

无线局域网控制器(WLC)最优配置方法

目录

介绍.....	2
先决条件.....	2
要求.....	2
使用组件.....	2
公约.....	3
最佳做法.....	3
无线/射频	3
网络连接.....	4
网络设计.....	8
移动性.....	8
安全.....	13
总结.....	16
如何把 WLC 崩溃文件从 WLC 传输到 TFTP 服务器.....	21

介绍

本文档提供了 WLC 的简短配置窍门，包括在 TAC 中心常见的几个有关无线统一基础设施问题。

该文档适用于大多数网络实现环境，以便最大限度减少可能发生的问题。

注意：并不是所有的网络都是等同的，因此，一些建议可能并不适用于您的网络安装环境。总是需要核实，然后再进行一些更改。

先决条件

要求

思科建议您了解这些议题：

- 了解如何配置无线局域网控制器（ WLC ）和轻量级接入点（LAP）的基本操作
- 轻量级接入点协议（ LWAPP ）和无线安全的基本知识

使用组件

此文档中的信息是基于这些软件和硬件版本：

- 思科 2000/2100/4400 系列 WLC ， 运行软件版本在 4.2 或 5.0
- LWAPP 的接入点， 1230， 1240， 1130， 10x0 和 1510 系列

本文件中所涉及的设备均在特定的实验室环境。本文件中所有设备开始为默认配置，在配置网络之前，要确保了解潜在影响的任何命令。

公约

在文件公约中，如了解更多信息请参考 [Cisco Technical Tips Conventions](#) 连接。

最佳做法

无线/射频

对于无线/射频（ RF ）最佳做法如下：

- 对于任何无线部署，前期必须要进行一个适当的实地勘察，以确保为无线用户提供适当的服务质量。对于部署语音或定位业务要比单纯的提供数据服务更为严格。自动射频功能可有助于对频道和发射功率的设置管理，但不能纠正一个糟糕的射频设计。
- 在做前期站点勘查时所用设备必须与实际网络中选择的设备一致。例如，如果最后的网络使用 1240 系列双频 802.11A/G 时，不要使用 350 的 802.11b 无线 AP 去进行勘查。
- 建议在控制器上限制服务设置标识符（ SSIDs ）的配置数量。根据您的接入点模式，您可以同时配置 8 个或 16 个 SSIDs，但由于每个 WLAN/SSID 的需要单独的探针和信标响应，因此使用更多的 SSIDs 数量，会增加射频的污染。结果会导致一些规模较小的无线终端，像 PDA、WiFi 电话和条码扫描器无法应付大量的 BSSID 信息。这会导致终端设备被锁定、重新加载或关联失败，因此减少射频空间的污染有利于实时数据传输。
- 射频环境在空旷空间环境，如 AP 在一个比较空旷环境中，调整发射功率阈值从默认的 -65 dBm，调整至较低的价格 -76 dBm 是有必要的。这样就可以降低同信道间的相互干扰（在某一特定时刻，无线客户端听到的 BSSID 数量）。设定合适的功率阈值主要还是依赖于每个站点的环境特性，因此前期应该仔细进行实地的站点勘察。

发射功率阈值-这个值用 dBm 表示，是由发射功率控制（TPC）算法调整功率级别下降的信号级别分界点，这个值是 AP 听到的邻居三个最强信号 AP 的强度值。

- 有些 802.11 客户端软件听到超过一定数量的 BSSIDs（例如，24 或 32 BSSIDs）可能会遇到问题，你可以通过降低 AP 发射功率的阈值来缩减覆盖范围，从而可以减少客户端听到 BSSIDs 的数量。
- 不要启用负载均衡功能，除非在该区域部署了高密度的 AP 数量，如果有语音业务应用也尽量不要启用负载均衡功能。如果您启用此功能，并且部署 AP 的间距相距很远，对一些无线客户端可能会导致混淆漫游，在某些情况下也会引起覆盖漏洞。在最新的软件版本中，此功能默认为关闭。请记住，不要将该功能用于语音网络，以及一些较旧的客户端。

网络连接

下面是对于网络连接的最好做法：

- 在控制器上不要使用生成树。

对于大多数拓扑，在控制器上是不需要运行生成树协议的，STP 默认是关闭的。

对于非思科交换机，也建议您在每个端口上关闭 STP。

使用此命令来验证：

```
Cisco Controller) >show spanningtree switch
STP Specification..... IEEE 802.1D
STP Base MAC Address..... 00:18:B9:EA:5E:60
Spanning Tree Algorithm..... Disable
STP Bridge Priority..... 32768
STP Bridge Max. Age (seconds)..... 20
```

STP Bridge Hello Time (seconds)..... 2
STP Bridge Forward Delay (seconds)..... 15

- 您在控制器上作出的配置大部分是即时生效的，但建议您更改以下配置并保存后，重新加载控制器：
 - 管理地址
 - SNMP 配置，这一点非常重要，如果您使用的旧软件。
- 对于所有连接到控制器的交换机中继端口，将不需要的 VLAN 筛选掉。

例如，在思科 IOS ®交换机，如果管理接口是 VLAN 20 ，无线客户端 VLAN 是 40 和 50，使用此配置命令在交换机上：

```
switchport trunk allowed vlans 20,40,50
```

- 不要配置一个地址为 0.0.0.0 的接口，例如一个未配置的服务端口（service port），这可能会影响控制器上对 DHCP 的处理。

验证命令如下：

```
(Cisco Controller) >show interface summary
```

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr
ap-manager	LAG	15	192.168.15.66	Static	Yes
example	LAG	30	0.0.0.0	Dynamic	No
management	LAG	15	192.168.15.65	Static	No
service-port	N/A	N/A	10.48.76.65	Static	No
test	LAG	50	192.168.50.65	Dynamic	No
virtual	N/A	N/A	1.1.1.1	Static	No

- 除非在交换机上所连接控制器的端口的二层配置相同，否则不要使用 LAG。例如，在一个端口上过滤了一些 VLAN ，而另一个端口没有配置。
- 当您使用 LAG 时，控制器是依赖于交换机实现网络流量负载均衡的，到同一个 AP 或者是无线客户端的流量总是使用相同的端口。在交换机以太网通道

配置中，使用 ip-src 或 ip-src ip-dst 的配置可选项。一些交换机默认情况下可能不支持以上的负载均衡机制，因此需要确认。

下面是如何验证以太通道负载均衡机制：

```
switch#show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
src-dst-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
IPv4: Source XOR Destination IP address
IPv6: Source XOR Destination IP address
```

下面是如何更改交换机配置（IOS）：

```
switch(config)#port-channel load-balance src-dst-ip
```

- 当控制器与交换机之间连接跨越多个交换机时，请不要配置 LAG。当您使用 LAG 后，必须确保属于同一个以太通道的所有端口要在一台物理交换机上。
- 如果你想把 WLC 连接到多个交换机时，你必须为每个物理端口创建一个 AP-manager，以提供冗余和可扩展性。

注：在思科 4400-100 型号 WLCs 上，你需要至少使用三个物理端口，为 100 个 AP 提供接入容量。在思科 4400-50 型号 WLCs 上，你需要使用两个物理端口，为 50 个 AP 提供接入容量。

- 只要有可能，对于一个 AP-manager 接口不要建立一个备份端口，即使在旧版本的软件中是允许的。有关多个 AP-manager 接口提供冗余方式，在本文档的前面已经叙述过了。
- 对于组播转发，最好的性能和较少的带宽利用率是通过多播模式来完成。

下面是在控制器上验证多播模式：

```
(WiSM-slot1-1) >show network summary
```

```

RF-Network Name..... 705
Web Mode..... Enable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Disable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Enable Mode:
Mcast 239.0.1.1
Ethernet Broadcast Mode..... Disable
IGMP snooping..... Disabled
IGMP timeout..... 60 seconds
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Disable
Mgmt Via Dynamic Interface..... Disable
Bridge MAC filter Config..... Enable
Bridge Security Mode..... EAP
Over The Air Provisioning of AP' s..... Enable
Apple Talk ..... Disable
AP Fallback ..... Enable

```

这是如何更改交换机配置 (IOS) :

```

config network multicast mode multicast 239.0.1.1
config network multicast global enable

```

- 控制器使用组播地址是为了转发组播流量给 AP。重要的是在您的网络上它不匹配其他地址。例如,如果您使用 224.0.0.251,它将和一些第三方基于 mDNS 的应用程序产生冲突。建议的地址是在私有范围 (239.0.0.0-239.255.255.255, 其中不包括 239.0.0.x 和 239.128.0.x)
- 如果 AP 使用的地址与控制器管理接口地址在不同子网,您的网络基础设施必须为管理接口子网和 AP 子网提供多播路由。

网络设计

下面是对于网络设计的最佳做法：

- 基于每个 VLAN 的 AP 数量限制。如果您使用最新版本，每个 VLAN 的 AP 数量最好在 60 到 100 个。在网络故障情况下，这将有助于最大限度地减少重关联问题。基于思科 IOS AP 可以部署在高密度子网，但务必确保 Layer 2 和 Layer 3 拓扑的正确配置（生成树，负载均衡等）。
- 连接 AP 的交换机端口模式配置为 portfast。为了做到这一点，设置端口连接作为一个“主机”端口（switchport host 命令），或直接配置 portfast 命令。这使得 AP 加快加入控制器的进程并没有任何循环的风险，因为 LWAPP AP 从不做两个 VLAN 之间的桥梁。
- 关于第一个提示，与控制器管理接口在同一个 VLAN 的 AP 数量不要超过 20 个，除非您使用的是 4.2.112.0 或更新版本。由于 AP 会产生大量的广播信息，当其中一些发现信息被抛弃时，这会导致 AP 加入控制器的进程较慢。
- 在控制器上，大部分的 CPU 发送流量都是由管理地址作为源地址发出的。例如，SNMP traps，RADIUS 身份验证请求，组播转发，等等。

DHCP 相关流量除外，对于控制器的软件版本在 4.0 或更高版本，它是从设置相关的 WLAN 接口转发的。例如，如果一个 WLAN 采用了动态接口，DHCP 请求将使用动态接口的 3 层地址转发。

当您设定防火墙策略或设计网络拓扑结构时，有一些因素是必需考虑的。避免配置一个动态接口和某些需要控制器 CPU 流量可达的服务器在同一子网内，例如 RADIUS 服务器，因为它可能导致非对称路由的问题。

移动性

下面是对于移动性的最佳做法：

- 在一个移动组中的所有控制器应具有一个相同的虚拟的接口 IP 地址，例如 1.1.1.1。这是为漫游提供的非常重要的服务。如果在一个移动组中的所有控制器没有使用相同的虚拟接口，跨控制器漫游看起来好像可以工作，但是切换是不完整的，客户端将在一段时间内失去连接。

这是如何验证：

(Cisco Controller) > **show interface summary**

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr
ap-manager	LAG	15	192.168.15.66	Static	Yes
management	LAG	15	192.168.15.65	Static	No
service-port	N/A	N/A	10.48.76.65	Static	No
test	LAG	50	192.168.50.65	Dynamic	No
virtual	N/A	N/A	1.1.1.1	Static	No

- 在您的网络架构中，虚拟网关地址必须是**不可被路由的**。其目的只为可以让一个无线客户端连接到一个控制器，而不是通过有线连接。
- 所有控制器都必须配置为相同的 LWAPP 传送模式（第 2 层或第 3 层）。
- 所有控制器之间的管理接口必须 IP 可达。
- 在大多数情况下，所有的控制器都必须配置相同的移动组名称。例如，在思科 WiSM，两个控制器必须配置相同的移动组名，为 300 个 AP 提供无缝漫游。对于访客功能将不使用此规则进行部署，它是通过 DMZ 方式部署。
- 所有控制器必须运行同一软件版本。对于访客应用，部署在 DMZ 区域的控制器软件版本可以与其他控制器软件版本不同，部署在 DMZ 区域的控制器软件版本需要运行在 4.2.112.0 版本，内部网络的控制器至少运行在 4.1.185.0 版本。
- 您必须收集包含在移动组中的每个控制器的 MAC 地址和 IP 地址，以便于在同一个移动组中的控制器上指定其他控制器的 MAC 地址和 IP 地址。您可以在每个控制器上通过 Controller > Mobility Groups GUI 页面找到控制器的 MAC 和 IP 地址。

- 不要建立一个较大的移动组。一个移动组应该是无线客户端在物理上可以实现漫游的区域，例如控制器所管理的 AP 在同一个建筑物内。如果您有几座建筑物是分开的，他们应该分为几个移动组群。这样可以节省内存和 CPU，作为控制器不需要维护较大的在线用户数和非法 AP 信息，不会造成相互之间的影响。

请记住，WLC 冗余是通过创建移动组来完成的。所以，可能有必要在某些情况下，增加移动组的规模，其中包括额外的控制器冗余（例如 N+1 拓扑）。

- 大多数情况下，在一个移动组中会有多个控制器。在控制器重新加载之后，可能会在网络中看到我们自己 AP 被看成非法 AP，这是因为它在组成员之间更新 AP，客户端和非法 AP 的信息。
- 在 WLAN 设置中，DHCP 有个可选项是允许您强制客户端必须通过 DHCP 自动获取地址方式连入到无线网络。从安全观点看来，这样可以更严格控制 IP 地址的使用，但这有可能对总的漫游时间上有所影响。

此外，这可能影响到某些客户端直到租用地址过期后，无法从 DHCP 重新获取 IP 地址。例如，如果启用该项功能，对思科 7920 或 7921 手机在漫游时可能有问题，因为在 DHCP 阶段完成之前，控制器是不允许语音或信令流量传递的。有些第三方打印机服务器可能也将受到影响。一般情况下，如果 WLAN 是非 Windows 客户端，建议不使用此选项。这是因为更严格的控制可能会引起连接上的问题。下面是验证命令：

```
(Cisco Controller) >show wlan 1
```

```
WLAN Identifier..... 1
Profile Name..... 4400
Network Name (SSID)..... 4400
Status..... Enabled
MAC Filtering..... Disabled
```

```

Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None

```

- 如果您使用 Layer 3 漫游，例如在一个控制器上的一个 WLAN 子网没有在另一个控制器上匹配，或 AP 组，我们建议在所有控制器上启用对称漫游移动，以避免非对称路由的问题。这一点非常重要，如果您的网络中有基于状态的防火墙，它将中断数据流量。因此在同一个移动组中设置必须相同。

使用下面命令进行验证：

```
(Cisco Controller) >show mobility summary
```

```

Symmetric Mobility Tunneling (current) ..... Disabled
Symmetric Mobility Tunneling (after reboot) ..... Disabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... 100
Mobility Keepalive interval..... 10
Mobility Keepalive count..... 3
Mobility Group members configured..... 1

```

Controllers configured in the Mobility Group

MAC Address	IP Address	Group Name	Status
00:16:9d:ca:e4:a0	192.168.100.28	100	Up

这是如何配置：

```
config mobility symmetric-tunneling enable
```

注意： 您必须重新启动控制器才能生效。

- 如果您使用 5.0 或更新的版本，对移动组可以配置组播模式。这使得客户在移动时可以发送组播信息，代替了以单播方式发送到每个控制器上，这将对 CPU 使用率和网络利用率都是有好处的。

通过下面命令进行验证：

```
(WiSM-slot1-1) >show mobility summary
```

```
Symmetric Mobility Tunneling (current) ..... Disabled
Symmetric Mobility Tunneling (after reboot) ..... Disabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... 705
Multicast Mode ..... Enabled
Mobility Domain ID for 802.11r..... 0x8e5e
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 2
Mobility Control Message DSCP Value..... 0
```

Controllers configured in the Mobility Group

MAC Address	IP Address	Group Name	Multicast IP
00:14:a9:bd:da:a0	192.168.100.22	705	239.0.1.1
Up			
00:19:06:33:71:60	192.168.100.67	705	239.0.1.1
Up			

安全

下面是有关安全的最佳做法：

- 建议更改 RADIUS 超时为 5 秒，对于默认值 2 秒是针对快速 RADIUS 故障切换的，但对于可扩展认证协议-传输层安全（EAP - TLS）身份验证或者如果 RADIUS 服务器已联接外部数据库（Active Directory, NAC, SQL, 等等）是不够的。

使用下面命令进行验证：

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Credentials Caching..... Disabled
Call Station Id Type..... IP Address
Administrative Authentication via RADIUS.... Enabled
Aggressive Failover..... Disabled
Keywrap.....
DisabledAuthentication Servers
```

! ---由于内容较多，这部分使用单独几行

Idx	Type	Server Address	Port	State	Tout	RFC3576
1	N	10.48.76.50	1812	Enabled	2	Enabled

```
IPSec -AuthMode/Phase1/Group/Lifetime/Auth/Encr
```

```
-----
Disabled - none/unknown/group-0/0 none/none
```

下面是如何配置：

```
config radius auth retransmit-timeout 1 5
```

- 检查 SNMPv3 的默认用户。 控制器默认情况下使用的用户名应停用或改变。

使用下面命令进行验证：

```
(Cisco Controller) >show snmpv3user
```

```
SNMP v3 User SNMP v3 User Name AccessMode Authentication  
Encryption
```

```
-----  
default Read/Write HMAC-MD5 CBC-DES
```

下面是如何配置：

```
config snmp v3user delete default
```

```
config snmp v3user create nondefault rw hmacsha des authkey  
encrkey
```

请记住，您的 SNMP 设置必须在控制器和无线控制系统（ WCS ）之间匹配。此外，您应该使用加密和散列值匹配您的安全政策。

- 当您使用外部 Web 身份验证页面时，在同一时间请不要在该服务器上使用 Web 服务和代理服务。在验证完成之前，控制器是允许 HTTP 流量从无线客户端向服务器发送的。目前在服务器上允许客户端使用代理服务进行浏览的。
- 在控制器上，默认 EAP 身份请求超时为 1 秒。在某些情况下，使用默认超时是不够的，比如像一次性密码或智能卡，在无线客户端回答身份请求之前会提示使用者写 PIN 或密码。在胖 AP 模式下，默认为 30 秒，所以应考虑将控制器上的默认 EAP 身份请求超时改为 30 秒。

通过下面命令进行更改：

```
config advanced eap identity-request-timeout 30
```

- 在一些攻击环境中，AP 上启用验证功能并设置一个阈值为 2 是有好处的，该功能可以发现并尽量减少虚假信息。

下面是如何配置：

```
config wps ap-authentication enable
```

```
config wps ap-authentication threshold 2
```

- 关于上一个提示，在无线网络架构中，管理帧保护（MFP）可以被用来验证 AP 之间所有 802.11 管理帧。考虑到一些普通第三方无线网卡有驱动程序执行问题，不能够通过 MFP 正确处理额外增加的信息。请务必从原厂下载最新的驱动程序，然后再测试并使用 MFP。
- 对于一些功能 NTP 是非常重要的。在控制器上，如果您使用下面这些功能的任意一个都需要强制使用 NTP 同步，如定位、SNMPv3、AP 认证或 MFP 功能。


下面是如何配置：

```
config time ntp server 1 10.1.1.1
```

为了验证，在您的日志中会产生像下面的一些信息：

```
30 Tue Feb 6 08:12:03 2007 Controller time base status -
```

```
Controller is in sync with the central timebase.
```

- 当在微软 XP SP2 操作系统中使用受保护的 EAP 微软挑战握手验证协议版本 2（PEAP-MSCHAPv2）认证，无线网卡并通过微软无线零配置（WZC）来管理时，你应该安装微软的修补程序 KB885453 。这可以防止有关认证上面的 PEAP 快速恢复问题。
- 出于安全考虑，在几个子网中，每个客户端应该是相互分离的，每一个应该有不同的安全政策。这是好注意，使用一个或两个无线网络 WLAN（例如，

每个都有不同的 2 层加密策略) 连同 AAA 覆盖 (AAA-Override) 特性。此功能可让您为每个用户制定不同的设置。例如, 将用户分配到不同的 VLAN 中, 或为个用户应用不同的访问控制列表。

- 虽然控制器和 AP 都同时支持无线局域网 SSID 使用的 Wi-Fi 保护访问 (WPA) 和 WPA2, 但一些无线客户端驱动器不能处理复杂的 SSID 设置也是常见的。一般情况下, 对于任何 SSID 使用简单的安全策略是一个好主意, 例如, 使用一个 WLAN/ SSID 的 WPA 和临时密钥完整性协议 (TKIP), 外加一个 WPA2 和高级加密标准 (AES) 。

总结

下面是最佳做法的总结:

- 一般来说, 在任何升级之前建议做一次配置的备份。WLCs 支持旧的配置信息到新的版本, 但不支持相反的处理。这同时适用于主要或次要版本的变化。
- 使用新的配置到一个老的版本可能会导致部分配置丢失 (访问控制列表, 接口, 等等), 或运行不正常。如果您需要对控制器进行降级, 在降级后需清除配置, 然后配置管理接口地址后, 再通过 TFTP 加载备份的配置文件。
- 如果您降级从一个 XML 配置文件版本 (例如 4.2, 5.0) 到一个二进制配置文件版本 (4.0, 4.1), 该控制器的原有 XML 配置将被清除, 设备降级后的第一次启动后, 您将看到的是安装向导。
- 进入 AP 设置配置控制器名字是可取的, 这样您就可以控制 AP 第一次加入到控制器的选择。您可以使用下面命令进行验证:

```
(WiSM-slot1-1) >show ap config general AP1130-9064
```

```
Cisco AP Identifier..... 164  
Cisco AP Name..... AP1130-9064  
Country code..... BE - Belgium
```

```

Regulatory Domain allowed by Country..... 802.11bg:-E
802.11a:-E
AP Country code..... BE - Belgium
AP Regulatory Domain..... 802.11bg:-E
802.11a:-E
Switch Port Number ..... 29
MAC Address..... 00:16:46:f2:90:64
IP Address Configuration..... DHCP
IP Address..... 192.168.100.200
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 192.168.100.1
Telnet State..... Disabled
Ssh State..... Disabled
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch Name..... Cisco_ea:5e:63
Primary Cisco Switch IP Address..... Not Configured
Secondary Cisco Switch Name.....
Secondary Cisco Switch IP Address..... Not Configured
Tertiary Cisco Switch Name.....

```

为了设置此值（记住这是该控制器的系统的名字，而不是 DNS 名称）：

```
config ap primary-base Cisco_ea:5e:63
```

- 在 4.2 或更高版本的控制器上，AP 可以使用 Syslog 服务器发送故障排查信息。默认情况下，信息是以本地广播形式发送。如果 AP 与 syslog 服务器不在同一子网，最好改为单播地址，以便能够收集这些信息，并减少可能的由于 syslog 消息发送给本地的广播而造成的广播风暴，这种情况下，在同一子网的所有 AP 将受到影响。下面是检查这个设定的命令：

```
(WiSM-slot1-1) >show ap config general AP1130-9064
```

```

Cisco AP Identifier..... 164
Cisco AP Name..... AP1130-9064
Country code..... BE - Belgium
Regulatory Domain allowed by Country..... 802.11bg:-E
802.11a:-E

```

```

AP Country code..... BE - Belgium
AP Regulatory Domain..... 802.11bg:-E
802.11a:-E
Switch Port Number ..... 29
MAC Address..... 00:16:46:f2:90:64
IP Address Configuration..... DHCP
IP Address..... 192.168.100.200
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 192.168.100.1
Telnet State..... Disabled
Ssh State..... Disabled
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch Name..... Cisco_ea:5e:63
Primary Cisco Switch IP Address..... Not Configured
Secondary Cisco Switch Name.....
Secondary Cisco Switch IP Address..... Not Configured
Tertiary Cisco Switch Name.....
Tertiary Cisco Switch IP Address..... Not Configured
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Global: Disabled,
Local:
  Disabled
Remote AP Debug ..... Disabled
S/W Version ..... 5.0.152.0
Boot Version ..... 12.3.7.1
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... Power injector /
Normal mode
Number Of Slots..... 2
AP Model..... AIR-LAP1131AG-E-K9
IOS Version.....
12.4(20080324:062820)
Reset Button..... Enabled

```

```

AP Serial Number..... FHK0952C0FC
AP Certificate Type..... Manufacture
Installed
Management Frame Protection Validation..... Enabled (Global MFP
Disabled)
AP User Mode..... AUTOMATIC
AP User Name..... cisco
Cisco AP system logging host..... 255. 255. 255. 255

```

在控制器上为所有 AP 指定可用的 Syslog 服务器地址：

```
config ap syslog host global 10.48.76.33
```

- 在 4.2 或更高版本的控制器上，可以对 AP 的控制端口设置本地验证（物理访问 AP），建议为所有 AP 设置一个用户名和密码。下面是检测这个配置的命名：

```
(WiSM-slot1-1) >show ap config general AP1130-9064
```

```

Cisco AP Identifier..... 164
Cisco AP Name..... AP1130-9064
Country code..... BE - Belgium
Regulatory Domain allowed by Country..... 802.11bg:-E
802.11a:-E
AP Country code..... BE - Belgium
AP Regulatory Domain..... 802.11bg:-E
802.11a:-E
Switch Port Number ..... 29
MAC Address..... 00:16:46:f2:90:64
IP Address Configuration..... DHCP
IP Address..... 192.168.100.200
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 192.168.100.1
Telnet State..... Disabled
Ssh State..... Disabled
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch Name..... Cisco_ea:5e:63
Primary Cisco Switch IP Address..... Not Configured
Secondary Cisco Switch Name.....

```

```

Secondary Cisco Switch IP Address..... Not Configured
Tertiary Cisco Switch Name.....
Tertiary Cisco Switch IP Address..... Not Configured
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Global: Disabled,
Local:
  Disabled
Remote AP Debug ..... Disabled
S/W Version ..... 5.0.152.0
Boot Version ..... 12.3.7.1
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... Power injector /
Normal mode
Number Of Slots..... 2
AP Model..... AIR-LAP1131AG-E-K9
IOS Version.....
12.4(20080324:062820)
Reset Button..... Enabled
AP Serial Number..... FHK0952C0FC
AP Certificate Type..... Manufacture
Installed
Management Frame Protection Validation..... Enabled (Global MFP
Disabled)
AP User Mode..... AUTOMATIC
AP User Name..... cisco

```

控制器在 4.2 和 4.1 Mesh 版本中，为所有 AP 设置的用户名及密码配置：

```
config ap username Cisco password AnotherComplexPass all
```

控制器在 5.0 或 5.0 以后版本，为所有 AP 设置的用户名及密码配置：

```
config ap mgmtuser add username cisco password Cisco123 secret
  AnotherComplexPass all
```

如何把 WLC 崩溃文件从 WLC 传输到 TFTP 服务器

这些命令是为了把 WLC 崩溃文件从 WLC 传输到 TFTP 服务器。

```
transfer upload datatype crashfile
transfer upload serverip <IP address of the TFTP Server>

transfer upload path <Enter directory path>

transfer upload filename <Name of the Crash File>

transfer upload start <yes>
```

注:当你输入目录路径时, "/"通常代表在 TFTP 服务器上的缺省根目录。

这是一个例子:

```
(Cisco Controller) > debug transfer tftp enable

(Cisco Controller) > debug transfer trace enable

(Cisco Controller) > transfer upload datatype crashfile

(Cisco Controller) > transfer upload filename aire2cra.txt

(Cisco Controller) > transfer upload path /

(Cisco Controller) > transfer upload serverip XYZA

(Cisco Controller) > transfer upload start

Mode..... TFTP TFTP Server
IP..... XYZA TFTP
Path..... / TFTP
Filename..... aire2cra.txt Data
Type..... Crash File

Are you sure you want to start? (y/N) yes
```

Thu Dec 29 10:13:17 2005: RESULT_STRING: TFTP Crash File transfer starting.

Thu Dec 29 10:13:17 2005: RESULT_CODE:1

TFTP Crash File transfer starting.

Thu Dec 29 10:13:21 2005: Locking tftp semaphore, pHost=XYZA

pFilename=/aire2cra.txt Thu Dec 29 10:13:22 2005:

Semaphore locked, now unlocking,

pHost=XYZA pFilename=/aire2cra.txt Thu Dec 29 10:13:22 2005:

Semaphore successfully unlocked,

pHost=XYZA pFilename=/aire2cra.txt Thu Dec 29 10:13:22 2005:

tftp rc=0, pHost=XYZA pFilename=/aire2cra.txt

pLocalFilename=/mnt/application/bigcrash

Thu Dec 29 10:13:22 2005: RESULT_STRING: File transfer operation completed successfully.

Thu Dec 29 10:13:22 2005: RESULT_CODE:11 File transfer operation completed successfully.

【译者注】