

Configuration du point d'accès OfficeExtend de la gamme Aironet 600

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Instructions de configuration](#)

[Présentation de la solution Office Extend](#)

[Consignes de configuration du pare-feu](#)

[Étapes de configuration d'Office Extend AP-600](#)

[Paramètres de configuration WLAN et LAN distant](#)

[Paramètres de sécurité WLAN](#)

[Filtrage MAC](#)

[Nombre d'utilisateurs pris en charge](#)

[Gestion et paramètres des canaux](#)

[Mises En Garde Additionnelles](#)

[Configuration du point d'accès OEAP-600](#)

[Installation matérielle du point d'accès OEAP-600](#)

[Dépannage de l'OEAP-600](#)

[Comment déboguer les problèmes d'association client](#)

[Comment interpréter le journal des événements](#)

[Lorsque la connexion Internet ne semble pas fiable](#)

[Commandes de débogage supplémentaires](#)

[Problèmes connus/Avertissement](#)

[Informations connexes](#)

Introduction

Ce document fournit des informations sur la configuration requise pour configurer un contrôleur de réseau local sans fil (WLAN) Cisco pour une utilisation avec le point d'accès OfficeExtend (OEAP) de la gamme Cisco Aironet® 600. Le point d'accès OEAP de la gamme Cisco Aironet 600 prend en charge le fonctionnement en mode partagé et dispose d'installations qui nécessitent une configuration via le contrôleur WLAN et de fonctionnalités qui peuvent être configurées localement par l'utilisateur final. Ce document fournit également des informations sur les configurations nécessaires pour une connexion correcte et des jeux de fonctions pris en charge.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur le point d'accès OfficeExtend (OEAP) de la gamme Cisco Aironet 600.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

Instructions de configuration

- Le protocole OEAP de la gamme Cisco Aironet 600 est pris en charge sur les contrôleurs suivants : Cisco 5508, WiSM-2 et Cisco 2504.
- La première version de contrôleur prenant en charge le protocole OEAP de la gamme Cisco Aironet 600 est 7.0.116.0
- Les interfaces de gestion du contrôleur doivent se trouver sur un réseau IP routable.
- La configuration du pare-feu d'entreprise doit être modifiée pour autoriser le trafic avec les numéros de port UDP 5246 et 5247.

Présentation de la solution Office Extend

- Un utilisateur reçoit un point d'accès (AP) avec l'adresse IP du contrôleur d'entreprise, ou l'utilisateur peut entrer l'adresse IP du contrôleur à partir de l'écran de configuration (pages HTML de configuration).
- L'utilisateur connecte le point d'accès à son routeur domestique.
- Le point d'accès obtient une adresse IP de son routeur domestique, joint le contrôleur amorcé et crée un tunnel sécurisé.
- La gamme Cisco Aironet 600 OEAP annonce ensuite le SSID d'entreprise, qui étend les

mêmes méthodes et services de sécurité sur le WAN jusqu'au domicile de l'utilisateur.

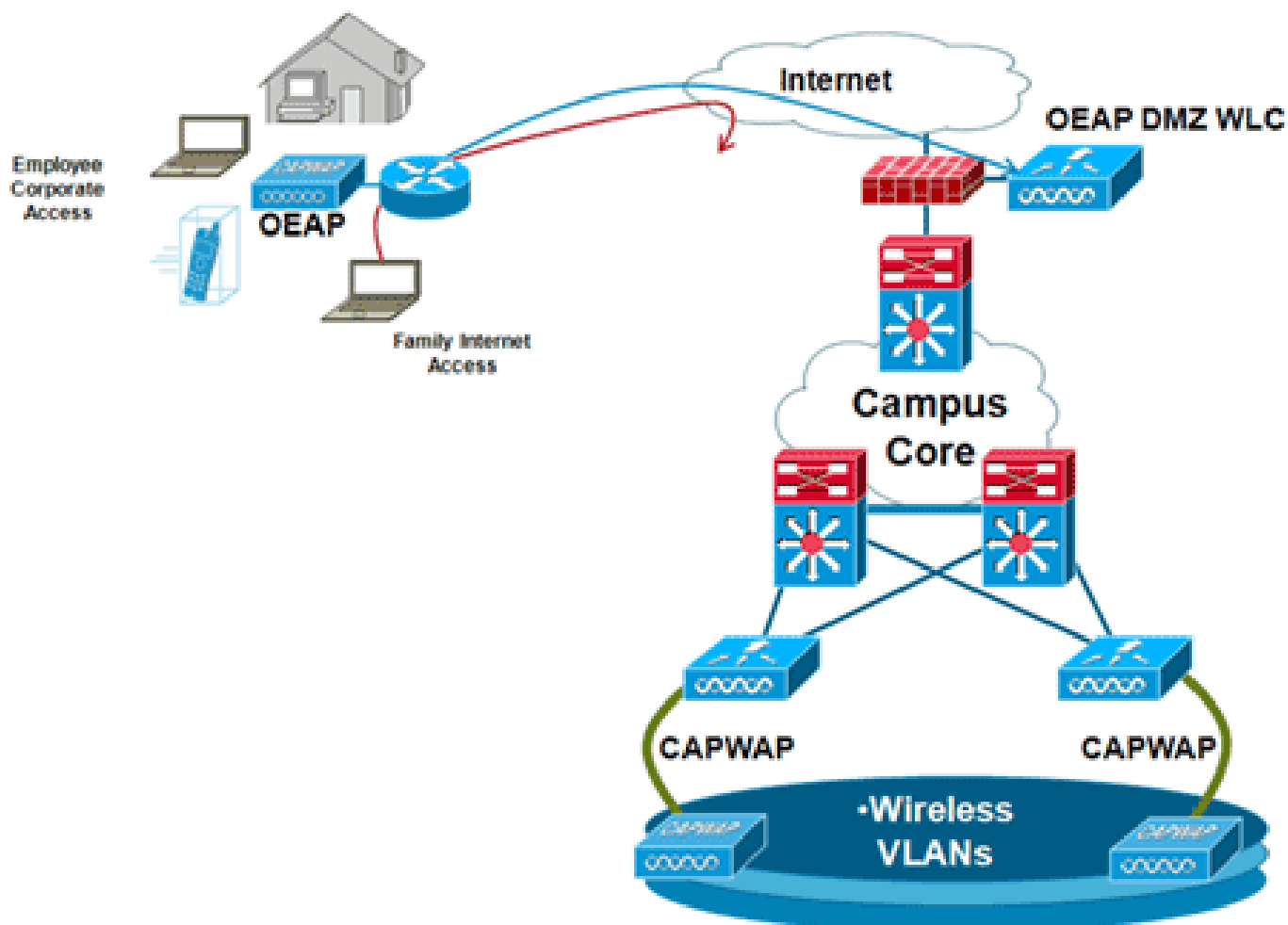
- Si le LAN distant est configuré, un port filaire sur le point d'accès est renvoyé au contrôleur par tunnel.
- L'utilisateur peut alors activer en plus un SSID local pour un usage personnel.

Consignes de configuration du pare-feu

La configuration générale sur le pare-feu est de permettre le contrôle CAPWAP et les numéros de port de gestion CAPWAP à travers le pare-feu. Le contrôleur OEAP de la gamme Cisco Aironet 600 peut être placé dans la zone DMZ.

Remarque : les ports UDP 5246 et 5247 doivent être ouverts sur le pare-feu entre le contrôleur WLAN et le point d'accès OEAP Cisco Aironet 600.

Ce schéma montre un contrôleur OEAP de la gamme Cisco Aironet 600 sur la DMZ :



Voici un exemple de configuration de pare-feu :

```
interface Ethernet0/0
 nameif outside
```

```
security-level 0
ip address X.X.X.X 255.255.255.224
```

!--- X.X.X.X represents a public IP address

```
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.2 255.255.255.0
!
access-list Outside extended permit udp any host X.X.X.Y eq 5246
```

!--- Public reachable IP of corporate controller

```
access-list Outside extended permit udp any host X.X.X.Y eq 5247
```

!--- Public reachable IP of corporate controller

```
access-list Outside extended permit icmp any any
!
global (outside) 1 interface
nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255
access-group Outside in interface outside
```

Afin de transmettre l'adresse IP interne du gestionnaire d'AP au point d'accès OfficeExtend dans le cadre du paquet de réponse de détection CAPWAPP, l'administrateur du contrôleur doit s'assurer que la NAT est activée dans l'interface du gestionnaire d'AP et que l'adresse IP NAT correcte est envoyée au point d'accès.

Remarque : par défaut, le WLC répondra uniquement avec l'adresse IP NAT pendant la détection AP lorsque NAT est activé. Si des AP existent à l'intérieur et à l'extérieur de la passerelle NAT, émettez cette commande afin de configurer le WLC pour répondre avec l'adresse IP NAT et l'adresse IP de gestion non-NAT (interne) :

```
<#root>
```

```
config network ap-discovery nat-ip-only disable
```

Remarque : ceci est seulement requis si le WLC a une adresse IP NAT.

Ce schéma montre que la NAT est activée, en supposant que le WLC a une adresse IP NAT :

The screenshot shows the Cisco Controller configuration page for the 'management' interface. The page is divided into several sections: General Information, Configuration, NAT Address, Interface Address, Physical Information, and DHCP Information. The 'Enable NAT Address' checkbox is highlighted with a red circle.

General Information	
Interface Name	management
MAC Address	00:24:97:69:52:8f

Configuration	
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	<input type="text" value="0"/>

NAT Address	
Enable NAT Address	<input checked="" type="checkbox"/>
NAT IP Address	<input type="text" value="X.X.X.Y"/>

Interface Address	
VLAN Identifier	<input type="text" value="0"/>
IP Address	<input type="text" value="172.16.1.25"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="172.16.1.2"/>

Physical Information	
The interface is attached to a LAG.	
Enable Dynamic AP Management	<input checked="" type="checkbox"/>

DHCP Information	
Primary DHCP Server	<input type="text" value="172.20.225.153"/>
Secondary DHCP Server	<input type="text" value="0.0.0.0"/>

Remarque : cette configuration n'est pas requise dans le contrôleur, à condition qu'il soit configuré avec une adresse IP routable sur Internet et non derrière un pare-feu.

Étapes de configuration d'Office Extend AP-600

Le point d'accès OEAP de la gamme Cisco Aironet 600 se connecte au WLC en tant que point d'accès en mode local.

Remarque : les modes Monitor, H-REAP, Sniffer, Rogue Detection, Bridge et SE-Connect ne sont pas pris en charge sur la gamme 600 et ne sont pas configurables.

Remarque : la fonctionnalité OEAP de la gamme Cisco Aironet 600 dans les points d'accès des gammes 1040, 1130, 1140 et 3502i nécessite la configuration des points d'accès pour le protocole Hybrid REAP (H-REAP) et la définition du sous-mode pour le point d'accès sur le protocole Cisco

Aironet 600. Cette opération n'est pas effectuée avec la gamme 600, car elle utilise le mode local et ne peut pas être modifiée.

Le filtrage MAC peut être utilisé dans l'authentification AP lors du processus de jonction initial pour empêcher les unités OEAP non autorisées de la gamme Cisco Aironet 600 de rejoindre le contrôleur. Cette image montre où vous activez le filtrage MAC et configurez les stratégies de sécurité des points d'accès :

The screenshot shows the Cisco Aironet 600 configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Security menu with options: AAA (General, RADIUS, Authentication, Accounting, Fallback, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies), Local EAP, Priority Order, Certificate, and Access Control Lists. The main content area is titled 'AP Policies' and 'Policy Configuration'. It lists several settings with checkboxes: 'Accept Self Signed Certificate (SSC)' (checked), 'Accept Manufactured Installed Certificate (MIC)' (checked), 'Accept Local Significant Certificate (LSC)' (unchecked), 'Authorize MIC APs against auth-list or AAA' (checked), and 'Authorize LSC APs against auth-list' (unchecked). Below this is the 'AP Authorization List' section, which includes a search box for MAC addresses and a table with columns for MAC Address, Certificate Type, and SHA1 Key Hash. The table contains two entries for MAC address 00:01:36:1f:e4:60, both with Certificate Type SSC and the same SHA1 Key Hash.

MAC Address	Certificate Type	SHA1 Key Hash
00:01:36:1f:e4:59	SSC	4073c833036f05f68acbc9329f67182102623c7f
00:01:36:1f:e4:60	SSC	4073c833036f05f68acbc9329f67182102623c7f

L'adresse MAC Ethernet (et non l'adresse MAC radio) est entrée ici. En outre, si vous saisissez l'adresse MAC dans un serveur Radius, vous devez utiliser des minuscules. Vous pouvez examiner le journal des événements AP pour obtenir des informations sur la façon de découvrir l'adresse MAC Ethernet (plus sur ce sujet plus tard).

Paramètres de configuration WLAN et LAN distant

Il y a un port LAN distant physique (port jaune #4) sur le point d'accès OEAP de la gamme Cisco Aironet 600. Il est très similaire à un WLAN dans la façon dont il est configuré. Cependant, parce qu'il n'est pas sans fil et un port LAN filaire à l'arrière du point d'accès, il est appelé et géré comme un port LAN distant.

Bien qu'il n'y ait qu'un seul port physique sur le périphérique, jusqu'à quatre clients filaires peuvent être connectés si un concentrateur ou un commutateur est utilisé.

Remarque : la limite de client LAN distant prend en charge la connexion d'un commutateur ou d'un concentrateur au port LAN distant pour plusieurs périphériques ou la connexion directe à un téléphone IP Cisco connecté à ce port.

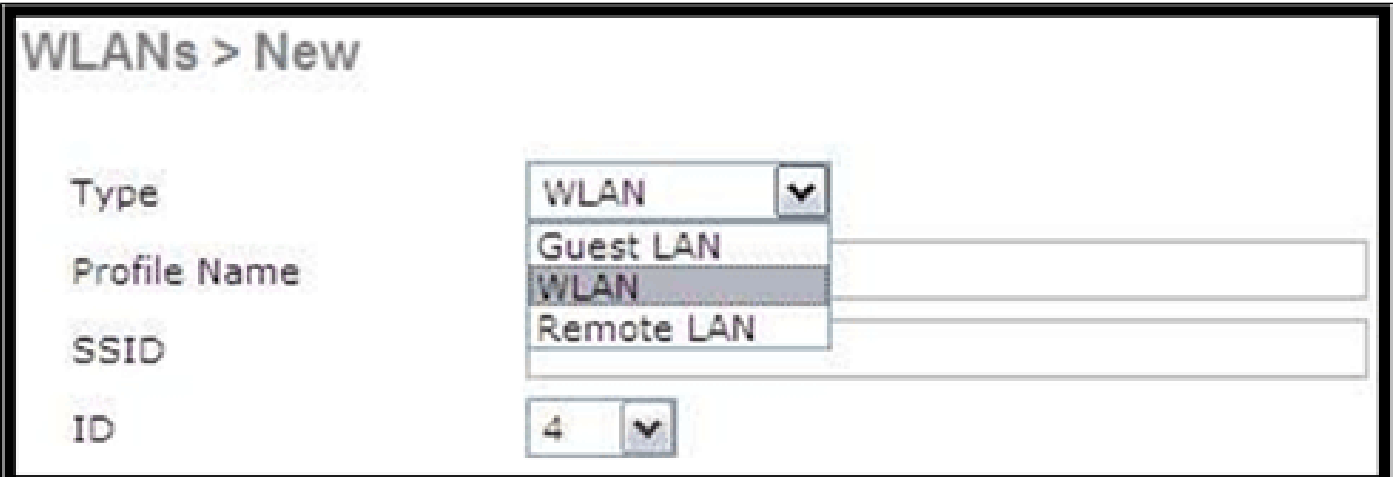
Remarque : seuls les quatre premiers périphériques peuvent se connecter jusqu'à ce qu'un des périphériques soit inactif pendant plus d'une minute. Si vous utilisez l'authentification 802.1x, il peut y avoir des problèmes lors de la tentative d'utilisation de plusieurs clients sur le port filaire.

Remarque : ce nombre n'affecte pas la limite de quinze imposée pour les WLAN du contrôleur.

Un réseau local distant est configuré de la même manière qu'un réseau local sans fil et un réseau local invité configurés sur le contrôleur.

Les WLAN sont des profils de sécurité sans fil. Il s'agit des profils utilisés par votre réseau d'entreprise. La gamme Cisco Aironet 600 OEAP prend en charge au maximum deux WLAN et un LAN distant.

Un réseau local distant est similaire à un réseau local sans fil, sauf qu'il est mappé au port filaire situé à l'arrière du point d'accès (port #4 en jaune), comme illustré dans cette image :



WLANs > New

Type: WLAN

Profile Name: Guest LAN, WLAN, Remote LAN

SSID: [Empty]

ID: 4

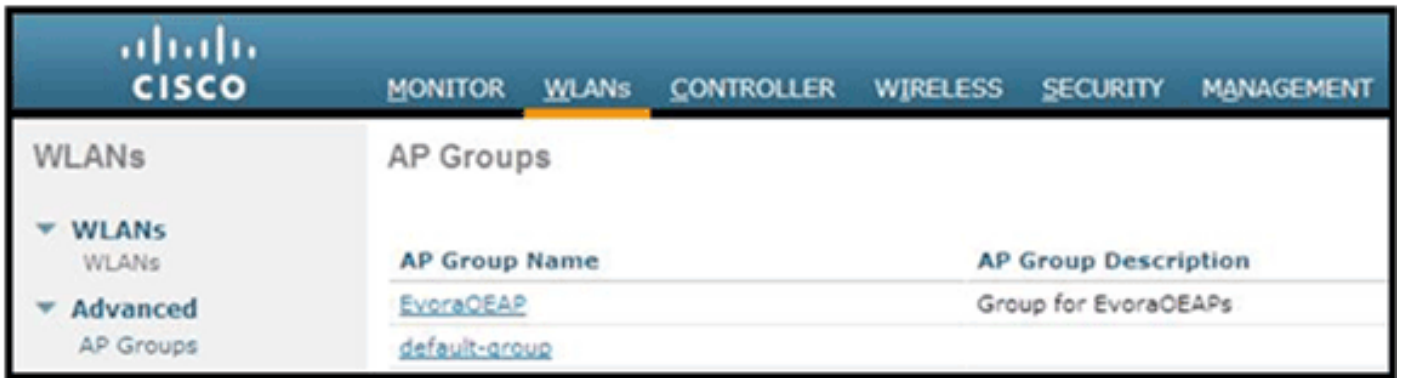
Remarque : si vous avez plus de deux WLAN ou plus d'un LAN distant, tous doivent être placés dans un groupe AP.

Cette image montre où les WLAN et le LAN distant sont configurés :

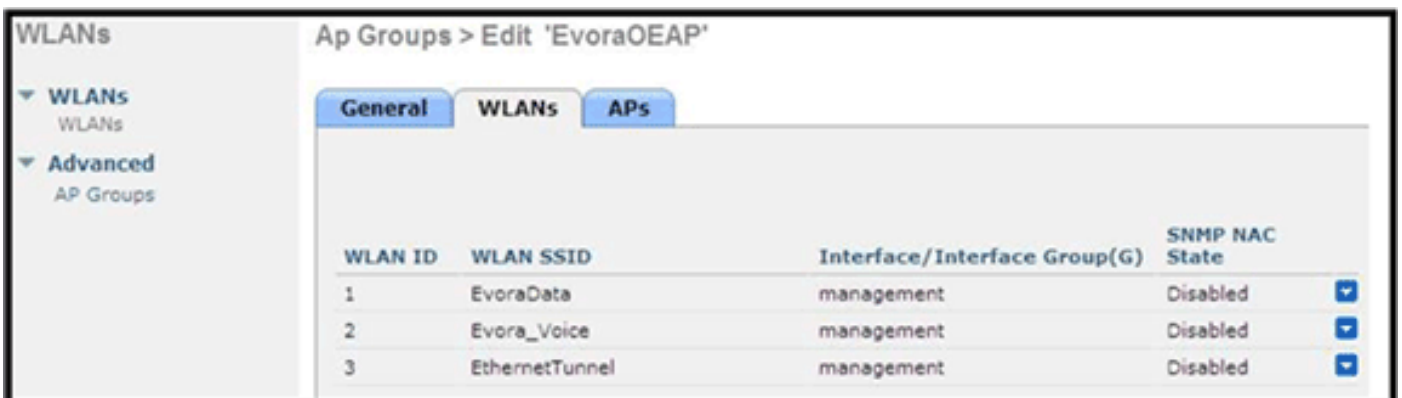


WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	EvoraData	EvoraData	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	EvoraVoice	Evora_Voice	Enabled	[WPA2][Auth(802.1X)]
3	Remote LAN	EthernetTunnel	---	Enabled	None

Cette image présente un exemple de nom de groupe OEAP :

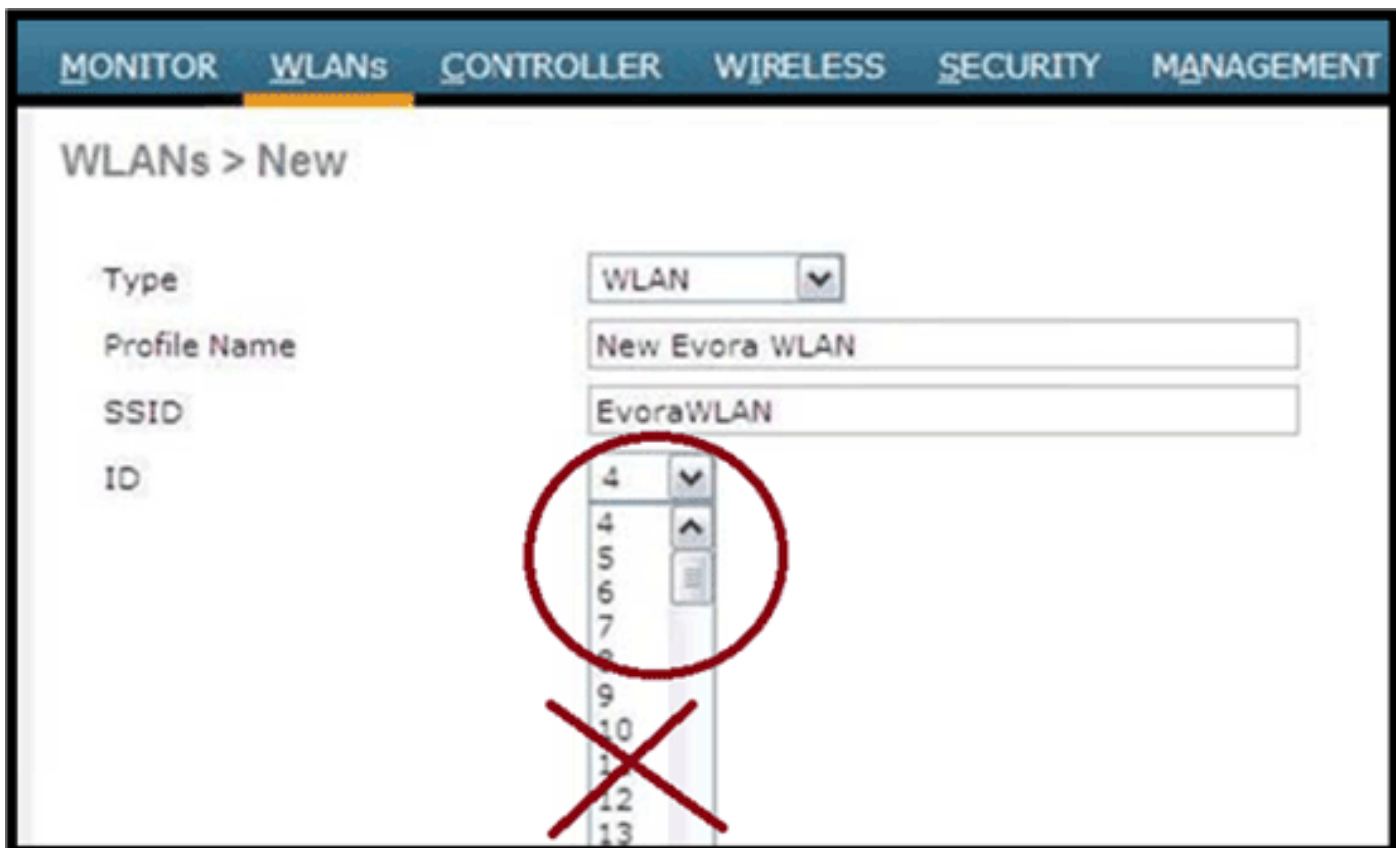


Cette image présente une configuration SSID WLAN et LAN :



Si le protocole OEAP de la gamme Cisco Aironet 600 est entré dans un groupe AP, les mêmes limites de deux WLAN et d'un LAN distant s'appliquent à la configuration du groupe AP. En outre, si le point d'accès OEAP de la gamme Cisco Aironet 600 se trouve dans le groupe par défaut, ce qui signifie qu'il ne se trouve pas dans un groupe AP défini, les ID WLAN/LAN distant doivent être définis à une valeur inférieure à l'ID 8, car ce produit ne prend pas en charge les jeux d'ID supérieurs.

Conservez les jeux d'ID inférieurs à 8, comme illustré dans cette image :



Remarque : si des WLAN ou des LAN distants supplémentaires sont créés dans le but de modifier les WLAN ou les LAN distants utilisés par l'OEAP de la gamme Cisco Aironet 600, désactivez les WLAN ou les LAN distants actuels que vous supprimez avant d'activer les nouveaux WLAN ou les LAN distants sur la gamme 600. Si plusieurs réseaux locaux distants sont activés pour un groupe de points d'accès, désactivez tous les réseaux locaux distants, puis activez-en un seul.

Si plus de deux WLAN sont activés pour un groupe AP, désactivez tous les WLAN, puis n'activez que deux d'entre eux.

Paramètres de sécurité WLAN

Lors de la définition du paramètre de sécurité dans le WLAN, certains éléments spécifiques ne sont pas pris en charge sur la gamme 600.

Pour la sécurité de couche 2, seules ces options sont prises en charge pour le point d'accès OEAP de la gamme Cisco Aironet 600 :

- Aucune
- WPA+WPA2
- Le WEP statique peut également être utilisé, mais pas pour les débits de données .11n.

WLANs > Edit

General

Security

QoS

Advanced

Layer 2

Layer 3

AAA Servers

Layer 2 Security ⁶

WPA+WPA2

None

WPA+WPA2

WPA+WPA2 Parameters: 802.1X

Static WEP

Static-WEP + 802.1X

CKIP

WPA Policy

WPA Encryption

WPA2 Policy

WPA2 Encryption

Auth Key Mgmt



AES

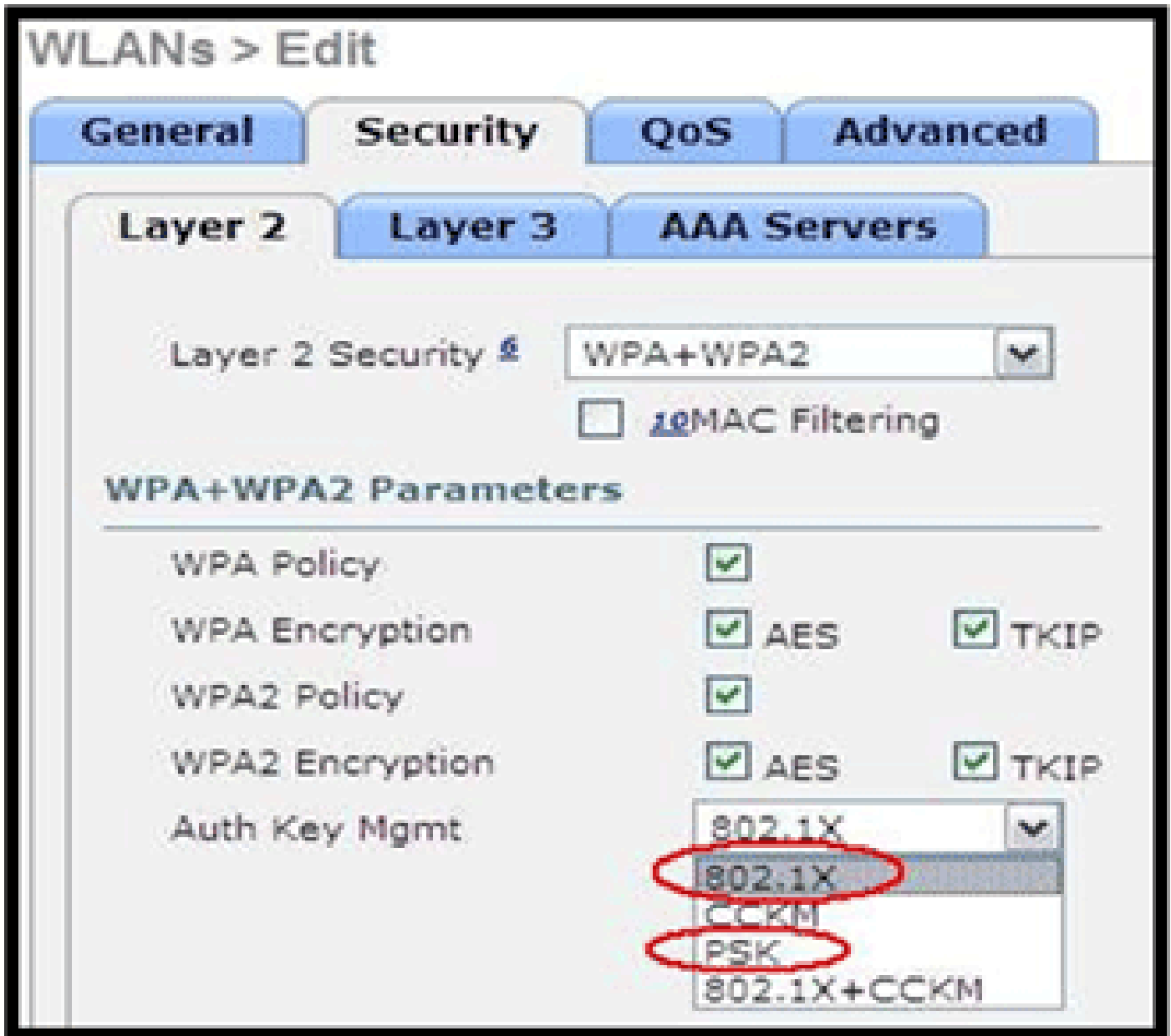


TKIP

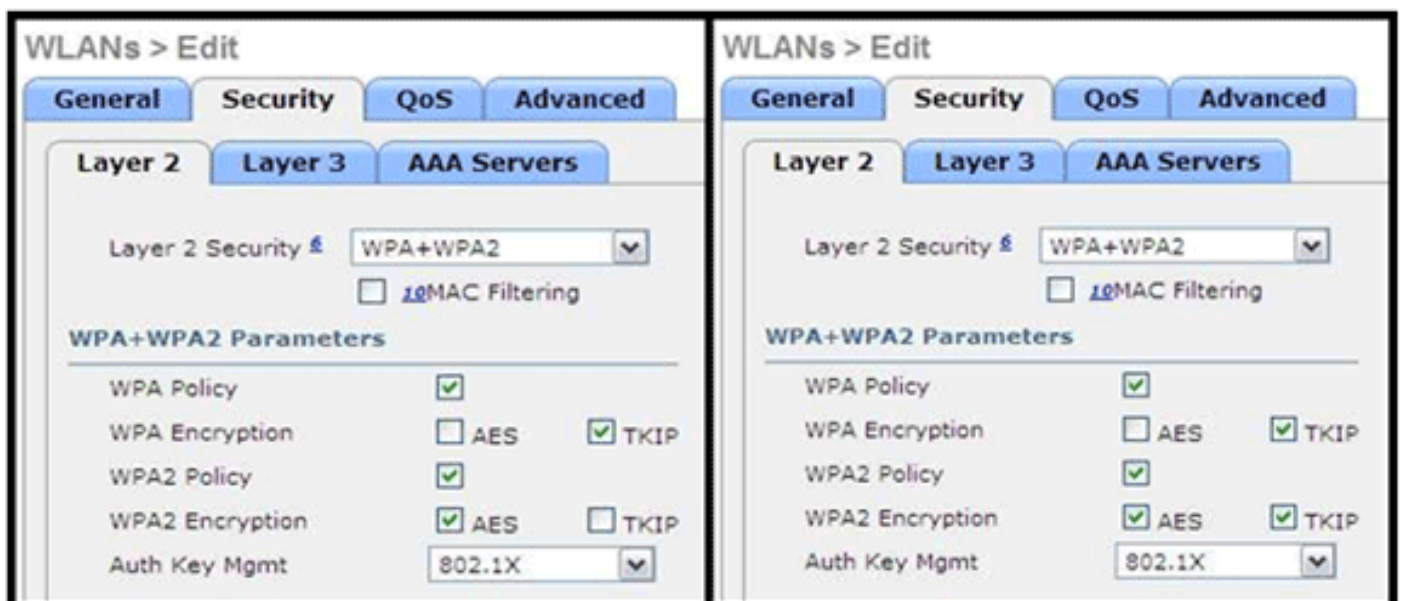
802.1X

Remarque : seuls 802.1x ou PSK doivent être sélectionnés.

Les paramètres de cryptage de sécurité doivent être identiques pour WPA et WPA2 pour TKIP et AES, comme illustré dans cette image :

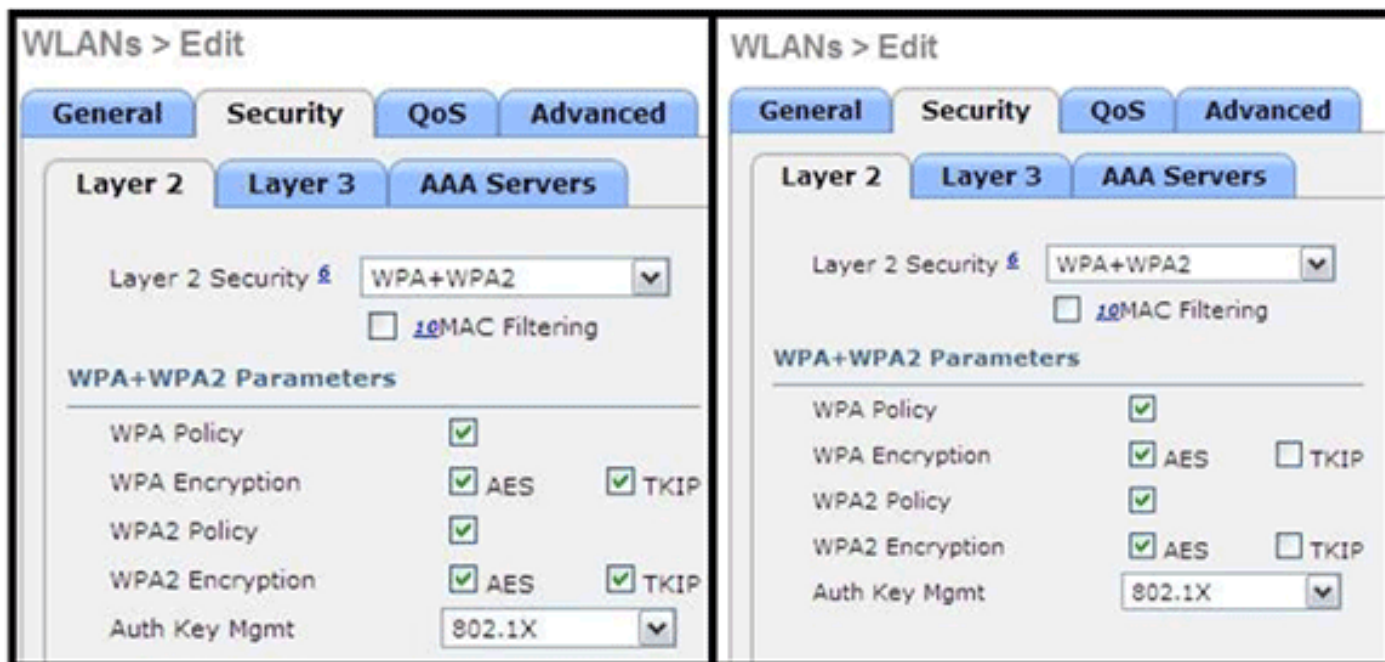


Ces images fournissent des exemples de paramètres incompatibles pour TKIP et AES :



Remarque : sachez que les paramètres de sécurité autorisent les fonctionnalités non prises en charge.

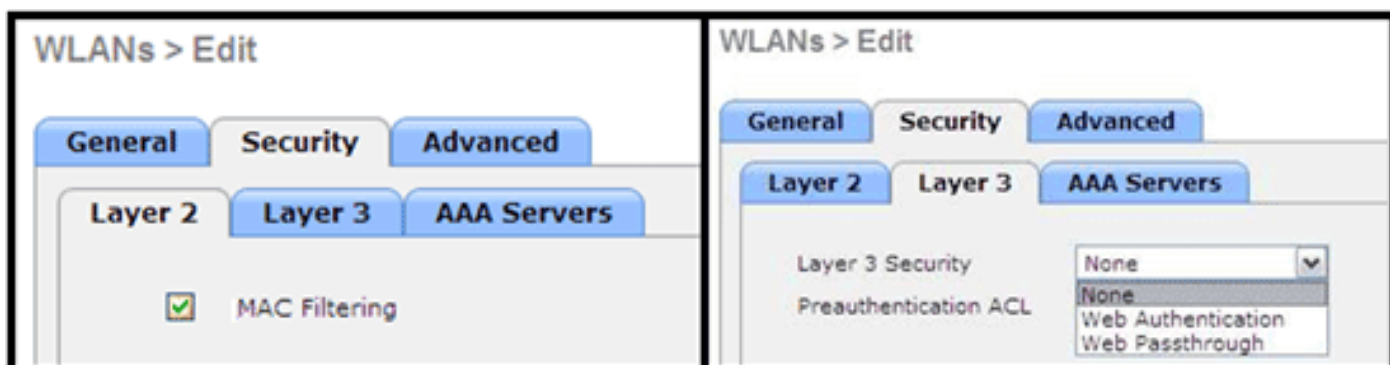
Ces images fournissent des exemples de paramètres compatibles :



Filtrage MAC

Les paramètres de sécurité peuvent être laissés ouverts, définis pour le filtrage MAC ou définis pour l'authentification Web. La valeur par défaut est d'utiliser le filtrage MAC.

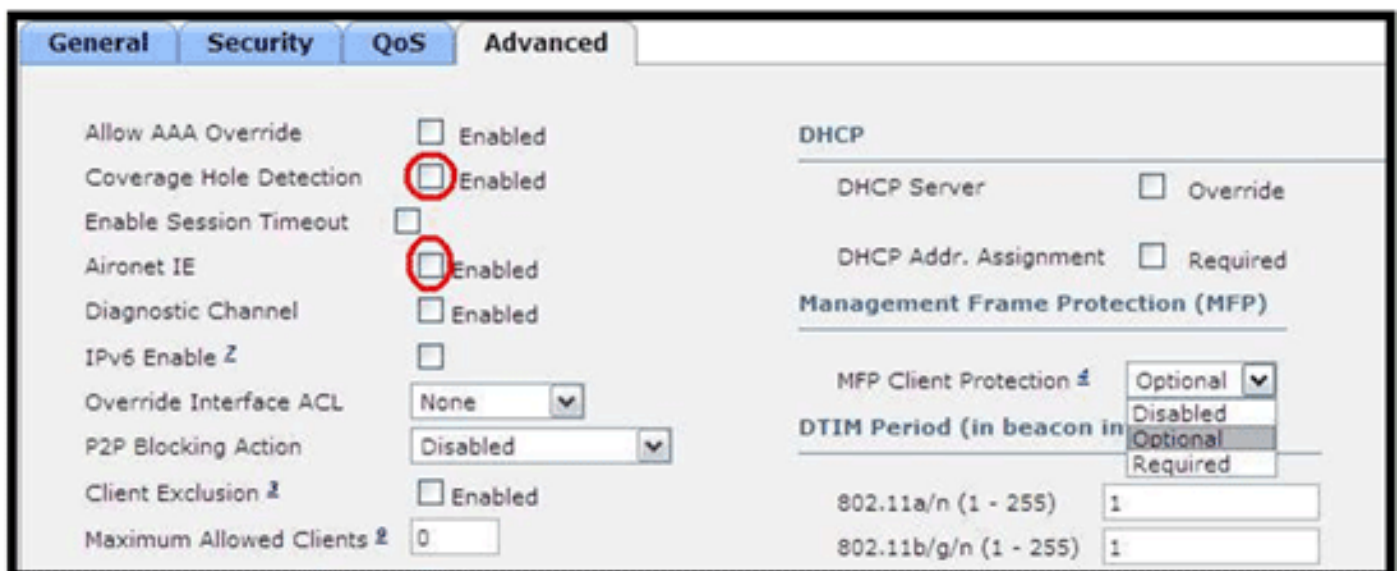
Cette image présente le filtrage MAC des couches 2 et 3 :



Les paramètres QoS sont gérés :

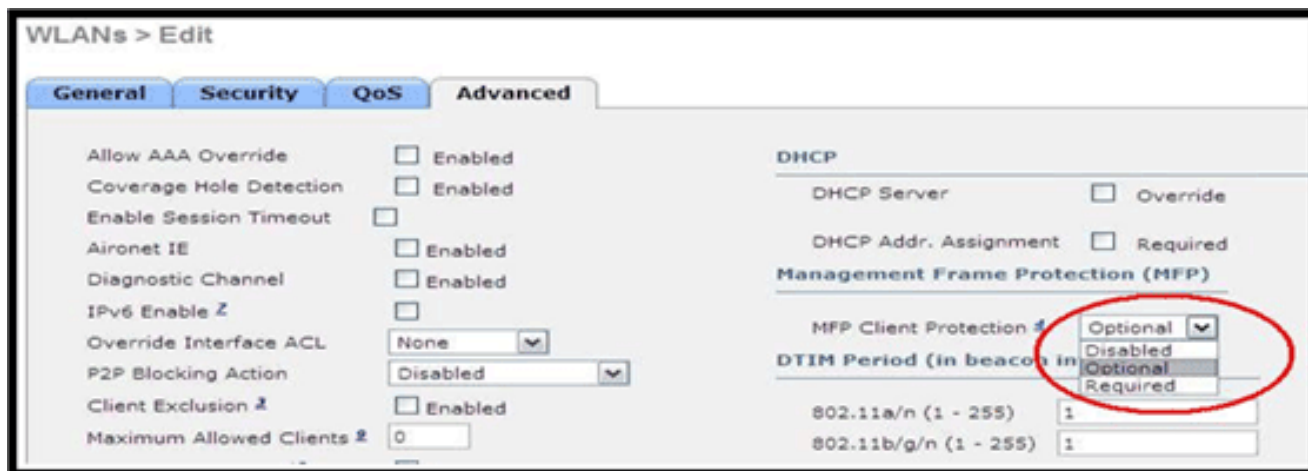


Les paramètres avancés doivent également être gérés :

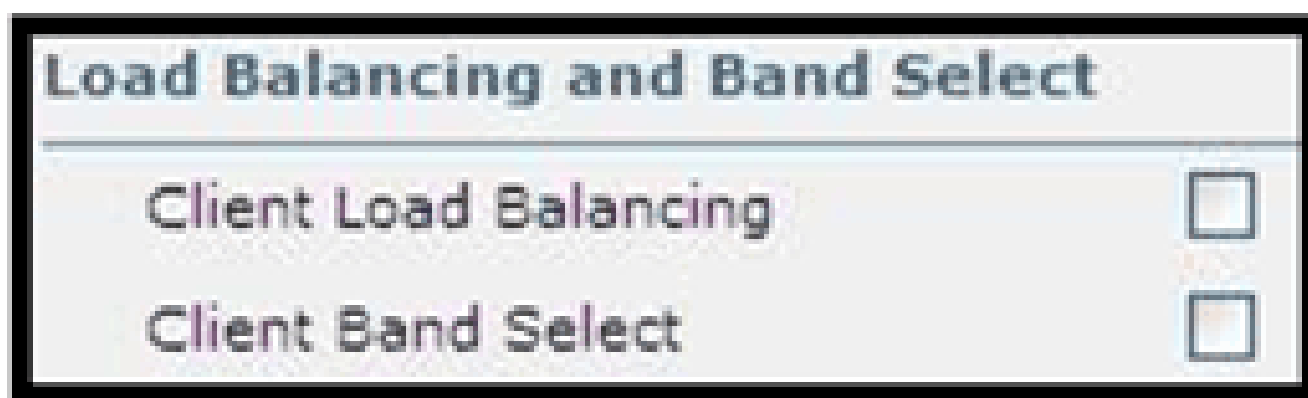


Remarques :

- La détection des trous de couverture ne doit pas être activée.
- Les éléments d'information (IE) Aironet ne doivent pas être activés car ils ne sont pas utilisés.
- La protection de trame de gestion (MFP) n'est pas non plus prise en charge et doit être désactivée ou configurée comme étant facultative, comme illustré dans cette image :



- L'équilibrage de charge client et la sélection de bande client ne sont pas pris en charge et ne doivent pas être activés :



Nombre d'utilisateurs pris en charge

Seuls quinze utilisateurs sont autorisés à se connecter à tout moment sur les WLAN du contrôleur WLAN fournis sur la gamme 600. Un seizième utilisateur ne peut pas s'authentifier tant que l'un des premiers clients ne se désauthentifie pas ou qu'un délai d'attente n'a pas été atteint sur le contrôleur.

Remarque : ce nombre est cumulé sur les WLAN des contrôleurs de la gamme 600.

Par exemple, si deux WLAN de contrôleur sont configurés et qu'il y a quinze utilisateurs sur l'un des WLAN, aucun utilisateur ne pourra se connecter à l'autre WLAN sur la gamme 600 à ce moment-là. Cette limite ne s'applique pas aux WLAN privés locaux que l'utilisateur final configure sur la gamme 600 conçue pour un usage personnel et les clients connectés sur ces WLAN privés ou sur les ports câblés n'affectent pas ces limites.

Gestion et paramètres des canaux

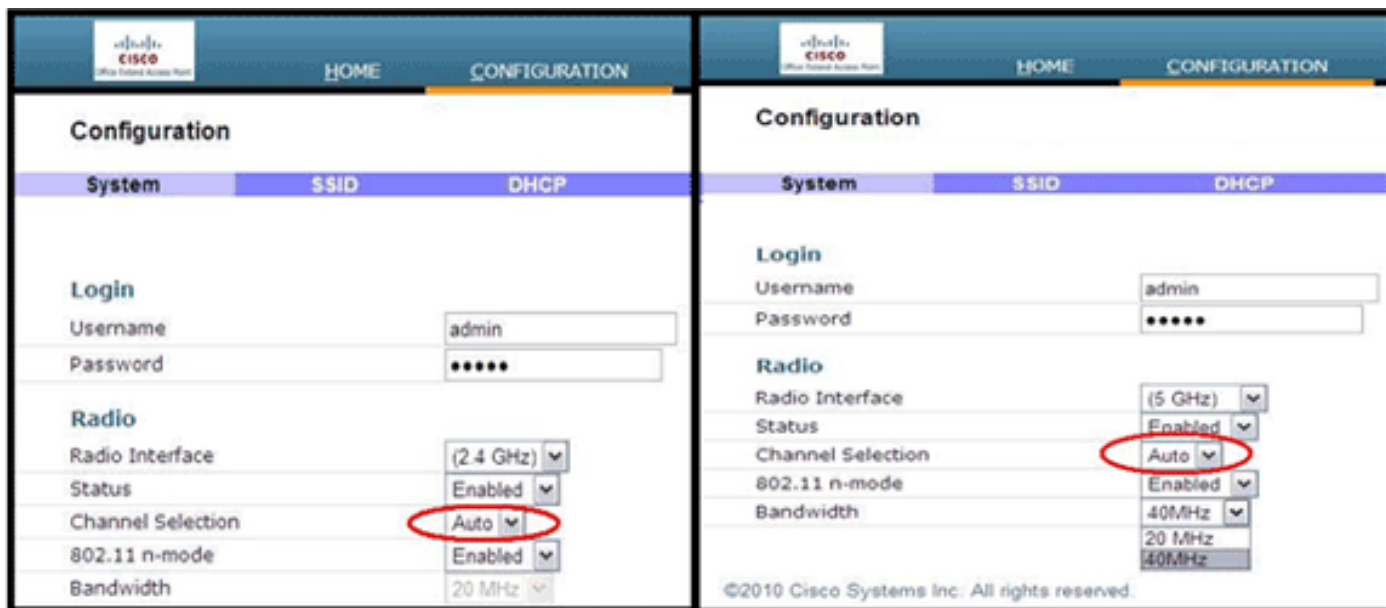
Les radios de la gamme 600 sont contrôlées via l'interface utilisateur graphique locale de la gamme 600 et non via le contrôleur de réseau local sans fil.

Toute tentative de contrôle du canal de spectre, de la puissance ou de la désactivation des radios via le contrôleur n'aura aucun effet sur la gamme 600.

La gamme 600 scanne et sélectionne des canaux pour 2,4 GHz et 5 GHz au démarrage, à condition que les paramètres par défaut de l'interface utilisateur graphique locale soient conservés par défaut dans les deux spectres.

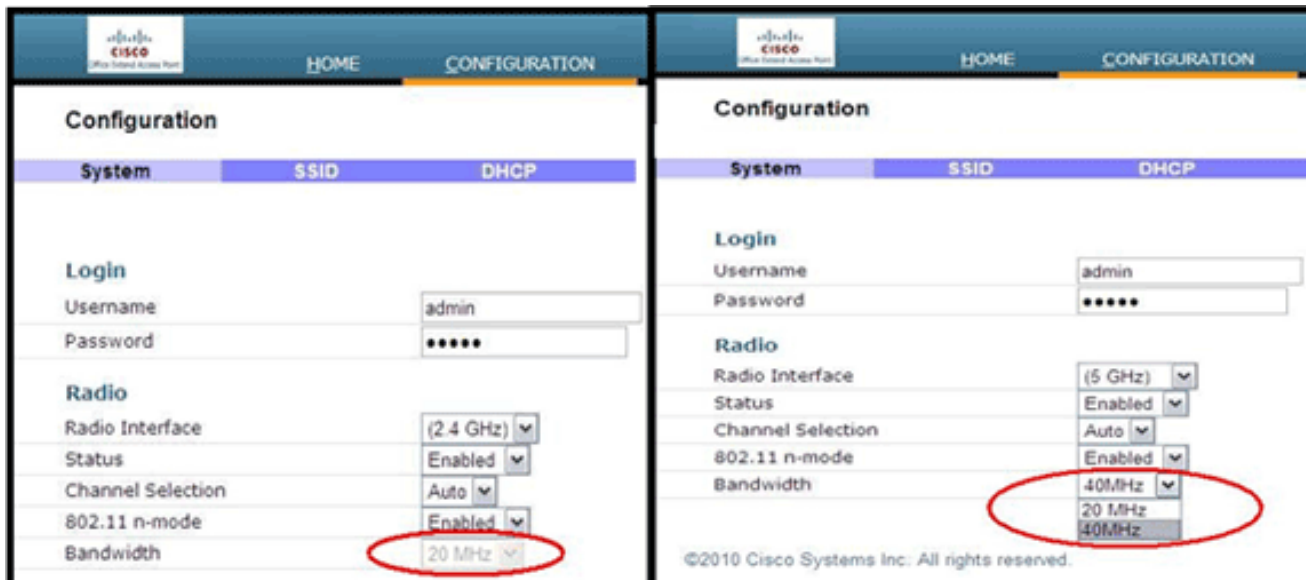
Remarque : si l'utilisateur désactive une ou les deux radios localement (cette radio est également désactivée pour l'accès d'entreprise), comme indiqué précédemment, RRM et des fonctionnalités avancées telles que le moniteur, H-REAP, l'analyseur dépassent les capacités du point d'accès OEAP de la gamme Cisco Aironet 600, qui est destiné à une utilisation à domicile et en télétravail.

La sélection de canal et la bande passante pour 5 GHz sont configurées ici sur l'interface utilisateur graphique locale du point d'accès OEAP de la gamme Cisco Aironet 600.



Remarques :

- Les paramètres 20 et 40 MHz sont disponibles pour 5 GHz.
- 2,4 GHz 40 MHz de large n'est pas pris en charge et fixé à 20 MHz.
- La largeur 40 MHz (liaison de canaux) n'est pas prise en charge dans 2,4 GHz.



Mises En Garde Additionnelles

La gamme Cisco Aironet 600 OEAP est conçue pour les déploiements à point d'accès unique. Par conséquent, l'itinérance des clients entre les gammes 600 n'est pas prise en charge.

Remarque : la désactivation de la norme 802.11a/n ou 802.11b/g/n sur le contrôleur peut ne pas désactiver ces spectres sur le point d'accès OEAP de la gamme Cisco Aironet 600, car le SSID local peut toujours fonctionner.

L'utilisateur final dispose d'un contrôle actif/désactivé sur les radios à l'intérieur du point d'accès OEAP Cisco Aironet 600.



Prise en charge 802.1x sur le port filaire

Dans cette version initiale, 802.1x est uniquement pris en charge sur l'interface de ligne de commande (CLI).

Remarque : la prise en charge GUI n'a pas encore été ajoutée.

Il s'agit du port filaire (port #4 en jaune) situé à l'arrière du point d'accès OEAP de la gamme Cisco Aironet 600 et relié au réseau local distant (voir la section précédente sur la configuration du réseau local distant).

À tout moment, vous pouvez utiliser la commande show pour afficher la configuration actuelle du

réseau local distant :

```
<#root>
```

```
show remote-lan <remote-lan-id>
```

Pour modifier la configuration du réseau local distant, vous devez d'abord la désactiver :

```
<#root>
```

```
remote-lan disable <remote-lan-id>
```

Activez l'authentification 802.1X pour le réseau local distant :

```
<#root>
```

```
config remote-lan security 802.1X enable <remote-lan-id>
```

Vous pouvez l'annuler à l'aide de cette commande :

```
<#root>
```

```
config remote-lan security 802.1X disable <remote-lan-id>
```

Pour le réseau local distant, « Encryption » est toujours « None » (comme affiché dans show remote-lan) et n'est pas configurable.

Si vous voulez utiliser l'EAP local (dans le contrôleur) comme serveur d'authentification :

```
<#root>
```

```
config remote-lan local-auth enable <profile-name> <remote-lan-id>
```

Où le `profil` est défini soit par l'interface graphique du contrôleur (Sécurité > EAP local) ou par l'interface de ligne de commande (config local-auth). Reportez-vous au guide du contrôleur pour plus de détails sur cette commande.

Vous pouvez l'annuler à l'aide de cette commande :

```
<#root>
```

```
config remote-lan local-auth disable <remote-lan-id>
```

Ou, si vous utilisez un serveur d'authentification AAA externe :

- config remote-lan radius_server auth add/delete <remote-lan-id> <server-id>
- config remote-lan radius_server auth enable/disable <remote-lan-id>

Où le serveur est configuré via l'interface graphique du contrôleur (Sécurité > RADIUS > Authentification) ou l'interface de ligne de commande (config radius auth). Reportez-vous au guide du contrôleur pour plus d'informations sur cette commande.

Une fois la configuration terminée, activez le réseau local distant :

```
<#root>
```

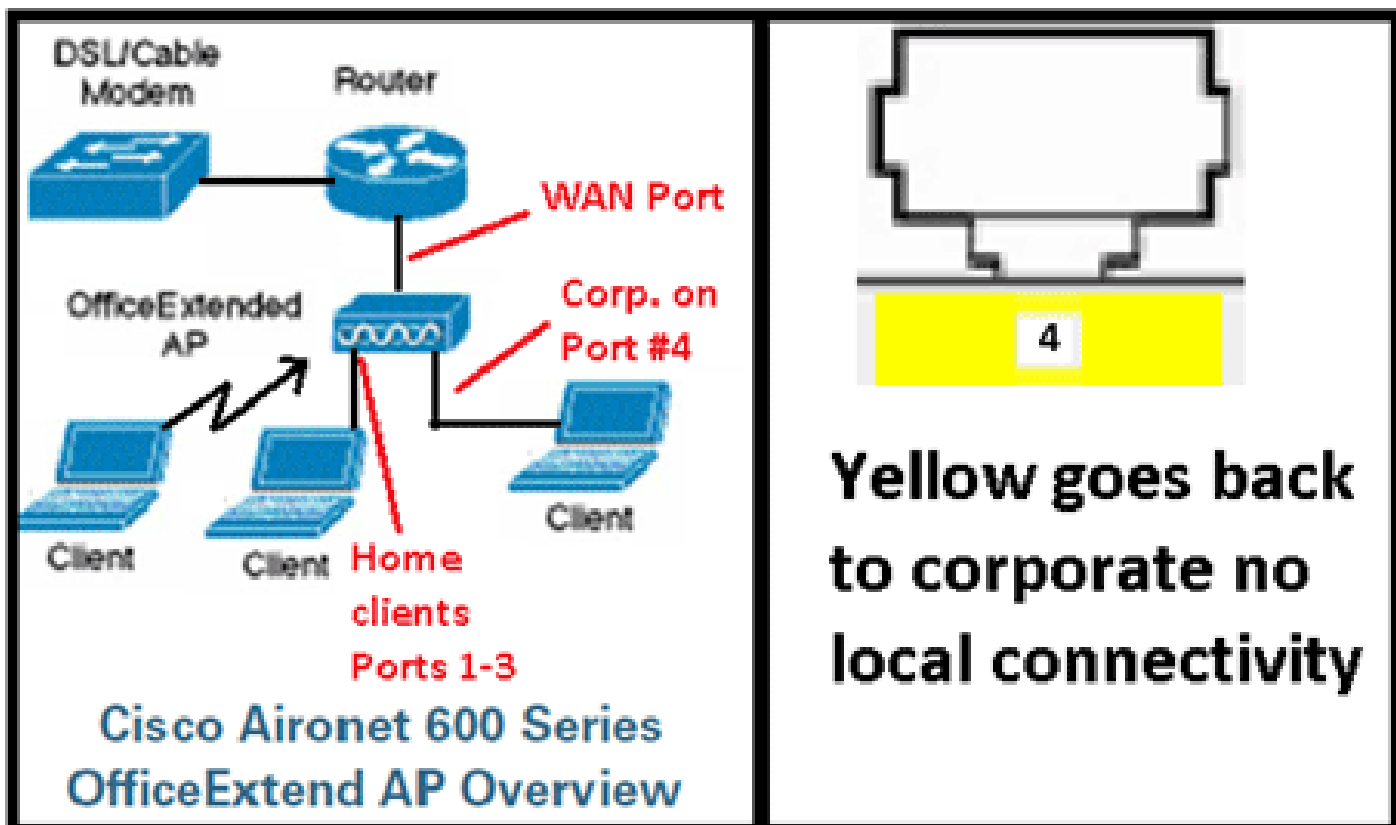
```
config remote-lan enable <remote-lan-id>
```

Utilisez la commande show remote-lan <remote-lan-id> afin de vérifier votre paramètre.

Pour le client LAN distant, vous devez activer l'authentification 802.1X et configurer en conséquence. Reportez-vous au guide de l'utilisateur du périphérique.

Configuration du point d'accès OEAP-600

Cette image présente le schéma de câblage du point d'accès OEAP de la gamme Cisco Aironet 600 :

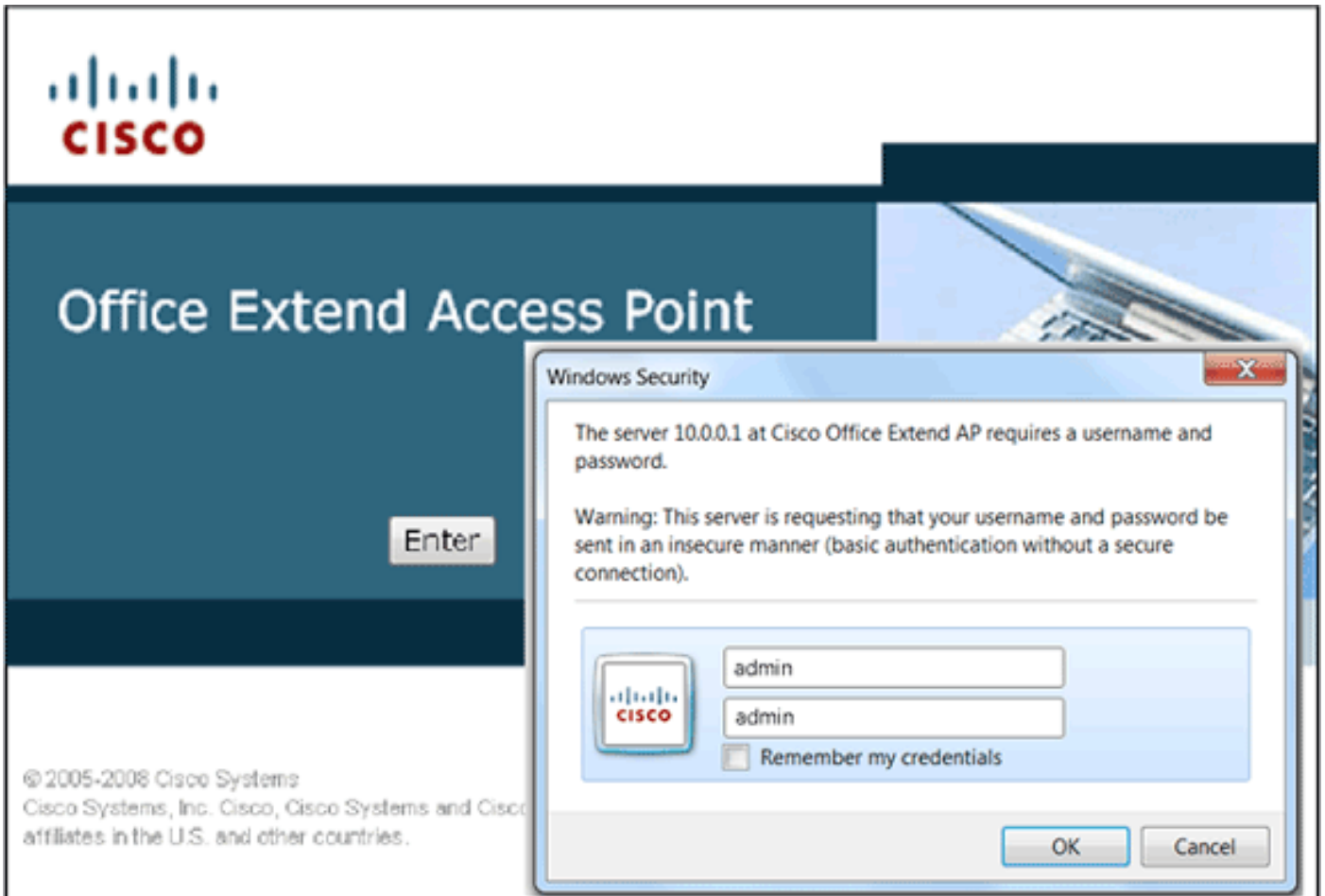


L'étendue DHCP par défaut du point d'accès OEAP de la gamme Cisco Aironet 600 est 10.0.0.x. Vous pouvez donc accéder au point d'accès sur les ports 1 à 3 en utilisant l'adresse 10.0.0.1. Le nom d'utilisateur et le mot de passe par défaut sont admin.

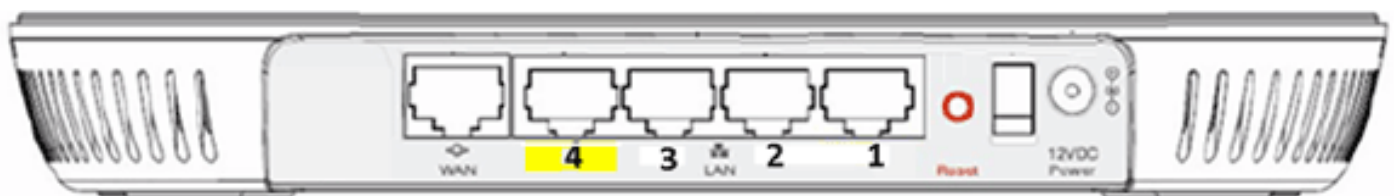
Remarque : ce paramètre est différent des AP1040, 1130, 1140 et 3502i qui utilisaient Cisco comme nom d'utilisateur et mot de passe.

Si les radios sont activées et qu'un SSID personnel a déjà été configuré, vous pouvez accéder à l'écran de configuration sans fil. Sinon, vous devez utiliser les ports Ethernet locaux 1 à 3.

Pour vous connecter, le nom d'utilisateur et le mot de passe par défaut sont admin.



Remarque : le port jaune #4 n'est pas actif pour une utilisation locale. Si un réseau local distant est configuré sur le contrôleur, ce port effectue un retour en tunnel après que le point d'accès ait rejoint le contrôleur. Pour accéder au périphérique, utilisez localement les ports 1 à 3 :



Une fois que vous avez accédé au périphérique, l'écran d'état d'accueil s'affiche. Cet écran fournit des statistiques radio et MAC. Si les radios n'ont pas été configurées, l'écran de configuration permet à l'utilisateur d'activer les radios, de définir les canaux et les modes, de configurer les SSID locaux et d'activer les paramètres WLAN.

Configuration Apply

System **SSID** **DHCP** **WAN**

Login

Username:

Password:

Radio

Radio Interface: ⓘ Select Each Radio and Configure Independently

Status:

Channel Selection:

802.11 n-mode: ⓘ 802.11n is not supported with TKIP-only WPA Encryption

Bandwidth:

L'écran SSID permet à l'utilisateur de configurer le réseau WLAN personnel. Le SSID radio d'entreprise et les paramètres de sécurité sont configurés et poussés vers le bas à partir du contrôleur (après que vous ayez configuré le WAN avec l'IP du contrôleur), et une jonction réussie s'est produite.

Cette image présente une configuration de filtrage MAC local SSID :

Configuration Apply

System **SSID** **DHCP** **WAN**

Personal Network

Band Selection: ⓘ Select Each Radio and Configure SSID Individually

Enabled:

Broadcast:

SSID: ⓘ Personal SSID should be different from Corporate SSID

MAC Filter

Enabled:

Allowed MAC Addresses: e.g. 00:1D:E0:34:E2:1F

<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Une fois que l'utilisateur a configuré le SSID personnel, l'écran ci-dessous permet à l'utilisateur de configurer la sécurité sur le SSID domestique privé, d'activer les radios et de configurer le filtrage MAC si nécessaire. Si le réseau personnel utilise des débits 802.11n, il est recommandé que l'utilisateur choisisse un type d'authentification, un type de cryptage et une phrase de passe activant WPA2-PSK et AES.

Remarque : ces paramètres SSID sont différents des paramètres d'entreprise si l'utilisateur décide de désactiver l'une des radios ou les deux (elles sont également désactivées pour une utilisation en entreprise).

Les utilisateurs qui ont accès localement aux paramètres de contrôle d'administration contrôlent les fonctions principales telles que l'activation/la désactivation radio, à moins que le périphérique ne soit protégé par mot de passe et configuré par l'administrateur. Par conséquent, veuillez à ne pas désactiver les deux radios, car cela peut entraîner une perte de connectivité même si le périphérique parvient à se connecter au contrôleur.

Cette image présente les paramètres de sécurité du système :

Security	
WPA-PSK	Disabled ▾
WPA2-PSK	Enabled ▾
WEP Encryption	Disabled ▾
WPA Encryption	AES ▾
WPA passphrase	••••• Click here to display
Network Key 1	
Network Key 2	
Network Key 3	
Network Key 4	
Current Network Key	2 ▾

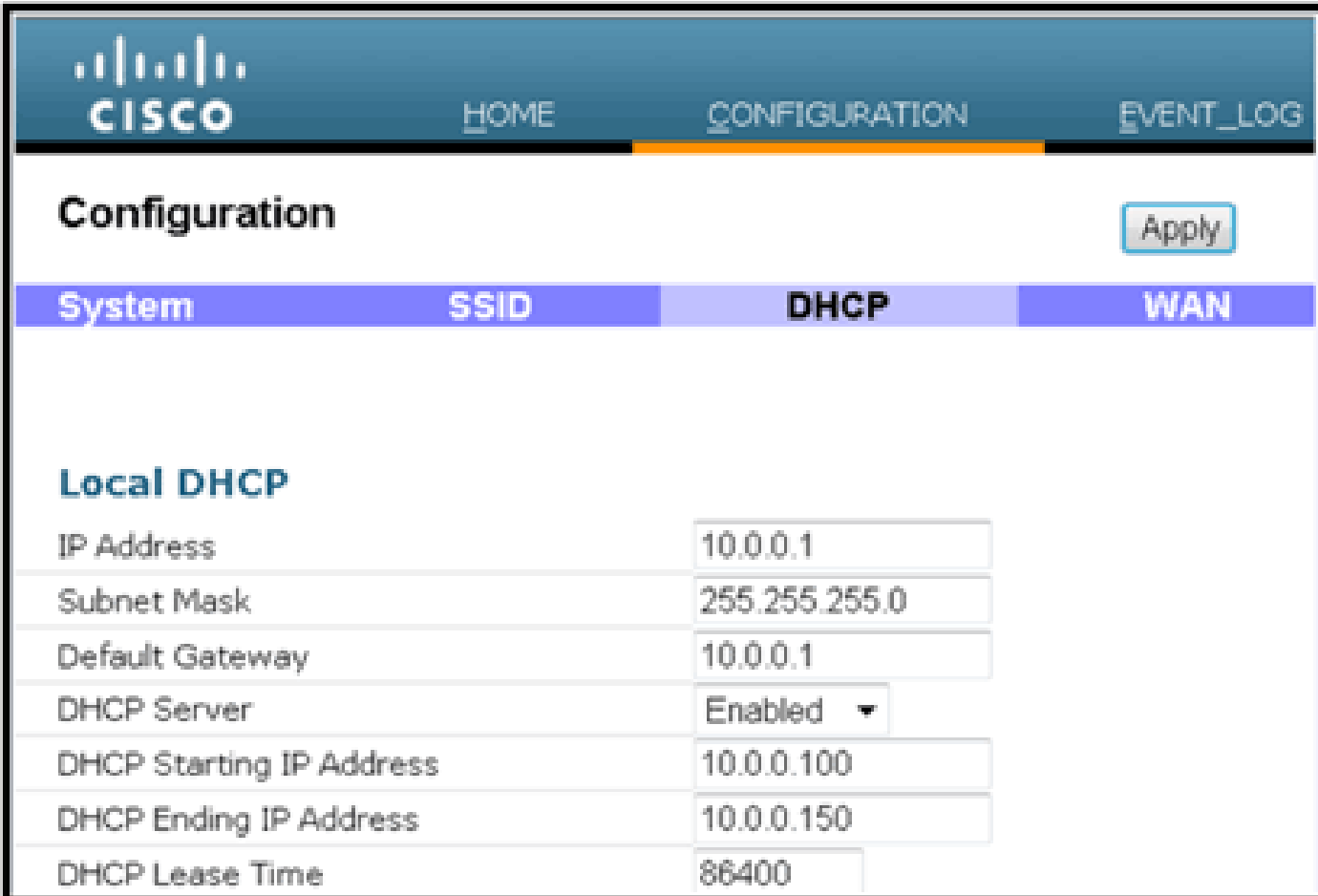
Le télétravailleur à domicile doit installer le point d'accès OEAP de la gamme Cisco Aironet 600 derrière un routeur domestique, car ce produit n'est pas conçu pour remplacer la fonctionnalité d'un routeur domestique. En effet, la version actuelle de ce produit ne prend pas en charge le pare-feu, le protocole PPPoE ou le transfert de port. Ce sont des fonctionnalités que les clients s'attendent à trouver dans un routeur domestique.

Bien que ce produit puisse fonctionner sans routeur domestique, il est recommandé de ne pas le positionner de cette manière pour les raisons indiquées. Il peut également y avoir des problèmes de compatibilité lors de la connexion directe à certains modems.

Étant donné que la plupart des routeurs domestiques ont une étendue DHCP dans la plage 192.168.x.x, ce périphérique a une étendue DHCP par défaut de 10.0.0.x et est configurable.

Si le routeur domestique utilise 10.0.0.x, vous devez configurer le point d'accès OEAP de la gamme Cisco Aironet 600 pour utiliser une adresse IP 192.168.1.x ou compatible afin d'éviter les conflits de réseau.

Cette image montre une configuration d'étendue DHCP :



The screenshot shows the Cisco Aironet 600 configuration interface. At the top, there is a navigation bar with the Cisco logo and three tabs: HOME, CONFIGURATION (which is selected), and EVENT_LOG. Below the navigation bar, the word "Configuration" is displayed in a large font, with an "Apply" button to its right. A horizontal menu below "Configuration" has four items: System, SSID, DHCP (which is highlighted), and WAN. Under the "Local DHCP" section, there is a table of configuration parameters:

Parameter	Value
IP Address	10.0.0.1
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.1
DHCP Server	Enabled
DHCP Starting IP Address	10.0.0.100
DHCP Ending IP Address	10.0.0.150
DHCP Lease Time	86400

Attention : si le point d'accès OEAP de la gamme Cisco Aironet 600 n'est pas préparé ou configuré par l'administrateur informatique, l'utilisateur doit entrer l'adresse IP du contrôleur d'entreprise (voir ci-dessous) pour que le point d'accès puisse rejoindre le contrôleur. Après une jonction réussie, le point d'accès doit télécharger la dernière image du contrôleur et les paramètres de configuration tels que les paramètres WLAN d'entreprise. En outre, s'ils sont configurés, les paramètres LAN à distance sont configurés sur le port filaire #4 à l'arrière du point d'accès OEAP de la gamme Cisco Aironet 600.

S'il ne se connecte pas, vérifiez que l'adresse IP du contrôleur est accessible via Internet. Si le filtrage MAC est activé, vérifiez que l'adresse MAC est correctement entrée dans le contrôleur.

Cette image montre l'adresse IP du contrôleur OEAP de la gamme Cisco Aironet 600 :

CISCO HOME CONFIGURATION EVENT_LOG

Configuration

Apply

System SSID DHCP **WAN**

Controller

This is where you enter the IP address of the DMZ OEAP controller

IP Address **YYYY**

Uplink IP Configuration

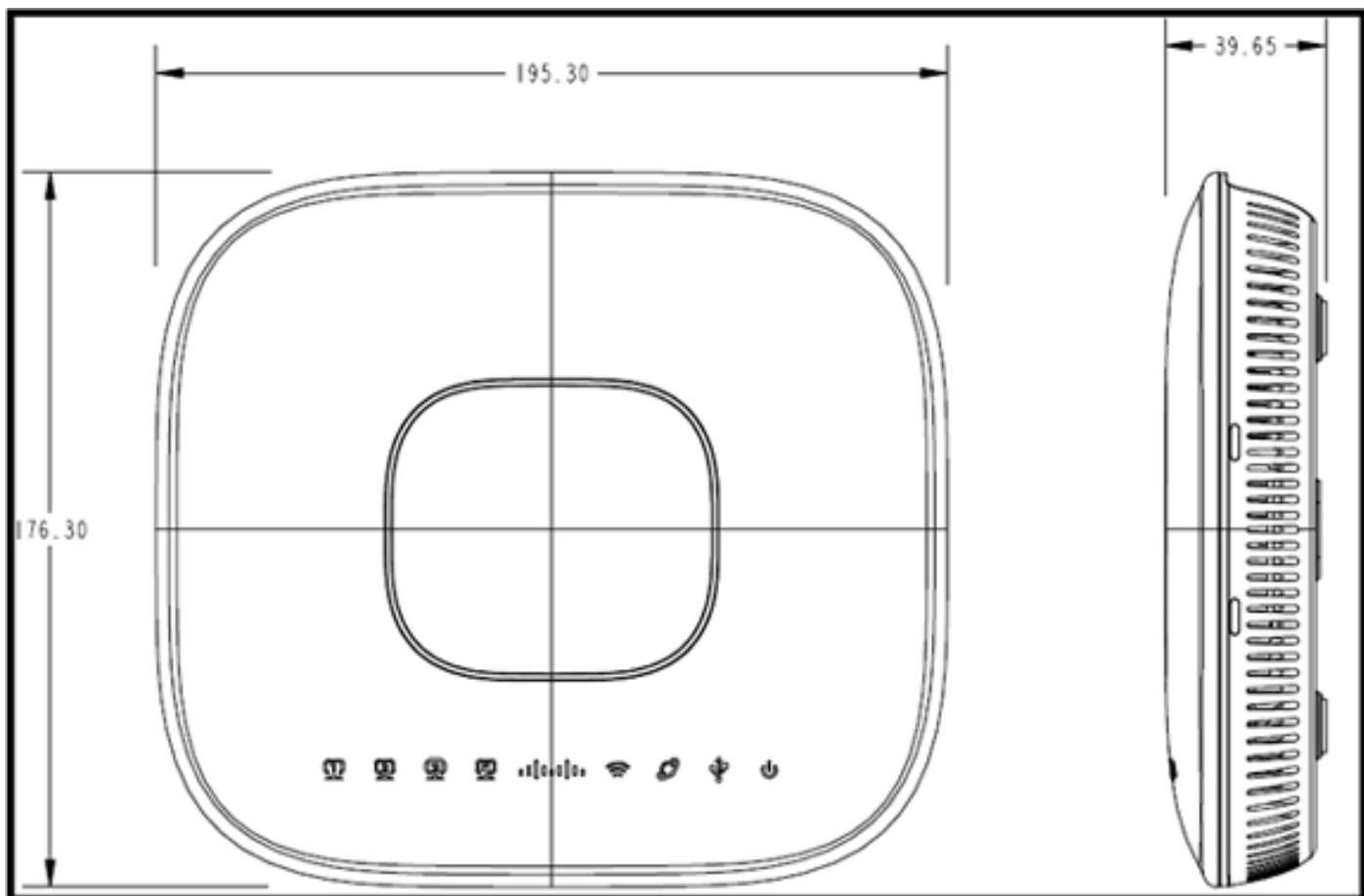
Example IP

Static IP

Domain Name	gateway.2wire.net
IP Address	192.168.1.68
Subnet Mask :	255.255.255.0
Default Gateway	192.168.1.254
DNS Server	192.168.1.254

Installation matérielle du point d'accès OEAP-600

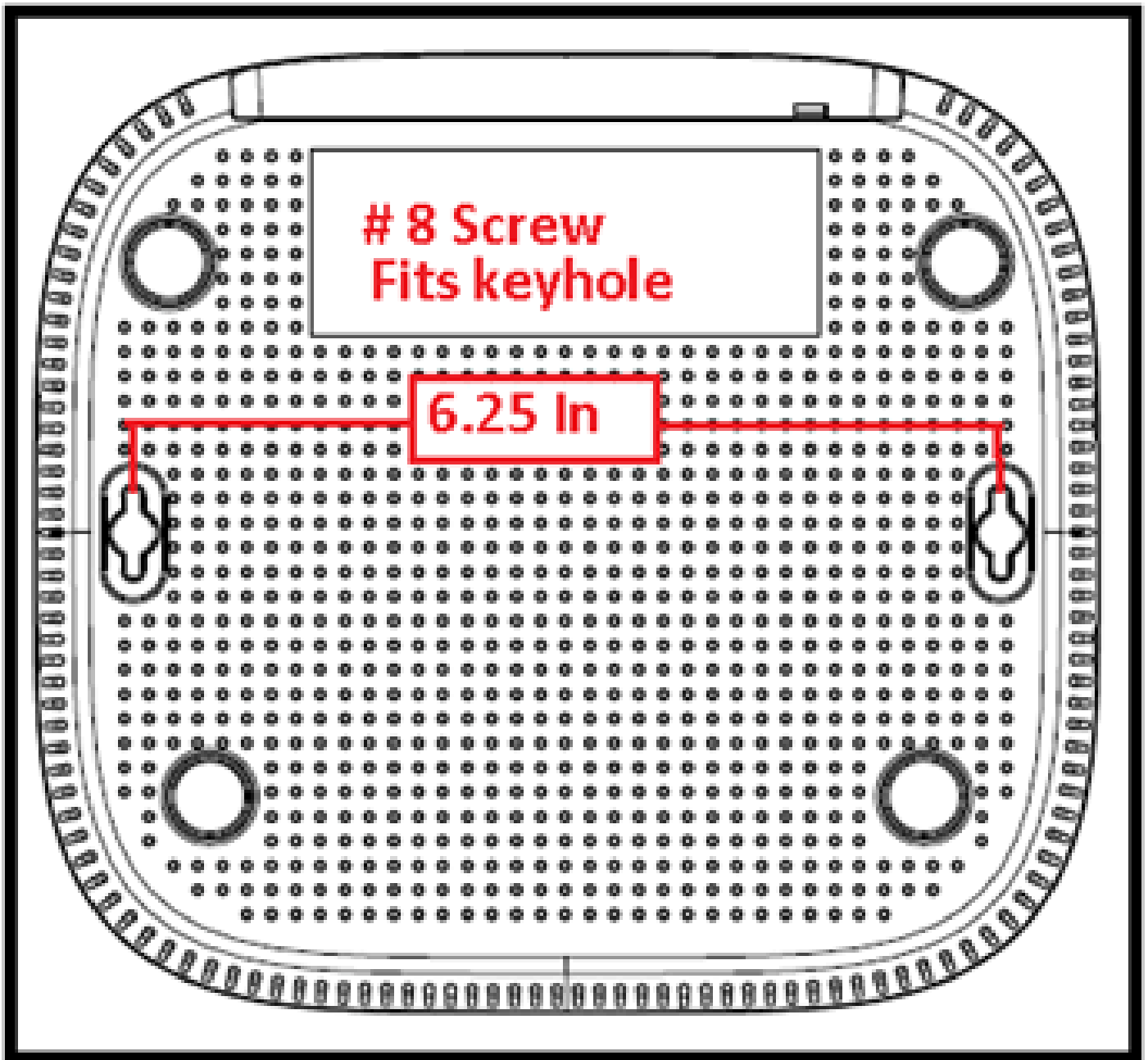
Cette image présente les aspects physiques du protocole OEAP de la gamme Cisco Aironet 600 :



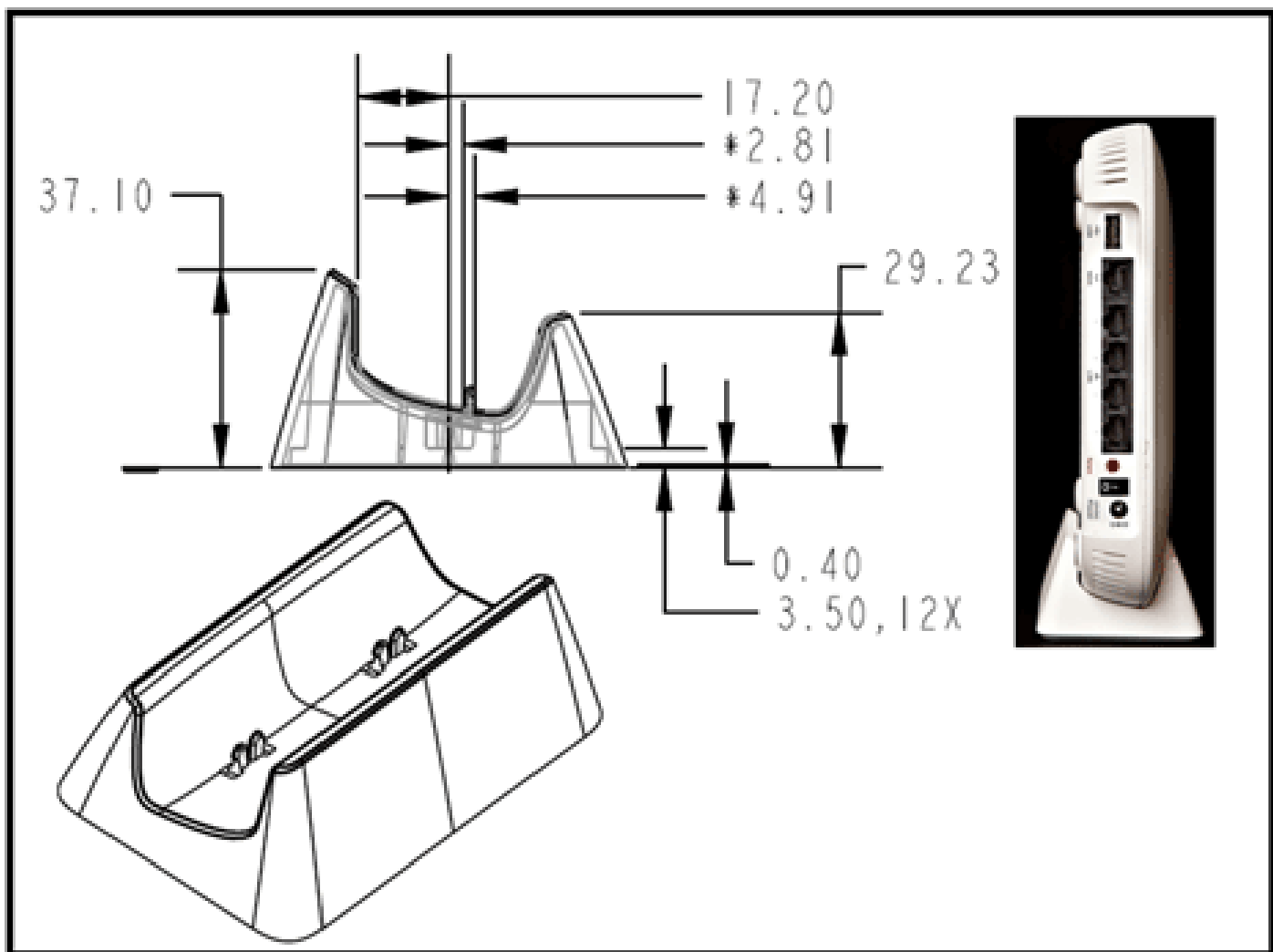
Ce point d'accès est conçu pour être monté sur une table et comporte des pieds en caoutchouc. Il peut également être fixé au mur, ou peut s'asseoir verticalement à l'aide du berceau fourni. Essayez de localiser le point d'accès aussi près que possible des utilisateurs prévus. Évitez les zones présentant de grandes surfaces métalliques, comme l'installation sur un bureau en métal ou près d'un grand miroir. Plus il y a de murs et d'objets entre le point d'accès et l'utilisateur, plus la puissance du signal est faible et plus les performances peuvent être réduites.

Remarque : ce point d'accès utilise un bloc d'alimentation +12 volts et n'utilise pas la technologie PoE (Power over Ethernet). En outre, le périphérique ne fournit pas de PoE. Assurez-vous que l'adaptateur électrique approprié est utilisé avec le point d'accès. Assurez-vous également de ne pas utiliser d'autres adaptateurs d'autres périphériques tels que des ordinateurs portables et des téléphones IP, car ceux-ci peuvent endommager le point d'accès.

L'unité peut être fixée au mur à l'aide d'ancrages en plastique ou de vis en bois.



L'unité peut être montée verticalement à l'aide du berceau fourni.



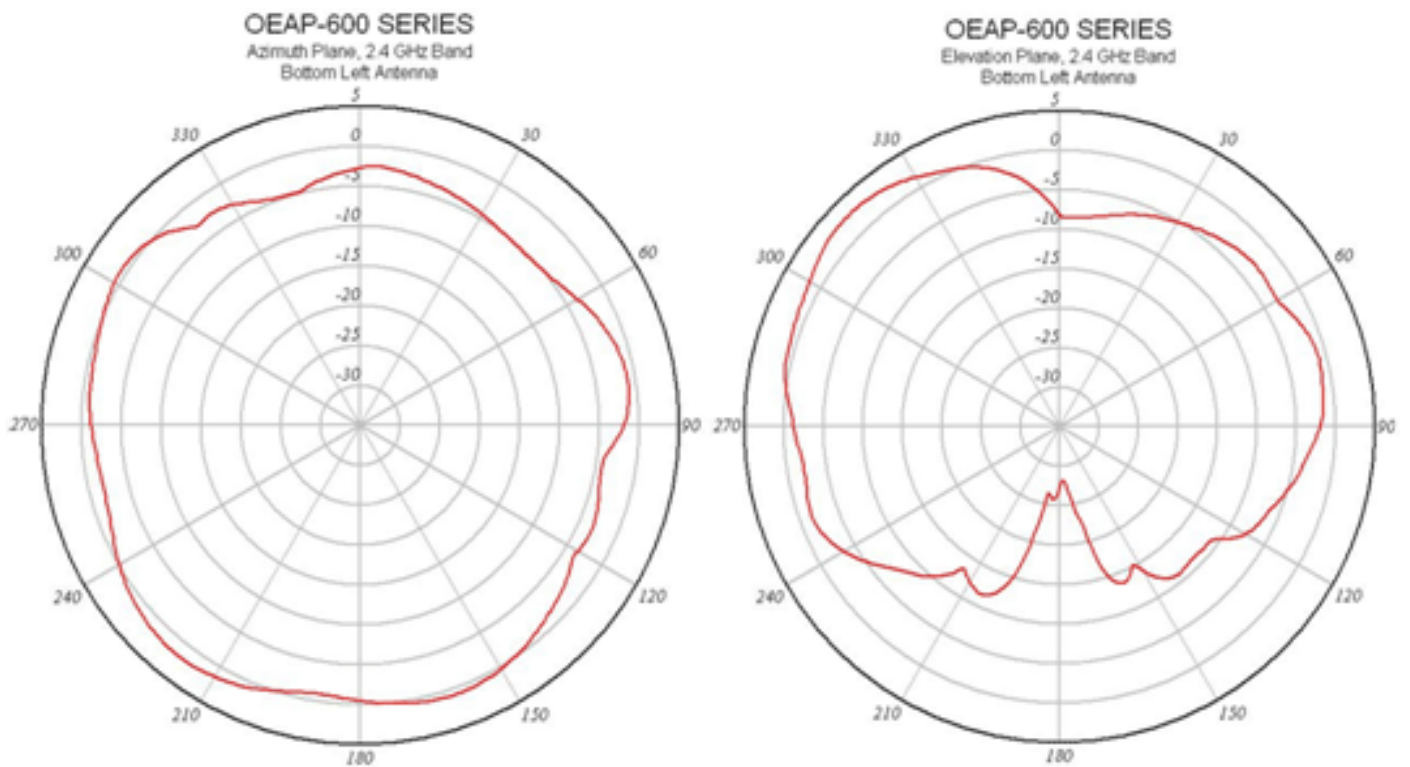
Le point d'accès OEAP de la gamme Cisco Aironet 600 comporte des antennes situées sur les bords du point d'accès. L'utilisateur doit prendre soin de ne pas placer le point d'accès dans des zones proches d'objets métalliques ou d'obstacles qui peuvent entraîner la directivité ou la diminution du signal. Le gain de l'antenne est d'environ 2 dBi dans les deux bandes et est conçu pour rayonner selon un diagramme de 360 degrés. Tout comme une ampoule (sans abat-jour), le but est de rayonner dans toutes les directions. Imaginez le point d'accès comme vous le feriez avec une lampe et essayez de le placer à proximité des utilisateurs.

Les objets métalliques, tels que les miroirs, obstruent le signal comme l'analogie avec l'abat-jour. Le débit ou la portée du signal peut être dégradé si le signal doit pénétrer ou traverser des objets solides. Si vous prévoyez une connectivité, par exemple dans une maison à trois étages, évitez de placer le point d'accès dans le sous-sol et essayez de le monter dans un emplacement central dans la maison.

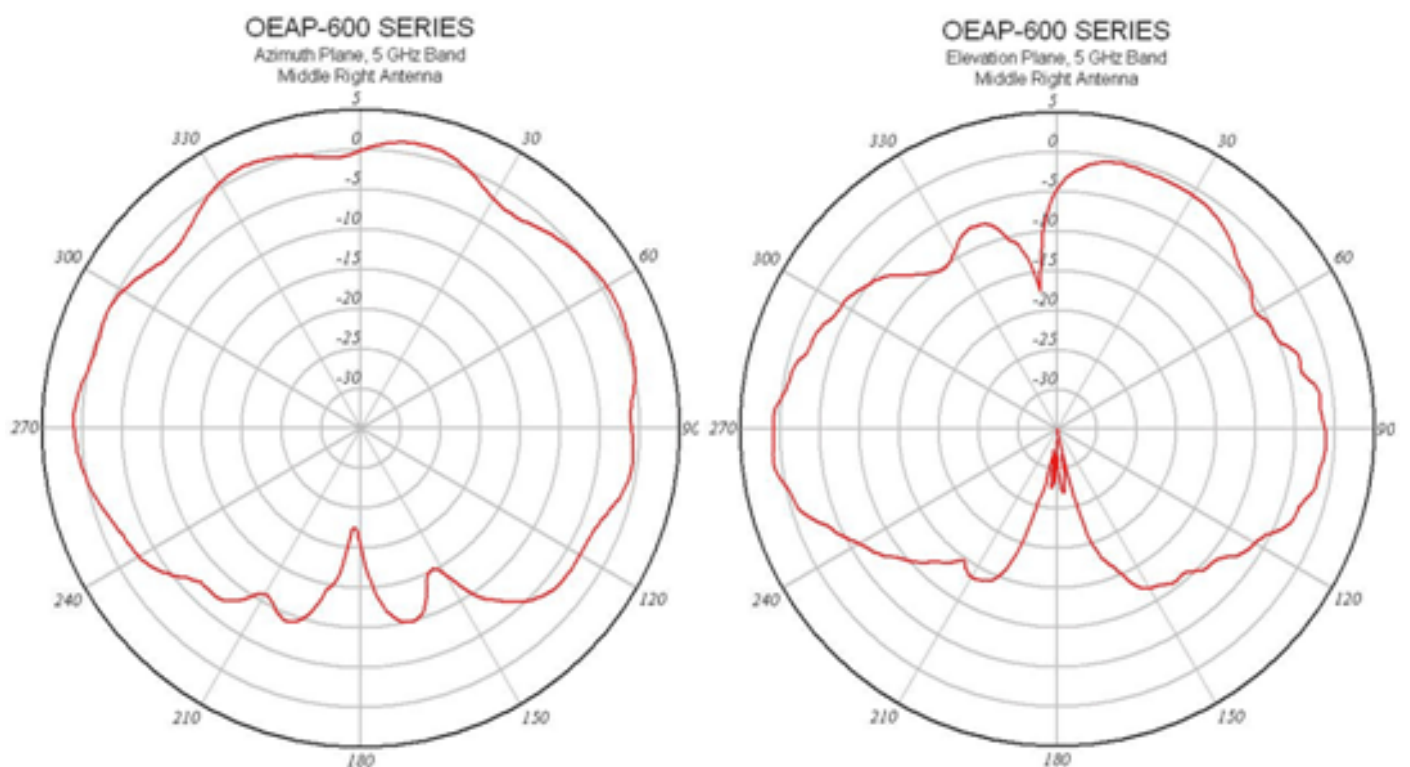
Le point d'accès dispose de six antennes (trois par bande).



Cette image montre un diagramme de rayonnement d'antenne 2,4 GHz (pris à partir de l'antenne inférieure gauche).



Cette image montre un diagramme de rayonnement d'antenne 5 GHz (pris à partir de l'antenne du milieu à droite) :



Dépannage de l'OEAP-600

Vérifiez que le câblage initial est correct. Cela confirme que le port WAN du point d'accès OEAP de la gamme Cisco Aironet 600 est connecté au routeur et peut recevoir une adresse IP avec succès. Si le point d'accès ne semble pas joindre le contrôleur, connectez un PC au port 1-3

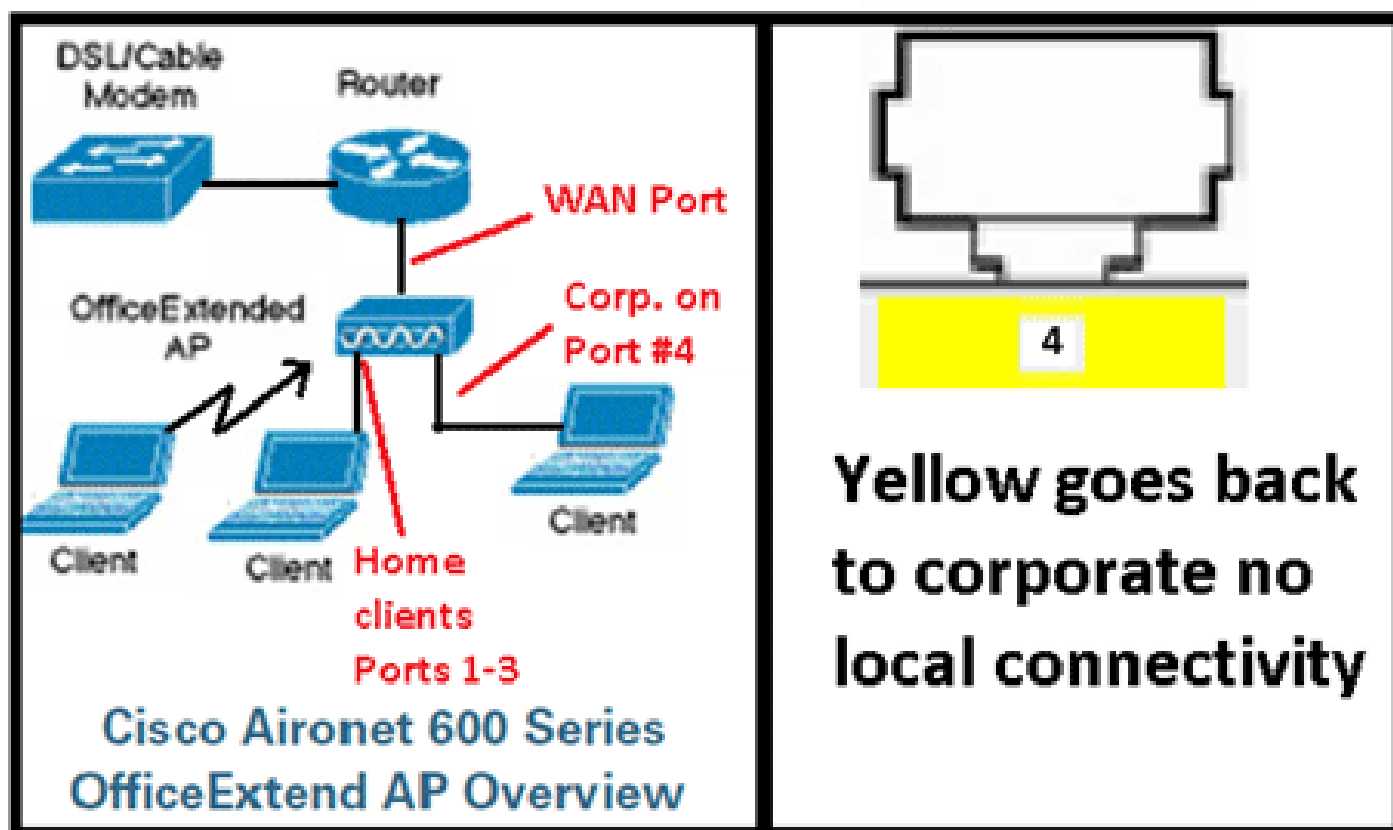
(ports du client domestique) et voyez si vous pouvez accéder au point d'accès en utilisant l'adresse IP par défaut 10.0.0.1. Le nom d'utilisateur et le mot de passe par défaut sont admin.

Vérifiez que l'adresse IP du contrôleur d'entreprise est définie. Si ce n'est pas le cas, entrez l'adresse IP et redémarrez le point d'accès OEAP de la gamme Cisco Aironet 600 afin qu'il puisse essayer d'établir une liaison avec le contrôleur.

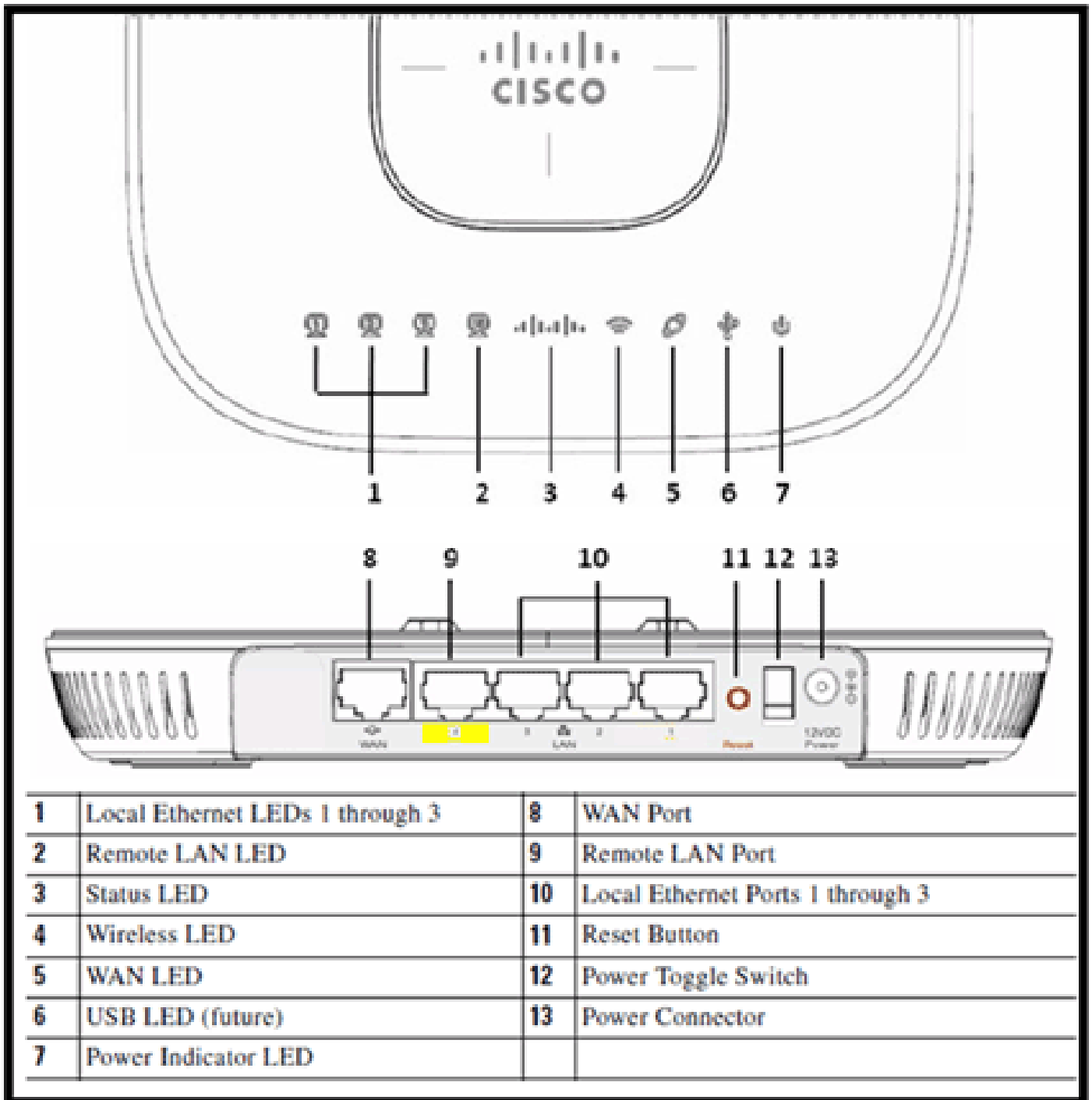
Remarque : le port d'entreprise #4 (en jaune) ne peut pas être utilisé pour accéder au périphérique à des fins de configuration. Il s'agit essentiellement d'un « port mort », sauf si un réseau local distant est configuré. Ensuite, le tunnel reviendra à l'entreprise (utilisé pour la connectivité filaire de l'entreprise)

Consultez le journal des événements pour voir comment l'association a progressé (plus d'informations sur ce sujet plus tard).

Cette image présente le schéma de câblage OEAP de la gamme Cisco Aironet 600 :



Cette image présente les ports de connectivité OEAP de la gamme Cisco Aironet 600 :

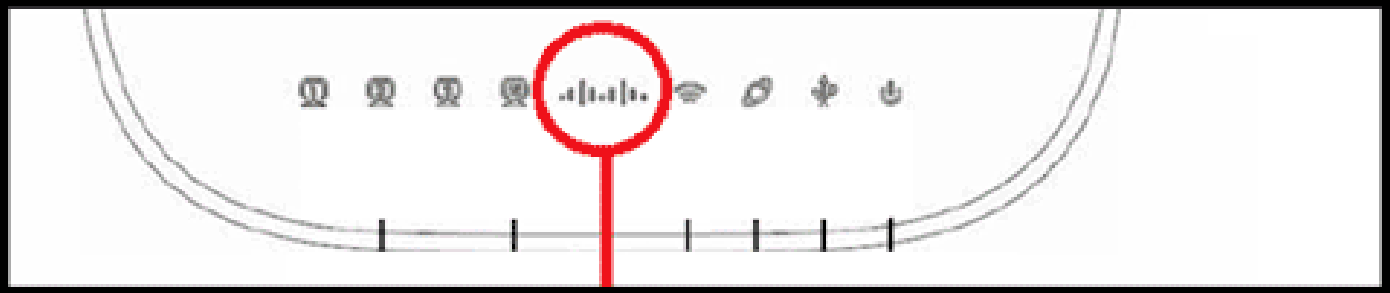


Si le point d'accès OEAP de la gamme Cisco Aironet 600 ne parvient pas à joindre le contrôleur, il est recommandé de vérifier les éléments suivants :

1. Vérifiez que le routeur fonctionne et qu'il est connecté au port WAN du point d'accès OEAP de la gamme Cisco Aironet 600.
2. Connectez un PC à l'un des ports 1 à 3 du point d'accès OEAP Cisco Aironet 600. Il devrait voir Internet.
3. Vérifiez que l'adresse IP du contrôleur d'entreprise se trouve dans le point d'accès.
4. Vérifiez que le contrôleur se trouve sur la zone DMZ et qu'il est accessible via Internet.

5. Vérifiez que le voyant du logo Cisco est bleu ou violet.
6. Prévoyez suffisamment de temps au cas où le point d'accès aurait besoin de charger une nouvelle image et de redémarrer.
7. Si un pare-feu est utilisé, vérifiez que les ports UDP 5246 et 5247 ne sont pas bloqués.

Cette image présente l'état des voyants du logo OEAP de la gamme Cisco Aironet 600 :



Understanding Cisco Aironet 600 Series OfficeExtend AP LEDs

Status LED	Meaning
Purple	Association status, when CAPWAP is connected: Normal operating condition, but no wireless client associated.
Blue	Association status, when CAPWAP is connected: Normal operating condition, at least one wireless client association.
Flashing blue	Operating Status: Software upgrade in progress.
Flashing orange	Operating Status: No IP address, waiting for DHCP IP.
Cycling through purple, orange and blue	Operating Status: Discovery/join process in progress, no client associated.
Cycling through purple, orange	Operating Status: Discovery/join process in progress, with client associated.
Orange	Cisco IOS errors: Software failure; try disconnecting and reconnecting unit power.

Si le processus de jonction échoue, le voyant bascule sur les couleurs ou clignote en orange. Dans ce cas, consultez le journal des événements pour plus de détails. Afin d'accéder au journal des événements, accédez au point d'accès (à l'aide du SSID personnel ou des ports câblés 1 à 3) et capturez ces données pour que l'administrateur informatique les examine.

Cette image présente le journal des événements OEAP de la gamme Cisco Aironet 600 :

Refresh Close window

HOME CONFIGURATION **EVENT_LOG** HELP

Event Log

```

*Nov 12 06:31:59.393:
SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1298, Controller : IP Address 0xc0a801e1
*Nov 12 06:31:59.394: Discovery Response from -1062731295
*Nov 12 06:31:59.411: Dot11 binding decode: Discovery Response
*Nov 12 06:32:09.391: Selected NVAR 'Evora-3C' (index 0).
*Nov 12 06:32:09.391: Ap mgr count=1
*Nov 12 06:32:09.391: Go join a capwap controller
*Nov 12 06:32:09.392: Choosing AP Mgr with index 0, IP = 0xc0a801e1, load = 0..
*Nov 12 06:32:09.392: Synchronizing time with AC time.
*Nov 11 14:31:45.000: CAPWAP State: DTLS Setup.
*Nov 11 14:31:45.619: Dtls Session Established with the AC -1062731295,port= 5246
*Nov 11 14:31:45.620: CAPWAP State: Join.
*Nov 11 14:31:45.620: Join request: version=117469704
*Nov 11 14:31:45.621: Join request: hasMaximum Message Payload
*Nov 11 14:31:45.621: Dot11 binding encode: Encoding join request
*Nov 11 14:31:45.622: Sending Join Request Path MTU payload, Length 1376

*Nov 11 14:31:45.625: Join Response from -1062731295
*Nov 11 14:31:45.626: PTHU : Setting MTU to : 1485

*Nov 11 14:31:45.626: Dot11 binding decode: Join Response
*Nov 11 14:31:45.627: Starting Post Join timer
*Nov 11 14:31:45.627: CAPWAP State: Image Data.
*Nov 11 14:31:45.628: Stopping Post Join Timer and Starting HeartBeat Timer
*Nov 11 14:31:45.628: Image Data Request sent to -1062731295
*Nov 11 14:31:45.630: Image Data Response from -1062731295
*Nov 11 14:31:45.630: Starting image download.....
*Nov 11 14:31:52.467: Successfully downloaded image
*Nov 11 14:32:46.398: Rebooting....
*Nov 11 14:32:46.422: Duplicate sequence number 240 in request.

```

Si le processus de jonction échoue et que c'est la première fois que le point d'accès OEAP de la gamme Cisco Aironet 600 tente de se connecter au contrôleur, vérifiez les statistiques de jonction AP pour le point d'accès OEAP de la gamme Cisco Aironet 600. Pour ce faire, vous avez besoin de l'adresse MAC radio de base du point d'accès. Vous pouvez le trouver dans le journal des événements. Voici un exemple de journal des événements avec des commentaires pour vous aider à interpréter ceci :

Event log 1

WAN port has not obtained IP address, otherwise it will be shown here.

AP Mac address

Base Radio MAC is 00:22:BD:DA:B6:00

```
*Jan 01 08:00:05.420: eth0  Linkencap:Ethernet HWaddrC0:C1:C0:05:48:86
*Jan 01 08:00:05.420:  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
*Jan 01 08:00:05.420:  RX packets:1 errors:0 dropped:0 overruns:0 frame:0
*Jan 01 08:00:05.420:  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
*Jan 01 08:00:05.420:  collisions:0 txqueuelen:100
*Jan 01 08:00:05.421:  RX bytes:64 (64.0 b) TX bytes:0 (0.0 b)
*Jan 01 08:00:05.421:  Interrupt:4 Base address:0x2000
*Jan 01 08:00:05.444: eth1  Linkencap:Ethernet HWaddr00:22:BD:DA:B6:07
*Jan 01 08:00:05.444:  UP BROADCAST RUNNING ALLMULTI MULTICAST MTU:1500 Metric:1
*Jan 01 08:00:05.444:  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
*Jan 01 08:00:05.444:  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
*Jan 01 08:00:05.444:  collisions:0 txqueuelen:100
*Jan 01 08:00:05.444:  RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
*Jan 01 08:00:05.445:  Interrupt:3 Base address:0x1000
*Jan 01 08:00:05.467: Kernel IP routing table
*Jan 01 08:00:05.467: Destination Gateway Genmask Flags Metric Ref Use Iface
*Jan 01 08:00:05.467: 127.0.0.0 * 255.0.0.0 U 0 0 0 lo
*Jan 01 08:00:05.489: IP address HW type Flags HW address Mask Device
*Jan 01 08:00:05.540: oep_mwar_ipaddr= Y.Y.Y.Y
*Jan 01 08:00:07.074: Subject: C=US, ST=California, L=San Jose, O=CISCO, OU=WNBU, CN=OEAP602-C0C1C0054886/emailAd
```

Controller IP address configured in local GUI

certificate

Une fois que cela est connu, vous pouvez regarder dans les statistiques de surveillance du contrôleur pour déterminer si le point d'accès OEAP de la gamme Cisco Aironet 600 a rejoint le contrôleur ou s'il l'a déjà rejoint. En outre, cela devrait fournir une indication sur la raison ou le fait qu'une défaillance s'est produite.

Si l'authentification AP est requise, vérifiez que l'adresse MAC Ethernet OEAP de la gamme Cisco Aironet 600 (et non l'adresse MAC radio) a été entrée dans le serveur Radius en minuscules. Vous pouvez également déterminer l'adresse MAC Ethernet à partir du journal des événements.

Recherche du point d'accès OEAP de la gamme Cisco Aironet 600 sur le contrôleur

The screenshot shows the Cisco Controller GUI with the 'AP Join Stats' page. A search dialog box is open, allowing users to search for APs by MAC Address or AP Name. A red arrow points to the 'MAC Address' input field in the search dialog.

Base Radio MAC	AP Name	Status	Ethernet MAC	IP Address	Last Join Time
00:1f:3e:28:0a:00	devo-homeap	Not Joined	00:00:00:00:00:00	71.84.14.82	
00:1f:3e:28:0a:00	devo-homeap			13	Feb 18 14:00:02.496
00:1f:3e:28:0a:00	phil-homeap			167	Feb 18 18:33:33.130
00:22:bd:da:b6:00	rajevem-evors			95	Feb 20 03:18:26.226
00:22:bd:da:b6:00	chang-evors			57	Feb 17 12:08:19.429
00:22:bd:da:b6:00	wegurie-evors			243	Feb 20 09:01:15.873
00:22:bd:da:b6:00	arikamad-evors			225	Feb 17 12:06:32.529
00:22:bd:da:b6:00	psakna-evors			95	Feb 18 20:00:51.936
00:22:bd:da:b6:00	jakov-THE-evors	Joined	c0:c1:c0:05:48:24	216.139.18.67	Feb 18 11:06:12.427
00:22:bd:da:b6:00	mehulpat-evors	Joined	c0:c1:c0:05:47:c8	96.124.238.245	Feb 20 05:08:17.453

Si vous avez déterminé qu'Internet est accessible à partir d'un PC connecté au port Ethernet local,

mais que le point d'accès ne peut toujours pas joindre le contrôleur, et que vous avez confirmé que l'adresse IP du contrôleur est configurée dans l'interface utilisateur graphique du point d'accès local et est accessible, vérifiez si le point d'accès s'est joint avec succès. Peut-être que l'AP n'est pas dans le serveur AAA. Ou, si l'établissement de liaison DTLS échoue, l'AP peut avoir un certificat incorrect ou une erreur de date/heure sur le contrôleur.

Si aucune unité OEAP de la gamme Cisco Aironet 600 ne peut joindre le contrôleur, vérifiez que le contrôleur se trouve sur la DMZ accessible et que les ports UDP 5246 et 5247 sont ouverts.

Comment déboguer les problèmes d'association client

Le point d'accès joint correctement le contrôleur, mais le client sans fil ne peut pas s'associer au SSID d'entreprise. Consultez le journal des événements pour voir si un message d'association atteint le point d'accès.

La figure suivante illustre les événements normaux d'association du client avec le SSID d'entreprise avec WPA ou WPA2. Pour le SSID avec authentification ouverte ou WEP statique, il n'y a qu'un seul événement ADD_MOBILE.

Journal des événements - Association de clients

```
*Feb 19 20:26:58.876: (Re)Assoc-Req from 00:24:d7:2a:72:c0 forwarded to WLC, wired: no
*Feb 19 20:26:58.941: received assoc-rsp for wireless client, status=0000
*Feb 19 20:26:58.942:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=1
*Feb 19 20:26:58.942: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
*Feb 19 20:27:00.648:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=4
*Feb 19 20:27:00.649: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
```

Si l'événement (Re)Assoc-Req ne figure pas dans le journal, vérifiez que le client dispose des paramètres de sécurité appropriés.

Si l'événement (Re)Assoc-Req apparaît dans le journal mais que le client ne peut pas s'associer correctement, activez la commande debug client <adresse MAC> sur le contrôleur pour le client et examinez le problème de la même manière qu'un client travaillant avec d'autres points d'accès Cisco non-OEAP.

Comment interpréter le journal des événements

Les journaux d'événements suivants, accompagnés de commentaires, peuvent vous aider à résoudre d'autres problèmes de connexion OEAP de la gamme Cisco Aironet 600.

Voici quelques exemples recueillis à partir des fichiers journaux des événements OEAP de la gamme Cisco Aironet 600 avec des commentaires pour faciliter l'interprétation du journal des événements :

Event log 2

```

*Jan 01 08:00:07.093: Build version 7.0.112.66 (compiled Feb 19 2011 at 16:29:58).
*Jan 01 08:00:08.975: CAPWAP State: Init.
*Jan 01 08:00:09.009: CAPWAP State: Discovery.
*Jan 01 08:00:09.042: Starting Discovery.
*Jan 01 08:00:09.044: CAPWAP State: Discovery.
*Jan 01 08:00:09.193: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
*Jan 01 08:00:09.194: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
*Jan 01 08:00:09.194:
SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1338, Controller Cisco_7d:88:00: IP Address
*Jan 01 08:00:09.195: Discovery Request sent to Y.Y.Y.Y with discovery type set to 0
*Jan 01 08:00:09.256: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.272: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.272: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.272: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.273: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.273: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.273: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.274: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.274: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:12.133: Dropping dtls packet since session is not established. ab462383, 147e, c0a80121, 147e, 0
*Jan 01 08:00:19.182: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Ap mgr count=1
*Jan 01 08:00:19.183: Go join a capwap controller
*Jan 01 08:00:19.183: Choosing AP Mgr with index 0, IP = Y.Y.Y.Y , load=151.
*Jan 01 08:00:19.183: Synchronizing time with AC time.
*Feb 19 23:33:56.000: CAPWAP State: DTLS Setup.
*Feb 19 23:34:16.813: Dtls Session Established with the AC: Y.Y.Y.Y , port= 5246
  
```

Discovery Request sent if AP can not get IP address, then Discovery Req. will not be sent

Discovery resp. received from controller. If no response from controller, then need to check whether controller is accessible

Selected controller to join, timestamp synced to the controller

DTLS handshaking with the controller completed. If certificate has problem, then the failure will happen here

Event log 3

```

*Feb 19 23:34:16.813: CAPWAP State: Join.
*Feb 19 23:34:16.814: Join request: version=7.0.114.76

*Feb 19 23:34:16.815: Join request: hasMaximum Message Payload
*Feb 19 23:34:16.815: Dot11 binding encode: Encoding join request
*Feb 19 23:34:16.815: Sending Join Request Path MTU payload, Length 1376

*Feb 19 23:34:16.887: Join Response from Y.Y.Y.Y
*Feb 19 23:34:16.888: PTMU : Setting MTU to : 1485

*Feb 19 23:34:16.888: Dot11 binding decode: Join Response
*Feb 19 23:34:16.889: Starting Post Join timer
*Feb 19 23:34:16.890: CAPWAP State: Image Data.
*Feb 19 23:34:16.890: Controller Version: 7.0.114.76
*Feb 19 23:34:16.890: AP Version: 7.0.114.76
*Feb 19 23:34:16.891: CAPWAP State: Configure.
*Feb 19 23:34:16.891: Dot11 binding encode: Encoding configuration status request.
*Feb 19 23:34:16.893: lwapp_encode_ap_reset_button_payload: reset button state off
*Feb 19 23:34:16.895: Configuration Status sent to Y.Y.Y.Y
*Feb 19 23:34:17.019: Configuration Status Response from Y.Y.Y.Y
*Feb 19 23:34:17.022: CAPWAP State: Run.
*Feb 19 23:34:17.022: Dot11 binding encode: Encoding change state event request.
*Feb 19 23:34:17.023: CAPWAP State: Run.
  
```

**Join Resp. from controller
If AP is not added to AAA server, this step will fail.**

Controller and AP have same version SW, no image download is need. When controller is upgraded to new version SW, image download will happen.

Capwap configuration completes

Event log 4

```
*Feb 19 23:34:17.023: CAPWAP moved to RUN state stopping post join timer
*Feb 19 23:34:17.399: capwapWtpDlForwarding() returned 1
*Feb 19 23:34:17.602: capwapWtpDlForwarding() returned 1
*Feb 19 23:34:17.762: Change State Event Response from -1421466749
*Feb 19 23:34:17.853: SSID alpha,WLAN ID 1, added to the slot[0], enabled
*Feb 19 23:34:18.045: SSID alpha_phone,WLAN ID 2, added to the slot[0], enabled
*Feb 19 23:34:18.118: Ethernet Backhaul WLAN ID = 3,qos=0
*Feb 19 23:34:18.281: SSID alpha,WLAN ID 1, added to the slot[1], enabled
*Feb 19 23:34:18.522: SSID alpha_phone,WLAN ID 2, added to the slot[1], enabled
```

WLANs are configured for 2.4 GHz Radio

Remote-lan is configured

WLANs are configured for 5 GHz Radio

Lorsque la connexion Internet ne semble pas fiable

L'exemple de journal des événements de cette section peut se produire lorsque la connexion Internet échoue ou se révèle très lente ou intermittente. Cela peut être dû à votre réseau FAI, au modem FAI ou à votre routeur domestique. Parfois, la connectivité du FAI est interrompue ou n'est plus fiable. Dans ce cas, la liaison CAPWAP (retour du tunnel vers l'entreprise) peut échouer ou présenter des difficultés.

Voici un exemple d'une telle défaillance dans le journal des événements :

```
*Feb 16 07:13:24.918: Re-Tx Count= 0, Max Re-Tx Value=5, NumofPendingMsgs=1
*Feb 16 07:13:36.919: Re-Tx Count= 4, Max Re-Tx Value=5, NumofPendingMsgs=2
*Feb 16 07:13:39.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:39.919: Retransmission count for packet exceeded max{UNKNOWN_MESSAGE_TYPE (218103808), 2}
*Feb 16 07:13:39.919: Retransmission count exceeded max, ignoring as the ethernet is overloaded
*Feb 16 07:13:42.918: Re-Tx Count= 6, Max Re-Tx Value=5, NumofPendingMsgs=2
Comment : This Retransmission continues on..... Multiple times..
*Feb 16 07:13:42.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:42.919: Retransmission count for packet exceeded max{UNKNOWN_MESSAGE_TYPE (218103808)
*Feb 16 07:14:09.919: GOING BACK TO DISCOVER MODE
*Feb 16 07:14:09.920: CAPWAPState: DTLS Teardown.
*Feb 16 07:14:14.918: DTLS session cleanup completed. Restarting capwap state machine.
*Feb 16 07:14:14.919:
Lost connection to the controller, going to re-start evora...
```

Commandes de débogage supplémentaires

Lorsque vous utilisez le point d'accès OEAP de la gamme Cisco Aironet 600 dans un hôtel ou dans un autre lieu payant, avant que le point d'accès OEAP de la gamme Cisco Aironet 600 ne puisse retourner au contrôleur par tunnel, vous devez passer par le jardin clos. Pour ce faire, branchez un ordinateur portable sur l'un des ports locaux câblés (ports 1 à 3) ou utilisez un SSID personnel pour vous connecter à l'hôtel et satisfaire l'écran de démarrage.

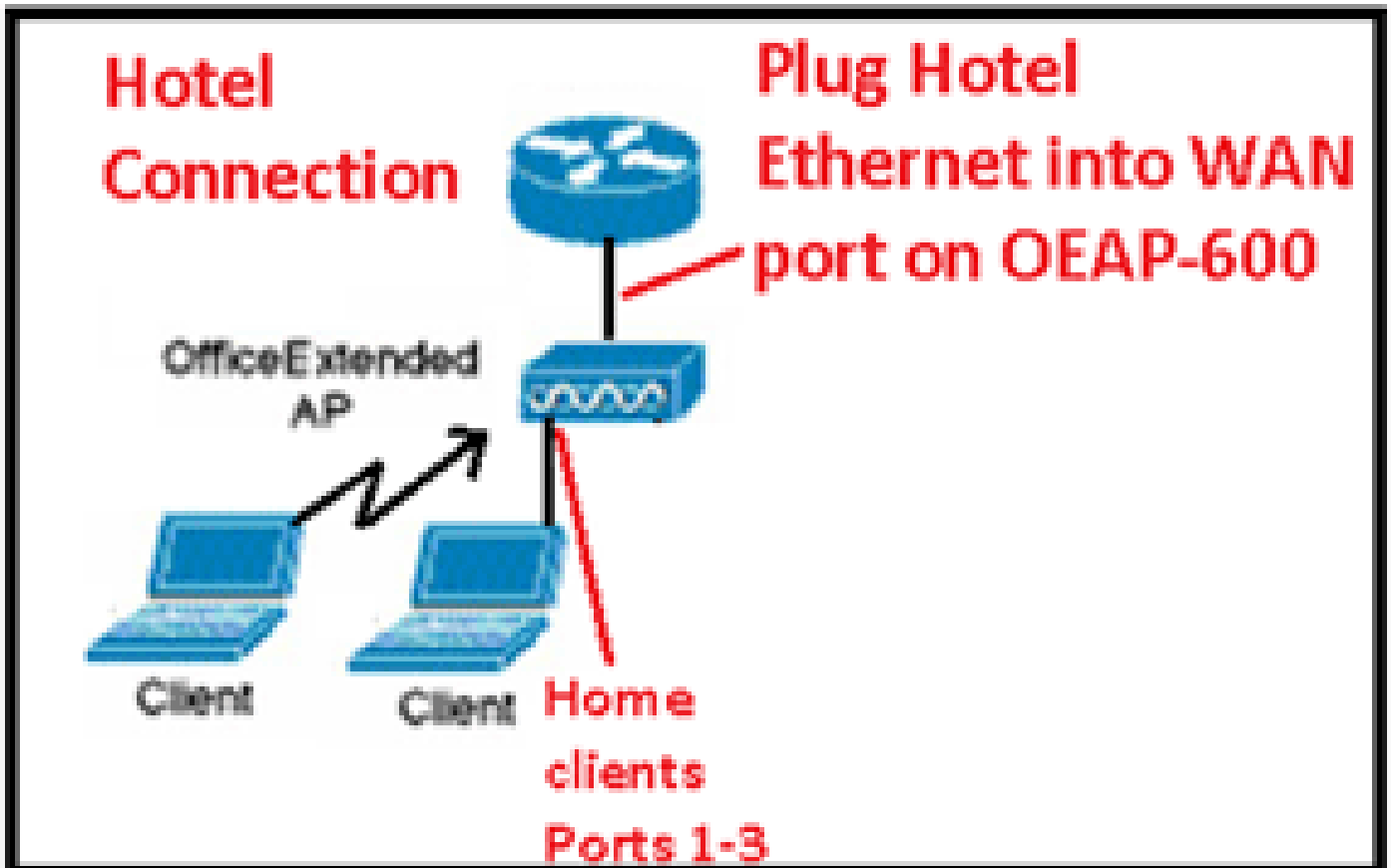
Une fois que vous avez la connectivité Internet du côté maison du point d'accès, l'unité établit un tunnel DTLS et vos SSID d'entreprise. Ensuite, le port filaire #4 (en supposant qu'un réseau local

distant soit configuré) devient actif.

Remarque : cette opération peut prendre quelques minutes. Regardez le voyant du logo Cisco s'allumer en bleu ou en violet pour savoir si l'inscription a réussi. À ce stade, la connectivité personnelle et d'entreprise est active.

Remarque : le tunnel se brise lorsque l'hôtel ou un autre FAI se déconnecte (généralement 24 heures). Ensuite, vous devez recommencer le même processus. C'est par conception et c'est normal.

Cette image montre Office Extend dans une configuration de paiement à l'utilisation :



Cette image montre des commandes debug supplémentaires (informations d'interface radio) :

Below are the new diagnostics commands for the OEAP 600

The WLC CLI of "show tech" is:

```
debugap enable <apname>
```

then:

```
debugap command "evoraTechSupport" <apname> → the information about system and radio slot 0/1
```

```
debugap command "evoraTechSupport 2" <apname> → more info about radio slot 0 (2.4G)
```

```
debugap command "evoraTechSupport 3" <apname> → more info about radio slot 1 (5G)
```

The "show eventlog" is the same as other APs:

```
show ap eventlog <apname>
```

Problèmes connus/Avertissement

Lorsque vous téléchargez le fichier de configuration d'un contrôleur vers un serveur TFTP/FTP, les configurations de réseau local distant sont téléchargées en tant que configurations de réseau local sans fil. Référez-vous aux [Notes de version pour les contrôleurs LAN sans fil Cisco et les points d'accès légers pour la version 7.0.116.0](#) pour plus d'informations.

Sur l'OEAP-600, si la connexion CAPWAP échoue en raison d'un échec d'authentification sur le contrôleur, la LED du logo Cisco sur l'OEAP-600 peut s'éteindre pendant un certain temps avant que l'OEAP-600 essaie de redémarrer la tentative CAPWAP. C'est normal donc vous devez être conscient que le point d'accès n'est pas mort si le voyant du logo s'éteint momentanément.

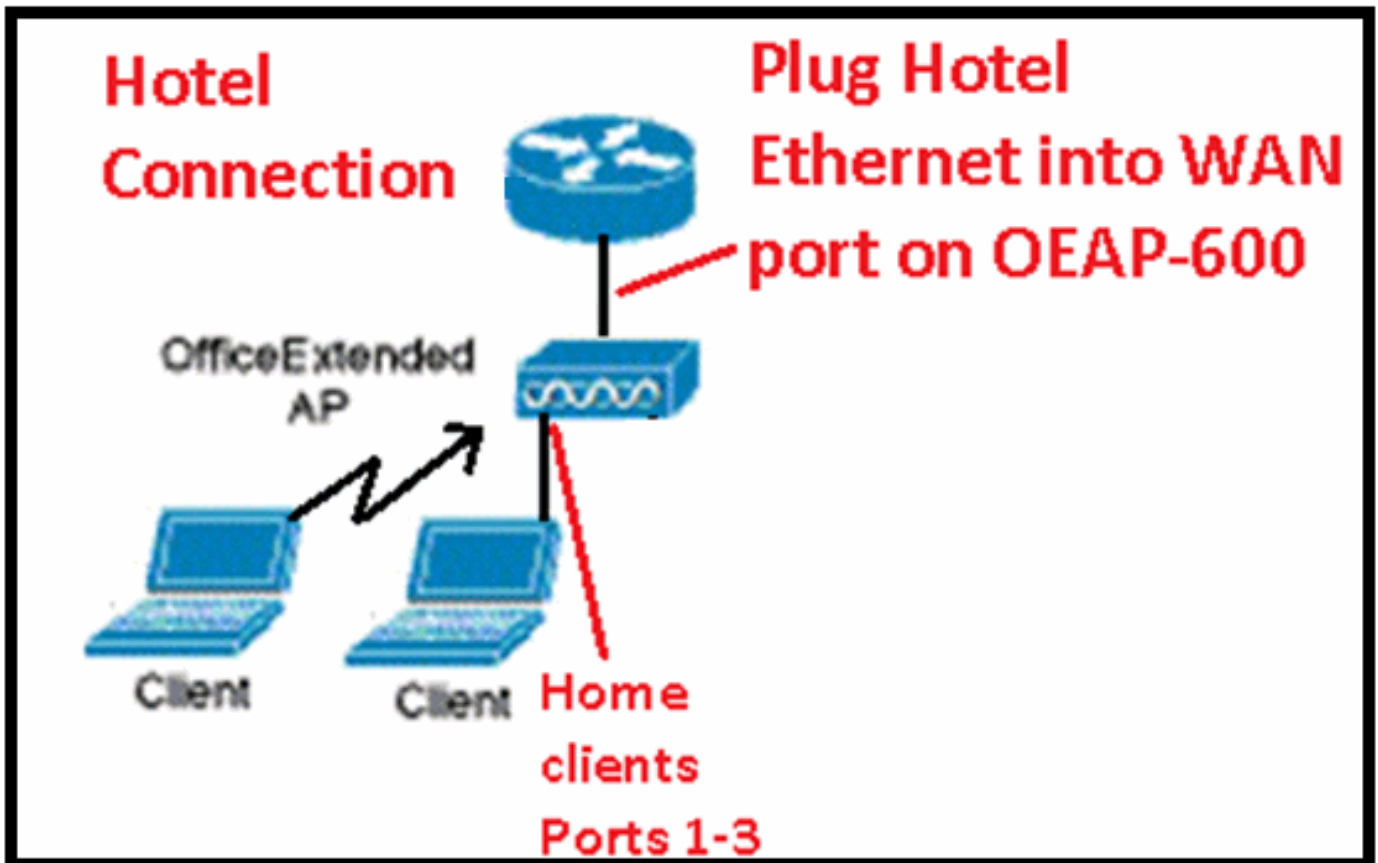
Ce produit OEAP-600 a un nom de connexion différent de celui des points d'accès OEAP précédents, pour être cohérent avec les produits domestiques tels que Linksys, le nom d'utilisateur par défaut est admin avec un mot de passe admin, les autres points d'accès Cisco OEAP tels que AP-1130 et AP-1140 ont un nom d'utilisateur par défaut de Cisco avec un mot de passe de Cisco.

Cette première version de l'OEAP-600 prend en charge la norme 802.1x, mais uniquement sur l'interface de ligne de commande. Les utilisateurs qui tentent d'apporter des modifications à l'interface utilisateur graphique peuvent perdre leurs configurations.

Lorsque vous utilisez l'OEAP-600 dans un hôtel ou dans un autre lieu payant, avant que l'OEAP-600 ne puisse retourner au contrôleur, vous devez passer par le jardin clos. Il vous suffit de brancher un ordinateur portable sur l'un des ports locaux câblés (ports 1 à 3) ou d'utiliser un SSID personnel pour vous connecter à l'hôtel et satisfaire l'écran de démarrage. Une fois que vous avez la connectivité Internet du côté maison de l'AP, l'unité établit alors un tunnel DTLS et vos SSID d'entreprise et le port filaire #4, qui est supposé que Remote-LAN est configuré, puis devient actif. Notez que cette opération peut prendre quelques minutes. Regardez le voyant du logo Cisco, bleu ou violet, pour savoir si l'inscription a réussi. À ce stade, la connectivité personnelle et d'entreprise est active.

Remarque : le tunnel peut se rompre lorsque l'hôtel ou un autre FAI se déconnecte (généralement 24 heures) et que vous devez redémarrer le même processus. C'est par conception et c'est normal.

Office Prolonger dans le site payant

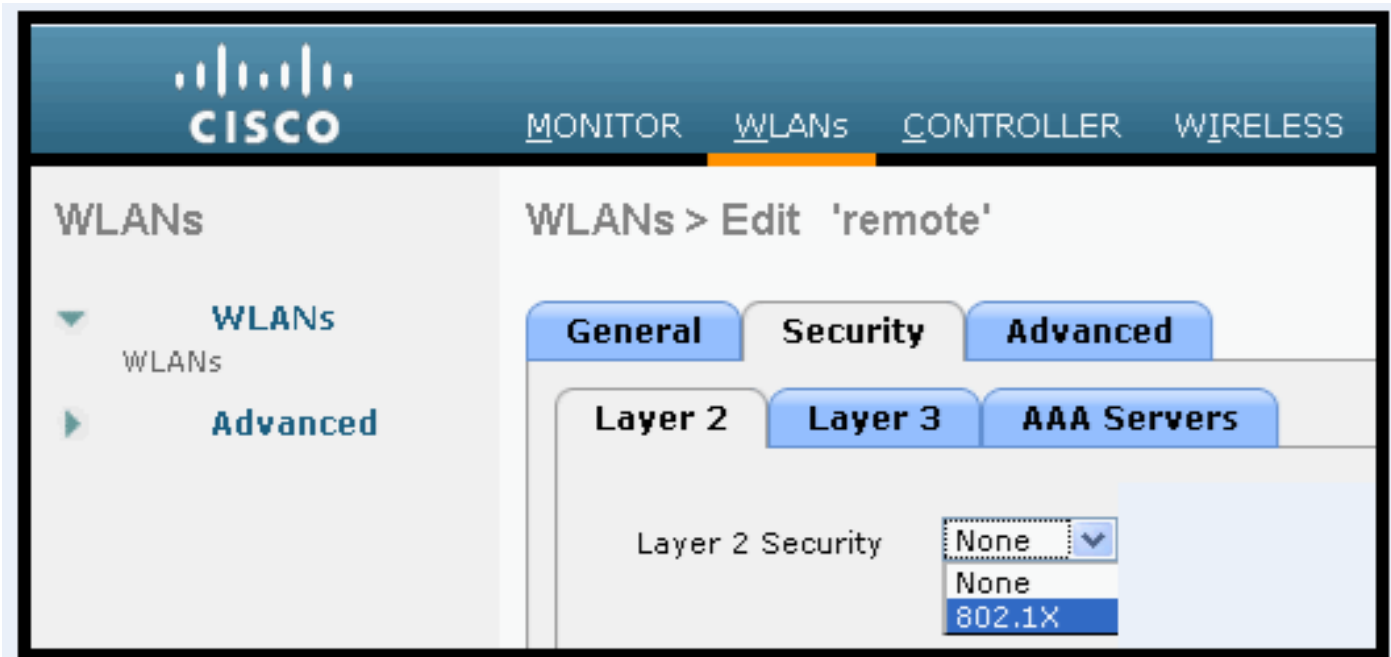


Voici quelques améliorations supplémentaires introduites dans la version 7.2 de Cisco :

- Ajout de la sécurité 802.1x dans l'interface utilisateur graphique
- Possibilité de désactiver l'accès WLAN local sur le point d'accès à partir du contrôleur - désactivation du SSID personnel autorisant uniquement la configuration d'entreprise
- Options sélectionnables d'affectation de canal
- La prise en charge est passée de 2 SSID d'entreprise à 3 SSID
- Prise en charge de la fonctionnalité de port double RLAN

Ajout de la sécurité 802.1x dans l'interface utilisateur graphique

802.1x désormais ajouté à l'interface utilisateur graphique



Remarques relatives à l'authentification du port LAN distant.

802.1x authentication for remote-LAN port

WCS shall be provided to enable 802.1x Layer 2 Security and configure AAA server for remote-LAN. WEP encryption shall be always disabled.

Same as 802.1x authentication for wireless clients, in 802.1x authentication for remote-LAN client, WLC acts as authenticator. Evora AP just forwards the EAPOL packets. AP converts EAPOL Ethernet packet to 802.11 data frame before sending it to WLC. The destination address in the 802.11 data frame shall be set to BSSID for remote-LAN. There is no data encryption for the Ethernet packets transferred on remote-LAN port. So there is no key exchange on EAPOL. The data security is provided by DTLS on CAPWAP data channel.

Following EAP methods are supported:

- EAP-TLS
- PEAP
- EAP-TTLS.

Possibilité de désactiver l'accès WLAN local sur le point d'accès à partir du contrôleur - désactivation du SSID personnel autorisant uniquement la configuration d'entreprise

Désactiver l'accès WLAN local

The screenshot shows the Cisco WLC Global Configuration page. The left sidebar lists various configuration sections like Access Points, RF Profiles, and QoS. The main content area is titled 'Global Configuration' and includes sections for CDP, High Availability, TCP MSS, and AP Retransmit Config Parameters. The 'GEAP Config Parameters' section is highlighted with a red dashed circle, showing a checkbox for 'Disable Local Admin' which is currently unchecked.

Les options d'attribution de canal sélectionnables sont les suivantes :

- Point d'accès contrôlé localement
- Contrôlé par WLC

Attributions de canaux RF et de puissance désormais contrôlées localement ou par WLC

The screenshot shows the Cisco WLC configuration page for a specific AP (BD2-11a/n). The left sidebar lists configuration sections like Access Points, RF Profiles, and QoS. The main content area is titled 'BD2-11a/n Cisco APs > Configure' and includes sections for General, 11n Parameters, CleanAir, RF Channel Assignment, and Tx Power Level Assignment. The 'RF Channel Assignment' and 'Tx Power Level Assignment' sections are highlighted with a red dashed circle. In both sections, the 'WLC Controlled' radio button is selected, and the 'Assignment Method' is set to 'WLC Controlled'.

Manually configure channel and power level

In JMR1 release, there is no configuration option for 802.11a/n and 802.11b/g/n radios for the OEAP-600 AP. In 7.2 release; the configuration window is added back with only "General", "RF Channel Assignment" and "Tx Power Level Assignment" portions. The "Admin Status" in "General" shall be display only. The options for "Assign Method" are changed to "Custom Configured" and "AP Controlled". By default "AP Controlled" is selected. Channel and Tx power level can be configured only when they are in "Custom Configured" mode.

OEAP-600 does not support DFS channels so that WLC shall not allow these channels to be configured. [This new assignment method is passed to AP with CAPWAP payload.

In AP, when the channel is "AP Controlled", then the channel is controlled by the setting from local AP GUI. Otherwise the channel set by WCS is used.

The channel assign method and the assigned channel are saved in NVRAM and displayed in local GUI.

In AP, when the power is "AP controlled", then the maximum power level is always used. Otherwise the power level set by WCS is used.

The assign method for TX power level and assigned TX power level shall be saved in flash so that they can take effect after AP reboots.

When "Reset to Default" operation is performed, the assign method is set to "AP controlled".

Prise en charge de la fonctionnalité de port double RLAN (CLI uniquement)

Cette remarque s'applique aux points d'accès de la gamme OEAP-600 utilisant la fonctionnalité Ports double RLAN, qui permet au port Ethernet OEAP-600 3 de fonctionner comme un LAN distant. La configuration n'est autorisée que via l'interface de ligne de commande. En voici un exemple :

```
Config network oeap-600 dual-r1an-ports enable|disable
```

Si cette fonctionnalité n'est pas configurée, le réseau local distant à port unique 4 continue de fonctionner. Chaque port utilise un réseau local distant unique pour chaque port. Le mappage du réseau local distant est différent, selon que le groupe par défaut ou les groupes AP est utilisé ou non.

Default-group

Si le groupe par défaut est utilisé, un seul réseau local distant avec un ID de réseau local distant pair est mappé au port 4. Par exemple, le réseau local distant avec l'ID de réseau local distant 2 est mappé au port 4 (sur l'OEAP-600). Le réseau local distant avec un ID de réseau local distant impair est mappé au port 3 (sur l'OEAP-600).

Par exemple, prenez ces deux réseaux locaux distants :

```
(Cisco Controller) >show remote-lan summary
```

```
Number of Remote LANS..... 2
```

RLAN ID	RLAN Profile Name	Status	Interface Name
2	r1an2	Enabled	management
3	r1an3	Enabled	management

r1an2 a un ID de réseau local distant pair, 2, et en tant que tel mappe au port 4. r1an3 a un ID de réseau local distant impair 3, et mappe donc au port 3.

Groupes AP

Si vous utilisez un groupe AP, le mappage aux ports OEAP-600 est déterminé par l'ordre du groupe AP. Pour utiliser un groupe AP, vous devez d'abord supprimer tous les LAN et WLAN distants du groupe AP et le laisser vide. Ajoutez ensuite les deux réseaux locaux distants au groupe AP. Ajoutez d'abord le port 3 AP remote-LAN, puis le port 4 remote group, et enfin tous les WLAN.

Un réseau local distant à la première position de la liste est mappé au port 3 et à la seconde position de la liste est mappé au port 4, comme dans cet exemple :

RLAN ID	RLAN Profile Name	Status	Interface Name
2	r1an2	Enabled	management
3	r1an3	Enabled	management

Informations connexes

- [Guide de configuration du contrôleur de réseau local sans fil Cisco, version 7.0](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.