

# Configurar o ponto de acesso Aironet 600 Series OfficeExtend

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Diretrizes de configuração](#)

[Visão geral da solução Office Extend](#)

[Diretrizes de configuração de firewall](#)

[Etapas de configuração do Office Extend AP-600](#)

[Configurações de WLAN e LAN remota](#)

[Configurações de segurança da WLAN](#)

[Filtragem MAC](#)

[Contagem de usuários suportados](#)

[Gerenciamento e configurações de canal](#)

[Avisos adicionais](#)

[Configuração do ponto de acesso OEAP-600](#)

[Instalação de hardware do ponto de acesso OEAP-600](#)

[Troubleshooting do OEAP-600](#)

[Como depurar problemas de associação de cliente](#)

[Como interpretar o registro de eventos](#)

[Quando a conexão com a Internet não parecer confiável](#)

[Comandos debug adicionais](#)

[Problemas conhecidos/Aviso](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento fornece informações sobre os requisitos para configurar um Cisco Wireless LAN (WLAN) Controller para uso com o Cisco Aironet<sup>®</sup> 600 Series OfficeExtend Access Point (OEAP). O Cisco Aironet 600 Series OEAP suporta operação de modo dividido e tem instalações que exigem configuração através do controlador de WLAN e recursos que podem ser configurados localmente pelo usuário final. Este documento também fornece informações sobre as configurações necessárias para conexão apropriada e conjuntos de recursos suportados.

## [Prerequisites](#)

## Requirements

Não existem requisitos específicos para este documento.

## Componentes Utilizados

As informações neste documento são baseadas no Cisco Aironet 600 Series OfficeExtend Access Point (OEAP).

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

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

## Informações de Apoio

### Diretrizes de configuração

- O Cisco Aironet 600 Series OEAP é suportado nestas controladoras: Cisco 5508, WiSM-2 e Cisco 2504.
- A primeira versão do controlador que suporta o Cisco Aironet 600 Series OEAP é 7.0.116.0
- As interfaces de gerenciamento do controlador precisam estar em uma rede IP roteável.
- A configuração do firewall corporativo precisa ser alterada para permitir o tráfego com os números de porta UDP **5246** e **5247**.

### Visão geral da solução Office Extend

- Um usuário recebe um ponto de acesso (AP) com o endereço IP do controlador corporativo, ou o usuário pode inserir o endereço IP do controlador na tela de configuração (páginas HTML de configuração).
- O usuário conecta o AP ao seu roteador residencial.
- O AP obtém um endereço IP de seu roteador residencial, junta-se ao controlador primário e cria um túnel seguro.
- Em seguida, o Cisco Aironet 600 Series OEAP anuncia o SSID corporativo, que estende os mesmos métodos e serviços de segurança na WAN até a casa do usuário.
- Se a LAN remota estiver configurada, uma porta com fio no AP é encapsulada de volta ao controlador.
- O usuário pode, então, habilitar adicionalmente um SSID local para uso pessoal.

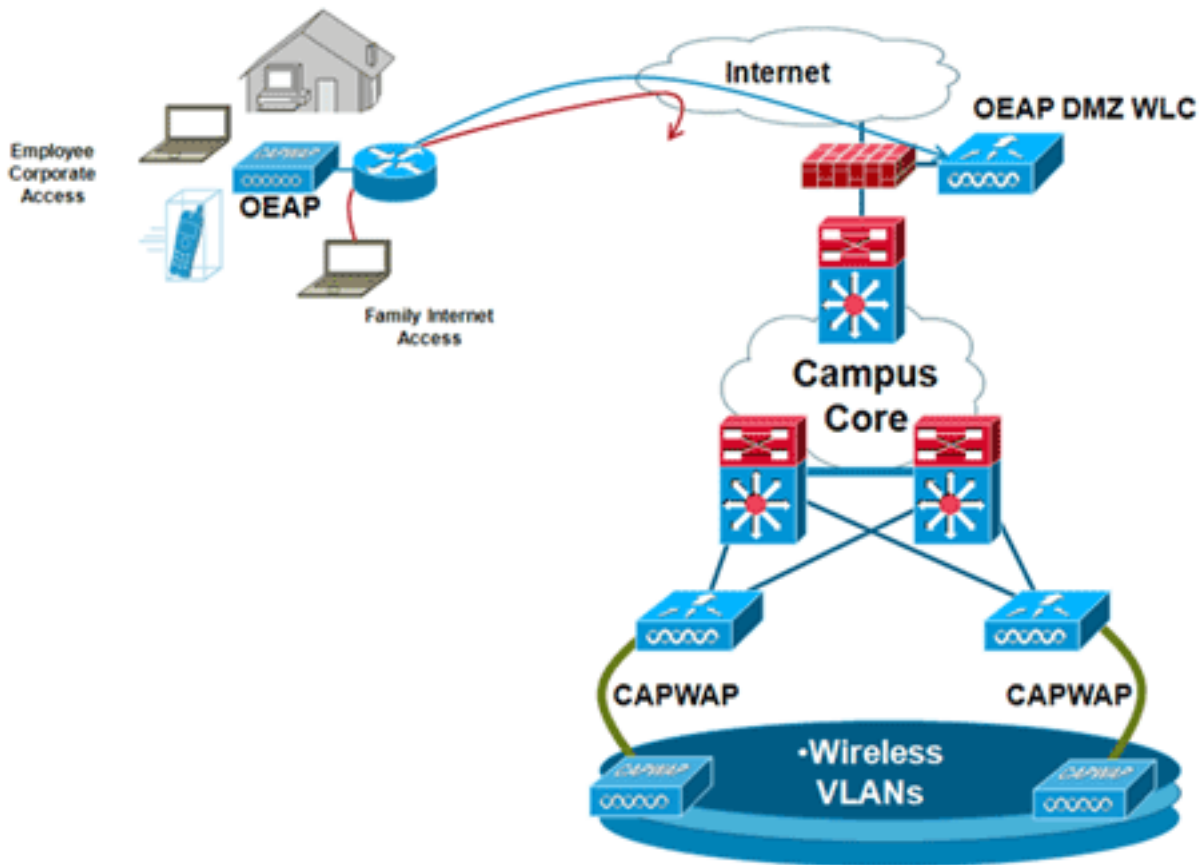
### Diretrizes de configuração de firewall

A configuração geral no firewall é permitir o controle do CAPWAP e os números de porta de gerenciamento do CAPWAP através do firewall. O controlador OEAP Cisco Aironet 600 Series

pode ser colocado na zona DMZ.

**Observação:** as portas UDP 5246 e 5247 precisam ser abertas no firewall entre o controlador de WLAN e o Cisco Aironet 600 Series OEAP.

Este diagrama mostra um controlador Cisco Aironet 600 Series OEAP no DMZ:



Aqui está um exemplo de configuração de firewall:

```
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
```

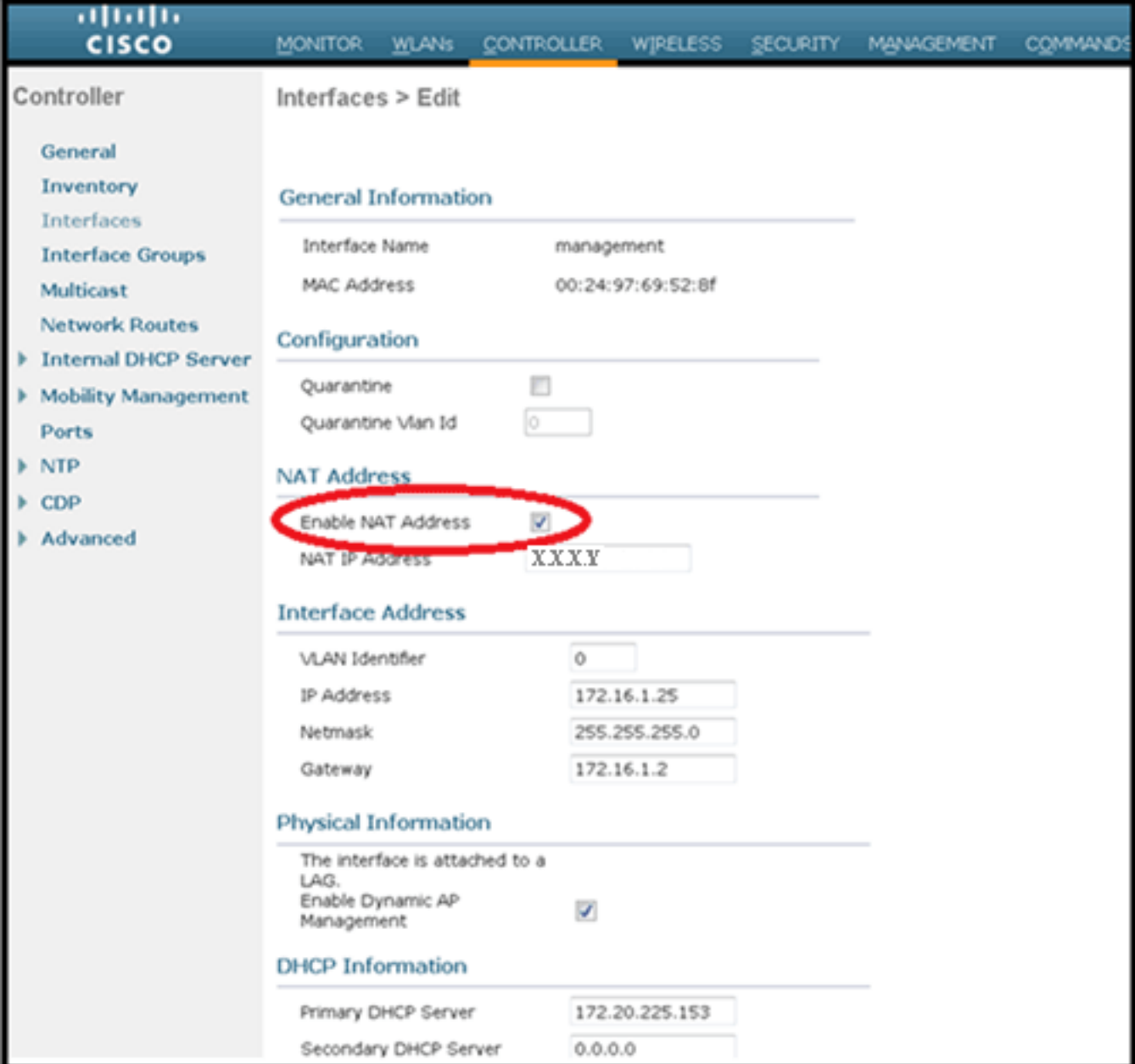
Para transmitir o endereço IP interno do gerenciador de AP para o AP OfficeExtend como parte do pacote CAPWAPP Discovery Response, o administrador do controlador precisa certificar-se de que o NAT esteja habilitado na interface do gerenciador de AP e que o endereço IP NAT correto seja enviado para o AP.

**Observação:** por padrão, a WLC responderá apenas com o endereço IP do NAT durante a descoberta do AP quando o NAT estiver habilitado. Se os APs existirem dentro e fora do gateway NAT, execute este comando para configurar o WLC para responder com o endereço IP NAT e o endereço IP de gerenciamento não NAT (interno):

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

**Observação:** isso só é necessário se a WLC tiver um endereço IP de NAT.

Este diagrama mostra que o NAT está ativado, supondo que o WLC tenha um endereço IP NAT:



The screenshot shows the Cisco WLC configuration interface for the 'management' interface. The 'NAT Address' section is highlighted with a red circle, indicating that 'Enable NAT Address' is checked and the 'NAT IP Address' is set to 'X.X.X.Y'.

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

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

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

Interface Address	
VLAN Identifier	0
IP Address	172.16.1.25
Netmask	255.255.255.0
Gateway	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	172.20.225.153
Secondary DHCP Server	0.0.0.0

**Observação:** essa configuração não é necessária no controlador, desde que esteja configurada com um endereço IP roteável da Internet e não atrás de um firewall.

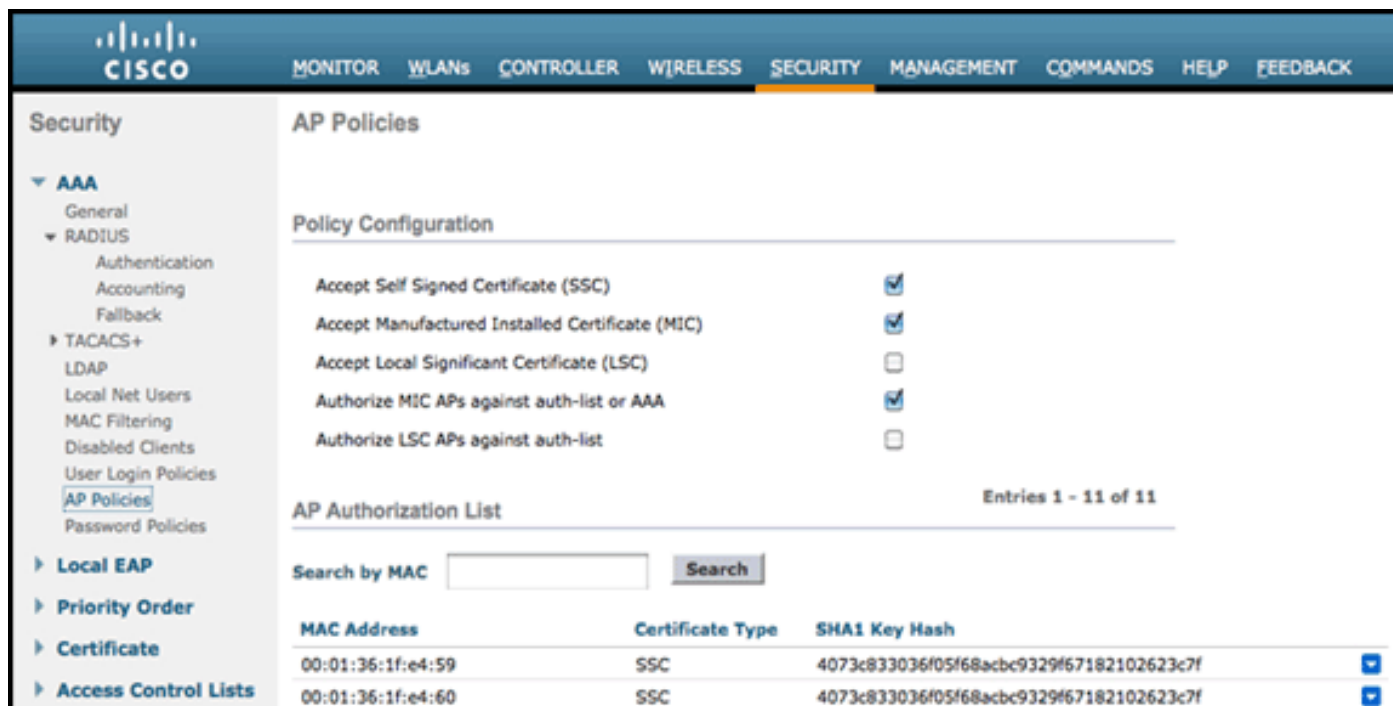
## [Etapas de configuração do Office Extend AP-600](#)

O Cisco Aironet 600 Series OEAP se conectará à WLC como um ponto de acesso de modo local.

**Observação:** os modos Monitor, H-REAP, Sniffer, Rogue Detection, Bridge e SE-Connect não são suportados no 600 Series e não são configuráveis.

**Observação:** a funcionalidade OEAP do Cisco Aironet 600 Series nos Access Points 1040, 1130, 1140 e 3502i Series requer a configuração dos APs para o Hybrid REAP (H-REAP) e a definição do submodo do AP para o OEAP do Cisco Aironet 600 Series. Isso não é feito com o 600 Series porque ele usa o modo local e não pode ser alterado.

A filtragem MAC pode ser usada na autenticação do AP durante o processo de junção inicial para impedir que unidades OEAP não autorizadas do Cisco Aironet 600 Series se juntem ao controlador. Esta imagem mostra onde você habilita a filtragem MAC e configura as políticas de segurança de AP:



The screenshot shows the Cisco Aironet 600 Series 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, Password Policies), Local EAP, Priority Order, Certificate, and Access Control Lists. The main content area is titled 'AP Policies' and 'Policy Configuration'. It lists several policies 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 of entries. The table has columns for MAC Address, Certificate Type, and SHA1 Key Hash. Two entries are shown, both with MAC address 00:01:36:1f:e4:60 and Certificate Type SSC, with the same SHA1 Key Hash: 4073c833036f05f68acbc9329f67182102623c7f.

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

O MAC Ethernet (não o endereço MAC do rádio) é inserido aqui. Além disso, se você digitar o endereço MAC em um servidor Radius, use letras minúsculas. Você pode examinar o registro de eventos do AP para obter informações sobre como descobrir o endereço MAC Ethernet (mais sobre isso posteriormente).

## [Configurações de WLAN e LAN remota](#)

Há uma porta LAN remota física (porta #4 amarela) no Cisco Aironet 600 Series OEAP. É muito semelhante a uma WLAN em como ela é configurada. No entanto, como não é sem fio e uma porta LAN com fio na parte traseira do AP, ela é chamada e gerenciada como uma porta LAN remota.

Embora haja apenas uma porta física no dispositivo, até quatro clientes com fio podem ser conectados se um hub ou switch for usado.

**Observação:** o limite de cliente LAN remoto suporta a conexão de um switch ou hub à porta LAN remota para vários dispositivos ou a conexão direta a um telefone IP Cisco que esteja conectado a essa porta.

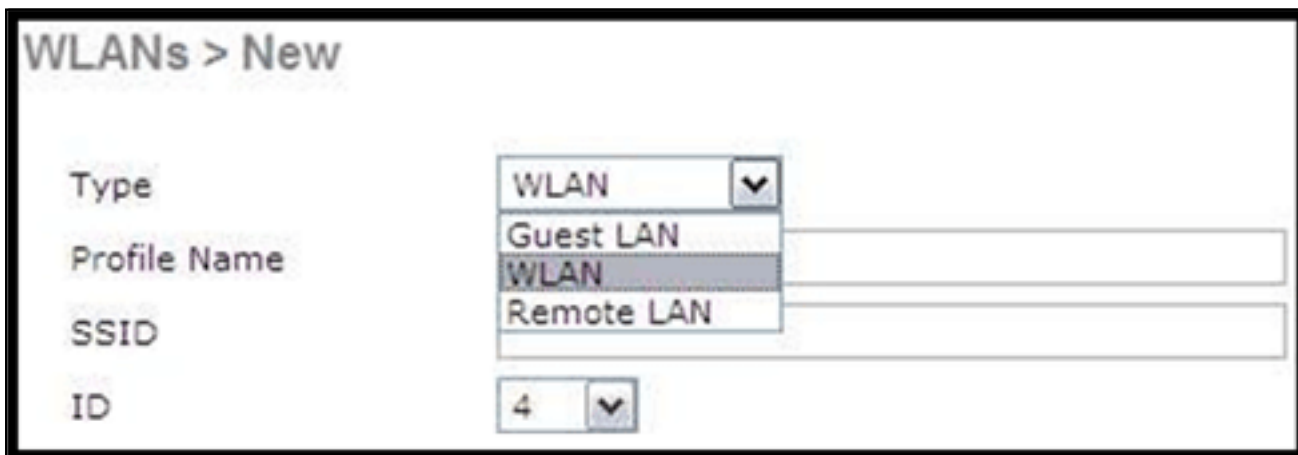
**Observação:** somente os quatro primeiros dispositivos podem se conectar até que um dos dispositivos fique ocioso por mais de um minuto. Se estiver usando a autenticação 802.1x, pode haver problemas ao tentar usar mais de um cliente na porta com fio.

**Observação:** esse número não afeta o limite de quinze imposto para as WLANs do controlador.

Uma LAN remota é configurada de forma semelhante a uma WLAN e LAN de convidado configuradas no controlador.

As WLANs são perfis de segurança sem fio. Esses são os perfis usados pela rede corporativa. O Cisco Aironet 600 Series OEAP suporta no máximo duas WLANs e uma LAN remota.

Uma LAN remota é semelhante a uma WLAN, exceto pelo fato de ser mapeada para a porta com fio na parte traseira do access point (porta #4 em amarelo), conforme mostrado nesta imagem:



**Observação:** se você tiver mais de duas WLANs ou mais de uma LAN remota, todas precisam ser colocadas em um grupo AP.

Esta imagem mostra onde as WLANs e a LAN remota estão configuradas:



Esta imagem mostra um nome de grupo OEAP de exemplo:



Esta imagem mostra uma configuração de WLAN SSID e RLAN:



WLANs

Ap Groups > Edit 'EvoraOEAP'

General | **WLANs** | APs

WLAN ID	WLAN SSID	Interface/Interface Group(G)	SNMP NAC State
1	EvoraData	management	Disabled
2	Evora_Voice	management	Disabled
3	EthernetTunnel	management	Disabled

Se o OEAP Cisco Aironet 600 Series for inserido em um grupo AP, os mesmos limites de duas WLANs e uma LAN remota se aplicam à configuração do grupo AP. Além disso, se o Cisco Aironet 600 Series OEAP estiver no grupo padrão, o que significa que ele não está em um grupo de AP definido, as IDs de WLAN/LAN remota precisam ser definidas com menos de ID 8 porque este produto não suporta os conjuntos de ID mais altos.

Mantenha os conjuntos de IDs em menos de 8, como mostrado nesta imagem:

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT

WLANs > New

Type: WLAN

Profile Name: New Evora WLAN

SSID: EvoraWLAN

ID: 4

4

5

6

7

8

9

10

11

12

13

**Observação:** se WLANs ou LANs remotas adicionais forem criadas com a intenção de alterar as WLANs ou LANs remotas que estão sendo usadas pelo Cisco Aironet 600 Series OEAP, desabilite as WLANs ou LANs remotas atuais que você está removendo antes de habilitar as novas WLANs ou LAN remota no 600 Series. Se houver mais de uma LAN remota habilitada para um grupo de AP, desabilite todas as LANs remotas e habilite apenas uma.

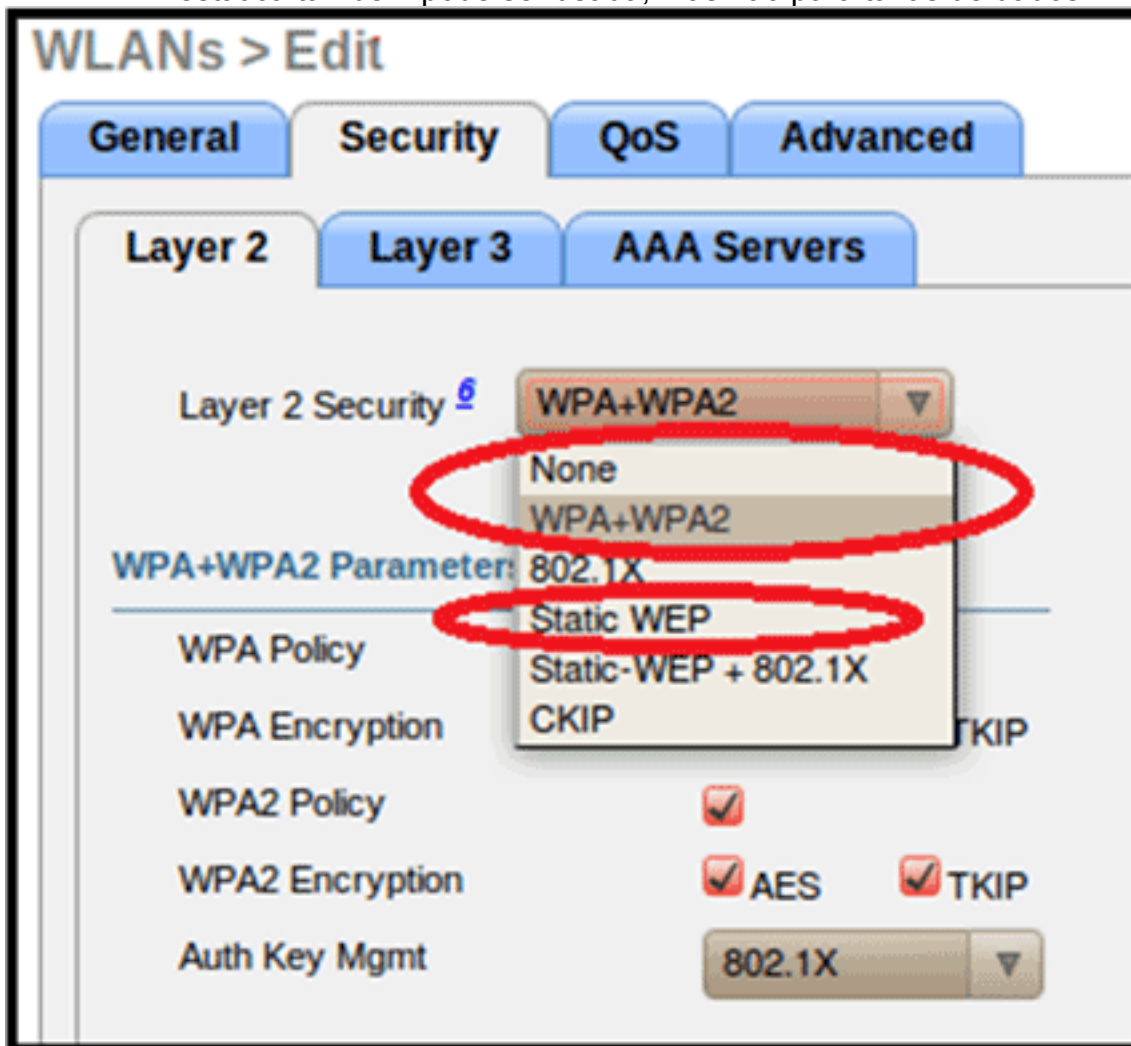
Se houver mais de duas WLANs habilitadas para um grupo AP, desabilite todas as WLANs e habilite apenas duas.

[Configurações de segurança da WLAN](#)

Ao definir a configuração de segurança na WLAN, há elementos específicos que não são suportados na série 600.

Para segurança de camada 2, somente estas opções são suportadas para o Cisco Aironet 600 Series OEAP:

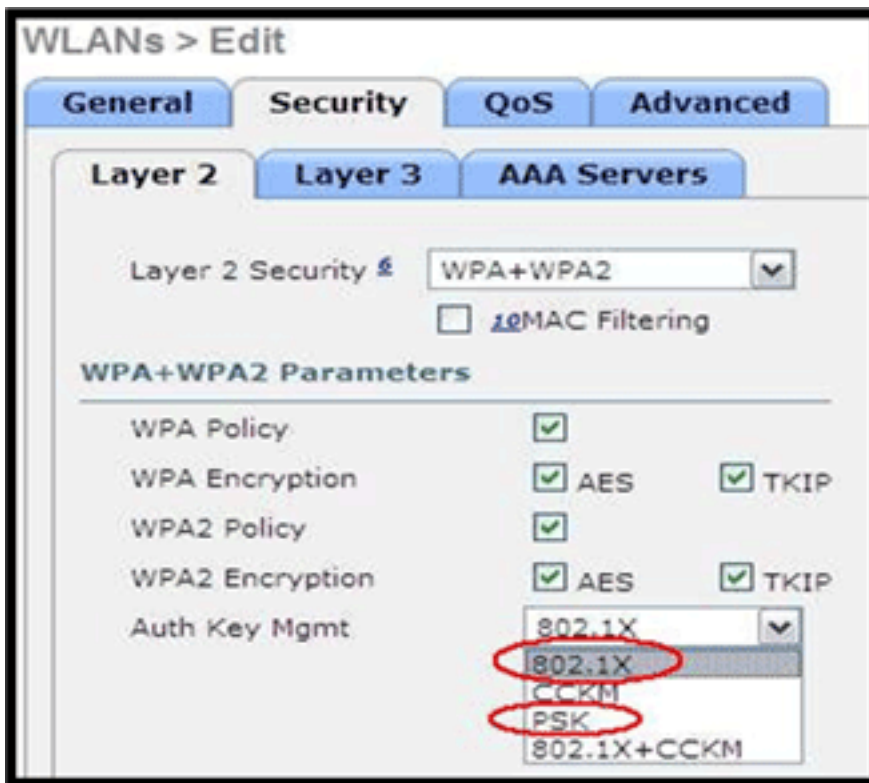
- Nenhum
- WPA+WPA2
- A WEP estática também pode ser usada, mas não para taxas de dados .11n.



**Observação:** somente 802.1x ou PSK deve ser selecionado.

As configurações de criptografia de segurança precisam ser idênticas para WPA e WPA2 para TKIP e AES, como mostrado na imagem a seguir:



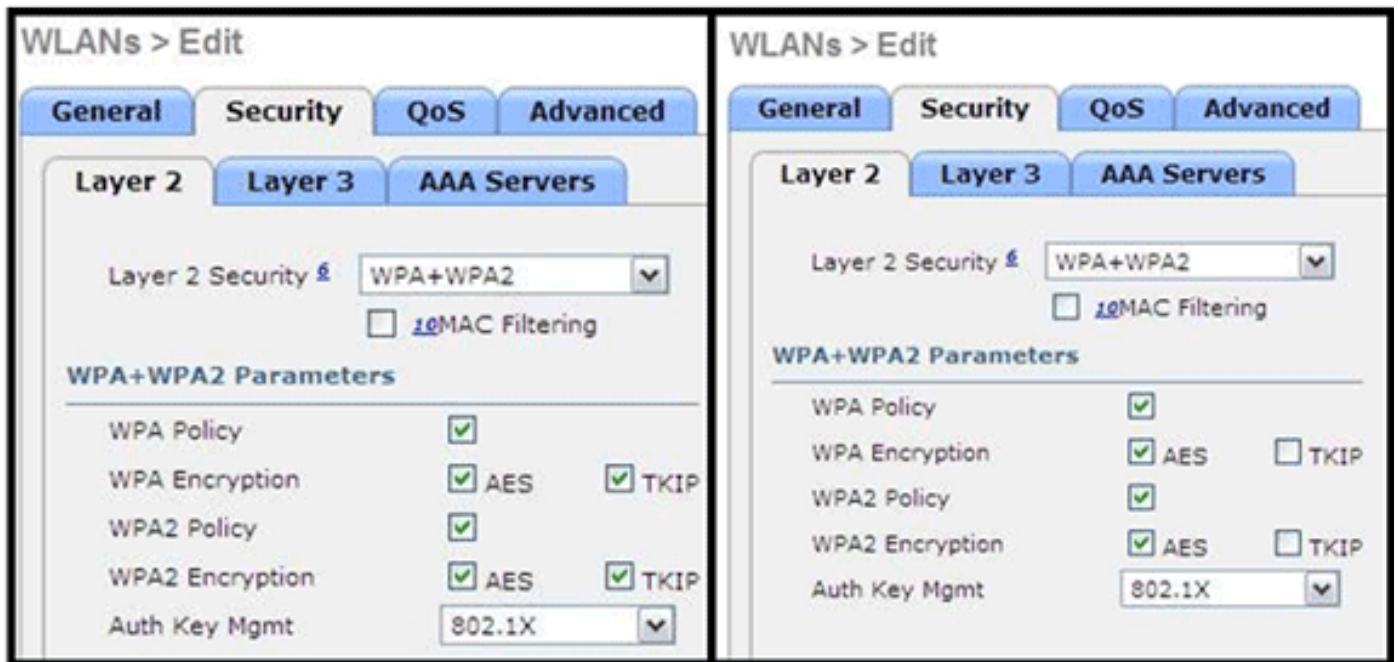


Essas imagens fornecem exemplos de configurações incompatíveis para TKIP e AES:



**Observação:** lembre-se de que as configurações de segurança permitem recursos sem suporte.

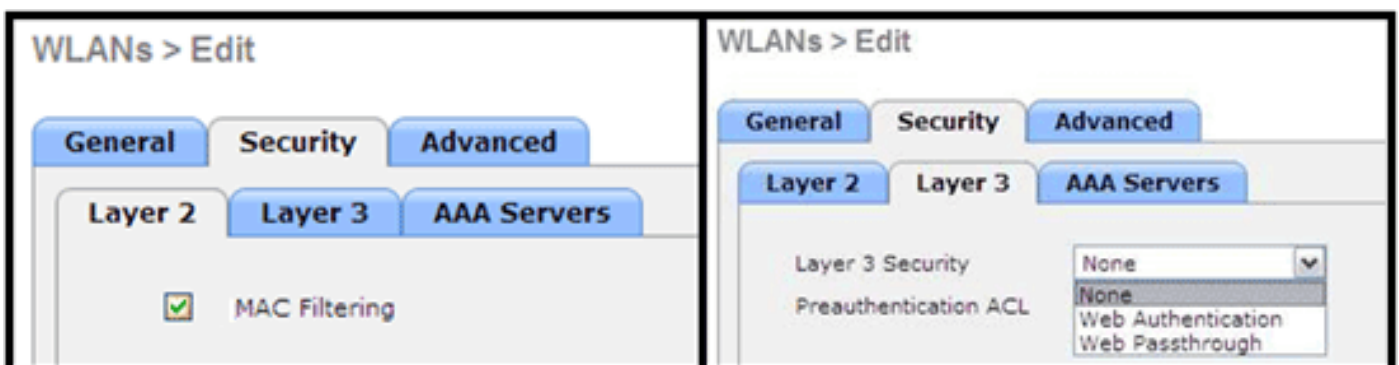
Estas imagens fornecem exemplos de configurações compatíveis:



## Filtragem MAC

As configurações de segurança podem ser deixadas abertas, definidas para filtragem MAC ou definidas para Autenticação da Web. O padrão é utilizar a filtragem MAC.

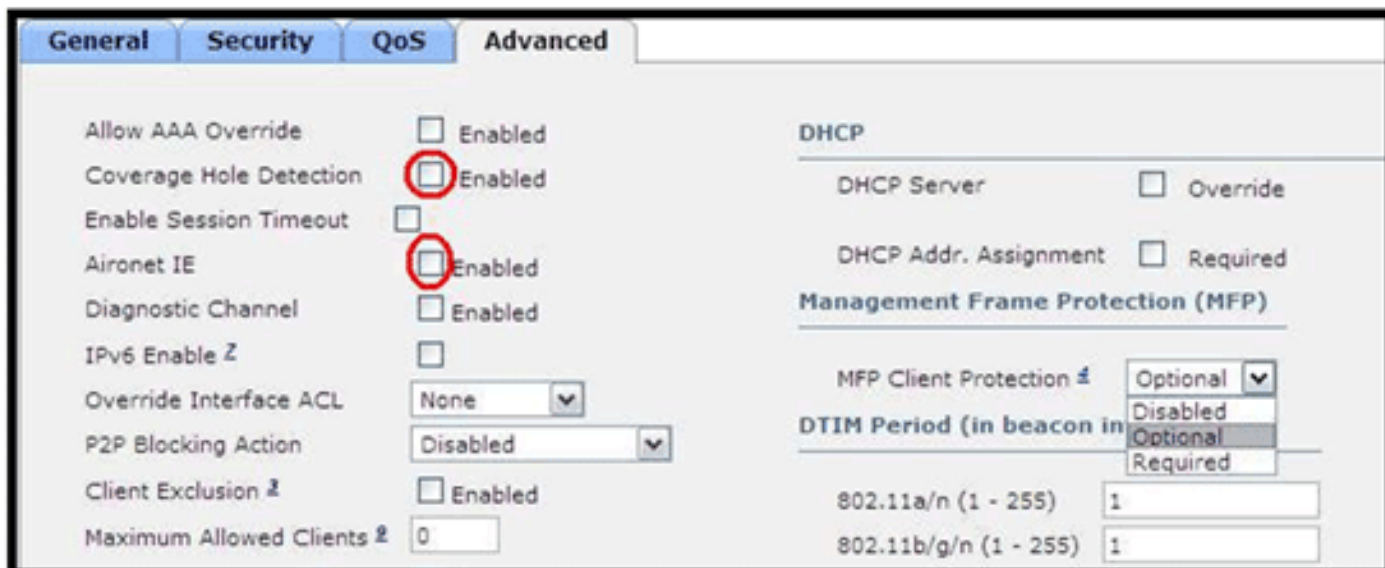
Esta imagem mostra a filtragem MAC de Camada 2 e Camada 3:



As configurações de QoS são gerenciadas:

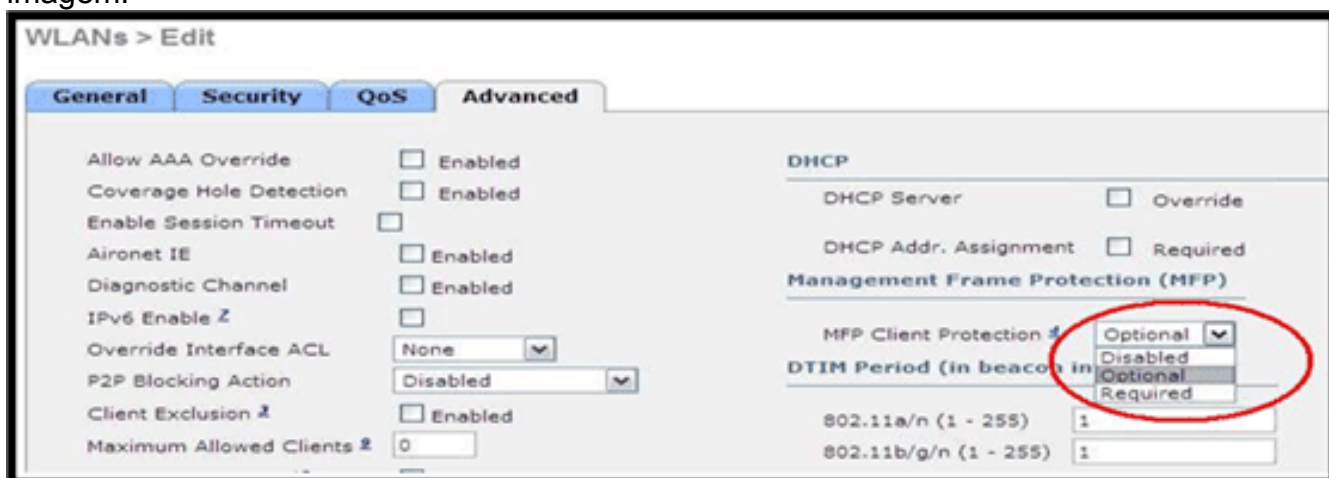


As configurações avançadas também devem ser gerenciadas:

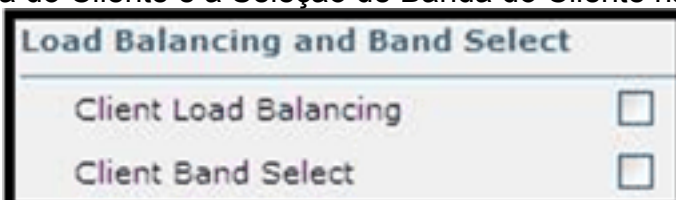


Notas:

- A Detecção de Buraco de Cobertura não deve ser habilitada.
- Aironet IE (Elementos de informação) não deve ser habilitado, pois não é usado.
- A Proteção de Quadro de Gerenciamento (MFP - Management Frame Protection) também não é suportada e deve ser desativada ou configurada como opcional, conforme mostrado nesta imagem:



- O Balanceamento de Carga do Cliente e a Seleção de Banda do Cliente não têm suporte e



não devem ser habilitados:

## Contagem de usuários suportados

Apenas quinze usuários podem se conectar nas WLANs da controladora de WLAN fornecidas na série 600 a qualquer momento. Um décimo sexto usuário não pode autenticar até que um dos primeiros clientes cancele a autenticação ou que ocorra um tempo limite na controladora.

**Observação:** esse número é cumulativo nas WLANs da controladora na série 600.

Por exemplo, se duas WLANs da controladora estiverem configuradas e houver quinze usuários em uma das WLANs, nenhum usuário poderá se unir à outra WLAN na série 600 naquele momento. Esse limite não se aplica às WLANs privadas locais que o usuário final configura na série 600, projetadas para uso pessoal, e os clientes conectados a essas WLANs privadas ou às portas com fio não afetam esses limites.

## Gerenciamento e configurações de canal

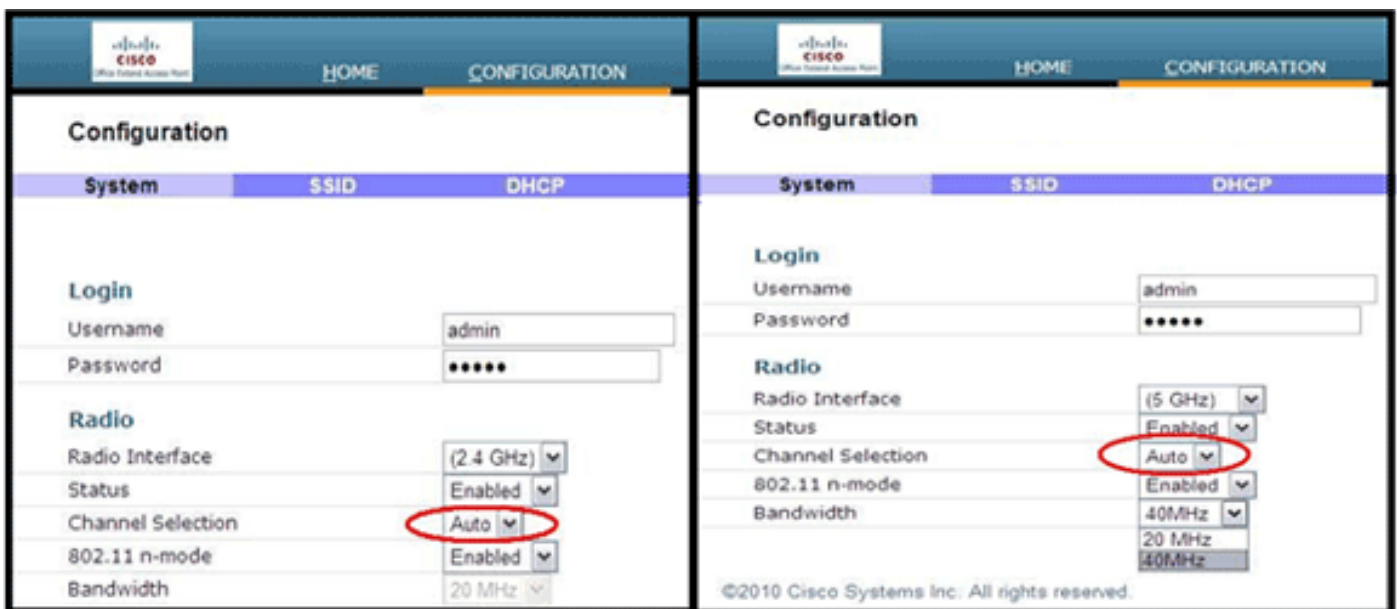
Os rádios para a série 600 são controlados através da GUI local na série 600 e não através do Wireless LAN Controller.

Tentar controlar o canal de espectro, a alimentação ou desativar os rádios através do controlador não terá nenhum efeito sobre a série 600.

A série 600 verificará e escolherá canais para 2,4 GHz e 5,0 GHz durante a inicialização, desde que as configurações padrão na GUI local sejam deixadas como padrão em ambos os espectros.

**Observação:** se o usuário desabilitar um ou ambos os rádios localmente (esse rádio também está desabilitado para acesso corporativo), também como declarado anteriormente, o RRM e recursos avançados como monitor, H-REAP, sniffer estão além dos recursos do Cisco Aironet 600 Series OEAP, que está posicionado para uso doméstico e de trabalhadores à distância.

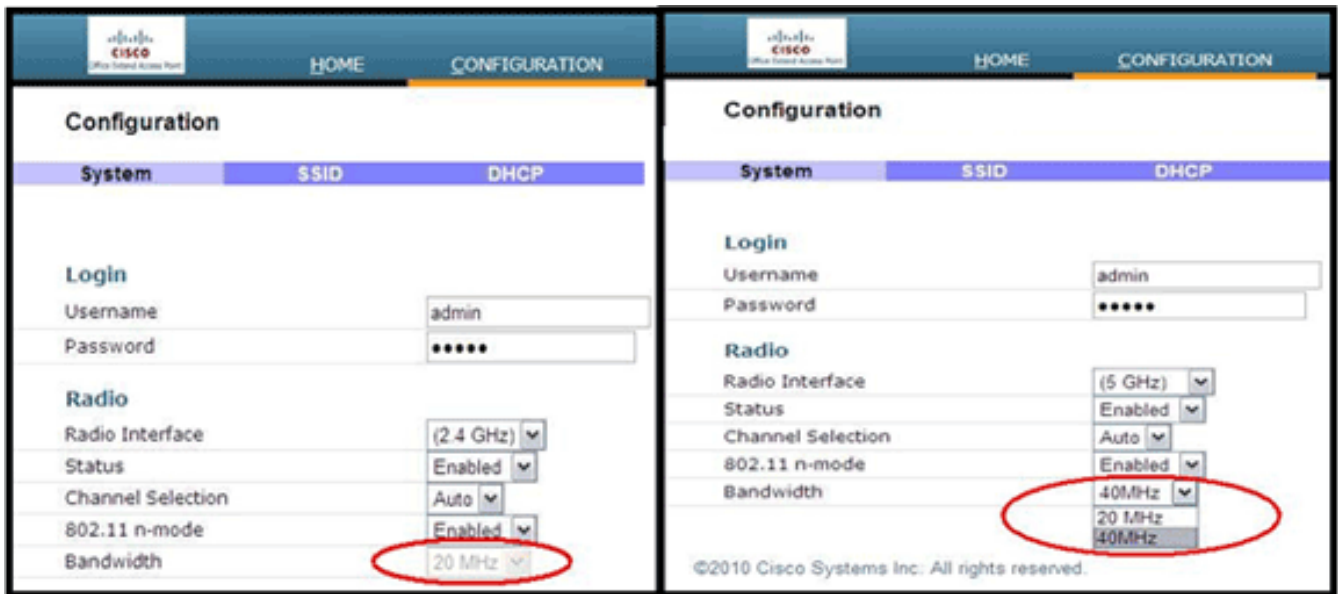
A seleção de canal e a largura de banda para 5,0 GHz são configuradas aqui na GUI local do Cisco Aironet 600 Series OEAP.



### Notas:

- Configurações de largura de 20 e 40 MHz estão disponíveis para 5 GHz.
- 2,4 GHz 40 MHz de largura não é suportado e é fixado em 20 MHz.
- A largura de 40 MHz (combinação de canais) não é suportada em 2,4 GHz.





## Avisos adicionais

O Cisco Aironet 600 Series OEAP é projetado para implantações de AP único. Portanto, o roaming de clientes entre a série 600 não é suportado.

**Observação:** desabilitar o 802.11a/n ou 802.11b/g/n no controlador pode não desabilitar esses espectros no Cisco Aironet 600 Series OEAP porque o SSID local ainda pode estar funcionando.

O usuário final habilita/desabilita o controle sobre os rádios dentro do Cisco Aironet 600 Series OEAP.



## Suporte 802.1x na porta com fio

Nesta versão inicial, o 802.1x só é suportado na Interface de Linha de Comando (CLI).

**Observação:** o suporte à GUI ainda não foi adicionado.

Esta é a porta com fio (porta #4 em amarelo) na parte traseira do Cisco Aironet 600 Series OEAP e está ligada à LAN remota (consulte a seção anterior sobre configuração de LAN remota).

A qualquer momento, você pode usar o comando **show** para exibir a configuração de LAN remota atual:

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

Para alterar a configuração da LAN remota, você deve primeiro desabilitá-la:

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

Habilitar a autenticação 802.1X para a LAN remota:

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

Você pode desfazê-lo usando este comando:

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

Para a LAN remota, "Encryption" é sempre "None" (como exibido em **show remote-lan**) e não configurável.

Se quiser usar EAP local (no controlador) como servidor de autenticação:

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

Onde o `perfil` é definido através da GUI da controladora (Security > Local EAP) ou da CLI (**config local-auth**). Consulte o guia da controladora para obter detalhes sobre esse comando.

Você pode desfazê-lo com este comando:

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

Ou, se você usar um servidor de autenticação AAA externo:

- **config remote-lan radius\_server auth add/delete <remote-lan-id> <server-id>**
- **config remote-lan radius\_server auth enable/disable <remote-lan-id>**

Onde `server` é configurado através da GUI do controlador (Security > RADIUS > Authentication) ou CLI (**config radius auth**). Consulte o guia da controladora para obter mais informações sobre esse comando.

Depois de concluir a configuração, ative a LAN remota:

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

Use o comando **show remote-lan <remote-lan-id>** para verificar sua configuração.

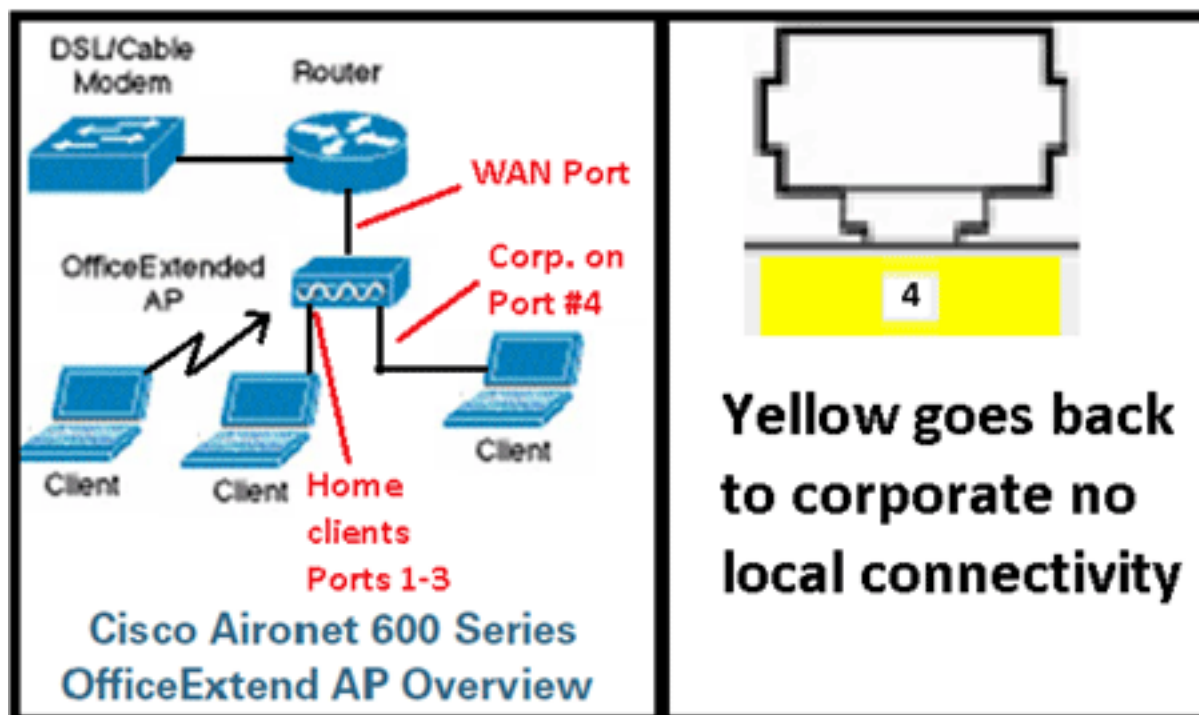
Para o cliente LAN remoto, você precisa habilitar a autenticação 802.1X e configurar de forma



correspondente. Consulte o guia do usuário do dispositivo.

## Configuração do ponto de acesso OEAP-600

Esta imagem mostra o diagrama de cabeamento para o Cisco Aironet 600 Series OEAP:



O escopo de DHCP padrão do Cisco Aironet 600 Series OEAP é 10.0.0.x para que você possa navegar até o AP nas portas 1-3 usando o endereço 10.0.0.1. O nome de usuário e a senha padrão são admin.

**Observação:** isso é diferente dos AP1040, 1130, 1140 e 3502i que usavam Cisco como nome de usuário e senha.

Se os rádios estiverem ativos e um SSID pessoal já tiver sido configurado, você poderá acessar a tela de configuração sem fio. Caso contrário, você precisará usar as portas Ethernet locais de 1 a 3.

Para fazer login, o nome de usuário e a senha padrão são admin.



## Office Extend Access Point

Enter

© 2005-2008 Cisco Systems  
Cisco Systems, Inc. Cisco, Cisco Systems and Cisco  
affiliates in the U.S. and other countries.

### Windows Security

The server 10.0.0.1 at Cisco Office Extend AP requires a username and password.

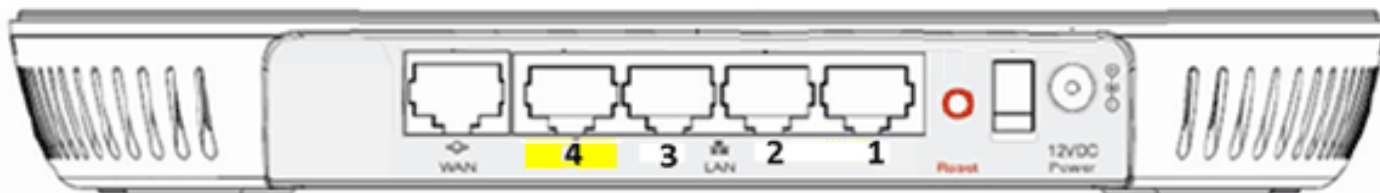
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

 Remember my credentials

OK

Cancel

**Observação:** o #4 da porta amarela não está ativo para uso local. Se uma LAN remota estiver configurada no controlador, essa porta retorna ao túnel depois que o AP se une com êxito ao controlador. Para navegar até o dispositivo, use localmente as portas 1-3:



Depois de navegar com êxito até o dispositivo, você verá a tela de status inicial. Esta tela fornece estatísticas de rádio e MAC. Se os rádios não tiverem sido configurados, a tela de configuração permitirá que o usuário ative os rádios, defina canais e modos, configure SSIDs locais e ative as configurações da WLAN.

**Configuration** Apply

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

**Login**

Username: admin  
 Password: \*\*\*\*

**Radio**

Radio Interface: 2.4 GHz ⓘ Select Each Radio and Configure Independently  
 Status: Enabled  
 Channel Selection: Auto  
 802.11 n-mode: Enabled ⓘ 802.11n is not supported with TKIP-only WPA Encryption  
 Bandwidth: 20 MHz

Na tela SSID, é onde o usuário pode configurar a rede WLAN pessoal. O SSID do rádio corporativo e os parâmetros de segurança são configurados e removidos do controlador (depois que você configura a WAN com o IP do controlador), e ocorreu uma junção bem-sucedida.

Esta imagem mostra uma configuração de filtragem de MAC local de SSID:

**Configuration** Apply

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

**Personal Network**

Band Selection: 2.4 GHz ⓘ Select Each Radio and Configure SSID Individually  
 Enabled:   
 Broadcast:   
 SSID: EVORA24 ⓘ Personal SSID should be different from Corporate SSID

**MAC Filter**

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


Depois que o usuário configura o SSID pessoal, a tela abaixo permite que o usuário configure a segurança no SSID residencial privado, ative rádios e configure a filtragem MAC, se desejado. Se a rede pessoal estiver usando taxas de 802.11n, é recomendável que o usuário escolha um tipo de autenticação, um tipo de criptografia e uma senha para habilitar WPA2-PSK e AES.

**Observação:** essas configurações de SSID serão diferentes das configurações corporativas se o usuário optar por desativar um ou ambos os rádios (ambos também são desativados para uso

corporativo).

Os usuários que têm acesso local às configurações de controle do administrador têm controle sobre as funções principais, como habilitar/desabilitar o rádio, a menos que o dispositivo seja protegido por senha e configurado pelo administrador. Portanto, deve-se tomar cuidado para não desativar ambos os rádios, pois isso pode resultar em perda de conectividade mesmo se o dispositivo se unir com êxito ao controlador.

Esta imagem mostra as configurações de segurança do sistema:

Security	
WPA-PSK	Disabled ▼
WPA2-PSK	Enabled ▼
WEP Encryption	Disabled ▼
WPA Encryption	AES ▼
WPA passphrase	••••• <a href="#">Click here to display</a>
Network Key 1	
Network Key 2	
Network Key 3	
Network Key 4	
Current Network Key	2 ▼

Espera-se que o funcionário remoto doméstico instale o Cisco Aironet 600 Series OEAP atrás de um roteador residencial, pois esse produto não foi projetado para substituir a funcionalidade de um roteador residencial. Isso ocorre porque a versão atual deste produto não tem suporte a firewall, suporte a PPPoE ou encaminhamento de portas. Esses são recursos que os clientes esperam encontrar em um roteador residencial.

Embora esse produto possa funcionar sem um roteador residencial, é recomendável não posicioná-lo dessa maneira pelas razões apresentadas. Além disso, pode haver problemas de compatibilidade se conectando diretamente a alguns modems.

Considerando que a maioria dos roteadores residenciais tem um escopo de DHCP no intervalo 192.168.x.x, esse dispositivo tem um escopo de DHCP padrão de 10.0.0.x e é configurável.

Se o roteador doméstico estiver usando 10.0.0.x, você deverá configurar o Cisco Aironet 600 Series OEAP para usar um 192.168.1.x ou um endereço IP compatível para evitar conflitos de rede.

Esta imagem mostra uma configuração de escopo DHCP:

The screenshot shows the Cisco configuration interface with the 'CONFIGURATION' tab selected. Under the 'DHCP' section, the 'Local DHCP' settings are displayed in a table format.

System	SSID	DHCP	WAN
<b>Local DHCP</b>			
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		

**Cuidado:** se o Cisco Aironet 600 Series OEAP não for preparado ou configurado pelo administrador de TI, o usuário precisará inserir o endereço IP do controlador corporativo (veja abaixo) para que o AP possa se unir com êxito ao controlador. Após uma junção bem-sucedida, o AP deve baixar a imagem mais recente do controlador e os parâmetros de configuração, como as configurações de WLAN corporativas. Além disso, se configurada, a porta com fio das configurações de LAN remota #4 na parte traseira do Cisco Aironet 600 Series OEAP.

Se ele não se unir, verifique se o endereço IP do controlador pode ser acessado via Internet. Se a filtragem de endereços MAC estiver habilitada, verifique se o endereço MAC foi inserido com êxito no controlador.

Esta imagem mostra o endereço IP do controlador OEAP Cisco Aironet 600 Series:

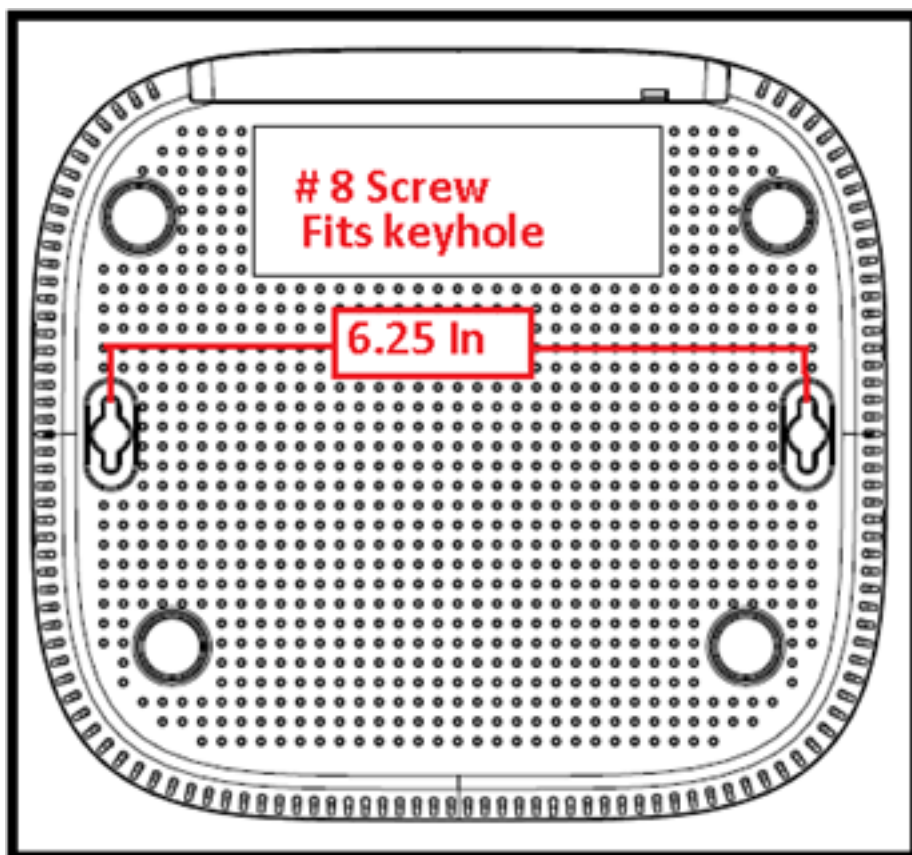




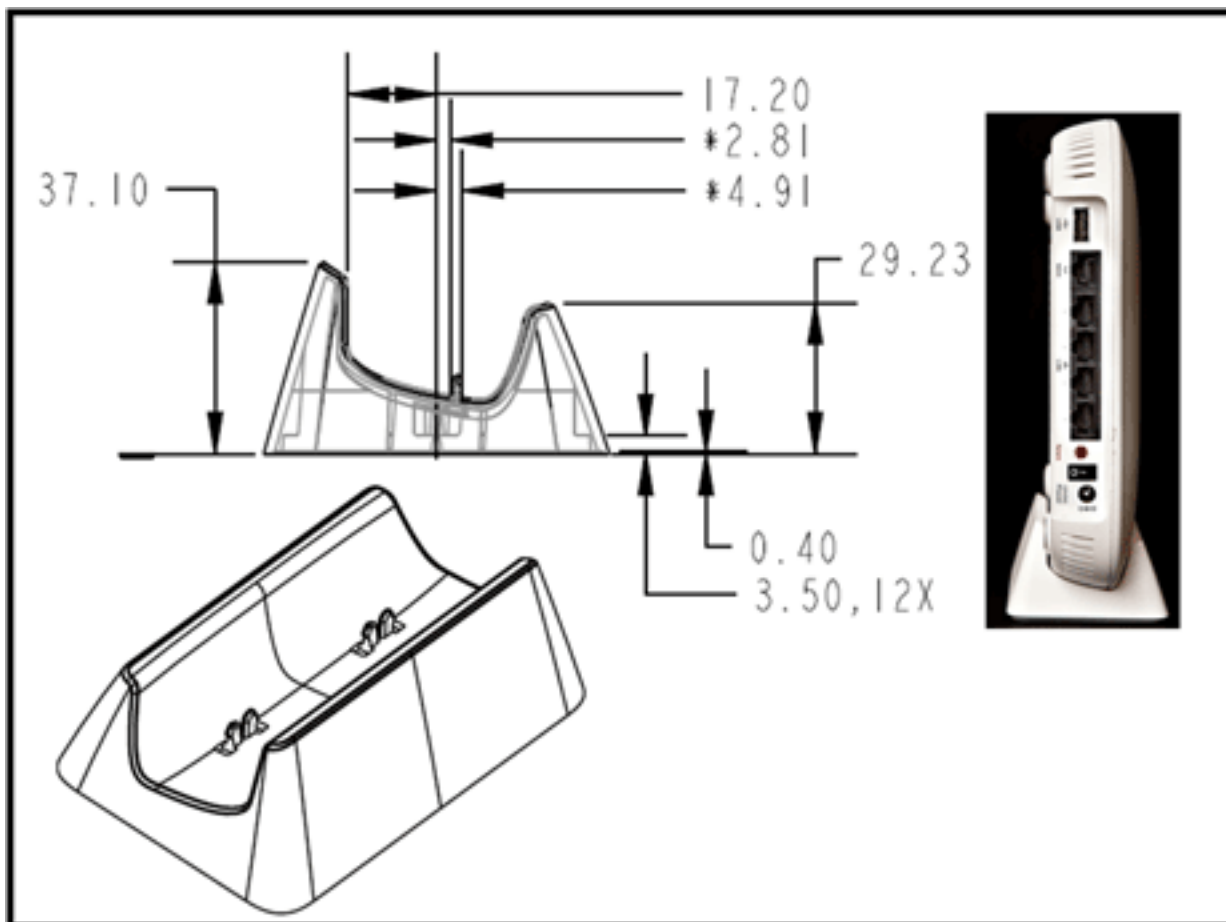
localizar o AP o mais próximo possível dos usuários pretendidos. Evite áreas com grandes superfícies metálicas, como sentar o dispositivo em uma mesa de metal ou perto de um espelho grande. Quanto mais paredes e objetos entre o AP e o usuário resultarem em menor intensidade de sinal e poderão reduzir o desempenho.

**Observação:** este AP utiliza uma fonte de alimentação de +12 Volts e não utiliza Power over Ethernet (PoE). Além disso, o dispositivo não fornece PoE. Verifique se o adaptador de energia correto está sendo usado com o AP. Além disso, certifique-se de não usar outros adaptadores de outros dispositivos, como laptops e telefones IP, pois eles podem danificar o AP.

A unidade pode ser montada na parede com âncoras plásticas ou parafusos de madeira.



A unidade pode ser montada na vertical usando o suporte fornecido.



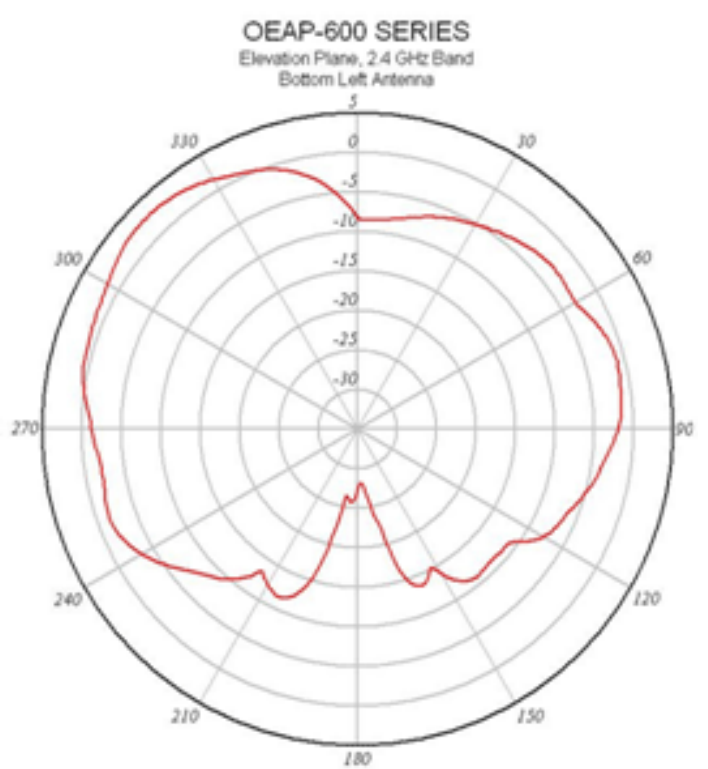
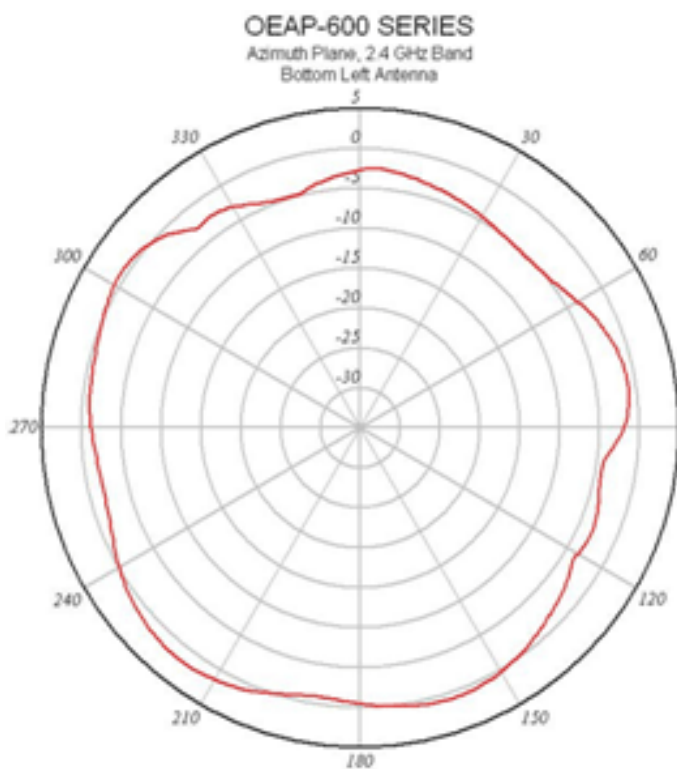
O Cisco Aironet 600 Series OEAP tem antenas localizadas nas bordas do AP. O usuário deve tomar cuidado para não colocar o AP em áreas próximas a objetos metálicos ou obstruções que possam fazer com que o sinal se torne direcional ou diminua. O ganho da antena é de aproximadamente 2 dBi em ambas as bandas e projetado para irradiar em um padrão de 360 graus. Semelhante a uma lâmpada (sem uma sombra de lâmpada), o objetivo é irradiar em todas as direções. Pense no AP como você faria com uma lâmpada e tente colocá-lo próximo aos usuários.

Objetos de metal, como espelhos, obstruem o sinal de forma muito parecida com a analogia da lâmpada. Você pode experimentar throughput ou alcance degradado se o sinal precisar penetrar ou atravessar objetos sólidos. Se você espera conectividade, por exemplo, em uma casa de três andares, evite colocar o AP no porão e tente montar o AP em um local central dentro da casa.

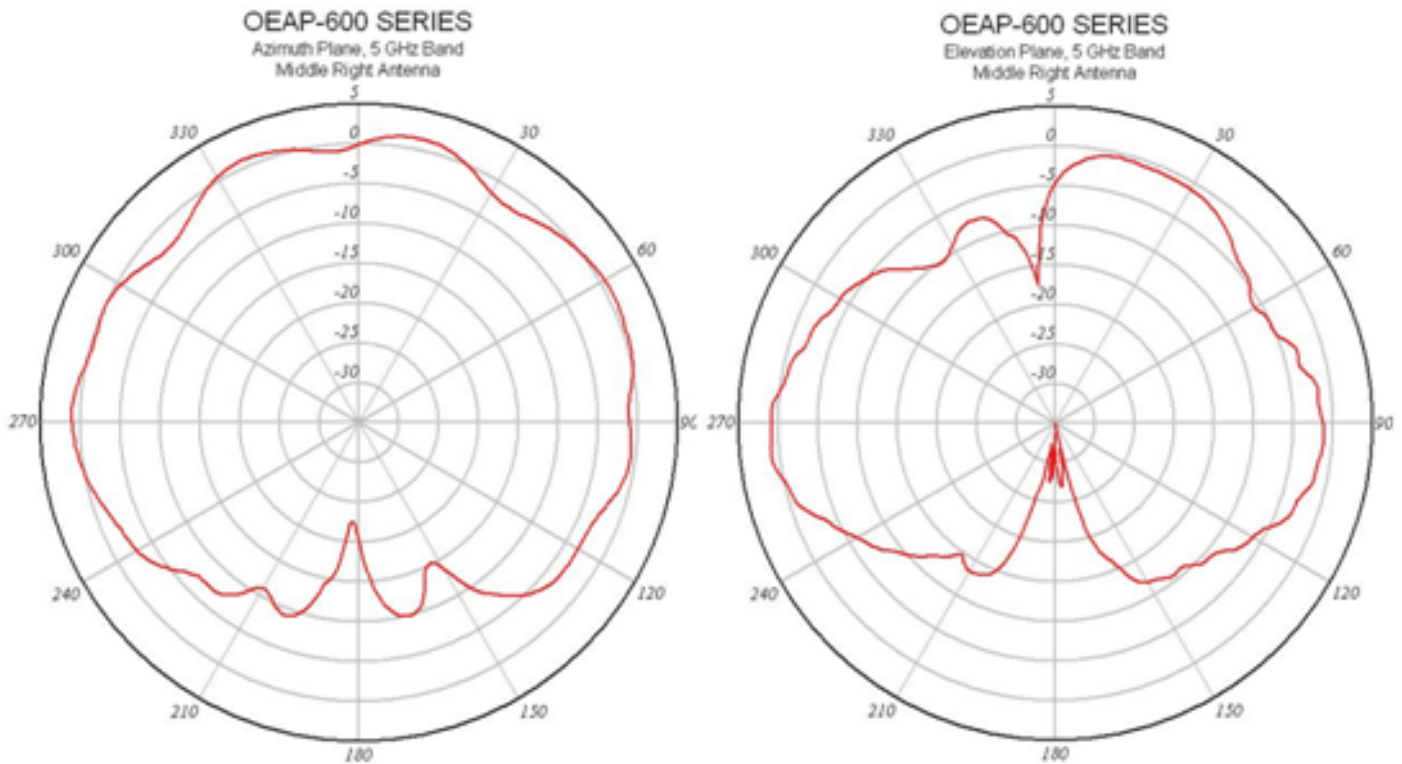
O access point tem seis antenas (três por banda).



Esta imagem mostra um padrão de radiação da antena de 2,4 GHz (tirado da antena inferior esquerda).



Esta imagem mostra um padrão de radiação da antena de 5 GHz (tirado da antena do meio à direita):



## [Troubleshooting do OEAP-600](#)

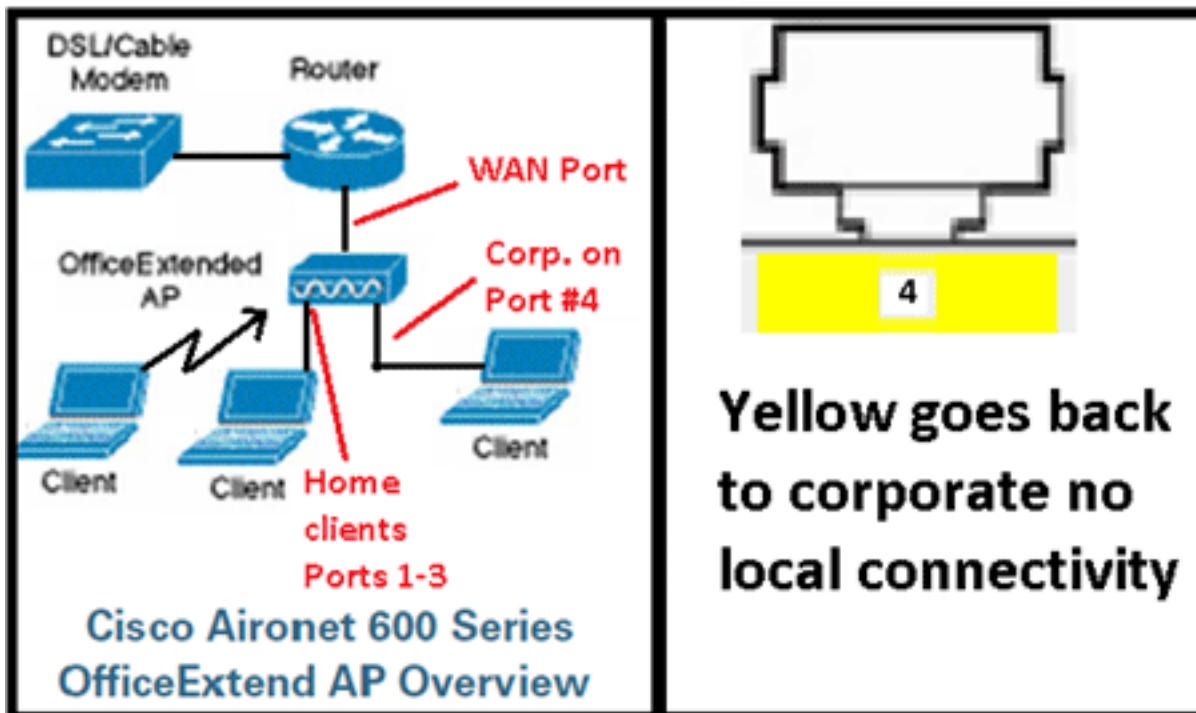
Verifique se o cabeamento inicial está correto. Isso confirma que a porta WAN no Cisco Aironet 600 Series OEAP está conectada ao roteador e pode receber um endereço IP com êxito. Se o AP não parecer se unir à controladora, conecte um PC à porta 1-3 (portas de cliente doméstico) e veja se você pode navegar até o AP usando o endereço IP padrão de 10.0.0.1. O nome de usuário e a senha padrão são admin.

Verifique se o endereço IP do controlador corporativo está definido. Caso contrário, insira o endereço IP e reinicialize o Cisco Aironet 600 Series OEAP para que ele possa tentar estabelecer um link para o controlador.

**Observação:** o #4 da porta corporativa (em amarelo) não pode ser usado para navegar até o dispositivo para fins de configuração. Essa é essencialmente uma "porta inoperante", a menos que uma LAN remota seja configurada. Em seguida, ela será encapsulada de volta para a empresa (usada para conectividade corporativa com fio)

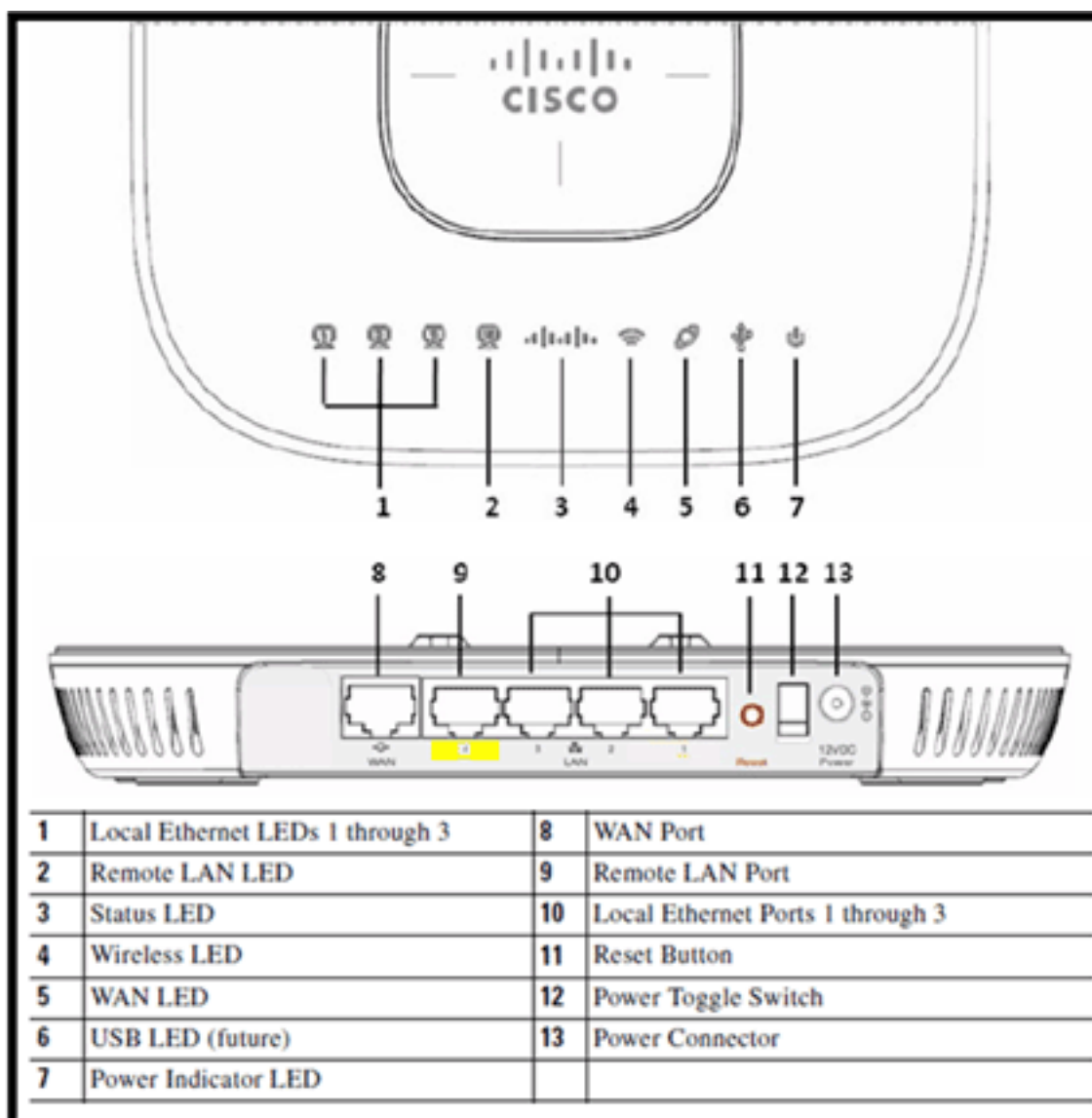
Verifique o log de eventos para ver como a associação progrediu (mais sobre isso posteriormente).

Esta imagem mostra o diagrama de cabeamento do Cisco Aironet 600 Series OEAP:



Yellow goes back to corporate no local connectivity

Esta imagem mostra as portas de conectividade do Cisco Aironet 600 Series OEAP:

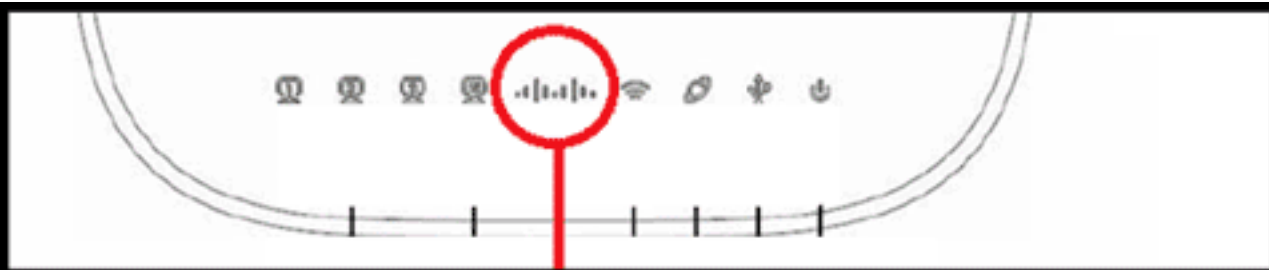




Se o OEAP Cisco Aironet 600 Series falhar ao se unir ao controlador, é recomendável que você verifique estes itens:

1. Verifique se o roteador está funcionando e conectado à porta WAN do Cisco Aironet 600 Series OEAP.
2. Conecte um PC a uma das portas 1-3 no Cisco Aironet 600 Series OEAP. Ele deve ver a Internet.
3. Verifique se o endereço IP do controlador corporativo está no AP.
4. Confirme se o controlador está na DMZ e se pode ser acessado via Internet.
5. Verifique se a junção e confirme se o LED do logotipo da Cisco está azul ou roxo estável.
6. Aguarde tempo suficiente caso o AP precise carregar uma nova imagem e reiniciar.
7. Se um firewall estiver em uso, verifique se as portas UDP 5246 e 5247 não estão bloqueadas.

Esta imagem mostra o status do LED do logotipo do Cisco Aironet 600 Series OEAP:



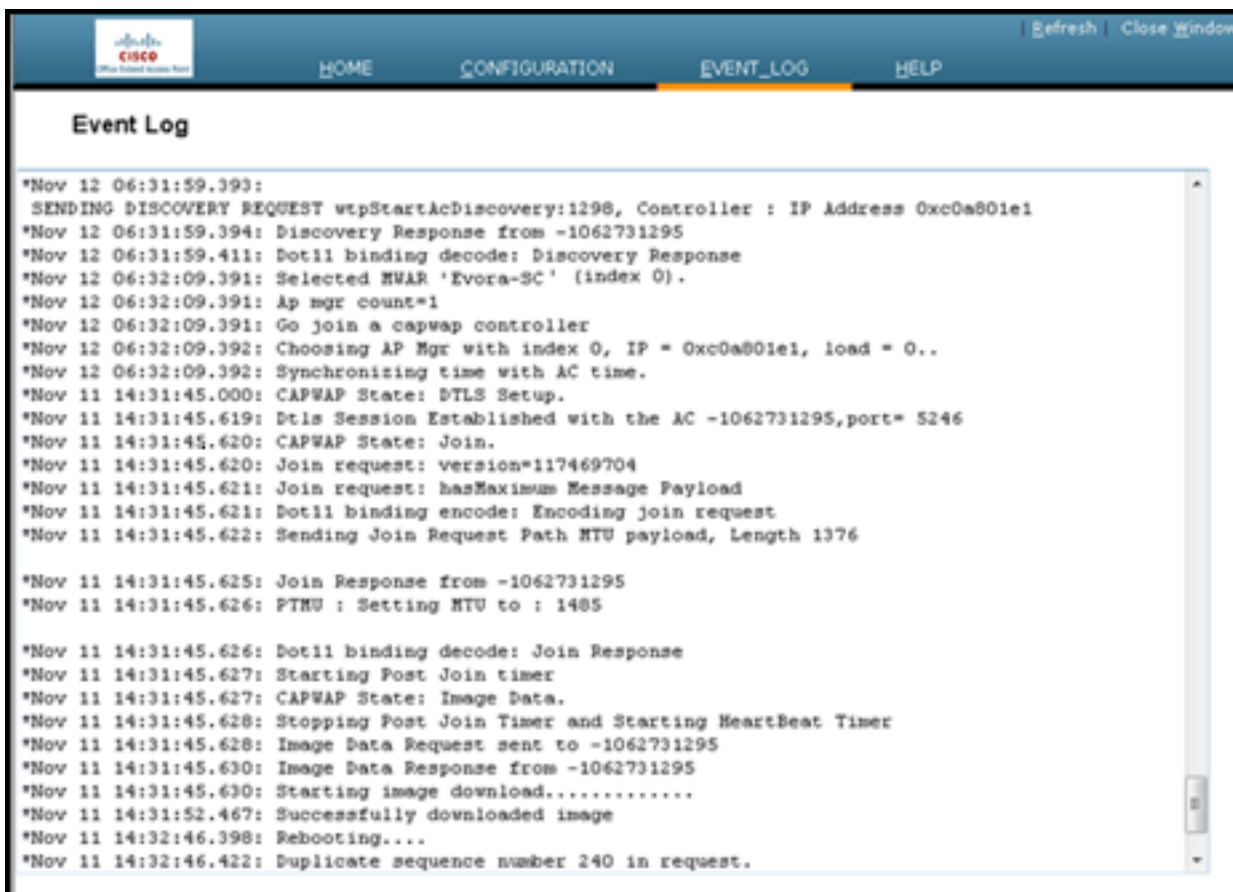
**Understanding Cisco Aironet 600 Series OfficeExtend AP LEDs**

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.

Se o processo de junção falhar, o LED percorre o ciclo de cores ou pisca em laranja. Se isso ocorrer, verifique o log de eventos para obter mais detalhes. Para acessar o registro de eventos, navegue até o AP (usando o SSID pessoal ou as portas com fio 1-3) e capture esses dados para que o administrador de TI analise.

Esta imagem mostra o log de eventos do Cisco Aironet 600 Series OEAP:





Se o processo de junção falhar e esta for a primeira vez que o Cisco Aironet 600 Series OEAP tenta se conectar ao controlador, verifique as estatísticas de junção do AP para o Cisco Aironet 600 Series OEAP. Para fazer isso, você precisa do MAC de rádio base do AP. Isso pode ser encontrado no registro de eventos. Aqui está um exemplo de um log de eventos com comentários para ajudá-lo a interpretar isso:

**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 08:00:05.421:      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: oeap_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-COC1C0054886/emailAd
  
```

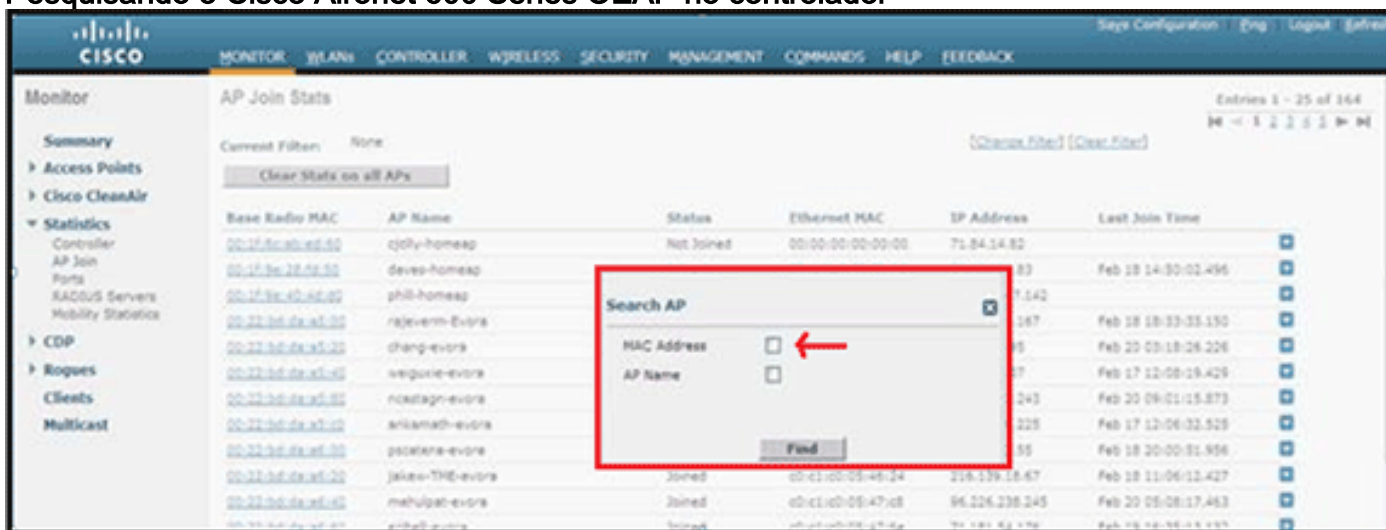
**Controller IP address configured in local GUI**

**certificate**

Quando isso for conhecido, você poderá examinar as estatísticas do monitor do controlador para determinar se o Cisco Aironet 600 Series OEAP se uniu ao controlador ou se já se uniu ao controlador. Além disso, isso deve fornecer uma indicação sobre o motivo ou se ocorreu uma falha.

Se a autenticação do AP for necessária, verifique se o endereço MAC Ethernet do Cisco Aironet 600 Series OEAP (não o endereço MAC do rádio) foi inserido no servidor Radius em letras minúsculas. Você também pode determinar o endereço MAC Ethernet a partir do registro de eventos.

## Pesquisando o Cisco Aironet 600 Series OEAP no controlador



Base Radio MAC	AP Name	Status	Ethernet MAC	IP Address	Last Join Time
00:12:00:00:00:00	q0ly-homeap	Not Joined	00:00:00:00:00:00	71.84.14.82	
00:12:00:00:00:00	devo-homeap			83	Feb 18 14:30:02.496
00:12:00:00:00:00	phil-homeap			1,042	
00:12:00:00:00:00	rajewm-evora			167	Feb 18 18:33:33.150
00:12:00:00:00:00	chang-evora			65	Feb 20 03:18:28.226
00:12:00:00:00:00	wegune-evora			57	Feb 17 12:08:19.429
00:12:00:00:00:00	nostagn-evora			243	Feb 20 09:01:15.873
00:12:00:00:00:00	arismad-evora			225	Feb 17 12:06:32.525
00:12:00:00:00:00	psatara-evora			55	Feb 18 20:00:51.956
00:12:00:00:00:00	jakeo-THÉ-evora	Joined	00:12:00:00:00:00	215.139.18.67	Feb 18 11:06:12.427
00:12:00:00:00:00	mehupal-evora	Joined	00:12:00:00:00:00	96.226.238.245	Feb 20 05:08:17.463
00:12:00:00:00:00	enilb-evora	Joined	00:12:00:00:00:00	76.181.83.176	Feb 18 18:35:19.197

Se você determinou que a Internet é acessível de um PC conectado à porta Ethernet local, mas o AP ainda não pode se unir ao controlador, e você confirmou que o endereço IP do controlador está configurado na GUI do AP local e está acessível, confirme se o AP já se uniu com êxito. Talvez o AP não esteja no servidor AAA. Ou, se o handshake DTLS falhar, o AP pode ter um certificado incorreto ou erro de data/hora no controlador.

Se nenhuma unidade Cisco Aironet 600 Series OEAP puder se unir ao controlador, verifique se o controlador está no DMZ e se pode ser alcançado e se as portas UDP 5246 e 5247 estão abertas.

## [Como depurar problemas de associação de cliente](#)

O AP ingressa no controlador corretamente, mas o cliente sem fio não pode se associar ao SSID corporativo. Verifique o registro de eventos para ver se uma mensagem de associação alcança o AP.

A próxima figura mostra os eventos normais para a associação do cliente com o SSID corporativo com WPA ou WPA2. Para o SSID com autenticação aberta ou WEP estático, há apenas um evento `ADD MOBILE`.

## Registro de eventos - Associação do cliente

```
*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
```

Se o evento (Re)Assoc-Req não estiver no log, verifique se o cliente tem as configurações de segurança corretas.

Se o evento (Re)Assoc-Req aparecer no registro, mas o cliente não puder se associar corretamente, ative o comando **debug client <endereço MAC>** no controlador do cliente e investigue o problema da mesma forma que um cliente que trabalha com outros pontos de acesso Cisco não OEAP.

### [Como interpretar o registro de eventos](#)

Os seguintes registros de eventos com comentários podem ajudá-lo a solucionar outros problemas de conexão do Cisco Aironet 600 Series OEAP.

Aqui estão alguns exemplos coletados dos arquivos de log de eventos do Cisco Aironet 600 Series OEAP com comentários para ajudar na interpretação do log de eventos:



## 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: **Discovery Request sent if AP can not get IP address, then Discovery Req. will not be sent**  
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. **Selected controller to join, timestamp synced to the controller**  
\*Jan 01 08:00:19.183: Synchronizing time with AC time. **DTLS handshaking with the controller completed. If certificate has problem, then the failure will happen here**  
\*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

## 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** **Join Resp. from controller If AP is not added to AAA server, this step will fail.**  
\*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 **Controller and AP have same version SW, no image download is need. When controller is upgraded to new version SW, image download will happen.**  
\*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: hwapp\_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. **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

### Quando a conexão com a Internet não parecer confiável

O exemplo de log de eventos nesta seção pode ocorrer quando a conexão com a Internet falha ou acaba sendo muito lenta ou intermitente. Isso pode ser causado pela rede do ISP, pelo modem do ISP ou pelo roteador residencial. Às vezes, a conectividade do ISP cai ou se torna não confiável. Quando isso ocorre, o link CAPWAP (túnel de volta para a empresa) pode falhar ou ter dificuldade.

Aqui está um exemplo de uma falha no registro de eventos:

```
*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...
```

### Comandos debug adicionais

Ao usar o Cisco Aironet 600 Series OEAP em um hotel ou outro local de pagamento pelo uso, antes que o Cisco Aironet 600 Series OEAP possa fazer o túnel de volta para o controlador, você precisa atravessar o jardim murado. Para fazer isso, conecte um notebook a uma das portas locais com fio (portas 1 a 3) ou use um SSID pessoal para fazer login no hotel e atender à tela inicial.

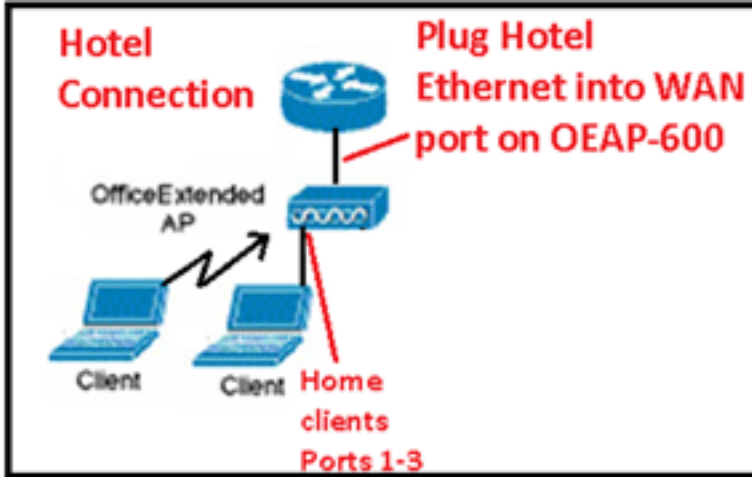
Uma vez que você tenha conectividade com a Internet do lado da casa do AP, a unidade estabelece um túnel DTLS e seus SSIDs corporativos. Em seguida, a porta com fio #4 (supondo que uma LAN remota esteja configurada) se torna ativa.

**Observação:** isso pode levar alguns minutos, observe o LED do logotipo da Cisco para azul sólido

ou roxo para indicar uma junção bem-sucedida. Neste ponto, a conectividade pessoal e corporativa está ativa.

**Observação:** o túnel é interrompido quando um hotel ou outro ISP se desconecta (geralmente 24 horas). Então, você tem que recomençar o mesmo processo. Isso é normal e é por design.

Esta imagem mostra o Office Extend em uma configuração de pagamento para uso:



Esta imagem mostra comandos debug adicionais (informações de interface de rádio):

```
Below are the new diagnostics commands for the OEAP 600
The WLC CLI of "show tech" is:
debug ap enable <apname>
then:
debug ap command "evoraTechSupport" <apname> → the information about system and radio slot 0/1
debug ap command "evoraTechSupport 2" <apname> → more info about radio slot 0 (2.4G)
debug ap command "evoraTechSupport 3" <apname> → more info about radio slot 1 (5G)

The "show eventlog" is the same as other APs:
show ap eventlog <apname>
```

## Problemas conhecidos/Aviso

Quando você carrega o arquivo de configuração de um controlador para um servidor TFTP/FTP, as configurações de LAN remota são carregadas como configurações de WLAN. Consulte [Release Notes para Cisco Wireless LAN Controllers e Lightweight Access Points para Release 7.0.116.0](#) para obter mais informações.

No OEAP-600, se a conexão CAPWAP falhar devido a uma falha de autenticação no controlador, o LED do logotipo da Cisco no OEAP-600 pode desligar por algum tempo antes que o OEAP-600 tente reiniciar a tentativa CAPWAP. Isso é normal, portanto você deve estar ciente de que o AP não morreu se o LED do logotipo apagar momentaneamente.

Este produto OEAP-600 tem um nome de login diferente dos Access Points OEAP anteriores, para ser consistente com os produtos domésticos, como Linksys, o nome de usuário padrão é *admin* com uma senha de *admin*. Os outros Access Points OEAP da Cisco, como o AP-1130 e o AP-1140, têm um nome de usuário padrão *Cisco* com uma senha de *Cisco*.

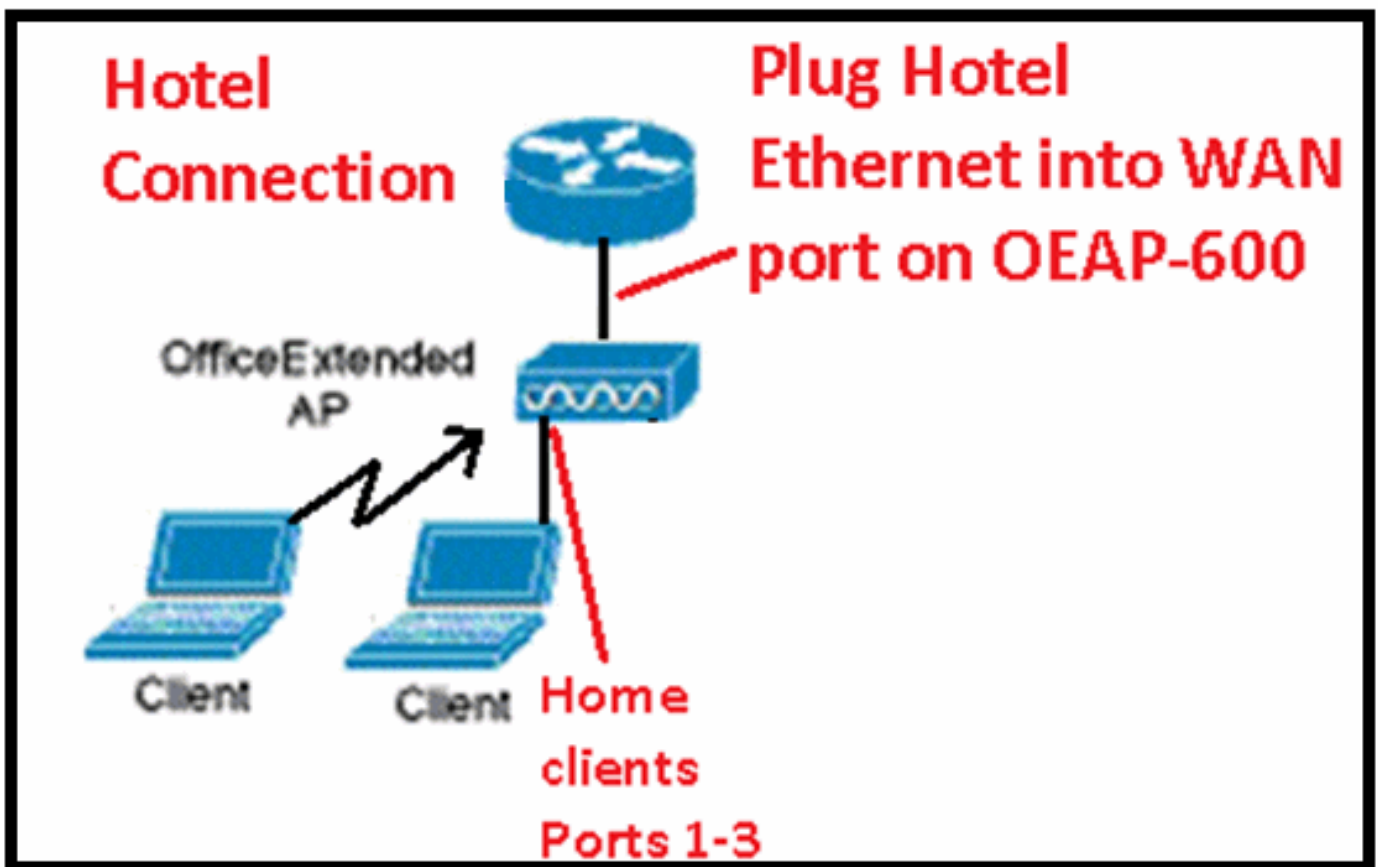


Esta primeira versão do OEAP-600 tem suporte para 802.1x, mas só é suportada na CLI. Os usuários que tentarem fazer alterações na GUI podem perder suas configurações.

Quando você usa o OEAP-600 em um hotel ou outro local de pagamento para uso, antes que o OEAP-600 possa fazer o túnel de volta para o controlador, você precisa passar pelo jardim murado. Basta conectar um notebook a uma das portas locais com fio (porta 1-3) ou usar um SSID pessoal para fazer login no hotel e atender à tela inicial. Uma vez que você tenha conectividade com a Internet a partir do lado da casa do AP, a unidade estabelece um túnel DTLS e seus SSIDs corporativos e #4 de porta com fio, o que pressupõe que a LAN remota esteja configurada e, em seguida, se torne ativa. Observe que isso pode levar alguns minutos, observe o LED do logotipo da Cisco para azul sólido ou roxo para indicar uma associação bem-sucedida. Neste ponto, a conectividade pessoal e corporativa está ativa.

**Observação:** o túnel pode ser interrompido quando o hotel ou outro ISP se desconecta (geralmente 24 horas) e você teria que reiniciar o mesmo processo. Isso é normal e é por design.

#### Escritório Estender local de pagamento para uso

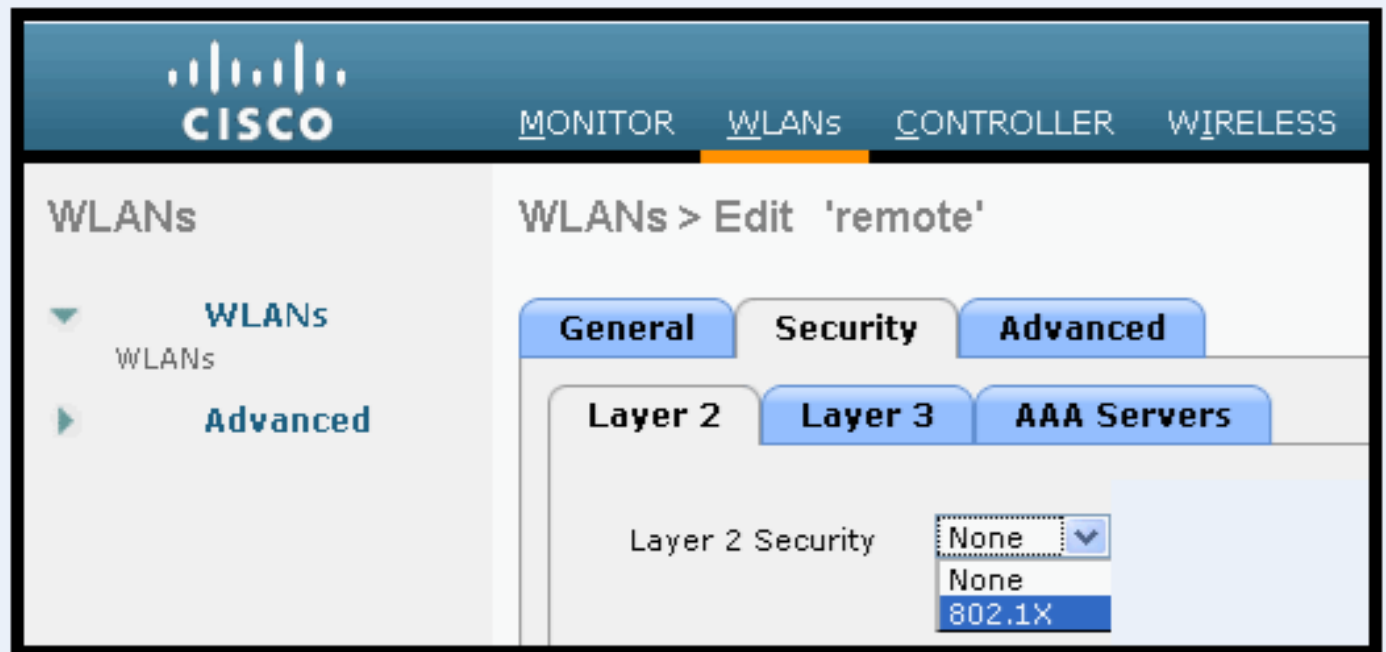


Estes são alguns aprimoramentos adicionais introduzidos na versão 7.2 do Cisco:

- Adição de segurança 802.1x adicionada à GUI
- Capacidade de desabilitar o acesso à WLAN local no AP do controlador - desabilitando o SSID pessoal permitindo apenas a configuração corporativa
- Opções selecionáveis de atribuição de canal
- O suporte mudou de 2 SSID corporativos para 3 SSIDs
- Suporte para recurso de porta RLAN dupla

**Adição de segurança 802.1x adicionada à GUI**

802.1x agora adicionado à GUI



Observações com relação à autenticação da porta LAN remota.

## 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.

Capacidade de desabilitar o acesso à WLAN local no AP do controlador - desabilitando o SSID pessoal permitindo apenas a configuração corporativa

Desabilitar o acesso à WLAN local

The screenshot shows the Cisco WLC configuration interface. The 'Global Configuration' page is active. On the left, the 'Wireless' menu is expanded to 'Access Points' > '802.11a/n'. The main content area is divided into several sections:

- CDP:** A table showing CDP State (checked) and Ethernet/Radio States for interfaces 0-3.
- Login Credentials:** Fields for Username, Password, and Profile Name.
- 802.1x Supplicant Credentials:** A checkbox for 802.1x Authentication.
- AP Failover Priority:** A dropdown menu set to 'Enable'.
- High Availability:** Settings for AP heartbeat timer, discovery timeout, and backup controller names.
- TCP MSS:** A checkbox for Global TCP Adjust MSS.
- AP Retransmit Config Parameters:** Checkboxes for AP Retransmit Count and AP Retransmit Interval.
- GEAP Config Parameters:** A checkbox for 'Disable local APs' which is checked and circled in red.

As opções selecionáveis de atribuição de canal são:

- AP controlado localmente
- WLC controlado

Canal de RF e atribuições de energia agora controladas por WLC ou local

The screenshot shows the configuration page for a specific AP (802.11a/n Cisco APs > Configure). The 'RF Channel Assignment' and 'Tx Power Level Assignment' sections are circled in red:

- RF Channel Assignment:**
  - Current Channel: 64
  - Channel Width: 40 MHz
  - Assignment Method:  WLC Controlled
- Tx Power Level Assignment:**
  - Current Tx Power Level: 1
  - Assignment Method:  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”.

### Suporte para recurso de porta RLAN dupla (somente CLI)

Esta observação se aplica aos APs da série OEAP-600 que usam o recurso de portas de RLAN duplas, que permite que a porta 3 Ethernet OEAP-600 opere como uma LAN remota. A configuração só é permitida através do CLI, e aqui está um exemplo:

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

Caso esse recurso não esteja configurado, a lan remota de porta única 4 continuará a funcionar. Cada porta usa uma lan remota exclusiva para cada porta. O mapeamento da lan remota é diferente, o que depende se o grupo padrão ou os grupos AP são usados.

### Grupo padrão

Se o grupo padrão for usado, uma única LAN remota com um ID de LAN remota par será mapeada para a porta 4. Por exemplo, a lan remota com lan-id 2 remota é mapeada para a porta 4 (no OEAP-600). A lan remota com um ID de lan remota com número ímpar é mapeada para a porta 3 (no OEAP-600).

Como exemplo, considere estas duas lans remotas:

(Cisco Controller) >show remote-lan summary

Number of Remote LANS..... 2

RLAN ID	RLAN Profile Name	Status	Interface Name
2	rlan2	Enabled	management
3	rlan3	Enabled	management

a rlan2 tem um ID de lan remota par numerado, 2, e como tal mapeia para a porta 4. a rlan3 tem um ID de lan remota ímpar 3 e, portanto, mapeia para a porta 3.

## Grupos AP

Se você usar um grupo AP, o mapeamento para as portas OEAP-600 será determinado pela ordem do grupo AP. Para usar um grupo de AP, você deve primeiro excluir todas as LANs e WLANs remotas do grupo de AP e deixá-lo vazio. Em seguida, adicione as duas lans remotas ao grupo AP. Primeiro adicione a LAN remota do AP da porta 3, depois adicione o grupo remoto da porta 4 e, finalmente, adicione qualquer WLAN.

Uma lan remota na primeira posição da lista é mapeada para a porta 3 e a segunda na lista é mapeada para a porta 4, como neste exemplo:

RLAN ID	RLAN Profile Name	Status	Interface Name
2	rlan2	Enabled	management
3	rlan3	Enabled	management

## [Informações Relacionadas](#)

- [Guia de configuração de Cisco Wireless LAN Controller, versão 7.0](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.



Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.