA). Suivez les instructions de la section « **Afficher l'utilitaire de configuration en utilisant Cisco Configuration Assistant 2.1 ou version ultérieure** ».
- Utilisation d'une adresse IP attribuée au commutateur via DHCP. Suivez les instructions de la section « **Afficher l'utilitaire de configuration en utilisant une autre adresse IP** ».

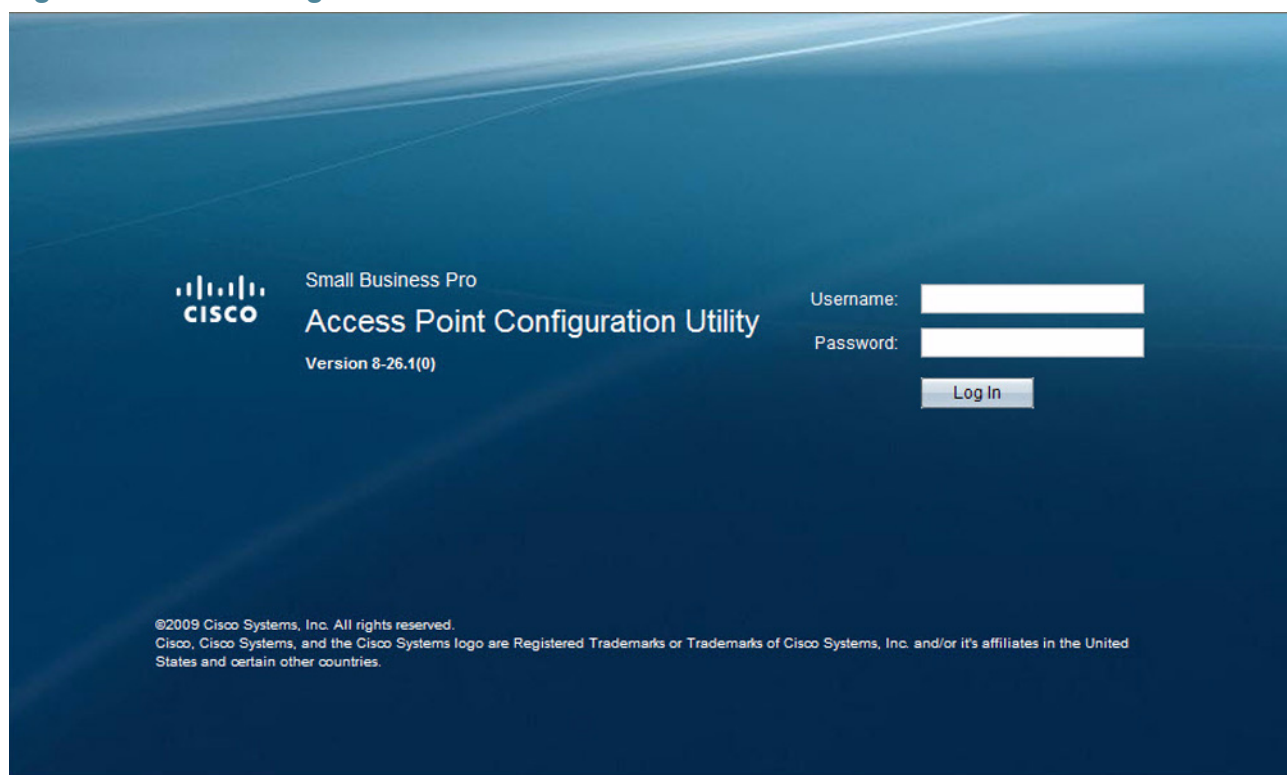
Afficher l'utilitaire de configuration en utilisant l'adresse IP par défaut

Pour accéder à l'Utilitaire de configuration du point d'accès, saisissez l'adresse IP statique par défaut du point d'accès dans un navigateur Web et effectuez les actions suivantes :

ÉTAPE 1 Entrez l'adresse IP statique par défaut du Cisco AP 541N dans la barre d'adresse, puis appuyez sur **Entrée**. Par exemple, **http://192.168.10.10**.

La fenêtre **Login** apparaît, comme illustré dans la **Figure 3**.

Figure 3 Fenêtre Login

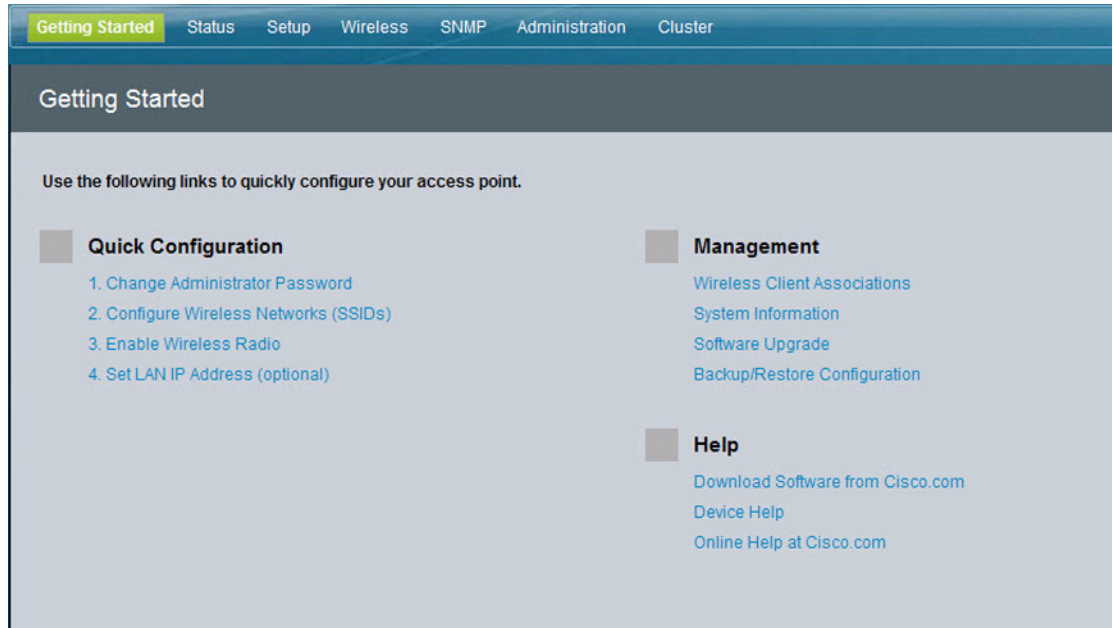


ÉTAPE 2 Saisissez les informations de connexion :

Nom d'utilisateur = **cisco**

Mot de passe par défaut *cisco*. (Les mots de passe sont sensibles à la casse.)

Lorsque vous vous connectez, la page **Getting Started** de l'Utilitaire de configuration du point d'accès apparaît, comme illustré dans la **Figure 4**.

Figure 4 Page Getting Started

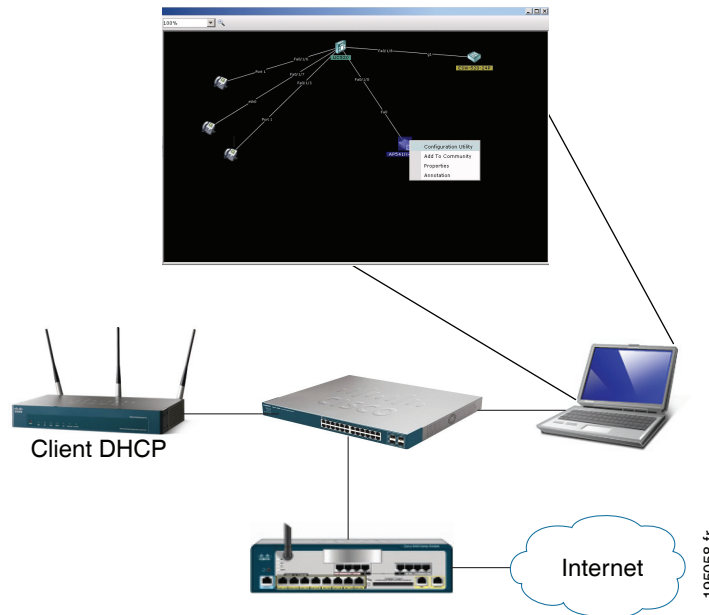
ÉTAPE 3 Mettez à jour le logiciel Cisco AP 541N avec la dernière version en cliquant sur le lien **Software Upgrade**, comme illustré dans la **Figure 4**.

Ensuite, nous vous recommandons d'effectuer les actions suivantes :

- Modifiez le mot de passe en cliquant sur **Change Administrator Password**.
- Configurez le SSID et activez la sécurité sans fil, en cliquant sur **Configure Wireless Networks (SSIDs)**.
- Activez la radio sans fil, en cliquant sur **Enable Wireless Radio**.
- Attribuez une nouvelle adresse IP statique au point d'accès si vos périphériques réseau sont configurés avec des adresses IP statiques, en cliquant sur **Set LAN IP Address**.

Afficher l'utilitaire de configuration en utilisant Cisco Configuration Assistant 2.1 ou version ultérieure

Utilisez Cisco Configuration Assistant 2.1 ou version ultérieure (CCA) pour configurer le point d'accès lorsqu'il est déployé dans un réseau Cisco Configuration Assistant 2.1 ou version ultérieure avec un UC520 ou SR520.



Pour utiliser cette procédure, vous devez connaître l'assistant CCA. Vous pouvez obtenir des informations supplémentaires concernant l'assistant CCA à l'adresse www.cisco.com/en/US/products/ps7287/tsd_products_support_series_home.html

Pour configurer le point d'accès à l'aide de l'assistant CCA, procédez comme suit :

- ÉTAPE 1** Connectez le port Ethernet du point d'accès à un port de commutation sur un périphérique SBCS.
- ÉTAPE 2** Mettez le Cisco AP54 1N sous tension.
- ÉTAPE 3** Connectez un ordinateur sur lequel l'assistant CCA est installé à n'importe quel port de commutation d'accès du routeur UC520 ou SR520.
- ÉTAPE 4** Créez un site CCA en saisissant un nom et l'adresse IP du routeur UC520 ou SR520.
- ÉTAPE 5** Connectez-vous au site CCA à l'aide des informations d'identification de connexion appropriées.

ÉTAPE 6 Cliquez sur **Window > Topology View**.

Une fois que vous êtes connecté au site CCA et lorsque les périphériques ont été repérés, la carte topologique contient le Cisco AP541N.



REMARQUE Les périphériques autres que ceux de Cisco connectés au commutateur n'apparaissent pas dans la carte topologique.

ÉTAPE 7 Cliquez avec le bouton droit de la souris sur le point d'accès pour afficher les options suivantes : Configuration Utility, Properties et Annotation.**ÉTAPE 8** Cliquez sur **Configuration Utility**.

L'*Utilitaire de configuration du point d'accès* apparaît dans une nouvelle fenêtre, comme illustré dans la [Figure 4](#).

Ensuite, nous vous recommandons d'effectuer les actions suivantes :

- Modifiez le mot de passe en cliquant sur **Change Administrator Password**.
 - Configurez le SSID et activez la sécurité sans fil, en cliquant sur **Configure Wireless Networks (SSIDs)**.
 - Activez la radio sans fil en cliquant sur **Enable Wireless Radio**.
 - Attribuez une nouvelle adresse IP statique au point d'accès si vos périphériques réseau sont configurés avec des adresses IP statiques, en cliquant sur **Set LAN IP Address**.
-

Afficher l'utilitaire de configuration en utilisant une autre adresse IP

Vous pouvez afficher l'*Utilitaire de configuration du point d'accès* en utilisant une adresse IP attribuée au point d'accès lors d'une précédente configuration ou par un serveur DHCP.

Lorsque vous mettez le point d'accès sous tension, le client DHCP intégré recherche un serveur DHCP sur le réseau pour obtenir une adresse IP et d'autres informations sur le réseau. Si le point d'accès ne trouve pas de serveur DHCP sur le réseau, le point d'accès utilise son adresse IP statique par défaut (192.168.10.10), sauf si vous lui avez attribué une adresse IP statique (et spécifié une stratégie d'adressage IP statique) ou jusqu'à ce que le point d'accès récupère des informations sur le réseau à partir du serveur DHCP.



AVERTISSEMENT

Si l'adresse IP du point d'accès est modifiée, manuellement ou par un serveur DHCP, votre lien vers le point d'accès sera perdu et vous devrez saisir la nouvelle adresse IP pour utiliser l'*Utilitaire de configuration du point d'accès*.

Pour configurer le point d'accès en utilisant une adresse IP différente de l'adresse IP statique par défaut, procédez comme suit :

ÉTAPE 1 Mettez le Cisco AP541N sous tension.

ÉTAPE 2 Si vous avez utilisé un serveur DHCP sur votre réseau pour configurer automatiquement les informations réseau pour le point d'accès, saisissez l'adresse IP attribuée au point d'accès par le serveur DHCP dans le navigateur Web.

Si vous avez accès au serveur DHCP sur votre réseau et si vous connaissez l'adresse MAC de votre point d'accès, vous pouvez visualiser l'adresse IP associée à l'adresse MAC du point d'accès. Sinon, nous vous recommandons de déconnecter le point d'accès du réseau, de le réinitialiser sur la configuration par défaut à l'aide de la procédure dans la section « **Réinitialisation du périphérique à l'aide du bouton Reset** », et de configurer le périphérique en suivant la procédure de la section « **Afficher l'utilitaire de configuration en utilisant l'adresse IP par défaut** ».

Si vous avez remplacé l'adresse IP statique par défaut par une nouvelle adresse IP statique, saisissez la nouvelle adresse IP du point d'accès dans le navigateur Web.

La fenêtre **Login** apparaît, comme illustré dans la **Figure 3**.

ÉTAPE 3 Saisissez les informations de connexion :

Le nom d'utilisateur est **cisco**.

Le mot de passe par défaut est *cisco* (les mots de passe sont sensibles à la casse).

Lorsque vous vous connectez, la page **Getting Started** de l'Utilitaire de configuration du point d'accès apparaît, comme illustré dans la **Figure 4**.

ÉTAPE 4 Mettez à jour le logiciel Cisco AP 541N avec la dernière version en cliquant sur le lien **Software Upgrade**, comme illustré dans la **Figure 4**.

Ensuite, nous vous recommandons d'effectuer les actions suivantes :

- Modifiez le mot de passe en cliquant sur **Change Administrator Password**.
- Configurez le SSID et activez la sécurité sans fil, en cliquant sur **Configure Wireless Networks (SSIDs)**.
- Activez la radio sans fil en cliquant sur **Enable Wireless Radio**.
- Attribuez une nouvelle adresse IP statique au point d'accès si vos périphériques réseau sont configurés avec des adresses IP statiques, en cliquant sur **Set LAN IP Address**.



AVERTISSEMENT Si vous ne disposez pas d'un serveur DHCP dans votre réseau interne et que vous n'avez pas l'intention d'en utiliser un, nous vous recommandons d'utiliser une nouvelle adresse IP, de sorte que si vous activez un autre WLAN Cisco AP541N sur le même réseau, l'adresse IP pour chaque point d'accès soit unique. Si l'adresse IP n'est pas unique, cela entraîne un conflit provoquant des résultats imprévisibles.

Pour modifier le type de connexion et attribuer une adresse IP statique en utilisant l'*Utilitaire de configuration du point d'accès*, reportez-vous à **Paramètres LAN**, page 47.

Dépannage de votre connexion

Si vous ne pouvez pas afficher la fenêtre de connexion, vous pouvez tester l'adresse IP à l'aide de la **commande** ping. Si vous ne connaissez pas l'adresse IP, vous pouvez configurer le périphérique en le réinitialisant sur la configuration d'usine par défaut et en accédant à l'*Utilitaire de configuration du point d'accès* à l'aide de l'adresse IP par défaut.

Utilisation de la commande ping pour tester la connexion

Si vous ne pouvez pas afficher l'utilitaire de configuration, vous pouvez tester la capacité de l'ordinateur à communiquer avec le point d'accès à l'aide de la commande **ping**. Pour utiliser la commande **ping** sur un ordinateur exécutant Windows, procédez comme suit :

-
- ÉTAPE 1** Assurez-vous que le Cisco AP 541N est mis sous tension et que les DEL indiquent les liens appropriés.
- ÉTAPE 2** Ouvrez une fenêtre de commande en utilisant **Start > Run** et saisissez **cmd**.
- ÉTAPE 3** Lorsque vous y serez invité par la fenêtre **Command**, saisissez **ping** ainsi que *point d'accès* l'adresse IP. Par exemple, **ping 192.168.10.10** (l'adresse IP statique par défaut du point d'accès).

Si l'opération a réussi, vous obtiendrez une réponse semblable à la suivante :

```
Pinging 192.168.10.10 with 32 bytes of data:  
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128  
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128  
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
```

Si l'opération a échoué, vous utilisez sans doute la mauvaise adresse IP du point d'accès et vous obtiendrez une réponse semblable à la suivante :

```
Pinging 192.168.10.10 with 32 bytes of data:  
Request timed out.
```

Cause possible de l'échec

La cause la plus probable de l'échec de la connectivité est l'utilisation d'une adresse IP incorrecte.

Le navigateur Web pointe vers une mauvaise adresse IP. Votre ordinateur peut également être configuré avec une adresse IP qui n'est pas située dans le même sous-réseau que le point d'accès.

Le serveur DHCP est activé sur le Cisco AP 541N par défaut. Lorsqu'un serveur DHCP est activé sur votre réseau et que le point d'accès est connecté au réseau, le serveur DHCP remplace l'adresse IP statique par défaut par une adresse IP qu'il attribue lui-même. Si cela survient avant que vous n'affichiez la fenêtre *Utilitaire de configuration du point d'accès*, vous devez utiliser l'adresse IP pour afficher l'utilitaire. Si cela survient pendant la configuration, l'*Utilitaire de configuration du point d'accès* perdra sa connectivité.

Vous pouvez interroger le serveur DHCP concernant la nouvelle adresse IP ou déconnecter le point d'accès du réseau et réinitialiser le périphérique pour utiliser l'adresse IP statique du point d'accès par défaut en utilisant la procédure **Réinitialisation de la configuration par défaut du point d'accès, page 132**.

Réinitialisation du périphérique à l'aide du bouton Reset

Pour utiliser le bouton **Reset** afin de redémarrer ou réinitialiser le point d'accès, procédez comme suit :

- Pour **redémarrer** le point d'accès, appuyez sur le bouton **Reset**. Ne le maintenez pas enfoncé pendant plus de 10 secondes.
- Pour **restaurer** les paramètres par défaut du point d'accès, procédez comme suit :
 1. Déconnectez le point d'accès du réseau ou désactivez tous les serveurs DHCP de votre réseau.
 2. Lorsque le périphérique est sous tension, appuyez sur le bouton **Reset** et maintenez-le enfoncé pendant plus de 10 secondes.

Configuration du point d'accès à l'aide de la page Getting Started

À partir de la page **Getting Started**, vous pouvez utiliser les liens suivants pour configurer rapidement votre point d'accès :

- [Configuration du point d'accès](#)
- [Page Access Point Management](#)
- [Page Wireless Configuration](#)

Configuration du point d'accès

Pour modifier l'adresse IP, le mot de passe et la configuration VLAN du point d'accès, procédez comme suit :

-
- ÉTAPE 1** Cliquez sur **Change Administrator Password** afin de fournir un nouveau mot de passe d'administration pour le point d'accès. (Le nom d'utilisateur est **cisco** et ne peut pas être modifié. Le mot de passe par défaut est *cisco*.)
- ÉTAPE 2** Si vous ne disposez pas d'un serveur DHCP sur le réseau et que vous n'avez pas l'intention d'en utiliser un, cliquez sur **Change IP Address** pour passer d'une connexion de type DHCP à une connexion de type IP statique et définissez une adresse IP statique ainsi qu'un masque de sous-réseau.



REMARQUE Nous vous recommandons d'attribuer une nouvelle adresse IP statique. Sinon, si vous activez un autre Cisco AP 541N sur le même réseau, l'adresse IP pour chaque point d'accès ne sera pas unique. La duplication d'une adresse IP sur un réseau entraînera un conflit.

En outre, si vous modifiez l'adresse IP statique, vous perdrez la connectivité. Pour rétablir la connectivité, saisissez la nouvelle adresse IP dans votre navigateur Web et connectez-vous à l'Utilitaire de configuration.

Pour modifier le type de connexion et attribuer une adresse IP statique, reportez-vous à [Paramètres LAN, page 47](#).

- ÉTAPE 3** Si votre réseau utilise des VLAN, vous devrez peut-être configurer l'ID VLAN de gestion ou non balisé sur le point d'accès pour qu'il fonctionne avec votre réseau.
- Pour obtenir des informations concernant la configuration des informations sur les VLAN, reportez-vous à [Paramètres LAN, page 47](#).
- ÉTAPE 4** Si votre réseau utilise la sécurité de ports WEP dynamique pour contrôler l'accès au réseau, vous devez configurer les informations du demandeur 802.1X sur le point d'accès. Pour obtenir plus d'informations concernant la configuration du nom d'utilisateur et du mot de passe 802.1X, reportez-vous à [Configuration de l'authentification 802.1X, page 51](#).
-

Page Access Point Management

Cliquez sur **System Information** pour afficher les informations sur le périphérique. Pour obtenir plus d'informations, reportez-vous à [Informations périphérique, page 33](#).

Lorsque de nouvelles versions du logiciel de point d'accès sont disponibles, vous pouvez mettre à niveau le logiciel sur vos périphériques pour bénéficier des nouvelles fonctionnalités et améliorations. Pour obtenir plus d'informations, reportez-vous à [Mise à niveau du logiciel, page 135](#).

Pour obtenir des informations concernant la sauvegarde et la restauration de la configuration, consultez [Configuration du point d'accès, page 131](#).

Page Wireless Configuration

Pour obtenir plus d'informations concernant les paramètres de la radio sans fil, reportez-vous à [Configuration des paramètres de la radio sans fil, page 173](#).

Pour configurer le SSID, l'accès invité et la configuration de sécurité, reportez-vous à [Modification des paramètres de point d'accès virtuel, page 63](#).

Configuration requise du client

Le point d'accès fournit un accès sans fil à n'importe quel client disposant d'un adaptateur client Wi-Fi configuré pour le mode 802.11 dans lequel le point d'accès est exécuté. Le point d'accès prend en charge plusieurs systèmes d'exploitation client. Les clients peuvent être des ordinateurs de bureau ou portables, des assistants numériques personnels (PDA) ou tout autre périphérique portable, portable ou fixe équipé d'un adaptateur Wi-Fi et prenant en charge les pilotes.

Pour vous connecter au point d'accès, les clients sans fil ont besoin des logiciels et matériels décrits dans le [Tableau 2](#).

Tableau 2 Configuration requise pour les clients sans fil

Composant requis	Description
Adaptateur client Wi-Fi	Adaptateur client Wi-Fi portable ou intégré prenant en charge au moins l'un des modes IEEE 802.11 dans lesquels vous avez l'intention d'exécuter le point d'accès. (Les modes IEEE 802.11a, 802.11b, 802.11g et 802.11n sont pris en charge.)
Logiciel client sans fil	Logiciel client, tel que Microsoft Windows Suppliquant, configuré pour être associé au point d'accès.
Paramètres de la sécurité client	<p>La sécurité doit être désactivée sur le client utilisé pour effectuer la configuration initiale du point d'accès.</p> <p>Si le mode de sécurité du point d'accès n'est pas défini sur texte brut, les clients sans fil doivent avoir un profil défini sur le même mode d'authentification que celui utilisé par le point d'accès et fournir un nom d'utilisateur et un mot de passe valides, un certificat ou l'identité utilisateur requise par le serveur d'authentification. Les modes de sécurité sont WEP statique, IEEE 802.1X, WPA avec serveur RADIUS et PSK-WPA.</p> <p>Pour obtenir des informations concernant la configuration de la sécurité sur le point d'accès, reportez-vous à Configuration du système de distribution sans fil (WDS), page 100.</p>

Vérification de l'installation

Assurez-vous que le point d'accès est connecté au LAN et associé aux clients sans fil sur le réseau. Une fois les bases de votre réseau sans fil testées, vous pouvez activer davantage de sécurité et affiner le point d'accès en modifiant les fonctionnalités de configuration avancées.

ÉTAPE 1 Connectez le point d'accès au LAN.

Si vous avez configuré le point d'accès en utilisant une connexion par câble directe de votre ordinateur au point d'accès, procédez comme suit :

- a. Débranchez le câble de l'ordinateur et du point d'accès.
- b. Montez le point d'accès à l'emplacement souhaité.
- c. Connectez un câble Ethernet du point d'accès au LAN.
- d. Mettez le point d'accès sous tension.
- e. Connectez votre ordinateur au LAN à l'aide d'un câble Ethernet ou d'une carte sans fil.

Si vous avez configuré un point d'accès et un ordinateur d'administrateur en les connectant tous les deux à un hub ou à un commutateur réseau, votre point d'accès est déjà connecté au LAN. La prochaine étape consiste à tester quelques clients sans fil.

ÉTAPE 2 Testez le point d'accès en essayant de le détecter et de l'associer à un client sans fil. Pour obtenir des informations concernant la configuration requise pour les périphériques client, reportez-vous à [Configuration requise du client, page 29](#).



REMARQUE Le point d'accès n'est pas conçu pour des modifications de configuration multiples et simultanées. Si plus d'un administrateur est connecté à l'Utilitaire de configuration et modifie la configuration, rien ne garantit que toutes les modifications de configuration spécifiées par plusieurs utilisateurs seront appliquées.

**AVERTISSEMENT**

Par défaut, aucune sécurité n'est activée sur le point d'accès, par conséquent, n'importe quel client peut y être associé et accéder à votre LAN, y compris les périphériques non autorisés. L'étape suivante est également très importante : il s'agit de configurer la sécurité. Pour obtenir plus d'informations, poursuivez avec [Configuration de la sécurité sur le point d'accès sans fil, page 31](#).

Configuration de la sécurité sur le point d'accès sans fil

Vous pouvez définir un accès client sans fil sécurisé en configurant la sécurité pour chaque point d'accès virtuel (VAP) activé. Vous pouvez configurer jusqu'à 16 points d'accès virtuels par radio sans fil qui stimulent plusieurs points d'accès sur un point d'accès physique. Pour chaque point d'accès virtuel, vous pouvez configurer un mode de sécurité unique pour contrôler l'accès client sans fil.

Chaque radio sans fil possède 16 points d'accès virtuels, portant des ID de VAP compris entre 0 et 15. Les points d'accès virtuels VAP 0, VAP 1 et VAP 2 disposent de paramètres par défaut différents de ceux des points d'accès virtuels 3 à 15. Par défaut, les points d'accès virtuels VAP 0, VAP 1, et VAP 2 sont activés.

VAP0 dispose des paramètres par défaut suivants :

- ID VLAN : 1
- SSID : cisco-data
- Diffusion SSID : activée
- Sécurité : aucune
- Type d'authentification MAC : activée
- Isolation de la station : désactivée
- Redirection HTTP : désactivée

VAP1 dispose des paramètres par défaut suivants :

- ID VLAN : 100
- SSID : cisco-voice
- Diffusion SSID : activée
- Sécurité : aucune

- Type d'authentification MAC : activée
- Isolation de la station : désactivée
- Redirection HTTP : désactivée

VAP2 dispose des paramètres par défaut suivants :

- ID VLAN : 1
- SSID : cisco-scan
- Diffusion SSID : activée
- Sécurité : WPA Personal
- Versions WPA : WPA2
- Suites d'algorithmes : CCMP (AES)
- Clé : intermec
- Type d'authentification MAC : activée
- Isolation de la station : désactivée
- Redirection HTTP : désactivée

Les points d'accès virtuels VAP3 à 15 sont désactivés par défaut. Lorsqu'ils sont activés, ils disposent des paramètres par défaut suivants :

- ID VLAN : 1
- SSID : point d'accès virtuel x (où x est l'ID du point d'accès virtuel)
- Diffusion SSID : activée
- Sécurité : aucune
- Type d'authentification MAC : activée
- Isolation de la station : désactivée
- Redirection HTTP : désactivée

Pour empêcher l'accès non autorisé au point d'accès, nous vous recommandons de sélectionner et de configurer une option de sécurité autre que None pour le point d'accès virtuel par défaut et pour tous ceux que vous activez.

Pour obtenir des informations concernant la configuration des paramètres de sécurité de chaque point d'accès virtuel, reportez-vous à [Configuration du système de distribution sans fil \(WDS\), page 100](#).

État

La page Status fournit des informations sur les éléments suivants :

- **Informations périphérique**
- **Interfaces réseau**
- **Statistiques de trafic**
- **Clients associés**
- **Détection des points d'accès indésirables**

Informations périphérique

Vous pouvez afficher les informations relatives au matériel et au produit sur la page **Device Information**.

Figure 5 Informations périphérique

The screenshot displays the Cisco AP 541N web interface. The top navigation bar includes 'Getting Started', 'Status' (highlighted), 'Setup', 'Wireless', 'SNMP', 'Administration', and 'Cluster'. Below this, a sub-menu contains 'Device Information' (highlighted), 'Network Interfaces', 'Traffic Statistics', 'Associated Clients', and 'Rogue AP Detection'. The main content area is titled 'Device Information' and lists the following details:

Product Identifier:	AP541N
Hardware Version:	V01
Software Version:	8-22.1(0)
Serial Number:	DNI13110010
Device Name:	AP541N-A-K9
Device Description:	802.11n Dual Band Access Point - Single Radio
System Uptime:	2 days, 15 hours, 28 minutes
System Time:	Tue Aug 25 2009 15:21:19 UTC

Tableau 3 décrit les champs affichés sur la page **Device Information**.

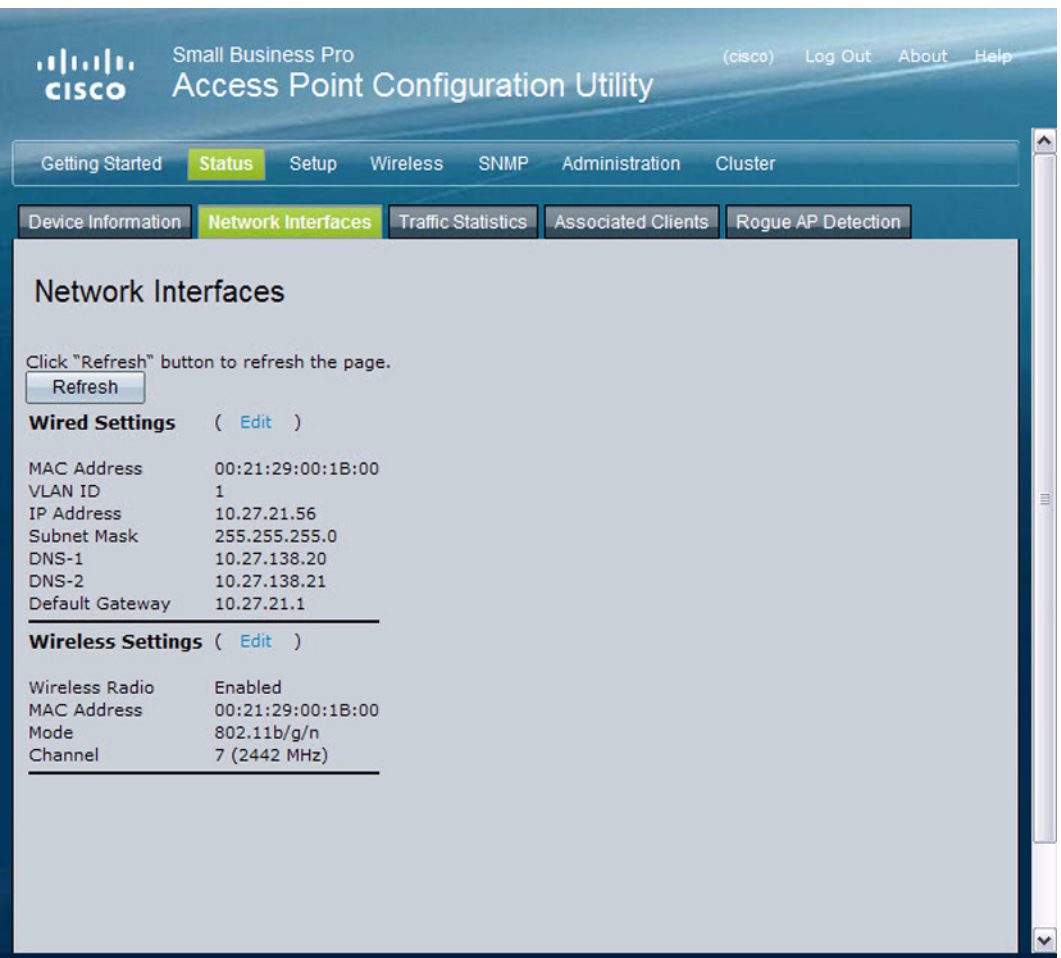
Tableau 3 Page Device Information

Champ	Description
Product Identifier	Identifie le modèle matériel du point d'accès.
Hardware Version	Identifie la version matérielle du point d'accès.
Software Version	Affiche les informations relatives à la version du logiciel installé sur le point d'accès. Mettez à niveau le logiciel lorsque de nouvelles versions du logiciel du point d'accès WLAN sont disponibles.
Serial Number	Affiche le numéro de série du point d'accès.
Device Name	Nom générique permettant d'identifier le type de matériel.
Device Description	Fournit des informations sur le matériel du produit.
System Uptime	Durée de fonctionnement du point d'accès depuis sa dernière mise sous tension ou son dernier redémarrage.

Interfaces réseau

La fenêtre Network Interface Status affiche les **Wired Settings** actuels et les **Wireless Settings** du point d'accès. Cliquez sur **Refresh** pour actualiser la page.

Figure 6 État de l'interface



The screenshot displays the Cisco Small Business Pro Access Point Configuration Utility interface. The main navigation bar includes 'Getting Started', 'Status' (highlighted), 'Setup', 'Wireless', 'SNMP', 'Administration', and 'Cluster'. Below this, a secondary navigation bar shows 'Device Information', 'Network Interfaces' (highlighted), 'Traffic Statistics', 'Associated Clients', and 'Rogue AP Detection'. The 'Network Interfaces' section contains a 'Refresh' button and instructions: 'Click "Refresh" button to refresh the page.' Below this, there are two sections: 'Wired Settings' and 'Wireless Settings', each with an 'Edit' link. The 'Wired Settings' table lists: MAC Address (00:21:29:00:1B:00), VLAN ID (1), IP Address (10.27.21.56), Subnet Mask (255.255.255.0), DNS-1 (10.27.138.20), DNS-2 (10.27.138.21), and Default Gateway (10.27.21.1). The 'Wireless Settings' table lists: Wireless Radio (Enabled), MAC Address (00:21:29:00:1B:00), Mode (802.11b/g/n), and Channel (7 (2442 MHz)).

Wired Settings

Les paramètres câblés comprennent l'adresse MAC, l'ID du VLAN de gestion, l'adresse IP, le masque de sous-réseau et les informations DNS. Pour modifier ces paramètres, cliquez sur **Edit** pour être redirigé sur la page **Setup > LAN Settings**.

Pour obtenir plus d'informations sur la configuration de ces paramètres, reportez-vous à **Paramètres LAN, page 47**.

Wireless Settings

La section **Wireless Settings** indique l'état du radio sans fil et comprend le mode Radio et Channel. La section **Wireless Settings** affiche également l'adresse MAC (lecture seule) associée à chaque interface radio sans fil.

Pour modifier les paramètres du mode Radio ou du canal, cliquez sur **Edit**. Vous êtes redirigé sur la page **Wireless > Radio Settings**.

Pour obtenir plus d'informations sur la configuration de ces paramètres, reportez-vous à [Modification des paramètres radio sans fil, page 59](#) et [Modification des paramètres avancés, page 89](#).

Statistiques de trafic

La page **Traffic Statistics** fournit des informations de base sur le point d'accès, un affichage en temps réel des statistiques d'envoi et de réception de l'interface Ethernet et les statistiques du VAP (point d'accès virtuel). Les statistiques d'envoi et de réception correspondent aux totaux depuis le dernier démarrage du point d'accès. En cas de redémarrage du point d'accès, ces chiffres indiquent les totaux d'envoi et de réception depuis le redémarrage.

Pour afficher les statistiques d'envoi et de réception du point d'accès, cliquez sur l'onglet **Traffic Statistics**. Cliquez sur **Refresh** pour actualiser la page.

Figure 7 Affichage des statistiques de trafic

Click "Refresh" button to refresh the page.

Network Interfaces	Status	MAC Address	VLAN ID	Name (SSID)
LAN	up	00:21:29:00:00:E0	1	NA
vap0	up	00:21:29:00:00:E0	1	cisco-data
vap1	up	00:21:29:00:00:E1	1	cisco-voice
vap2	down		1	Virtual Access
vap3	down		1	Virtual Access
vap4	down		1	Virtual Access
vap5	down		1	Virtual Access
vap6	down		1	Virtual Access
vap7	down		1	Virtual Access
vap8	down		1	Virtual Access
vap9	down		1	Virtual Access
vap10	down		1	Virtual Access
vap11	down		1	Virtual Access
vap12	down		1	Virtual Access
vap13	down		1	Virtual Access
vap14	down		1	Virtual Access
vap15	down		1	Virtual Access
wlan0wds0	down		NA	NA
wlan0wds1	down		NA	NA
wlan0wds2	down		NA	NA
wlan0wds3	down		NA	NA

Transmit				
Network Interfaces	Total packets	Total bytes	Total dropped packets	Total dropped bytes
LAN	54480	37507534	0	0
vap0	408405	42983291	NA	NA
vap1	435605	46921280	NA	NA
vap2	0	0	NA	NA

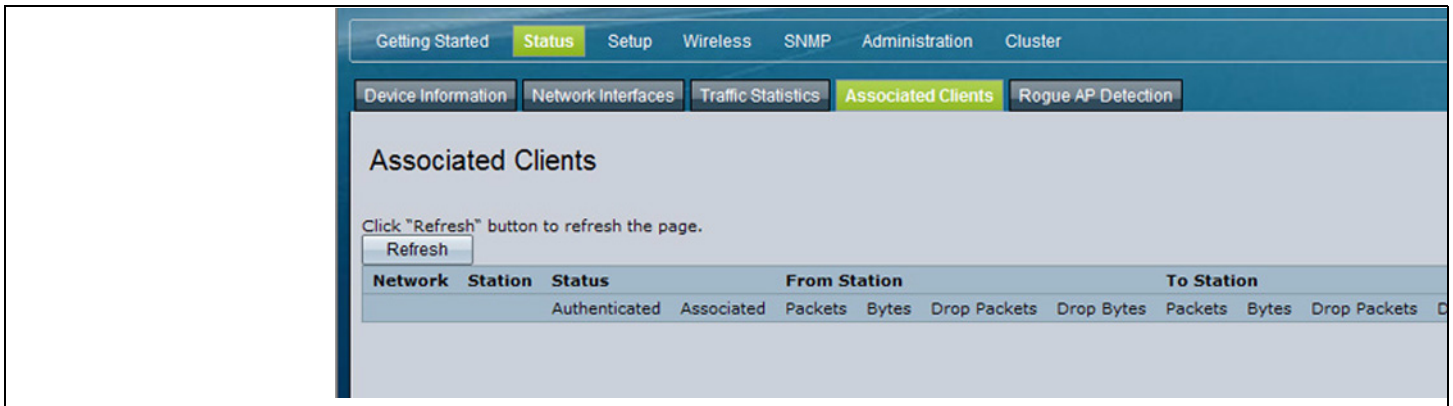
Tableau 4 Description des statistiques de trafic

Champ	Description
Network Interfaces	Nom des interfaces Ethernet ou VAP.
Status	Indique si l'interface est active ou non.
MAC Address	Adresse MAC de l'interface spécifiée. Chaque interface VAP possède une adresse MAC unique.
VLAN ID	Un ID de réseau LAN (VLAN) virtuel est utilisé pour établir plusieurs réseaux sur le même point d'accès. L'ID du VLAN est configuré à l'aide de Wireless > onglet VAP. (Reportez-vous à l' Utilisation de la bande passante, page 106.)
Name (SSID)	Le nom du réseau, également appelé SSID, est une clé alphanumérique permettant d'identifier un VAP de manière unique. Le nom (SSID) est configuré à l'aide de l'onglet VAP. (Reportez-vous à l' Utilisation de la bande passante, page 106.) NA indique que l'entrée n'est pas applicable ou n'est pas prise en charge.
<i>Informations de transmission et de réception</i>	
Total Packets	Indique le nombre total de paquets envoyés (dans le tableau Transmit) ou reçus (dans le tableau Received) sur cette interface.
Total Bytes	Indique le nombre total d'octets envoyés (dans le tableau Transmit) ou reçus (dans le tableau Received) sur cette interface.
Total Dropped Packets	Indique le nombre total de paquets rejetés envoyés (dans le tableau Transmit) ou reçus (dans le tableau Received) sur cette interface. NA indique que les compteurs de rejets et d'erreurs des interfaces VAP et des interfaces WDS ne sont pas pris en charge.
Total Dropped Bytes	Indique le nombre total d'octets rejetés envoyés (dans le tableau Transmit) ou reçus (dans le tableau Received) sur cette interface. NA indique que les compteurs de rejets et d'erreurs des interfaces VAP et des interfaces WDS ne sont pas pris en charge.
Errors	Affiche le nombre total d'erreurs de transmission et de réception détecté par le point d'accès. NA indique que les compteurs de rejets et d'erreurs des interfaces VAP et des interfaces WDS ne sont pas pris en charge.

Clients associés

Pour afficher les stations clientes associées au point d'accès, cliquez sur l'onglet **Associated Clients**.

Figure 8 Affichage des informations concernant l'association de clients



Les stations associées s'affichent avec les informations concernant le trafic de paquets transmis et reçus par chaque station. Cliquez sur **Refresh** pour actualiser la page.

Le **Tableau 5** décrit les champs de la page **Associated Clients**.

Tableau 5 Description des champs de la page **Associated Clients**

Champ	Description
Network	Affiche le point d'accès virtuel auquel le client est associé. Par exemple, l'entrée wlan0vap2 signifie que le client est associé à la radio sans fil 1 et au point d'accès virtuel 2.
Station	Affiche l'adresse MAC du client sans fil associé.

Tableau 5 Description des champs de la page Associated Clients (suite)

Champ	Description
Status	<p>L'état Authenticated et Associated affiche l'état d'authentification et d'association IEEE 802.11 sous-jacent, quel que soit le type de sécurité utilisé par le client pour se connecter au point d'accès. Cet état ne permet pas l'affichage de l'état d'authentification ou d'association IEEE 802.1X.</p> <p>Certains points concernant ce champ doivent être pris en considération :</p> <ul style="list-style-type: none"> ▪ Si le mode de sécurité du point d'accès est réglé sur None ou Static WEP, l'état d'authentification et d'association des clients affichés dans l'onglet Client Associations doit être conforme aux exigences. C'est-à-dire que, si un client apparaît comme authentifié par le point d'accès, il sera en mesure de transmettre et de recevoir des données. (Cela car le WEP statique utilise uniquement une authentification IEEE 802.11.) ▪ Cependant, si le point d'accès utilise la sécurité IEEE 802.1X ou WPA, il est possible que l'association client s'affiche comme authentifiée dans cet onglet (à l'aide de la sécurité IEEE 802.11) alors qu'elle n'est pas authentifiée par le point d'accès en utilisant la deuxième couche de sécurité.
From Station	Affiche le nombre de paquets et d'octets reçus depuis le client sans fil et le nombre de paquets et d'octets rejetés après réception.
To Station	Affiche le nombre de paquets et d'octets transmis depuis le point d'accès au client sans fil et le nombre de paquets et d'octets rejetés durant la transmission.

Surveillance de l'intégrité de la liaison

Le point d'accès permet la surveillance de l'intégrité de la liaison pour vérifier en continu ses connexions avec chacun des clients associés. Pour ce faire, le point d'accès envoie toutes les secondes des paquets de données aux clients si aucun autre trafic ne circule. Cela permet au point d'accès de détecter lorsqu'un client dépasse la plage définie, même durant les périodes sans échange de trafic normal. La connexion du client rejette la liste après 300 secondes si ces paquets de données ne sont pas reconnus, même si aucun message de dissociation n'est reçu.

Détection des points d'accès indésirables

Un point d'accès indésirable est un point d'accès installé sur un réseau sécurisé sans autorisation de l'administrateur système. Les points d'accès indésirables constituent une menace de sécurité car toute personne ayant accès aux locaux peut installer, par ignorance ou malveillance, un point d'accès sans fil permettant aux personnes non autorisées d'accéder au réseau.

La page **Rogue AP Detection** affiche les informations concernant tous les points d'accès détectés par le Cisco AP 541N à proximité du réseau. Si le point d'accès identifié comme indésirable est en réalité un point d'accès légitime, vous pouvez l'ajouter à la liste des points d'accès connus. Cliquez sur **Refresh** pour actualiser la page.



REMARQUE

La liste des points d'accès indésirables détectés et la liste des points d'accès connus fournissent des informations. Le modèle Cisco AP 541N n'a aucun contrôle sur les points d'accès figurant sur les listes et ne peut pas appliquer de stratégie de sécurité aux points d'accès détectés par le système d'analyse RF.

Figure 9 Affichage des points d'accès voisins

Action	MAC	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Grant	00:21:29:00:03:00	100	AP	(Non Broadcasting)	Off	Off	2.4	6	1	📶	562342	Sun Jul 26 18:06:40 1970	1.2.5.5.11.18.24.3
Grant	00:10:18:02:d2:c0	100	AP	B120Nain_1	Off	Off	2.4	6	1	📶	131609	Sat Jul 25 14:12:32 1970	1.2.5.5.11.18.24.3
Grant	00:90:4c:08:ad:00	100	AP	Broadcom VAP	Off	Off	2.4	2	1	📶	29177	Sun Jul 26 18:02:43 1970	1.2.5.5.11.18.24.3
Grant	00:1b:e9:16:26:00	100	AP	Broadcom VAP	Off	Off	2.4	2	1	📶	11787	Sun Jul 26 15:26:43 1970	1.2.5.5.11.18.24.3
Grant	00:21:29:00:1c:70	100	AP	B120Nain_1	Off	Off	2.4	6	1	📶	20370	Sat Jul 25 14:32:30 1970	1.2.5.5.11.18.24.3
Grant	00:1b:e9:16:29:80	100	AP	HSHI BRCH 1	On	On	2.4	5	1	📶	53	Sun Jul 26 14:22:54 1970	1.2.5.5.11.18.24.3
Grant	00:0e:84:e2:11:50	100	AP	bromepa	On	On	2.4	1	1	📶	31051	Sun Jul 26 17:59:43 1970	1.2.5.5.6.9.11.12.1
Grant	00:14:2a:ba:eb:50	100	AP	NETGEAR_11g	Off	Off	2.4	1	1	📶	21163	Sun Jul 26 17:59:36 1970	1.2.5.5.11.6.9.12.
Grant	00:14:2a:ba:eb:51	100	AP	NETGEAR_11g-1	Off	Off	2.4	1	1	📶	19801	Sun Jul 26 17:59:36 1970	1.2.5.5.11.6.9.12.
Grant	00:1b:e9:16:22:80	100	AP	TRG_TestSSID	Off	Off	2.4	1	1	📶	549	Sun Jul 26 17:59:25 1970	1.2.5.5.11.18.24.3
Grant	00:02:bc:00:13:80	100	AP	dbbicgtest1	On	On	2.4	6	1	📶	93	Sun Jul 26 16:46:41 1970	1.2.5.5.11.18.24.3
Grant	00:21:29:00:06:20	100	AP	MFLSrv0	On	Off	2.4	8	1	📶	24	Sun Jul 26 17:45:17 1970	1.2.5.5.11.18.24.3
Grant	00:1b:e9:16:34:c2	100	AP	GP Net 2	On	On	2.4	11	1	📶	12	Sun Jul 26 16:29:41 1970	1.2.5.5.11.18.24.3
Grant	00:90:4c:06:28:90	100	AP	juniper-default	On	Off	2.4	3	1	📶	6487	Sat Jul 25 15:27:52 1970	1.2.5.5.11.18.24.3
Grant	00:22:80:3a:c2:10	100	AP	(Non Broadcasting)	Off	Off	2.4	1	1	📶	6	Sun Jul 26 17:04:42 1970	1.2.5.5.11.18.24.3
Grant	00:0e:84:f5:f2:d0	100	AP	bromepa	On	On	2.4	6	1	📶	61	Sun Jul 26 18:05:44 1970	1.2.5.5.6.9.11.12.1
Grant	00:21:29:00:17:60	100	AP	LOCATION	On	On	2.4	11	1	📶	11	Sun Jul 26 17:14:42 1970	1.2.5.5.11.18.24.3
Grant	00:21:29:00:11:20	100	AP	LOCATION	On	On	2.4	11	1	📶	10	Sun Jul 26 15:46:39 1970	1.2.5.5.11.18.24.3
Grant	00:21:29:00:17:40	100	AP	LOCATION	On	On	2.4	11	1	📶	9	Sun Jul 26 13:01:34 1970	1.2.5.5.11.18.24.3
Grant	00:1f:12:e0:86:d0	100	AP	juniper-default	On	Off	2.4	3	1	📶	45187	Sun Jul 26 18:03:44 1970	1.2.5.5.11.18.24.3
Grant	00:90:4c:08:ad:40	100	AP	Broadcom VAP	Off	Off	2.4	2	1	📶	3	Sat Jul 25 19:25:30 1970	1.2.5.5.11.18.24.3
Grant	00:90:4c:08:ad:80	100	AP	Broadcom VAP	Off	Off	2.4	7	1	📶	5410	Sat Jul 25 22:38:22 1970	1.2.5.5.11.18.24.3
Grant	00:0c:41:d7:ee:a7	100	AP	b6oronewap54gv11	On	Off	2.4	1	1	📶	3	Sun Jul 26 13:35:35 1970	1.2.5.5.11.18.24.3
Grant	00:21:29:00:11:00	100	AP	LOCATION	On	On	2.4	11	1	📶	1	Sun Jul 26 01:28:12 1970	1.2.5.5.11.18.24.3
Grant	00:1b:e9:16:25:c0	100	AP	edfdf	On	On	2.4	6	1	📶	2	Sun Jul 26 04:19:17 1970	1.2.5.5.11.18.24.3

Vous devez activer la détection du point d'accès pour rassembler des informations sur les autres points d'accès situés dans la plage. Le **Tableau 6** décrit les informations sur les autres points d'accès situés dans la plage.

Tableau 6 Informations relatives aux points d'accès voisins

Champ	Description
AP Detection	<p>Pour activer la détection du point d'accès voisin et rassembler des informations sur les points d'accès voisins, cliquez sur Enabled. (par défaut)</p> <p>Pour désactiver la détection du point d'accès voisin, cliquez sur Disabled.</p> <p>Cliquez sur Apply pour enregistrer les paramètres.</p>

Tableau 6 Informations relatives aux points d'accès voisins (suite)

Champ	Description
Action	<p>Si un point d'accès figure dans la liste des points d'accès indésirables détectés, cliquez sur Grant pour déplacer le point d'accès de la liste des points d'accès indésirables détectés vers la liste des points d'accès connus.</p> <p>Si un point d'accès figure dans la liste des points d'accès connus, cliquez sur le bouton Delete pour déplacer le point d'accès de la liste des points d'accès connus vers la liste des points d'accès indésirables détectés.</p> <p>REMARQUE : La liste des points d'accès indésirables détectés et la liste des points d'accès connus figurent à titre d'information uniquement. Le modèle Cisco AP 541N n'a aucun contrôle sur les points d'accès figurant dans la liste et ne peuvent pas appliquer de stratégie de sécurité aux points d'accès détectés par le système d'analyse RF.</p>
MAC	Affiche l'adresse MAC du point d'accès détecté.
Beacon Int.	<p>Affiche l'intervalle de balise d'un autre point d'accès.</p> <p>Les trames de balise sont transmises à intervalles réguliers par le point d'accès pour annoncer leur présence sur le réseau sans fil. La procédure par défaut consiste à envoyer une trame de balise toutes les 100 millisecondes (ou 10 par seconde).</p> <p>L'intervalle de balise de votre point d'accès est réglé sur la page Wireless > Advanced Settings. (Reportez-vous à la Modification des paramètres avancés, page 89.)</p>
Type	<p>Indique le type de périphérique :</p> <ul style="list-style-type: none"> ▪ AP indique que le périphérique détecté est un point d'accès prenant en charge l'infrastructure de mise en réseau sans fil IEEE 802.11 en mode Infrastructure. ▪ Ad hoc indique qu'une station voisine fonctionne en mode Ad Hoc. Les stations réglées sur le mode Ad Hoc communiquent directement entre elles, sans utiliser de point d'accès traditionnel. Le mode Ad Hoc est une infrastructure de mise en réseau sans fil IEEE 802.11 également appelé mode <i>Poste à poste</i> ou <i>Independent Basic Service Set (IBSS)</i>.

Tableau 6 Informations relatives aux points d'accès voisins (suite)

Champ	Description
SSID	<p>Identifiant SSID (Service Set Identifier) d'un autre point d'accès détecté.</p> <p>L'identifiant SSID est une chaîne alphanumérique de 32 caractères maximum permettant d'identifier de manière unique un réseau local sans fil. Il est également désigné par <i>Network Name</i>.</p> <p>L'identifiant SSID est réglé dans l'onglet Virtual Access Point. (Reportez-vous à l'Utilisation de la bande passante, page 106.)</p>
Privacy	<p>Indique si une sécurité est appliquée au point d'accès voisin.</p> <ul style="list-style-type: none"> ▪ Off indique que le mode de sécurité du point d'accès voisin est réglé sur None (aucune sécurité). ▪ On indique que le point d'accès voisin dispose d'une certaine sécurité. <p>La sécurité est configurée sur le point d'accès à partir de la page Virtual Access Point.</p>
WPA	<p>Indique si une sécurité WPA est activée ou désactivée sur le point d'accès détecté.</p>
Band	<p>Indique le mode IEEE 802.11 utilisé sur le point d'accès détecté. (Par exemple, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.)</p> <p>Le nombre affiché indique le mode en fonction du mappage suivant :</p> <ul style="list-style-type: none"> ▪ 2.4 indique le mode IEEE 802.11b, 802.11g ou 802.11n (ou une combinaison de ces modes) ▪ 5 indique le mode IEEE 802.11a, 802.11n ou une combinaison de ces modes.

Tableau 6 Informations relatives aux points d'accès voisins (suite)

Champ	Description
Channel	<p>Affiche le canal de diffusion du point d'accès détecté.</p> <p>Le canal définit la partie du spectre radio sans fil utilisée par la radio sans fil pour la transmission et la réception.</p> <p>Le canal de votre point d'accès est réglé sur la page Wireless > Advanced Settings. (Reportez-vous à la Modification des paramètres avancés, page 89.)</p>
Rate	<p>Affiche le débit (en mégabits par seconde) de transmission actuel du point d'accès détecté.</p> <p>Le débit actuel correspond toujours à l'un des débits affichés dans les débits pris en charge.</p>
Signal	<p>Indique la puissance du signal radio sans fil émis à partir du point d'accès détecté. Si vous pointez le curseur sur les barres, un chiffre apparaît indiquant la puissance en décibels (dB).</p>
Beacons	<p>Affiche le nombre total de balises reçues du point d'accès détecté depuis sa première détection.</p>
Last Beacon	<p>Affiche la date et l'heure de la dernière balise reçue du point d'accès détecté.</p>
Rates	<p>Affiche l'ensemble des débits pris en charge et de base (signalés) pour le point d'accès détecté. Les débits sont affichés en mégabits par seconde (Mbits/s).</p> <p>Tous les débits pris en charge sont signalés. Les débits de base s'affichent en gras.</p> <p>Les ensembles de débits sont configurés sur la page Wireless > Advanced Settings. (Reportez-vous à la Modification des paramètres avancés, page 89.)</p>

Enregistrer ou importer la liste des points d'accès connus

Pour enregistrer la liste des points d'accès connus dans un fichier, cliquez sur **Save**. La liste contient les adresses MAC de tous les points d'accès ajoutés à la liste des points d'accès connus. Par défaut, le nom de fichier est `Rogue2.cfg`. Vous pouvez utiliser un éditeur de texte ou un navigateur Web pour ouvrir le fichier et afficher son contenu.

Utilisez la fonction d'importation pour importer une liste de points d'accès connus à partir d'une liste enregistrée. La liste peut provenir d'un autre Cisco point d'accès ou être créée à partir d'un fichier texte. Si l'adresse MAC d'un point d'accès apparaît dans la liste des points d'accès connus, il n'est pas signalé comme indésirable.

Le fichier importé doit être un fichier texte brut avec une extension `.txt` ou `.cfg`. Les entrées du fichier sont des adresses MAC au format hexadécimal avec chaque octet séparé par un signe deux-points. Par exemple : `00:11:22:33:44:55`. Séparez les entrées par un espace simple. Le fichier doit contenir des adresses MAC uniquement pour que le point d'accès l'accepte.

Procédez comme suit pour importer une liste de points d'accès à partir d'un fichier :

ÉTAPE 1 Choisissez de remplacer la liste des points d'accès connus existante ou d'ajouter les entrées dans le fichier importé sur la liste des points d'accès connus.

- Sélectionnez la case d'option **Replace** pour importer la liste et remplacer tout le contenu de la liste des points d'accès connus.
- Sélectionnez la case d'option **Merge** pour importer la liste et ajouter les points d'accès dans le fichier importé aux points d'accès actuellement affichés dans la liste des points d'accès connus.

ÉTAPE 2 Cliquez sur **Browse** et sélectionnez le fichier à importer.

ÉTAPE 3 Cliquez sur **Import**.

Une fois l'importation terminée, l'écran est actualisé et les adresses MAC des points d'accès figurant dans le fichier importé apparaissent dans la liste des points d'accès connus.

Configuration

Paramètres LAN

Il est possible que les paramètres par défaut de l'interface de réseau LAN câblé, comprenant les paramètres DHCP et VLAN par défaut, ne fonctionnent pas correctement sur votre réseau.

Par défaut, le client DHCP du point d'accès diffuse des demandes pour obtenir des informations sur le réseau. Pour utiliser une adresse IP statique, désactivez le client DHCP et configurez manuellement l'adresse IP et les autres informations réseau.

Le VLAN de gestion par défaut du point d'accès est `VLAN 1`. Ce VLAN correspond également au VLAN non balisé (sans balise) par défaut. Si vous avez configuré le VLAN de gestion sur votre réseau à l'aide d'un ID VLAN différent, vous devez modifier l'ID VLAN du VLAN de gestion du point d'accès.

Cliquez sur l'onglet **LAN Settings** pour configurer les paramètres de l'interface LAN.

Figure 10 Paramètres LAN

The screenshot shows the LAN Settings configuration page. At the top, there is a navigation bar with tabs: Getting Started, Status, Setup (highlighted), Wireless, SNMP, Administration, and Cluster. Below this, there are sub-tabs: LAN Settings (highlighted), 802.1X Authentication, and Time Settings (NTP). The main content area is titled "LAN Settings" and contains the following sections:

- Internal Interface Settings**
 - Connection Type: DHCP (dropdown menu)
 - Static IP Address: 192 . 168 . 10 . 10
 - Subnet Mask: 255 . 255 . 255 . 0
 - Default Gateway: 192 . 168 . 10 . 1
 - DNS Nameservers: Dynamic Manual
[] . [] . [] . []
[] . [] . [] . []
- Hostname: AP541N-A-K9
- MAC Address: 00:21:29:00:1F:70
- Management VLAN ID: 1
- Untagged VLAN: Enabled Disabled
- Untagged VLAN ID: 1

At the bottom, there is a text prompt: "Click 'Apply' to save the new settings." followed by an "Apply" button.

Le **Tableau 7** décrit les champs à afficher ou à configurer sur la page **LAN Settings**.

Tableau 7 Description des champs LAN Settings

Champ	Description
Hostname	Nom DNS (nom de l'hôte) du point d'accès. Le nom DNS doit répondre aux exigences suivantes : <ul style="list-style-type: none">▪ 20 caractères maximum▪ Lettres, chiffres et tirets uniquement. Le guillemet ("") n'est pas un caractère valide.▪ Doit commencer par une lettre et se terminer par une lettre ou un chiffre.
MAC Address	Adresse MAC du port Ethernet de ce point d'accès. Il s'agit d'un champ en lecture seule que vous ne pouvez pas modifier.
Management VLAN ID	Saisissez un nombre compris entre 1 et 4094 pour l'ID du VLAN de gestion utilisé sur le réseau. L'ID du VLAN de gestion par défaut est 1.
Untagged VLAN	Active ou désactive le balisage VLAN. Si vous activez le VLAN non balisé, tout le trafic est balisé à l'aide d'un ID de VLAN. Par défaut, tout le trafic du point d'accès utilise le VLAN 1, le VLAN non balisé par défaut. Cela signifie que tout le trafic n'est pas balisé jusqu'à désactivation du VLAN non balisé, modification de l'ID VLAN du trafic non balisé ou modification de l'ID VLAN du VAP ou du client utilisant RADIUS.
Untagged VLAN ID	Saisissez un nombre compris entre 1 et 4094 pour l'ID du VLAN non balisé. Le trafic du VLAN spécifié dans ce champ n'est pas balisé à l'aide d'un ID de VLAN.

Tableau 7 Description des champs LAN Settings (suite)

Champ	Description
Connection Type	Si vous sélectionnez DHCP , le point d'accès obtient les informations sur l'adresse IP, le masque de sous-réseau, le DNS et la passerelle à partir d'un serveur DHCP. Si vous sélectionnez Static IP , vous devez saisir les informations dans les champs Static IP Address, Subnet Mask et Default Gateway.
Static IP Address	L'adresse IP statique du point d'accès. Ce champ est désactivé si vous utilisez DHCP comme type de connexion.
Subnet Mask	Masque de sous-réseau du point d'accès.
Default Gateway	Passerelle par défaut du point d'accès.
DNS Nameservers	Mode DNS. En mode Dynamic , les adresses IP des serveurs DNS sont attribuées automatiquement à l'aide du DHCP. Cette option est disponible uniquement si vous avez choisi le type de connexion DHCP. En mode Manual , vous devez attribuer les adresses IP des noms de serveurs DNS qui résolvent les noms de domaine.



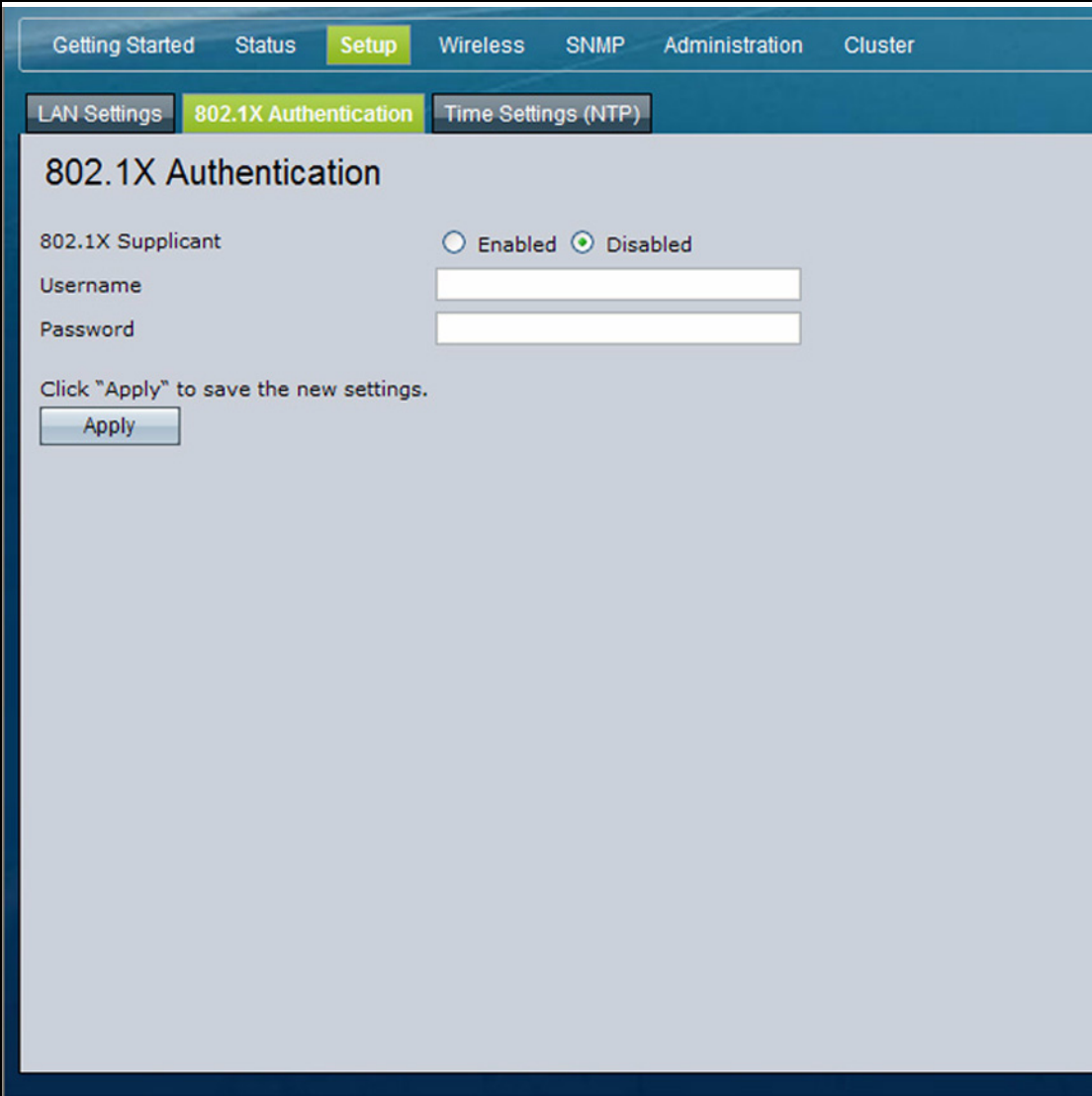
REMARQUE Après la configuration des paramètres câblés, cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt du point d'accès et le redémarrage des processus système. Si cela se produit, la connectivité des clients sans fil est temporairement perdue. Il est recommandé de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Configuration de l'authentification 802.1X

Sur les réseaux utilisant la méthode de contrôle d'accès au réseau s'appuyant sur les ports IEEE 802.1X, le demandeur (client) ne peut pas accéder au réseau tant que le serveur d'authentification 802.1X n'a pas autorisé l'accès. Si votre réseau utilise la méthode 802.1X, vous devez configurer les informations d'authentification 802.1X que le point d'accès fournira au serveur d'authentification.

Pour configurer le nom d'utilisateur et le mot de passe du demandeur 802.1X du point d'accès, cliquez sur l'onglet **802.1X Authentication** et configurez les champs affichés dans le **Tableau 8**.

Figure 11 Authentification IEEE 802.1X



The screenshot shows the configuration page for 802.1X Authentication on a Cisco AP. The interface includes a top navigation bar with tabs for 'Getting Started', 'Status', 'Setup' (selected), 'Wireless', 'SNMP', 'Administration', and 'Cluster'. Below this is a sub-navigation bar with tabs for 'LAN Settings', '802.1X Authentication' (selected), and 'Time Settings (NTP)'. The main content area is titled '802.1X Authentication' and contains the following elements:

- 802.1X Supplicant:** A radio button selection with 'Enabled' (unselected) and 'Disabled' (selected).
- Username:** A text input field.
- Password:** A text input field.
- Instructions:** The text 'Click "Apply" to save the new settings.'
- Apply Button:** A button labeled 'Apply'.

Tableau 8 Description des champs dans l'authentification IEEE 802.1X

Champ	Description
802.1X Supplicant	<p>Cliquez sur Enabled pour activer l'état d'administration du demandeur 802.1X.</p> <p>Cliquez sur Disabled pour désactiver l'état d'administration du demandeur 802.1X.</p>
Username	<p>Saisissez le nom d'utilisateur MD5 du point d'accès à utiliser lorsque vous répondez à une requête d'un serveur d'authentification 802.1X. Le nom d'utilisateur peut comporter de 1 à 64 caractères. Les caractères ASCII imprimables sont autorisés. Ils comprennent les lettres majuscules et minuscules, les chiffres et les symboles spéciaux tels que @ et #. Le guillemet (") n'est pas un caractère valide.</p> <p>REMARQUE : Si le demandeur 802.1X est désactivé, le champ Username ne peut pas être modifié.</p>
Password	<p>Saisissez le mot de passe MD5 du point d'accès à utiliser lorsque vous répondez à une requête d'un serveur d'authentification 802.1X. Le mot de passe peut comporter de 1 à 64 caractères. Les caractères ASCII imprimables sont autorisés. Ils comprennent les lettres majuscules et minuscules, les chiffres et les symboles spéciaux tels que @ et #. Le guillemet (") n'est pas un caractère valide.</p> <p>REMARQUE : Si le demandeur 802.1X est désactivé, le champ Password ne peut pas être modifié.</p>



REMARQUE Après la configuration des paramètres sur la page Authentication, cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt du point d'accès et le redémarrage des processus système. Si cela se produit, la connectivité des clients sans fil est temporairement perdue. Il est recommandé de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Activation du protocole Network Time

Le protocole NTP (Network Time Protocol) est un protocole standard Internet qui permet de synchroniser l'heure de l'ordinateur sur le réseau. Les serveurs NTP transmettent le temps universel coordonné (UTC, également appelé Temps moyen de Greenwich) à leurs systèmes clients. Le NTP envoie périodiquement des demandes d'heure aux serveurs et utilise l'horodatage renvoyé pour régler son horloge. L'horodatage est utilisé pour indiquer la date et l'heure de chaque événement dans les messages de journalisation.

En utilisant le NTP, le point d'accès peut obtenir et conserver l'heure à partir d'un serveur du réseau. L'utilisation d'un serveur NTP permet à votre point d'accès d'indiquer l'heure correcte dans les messages de journalisation et les informations de session.

Reportez-vous à l'adresse www.ntp.org pour obtenir plus d'informations sur le NTP.

Pour configurer manuellement le NTP utilisé par le point d'accès comme indiqué dans la **Figure 12, page 54** ou en utilisant un serveur comme indiqué dans la **Figure 13, page 55**, cliquez sur l'onglet **Time** et mettez les champs à jour comme décrit dans le **Tableau 9**.

Figure 12 Activation manuelle du protocole d'heure réseau

Small Business Pro
Access Point Configuration Utility

(cisco) Log Out About Help

Getting Started Status **Setup** Wireless SNMP Administration Cluster

LAN Settings 802.1X Authentication **Time Settings (NTP)**

Time Settings (NTP)

System Time Mon Oct 5 2009 14:48:39 EDT

Set System Time

Using Network Time Protocol (NTP)

Manually

System Date October 5 2009

System Time (24 HR) 14 : 48

Time Zone USA (Eastern)

Adjust Time for Daylight Savings

DST Start (24 HR) Second Sunday in March at 02 : 00

DST End (24 HR) First Sunday in November at 02 : 00

DST Offset (minutes) 90

Click "Apply" to save the new settings.

Apply

© 2009 Cisco Systems. All rights reserved. AP541N Dual Band Access Point

Figure 13 Activation du serveur de protocole Network Time



Tableau 9 Time Settings (NTP)

Champ	Description
System Time	Affiche l'heure actuelle du système.
Set System Time	Pour permettre au point d'accès d'interroger le serveur NTP, cliquez sur Using Network Time Protocol (NTP) . Pour régler manuellement l'heure du système, cliquez sur Manually .
NTP Server	Ce champ apparaît lorsque vous sélectionnez Using Network Time Protocol (NTP) dans le champ Set System Time . Si vous utilisez un serveur NTP, indiquez-le à l'aide du nom de l'hôte ou de l'adresse IP. Il n'est pas recommandé d'utiliser l'adresse IP car elle est susceptible de changer.
Time Zone	Sélectionnez le fuseau horaire international dans lequel le point d'accès fonctionne (USA (Eastern) par exemple).
System Date	Ce champ apparaît lorsque vous sélectionnez Manually dans le champ Set System Time . Utilisez la liste System Date pour sélectionner le mois, le jour et l'année.
System Time (24 HR)	Ce champ apparaît lorsque vous sélectionnez Manually dans le champ Set System Time . Utilisez la liste System Time pour sélectionner les heures et les minutes. Toutes les heures se réfèrent au fuseau horaire local.
Adjust Time for Daylight Savings	Sélectionnez l'option Daylight Savings pour régler l'heure du système sur Daylight Savings Time (DST). Les champs apparaissent dans l'ordre pour sélectionner la date et l'heure de début et de fin du DST.

Tableau 9 Time Settings (NTP) (suite)

Champ	Description
DST Start (24 HR)	<p>Utilisez ce champ pour configurer le début de l'heure d'été. L'heure de début se réfère à l'heure standard. Si le mois de début se situe après le mois de fin, le système suppose que vous vous trouvez dans l'hémisphère sud.</p> <p>Dans la liste des semaines, sélectionnez la semaine du mois (First, Second, ..., Last).</p> <p>Dans la liste des jours, sélectionnez le jour de la semaine (Sunday, Monday...).</p> <p>Dans la liste des mois, sélectionnez le mois (January, February...).</p> <p>Indiquez l'heure (format 24 heures) en sélectionnant les heures et les minutes.</p>
DST End (24 HR)	<p>Utilisez ce champ pour configurer la fin de l'heure d'été. L'heure de fin se réfère à l'heure standard.</p> <p>Dans la liste des semaines, sélectionnez la semaine du mois (First, Second, ..., Last).</p> <p>Dans la liste des jours, sélectionnez le jour de la semaine (Sunday, Monday...).</p> <p>Dans la liste des mois, sélectionnez le mois (January, February...).</p> <p>Indiquez l'heure (format 24 heures) en sélectionnant les heures et les minutes.</p>
DST Offset (minutes)	<p>Dans la liste DST Offset, sélectionnez le nombre de minutes à ajouter à l'heure d'été (15 à 120 par incréments de 15 minutes).</p>



REMARQUE Après la configuration des paramètres de l'heure, cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt du point d'accès et le redémarrage des processus système. Si cela se produit, la connectivité des clients sans fil est temporairement perdue. Il est recommandé de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

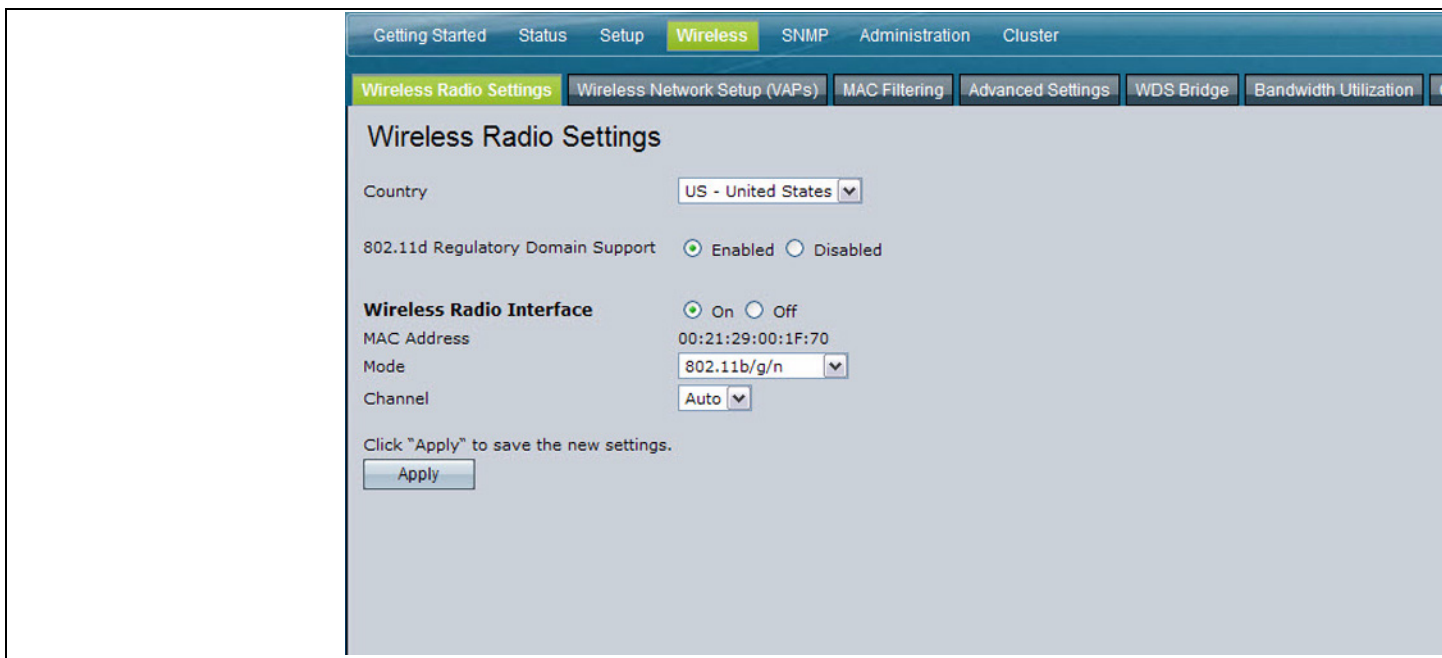
Sans fil

Modification des paramètres radio sans fil

Les paramètres sans fil permettent de configurer la radio sans fil pour le point d'accès (mode et canal 802.11) et l'interface réseau du point d'accès (adresse MAC du point d'accès).

Pour configurer l'interface sans fil, cliquez sur l'onglet **Wireless Radio Settings**.

Figure 14 Configuration de l'interface sans fil



The screenshot shows the 'Wireless Radio Settings' configuration page. At the top, there is a navigation bar with tabs: 'Getting Started', 'Status', 'Setup', 'Wireless' (highlighted), 'SNMP', 'Administration', and 'Cluster'. Below this, there are sub-tabs: 'Wireless Radio Settings' (highlighted), 'Wireless Network Setup (VAPs)', 'MAC Filtering', 'Advanced Settings', 'WDS Bridge', and 'Bandwidth Utilization'. The main content area is titled 'Wireless Radio Settings' and contains the following fields:

- Country: US - United States (dropdown menu)
- 802.11d Regulatory Domain Support: Enabled Disabled
- Wireless Radio Interface: On Off
- MAC Address: 00:21:29:00:1F:70
- Mode: 802.11b/g/n (dropdown menu)
- Channel: Auto (dropdown menu)

Below the fields, there is a note: 'Click "Apply" to save the new settings.' and an 'Apply' button.

Le **Tableau 10** décrit les champs et les options de configuration disponibles sur la page **Radio Settings**.

Tableau 10 Description des champs de la page Radio Settings

Champ	Description
Country	<p>Pays dans lequel le point d'accès est utilisé.</p> <p>Les réglementations relatives aux dispositifs sans fil varient selon les pays. Veillez à sélectionner le bon code de pays pour que le point d'accès soit conforme aux réglementations de votre pays. La sélection du code de pays affecte les modes radio sans fil que le point d'accès peut prendre en charge ainsi que la liste des canaux et la puissance d'émission de la radio sans fil.</p>
802.11d Regulatory Domain Support	<p>L'activation de la prise en charge de la norme IEEE 802.11d (mode international) sur le point d'accès permet à ce point d'accès de diffuser le pays dans lequel il est utilisé dans ses balises et dans les réponses de la sonde. Ainsi, les stations de client fonctionnent dans tous les pays sans reconfiguration nécessaire.</p> <p>La désactivation de la prise en charge de la norme 802.11d empêche la diffusion du paramètre de code de pays dans les balises. Cependant, cette option n'est valable que si la radio sans fil est configurée pour fonctionner sur la bande <i>G</i> (bande 2,4 GHz). Si la radio sans fil fonctionne sur la bande <i>A</i> (bande 5 GHz), le logiciel du point d'accès configure la prise en charge de la norme 802.11h. Dans cette configuration, les informations relatives au code de pays sont diffusées dans les balises.</p> <p>Pour activer la prise en charge du domaine réglementaire 802.11d, cliquez sur Enabled.</p> <p>Pour désactiver la prise en charge du domaine réglementaire 802.11d, cliquez sur Disabled.</p>
Wireless Radio Interface	Active ou désactive l'interface de la radio sans fil.

Tableau 10 Description des champs de la page Radio Settings (suite)

Champ	Description
MAC Address	<p>Indique l'adresse MAC (Media Access Control) de l'interface.</p> <p>Cette page affiche les adresses MAC de l'interface radio 1.</p> <p>Une adresse MAC est une adresse matérielle unique et permanente pour tout périphérique représentant une interface sur le réseau. L'adresse MAC est attribuée par le fabricant. Vous ne pouvez pas la modifier. Elle est indiquée ici à des fins informatives en tant qu'identificateur unique pour l'interface.</p>
Mode	<p>Norme de couche physique (PHY) que la radio sans fil utilise.</p> <p>REMARQUE : Si l'interface de la radio sans fil est désactivée, le mode ne peut pas être modifié.</p> <p>REMARQUE : Les modes disponibles sur le point d'accès dépendent du paramètre de code de pays.</p> <p>Sélectionnez l'un des modes suivants pour l'interface de la radio sans fil :</p> <ul style="list-style-type: none"> ▪ 802.11a : seuls les clients 802.11a peuvent se connecter au point d'accès. ▪ 802.11b/g : les clients 802.11b et 802.11g peuvent se connecter au point d'accès. ▪ 802.11a/n : les clients 802.11a et 802.11n qui fonctionnent sur une fréquence de 5 GHz peuvent se connecter au point d'accès. ▪ 802.11b/g/n (mode par défaut) : les clients 802.11b, 802.11g et 802.11n qui fonctionnent sur une fréquence de 2,4 GHz peuvent se connecter au point d'accès. ▪ 802.11n 2,4 GHz : seuls les clients 802.11n qui fonctionnent sur une fréquence de 2,4 GHz peuvent se connecter au point d'accès. ▪ 802.11n 5 GHz : seuls les clients 802.11n qui fonctionnent sur une fréquence de 5 GHz peuvent se connecter au point d'accès.

Tableau 10 Description des champs de la page Radio Settings (suite)

Champ	Description
Channel	<p>Sélectionnez le canal.</p> <p>REMARQUE : Si l'interface de la radio est désactivée, le canal ne peut pas être modifié.</p> <p>La plage de canaux disponibles est déterminée par le mode de l'interface de la radio sans fil et le paramètre de code de pays. Si vous sélectionnez Auto pour le paramètre de canal, le point d'accès analyse tous les canaux disponibles, en sélectionne un immédiatement et lance son fonctionnement. En cas d'interférences ou d'erreurs sur ce canal, un nouveau canal est sélectionné automatiquement.</p> <p>Le canal définit la portion du spectre de la radio sans fil que cette radio sans fil utilise pour l'émission et la réception. Chaque mode propose un certain nombre de canaux, en fonction des conditions de licence du spectre par les autorités nationales et internationales telles que la Federal Communications Commission (FCC) ou l'Union Internationale des Télécommunications (UIT-R).</p>



REMARQUE Une fois que les paramètres sans fil sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans cette situation, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Modification des paramètres de point d'accès virtuel

Pour modifier le VAP (point d'accès virtuel) 0 ou pour activer et configurer des VAP supplémentaires, sélectionnez l'onglet **Virtual Access Points (SSIDs)** de la section **Wireless**.

Les VAP divisent le LAN sans fil en plusieurs domaines de diffusion représentant l'équivalent sans fil des VLAN Ethernet. Les VAP simulent la présence de plusieurs points d'accès sur un seul point d'accès physique. Le point d'accès Cisco AP 541N prend en charge jusqu'à 16 VAP.



REMARQUE

Seuls les VAP dont la configuration est différente de la configuration par défaut sont affichés lorsque la page est chargée initialement. Pour configurer des VAP supplémentaires, cliquez sur **Add Another** pour afficher de nouvelles entrées de VAP (vides).

Pour chaque VAP, vous pouvez personnaliser le mode de sécurité pour contrôler l'accès au client sans fil. Chaque VAP peut également posséder un SSID unique. Plusieurs SSID font qu'un seul point d'accès apparaît comme au moins deux points d'accès pour les autres systèmes sur le réseau. En configurant des VAP, vous conservez un plus grand contrôle sur le trafic de diffusion et de multidiffusion qui affecte les performances du réseau.

Vous pouvez configurer les VAP de sorte que chacun d'entre eux utilise un VLAN différent ou qu'ils utilisent tous le même VLAN. Le VAP0, qui est toujours activé, est attribué au VLAN 1 par défaut. Le VAP1 est également activé par défaut et attribué au VLAN 100.

Le point d'accès ajoute les balises d'ID de VLAN au trafic du client sans fil en fonction de l'ID de VLAN configuré sur la page VAP ou à l'aide de l'affectation de serveur RADIUS. Si vous utilisez un serveur RADIUS externe, vous pouvez configurer plusieurs VLAN sur chaque VAP. Le serveur RADIUS externe affecte des clients sans fil au VLAN au moment de l'association et de l'authentification des clients.

Vous pouvez configurer jusqu'à quatre serveurs RADIUS IPv4 globaux. L'un d'entre eux fait toujours office de serveur principal tandis que les autres jouent le rôle de serveurs de sauvegarde. Le type de réseau et le mode de comptabilité sont communs à tous les serveurs RADIUS configurés. Vous pouvez configurer chaque VAP afin qu'il utilise les paramètres de serveur RADIUS global (configuration par défaut) ou définir la configuration de serveur RADIUS VAP par VAP. Vous pouvez également établir des paramètres de serveur RADIUS différents pour chaque VAP.

Les paramètres de serveur RADIUS global sont réduits lors du chargement initial de la page. Pour afficher (développer) la section des paramètres de serveur RADIUS global de la page, cliquez sur l'icône représentant une flèche qui pointe vers la droite située à gauche du titre de la section. Pour réduire la section des paramètres de serveur RADIUS global, cliquez sur l'icône représentant une flèche qui pointe vers le bas située à gauche du titre de la section.

Si les clients sans fil utilisent un mode de sécurité qui ne communique pas avec le serveur RADIUS ou si ce dernier ne fournit pas d'informations sur le VLAN, vous pouvez attribuer un ID de VLAN à chaque VAP. Le point d'accès affecte le VLAN à tous les clients sans fil connectés au point d'accès via ce VAP.



REMARQUE Avant de configurer des VLAN sur le point d'accès, vérifiez que le commutateur et le serveur DHCP utilisés par le point d'accès peuvent prendre en charge l'encapsulation VLAN IEEE 802.1Q.

Pour configurer plusieurs VAP, cliquez sur l'onglet **VAP**.

Figure 15 Configuration de points d'accès virtuels

Wireless Network Setup (VAPs)

▼ Global RADIUS server settings

RADIUS IP Address: 0.0.0.0

RADIUS IP Address-1:

RADIUS IP Address-2:

RADIUS IP Address-3:

RADIUS Key:

RADIUS Key-1:

RADIUS Key-2:

RADIUS Key-3:

Enable radius accounting

▼ Configure Virtual Access Points (SSIDs)

VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security	MAC Filtering	Station Isolation	HTTP Redirect	Redirect URL	Delete
0	<input checked="" type="checkbox"/>	1	cisco-data	<input checked="" type="checkbox"/>	None	Disabled	Disabled	Disable		
2	<input checked="" type="checkbox"/>	1	cisco-scan	<input checked="" type="checkbox"/>	WPA Personal	Disabled	Disabled	Disable		<input checked="" type="checkbox"/>
Hide details										
				WPA Versions:		<input type="checkbox"/> WPA		<input checked="" type="checkbox"/> WPA2		
				Cipher Suites:		<input type="checkbox"/> TKIP		<input checked="" type="checkbox"/> CCMP (AES)		
				Key:		intermec				
				Broadcast Key Refresh Rate (Range: 0-86400)		300				
3	<input checked="" type="checkbox"/>	1	GAM cisco R0 VAP3	<input checked="" type="checkbox"/>	None	Disabled	Disabled	Disable		<input checked="" type="checkbox"/>

Le **Tableau 11** décrit les champs et les options de configuration disponibles sur la page VAP.

Tableau 11 Description des champs de la page VAP

Champ	Description
RADIUS IP Address	<p>Saisissez l'adresse du serveur RADIUS global principal. Par défaut, chaque VAP utilise les paramètres de serveur RADIUS global définis pour le point d'accès en haut de la page VAP.</p> <p>Lorsque le premier client sans fil tente de s'authentifier auprès du point d'accès, ce dernier envoie une demande d'authentification au serveur principal. Si le serveur principal répond à la demande d'authentification, le point d'accès continue à utiliser ce serveur RADIUS en tant que serveur principal et les demandes d'authentification sont envoyées à l'adresse que vous avez indiquée.</p>
RADIUS IP Address 1–3	<p>Saisissez jusqu'à trois adresses IPv4 à utiliser en tant que serveurs RADIUS de sauvegarde.</p> <p>En cas d'échec de l'authentification sur le serveur principal, chaque serveur de sauvegarde configuré fait l'objet d'une tentative, dans l'ordre. L'adresse doit être valide pour que le point d'accès tente d'entrer en contact avec le serveur.</p>
RADIUS Key	<p>Saisissez la clé RADIUS dans la zone de texte.</p> <p>La <i>clé RADIUS</i> est la clé secrète partagée du serveur RADIUS global. Vous pouvez utiliser jusqu'à 63 caractères alphanumériques et spéciaux standard. La clé est sensible à la casse et vous devez configurer la même clé sur le point d'accès et sur le serveur RADIUS. Le texte que vous tapez est affiché sous forme de larges points pour empêcher que d'autres personnes puissent voir la clé RADIUS lorsque vous la saisissez.</p>
RADIUS Key 1–3	<p>Saisissez la clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur avec l'adresse IP RADIUS 1 utilise la clé RADIUS 1, le serveur avec l'adresse IP RADIUS 2 utilise la clé RADIUS 2, etc.</p>

Tableau 11 Description des champs de la page VAP (suite)

Champ	Description
Enable RADIUS Accounting	<p>Sélectionnez cette option pour suivre et mesurer les ressources employées par un utilisateur particulier telles que l'heure système, la quantité de données transmises et reçues, etc.</p> <p>Si vous activez la comptabilité RADIUS, elle est activée pour le serveur RADIUS principal et pour tous les serveurs de sauvegarde.</p>
VAP	<p>Vous pouvez configurer jusqu'à 16 VAP pour chaque radio sans fil. Le VAP0 est l'interface de radio sans fil physique. Pour désactiver le VAP0, vous devez désactiver la radio sans fil. Les liens WDS dépendant du mode de sécurité du VAP0, celui-ci ne peut pas être configuré sur None, Static WEP ou 802.1X si le mode de sécurité des liens WDS est défini sur WPA Personal. Pour que la sécurité du VAP0 passe de WPA Personal ou WPA Enterprise à None, Static WEP ou 802.1X, supprimez le mode de sécurité WPA pour tous les liens WDS.</p>
Enabled	<p>Vous pouvez activer ou désactiver un réseau configuré.</p> <ul style="list-style-type: none"> ▪ Pour activer le réseau spécifié, sélectionnez l'option Enabled à côté du VAP approprié. ▪ Pour désactiver le réseau spécifié, désélectionnez l'option Enabled à côté du VAP approprié. <p>Si vous désactivez le réseau spécifié, vous perdez l'ID de VLAN saisi.</p>

Tableau 11 Description des champs de la page VAP (suite)

Champ	Description
VLAN ID	<p>Lorsqu'un client sans fil se connecte au point d'accès à l'aide de ce VAP, le point d'accès marque l'intégralité du trafic issu du client sans fil avec l'ID de VLAN saisi dans ce champ, sauf si vous activez l'ID de VLAN non balisé ou si vous utilisez un serveur RADIUS pour affecter un client sans fil à un VLAN. La plage possible pour l'ID de VLAN est comprise entre 1 et 4 094.</p> <p>Si vous utilisez l'authentification RADIUS pour les clients, vous pouvez également ajouter les attributs suivants au fichier approprié sur le serveur RADIUS ou AAA pour configurer un VLAN pour le client :</p> <ul style="list-style-type: none">▪ Type de tunnel▪ Type de support de tunnel▪ ID de groupe privé de tunnel <p>L'ID de VLAN attribué via RADIUS remplace l'ID de VLAN configuré à la page VAP.</p> <p>Vous configurez les ID de VLAN de gestion et non balisés sur la page Ethernet Settings. Pour obtenir plus d'informations, reportez-vous à la section Paramètres LAN, page 47.</p>
SSID	<p>Saisissez le nom du réseau sans fil. Le SSID est une chaîne alphanumérique de 32 caractères maximum. Le guillemet (") n'est pas un caractère valide. Vous pouvez utiliser le même SSID pour plusieurs VAP ou choisir un SSID unique pour chaque VAP.</p> <p>REMARQUE : Si vous êtes connecté en tant que client sans fil au point d'accès que vous administrez, la réinitialisation du SSID entraîne la perte de la connexion au point d'accès. Vous devez alors vous reconnecter au nouveau SSID une fois que ce paramètre est enregistré.</p>

Tableau 11 Description des champs de la page VAP (suite)

Champ	Description
Broadcast SSID	<p>Indiquez si vous autorisez le point d'accès à diffuser le <i>SSID</i> dans ses trames de balises. Le paramètre Broadcast SSID est désactivé par défaut. Lorsque le VAP ne diffuse pas son SSID, le nom du réseau n'apparaît pas dans la liste des réseaux disponibles sur une station de client. Le client doit alors disposer du nom exact du réseau configuré sur le demandeur avant de pouvoir se connecter.</p> <ul style="list-style-type: none"> ▪ Pour activer la diffusion SSID, sélectionnez la case Broadcast SSID. ▪ Pour interdire la diffusion SSID, désélectionnez la case Broadcast SSID. <p>REMARQUE : La désactivation de la diffusion SSID est suffisante pour éviter que les clients se connectent accidentellement au réseau, mais pas pour faire échouer la moindre tentative de connexion ou de surveillance du trafic non crypté de la part d'un pirate informatique. La suppression de la diffusion SSID offre un niveau de protection des plus faibles sur les réseaux exposés d'une autre manière (comme les réseaux invités) pour lesquels la priorité facilite l'obtention d'une connexion pour les clients et aucune information confidentielle n'est disponible.</p>
Security	<p>Sélectionnez l'un des modes de sécurité suivants pour le VAP :</p> <ul style="list-style-type: none"> ▪ None ▪ Static WEP ▪ Dynamic WEP ▪ IEEE 802.1X ▪ WPA Personal ▪ WPA Enterprise <p>Si vous sélectionnez un mode de sécurité différent de None, des champs supplémentaires apparaissent. Ces champs sont décrits dans la section « Security (mode) ».</p>

Tableau 11 Description des champs de la page VAP (suite)

Champ	Description
MAC Auth Type	<p>Vous pouvez configurer une liste globale des adresses MAC dont l'accès au réseau est autorisé ou refusé. Le menu déroulant de cette fonctionnalité vous permet de sélectionner le type d'authentification MAC à utiliser :</p> <ul style="list-style-type: none">▪ Disabled : n'utilise pas l'authentification MAC.▪ Local : utilise la liste d'authentification MAC configurée à la page Wireless Connection Control.▪ RADIUS : utilise la liste d'authentification MAC sur le serveur RADIUS externe. <p>Pour obtenir plus d'informations sur l'authentification MAC, reportez-vous à la section Contrôle de la connexion des clients, page 85.</p>
Station Isolation	<p>Utilisez le menu déroulant pour configurer l'isolation de la station pour le VAP :</p> <ul style="list-style-type: none">▪ Lorsque l'isolation est désactivée, les clients sans fil peuvent communiquer entre eux normalement en envoyant du trafic via le point d'accès.▪ Lorsque l'isolation est activée, le point d'accès bloque la communication entre les clients sans fil sur le même VAP. Le point d'accès autorise toujours le trafic de données entre ses clients sans fil et les périphériques câblés sur le réseau, via un lien WDS, et avec les autres clients sans fil associés à un VAP différent.

Tableau 11 Description des champs de la page VAP (suite)

Champ	Description
Redirect Mode	<p>Activez la fonction de redirection HTTP pour rediriger les clients sans fil vers une page Web personnalisée.</p> <p>Lorsque le mode de redirection est activé, l'utilisateur est redirigé vers l'URL que vous indiquez une fois que le client sans fil est associé à un point d'accès et que l'utilisateur ouvre un navigateur Web sur le client pour accéder à Internet.</p> <p>La page Web personnalisée doit se trouver sur un serveur Web externe et peut contenir des informations telles que le logo et la politique d'utilisation du réseau de la société.</p> <p>REMARQUE : Le client sans fil est redirigé vers le serveur Web externe une seule fois, lorsqu'il est associé pour la première fois au point d'accès.</p>
Redirect URL	<p>Indiquez l'URL vers laquelle le navigateur Web doit être redirigé une fois que le client sans fil est associé au point d'accès et envoie du trafic HTTP. Sa longueur va de 1 à 120 caractères alphanumériques et spéciaux, sous la forme « <code>^[A-Za-z]+://[A-Za-z0-9-]+\.[A-Za-z0-9]+</code> ». Par exemple : <code>http://cisco.com</code>.</p>
Supprimer	<p>Cliquez sur l'icône de suppression apparaissant sous forme de « X » rouge pour supprimer la configuration d'un VAP particulier. Lorsqu'un VAP est supprimé, l'ensemble de sa configuration est restaurée sur ses paramètres par défaut. L'entrée disparaît de la liste des VAP affichés.</p> <p>REMARQUE : Le VAP0 correspond à l'interface de radio sans fil physique et ne peut être supprimé. L'icône de suppression n'est pas affichée pour ce VAP.</p>



REMARQUE Une fois que les paramètres du VAP sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans cette situation, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Security (mode)

Le mode de sécurité défini ici est propre au VAP.

Lors du chargement initial de la page, tous les VAP dont le mode de sécurité est différent de **None** disposent d'un lien **Show details** sous la zone de sélection **Security**. Cliquez sur le lien **Show details** pour afficher les paramètres de sécurité en cours. Lorsque vous affichez ces paramètres, le lien se transforme en **Hide details**. Cliquez sur **Hide details** pour réduire les paramètres.

None (Plain-text)

Si vous sélectionnez **None** comme mode de sécurité, aucune autre option n'est configurable sur le point d'accès. Dans ce mode, aucune donnée transférée vers ou depuis le point d'accès n'est cryptée. Il peut être utile lors de la configuration initiale du réseau ou pour la résolution de problèmes, mais il n'est pas recommandé pour une utilisation régulière sur le réseau interne car il n'est pas sécurisé.

Static WEP

Le protocole WEP (Wired Equivalent Privacy) est un protocole de cryptage de données pour les réseaux sans fil 802.11. Toutes les stations sans fil et tous les points d'accès sur le réseau sont configurés avec une clé partagée statique de 64 bits (clé secrète de 40 bits + vecteur d'initialisation de 24 bits) ou de 128 bits (clé secrète de 104 bits + vecteur d'initialisation de 24 bits) pour le cryptage des données.

Le mode Static WEP n'est pas le mode disponible le plus sécurisé, mais il offre une protection plus importante que le mode None (Plain-text) car il évite que des personnes extérieures surveillent le trafic sans fil non crypté.

Le protocole WEP crypte les données transmises sur le réseau sans fil à partir d'une clé statique. (L'algorithme de cryptage est un chiffre de flux appelé RC4.)

Si vous utilisez le mode Static WEP, les règles suivantes s'appliquent :

- La sécurité WLAN de toutes les stations de client doit être définie sur WEP et tous les clients doivent disposer de l'une des clés WEP indiquées sur le point d'accès afin de décoder les transmissions de données du point d'accès vers les stations.
- Le point d'accès doit disposer de toutes les clés utilisées par les clients pour les transmissions depuis les stations vers le point d'accès afin de décoder ces transmissions.

- La même clé doit occuper le même emplacement sur tous les nœuds (le point d'accès et les clients). Par exemple, si le point d'accès définit la clé abc123 comme clé WEP 3, les stations de client doivent définir cette même chaîne comme clé WEP 3.
- Les stations de client peuvent utiliser des clés différentes pour transmettre des données au point d'accès. (Elles peuvent aussi utiliser la même clé, mais cette méthode est moins sécurisée car les stations peuvent alors décrypter les données envoyées par les autres stations.)
- Sur certains logiciels de client sans fil, vous pouvez configurer plusieurs clés WEP et un « index de clé de transfert » de station de client, puis paramétrer les stations afin qu'elles cryptent les données qu'elles transmettent à l'aide de différentes clés. Ainsi, vous êtes sûr que les points d'accès voisins ne peuvent pas décoder les transmissions des autres points d'accès.
- Vous ne pouvez pas combiner des clés WEP de 64 bits et de 128 bits entre le point d'accès et ses stations de client.

Le **Tableau 12** décrit les champs WEP.


Tableau 12 Description des champs WEP

Champ	Description
Transfer Key Index	<p>Sélectionnez un index de clé dans le menu déroulant. Les index de clé 1 à 4 sont disponibles. L'index par défaut est le 1.</p> <p>L'index de clé de transfert indique quelle clé WEP est utilisée par le point d'accès pour crypter les données qu'il transmet.</p>
Key Length	<p>Indiquez la longueur de la clé en cliquant sur l'une des cases d'option suivantes :</p> <ul style="list-style-type: none"> ▪ 64 bits ▪ 128 bits
Key Type	<p>Sélectionnez le type de clé en cliquant sur l'une des cases d'option suivantes :</p> <ul style="list-style-type: none"> ▪ ASCII ▪ Hex

Tableau 12 Description des champs WEP (suite)

Champ	Description
WEP Keys	<p>Vous pouvez indiquer jusqu'à quatre clés WEP. Dans chaque zone de texte, saisissez une chaîne de caractères pour chaque clé. Les clés saisies dépendent du type de clé sélectionné :</p> <ul style="list-style-type: none">▪ ASCII : inclut des lettres majuscules et minuscules, des chiffres et des symboles spéciaux tels que « @ » et « # ».▪ Hex : inclut des chiffres compris entre 0 et 9 et des lettres entre A et F. <p>Utilisez le même nombre de caractères pour chaque clé, comme l'indique le champ Characters Required. Il s'agit de clés WEP RC4 partagées avec les stations utilisant le point d'accès.</p> <p>Chaque station de client doit être configurée afin d'utiliser l'une de ces clés WEP à l'emplacement indiqué ici sur le point d'accès.</p> <p>Characters Required : le nombre de caractères saisis dans les champs de clé WEP est déterminé par la longueur et le type sélectionnés pour les clés. Par exemple, si vous utilisez des clés ASCII 128 bits, vous devez saisir 13 caractères pour la clé WEP. Le nombre de caractères requis est mis à jour automatiquement en fonction de la longueur et du type définis pour les clés.</p>

Tableau 12 Description des champs WEP (suite)

Champ	Description
802.1X Authentication	<p>L'algorithme d'authentification définit la méthode utilisée pour déterminer si une station de client est autorisée à s'associer à un point d'accès lorsque le mode de sécurité WEP statique est activé.</p> <p>Pour déterminer l'algorithme d'authentification à utiliser, choisissez l'une des options suivantes :</p> <ul style="list-style-type: none"> ▪ L'authentification Open system autorise toutes les stations de client à s'associer au point d'accès qu'elles disposent de la bonne clé WEP ou pas. Cet algorithme est également utilisé en mode texte brut, WEP dynamique, IEEE 802.1X et WPA. Lorsque l'algorithme d'authentification est défini sur Open System, tous les clients peuvent s'associer au point d'accès.
	<p> REMARQUE Le fait qu'une station de client soit autorisée à s'associer ne garantit pas qu'elle puisse échanger du trafic avec un point d'accès. Une station doit disposer de la bonne clé WEP pour pouvoir accéder aux données d'un point d'accès puis les décrypter pour transmettre des données lisibles au point d'accès.</p>
	<ul style="list-style-type: none"> ▪ L'authentification Shared key oblige la station de client à disposer de la bonne clé WEP pour s'associer avec le point d'accès. Lorsque l'algorithme d'authentification est défini sur Shared Key, une station avec une clé WEP incorrecte ne peut pas s'associer avec le point d'accès. ▪ Authentifications Open system et Shared key. Lorsque vous sélectionnez les deux algorithmes d'authentification : <ul style="list-style-type: none"> - Les stations de client configurées pour utiliser le protocole WEP en mode de clé partagée doivent disposer d'une clé WEP valide pour s'associer avec le point d'accès. - Les stations de client configurées pour utiliser le protocole WEP en système ouvert (mode de clé partagée désactivé) peuvent s'associer avec le point d'accès, même si elles ne disposent pas de la bonne clé WEP.

Authentification IEEE 802.1X

IEEE 802.1X est l'authentification de définition par port et l'infrastructure de gestion de clé standard. Les messages EAP (Extensible Authentication Protocol) sont envoyés sur un réseau sans fil IEEE 802.11 à l'aide d'un protocole appelé EAPOL (EAP Encapsulation Over LANs). L'authentification IEEE 802.1X fournit des clés générées de façon dynamique et actualisées régulièrement. Un chiffre de flux RC4 est utilisé pour crypter le corps des trames et le contrôle de redondance cyclique (CRC) de chaque trame 802.11.

Ce mode requiert l'utilisation d'un serveur RADIUS externe pour l'authentification des utilisateurs. Le point d'accès nécessite un serveur RADIUS pouvant utiliser le protocole EAP, tel que le serveur d'authentification de Microsoft. Pour fonctionner avec les clients Windows, le serveur d'authentification doit prendre en charge les protocoles PEAP (Protected EAP) et MSCHAP V2.

Vous pouvez utiliser n'importe quelle méthode d'authentification prise en charge par le mode IEEE 802.1X, y compris l'authentification Kerberos, par certificat et par clé publique. Vous devez configurer les stations de client de sorte qu'elles utilisent la même méthode d'authentification que le point d'accès.



REMARQUE Une fois que les paramètres de sécurité sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres.

Tableau 13 IEEE 802.1X

Champ	Description
Use Global RADIUS Server Settings	<p>Par défaut, chaque VAP utilise les paramètres de serveur RADIUS global définis pour le point d'accès en haut de la page VAP. Vous pouvez néanmoins configurer les VAP un par un de sorte qu'ils utilisent des jeux de serveurs RADIUS différents.</p> <p>Pour utiliser les paramètres de serveur RADIUS global, veillez à ce que la case soit sélectionnée.</p> <p>Pour utiliser un serveur RADIUS distinct pour le VAP, désélectionnez la case et saisissez l'adresse IP et la clé du serveur RADIUS dans les champs suivants.</p>
RADIUS IP Address	Saisissez l'adresse du serveur RADIUS principal pour ce VAP.

Tableau 13 IEEE 802.1X (suite)

Champ	Description
RADIUS IP Address 1–3	<p>Saisissez jusqu'à trois adresses IPv4 à utiliser comme serveurs RADIUS de sauvegarde pour ce VAP.</p> <p>En cas d'échec de l'authentification sur le serveur principal, chaque serveur de sauvegarde configuré fait l'objet d'une tentative, dans l'ordre.</p>
RADIUS Key	<p>Saisissez la clé RADIUS dans la zone de texte.</p> <p>La <i>clé RADIUS</i> est la clé secrète partagée du serveur RADIUS global. Vous pouvez utiliser jusqu'à 63 caractères alphanumériques et spéciaux standard. La clé est sensible à la casse et vous devez configurer la même clé sur le point d'accès et sur le serveur RADIUS. Le texte que vous tapez est affiché sous forme d'astérisques (*) pour empêcher que d'autres personnes puissent voir la clé RADIUS lorsque vous la saisissez.</p>
RADIUS Key 1–3	<p>Saisissez la clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur avec l'adresse IP RADIUS 1 utilise la clé RADIUS 1, le serveur avec l'adresse IP RADIUS 2 utilise la clé RADIUS 2, etc.</p>
Enable RADIUS Accounting	<p>Sélectionnez cette option pour suivre et mesurer les ressources employées par un utilisateur particulier telles que l'heure système, la quantité de données transmises et reçues, etc.</p> <p>Si vous activez la comptabilité RADIUS, elle est activée pour le serveur RADIUS principal et pour tous les serveurs de sauvegarde.</p>
Broadcast Key Refresh Rate	<p>Saisissez une valeur pour définir l'intervalle d'actualisation de la clé (du groupe) de diffusion pour les clients associés à ce VAP.</p> <p>La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.</p>

Tableau 13 IEEE 802.1X (suite)

Champ	Description
Session Key Refresh Rate	Saisissez une valeur pour définir l'intervalle auquel le point d'accès actualise les clés de session (monodiffusion) pour chaque client associé au VAP. La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

Dynamic WEP

Le mode Dynamic WEP utilise IEEE 802.1X, l'authentification de définition par port et l'infrastructure de gestion de clé standard. Les messages EAP (Extensible Authentication Protocol) sont envoyés sur un réseau sans fil IEEE 802.11 à l'aide d'un protocole appelé EAPOL (EAP Encapsulation Over LANs). Le mode Dynamic WEP fournit des clés générées de façon dynamique et actualisées régulièrement. Un chiffre de flux RC4 est utilisé pour crypter le corps des trames et le contrôle de redondance cyclique (CRC) de chaque trame 802.11.

Ce mode requiert l'utilisation d'un serveur RADIUS externe pour l'authentification des utilisateurs. Le point d'accès nécessite un serveur RADIUS pouvant utiliser le protocole EAP, tel que le serveur d'authentification de Microsoft. Pour fonctionner avec les clients Windows, le serveur d'authentification doit prendre en charge les protocoles PEAP (Protected EAP) et MSCHAP V2.

Vous pouvez utiliser n'importe quelle méthode d'authentification prise en charge par le mode Dynamic WEP, y compris l'authentification Kerberos, par certificat et par clé publique. Vous devez configurer les stations de client de sorte qu'elles utilisent la même méthode d'authentification que le point d'accès.

Tableau 14 Dynamic WEP

Champ	Description
Use Global RADIUS Server Settings	<p>Par défaut, chaque VAP utilise les paramètres de serveur RADIUS global définis pour le point d'accès en haut de la page VAP. Vous pouvez néanmoins configurer les VAP un par un de sorte qu'ils utilisent des jeux de serveurs RADIUS différents.</p> <p>Pour utiliser les paramètres de serveur RADIUS global, veillez à ce que la case soit sélectionnée.</p> <p>Pour utiliser un serveur RADIUS distinct pour le VAP, désélectionnez la case et saisissez l'adresse IP et la clé du serveur RADIUS dans les champs suivants.</p>
RADIUS IP Address	Saisissez l'adresse du serveur RADIUS principal pour ce VAP.
RADIUS IP Address 1-3	<p>Saisissez jusqu'à trois adresses IPv4 à utiliser comme serveurs RADIUS de sauvegarde pour ce VAP.</p> <p>En cas d'échec de l'authentification sur le serveur principal, chaque serveur de sauvegarde configuré fait l'objet d'une tentative, dans l'ordre.</p>
RADIUS Key	<p>Saisissez la clé RADIUS dans la zone de texte.</p> <p>La <i>clé RADIUS</i> est la clé secrète partagée du serveur RADIUS global. Vous pouvez utiliser jusqu'à 63 caractères alphanumériques et spéciaux standard. La clé est sensible à la casse et vous devez configurer la même clé sur le point d'accès et sur le serveur RADIUS. Le texte que vous tapez est affiché sous forme d'astérisques (*) pour empêcher que d'autres personnes puissent voir la clé RADIUS lorsque vous la saisissez.</p>
RADIUS Key 1-3	Saisissez la clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur avec l'adresse IP RADIUS 1 utilise la clé RADIUS 1, le serveur avec l'adresse IP RADIUS 2 utilise la clé RADIUS 2, etc.

Tableau 14 Dynamic WEP (suite)

Champ	Description
Enable RADIUS Accounting	<p>Sélectionnez cette option pour suivre et mesurer les ressources employées par un utilisateur particulier telles que l'heure système, la quantité de données transmises et reçues, etc.</p> <p>Si vous activez la comptabilité RADIUS, elle est activée pour le serveur RADIUS principal et pour tous les serveurs de sauvegarde.</p>
Broadcast Key Refresh Rate	<p>Saisissez une valeur pour définir l'intervalle d'actualisation de la clé (du groupe) de diffusion pour les clients associés à ce VAP.</p> <p>La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.</p>
Session Key Refresh Rate	<p>Saisissez une valeur pour définir l'intervalle auquel le point d'accès actualise les clés de session (monodiffusion) pour chaque client associé au VAP.</p> <p>La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.</p>



REMARQUE Une fois que les paramètres de sécurité sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres.

WPA Personal

WPA Personal est une norme IEEE 802.11i Wi-Fi Alliance, qui inclut les mécanismes AES-CCMP et TKIP. La version Personal du protocole WPA utilise une clé pré-partagée (tandis que le mode de sécurité WPA Enterprise utilise IEEE 802.1X et EAP). PSK est utilisé uniquement pour la vérification initiale des identifiants.

Ce mode de sécurité est rétrocompatible pour les clients sans fil prenant en charge le mode WPA d'origine.

Tableau 15 Description des champs disponibles pour le mode WPA Personal

Champ	Description
WPA Versions	<p>Sélectionnez les types de stations de client à prendre en charge :</p> <p>WPA : si toutes les stations de client sur le réseau prennent en charge le mode WPA d'origine mais qu'aucune ne prend en charge le nouveau mode WPA2, sélectionnez WPA.</p> <p>WPA2 : si toutes les stations de client sur le réseau prennent en charge le mode WPA2, nous vous suggérons de l'utiliser, car il offre la meilleure sécurité possible grâce à la prise en charge de la norme IEEE 802.11i.</p> <p>WPA et WPA2 : si vous avez un mélange de clients, dont certains prennent en charge le mode WPA2 et d'autres le mode WPA d'origine, sélectionnez les deux cases. Ainsi, les stations de client WPA et WPA2 peuvent s'associer et s'authentifier, le mode WPA2, plus robuste, étant utilisé pour les clients qui le prennent en charge. Cette configuration WPA permet une plus grande interopérabilité, aux dépens de la sécurité.</p>
Cipher Suites	<p>Sélectionnez la suite de chiffrement à utiliser :</p> <ul style="list-style-type: none"> ▪ TKIP ▪ CCMP (AES) ▪ TKIP et CCMP (AES) <p>Les clients TKIP et AES peuvent s'associer au point d'accès. Les clients WPA doivent disposer de l'une des clés suivantes pour s'associer au point d'accès :</p> <ul style="list-style-type: none"> ▪ clé TKIP valide ; ▪ clé AES-CCMP valide. <p>Les clients qui ne sont pas configurés de façon à utiliser le mode WPA Personal ne peuvent pas s'associer au point d'accès.</p>

Tableau 15 Description des champs disponibles pour le mode WPA Personal

Champ	Description
Key	La clé pré-partagée est la clé secrète partagée pour le mode WPA Personal. Saisissez une chaîne comprenant entre 8 et 63 caractères. Les caractères autorisés sont les lettres majuscules et minuscules, les chiffres et les symboles spéciaux tels que « @ » et « # ».
Broadcast Key Refresh Rate	Saisissez une valeur pour définir l'intervalle d'actualisation de la clé (du groupe) de diffusion pour les clients associés à ce VAP. La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

WPA Enterprise

Le mode WPA Enterprise avec RADIUS est une application de la norme IEEE 802.11i Wi-Fi Alliance, qui inclut les mécanismes CCMP (AES) et TKIP. Le mode Enterprise requiert l'utilisation d'un serveur RADIUS pour authentifier les utilisateurs.

Ce mode de sécurité est rétrocompatible pour les clients sans fil prenant en charge le mode WPA d'origine.

Tableau 16 Description des champs disponibles pour le mode WPA Enterprise

Champ	Description
WPA Versions	<p>Sélectionnez les types de stations de client à prendre en charge :</p> <ul style="list-style-type: none"> ▪ WPA : si toutes les stations de client sur le réseau prennent en charge le mode WPA d'origine mais qu'aucune ne prend en charge le nouveau mode WPA2, sélectionnez WPA. ▪ WPA2 : si toutes les stations de client sur le réseau prennent en charge le mode WPA2, nous vous suggérons de l'utiliser, car il offre la meilleure sécurité possible grâce à la prise en charge de la norme IEEE 802.11i. ▪ WPA et WPA2 : si vous avez un mélange de clients, dont certains prennent en charge le mode WPA2 et d'autres le mode WPA d'origine uniquement, sélectionnez WPA et WPA2. Ainsi, les stations de client WPA et WPA2 peuvent s'associer et s'authentifier, le mode WPA2, plus robuste, étant utilisé pour les clients qui le prennent en charge. Cette configuration WPA permet une plus grande interopérabilité, aux dépens de la sécurité.
Enable pre-authentication	<p>Dans le champ WPA Versions, si vous avez sélectionné uniquement WPA2 ou WPA et WPA2, vous pouvez activer la pré-authentication pour les clients WPA2.</p> <p>Cliquez sur Enable pre-authentication pour que les clients WPA2 sans fil envoient un paquet de pré-authentication. Les informations de pré-authentication sont transmises du point d'accès utilisé par le client vers le point d'accès cible. L'activation de cette fonctionnalité peut accélérer l'authentification des clients itinérants qui se connectent à plusieurs points d'accès.</p> <p>Cette option n'est pas disponible si vous sélectionnez uniquement WPA dans le champ WPA Versions car le mode WPA ne prend pas en charge cette fonctionnalité.</p>

Tableau 16 Description des champs disponibles pour le mode WPA Enterprise (suite)

Champ	Description
Cipher Suites	<p>Sélectionnez la suite de chiffrement à utiliser :</p> <ul style="list-style-type: none"> ▪ TKIP ▪ CCMP (AES) ▪ TKIP et CCMP (AES) <p>Par défaut, les suites TKIP et CCMP sont sélectionnées. Lorsqu'elles sont toutes deux sélectionnées, les stations de client configurées pour utiliser le mode WPA avec RADIUS doivent disposer de l'une des combinaisons suivantes :</p> <ul style="list-style-type: none"> ▪ adresse IP TKIP RADIUS et clé RADIUS valides ; ▪ adresse IP CCMP (AES) et clé RADIUS valides.
Active Server	<p>Affiche le serveur RADIUS utilisé. Vous pouvez passer manuellement de ce serveur à un serveur différent en sélectionnant le serveur souhaité dans la zone de liste déroulante.</p> <p>REMARQUE : Le serveur actif n'est pas stocké après un redémarrage. Le premier serveur RADIUS configuré est sélectionné lorsque le périphérique est redémarré ou réinitialisé.</p>
Use Global RADIUS Server Settings	<p>Par défaut, chaque VAP utilise les paramètres de serveur RADIUS global définis pour le point d'accès en haut de la page VAP. Vous pouvez néanmoins configurer les VAP un par un de sorte qu'ils utilisent des jeux de serveurs RADIUS différents.</p> <p>Pour utiliser les paramètres de serveur RADIUS global, veillez à ce que la case soit sélectionnée.</p> <p>Pour utiliser un serveur RADIUS distinct pour le VAP, désélectionnez la case et saisissez l'adresse IP et la clé du serveur RADIUS dans les champs suivants.</p>
RADIUS IP Address	<p>Saisissez l'adresse du serveur RADIUS principal pour ce VAP.</p>

Tableau 16 Description des champs disponibles pour le mode WPA Enterprise (suite)

Champ	Description
RADIUS IP Address 1–3	<p>Saisissez jusqu'à trois adresses IPv4 à utiliser comme serveurs RADIUS de sauvegarde pour ce VAP.</p> <p>En cas d'échec de l'authentification sur le serveur principal, chaque serveur de sauvegarde configuré fait l'objet d'une tentative, dans l'ordre.</p>
RADIUS Key	<p>Saisissez la clé RADIUS dans la zone de texte.</p> <p>La <i>clé RADIUS</i> est la clé secrète partagée du serveur RADIUS global. Vous pouvez utiliser jusqu'à 63 caractères alphanumériques et spéciaux standard. La clé est sensible à la casse et vous devez configurer la même clé sur le point d'accès et sur le serveur RADIUS. Le texte que vous tapez est affiché sous forme d'astérisques (*) pour empêcher que d'autres personnes puissent voir la clé RADIUS lorsque vous la saisissez.</p>
RADIUS Key 1–3	<p>Saisissez la clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur avec l'adresse IP RADIUS 1 utilise la clé RADIUS 1, le serveur avec l'adresse IP RADIUS 2 utilise la clé RADIUS 2, etc.</p>
Enable RADIUS Accounting	<p>Sélectionnez cette option pour suivre et mesurer les ressources employées par un utilisateur particulier telles que l'heure système, la quantité de données transmises et reçues, etc.</p> <p>Si vous activez la comptabilité RADIUS, elle est activée pour le serveur RADIUS principal et pour tous les serveurs de sauvegarde.</p>
Broadcast Key Refresh Rate	<p>Saisissez une valeur pour définir l'intervalle d'actualisation de la clé (du groupe) de diffusion pour les clients associés à ce VAP.</p> <p>La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.</p>

Tableau 16 Description des champs disponibles pour le mode WPA Enterprise (suite)

Champ	Description
Session Key Refresh Rate	Saisissez une valeur pour définir l'intervalle auquel le point d'accès actualise les clés de session (monodiffusion) pour chaque client associé au VAP. La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.



REMARQUE Une fois que les paramètres de sécurité sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres.

Contrôle de la connexion des clients

Une adresse MAC (Media Access Control) est une adresse matérielle qui identifie de façon unique chaque nœud d'un réseau. Tous les périphériques réseau IEEE 802 partagent un format d'adresse MAC de 48 bits commun, généralement affiché sous forme de chaîne de 12 chiffres hexadécimaux séparés par un signe deux-points, par exemple 00 : DC : BA : 09 : 87 : 65. Chaque carte d'interface réseau (NIC) sans fil utilisée par un client sans fil dispose d'une adresse MAC unique.

Vous pouvez utiliser l'utilitaire *Utilitaire de configuration du point d'accès* sur le point d'accès ou un serveur RADIUS externe pour contrôler l'accès au réseau via le point d'accès en fonction de l'adresse MAC du client sans fil. Cette fonctionnalité est appelée authentification MAC ou filtrage MAC. Pour contrôler l'accès, vous devez configurer une liste globale d'adresses MAC en local sur le point d'accès ou sur un serveur RADIUS externe. Vous devez ensuite définir un filtre pour déterminer si l'accès au réseau des clients qui possèdent ces adresses MAC est autorisé ou refusé. Lorsqu'un client sans fil tente de s'associer à un point d'accès, ce dernier recherche l'adresse MAC du client dans la liste locale des stations ou sur le serveur RADIUS. S'il la trouve, le paramètre global d'autorisation ou de refus est appliqué. S'il ne la trouve pas, c'est l'opposé qui est appliqué.

Sur la page **Virtual Access Point Settings**, le paramètre de type d'authentification MAC détermine si le point d'accès utilise la liste de stations configurée localement sur la page **Client Connection Control** ou sur le serveur RADIUS externe. Le paramètre de filtrage Allow/Block de la page **Client Connection Control** détermine si les clients présents dans la liste de stations (locale ou RADIUS) peuvent accéder au réseau via le point d'accès. Pour obtenir plus d'informations sur la définition du type d'authentification MAC, reportez-vous à la section **Configuration du système de distribution sans fil (WDS), page 100**.

Configuration d'un filtre MAC et d'une liste de stations sur le point d'accès

La page **Client Connection Control** vous permet de contrôler l'accès au point d'accès en fonction des adresses MAC. Selon le filtre défini, vous pouvez *autoriser* uniquement les stations de client avec une adresse MAC listée ou refuser *l'accès* aux stations listées.

Lorsque vous activez l'authentification MAC et établissez une liste d'adresses MAC approuvées, seuls les clients dont l'adresse MAC est listée peuvent accéder au réseau. Si vous indiquez des adresses MAC à refuser, tous les clients peuvent accéder au réseau sauf ceux qui figurent dans cette liste de *refus*.

Pour activer le filtrage par adresse MAC, cliquez sur l'onglet **Client Connection Control**.

Figure 16 Configuration de l'authentification MAC

The screenshot shows the 'MAC Filtering' configuration page. At the top, there is a navigation bar with tabs: 'Getting Started', 'Status', 'Setup', 'Wireless', 'SNMP', 'Administration', and 'Cluster'. Below this, there is a sub-navigation bar with tabs: 'Wireless Radio Settings', 'Wireless Network Setup (VAPs)', 'MAC Filtering', 'Advanced Settings', 'WDS Bridge', 'Bandwidth Utilization', and 'QoS Parameters'. The main content area is titled 'MAC Filtering' and contains the following elements:

- Filter:** Two radio buttons are present: 'Allow only stations in list' (unselected) and 'Block all stations in list' (selected).
- Stations List:** A large empty rectangular box for listing MAC addresses. Below it is a 'Remove' button.
- MAC Address:** A form with six input fields separated by colons (e.g., ' : : : : ') and an 'Add' button.
- Instructions:** The text 'Click "Apply" to save the new settings.' is displayed above an 'Apply' button.



REMARQUE Les paramètres d'authentification MAC globale concernent tous les VAP.

Le **Tableau 17** décrit les champs et les options de configuration disponibles sur la page **MAC Authentication**.

Tableau 17 Description des champs de la page **MAC Authentication**

Champ	Description
Filter	<p>Pour définir le filtre par adresse MAC, sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none">▪ Allow only stations in list : toutes les stations figurant dans la liste sont autorisées à accéder au réseau via le point d'accès ; toutes les autres stations n'y sont pas autorisées.▪ Block all stations in list : l'accès au réseau via le point d'accès est refusé uniquement aux stations figurant dans la liste. Toutes les autres stations peuvent accéder au réseau. <p>REMARQUE : Le filtre sélectionné concerne les clients de la liste de stations, que cette dernière soit locale ou sur le serveur RADIUS.</p>

Tableau 17 Description des champs de la page MAC Authentication (suite)

Champ	Description
Stations List	<p>Il s'agit de la liste locale des clients pour lesquels l'accès au réseau via le point d'accès est soit autorisé, soit refusé.</p> <p>Pour ajouter une adresse MAC à la liste locale des stations, saisissez son adresse MAC de 48 bits dans la zone de texte MAC Address, puis cliquez sur Add.</p> <p>Pour retirer une adresse MAC de la liste des stations, sélectionnez son adresse MAC de 48 bits, puis cliquez sur Remove.</p> <p>Pour les stations appartenant à la liste, l'accès au réseau est soit autorisé, soit refusé, en fonction de la définition du filtre dans le champ précédent.</p> <p>REMARQUE : Si le type d'authentification MAC pour le VAP est défini sur Local, le point d'accès utilise la liste des stations pour permettre ou interdire aux clients d'accéder au réseau. Si le type d'authentification MAC est défini sur RADIUS, le point d'accès ignore les adresses MAC configurées dans cette liste et utilise celle qui est stockée sur le serveur RADIUS. Vous pouvez définir le type d'authentification MAC sur la page de configuration du VAP.</p>



REMARQUE Une fois que les paramètres d'authentification MAC locale sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans ce cas, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Configuration de l'authentification MAC sur le serveur RADIUS

Si vous utilisez l'authentification MAC RADIUS pour le contrôle d'accès basé sur MAC, vous devez configurer une liste de stations sur le serveur RADIUS. Cette liste contient des entrées d'adresse MAC de client et son format est décrit dans le tableau suivant.

Tableau 18 Configuration de l'authentification MAC sur le serveur RADIUS

Attribut du serveur RADIUS	Description	Valeur
User-Name (1)	Adresse MAC de la station de client.	Adresse MAC Ethernet valide.
User-Password (2)	Mot de passe global fixe utilisé pour rechercher une entrée MAC de client.	NOPASSWORD

Modification des paramètres avancés

Les paramètres sans fil avancés contrôlent directement le comportement de la radio sans fil dans le point d'accès et son interaction avec le support physique, c'est-à-dire quel type d'ondes électromagnétiques sont émises par le point d'accès et comment.

Pour définir les paramètres de la radio sans fil, cliquez sur l'onglet **Advanced Settings**.

Figure 17 Configuration des paramètres de la radio sans fil

Getting Started	Status	Setup	Wireless	SNMP	Administration	Cluster
Wireless Radio Settings	Wireless Network Setup (VAPs)	MAC Filtering	Advanced Settings	WDS Bridge	Bandwidth Utilization	

Advanced Settings

Status On Off

Mode

Channel

Channel Bandwidth

Primary Channel

Short Guard Interval Supported

Protection

Beacon Interval (Msec, Range: 20 - 2000)

DTIM Period (Range: 1-255)

Fragmentation Threshold (Range: 256-2346, Even Numbers)

RTS Threshold (Range: 0-2347)

Maximum Stations (Range: 0-200)

Transmit Power

Fixed Multicast Rate Mbps

	Rate Supported	Basic
54 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
48 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
36 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
24 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Rate Sets

Des paramètres différents sont affichés en fonction du mode sélectionné. Le **Tableau 19** décrit les champs et les options de configuration de la page Advanced Settings.

Tableau 19 Description des champs disponibles sur la page Advanced Settings

Champ	Description
Status (On/Off)	<p>Indiquez si la radio sans fil doit être activée ou désactivée en cliquant sur On ou sur Off.</p> <p>Si vous désactivez la radio sans fil, le point d'accès envoie des trames de dissociation à tous les clients sans fil pris en charge afin que la radio sans fil puisse être arrêtée sans problème et que les clients puissent démarrer le processus d'association avec les autres points d'accès disponibles.</p> <p>REMARQUE : Si le statut est défini sur Off, aucun champ ne peut être modifié.</p>
Mode	<p>Le champ Mode définit la norme de couche physique utilisée par la radio sans fil.</p> <p>REMARQUE : Les modes disponibles sur le point d'accès dépendent du paramètre de code de pays.</p> <p>Sélectionnez l'un des modes suivants pour l'interface de la radio sans fil :</p> <ul style="list-style-type: none">▪ 802.11a▪ 802.11b/g▪ 802.11a/n▪ 802.11b/g/n▪ 802.11n 5 GHz▪ 802.11n 2,4 GHz

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
Channel	<p>La plage de canaux disponibles est déterminée par le mode de l'interface de la radio sans fil et le paramètre de code de pays. Si vous sélectionnez Auto pour le paramètre de canal et que le canal Auto est configuré, le point d'accès analyse les canaux disponibles, sélectionne immédiatement un canal et commence à fonctionner. En cas d'interférences ou d'erreurs sur ce canal, un nouveau canal est sélectionné automatiquement.</p> <p>Le canal définit la portion du spectre de la radio sans fil que cette radio sans fil utilise pour l'émission et la réception. Chaque mode propose un certain nombre de canaux, en fonction des conditions de licence du spectre par les autorités nationales et internationales telles que la Federal Communications Commission (FCC) ou l'Union Internationale des Télécommunications (UIT-R).</p>
Channel Bandwidth	<p>Ce champ est disponible uniquement si le mode de la radio sans fil inclut le mode 802.11n.</p> <p>La norme 802.11n permet d'utiliser un canal de 40 MHz en plus du canal de 20 MHz existant disponible dans les autres modes. Le canal de 40 MHz offre de plus hauts débits de données mais laisse moins de canaux disponibles à l'utilisation pour les autres périphériques 2,4 GHz et 5 GHz.</p> <p>Sélectionnez une valeur pour définir l'utilisation de la bande passante du canal.</p> <p>La valeur par défaut est de 20 MHz.</p>

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
Primary Channel	<p>Ce champ est disponible uniquement si le mode de la radio inclut le mode 802.11n.</p> <p>Ce paramètre ne peut être modifié que si la bande passante du canal est définie sur 40 MHz. Le canal de 40 MHz est constitué de deux canaux contigus de 20 MHz du même domaine de fréquences. Ces deux canaux de 20 MHz sont généralement dénommés Primary Channel (principal) et Secondary Channel (secondaire). Le Primary Channel est utilisé pour les clients 802.11n qui prennent uniquement en charge une bande passante de canal de 20 MHz et pour les clients existants.</p> <p>Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> ▪ Upper : définissez le Primary Channel comme canal de 20 MHz supérieur sur la bande de 40 MHz. ▪ Lower : définissez le Primary Channel comme canal de 20 MHz inférieur sur la bande de 40 MHz.
Short Guard Interval Supported	<p>Ce champ est disponible uniquement si le mode de la radio inclut le mode 802.11n.</p> <p>L'intervalle de garde est le temps mort, en nanosecondes, entre les symboles OFDM. Il empêche les interférences inter-symboles et inter-opérateurs (ISI, ICI). Le mode 802.11n permet une réduction de cet intervalle de garde en passant de la définition a et g de 800 nanosecondes à 400 nanosecondes. Cette réduction de l'intervalle de garde peut mener à une amélioration de 10 % du débit de données.</p> <p>Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> ▪ Yes : le point d'accès transmet les données avec un intervalle de garde de 400 ns lorsqu'il communique avec des clients prenant également en charge l'intervalle de garde court. ▪ No : le point d'accès transmet les données avec un intervalle de garde de 800 ns.

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
STBC Mode	<p>Ce champ est disponible uniquement si le mode de la radio inclut le mode 802.11n.</p> <p>Le codage STBC (Space Time Block Coding) est une technique 802.11n destinée à améliorer la fiabilité des transmissions de données. Le flux de données est transmis sur plusieurs antennes afin que le système de réception ait de meilleures chances de détecter au moins l'un de ces flux de données.</p> <p>Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> ▪ On : le point d'accès transmet le même flux de données sur plusieurs antennes en même temps. ▪ Off : le point d'accès ne transmet pas les mêmes données sur plusieurs antennes.
Protection	<p>La fonctionnalité de protection contient des règles qui garantissent que les transmissions 802.11 ne causent aucune interférence avec les stations ou applications existantes. Par défaut, ces mécanismes de protection sont activés (Auto). Lorsque la protection est activée, les mécanismes de protection sont appelés uniquement si les périphériques existants se trouvent à portée du point d'accès.</p> <p>Vous pouvez désactiver (Off) ces mécanismes de protection ; cependant, lorsque la protection est désactivée, les clients ou les points d'accès existants à portée peuvent être affectés par les transmissions 802.11n. La protection est également disponible avec le mode 802.11b/g. Lorsqu'elle est activée dans ce mode, elle protège les clients et les points d'accès 802.11b des transmissions 802.11g.</p> <p>Remarque : ce paramètre n'affecte pas la capacité du client à s'associer au point d'accès.</p>

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
Beacon Interval	<p>Les trames des balises sont transmises par un point d'accès à intervalles réguliers pour annoncer l'existence du réseau sans fil. Le comportement par défaut est l'envoi d'une trame de balise toutes les 100 millisecondes (soit 10 par seconde).</p> <p>Saisissez une valeur comprise entre 20 et 2 000 millisecondes.</p>
DTIM Period	<p>Indiquez une période DTIM comprise entre 1 et 255 trames.</p> <p>Le message DTIM (Delivery Traffic Information Map) est un élément inclus dans certaines trames de balise. Il indique quelles sont les stations de client actuellement en veille en mode basse puissance qui disposent de données en mémoire tampon sur le point d'accès et attendent leur récupération.</p> <p>La période DTIM que vous choisissez indique à quelle fréquence les clients desservis par ce point d'accès doivent vérifier la présence de données en mémoire tampon sur le point d'accès attendant leur récupération.</p> <p>Les balises servent de mesures. Par exemple, si vous définissez ce champ sur 1, les clients vérifient la présence de données en mémoire tampon sur le point d'accès à chaque balise. Si vous le définissez sur 10, les clients vérifient ce paramètre toutes les 10 balises.</p>

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
Fragmentation Threshold	<p>Indiquez un nombre entre 256 et 2 346 pour définir la limite de taille des trames en octets. Le seuil de fragmentation doit être défini sur un nombre pair compris dans la plage valide.</p> <p>Il s'agit d'un moyen de limiter la taille des paquets (trames) transmis sur le réseau. Si un paquet dépasse le seuil de fragmentation défini, la fonction de fragmentation est activée et le paquet est envoyé sous forme de plusieurs trames 802.11.</p> <p>Si le paquet en cours de transmission est égal ou inférieur au seuil, la fragmentation n'est pas utilisée.</p> <p>Si vous définissez le seuil sur la valeur la plus élevée (2 346 octets), la fragmentation se trouve désactivée. Elle n'entre pas en jeu lorsque l'agrégation est activée.</p> <p>La fragmentation implique des coûts d'exploitation plus importants en raison du travail supplémentaire fourni pour diviser et réassembler les trames concernées et de l'augmentation du trafic de messages qu'elle génère sur le réseau. Elle peut cependant contribuer à <i>améliorer</i> les performances et la fiabilité du réseau si elle est configurée correctement.</p> <p>L'envoi de trames plus petites (à l'aide d'un seuil de fragmentation plus bas) peut aider à résoudre certains problèmes d'interférences, par exemple, avec les fours à micro-ondes.</p> <p>Par défaut, la fragmentation est désactivée. Nous vous recommandons de ne pas l'utiliser sauf si vous suspectez la présence d'interférences avec la radio sans fil. Les en-têtes supplémentaires appliqués à chaque fragment augmentent les coûts d'exploitation du réseau et peuvent réduire significativement le débit.</p>

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
RTS Threshold	<p>Indiquez une valeur pour le seuil RTS (Request to Send) comprise entre 0 et 2 347.</p> <p>Le seuil RTS détermine le nombre d'octets d'un MPDU, en dessous duquel aucune liaison RTS/CTS n'est établie.</p> <p>La modification du seuil RTS peut contribuer à contrôler le flux de trafic via le point d'accès, particulièrement s'il possède de nombreux clients. Si la valeur du seuil est basse, les paquets RTS sont envoyés plus fréquemment. Cela a pour effet d'utiliser plus de bande passante et de réduire le débit du paquet. Par ailleurs, l'envoi d'un plus grand nombre de paquets RTS peut aider le réseau à se rétablir en cas d'interférences ou de collisions pouvant se produire si le réseau est occupé ou en cas de perturbations électromagnétiques.</p>
Maximum Stations	<p>Indiquez le nombre maximal de stations autorisées à accéder à ce point d'accès en même temps.</p> <p>Vous pouvez choisir une valeur comprise entre 0 et 200.</p>

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
Transmit Power	<p>Sélectionnez la valeur du niveau de puissance de transmission pour ce point d'accès :</p> <ul style="list-style-type: none">▪ Low▪ Medium▪ High▪ Full <p>La valeur par défaut, qui est Full, peut se révéler plus rentable qu'un niveau inférieur car elle offre au point d'accès une plage de diffusion maximale et réduit le nombre de points d'accès nécessaires.</p> <p>Pour augmenter la capacité du réseau, rapprochez les points d'accès les uns des autres et diminuez la valeur de la puissance de transmission. Vous réduisez ainsi le chevauchement et les interférences entre les points d'accès. Une puissance de transmission plus basse peut également augmenter la sécurité du réseau car des signaux sans fil plus faibles ont moins tendance à se propager en dehors de l'emplacement physique du réseau.</p>
Fixed Multicast Rate	Sélectionnez le débit de transmission de trafic de multidiffusion que le point d'accès doit prendre en charge.

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
Rate Sets	<p>Indiquez les jeux de débits de transmission que le point d'accès doit prendre en charge et les jeux de débits primaires que le point d'accès doit annoncer :</p> <ul style="list-style-type: none"> Le débit (Rate) est exprimé en mégabits par seconde. L'option Supported indique les débits pris en charge par le point d'accès. Vous pouvez sélectionner plusieurs débits (cliquez sur la case pour sélectionner ou désélectionner le débit). Le point d'accès choisit automatiquement le débit le plus efficace en fonction de facteurs tels que le taux d'erreurs et la distance entre les stations de client et le point d'accès. L'option Basic indique les débits que le point d'accès annonce sur le réseau dans le but d'établir la communication avec les autres points d'accès et stations de client sur le réseau. En général, le point d'accès est plus efficace lorsqu'il diffuse un sous-ensemble des jeux de débits qu'il prend en charge.
Broadcast/Multicast Rate Limiting	<p>Si vous activez la limitation du débit de multidiffusion et de diffusion, vous pouvez améliorer les performances globales du réseau en limitant le nombre de paquets transmis.</p> <p>Par défaut, l'option Multicast/Broadcast Rate Limiting est activée. Lorsque cette option Multicast/Broadcast Rate Limiting est désactivée, les champs Rate Limit et Rate Limit Burst ne peuvent pas être modifiés.</p>
Rate Limit	<p>Saisissez la limite de débit à définir pour le trafic de multidiffusion et de diffusion. Cette limite doit être supérieure à 1 ; la valeur maximale est de 100 paquets par seconde (pps). Le trafic situé en dessous de cette limite de débit est toujours conforme et transmis à la destination appropriée.</p> <p>La limite de débit par défaut est de 100 paquets par seconde.</p>

Tableau 19 Description des champs disponibles sur la page Advanced Settings (suite)

Champ	Description
Rate Limit Burst	<p>La définition d'une salve limite de débit détermine la quantité de salves de trafic autorisée avant que l'ensemble du trafic ne dépasse la limite de débit. Cette limite autorise les salves intermittentes de trafic sur un réseau supérieures à la limite de débit définie.</p> <p>La salve limite est comprise entre 1 et 150 paquets par seconde. La salve limite de débit par défaut est de 150 paquets par seconde.</p>

Configuration du système de distribution sans fil (WDS)

Le système WDS (Wireless Distribution System) vous permet de connecter plusieurs points d'accès. Avec le WDS, les points d'accès communiquent entre eux sans câble de manière standardisée. Cette fonctionnalité est essentielle pour faire vivre aux clients itinérants une expérience sans heurts et pour gérer plusieurs réseaux sans fil. Elle permet également de simplifier l'infrastructure réseau en réduisant la quantité de câbles nécessaire. Vous pouvez configurer le point d'accès en mode pont point à point ou point à multipoint en fonction du nombre de liaisons à établir.

En mode point à point, le point d'accès accepte les associations de client et communique avec les clients sans fil et les autres répéteurs. Le point d'accès achemine l'ensemble du trafic destiné à l'autre réseau via le tunnel établi entre les points d'accès. Le pont ne s'ajoute pas au compte des sauts. Il fonctionne comme un simple périphérique réseau OSI de couche 2.

En mode pont point à multipoint, un point d'accès agit en tant que liaison commune entre plusieurs points d'accès. Dans ce mode, le point d'accès central accepte les associations de client et communique avec les clients et les autres répéteurs. Tous les autres points d'accès s'associent uniquement au point d'accès central qui achemine les paquets vers le pont sans fil approprié à des fins de routage.

Le point d'accès peut également agir en tant que répéteur. Dans ce mode, le point d'accès sert de connexion entre deux points d'accès pouvant être trop éloignés l'un de l'autre mais à portée de la cellule. Lorsqu'il agit comme un répéteur, le point d'accès ne dispose pas de connexion câblée au LAN et répète les signaux à l'aide de la connexion sans fil. Aucune configuration spéciale n'est requise pour que le point d'accès fonctionne comme un répéteur et il n'existe aucun paramètre de mode répéteur. Les clients sans fil peuvent toujours se connecter au point d'accès s'il fonctionne en tant que répéteur.

Pour définir les détails de l'échange de trafic depuis ce point d'accès vers les autres, cliquez sur l'onglet **WDS Bridge**.

Figure 18 Configuration des paramètres de pont WDS

The screenshot shows the 'WDS Bridge' configuration page in a network management interface. The page has a blue header with navigation tabs: 'Getting Started', 'Status', 'Setup', 'Wireless', 'SNMP', 'Administration', and 'Cluster'. Below the header, there are several sub-tabs: 'Wireless Radio Settings', 'Wireless Network Setup (VAPs)', 'MAC Filtering', 'Advanced Settings', 'WDS Bridge' (which is highlighted), 'Bandwidth Utilization', and 'QoS Parameters'. The main content area is titled 'WDS Bridge' and contains several configuration sections. The first section has 'Spanning Tree Mode' with radio buttons for 'Enabled' and 'Disabled' (selected), and 'Local Address' with the value '00:21:29:00:1B:00'. The second section has 'WDS Interface' with radio buttons for 'Enabled' and 'Disabled' (selected), 'Remote Address' with the value '00:21:29:00:1C:D0', and 'Encryption' with a dropdown menu set to 'None (Plain-text)'. There are three more identical sections below, each with 'WDS Interface' radio buttons (selected 'Disabled'), empty 'Remote Address' fields, and 'Encryption' dropdowns set to 'None (Plain-text)'. At the bottom, there is a message 'Click "Apply" to save the new settings.' and an 'Apply' button.

Avant de configurer le WDS sur le point d'accès, tenez compte des consignes suivantes :

- Lorsque vous utilisez le WDS, veillez à configurer les paramètres WDS sur les deux points d'accès qui forment le lien WDS.
- Un seul lien WDS peut être établi entre deux points d'accès donnés. En d'autres termes, une adresse MAC distante ne peut apparaître qu'une seule fois sur la page WDS d'un point d'accès particulier.
- Les deux points d'accès formant un lien WDS doivent être sur le même canal de radio sans fil et utiliser le même mode IEEE 802.11. (Pour plus d'informations sur la configuration du mode et du canal de la radio, reportez-vous à la section **Modification des paramètres avancés**, page 89.)
- Lorsque le mode 802.11h est actif, la définition de deux liens WDS peut être difficile. Reportez-vous à la section **Modification des paramètres avancés**, page 89.
- Si vous utilisez le cryptage WPA sur le lien WDS, le mode de sécurité du VAP0 doit être défini sur WPA Personal ou WPA Enterprise.

Pour configurer le WDS sur ce point d'accès, décrivez chaque point d'accès distant destiné à recevoir et à envoyer des informations à ce point d'accès. Pour chaque point d'accès de destination, configurez les champs répertoriés dans le **Tableau 20**.

Tableau 20 Paramètres de pont WDS

Champ	Description
Spanning Tree Mode	Le protocole STP (Spanning Tree Protocol) empêche le basculement des boucles. Il est recommandé si vous configurez des liens WDS. Sélectionnez Enabled pour utiliser le protocole STP. Sélectionnez Disabled pour désactiver les liens STP (non recommandé).
Local Address	Adresse MAC du point d'accès.

Tableau 20 Paramètres de pont WDS (suite)

Champ	Description
Remote Address	<p>Adresse MAC du point d'accès de destination ; le point d'accès qui se trouve à l'autre extrémité du lien WDS auquel les données sont envoyées et depuis lequel les données sont reçues.</p> <p>Cliquez sur la flèche déroulante à droite du champ Remote Address pour afficher une liste de toutes les adresses MAC disponibles et leurs SSID associés sur le réseau. Sélectionnez l'adresse MAC appropriée dans la liste.</p> <p>REMARQUE : Le SSID affiché dans la liste déroulante est le SSID du point d'accès distant.</p>
Encryption	<p>Vous pouvez utiliser le cryptage WEP ou WPA (PSK) sur le lien WDS, ou aucun cryptage.</p> <p>Si vous n'êtes pas préoccupé par des questions de sécurité sur le lien WDS, vous pouvez décider de ne définir aucun type de cryptage. En revanche, en cas de problèmes de sécurité, vous pouvez choisir entre le mode de cryptage Static WEP et WPA (PSK). En mode WPA (PSK), le point d'accès utilise le mécanisme WPA2-PSK avec le cryptage CCMP (AES) sur le lien WDS.</p> <p>REMARQUE : Pour configurer le mode WPA-PSK sur un lien WDS, le VAP0 de la radio sans fil sélectionnée doit être configuré pour WPA-PSK ou WPA-Enterprise.</p>

Si vous sélectionnez **None** comme option de cryptage WDS de préférence, vous ne devez remplir aucun champ supplémentaire sur la page **WDS**. Toutes les données transférées entre les deux points d'accès sur le lien WDS ne sont pas cryptées.



REMARQUE Pour désactiver un lien WDS, vous devez supprimer la valeur configurée dans le champ Remote Address.

Cryptage WEP sur les liens WDS

Le **Tableau 21** décrit les champs supplémentaires qui apparaissent lorsque vous sélectionnez le mode de cryptage WEP.

Tableau 21 Cryptage WEP sur les liens WDS

Champ	Description
Encryption	WEP
WEP	Sélectionnez cette option pour définir le cryptage WEP sur le lien WDS.
Key Length	Si le cryptage WEP est activé, indiquez la longueur de la clé WEP : 64 bits 128 bits
Key Type	Si le cryptage WEP est activé, indiquez le type de la clé WEP : ASCII Hex
Characters Required	Nombre de caractères requis pour la clé WEP. Ce champ est mis à jour automatiquement en fonction de la longueur et du type définis pour la clé.
WEP Key	Saisissez une chaîne de caractères. Si vous sélectionnez ASCII, saisissez une combinaison de caractères compris entre 0 et 9, a et z et A et Z. Si vous sélectionnez HEX, saisissez des chiffres hexadécimaux (combinaison de caractères compris entre 0 et 9 et a et f ou A et F). Il s'agit des clés de cryptage RC4 partagées avec les stations utilisant le point d'accès.

Cryptage WPA/PSK sur les liens WDS

Le **Tableau 22** décrit les champs supplémentaires qui apparaissent lorsque vous sélectionnez le mode de cryptage WPA/PSK.



REMARQUE Pour configurer le mode WPA-PSK sur un lien WDS, le VAP0 de la radio sans fil sélectionnée doit être configuré pour WPA-PSK ou WPA-Enterprise.

Tableau 22 Cryptage WPA/PSK sur les liens WDS

Champ	Description
Encryption	WPA (PSK)
SSID	<p>Saisissez un nom approprié pour le lien WDS que vous avez créé. Ce SSID doit être différent des autres SSID utilisés par ce point d'accès. Cependant, il est important que le même SSID soit également saisi à l'autre extrémité du lien WDS. Si ce SSID n'est pas identique pour les deux points d'accès sur le lien WDS, ils ne peuvent pas communiquer et échanger des données.</p> <p>Le SSID peut être n'importe quelle combinaison de caractères alphanumériques.</p>
Key	<p>Saisissez une clé partagée unique pour le pont WDS. Cette clé partagée unique doit également être saisie pour le point d'accès qui se trouve à l'autre extrémité du lien WDS. Si cette clé n'est pas identique pour les deux points d'accès, ils ne peuvent pas communiquer et échanger des données.</p> <p>La clé WPA-PSK est une chaîne constituée de 8 à 63 caractères. Les caractères autorisés sont les lettres majuscules et minuscules, les chiffres et les symboles spéciaux tels que « @ » et « # ».</p>



REMARQUE Une fois que les paramètres WDS sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans ce cas, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Utilisation de la bande passante

Vous pouvez définir des seuils d'utilisation du réseau sur le point d'accès pour maintenir la vitesse et les performances du réseau sans fil lorsque les clients s'associent au point d'accès et s'en dissocient.

Pour configurer l'équilibrage des charges et définir les limites et le comportement qu'un taux d'utilisation donné sur le point d'accès doit déclencher, cliquez sur l'onglet **Bandwidth Utilization** et mettez à jour les champs qui apparaissent dans la figure suivante.

Figure 19 Configuration de l'utilisation de la bande passante

Tableau 23 Utilisation de la bande passante

Champ	Description
Bandwidth Utilization	<p>Activez ou désactivez l'utilisation de la bande passante comme suit :</p> <p>Pour activer l'utilisation de la bande passante sur le point d'accès, cliquez sur Enable.</p> <p>Pour désactiver l'utilisation de la bande passante sur le point d'accès, cliquez sur Disable.</p>
Maximum Utilization Threshold	<p>Indiquez le pourcentage d'utilisation de la bande passante du réseau autorisé sur la radio sans fil avant que le point d'accès ne cesse d'accepter de nouvelles associations de client.</p> <p>La valeur par défaut est 0, ce qui signifie que toutes les nouvelles associations sont autorisées, quel que soit le taux d'utilisation.</p>



REMARQUE Une fois que les paramètres d'utilisation de la bande passante sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans ce cas, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Configuration de la qualité de service (QoS)

La qualité de service (QoS) vous permet de déterminer des paramètres sur plusieurs files d'attente pour un débit plus élevé et de meilleures performances du trafic sans fil différencié, comme la *voix sur IP (VoIP)*, les autres types de contenu audio, vidéo et de flux, ainsi que les données IP traditionnelles sur le point d'accès.

La configuration de la QoS sur le point d'accès consiste à définir des paramètres sur les files d'attente existantes pour différents types de trafic sans fil et à spécifier les délais d'attente minimal et maximal (via les *fenêtres Contention*) pour les transmissions. Les paramètres décrits ici concernent le comportement de transmission des données sur le point d'accès uniquement, pas sur les stations de client.

Les paramètres EDCA (Enhanced Distributed Channel Access) du point d'accès affectent le trafic passant du point d'accès à la station de client.

Les paramètres EDCA (Enhanced Distributed Channel Access) de la station affectent le trafic passant de la station de client au point d'accès.

Les valeurs par défaut des paramètres EDCA du point d'accès et de la station sont celles qui sont proposées par l'association Wi-Fi Alliance dans ses informations relatives à la fonction Wi-Fi Multimedia (WMM). Pour une utilisation normale, ces valeurs n'ont pas besoin d'être modifiées. Si elles le sont, cela affecte la QoS fournie.

Pour configurer des files d'attente pour la QoS, cliquez sur l'onglet **QoS** sous l'entête **Services** et définissez les paramètres comme le décrit le [Tableau 24](#).

Figure 20 Configuration des paramètres QoS

QoS Parameters

QoS Presets: WFA Defaults (selected), Factory Defaults, WFA Defaults, Optimized for Voice, Custom

AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Wi-Fi Multimedia (WMM) Enabled Disabled

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	63	1023	0

Tableau 24 Paramètres QoS

Champ	Description
<i>Paramètres EDCA du point d'accès</i>	
Queue	<p>Les files d'attente sont définies pour différents types de données transmises du point d'accès vers la station :</p> <p>Data 0 (Voix) : file d'attente avec priorité haute, délai minimal. Les données dépendantes du temps, comme les supports VoIP et de flux, sont envoyées automatiquement vers la file d'attente.</p> <p>Data 1 (Vidéo) : file d'attente avec priorité haute, délai minimal. Les données vidéo dépendantes du temps sont envoyées automatiquement vers la file d'attente.</p> <p>Data 2 (Au mieux) : file d'attente avec priorité moyenne, débit et délai moyens. Les données IP les plus traditionnelles sont envoyées vers cette file d'attente.</p> <p>Data 3 (Arrière-plan) : file d'attente avec priorité basse, haut débit. Les données de masse qui nécessitent un débit maximal et ne dépendent pas du temps sont envoyées vers cette file d'attente (données FTP, par exemple).</p>

Tableau 24 Paramètres QoS (suite)

Champ	Description
AIFS (Inter-Frame Space)	<p>Le paramètre AIFS (Arbitration Inter-Frame Spacing) définit un délai d'attente pour les trames de données. Ce délai d'attente s'exprime en emplacements. Les valeurs valides pour l'AIFS sont comprises entre 1 et 255.</p>
cwMin (Minimum Contention Window)	<p>Ce paramètre est entré dans l'algorithme qui détermine le délai d'attente de déblocage aléatoire initial (fenêtre) avant une nouvelle tentative de transmission.</p> <p>La valeur indiquée pour la fenêtre Minimum Contention est la limite supérieure (en millisecondes) de la plage à partir de laquelle le délai d'attente de déblocage aléatoire initial est déterminé.</p> <p>Le premier nombre aléatoire généré est compris entre 0 et le nombre indiqué ici.</p> <p>Si le premier délai d'attente de déblocage aléatoire expire avant l'envoi de la trame de données, le nombre de tentatives est augmenté et la valeur de déblocage aléatoire (fenêtre) est doublée. Le doublement se poursuit jusqu'à ce que la valeur de déblocage aléatoire atteigne le nombre défini dans la fenêtre Maximum Contention.</p> <p>Les valeurs valides pour le paramètre cwMin sont 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1023. Cette valeur doit être inférieure ou égale à la valeur du paramètre cwMax.</p>
cwMax (Maximum Contention Window)	<p>La valeur indiquée pour la fenêtre Maximum Contention est la limite supérieure (en millisecondes) pour le doublement de la valeur de déblocage aléatoire. Ce doublement se poursuit jusqu'à ce que la trame de données soit envoyée ou que la valeur de la fenêtre Maximum Contention soit atteinte.</p> <p>Une fois cette valeur atteinte, les tentatives continuent jusqu'à ce que le nombre maximal de tentatives autorisé soit atteint.</p> <p>Les valeurs valides pour le paramètre cwMax sont 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1023. Cette valeur doit être supérieure ou égale à la valeur du paramètre cwMin.</p>

Tableau 24 Paramètres QoS (suite)

Champ	Description
Max. Burst	<p>Le paramètre Max. Burst est un paramètre EDCA du point d'accès qui concerne uniquement le trafic passant du point d'accès à la station de client.</p> <p>Cette valeur détermine (en millisecondes) la longueur de salve maximale autorisée pour les salves de paquets sur le réseau sans fil. Une salve de paquets est un ensemble de plusieurs trames transmises sans informations d'en-tête. La diminution des frais généraux entraîne un plus haut débit et de meilleures performances.</p> <p>Les valeurs valides pour la longueur de salve maximale sont comprises entre 0,0 et 999,0.</p>
<i>Paramètres WMM (Wi-Fi Multimedia)</i>	
Wi-Fi MultiMedia (WMM)	<p>Le WMM (Wi-Fi Multimedia) est activé par défaut. Si le WMM est activé, la hiérarchisation QoS et la coordination de l'accès aux supports sans fil sont également activées. Dans ce cas, les paramètres QoS du point d'accès contrôlent le trafic <i>descendant</i> passant du point d'accès à la station de client (paramètres EDCA du point d'accès) et le trafic <i>montant</i> passant de la station au point d'accès (paramètres EDCA de la station).</p> <p>La désactivation du WMM désactive également le contrôle QoS des paramètres EDCA de la station sur le trafic <i>montant</i> passant de la station au point d'accès.</p> <p>Si le WMM est désactivé, tous les champs situés en dessous ne peuvent pas être modifiés.</p> <p>Pour désactiver le WMM, cliquez sur Disabled.</p> <p>Pour activer le WMM, cliquez sur Enabled.</p>

Tableau 24 Paramètres QoS (suite)

Champ	Description
<i>Paramètres EDCA de la station</i>	
Queue	<p>Les files d'attente sont définies pour différents types de données transmises de la station vers le point d'accès :</p> <p>Data 0 (Voix) : file d'attente avec la priorité la plus haute, délai minimal. Les données dépendantes du temps, comme les supports VoIP et de flux, sont envoyées automatiquement vers la file d'attente.</p> <p>Data 1 (Vidéo) : file d'attente avec la priorité la plus haute, délai minimal. Les données vidéo dépendantes du temps sont envoyées automatiquement vers la file d'attente.</p> <p>Data 2 (Au mieux) : file d'attente avec priorité moyenne, débit et délai moyens. Les données IP les plus traditionnelles sont envoyées vers cette file d'attente.</p> <p>Data 3 (Arrière-plan) : file d'attente avec priorité basse, haut débit. Les données de masse qui nécessitent un débit maximal et ne dépendent pas du temps sont envoyées vers cette file d'attente (données FTP, par exemple).</p>
AIFS (Inter-Frame Space)	Le paramètre AIFS (Arbitration Inter-Frame Spacing) définit un délai d'attente pour les trames de données. Ce délai d'attente s'exprime en emplacements. Les valeurs valides pour l'AIFS sont comprises entre 1 et 255.
cwMin (Minimum Contention Window)	Ce paramètre est utilisé par l'algorithme qui détermine le délai d'attente aléatoire initial pour la transmission des données pendant une certaine période de contention pour les ressources du point d'accès. La valeur indiquée ici dans la fenêtre Minimum Contention est la limite supérieure à partir de laquelle le délai d'attente de déblocage aléatoire initial est défini. Le premier nombre aléatoire généré est compris entre 0 et le nombre indiqué ici. Si le délai expire avant l'envoi de la trame de données, le nombre de tentatives est incrémenté et la valeur de déblocage aléatoire est doublée. Le doublement se poursuit jusqu'à ce que la valeur de déblocage aléatoire atteigne le nombre défini dans la fenêtre Maximum Contention.

Tableau 24 Paramètres QoS (suite)

Champ	Description
cwMax (Maximum Contention Window)	<p>La valeur indiquée ici dans la <i>fenêtre Maximum Contention</i> est la limite supérieure (en millisecondes) pour le doublement de la valeur de déblocage aléatoire. Ce doublement se poursuit jusqu'à ce que la trame de données soit envoyée ou que la valeur de la fenêtre Maximum Contention soit atteinte.</p> <p>Une fois cette valeur atteinte, les tentatives continuent jusqu'à ce que le nombre maximal de tentatives autorisé soit atteint.</p>
TXOP Limit	<p>La limite TXOP est un paramètre EDCA de la station qui concerne uniquement le trafic passant de la station de client au point d'accès. Le TXOP (Transmission Opportunity) est l'intervalle de temps, en millisecondes, pendant lequel un client peut lancer des transmissions vers le point d'accès. La valeur maximale de la limite TXOP est de 65 535.</p>
<i>Autres paramètres QoS</i>	
No Acknowledgement	<p>Sélectionnez On pour indiquer que le point d'accès ne doit pas valider les trames dont la valeur de classe de service est QoSNoAck.</p>
Automatic Power Save Delivery	<p>Sélectionnez On pour activer l'APSD (Automatic Power Save Delivery), qui est une méthode de gestion de l'alimentation. L'APSD est la méthode recommandée si les téléphones VoIP accèdent au réseau via le point d'accès.</p>



REMARQUE Une fois que les paramètres QoS sont configurés, vous devez cliquer sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans ce cas, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

SNMP

Configuration du SNMP sur le point d'accès

Le protocole SNMP (Simple Network Management Protocol) définit une norme d'enregistrement, de stockage et de partage des informations pour les périphériques du réseau. Le protocole SNMP facilite la gestion, le dépannage et la maintenance du réseau. Le point d'accès prend en charge les versions SNMP 1, 2 et 3. Sauf indications spécifiques, tous les paramètres de configuration figurant sur cette page s'appliquent aux protocoles SNMPv1 et SNMPv2c uniquement.

Les principaux composants de tout réseau géré par SNMP sont des périphériques gérés, des agents SNMP et un système de gestion. Les agents stockent les données concernant leurs périphériques dans des MIB (Management Information Bases) et renvoient ces données au gestionnaire SNMP sur demande. Les périphériques gérés peuvent être des nœuds de réseau tels que des points d'accès, routeurs, commutateurs, ponts, concentrateurs, serveurs ou imprimantes.

Le point d'accès peut fonctionner comme un périphérique SNMP géré permettant une intégration transparente dans des systèmes de gestion réseau tels que HP OpenView.

Vous pouvez, à partir de la page **SNMP**, démarrer ou arrêter le contrôle des agents SNMP, configurer les mots de passe de communauté, accéder aux MIB et configurer les destinations du déroulement SNMP.

Vous pouvez, à partir des pages figurant sous l'en-tête SNMP, gérer les utilisateurs SNMPv3 ainsi que leurs niveaux de sécurité et définir le contrôle d'accès aux MIB SNMP. Pour obtenir plus d'informations sur la configuration des vues, groupes, utilisateurs et cibles SNMPv3, reportez-vous à **Configuration des vues SNMP, page 118**.

Pour configurer le SNMP, cliquez sur l'onglet **General** sous l'en-tête **SNMP** et mettez à jour les champs décrits dans le **Tableau 25, page 114**.

Figure 21 Modification des paramètres SNMP

Getting Started Status Setup Wireless **SNMP** Administration Cluster

General Views Groups Users Targets

General SNMP Settings

SNMP Enabled Disabled

Read-only community name (for permitted SNMP get operations)

Port number the SNMP agent will listen to

Allow SNMP set requests Enabled Disabled

Read-write community name (for permitted SNMP set operations)

Restrict the source of SNMP requests to only the designated hosts or subnets Enabled Disabled

Hostname, address, or subnet of Network Management System

Trap Destinations

Community name for traps

Enabled Hostname or IP Address

Tableau 25 Paramètres SNMP

Champ	Description
SNMP Enabled/Disabled	<p>Vous pouvez spécifier le mode d'administration SNMP sur votre réseau. Par défaut, le SNMP est désactivé. Pour activer le SNMP, cliquez sur Enabled. Pour désactiver le SNMP, cliquez sur Disabled. Après la modification du mode, cliquez sur Apply pour enregistrer les modifications apportées à la configuration.</p> <p>REMARQUE : Si vous désactivez le SNMP, tous les champs restants figurant sur la page SNMP sont désactivés. Il s'agit d'un paramètre SNMP global qui s'applique à SNMPv1, SNMPv2c et SNMPv3.</p>

Tableau 25 Paramètres SNMP (suite)

Champ	Description
Read-only community name (for permitted SNMP get operations)	<p>Saisissez un nom de communauté en lecture seule.</p> <p>Le nom de communauté, tel qu'il est défini dans SNMPv2c, agit comme un simple mécanisme d'authentification permettant de limiter les machines du réseau capables de demander des données à l'agent SNMP. Ce nom fonctionne comme un mot de passe et la requête est considérée comme authentique si l'expéditeur connaît le mot de passe.</p> <p>Le nom de communauté peut avoir un format alphanumérique. Le guillemet (") n'est pas un caractère valide.</p>
Port number the SNMP agent will listen to	<p>Par défaut, l'agent SNMP écoute uniquement les requêtes émanant du port 161. Cependant, vous pouvez configurer ce paramètre afin que l'agent puisse écouter les requêtes émanant d'un autre port.</p> <p>Saisissez le numéro du port dont vous souhaitez que les agents SNMP écoutent les requêtes.</p> <p>REMARQUE : Il s'agit d'un paramètre SNMP global qui s'applique à SNMPv1, SNMPv2c et SNMPv3.</p>
Allow SNMP set requests	<p>Vous pouvez choisir d'autoriser les requêtes du dispositif SNMP définies sur le point d'accès. L'activation des requêtes du dispositif SNMP définies signifie que les machines du réseau peuvent modifier la configuration en utilisant l'agent SNMP du point d'accès dans la MIB Cisco du système.</p> <p>Pour activer les requêtes du dispositif SNMP, cliquez sur Enabled.</p> <p>Pour désactiver les requêtes du dispositif SNMP, cliquez sur Disabled.</p>

Tableau 25 Paramètres SNMP (suite)

Champ	Description
Read-write community name (for permitted SNMP set operations)	<p>Si vous avez activé les requêtes du dispositif SNMP, vous pouvez définir un nom de communauté lecture-écriture.</p> <p>Définir un nom de communauté équivaut à définir un mot de passe. Seules les requêtes émanant de machines identifiées à l'aide de ce nom de communauté sont acceptées.</p> <p>Le nom de communauté peut être un format alphanumérique. Le guillemet (") n'est pas un caractère valide.</p>
Restrict the source of SNMP requests to only the designated hosts or subnets	<p>Vous pouvez limiter la source des requêtes SNMP autorisées.</p> <p>Pour limiter la source des requêtes SNMP autorisées, cliquez sur Enabled.</p> <p>Pour autoriser toute source transmettant une requête SNMP, cliquez sur Disabled.</p>

Tableau 25 Paramètres SNMP (suite)

Champ	Description
Hostname, address or subnet of Network Management System	<p>Spécifiez le nom d'hôte ou le sous-réseau DNS IPv4 des machines pouvant exécuter les requêtes <i>get</i> et <i>set</i> vers les périphériques gérés.</p> <p>Comme pour les noms de communauté, cela fournit un niveau de sécurité aux paramètres SNMP. L'agent SNMP accepte uniquement les requêtes émanant du nom d'hôte ou du sous-réseau spécifié ici.</p> <p>Pour spécifier un sous-réseau, saisissez une ou plusieurs plages d'adresses de sous-réseau sous la forme <i>adresse/longueur_masque</i> où <i>adresse</i> correspond à une adresse IP et <i>longueur_masque</i> correspond au nombre de bits du masque. Les formats <i>adresse/masque</i> et <i>adresse/longueur_masque</i> sont pris en charge. Des hôtes individuels peuvent être fournis, adresse IP ou nom d'hôte par exemple. Par exemple, si vous saisissez la plage <code>192.168.1.0/24</code>, cela spécifie un sous-réseau avec une adresse <code>192.168.1.0</code> et un masque de sous-réseau <code>255.255.255.0</code>.</p> <p>Cette plage d'adresses est utilisée pour spécifier le sous-réseau du NMS désigné. Seules les machines dont les adresses IP sont comprises dans cette plage sont autorisées à exécuter des requêtes Collecter et Définir sur le périphérique géré. Compte tenu de l'exemple ci-dessus, les machines dont les adresses sont comprises entre <code>192.168.1.1</code> et <code>192.168.1.254</code> peuvent exécuter des commandes SNMP sur le périphérique. (L'adresse identifiée par le suffixe <code>.0</code> dans la plage de sous-réseau est toujours réservée à l'adresse de sous-réseau et l'adresse identifiée par <code>.255</code> est toujours réservée à l'adresse de diffusion.)</p> <p>Par exemple, si vous saisissez une plage <code>10.10.1.128/25</code>, les machines dont les adresses IP sont comprises entre <code>10.10.1.129</code> et <code>10.10.1.254</code> peuvent exécuter des requêtes SNMP sur les périphériques gérés. Dans cet exemple, <code>10.10.1.128</code> correspond à l'adresse de réseau et <code>10.10.1.255</code> à l'adresse de diffusion. 126 adresses sont désignées.</p>

Tableau 25 Paramètres SNMP (suite)

Champ	Description
Community name for traps	<p>Saisissez la chaîne de communauté globale associée aux déroutements SNMP.</p> <p>Les déroutements envoyés par le périphérique fournissent cette chaîne qui fonctionne comme un nom de communauté.</p> <p>Le nom de communauté peut être un format alphanumérique. Les caractères spéciaux ne sont pas autorisés. Le guillemet (") n'est pas un caractère valide.</p>
Hostname or IP address	<p>Saisissez le nom d'hôte DNS de l'ordinateur auquel vous souhaitez envoyer les déroutements SNMP. Exemple de nom d'hôte DNS : <code>snmptraps.foo.com</code>. Les déroutements SNMP étant envoyés de manière aléatoire par l'agent SNMP, il est utile d'indiquer où exactement les déroutements devraient être envoyés. Vous pouvez ajouter trois noms d'hôte DNS maximum.</p> <p>Cochez la case Enabled à côté du nom d'hôte approprié.</p>



REMARQUE Après la configuration des paramètres SNMP, cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres. La modification de certains paramètres peut entraîner l'arrêt du point d'accès et le redémarrage des processus système. Si cela se produit, la connectivité des clients sans fil est temporairement perdue. Il est recommandé de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Configuration des vues SNMP

Une vue MIB est la combinaison d'un ensemble d'arborescences secondaires de vues ou une famille d'arborescences secondaires de vues où chaque arborescence secondaire de vue correspond à une arborescence secondaire au sein de l'arbre de dénomination de l'objet géré. Vous pouvez créer des vues MIB pour contrôler la plage OID accessible aux utilisateurs SNMPv3.

Une vue MIB appelée **all** et contenant tous les objets de gestion pris en charge par le système est créée par défaut.



REMARQUE Si vous créez une arborescence secondaire de vue *exclude*, créez l'entrée *include* correspondante avec le même nom de vue pour autoriser l'inclusion des arborescences secondaires situées à l'extérieur de l'arborescence secondaire exclue. Par exemple, pour créer une vue excluant l'arborescence secondaire 1.3.6.1.4, créez une entrée *exclude* à l'aide de l'OID 1.3.6.1.4. Puis, créez une entrée *include* à l'aide de l'OID .1 avec le même nom de vue.

Figure 22 Vues SNMPv3

The screenshot shows the 'SNMP Views' configuration page. At the top, there are navigation tabs: 'Getting Started', 'Status', 'Setup', 'Wireless', 'SNMP', 'Administration', and 'Cluster'. Below these are sub-tabs: 'General', 'Views', 'Groups', 'Users', and 'Targets'. The main content area is titled 'SNMP Views' and contains a table with the following columns: 'View Name', 'Type', 'OID', and 'Mask'. Below the table is an 'Add' button. Underneath, there is a section labeled 'SNMPV3 VIEWS' containing a list of two views: 'view-all---included---.1---' and 'view-none---excluded---.1---'. Below this list is a 'Remove' button. At the bottom, there is a message: 'Click "Apply" to save the new settings.' and an 'Apply' button.

Le **Tableau 26** décrit les champs que vous pouvez configurer sur la page SNMPv3 Views.

Tableau 26 Vues SNMPv3

Champ	Description
View Name	<p>Saisissez un nom pour identifier la vue MIB.</p> <p>Les noms de vues peuvent contenir jusqu'à 32 caractères alphanumériques. Le guillemet (") n'est pas un caractère valide.</p>
Type	Spécifie l'inclusion ou l'exclusion de l'arborescence secondaire de vue ou de la famille d'arborescences secondaires à/de la vue MIB.
OID	<p>Saisissez la chaîne OID de l'arborescence secondaire à inclure ou exclure de la vue. La chaîne OID peut contenir jusqu'à 256 caractères.</p> <p>Par exemple, l'arborescence secondaire du système est spécifiée à l'aide de la chaîne OID .1.3.6.1.2.1.1.</p>
Mask	<p>Le masque OID peut contenir jusqu'à 47 caractères. Le format du masque OID est xx.xx.xx...ou xx.xx.xx... et sa longueur est de 16 octets. Chaque octet est composé de deux caractères hexadécimaux séparés par un « . » (point) ou « : » (deux-points). Ce champ n'accepte que les caractères hexadécimaux. Par exemple, le masque OID FA.80 est 11111010.10000000.</p> <p>Un masque de famille est utilisé pour définir une famille d'arborescences secondaires de vues. Le masque de famille indique quels identifiants secondaires de la chaîne OID de la famille associée sont significatifs par rapport à la définition de la famille.</p> <p>Une famille d'arborescences secondaires de vues permet le contrôle de l'accès à une rangée de tableau de manière plus efficace.</p>
SNMPv3 Views	Ce champ affiche les vues MIB sur le point d'accès. Pour supprimer une vue, sélectionnez-la et cliquez sur Remove .



REMARQUE Après la configuration des vues SNMPv3, cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres.

Configuration des groupes SNMP

Les groupes SNMPv3 permettent de regrouper les utilisateurs dans des groupes disposant de privilèges d'autorisation et d'accès différents.

Par défaut, le point d'accès dispose de trois groupes :

- **RO** : un groupe en lecture seule sans authentification ni cryptage des données. Aucune sécurité n'est fournie par ce groupe. Par défaut, les utilisateurs de ce groupe disposent d'un accès en lecture à toutes les vues MIB par défaut pouvant être modifiées par l'utilisateur.
- **RWAuth** : un groupe en lecture/écriture utilisant l'authentification mais pas le cryptage des données. Les utilisateurs de ce groupe envoient des messages SNMP utilisant une clé/un mot de passe MD5 pour l'authentification, mais pas de clé/mot de passe DES pour le cryptage. Par défaut, les utilisateurs de ce groupe disposent d'un accès en lecture et en écriture à toutes les vues MIB par défaut pouvant être modifiées par l'utilisateur.
- **RWPriv** : un groupe en lecture/écriture utilisant l'authentification et le cryptage des données. Les utilisateurs de ce groupe utilisent une clé/un mot de passe MD5 pour l'authentification et une clé/un mot de passe DES pour le cryptage. Les clés et mots de passe MD5 et DES doivent être définis. Par défaut, les utilisateurs de ce groupe disposent d'un accès en lecture et en écriture à toutes les vues MIB par défaut pouvant être modifiées par l'utilisateur.

Les groupes RWPriv, RWAuth et RO sont définis par défaut.

Pour définir des groupes supplémentaires, accédez à la page **SNMP Groups** et configurez les paramètres décrits dans le [Tableau 27](#).

Figure 23 Groupes SNMPv3

The screenshot shows the 'SNMP Groups' configuration page. At the top, there are navigation tabs: Getting Started, Status, Setup, Wireless, **SNMP**, Administration, and Cluster. Below these are sub-tabs: General, Views, **Groups**, Users, and Targets. The main content area is titled 'SNMP Groups' and contains a form with the following fields:

- Name:** An empty text input field.
- Security Level:** A dropdown menu set to 'noAuthentication-noPrivacy'.
- Write Views:** A dropdown menu set to 'view-all'.
- Read Views:** A dropdown menu set to 'view-all'.
- Add:** A button to add the new group.

Below the form, there is a section titled 'SNMPv3 GROUPS' containing a list of existing groups:

- RO--noAuthNoPriv--view-none--view-all
- RWAuth--authNoPriv--view-all--view-all
- RWPriv--authPriv--view-all--view-all

There is a 'Remove' button below the list. At the bottom of the page, there is a note: 'Click "Apply" to save the new settings.' and an 'Apply' button.

Tableau 27 Groupes SNMPv3

Champ	Description
Name	<p>Spécifiez un nom permettant d'identifier le groupe. Les noms de groupe par défaut sont RWPriv, RWAuth et RO.</p> <p>Les noms de groupes peuvent contenir jusqu'à 32 caractères alphanumériques. Le guillemet (") n'est pas un caractère valide.</p>

Tableau 27 Groupes SNMPv3

Champ	Description
Security Level	<p>Sélectionnez l'un des niveaux de sécurité suivants pour le groupe :</p> <p>noAuthentication-noPrivacy : pas d'authentification ni de cryptage des données (aucune sécurité).</p> <p>Authentication-noPrivacy : authentification mais pas de cryptage des données. Avec ce niveau de sécurité, les utilisateurs envoient des messages SNMP utilisant une clé/un mot de passe MD5 pour l'authentification, mais pas de clé/mot de passe DES pour le cryptage.</p> <p>Authentication-Privacy : authentification et cryptage des données. Avec ce niveau de sécurité, les utilisateurs envoient une clé/un mot de passe MD5 pour l'authentification et une clé/un mot de passe DES pour le cryptage.</p> <p>Pour les groupes nécessitant une authentification, un cryptage ou les deux, définissez les clés et mots de passe MD5 et DES sur la page SNMPv3 Users.</p>
Write Views	<p>Sélectionnez l'accès en écriture des objets de gestion (MIB) du groupe :</p> <p>write-all : le groupe peut créer, modifier et supprimer les MIB.</p> <p>write-none : le groupe n'est pas autorisé à créer, modifier ou supprimer les MIB.</p>
Read Views	<p>Sélectionnez l'accès en lecture des objets de gestion (MIB) du groupe :</p> <p>view-all : le groupe est autorisé à afficher et lire toutes les MIB.</p> <p>view-none : le groupe ne peut pas afficher ou lire les MIB.</p>
SNMPv3 Groups	<p>Ce champ affiche les groupes par défaut et les groupes définis sur le point d'accès. Pour supprimer un groupe, sélectionnez-le et cliquez sur Remove.</p>



REMARQUE Après la configuration des paramètres SNMPv3 Groups, cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres.

Configuration des utilisateurs SNMP

Sur la page **SNMP Users**, vous pouvez définir plusieurs utilisateurs, associer le niveau de sécurité souhaité à chaque utilisateur et configurer des clés de sécurité.

Pour l'authentification, seul le type MD5 est pris en charge et pour le cryptage, seul le type DES est pris en charge. Il n'y a pas d'utilisateurs SNMPv3 par défaut sur le point d'accès.

Figure 24 Utilisateurs SNMPv3

Le **Tableau 28** décrit les champs permettant de configurer les utilisateurs SNMPv3.

Tableau 28 Utilisateurs SNMP v3

Champ	Description
Name	Saisissez le nom d'utilisateur permettant d'identifier l'utilisateur SNMPv3. Les noms d'utilisateurs peuvent contenir jusqu'à 32 caractères alphanumériques. Le guillemet (") n'est pas un caractère valide.

Tableau 28 Utilisateurs SNMP v3 (suite)

Champ	Description
Group	Mappez l'utilisateur vers un groupe. Les groupes par défaut sont RWAuth, RWPriv et RO. Vous pouvez définir des groupes supplémentaires sur la page SNMP Groups .
Authentication Type	Sélectionnez le type d'authentification à utiliser sur les requêtes SNMP de l'utilisateur : <p>MD5 : demandez une authentification MD5 sur les requêtes SNMPv3 de l'utilisateur.</p> <p>None : les requêtes SNMPv3 de cet utilisateur ne nécessitent pas d'authentification.</p>
Authentication Key	Si vous spécifiez MD5 comme type d'authentification, saisissez un mot de passe pour permettre à l'agent SNMP d'authentifier les requêtes envoyées par l'utilisateur. Ce mot de passe doit contenir entre 8 et 32 caractères.
Encryption Type	Sélectionnez le type de confidentialité à utiliser sur les requêtes SNMP de l'utilisateur : <p>DES : utilisez le cryptage DES sur les requêtes SNMPv3 de l'utilisateur.</p> <p>None : les requêtes SNMPv3 de cet utilisateur ne nécessitent pas de paramètres de confidentialité.</p>
Encryption Key	Si vous spécifiez DES comme type de confidentialité, saisissez une clé à utiliser pour le cryptage des requêtes SNMP. Ce mot de passe doit contenir entre 8 et 32 caractères.
SNMPv3 Users	Ce champ affiche les utilisateurs définis sur le point d'accès. Pour supprimer un utilisateur, sélectionnez-le et cliquez sur Remove .



REMARQUE Après la configuration des paramètres SNMPv3 Users, cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres.

Cibles SNMP

Les cibles SNMPv3 envoient des messages de déROUTement au gestionnaire SNMP. Chaque cible est identifiée à l'aide d'un nom cible et associée à une adresse IP, un port UDP et un nom d'utilisateur SNMP cibles.

Figure 25 Cible SNMPv3

Tableau 29 Cibles SNMPv3

Champ	Description
IP Address	Saisissez l'adresse IP du gestionnaire SNMP à distance pour recevoir la cible.
Port	Saisissez le port UDP à utiliser pour l'envoi des cibles SNMP.
Users	Saisissez le nom de l'utilisateur SNMP à associer à la cible. Pour configurer les utilisateurs SNMP, reportez-vous à la Configuration des utilisateurs SNMP, page 124 .
SNMPv3 Targets	Ce champ affiche les cibles SNMPv3 sur le point d'accès. Pour supprimer une cible, sélectionnez-la et cliquez sur Remove .



REMARQUE Après la configuration des paramètres SNMPv3 Target, cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres.

Administration

Administrateur

Cette page permet de configurer les informations relatives à l'administrateur, ainsi que d'entrer un nouveau mot de passe d'administration associé au point d'accès. Le mot de passe par défaut est *cisco*.



REMARQUE Afin d'assurer la sécurité de votre réseau sans fil, il est recommandé de modifier le mot de passe d'administration par défaut le plus tôt possible.

Figure 26 Page de configuration de l'administrateur

Getting Started Status Setup Wireless SNMP Administration Cluster

Administrator AP Configuration Software Upgrade Event Logs Web Server Administration Access Control

Administrator

Administrator Information

Administrator Name

Administrator Contact

Access Point Location

Change Password

Current Password

New Password

Confirm New Password

Click "Apply" to save the new settings.

Le **Tableau 30** décrit les champs et options de configuration disponibles sur la page **Administrator**.

Tableau 30 Page Administrator

Champ	Description
Administrator Name	Entrez le nom de l'administrateur. Vous pouvez entrer jusqu'à 64 caractères alphanumériques ou symboles [valeurs ASCII de 32 à 126 caractères, à l'exclusion des guillemets ("")].
Administrator Contact	Entrez l'adresse e-mail ou le numéro de téléphone de la personne à contacter pour tout problème relatif au point d'accès. Vous pouvez entrer jusqu'à 255 caractères alphanumériques ou symboles (valeurs ASCII de 32 à 126 caractères, à l'exclusion des guillemets).
Access Point Location	Entrez l'emplacement physique du point d'accès, par exemple <i>Salle de conférence A</i> . Vous pouvez entrer jusqu'à 255 caractères alphanumériques ou symboles (valeurs ASCII de 32 à 126 caractères, à l'exclusion des guillemets).
Current Password	Saisissez le mot de passe actuel de l'administrateur. Vous devez entrer le mot de passe actuel correct pour être en mesure de le modifier.
New Password	Saisissez le nouveau mot de passe de l'administrateur. Les caractères apparaissent sous forme de points pour empêcher les autres personnes de voir le mot de passe lorsque vous le saisissez. Le mot de passe de l'administrateur doit consister en une chaîne de huit caractères alphanumériques au maximum. N'utilisez pas de caractères spéciaux ni d'espaces.
Confirm New Password	Saisissez une nouvelle fois le nouveau mot de passe de l'administrateur pour confirmer qu'il correspond à votre choix.

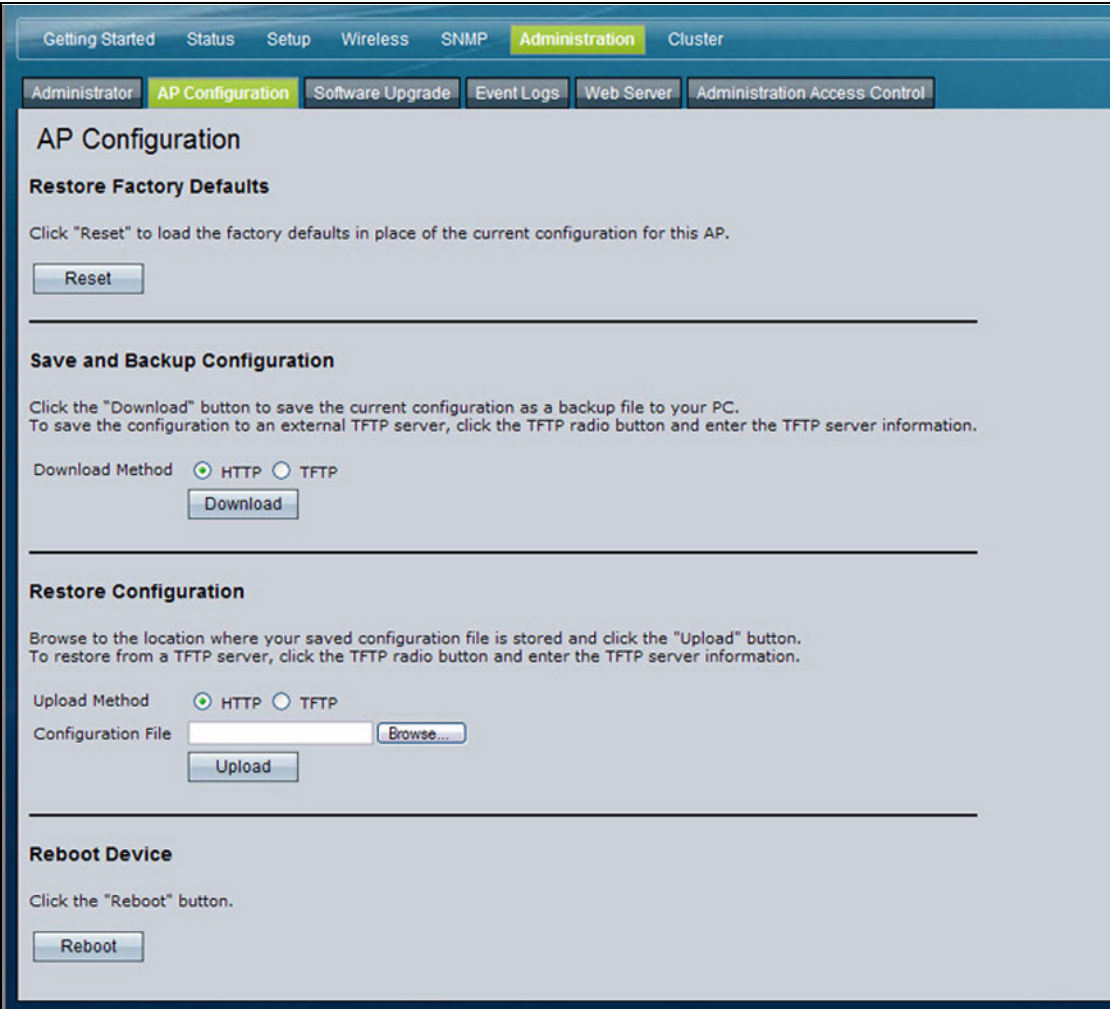


REMARQUE Après avoir configuré les paramètres de la page Administrator, cliquez sur **Apply** pour appliquer et enregistrer les modifications. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans cette situation, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Configuration du point d'accès

Le fichier de configuration du point d'accès est au format XML. Il contient toutes les informations relatives aux paramètres du point d'accès. Vous pouvez télécharger le fichier de configuration sur un poste de gestion pour en modifier manuellement le contenu ou enregistrer une copie de sauvegarde. Lorsque vous téléchargez un fichier de configuration dans le point d'accès, les informations relatives à la configuration correspondantes lui sont appliquées. Cliquez sur l'onglet **AP Configuration** pour accéder à la page de gestion de la configuration, représentée à la **Figure 27**.

Figure 27 Page de gestion de la configuration



The screenshot shows a web interface for AP Configuration. At the top, there is a navigation bar with tabs: Getting Started, Status, Setup, Wireless, SNMP, Administration (highlighted), and Cluster. Below this, there is a sub-navigation bar with tabs: Administrator, AP Configuration (highlighted), Software Upgrade, Event Logs, Web Server, and Administration Access Control.

The main content area is titled "AP Configuration" and contains four sections:

- Restore Factory Defaults:** A section with a "Reset" button. The text below the button says: "Click 'Reset' to load the factory defaults in place of the current configuration for this AP."
- Save and Backup Configuration:** A section with a "Download" button. The text above the button says: "Click the 'Download' button to save the current configuration as a backup file to your PC. To save the configuration to an external TFTP server, click the TFTP radio button and enter the TFTP server information." Below the text, there are radio buttons for "Download Method": HTTP and TFTP.
- Restore Configuration:** A section with an "Upload" button. The text above the button says: "Browse to the location where your saved configuration file is stored and click the 'Upload' button. To restore from a TFTP server, click the TFTP radio button and enter the TFTP server information." Below the text, there are radio buttons for "Upload Method": HTTP and TFTP. There is also a text input field for "Configuration File" with a "Browse..." button next to it.
- Reboot Device:** A section with a "Reboot" button. The text above the button says: "Click the 'Reboot' button."

Réinitialisation de la configuration par défaut du point d'accès

Si le point d'accès rencontre des problèmes et que vous avez essayé toutes les autres mesures de dépannage, cliquez sur **Reset**. Cette action rétablit les valeurs par défaut définies en usine et supprime tous les paramètres, notamment le mot de passe ou les paramètres de communication sans fil. Vous pouvez également utiliser le bouton **Reset** pour rétablir la configuration par défaut du système.

Enregistrement de la configuration actuelle dans un fichier de sauvegarde

Vous pouvez utiliser les protocoles HTTP ou TFTP pour transférer des fichiers vers le point d'accès ou à partir de celui-ci. Les fichiers de configuration sont téléchargés sur le poste de gestion au format XML et peuvent être modifiés manuellement. Vous pouvez ensuite télécharger un fichier de configuration modifié vers le point d'accès afin d'y appliquer ces paramètres de configuration.

Enregistrement de la configuration actuelle via TFTP

Pour enregistrer une copie des paramètres actuels du point d'accès dans un fichier de configuration de sauvegarde via TFTP, procédez comme suit :

- ÉTAPE 1** Si elle n'est pas déjà sélectionnée, cliquez sur la case d'option permettant d'utiliser TFTP pour télécharger le fichier.
- ÉTAPE 2** Entrez le nom du fichier de sauvegarde dans le champ **Configuration File**, en incluant l'extension .xml et le chemin d'accès du répertoire dans lequel vous souhaitez l'enregistrer.
- ÉTAPE 3** Saisissez l'adresse IP du serveur TFTP.

Save and Backup Configuration

Click the "Download" button to save the current configuration as a backup file to your PC. To save the configuration to an external TFTP server, click the TFTP radio button and enter the TFTP server information.

Download Method HTTP TFTP

Configuration File

TFTP Server IP

- ÉTAPE 4** Cliquez sur **Download** pour enregistrer le fichier.

Enregistrement de la configuration actuelle via HTTP

Pour enregistrer une copie des paramètres actuels du point d'accès dans un fichier de configuration de sauvegarde via HTTP, procédez comme suit :

-
- ÉTAPE 1** Cliquez sur la case d'option HTTP.
 - ÉTAPE 2** Cliquez sur le bouton **Download**. La boîte de dialogue de téléchargement ou d'ouverture du fichier apparaît.
 - ÉTAPE 3** Dans cette boîte de dialogue, choisissez l'option **Save**. Un gestionnaire de fichiers s'affiche.
 - ÉTAPE 4** Naviguez jusqu'au répertoire dans lequel vous souhaitez enregistrer le fichier, puis cliquez sur **OK**.

Vous pouvez conserver le nom par défaut du fichier (config.xml) ou le renommer, mais veillez à bien l'enregistrer avec l'extension .xml.

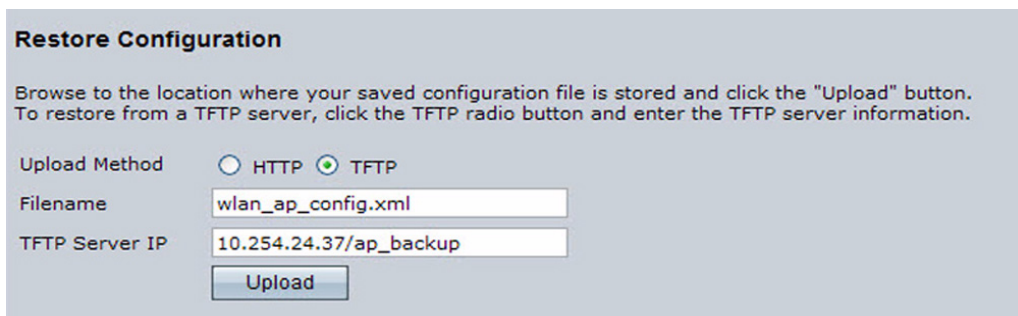
Restauration de la configuration à partir d'un fichier enregistré

Vous pouvez utiliser les protocoles HTTP ou TFTP pour transférer des fichiers vers le point d'accès ou à partir de celui-ci. Les fichiers de configuration sont téléchargés sur le poste de gestion au format XML et peuvent être modifiés manuellement. Vous pouvez ensuite télécharger un fichier de configuration modifié vers le point d'accès afin d'y appliquer ces paramètres de configuration.

Restauration de la configuration actuelle via TFTP

Pour restaurer les paramètres de configuration précédemment enregistrés du point d'accès via TFTP, procédez comme suit :

-
- ÉTAPE 1** Si elle n'est pas déjà sélectionnée, cliquez sur la case d'option **TFTP**.
 - ÉTAPE 2** Saisissez le nom du fichier de sauvegarde dans le champ **Filename**, en incluant l'extension de fichier .xml et le chemin d'accès du répertoire qui contient le fichier de configuration à télécharger.
 - ÉTAPE 3** Saisissez l'adresse IP du serveur TFTP.



Restore Configuration

Browse to the location where your saved configuration file is stored and click the "Upload" button. To restore from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Upload Method HTTP TFTP

Filename

TFTP Server IP

ÉTAPE 4 Cliquez sur le bouton **Restore**.

Le point d'accès redémarre. Une boîte de dialogue de confirmation du redémarrage s'affiche, suivie d'un message d'état de redémarrage. Attendez la fin du processus de redémarrage. Celui-ci peut durer plusieurs minutes.

L'Utilitaire de configuration n'est pas accessible tant que le point d'accès n'a pas redémarré.

Restauration de la configuration actuelle via HTTP

Pour enregistrer une copie des paramètres actuels du point d'accès dans un fichier de configuration de sauvegarde via HTTP, procédez comme suit :

ÉTAPE 1 Désactivez l'option **Use TFTP to upload the file**.

Lorsque vous désélectionnez cette case d'option, le champ Server IP est désactivé.

ÉTAPE 2 Entrez le nom du fichier à restaurer.

ÉTAPE 3 Cliquez sur **Restore**.

La boîte de dialogue **File Upload** ou **Choose File** s'affiche.

ÉTAPE 4 Naviguez jusqu'au répertoire qui contient le fichier, puis sélectionnez le fichier à télécharger et cliquez sur **Open**.



REMARQUE Seuls les fichiers enregistrés comme fichiers de configuration de sauvegarde au format .xml peuvent être utilisés avec la fonction de restauration ; par exemple, ap_config.xml.

ÉTAPE 5 Cliquez sur **Restore**.

Le point d'accès redémarre. Une boîte de dialogue de confirmation du redémarrage s'affiche, suivie d'un message d'état de redémarrage. Attendez la fin du processus de redémarrage. Celui-ci peut durer plusieurs minutes.

L'Utilitaire de configuration n'est pas accessible tant que le point d'accès n'a pas redémarré.

Redémarrage du point d'accès

À des fins de maintenance ou de dépannage, vous pouvez être amené à redémarrer le point d'accès. Pour redémarrer le point d'accès, cliquez sur le bouton **Reboot**, dans la page **Configuration**.

Mise à niveau du logiciel

Au fur et à mesure de la mise à disposition de nouvelles versions du logiciel du point d'accès, vous pouvez mettre à niveau vos périphériques pour bénéficier de nouvelles fonctionnalités et d'améliorations. Le point d'accès utilise un client TFTP pour effectuer les mises à niveau du logiciel. Vous pouvez également procéder aux mises à niveau via HTTP.



REMARQUE Lorsque vous mettez le logiciel à niveau, le point d'accès conserve les informations sur la configuration existante.



REMARQUE Par défaut, le point d'accès utilise le protocole HTTP plutôt que TFTP pour les mises à niveau.

Mise à niveau du logiciel via TFTP

Pour mettre à niveau le logiciel du point d'accès via TFTP, procédez comme suit :

ÉTAPE 1 Cliquez sur l'onglet **Software Upgrade** dans la section **Administration**.

Des informations sur la version actuelle s'affichent, ainsi qu'une option permettant de télécharger une nouvelle image logicielle.

ÉTAPE 2 Assurez-vous que la case d'option **Upload Method TFTP** est sélectionnée.

ÉTAPE 3 Entrez le nom du fichier image dans le champ **New Software Image**, en incluant le chemin d'accès du répertoire contenant l'image à télécharger.

Par exemple, pour télécharger l'image *ap_upgrade.tar* située dans le répertoire */share/builds/ap*, entrez */share/builds/ap/ap_upgrade.tar* dans le champ **New Software Image**.

Le fichier de mise à niveau du logiciel fourni doit être au format *tar*. N'essayez pas d'utiliser des fichiers *bin* ou d'autres formats pour la mise à niveau ; ils ne fonctionneront pas.

ÉTAPE 4 Entrez l'adresse IP du serveur TFTP dans le champ **Server IP**.

The screenshot shows the 'Software Upgrade' configuration page in the Cisco AP541N AP web interface. The page is titled 'Software Upgrade' and displays the following information:

- Model: Cisco AP541N AP
- Software Version: 6-21.1(0)
- Upload Method: HTTP TFTP
- Image Filename:
- TFTP Server IP:
- Upgrade button:

Please note: Uploading the new software may take several minutes. Please do not refresh the page or navigate to another page while uploading the new software, or the software upload will be aborted. When the process is complete the access point will restart and resume normal operation.

ÉTAPE 5 Cliquez sur **Upgrade**.

Lorsque vous cliquez sur **Upgrade**, une fenêtre contextuelle de confirmation s'affiche pour décrire le processus de mise à niveau.

ÉTAPE 6 Cliquez sur **OK** pour confirmer la mise à niveau et lancer le processus.

REMARQUE Le processus de mise à niveau logicielle commence une fois que vous avez cliqué sur **Upgrade** et sur **OK** dans la fenêtre contextuelle.

La mise à niveau peut prendre plusieurs minutes, pendant lesquelles le point d'accès n'est pas accessible. Ne mettez pas le point d'accès hors tension pendant que la mise à niveau est en cours. Une fois la mise à niveau terminée, le point d'accès redémarre. Le point d'accès se remet à fonctionner normalement, avec les mêmes paramètres de configuration qu'avant la mise à niveau.

ÉTAPE 7 Pour vous assurer que la mise à niveau s'est effectuée correctement, vérifiez le numéro de version figurant dans l'onglet **Software Upgrade** (ainsi que dans la section **Summary**). Si la mise à niveau a réussi, le nom ou le numéro de la version à jour est indiqué.

Mise à niveau du logiciel via HTTP

Pour mettre à niveau le logiciel du point d'accès via HTTP, procédez comme suit :

ÉTAPE 1 Désactivez l'option **Upload Method TFTP**.

Lorsque vous désélectionnez cette case d'option, le champ Server IP est désactivé.

ÉTAPE 2 Si vous connaissez le chemin d'accès du fichier **de la nouvelle image logicielle**, entrez-le dans le champ **New Software Image**. Sinon, cliquez sur le bouton **Browse** afin de sélectionner le fichier.

Le fichier de mise à niveau du logiciel fourni doit être au format *tar*. N'essayez pas d'utiliser des fichiers *bin* ou d'autres formats pour la mise à niveau ; ils ne fonctionneront pas.

ÉTAPE 3 Cliquez sur **Upgrade** pour appliquer la nouvelle image logicielle.

Lorsque vous cliquez sur **Upgrade**, une fenêtre contextuelle de confirmation s'affiche pour décrire le processus de mise à niveau.

ÉTAPE 4 Cliquez sur **OK** pour confirmer la mise à niveau et lancer le processus.



REMARQUE Le processus de mise à niveau logicielle commence une fois que vous avez cliqué sur **Upgrade** et sur **OK** dans la fenêtre contextuelle.

La mise à niveau peut prendre plusieurs minutes, pendant lesquelles le point d'accès n'est pas accessible. Ne mettez pas le point d'accès hors tension pendant que la mise à niveau est en cours. Une fois la mise à niveau terminée, le point d'accès redémarre. Le point d'accès se remet à fonctionner normalement, avec les mêmes paramètres de configuration qu'avant la mise à niveau.

ÉTAPE 5 Pour vous assurer que la mise à niveau s'est effectuée correctement, vérifiez le numéro de version figurant dans l'onglet **Software Upgrade** (il apparaît également dans la section **Summary**). Si la mise à niveau a réussi, le nom ou le numéro de la version à jour est indiqué.

Journaux d'événements

La page **Events** présente les événements système en temps réel du point d'accès, par exemple l'association de clients sans fil au point d'accès et leur authentification.

Vous pouvez afficher les événements les plus récents générés par le point d'accès et configurer des paramètres de consignation. Vous pouvez activer et configurer une consignation persistante afin d'écrire les journaux d'événements système en mémoire non volatile, de telle sorte que les événements ne soient pas supprimés lorsque le système redémarre. Vous pouvez également autoriser un hôte de relais de consignation distant à collecter les événements système et les erreurs dans un journal de noyau.

Pour afficher les événements système, cliquez sur l'onglet **Events**.

Figure 28 Journaux d'événements

Options

Persistence Enabled Disabled

Severity

Depth

Click "Apply" to save the new settings.

Apply

Relay Options

Relay Log Enabled Disabled

Relay Host

Relay Port

Click "Apply" to save the new settings.

Apply

Events

Click "Refresh" button to refresh the page.

Refresh

Time Settings (NTP)	Type	Service	Description
Jan 1 00:00:08	info	syslog	managed_ap.c:405:map_init_sub_components - Created the MAP Switch Comm Control Block
Jan 1 00:00:07	warn	mini_httpd-ssl [359]	started as root without requesting chroot(), warning only
Jan 1 00:00:06	notice	mini_httpd-ssl [360]	mini_httpd/1.19 19dec2003 starting on AP541N-A-K9, port 443
Jan 1 00:00:06	warn	mini_httpd-ssl [360]	started as root without requesting chroot(), warning only

Click "Clear All" to erase all events.

Clear All

Cliquez sur **Refresh** pour actualiser la page.



REMARQUE Le point d'accès récupère les informations de date et d'heure au moyen du protocole NTP (Network Time Protocol). Ces données sont renvoyées au format UTC, également nommé GMT (Greenwich Mean Time, heure de Greenwich). Convertissez ensuite l'heure renvoyée dans votre heure locale. Pour obtenir des informations sur le protocole NTP, reportez-vous à la section **Activation du protocole Network Time, page 53**.

Configuration des options de consignation persistante

Si le système effectue un redémarrage intempestif, les messages du journal peuvent vous aider à identifier l'origine du problème. Toutefois, si la consignation persistante n'a pas été activée, ces messages sont effacés au redémarrage du système.



ATTENTION L'activation de la consignation persistante peut épuiser la mémoire flash (non volatile) et nuire aux performances du réseau. Activez uniquement la consignation persistante dans le cadre d'un débogage. Veillez à bien désactiver la consignation persistante une fois le problème résolu.

Pour configurer la consignation persistante dans la page **Event Logs**, définissez la persistance, la gravité et les options de profondeur décrites dans le **Tableau 31**, puis cliquez sur **Apply**.

Figure 29 Options de consignation persistante

The screenshot shows a dialog box titled "Options" with the following settings:

- Persistence:** Radio buttons for "Enabled" and "Disabled". The "Disabled" option is selected.
- Severity:** A dropdown menu showing the value "6".
- Depth:** A text input field containing the value "128".

Below the settings, there is a text instruction: "Click 'Apply' to save the new settings." and an "Apply" button.

Tableau 31 Options de consignation

Champ	Description
Persistence	Choisissez Enabled pour enregistrer les journaux système en mémoire non volatile, de telle sorte que les journaux ne soient pas effacés au redémarrage du point d'accès. Choisissez Disabled pour enregistrer les journaux système en mémoire volatile. Les journaux en mémoire volatile sont supprimés lorsque le système redémarre.
Gravité	Indiquez le niveau de gravité des messages du journal à écrire en mémoire non volatile. Par exemple, si vous indiquez 2, les journaux critique, d'alerte et d'urgence sont écrits en mémoire non volatile. Les messages d'erreur dont le niveau de gravité est compris entre 3 et 7 sont écrits en mémoire volatile. 0 : urgence 1 : alerte 2 : critique 3 : erreur 4 : avertissement 5 : notification 6 : infos 7 : débogage
Profondeur	Vous pouvez stocker jusqu'à 128 messages en mémoire non volatile. Une fois que la valeur configurée dans ce champ a été atteinte, l'événement le plus ancien du journal est remplacé par le plus récent.



REMARQUE Pour appliquer les modifications, cliquez sur **Apply**. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans cette situation, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Configuration de l'hôte de relais de consignation pour les messages de noyau

Le journal de noyau est une liste exhaustive d'événements système (affichés dans le journal système) et de messages du noyau relatifs à des conditions d'erreur, telles que la perte de trames.

Il n'est pas possible de voir directement les messages du journal de noyau dans l'*Utilitaire de configuration du point d'accès* d'un point d'accès. En effet, vous devez tout d'abord configurer un serveur distant exécutant un processus syslog et servant d'hôte de relais de consignation du journal système sur votre réseau. Vous pouvez ensuite configurer le point d'accès pour qu'il envoie les messages syslog au serveur distant.

Les options suivantes sont proposées pour la collecte des messages syslog du point d'accès sur un serveur distant :

- Agrégation des messages provenant de plusieurs points d'accès
- Stockage d'un historique des messages plus long que sur un seul point d'accès
- Déclenchement d'opérations de gestion et d'alertes par script

Pour utiliser le relais du journal de noyau, vous devez configurer au moins un serveur distant pour lui permettre de recevoir les messages syslog. La procédure de configuration d'un hôte de consignation distant dépend du type de système utilisé par cet hôte distant.



REMARQUE Par défaut, le processus syslog utilise le port 514. Il est recommandé de conserver ce port par défaut. Si vous choisissez toutefois de reconfigurer le port de consignation, assurez-vous que le numéro de port que vous attribuez au syslog n'est pas utilisé par un autre processus.

Activation ou désactivation de l'hôte de relais de consignation dans la page Events

Pour activer et configurer le relais de la consignation dans la page **Event Logs**, configurez les options décrites dans le tableau **Hôte de relais de consignation**, [page 143](#), puis cliquez sur **Apply**.

Figure 30 Hôte de relais de consignation

Tableau 32 Hôte de relais de consignation

Champ	Description
Relay Log	Permet d'activer ou de désactiver l'hôte de relais de consignation. Si vous sélectionnez la case d'option Relay Log , l'hôte de relais de consignation est activé et les champs Relay Host et Relay Port deviennent accessibles.
Relay Host	Indiquez l'adresse IP ou le nom DNS du serveur de consignation distant.
Relay Port	Indiquez le numéro de port du processus syslog sur l'hôte de relais. Le port par défaut est le port 514.



REMARQUE Pour appliquer les modifications, cliquez sur **Apply**. La modification de certains paramètres peut entraîner l'arrêt et le redémarrage des processus système du point d'accès. Dans cette situation, les clients sans fil perdent temporairement leur connexion. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Si vous avez activé l'hôte de relais, cliquez sur **Apply** pour activer la consignation à distance. Le point d'accès envoie les messages de noyau en temps réel pour les afficher sur le moniteur du serveur de consignation, dans un fichier journal de noyau spécifié ou vers un autre emplacement de stockage, en fonction de la configuration de l'hôte de relais de consignation.

Si vous avez désactivé l'hôte de relais, cliquez sur **Apply** pour désactiver la consignation à distance.

Configuration des paramètres du serveur Web

La gestion du point d'accès peut s'effectuer par l'intermédiaire de sessions HTTP ou HTTPS (HTTP sécurisé). Par défaut HTTP et HTTPS sont tous deux activés. Chaque type d'accès peut être désactivé.

Pour configurer les paramètres du serveur Web, cliquez sur l'onglet Web Server.

Figure 31 Configuration des paramètres du serveur Web

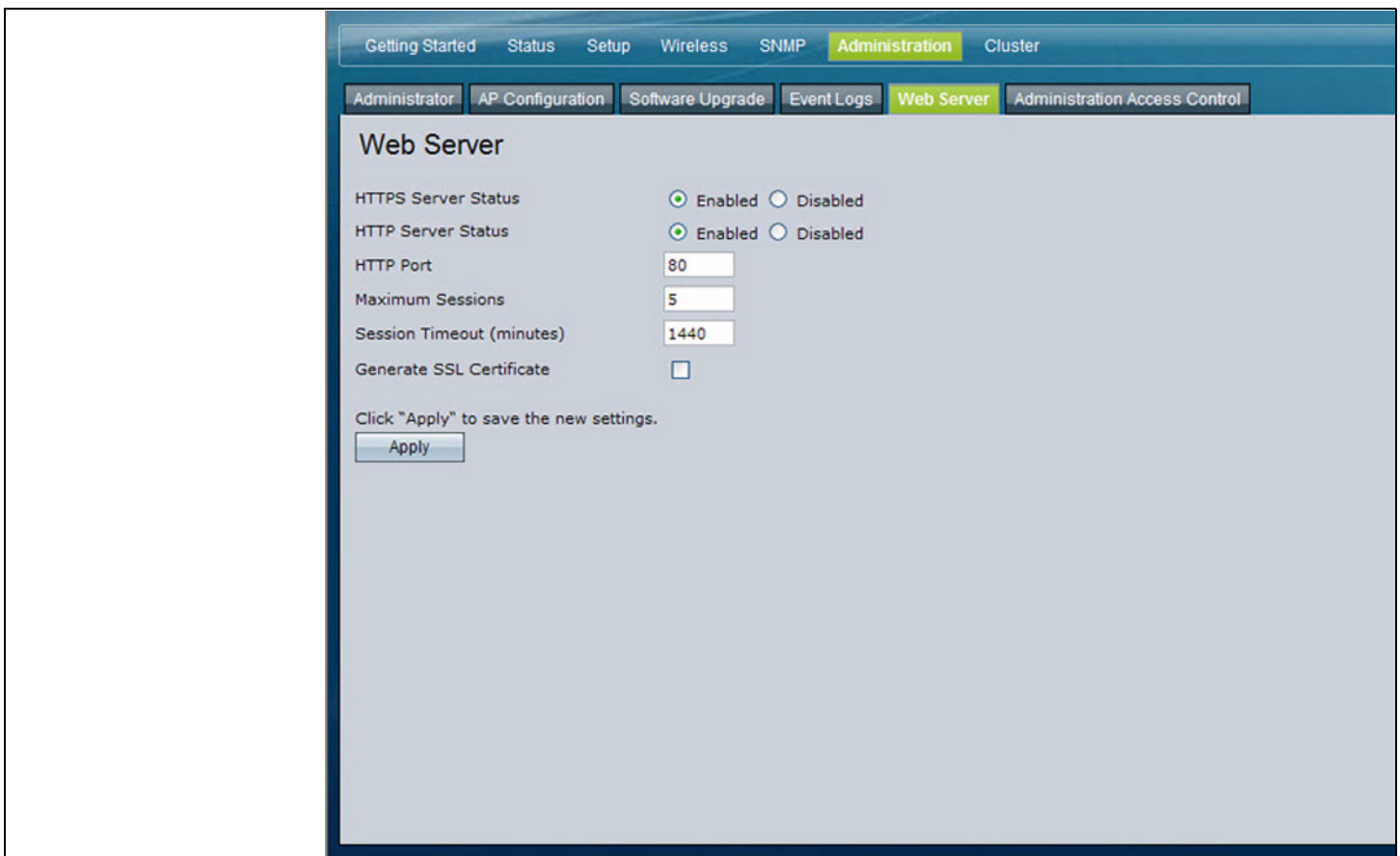


Tableau 33 Paramètres du serveur Web

Champ	Description
HTTPS Server Status	Permet d' activer ou de désactiver l'accès via un serveur HTTP sécurisé (HTTPS). Ce paramètre est indépendant de l'état du serveur HTTP.
HTTP Server Status	Permet d' activer ou de désactiver l'accès via HTTP. Ce paramètre est indépendant de l'état du serveur HTTPS.
HTTP Port	Permet d'indiquer le numéro de port utilisé pour le trafic HTTP. (La valeur par défaut est 80.)
Maximum Sessions	Permet d'indiquer le nombre maximal de connexions HTTP et HTTPS autorisées simultanément vers le serveur Web du point d'accès. La plage de connexions est comprise entre 1 et 10. Le nombre que vous saisissez a une incidence sur le nombre de connexions à l'utilitaire de configuration du point d'accès. En revanche, il n'a aucun impact sur le nombre de clients sans fil autorisés à s'associer avec le point d'accès.
Session Timeout	Entrez la durée, en minutes, pendant laquelle une session HTTP ou HTTPS peut demeurer inactive avant de prendre fin. La plage valide est comprise entre 1 et 1 440 minutes (24 heures).
Generate SSL Certificate	Sélectionnez cette option pour générer un nouveau certificat SSL pour le serveur Web sécurisé. Cette opération doit être effectuée après que le point d'accès a obtenu une adresse IP, afin d'assurer que le nom commun du certificat correspond à l'adresse IP du point d'accès. La génération d'un certificat SSL entraîne le redémarrage du serveur Web sécurisé. La connexion sécurisée ne fonctionne pas tant que le nouveau certificat n'est pas accepté par le navigateur.



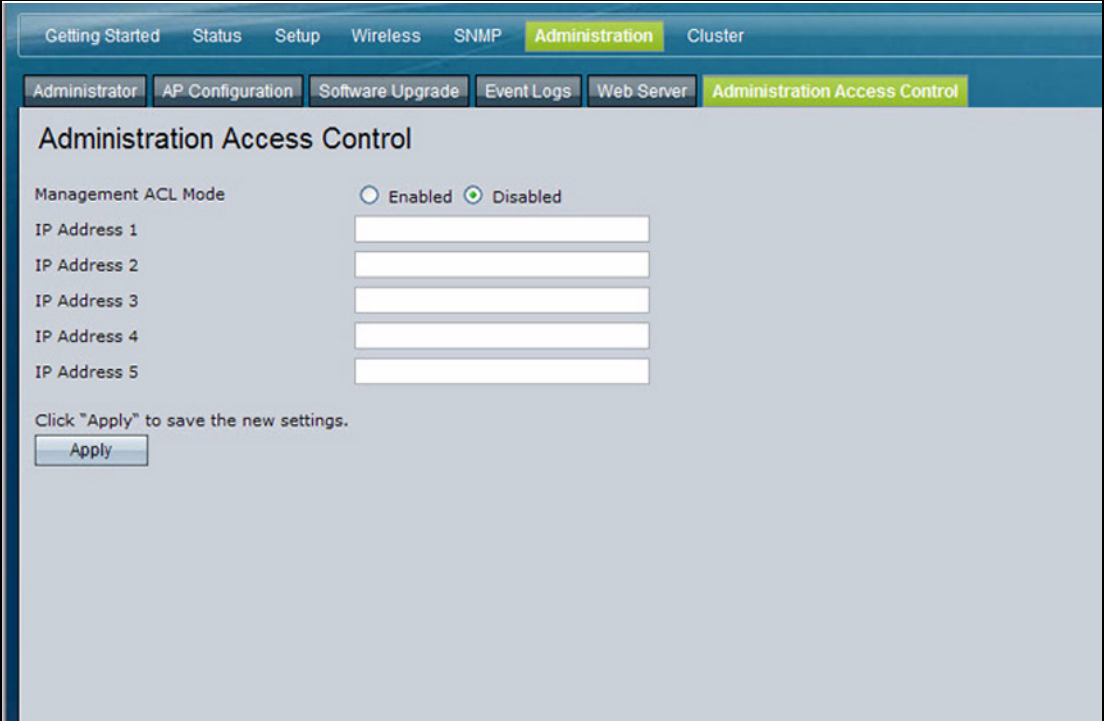
REMARQUE Cliquez sur **Apply** pour appliquer les modifications et enregistrer les paramètres. Si vous désactivez le protocole utilisé pour accéder à l'interface de gestion du point d'accès, la connexion en cours prend fin et vous ne pouvez pas accéder au point d'accès par l'intermédiaire de ce protocole tant qu'il n'a pas été réactivé.

Création d'une liste de contrôle d'accès d'administration

Vous pouvez créer une liste de contrôle d'accès (ACL) pouvant contenir jusqu'à cinq hôtes IPv4 autorisés à accéder à l'interface de gestion du point d'accès via le Web, Telnet et SNMP. Si cette fonctionnalité est désactivée, n'importe quel utilisateur peut accéder à l'interface de gestion à partir de n'importe quel client du réseau en entrant le nom d'utilisateur et le mot de passe corrects du point d'accès.

Pour créer une liste de contrôle d'accès, cliquez sur l'onglet Administration Access Control.

Figure 32 Liste de contrôle d'accès de gestion



The screenshot shows a web interface for configuring the Administration Access Control. The top navigation bar includes tabs for Getting Started, Status, Setup, Wireless, SNMP, Administration (highlighted), and Cluster. Below this, a secondary navigation bar contains tabs for Administrator, AP Configuration, Software Upgrade, Event Logs, Web Server, and Administration Access Control (highlighted). The main content area is titled "Administration Access Control" and features a "Management ACL Mode" section with radio buttons for "Enabled" and "Disabled" (the "Disabled" option is selected). Below this are five input fields labeled "IP Address 1" through "IP Address 5". At the bottom of the form, there is a text instruction "Click 'Apply' to save the new settings." and an "Apply" button.



REMARQUE Une fois que vous avez configuré les paramètres, cliquez sur **Apply** pour appliquer et enregistrer les modifications.

Tableau 34 Liste de contrôle d'accès de gestion

Champ	Description
Management ACL Mode	Permet d' activer ou de désactiver la fonctionnalité ACL. Configurez au moins une adresse IPv4 avant d'activer le mode ACL de gestion. Si vous sélectionnez Enabled , seules les adresses IP que vous spécifiez disposeront d'un accès Web, Telnet, SSH et SNMP à l'interface de gestion.
IP Address (1–5)	Entrez jusqu'à cinq adresses IPv4 autorisées à accéder à la gestion du point d'accès. Utilisez le format décimal à points (par exemple, <i>192.168.10.100</i>).

Mise en grappe de plusieurs points d'accès

L'unité Cisco AP 541N prend en charge la mise en grappe des points d'accès. Une grappe fournit un point d'administration unique et permet de visualiser, déployer, configurer et sécuriser le réseau sans fil comme s'il s'agissait d'une entité unique et non de périphériques sans fil séparés.

Gestion des points d'accès de la grappe

La grappe de points d'accès constitue un groupe de points d'accès dynamiques et reconnaissant la configuration, présents sur un même sous-réseau. Chaque grappe peut comporter jusqu'à dix membres. Avec la mise en grappe, vous bénéficiez d'un point d'administration unique et êtes ainsi en mesure de gérer le déploiement de vos points d'accès sous la forme d'un réseau sans fil unique plutôt que d'un ensemble de périphériques distincts. Un sous-réseau peut comporter plusieurs grappes. Les grappes peuvent partager diverses informations relatives à la configuration, telles que les paramètres VAP et de file d'attente QoS.

Une grappe peut être formée entre deux points d'accès si les conditions suivantes sont réunies :

- Les points d'accès utilisent le même mode radio (par exemple, les deux radios utilisent 802.11g).
- Les points d'accès sont connectés au même segment ponté.
- Les points d'accès joignant la grappe ont le même nom de grappe.
- Le mode grappe est activé sur les deux points d'accès.



REMARQUE Pour que deux points d'accès coexistent dans une même grappe, il n'est pas nécessaire qu'ils disposent du même nombre de modules radio, mais les radios doivent prendre en charge les mêmes fonctionnalités.

Mise en grappe de points d'accès à un ou deux modules radio

Les grappes peuvent contenir une combinaison de points d'accès avec deux modules radio et de points d'accès avec un module radio unique. Lorsque la configuration d'un point d'accès avec module radio unique de la grappe est modifiée, le point d'accès propage cette modification au premier module radio de tous les membres de la grappe. La configuration du deuxième module radio des éventuels points d'accès à deux radios de la grappe n'est pas modifiée.

Si une grappe ne contient que des points d'accès avec module radio unique et qu'un point d'accès à deux radios rejoint la grappe, seul le module radio 1 de ce dernier point d'accès sera pris en compte dans la configuration de la grappe. Le module radio 2 du point d'accès conserve l'état dans lequel il était avant son adjonction à la grappe. En revanche, si la grappe comporte déjà au moins un point d'accès à deux modules radio, la deuxième radio du point d'accès qui rejoint la grappe est configurée selon les paramètres de la grappe.

Affichage et configuration des membres d'une grappe

L'onglet **Access Points** permet de démarrer ou d'arrêter la mise en grappe sur un point d'accès, d'afficher les membres de la grappe et de configurer l'emplacement et le nom d'un membre. Dans la page **Access Points**, vous pouvez également cliquer sur l'adresse IP de chaque membre de la grappe, afin d'accéder aux paramètres de configuration et aux données de chacun de ces points d'accès.

Pour afficher des informations sur les membres d'une grappe et configurer l'emplacement et la grappe d'un membre individuel, cliquez sur l'onglet **Access Points**.

Figure 33 Informations sur la grappe et configuration des membres



Si la mise en grappe est désactivée sur le point d'accès, le bouton **Enable Clustering** est alors visible. Si la mise en grappe est activée, c'est le bouton **Disable Clustering** qui est visible. Vous pouvez entrer des informations, que la mise en grappe soit activée ou désactivée.

Le **Tableau 35** décrit les informations de configuration et d'état disponibles sur la page **Access Points** lorsque la mise en grappe est activée.

Tableau 35 Points d'accès de la grappe

Champ	Description
État	Si le champ d'état est visible, la mise en grappe est activée sur le point d'accès. Si la mise en grappe n'est pas activée, le point d'accès fonctionne en mode autonome et aucune des informations figurant dans ce tableau n'apparaît. Pour désactiver la mise en grappe du point d'accès, cliquez sur Disable Clustering .
Location	Description de l'emplacement physique du point d'accès.

Tableau 35 Points d'accès de la grappe (suite)

Champ	Description
MAC Address	<p>Adresse MAC (Media Access Control) du point d'accès.</p> <p>L'adresse présentée ici est l'adresse MAC du pont (br0). Il s'agit de l'adresse externe sous laquelle les autres réseaux reconnaissent le point d'accès.</p>
IP Address	<p>Adresse IP du point d'accès.</p> <p>Chaque adresse IP constitue un lien vers les pages Web d'administration du point d'accès. Vous pouvez utiliser ces liens pour naviguer jusqu'aux pages Web d'administration d'un point d'accès spécifique. Ceci s'avère utile pour visualiser les données d'un point d'accès particulier, afin d'assurer qu'un membre de la grappe récupère bien les modifications de configuration de manière à configurer les paramètres avancés d'un point d'accès donné ou faire passer un point d'accès autonome en mode grappe.</p>

Le **Tableau 36** décrit les informations de grappe à configurer sur un membre.

Tableau 36 Options de mise en grappe

Champ	Description
Location	Entrez la description de l'emplacement physique du point d'accès. Cet emplacement peut comporter 64 caractères au maximum. Tous les caractères alphanumériques sont valides, à l'exception des guillemets ("). Les espaces nuls ou vides ne sont pas autorisés.

Tableau 36 Options de mise en grappe (suite)

Champ	Description
Cluster Name	<p>Entrez le nom de la grappe que le point d'accès doit rejoindre. Ce nom peut comporter 64 caractères au maximum. Tous les caractères alphanumériques sont valides, à l'exception des guillemets ("). Les espaces nuls ou vides ne sont pas autorisés.</p> <p>Le nom de la grappe n'est pas envoyé aux autres points d'accès qu'elle contient. Vous devez configurer le même nom de grappe sur chaque point d'accès membre. Chaque grappe configurée sur le réseau doit porter un nom unique.</p>

Suppression d'un point d'accès de la grappe

Pour supprimer un point d'accès de la grappe, procédez comme suit :

- ÉTAPE 1** Accédez aux pages d'**administration** du point d'accès mis en grappe.
- ÉTAPE 2** Cliquez sur l'onglet **Cluster > Access Points** des pages d'administration.
- ÉTAPE 3** Cliquez sur **Disable Clustering**.

La modification apparaît sous l'option **Status** du point d'accès, qui indique *standalone* (et non plus *cluster*).

Ajout d'un point d'accès à une grappe

Pour ajouter à une grappe un point d'accès actuellement en mode autonome, procédez comme suit :

- ÉTAPE 1** Accédez aux pages d'**administration** du point d'accès autonome.
- ÉTAPE 2** Cliquez sur l'onglet **Cluster > Access Points** des pages d'administration du point d'accès autonome.

L'onglet **Access Points** d'un point d'accès autonome indique que le mode autonome est en vigueur et contient un bouton permettant d'ajouter le point d'accès à une grappe (un groupe).

ÉTAPE 3 Cliquez sur **Enable Clustering**.

Le point d'accès est maintenant membre de la grappe. Son état (mode), qui apparaît dans l'onglet **Cluster > Access Points**, est défini sur **Cluster** au lieu de **Not Clustered**.

Navigation jusqu'aux informations de configuration d'un point d'accès spécifique

Tous les points d'accès d'une grappe présentent la même configuration. Cela signifie que vous pouvez vous connecter à n'importe lequel des points d'accès pour administrer la grappe.

Toutefois, il peut parfois s'avérer nécessaire de visualiser ou de gérer les informations relatives à un point d'accès en particulier. Par exemple, vous pouvez consulter certaines informations d'état, telles que les associations avec les clients ou les événements survenus sur un point d'accès. Dans ce cas, vous pouvez naviguer jusqu'à la page **Administration** de points d'accès individuels en cliquant sur les liens d'adresses IP de l'onglet **Access Points**.

Tous les points d'accès mis en grappe sont présentés dans la page **Cluster > Access Points**. Pour naviguer jusqu'à des points d'accès mis en grappe, vous pouvez simplement cliquer sur l'adresse IP d'un membre spécifique de la grappe figurant dans la liste.

Navigation jusqu'à un point d'accès à l'aide de son adresse IP dans une URL

Vous pouvez également établir un lien vers les pages **Administration** d'un point d'accès spécifique en entrant directement l'adresse IP correspondante sous la forme d'une URL dans la barre d'adresse d'un navigateur Web, au format suivant :

AdresseIPduPointd'Accès

où *AdresseIPduPointd'Accès* représente l'adresse du point d'accès que vous souhaitez surveiller ou configurer.

Gestion des sessions de grappe

La page **Sessions** présente des informations relatives aux stations de client associées aux points d'accès de la grappe. Chaque client est identifié par son adresse MAC et le point d'accès (emplacement) auquel il est connecté.



REMARQUE Lorsque la page **Cluster - Sessions** apparaît, elle renvoie un maximum de 20 clients par radio. Pour visualiser tous les clients associés, accédez à la page **Client Associations** du point d'accès.

Pour afficher une statistique en particulier des sessions client, sélectionnez un élément dans la liste déroulante **Display**, puis cliquez sur **Go**. Vous pouvez consulter des informations sur la durée d'inactivité, le débit de données, la puissance du signal, etc. Toutes ces informations sont décrites en détail dans le **Tableau 37**.

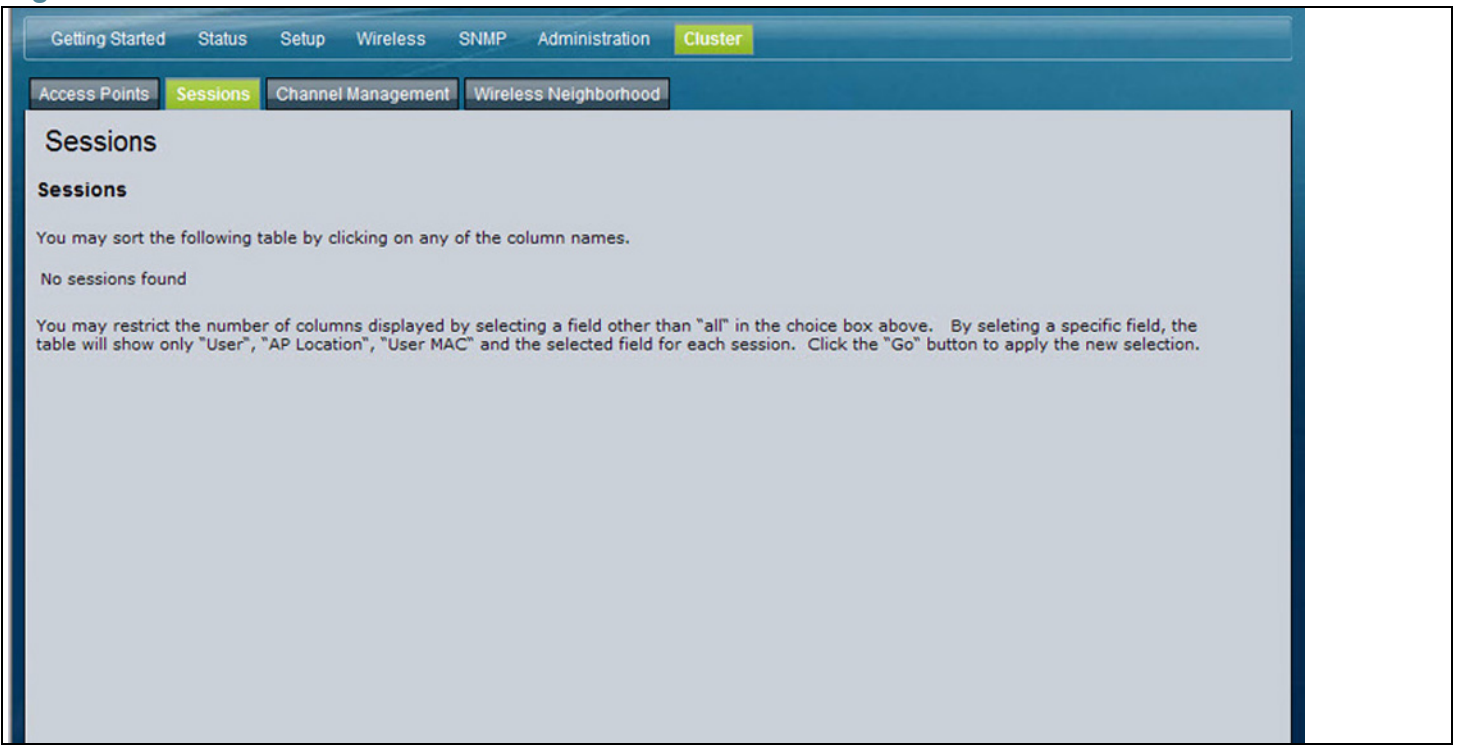
Dans le présent contexte, une session représente la durée pendant laquelle l'utilisateur d'un périphérique client (station), possédant une adresse MAC unique, reste connecté au réseau sans fil. La session commence quand le client se connecte au réseau et se termine lorsqu'il se déconnecte délibérément ou que la connexion est interrompue pour un autre motif.



REMARQUE Une session n'est pas une association, laquelle décrit la connexion d'un client à un point d'accès en particulier. La connexion réseau d'un client peut passer d'un point d'accès de la grappe à un autre dans le cadre d'une même session. Une station de client peut se déplacer d'un point d'accès à un autre tout en conservant la session.

Pour gérer les sessions associées à la grappe, cliquez sur l'onglet **Sessions**.

Figure 34 Gestion de la session



Les informations relatives à la session sont décrites dans le [Tableau 37](#).

Tableau 37 Gestion de la session

Champ	Description
AP Location	Indique l'emplacement physique du point d'accès. Cet emplacement peut comporter 64 caractères au maximum. Tous les caractères alphanumériques sont valides, à l'exception des guillemets (""). Les espaces nuls ou vides ne sont pas autorisés.
Cluster Name	Entrez le nom de la grappe que le point d'accès doit rejoindre. Ce nom peut comporter 64 caractères au maximum. Tous les caractères alphanumériques sont valides, à l'exception des guillemets (""). Les espaces nuls ou vides ne sont pas autorisés. Le nom de la grappe n'est pas envoyé aux autres points d'accès qu'elle contient. Vous devez configurer le même nom de grappe sur chaque point d'accès membre. Chaque grappe configurée sur le réseau doit porter un nom unique.

Tableau 37 Gestion de la session (suite)

Champ	Description
User MAC	Indique l'adresse MAC du périphérique client sans fil. Une adresse MAC est une adresse matérielle qui identifie de façon unique chaque nœud d'un réseau.
Idle	Indique la durée pendant laquelle cette station est restée inactive. On considère qu'une station est inactive lorsqu'elle ne reçoit ou ne transmet aucune donnée.
Rate	Débit de transfert des données du point d'accès au client indiqué. Le débit de transmission des données est mesuré en <i>mégabits par seconde</i> (Mbits/s). Cette valeur doit figurer dans la plage de débit annoncée pour le mode utilisé par le point d'accès. Par exemple, de 6 à 54 Mbits/s pour 802.11a.
Signal	Puissance du signal de radiofréquences que le client reçoit du point d'accès. La mesure utilisée est une valeur appelée <i>indication de puissance de signal reçu</i> (RSSI, Received Signal Strength Indication), qui peut varier de 0 à 100. Le RSSI est déterminé par un mécanisme mis en œuvre sur la carte d'interface réseau de la station de client.
Receive Total	Nombre total de paquets reçus par le client au cours de la session.
Transmit Total	Nombre total de paquets transmis au client au cours de la session.
Error Rate	Pourcentage de fois où des trames sont abandonnées au cours de la transmission sur ce point d'accès.

Tri des informations de session

Pour trier les informations présentées dans les tableaux sur un indicateur en particulier, cliquez sur le libellé de la colonne que vous souhaitez utiliser pour le classement. Par exemple, si vous souhaitez classer les lignes du tableau en fonction de la puissance du signal, cliquez sur le libellé de colonne **Signal**. Les entrées sont alors triées par puissance du signal.

Configuration et affichage des paramètres de gestion des canaux

Lorsque la gestion des canaux est activée, le point d'accès attribue automatiquement les canaux radio utilisés par les points d'accès mis en grappe. Cette affectation automatique des canaux réduit les interférences mutuelles (ou les interférences avec d'autres points d'accès situés en dehors de la grappe) et optimise la bande passante Wi-Fi pour mieux gérer l'efficacité des communications sur le réseau sans fil.

Pour activer l'affectation automatique des canaux, vous devez démarrer la gestion des canaux ; celle-ci est désactivée par défaut sur les points d'accès neufs.

Selon un intervalle spécifié, le gestionnaire de canaux met en correspondance les points d'accès avec l'utilisation des canaux et mesure les niveaux d'interférences dans la grappe. En cas de détection d'interférences importantes, le gestionnaire de canaux réattribue automatiquement certains points d'accès, ou la totalité d'entre eux, à de nouveaux canaux selon un algorithme d'efficacité (ou *plan de canaux automatique*).

La page Channel Management présente les affectations de canaux précédentes, actuelles et prévues des points d'accès mis en grappe. Par défaut, l'affectation automatique de canaux est désactivée. Vous pouvez lancer la gestion des canaux pour optimiser leur utilisation sur l'ensemble de la grappe, à des intervalles programmés.

Pour configurer et afficher les affectations de canaux des membres de la grappe, cliquez sur l'onglet **Channel Management**.

Figure 35 Gestion des canaux

Getting Started Status Setup Wireless SNMP Administration **Cluster**

Access Points Sessions **Channel Management** Wireless Neighborhood

Channel Management

Channels

automatically re-assigning channels

Current Channel Assignments

IP Address	Wireless Radio	Band	Channel	Locked
10.27.65.83	00:21:29:00:1F:70	B/G/N	6	<input type="checkbox"/>

No New channels proposed in the last iteration. Proposed Channel Assignments (ago)

IP Address	Wireless Radio	Proposed Channel
------------	----------------	------------------

Advanced

Change channels if interference is reduced by at least

Determine if there is better set of channel settings every

Clustered

1 Access Points

Dans cette page, vous pouvez afficher les affectations de canaux de tous les points d'accès de la grappe, et démarrer ou arrêter la gestion automatique des canaux. Les paramètres avancés de cette page vous permettent de modifier le potentiel de réduction des interférences qui déclenche la réaffectation des canaux, modifier le programme de mise à jour automatique et reconfigurer le jeu de canaux utilisé pour les affectations.

Démarrage/arrêt de l'affectation automatique des canaux

Par défaut, l'affectation automatique de canaux est désactivée.



REMARQUE La gestion des canaux prend la priorité sur le comportement par défaut des grappes, qui consiste à synchroniser les canaux radio de tous les points d'accès au sein d'une grappe. Lorsque la gestion des canaux est activée, les canaux radio ne sont pas synchronisés sur les autres points d'accès de la grappe.

- Cliquez sur **Start** pour reprendre l'affectation automatique des canaux.
 Lorsque l'affectation automatique des canaux est activée, le gestionnaire de canaux met régulièrement en correspondance les canaux radio utilisés par les points d'accès mis en grappe et, le cas échéant, réaffecte les canaux sur les points d'accès mis en grappe afin de réduire les interférences avec les membres de la grappe ou avec d'autres points d'accès extérieurs à celle-ci.
- Cliquez sur **Stop** pour arrêter l'affectation automatique des canaux. (Plus aucune correspondance ou réaffectation de canaux ne sera effectuée et seules les mises à jour manuelles auront un impact sur l'affectation des canaux.)



REMARQUE L'affectation de canaux proposée n'est pas mise en place si le champ **Channel** de la page **Wireless Radio** est défini sur **auto**. Le canal doit être configuré en mode statique.

Affichage des affectations de canaux et définition de verrous

La section **Current Channel Assignments** contient la liste de tous les points d'accès de la grappe, classés par adresse IP. Sont affichés la bande de diffusion de chaque point d'accès (a/b/g/n), le canal utilisé par chaque point d'accès, ainsi qu'une option de verrouillage d'un point d'accès sur son canal radio actuel, de telle sorte qu'il ne puisse pas être réaffecté à un autre.

Le **Tableau 38** contient des détails sur les affectations de canaux en cours.

Tableau 38 Affectations de canaux

Champ	Description
IP Address	Adresse IP du point d'accès.
Wireless Radio	Adresse MAC de la radio.
Band	Bande sur laquelle le point d'accès diffuse.
Channel	Canal radio sur lequel le point d'accès diffuse.

Tableau 38 Affectations de canaux (suite)

Champ	Description
Locked	<p>Cliquez sur Locked pour forcer le point d'accès à rester sur le canal actuel.</p> <p>Lorsque l'option Locked est sélectionnée (activée) pour un point d'accès, les plans de gestion automatique des canaux ne réaffectent pas le point d'accès à un autre canal dans le cadre de la stratégie d'optimisation. Au contraire, les points d'accès dont les canaux sont verrouillés sont pris en compte en tant qu'éléments indispensables du plan.</p> <p>Si vous cliquez sur Apply, vous pouvez constater que sur les points d'accès verrouillés, les champs Current Channel et Proposed Channel contiennent le même canal. Les points d'accès verrouillés conservent leurs canaux actuels.</p>

Affichage du dernier ensemble de modifications proposé

La section *Proposed Channel Assignments* présente le dernier plan de canaux. Ce plan répertorie tous les points d'accès de la grappe par adresse IP, et présente les canaux actuels et proposés pour chaque point d'accès. Les canaux verrouillés ne sont pas réaffectés et l'optimisation de leur répartition sur les points d'accès tient compte du fait qu'ils doivent demeurer sur leurs canaux actuels. Les points d'accès qui ne sont pas verrouillés peuvent être affectés à d'autres canaux que ceux qu'ils utilisaient précédemment, en fonction des résultats du plan.

Tableau 39 Dernières modifications proposées

Champ	Description
IP Address	Adresse IP du point d'accès.
Wireless Radio	Canal radio sur lequel le point d'accès diffuse.
Proposed Channel	Canal radio auquel ce point d'accès serait réaffecté si le plan de canaux était exécuté.

Configuration des paramètres avancés

Les paramètres avancés permettent de personnaliser et de programmer le plan de canaux sur la grappe. Si vous utilisez la gestion des canaux telle quelle (sans mettre à jour les paramètres avancés), les canaux sont optimisés automatiquement une fois par heure si les interférences peuvent être réduites de 25 % ou davantage. Les canaux sont réaffectés même si le réseau est occupé. Les ensembles de canaux appropriés sont utilisés (b/g pour les points d'accès utilisant IEEE 802.11b/g et a pour les points d'accès utilisant IEEE 802.11a).

Les paramètres par défaut sont conçus pour répondre à la plupart des situations dans lesquelles la gestion des canaux doit être mise en œuvre.

Utilisez les **paramètres avancés** pour modifier le potentiel de réduction d'interférences qui déclenche la réaffectation des canaux, reprogrammer les mises à jour automatiques et reconfigurer l'ensemble de canaux utilisé pour les affectations. Si aucun champ n'est visible dans la section relative aux paramètres avancés, cliquez sur le bouton d'activation/de désactivation pour afficher les paramètres permettant de modifier la synchronisation et les détails de l'algorithme de programmation des canaux.

Tableau 40 Paramètres avancés de gestion des canaux

Champ	Description
Change channels if interference is reduced by at least	<p>Indiquez le pourcentage minimum de réduction des interférences qu'un plan proposé doit atteindre pour être appliqué. La valeur par défaut est 75 %.</p> <p>Choisissez un pourcentage compris entre 5 et 75 % dans le menu déroulant.</p> <p>Ce paramètre permet de définir une limite de réaffectation des canaux, de telle sorte que le réseau ne soit pas constamment perturbé pour des gains d'efficacité négligeables.</p> <p>Par exemple, si les interférences de canaux doivent être réduites de 75 % et que les affectations de canaux proposées ne les réduisent que de 30 %, les canaux ne sont pas réaffectés. En revanche, si vous redéfinissez la valeur minimale d'interférence des canaux sur 25 % et cliquez sur Apply, le plan de canaux proposé sera mis en œuvre et les canaux réaffectés au besoin.</p>

Tableau 40 Paramètres avancés de gestion des canaux (suite)

Champ	Description
Determine if there is better set of channels every	<p>Utilisez le menu déroulant pour spécifier la fréquence des mises à jour automatiques.</p> <p>Une plage d'intervalles est proposée, allant de 30 minutes à 6 mois.</p> <p>La valeur par défaut est d'une heure (l'utilisation des canaux est réévaluée et le plan de canaux obtenu appliqué toutes les heures).</p>

Cliquez sur **Apply** dans les paramètres avancés pour appliquer ces paramètres.

Les paramètres avancés prennent effet au moment où ils sont appliqués et influent sur l'exécution de la gestion automatique des canaux.

Affichage des informations sur le voisinage réseau sans fil

Le voisinage réseau sans fil présente tous les points d'accès situés à la portée de chacun des membres de la grappe, indique quels points d'accès sont à portée de quels membres de la grappe et établit une distinction entre les membres de la grappe et les éléments extérieurs à celle-ci.



REMARQUE À l'ouverture de la page **Cluster - Wireless Neighborhood**, un maximum de 20 points d'accès détectés est indiqué pour chaque point d'accès. Pour voir tous les points d'accès détectés, accédez directement à la page **Neighboring Access Points** de chaque point d'accès spécifique.

Pour chaque point d'accès voisin, la vue **Wireless Neighborhood** présente des informations d'identification (SSID ou nom réseau, adresse IP, adresse MAC), ainsi que des statistiques radio (puissance du signal, canal, intervalle de balise). Vous pouvez cliquer sur un point d'accès pour obtenir des statistiques supplémentaires sur les points d'accès à portée radio.

La vue Wireless Neighborhood peut vous aider à effectuer les opérations suivantes :

- Détecter et localiser les points d'accès inattendus (ou *indésirables*) d'un domaine sans fil, afin de prendre des mesures pour limiter les risques associés.
- Vérifier les attentes de couverture. Vous pouvez vérifier si le déploiement répond à vos objectifs de programmation en déterminant quels points d'accès sont visibles des autres à quelle puissance.
- Détecter les erreurs. Les modifications inattendues du modèle de couverture sont mises en évidence dans le tableau à l'aide de codes de couleurs.

Figure 36 Voisinage réseau sans fil

The screenshot displays the 'Wireless Neighborhood' configuration page. At the top, there are navigation tabs: Getting Started, Status, Setup, Wireless, SNMP, Administration, and Cluster. Below these are sub-tabs: Access Points, Sessions, Channel Management, and Wireless Neighborhood. The main content area is titled 'Wireless Neighborhood' and includes a description: 'The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.'

Below the description, there are radio buttons for 'Display Neighboring APs': In cluster, Not in cluster, and Both (selected). The main table shows the following data:

Cluster	
10.27.64.177 00:21:29:00:00:E0 (GAM's Cube 5)	
Neighbors (21)	
cisco-data	
ALT-VLAN-8	4 MBP _s
b9tcronewap54gv11	18 MBP _s
Holiday Inn	0 MBP _s
brcmwpa	28 MBP _s
dlink1	7 MBP _s
DL VAP w1 g	28 MBP _s
Guest Network	29 MBP _s
GP Net 0	25 MBP _s
NETGEAR_11g	21 MBP _s
NETGEAR_11g-1	23 MBP _s

Le **Tableau 41** décrit les informations liées au voisinage réseau sans fil.

Tableau 41 Informations relatives au voisinage réseau sans fil

Champ	Description
Display neighboring APs	<p>Cliquez sur l'une des cases d'option suivantes pour modifier la vue :</p> <p>In cluster : affiche uniquement les points d'accès voisins qui sont membres de la grappe.</p> <p>Not in cluster : affiche uniquement les points d'accès voisins qui ne sont pas membres de la grappe.</p> <p>Both : affiche tous les points d'accès voisins (membres de la grappe ou non).</p>
Cluster	<p>La liste Cluster, située en haut du tableau, présente les adresses IP de tous les points d'accès de la grappe. (Cette liste de membres de la grappe est identique à celle affichée sous l'onglet Cluster > Access Points.)</p> <p>S'il n'y a qu'un seul point d'accès dans la grappe, une seule colonne d'adresse IP est affichée. Elle indique que le point d'accès est mis en grappe avec lui-même.</p> <p>Vous pouvez cliquer sur une adresse IP spécifique pour afficher des détails complémentaires sur un point d'accès spécifique.</p>

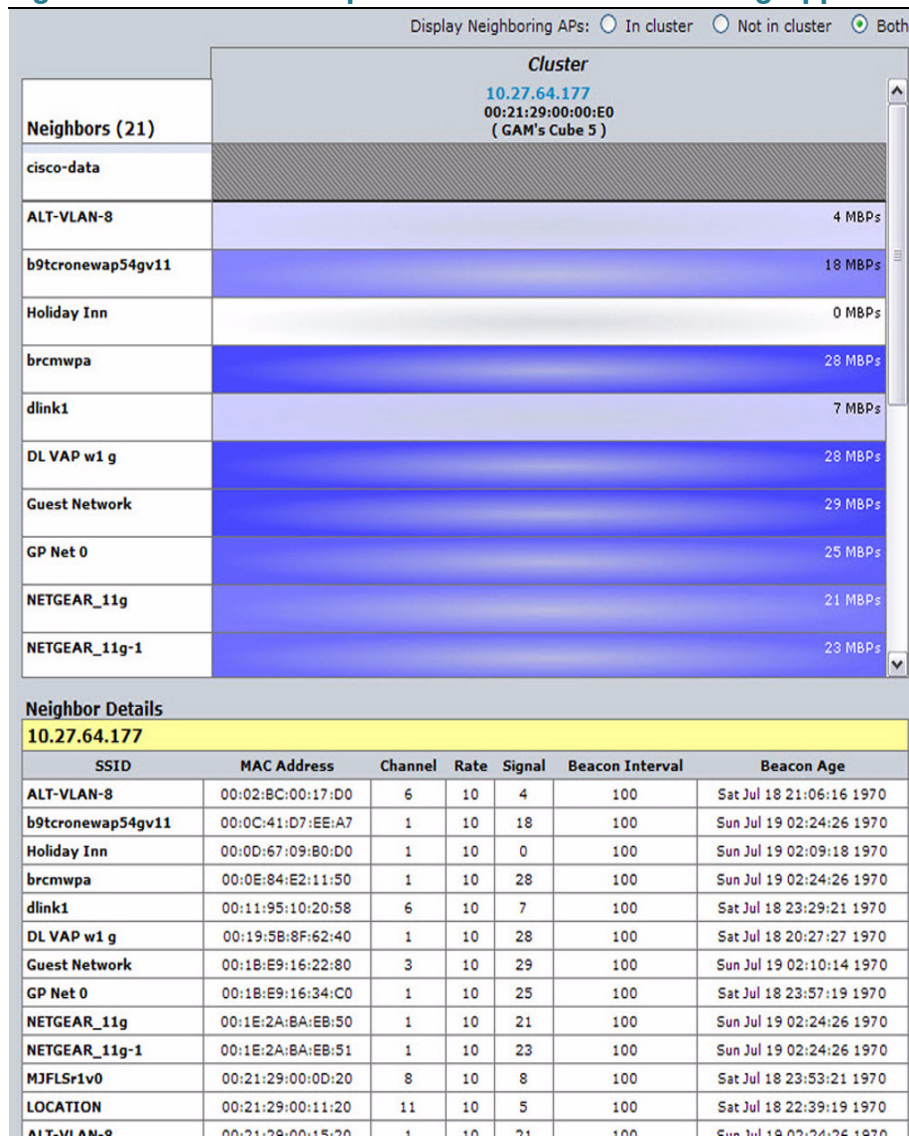
Tableau 41 Informations relatives au voisinage réseau sans fil (suite)

Champ	Description
Neighbors	<p>Les points d'accès voisins d'un ou plusieurs des points d'accès mis en grappe sont répertoriés dans la colonne de gauche et triés par SSID (nom réseau).</p> <p>Un point d'accès détecté comme voisin d'un membre de grappe peut également être membre de la grappe. Les voisins qui sont également membres de la grappe sont toujours affichés en haut de la liste. Ils sont surmontés d'une barre épaisse et contiennent un indicateur d'emplacement.</p> <p>Les barres de couleur figurant à droite de chaque point d'accès dans la liste des voisins indiquent la puissance du signal de chacun des points d'accès voisins, telle qu'elle est détectée par le membre de la grappe. L'adresse IP est affichée en haut de la colonne.</p> <p>La couleur de la barre indique la puissance du signal, comme suit :</p> <p>Barre bleu foncé : une barre bleu foncé et une valeur de puissance du signal élevée (par exemple 50) indiquent une puissance du signal élevée sur le voisin détecté par le point d'accès dont l'adresse IP figure au-dessus de la colonne.</p> <p>Barre bleu clair : une barre bleu clair et une valeur de puissance du signal moins élevée (par exemple 20 ou moins) indiquent une puissance du signal moyenne ou faible du voisin détecté par le point d'accès dont l'adresse IP figure au-dessus de la colonne.</p> <p>Barre blanche : une barre blanche et le chiffre 0 indiquent qu'un point d'accès voisin détecté par l'un des membres de la grappe n'est pas détectable par le point d'accès dont l'adresse IP figure au-dessus de la colonne.</p> <p>Barre gris clair : une barre gris clair sans valeur de puissance du signal indique qu'un voisin est détecté par d'autres membres de la grappe, mais pas par le point d'accès dont l'adresse IP figure au-dessus de la colonne.</p> <p>Barre gris foncé : une barre gris foncé sans valeur de puissance du signal indique qu'il s'agit du point d'accès dont l'adresse IP figure au-dessus de la colonne (car aucune valeur n'indique la manière dont le point d'accès peut se détecter lui-même).</p>

Affichage des détails relatifs à un membre de la grappe

Pour afficher des détails relatifs à un point d'accès membre de la grappe, cliquez sur l'adresse IP du membre, en haut de la page. La **Figure 37** présente les détails de voisinage du module radio 1 du point d'accès dont l'adresse IP est 10.27.64.177.

Figure 37 Détails d'un point d'accès membre d'une grappe



Le **Tableau 42** décrit les paramètres d'un point d'accès.

Tableau 42 Détails d'un membre de grappe

Champ	Description
SSID	<p>Identifiant SSID (Service Set Identifier) sur lequel ce point d'accès est présent.</p> <p>Le SSID est une chaîne alphanumérique composée de 32 caractères au maximum identifiant de façon unique un réseau local sans fil. Il est également appelé <i>nom réseau</i>.</p> <p>Un réseau invité et un réseau interne exécutés sur le même point d'accès doivent porter deux noms réseau différents.</p>
MAC Address	<p>Affiche l'adresse MAC du point d'accès voisin.</p> <p>Une adresse MAC est une adresse matérielle qui identifie de façon unique chaque nœud d'un réseau.</p>
Channel	<p>Affiche le canal de diffusion du point d'accès.</p> <p>Le canal définit la partie du spectre radio utilisée par le module radio pour transmettre et recevoir.</p>
Rate	<p>Affiche le débit (en mégabits par seconde) de transmission du point d'accès.</p> <p>Le débit est toujours l'un de ceux présentés sous Supported Rates.</p>
Signal	<p>Indique la puissance en décibels (Db) du signal radio émis par ce point d'accès.</p>
Beacon Interval	<p>Affiche l'intervalle de balise utilisé par ce point d'accès.</p> <p>Les intervalles de trame sont transmis à intervalles réguliers par un point d'accès pour annoncer l'existence du réseau sans fil. Par défaut, une trame de balise est envoyée toutes les 100 millisecondes (soit 10 par seconde).</p>
Beacon Age	<p>Affiche la date et l'heure de la dernière balise reçue de ce point d'accès.</p>

Des exemples de configuration

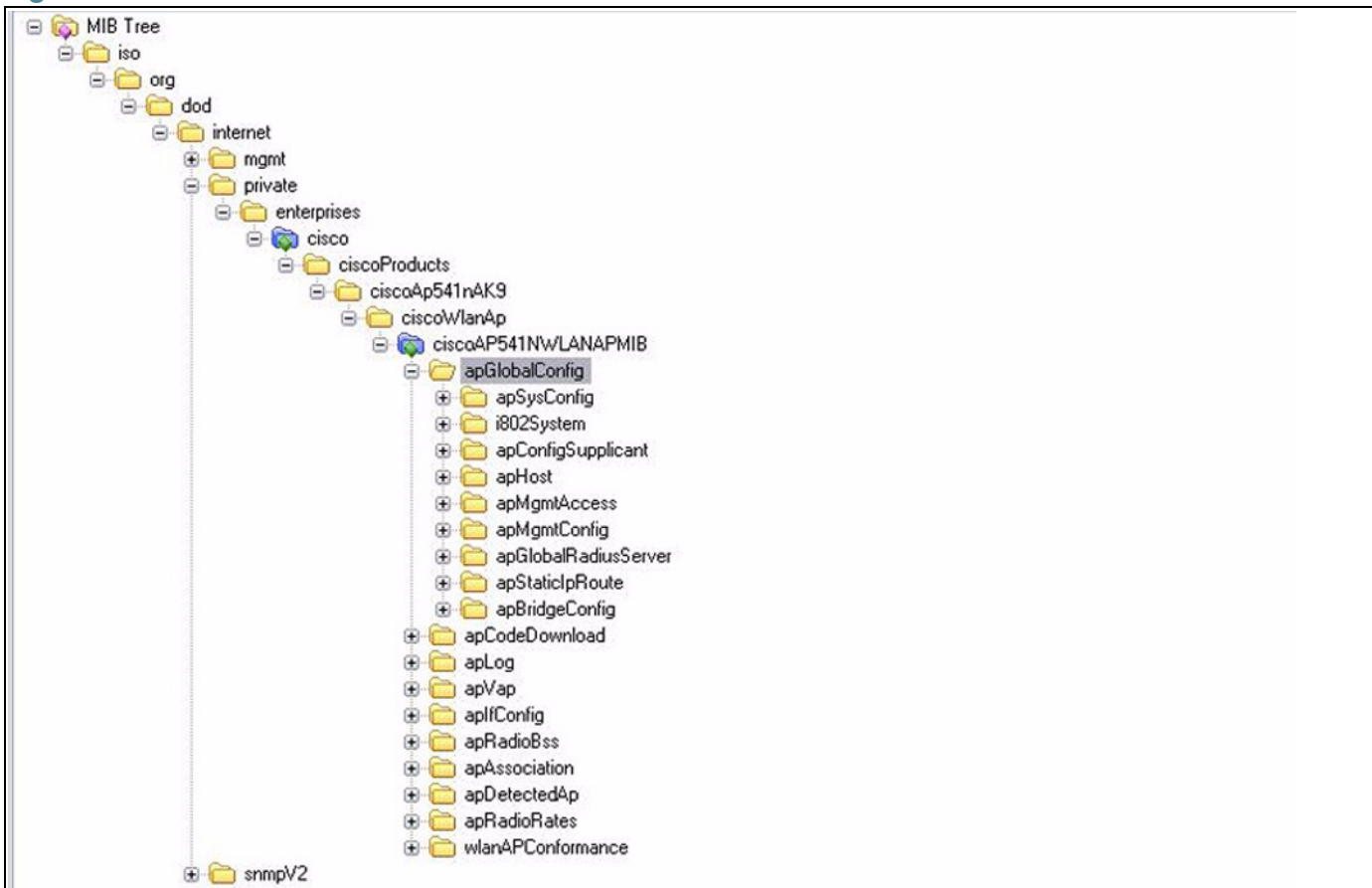
Ce chapitre contient des exemples de configuration des fonctions sélectionnées disponibles sur le point d'accès. Chaque exemple comporte les procédures à suivre pour la configuration de la fonction en utilisant *Utilitaire de configuration du point d'accès*, ou SNMP.

Ce chapitre décrit la réalisation des procédures suivantes :

- **Configuration d'un point d'accès virtuel (VAP)**
- **Configuration des paramètres de la radio sans fil**
- **Configuration du système de distribution sans fil**
- **Mise en grappe des points d'accès**

Pour tous les exemples SNMP, les objets utilisés pour modifier le point d'accès figurent dans une MIB privée. Le chemin d'accès aux tableaux contenant les objets est `iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).lv17(6132).lv17Products(1).fastPath(1).fastPathWLANAP(28)`, comme indiqué dans la **Figure 38**.

Figure 38 Arborecence MIB



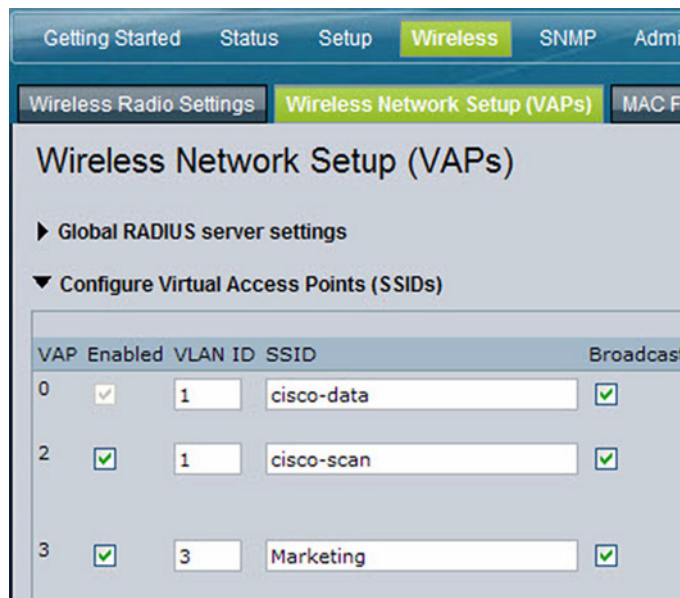
Configuration d'un point d'accès virtuel (VAP)

Cet exemple indique comment configurer le VAP 3 en utilisant des paramètres autres que les paramètres par défaut :

- ID de VLAN : 3
- SSID : marketing
- Sécurité : WPA Personal utilisant WPA2 avec CCMP (AES)

Configuration du VAP à partir de l'interface Web

- ÉTAPE 1** Connectez-vous au point d'accès et accédez à la page **Wireless > Wireless Network Setup (VAPs)**.
- ÉTAPE 2** Cochez la case correspondant au VAP 3 dans la colonne **Enabled**.
- ÉTAPE 3** Saisissez 3 dans la colonne VLAN ID.
- ÉTAPE 4** Dans la colonne **SSID**, supprimez le SSID existant et saisissez Marketing.



- ÉTAPE 5** Sélectionnez **WPA Personal** dans le menu dans la colonne **Security**.
L'écran est actualisé et des champs supplémentaires apparaissent.
- ÉTAPE 6** Sélectionnez les options **WPA2** et **CCMP (AES)** et décochez les options **WPA** et **TKIP**.
- ÉTAPE 7** Saisissez une clé de cryptage WPA dans le champ **Key**.
La clé peut être un mélange de caractères alphanumériques et de caractères spéciaux. La clé est sensible à la casse et peut contenir de 8 à 63 caractères.

The screenshot shows a configuration window for a Virtual Access Point (VAP). At the top, there are four dropdown menus: 'WPA Personal', 'Disabled', 'Disabled', and 'None'. Below these is a 'Hide details' link. The main configuration area includes:

- WPA Versions:** WPA (unchecked), WPA2 (checked)
- Cipher Suites:** TKIP (unchecked), CCMP (AES) (checked)
- Key:** JuPXkC7GvY\$moQiUttp
- Broadcast Key Refresh Rate (Range: 0-86400):** 300

ÉTAPE 8 Cliquez sur **Apply** pour appliquer les nouveaux paramètres au point d'accès.

Configuration du VAP à partir du SNMP

- ÉTAPE 1** Chargez le module FASTPATH-WLAN-ACCESS-POINT-MIB.
- ÉTAPE 2** À partir de l'arborescence MIB, accédez aux objets du tableau apVap.
- ÉTAPE 3** Consultez l'objet apVapDescription pour afficher l'ID de l'instance pour VAP 2 (wlan0vap2).
- VAP 2 sur la radio sans fil 1 correspond à l'instance 5.
- ÉTAPE 4** Utilisez l'objet apVapStatus pour régler l'état du VAP 2 au maximum (1).
- ÉTAPE 5** Utilisez l'objet apVapVlanID pour régler l'ID du VLAN du VAP 2 sur 2.
- ÉTAPE 6** Accédez aux objets du tableau apIfConfig.
- ÉTAPE 7** Consultez l'objet apIfConfigName pour afficher l'ID de l'instance pour VAP 2 (wlan0vap2).
- VAP 2 sur la radio sans fil 1 correspond à l'instance 7.
- ÉTAPE 8** Réglez la valeur de l'instance 7 dans l'objet apIfConfigSsid sur Marketing.
- ÉTAPE 9** Réglez la valeur de l'instance 7 dans l'objet apIfConfigSecurity sur wpa-personal (3).
- ÉTAPE 10** Réglez la valeur de l'instance 7 dans l'objet apIfConfigWpaPersonalKey sur JuPXkC7GvY\$moQiUttp2, qui correspond à la clé prépartagée WPA.
- ÉTAPE 11** Accédez aux objets du tableau apRadioBss > apBssTable.

ÉTAPE 12 Consultez l'objet apBssDescr pour afficher l'ID de l'instance pour VAP 2.

VAP 2 sur la radio sans fil 1 correspond à l'instance 3.

ÉTAPE 13 Réglez la valeur de l'instance 3 dans l'objet apBssWpaAllowed sur false (2).

ÉTAPE 14 Réglez la valeur de l'instance 3 dans l'objet apBssWpaCipherTkip sur false (2).

ÉTAPE 15 Réglez la valeur de l'instance 3 dans l'objet apBssWpaCipherCcmp sur true (1).

Configuration des paramètres de la radio sans fil

Cet exemple indique comment configurer la radio sans fil 1 à l'aide des paramètres suivants :

- Mode : IEEE 802.11b/g/n
- Canal : 6
- Bande passante du canal : 40 MHz
- Nombre maximal de stations : 100
- Puissance de transmission : 75 %

Configuration de la radio sans fil à partir de l'interface Web

ÉTAPE 1 Connectez-vous au point d'accès et accédez à la page **Wireless > Advanced Settings**.

ÉTAPE 2 Assurez-vous que 1 s'affiche dans le champ Wireless Radio et que l'état est **On**.

ÉTAPE 3 Sélectionnez 802.11b/g/n dans le menu **Mode**.

ÉTAPE 4 Sélectionnez 6 dans le champ **Channel**.

ÉTAPE 5 Sélectionnez 40 MHz dans le champ **Channel Bandwidth**.

ÉTAPE 6 Réglez la valeur sur 100 dans le champ **Maximum Stations**.

ÉTAPE 7 Réglez la valeur sur High dans le champ **Transmit Power**.

La fenêtre suivante affiche la page **Advanced Settings** avec les paramètres spécifiés dans cet exemple.

Getting Started Status Setup **Wireless** SNMP Administration Cluster

Wireless Radio Settings Wireless Network Setup (VAPs) MAC Filtering **Advanced Settings** WDS Bridge Bandwidth Utilization QoS Parameters

Advanced Settings

Status On Off

Mode 802.11b/g/n

Channel 6

Channel Bandwidth 40 MHz

Primary Channel Lower

Short Guard Interval Supported Yes

Protection Auto

Beacon Interval 100 (Msec, Range: 20 - 2000)

DTIM Period 2 (Range: 1-255)

Fragmentation Threshold 2346 (Range: 256-2346, Even Numbers)

RTS Threshold 2347 (Range: 0-2347)

Maximum Stations 100 (Range: 0-200)

Transmit Power High

Fixed Multicast Rate Auto Mbps

	Rate Supported	Basic
54 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
48 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
36 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
24 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ÉTAPE 8 Cliquez sur **Apply** pour appliquer les nouveaux paramètres au point d'accès.

Configuration de la radio sans fil à l'aide du SNMP

- ÉTAPE 1** Chargez le module MIB Cisco spécifique.
- ÉTAPE 2** À partir de l'arborescence MIB, accédez aux objets du tableau apRadio (apRadioBss > apRadioTable).
- ÉTAPE 3** Utilisez l'objet apRadioStatus pour régler l'état de la radio sans fil 1 au maximum (1).
- ÉTAPE 4** Utilisez l'objet apRadioMode pour régler le mode de la radio sans fil 1 sur IEEE 802.11b/g/n, qui correspond à bg-n (4).
- ÉTAPE 5** Utilisez l'objet apRadioChannelPolicy pour régler la stratégie du canal sur Static (1), ce qui désactive l'affectation automatique des canaux.
- ÉTAPE 6** Utilisez l'objet apRadioStaticChannel pour régler le canal sur 6.
- ÉTAPE 7** Utilisez l'objet apRadioChannelBandwidth pour régler la bande passante du canal de la radio sans fil 1 sur 40 MHz (2).
- ÉTAPE 8** Utilisez l'objet apRadioTxPower pour régler la puissance de transmission de la radio sans fil 1 sur 75.
- ÉTAPE 9** Accédez aux objets du tableau apBssTable.
- ÉTAPE 10** Utilisez l'objet apBssMaxStations pour régler le nombre maximal de stations autorisées sur 100.

Configuration du système de distribution sans fil

Cet exemple indique comment configurer une liaison WDS entre deux points d'accès. Le point d'accès local correspond à MyAP1 et comporte l'adresse MAC 00:1B:E9:16:32:40. Le point d'accès à distance correspond à MyAP2 et comporte l'adresse MAC 00:30:AB:00:00:B0.

La liaison WDS dispose des paramètres suivants devant être configurés sur les deux points d'accès :

- Cryptage : WPA (PSK)
- SSID : wds-link
- Clé : abcdefghijk

Configuration du WDS à partir de l'interface Web

Pour créer une liaison WDS entre deux points d'accès **MyAP1** et **MyAP2**, respectez les étapes suivantes :

ÉTAPE 1 Connectez-vous à MyAP1 et accédez à la page **Wireless > WDS Bridge**.

L'adresse MAC de MyAP1 (le point d'accès actuellement affiché) s'affiche automatiquement dans le champ Local Address.

ÉTAPE 2 Saisissez l'adresse MAC de MyAP2 dans le champ Remote Address.

ÉTAPE 3 Sélectionnez **WPA (PSK)** dans le menu Encryption.



REMARQUE L'option WPA (PSK) est disponible uniquement si le VAP 0 de la radio sans fil 1 utilise WPA (PSK) comme méthode de sécurité. Si VAP 0 n'est pas réglé sur WPA Personal ou WPA Enterprise, vous devez sélectionner None (texte brut) ou WEP pour le cryptage de la liaison WDS.

ÉTAPE 4 Saisissez `wds-link` dans le champ **SSID** et `abcdefghijkl` dans le champ **Key**.

ÉTAPE 5 Cliquez sur **Apply** pour appliquer les paramètres WDS au point d'accès.

Spanning Tree Mode	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Local Address	00:21:29:00:00:E0
Remote Address	00:21:29:00:15:20
Encryption	WPA (PSK)
SSID	wds-link
Key	abcdefghijkl

ÉTAPE 6 Connectez-vous à MyAP2 et répétez les étapes 2 à 5 (veillez à utiliser l'adresse MAC de MyAP1 dans le champ Remote Address).



REMARQUE MyAP1 et MyAP2 doivent être réglés sur le même mode IEEE 802.11 et émettre sur le même canal.

Configuration du WDS à partir du SNMP

ÉTAPE 1 Chargez le module FASTPATH-WLAN-ACCESS-POINT-MIB.

ÉTAPE 2 À partir de l'arborescence MIB, accédez aux objets du tableau apIfConfig.

ÉTAPE 3 Consultez l'objet apIfConfigName pour afficher l'ID de l'instance de la première liaison WDS (wlan0wds0).

La première liaison WDS correspond à l'instance 1.

ÉTAPE 4 Réglez la valeur de l'instance 1 dans l'objet apIfConfigRemoteMac sur 00:30:AB:00:00:B0.

Dans le navigateur MG-Soft, la valeur de l'adresse MAC à définir est au format # 0x00 0x30 0xAB 0x00 0x00 0xB0.

ÉTAPE 5 Réglez la valeur de l'instance 1 dans l'objet apIfConfigWdsSecPolicy sur WPA Personal (3).

ÉTAPE 6 Réglez la valeur de l'instance 1 dans l'objet apIfConfigSsid sur wds-link.

ÉTAPE 7 Réglez la valeur de l'instance 1 dans l'objet apIfConfigWdsWpaPskKey sur abcdefthijk.

Certains navigateurs MIB requièrent que des valeurs HEX soient saisies au lieu de valeurs ASCII.

ÉTAPE 8 Respectez les mêmes étapes de configuration pour MyAP2.

Mise en grappe des points d'accès

Cet exemple montre comment configurer une grappe avec deux points d'accès et activer la réattribution automatique des canaux. L'emplacement du point d'accès local est la salle 214 et le nom de la grappe est MyCluster.

Mise en grappe des points d'accès à l'aide de l'interface Web

- ÉTAPE 1** Connectez-vous au point d'accès et accédez à la page **Cluster > Access Points**.
- ÉTAPE 2** Saisissez l'emplacement du point d'accès et le nom de la grappe à ajouter.
- ÉTAPE 3** Cliquez sur **Apply**.
- ÉTAPE 4** Cliquez sur **Enable Clustering** pour activer la fonction de mise en grappe.

Une fois la page actualisée, la mise en grappe est activée pour d'autres points d'accès se trouvant sur le même segment ponté et dont les radios sans fil se trouvent dans le même mode d'exploitation. Ces points d'accès présentent le même nom de grappe qui est affiché dans le tableau Access Points.

Access Points

Access Points

Status: Clustering is enabled

Location	MAC Address	IP Address
Room 214	00:21:29:00:00:E0	10.27.64.177

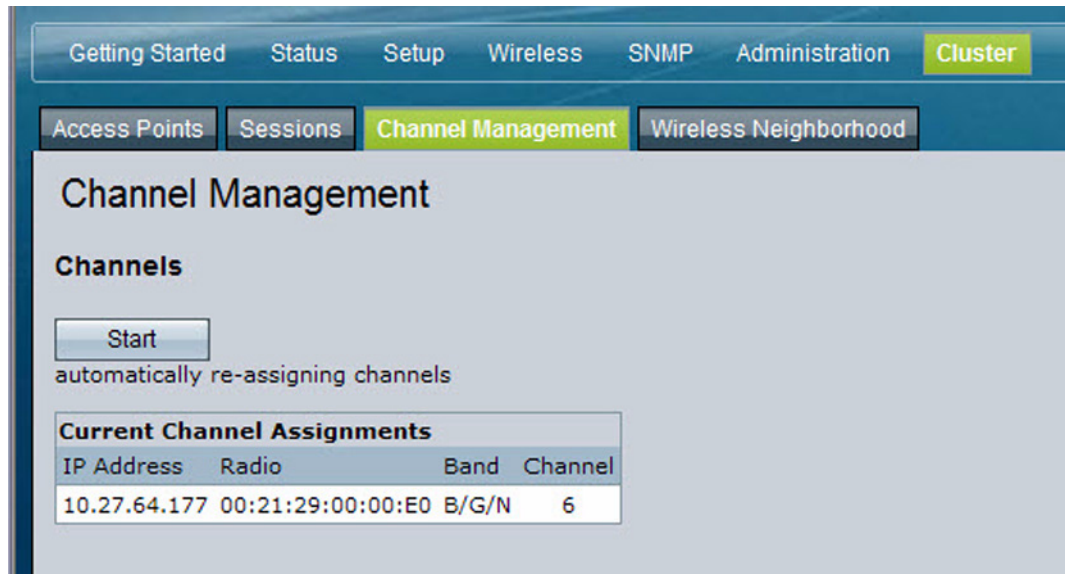
Clustering Options...

Location:

Cluster Name:

ÉTAPE 5 Pour lancer la fonction d'attribution automatique des canaux, accédez à la page **Channel Management**.

Sur la page, un tableau affiche les attributions actuelles de canaux.



ÉTAPE 6 Cliquez sur **Start**.

La page s'actualise et affiche les modifications de canaux proposées pour tous les points d'accès de la grappe. Le paramètre d'intervalle dans la section Advanced permet de déterminer la fréquence d'application des modifications proposées.

The screenshot displays the 'Channel Management' configuration page in the Cisco AP 541N web interface. The navigation menu at the top includes 'Getting Started', 'Status', 'Setup', 'Wireless', 'SNMP', 'Administration', and 'Cluster'. The 'Cluster' tab is active. Below the navigation, there are sub-tabs for 'Access Points', 'Sessions', 'Channel Management', and 'Wireless Neighborhood'. The 'Channel Management' sub-tab is selected.

Channel Management

Channels

automatically re-assigning channels

Current Channel Assignments

IP Address	Radio	Band	Channel	Locked
10.27.64.177	00:21:29:00:00:E0	B/G/N	6	<input type="checkbox"/>

Proposed Channel Assignments (1 minute and 5 seconds ago)

IP Address	Radio	Proposed Channel
10.27.64.177	00:21:29:00:00:E0	5

Advanced

Change channels if interference is reduced by at least

Determine if there is better set of channel settings every

Mise en grappe des points d'accès à l'aide du SNMP

La configuration de la mise en grappe à l'aide du SNMP n'est pas prise en charge.

Paramètres par défaut

Lors de la première mise sous tension d'un point d'accès, les paramètres par défaut affichés dans le **Tableau 43** s'appliquent.

Tableau 43 Paramètres UAP par défaut

Fonctionnalité	Par défaut
Informations sur le système	
User Name (Nom d'utilisateur)	<i>cisco</i>
Mot de passe	<i>cisco</i>
Paramètres de l'interface Ethernet	
Type de connexion	DHCP
DHCP	Activée
Adresse IP	192.168.10.10 (si aucun serveur DHCP n'est connecté)
Masque de sous-réseau	255.255.255.0
Nom du DNS	Aucun
ID du VLAN de gestion	1
ID du VLAN non balisé	1
Paramètres radio	
Radio	Arrêt
Mode Radio 1 IEEE 802.11	802.11b/g/n
Canal 802.11b/g/n	Auto
Bande passante du canal radio 1 sans fil	20 Mhz

Tableau 43 Paramètres UAP par défaut (suite)

Fonctionnalité	Par défaut
Canal 802.11a/n	Auto
Canal principal	Faible
Protection	Auto
Clients sans fil MAX	200
Puissance de transmission	100 %
Débits pris en charge (Mbits/s)	IEEE 802.11a : 54, 48, 36, 24, 18, 12, 9, 6 IEEE 802.11b : 11, 5.5, 2, 1 IEEE 802.11g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 IEEE 5-GHz 802.11n : 54, 48, 36, 24, 18, 12, 9, 6 IEEE 2.4 GHz 802.11g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1
Débits (Mbits/s) (Basiques/Signalés)	IEEE 802.11a : 24, 12, 6 IEEE 802.11b : 2, 1 IEEE 802.11g : 11, 5.5, 2, 1 EEE 5-GHz 802.11n : 24, 12, 6 IEEE 2.4 GHz 802.11n : 11, 5.5, 2, 1
SSID	données Cisco, voix Cisco, analyse Cisco
Limitation du débit de diffusion/multidiffusion	Activée
Débit de multidiffusion fixe	Auto
Beacon Interval (Intervalle de balise)	100
Période DTIM	2
Fragmentation Threshold (Seuil de fragmentation)	2346
RTS Threshold (Seuil RTS)	2347

Tableau 43 Paramètres UAP par défaut (suite)

Fonctionnalité	Par défaut
Paramètres du point d'accès virtuel	
État	Le VAP0 est activé sur les deux radios, tous les autres VAP sont désactivés
VLAN ID	1
Network Name (SSID) (Nom du réseau (SSID))	Cisco VAP pour VAP0 Le SSID pour tous les autres VAP est un point d'accès virtuel x où x correspond au numéro de VAP.
Broadcast SSID	Autoriser
Sécurité (mode)	VAP2 correspond à WPA Personal Tous les autres correspondent à None (texte brut)
Type d'authentification	Aucun
Adresse IP RADIUS	0.0.0.0
Clé RADIUS	secret
Comptabilité RADIUS	Désactivée
Redirection HTTP	Aucune
Autres paramètres par défaut	
Paramètres WDS	Aucun
STP	Désactivé
Authentification MAC	Aucune station dans la liste
Équilibrage de charge	Désactivé
SNMP	Activé
Nom de communauté RO SNMP	Public
Mode Managed AP	Désactivé
Authentification (demandeur 802.1X)	Désactivée
ACL de gestion	Désactivé

Tableau 43 Paramètres UAP par défaut (suite)

Fonctionnalité	Par défaut
Accès HTTP	Activé
Accès HTTPS	Activé
Port de l'agent SNMP	161
Requêtes du dispositif SNMP	Désactivées
Accès au port de console	Activé
Accès Telnet	Activé
Accès SSH	Activé
WMM	Activé
Protocole NTP (Network Time Protocol)	Aucun
Clustering	Arrêté
Mode Client QoS Global Admin	Désactivé
Mode VAP QoS	Désactivé

Pour en savoir plus

Cisco propose une vaste gamme de ressources pour vous aider à tirer pleinement parti du Point d'accès à radio unique bi-bande AP 541N.

Ressources sur les produits

Ressource	Emplacement
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Documentation technique	www.cisco.com/en/US/products/ps10024/tsd_products_support_series_home.html
Cisco AP 541N Dual-band Single-radio Access Point Administration Guide (dernière version)	www.cisco.com/en/US/docs/wireless/access_point/csbap/AP541N/administration/guide/AP541Nadmin.pdf
Guide d'administration Cisco Small Business Pro AP541N Dual-band Single-radio Access Point	https://www.cisco.com/en/US/docs/wireless/access_point/csbap/AP541N/administration/guide/AP541N.pdf
Cisco AP541N Wall Mount Template	www.cisco.com/en/US/docs/wireless/access_point/csbap/AP541N/release_notes/78-19205.pdf
Téléchargement de microprogrammes	www.cisco.com/en/US/products/ps10024/index.html
Service clientèle	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html

Ressource	Emplacement
Assistance technique et documentation en ligne (identification obligatoire)	www.cisco.com/support
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Garantie et Contrat de licence de l'utilisateur final	www.cisco.com/ca/allergarantie
Remarques sur les licences Open Source	www.cisco.com/go/osln
Informations relatives à la conformité et à la sécurité	www.cisco.com/en/US/products/ps10024/tsd_products_support_series_home.html
Assistant de configuration Cisco	www.cisco.com/en/US/products/ps7287/index.html
Site Cisco Partner Central pour les PME	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace