

Solucionar problemas de APs COS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Capturar Rastreamentos de Pacotes \(Rastreamentos de Farejador\)](#)

[PCAP com fio na porta AP](#)

[Procedimento](#)

[Opções de comando](#)

[PCAP com fio através do uso do filtro](#)

[Captura de rádio](#)

[Procedimento](#)

[Verificar](#)

[Outras opções](#)

[Controle o rastreamento do AP Client a partir do 9800 WLC](#)

[Pacote de depuração do cliente no AP](#)

[APs Catalyst 91xx em modo farejador](#)

[Dicas para Troubleshooting](#)

[MTU de Caminho](#)

[Para ativar depurações no momento da inicialização](#)

[Mecanismo de economia de energia](#)

[Clientes QoS](#)

[Verificação fora do canal](#)

[Conectividade do cliente](#)

[Cenários do Flexconnect](#)

[Sistema de arquivos AP](#)

[Armazenar e enviar syslogs](#)

[Pacote de suporte AP](#)

[Coletar arquivos centrais de AP remotamente](#)

[CLI AireOS](#)

[GUI do AireOS](#)

[CLI do Cisco IOS®](#)

[GUI do Cisco IOS®](#)

[IoT e Bluetooth](#)

[Conclusão](#)

Introdução

Este documento descreve algumas das ferramentas de solução de problemas disponíveis para APs que executam o sistema operacional COS (Cheetah OS, Click OS, simplesmente Cisco AP OS).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento concentra-se nos APs COS, como os modelos de APs das séries 2800, 3800, 1560 e 4800, bem como os novos APs 11ax Catalyst 91xx.

Este documento se concentra em muitos recursos disponíveis no AireOS 8.8 e posterior. E também o Cisco IOS® XE 16.12.2s e posterior.

Pode haver comentários sobre a disponibilidade de certos recursos em versões anteriores.

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.

Capturar Rastreamentos de Pacotes (Rastreamentos de Farejador)

PCAP com fio na porta AP

É possível (a partir do 8.7 com o filtro disponível no 8.8) tomar um pcap na porta Ethernet do AP. Você pode exibir o resultado ao vivo na CLI (apenas com detalhes resumidos do pacote) ou salvá-lo como um pcap completo na flash do AP.

O pcap com fio captura tudo no lado Ethernet (tanto Rx/Tx) e o ponto de toque dentro do AP é imediatamente antes do pacote ser colocado no fio.

No entanto, ele apenas captura o tráfego plano de CPU do AP, o que significa o tráfego de e para o AP (DHCP do AP, túnel de controle de capwap do AP, ...) e não mostra o tráfego do cliente.

Observe que o tamanho é muito limitado (limite de tamanho máximo de 5 MB), portanto, pode ser necessário configurar filtros para capturar apenas o tráfego no qual você está interessado.

Certifique-se de interromper a captura de tráfego com "no debug traffic wired ip capture" ou simplesmente "undebug all" antes de tentar copiá-la (caso contrário, a cópia não termina quando os pacotes ainda são gravados).

Procedimento

Etapa 1. Inicie o pcap; selecione o tipo de tráfego com "debug traffic wired ip capture":

```
<#root>
```

```
AP70DB.98E1.3DEC#debug traffic wired ip capture  
% Writing packets to "/tmp/pcap/
```

```
AP70DB.98E1.3DEC_capture.pcap0"
```

```
AP70DB.98E1.3DEC#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
```

Etapa 2. Aguarde até que o tráfego flua e, em seguida, pare a captura com o comando "no debug traffic wired ip capture" ou simplesmente "undebug all":

```
AP70DB.98E1.3DEC#no debug traffic wired ip capture
```

Etapa 3. Copie o arquivo para o servidor tftp/scp:

```
<#root>
```

```
AP70DB.98E1.3DEC#copy pcap
```

```
AP70DB.98E1.3DEC_capture.pcap0
```

```
tftp 192.168.1.100
```

```
#####  
AP70DB.98E1.3DEC#
```

Etapa 4. Agora você pode abrir o arquivo no Wireshark. O arquivo é pcap0. Altere para pcap de modo que ele se associe automaticamente ao wireshark.

Opções de comando

O comando debug traffic wired tem várias opções que podem ajudá-lo a capturar tráfego específico:

```
APC4F7.D54C.E77C#debug traffic wired  
<0-3>  wired debug interface number  
filter filter packets with tcpdump filter string  
ip      Enable wired ip traffic dump  
tcp     Enable wired tcp traffic dump  
udp     Enable wired udp traffic dum
```

Você pode adicionar "verbose" no final do comando debug para ver o dump hexadecimal do pacote. Esteja ciente de que isso pode sobrecarregar sua sessão de CLI muito rapidamente se o

filtro não for estreito o suficiente.

PCAP com fio através do uso do filtro

O formato do filtro corresponde ao formato do filtro de captura tcpdump.

	Exemplo de filtro	Descrição
Host	"host 192.168.2.5"	Isso filtra a captura de pacotes para coletar apenas pacotes que vão para ou vêm do host 192.168.2.5.
	"src host 192.168.2.5"	Isso filtra a captura de pacotes para coletar apenas pacotes que vêm de 192.168.2.5.
	"dst host 192.168.2.5"	Isso filtra a captura de pacotes para coletar apenas pacotes que vão para 192.168.2.5.
Porta	"porta 443"	Isso filtra a captura de pacotes para coletar apenas pacotes com uma origem ou um destino da porta 443.
	"src port 1055"	Isso captura o tráfego originado na porta 1055.
	"dst port 443"	Isso captura o tráfego destinado à porta 443.

Aqui está um exemplo onde a saída é exibida no console, mas também filtrada para ver apenas pacotes de dados CAPWAP:

```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246"  
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)  
12:20:50.483125 IP APC4F7-D54C-E77C.lan.5264 > 192.168.1.15.5246: UDP, length 81  
12:20:50.484361 IP 192.168.1.15.5246 > APC4F7-D54C-E77C.lan.5264: UDP, length 97
```

```
APC4F7.D54C.E77C#no debug traffic wired filter "port 5246"  
APC4F7.D54C.E77C#Killed  
APC4F7.D54C.E77C#
```

Exemplo de saída no arquivo:

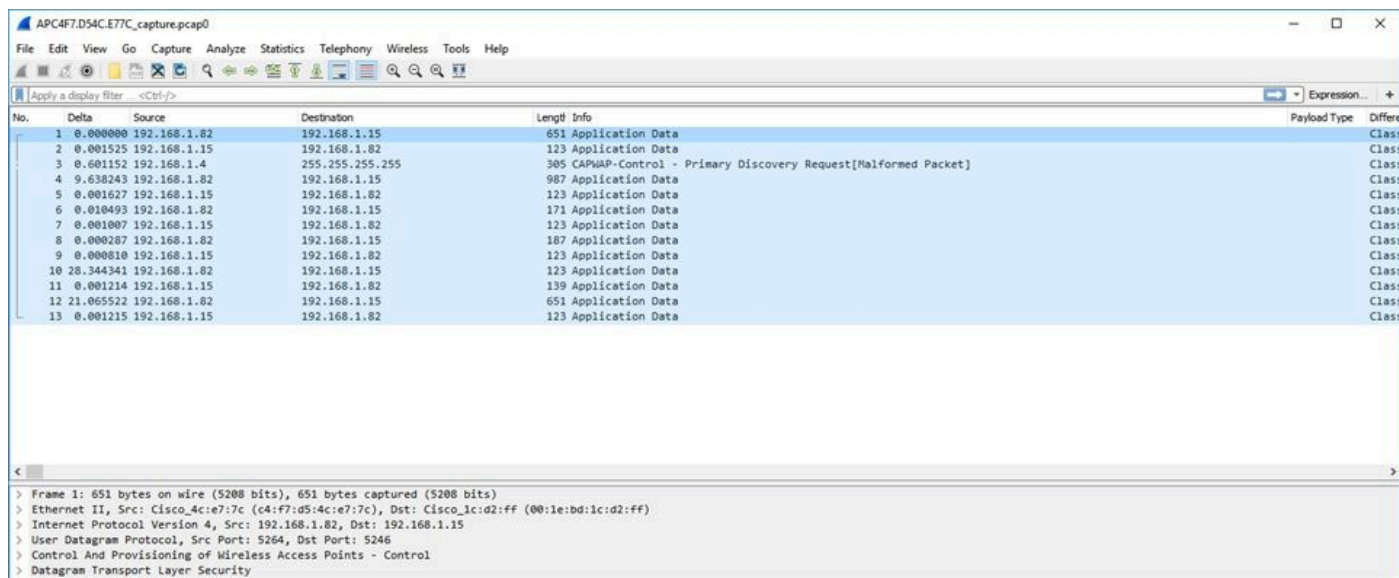
```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246" capture  
% Writing packets to "/tmp/pcap/APC4F7.D54C.E77C_capture.pcap0"
```

```

APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
APC4F7.D54C.E77C#no debug traffic wired filter "port 5246" capture
APC4F7.D54C.E77C#copy pcap APC4F7.D54C.E77C_capture.pcap0 tftp 192.168.1.100
#####
APC4F7.D54C.E77C#

```

Para abrir a captura no Wireshark:



Captura de rádio

É possível ativar a captura de pacotes no plano de controle do rádio. Devido ao impacto no desempenho, não é possível capturar dados no painel de rádio.

Isso significa que o fluxo de associação do cliente (testes, autenticação, associação, eap, arp, pacotes dhcp, bem como pacotes de controle ipv6, icmp e ndp) é visível, mas não os dados que o cliente passa após a movimentação para o estado conectado.

Procedimento

Etapa 1. Adicione o endereço mac do cliente rastreado. Vários endereços MAC podem ser adicionados. Também é possível executar o comando para todos os clientes, mas isso não é recomendado.

```

config ap client-trace address add < client-mac> --- Per client debugging. Allows multiple macs.
config ap client-trace all-clients <enable | disable> -- All clients debugging. Not recommended.

```

Etapa 2. Defina um filtro para registrar apenas protocolos específicos ou todos os protocolos suportados:

```
config ap client-trace filter <all|arp|assoc|auth|dhcp|eap|icmp|ipv6|ndp|probe> <enable|disable>
```

Etapa 3. Escolha exibir a saída no console (de forma assíncrona):

```
configure ap client-trace output console-log enable
```

Etapa 4. Inicie o rastreamento.

```
config ap client-trace start
```

Exemplo:

```
<#root>
```

```
APOCD0.F894.46E4#show dot11 clients
```

```
Total dot11 clients: 1
```

```
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate WGB
```

```
A8:DB:03:08:4C:4A
```

```
0 1 1 testewlclan -41 MCS92SS No
```

```
APOCD0.F894.46E4#config ap client-trace address add
```

```
A8:DB:03:08:4C:4A
```

```
APOCD0.F894.46E4#config ap client-trace filter
```

```
all Trace ALL filters  
arp Trace arp Packets  
assoc Trace assoc Packets  
auth Trace auth Packets  
dhcp Trace dhcp Packets  
eap Trace eap Packets  
icmp Trace icmp Packets  
ipv6 Trace IPv6 Packets  
ndp Trace ndp Packets  
probe Trace probe Packets
```

```
APOCD0.F894.46E4#config ap client-trace filter all enable
```

```
APOCD0.F894.46E4#configure ap client-trace output console-log enable
```

```
APOCD0.F894.46E4#configure ap client-trace start
```

```
APOCD0.F894.46E4#term mon
```

Para interromper a captura:

```
configure ap client-trace stop
configure ap client-trace clear
configure ap client-trace address clear
```

Verificar

Verificar Rastreamento de Cliente:

```
<#root>
```

```
AP70DB.98E1.3DEC#
```

```
show ap client-trace status
```

```
Client Trace Status           : Started
Client Trace ALL Clients      : disable
Client Trace Address          : a8:db:03:08:4c:4a
Remote/Dump Client Trace Address : a8:db:03:08:4c:4a

Client Trace Filter           : probe
Client Trace Filter           : auth
Client Trace Filter           : assoc
Client Trace Filter           : eap
Client Trace Filter           : dhcp
Client Trace Filter           : dhcpv6
Client Trace Filter           : icmp
Client Trace Filter           : icmpv6
Client Trace Filter           : ndp
Client Trace Filter           : arp

Client Trace Output           : eventbuf
Client Trace Output           : console-log
Client Trace Output           : dump
Client Trace Output           : remote

Remote trace IP               : 192.168.1.100
Remote trace dest port        : 5688
NOTE - Only VIP packets are seen on remote if VIP is enabled

Dump packet length           : 10
Client Trace Inline Monitor    : disable
Client Trace Inline Monitor pkt-attach : disable
```

Exemplo de uma conexão de cliente bem-sucedida:

```

Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5351] [1586169921:535099] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_AUTHENTICATION : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5351] [1586169921:535224] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_AUTHENTICATION : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5361] [1586169921:536158] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_AUTHENTICATION : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5416] [1586169921:541598] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ASSOC_REQUEST : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5441] [1586169921:544114] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ASSOC_RESPONSE : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5501] [1586169921:550153] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M1 : DescType 0x02 KeyInfo 0x008b
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5578] [1586169921:577836] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M2 : DescType 0x02 KeyInfo 0x010b
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5784] [1586169921:578476] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M3 : DescType 0x02 KeyInfo 0x013b
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.5955] [1586169921:595522] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M4 : DescType 0x02 KeyInfo 0x030b
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.6003] [1586169921:600341] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.6028] [1586169921:602817] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.6475] [1586169921:647518] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.6475] [1586169921:647594] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8636] [1586169921:863610] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DHCP_DISCOVER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8636] [1586169921:863644] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:C] DHCP_DISCOVER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863700] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:C] DHCP_DISCOVER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863731] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:C] DHCP_DISCOVER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863741] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:C] DHCP_DISCOVER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863762] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:E] DHCP_DISCOVER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863762] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:E] DHCP_DISCOVER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8676] [1586169921:867627] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:E] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8676] [1586169921:867664] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:C] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8677] [1586169921:867709] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:C] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8677] [1586169921:867740] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8684] [1586169921:868414] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8684] [1586169921:868445] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:C] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868476] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:C] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868507] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:C] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868538] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868569] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868600] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868631] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868662] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868693] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868724] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:868755] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6
Apr 6 10:45:22 kernel: [*04/06/2020 10:45:22.1611] [1586169922:161177] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1
Apr 6 10:45:22 kernel: [*04/06/2020 10:45:22.1612] [1586169922:161213] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:C] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1
Apr 6 10:45:22 kernel: [*04/06/2020 10:45:22.1646] [1586169922:164673] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:E] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1
Apr 6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164699] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:E] ARP_REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:42
Apr 6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164722] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:C] ARP_REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:42
Apr 6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164751] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] ARP_REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:42

```

U - Uplink packet (from client)
D - Downlink packet (to client)
W - module Wireless driver
E - module Ethernet driver
C - module Click

As letras entre colchetes ajudam você a entender onde o quadro foi visto (E para Ethernet, W para Wireless, C para o módulo Click quando ele é interno ao AP) e em que direção (Upload ou Download).

Aqui está uma pequena tabela do significado dessas letras:

- U - pacote de uplink (do cliente)
- D - pacote downlink(para clicar)
- W - driver de módulo sem fio
- E - driver de módulo Ethernet
- C - clique no módulo

Outras opções

Exibir log de forma assíncrona:

Os logs podem ser consultados com o comando: "show ap client-trace events mac xx:xx:xx:xx:xx:xx" (ou substitua o mac por "all")

```
<#root>
```

```
APOCD0.F894.46E4#
```

```
show ap client-trace events mac a8:db:03:08:4c:4a
```

```

[*04/06/2020 10:11:54.287675] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v1> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:11:54.288144] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:11:54.289870] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:11:54.317341] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:11:54.341370] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M1 : Desc
[*04/06/2020 10:11:54.374500] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M2 : Desc

```



```

[*04/06/2020 10:11:54.377237] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M3 : Desc
[*04/06/2020 10:11:54.390255] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M4 : Desc
[*04/06/2020 10:11:54.396855] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.416650] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469089] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469157] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921877] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921942] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:15:36.123119] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DEAUTHENTICATI
[*04/06/2020 10:15:36.127731] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DISASSOC : (.)
[*04/06/2020 10:17:24.128751] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.128870] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.129303] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.133026] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:17:24.136095] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:17:24.138732] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M1 : Desc
[*04/06/2020 10:17:24.257295] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M2 : Desc
[*04/06/2020 10:17:24.258105] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M3 : Desc
[*04/06/2020 10:17:24.278937] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M4 : Desc
[*04/06/2020 10:17:24.287459] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.301344] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327482] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327517] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430136] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430202] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:19:08.075326] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_PROBE_REQUEST
[*04/06/2020 10:19:08.075392] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_PROBE_RESPONS
[*04/06/2020 10:19:08.075437] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_PROBE_REQUEST

```

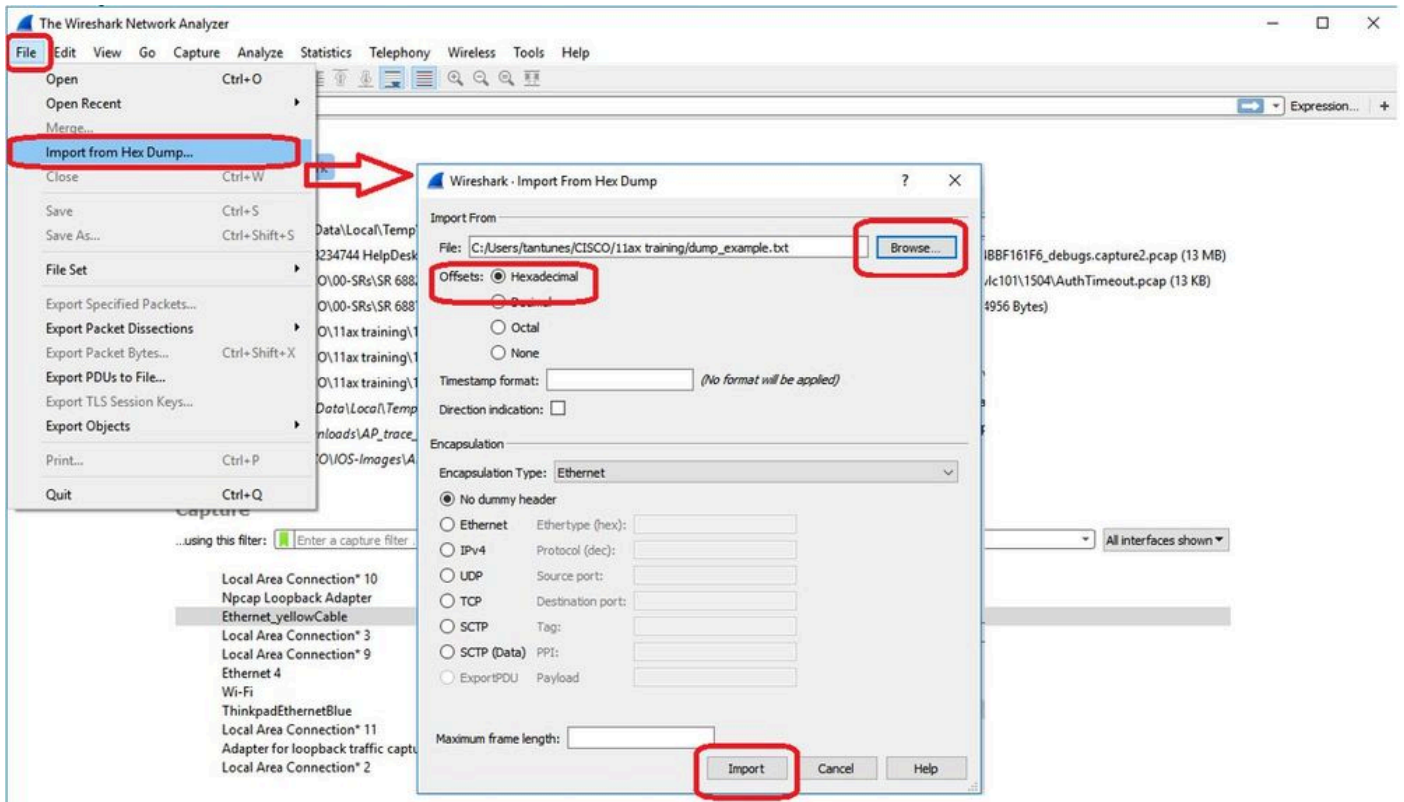
Despejar os pacotes no formato hexadecimal

Você pode despejar os pacotes no formato hexadecimal na CLI:

```

configure ap client-trace output dump address add xx:xx:xx:xx:xx:xx
configure ap client-trace output dump enable x -> Enter the packet dump length value

```

Como a saída pode ser muito grande e considerar que a saída menciona apenas que tipo de quadro é visto e não qualquer detalhe interno, pode ser mais eficiente redirecionar a captura de pacotes para um laptop que execute um aplicativo de captura (como o wireshark).

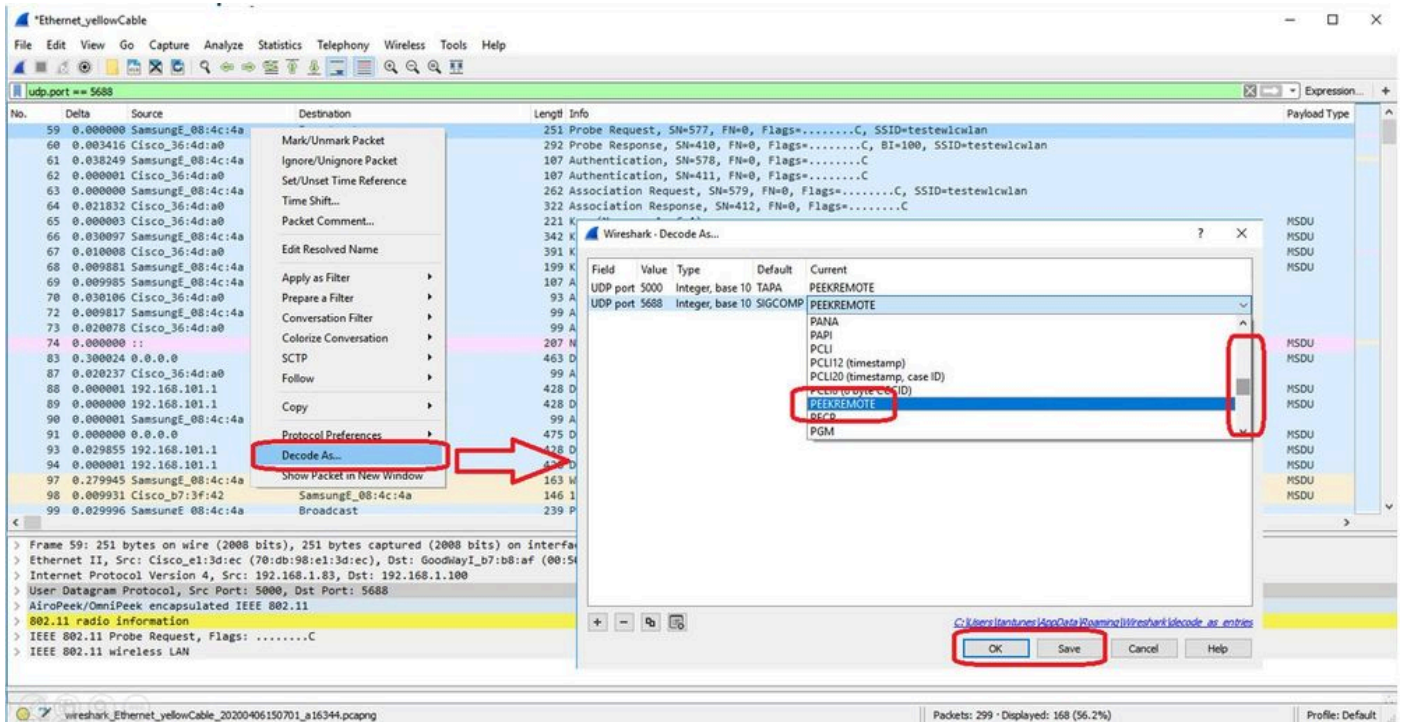
Ative o recurso de captura remota para enviar os pacotes para um dispositivo externo com o Wireshark:

```
config ap client-trace output remote enable
```

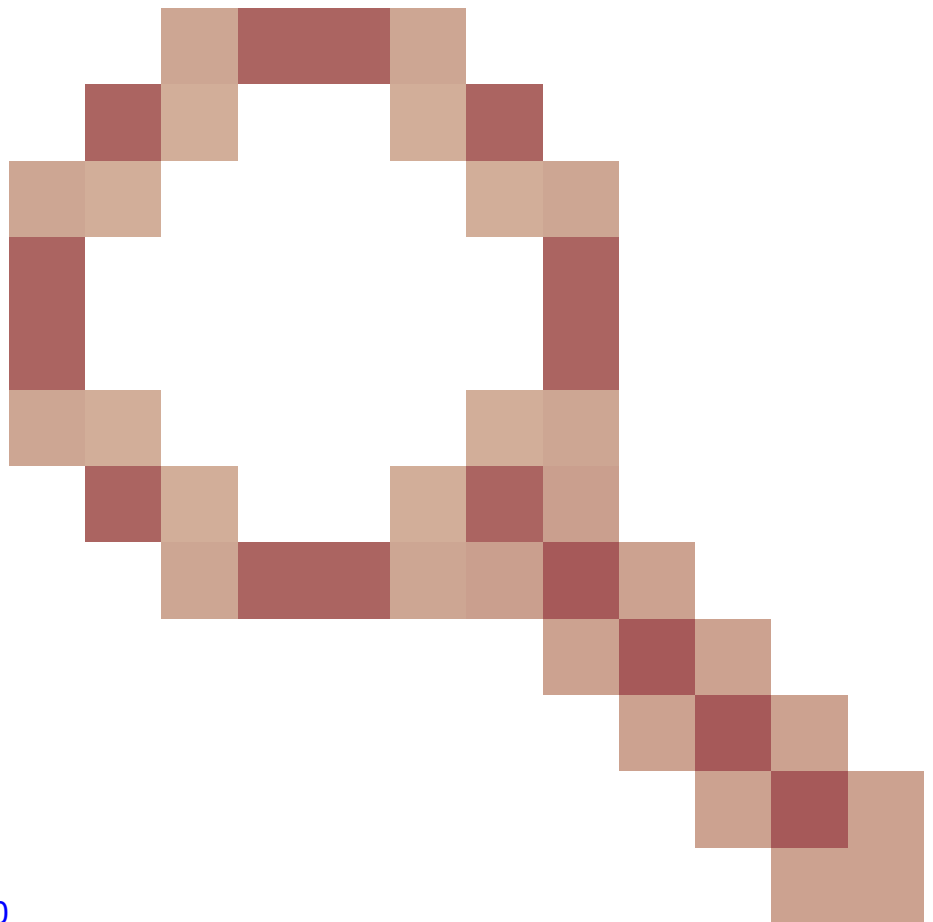
O comando significa que o AP encaminha todos os quadros capturados pelo filtro de rastreamento do cliente em direção ao laptop em 192.168.68.68 e usa o encapsulamento PEEKREMOTE (como os APs no modo farejador) na porta 5000.

Uma limitação é que o laptop de destino deve estar na mesma sub-rede do AP em que você executa esse comando. Você pode alterar o número da porta para acomodar quaisquer políticas de segurança em vigor na sua rede.

Depois de receber todos os pacotes no laptop que executa o Wireshark, você pode clicar com o botão direito no cabeçalho udp 5000 e escolher decodificar como e escolher PEEKREMOTE como ilustrado nesta figura:



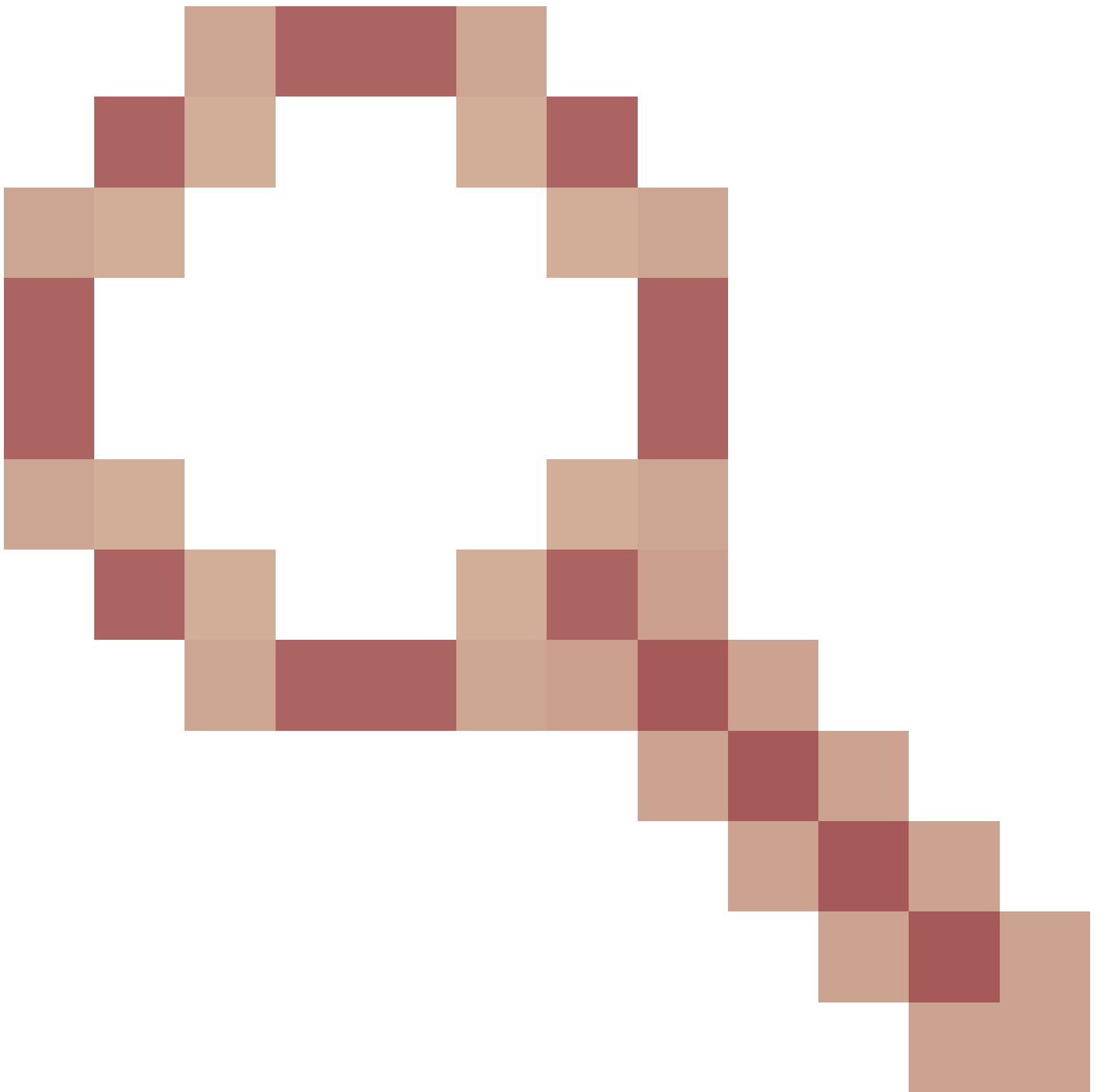
Lista de bugs e aprimoramentos relacionados a esse recurso:



[ID de bug da Cisco CSCvm09020](#)

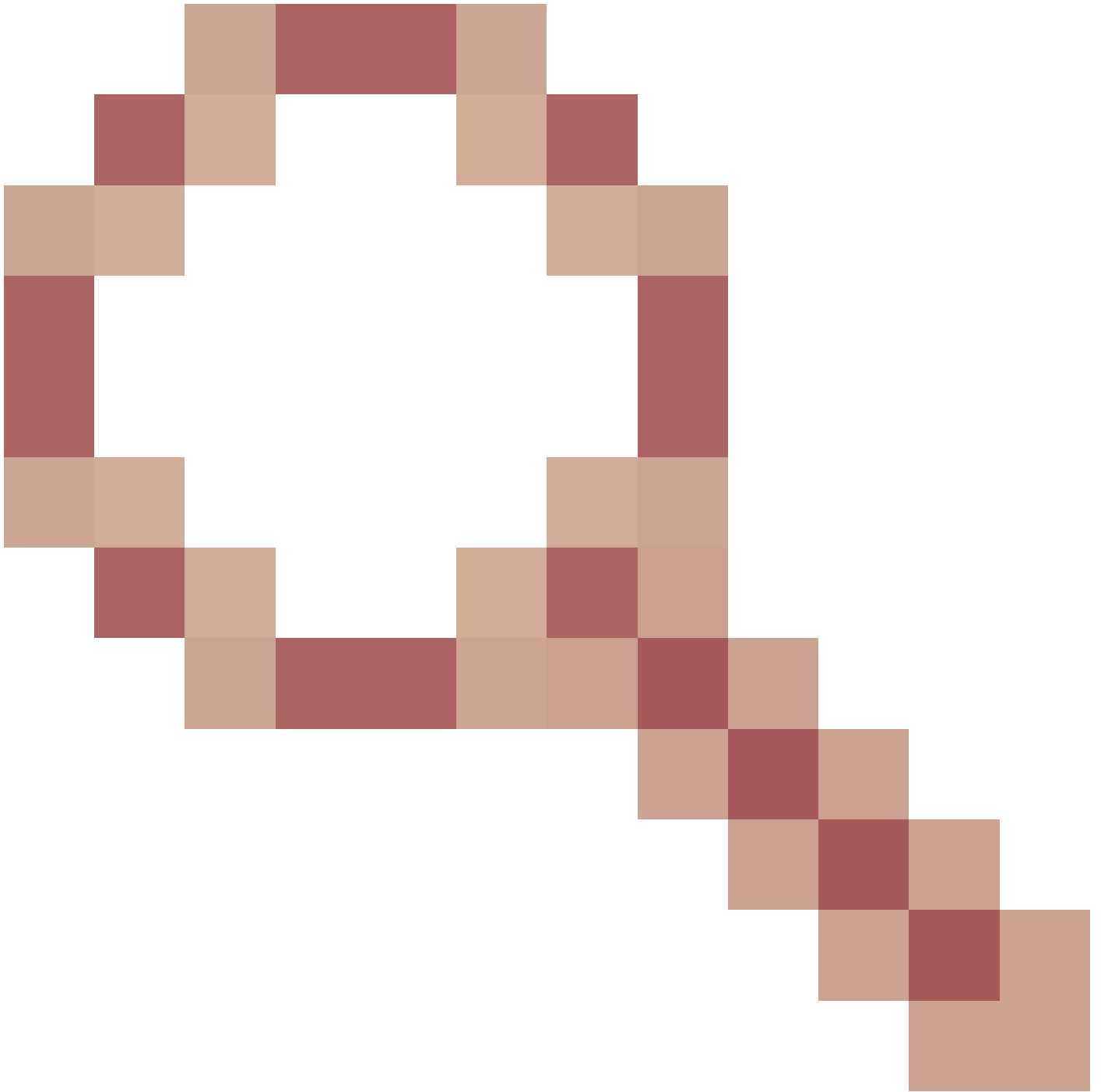
O DNS não é mais visto pelo rastreamento do cliente no 8.8

[ID de bug da Cisco CSCvm09015](#)



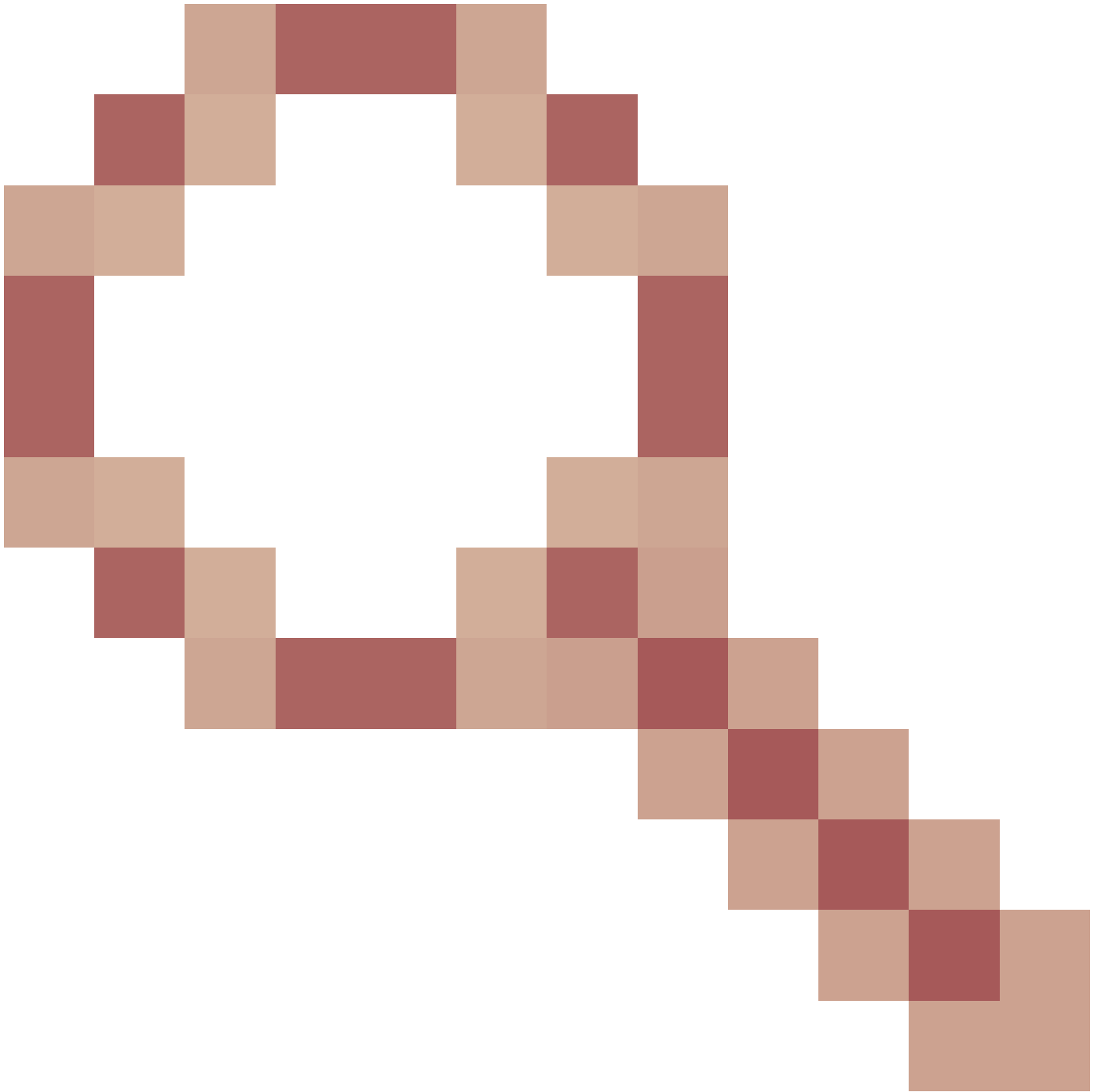
rastreamento de cliente mostra muitos ICMP_other com número de sequência nulo

[ID de bug da Cisco CSCvm02676](#)



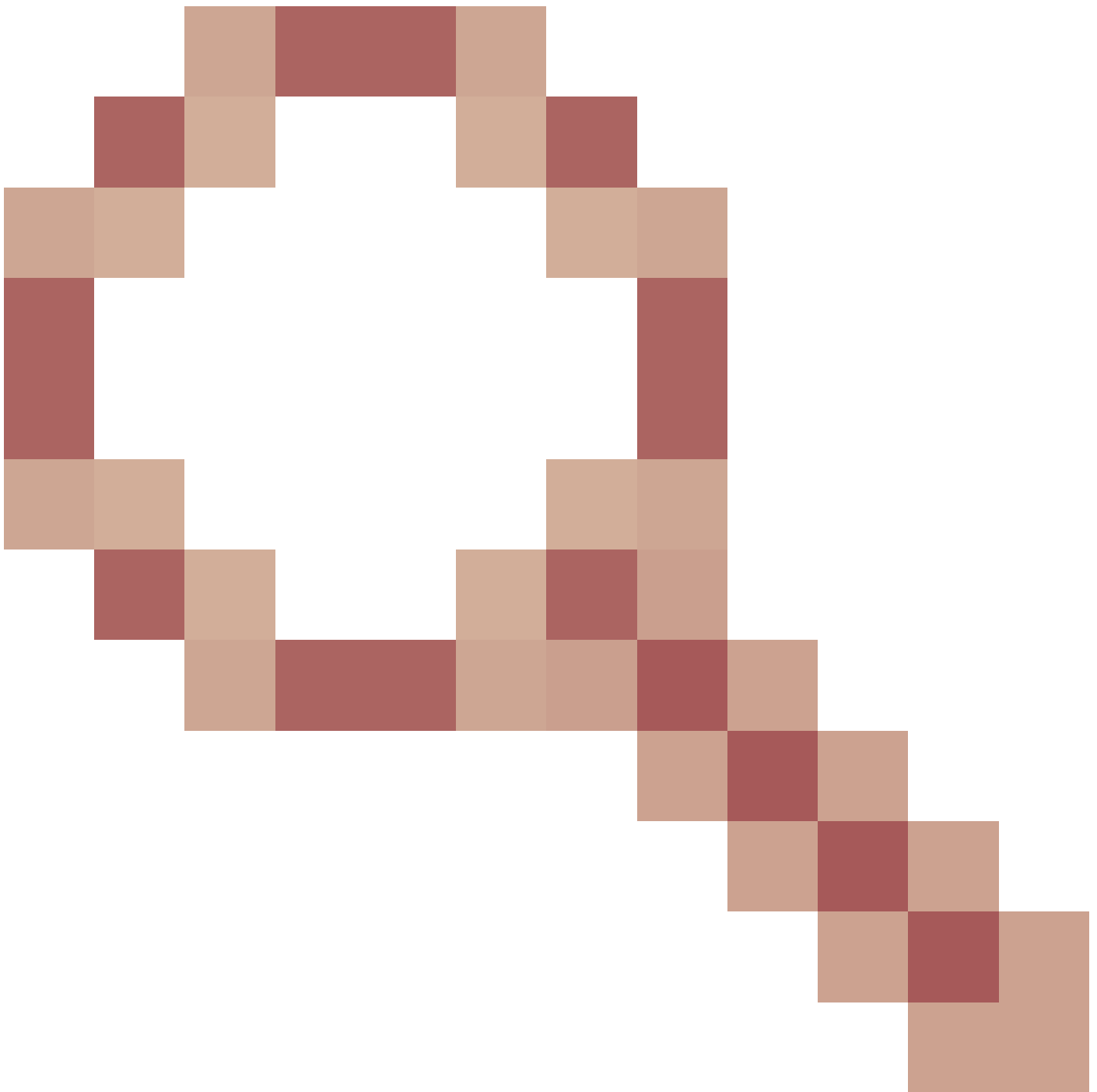
O rastreamento de cliente do AP COS não captura pacotes de webauth

ID de bug da Cisco [CSCvm02613](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvm02613)



A saída remota de rastreamento de cliente AP COS não funciona

ID de bug da Cisco [CSCvm00855](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvm00855)



Números SEQ de rastreamento de cliente inconsistentes

Controle o rastreamento do AP Client a partir do 9800 WLC

Você pode configurar vários APs para fazer um rastreamento de cliente de rádio e acioná-lo a partir do

Etapa 1. Configurar um perfil de rastreamento de AP que defina qual tráfego capturar

```
config term  
  wireless profile ap trace
```



```
filter all no filter probe output console-log
```

Etapa 2. Adicione o perfil de rastreamento de AP a um perfil de junção de AP usado pelos APs que você direciona.

```
ap profile < ap join profile name>  
  trace
```

Certifique-se de que esse perfil de ingresso no aplicativo seja aplicado a uma marca de site usada por seus APs de destino

Etapa 4 Disparar início/parada

```
ap trace client start ap
```

```
client all/
```

```
ap trace client stop ap
```

```
client all/
```

```
ap trace client start site
```

```
client all/
```

```
ap trace client stop site
```

```
client all/
```

Comandos de verificação:

```
show wireless profile ap trace summary  
show wireless profile ap trace detailed PROF_NAME detail  
sh ap trace client summary  
show ap trace unsupported-ap summary
```

Pacote de depuração do cliente no AP

Em vez de coletar uma depuração/captura de rádio, pode ser mais fácil usar o recurso de pacote de depuração de cliente se você estiver depurando um ou mais clientes específicos.

Etapa 1. Identifique o cliente cujos problemas você deseja solucionar.

```
9164#show dot11 clients
```

```
Total dot11 clients: 6
```

Client MAC	Slot	ID	WLAN ID	AID	WLAN Name	RSSI	Maxrate	is_wgb_wired	is_
mld_sta									
52:1E:34:C9:D6:F3		1	2	35	MySSID	-62	M7	No	
No									
80:A9:97:2C:DC:6E		1	2	34	MySSID	-47	MCS112SS	No	
No									
E8:D8:D1:1F:71:F3		0	2	35	MySSID	-62	M7	No	
No									
6A:E4:06:E7:AB:E1		1	2	33	MySSID	-44	MCS112SS	No	
No									
00:1D:63:70:AC:23		0	2	33	MySSID	-56	M7	No	
No									
68:72:C3:FD:17:F5		0	2	34	MySSID	-53	M15	No	
No									

Etapa 2. Inicie a depuração para um ou mais endereços MAC do cliente

```
9164#debug client-bundle start debug 80:A9:97:2C:DC:6E  
WORD
```

Por padrão, nada será impresso na tela. Você pode habilitar o monitor de terminal e ver as depurações sendo impressas ao vivo, mas lembre-se de que isso tornará o terminal muito difícil de usar. Não é necessário imprimir as depurações no terminal para coletar o pacote.

Etapa 3. Você deve parar o pacote de depuração antes de carregar a saída dele:

```
debug client-bundle start debug 80:A9:97:2C:DC:6E
```

Etapa 4. Carregue o pacote em um servidor FTP ou SCP (como lembrete, a WLC pode atuar como servidor SCP)

```
9164#debug client-bundle upload tftp 192.168.129.29 80:a9:97:2c:dc:6e
2024-09-04 11:58:48 Creating client bundle, please wait...
```

```
2024-09-04 11:59:01 Client bundle file 9164-_client_bundle.17.15.1.6.20240904.115848.tgz created.
2024-09-04 11:59:01 TFTP uploading...
Successful file transfer:
9164_client_bundle.17.15.1.6.20240904.115848.tgz
```

9164#

O pacote TGZ contém 4 arquivos:

- 2 contendo comandos show relativos aos rádios e ao cliente
- 1 sobre a depuração real (que é exibida no terminal se você usar o termo mon)
- 1 contendo syslogs

APs Catalyst 91xx em modo farejador

Os novos Catalyst 9115, 9117, 9120 e 9130 podem ser configurados no modo farejador. O procedimento é semelhante aos modelos de AP anteriores.

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller configuration page. The left sidebar shows navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled 'Configuration > Wireless > Access Points' and shows a table of 'All Access Points' with 4 APs listed. The selected AP is 'APC4F7.D54C.E77C' with model 'C9120AXI-B' and IP address '192.168.1.82'. The right pane shows the 'Edit AP' configuration for this AP. The 'General' tab is active, and the 'AP Mode' is set to 'Sniffer', which is highlighted with a red box. Other configuration details include AP Name, Location, Base Radio MAC, Ethernet MAC, Admin Status (ENABLED), Operation Status (Registered), Fabric Status (Disabled), LED State (ENABLED), LED Brightness Level (8), CleanAir (NSL/Kgy), Policy (FlexPolicy), and Site (TiagoOfficeSite). The 'Version' section shows Primary Software Version 16.12.3.13, Predownloaded Status N/A, Predownloaded Version N/A, Next Retry Time N/A, Boot Version 1.1.2.4, IOS Version 16.12.3.13, and Mini IOS Version 0.0.0.0. The 'IP Config' section shows CAPWAP Preferred Mode IPv4, DHCP IPv4 Address 192.168.1.82, and Static IP (IPv4/IPv6) unchecked. The 'Time Statistics' section shows Up Time as 0 days -22 hrs -58 mins -49 secs. The bottom right corner has an 'Update & Apply to Device' button.

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Search APs and Clients

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 4

AP Name	AP Model	Slots	Admin Status	IP Address
AP70DB.98E1.3DEC	AIR-AP3802I-I-K9	2	✓	192.168.1.83
APCCDD.F894.46E4	C9117AXI-B	2	✓	192.168.1.95
APb4de.318b.fee0	AIR-CAP3702I-I-K9	2	✓	192.168.1.79
APC4F7.D54C.E77C	C9120AXI-B	2	✓	192.168.1.82

5 GHz Radios

2.4 GHz Radios

Number of AP(s): 4

AP Name	Slot No.	Base Radio MAC	Admin Status
AP70DB.98E1.3DEC	0	0027.e336.4da0	✓
APCCDD.F894.46E4	0	0cd0.897.03e0	✓
APb4de.318b.fee0	0	b4de.31a4.e030	✓
APC4F7.D54C.E77C	0	cd64.e422.1780	✓

Edit Radios 2.4 GHz Band

Configure

Admin Status: ENABLED

CleanAir Admin Status: ENABLED

Assignment Method: Global

Tx Power Level Assignment

Antenna Parameters

Antenna Type: Internal

Current Tx Power Level: 1

Assignment Method: Global

Antenna A:

Antenna B:

Antenna C:

Antenna D:

Antenna Gain: 10

Sniffer Channel Assignment

Enable Sniffing:

Sniff Channel: 6

Sniffer IP*: 192.168.1.100

Sniffer IP Status: Valid

Download Core Dump to bootflash

Update & Apply to Device

*ThinkpadEthernetBlue

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 5000

No.	Delta	Source	Destination	Length	Info	Channel	BSS Color
2..	0.032866	SamsungE_08:4c:4a	Cisco_97:03:ef	107	Authentication, SN=37, FN=0, Flags=.....C	100	
2..	0.009001	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.001720	Cisco_97:03:ef	SamsungE_08:4c:4a	107	Authentication, SN=0, FN=0, Flags=.....C	100	
2..	0.000301	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.000791	SamsungE_08:4c:4a	Cisco_97:03:ef	360	Association Request, SN=38, FN=0, Flags=.....C, SSID=testewlclan	100	
2..	0.000230	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.004269	Cisco_97:03:ef	SamsungE_08:4c:4a	398	Association Response, SN=1, FN=0, Flags=.....C	100	0x01
2..	0.000750	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.010966	Cisco_97:03:ef	SamsungE_08:4c:4a	221	Key (Message 1 of 4)	100	
2..	0.000001	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.021911	SamsungE_08:4c:4a	Cisco_97:03:ef	342	Key (Message 2 of 4)	100	
2..	0.000002	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.002186	Cisco_97:03:ef	SamsungE_08:4c:4a	391	Key (Message 3 of 4)	100	
2..	0.000935	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.013829	SamsungE_08:4c:4a	Cisco_97:03:ef	199	Key (Message 4 of 4)	100	
2..	0.000174	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	

> Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]

> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

> Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (44)

> Tag: HT Capabilities (802.11n D1.10)

> Tag: HT Information (802.11n D1.10)

> Tag: Extended Capabilities (8 octets)

> Tag: VHT Capabilities

> Tag: VHT Operation

> Tag: Mobility Domain

> Tag: Fast BSS Transition

> Tag: RM Enabled Capabilities (5 octets)

> Tag: BSS Max Idle Period

> Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)

Tag Number: Element ID Extension (255)

Ext Tag length: 46

Ext Tag Number: HE Capabilities (IEEE Std 802.11ax/D3.0) (35)

> HE MAC Capabilities Information: 0x800002100009

> HE Phy Capabilities Information

> Supported HE-MCS and NSS Set

> Rx and Tx MCS Maps <= 80 MHz

> Rx HEX-MCS Map <= 80 MHz: 0xaaaa

.... 10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)

.... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)

.... .10 = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)

.... 10.. = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)

.... .10 = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)

.... 10.. = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)

.... .10 = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)

.... 10.. = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)

> Tx HEX-MCS Map <= 80 MHz: 0xaaaa

> PPE Thresholds

> Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)

Tag Number: Element ID Extension (255)

Ext Tag length: 9


Ext Tag Number: HE Operation (IEEE Std 802.11ax/D3.0) (36)


> HE Operation Parameters: 0x003fff4

> BSS Color Information: 0x01

> Basic HE-MCS and NSS Set: 0xffffc

Observação: os quadros de dados enviados com taxas de dados WIFI 6 são capturados,

 mas, como o peekremote não está atualizado no Wireshark, eles são mostrados como tipo phy 802.11ax a partir de agora. A correção está no Wireshark 3.2.4, em que o Wireshark exibe a taxa de phy correta do wifi6.

 Observação: os APs Cisco não podem capturar quadros MU-OFDMA no momento, mas podem capturar os quadros de acionamento (enviados na taxa de dados de gerenciamento) que anunciam uma janela MU-OFDMA. Você já pode inferir que a MU-OFDMA acontece (ou não) e com qual cliente.

Dicas para Troubleshooting

MTU de Caminho

Embora a Path MTU Discovery encontre a MTU ideal para o AP, é possível substituir essas configurações manualmente.

No AireOS 8.10.130 WLC, o comando `config ap pmtu disable <ap/all>` define uma MTU estática para um ou todos os APs em vez de confiar no mecanismo de descoberta dinâmica.

Para ativar depurações no momento da inicialização

Você pode executar `config boot debug capwap` para ativar as depurações capwap,DTLS e DHCP na próxima inicialização, antes mesmo de o SO ser inicializado e o prompt ser mostrado.

Você também tem "`config boot debug memory xxxx`" para várias depurações de memória.

Você pode ver se as depurações de inicialização estão ativadas ou não na próxima reinicialização com "`show boot`".

Eles podem ser desativados com a adição da palavra-chave `disable` no final, como "`config boot debug capwap disable`".

Mecanismo de economia de energia

A economia de energia de um determinado cliente pode ser solucionada com a execução `debug client trace <mac address>`

Cientes QoS

Para verificar se as tags de QoS estão aplicadas, você pode executar "`debug capwap client qos`".

Ele exibe o valor UP de pacotes para clientes sem fio.

Não é filtrável por mac a partir do 8.8 ; solicitação de aprimoramento Cisco bug [IDCSCvm08899](#)).

```
LabAP#debug capwap client qos
```

```
[*08/20/2018 09:43:36.3171] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8  
[*08/20/2018 09:43:45.0051] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8  
[*08/20/2018 09:43:45.5463] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8  
[*08/20/2018 09:43:46.5687] chatter: set_qos_up :: SetQosPriority: bridged packet dst: AC:81:12:C7:CD:3  
[*08/20/2018 09:43:47.0982] chatter: set_qos_up :: SetQosPriority: bridged packet dst: AC:81:12:C7:CD:3
```

Você também pode verificar a tabela Qos UP to DSCP no AP, bem como a quantidade total de pacotes marcados, modelados e descartados por Qos:

```
LabAP#show dot11 qos  
Qos Policy Maps (UPSTREAM)
```

```
no policymap  
Qos Stats (UPSTREAM)
```

```
total packets: 0  
dropped packets: 0  
marked packets: 0  
shaped packets: 0  
policed packets: 0  
copied packets: 0
```

```
DSCP TO DOT1P (UPSTREAM)
```

```
Default dscp2dot1p Table Value:
```

```
[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48
```

```
Active dscp2dot1p Table Value:
```

```
[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48
```

```
Qos Policy Maps (DOWNSTREAM)
```

```
no policymap  
Qos Stats (DOWNSTREAM)
```

```
total packets: 0  
dropped packets: 0  
marked packets: 0  
shaped packets: 0  
policed packets: 0  
copied packets: 0
```

```
DSCP TO DOT1P (DOWNSTREAM)
```

```
Default dscp2dot1p Table Value:
```

```
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
```

```
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
```

```
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
```

```
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
```

```
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
```

```
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
```

```
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
```

```
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
```

```
Active dscp2dot1p Table Value:
```

```
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
```

```
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
LabAP#
```

Quando as políticas de Qos são definidas na WLC e baixadas no AP Flexconnect, você pode verificá-las com :

```
AP780C-F085-49E6#show policy-map
2 policymaps
Policy Map BWLimitAAAClients          type:qos client:default
  Class BWLimitAAAClients_AVC_UI_CLASS
    drop

  Class BWLimitAAAClients_ADV_UI_CLASS
    set dscp af41 (34)

  Class class-default
    police rate 5000000 bps (625000Bytes/s)
    conform-action
    exceed-action

Policy Map platinum-up                type:qos client:default
  Class cm-dscp-set1-for-up-4
    set dscp af41 (34)

  Class cm-dscp-set2-for-up-4
    set dscp af41 (34)

  Class cm-dscp-for-up-5
    set dscp af41 (34)

  Class cm-dscp-for-up-6
    set dscp ef (46)

  Class cm-dscp-for-up-7
    set dscp ef (46)

  Class class-default
    no actions
```

No caso de limitação de taxa de Qos:


```
AP780C-F085-49E6#show rate-limit client
```

```
Config:
```

```
          mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst
A8:DB:03:6F:7A:46 2          0          0          0          0          0          0          0
```

```
Statistics:
```

```
          name      up   down
          Unshaped    0    0
          Client RT pass    0    0
          Client NRT pass    0    0
          Client RT drops    0    0
          Client NRT drops    0 38621
          9 54922    0
```

Verificação fora do canal

A depuração da verificação fora do canal do AP pode ser útil ao solucionar problemas de detecção de invasor (para validar se e quando o AP vai em um canal específico para verificar), mas também pode ser útil na solução de problemas de vídeo, em que um fluxo sensível em tempo real obtém interrupções constantes se o recurso "adiamento da verificação fora do canal" não for usado.

```
debug rrm off-channel defer
debug rrm off-channel dbg (starting 17.8.1)
debug rrm off-channel schedule
debug rrm off-channel voice (starting 17.8.1)
debug rrm schedule (starting 17.8.1, debug NDP packet tx)
show trace dot11 channel enable
```

```
[*06/11/2020 09:45:38.9530] wcp/rrm_userspace_0/rrm_schedule :: RRMSchedule process_int_duration_timer_
[*06/11/2020 09:45:39.0550] noise measurement channel 5 noise 89
[*06/11/2020 09:45:43.5490] wcp/rrm_userspace_1/rrm_schedule :: RRMSchedule process_int_duration_timer_
[*06/11/2020 09:45:43.6570] noise measurement channel 140 noise 97
```

Conectividade do cliente

É possível listar os clientes que foram desautenticados pelo ponto de acesso com o carimbo de data/hora do último evento:

```
LabAP#show dot11 clients deauth
          timestamp          mac vap reason_code
Mon Aug 20 09:50:59 2018 AC:BC:32:A4:2C:D3 9 4
Mon Aug 20 09:52:14 2018 00:AE:FA:78:36:89 9 4
Mon Aug 20 10:31:54 2018 00:AE:FA:78:36:89 9 4
```

Na saída anterior, o código de razão é o código de razão de desautenticação, conforme detalhado

neste link :

<https://community.cisco.com:443/t5/wireless-mobility-knowledge-base/802-11-association-status-802-11-deauth-reason-codes/ta-p/3148055>

O vap refere-se ao identificador da WLAN dentro do AP (que é diferente do ID da WLAN no !!! da WLC).

Você pode relacioná-lo com outras saídas detalhadas posteriormente, que sempre mencionam o vap de clientes associados.

Você pode ver a lista de IDs de VAP com "show controllers Dot11Radio 0/1 wlan".

Quando os clientes ainda estiverem associados, você poderá obter detalhes sobre sua conexão com:

```
LabAP#show dot11 clients
```

```
Total dot11 clients: 1
      Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate WGB
00:AE:FA:78:36:89      1      10  1  TestSSID -25 MCS82SS No
```

É possível obter muito mais detalhes sobre a entrada do cliente com:

```
LabAP#show client summ
```

```
Radio Driver client Summary:
```

```
=====
wifi0
[*08/20/2018 11:54:59.5340]
[*08/20/2018 11:54:59.5340] Total STA List Count 0
[*08/20/2018 11:54:59.5340] | NO|          MAC|STATE|
[*08/20/2018 11:54:59.5340] -----
wifi1
[*08/20/2018 11:54:59.5357]
[*08/20/2018 11:54:59.5357] Total STA List Count 1
[*08/20/2018 11:54:59.5357] | NO|          MAC|STATE|
[*08/20/2018 11:54:59.5357] -----
[*08/20/2018 11:54:59.5357] | 1| 0:ffffffae:fffffffa:78:36:ffffff89|      8|
```

```
Radio Driver Client AID List:
```

```
=====
wifi0
[*08/20/2018 11:54:59.5415]
[*08/20/2018 11:54:59.5415] Total STA-ID List Count 0
[*08/20/2018 11:54:59.5415] | NO|          MAC|STA-ID|
[*08/20/2018 11:54:59.5415] -----
wifi1
[*08/20/2018 11:54:59.5431]
[*08/20/2018 11:54:59.5431] Total STA-ID List Count 1
[*08/20/2018 11:54:59.5431] | NO|          MAC|STA-ID|
[*08/20/2018 11:54:59.5432] -----
```

[*08/20/2018 11:54:59.5432] | 1| 0:ffffffae:fffffffa:78:36:ffffff89| 6|

WCP client Summary:

=====

mac	radio	vap	aid	state	encr	Maxrate	is_wgb_wired	wgb_mac_addr
00:AE:FA:78:36:89	1	9	1	FWD	AES_CCM128	MCS82SS	false	00:00:00:00:00:00

NSS client Summary:

=====

Current Count: 3

MAC	OPAQUE	PRI	POL	VLAN	BR	TN	QCF	BSS	RADID	MYMAC
F8:0B:CB:E4:7F:41	00000000		3	0	1	1	0	2	3	1
F8:0B:CB:E4:7F:40	00000000		3	0	1	1	0	2	3	1
00:AE:FA:78:36:89	00000003		1	0	1	1	0	9	1	0

Datapath IPv4 client Summary:

=====

id	vap	port	node	tunnel	mac	seen_ip	hashed_ip	sniff_a
00:AE:FA:78:36:89	9	apr1v9	192.0.2.13	-	00:AE:FA:78:36:89	192.168.68.209	10.228.153.45	5.990000

Datapath IPv6 client Summary:

=====

client	mac	seen_ip6	age	scope	port
1	00:AE:FA:78:36:89	fe80::2ae:faff:fe78:3689	61	link-local	apr1v9

Wired client Summary:

=====

mac	port	state	local_client	detect_ago	associated_ago	tx_pkts	tx_bytes	rx_pkts	rx_bytes
-----	------	-------	--------------	------------	----------------	---------	----------	---------	----------

Você pode forçar a desconexão de um cliente específico com :

test dot11 client deauthenticate

Os contadores de tráfego podem ser obtidos por cliente com:

```
LabAP#show client statistics wireless 00:AE:FA:78:36:89
Client MAC address: 00:AE:FA:78:36:89
Tx Packets           : 621
Tx Management Packets : 6
Tx Control Packets   : 153
Tx Data Packets      : 462
Tx Data Bytes        : 145899
Tx Unicast Data Packets : 600
Rx Packets           : 2910
Rx Management Packets : 13
Rx Control Packets   : 943
Rx Data Packets      : 1954
Rx Data Bytes        : 145699
LabAP#
```

Mais no nível do rádio, muitas informações podem ser obtidas nos "show controllers". Quando você adiciona o endereço mac do cliente, as taxas de dados suportadas, as taxas de dados atuais, os recursos PHY, bem como a quantidade de novas tentativas e txfail, são exibidos:

<#root>

```
LabAP#show controllers dot11Radio 0 client 00:AE:FA:78:36:89
      mac radio vap aid state      encr Maxrate is_wgb_wired      wgb_mac_addr
00:AE:FA:78:36:89    0  9  1  FWD AES_CCM128    M15          false 00:00:00:00:00:00
Configured rates for client 00:AE:FA:78:36:89
Legacy Rates(Mbps): 11
HT Rates(MCS):M0 M1 M2 M3 M4 M5 M6 M7 M8 M9 M10 M11 M12 M13 M14 M15
VHT Rates: 1SS:M0-7 2SS:M0-7
```

```
HT:yes      VHT:yes      HE:no      40MHz:no    80MHz:no    80+80MHz:no    160MHz:no
11w:no      MFP:no      11h:no     encrypt_polocy: 4
_wmm_enabled:yes  qos_capable:yes  WME(11e):no    WMM_MIXED_MODE:no
short_preamble:yes  short_slot_time:no  short_hdr:yes  SM_dyn:yes
short_GI_20M:yes  short_GI_40M:no  short_GI_80M:yes  LDPC:yes  AMSDU:yes  AMSDU_long:no
su_mimo_capable:yes  mu_mimo_capable:no  is_wgb_wired:no  is_wgb:no
```

Additional info for client 00:AE:FA:78:36:89

```
RSSI: -90
PS : Legacy (Sleeping)
Tx Rate: 0 Kbps
Rx Rate: 117000 Kbps
VHT_TXMAP: 0
CCX Ver: 4
```

Statistics for client 00:AE:FA:78:36:89

```
      mac      intf TxData TxMgmt TxUC TxBytes
```

TxFail

```
TxDcrd TxCumRetries RxData RxMgmt RxBytes RxErr TxRt      RxRt idle_counter stats_ago expiration
00:AE:FA:78:36:89 apr0v9      8      1      6      1038      1      0      0      31      1      1599
```

Per TID packet statistics for client 00:AE:FA:78:36:89

Priority	Rx Pkts	Tx Pkts	Rx(last 5 s)	Tx (last 5 s)	QID	Tx Drops	Tx Cur	Qlimit
0	899	460	1	1	144	0	0	1024
1	0	0	0	0	145	0	0	1024
2	0	0	0	0	146	0	0	1024
3	59	0	0	0	147	0	0	1024
4	0	0	0	0	148	0	0	1024
5	0	0	0	0	149	0	0	1024
6	0	0	0	0	150	0	0	1024
7	0	0	0	0	151	0	0	1024

Legacy Rate Statistics:

```
(Mbps : Rx, Tx, Tx-Retries)
11 Mbps : 2, 0, 0
6 Mbps : 0, 9, 0
```

HT/VHT Rate Statistics:

```
(Rate/SS/Width : Rx, Rx-Ampdu, Tx, Tx-Ampdu, Tx-Retries)
0/1/20 : 4, 4, 0, 0, 0
6/2/20 : 4, 4, 0, 0, 0
7/2/20 : 5, 5, 0, 0, 0
```

webauth done:

false

Para acompanhar constantemente uma taxa de dados de cliente e/ou valor RSSI, você pode executar "debug dot11 client rate address <mac> " e isso registra essas informações a cada segundo:

```
LabAP#debug dot11 client rate address 00:AE:FA:78:36:89
[*08/20/2018 14:17:28.0928]          MAC      Tx-Pkts    Rx-Pkts    Tx-Rate    Rx-Rate    RSSI    SNR    Tx-R
[*08/20/2018 14:17:28.0928] 00:AE:FA:78:36:89          0          0         12    a8.2-2s   -45    53
[*08/20/2018 14:17:29.0931] 00:AE:FA:78:36:89          7         18         12    a8.2-2s   -45    53
[*08/20/2018 14:17:30.0934] 00:AE:FA:78:36:89          3         18         12    a8.2-2s   -45    53
[*08/20/2018 14:17:31.0937] 00:AE:FA:78:36:89          2         20         12    a8.2-2s   -45    53
[*08/20/2018 14:17:32.0939] 00:AE:FA:78:36:89          2         20         12    a8.2-2s   -45    53
[*08/20/2018 14:17:33.0942] 00:AE:FA:78:36:89          2         21         12    a8.2-2s   -46    52
[*08/20/2018 14:17:34.0988] 00:AE:FA:78:36:89          1          4         12    a8.2-2s   -46    52
[*08/20/2018 14:17:35.0990] 00:AE:FA:78:36:89          9         23         12    a8.2-2s   -46    52
[*08/20/2018 14:17:36.0993] 00:AE:FA:78:36:89          3          7         12    a8.2-2s   -46    52
[*08/20/2018 14:17:37.0996] 00:AE:FA:78:36:89          2          6         12    a8.2-2s   -46    52
[*08/20/2018 14:17:38.0999] 00:AE:FA:78:36:89          2         14         12    a8.2-2s   -46    52
[*08/20/2018 14:17:39.1002] 00:AE:FA:78:36:89          2         10         12    a8.2-2s   -46    52
[*08/20/2018 14:17:40.1004] 00:AE:FA:78:36:89          1          6         12    a8.2-2s   -46    52
[*08/20/2018 14:17:41.1007] 00:AE:FA:78:36:89          9         20         12    a8.2-2s   -46    52
[*08/20/2018 14:17:42.1010] 00:AE:FA:78:36:89          0          0         12    a8.2-2s   -46    52
[*08/20/2018 14:17:43.1013] 00:AE:FA:78:36:89          2          8         12    a8.2-2s   -46    52
[*08/20/2018 14:17:44.1015] 00:AE:FA:78:36:89          0          0         12    a8.2-2s   -46    52
[*08/20/2018 14:17:45.1018] 00:AE:FA:78:36:89          0          0         12    a8.2-2s   -46    52
[*08/20/2018 14:17:46.1021] 00:AE:FA:78:36:89          0          0         12    a8.2-2s   -46    52
[*08/20/2018 14:17:47.1024] 00:AE:FA:78:36:89          0          0         12    a8.2-2s   -46    52
[*08/20/2018 14:17:48.1026] 00:AE:FA:78:36:89          7         15         12    a8.2-2s   -46    52
[*08/20/2018 14:17:49.1029] 00:AE:FA:78:36:89          0          6         12    a8.2-2s   -46    52
[*08/20/2018 14:17:50.1032] 00:AE:FA:78:36:89          0          0         12    a8.2-2s   -46    52
[*08/20/2018 14:17:51.1035] 00:AE:FA:78:36:89          1          7         12    a8.2-2s   -46    52
[*08/20/2018 14:17:52.1037] 00:AE:FA:78:36:89          0         17         12    a8.2-2s   -46    52
[*08/20/2018 14:17:53.1040] 00:AE:FA:78:36:89          1         19         12    a8.2-2s   -46    52
[*08/20/2018 14:17:54.1043] 00:AE:FA:78:36:89          2         17         12    a8.2-2s   -46    52
[*08/20/2018 14:17:55.1046] 00:AE:FA:78:36:89          2         22         12    a8.2-2s   -45    53
[*08/20/2018 14:17:56.1048] 00:AE:FA:78:36:89          1         18         12    a8.2-2s   -45    53
[*08/20/2018 14:17:57.1053] 00:AE:FA:78:36:89          2         18         12    a8.2-2s   -45    53
[*08/20/2018 14:17:58.1055] 00:AE:FA:78:36:89         12         37         12    a8.2-2s   -45    53
```

Nesta saída, os contadores de pacotes Tx e Rx são pacotes transmitidos no segundo intervalo desde a última impressão, o mesmo para as Tentativas de Tx. No entanto, o RSSI, o SNR e a taxa de dados são os valores do último pacote desse intervalo (e não uma média para todos os pacotes nesse intervalo).

Cenários do Flexconnect

Você pode verificar quais ACLs estão atualmente aplicadas a um cliente em um cenário de pré-autorização (CWA, por exemplo) ou pós-autorização:

```
AP#show client access-lists pre-auth all f48c.507a.b9ad
Pre-Auth URL ACLs for Client: F4:8C:50:7A:B9:AD
IPv4 ACL: IPv6 ACL:
ACTION URL-LIST
```

```
Resolved IPs for Client: F4:8C:50:7A:B9:AD
HIT-COUNT URL ACTION IP-LIST
```

REDIRECT

```
rule 0: allow true and ip proto 17 and src port 53
rule 1: allow true and ip proto 17 and dst port 53
rule 2: allow true and src 10.48.39.161mask 255.255.255.255
rule 3: allow true and dst 10.48.39.161mask 255.255.255.255
rule 4: deny true
No IPv6 ACL found
```

```
AP#show client access-lists post-auth all f48c.507a.b9ad
Post-Auth URL ACLs for Client: F4:8C:50:7A:B9:AD
IPv4 ACL: IPv6 ACL:
ACTION URL-LIST
```

```
Resolved IPs for Client: F4:8C:50:7A:B9:AD
HIT-COUNT URL ACTION IP-LIST
```

post-auth

```
rule 0: deny true and dst 192.0.0.0mask 255.0.0.0
rule 1: deny true and src 192.0.0.0mask 255.0.0.0
rule 2: allow true
No IPv6 ACL found
```

Você pode ver os contadores de acertos nas ACLs do Flexconnect habilitando debug flexconnect access-list counter client <cliente MAC>

As execuções subsequentes do comando show client access-list pre-auth/post-auth all <MAC> depois adicionam contadores de acertos para cada entrada da ACL. Isso funciona para todos os tipos de ACLs flex a partir do Cisco IOS® XE 17.13. Em versões anteriores, os mesmos comandos existem, mas somente as ACLs de VLAN têm seus contadores de ocorrências atualizados.

Você pode redefinir os contadores de acerto da ACL com clear counters access-list client <mac>

Sistema de arquivos AP

Os APs COS não permitem listar todo o conteúdo do sistema de arquivos como em plataformas unix.

O comando "show filesystems" fornece detalhes do uso e da distribuição de espaço na partição atual:

```
2802#show filesystems
Filesystem      Size      Used Available Use% Mounted on
/dev/ubivol/storage 57.5M    364.0K    54.1M    1% /storage
```

2802#

O comando "show flash" lista os arquivos principais na flash do AP. Você também pode anexar a palavra-chave syslog ou core para listar essas pastas específicas.

```
ap_2802#show flash
Directory of /storage/
total 84
-rw-r--r-- 1 root root 0 May 21 2018 1111
-rw-r--r-- 1 root root 6 Apr 15 11:09 BOOT_COUNT
-rw-r--r-- 1 root root 6 Apr 15 11:09 BOOT_COUNT.reserve
-rw-r--r-- 1 root root 29 Apr 15 11:09 RELOADED_AT_UTC
drwxr-xr-x 2 root root 160 Mar 27 13:53 ap-images
drwxr-xr-x 4 5 root 2016 Apr 15 11:10 application
-rw-r--r-- 1 root root 6383 Apr 26 09:32 base_capwap_cfg_info
-rw-r--r-- 1 root root 20 Apr 26 10:31 bigacl
-rw-r--r-- 1 root root 1230 Mar 27 13:53 bootloader.log
-rw-r--r-- 1 root root 5 Apr 26 09:29 bootloader_verify.shadow
-rw-r--r-- 1 root root 18 Jun 30 2017 config
-rw-r--r-- 1 root root 8116 Apr 26 09:32 config.flex
-rw-r--r-- 1 root root 21 Apr 26 09:32 config.flex.mgroup
-rw-r--r-- 1 root root 0 Apr 15 11:09 config.local
-rw-r--r-- 1 root root 0 Jul 26 2018 config.mesh.dhcp
-rw-r--r-- 1 root root 180 Apr 15 11:10 config.mobexp
-rw-r--r-- 1 root root 0 Jun 5 2018 config.oep
-rw-r--r-- 1 root root 2253 Apr 26 09:43 config.wireless
drwxr-xr-x 2 root root 160 Jun 30 2017 cores
drwxr-xr-x 2 root root 320 Jun 30 2017 dropbear
drwxr-xr-x 2 root root 160 Jun 30 2017 images
-rw-r--r-- 1 root root 222 Jan 2 2000 last_good_uplink_config
drwxr-xr-x 2 root root 160 Jun 30 2017 lists
-rw-r--r-- 1 root root 215 Apr 16 11:01 part1_info.ver
-rw-r--r-- 1 root root 215 Apr 26 09:29 part2_info.ver
-rw-r--r-- 1 root root 4096 Apr 26 09:36 random_seed
-rw-r--r-- 1 root root 3 Jun 30 2017 rxtx_mode
-rw-r--r-- 1 root root 64 Apr 15 11:11 sensord_CSPRNG0
-rw-r--r-- 1 root root 64 Apr 15 11:11 sensord_CSPRNG1
drwxr-xr-x 3 support root 224 Jun 30 2017 support
drwxr-xr-x 2 root root 2176 Apr 15 11:10 syslogs
```

```
-----
Filesystem      Size      Used Available Use% Mounted on
flash           57.5M    372.0K    54.1M    1% /storage
```

Armazenar e enviar syslogs

A pasta syslog armazena a saída de syslog de reinicializações anteriores. O comando "show log" mostra apenas syslog desde a última reinicialização.

A cada ciclo de reinicialização, os syslogs são gravados em arquivos incrementais.

```
artaki# show flash syslogs
```

```
Directory of /storage/syslogs/
```

```
total 128
```

```
-rw-r--r-- 1 root root 11963 Jul 6 15:23 1
-rw-r--r-- 1 root root 20406 Jan 1 2000 1.0
-rw-r--r-- 1 root root 313 Jul 6 15:23 1.last_write
-rw-r--r-- 1 root root 20364 Jan 1 2000 1.start
-rw-r--r-- 1 root root 33 Jul 6 15:23 1.watchdog_status
-rw-r--r-- 1 root root 19788 Jul 6 16:46 2
-rw-r--r-- 1 root root 20481 Jul 6 15:23 2.0
-rw-r--r-- 1 root root 313 Jul 6 16:46 2.last_write
-rw-r--r-- 1 root root 20422 Jul 6 15:23 2.start
```

```
-----
Filesystem      Size      Used Available Use% Mounted on
flash           57.6M    88.0K    54.5M    0% /storage
```

```
artaki# show flash cores
```

```
Directory of /storage/cores/
```

```
total 0
```

```
-----
Filesystem      Size      Used Available Use% Mounted on
flash           57.6M    88.0K    54.5M    0% /storage
```

A primeira saída após a inicialização inicial é o arquivo 1.0 e um arquivo 1.1 é criado se 1.0 se tornar muito longo. Após a reinicialização, um novo arquivo 2.0 é criado e assim por diante.

Na WLC, você pode configurar o destino Syslog se quiser que seus APs enviem mensagens de syslog unicast para um servidor específico.

Por padrão, os APs enviam seus syslogs para um endereço de broadcast que pode causar uma certa tempestade de broadcast, portanto, assegure-se de configurar um servidor syslog.

O AP envia via syslog por padrão o que for impresso na saída do console.

No Controlador 9800, você pode alterar esses parâmetros no perfil Configuration -> AP Join, em Management.

Edit AP Join Profile

General Client CAPWAP AP **Management** Security ICap QoS

Device User Credentials CDP Interface

TFTP Downgrade

IPv4/IPv6 Address

Image File Name

System Log

Facility Value

Host IPv4/IPv6 Address

Log Trap Value

Secured ⓘ

Telnet/SSH Configuration

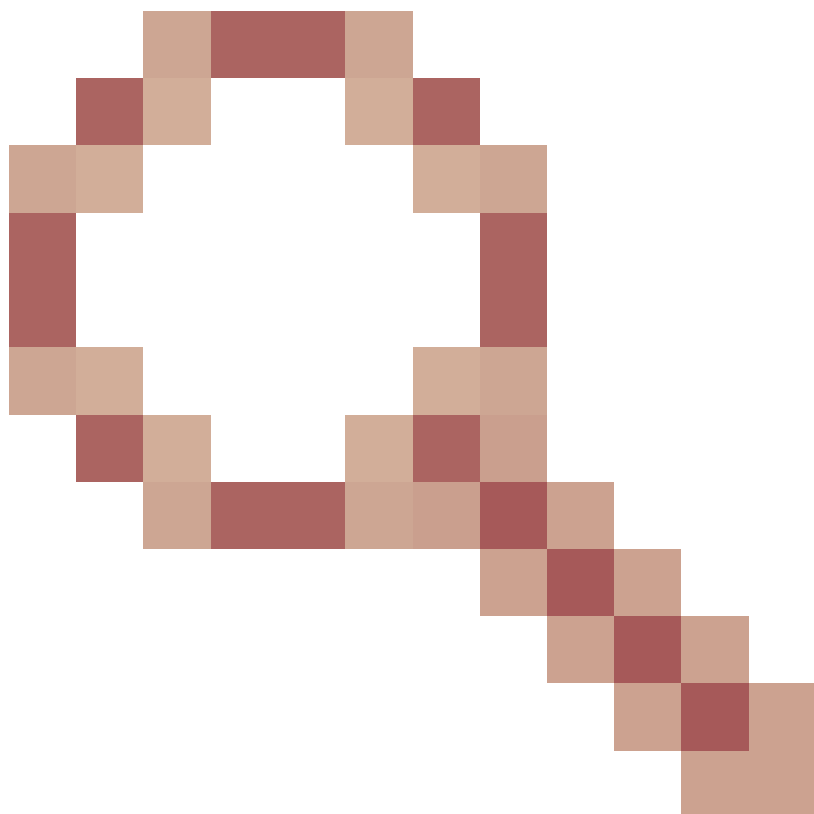
Telnet

SSH

AP Core Dump

Enable Core Dump

Você pode alterar o valor de interceptação de log para também enviar depurações via syslog. Você pode, então, habilitar depurações na CLI do AP e a saída delas é enviada através de mensagens de syslog para seu servidor configurado .



Devido ao bug da Cisco ID [CSCvu75017](#)

,somente quando você define o recurso de syslog como KERN (o valor padrão), o AP envia mensagens de syslog.

Se você estiver solucionando problemas em que um AP possivelmente perde a conectividade de rede (ou em um WGB, por exemplo), o syslog não será tão confiável quanto nenhuma mensagem será enviada se o AP perder a conectividade de uplink.

Portanto, depender dos arquivos de syslog armazenados na memória flash é uma ótima maneira de depurar e armazenar a saída no próprio AP e depois carregá-la periodicamente mais tarde.

Pacote de suporte AP

Algumas informações de diagnóstico comumente coletadas de vários tipos podem ser disponibilizadas em um único pacote que pode ser carregado de pontos de acesso.

As informações de diagnóstico que podem ser incluídas no pacote são:

- AP show tech
- Syslogs AP
- AP Capwapd Brain logs
- Logs de inicialização e mensagens do AP
- Arquivos Coredump AP

Para obter o pacote de suporte do AP, você pode acessar a CLI do AP e inserir o comando "copy support-bundle tftp: x.x.x.x".

Depois disso, você pode verificar o arquivo nomeado com o nome do AP anexado a support.apversion.date.time.tgz, como mostrado subseqüentemente:

```
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
<cr>
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
Creating support bundle, please wait...ifconfig: wired1: error fetching interface information: Device not found
Unit systemd-journald.socket could not be found.
tar: ./*.tgz: No such file or directory
tar: error exit delayed from previous errors
tar: *.tgz: No such file or directory
tar: error exit delayed from previous errors
+== Support file APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tgz created ==+
##### 100.0%
Successful file transfer:
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tgz
APC4F7.D54C.E77C#
```

Ao "descompactar" o arquivo, você pode exibir os vários arquivos coletados:

i-Images > APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526

Name	Date modified	Type	Size
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.brain.error.log.gz	4/8/2020 4:55 PM	GZ File	1 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.brain.log.gz	4/8/2020 4:55 PM	GZ File	3 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.info	4/8/2020 4:55 PM	INFO File	1 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.messages.gz	4/8/2020 4:55 PM	GZ File	11 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.startlog.gz	4/8/2020 4:55 PM	GZ File	5 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.syslogs.gz	4/8/2020 4:55 PM	GZ File	2 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tech_support.gz	4/8/2020 4:55 PM	GZ File	34 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.wsa_info.json.gz	4/8/2020 4:55 PM	GZ File	1 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.wsa_status.json.gz	4/8/2020 4:55 PM	GZ File	1 KB

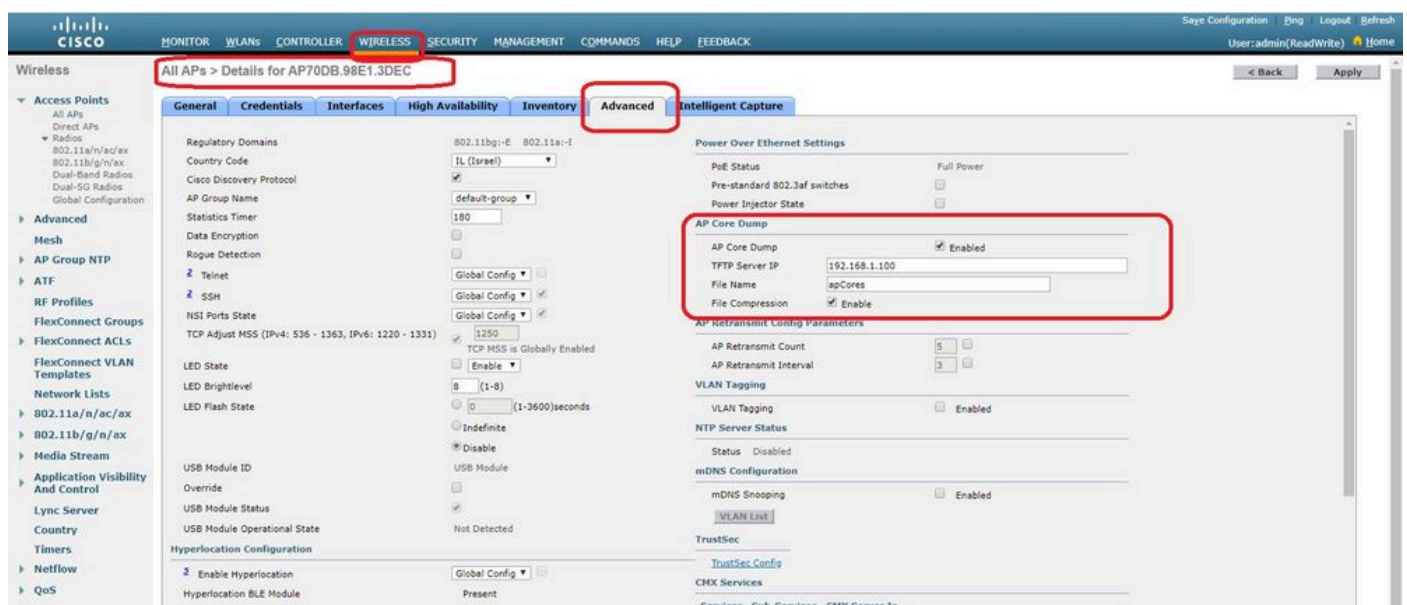
Coletar arquivos centrais de AP remotamente

Para coletar arquivos de núcleo de AP remotamente, habilite o dump de núcleo para ser incluído no pacote de suporte e, em seguida, carregue o pacote de suporte do AP ou envie diretamente para o servidor ftp. Os exemplos subsequentes usam o servidor tftp 192.168.1.100.

CLI AireOS

```
(c3504-01) >config ap core-dump enable 192.168.1.100 apCores uncompress ?  
<Cisco AP> Enter the name of the Cisco AP.  
all Applies the configuration to all connected APs.
```

GUI do AireOS



CLI do Cisco IOS®

<#root>

eWLC-9800-01C

config

)#ap profile TiagoOffice

eWLC-9800-01C

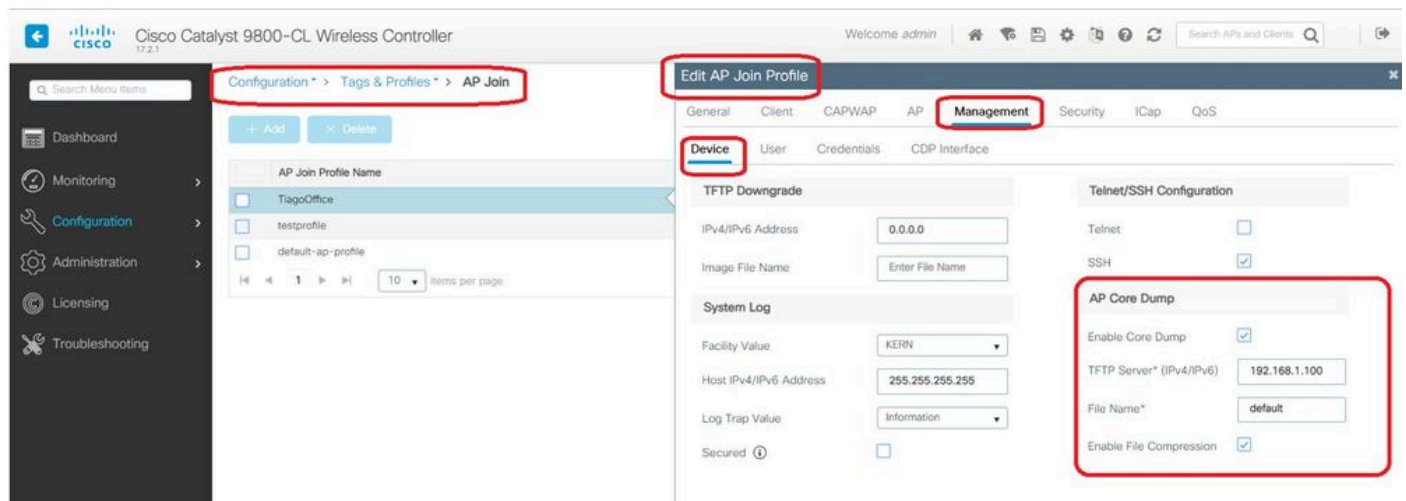
config-

ap

-profile

)#core-dump tftp-server 192.168.1.100 file apCores uncompress

GUI do Cisco IOS®



A partir do Cisco IOS® XE 17.3.1, você tem uma guia Support Bundle e pode baixar o AP SB da GUI da WLC.

Tudo o que ele faz é executar o comando "copy support-bundle" no AP e enviá-lo via SCP para a WLC (porque a WLC pode ser um servidor SCP).

E então você pode baixá-lo do seu navegador:



Isso significa que você pode fazer manualmente o mesmo truque em versões de eWLC anteriores à 17.3.1:

Copie o pacote de suporte do AP via SCP para o IP do eWLC se você não tiver um servidor TFTP acessível para o AP.

O eWLC é geralmente alcançável via SSH a partir do AP, então esse é um bom truque para o pré-17.3.

Etapa 1. [Ative o SSH no 9800 v17.2.1](#)

Etapa 2. [Ative a SCP no Cisco IOS® XE v17.2.1](#)

Este exemplo mostra como configurar a funcionalidade do servidor do SCP. Este exemplo usa um nome de usuário e uma senha definidos localmente:

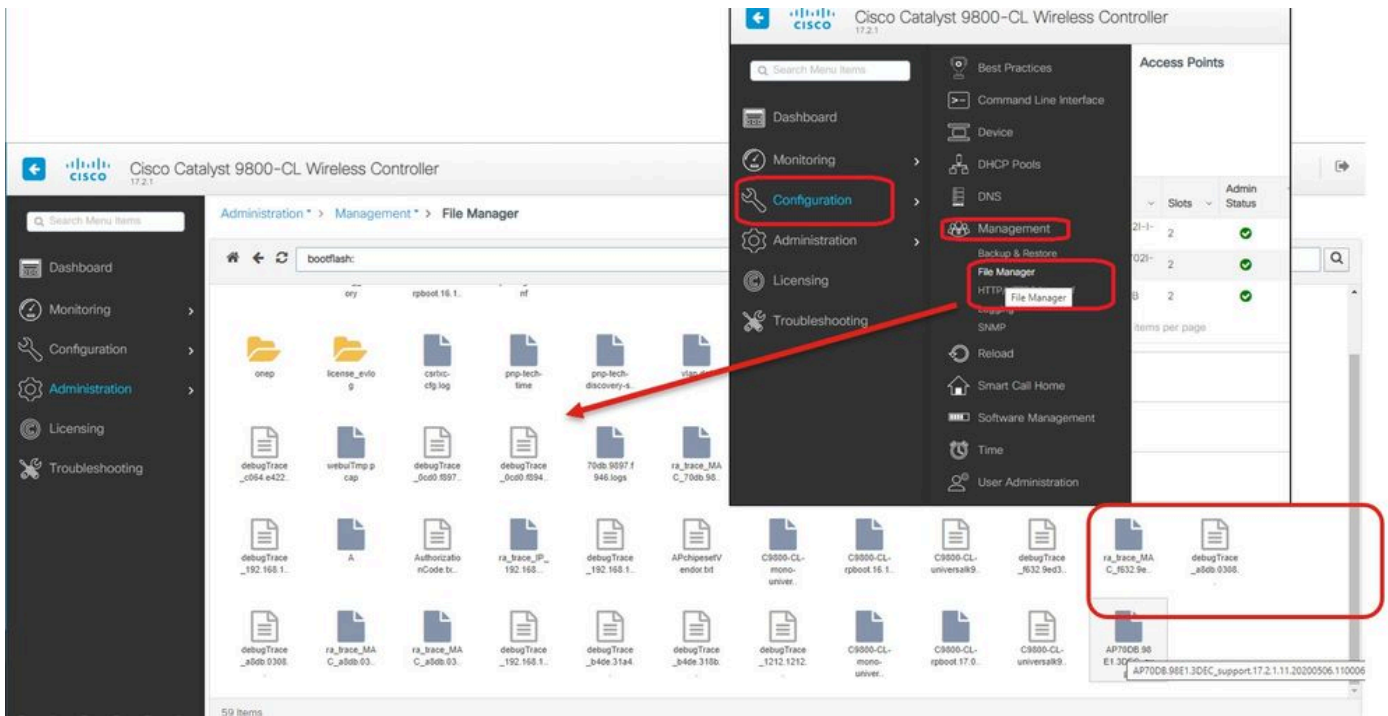
```
! AAA authentication and authorization must be configured properly in order for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
Device(config)# ip scp server enable
Device(config)# end
```

Etapa 3. Use o comando "copy support-bundle" e precisamos especificar o nome de arquivo a ser criado no servidor SCP.

Dica: você pode executar o comando uma vez para obter um nome de arquivo significativo e, em seguida, copiar/colar esse nome de arquivo no comando:

```
AP700B.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/
Creating support bundle, please wait...tar: ./*.tgz: No such file or directory
tar: error exit delayed from previous errors
tar: *.tgz: No such file or directory
tar: error exit delayed from previous errors
==== Support file AP700B.98E1.3DEC_support.17.2.1.11.20200506.110006.tgz created ====
Warning: Permanently added '192.168.1.15' (RSA) to the list of known hosts.
Password:
Connection closed by 192.168.1.15 port 22
lost connection
AP700B.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/AP700B.98E1.3DEC_support.17.2.1.11.20200506.110006.tgz
Creating support bundle, please wait...tar: ./*.tgz: No such file or directory
tar: error exit delayed from previous errors
tar: *.tgz: No such file or directory
tar: error exit delayed from previous errors
==== Support file AP700B.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz created ====
Password:
AP700B.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz                               100% 50KB 3.3MB/s 00:00
Connection to 192.168.1.15 closed by remote host.
AP700B.98E1.3DEC#
```

Etapa 4. Em seguida, você pode acessar a GUI do eWLC e obter o arquivo em: Administration > Management > File Manager:



IoT e Bluetooth

Os logs do servidor gRPC podem ser verificados no AP com:

```

AP# show grpc server log
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces conn url 10.22.243.33:8000"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering stopDNASpacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting stopDNASpacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering startDNASpacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] launching token request cycle"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting startDNASpacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces token expiration time 2020-04-02 01:36:52 +0000"
time="2020-04-01T01:36:52Z" level=info msg="Calling startDNASpacesConn routine "
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Receive Success status"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Connection not in ready state sleeping for 10 second"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Setup Stream for the gRPC connection"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Connect RPC Succeeded."
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] RX routine got enabled "
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] TX routine got enabled "

```

A conectividade com o conector do Cisco DNA Spaces pode ser verificada com:

```

AP# show cloud connector key access
Token Valid : Yes
Token Stats :
    Number of Attempts : 44
    Number of Failures : 27
    Last Failure on : 2020-03-28 02:02:15.649556818 +0000 UTC m=+5753.097022576
    Last Failure reason : curl: SSL connect error
    Last Success on : 2020-04-01 00:48:37.313511596 +0000 UTC m=+346934.760976625
    Expiration time : 2020-04-02 00:48:37 +0000 UTC

```


Unknown	3C:1D:AF:62:EC:EC	88	0	0000D:00H:00M:01S
iBeacon	18:04:ED:04:1C:5F	86	65	0000D:00H:00M:01S
Unknown	18:04:ED:04:1C:5F	78	65	0000D:00H:00M:01S
Unknown	04:45:E5:28:8E:E7	85	65	0000D:00H:00M:01S
Unknown	2D:97:FA:0F:92:9A	91	65	0000D:00H:00M:01S
iBeacon	E0:7D:EA:16:35:35	68	65	0000D:00H:00M:01S
Unknown	E0:7D:EA:16:35:35	68	65	0000D:00H:00M:01S
iBeacon	04:EE:03:53:74:22	45	256	0000D:00H:00M:01S
Unknown	04:EE:03:53:74:22	45	256	0000D:00H:00M:01S
	04:EE:03:53:6A:3A	72	N/A	0000D:00H:00M:01S
Unknown	04:EE:03:53:6A:3A	72	65	0000D:00H:00M:01S
iBeacon	E0:7D:EA:16:35:35	68	65	0000D:00H:00M:01S
Unknown	E0:7D:EA:16:35:35	67	65	0000D:00H:00M:01S
iBeacon	04:EE:03:53:74:22	60	256	0000D:00H:00M:01S
Unknown	04:EE:03:53:74:22	60	256	0000D:00H:00M:01S
Eddystone URL	04:EE:03:53:6A:3A	72	N/A	0000D:00H:00M:01S

Quando o AP atua no modo de gateway BLE avançado onde um aplicativo é implantado, você pode verificar o status do aplicativo loX com :

```

AP#show iox applications
Total Number of Apps : 1
-----
App Name                : cisco_dnas_ble_iox_app
App Ip                  : 192.168.11.2
App State               : RUNNING
App Token               : 02fb3e98-ac02-4356-95ba-c43e8a1f4217
App Protocol           : ble
App Grpc Connection    : Up
Rx Pkts From App       : 3878345
Tx Pkts To App         : 6460
Tx Pkts To Wlc         : 0
Tx Data Pkts To DNASpaces : 3866864
Tx Cfg Resp To DNASpaces : 1
Rx KeepAlive from App  : 11480
Dropped Pkts           : 0
App keepAlive Received On : Mar 24 05:56:49

```

Você pode se conectar ao aplicativo IOX com esses comandos e, em seguida, monitorar os logs durante a configuração de beacon da tribuna:

```

AP#connect iox application
/ #

/# tail -F /tmp/dnas_ble.log
Tue Mar 24 06:55:21 2020 [INFO]: Starting DNA Spaces BLE IOx Application
Tue Mar 24 06:55:21 2020 [INFO]: Auth token file contents: db26a8ab-e800-4fe9-a128-80683ea17b12
Tue Mar 24 06:55:21 2020 [INFO]: Setting gRPC endpoint to: 1.1.7.101:57777
Tue Mar 24 06:55:21 2020 [INFO]: Auth with token: db26a8ab-e800-4fe9-a128-80683ea17b12
Tue Mar 24 06:55:21 2020 [INFO]: Attempt to connect to DNAS Channel
Tue Mar 24 06:55:21 2020 [INFO]: Starting to run metrics
Tue Mar 24 06:55:21 2020 [INFO]: Starting to run Channel Keepalive
Tue Mar 24 06:55:21 2020 [INFO]: Initialize DNAS Reader Channel

```


Tue Mar 24 06:55:21 2020 [INFO]: Start listener for messages
Tue Mar 24 06:55:21 2020 [INFO]: Running BLE scan thread

Conclusão

Há muitas ferramentas de solução de problemas disponíveis para nos ajudar na resolução de problemas relacionados aos APs COS.

Este documento lista os mais usados e é atualizado regularmente.

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.