Projeto do controlador do Wireless LAN (WLC) e características FAQ

ID do Documento: 118833

Atualizado em: março 02, 2015

Produtos Relacionados

- Cisco 4400 Series Wireless LAN Controllers
- Controladores sem fio Cisco série 5500
- Cisco Wireless Services Module 2 (WiSM2)
- Controladores sem fio Cisco série 2500
- Cisco 2100 Series Wireless LAN Controllers
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers
- Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM)
- Cisco 2000 Series Wireless LAN Controllers
- Cisco Wireless LAN Controller Module
- Cisco 4100 Series Wireless LAN Controllers
- + mostra mais

Índice

Introdução

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

Q. Como eu configuro o interruptor para conectar com o WLC?

A. Configurar a porta de switch, a que o WLC é conectado, como uma porta de tronco do IEEE 802.1Q. Certifique-se de que somente os VLAN necessários estão permitidos no interruptor. Geralmente, o Gerenciamento e a relação do gerenciador AP do WLC são deixados o sem etiqueta. Isto significa que supõem o VLAN nativo do switch conectado. Isto não é necessário. Você pode atribuir um VLAN separado a estas relações. Para mais informação, refira *configurar ao interruptor para a* seção *WLC do* controlador do Wireless LAN e do exemplo de pouco peso da configuração básica do Access point.

Q. Todo o tráfego de rede e a um cliente de WLAN escava um túnel através de um controlador do Wireless LAN (WLC) uma vez que o Access Point (AP) obtém registrado com o controlador?

A. Quando o AP se junta a um WLC, um controle e um abastecimento do túnel do protocolo dos pontos de acesso Wireless (CAPWAP) estão formados entre os dois dispositivos. Todo o tráfego, que inclui todo o tráfego do cliente, é enviado através do túnel CAPWAP.

A única exceção a esta é quando um AP é híbrido-COLHE dentro o modo. Os Access point da híbrido-COLHEITA podem comutar o tráfego de dados do cliente localmente e executar a authenticação do cliente localmente quando sua conexão ao controlador é perdida. Quando são conectados ao controlador, podem igualmente enviar o tráfego de volta ao controlador.

Q. Posso eu instalar o Lightweight Access Points (regaços) em um escritório remoto e instalar um controlador de LAN do Cisco Wireless (WLC) em minhas matrizes? O LWAPP/CAPWAP trabalha sobre WAN?

A. Sim, você pode ter os WLC através de WAN dos AP. LWAPP/CAPWAP trabalha sobre WAN quando os regaços estão configurados na borda remota AP (COLHA) ou no modo remoto híbrido da borda AP (H-REAP). Qualquer um destes modos permite o controle de um AP por um controlador remoto que seja conectado através de um link MACILENTO. O tráfego é construído uma ponte sobre no link LAN localmente, que evita a necessidade de enviar desnecessariamente o tráfego local sobre o link MACILENTO. Este é precisamente uma das grandes vantagens de ter WLC em sua rede Wireless.

Note: Não todos os AP de pouco peso apoiam estes modos. Por exemplo, o modo H-REAP é apoiado somente em 1131, 1140,1242, 1250, e os regaços AP801. COLHA o modo é apoiado somente nos 1030 AP, mas os 1010 e 1020 AP não apoiam COLHEM. Antes que você planeie executar estes modos, verifique para determinar se os regaços o apoiam. O software AP de Cisco IOS® (AP autônomos) que foi convertido ao LWAPP não apoia COLHE.

Q. Como COLHEM e os modos H-REAP trabalham?

A. No modo da **COLHEITA**, o todo o controle e tráfego de gerenciamento, que inclui o tráfego da autenticação, são escavados um túnel de volta ao WLC. Mas todo o tráfego de dados é comutado localmente dentro do escritório remoto LAN. Quando a conexão ao WLC é perdida, todos os WLAN estão terminados exceto o primeiro WLAN (WLAN1). Todos os clientes que são associados atualmente a este WLAN são retidos. A fim permitir que os clientes novos com sucesso autentiquem e recebam o serviço neste WLAN dentro do tempo ocioso da máquina, configurar o método de autenticação para este WLAN como o WEP ou o WPA-PSK de modo que

a autenticação seja feita localmente na COLHEITA. Para obter mais informações sobre de COLHA o desenvolvimento, consultam PARA COLHER o guia de distribuição no escritório filial.

No modo **H-REAP**, um Access point escava um túnel o controle e o tráfego de gerenciamento, que inclui o tráfego da autenticação, de volta ao WLC. O tráfego de dados de um WLAN está construído uma ponte sobre localmente no escritório remoto se o WLAN é configurado com switching local H-REAP, ou o tráfego de dados está enviado para trás ao WLC. Quando a conexão ao WLC é perdida, todos os WLAN estão terminados exceto os primeiros oito WLAN configurados com switching local H-REAP. Todos os clientes que são associados atualmente a estes WLAN são retidos. A fim permitir que os clientes novos com sucesso autentiquem e recebam o serviço nestes WLAN dentro do tempo ocioso da máquina, configurar o método de autenticação para este WLAN como o WEP, o WPA PSK, ou o WPA2 PSK de modo que a autenticação seja feita localmente em H-REAP.

Para obter mais informações sobre de H-REAP, refira o projeto e o guia de distribuição H-REAP.

Q. Que é a diferença entre a Remoto-borda AP (COLHA) e Híbrido-COLHE (H-REAP)?

A. **REAP** não apoia a colocação de etiquetas do IEEE 802.1Q VLAN. Como tal, não apoia vlan múltiplos. O tráfego de todos os service set identifier (SSID) termina na colocação de etiquetas do IEEE 802.1Q VLAN da mesma sub-rede, mas dos apoios H-REAP. O tráfego de cada SSID pode ser segmentado a um VLAN original.

Quando a Conectividade ao WLC é perdida, isto é, no modo independente, COLHA saques somente um WLAN, isto é, o primeiro WLAN. Todos WLAN restantes são desativados. Em H-REAP, até 8 WLAN são apoiados dentro do tempo ocioso da máquina.

Uma outra diferença principal é que, COLHA dentro o modo, tráfego de dados pode somente ser construída uma ponte sobre localmente. Não pode ser comutada de volta ao escritório central, mas, no modo H-REAP, você tem a opção para comutar o tráfego de volta ao escritório central. O tráfego dos WLAN configurados com switching local H-REAP é comutado localmente. O tráfego de dados de outros WLAN é comutado de volta ao escritório central.

Refira a Remoto-borda AP (COLHA) com AP de pouco peso e controladores do Wireless LAN (WLC) que o exemplo de configuração para obter mais informações sobre de COLHE.

Refira configurar o híbrido COLHEM para obter mais informações sobre de H-REAP.

Q. Quantos WLAN são apoiados no WLC?

A. Desde a versão de software 5.2.157.0, o WLC pode agora controlar até 512 WLAN para o Lightweight Access Points. Cada WLAN tem um ID de WLAN separado (1 a 512), um nome de perfil separado, e um WLAN SSID, e pode ser atribuído as políticas de segurança originais. O controlador publica até 16 WLAN a cada Access point conectado, mas você pode criar até 512 WLAN no controlador e então seletivamente publicar estes WLAN (que usam grupos do Access point) aos Access point diferentes para controlar melhor sua rede Wireless.

Note: Os controladores de Cisco 2106, 2112, e 2125 apoiam somente até 16 WLAN.

Note: Para informações detalhadas sobre das diretrizes para configurar WLAN em WLC, leia a seção criadora WLAN do manual de configuração do controlador de LAN do Cisco Wireless,

liberação 7.0.116.0.

Q. Como posso eu configurar VLAN em meu controlador do Wireless LAN (WLC)?

A. No WLC, os VLAN são amarrados a uma relação configurada em uma sub-rede de IP exclusivo. Esta relação é traçada em um WLAN. Então, os clientes que associam a este WLAN pertencem ao VLAN da relação e são atribuídos um endereço IP de Um ou Mais Servidores Cisco ICM NT da sub-rede a que a relação pertence. A fim configurar VLAN em seu WLC, termine o procedimento nos VLAN no exemplo de configuração dos controladores do Wireless LAN.

Q. Nós temos dois WLAN fornecida com duas interfaces dinâmica diferentes. Cada relação tem seu próprio VLAN, que é diferente do que a interface de gerenciamento VLAN. Isto parece trabalhar, mas nós temos não fornecida as portas de tronco para permitir os VLAN que nossos WLAN usam. O Access Point (AP) etiqueta os pacotes com a interface de gerenciamento VLAN?

A. O AP não etiqueta pacotes com a interface de gerenciamento VLAN. O AP encapsula os pacotes dos clientes no protocolo de pouco peso AP (LWAPP) /CAPWAP, e passa então os pacotes sobre ao WLC. O WLC descasca então o encabeçamento LWAPP/CAPWAP e para a frente os pacotes ao gateway com o VLAN apropriado etiquetam. A etiqueta VLAN depende do WLAN a que o cliente pertence. O WLC depende do gateway para distribuir os pacotes a seu destino. A fim poder passar o tráfego para vlan múltiplos, você deve configurar o interruptor do uplink como uma porta de tronco. Este diagrama explica como os VLAN trabalham com controladores:

Q. Que endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC é usado para a autenticação com o servidor AAA?

A. O WLC usa o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento para todo o mecanismo da autenticação (camada 2 ou camada 3) que envolver um servidor AAA. Para obter mais informações sobre das portas e das relações no WLC, refira a seção *configurando das portas e das relações do* manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0.116.0.

Q. Eu tenho dez Lightweight Access Points do Cisco 1000 Series (regaços) e dois controladores do Wireless LAN (WLC) no mesmo VLAN. Como podem eu registrar seis regaços para associar a WLC1, e outros quatro regaços a associar ao WLC2?

A. O LWAPP/CAPWAP permite a redundância dinâmica e o Balanceamento de carga. Por exemplo, se você especifica mais de um endereço IP de Um ou Mais Servidores Cisco ICM NT para a opção 43, um REGAÇO envia pedidos da descoberta LWAPP/CAPWAP a cada um dos endereços IP de Um ou Mais Servidores Cisco ICM NT que o AP recebe. Na resposta da descoberta WLC LWAPP/CAPWAP, o WLC encaixa esta informação:

- Informação na carga atual do REGAÇO, que é definida como o número de regaços que são juntados ao WLC naquele tempo
- A capacidade do REGAÇO
- O número de clientes Wireless que são conectados ao WLC

O REGAÇO tenta então juntar-se ao WLC menos-carregado, que é o WLC com a grande

capacidade disponível do REGAÇO. Além disso, depois que um REGAÇO se junta a um WLC, o REGAÇO aprende os endereços IP de Um ou Mais Servidores Cisco ICM NT dos outros WLC no grupo da mobilidade de seu WLC juntado.

Uma vez um REGAÇO junta-se a um WLC, você pode fazer o REGAÇO juntar-se a um WLC específico dentro de sua repartição seguinte. A fim fazer isto, atribua um WLC preliminar, secundário, e terciário para um REGAÇO. Quando as repartições do REGAÇO, ele procurarem o WLC preliminar e se juntarem a esse independente WLC da carga nesse WLC. Se o WLC preliminar não responde, procura o secundário, e, se nenhuma resposta, o terciário. Para obter mais informações sobre de como configurar o WLC preliminar para um REGAÇO, refira a *atribuição preliminar, secundária, e controladores terciários para a* seção *de pouco peso AP do* Failover do controlador de WLAN para o exemplo de configuração do Lightweight Access Points.

Q. Que são as características que não são apoiadas nos controladores do Wireless LAN do 2100 Series (WLC)?

A. Estes recursos de hardware não são 2100 controladores da série apoiados:

- Preste serviços de manutenção à porta (a interface Ethernet separada do gerenciamento fora de banda 10/100-Mb/s)

Estes recursos de software não são 2100 controladores da série apoiados:

- Terminação VPN (tal como o IPsec e o L2TP)
- Terminação de túneis do controlador do convidado (a origem de túneis do controlador do convidado é apoiada)
- Lista de servidores Web de autenticação da Web externa
- LWAPP da camada 2
- Medida - árvore
- Espelhamento de portas
- Cranite
- Fortaleza
- Apple Talk
- De QoS contratos da largura de banda por usuário
- Passagem de IPv6
- Agregação do link (RETARDAÇÃO)
- Modo de Unicast do Multicast
- Acesso prendido do convidado

Q. Que características não são apoiadas em controladores do 5500 Series?

A. Estes recursos de software não são apoiados em controladores do 5500 Series:

- Relação estática do gerenciador APNote: Para controladores do 5500 Series, você não é exigido configurar uma relação do gerenciador AP. A interface de gerenciamento atua como uma relação do gerenciador AP à revelia, e os Access point podem juntar-se nesta relação.
- Tunelamento assimétrico da mobilidade
- STP (Spanning Tree Protocol)
- Espelhamento de portas
- Apoio do Access Control List da camada 2 (ACL)

- Terminação de VPN (como IPSec e L2TP)
- Opção da transmissão VPN
- Configuração da construção de uma ponte sobre, do APPLETALK, e do Point-to-Point Protocol sobre Ethernet (PPPoE) de 802.3

Q. Que características não são apoiadas em redes de malha?

A. Estas características do controlador não são apoiadas em redes de malha:

- apoio do Multi-país
- CAC Carga-baseado (apoio das redes de malha largura de banda-baseado somente, ou estática, CAC.)
- Alta disponibilidade (a pulsação do coração rápida e a descoberta preliminar se juntam ao temporizador)
- Autenticação EAP-FASTv1 e de 802.1X
- O Access point junta-se à prioridade (os Access point da malha têm uma prioridade fixa.)
- Localmente - certificado significativo
- Serviços com base na localização

Q. Que é o período de validade dos Certificados instalados fabricante (MIC) em um controlador do Wireless LAN e dos Certificados do AP de pouco peso?

A. O período de validade de um MIC em um WLC é os anos 10. O mesmo período de validade dos anos 10 aplica-se aos Certificados do AP de pouco peso da criação (se é um MIC ou um certificado auto-assinado (SSC)).

Q. Eu tenho dois controladores do Wireless LAN (WLC) WLC1 nomeado e WLC2 configurados dentro do mesmo grupo da mobilidade para o Failover. Meu Access point de pouco peso (REGAÇO) é registrado atualmente com WLC1. Se WLC1 falha, faz o AP registrado à repartição WLC1 durante sua transição para a sobrevivência WLC (WLC2)? Também, durante este Failover, o cliente de WLAN perde a Conectividade WLAN com o REGAÇO?

A. Sim, o REGAÇO cancela a matrícula de WLC1, recarrega, e registrar novamente então com WLC2, se WLC1 falha. Porque as repartições do REGAÇO, os clientes de WLAN associados perdem a Conectividade ao REGAÇO de repartição. Para a informação relacionada, refira o Balanceamento de carga AP e a reserva AP em redes Wireless unificadas.

Q. É vagueando dependente do modo de pouco peso do protocolo do Access point (LWAPP) que o controlador do Wireless LAN (WLC) é configurado para usar? Pode um WLC que se opere no modo LWAPP da camada 2 executar a camada 3 que vagueia?

A. Enquanto a mobilidade que agrupa nos controladores é configurada corretamente, o cliente que vagueia deve trabalhar muito bem. Vaguear é não afetado pelo modo LWAPP (camada 2 ou camada 3). Contudo, recomenda-se usar na medida do possível a camada 3 LWAPP.

Note: O modo da camada 2 é apoiado somente pelo Cisco e Series dos WLC e dos Access point

do Cisco 1000 Series. A camada 2 LWAPP não é apoiada pelo outro controlador do Wireless LAN e Plataformas de pouco peso do Access point.

Q. Que é o processo vagueando que ocorre quando um cliente decide vaguear a um Access Point (AP) ou a um controlador novo?

A. Esta é a sequência de evento que ocorre quando um cliente vagueia a um AP novo:

1. O cliente envia um pedido da reassociação ao WLC através do REGAÇO.
2. O WLC envia a mensagem da mobilidade a outros WLC no grupo da mobilidade a fim encontrar com que WLC o cliente era previamente associado.
3. O WLC original responde com informação, tal como o MAC address, o endereço IP de Um ou Mais Servidores Cisco ICM NT, o QoS, o contexto de segurança, etc. sobre o cliente através da mensagem da mobilidade.
4. O WLC atualiza seu base de dados com os detalhes fornecidos do cliente; o cliente atravessa então o processo do reauthentication, caso necessário. O REGAÇO novo com que o cliente é associado atualmente é atualizado igualmente junto com outros detalhes no base de dados do WLC. Esta maneira, o endereço IP cliente é retida transversalmente vagueia entre WLC, que ajuda a fornecer vaguear sem emenda.

Para obter mais informações sobre de vaguear em um ambiente unificado, refira a seção *configurando dos Grupos de mobilidade do* manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0.116.0.

Note: O cliente Wireless não manda um pedido de autenticação (do 802.11) durante a reassociação. O cliente Wireless apenas manda a reassociação imediatamente. Então, atravessará a autenticação do 802.1x.

Q. Que portas eu preciso de permitir para uma comunicação LWAPP/CAPWAP quando há um Firewall na rede?

A. Você deve ativar estas portas:

- Ative essas portas UDP para o tráfego LWAPP:Dados - 12222Controle - 12223
- Permita estas portas UDP para o tráfego CAPWAP:Dados - 5247Controle - 5246
- Ative estas portas UDP para o tráfego de mobilidade:16666 - Modo fixado16667 - Modo inseguro

A mobilidade e os mensagens de dados são trocados geralmente através dos pacotes de EtherIP. **O protocolo IP 97** deve ser permitido no Firewall permitir pacotes de EtherIP. Se você usa o **ESP** para encapsular pacotes da mobilidade, você tem que permitir o **ISAKMP** com o Firewall quando você abre a **porta 500 UDP**. Você igualmente tem que abrir os **50 pés do protocolo IP** para permitir que os dados criptografados passem com o 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 o telnet ou Shell Seguro (ssh) para o acesso CLI

Q. Os controladores do Wireless LAN apoiam SSHv1 e SSHv2?

A. Os controladores do Wireless LAN apoiam somente SSHv2.

Q. O ARP reverso (RARP) é apoiado através dos controladores do Wireless LAN (WLC)?

A. O Reverse Address Resolution Protocol (RARP) é um protocolo de camada de link usado para obter um endereço IP de Um ou Mais Servidores Cisco ICM NT para um endereço de camada de link dado tal como um endereço de Ethernet. O RARP é apoiado com os WLC com versão de firmware 4.0.217.0 ou mais tarde. O RARP não é apoiado em algumas das versões anterior.

Q. Posso eu usar o servidor DHCP interno no controlador do Wireless LAN (WLC) a fim atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT ao Lightweight Access Points (regaços)?

A. Os controladores contêm um servidor DHCP interno. Este server é usado tipicamente nos escritórios filiais que já não têm um servidor DHCP. A fim alcançar o serviço DHCP, clique o menu do **controlador do** WLC GUI; clique então o **servidor DHCP interno da** opção no lado esquerdo da página. Para obter mais informações sobre de como configurar o escopo de DHCP no WLC, refira a seção *configurando DHCP do* manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0.116.0.

O servidor interno fornecem endereços de DHCP aos clientes Wireless, os regaços, o dispositivo-MODE AP na interface de gerenciamento, e as requisições DHCP que são retransmitidas dos regaços. Os WLC nunca oferecem endereços aos dispositivos rio acima na rede ligada com fio. A opção de DHCP 43 não é apoiada no servidor interno, assim que o AP deve usar um método alternativo para encontrar o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento do controlador, tal como a transmissão da sub-rede local, o DNS, escorva, ou sobre - areje a descoberta.

Note: Versões de firmware WLC antes que 4.0 não apoiarem o serviço DHCP para regaços a menos que os regaços estiverem conectados diretamente ao WLC. A característica interna do servidor DHCP foi usada para fornecer somente endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes que conectam à rede de Wireless LAN.

Q. Que o campo requerido DHCP sob um WLAN significa?

A. O DHCP exigido é uma opção que possa ser permitida para um WLAN. Necessita que todos os clientes que associam a esse WLAN particular obtêm endereços IP de Um ou Mais Servidores Cisco ICM NT com o DHCP. Não são permitidos aos clientes com endereços IP estáticos associar ao WLAN. Esta opção é encontrada sob o guia avançada de um WLAN. O WLC permite o tráfego para/desde um cliente somente se seu endereço IP de Um ou Mais Servidores Cisco ICM NT esta presente na tabela MSCB do WLC. O WLC grava o endereço IP de Um ou Mais Servidores Cisco ICM NT de um cliente durante sua requisição DHCP ou o DHCP renova. Isto exige que um cliente renova seu endereço IP de Um ou Mais Servidores Cisco ICM NT todas as vezes que reassocia ao WLC porque todas as vezes o cliente se dissocia como parte de um seu vagueia o processo ou o timeout de sessão, sua entrada é apagado da tabela MSCB. O cliente deve outra vez autenticar novamente e reassociar ao WLC, que faz outra vez a entrada de cliente na tabela.

Q. Como faz o gerenciamento chave centralizado Cisco (CCKM) trabalha em um ambiente LWAPP/CAPWAP?

A. Durante a associação de cliente inicial, o AP ou o WLC negociam por pares um chave mestre (PMK) depois que o cliente Wireless passa a autenticação do 802.1x. O WLC ou o WDS AP põem em esconderijo o PMK para cada cliente. Quando um cliente Wireless reassocia ou vagueia, salta a autenticação do 802.1x e valida o PMK imediatamente.

A única aplicação especial do WLC no CCKM é que os WLC trocam o cliente PMK através dos pacotes da mobilidade, tais como UDP 16666.

Q. Como eu ajusto as configurações bidirecional no controlador do Wireless LAN (WLC) e no Lightweight Access Points (regaços)?

A. O Produtos de Cisco Wireless funciona melhor quando a velocidade e duplexação é negociado automaticamente, mas você tem a opção para ajustar as configurações bidirecional no WLC e nos regaços. A fim ajustar as configurações speed/duplex AP, você pode configurar as configurações bidirecional para os regaços no controlador e então, por sua vez, empurra-os para os regaços.

configurar a velocidade <auto/10/100/1000> <all/Cisco AP Name> do duplex Ethernet <auto/half/full> ap é o comando ajustar as configurações bidirecional com o CLI. Este comando é apoiado com versões 4.1 e mais recente somente.

A fim ajustar as configurações bidirecional para as interfaces física WLC, use o **physicalmode da porta da configuração {tudo | porta} {100h | 100f | 10h |** comando **10f}**.

Este conjuntos de comandos especificada ou todas as portas Ethernet do painel frontal 10/100BASE-T para 10 Mbps dedicado ou 100 Mbps, metade-frente e verso ou operação bidirecional. Note que você deve desabilitar a negociação automática com o **comando disable da autonegociação da porta da configuração** antes que você configure manualmente todo o modo físico na porta. Também, note que o **comando autoneg da porta da configuração** cancela os ajustes feitos com o comando do **physicalmode da porta da configuração**. À revelia, todas as portas são ajustadas ao automóvel negociam.

Note: Não há nenhuma maneira de mudar os ajustes da velocidade nas portas de fibra.

Q. Há uma maneira de seguir o nome do Access point de pouco peso (REGAÇO) quando não é registrado ao controlador?

A. Se seu AP completamente para baixo e não é registrado ao controlador, não há nenhuma maneira que você pode seguir o REGAÇO através do controlador. A única maneira que permanece é que você pode alcançar o interruptor em que estes AP são conectados, e você pode encontrar o switchport em que são conectados usando este comando:

```
show mac-address-table address <mac address>
```

Isto dá-lhe o número de porta no interruptor a que este AP é conectado. Então, emita este comando:

```
show cdp nei <type/num> detail
```

A saída deste comando igualmente dá o nome do REGAÇO. Contudo, este método é somente possível quando seu AP é posto acima e conectado ao interruptor.

Q. Eu configurei 512 usuários em meu controlador. Há alguma maneira de aumentar o número de usuários no controlador do Wireless LAN (WLC)?

A. A base de dados de usuário local é limitada a um máximo de 2048 entradas na **Segurança >** página **geral**. Este base de dados é compartilhado por usuários do gerenciamento local (que inclui embaixadores da entrada), pelos usuários líquidos (que inclui usuários convidado), pelo filtro MAC entradas, de autorização do Access point entradas de lista, e entradas de lista da exclusão. Junto, todos estes tipos de usuários não podem exceder o tamanho de base de dados configurado.

A fim aumentar o base de dados local, use este comando do CLI:

```
show cdp nei <type/num> detail
```

Note: Você tem que salvar a configuração e restaurar o sistema (que usa o **comando reset system**) para que a mudança tome o efeito.

Q. Como eu reforço uma política de senha elaborada em WLC?

A. Os WLC permitem que você defina uma política de senha elaborada. Isto pode ser feito usando o CLI ou o GUI.

No GUI, vá à **Segurança >** ao **AAA >** às **políticas de senha**. Esta página tem uma série de opções que possa ser selecionada a fim reforçar uma senha elaborada. Aqui está um exemplo:

A fim fazer isto do WLC CLI, use o forte-**pwd do switchconfig da configuração** *{caso-verificação | consecutivo-verificação | padrão-verificação | username-verificação | todo-verificação} {permita |* comando do *desabilitação}*:

```
show cdp nei <type/num> detail
```

- **caso-verificação** - Verifica a ocorrência do mesmos caráter três vezes consecutivamente.
- **consecutivo-verificação** - Verifica se os valores padrão ou suas variações estão sendo usadas.
- **padrão-verificação** - Verifica se ou username ou seu o reverso está sendo usado.
- **todo-verificações** - Permite/desabilita todo o forte verificações da senha.

P.. Como os recursos de cliente passivos são usados em controladores do Wireless LAN?

A. Os clientes passivos são dispositivos Wireless, tais como escalas e impressoras isso são

configurados com um endereço IP estático. Estes clientes não transmitem nenhum IP informação tal como o endereço IP de Um ou Mais Servidores Cisco ICM NT, a máscara de sub-rede, e a informação de gateway quando eles associado com um Access point. Em consequência, quando os clientes passivos forem usados, o controlador nunca conhece o endereço IP de Um ou Mais Servidores Cisco ICM NT a menos que usarem o DHCP.

Os WLC atuam atualmente como um proxy para requisições ARP. Em cima de receber um ARP o pedido, o controlador responde com uma reação ARP em vez da passagem pedido diretamente ao cliente. Esta encenação tem duas vantagens:

- O dispositivo ascendente que manda a requisição ARP ao cliente vai faz4e-lo para não saber onde o cliente é encontrado.
- Potência para dispositivos a pilhas tais como telefones celulares e impressoras é preservado porque não têm que responder a cada ARP pedidos.

Desde que o controlador wireless não tem nenhuma informação relacionada IP sobre os clientes passivos, não pode responder a nenhuma requisições ARP. A corrente o comportamento não permite transferência das requisições ARP aos clientes passivos. Alguns o aplicativo que tenta alcançar um cliente passivo falhará.

Os recursos de cliente passivos permitem as requisições ARP e as respostas ser trocado entre prendido e clientes Wireless. Esta característica, quando permitida, permite que o controlador passe requisições ARP do prendido aos clientes Wireless até o cliente Wireless desejado obtém ao estado de CORRIDA.

Para obter informações sobre de como configurar os recursos de cliente passivos, leia a seção sobre Utilização o GUI para configurar dentro o cliente passivo Cisco Guia de configuração de controle do Wireless LAN, liberação 7.0.116.0.

P.. Como possa I estabelece o cliente para autenticar novamente com o servidor Radius cada três minutos ou em algum período especificado?

A. O parâmetro de timeout de sessão no WLC pode ser usado para realizar isto. À revelia, o parâmetro de timeout de sessão é configurado por 1800 segundos antes de um reauthentication ocorre.

Mude este valor a 180 segundos a fim fazer o cliente reauthenticate após três minutos.

A fim alcançar o parâmetro de timeout de sessão, clique Menu **WLAN no** GUI. Indica a lista de WLAN configurado no WLC. Clique o WLAN a que o cliente pertence. Vá a **o guia avançada** e você encontram *para permitir a sessão Parâmetro de timeout*. Mude o valor padrão a 180, e clique-o **Aplique** para que as mudanças tomem o efeito.

Quando enviado em uma aceitação de acesso, junto com um valor da Terminação-ação de A requisição RADIUS, o atributo do Sessão-intervalo especifica o número máximo de segundos do serviço fornecidos antes da reautenticação. Neste caso, O atributo do Sessão-intervalo é usado para carregar o ReAuthPeriod constante dentro do Máquina de estado do temporizador do Reauthentication do 802.1X.

P.. Eu tenho um Tunelamento do convidado, Ethernet sobre o túnel IP (EoIP), configurado entre meu controlador do Wireless LAN 4400 (WLC), que atua como a âncora o WLC, e diversos WLC remotos. Podem este os broadcasts de sub-rede

da âncora WLC para a frente completamente o túnel de EoIP da rede ligada com fio aos clientes Wireless associados com controladores remotos?

A. Não, o WLC 4400 não envia broadcasts de sub-rede IP do prendido lado aos clientes Wireless através do túnel de EoIP. Este não é apoiado característica. Cisco não apoia o Tunelamento do broadcast de sub-rede ou do Multicast dentro topologia do acesso do convidado. Desde que o convidado WLAN força o Point of Presence do cliente a um lugar muito específico na rede, na maior parte fora do Firewall, o Tunelamento do broadcast de sub-rede pode ser um problema de segurança.

P.. Em um controlador do Wireless LAN (WLC) e no protocolo de pouco peso do Access point (LWAPP) setup, que Differentiated Services Code Point (DSCP) avalia são passados para o tráfego de voz? Como QoS é executado no WLC?

A. A solução WLAN da rede de Cisco Unified Wireless (UWN) apoia quatro níveis de QoS:

- Platina/Voz
- Ouro/vídeo
- De prata/melhor esforço (padrão)
- Bronze/fundo

Você pode configurar o tráfego de voz WLAN para usar a platina QoS, atribui a largura de banda baixa WLAN para usar QoS de bronze, e para atribuir no meio todo tráfego restante os outros níveis de QoS. Consulte Atribuição um perfil de QoS a um WLAN para mais informação.

P.. São os bridges Ethernet de Linksys apoiados em um Cisco Wireless unificado Solução?

A. Não, o WLC apoia somente o Produtos de Cisco WGB. Linksys WGB não é apoiado. Embora a solução unificada do Cisco Wireless não apoie Linksys WET54G e bridges Ethernet WET11B, você pode usar estes dispositivos na Configuração wireless da solução unificada se você usa estas diretrizes:

- Conecte somente um dispositivo ao WET54G ou ao WET11B.
- Permita a característica da clonagem MAC no WET54G ou no WET11B de clonar dispositivo conectado.
- Instale os direcionadores e o firmware os mais novos nos dispositivos conectados ao WET54G ou WET11B. Esta diretriz é especialmente importante para impressoras de JetDirect porque umas versões de firmware mais adiantadas causam problemas com DHCP.

Note: Outras pontes da terceira não são apoiadas. As etapas mencionadas podem seja tentado igualmente para outras pontes da terceira.

P.. Como faço eu armazene os arquivos de configuração no controlador do Wireless LAN (WLC)?

A. O WLC contém dois tipos de memória:

- RAM temporário — Guarda a corrente, controlador ativo configuração
- RAM não-volátil (NVRAM) — Guarda a repartição configuração

Quando você configura o sistema operacional no WLC, você está alterando RAM temporário. Você deve salvar a configuração de RAM temporário ao NVRAM a fim certificar-se de que as repartições WLC na configuração atual.

Éimportante saber que memória você está alterando quando você executa estas tarefas:

- Use o wizard de configuração.
- Cancele a configuração de controle.
- Salvar configurações.
- Restaure o controlador.
- Saída do CLI.

Características FAQ

P.. Como eu ajusto o tipo do Extensible Authentication Protocol (EAP) no Controlador do Wireless LAN (WLC)? Eu quero autenticar contra um controle de acesso O dispositivo do server (ACS), e eu obtemos “um EAP unsupported” datilografamos dentro logs.

A. Não há nenhuma configuração de tipo separada EAP no WLC. Para a luz EAP (PULO), Autenticação Flexível de EAP através do Tunelamento seguro (EAP-FAST), ou Microsoft O EAP protegido (MS-PEAP), apenas configura o IEEE 802.1X ou o acesso protegido por wi-fi (WPA) (se você usa o 802.1x com WPA). Algum tipo EAP que for apoiado no O servidor de retaguarda do RAIO e no cliente é apoiado através da etiqueta do 802.1x. O EAP ajustar-se no cliente e no servidor Radius deve combinar.

Termine estas etapas a fim permitir o EAP com o GUI no WLC:

1. Do WLC GUI, clique **WLAN**.
2. Uma lista de WLAN configurados no WLC aparece. Clique um WLAN.
3. Nos **WLAN > editam**, clicam **ABA de segurança**.
4. Clique a **camada 2**, e escolha a Segurança da camada 2 como 802.1x ou WPA+WPA2. Você pode igualmente configurar os parâmetros do 802.1x que estão disponíveis dentro o mesmo indicador. Então, WLC os pacotes da autenticação de EAP para a frente entre cliente Wireless e o Authentication Server.
5. Clique os **servidores AAA**, e escolha Authentication Server do menu suspenso para este WLAN. Nós supomos que o Authentication Server é configurado já globalmente. Para obter informações sobre de como permita a opção de EAP em WLC através do comando line interface(cli), consulte ao *Utilização o CLI para configurar o RAIO* seção do Cisco Guia de configuração de controle do Wireless LAN, liberação 7.0.116.0.

P.. Que o SSID rápido está mudando?

A. A mudança rápida SSID permite que os clientes movam-se entre SSID. Quando o cliente envia uma associação nova para um SSID diferente, a entrada de cliente no a tabela de conexão do controlador é cancelada antes que o cliente esteja adicionado ao novo SSID. Quando a mudança rápida SSID é desabilitada, o controlador reforça um atraso antes que estiverem permitidos aos clientes se transportar a um SSID novo. Para obter informações sobre de como permita o SSID rápido que muda, refira *Configurando Mudança rápida SSID* seção do Cisco Guia de configuração

de controle do Wireless LAN, liberação 7.0.116.0.

P.. Posso eu ajustar um limite no número de clientes que podem conectar a um Sem fio LAN?

A. Você pode ajustar um limite ao número de clientes que podem conectar à WLAN, que é útil nas encenações onde você tem um número limitado de clientes isso pode conectar a um controlador. O número de clientes que você pode configurar pelo WLAN depende da plataforma que você está usando.

Leia a seção Configurando o número máximo de clientes pelo WLAN do Cisco Guia de configuração de controle do Wireless LAN, liberação 7.0.116.0 para informação nos limites do cliente pelo WLAN para as Plataformas diferentes de Controladores do Wireless LAN.

P.. O que são PKC e como ele trabalha com o controlador do Wireless LAN (WLC)?

A. PKC representa pôr em esconderijo chave dinâmico. Foi projetado como uma extensão ao padrão de IEEE 802.11i.

PKC é uma característica permitida em controladores do 2006/410x/440x Series de Cisco que licenças equiparam corretamente clientes Wireless para vaguear sem completamente reautenticação com um servidor AAA. A fim compreender primeiramente PKC, você necessidade de compreender pôr em esconderijo chave.

Pôr em esconderijo chave é uma característica que seja adicionada ao WPA2. Isto permite um móbil poste para pôr em esconderijo os chaves mestres (por pares [PMK] do chave mestre) que ganha com a a autenticação bem sucedida com um Access Point (AP), e **reutiliza-o na associação futura com o mesmo AP**. Isto significa que um móbil dado o dispositivo precisa de autenticar uma vez com um AP específico, e põe em esconderijo a chave para uso futuro. Pôr em esconderijo chave é segurado através de um mecanismo conhecido como o identificador PMK (PMKID), que é uma mistura do PMK, de uma corda, da estação e do MAC endereços do AP. O PMKID identifica excepcionalmente o PMK.

Mesmo com pôr em esconderijo chave, uma estação wireless deve autenticar com cada um AP que deseja obter o serviço de. Isto introduz a latência significativa e sobrecargas, a que atrase o processo da mão-fora e possa inibir a capacidade apoie aplicativos em tempo real. A fim resolver esta edição, PKC era introduzido com WPA2.

PKC permite que uma estação reutilize um PMK que ganhe previamente com a processo de autenticação bem sucedida. Isto elimina a necessidade para a estação a autentique contra AP novos ao vaguear.

Consequentemente, em um intra-controlador que vagueia, quando um dispositivo móvel se mover de um AP a outro no mesmo controlador, os re-cálculos do cliente um PMKID usar o PMK previamente usado e apresenta-o durante o processo de associação. O WLC procura seu esconderijo PMK para determinar se tem tal entrada. Se ele faz, contorneia o processo de autenticação e imediatamente os novatos do 802.1x as trocas de chave WPA2. Se não fazem, atravessam o 802.1X padrão processo de autenticação.

PKC é permitido à revelia com WPA2. Consequentemente, quando você permitir o WPA2 como A Segurança da camada 2 sob a configuração WLAN do WLC, PKC é permitida no WLC. Também, configurar o servidor AAA e o cliente Wireless para o EAP apropriado autenticação.

O suplicante usado no lado do cliente deve igualmente apoiar o WPA2 dentro ordem para que PKC trabalhe. PKC pode igualmente ser executado em um inter-controlador ambiente vagueando.

Note: PKC não trabalha com utilitário de Desktop de Aironet (ADU) como o cliente suplicante.

P.. O que são as explicações para estas configurações de timeout no controlador: Intervalo do Address Resolution Protocol (ARP), idle timeout do usuário, e sessão Intervalo?

A. **O arp timeout** é usado para suprimir de entradas de ARP no WLC para os dispositivos aprendidos da rede.

O idle timeout do usuário: Quando um usuário for inativo sem alguns uma comunicação com o REGAÇO para a quantidade de tempo ajustada como o idle timeout do usuário, o cliente deauthenticated pelo WLC. O cliente tem que reauthenticate e reassocie ao WLC. É usado nas situações onde um cliente pode sair de seu REGAÇO associado sem notificar o REGAÇO. Isto pode ocorrer se a bateria vai absolutamente no cliente ou os associados do cliente afastam-se.

Note: A fim alcançar o ARP e o idle timeout do usuário no WLC GUI, vá a o menu do **controlador**. Escolha o **general do** o lado esquerdo para encontrar o ARP e o idle timeout do usuário coloca.

O timeout de sessão é o tempo máximo para um cliente sessão com o WLC. Após este tempo, o WLC de-autentica o cliente, e o cliente atravessa o processo inteiro da autenticação (reautenticação) outra vez. Isto é parte de uma precaução da Segurança para girar as chaves de criptografia. Se você use um método do Extensible Authentication Protocol (EAP) com o gerenciamento chave, rekeying ocorre em cada intervalo regular a fim derivar uma criptografia nova chave. Sem gerenciamento chave, este valor de timeout é o tempo que Sem fio os clientes precisam de fazer um reauthentication completo. O timeout de sessão é específico a o WLAN. Este parâmetro pode ser alcançado do **WLAN > Edite o** menu.

P.. Que é um sistema RFID? Que RFID etiqueta é apoiado atualmente por Cisco?

A. O Radio Frequency Identification (RFID) é uma tecnologia que use o rádio uma comunicação da frequência para uma comunicação razoavelmente de curto prazo. Um RFID básico o sistema é composto de etiquetas RFID, de leitores RFID, e do software de processamento.

Atualmente Cisco apoia etiquetas RFID de AeroScout e de Pango. Para mais a informação sobre como configurar etiquetas de AeroScout, refere WLC Configuração para etiquetas de AeroScout RFID.

P.. Posso eu executar a autenticação de EAP localmente no WLC? Há alguns documente que explica esta característica local EAP?

A. Sim, a autenticação de EAP pode ser executada localmente no WLC. EAP local é um método de autenticação que permita que os usuários e os clientes Wireless sejam autenticado localmente no WLC. É projetado para o uso nos escritórios remotos isso queira manter a Conectividade aos clientes Wireless quando o sistema backend torna-se interrompido, ou o servidor de autenticação externa vai para baixo. Quando você permita o EAP local, os saques WLC como o Authentication Server. Para mais a informação sobre como configurar um WLC para a autenticação EAP-rápida local, consulta ao Local Autenticação de EAP no controlador do Wireless LAN com EAP-FAST e o servidor ldap Exemplo de configuração.

P.. Que é a característica da ultrapassagem WLAN? Como eu configuro esta característica? Vá faz4e-lo os regaços mantêm os valores da ultrapassagem WLAN quando falham sobre ao backup WLC?

A. A característica da ultrapassagem WLAN permite-nos de escolher WLAN entre do WLAN configurados em um WLC que possa ativamente ser usado em uma base individual do REGAÇO. Termine estas etapas a fim configurar uma ultrapassagem WLAN:

1. No WLC GUI, clique o **Sem fio** menu.
2. Clique os **rádios da** opção no lado esquerdo, e escolha o **802.11 a/n** ou o **802.11 b/g/n.**
3. Clique o link **configurar do** menu suspenso encontrado no lado direito que corresponde ao nome do AP em que você queira configurar a ultrapassagem WLAN.
4. Escolha **permitem da** gota-para baixo da ultrapassagem WLAN menu. O menu de cancelamento de WLAN é o último artigo no lado esquerdo do indicador.
5. A lista de todos os WLAN que são configurados no WLC aparece.
6. Desta lista, verifique os **WLAN a** que você quer apareça no REGAÇO, e o clique **aplica-se** para que as mudanças tomem efeito.
7. Salvar sua configuração depois que você faz estes mudanças.

Os AP retêm os valores da ultrapassagem WLAN quando obtêm registrados a outros WLC, contanto que os perfis WLAN e os SSID que você quer cancelar são configurado através de todos os WLC.

Note: No software release 5.2.157.0 do controlador, a característica da ultrapassagem WLAN foi removido do controlador GUI e do CLI. Se seu controlador é configurado para a ultrapassagem e você WLAN promova ao software release do controlador 5.2.157.0, o controlador suprime da configuração WLAN e transmite tudo WLAN. Você pode especificar que somente determinados WLAN estejam transmitidos se você configura grupos do Access point. Cada Access point anuncia somente os WLAN permitidos isso pertença a seu grupo do Access point.

Note: Os grupos do Access point não permitem WLAN de ser transmitidos sobre por interface de rádio do AP.

P.. É o IPv6 apoiado nos controladores de LAN do Cisco Wireless (WLC) e Lightweight Access Points (regaços)?

A. Atualmente, os controladores do 4400 e 4100 Series apoiam somente o IPv6 transmissão do cliente. O apoio nativo do IPv6 não é apoiado.

A fim permitir o IPv6 no WLC, verifique o **IPv6 Permita a** caixa de verificação na configuração WLAN SSID sob WLAN > Edite a página.

Também, o Modo multicast dos Ethernet (EMM) é exigido para apoiar o IPv6. Se você desabilite EMM, os dispositivos do cliente que usam o IPv6 perdem a Conectividade. A fim permitir EMM, vão ao controlador > página geral e do Multicast dos Ethernet O modo deixa cair para baixo o menu, escolhe o **unicast** ou **Multicast**. Isto permite o Multicast ou no modo de Unicast ou Modo multicast. Quando o Multicast é permitido como o unicast do Multicast, os pacotes são replicated para cada AP. Esta pode ser utilização de processador, assim que use-a com cuidado. O Multicast permitido como o Multicast do Multicast usa o usuário atribuído endereço de multicast para fazer para fora um Multicast mais tradicional aos Access point (AP).

Note: O IPv6 não é apoiado nos 2006 controladores.

Também, há a identificação de bug Cisco CSCsg78176, que impede usar o IPv6 transmissão quando a característica AAA Overrride for usada.

P.. Faz a Web do apoio do controlador do Wireless LAN do Cisco 2000 Series (WLC) Autenticação para usuários convidado?

A. A autenticação da Web é apoiada em todo o Cisco WLC. Autenticação da Web é um método de autenticação da camada 3 usado para autenticar usuários com simples credenciais de autenticação. O no encryption é involvido. Termine estas etapas dentro ordem para permitir esta característica:

1. Do GUI, clique o **WLAN** menu.
2. Clique um **WLAN**.
3. Vá à **ABA de segurança** e escolha a **camada 3.**
4. Verifique a caixa da **política da Web** e escolha-a **Autenticação**.
5. Clique em **Apply** para salvar as alterações.
6. A fim criar um base de dados no WLC contra a que autentique usuários, vá ao **menu Segurança no** GUI, escolha-os **O usuário líquido local**, e termina estas ações: Defina o nome de usuário e senha do convidado para que o convidado use-se dentro ordem a entrar. Estes valores são diferenciando maiúsculas e minúsculas.Escolha o ID de WLAN que você usa.**Note**: Para mais configuração detalhada, refira Tecnologia Wireless Exemplo de configuração da autenticação da Web do controlador de LAN.

P.. Pode o WLC ser controlado no modo wireless?

A. O WLC pode ser controlado com o modo wireless uma vez que é permitido. Para mais a informação em como permitir o modo wireless refere *Possibilidade Conexões Wireless ao GUI e ao CLI* seção do Cisco Guia de configuração de controle do Wireless LAN, liberação 7.0.116.0.

P.. Que é agregação do link (RETARDAÇÃO)? Como eu permito a RETARDAÇÃO no Wireless LAN Controladores (WLC)?

A. A RETARDAÇÃO empacota todas as portas no WLC em um único EtherChannel relação. O sistema controla dinamicamente o equilíbrio e a porta da carga de tráfego Redundância com RETARDAÇÃO.

Geralmente, a relação no WLC tem os parâmetros múltiplos associados com ele, que inclui o endereço IP de Um ou Mais Servidores Cisco ICM NT, gateway padrão (para a sub-rede IP), preliminar porta física, porta física secundária, etiqueta VLAN, e servidor DHCP. Quando a RETARDAÇÃO for não usada, cada relação é traçada geralmente a uma porta física, mas ao múltiplo as relações podem igualmente ser traçadas a uma única porta WLC. Quando a RETARDAÇÃO for usada, o sistema traça dinamicamente as relações ao Canal de porta agregado. Isto ajudas na redundância de porta e no Balanceamento de carga. Quando uma porta falhar, a relação é traçado dinamicamente à porta física disponível seguinte, e os regaços são equilibrado através das portas.

Quando a RETARDAÇÃO for permitida em um WLC, WLC os frames de dados para a frente no mesmos porta em que foram recebidos. O WLC confia no switch vizinho a tráfego do

balanceamento de carga através do EtherChannel. O WLC não executa alguns Função de balanceamento de carga do EtherChannel no seus próprios.

P.. O que modela da agregação do link de suporte dos controladores do Wireless LAN (WLC) (RETARDAÇÃO)?

A. RETARDAÇÃO do apoio dos controladores do Cisco 5500 Series no Software Release 6.0 ou mais tarde, RETARDAÇÃO do apoio dos controladores do Cisco 4400 Series no Software Release 3.2 ou mais tarde, e RETARDAÇÃO é permitido automaticamente nos controladores dentro de Cisco WiSM e o catalizador 3750G integraram o interruptor do controlador do Wireless LAN. Sem RETARDAÇÃO, cada porta do sistema de distribuição em apoios de um controlador do Cisco 4400 Series até 48 Access point. Com a RETARDAÇÃO permitida, um controlador de Cisco 4402 lógico a porta apoia até 50 pés Access point, a porta lógica de um controlador de Cisco 4404 apoios até 100 Access point, e a porta lógica no catalizador 3750G O controlador integrado do Wireless LAN liga e cada controlador de Cisco WiSM apoios até 150 Access point.

Os WLC de Cisco 2106 e 2006 não apoiam a RETARDAÇÃO. Modelos anteriores, tais como o Cisco 4000 Series WLC, não apoie a RETARDAÇÃO.

P.. O que é a característica da mobilidade da auto-âncora no Sem fio unificado Redes?

A. a mobilidade da Auto-âncora (ou a mobilidade do convidado WLAN) são usadas para melhorar a carga equilíbrio e Segurança para clientes vagueando em seu Sem fio LAN (WLAN). Sob as circunstâncias vagueando normais, dispositivos do cliente juntam-se a um WLAN e são ancoradas ao primeiro controlador que contactam. Se um cliente vagueia a uma sub-rede diferente, o controlador a que o cliente vagueia grupos - acima de uma sessão estrangeira para cliente com o controlador da âncora. Com o uso da mobilidade da auto-âncora característica, você pode especificar um controlador ou um grupo de controladores como a âncora pontos para clientes em um WLAN.

Note: A âncora da mobilidade não deve ser configurada para a mobilidade da camada 3. a âncora da mobilidade é usada somente para o Tunelamento do convidado.

P.. Pode um controlador do Wireless LAN de Cisco 2006 (WLC) seja configurado como uma âncora para um WLAN?

A. Um Cisco 2000 Series WLC não pode ser designado como uma âncora para um WLAN. Contudo, um WLAN criado em um Cisco 2000 Series WLC pode ter um Cisco 4100 Series WLC e Cisco 4400 Series WLC como sua âncora.

P.. Que tipo de Tunelamento da mobilidade o controlador do Wireless LAN usa?

A. Software Release 4.1 do controlador através 5.1 do apoio ambos assimétricos e Tunelamento simétrico da mobilidade. Software Release 5.2 ou Mais Recente do controlador apoie somente o Tunelamento simétrico da mobilidade, por que é permitido agora sempre padrão.

No Tunelamento assimétrico, o tráfego do cliente à rede ligada com fio é distribuído diretamente através do controlador estrangeiro. Rupturas assimétricas do Tunelamento quando o roteador fluxo acima tem a filtração do caminho reverso (RPF) permitida. Neste caso, o tráfego do cliente é

deixado cair no roteador porque a verificação RPF assegura aquela o trajeto de volta ao endereço de origem combina o trajeto de que o pacote vem.

Quando o Tunelamento simétrico da mobilidade é permitido, todo o tráfego do cliente é enviado ao controlador da âncora e pode então com sucesso passar a verificação RPF. O Tunelamento simétrico da mobilidade é igualmente útil nestas situações:

- Se uma instalação do Firewall no trajeto do pacote cliente deixa cair pacotes porque o endereço IP de origem não combina a sub-rede em que os pacotes são recebidos, isto é útil.
- Se o grupo VLAN do acesso-ponto no controlador da âncora é diferente do que a relação VLAN WLAN no controlador estrangeiro: neste caso, cliente o tráfego pode ser enviado em um VLAN incorreto durante a mobilidade eventos.

P.. Como faça nós alcançamos o WLC quando a rede é para baixo?

A. Quando a rede está para baixo, o WLC pode ser alcançado pela porta do serviço. Esta porta é atribuída um endereço IP de Um ou Mais Servidores Cisco ICM NT em uma sub-rede totalmente diferente de outro as portas do WLC e são chamadas assim gerenciamento fora de banda. Para mais informação, consulte *Configurando Portas e relações* seção do Cisco Guia de configuração de controle do Wireless LAN, liberação 7.0.116.0.

P.. Faça os controladores de LAN do Cisco Wireless (WLC) apoiam o Failover (ou característica da Redundância)?

A. Sim, se você tem dois ou mais WLC em sua rede de WLAN, você pode configurar-los para a Redundância. Geralmente, um REGAÇO junta-se ao preliminar configurado WLC. Uma vez que o WLC preliminar falha, o REGAÇO recarrega e junta-se a um outro WLC no grupo da mobilidade. O Failover é uma característica onde o REGAÇO vota para o WLC preliminar e junta-se ao WLC preliminar uma vez que é funcional. Consulte a seção WLAN Failover do controlador para o exemplo de configuração do Lightweight Access Points para obter mais informações.

P.. O que é o uso do Access Control Lists (ACLs) da PRE-autenticação dentro Controladores do Wireless LAN (WLC)?

A. Com PRE-autenticação ACL, como o nome implica, você pode permitir o cliente o tráfego a e de um endereço IP de Um ou Mais Servidores Cisco ICM NT específico mesmo antes do cliente autentica. Ao usar um servidor de Web externo para a autenticação da Web, algum do WLC as Plataformas precisam uma PRE-autenticação ACL para o servidor de Web externo (Cisco Controlador do 5500 Series, um Cisco 2100 Series controlador, Cisco 2000 Series e o módulo de rede do controlador). Para as outras Plataformas WLC, a PRE-autenticação ACL não é imperativa. Contudo, é uma boa prática a configurar uma PRE-autenticação ACL para o servidor de Web externo ao usar-se autenticação do web externa.

P.. Eu tenho um WLAN MAC-filtrado e um WLAN completamente aberto em minha rede. O cliente escolhe o WLAN aberto à revelia? Ou faz o cliente associe automaticamente com o ID de WLAN que é ajustado no filtro MAC? Também, por que há uma opção da “relação” em um filtro MAC?

A. O cliente pode associar a todo o WLAN a que o cliente for configurado para conectar. A opção de interface no filtro MAC dá a capacidade para aplicar-se o filtro a um WLAN ou a uma relação.

Se múltiplo os WLAN são amarrados ao a mesma relação, você pode aplicar o filtro MAC à relação sem a necessidade para criar um filtro para cada WLAN individual.

P.. Como posso eu configurar a autenticação TACACS para usuários do Gerenciamento no Controlador do Wireless LAN (WLC)?

A. Partindo da versão 4.1 WLC, o TACACS é apoiado nos WLC. Consulte para Configurando TACACS+ a fim compreender como configurar o TACACS+ para autenticar usuários do Gerenciamento do WLC.

P.. O que é o uso do ajuste excessivo da falha de autenticação na Controlador do Wireless LAN (WLC)?

A. Este ajuste é uma das políticas da exclusão do cliente. O cliente a exclusão é uns recursos de segurança no controlador. A política é usada a pôr clientes a fim impedir o acesso ilegal à rede ou aos ataques à rede Wireless.

Com esta política excessiva da falha da autenticação da Web permitida, quando a o número de cliente de tentativas falhadas da autenticação da Web excede 5, o controlador considera que o cliente excedeu as tentativas máximas da Web a autenticação e pôr o cliente.

Termine estas etapas a fim permitir ou desabilitar isto ajuste:

1. Do WLC GUI, vai à **Segurança > a proteção wireless Políticas > políticas da exclusão do cliente**.
2. Verifique ou desmarcar a **autenticação da Web excessiva Falhas**.

P.. Eu converti meu Access Point (AP) autônomo ao modo leve. Em o modo de pouco peso do protocolo AP (LWAPP) com o server dos RADIUS AAA para o cliente explicando, o cliente é seguido normalmente com a contabilidade do RAIO baseada no Endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC. É possível ajustar a contabilidade do RAIO baseada no MAC address do AP associado a esse WLC e não ao endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC?

A. Sim, isto pode ser feito com a configuração do lado WLC. Termine estes etapas:

1. Do controlador GUI, sob a **Segurança > o raio Explicar**, há uma caixa suspensa para o tipo do ID de estação do atendimento. Escolha **MAC address AP**.
2. Verifique isto através do log LWAPP AP. Lá, você pode ver o campo da estação chamada ID que indica MAC address do AP a que o cliente específico é associado.

P.. Como você muda o intervalo do aperto de mão do Wi-Fi Protected Access (WPA) avalie em um controlador do Wireless LAN (WLC) com o CLI? Eu sei que eu posso fazer este sobre Access point de Cisco IOS® (AP) com o aperto de mão do wpa do dot11 valor de timeout comando, mas como o faça execute isto em um WLC?

A. A capacidade para configurar o intervalo do WPA-aperto de mão com os WLC era integrado no Software Release 4.2 e Mais Recente. Você não precisa esta opção dentro versões de software WLC mais adiantadas.

Estes comandos podem ser usados para mudar o intervalo do aperto de mão WPA:

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

Os valores padrão continuam a refletir os WLC atuais comportamento.

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

Note: Em IO AP, este ajuste é configurável com o **dot11** comando do **aperto de mão do wpa**.

Você pode igualmente configurar os outros parâmetros EAP com as opções abaixo o comando **avançado do eap da configuração**.

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

P.. O que é a finalidade da característica diagnóstica do canal no WLAN > Edite > avançou a página?

A. A característica diagnóstica do canal permite-o de pesquisar defeitos dentro problemas consideração a uma comunicação cliente com um WLAN. O cliente e os Access point podem ser põe completamente um grupo definido de testes para identificar a causa de uma comunicação as dificuldades a que as experiências do cliente e reservam então medidas corretiva seja tomado para fazer o cliente operacional na rede. Você pode usar o controlador GUI ou CLI para permiti-lo o canal diagnóstico, e pode usar controlador CLI ou WCS para executar os testes diagnósticos.

O canal diagnóstico pode ser usado para testar somente. Se você tenta a configurar a autenticação ou a criptografia para o WLAN com o canal diagnóstico permitido, você vê este erro:

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

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

- Um máximo de grupos do Access point dos 50 pés para o Cisco 2100 Series Controlador e módulos de rede do controlador
- Um máximo de grupos de 300 Access point para o Cisco 4400 Series Controlador do Wireless LAN dos controladores, do Cisco WiSM, e do Cisco 3750G Switch
- Um máximo de grupos de 500 Access point para o Cisco 5500 Series Controladores

Informações Relacionadas

- Tecnologia Wireless Controlador de LAN (WLC) FAQ
- Tecnologia Wireless Erro do controlador de LAN (WLC) e mensagens de sistema FAQ

- De pouco peso Access point FAQ
- Cisco Guia de configuração de controle do Wireless LAN, liberação 7.0.116.0
- Apoio do IPv6 no controlador do Wireless LAN
- Tecnologia Wireless Suporte de Produto
-
- Suporte Técnico e Documentação - Cisco Systems

Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabore com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções usadas neste documento.

Atualizado em: março 02, 2015
ID do Documento: 118833