GUIDE D'ADMINISTRATION

Cisco Small Business

Point d'accès sans fil N WAP4410N avec Power Over Ethernet

Numéro de révision du document OL-23753-02

Table des matières

1

Introduction

Le point d'accès Cisco WAP4410N offre une plus grande portée et une plus grande mobilité à votre réseau sans fil tout en vous permettant de connecter le réseau sans fil à un environnement câblé. Il prend également en charge la fonctionnalité de configuration Wi-Fi protégée (WPS) qui contribue à simplifier la configuration de la sécurité sur un réseau sans fil. Le point d'accès Cisco WAP4410N offre la fonction PoE (Power over Ethernet), en complément du cordon d'alimentation 12 V CC standard, pour permettre de recevoir à la fois les données et l'alimentation sur un même câble réseau Ethernet.

Le Cisco WAP4410N prend en charge la norme 802.11n Draft 2.0 établie par l'IEEE. Il prend également en charge les clients 802.11g et 802.11b dans un environnement mixte. Grâce à l'utilisation de plusieurs antennes, dont la transmission et la réception des flux de données sont multidirectionnelles, ce point d'accès garantit une portée plus longue.

Suivez les instructions de ce guide pour vous aider à connecter le point d'accès, l'installer et le configurer pour relier vos différents réseaux. Ces instructions devraient s'avérer suffisantes pour vous permettre de tirer le meilleur parti du point d'accès.

Public ciblé

Le public visé par ce document comprend les utilisateurs, administrateurs et responsables du réseau sans fil.

Société

Ce tableau décrit le contenu de chaque chapitre de ce document.

Titre du chapitre	Description
« Introduction » page 6	Présente le point d'accès et ses fonctionnalités.
« Planification de votre réseau sans fil » page 8	Explique comment connecter le point d'accès au réseau.
« Présentation du point d'accès sans fil N » page 13	Décrit les caractéristiques physiques du point d'accès.
« Connexion du point d'accès Cisco WAP4410N » page 15	Explique comment positionner et connecter le point d'accès.
« Configuration du point d'accès sans fil N Cisco WAP4410N » page 19	Explique comment utiliser l'utilitaire Web afin de configurer les paramètres de base du point d'accès via le navigateur Web.
« Configuration du point d'accès sans fil N Cisco WAP4410N » page 24	Explique comment configurer et gérer votre point d'accès WAP4410.
« Dépannage » page 57	Fournit des solutions aux problèmes susceptibles de se produire lors de l'installation et de l'utilisation du point d'accès.
« Pour en savoir plus » page 64	Fournit des liens vers les sources d'informations connexes.

2

Planification de votre réseau sans fil

Topologie du réseau

Un réseau sans fil est un groupe d'ordinateurs, équipés chacun d'un ou de plusieurs adaptateurs sans fil. Pour communiquer entre eux, les ordinateurs d'un réseau sans fil doivent être configurés de façon à partager le même canal radio. Plusieurs ordinateurs équipés de cartes ou d'adaptateurs sans fil peuvent communiquer entre eux et constituer un réseau point à point (ad hoc) sans utiliser de point d'accès.

Cisco propose également des produits permettant aux adaptateurs sans fil d'accéder à des réseaux filaires au moyen d'un pont tel que le point d'accès sans fil ou le routeur sans fil. Un réseau sans fil et filaire intégré est appelé un réseau d'infrastructure. Dans un réseau d'infrastructure, chaque ordinateur sans fil peut communiquer avec tous les ordinateurs câblés ou sans fil via le point d'accès ou le routeur sans fil.

Une configuration d'infrastructure étend l'accessibilité d'un ordinateur sans fil à un réseau filaire et peut doubler l'étendue de transmission sans fil réelle de deux ordinateurs dotés d'adaptateur sans fil. Un point d'accès étant capable de transmettre des données dans un réseau, la portée de la transmission réelle d'un réseau d'infrastructure peut être plus que doublée car le point d'accès peut transmettre un signal à une puissance plus élevée dans l'espace sans fil.

Itinérance

Le mode Infrastructure prend également en charge les capacités d'itinérance des utilisateurs mobiles. L'itinérance signifie que vous pouvez déplacer votre ordinateur sans fil au sein de votre réseau. Dans ce cas, les points d'accès captent le signal de l'ordinateur sans fil, à condition qu'ils partagent le même réseau sans fil (SSID) et les mêmes paramètres de sécurité sans fil.

Avant d'utiliser l'itinérance, choisissez un canal radio exploitable et une position optimale du point d'accès. Les performances seront considérablement améliorées en combinant un positionnement approprié du point d'accès et un signal radio clair.

Présentation du réseau

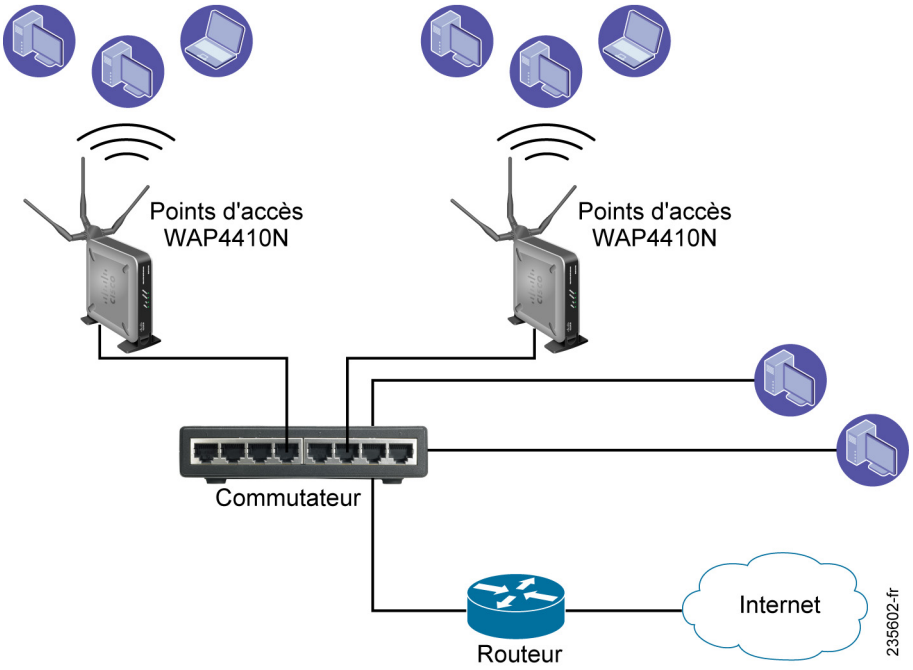
Le point d'accès sans fil N a été conçu pour être utilisé avec des produits 802.11n, 802.11g et 802.11b. Il est compatible avec des adaptateurs 802.11n, 802.11g et 802.11b, tels que les adaptateurs pour ordinateurs portables, les adaptateurs PCI pour ordinateurs de bureau et les adaptateurs USB pour tous les ordinateurs, afin de vous permettre de bénéficier d'une connectivité sans fil. Ces produits sans fil peuvent également communiquer avec un serveur d'impression sans fil 802.11n, 802.11g ou 802.11b (si disponible).

Pour raccorder votre réseau filaire à votre réseau sans fil, connectez le port du réseau Ethernet du point d'accès à n'importe quel commutateur ou routeur équipé de Power over Ethernet (PoE). Vous pouvez également le connecter à un routeur ou un commutateur non-PoE à l'aide de l'adaptateur secteur du point d'accès.

Si vous ajoutez à cela les nombreux autres produits Cisco, vos possibilités en matière de développement réseau sont illimitées. Pour plus d'informations sur les produits sans fil, rendez-vous sur le site Web de Cisco à l'adresse www.cisco.com.

Exemple d'un réseau sans fil simple

Le diagramme ci-dessous montre une configuration de réseau d'infrastructure sans fil standard.



Dans cette illustration, le commutateur se connecte à un routeur, lui-même raccordé à Internet. Le réseau assure la connectivité parmi les périphériques réseau sans fil et les ordinateurs disposant d'une connexion filaire avec le commutateur. Les points d'accès sans fil se connectent à un commutateur Cisco qui assure leur alimentation. Chaque point d'accès connecte plusieurs périphériques sans fil au réseau.

Protection de votre réseau

Les réseaux sans fil sont faciles à localiser. Les pirates informatiques savent que pour se connecter à un réseau sans fil, les produits réseau sans fil doivent d'abord écouter et détecter les « messages de balises ». Ces messages sont faciles à déchiffrer et renferment la plupart des informations relatives au réseau, notamment son SSID (Service Set Identifier).

Les mesures suivantes vous permettront de protéger votre réseau :

Changez régulièrement le mot de passe de l'administrateur.

Les paramètres réseau (par exemple, le SSID et les clés WEP) de chacun de vos périphériques sans fil sont stockés dans leurs microprogrammes respectifs.

L'administrateur réseau est la seule personne qui puisse modifier les paramètres réseau. Si un pirate informatique découvre le mot de passe de l'administrateur, il peut lui aussi changer ces paramètres.

Protégez votre SSID

- Désactivez la diffusion SSID. La plupart des périphériques réseau sans fil vous donnent la possibilité de diffuser le SSID. Bien que cette option puisse s'avérer pratique, elle permet à n'importe qui de se connecter à votre réseau sans fil, y compris aux pirates informatiques. Par conséquent, ne diffusez pas le SSID.
- Rendez le SSID unique. Les périphériques réseau sans fil possèdent un SSID par défaut, configuré en usine. Les pirates informatiques connaissent ces noms par défaut et peuvent vérifier s'ils sont utilisés sur votre réseau. Modifiez votre SSID afin qu'il soit unique tout en évitant d'en choisir un en relation avec votre société ou avec les périphériques réseau que vous utilisez.
- Modifiez souvent le SSID. Changez régulièrement de SSID afin de contraindre les pirates informatiques qui ont réussi à accéder à votre réseau de s'y connecter à nouveau.

Activez le filtrage des adresses MAC

Ce type de filtrage vous permet d'autoriser l'accès seulement aux nœuds sans fil dotés de certaines adresses MAC. Les pirates informatiques rencontrent ainsi plus de difficultés pour accéder à votre réseau au moyen d'une adresse MAC choisie au hasard.

Protégez votre réseau

- **WEP** : le chiffrement WEP est souvent considéré comme la panacée en matière de protection sans fil. Mais son efficacité est souvent surestimée. Cette protection fournit seulement un niveau de sécurité suffisant pour compliquer la tâche du pirate informatique.

  Plusieurs moyens permettent d'optimiser l'efficacité du chiffrement WEP :

  - Utilisez le niveau de chiffrement le plus élevé.
  - Optez pour une authentification par clé partagée.
  - Modifiez régulièrement votre clé WEP.

- **WPA/WPA2 Personal** : les méthodes WPA-Personal et WPA2-Personal proposent deux modes de chiffrement, TKIP et AES, associés à des clés de chiffrement dynamiques.

- **WPA /WPA2 Enterprise** : l'option WPA-Enterprise et WPA2-Enterprise nécessite que votre réseau utilise un serveur RADIUS pour l'authentification.

  Un réseau chiffré par WPA/WPA2 est mieux sécurisé qu'un réseau chiffré en WEP, car le WPA/WPA2 utilise le chiffrement par clé dynamique. Pour protéger les informations à mesure qu'elles sont transmises sur les ondes, vous devez définir le niveau de protection le plus élevé.

  La mise en place du chiffrement peut affecter les performances de votre réseau de manière néfaste. Cependant, il est préférable d'utiliser le chiffrement si des données confidentielles transitent par votre réseau.

AVERTISSEMENT Gardez à l'esprit que chaque périphérique de votre réseau sans fil *doit* utiliser la même méthode et la même clé de chiffrement pour que votre réseau sans fil fonctionne correctement.

3

Présentation du point d'accès sans fil N

Ce chapitre décrit les caractéristiques externes du point d'accès Cisco WAP4410N.

Façade

Les voyants situés sur la façade du point d'accès affichent les informations concernant l'activité du réseau.

- **Voyant POWER** (vert) : s'allume et reste allumé lorsque le périphérique est mis sous tension.
- **Voyant PoE** (vert) : s'allume lorsque le point d'accès est alimenté avec un câble Ethernet.
- **Voyant WIRELESS** (vert) : s'allume pour indiquer que le module sans fil est actif sur le point d'accès. Ce voyant clignote lorsque le point d'accès envoie des données au dispositif sans fil ou reçoit des données de ce dernier.
- **Voyant ETHERNET** (vert) : s'allume lorsque le point d'accès se connecte correctement à un dispositif via le port réseau Ethernet. Ce voyant clignote lorsque le point d'accès transmet des données à l'un des dispositifs ou reçoit des données de ces derniers, par le biais du port réseau Ethernet.

Panneau arrière

Le panneau arrière de l'appareil comporte les éléments suivants :

- **Bouton Reset** : pour rétablir la configuration par défaut du point d'accès, vous disposez de deux possibilités. Vous pouvez appuyer sur le bouton RESET, pendant environ 10 secondes, ou restaurer les valeurs par défaut à l'aide de l'utilitaire Web du point d'accès.
- **Port ETHERNET** : ce port se connecte aux périphériques réseau Ethernet, tels qu'un commutateur ou un routeur.
- **Port d'alimentation POWER** : ce port connecte le point d'accès au courant à l'aide du bloc d'alimentation 12 V CC fourni. Utilisez-le si votre commutateur ou routeur ne prend pas en charge la fonctionnalité PoE.

Antennes et positions

Le point d'accès Cisco WAP4410N est équipé de trois antennes omnidirectionnelles 2 dBi détachables. Ces antennes sont situées à l'arrière de l'appareil.

La base de chaque antenne peut pivoter de 90 degrés en position verticale. Les trois antennes prennent en charge la diversité 3x3 MIMO (multiple in, multiple out, entrée multiple, sortie multiple), en mode sans fil N.

4

Connexion du point d'accès Cisco WAP4410N

Ce chapitre décrit l'implantation et la connexion du point d'accès Cisco WAP4410N à votre réseau.

En fonction de votre application, vous devrez peut-être configurer le périphérique avant de le monter.

Dispositions possibles

Vous pouvez positionner le point d'accès Cisco WAP4410N à l'horizontale, sur ses pieds en caoutchouc ou à la verticale, sur un support. Vous pouvez également le fixer sur un mur.

Positionnement sur un bureau

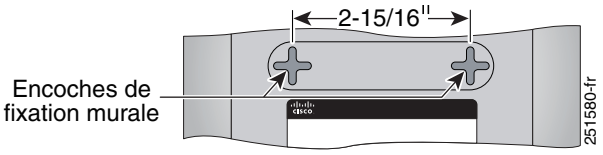
Pour installer le point d'accès sur un bureau, positionnez-le horizontalement, sur ses quatre pieds en caoutchouc.

Montage mural

Pour fixer le point d'accès Cisco WAP4410N à un mur, procédez comme suit :

ÉTAPE 1 Déterminez l'emplacement d'installation de l'appareil et insérez deux vis (non fournies) dans le mur en les espaçant d'environ 7,46 cm (2-15/16 pouces).

ÉTAPE 2 Pour fixer le point d'accès Cisco WAP4410N en position verticale, orientez le panneau arrière vers le haut, puis positionnez le point d'accès de telle sorte que les encoches de fixation murale en croisillons situées sur sa partie inférieure s'alignent sur les deux vis.



ÉTAPE 3 Placez les encoches de fixation murale au-dessus des vis et faites glisser l'appareil vers le bas jusqu'à ce que les vis s'insèrent parfaitement dans ces encoches.

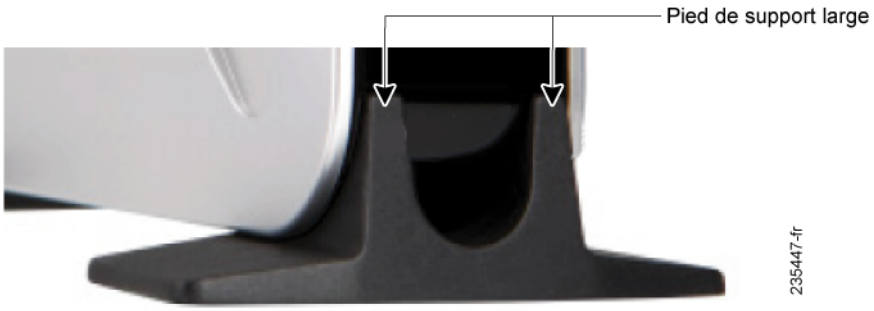
Montage sur support

Pour placer le point d'accès sur un support, en position verticale, procédez comme suit :

ÉTAPE 1 Repérez le panneau gauche de l'appareil (du côté opposé de l'antenne).

ÉTAPE 2 Placez les broches les plus grandes de l'un des socles vers l'extérieur et insérez les petites broches dans les logements de l'appareil, puis poussez le socle vers le haut, jusqu'à ce qu'il s'enclenche correctement.

Répétez cette étape pour l'autre support.



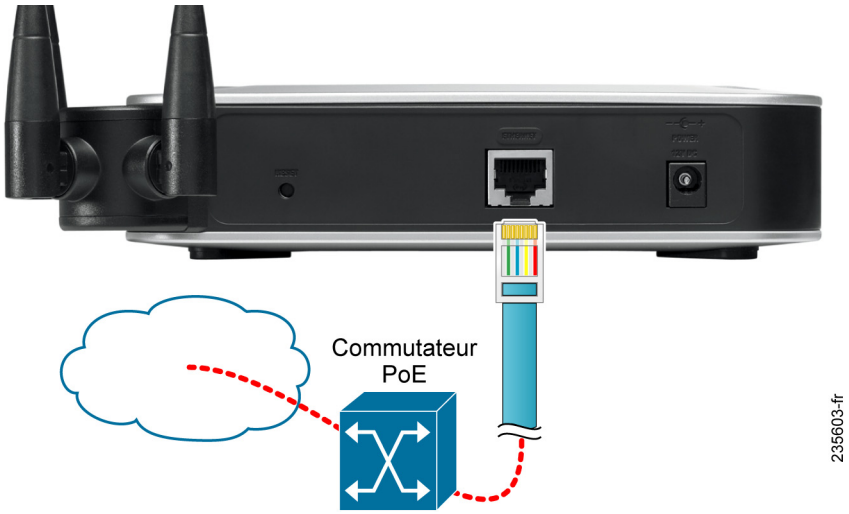
Connexion du point d'accès Cisco WAP4410N au réseau

Vous pouvez connecter le point d'accès Cisco WAP4410N à votre réseau en suivant l'une des méthodes ci-après :

- **Utilisation d'un routeur ou d'un commutateur PoE**
- **Utilisation d'un routeur ou d'un commutateur standard**

Utilisation d'un routeur ou d'un commutateur PoE

Pour connecter le point d'accès Cisco WAP4410N à votre réseau, en utilisant un routeur ou un commutateur PoE, connectez le port Ethernet du point d'accès à un port PoE du commutateur PoE.



Les voyants situés sur la façade s'allument dès que le point d'accès Cisco WAP4410N est sous tension.

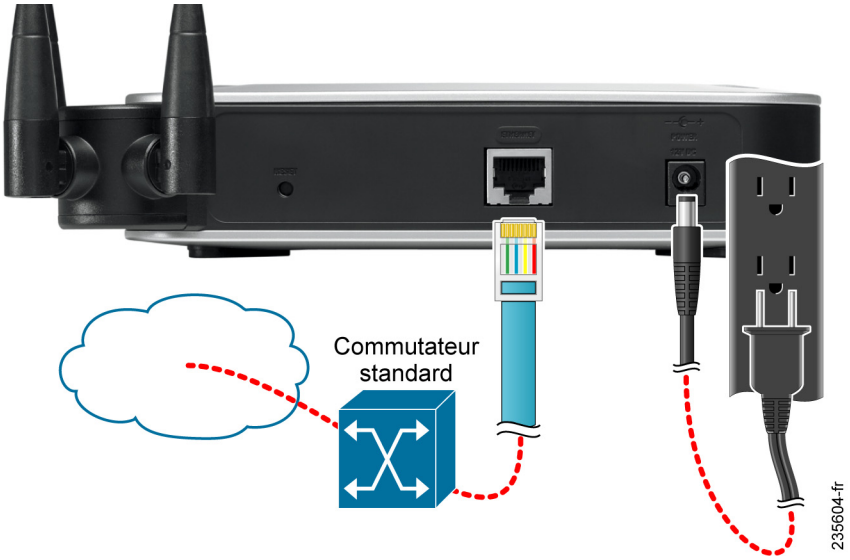
Utilisation d'un routeur ou d'un commutateur standard

Pour connecter le point d'accès Cisco WAP4410N à votre réseau, en utilisant un routeur ou un commutateur standard, suivez les étapes ci-après.

ÉTAPE 1 Utilisez le câble Ethernet fourni pour connecter le port Ethernet du point d'accès à un port Ethernet du commutateur.

ÉTAPE 2 Connectez l'adaptateur électrique (inclus) au port d'alimentation du point d'accès Cisco WAP4410N.

ÉTAPE 3 Branchez l'adaptateur électrique sur une prise secteur.



Les voyants situés sur la façade s'allument dès que le point d'accès Cisco WAP4410N est sous tension.

5

Configuration du point d'accès sans fil N Cisco WAP4410N

Le point d'accès Cisco WAP4410N fonctionne avec ses paramètres par défaut. Néanmoins, vous pouvez modifier ces paramètres, en fonction de vos besoins. Pour cela, vous devez accéder au point d'accès, à l'aide d'un utilitaire Web de configuration.

REMARQUE Assurez-vous que le protocole TCP/IP est activé sur vos ordinateurs avant de poursuivre. Les ordinateurs utilisent ce protocole pour communiquer sur le réseau.

Lancez l'utilitaire Web de configuration

Le microprogramme v2.0.0.5 ou version ultérieure a remplacé la configuration de l'adresse IP par défaut par DHCP. Avant de procéder à l'installation, assurez-vous que votre serveur DHCP est en cours d'exécution et accessible. Vous devrez peut-être débrancher et reconnecter les appareils pour qu'ils puissent détecter leur nouvelle adresse IP à partir du serveur DHCP.

Si le point d'accès Cisco WAP4410N ne reçoit pas de réponse DHCP au bout de 60 secondes, il reprend l'adresse IP statique par défaut suivante : 192.168.1.245 et un masque par défaut de 255.255.255.0.

REMARQUE Pour les microprogrammes antérieurs à la version v2.0.0.5, l'adresse IP statique est 192.168.1.245.

Pour configurer le point d'accès Cisco WAP4410N, accédez à l'utilitaire Web de configuration du Cisco WAP4410N depuis votre ordinateur en suivant les étapes ci-après.

ÉTAPE 1 Connectez le Cisco WAP4410N au même réseau que votre ordinateur.

ÉTAPE 2 Localisez l'adresse IP du point d'accès Cisco WAP4410N.

a. Pour les microprogrammes ultérieurs à la version v2.0.0.5, localisez l'adresse IP attribuée par votre serveur DHCP en accédant à votre routeur/serveur DHCP.

b. Pour les microprogrammes antérieurs à la version v2.0.0.5, l'adresse IP statique du périphérique WAP est 192.168.1.245, avec un masque par défaut de 255.255.255.0. Pour atteindre cette adresse IP, assurez-vous que votre ordinateur se trouve sur le réseau 192.168.1.xxx.

c. Les points d'accès sans fil peuvent être atteints et gérés par les outils et services réseau Cisco Small Business, y compris l'utilitaire Cisco FindIT Network Discovery Utility qui vous permet de trouver automatiquement tous les périphériques Cisco Small Business pris en charge dans le même segment du réseau local que votre ordinateur. Vous pouvez obtenir une vue instantanée de chaque périphérique ou lancer l'utilitaire de configuration du produit pour afficher et configurer les paramètres. Pour en savoir plus, consultez www.cisco.com/go/findit.

d. Les points d'accès sans fil sont des périphériques équipés de la fonction Bonjour qui émettent automatiquement leurs services et écoutent les services publiés par d'autres périphériques équipés de la fonction Bonjour. Si vous disposez d'un navigateur équipé de la fonction Bonjour, tel que Microsoft Internet Explorer avec un composant logiciel enfichable Bonjour ou le navigateur Apple Mac Safari, vous trouverez le point d'accès sans fil sur votre réseau local sans avoir à fournir son adresse IP. Vous pouvez télécharger la fonction Bonjour complète pour Internet Explorer à partir du site Web Apple, à l'adresse www.apple.com/bonjour/.

ÉTAPE 3 Lancez un navigateur Web, tel qu'Internet Explorer ou Mozilla Firefox.

ÉTAPE 4 Saisissez l'adresse du serveur DHCP par défaut dans le champ Adresse, puis appuyez sur la touche **Entrée**.

ÉTAPE 5 Saisissez le nom d'utilisateur par défaut **admin** et le mot de passe **admin** dans les champs Nom d'utilisateur et Mot de passe.

ÉTAPE 6 Cliquez sur **Login**. Lancez l'utilitaire Web de configuration pour configurer votre périphérique.

ÉTAPE 7 Pour les microprogrammes de version v2.0.5.0 ou ultérieure, l'assistant de configuration de point d'accès sans fil s'affiche. Pour terminer l'installation du périphérique WAP, suivez les instructions de l'assistant de configuration.

Navigation dans l'utilitaire

L'utilitaire Web de configuration se compose des pages principales suivantes :

- Setup (Configuration)
- Wireless (Réseau sans fil)
- AP Mode (Mode du point d'accès)
- Administration
- Status (État)

Setup (Configuration)

Cette page vous permet de configurer les paramètres de nom de l'hôte et d'adresse IP ainsi que de régler l'heure.

- **Basic Setup (Configuration de base)** : permet de configurer les paramètres de nom d'hôte et d'adresse IP pour ce point d'accès.
- **Time (Heure)** : permet de régler l'heure sur ce point d'accès.
- **Advanced (Avancé)** : permet de définir les paramètres de redirection HTTP et de demandeur 802.1x pour ce point d'accès.

Wireless (Sans fil)

Cette page vous permet de saisir plusieurs paramètres du réseau sans fil pour ce point d'accès.

- **Basic Settings (Paramètres de base)** : permet de configurer le mode du réseau sans fil (par exemple : B/G/N-Mixed), le SSID et le canal radio.
- **Security (Sécurité)** : permet de configurer les paramètres de sécurité du point d'accès.
- **Connection Control (Contrôle de la connexion)** : permet de contrôler les connexions sans fil des périphériques clients à ce point d'accès.
- **Configuration de WPS (configuration protégée par Wi-Fi)** : simplifie le processus de paramétrage et de configuration de la sécurité sur un réseau sans fil.

- **VLAN and QoS (Réseau VLAN et qualité de service)** : permet de configurer les paramètres VLAN 802.1Q et de qualité de service (QoS).
- **Advanced Setting (Paramètres avancés)** : permet de configurer les paramètres de réseau sans fil plus avancés du point d'accès (par exemple : équilibrage de la charge et bande passante du canal).

AP Mode (Mode du point d'accès)

Cette page vous permet de sélectionner le mode de fonctionnement du point d'accès. Le mode par défaut est le point d'accès.

Administration

Cette page vous permet de gérer le point d'accès.

- **Management (Gestion)** : permet de configurer les paramètres de mot de passe et du protocole de gestion SNMP (Simple Network Management Protocol).
- **Log (Journal)** : permet de configurer les paramètres de journal.
- **Diagnostics** : permet d'effectuer les activités de diagnostic, ce qui peut s'avérer utile pour résoudre les problèmes de réseau.
- **Factory Default (Valeurs par défaut d'usine)** : permet de réinitialiser le point d'accès sur ses paramètres par défaut d'usine.
- **Firmware Upgrade (Mise à niveau du microprogramme)** : permet la mise à niveau du microprogramme du point d'accès sur cet écran.
- **Reboot (Redémarrer)** : redémarre le point d'accès.
- **Configuration Management (Gestion des configurations)** : permet d'enregistrer et de restaurer la configuration du point d'accès.
- **SSL Certification Management (Gestion de la certification SSL)** : exporte ou installe un certificat SSL.

Status (État)

Cette page vous permet de visualiser les informations relatives à l'état de votre réseau local, des réseaux sans fil et des performances du réseau.

- **Local Network (Réseau local)** : affiche les informations du système, dont les versions de logiciel et de matériel, l'adresse MAC et l'adresse IP du côté LAN du point d'accès.
- **Wireless (paquets d'erreurs fil)** : affiche les paramètres du réseau sans fil, notamment le SSID, le mode de réseau, le paramétrage de priorité, les liaisons VLAN et le canal sans fil.
- **System Performance (Performances du système)** : affiche les statistiques de trafic actuelles de ce point d'accès à la fois pour le réseau sans fil et pour les ports LAN.

6

Configuration du point d'accès sans fil N Cisco WAP4410N

Ce chapitre explique comment configurer votre point d'accès Cisco WAP4410N à l'aide de l'utilitaire de configuration Web. Cet utilitaire Web comporte les rubriques suivantes, lesquelles font l'objet d'une description dans ce chapitre.

- **Setup (Configuration)**
- **Wireless (Réseau sans fil)**
- **AP Mode (Mode du point d'accès)**
- **Administration**
- **Status (État)**

Setup (Configuration)

La section Setup explique comment configurer les paramètres généraux du point d'accès.

Basic Setup (Configuration de base)

La page *Setup > Basic Setup* affiche les paramètres généraux du point d'accès. Vous pouvez définir les paramètres de configuration de base suivants :

- « Définition des paramètres de configuration de périphérique » page 25
- « Définition des paramètres de configuration réseau » page 26

Définition des paramètres de configuration de périphérique

Pour définir les paramètres de configuration de périphérique du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Setup > Basic Setup**.

ÉTAPE 2 Dans la section Device Setup, saisissez les informations suivantes :

- **Host Name** : nom alloué de façon administrative au périphérique WAP. Le nom d'hôte par défaut est « wap », concaténé avec les 6 derniers chiffres hexadécimaux de l'adresse MAC du périphérique WAP. Le nom d'hôte ne peut comporter que des lettres, des chiffres et des tirets. Les noms d'hôte ne peuvent pas être précédés ni suivis d'un tiret. Les autres symboles, les signes de ponctuation et les espaces ne sont pas autorisés.

  Vous pouvez utiliser le nom d'hôte pour accéder à l'utilitaire de configuration Web via le réseau si ce nom d'hôte est enregistré dans votre serveur DNS. Le point d'accès publie le nom d'hôte sur votre serveur DNS si vous avez configuré le point d'accès afin d'acquérir son adresse IP à partir d'un serveur DHCP.

- **Device Name** : saisissez le nom de périphérique du point d'accès.

  Ce nom est utilisé à des fins d'identification uniquement. L'utilisation de noms uniques et facilement mémorisables est pratique, notamment si vous déployez plusieurs points d'accès sur le même réseau. Ce nom vous permet d'identifier le point d'accès une fois que vous êtes connecté.

  Le nom par défaut est **WAP4410N**.

ÉTAPE 3 Cliquez sur **Save** (Enregistrer).

Définition des paramètres de configuration réseau

Cette section explique comment définir les paramètres de configuration réseau du point d'accès. Pour plus d'informations sur l'adresse IP par défaut du point d'accès, reportez-vous à **Lancez l'utilitaire Web de configuration**

ÉTAPE 1 Cliquez sur **Setup** > **Basic Setup**.

ÉTAPE 2 Dans le menu déroulant **IP Settings**, sélectionnez l'une des options suivantes :

- **Static IP Address** : sélectionnez cette option pour affecter une adresse IP statique ou fixe au point d'accès.
- **Automatic Configuration** : sélectionnez cette option pour configurer automatiquement les paramètres réseau IPv4 du point d'accès à l'aide d'un serveur DHCP sur votre réseau. Cette option permet également de configurer automatiquement les paramètres réseau IPv6 du point d'accès à l'aide d'un périphérique RADVD IPv6 activé sur votre réseau.

ÉTAPE 3 Si vous sélectionnez **Static IP Address** dans le menu déroulant **IP Settings**, saisissez les informations suivantes dans la section IPv4 de l'écran :

- **Local IP Address** : saisissez une adresse IP unique pour votre point d'accès. L'adresse IP par défaut est **192.168.1.245**.
- **Subnet Mask** : saisissez le même masque de sous-réseau que celui utilisé dans votre réseau. La valeur par défaut est **255.255.255.0**.
- **Default Gateway** : saisissez l'adresse IP de votre passerelle ou routeur. Saisissez la valeur utilisée par d'autres périphériques sur votre LAN.
- **Primary DNS** : saisissez l'adresse IP de votre serveur DNS principal.
- **Secondary DNS** : saisissez l'adresse IP de votre serveur DNS secondaire.

ÉTAPE 4 Pour configurer les paramètres IPv6 de votre point d'accès, procédez comme suit :

- **IPv6** : sélectionnez la valeur Enabled afin d'activer IPv6 pour votre point d'accès.
- **Accept Router Advertisement** : cochez cette case pour accepter l'annonce de routeur.
- **Local IP Address** : saisissez une adresse IP unique pour votre point d'accès.
- **Default Gateway** : saisissez l'adresse IP de votre passerelle ou routeur. Cette adresse est utilisée par les autres périphériques sur votre réseau.

- **Primary DNS** : saisissez l'adresse IP de votre serveur DNS principal.
- **Secondary DNS** : saisissez l'adresse IP de votre serveur DNS secondaire.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Time (Heure)

La page *Setup* > *Time* affiche les paramètres de date/heure du point d'accès. En configurant la date et l'heure correctes, vous pouvez aider votre administrateur réseau dans la recherche du journal système afin d'identifier les problèmes. Par défaut, le périphérique WAP est configuré de manière à obtenir l'heure depuis une liste prédéfinie de serveurs NTP.

Pour configurer les paramètres de date/heure du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Setup** > **Time**.

ÉTAPE 2 Pour configurer manuellement les paramètres de date/heure, procédez comme suit :

a. Sélectionnez **Manually**.

b. Saisissez la date et l'heure.

ÉTAPE 3 Pour configurer automatiquement les paramètres de date/heure afin d'obtenir la date et l'heure depuis un serveur temporel sur votre réseau ou sur Internet, procédez comme suit :

a. Sélectionnez **Automatically**.

b. Dans le menu déroulant **Time Zone**, sélectionnez un fuseau horaire.

c. Au besoin, cochez la case **Automatically adjust clock for Daylight Saving Changes**.

ÉTAPE 4 Pour configurer un serveur NTP local, activez la case de l'option **User Defined NTP Server**. La valeur par défaut est **Disabled**.

- **NTP Server IP** : saisissez l'adresse IP du serveur NTP défini par l'utilisateur.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Advanced (Avancé)

La page *Setup > Advanced* affiche les paramètres avancés. Pour configurer les paramètres de configuration avancés du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Setup > Advanced**.

ÉTAPE 2 L'option LAN Port Speed Settings permet de configurer les paramètres du port qui connecte physiquement le périphérique WAP à un réseau local.

a. S'il existe des problèmes de compatibilité entre le périphérique WAP et votre commutateur, activez la case **Force LAN Port Speed to 100M**. La valeur par défaut est Disabled.

b. Activez ou désactivez le champ Auto Negotiation. Ce champ est désactivé par défaut. Lorsqu'il est activé, le port négocie avec son partenaire de liaison afin de définir la vitesse de liaison la plus rapide et le mode duplex disponible. S'il est désactivé, vous pouvez configurer manuellement la vitesse du port et le mode duplex.

c. Si la négociation automatique est désactivée, sélectionnez 10 Mbit/s, 100 Mbit/s ou 1000 Mbit/s comme vitesse de port (**Port Speed**) et choisissez le mode duplex intégral (Full duplex) ou semi-duplex (Half duplex).

ÉTAPE 3 Pour activer Bonjour, cliquez sur **Enabled**. La valeur par défaut est **Enabled**. Bonjour permet au périphérique WAP et à ses services d'être découverts à l'aide de mDNS (DNS à multidiffusion). Bonjour annonce ses services au réseau et répond aux questions concernant les types de service pris en charge, ce qui simplifie la configuration du réseau dans les petites entreprises.

ÉTAPE 4 Activez ou désactivez la fonction de redirection des clients sans fil vers une page Web personnalisée. 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 périphérique WAP et que l'utilisateur ouvre un navigateur Web sur le client pour accéder à Internet. 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.

REMARQUE Le client sans fil est redirigé vers le serveur Web externe une seule fois, lorsqu'il est associé au périphérique WAP.

Dans le champ URL, indiquez l'URL vers laquelle le navigateur Web doit être redirigé une fois que le client sans fil est associé au périphérique WAP et envoie du trafic HTTP.

ÉTAPE 5 L'authentification IEEE 802.1X permet au point d'accès d'atteindre un réseau filaire sécurisé. Vous pouvez activer le point d'accès en tant que demandeur (client) 802.1X sur le réseau filaire. Pour activer les paramètres de demandeur 802.1X, procédez comme suit :

a. Dans le champ 802.1x Supplicant, cliquez sur **Enabled**.

b. Pour utiliser l'adresse MAC à des fins d'authentification, cliquez sur **Authentication via MAC Address**.

c. Pour utiliser un nom et un mot de passe pour l'authentification, cliquez sur **Authentication via Name and Password** et saisissez le nom et le mot de passe dans les champs correspondants.

ÉTAPE 6 Cliquez sur **Save** (Enregistrer).

Wireless (Réseau sans fil)

La section Wireless explique comment configurer les paramètres sans fil du point d'accès.

Basic Settings (Paramètres de base)

La page *Wireless > Basic Settings* affiche les paramètres de réseau sans fil de base. Pour configurer les attributs de base de ce point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless > Basic Settings**.

ÉTAPE 2 Dans le champ Wireless Network Mode, sélectionnez l'un des modes suivants :

- **Disabled** : désactive complètement la connectivité sans fil. Cela peut s'avérer utile lors de la maintenance du système.
- **B-Only** : connecte tous les périphériques clients sans fil au point d'accès à des débits sans fil B avec une vitesse maximale de 11 Mbit/s.
- **G-Only** : connecte les périphériques clients sans fil N et sans fil G à des débits sans fil G avec une vitesse maximale de 54 Mbit/s. Les clients sans fil B ne peuvent pas être connectés dans ce mode.

- **N-Only** : connecte uniquement les périphériques clients sans fil N à des débits sans fil N avec une vitesse maximale de 300 Mbit/s. Pour plus d'informations, reportez-vous à la **REMARQUE**.
- **B/G-Mixed** : connecte les périphériques clients sans fil B et sans fil G à leurs débits respectifs. Les périphériques sans fil N peuvent être connectés à des débits sans fil G.
- **B/G/N-Mixed** : (par défaut) connecte tous les périphériques clients sans fil à leurs débits respectifs dans ce mode mixte.

ÉTAPE 3 Dans le menu déroulant Wireless Channel, sélectionnez le canal approprié à utiliser sur votre point d'accès et vos périphériques clients. Le canal par défaut est le canal 6.

Vous pouvez également sélectionner **Auto** dans le menu déroulant Wireless Channel de sorte que votre point d'accès sélectionne le canal présentant le moins d'interférences sans fil lorsque le système est mis sous tension. La sélection automatique des canaux démarre lorsque vous cliquez sur **Save**. L'analyse de l'ensemble des canaux peut prendre plusieurs secondes pour trouver le meilleur d'entre eux.

REMARQUE Pour l'option de canal 40 MHz sans fil N (reportez-vous à l'écran Wireless > Advanced), le point d'accès peut combiner deux canaux 20 MHz en un canal plus large et ainsi multiplier le débit par deux.

La norme N est capable d'utiliser 40 MHz de bande passante pour des débits accrus, mais elle requiert un canal 20 MHz principal, plus un canal adjacent libre à ±20 MHz pour maintenir la compatibilité avec les systèmes existants. Le canal principal est utilisé pour les anciens modes (a/b/g) ou d'autres clients qui ne sont pas en mesure d'assurer la transmission à 40 MHz.

Nous vous conseillons de ne pas activer 40 MHz dans la bande de 2,4 GHz dans les zones commerciales à forte densité.

ÉTAPE 4 Dans les champs **SSID Name** et **SSID Broadcast**, saisissez les SSID que vous souhaitez que votre point d'accès diffuse :

- **SSID Name** : ce champ indique un SSID unique partagé par tous les périphériques dans un réseau sans fil. Il est sensible à la casse, ne doit pas dépasser 32 caractères alphanumériques et peut contenir n'importe quel caractère saisissable au clavier. Assurez-vous que ce nom est utilisé par tous les périphériques de votre réseau sans fil. Le nom SSID par défaut est **ciscosb**.
- **SSID Broadcast** : permet la diffusion du SSID sur votre réseau. Vous pouvez activer cette fonctionnalité lors de la configuration du réseau.

Toutefois, n'oubliez pas de la désactiver lorsque vous avez terminé. Lorsque cette option est activée, les informations de SSID peuvent être facilement obtenues à l'aide d'un logiciel d'analyse de site ou de Windows XP, pour obtenir un accès non autorisé à votre réseau. Sélectionnez **Enabled** pour diffuser le nom SSID à tous les périphériques sans fil autorisés. Sélectionnez **Disabled** pour augmenter la sécurité du réseau et empêcher que le SSID ne soit visible par des PC en réseau. La valeur par défaut est **Enabled** pour permettre aux utilisateurs de configurer facilement leur réseau avant de l'utiliser.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Security (Sécurité)

La page *Wireless > Security* affiche les paramètres de sécurité sans fil du point d'accès. Pour configurer les paramètres de sécurité sans fil du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Pour configurer l'isolation sans fil entre les SSID, procédez comme suit :

a. Dans le menu déroulant **Select SSID**, sélectionnez un SSID.

b. Pour isoler les clients sans fil les uns des autres, cliquez sur **Enabled**. Sinon, cliquez sur **Disabled**.

ÉTAPE 3 Pour désactiver complètement la sécurité sans fil, dans le menu déroulant Security Mode, sélectionnez **Disabled**. Il s'agit du paramètre par défaut.

ÉTAPE 4 Pour activer la sécurité sans fil, dans le menu déroulant Security Mode, sélectionnez l'un des modes de sécurité suivants et fournissez les informations requises, comme indiqué dans les sections ci-dessous.

- **WPA-Personal**
- **WPA2-Personal**
- **WPA2-Personal Mixed**
- **WPA-Enterprise**
- **WPA2-Enterprise**
- **WPA2-Enterprise Mixed**

- **Radius**
- **WEP**

ÉTAPE 5 Pour empêcher les ordinateurs sans fil associés à un même SSID de visualiser et de transférer des fichiers entre eux, dans le champ Wireless Isolation (within SSID), cliquez sur **Enabled.**

Cette fonctionnalité est très utile pour configurer l'emplacement d'un point d'accès sans fil. La valeur par défaut est **Disabled**.

ÉTAPE 6 Cliquez sur **Save** (Enregistrer).

Configuration de WPA-Personal

Wi-Fi Protected Access (WPA) Personal (WPA-Personal) est une norme de sécurité plus puissante que le chiffrement WEP et compatible en aval avec la norme IEEE 802.11e. Le protocole WPA-Personal est également appelé WPA-PSK. Pour activer la sécurité WPA-Personal sans fil, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Dans le menu déroulant Security Mode, sélectionnez **WPA-Personal**.

ÉTAPE 3 Pour activer l'isolation sans fil au sein du SSID, cliquez sur **Enabled**.

ÉTAPE 4 Fournissez les informations suivantes :

- **WPA Algorithms** : WPA offre deux méthodes de chiffrement pour les données : TKIP et AES. Sélectionnez le type d'algorithme que vous souhaitez utiliser (**TKIP** ou **AES**). La valeur par défaut est **TKIP**.
- **Pre-Shared Key** : saisissez une clé partagée WPA comprenant entre 8 et 63 caractères.
- **Key Renewal** : saisissez un délai de renouvellement des clés pour indiquer au point d'accès la fréquence à laquelle il doit modifier les clés de chiffrement. La valeur par défaut est **3600** secondes.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Configuration de la sécurité WPA2-Personal

Ce mode de sécurité prend en charge le protocole WPA2-Personal. Pour activer la sécurité WPA2-Personal sans fil, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Dans le menu déroulant Security Mode, sélectionnez **WPA2-Personal**.

ÉTAPE 3 Pour activer l'isolation sans fil au sein du SSID, cliquez sur **Enabled**.

ÉTAPE 4 Fournissez les informations suivantes :

- **WPA Algorithms** : (lecture seule) WPA2-Personal choisit automatiquement AES pour le chiffrement des données.
- **Pre-Shared Key** : saisissez une clé partagée WPA comprenant entre 8 et 63 caractères.
- **Key Renewal** : saisissez un délai de renouvellement des clés pour indiquer au point d'accès la fréquence à laquelle il doit modifier les clés de chiffrement. La valeur par défaut est **3600** secondes.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Configuration de WPA2-Personal Mixed

Ce mode de sécurité prend en charge la transition entre les modes WPA-Personal et WPA2-Personal. Vous disposez peut-être de périphériques clients utilisant WPA-Personal ou WPA2-Personal. Le point d'accès choisira automatiquement l'algorithme de chiffrement utilisé par chaque périphérique client. Pour activer la sécurité WPA2-Personal Mixed sans fil, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Dans le menu déroulant Security Mode, sélectionnez **WPA2-Personal Mixed**.

ÉTAPE 3 Pour activer l'isolation sans fil au sein du SSID, cliquez sur **Enabled**.

ÉTAPE 4 Fournissez les informations suivantes :

- **WPA Algorithms** : (lecture seule) le mode de sécurité WPA2-Personal Mixed choisit automatiquement TKIP ou AES pour le chiffrement des données.

- **Pre-Shared Key** : saisissez une clé partagée WPA comprenant entre 8 et 63 caractères.
- **Key Renewal** : saisissez un délai de renouvellement des clés pour indiquer au point d'accès la fréquence à laquelle il doit modifier les clés de chiffrement. La valeur par défaut est **3600** secondes.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Configuration de WPA-Enterprise

Le mode WPA-Enterprise utilise WPA conjointement à un serveur RADIUS pour l'authentification client.

AVERTISSEMENT Utilisez ce mode uniquement lorsqu'un serveur RADIUS est connecté au point d'accès.

Pour activer la sécurité WPA-Enterprise sans fil, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Dans le menu déroulant Security Mode, sélectionnez **WPA-Enterprise**.

ÉTAPE 3 Pour activer l'isolation sans fil au sein du SSID, cliquez sur **Enabled**.

ÉTAPE 4 Fournissez les informations suivantes :

- **Primary/Backup RADIUS Server** : saisissez l'adresse IP du serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup RADIUS Server Port** : saisissez le numéro de port utilisé par le serveur RADIUS. La valeur par défaut est 1812. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup Shared Secret** : saisissez la clé secrète partagée utilisée par le point d'accès et le serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **WPA Algorithms** : WPA offre deux méthodes de chiffrement pour les données : TKIP et AES. Sélectionnez l'un de ces deux algorithmes dans le menu déroulant. La valeur par défaut est **TKIP**.

- **Key Renewal Timeout** : saisissez un délai de renouvellement des clés pour indiquer au point d'accès la fréquence à laquelle il doit modifier les clés de chiffrement. La valeur par défaut est **3600** secondes.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Configuration de WPA2-Enterprise

Le mode WPA2-Enterprise utilise WPA2 conjointement à un serveur RADIUS pour l'authentification client.

AVERTISSEMENT Utilisez ce mode uniquement lorsqu'un serveur RADIUS est connecté au point d'accès.

Pour activer la sécurité WPA2-Enterprise sans fil, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Dans le menu déroulant Security Mode, sélectionnez **WPA2-Enterprise**.

ÉTAPE 3 Pour activer l'isolation sans fil au sein du SSID, cliquez sur **Enabled**.

ÉTAPE 4 Fournissez les informations suivantes :

- **Primary/Backup RADIUS Server** : saisissez l'adresse IP du serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup RADIUS Server Port** : saisissez le numéro de port utilisé par le serveur RADIUS. La valeur par défaut est 1812. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup Shared Secret** : saisissez la clé secrète partagée utilisée par le point d'accès et le serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **WPA Algorithms** : WPA2 utilise toujours AES pour le chiffrement des données.
- **Key Renewal Timeout** : saisissez un délai de renouvellement des clés pour indiquer au point d'accès la fréquence à laquelle il doit modifier les clés de chiffrement. La valeur par défaut est **3600** secondes.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Configuration de WPA2-Enterprise Mixed

Ce mode de sécurité prend en charge la transition entre les modes WPA-Enterprise et WPA2-Enterprise. Vous disposez peut-être de périphériques clients utilisant WPA-Enterprise ou WPA2-Enterprise. Le point d'accès choisira automatiquement l'algorithme de chiffrement utilisé par chaque périphérique client.

AVERTISSEMENT Utilisez ce mode uniquement lorsqu'un serveur RADIUS est connecté au point d'accès.

Pour activer la sécurité WPA2-Enterprise Mixed sans fil, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Dans le menu déroulant Security Mode, sélectionnez **WPA2-Enterprise Mixed**.

ÉTAPE 3 Pour activer l'isolation sans fil au sein du SSID, cliquez sur **Enabled**.

ÉTAPE 4 Fournissez les informations suivantes :

- **Primary/Backup RADIUS Server** : saisissez l'adresse IP du serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup RADIUS Server Port** : saisissez le numéro de port utilisé par le serveur RADIUS. La valeur par défaut est 1812. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup Shared Secret** : saisissez la clé secrète partagée utilisée par le point d'accès et le serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **WPA Algorithms** : WPA offre deux méthodes de chiffrement pour les données : TKIP et AES. Sélectionnez l'un de ces algorithmes. La valeur par défaut est **TKIP**.
- **Key Renewal Timeout** : saisissez un délai de renouvellement des clés pour indiquer au point d'accès la fréquence à laquelle il doit modifier les clés de chiffrement. La valeur par défaut est **3600** secondes.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Configuration de RADIUS

Cette option utilise un serveur RADIUS pour l'authentification client.

AVERTISSEMENT Utilisez ce mode uniquement lorsqu'un serveur RADIUS est connecté au point d'accès.

Pour activer la sécurité Remote Authentication Dial-In User Service (RADIUS) sans fil, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Dans le menu déroulant Security Mode, sélectionnez **RADIUS**.

ÉTAPE 3 Pour activer l'isolation sans fil au sein du SSID, cliquez sur **Enabled**.

ÉTAPE 4 Fournissez les informations suivantes :

- **Primary/Backup RADIUS Server** : saisissez l'adresse IP du serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup RADIUS Server Port** : saisissez le numéro de port utilisé par le serveur RADIUS. La valeur par défaut est 1812. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup Shared Secret** : saisissez la clé secrète partagée utilisée par le point d'accès et le serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Configuration de WEP

Ce mode de sécurité est défini dans la norme IEEE 802.11 d'origine. Il est désormais déconseillé d'utiliser ce mode, étant donné le faible niveau de protection qu'il offre. Pour améliorer la sécurité, migrez vers WPA ou WPA2.

Pour activer la sécurité Wired Equivalent Privacy (WEP) sans fil, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Security**.

ÉTAPE 2 Dans le menu déroulant Security Mode, sélectionnez **WEP**.

ÉTAPE 3 Pour activer l'isolation sans fil au sein du SSID, cliquez sur **Enabled**.

ÉTAPE 4 Fournissez les informations suivantes :

- **Authentication Type** : choisissez **Open System** ou **Shared Key** comme type d'authentification 802.11. La valeur par défaut est **Open System**.
- **Default Transmit Key** : sélectionnez la clé à utiliser pour le chiffrement des données.
- **WEP Encryption** : sélectionnez un niveau de chiffrement WEP, **64 bits (10 chiffres hexadécimaux)** ou **128 bits (26 chiffres hexadécimaux)**.
- **Passphrase** : pour générer des clés WEP à l'aide d'une phrase secrète, saisissez cette dernière dans le champ Passphrase et cliquez sur **Generate**. Les clés générées automatiquement ne sont pas aussi robustes que les clés WEP manuelles.
- **Key 1-4** : pour créer manuellement des clés WEP, saisissez-les dans les champs Key 1, Key 2, Key 3 et Key 4. Chaque clé WEP peut comporter les lettres « A » à « F » et les chiffres « 0 » à « 9 ». Elle doit contenir 10 caractères pour le chiffrement 64 bits ou 26 caractères pour le chiffrement 128 bits.

ÉTAPE 5 Cliquez sur **Save** (Enregistrer).

Connection Control (Contrôle de la connexion)

La page *Wireless > Connection Control* permet d'autoriser ou d'exclure uniquement les stations de client répertoriées à authentifier avec le point d'accès. Selon la configuration de WAP, le périphérique WAP peut faire référence à une liste de filtrage des adresses MAC stockée sur un serveur RADIUS externe, ou stockée localement sur le périphérique WAP.

Activation du contrôle de connexion local

Pour faire référence à une liste de filtrage d'adresses MAC stockée localement, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless > Connection Control**.

ÉTAPE 2 Cliquez sur **Local**.

Il existe deux façons de contrôler la connexion (association) des périphériques clients sans fil. Vous pouvez **empêcher** des périphériques spécifiques de se connecter au point d'accès, ou vous pouvez **autoriser** uniquement des périphériques clients spécifiques à s'y connecter.

Les périphériques clients sont spécifiés par leur adresse MAC. La valeur par défaut consiste à **autoriser** uniquement des périphériques clients spécifiques.

ÉTAPE 3 Pour ajouter une adresse MAC à la liste de contrôle de connexion, cliquez sur **Wireless Client List**.

Dans la fenêtre qui apparaît, sélectionnez l'adresse MAC à ajouter à la liste.

Vous pouvez également ajouter manuellement des adresses MAC à la liste de contrôle de connexion en saisissant ces adresses dans les champs MAC 01–20.

ÉTAPE 4 Cliquez sur **Save** (Enregistrer).

Activation du contrôle de connexion RADIUS

Pour faire référence à une liste de filtrage d'adresses MAC stockée sur un serveur RADIUS externe, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless > Connection Control**.

ÉTAPE 2 Cliquez sur **RADIUS**.

ÉTAPE 3 Fournissez les informations suivantes :

- **Primary/Backup RADIUS Server** : saisissez l'adresse IP du serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.
- **Primary/Backup RADIUS Server Port** : saisissez le numéro de port utilisé par le serveur RADIUS. La valeur par défaut est 1812. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.

- **Primary/Backup Shared Secret** : saisissez la clé secrète partagée utilisée par le point d'accès et le serveur RADIUS. Le serveur Radius de sauvegarde est utilisé uniquement si le serveur principal n'est pas disponible.

ÉTAPE 4 Cliquez sur **Save** (Enregistrer).

Désactivation du contrôle de connexion

Pour désactiver le contrôle de connexion localement ou sur un serveur RADIUS, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless > Connection Control**.

ÉTAPE 2 Cliquez sur **Disabled**.

ÉTAPE 3 Cliquez sur **Save** (Enregistrer).

Configuration de WPS (configuration protégée par Wi-Fi)

La page *Wireless > Wi-Fi Protected Setup* vous permet de configurer les paramètres WPS (Wi-Fi Protected Setup) pour le point d'accès. WPS a été conçu afin de normaliser les méthodes de configuration de la sécurité sur un réseau sans fil : il suffit de saisir un code PIN (code numérique) ou d'appuyer sur un bouton (Push-Button Configuration ou PBC) dans l'utilitaire Web de configuration du périphérique.

Sur le Cisco WAP4410N, WPS a été désactivé par défaut dans les versions 2.0.5.3 et ultérieures du microprogramme afin d'améliorer la protection de la sécurité. Pour configurer les paramètres WPS sans fil du Cisco WAP4410N, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **Wi-Fi Protected Setup**.

ÉTAPE 2 Configurez les paramètres wi-fi sans fil en procédant selon l'une des trois méthodes suivantes :

1. Un administrateur clique sur le bouton WPS dans la page Wi-Fi Protected Setup pour autoriser un utilisateur à inscrire un client sans fil auprès de Cisco WAP4410N. L'utilisateur doit également cliquer sur le bouton logiciel WPS de son périphérique sans fil (côté client) en même temps que sur le bouton WPS sur le Cisco WAP4410N. La connexion est configurée automatiquement.
2. Il s'agit de l'option la plus sécurisée permettant à un administrateur d'inscrire un client sans fil de l'utilisateur auprès de Cisco WAP4410N. L'utilisateur indique à l'administrateur le code PIN WPS de son périphérique, lequel est indiqué dans l'utilitaire WPS. Après avoir inscrit le code PIN WPS du client, l'administrateur clique sur **Register** pour inscrire l'utilisateur. Puis il clique sur **Save**. L'utilisateur peut ensuite se connecter au Cisco WAP4410N.
3. L'utilisateur saisit le code PIN WPS du Cisco WAP4410N dans le périphérique client à l'aide de tout utilitaire client WPS ou de Microsoft Vista. Le code PIN Cisco WAP4410N est indiqué sur la page Wi-Fi Protected Setup.

VLAN and QoS (Réseau VLAN et qualité de service)

La page *Wireless > VLAN and QoS* vous permet de configurer les paramètres QoS et de réseau VLAN pour le point d'accès.

La fonctionnalité de qualité de service (QoS) vous permet de définir des priorités pour différents types de trafic. Un trafic de faible priorité est ralenti pour permettre un meilleur débit ou un passage plus rapide du trafic de priorité supérieure. La fonctionnalité de VLAN 802.1Q permet de segmenter le trafic depuis différentes sources. Combinée à la fonctionnalité de SSID multiples, elle fournit un outil puissant permettant de contrôler l'accès à votre réseau. Pour configurer les paramètres de QoS et de VLAN sans fil du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Wireless** > **VLAN & QoS**.

ÉTAPE 2 Pour configurer les paramètres de VLAN, procédez comme suit :

REMARQUE Vous pouvez activer cette fonctionnalité uniquement si les concentrateurs/commutateurs sur votre réseau prennent en charge la norme VLAN.

a. Pour activer le VLAN, cliquez sur **Enabled**.

b. Fournissez les informations suivantes :

- **Default VLAN ID** : saisissez l'ID de VLAN par défaut.

- **VLAN Tag** : sélectionnez **Tagged** pour déterminer le VLAN associé à partir de la balise VLAN. La valeur par défaut est **Untagged**.
- **AP Management VLAN** : indiquez l'ID de VLAN utilisé pour la gestion.
- **VLAN Tag over WDS** : sélectionnez **Enabled** ou **Disabled**, selon le cas.

ÉTAPE 3 Pour configurer les paramètres de QoS, saisissez les informations suivantes :

- **VLAN ID** : saisissez l'ID à attribuer au VLAN.
- **Priority** : sélectionnez une priorité dans la liste. Plus cette valeur est élevée, plus la priorité attribuée au périphérique est importante. Par exemple, si vous configurez plusieurs réseaux, vous pouvez attribuer une valeur faible à un réseau visiteurs et une valeur élevée à un réseau privé.
- **WMM** : pour activer WMM, cochez la case correspondante.

  Wi-Fi Multimedia est une fonctionnalité QoS qui a été définie par WiFi Alliance avant que la norme IEEE 802.11e n'ait été finalisée. Elle fait maintenant partie de la norme IEEE 802.11e. Lorsqu'elle est activée, elle fournit quatre files d'attente de priorité pour différents types de trafic. Elle dirige automatiquement les paquets entrants vers les files appropriées en fonction de paramètres QoS (dans les en-têtes IP ou de couche 2). WMM donne la possibilité d'attribuer des priorités au trafic dans votre environnement. La valeur par défaut est **Enabled**.

ÉTAPE 4 Cliquez sur **Save** (Enregistrer).

Advanced Setting (Paramètres avancés)

La page *Wireless > Advanced Settings* vous permet de configurer les paramètres d'équilibrage de charge et de réseau sans fil avancés pour le point d'accès. Le point d'accès utilise plusieurs paramètres permettant d'ajuster la bande passante du canal et de garder des intervalles de sûreté pour améliorer le débit des données. Nous vous recommandons de laisser votre point d'accès ajuster automatiquement ces paramètres pour obtenir un débit maximal.

ÉTAPE 1 Cliquez sur **Wireless** > **Advanced**.

ÉTAPE 2 Dans la section Options, configurez les paramètres avancés suivants (certains uniquement pour le mode sans fil N) de ce point d'accès :

- **Country/Region** : choisissez le pays où vous vous trouvez dans la liste déroulante.

- **Worldwide Mode (802.11d)** : cliquez sur **Enabled** pour activer ce mode. Vos stations sans fil doivent prendre en charge ce mode pour que ce paramètre fonctionne.
- **Channel Bandwidth** : sélectionnez la bande passante du canal pour les connexions sans fil N. Si vous choisissez **20MHz**, seul le canal de 20 MHz est utilisé. Si vous choisissez **40MHz**, les connexions sans fil N utilisent le canal de 40 MHz, mais les connexions sans fil B et sans fil G continuent d'utiliser le canal de **20MHz**. La valeur par défaut est **20MHz**.
- **Guard Interval** : sélectionnez un intervalle de sûreté pour les connexions sans fil N. Les trois options sont **Auto**, **Short (400ns)** et **Long (800ns)**. La valeur par défaut est **Auto**.
- **CTS Protection Mode** : conservez le paramètre par défaut, **Auto**, pour que le point d'accès puisse utiliser cette fonctionnalité si nécessaire, lorsque les produits sans fil N/G ne sont pas capables d'émettre vers le point d'accès dans un environnement à fort trafic 802.11b. Sélectionnez **Disabled** si vous souhaitez désactiver cette fonctionnalité de manière permanente.

  Ce mode renforce la capacité du point d'accès à intercepter l'ensemble des transmissions sans fil, mais diminue gravement les performances.
- **Beacon Interval** : saisissez l'intervalle de fréquence de la balise (20–1000). La valeur par défaut est **100** ms.

  Une balise désigne un paquet diffusé par le point d'accès pour synchroniser le réseau. Cette balise contient la zone de service des réseaux sans fil, l'adresse du point d'accès, les adresses de destination de la diffusion, un horodatage, des cartes DTIM (Delivery Traffic Indicator Maps) et un message TIM (Traffic Indicator Message).
- **DTIM Interval** : saisissez un intervalle de message DTIM (Delivery Traffic Indication Message) compris entre 1 et 255. La valeur par défaut est de **1** intervalle. Cela signifie que le Cisco WAP4410N envoie des messages de diffusion ou multidiffusion à chaque intervalle de balise, si le champ **Beacon Interval** est défini avec la valeur par défaut de 100 ms.

  Des paramètres plus faibles permettent d'optimiser la mise en réseau tout en évitant que votre ordinateur passe en mode économie d'énergie. Des paramètres plus élevés permettent à votre ordinateur de passer en mode veille et d'économiser l'énergie, mais il risque de porter atteinte aux transmissions sans fil.

- **RTS Threshold** : saisissez un seuil RTS (de 1 à 2347).

  Ce paramètre permet de déterminer la taille d'un paquet avant que le point d'accès ne coordonne la transmission et la réception afin de s'assurer de l'efficacité de la communication. Ce paramètre devrait conserver sa valeur par défaut, **2347**. Si vous êtes confronté à un flux de données incohérent, seules des modifications légères sont conseillées.

- **Fragmentation Threshold** : saisissez le paramétrage de votre choix, compris entre 256 et 2346. Nous vous recommandons de ne pas utiliser la fragmentation sauf si vous suspectez la présence d'interférences radio. Les en-têtes supplémentaires appliqués à chaque fragment augmentent les coûts d'exploitation du réseau et peuvent réduire significativement le débit. La valeur recommandée par défaut est de **2346**.

ÉTAPE 3 Dans la section Load Balancing, configurez les paramètres avancés suivants pour ce point d'accès :

- **Load Balancing** : activez cette fonctionnalité pour répartir le travail entre deux ou plusieurs points d'accès afin d'optimiser l'utilisation des ressources, le débit ou le temps de réponse.
- **Utilization Threshold** : saisissez la valeur d'utilisation désirée pour le SSID.
- **Current Utilization** : affiche la valeur en cours de l'utilisation du processeur.

ÉTAPE 4 Cliquez sur **Save** (Enregistrer).

AP Mode (Mode du point d'accès)

La page *AP Mode* affiche les paramètres du mode AP pour le point d'accès. Pour configurer le mode AP du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **AP Mode > AP Mode**.

ÉTAPE 2 Configurez les paramètres du mode AP.

- **Access point** : sélectionnez cette option pour que le périphérique fonctionne comme un point d'accès normal.
  - **Allow Wireless Signal to be repeated by a repeater** : si ce paramètre est sélectionné, le périphérique jouera le rôle de répéteur pour un autre point d'accès. Indiquez les adresses MAC des autres points d'accès dans les champs.
- **Wireless WDS Repeater** : sélectionnez cette option pour que le point d'accès fonctionne comme un répéteur sans fil afin d'étendre la portée radio du point d'accès distant associé, pour surmonter tout obstacle bloquant la communication radio.
  - **Remote Access Point's MAC Address** : saisissez directement l'adresse MAC du point d'accès distant, ou cliquez sur le bouton **Site Survey** pour faire votre choix dans la liste des points d'accès disponibles.
- **Wireless WDS Bridge** : sélectionnez cette option pour que le point d'accès fonctionne comme un pont sans fil afin de réaliser un pontage transparent avec les autres ponts sans fil associés, et d'interdire aux clients ou stations sans fil d'y accéder.
  - **Remote Wireless Bridge's MAC Address** : saisissez les adresses MAC des autres points d'accès dans les champs.
- **Wireless Client/Repeater** : sélectionnez cette option pour que le point d'accès sans fil fonctionne comme un point d'accès client ou répéteur, envoyant l'ensemble du trafic reçu vers un autre point d'accès.
  - **Allow wireless stations to associate** : activez ou désactivez ce paramètre.
  - **Remote access point** : saisissez l'adresse MAC et le SSID du point d'accès désiré ou cliquez sur le bouton **Site Survey** pour choisir le point d'accès parmi les réseaux disponibles.

- **Wireless Monitor** : permet au point d'accès de détecter des points d'accès non autorisés (indésirables) sur votre réseau.
  - **No Security** : cochez cette case pour identifier tout point d'accès dont la sécurité est désactivée en tant que point d'accès indésirable.
  - **Not in Legal AP List** : cochez cette case pour signaler tout point d'accès non répertorié dans la liste des points d'accès autorisés comme étant un point d'accès indésirable. Si vous cochez cette case, vous devez mettre à jour la liste des points d'accès autorisés.
  - **Define Legal AP** : cliquez sur ce bouton pour ouvrir un sous-écran dans lequel vous pouvez modifier la liste des points d'accès autorisés. Cette liste doit contenir tous les points d'accès connus. Vous devez conserver cette liste à jour.

ÉTAPE 3 Cliquez sur **Save** (Enregistrer).

Administration

La section Administration explique comment configurer les paramètres d'administration du point d'accès :

Management (Gestion)

La page *Administration > Management* vous permet de configurer le mot de passe, l'accès Web et les paramètres SNMP. Il est conseillé de changer le nom d'utilisateur/mot de passe contrôlant l'accès à l'utilitaire Web du point d'accès pour empêcher tout accès non autorisé.

Pour modifier les paramètres de gestion du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Administration > Management**.

ÉTAPE 2 Configurez les paramètres de gestion.

- **Local AP Password**
  - **User Name** : modifiez le nom d'utilisateur de l'administrateur. La valeur par défaut est **admin**.

- **AP Password** : modifiez le mot de passe de l'administrateur pour l'utilitaire Web du point d'accès. La valeur par défaut est **admin**.
- **Re-enter to confirm** : confirmez le nouveau mot de passe en le saisissant à nouveau dans ce champ.

- **Web Access** : activez HTTPS pour accroître la sécurité lors de l'accès à l'utilitaire Web. Une fois ce protocole activé, les utilisateurs devront utiliser https:// pour accéder à l'utilitaire Web.
  - **Web HTTPS Access** : activez HTTPS si nécessaire. La valeur par défaut est **Disabled**.
  - **Wireless Web Access** : accordez ou refusez aux clients sans fil l'accès à l'utilitaire Web. La valeur par défaut est **Disabled**.
- **Remote Console** : activez SSH (Secure Shell) pour échanger des données entre deux ordinateurs sur un canal sécurisé.
  - **Secure Shell (SSH)** : activez SSH si nécessaire. La valeur par défaut est **Disabled**.
- **SNMP** : SNMP (Simple Network Management Protocol) est un protocole de gestion et de surveillance du réseau couramment utilisé. Il permet aux administrateurs réseau de surveiller l'état du point d'accès et de recevoir une notification des événements essentiels survenant sur le point d'accès.

  Pour activer la fonctionnalité de prise en charge du protocole SNMP, cliquez sur **Enabled**. Sinon, cliquez sur **Disabled**. La valeur par défaut est **Disabled**.
  - **Contact** : saisissez le nom du contact (par exemple, l'administrateur réseau) du point d'accès.
  - **Device Name** : saisissez le nom que vous souhaitez attribuer au point d'accès.
  - **Location** : saisissez l'emplacement du point d'accès.
  - **Get Community** : saisissez le mot de passe permettant d'accéder en lecture seule aux informations SNMP du point d'accès. La valeur par défaut est **public**.
  - **Set Community** : saisissez le mot de passe permettant d'accéder en lecture-écriture aux informations SNMP du point d'accès. La valeur par défaut est **private**.
  - **SNMP Trap-Community** : saisissez le mot de passe requis par l'ordinateur hôte distant qui recevra des messages ou des notes d'interception envoyés par le point d'accès.

- **SNMP Trusted Host** : vous pouvez restreindre l'accès aux informations SNMP du point d'accès par adresse IP. Saisissez l'adresse IP dans le champ approprié. Si ce champ est laissé vide, l'accès sera autorisé depuis toutes les adresses IP.
- **SNMP Trap-Destination** : saisissez l'adresse IP de l'ordinateur hôte distant qui recevra les messages d'interception.

ÉTAPE 3 Cliquez sur **Save** (Enregistrer).

Log (Journal)

La page *Administration > Log* vous permet de disposer de journaux conservant la trace des activités du point d'accès.

ÉTAPE 1 Cliquez sur **Administration > Log**.

ÉTAPE 2 Configurez les paramètres de journal.

- **Email Alert**
  - **E-Mail Alert** : si vous souhaitez que le point d'accès envoie des e-mails d'alerte dans le cas de certaines attaques, cliquez sur **Enabled**. La valeur par défaut est **Disabled**.
  - **SMTP Server** : saisissez l'adresse ou l'adresse IP du serveur SMTP (Simple Mail Transport Protocol), qui est un serveur de messagerie pour courrier entrant.
  - **E-Mail Address for Logs** : saisissez l'adresse e-mail qui recevra les journaux.
  - **Log Queue Length** : saisissez la longueur du journal que vous recevrez par e-mail. La valeur par défaut est de **20** entrées.
  - **Log Time Threshold** : saisissez la fréquence à laquelle vous recevrez le journal par e-mail. La valeur par défaut est de **600** secondes (10 minutes).
- **Syslog Notification** : Syslog est un protocole standard utilisé pour obtenir des informations sur l'activité du réseau. Le point d'accès prend en charge ce protocole et envoie ses journaux d'activité à un serveur externe. Pour activer Syslog, cliquez sur **Enabled**. La valeur par défaut est **Disabled**.

- **Syslog Server IP Address** : saisissez l'adresse IP du serveur Syslog. En plus du journal d'événements standard, le point d'accès peut envoyer un journal détaillé à un serveur Syslog externe. Le serveur Syslog du point d'accès intercepte toutes les activités du journal et inclut ces informations sur toutes les transmissions de données : l'adresse IP source et de destination, le serveur IP et le nombre d'octets transférés de chaque connexion.

▪ **Log** : sélectionnez les événements que vous souhaitez voir conservés dans un journal par le point d'accès.

- **Unauthorized Login Attempt** : cochez cette case si vous souhaitez recevoir des fichiers journaux d'alertes sur toutes les tentatives de connexion non autorisées.
- **Authorized Login** : cochez cette case pour consigner les connexions autorisées.
- **System Error Messages** : cochez cette case pour consigner les messages d'erreur système.
- **Configuration Changes** : cochez cette case pour consigner tout changement de configuration.
- **View Log** : cochez cette case pour afficher les journaux.

ÉTAPE 3 Cliquez sur **Save** (Enregistrer).

Diagnostics

La page *Administration > Diagnostics* vous permet d'utiliser le point d'accès pour effectuer un test ping. Cette activité peut être utile pour résoudre les problèmes de réseau. Pour effectuer un test ping afin de diagnostiquer les problèmes liés au point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Administration > Diagnostics**.

ÉTAPE 2 Configurez le test ping :

▪ **IP or URL Address** : saisissez l'adresse IP sur laquelle vous souhaitez effectuer le test ping. L'adresse IP peut se trouver sur votre réseau ou sur Internet.

REMARQUE Si l'adresse se trouve sur Internet, et qu'aucune connexion n'existe actuellement, une erreur de délai d'attente risque de se produire. Dans ce cas, attendez quelques secondes avant de faire une nouvelle tentative.

- **Packet Size** : saisissez la taille du paquet.
- **Times to Ping** : sélectionnez dans la liste le nombre de tests Ping à effectuer.
- **Start to Ping** : cochez cette case pour lancer la procédure de test ping.

Factory Default (Valeurs par défaut d'usine)

La page *Administration > Factory Default* vous permet de restaurer les paramètres par défaut définis en usine du point d'accès. Notez les éventuels paramètres personnalisés avant de restaurer les réglages d'usine par défaut. Une fois le point d'accès réinitialisé, vous devrez à nouveau saisir tous les paramètres de votre configuration.

ÉTAPE 1 Cliquez sur **Administration > Factory Default**.

ÉTAPE 2 Cliquez sur **Yes** pour restaurer les paramètres par défaut définis en usine.

ÉTAPE 3 Cliquez sur **Save** (Enregistrer). Votre point d'accès redémarre.

Firmware Upgrade (Mise à niveau du microprogramme)

La page *Administration > Firmware Upgrade* vous permet de mettre à niveau le microprogramme du point d'accès.

AVERTISSEMENT Ne mettez à jour le microprogramme que si vous rencontrez des problèmes avec le point d'accès ou si le nouveau microprogramme contient une fonctionnalité que vous souhaitez utiliser.

AVERTISSEMENT La mise à niveau du microprogramme supprime tous les paramètres personnalisés.

Pour mettre à niveau le microprogramme du point d'accès, procédez comme suit :

ÉTAPE 1 Sauvegardez les paramètres de configuration de vos points d'accès (reportez-vous à « Configuration Management (Gestion des configurations) » page 52).

ÉTAPE 2 Mettez à niveau le microprogramme du point d'accès :

a. Téléchargez le fichier de mise à niveau du microprogramme à l'adresse suivante :

www.cisco.com/en/US/products/ps10052/index.html

b. Extrayez le fichier de mise à niveau du microprogramme.

c. Cliquez sur **Administration > Firmware Upgrade**.

d. Dans le champ File, saisissez l'emplacement du fichier de mise à niveau du microprogramme ou cliquez sur le bouton **Browse** pour localiser le fichier.

e. Cliquez sur **Upgrade** et suivez les instructions qui s'affichent à l'écran.

ÉTAPE 3 Saisissez à nouveau l'ensemble de vos paramètres de configuration personnalisés.

Reboot (Redémarrer)

La page *Administration > Reboot* vous permet de redémarrer le point d'accès. Pour redémarrer le point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Administration > Reboot**.

ÉTAPE 2 Dans le champ Device Reboot, cliquez sur **Yes**.

ÉTAPE 3 Cliquez sur **Save** (Enregistrer).

Configuration Management (Gestion des configurations)

La page *Administration > Configuration Management* vous permet de créer un fichier de configuration de sauvegarde ou de télécharger un fichier de configuration vers le point d'accès. Pour gérer la configuration du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Administration > Configuration Management**.

ÉTAPE 2 Pour créer un fichier de configuration de sauvegarde, cliquez sur **Save Configuration to File** et suivez les instructions qui s'affichent à l'écran.

ÉTAPE 3 Pour restaurer la configuration de votre point d'accès, procédez comme suit :

a. Assurez-vous que le fichier de configuration du point d'accès se trouve sur votre ordinateur.

b. Dans le champ **Restore Configuration**, saisissez l'emplacement du fichier de configuration ou cliquez sur **Browse** et localisez le fichier de configuration.

c. Cliquez sur **Load**.

SSL Certification Management (Gestion de la certification SSL)

Pour générer le certificat avec le périphérique WAP, cliquez sur **Export Certificate.** 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.

S'il existe un certificat SSL (avec une extension .pem) sur le périphérique WAP, vous pouvez l'installer sur votre ordinateur en tant que sauvegarde. Accédez au fichier du certificat et cliquez sur **Install Certificate**.

Status (État)

La section Status explique comment modifier les paramètres d'état du point d'accès :

Local Network (Réseau local)

La page *Status > Local Network* affiche des informations sur l'état actuel du point d'accès pour le réseau local. Pour vérifier l'état du réseau local, procédez comme suit :

ÉTAPE 1 Cliquez sur **Status > Local Network**.

Cette page affiche des informations sur l'état de votre point d'accès :

- **PID VID** : version et modèle matériel WAP.
- **Software Version** : version du logiciel actuel du point d'accès.
- **Local MAC Address** : adresse MAC de l'interface du réseau local du point d'accès.
- **System Up Time** : durée d'exécution du point d'accès.

▪ **Local Network (Réseau local)**

- **IP Address** : adresse IP du point d'accès telle qu'elle apparaît sur votre réseau local.
- **Subnet Mask** : masque de sous-réseau du point d'accès.
- **Default Gateway** : adresse IP de votre passerelle ou routeur. Valeur utilisée par d'autres périphériques sur votre LAN.
- **Primary DNS** : adresse IP de votre serveur DNS principal.
- **Secondary DNS** : adresse IP de votre serveur DNS secondaire.

ÉTAPE 2 Pour mettre à jour les informations d'état, cliquez sur **Refresh**.

Wireless (paquets d'erreurs fil)

La page *Status > Wireless* affiche des informations sur l'état actuel du point d'accès pour le réseau sans fil. Pour vérifier l'état du réseau sans fil du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Status > Wireless**.

Cette page affiche l'état du réseau sans fil :

- **Mode** : mode du réseau sans fil du point d'accès.
- **Channel** : paramètre de canal du point d'accès.
- **SSID 1–4 MAC Address** : adresse MAC de l'interface sans fil du point d'accès.
- **SSID 1–4** : SSID du point d'accès.
- **VLAN Trunk** : état de la liaison VLAN du point d'accès.
- **Priority Setting** : paramètre de priorité en cours.
- **SSID 1–4 Security Mode** : mode de sécurité du SSID.
- **SSID 1–4 Priority** : état de la priorité du SSID.

ÉTAPE 2 Pour mettre à jour les informations d'état du réseau sans fil, cliquez sur **Refresh**.

System Performance (Performances du système)

La page *Status > System Performance* affiche les informations d'état du point d'accès concernant ses transmissions de données et paramètres en cours. Pour vérifier les performances système du point d'accès, procédez comme suit :

ÉTAPE 1 Cliquez sur **Status > System Performance**.

Cette page affiche les valeurs des performances système du point d'accès :

- **Wired** : statistiques du réseau filaire.
  - **IP Address** : adresse IP locale du point d'accès.
  - **MAC Address** : adresse MAC de l'interface filaire du point d'accès.
  - **Connection** : état de la connexion du point d'accès pour le réseau filaire.
  - **Packets Received** : nombre de paquets reçus.
  - **Packets Sent** : nombre de paquets envoyés.
  - **Bytes Received** : nombre d'octets reçus.
  - **Bytes Sent** : nombre d'octets envoyés.
  - **Error Packets Received** : nombre de paquets d'erreurs reçus.
  - **Drop Received Packets** : nombre de paquets rejetés après leur réception.
- **Wireless** : statistiques du réseau sans fil.
  - **Name** : réseau sans fil/SSID auxquels les statistiques font référence.
  - **IP Address** : adresse IP locale du point d'accès.
  - **MAC Address** : adresse MAC de l'interface sans fil du point d'accès.
  - **Connection** : état des réseaux sans fil du point d'accès.
  - **Packets Received** : nombre de paquets reçus pour chaque réseau sans fil.
  - **Packets Sent** : nombre de paquets envoyés pour chaque réseau sans fil.
  - **Bytes Received** : nombre d'octets reçus pour chaque réseau sans fil.
  - **Bytes Sent** : nombre d'octets envoyés pour chaque réseau sans fil.

- **Error Packets Received** : nombre de paquets d'erreurs reçus pour chaque réseau sans fil.
- **Drop Received Packets** : nombre de paquets rejetés après leur réception.

ÉTAPE 2 Pour mettre à jour les informations d'état des performances système, cliquez sur **Refresh**.

A

Dépannage

Cette annexe propose des solutions à certains problèmes susceptibles de survenir lors de l'installation et de l'utilisation du point d'accès Cisco WAP4410N.

Les explications ci-dessous vous aideront à résoudre les problèmes que vous rencontrez. Si vous ne trouvez pas la solution à votre problème, consultez le site Web Cisco.com à l'adresse www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html.

Foire aux questions

Q. Le point d'accès peut-il être utilisé en tant que serveur DHCP ?

Non. Le point d'accès n'est rien d'autre qu'un concentrateur sans fil et de ce fait, il ne peut pas être configuré pour prendre en charge les fonctionnalités DHCP.

Q. Puis-je exécuter une application à partir d'un ordinateur distant, sur le réseau sans fil ?

Cela dépend si votre application est conçue ou non pour une utilisation en réseau. Consultez la documentation de l'application pour déterminer si elle prend en charge le fonctionnement en réseau.

Q. Puis-je m'adonner à des jeux multi-joueurs avec d'autres utilisateurs du réseau sans fil ?

Oui, si le jeu accepte le mode multi-joueurs sur un réseau local (LAN). Reportez-vous à la documentation du jeu en question pour obtenir plus d'informations.

Q. Le point d'accès peut-il fonctionner avec un client Centrino ?

Oui. Cependant, un client Centrino peut ne prendre en charge que les canaux de 20 MHz. Le débit maximal avec ce client sera donc inférieur à 130 Mbit/s.

Q. Qu'est-ce que la norme IEEE 802.11b ?

Il s'agit de l'une des normes IEEE appliquées aux réseaux sans fil. La norme 802.11b permet à des périphériques réseau sans fil de différentes marques de communiquer entre eux, à condition qu'ils soient conformes à cette norme. La norme 802.11b établit un débit de transfert de données maximal de 11 Mbit/s et une fréquence de fonctionnement de 2,4 GHz.

Q. Qu'est-ce que la norme IEEE 802.11g ?

Il s'agit de l'une des normes IEEE appliquées aux réseaux sans fil. La norme 802.11g permet à des périphériques réseau sans fil de différentes marques de communiquer entre eux, à condition qu'ils soient conformes à cette norme. La norme 802.11g établit un débit de transfert de données maximal de 54 Mbit/s et une fréquence de fonctionnement de 2,4 GHz.

Q. Qu'est-ce que le projet de norme IEEE 802.11n ?

Il s'agit de l'une des normes IEEE des réseaux sans fil en cours de finalisation. La norme 802.11n permet à des périphériques réseau sans fil de différentes marques de communiquer entre eux, à condition qu'ils soient conformes à cette norme. La norme 802.11n établit un débit de transfert des données maximal de 600 Mbit/s et une fréquence de fonctionnement de 2,4 GHz ou 5 GHz.

Q. Quelles sont les fonctionnalités IPv6 prises en charge ?

Le point d'accès Cisco WAP4410N prend en charge les fonctionnalités IPv6 suivantes :

- Découverte du MTU de chemin (RFC1981)
- Protocole Internet v6 -IPv6 (RFC2460)
- Découverte des voisins IPv6 (ND) (RFC2461)
- Configuration automatique des adresses sans état IPv6 (RFC2462)
- ICMPv6 : protocole des messages de commande Internet v6 ICMPv6 (RFC2643)
- Architecture d'adresses IPv6 (RFC3513)
- Sélection de l'adresse par défaut (RFC3484)
- Transmission de paquets IPv6 sur réseaux Ethernet (RFC 2464)
- Nœud IPv6 - (RFC4294)
- Double pile IPv4/IPv6 : accès simultané à partir des clients IPv4 et IPv6.

Le point d'accès Cisco WAP4410N prend en charge les applications IPv6 suivantes :

- WEB/SSL
- SNTP
- PING6
- Routage TRACE

Q. Qu'est-ce que l'itinérance ?

L'itinérance consiste, pour l'utilisateur d'un ordinateur portable, à continuer de communiquer tout en se déplaçant librement dans une zone plus vaste que celle couverte par un point d'accès donné. Avant d'utiliser la fonction d'itinérance, la station de travail doit s'assurer que le numéro de canal est identique à celui du point d'accès de la zone de couverture dédiée.

Pour garantir une connectivité transparente, le réseau local (LAN) sans fil doit incorporer différentes fonctions. Ainsi, chaque nœud et chaque point d'accès doivent systématiquement accuser réception de chacun des messages. Chaque nœud doit maintenir le contact avec le réseau sans fil, même en l'absence de transmission de données.

L'application simultanée de ces fonctions requiert une technologie de mise en réseau RF dynamique qui relie les points d'accès et les nœuds. Dans ce système, le nœud final de l'utilisateur recherche le meilleur accès possible au système. Il évalue tout d'abord les facteurs tels que la puissance et la qualité du signal, ainsi que la charge de messages supportée par chaque point d'accès et la distance entre chaque point d'accès et le réseau fédérateur câblé. Sur la base de ces informations, le nœud sélectionne ensuite le point d'accès correct et enregistre son adresse.

Les communications entre le nœud final et l'ordinateur hôte peuvent alors s'effectuer dans les deux sens avec le réseau fédérateur.

Lorsque l'utilisateur se déplace, l'émetteur RF du nœud final vérifie régulièrement le système afin de déterminer s'il est en contact avec le point d'accès d'origine ou s'il doit en rechercher un autre. Lorsqu'un nœud ne reçoit plus de confirmation de son point d'accès d'origine, il entreprend une nouvelle recherche. Une fois un nouveau point d'accès trouvé, il l'enregistre à nouveau et le processus de communication se poursuit.

Q. Qu'est-ce que la bande ISM ?

La FCC et ses homologues internationaux ont défini une bande passante supplémentaire destinée à une utilisation hors licence : la bande ISM (destinée aux applications industrielles, scientifiques et médicales).

Le spectre situé aux alentours de 2,4 GHz est disponible dans le monde entier. Il s'agit de la possibilité sans précédent de mettre à la disposition des utilisateurs du monde entier un système haut débit sans fil.

Q. Qu'est-ce que la technologie d'étalement du spectre ?

La technologie d'étalement du spectre est une technique hautes fréquences à large bande développée par l'armée pour disposer d'un système fiable et sécurisé de transmission des communications jugées sensibles. Elle est conçue pour optimiser l'efficacité de la bande passante pour plus de fiabilité, d'intégrité et de sécurité.

En d'autres termes, ce système utilise plus de bande passante que la transmission à bande étroite. Cependant, l'optimisation produit un signal qui, dans les faits, est plus important et donc plus facile à détecter, pourvu que le récepteur connaisse les paramètres du signal d'étalement du spectre transmis. Si un récepteur n'est pas réglé sur la bonne fréquence, le signal d'étalement du spectre est perçu comme un bruit de fond.

Il existe deux systèmes principaux : DSSS (Direct Sequence Spread Spectrum) et FHSS (Frequency Hopping Spread Spectrum).

Q. Qu'est-ce que DSSS ? Qu'est-ce que FHSS ? Et quelles sont leurs différences ?

Le système FHSS (Frequency-Hopping Spread-Spectrum) utilise une porteuse à bande étroite qui modifie la fréquence en un modèle connu à la fois de l'émetteur et du récepteur.

S'il est synchronisé correctement, l'effet immédiat est le maintien d'un canal logique unique. Pour un récepteur non concerné, le signal FHSS ressemble à un bruit à impulsions courtes. Le système DSSS (Direct-Sequence Spread-Spectrum) génère un modèle de bit redondant pour chaque bit transmis. Pour ce modèle de bit, on parlera alors de hachage.

Plus la partie hachée est longue, plus la probabilité de récupérer les données d'origine est grande. Même si une ou plusieurs parties hachées sont endommagées au cours de la transmission, les techniques statistiques intégrées à la radio peuvent récupérer les données d'origine sans avoir à les retransmettre.

Pour un récepteur non concerné, le signal DSSS apparaît comme un faible bruit de transmission à large bande et est rejeté (ignoré) par la plupart des récepteurs à bande étroite.

Q. Les informations sont-elles interceptées lors de la transmission sur les ondes ?

Un réseau local sans fil offre deux types de protection. Sur le matériel, il offre une sécurité inhérente de cryptage via la technologie DSSS (Direct Sequence Spread Spectrum). Au niveau logiciel, il offre différentes méthodes de sécurité sans fil pour améliorer la sécurité et le contrôle d'accès. Les utilisateurs les configurent en fonction de leurs besoins.

Q. Les produits sans fil Cisco prennent-ils en charge le partage des fichiers et des imprimantes ?

Les produits Cisco sans fil remplissent les mêmes fonctions que les produits des réseaux locaux. Les produits Cisco sans fil peuvent ainsi fonctionner avec les systèmes d'exploitation NetWare, Windows NT/2000 ou d'autres systèmes d'exploitation de réseaux locaux pour prendre en charge le partage des imprimantes ou des fichiers.

Q. Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est un numéro unique affecté à tout périphérique réseau Ethernet, tel qu'un adaptateur réseau, par son constructeur, et qui permet au réseau d'identifier ce périphérique au niveau matériel. Pour des raisons de simplicité d'utilisation, ce numéro est généralement permanent. À la différence des adresses IP qui peuvent changer dès qu'un ordinateur se connecte au réseau, l'adresse MAC d'un périphérique reste identique, ce qui en fait un identifiant réseau particulièrement fiable.

Q. Comment éviter les interférences ?

L'utilisation de plusieurs points d'accès sur le même canal, proches les uns des autres, peut générer des interférences. Lorsque vous utilisez plusieurs points d'accès, assurez-vous de faire fonctionner chacun sur un canal (une fréquence) différent.

Q. Comment puis-je réinitialiser le point d'accès ?

Appuyez pendant environ 10 secondes sur le bouton Reset situé à l'arrière du point d'accès. Les paramètres par défaut sont réinitialisés.

Q. Comment puis-je résoudre les problèmes liés à une perte de signal ?

Il n'est pas possible de connaître l'étendue exacte de votre réseau sans fil sans le tester. Chaque obstacle rencontré entre le point d'accès et un ordinateur sans fil génère une perte de signal. Le verre au plomb, le métal, les planchers en béton, l'eau et les murs inhibent le signal et réduisent la portée. Placez tout d'abord le point d'accès et votre ordinateur sans fil dans la même pièce et déplacez-le progressivement afin d'évaluer l'étendue maximale dans votre environnement.

Vous pouvez également essayer d'utiliser différents canaux et éliminer ainsi les interférences liées à un canal unique. Ouvrez l'utilitaire Web de votre point d'accès, cliquez sur **Wireless** > **Advanced Wireless** et assurez-vous que la puissance de sortie est réglée sur 100 %.

Q. Le point d'accès fait-il office de pare-feu ?

Non. Le point d'accès n'est qu'un pont entre les clients Ethernet câblés et les clients sans fil.

Q. Mon signal est excellent, mais mon réseau n'apparaît pas.

Une fonction de sécurité sans fil, telle que WEP ou WPA, est probablement activée sur le point d'accès, mais pas sur votre adaptateur sans fil (ou vice versa). Vérifiez que tous les périphériques de votre réseau sans fil utilisent les mêmes paramètres de sécurité.

Q. Quel est le nombre maximal d'utilisateurs gérables par le point d'accès ?

Pas plus de 63, mais cela dépend du volume de données. Ce nombre pourra être inférieur si plusieurs utilisateurs génèrent un trafic réseau important.

Q. Comment définir plusieurs points d'accès Cisco WAP4410N avec la même configuration ?

ÉTAPE 1 Configurez un point d'accès, puis enregistrez le fichier de configuration par le biais de sa page Web.

ÉTAPE 2 À l'aide d'un éditeur de texte, remplacez la commande « `secret_shown=1` » par « `secret_shown=0` » dans le fichier de configuration et enregistrez le fichier.

ÉTAPE 3 Restaurez le fichier sur le point d'accès via sa page Web et enregistrez la configuration en le nommant `AP_Config.cfg`.

ÉTAPE 4 À ce stade, toutes les clés et tous les mots de passe s'affichent en texte clair.

ÉTAPE 5 Restaurez le fichier `AP_config.cfg` sur un autre point d'accès via sa page Web.

Aide Windows

La plupart des produits sans fil exigent l'utilisation de Microsoft Windows. Windows propose différentes fonctionnalités qui facilitent la mise en réseau. Vous pouvez accéder à ces fonctionnalités à partir de l'aide de Windows. Elles sont décrites dans la présente annexe.

TCP/IP

Pour qu'un ordinateur puisse communiquer avec le point d'accès, vous devez au préalable activer le protocole TCP/IP. TCP/IP désigne un ensemble d'instructions (ou protocole) que tous les ordinateurs suivent pour communiquer sur un réseau. Il s'applique aussi dans le cadre des réseaux sans fil. Vos ordinateurs ne pourront pas exploiter les capacités de votre réseau sans fil si le protocole TCP/IP n'est pas activé. L'aide de Windows fournit des instructions exhaustives sur l'activation du protocole TCP/IP.

Ressources partagées

Si vous souhaitez partager des imprimantes, des dossiers ou des fichiers sur votre réseau, l'aide de Windows offre également des instructions complètes sur l'utilisation des ressources partagées.

Voisinage réseau/Favoris réseau

En fonction de la version de Windows que vous utilisez, d'autres ordinateurs de votre réseau peuvent apparaître dans le Voisinage réseau ou dans les Favoris réseau. Là encore, l'aide de Windows fournit des instructions expliquant comment ajouter des ordinateurs à votre réseau.

B

Pour en savoir plus

Cisco propose une vaste gamme de ressources pour vous aider à tirer pleinement parti du point d'accès sans fil N Cisco WAP4410N avec Power over Ethernet.

Assistance	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Ressources et assistance Cisco Small Business	www.Cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Téléchargements de microprogrammes Cisco Small Business	www.cisco.com/go/smallbizfirmware Sélectionnez un lien pour télécharger le microprogramme d'un produit Cisco Small Business. Aucune connexion n'est requise. Les téléchargements se rapportant à tous les autres produits Cisco Small Business, notamment aux unités de stockage réseau, sont disponibles dans la zone de téléchargement de Cisco.com, à l'adresse www.cisco.com/go/software (enregistrement/ouverture de session requis).
Requêtes Open Source Cisco Small Business	www.cisco.com/go/smallbiz_opensource_request
Documentation sur les produits	
Documentation relative à Cisco WAP4410N	www.cisco.com/en/US/products/ps10047/tsd_products_support_series_home.html
RCSI	http://www.cisco.com/en/US/docs/routers/csbr/rcsi/78-19314.pdf

Cisco Small Business	
Site Cisco Partner Central pour les petites entreprises (connexion partenaire requise)	www.Cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.Cisco.com/smb