283935

GUIDE D'ADMINISTRATION

Cisco Small Business

Point d'accès WAP121 Wireless-N avec technologie PoE

et

Point d'accès WAP321 Wireless-N à sélection de bande avec technologie PoE

78-20373-02

Table des matières

Chapitre 1 : Démarrage 7

Démarrage de l'utilitaire de configuration Web 7

Lancement de l'utilitaire de configuration Web 8

Déconnexion 9

Utilisation de l'assistant d'installation de point d'accès 9

Mise en route 12

Navigation dans les fenêtres 13

En-tête de l'utilitaire de configuration 13

Volet de navigation 14

Boutons de gestion 14

Chapitre 2 : État et statistiques 16

Récapitulatif système 16

Interfaces réseau 18

Statistiques de trafic 19

Transmission/Réception de pont de groupe de travail 20

Clients associés 21

Associations de client TSPEC 22

État et statistiques TSPEC 24

Statistiques de point d'accès TSPEC 26

Statistiques sur la radio 27

État des alertes par e-mail 28

Journal 29

Chapitre 3 : Administration 30

Paramètres système 31

Comptes d'utilisateurs 31

Ajout d'un utilisateur 32

Modification d'un mot de passe utilisateur 33

Paramètres de l'heure 33

Paramètres des journaux 35
Configuration du journal persistant 35
Serveur de journalisation distant 36
Alertes par e-mail 38
Exemples d'alertes par e-mail 40
Service HTTP/HTTPS 41
Configuration des services HTTP et HTTPS 41
Gestion des certificats SSL 42
Management Access Control 43
Mise à niveau du micrologiciel 44
Mise à niveau TFTP 45
Mise à niveau HTTP 46
Mise à niveau du micrologiciel 46
Téléchargement/sauvegarde du fichier de configuration 48
Sauvegarde d'un fichier de configuration 49
Téléchargement d'un fichier de configuration 50
Propriétés des fichiers de configuration 51
Copie/enregistrement de la configuration 51
Redémarrage 52
Discovery—Bonjour 53
Capture de paquets 54
Configuration de la capture de paquets 55
Capture locale de paquets 56
Capture distante de paquets 57
Téléchargement du fichier de capture de paquets 60
Informations de support 61

Chapitre 4 : Réseau local 62

Paramètres de port 62
Paramètres d'adresse VLAN et IPv4 63
Adresses IPv6 65

Chapitre 5 : Sans fil 67

Radio 67

Détection de point d'accès non autorisé 76

Affichage de la Rogue AP List 76

Création et enregistrement d'une Trusted AP List 78

Importation d'une Trusted AP List 79

Networks 80

Conventions d'affectation de noms SSID 80

ID de VLAN 81

Configuration des VAP 81

Définition des paramètres de sécurité 84

None (Plain-text) 84

Static WEP 84

Dynamic WEP 87

WPA Personal 89

WPA Enterprise 91

Planificateur 93

Ajout de profils de planificateur 94

Configuration des règles de planificateur 94

Association de planificateur 96

Utilisation de la bande passante 96

Filtrage MAC 97

Configuration d'une liste de filtrage MAC stockée localement sur le périphérique WAP 97

Configuration de l'authentification MAC sur le serveur RADIUS 98

Pont WDS 99

WEP sur les liaisons WDS 101

WPA/PSK sur les liaisons WDS 102

Pont de groupe de travail 102

Qualité de service 106

Configuration de WPS 109

Vue d'ensemble du protocole WPS 109

Scénarios d'utilisation 110
Rôles WPS 111
Activation et désactivation de WPS sur un VAP. 111
Enregistrement externe et interne 112
Inscription de client 112
Utilisation facultative du registre intégré 113
Fonctionnalité de verrouillage 113
Modifications apportées à la configuration du VAP 114
Enregistrement externe 115
Fonctionnement exclusif des transactions WPS 115
Compatibilité descendante avec WPS version 1.0 115
Définition des paramètres WPS 116
Instance Status 117
Processus WPS 118
Inscription d'un client à l'aide de la méthode PIN 118
Inscription d'un client à l'aide de la méthode PBC 119
Affichage des informations d'état de l'instance 120
Affichage des informations de résumé de l'instance 120

Chapitre 6 : Sécurité du système 121

Serveur RADIUS 121
Demandeur 802.1X 123
Complexité des mots de passe 125
Complexité WPA-PSK 126

Chapitre 7 : Qualité de service (QoS) de client 128

Paramètres globaux relatifs à la QoS de client 128
ACL 129
ACL IPv4 et IPv6 129
ACL MAC 129
Configuration des ACL 129
Mappage de classe 137
Ajout d'un mappage de classe 137
Définition d'un mappage de classe 138

Mappage de stratégie 142
Association de la QoS de client 144
État de la QoS de client 146

Chapitre 8 : Protocole SNMP (Simple Network Management Protocol, Protocole de gestion de réseau simple) 149

Présentation de SNMP 149
Paramètres généraux de SNMP 150
Vues 153
Groupes 154
Utilisateurs 156
Cibles 158

Chapitre 9 : Portail captif 159

Configuration globale de portail captif 160
Configuration d'instance 161
Association d'instance 165
Personnalisation de portail Web 165
Chargement et suppression d'images 168
Groupes locaux 170
Utilisateurs locaux 170
Clients authentifiés 172
Clients dont l'authentification a échoué 173

Chapitre 10 : Configuration de point unique 175

Présentation de la configuration de point unique 175
Gestion de la configuration de point unique sur les périphériques WAP 176
Négociation de la configuration de point unique 177
Fonctionnement d'un périphérique WAP exclu d'une configuration de point unique 178
Propagation des paramètres de configuration dans une configuration de point unique 178

Points d'accès 180
Configuration du périphérique WAP pour la configuration de point unique 181
Affichage des informations de la configuration de point unique 182
Ajout d'un nouveau point d'accès à un cluster à configuration de point unique 183
Suppression d'un point d'accès d'un cluster à configuration de point unique 183
Accès aux informations de configuration d'un périphérique WAP spécifique 184
Accès à un périphérique WAP à l'aide de son adresse IP dans une URL 184
Sessions 184
Gestion des canaux 186
Affichage des attributions de canaux et configuration des verrouillages 187
Tableau Current Channel Assignments 188
Tableau Proposed Channel Assignments 188
Configuration des paramètres avancés 189
Voisinage sans fil 190
Affichage des détails d'un membre du cluster 192

Annexe A : Codes des motifs des messages de désauthentification 193

Annexe B : Pour en savoir plus 195

1

Démarrage

Ce chapitre offre une introduction à l'utilitaire de configuration Web des périphériques WAP (Wireless Access Point) et inclut les rubriques suivantes :

- **Démarrage de l'utilitaire de configuration Web**
- **Utilisation de l'assistant d'installation de point d'accès**
- **Mise en route**
- **Navigation dans les fenêtres**

Démarrage de l'utilitaire de configuration Web

Cette section décrit la configuration système requise ainsi que la manière de se déplacer dans l'utilitaire de configuration Web.

Navigateurs pris en charge

- Internet Explorer 7.0 ou version ultérieure
- Chrome 5.0 ou version ultérieure
- Firefox 3.0 ou version ultérieure
- Safari 3.0 ou version ultérieure

Restrictions s'appliquant aux navigateurs

- Si vous utilisez Internet Explorer 6, vous ne pouvez pas utiliser directement une adresse IPv6 pour accéder au Périphérique WAP. Vous pouvez néanmoins utiliser le serveur DNS (Domain Name System, système de noms de domaine) pour créer un nom de domaine contenant l'adresse IPv6, puis utiliser ce nom de domaine dans la barre d'adresse à la place de l'adresse IPv6.

- Si vous utilisez Internet Explorer 8, vous pouvez configurer les paramètres de sécurité à partir d'Internet Explorer. Sélectionnez **Outils > Options Internet**, puis sélectionnez l'onglet **Sécurité**. Sélectionnez **Intranet local**, puis **Sites**. Sélectionnez **Avancé**, puis **Ajouter**. Ajoutez l'adresse Intranet du Périphérique WAP (http://*<adresse-ip>*) dans la zone Intranet locale. L'adresse IP peut également être spécifiée en tant qu'adresse IP du sous-réseau, afin que toutes les adresses du sous-réseau soient ajoutées à la zone Intranet locale.
- Si vous disposez de plusieurs interfaces IPv6 sur votre station de gestion, utilisez l'adresse globale IPv6 au lieu de l'adresse locale IPv6 pour accéder au Périphérique WAP à partir de votre navigateur.

Lancement de l'utilitaire de configuration Web

Pour ouvrir l'utilitaire de configuration :

ÉTAPE 1 Ouvrez un navigateur Web.

Saisissez l'adresse IP du Périphérique WAP que vous configurez dans la barre d'adresse du navigateur, puis appuyez sur **Entrée**. La page *Connexion* s'ouvre.

- Vous pouvez utiliser l'utilitaire Cisco FindIT Network Discovery Utility pour trouver votre adresse IP. Cet outil vous permet de détecter automatiquement tous les périphériques Cisco Small Business pris en charge dans le même segment de réseau local que votre ordinateur. Pour plus d'informations, accédez à cisco.com et visitez la page www.cisco.com/go/findit.
- Pour obtenir des instructions supplémentaires sur la manière de rechercher l'adresse IP de votre périphérique WAP, reportez-vous au Guide de démarrage rapide du périphérique WAP.

ÉTAPE 2 Entrez le nom d'utilisateur et le mot de passe. Le nom d'utilisateur définit en usine est **cisco**, et le mot de passe par défaut **cisco**.

ÉTAPE 3 Cliquez sur **Se connecter**. La page Access Point Setup Wizard s'ouvre.

S'il s'agit de votre première ouverture de session avec le nom d'utilisateur par défaut (**cisco**) et le mot de passe par défaut (**cisco**), ou si votre mot de passe a expiré, la page *Modifier le mot de passe Administrateur* s'ouvre. Saisissez le nouveau mot de passe, confirmez-le, cliquez sur **Appliquer**, puis sur **Fermer**. Le nouveau mot de passe est enregistré. Saisissez ensuite le nom d'utilisateur **cisco** ainsi que le nouveau mot de passe sur la page *Connexion*.

Voir **Utilisation de l'assistant d'installation de point d'accès** pour obtenir des instructions sur l'utilisation de l'assistant.

Déconnexion

Par défaut, l'utilitaire de configuration se déconnecte au bout de 10 minutes d'inactivité. Consultez la section **Service HTTP/HTTPS** pour obtenir des instructions sur la modification du délai d'expiration par défaut.

Pour vous déconnecter, cliquez sur **Se déconnecter** en haut à droite de l'utilitaire de configuration.

Utilisation de l'assistant d'installation de point d'accès

La première fois que vous vous connectez au Périphérique WAP (ou après une réinitialisation aux paramètres d'usine par défaut), l'assistant d'installation de point d'accès apparaît afin de vous aider à effectuer les configurations initiales. Procédez comme suit pour exécuter l'assistant :

REMARQUE Si vous cliquez sur **Annuler** pour ignorer l'assistant, la page Change Password apparaît. Vous pouvez alors modifier le mot de passe de connexion par défaut. Pour l'ensemble des autres paramètres, les configurations d'usine par défaut s'appliquent.

Vous devrez vous reconnecter après avoir modifié votre mot de passe.

ÉTAPE 1 Cliquez sur **Suivant** dans la page d'accueil de l'assistant. La fenêtre Configure Device - IP Address apparaît.

ÉTAPE 2 Cliquez sur **Dynamic IP Address (DHCP)** si vous voulez que le périphérique WAP reçoive une adresse IP d'un serveur DHCP. Sinon, sélectionnez **Static IP Address** pour configurer manuellement l'adresse IP. Pour obtenir une description de ces champs, reportez-vous à **Paramètres d'adresse VLAN et IPv4**.

ÉTAPE 3 Cliquez sur **Suivant**. La fenêtre Single Point Setup - Set a Cluster apparaît. Pour obtenir une description de la configuration de point unique, reportez-vous à **Configuration de point unique**.

ÉTAPE 4 Pour créer une nouvelle configuration de point unique de périphériques WAP, sélectionnez **Créer un nouveau cluster** et spécifiez un **Nouveau nom de cluster**. Si vous configurez vos périphériques avec le même nom de cluster et que vous activez le mode de configuration de point unique sur d'autres périphériques WAP, ils rejoignent automatiquement le groupe.

Si votre réseau possède déjà un cluster, vous pouvez lui ajouter ce périphérique en cliquant sur **Rejoindre un cluster existant**, puis en saisissant le **Nom du cluster existant**.

Si vous ne voulez pas que ce périphérique participe à la configuration de point unique pour le moment, cliquez sur **Ne pas activer la configuration de point unique**.

(Facultatif) Vous pouvez entrer du texte dans le champ AP Location pour noter l'emplacement physique du périphérique WAP.

ÉTAPE 5 Cliquez sur **Suivant**. La fenêtre Configure Device - Set System Date and Time apparaît.

ÉTAPE 6 Sélectionnez votre fuseau horaire, puis réglez l'heure système manuellement ou configurez le périphérique WAP de telle sorte qu'il obtienne l'heure à partir d'un serveur NTP. Pour obtenir une description de ces options, reportez-vous à **Paramètres de l'heure**.

ÉTAPE 7 Cliquez sur **Suivant**. La fenêtre Enable Security - Set Password apparaît.

ÉTAPE 8 Saisissez un **Nouveau mot de passe** et saisissez-le à nouveau dans la zone de texte **Confirmer le mot de passe**. Pour obtenir plus d'informations sur les mots de passe, reportez-vous à **Comptes d'utilisateurs**.

> **REMARQUE** Vous pouvez désactiver la case à cocher Password Complexity si vous souhaitez désactiver les règles de sécurité de mot de passe. Nous vous recommandons toutefois fortement de conserver les règles de sécurité de mot de passe activées.

ÉTAPE 9 Cliquez sur **Suivant**. La fenêtre Enable Security - Name Your Wireless Network apparaît .

ÉTAPE 10 Saisissez un **Nom de réseau**. Ce nom fait office de SSID pour le réseau sans fil par défaut.

ÉTAPE 11 Cliquez sur **Suivant**. La fenêtre Enable Security - Secure Your Wireless Network apparaît.

ÉTAPE 12 Choisissez un type de cryptage de sécurité et entrez une clé de sécurité. Pour obtenir une description de ces options, reportez-vous à **Sécurité du système**.

ÉTAPE 13 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Enable Security - Assign the VLAN ID For Your Wireless Network.

ÉTAPE 14 Entrez un ID de VLAN pour le trafic reçu sur le réseau sans fil.

Nous vous recommandons d'affecter un ID de VLAN différent de celui par défaut (1) vers le trafic sans fil, afin de le séparer du trafic de gestion sur le VLAN 1.

ÉTAPE 15 Cliquez sur **Suivant**.

Dans le cas du périphérique WAP121, l'assistant affiche la fenêtre Summary - Confirm Your Settings. Passez à l'**ÉTAPE 24**.

Dans le cas du périphérique WAP321, l'assistant affiche la fenêtre Enable Captive Portal - Create Your Guest Network.

ÉTAPE 16 Sélectionnez si vous voulez configurer ou non une méthode d'authentification pour les invités sur votre réseau (WAP321 uniquement), puis cliquez sur **Next**.

Si vous cliquez sur **Non**, passez à l'**ÉTAPE 24**.

Si vous cliquez sur **Oui**, l'assistant affiche la fenêtre Enable Captive Portal - Name Your Guest Network.

ÉTAPE 17 Spécifiez un **Guest Network Name**.

ÉTAPE 18 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Enable Captive Portal - Secure Your Guest Network.

ÉTAPE 19 Choisissez un type de cryptage de sécurité pour le réseau invité et entrez une clé de sécurité. Pour obtenir une description de ces options, reportez-vous à **Sécurité du système**.

ÉTAPE 20 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Enable Captive Portal - Assign the VLAN ID.

ÉTAPE 21 Spécifiez un ID de VLAN pour le réseau invité. L'ID de VLAN du réseau invité doit être différent de l'ID de VLAN de gestion.

ÉTAPE 22 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Enable Captive Portal - Enable Redirect URL.

ÉTAPE 23 Sélectionnez **Activer la redirection URL** et spécifiez un nom de domaine complet ou une adresse IP dans le champ Redirect URL (y compris http://). S'ils sont spécifiés, les utilisateurs du réseau invité sont redirigés vers l'URL spécifiée après leur authentification.

ÉTAPE 24 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Summary - Confirm Your Settings.

ÉTAPE 25 Vérifiez les paramètres que vous configurez. Cliquez sur **Précédent** pour reconfigurer un ou plusieurs paramètres. Si vous cliquez sur **Annuler**, tous les paramètres sont rétablis aux valeurs précédentes ou par défaut.

ÉTAPE 26 S'ils sont corrects, cliquez sur **Submit**. Vos paramètres de configuration WAP sont enregistrés et une fenêtre de confirmation apparaît.

ÉTAPE 27 Cliquez sur **Terminer**. La fenêtre Getting Started apparaît.

Mise en route

Afin de simplifier la configuration du périphérique grâce à une navigation rapide, la page Getting Started offre des liens permettant d'effectuer des tâches courantes. La page Getting Started est la fenêtre par défaut qui apparaît chaque fois que vous vous connectez à l'utilitaire de configuration.

Liens de la page Prise en main

Catégorie	Nom du lien (sur la page)	Page correspondante
Configuration initiale	Exécuter l'assistant d'installation	Utilisation de l'assistant d'installation de point d'accès
	Configurer les paramètres de radio	Radio
	Configurer les paramètres de réseau sans fil	Networks
	Configurer les paramètres LAN	Réseau local
	Exécuter WPS	Configuration de WPS
	Configurer un point unique	Configuration de point unique
État du périphérique	Récapitulatif du système	Récapitulatif système
	État du réseau sans fil	Interfaces réseau

Liens de la page Prise en main (Suite)

Catégorie	Nom du lien (sur la page)	Page correspondante
Accès rapide	Modifier le mot de passe du compte	**Comptes d'utilisateurs**
	Mettre à niveau le microprogramme du périphérique	**Mise à niveau du micrologiciel**
	Sauvegarder/Restaurer la configuration	**Téléchargement/ sauvegarde du fichier de configuration**
Autres ressources	Assistance	Un lien vers le site d'assistance Cisco WAP.
	Forums	Un lien vers le site d'assistance de la communauté Cisco.
	Outil de planification sans fil	Un lien vers AirMagnet Planner de Fluke Networks pour Cisco Small Business.

Navigation dans les fenêtres

Cette section décrit les fonctions de l'utilitaire de configuration.

En-tête de l'utilitaire de configuration

L'en-tête de l'utilitaire de configuration contient des informations standard et apparaît en haut de chaque page. Il comporte les boutons suivants :

Boutons

Nom du bouton	Description
(Utilisateur)	Nom du compte (Administrateur ou Invité) de l'utilisateur connecté au Périphérique WAP. Le nom d'utilisateur par défaut défini en usine est **cisco**.

Boutons (Suite)

Nom du bouton	Description
Se déconnecter	Cliquez sur ce bouton pour vous déconnecter de l'utilitaire de configuration.
À propos de	Cliquez sur ce bouton pour afficher le type du Périphérique WAP ainsi que son numéro de version.
Aide	Cliquez sur ce bouton pour afficher l'aide en ligne. L'aide en ligne est conçue pour être affichée à l'aide de navigateurs utilisant le codage UTF-8. Si l'aide en ligne affiche des caractères errants, vérifiez que les paramètres de codage de votre navigateur sont définis à UTF-8.

Volet de navigation

Un volet de navigation, ou menu principal, est présent sur le côté gauche de chaque page. Le volet de navigation contient la liste des fonctionnalités de niveau supérieur des périphériques WAP. Si un élément du menu principal est précédé d'une flèche, choisissez de développer et d'afficher le sous-menu de chaque groupe. Vous pouvez ensuite sélectionner l'élément de sous-menu souhaité pour ouvrir la page associée.

Boutons de gestion

Le tableau ci-dessous décrit les boutons fréquemment utilisés qui apparaissent sur les différentes pages du système.

Boutons de gestion

Nom du bouton	Description
Ajout	Ajoute une nouvelle entrée à la table ou à la base de données.
Annuler	Annule les modifications apportées à la page.
Effacer tout	Efface toutes les entrées dans la table du journal.
Suppr.	Supprime une entrée dans une table. Sélectionnez tout d'abord une entrée.

Boutons de gestion (Suite)

Nom du bouton	Description
Modifier	Édite ou modifie une entrée existante. Sélectionnez tout d'abord une entrée.
Actualiser	Affiche à nouveau la page en cours avec les dernières données.
Enregistrer	Enregistre les paramètres ou la configuration.
Mettre à jour	Met à jour la configuration initiale avec les nouvelles informations.

2

État et statistiques

Ce chapitre explique comment afficher l'état et les statistiques, et il contient les rubriques suivantes :

- **Récapitulatif système**
- **Interfaces réseau**
- **Statistiques de trafic**
- **Transmission/Réception de pont de groupe de travail**
- **Clients associés**
- **Associations de client TSPEC**
- **État et statistiques TSPEC**
- **Statistiques de point d'accès TSPEC**
- **Statistiques sur la radio**
- **État des alertes par e-mail**
- **Journal**

Récapitulatif système

La page System Summary affiche des informations de base, telles que la description du modèle du matériel, la version du logiciel et le temps qui s'est écoulé depuis le dernier redémarrage.

Pour afficher les informations système, sélectionnez **Status and Statistics** > **System Summary** dans le volet de navigation. Ou bien, sélectionnez **System Summary** sous **Device Status** à la page Getting Started.

La page System Summary affiche les informations suivantes :

- **PID VID** : modèle et version du matériel WAP.
- **Serial Number** : numéro de série du périphérique Cisco WAP.
- **Base MAC Address** : adresse MAC WAP.
- **Firmware Version** : numéro de version du microprogramme de l'image active.
- **Firmware MD5 Checksum** : somme de contrôle de l'image active.
- **Host Name** : nom affecté au périphérique.
- **System Uptime** : temps qui s'est écoulé depuis le dernier redémarrage.
- **System Time** : heure système actuelle.
- **Power Source** : le système peut être alimenté par un adaptateur secteur ou fonctionner en tant que port PSE (Power Sourcing Equipment, équipement source d'alimentation) PoE (Power-over-Ethernet).

Le tableau des services TCP/UDP affiche des informations de base sur les protocoles et les services fonctionnant sur le périphérique WAP.

- **Service** : nom du service, si ce dernier est disponible.
- **Protocol** : protocole de transport sous-jacent utilisé par le service (TCP ou UDP).
- **Local IP Address** : adresse IP, le cas échéant, d'un périphérique distant connecté à ce service sur le périphérique WAP. La valeur **All** indique que toutes les adresses IP sur le périphérique peuvent utiliser ce service.
- **Local Port** : numéro de port du service.
- **Remote IP Address** : adresse IP d'un hôte distant, le cas échéant, qui utilise ce service. La valeur **All** indique que le service est disponible pour l'ensemble des hôtes distants qui accèdent au système.
- **Remote Port** : numéro de port de tout périphérique distant qui communique avec ce service.
- **Connection State** : état du service. Pour les services UDP, seules les connexions actives s'affichent dans la table. Lorsque l'état d'une connexion est défini sur Actif, une connexion est établie entre le périphérique WAP et un client ou un serveur. Les états TCP suivants sont disponibles :
  - **Listening** : le service est à l'écoute des demandes de connexion.

- **Active** : une connexion est établie et les paquets sont transmis et reçus.
- **Established** : une session de connexion est établie entre le périphérique WAP et un serveur ou un client, selon le rôle de chaque périphérique par rapport à ce protocole.
- **Time Wait** : la séquence de fermeture a été initiée et le périphérique WAP attend l'expiration d'un délai défini par le système (généralement 60 secondes) avant de fermer la connexion.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Interfaces réseau

La page Network Interfaces permet d'afficher des informations de configuration et d'état relatives aux interfaces filaires et sans fil. Pour afficher la page Network Interfaces, sélectionnez **Status and Statistics** > **Network Interface** dans le volet de navigation.

La page Network Interfaces affiche les informations suivantes :

- **LAN Status** : ces paramètres s'appliquent à l'interface interne. Dans le cas du périphérique WAP321, les informations indiquent si le mode Green Ethernet est activé ou non.

  Pour modifier l'un de ces paramètres, cliquez sur le lien **Modifier**. Après avoir cliqué sur Modifier, vous êtes redirigé vers la page VLAN and IPv4 Address Settings. Pour plus d'informations sur ces champs, consultez la rubrique **Paramètres d'adresse VLAN et IPv4**.

- **Radio Status** : ces paramètres incluent le mode radio sans fil (valeur Enabled ou Disabled), l'adresse MAC associée à l'interface radio, le mode 802.11 (a/b/g/n) et le canal utilisé par l'interface.

  Pour modifier les paramètres sans fil, cliquez sur le lien **Modifier**. Après avoir cliqué sur Modifier, vous êtes redirigé vers la page Radio. Pour plus d'informations sur ces champs, consultez la rubrique **Radio**.

- **Interface Status** : ce tableau répertorie les informations d'état de chaque point d'accès virtuel et de chaque interface de système de distribution sans fil (WDS, Wireless Distribution System).

Si le point d'accès virtuel a été configuré, le tableau répertorie le SSID, l'état administratif (démarré ou arrêté), l'adresse MAC de l'interface radio, l'ID de VLAN, le nom de tout profil de planificateur associé, ainsi que l'état en cours (actif ou inactif). L'état indique si le point d'accès virtuel échange des données avec un client.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Statistiques de trafic

La page Traffic Statistics permet d'afficher des informations de base sur le périphérique WAP. Elle offre également un affichage en temps réel des statistiques de transmission et de réception de l'interface Ethernet, des points d'accès virtuels et de toute interface WDS. Toutes les statistiques de transmission et de réception reflètent les totaux obtenus depuis le dernier démarrage du périphérique WAP. Si vous avez redémarré le périphérique WAP, ces données chiffrées indiquent les totaux de transmission et de réception depuis le redémarrage.

Pour afficher la page Traffic Statistics, sélectionnez **Status and Statistics** > **Traffic Statistics** dans le volet de navigation.

La page Traffic Statistics affiche des données récapitulatives et des statistiques sur le trafic dans chaque direction.

- **Network Interface** : nom de l'interface Ethernet et de chaque interface de point d'accès virtuel et WDS.

  Chaque nom d'interface de point d'accès virtuel est suivi de son SSID entre parenthèses.

- **Total Packets** : nombre total de paquets envoyés (dans la table Transmit) ou reçus (dans la table Received) par ce périphérique WAP.

- **Total Bytes** : nombre total d'octets envoyés (dans la table Transmit) ou reçus (dans la table Received) par ce périphérique WAP.

- **Total Dropped Packets** : nombre total de paquets abandonnés envoyés (dans la table Transmit) ou reçus (dans la table Received) par ce périphérique WAP.

- **Total Dropped Bytes** : nombre total d'octets abandonnés envoyés (dans la table Transmit) ou reçus (dans la table Received) par ce périphérique WAP.

- **Errors** : nombre total d'erreurs relatives à l'envoi et à la réception de données sur ce périphérique WAP.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Transmission/Réception de pont de groupe de travail

La page WorkGroup Bridge Transmit/Receive affiche le nombre de paquets et d'octets du trafic entre postes sur un pont de groupe de travail. Pour obtenir des informations sur la configuration des ponts de groupe de travail, reportez-vous à la section **Pont de groupe de travail**.

Pour afficher la page WorkGroup Bridge Transmit/Receive, sélectionnez **Status and Statistics** > **WorkGroup Bridge** dans le volet de navigation.

Chaque interface réseau configurée en tant qu'interface de pont de groupe de travail affiche les champs suivants :

- **Network Interface** : nom de l'interface Ethernet ou de point d'accès virtuel.
- **Status and Statistics** : indique si l'interface est déconnectée ou si son état administratif est démarré ou arrêté.
- **VLAN ID** : ID de réseau local virtuel (VLAN). Vous pouvez utiliser des VLAN pour créer plusieurs réseaux internes et invités sur le même périphérique WAP. L'ID de VLAN (VLAN ID) est défini dans l'onglet VAP. Reportez-vous à la section **Configuration des VAP**.
- **Name (SSID)** : nom du réseau sans fil. Également appelée SSID, cette clé alphanumérique identifie de manière unique un réseau local sans fil. Le SSID est défini dans l'onglet VAP. Reportez-vous à la section **Configuration des VAP**.

Des informations supplémentaires s'affichent pour les directions de transmission et de réception pour chaque interface de pont de groupe de travail :

- **Total Packets** : nombre total de paquets pontés entre les clients filaires dans le pont de groupe de travail et le réseau sans fil.
- **Total Bytes** : nombre total d'octets pontés entre les clients filaires dans le pont de groupe de travail et le réseau sans fil.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Clients associés

Vous pouvez utiliser la page Associated Clients pour afficher les postes client associés à un point d'accès particulier.

Pour afficher la page Associated Clients, sélectionnez **Status and Statistics** > **Associated Clients** dans le volet de navigation.

Les postes associés sont affichés avec des informations relatives au trafic des paquets transmis et reçus pour chaque poste.

- **Total Number of Associated Clients** : nombre total des clients actuellement associés au Périphérique WAP.
- **Network Interface** : point d'accès virtuel auquel le client est associé.
- **Station** : adresse MAC du client sans fil associé.
- **Status** : l'état authentifié et associé affiche l'état d'authentification et d'association IEEE 802.11 sous-jacent, qui est présent quel que soit le type de sécurité utilisé par le client pour se connecter au périphérique WAP. Cet état n'affiche pas l'état d'authentification ou d'association IEEE 802.1X.

  Quelques points importants sont à garder à l'esprit en ce qui concerne ce champ :

  - Si le mode de sécurité du périphérique WAP est None ou Static WEP, l'état d'authentification et d'association des clients apparaît comme prévu, ce qui signifie que si un client s'affiche comme étant authentifié sur le périphérique WAP, il est capable de transmettre et de recevoir des données. (C'est la raison pour laquelle le mode Static WEP utilise uniquement l'authentification IEEE 802.11.)
  - Si le périphérique WAP utilise la sécurité IEEE 802.1X ou WPA, il se peut qu'une association de client apparaisse comme étant authentifiée (par le biais de la sécurité IEEE 802.11), bien qu'elle ne soit pas réellement authentifiée par la deuxième couche de sécurité.
- **From Station/To Station** : dans le cas de l'option From Station, les compteurs indiquent les paquets ou octets reçus par le client sans fil. Dans le cas de l'option To Station, les compteurs indiquent le nombre de paquets ou d'octets transmis à partir du périphérique WAP vers le client sans fil.
  - **Packets** : nombre de paquets reçus (transmis) à partir du client sans fil.
  - **Bytes** : nombre d'octets reçus (transmis) à partir du client sans fil.

- **Drop Packets** : nombre de paquets abandonnés après leur réception (transmission).
- **Drop Bytes** : nombre d'octets abandonnés après leur réception (transmission).
- **TS Violate Packets (From Station)** : nombre de paquets envoyés à partir d'un poste client vers le périphérique WAP au-delà de sa bande passante de liaison montante active de flux de trafic (TS, Traffic Stream) ou pour une catégorie d'accès nécessitant un contrôle d'admission auquel le poste client n'a pas été admis.
- **TS Violate Packets (To Station)** : nombre de paquets envoyés à partir du périphérique WAP vers un poste client au-delà de sa bande passante de liaison descendante active de flux de trafic ou pour une catégorie d'accès nécessitant un contrôle d'admission auquel le poste client n'a pas été admis.

▪ **Up Time** : temps pendant lequel le client a été associé au périphérique WAP.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Associations de client TSPEC

La page TSPEC Client Associations fournit des informations en temps réel sur les données de client TSPEC transmises et reçues par ce point d'accès. Les tableaux de la page TSPEC Client Associations affichent les paquets voix et vidéo transmis et reçus depuis le démarrage de l'association, ainsi que des informations d'état.

Un TSPEC est une spécification de trafic envoyée à partir d'un client sans fil compatible QoS vers un périphérique WAP et nécessitant un certain niveau d'accès réseau pour le flux de trafic qu'il représente. Un flux de trafic est un ensemble de paquets de données identifiés par le client sans fil comme appartenant à une priorité d'utilisateur spécifique. Exemple de flux de trafic voix : combiné téléphonique CERTIFIÉ Wi-Fi marquant ses paquets de données générés par codec en tant que trafic de priorité voix. Exemple de flux de trafic vidéo : application de lecteur vidéo sur un ordinateur portable sans fil donnant la priorité à un flux de vidéoconférence à partir d'un serveur d'entreprise.

Pour afficher les statistiques des associations de client TSPEC, sélectionnez **Status and Statistics > TSPEC Client Associations** dans le volet de navigation.

La page TSPEC Client Associations affiche les informations suivantes :

État et statistiques :

- **Network Interface** : interface radio utilisée par le client.
- **SSID** : identificateur d'ensemble de services associé à ce client de flux de trafic.
- **Station** : adresse MAC du poste client.
- **TS Identifier** : identificateur de session de trafic TSPEC (plage de valeurs de 0 à 7).
- **Access Category** : catégorie d'accès au flux de trafic (voix ou vidéo).
- **Direction** : direction du trafic pour ce flux de trafic. Les options possibles pour la direction sont les suivantes :
  - uplink : du client vers le périphérique (liaison montante).
  - downlink : du périphérique vers le client (liaison descendante).
  - bidirectional : dans les deux sens (liaison bidirectionnelle).
- **User Priority** : priorité d'utilisateur (UP, User Priority) de ce flux de trafic. La priorité d'utilisateur est envoyée avec chaque paquet dans la partie correspondante de l'en-tête IP. Les valeurs typiques sont les suivantes :
  - 6 ou 7 pour la voix
  - 4 ou 5 pour la vidéo

  La valeur peut varier en fonction des autres sessions de trafic de priorité.
- **Medium Time** : temps pendant lequel le flux de trafic occupe le support de transmission.
- **Excess Usage Events** : nombre de fois que le client a dépassé le temps moyen établi pour son TSPEC. Les violations mineures et peu fréquentes sont ignorées.
- **VAP MAC Address** : adresse MAC de point d'accès virtuel.

Statistiques :

- **Network Interface** : interface radio utilisée par le client.
- **Station** : adresse MAC du poste client.

- **TS Identifier** : identificateur de session de trafic TSPEC (plage de valeurs de 0 à 7).
- **Access Category** : catégorie d'accès au flux de trafic (voix ou vidéo).
- **Direction** : direction du trafic pour ce flux de trafic. Les options possibles pour la direction sont les suivantes :
  - uplink : du client vers le périphérique (liaison montante).
  - downlink : du périphérique vers le client (liaison descendante).
  - bidirectional : dans les deux sens (liaison bidirectionnelle).
- **From Station** : affiche le nombre de paquets et d'octets reçus du client sans fil ainsi que le nombre de paquets et d'octets abandonnés après leur réception.
  - **Packets** : nombre de paquets excédentaires par rapport à un TSPEC admis.
  - **Bytes** : nombre d'octets pour lesquels aucun TSPEC n'a été établi et avec une admission requise par le périphérique WAP.
- **To Station** : affiche le nombre de paquets et d'octets transmis à partir du périphérique WAP vers le client sans fil ainsi que le nombre de paquets et d'octets abandonnés durant leur transmission.
  - **Packets** : nombre de paquets excédentaires par rapport à un TSPEC admis.
  - **Bytes** : nombre d'octets pour lesquels aucun TSPEC n'a été établi et avec une admission requise par le périphérique WAP.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

État et statistiques TSPEC

La page TSPEC Status and Statistics fournit les informations suivantes :

- Informations récapitulatives à propos des sessions TSPEC par radio
- Informations récapitulatives à propos des sessions TSPEC par point d'accès virtuel

- Statistiques en temps réel de transmission et de réception pour l'interface radio et la ou les interfaces réseau

Toutes les statistiques de transmission et de réception reflètent les totaux obtenus depuis le dernier démarrage du périphérique WAP. Si vous avez redémarré le périphérique WAP, ces données chiffrées indiquent les totaux de transmission et de réception depuis le redémarrage.

Pour afficher l'état et les statistiques TSPEC, sélectionnez **Status and Statistics > TSPEC Status and Statistics** dans le volet de navigation.

La page TSPEC Status and Statistics fournit les informations d'état suivantes relatives aux interfaces WLAN (Radio) et de point d'accès virtuel :

- **Network Interface** : nom de l'interface radio ou de point d'accès virtuel.
- **Access Category** : catégorie d'accès actuelle associée à ce flux de trafic (voix ou vidéo).
- **Status** : indique si la session TSPEC est activée (démarrée) ou désactivée (arrêtée) pour la catégorie d'accès correspondante.

  REMARQUE L'état est un état de configuration, qui ne représente pas nécessairement l'activité de la session en cours.
- **Active Traffic Stream** : nombre de flux de trafic TSPEC actuellement actifs pour cette radio et cette catégorie d'accès.
- **Traffic Stream Clients** : nombre de clients de flux de trafic associés à cette radio et à cette catégorie d'accès.
- **Medium Time Admitted** : temps alloué à cette catégorie d'accès pour transporter des données sur le support de transmission. Cette valeur doit être inférieure ou égale à celle de la bande passante maximale autorisée sur le support pour ce flux de trafic.
- **Medium Time Unallocated** : temps de bande passante non utilisée pour cette catégorie d'accès.

Ces statistiques apparaissent séparément pour les chemins de transmission et de réception sur l'interface radio sans fil :

- **Access Category** : catégorie d'accès associée à ce flux de trafic (voix ou vidéo).
- **Total Packets** : nombre total de paquets de flux de trafic envoyés (dans la table Transmit) ou reçus (dans la table Received) par cette radio pour la catégorie d'accès spécifiée.

- **Total Bytes** : nombre total d'octets reçus dans la catégorie d'accès spécifiée.

Ces statistiques apparaissent séparément pour les chemins de transmission et de réception sur les interfaces réseau (points d'accès virtuels) :

- **Total Voice Packets** : nombre total de paquets voix de flux de trafic envoyés (dans la table Transmit) ou reçus (dans la table Received) par ce périphérique WAP pour ce point d'accès virtuel.
- **Total Voice Bytes** : nombre total d'octets voix de flux de trafic envoyés (dans la table Transmit) ou reçus (dans la table Received) par ce périphérique WAP pour ce point d'accès virtuel.
- **Total Video Packets** : nombre total de paquets vidéo de flux de trafic envoyés (dans la table Transmit) ou reçus (dans la table Received) par ce périphérique WAP pour ce point d'accès virtuel.
- **Total Video Bytes** : nombre total d'octets vidéo de flux de trafic envoyés (dans la table Transmit) ou reçus (dans la table Received) par ce périphérique WAP pour ce point d'accès virtuel.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Statistiques de point d'accès TSPEC

La page TSPEC AP Statistics fournit des informations sur les flux de trafic voix et vidéo acceptés et rejetés par le périphérique WAP. Pour afficher la page TSPEC AP Statistics, sélectionnez **Status and Statistics > TSPEC AP Statistics** dans le volet de navigation.

- **TSPEC Statistics Summary for Voice ACM** : nombre total de flux de trafic voix acceptés et nombre total de flux de trafic voix rejetés.
- **TSPEC Statistics Summary for Video ACM** : nombre total de flux de trafic vidéo acceptés et nombre total de flux de trafic vidéo rejetés.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Statistiques sur la radio

Utilisez la page Radio Statistics pour afficher des statistiques au niveau des paquets et des octets pour interface radio sans fil. Pour afficher la page Radio Statistics, sélectionnez **Status and Statistics > Radio Statistics** dans le volet de navigation.

- **Packets Received** : nombre total de paquets reçus par le périphérique WAP.
- **Packets Transmitted** : nombre total de paquets transmis par le périphérique WAP.
- **Bytes Received** : nombre total d'octets reçus par le périphérique WAP.
- **Bytes Transmitted** : nombre total d'octets transmis par le périphérique WAP.
- **Packets Receive Dropped** : nombre de paquets reçus par le périphérique WAP et abandonnés.
- **Packets Transmit Dropped** : nombre de paquets transmis par le périphérique WAP et abandonnés.
- **Bytes Receive Dropped** : nombre d'octets reçus par le périphérique WAP et abandonnés.
- **Bytes Transmit Dropped** : nombre d'octets transmis par le périphérique WAP et abandonnés.
- **Fragments Received** : nombre de trames fragmentées reçues par le périphérique WAP.
- **Fragments Transmitted** : nombre de trames fragmentées envoyées par le périphérique WAP.
- **Multicast Frames Received** : nombre de trames MSDU reçues avec le bit de multidiffusion défini dans l'adresse MAC de destination.
- **Multicast Frames Transmitted** : nombre de trames MSDU transmises avec succès et pour lesquelles le bit de multidiffusion était défini dans l'adresse MAC de destination.
- **Duplicate Frame Count** : nombre de fois qu'une trame a été reçue et que le champ Sequence Control indique qu'il s'agit d'un doublon.

- **Failed Transmit Count** : nombre de fois qu'une trame MSDU n'a pas été transmise avec succès, car le nombre de tentatives de transmission dépassait la limite de tentatives trames courtes ou la limite de tentatives trames longues.
- **FCS Error Count** : nombre d'erreurs FCS détectées dans une trame MPDU reçue.
- **Transmit Retry Count** : nombre de fois qu'une trame MSDU a été transmise avec succès après une ou plusieurs tentatives.
- **ACK Failure Count** : nombre de trames ACK non reçues au moment où elles étaient attendues.
- **RTS Failure Count** : nombre de trames CTS non reçues en réponse à une trame RTS.
- **WEP Undecryptable Count** : nombre de trames abandonnées, car ne pouvant pas être décryptées par la radio. Les trames peuvent être abandonnées parce qu'elles n'ont pas été décryptées ou parce qu'elles ont été décryptées avec une option de confidentialité non prise en charge par le périphérique WAP.
- **RTS Success Count** : nombre de trames CTS reçues en réponse à une trame RTS.
- **Multiple Retry Count** : nombre de fois qu'une trame MSDU a été transmise avec succès après plus d'une tentative.
- **Frames Transmitted Count** : nombre de trames MSDU transmises avec succès.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

État des alertes par e-mail

La page Email Alert Status fournit des informations sur les alertes par e-mail envoyées sur la base des messages syslog générés par le périphérique WAP. Pour afficher la page Email Alert Status, sélectionnez **Status and Statistics > Email Alert Status** dans le volet de navigation.

- **Email Alert Status** : état configuré des alertes par e-mail. L'état est soit Enabled soit Disabled. La valeur par défaut est Disabled.

- **Number of Emails Sent** : nombre total de messages électroniques envoyés. La valeur est un entier de 32 bits, non affecté d'un signe. La valeur par défaut est 0.
- **Number of Emails Failed** : nombre total de messages électroniques ayant échoué. La valeur est un entier de 32 bits, non affecté d'un signe. La valeur par défaut est 0.
- **Time Last Email Sent** : jour, date et heure d'envoi du dernier message électronique.

Journal

La page Log répertorie les événements système qui ont généré une entrée de journal, comme les tentatives de connexion et les modifications de configuration. Le contenu du journal est effacé lors d'un redémarrage et il peut également l'être par un administrateur. Le journal peut afficher un maximum de 512 événements. Lorsque cela s'avère nécessaire, les entrées les plus anciennes sont supprimées de la liste, afin de créer de la place pour les nouveaux événements.

Pour afficher la page Log, sélectionnez **Status and Statistics > Log Status** dans le volet de navigation.

- **Time Stamp** : heure système de l'occurrence de l'événement.
- **Severity** : indique si l'événement est dû à une erreur (err) ou est fourni à titre indicatif (info).
- **Service** : composant logiciel associé à l'événement.
- **Description** : description de l'événement.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Cliquez sur **Effacer tout** pour effacer toutes les entrées du journal.

3

Administration

Ce chapitre explique comment configurer les paramètres système globaux et effectuer des diagnostics.

Il contient les sections suivantes :

- **Paramètres système**
- **Comptes d'utilisateurs**
- **Paramètres de l'heure**
- **Paramètres des journaux**
- **Alertes par e-mail**
- **Service HTTP/HTTPS**
- **Management Access Control**
- **Mise à niveau du micrologiciel**
- **Mise à niveau du micrologiciel**
- **Téléchargement/sauvegarde du fichier de configuration**
- **Propriétés des fichiers de configuration**
- **Copie/enregistrement de la configuration**
- **Redémarrage**
- **Discovery—Bonjour**
- **Capture de paquets**
- **Informations de support**

Paramètres système

La page System Settings vous permet de configurer les informations qui identifient le périphérique WAP sur le réseau.

Pour définir les paramètres système :

ÉTAPE 1 Sélectionnez **Administration** > **System Settings** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Host Name** : nom attribué de façon administrative au périphérique WAP. Par convention, il s'agit du nom de domaine complet du nœud. Le nom d'hôte par défaut est **wap** concaténé avec les 6 derniers chiffres hexadécimaux de l'adresse MAC du périphérique WAP. Les noms d'hôte ne peuvent 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. Le nom d'hôte peut comporter de 1 à 63 caractères.
- **System Contact** : personne à contacter pour le périphérique WAP. Le contact système peut comporter de 0 à 255 caractères et peut inclure des espaces et des caractères spéciaux.
- **System Location** : description de l'emplacement physique du périphérique WAP. L'emplacement système peut comporter de 0 à 255 caractères et peut inclure des espaces et des caractères spéciaux.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Comptes d'utilisateurs

Par défaut, un utilisateur de gestion est configuré sur le périphérique WAP :

- Nom d'utilisateur : **cisco**
- Password : **cisco**

Vous pouvez utiliser la page User Accounts pour configurer un maximum de quatre utilisateurs supplémentaires et modifier le mot de passe d'un utilisateur.

Ajout d'un utilisateur

Pour ajouter un nouvel utilisateur :

ÉTAPE 1 Sélectionnez **Administration** > **User Accounts** dans le volet de navigation.

La table des comptes d'utilisateur affiche les utilisateurs actuellement configurés. L'utilisateur **cisco** est préconfiguré dans le système pour avoir les privilèges de lecture/écriture.

Tous les autres utilisateurs peuvent disposer de l'accès en lecture seule, mais pas de l'accès en lecture/écriture.

ÉTAPE 2 Cliquez sur **Ajouter**. Une nouvelle ligne de zones de texte s'affiche.

ÉTAPE 3 Cochez la case correspondant au nouvel utilisateur, puis sélectionnez **Edit**.

ÉTAPE 4 Dans **User Name**, saisissez un nom d'utilisateur constitué de 1 à 32 caractères alphanumériques. Les noms d'utilisateur ne peuvent comporter que les chiffres 0 à 9 et les lettres a à z (en majuscules ou minuscules).

ÉTAPE 5 Dans **New Password**, saisissez un nouveau mot de passe constitué de 1 à 64 caractères, puis saisissez le même mot de passe dans la zone de texte **Confirm New Password**.

Une fois que vous avez saisi un mot de passe, le nombre et la couleur des barres verticales changent pour indiquer la sécurité du mot de passe, comme suit :

- Rouge : le mot de passe ne répond pas aux exigences minimales en termes de complexité.
- Orange : le mot de passe répond aux exigences minimales en termes de complexité, mais offre une faible sécurité.
- Vert : le mot de passe offre une sécurité élevée.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Pour supprimer un utilisateur, cochez la case en regard de son nom, puis sélectionnez **Delete**. Pour enregistrer définitivement votre suppression, sélectionnez **Save** lorsque vous avez terminé.

Modification d'un mot de passe utilisateur

Pour modifier un mot de passe utilisateur :

ÉTAPE 1 Sélectionnez **Administration** > **User Accounts** dans le volet de navigation.

La table des comptes d'utilisateur affiche les utilisateurs actuellement configurés. L'utilisateur **cisco** est préconfiguré dans le système pour avoir les privilèges de lecture/écriture. Le mot de passe de l'utilisateur **cisco** peut être modifié.

ÉTAPE 2 Sélectionnez l'utilisateur à configurer et cliquez sur **Edit**.

ÉTAPE 3 Dans **New Password**, saisissez un nouveau mot de passe constitué de 1 à 64 caractères, puis saisissez le même mot de passe dans la zone de texte **Confirm New Password**.

Une fois que vous avez saisi un mot de passe, le nombre et la couleur des barres verticales changent pour indiquer la sécurité du mot de passe, comme suit :

- Rouge : le mot de passe ne répond pas aux exigences minimales en termes de complexité.
- Orange : le mot de passe répond aux exigences minimales en termes de complexité, mais offre une faible sécurité.
- Vert : le mot de passe offre une sécurité élevée.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Si vous modifiez votre mot de passe, vous devez vous reconnecter au système.

Paramètres de l'heure

Une horloge système fournit un service d'horodatage synchronisé sur le réseau pour les événements logiciels, tels que les journaux de messages. Vous pouvez configurer l'horloge système manuellement ou configurer le périphérique WAP en tant que client Network Time Protocol (NTP) qui obtient les données d'horloge d'un serveur.

Utilisez la page Time Settings pour définir l'heure système manuellement ou pour configurer le système afin qu'il récupère ses paramètres d'heure d'un serveur NTP préconfiguré. Par défaut, le Périphérique WAP est configuré de manière à obtenir l'heure à partir d'une liste prédéfinie de serveurs NTP.

L'heure système actuelle apparaît en haut de la page avec l'option System Clock Source.

Pour utiliser NTP afin que le périphérique WAP acquière automatiquement ses paramètres d'heure :

ÉTAPE 1 Pour le champ System Clock Source, sélectionnez **Network Time Protocol (NTP)**.

ÉTAPE 2 Définissez les paramètres suivants :

- **NTP Server/IPv4/IPv6 Address Name** : spécifiez l'adresse IPv4, l'adresse IPv6 ou le nom d'hôte d'un serveur NTP. Un serveur NTP par défaut est répertorié.

  Un nom d'hôte peut se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter jusqu'à 253 caractères.

- **Time Zone** : sélectionnez le fuseau horaire où vous vous trouvez.

ÉTAPE 3 Sélectionnez **Adjust Time for Daylight Savings** si l'heure d'été s'applique à votre fuseau horaire. Si vous sélectionnez cette option, configurez les champs suivants :

- **Daylight Savings Start** : sélectionnez l'heure, le jour, la semaine et le mois du passage à l'heure d'été.
- **Daylight Savings End** : sélectionnez l'heure, le jour, la semaine et le mois du passage à l'heure d'hiver.
- **Daylight Savings Offset** : indiquez de combien de minutes vous devez avancer l'horloge lors du passage à l'heure d'été et de combien vous devez la reculer lors du passage à l'heure d'hiver.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Pour configurer manuellement les paramètres d'heure, procédez comme suit :

ÉTAPE 1 Pour le champ System Clock Source, sélectionnez **Manually**.

ÉTAPE 2 Définissez les paramètres suivants :

- **System Date** : sélectionnez le jour, le mois et l'année actuels dans les listes déroulantes.

- **System Time** : sélectionnez l'heure et les minutes actuelles au format 24 heures, tel que 22:00:00.
- **Time Zone** : sélectionnez le fuseau horaire où vous vous trouvez.

ÉTAPE 3 Sélectionnez **Adjust Time for Daylight Savings** si l'heure d'été s'applique à votre fuseau horaire. Si vous sélectionnez cette option, configurez les champs suivants :

- **Daylight Savings Start** : sélectionnez l'heure, le jour, la semaine et le mois du passage à l'heure d'été.
- **Daylight Savings End** : sélectionnez l'heure, le jour, la semaine et le mois du passage à l'heure d'hiver.
- **Daylight Savings Offset** : indiquez de combien de minutes vous devez avancer l'horloge lors du passage à l'heure d'été et de combien vous devez la reculer lors du passage à l'heure d'hiver.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Paramètres des journaux

Vous pouvez utiliser la page Log Settings pour permettre l'enregistrement des messages de journal dans la mémoire permanente. Vous pouvez également envoyer des journaux à un hôte distant.

Configuration du journal persistant

Si le système redémarre de manière inattendue, les messages de journal peuvent être utiles pour diagnostiquer la cause. Toutefois, les messages de journal sont effacés au redémarrage du système sauf si vous activez la journalisation persistante.

AVERTISSEMENT L'activation de la journalisation persistante peut épuiser la mémoire flash (non volatile) et dégrader les performances réseau. Activez uniquement la journalisation persistante pour déboguer un problème. Veillez à désactiver la journalisation persistante une fois que vous avez débogué le problème.

Pour configurer la journalisation persistante :

ÉTAPE 1 Sélectionnez **Administration** > **Log Settings** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Persistence** : cliquez sur **Enable** pour enregistrer les journaux système dans la mémoire non volatile, afin de permettre la conservation des journaux au redémarrage du périphérique WAP. Vous pouvez enregistrer jusqu'à 128 messages de journal dans la mémoire non volatile. Lorsque la limite de 128 est atteinte, le message le plus ancien du journal est remplacé par le nouveau message. Effacez le contenu de ce champ si vous souhaitez enregistrer les journaux système dans la mémoire volatile. Les journaux présents dans la mémoire volatile sont supprimés au redémarrage du système.
- **Severity** : gravité minimale qu'un événement doit avoir pour être écrit dans le journal de la mémoire non volatile. Par exemple, si vous spécifiez 2 (critique), alors les événements de niveau critique, alerte et urgence sont journalisés dans la mémoire non volatile. Les messages d'erreur ayant un niveau de gravité 3 à 7 sont écrits dans la mémoire volatile.
- **Depth** : nombre maximal de messages (jusqu'à 512) pouvant être stockés dans la mémoire volatile. Lorsque le nombre défini dans ce champ est atteint, l'événement le plus ancien du journal est remplacé par le nouvel événement. Veuillez noter que le nombre maximal de messages de journal pouvant être stockés dans la mémoire non volatile (le journal persistant) est 128, celui-ci n'étant pas configurable.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Serveur de journalisation distant

Le journal du noyau est une liste complète d'événements système (présentée dans le System Log) et de messages du noyau, tels que des conditions d'erreur.

Vous ne pouvez pas consulter les messages de journal du noyau directement à partir de l'interface Web. Vous devez d'abord configurer un serveur de journalisation distant qui recevra et capturera les journaux. Vous pouvez ensuite configurer le périphérique WAP à journaliser sur le serveur de journalisation distant.

La collecte du serveur de journalisation distant pour les messages syslog du périphérique WAP offre les fonctions suivantes :

- Permet l'agrégation des messages syslog depuis plusieurs points d'accès
- Stocke un historique des messages plus long que celui conservé sur un seul périphérique WAP
- Déclenche des opérations de gestion scriptées et des alertes

Pour spécifier un hôte de votre réseau en tant que serveur de journalisation distant :

ÉTAPE 1 Sélectionnez **Administration** > **Log Settings** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Remote Log** : permet au Périphérique WAP d'envoyer des messages de journal à un hôte distant. Si cette fonction est désactivée, tous les messages de journal sont conservés sur le système local.
- **Server IPv4/IPv6 Address/Name** : adresse IPv4 ou IPv6, ou nom d'hôte du serveur de journalisation distant.

  Un nom d'hôte peut se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter jusqu'à 253 caractères.
- **UDP Port** : numéro de port logique pour le processus syslog sur l'hôte distant. La plage est comprise entre 1 et 65 535. Le port par défaut est 514.

  Il est recommandé d'utiliser le port par défaut. Si vous choisissez de reconfigurer le port du journal, vérifiez que le numéro de port que vous attribuez à syslog est disponible.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Si vous avez activé un hôte Remote Log et que vous cliquez sur **Save**, vous activez alors la journalisation distante. Le périphérique WAP envoie ses messages du noyau en temps réel afin qu'ils soient affichés sur le moniteur du serveur de journalisation distant, un fichier journal du noyau spécifié ou un autre système de stockage, selon vos configurations.

Si vous avez désactivé un hôte Remote Log et que vous cliquez sur **Save**, vous désactivez alors la journalisation distante.

REMARQUE Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Alertes par e-mail

Utilisez la fonction d'alerte par e-mail pour envoyer des messages aux adresses e-mail configurées lorsque des événements système spécifiques se produisent.

Cette fonction prend en charge la configuration du serveur de messagerie, la configuration de la gravité des messages et la configuration de trois adresses e-mail maximum pour l'envoi par e-mail des alertes urgentes et non urgentes.

CONSEIL N'utilisez pas votre adresse e-mail personnelle, car les identifiants de connexion à votre messagerie personnelle seraient dévoilés inutilement. Utilisez plutôt un compte de messagerie distinct. Notez également que de nombreux comptes de messagerie conservent par défaut une copie de tous les messages envoyés. Toutes les personnes ayant accès à ce compte de messagerie ont accès aux messages envoyés. Vérifiez les paramètres de votre messagerie afin de vous assurer qu'ils sont conformes à la politique de confidentialité de votre entreprise.

Pour configurer le Périphérique WAP afin qu'il envoie des alertes par e-mail :

ÉTAPE 1 Sélectionnez **Administration** > **Email Alert** dans le volet de navigation.

ÉTAPE 2 Dans la zone Global Configuration, définissez les paramètres suivants :

- **Administrative Mode** : choisissez d'activer la fonction d'alerte par e-mail globalement.
- **From Email Address** : entrez l'adresse à afficher en tant qu'expéditeur de l'e-mail. L'adresse est une chaîne de 255 caractères uniquement imprimables. Aucune adresse n'est configurée par défaut.
- **Log Duration** : choisissez la fréquence à laquelle les messages planifiés sont envoyés. La plage valide va de 30 à 1440 minutes. La valeur par défaut est 30 minutes.

- **Scheduled Message Severity** : les messages de journal de ce niveau de gravité ou d'un niveau plus élevé sont regroupés et envoyés à l'adresse e-mail de configuration, à la fréquence définie dans Log Duration. Sélectionnez l'une des valeurs suivantes : None, Emergency, Alert, Critical, Error, Warning, Notice, Info et Debug. Si vous sélectionnez None, aucun message de gravité planifié n'est envoyé. La gravité par défaut est Warning.
- **Urgent Message Severity** : les messages de journal de ce niveau de gravité ou d'un niveau plus élevé sont immédiatement envoyés à l'adresse e-mail configurée. Sélectionnez l'une des valeurs suivantes : None, Emergency, Alert, Critical, Error, Warning, Notice, Info et Debug. Si vous sélectionnez None, aucun message de gravité urgente n'est envoyé. La valeur par défaut est Alert.

ÉTAPE 3 Dans la zone Mail Server Configuration, définissez les paramètres suivants :

- **Server IPv4 Address/Name** : saisissez l'adresse IP ou le nom d'hôte du serveur SMTP sortant. (Vous pouvez demander à votre fournisseur de messagerie de vous indiquer le nom d'hôte.) L'adresse du serveur doit être une adresse IPv4 ou un nom d'hôte valide. La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (192.0.2.10).

  Un nom d'hôte peut se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter jusqu'à 253 caractères.
- **Data Encryption** : saisissez le mode de sécurité de l'alerte par e-mail sortante. L'alerte peut être envoyée via le protocole TLS sécurisé ou le protocole Open par défaut. L'utilisation du protocole TLSv1 sécurisé empêche l'espionnage électronique et la falsification lors des communications via le réseau public.
- **Port** : saisissez le numéro de port SMTP à utiliser pour les e-mails sortants. Le numéro de port doit être compris entre 0 et 65 535. Le port par défaut est 465. Le port dépend généralement du mode utilisé par le fournisseur de messagerie.
- **Username** : saisissez le nom d'utilisateur du compte de messagerie qui sera utilisé pour envoyer ces e-mails. Généralement (pas systématiquement), le nom d'utilisateur correspond à l'adresse e-mail complète incluant le domaine (par exemple, Nom@exemple.com). Le compte spécifié sera utilisé en tant qu'adresse e-mail de l'expéditeur. Le nom d'utilisateur peut être constitué de 1 à 64 caractères alphanumériques.

- **Password** : saisissez le mot de passe du compte de messagerie qui sera utilisé pour l'envoi de ces e-mails. Le mot de passe peut être constitué de 1 à 64 caractères.

ÉTAPE 4 Configurez les adresses e-mail et la ligne d'objet.

- **To Email Address 1/2/3** : saisissez au maximum trois adresses de réception des alertes par e-mail. Chaque adresse e-mail doit être valide.
- **Email Subject** : saisissez le texte qui s'affichera dans la ligne d'objet de l'e-mail. Il peut s'agir d'une chaîne alphanumérique de 255 caractères maximum.

ÉTAPE 5 Cliquez sur **Test Mail** pour envoyer un e-mail de test afin de valider le compte de messagerie configuré.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Exemples d'alertes par e-mail

L'exemple suivant indique comment renseigner les paramètres de la zone Mail Server Configuration :

```
Gmail
Server IPv4 Address/Name : smtp.gmail.com
Data Encryption : TLSv1
Port : 465
Username : votre adresse e-mail complète qui vous permet de vous connecter à
votre compte de messagerie associé au serveur ci-dessus
Password : xxxxxxxx est un mot de passe valide de votre compte de messagerie
valide
To Email Address 1 : mon_email@gmail.com

Windows Live Hotmail
Windows Live Hotmail recommande les paramètres suivants :
Data Encryption : TLSv1
SMTP Server : smtp.live.com
SMTP Port : 587
Username : votre adresse e-mail complète, telle que monNom@hotmail.com ou
monNom@monDomaine.com
Password : votre mot de passe de compte Windows Live

Yahoo! Mail
Pour pouvoir profiter de ce type de service, Yahoo impose l'utilisation d'un
compte payant. Yahoo recommande les paramètres suivants :
Data Encryption : TLSv1
SMTP Server : plus.smtp.mail.yahoo.com
SMTP Port : 465 ou 587
```

```
Username : votre adresse e-mail sans le nom du domaine, telle que monNom
(sans @yahoo.com)
Password : votre mot de passe de compte Yahoo
```

L'exemple suivant présente la mise en forme d'un e-mail de journal général :

```
From : AP-192.168.2.10@mailserver.com
Sent: Wednesday, September 09, 2009 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP

TIME           PriorityProcess Id          Message
Sep 8 03:48:25 info    login[1457]         root login on ttyp0
Sep 8 03:48:26 info    mini_http-ssl[1175] Max concurrent connections of 20
reached
```

Service HTTP/HTTPS

Utilisez la page HTTP/HTTPS Service pour activer et configurer des connexions de gestion Web. Si HTTPS est utilisé pour sécuriser les sessions de gestion, vous pouvez aussi utiliser la page HTTP/HTTPS Service pour gérer les certificats SSL requis.

Configuration des services HTTP et HTTPS

Pour configurer les services HTTP et HTTPS :

ÉTAPE 1 Sélectionnez **Administration** > **HTTP/HTTPS Service** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres globaux suivants :

- **Maximum Sessions** : nombre de sessions Web, y compris HTTP et HTTPS, pouvant être utilisées simultanément.

  Lorsqu'un utilisateur se connecte à l'utilitaire de configuration de périphérique WAP, une session est créée. Cette session reste active jusqu'à ce que l'utilisateur se déconnecte ou jusqu'à la fin du délai d'expiration de la session. La plage est comprise entre 1 et 10 sessions. La valeur par défaut est 5. Si le nombre maximal de sessions est atteint, le prochain utilisateur qui tente de se connecter à l'utilitaire de configuration reçoit un message d'erreur relatif à la limite de session.

- **Session Timeout** : durée maximale en minutes pendant laquelle un utilisateur inactif peut rester connecté à l'utilitaire de configuration de périphérique WAP. Lorsque le délai d'expiration est atteint, l'utilisateur est automatiquement déconnecté. La plage valide va de 1 à 60 minutes. La valeur par défaut est 10 minutes.

ÉTAPE 3 Configurez les services HTTP et HTTPS :

- **HTTP Server** : active l'accès par HTTP. L'accès HTTP est activé par défaut. Si vous le désactivez, toutes les connexions actives qui utilisent ce protocole sont déconnectées.
- **HTTP Port** : numéro de port logique à utiliser pour les connexions HTTP, de 1 025 à 65 535. Le numéro de port par défaut pour les connexions HTTP est le numéro de port bien connu IANA 80.
- **HTTPS Server** : active l'accès par HTTP sécurisé. L'accès HTTPS est activé par défaut. Si vous le désactivez, toutes les connexions actives qui utilisent ce protocole sont déconnectées.
- **HTTPS Port** : numéro de port logique à utiliser pour les connexions HTTP, de 1 025 à 65 535. Le numéro de port par défaut pour les connexions HTTP est le numéro de port bien connu IANA 443.
- **Redirect HTTP to HTTPS** : redirige les tentatives d'accès HTTP de gestion sur le port HTTP vers le port HTTPS. Ce champ est uniquement disponible lorsque l'accès HTTP est désactivé.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Gestion des certificats SSL

Pour utiliser les services HTTPS, le périphérique WAP doit avoir un certificat SSL valide. Le périphérique WAP peut générer un certificat ou vous pouvez le télécharger depuis votre réseau ou un serveur TFTP.

Pour générer le certificat avec le périphérique WAP, cliquez sur **Generate SSL Certificate**. L'opération est effectuée une fois que le Périphérique WAP a obtenu une adresse IP, afin de garantir que le nom commun du certificat correspond à l'adresse IP du Périphérique WAP. La génération d'un nouveau 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.

Dans la zone Certificate File Status, vous pouvez voir s'il existe déjà un certificat sur le périphérique WAP et obtenir les informations suivantes sur celui-ci :

- Certificate File Present
- Certificate Expiration Date
- Certificate Issuer Common Name

S'il existe un certificat SSL (avec une extension .pem) sur le périphérique WAP, vous pouvez le télécharger vers votre ordinateur en tant que sauvegarde. Dans la zone Download SSL Certificate (From Device to PC), sélectionnez la méthode de téléchargement **HTTP** ou **TFTP** dans **Download Method**, puis cliquez sur **Download**.

- Si vous sélectionnez HTTP, vous devez confirmer le téléchargement, puis accéder à l'emplacement d'enregistrement du fichier sur votre réseau.
- Si vous sélectionnez TFTP, d'autres champs apparaissent pour vous permettre de saisir le nom de fichier à attribuer au fichier téléchargé. Vous devez ensuite saisir l'adresse du serveur TFTP où le fichier sera téléchargé.

Vous pouvez également télécharger un fichier de certificat (portant une extension .pem) depuis votre ordinateur vers le périphérique WAP. Dans la zone Upload SSL Certificate (From PC to Device), sélectionnez la méthode de téléchargement **HTTP** ou **TFTP** dans **Upload Method**.

- Pour HTTP, accédez à l'emplacement réseau, sélectionnez le fichier, puis cliquez sur **Upload**.
- Pour TFTP, renseignez **File Name** puisqu'il existe sur le serveur TFTP et **TFTP Server IPv4 Address**, puis cliquez sur **Upload**. Le nom de fichier ne peut pas contenir les caractères suivants : espaces, <, >, |, \, : , (,), &, ; , #, ? , *, ainsi que deux points successifs ou plus.

Un message de confirmation s'affiche lorsque le téléchargement a été correctement effectué.

Management Access Control

Vous pouvez créer une liste de contrôle d'accès (ACL) contenant jusqu'à cinq hôtes IPv4 et cinq hôtes IPv6 autorisés à accéder à l'utilitaire de configuration de périphérique WAP. Si cette fonction est désactivée, tout le monde peut accéder à l'utilitaire de configuration depuis n'importe quel client réseau en fournissant le nom d'utilisateur et le mot de passe corrects du périphérique WAP.

Si la liste de contrôle d'accès de gestion est activée, l'accès via le Web et SNMP est limité aux hôtes IP spécifiés.

AVERTISSEMENT Vérifiez chaque adresse IP que vous saisissez. Si vous saisissez une adresse IP qui ne correspond pas à votre ordinateur d'administration, vous n'aurez plus accès à l'interface de configuration. Il est fortement recommandé d'attribuer une adresse IP statique à l'ordinateur d'administration, afin que cette adresse reste toujours la même.

Pour créer une liste d'accès :

ÉTAPE 1 Sélectionnez **Administration** > **Management Access Control** dans le volet de navigation.

ÉTAPE 2 Sélectionnez **Enable** pour **Management ACL Mode**.

ÉTAPE 3 Saisissez un maximum de cinq adresses IPv4 et cinq adresses IPv6 auxquelles vous donnez accès.

ÉTAPE 4 Vérifiez que les adresses IP sont correctes.

ÉTAPE 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Mise à niveau du micrologiciel

Lorsque de nouvelles versions du microprogramme de Périphérique WAP deviennent disponibles, vous pouvez le mettre à niveau sur vos périphériques afin de bénéficier des nouvelles fonctionnalités et améliorations. Le Périphérique WAP utilise un client TFTP ou HTTP pour les mises à niveau du microprogramme.

Une fois que vous avez chargé le nouveau microprogramme et que le système redémarre, le microprogramme nouvellement ajouté devient l'image principale. Si la mise à niveau échoue, le microprogramme d'origine reste l'image principale.

REMARQUE Lorsque vous mettez à niveau le microprogramme, le point d'accès conserve les informations de configuration existantes.

Mise à niveau TFTP

Pour mettre à niveau le microprogramme sur un point d'accès via TFTP :

ÉTAPE 1 Sélectionnez **Administration** > **Update Firmware** dans le volet de navigation.

L'ID de produit (PID) ainsi que les versions du microprogramme active et inactive apparaissent.

ÉTAPE 2 Sélectionnez **TFTP for Transfer Method**.

ÉTAPE 3 Saisissez un nom (de 1 à 256 caractères) pour le fichier image dans le champ **Source File Name**, en incluant le chemin d'accès au répertoire qui contient l'image à télécharger.

Par exemple, pour télécharger l'image ap_upgrade.tar située dans le répertoire /share/builds/ap, saisissez : */share/builds/ap/ap_upgrade.tar*

Le fichier de mise à niveau du microprogramme fourni doit être un fichier tar. Pour la mise à niveau, n'essayez pas d'utiliser des fichiers bin ou des fichiers ayant un autre format ; ces types de fichiers ne fonctionnent pas.

Le nom de fichier ne peut pas contenir les éléments suivants : espaces, <, >, |, \, : , (,), &, ; , #, ? , *, ainsi que deux points successifs ou plus.

ÉTAPE 4 Renseignez **TFTP Server IPv4 Address**, puis cliquez sur **Upgrade**.

Le téléchargement du nouveau logiciel peut prendre quelques minutes. N'actualisez pas la page et n'ouvrez pas d'autre page pendant le téléchargement du nouveau logiciel, sous peine d'interrompre celui-ci. Une fois le processus terminé, le point d'accès redémarre et reprend son fonctionnement normal.

ÉTAPE 5 Pour vous assurer que la mise à niveau du microprogramme s'est correctement effectuée, connectez-vous à l'interface utilisateur, affichez la page Upgrade Firmware, puis vérifiez la version active du microprogramme.

Mise à niveau HTTP

Pour effectuer une mise à niveau via HTTP :

ÉTAPE 1 Sélectionnez **HTTP for Transfer Method**.

ÉTAPE 2 Si vous connaissez le nom du nouveau fichier et le chemin d'accès à celui-ci, saisissez-les dans le champ **Source File Name**. Sinon, cliquez sur le bouton **Browse** et recherchez le fichier image du microprogramme sur votre réseau.

Le fichier de mise à niveau du microprogramme fourni doit être un fichier tar. Pour la mise à niveau, n'essayez pas d'utiliser des fichiers bin ou des fichiers ayant un autre format ; ces types de fichiers ne fonctionnent pas.

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

Le téléchargement du nouveau logiciel peut prendre quelques minutes. N'actualisez pas la page et n'ouvrez pas d'autre page pendant le téléchargement du nouveau logiciel, sous peine d'interrompre celui-ci. Une fois le processus terminé, le point d'accès redémarre et reprend son fonctionnement normal.

ÉTAPE 4 Pour vous assurer que la mise à niveau du micrologiciel s'est correctement effectuée, connectez-vous à l'interface utilisateur, affichez la page Upgrade Firmware, puis vérifiez la version active du microprogramme.

Mise à niveau du micrologiciel

Le Périphérique WAP dispose d'une fonction de récupération du microprogramme qui permet de restaurer une image valide sur le Périphérique WAP après l'échec d'un téléchargement. En cas de panne de courant au cours du téléchargement d'une image, le Périphérique WAP est susceptible de ne pas pouvoir démarrer. Dans ce cas, bien que l'image ne soit pas utilisable, le fichier du programme d'amorçage qui charge l'image du microprogramme depuis la mémoire flash vers la RAM continue d'être fonctionnel. Le fichier du programme d'amorçage intègre un serveur HTTP permettant à l'administrateur de se connecter au Périphérique WAP via un port LAN et d'utiliser un navigateur Web pour télécharger et installer une nouvelle image du microprogramme.

Le Périphérique WAP passe en mode de récupération HTTP du microprogramme lorsque, au démarrage, le programme d'amorçage ne trouve d'image valide dans la mémoire flash. Dans ce mode, le programme d'amorçage définit le port réseau interne sur l'adresse IP statique suivante :

- Adresse IP : 192.168.1.254
- Masque de réseau : 255.255.255.0
- Passerelle par défaut : 192.168.1.1

Un serveur HTTP démarre et écoute les connexions client sur le port 80.

REMARQUE La page Firmware Recovery s'affiche dans l'utilitaire de configuration Web uniquement lorsqu'une image doit être restaurée.

Pour utiliser cette fonction afin de télécharger une nouvelle image du microprogramme :

ÉTAPE 1 Connectez directement un ordinateur au port LAN.

ÉTAPE 2 Configurez l'adresse IP et le masque sur l'ordinateur de gestion de telle façon qu'il se trouve sur le même sous-réseau que le commutateur.

REMARQUE Vous pouvez accéder au système via un réseau si l'adresse IP par défaut de la passerelle est 192.168.1.1.

ÉTAPE 3 Ouvrez un navigateur Web et saisissez l'adresse IP du commutateur dans la barre d'adresse (192.168.1.254).

REMARQUE Les fonctions de récupération HTTP du microprogramme prennent en charge les navigateurs suivants :

- Firefox 3.0 et versions ultérieures ;
- Internet Explorer 6 et versions ultérieures.

Une page Firmware Recovery s'affiche. Aucune authentification n'est requise.

La page Web affiche le PIC VID (ID du produit et ID du fournisseur), le numéro de série et l'adresse MAC du Périphérique WAP.

ÉTAPE 4 Sélectionnez **Browse** et sélectionnez une image du microprogramme valide à télécharger.

Une barre de progression montre l'avancement du téléchargement du fichier. Le message suivant s'affiche une fois le téléchargement terminé :

100% Complete
File downloaded successfully. Please wait while the file is being written to flash. System will automatically reboot.

Le fichier sélectionné par l'administrateur est téléchargé dans la mémoire RAM et validé pour les conditions suivantes :

- Le CRC du fichier est bon.
- Le fichier STK est compatible avec cette plate-forme.
- La taille du fichier STK se situe dans les limites de la partition (4,5 Mo sont réservés pour ce fichier).

Si ces conditions sont remplies, le fichier est enregistré dans la mémoire flash et le système est redémarré avec le nouveau microprogramme.

En cas d'échec d'une de ces vérifications, l'image n'est pas enregistrée dans la mémoire flash et le processus de récupération s'arrête. Vous pouvez redémarrer ce processus avec un fichier image correct.

En cas d'abandon du transfert suite à l'actualisation ou à la fermeture de la fenêtre du navigateur, la session est effacée et expire immédiatement. En cas d'abandon du transfert parce que le réseau est inaccessible, la session expire au bout de 45 secondes. Une fois la session expirée, vous pouvez relancer le processus de récupération.

Téléchargement/sauvegarde du fichier de configuration

Les fichiers de configuration du Périphérique WAP sont au format XML et contiennent toutes les informations relatives aux paramètres du périphérique WAP. Vous pouvez sauvegarder (télécharger) les fichiers de configuration sur un hôte réseau ou un serveur TFTP, afin de modifier manuellement le contenu ou de créer des sauvegardes. Une fois que vous avez modifié un fichier de configuration sauvegardé, vous pouvez le télécharger vers le point d'accès afin de modifier la configuration.

Le Périphérique WAP prend en charge les fichiers de configuration suivants :

- **Configuration de démarrage** : fichier de configuration enregistré dans la mémoire flash.

- **Configuration de secours** : fichier de configuration supplémentaire enregistré sur le périphérique WAP pour être utilisé comme sauvegarde.
- **Configuration miroir** : si la configuration de démarrage n'est pas modifiée pendant au moins 24 heures, elle est automatiquement enregistrée dans un fichier de configuration miroir. Le fichier de configuration miroir est un instantané d'une configuration de démarrage antérieure. La configuration miroir est conservée malgré les restaurations des paramètres d'usine. Elle peut donc être utilisée pour récupérer une configuration système après une restauration des paramètres d'usine en copiant la configuration miroir vers la configuration de démarrage.

REMARQUE En plus du téléchargement et du transfert de ces fichiers vers un autre système, vous pouvez les copier vers différents types de fichier sur le périphérique WAP. Reportez-vous à la section **Copie/enregistrement de la configuration**.

Sauvegarde d'un fichier de configuration

Pour sauvegarder (télécharger) le fichier de configuration vers un hôte réseau ou le serveur TFTP :

ÉTAPE 1 Sélectionnez **Administration** > **Download/Backup Configuration File** dans le volet de navigation.

ÉTAPE 2 Sélectionnez la méthode de transfert **Via TFTP** ou **Via HTTP/HTTPS** dans **Transfer Method**.

ÉTAPE 3 Sélectionnez l'action d'enregistrement **Backup (AP to PC)** dans **Save Action**.

ÉTAPE 4 Pour une sauvegarde TFTP uniquement, renseignez **Destination File Name** avec une extension .xml. Incluez également le chemin d'accès à l'emplacement de stockage du fichier sur le serveur, puis renseignez **TFTP Server IPv4 Address**.

Le nom de fichier ne peut pas contenir les caractères suivants : espaces, <, >, |, \, : , (,), &, ; , #, ? , *, ainsi que deux points successifs ou plus.

ÉTAPE 5 Pour une sauvegarde TFTP uniquement, renseignez **TFTP Server IPv4 Address**.

ÉTAPE 6 Sélectionnez le fichier de configuration que vous souhaitez sauvegarder :

- **Configuration de démarrage** : type de fichier de configuration utilisé lors du dernier démarrage du périphérique WAP. Ce fichier n'inclut pas les modifications de configuration appliquées mais non encore enregistrées sur le périphérique WAP.

- **Configuration de sauvegarde** : type de fichier de configuration de sauvegarde enregistré sur le périphérique WAP.
- **Configuration miroir** : si la configuration de démarrage n'est pas modifiée pendant au moins 24 heures, elle est automatiquement enregistrée dans un fichier de configuration miroir. Le fichier de configuration miroir est un instantané d'une configuration de démarrage antérieure. La configuration miroir est conservée malgré les restaurations des paramètres d'usine. Elle peut donc être utilisée pour récupérer une configuration système après une restauration des paramètres d'usine en copiant la configuration miroir vers la configuration de démarrage.

ÉTAPE 7 Cliquez sur **Save** pour commencer la sauvegarde. Pour les sauvegardes HTTP, une fenêtre s'affiche afin de vous permettre d'accéder à l'emplacement souhaité pour l'enregistrement du fichier.

Téléchargement d'un fichier de configuration

Vous pouvez télécharger un fichier vers le Périphérique WAP pour mettre à jour la configuration ou restaurer le Périphérique WAP à une configuration précédemment sauvegardée.

Pour télécharger un fichier de configuration vers le périphérique WAP :

ÉTAPE 1 Sélectionnez **Administration** > **Download/Backup Configuration File** dans le volet de navigation.

ÉTAPE 2 Sélectionnez la méthode de transfert **Via TFTP** ou **Via HTTP/HTTPS** dans **Transfer Method**.

ÉTAPE 3 Sélectionnez l'action d'enregistrement **Download (PC to AP)** dans **Save Action**.

ÉTAPE 4 Pour un téléchargement TFTP uniquement, renseignez **Source File Name** avec une extension .xml. Incluez le chemin d'accès à l'emplacement du fichier sur le serveur, puis renseignez **TFTP Server IPv4 Address**.

Le nom de fichier ne peut pas contenir les caractères suivants : espaces, <, >, |, \, : , (,), &, ; , #, ? , *, ainsi que deux points successifs ou plus.

ÉTAPE 5 Sélectionnez le fichier de configuration sur le Périphérique WAP que vous souhaitez remplacer par le fichier téléchargé : la **configuration de démarrage** ou la **configuration de sauvegarde**.

Si le fichier téléchargé écrase le fichier de configuration de démarrage et que le fichier réussit un contrôle de validité, la configuration téléchargée prendra effet au prochain redémarrage du Périphérique WAP.

ÉTAPE 6 Cliquez sur **Save** pour commencer la mise à niveau ou la sauvegarde. Pour les téléchargements HTTP, une fenêtre s'affiche afin de vous permettre de sélectionner le fichier à télécharger. Une fois le téléchargement terminé, une fenêtre vous confirme le succès de l'opération.

AVERTISSEMENT Veillez à ce que le Périphérique WAP soit en permanence alimenté lors du téléchargement du fichier de configuration. En cas de panne de courant lors du téléchargement du fichier de configuration, ce dernier est perdu et le processus doit être redémarré.

Propriétés des fichiers de configuration

La page Configuration Files Properties vous permet d'effacer le fichier de configuration de démarrage ou de sauvegarde. Si vous effacez le fichier de configuration de démarrage, le fichier de configuration de sauvegarde s'activera lors du prochain redémarrage du Périphérique WAP.

Pour supprimer le fichier de configuration de démarrage ou de configuration de sauvegarde :

ÉTAPE 1 Sélectionnez **Administration** > **Configuration Files Properties** dans le volet de navigation.

ÉTAPE 2 Sélectionnez le type de fichier **Startup Configuration** ou **Backup Configuration**.

ÉTAPE 3 Cliquez sur **Clear Files**.

Copie/enregistrement de la configuration

La page Copy/Save Configuration vous permet de copier des fichiers au sein du système de fichiers du Périphérique WAP. Vous pouvez par exemple copier le fichier de configuration de sauvegarde dans le type de fichier de configuration de démarrage, afin qu'il soit utilisé lors du prochain démarrage du périphérique WAP.

Pour copier un fichier vers un autre type de fichier :

ÉTAPE 1 Sélectionnez **Administration** > **Copy/Save Configuration** dans le volet de navigation.

ÉTAPE 2 Sélectionnez le **Source File Name** :

- **Configuration de démarrage** : type de fichier de configuration utilisé lors du dernier démarrage du périphérique WAP. Ce fichier n'inclut pas les modifications de configuration appliquées mais non encore enregistrées sur le périphérique WAP.
- **Configuration de sauvegarde** : type de fichier de configuration de sauvegarde enregistré sur le périphérique WAP.
- **Configuration miroir** : si la configuration de démarrage n'est pas modifiée pendant au moins 24 heures, elle est automatiquement enregistrée dans un fichier de configuration miroir. Le fichier de configuration miroir est un instantané d'une configuration de démarrage antérieure. La configuration miroir est conservée malgré les restaurations des paramètres d'usine. Elle peut donc être utilisée pour récupérer une configuration système après une restauration des paramètres d'usine en copiant la configuration miroir vers la configuration de démarrage.

ÉTAPE 3 Pour **Destination File Name**, sélectionnez le type de fichier à remplacer par le fichier que vous copiez.

ÉTAPE 4 Cliquez sur **Save** pour commencer la copie.

Une fois l'opération terminée, une fenêtre affiche le message Copy Operation Successful.

Redémarrage

Vous pouvez utiliser la page Reboot pour redémarrer le Périphérique WAP.

ÉTAPE 1 Pour redémarrer le WAP, sélectionnez **Administration** > **Reboot** dans le volet de navigation.

ÉTAPE 2 Sélectionnez l'une des options suivantes :

- **Reboot** : redémarre le WAP en utilisant la configuration de démarrage.

- **Reboot to Factory Default** : redémarre le WAP en utilisant le fichier de configuration par défaut d'origine. Tous les paramètres personnalisés sont perdus.

Une fenêtre s'affiche pour vous permettre de confirmer ou d'annuler le redémarrage. Il est possible que la session de gestion en cours soit arrêtée.

ÉTAPE 3 Cliquez sur **OK** pour redémarrer.

Discovery—Bonjour

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.

Le Périphérique WAP notifie les types de service suivants :

- **Description d'appareils spécifiques à Cisco** (csco-sb) : ce service permet aux clients de détecter les périphériques WAP Cisco et d'autres produits déployés sur des réseaux de petites entreprises.
- **Interfaces utilisateur de gestion** : ce service identifie les interfaces de gestion disponibles sur le périphérique WAP (HTTP et SNMP).

Lorsqu'un périphérique WAP compatible avec Bonjour est connecté à un réseau, tout client Bonjour peut détecter l'utilitaire de configuration et y accéder sans configuration préalable.

Un administrateur système peut utiliser un module d'extension Internet Explorer installé pour détecter le périphérique WAP. L'utilitaire de configuration Web apparaît sous forme d'onglet dans le navigateur.

Bonjour fonctionne sur les réseaux IPv4 et IPv6.

Pour activer la détection du périphérique WAP via Bonjour :

ÉTAPE 1 Sélectionnez **Administration** > **Discovery - Bonjour** dans le volet de navigation.

ÉTAPE 2 Cochez la case **Activer**.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Capture de paquets

La fonction de capture de paquets sans fil permet de capturer et stocker les paquets reçus et transmis par le périphérique WAP. Les paquets capturés peuvent ensuite être analysés par un analyseur de protocole réseau pour des opérations de dépannage ou d'optimisation des performances. Les deux méthodes de capture de paquets sont les suivantes :

- Méthode de capture locale : les paquets capturés sont stockés dans un fichier sur le périphérique WAP. Le périphérique WAP peut transférer le fichier vers un serveur TFTP. Le fichier est mis au format pcap et peut être examiné à l'aide d'outils comme Wireshark et OmniPeek.
- Méthode de capture distante : les paquets capturés sont redirigés en temps réel vers un ordinateur externe qui exécute l'outil Wireshark.

Le périphérique WAP peut capturer les types de paquets suivants :

- Les paquets 802.11 reçus et transmis sur les interfaces radio. Les paquets capturés sur les interfaces radio incluent l'en-tête 802.11.
- Les paquets 802.3 reçus et transmis sur l'interface Ethernet.
- Les paquets 802.3 reçus et transmis sur les interfaces logiques internes, telles que les interfaces VAP et WDS.

Cliquez sur **Administration > Packet Capture** pour afficher la page Packet Capture. Depuis la page Packet Capture, vous pouvez :

- Définir les paramètres de capture de paquets.
- Démarrer une capture de paquets locale ou distante.
- Afficher l'état de la capture de paquets en cours.
- Télécharger un fichier de capture de paquets.

Configuration de la capture de paquets

La zone Packet Capture Configuration vous permet de définir les paramètres d'une capture de paquets et de lancer cette dernière.

Pour définir les paramètres d'une capture de paquets :

ÉTAPE 1 Définissez les paramètres suivants :

- **Capture Beacons** : active ou désactive la capture des balises 802.11 détectées ou transmises par radio.
- **Promiscuous Capture** : active ou désactive le mode de proximité lorsque la capture est active.

  En mode de proximité, la radio reçoit tout le trafic sur le canal, y compris le trafic qui n'est pas destiné à ce périphérique WAP. Lorsque la radio fonctionne en mode de proximité, elle continue à servir les clients associés. Les paquets qui ne sont pas destinés au périphérique WAP ne sont pas transférés.

  Lorsque la capture est terminée, la radio repasse en mode de non-proximité.
- **Radio Client Filter** : active ou désactive le filtre de client WLAN de façon à capturer uniquement les trames transmises à un client WLAN ayant une adresse MAC spécifiée ou reçues de celui-ci.
- **Client Filter MAC Address** : spécifie l'adresse MAC pour le filtrage de client WLAN.

  REMARQUE Le filtre MAC est uniquement actif lorsqu'une capture est réalisée sur une interface 802.11.
- **Packet Capture Method** : sélectionnez l'une des options suivantes :
  - **Local File** : les paquets capturés sont stockés dans un fichier sur le périphérique WAP.
  - **Remote** : les paquets capturés sont redirigés en temps réel vers un ordinateur externe qui exécute l'outil Wireshark.

ÉTAPE 2 En fonction de la méthode sélectionnée, suivez les étapes de la section Local Packet Capture ou Remote Packet Capture pour continuer.

REMARQUE Les modifications apportées aux paramètres de configuration de la capture de paquets prendront effet une fois la capture de paquets redémarrée. La modification des paramètres alors que la capture de paquets est en cours d'exécution n'a

aucune incidence sur la session de capture de paquets active. Pour commencer à utiliser les nouvelles valeurs des paramètres, vous devez arrêter puis redémarrer une session de capture de paquets existante.

Capture locale de paquets

Pour initier une capture de paquets locale :

ÉTAPE 1 Assurez-vous que **Local File** est sélectionné pour **Packet Capture Method**.

ÉTAPE 2 Définissez les paramètres suivants :

- **Capture Interface** : saisissez un type d'interface de capture pour la capture de paquets :
  - **radio1** : trafic 802.11 sur l'interface radio.
  - **eth0** : trafic 802.3 sur le port Ethernet.
  - **VAP0** : trafic VAP0.
  - **VAP1** à **VAP15**, si configuré : trafic sur le VAP spécifié.
  - **brtrunk** : interface bridge Linux dans le périphérique WAP.
- **Capture Duration** : saisissez la durée en secondes de la capture. La plage est comprise entre 10 et 3 600. La valeur par défaut est 60.
- **Max Capture File Size** : saisissez la taille maximale autorisée pour le fichier de capture en Ko. La plage est comprise entre 64 et 4 096. La valeur par défaut est 1 024.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

ÉTAPE 4 Cliquez sur **Start Capture**.

En mode Packet File Capture, le périphérique WAP stocke les paquets capturés dans le système de fichiers RAM. Une fois l'activation terminée, la capture de paquets s'effectue jusqu'à ce qu'un des événements suivants se produise :

- La durée de capture atteint la durée configurée.
- Le fichier de capture atteint sa taille maximale.
- L'administrateur arrête la capture.

La zone Packet Capture Status de la page indique l'état d'une capture de paquets si celle-ci est active sur le périphérique WAP.

- **Current Capture Status** : indique si la capture de paquets est en cours d'exécution ou arrêtée.
- **Packet Capture Time** : durée de capture écoulée.
- **Packet Capture File Size** : taille actuelle du fichier de capture.

Cliquez sur **Refresh** pour afficher les dernières données issues du périphérique WAP.

REMARQUE Pour arrêter la capture d'un fichier de paquets, cliquez sur **Stop Capture**.

Capture distante de paquets

La fonction Remote Packet Capture vous permet de spécifier un port distant comme destination des captures de paquets. Cette fonction opère conjointement avec l'outil d'analyse réseau Wireshark pour Windows. Un serveur de capture de paquets est exécuté sur le périphérique WAP et envoie les paquets capturés via une connexion TCP vers l'outil Wireshark. Wireshark est un outil open source disponible gratuitement ; vous pouvez le télécharger à l'adresse http://www.wireshark.org.

Un ordinateur Microsoft Windows exécutant l'outil Wireshark vous permet d'afficher, de journaliser et d'analyser le trafic capturé. La fonction de capture de paquets distante est une fonction standard de l'outil Wireshark pour Windows. La version Linux ne fonctionne pas avec le périphérique WAP.

Lorsque le mode de capture distante est utilisé, le périphérique WAP ne stocke pas les données capturées localement dans son système de fichiers.

Si un pare-feu est installé entre l'ordinateur Wireshark et le périphérique WAP, le trafic de ces ports doit être autorisé à traverser le pare-feu. Le pare-feu doit aussi être configuré pour autoriser l'ordinateur Wireshark à initier une connexion TCP vers le périphérique WAP.

Pour initier une capture distante sur un périphérique WAP :

ÉTAPE 1 Cliquez sur **Administration** > **Packet Capture**.

ÉTAPE 2 Activez **Promiscuous Capture**.

ÉTAPE 3 Pour **Packet Capture Method**, sélectionnez **Remote**.

ÉTAPE 4 Pour **Remote Capture Port**, utilisez le port par défaut (2002) ou si vous utilisez un autre port que celui par défaut, saisissez le numéro de port souhaité pour la connexion de Wireshark au périphérique WAP. La plage de ports est comprise entre 1 025 et 65 530.

ÉTAPE 5 Si vous souhaitez enregistrer les paramètres en vue d'une utilisation ultérieure, cliquez sur **Save**. (Cependant, la sélection de **Remote** comme **Packet Capture Method** n'est pas enregistrée.)

ÉTAPE 6 Cliquez sur **Start Capture**.

Pour lancer l'outil d'analyse réseau Wireshark pour Microsoft Windows :

ÉTAPE 1 Sur le même ordinateur, lancez l'outil Wireshark.

ÉTAPE 2 Dans le menu, sélectionnez **Capture** > **Options**. Une fenêtre contextuelle s'affiche.

ÉTAPE 3 Pour **Interface**, sélectionnez **Remote**. Une fenêtre contextuelle s'affiche.

ÉTAPE 4 Pour **Host**, saisissez l'adresse IP du périphérique WAP.

ÉTAPE 5 Pour **Port**, saisissez le numéro de port du WAP. Par exemple, saisissez 2002 si vous avez utilisé le port par défaut ou saisissez le numéro de port si vous avez utilisé un autre port que le port par défaut.

ÉTAPE 6 Cliquez sur **OK**.

ÉTAPE 7 Sélectionnez l'interface à partir de laquelle vous devez capturer les paquets. Dans la fenêtre contextuelle Wireshark, en regard de l'adresse IP, une liste déroulante vous permet de sélectionner les interfaces. L'interface peut être l'une des suivantes :

Interface bridge Linux dans le périphérique WAP
`--rpcap://[192.168.1.220]:2002/brtrunk`
Interface LAN filaire
`-- rpcap://[192.168.1.220]:2002/eth0`
Trafic VAP0 sur radio 1
`-- rpcap://[192.168.1.220]:2002/wlan0`
Trafic 802.11
`-- rpcap://[192.168.1.220]:2002/radio1`
Sur WAP321, VAP1 ~ trafic VAP7
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7`
Sur WAP321, VAP1 ~ trafic VAP3
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3`

Vous pouvez effectuer le suivi simultané de quatre interfaces maximum sur le périphérique WAP. Toutefois, vous devez démarrer une session Wireshark distincte pour chaque interface. Pour initier des sessions de capture distante supplémentaires, répétez les étapes de configuration Wireshark ; aucune configuration n'est requise sur le périphérique WAP.

REMARQUE Le système utilise quatre numéros de port consécutifs, en commençant par le port configuré pour les sessions de capture de paquets distante. Vérifiez que vous disposez de quatre numéros de port consécutifs. Si vous n'utilisez pas le port par défaut, nous vous recommandons d'utiliser un numéro de port supérieur à 1 024.

Lorsque vous capturez le trafic sur l'interface radio, vous pouvez désactiver la capture des balises, mais les autres trames de contrôle 802.11 sont toujours envoyées à Wireshark. Vous pouvez configurer un filtre d'affichage de façon à afficher uniquement :

- Les trames de données dans le suivi
- Le trafic sur des BSSID (Basic Service Set ID) spécifiques
- Le trafic entre deux clients

Voici quelques exemples de filtres d'affichage utiles :

- Exclure les balises et les trames ACK/RTS/CTS :

  !(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)

- Les trames de données uniquement :

  wlan.fc.type == 2

- Le trafic sur un BSSID spécifique :

  wlan.bssid == 00:02:bc:00:17:d0

- Tout le trafic de et vers un client spécifique :

  wlan.addr == 00:00:e8:4e:5f:8e

En mode de capture distante, le trafic est envoyé vers l'ordinateur qui exécute Wireshark via l'une des interfaces réseau. Selon l'emplacement de l'outil Wireshark, le trafic peut être envoyé sur une interface Ethernet ou l'une des radios. Pour éviter un flux de trafic causé par le suivi des paquets, le périphérique WAP installe automatiquement un filtre de capture afin d'éliminer tous les paquets destinés à l'application Wireshark. Par exemple, si le port IP Wireshark est configuré sur 58 000, alors le filtre de capture suivant est automatiquement installé sur le périphérique WAP :

not portrange 58000-58004

Pour éviter les problèmes de performances et de sécurité, le mode de capture de paquets n'est pas enregistré dans la NVRAM du périphérique WAP ; si le périphérique WAP est réinitialisé, le mode de capture est désactivé et vous devez le réactiver pour rétablir la capture du trafic. Les paramètres de capture de paquets (autres que le mode) sont enregistrés dans la NVRAM.

L'activation de la fonction de capture de paquets peut engendrer un problème de sécurité : des clients non autorisés sont susceptibles de pouvoir se connecter au périphérique WAP et d'effectuer un suivi des données utilisateur. En outre, les performances du périphérique WAP sont dégradées pendant la capture de paquets et cet impact négatif continue à être détecté dans une moindre mesure même lorsqu'il n'y a pas de session Wireshark active. Pour réduire cet impact sur les performances du périphérique WAP pendant la capture du trafic, installez des filtres de capture afin de contrôler le trafic envoyé vers l'outil Wireshark. Pendant la capture du trafic 802.11, les trames capturées sont pour une grande partie des balises (généralement envoyées toutes les 100 ms par tous les points d'accès). Même si Wireshark prend en charge un filtre d'affichage pour les trames de balise, il ne prend pas en charge un filtre de capture empêchant le périphérique WAP de réacheminer les paquets de balise capturés vers l'outil Wireshark. Pour réduire l'impact de la capture des balises 802.11 sur les performances, désactivez le mode de capture des balises.

Téléchargement du fichier de capture de paquets

Vous pouvez télécharger un fichier de capture par TFTP vers un serveur TFTP configuré, ou par HTTP(S) vers un ordinateur. Une capture est automatiquement arrêtée dès le déclenchement de la commande de téléchargement du fichier de capture.

Puisque le fichier de capture est stocké dans le système de fichiers RAM, il disparaît si le périphérique WAP est réinitialisé.

Pour télécharger un fichier de capture de paquets via TFTP :

ÉTAPE 1 Sélectionnez **Use TFTP to download the capture file**.

ÉTAPE 2 Dans **TFTP Server Filename**, saisissez le nom de fichier du serveur TFTP à télécharger s'il diffère du nom par défaut. Par défaut, les paquets capturés sont stockés dans le fichier de dossiers /tmp/apcapture.pcap sur le périphérique WAP.

ÉTAPE 3 Renseignez **TFTP Server IPv4 Address** dans le champ prévu à cet effet.

ÉTAPE 4 Cliquez sur **Download**.

Pour télécharger un fichier de capture de paquets via HTTP :

ÉTAPE 1 Décochez **Use TFTP to download the captured file**.

ÉTAPE 2 Cliquez sur **Download**. Une fenêtre de confirmation s'affiche.

ÉTAPE 3 Cliquez sur **OK**. Une boîte de dialogue apparaît. Celle-ci vous permet de choisir l'emplacement d'enregistrement du fichier sur le réseau.

Informations de support

La page Support Information vous permet de télécharger un fichier texte qui contient des informations de configuration détaillées sur le point d'accès. Le fichier inclut les informations de version matérielle et logicielle, les adresses MAC et IP, l'état d'administration et opérationnel des fonctions, les paramètres définis par l'utilisateur, les statistiques de trafic, etc. Vous pouvez fournir ce fichier texte aux membres de l'assistance technique pour les aider à résoudre les différents problèmes.

Pour afficher la page Support Information, sélectionnez **Administration > Support Information** dans le volet de navigation.

Cliquez sur **Download** pour générer le fichier à partir des paramètres système actuels. Après un bref instant, une fenêtre s'affiche pour vous permettre d'enregistrer le fichier sur votre ordinateur.

4

Réseau local

Ce chapitre explique comment configurer les paramètres de port, de réseau et d'horloge des périphériques WAP.

Il contient les rubriques suivantes :

- **Paramètres de port**
- **Paramètres d'adresse VLAN et IPv4**
- **Adresses IPv6**

Paramètres de port

La page Port Settings permet d'afficher et de configurer les paramètres du port qui connecte physiquement le périphérique WAP à un réseau local.

Pour afficher et configurer les paramètres de réseau local :

ÉTAPE 1 Sélectionnez **LAN** > **Port Settings** dans le volet de navigation.

La zone Operational Status indique le type de port utilisé pour le port de réseau local ainsi que les caractéristiques de liaison, tels que configurés dans la zone Administrative Settings. En cas de modification des paramètres lors de la configuration ou de la négociation automatique, cliquez sur **Actualiser** pour afficher les derniers paramètres.

ÉTAPE 2 Activez ou désactivez l'option **Auto Negotiation**.

- Lorsque cette option est activée, le port négocie avec son partenaire de liaison afin de définir la vitesse de liaison la plus rapide et le mode duplex disponible.
- Si cette option est désactivée, vous pouvez configurer manuellement la vitesse du port et le mode duplex.

ÉTAPE 3 Si la négociation automatique est désactivée, sélectionnez un **Débit du port** (10/100 Mbit/s pour le WAP121 et 10/100/1000 Mbit/s pour le WAP321) et choisissez le mode Duplex intégral ou Semi-duplex.

ÉTAPE 4 Activez ou désactivez l'option **Green Ethernet Mode** (WAP321 uniquement).

- Le mode Green Ethernet est un mode basse puissance automatique qui permet de diminuer la consommation énergétique des puces en cas d'absence de signal émanant d'un partenaire de liaison. Le mode Green Ethernet fonctionne avec la négociation automatique de port activée ou désactivée.
- Lorsque le mode Green Ethernet est activé, le périphérique WAP passe automatiquement en mode basse puissance en cas de perte d'énergie sur la ligne et il reprend un fonctionnement normal lorsqu'il détecte de l'énergie.

ÉTAPE 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Paramètres d'adresse VLAN et IPv4

Vous pouvez utiliser la page VLAN and IPv4 Address Settings pour configurer les paramètres de l'interface LAN, y compris l'affectation d'adresse IPv4 statique ou dynamique.

Pour configurer les paramètres de réseau local :

ÉTAPE 1 Sélectionnez **LAN** > **VLAN and IPv4 Address** dans le volet de navigation.

La page affiche les paramètres globaux et les paramètres IPv4. La zone Global Settings indique l'adresse MAC du port de l'interface LAN. Ce champ est en lecture seule.

ÉTAPE 2 Configurez les paramètres globaux suivants :

- **Untagged VLAN** : active ou désactive le balisage de VLAN. Lorsque cette option est activée (paramètre par défaut), tout le trafic est balisé avec un ID de VLAN.

  Par défaut, la totalité du trafic sur le point d'accès utilise le VLAN 1, à savoir le VLAN non balisé par défaut. Cela signifie que l'ensemble du trafic est non balisé jusqu'à la désactivation du VLAN non balisé, la modification de l'ID de VLAN du trafic non balisé ou la modification de l'ID de VLAN d'un point d'accès virtuel (VAP) ou d'un client utilisant un serveur RADIUS.

- **Untagged VLAN ID** : indique un nombre compris entre 1 et 4094 pour l'ID de VLAN non balisé. La valeur par défaut est 1. Le trafic sur le VLAN que vous spécifiez dans ce champ n'est pas balisé avec un ID de VLAN lors de son transfert sur le réseau.

  VLAN 1 est à la fois le VLAN non balisé par défaut et le VLAN de gestion par défaut. Si vous souhaitez séparer le trafic de gestion du trafic du VLAN non balisé, configurez le nouvel ID de VLAN au niveau de votre routeur, puis utilisez ce nouvel ID de VLAN sur votre périphérique WAP.

- **Management VLAN ID** : VLAN associé à l'adresse IP que vous utilisez pour accéder au périphérique WAP. Entrez un nombre compris entre 1 et 4094 pour l'ID de VLAN de gestion. La valeur par défaut est 1.

  Ce VLAN est également le VLAN non balisé par défaut. Si vous possédez déjà un VLAN de gestion configuré sur votre réseau avec un ID de VLAN différent, vous devez modifier l'ID de VLAN du VLAN de gestion sur le périphérique WAP.

ÉTAPE 3 Configurez les paramètres IPv4 suivants :

- **Connection Type** : par défaut, le client DHCP sur le Cisco WAP121 et WAP321 diffuse automatiquement les demandes d'informations de réseau. Si vous voulez utiliser une adresse IP statique, vous devez désactiver le client DHCP et configurer manuellement l'adresse IP ainsi que les autres informations de réseau.

  Sélectionnez l'une des valeurs de la liste ci-dessous :

  - **DHCP** : le Périphérique WAP acquiert son adresse IP d'un serveur DHCP sur le réseau local.
  - **Static IP** : vous configurez manuellement l'adresse IPv4. La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (192.0.2.10).

- **Static IP Address, Subnet Mask et Default Gateway** : si vous avez choisi d'affecter une adresse IP statique, entrez ici les informations IP.

- **Domain Name Servers** : sélectionnez une option dans la liste suivante :

  - **Dynamic** : le Périphérique WAP acquiert les adresses de serveur DNS d'un serveur DHCP sur le réseau local.
  - **Manual** : vous configurez manuellement une ou plusieurs adresses de serveur DNS. Entrez jusqu'à deux adresses IP dans les zones de texte.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Adresses IPv6

Utilisez la page IPv6 Addresses pour configurer le périphérique WAP de telle sorte qu'il utilise les adresses IPv6.

Pour configurer les paramètres d'adresse IPv6 :

ÉTAPE 1 Sélectionnez **LAN** > **IPv6 Addresses** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **IPv6 Connection Type** : choisissez comment le périphérique WAP obtient une adresse IPv6 :
  - **DHCPv6** : l'adresse IPv6 est affectée par un serveur DHCPv6.
  - **Static IPv6** : vous configurez manuellement l'adresse IPv6. La forme de l'adresse IPv6 doit être similaire à celle-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).
- **IPv6 Administration Mode** : active l'accès de gestion IPv6.
- **IPv6 Auto Configuration Administration Mode** : active la configuration automatique des adresses IPv6 sur le périphérique WAP.

  Lorsque cette option est activée, le Périphérique WAP apprend ses adresses et sa passerelle IPv6 en traitant les messages de notification de routeur reçus sur le port LAN. Le périphérique WAP peut posséder plusieurs adresses IPv6 configurées automatiquement.
- **Static IPv6 Address** : adresse IPv6 statique. Le périphérique WAP peut posséder une adresse IPv6 statique, même si des adresses ont déjà été configurées automatiquement.
- **Static IPv6 Address Prefix Length** : longueur de préfixe de l'adresse statique, à savoir un entier compris entre 0 et 128. La valeur par défaut est 0.
- **Static IPv6 Address Status** : une des valeurs suivantes apparaît :

- **Operational** : l'adresse IP a été vérifiée comme étant unique sur le réseau local et elle est utilisable sur l'interface.
- **Tentative** : le périphérique WAP initie automatiquement un processus de détection des adresses en double (DAD, Duplicate Address Detection) lors de l'affectation d'une adresse IP statique. Une adresse IPv6 reste à l'état provisoire pendant que le système vérifie qu'elle est unique sur le réseau. Lorsqu'elle se trouve dans cet état, l'adresse IPv6 ne peut pas être utilisée pour transmettre ou recevoir le trafic normal.
- **Vide (aucune valeur)** : aucune adresse IP n'est affectée ou l'adresse affectée n'est pas opérationnelle.

- **IPv6 Autoconfigured Global Addresses** : si une ou plusieurs adresses IPv6 ont été affectées automatiquement au périphérique WAP, ces adresses sont répertoriées ici.
- **IPv6 Link Local Address** : adresse IPv6 utilisée par la liaison physique locale. L'adresse locale de liaison n'est pas configurable et elle est affectée à l'aide du processus de détection de voisinage IPv6.
- **Default IPv6 Gateway** : passerelle IPv6 par défaut configurée de manière statique.
- **IPv6 DNS Nameservers** : sélectionnez l'une des valeurs suivantes :
  - **Dynamic** : les serveurs de noms DNS sont appris dynamiquement par le biais de DHCPv6.
  - **Manual** : spécifiez jusqu'à deux serveurs de noms DNS IPv6 dans les champs prévus à cet effet.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

5

Sans fil

Ce chapitre décrit comment configurer les propriétés de fonctionnement de la radio sans fil.

Il contient les rubriques suivantes :

- **Radio**
- **Détection de point d'accès non autorisé**
- **Networks**
- **Planificateur**
- **Association de planificateur**
- **Utilisation de la bande passante**
- **Filtrage MAC**
- **Pont WDS**
- **Pont de groupe de travail**
- **Qualité de service**
- **Configuration de WPS**
- **Processus WPS**

Radio

Les paramètres radio contrôlent directement le comportement de la radio dans le périphérique WAP et son interaction avec le support physique, à savoir le type de signal émis par le périphérique WAP et la façon dont il procède.

Pour définir les paramètres radio :

ÉTAPE 1 Sélectionnez **Wireless** > **Radio** dans le volet de navigation.

ÉTAPE 2 Dans la zone Global Settings, configurez le **TSPEC Violation Interval**, qui est la durée en secondes pendant laquelle le périphérique WAP doit consigner les clients associés qui ne respectent pas les procédures de contrôle d'admission obligatoires. La consignation s'effectue via le journal système et les déroutements SNMP. Entrez une durée comprise entre 0 et 900 secondes. La valeur par défaut est 300 secondes.

ÉTAPE 3 Dans la zone Basic Settings, définissez les paramètres suivants :

REMARQUE Les réglementations locales peuvent interdire l'utilisation de certains modes radio. Les modes ne sont pas tous disponibles dans l'ensemble des pays.

- **Radio** : active ou désactive l'interface radio. Par défaut, la radio est désactivée.
- **MAC Address** : adresse Media Access Control (MAC) de l'interface. L'adresse MAC est attribuée par le fabricant et ne peut pas être modifiée.
- **Mode** : norme IEEE 802.11 et fréquence utilisées par la radio. l'un des modes disponibles :
  - 802.11a—Seuls les clients 802.11a peuvent se connecter au périphérique WAP.
  - 802.11b/g—Les clients 802.11b et 802.11g peuvent se connecter au périphérique WAP.
  - 802.11a/n—Les clients 802.11a et 802.11n fonctionnant à la fréquence 5-GHz peuvent se connecter au périphérique WAP.
  - 802.11b/g/n (par défaut)—Les clients 802.11b, 802.11g et 802.11n fonctionnant à la fréquence 2,4 GHz peuvent se connecter au périphérique WAP.
  - 5 GHz 802.11n—Seuls les clients 802.11n fonctionnant à la fréquence 5 GHz peuvent se connecter au périphérique WAP.
  - 2,4 GHz 802.11n—Seuls les clients 802.11n fonctionnant à la fréquence 2,4 GHz peuvent se connecter au périphérique WAP.

- **Channel Bandwidth** : la spécification 802.11n autorise un canal de 20/40 MHz en plus du canal de 20 MHz hérité qui est disponible avec les autres modes. Le canal de 20/40 MHz offre des débits de données plus élevés, mais laisse moins de canaux à la disposition des autres périphériques de 2,4 GHz et 5 GHz.

  Par défaut, lorsque le mode radio inclut 802.11n, la bande passante du canal est définie sur 20/40 MHz pour autoriser les deux largeurs de bande. Définissez le champ sur 20 MHz pour restreindre l'utilisation de la bande passante du canal à un canal de 20 MHz.

- **Primary Channel** (modes 802.11n avec une bande passante de 20/40 MHz seulement) : on peut considérer qu'un canal de 40 MHz se compose de deux canaux de 20 MHz qui sont contigus dans le domaine de fréquence. On appelle souvent ces deux canaux de 20 MHz le canal principal et le canal secondaire. Le canal principal est utilisé pour les clients 802.11n qui prennent uniquement en charge une bande passante de canal de 20 MHz et pour les clients hérités.

  Sélectionnez l'une des options suivantes :

  - **Upper** : définit le canal principal en tant que canal de 20 MHz supérieur dans la bande de 40 MHz.
  - **Lower** : définit le canal principal en tant que canal de 20 MHz inférieur dans la bande de 40 MHz. Lower est la sélection par défaut.

- **Channel** : partie du spectre radio utilisée par la radio pour la transmission et la réception.

  La plage des canaux disponibles est déterminée par le mode de l'interface radio et le paramètre de code de pays. Si vous sélectionnez **Auto** pour le paramètre de canal, le périphérique WAP recherche les canaux disponibles et sélectionne le canal ayant le moins de trafic.

  Chaque mode offre plusieurs canaux en fonction du spectre attribué sous licence par les autorités nationales et internationales, telles que la Federal Communications Commission (FCC) ou la International Telecommunication Union (ITU-R).

ÉTAPE 4 Dans la zone Advanced Settings, définissez les paramètres suivants :

- **Short Guard Interval Supported** : ce champ est uniquement disponible si le mode radio sélectionné inclut 802.11n.

L'intervalle de sûreté est le temps mort, en nanosecondes, entre les symboles OFDM. L'intervalle de sûreté empêche les interférences ISI (Inter-Symbol Interference) et ICI (Inter-Carrier Interference). Le mode 802.11n permet dans cet intervalle de sûreté de diminuer la définition a et g de 800 nanosecondes à 400 nanosecondes. La diminution de l'intervalle de sûreté peut entraîner une amélioration de 10 pour cent du débit de données.

Le client avec lequel le périphérique WAP communique doit aussi prendre en charge l'intervalle de sûreté court.

Sélectionnez l'une des options suivantes :

- **Yes** : le périphérique WAP transmet les données avec un intervalle de sûreté de 400 nanosecondes lorsqu'il communique avec des clients qui prennent aussi en charge l'intervalle de sûreté court. Yes est la sélection par défaut.
- **No** : le périphérique WAP transmet les données avec un intervalle de sûreté de 800 nanosecondes.

- **Protection** : la fonction de protection contient les règles garantissant que les transmissions 802.11 ne créent pas d'interférences avec les stations ou applications héritées. Par défaut, la protection est activée (Auto). Lorsque la protection est activée, celle-ci est appelée si des périphériques hérités se trouvent à portée du périphérique WAP.

  Vous pouvez désactiver la protection (Off) ; cependant, les clients hérités ou les périphériques WAP à portée peuvent être affectés par les transmissions 802.11n. La protection est également disponible lorsque le mode est 802.11b/g. Si la protection est activée dans ce mode, elle protège les clients 802.11b et les périphériques WAP contre les transmissions 802.11g.

  REMARQUE Ce paramètre n'empêche pas le client de s'associer au périphérique WAP.

- **Beacon Interval** : intervalle entre la transmission des trames de balise. Le périphérique WAP les transmet à intervalles réguliers pour annoncer l'existence du réseau sans fil. Le comportement par défaut consiste à envoyer une trame de balise toutes les 100 millisecondes (ou 10 par seconde).

  Entrez un entier compris entre 20 et 2 000 millisecondes. La valeur par défaut est 100 millisecondes.

- **DTIM Period** : période DTIM (Delivery Traffic Information Map). Entrez un entier compris entre 1 et 255 balises. La valeur par défaut est 2 balises.

Le message DTIM est un élément inclus dans certaines trames de balise. Il indique les stations clientes actuellement en mode basse puissance qui ont des données mises en mémoire tampon sur le périphérique WAP en attente de sélection.

La période DTIM que vous spécifiez indique la fréquence à laquelle les clients servis par ce périphérique WAP doivent rechercher les données mises en mémoire tampon qui se trouvent encore sur le périphérique WAP en attente de sélection.

La mesure s'effectue en balises. Par exemple, si vous définissez ce champ à 1, les clients recherchent les données mises en mémoire tampon sur le périphérique WAP à chaque balise. Si vous définissez ce champ à 10, les clients effectuent leur recherche toutes les 10 balises.

- **Fragmentation Threshold** : seuil de la taille de trame en octets. L'entier valide doit être pair et se trouver dans la plage comprise entre 256 et 2 346. La valeur par défaut est 2 346.

  Le seuil de fragmentation est un moyen de limiter la taille des paquets (trames) transmis sur le réseau. Si un paquet dépasse le seuil de fragmentation que vous avez défini, la fonction de fragmentation est activée et le paquet est envoyé sous forme de plusieurs trames 802.11.

  Si le paquet transmis est égal ou inférieur au seuil, la fragmentation n'est pas utilisée. La définition du seuil à une valeur la plus élevée (2 346 octets, qui est la valeur par défaut) désactive effectivement la fragmentation.

  La fragmentation implique une charge de traitement supérieure, en raison du travail supplémentaire nécessaire à la division et au réassemblage des trames, mais aussi parce qu'elle augmente le trafic des messages sur le réseau. Toutefois, la fragmentation améliore la performance et la fiabilité du réseau si elle est correctement configurée.

  L'envoi de trames plus petites (par l'intermédiaire d'un seuil de fragmentation plus bas) peut aider à résoudre les problèmes d'interférences, par exemple avec les fours à micro-ondes.

  Par défaut, la fragmentation est désactivée. Nous vous conseillons de ne pas utiliser la fragmentation à moins que vous ne suspectiez des interférences radio. Les en-têtes supplémentaires appliqués à chaque fragment augmentent la charge de traitement sur le réseau et peuvent réduire significativement le débit.

- **RTS Threshold** : valeur de seuil Request to Send (RTS). La plage de nombres entiers valides est comprise entre 0 et 2 347. La valeur par défaut est 2 347.

Le seuil RTS indique le nombre d'octets dans un MPDU au-dessous duquel aucune liaison RTS/CTS n'est établie.

La modification du seuil RTS peut aider à contrôler le flux de trafic dans le périphérique WAP, notamment lorsqu'il comporte un grand nombre de clients. Si vous spécifiez une faible valeur de seuil, les paquets RTS sont envoyés plus fréquemment, ce qui consomme davantage de bande passante et réduit le débit du paquet. Cependant, l'envoi d'un plus grand nombre de paquets RTS peut permettre le rétablissement du réseau suite à des interférences ou des collisions susceptibles de se produire sur un réseau chargé ou sur un réseau rencontrant des interférences électromagnétiques.

- **Maximum Associated Clients** : nombre maximal de stations autorisées à accéder à ce périphérique WAP à tout moment. Vous pouvez saisir un nombre entier compris entre 0 et 200. La valeur par défaut est 200 stations.
- **Transmit Power** : valeur de pourcentage du niveau de puissance de transmission pour ce périphérique WAP.

  La valeur par défaut de 100 pour cent peut être plus économique qu'un pourcentage inférieur, car elle donne au périphérique WAP une plage de diffusion maximale et réduit le nombre de points d'accès requis.

  Pour accroître la capacité du réseau, rapprochez les périphériques WAP les uns des autres et diminuez la valeur de puissance de transmission. Vous réduisez ainsi le chevauchement et les interférences entre les points d'accès. Une puissance de transmission plus basse permet également de sécuriser davantage votre réseau, car des signaux sans fil plus faibles sont moins susceptibles de se propager à l'extérieur de l'emplacement physique de votre réseau.

  Certaines combinaisons de plages de canaux et de code de pays ont une puissance de transmission maximale relativement basse. Si vous essayez de définir la puissance de transmission sur des plages plus basses (par exemple, 25 % ou 12 %), la baisse de puissance attendue est susceptible de ne pas se produire, car certains amplificateurs de puissance doivent respecter une puissance de transmission minimale.
- **Fixed Multicast Rate** : vitesse de transmission en Mbit/s pour les paquets de diffusion et de multidiffusion. Ce paramètre peut être utile dans un environnement offrant une lecture vidéo à multidiffusion sans fil, pourvu que les clients sans fil prennent en charge le débit configuré.

Lorsque **Auto** est sélectionné, le périphérique WAP choisit le meilleur débit pour les clients associés. La plage de valeurs valides est déterminée par le mode radio configuré.

- **Legacy Rate Sets** : les débits sont exprimés en mégabits par seconde.

  Supported Rate Sets indique les débits pris en charge par le périphérique WAP. Vous pouvez sélectionner plusieurs débits (cochez une case pour sélectionner un débit ou décochez-la pour le désélectionner). Le périphérique WAP choisit automatiquement le débit le plus efficace en fonction de facteurs comme les taux d'erreur et la distance à laquelle les stations clientes se trouvent du périphérique WAP.

  Basic Rate Sets indique les débits annoncés au réseau par le périphérique WAP, de façon à établir la communication avec les autres points d'accès et stations clientes du réseau. Il est généralement plus efficace d'avoir un périphérique WAP qui diffuse un sous-ensemble de ses ensembles de débits pris en charge.

- **MCS (Data Rate) Settings** : valeurs d'index Modulation and Coding Scheme (MCS) annoncées par le périphérique WAP. Les MCS peuvent augmenter le débit pour les clients sans fil 802.11n.

  Cochez la case située sous le numéro d'index MCS pour l'activer ou décochez-la pour désactiver l'index. Vous ne pouvez pas désactiver tous les index simultanément.

  Le périphérique WAP prend en charge les index MCS 0 à 15. L'index MSC 15 permet une vitesse de transmission maximale de 300 Mbit/s. Si aucun index MCS n'est sélectionné, la radio fonctionne à un index MCS 0, ce qui offre une vitesse de transmission maximale de 15 Mbit/s.

  Les paramètres MCS ne peuvent être configurés que si le mode radio inclut la prise en charge 802.11n.

- **Broadcast/Multicast Rate Limiting** : la limite du débit de diffusion et multidiffusion peut augmenter la performance globale du réseau en limitant le nombre de paquets transmis sur le réseau.

  Par défaut, l'option Multicast/Broadcast Rate Limiting est désactivée. Tant que vous n'activez pas l'option Multicast/Broadcast Rate Limiting, les champs suivants sont désactivés :

- **Rate Limit** : limite de débit pour le trafic de diffusion et multidiffusion. La limite doit être supérieure à 1, mais inférieure à 50 paquets par seconde. Tout le trafic inférieur à cette limite de débit est conforme et est toujours transmis vers la destination appropriée. Le paramètre de limite de débit par défaut et maximale est de 50 paquets par seconde.
- **Rate Limit Burst** : volume de trafic, mesuré en octets, autorisé à transiter sous forme de rafale temporaire même s'il dépasse le débit maximal défini. Le paramètre de rafale de limite de débit par défaut et maximale est de 75 paquets par seconde.

- **TSPEC Mode** : régule le mode TSPEC global sur le périphérique WAP. Par défaut, le mode TSPEC est désactivé. Les options sont les suivantes :
  - **On** : le périphérique WAP traite les demandes TSPEC en fonction des paramètres TSPEC définis sur la page Radio. Utilisez ce paramètre si le périphérique WAP gère le trafic provenant de périphériques QoS, tels qu'un téléphone Wi-Fi CERTIFIED.
  - **Off** : le périphérique WAP ignore les demandes TSPEC des stations clientes. Utilisez ce paramètre si vous ne souhaitez pas utiliser TSPEC pour donner la priorité aux périphériques QoS en cas de trafic urgent.
- **TSPEC Voice ACM Mode** : régule le contrôle d'admission obligatoire (ACM) pour la catégorie d'accès vocal. Par défaut, le mode TSPEC Voice ACM est désactivé. Les options sont les suivantes :
  - **On** : une station doit envoyer une demande TSPEC de bande passante au périphérique WAP avant d'envoyer ou de recevoir un flux de trafic vocal. Le périphérique WAP répond avec le résultat de la demande, qui inclut le temps moyen alloué si la TSPEC a été autorisée.
  - **Off** : une station peut envoyer et recevoir le trafic de priorité vocale sans nécessiter de TSPEC autorisée ; le périphérique WAP ignore les demandes TSPEC vocales des stations clientes.
- **TSPEC Voice ACM Limit** : limite supérieure du volume de trafic que le périphérique WAP tente de transmettre sur le support sans fil via un contrôle d'autorisation vocal pour obtenir l'accès. La limite par défaut est de 20 pour cent du trafic total.
- **TSPEC Video ACM Mode** : régule le contrôle d'admission obligatoire pour la catégorie d'accès vidéo. Par défaut, le mode TSPEC Video ACM est désactivé. Les options sont les suivantes :

- **On** : une station doit envoyer une demande TSPEC de bande passante au périphérique WAP avant d'envoyer ou de recevoir un flux de trafic vidéo. Le périphérique WAP répond avec le résultat de la demande, qui inclut le temps moyen alloué si la TSPEC a été autorisée.
- **Off** : une station peut envoyer et recevoir le trafic de priorité vidéo sans nécessiter de TSPEC autorisée ; le périphérique WAP ignore les demandes TSPEC vidéo des stations clientes.

- **TSPEC Video ACM Limit** : limite supérieure du volume de trafic que le périphérique WAP tente de transmettre sur le support sans fil via un contrôle d'autorisation vidéo pour obtenir l'accès. La limite par défaut est de 15 pour cent du trafic total.
- **TSPEC AP Inactivity Timeout** : durée nécessaire à un périphérique WAP pour détecter une spécification inactive de trafic descendant avant de la supprimer. La plage de nombres entiers valides est comprise entre 0 et 120 secondes. La valeur par défaut est 30 secondes.
- **TSPEC Station Inactivity Timeout** : durée nécessaire à un périphérique WAP pour détecter une spécification inactive de trafic montant avant de la supprimer. La plage de nombres entiers valides est comprise entre 0 et 120 secondes. La valeur par défaut est 30 secondes.
- **TSPEC Legacy WMM Queue Map Mode** : active ou désactive l'interaction du trafic hérité dans les files d'attente fonctionnant comme ACM. Par défaut, ce mode est désactivé.

ÉTAPE 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

AVERTISSEMENT Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Détection de point d'accès non autorisé

Un point d'accès non autorisé est un point d'accès qui a été installé sur un réseau sécurisé sans l'autorisation explicite d'un administrateur système. Les points d'accès non autorisés constituent une menace en matière de sécurité car toute personne ayant accès aux locaux peut, par ignorance ou par malveillance, installer un Périphérique WAP sans fil bon marché pouvant potentiellement permettre à des personnes non autorisées d'accéder au réseau.

Le Périphérique WAP effectue une analyse RF sur tous les canaux afin de détecter tous les points d'accès à proximité du réseau. Si des points d'accès non autorisés sont détectés, ils apparaissent sur la page Rogue AP Detection. Si un point d'accès identifié comme non autorisé est en réalité légitime, vous pouvez l'ajouter à la Known AP List.

REMARQUE La Detected Rogue AP List et la Trusted AP List fournissent les informations vous permettant de prendre les mesures adéquates. Le point d'accès n'a aucun contrôle sur les points d'accès non autorisés qui sont indiqués dans les listes et ne peut pas appliquer de stratégies de sécurité aux points d'accès détectés via l'analyse RF.

Lorsque la détection de point d'accès est activée, la radio bascule régulièrement de son canal de fonctionnement pour analyser les autres canaux de la même bande.

Affichage de la Rogue AP List

La détection de point d'accès non autorisé peut être activée et désactivée. Pour que la radio puisse collecter des informations sur les points d'accès non autorisés, cliquez sur **Enable** en regard de **AP Detection**, puis cliquez sur **Save**.

Les informations relatives aux points d'accès non autorisés détectés et approuvés s'affichent. Vous pouvez cliquer sur **Refresh** pour actualiser l'écran et afficher les informations les plus à jour :

- **Action** : si le point d'accès se trouve dans la Detected Rogue AP List, vous pouvez cliquer sur **Trust** pour le déplacer vers la Trusted AP List.

  Si le point d'accès se trouve dans la Trusted AP List, vous pouvez cliquer sur **Untrust** pour le déplacer vers la Detected Rogue AP List.

  REMARQUE La Detected Rogue AP List et la Trusted AP List fournissent des informations. Le Périphérique WAP n'a aucun contrôle sur les points d'accès indiqués dans la liste et ne peut pas appliquer de stratégies de sécurité aux points d'accès détectés via l'analyse RF.

- **MAC Address** : adresse MAC du point d'accès non autorisé.
- **Beacon Interval** : intervalle de balise utilisé par le point d'accès non autorisé.

  Les trames de balise sont transmises par un point d'accès à intervalles réguliers pour annoncer l'existence du réseau sans fil. Le comportement par défaut consiste à envoyer une trame de balise toutes les 100 millisecondes (ou 10 par seconde).

  REMARQUE Vous pouvez définir l'intervalle de balise sur la page **Radio**.
- **Type** : type de périphérique :
  - AP indique que le périphérique non autorisé est un point d'accès qui prend en charge la structure IEEE 802.11 Wireless Networking Framework en mode Infrastructure.
  - Ad hoc indique une station non autorisée fonctionnant en mode Ad hoc. Les stations définies en mode Ad hoc communiquent directement entre elles, sans utiliser de point d'accès classique. Le mode Ad hoc est une structure IEEE 802.11 Wireless Networking Framework, également appelée mode peer-to-peer, ou un Independent Basic Service Set (IBSS).
- **SSID** : SSID (Service Set Identifier) du périphérique WAP.

  Le SSID est une chaîne alphanumérique de 32 caractères maximum qui identifie de manière unique un réseau local sans fil. Il porte également le nom de Network Name (nom réseau).
- **Privacy** : indique si un processus de sécurité est appliqué au périphérique non autorisé :
  - Off indique que le mode Security sur le périphérique non autorisé est défini sur None (aucune sécurité).
  - On indique que le périphérique non autorisé intègre un processus de sécurité.

  REMARQUE Vous pouvez utiliser la page **Networks** pour configurer la sécurité sur le point d'accès.
- **WPA** : spécifie si la sécurité WPA est activée ou désactivée pour le point d'accès non autorisé.
- **Band** : mode IEEE 802.11 utilisé sur le point d'accès non autorisé. (Par exemple, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.)

Le numéro affiché indique le mode :

- 2,4 indique le mode IEEE 802.11b, 802.11g ou 802.11n (ou une combinaison des modes).
- 5 indique le mode IEEE 802.11a ou 802.11n (ou les deux modes).

- **Channel** : canal sur lequel le point d'accès non autorisé diffuse actuellement.

  Le canal définit la partie du spectre radio utilisée par la radio pour la transmission et la réception.

  REMARQUE La page **Radio** vous permet de définir le canal.

- **Rate** : débit, en mégabits par seconde, auquel le point d'accès non autorisé transmet actuellement.

  Le débit actuel est toujours l'un des débits spécifiés dans Supported Rates.

- **Signal** : puissance du signal radio qui émet depuis le point d'accès non autorisé. Si vous passez le pointeur de la souris sur les barres, un nombre représentant la puissance en décibels (dB) apparaît.
- **Beacons** : nombre total de balises reçues du point d'accès non autorisé depuis sa première détection.
- **Last Beacon** : date et heure de la dernière balise reçue du point d'accès non autorisé.
- **Rates** : ensembles de débits de base (annoncés) et pris en charge pour le point d'accès non autorisé. Les débits sont affichés en mégabits par seconde (Mbit/s).

  Tous les débits pris en charge sont répertoriés ; les débits de base apparaissent en gras. Vous pouvez configurer les ensembles de débits sur la page **Radio**.

Création et enregistrement d'une Trusted AP List

Pour créer une Trusted AP List et l'enregistrer dans un fichier :

ÉTAPE 1 Dans la Detected Rogue AP List, cliquez sur **Trust** pour les points d'accès que vous connaissez. Les points d'accès approuvés sont déplacés vers la Trusted AP List.

ÉTAPE 2 Dans la zone Download/Backup Trusted AP List, sélectionnez **Backup (AP to PC)**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

La liste contient les adresses MAC de tous les points d'accès qui ont été ajoutés à la Known AP List. Par défaut, le nom du fichier est Rogue2.cfg. Vous pouvez utiliser un éditeur de texte ou un navigateur Web pour ouvrir le fichier et afficher son contenu.

Importation d'une Trusted AP List

Vous pouvez importer une liste de points d'accès connus à partir d'une liste enregistrée. Vous pouvez obtenir la liste depuis un autre point d'accès ou la créer à partir d'un fichier texte. Si l'adresse MAC d'un point d'accès apparaît dans la Trusted AP List, elle ne sera plus détectée comme non autorisée.

Pour importer une liste de points d'accès à partir d'un fichier, procédez comme suit :

ÉTAPE 1 Dans la zone Download/Backup Trusted AP List, sélectionnez **Download (PC to AP)**.

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

Le fichier que vous importez doit être un fichier texte brut portant une extension .txt ou .cfg. Les entrées du fichier sont des adresses MAC au format hexadécimal, dont chaque octet est séparé par le signe deux points (par exemple, 00:11:22:33:44:55). Vous devez séparer les entrées par un espace. Pour que le point d'accès accepte le fichier, il doit uniquement contenir des adresses MAC.

ÉTAPE 3 Indiquez si vous souhaitez remplacer la Trusted AP List existante ou ajouter les entrées du fichier importé à la Trusted AP List.

a. Sélectionnez **Replace** pour importer la liste et remplacer le contenu de la Known AP List.

b. Sélectionnez **Merge** pour importer la liste et ajouter les points d'accès du fichier importé aux points d'accès qui sont déjà présents dans la Known AP List.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Une fois l'importation terminée, l'écran s'actualise et les adresses MAC des points d'accès du fichier importé apparaissent dans la Known AP List.

Networks

Les points d'accès virtuels (VAP) segmentent le réseau local sans fil en plusieurs domaines de diffusion qui constituent l'équivalent sans fil des VLAN Ethernet. Les VAP simulent plusieurs points d'accès dans un seul périphérique WAP physique. Quatre VAP maximum sont pris en charge sur le WAP121 et huit VAP maximum sont pris en charge sur le WAP321.

Chaque VAP peut être activé ou désactivé indépendamment, à l'exception du VAP0. Le VAP0 est l'interface radio physique et reste activé tant que la radio est activée. Pour désactiver le VAP0, la radio elle-même doit être désactivée.

Chaque VAP est identifié par un SSID (Service Set Identifier) configuré par l'utilisateur. Plusieurs VAP ne peuvent pas avoir le même nom SSID. Les diffusions SSID peuvent être activées ou désactivées indépendamment sur chaque VAP. La diffusion SSID est activée par défaut.

Conventions d'affectation de noms SSID

Le SSID par défaut de VAP0 est ciscosb. Chaque VAP supplémentaire créé a un nom SSID vierge. Les SSID de tous les VAP peuvent être définis sur d'autres valeurs.

Le SSID peut être n'importe quelle entrée alphanumérique sensible à la casse constituée de 2 à 32 caractères. Les caractères imprimables plus l'espace (ASCII 0x20) sont autorisés, mais les six caractères suivants ne le sont pas :

?, ", $, [, \,] et +.

Les caractères autorisés sont les suivants :

ASCII 0x20, 0x21, 0x23, 0x25 à 0x2A, 0x2C à 0x3E, 0x40 à 0x5A, 0x5E à 0x7E.

En outre, les trois caractères suivants ne peuvent pas être le premier caractère :

!, # et ; (respectivement ASCII 0x21, 0x23 et 0x3B).

Les espaces au début et à la fin (ASCII 0x20) ne sont pas autorisés.

REMARQUE Cela signifie que les espaces sont autorisés dans le SSID, mais pas comme premier ou dernier caractère. Le point « . » (ASCII 0x2E) est aussi autorisé.

ID de VLAN

Chaque VAP est associé à un VLAN, qui est identifié par un ID de VLAN (VID). Un VID peut avoir n'importe quelle valeur comprise entre 1 et 4 094 inclus. Le WAP121 prend en charge cinq VLAN actifs (quatre pour le WLAN plus un VLAN de gestion). Les périphériques WAP321 prennent en charge neuf VLAN actifs (huit pour le WLAN plus un VLAN de gestion).

Par défaut, le VID attribué à l'utilitaire de configuration pour le périphérique WAP est 1, qui est aussi le VID non balisé par défaut. Si le VID de gestion est le même que le VID attribué à un VAP, les clients WLAN associés à ce VAP spécifique peuvent administrer le périphérique WAP. Si nécessaire, une liste de contrôle d'accès (ACL) peut être créée pour désactiver l'administration depuis les clients WLAN.

Configuration des VAP

Pour configurer les VAP :

ÉTAPE 1 Sélectionnez **Wireless** > **Networks** dans le volet de navigation.

ÉTAPE 2 Cochez la case **Enabled** pour le VAP que vous souhaitez configurer.

—Ou—

Si VAP0 est le seul VAP configuré sur le système et que vous souhaitez ajouter un VAP, cliquez sur **Add**. Sélectionnez ensuite le VAP, puis cliquez sur **Edit**.

ÉTAPE 3 Configurez les paramètres suivants :

- **VLAN ID** : VID du VLAN à associer au VAP.

AVERTISSEMENT Veillez à saisir un ID de VLAN correctement configuré sur le réseau. Des problèmes réseau peuvent survenir si le VAP associe des clients sans fil dont le VLAN est incorrectement configuré.
Si un client sans fil se connecte au périphérique WAP par l'intermédiaire de ce VAP, le périphérique WAP balise tout le trafic à partir du client sans fil avec l'ID de VLAN que vous saisissez dans ce champ, sauf si vous saisissez l'ID de VLAN du port ou que vous utilisez un serveur RADIUS pour attribuer un client sans fil à un VLAN. La plage de l'ID de VLAN est comprise entre 1 et 4 094.

REMARQUE Si vous définissez l'ID de VLAN sur un autre ID que l'ID de VLAN de gestion actuel, les clients WLAN associés à ce VAP spécifique ne pourront pas administrer le périphérique. Vérifiez la configuration des ID de VLAN non balisés et de gestion sur la page du réseau local (LAN). Pour plus d'informations, reportez-vous à la section **Paramètres d'adresse VLAN et IPv4**.

- **SSID Name** : nom du réseau sans fil. Le SSID est une chaîne alphanumérique constituée de 32 caractères maximum. Choisissez un SSID unique pour chaque VAP.

  REMARQUE Si vous êtes connecté en tant que client sans fil au périphérique WAP que vous administrez, la réinitialisation du SSID entraînera une perte de connexion au périphérique WAP. Vous devrez vous reconnecter au nouveau SSID une fois cette nouvelle configuration enregistrée.

- **Broadcast SSID** : active et désactive la diffusion du SSID.

  Indiquez si vous souhaitez autoriser le périphérique WAP à diffuser le SSID dans ses trames de balise. Le paramètre Broadcast SSID est activé par défaut. Lorsque le VAP ne diffuse pas son SSID, le nom réseau n'apparaît pas dans la liste des réseaux disponibles sur une station cliente. Vous devez donc saisir manuellement le nom réseau exact dans l'utilitaire de connexion sans fil sur le client, afin de permettre l'établissement de la connexion.

  La désactivation du SSID de diffusion est suffisante pour empêcher les clients de se connecter accidentellement à votre réseau, mais celle-ci n'empêche aucunement la plus simple des tentatives d'un pirate informatique de se connecter ou de surveiller le trafic déchiffré. La suppression de la diffusion SSID offre un niveau de protection très bas sur un réseau autrement exposé (comme un réseau d'invité) où la priorité est de permettre aux clients d'obtenir une connexion et où aucune information sensible n'est disponible.

- **Security** : type d'authentification requis pour l'accès au VAP :
  - None
  - Static WEP
  - Dynamic WEP
  - WPA Personal
  - WPA Enterprise

Si vous sélectionnez un autre mode de sécurité que None, des champs supplémentaires s'affichent. Ces champs sont décrits à la section **Définition des paramètres de sécurité**.

REMARQUE Nous vous conseillons d'utiliser WPA Personal ou WPA Enterprise comme type d'authentification, car ils offrent une sécurité plus élevée. Utilisez Static WEP ou Dynamic WEP uniquement pour les périphériques ou ordinateurs sans fil hérités qui ne prennent pas en charge WPA Personal/Enterprise. Si vous devez définir la sécurité sur Static WEP ou Dynamic WEP, configurez Radio sur le mode 802.11a ou 802.11b/g (voir **Radio**). Le mode 802.11n restreint l'utilisation de Static WEP ou Dynamic WEP en tant que mode de sécurité.

- **MAC Filtering** : indique si les stations qui peuvent accéder à ce VAP sont limitées à une liste globale configurée d'adresses MAC. Vous pouvez sélectionner l'un de ces types de filtrage MAC :
  - **Disabled** : vous n'utilisez pas le filtrage MAC.
  - **Local** : vous utilisez la liste d'authentification MAC que vous configurez sur la page **Filtrage MAC**.
  - **RADIUS** : vous utilisez la liste d'authentification MAC sur un serveur RADIUS externe.
- **Channel Isolation** : active et désactive l'isolation des stations.
  - Lorsque ce paramètre est désactivé, les clients sans fil peuvent communiquer entre eux normalement en envoyant le trafic via le périphérique WAP.
  - Lorsque ce paramètre est activé, le périphérique WAP bloque les communications entre les clients sans fil situés sur le même VAP. Le périphérique WAP autorise toujours le trafic de données entre ses clients sans fil et les périphériques filaires du réseau, via une liaison WDS, et avec les autres clients sans fil associés à un autre VAP, mais pas au sein même des clients sans fil.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

AVERTISSEMENT Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

REMARQUE Pour supprimer un VAP, sélectionnez-le, puis cliquez sur **Delete**. Pour enregistrer définitivement votre suppression, cliquez sur **Save** lorsque vous avez terminé.

Définition des paramètres de sécurité

Ces sections décrivent les paramètres de sécurité que vous définissez, en fonction de votre sélection dans la liste Security de la page Networks.

None (Plain-text)

Si vous sélectionnez **None** comme mode de sécurité, aucun paramètre de sécurité supplémentaire ne peut être défini sur le Périphérique WAP. Ce mode signifie que toutes les données transférées de et vers le Périphérique WAP ne sont pas chiffrées. Ce mode de sécurité peut être utile lors de la configuration initiale du réseau pour la résolution des problèmes, mais il n'est pas recommandé pour une utilisation régulière sur le réseau interne, car il n'offre pas la sécurité nécessaire.

Static WEP

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

Static WEP n'est pas le mode offrant le plus de sécurité, mais il fournit davantage de protection que le mode None (Plain-text), puisqu'il empêche un utilisateur externe de facilement détecter le trafic sans fil non chiffré.

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

Les paramètres suivants vous permettent de configurer le mode Static WEP :

- **Transfer Key Index** : liste des index de clé. Les index de clé 1 à 4 sont disponibles. La valeur par défaut est 1.

  Transfer Key Index indique la clé WEP utilisée par le périphérique WAP pour chiffrer les données qu'il transmet.

- **Key Length** : longueur de la clé. Sélectionnez-en un :
  - 64 bits
  - 128 bits
- **Key Type** : type de clé. Sélectionnez-en un :
  - ASCII
  - Hex
- **WEP Keys** : vous pouvez spécifier un maximum de quatre clés WEP. Dans chaque zone de texte, saisissez une chaîne de caractères pour chaque clé. Les clés que vous saisissez dépendent du type de clé sélectionné :
  - ASCII — Inclut les lettres alphabétiques majuscules et minuscules, les chiffres numériques et les symboles spéciaux comme @ et #.
  - Hex — Inclut les chiffres 0 à 9 et les lettres A à F.

  Utilisez le même nombre de caractères pour chaque clé, comme spécifié dans le champ Characters Required. Il s'agit des clés RC4 WEP partagées avec les stations par l'intermédiaire du périphérique WAP.

  Chaque station cliente doit être configurée pour utiliser l'une de ces mêmes clés WEP, dans le même logement que celui spécifié sur le périphérique WAP.
- **Characters Required** : le nombre de caractères que vous saisissez dans les champs WEP Key est déterminé par la longueur de clé et le type de clé que vous sélectionnez. Par exemple, si vous utilisez des clés ASCII 128 bits, vous devez saisir 26 caractères dans le champ WEP key. Le nombre de caractères requis est automatiquement mis à jour en fonction de votre sélection de la longueur de clé et du type de clé.
- **802.1X Authentication** : l'algorithme d'authentification définit la méthode utilisée pour déterminer si une station cliente est autorisée à s'associer à un périphérique WAP lorsque le mode de sécurité Static WEP est sélectionné.

Spécifiez l'algorithme d'authentification que vous souhaitez utiliser en choisissant l'une des options suivantes :

- L'authentification **Open System** permet à n'importe quelle station cliente de s'associer au périphérique WAP, peu importe si cette station cliente dispose de la clé WEP correcte. Cet algorithme est aussi utilisé en mode plaintext (texte en clair), IEEE 802.1X et WPA. Lorsque l'algorithme d'authentification est défini sur Open System, tout client peut s'associer au périphérique WAP.

  REMARQUE Le fait qu'une station cliente soit autorisée à s'associer ne signifie pas qu'elle pourra systématiquement échanger des données avec un périphérique WAP. Une station doit disposer de la clé WEP correcte pour pouvoir accéder au périphérique WAP et déchiffrer ses données, mais aussi pour transmettre des données lisibles à celui-ci.

- L'authentification **Shared Key** nécessite que la station cliente dispose de la clé WEP correcte pour s'associer au périphérique WAP. Lorsque l'algorithme d'authentification est défini sur Shared Key, une station ayant une clé WEP incorrecte ne peut pas s'associer au périphérique WAP.

- **Open System** et **Shared Key**. Si vous sélectionnez les deux algorithmes d'authentification, les stations clientes configurées pour utiliser le WEP en mode de clé partagée doivent disposer d'une clé WEP valide pour s'associer au périphérique WAP. En outre, les stations clientes configurées pour utiliser le WEP en mode Open System (Shared Key désactivé) peuvent s'associer au périphérique WAP même si elles ne disposent pas de la clé WEP correcte.

Règles du mode Static WEP

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

- Toutes les stations clientes doivent avoir la sécurité Wireless LAN (WLAN) définie sur WEP, et tous les clients doivent disposer de l'une des clés WEP spécifiées sur le périphérique WAP pour pouvoir décoder les transmissions de données du point d'accès vers la station.
- Le périphérique WAP doit avoir toutes les clés utilisées par les clients pour les transmissions de la station vers le point d'accès, afin de pouvoir décoder les transmissions de la station.
- La même clé doit occuper le même logement sur tous les nœuds (point d'accès et clients). Par exemple, si le périphérique WAP définit la clé abc123 comme clé WEP 3, alors les stations clientes doivent définir cette même chaîne comme clé WEP 3.

- Les stations clientes peuvent utiliser différentes clés pour transmettre des données au point d'accès. (Elles peuvent aussi toutes utiliser la même clé, mais cela s'avère moins sûr car cela signifie qu'une station peut déchiffrer les données envoyées par une autre.)
- Sur certains logiciels de clients sans fil, vous pouvez configurer plusieurs clés WEP et définir un index de clé de transfert de station cliente, puis définir les stations afin de chiffrer les données qu'elles transmettent par l'intermédiaire de différentes clés. Cela permet de s'assurer que les points d'accès situés à proximité ne pourront pas décoder les transmissions des autres points d'accès.
- Vous ne pouvez pas placer à la fois des clés WEP 64 bits et 128 bits entre le point d'accès et ses stations clientes.

Dynamic WEP

Dynamic WEP se réfère à la combinaison de la technologie 802.1x et du protocole EAP (Extensible Authentication Protocol). Avec la sécurité Dynamic WEP, les clés WEP sont changées dynamiquement.

Les messages EAP sont envoyés via un réseau sans fil IEEE 802.11 par l'intermédiaire d'un protocole appelé EAP Encapsulation Over LANs (EAPOL). IEEE 802.1X fournit des clés générées dynamiquement qui sont régulièrement actualisées. Un chiffrement de flux RC4 est utilisé pour déchiffrer le corps de trame et le contrôle de redondance cyclique (CRC) de chaque trame 802.11.

Ce mode nécessite l'utilisation d'un serveur RADIUS externe pour l'authentification des utilisateurs. Le périphérique WAP requiert un serveur RADIUS prenant en charge EAP, tel que le Microsoft Internet Authentication Server. Pour fonctionner avec les clients Microsoft Windows, le serveur d'authentification doit prendre en charge Protected EAP (PEAP) et MSCHAP V2.

Vous pouvez recourir à un large choix de méthodes d'authentification prises en charge par le mode IEEE 802.1X, notamment les certificats, Kerberos et l'authentification par clé publique. Vous devez configurer les stations clientes afin qu'elles utilisent la même méthode d'authentification que le périphérique WAP.

Les paramètres suivants vous permettent de configurer le mode Dynamic WEP :

- **Use Global RADIUS Server Settings** : par défaut, chaque VAP utilise les paramètres RADIUS globaux que vous définissez pour le périphérique WAP (voir **Serveur RADIUS**). Toutefois, vous pouvez configurer chaque VAP de façon à ce qu'il utilise un autre groupe de serveurs RADIUS.

Pour utiliser les paramètres de serveur RADIUS globaux, veillez à cocher la case.

Pour utiliser un serveur RADIUS distinct pour le VAP, décochez la case et saisissez l'adresse IP du serveur RADIUS, puis renseignez les champs ci-dessous :

- **Server IP Address Type** : version IP utilisée par le serveur RADIUS.

  Vous pouvez basculer entre les différents types d'adresse afin de définir les paramètres d'adresse RADIUS globaux IPv4 et IPv6, mais le périphérique WAP ne contactera que le ou les serveurs RADIUS répondant au type d'adresse que vous sélectionnez dans ce champ.

- **Server IP Address 1** ou **Server IPv6 Address 1** : adresse du serveur RADIUS principal pour ce VAP.

  Lorsque le premier client sans fil tente de s'authentifier auprès du périphérique WAP, le périphérique WAP envoie une demande d'authentification au serveur principal. Si le serveur principal répond à la demande d'authentification, le périphérique WAP continue à utiliser ce serveur RADIUS comme serveur principal et les demandes d'authentification sont envoyées à l'adresse spécifiée.

  La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (192.0.2.10). La forme de l'adresse IPv6 doit être similaire à celle-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

- **Server IP Address 2** à **4** ou **Server IPv6 Address 2** à **4** : jusqu'à trois adresses de serveur RADIUS IPv4 ou IPv6 de sauvegarde.

  Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.

- **Key** : clé secrète partagée que le périphérique WAP utilise pour s'authentifier sur le serveur RADIUS principal.

  Vous pouvez utiliser jusqu'à 63 caractères alphanumériques standard et caractères spéciaux. La clé est sensible à la casse et doit correspondre à la clé configurée sur le serveur RADIUS. Le texte que vous saisissez s'affiche sous forme d'astérisques.

- **Key 2** à **Key 4** : clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur spécifié dans le champ **Server IP (IPv6) Address 2** utilise **Key 2** ; le serveur spécifié dans le champ **Server IP (IPv6) Address 3** utilise **Key 3**, etc.

- **Enable RADIUS Accounting** : active le suivi et la mesure des ressources consommées par un utilisateur donné (heure système, volume de données transmises et reçues, etc.)

  Si vous activez la gestion des comptes RADIUS, cette fonctionnalité est activée à la fois pour le serveur RADIUS principal et pour l'ensemble des serveurs de sauvegarde.

- **Active Server** : permet de sélectionner administrativement le serveur RADIUS actif, ce qui évite au périphérique WAP de devoir contacter dans l'ordre chaque serveur configuré et de choisir le premier serveur actif.

- **Broadcast Key Refresh Rate** : intervalle auquel la clé (groupe) de diffusion est actualisée pour les clients associés à ce VAP.

  La valeur par défaut est 300. La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

- **Session Key Refresh Rate** : intervalle auquel le périphérique WAP actualise les clés de session (monodiffusion) pour chaque client associé au VAP.

  La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

WPA Personal

WPA Personal est une norme IEEE 802.11i Wi-Fi Alliance qui inclut le chiffrement AES-CCMP et TKIP. La version Personal de WPA utilise une clé prépartagée (PSK) au lieu de IEEE 802.1X et EAP comme dans le mode de sécurité Enterprise WPA. Le PSK est uniquement utilisé pour le contrôle initial des informations d'identification. WPA Personal est également appelé WPA-PSK.

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

Les paramètres ci-après permettent de configurer WPA Personal :

- **WPA Versions** : types de stations clientes que vous souhaitez prendre en charge :

  - **WPA** : le réseau intègre des stations clientes qui prennent en charge le WPA d'origine et aucune qui ne soit compatible avec le WPA2 (plus récent).

  - **WPA2** : toutes les stations clientes du réseau prennent en charge le WPA2. Cette version du protocole fournit une sécurité optimale avec la norme IEEE 802.11i.

Si le réseau intègre un mélange de clients, certains prenant en charge le WPA2 et d'autres prenant uniquement en charge le WPA d'origine, cochez les deux cases. Les stations clientes WPA et WPA2 peuvent ainsi s'associer et s'authentifier, mais peuvent aussi utiliser le WPA2 (plus robuste) pour les clients qui le prennent en charge. Cette configuration WPA offre davantage d'interopérabilité et un peu moins de sécurité.

- **Cipher Suites** : suite de chiffrement que vous souhaitez utiliser :
  - TKIP
  - CCMP (AES)

  Vous pouvez sélectionner l'un ou l'autre, ou les deux. Les clients TKIP et AES peuvent s'associer au périphérique WAP. Les clients WPA doivent avoir l'une des clés ci-dessous pour pouvoir s'associer au périphérique WAP :
  - Une clé TKIP valide
  - Une clé AES-CCMP valide

  Les clients non configurés pour utiliser WPA Personal ne peuvent pas s'associer au périphérique WAP.
- **Key** : clé secrète partagée pour la sécurité WPA Personal. Saisissez une chaîne de 8 caractères minimum et de 63 caractères maximum. Les caractères acceptés sont les lettres alphabétiques majuscules et minuscules, les chiffres numériques et les symboles spéciaux comme @ et #.
- **Key Strength Meter** : le périphérique WAP contrôle la clé sur la base de critères de complexité comme le nombre de types de caractères différents utilisés (lettres alphabétiques majuscules et minuscules, nombres et caractères spéciaux), mais vérifie également la longueur de la clé. Lorsque la fonction de contrôle de la complexité WPA-PSK est activée, la clé n'est pas acceptée si elle ne respecte pas les critères minimaux. Pour obtenir des informations sur la configuration du contrôle de la complexité, reportez-vous à la section **Complexité WPA-PSK**.
- **Broadcast Key Refresh Rate** : intervalle auquel la clé (groupe) de diffusion est actualisée pour les clients associés à ce VAP. La valeur par défaut est 300 secondes et la plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

WPA Enterprise

WPA Enterprise avec RADIUS est une implémentation de la norme IEEE 802.11i Wi-Fi Alliance, qui inclut le chiffrement CCMP (AES) et TKIP. Le mode Enterprise nécessite l'utilisation d'un serveur RADIUS pour l'authentification des utilisateurs.

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

Les paramètres ci-après permettent de configurer WPA Enterprise :

- **WPA Versions** : types de stations clientes à prendre en charge :
  - **WPA** : si toutes les stations clientes du réseau prennent en charge le WPA d'origine, mais qu'aucune d'entre elles n'est compatible avec le WPA2 (plus récent), sélectionnez WPA.
  - **WPA2** : si toutes les stations clientes du réseau prennent en charge WPA2, nous vous conseillons d'utiliser WPA2 qui offre une sécurité optimale avec la norme IEEE 802.11i.
  - **WPA et WPA2** : si vous disposez d'un ensemble de clients, dont certains prennent en charge WPA2 et d'autres prennent en charge uniquement le WPA d'origine, sélectionnez WPA et WPA2. Les stations clientes WPA et WPA2 peuvent ainsi s'associer et s'authentifier, mais peuvent aussi utiliser le WPA2 (plus robuste) pour les clients qui le prennent en charge. Cette configuration WPA offre davantage d'interopérabilité et un peu moins de sécurité.
- **Enable pre-authentication** : si pour WPA Versions, vous sélectionnez uniquement WPA2, ou à la fois WPA et WPA2, vous pouvez activer la pré-authentification pour les clients WPA2.

  Cliquez sur **Enable pre-authentication** si vous souhaitez que les clients sans fil WPA2 puissent envoyer des paquets de pré-authentification. Les informations de pré-authentification sont relayées du périphérique WAP que le client utilise actuellement vers le périphérique WAP cible. L'activation de cette fonction permet d'accélérer l'authentification pour les clients en itinérance qui se connectent à plusieurs points d'accès.

  Cette option ne s'applique pas si vous avez sélectionné WPA pour WPA Versions, car le WPA d'origine ne prend pas en charge cette fonction.
- **Cipher Suites** : suite de chiffrement que vous souhaitez utiliser :
  - TKIP
  - CCMP (AES)

- TKIP et CCMP (AES)

Par défaut, TKIP et CCMP sont sélectionnés. Lorsque TKIP et CCMP sont tous les deux sélectionnés, les stations clientes configurées pour utiliser WPA avec RADIUS doivent avoir l'une des adresses et clés suivantes :

- Une adresse IP RADIUS TKIP et une clé RADIUS valides
- Une adresse IP CCMP (AES) et une clé RADIUS valides

- **Use Global RADIUS Server Settings** : par défaut, chaque VAP utilise les paramètres RADIUS globaux que vous définissez pour le périphérique WAP (voir **Serveur RADIUS**). Toutefois, vous pouvez configurer chaque VAP de façon à ce qu'il utilise un autre groupe de serveurs RADIUS.

  Pour utiliser les paramètres de serveur RADIUS globaux, veillez à cocher la case.

  Pour utiliser un serveur RADIUS distinct pour le VAP, décochez la case et saisissez l'adresse IP du serveur RADIUS, puis renseignez les champs ci-dessous :

- **Server IP Address Type** : version IP utilisée par le serveur RADIUS.

  Vous pouvez basculer entre les différents types d'adresse afin de définir les paramètres d'adresse RADIUS globaux IPv4 et IPv6, mais le périphérique WAP ne contactera que le ou les serveurs RADIUS répondant au type d'adresse que vous sélectionnez dans ce champ.

- **Server IP Address 1** ou **Server IPv6 Address 1** : adresse du serveur RADIUS principal pour ce VAP.

  Si **IPv4** est sélectionné en tant que **Server IP Address Type**, saisissez l'adresse IP du serveur RADIUS que tous les VAP utilisent par défaut (par exemple, 192.168.10.23). Si **IPv6** est sélectionné, saisissez l'adresse IPv6 du serveur RADIUS global principal (par exemple, 2001:DB8:1234::abcd).

- **Server IP Address 2** à **4** ou **Server IPv6 Address 2** à **4** : jusqu'à trois adresses IPv4 et/ou IPv6 à utiliser comme serveurs RADIUS de sauvegarde pour ce VAP.

  Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.

- **Key 1** : clé secrète partagée pour le serveur RADIUS global. Vous pouvez utiliser jusqu'à 63 caractères alphanumériques standard et caractères spéciaux. La clé est sensible à la casse. Vous devez en outre configurer la

même clé sur le périphérique WAP et sur votre serveur RADIUS. Le texte que vous entrez s'affiche sous forme d'astérisques pour empêcher d'autres personnes de voir la clé RADIUS pendant que vous la saisissez.

- **Key 2** à **Key 4** : clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur spécifié dans le champ **Server IP (IPv6) Address 2** utilise **Key 2** ; le serveur spécifié dans le champ **Server IP (IPv6) Address 3** utilise **Key 3**, etc.
- **Enable RADIUS Accounting** : effectue le suivi et la mesure des ressources qui ont été consommées par un utilisateur donné (heure système, volume de données transmises et reçues, etc.)

  Si vous activez la gestion des comptes RADIUS, cette fonctionnalité est activée à la fois pour le serveur RADIUS principal et pour l'ensemble des serveurs de sauvegarde.
- **Active Server** : permet de sélectionner administrativement le serveur RADIUS actif, ce qui évite au périphérique WAP de devoir contacter dans l'ordre chaque serveur configuré et de choisir le premier serveur actif.

  Broadcast Key Refresh Rate : intervalle auquel la clé (groupe) de diffusion est actualisée pour les clients associés à ce VAP.

  La valeur par défaut est 300 secondes. La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.
- **Session Key Refresh Rate** : intervalle auquel le périphérique WAP actualise les clés de session (monodiffusion) pour chaque client associé au VAP.

  La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de session n'est pas actualisée.

Planificateur

Le planificateur de radio et VAP vous permet de configurer une règle avec un intervalle de temps spécifique pour que les VAP ou radios soient opérationnels, ce qui automatise l'activation ou la désactivation des VAP et de la radio.

L'une des manières d'utiliser cette fonction est de planifier la radio pour qu'elle ne fonctionne que pendant les heures de bureau, afin de bénéficier de la sécurité adéquate et de diminuer la consommation électrique. Vous pouvez aussi utiliser le planificateur pour autoriser les clients sans fil à accéder aux VAP uniquement à certaines heures de la journée.

Le Périphérique WAP prend en charge jusqu'à 16 profils. Seules les règles valides sont ajoutées au profil. Vous pouvez regrouper 16 règles maximum pour former un profil de planification. Les entrées de période appartenant au même profil ne peuvent pas se chevaucher.

Ajout de profils de planificateur

Vous pouvez créer jusqu'à 16 noms de profil de planificateur. Par défaut, aucun profil n'est créé.

Pour afficher l'état du planificateur et ajouter un profil de planificateur :

ÉTAPE 1 Sélectionnez **Wireless** > **Scheduler** dans le volet de navigation.

ÉTAPE 2 Assurez-vous que **Administrative Mode** est activé. Il est désactivé par défaut.

La zone Scheduler Operational Status indique l'état de fonctionnement en cours du planificateur :

- **Status** : état opérationnel du planificateur. Les valeurs possibles sont Up et Down. La valeur par défaut est Down.
- **Reason** : raison de l'état opérationnel du planificateur. Les valeurs possibles sont :
  - IsActive : le planificateur est activé administrativement.
  - ConfigDown : l'état opérationnel est désactivé car la configuration globale est désactivée.
  - TimeNotSet : l'heure n'est pas définie sur le périphérique WAP, soit manuellement, soit via le NTP.

ÉTAPE 3 Pour ajouter un profil, saisissez un nom de profil dans la zone de texte **Scheduler Profile Configuration**, puis cliquez sur **Add**. Le nom de profil peut comporter jusqu'à 32 caractères alphanumériques.

Configuration des règles de planificateur

Vous pouvez configurer un maximum de 16 règles par profil. Chaque règle spécifie l'heure de début, l'heure de fin ainsi que le ou les jours de la semaine pendant lesquels la radio ou le VAP peut fonctionner. Les règles sont périodiques et se répètent chaque semaine. Une règle valide doit contenir tous les paramètres

(jours de la semaine, heure et minute) relatifs à l'heure de début et à l'heure de fin. Il ne doit y avoir aucun conflit de règles. Par exemple, vous pouvez configurer une règle commençant chaque jour ouvrable de la semaine et une autre commençant chaque jour du week-end, mais vous ne pouvez pas configurer une règle commençant quotidiennement et une autre commençant le week-end.

Pour configurer une règle pour un profil :

ÉTAPE 1 Sélectionnez le profil dans la liste **Select a Profile Name**.

ÉTAPE 2 Cliquez sur **Ajouter une règle**.

La nouvelle règle s'affiche dans la table des règles.

ÉTAPE 3 Cochez la case en regard du **Profile Name**, puis cliquez sur **Edit**.

ÉTAPE 4 Dans le menu **Day of the Week**, sélectionnez le planning récurrent de la règle. Vous pouvez configurer la règle pour qu'elle s'exécute quotidiennement, chaque jour ouvrable de la semaine, chaque jour du week-end (samedi et dimanche) ou n'importe quel jour de la semaine.

ÉTAPE 5 Définissez les heures de début et de fin :

- **Start Time** : heure à laquelle la radio ou le VAP est opérationnellement activé(e). L'heure est au format 24 heures HH:MM. La plage est <00-23>:<00-59>. La valeur par défaut est 00:00.
- End Time : heure à laquelle la radio ou le VAP est opérationnellement désactivé(e). L'heure est au format 24 heures HH:MM. La plage est <00-23>:<00-59>. La valeur par défaut est 00:00.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Pour être mis en œuvre, un profil de planificateur doit être associé à une interface radio ou une interface VAP. Reportez-vous à la page **Association de planificateur**.

REMARQUE Pour supprimer une règle, sélectionnez le profil dans la colonne **Profile Name**, puis cliquez sur **Delete**.

Association de planificateur

Pour être mis en œuvre, les profils de planificateur doivent être associés à l'interface WLAN ou à une interface VAP. Par défaut, aucun profil de planificateur n'est créé et aucun profil n'est associé à une radio ou un VAP.

Un seul profil de planificateur peut être associé à l'interface WLAN ou à chaque VAP. Un seul profil peut être associé à plusieurs VAP. En cas de suppression du profil de planificateur associé à un VAP ou à l'interface WLAN, l'association est supprimée.

Pour associer un profil de planificateur à l'interface WLAN ou un VAP :

ÉTAPE 1 Sélectionnez **Wireless** > **Scheduler Association** dans le volet de navigation.

ÉTAPE 2 Pour l'interface WLAN ou un VAP, sélectionnez le profil dans la liste **Profile Name**.

La colonne **Interface Operational Status** indique si l'interface est actuellement activée ou désactivée.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Utilisation de la bande passante

La page Bandwidth Utilization vous permet de définir le volume de bande passante radio pouvant être consommé avant que le périphérique WAP ne cesse d'autoriser de nouvelles associations de clients. Cette fonctionnalité est désactivée par défaut.

Pour activer l'utilisation de la bande passante :

ÉTAPE 1 Sélectionnez **Wireless** > **Bandwidth Utilization** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Enable** pour le paramètre **Bandwidth Utilization**.

ÉTAPE 3 Dans le champ **Maximum Utilization Threshold**, saisissez le pourcentage d'utilisation de la bande passante réseau autorisé sur la radio avant que le périphérique WAP ne cesse d'accepter de nouvelles associations de clients.

La plage de nombres entiers valide est comprise entre 0 et 100 pour cent. La valeur par défaut est 70 pour cent. Si elle est définie à 0, toutes les nouvelles associations sont autorisées quel que soit le taux d'utilisation.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Filtrage MAC

Le filtrage Media Access Control (MAC) peut être utilisé pour interdire ou autoriser uniquement l'authentification des stations clientes répertoriées sur le point d'accès. L'authentification MAC doit être activée ou désactivée pour chaque VAP sur la page **Networks**. Selon la configuration du VAP, le périphérique WAP peut se référer à une liste de filtrage MAC stockée sur un serveur RADIUS externe ou stockée localement sur le périphérique WAP.

Configuration d'une liste de filtrage MAC stockée localement sur le périphérique WAP

Le périphérique WAP ne prend en charge qu'une seule liste de filtrage MAC locale. Ainsi, la même liste s'applique à tous les VAP autorisés à utiliser la liste locale. Le filtre peut être configuré pour accorder l'accès uniquement aux adresses MAC spécifiées dans la liste, ou pour interdire l'accès uniquement aux adresses spécifiées dans la liste.

Vous pouvez ajouter un maximum de 512 adresses MAC dans la liste de filtrage.

Pour configurer le filtrage MAC :

ÉTAPE 1 Sélectionnez **Wireless** > **MAC Filtering** dans le volet de navigation.

ÉTAPE 2 Sélectionnez la façon dont le périphérique WAP utilise la liste de filtrage :

- **Allow only stations in the list** : toute station qui n'apparaît pas dans la Stations List se voit interdire l'accès au réseau via le périphérique WAP.

- **Block all stations in list** : seules les stations qui apparaissent dans la liste se voient interdire l'accès au réseau via le périphérique WAP. L'accès est autorisé pour toutes les autres stations.

  REMARQUE Le paramètre de filtre s'applique également à la liste de filtrage MAC stockée sur le serveur RADIUS, s'il en existe une.

ÉTAPE 3 Dans le champ **MAC Address**, saisissez l'adresse MAC à autoriser ou bloquer, puis cliquez sur **Add**.

L'adresse MAC s'affiche dans la **Stations List**.

ÉTAPE 4 Continuez à saisir des adresses MAC jusqu'à ce que la liste soit terminée, puis cliquez sur **Save**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Pour supprimer une adresse MAC de la Stations List, sélectionnez-la, puis cliquez sur **Remove**.

REMARQUE Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Configuration de l'authentification MAC sur le serveur RADIUS

Si un ou plusieurs VAP sont configurés pour utiliser un filtre MAC stocké sur un serveur d'authentification RADIUS, vous devez configurer la liste des stations sur le serveur RADIUS. Le format de la liste est décrit dans le tableau ci-dessous :

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

Pont WDS

Le Wireless Distribution System (WDS) vous permet de connecter plusieurs périphériques WAP121 et WAP321. Avec WDS, les points d'accès peuvent communiquer entre eux sans câbles. Cette fonctionnalité est essentielle à la satisfaction des clients en itinérance et à la gestion de plusieurs réseaux sans fil. Elle simplifie également l'infrastructure réseau en réduisant la quantité de câbles nécessaire. Vous pouvez configurer le périphérique WAP en mode point à point ou point à multipoint en fonction du nombre de liaisons à connecter.

En mode point à point, le périphérique WAP accepte les associations de clients et communique avec les clients sans fil et autres répéteurs. Le périphérique WAP transfère tout le trafic destiné à l'autre réseau via le tunnel établi entre les points d'accès. Le pont n'est pas ajouté au nombre de sauts. Il fonctionne comme simple périphérique réseau OSI Layer 2.

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

Le Périphérique WAP peut également fonctionner en tant que répéteur. Dans ce mode, le Périphérique WAP sert de connexion entre deux périphériques WAP qui sont trop éloignés pour être à portée cellulaire. Lorsqu'il fonctionne en tant que répéteur, le Périphérique WAP n'a aucune connexion filaire au réseau local (LAN) et répète les signaux par l'intermédiaire de la connexion sans fil. Aucune configuration spéciale n'est requise pour permettre au Périphérique WAP de fonctionner en tant que répéteur et il n'existe pas de paramètres de mode répéteur. Les clients sans fil peuvent toujours se connecter à un périphérique WAP qui fonctionne en tant que répéteur.

Avant de configurer WDS sur le périphérique WAP, veuillez noter les informations ci-après :

- WDS fonctionne seulement avec les périphériques Cisco WAP121 et Cisco WAP321.
- Tous les périphériques WAP Cisco intégrés à une liaison WDS doivent avoir les paramètres identiques suivants :
  - Radio
  - IEEE 802.11 Mode

- Channel Bandwidth
- Channel (l'option Auto n'est pas recommandée)

REMARQUE Si vous effectuez un pontage dans la bande 802.11n 2,4 GHz, définissez Channel Bandwidth sur 20 MHz au lieu du paramètre 20/40 MHz par défaut. Dans la bande 2,4 GHz 20/40 MHz, la bande passante de fonctionnement peut passer de 40 MHz à 20 MHz si des périphériques WAP 20 MHz sont détectés dans la zone. Une bande passante de canal incohérente peut entraîner la déconnexion du lien.

Reportez-vous à la section **Radio** (paramètres de base) pour obtenir des informations sur la définition de ces paramètres.

- Lorsque vous utilisez WDS, veillez à le configurer sur les deux périphériques WAP intégrés à la liaison WDS.
- Vous ne pouvez avoir qu'une seule liaison WDS entre n'importe quelle paire de périphériques WAP. Ainsi, une adresse MAC distante ne peut apparaître qu'une seule fois sur la page WDS pour un périphérique WAP donné.

Pour configurer un pont WDS :

ÉTAPE 1 Sélectionnez **Wireless** > **WDS Bridge** dans le volet de navigation.

ÉTAPE 2 Sélectionnez **Enable** pour **Spanning Tree Mode**. Une fois l'activation effectuée, STP empêche les boucles de basculement. STP est recommandé si vous configurez des liaisons WDS.

ÉTAPE 3 Sélectionnez **Enable** pour **WDS Interface**.

ÉTAPE 4 Définissez les paramètres restants :

- **Remote MAC Address** : spécifie l'adresse MAC du périphérique WAP de destination, à savoir le périphérique WAP situé à l'autre extrémité de la liaison WDS et auquel les données sont envoyées ou transmises et à partir duquel les données sont reçues.

CONSEIL L'adresse MAC est indiquée sur la page Status and Statistics > Network Interface.

- **Encryption** : type de chiffrement à utiliser sur la liaison WDS ; il ne doit pas obligatoirement correspondre au VAP pour lequel vous effectuez un pontage. Les paramètres de chiffrement WDS sont propres au pont WDS. Les options disponibles sont none, WEP et WPA Personal.

Si vous ne souhaitez pas sécuriser la liaison WDS, vous pouvez choisir de ne définir aucun type de chiffrement. De même, si vous souhaitez sécuriser la liaison, vous pouvez choisir entre Static WEP et WPA Personal. En mode WPA Personal, le périphérique WAP utilise le chiffrement WPA2-PSK avec CCMP (AES) sur la liaison WDS. Pour plus d'informations sur les options de chiffrement, reportez-vous à la section **WEP sur les liaisons WDS** ou **WPA/PSK sur les liaisons WDS** après cette procédure.

ÉTAPE 5 Répétez ces étapes pour un maximum de trois interfaces WDS supplémentaires.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

ÉTAPE 7 Répliquez cette procédure sur le ou les autres périphériques connectés au pont.

CONSEIL Vous pouvez vérifier si la liaison de pont est active en vous rendant sur la page Status and Statistics > Network Interface. Dans le tableau Interface Status, l'état Up doit être spécifié pour WLAN0:WDS(x).

AVERTISSEMENT Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

WEP sur les liaisons WDS

Ces champs supplémentaires apparaissent lorsque vous sélectionnez le type de chiffrement WEP.

- **Key Length** : si le WEP est activé, spécifiez si la clé WEP doit avoir une longueur de **64 bits** ou **128 bits**.
- **Key Type** : si le WEP est activé, spécifiez le type de clé WEP : **ASCII** ou **Hex**.
- **WEP Key** : si vous avez sélectionné **ASCII**, saisissez toute combinaison de 0 à 9, a à z, et A à Z. Si vous avez sélectionné **Hex**, saisissez des chiffres hexadécimaux (toute combinaison de 0 à 9, a à f, ou A à F). Il s'agit des clés de chiffrement RC4 partagées avec les stations par l'intermédiaire du périphérique WAP.

Veuillez noter que le nombre de caractères requis est indiqué à droite du champ et change en fonction de vos sélections dans les champs **Key Type** et **Key Length**.

WPA/PSK sur les liaisons WDS

Ces champs supplémentaires apparaissent lorsque vous sélectionnez le type de chiffrement WPA/PSK.

- **WDS ID** : saisissez un nom approprié pour la nouvelle liaison WDS que vous avez créée. Il est important que le même WDS ID soit aussi entré à l'autre extrémité de la liaison WDS. Si ce WDS ID n'est pas identique pour les deux périphériques WAP sur la liaison WDS, ils ne pourront pas communiquer et échanger des données.

  Le WDS ID peut être n'importe quelle combinaison alphanumérique.

- **Key** : saisissez une clé partagée unique pour le pont WDS. Cette clé partagée unique doit aussi être saisie pour le périphérique WAP situé à l'autre extrémité de la liaison WDS. Si cette clé n'est pas identique pour les deux WAP, ceux-ci ne pourront pas communiquer et échanger des données.

  La clé WPA-PSK est une chaîne de 8 caractères minimum et de 63 caractères maximum. Les caractères acceptés sont les lettres alphabétiques majuscules et minuscules, les chiffres numériques et les symboles spéciaux comme @ et #.

Pont de groupe de travail

La fonction WorkGroup Bridge du Périphérique WAP permet au périphérique WAP d'étendre l'accessibilité d'un réseau distant. En mode WorkGroup Bridge, le Périphérique WAP fonctionne comme une station sans fil (STA) sur le réseau local (LAN) sans fil. Il peut acheminer le trafic entre un réseau filaire distant ou des clients sans fil associés et le réseau local (LAN) sans fil qui est connecté via le mode WorkGroup Bridge.

La fonction WorkGroup Bridge permet la prise en charge simultanée du mode STA et du mode AP. Le périphérique WAP peut fonctionner dans un seul BSS (Basic Service Set) en tant que périphérique STA tout en fonctionnant sur un autre BSS en tant que Périphérique WAP. Lorsque le mode WorkGroup Bridge est activé, le Périphérique WAP prend en charge un seul BSS pour les clients sans fil qui s'associent à celui-ci, et un autre BSS auquel le Périphérique WAP s'associe en tant que client sans fil.

Il est recommandé d'utiliser le mode WorkGroup Bridge uniquement lorsque la fonction WDS Bridge ne peut pas fonctionner avec un Périphérique WAP homologue. WDS est une meilleure solution et doit être préférée à la solution WorkGroup Bridge. Utilisez WDS si vous effectuez un pontage des périphériques Cisco WAP121 et WAP321. Si ce n'est pas le cas, optez pour WorkGroup Bridge. Lorsque la fonction WorkGroup Bridge est activée, les configurations VAP ne sont pas appliquées ; seule la configuration WorkGroup Bridge est appliquée.

REMARQUE La fonction WDS ne fonctionne pas lorsque le mode WorkGroup Bridge est activé sur le Périphérique WAP.

En mode WorkGroup Bridge, le BSS géré par le périphérique WAP fonctionnant en mode de périphérique WAP est appelé l'interface de point d'accès, et les STA associés sont appelés les STA descendants. Le BSS géré par l'autre périphérique WAP (c'est-à-dire celui auquel le périphérique WAP s'associe en tant que STA) est appelé l'interface cliente d'infrastructure, et l'autre périphérique WAP est appelé le point d'accès montant.

Les périphériques connectés à l'interface filaire du périphérique WAP, ainsi que les stations descendantes associées à l'interface de point d'accès du périphérique, peuvent accéder au réseau connecté par l'interface cliente d'infrastructure. Pour autoriser le pontage des paquets, les configurations VLAN de l'interface de point d'accès et de l'interface filaire doivent correspondre à celle de l'interface cliente d'infrastructure.

Le mode WorkGroup Bridge peut être utilisé comme extension de portée afin de permettre au BSS de fournir un accès aux réseaux distants ou difficiles d'accès. Une radio unique peut être configurée pour transférer les paquets des STA associés vers un autre périphérique WAP du même ESS, sans utiliser de WDS.

Avant de configurer WorkGroup Bridge sur le périphérique WAP, veuillez noter les informations ci-après :

- Tous les périphériques WAP intégrés à WorkGroup Bridge doivent avoir les paramètres identiques suivants :
  - Radio
  - IEEE 802.11 Mode
  - Channel Bandwidth
  - Channel (l'option Auto n'est pas recommandée)

  Reportez-vous à la section **Radio** (paramètres de base) pour obtenir des informations sur la définition de ces paramètres.

- Le mode WorkGroup Bridge prend actuellement en charge le trafic IPv4 uniquement.
- Le mode WorkGroup Bridge n'est pas pris en charge via une configuration de point unique.

Pour configurer le mode WorkGroup Bridge :

ÉTAPE 1 Sélectionnez **Wireless** > **WorkGroup Bridge** dans le volet de navigation.

ÉTAPE 2 Sélectionnez **Enable** pour **WorkGroup Bridge Mode**.

ÉTAPE 3 Définissez les paramètres suivants pour l'interface cliente d'infrastructure (montante) :

- **SSID** : SSID du BSS.

  REMARQUE Une flèche est présente à côté du SSID pour l'analyse SSID (SSID Scanning) ; cette fonction est désactivée par défaut et est uniquement activée si la détection de point d'accès (AP Detection) est activée dans la détection de point d'accès non autorisé (Rogue AP Detection) (qui est également désactivée par défaut).

- **Security** : type de sécurité à utiliser pour l'authentification en tant que station cliente sur le périphérique WAP montant. Les choix possibles sont :
  - **None**
  - **Static WEP**
  - **WPA Personal**
  - **WPA Enterprise**

  Reportez-vous à la section **Définition des paramètres de sécurité** pour plus d'informations sur les paramètres de sécurité WEP et WPA Personal.

- **VLAN ID** : VLAN associé au BSS.

  REMARQUE L'interface cliente d'infrastructure sera associée au périphérique WAP montant avec les informations d'identification configurées. Le périphérique WAP peut obtenir son adresse IP d'un serveur DHCP sur la liaison montante. Vous pouvez également attribuer une adresse IP statique. Le champ **Connection Status** indique si le WAP est connecté au périphérique WAP montant. Vous pouvez cliquer sur le bouton **Refresh** en haut de la page pour afficher l'état actuel de la connexion.

ÉTAPE 4 Configurez les champs supplémentaires suivants pour l'interface de point d'accès :

- **Status** : sélectionnez **Enable** pour l'interface de point d'accès.
- **SSID** : le SSID de l'interface de point d'accès ne doit pas être identique au SSID client d'infrastructure. Toutefois, si vous souhaitez une prise en charge d'un type de scénario d'itinérance, le SSID et la sécurité doivent être identiques.
- **SSID Broadcast** : indiquez si vous souhaitez que le SSID descendant soit diffusé. La diffusion SSID est activée par défaut.
- **Security** : type de sécurité à utiliser pour l'authentification. Les choix possibles sont :
  - **None**
  - **Static WEP**
  - **WPA Personal**
- **MAC Filtering** : sélectionnez l'une des options ci-après :
  - **Disabled** : le groupe de clients dans le BSS de points d'accès pouvant accéder au réseau montant n'est pas restreint aux clients spécifiés dans une liste d'adresses MAC.
  - **Local** : le groupe de clients dans le BSS de points d'accès pouvant accéder au réseau montant est restreint aux clients spécifiés dans une liste d'adresses MAC localement définie.
  - **RADIUS** : le groupe de clients dans le BSS de points d'accès pouvant accéder au réseau montant est restreint aux clients spécifiés dans une liste d'adresses MAC sur un serveur RADIUS.

  Si vous sélectionnez Local ou RADIUS, reportez-vous à la section **Filtrage MAC** pour obtenir des instructions sur la création de la liste de filtrage MAC.
- **VLAN ID** : configurez l'interface de point d'accès avec le même ID de VLAN que celui annoncé sur l'interface cliente d'infrastructure.

ÉTAPE 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Les clients descendants associés sont désormais connectés au réseau montant.

Qualité de service

Les paramètres de qualité de service (QoS) vous permettent de configurer des files d'attente de transmission pour bénéficier d'un meilleur débit et de meilleures performances si vous administrez un trafic sans fil différencié, comme la voix sur IP (VoIP), d'autres types de lecture audio, vidéo et multimédia en continu, ainsi que des données IP classiques.

Pour configurer la qualité de service (QoS) sur le Périphérique WAP, définissez les paramètres sur les files d'attente de transmission pour les différents types de trafic sans fil et spécifiez les temps d'attente minimum et maximum (via les fenêtres de contention) pour la transmission.

Les paramètres EDCA (Enhanced Distributed Channel Access) du WAP affectent le trafic transmis du périphérique WAP vers la station cliente.

Les paramètres EDCA de la station affectent le trafic transmis de la station cliente vers le périphérique WAP.

En utilisation normale, les valeurs EDCA par défaut du périphérique WAP et de la station ne requièrent aucune modification. La modification de ces valeurs affecte la qualité de service (QoS) fournie.

Pour définir les paramètres EDCA du périphérique WAP et de la station :

ÉTAPE 1 Sélectionnez **Wireless** > **QoS** dans le volet de navigation.

ÉTAPE 2 Sélectionnez une option dans la liste **EDCA Template** :

- **WFA Defaults** : renseigne les paramètres EDCA du périphérique WAP et de la station avec les valeurs WiFi Alliance par défaut, qui sont optimales pour un trafic mixte général.
- **Optimized for Voice** : renseigne les paramètres EDCA du périphérique WAP et de la station avec les valeurs les plus adaptées au trafic vocal.
- **Custom** : vous permet de choisir des paramètres EDCA personnalisés.

Ces quatre files d'attente sont définies pour les différents types de données transmises du WAP vers la station. Si vous choisissez un modèle personnalisé, les paramètres qui définissent les files d'attente sont configurables ; sinon, ils ont des valeurs prédéfinies appropriées à votre sélection. Les quatre files d'attente sont :

- Data 0 (Voice) : file d'attente de haute priorité, délai minimal. Les données devant être transmises rapidement, comme le VoIP et la lecture multimédia en continu, sont automatiquement envoyées vers cette file d'attente.

- Data 1 (Video) : file d'attente de haute priorité, délai minimal. Les données vidéo devant être transmises rapidement sont automatiquement envoyées vers cette file d'attente.
- Data 2 (Best Effort) : file d'attente de moyenne priorité, débit et délai moyens. La plupart des données IP classiques sont envoyées vers cette file d'attente.
- Data 3 (Background) : file d'attente de basse priorité, haut débit. Les données en bloc nécessitant un débit maximal et dont la rapidité n'est pas essentielle sont envoyées vers cette file d'attente (les données FTP, par exemple).

ÉTAPE 3 Définissez les paramètres EDCA de station suivants :

REMARQUE Ces paramètres ne peuvent être définis que si vous avez sélectionné Custom à l'étape précédente.

- **Arbitration Inter-Frame Space** : temps d'attente pour les trames de données. Le temps d'attente se mesure en emplacements. Les valeurs valides pour AIFS sont comprises entre 1 et 255.
- **Minimum Contention Window** : entrée dans l'algorithme qui détermine le temps d'attente d'interruption aléatoire initial (fenêtre) pour une nouvelle tentative de transmission.

  Cette valeur est la limite supérieure (en millisecondes) d'une plage à partir de laquelle le temps d'attente d'interruption aléatoire initial est déterminé.

  Le premier nombre aléatoire généré est un nombre compris entre 0 et le nombre spécifié ici.

  Si le premier temps d'attente d'interruption aléatoire expire avant l'envoi de la trame de données, un compteur de tentatives est incrémenté et la valeur d'interruption aléatoire (fenêtre) est doublée. Le doublage continue jusqu'à ce que la taille de la valeur d'interruption aléatoire atteigne le nombre défini dans le champ Maximum Contention Window.

  Les valeurs valides sont 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1024. La valeur spécifiée doit être inférieure à celle du champ Maximum Contention Window.
- **Maximum Contention Window** : limite supérieure (en millisecondes) pour le doublage de la valeur d'interruption aléatoire. Ce doublage continue jusqu'à ce que la trame de données soit envoyée ou que la taille Maximum Contention Window soit atteinte.

  Une fois la taille Maximum Contention Window atteinte, les nouvelles tentatives se poursuivent jusqu'à ce que le nombre maximal autorisé de tentatives soit atteint.

Les valeurs valides sont 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1024. La valeur spécifiée doit être supérieure à celle du champ Minimum Contention Window.

- **Maximum Burst** (WAP only) : paramètre EDCA WAP qui s'applique uniquement au trafic ente le WAP et la station cliente.

  Cette valeur spécifie (en millisecondes) la longueur de rafale maximale autorisée pour les rafales de paquets sur le réseau sans fil. Une rafale de paquets est un groupe de plusieurs trames transmises sans informations d'en-tête. La baisse de la charge de traitement génère un débit plus élevé et de meilleures performances.

  Les valeurs valides sont comprises entre 0,0 et 999.

- **Wi-Fi MultiMedia (WMM)** : sélectionnez **Enable** pour activer les extensions Wi-Fi MultiMedia (WMM). Ce champ est activé par défaut. Lorsque WMM est activé, la définition des priorités de qualité de service (QoS) et la coordination de l'accès au support sans fil sont activées. Lorsque WMM est activé, les paramètres de qualité de service (QoS) sur le Périphérique WAP contrôlent le trafic descendant transmis du périphérique WAP vers la station cliente (paramètres EDCA de point d'accès), ainsi que le trafic montant transmis de la station vers le point d'accès (paramètres EDCA de station).

  La désactivation de WMM désactive le contrôle de qualité de service (QoS) des paramètres EDCA de station sur le trafic montant transmis de la station vers le périphérique WAP. Lorsque WMM est désactivé, vous pouvez toujours définir certains paramètres sur le trafic descendant transmis du périphérique WAP vers la station cliente (paramètres EDCA de point d'accès).

- **TXOP Limit** (Station only) : la limite TXOP est un paramètre EDCA de station. Il s'applique uniquement au trafic transmis de la station cliente vers le périphérique WAP. L'opportunité de transmission (Transmission Opportunity, TXOP) est l'intervalle en millisecondes pendant lequel une station cliente WME est autorisée à initier des transmissions sur le support sans fil (Wireless Medium, WM) vers le périphérique WAP. La valeur maximale du paramètre TXOP Limit est 65 535.

ÉTAPE 4 Définissez les paramètres supplémentaires suivants :

- **No Acknowledgement** : sélectionnez **Enable** pour spécifier que le périphérique WAP ne doit pas accepter les trames ayant la valeur de classe de service QosNoAck.

- **Unscheduled Automatic Power Save Delivery** : sélectionnez **Enable** pour activer APSD, qui est une méthode de gestion de l'alimentation. APSD est recommandée si les téléphones VoIP accèdent au réseau via le périphérique WAP.

ÉTAPE 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

AVERTISSEMENT Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Configuration de WPS

Cette section décrit le protocole Wi-Fi Protected Setup (WPS) et sa configuration sur le périphérique WAP.

Vue d'ensemble du protocole WPS

WPS est une norme qui permet d'établir simplement des réseaux sans fil sans compromettre la sécurité du réseau. Il évite aux utilisateurs de clients sans fil et aux administrateurs de périphériques WAP de devoir connaître les noms réseau, clés et autres options de configuration du chiffrement.

WPS simplifie la configuration du réseau en permettant à l'administrateur d'utiliser un bouton poussoir ou un code PIN pour établir des réseaux sans fil, ce qui évite de devoir saisir manuellement les noms réseau (SSID) et les paramètres de sécurité sans fil :

- **Bouton poussoir** : le bouton WPS est soit un bouton se trouvant sur le produit, soit un bouton cliquable dans l'interface utilisateur.
- **Personal Identification Number (PIN)** : le code PIN est disponible dans l'interface utilisateur du produit.

WPS gère la sécurité du réseau en demandant aux utilisateurs des nouveaux périphériques clients et aux administrateurs WLAN de disposer d'un accès physique à leurs périphériques respectifs ou de sécuriser l'accès distant à ces périphériques.

Scénarios d'utilisation

Il existe plusieurs scénarios typiques d'utilisation de WPS :

- Un utilisateur souhaite inscrire une station cliente dans un WLAN compatible WPS. (Le périphérique client en cours d'inscription peut détecter le réseau et inviter l'utilisateur à effectuer l'inscription, bien que cela ne soit pas nécessaire.) L'utilisateur déclenche l'inscription en appuyant sur un bouton situé sur le périphérique client. L'administrateur du périphérique WAP appuie alors sur un bouton situé sur le périphérique WAP. Au cours d'un bref échange de messages de protocole WPS, le périphérique WAP fournit au nouveau client une nouvelle configuration de sécurité par l'intermédiaire du protocole EAP (Extensible Authentication Protocol). Les deux périphériques se dissocient, s'associent à nouveau, puis s'authentifient avec les nouveaux paramètres.
- Un utilisateur souhaite inscrire une station cliente dans un WLAN compatible WPS en fournissant le code PIN du périphérique client à l'administrateur du périphérique WAP. L'administrateur saisit ce code PIN dans l'utilitaire de configuration du périphérique WAP et déclenche l'inscription du périphérique. Le nouveau candidat à l’inscription et le périphérique WAP échangent des messages WPS qui incluent une nouvelle configuration de sécurité, se dissocient, s'associent à nouveau et s'authentifient.
- Un administrateur de périphérique WAP achète un nouveau périphérique WAP qui a été certifié par Wi-Fi Alliance comme étant compatible avec WPS version 2.0, et souhaite ajouter le périphérique WAP à un réseau (filaire ou sans fil) existant. L'administrateur met le périphérique WAP sous tension, puis accède à un hôte réseau prenant en charge le protocole d'enregistrement WPS. L'administrateur saisit le code PIN du périphérique WAP dans l'utilitaire de configuration de ce registre externe, puis déclenche le processus d'enregistrement WPS. (Sur un réseau local filaire, les messages de protocole WPS sont transmis via le protocole Universal Plug and Play, abrégé UPnP.) L'hôte inscrit le WAP en tant que nouveau périphérique réseau et le configure avec les nouveaux paramètres de sécurité.

- Un administrateur de périphérique WAP a ajouté un nouveau périphérique WAP à un réseau (sans fil ou filaire) existant via WPS, et souhaite donner un accès réseau à un nouveau périphérique client. Le périphérique est inscrit via la méthode PIN ou PBC (Push-Button Control) décrite ci-dessus, mais cette fois le périphérique s'inscrit dans le registre externe, le périphérique WAP fonctionnant uniquement comme proxy.
- Un périphérique sans fil qui ne prend pas en charge WPS doit intégrer le WLAN compatible WPS. L'administrateur, qui ne peut pas utiliser WPS dans ce cas, configure alors manuellement le périphérique avec le SSID, la clé publique partagée et les modes de chiffrement du périphérique WAP compatible WPS. Le périphérique intègre le réseau.

Le code PIN est soit un numéro à huit chiffres qui utilise son dernier chiffre comme valeur de somme de contrôle, soit un numéro à quatre chiffres sans somme de contrôle. Chacun de ces nombres peut commencer par des zéros.

Rôles WPS

La norme WPS attribue des rôles spécifiques aux divers composants de son architecture :

- **Enrollee** : périphérique pouvant intégrer le réseau sans fil.
- **AP** : périphérique fournissant un accès sans fil au réseau.
- **Registrar** : entité qui transmet des informations d'identification de sécurité aux candidats à l'inscription et qui configure les points d'accès.

Les périphériques WAP fonctionnent en tant que points d'accès et prennent en charge un registre intégré. Ils ne fonctionnent pas en tant que candidat à l'inscription.

Activation et désactivation de WPS sur un VAP.

L'administrateur ne peut activer ou désactiver WPS que sur un seul VAP. WPS est uniquement opérationnel si ce VAP respecte les conditions suivantes :

- Le périphérique WAP est configuré pour diffuser le SSID du VAP.
- Le filtrage des adresses MAC est désactivé sur le VAP.
- Le chiffrement WEP est désactivé sur le VAP.
- Le VAP est configuré pour utiliser la sécurité WPA-Personal ou none. Si le mode de chiffrement WPA2-PSK est activé, une clé prépartagée (PSK) valide doit être configurée et le chiffrement CCMP (AES) doit être activé.

- Le VAP est opérationnellement activé.

WPS est opérationnellement désactivé sur le VAP si une des conditions suivantes n'est pas remplie.

REMARQUE La désactivation de WPS sur un VAP n'entraîne pas la dissociation des clients précédemment authentifiés via WPS sur ce VAP.

Enregistrement externe et interne

Il n'est pas nécessaire que les périphériques WAP gèrent l'enregistrement des clients sur les réseaux eux-mêmes. Le périphérique WAP peut soit utiliser son registre intégré, soit fonctionner en tant que proxy pour un registre externe. Le registre externe est accessible via le réseau local (LAN) filaire ou sans fil. Un registre externe peut aussi configurer le SSID, le mode de chiffrement et la clé publique partagée d'un BSS compatible WPS. Cette fonctionnalité est très utile pour les déploiements prêts à l'emploi, c'est-à-dire lorsqu'un administrateur associe simplement un nouveau périphérique WAP à un réseau local (LAN) pour la première fois.

Si le Périphérique WAP utilise un registre intégré, il inscrit les nouveaux clients en utilisant la configuration du VAP associé au service WPS, que cette configuration ait été définie directement sur le périphérique WAP ou acquise par un registre externe via WPS.

Inscription de client

Méthode Push-Button Control (PBC)

Le Périphérique WAP inscrit les clients 802.11 via WPS grâce à l'une des deux méthodes suivantes : la méthode Push-Button Control (PBC) ou la méthode Personal Identification Number (PIN).

La méthode PBC est utilisée lorsque l'utilisateur d'un client potentiel appuie sur un bouton situé sur le périphérique en cours d'inscription, et que l'administrateur du périphérique WAP équipé d'un registre intégré appuie sur un bouton (matériel ou logiciel) similaire. Cette séquence commence le processus d'inscription et le périphérique client intègre le réseau. Même si les périphériques WAP Cisco ne comportent pas de bouton physique, l'administrateur peut initier l'inscription pour un VAP donné à l'aide d'un bouton logiciel présent dans l'utilitaire de configuration Web.

REMARQUE Il est possible d'appuyer sur les boutons du périphérique client et du périphérique WAP dans n'importe quel ordre. N'importe quel périphérique peut initier l'inscription. Toutefois, si vous appuyez sur le bouton logiciel du Périphérique WAP, et qu'aucun client ne tente de s'inscrire au bout de 120 secondes, le Périphérique WAP met fin à la transaction d'inscription WPS en cours.

Méthode Personal Identification Number (PIN)

Un client peut aussi s'inscrire dans un registre à l'aide d'un code PIN. Par exemple, l'administrateur du Périphérique WAP peut commencer une transaction d'inscription pour un VAP particulier en saisissant le code PIN d'un client. Lorsque le client détecte le périphérique compatible WPS, l'utilisateur peut fournir son code PIN au Périphérique WAP afin de poursuivre le processus d'inscription. Une fois le protocole WPS terminé, le client intègre le réseau en toute sécurité. Le client peut aussi initier ce processus.

Comme pour la méthode PBC, si le Périphérique WAP commence la transaction d'inscription et qu'aucun client ne tente de s'inscrire au bout de 120 secondes, le Périphérique WAP met fin à la transaction en cours.

Utilisation facultative du registre intégré

Bien que le Périphérique WAP prenne en charge un registre intégré pour WPS, son utilisation est facultative. Une fois qu'un registre externe a configuré le Périphérique WAP, le Périphérique WAP fonctionne en tant que proxy pour ce registre externe, peu importe si le registre intégré du périphérique WAP est activé (par défaut, il est activé).

Fonctionnalité de verrouillage

Chaque Périphérique WAP stocke un code PIN de périphérique compatible WPS dans la mémoire vive (RAM) non volatile. WPS requiert ce code PIN si un administrateur souhaite autoriser un Périphérique WAP non configuré (à savoir paramétré avec les valeurs d'usine, WPS étant activé sur un VAP) à intégrer un réseau. Dans ce scénario, l'administrateur obtient la valeur du code PIN à partir de l'utilitaire de configuration du Périphérique WAP.

L'administrateur peut souhaiter changer le code PIN si l'intégrité du réseau a été compromise. Le Périphérique WAP offre une méthode permettant de générer un nouveau code PIN et de stocker cette valeur dans la NVRAM. Si la valeur présente dans la NVRAM est corrompue, effacée ou manquante, un nouveau code PIN est généré par le Périphérique WAP et stocké dans la NVRAM.

La méthode PIN d'inscription est potentiellement vulnérable en cas d'attaques en force brute. Un intrus réseau peut essayer de se faire passer pour un registre externe sur le réseau local (LAN) sans fil et tenter d'extraire la valeur PIN du périphérique WAP en appliquant de manière exhaustive des codes PIN compatibles WPS. Pour ne pas être soumis à cette vulnérabilité, au cas où un registre ne parvient pas à fournir un code PIN correct en trois tentatives et en 60 secondes, le Périphérique WAP empêche toute tentative ultérieure d'un registre externe de s'inscrire avec le Périphérique WAP sur le VAP compatible WPS en 60 secondes. La durée de verrouillage augmente si d'autres échecs se produisent ; elle peut atteindre 64 minutes maximum. La fonctionnalité d'enregistrement des périphériques WAP passe en verrouillage permanent après 10 échecs consécutifs. Réinitialisez le périphérique pour redémarrer la fonctionnalité d'enregistrement.

Cependant, les stations clientes sans fil peuvent s'inscrire dans le registre intégré du Périphérique WAP, si celui-ci est activé, pendant cette période de verrouillage. Le Périphérique WAP continue également à fournir les services de proxy pour les demandes d'inscription sur les registres externes.

Le Périphérique WAP dispose de fonctions de sécurité supplémentaires pour la protection de son code PIN de périphérique. Lorsque le Périphérique WAP a terminé son enregistrement sur un registre externe, et que la transaction WPS qui en résulte est terminée, le code PIN du périphérique est automatiquement regénéré.

Modifications apportées à la configuration du VAP

Le protocole WPS peut définir les paramètres suivants pour un VAP compatible WPS sur un périphérique WAP :

- SSID réseau
- Options de gestion des clés (WPA-PSK, ou WPA-PSK et WPA2-PSK)
- Options de chiffrement (CCMP/AES, ou TKIP et CCMP/AES)
- Clé (publique partagée) réseau

Si un VAP est activé pour WPS, ces paramètres de configuration peuvent être modifiés, mais restent inchangés entre les différents redémarrages du périphérique WAP.

Enregistrement externe

Le Périphérique WAP prend en charge l'enregistrement sur les registres externes (External Registrars, ER) WPS qui sont présents sur le réseau local filaire ou sans fil. Sur le WLAN, les registres externes annoncent leurs fonctionnalités dans des éléments d'informations (Information Elements, IEs) spécifiques à WPS de leurs trames de balise ; sur le réseau local filaire, les registres externes annoncent leur présence via UPnP.

WPS v2.0 ne nécessite pas d'enregistrement sur un ER via l'interface utilisateur. L'administrateur peut inscrire le Périphérique WAP sur un ER en procédant comme suit :

ÉTAPE 1 Saisir le code PIN ER sur le périphérique WAP.

ÉTAPE 2 Saisir le code PIN du périphérique WAP sur l'interface utilisateur du ER.

REMARQUE Le processus d'enregistrement peut aussi configurer le Périphérique WAP comme spécifié à la section Modifications apportées à la configuration du VAP, si le Périphérique WAP a déclaré dans les IE WPS de ses trames de balise ou messages UPnP qu'il requiert cette configuration.

Le Périphérique WAP peut fonctionner comme proxy pour un maximum de trois registres externes simultanément.

Fonctionnement exclusif des transactions WPS

Tout VAP sur le Périphérique WAP peut être activé pour WPS. Une seule transaction WPS à la fois (par exemple, l'inscription et l'association d'un client 802.11) peut être en cours sur le Périphérique WAP. L'administrateur du Périphérique WAP peut mettre fin à la transaction en cours à partir de l'utilitaire Web de configuration. La configuration du VAP ne doit toutefois pas être changée pendant la transaction ; le VAP ne doit pas non plus être modifié au cours du processus d'authentification. Cette restriction est recommandée mais pas appliquée sur le Périphérique WAP.

Compatibilité descendante avec WPS version 1.0

Bien que les périphériques WAP prennent en charge WPS version 2.0, le Périphérique WAP interagit avec les candidats à l'inscription et les registres qui sont certifiés par Wi-Fi Alliance comme étant conformes à la version 1.0 du protocole WPS.

Définition des paramètres WPS

Vous pouvez utiliser la page WPS Setup pour activer le Périphérique WAP en tant que périphérique compatible WPS mais aussi définir les paramètres de base. Lorsque vous êtes prêt à utiliser la fonction pour inscrire un nouveau périphérique ou ajouter le Périphérique WAP à un réseau compatible WPS, utilisez la page **Processus WPS**.

AVERTISSEMENT Pour des raisons de sécurité, il est recommandé (mais pas obligatoire) d'utiliser une connexion HTTPS à l'utilitaire Web de configuration lors de la configuration du WPS.

Pour configurer le Périphérique WAP en tant que périphérique compatible WPS :

ÉTAPE 1 Sélectionnez **Wireless** > **WPS Setup** dans le volet de navigation.

La page WPS Setup affiche l'état et les paramètres globaux, ainsi que l'état et les paramètres de l'instance WPS. Une instance est une implémentation de WPS qui est associée à un VAP sur le réseau. Le Périphérique WAP ne prend en charge qu'une seule instance.

ÉTAPE 2 Définissez les paramètres globaux :

- **Supported WPS Version** : version du protocole WPS qui est prise en charge par le Périphérique WAP.
- **WPS Device Name** : fournit un nom de périphérique par défaut. Vous pouvez attribuer un autre nom constitué de 1 à 32 caractères, en incluant les espaces et les caractères spéciaux.
- **WPS Global Operational Status** : indique si le protocole WPS est activé ou désactivé sur le Périphérique WAP. Le protocole Bonjour est activé par défaut.
- **WPS Device PIN** : code PIN WPS à huit chiffres généré par le système pour le Périphérique WAP. L'administrateur peut utiliser ce code PIN généré pour inscrire le Périphérique WAP sur un registre externe.

  Vous pouvez cliquer sur **Generate** pour générer un nouveau code PIN. La génération d'un nouveau code PIN est conseillée si l'intégrité du réseau a été compromise.

ÉTAPE 3 Définissez les paramètres de l'instance WPS :

- **WPS Instance ID** : identifiant de l'instance. Puisqu'il n'y a qu'une seule instance, la seule option est wps1.
- **WPS Mode** : active ou désactive l'instance.
- **WPS VAP** : VAP associé à cette instance WPS.
- **WPS Built-in Registrar** : active la fonction de registre intégré. Lorsque cette fonction est activée, les candidats à l'inscription (généralement les clients WLAN) peuvent s'inscrire sur le périphérique WAP. Lorsque cette fonction est désactivée, la fonctionnalité de registre du périphérique WAP est également désactivée et le candidat à l'inscription doit s'inscrire sur un autre registre du réseau. Dans ce cas, un autre périphérique du réseau fonctionne en tant que registre et le périphérique WAP fonctionne en tant que proxy pour le réacheminement des demandes d'enregistrement des clients et des réponses du registre.
- **WPS Configuration State** : spécifie si le VAP sera configuré à partir du registre externe dans le cadre du processus WPS. Il peut être défini sur l'une des valeurs suivantes :
  - **Unconfigured** : les paramètres du VAP sont définis via WPS. Une fois cette opération effectuée, l'état deviendra Configured.
  - **Configured** : les paramètres du VAP ne sont pas définis par le registre externe et conserveront la configuration existante.

ÉTAPE 4 Cliquez sur **Mettre à jour**. Les modifications sont enregistrées dans la configuration de démarrage.

L'état opérationnel de l'instance et la raison de celui-ci s'affichent. Pour obtenir des informations sur les conditions susceptibles d'entraîner la désactivation de l'instance, reportez-vous à la section Activation ou désactivation de WPS sur un VAP.

Instance Status

La zone Instance Status indique les informations suivantes sur l'instance WPS sélectionnée :

- **WPS Operational Status** : indique si l'instance WPS est opérationnelle.
- **AP Lockdown Status** : indique si le point d'accès est en mode de verrouillage. Dans ce mode, les registres externes ne peuvent pas effectuer

d'inscription sur le point d'accès. Si le mode de verrouillage est activé, ce champ spécifie l'heure de début du verrouillage et indique s'il est temporaire ou permanent. S'il est temporaire, il affiche la durée de la période de verrouillage. Si le mode de verrouillage est désactivé, l'état **Disabled** apparaît.

- **Failed Attempts with Invalid PIN** : nombre de fois qu'un registre externe a tenté et échoué une inscription sur le périphérique WAP.

Lorsque l'état de verrouillage est activé, les champs suivants apparaissent :

- **AP Lockdown Duration** : durée en minutes pendant laquelle le WAP est verrouillé. Lorsque le WAP est verrouillé de manière permanente, cette valeur est définie sur –1.
- **AP Lockdown Timestamp** : heure à laquelle le périphérique WAP a été verrouillé.

Vous pouvez cliquer sur **Refresh** pour mettre à jour la page avec les informations d'état actualisées.

Processus WPS

Vous pouvez utiliser la page WPS Process pour inscrire une station cliente sur le réseau par l'intermédiaire de WPA. Vous pouvez inscrire un client à l'aide de la méthode PIN (Personal Identification Number) ou PBC (Push-Button Control) si celle-ci est prise en charge sur la station cliente.

Inscription d'un client à l'aide de la méthode PIN

Pour inscrire une station cliente à l'aide de la méthode PIN :

ÉTAPE 1 Obtenez le code PIN en y accédant sur le périphérique client. Le code PIN peut être soit imprimé sur le matériel lui-même, soit présent dans l'interface logicielle du périphérique.

ÉTAPE 2 Sélectionnez **Wireless** > **WPS Process** dans le volet de navigation.

ÉTAPE 3 Saisissez le code PIN du client dans la zone de texte **PIN Enrollment**, puis cliquez sur **Start**.

ÉTAPE 4 Vous avez alors deux minutes pour saisir le code PIN du WAP dans l'interface logicielle du périphérique client. Le code PIN du WAP est configuré sur la page **Configuration de WPS**.

Lorsque vous saisissez le code PIN sur le périphérique client, WPS Operational Status devient Adding Enrollee. Une fois le processus d'inscription terminé, WPS Operational Status devient Ready et Transaction Status devient Success.

Lorsque le client est inscrit, le registre intégré du périphérique WAP ou le registre externe sur le réseau effectue la configuration du client avec le SSID, le mode de chiffrement et la clé partagée publique d'un BSS compatible WPS.

AVERTISSEMENT Cette séquence d'inscription peut également fonctionner à l'envers, à savoir que vous pouvez initier le processus sur la station cliente en saisissant le code PIN du périphérique WAP. Toutefois, cette méthode n'est **pas recommandée** pour des raisons de sécurité, car elle permet au client de configurer le SSID et les paramètres de sécurité sur le point d'accès. L'administrateur doit veiller à uniquement communiquer le code PIN aux périphériques de confiance.

Inscription d'un client à l'aide de la méthode PBC

Pour inscrire une station cliente à l'aide de la méthode PBC :

ÉTAPE 1 Cliquez sur **Start** en regard de **PBC Enrollment**.

ÉTAPE 2 Appuyez sur le bouton physique de la station cliente.

REMARQUE Vous pouvez également initier ce processus sur la station cliente, puis cliquer sur le bouton PBC Enrollment Start du périphérique WAP.

Lorsque vous appuyez sur le bouton de la station cliente, WPS Operational Status devient Adding Enrollee. Une fois le processus d'inscription terminé, WPS Operational Status devient Ready et Transaction Status devient Success.

Lorsque le client est inscrit, le registre intégré du périphérique WAP ou le registre externe sur le réseau effectue la configuration du client avec le SSID, le mode de chiffrement et la clé partagée publique d'un BSS compatible WPS.

Affichage des informations d'état de l'instance

La section Instance Status indique les informations suivantes sur l'instance WPS sélectionnée dans la liste **WPS Instance ID** :

- **WPS Status** : indique si l'instance WPS sélectionnée est activée ou désactivée.
- **WPS Configuration State** : spécifie si le VAP sera configuré à partir du registre externe dans le cadre du processus WPS.
- **Transaction Status** : état de la dernière transaction WPS. Les valeurs possibles sont None, Success, WPS Message Error et Timed Out.
- **WPS Operational Status** : état de la transaction WPS la plus récente ou actuelle. Les valeurs possibles sont Disabled, Ready, Configuring, Proxying et Adding Enrollee. Si aucune transaction WPS n'a été effectuée depuis l'activation de WPS, Ready s'affiche.
- **AP Lockdown Status** : indique si l'instance est actuellement en mode de verrouillage.
- **Failed Attempts with Invalid PIN** : nombre de fois qu'une tentative d'authentification d'un registre externe a échoué en raison d'un mot de passe non valide.

Affichage des informations de résumé de l'instance

Les informations suivantes s'affichent pour l'instance WPS :

- **WPS Radio**
- **WPS VAP**
- **SSID**
- **Security**

Si le champ WPS Configuration State de la page WPS Setup est défini sur Unconfigured, alors les valeurs SSID et Security sont configurées par le registre externe. Si le champ est défini sur Configured, alors ces valeurs sont configurées par l'administrateur.

REMARQUE Vous pouvez cliquer sur **Refresh** pour mettre à jour la page avec les informations d'état actualisées.

6

Sécurité du système

Ce chapitre explique comment configurer les paramètres de sécurité sur le périphérique Périphérique WAP.

Il contient les sections suivantes :

- **Serveur RADIUS**
- **Demandeur 802.1X**
- **Complexité des mots de passe**
- **Complexité WPA-PSK**

Serveur RADIUS

Plusieurs fonctionnalités nécessitent une communication avec un serveur d'authentification RADIUS. Par exemple, lorsque vous configurez des points d'accès virtuels (VAP) sur le Périphérique WAP, vous pouvez configurer des méthodes de sécurité qui contrôlent l'accès des clients sans fil (voir la page **Radio**). Les méthodes de sécurité WEP dynamique et WPA Entreprise utilisent un serveur RADIUS externe pour authentifier les clients. La fonctionnalité de filtrage des adresses MAC, dans laquelle l'accès des clients est limité à une liste, peut également être configurée afin d'utiliser un serveur RADIUS pour le contrôle des accès. La fonctionnalité de portail captif utilise également un serveur RADIUS pour l'authentification des clients.

Vous pouvez utiliser la page Radius Server pour configurer les serveurs RADIUS qui seront utilisés par ces fonctionnalités. Vous pouvez configurer jusqu'à quatre serveurs RADIUS IPv4 ou IPv6 disponibles globalement. Toutefois, vous devez indiquer si le client RADIUS fonctionne en mode IPv4 ou IPv6 par rapport aux serveurs globaux. Un des serveurs joue toujours le rôle de serveur principal, tandis que les autres font office de serveurs de sauvegarde.

REMARQUE En plus d'utiliser les serveurs RADIUS globaux, vous pouvez aussi configurer chaque point d'accès virtuel (VAP) de telle sorte qu'il utilise un ensemble spécifique de serveurs RADIUS. Reportez-vous à la page **Networks**.

Pour configurer des serveurs RADIUS globaux :

ÉTAPE 1 Sélectionnez **Security** > **RADIUS Server** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Server IP Address Type** : version IP utilisée par le serveur RADIUS.

  Vous pouvez basculer entre les types d'adresses pour configurer les paramètres d'adresse RADIUS globale IPv4 et IPv6, mais notez que le périphérique WAP ne contacte que le ou les serveurs RADIUS correspondant au type d'adresse sélectionné dans ce champ.

- **Server IP Address 1** ou **Server IPv6 Address 1** : adresses du serveur RADIUS global principal.

  Lorsque le premier client sans fil tente de s'authentifier à l'aide du périphérique WAP, le périphérique envoie une demande d'authentification au serveur principal. Si le serveur principal répond à la demande d'authentification, le périphérique WAP continue à utiliser ce serveur RADIUS en guise de serveur principal et les demandes d'authentification sont envoyées à l'adresse spécifiée.

- **Server IP Address (2** à **4)** ou **Server IPv6 Address (2** à **4)** : jusqu'à trois adresses de serveur RADIUS IPv4 ou IPv6 de sauvegarde.

  Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.

- **Key 1** : clé secrète partagée utilisée par le périphérique WAP pour s'authentifier au serveur RADIUS principal.

  Vous pouvez utiliser de 1 à 64 caractères alphanumériques standard et caractères spéciaux. La clé est sensible à la casse et doit correspondre à la clé configurée sur le serveur RADIUS. Le texte que vous entrez apparaît sous la forme d'astérisques.

- **Key (2** à **4)** : clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur spécifié dans le champ **Server IP (IPv6) Address 2** utilise **Key 2** ; le serveur spécifié dans le champ **Server IP (IPv6) Address -3** utilise **Key 3**, etc.

- **Enable RADIUS Accounting** : active le suivi et la mesure des ressources consommées par un utilisateur donné (heure système, volume de données transmises et reçues, etc.)

  Si vous activez la gestion des comptes RADIUS, cette fonctionnalité est activée à la fois pour le serveur RADIUS principal et pour l'ensemble des serveurs de sauvegarde.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Demandeur 802.1X

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. Il est possible de configurer un nom d'utilisateur et un mot de passe cryptés à l'aide de l'algorithme MD5 afin d'autoriser le point d'accès à effectuer une authentification à l'aide de la technologie 802.1X.

Sur les réseaux qui utilisent le contrôle d'accès réseau basé sur les ports IEEE 802.1X, un demandeur ne peut pas accéder au réseau tant que l'authentificateur 802.1X ne lui en a pas donné l'autorisation. Si votre réseau utilise la technologie 802.1X, vous devez configurer les informations d'authentification 802.1X sur le périphérique WAP, de telle sorte qu'il puisse les transmettre à l'authentificateur.

La page 802.1X Supplicant est divisée en trois zones : Supplicant Configuration, Certificate File Status et Certificate File Upload.

La zone Supplicant Configuration permet de configurer l'état opérationnel et les paramètres de base de 802.1X.

ÉTAPE 1 Sélectionnez **System Security** > **802.1X Supplicant** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Administrative Mode** : active la fonctionnalité de demandeur 802.1X.
- **EAP Method** : algorithme à utiliser pour le cryptage des noms d'utilisateur et des mots de passe utilisés lors de l'authentification.
  - **MD5** : fonction de hachage définie dans la norme RFC 3748 et offrant une sécurité de base.

- **PEAP** : protocole (PEAP, Protected Extensible Authentication Protocol) offrant un niveau de sécurité supérieur à celui de la technologie MD5, grâce à l'encapsulation de celle-ci à l'intérieur d'un tunnel TLS.
- **TLS** : sécurité de la couche transport (TLS, Transport Layer Security), telle que définie dans la norme RFC 5216, à savoir une norme ouverte offrant un haut niveau de sécurité.

- **Username** : le périphérique WAP utilise ce nom d'utilisateur lorsqu'il répond à des demandes émanant d'un authentificateur 802.1X. Le nom d'utilisateur peut comporter de 1 à 64 caractères. Les caractères imprimables ASCII sont autorisés, ce qui inclut les lettres majuscules et minuscules, les chiffres et tous les caractères spéciaux à l'exception des guillemets.
- **Password** : le périphérique WAP utilise ce mot de passe MD5 lorsqu'il répond à des demandes émanant d'un authentificateur 802.1X. La longueur du mot de passe peut être de 1 à 64 caractères. Les caractères imprimables ASCII sont autorisés, ce qui inclut les lettres majuscules et minuscules, les chiffres et tous les caractères spéciaux à l'exception des guillemets.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

La zone Certificate File Status indique s'il existe un certificat actuel :

- **Certificate File Present** : indique si le fichier de certificat SSL HTTP est présent. Ce champ contient la valeur Yes si ce fichier est présent. La valeur par défaut est No.
- **Certificate Expiration Date** : indique la date d'expiration du fichier de certificat SSL HTTP. La plage est une date valide.

La zone Certificate File Upload permet de télécharger un fichier de certificat vers le Périphérique WAP :

ÉTAPE 1 Sélectionnez **HTTP** ou **TFTP** en guise de **Méthode de transfert**).

ÉTAPE 2 Si vous avez sélectionné HTTP, cliquez sur **Parcourir** pour sélectionner le fichier.

REMARQUE Pour configurer les paramètres des serveurs HTTP et HTTPS, reportez-vous à **Service HTTP/HTTPS**.

Si vous avez sélectionné TFTP, complétez les champs **Filename** et **TFTP Server IPv4 Address**. Le nom de fichier ne peut pas contenir les caractères suivants : espaces, <, >, |, \, : , (,), &, ; , #, ? , *, ainsi que deux points successifs ou plus.

ÉTAPE 3 Cliquez sur **Upload**.

Une fenêtre de confirmation apparaît, suivie d'une barre de progression indiquant l'état du téléchargement.

Complexité des mots de passe

Vous pouvez configurer les exigences de complexité des mots de passe utilisés pour accéder à l'utilitaire de configuration du périphérique WAP. Des mots de passe complexes augmentent la sécurité.

Pour configurer les exigences de complexité des mots de passe :

ÉTAPE 1 Sélectionnez **Security** > **Password Complexity** dans le volet de navigation.

ÉTAPE 2 Pour le paramètre **Password Complexity**, sélectionnez **Enable**.

ÉTAPE 3 Configurez les paramètres suivants :

- **Password Minimum Character Class** : nombre minimal de classes de caractères devant être représentées dans la chaîne de mot de passe. Les quatre classes de caractères possibles sont les lettres majuscules, les lettres minuscules, les chiffres et les caractères spéciaux disponibles sur un clavier standard.
- **Password Different From Current** : sélectionnez cette option afin de permettre aux utilisateurs d'entrer un autre mot de passe lorsque leur mot de passe actuel arrive à expiration. Si vous ne sélectionnez pas cette option, les utilisateurs peuvent entrer à nouveau le même mot de passe une fois celui-ci arrivé à expiration.
- **Maximum Password Length** : la longueur maximale du mot de passe est comprise entre 64 et 80 caractères. La valeur par défaut est 64.
- **Minimum Password Length** : la longueur minimale du mot de passe est comprise entre 0 et 32 caractères. La valeur par défaut est 8.

- **Password Aging Support** : sélectionnez cette option pour que les mots de passe expirent après une période déterminée que vous configurez.
- **Password Aging Time** : nombre de jours avant qu'un nouveau mot de passe n'expire. Cette valeur est comprise entre 1 et 365. La valeur par défaut est de 180 jours.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Complexité WPA-PSK

Lorsque vous configurez des points d'accès virtuels (VAP) sur le périphérique WAP, vous pouvez sélectionner une méthode d'authentification sécurisée des clients. Si vous sélectionnez le protocole WPA personnel (également connu sous le nom de clé prépartagée WPA ou WPA-PSK) en guise de méthode de sécurité pour tous les points d'accès virtuels (VAP), vous pouvez également utiliser la page WPA-PSK Complexity pour configurer les exigences de complexité de la clé utilisée dans le processus d'authentification. Des clés plus complexes offrent une sécurité accrue.

Pour configurer la complexité WPA-PSK :

ÉTAPE 1 Sélectionnez **Security** > **WPA-PSK Complexity** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Enable** pour le paramètre **WPA-PSK Complexity** afin de permettre au périphérique WAP de contrôler les clés WPA-PSK en fonction des critères que vous configurez. Si vous désactivez cette case à cocher, aucun de ces paramètres ne sera utilisé. La complexité WPA-PSK est désactivée par défaut.

ÉTAPE 3 Configurez les paramètres suivants :

- **WPA-PSK Minimum Character Class** : nombre minimal de classes de caractères devant être représentées dans la chaîne de clé. Les quatre classes de caractères possibles sont les lettres majuscules, les lettres minuscules, les chiffres et les caractères spéciaux disponibles sur un clavier standard. La valeur par défaut est trois.

- **WPA-PSK Different From Current** : sélectionnez l'une des options suivantes :
  - **Enable** : les utilisateurs doivent configurer une autre clé lorsque leur clé actuelle arrive à expiration.
  - **Disable** : les utilisateurs peuvent continuer à utiliser leur ancienne clé ou leur clé précédente lorsque leur clé actuelle arrive à expiration.
- **Maximum WPA-PSK Length** : la longueur maximale de la clé est comprise entre 32 et 63 caractères. La valeur par défaut est 63.
- **Minimum WPA-PSK Length** : la longueur minimale de la clé est comprise entre 8 et 16 caractères. La valeur par défaut est 8. Activez cette case à cocher pour rendre le champ modifiable et activer cette condition.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

7

Qualité de service (QoS) de client

Ce chapitre offre un aperçu de la qualité de service (QoS) de client et explique les fonctionnalités QoS disponibles depuis le menu Client QoS. Il contient les sections suivantes :

- **Paramètres globaux relatifs à la QoS de client**
- **ACL**
- **Mappage de classe**
- **Mappage de stratégie**
- **Association de la QoS de client**
- **État de la QoS de client**

Paramètres globaux relatifs à la QoS de client

Utilisez la page Client QoS Global Settings pour activer ou désactiver la fonctionnalité de qualité de service sur le périphérique WAP.

Si vous désactivez le mode QoS client **Client QoS Mode**, toutes les ACL, les limitations de débit et les configurations DiffServ seront désactivées de manière globale.

Si vous activez ce mode, vous pouvez également activer ou désactiver le mode QoS de client sur des points d'accès virtuels spécifiques. Reportez-vous au paramètre **Client QoS Mode** à la page *Association de la QoS de client*.

ACL

Une ACL ou liste de contrôle d'accès est un ensemble de conditions d'autorisation et de refus, appelées règles, qui offrent de la sécurité en bloquant les utilisateurs non autorisés et en permettant aux utilisateurs autorisés d'accéder à des ressources spécifiques. Les ACL peuvent bloquer toutes les tentatives non fondées d'accès aux ressources réseau.

Le Périphérique WAP peut prendre en charge jusqu'à 50 ACL IPv4, IPv6 et MAC.

ACL IPv4 et IPv6

Les ACL IP classent le trafic selon les couches 3 et 4.

Chaque ACL est un ensemble de 10 règles au maximum, appliquées au trafic envoyé ou reçu par le périphérique WAP. Chaque règle spécifie si le contenu d'un champ donné doit être utilisé pour autoriser ou refuser l'accès au réseau. Les règles peuvent être basées sur divers critères et elles peuvent s'appliquer à un ou plusieurs champs au sein d'un paquet, comme l'adresse IP source ou de destination, le port source ou de destination, ou le protocole transporté dans le paquet.

REMARQUE Chaque règle créée se termine par une instruction de refus implicite. Afin d'éviter un refus complet, il est fortement recommandé d'ajouter une règle d'autorisation dans l'ACL en vue d'autoriser le trafic.

ACL MAC

Les ACL MAC sont des ACL de couche 2. Vous pouvez configurer les règles de manière à inspecter les champs d'une trame, comme l'adresse MAC source ou de destination, l'ID de VLAN ou la classe de service. Lorsqu'une trame entre dans le port du périphérique WAP ou le quitte (selon que l'ACL est appliquée dans la direction montante ou descendante), le périphérique WAP inspecte la trame et vérifie son contenu par rapport aux règles ACL. Si l'une des règles correspond à ce contenu, une action d'autorisation ou de refus est entreprise sur la trame.

Configuration des ACL

Configurez des ACL et des règles sur la page ACL Configuration, puis appliquez ces règles au point d'accès virtuel spécifié.

Les étapes suivantes donnent une description générale de la manière de configurer des ACL :

ÉTAPE 1 Sélectionnez **Client QoS** > **ACL** dans le volet de navigation.

ÉTAPE 2 Spécifiez le nom de l'ACL.

ÉTAPE 3 Sélectionnez le type d'ACL à ajouter.

ÉTAPE 4 Ajoutez l'ACL.

ÉTAPE 5 Ajoutez de nouvelles règles à l'ACL.

ÉTAPE 6 Configurez les critères de correspondance des règles.

ÉTAPE 7 Utilisez la page **Association de la QoS de client** pour appliquer l'ACL à un ou plusieurs points d'accès virtuels.

Les étapes suivantes donnent une description détaillée de la manière de configurer des ACL :

ÉTAPE 1 Sélectionnez **Client QoS** > **ACL** dans le volet de navigation.

ÉTAPE 2 Entrez les paramètres suivants pour créer une nouvelle ACL :

- **ACL Name** : nom de l'ACL. Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.
- **ACL Type** : type d'ACL à configurer :
  - IPv4
  - IPv6
  - MAC

  Les ACL IPv4 et IPv6 contrôlent l'accès aux ressources réseau sur la base des critères des couches 3 et 4. Les ACL MAC contrôlent l'accès aux ressources réseau sur la base des critères de la couche 2.

ÉTAPE 3 Cliquez sur **Add ACL**.

La page affiche des champs supplémentaires pour la configuration de l'ACL.

ÉTAPE 4 Configurez les paramètres de règle suivants :

- **ACL Name - ACL Type** : ACL à configurer avec la nouvelle règle. La liste contient toutes les ACL qui ont été ajoutées à la section ACL Configuration.
- **Rule** : action à entreprendre :
  - Sélectionnez **New Rule** pour configurer une nouvelle règle pour l'ACL sélectionnée.
  - Si des règles existent déjà (même si elles ont été créées en vue d'être utilisées avec d'autres ACL), vous pouvez sélectionner le numéro de la règle à ajouter à l'ACL sélectionnée ou à modifier.

  Lorsqu'une ACL possède plusieurs règles, celles-ci sont appliquées au paquet ou à la trame dans l'ordre selon lequel vous les avez ajoutées à l'ACL. La règle finale est une instruction implicite de refus de tout trafic.
- **Action** : indique si la règle ACL autorise ou refuse une action.

  Si vous sélectionnez Permit, la règle autorise tout le trafic qui satisfait aux critères de la règle en matière d'entrée ou de sortie du périphérique WAP (en fonction de la direction d'ACL sélectionnée). Le trafic qui ne satisfait pas aux critères est abandonné.

  Si vous sélectionnez Deny, la règle bloque tout le trafic qui satisfait aux critères de la règle en matière d'entrée ou de sortie du périphérique WAP (en fonction de la direction d'ACL sélectionnée). Le trafic qui ne satisfait pas aux critères est transféré, sauf si cette règle est la règle finale. Étant donné la présence d'une règle implicite de refus de tout trafic à la fin de chaque ACL, le trafic qui n'est pas explicitement autorisé est abandonné.
- **Match Every Packet** : si cette option est sélectionnée, la règle, qui possède une action d'autorisation ou de refus, met en correspondance la trame ou le paquet, quel que soit son contenu.

  Si vous sélectionnez ce champ, vous ne pouvez pas configurer de critères de correspondance supplémentaires. L'option Match Every Packet est sélectionnée par défaut en cas de nouvelle règle. Vous devez désactiver cette option pour configurer d'autres champs de correspondance.

Dans le cas des ACL IPv4, configurez les paramètres suivants :

- **Protocol** : sélectionnez le champ Protocol pour utiliser une condition de correspondance de protocole de couche 3 ou 4 sur la base de la valeur du champ IP Protocol dans les paquets IPv4 ou du champ Next Header dans les paquets IPv6.

Si vous sélectionnez le champ Protocol, sélectionnez l'une des options suivantes :

- **Select From List** : sélectionnez l'un des protocoles suivants : IP, ICMP, IGMP, TCP ou UDP.
- **Match to Value** : entrez un ID de protocole standard affecté par l'IANA, compris entre 0 et 255. Choisissez cette méthode pour identifier un protocole dont le nom ne figure pas dans le champ Select From List.

- **Source IP Address** : nécessite que l'adresse IP source d'un paquet corresponde à l'adresse répertoriée ici. Entrez une adresse IP dans le champ approprié pour appliquer ces critères.
- **Wild Card Mask** : masque générique de l'adresse IP source.

  Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque générique égal à 255.255.255.255 indique qu'aucun bit n'est important. Un masque générique égal à 0.0.0.0 indique en revanche que tous les bits sont importants. Ce champ est requis lors de la vérification de l'adresse IP source.

  Un masque générique est en fait l'inverse d'un masque de sous-réseau. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque générique égal à 0.0.0.0. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque générique égal à 0.0.0.255.
- **Source Port** : inclut un port source dans la condition de correspondance de la règle. Le port source est identifié dans l'en-tête de datagramme.

  Si vous sélectionnez le champ Source Port, choisissez le nom du port ou entrez son numéro.

  - **Select From List** : mot clé associé au port source à mettre en correspondance : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www.

    Chacun de ces mots clés est traduit en son numéro de port équivalent.
  - **Match to Port** : numéro de port IANA à mettre en correspondance avec le port source identifié dans l'en-tête de datagramme. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :

    0 à 1023 : ports réservés

    1024 à 49151 : ports inscrits

    49152 à 65535 : ports dynamiques et/ou privés

- **Destination IP Address** : nécessite que l'adresse IP de destination d'un paquet corresponde à l'adresse répertoriée ici. Entrez une adresse IP dans le champ approprié pour appliquer ces critères.
- **Wild Card Mask** : masque générique de l'adresse IP de destination.

  Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque générique égal à 255.255.255.255 indique qu'aucun bit n'est important. Un masque générique égal à 0.0.0.0 indique en revanche que tous les bits sont importants. Ce champ est requis lors de la sélection de l'adresse IP source.

  Un masque générique est en fait l'inverse d'un masque de sous-réseau. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque générique égal à 0.0.0.0. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque générique égal à 0.0.0.255.
- **Destination Port** : inclut un port de destination dans la condition de correspondance de la règle. Le port de destination est identifié dans l'en-tête de datagramme.

  Si vous sélectionnez le champ Destination Port, choisissez le nom du port ou entrez son numéro.

  - **Select From List** : sélectionnez le mot clé associé au port de destination à mettre en correspondance : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www.

    Chacun de ces mots clés est traduit en son numéro de port équivalent.
  - **Match to Port** : numéro de port IANA à mettre en correspondance avec le port de destination identifié dans l'en-tête de datagramme. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :

    0 à 1023 : ports réservés

    1024 à 49151 : ports inscrits

    49152 à 65535 : ports dynamiques et/ou privés
- **IP DSCP** : met en correspondance les paquets sur la base de leur valeur IP DSCP.

Si vous sélectionnez IP DSCP, choisissez l'une des options suivantes en tant que critères de correspondance :

- **Select From List** : valeurs Transfert DSCP (AF), Classe de service (CS) ou Acheminement attendu (EF).
- **Match to Value** : valeur DSCP personnalisée, comprise entre 0 et 63.

- **IP Precedence** : met en correspondance les paquets sur la base de leur valeur IP Precedence. Si vous sélectionnez cette option, entrez une valeur IP Precedence comprise entre 0 et 7.
- **IP TOS Bits** : spécifie une valeur relative à l'utilisation des bits du type de service du paquet dans l'en-tête IP en guise de critères de correspondance.

  Le champ IP TOS dans un paquet est défini comme l'ensemble des huit bits de l'octet du type de service dans l'en-tête IP. La valeur IP TOS Bits est un nombre hexadécimal à deux chiffres, compris entre 00 et ff.

  Les trois bits d'ordre haut représentent la valeur IP Precedence. Les six bits d'ordre haut représentent la valeur DSCP (Differentiated Services Code Point) IP.
- **IP TOS Mask** : entrez une valeur IP TOS Mask pour identifier les positions de bits dans la valeur IP TOS Bits, utilisées pour la comparaison avec le champ IP TOS dans un paquet.

  La valeur IP TOS Mask est un nombre hexadécimal à deux chiffres, compris entre 00 et FF, représentant un masque inversé (à savoir un masque générique). Les bits égaux à zéro dans le champ IP TOS Mask indiquent les positions de bits dans la valeur IP TOS Bits qui sont utilisées pour la comparaison avec le champ IP TOS d'un paquet. Par exemple, pour vérifier une valeur IP TOS possédant les bits 7 et 5 définis et le bit 1 vide, dans laquelle le bit 7 est le plus significatif, utilisez une valeur IP TOS Bits égale à 0 et une valeur IP TOS Mask égale à 00.

Dans le cas des ACL IPv6, configurez les paramètres suivants :

- **Protocol** : sélectionnez le champ Protocol pour utiliser une condition de correspondance de protocole de couche 3 ou 4 sur la base de la valeur du champ IP Protocol dans les paquets IPv4 ou du champ Next Header dans les paquets IPv6.

  Si vous sélectionnez ce champ, choisissez le protocole à mettre en correspondance par mot clé ou ID de protocole.

- **Source IPv6 Address** : sélectionnez ce champ pour exiger que l'adresse IPv6 source d'un paquet corresponde à l'adresse répertoriée ici. Entrez une adresse IPv6 dans le champ approprié pour appliquer ces critères.
- **Source IPv6 Prefix Length** : entrez la longueur de préfixe de l'adresse IPv6 source.
- **Source Port** : sélectionnez cette option pour inclure un port source dans la condition de correspondance de la règle. Le port source est identifié dans l'en-tête de datagramme. Si vous sélectionnez cette option, choisissez le nom du port ou entrez son numéro.
- **Destination IPv6 Address** : sélectionnez ce champ pour exiger que l'adresse IPv6 de destination d'un paquet corresponde à l'adresse répertoriée ici. Entrez une adresse IPv6 dans le champ approprié pour appliquer ces critères.
- **Destination IPv6 Prefix Length** : entrez la longueur de préfixe de l'adresse IPv6 de destination.
- **Destination Port** : sélectionnez cette option pour inclure un port de destination dans la condition de correspondance de la règle. Le port de destination est identifié dans l'en-tête de datagramme. Si vous sélectionnez cette option, choisissez le nom du port ou entrez son numéro.
- **IPv6 Flow Label** : nombre de 20 bits unique pour un paquet IPv6. Ce nombre est utilisé par les postes finaux pour indiquer la gestion de la QoS dans les routeurs (plage de 0 à 1048575).
- **IP DSCP** : met en correspondance les paquets sur la base de leur valeur IP DSCP. Si vous sélectionnez cette option, choisissez l'une des options suivantes en tant que critères de correspondance :
  - **Select From List** : valeurs Transfert DSCP (AF), Classe de service (CS) ou Acheminement attendu (EF).
  - **Match to Value** : valeur DSCP personnalisée, comprise entre 0 et 63.

Dans le cas d'une ACL MAC, configurez les paramètres suivants :

- **EtherType** : sélectionnez cette option pour comparer les critères de correspondance avec la valeur figurant dans l'en-tête d'une trame Ethernet.

  Sélectionnez le mot clé EtherType ou entrez une valeur EtherType pour spécifier les critères de correspondance.
  - **Select from List** : sélectionnez l'un des types de protocole suivants : appletalk, arp, ipv4, ipv6, ipx, netbios ou pppoe.

- **Match to Value** : entrez un identificateur de protocole personnalisé avec lequel les paquets sont mis en correspondance. La valeur est un nombre hexadécimal à 4 chiffres dans la plage 0600 à FFFF.

- **Class of Service** : sélectionnez ce champ et entrez une priorité d'utilisateur 802.1p à comparer à une trame Ethernet.

  La plage valide va de 0 à 7. Ce champ se trouve dans la première et seule balise VLAN 802.1Q.

- **Source MAC Address** : sélectionnez ce champ et entrez l'adresse MAC source à comparer à une trame Ethernet.

- **Source MAC Mask** : sélectionnez ce champ et entrez le masque d'adresse MAC source indiquant quels bits de l'adresse MAC source il faut comparer à une trame Ethernet.

  Pour chaque position de bit dans le masque MAC, une valeur 0 indique que le bit d'adresse correspondant est significatif et une valeur 1 indique que le bit d'adresse est ignoré. Par exemple, pour ne vérifier que les quatre premiers octets d'une adresse MAC, utilisez un masque MAC de 00:00:00:00:ff:ff. Un masque MAC de 00:00:00:00:00:00 vérifie tous les bits d'adresse et est utilisé pour mettre en correspondance une seule adresse MAC.

- **Destination MAC Address** : sélectionnez ce champ et entrez l'adresse MAC de destination à comparer à une trame Ethernet.

- **Destination MAC Mask** : entrez le masque d'adresse MAC de destination afin de spécifier quels bits de l'adresse MAC de destination il faut comparer à une trame Ethernet.

  Pour chaque position de bit dans le masque MAC, une valeur 0 indique que le bit d'adresse correspondant est significatif et une valeur 1 indique que le bit d'adresse est ignoré. Par exemple, pour ne vérifier que les quatre premiers octets d'une adresse MAC, utilisez un masque MAC de 00:00:00:00:ff:ff. Un masque MAC de 00:00:00:00:00:00 vérifie tous les bits d'adresse et est utilisé pour mettre en correspondance une seule adresse MAC.

- **VLAN ID** : sélectionnez ce champ et entrez l'ID de VLAN spécifique à comparer à une trame Ethernet.

  Ce champ se trouve dans la première et seule balise VLAN 802.1Q.

ÉTAPE 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Pour supprimer une ACL, assurez-vous qu'elle est sélectionnée dans la liste **ACL Name-ACL Type**, sélectionnez **Delete ACL** et cliquez sur **Enregistrer**.

Mappage de classe

La fonctionnalité QoS de client inclut la prise en charge de services différenciés (DiffServ) permettant la classification du trafic en flux et offrant un traitement QoS correspondant à des comportements par saut définis.

Les réseaux IP standard sont conçus pour offrir un service de livraison des données de type « au mieux ». Le service « au mieux » implique que le réseau livre les données dans des délais corrects, mais sans garantie totale de livraison. En cas d'encombrement du réseau, il se peut que des paquets soient retardés, envoyés de manière sporadique, voire abandonnés. En ce qui concerne les applications Internet typiques, comme le courrier électronique et le transfert de fichiers, une légère dégradation du service est acceptable et dans de nombreux cas indétectable. Toutefois, dans le cas des applications présentant des exigences strictes en matière de délais d'exécution, comme la voix ou le multimédia, toute dégradation du service a des effets indésirables.

Une configuration DiffServ débute par la définition de mappages de classe, ce qui permet de classifier le trafic en fonction du protocole IP et d'autres critères. Chaque mappage de classe peut ensuite être associé à un mappage de stratégie, qui définit le mode de traitement de la classe de trafic. Les classes contenant du trafic devant être transmis rapidement peuvent être affectées à des mappages de stratégie accordant la priorité sur les autres types de trafic.

Utilisez la page Class Map pour définir des classes de trafic. Utilisez la page *Mappage de stratégie* pour définir des stratégies et leur associer des mappages de classe.

Ajout d'un mappage de classe

Pour ajouter un mappage de classe :

ÉTAPE 1 Sélectionnez **Client QoS** > **Class Map** dans le volet de navigation.

ÉTAPE 2 Saisissez un **Nom de mappage de classe**. Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.

ÉTAPE 3 Sélectionnez une valeur dans la liste **Match Layer 3 Protocol** :

- **IPv4** : le mappage de classe s'applique uniquement au trafic IPv4 sur le périphérique WAP.
- **IPv6** : le mappage de classe s'applique uniquement au trafic IPv6 sur le périphérique WAP.

La page Class Map contient des champs supplémentaires, en fonction du protocole de couche 3 sélectionné :

Utilisez les champs de la zone Match Criteria Configuration pour faire correspondre les paquets à une classe. Activez la case à cocher relative à chaque champ à utiliser en guise de critère pour une classe et entrez des données dans le champ en question. Notez qu'une classe peut posséder plusieurs critères de correspondance.

Les champs des critères de correspondance qui sont disponibles dépendent du type de mappage de classe, à savoir IPv4 ou IPv6.

Définition d'un mappage de classe

Pour configurer un mappage de classe :

ÉTAPE 1 Sélectionnez le mappage de classe dans la liste **Class Map Name**.

ÉTAPE 2 Configurez les paramètres suivants (les paramètres qui apparaissent uniquement pour les mappages de classe IPv4 ou IPv6 sont indiqués) :

- **Match Every Packet** : la condition de correspondance est vraie pour l'ensemble des paramètres dans un paquet de couche 3.

  Si vous sélectionnez cette option, tous les paquets de couche 3 répondront à la condition.

- **Protocol** : utilisez une condition de correspondance de protocole de couche 3 ou 4 sur la base de la valeur du champ IP Protocol dans les paquets IPv4 ou du champ Next Header dans les paquets IPv6.

  Si vous sélectionnez ce champ, choisissez le protocole à mettre en correspondance par mot clé ou entrez un ID de protocole.

  - **Select From List** : mettez en correspondance le protocole sélectionné : IP, ICMP, IPv6, ICMPv6, IGMP, TCP ou UDP.

- **Match to Value** : mettez en correspondance un protocole dont le nom ne figure pas dans la liste. Entrez l'ID de protocole. L'ID de protocole est une valeur standard affectée par l'IANA. La valeur est un nombre compris entre 0 et 255.

- **Source IP Address** ou **Source IPv6 Address** : nécessite que l'adresse IP source d'un paquet corresponde à l'adresse répertoriée ici. Activez la case à cocher et entrez une adresse IP.
- **Source IP Mask** (IPv4 uniquement) : masque d'adresse IP source.

  Le masque de DiffServ est un masque de bits de type réseau au format décimal IP séparé par des points, indiquant quelle(s) partie(s) de l'adresse IP de destination il faut utiliser pour effectuer la correspondance avec le contenu des paquets.

  Un masque DiffServ égal à 255.255.255.255 indique que tous les bits sont importants, tandis qu'un masque égal à 0.0.0.0 indique qu'aucun bit n'est important. Le contraire est vrai avec un masque générique d'ACL. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque égal à 255.255.255.255. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque égal à 255.255.255.0.
- **Source IPv6 Prefix Length** (IPv6 uniquement) : longueur de préfixe de l'adresse IPv6 source.
- **Destination IP Address** ou **Destination IPv6 Address** : nécessite que l'adresse IP de destination d'un paquet corresponde à l'adresse répertoriée ici. Entrez une adresse IP dans le champ approprié pour appliquer ces critères.
- **Destination IP Mask** (IPv4 uniquement) : masque d'adresse IP de destination.

  Le masque de DiffServ est un masque de bits de type réseau au format décimal IP séparé par des points, indiquant quelle(s) partie(s) de l'adresse IP de destination il faut utiliser pour effectuer la correspondance avec le contenu des paquets.

  Un masque DiffServ égal à 255.255.255.255 indique que tous les bits sont importants, tandis qu'un masque égal à 0.0.0.0 indique qu'aucun bit n'est important. Le contraire est vrai avec un masque générique d'ACL. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque égal à 255.255.255.255. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque égal à 255.255.255.0.

- **Destination IPv6 Prefix Length** (IPv6 uniquement) : longueur de préfixe de l'adresse IPv6 de destination.
- **IPv6 Flow Label** (IPv6 uniquement) : nombre de 20 bits unique pour un paquet IPv6. Ce nombre est utilisé par les postes finaux pour indiquer la gestion de la QoS dans les routeurs (plage de 0 à 1048575).
- **IP DSCP** : voir la description sous les champs Service Type.
- **Source Port** : inclut un port source dans la condition de correspondance de la règle. Le port source est identifié dans l'en-tête de datagramme.

  Si vous sélectionnez ce champ, choisissez le nom du port ou entrez son numéro.

  - **Select From List** : met en correspondance un mot clé associé au port source : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www.

    Chacun de ces mots clés est traduit en son numéro de port équivalent.

  - **Match to Port** : met en correspondance le numéro de port source figurant dans l'en-tête de datagramme avec un numéro de port IANA que vous spécifiez. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :

    0 à 1023 : ports réservés

    1024 à 49151 : ports inscrits

    49152 à 65535 : ports dynamiques et/ou privés

- **Destination Port** : inclut un port de destination dans la condition de correspondance de la règle. Le port de destination est identifié dans l'en-tête de datagramme.

  Si vous sélectionnez ce champ, choisissez le nom du port ou entrez son numéro.

  - **Select From List** : met en correspondance le port de destination figurant dans l'en-tête de datagramme avec le mot clé sélectionné : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www.

    Chacun de ces mots clés est traduit en son numéro de port équivalent.

  - **Match to Port** : met en correspondance le port de destination figurant dans l'en-tête de datagramme avec un numéro de port IANA que vous spécifiez. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :

    0 à 1023 : ports réservés

1024 à 49151 : ports inscrits

49152 à 65535 : ports dynamiques et/ou privés

- **EtherType** : compare les critères de correspondance avec la valeur figurant dans l'en-tête d'une trame Ethernet.

  Sélectionnez le mot clé EtherType ou entrez une valeur EtherType pour spécifier les critères de correspondance.

  - **Select from List** : met en correspondance la valeur Ethertype figurant dans l'en-tête de datagramme avec les types de protocole sélectionnés : appletalk, arp, ipv4, ipv6, ipx, netbios ou pppoe.
  - **Match to Value** : met en correspondance la valeur Ethertype figurant dans l'en-tête de datagramme avec un identificateur de protocole personnalisé que vous spécifiez. La valeur est un nombre hexadécimal à 4 chiffres dans la plage 0600 à FFFF.

- **Class of Service** : valeur de priorité utilisateur 802.1p de classe de service à mettre en correspondance pour les paquets. La plage valide va de 0 à 7.
- **Source MAC Address** : adresse MAC source à comparer à une trame Ethernet.
- **Source MAC Mask** : masque d'adresse MAC source indiquant quels bits de l'adresse MAC de destination il faut comparer à une trame Ethernet.

  Pour chaque position de bit dans le masque MAC, une valeur 0 indique que le bit d'adresse correspondant est significatif et une valeur 1 indique que le bit d'adresse est ignoré. Par exemple, pour ne vérifier que les quatre premiers octets d'une adresse MAC, utilisez un masque MAC de 00:00:00:00:ff:ff. Un masque MAC de 00:00:00:00:00:00 vérifie tous les bits d'adresse et est utilisé pour mettre en correspondance une seule adresse MAC.

- **Destination MAC Address** : adresse MAC de destination à comparer à une trame Ethernet.
- **Destination MAC Mask** : masque d'adresse MAC de destination indiquant quels bits de l'adresse MAC de destination il faut comparer à une trame Ethernet.

  Pour chaque position de bit dans le masque MAC, une valeur 0 indique que le bit d'adresse correspondant est significatif et une valeur 1 indique que le bit d'adresse est ignoré. Par exemple, pour ne vérifier que les quatre premiers octets d'une adresse MAC, utilisez un masque MAC de 00:00:00:00:ff:ff. Un masque MAC de 00:00:00:00:00:00 vérifie tous les bits d'adresse et est utilisé pour mettre en correspondance une seule adresse MAC.

- **VLAN ID** : ID de VLAN à mettre en correspondance pour les paquets. L'ID de VLAN doit être compris entre 0 et 4095.

Les champs Service Type suivants apparaissent uniquement pour IPv4. Vous pouvez spécifier un type de service à utiliser dans les paquets concordants avec les critères de classe.

- **IP DSCP** : valeur DSCP (Differentiated Services Code Point) à utiliser en guise de critère de correspondance :
  - **Select from List** : liste des types DSCP.
  - **Match to Value** : valeur DSCP que vous spécifiez (valeur comprise entre 0 et 63).
- **IP Precedence** (IPv4 uniquement) : met en correspondance la valeur IP Precedence du paquet avec la valeur IP Precedence des critères de classe. La plage des valeurs IP Precedence va de 0 à 7.
- **IP TOS Bits** (IPv4 uniquement) : utilise les bits du type de service du paquet dans l'en-tête IP en guise de critères de correspondance.

  Cette valeur est comprise entre 00 et FF. Les trois bits d'ordre haut représentent la valeur IP Precedence. Les six bits d'ordre haut représentent la valeur DSCP (Differentiated Services Code Point) IP.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Pour supprimer un mappage de classe, sélectionnez-le dans la liste **Class Map Name** et cliquez sur **Supprimer**. Le mappage de classe ne peut pas être supprimé s'il est déjà lié à une stratégie.

Mappage de stratégie

Les paquets sont classifiés et traités sur la base des critères définis. Les critères de classification sont définis par l'intermédiaire d'une classe à la page *Mappage de classe*. Le traitement est défini par les attributs d'une stratégie à la page Policy Map. Les attributs de stratégie peuvent être définis sur la base d'une instance par classe et ils déterminent le mode de traitement du trafic correspondant aux critères de classe.

Le périphérique WAP peut prendre en charge un maximum de 50 mappages de stratégie. Un mappage de stratégie peut contenir jusqu'à 10 mappages de classe.

Pour ajouter et configurer un mappage de stratégie :

ÉTAPE 1 Sélectionnez **Client QoS** > **Policy Map** dans le volet de navigation.

ÉTAPE 2 Entrez un nom de mappage de stratégie (**Policy Map Name**). Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.

ÉTAPE 3 Cliquez sur **Add Policy Map**. La page s'actualise avec des champs supplémentaires pour la configuration du mappage de stratégie.

ÉTAPE 4 Dans la zone Policy Class Definition, assurez-vous que le nouveau mappage de stratégie apparaît dans la liste **Policy Map Name**.

ÉTAPE 5 Dans la liste **Class Map Name**, sélectionnez le mappage de classe à appliquer à cette stratégie.

ÉTAPE 6 Configurez les paramètres suivants :

- **Police Simple** : établit le style de réglementation du trafic de la classe. La forme simple du style de réglementation utilise un seul débit de données et une seule taille de rafale, d'où deux résultats possibles : conforme et non conforme. Si vous sélectionnez ce champ, configurez l'un des champs suivants :
  - **Committed Rate** : débit garanti, en Kbit/s, auquel le trafic doit se conformer. Cette valeur est comprise entre 1 et 1.000.000 Kbit/s.
  - **Committed Burst** : taille de rafale engagée, en octets, à laquelle le trafic doit se conformer. Cette valeur est comprise entre 1 et 204.800.000 octets.
- **Send** : spécifie que tous les paquets du flux de trafic associé doivent être transférés si les critères de mappage de classe sont satisfaits.
- **Drop** : spécifie que tous les paquets du flux de trafic associé doivent être abandonnés si les critères de mappage de classe sont satisfaits.
- **Mark Class of Service** : marque tous les paquets du flux de trafic associé avec la valeur de la classe de service spécifiée dans le champ de priorité de l'en-tête 802.1p. Si le paquet ne contient pas encore cet en-tête, celui-ci est inséré. La valeur CoS est un entier compris entre 0 et 7.
- **Mark IP DSCP** : marque tous les paquets du flux de trafic associé avec la valeur IP DSCP que vous sélectionnez dans la liste ou que vous spécifiez.

- **Select from List** : liste des types DSCP.
- **Match to Value** : valeur DSCP que vous spécifiez. Cette valeur doit être un entier compris entre 0 et 63.

- **Mark IP Precedence** : marque tous les paquets du flux de trafic associé avec la valeur IP Precedence spécifiée. La valeur IP Precedence est un entier compris entre 0 et 7.
- **Disassociate Class Map** : supprime la classe sélectionnée dans la liste Class Map Name de la stratégie sélectionnée dans la liste Policy Map Name.
- **Member Classes** : répertorie toutes les classes DiffServ actuellement définies en tant que membres de la stratégie sélectionnée. Ce champ est vide si aucune classe n'est associée à la stratégie.

ÉTAPE 7 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Pour supprimer un mappage de stratégie, sélectionnez-le dans la liste **Policy Map Name** et cliquez sur **Supprimer**.

Association de la QoS de client

La page Client QoS Association offre un contrôle supplémentaire de certains aspects de la qualité de service des clients sans fil qui se connectent au réseau, comme la quantité de bande passante qu'un client individuel est autorisé à envoyer et à recevoir. Vous pouvez configurer des listes de contrôle d'accès (ACL) et les affecter à un ou plusieurs points d'accès virtuels afin de contrôler des catégories générales de trafic, comme le trafic HTTP ou le trafic issu d'un sous-réseau spécifique.

En plus de contrôler les catégories générales de trafic, la QoS de client vous permet également de configurer le conditionnement par client de divers micro-flux par le biais de services différenciés (DiffServ, Differentiated Services). Les stratégies DiffServ sont un outil utile pour l'établissement d'une définition générale des micro-flux et de caractéristiques de traitement pouvant être appliquées à chaque client sans fil, entrant et sortant, lors de son authentification sur le réseau.

Pour configurer les paramètres d'association de la QoS de client :

ÉTAPE 1 Sélectionnez **Client QoS** > **Client QoS Association** dans le volet de navigation.

ÉTAPE 2 Dans la liste des points d'accès virtuels, sélectionnez le point d'accès virtuel sur lequel vous voulez configurer des paramètres QoS de client.

ÉTAPE 3 Sélectionnez **Enable** pour l'option **Client QoS Global** pour activer cette fonctionnalité.

ÉTAPE 4 Configurez les paramètres suivants pour le point d'accès virtuel sélectionné :

- **Client QoS Mode** : sélectionnez **Enable** pour activer la fonctionnalité QoS de client sur le point d'accès virtuel sélectionné.
- **Bandwidth Limit Down** : vitesse de transmission maximale autorisée depuis le périphérique WAP vers le client en bits par seconde (bit/s). La plage valide va de 0 à 300 Mbit/s.
- **Bandwidth Limit Up** : vitesse de transmission maximale autorisée depuis le client vers le périphérique WAP en bits par seconde (bit/s). La plage valide va de 0 à 300 Mbit/s.
- **ACL Type Down** : type d'ACL à appliquer au trafic dans la direction sortante (du périphérique WAP vers le client), qui peut être l'une des valeurs ci-dessous :
  - IPv4 : l'ACL examine les paquets IPv4 en ce qui concerne les correspondances aux règles ACL.
  - IPv6 : l'ACL examine les paquets IPv6 en ce qui concerne les correspondances aux règles ACL.
  - MAC : l'ACL examine les trames de couche 2 en ce qui concerne les correspondances aux règles ACL.
- **ACL Name Down** : nom de l'ACL appliquée au trafic dans la direction sortante.

  Après la commutation du paquet ou de la trame vers l'interface sortante, une correspondance avec les règles ACL est vérifiée. Le paquet ou la trame est transmis s'il est autorisé, ou abandonné s'il est refusé.
- **ACL Type Up** : type d'ACL appliqué au trafic dans la direction entrante (du client vers le périphérique WAP), qui peut être l'une des valeurs ci-dessous :
  - IPv4 : l'ACL examine les paquets IPv4 en ce qui concerne les correspondances aux règles ACL.

  - IPv6 : l'ACL examine les paquets IPv6 en ce qui concerne les correspondances aux règles ACL.
  - MAC : l'ACL examine les trames de couche 2 en ce qui concerne les correspondances aux règles ACL.

- **ACL Name Up** : nom de l'ACL appliquée au trafic entrant dans le périphérique WAP (direction entrante).

  Lors de la réception d'un paquet ou d'une trame par le périphérique WAP, une correspondance avec les règles ACL est vérifiée. Le paquet ou la trame est traité s'il est autorisé, ou abandonné s'il est refusé.

- **DiffServ Policy Down** : nom de la stratégie DiffServ appliquée au trafic issu du périphérique WAP dans la direction sortante (du périphérique WAP vers le client).

- **DiffServ Policy Up** : nom de la stratégie DiffServ appliquée au trafic envoyé vers le périphérique WAP dans la direction entrante (du client vers le périphérique WAP).

ÉTAPE 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

État de la QoS de client

La page Client QoS Status affiche les paramètres QoS de client appliqués à chaque client actuellement associé au périphérique WAP.

Pour afficher la page Client QoS Status, sélectionnez **Client QoS** > **Client QoS Status** dans le volet de navigation.

Utilisez les champs suivants pour configurer l'état de la QoS de client :

- **Station** : le menu Station contient l'adresse MAC de chaque client actuellement associé au périphérique WAP. Pour afficher les paramètres QoS appliqués à un client, sélectionnez son adresse MAC dans la liste.
- **Global QoS Mode** : indique si la QoS est activée globalement sur le périphérique WAP. Cet état est configuré à la page *Association de la QoS de client*.
- **Client QoS Mode** : indique si la QoS est activée sur le point d'accès virtuel associé. Cet état est configuré à la page *Association de la QoS de client*.

- **Bandwidth Limit Down** : vitesse de transmission maximale autorisée depuis le périphérique WAP vers le client en bits par seconde (bit/s). La plage valide va de 0 à 4294967295 bit/s.
- **Bandwidth Limit Up** : vitesse de transmission maximale autorisée depuis le client vers le périphérique WAP en bits par seconde (bit/s). La plage valide va de 0 à 4294967295 bit/s.
- **ACL Type Up** : type d'ACL appliqué au trafic dans la direction entrante (du client vers le périphérique WAP), qui peut être l'une des valeurs ci-dessous :
  - IPv4 : l'ACL examine les paquets IPv4 en ce qui concerne les correspondances aux règles ACL.
  - IPv6 : l'ACL examine les paquets IPv6 en ce qui concerne les correspondances aux règles ACL.
  - MAC : l'ACL examine les trames de couche 2 en ce qui concerne les correspondances aux règles ACL.
- **ACL Name Up** : nom de l'ACL appliquée au trafic entrant dans le périphérique WAP (direction entrante). Lors de la réception d'un paquet ou d'une trame par le périphérique WAP, une correspondance avec les règles ACL est vérifiée. Le paquet ou la trame est traité s'il est autorisé, ou abandonné s'il est refusé.
- **ACL Type Down** : type d'ACL à appliquer au trafic dans la direction sortante (du périphérique WAP vers le client), qui peut être l'une des valeurs ci-dessous :
  - IPv4 : l'ACL examine les paquets IPv4 en ce qui concerne les correspondances aux règles ACL.
  - IPv6 : l'ACL examine les paquets IPv6 en ce qui concerne les correspondances aux règles ACL.
  - MAC : l'ACL examine les trames de couche 2 en ce qui concerne les correspondances aux règles ACL.
- **ACL Name Down** : nom de l'ACL appliquée au trafic dans la direction sortante. Après la commutation du paquet ou de la trame vers l'interface sortante, une correspondance avec les règles ACL est vérifiée. Le paquet ou la trame est transmis s'il est autorisé, ou abandonné s'il est refusé.
- **DiffServ Policy Up** : nom de la stratégie DiffServ appliquée au trafic envoyé vers le périphérique WAP dans la direction entrante (du client vers le périphérique WAP).

- **DiffServ Policy Down** : nom de la stratégie DiffServ appliquée au trafic issu du périphérique WAP dans la direction sortante (du périphérique WAP vers le client).

8

Protocole SNMP (Simple Network Management Protocol, Protocole de gestion de réseau simple)

Ce chapitre explique comment configurer le protocole SNMP (Simple Network Management Protocol, Protocole de gestion de réseau simple) en vue d'effectuer des tâches de configuration et de collecte de statistiques.

Il contient les sections suivantes :

- **Présentation de SNMP**
- **Paramètres généraux de SNMP**
- **Vues**
- **Groupes**
- **Utilisateurs**
- **Cibles**

Présentation de SNMP

Le protocole SNMP définit une norme pour l'enregistrement, le stockage et le partage d'informations relatives à des périphériques réseau. Il permet également de faciliter la gestion, le dépannage et la maintenance des réseaux.

Le périphérique WAP prend en charge les versions 1, 2 et 3 du protocole SNMP. Sauf mention contraire, tous les paramètres de configuration s'appliquent uniquement aux versions SNMPv1 et SNMPv2c. Les composants clés de tout réseau géré par le protocole SNMP sont les périphériques gérés, les agents SNMP ainsi qu'un système de gestion. Les agents stockent les données relatives à leurs périphériques dans des bases d'informations de gestion MIB (Management

Information Bases) et ils renvoient ces données au gestionnaire SNMP lorsque celui-ci le leur demande. Les périphériques gérés peuvent être des nœuds réseau tels que des périphériques WAP, des routeurs, des commutateurs, des ponts, des concentrateurs, des serveurs ou des imprimantes.

Le périphérique WAP peut fonctionner en tant que périphérique SNMP géré pour une intégration aisée dans des systèmes de gestion de réseau.

Paramètres généraux de SNMP

Utilisez la page General pour activer SNMP et configurer les paramètres de base de ce protocole.

Pour configurer les paramètres SNMP généraux :

ÉTAPE 1 Sélectionnez **SNMP** > **General** dans le volet de navigation.

ÉTAPE 2 Sélectionnez **Enabled** pour le paramètre **SNMP**. SNMP est désactivé par défaut.

ÉTAPE 3 Spécifiez un **Port UDP** pour le trafic SNMP.

Par défaut, un agent SNMP n'écoute que les demandes qui émanent du port 161. Toutefois, vous pouvez configurer le protocole de telle sorte que l'agent écoute les demandes issues d'un autre port. La plage valide va de 1025 à 65535.

ÉTAPE 4 Configurez les paramètres SNMPv2 :

- **Read-only Community** : nom de communauté en lecture seule pour l'accès SNMPv2. La plage valide va de 1 à 256 caractères alphanumériques et caractères spéciaux.

  Le nom de communauté agit en tant que fonctionnalité d'authentification simple visant à limiter le nombre d'ordinateurs sur le réseau pouvant demander des données à l'agent SNMP. Ce nom fonctionne comme un mot de passe et la demande est supposée être authentique si son émetteur connaît le mot de passe.

- **Read-write Community** : nom de communauté en lecture-écriture, utilisé pour les demandes de configuration SNMP. La plage valide va de 1 à 256 caractères alphanumériques et caractères spéciaux.

  La définition d'un nom de communauté est similaire à celle d'un mot de passe. Seules les demandes émanant des ordinateurs qui s'identifient avec ce nom de communauté sont acceptés.

- **Management Station** : détermine quelles stations peuvent accéder au périphérique WAP par le biais du protocole SNMP. Sélectionnez l'une des options suivantes :
  - **All** : l'ensemble des stations pouvant accéder au périphérique WAP par le biais du protocole SNMP n'est pas limité.
  - **User Defined** : l'ensemble des demandes SNMP autorisées est limité aux demandes spécifiées.
- **NMS, IPv4 Address/Name** : adresse IP IPv4, nom d'hôte DNS ou sous-réseau du système de gestion de réseau (NMS, Network Management System), ou ensemble d'ordinateurs pouvant exécuter des demandes d'obtention et de configuration vers les périphériques gérés.

  Un nom d'hôte DNS peut se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter jusqu'à 253 caractères.

  Comme dans le cas des noms de communauté, ce paramètre assure un certain niveau de sécurité sur les paramètres SNMP. L'agent SNMP accepte uniquement les demandes émanant de l'adresse IP, du nom d'hôte ou du sous-réseau spécifiés ici.

  Pour spécifier un sous-réseau, entrez une ou plusieurs plages d'adresses de sous-réseau sous la forme *adresse/longueur_masque* où *adresse* est une adresse IP et *longueur_masque* est le nombre de bits du masque. Les deux formats *adresse/masque* et *adresse/longueur_masque* sont pris en charge. Par exemple, si vous entrez la plage 192.168.1.0/24, cela signifie que l'adresse du sous-réseau est 192.168.1.0 et que le masque du sous-réseau est 255.255.255.0.

  La plage d'adresses est utilisée pour spécifier le sous-réseau du système de gestion de réseau (NMS) désigné. Seuls les ordinateurs dont les adresses IP sont incluses dans cette plage sont autorisés à exécuter des demandes d'obtention et de configuration sur le périphérique géré. Dans l'exemple ci-dessus, les ordinateurs dont les adresses sont comprises entre 192.168.1.1 et 192.168.1.254 peuvent exécuter des commandes SNMP sur le périphérique. (L'adresse identifiée par le suffixe .0 dans une plage de sous-réseau est toujours réservée à l'adresse de sous-réseau, tandis que l'adresse identifiée par .255 dans la plage est toujours réservée à l'adresse de diffusion.)

Autre exemple : si vous entrez la plage 10.10.1.128/25, les ordinateurs dont les adresses IP sont comprises entre 10.10.1.129 et 10.10.1.254 peuvent exécuter des demandes SNMP sur les périphériques gérés. Dans cet exemple, 10.10.1.128 est l'adresse réseau et 10.10.1.255 est l'adresse de diffusion. Un total de 126 adresses seront dans ce cas désignées.

- **NMS IPv6 Address/Name** : adresse IP IPv6, nom d'hôte DNS ou sous-réseau des ordinateurs pouvant exécuter des demandes d'obtention et de configuration vers les périphériques gérés. La forme de l'adresse IPv6 doit être similaire à celle-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

  Un nom d'hôte peut se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter jusqu'à 253 caractères.

ÉTAPE 5 Configurez les paramètres de déroutement SNMPv2 suivants :

- **Trap Community** : chaîne de communauté globale associée aux déroutements SNMP. Les déroutements envoyés à partir du périphérique fournissent cette chaîne en tant que nom de communauté. La plage valide va de 1 à 60 caractères alphanumériques et caractères spéciaux.
- **Trap Destination Table** : liste de trois adresses IP ou noms d'hôtes au maximum pouvant recevoir des déroutements SNMP. Activez la case à cocher et choisissez un **Type d'adresse IP hôte** (IPv4 ou IPv6) avant d'ajouter le **Nom d'hôte/Adresse IP**).

  Un exemple de nom d'hôte DNS est déroutementssnmp.foo.com. Les déroutements SNMP étant envoyés de manière aléatoire à partir de l'agent SNMP, il est logique de spécifier à quel emplacement exact les déroutements doivent être envoyés. Le nombre maximal de noms d'hôte DNS est égal à trois. Vérifiez que vous avez activé la case à cocher **Activé** et sélectionnez le **Type d'adresse IP hôte** approprié.

  Consultez également la remarque relative aux noms d'hôte dans l'étape précédente.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Vues

Une vue MIB SNMP est une famille de sous-arborescences de vues dans la hiérarchie MIB. Une sous-arborescence de vues est identifiée par l'association d'une valeur de sous-arborescence d'ID d'objet (OID) et d'une valeur de masque de chaîne de bits. Chaque vue MIB est définie par deux ensembles de sous-arborescences de vues, inclus dans la vue MIB ou exclus de celle-ci. Vous pouvez créer des vues MIB dans le but de contrôler la plage d'OID à laquelle les utilisateurs SNMPv3 peuvent accéder.

Le Périphérique WAP prend en charge un maximum de 16 vues.

Les remarques suivantes résument quelques consignes importantes relatives à la configuration des vues SNMPv3. Veuillez lire l'ensemble de ces remarques avant de continuer.

REMARQUE Une vue MIB appelée « all » est créée par défaut dans le système. Cette vue contient l'ensemble des objets de gestion pris en charge par le système.

REMARQUE Par défaut, les vues SNMPv3 « view-all » et « view-none » sont créées sur le périphérique WAP. Ces vues ne peuvent pas être supprimées ou modifiées.

Pour ajouter et configurer une vue SNMP :

ÉTAPE 1 Sélectionnez **SNMP** > **Views** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Ajouter** pour créer une nouvelle ligne dans le tableau des vues SNMPv3.

ÉTAPE 3 Activez la case à cocher dans la nouvelle ligne et cliquez sur **Modifier**.

- **View Name** : entrez le nom de la vue MIB. Les noms de vue peuvent comporter jusqu'à 32 caractères alphanumériques.
- **Type** : choisissez d'inclure la sous-arborescence de vues ou la famille de sous-arborescences dans la vue MIB ou de l'en exclure.

- **OID** : entrez une chaîne d'OID pour la sous-arborescence à inclure dans la vue ou à exclure de celle-ci.

  Par exemple, la sous-arborescence système est spécifiée par la chaîne d'OID .1.3.6.1.2.1.1.

- **Mask** : entrez un masque d'OID. La longueur du masque est de 47 caractères. Le format du masque d'OID est xx.xx.xx (.)... ou xx:xx:xx.... (:) et sa longueur est de 16 octets. Chaque octet se compose de deux caractères hexadécimaux séparés par un point (.) ou par un caractère deux-points (:). Seuls les caractères hexadécimaux sont autorisés dans ce champ.

  Par exemple, le masque d'OID FA.80 est 11111010.10000000.

  Un masque de famille est utilisé pour définir une famille de sous-arborescences de vues. Le masque de famille indique quels sous-identificateurs de la chaîne d'OID de la famille associée sont significatifs pour la définition de la famille. Une famille de sous-arborescences de vues permet un accès de contrôle efficace à une ligne du tableau.

ÉTAPE 4 Cliquez sur **Enregistrer**. La vue est ajoutée à la liste des vues SNMPv3 et vos modifications sont enregistrées dans la configuration initiale.

REMARQUE Pour supprimer une vue, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

Groupes

Les groupes SNMPv3 permettent de répartir les utilisateurs en groupes de privilèges d'autorisation et d'accès différents. Chaque groupe est ainsi associé à l'un des trois niveaux de sécurité suivants :

- noAuthNoPriv
- authNoPriv
- authPriv

L'accès aux bases d'informations de gestion (MIB) pour chaque groupe est contrôlé en associant une vue MIB à un groupe pour l'accès en lecture ou en écriture, et ce, de manière séparée.

Par défaut, le Périphérique WAP possède deux groupes :

- **RO** : groupe en lecture seule utilisant l'authentification et le cryptage des données. Les utilisateurs figurant dans ce groupe utilisent une clé ou un mot de passe MD5 pour l'authentification et une clé ou un mot de passe DES pour le cryptage. Les clés ou mots de passe MD5 et DES doivent être définis. Par défaut, les utilisateurs de ce groupe ont un accès en lecture à la vue MIB par défaut « all ».
- **RW** : groupe en lecture-écriture utilisant l'authentification et le cryptage des données. Les utilisateurs figurant dans ce groupe utilisent une clé ou un mot de passe MD5 pour l'authentification et une clé ou un mot de passe DES pour le cryptage. Les clés ou mots de passe MD5 et DES doivent être définis. Par défaut, les utilisateurs de ce groupe ont un accès en lecture et en écriture à la vue MIB par défaut « all ».

REMARQUE Les groupes par défaut RO et RW ne peuvent pas être supprimés.

REMARQUE Le Périphérique WAP prend en charge un maximum de huit groupes.

Pour ajouter et configurer un groupe SNMP :

ÉTAPE 1 Sélectionnez **SNMP** > **Groups** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Ajouter** pour créer une nouvelle ligne dans le tableau des groupes SNMPv3.

ÉTAPE 3 Activez la case à cocher du nouveau groupe et cliquez sur **Modifier**.

ÉTAPE 4 Configurez les paramètres suivants :

- **Group Name** : nom du groupe. Les noms de groupe par défaut sont RO et RW.

  Les noms de groupe peuvent comporter jusqu'à 32 caractères alphanumériques.

- **Security Level** : définit le niveau de sécurité du groupe, qui peut être l'une des valeurs ci-dessous :
  - **noAuthentication-noPrivacy** : pas d'authentification et pas de cryptage des données (aucune sécurité).
  - **Authentication-noPrivacy** : présence d'authentification, mais pas de cryptage des données. Avec ce niveau de sécurité, les utilisateurs envoient des messages SNMP utilisant une clé ou un mot de passe MD5 pour l'authentification, mais n'utilisant pas de clé ou de mot de passe DES pour le cryptage.

- **Authentication-Privacy** : présence d'authentification et de cryptage des données. Avec ce niveau de sécurité, les utilisateurs envoient une clé ou un mot de passe MD5 pour l'authentification et une clé ou un mot de passe DES pour le cryptage.

  En ce qui concerne les groupes qui nécessitent l'authentification, le cryptage ou les deux, vous devez définir les clés ou les mots de passe MD5 et DES à la page SNMP Users.

- **Write Views** : accès en écriture aux MIB pour le groupe, qui peut être l'une des valeurs ci-dessous :
  - **write-all** : le groupe peut créer, modifier et supprimer des MIB.
  - **write-none** : le groupe ne peut pas créer, ni modifier, ni supprimer des MIB.
- **Read Views** : accès en lecture aux MIB pour le groupe :
  - **view-all** : le groupe est autorisé à afficher et à lire l'ensemble des MIB.
  - **view-none** : le groupe ne peut ni afficher ni lire des MIB.

ÉTAPE 5 Cliquez sur **Enregistrer**. Le groupe est ajouté à la liste des groupes SNMPv3 et vos modifications sont enregistrées dans la configuration initiale.

REMARQUE Pour supprimer un groupe, sélectionnez-le dans la liste et cliquez sur **Supprimer**.

Utilisateurs

Utilisez la page SNMP Users pour définir des utilisateurs, associer un niveau de sécurité à chaque utilisateur et configurer des clés de sécurité pour chacun d'entre eux.

Chaque utilisateur est mappé sur un groupe SNMPv3, à partir des groupes prédéfinis ou des groupes définis par l'utilisateur, et, éventuellement, est configuré pour l'authentification et le cryptage. Pour l'authentification, seul le type MD5 est pris en charge. Pour le cryptage, seul le type DES est pris en charge. Il n'y a pas d'utilisateur SNMPv3 par défaut sur le Périphérique WAP et vous pouvez ajouter jusqu'à huit utilisateurs.

Pour ajouter des utilisateurs SNMP :

ÉTAPE 1 Sélectionnez **SNMP** > **Users** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Ajouter** pour créer une nouvelle ligne dans le tableau des utilisateurs SNMPv3.

ÉTAPE 3 Activez la case à cocher dans la nouvelle ligne et cliquez sur **Modifier**.

ÉTAPE 4 Configurez les paramètres suivants :

- **User Name** : nom identifiant l'utilisateur SNMPv3. Les noms d'utilisateur peuvent comporter jusqu'à 32 caractères alphanumériques.
- **Group** : groupe sur lequel l'utilisateur est mappé. Les groupes par défaut sont RWAuth, RWPriv et RO. Vous pouvez définir des groupes supplémentaires à la page SNMP Groups.
- **Authentication Type** : type d'authentification à utiliser dans le cas des demandes SNMPv3 émanant de l'utilisateur, pouvant être l'une des options suivantes :
  - **MD5** : requérir l'authentification MD5 dans le cas des demandes SNMP émanant de l'utilisateur.
  - **None** : les demandes SNMPv3 émanant de cet utilisateur ne requièrent pas d'authentification.
- **Authentication Pass Phrase** : (si vous spécifiez MD5 en tant que type d'authentification) phrase secrète permettant à l'agent SNMP d'authentifier les demandes envoyées par l'utilisateur. La longueur de la phrase secrète doit être comprise entre 8 et 32 caractères.
- **Encryption Type** : type de confidentialité à utiliser dans le cas des demandes SNMP émanant de l'utilisateur, pouvant être l'une des options suivantes :
  - **DES** : utiliser le cryptage DES dans le cas des demandes SNMPv3 émanant de l'utilisateur.
  - **None** : les demandes SNMPv3 émanant de cet utilisateur ne requièrent pas de confidentialité.
- **Encryption Pass Phrase** : (si vous spécifiez DES en tant que type de confidentialité) phrase secrète utilisée pour le cryptage des demandes SNMP. La longueur de la phrase secrète doit être comprise entre 8 et 32 caractères.

ÉTAPE 5 Cliquez sur **Enregistrer**. L'utilisateur est ajouté à la liste des utilisateurs SNMPv3 et vos modifications sont enregistrées dans la configuration initiale.

REMARQUE Pour supprimer un utilisateur, sélectionnez-le dans la liste et cliquez sur **Supprimer**.

Cibles

Les cibles SNMPv3 envoient des notifications SNMP à l'aide de messages d'information au gestionnaire SNMP. Dans le cas des cibles SNMPv3, seuls des messages d'information sont envoyés et pas des déroutements. Dans le cas des versions 1 et 2 du protocole SNMP, des déroutements sont envoyés. Chaque cible est définie avec une adresse IP cible, un port UDP et un nom d'utilisateur SNMPv3.

REMARQUE La configuration des utilisateurs SNMPv3 (voir la page **Utilisateurs**) doit être terminée avant celle des cibles SNMPv3.

REMARQUE Le Périphérique WAP prend en charge un maximum de huit cibles.

Pour ajouter des cibles SNMP :

ÉTAPE 1 Sélectionnez **SNMP** > **Targets** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Ajouter**. Une nouvelle ligne est créée dans le tableau.

ÉTAPE 3 Activez la case à cocher dans la nouvelle ligne et cliquez sur **Modifier**.

ÉTAPE 4 Configurez les paramètres suivants :

- **IP Address** : entrez l'adresse IPv4 du gestionnaire SNMP distant qui doit recevoir la cible.
- **UDP Port** : entrez le port UDP à utiliser pour l'envoi des cibles SNMPv3.
- **Users** : entrez le nom de l'utilisateur SNMP à associer à la cible. Pour configurer les utilisateurs SNMP, reportez-vous à la page **Utilisateurs**.

ÉTAPE 5 Cliquez sur **Enregistrer**. L'utilisateur est ajouté à la liste des cibles SNMPv3 et vos modifications sont enregistrées dans la configuration initiale.

REMARQUE Pour supprimer une cible SMMP, sélectionnez l'utilisateur dans la liste et cliquez sur **Supprimer**.

9

Portail captif

Ce chapitre décrit la fonctionnalité de portail captif (CP, Captive Portal), qui permet de bloquer l'accès au réseau pour les clients sans fil tant que la vérification de l'utilisateur n'a pas été établie. Vous pouvez configurer la vérification de portail captif de manière à autoriser l'accès à la fois pour les utilisateurs invités et les utilisateurs authentifiés.

REMARQUE La fonctionnalité de portail captif est disponible uniquement sur le périphérique Cisco WAP321.

Les utilisateurs authentifiés doivent être validés à l'aide d'une base de données des groupes ou des utilisateurs de portail captif autorisés avant de se voir autoriser l'accès. Cette base de données peut être stockée localement sur le périphérique WAP ou sur un serveur RADIUS.

Le portail captif se compose de deux instances de portail captif. Il est possible de configurer chaque instance de manière indépendante, avec des méthodes de vérification différentes pour chaque point d'accès virtuel ou SSID. Les périphériques Cisco WAP321 fonctionnent simultanément avec certains points d'accès virtuels configurés pour l'authentification de portail captif et d'autres points d'accès virtuels configurés pour les méthodes normales d'authentification sans fil, comme WPA ou WPA Entreprise.

Ce chapitre inclut les rubriques suivantes :

- **Configuration globale de portail captif**
- **Configuration d'instance**
- **Association d'instance**
- **Personnalisation de portail Web**
- **Groupes locaux**
- **Utilisateurs locaux**
- **Clients authentifiés**
- **Clients dont l'authentification a échoué**

Configuration globale de portail captif

Utilisez la page Global CP Configuration pour contrôler l'état administratif de la fonctionnalité de portail captif et configurer les paramètres globaux qui affectent toutes les instances de portail captif configurées sur le périphérique WAP.

Pour configurer les paramètres globaux de portail captif :

ÉTAPE 1 Sélectionnez **Captive Portal** > **Global Configuration** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Captive Portal Mode** : active le fonctionnement de portail captif sur le périphérique WAP.
- **Authentication Timeout** : pour pouvoir accéder au réseau par l'intermédiaire d'un portail, le client doit tout d'abord entrer des informations d'authentification sur une page Web d'authentification. Ce champ spécifie le temps en secondes pendant lequel le périphérique WAP maintient une session d'authentification ouverte avec le client sans fil associé. Si le client n'entre pas ses identifiants d'authentification durant le temps alloué, il se peut qu'il doive actualiser la page Web d'authentification. Le délai d'authentification par défaut est de 300 secondes. La plage valide va de 60 à 600 secondes.
- **Additional HTTP Port** : le trafic HTTP utilise le port de gestion HTTP, qui est le port 80 par défaut. Vous pouvez configurer un port supplémentaire pour le trafic HTTP. Entrez un numéro de port compris entre 1025 et 65535, ou 80. Les ports HTTP et HTTPs ne peuvent pas être identiques.
- **Additional HTTPS Port** : le trafic HTTP sur SSL (HTTPS) utilise le port de gestion HTTPS, qui est le port 443 par défaut. Vous pouvez configurer un port supplémentaire pour le trafic HTTPS. Entrez un numéro de port compris entre 1025 et 65535, ou 443. Les ports HTTP et HTTPs ne peuvent pas être identiques.

La zone Captive Portal Configuration Counters affiche des informations de portail captif en lecture seule :

- **Instance Count** : nombre d'instances de portail captif actuellement configurées sur le périphérique WAP. Il est possible de configurer jusqu'à deux instances.
- **Group Count** : nombre de groupes de portail captif actuellement configurés sur le périphérique WAP. Il est possible de configurer jusqu'à deux groupes. Un groupe par défaut existe et ne peut pas être supprimé.

- **User Count** : nombre d'utilisateurs de portail captif actuellement configurés sur le périphérique WAP. Il est possible de configurer jusqu'à 128 utilisateurs.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Configuration d'instance

Vous pouvez créer jusqu'à deux instances de portail captif, chacune d'entre elles étant un ensemble défini de paramètres d'instance. Les instances peuvent être associées à un ou plusieurs points d'accès virtuels. Des instances différentes peuvent être configurées de manière à répondre différemment aux utilisateurs lorsque ceux-ci tentent d'accéder au point d'accès virtuel associé.

REMARQUE Commencez par passer en revue les puces suivantes avant de créer une instance :

- Avez-vous besoin d'ajouter un nouveau point d'accès virtuel ? Si oui, accédez à **Networks** pour ajouter un point d'accès virtuel.
- Avez-vous besoin d'ajouter un nouveau groupe ? Si oui, accédez à **Groupes locaux** pour ajouter un groupe.
- Avez-vous besoin d'ajouter un nouvel utilisateur ? Si oui, accédez à **Utilisateurs locaux** pour ajouter un utilisateur.

Pour créer une instance de portail captif et configurer ses paramètres :

ÉTAPE 1 Sélectionnez **Captive Portal** > **Instance Configuration** dans le volet de navigation.

ÉTAPE 2 Assurez-vous que la valeur **Créer** est sélectionnée dans la liste **Captive Port Instances**.

ÉTAPE 3 Saisissez un **Nom d'instance** comportant de 1 à 32 caractères alphanumériques, puis cliquez sur **Enregistrer**.

ÉTAPE 4 Sélectionnez le nom d'instance dans la liste **Captive Port Instances**.

Les champs Captive Portal Instance Parameters réapparaissent avec des options supplémentaires.

ÉTAPE 5 Configurez les paramètres suivants :

- **Instance ID** : ID d'instance. Ce champ n'est pas configurable.

- **Administrative Mode** : active et désactive l'instance de portail captif.
- **Protocol** : spécifie HTTP ou HTTPs en tant que protocole utilisé par l'instance de portail captif durant le processus de vérification.
  - **HTTP** : n'utilise pas le cryptage durant la vérification.
  - **HTTPS** : utilise le protocole SSL (Secure Sockets Layer), qui nécessite un certificat pour le cryptage.

    Le certificat est présenté à l'utilisateur lors de la connexion.
- **Verification** : méthode d'authentification utilisée par le portail captif pour la vérification des clients :
  - **Guest** : l'utilisateur n'a pas besoin d'être authentifié par une base de données.
  - **Local** : le périphérique WAP utilise une base de données locale pour authentifier les utilisateurs.
  - **RADIUS** : le périphérique WAP utilise une base de données située sur un serveur RADIUS distant pour authentifier les utilisateurs.
- **Redirect** : spécifie que le portail captif doit rediriger le client nouvellement authentifié vers l'URL configurée. Si cette option est désactivée, l'utilisateur voit la page d'accueil correspondant à ses paramètres régionaux après une vérification réussie.
- **Redirect URL** : entrez l'URL (y compris http://) vers laquelle le client nouvellement authentifié est redirigé si le mode de redirection d'URL est activé. La plage valide va de 0 à 256 caractères.
- **Away Timeout** : période pendant laquelle un utilisateur reste dans la liste des clients authentifiés de portail captif après la dissociation du client du périphérique WAP. Si la période spécifiée dans ce champ expire avant que le client ne tente de se réauthentifier, l'entrée du client est supprimée de la liste des clients authentifiés. La plage valide va de 0 à 1440 minutes. La valeur par défaut est de 60 minutes.

  REMARQUE Une valeur Away Timeout est également configurée pour chaque utilisateur. Reportez-vous à la page **Utilisateurs locaux**. La valeur Away Timeout définie à la page Local Users a priorité sur la valeur configurée ici, sauf si la valeur est définie à 0 (valeur par défaut). Une valeur égale à 0 indique que la valeur d'expiration de l'instance est utilisée.

- **Session Timeout** : temps de validité restant, en secondes, de la session de portail captif. Lorsque ce temps atteint la valeur zéro, le client est désauthentifié. La plage valide va de 0 à 1440 minutes. La valeur par défaut est 0.
- **Maximum Bandwidth Upstream** : vitesse maximale de chargement, en mégabits par seconde, à laquelle un client peut transmettre du trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante à laquelle le client peut envoyer des données sur le réseau. La plage valide va de 0 à 300 Mbits/s. La valeur par défaut est 0.
- **Maximum Bandwidth Downstream** : vitesse maximale de téléchargement, en mégabits par seconde, à laquelle un client peut recevoir du trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante à laquelle le client peut recevoir des données du réseau. La plage valide va de 0 à 300 Mbits/s. La valeur par défaut est 0.
- **User Group Name** : si le mode de vérification est Local ou RADIUS, ce paramètre affecte un groupe d'utilisateurs existant à l'instance de portail captif. Tous les utilisateurs appartenant à ce groupe sont autorisés à accéder au réseau par l'intermédiaire de ce portail.
- **RADIUS IP Network** : déterminez si le client WAP RADIUS utilise les adresses configurées de serveur RADIUS IPv4 ou IPv6.
- **Global RADIUS** : si le mode de vérification est RADIUS, sélectionnez cette option dans la liste de serveurs globaux RADIUS par défaut pour authentifier les clients. (Reportez-vous à **Serveur RADIUS** pour plus d'informations sur la configuration des serveurs RADIUS globaux.) Si vous souhaitez que la fonctionnalité de portail captif utilise un ensemble différent de serveurs RADIUS, décochez la case et configurez les serveurs dans les champs correspondants de cette page.
- **RADIUS Accounting** : active le suivi et la mesure des ressources consommées par un utilisateur donné, comme le temps système ou les quantités de données transmises et reçues.

  Si vous activez la gestion des comptes RADIUS, cette fonctionnalité est active à la fois pour le serveur RADIUS principal, pour l'ensemble des serveurs de sauvegarde et pour les serveurs configurés globalement et localement.

- **Server IP Address 1 ou Server IPv6 Address 1** : adresse IPv4 ou IPv6 du serveur RADIUS principal pour ce VAP. La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (192.0.2.10). La forme de l'adresse IPv6 doit être similaire à celle-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

  Lorsque le premier client sans fil tente de s'authentifier à l'aide du VAP, le périphérique WAP envoie une demande d'authentification au serveur principal. Si le serveur principal répond à la demande d'authentification, le périphérique WAP continue à utiliser ce serveur RADIUS en guise de serveur principal et les demandes d'authentification sont envoyées à l'adresse spécifiée.

- **Server IP Address (2** à **4)** ou **Server IPv6 Address (2** à **4)** : jusqu'à trois adresses de serveur RADIUS IPv4 ou IPv6 de sauvegarde.

  Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.

- **Key 1** : clé secrète partagée utilisée par le périphérique WAP pour s'authentifier au serveur RADIUS principal.

  Vous pouvez utiliser jusqu'à 63 caractères alphanumériques standard et caractères spéciaux. La clé est sensible à la casse et doit correspondre à la clé configurée sur le serveur RADIUS. Le texte que vous saisissez s'affiche sous forme d'astérisques.

- **Key 2 to 4** : clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur associé à Server IP Address 1 utilise Key 1 et Server IP Address 2 utilise Key 2, etc.

- **Locale Count** : nombre de paramètres régionaux associés à l'instance. Vous pouvez créer et affecter jusqu'à trois paramètres régionaux différents à chaque instance de portail captif à partir de la page Web Customization.

- **Delete Instance** : supprime l'instance en cours.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration initiale.

Association d'instance

Lorsque vous créez une instance, vous pouvez utiliser la page Instance Association pour associer une instance de portail captif à un point d'accès virtuel. Les paramètres de l'instance de portail captif associée s'appliquent aux utilisateurs qui tentent de s'authentifier sur le point d'accès virtuel.

Pour associer une instance à un point d'accès virtuel :

ÉTAPE 1 Sélectionnez **Captive Portal** > **Instance Association** dans le volet de navigation.

ÉTAPE 2 Sélectionnez le nom d'instance pour chaque point d'accès virtuel auquel vous voulez associer une instance.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration initiale.

Personnalisation de portail Web

Lorsque votre instance de portail captif a été associée à un point d'accès virtuel, vous devez créer des paramètres régionaux (une page Web d'authentification) et les mapper à l'instance de portail captif. Lorsqu'un utilisateur accède à un point d'accès virtuel associé à une instance de portail captif, une page d'authentification s'affiche. Utilisez la page Web Portal Customization pour créer des pages uniques pour les différents paramètres régionaux sur votre réseau et personnaliser le texte et les images sur les pages.

Pour créer et personnaliser une page d'authentification de portail captif :

ÉTAPE 1 Sélectionnez **Captive Portal > Web Portal Customization** dans le volet de navigation.

ÉTAPE 2 Sélectionnez **Créer** dans la liste **Captive Portal Web Locale**.

Vous pouvez créer jusqu'à trois pages d'authentification différentes avec différents paramètres régionaux sur votre réseau.

ÉTAPE 3 Saisissez un (**Nom de paramètres régionaux Web**) à affecter à la page. Le nom peut être constitué de 1 à 32 caractères alphanumériques.

ÉTAPE 4 Dans la liste **Captive Portal Instances**, sélectionnez l'instance de portail captif avec laquelle ces paramètres régionaux sont associés.

Vous pouvez associer plusieurs paramètres régionaux à une instance. Lorsqu'un utilisateur tente d'accéder à un point d'accès virtuel spécifique associé à une instance de portail captif, les paramètres régionaux qui sont associés à cette instance apparaissent sous la forme de liens sur la page d'authentification. L'utilisateur peut alors sélectionner un lien pour passer à ces paramètres régionaux.

ÉTAPE 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

ÉTAPE 6 Dans la liste **Captive Portal Web Locale**, sélectionnez les paramètres régionaux que vous avez créés.

La page affiche des champs supplémentaires pour la modification des paramètres régionaux. Les champs **Locale ID** et **Instance Name** ne peuvent pas être modifiés. Les champs modifiables sont préremplis avec les valeurs par défaut.

ÉTAPE 7 Configurez les paramètres suivants :

- **Background Image Name** : image à afficher en tant qu'arrière-plan de page. Vous pouvez cliquer sur **Upload/Delete Custom Image** pour charger des images pour les instances de portail captif. Voir Chargement et suppression d'images.
- **Logo Image Name** : fichier image à afficher dans le coin supérieur gauche de la page. Cette image est utilisée à des fins commerciales (il s'agit par exemple du logo de l'entreprise). Si vous avez téléchargé un logo personnalisé vers le périphérique WAP, vous pouvez le sélectionner dans la liste.
- **Foreground color** : code HTML de la couleur de premier plan au format hexadécimal à 6 chiffres. La plage valide va de 1 à 32 caractères. La valeur par défaut est #999999.
- **Background color** : code HTML de la couleur d'arrière-plan au format hexadécimal à 6 chiffres. La plage valide va de 1 à 32 caractères. La valeur par défaut est #BFBFBF.
- **Separator** : code HTML de la couleur de l'épaisse ligne horizontale séparant l'en-tête de page du corps de page, au format hexadécimal à 6 chiffres. La plage valide va de 1 à 32 caractères. La valeur par défaut est #BFBFBF.

- **Locale Label** : étiquette descriptive des paramètres régionaux, composée de 1 à 32 caractères. La langue par défaut est l'anglais.
- **Locale** : abréviation des paramètres régionaux, composée de 1 à 32 caractères. La valeur par défaut est en.
- **Account Image** : fichier image à afficher au-dessus du champ de connexion pour représenter une connexion authentifiée.
- **Account Label** : texte demandant à l'utilisateur d'entrer un nom d'utilisateur. La plage valide va de 1 à 32 caractères.
- **User Label** : étiquette de la zone de texte du nom d'utilisateur. La plage valide va de 1 à 32 caractères.
- **Password Label** : étiquette de la zone de texte du mot de passe d'utilisateur. La plage valide va de 1 à 64 caractères.
- **Button Label** : étiquette du bouton sur lequel les utilisateurs cliquent afin de soumettre leur nom d'utilisateur et leur mot de passe pour authentification. La plage valide va de 2 à 32 caractères. La valeur par défaut est Connect.
- **Fonts** : nom de la police à utiliser pour l'ensemble du texte de la page de portail captif. Vous pouvez entrer plusieurs noms de police, chaque nom devant être séparé des autres par une virgule. Si la première police n'est pas disponible sur le système client, la police suivante est utilisée, etc. Si un nom de police contient des espaces, mettez le nom complet entre guillemets. La plage valide va de 1 à 512 caractères. La valeur par défaut est MS UI Gothic, Arial, sans-serif.
- **Browser Title** : texte à afficher dans la barre de titre du navigateur. La plage valide va de 1 à 128 caractères. La valeur par défaut est Captive Portal.
- **Browser Content** : texte qui apparaît dans l'en-tête de page, à droite du logo. La plage valide va de 1 à 128 caractères. La valeur par défaut est Welcome to the Wireless Network.
- **Content** : texte d'instruction qui s'affiche dans le corps de page en dessous des zones de texte du nom d'utilisateur et du mot de passe. La plage valide va de 1 à 256 caractères. La valeur par défaut est To start using this service, enter your credentials and click the connect button.
- **Acceptance Use Policy** : texte qui apparaît dans la zone de texte Acceptance Use Policy. La plage valide va de 1 à 4096 caractères. La valeur par défaut est Acceptance Use Policy.

- **Accept Label** : texte demandant aux utilisateurs d'activer la case à cocher relative à la lecture et à l'acceptation de la stratégie d'utilisation. La plage valide va de 1 à 128 caractères. La valeur par défaut est Check here to indicate that you have read and accepted the Acceptance Use Policy.
- **No Accept Text** : texte qui s'affiche dans une fenêtre contextuelle lorsqu'un utilisateur soumet ses informations d'identification de connexion sans avoir activé la case à cocher Acceptance Use Policy. La plage valide va de 1 à 128 caractères. La valeur par défaut est Error: You must acknowledge the Acceptance Use Policy before connecting!
- **Work In Progress Text** : texte qui s'affiche durant l'authentification. La plage valide va de 1 à 128 caractères. La valeur par défaut est Connecting, please be patient....
- **Denied Text** : texte qui s'affiche lors de l'échec de l'authentification d'un utilisateur. La plage valide va de 1 à 128 caractères. La valeur par défaut est Error Invalid Credentials, please try again!
- **Welcome Title** : texte qui s'affiche lorsque le client s'est authentifié sur le point d'accès virtuel. La plage valide va de 1 à 128 caractères. La valeur par défaut est Congratulations!
- **Welcome Content** : texte qui s'affiche lorsque le client s'est connecté au réseau. La plage valide va de 1 à 256 caractères. La valeur par défaut est You are now authorized and connected to the network.
- **Delete Locale** : supprime les paramètres régionaux actuels.

ÉTAPE 8 Cliquez sur **Enregistrer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration initiale.

ÉTAPE 9 Cliquez sur **Aperçu** pour afficher la page mise à jour.

REMARQUE Vous pouvez cliquer sur **Aperçu** pour afficher le texte et les images qui ont déjà été enregistrés dans la configuration initiale. Si vous apportez des modifications, cliquez sur **Enregistrer** avant de cliquer sur **Aperçu** pour voir vos modifications.

Chargement et suppression d'images

Lorsque des utilisateurs créent un accès à un point d'accès virtuel associé à une instance de portail captif, une page d'authentification apparaît. Vous pouvez personnaliser la page d'authentification avec votre propre logo ou d'autres images.

Vous pouvez charger jusqu'à 18 images (à savoir six valeurs de paramètres régionaux, chaque valeur possédant trois images). Les images doivent être au format GIF ou JPG, et leur taille maximale est de 5 kilo-octets.

Les images sont redimensionnées en vue de correspondre aux dimensions spécifiées. Pour obtenir des résultats optimaux, les images de votre logo et de votre compte doivent être de proportions similaires à celles des images par défaut, comme indiqué ci-dessous :

Type d'image	Utilisation	Largeur x hauteur par défaut
Arrière-plan	S'affiche en tant qu'arrière-plan de page.	10 x 800 pixels
Logo	S'affiche en haut à gauche de la page en vue de fournir des informations commerciales.	168 x 78 pixels
Compte	S'affiche au-dessus du champ de connexion pour représenter une connexion authentifiée.	295 x 55 pixels

Pour charger des fichiers graphiques binaires sur le périphérique WAP :

ÉTAPE 1 Sur la page Web Portal Customization, cliquez sur **Upload/Delete Custom Image** à côté des champs **Background Image Name**, **Logo Image Name** ou **Account Image**.

La page Web Portal Custom Image apparaît.

ÉTAPE 2 Recherchez l'image que vous voulez sélectionner.

ÉTAPE 3 Cliquez sur **Upload**.

ÉTAPE 4 Cliquez sur **Précédent** pour revenir à la page Web Portal Custom Image.

ÉTAPE 5 Sélectionnez les **Paramètres régionaux Web de portail captif** que vous voulez configurer.

ÉTAPE 6 Pour les champs **Background Image Name**, **Logo Image Name** ou **Account Image**, sélectionnez l'image nouvellement chargée.

ÉTAPE 7 Cliquez sur **Enregistrer**.

REMARQUE Pour supprimer une image, sur la page Web Portal Custom Image, sélectionnez-la dans la liste **Delete Web Customization Image**, puis cliquez sur **Supprimer**. Vous ne pouvez pas supprimer les images par défaut.

Groupes locaux

Chaque utilisateur local est affecté à un groupe d'utilisateurs. Chaque groupe est affecté à une instance de portail captif. Le groupe facilite la gestion de l'affectation des utilisateurs aux instances de portail captif.

Le groupe d'utilisateurs nommé Default est intégré et ne peut pas être supprimé. Vous pouvez créer jusqu'à deux groupes d'utilisateurs supplémentaires.

Pour ajouter des groupes d'utilisateurs locaux :

ÉTAPE 1 Sélectionnez **Captive Portal** > **Local Groups** dans le volet de navigation.

ÉTAPE 2 Saisissez un **Nom de groupe** et cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE Pour supprimer un groupe, sélectionnez-le dans la liste **Captive Portal Groups**, activez la case à cocher **Delete Group** et cliquez sur **Enregistrer**.

Utilisateurs locaux

Vous pouvez configurer une instance de portail captif de telle sorte qu'elle réponde à la fois aux besoins des utilisateurs invités et des utilisateurs autorisés. Les utilisateurs invités ne possèdent pas de noms d'utilisateur et de mots de passe.

Les utilisateurs autorisés fournissent un nom d'utilisateur et un mot de passe valides qui doivent tout d'abord être validés à partir d'une base de données locale ou d'un serveur RADIUS. Les utilisateurs autorisés sont généralement affectés à une instance de portail captif associée à un autre point d'accès virtuel que les utilisateurs invités.

Utilisez la page Local Users pour configurer jusqu'à 128 utilisateurs autorisés dans la base de données locale.

Pour ajouter et configurer un utilisateur local :

ÉTAPE 1 Sélectionnez **Captive Portal** > **Local Users** dans le volet de navigation.

ÉTAPE 2 Saisissez un **Nom d'utilisateur** et cliquez sur **Enregistrer**.

Des champs supplémentaires apparaissent pour la configuration de l'utilisateur.

ÉTAPE 3 Configurez les paramètres suivants :

- **User Password** : entrez le mot de passe, composé de 8 à 64 caractères alphanumériques et caractères spéciaux. Un utilisateur doit entrer son mot de passe pour se connecter au réseau par l'intermédiaire du portail captif.
- **Show Password as Clear Text** : lorsque cette option est activée, le texte que vous tapez est visible. Si cette option est désactivée, le texte n'est pas masqué lors de sa saisie.
- **Away Timeout** : période pendant laquelle un utilisateur reste dans la liste des clients authentifiés de portail captif après la dissociation du client du point d'accès. Si la période spécifiée dans ce champ expire avant que le client ne tente de se réauthentifier, l'entrée du client est supprimée de la liste des clients authentifiés. La plage valide va de 0 à 1440 minutes. La valeur par défaut est 60. La valeur d'expiration configurée ici a priorité sur la valeur configurée pour l'instance de portail captif, sauf si la valeur utilisateur est définie à 0. Lorsque cette valeur est définie à 0, la valeur d'expiration configurée pour l'instance de portail captif est utilisée.
- **Group Name** : groupe d'utilisateurs affecté. Chaque instance de portail captif est configurée de manière à prendre en charge un groupe d'utilisateurs particulier.
- **Maximum Bandwidth Up** : vitesse maximale de chargement, en mégabits par seconde, à laquelle un client peut transmettre du trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante utilisée pour envoyer des données sur le réseau. La plage valide va de 0 à 300 Mbits/s. La valeur par défaut est 0.
- **Maximum Bandwidth Down** : vitesse maximale de téléchargement, en mégabits par seconde, à laquelle un client peut recevoir du trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante utilisée pour recevoir des données du réseau. La plage valide va de 0 à 300 Mbits/s. La valeur par défaut est 0.
- **Delete User** : supprime l'utilisateur en cours.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Clients authentifiés

La page Authenticated Clients fournit des informations sur les clients qui ont été authentifiés sur n'importe quelle instance de portail captif.

Pour afficher la liste des clients authentifiés, sélectionnez **Captive Portal** > **Authenticated Clients** dans le volet de navigation.

- **MAC Address** : adresse MAC du client.
- **IP Address** : adresse IP du client.
- **User Name** : nom d'utilisateur de portail captif du client.
- **Protocol** : protocole employé par l'utilisateur pour établir la connexion (HTTP ou HTTPS).
- **Verification** : méthode utilisée pour l'authentification de l'utilisateur sur le portail captif. Les valeurs possibles sont les suivantes :
  - **Guest** : l'utilisateur n'a pas besoin d'être authentifié par une base de données.
  - **Local** : le périphérique WAP utilise une base de données locale pour authentifier les utilisateurs.
  - **RADIUS** : le périphérique WAP utilise une base de données située sur un serveur RADIUS distant pour authentifier les utilisateurs.
- **VAP ID** : point d'accès virtuel auquel l'utilisateur est associé.
- **Radio ID** : ID de la radio. Le périphérique WAP321 ne possédant qu'une seule fréquence, ce champ affiche toujours Radio 1.
- **Captive Portal ID** : ID de l'instance de portail captif à laquelle l'utilisateur est associé.
- **Session Timeout** : temps de validité restant, en secondes, de la session de portail captif. Lorsque ce temps atteint la valeur zéro, le client est désauthentifié.
- **Away Timeout** : temps de validité restant, en secondes, de l'entrée du client. La minuterie démarre lorsque le client se dissocie du portail captif. Lorsque le temps atteint la valeur zéro, le client est désauthentifié.
- **Received Packets** : nombre de paquets IP reçus par le périphérique WAP depuis la station utilisateur.

- **Transmitted Packets** : nombre de paquets IP transmis depuis le périphérique WAP vers la station utilisateur.
- **Received Bytes** : nombre d'octets reçus par le périphérique WAP depuis la station utilisateur.
- **Transmitted Bytes** : nombre d'octets transmis depuis le périphérique WAP vers la station utilisateur.

Vous pouvez cliquer sur **Refresh** pour afficher les dernières données en provenance du périphérique WAP.

Clients dont l'authentification a échoué

La page Failed Authenticated Clients fournit des informations sur les clients qui ont tenté de s'authentifier sur un portail captif et qui ont échoué.

Pour afficher la liste des clients dont l'authentification a échoué, sélectionnez **Captive Portal** > **Failed Authentication Clients** dans le volet de navigation.

- **MAC Address** : adresse MAC du client.
- **IP Address** : adresse IP du client.
- **User Name** : nom d'utilisateur de portail captif du client.
- **Verification** : méthode que le client a tenté d'utiliser pour s'authentifier sur le portail captif. Les valeurs possibles sont les suivantes :
  - **Guest** : l'utilisateur n'a pas besoin d'être authentifié par une base de données.
  - **Local** : le périphérique WAP utilise une base de données locale pour authentifier les utilisateurs.
  - **RADIUS** : le périphérique WAP utilise une base de données située sur un serveur RADIUS distant pour authentifier les utilisateurs.
- **VAP ID** : point d'accès virtuel auquel l'utilisateur est associé.
- **Radio ID** : ID de la radio. Le périphérique WAP321 ne possédant qu'une seule fréquence, ce champ affiche Radio 1.
- **Captive Portal ID** : ID de l'instance de portail captif à laquelle l'utilisateur est associé.

- **Failure Time** : heure à laquelle l'échec de l'authentification s'est produit. Un horodatage est inclus, indiquant l'heure de l'échec.

Vous pouvez cliquer sur **Refresh** pour afficher les dernières données en provenance du périphérique WAP.

10

Configuration de point unique

Ce chapitre explique comment paramétrer une configuration de point unique sur plusieurs périphériques WAP.

Il contient les rubriques suivantes :

- Présentation de la configuration de point unique
- Points d'accès
- Sessions
- Gestion des canaux
- Voisinage sans fil

Présentation de la configuration de point unique

Les périphériques Cisco WAP121 et WAP321 prennent en charge la configuration de point unique. La configuration de point unique est une méthode centralisée permettant d'administrer et de contrôler les services sans fil sur plusieurs périphériques. La configuration de point unique sert à créer un groupe ou un cluster unique de périphériques sans fil. Lorsque les périphériques WAP sont regroupés en un cluster, vous pouvez afficher, déployer, configurer et sécuriser le réseau sans fil en tant qu'entité unique. Après la création d'un cluster sans fil, la configuration de point unique facilite également la planification des canaux sur l'ensemble de vos services sans fil afin de réduire les interférences radio et d'optimiser la bande passante du réseau sans fil.

Lors de la première configuration d'un périphérique WAP, vous pouvez paramétrer la configuration de point unique à l'aide de l'assistant de configuration ou ajouter le périphérique à une configuration de point unique existante. Si vous ne souhaitez pas utiliser l'assistant de configuration, vous pouvez vous servir de l'utilitaire de configuration Web.

Gestion de la configuration de point unique sur les périphériques WAP

La configuration de point unique créé, dans le même sous-réseau, un cluster ou un groupe de périphériques WAP dynamique et sensible à la configuration. Un cluster ne prend en charge qu'un groupe de périphériques WAP121 configurés ou un groupe de périphériques WAP321 configurés. Un seul cluster ne prend pas en charge un mélange de périphériques WAP121 et WAP321 dans le même groupe.

La configuration de point unique permet la gestion de plusieurs clusters dans un même sous-réseau ou réseau. Toutefois, les clusters sont gérés en tant qu'entités indépendantes uniques. Le tableau ci-dessous indique les limites des services sans fil à configuration de point unique.

Type de groupe/ cluster	Nombre de périphériques WAP par configuration de point unique	Nombre de clients actifs par configuration de point unique	Nombre maximal de clients (actifs et inactifs)
WAP121	4	40	64
WAP321	8	160	256

Un cluster peut propager des informations de configuration, telles que les paramètres du point d'accès virtuel, de file d'attente QoS et de radio. Lorsque vous paramétrez une configuration de point unique sur un périphérique, les paramètres de celui-ci (qu'ils aient été définis manuellement ou par défaut) sont propagés aux autres périphériques lorsqu'ils rejoignent le cluster. Pour former un cluster, suivez la procédure suivante :

ÉTAPE 1 Planifiez votre cluster à configuration de point unique. Vérifiez que les périphériques WAP que vous souhaitez regrouper dans le cluster sont du même modèle. Par exemple, les périphériques Cisco WAP121 peuvent uniquement être regroupés dans un cluster contenant des périphériques Cisco WAP121.

Il est fortement recommandé d'utiliser la dernière version du microprogramme sur tous les périphériques WAP du cluster.

> **REMARQUE** Les mises à niveau du microprogramme **ne sont pas** propagées sur tous les périphériques WAP d'un cluster. Vous devez donc mettre à niveau individuellement chaque périphérique.

ÉTAPE 2 Configurez les périphériques WAP qui seront regroupés en cluster sur un même sous-réseau IP et vérifiez qu'ils sont interconnectés et accessibles sur l'ensemble du réseau local commuté.

ÉTAPE 3 Activez la configuration de point unique sur tous les périphériques WAP. Reportez-vous à la section **Points d'accès**.

ÉTAPE 4 Vérifiez que tous les périphériques WAP indiquent le même nom de configuration de point unique. Reportez-vous à la section **Points d'accès**.

Négociation de la configuration de point unique

Lorsque la configuration de point unique est activée et paramétrée sur un Périphérique WAP, celui-ci commence à envoyer des annonces toutes les 10 secondes pour signaler sa présence. Si d'autres périphériques WAP correspondent aux critères du cluster, un arbitrage a lieu afin de déterminer quel périphérique WAP distribuera la configuration principale aux autres membres du cluster.

Les règles suivantes s'appliquent à la formation et à l'arbitrage du cluster à configuration de point unique :

- Pour les clusters à configuration de point unique existants, dès que l'administrateur met à jour la configuration de l'un des membres du cluster, la modification est propagée à tous les membres du cluster et le périphérique WAP configuré prend le contrôle du cluster.
- Lorsque deux clusters à configuration de point unique distincts sont regroupés en un seul cluster, le cluster modifié en dernier remporte l'arbitrage de la configuration. Il écrase et met alors à jour la configuration de tous les périphériques WAP du cluster.
- Si un périphérique WAP d'un cluster ne reçoit pas les annonces d'un autre périphérique WAP pendant plus de 60 secondes (par exemple si le périphérique n'est plus connecté aux autres périphériques du cluster), celui-ci est supprimé du cluster.
- Si un périphérique WAP en mode de configuration de point unique perd sa connexion, il n'est pas immédiatement exclu du cluster. S'il se reconnecte et rejoint le cluster sans être exclu et que des modifications ont été apportées à la configuration de ce périphérique lorsqu'il était déconnecté, les modifications sont propagées aux autres membres du cluster lorsque la connexion est rétablie.

- Si un périphérique WAP d'un cluster perd sa connexion, est exclu, puis rejoint à nouveau le cluster et que des modifications ont été apportées à la configuration du cluster lorsqu'il était déconnecté, les modifications sont propagées au périphérique lorsqu'il rejoint le cluster. Si des modifications de configuration sont effectuées à la fois sur le périphérique déconnecté et sur le cluster, le périphérique ayant subi le plus de modifications, puis, en deuxième lieu, celui ayant subi la modification la plus récente propagera sa configuration au cluster. (C'est-à-dire que WAP1 a subi davantage de modifications, mais que WAP2 a subi la modification la plus récente, c'est WAP1 qui propagera sa configuration. S'ils ont tous les deux subi le même nombre de modifications, mais que WAP2 a subi la modification la plus récente, alors c'est WAP2 qui propagera sa configuration.)

Fonctionnement d'un périphérique WAP exclu d'une configuration de point unique

Lorsqu'un périphérique WAP qui était auparavant un membre d'un cluster est déconnecté de celui-ci, les règles suivantes s'appliquent :

- La perte du contact avec le cluster empêche le périphérique WAP de recevoir les derniers paramètres de configuration opérationnels. La déconnexion provoque l'interruption du service sans fil correct sur l'ensemble du réseau de production.
- Le périphérique WAP continue de fonctionner selon les paramètres sans fil qu'il a reçus en dernier du cluster.
- Les clients sans fil associés au périphérique WAP non inclus dans le cluster continuent à s'associer au périphérique sans provoquer d'interruption de la connexion sans fil. En d'autres termes, la perte du contact avec le cluster n'interrompt pas forcément l'accès aux ressources réseau des clients sans fil associés au périphérique WAP déconnecté.
- Si la perte du contact avec le cluster est liée à une déconnexion physique ou logique de l'infrastructure LAN, elle peut avoir une incidence sur les services réseau voire sur les clients sans fil, selon la nature de la panne.

Propagation des paramètres de configuration dans une configuration de point unique

Le tableau suivant récapitule les configurations partagées et propagées à l'ensemble des périphériques WAP du cluster.

Paramètres de configuration communs propagés en mode de configuration de point unique	
Portail captif	Password Complexity
Client QoS	User Accounts
Email Alert	QoS
HTTP/HTTPs Service (sauf SSL Certificate Configuration)	Radio Settings y compris TSpec Settings (sauf quelques exceptions)
Log Settings	Rogue AP Detection
MAC Filtering	Scheduler
Management Access Control	SNMP General et SNMPv3
Networks	WPA-PSK Complexity
Paramètres horaires	

Paramètres de configuration radio propagés en mode de configuration de point unique
Mode
Fragmentation Threshold
RTS Threshold
Rate Sets
Primary Channel
Protection
Fixed Multicast Rate
Broadcast or Multicast Rate Limiting
Channel Bandwidth
Short Guard Interval Supported

Paramètres de configuration radio non propagés en mode de configuration de point unique
Canal
Beacon Interval
DTIM Period
Maximum Stations
Transmit Power

Autres paramètres de configuration non propagés en mode de configuration de point unique	
Bandwidth Utilization	Port Settings
Bonjour	VLAN et IPv4
IPv6 Address	WDS Bridge
IPv6 Tunnel	WPS
Packet Capture	WorkGroup Bridge

Points d'accès

La page Access Points vous permet d'activer et de désactiver la configuration de point unique sur un périphérique WAP, d'afficher les membres d'un cluster et de configurer l'emplacement et le nom du cluster sur un membre. Vous pouvez également cliquer sur l'adresse IP d'un membre pour configurer et afficher les données de ce périphérique.

Configuration du périphérique WAP pour la configuration de point unique

Pour configurer l'emplacement et le nom d'un membre d'un cluster à configuration de point unique, procédez comme suit :

ÉTAPE 1 Cliquez sur **Single Point Setup > Access Points** dans le volet de navigation.

La configuration de point unique est désactivée par défaut sur le Périphérique WAP. Lorsque celle-ci est désactivée, le bouton **Enable Single Point Setup** est visible. Si la configuration de point unique est désactivée, le bouton **Disable Single Point Setup** est visible. Vous ne pouvez modifier les options de configuration de point unique que si la configuration de point unique est désactivée.

Des icônes situées sur la droite de la page indiquent si elle est activée et, dans l'affirmative, elles spécifient également le nombre de périphériques WAP formant actuellement le cluster.

ÉTAPE 2 Après vous être assuré que la configuration de point unique est désactivée, configurez les paramètres suivants pour chaque membre du cluster à configuration de point unique.

- **Location** : saisissez une description de l'emplacement physique du point d'accès, par exemple « Réception ». Ce champ est facultatif.
- **Cluster Name** : indiquez le nom du cluster auquel le périphérique WAP doit se joindre, par exemple « Cluster_Réception ».

  Le nom du cluster n'est pas envoyé aux autres périphériques WAP. Vous devez donc configurer le même nom sur chaque périphérique membre d'un même cluster. Le nom du cluster doit par ailleurs être unique pour chaque configuration de point unique que vous paramétrez sur le réseau. Le nom par défaut est « ciscosb-cluster ».
- **Clustering IP Version** : indiquez la version du protocole IP que les périphériques WAP du cluster utilisent pour communiquer avec les autres membres du cluster. La version par défaut est IPv4.

  Si vous choisissez la version IPv6, la configuration de point unique peut utiliser l'adresse de liaison locale, l'adresse IPv6 globale autoconfigurée et l'adresse IPv6 globale configurée de manière statique. Dans ce cas, assurez-vous que tous les périphériques WAP du cluster utilisent soit uniquement des adresses de liaison locales soit uniquement des adresses globales.

La configuration de point unique fonctionne uniquement sur des périphériques utilisant le même type d'adressage IP. Elle ne fonctionne pas dans les groupes de périphériques WAP dont certains utilisent des adresses IPv4 et d'autres des adresses IPv6.

ÉTAPE 3 Cliquez sur **Enable Single Point Setup**.

Le périphérique WAP commence à rechercher dans le sous-réseau d'autres périphériques WAP configurés avec le même nom de cluster et la même version du protocole IP. Les membres éventuels du cluster envoient des annonces toutes les 10 secondes afin de signaler leur présence.

Pendant la recherche d'autres membres du cluster, l'état indique que la configuration est en cours d'application. Actualisez la page pour afficher la nouvelle configuration.

Si un ou plusieurs périphériques WAP sont déjà configurés avec les mêmes paramètres de cluster, le périphérique WAP rejoint le cluster et les informations sur chaque membre s'affichent dans un tableau.

ÉTAPE 4 Répétez cette procédure sur les autres périphériques WAP que vous souhaitez ajouter à la configuration de point unique.

Affichage des informations de la configuration de point unique

Lorsque le mode Configuration de point unique est activé, le Périphérique WAP forme automatiquement un cluster avec les autres périphériques WAP dotés de la même configuration. Sur la page Access Points, les périphériques WAP détectés sont répertoriés dans un tableau et les informations suivantes sont affichées :

- **Location** : description de l'emplacement physique du point d'accès.
- **MAC Address** : adresse MAC (Media Access Control) du point d'accès. Cette adresse correspond à l'adresse MAC du pont (br0) et à l'adresse du périphérique WAP connue des autres réseaux.
- **IP Address** : adresse IP du point d'accès.

Remarque : l'état de la configuration de point unique et le nombre de périphériques WAP sont indiqués par des graphiques sur la droite de la page.

Ajout d'un nouveau point d'accès à un cluster à configuration de point unique

Pour ajouter à un cluster à configuration de point unique un nouveau point d'accès actuellement en mode autonome, procédez comme suit :

ÉTAPE 1 Accédez à l'utilitaire de configuration Web sur le point d'accès autonome.

ÉTAPE 2 Cliquez sur **Single Point Setup > Access Points** dans le volet de navigation.

ÉTAPE 3 Dans **Cluster name**, indiquez le nom de cluster que vous avez configuré sur les membres du cluster.

ÉTAPE 4 Dans le champ Location, saisissez une description de l'emplacement physique du point d'accès, par exemple « Réception » (facultatif).

ÉTAPE 5 Cliquez sur **Enable Single Point Setup**.

Le point d'accès rejoint automatiquement la configuration de point unique.

Suppression d'un point d'accès d'un cluster à configuration de point unique

Pour supprimer un point d'accès d'un cluster à configuration de point unique, procédez comme suit :

ÉTAPE 1 Dans le tableau affichant les périphériques détectés, cliquez sur l'adresse IP du périphérique WAP que vous souhaitez supprimer du cluster.

L'utilitaire de configuration Web de ce périphérique s'affiche.

ÉTAPE 2 Cliquez sur **Single Point Setup > Access Points** dans le volet de navigation.

ÉTAPE 3 Cliquez sur **Disable Single Point Setup**.

Le champ d'état **Single Point Setup** de ce point d'accès indique alors **Disabled**.

Accès aux informations de configuration d'un périphérique WAP spécifique

Tous les périphériques WAP d'un cluster à configuration de point unique présentent la même configuration (à condition que la propagation des éléments configurables soit possible). Peu importe le périphérique WAP auquel vous vous connectez pour l'administration, les modifications de la configuration de n'importe quel périphérique WAP du cluster sont propagées aux autres membres.

Cependant, il peut arriver que vous souhaitiez afficher ou gérer des informations d'un périphérique WAP spécifique. Par exemple, vous souhaiterez peut-être consulter des informations relatives à l'état d'un point d'accès, notamment les associations de clients ou les événements. Dans ce cas, vous pouvez cliquer sur l'adresse IP figurant dans le tableau de la page Access Points pour afficher l'utilitaire de configuration Web de ce point d'accès.

Accès à un périphérique WAP à l'aide de son adresse IP dans une URL

Vous pouvez également vous connecter à l'utilitaire de configuration Web d'un périphérique spécifique en saisissant l'adresse IP de ce point d'accès directement dans la barre d'adresse d'un navigateur Web. Pour cela, utilisez la forme d'URL suivante :

http://*AdresseIPDuPointD'Accès* (si vous utilisez le protocole HTTP)

https://AdresseIPDuPointD'Accès (si vous utilisez le protocole HTTPS)

Sessions

La page Sessions affiche des informations sur les clients WLAN associés aux périphériques WAP du cluster à configuration de point unique. Chaque client WLAN est identifié par son adresse MAC et l'emplacement du périphérique auquel il est actuellement connecté.

REMARQUE La page Sessions affiche un maximum de 20 clients par radio des périphériques WAP du cluster. Pour afficher tous les clients WLAN associés à un périphérique WAP, consultez la page Status > Associated Clients directement sur ce périphérique.

Pour afficher une statistique spécifique d'une session de client WLAN, sélectionnez un élément de la liste Display et cliquez sur **Go**. Vous pouvez consulter des informations sur le temps d'inactivité, le débit et la puissance du signal.

Dans ce contexte, une session correspond à la période pendant laquelle un utilisateur d'un périphérique client (station) doté d'une adresse MAC unique maintient une connexion au réseau sans fil. La session commence lorsque le client WLAN se connecte au réseau. Elle se termine lorsque le client WLAN se déconnecte, intentionnellement ou non.

REMARQUE Une session diffère d'une association, qui décrit la connexion de clients WLAN à un point d'accès spécifique. Une association de clients WLAN peut passer d'un point d'accès du cluster à un autre au cours d'une même session.

Pour afficher les sessions associées au cluster, cliquez sur **Single Point Setup > Sessions** dans le volet de navigation.

Les données suivantes s'affichent pour chaque session de client WLAN avec une configuration de point unique.

- **AP Location** : emplacement du point d'accès

  L'emplacement est celui spécifié sur la page Administration > System Settings.

- **User MAC** : adresse MAC du client sans fil.

  Une adresse MAC est une adresse matérielle unique qui identifie chaque nœud d'un réseau.

- **Idle** : temps d'inactivité d'un client WLAN.

  Un client WLAN est considéré comme inactif lorsqu'il ne reçoit et ne transmet aucune donnée.

- **Rate** : débit de données négocié. Les débits réels peuvent varier en fonction de la surcharge.

  La vitesse de transmission des données est mesurée en mégabits par seconde (Mbits/s). Cette valeur doit être comprise dans la plage de débit annoncée pour le mode utilisé sur le point d'accès. Par exemple entre 6 et 54 Mbits/s pour le mode 802.11a.

- **Signal** : puissance du signal de radiofréquence (RF) reçu du point d'accès par le client WLAN. Cette valeur est appelée RSSI (Received Signal Strength Indication) et se situe entre 0 et 100.

- **Receive Total** : nombre total de paquets reçus par le client WLAN au cours de la session actuelle.
- **Transmit Total** : nombre total de paquets transmis au client WLAN au cours de cette session.
- **Error Rate** : pourcentage d'abandons de trames au cours de la transmission sur ce point d'accès.

Pour trier les informations affichées dans les tableaux selon un indicateur spécifique, cliquez sur l'étiquette de la colonne qui déterminera le tri. Par exemple, si vous souhaitez classer les lignes du tableau en fonction de la puissance du signal, cliquez sur l'étiquette de colonne Signal.

Gestion des canaux

La page Channel Management affiche les attributions actuelles et prévues des canaux aux périphériques WAP d'un cluster à configuration de point unique.

Lorsque la gestion des canaux est activée, le Périphérique WAP attribue automatiquement les canaux radio utilisés par les périphériques WAP dans un cluster à configuration de point unique. L'attribution automatique des canaux réduit les interférences mutuelles des périphériques du cluster (ou les interférences avec d'autres périphériques WAP extérieurs au cluster) et optimise la bande passante Wi-Fi afin d'assurer une communication efficace sur le réseau sans fil.

La fonction d'attribution automatique des canaux est désactivée par défaut. L'état de la fonction de gestion des canaux (activé ou désactivé) est propagé aux autres périphériques du cluster à configuration de point unique.

À un intervalle défini, le gestionnaire des canaux (c'est-à-dire le périphérique ayant fourni la configuration au cluster) mappe tous les périphériques WAP du cluster avec différents canaux et mesure les niveaux d'interférence des membres du cluster. Si des interférences importantes sont détectées entre les canaux, le gestionnaire de canaux réattribue automatiquement certains ou tous les périphériques à d'autres canaux à l'aide d'un algorithme d'efficacité (ou d'une stratégie de canaux automatisée). Si le gestionnaire de canaux détermine qu'un changement est nécessaire, les informations de réattribution sont envoyées à tous les membres du cluster. Un message Syslog indiquant également le périphérique d'émission et les nouvelles et anciennes attributions des canaux est généré.

Pour configurer et afficher les attributions des canaux des membres de la configuration de point unique, procédez comme suit :

ÉTAPE 1 Cliquez sur **Single Point Setup** > **Channel Management** dans le volet de navigation.

La page Channel Management affiche les attributions de canaux de tous les périphériques WAP du cluster et vous permet d'interrompre ou de démarrer la gestion automatique des canaux. Les paramètres avancés vous permettent de modifier le potentiel de réduction des interférences qui entraîne la réattribution des canaux, de modifier le calendrier des mises à jour automatiques et de reconfigurer l'ensemble de canaux utilisé pour l'attribution.

ÉTAPE 2 Pour lancer l'attribution automatique des canaux, cliquez sur **Démarrer**.

La gestion des canaux remplace le comportement par défaut du cluster qui consiste à synchroniser les canaux radio de tous les périphériques WAP membres du cluster. Lorsque la gestion des canaux est activée, le canal radio n'est pas synchronisé entre le cluster et les autres périphériques.

Lorsque l'attribution automatique des canaux est activée, le gestionnaire de canaux mappe régulièrement les canaux radio utilisés par les périphériques WAP d'un cluster à configuration de point unique et réattribue les canaux, le cas échéant, pour réduire les interférences entre les membres du cluster ou avec les périphériques extérieurs au cluster. La stratégie de canaux radio est définie automatiquement sur le mode statique et l'option **Auto** n'est pas disponible pour le champ **Channel** de la page Wireless > Radio.

Reportez-vous à la section Affichage des attributions de canaux et configuration des verrouillages pour obtenir des informations sur les attributions de canaux actuelles et proposées.

ÉTAPE 3 Pour interrompre l'attribution automatique des canaux, cliquez sur **Arrêter**.

Aucun mappage de l'utilisation des canaux ni aucune réattribution de ceux-ci ne sont effectués. Seules les mises à jour manuelles affectent l'attribution des canaux.

Affichage des attributions de canaux et configuration des verrouillages

Lorsque la gestion des canaux est activée, la page affiche le tableau Current Channel Assignations et le tableau Proposed Channel Assignments.

Tableau Current Channel Assignments

Le tableau Current Channel Assignments affiche la liste de tous les périphériques WAP du cluster à configuration de point unique par adresse IP.

Il indique les informations suivantes sur les attributions de canaux actuelles.

- **Location** : emplacement physique du périphérique.
- **IP Address** : adresse IP du point d'accès.
- **Wireless Radio** : adresse MAC de la radio.
- **Band** : bande de diffusion du point d'accès.
- **Channel** : canal radio sur lequel le point d'accès diffuse actuellement.
- **Locked** : force le point d'accès à rester sur le canal actuel.
- **Status** : état de la radio sans fil du périphérique. (Pour les périphériques WAP disposant de plusieurs radios sans fil, chaque radio est indiquée sur une ligne distincte du tableau.) L'état de la radio est soit Up (opérationnel) soit Down (non opérationnel).

Lorsqu'elles sont sélectionnées pour un point d'accès, les stratégies de gestion automatique des canaux ne réattribuent pas les périphériques WAP à un autre canal dans le cadre de la stratégie d'optimisation. Les périphériques WAP dont les canaux sont verrouillés sont considérés comme immuables dans la stratégie de gestion.

Cliquez sur **Enregistrer** pour mettre à jour le paramètre Locked. Le canal des périphériques verrouillés est le même dans le tableau Current Channel Assignments et le tableau Proposed Channel Assignments. Les périphériques verrouillés conservent leurs canaux actuels.

Tableau Proposed Channel Assignments

Le tableau Proposed Channel Assignments affiche les canaux proposés qui seront attribués à chaque périphérique WAP lors de la prochaine mise à jour. Les canaux verrouillés ne sont pas réattribués ; l'optimisation de la distribution des canaux entre les périphériques tient compte du fait que les périphériques verrouillés doivent rester sur leurs canaux actuels. Les périphériques WAP non verrouillés peuvent être attribués à des canaux différents de ceux qu'ils utilisaient auparavant, selon les résultats de la stratégie.

Pour chaque périphérique WAP de la configuration de point unique, le tableau Proposed Channel Assignments indique l'emplacement, l'adresse IP et la radio sans fil, de la même manière que le tableau Current Channel Assignations. Il affiche également le Canal proposé, c'est-à-dire le canal radio auquel le périphérique WAP devrait être réattribué lors de l'application de la stratégie.

Configuration des paramètres avancés

La zone Advanced settings vous permet de personnaliser et de planifier la stratégie de canaux de la configuration de point unique.

Par défaut, les canaux sont réattribués automatiquement toutes les heures, à condition que les interférences puissent être réduites d'au moins 25 pour cent. Les canaux sont réattribués même si le réseau est occupé. Les paramètres par défaut sont conçus pour servir la plupart des scénarios qui vous obligeraient à mettre en œuvre la gestion des canaux.

Vous pouvez modifier les paramètres avancés pour configurer les options suivantes :

- **Change channels if interference is reduced by at least** : pourcentage minimal de réduction des interférences qu'une stratégie proposée doit atteindre pour être appliquée. La valeur par défaut est 75 pour cent. Choisissez le pourcentage souhaité entre 5 et 75 pour cent dans le menu déroulant. L'utilisation de ce paramètre vous permet de définir un seuil de gain d'efficacité relatif à la réattribution des canaux pour éviter une interruption trop fréquente du réseau alors que le gain d'efficacité est minime.

  Par exemple, si les interférences des canaux doivent être réduites de 75 pour cent et que les attributions de canaux proposées permettent de réduire les interférences de seulement 30 pour cent, alors la réattribution n'est pas effectuée. Cependant, si vous réglez le gain minimal sur 25 pour cent et cliquez sur **Enregistrer**, la stratégie de canaux proposée sera mise en œuvre et les canaux seront réattribués selon les besoins.

- **Determine if there is better set of channels every** : calendrier des mises à jour automatiques. Une plage d'intervalles allant de 30 minutes à 6 mois est proposée.

  La valeur par défaut est de 1 heure, ce qui signifie que l'utilisation des canaux est réévaluée et que le plan de canal résultant est appliqué toutes les heures.

Si vous modifiez ces paramètres, cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration active et la configuration initiale.

Voisinage sans fil

La page Wireless Neighborhood affiche jusqu'à 20 périphériques dans la plage de chaque radio sans fil au sein du cluster. (Par exemple, si un périphérique WAP possède deux radios sans fil, 40 périphériques s'affichent pour ce périphérique.) La page Wireless Neighborhood effectue également une distinction entre les membres et les non membres du cluster.

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

- détecter et localiser les périphériques inattendus (ou non autorisés) dans un domaine sans fil, de telle sorte que vous puissiez entreprendre des actions visant à limiter les risques associés ;
- vérifier les attentes en matière de couverture. En évaluant quels périphériques WAP sont visibles et à quelle puissance de signal à partir des autres périphériques, vous pouvez vérifier que le déploiement satisfait vos objectifs de planification ;
- détecter les défaillances. Les modifications inattendues dans le modèle de couverture apparaissent de manière évidente grâce au système de couleurs.

Pour afficher les périphériques de voisinage, sélectionnez **Single Point Setup** > **Wireless Neighborhood** dans le volet de navigation. Pour afficher l'ensemble des périphériques détectés au cours d'une même configuration de point unique, accédez à l'interface Web d'un membre et sélectionnez **Wireless** > **Rogue AP Detection** dans le volet de navigation.

Pour chaque point d'accès voisin, les informations suivantes sont affichées :

- **Display Neighboring APs** : sélectionnez l'une des cases d'option suivantes pour modifier la vue :
  - **In cluster** : affiche uniquement les périphériques WAP voisins qui sont membres du cluster.
  - **Not in cluster** : affiche uniquement les périphériques WAP voisins qui ne sont pas membres du cluster.

  - **Both** : affiche tous les périphériques WAP voisins (membres et non membres du cluster).

- **Cluster** : la liste présente en haut du tableau affiche les adresses IP de l'ensemble des périphériques WAP qui appartiennent au même cluster. (Cette liste est identique à la liste des membres figurant à la page **Single Point Setup** > **Access Points**.)

  S'il n'y a qu'un seul périphérique WAP dans le cluster, une seule colonne d'adresses IP s'affiche, indiquant que le périphérique WAP est groupé avec lui-même.

  Vous pouvez cliquer sur une adresse IP pour afficher plus de détails sur un périphérique WAP particulier.

- **Neighbors** : les périphériques qui sont voisins d'un ou plusieurs périphériques en cluster sont répertoriés dans la colonne de gauche par SSID (nom de réseau).

Un périphérique détecté en tant que voisin peut également être lui-même membre du cluster. Les voisins qui sont aussi des membres de cluster sont toujours affichés en haut de la liste avec une barre épaisse et un indicateur d'emplacement.

Les barres de couleur situées à droite de chaque périphérique WAP dans la liste Neighbors représentent la puissance du signal de chaque périphérique WAP voisin, tel que détecté par le membre de cluster dont l'adresse IP est affichée en haut de la colonne.

La couleur de la barre indique la puissance du signal :

- Barre bleu foncé : une barre bleu foncé et un nombre de puissance de signal élevé (par exemple 50) indiquent une bonne puissance de signal détectée à partir du voisin, comme le voit le périphérique dont l'adresse IP est affichée en haut de cette colonne.
- Barre bleu clair : une barre bleu clair et un nombre de puissance de signal peu élevé (par exemple 20 ou moins) indiquent une puissance de signal moyenne ou faible détectée à partir du voisin, comme le voit le périphérique dont l'adresse IP est affichée en haut de cette colonne.
- Barre blanche : une barre blanche et le nombre 0 indiquent qu'un périphérique voisin détecté par l'un des membres du cluster ne peut pas l'être par le périphérique dont l'adresse IP est affichée en haut de cette colonne.

- Barre gris clair : une barre gris clair et aucun nombre de puissance de signal indiquent qu'aucun signal n'a été détecté à partir du voisin, mais que celui-ci peut avoir été détecté par d'autres membres du cluster.
- Barre gris foncé : une barre gris foncé et aucun nombre de puissance de signal indiquent le périphérique WAP lui-même, correspondant à l'adresse IP affichée au-dessus de lui. Une puissance de signal égale à zéro est affichée, car la propre puissance de signal du périphérique n'est pas mesurée.

Affichage des détails d'un membre du cluster

Pour afficher les détails relatifs à un membre du cluster, cliquez sur l'adresse IP d'un membre en haut de la page.

Les détails suivants du périphérique apparaissent en dessous de la liste Neighbors.

- **SSID** : identificateur d'ensemble de services du point d'accès voisin.
- **MAC Address** : adresse MAC du point d'accès voisin.
- **Channel** : canal sur lequel le point d'accès diffuse actuellement.
- **Rate** : débit, en mégabits par seconde, auquel ce point d'accès transmet actuellement. Le débit actuel est toujours l'un des débits spécifiés dans Supported Rates.
- **Signal** : puissance du signal radio détecté à partir du point d'accès, mesurée en décibels (dB).
- **Beacon Interval** : intervalle de balise utilisé par le point d'accès.
- **Beacon Age** : date et heure de la dernière balise reçue de ce point d'accès.

A

Codes des motifs des messages de désauthentification

Lorsqu'un client se désauthentifie du périphérique WAP, un message est envoyé au journal système. Ce message contient un code de motif pouvant être utile pour déterminer pourquoi le client a été désauthentifié. Vous pouvez afficher les messages du journal en cliquant sur **Status and Statistics > Log Status**.

Le tableau suivant décrit les codes des motifs de désauthentification.

Code de motif	Signification
0	Réservé
1	Motif non spécifié
2	L'authentification précédente n'est plus valide
3	Désauthentification due au fait que la station émettrice quitte ou a quitté l'ensemble de services de base indépendants (IBSS, Independent Basic Service Set) ou l'ESS
4	Désassociation due à l'inactivité
5	Désassociation due au fait que le périphérique WAP n'est pas capable de gérer l'ensemble des stations actuellement associées
6	Trame de classe 2 reçue d'une station non authentifiée
7	Trame de classe 3 reçue d'une station non associée
8	Désassociation due au fait que la station émettrice quitte ou a quitté l'ensemble de services de base (BSS, Basic Service Set)
9	La station qui demande l'association ou la réassociation n'est pas authentifiée avec la station répondante

Code de motif	Signification
10	Désassociation due au fait que les informations figurant dans l'élément de capacité d'alimentation ne sont pas acceptables
11	Désassociation due au fait que les informations figurant dans l'élément des canaux pris en charge ne sont pas acceptables
12	Désassociation due à la gestion des transitions BSS
13	Élément non valide, par exemple un élément défini dans cette norme et dont le contenu ne satisfait pas aux spécifications figurant dans la clause 8
14	Échec du code d'intégrité du message (MIC, Message Integrity Code)
15	Délai d'expiration de connexion en quatre étapes
16	Délai d'expiration de connexion de clé de groupe
17	Élément de connexion en quatre étapes différent de la trame Demande/Réponse de la sonde/Balise d'association ou de réassociation
18	Chiffrement de groupe non valide
19	Chiffrement par paire non valide
20	AKMP non valide
21	Version RSNE non prise en charge
22	Capacités RSNE non valides
23	Échec de l'authentification IEEE 802.1X
24	Suite de chiffrement rejetée en raison de la stratégie de sécurité

B

Pour en savoir plus

Cisco fournit une gamme étendue de ressources pour vous aider, ainsi que votre client, à profiter de tous les avantages du système Points d'accès Cisco WAP121 et WAP321.

Assistance	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Assistance et ressources 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
Téléchargement de microprogrammes Cisco Small Business	www.cisco.com/go/smallbizfirmware Sélectionnez un lien pour télécharger les microprogrammes des produits 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	
Guide de démarrage rapide et Guide d'administration du point d'accès Cisco Small Business WAP121 et WAP321 Wireless-N avec PoE	http://www.cisco.com/go/100_wap_resources ou http://www.cisco.com/go/300_wap_resources
Cisco Small Business	
Cisco Partner Central pour les petites entreprises (connexion partenaire obligatoire)	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.cisco.com/smb