

Solucionar problemas de controladores LAN sem fio AireOS

Contents

- [Introdução](#)
- [Pré-requisitos](#)
- [Requisitos](#)
- [Componentes Utilizados](#)
- [Conventions](#)
- [Problemas de componentes da controladora](#)
- [Assinaturas IDS](#)
- [NAC](#)
- [OEAP](#)
- [Classificação de invasor baseada em regras](#)
- [Assinatura IDS](#)
- [RLDP](#)
- [Canal de diagnóstico](#)
- [Mobilidade entre controladores](#)
- [AP Honeypot](#)
- [Integração com AirMagnet](#)
- [Autenticação Local](#)
- [Depuração do controlador](#)
- [Autenticação geral de AAA](#)
- [TACACS+](#)
- [LDAP](#)
- [Proteção de Quadro de Gerenciamento de Cliente \(MFP - Client Management Frame Protection\)](#)
- [Mobilidade](#)
- [Relatar Problemas](#)
- [Problemas relacionados ao FIPS](#)
- [O cliente sem fio usa autenticador local com EAP-TLS, EAP-FAST e PEAP](#)
- [512 grupos de WLANs/AP](#)
- [ACLs, ACLs de pré-autenticação e ACLs de CPU](#)
- [DHCP](#)
- [Problemas relacionados ao acesso de convidados](#)
- [Problemas de alta disponibilidade da WLC](#)
- [Problemas relacionados ao H-REAP do controlador](#)
- [Fluxo de mídia](#)
- [Problemas relacionados ao local](#)
- [Memória do sistema, problemas de memória insuficiente](#)
- [Problemas relacionados à malha](#)
- [Problemas com o cliente NTP e a configuração de tempo no controlador](#)
- [Problemas de componentes de RF para as WLCs](#)
- [Componente SNMP para WLCs](#)
- [Problemas de upload/download de TFTP que incluem upgrade/downgrade](#)
- [Componente Web GUI para WLCs](#)
- [WLC-Webauth-Template](#)
- [Problemas e aprimoramentos relacionados à configuração XML do controlador](#)
- [Canal de diagnóstico](#)
- [Alocação de canal dinâmico](#)
- [TACACS+](#)

[WLC-Multicast-Guide](#)

[WLC-QoS-Guide](#)

[Depuração de controle de chamada \(classificação SIP\)](#)

[Controle de admissão baseado em carga e métricas de voz](#)

[WLC-License-Guide](#)

[Problemas do ARP](#)

[Problemas de rede](#)

[Problemas com o ponto de acesso](#)

[IAPP](#)

[Problemas de associação WGB](#)

[O cliente com fio ou WGB não obtém o endereço DHCP](#)

[O cliente com fio ou WGB usa endereço IP estático, mas o endereço IP não aparece no controlador](#)

[Senha do nome de usuário do AP](#)

[Problemas de conexão do cliente](#)

[O controlador não gosta da solicitação de associação](#)

[O cliente não responde às solicitações EAP](#)

[O CCKM em roaming falha](#)

[Falha no cache de PMKID](#)

[Problemas de reautenticação](#)

[802.11R \(Transição Rápida\) Roaming Não Funciona](#)

[Mobilidade entre controladores](#)

[Desabilitar depurações](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como usar o comando `debug` e `show` comandos para solucionar problemas de controladoras Wireless LAN (WLCs).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Os comandos usados neste documento são específicos das versões do software Cisco AireOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

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

Problemas de componentes da controladora

Assinaturas IDS

- debug wips sig enable

NAC

- debug nac events enable
- debug nac packets enable

OEAP

Comandos show do controlador

- show ap join stats detail <adição de Mac AP Cisco>
- show ap link-encryption <AP Cisco | tudo>
- show ap data-plane <Cisco AP | tudo>

Apresentação/depurações do AP

- show logging
- show lwapp/capwap client rcb
- show lwapp/capwap client config
- test lwapp/capwap iapp-data-echo
- debug lwapp/capwap iapp-data-echo
- show lwapp/capwap reap
- show controller

Classificação de invasor baseada em regras

Depurações a serem coletadas

- debug dot11 rogue rule enable

Capturas a serem feitas

Não aplicável.

Configuração e Mostrar Saída a Serem Coletadas

- show rogue rule summary
- show rogue rule detailed <rule_name>
- show rogue ap detailed <endereço MAC> (se um rogue específico for classificado incorretamente)

Depurações a serem coletadas

- debug dot11 rogue enable

Capturas a serem feitas

Rastreamento de Airoppeek no canal invasor.

Observação: fique atento aos quadros desassociados.

Configuração e Mostrar Saída a Serem Coletadas

- `show rogue ap detailed <rogue MAC addr>`
- `show ap config 802.11b/a <nome-ap do comando anterior>`

Assinatura IDS

Verifique se há um servidor DHCP configurado na rede para o AP invasor usar se o endereçamento IP estático for usado.

Depurações a serem coletadas

- `debug wips sig enable`

Capturas a serem feitas

Detectada captura Airoppeek na assinatura do canal.

Depurar e mostrar saída a ser coletada

No software anterior à versão 5.2, o LWAPP pode ser usado no lugar do CAPWAP para estes comandos:

- `show capwap ids sig dump` - Despeja assinaturas e contagens de ocorrências de detecção de assinatura que incluem o endereço MAC com as maiores ocorrências. Também inclui o status atual do rastreamento de pacote IDS.
- `show capwap ids rogue containment`

chan

- Exibe a lista atual de solicitações de Contenção de Invasor neste AP. As solicitações de contenção são agrupadas por canal.

- `show capwap ids rogue containment`

rad

- Exibe a lista atual de solicitações de Contenção de Invasor neste AP. Essa lista corresponde à lista de solicitações recebidas da controladora.

- `debug capwap ids sig` - Ativa depurações para Detecção de Contenção e Assinatura IDS.
- `t est capwap ids trace match`
 - Rastreia todos os pacotes recebidos pelo Módulo de Detecção de Assinatura IDS da mensagem `type=<message type-name>; <message type-name> = FF` para rastrear todos os tipos de mensagem. As depurações de assinatura na seção 8.2.1 precisam ser ativadas para que os pacotes rastreados sejam exibidos.

- test capwap ids trace rev
 - Rastreia todos os pacotes que correspondem a qualquer assinatura atualmente instalada para o Módulo de Detecção de Assinatura IDS de tipo de mensagem=<nome-tipo-de-mensagem>; <nome-tipo-de-mensagem> = FF para rastrear todos os tipos de mensagem que correspondem a uma assinatura. As depurações de assinatura na seção 8.2.1 precisam ser ativadas para que os pacotes rastreados sejam exibidos.

RLDP

Depurações a serem coletadas

Na WLC:

- debug dot11 rldp enable

No AP:

- debug lwapp client mgmt

Capturas a serem feitas

Captura Airopeek no canal invasor.

Configuração e Mostrar Saída a Serem Coletadas

- config rogue ap rldp initiate <endereço MAC invasor>

Canal de diagnóstico

Depurações a serem coletadas

- debug client <client MAC addr>
- debug ccxdiag all enable

Capturas a serem feitas

Captura Airopeek no canal a partir do qual o AP é definido. É recomendável evitar a filtragem, pois os pacotes beacon e req/resp de sondagem podem ser perdidos.

Configuração e Mostrar Saída a Serem Coletadas

- show sysinfo
- show wlan <WLAN id>
- show run-config
- show tech-support
- show debug
- show msglog
- show client summary

- show client detail <endereço MAC>

Detalhes do cliente

- Hardware do cliente
- Detalhes do software solicitante, como versão do software, nome do software (por exemplo, Aironet Desktop Utility [ADU] ou Odyssey) e versão do driver no caso do ADU
- Sistema Operacional do Cliente

Mobilidade entre controladores

Depurações a serem coletadas

- debug client <MAC addr> em ambas as WLCs
- debug mobility handoff enable nas duas WLCs (Lembre-se da ordem e sempre ative o cliente de depuração primeiro)
- debug pem state enable
- Se o caminho de controle de mobilidade ou os dados ativos estiverem inativos, ative debug mobility keepalive enable em ambos os dispositivos (lembre-se da versão do software em ambos os controladores).
- Se o Address Resolution Protocol (ARP) não funcionar, ative debug arp all enable em ambos os dispositivos.
- Se o DHCP não funcionar, ative debug dhcp message enable e debug dhcp packet enable em ambos os dispositivos.
- Se o cliente se conectar após um tempo, rastreie quanto tempo ele levou.

Capturas a serem feitas

Capturar pelo tipo de roaming, como CCKM, PMKID ou TGR.

Configuração e Mostrar Saída a Serem Coletadas

O mesmo que o [problema de conexão do cliente](#) e também estes:

- show pmk-cache <MAC addr> no controlador de destino
- show client detail <endereço MAC> quando o cliente está conectado ao AP antigo
- show mobility summary em ambas as WLCs

Detalhes do cliente

Igual ao tipo de roaming particular, como CCKM, PMKID ou TGR.

AP Honeypot

Depurações a serem coletadas

Não aplicável.

Capturas a serem feitas

Capture o rastreamento Airopeek no canal em que a interceptação é recebida para confirmar se o invasor usa o SSID da Cisco.

Configuração e Mostrar Saída a Serem Coletadas

- show traplog

Integração com AirMagnet

Depurações a serem coletadas

Na WLC para problemas relacionados ao NMSP:

- debug wips nmsp enable
- debug wips event enable
- debug wips error enable

Para problemas relacionados ao CAPWAP:

- debug wips event enable
- debug wips error enable
- debug iapp error enable

Para informações de relatório de alarme/dispositivo corrompido:

- debug wips all enable

No AP:

- debug capwap am event
- debug capwap am error

Capturas a serem feitas

- Captura Airopeek do ataque
- Captura etérea dos relatórios (enviados como pacote de dados)

Configuração e Mostrar Saída a Serem Coletadas

No AP:

- show capwap am stats
- show capwap am buffer [execute-o algumas vezes]
- show capwap am policy [alarm-id]
- show capwap am alarm [alarm-id]

Autenticação Local

Itens a verificar antes de registrar um bug

Verifique se o cliente pode se associar à WLAN. Se o cliente não puder, o problema está no nível dot1x. Se os certificados forem usados, verifique se há dispositivos e certificados CA instalados na WLC. Além disso, verifique se você selecionou o emissor de certificado correto na configuração de autenticação local para selecionar o conjunto correto de certificados na WLC.

Se o banco de dados local for usado para credenciais de usuário, verifique se o nome de usuário existe no banco de dados. Se o Lightweight Directory Access Protocol (LDAP) for usado, consulte a seção [debugging LDAP](#) para obter mais informações sobre depuração.

Depurações a serem coletadas

WLC:

- debug aaa local-auth eap framework errors enable
- debug aaa local-auth eap method errors enable
- debug aaa local-auth eap method events enable
- debug aaa local-auth eap method sm enable
- debug aaa local-auth db enable
- debug aaa local-auth shim enable

Configuração e Mostrar Saída a Serem Coletadas

- show local-auth config
- show local-auth statistics
- show local-auth certificates (quando um método EAP [Extensible Authentication Protocol] com certificados é usado)

Detalhes do cliente

O tipo de cliente, mais os detalhes de configuração de EAP que mostram qual método está selecionado e quais parâmetros estão definidos para esse método no cliente. Além disso, o texto de qualquer mensagem de erro vista no cliente.

Depuração do controlador

- debug pm pki enable “ Detalhes sobre a validação do certificado.
- debug aaa events enable “ Isso ajuda se houver qualquer problema relacionado à lista de autorização.
- show certificate lsc summary “ Para qualquer resumo relacionado ao LSC.

Autenticação geral de AAA

Estas depurações são úteis para a depuração de problemas de autenticação, autorização ou conta RADIUS:

Depurações a serem coletadas

- debug client <endereço MAC> – Fornece informações sobre como os atributos relacionados à reautenticação, como session-timeout e action-type, são aplicados.
- debug aaa events enable – Ajuda a solucionar problemas de como diferentes servidores AAA são usados para autenticação, autorização e conta.
- debug aaa packet enable – Ajuda a identificar e solucionar problemas de diferentes atributos AAA que são recebidos e aplicados.

Capturas a serem feitas

Uma captura com fio pode ser coletada entre o controlador e o servidor RADIUS se as depurações anteriores não indicarem o problema.

Configuração e Mostrar Saída a Serem Coletadas

O mesmo que o [problema de conexão do cliente](#) e também isto:

- show radius summary

Detalhes do cliente

O mesmo que o [problema de conexão do cliente](#).

TACACS+

Depurações a serem coletadas

- debug aaa tacacs enable – Na WLC, colete o registro no servidor ACS/RADIUS para a conta
- debug aaa events enable
- debug aaa detail enable
- debug dot11 mobile enable
- debug dot11 state enable
- debug pem events enable
- debug pem state enable

Capturas a serem feitas

- Uma captura com fio pode ser coletada entre o controlador e o servidor RADIUS se as depurações anteriores não indicarem o problema.

Configuração e Mostrar Saída a Serem Coletadas

- show tacacs summary
- Problema de Alteração de Autorização (CoA - Change of Authorization) e Pacote de Desconexão (PD

- Packet of Disconnect) - RFC 3576

- show radius summary

LDAP

Itens a verificar antes de registrar um bug

Certifique-se de que o servidor LDAP possa receber ping do WLC.

Se você usar o Active Directory e a autenticação EAP local, estes métodos EAP não serão suportados:

- LEAP
- EAP-FAST MSCHAPv2
- PEAP MSCHAPv2

Isso ocorre porque o Active Directory não pode retornar uma senha de texto não criptografado que possa ser usada para a autenticação MSCHAPv2.

Depurações a serem coletadas

- debug aaa ldap enable

Se o problema ocorrer quando você usar o LDAP com autenticação local, consulte a seção [Autenticação local](#) para obter mais depurações.

Configuração e Mostrar Saída a Serem Coletadas

- show ldap summary
- show ldap <server index>
- show ldap statistics
- show local-auth statistics (se o problema ocorrer quando usado com LDAP com autenticação EAP local)

Proteção de Quadro de Gerenciamento de Cliente (MFP - Client Management Frame Protection)

Para todos os problemas

- debug wps mfp client enable
- show wps mfp summary

Configuração e Mostrar Saída a Serem Coletadas

- show wps mfp statistics

Problemas de configuração

Depurações do controlador:

- debug wps mfp capwap enable

O cliente não associa

Depurações do controlador:

- debug wps mfp client enable
- debug wps mfp detail enable
- debug pem state enable
- debug pem events enable
- debug dot1x events enable

Saída de configuração e exibição a ser coletada:

- show msglog
- show client detail <endereço MAC>

Depurações adicionais de AP 1130/1240 quando o cliente não se associa

- debug dot11 mgmt msg
- debug dot11 aaa manager all (para o modo autônomo H-REAP)

Depurações de AP Aironet quando o cliente não se associa no modo autônomo H-REAP

- debug dot11 mfp client
- debug dot11 mgmt msg
- debug dot11 mgmt interface
- debug dot11 mgmt station
- debug dot11 supp-sm-dot1x
- debug dot11 aaa manager all
- debug dot11 wpa-cckm-km-dot1x

Mobilidade

Depurações do controlador

- debug wps mfp mm enable
- debug mobility directory enable

Configuração e Mostrar Saída a Serem Coletadas

- show mobility summary
- show mobility statistics

Relatar Problemas

Depurações do controlador

- debug wps mfp report enable

Configuração e Mostrar Saída a Serem Coletadas

- show wps mfp statistics

Observação: isso deve ser chamado imediatamente após a geração de erros.

Problemas relacionados ao FIPS

Quando a controladora é colocada no modo FIPS (Federal Information Processing Standard), somente funções criptográficas aprovadas podem ser usadas. Como resultado, você deve bloquear o SSL para usar o algoritmo de autenticação TLS_RSA com cifra AES.

Não é possível entrar no menu de inicialização

Este é um recurso do FIPS. O recurso é ativado com este comando:

- config switchconfig boot-break disable

Não é possível fazer download da nova imagem

- Este é um recurso do FIPS. A transferência é desativada quando a quebra de inicialização é desativada.

O cliente sem fio usa autenticador local com EAP-TLS, EAP-FAST e PEAP

Depurações a serem coletadas

Com base na comunicação em problema, estas depurações podem ser habilitadas:

- debug wps cids enable
- debug aaa local-auth eap method events enable

Capturas a serem feitas

O farejador de rastreamento entre a WLC e o dispositivo com o problema.

Observação: a WLC pode iniciar a comunicação assim que o serviço relevante for iniciado. Recomenda-se iniciar o farejador antes que a WLC seja ligada.

Configuração e Mostrar Saída a Serem Coletadas

- show switchconfig

512 grupos de WLANs/AP

512 WLANs

Um problema de WLANs 512 é se o cliente pode se conectar a um AP de "grupo padrão", mas não pode se conectar a um AP definido para um grupo AP personalizado.

Mostrar saída a ser coletada no controlador:

- show sysinfo
- show running-config
- show wlan summary
- show wlan apgroup
- show msglog

Mostrar saída a ser coletada no AP:

- show controller
- show capwap client mn
- show log

Depurações a serem coletadas:

- debug client <MAC addr>
- debug group enable
- debug capwap events enable

Observação: essas depurações ou qualquer outra depuração devem ser ativadas após o comando `debug client`

é usado. Esse comando faz com que todas as depurações anteriores sejam desativadas.

Rastrear para Coletar:

- rastreamento sem fio

Grupos AP

Quaisquer problemas relacionados à adição ou exclusão do grupo AP ou à adição de uma interface ao grupo AP.

Mostrar saída a ser coletada:

- show sysinfo
- show running-config
- show wlan summary
- show wlan apgroup

- show msglog

Depurações a serem coletadas:

- debug group enable

ACLs, ACLs de pré-autenticação e ACLs de CPU

<#root>

>

show acl ?

summary	Display a summary of the Access Control Lists.
detailed	Display detailed Access Control List information.
cpu	Display CPU Acl Information

DHCP

Depurar DHCP In-Band

- debug dhcp message enable
- debug dhcp packet enable

Debug DHCP for the Service-Port Enable

- debug dhcp service-port enable

Problemas relacionados ao acesso de convidados

WLAN de convidado

- debug mobility handoff enable
- debug pem events enable
- debug pem state enable

Para problemas de DHCP:

- debug dhcp packet enable
- debug dhcp message enable

Para problemas de conexão móvel:

- debug dot11 events enable
- debug dot11 mobile enable

Para problemas de RADIUS/AAA:

- debug dot1x aaa enable

Problemas de alta disponibilidade da WLC

Failover de AP

Problema de configuração

Colete e examine estes arquivos de configuração:

Todos os arquivos de configuração da WLC relacionados a show run-config e show running-config.

A prioridade de failover do AP está configurada?

Por WLC primária de AP ("Primary Cisco Switch [Nome | Endereço IP]" em "Config. AP")

Por WLC secundária de AP ("switch Cisco secundário [Nome | Endereço IP]" em "Config. AP")

Por WLC terciária AP ("Switch Cisco terciário [Nome | Endereço IP]" em "Config. AP")

Os parâmetros de configuração do AP correspondentes na WLC a show ap config <AP name>.

Os únicos modos de AP suportados para batimento rápido são o local e o h-reap (campo "AP Mode").

Os parâmetros de configuração de AP correspondentes no AP a show capwap client config.

Failover para WLC inesperado

- show sysinfo a O número máximo de APs suportados pelo WLC esperado.
- show ap summary a APs que ingressaram na WLC esperada.
- show capwap client ha a Se o heartbeat rápido estiver habilitado, examine a lista de backup no AP.

Problema de transporte

Se o DHCP estiver habilitado para a interface Ethernet do AP, ele buscou um endereço IP? Use show interface FastEthernet0.

- ping <IP address> a Decide se o AP e a WLC podem fazer ping entre si.

Protocolos CAPWAP

Comandos de depuração comuns de WLC e AP:

- Debug CAPWAP events and state a debug capwap events enable/disable
- Debug CAPWAP errors a debug capwap errors enable/disable
- Debug CAPWAP details a debug capwap detail enable/disable
- Debug CAPWAP info a debug capwap info message enable/disable
- Debug CAPWAP payload a debug capwap payload enable/disable
- Debug CAPWAP hexdump a debug capwap hexdump enable/disable

Comando de depuração específico do AP fast-heartbeat:

- Debug fast-heartbeat “ show capwap client ha

Observação: às vezes, você precisa da saída do analisador de rede (como o Wireshark).

Prioridade de AP

Decida se a prioridade de AP está habilitada “show run-conf ("AP Join Priority" campo em "Network Information")

Decidir o número máximo de APs suportados pela WLC “show sysinfo ("Maximum number of AP supported")

Decida quantos APs ingressaram na WLC - show ap summary

Examine a prioridade de junção de cada AP “show ap summary (última coluna)

Problemas de transportador e CAPWAP

Consulte as sessões correspondentes na seção [Failover do AP](#).

- show tech-support
- show run-config
- show running-config
- show ap config general <Cisco AP name>
- show capwap client config

Problemas relacionados ao H-REAP do controlador

H-REAP

Depurações do controlador:

- debug client <MAC addr>

Depurações de AP:

- debug lwapp reap mgmt
- debug dot11 mgmt msg
- debug dot11 mgmt int

Problemas do CCKM H-REAP

Depurações do controlador:

- debug cckm detailed enable

AP Show/Debugs:

- debug lwapp reap mgmt

- debug dot11 aaa manager key
- debug lwapp reap cckm
- debug dot11 mgmt msg
- show lwapp reap cckm

RADIUS local H-REAP

Depurações do controlador:

- debug hreap group
- debug hreap aaa

AP/Mostrar depurações:

- debug lwapp reap
- debug lwapp client config
- show run

Fluxo de mídia

- debug media-stream [admissão/config/erros/evento/rrc] [ativar/desativar]
- debug bcast igmp enable – Mensagens de solicitação/relatório de junção IGMP de cliente.

Admissão – Depurações de admissão de cliente que são úteis ao depurar problemas de negação/exclusão de cliente.

Evento – Despeja atualizações de clientes diretas de IGMP / Mídia.

RRC – Atualizações da máquina de estado RRC.

Problemas relacionados ao local

```
<#root>
```

```
>
```

```
show location ?
```

ap-detect	Display devices detected by specified AP
detail	Display detailed location information.
plm	Display Location's Path Loss Measurement(CCX S60) Configuration
statistics	Display Location Based System statistics.
summary	Display Location Based System summary information.

Memória do sistema, problemas de memória insuficiente

Configuração e Mostrar Saída a Serem Coletadas

- show memory statistics
- show buffers
- show process memory

Observação: se a `config memory monitor errors flag` está definido como `disable`, os detalhes de corrupção de memória podem ser carregados com estes comandos:

- log de erros de tipo de dados de upload de transferência
- transfer upload filename memerrors.txt
- início do upload de transferência

Problemas relacionados à malha

Há vários pontos de falha:

- Controlador
- APs de malha
- GUI/WLC

Diretrizes gerais

Localize o ponto de falha e isole o componente com falha.

Correlacione rastreamentos do controlador, APs em malha e também saída visual na CLI/GUI/WLC para encontrar o ponto de falha.

No caso de problemas relacionados a pacotes, colete rastros Airopeek ou etéreos para confirmar a análise preliminar.

Analise o motivo da falha e como o problema pode ser reproduzido.

Configuração

Ação de disparo

Diretrizes gerais

Esta seção tem o objetivo de fornecer ponteiros suficientes para depurar um bug de malha e coletar informações relevantes para ajudar a entender o comportamento com mais eficiência. Dado que pode ser impossível apontar um bug à primeira vista, este documento é um conjunto de sugestões para o DT e não um livro de regras. O DT usa discrição para anexar depurações relevantes a fim de ajudar a estudar eficientemente e resolver o bug o mais rápido possível.

Pacotes Suspeitos Faltam

Coletar traços Ethereal e Airopeek.

Conjuntos de Comandos de Depuração

Este é um conjunto de debug comandos que podem ser usados para obter informações sobre o sistema.

General Show CLI:

- show version
- show capwap client rcb
- show mesh status
- show mesh module adjacency
- show mesh channel [current]

Testar CLI da malha:

- testar adjacência de malha para comandos de teste de adjacência de malha
- ferramentas de teste de malha para ferramentas MESH Anti-strand
- test mesh awpp para comandos de teste do AWPP de malha
- test mesh disable para desativar um recurso
- test mesh enable para ativar um recurso
- test mesh forwarding para comandos de teste de encaminhamento de malha
- test mesh linktest para o teste de enlace de malha
- test mesh mperf para a ferramenta de teste MESH BW

Questões específicas

- qualquer problema de conexão de link
- debug mesh link
- show mesh adjacency (filho/pai/todos)

Rádio:

- show controller d0, d1, ... (para todos os problemas relacionados ao Rádio)
- Traços do ar (entre os nós afetados)

Problemas de interface (relacionados ao tráfego de dados):

- show int d0, d1, G0, G1, ...

A Ethernet rastreia entre o controlador e o ponto de acesso no telhado (RAP)

Transmissão:

- show mesh forwarding table
- debug mesh forwarding [tabela/pacote]

- show mesh forwarding links
- show mesh forwarding port-state
- debug mesh forwarding port-filter

Endereço IP/DHCP:

- debug ip address
- show ip int bri
- show int bvi1
- show run int bvi 1
- show mesh forwarding port-state
- test mesh desativa o filtro de porta e executa ping no roteador

Tráfego IP e DHCP:

- debug ip udp
- debug ip icmp
- debug dhcp [detail]

Listagem de Exclusão:

- debug mesh adjacency exclude “” Monitora eventos que excluem país.
- test mesh adjacency exclude clear “” Limpe os contadores da lista de exclusão atual e inicie novamente.

Máquina de Estado de Adjacência:

- debug mesh adjacency event
- debug mesh adjacency state
- debug mesh adjacency timer

Comunicação de adjacência:

- debug mesh adjacency packet
- mensagem debug mesh adjacency

Problemas de link de adjacência:

- debug mesh adjacency channel
- debug mesh adjacency neighbor
- debug mesh adjacency parent

Alterações na razão sinal/ruído (SNR):

- debug mesh adjacency snr

Seleção de frequência dinâmica (DFS):

- debug mesh adjacency dfs

A ligação de grupo de trabalho (WGB) não associa:

Colete depurações de clientes no controlador e no AP.

Colete rastreamentos de farejador Airopeek entre o WGB e o AP Mesh pai.

O cliente com fio por trás do WGB não pode transmitir tráfego.

Obter o estado do WGB pai no controlador.

Colete depurações no controlador, Mesh AP e WGB.

Colete rastreamentos Ethereal entre o AP de Malha pai e o controlador.

AP não pode ser associado:

- Coletar mensagem de depuração no controlador:
- debug capwap errors enable
- debug capwap events enable

Coletar mensagem de depuração no AP:

- debug capwap client event
- debug capwap client error

Para obter mais informações, use estas depurações adicionais:

Depurações do controlador:

- debug capwap detail enable
- debug capwap info enable
- debug capwap payload enable
- debug capwap hexdump enable

Depurações de AP:

- debug capwap client config
- debug capwap client detail
- debug capwap client fwd
- debug capwap client hexdump

- debug capwap client info
- debug capwap client payload
- debug capwap client reassembly

Comandos show:

- show capwap client rcbâ€™’mostra a configuração do bloco de controle de rádio
- show capwap client configâ€™’mostra a configuração de rádio da nvram

Comandos de Teste:

- reinicialização de lwapp de malha de teste
- test mesh mode bridge/local
- test mesh role rap/map
- malha de teste bgn xxxx
- test lwapp console cli
- test lwapp controller ip

Ferramentas Anti-Transformação:

Comandos AP

<#root>

debug mesh astools

event -- Event debugs
level -- Level of detail in debugs
packet -- packet related debugs
timer -- timer debugs

Controlador

- debug mesh astools troubleshoot <endereço MAC> â€™’ O endereço MAC de rádio b/g do AP retido

APs - Nenhum Beacon é Ouvido

Verifique se há pelo menos um AP adjacente que se juntou ao controlador e pode ouvir o AP retido.

Mostre a cont d0 para determinar o canal atual de rádios 11b que operam.

Colete todas as depurações possíveis que sejam relevantes.

Ferramenta de medição de largura de banda Mperf:

- comandos show

<#root>

show mesh mperf ?

globals --- Print configuration used to spawn objects
print [all/id] --- Print active connections

- Comandos debug

<#root>

debug mesh mperf ?

bwreport -- Bandwidth output reports
fds -- Multiple connection state machine multiplexing
general -- All general debugs
jitter -- Jitter calculations
sockdata -- Socket data RX and TX
timer -- Timer related

Problemas com o cliente NTP e a configuração de tempo no controlador

- debug ntp packet enable
- debug ntp low enable
- debug ntp detail enable
- show time

Captura etérea na porta de gerenciamento do controlador.

Problemas de componentes de RF para as WLCs

<#root>

>

debug airewave-director ?

all	Configures debug of all Airewave Director logs
channel	Configures debug of Airewave Director channel assignment protocol
error	Configures debug of Airewave Director error logs
detail	Configures debug of Airewave Director detail logs
group	Configures debug of Airewave Director grouping protocol
manager	Configures debug of Airewave Director manager
message	Configures debug of Airewave Director messages
packet	Configures debug of Airewave Director packets
power	Configures debug of Airewave Director power assignment protocol
radar	Configures debug of Airewave Director radar detection/avoidance protocol
plm	Configures debug of CCX S60 Power Measurement Loss messages
rf-change	Configures logging of Airewave Director rf changes
profile	Configures logging of Airewave Director profile events

Componente SNMP para WLCs

```
<#root>
```

```
>
```

```
debug snmp ?
```

all	Configures debug of all SNMP messages.
agent	Configures debug of SNMP agent.
mib	Configures debug of SNMP MIB.
trap	Configures debug of SNMP traps.
engine	Configures debug of SNMP engine.

Anexe o comando do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) que falhou.

Se o WCS indicar que o SNMP falhou, tente executar o comando SNMP set/get a partir do MG-soft ou de qualquer outro gerenciador SNMP.

Verifique se funciona na interface do usuário ou na CLI da controladora.

Anexe uma captura de tela da interface de usuário da CLI/controladora.

Se houver vazamentos de memória ou problemas de CPU, mencione há quanto tempo o sistema está ativo.

Examine as depurações de SNMP para ver se algo está evidente.

- debug snmp mib enable OR debug snmp agent enable
- **debug snmp trap enable**

Anexar as depurações anteriores.

Problemas de upload/download de TFTP que incluem upgrade/downgrade

```
<#root>
```

```
>
```

```
debug transfer tftp ?
```

disable	Disables debug.
enable	Enables debug.

Componente Web GUI para WLCs

Mencione qual problema do navegador é visto.

Verifique se há algum problema com o script java. Se o Firefox for usado, verifique o console de erro.

Anexe uma captura de tela do erro de script java. O Internet Explorer exibe uma janela pop-up. Para o Firefox, anexe a janela do console de erro.

Se a configuração falhar, verifique com o CLI. Anexe a saída CLI.

Anexe a captura de tela ao bug.

Mencione a controladora e a plataforma AP.

Se houver uma falha na tarefa emweb, examine o rastreamento da pilha de falhas. Se o rastreamento de pilha indicar CLI, não use este componente.

WLC-Webauth-Template

Informações básicas

Determine a topologia da rede no momento em que o webauth foi executado.

É uma configuração de convidado ou associação normal em uma única WLC ou após a realização de webauth de roam?

Que tipo de webauth está configurado (interno, externo, personalizado ou de passagem da Web)?

Qual é a página de login usada?

Faça o download do pacote webauth e forneça isso.

Você ativou o secure-web? Se sim, desabilite e veja se webauth funciona.

Comandos show:

- show client detail <endereço MAC>
- show wlan <WLAN id>
- show rules
- show custom-web all

Debug

- debug mobility handoff enable

Observação: execute esta depuração se webauth não funcionar após roaming.

Sniffers

Porta DS da WLC – Isso é útil para um problema de autenticação RADIUS.

Porta AP da WLC – se os pacotes http forem descartados entre a WLC e o AP

Pelo ar - se o AP descartar pacotes

Problemas e aprimoramentos relacionados à configuração XML do controlador

Validação de XML

Mensagens de erro de validação de XML, como `Validation for node ptr_apfCfgData.apfVAPIDData.apfVapSecurity.<qualquer dado de configuração>`, são observadas durante a inicialização do sistema.

toda a mensagem de erro de validação de XML

o procedimento CLI ou GUI para configurar as WLANs antes da inicialização do sistema

o arquivo de configuração CLI ou XML gerado e salvo no TFTP antes da inicialização do sistema

- `show invalid-config`

Canal de diagnóstico

- `debug client <MAC addr>`
- `debug ccxdiag all enable`

Alocação de canal dinâmico

- `debug airwave-diretor channel enable`
- `debug airwave-diretor radar enable`

TACACS+

- `debug aaa tacacs enable`
- `show tacacs summary`

WLC-Multicast-Guide

Informações básicas

Topologia da rede

Verifique se o endereço de fluxo multicast não é o endereço reservado IANA para o aplicativo que está em uso.

Endereços multicast usados

A taxa de fluxo multicast e o tamanho do pacote

Certifique-se de que o endereço multicast do grupo AP configurado não seja o mesmo que o endereço multicast de fluxo.

O modelo WLC (2106, 4404, 4402, WiSM...)

O modelo AP (1131, 1232, 1242, 1250...)

Rádio usado pelo cliente

Endereço MAC do cliente

Informações de WLC (todos os tipos)

Despejos de:

- show interface summary
- debug bcast all enable
- show network summary
- show network multicast mgid summary
- show network multicast mgid detail <mgid>
- Para a versão G e posterior: show wlan apgroups
- Para TALWAR/2106 com novo código FP:
 - Se o rastreamento de IGMP estiver habilitado, debug fastpath cfgtool â€”mcast4db.dump debug fastpath cfgtool â€”mcast2db.dump
 - Se a espionagem de IGMP estiver desativada, debug fastpath cfgtool â€”mcast2db.dump
 - Se Multicast-Unicast estiver habilitado, debug fastpath cfgtool â€”mcastrgdb.dump

Informações AP (todos os tipos)

Despejos de:

- show lwapp mcast
- show lwapp mcast mgid all
- show lwapp mcast mgid id <mgid>
- show lwapp client traffic - quatro vezes com intervalo de 1 minuto

Depurações de rádio:

1. A taxa de saturação da Ethernet
2. A taxa de transmissão de rádio
3. A taxa de descarte de rádio
4. O modo de economia de energia do conjunto de serviços básicos (BSS)
5. A taxa total de Ethernet RX
6. A taxa RX multicast Ethernet

Por #1, execute o comando `show int g0 | inc overrun` periodicamente.

Para #2, #3 e #4, execute o comando `show cont d0 | beg queues` periodicamente. Examine as contagens de envio/descarte para cada fila.

Além disso, por #3, execute o comando `show int d0 | inc output drop` periodicamente.

Por #5, execute o comando `show cont g0 | inc RX count` periodicamente.

Por #6, execute o comando `show cont g0 | inc multicast` periodicamente. A primeira linha mostra o multicast/broadcast RX.

Para obter as taxas de pacotes, execute um comando a cada 10 segundos e divida a diferença por 10. Se muitos pacotes forem enviados na fila Mcast (para um BSS), o BSS estará no modo de economia de energia. A taxa máxima de pacotes multicast para um BSS com economia de energia é relativamente baixa. Trata-se de um problema bem conhecido.

Informações do Switch

Verifique a versão do switch com o comando `show version` comando. O switch pode ter a versão "base ip avançada" (por exemplo, Cisco IOS® Software, C3750 Software [C3750-ADVIPSERVICESK9-M], Versão 12.2(40)SE, RELEASE SOFTWARE (fc3). [imagem: c3750-advipservicesk9-mz.122-40.SE.bin]). A versão "ip base" tem um problema no roteamento do tráfego multicast entre VLANs.

Algumas depurações:

- Verifique se o roteamento multicast está ativado. ("show run" pode incluir "ip multicast-routing distributed")
- Verifique se a configuração "ip pim sparse-dense-mode" foi adicionada à VLAN configurada.
- `show ip igmp group`

Capturas do farejador

- Interface DS da WLAN
- Interface de gerenciamento do WLC
- Ap-Mgr ao qual o AP está conectado (necessário apenas quando mcast src é sem fio)
- Eth interface do AP
- No ar

Análise de Capturas de Farejador

A origem do multicast é o lado com fio

- Verifique se os pacotes chegam à WLC na interface DS.
- Verifique se o pacote multicast encapsulado do LWAPP foi enviado na interface de gerenciamento. O pacote deve ter:
 - endereço ip dst externo = endereço multicast do grupo ap configurado
 - porta udp dst = 12224
- Verifique se o pacote visto em 'b' é visto no eth intf do AP.
- Verifique se o pacote de fluxo mcast é visto no ar.

A origem do multicast é o lado sem fio

- Verifique se os pacotes encapsulados do LWAPP são recebidos no ap-mgr intf. Aqui, o LWAPP é

unicast.

- Verifique se um pacote multicast é enviado do DS intf.
- Verifique se o pacote multicast encapsulado do LWAPP foi enviado na interface de gerenciamento. O pacote deve ter:
 - endereço ip dst externo = endereço multicast do grupo ap configurado
 - porta udp dst = 12224
- Verifique se o pacote visto em 'b' é visto no eth intf do AP.
- Verifique se o pacote de fluxo mcast é visto no ar.

Verificação da configuração do switch para WiSM

- Quando você usar um Wireless Services Module (WiSM), verifique se o mesmo problema foi mencionado na seção após este.
- ID de bug da Cisco [CSCsj48453](#) – O CAT6k não encaminha o tráfego multicast para o WiSM no modo L3.
- Sintoma – O tráfego multicast não flui de um host com fio para um host sem fio através da placa WiSM no modo L3, por exemplo, quando ambos os hosts estão em VLANs diferentes. Somente o primeiro pacote é atingido com êxito. Depois disso, o tráfego para.
- Condições – O tráfego pára apenas quando o modo de replicação multicast é saída.
- Solução alternativa – uma solução alternativa é alterar o modo de replicação multicast para entrar com o `mls ip multicast replication-mode ingress` comando. O tráfego flui corretamente no modo de entrada. Verificar se ele usa o mesmo `show mls ip multicast capability` comando.

Descrição adicional do problema – O problema é visto com CAT6k e um WiSM. O tráfego multicast flui do host sem fio para o host com fio funciona bem, mesmo em L3. Além disso, o tráfego multicast flui do host com fio para o host sem fio através da placa WiSM funciona bem no modo L2.

WLC-QoS-Guide

Mínimo de depurações

Obtenha o `show run-config` de todos os dispositivos no grupo de mobilidade.

Quando o problema ocorrer, capture estas depurações:

- `debug aaa all enable`
- `debug pem state enable`
- `debug pem events enable`
- `debug mobility handoff enable`
- `debug dot11 mobile enable`
- `debug dot11 state enable`

Obtenha um rastro do AiropEEK ou do AirMagnet próximo ao AP/telefone/aparelho telefônico problemático.

Obtenha uma captura Ethereal ou Etherpeek da porta DS do switch, do switch upstream do AP e das SVPs

(Prioridades de Voz) do SpectraLink.

Depuração de controle de chamada (classificação SIP)

Perguntas

É um cliente do Protocolo de Iniciação de Sessão (SIP - Session Initiation Protocol)?

Que servidor IP PBX\sip é usado?

Ele mostra que está registrado em um determinado servidor SIP?

O 7921 funciona como esperado e apenas os clientes SIP têm um problema?

Informações de WLC

- show wlan summary [wlan #]
- debug call-control all
- debug call-control events
- show call-control errors
- show call-control calls

Informações AP

- debug dot11 cc details
- debug dot11 cc errors
- debug dot11 cc events
- show lwapp client call-info mac (endereço MAC do cliente em questão)

Controle de admissão baseado em carga e métricas de voz

Perguntas a responder

Isso acontece com os rádios "a" e "b"?

Qual é o valor de utilização do canal quando a chamada é rejeitada?

Isso ocorre apenas com telefones 7921 ou com outros telefones também? Em caso afirmativo, quais são os telefones? Caso contrário, isso pode ser tentado em outro telefone TSPEC?

Isso ocorre com APs 11n ou regulares?

Você usa a mobilidade entre controladores?

O telefone TSPEC é compatível?

Ele faz o UAPSD?

Isso pode ser reproduzido nas plataformas 2006 ou 4100?

É um ambiente de sala blindada?

Houve uma condição especial para a qual a chamada foi rejeitada?

Comandos debug e show na WLC para LBCAC

- debug cac all enable
- show 802.11a/b/g
- show wlan <wlan id>
- show ap stats 802.11a/b/g <ap-name>
- show ap auto-rf 802.11a/b/g <ap-name>

Depurar o AP para LBCAC

- debug dot11 cac unit
- debug dot11 cac metrics
- debug dot11 cac events

Métricas de voz

Capturas pelo ar e farejador de fios

Verifique se o tráfego UP6 é gerado continuamente.

Certifique-se de que a WLAN tenha o perfil QoS correto e a política Wi-Fi Multimedia (WMM).

A maioria das perguntas feitas para LBCAC é aplicável para métricas de voz.

Depurações e comandos show na WLC para métricas de voz:

- show 802.11a/b/g o show wlan <wlan id>
- show ap stats 802.11a/b/g <ap-name>
- show ap stats 802.11a/b/g <ap-name> tsm
- show client tsm 802.11a/b/g <client-mac> <AP mac>
- debug iapp packet enable o debug iapp error enable
- debug iapp all enable o debug client <client mac>

Depurações no AP para métricas de voz:

- debug dot11 tsm
- debug lwapp client voice-metrics

WLC-License-Guide

Depurações a serem coletadas no controlador

- Saída do console
- msglog

Problemas do ARP

Depurações a serem coletadas no controlador

- debug arp all enable

Problemas de rede

Depurações a serem coletadas no controlador

- debug packet logging enable
- dump-low-level-debug

Problemas com o ponto de acesso

IAPP

- show wgb summary
- show wgb detail <wgb mac>

Problemas de associação WGB

- debug dot11 mobile enable
- debug dot11 state enable
- debug pem events enable
- debug pem state enable
- debug iapp all enable

O cliente com fio ou WGB não obtém o endereço DHCP

- debug dhcp packet enable
- debug dhcp message enable

O cliente com fio ou WGB usa endereço IP estático, mas o endereço IP não aparece no controlador

- debug dot11 mobile enable
- debug dot11 state enable

Senha do nome de usuário do AP

Depurações a serem coletadas no AP

- debug lwapp client config

Capturas a serem feitas

- Não aplicável.

Configuração e Mostrar Saída a Serem Coletadas

- config ap mgmtuser

Problemas de conexão do cliente

Depuração do cliente

- debug client <MAC addr>

O controlador não gosta da solicitação de associação

Captura do pacote

Captura Airopeek no canal a partir do qual o AP é definido. É recomendável evitar a filtragem, pois os pacotes beacon e probe req/resp podem ser perdidos. Não se esqueça de capturar o evento quando a conexão for encerrada.

Caso o cliente não se conecte, capture o evento inteiro da solicitação de teste até que a sessão seja encerrada (por exemplo, deauth é enviada e resposta de associação com código de status não 0).

Forneça os endereços MAC do cliente e do AP.

Observação: o MACi do AP é o MAC de rádio base + WLAN-ID.

Saída de configuração e exibição a ser coletada no controlador

- show sysinfo “Detalhes da versão do WLC
- show wlan x “na WLC para a WLAN afetada
- show run-config “of WLC
- show debug
- show msglog
- show tech-support “de WLC (bom de ter, mas não necessário)

Detalhes do cliente

Hardware cliente “Detalhes do software solicitante, como versão e nome do software (por exemplo, ADU ou Odyssey).

SO cliente “Se for Windows, forneça a configuração do sistema cliente, vá para **Programas > Acessórios > Ferramentas do Sistema > Informações do Sistema**.

Detalhes do servidor RADIUS

Forneça o tipo de servidor RADIUS (SBR, Cisco ACS, Linux e assim por diante) e a configuração, se aplicável.

O cliente não responde às solicitações EAP

Consulte a seção [O controlador não gosta da solicitação de associação](#).

A autenticação EAP não é realizada

Consulte a seção [O controlador não gosta da solicitação de associação](#).

Falha na Solicitação DHCP do Cliente

Consulte a seção [O controlador não gosta da solicitação de associação](#).

O EAPOL Exchange não é aprovado

Consulte a seção [O controlador não gosta da solicitação de associação](#).

O CCKM em roaming falha

Depurações a serem coletadas

A maioria das depurações é a mesma da seção anterior, [Problema de conexão do cliente](#). No entanto, essas novas depurações ajudam mais na depuração CCKM. Este comando debug está disponível a partir da versão 5.0 e mais recente:

- debug cckm enable
- show pmk-cache <client mac> “” no controlador de destino
- show client details <client mac> “” quando o cliente está conectado ao AP antigo
- debug cckm enable

Observação: essas depurações ou qualquer outra depuração devem ser ativadas após o problema debug client

. Isso ocorre porque o debug client

faz com que todas as depurações anteriores sejam desativadas.

Capturas a serem feitas

Certifique-se de capturar no canal onde o AP de destino está. Por exemplo, você deseja capturar todos os pacotes de gerenciamento entre o cliente e o AP de destino. Consulte a seção [O controlador não gosta da solicitação de associação](#) para obter mais informações.

Saída de configuração e exibição a ser coletada no controlador

Consulte a seção [Controller Does Not Like the Association Request](#) e emita estes comandos:

- show pmk-cache <client mac> “” no controlador de destino
- show client details <client mac> “” quando o cliente está conectado ao AP antigo

Detalhes do cliente

Consulte a seção [O controlador não gosta da solicitação de associação](#).

Falha no cache de PMKID

Verifique se o cliente oferece suporte ao cache de chave oportunista (OKC).

Observação: OKC não é o mesmo que cache de chave proativa (PKC) como especificado em 802.11I. A WLC suporta apenas OKC.

Capturas a serem feitas

Certifique-se de capturar no canal onde o AP de destino está. Por exemplo, você deseja capturar todos os pacotes de gerenciamento entre o cliente e o AP de destino.

Saída de configuração e exibição a ser coletada no controlador

Consulte a seção [O controlador não gosta da solicitação de associação](#) e emita estes comandos:

- `show pmk-cache <client mac>` no controlador de destino
- `show client details <client mac>` quando o cliente está conectado ao AP antigo

Problemas de reautenticação

Capturas a serem feitas

Não aplicável.

Saída de configuração e exibição a ser coletada no controlador

Consulte a seção [Controller Does Not Like the Association Request](#) e emita estes comandos:

- `show radius summary`
- `show client details <client mac>`
- `show pmk-cache <client mac>`

802.11R (Transição Rápida) Roaming Não Funciona

Depurações a serem coletadas

- `debug client <client mac>`
- `debug ft events enable`
- `debug ft keys enable`

Observação: essas depurações ou qualquer outra depuração devem ser ativadas depois que você emitir o comando **debug client <client mac>**. Isso ocorre porque o comando **debug client <mac>** faz com que todas as depurações anteriores sejam desabilitadas.

Capturas a serem feitas

Quando você percorre o ar, colete a captura Airopcap no canal onde o AP de destino está. Por exemplo, você deseja capturar todos os quadros de req/resp FT de 802.11 aut e req/resp de reassociação.

Quando você percorre o DS, colete a captura Airopcap no canal onde o AP de origem está. Por exemplo, se desejar capturar quadros de reassociação de requisição/resp. Você também deseja capturar a solicitação de FT/resp do quadro de ação no canal do AP de origem.

Observação: é recomendável manter os APs origem e destino no mesmo canal para depurar o problema de roaming do 802.11R. Isso permite capturar FT req/resp e reassociation req/resp em um único arquivo de captura.

Saída de configuração e exibição a ser coletada no controlador

Consulte a seção [Controller Does Not Like the Association Request](#) e emita estes comandos:

- `show pmk-cache <client mac>` no controlador de origem e de destino
- `show client details <client mac>`. Quando o cliente está conectado no AP antigo
- `show mobility summary` para obter o ID de domínio de mobilidade

Detalhes do cliente

Atualmente, somente o WGB é o cliente 802.11R conhecido.

Mobilidade entre controladores

Depurações a serem coletadas

- `debug client <client mac>` em ambas as WLCs
- `debug mobility handoff enable` nas duas WLCs (Lembre-se da ordem: sempre ative `debug client` primeiro.)
- `debug pem state enable`
- `Eping <ip>`
- `Mping <ip>`

Se o caminho de controle de mobilidade ou os dados ativos estiverem inativos, ative `debug mobility keepalive enable` em ambos os dispositivos (anote a versão do software em ambos os controladores).

Se o ARP não funcionar, ative `debug arp all enable` em ambos os dispositivos.

Se o DHCP não funcionar, ative `debug dhcp message enable` e `debug dhcp packet enable` em ambos os dispositivos.

Se o cliente se conectar após um tempo, rastreie quanto tempo ele levou.

Capturas a serem feitas

Capturar pelo tipo de roaming, como CCKM, PMKID ou TGR.

Configuração e Mostrar Saída a Serem Coletadas

Consulte a seção [Controller Does Not Like the Association Request](#) e emita estes comandos:

- `show pmk-cache <client mac>` no controlador de destino
- `show client details <client mac>` quando o cliente está conectado ao AP antigo
- `show mobility summary` em ambas as WLCs

Detalhes do cliente

Veja o tipo de roaming específico, como CCKM, PMKID ou TGR.

Desabilitar depurações

Para desativar todas as mensagens de depuração, use o comando `debug disable-all` comando.

Como alternativa, você pode desativar depurações específicas com o comando `debug` e a palavra-chave `disable`:

```
debug capwap events disable
```

Informações Relacionadas

- [Entender depurações sem fio e coleta de logs em controladores LAN sem fio Catalyst 9800](#)
- [Suporte técnico e downloads da Cisco](#)

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.