Perguntas frequentes sobre o design e os recursos do controlador de LAN sem fio (WLC)

Contents

Introduction

Este documento fornece informações das perguntas mais frequentes (FAQ) sobre o projeto e as características disponíveis de um Controller de LAN Wireless (WLC).

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Projete o FAQ

P. Como configuro o switch para conectar-se à WLC?

R. Configure a porta do switch à qual o WLC está conectado como uma porta de tronco IEEE 802.1Q. Certifique-se de que somente as VLANs necessárias sejam permitidas no switch. Geralmente, o gerenciamento e a interface do gerenciador de AP da WLC não são marcados. Isso significa que eles assumem a VLAN nativa do switch conectado. Isso não é necessário. Você pode atribuir uma VLAN separada a essas interfaces. Para obter mais informações, consulte a seção *Configuração do Switch para a WLC* do Exemplo de Configuração Básica de Controladoras Wireless LAN e Pontos de Acesso Lightweight.

P. Todo o tráfego de rede de e para um túnel de cliente WLAN através de uma controladora Wireless LAN (WLC) quando o ponto de acesso (AP) é registrado com a controladora?

R. Quando o AP ingressa em uma WLC, um túnel do protocolo de controle e provisionamento de pontos de acesso sem fio (CAPWAP) é formado entre os dois dispositivos. Todo o tráfego, que inclui todo o tráfego do cliente, é enviado através do túnel CAPWAP.

A única exceção é quando um AP está no modo REAP híbrido. Os pontos de acesso REAP híbridos podem comutar o tráfego de dados do cliente localmente e executar a autenticação do cliente localmente quando a conexão com o controlador é perdida. Quando estão conectados ao controlador, eles também podem enviar tráfego de volta ao controlador.

P. Posso instalar Pontos de Acesso Lightweight (LAPs) em um escritório remoto e instalar um Cisco Wireless LAN Controller (WLC) em minha sede? O LWAPP/CAPWAP funciona em uma WAN?

R. Sim, você pode ter as WLCs através da WAN a partir dos APs. O LWAPP/CAPWAP funciona em uma WAN quando os LAPs são configurados no modo Remote Edge AP (REAP) ou Hybrid Remote Edge AP (H-REAP). Qualquer um desses modos permite o controle de um AP por um controlador remoto que está conectado através de um link WAN. O tráfego é ligado localmente no link da LAN, o que evita a necessidade de enviar desnecessariamente o tráfego local pelo link da WAN. Essa é precisamente uma das maiores vantagens de ter WLCs em sua rede sem fio.

Observação: nem todos os APs Lightweight suportam esses modos. Por exemplo, o modo H-REAP é suportado apenas em LAPs 1131, 1140,1242, 1250 e AP801. O modo REAP é suportado somente no AP 1030, mas os APs 1010 e 1020 não suportam REAP. Antes de planejar implementar esses modos, verifique se os LAPs oferecem suporte a eles. Os APs do Cisco IOS® Software (APs autônomos) que foram convertidos para o LWAPP não suportam REAP.

P. Como funcionam os modos REAP e H-REAP?

R. No modo **REAP**, todo o tráfego de controle e gerenciamento, que inclui o tráfego de autenticação, é enviado de volta para a WLC. Mas todo o tráfego de dados é comutado localmente na LAN do escritório remoto. Quando a conexão com a WLC é perdida, todas as WLANs são terminadas, exceto a primeira WLAN (WLAN1). Todos os clientes atualmente associados a esta WLAN são mantidos. Para permitir que os novos clientes autentiquem e recebam com êxito o serviço nesta WLAN durante o tempo de inatividade, configure o método de autenticação para esta WLAN como WEP ou WPA-PSK para que a autenticação seja feita localmente no REAP. Para obter mais informações sobre a implantação do REAP, consulte o Guia de implantação do REAP na filial.

No modo **H-REAP**, um access point envia o tráfego de controle e gerenciamento, que inclui o tráfego de autenticação, de volta para a WLC. O tráfego de dados de uma WLAN será ligado localmente no escritório remoto se a WLAN estiver configurada com a comutação local H-REAP ou se o tráfego de dados for enviado de volta para a WLC. Quando a conexão com a WLC é perdida, todas as WLANs são terminadas, exceto as primeiras oito WLANs configuradas com switching local H-REAP. Todos os clientes atualmente associados a essas WLANs são mantidos. Para permitir que os novos clientes autentiquem e recebam com êxito o serviço nessas WLANs durante o tempo de inatividade, configure o método de autenticação para essa WLAN como WEP, WPA PSK ou WPA2 PSK para que a autenticação seja feita localmente em H-REAP.

Para obter mais informações sobre o H-REAP, consulte o Guia de design e implantação do H-REAP.

P. Qual é a diferença entre o Remote-Edge AP (REAP) e o Hybrid-REAP (H-REAP)?

R. **REAP não suporta marcação de VLAN IEEE 802.1Q.** Como tal, ele não suporta várias VLANs. O tráfego de todos os Service Set Identifiers (SSID) termina na mesma sub-rede, mas o H-REAP oferece suporte à marcação de VLAN IEEE 802.1Q. O tráfego de cada SSID pode ser segmentado para uma VLAN exclusiva.

Quando a conectividade com a WLC é perdida, isto é, no modo independente, o REAP serve

apenas uma WLAN, isto é, a Primeira WLAN. Todas as outras WLANs são desativadas. Em H-REAP, até 8 WLANs são suportadas durante o tempo de inatividade.

Outra grande diferença é que, no modo REAP, o tráfego de dados só pode ser ligado localmente. Não é possível voltar para o escritório central, mas, no modo H-REAP, você tem a opção de voltar o tráfego para o escritório central. O tráfego das WLANs configuradas com comutação local H-REAP é comutado localmente. O tráfego de dados de outras WLANs é comutado de volta para o escritório central.

Consulte Exemplo de Configuração do Remote-Edge AP (REAP) com APs Lightweight e Controladoras Wireless LAN (WLCs) para obter mais informações sobre o REAP.

Consulte Configuração do REAP Híbrido para obter mais informações sobre o H-REAP.

P. Quantas WLANs são suportadas na WLC?

R. Desde a versão 5.2.157.0 do software, a WLC agora pode controlar até 512 WLANs para pontos de acesso lightweight. Cada WLAN tem um ID de WLAN separado (1 a 512), um nome de perfil separado e um SSID de WLAN, e pode receber políticas de segurança exclusivas. O controlador publica até 16 WLANs para cada ponto de acesso conectado, mas você pode criar até 512 WLANs no controlador e depois publicar seletivamente essas WLANs (usando grupos de pontos de acesso) em diferentes pontos de acesso para gerenciar melhor sua rede sem fio.

Observação: os controladores Cisco 2106, 2112 e 2125 suportam apenas até 16 WLANs.

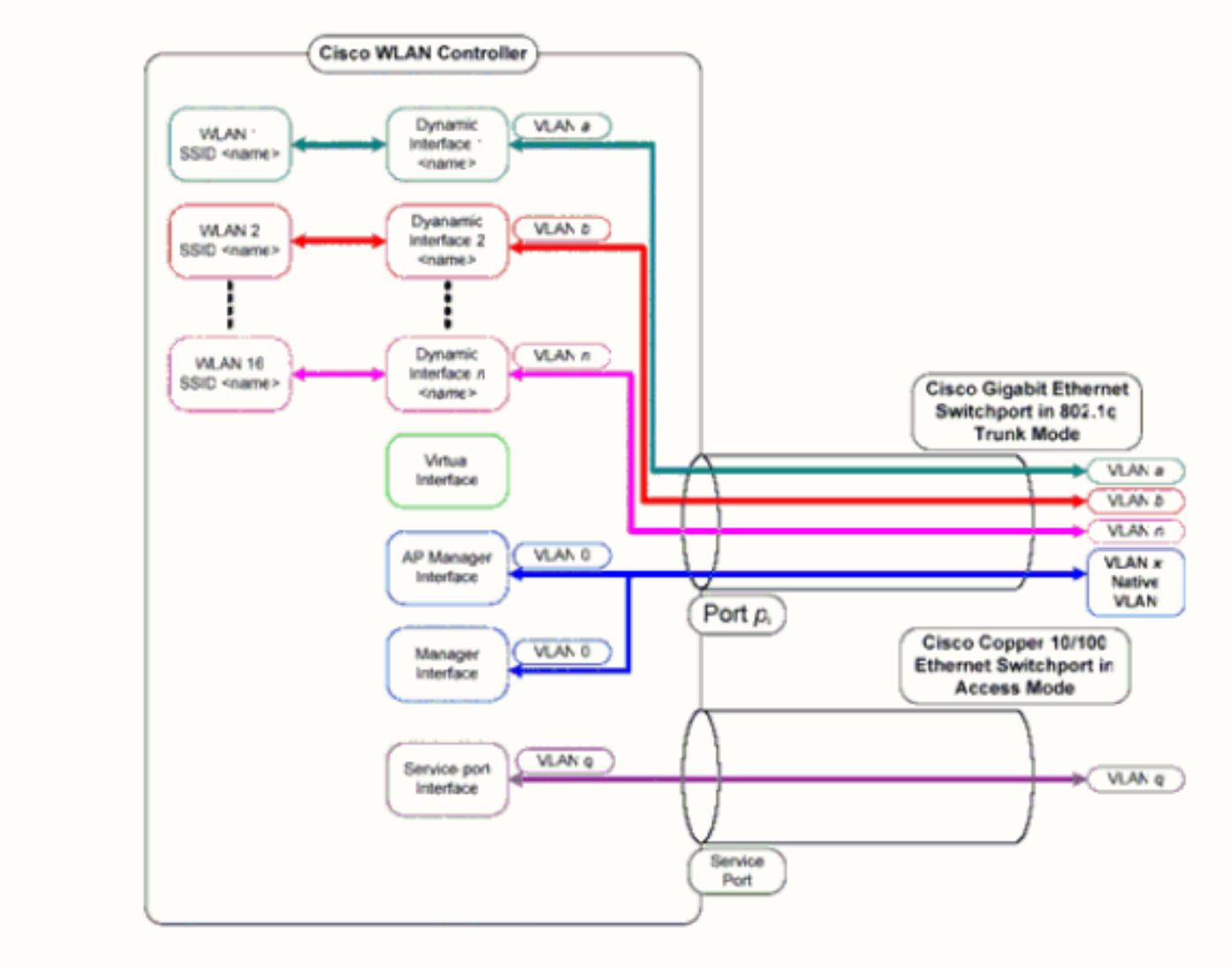
Observação: Para obter informações detalhadas sobre as diretrizes para configuração de WLANs em WLCs, leia a seção Criação de WLANs do Guia de Configuração da Cisco Wireless LAN Controller Release 7.0.116.0.

P. Como posso configurar VLANs em minha controladora Wireless LAN (WLC)?

R. Na WLC, as VLANs são vinculadas a uma interface configurada em uma sub-rede IP exclusiva. Essa interface é mapeada em uma WLAN. Em seguida, os clientes que se associam a essa WLAN pertencem à VLAN da interface e recebem um endereço IP da sub-rede à qual a interface pertence. Para configurar VLANs em sua WLC, conclua o procedimento no Exemplo de Configuração de VLANs em Wireless LAN Controllers.

P. Nós provisionamos duas WLANs com duas interfaces dinâmicas diferentes. Cada interface tem sua própria VLAN, que é diferente da VLAN da interface de gerenciamento. Isso parece funcionar, mas não provisionamos as portas de tronco para permitir as VLANs que nossas WLANs usam. O ponto de acesso (AP) marca os pacotes com a VLAN da interface de gerenciamento?

R. O AP não marca pacotes com a VLAN da interface de gerenciamento. O AP encapsula os pacotes dos clientes no Lightweight AP Protocol (LWAPP)/CAPWAP e, em seguida, passa os pacotes para a WLC. A WLC então retira o cabeçalho LWAPP/CAPWAP e encaminha os pacotes para o gateway com a marca de VLAN apropriada. A marca da VLAN depende da WLAN à qual o cliente pertence. A WLC depende do gateway para rotear os pacotes ao seu destino. Para poder transmitir tráfego para várias VLANs, você deve configurar o switch de uplink como uma porta de tronco. Este diagrama explica como as VLANs funcionam com os controladores:



P. Qual endereço IP da WLC é usado para autenticação com o servidor AAA?

R. A WLC usa o endereço IP da interface de gerenciamento para qualquer mecanismo de autenticação (Camada 2 ou Camada 3) que envolva um servidor AAA. Para obter mais informações sobre portas e interfaces na WLC, consulte a seção *Configuração de Portas e Interfaces* do Guia de Configuração da Cisco Wireless LAN Controller Release 7.0.116.0.

P. Tenho dez Pontos de Acesso Lightweight (LAPs) Cisco 1000 Series e dois Controladores de LAN Wireless (WLCs) na mesma VLAN. Como posso registrar seis LAPs para associar à WLC1 e os outros quatro LAPs para associar à WLC2?

R. O LWAPP/CAPWAP permite redundância dinâmica e balanceamento de carga. Por exemplo, se você especificar mais de um endereço IP para a opção 43, um LAP enviará solicitações de descoberta LWAPP/CAPWAP para cada um dos endereços IP que o AP receber. Na resposta de descoberta de WLC LWAPP/CAPWAP, a WLC incorpora estas informações:

- Informações sobre a carga de LAP atual, que é definida como o número de LAPs que estão unidos à WLC no momento
- A capacidade do LAP
- O número de clientes sem fio conectados à WLC

Em seguida, o LAP tenta se unir à WLC menos carregada, que é a WLC com a maior capacidade de LAP disponível. Além disso, depois que um LAP se une a uma WLC, ele aprende os

endereços IP das outras WLCs do grupo de mobilidade de sua WLC associada.

Quando um LAP se une a uma WLC, você pode fazer com que ele se junte a uma WLC específica na próxima reinicialização. Para fazer isso, atribua uma WLC primária, secundária e terciária para um LAP. Quando o LAP é reinicializado, ele procura a WLC primária e a une independentemente da carga nessa WLC. Se a WLC primária não responder, ela procurará a secundária e, se não houver resposta, a terciária. Para obter mais informações sobre como configurar a WLC primária para um LAP, consulte a seção *Atribuir Controladoras Primárias, Secundárias e Terciárias para o AP Lightweight* do Exemplo de Configuração de Failover de Controladora WLAN para Pontos de Acesso Lightweight.

P. Quais são os recursos que não são suportados nas controladoras Wireless LAN (WLCs) 2100 Series?

R. Estes recursos de hardware não são suportados nos 2100 Series Controllers:

- Porta de serviço (interface Ethernet 10/100-Mb/s de gerenciamento fora de banda separada)

Estes recursos de software não são suportados nos 2100 Series Controllers:

- Terminação de VPN (como IPSec e L2TP)
- Término de túneis de controlador convidado (a origem de túneis de controlador convidado é suportada)
- Lista de servidores Web de autenticação da Web externa
- LWAPP da camada 2
- Spanning Tree
- Espelhamento de portas
- Cranite
- Fortaleza
- Apple Talk
- Contratos de largura de banda de QoS por usuário
- Passagem de IPv6
- Agregação de links (LAG)
- modo multicast unicast
- Acesso para convidado com fio

P. Que recursos não são suportados nos controladores 5500 Series?

R. Estes recursos de software não são suportados nos 5500 Series Controllers:

- Interface do gerenciador de AP estático**Observação:** para controladores 5500 Series, não é necessário configurar uma interface do gerenciador de AP. A interface de gerenciamento atua como uma interface de gerenciador de AP por padrão, e os pontos de acesso podem se unir a essa interface.
- Encapsulamento de mobilidade assimétrica
- STP (Spanning Tree Protocol)
- Espelhamento de portas
- Suporte à lista de controle de acesso (ACL - Access Control List) da camada 2
- Terminação de VPN (como IPSec e L2TP)
- opção de passagem de VPN

- Configuração de 802.3 Bridging, AppleTalk e Point-to-Point Protocol over Ethernet (PPPoE)

P. Que recursos não são suportados em redes de malha?

R. Estes recursos do controlador não são suportados em redes de malha:

- Suporte a vários países
- CAC baseado em carga (as redes em malha suportam apenas CAC baseado em largura de banda, ou estático).
- Alta disponibilidade (pulsação rápida e temporizador de junção de descoberta primária)
- Autenticação EAP-FASTv1 e 802.1X
- Prioridade de junção do ponto de acesso (os pontos de acesso da malha têm uma prioridade fixa).
- Certificado localmente significativo
- Serviços baseados no local

P. Qual é o período de validade dos certificados instalados pelo fabricante (MICs) em uma controladora de LAN sem fio e dos certificados dos APs leves?

R. O período de validade de um MIC em uma WLC é de 10 anos. O mesmo período de validade de 10 anos se aplica aos certificados de AP leves a partir da criação (seja um MIC ou um certificado autoassinado (SSC)).

P. Tenho duas controladoras Wireless LAN (WLCs) chamadas WLC1 e WLC2 configuradas no mesmo grupo de mobilidade para failover. Meu ponto de acesso leve (LAP) está registrado no momento com a WLC1. Se a WLC1 falhar, o AP registrado na WLC1 reinicializa durante sua transição para a WLC sobrevivente (WLC2)? Além disso, durante esse failover, o cliente WLAN perde a conectividade WLAN com o LAP?

R. Sim, o LAP cancela o registro da WLC1, reinicializa e registra novamente na WLC2, se a WLC1 falhar. Como o LAP é reinicializado, os clientes WLAN associados perdem a conectividade com o LAP de reinicialização. Para obter informações relacionadas, consulte Balanceamento de carga de AP e Fallback de AP em redes sem fio unificadas.

P. O roaming depende do modo LWAPP (Lightweight Access Point Protocol) que a controladora Wireless LAN (WLC) está configurada para usar? Uma WLC que opera no modo LWAPP da camada 2 pode executar roaming da camada 3?

R. Desde que o agrupamento de mobilidade nos controladores esteja configurado corretamente, o roaming de clientes deverá funcionar bem. O roaming não é afetado pelo modo LWAPP (camada 2 ou camada 3). No entanto, recomenda-se usar o LWAPP da camada 3 sempre que possível.

Observação: o modo de Camada 2 é suportado apenas pelas séries Cisco 410x e 440x de WLCs e pelos pontos de acesso Cisco 1000 Series. O LWAPP da camada 2 não é suportado por outras plataformas de controlador de LAN sem fio e de ponto de acesso leve.

P. Qual é o processo de roaming que ocorre quando um cliente decide fazer

roaming para um novo ponto de acesso (AP) ou controlador?

R. Esta é a sequência de eventos que ocorre quando um cliente faz roaming para um novo AP:

1. O cliente envia uma solicitação de reassociação à WLC através do LAP.
2. A WLC envia a mensagem de mobilidade para outras WLCs no grupo de mobilidade para descobrir com qual WLC o cliente estava anteriormente associado.
3. A WLC original responde com informações, como endereço MAC, endereço IP, QoS, contexto de segurança, etc. sobre o cliente através da mensagem de mobilidade.
4. A WLC atualiza seu banco de dados com os detalhes fornecidos do cliente; o cliente passa pelo processo de reautenticação, se necessário. O novo LAP com o qual o cliente está atualmente associado também é atualizado juntamente com outros detalhes no banco de dados do WLC. Dessa forma, o endereço IP do cliente é retido em roams entre WLCs, o que ajuda a fornecer roaming contínuo.

Para obter mais informações sobre roaming em um ambiente unificado, consulte a seção *Configuração de Grupos de Mobilidade* do Guia de Configuração da Cisco Wireless LAN Controller Release 7.0.116.0.

Observação: o cliente sem fio não envia uma solicitação de autenticação (802.11) durante a reassociação. O cliente sem fio simplesmente envia a reassociação imediatamente. Em seguida, ele passará pela autenticação 802.1x.

P. Quais portas são necessárias para permitir a comunicação LWAPP/CAPWAP quando há um firewall na rede?

R. Você deve habilitar estas portas:

- Ative essas portas UDP para o tráfego LWAPP:Dados - 12222Controle - 12223
- Ative estas portas UDP para o tráfego CAPWAP:Dados - 5247Controle - 5246
- Ative estas portas UDP para o tráfego de mobilidade:16666 - Modo protegido16667 - Modo não seguro

As mensagens de mobilidade e de dados são normalmente trocadas através de pacotes EtherIP. **O protocolo IP 97** deve ser permitido no firewall para permitir pacotes EtherIP. Se você usar o **ESP** para encapsular pacotes de mobilidade, você terá que permitir o **ISAKMP** através do firewall quando você abrir a **porta UDP 500**. Você também precisa abrir o **protocolo IP 50** para permitir que os dados criptografados passem pelo firewall.

Estas portas são opcionais (dependendo de seus requisitos):

- TCP 161 e 162 para o SNMP (para o Wireless Control System [WCS])
- UDP 69 para o TFTP
- TCP 80 e/ou 443 para o HTTP ou o HTTPS para o acesso a GUI
- TCP 23 e/ou 22 para Telnet ou secure shell (SSH) para acesso CLI

P. Os controladores de LAN sem fio suportam SSHv1 e SSHv2?

R. Controladores de LAN sem fio suportam apenas SSHv2.

P. O ARP reverso (RARP) é suportado através das controladoras Wireless LAN

(WLCs)?

R. O Reverse Address Resolution Protocol (RARP) é um protocolo da camada de enlace usado para obter um endereço IP para um determinado endereço da camada de enlace, como um endereço Ethernet. O RARP é suportado com WLCs com a versão de firmware 4.0.217.0 ou posterior. O RARP não é suportado em nenhuma das versões anteriores.

P. Posso usar o servidor DHCP interno no Wireless LAN Controller (WLC) para atribuir endereços IP aos Lightweight Access Points (LAPs)?

R. Os controladores contêm um servidor DHCP interno. Esse servidor é geralmente usado em filiais que ainda não têm um servidor DHCP. Para acessar o serviço DHCP, clique no menu **Controller** na GUI da WLC; em seguida, clique na opção **Internal DHCP Server** no lado esquerdo da página. Para obter mais informações sobre como configurar o escopo de DHCP no WLC, consulte a seção *Configuração de DHCP* do Guia de Configuração do Cisco Wireless LAN Controller Release 7.0.116.0.

O servidor interno fornece endereços DHCP para clientes sem fio, LAPs, APs de modo de dispositivo na interface de gerenciamento e solicitações DHCP que são retransmitidas de LAPs. As WLCs nunca oferecem endereços para dispositivos upstream na rede com fio. A opção de DHCP 43 não é suportada no servidor interno, portanto, o AP deve usar um método alternativo para localizar o endereço IP da interface de gerenciamento do controlador, como broadcast de sub-rede local, DNS, Priming ou descoberta no ar.

Observação: as versões do firmware da WLC anteriores à 4.0 não suportam o serviço DHCP para LAPs, a menos que os LAPs estejam diretamente conectados à WLC. O recurso do servidor DHCP interno foi usado apenas para fornecer endereços IP aos clientes que se conectam à rede LAN sem fio.

P. O que significa o campo DHCP necessário em uma WLAN?

R. DHCP Required é uma opção que pode ser habilitada para uma WLAN. É necessário que todos os clientes que se associam a essa WLAN específica obtenham endereços IP através do DHCP. Clientes com endereços IP estáticos não podem se associar à WLAN. Essa opção está na guia Advanced (Avançado) de uma WLAN. A WLC permite o tráfego de/para um cliente somente se o seu endereço IP estiver presente na tabela MSCB da WLC. A WLC registra o endereço IP de um cliente durante sua solicitação DHCP ou renovação DHCP. Isso exige que um cliente renove seu endereço IP toda vez que se reassocia à WLC, pois toda vez que o cliente se desassocia como parte de seu processo de roam ou tempo limite de sessão, sua entrada é apagada da tabela MSCB. O cliente deve autenticar-se novamente e reassociar-se à WLC, que novamente faz a entrada do cliente na tabela.

P. Como o Cisco Centralized Key Management (CCKM) funciona em um ambiente LWAPP/CAPWAP?

R. Durante a associação inicial do cliente, o AP ou a WLC negocia uma chave mestra (PMK) em pares depois que o cliente sem fio passa a autenticação 802.1x. O AP WLC ou WDS armazena em cache o PMK para cada cliente. Quando um cliente sem fio se reassocia ou faz roaming, ele pula a autenticação 802.1x e valida a PMK imediatamente.

A única implementação especial da WLC no CCKM é que as WLCs trocam PMK do cliente

através de pacotes de mobilidade, como 16666 UDP.

P. Como defino as configurações duplex na controladora Wireless LAN (WLC) e nos Pontos de Acesso Lightweight (LAPs)?

R. Os produtos Cisco Wireless funcionam melhor quando a velocidade e o duplex são negociados automaticamente, mas você tem a opção de definir as configurações de duplex na WLC e nos LAPs. Para definir as configurações de velocidade/duplex do AP, você pode definir as configurações de duplex para os LAPs no controlador e depois, por sua vez, empurrá-los para os LAPs.

configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name> é o comando para definir as configurações de duplex através da CLI. Este comando é suportado somente nas versões 4.1 e posteriores.

Para definir as configurações duplex para as interfaces físicas da WLC, use o comando **config port physicalmode {all | port} {100h | 100 F | 10 h | 10f}**.

Esse comando define as portas Ethernet 10/100BASE-T do painel frontal ou todas elas especificadas para a operação dedicada de 10 Mbps ou 100 Mbps, half-duplex ou full-duplex. Observe que você deve desabilitar a negociação automática com o comando **config port autoneg disable** antes de configurar manualmente qualquer modo físico na porta. Além disso, observe que o comando **config port autoneg** substitui as configurações feitas com o comando **config port physicalmode**. Por padrão, todas as portas são definidas para negociação automática.

Observação: não há como alterar as configurações de velocidade nas portas de fibra.

P. Há uma maneira de rastrear o nome do ponto de acesso leve (LAP) quando ele não está registrado na controladora?

R. Se seu AP estiver completamente inoperante e não registrado na controladora, não há como você rastrear o LAP através da controladora. A única maneira que resta é que você pode acessar o switch no qual esses APs estão conectados e você pode encontrar a porta do switch na qual eles estão conectados usando este comando:

```
show mac-address-table address
```

Isso fornece o número da porta no switch ao qual esse AP está conectado. Em seguida, emita este comando:

```
show cdp nei detail
```

A saída desse comando também fornece o nome do LAP. No entanto, esse método só é possível quando seu AP está ligado e conectado ao switch.

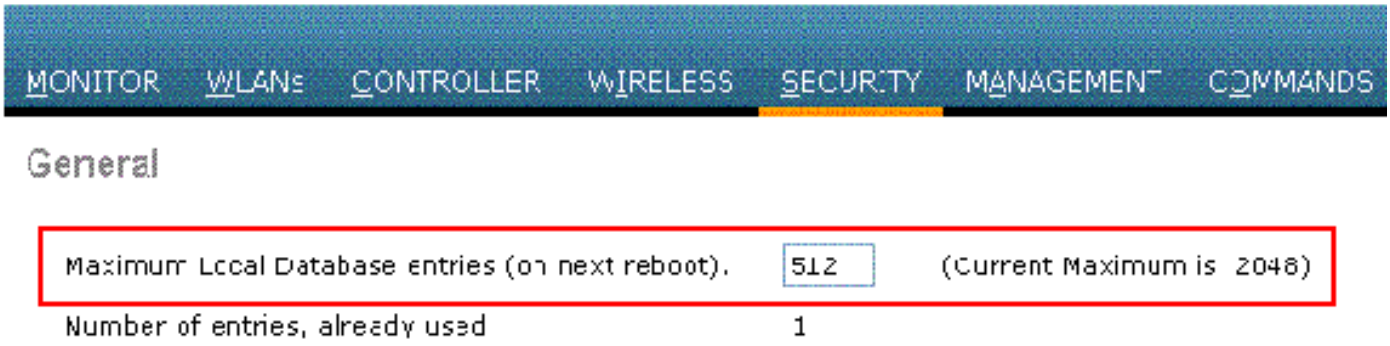
P. Eu configurei 512 usuários em meu controlador. Há alguma maneira de aumentar o número de usuários na controladora Wireless LAN (WLC)?

R. O banco de dados de usuário local é limitado a um máximo de 2048 entradas na página **Segurança > Geral**. Esse banco de dados é compartilhado por usuários de gerenciamento local (que inclui receptores de lobby), usuários de rede (que inclui usuários convidados), entradas de filtro MAC, entradas de lista de autorização de ponto de acesso e entradas de lista de exclusão. Juntos, todos esses tipos de usuários não podem exceder o tamanho do banco de dados configurado.

Para aumentar o banco de dados local, use este comando da CLI:

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```

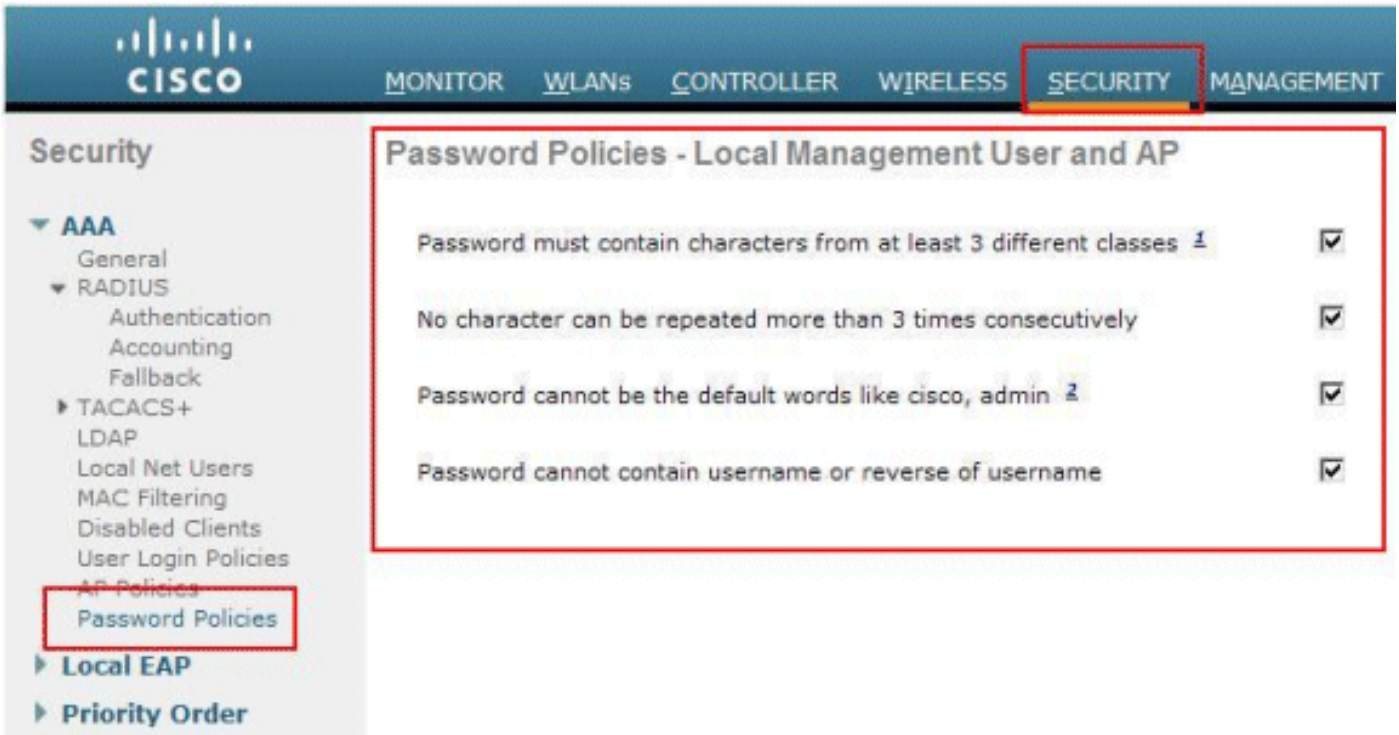
Observação: você deve salvar a configuração e redefinir o sistema (usando o comando **reset system**) para que a alteração tenha efeito.



P. Como faço para aplicar uma política de senha forte nas WLCs?

R. As WLCs permitem definir uma política de senha forte. Isso pode ser feito usando a CLI ou a GUI.

Na GUI, vá para **Security > AAA > Password Policies**. Esta página tem uma série de opções que podem ser selecionadas para impor uma senha forte. Aqui está um exemplo:



Para fazer isso a partir da CLI da WLC, use o comando **config switchconfig strong-pwd** {case-check | *controlo consecutivo* | *verificação padrão* | *verificação de nome de usuário* | *all-check}* *{ativar* comando | *disable}*:

- **case-check** - Verifica a ocorrência do mesmo caractere três vezes consecutivas.
- **sequence-check** - Verifica se os valores padrão ou suas variantes estão sendo usados.
- **default-check** - Verifica se o nome de usuário ou seu inverso está sendo usado.
- **todas as verificações** - Habilita/desabilita todas as verificações de senha forte.

P. Como o recurso de cliente passivo é usado em controladores de LAN sem fio?

R. Os clientes passivos são dispositivos sem fio, como escalas e impressoras configuradas com um endereço IP estático. Esses clientes não transmitem informações de IP, como endereço IP, máscara de sub-rede e informações de gateway, quando se associam a um ponto de acesso. Como resultado, quando clientes passivos são usados, o controlador nunca sabe o endereço IP a menos que use o DHCP.

As WLCs atuam atualmente como um proxy para solicitações ARP. Ao receber uma solicitação ARP, a controladora responde com uma resposta ARP em vez de passar a solicitação diretamente ao cliente. Esse cenário tem duas vantagens:

- O dispositivo upstream que envia a solicitação ARP ao cliente não saberá onde o cliente está localizado.
- A energia para dispositivos operados por bateria, como telefones celulares e impressoras, é preservada porque eles não precisam responder a todas as solicitações ARP.

Como o controlador sem fio não tem nenhuma informação relacionada a IP sobre os clientes passivos, ele não pode responder a nenhuma solicitação ARP. O comportamento atual não permite a transferência de solicitações ARP para clientes passivos. Qualquer aplicativo que tente acessar um cliente passivo falhará.

O recurso de cliente passivo permite que solicitações e respostas ARP sejam trocadas entre clientes com e sem fio. Este recurso, quando habilitado, permite que a controladora passe solicitações ARP de clientes com fio para sem fio até que o cliente sem fio desejado chegue ao estado RUN.

Para obter informações sobre como configurar o recurso de cliente passivo, leia a seção Using the GUI to Configure Passive Client no Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0.

P. Como posso configurar o cliente para reautenticar com o servidor RADIUS a cada três minutos ou em qualquer período de tempo especificado?

R. O parâmetro de timeout de sessão na WLC pode ser usado para fazer isso. Por padrão, o parâmetro de tempo limite da sessão é configurado para 1800 segundos antes que ocorra uma nova autenticação.

Altere esse valor para 180 segundos para fazer com que o cliente seja autenticado novamente após três minutos.

Para acessar o parâmetro de tempo limite da sessão, clique no menu **WLANs** na GUI. Ele exibe a lista de WLANs configuradas na WLC. Clique na WLAN à qual o cliente pertence. Vá até a guia **Avançado** e encontre o parâmetro *Ativar tempo limite da sessão*. Altere o valor padrão para 180 e clique em **Apply** para que as alterações tenham efeito.

Quando enviado em um Access-Accept, junto com um valor Termination-Action de RADIUS-Request, o atributo Session-Timeout especifica o número máximo de segundos de serviço fornecido antes da reautenticação. Nesse caso, o atributo Session-Timeout é usado para carregar a constante ReAuthPeriod na máquina de estado de Temporizador de Reautenticação de 802.1X.

P. Tenho um túnel de convidado, Ethernet over IP (EoIP), configurado entre meu Wireless LAN Controller (WLC) 4400, que atua como o WLC âncora, e vários WLCs remotos. Essa WLC âncora pode encaminhar broadcasts de sub-rede através do túnel EoIP da rede com fio para clientes sem fio associados aos controladores remotos?

R. Não, a WLC 4400 não encaminha broadcasts de sub-rede IP do lado com fio para os clientes sem fio através do túnel EoIP. Este não é um recurso suportado. A Cisco não suporta o tunelamento de broadcast ou multicast de sub-rede na topologia de acesso de convidado. Como a WLAN convidada força o ponto de presença do cliente para um local muito específico na rede, principalmente fora do firewall, o tunelamento de broadcast de sub-rede pode ser um problema de segurança.

P. Em uma configuração de controladora Wireless LAN (WLC) e Lightweight Access Point Protocol (LWAPP), que valores de Differentiated Services Code Point (DSCP) são passados para o tráfego de voz? Como a QoS é implementada na WLC?

R. As WLANs da solução Cisco Unified Wireless Network (UWN) suportam quatro níveis de QoS:

- Platinum/Voz
- Gold/Vídeo
- Prata/Melhor esforço (padrão)
- Bronze/Plano de fundo

Você pode configurar a WLAN de tráfego de voz para usar o QoS Platinum, atribuir a WLAN de banda curta para usar o QoS Bronze e atribuir todo o tráfego restante entre os outros níveis de QoS. Consulte Atribuição de um Perfil de QoS a uma WLAN para obter mais informações.

P. As bridges Ethernet Linksys são suportadas em uma Cisco Wireless Unified Solution?

R. Não, o WLC suporta apenas produtos Cisco WGB. Não há suporte para WGBs da Linksys. Embora a Cisco Wireless Unified Solution não ofereça suporte às pontes Ethernet Linksys WET54G e WET11B, você poderá usar esses dispositivos em uma configuração da Wireless Unified Solution se usar estas diretrizes:

- Conecte apenas um dispositivo ao WET54G ou WET11B.
- Ative o recurso de clonagem MAC no WET54G ou WET11B para clonar o dispositivo conectado.

- Instale os drivers e o firmware mais recentes em dispositivos conectados à WET54G ou WET11B. Esta diretriz é especialmente importante para impressoras JetDirect porque versões de firmware anteriores causam problemas com o DHCP.

Observação: outras bridges de terceiros não são suportadas. As etapas mencionadas também podem ser tentadas para outras bridges de terceiros.

P. Como eu armazeno os arquivos de configuração na controladora Wireless LAN (WLC)?

R. A WLC contém dois tipos de memória:

- RAM volátil—Mantém a configuração atual e ativa da controladora.
- RAM não volátil (NVRAM) — retém a configuração de reinicialização

Ao configurar o sistema operacional na WLC, você está modificando a RAM volátil. Você deve salvar a configuração da RAM volátil na NVRAM para certificar-se de que a WLC seja reinicializada na configuração atual.

Éimportante saber qual memória você está modificando quando executa estas tarefas:

- Use o assistente de configuração.
- Limpe a configuração da controladora.
- Salvar configurações.
- Reinicialize o controlador.
- Faça logoff do CLI.

Perguntas frequentes sobre recursos

P. Como defino o tipo de EAP (Extensible Authentication Protocol) na controladora Wireless LAN (WLC)? Desejo autenticar em um dispositivo do Access Control Server (ACS) e obtenho um tipo de "EAP sem suporte" nos logs.

R. Não há configuração de tipo EAP separada no WLC. Para LEAP (Light EAP), EAP Flexible Authentication via Secure Tunneling (EAP-FAST) ou Microsoft Protected EAP (MS-PEAP), basta configurar IEEE 802.1x ou Wi-Fi Protected Access (WPA) (se você usar 802.1x com WPA). Qualquer tipo de EAP suportado no back-end RADIUS e no cliente é suportado através da marca 802.1x. A configuração de EAP no cliente e no servidor RADIUS deve corresponder.

Conclua estes passos para habilitar o EAP através da GUI no WLC:

1. Na GUI da WLC , clique em **WLANs**.
2. Uma lista de WLANs configuradas na WLC é exibida. Clique em uma WLAN.
3. Em **WLANs > Edit**, clique na guia **Security**.
4. Clique em **Layer 2** e escolha Layer 2 Security como 802.1x ou WPA+WPA2. Você também pode configurar os parâmetros 802.1x que estão disponíveis na mesma janela. Em seguida, a WLC encaminha pacotes de autenticação EAP entre o cliente sem fio e o servidor de autenticação.
5. Clique nos servidores **AAA** e escolha o servidor de autenticação no menu suspenso para esta WLAN. Supomos que o servidor de autenticação já está configurado globalmente. Para

obter informações sobre como habilitar a opção EAP em WLCs através da interface de linha de comando (CLI), consulte a seção *Uso da CLI para Configurar o RADIUS* do Guia de Configuração da Cisco Wireless LAN Controller Release 7.0.116.0.

P. O que é mudança rápida de SSID?

R. A alteração rápida de SSID permite que os clientes se movam entre SSIDs. Quando o cliente envia uma nova associação para um SSID diferente, a entrada do cliente na tabela de conexão do controlador é apagada antes que o cliente seja adicionado ao novo SSID. Quando a Alteração rápida de SSID está desativada, o controlador impõe um atraso antes que os clientes tenham permissão para mudar para um novo SSID. Para obter informações sobre como habilitar a Alteração rápida de SSID, consulte a seção *Configuração da Alteração Rápida de SSID* do Guia de Configuração da Cisco Wireless LAN Controller Release 7.0.116.0.

P. Posso definir um limite para o número de clientes que podem se conectar a uma LAN sem fio?

R. Você pode definir um limite para o número de clientes que podem se conectar a uma WLAN, o que é útil em cenários onde você tem um número limitado de clientes que podem se conectar a uma controladora. O número de clientes que você pode configurar por WLAN depende da plataforma que você está usando.

Leia a seção Configuring the Maximum Number of Clients per WLAN do Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0 para obter informações sobre os limites de clientes por WLAN para as diferentes plataformas de Wireless LAN Controllers.

P. O que é PKC e como ele funciona com a controladora Wireless LAN (WLC)?

R. PKC significa Proactive Key Caching (Cache de chave pró-ativo). Ele foi projetado como uma extensão do padrão IEEE 802.11i.

O PKC é um recurso habilitado nos Cisco 2006/410x/440x Series Controllers que permite que clientes sem fio adequadamente equipados façam roaming sem reautenticação completa com um servidor AAA. Para entender o PKC, primeiro você precisa entender o armazenamento de chaves em cache.

O cache de chaves é um recurso que foi adicionado ao WPA2. Isso permite que uma estação móvel armazene em cache as chaves mestras (PMK [Pairwise Master Key]) obtidas por meio de uma autenticação bem-sucedida com um ponto de acesso (AP) e **reutilize-o em uma associação futura com o mesmo AP**. Isso significa que um determinado dispositivo móvel precisa se autenticar uma vez com um AP específico e armazenar em cache a chave para uso futuro. O cache de chaves é manipulado por meio de um mecanismo conhecido como PMK Identifier (PMKID), que é um hash do PMK, uma sequência de caracteres, a estação e os endereços MAC do AP. A PMKID identifica exclusivamente a PMK.

Mesmo com o Key Caching, uma estação sem fio deve autenticar com cada AP do qual deseja obter o serviço. Isso introduz latência e sobrecarga significativas, que atrasam o processo de transferência e podem inibir a capacidade de suportar aplicativos em tempo real. Para resolver esse problema, o PKC foi introduzido com WPA2.

O PKC permite que uma estação reutilize uma PMK que tinha obtido anteriormente através de um

processo de autenticação bem-sucedido. Isso elimina a necessidade de a estação autenticar em novos APs quando estiver em roaming.

Portanto, em um roaming dentro do controlador, quando um dispositivo móvel se move de um AP para outro no mesmo controlador, o cliente recalcula um PMKID usando o PMK usado anteriormente e o apresenta durante o processo de associação. A WLC pesquisa seu cache PMK para determinar se ela tem tal entrada. Em caso afirmativo, ele ignora o processo de autenticação 802.1x e inicia imediatamente a troca de chaves WPA2. Caso contrário, ele passa pelo processo de autenticação padrão 802.1X.

O PKC é ativado por padrão com WPA2. Portanto, quando você habilita a WPA2 como segurança de Camada 2 na configuração de WLAN da WLC, o PKC é habilitado na WLC. Além disso, configure o servidor AAA e o cliente sem fio para a autenticação EAP apropriada.

O suplicante usado no lado do cliente também deve suportar WPA2 para que o PKC funcione. O PKC também pode ser implementado em um ambiente de roaming entre controladores.

Observação: o PKC não funciona com o Aironet Desktop Utility (ADU) como o solicitante do cliente.

P. Quais são as explicações para essas configurações de timeout no controlador: Address Resolution Protocol (ARP) Timeout, User Idle Timeout e Session Timeout?

R. O **tempo limite ARP** é usado para excluir entradas ARP na WLC para os dispositivos aprendidos da rede.

O **User Idle Timeout:** Quando um usuário fica ocioso sem qualquer comunicação com o LAP durante o tempo definido como User Idle Timeout, o cliente é desautenticado pelo WLC. O cliente precisa reautenticar e reassociar-se à WLC. É usado em situações em que um cliente pode sair do LAP associado sem notificar o LAP. Isso pode ocorrer se a bateria falhar no cliente ou se os associados do cliente saírem.

Observação: Para acessar o ARP e o User Idle Timeout na GUI da WLC , vá para o menu **Controller**. Escolha **General** no lado esquerdo para encontrar os campos ARP e User Idle Timeout.

O tempo limite da sessão é o tempo máximo para uma sessão de cliente com o WLC. Depois desse tempo, a WLC desautentica o cliente e o cliente passa por todo o processo de autenticação (reautenticação) novamente. Isso faz parte de uma precaução de segurança para girar as chaves de criptografia. Se você usar um método EAP (Extensible Authentication Protocol) com gerenciamento de chave, a rechaveamento ocorrerá a cada intervalo regular para derivar uma nova chave de criptografia. Sem o gerenciamento de chaves, esse valor de tempo limite é o tempo que os clientes sem fio precisam para fazer uma reautenticação completa. O tempo limite da sessão é específico para a WLAN. Esse parâmetro pode ser acessado no menu **WLANs > Edit**.

P. O que é um sistema RFID? Quais tags RFID são suportadas atualmente pela Cisco?

R. A RFID (Radio Frequency Identification, identificação por radiofrequência) é uma tecnologia que usa a comunicação por radiofrequência para uma comunicação de alcance relativamente curto. Um sistema RFID básico é composto de tags RFID, leitores RFID e o software de

processamento.

Atualmente, a Cisco oferece suporte a tags de RFID do AeroScout e do Pango. Para obter mais informações sobre como configurar tags do AeroScout, consulte Configuração de WLC para Tags RFID do AeroScout.

P. Posso executar a autenticação EAP localmente na WLC? Há algum documento que explique esse recurso de EAP local?

R. Sim, a autenticação EAP pode ser executada localmente na WLC. O EAP local é um método de autenticação que permite que usuários e clientes sem fio sejam autenticados localmente na WLC. Ele foi projetado para uso em escritórios remotos que desejam manter a conectividade com clientes sem fio quando o sistema de back-end for interrompido ou o servidor de autenticação externo for desativado. Quando você habilita o EAP local, o WLC serve como o servidor de autenticação. Para obter mais informações sobre como configurar uma WLC para a autenticação EAP-Fast local, consulte Autenticação EAP Local na Controladora Wireless LAN com EAP-FAST e Exemplo de Configuração de Servidor LDAP.

P. O que é o recurso de substituição de WLAN? Como configuro esse recurso? Os LAPs manterão os valores de substituição da WLAN quando fizerem failover para a WLC de backup?

R. O recurso de substituição de WLAN nos permite escolher WLANs entre as WLANs configuradas em uma WLC que pode ser usada ativamente em uma base LAP individual. Conclua estes passos para configurar uma substituição de WLAN:

1. Na GUI da WLC, clique no menu **Wireless**.
2. Clique na opção **Radios** no lado esquerdo e escolha **802.11 a/n** ou **802.11 b/g/n**.
3. Clique no link **Configure** no menu suspenso localizado no lado direito que corresponde ao nome do AP no qual você deseja configurar a substituição da WLAN.
4. Escolha **Enable** no menu suspenso WLAN Override. O menu WLAN Override é o último item no lado esquerdo da janela.
5. A lista de todas as WLANs configuradas na WLC é exibida.
6. Nessa lista, marque as **WLANs** que você deseja que apareçam no LAP e clique em **Apply** para que as alterações entrem em vigor.
7. Salve sua configuração depois de fazer essas alterações.

Os APs retêm os valores de substituição da WLAN quando são registrados em outras WLCs, desde que os perfis de WLAN e SSIDs que você deseja substituir estejam configurados em todas as WLCs.

Observação: no software release 5.2.157.0 da controladora, o recurso de substituição de WLAN foi removido da GUI e da CLI da controladora. Se a sua controladora estiver configurada para WLAN override e você fizer o upgrade para a versão 5.2.157.0 do software da controladora, a controladora excluirá a configuração da WLAN e transmitirá todas as WLANs. Você pode especificar que apenas determinadas WLANs sejam transmitidas se configurar grupos de pontos de acesso. Cada ponto de acesso anuncia apenas as WLANs habilitadas que pertencem ao seu grupo de pontos de acesso.

Observação: os grupos de pontos de acesso não permitem que as WLANs sejam transmitidas por interface de rádio do AP.

P. O IPv6 é suportado nas controladoras Cisco Wireless LAN (WLCs) e nos pontos de acesso Lightweight (LAPs)?

R. Atualmente, os controladores das séries 4400 e 4100 suportam apenas passagem de cliente IPv6. Não há suporte para suporte nativo a IPv6.

Para habilitar o IPv6 na WLC, marque a caixa de seleção **IPv6 Enable** na configuração de SSID da WLAN na página WLAN > Edit.

Além disso, o modo multicast Ethernet (EMM) é necessário para suportar IPv6. Se você desabilitar o EMM, os dispositivos clientes que usam IPv6 perderão a conectividade. Para habilitar o EMM, vá para a página Controller > General e, no menu suspenso Ethernet Multicast Mode, escolha **Unicast** ou **Multicast**. Isso ativa o multicast no modo Unicast ou no modo Multicast. Quando o multicast é habilitado como multicast unicast, os pacotes são replicados para cada AP. Isso pode exigir muito do processador, portanto, use-o com cuidado. O multicast ativado como multicast multicast usa o endereço multicast atribuído pelo usuário para fazer um multicast mais tradicional para os access points (APs).

Observação: não há suporte para IPv6 nos controladores 2006.

Além disso, há o bug da Cisco ID CSCsg78176, que impede o uso da passagem IPv6 quando o recurso AAA Override é usado.

P. O Cisco 2000 Series Wireless LAN Controller (WLC) oferece suporte à autenticação da Web para usuários convidados?

R. A autenticação da Web é suportada em todas as WLCs da Cisco. A autenticação da Web é um método de autenticação da camada 3 usado para autenticar usuários com credenciais de autenticação simples. Não há criptografia envolvida. Conclua estas etapas para habilitar este recurso:

1. Na GUI, clique no menu **WLAN**.
2. Clique em uma **WLAN**.
3. Vá até a guia **Security** e escolha **Layer 3**.
4. Marque a caixa **Web Policy** e escolha **Authentication**.
5. Clique em **Apply para salvar as alterações.**
6. Para criar um banco de dados na WLC para autenticar usuários, vá para o menu **Security** na GUI, escolha **Local Net User** e conclua estas ações: Defina o nome de usuário e a senha do convidado a serem usados para fazer logon. Esses valores diferenciam maiúsculas de minúsculas.Escolha a ID da WLAN que você usa.**Observação:** para obter uma configuração mais detalhada, consulte o Exemplo de Configuração de Autenticação da Web do Wireless LAN Controller.

P. A WLC pode ser gerenciada no modo sem fio?

R. A WLC pode ser gerenciada através do modo sem fio quando estiver habilitada. Para obter mais informações sobre como habilitar o modo sem fio, consulte a seção *Habilitação de Conexões Sem Fio para a GUI e CLI* do Guia de Configuração da Cisco Wireless LAN Controller Release 7.0.116.0.

P. O que é Agregação de Links (LAG)? Como habilito o LAG em controladoras Wireless LAN (WLCs)?

R. O LAG agrupa todas as portas do WLC em uma única interface EtherChannel. O sistema gerencia dinamicamente o balanceamento de carga de tráfego e a redundância de porta com LAG.

Geralmente, a interface na WLC tem vários parâmetros associados a ela, o que inclui o endereço IP, o gateway padrão (para a sub-rede IP), a porta física primária, a porta física secundária, a marca de VLAN e o servidor DHCP. Quando o LAG não é usado, cada interface é geralmente mapeada para uma porta física, mas várias interfaces também podem ser mapeadas para uma única porta WLC. Quando o LAG é usado, o sistema mapeia dinamicamente as interfaces para o canal de porta agregado. Isso ajuda na redundância de porta e no balanceamento de carga. Quando uma porta falha, a interface é mapeada dinamicamente para a próxima porta física disponível e os LAPs são balanceados entre as portas.

Quando o LAG é ativado em uma WLC, a WLC encaminha quadros de dados na mesma porta em que eles foram recebidos. A WLC depende do switch vizinho para balancear a carga do tráfego no EtherChannel. A WLC não executa nenhum balanceamento de carga EtherChannel sozinha.

P. Que modelos de controladoras Wireless LAN (WLCs) suportam a agregação de links (LAG)?

R. Os Cisco 5500 Series Controllers oferecem suporte ao LAG na versão de software 6.0 ou posterior, os Cisco 4400 Series Controllers oferecem suporte ao LAG na versão de software 3.2 ou posterior e o LAG é ativado automaticamente nos controladores dentro do Cisco WiSM e do Catalyst 3750G Integrated Wireless LAN Controller Switch. Sem o LAG, cada porta do sistema de distribuição em um Cisco 4400 Series Controller suporta até 48 pontos de acesso. Com o LAG habilitado, uma porta lógica do Cisco 4402 Controller suporta até 50 pontos de acesso, uma porta lógica do Cisco 4404 Controller suporta até 100 pontos de acesso e a porta lógica no Switch do Catalyst 3750G Integrated Wireless LAN Controller e em cada controlador Cisco WiSM suporta até 150 pontos de acesso.

As WLCs Cisco 2106 e 2006 não suportam LAG. Modelos anteriores, como o Cisco 4000 Series WLC, não suportam LAG.

P. Qual é o recurso de mobilidade de âncora automática nas redes sem fio unificadas?

R. A mobilidade de âncora automática (ou mobilidade de WLAN de convidado) é usada para melhorar o balanceamento de carga e a segurança para clientes de roaming em suas LANs sem fio (WLANs). Em condições normais de roaming, os dispositivos clientes se juntam a uma WLAN e são ancorados no primeiro controlador que eles entram em contato. Se um cliente faz roaming para uma sub-rede diferente, o controlador para o qual o cliente faz roaming configura uma sessão externa para o cliente com o controlador âncora. Com o uso do recurso de mobilidade de âncora automática, você pode especificar um controlador ou um conjunto de controladores como pontos âncora para clientes em uma WLAN.

Observação: a âncora de mobilidade não deve ser configurada para mobilidade da camada 3. A âncora de mobilidade é usada apenas para o tunelamento de convidados.

P. Um Cisco 2006 Wireless LAN Controller (WLC) pode ser configurado como uma âncora para uma WLAN?

R. Uma WLC Cisco 2000 Series não pode ser designada como âncora para uma WLAN. No entanto, uma WLAN criada em uma WLC Cisco 2000 Series pode ter uma WLC Cisco 4100 Series e uma WLC Cisco 4400 Series como sua âncora.

P. Que tipo de tunelamento de mobilidade é usado pelo Wireless LAN Controller?

R. As versões 4.1 a 5.1 do software do controlador suportam tunelamento de mobilidade assimétrica e simétrica. O software da controladora versão 5.2 ou posterior suporta apenas tunelamento de mobilidade simétrica, que agora está sempre habilitado por padrão.

No tunelamento assimétrico, o tráfego do cliente para a rede com fio é roteado diretamente através do controlador externo. O tunelamento assimétrico é interrompido quando um roteador upstream tem a filtragem de caminho reverso (RPF) habilitada. Nesse caso, o tráfego do cliente é descartado no roteador porque a verificação de RPF garante que o caminho de volta para o endereço de origem corresponda ao caminho do qual o pacote vem.

Quando o tunelamento de mobilidade simétrica está habilitado, todo o tráfego do cliente é enviado para o controlador âncora e pode passar com êxito na verificação de RPF. O tunelamento de mobilidade simétrica também é útil nestas situações:

- Se uma instalação de firewall no caminho do pacote do cliente descartar pacotes porque o endereço IP de origem não corresponde à sub-rede na qual os pacotes são recebidos, isso é útil.
- Se a VLAN do grupo de access-point no controlador âncora for diferente da VLAN da interface WLAN no controlador externo: nesse caso, o tráfego do cliente pode ser enviado em uma VLAN incorreta durante eventos de mobilidade.

P. Como acessamos a WLC quando a rede está inativa?

R. Quando a rede está inativa, a WLC pode ser acessada pela porta de serviço. A essa porta é atribuído um endereço IP em uma sub-rede totalmente diferente de outras portas da WLC e, por isso, é chamado de gerenciamento out-of-band. Para obter mais informações, consulte a seção *Configuração de Portas e Interfaces* do Guia de Configuração da Cisco Wireless LAN Controller Release 7.0.116.0.

P. Os Cisco Wireless LAN Controllers (WLCs) suportam o recurso de failover (ou redundância)?

R. Sim, se você tiver duas ou mais WLCs em sua rede WLAN, poderá configurá-las para redundância. Geralmente, um LAP se une à WLC primária configurada. Quando a WLC primária falha, o LAP é reinicializado e junta-se a outra WLC no grupo de mobilidade. O failover é um recurso no qual o LAP pesquisa a WLC primária e se junta à WLC primária quando ela está funcional. Consulte o Exemplo de Configuração de Failover de Controladora WLAN para Pontos de Acesso Lightweight para obter mais informações.

P. Qual é o uso de listas de controle de acesso (ACLs) de pré-autenticação em controladoras Wireless LAN (WLCs)?

R. Com a ACL de pré-autenticação, como o nome indica, você pode permitir o tráfego de cliente de e para um endereço IP específico antes mesmo que o cliente se autentique. Ao usar um servidor Web externo para autenticação da Web, algumas das plataformas WLC precisam de uma ACL de pré-autenticação para o servidor Web externo (o Cisco 5500 Series Controller, um Cisco 2100 Series Controller, o Cisco 2000 Series e o módulo de rede do controlador). Para as outras plataformas WLC, a ACL de pré-autenticação não é obrigatória. No entanto, é uma boa prática configurar uma ACL de pré-autenticação para o servidor Web externo ao usar a autenticação da Web externa.

P. Tenho uma WLAN filtrada por MAC e uma WLAN completamente aberta em minha rede. O cliente escolhe a WLAN aberta por padrão? Ou o cliente se associa automaticamente ao ID da WLAN que está definido no filtro MAC? Além disso, por que existe uma opção de "interface" em um filtro MAC?

R. O cliente pode se associar a qualquer WLAN à qual o cliente esteja configurado para se conectar. A opção de interface no filtro MAC permite aplicar o filtro a uma WLAN ou a uma interface. Se várias WLANs estiverem ligadas à mesma interface, você poderá aplicar o filtro MAC à interface sem a necessidade de criar um filtro para cada WLAN individual.

P. Como posso configurar a autenticação TACACS para usuários de gerenciamento na controladora Wireless LAN (WLC)?

R. A partir da versão 4.1 da WLC, o TACACS é suportado nas WLCs. Consulte Configurando o TACACS+ para entender como configurar o TACACS+ para autenticar usuários de gerenciamento do WLC.

P. Qual é o uso da configuração de falha de autenticação excessiva em uma controladora Wireless LAN (WLC)?

R. Essa configuração é uma das políticas de exclusão de cliente. A exclusão de cliente é um recurso de segurança no controlador. A política é usada para fazer a lista negra de clientes a fim de impedir o acesso ilegal à rede ou ataques à rede sem fio.

Com essa política de falha excessiva de autenticação da Web habilitada, quando o número de tentativas de autenticação da Web com falha de um cliente excede 5, o controlador considera que o cliente excedeu o número máximo de tentativas de autenticação da Web e faz uma lista negra do cliente.

Conclua estes passos para habilitar ou desabilitar esta configuração:

1. Na GUI da WLC, vá para **Security > Wireless Protection Policies > Client Exclusion Policies**.
2. Marque ou desmarque **Excessive Web Authentication Failures**.

P. Converti meu ponto de acesso autônomo (AP) para o modo lightweight. No modo Lightweight AP Protocol (LWAPP) com o servidor AAA RADIUS para tarifação de cliente, normalmente o cliente é rastreado com tarifação RADIUS baseada no endereço IP da WLC. É possível definir a contabilidade do RADIUS com base no endereço MAC do AP associado a essa WLC e não no endereço IP da WLC?

R. Sim, isso pode ser feito com a configuração do lado da WLC. Conclua estes passos:

1. Na GUI do controlador, em **Security > Radius Accounting**, há uma caixa suspensa para Tipo de ID de estação de chamada. Escolha **AP MAC Address**.
2. Verifique isso por meio do registro de AP do LWAPP. Lá, você pode ver o campo ID da estação chamada que exibe o endereço MAC do AP ao qual o cliente específico está associado.

P. Como você altera o valor de tempo limite de handshake do Wi-Fi Protected Access (WPA) em uma controladora Wireless LAN (WLC) através da CLI? Sei que posso fazer isso nos pontos de acesso (APs) do Cisco IOS® com o comando dot11 wpa handshake timeout *value*, mas como você faz isso em uma WLC?

R. A capacidade de configurar o timeout de WPA-Handshake através das WLCs foi integrada no software release 4.2 e posterior. Essa opção não é necessária em versões anteriores do software WLC.

Estes comandos podem ser usados para alterar o tempo limite de handshake WPA:

```
    config advanced eap eapol-key-timeout <value>
    config advanced eap eapol-key-retries <value>
```

Os valores padrão continuam a refletir o comportamento atual das WLCs.

```
   - the default value for eapol-key-timeout is 1 second.
   - the default value for eapol-key-retries is 2 retries
```

Observação: em APs IOS, essa configuração é configurável com o comando **dot11 wpa handshake**.

Você também pode configurar os outros parâmetros EAP com as opções no comando **config advanced eap**.

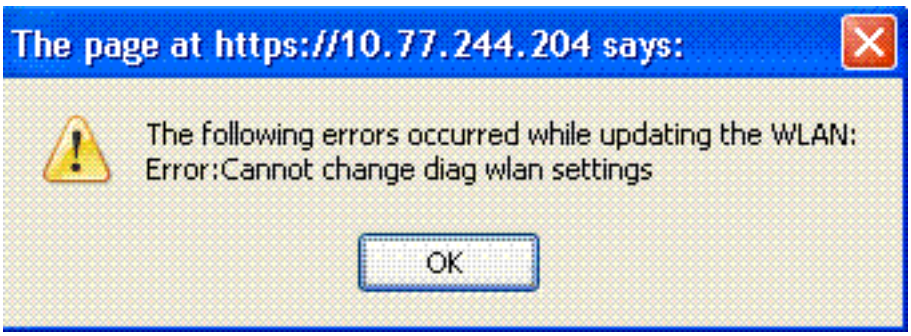
```
(Cisco Controller) >config advanced eap ?

eapol-key-timeout
   Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
   Configures EAPOL-Key Max Retries.
identity-request-timeout
   Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
   Configures EAP-Identity-Request Max Retries.
key-index
   Configure the key index used for
   dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
   Configure to ignore the same username count
   reaching max in the EAP identity response
request-timeout
   Configures EAP-Request Timeout in seconds.
request-retries
   Configures EAP-Request Max Retries.
```

P. Qual é a finalidade do recurso de canal de diagnóstico na página WLAN > Edit >

Advanced?

R. O recurso de canal de diagnóstico permite que você solucione problemas relacionados à comunicação do cliente com uma WLAN. O cliente e os pontos de acesso podem passar por um conjunto definido de testes para identificar a causa das dificuldades de comunicação que o cliente enfrenta e, em seguida, permitir que medidas corretivas sejam tomadas para tornar o cliente operacional na rede. Você pode usar a GUI ou a CLI do controlador para ativar o canal de diagnóstico e pode usar a CLI ou o WCS do controlador para executar os testes de diagnóstico.

O canal de diagnóstico pode ser usado apenas para teste. Se você tentar configurar a autenticação ou a criptografia para a WLAN com o canal de diagnóstico habilitado, verá este erro:



P. Qual é o número máximo de grupos de AP que podem ser configurados em uma WLC?

R. Esta lista mostra o número máximo de grupos de AP que você pode configurar em uma WLC:

- Um máximo de 50 grupos de access point para o Cisco 2100 Series Controller e módulos de rede do controlador
- Um máximo de 300 grupos de access point para os Cisco 4400 Series Controllers, Cisco WiSM e Cisco 3750G Wireless LAN Controller Switch
- Máximo de 500 grupos de access point para Cisco 5500 Series Controllers

Informações Relacionadas

- Perguntas frequentes sobre a controladora Wireless LAN (WLC)
- Perguntas frequentes sobre mensagens de sistema e erros da controladora Wireless LAN (WLC)
- Perguntas frequentes sobre o Lightweight Access Point
- Guia de configuração do Cisco Wireless LAN Controller Release 7.0.116.0
- Suporte IPv6 no controlador de LAN sem fio
- Suporte de produtos Wireless
- Suporte Técnico e Documentação - Cisco Systems

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

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

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