

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[控制器组件问题](#)

[IDS签名](#)

[美洲台](#)

[OEAP](#)

[基于规则的恶意分类](#)

[恶意遏制](#)

[IDS签名](#)

[RLDP](#)

[诊断信道](#)

[相互控制器移动性](#)

[蜂蜜AP](#)

[AirMagnet集成](#)

[本地认证](#)

[控制器调试](#)

[一般AAA认证](#)

[TACACS+](#)

[LDAP](#)

[客户端管理帧保护\(MFP\)](#)

[移动性](#)

[报告问题](#)

[FIP相关问题](#)

[使用本地验证器的无线客户端以EAP-TLS、EAP-FAST和PEAP](#)

[512 WLANs/AP组](#)

[ACL, 前验证ACL和CPU ACL](#)

[DHCP](#)

[访客访问相关问题](#)

[WLC高可用性问题](#)

[控制器H-REAP相关问题](#)

[媒体流](#)

[位置相关问题](#)

[系统内存, 在内存问题外面](#)

[Mesh相关问题](#)

[与NTP客户机的问题和在控制器的时间配置](#)

[RF WLCs的组件问题](#)

[WLCs的SNMP组件](#)

[与TFTP加载/下载的问题包括升级/降级](#)

[Web WLCs的GUI组件](#)
[Webauth设置和验证问题](#)
[WLC Webauth模板](#)
[控制器XML设置相关问题和增强](#)
[诊断信道](#)
[动态信道分配](#)
[TACACS+](#)
[WLC组播指南](#)
[WLC QoS指南](#)
[呼叫控制\(SIP分类\)调试](#)
[负载根据准入控制和语音量度](#)
[WLC许可证指南](#)
[ARP问题](#)
[网络问题](#)
[其他](#)
[接入点问题](#)
[IAPP](#)
[WGB关联问题](#)
[WGB或有线的客户端没获得DHCP地址](#)
[WGB或有线的客户端用途静态IP地址，然而IP地址不出现在控制器](#)
[AP Username password](#)
[客户端连接问题](#)
[客户端调试](#)
[控制器不类似关联申请](#)
[客户端不回答EAP请求](#)
[CCKM漫游发生故障](#)
[PMKID高速缓冲存储发生故障](#)
[Reauth问题](#)
[漫游的802.11R \(快速转换\)不工作](#)
[相互控制器移动性](#)
[禁用的调试](#)
[相关信息](#)

[简介](#)

本文提供关于可用排除故障无线局域网控制器的Debug与Show调试指令的信息(WLCs)。

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

[使用的组件](#)

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

控制器组件问题

IDS签名

- 调试wips信号enable (event)

美洲台

- debug nac事件enable (event)
- debug nac数据包enable (event)

OEAP

控制器显示命令

- 显示ap加入stats详细信息<ap mac add>
- 显示h收割摘要
- 显示h收割延迟
- 显示ap林克加密
- 显示ap数据平面

AP侧显示/调试

- show logging
- 显示lwapp/capwap客户端rcb
- 显示lwapp/capwap客户端设置
- 测试lwapp/capwap iapp数据响应
- 调试lwapp/capwap iapp数据响应
- 显示lwapp/capwap收割
- show controller

基于规则的恶意分类

收集的调试

- 调试dot11歹徒规则enable (event)

采取的捕获

不可适用。

[配置并且显示输出收集](#)

- show rogue rule summary
- 显示恶意规则被选派的<rule>
- 请显示恶意ap被选派的<rogue-mac> (如果一个特定的歹徒错误分类)

[欺诈遏制](#)

确保那里是在非法接入点的(AP)网络配置的DHCP服务器使用，如果使用静态IP寻址。

[收集的调试](#)

- 调试dot11歹徒enable (event)

[采取的捕获](#)

在恶意信道的Airopeek trace。

注意：密切注意不相关帧。

[配置并且显示输出收集](#)

- 显示恶意ap被选派的<contained rogue-mac>
- 显示ap从上述command>的设置802.11b/a <Ap NAME

[IDS签名](#)

如果使用，请确保那里是在非法AP的网络配置的DHCP服务器能使用静态IP寻址。

[收集的调试](#)

- 调试wips信号enable (event)

[采取的捕获](#)

在检测的信道签名的Airopeek捕获。

[收集的Debug与Show输出](#)

在5.2前的软件方面，应该在CAPWAP位置使用LWAPP这些命令：

- 显示capwap ID信号转储-转存签名和签名检测命中数统计包括MAC地址与最大命中数。并且包括IDS包跟踪当前状态。
- 显示capwap ID歹徒遏制<slot-> chan -显示恶意遏制请求当前列表在此AP。遏制请求由信道分组。
- 显示capwap ID歹徒遏制<slot-> rad -显示恶意遏制请求当前列表在此AP。此列表对应于请求列表如接收从控制器。

- **调试capwap ID信号**-打开IDS签名和遏制检测的调试。
- **测验capwap ID trace匹配<message type-name>** -启用跟踪消息type=<message type-name> IDS签名检测模块接收的所有信息包的;<message跟踪所有消息类型的type-name> = FF。在第8.2.1部分的签名调试需要打开安排跟踪的数据包显示。
- **测验capwap ID trace rcv <type-name>** -启用跟踪匹配消息type=<message type-name> IDS签名检测模块的所有当前安装的签名的所有信息包的;<message跟踪匹配签名的所有消息类型的type-name> = FF。在第8.2.1部分的签名调试需要打开安排跟踪的数据包显示。

[RLDP](#)

[收集的调试](#)

在WLC :

- 调试dot11 rldp enable (event)

在AP :

- 调试lwapp客户端mgmt

[采取的捕获](#)

在恶意信道的Airopeek捕获。

[配置并且显示输出收集](#)

- 配置恶意ap rldp启动<rogue-mac>

[诊断信道](#)

[收集的调试](#)

- 调试客户端<client mac>
- 调试ccxdiag全部启用

[采取的捕获](#)

在AP设置的信道的Airopeek捕获。因为信标和探测器req/响应数据包可以未命中，推荐避免过滤。

[配置并且显示输出收集](#)

- 显示sysinfo
- 显示WLAN x
- 显示运行设置
- show tech-support
- show debug
- show msglog

- 显示客户端摘要
- 显示客户端详细信息<client mac>

客户端详细信息

- 客户端硬件
- 请求方软件细节例如软件版本、在ADU的情况下软件名字(例如， Aironet Desktop软件[ADU]或冒险旅行)和驱动版本
- 客户端操作系统(OS)

相互控制器移动性

收集的调试

- 调试客户端在两WLCs的<client mac>
- 调试移动性在两WLCs的移交enable (event) (请确保记住命令：首先总是请启用调试客户端。)
- Debug pem state enable

如果移动性控制路径或数据发生故障那么请打开‘调试移动性Keepalive enable (event)’在两交换机(请记录下来软件版本运行在两个控制器)。

如果地址解析服务(ARP)不工作，打开？ debug arp全部启用？在两交换机上。

如果DHCP不工作，打开？ debug dhcp消息enable (event) ？并且？ debug dhcp数据包enable (event) ？在两交换机上。

如果IPSec是包含的：调试下午SA出口enable (event)，调试下午SA导入enable (event)。

如果客户端在一会儿以后连接，请指示多长时间需要了。

采取的捕获

根据漫游类型的捕获，例如CCKM、PMKID或者TGR。

配置并且显示输出收集

同[客户端连接问题](#)并且这些一样：

- 显示PMK缓存<client mac> (在目标控制器)
- 请显示客户端详细信息<client mac> (当客户端在旧有AP连接)时
- 显示移动性摘要(在两WLCs)

客户端详细信息

同特定的漫游类型一样，例如CCKM、PMKID或者TGR。

蜂蜜AP

收集的调试

采取的捕获捕获活信道的Airopeek trace陷阱接收为了确认歹徒使用思科的SSID。

[配置并且显示输出收集](#)

- 显示traplog

[AirMagnet集成](#)

[收集的调试](#)

在NMSP相关问题的WLC :

- 调试wips nmsp enable (event)
- 调试wips事件enable (event)
- 调试wips错误enable (event)

CAPWAP相关问题 :

- 调试wips事件enable (event)
- 调试wips错误enable (event)
- debug iapp错误enable (event)
- debug iapp事件enable (event)

损坏的报警/设备报告信息 :

- 调试wips全部启用

在AP :

- 调试capwap上午事件
- 调试capwap上午错误

[采取的捕获](#)

- 攻击的Airopeek捕获
- 报告的Ethereal捕获(被发送作为数据包)

[配置并且显示输出收集](#)

在AP :

- 显示capwap上午stats
- 显示capwap上午缓冲区[run it few times]
- 显示capwap上午策略[alarm-id]
- 显示capwap上午报警[alarm-id]

[本地 认证](#)

[检查的事，在您记录Bug前](#)

确保客户端能联合到WLAN。如果客户端不能，则问题在级的dot1x。如果曾经证书，请确保那里是设备和在WLC安装的CA证书。并且，请确保您选择在本地验证设置的正确证书发布者为了选择正

确套在WLC的证书。

如果曾经本地数据库用户凭证，请检查用户名在数据库存在。欲知更多调试信息，如果曾经轻量级目录访问协议(LDAP)，请参阅[调试的LDAP](#)部分。

[收集的调试](#)

WLC :

- debug aaa local-auth eap框架错误enable (event)
- debug aaa local-auth eap方法误差enable (event)
- debug aaa local-auth eap method events enable
- debug aaa local-auth eap方法sm enable (event)
- debug aaa本地验证db enable (event)
- debug aaa本地验证填充码enable (event)

[配置并且显示输出收集](#)

- 显示本地验证设置
- 显示本地验证统计信息
- 显示本地验证证书(如果使用可扩展的认证协议[EAP]方法以证书)

[客户端详细信息](#)

客户端种类，加上指示的EAP配置细节哪个方法选择，并且什么参数为在客户端的该方法设置。并且，任何错误消息文本被看到在客户端。

[控制器调试](#)

- 调试下午pki enable (event) ? 在证书确认的详细信息。
- debug aaa事件enable (event) ? 如果有任何authorization list相关问题，这帮助。
- 显示证书lsc摘要? 任何lsc相关摘要。

[一般AAA认证](#)

这些调试为调试RADIUS验证、授权或者核算问题是有用：

[收集的调试](#)

- 调试客户端<client mac> ? 提供关于reauth如何的信息涉及属性，例如session-timeout和操作类型，应用。
- debug aaa事件enable (event) ? 帮助排除故障不同的AAA服务器如何使用验证、核算和授权。
- debug aaa数据包enable (event) ? 帮助排除故障什么不同的AAA属性接收并且应用。

[采取的捕获](#)

如果上述调试不指示问题，一个有线的捕获可以收集在控制器和RADIUS服务器之间。

[配置并且显示输出收集](#)

同[客户端连接问题](#)并且此一样：

- show radius摘要

[客户端详细信息](#)

同[客户端连接问题](#)一样。

[TACACS+](#)

[收集的调试](#)

- debug aaa TACACS enable (event) (在WLC请收集日志在核算的ACS/RADIUS服务器)
- debug aaa事件
- debug aaa详细信息
- 调试dot11移动
- 调试dot11状态
- 调试pem事件
- 调试pem状态

[采取的捕获](#)

如果上述调试不指示问题，一个有线的捕获可以收集在控制器和RADIUS服务器之间。

[配置并且显示输出收集](#)

- show tacacs summary
- 授权(CoA)和断开信息包(PD)问题更改- RFC 3576
- show radius摘要

[LDAP](#)

[检查的事，在您记录Bug前](#)

确保LDAP服务器从WLC是可ping通的。

如果曾经活动目录和本地EAP验证，不支持这些EAP方法：

- LEAP
- EAP-FAST MSCHAPv2
- PEAP MSCHAPv2

这归结于的活动目录能返回能使用MSCHAPv2验证的明文密码。

[收集的调试](#)

- debug aaa ldap enable (event)

如果问题发生，当使用LDAP以本地认证，为更多调试参见[本地认证](#)部分。

[配置并且显示输出收集](#)

- show ldap summary
- show ldap <server no.>
- show ldap统计信息
- 请显示本地验证统计信息(如果问题发生，当使用LDAP以本地EAP验证)

[客户端管理帧保护\(MFP\)](#)

[所有问题](#)

- 调试wps mfp客户端
- show wps mfp摘要

[配置并且显示输出收集](#)

- show wps mfp统计信息

[配置问题](#)

控制器调试：

- 调试wps mfp lwapp
- 调试lwapp mfp (在Aironet AP)

[客户端不联合](#)

控制器调试：

- 调试wps mfp客户端
- 调试wps mfp详细信息
- 调试pem状态
- 调试pem事件
- debug dot1x事件

配置并且显示输出收集：

- show msglog
- 显示客户端详细信息

[其他1130/1240 AP调试，当客户端不联合](#)

- debug dot11 mgmt msg
- 调试dot11 aaa管理器所有(H-REAP独立模式)

[Aironet AP调试，当客户端在H-REAP独立模式不联合](#)

- 调试dot11 mfp客户端
- debug dot11 mgmt msg
- 调试dot11 mgmt接口
- 调试dot11 mgmt站点
- 调试dot11 supp-sm-dot1x
- 调试dot11 aaa管理器全部
- 调试dot11 wpa-cckm-km-dot1x

[移动性](#)

[控制器调试](#)

- 调试wps mfp分enable (event)
- 调试移动性目录

[配置并且显示输出收集](#)

- 显示移动性摘要
- show mobility statistics

[报告问题](#)

[控制器调试](#)

- 调试wps mfp报告

[配置并且显示输出收集](#)

- show wps mfp统计信息**注意**：在错误生成之后，必须调用。

[FIP相关问题](#)

当控制器在联邦信息处理标准(FIP)模式安置，只有可以使用已批准密码功能。结果，您必须锁起来SSL以AES密码器使用TLS_RSA验证算法。

[不能进入引导程序菜单](#)

这是FIP的一个功能。使用此命令，功能启用：

[不能下载新建的镜像](#)

这是FIP的一个功能。当BOOT工间休息时间禁用以上时，转移禁用。

[使用本地验证器的无线客户端以EAP-TLS、EAP-FAST和PEAP](#)

[收集的调试](#)

根据在麻烦的通信，这些调试可以启用：

- 调试wps cids enable (event)
- 调试locp事件enable (event)
- 调试emweb服务器enable (event)
- debug aaa local-auth eap method events enable

[采取的捕获](#)

在WLC和设备之间的嗅探器跟踪有问题的。

注意：当相关服务开始，WLC能开始通信。在WLC启动前，推荐启动嗅探器。

[配置并且显示输出收集](#)

- 显示switchconfig

[512 WLANs/AP组](#)

[512 WLAN](#)

—512 WLAN bug是，如果客户端能连接到‘默认组’AP，但是不能连接到AP设置为自定义AP组。

显示输出收集在控制器：

- 显示sysinfo
- show running-config
- 显示WLAN摘要
- 显示WLAN apgroup
- show msglog

显示输出收集在AP：

- show controller
- 显示capwap客户端mn
- show log

收集的调试：

- 调试客户端xx:xx : xx : xx : xx : xx
- 调试组enable (event)
- 调试capwap事件

注意：应该在发出**调试客户端**<client mac>命令以后交换这些调试或其他调试。此命令造成所有上一个调试禁用。

收集的Trace：

- 无线trace

[AP组](#)

与添加或删除AP组或者添加接口涉及的任何问题到AP组。

显示输出收集：

- 显示sysinfo
- show running-config
- 显示WLAN摘要
- 显示WLAN apgroup
- show msglog

收集的调试：

- 调试组enable (event)

[ACL，前验证ACL和CPU ACL](#)

[DHCP](#)

[Debug dhcp带内](#)

- debug dhcp message enable
- debug dhcp packet enable

[服务端口Enable \(event\)的Debug dhcp](#)

- debug dhcp服务端口enable (event)

[访客访问相关问题](#)

[访客WLAN](#)

- 调试移动性移交enable (event)
- debug pem events enable
- debug pem state enable

DHCP问题：

- debug dhcp packet enable
- debug dhcp message enable

移动连接问题：

- 调试dot11事件enable (event)
- 调试dot11移动enable (event)

RADIUS/AAA问题：

- debug dot1x aaa enable

[WLC高可用性问题](#)

[AP故障切换](#)

配置问题

收集并且检查这些配置文件：

- 所有涉及WLC配置文件？显示运行设置和show running-config。
- AP故障切换优先级配置？
- 每AP主要的WLC (“主要的Cisco交换机[名称]在“AP设置下的” IP地址]”字段)
- 每AP附属WLC (“附属Cisco交换机[名称]在“AP设置下的” IP地址]”字段)
- 每AP第三WLC (“第三Cisco交换机[名称]在“AP设置下的” IP地址]”字段)
- 在WLC的对应的AP配置参数？显示ap设置<AP name>。
- 法塞特检测信号的唯一的支持的AP modea是本地并且h收割(“AP模式”字段)。
- 在AP的对应的AP配置参数？显示capwap客户端设置。

[对意外的WLC的故障切换](#)

显示sysinfo ？预计WLC支持的AP最大。

显示ap摘要？加入预计WLC的AP。

显示capwap客户端ha ？如果法塞特检测信号启用，请检查在AP的备份列表。

[传输问题](#)

如果DHCP为AP以太网接口启用，拿来了一个IP地址？请使用show interface FastEthernet0。

- ping < IP地址> ？确定AP和WLC是否能互相ping。

[CAPWAP协议](#)

普通的WLC和AP调试指令：

- 调试CAPWAP事件和状态？调试capwap事件启用/禁用
- 调试CAPWAP错误？调试capwap错误启用/禁用
- 调试CAPWAP详细信息？调试capwap详细信息启用/禁用
- 调试CAPWAP信息？调试capwap信息消息启用/禁用
- 调试CAPWAP有效负载？调试capwap有效负载启用/禁用
- 调试CAPWAP hexdump ？调试capwap hexdump启用/禁用

AP debug命令法塞特检测信号的特定：

- 调试法塞特检测信号？显示capwap客户端ha

注意：有时您需要(例如wireshark)输出的网络分析器。

[AP优先级](#)

- 确定AP优先级是否启用？显示运行conf (“AP加入在“网络信息下的”优先级”字段)
- 确定WLC支持的AP最大？显示sysinfo (“支持的AP最大”)
- 确定多少AP加入WLC？显示ap摘要
- 检查每个AP加入优先级？显示ap摘要(最后一栏)

运输者和CAPWAP问题

请参阅[AP故障切换](#)部分的对应的会话。

- show tech-support
- 显示运行设置
- show running-config
- 显示ap设置常规<AP name>
- 显示capwap客户端设置

控制器H-REAP相关问题

H-REAP

控制器调试：

- 调试客户端<mac>

AP调试：

- 调试lwapp收割mgmt
- debug dot11 mgmt msg
- 调试dot11 mgmt int

H-REAP CCKM问题

控制器调试：

- 调试cckm
- 调试hheap cckm

AP显示/调试：

- 调试lwapp收割mgmt
- 调试dot11 aaa管理器密钥
- 调试lwapp收割cckm
- debug dot11 mgmt msg
- 显示lwapp收割cckm

H-REAP本地RADIUS

控制器调试：

- 调试hheap组
- 调试hheap aaa

AP/Show调试：

- 调试lwapp收割
- 调试lwapp客户端设置
- show run

媒体流

调试媒体流

- 接纳？客户端是有用的，当调试客户端否认/时的接纳调试从表上删除问题。
- 事件？转存IGMP /Media直接客户端更新。
- RRC？RRC状态机更新。

debug bcast

- igmp？客户端IGMP加入请求/报告消息。

位置相关问题

系统内存，在内存问题外面

配置并且显示输出收集

- show memory stat
- show buffers
- show process memory

注意：如果“配置存储器监视器错误”标志设置“禁用”，使用这些命令，存储器损坏详细信息可以上传：

- transfer upload datatype错误日志
- 转移加载文件名memerrors.txt
- transfer upload start

Mesh相关问题

有失败多点(或请烦扰在线状态)：

- 控制器
- Mesh AP
- GUI/WLC

一般准则

- 识别问题的失败并且隔离失败组件。
- 关联从控制器、Mesh AP，并且视觉输出的跟踪在CLI/GUI/WLC识别失败点。
- 在数据包相关问题的情况下，请收集Airopeek或Ethereal跟踪确认初步的分析。
- 分析失败的原因，并且问题如何可以被再次产生。

- [配置](#)
- 触发操作

[整体指南](#)

此部分打算提供足够的指示器调试mesh bug和收集相关信息帮助DE效率更高了解bug。在的情况下精确定位bug在第一扫视也许是不可能的，本文写入作为一套DT的建议而不是规则说明手册。预计DT将运用判断力附加相关调试为了帮助高效地学习和尽快解决bug。

[可疑的数据包失踪](#)

收集的Ethereal和Airopeek跟踪。

[Debug命令集](#)

这是能使用得到关于系统的信息的一套通用的调试指令。

一般请显示CLI：

- show version
- 显示capwap客户端rcb
- 显示mesh状态
- 显示mesh模块邻接
- 显示mesh信道[current]

测试Mesh CLI：

- 测试mesh邻接？Mesh邻接测验命令
- 测验mesh astools？MESH反子线工具
- 测验mesh awpp？Mesh AWPP测验命令
- 测验mesh禁用？为禁用功能
- 测验mesh enable (event)？启用功能
- 测验mesh转发？转发测验命令的Mesh
- linktest测验的mesh？mesh链路测验的测验
- 测验mesh mperf？MESH BW测试工具

[特定问题](#)

- 任何链路连接问题
- 调试mesh链路
- 显示mesh邻接(孩子/parent/全部)

无线电：

- show controller d0， d1， ... (所有无线电相关的问题)
- 从空气的跟踪(在受影响的节点之间)

接口(涉及的数据流)问题：

- show int d0， d1， G0， G1， ...
- 在控制器和天窗接入点(说唱)之间的以太网跟踪

转发：

- 显示mesh转发表
- 调试转发[table/packet]的mesh
- 显示转发链路的mesh
- 显示转发端口状态的mesh
- 调试转发端口过滤器的mesh

IP地址/DHCP：

- 调试IP地址
- 显示ip int BRI
- show int bvi1
- show run int BVI 1
- 显示转发端口状态的mesh
- 测试mesh禁用端口过滤器和ping路由器

IP数据流和DHCP：

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

排除列表：

- 调试mesh邻接排除？与排除父母涉及的观察事件。
- 测验mesh邻接排除结算？清除当前排除列表计数器并且开始新鲜。

邻接状态机：

- 调试mesh邻接事件
- 调试mesh邻接状态
- 调试mesh邻接计时器

邻接通信：

- 调试mesh邻接数据包
- 调试mesh邻接消息

邻接林克问题：

- 调试mesh邻接信道
- 调试mesh邻接邻居
- 调试mesh邻接parent

信噪比(SNR)更改：

- 调试mesh邻接snr

动态频率选择(DFS)：

- 调试mesh邻接dfs

工作组网桥(WGB)不联合：

- 在控制器和AP的收集的客户端调试。
- 收集在WGB之间的Airopeek嗅探器跟踪并且来源于Mesh AP。

- 在WGB后的有线的客户端不能通过流量。
- 到parent WGB的状态在控制器的。
- 收集在控制器、Mesh AP和WGB的调试。
- 在parent Mesh AP和控制器之间的收集的Ethereal跟踪。

AP不可能加入：

- 在控制器的收集的调试消息：调试capwap错误enable (event)调试capwap事件enable (event)
- 在AP的收集的调试消息：调试capwap客户端事件调试capwap客户端错误

欲知更多信息，请使用这些另外的调试：

- 控制器调试：调试capwap详细信息enable (event)调试capwap信息enable (event)调试capwap有效负载enable (event)调试capwap hexdump enable (event)
- AP调试：调试capwap客户端设置调试capwap客户端详细信息调试capwap客户端fwd调试capwap客户端hexdump调试capwap客户端信息调试capwap客户端有效负载调试capwap客户端重组

显示命令：

- 显示capwap客户端rcb ? 显示无线电控制块配置
- 显示capwap客户端设置? 显示从nvram的无线电配置

测验命令：

- 测验mesh lwapp重新启动
- 测验mesh模式网桥/本地
- 测验mesh角色说唱/地图
- 测验mesh bgn xxxx
- 测验lwapp控制台cli
- 测验lwapp控制器ip

反股工具：

- AP命令
- 控制器调试mesh astools排除故障<MAC addr> ? 被中断的AP的b/g无线电MAC地址。
- 显示命令显示mesh astools设置? 当前配置显示mesh astools中断AP列表? 打印列表检测中断
- AP -信标听不到确保那里是至少一个相邻的AP加入的控制器并且能够侦听对被中断的AP。显示继续的d0确定11b无线电当前操作的信道。收集是相关的所有可能的调试。

Mperf带宽测量工具：

- 显示命令
- debug 命令

与NTP客户机的问题和在控制器的时间配置

- debug ntp packet enable (event)
- 调试ntp低enable (event)
- 调试ntp详细信息enable (event)
- **show time**
- 在控制器管理端口的Ethereal捕获

RF WLCs的组件问题

WLCs的SNMP组件

- 附加失败的简单网络管理协议(SNMP)命令。
- 如果WCS表明SNMP失败，则请设法从MG软奇或其他SNMP Manager运行get命令的SNMP设置/。
- 确认它是否从控制器UI或CLI工作。
- 附加CLI/Controller UI的屏幕画面。
- 如果有内存泄漏或CPU问题，请提及系统多久是UP。
- 查看SNMP调试发现任何是否是明显的。调试snmp MIB enable (event) o调试snmp代理程序 enable (event)调试SNMP陷阱enable (event)。
- 在上述调试外面的附上。

与TFTP加载/下载的问题包括升级/降级

Web WLCs的GUI组件

- 浏览器问题被看到的提及。
- 检查任何Java脚本问题是否存在。如果曾经Firefox，请检查错误控制台。附加Java脚本错误的屏幕画面。Internet Explorer将显示弹出窗口。对于Firefox，请附加错误控制台窗口。
- 如果配置失败，请检查与CLI。附加CLI输出。
- 附加屏幕画面对bug。
- 提及控制器和AP平台。
- 如果有在emweb任务的失败，则看看失败堆栈跟踪。如果堆栈跟踪指示CLI，则请勿使用此组件。

Webauth设置和验证问题

- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

WLC Webauth模板

基本信息

在webauth执行时候，请确定网络的拓扑。

- 它是否是访客设置或正常关联在单个WLC，或者以后漫游webauth执行？
- 什么样的webauth配置(内部，外部，定制或Web Passthru)？
- 什么是使用的登录页？
- 下载webauth套件并且提供那。
- 启用安全Web？如果是，禁用并且看到webauth是否工作。

显示命令：

- 显示客户端详细信息<mac>
- 显示WLAN <wlanid>
- 显示规则显示自定义Web

[调试](#)

- 调试emweb服务器enable (event)
- debug pm ssh-tcp enable
- 调试下午SSH引擎enable (event)数据包<>
- debug pm ssh-appgw enable
- 调试客户端<mac>**注意**：如果页没有显示，请发出此调试。确保分开收集此调试。
- 调试移动性移交enable (event)**注意**：如果webauth不工作以后漫游，请发出此调试。

[嗅探器](#)

- WLC DS端口？这为RADIUS验证问题是有用。WLC AP端口？如果http数据包丢弃在WLC和AP之间在空气？如果AP丢弃数据包

[控制器XML设置相关问题和增强](#)

XML验证

- XML验证错误错误消息，例如ptr_apfCfgData.apfVAPIDData.apfVapSecurity.<anydata>
- 全部的XML验证错误错误消息
- 配置WLAN的CLI或GUI步骤在系统前启动
- 生成并且保存对TFTP的CLI或XML配置文件，在系统启动前
- 显示无效设置

[诊断信道](#)

- 调试客户端<client mac>
- 调试ccxdia全部启用

[动态信道分配](#)

- 调试广播频道导向器信道enable (event)
- 调试广播频道导向器雷达enable (event)

[TACACS+](#)

- debug aaa TACACS enable (event)
- show tacacs summary

[WLC组播指南](#)

[基本信息](#)

- 网络的拓扑
- 确保组播流地址不是在使用中的应用程序的IANA保留地址。
- 使用的组播地址

- 组播流速率和数据包大小
- 确保组播地址不是相同的象组播流地址的已配置的AP组。
- WLC型号(2106 , 4404 , 4402 , WiSM...)
- AP型号(1131 , 1232 , 1242 , 1250...)
- 收音客户端使用
- 客户端的MAC地址

WLC信息(所有类似)

转存：

- show interface摘要debug bcast * enable (event)
- show network摘要
- show network multicast mgid summary
- show network组播mgid详细信息 <mgid>
- G版本和以后：显示WLAN apgroups
- 与新的FP代码的TALWAR/2106：如果IGMP探听启用，调试快速路径cfgtool --mcast4db.dump调试快速路径cfgtool --mcast2db.dump如果IGMP探听禁用，请调试快速路径cfgtool --mcast2db.dump如果组播单播启用，请调试快速路径cfgtool--mcastrgdb.dump

AP信息(所有类似)

转存：

- 显示lwapp mcast显示lwapp mcast mgid全部显示lwapp mcast mgid id <mgid>显示lwapp客户端与1个分钟间隔的流量四时间

无线电调试：

1. 以太网超出速率
2. 无线电发送速度
3. 无线电丢弃速率
4. 基本类型服务集(BSS)的节电模式
5. 总以太网RX速率
6. 以太网组播RX速率

对于#1，请运行show int g0|周期地超出命令。

对于#2，#3和#4，运行显示继续的d0|周期地发出命令。注视着发送/丢弃计数为每个队列。

并且对于#3，请运行show int d0|周期地输出丢弃命令。

对于#5，请运行显示继续的g0|周期地。

对于#6，请运行显示继续的g0|周期地。广播第一的行显示RX组播/。

为了获得数据包速率，请运行命令每10秒并且除差异10。

如果很多数据包在Mcast队列被发送(BSS)，则BSS在节电模式。节能BSS的最大组播信息包速率相对低。这是一个著名的问题。

交换机信息

用show version命令检查交换版本。交换机应该有“预先的ip基础”版本(例如，Cisco IOS软件，C3750软件[C3750-ADVIPSERVICESK9-M]，版本12.2(40)SE，发行软件(fc3)。[镜像：c3750-advipservicesk9-mz.122-40.SE.bin])。“ip基本”版本有一个问题在路由VLAN间组播数据流。

一些调试：

- 检查组播路由是否启用。“show run”应该包括“被分配的ip multicast-routing”)检查“ip pim sparse-dense-mode”设置是否被添加到配置的VLAN。显示ip igmp组

嗅探器捕获

- WLAN的DS接口
- WLC的Mgmt接口
- AP连接的AP Mgr (只要求，当mcast src是无线)
- AP的Eth接口
- 在空气

嗅探器捕获分析

组播源是有线旁拉

- 检查数据包是否到达在DS接口的WLC。
- 检查LWAPP被封装的组播信息包是否在mgmt接口发送。数据包必须有：外面ip dst地址=已配置的ap组组播地址udp dst port= 12224
- 检查在‘b’看到的数据包是否被看到在AP的eth intf。
- 检查mcast数据流数据包是否在空气被看到。

组播源是无线旁拉

- 检查LWAPP封装数据包是否接收在AP Mgr intf。这里，LWAPP是单播。
- 检查组播信息包是否从DS intf发送。
- 检查LWAPP被封装的组播信息包是否在mgmt接口发送。数据包必须有：外面ip dst地址=已配置的ap组组播地址udp dst port= 12224
- 检查在‘b’看到的数据包是否被看到在AP eth intf。
- 检查mcast数据流数据包是否在空气被看到。

交换机配置检查WiSM

检查是否面对如下所述的问题，当您使用一个无线服务模块(WiSM)。

Cisco Bug ID CSCsj48453?CAT6k不寄组播数据流给在L3模式的WiSM。

症状？例如，当两台主机用不同的VLAN时，组播数据流终止流从一台有线的主机到一台无线主机通过WiSM卡在L3模式。仅第一数据包顺利地到达。之后，流量终止。

条件？只有当组播复制模式是出口时，流量终止。

应急方案？应急方案是更改组播复制模式对入口使用mls ip multicast replication-mode入口命令。适当通信流在入口模式。使用show mls IP组播功能命令，验证同样。

促进问题说明？问题在Cat6k和WiSM看到。流从无线主机的组播数据流到有线的主机良好工作，在L3。并且，流经从有线的主机的组播数据流到无线主机WiSM卡在L2模式良好工作。

[WLC QoS指南](#)

[最低的调试](#)

- 获得？显示运行设置？从在移动组的所有交换机。
- 当问题发生时，请获取这些调试：debug aaa all enable debug pem state enable debug pem events enable 调试移动性移交 enable (event) 调试 dot11 移动 enable (event) 调试 dot11 状态 enable (event)
- 在有问题的AP/phone/handset附近获得Airopeek或AirMagnet trace。
- 获得交换机DS端口、AP上行交换机和SpectraLink语音优先级(SVPs)的Ethereal或Etherpeek捕获。

[呼叫控制\(SIP分类\)调试](#)

[问题](#)

- 它是否是会话初始化协议(SIP)客户端？
- 什么IP PBX \ sip服务器是它使用？
- 它显示注册在那给的SIP服务器？
- 7921工作正如所料和只有SIP客户端有问题？

[WLC信息](#)

- 显示WLAN摘要[wlan -]
- 调试呼叫控制全部
- 调试呼叫控制事件
- 显示控制错误
- 显示呼叫控制呼叫

[AP信息](#)

- 调试dot11 cc详细信息
- 调试dot11 cc错误
- 调试dot11 cc事件
- 显示lwapp客户端呼叫INFO mac (有问题的客户端的MAC地址)

[装载基于准入控制和语音量度](#)

[回答的问题](#)

- 它是否用两无线电发生？a？并且？b？？

- 当呼叫拒绝时，什么是信道利用值？
- 这用仅7921个电话，或者用其他电话？如果是，什么是电话？否则，这能尝试在另一个TSPEC电话？
- 这11n或正常AP？
- 执行控制器之间移动性？
- TSPEC电话是否有能力？
- 它执行UAPSD？
- 再现的这在2006年或4100平台？
- 它是否是一个被保护的空间环境？
- 有没有呼叫拒绝的特殊条件？

Debug与Show LBCAC的On命令WLC

- debug cac全部启用
- 显示802.11a/b/g
- 显示wlan <wlan id>
- show ap stats 802.11a/b/g <ap-name>
- 显示ap自动RF 802.11a/b/g <ap-name>

调试LBCAC的AP

- debug dot11 cac单元
- debug dot11 cac量度
- debug dot11 cac事件

语音量度

- 在空气和电线嗅探器捕获确认UP6流量是否不断地生成。确保WLAN有权利QoS配置文件和wi-fi多媒体(WMM)策略。为LBCAC询问的大多问题为语音量度是可适用的。Debug与Show on命令语音量度的WLC：显示802.11a/b/g o显示wlan <wlan id>show ap stats 802.11a/b/g <ap-name>show ap stats 802.11a/b/g <ap-name> tsm显示客户端tsm 802.11a/b/g <client-mac> <AP mac>debug iapp数据包enable (event) o debug iapp错误enable (event)debug iapp所有enable (event) o调试客户端<client mac>
- 在AP的调试语音量度的：调试dot11 tsm调试lwapp客户端语音量度

WLC许可证指南

收集的调试在控制器

- 控制台输出
- msglog

ARP问题

收集的调试在控制器

- debug arp全部启用

网络问题

收集的调试在控制器

- 调试数据包logging enable
- 转储LOW级别调试

其他

收集的调试在控制器

- 转储LOW级别调试
- msglog

接入点问题

IAPP

- 显示wgb摘要
- 显示wgb详细信息<wgb mac>

WGB关联问题

- 调试dot11移动enable (event)
- 调试dot11状态enable (event)
- debug pem events enable
- debug pem state enable
- debug iapp全部启用

WGB或有线的客户端没获得DHCP地址

- debug dhcp packet enable
- debug dhcp message enable

WGB或有线的客户端用途静态IP地址，然而IP地址不出现在控制器

- 调试dot11移动enable (event)
- 调试dot11状态enable (event)

AP Username password

收集的调试在AP

- 调试lwapp客户端设置

[采取的捕获](#)

不可适用。

[配置并且显示输出收集](#)

- 配置ap mgmtuser

[客户端连接问题](#)

[客户端调试](#)

- 调试客户端xx.xx.xx.xx.xx.xx

[控制器不类似关联申请](#)

[数据包捕获](#)

在AP设置的信道的Airopeek捕获。因为信标和探测器req/响应数据包可以未命中，推荐避免过滤。当连接终止时，请确保捕获事件。

万一客户端不连接，然后请从prob请求开始捕获整件事，直到会话终止(例如， deauth发送和与状态代码的关联答复作为非0)。

提供客户端和AP MAC地址。

注意： AP MAC将是基本无线电MAC + WLAN-ID。

[配置并且显示输出收集在控制器](#)

- 显示sysinfo ? WLC ? s版本详细信息显示WLAN x ? 在受影响的WLAN的WLC显示运行设置 ? WLCshow debugshow msglogshow tech-support ? WLC (好有，但是不必要)

[客户端详细信息](#)

- 客户端硬件 ? 请求方软件细节例如版本和软件名字(例如， ADU或冒险旅行)
- 客户端OS ? 如果它是Windows，请通过去提供客户端系统系统构成给Programs > Accessories >System Tools>系统信息。

[RADIUS服务器详细信息](#)

如果适用提供RADIUS服务器类型(SBR、Cisco ACS、Linux等等)和配置。

[客户端不回答EAP请求](#)

请参阅[控制器不类似关联申请](#)部分。

[EAP验证不经历](#)

请参阅[控制器不类似关联申请](#)部分。

[从客户端的DHCP请求发生故障](#)

请参阅[控制器不类似关联申请](#)部分。

[EAPOL Exchange不经历](#)

请参阅[控制器不类似关联申请](#)部分。

[CCKM漫游发生故障](#)

[收集的调试](#)

大多调试是相同的象前面部分，[客户端连接问题](#)。然而，这些新的调试在CCKM调试将帮助更多。此debug命令从5.0及以上版本是可得到：

- 调试cckm enable (event)显示PMK缓存<client mac> ？在目标控制器上显示客户端详细信息<client mac> ？当客户端在旧有AP连接调试cckm enable (event)

注意： 在您发出[调试客户端](#)<client mac>后，必须交换这些调试或其他调试。这是因为[调试客户端](#)<mac>命令造成所有上一个调试禁用。

[采取的捕获](#)

确保您捕获在目标AP的信道。例如，您要获取在客户端和目标AP之间的管理信息包。请参阅[控制器不类似关联申请](#)部分欲知更多信息。

[配置并且显示输出收集在控制器](#)

请参阅[控制器不类似关联申请](#)部分和发出这些命令：

- 显示PMK缓存<client mac> ？在目标控制器上
- 显示客户端详细信息<client mac> ？当客户端在旧有AP连接

[客户端详细信息](#)

请参阅[控制器不类似关联申请](#)部分。

[PMKID高速缓冲存储发生故障](#)

是否检查客户端支持机会主义的关键缓存(OKC)。

注意： OKC不是作为积极的关键缓存的相同的(PKC)在802.11i上指定。仅WLC支持OKC。

[收集的调试](#)

请参阅[控制器不类似关联申请](#)部分。

[采取的捕获](#)

确保您捕获在目标AP的信道。例如，您要获取在客户端和目标AP之间的管理信息包。

请参阅[控制器不类似关联申请](#)部分。

[配置并且显示输出收集在控制器](#)

请参阅[控制器不类似关联申请](#)部分和发出这些命令：

- 显示PMK缓存<client mac>？在目标控制器上
- 显示客户端详细信息<client mac>？当客户端在旧有AP连接

[客户端详细信息](#)

请参阅[控制器不类似关联申请](#)部分。

[Reauth问题](#)

[收集的调试](#)

请参阅[控制器不类似关联申请](#)部分。

[采取的捕获](#)

不可适用。

[配置并且显示输出收集在控制器](#)

请参阅[控制器不类似关联申请](#)部分和发出这些命令：

- show radius摘要
- 显示客户端详细信息<client mac>
- 显示PMK缓存<client mac>

[客户端详细信息](#)

请参阅[控制器不类似关联申请](#)部分。

[漫游的802.11R \(快速转换\)不工作](#)

[收集的调试](#)

- 调试客户端<client mac>
- 调试ft事件enable (event)
- 调试ft密钥enable (event)

注意：在您发出**调试客户端<client mac>**后，必须交换这些调试或其他调试。这是因为**调试客户端<mac>**命令造成所有上一个调试禁用。

采取的捕获

在漫游的漫游的情况下，请收集在目标AP的信道的Airopeek捕获。例如，您要捕获所有802.11验证FT req/响应帧和再聚集req/响应。

在漫游的DS的情况下，请收集在来源AP的信道的Airopeek捕获。例如，您要捕获再聚集req/响应帧。您也要捕获操作帧？s FT req/在来源AP的响应？s信道。

注意：在同一个信道推荐保留源和目的AP为了调试漫游问题的802.11R。这允许您捕获FT req/响应和再聚集req/在单个捕获文件的响应。

配置并且显示输出收集在控制器

请参阅[控制器不类似关联申请](#)部分和发出这些命令：

- 显示PMK缓存<client mac>？在目标和来源控制器上
- 显示客户端详细信息<client mac>？当客户端在旧有AP连接
- 显示移动性摘要？获得移动性域ID

客户端详细信息

目前，仅WGB是已知802.11R客户端。请参阅[控制器不类似关联申请](#)部分欲知更多信息。

相互控制器移动性

收集的调试

- 调试客户端<client mac>？在两WLCs
- 调试移动性移交enable (event)？在两WLCs (请记住命令：首先总是请启用调试客户端。)
- Debug pem state enable
- Eping <ip>
- Mping <ip>

如果移动性控制路径或数据发生故障那么请打开‘调试移动性Keepalive enable (event)’在两交换机 (请记录下来软件版本运行在两个控制器)。

如果ARP不工作，打开？debug arp全部启用？在两交换机上。

如果DHCP不工作，打开？debug dhcp消息enable (event)？并且？debug dhcp数据包enable (event)？在两交换机上。

如果IPSec是包含的：调试下午SA出口enable (event)，调试下午SA导入enable (event)。

如果客户端在一会儿以后连接，请指示多长时间需要了。

[采取的捕获](#)

根据漫游类型的捕获，例如CCKM、PMKID或者TGR。

[配置并且显示输出收集](#)

请参阅[控制器不类似关联申请](#)部分和发出这些命令：

- 显示PMK缓存<client mac>？在目标控制器上
- 显示客户端详细信息<client mac>？当客户端在旧有AP连接
- 显示移动性摘要？在两WLCs

[客户端详细信息](#)

请参阅特定漫游类型，例如CCKM、PMKID或者TGR。

[禁用的调试](#)

为了禁用所有调试消息，请使用[调试禁用所有command](#)命令。

或者，使用[debug](#)命令与禁用关键字，您能禁用特定调试。示例如下：

[相关信息](#)

- [技术支持和文档 - Cisco Systems](#)