

Guia de implantação do controlador sem fio de ramificações Flex 7500

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Visão geral do produto](#)

[Especificações do produto](#)

[Data Sheet](#)

[Recurso da plataforma](#)

[Inicialização do Flex 7500](#)

[Licenciamento Flex 7500](#)

[Licenciamento de contagem base AP](#)

[Licenciamento de atualização de AP](#)

[Suporte à versão de software](#)

[Pontos de acesso suportados](#)

[Arquitetura FlexConnect](#)

[Vantagens da centralização do tráfego de controle de ponto de acesso](#)

[Vantagens da distribuição do tráfego de dados do cliente](#)

[Modos de operação do FlexConnect](#)

[Requisitos de WAN](#)

[Projeto de rede para filiais sem fio](#)

[Principais requisitos de design](#)

[Overview](#)

[Vantagens](#)

[Recursos Abordando o projeto de rede da filial](#)

[Matriz de suporte IPv6](#)

[Matriz de recursos](#)

[Grupos AP](#)

[Configurações do WLC](#)

[Summary](#)

[Grupos FlexConnect](#)

[Principais objetivos dos grupos FlexConnect](#)

[Configuração do grupo FlexConnect do WLC](#)

[Verificação usando CLI](#)

[Substituição de VLAN FlexConnect](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[Comutação central baseada em VLAN FlexConnect](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[ACL FlexConnect](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[Encapsulamento dividido FlexConnect](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[Tolerância a falhas](#)

[Summary](#)

[Limitações](#)

[Limite do cliente por WLAN](#)

[Objetivo principal](#)

[Limitações](#)

[Configuração de WLC](#)

[Configuração do NCS](#)

[Bloqueio ponto-a-ponto](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[Download de pré-imagem de AP](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[Atualização de imagem do FlexConnect Smart AP](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[Converter automaticamente APs no modo FlexConnect](#)

[Modo manual](#)

[Modo de conversão automática](#)

[Suporte FlexConnect WGB/uWGB para WLANs de switching local](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[Suporte para um número maior de servidores Radius](#)

[Summary](#)

[Procedimento](#)

[Limitações](#)

[Enhanced Local Mode \(ELM\)](#)

[Suporte de acesso para convidados no Flex 7500](#)

[Gerenciamento do WLC 7500 do NCS](#)

[FAQ](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como implementar um controlador de filial sem fio Cisco Flex 7500. O objetivo deste documento é:

- Explicar vários elementos de rede da solução Cisco FlexConnect, juntamente com seu fluxo de comunicação.
- Forneça diretrizes gerais de implantação para projetar a solução de filial sem fio Cisco FlexConnect.
- Explique os recursos de software na versão de código 7.2.103.0 que reforça a base de informações sobre o produto.

Observação: antes da versão 7.2, o FlexConnect era chamado de REAP Híbrido (HREAP). Agora chama-se FlexConnect.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

[Conventions](#)

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

[Visão geral do produto](#)

Figura 1: Cisco Flex 7500



O Cisco Flex 7500 Series Cloud Controller é um controlador de filial altamente escalável para implantações [sem fio](#) em vários locais. Implantado na nuvem privada, o Cisco Flex 7500 Series

Controller estende os serviços sem fio para filiais distribuídas com controle centralizado que reduz o custo total das operações.

O Cisco Flex 7500 Series ([Figura 1](#)) pode gerenciar [access points](#) sem fio em até 500 filiais e permite que os gerentes de TI configurem, gerenciem e solucionem problemas de até 3.000 access points (APs) e 30.000 clientes do data center. O controlador Cisco Flex 7500 Series oferece suporte a acesso seguro para convidados, detecção de invasores para conformidade com o Payment Card Industry (PCI) e voz e vídeo Wi-Fi na filial (comutado localmente).

Esta tabela destaca as diferenças de escalabilidade entre os controladores Flex 7500, WiSM2 e WLC 5500:

Escalabilidade	Flex 7500	WiSM2	WLC 5500
Total de access points	6,000	1000	500
Total de clientes	64,000	15,000	7,000
Máximo de grupos FlexConnect	2000	100	100
Máximo de APs por grupo FlexConnect	100	25	25
Máximo de grupos AP	6000	1000	500

[Especificações do produto](#)

[Data Sheet](#)

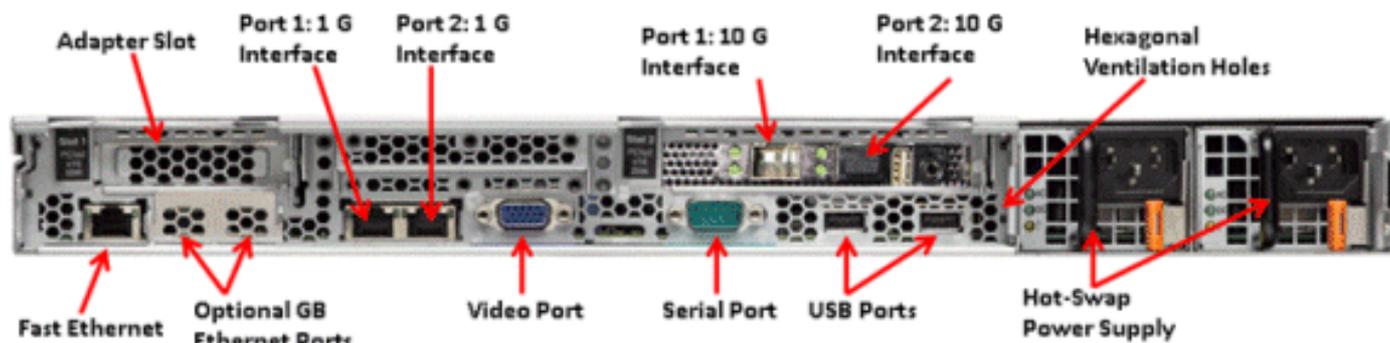
Consulte

http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data_sheet_c78-650053.html.

[Recurso da plataforma](#)

Figura 2: Visão traseira do Flex 7500

Rear View



[Portas de interface de rede](#)

Portas de interface	Uso

Fast Ethernet	Módulo de gerenciamento integrado (IMM)
Porta 1: 1 G	Porta de serviço WLC
Porta 2: 1 G	Porta redundante (RP) WLC
Porta 1: 10G	Interface de gerenciamento WLC
Porta 2: 10G	Porta da interface de gerenciamento de backup WLC (falha de porta)
Portas Ethernet Gb opcionais	N/A

Note:

- O suporte LAG para interfaces 2x10G permite a operação de link ativo-ativo com redundância de link de failover rápida. Um link 10G ativo adicional com LAG não altera o throughput wireless do controlador.
- Interfaces 2x10G
- As interfaces 2x10G suportam apenas cabos óticos com SFP Product # SFP-10G-SR.
- Produto SFP do lado do switch nº X2-10GB-SR

[Endereços MAC do sistema](#)

Porta 1: 10G (Interface de gerenciamento)	Endereço MAC do sistema/base
Porta 2: 10G (Backup Management Interface, interface de gerenciamento de backup)	Endereço MAC base + 5
Porta 1: 1G (Porta de serviço)	Endereço MAC base + 1
Porta 2: 1G (porta redundante)	Endereço MAC básico + 3

[Redirecionamento do console serial](#)

O WLC 7500 permite o redirecionamento do console por padrão à taxa de baud de 9600, simulando o terminal Vt100 sem controle de fluxo.

[Informações do inventário](#)

Figura 3: Console do WLC 7500

```
(Cisco Controller) >show inventory
```

```
Burned-in MAC Address..... E4:1F:13:65:DB:6C
Maximum number of APs supported..... 2000
NAME: "Chassis" , DESCR: "Cisco Wireless Controller"
PID: AIR-CT7510-K9, VID: V01, SN: KQZZXWL
```

A tabela DMI (Desktop Management Interface) contém informações de hardware e BIOS do servidor.

O WLC 7500 exibe a versão do BIOS, PID/VID e número de série como parte do inventário.

Inicialização do Flex 7500

As opções do carregador de inicialização da Cisco para manutenção de software são idênticas às plataformas de controlador existentes da Cisco.

Figura 4: Ordem de inicialização

```
Cisco Bootloader (Version      )

      .o88b. d8888888b .d8888. .o88b. .d88b.
d8P  Y8   `88'  88'  YP d8P  Y8  .8P  Y8.
8P      88   `8bo.  8P      88   88
8b      88   `Y8b.  8b      88   88
Y8b  d8   .88.   db   8D Y8b  d8  `8b  d8'
`Y88P' Y888888P `8888Y' `Y88P' `Y88P'

Booting Primary Image...
Press <ESC> now for additional boot options...

      Boot Options

Please choose an option from below:

1. Run primary image (Version      ) (default)
2. Run backup image (Version      )
3. Manually upgrade primary image
4. Change active boot image
5. Clear Configuration
```

Figura 5: Assistente de configuração de WLC

```
Would you like to terminate autoinstall? [yes]:
System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max): admin
Default values (admin or Cisco or its variants) in password is not allowed.
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password          : *****

Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1 ← Management Port 1: 10G
Management Interface DHCP Server IP Address: 172.20.227.161

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: mobility

Network Name (SSID): DataCenter

Configure DHCP Bridging Mode [yes][NO]: NO

Allow Static IP Addresses [YES][no]: Yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 09/02/10
Enter the time in HH:MM:SS format: 11:50:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

Observação: a sequência de inicialização do Flex 7500 é equivalente e consistente com as plataformas de controlador existentes. A inicialização inicial requer a configuração da WLC usando o Assistente.

[Licenciamento Flex 7500](#)

[Licenciamento de contagem base AP](#)

SKUs de contagem base de AP

300
500
1000
2000
3000
6000

[Licenciamento de atualização de AP](#)

SKUs de atualização de AP
100
250
500
1000

Com exceção das contagens de base e atualização, todo o procedimento de licenciamento que cobre pedidos, instalação e visualização é semelhante ao WLC 5508 atual da Cisco.

Consulte o [guia de configuração do WLC 7.3](#), que abrange todo o procedimento de licenciamento.

[Suporte à versão de software](#)

O Flex 7500 suporta apenas o código WLC versão 7.0.116.x e posterior.

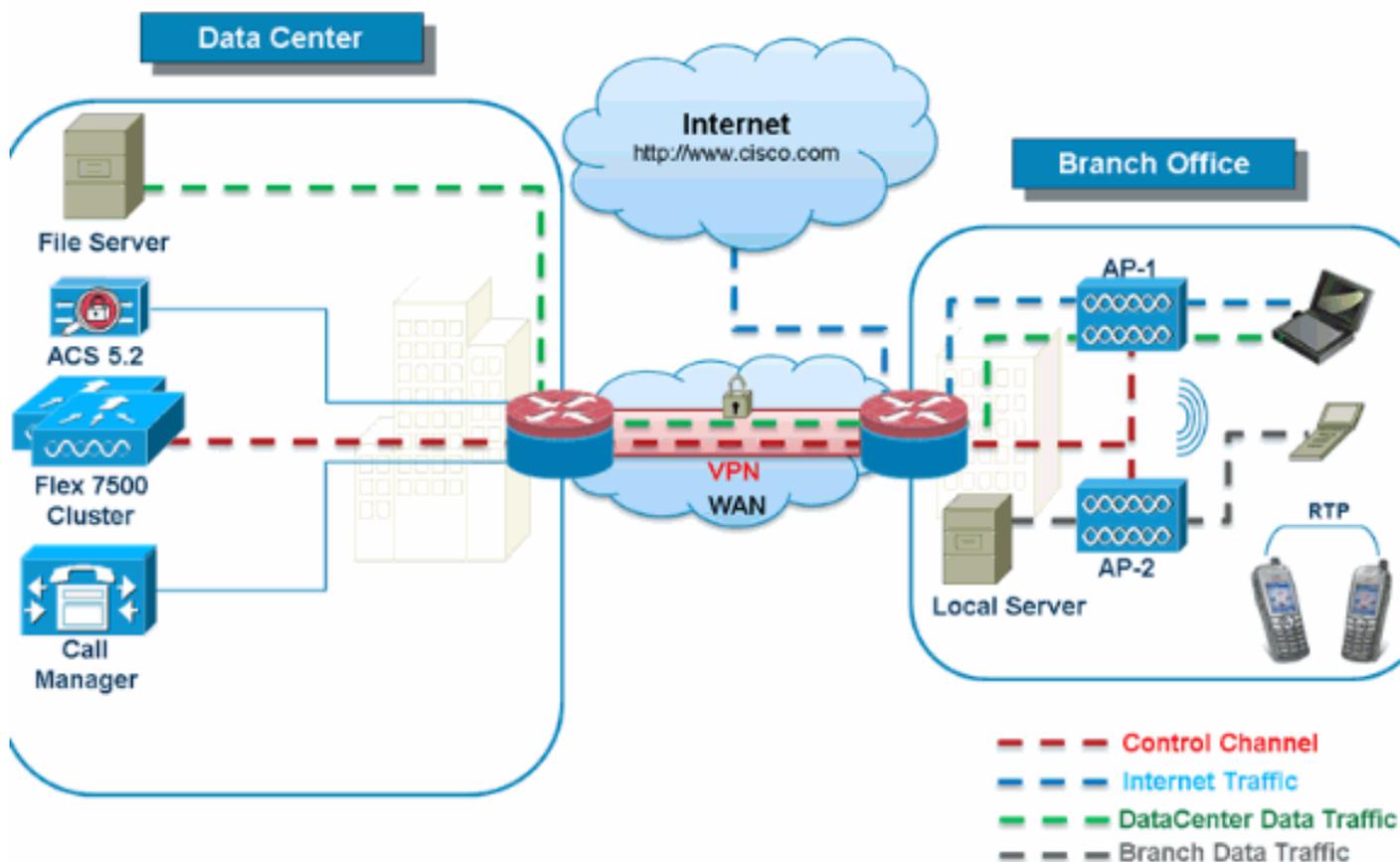
[Pontos de acesso suportados](#)

Pontos de acesso 1040, 1130, 1140, 1550, 3500, 3600, 2600, 1250, 1260, 1240, OEAP 600, ISR 891 e O R 881 é compatível com o Flex 7500.

[Arquitetura FlexConnect](#)

Figura 6: Topologia típica de filial sem fio

FlexConnect Architecture



O FlexConnect é uma solução sem fio para implantações em filiais e escritórios remotos. Ele também é conhecido como uma solução de REAP híbrido, mas este documento fará referência a ele como FlexConnect.

A solução FlexConnect permite que o cliente:

- Centralize o tráfego de controle e gerenciamento de APs a partir do data center. O tráfego de controle é marcado por traços vermelhos na [Figura 6](#).
- Distribua o tráfego de dados do cliente em cada filial. O tráfego de dados é marcado por traços azuis, verdes e roxos na [Figura 6](#). Cada fluxo de tráfego vai para seu destino final da maneira mais eficiente.

Vantagens da centralização do tráfego de controle de ponto de acesso

- Painel único de monitoramento e solução de problemas
- Facilidade de gerenciamento
- Acesso móvel seguro e perfeito aos recursos do data center
- Redução na área ocupada pela filial
- Aumento na economia operacional

Vantagens da distribuição do tráfego de dados do cliente

- Sem tempo de inatividade operacional (sobrevivência) contra falhas completas de link de WAN ou indisponibilidade do controlador
- Resiliência de mobilidade na filial durante falhas de link da WAN

- Aumento na escalabilidade da filial. Suporta tamanho de filial que pode ser dimensionado para até 100 APs e 250.000 pés quadrados (5.000 pés quadrados). pés por AP).

A solução Cisco FlexConnect também oferece suporte ao tráfego de dados do cliente central, mas deve ser limitada apenas ao tráfego de dados do convidado. Esta próxima tabela descreve as restrições dos tipos de segurança L2 da WLAN somente para clientes não convidados cujo tráfego de dados também é comutado centralmente no data center.

Suporte de segurança L2 para usuários não convidados comutados centralmente

Segurança L2 da WLAN	Tipo	Resultado
Nenhum	N/A	Permitido
WPA + WPA2	802,1x	Permitido
	CCKM	Permitido
	802.1x + CCKM	Permitido
	PSK	Permitido
802,1x	WEP	Permitido
WEP estático	WEP	Permitido
WEP + 802,1x	WEP	Permitido
CKIP		Permitido

Observação: essas restrições de autenticação não se aplicam a clientes cujo tráfego de dados é distribuído na filial.

Suporte de segurança L3 para usuários com switches centrais e locais

Segurança L3 da WLAN	Tipo	Resultado
Autenticação da Web	Interno	Permitido
	Externos	Permitido
	Personalizado	Permitido
Passagem da Web	Interno	Permitido
	Externos	Permitido
	Personalizado	Permitido
Redirecionamento condicional da Web	Externos	Permitido
Redirecionamento da Web da página inicial	Externos	Permitido

Para obter mais informações sobre a implantação externa da Web do Flexconnect, consulte o [Guia de implantação do Flexconnect External WebAuth](#)

Para obter mais informações sobre estados de AP HREAP/FlexConnect e opções de comutação de tráfego de dados, consulte [Configuração do FlexConnect](#).

Modos de operação do FlexConnect

Modo	Descrição
------	-----------

FlexConnect	
Conectado	Diz-se que o FlexConnect está no modo conectado quando seu plano de controle CAPWAP de volta ao controlador está ativo e operacional, o que significa que o link da WAN não está inoperante.
Autônomo	O modo autônomo é especificado como o estado operacional que o FlexConnect insere quando não tem mais a conectividade de volta ao controlador. Os APs FlexConnect no modo autônomo continuarão a funcionar com a última configuração conhecida, mesmo no caso de falha de energia e WLC ou WAN.

Para obter mais informações sobre a Teoria das operações do FlexConnect, consulte o [Guia de design e implantação do H-Reap / FlexConnect](#).

[Requisitos de WAN](#)

Os APs FlexConnect são implantados na filial e gerenciados a partir do data center em um link de WAN. É altamente recomendado que a restrição mínima de largura de banda permaneça de 12,8 kbps por AP com latência de round trip não superior a 300 ms para implantações de dados e 100 ms para implantações de dados + voz. A unidade de transmissão máxima (MTU) deve ter pelo menos 500 bytes.

Tipo de implantação	Largura de banda da WAN (mín.)	Latência de WAN RTT (máx.)	Máximo de APs por filial	Máximo de clientes por filial
Dados	64 kbps	300 ms	5	25
Dados + voz	128 Kbps	100 ms	5	25
Monitor	64 kbps	2 s	5	N/A
Dados	640 Kbps	300 ms	50	1000
Dados + voz	1.44 Mbps	100 ms	50	1000
Monitor	640 Kbps	2 s	50	N/A

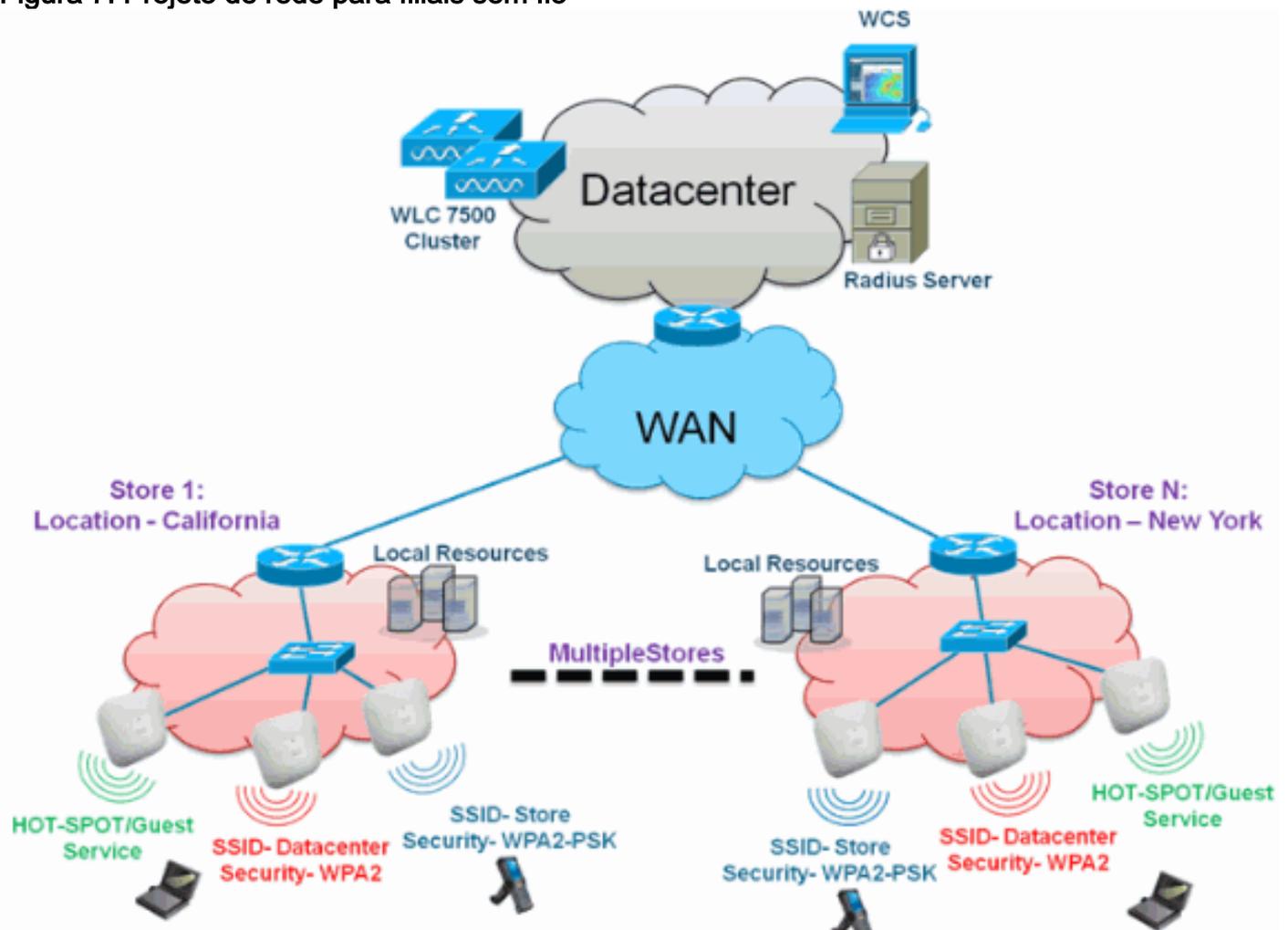
[Projeto de rede para filiais sem fio](#)

O restante deste documento destaca as diretrizes e descreve as melhores práticas para implementar redes de filiais distribuídas seguras. A arquitetura FlexConnect é recomendada para redes de filiais sem fio que atendem a esses requisitos de projeto.

[Principais requisitos de design](#)

- Tamanho da filial que pode escalar até 100 APs e 250.000 pés quadrados (5.000 m²). pés por AP)
- Gerenciamento central e solução de problemas
- Sem tempo de inatividade operacional
- Segmentação de tráfego baseada em cliente
- Conectividade sem fio perfeita e segura para recursos corporativos
- Compatível com PCI
- Suporte para convidados

Figura 7: Projeto de rede para filiais sem fio



Overview

Os clientes da filial acham cada vez mais difícil e caro fornecer serviços de rede escaláveis e seguros completos em todas as localizações geográficas. Para oferecer suporte aos clientes, a Cisco está enfrentando esses desafios apresentando o Flex 7500.

A solução Flex 7500 virtualiza as complexas operações de segurança, gerenciamento, configurações e solução de problemas no data center e, em seguida, estende esses serviços de forma transparente para cada filial. As implantações que usam o Flex 7500 são mais fáceis para a TI configurar, gerenciar e, mais importante, dimensionar.

Vantagens

- Aumente a escalabilidade com suporte a 6000 APs
- Maior resiliência usando a tolerância a falhas do FlexConnect
- Aumentar a segmentação do tráfego usando o FlexConnect (switching central e local)
- Facilidade de gerenciamento com a replicação de designs de loja usando grupos AP e grupos FlexConnect.

Recursos Abordando o projeto de rede da filial

O resto das seções do guia capturam o uso de recursos e recomendações para realizar o projeto de rede mostrado na [Figura 7](#).

Recursos:

Principais recursos	Destaques
Grupos AP	Oferece facilidade operacional/de gerenciamento ao lidar com várias filiais. Além disso, oferece a flexibilidade de replicação de configurações para filiais semelhantes.
Grupos FlexConnect	Os grupos FlexConnect fornecem a funcionalidade de RADIUS de backup local, roaming rápido CCKM/OKC e autenticação local.
Tolerância a falhas	Melhora a resiliência da filial sem fio e não oferece tempo de inatividade operacional.
ELM (Enhanced Local Mode for Adaptive WIPS)	Forneça a funcionalidade WIPS adaptável ao atender aos clientes sem afetar o desempenho do cliente.
Limite do cliente por WLAN	Limitando o total de clientes convidados na rede da filial.
Download de pré-imagem de AP	Reduz o tempo de inatividade ao atualizar sua filial.
Converter automaticamente APs no FlexConnect	Funcionalidade para converter automaticamente APs no FlexConnect para sua filial.
Acesso de convidado	Continue a arquitetura de acesso para convidados da Cisco com o FlexConnect.

Matriz de suporte IPv6

Recursos	Comutado centralmente		Comutado localmente	
	5500 / WiSM-2	Flex 7500	5500 / WiSM-2	Flex 7500
IPv6 (mobilidade do cliente)	Supporte d	Not Supporte d	Not Supporte d	Not Supporte d
Protetor de RA IPv6	Supporte d	Supporte d	Supporte d	Supporte d
Proteção DHCP IPv6	Supporte d	Not Supporte d	Not Supporte d	Not Supporte d
Protetor de origem IPv6	Supporte d	Not Supporte d	Not Supporte d	Not Supporte d
Limitação de RA / Limite de taxa	Supporte d	Not Supporte d	Not Supporte d	Not Supporte d
ACL IPv6	Supporte d	Not Supporte d	Not Supporte d	Not Supporte d
Visibilidade do cliente IPv6	Supporte d	Not Supporte d	Not Supporte d	Not Supporte d
Cache de descoberta de vizinhos IPv6	Supporte d	Not Supporte d	Not Supporte d	Not Supporte d
Bridging IPv6	Supporte d	Not Supporte d	Supporte d	Supporte d

[Matriz de recursos](#)

Consulte a [Matriz de Recursos do FlexConnect](#) para obter uma matriz de recursos para o recurso FlexConnect.

[Grupos AP](#)

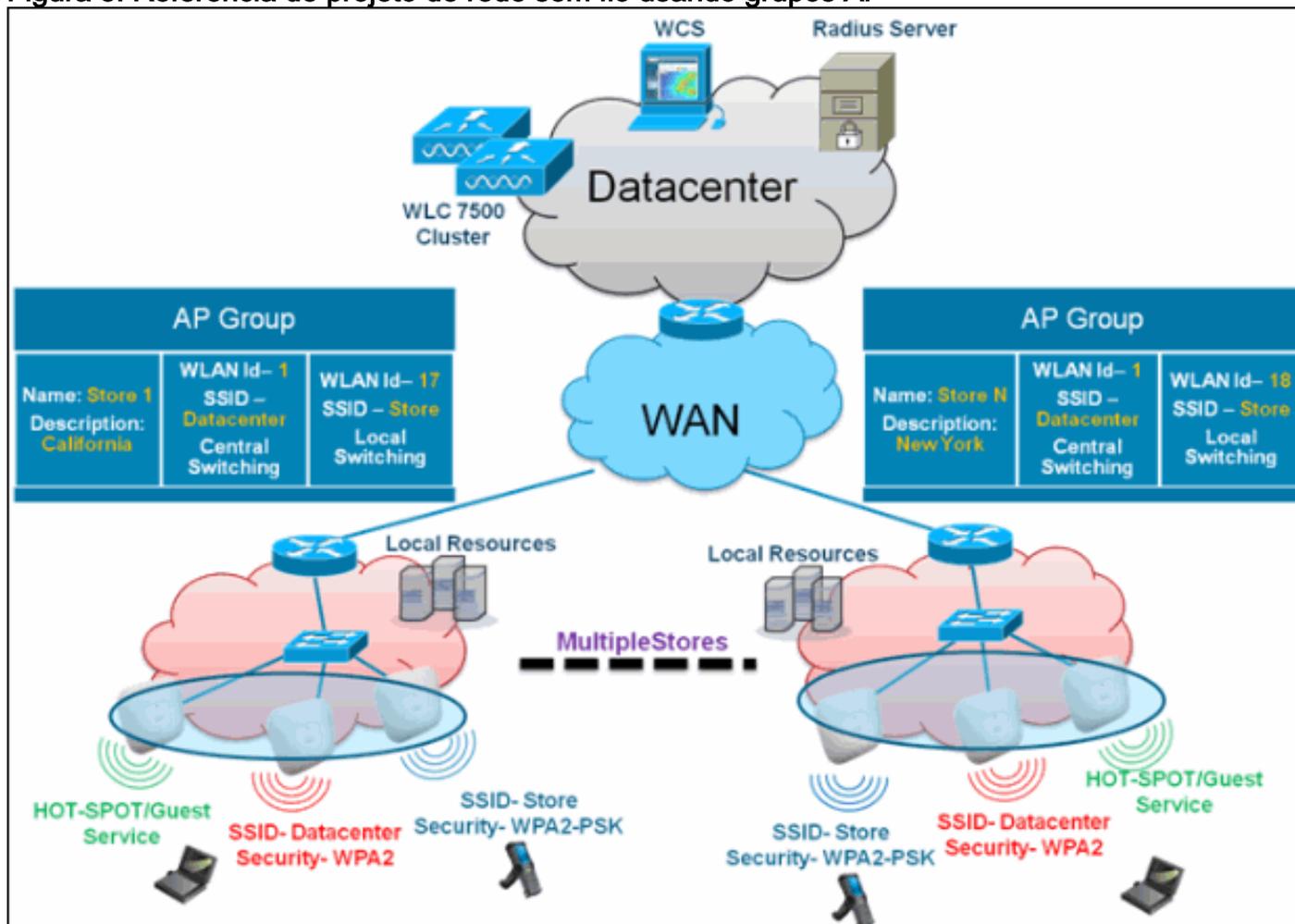
Depois de criar WLANs no controlador, você pode publicá-las seletivamente (usando grupos de pontos de acesso) em diferentes pontos de acesso para gerenciar melhor sua rede sem fio. Em uma implantação típica, todos os usuários em uma WLAN são mapeados para uma única interface no controlador. Portanto, todos os usuários associados a essa WLAN estão na mesma sub-rede ou VLAN. No entanto, você pode optar por distribuir a carga entre várias interfaces ou para um grupo de usuários com base em critérios específicos, como departamentos individuais (como Marketing, Engenharia ou Operações), criando grupos de pontos de acesso. Além disso,

esses grupos de access points podem ser configurados em VLANs separadas para simplificar a administração da rede.

Este documento usa grupos AP para simplificar a administração da rede ao gerenciar várias lojas em locais geográficos. Para facilidade operacional, o documento cria um grupo de AP por loja para atender a esses requisitos:

- **Datacenter** SSID comutado centralmente em todas as lojas para acesso administrativo ao Local Store Manager.
- **Loja** SSID comutada localmente com diferentes chaves WPA2-PSK em todas as lojas para scanners portáteis.

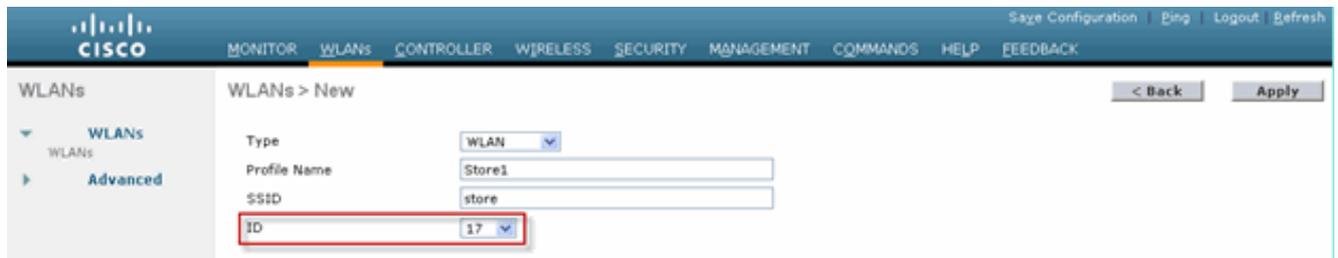
Figura 8: Referência de projeto de rede sem fio usando grupos AP



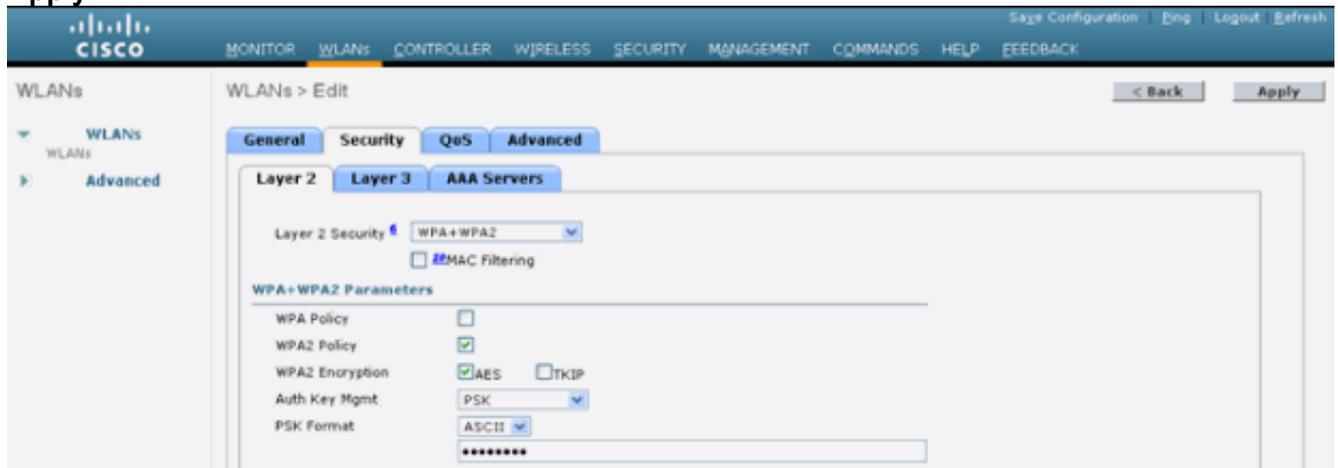
Configurações do WLC

Conclua estes passos:

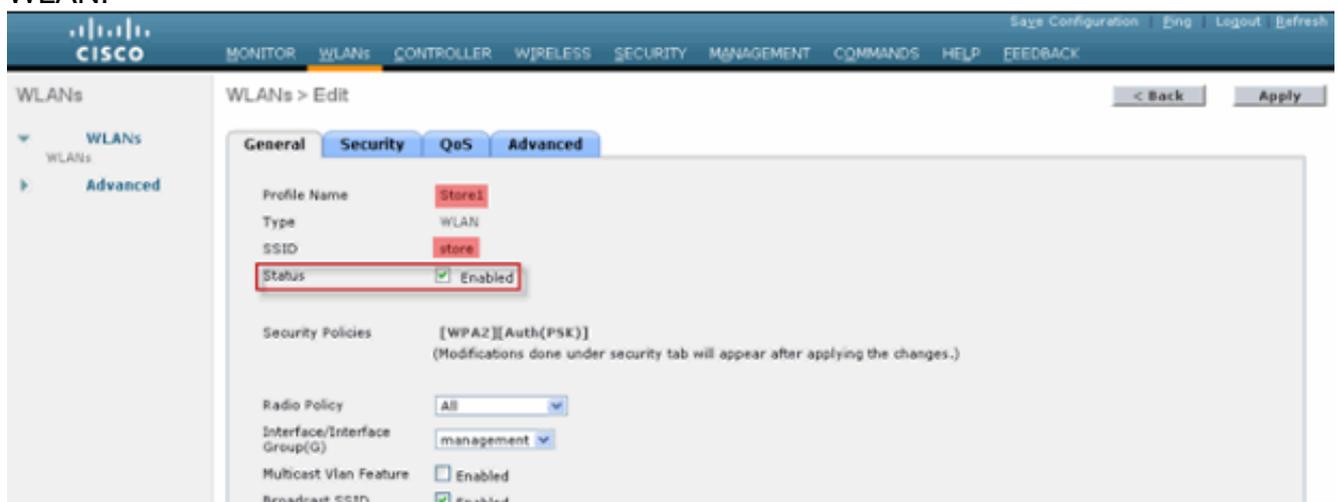
1. Na página WLANs > New, insira **Store1** no campo Profile Name, digite **store** no campo SSID e escolha **17** na lista suspensa ID. **Observação:** as IDs de WLAN 1-16 fazem parte do grupo padrão e não podem ser excluídas. Para atender à nossa exigência de usar o mesmo repositório de SSID por loja com um WPA2-PSK diferente, você precisa usar o ID de WLAN 17 e mais além, pois eles não fazem parte do grupo padrão e podem ser limitados a cada loja.



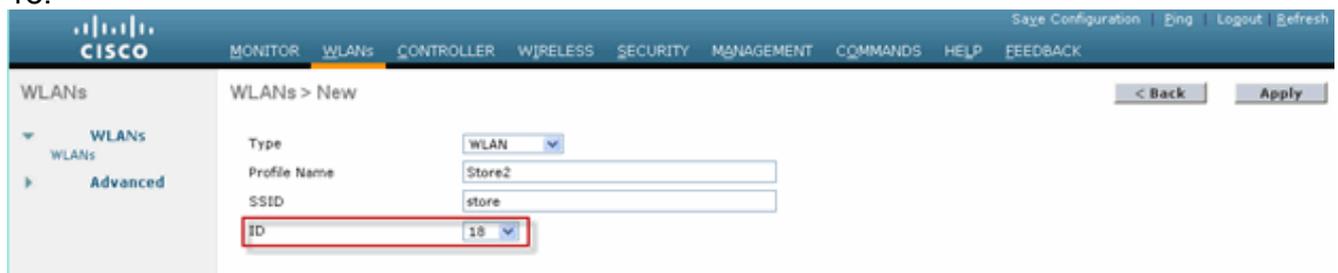
2. Em WLAN > Security, escolha **PSK** na lista suspensa Auth Key Management, escolha **ASCII** na lista suspensa PSK Format e clique em **Apply**.

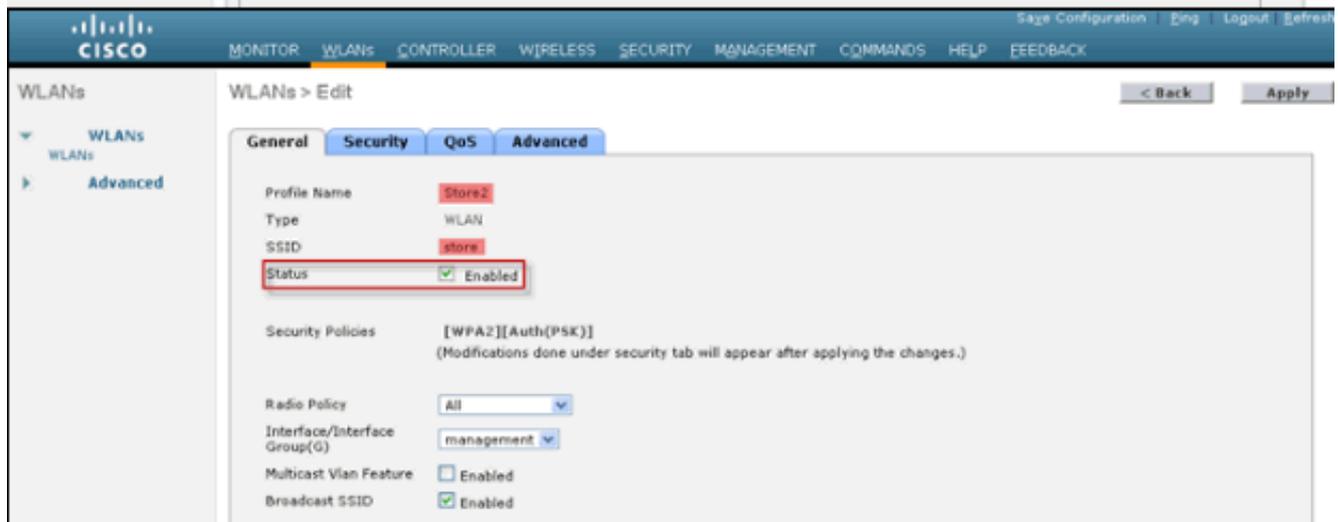
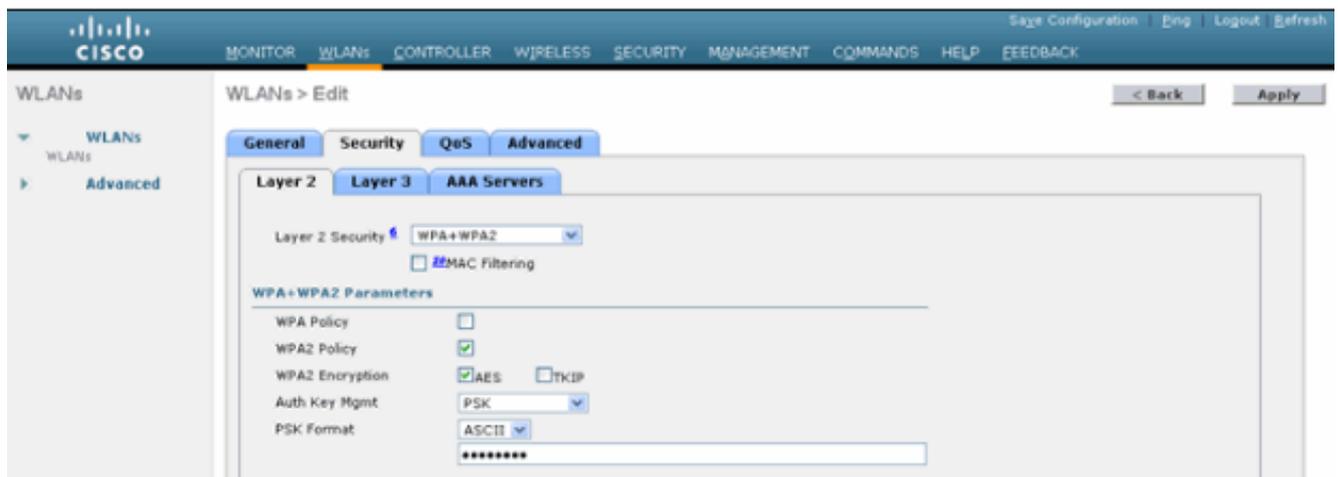


3. Clique em **WLAN > General**, verifique a alteração nas Políticas de segurança e marque a caixa **Status** para ativar a WLAN.



4. Repita as etapas 1, 2 e 3 para o novo perfil de WLAN **Store2**, com arquivo SSID e ID 18.





5. Crie ative o perfil da WLAN com o nome do perfil **DataCenter**, SSID **DataCenter** e ID **1**. **Observação:** na criação, as IDs de WLAN de 1 a 16 são automaticamente parte do grupo de AP padrão.
6. Em WLAN, verifique o status das IDs de WLAN 1, 17 e 18.

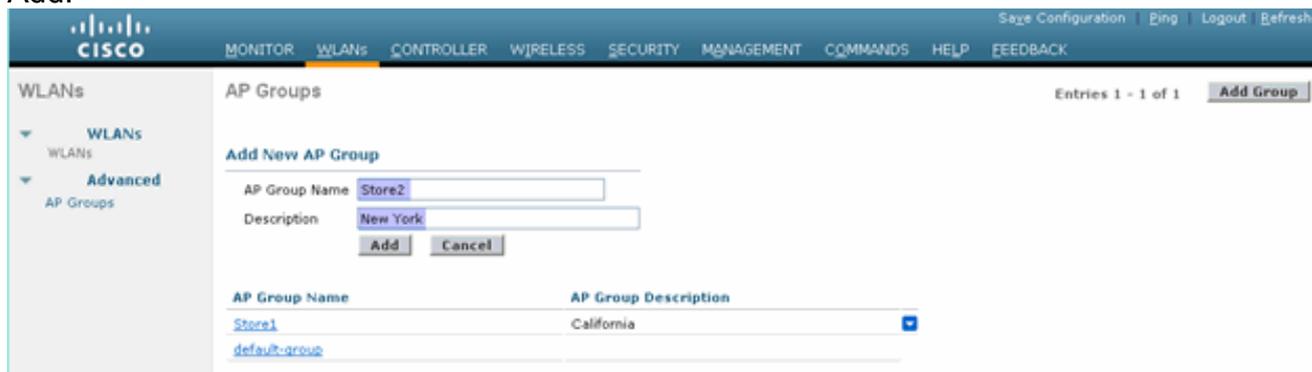


7. Clique em **WLAN > Avançado > Grupo de AP > Adicionar Grupo**.
8. Adicione o nome do grupo AP **Store1**, o mesmo que o perfil de WLAN **Store1**, e a descrição como o local da loja. Neste exemplo, a Califórnia é usada como a localização da loja.
9. Clique em **Adicionar** quando terminar.



10. Clique em **Add Group** e crie AP Group Name **Store2** e Description New York.

11. Clique em **Add**.



12. Verifique a criação do grupo clicando em **WLAN > Avançado > Grupos de AP**.



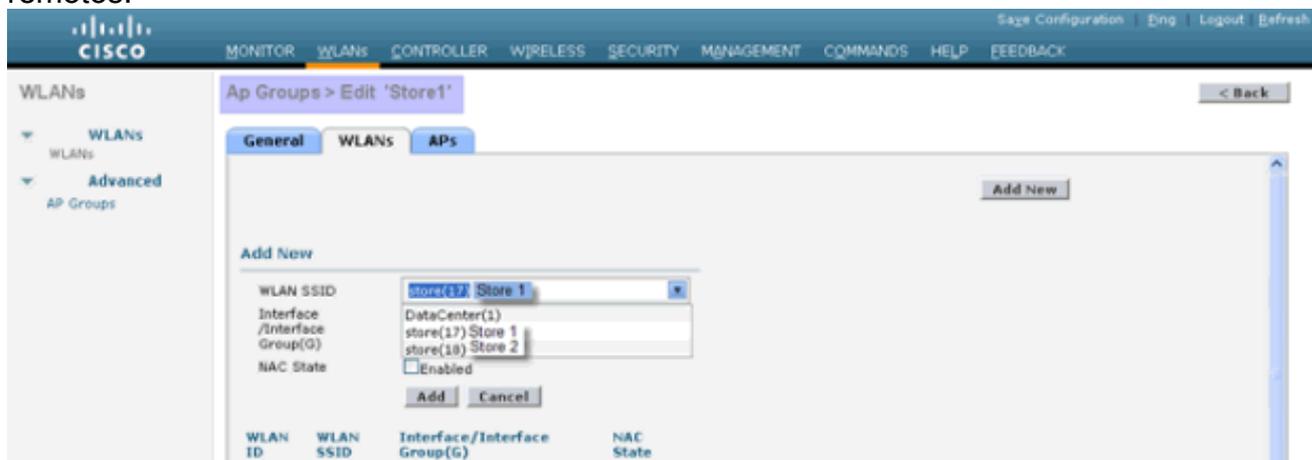
13. Clique em AP Group Name **Store1** para adicionar ou editar a WLAN.

14. Clique em **Adicionar novo** para selecionar a WLAN.

15. Em WLAN, no menu suspenso WLAN SSID, escolha **WLAN ID 17 store(17)**.

16. Clique em **Adicionar** depois que a ID de WLAN 17 for selecionada.

17. Repita as etapas de 14 a 16 para o Data Center do ID de WLAN 1(1). Esta etapa é opcional e necessária somente se você quiser permitir o acesso a recursos remotos.



18. Volte para a tela **WLAN > Avançado > Grupos de AP**.

19. Clique em AP Group Name **Store2** para adicionar ou editar a WLAN.

20. Clique em **Adicionar novo** para selecionar a WLAN.
21. Em WLAN, no menu suspenso WLAN SSID, escolha **WLAN ID 18 store(18)**.
22. Clique em **Adicionar** depois que a ID de WLAN 18 for selecionada.
23. Repita as etapas de 14 a 16 para o Data Center do ID de WLAN 1(1).



Observação: não é permitido adicionar vários perfis de WLAN com o mesmo SSID em um único grupo de



APs. **Observação:** a adição de APs ao grupo AP não é capturada neste documento, mas é necessária para que os clientes acessem serviços de rede.

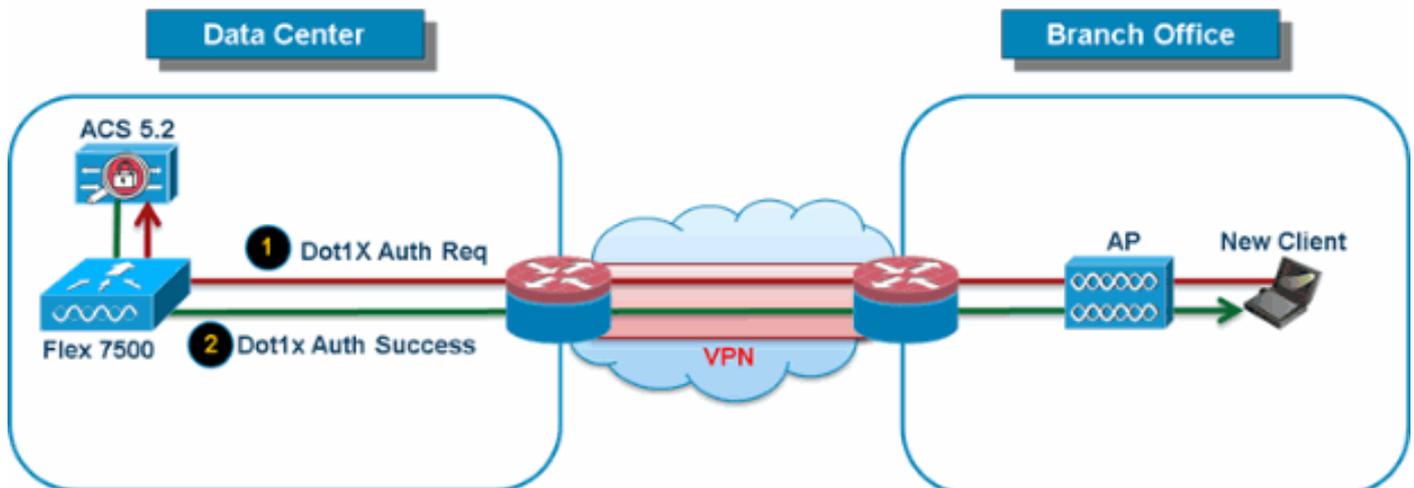
Summary

- Os grupos de AP simplificam a administração da rede.
- Solução de problemas com granularidade por filial
- Maior flexibilidade

Grupos FlexConnect

Figura 9: Autenticação Central Dot1X (Flex 7500 Atuando como Autenticador)

Central Authentication – Flex 7500 Authenticator



Na maioria das implantações típicas de filiais, é fácil prever que a autenticação 802.1X do cliente ocorra de forma central no data center, como mostrado na [Figura 9](#). Uma vez que o cenário acima é perfeitamente válido, suscita estas preocupações:

- Como os clientes sem fio podem executar a autenticação 802.1X e acessar os serviços do data center se o Flex 7500 falhar?
- Como os clientes sem fio podem executar a autenticação 802.1X se o link WAN entre a filial e o data center falhar?
- Há algum impacto na mobilidade da filial durante falhas de WAN?
- A solução FlexConnect não oferece tempo de inatividade operacional da filial?

O FlexConnect Group foi projetado principalmente e deve ser criado para lidar com esses desafios. Além disso, facilita a organização de cada filial, pois todos os pontos de acesso FlexConnect de cada filial fazem parte de um único grupo FlexConnect.

Observação: os grupos FlexConnect não são análogos aos grupos AP.

Principais objetivos dos grupos FlexConnect

Backup de failover de servidor RADIUS

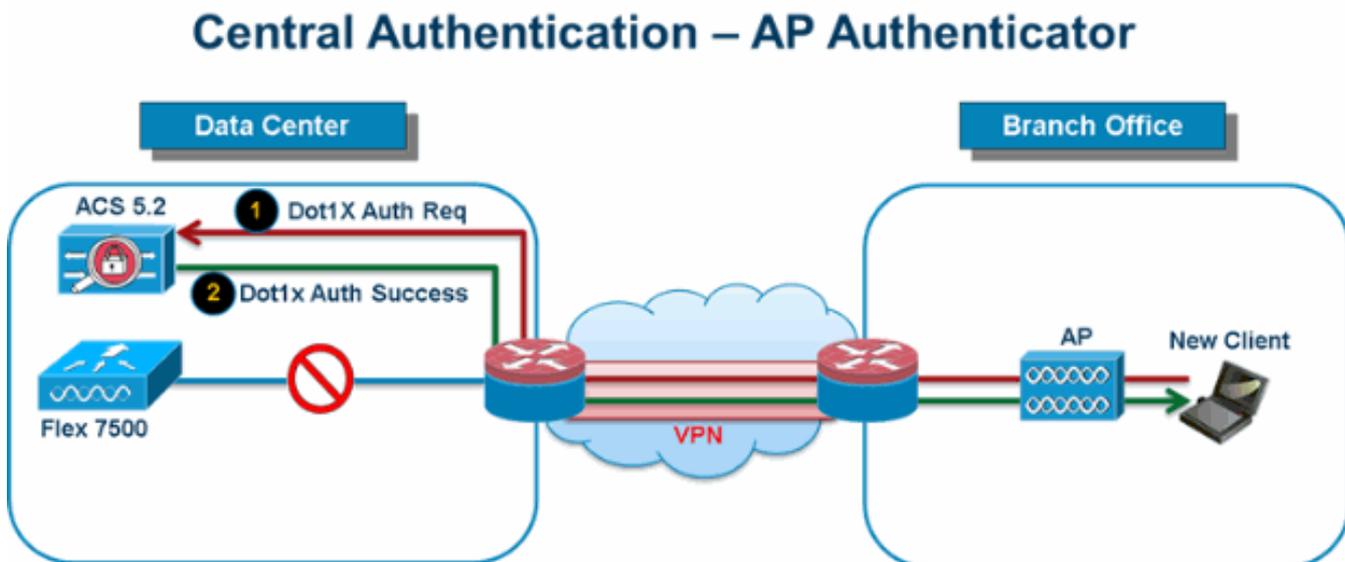
- Você pode configurar o controlador para permitir que um ponto de acesso FlexConnect no modo autônomo execute a autenticação 802.1X completa para um servidor RADIUS de backup. Para aumentar a resiliência da filial, os administradores podem configurar um servidor RADIUS de backup primário ou um servidor RADIUS de backup primário e secundário. Esses servidores são usados somente quando o ponto de acesso FlexConnect não está conectado ao controlador.

Observação: a contabilidade RADIUS de backup não é suportada.

Autenticação Local

- Antes da versão do código 7.0.98.0, a autenticação local era suportada somente quando o FlexConnect está no modo independente para garantir que a conectividade do cliente não seja afetada durante uma falha de link da WAN. Com a versão 7.0.116.0, esse recurso agora é suportado mesmo quando os pontos de acesso FlexConnect estão no modo

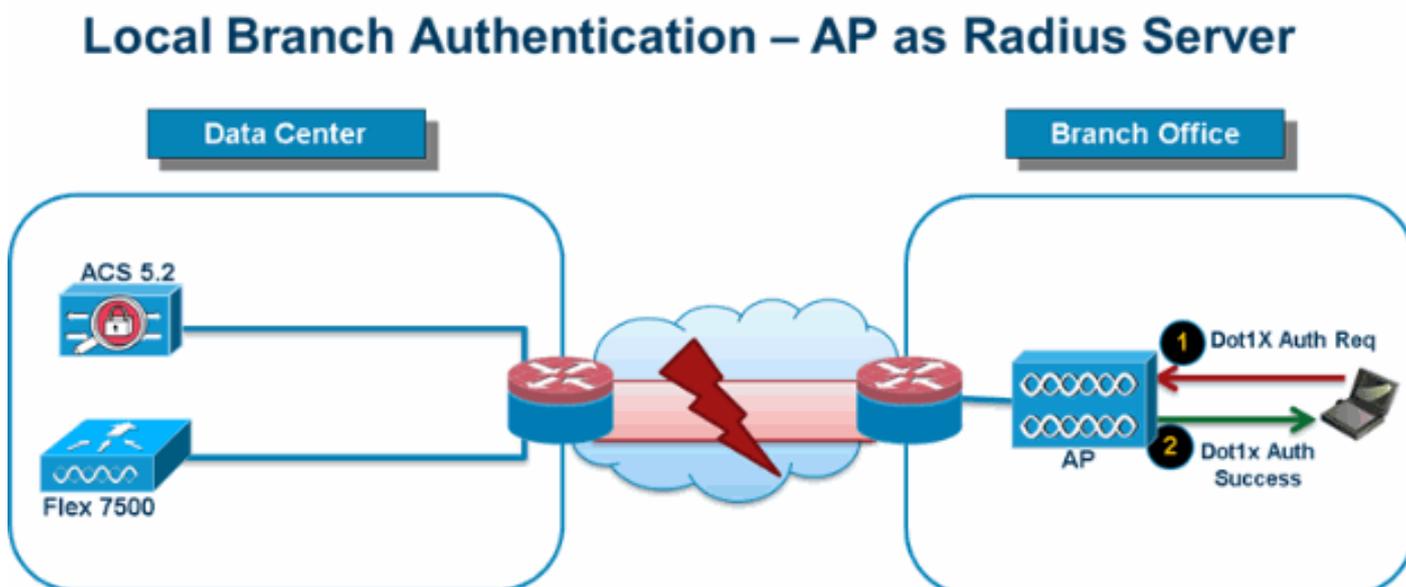
conectado. **Figura 10: Autenticação Central Dot1X (APs FlexConnect agindo como Autenticador)**



Como mostrado na [Figura 10](#), os clientes de filial podem continuar a executar a autenticação 802.1X quando os APs de filial FlexConnect perdem a conectividade com o Flex 7500. Enquanto o servidor RADIUS/ACS estiver acessível na filial, os clientes sem fio continuarão a autenticar e acessar serviços sem fio. Em outras palavras, se o RADIUS/ACS estiver localizado dentro da filial, os clientes autenticarão e acessarão serviços sem fio mesmo durante uma interrupção da WAN. **Observação:** esse recurso pode ser usado em conjunto com o recurso de servidor RADIUS de backup FlexConnect. Se um grupo FlexConnect estiver configurado com o servidor RADIUS de backup e a autenticação local, o access point FlexConnect sempre tentará autenticar os clientes usando primeiro o servidor RADIUS de backup primário, seguido pelo servidor RADIUS de backup secundário (se o primário não puder ser alcançado) e, finalmente, o servidor EAP local no próprio access point FlexConnect (se o primário e o secundário não puderem ser alcançados).

EAP local (continuação de autenticação local)

Figura 11: Autenticação Dot1X (APs FlexConnect agindo como servidor EAP local)



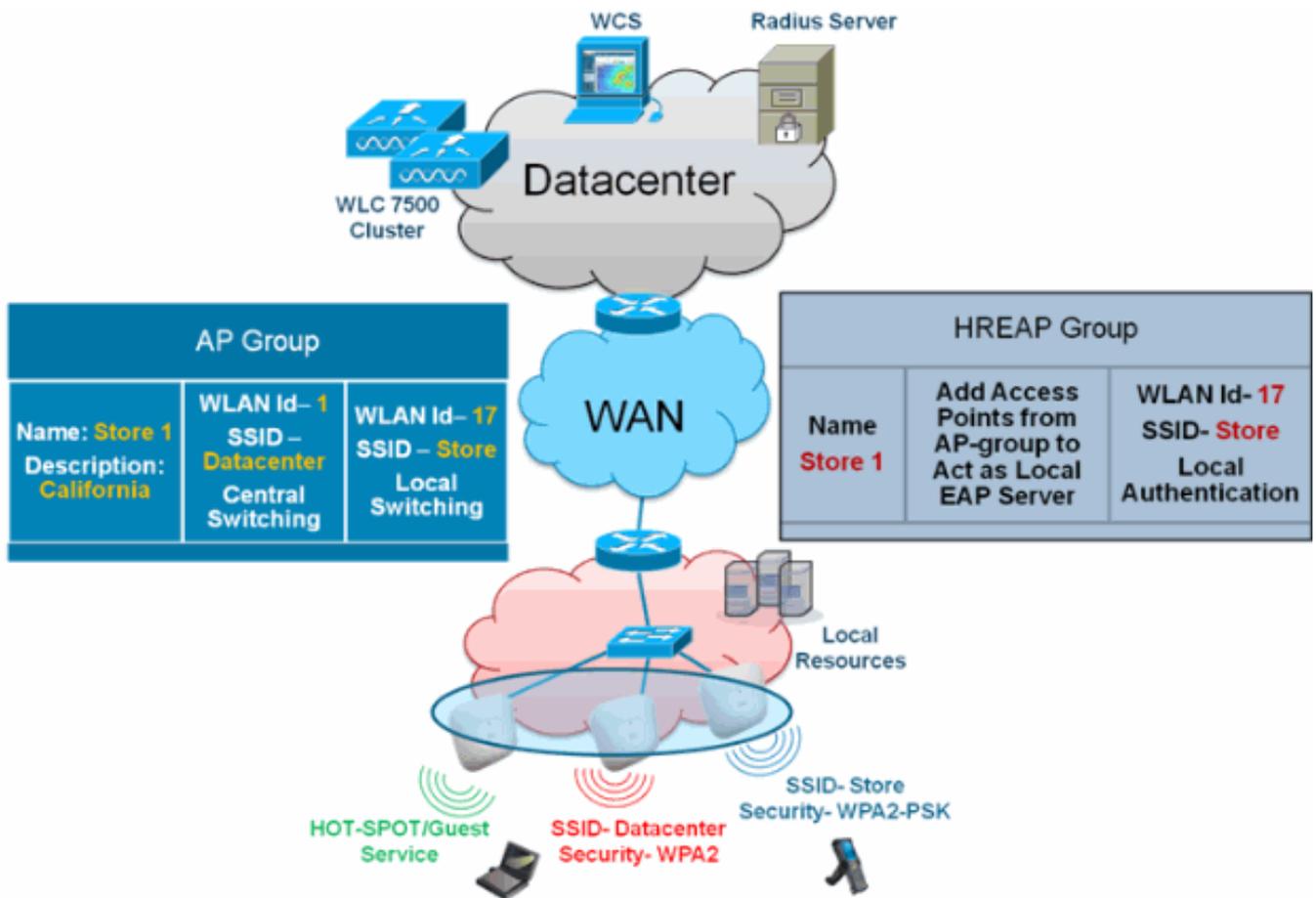
- Você pode configurar o controlador para permitir que um AP FlexConnect no modo autônomo ou conectado execute a autenticação LEAP ou EAP-FAST para até 100 usuários

configurados estaticamente. O controlador envia a lista estática de nomes de usuário e senhas para cada ponto de acesso FlexConnect desse grupo FlexConnect específico quando ele ingressa no controlador. Cada ponto de acesso no grupo autentica somente seus próprios clientes associados.

- Esse recurso é ideal para clientes que estão migrando de uma rede de access point autônoma para uma rede de access point FlexConnect leve e não estão interessados em manter um banco de dados de usuários grandes ou adicionar outro dispositivo de hardware para substituir a funcionalidade de servidor RADIUS disponível no access point autônomo.
- Como mostrado na [Figura 11](#), se o servidor RADIUS/ACS dentro do data center não for alcançável, os APs FlexConnect atuarão automaticamente como um servidor Local-EAP para executar a autenticação Dot1X para clientes de filial sem fio.

Roaming rápido CCKM/OKC

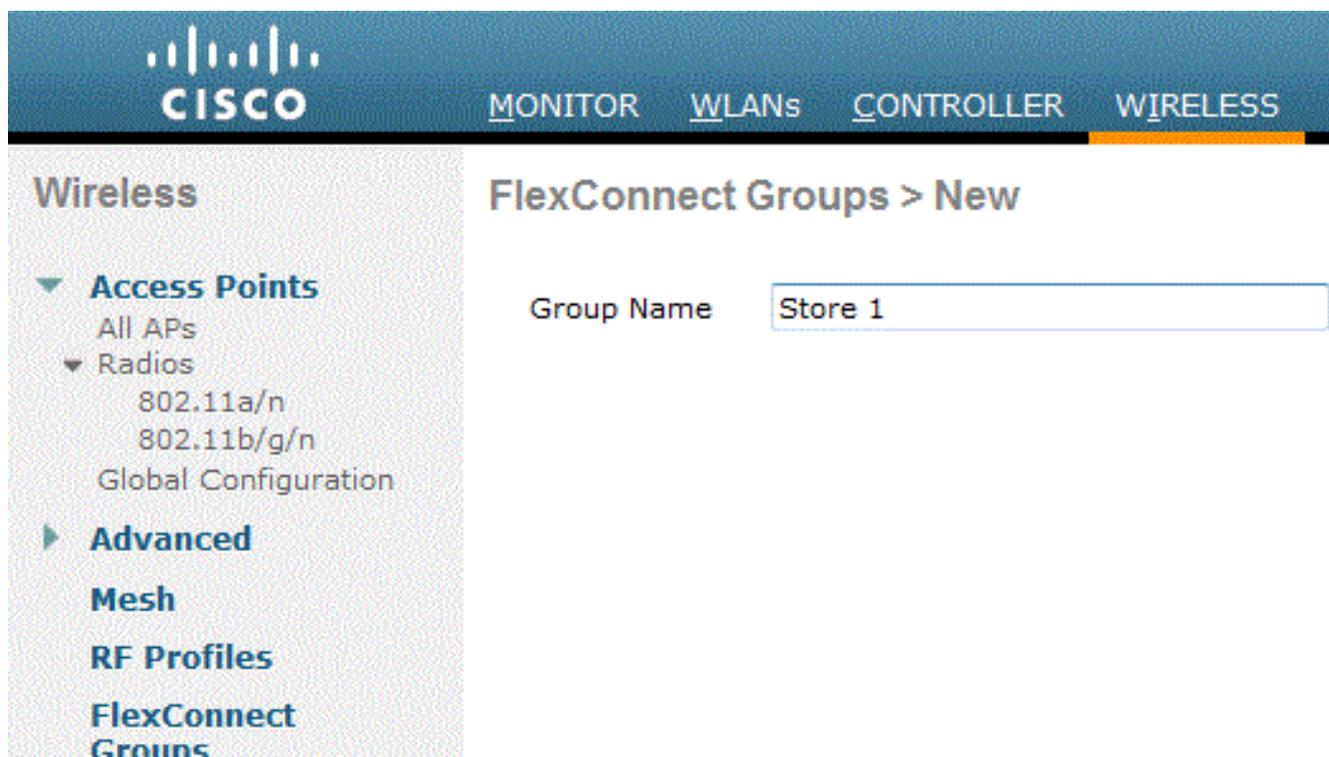
- Os grupos FlexConnect são necessários para que o roaming rápido CCKM/OKC funcione com pontos de acesso FlexConnect. O roaming rápido é obtido ao colocar em cache um derivado da chave mestra de uma autenticação EAP completa para que uma troca de chave simples e segura possa ocorrer quando um cliente sem fio faz roaming para um ponto de acesso diferente. Este recurso evita a necessidade de executar uma autenticação RADIUS EAP completa quando o cliente faz roaming de um ponto de acesso para outro. Os pontos de acesso FlexConnect precisam obter as informações do cache CCKM/OKC para todos os clientes que possam se associar para que possam processá-lo rapidamente em vez de enviá-lo de volta ao controlador. Se, por exemplo, você tiver um controlador com 300 access points e 100 clientes que possam se associar, o envio do cache CCKM/OKC para todos os 100 clientes não é prático. Se você criar um grupo FlexConnect composto por um número limitado de pontos de acesso (por exemplo, você cria um grupo para quatro pontos de acesso em um escritório remoto), os clientes fazem roaming apenas entre esses quatro pontos de acesso, e o cache CCKM/OKC é distribuído entre esses quatro pontos de acesso somente quando os clientes se associam a um deles.
- Este recurso, juntamente com o Backup Radius e a Autenticação Local (Local-EAP), garante **nenhum tempo de inatividade operacional** para suas filiais. **Observação:** o roaming rápido do CCKM/OKC entre os pontos de acesso FlexConnect e não FlexConnect não é suportado. **Figura 12: Referência de design de rede sem fio usando grupos FlexConnect**



Configuração do grupo FlexConnect do WLC

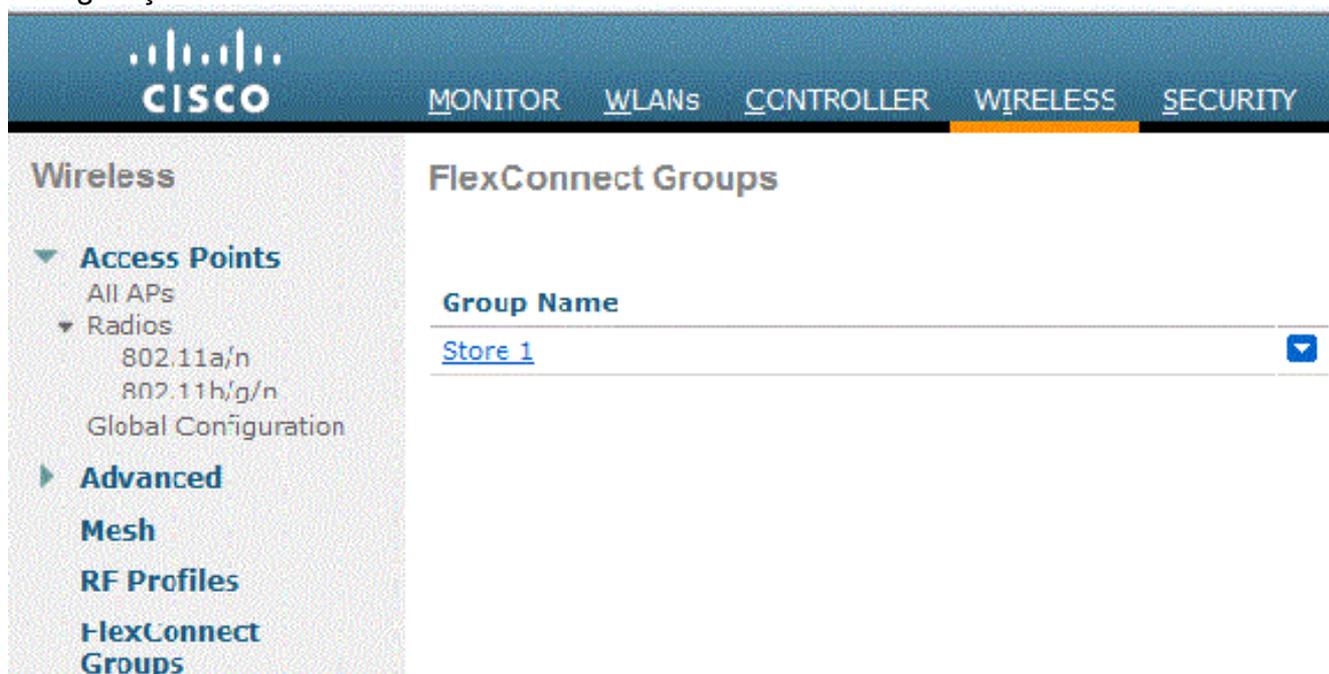
Conclua as etapas nesta seção para configurar grupos FlexConnect para suportar a autenticação local usando LEAP, quando o FlexConnect estiver no modo conectado ou independente. O exemplo de configuração na [Figura 12](#) ilustra as diferenças objetivas e o mapeamento 1:1 entre o grupo AP e o grupo FlexConnect.

1. Clique em **New** em Wireless > FlexConnect Groups.
2. Atribua Group Name Store 1, semelhante à configuração de exemplo, como mostrado na [Figura 12](#).
3. Clique em **Aplicar** quando o nome do grupo estiver definido.



The screenshot shows the Cisco FlexConnect Groups configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar is titled 'Wireless' and contains a tree view with 'Access Points' (All APs, Radios: 802.11a/n, 802.11b/g/n, Global Configuration), 'Advanced', 'Mesh', 'RF Profiles', and 'FlexConnect Groups'. The main content area is titled 'FlexConnect Groups > New' and features a 'Group Name' field with the value 'Store 1'.

4. Clique na **Loja** de nome de grupo **1** que você acabou de criar para outras configurações.



The screenshot shows the Cisco FlexConnect Groups configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar is titled 'Wireless' and contains a tree view with 'Access Points' (All APs, Radios: 802.11a/n, 802.11h/g/n, Global Configuration), 'Advanced', 'Mesh', 'RF Profiles', and 'FlexConnect Groups'. The main content area is titled 'FlexConnect Groups' and features a table with one entry: 'Store 1' with a blue dropdown arrow icon to its right.

5. Clique em **Adicionar AP**.

The screenshot shows the Cisco FlexConnect Groups configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar is titled 'Wireless' and contains a tree view with 'Access Points' (All APs, Radios: 802.11a/n, 802.11b/g/n, Global Configuration), 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups' (highlighted), and 'FlexConnect ACLs'. The main content area is titled 'FlexConnect Groups > Edit 'Store 1''. It features three tabs: 'General', 'Local Authentication' (selected), and 'Image Upgrade'. Under the 'Local Authentication' tab, the 'Group Name' is 'Store 1'. Below this is a section for 'FlexConnect APs' with an 'Add AP' button and a table with columns for 'AP MAC Address', 'AP Name', and 'Status'.

6. Marque a caixa **Enable AP Local Authentication** para habilitar Local Authentication quando o AP estiver no modo independente. **Observação:** a Etapa 20 mostra como habilitar a Autenticação Local para o AP do Modo Conectado.
7. Marque a caixa **Select APs from current controller** para habilitar o menu suspenso AP Name (Selecionar APs da controladora atual).
8. Escolha o AP na lista suspensa que precisa fazer parte desse grupo FlexConnect.
9. Clique em **Add** depois que o AP for escolhido na lista suspensa.
10. Repita as etapas 7 e 8 para adicionar todos os APs a esse grupo FlexConnect que também fazem parte do AP-Group Store 1. Veja a [Figura 12](#) para entender o mapeamento 1:1 entre o grupo AP-Group e o grupo FlexConnect. Se você criou um AP-Group por Store ([Figura 8](#)), então idealmente todos os APs desse AP-Group devem fazer parte desse FlexConnect Group ([Figura 12](#)). A manutenção da proporção de 1:1 entre o grupo AP e o grupo FlexConnect simplifica o gerenciamento da rede.

The screenshot displays the Cisco FlexConnect Groups configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar shows the 'Wireless' menu with options like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', and '802.11a/n'. The main content area is titled 'FlexConnect Groups > Edit 'Store 1''. The 'Local Authentication' tab is active. The 'Group Name' is 'Store 1'. Under 'FlexConnect APs', the 'Add AP' section is visible, showing a checked box for 'Select APs from current controller', a dropdown for 'AP Name' set to 'AP3500', and a text input for 'Ethernet MAC' set to '00:22:90:e3:37:df'. There are 'Add' and 'Cancel' buttons. At the bottom, a table header shows 'AP MAC Address', 'AP Name', and 'Status'.

11. Clique em **Local Authentication > Protocols** e marque a caixa **Enable LEAP Authentication**.
12. Clique em **Apply** depois que a caixa de seleção for definida. **Observação:** se você tiver um controlador de backup, verifique se os grupos FlexConnect são idênticos e se as entradas de endereço MAC do AP estão incluídas por grupo FlexConnect.

General **Local Authentication** **Image Upgrade** **VLAN-ACL mapping**

Local Users **Protocols**

LEAP

Enable LEAP Authentication

EAP Fast

Enable EAP Fast Authentication

Server Key (in hex) Enable Auto key generation

Authority ID (in hex) 436973636f00000000000000000000000000000000

Authority Info Cisco_A_ID

PAC Timeout (2 to 4095 days)

13. Em Autenticação local, clique em **Usuários locais**.
14. Defina os campos Nome de usuário, Senha e Confirmar senha e clique em **Adicionar** para criar uma entrada de usuário no servidor EAP local que reside no AP.
15. Repita a etapa 13 até que sua lista de nomes de usuário local esteja esgotada. Não é possível configurar ou adicionar mais de 100 usuários.
16. Clique em **Apply** depois que a etapa 14 for concluída e a contagem No of Users for verificada.

General **Local Authentication** **Image Upgrade** **VLAN-ACL mapping**

Local Users **Protocols**

No of Users 0 **Add User**

User Name

Upload CSV file

File Name

UserName cisco

Password

Confirm Password

Add

17. No painel superior, clique em **WLANs**.

18. Clique em **WLAN ID 17**. Isso foi criado durante a criação do Grupo AP. Consulte a [Figura 8](#).



19. Em WLAN > Edit for WLAN ID 17, clique em **Advanced**.

20. Marque a caixa **FlexConnect Local Auth** para habilitar a autenticação local no modo conectado. **Observação:** a autenticação local é suportada somente para FlexConnect com switching local. **Observação:** sempre certifique-se de criar o grupo FlexConnect antes de habilitar a autenticação local em

WLANs > Edit 'Store-1'

General	Security	QoS	Advanced
P2P Blocking Action			Disabled
Client Exclusion 3	<input checked="" type="checkbox"/> Enabled		60 Timeout Value (secs)
Maximum Allowed Clients 8		0	
Static IP Tunneling 11	<input type="checkbox"/> Enabled		
Wi-Fi Direct Clients Policy			Disabled
Maximum Allowed Clients Per AP Radio		200	
Off Channel Scanning Defer			
Scan Defer Priority		0 1 2 3 4 5 6 7	
		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	
Scan Defer Time (msecs)		100	
FlexConnect			
FlexConnect Local Switching 2	<input checked="" type="checkbox"/> Enabled		
FlexConnect Local Auth 12	<input checked="" type="checkbox"/> Enabled		
Learn Client IP Address 5	<input checked="" type="checkbox"/> Enabled		

WLAN.

NCS também fornece a caixa de seleção FlexConnect Local Auth para habilitar a autenticação local no modo conectado como mostrado aqui:

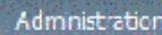
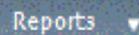
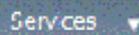
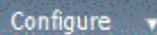
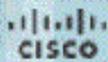
Properties > System > **WLANs** > WLAN Configuration

WLAN Configuration Details : 1
 Configure > Controllers > [Controller] > WLANs > WLAN Configuration :

General Security QoS **Advanced**

HexConnect Local Switching	<input checked="" type="checkbox"/>	Enable
FlexConnect Local Auth ⓘ	<input checked="" type="checkbox"/>	Enable
Learn Client IP Address	<input checked="" type="checkbox"/>	Enable
Session Timeout	<input type="checkbox"/>	Enable
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enable
Aironet IE	<input checked="" type="checkbox"/>	Enable
IPv6 ⓘ	<input type="checkbox"/>	Enable
Diagnostic Channel ⓘ	<input type="checkbox"/>	Enable
Override Interface ACL	IPv4	NONE
Peer to Peer Blocking ⓘ		Disable
Wi-Fi Direct Clients Policy		Disabled
Client Exclusion ⓘ	<input checked="" type="checkbox"/>	Enable
Timeout Value		60 (secs)

O NCS também oferece facilidade para filtrar e monitorar clientes FlexConnect localmente autenticados, como mostrado aqui:



Clients and Users



Refresh



Test



Useful



Remove



Wire



Track Clients



Identify Unknown Users

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name
<input type="radio"/>	00:22:90:1b:17:42		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	1c:df:0f:66:86:50		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:21:6e:97:9b:bc		IPv4	husl/vikal...		Intel	oeap-ta-war-2
<input type="radio"/>	00:22:90:1b:96:48		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:22:90:1b:17:8c		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	00:25:0b:4d:77:c4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	c4:7d:4f:3a:c5:d5		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:21:a0:d5:03:c4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	f3:66:f2:67:7f:50		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:17:ca:bc:d1:b4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	88:43:e1:d1:df:02		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:22:bd:1b:e2:b5		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	f3:66:f2:ab:1e:69		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:1c:58:d1:b4:4e		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:1e:7a:0b:21:8d		IPv4	ssimm		Cisco	oeap-ta-war-2

Virtual Domain: ROOT-DOMAIN root ▼ Log Out 🔍

Total 299

Location	VLAN	Status	Interface
Unknown	109	Associated	Gi1/0/34
Unknown	109	Associated	Gi1/0/26
Root Area	310	Associated	data
Unknown	109	Associated	Gi1/0/36
Unknown	109	Associated	Gi1/0/32
Unknown	109	Associated	Gi1/0/30
Unknown	109	Associated	Gi1/0/13
Unknown	109	Associated	Gi1/0/27
Unknown	109	Associated	Gi1/0/12
Unknown	109	Associated	Gi1/0/15
Unknown	109	Associated	Gi1/0/28
Unknown	109	Associated	Gi1/0/14
Unknown	109	Associated	Gi1/0/9
Unknown	109	Associated	Gi1/0/29
Root Area	311	Associated	voice

Associated Clients

- Quick Filter
- Advanced Filter
- All
- Manage Preset Filters
- 2.4GHz Clients
- 5GHz Clients
- All Lightweight Clients
- All Autonomous Clients
- All Wired Clients
- Associated Clients
- Clients known by ISE
- Clients detected by MSE
- Clients detected in the last 24 hours
- Clients with Problems
- Excluded Clients
- FlexConnect Locally Authenticated
- New clients detected in last 24 hours
- On Network Clients

Verificação usando CLI

O estado de autenticação do cliente e o modo de comutação podem ser verificados rapidamente usando esta CLI na WLC:

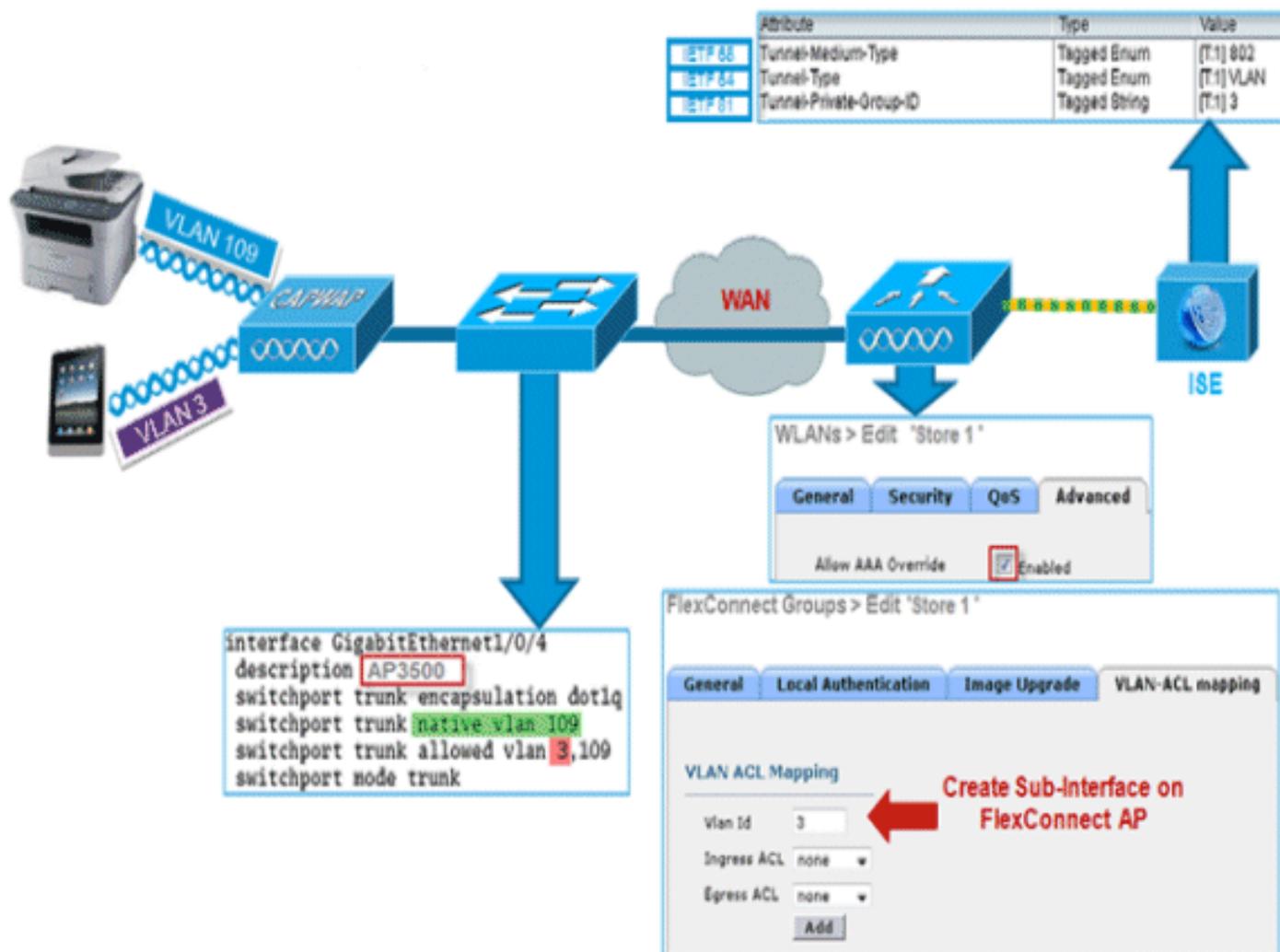
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
Client MAC Address..... 00:24:d7:2b:7c:0c
Client Username ..... N/A
AP MAC Address..... d0:57:4c:08:e6:70
Client State..... Associated
H-REAP Data Switching..... Local
H-REAP Authentication..... Local
```

Substituição de VLAN FlexConnect

Na arquitetura FlexConnect atual, há um mapeamento estrito de WLAN para VLAN, e, portanto, o cliente que está sendo associado a uma WLAN específica no AP FlexConnect deve obedecer a

uma VLAN que está mapeada para ela. Esse método tem limitações, pois exige que os clientes se associem a diferentes SSIDs para herdar diferentes políticas baseadas em VLAN.

A partir da versão 7.2, a substituição de AAA da VLAN em uma WLAN individual configurada para comutação local é suportada. Para ter uma atribuição de VLAN dinâmica, o AP teria as interfaces para a VLAN pré-criadas com base em uma configuração usando o mapeamento WLAN-VLAN existente para o AP FlexConnect individual ou usando o mapeamento ACL-VLAN em um grupo FlexConnect. A WLC é usada para pré-criar as subinterfaces no AP.



Summary

- A substituição da VLAN AAA é suportada a partir da versão 7.2 para WLANs configuradas para comutação local no modo de autenticação central e local.
- A substituição de AAA deve ser habilitada na WLAN configurada para switching local.
- O AP FlexConnect deve ter a VLAN pré-criada a partir da WLC para atribuição de VLAN dinâmica.
- Se as VLANs retornadas pela substituição AAA não estiverem presentes no cliente AP, elas obterão um IP da interface VLAN padrão do AP.

Procedimento

Conclua estes passos:

1. Crie uma WLAN para autenticação 802.1x.

WLANs > Edit 'Store 1'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security MAC Filtering

WPA+WPA2 Parameters

WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES <input type="checkbox"/> TKIP
Auth Key Mgmt	<input type="text" value="802.1X"/>
WPA gtk-randomize State	<input type="text" value="Disable"/>

2. Habilite o suporte de substituição de AAA para WLAN de switching local na WLC. Navegue até a GUI da WLAN > WLAN > ID da WLAN > guia Avançado.

WLANs > Edit 'Store 1'

General Security QoS Advanced

<input checked="" type="checkbox"/> Allow AAA Override	Enabled
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled
Enable Session Timeout	<input checked="" type="checkbox"/> 1800 Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/> Enabled
Diagnostic Channel	<input type="checkbox"/> Enabled
Override Interface ACL	IPv4 <input type="text" value="None"/> IPv6 <input type="text" value="None"/>
P2P Blocking Action	<input type="text" value="Disabled"/>
Client Exclusion	<input checked="" type="checkbox"/> Enabled 60 Timeout Value (secs)
Maximum Allowed Clients	<input type="text" value="0"/>
Static IP Tunneling	<input type="checkbox"/> Enabled
Wi-Fi Direct Clients Policy	<input type="text" value="Disabled"/>
Maximum Allowed Clients Per AP Radio	<input type="text" value="200"/>

Off Channel Scanning Defer

Scan Defer Priority	0 1 2 3 4 5 6 7
	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Scan Defer Time (msecs)	<input type="text" value="100"/>

FlexConnect

<input checked="" type="checkbox"/> FlexConnect Local Switching	Enabled
---	---------

DHCP

DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input type="checkbox"/> Required

Management Frame Protection (MFP)

MFP Client Protection	<input type="text" value="Optional"/>
-----------------------	---------------------------------------

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)	<input type="text" value="1"/>
802.11b/g/n (1 - 255)	<input type="text" value="1"/>

NAC

NAC State	<input type="text" value="None"/>
-----------	-----------------------------------

Load Balancing and Band Select

Client Load Balancing	<input type="checkbox"/>
Client Band Select	<input type="checkbox"/>

Passive Client

Passive Client	<input type="checkbox"/>
----------------	--------------------------

Voice

Media Session Snooping	<input type="checkbox"/> Enabled
Re-anchor Roamed Voice Clients	<input type="checkbox"/> Enabled
KTS based CAC Policy	<input type="checkbox"/> Enabled

3. Adicione os detalhes do servidor AAA na controladora para autenticação 802.1x. Para adicionar o servidor AAA, navegue até WLC GUI > Security > AAA > **Radius** > **Authentication** > **New**.

The screenshot displays the WLC GUI configuration page for a RADIUS Authentication Server. The left sidebar shows the navigation menu with 'Authentication' under 'RADIUS' highlighted. The main area shows the configuration for 'RADIUS Authentication Servers > Edit' with the following fields:

Server Index	1
Server Address	[Redacted]
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

4. O AP está no modo local por padrão, portanto, converta o modo para o modo FlexConnect. Os APs de modo local podem ser convertidos para o modo FlexConnect indo para **Wireless** > **All APs** e clicando no AP Individual.

All APs > Details for AP3500

General Credentials Interfaces High Availability Inventory Advanced

General Versions

AP Name	AP3500	Primary Software Version	7.2.1.69
Location	default location	Backup Software Version	7.2.1.72
AP MAC Address	cc:ef:48:c2:35:57	Predownload Status	None
Base Radio MAC	2c:3f:38:f6:98:b0	Predownload Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	FlexConnect	Predownload Retry Count	NA
AP Sub Mode	None	Boot Version	12.4.23.0
Operational Status	REG	IOS Version	12.4(20111122:141426)\$
Port Number	1	Mini IOS Version	7.0.112.74
Venue Group	Unspecified	IP Config	
Venue Type	Unspecified	IP Address	10.10.10.132
Venue Name		Static IP	<input type="checkbox"/>
Language		Time Statistics	
Network Spectrum Interface Key	0D45BA896226F4117D98BA920FBA8A16	UP Time	0 d, 00 h 01 m 14 s
		Controller Associated Time	0 d, 00 h 00 m 14 s
		Controller Association Latency	0 d, 00 h 00 m 59 s

5. Adicione os APs FlexConnect ao grupo FlexConnect. Navegue em WLC GUI > Wireless > FlexConnect Groups > **Select FlexConnect Group** > **General** tab > **Add AP**.

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

Group Name Store 1

FlexConnect APs AAA

Add AP

Select APs from current controller

AP Name AP3500

Ethernet MAC cc:ef:48:c2:35:57

Add Cancel

Primary Radius Server None

Secondary Radius Server None

Enable AP Local Authentication

6. O AP FlexConnect deve ser conectado em uma porta de tronco e a VLAN mapeada de WLAN e a VLAN substituída de AAA devem ser permitidas na porta de

```

interface GigabitEthernet1/0/4
description AP3500
switchport trunk encapsulation dot1q
switchport trunk native vlan 109
switchport trunk allowed vlan 3,109
switchport mode trunk

```

tronco.

Observação: nesta configuração, a vlan 109 é usada para mapeamento de VLAN de WLAN e a vlan 3 é usada para substituição de AAA.

- Configure o mapeamento de WLAN para VLAN para o AP FlexConnect. Com base nessa configuração, o AP teria as interfaces para a VLAN. Quando o AP recebe a configuração da VLAN, as subinterfaces correspondentes dot11 e Ethernet são criadas e adicionadas a um grupo de bridge. Associe um cliente nesta WLAN e quando o cliente se associar, sua VLAN (padrão, com base no mapeamento WLAN-VLAN) é atribuída. Navegue até WLAN GUI > **Wireless** > **All APs** > clique na guia específica AP > **FlexConnect** e clique em **VLAN**

All APs > AP3500 > VLAN Mappings

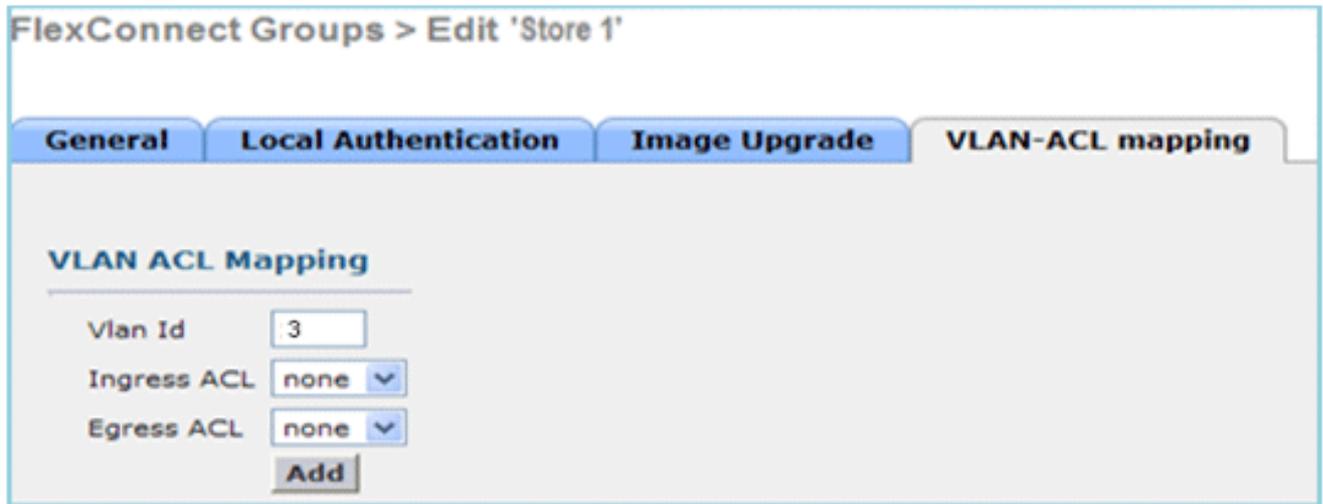
AP Name		AP3500
Base Radio MAC		2c:3f:38:f6:98:b0
WLAN Id	SSID	VLAN ID
1	Store 1	109

Mapping.

- Crie um usuário no servidor AAA e configure o usuário para retornar a ID da VLAN no atributo IETF Radius.

Attribute	Type	Value
IETF 65	Tunnel-Medium-Type	[T:1] 802
IETF 64	Tunnel-Type	[T:1] VLAN
IETF 81	Tunnel-Private-Group-ID	[T:1] 3

- Para ter uma atribuição de VLAN dinâmica, o AP teria as interfaces para a VLAN dinâmica pré-criada com base na configuração usando o mapeamento WLAN-VLAN existente para o AP FlexConnect individual ou usando o mapeamento ACL-VLAN no grupo FlexConnect. Para configurar a VLAN AAA no AP FlexConnect, navegue até a GUI da WLC > **Wireless** > **Grupo FlexConnect** > clique no grupo FlexConnect específico > **mapeamento VLAN-ACL** e insira a VLAN no campo ID da **VLAN**.



10. Associe um cliente nesta WLAN e autentique usando o nome de usuário configurado no servidor AAA para retornar a VLAN AAA.
11. O cliente deve receber um endereço IP da VLAN dinâmica retornada pelo servidor AAA.
12. Para verificar, clique em **WLC GUI > Monitor > Client** > clique no endereço MAC do cliente específico para verificar os detalhes do cliente.

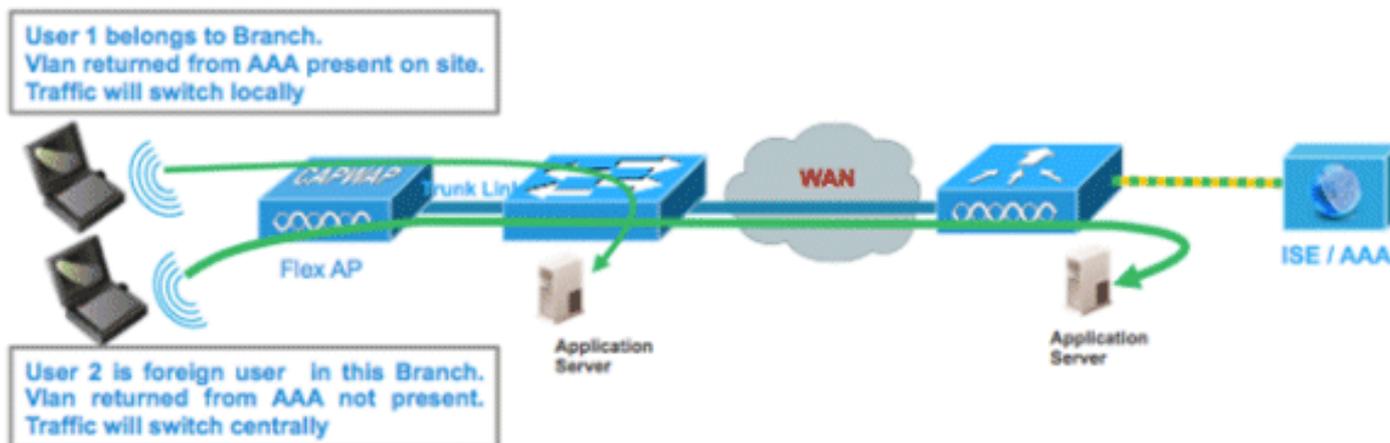
Limitações

- Os atributos específicos do **Cisco Airespace** não serão suportados e o ID da VLAN do atributo IETF será suportado somente.
- Um máximo de 16 VLANs podem ser configuradas na configuração por AP através do mapeamento WLAN-VLAN para AP FlexConnect individual ou usando o mapeamento ACL-VLAN no grupo FlexConnect.

Comutação central baseada em VLAN FlexConnect

Nas versões 7.2 do software da controladora, a substituição AAA da VLAN (atribuição de VLAN dinâmica) para WLANs comutadas localmente colocará os clientes sem fio na VLAN fornecida pelo servidor AAA. Se a VLAN fornecida pelo servidor AAA não estiver presente no AP, o cliente será colocado em uma VLAN mapeada de WLAN nesse AP e o tráfego será alternado localmente nessa VLAN. Além disso, antes da versão 7.3, o tráfego de uma WLAN específica de APs FlexConnect pode ser comutado de forma central ou local, dependendo da configuração da WLAN.

A partir da versão 7.3, o tráfego dos APs FlexConnect pode ser comutado de forma central ou local, dependendo da presença de uma VLAN em um AP FlexConnect.



Summary

Fluxo de tráfego em WLANs configuradas para switching local quando APs flexíveis estão no modo conectado:

- Se a VLAN for retornada como um dos atributos AAA e essa VLAN não estiver presente no banco de dados Flex AP, o tráfego será alternado centralmente e o cliente receberá essa VLAN/Interface retornada do servidor AAA, desde que a VLAN exista na WLC.
- Se a VLAN for retornada como um dos atributos AAA e essa VLAN não estiver presente no banco de dados Flex AP, o tráfego mudará centralmente. Se essa VLAN também não estiver presente na WLC, o cliente receberá uma VLAN/Interface mapeada para uma WLAN na WLC.
- Se a VLAN for retornada como um dos atributos AAA e essa VLAN estiver presente no banco de dados FlexConnect AP, o tráfego será alternado localmente.
- Se a VLAN não for retornada do servidor AAA, o cliente receberá uma VLAN mapeada de WLAN nesse AP FlexConnect e o tráfego será comutado localmente.

Fluxo de tráfego em WLANs configuradas para Switching Local quando APs Flex estão no modo autônomo:

- Se a VLAN retornada por um servidor AAA não estiver presente no banco de dados Flex AP, o cliente será colocado na VLAN padrão (ou seja, uma VLAN mapeada WLAN no Flex AP). Quando o AP se conectar novamente, esse cliente será desautenticado e mudará o tráfego centralmente.
- Se a VLAN retornada por um servidor AAA estiver presente no banco de dados Flex AP, o cliente será colocado em uma VLAN devolvida e o tráfego será comutado localmente.
- Se a VLAN não for retornada de um servidor AAA, o cliente receberá uma VLAN mapeada de WLAN nesse AP FlexConnect e o tráfego será comutado localmente.

Procedimento

Conclua estes passos:

1. Configure uma WLAN para comutação local e ative a substituição de AAA.

WLANs > Edit 'Store 1'

General	Security	QoS	Advanced
Allow AAA Override	<input checked="" type="checkbox"/>	Enabled	
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled	
Enable Session Timeout	<input checked="" type="checkbox"/>	1800	Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/>	Enabled	
Diagnostic Channel	<input type="checkbox"/>	Enabled	
Override Interface ACL		IPv4 None <input type="button" value="v"/>	IPv6 None <input type="button" value="v"/>
P2P Blocking Action		Disabled <input type="button" value="v"/>	
Client Exclusion ³	<input checked="" type="checkbox"/>	Enabled	60 Timeout Value (secs)
Maximum Allowed Clients ⁶		<input type="text" value="0"/>	
Static IP Tunneling ¹¹	<input type="checkbox"/>	Enabled	
Wi-Fi Direct Clients Policy		Disabled <input type="button" value="v"/>	
Maximum Allowed Clients Per AP Radio		<input type="text" value="200"/>	
FlexConnect			
FlexConnect Local Switching ²	<input checked="" type="checkbox"/>	Enabled	

2. Ative a **comutação central baseada em Vlan** na WLAN recém-criada.

WLANs > Edit 'Store 1'

General

Security

QoS

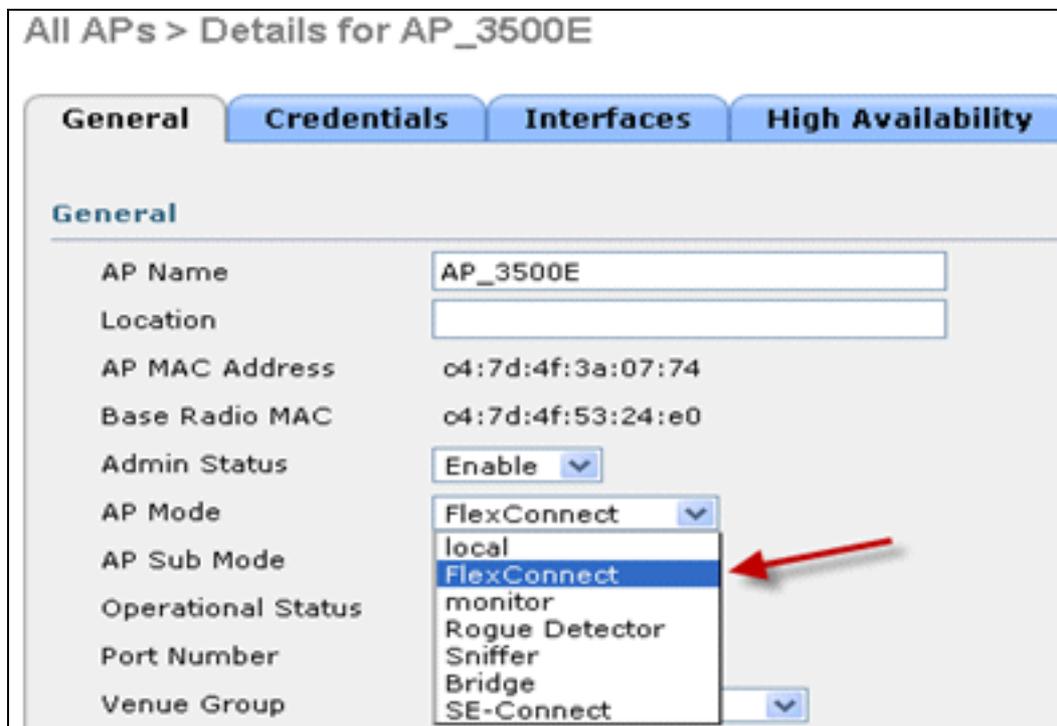
Advanced

Allow AAA Override	<input checked="" type="checkbox"/> Enabled
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled
Enable Session Timeout	<input checked="" type="checkbox"/> <input type="text" value="1800"/> Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/> Enabled
Diagnostic Channel	<input type="checkbox"/> Enabled
Override Interface ACL	IPv4 <input type="text" value="None"/> IPv6 <input type="text" value="None"/>
P2P Blocking Action	<input type="text" value="Disabled"/>
Client Exclusion 3	<input checked="" type="checkbox"/> Enabled <input type="text" value="60"/> Timeout Value (secs)
Maximum Allowed Clients 8	<input type="text" value="0"/>
Static IP Tunneling 11	<input type="checkbox"/> Enabled
Wi-Fi Direct Clients Policy	<input type="text" value="Disabled"/>
Maximum Allowed Clients Per AP Radio	<input type="text" value="200"/>

FlexConnect

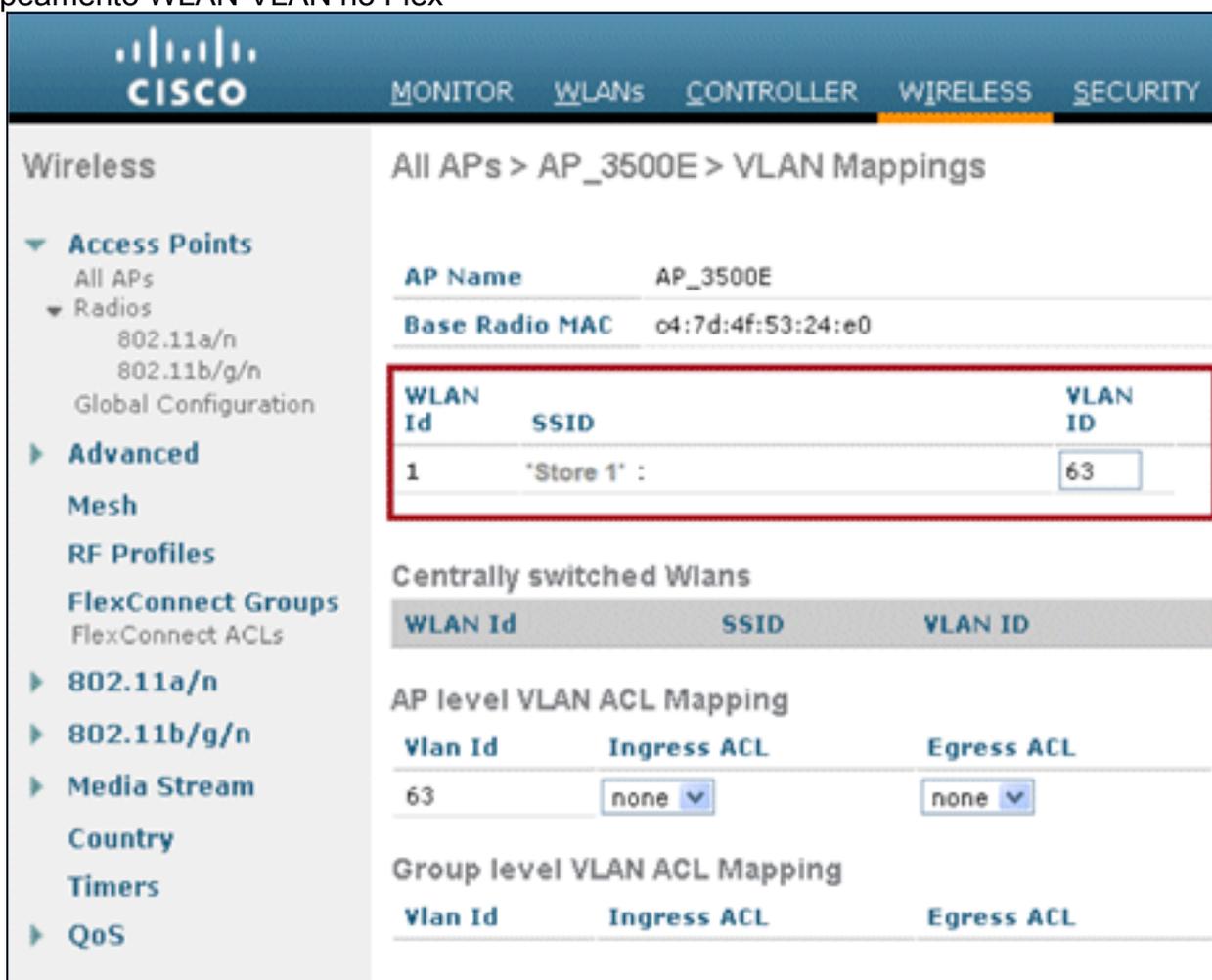
FlexConnect Local Switching 2	<input checked="" type="checkbox"/> Enabled
FlexConnect Local Auth 12	<input type="checkbox"/> Enabled
Learn Client IP Address 5	<input checked="" type="checkbox"/> Enabled
Vlan based Central Switching 13	<input checked="" type="checkbox"/> Enabled

3. Defina o modo AP como



FlexConnect.

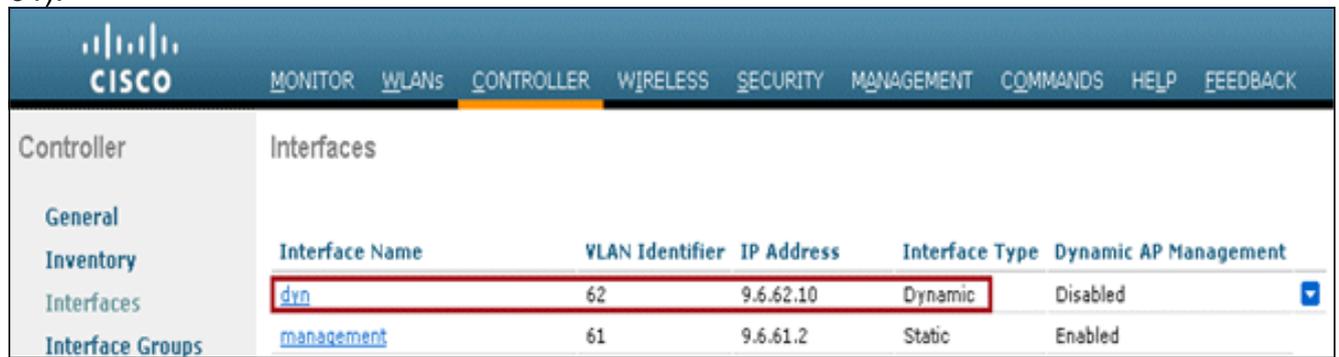
4. Certifique-se de que o AP FlexConnect tenha alguma subinterface presente em seu banco de dados, por meio do mapeamento WLAN-VLAN em um AP Flex específico ou por meio da configuração de VLAN de um grupo Flex. Neste exemplo, a VLAN 63 é configurada no mapeamento WLAN-VLAN no Flex



AP.

5. Neste exemplo, a VLAN 62 é configurada na WLC como uma das interfaces dinâmicas e não é mapeada para a WLAN na WLC. A WLAN na WLC é mapeada para a VLAN de gerenciamento (ou seja, VLAN

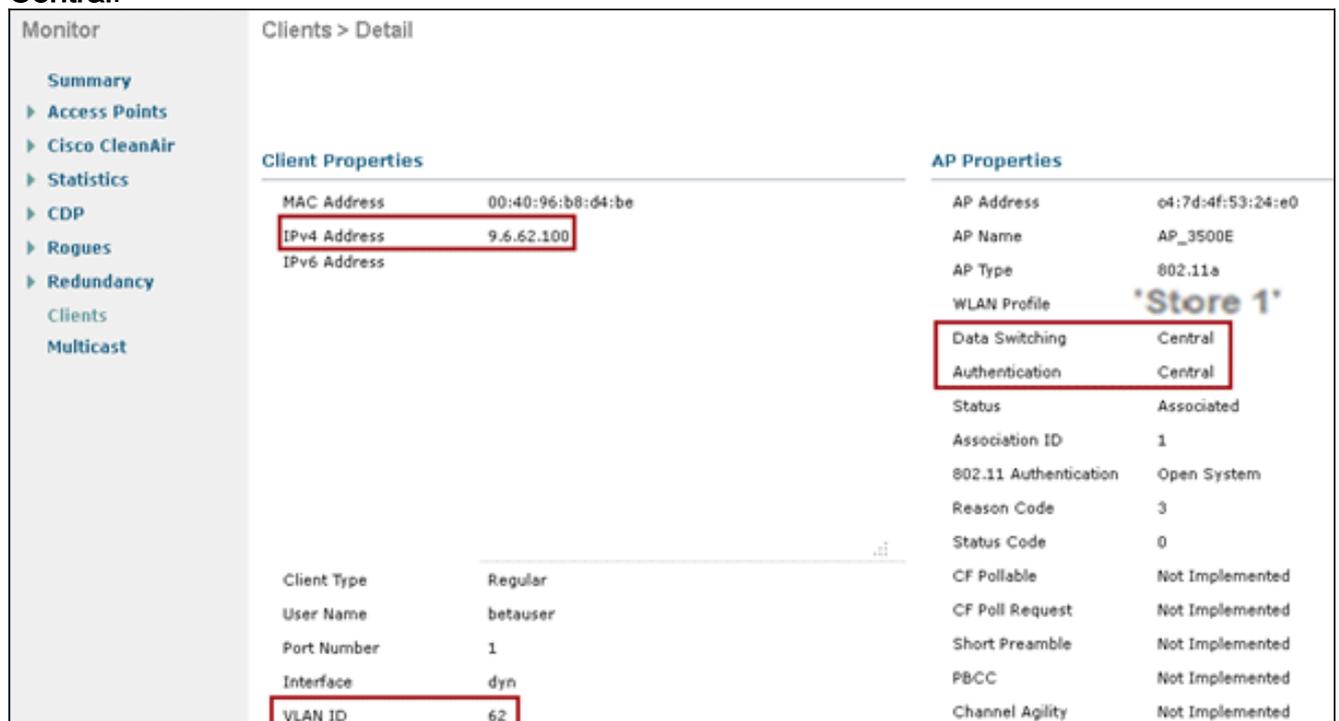
61).



The screenshot shows the Cisco WLC Controller configuration page for Interfaces. The 'Interfaces' tab is selected. A table lists the configured interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
dyn	62	9.6.62.10	Dynamic	Disabled
management	61	9.6.61.2	Static	Enabled

6. Associe um cliente à WLAN configurada na Etapa 1 neste AP Flex e retorne a VLAN 62 do servidor AAA. A VLAN 62 não está presente neste AP Flex, mas está presente na WLC como uma interface dinâmica para que o tráfego comute centralmente e o cliente receba a VLAN 62 na WLC. Na saída capturada aqui, a VLAN 62 foi atribuída ao cliente e a Autenticação e Comutação de Dados estão definidas como **Central**.



The screenshot shows the Cisco WLC Monitor Clients > Detail page. The 'Client Properties' and 'AP Properties' sections are visible. The 'Client Properties' section shows the client's IP address as 9.6.62.100 and the interface as 'dyn'. The 'AP Properties' section shows the WLAN Profile as 'Store 1' and the Data Switching and Authentication settings as 'Central'.

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.62.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	3
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented

Observação: observe que embora a WLAN esteja configurada para Switching Local, o campo Data Switching para este cliente é Central com base na presença de uma VLAN (ou seja, a VLAN 62, que é retornada do servidor AAA, não está presente no banco de dados AP).

7. Se outro usuário se associar ao mesmo AP nesta WLAN criada e alguma VLAN for retornada do servidor AAA que não está presente no AP, assim como na WLC, o tráfego será alternado centralmente e o cliente receberá a interface mapeada da WLAN na WLC (ou seja, a VLAN 61 neste exemplo de configuração), porque a WLAN é mapeada para a interface de gerenciamento configurada para a VLAN

61

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.61.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Central
		Authentication	Central
Client Type	Regular	Status	Associated
User Name	betouser2	Association ID	1
Port Number	1	802.11 Authentication	Open System
Interface	management	Reason Code	3
VLAN ID	61	Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented

Observação: observe que, embora a WLAN esteja configurada para Switching Local, o campo Data Switching desse cliente é Central com base na presença de uma VLAN. Ou seja, a VLAN 61, que é retornada do servidor AAA, não está presente no banco de dados AP, mas também não está presente no banco de dados WLC. Como resultado, ao cliente é atribuída uma interface VLAN/Interface padrão que é mapeada para a WLAN. Neste exemplo, a WLAN é mapeada para uma interface de gerenciamento (ou seja, VLAN 61) e, portanto, o cliente recebeu um endereço IP da VLAN 61.

8. Se outro usuário associado a ele nessa WLAN criada e a VLAN 63 for retornada do servidor AAA (presente neste AP Flex), o cliente receberá a VLAN 63 e o tráfego será comutado localmente.

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central

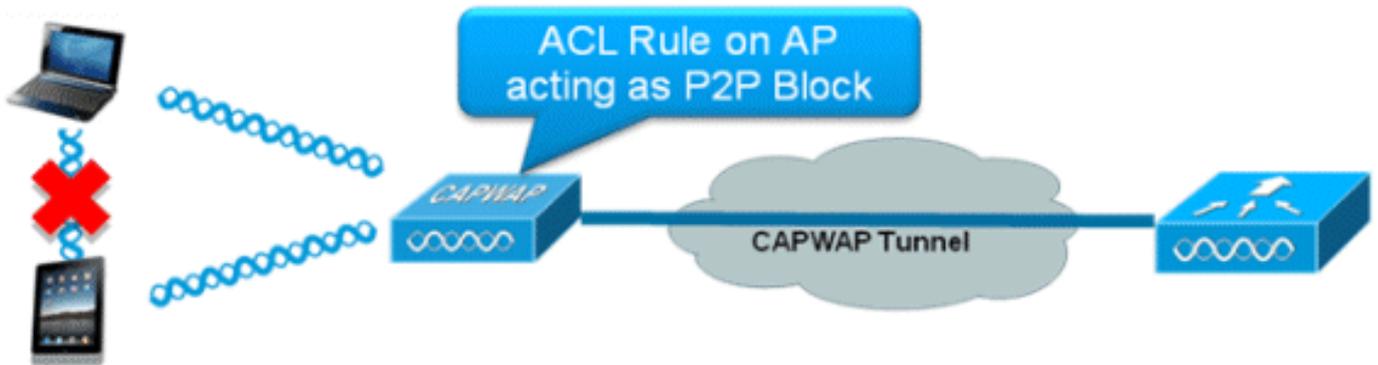
Limitações

- A comutação central baseada em VLAN só é suportada em WLANs configuradas para autenticação central e comutação local.
- A subinterface do AP (ou seja, o mapeamento de VLAN) deve ser configurada no AP

FlexConnect.

ACL FlexConnect

Com a introdução de ACLs no FlexConnect, há um mecanismo para atender à necessidade de controle de acesso no AP FlexConnect para proteção e integridade do tráfego de dados comutados localmente do AP. As ACLs FlexConnect são criadas na WLC e devem ser configuradas com a VLAN presente no AP FlexConnect ou no grupo FlexConnect usando o mapeamento VLAN-ACL que será para VLANs de substituição AAA. Eles são então empurrados para o AP.



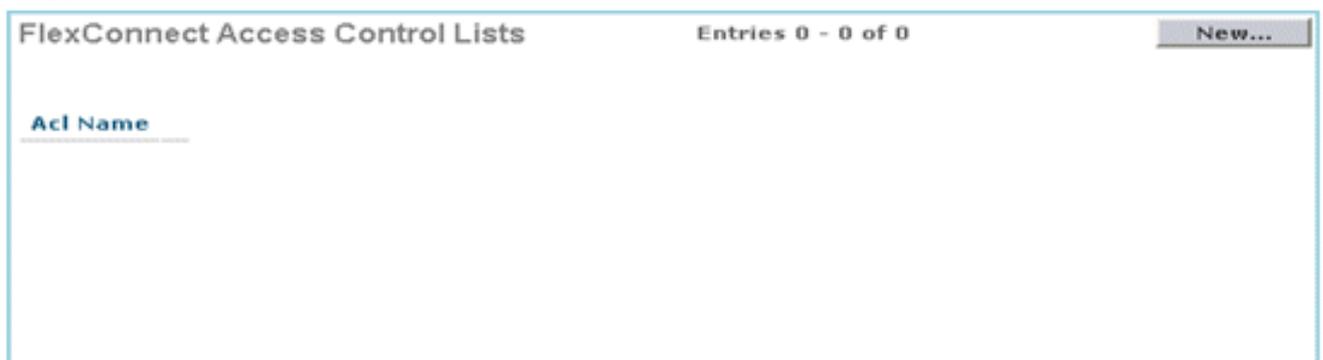
Summary

- Crie a ACL FlexConnect no controlador.
- Aplique o mesmo em uma VLAN presente no AP FlexConnect no mapeamento da ACL de VLAN de nível de AP.
- Pode ser aplicada em uma VLAN presente no grupo FlexConnect sob mapeamento VLAN-ACL (geralmente feito para VLANs sobrepostas AAA).
- Ao aplicar a ACL na VLAN, selecione a direção a ser aplicada, que será "ingresso", "egresso" ou "ingresso e saída".

Procedimento

Conclua estes passos:

1. Crie uma ACL FlexConnect na WLC. Navegue até **WLC GUI > Security > Access Control List > FlexConnect ACLs**.



2. Clique em **New**.
3. Configure o nome da ACL.

Access Control Lists > New

< Back Apply

Access Control List Name Flex-ACL-Ingress

4. Clique em Apply.
5. Crie regras para cada ACL. Para criar regras, navegue até **WLC GUI > Security > Access Control List > FlexConnect ACLs** e clique na ACL criada acima.

Access Control Lists > Edit

< Back Add New Rule

General

Access List Name Flex-ACL-Ingress

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
-----	--------	----------------	---------------------	----------	-------------	-----------	------

6. Clique em **Adicionar nova regra**.

Access Control Lists > Rules > New

< Back Apply

Sequence 1

Source IP Address IP Address 0.0.0.0 Netmask 0.0.0.0

Destination IP Address IP Address 0.0.0.0 Netmask 0.0.0.0

Protocol Any

DSCP Any

Action Deny

Observação: configure as regras de acordo com o requisito. Se a regra permit any any não estiver configurada no final, há uma negação implícita que bloqueará todo o tráfego.

7. Depois que as ACLs FlexConnect são criadas, elas podem ser mapeadas para mapeamento WLAN-VLAN em AP FlexConnect individual ou podem ser aplicadas no mapeamento VLAN-ACL no grupo FlexConnect.

8. Mapeie a ACL FlexConnect configurada acima no nível de AP para VLANs individuais em mapeamentos de VLAN para AP FlexConnect individual. Navegue até WLC GUI > **Wireless** > **All AP** > clique no AP específico > guia **FlexConnect** > **VLAN Mapping**.

All APs > AP3500 > VLAN Mappings

AP Name	AP3500	
Base Radio MAC	2c:3f:38:f6:98:b0	
WLAN Id	SSID	VLAN ID
1	Store 1	109

Centrally switched Wlans

WLAN Id	SSID	VLAN ID
2	Store 3	N/A

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
109	Flex-ACL-Ingress	Flex-ACL-Egress

9. A ACL FlexConnect também pode ser aplicada no mapeamento VLAN-ACL no grupo FlexConnect. As VLANs criadas no mapeamento VLAN-ACL no grupo FlexConnect são usadas principalmente para substituição dinâmica de VLAN.

FlexConnect Groups > Edit 'Store 1'

General | **Local Authentication** | **Image Upgrade** | **VLAN-ACL mapping**

VLAN ACL Mapping

Vlan Id:

Ingress ACL: Flex-ACL-Egress

Egress ACL: Flex-ACL-Egress

Vlan Id	Ingress ACL	Egress ACL
3	Flex-ACL-Ingress	Flex-ACL-Egress

Limitações

- Um máximo de 512 ACLs FlexConnect podem ser configuradas na WLC.
- Cada ACL individual pode ser configurada com 64 regras.
- Um máximo de 32 ACLs pode ser mapeado por grupo FlexConnect ou por AP FlexConnect.
- A qualquer momento, há um máximo de 16 VLANs e 32 ACLs no AP FlexConnect.

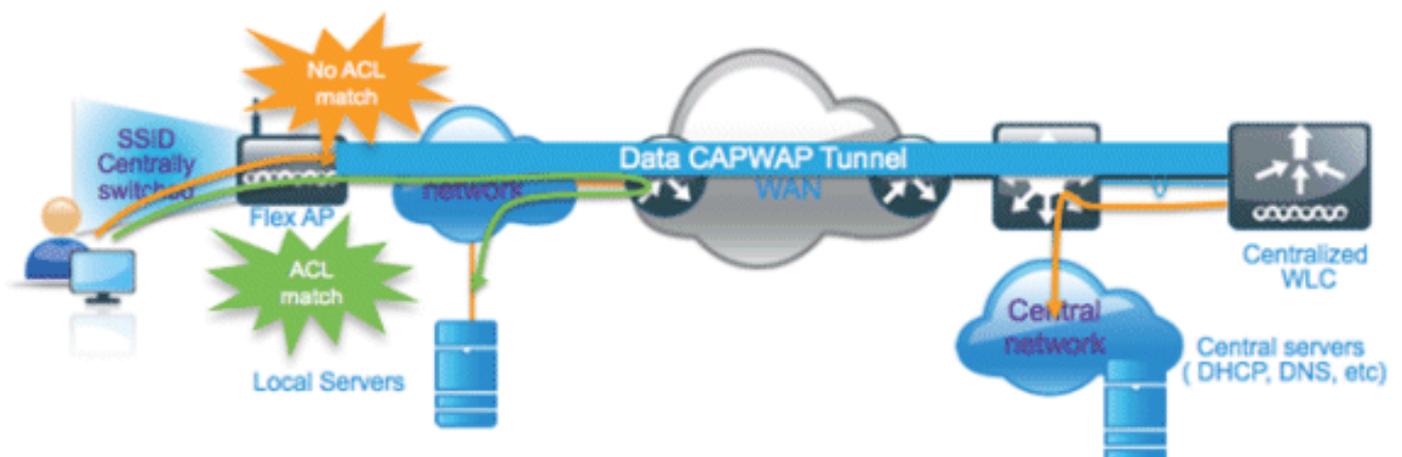
Encapsulamento dividido FlexConnect

Nas versões de WLC anteriores à 7.3, se um cliente que se conecta em um AP FlexConnect associado a uma WLAN centralmente comutada precisar enviar algum tráfego para um dispositivo presente no local/rede, ele precisará enviar o tráfego sobre CAPWAP para a WLC e, em seguida, obter o mesmo tráfego de volta para o local por CAPWAP ou usando alguma conectividade fora da banda.

A partir da versão 7.3, o **Split Tunneling** introduz um mecanismo pelo qual o tráfego enviado pelo cliente será classificado com base no conteúdo do pacote **usando a ACL Flex**. Os pacotes correspondentes são comutados localmente do AP Flex e o restante dos pacotes são comutados centralmente sobre o CAPWAP.

A funcionalidade Split Tunneling é uma vantagem adicional para a configuração do AP OEAP, onde os clientes em um SSID corporativo podem se comunicar com dispositivos em uma rede local (impressoras, máquinas com fio em uma porta LAN remota ou dispositivos sem fio em um SSID pessoal) diretamente sem consumir a largura de banda da WAN, enviando pacotes sobre CAPWAP. O tunelamento dividido não é suportado nos APs OEAP 600. A ACL flexível pode ser criada com regras para permitir todos os dispositivos presentes no local/rede. Quando os pacotes de um cliente sem fio no SSID corporativo correspondem às regras na ACL flexível configurada no AP OEAP, esse tráfego é comutado localmente e o restante do tráfego (ou seja, tráfego deny implícito) comutará centralmente sobre o CAPWAP.

A solução de tunelamento dividido pressupõe que a sub-rede/VLAN associada a um cliente no local central não está presente no local (ou seja, o tráfego para clientes que recebem um endereço IP da sub-rede presente no local central não poderá comutar localmente). A funcionalidade Split Tunneling foi projetada para comutar o tráfego localmente para as sub-redes que pertencem ao local, a fim de evitar o consumo de largura de banda da WAN. O tráfego que corresponde às regras da ACL Flex é comutado localmente e a operação NAT é executada alterando o endereço IP origem do cliente para o endereço IP da interface BVI do Flex AP, que é roteável no local/rede.



Summary

- A funcionalidade de tunelamento dividido é suportada em WLANs configuradas para switching central anunciadas somente por APs Flex.
- O DHCP necessário deve ser ativado nas WLANs configuradas para tunelamento dividido.
- A configuração de tunelamento dividido é aplicada por WLAN configurada para comutação central por AP Flex ou para todos os APs Flex em um grupo FlexConnect.

Procedimento

Conclua estes passos:

1. Configure uma WLAN para switching central (isto é, **Comutação local flexível** não deve ser habilitada).

WLANs > Edit 'Store 1'

General Security QoS Advanced

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

P2P Blocking Action

Client Exclusion Enabled 60
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

FlexConnect

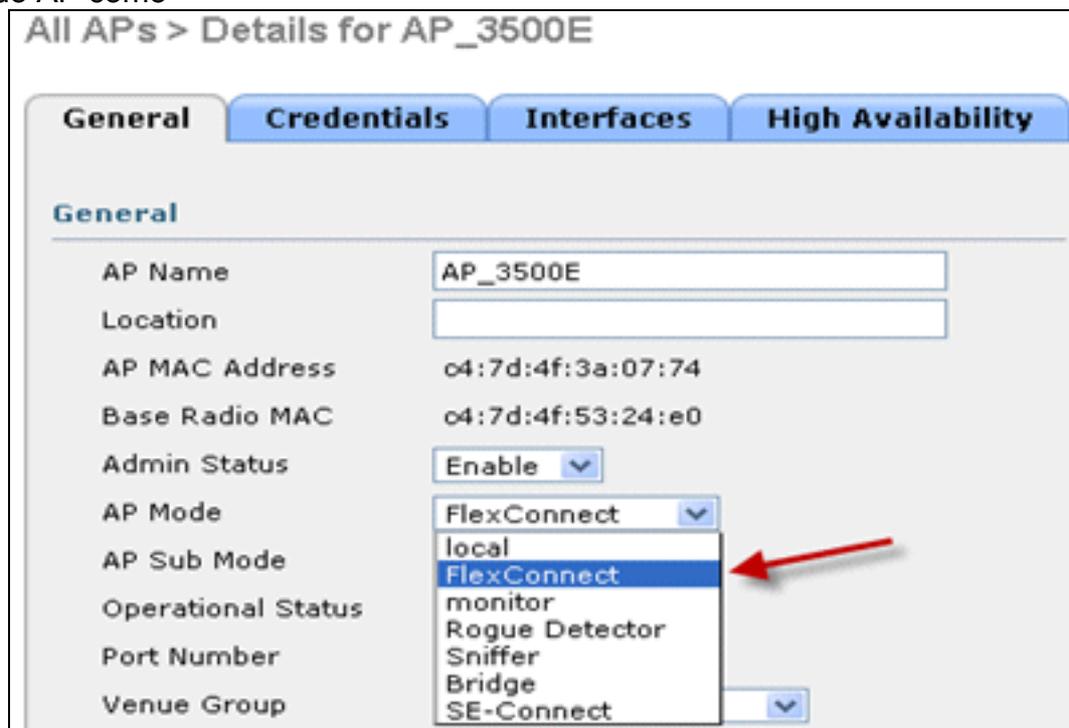
FlexConnect Local Switching Enabled

Flex Local Switching should not be enabled

2. Defina DHCP Address Assignment (Atribuição de endereço DHCP) como **Required (Obrigatório)**.



3. Defina o modo AP como



FlexConnect.

4. Configure a ACL FlexConnect com uma regra de permissão para tráfego que deve ser comutado localmente na WLAN do Switch Central. Neste exemplo, a regra da ACL FlexConnect é configurada para que ela alerte o tráfego ICMP de todos os clientes que estão na sub-rede 9.6.61.0 (ou seja, existe no local central) para 9.1.0.150 para que seja comutado localmente depois que a operação NAT é aplicada no AP Flex. O restante do tráfego atingirá uma regra de negação implícita e será comutado centralmente sobre CAPWAP.

Wireless

Access Points

- All APs
- Radios
 - 802.11a/n
 - 802.11b/g/n
- Global Configuration
- Advanced
- Mesh
- RF Profiles
- FlexConnect Groups
 - FlexConnect ACLs

Access Control Lists > Edit

General

Access List Name Flex-ACL

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	9.6.61.0	9.1.0.150	ICMP	Any	Any	Any
		255.255.255.0	255.255.255.255				

5. Essa ACL FlexConnect criada pode ser enviada como uma ACL de túnel dividido para AP Flex individual ou também pode ser enviada para todos os APs Flex em um grupo Flex Connect. Conclua estes passos para enviar a ACL Flex como uma ACL Dividida Local para o AP Flex individual: Clique em **Local Split** **ACLs**.

Wireless

All APs > Details for AP_3500E

General Credentials Interfaces High Availability Inventory FlexConnect Advanced

VLAN Support

Native VLAN ID 57 [VLAN Mappings](#)

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#)

[Local Split ACLs](#)

Selecione **WLAN Id** em que o recurso Split Tunnel deve estar habilitado, escolha **Flex-ACL** e clique em **Add**.

All APs > AP_3500E > ACL Mappings

AP Name AP_3500E

Base Radio MAC 04:7d:4f:53:24:e0

WLAN ACL Mapping

WLAN Id

Local-Split ACL

Enter WLAN ID on which Split Tunnel should be enabled

Click Add after selecting Flex ACL

WLAN Id	WLAN Profile Name	Local-Split ACL
---------	-------------------	-----------------

O Flex-ACL é enviado como ACL de divisão local para o AP

All APs > AP_3500E > ACL Mappings

AP Name AP_3500E

Base Radio MAC 04:7d:4f:53:24:e0

WLAN ACL Mapping

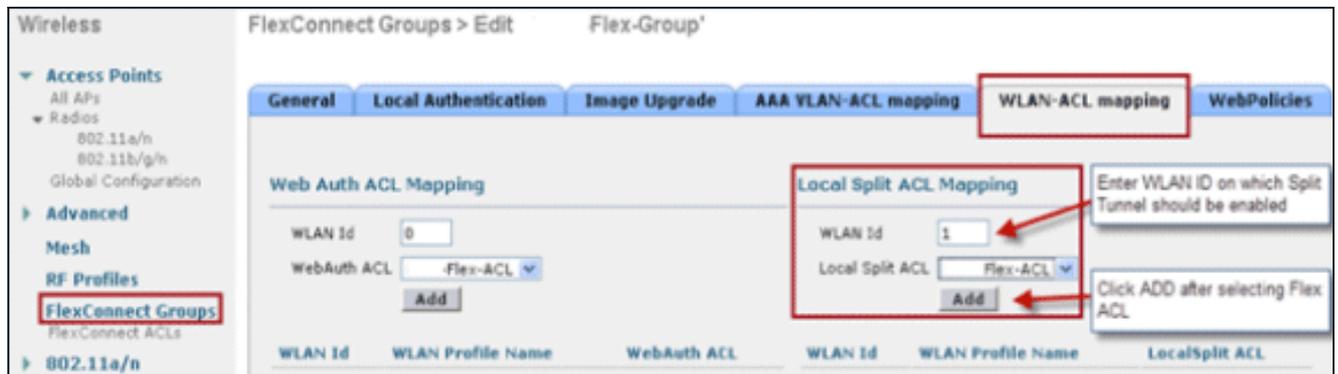
WLAN Id

Local-Split ACL

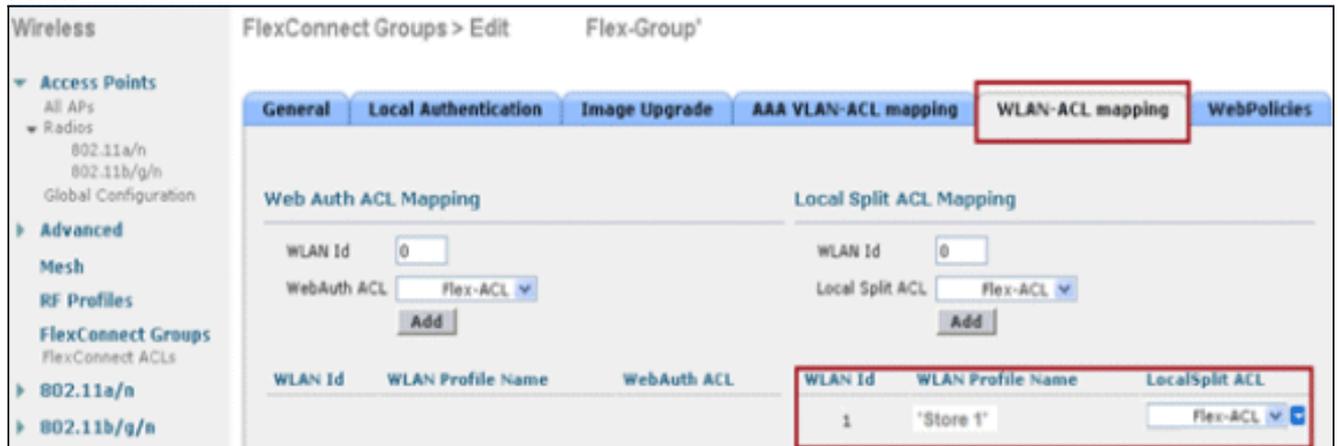
WLAN Id	WLAN Profile Name	Local-Split ACL
1	'Store 1'	Flex-ACL

Flex.

Conclua estes passos para enviar a ACL Flex como ACL de divisão local para um grupo FlexConnect:Selecione a ID da WLAN na qual o recurso Split Tunneling deve estar ativado. Na guia **WLAN-ACL mapping**, selecione FlexConnect ACL no grupo FlexConnect, onde os APs Flex específicos são adicionados, e clique em **Add**.



O Flex-ACL é enviado como ACL LocalSplit para APs Flex nesse grupo Flex.



Limitações

- As regras de ACL flexível não devem ser configuradas com a instrução permit/deny com a mesma sub-rede que a origem e o destino.
- O tráfego em uma WLAN Comutada Centralmente configurada para o Encapsulamento Dividido pode ser comutado localmente somente quando um cliente sem fio inicia o tráfego para um host presente no local. Se o tráfego for iniciado por clientes/hosts em um site local para clientes sem fio nessas WLANs configuradas, ele não poderá alcançar o destino.
- O tunelamento dividido não é compatível com o tráfego Multicast/Broadcast. O tráfego multicast/broadcast será comutado centralmente mesmo que corresponda à ACL Flex.

Tolerância a falhas

A tolerância a falhas do FlexConnect permite acesso sem fio e serviços para clientes de filiais quando:

- Os APs da filial FlexConnect perdem conectividade com o controlador Flex 7500 principal.
- Os APs FlexConnect Branch estão alternando para o controlador Flex 7500 secundário.
- Os APs FlexConnect Branch estão restabelecendo a conexão com o controlador Flex 7500 principal.

A tolerância a falhas do FlexConnect, juntamente com o EAP local conforme descrito acima, fornecem tempo de inatividade zero para a filial durante uma interrupção da rede. Esta funcionalidade está ativada por predefinição e não pode ser desativada. Ele não requer configuração no controlador ou no AP. No entanto, para garantir que a tolerância a falhas funcione sem problemas e seja aplicável, estes critérios devem ser mantidos:

- Os pedidos e as configurações de WLAN devem ser idênticos entre os controladores Flex 7500 principal e de backup.
- O mapeamento de VLAN deve ser idêntico entre os controladores Flex 7500 principal e de backup.
- O nome do domínio de mobilidade deve ser idêntico entre os controladores Flex 7500 principal e de backup.
- Recomenda-se usar o Flex 7500 como controladores principal e de backup.

Summary

- O FlexConnect não desconectará clientes quando o AP estiver se conectando de volta ao mesmo controlador, desde que não haja alteração na configuração do controlador.
- O FlexConnect não desconectará os clientes ao se conectar ao controlador de backup, desde que não haja alteração na configuração e o controlador de backup seja idêntico ao controlador principal.
- O FlexConnect não redefinirá seus rádios ao conectar-se novamente ao controlador principal, desde que não haja alteração na configuração do controlador.

Limitações

- Suportado somente para FlexConnect com autenticação central/local com switching local.
- Os clientes autenticados centralmente exigem uma reautenticação completa se o temporizador de sessão do cliente expirar antes que o FlexConnect AP alterne do modo autônomo para o modo conectado.
- Os controladores primário e de backup Flex 7500 devem estar no mesmo domínio de mobilidade.

Limite do cliente por WLAN

Juntamente com a segmentação de tráfego, surge a necessidade de restringir o acesso total do cliente aos serviços sem fio.

Exemplo: Limitando o total de clientes convidados do tunelamento de filial de volta ao data center.

Para lidar com esse desafio, a Cisco está introduzindo o recurso Client Limit per WLAN que pode restringir o total de clientes permitidos por WLAN.

Objetivo principal

- Definir limites para o máximo de clientes
- Facilidade operacional

Observação: esta não é uma forma de QoS.

Por padrão, o recurso está desabilitado e não força o limite.

Limitações

Este recurso não impõe o limite de cliente quando o FlexConnect está no estado de operação independente.

Configuração de WLC

Conclua estes passos:

1. Selecione o ID 1 da WLAN com switching central com SSID **DataCenter**. Essa WLAN foi criada durante a criação do Grupo AP. Consulte a [Figura 8](#).
2. Clique na guia **Advanced** para WLAN ID 1.
3. Defina o valor limite do cliente para o campo de texto Máximo de clientes permitidos.
4. Clique em **Apply** depois que o campo de texto Maximum Allowed Clients for definido.

The screenshot shows the 'WLANs > Edit' configuration page for a WLAN. The 'Advanced' tab is selected. The 'Maximum Allowed Clients' field is highlighted with a red box and contains the value '0'. Other visible fields include 'Session Timeout (secs)' set to 1800, 'Client Exclusion' set to 60, and 'Scan Defer Time(msecs)' set to 100. The 'Foot Notes' section at the bottom contains several numbered notes, with note 9 highlighted in red: '9 Value zero implies there is no restriction on maximum clients allowed.'

O padrão para Máximo de clientes permitidos é 0, o que implica que não há restrição e o recurso está desativado.

Configuração do NCS

Para habilitar esse recurso do NCS, vá para Configure > Controllers > Controller IP > **WLANs > WLAN Configuration > WLAN Configuration Details**.

WLAN Configuration Details : 17

Configure > Controllers > 172.20.225.154 > WLANs > WLAN Configuration > **WLAN Configuration Details**

General

Security

QoS

Advanced

FlexConnect Local Switching Enable

FlexConnect Local Auth ⓘ Enable

Learn Client IP Address Enable

Session Timeout Enable (secs)

Coverage Hole Detection Enable

Aironet IE Enable

IPv6 [?](#) Enable

Diagnostic Channel [?](#) Enable

Override Interface ACL IPv4 ▼

IPv6 ▼

Peer to Peer Blocking ⓘ ▼

Wi-Fi Direct Clients Policy ▼

Client Exclusion [!](#) Enable

Timeout Value (secs)

Maximum Clients ⓘ

DHCP

DHCP Server

DHCP Address Assignment

Management Frame Protection

MFP Client Protection [?](#)

MFP Version

Load Balancing and Band Sel

Client Load Balancing

Client Band Select

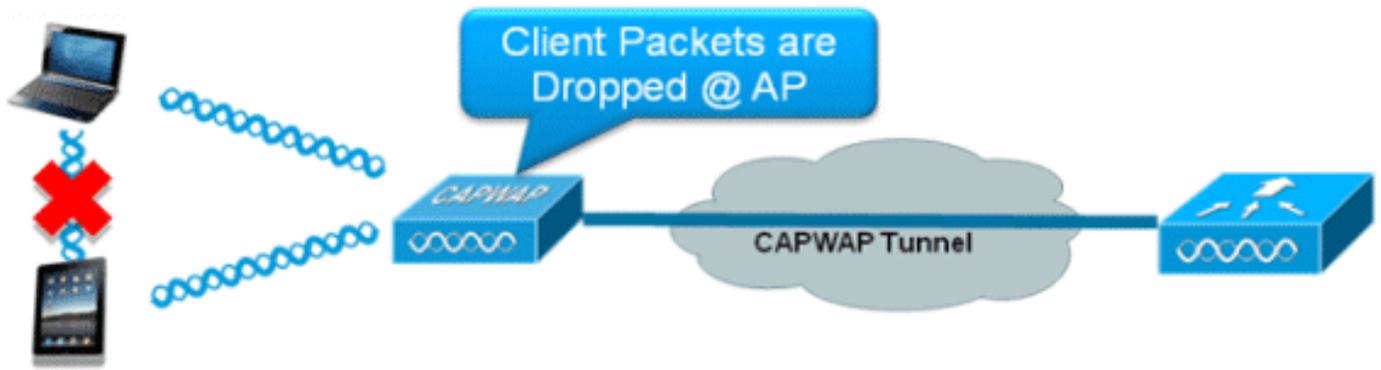
NAC

Bloqueio ponto-a-ponto

Nas versões de software do controlador anteriores à 7.2, o bloqueio peer-to-peer (P2P) só era suportado para WLANs de comutação central. O bloqueio ponto-a-ponto pode ser configurado na WLAN com qualquer uma destas três ações:

- **Disabled (Desabilitado)** - Desabilita o bloqueio ponto-a-ponto e o tráfego em ponte localmente no controlador para clientes na mesma sub-rede. Este é o valor padrão.
- **Drop** - Faz com que o controlador descarte pacotes para clientes na mesma sub-rede.
- **Forward Up-Stream** - Faz com que o pacote seja encaminhado na VLAN upstream. Os dispositivos acima do controlador decidem que ação tomar em relação ao pacote.

A partir da versão 7.2, o bloqueio ponto-a-ponto é suportado para clientes associados à WLAN de switching local. Por WLAN, a configuração ponto-a-ponto é enviada pelo controlador para o AP FlexConnect.



Summary

- O bloqueio ponto-a-ponto é configurado por WLAN
- Por WLAN, a configuração de bloqueio ponto-a-ponto é enviada pela WLC para APs FlexConnect.
- A ação de bloqueio ponto-a-ponto configurada como derivação ou upstream-forward na WLAN é tratada como bloqueio ponto-a-ponto ativado no AP FlexConnect.

Procedimento

Conclua estes passos:

1. Ative a ação de bloqueio ponto a ponto como **Drop** on WLAN configurado para FlexConnect Local Switching.

2. Quando a ação de bloqueio P2P é configurada como **Drop** ou **Forward-Upstream** na WLAN configurada para switching local, ela é enviada da WLC para o AP FlexConnect. Os APs FlexConnect armazenarão essas informações no arquivo de configuração do mapa na flash. Com isso, mesmo quando o AP FlexConnect está no modo autônomo, ele pode aplicar a configuração P2P nas subinterfaces correspondentes.

Limitações

- No FlexConnect, a configuração de bloqueio P2P da solução não pode ser aplicada somente a um AP FlexConnect específico ou a um subconjunto de APs. Ele é aplicado a todos os APs FlexConnect que transmitem o SSID.
- A solução unificada para clientes de switching central suporta encaminhamento de upstream P2P. No entanto, isso não será suportado na solução FlexConnect. Isso é tratado como descarte P2P e os pacotes do cliente são descartados em vez de encaminhados para o próximo nó de rede.
- A solução unificada para clientes de switching central suporta bloqueio P2P para clientes associados a APs diferentes. No entanto, essa solução destina-se somente a clientes conectados ao mesmo AP. As ACLs FlexConnect podem ser usadas como uma solução alternativa para essa limitação.

Download de pré-imagem de AP

Esse recurso permite que o AP faça o download do código enquanto estiver operacional. O download da pré-imagem do AP é extremamente útil para reduzir o tempo de inatividade da rede durante a manutenção ou atualizações do software.

Summary

- Facilidade de gerenciamento de software
- Agendar atualizações por loja: o NCS é necessário para realizar isso
- Reduz o tempo de inatividade

Procedimento

Conclua estes passos:

1. Atualize a imagem nos controladores principal e de backup. Navegue em **WLC GUI > Commands > Download File** para iniciar o

The screenshot shows the 'Download file to Controller' configuration page in the WLC GUI. It includes the following fields and settings:

- File Type:** Code
- Transfer Mode:** TFTP
- Server Details:**
 - IP Address:** [Redacted]
 - Maximum retries:** 10
 - Timeout (seconds):** 6
 - File Path:** [Empty]
 - File Name:** AS_5500_7_0_112_52.aes

download.

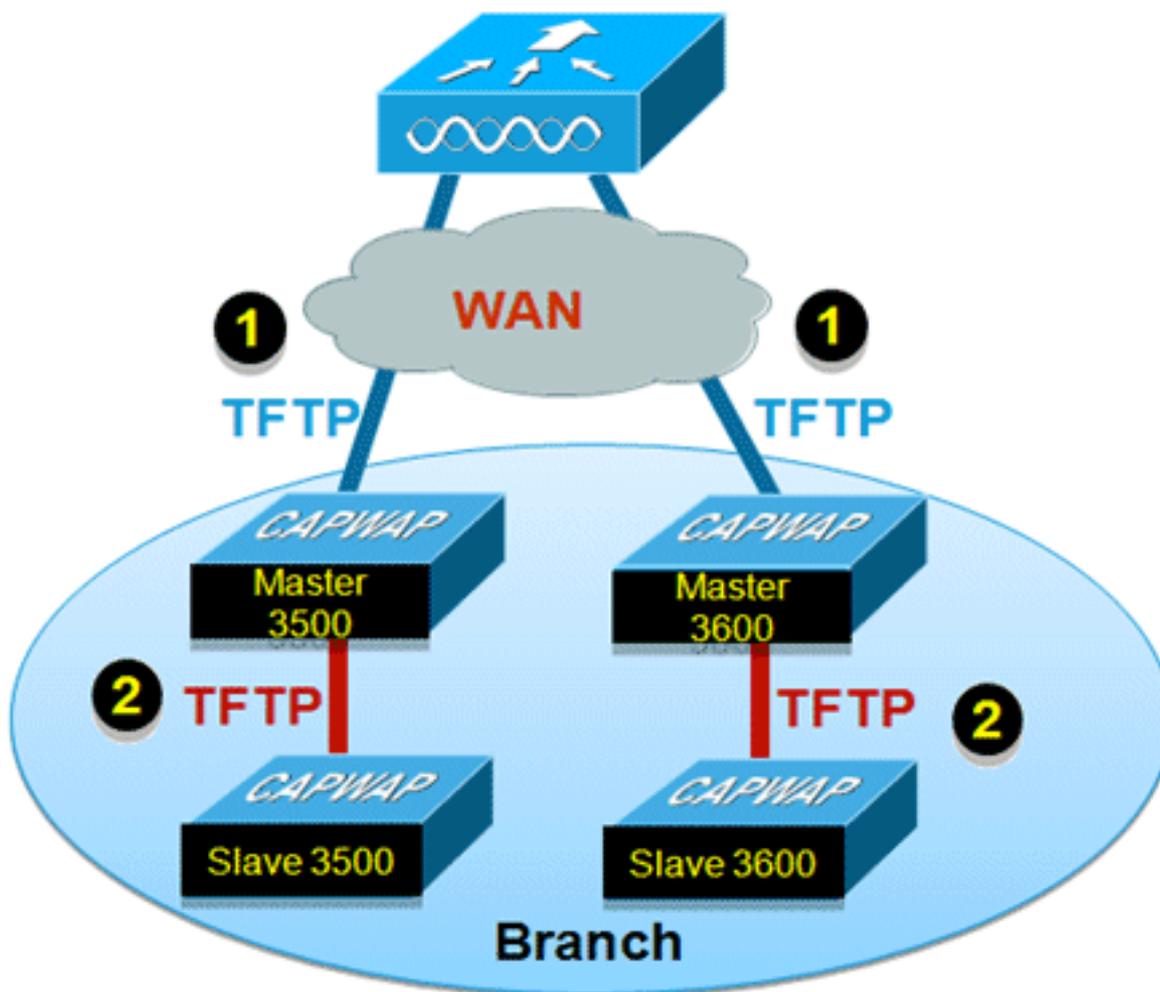
2. Salve as configurações nos controladores, mas não reinicialize o controlador.
3. Emita o comando AP pre-image download do controlador primário. Navegue até **WLC GUI > Wireless > Access Points > All APs** e escolha o access point para iniciar o download da pré-imagem. Depois de escolher o ponto de acesso, clique na guia **Avançado**. Clique em **Baixar primário** para iniciar o download de pré-

- Funciona somente com APs CAPWAP.

Atualização de imagem do FlexConnect Smart AP

O recurso de download de pré-imagem reduz a duração do tempo de inatividade em certa medida, mas ainda assim todos os APs FlexConnect têm que fazer o pré-download das respectivas imagens de AP sobre o link da WAN com maior latência.

A atualização eficiente da imagem do AP reduzirá o tempo de inatividade para cada AP FlexConnect. A ideia básica é que apenas um AP de cada modelo de AP baixará a imagem do controlador e atuará como Mestre/Servidor, e o restante dos APs do mesmo modelo funcionará como Slave/Client e fará o pré-download da imagem de AP do mestre. A distribuição da imagem do AP do servidor para o cliente estará em uma rede local e não experimentará a latência do link da WAN. Como resultado, o processo será mais rápido.



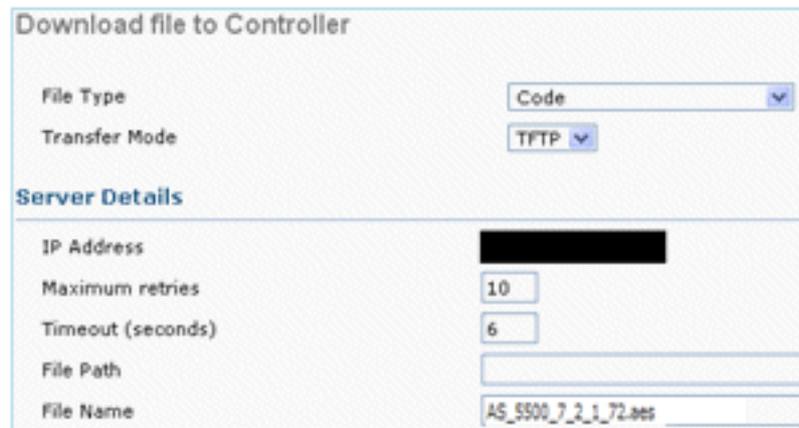
Summary

- Os APs Master e Slave são selecionados para cada modelo de AP por grupo FlexConnect
- O mestre faz o download da imagem do WLC
- O escravo faz o download da imagem do AP mestre
- Reduz o tempo de inatividade e economiza a largura de banda da WAN

Procedimento

Conclua estes passos:

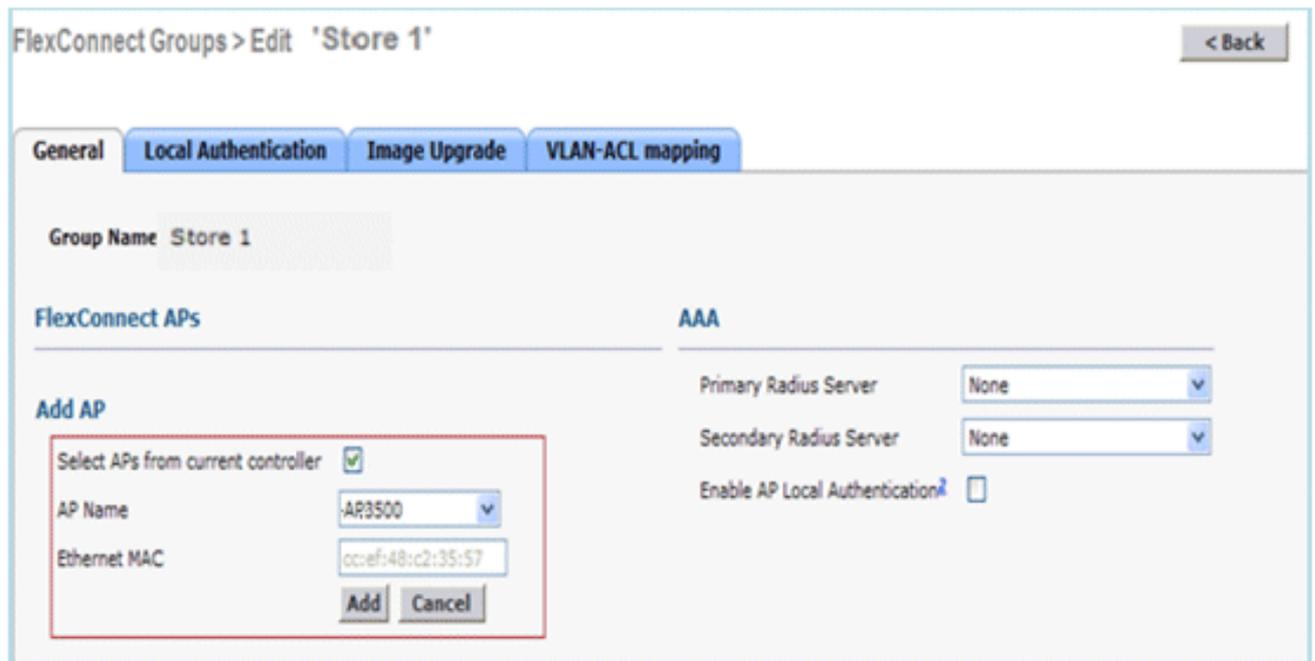
1. Atualize a imagem no controlador. Navegue até **WLC GUI > Commands > Download File**



File Type	Code
Transfer Mode	TFTP
Server Details	
IP Address	[REDACTED]
Maximum retries	10
Timeout (seconds)	6
File Path	
File Name	AS_5500_7_2_1_72.bin

para iniciar o download.

2. Salve as configurações nos controladores, mas não reinicialize o controlador.
3. Adicione os APs FlexConnect ao grupo FlexConnect. Navegue até **WLC GUI > Wireless > FlexConnect Groups > selecione FlexConnect Group > General tab > Add AP**.



FlexConnect Groups > Edit 'Store 1' < Back

General Local Authentication Image Upgrade VLAN-ACL mapping

Group Name Store 1

FlexConnect APs **AAA**

Add AP

Select APs from current controller

AP Name AR3500

Ethernet MAC cc:ef:48:c2:35:57

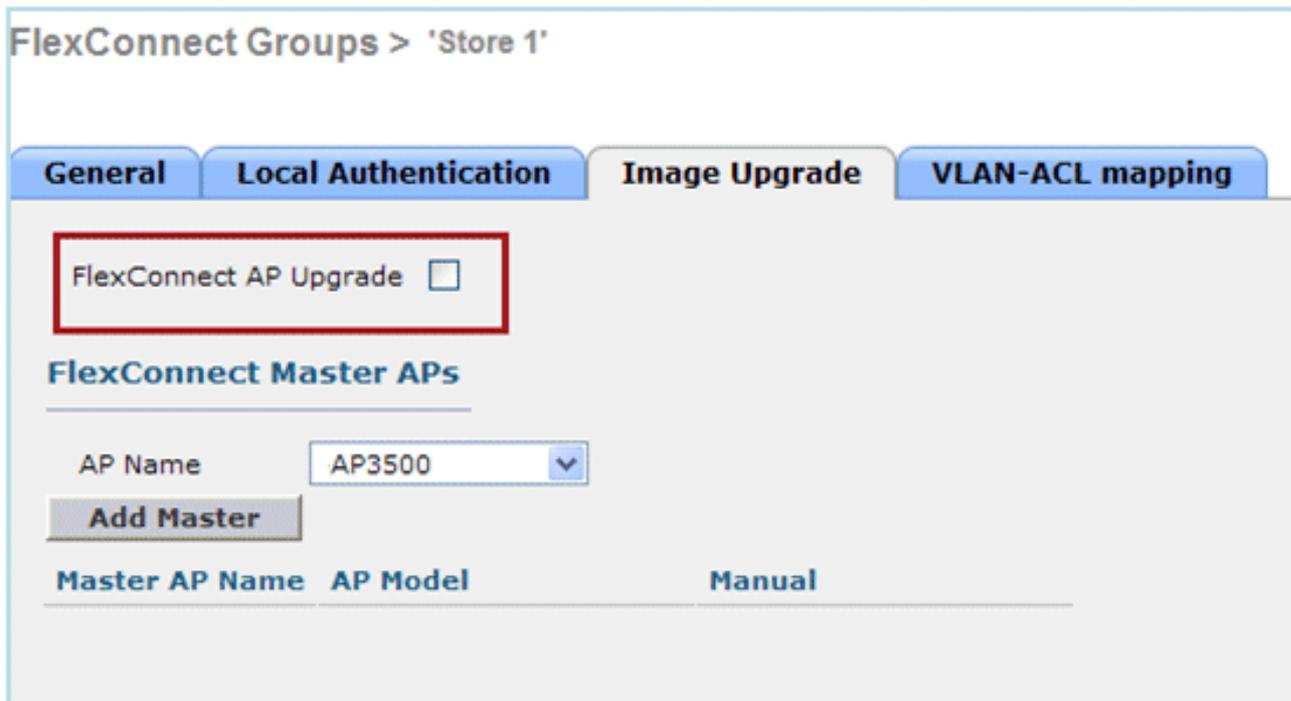
Add Cancel

Primary Radius Server None

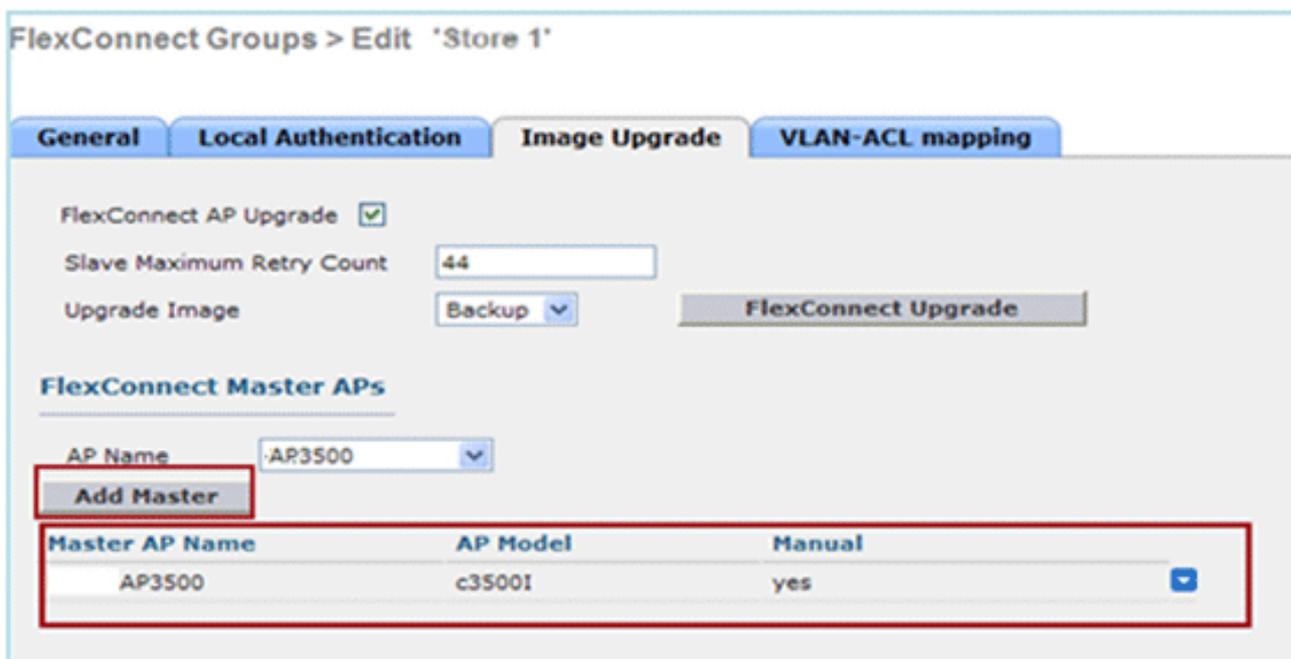
Secondary Radius Server None

Enable AP Local Authentication

4. Clique na caixa de seleção **FlexConnect AP Upgrade** para obter uma atualização eficiente da imagem do AP. Navegue até GUI do WLC > **Wireless > Grupos FlexConnect > selecione a guia Grupo FlexConnect > Atualização de imagem**.



5. O AP mestre pode ser selecionado manual ou automaticamente: Para selecionar manualmente o AP mestre, navegue até a GUI do WLC > Wireless > FlexConnect Groups > selecione FlexConnect Group > Image Upgrade tab > FlexConnect Master APs, selecione APs na lista suspensa e clique em **Add Master**.



Observação: somente um AP por modelo pode ser configurado como AP mestre. Se o AP mestre for configurado manualmente, o campo Manual será atualizado como **sim**. Para selecionar automaticamente o AP mestre, navegue até a GUI do WLC > Wireless > FlexConnect Groups > selecione a guia **FlexConnect Group** > **Image Upgrade** e clique em **FlexConnect Upgrade**.

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count

Upgrade Image

FlexConnect Master APs

AP Name

Master AP Name	AP Model	Manual
AP3500-1	c3500I	no

Observação: se o AP mestre for selecionado automaticamente, o campo Manual será atualizado como **não**.

6. Para iniciar a atualização eficiente da imagem do AP para todos os APs em um grupo FlexConnect específico, clique em **Atualização do FlexConnect**. Navegue até GUI do WLC > Wireless > FlexConnect Groups > selecione **FlexConnect group** > **Image Upgrade** tab e clique em **FlexConnect Upgrade**.

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count

Upgrade Image

Observação: Contagem máxima de tentativas escravas é o número de tentativas (44 por padrão) nas quais o AP escravo fará o download de uma imagem do AP mestre, após as quais ele voltará para fazer o download da imagem do WLC. Ele fará 20 tentativas contra a WLC para baixar uma nova imagem, após a qual o administrador precisa reiniciar o processo de download.

7. Depois que a atualização do FlexConnect for iniciada, somente o AP mestre baixará a imagem do WLC. Na página Todos os AP, a "**Função de Atualização**" será atualizada como **Mestre/Central**, o que significa que o AP Mestre baixou a imagem da WLC que está no local central. O AP escravo baixará a imagem do AP mestre que está no site local e é o motivo na página All AP "**Upgrade Role**" será atualizada como **Slave/Local**. Para verificar isso, navegue até **WLC GUI > Wireless**.

AP Name	AP Model	AP MAC	Download Status	Upgrade Role (Master/Slave)
AP3600	AIR-CAP3602I-A-K9	44:d3:ca:42:31:62	None	
AP3500	AIR-CAP3502I-A-K9	cc:ef:48:c2:35:57	Complete	Slave/Local
AP3500-1	AIR-CAP3502I-A-K9	c4:71:fe:49:ed:5e	Complete	Master/Central

8. Reinicie os controladores após o download de todas as imagens de AP. Os APs agora voltam para o modo autônomo até que os controladores sejam reinicializados. **Observação:** no modo independente, a tolerância a falhas manterá os clientes associados. Quando o controlador estiver de volta, os APs reinicializarão automaticamente com a imagem pré-baixada. Após a reinicialização, os APs entram novamente no controlador principal e retomam os serviços do cliente.

Limitações

- A seleção de AP mestre é por grupo FlexConnect e por modelo de AP em cada grupo.
- Apenas 3 APs escravos do mesmo modelo podem atualizar simultaneamente de seu AP mestre e o restante dos APs escravos usarão o temporizador de recuo aleatório para tentar novamente o AP mestre para fazer o download da imagem do AP.
- Caso o AP escravo falhe ao fazer download da imagem do AP mestre por algum motivo, ele irá para o WLC para buscar a nova imagem.
- Isso funciona somente com APs CAPWAP.

Converter automaticamente APs no modo FlexConnect

O Flex 7500 fornece estas duas opções para converter o modo AP em FlexConnect:

- Modo manual
- Modo de conversão automática

Modo manual

Esse modo está disponível em todas as plataformas e permite que a alteração ocorra somente por AP.

1. Navegue até **WLC GUI > Wireless > All APs** e escolha o AP.
2. Selecione **FlexConnect** como o modo AP e clique em **Apply**.
3. A alteração do modo AP faz com que o AP seja reinicializado.

All APs > Details for AP3500

General	Credentials	Interfaces	High Availability
General			
AP Name	AP3500		
Location	default location		
AP MAC Address	00:22:90:e3:37:df		
Base Radio MAC	00:22:bd:d1:71:30		
Admin Status	Disable ▾		
AP Mode	local ▾		
AP Sub Mode	local FlexConnect monitor Rogue Detector Sniffer Bridge SE-Connect		
Operational Status			
Port Number			
Venue Group	▾		

Essa opção também está disponível em todas as plataformas WLC atuais.

Modo de conversão automática

Esse modo está disponível somente para o Flex 7500 Controller e é suportado somente com CLI. Esse modo aciona a alteração em todos os APs conectados. Recomenda-se que o Flex 7500 seja implantado em um domínio de mobilidade diferente dos controladores de campus de WLC existentes antes que você habilite esta CLI:

```
(Cisco Controller) >config ap autoconvert ?
```

```
disable          Disables auto conversion of unsupported mode APs to supported
                  modes when AP joins
flexconnect      Converts unsupported mode APs to flexconnect mode when AP joins
monitor         Converts unsupported mode APs to monitor mode when AP joins
```

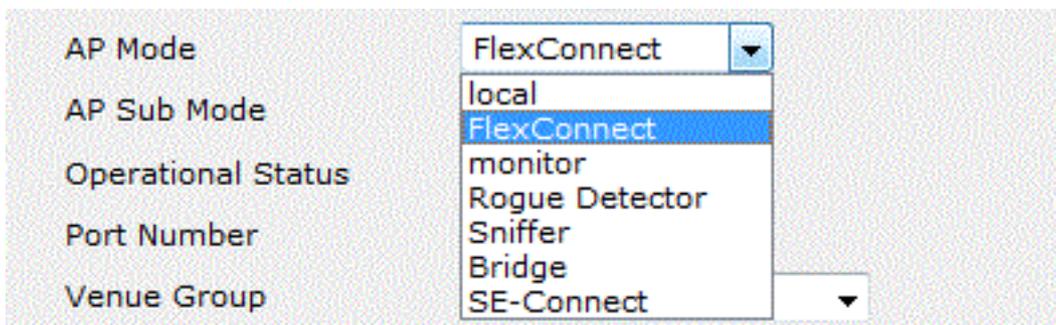
```
(Cisco Controller) >
```

1. O recurso de conversão automática está desabilitado por padrão, o que pode ser verificado usando este comando **show**:

```
(Cisco Controller) >show ap autoconvert
```

```
AP Autoconvert ..... Disabled
```

Modos AP não suportados = Modo local, Farejador, Detector de falha e



Bridge. Esta opção está disponível atualmente somente através de CLIs. Essas CLIs estão disponíveis somente no WLC 7500.

2. A execução do **config ap autoconvert flexconnect** CLI converte todos os APs na rede com o modo AP não suportado para o modo FlexConnect. Os APs que já estão no FlexConnect ou no modo de monitor não são afetados.

```
(Cisco Controller) >config ap autoconvert flexconnect
```

```
(Cisco Controller) >show ap autoconvert
```

```
AP Autoconvert ..... FlexConnect
```

```
(Cisco Controller) >
```

3. A execução do comando **config ap autoconvert monitor** CLI converte todos os APs na rede com o modo AP não suportado para o modo Monitor. Os APs que já estão no modo FlexConnect ou Monitor não são afetados.

```
(Cisco Controller) >config ap autoconvert monitor
```

```
(Cisco Controller) >show ap autoconvert
```

```
AP Autoconvert ..... Monitor
```

Não há opção para executar o **config ap autoconvert flexconnect** e o **config ap autoconvert monitor** ao mesmo tempo.

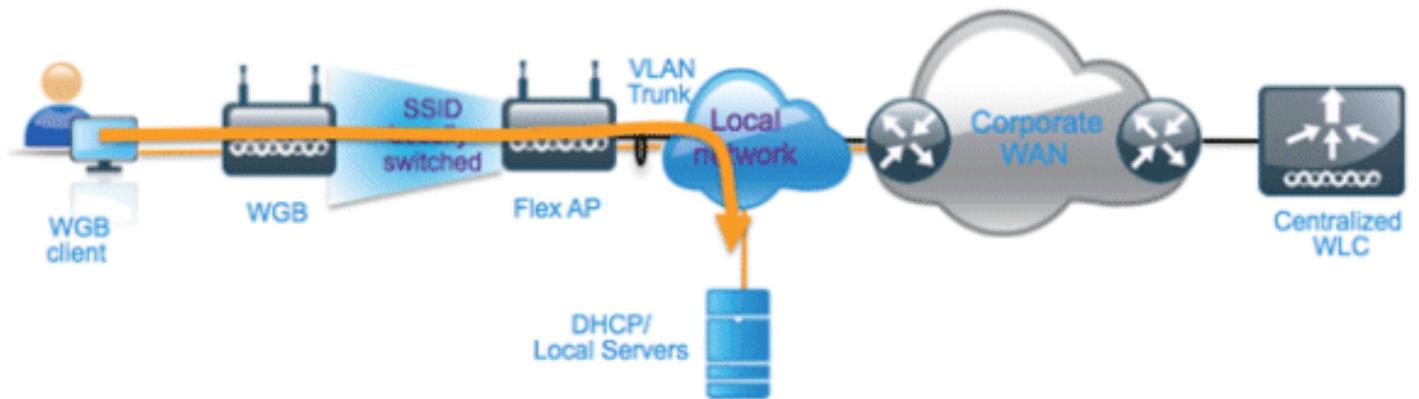
[Suporte FlexConnect WGB/uWGB para WLANs de switching local](#)

A partir da versão 7.3, os clientes WGB/uWGB e com/sem fio atrás das WGBs são suportados e funcionarão como clientes normais nas WLANs configuradas para switching local.

Após a associação, o WGB envia as mensagens IAPP para cada um de seus clientes com fio/sem fio, e o AP Flex se comportará da seguinte forma:

- Quando o AP Flex está no modo conectado, ele encaminha todas as mensagens do IAPP para o controlador e o controlador processará as mensagens do IAPP da mesma forma que o AP do modo Local. O tráfego para clientes com/sem fio será comutado localmente a partir de APs Flex.
- Quando o AP está no modo independente, ele processa as mensagens do IAPP, os clientes com/sem fio no WGB devem ser capazes de registrar e cancelar o registro. Após a transição para o modo conectado, o AP Flex enviará as informações dos clientes com fio de volta ao controlador. O WGB enviará mensagens de registro três vezes quando o Flex AP passar do modo autônomo para o modo conectado.

Os clientes com fio/sem fio herdarão a configuração do WGB, o que significa que não é necessária nenhuma configuração separada, como autenticação AAA, substituição AAA e ACL FlexConnect para clientes por trás do WGB.



Summary

- Não é necessária nenhuma configuração especial na WLC para oferecer suporte a WGB no Flex AP.
- A tolerância a falhas é suportada para WGB e clientes atrás de WGB.
- O WGB é suportado em um AP do IOS: 1240, 1130, 1140, 1260 e 1250.

Procedimento

Conclua estes passos:

1. Nenhuma configuração especial é necessária para habilitar o suporte WGB/uWGB em APs FlexConnect para WLANs configuradas para switching local como WGB. Além disso, os clientes atrás de WGB são tratados como clientes normais em WLANs configuradas de switching local por APs Flex. Ative a **comutação local FlexConnect** em uma WLAN.

WLANS > Edit 'Store 1'

General

Security

QoS

Advanced

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

P2P Blocking Action

Client Exclusion Enabled
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

Clear HotSpot Configuration Enabled

FlexConnect

FlexConnect Local Switching Enabled

2. Defina o modo AP como

All APs > Details for AP_3500E

General Credentials Interfaces High Availability

General

AP Name AP_3500E

Location

AP MAC Address 04:7d:4f:3a:07:74

Base Radio MAC 04:7d:4f:53:24:e0

Admin Status Enable

AP Mode FlexConnect

AP Sub Mode

Operational Status

Port Number

Venue Group

local
FlexConnect
monitor
Rogue Detector
Sniffer
Bridge
SE-Connect

FlexConnect.

- Associe a WGB a clientes com fio por trás dessa WLAN configurada.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Clients

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status	Auth	Port	WGB
00:40:96:b8:d4:be	AP_3500E	*Store 1*	*Store 1*	N/A	Associated	Yes	1	No
00:50:b6:09:e5:3b	AP_3500E	*Store 1*	*Store 1*	N/A	Associated	Yes	1	No
04:7d:4f:3a:08:10	AP_3500E	*Store 1*	*Store 1*	802.11an	Associated	Yes	1	Yes

- Para verificar os detalhes do WGB, vá para **Monitor > Clients** e selecione **WGB** na lista de clientes.

Clients > Detail

Client Properties		AP Properties	
MAC Address	04:7d:4f:3a:08:10	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.63.102	AP Name	AP_3500E
IPv6 Address		AP Type	802.11an
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	1
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
Client Type	WGB		
Number of Wired Client(s)	2		

5. Para verificar os detalhes dos clientes com/sem fio atrás do WGB, vá para **Monitor > Clients** e selecione o cliente.

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:50:b6:09:e5:3b	AP Address	04:7d:4f:53:24:e0
IPv4 Address	96.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	0
		802.11 Authentication	Open System
		Reason Code	1
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
Client Type	WGB Client		
WGB MAC Address	04:7d:4f:3a:08:10		

Limitações

- Os clientes com fio atrás do WGB sempre estarão na mesma VLAN que o próprio WGN. O suporte a várias VLANs para clientes por trás da WGB não é suportado no Flex AP para WLANs configuradas para switching local.
- Um máximo de 20 clientes (com fio/sem fio) são suportados atrás da WGB quando associados ao AP Flex na WLAN configurada para switching local. Esse número é igual ao que temos hoje para suporte WGB no modo local AP.

- O Web Auth não é suportado para clientes por trás do WGB associado em WLANs configuradas para comutação local.

Suporte para um número maior de servidores Radius

Antes da versão 7.4, a configuração de servidores RADIUS no grupo FlexConnect era feita de uma lista global de servidores RADIUS no controlador. O número máximo de servidores RADIUS, que podem ser configurados nesta lista global, é 17. Com um número cada vez maior de filiais, é necessário poder configurar um servidor RADIUS por filial. Na versão 7.4 em diante, será possível configurar servidores RADIUS primários e de backup por grupo FlexConnect, que podem ou não fazer parte da lista global de 17 servidores de autenticação RADIUS configurados no controlador.

Uma configuração específica de AP para os servidores RADIUS também será suportada. A configuração específica do AP terá maior prioridade do que a configuração do grupo FlexConnect.

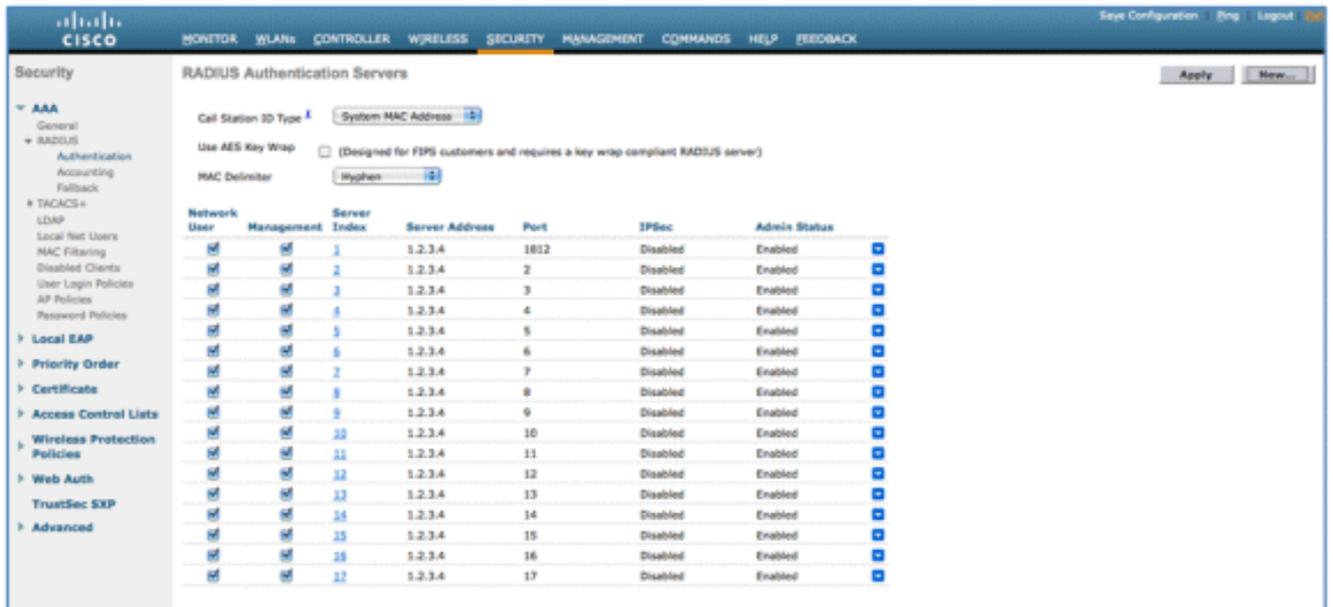
O comando de configuração existente no grupo FlexConnect, que precisa do índice do servidor RADIUS na lista global de servidores RADIUS no controlador, será substituído e substituído por um comando de configuração, que configura um servidor RADIUS no grupo Flexconnect usando o endereço IP do servidor e o segredo compartilhado.

Summary

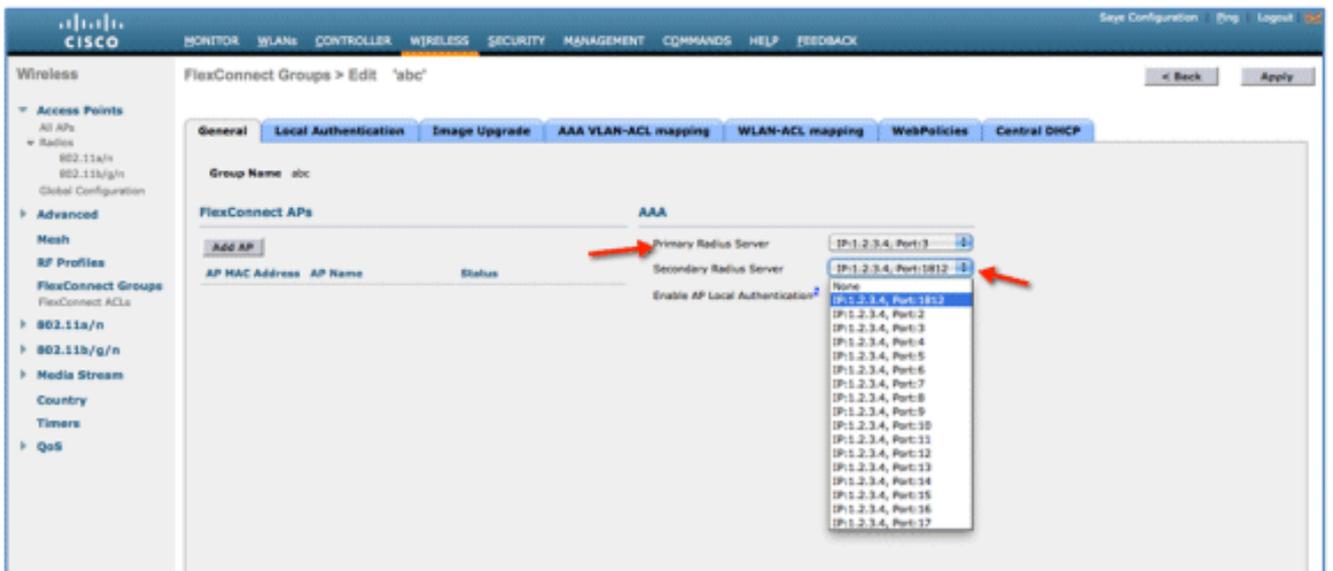
- Suporte para a configuração de servidores RADIUS primários e de backup por grupo FlexConnect, que podem ou não estar presentes na lista global de servidores de autenticação RADIUS.
- O número máximo de servidores RADIUS exclusivos que podem ser adicionados em uma WLC é o número de grupos FlexConnect que podem ser configurados em uma determinada plataforma vezes dois. Um exemplo é um servidor RADIUS primário e um secundário por grupo FlexConnect.
- A atualização do software de uma versão anterior para a versão 7.4 não causará nenhuma perda de configuração do RADIUS.
- A exclusão do servidor RADIUS primário é permitida sem a necessidade de excluir o servidor RADIUS secundário. Isso é consistente com a configuração atual do grupo FlexConnect para o servidor RADIUS.

Procedimento

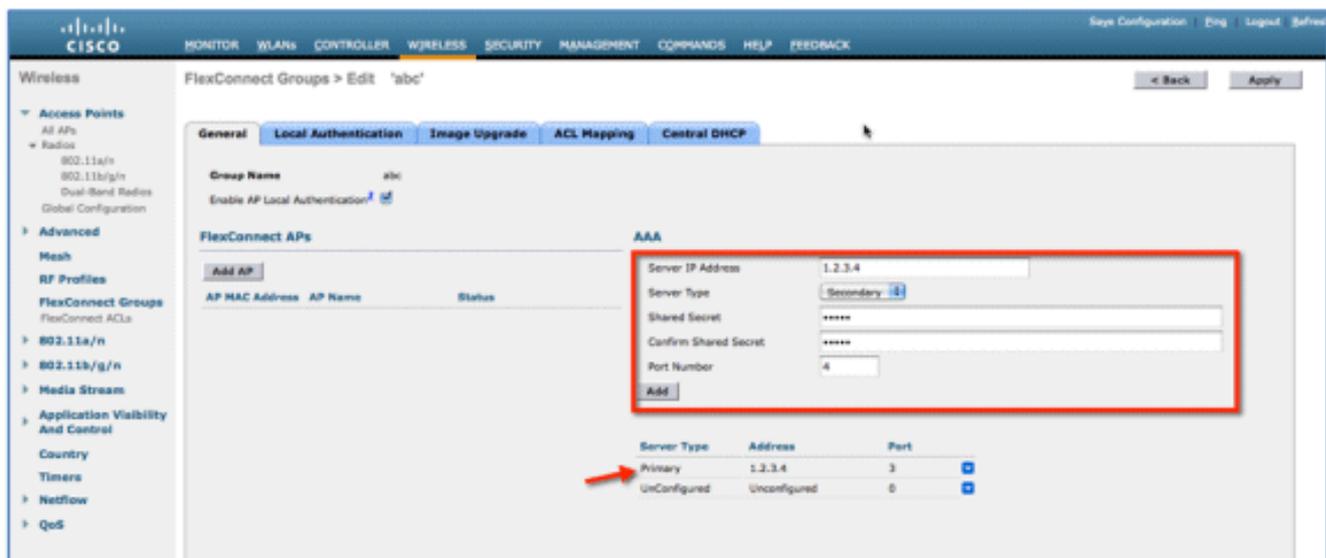
1. Modo de configuração anterior à versão 7.4. Um máximo de 17 servidores RADIUS podem ser configurados na configuração Autenticação AAA.



2. Os servidores RADIUS primário e secundário podem ser associados a um grupo FlexConnect usando uma lista suspensa composta de servidores RADIUS configurados na página Autenticação AAA.



3. Modo de configuração no FlexConnect Group na versão 7.4. Os servidores RADIUS primário e secundário podem ser configurados no grupo FlexConnect usando um endereço IP, número de porta e segredo compartilhado.



Limitações

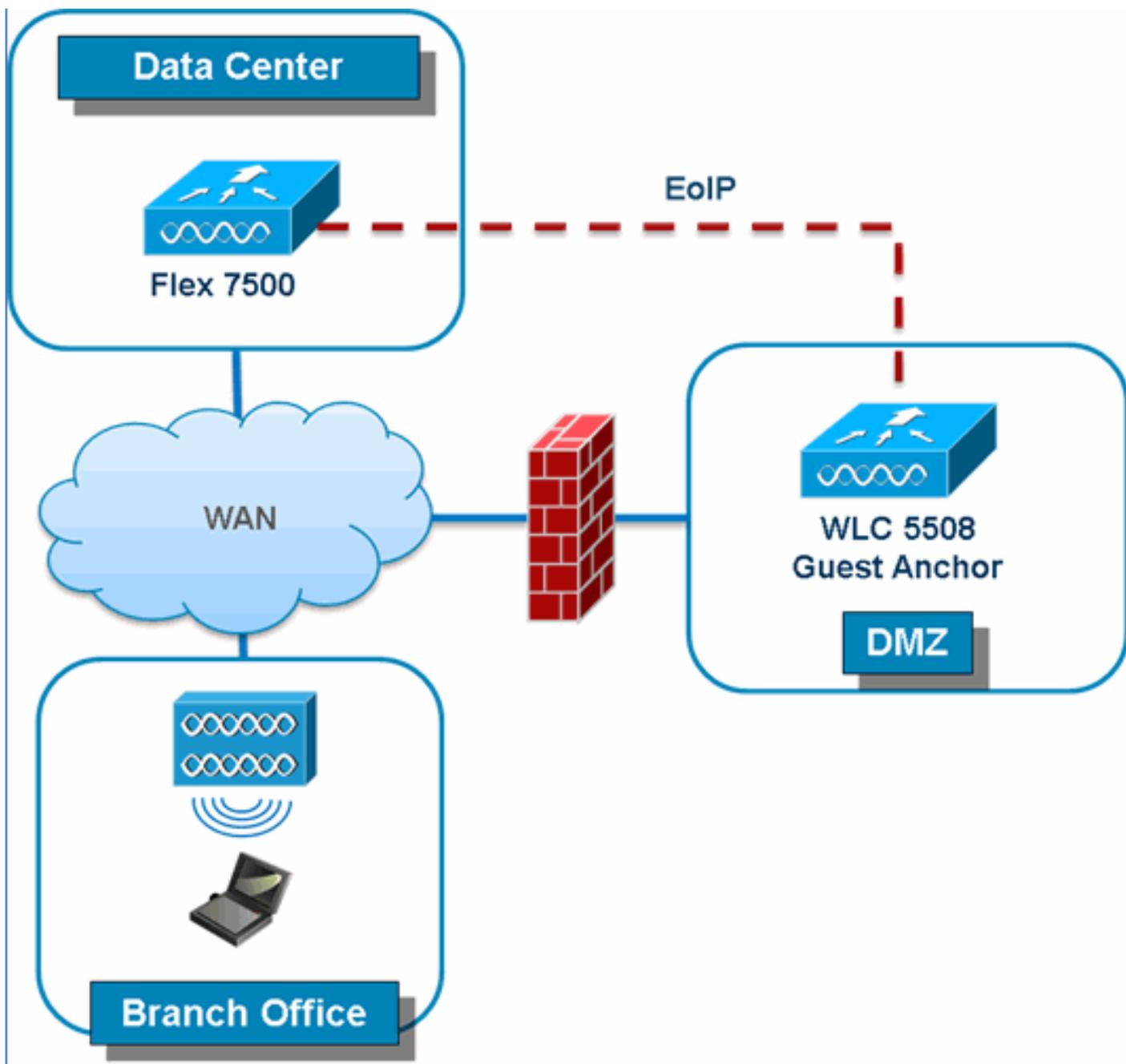
- O rebaixamento do software da versão 7.4 para uma versão anterior manterá a configuração, mas com algumas limitações.
- Configurar um servidor RADIUS primário/secundário quando um anterior estiver configurado fará com que a entrada mais antiga seja substituída pela nova.

Enhanced Local Mode (ELM)

O ELM é compatível com a solução FlexConnect. Consulte o guia de práticas recomendadas sobre ELM para obter mais informações.

Suporte de acesso para convidados no Flex 7500

Figura 13: Suporte de acesso para convidados no Flex 7500



O Flex 7500 permitirá e continuará a suportar a criação de túnel EoIP para o seu controlador de âncora convidado no DMZ. Para obter as melhores práticas sobre a solução de acesso sem fio para convidados, consulte o Guia de implantação para convidados.

[Gerenciamento do WLC 7500 do NCS](#)

O gerenciamento do WLC 7500 do NCS é idêntico às WLCs atuais da Cisco.

Monitor ▾ Reports ▾ Configure ▾ Services ▾

Add Controllers

Configure > Controllers > Add Controllers

General Parameters

Add Format Type: Device Info ▾

IP Addresses: **WLC 7500 IP Address**

Network Mask: 255.255.255.0

Verify Telnet/SSH Capabilities ⓘ

SNMP Parameters ⓘ

Version: v2c ▾

Retries: 2

Timeout: 10 (secs)

Community: private

Telnet/SSH Parameters ⓘ

User Name: admin

Password: ●●●●●●

Confirm Password: ●●●●●●

Retries: 3

Timeout: 60 (secs)

OK Cancel

Controllers -- Select a command --

Configure > Controllers

IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
172.20.227.174 ⓘ	Ambassador	7500		7.0.112.62	mobility	Reachable	Identical
172.20.227.177 ⓘ	5508-Primary	5500		7.0.112.52	mobility	Reachable	Identical

Para obter mais informações sobre como gerenciar WLC e descobrir modelos, consulte o [Guia de Configuração do Sistema de Controle Wireless da Cisco, versão 7.0.172.0](#).

FAQ

P. Se eu configurar LAPs em um local remoto como FlexConnect, posso dar a esses LAPs um controlador primário e secundário?

Exemplo: Há um controlador principal no local A e um controlador secundário no local B. Se o controlador no local A falhar, o LAP realizará failover para o controlador no local B. Se ambas as controladoras não estiverem disponíveis, o LAP cairá no modo autônomo FlexConnect?

A. Yes. Primeiro, o LAP falha para seu secundário. Todas as WLANs que são comutadas localmente não têm alterações, e todas as que são comutadas centralmente têm o tráfego direcionado para o novo controlador. E, se o secundário falhar, todas as WLANs marcadas para

comutação local (e autenticação de chave aberta/pré-compartilhada/você está fazendo o autenticador de AP) permanecerão ativas.

P. Como os access points configurados no modo local lidam com as WLANs configuradas com o FlexConnect Local Switching?

A. Os pontos de acesso no modo local tratam essas WLANs como WLANs normais. A autenticação e o tráfego de dados são encapsulados de volta para a WLC. Durante uma falha de link de WAN, essa WLAN está completamente inativa e nenhum cliente está ativo nessa WLAN até que a conexão com a WLC seja restaurada.

P. Posso fazer autenticação da Web com switching local?

A. Sim, você pode ter um SSID com autenticação da Web habilitada e descartar o tráfego localmente após a autenticação da Web. A autenticação da Web com comutação local funciona bem.

P. Posso usar meu Portal de Convidado no Controlador para um SSID, que é tratado localmente pelo H REAP? Em caso afirmativo, o que acontece se eu perder a conectividade com o controlador? Os clientes atuais caem imediatamente?

A. Yes. Como essa WLAN é comutada localmente, a WLAN está disponível, mas nenhum novo cliente pode se autenticar porque a página da Web não está disponível. Mas os clientes existentes não são abandonados.

P. O FlexConnect pode certificar a conformidade com PCI?

A. Yes. A solução FlexConnect oferece suporte à detecção de invasores para satisfazer a conformidade com PCI.

[Informações Relacionadas](#)

- [Guia de projeto e implantação do HREAP](#)
- [Cisco 4400 Series Wireless LAN Controllers](#)
- [Cisco 2000 Series Wireless LAN Controllers](#)
- [Cisco Wireless Control System](#)
- [Cisco 3300 Series Mobility Services Engine](#)
- [Cisco Aironet 3500 Series](#)
- [Cisco Secure Access Control System](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)