排除COS AP故障

目录

简介

先决条件

- 要求
- 使用的组件

捕获数据包跟踪（嗅探器跟踪）

- AP端口上的有线PCAP
  - 步骤
  - 命令选项
  - 使用过滤器实现有线PCAP
- 无线电捕获
  - 步骤
  - 验证
  - 其他选项
  - 从9800 WLC控制AP客户端跟踪
- AP上的客户端调试捆绑包
- 嗅探器模式下的AP Catalyst 91xx

故障排除提示

- 路径MTU
- 要在引导时启用调试，请执行以下操作：
- 省电机制
- 客户端Qos
- 信道外扫描
- 客户端连接
- Flexconnect方案
- AP文件系统
- 存储和发送系统日志
- AP支持套件
- 远程收集AP核心文件
  - AireOS CLI
  - AireOS GUI
  - Cisco IOS® CLI
  - Cisco IOS® GUI
- 物联网和蓝牙

结论

简介

本文档介绍适用于运行COS操作系统的AP的故障排除工具(Cheetah OS、Click OS、simply Cisco

AP OS)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档重点介绍COS AP，如2800、3800、1560和4800系列的AP型号，以及新的11ax AP Catalyst 91xx。

本文档重点介绍AireOS 8.8及更高版本中的许多功能。以及Cisco IOS® XE 16.12.2s及更高版本。

在之前的版本中，可能会出现有关某些功能可用性的注释。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

捕获数据包跟踪（嗅探器跟踪）

AP端口上的有线PCAP

可以对AP以太网端口使用pcap。您可以在CLI上显示实时结果（仅包含汇总的数据包详细信息），也可以将其保存为AP闪存中的完整pcap。

有线pcap捕获以太网端（包括Rx/Tx）上的所有内容，并且AP内的分路点紧接数据包连线之前。

但是，它仅捕获AP CPU平面流量，这意味着流入和流出AP的流量（AP DHCP、AP capwap控制隧道……），并且不显示客户端流量。

请注意，大小非常有限（最大大小限制为5MB），因此可能需要配置过滤器以仅捕获您感兴趣的流量。

在您尝试复制流量捕获之前，请确保使用“no debug traffic wired ip capture”或只使用“undebug

all”来停止流量捕获（否则，复制不会随着数据包的写入而结束）。

步骤

步骤1.启动pcap;使用“debug traffic wired ip capture”选择流量类型：

<#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)
```

步骤2.等待流量传输，然后使用命令“no debug traffic wired ip capture”或简单的“undebug all”停止捕获：

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

步骤3.将文件复制到tftp/scp服务器：

<#root>

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

AP70DB.98E1.3DEC_capture.pcap0

```
 tftp 192.168.1.100
##################################################################################################################
AP70DB.98E1.3DEC#
```

步骤4.现在您可以在wireshark中打开该文件。该文件是pcap0。请更改为pcap，以便它自动与wireshark关联。

命令选项

debug traffic wired命令有几个选项可以帮助您捕获特定流量：

```
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
```

您可以在debug命令末尾添加“verbose”以查看数据包的十六进制转储。请注意，如果您的过滤条件不够严格，这会很快淹没CLI会话。

使用过滤器实现有线PCAP

过滤器格式与tcpdump捕获过滤器格式相对应。

	过滤器示例	描述
主机	"主机192.168.2.5"	这将过滤数据包捕获，只收集进入或来自主机192.168.2.5的数据包。
	"源主机192.168.2.5"	这将过滤数据包捕获，仅收集来自192.168.2.5的数据包。
	"dst host 192.168.2.5"	这将过滤数据包捕获，只收集到达192.168.2.5的数据包。
端口	“端口 443”	这将过滤数据包捕获，仅收集源或目标端口为443的数据包。
	"源端口1055"	捕获来自端口1055的流量。
	"目标端口443"	这可以捕获发往端口443的流量。

以下是一个示例，输出显示在控制台上，但也经过过滤以仅查看CAPWAP数据包：

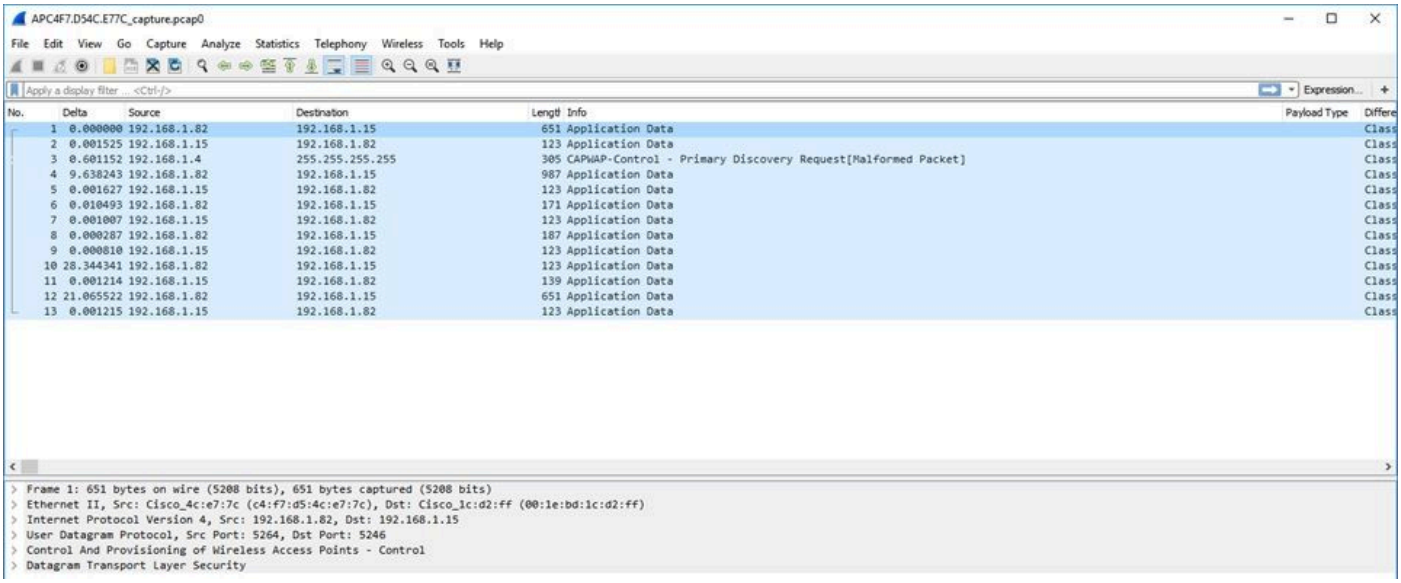
```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246"
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
12:20:50.483125 IP APC4F7-D54C-E77C.lan.5264 > 192.168.1.15.5246: UDP, length 81
12:20:50.484361 IP 192.168.1.15.5246 > APC4F7-D54C-E77C.lan.5264: UDP, length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

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

文件输出示例：

```
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#
```

要在wireshark上打开捕获，请执行以下操作：



无线电捕获

可以在无线电的控制平面上捕获数据包。由于性能影响，无法捕获无线电数据平面上的数据。

这意味着客户端关联流（探测、身份验证、关联、eap、arp、dhcp数据包以及ipv6控制数据包、icmp和ndp）可见，但客户端在移动到连接状态后传递的数据不可见。

步骤

步骤1.添加跟踪的客户端mac地址。可以添加多个mac地址。也可以对所有客户端运行该命令，但不建议这样做。

```
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.
```

步骤2.将过滤器设置为仅记录特定协议或所有支持的协议：

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

步骤3.选择在控制台上显示输出（异步）：

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

步骤4.开始跟踪。

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

示例：

<#root>

```
AP0CD0.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 testewlcwlan  -41 MCS92SS  No

AP0CD0.F894.46E4#config ap client-trace address add

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


AP0CD0.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
```

```
AP0CD0.F894.46E4#config ap client-trace filter all enable
AP0CD0.F894.46E4#configure ap client-trace output console-log enable
AP0CD0.F894.46E4#configure ap client-trace start
AP0CD0.F894.46E4#term mon
```

要停止捕获，请执行以下操作：

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

验证

验证客户端跟踪：

<#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
```

成功的客户端连接示例：



方括号中的字母可帮助您了解帧出现在何处（E表示以太网，W表示无线，C表示在AP内部的Click模块），以及在哪个方向（上传或下载）。

下面是一张小表，上面列出了这些字母的含义：

U — 上行链路数据包（来自客户端）
D — 下行链路数据包（单击）
W — 模块无线驱动程序
E — 模块以太网驱动程序
C — 模块点击

注意：从17.12.1开始，添加了一个附加字母A，以帮助验证数据包是否通过空中发送：
[D:W]部分，用于让aptrace知道通过kclick成功传递到驱动程序的mgmt/data数据包
[D:A]部分，用于在数据包通过空中发送时让aptrace了解相应的管理/数据数据包传输完成状态

其他选项

异步查看日志：

然后，可以使用命令“show ap client-trace events mac xx:xx:xx:xx:xx:xx:xx:xx”（或将mac替换为“all”）来查阅日志

<#root>

AP0CD0.F894.46E4#

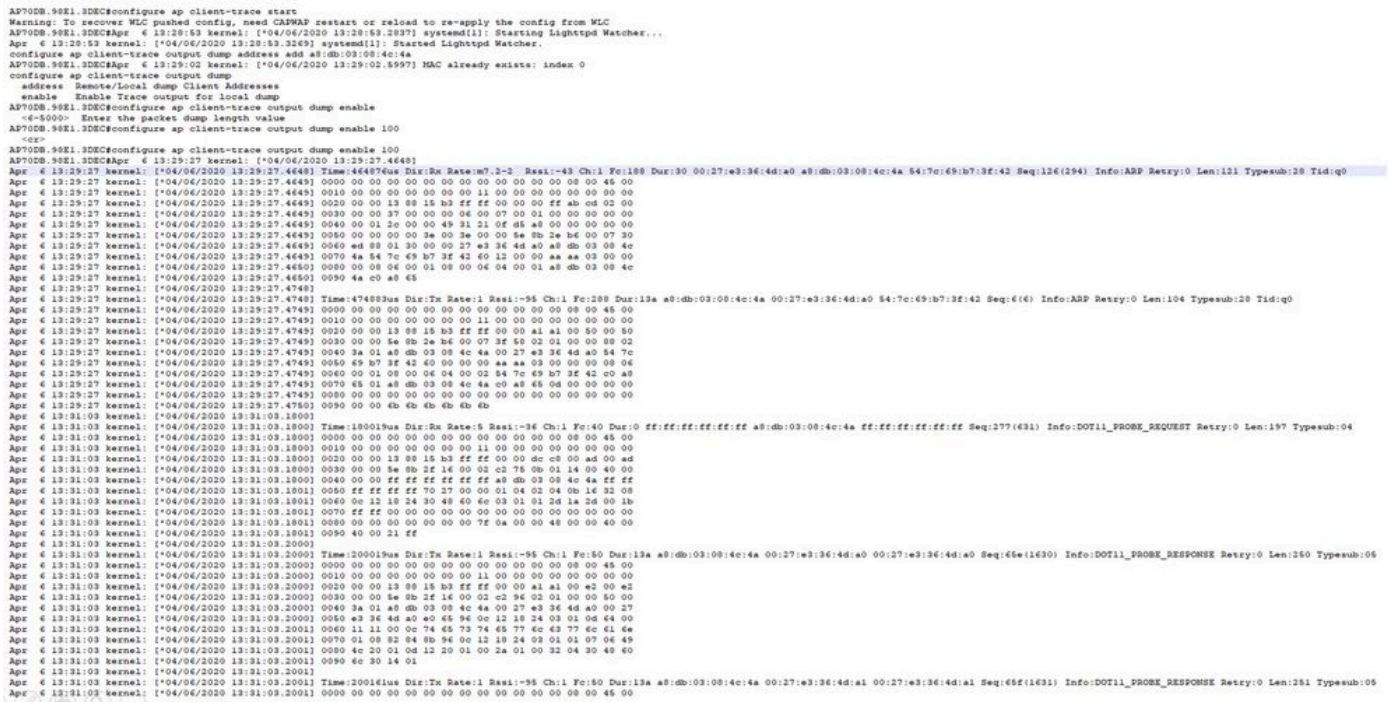
show ap client-trace events mac a8:db:03:08:4c:4a

```
[*04/06/2020 10:11:54.287675] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v1> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:11:54.288144] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:11:54.289870] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:11:54.317341] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:11:54.341370] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M1 : Desc
[*04/06/2020 10:11:54.374500] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M2 : Desc
[*04/06/2020 10:11:54.377237] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M3 : Desc
[*04/06/2020 10:11:54.390255] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M4 : Desc
[*04/06/2020 10:11:54.396855] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.416650] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469089] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469157] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921877] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921942] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:15:36.123119] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DEAUTHENTICAT
[*04/06/2020 10:15:36.127731] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DISASSOC : (.
[*04/06/2020 10:17:24.128751] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.128870] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.129303] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.133026] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:17:24.136095] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:17:24.138732] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M1 : Desc
[*04/06/2020 10:17:24.257295] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M2 : Desc
[*04/06/2020 10:17:24.258105] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M3 : Desc
[*04/06/2020 10:17:24.278937] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M4 : Desc
[*04/06/2020 10:17:24.287459] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.301344] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327482] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327517] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430136] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430202] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:19:08.075326] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_PROBE_REQUEST
[*04/06/2020 10:19:08.075392] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_PROBE_RESPONS
[*04/06/2020 10:19:08.075437] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_PROBE_REQUEST
```

以十六进制格式转储数据包

您可以在CLI中转储十六进制格式的数据包：

```
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
```



```
AP70DB.98E1.3DEC#configure ap client-trace start
Warning: To recover WLC pushed config, need CAPWAP restart or reload to re-apply the config from WLC
AP70DB.98E1.3DEC#Apr  6 13:28:53 kernel: [*04/06/2020 13:28:53.2837] systemd[1]: Starting Lighttpd Watcher...
Apr  6 13:28:53 kernel: [*04/06/2020 13:28:53.3269] systemd[1]: Started Lighttpd Watcher.
configure ap client-trace output dump address add a8:db:03:08:4c:4a
AP70DB.98E1.3DEC#Apr  6 13:29:02 kernel: [*04/06/2020 13:29:02.5997] MAC already exists: index 0
configure ap client-trace output dump
  address  Remote/Local dump Client Addresses
  enable   Enable Trace output for local dump
AP70DB.98E1.3DEC#configure ap client-trace output dump enable
  <6-5000>  Enter the packet dump length value
AP70DB.98E1.3DEC#configure ap client-trace output dump enable 100
  <cr>
AP70DB.98E1.3DEC#configure ap client-trace output dump enable 100
AP70DB.98E1.3DEC#Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4648]
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4648] Time:464876us Dir:Rx Rate:m7.2-2  Rssi:-43 Ch:1 Fc:188 Dur:30 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 54:7c:69:b7:3f:42 Seq:126(294) Info:ARP Retry:0 Len:121 Typesub:28 Tid:q0
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0020 00 00 13 88 15 b3 ff ff 00 00 00 ff ab cd 02 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0030 00 00 37 00 00 00 06 00 07 00 01 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0040 00 01 2c 00 00 49 31 21 0f d5 a8 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0050 00 00 00 00 3e 00 3e 00 00 5e 8b 2e b6 00 07 30
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0060 ed 88 01 30 00 00 27 e3 36 4d a0 a8 db 03 08 4c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0070 4a 54 7c 69 b7 3f 42 40 12 00 00 aa aa 03 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4650] 0080 00 08 06 00 01 08 00 06 04 00 01 a8 db 03 08 4c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4650] 0090 4a c0 a8 65
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4748]
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4748] Time:474883us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:288 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 54:7c:69:b7:3f:42 Seq:6(6) Info:ARP Retry:0 Len:104 Typesub:28 Tid:q0
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 50 00 50
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0030 00 00 5e 8b 2e b6 00 07 3f 50 02 01 00 00 88 02
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 54 7c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0050 69 b7 3f 42 40 00 00 00 aa aa 03 00 00 00 08 06
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0060 00 01 08 00 06 04 00 02 54 7c 69 b7 3f 42 c0 a8
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0070 65 01 a8 db 03 08 4c 4a c0 a8 65 0d 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4750] 0090 00 00 6b 6b 6b 6b 6b 6b
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] Time:180019us Dir:Rx Rate:5 Rssi:-36 Ch:1 Fc:40 Dur:0 ff:ff:ff:ff:ff:ff a8:db:03:08:4c:4a ff:ff:ff:ff:ff:ff Seq:277(631) Info:DOT11_PROBE_REQUEST Retry:0 Len:197 Typesub:04
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0020 00 00 13 88 15 b3 ff ff 00 00 dc c8 00 ad 00 ad
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0030 00 00 5e 8b 2f 16 00 02 c2 75 0b 01 14 00 40 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0040 00 00 ff ff ff ff ff ff a8 db 03 08 4c 4a ff ff
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0050 ff ff ff ff 70 27 00 00 01 04 02 04 0b 16 32 08
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0060 0c 12 18 24 30 48 60 6c 03 01 01 2d 1a 2d 00 1b
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0070 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0080 00 00 00 00 00 00 00 7f 0a 00 00 48 00 00 40 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0090 40 00 21 ff
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] Time:200019us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:50 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:65e(1630) Info:DOT11_PROBE_RESPONSE Retry:0 Len:250 Typesub:05
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 e2 00 e2
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0030 00 00 5e 8b 2f 16 00 02 c2 94 02 01 00 00 b0 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0050 e3 36 4d a0 e0 65 96 0c 12 18 24 03 01 0d 64 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0060 11 11 00 0c 74 65 73 74 65 77 6c 63 77 6c 61 6e
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0070 01 08 82 84 8b 96 0c 12 18 24 03 01 01 07 06 49
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0080 4c 20 01 0d 12 20 01 00 2a 01 00 32 04 30 48 60
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0090 6c 30 14 01
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] Time:200161us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:50 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a1 00:27:e3:36:4d:a1 Seq:65f(1631) Info:DOT11_PROBE_RESPONSE Retry:0 Len:251 Typesub:05
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
```

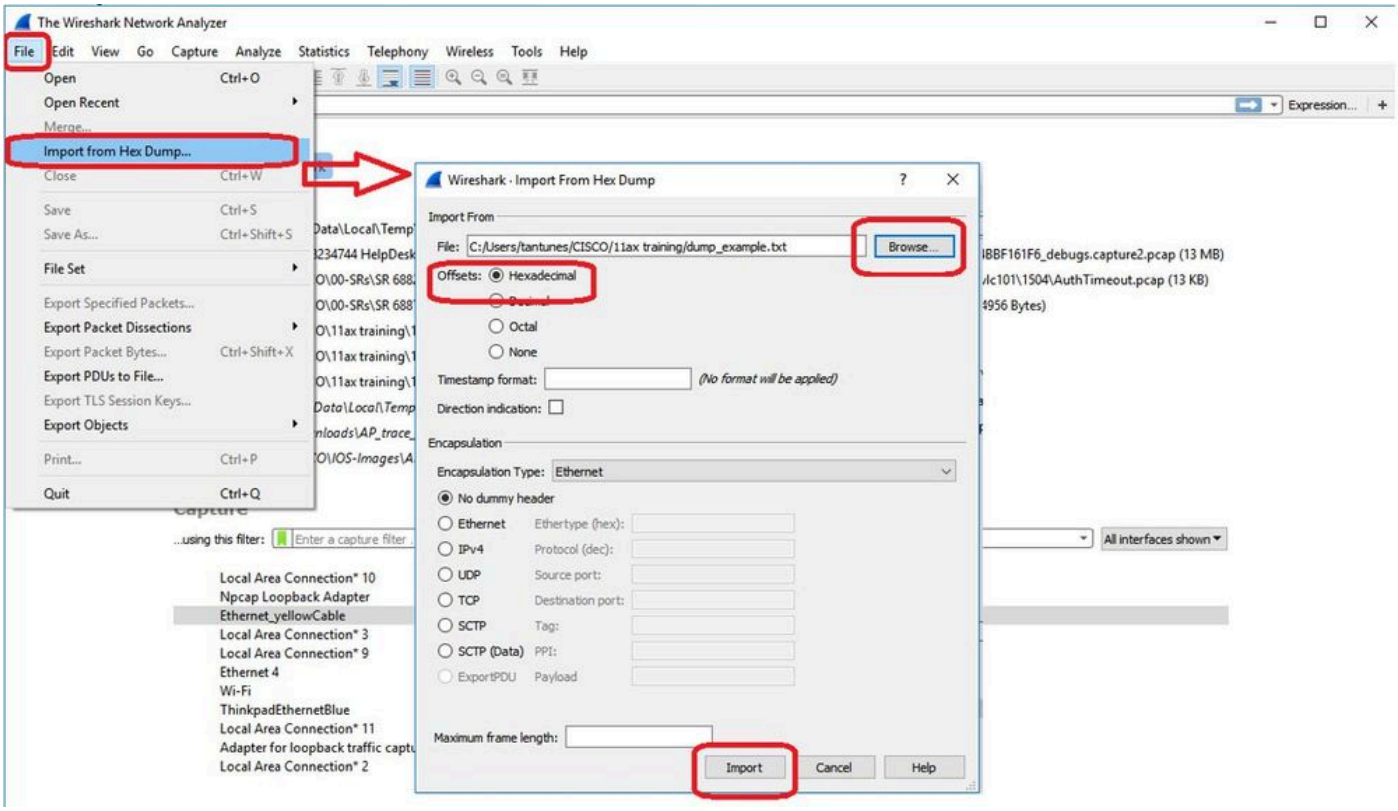
然后，您可以清除十六进制转储并以txt格式保存并导入到wireshark中：

```
Time:20010us Dir:Rx Rate:1 Rssi:-37 Ch:1 Fc:b0 Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:1(1) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 db c8 00 29 00 29
0030 00 00 5e 8b 2f 1f 00 00 57 36 02 01 13 00 b0 00
0040 3a 01 00 27 e3 36 4d a0 a8 db 03 08 4c 4a 00 27
0050 e3 36 4d a0 10 00 00 00 01 00 00 00 dd 09 00 10
0060 18 02 00 00 10 00 00 00 00 00 00 6b 6b 6b 6b 6b
0070 6b

Time:43054us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:d0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66c(1644) Info:DOT11_ACTION Retry:0 Len:54 Typesub:0d
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 1e 00 1e
0030 00 00 5e 8b 2f 1f 00 00 57 b2 02 01 00 00 d0 00
0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
0050 e3 36 4d a0 c0 66 03 02 00 08 01 00 00 00 00 00
0060 6b 6b 6b 6b 6b 6b

Time:43155us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:b0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66d(1645) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 29 00 29
0030 00 00 5e 8b 2f 1f 00 00 5d 06 02 01 00 00 b0 00
0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
0050 e3 36 4d a0 d0 66 00 00 02 00 00 00 dd 09 00 10
0060 18 02 00 00 10 00 00 00 00 00 00 6b 6b 6b 6b 6b
0070 6b

Time:43261us Dir:Rx Rate:1 Rssi:-34 Ch:1 Fc:800 Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:2(2) Info:DOT11_ASSOC_REQUEST Retry:1 Len:220 Typesub:00
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 de cc 00 c4 00 c4
0030 00 00 5e 8b 2f 1f 00 00 8a a1 02 01 12 00 00 08
0040 3a 01 00 27 e3 36 4d a0 a8 db 03 08 4c 4a 00 27
0050 e3 36 4d a0 20 00 31 15 0a 00 00 0c 74 65 73 74
0060 65 77 6c 63 77 6c 61 6e 01 08 82 84 8b 96 24 30
0070 48 6c 32 04 0c 12 18 60 21 02 05 13 24 02 01 0d
0080 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00
0090 00 0f ac 04
```



由于输出可能非常大，并且考虑到输出只提到看到的帧类型，而不提到任何内部细节，因此将数据包捕获重定向到运行捕获应用程序（如wireshark）的笔记本电脑会更有效。

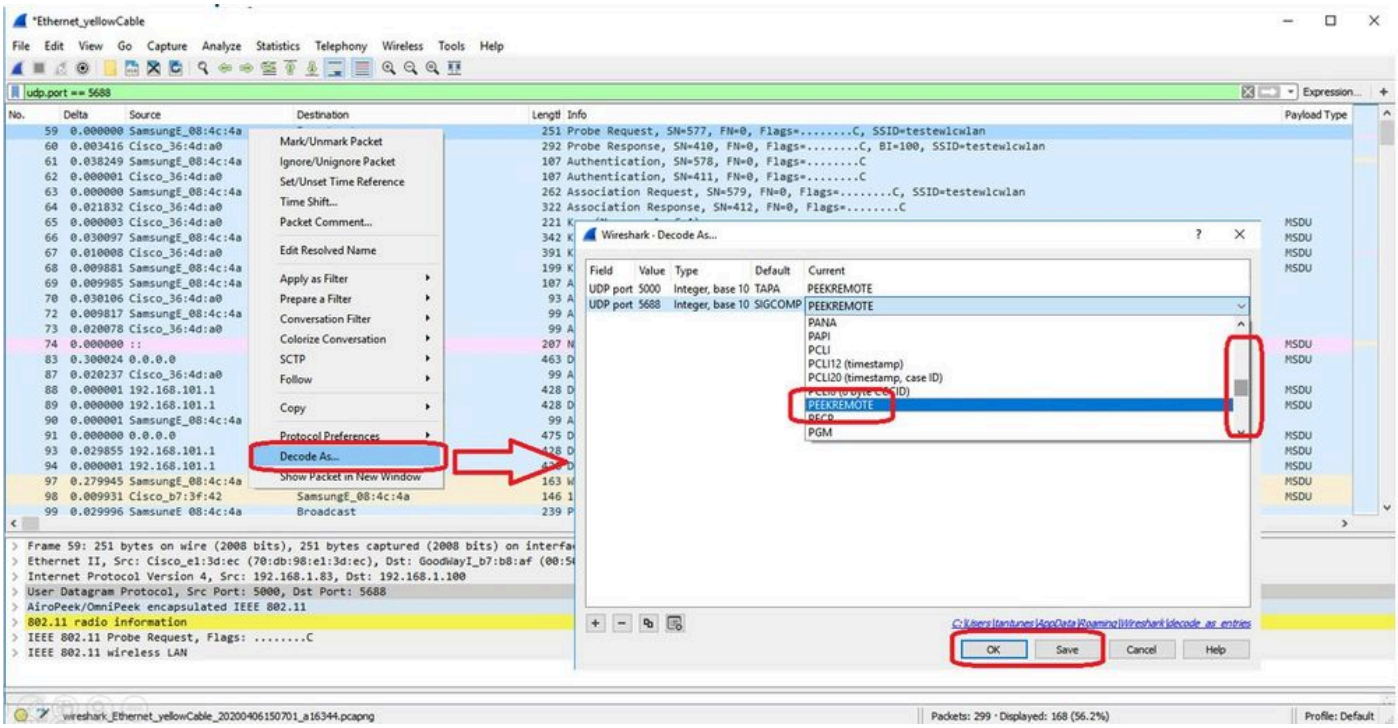
启用远程捕获功能，以通过wireshark将数据包发送到外部设备：

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

此命令意味着AP将客户端跟踪过滤器捕获的每个帧转发到位于192.168.68.68的笔记本电脑，并在端口5000上使用PEEKREMOTE封装（与嗅探器模式中的AP一样）。

一个限制是，目标笔记本电脑必须与您运行此命令的AP位于同一子网中。您可以更改端口号以容纳网络中的任何现有安全策略。

在运行Wireshark的笔记本电脑上收到所有数据包后，您可以右键点击udp 5000报头，然后选择decode as并选择PEEKREMOTE，如下图所示：



有关此功能的错误和增强功能的列表：

Cisco Bug ID CSCvm09020 客户端跟踪在8.8上不再显示DNS

Cisco Bug ID CSCvm09015 客户端跟踪显示多个ICMP_other，序列号为null

Cisco Bug ID CSCvm02676 AP COS client-trace不捕获webauth数据包

Cisco Bug ID CSCvm02613 AP COS客户端跟踪远程输出不起作用

Cisco Bug ID CSCvm00855 客户端跟踪SEQ号不一致

从9800 WLC控制AP客户端跟踪

您可以将多个AP配置为执行无线客户端跟踪并从

步骤1.配置AP跟踪配置文件，定义要捕获的流量

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

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

Step 2. 将AP跟踪配置文件添加到目标的AP使用的AP加入配置文件。

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

确保此AP加入配置文件应用于目标AP使用的站点标记

第4步触发启动/停止

```
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/
```

验证命令:

```
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
```

AP上的客户端调试捆绑包

如果您正在调试一个或多个特定客户端，使用客户端调试捆绑功能可能比收集无线电调试/捕获更容易。

步骤1.确定您要排除的客户端。

```
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
```

步骤2.启动一个或多个客户端MAC地址的调试

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

默认情况下，屏幕上不会打印任何内容。您可以启用terminal monitor并实时查看正在打印的调试，但请注意，这会使终端非常难以使用。收集捆绑包不需要在终端上打印调试。

步骤3.必须先停止调试捆绑包，然后才能上载其输出：

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

步骤4.将捆绑包上传到FTP或SCP服务器（提醒WLC可以充当SCP服务器）

```
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

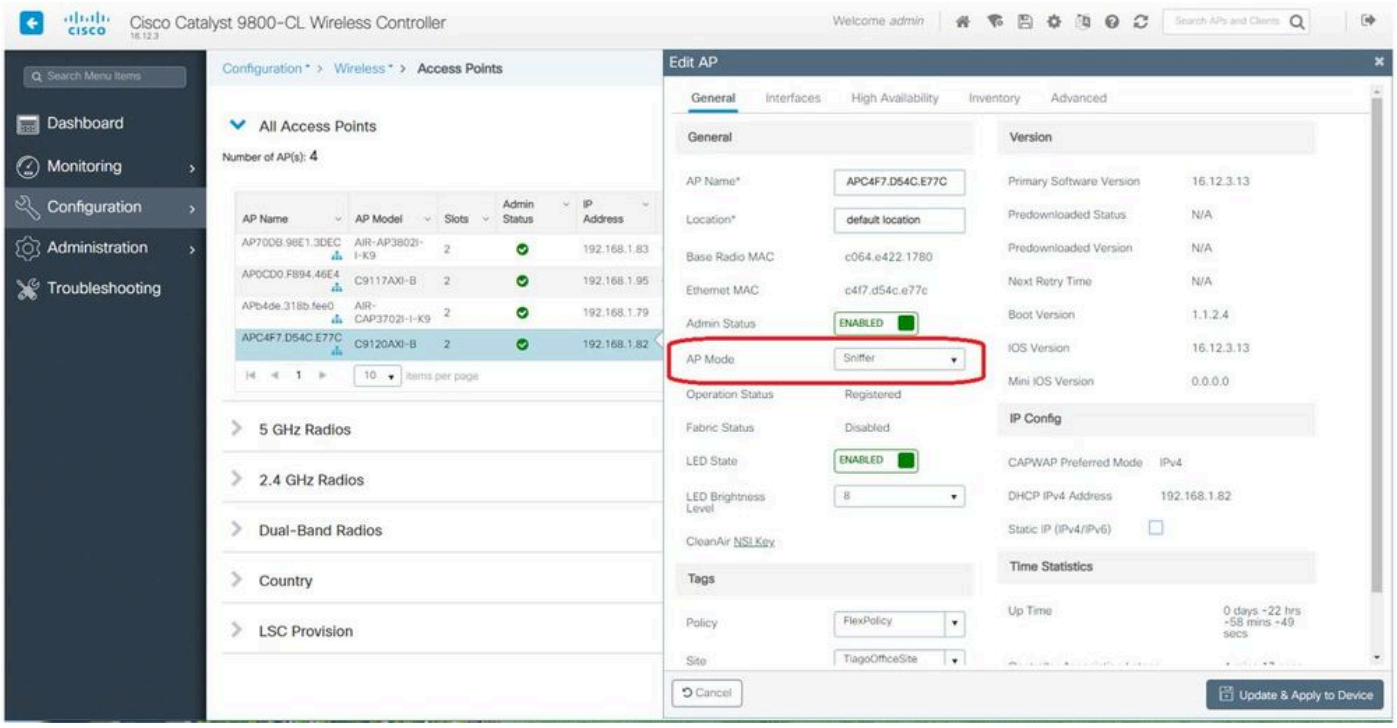
9164#
```

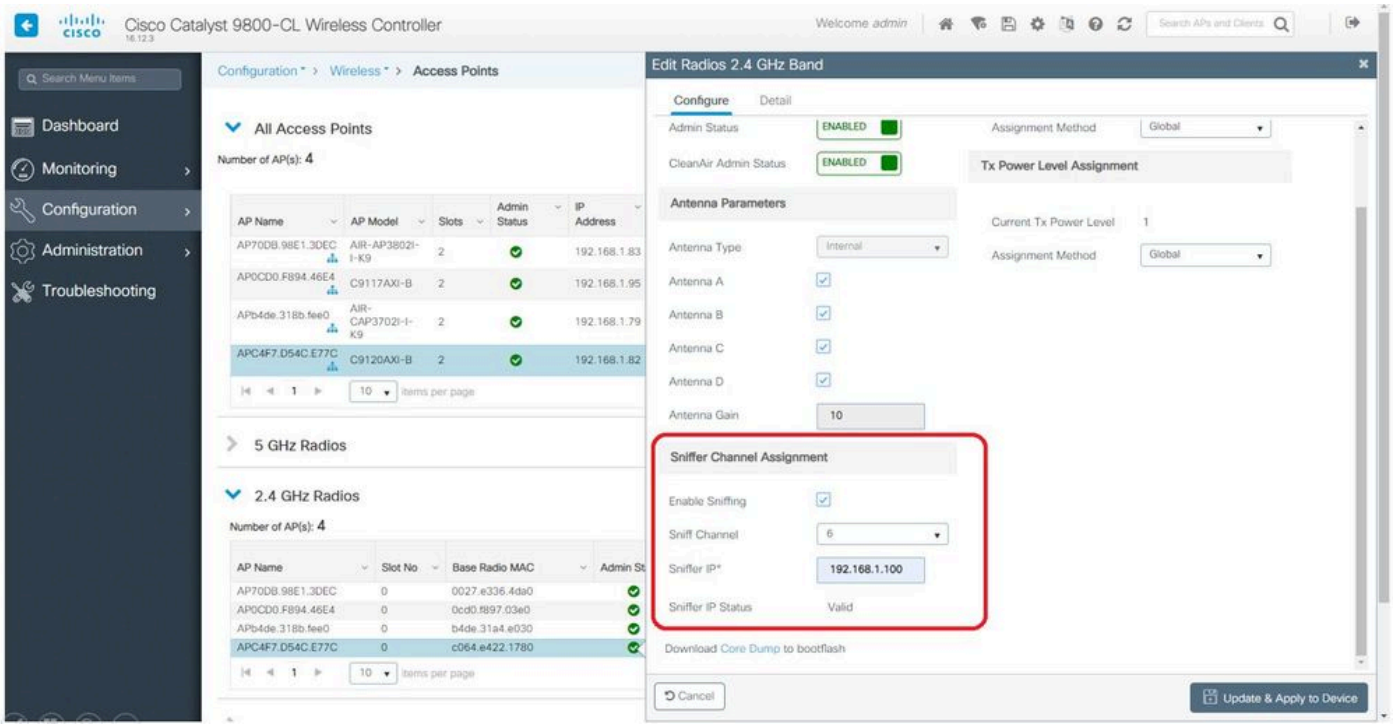
TGZ捆绑包包含4个文件：

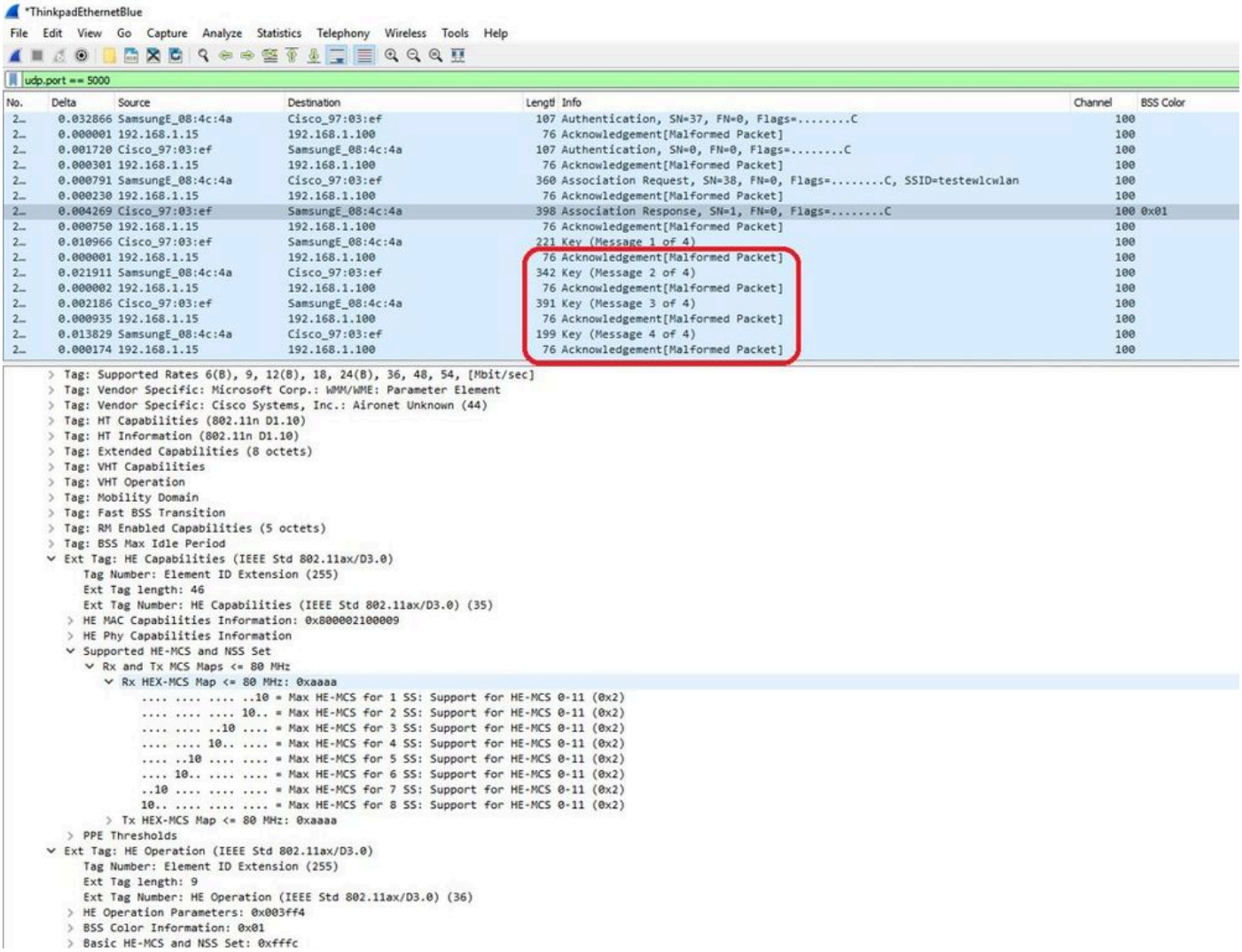
- 2个包含与无线电和客户端相关的show命令
- 1有关实际调试的信息(如果执行term mon，则显示在终端上)
- 1个包含系统日志

嗅探器模式下的AP Catalyst 91xx

新的Catalyst 9115、9117、9120和9130可在嗅探器模式下配置。此过程与之前的AP型号类似。







注意：捕获以WIFI 6数据速率发送的数据帧，但由于peekremote在Wireshark上不是最新的，因此它们现在显示为802.11ax phy类型。修复在Wireshark 3.2.4中，Wireshark显示适当的Wifi6物理速率。

注意：Cisco AP此时无法捕获MU-OFDMA帧，但可以捕获通告MU-OFDMA窗口的触发帧（以管理数据速率发送）。您已经可以推断MU-OFDMA发生（或没有）以及客户端与哪个发生。

故障排除提示

路径MTU

虽然路径MTU发现可找到AP的最佳MTU，但可以手动覆盖此设置。

在AireOS 8.10.130 WLC上，命令config ap pmtu disable <ap/all>为一个或所有AP设置静态MTU，而不是依赖动态发现机制。

要在引导时启用调试，请执行以下操作：

您可以在下次启动时运行config boot debug capwap以启用capwap、DTLS和DHCP调试，甚至在操作系统已启动并显示提示符之前。

您还有“config boot debug memory xxxx”用于几个内存调试。

您可以通过“show boot”查看下次重新启动时是否启用了引导调试。

可以通过在末尾添加disable关键字（例如“config boot debug capwap disable”）来禁用它们。

省电机制

可以通过运行以下命令排除给定客户端的节能故障

debug client trace <mac address>

客户端Qos

要验证是否已应用QoS标记，可以运行“debug capwap client qos”。

它显示无线客户端的数据包的UP值。

从8.8开始，它不能进行mac过滤； 增强请求Cisco bug IDCSCvm08899 影响。

```
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
```

您还可以验证AP上的Qos UP to DSCP表以及Qos标记、整形和丢弃的数据包总数：

```
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#
```

在WLC上定义Qos策略并在Flexconnect AP上下载时，可以使用进行验证：

```
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
```

对于Qos速率限制：

```
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_burs
A8:DB:03:6F:7A:46   2           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
```

信道外扫描

在排除欺诈检测故障时（验证AP是否和何时进入要扫描的特定信道）调试AP的信道外扫描非常有用，但在未使用“信道外扫描延迟”功能时，如果敏感实时流不断中断，则调试信道外扫描也非常有用。

```
debug rrm off-channel defer
debug rrm off-chanel 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 dot_11 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
```

客户端连接

可以使用最后一个事件时间戳列出已经由接入点取消身份验证的客户端：

```
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
```

在上一个输出中，原因代码是取消身份验证原因代码，如以下链接中所述：

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

vap是指AP内部WLAN的标识符(不同于WLC路由器上的WLAN !!!)。

您可以将其与随后详细描述的其他输出交叉关联，这些输出始终提及关联客户端的vap。

您可以使用“show controllers Dot11Radio 0/1 wlan”查看VAP ID列表。

当客户端仍然关联时，您可以获取有关其连接的详细信息：

```
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
```

有关客户端条目的更多详细信息，可以通过：

```
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
```

您可以使用强制断开特定客户端的连接：

```
test dot11 client deauthenticate
```

可以使用以下方式为每个客户端获取流量计数器：

```
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#
```

在无线电级别上，很多信息可以在“show controllers”中获得。 添加客户端mac地址时，将显示支持的数据速率、当前数据创建量、PHY功能以及重试次数和失败次数：

<#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
```

为了持续跟踪客户端数据速率和/或RSSI值，您可以运行“debug dot11 client rate <mac>”，此命令每秒记录一次以下信息：

```
LabAP#debug dot11 client rate 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
```

在此输出中，Tx和Rx数据包计数器是自上次打印以来的第二个间隔中传输的数据包，与Tx重试相同。但是，RSSI、SNR和数据速率是该间隔的最后一个数据包的值（而不是该间隔中所有数据包的平均值）。

Flexconnect方案

您可以在身份验证前（例如CWA）或身份验证后方案中验证当前应用于客户端的ACL:

```
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
```

通过启用debug flexconnect access-list counter client <client MAC>，您可以看到Flexconnect ACL上的命中计数器

后续执行show client access-list pre-auth/post-auth all <MAC> 然后为每个ACL条目添加命中计数器。这适用于自Cisco IOS® XE 17.13起的所有类型的flex ACL。在早期版本中，存在相同的命令，但只有VLAN ACL更新其命中计数器。

可以使用clear counters access-list client <mac>

AP文件系统

COS AP不允许在unix平台上列出文件系统的所有内容。

命令“show filesystems”提供当前分区上的空间使用情况和分布的详细信息：

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

命令“show flash”列出了AP闪存上的主文件。您还可以附加syslog或core关键字以列出这些特定文件夹。

```
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.oeap
-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
```

存储和发送系统日志

syslog文件夹存储先前重新启动的syslog输出。命令show log仅显示自上次重新启动后的系统日志。

在每个重新启动周期中，系统日志会写入增量文件。

```
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
```

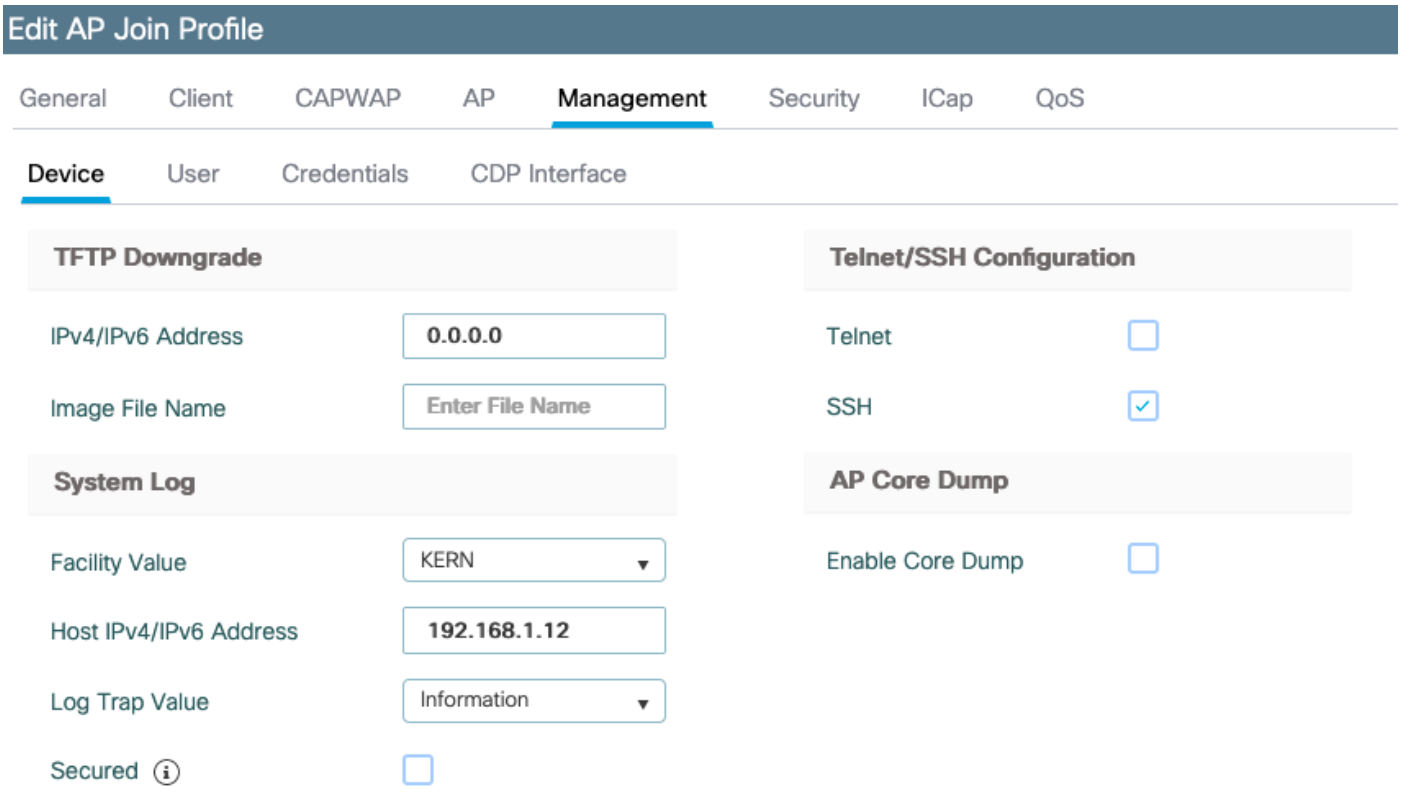
初始启动后的第一个输出是文件1.0，如果1.0过长，则会创建文件1.1。重新启动后，将创建一个新文件2.0，以此类推。

如果希望AP将其系统日志消息单播发送到特定服务器，可以从WLC配置系统日志目标。

默认情况下，AP将其syslog发送到可能导致相当多的广播风暴的广播地址，因此请确保配置syslog服务器。

默认情况下，AP通过syslog发送其控制台输出上打印的任何内容。

在9800控制器上，您可以在Management下的Configuration -> AP Join配置文件中更改这些参数。



您可以更改Log Trap Value，以便也通过syslog发送调试。然后，您可以在AP CLI上启用调试，这些调试的输出通过syslog消息发送到配置的服务器。

由于Cisco Bug ID CSCvu75017 ，只有当您将syslog设施设置为KERN（默认值）时，AP才会发

送syslog消息。

如果您正在排除AP可能失去网络连接（例如，在WGB上）的问题，则系统日志不如在AP失去上行链路连接时发送消息那么可靠。

因此，依靠闪存中存储的系统日志文件是调试和存储AP本身输出并在稍后定期上传输出的好方法。

AP支持套件

一些通常收集的各种类型的诊断信息可在单个捆绑包中提供，您可以从接入点上传。

可以包含在捆绑包中的诊断信息包括：

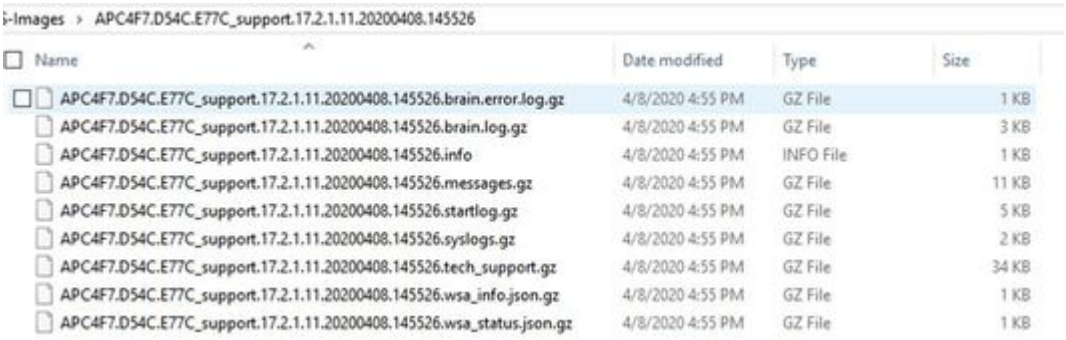
- AP show tech
- AP系统日志
- AP Capwapd大脑日志
- AP启动和消息日志
- AP核心转储文件

要获取AP支持捆绑包，您可以进入AP CLI并输入命令copy support-bundle tftp:x.x.x.x”。

之后，您可以检查名为AP名称并附加了support.apversion.date.time.tgz的文件，如下所示：

```
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#
```

当您“解压缩”该文件时，可以查看收集的各种文件：



远程收集AP核心文件

要远程收集AP核心文件，请启用要包含在支持捆绑包中的核心转储，然后从AP上传支持捆绑包，或直接发送到tftp服务器。后续示例使用tftp服务器192.168.1.100。

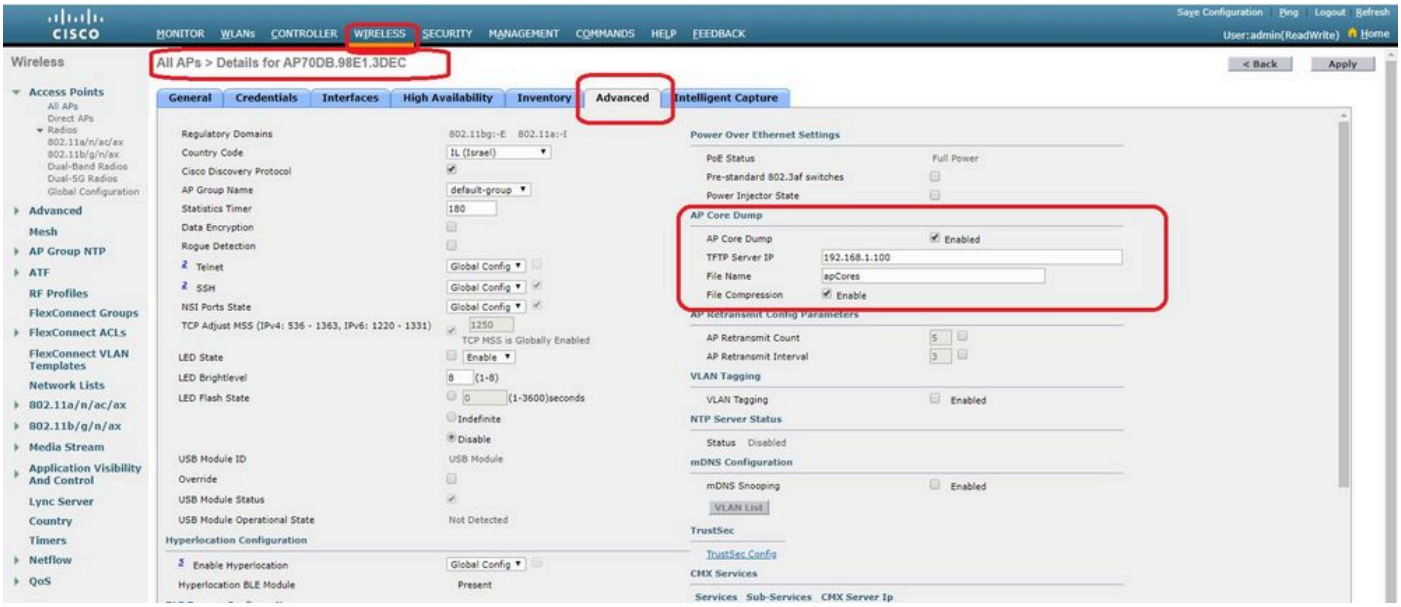
AireOS CLI

```
(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.
```

AireOS GUI



Cisco IOS® CLI

```
<#root>

eWLC-9800-01(

config

)#ap profile TiagoOffice
eWLC-9800-01(

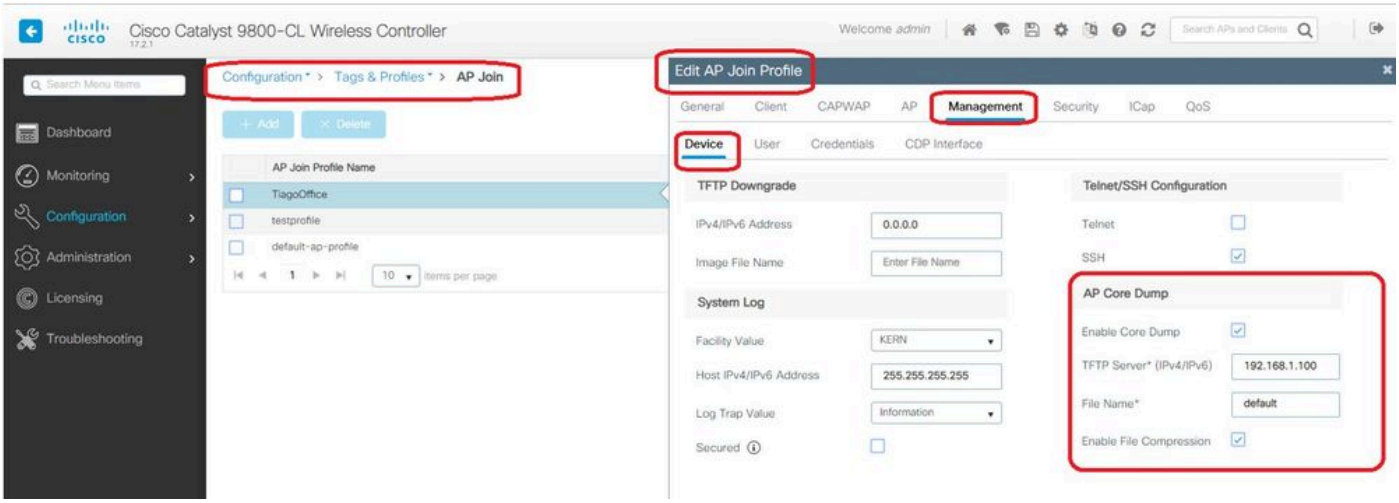
config-

ap

-profile

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

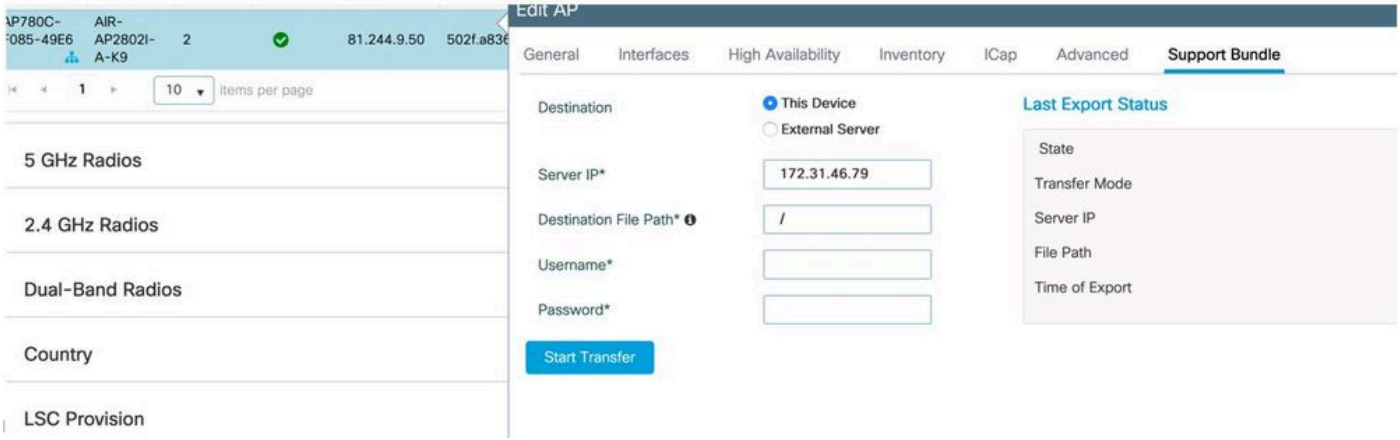
Cisco IOS® GUI



从Cisco IOS® XE 17.3.1，您有一个支持捆绑包选项卡，可以从WLC GUI下载AP SB。

它所做的只是在AP上执行“copy support-bundle”命令并通过SCP将其发送到WLC（因为WLC可以是SCP服务器）。

然后，您可以从浏览器下载：



这意味着，您可以在17.3.1之前的eWLC版本中手动执行相同的技巧：

如果您没有可连接到AP的TFTP服务器，请通过SCP将支持捆绑包从AP复制到eWLC IP。

eWLC通常通过SSH从AP到达，因此对于17.3之前版本来说这是一个不错的技巧。

步骤1.在9800 v17.2.1上启用SSH

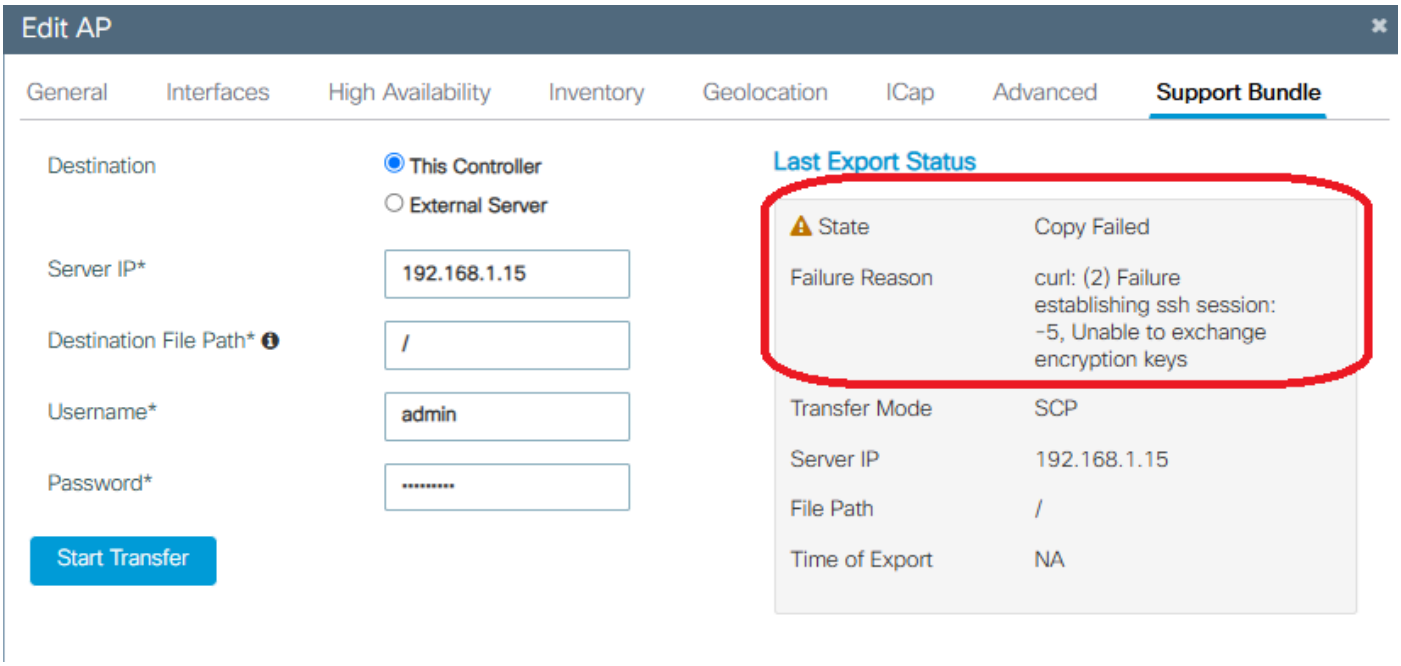
步骤2.在Cisco IOS® XE v17.2.1上启用SCP

此示例说明如何配置SCP的服务器端功能。此示例使用本地定义的用户名和密码：

```
! 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
```

在WLC IOS-XE 17.10.1之后，AP和WLC之间的默认加密算法不匹配，原因是 CSCwb68238 由CSCwn解决34344 17.15.4。

错误消息为："9120-AP的支持捆绑复制失败。理由：卷发：(2)建立ssh会话失败：-5，无法交换加密密钥":

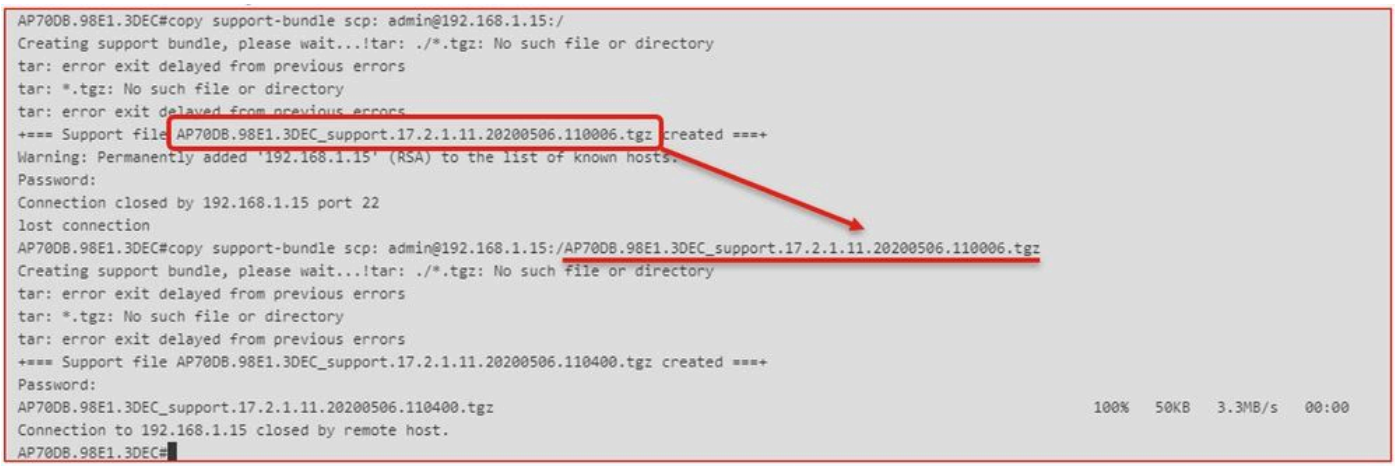


如果您看到此消息，请输入命令ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com。

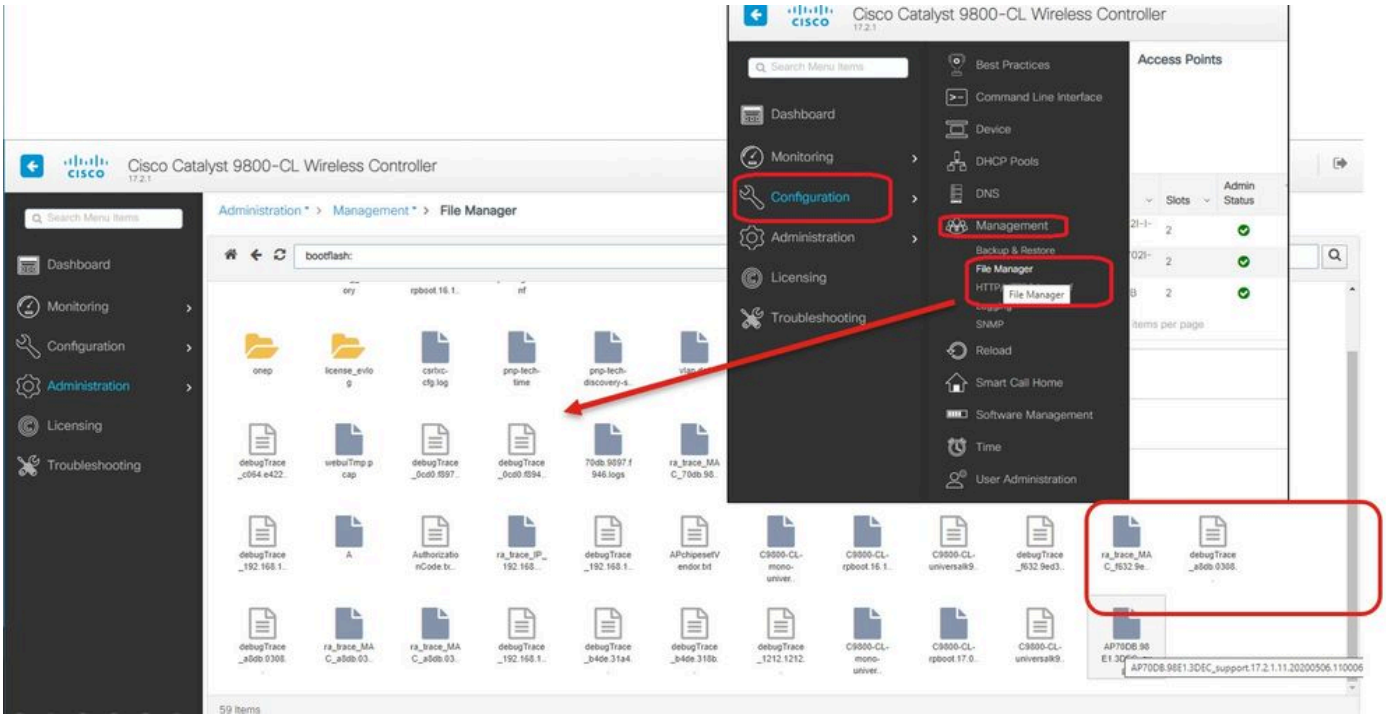


步骤3.使用命令copy support-bundle，我们需要指定要在SCP服务器中创建的文件名。

提示：您可以运行一次命令以获取有意义的文件名，然后在命令中复制/粘贴该文件名：



步骤4.然后进入eWLC GUI并获取以下文件：管理>管理>文件管理器:



物联网和蓝牙

可以在AP上使用检查gRPC服务器日志：

```
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 +00
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 "
```

可以通过验证与Cisco DNA Spaces连接器的连接：

```
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
Connection Retry Interval : 30
```

```
AP# show cloud connector connection detail
Connection State           : READY
Connection Url             :  10.22.243.33:8000
Certificate Available      :  true
Controller Ip              :  10.22.243.31
Stream Setup Interval      :  30
Keepalive Interval         :  30
Last Keepalive Rcvd On     :  2020-04-01 00:32:47.891433113 +0000 UTC m=+345985.338898246
Number of Dials               :  2
Number of Tx Pkts             :  2788175
Number of Rx Pkts             :  11341
Number of Dropped Pkts        :  0
Number of Rx Keepalive        :  11341
Number of Tx Keepalive        :  11341
Number of Rx Cfg Request      :  0
Number of Tx AP Cfg Resp      :  0
Number of Tx APP Cfg Resp     :  0
Number of Tx APP state pkts   :  5
Number of Tx APP data pkts    :  2776829
```

要查看AP的当前BLE广播配置：

```
AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config
------------------
Active profile           : v-iBeacon
Profile 0 (iBeacon)
UUID                     : 00001000000000000000000000000000
Interval (ms)            : 100
Power (dBm)              : -21
Advertised Power (dBm)   : -65
Minor                    : 0
Major                    : 0
TxPower byte             : bfbfbfbfbfbfbfbfbfbfbfbfbf

Profile 1 (Eddystone UID)
Namespace (hex)          : 00000000000005446089c
Instance-ID (hex)        : 7f0000001f00

Profile 2 (Eddystone URL)
URL                      : http://www.
```

要查看扫描结果，请执行以下操作：

```
AP# show controllers ioTRadio ble 0 scan brief
      Profile               MAC  RSSI(-dBm)  RSSI@1meter(-dBm)        Last-heard
      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
```

当AP在部署应用的高级BLE网关模式下工作时，您可以使用检查IoX应用的状态：

```
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
```

您可以使用以下命令连接到IOX应用，然后在楼层信标配置期间监控日志：

```
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
```

结论

有许多故障排除工具可以帮助我们解决与COS AP相关的问题。

本文档列出了最常用的文档，并会定期更新。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。