

目录

第 1 章 Local AP配置	1-1
1.1 Local AP配置介绍	1-1
1.2 Local AP基本配置	1-1
1.3 Local AP配置举例	1-3
1.4 Local AP排错帮助	1-5
第 2 章 无线特性开启与关闭	2-1
2.1 无线特性开启与关闭简介	2-1
2.2 无线特性开启与关闭配置	2-1
2.3 无线特性开启与关闭排错帮助	2-2
第 3 章 自动发现与集群建立	3-1
3.1 自动发现与集群建立简介	3-1
3.2 自动发现与集群建立配置	3-1
3.3 自动发现配置举例	3-2
3.4 自动发现排错帮助	3-5
第 4 章 自动部署与双向认证	4-1
4.1 双向认证简介	4-1
4.2 自动部署简介	4-1
4.3 自动部署与双向认证配置	4-1
4.4 自动部署配置举例	4-3
4.5 自动部署与双向认证排错帮助	4-6
第 5 章 集群自动选举	5-1
5.1 集群自动选举简介	5-1
5.2 集群自动选举配置	5-1
5.3 集群自动选举配置举例	5-1
5.4 集群自动选举排错帮助	5-2
第 6 章 配置推送	6-1
6.1 配置推送简介	6-1
6.2 配置推送配置	6-1
6.3 配置推送配置举例	6-2
6.4 配置推送排错帮助	6-2

第 7 章 AP FLOOD反制	7-1
7.1 AP FLOOD反制简介.....	7-1
7.2 AP FLOOD反制配置.....	7-1
7.3 AP FLOOD反制举例.....	7-2
7.4 AP FLOOD反制排错帮助.....	7-3
第 8 章 集群维护与调试	8-1
8.1 集群维护与调试简介.....	8-1
8.2 集群维护与调试配置.....	8-1

第1章 Local AP 配置

1.1 Local AP配置介绍

WLAN 的集群管理采用 AC+Fit AP 的模式。在 AC 上面可以对 AP 进行基本的配置管理操作。这些配置操作主要包括向 Valid AP 表中添加 AP、配置 AP 的位置信息、配置 AP 与 AC 之间进行认证的密码、为 AP 指定配置文件等。

AP 上线时需要向 AC 作认证，认证通过 AC 才允许 AP 上线，认证不通过则不能让 AP 上线。目前 AP 的认证方式有 mac、none、pass-phrase、serial-num 几种，其中 serial-num 方式为基于 AP 的序列号认证，该序列号是 AP 出厂时自带的，在 AP 的 console 模式使用 get system 命令可看到其序列号（“serial-number”一栏即是 AP 的序列号）。AP 向 AC 连接作认证时，AC 根据 AP 上报的序列号从本地查找该 AP 的序列号并作比较，如果相同则认证成功，如果不同则认证失败。

1.2 Local AP基本配置

Local AP 的基本配置序列：

- 1. 向 Valid AP 列表中添加 AP 记录
- 2. 配置 AP 的位置信息
- 3. 配置 AP 的管理模式
- 4. 配置 AP 与 AC 认证的密码
- 5. 配置 AP 认证模式
- 6. 配置 AC 上 AP 的序列号
- 7. 指定 AP 的认证方式
- 8. 配置 ap 的管理 ip 地址
- 9. 向关联到的 AP 下发配置参数

1. 向 Valid AP 列表中添加 AP 记录

命令	解释
无线全局配置模式	
ap database <macaddr> no ap database <macaddr>	向 Valid AP 表中添加一条记录，并进入到该 AP 的配置模式。本命令的 no 操作为从 Valid AP 表中删除记录。

2. 配置 AP 的位置信息

命令	解释
AP 配置模式	

location <value>	为 AP 添加位置描述信息。此命令的 no 操作
no location	为删除 AP 当前的位置描述信息。

3. 配置 AP 的管理模式

命令	解释
AP 配置模式	
mode {ws-managed standalone rogue}	配置 AP 的管理模式。默认 AP 的管理模式为 ws-managed。

4. 配置 AP 与 AC 认证的密码

命令	解释
AP 配置模式	
password plain <word> no password	为 AP 添加/取消与 AC 认证的密码。密码格式为明文密码。
password encrypted no password	为 AP 指定密文格式的密码。

5. 配置 AP 认证模式

命令	解释
无线全局配置模式	
ap authentication {none mac pass-phrase}	配置 AP 认证模式。
ap authentication serial-num	配置 AC 上 AP 的认证方式为序列号认证。

6. 配置 AC 上 AP 的序列号

命令	解释
AP database 配置模式	
serial-num no serial-num	在 AC 上配置 AP 的序列号, no 命令删除 AC 上配置的 AP 序列号。

7. 指定 AP 的认证方式

命令	解释
无线全局配置模式	
ap validation {local radius}	设置 AP 的认证方式为本地 (local) 或通过 RADIUS 服务器认证。默认采用本地认证方式。

8. 配置 ap 的管理 ip 地址

命令	解释
AP 配置模式	
management {ip A.B.C.D/M ipv6 X:X::X:X/M} no management {ip ipv6}	配置 ap 的管理 ip 地址。此命令的 no 命令删除 AP 的管理 ip 地址。

9. 向关联到的 AP 下发配置参数

命令	解释
特权模式	
wireless ap eth-parameter apply [macaddr profile<1-1024>]	向关联到的 AP 下发配置参数。

1.3 Local AP配置举例

典型案例 1:

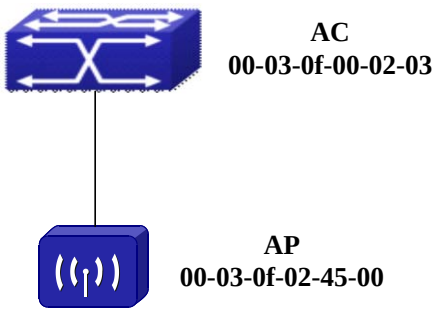


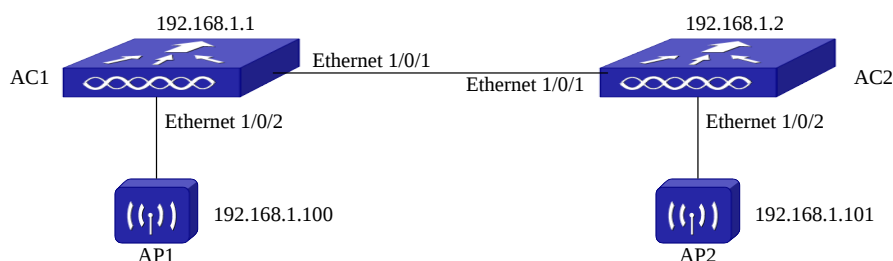
图 1-1 Local AP 典型案例

如图 1-1 所示的拓扑，在 AC 上面对与之关联的 AP 进行配置。配置 AP 的位置信息为“here”，profile id 为 2。

AC 的配置序列：

```
AC#config
AC(config)#wireless
AC(config-wireless)#ap database 00-03-0f-02-45-00
AC(config-ap)#location here
AC(config-ap)#profile 2
AC(config-ap)#exit
AC(config-wireless)#exit
AC(config)#
```

典型案例 2:



AC1 管理 AP1, AC1 和 AC2 之间建立集群关系, 默认 AC1 和 AC2 之间、AC1 和 AP1 之间采用 TLS 协议连接, 如果要使得 AP1 采用序列号认证被 AC1 管理需要进行如下设置:

首先, 开启 AC1 上 AP 的序列号认证:

```
AC#config
```

```
AC(config)#wireless
```

```
AC(config-wireless)# ap authentication serial-num
```

确认采用 TCP 连接方式, 提示会导致网络中断:

查看当前 AP 的认证方式:

```
AC#show wireless
```

```

Administrative Mode..... Enable
Operational Status..... Enabled
WS IP Address..... 172.20.32.2
WS IPv6 Address..... ----
WS Auto IP Assign Mode ..... Disable
WS Switch Static IP ..... 172.20.32.2
WS Switch Static IPv6 ..... ----
AP Authentication Mode..... Serial-Num
AP Auto Upgrade Mode..... Disable
AP Validation Method..... Local
Client Roam Timeout (secs)..... 30
Country Code..... CN - China
Peer Group ID..... 1
Cluster Priority..... 1
Cluster Controller..... Yes
Cluster Controller IP Address..... 172.20.32.2
Cluster Controller IPv6 Address..... ----
Wireless System IP control port..... 57775
Wireless Management Protocol..... TCP
AP Client QoS Mode..... Enable
AP Igmp Snooping Mode..... Disable
  
```

Switch Provisioning..... Enable
Network Mutual Authentication Mode..... Enable
Unmanaged AP Re-provisioning Mode..... Enable
Network Mutual Authentication Status..... Not Started
Regenerate X.509 Certificate Status..... Not In Progress
Keep Alive Interval(ms)..... 10000
Keep Alive Max Count..... 3
Force Wifi Compatible..... Disable
Statistics Interval(secs)..... Auto(5)
Rf Scan Report Interval(secs)..... Auto(30)

在 AC1 上配置 AP1 的序列号，假设 AP1 的 database 为 00-01-02-03-04-05，其序列号为 112233，配置方法如下：

```
AC#config
AC(config)#wireless
AC(config-wireless)# ap database 00-01-02-03-04-05
AC(config-ap)#serial-num 112233
```

1.4 Local AP排错帮助

- ☞ 如果对 AP 所做的配置不生效，请检查 AP 是否处于 Managed 状态。如果 AP 已经处于 Managed 状态，需要复位 AP 后才能使配置生效。
- ☞ 在使用 AP 序列号认证功能时，可能会出现 AP 认证失败等问题，请检查是否是如下原因：
 - (1) AP 是否有序列号，可在 AP 的 console 模式使用 get system 命令查看 serial-number 一行；
 - (2) AC 上是否配置了 AP 的序列号；
 - (3) AC 上是否开启了 AP 序列号认证模式，默认是 mac 认证。

第2章 无线特性开启与关闭

2.1 无线特性开启与关闭简介

无线特性作为控制器的一个重要功能，允许人为的启动和关闭。无线特性的开启过程，具体来说就是整个 WLAN 模块的初始化过程，它负责申请资源，并开启一个个的子功能；而关闭功能则负责释放资源，并关闭一个个的子功能。

2.2 无线特性开启与关闭配置

无线特性开启与关闭的配置序列如下：

1. 进入无线全局配置模式
2. 打开/关闭 AC 的无线特性
3. 配置无线特性自动指定 IP 地址功能（推荐通过配置 Loopback 接口及其三层接口地址以保证自动指定的无线 IP 地址的稳定性）
4. 为无线特性绑定静态 IP

1. 进入无线全局配置模式

命令	解释
全局配置模式	
wireless	进入 AC 的无线全局配置模式。

2. 打开/关闭 AC 的无线特性

命令	解释
无线全局配置模式	
enable no enable	开启/关闭 AC 的无线特性。

3. 配置无线特性自动指定 IP 地址的功能（推荐通过配置 Loopback 接口及其三层接口地址以保证自动指定的无线 IP 地址的稳定性）

命令	解释
无线全局配置模式	
auto-ip-assign no auto-ip-assign	打开/关闭无线特性自动指定 IP 地址功能。

4. 为无线特性绑定静态 IP

命令	解释
无线全局配置模式	
static-ip <ipaddr> no static-ip	为无线特性绑定静态 IP 地址。本命令的 no 操作为取消为无线特性绑定的静态 IP 地址。
static-ipv6 <ipv6addr> no static-ipv6	为无线特性绑定静态 IPv6 地址。本命令的 no 操作为取消为无线特性绑定的静态 IPv6 地址。

2.3 无线特性开启与关闭排错帮助

如果 AC 的无线特性开启失败，请检查是否是由于一下原因所导致：

- ☞ AC 是否存在 up 的三层接口或者 loopback 接口。
- ☞ AC 的三层接口或者 loopback 接口是否正确配置了 IP 地址。

第3章 自动发现与集群建立

3.1 自动发现与集群建立简介

通过自动发现功能，多台 AP 与 AC 设备可以自动两两建立连接，组成集群并提供无线服务。本功能提供了静态配置、DNS、DHCP 等多种自动发现模式。自动发现机制基于 IP，因此可以发现并不在同一网段的设备。

3.2 自动发现与集群建立配置

自动发现功能的配置序列如下：

1. 向 UDP 自动发现的 IP 地址列表中添加 IP 地址
2. 配置自动发现模式
3. 配置二层广播发现的 VLAN ID
4. 配置 AC 的集群标识
5. 配置保活消息发送的时间间隔
6. 配置保活消息发送的最大次数

1. 向 UDP 自动发现的 IP 地址列表中添加 IP 地址

命令	解释
无线全局配置模式	
discovery ip-list <ipaddr> no discovery ip-list [<ipaddr>]	向 UDP 自动发现的 IP 列表中添加/删除 IP 地址。
discovery ipv6-list <ipv6addr> no discovery ipv6-list [<ipv6addr>]	向 UDP 自动发现的 IPv6 列表中添加/删除 IPv6 地址。

2. 配置自动发现模式

命令	解释
无线全局配置模式	
discovery method [ip-poll l2-multicast] no discovery method [ip-poll l2-multicast]	配置自动发现的模式。本命令的 no 操作为取消自动发现模式。

3. 配置二层广播发现的 VLAN ID

命令	解释
----	----

无线全局配置模式	
discovery vlan-list <1-4094> no discovery vlan-list [<1-4094>]	向二层广播发现的 vlan 列表中添加/删除 vlan ID。

4. 配置 AC 的集群标识

命令	解释
无线全局配置模式	
peer-group <1-255> no peer-group	配置 AC 的集群标识。本命令的 no 操作为取消配置的 AC 集群标识, 恢复为默认值 1。

5. 配置保活消息发送的时间间隔

命令	解释
无线全局配置模式	
keep-alive-interval <5000-60000>	设置 AC 发送 keep alive 消息的时间间隔。

6. 配置保活消息发送的最大次数

命令	解释
无线全局配置模式	
keep-alive-max-count<1-15>	设置 AC 发送保活 keep alive 消息的最大发送次数。

3.3 自动发现配置举例

1. 基于 IP 列表的自动发现配置举例

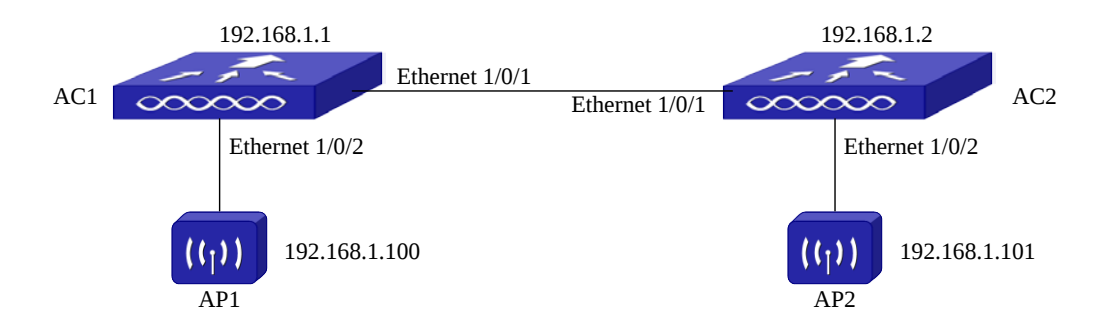


图 3-1 IP 自动发现典型应用环境

如图 3-1 所示拓扑, AC1 的无线地址为 192.168.1.1, AC2 的无线地址为 192.168.1.2。AP1 的地址为 192.168.1.100, AP2 的地址为 192.168.1.101。AC1 和 AC2 上面均有 AP1 和 AP2 的 ap database。现在 AC1、AC2 以及 AP1、AP2 需要建立集群, 可以通过下面的基于 IP 列表的自动发现配置来实现:

AC1 配置:

```
AC(config-wireless)#enable
AC(config-wireless)#discovery ip-list 192.168.1.2
AC(config-wireless)#discovery ip-list 192.168.1.100
AC(config-wireless)#discovery ip-list 192.168.1.101
AC(config-wireless)#discovery method ip-poll
```

AC2 配置:

```
AC(config-wireless)#enable
AC(config-wireless)#discovery ip-list 192.168.1.1
AC(config-wireless)#discovery ip-list 192.168.1.100
AC(config-wireless)#discovery ip-list 192.168.1.101
AC(config-wireless)#discovery method ip-poll
```

2. 基于 IPv6 列表的自动发现配置举例

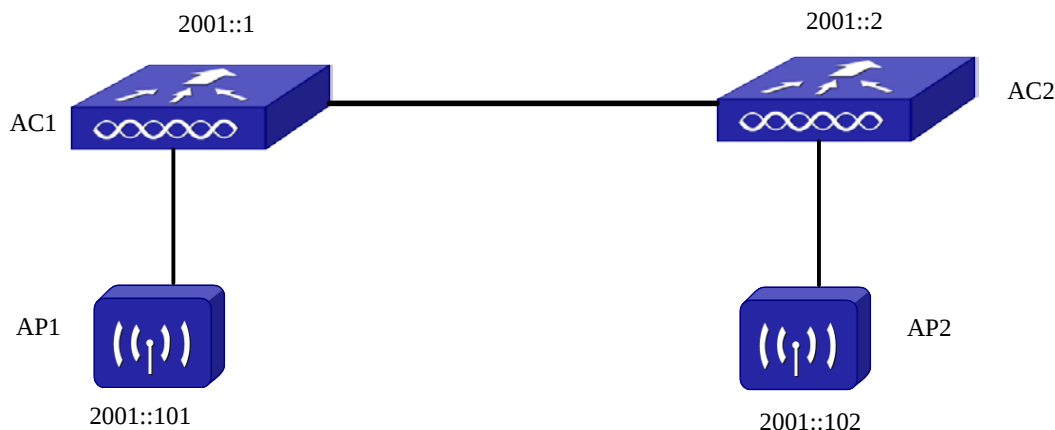


图 3-2 IPv6 自动发现典型应用环境

如图 3-2 所示拓扑，AC1 的无线地址为 2001::1，AC2 的无线地址为 2001::2。AP1 的地址为 2001::100，AP2 的地址为 2001::101。AC1 和 AC2 上面均有 AP1 和 AP2 的 ap database。现在 AC1、AC2 以及 AP1、AP2 需要建立集群，可以通过下面的基于 IP 列表的自动发现配置来实现：

AC1 配置:

```
AC (config-wireless)# no discovery ip-list 192.168.1.2
AC (config-wireless)#no auto-ip-assign
AC (config-wireless)#enable
AC (config-wireless)#static-ipv6 2001::1
AC (config-wireless)#enable
AC (config-wireless)#discovery ipv6-list 2001::2
AC(config-wireless)# discovery method ip-poll
AC (config-wireless)#sho wireless peer-switch
```

		Disc.	
IP Address	Vendor ID	Reason	Age

2001::2	Digital China (Shan.	IP Poll	0d:00:00:08
AC (config-wireless)#			
AC(config-wireless)# discovery ipv6-list 2001::101			
AC(config-wireless)# discovery ipv6-list 2001::102			
AC(config-wireless)#discovery method ip-poll			

AC2 配置:

```
AC (config-wireless)# no discovery ip-list 192.168.1.1
AC (config-wireless)#no auto-ip-assign
AC (config-wireless)#enable
AC (config-wireless)#static-ipv6 2001::2
AC (config-wireless)#enable
AC(config-wireless)# discovery method ip-poll
AC(config-wireless)# discovery ipv6-list 2001::101
AC(config-wireless)# discovery ipv6-list 2001::102
AC(config-wireless)# discovery method ip-poll
```

3. 基于二层广播的自动发现配置举例

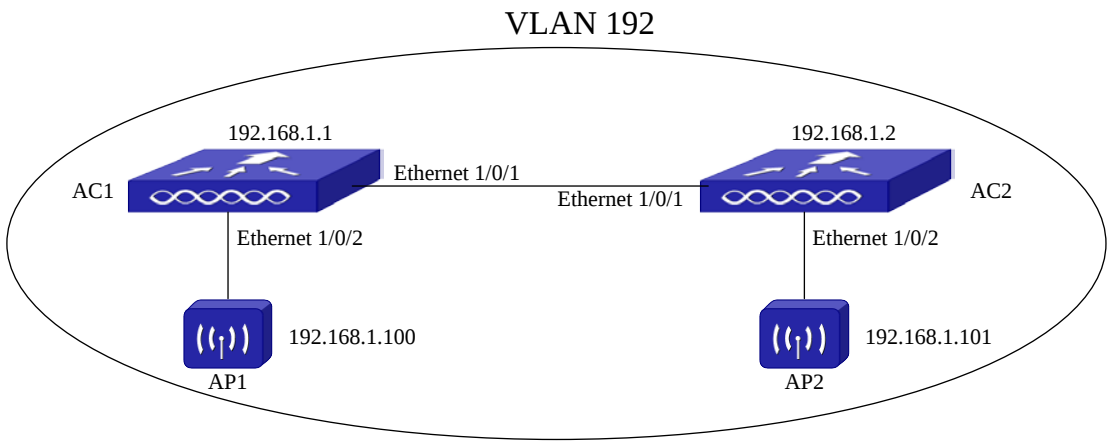


图 3-3 基于二层广播的自动发现典型环境

如图 3-3 所示，AC1、AC2 以及 AP1、AP2 建立集群。所有设备均在 VLAN192 中。AC1 和 AC2 的端口 Ethernet1/0/1 和 Ethernet1/0/2 均划入 VLAN192。AC1 和 AC2 采用二层广播自动发现，配置方法如下：

AC1 配置:

```
AC(config)#vlan 192
AC(config-vlan192)#switchport interface Ethernet 1/0/1;1/0/2
AC(config-vlan192)#exit
```

```
AC(config)#wireless
AC(config-wireless)#enable
AC(config-wireless)#discovery vlan-list 192
AC(config-wireless)#discovery method l2-multicast
```

AC2 配置:

```
AC(config)#vlan 192
AC(config-vlan192)#switchport interface Ethernet 1/0/1;1/0/2
AC(config-vlan192)#exit
AC(config)#wireless
AC(config-wireless)#enable
AC(config-wireless)#discovery vlan-list 192
AC(config-wireless)#discovery method l2-multicast
```

3.4 自动发现排错帮助

如果自动发现功能不能正常使用, 请检查是否是以下原因造成:

- ☞ 被发现的 AC 或者 AP 的 ip 地址是否存在于 ip 自动发现列表中;
- ☞ 被发现的 AC 或者 AP 所属的 VLAN 是否存在于二层广播自动发现的 VLAN 列表中;
- ☞ 在使用控制器作为 DHCP Server 时, 是否存在 AP 自动获取的地址与网络中其他设备的静态地址有冲突, 如果存在这种情况, 可以通过 `ip dhcp conflict ping-detection enable` 命令使能 DHCP Server 上面的防止冲突的 ping 检测功能来避免这种情况; 同样的, 这种方法也可以避免为关联到 AP 上面的客户端分配与其他设备静态地址冲突的 IP 地址;
- ☞ 通过 `show wireless discovery` 命令查看相应的自动发现方式是否已经打开;
- ☞ 网络是否连通。

第4章 自动部署与双向认证

4.1 双向认证简介

网络是一个开放的空间，为了避免未知的设备加入集群，而造成潜在的风险，可以开启双向认证的功能。此功能是通过颁发 X.509 证书的方式，仅能让拥有证书的设备通过认证，加入集群。此功能还包括证书的生成，分发，保存，使用等。

在 AC 之间和 AC 与 AP 之间建立连接，组成集群都是通过自动发现来实现的。自动发现机制配置灵活简便，但是缺乏安全性。无线控制器集群管理功能通过增加双向认证机制来增强安全性，防止未授权的设备接入集群中。具体的做法就是，每台设备通过 RC4+MD5 算法生成唯一的私钥和公钥（证书），然后通过证书交换功能或者证书请求功能为对方授权，进而交换证书。在此之后，双方进行 TLS 连接时，互相对比证书，在确定一致后，才能够建立 TLS 连接。对于本集群而言，AC 之间的证书传递是通过证书交换和证书请求功能实现的，而 AC 与 AP 之间的证书传递是通过 AP 自动部署实现的。

4.2 自动部署简介

本集群支持双向认证功能以提高安全性，而双向认证要求发现双方都保存有对端的证书，于是证书的分发和传递成为一个问题。集群管理支持最基本也最直接的人工分发功能，可以将证书认为的复制到相应的设备上。为了提高自动程度，也便于整个集群的统一管理，集群提供了自动部署功能来分发证书。

自动部署包括对 AP 的部署和对 AC 的部署。对 AP 的部署通过 AC Controller 来进行，既可以重新部署已加入集群的 AP，也可以部署未加入集群的 AP（AP 的重新部署）。只要在 AC Controller 上为 AP 指定了 AC，它们相互认证所需的证书就会在集群中自动传递，然后要做的就是自动发现了。对 AC 的部署就是将 AC 加入到集群中，这台 AC 需要获得集群中全部 AC 的证书，而集群中每台 AC 也需要获得这台 AC 的证书，具体是由集群中任意一台 AC 实现的，它负责 AC 之间证书的中转。

4.3 自动部署与双向认证配置

自动部署与双向认证配置序列：

1. 删除 AP Provisioning 表中的 AP 记录
2. 为 AP 指定在自动部署时生效的 Profile ID
3. 为自动部署的 AP 配置 Primary AC 和 Backup AC
4. 启动自动部署过程
 - （1）AC Controller 上启动 AP 的自动部署
 - （2）AC 上面启动本机的自动部署功能

(3) 与指定的 AC 开始自动部署

(4) Un-Managed AP 重部署

5. X.509 证书配置操作

(1) AC 上面生成 X.509 证书

(2) 触发 AC 自动部署前向对端请求 X.509 证书

(3) 初始化 X.509 证书交换的触发器

6. 设置 AP Provisioning 表中记录的老化时间

7. 开启集群的双向认证功能

1. 删除 AP Provisioning 表中的 AP 记录

命令	解释
特权模式	
clear wireless ap provisioning [<macaddr>]	删除 AP Provisioning 表中某一条 AP 的记录或者全部 AP 的记录。

2. 为 AP 指定在自动部署时生效的 Profile ID

命令	解释
特权模式	
wireless ap provision <macaddr> profile <1-1024> no wireless ap provision <macaddr> profile	为 AP 指定 Profile ID 并在自动部署的时候生效。本命令的 no 操作会取消为 AP 指定的 Profile ID。

3. 为自动部署的 AP 配置 Primary AC 和 Backup AC

命令	解释
特权模式	
wireless ap provision <macaddr> switch {backup primary} {<ipaddr> <ipv6addr>}	为自动部署的 AP 指定 Primary AC 和 Backup AC。默认 AC 的地址为 0.0.0.0。

4. 启动自动部署过程

命令	解释
特权模式	
wireless ap provision start	在 AC Controller 上面启动 AP 自动部署过程。
无线全局模式	
switch-provisioning no switch-provisioning	启动 AC 本机的自动部署过程。

特权模式	
wireless switch provision <ip address>	通知本地 AC 与指定的 AC 开始自动部署过程。

5. X.509 证书配置操作

命令	解释
特权模式	
wireless certificate-generate	在 AC 上面生成 X.509 证书。
wireless switch certificate-request {<ipaddr> <ipv6addr>}	使 AC 自动部署前向对端请求 X.509 证书。
wireless cluster exchange-certificate	初始化 X.509 证书交换的触发器。

6. 设置 AP Provisioning 表中记录的老化时间

命令	解释
无线全局配置模式	
agetime ap-provisioning-db <0-240> no agetime ap-provisioning-db	为 AP Provisioning 表中的记录设置老化时间。本命令的 no 操作恢复老化时间为默认值（72 小时）。

7. 开启集群的双向认证功能

命令	解释
无线全局配置模式	
mutual-authentication-mode no mutual-authentication-mode	在整个集群内开启双向认证功能。本命令的 no 操作在整个集群内关闭双向认证功能。

4.4 自动部署配置举例

1. 对已管理 AP 的自动部署举例

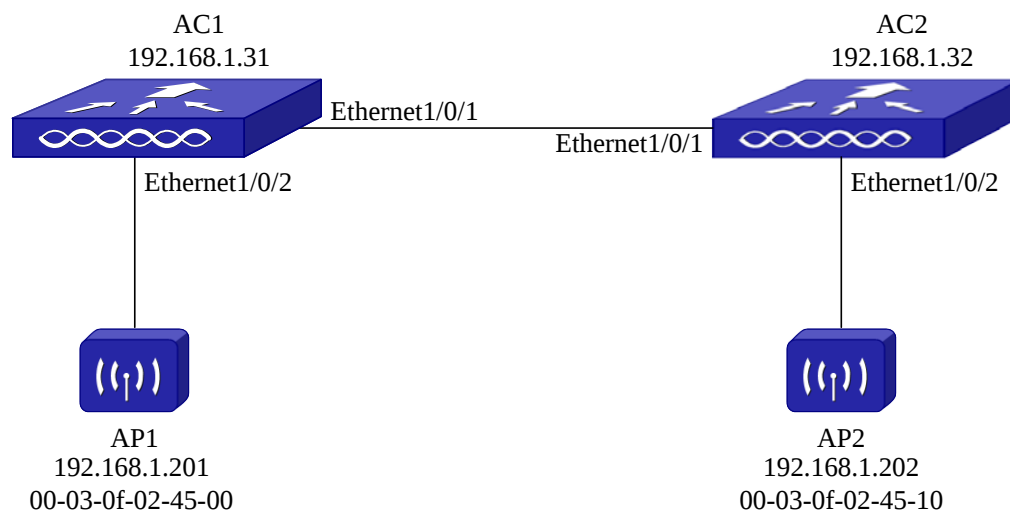


图 4-1 managed-AP 自动部署典型应用环境

如图 4-1 所示的环境。AC1 为 Controller。AP1 由 AC1 管理，AP2 由 AC2 管理。在 AC1 上面对 AP1 和 AP2 进行自动部署，primary AC 为 AC2，backup AC 为 AC1。配置方法如下：

AC1 配置：

```
AC#wireless ap provision 00-03-0f-02-45-00 switch primary 192.168.1.32
```

```
AC#wireless ap provision 00-03-0f-02-45-00 switch backup 192.168.1.31
```

```
AC#wireless ap provision 00-03-0f-02-45-10 switch primary 192.168.1.32
```

```
AC#wireless ap provision 00-03-0f-02-45-10 switch backup 192.168.1.31
```

```
AC#wireless ap provision start
```

```
AC# wireless ap reset /*AP1、AP2 重启后均被 AC2 管理*/
```

2. 对未管理的 AP 进行自动部署举例

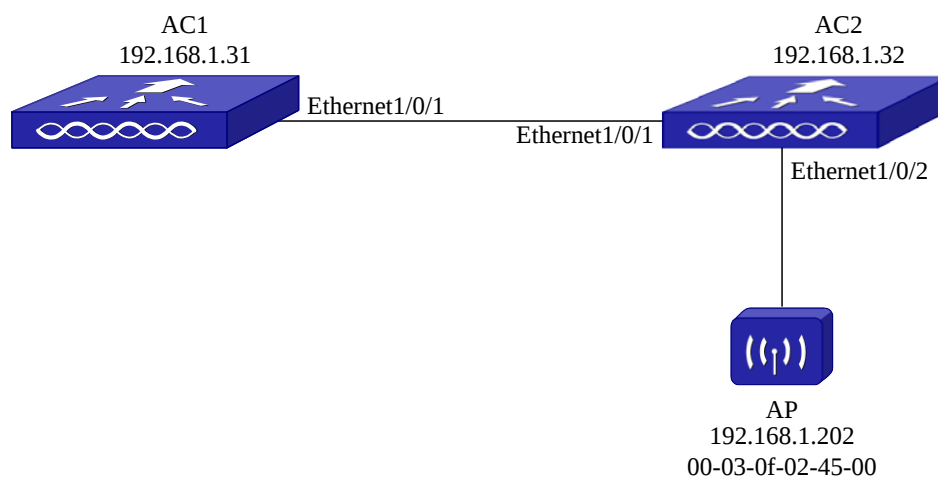


图 4-2 Unmanaged-AP 自动部署典型环境

如图 4-2 所示，AC1 和 AC2 建立集群，AC1 为 Controller。AP 处于未管理的状态。在 AC1 上面对 AP 进行自动部署，使之被 AC2 管理。

AC1 配置：

```
AC(config-wireless)#re-provisioning-unmanaged
```

This configuration will be sent to all switches in cluster.

Are you sure you want to continue? (y/n) y

Unmanaged AP Re-provisioning Mode set.

```
AC(config-wireless)#exit
```

```
AC(config)#exit
```

```
AC#wireless ap provision 00-03-0f-02-45-00 switch primary 192.168.1.32
```

```
AC#wireless ap provision start 00-03-0f-02-45-00
```

之后重启 AP，AP 重启后被 AC2 管理，AC2 上 show wi ap status 显示 AP 的“Status”为“Managed”，“Configuration Status”为“Success”

3. 对 AC 自动部署举例

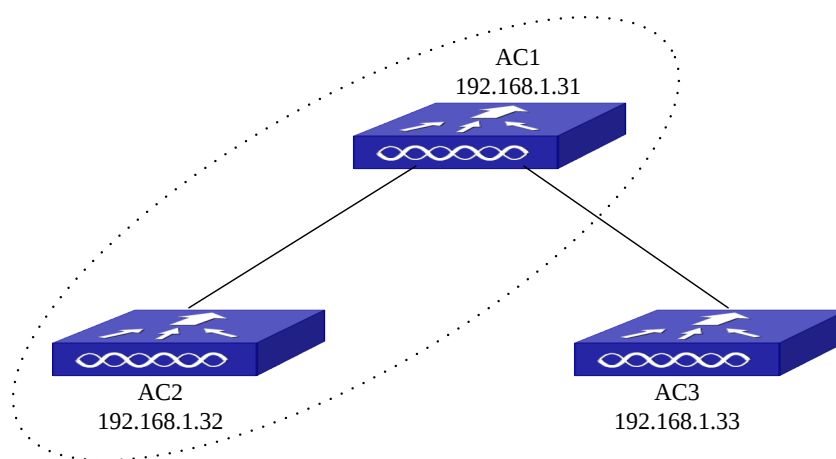


图 4-3 AC 自动部署典型环境

如图 4-3 所示，AC1 和 AC2 构成集群，AC1 为 AC Controller。AC3 在集群之外。现在需要让 AC3 加入到 AC1 和 AC2 的集群中，其方法是通过 AC 的自动部署，使得 AC3 与集群中任意一台 AC（此处为 AC1）建立 TLS 连接，进而使得 AC3 加入集群，并与集群中的其他 AC 建立连接。

配置方法：

首先，在 AC1 和 AC3 上面打开双向认证功能：

AC1 配置：

```
AC(config-wireless)# mutual-authentication-mode
```

Changing Mutual Authentication Mode might result in network traffic disruption. Are you

sure you want to continue? [Y/N]y

Network Mutual Authentication Mode set.

AC3 配置:

AC(config-wireless)# mutual-authentication-mode

Changing Mutual Authentication Mode might result in network traffic disruption. Are you sure you want to continue? [Y/N]y

Network Mutual Authentication Mode set.

其次, 在 AC1 上面请求 AC3 的 X.509 证书, 在 AC3 上面请求 AC1 的 X.509 证书:

AC1 配置:

AC#wireless switch certificate-request 192.168.1.33

AC3 配置:

AC#wireless switch certificate-request 192.168.1.31

最后, 在 AC3 上面与 AC1 进行自动部署:

AC3 配置:

AC#wireless switch provision 192.168.1.31

此时 AC3 和 AC1 可以建立连接, 进而与 AC2 建立连接。

4.5 自动部署与双向认证排错帮助

交换机作为有线无线智能一体化控制器存在第一次启动加载时间过长的现象。原因是交换机第一次启动需要生成双向认证所需的 X.509 证书, 这个时间大概在 20-30 分钟。此时终端无任何反应, 既无显示也无法输入, 等待 20-30 分钟后终端会提示端口 UP/DOWN 信息。这个是交换机正常现象。接下来用户可以输入相关命令进行管理。

在开启双向认证或者对 AP/AC 进行自动部署的过程中, 如果出现问题, 请检查是否如下原因引起:

- ☞ 对 AP 进行自动部署时, 是否指定了正确的 primary/backup AC 的 ip 地址。
- ☞ 双向认证时, AC 以及 AP 上面保存的证书是否正确。

第5章 集群自动选举

5.1 集群自动选举简介

为了使整个集群看起来像一个整体，用户需要一个统一的界面来进行统一的管理和配置。集群管理模块通过自动选举机制推举出一台 AC 来承担此角色。它负责收集集群中所有设备的全部信息，用户可以根据这些信息进行配置，然后这些配置会由它下发至对应的设备生效。这台 AC 称为 AC Controller。自动选举是根据预先配置的优先级和 IP 地址进行的，优先级最高，且 IP 最小的 AC 被共同推举为 AC Controller，如果这台 AC 发生了意外，集群成员会按照此规则推举出另一 AC 承担此角色，因此，自动选举机制还包含了备份的功能，即永远有后备的 AC Controller 存在。即使集群仅有一台 AC 构成，它自身就成为 AC Controller。在选举为 AC Controller 的那台 AC 上，可以查看集群中所有 AC、AP 和 Client 的信息，也可以查看到不属于该集群但是被发现的所有设备的情况。AC Controller 是自动生成的，相同的逻辑决定了集群中所有的 AC 选举结果的唯一性。

5.2 集群自动选举配置

集群自动选举功能的配置序列如下：

1. 配置 AC 在自动选举中的优先级

1. 配置 AC 在自动选举中的优先级

命令	解释
无线全局配置模式	
cluster-priority <0-255> no cluster-priority	配置/恢复 AC 的自动选举优先级。

5.3 集群自动选举配置举例

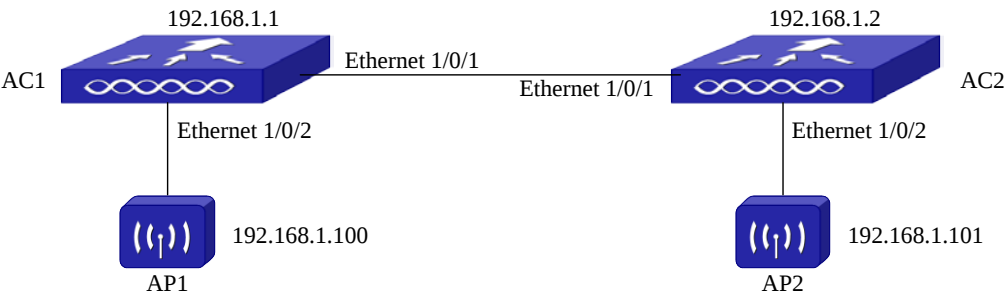


图 5-1 集群自动选举配置环境

如图 5-1 所示，AC1 和 AC2 建立集群。AC1 和 AC2 的地址分别为 192.168.1.1 和 192.168.1.2，初始的选举优先级均为 1，此时由于 AC1 的无线 ip 地址小，所以 AC1 为集群的 AC Controller。现在欲使 AC2 成为集群新的 AC Controller，可以将 AC2 的选举优先级配置为大于 1 的数值。

AC2 上面配置：

```
AC#config
```

```
AC(config)#wireless
```

```
AC(config-wireless)#cluster-priority 10
```

```
AC(config-wireless)#
```

修改了 AC2 的优先级以后，会触发新一轮 AC Controller 的选举，选举完成后 AC2 就可以成为集群新的 AC Controller。

5.4 集群自动选举排错帮助

如果指定的 AC 不能选举成为集群新的 AC Controller，请检查是否是如下原因造成的：

- ☞ 该 AC 的无线地址是否配置为集群中最小的无线 ip 地址；
- ☞ 该 AC 是否具有集群中最高的选举优先级；
- ☞ 该 AC 的选举优先级是否设置为 0，如果设置为 0 则不会参加 AC Controller 的选举。
- ☞ 可以通过 `debug wireless cluster packet all` 命令检查 AC 之间 keepalive 消息的发送与接收是否正常。

第6章 配置推送

6.1 配置推送简介

在很多情况下，都要求集群中某些或者全部 AC 的配置是一致的。本无线集群提供的功能是灵活多样的，但全部配置一遍也需要消耗不少时间。配置推送功能允许用户在配置完毕一台 AC 之后，将其配置自动传递并应用到集群中指定的任意多台 AC 上。只有 IP 地址，优先级和端口号等数据不在推送的范围内。

配置推送的发送方 AC 在推送出本地的配置之前，首先将保存全部配置，然后对这些配置属于予以推送。如果在推送过程中，发送方的配置被管理员改变了，改变后的配置在本地推送当中不会被传递至接收方。

目前 AC 所支持的能够进行配置推送的功能主要有：AP Database、AP Profile、Channel Power、Discovery、Global、Known Client、Captive Portal、RADIUS Client、QoS ACL 和 QoS DiffServ。其中，在进行配置推送时，Discovery 功能默认不进行推送，其余功能默认是进行配置推送的。

6.2 配置推送配置

AC 的配置推送功能配置序列如下：

1. 为 AC 指定配置推送时需要传递的配置；
2. 启动 AC 配置推送。

1. 为 AC 指定配置推送时需要传递的配置

命令	解释
无线全局配置模式	
peer-switch configuration [ap-database ap-profile captive-portal channel-power discovery global known-client radius-client] no peer-switch configuration [ap-database ap-profile captive-portal channel-power discovery global known-client radius-client]	为 AC 指定配置推送时需要传递的配置功能。 no 命令可以取消相应功能的配置推送。

2. 启动 AC 配置推送

命令	解释
特权用户模式	

wireless peer-switch configure [<ipaddr> <ipv6addr>]	启动 AC 的配置推送。
--	--------------

6.3 配置推送配置举例

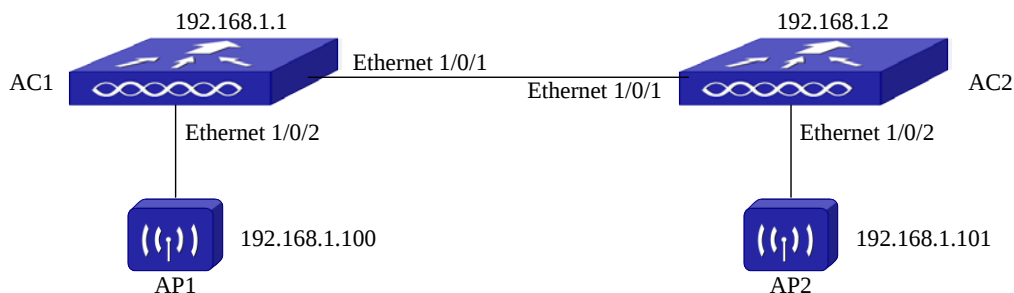


图 6-1 AC 配置推送功能典型应用环境

如图 6-1 所示的环境，AC1、AC2 以及 AP1、AP2 建立集群。现在要将 AC1 的无线配置推送到 AC2。需要传送的功能包括：AP Database、AP Profile、Channel Power、Discovery、Global、Known Client、QoS ACL 和 QoS DiffServ。

AC1 的配置如下：

```
AC(config)#wireless
AC(config-wireless)#peer-switch configuration discovery
AC(config-wireless)#no peer-switch configuration captive-portal
AC(config-wireless)#no peer-switch configuration radius-client
AC(config-wireless)#exit
AC(config)#exit
AC#wireless peer-switch configure 192.168.1.2
AC#
```

6.4 配置推送排错帮助

如果配置推送操作不能成功，请检查是否是由于下列原因造成的：

- ☞ 通过 show wireless peer-switch configuration 命令查看需要推送的功能是否已经选定（即状态为 Enabled）；
- ☞ 启动配置推送时 peer-switch 的 IP 地址是否正确；
- ☞ 启动配置推送时，如果对所有 peer-switch 进行推送（即不指定 peer-switch 的 IP 地址），请检查本机与 peer-switch 的 TLS 连接是否正常；
- ☞ 本机需要推送的配置中是否存在不正确或者配置推送不支持的配置内容。
- ☞ 如果配置推送的发送方和接收方的国家码不同，会由于不能推送 ap database 而导致配置推送失败。

第7章 AP FLOOD 反制

7.1 AP FLOOD反制简介

AP 与 AC 相互发现并建立 TLS 安全连接后，必须通过认证才能被 AC 成功管理。如果 AP 没有通过认证，则每隔 30 秒重新与 AC 进行一轮相互发现过程。当大量的 AP 都没有通过认证时，就会不断重复建立非常多的 TCP 连接，持续消耗大量的 CPU 资源，严重时 CPU 利用率持续为 100%。如果开启了 AP FLOOD 反制功能，当 AP 重连的次数在一定时间内超过限制，则暂时禁止其与 AC 建立 TCP 连接，防止 CPU 利用率持续过高。直到老化时间结束，或者管理员干预才能恢复连接。

7.2 AP FLOOD反制配置

AP FLOOD 反制功能配置序列如下：

1. 打开或关闭 AP FLOOD 反制功能
2. 配置 AP FLOOD 反制功能的检测时间
3. 配置 AP FLOOD 反制功能允许连接的最大次数
4. 配置 AP FLOOD 反制表的老化时间
5. 相关显示配置
6. 将 AP 从 AP FLOOD 反制表中清除

1. 打开或关闭 AP FLOOD 反制功能

命令	解释
无线全局配置模式	
wireless ap anti-flood no wireless ap anti-flood	打开/关闭 AP FLOOD 反制功能。

2. 配置 AP FLOOD 反制功能的检测时间

命令	解释
无线全局配置模式	
wireless ap anti-flood interval <1-15> no wireless ap anti-flood interval	设置 AP FLOOD 反制功能检测时间，no 命令将测时间恢复到默认值（5 分钟）。

3. 配置 AP FLOOD 反制功能允许连接的最大次数

命令	解释
----	----

无线全局配置模式	
wireless ap anti-flood max-conn-count <1-30> no wireless ap anti-flood max-conn-count	设置 AP FLOOD 反制功能的最大允许连接次数, no 命令将最大允许连接次数恢复到默认值 (4 次)。

4. 配置 AP FLOOD 反制表的老化时间

命令	解释
无线全局配置模式	
wireless ap anti-flood agetime <0-1440> no wireless ap anti-flood agetime	设置 AP FLOOD 反制表的老化时间, no 命令将老化时间恢复到默认值 (30 分钟)。

5. 相关显示配置

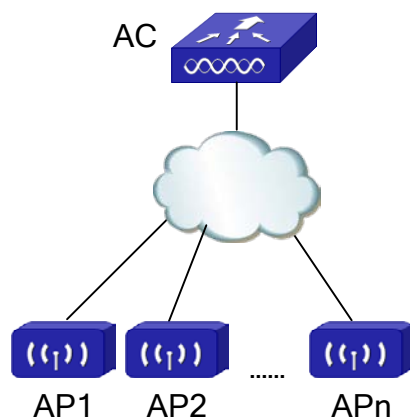
命令	解释
特权模式	
show wireless ap anti-flood	显示 AP FLOOD 反制当前的配置参数。
show wireless ap anti-flood status	显示 AP FLOOD 反制表中的所有记录。

6. 将 AP 从 AP FLOOD 反制表中清除

命令	解释
特权模式	
clear wireless ap anti-flood	清除 AP FLOOD 反制表中所有记录。

7.3 AP FLOOD反制举例

案例:



大量 AP 没有通过认证，不断的向 AC 发出连接请求。想实现检测到 AP 在 10 分钟之内与 AC 建立连接超过 5 次，则将其加入到 AP FLOOD 反制表中，并设置 60 分钟之内不允许 AP 再次连接，需要对 AC 进行如下操作：

首先，开启 AP FLOOD 反制功能，并配置参数

```
AC#config
```

```
AC(config)#wireless
```

```
AC(config-wireless)#wireless ap anti-flood
```

```
AC(config-wireless)#wireless ap anti-flood interval 10
```

```
AC(config-wireless)#wireless ap anti-flood max-conn-count 5
```

```
AC(config-wireless)#wireless ap anti-flood agetime 60
```

显示 AP FLOOD 反制参数配置：

```
AC(config-wireless)#show wireless ap anti-flood
```

显示 AP FLOOD 表中的所有记录：

```
AC(config-wireless)#show wireless ap anti-flood status
```

将 AP 从反制表中删除，使其再次进行连接，并关闭 AP FLOOD 反制功能：

```
AC#clear wireless ap anti-flood
```

```
Are you sure you want to clear the AP flood list? [Y/N]Y
```

```
All AP flood entries cleared.
```

```
AC#config
```

```
AC(config)#wireless
```

```
AC(config-wireless)#no wireless ap anti-flood
```

7.4 AP FLOOD反制排错帮助

在配置、使用 AP FLOOD 反制功能时，可能会由于物理连接、配置错误等原因导致本项反制未能正常运行或出现错误反制。请检查是否是如下原因：

- ☞ 应保证物理连接的正确无误
- ☞ 确认已启动 AP FLOOD 反制功能
- ☞ 可通过特权模式下的 `show logging buffered` 命令确认 AP 是否已在检测时间内完成了

限制的连接次数，连接最大次数之后才会被加入到 AP FLOOD 表中。

第8章 集群维护与调试

8.1 集群维护与调试简介

集群的维护与调试可以通过 debug 或者 SNMP 网管软件来进行。通过 SNMP 管理集群时，可以根据 AC 发送的 trap 信息来分析和定位集群中存在的故障。

8.2 集群维护与调试配置

集群维护与调试功能的配置序列如下：

1. 设置 trap 信息标志位
2. 设置 syslogs 信息标志位
3. 开启整个集群的 SNMP TRAP 功能
4. 打开/关闭集群 debug 信息
5. 打开/关闭 SSL 的 debug 信息

1. 设置 trap 信息的标志位

命令	解释
无线全局配置模式	
trapflags [{ap-failure ap-state client-failure client-state peer-ws rf-scan rogue-ap wids-status ws-status attack-event}]	开启 AC 上针对某些事件的 SNMP Trap 功能。本命令的 no 命令为关闭 AC 上面针对某些事件的 SNMP Trap 功能。
no trapflags [{ap-failure ap-state client-failure client-state peer-ws rf-scan rogue-ap wids-status ws-status attack-event }]	

2. 设置 syslogs 信息标志位

命令	解释
无线全局配置模式	
syslogflags [{ap-failure ap-state client-failure client-state peer-ws rogue-ap wids-status ws-status attack-event}]	开启无线 syslog 功能。本命令的 no 操作为关闭无线 syslog 功能。
no syslogflags [{ap-failure ap-state client-failure client-state peer-ws	

rogue-ap wids-status ws-status attack-event }}	
特权模式	
show wireless syslogsflags	显示 AC 的 syslogsflags 开关是否开启。

3. 开启整个集群的 SNMP TRAP 功能

命令	解释
全局配置模式	
snmp-server enable traps wireless no snmp-server enable traps wireless	开启整个集群中 AC 上的无线 SNMP Trap 功能。本命令的 no 命令为关闭整个集群中 AC 上的无线 SNMP Trap 功能。

4. 打开/关闭集群的 debug 信息

命令	解释
全局配置模式	
debug wireless cluster packet {all receive send dump} no debug wireless cluster packet {all receive send dump}	打开/关闭信息收集和集群控制报文打印调试信息。
debug wireless cluster internal no debug wireless cluster internal	打开/关闭信息收集和集群控制一般调试信息。

5. 打开/关闭 SSL 的 debug 信息

命令	解释
全局配置模式	
debug wireless ssl packet {all receive send} no debug wireless ssl packet {all receive send}	打开/关闭安全连接 SSL 报文打印调试信息。
debug wireless ssl timer no debug wireless ssl timer	打开/关闭安全连接 SSL 定时器调试信息。
debug wireless ssl error no debug wireless ssl error	打开/关闭安全连接 SSL 异常调试信息。
debug wireless ssl detail no debug wireless ssl detail	打开/关闭安全连接 SSL 详细调试信息。
debug wireless ssl internal no debug wireless ssl internal	打开/关闭安全连接 SSL 正常调试信息。