乾颐堂融合网络控制器

作者:现任明教教主

北京乾颐堂网络实验室出品

第一部分:Aireos漫游

第二部分:Intra-Controller Roaming

第三部分:Inter-Controller Roaming

第四部分:Inter-Subnet Roaming

内容简介

第一部分:Aireos漫游

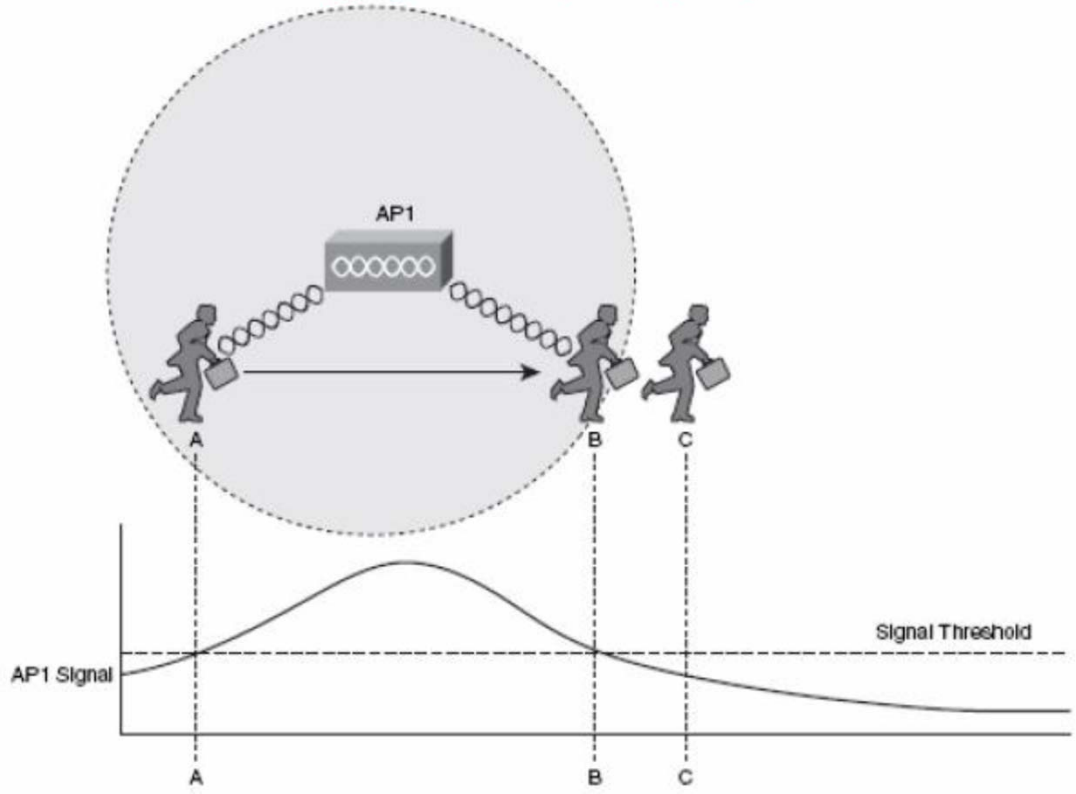
第二部分:Intra-Controller Roaming

第三部分:Inter-Controller Roaming

第四部分:Inter-Subnet Roaming

第一部分
Arieos漫游

AP覆盖范围



只要客户端在点A和B之间，就能够以可接受的质量接收AP的信号：客户端走出该覆盖范围（到达图中的C点）后，信号强度将低于可接受的阀值，导致客户端失去关联。

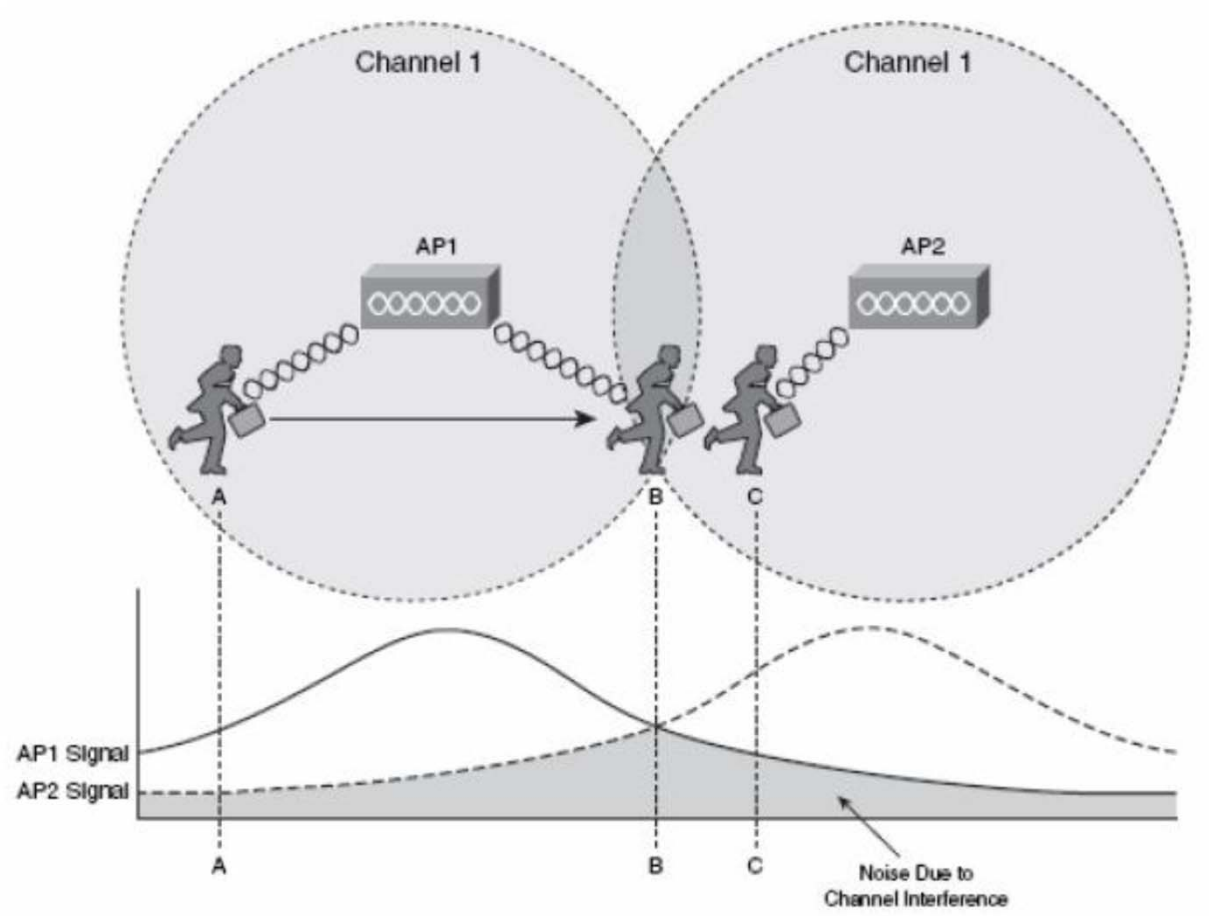
漫游

漫游指的是从一个AP将关联切换到与另一个AP关联，让无线连接在客户端移动时能够保持的过程。

两个AP被并排地放置，它们使用相同的信道，使用单个信道来建立大型覆盖区域看起来很直观，但实际上这是种糟糕的想法，因为客户端无法确定它在什么时候已离开一个 AP的蜂窝，进入到另一个 AP的蜂窝内。

当客户端移到B点时，应预测到需要漫游，即将关联从AP1切换到AP2，在两个AP的信道相互干扰的情况下，可能无法进行明确的漫游，实际上，客户端可能无法在两个蜂窝内不受干扰地运行。

漫游


Channel 1
Channel 1
AP1
AP2
A
B
C
AP1 Signal
AP2 Signal
A
B
C
Noise Due to
Channel Interference

漫游条件

漫游过程完全是由无线客户端设备驱动程序而不是AP驱动的，客户端可采取两种方法来确定何时进行漫游：

- 客户端可以在其需要漫游前主动搜索其他相邻AP
- 客户端可以在需要漫游时才搜索相邻 AP

无线客户端根据各种条件确定漫游的时机，802.11标准没有解决这个问题，因此使用的漫游算法随厂商而异，另外，漫游算法通常使用的是“秘密配方”，因此无法知道精确的阈值和条件。（在相同的情况下，有的厂商网卡的客户端会漫游，有的厂商的就不会漫游。）

漫游算法

在漫游算法中，使用的一些条件包括信号强度、信号质量、遗漏的信标数、由于冲突或干扰导致的错误等。选择这些条件通常是合乎逻辑的，因为他们说明了连接的整体的质量。

由于不同的客户端使用不同的阀值，因此在蜂窝内的同一个位置，有些客户端可能尝试进行漫游，而有些不这样做。有些客户端选择在几乎收不到当前AP的信号时才进行漫游，而有些客户端在有更佳的AP时就进行漫游。换句话说，我们不要过多的考虑控制漫游算法的因素，而只需熟悉漫游过程即可。

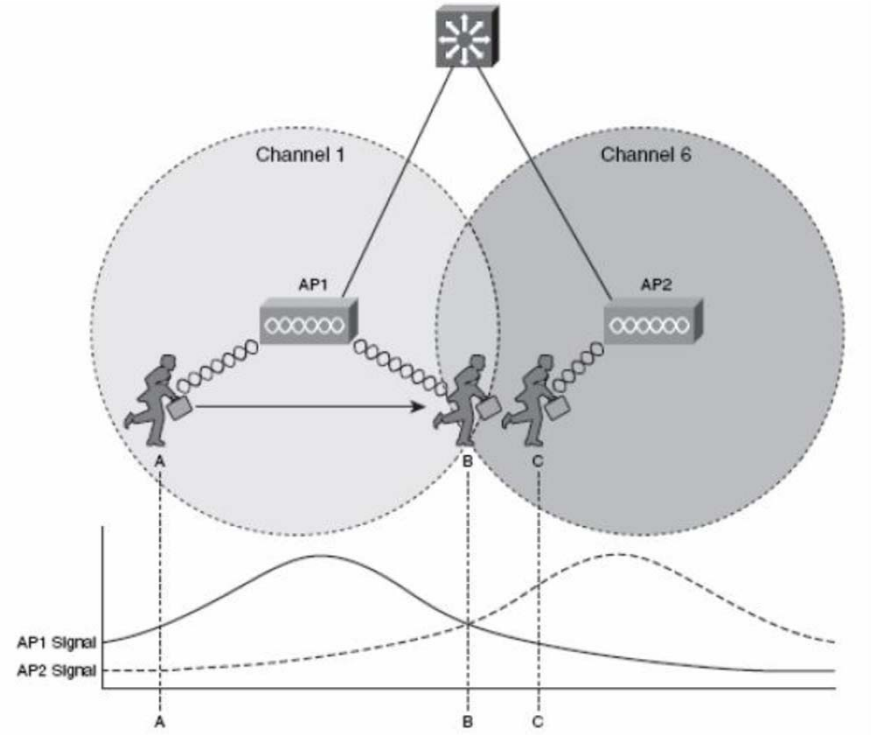
客户端扫描

客户端确定应该漫游后，它首先必须搜索潜在的新AP，这是通过扫描其他信道以找到其他活动AP实现的，客户端采取两种方法来执行扫描过程：

- 被动扫描：客户端花时间来扫描其他信道，但只侦听来自可用AP的802.11信标
- 主动扫描：客户端花时间来扫描其他信道，同时发送802.11探针请求帧来查询可用AP

客户端采用被动扫描时，只需等待接收信标即可，因此非常适合用于低功率的嵌入式无线客户端，主动扫描让客户端具有控制权，因为必须发送探针并等待接收探针应答，通常，主动扫描比被动扫描可实现更高效的漫游，因为可以根据需要查询和识别AP。

漫游过程



对两个AP进行了正确的配置，使其使用互不重叠的信道1和6，同时列出了两个AP的信号强度同客户端位置的关系图。在位置 A，客户端可以从AP1那里收到清晰的信号，因此它保持同该AP的关联。

漫游过程

当客户端向位置B移动时，它发现AP1的信号不再是最优的，在此过程的某个位置，客户端开始查找更佳的AP以便同其关联，无线客户端采取两个步骤来完成这个过程：

第1步：客户端发送802.11探针请求管理帧
第2步：侦听的AP使用802.11探针响应帧来应答客户，以通告自己的存在

客户端并不知道将遇到的下一个AP使用的信道，因此它必须通过每个可能的信道发送探针，所以它必须花时间来调整发射器，使其远离当前AP的信道，以便能够扫描其他信道并发送探针。

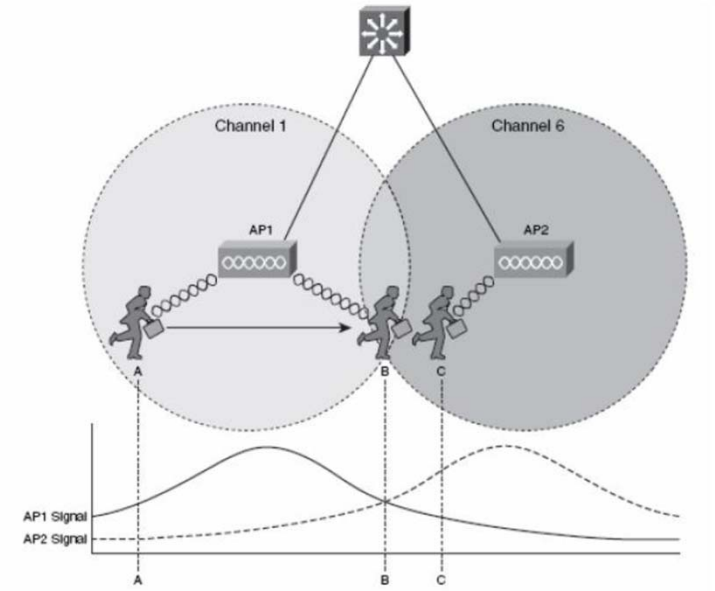
漫游过程

客户端移到位置B附近时，在各种信道中发送802.11探针请求帧。AP2在信道6中收到探针请求后，它通过在信道6中发送探针应答来进行响应，客户端收到探针应答后，对其进行评估，以确定同哪个AP关联是最合适的。

现在，在客户端必须进行漫游，客户端到达位置B后仍同AP1关联，虽然它可能能够从AP2接收到更佳的信号。

首先，必须删除现有的关联，因为每个客户端不能同时与多个AP关联，客户端通过信道1（AP1使用的信道）向AP1发送802.11解除关联消息，然后客户端便可以通过信道6向AP2发送关联请求，接下来AP2使用关联响应做出应答。

二层漫游



相邻AP连接到一个交换型网络，属于同一个VLAN，因此，AP之间的802.11漫游实际上发生在第2层，可以将其视为类似于这样：客户PC从连接到一台接入层交换机切换到连接到另一台接入层交换机，但位于同一个VLAN中，这意味着在漫游期间，客户端的IP地址保持不变，这提供了方便，因为客户端关联到另一个AP时，无需花时间来获得新的IP地址。

三层漫游漫游

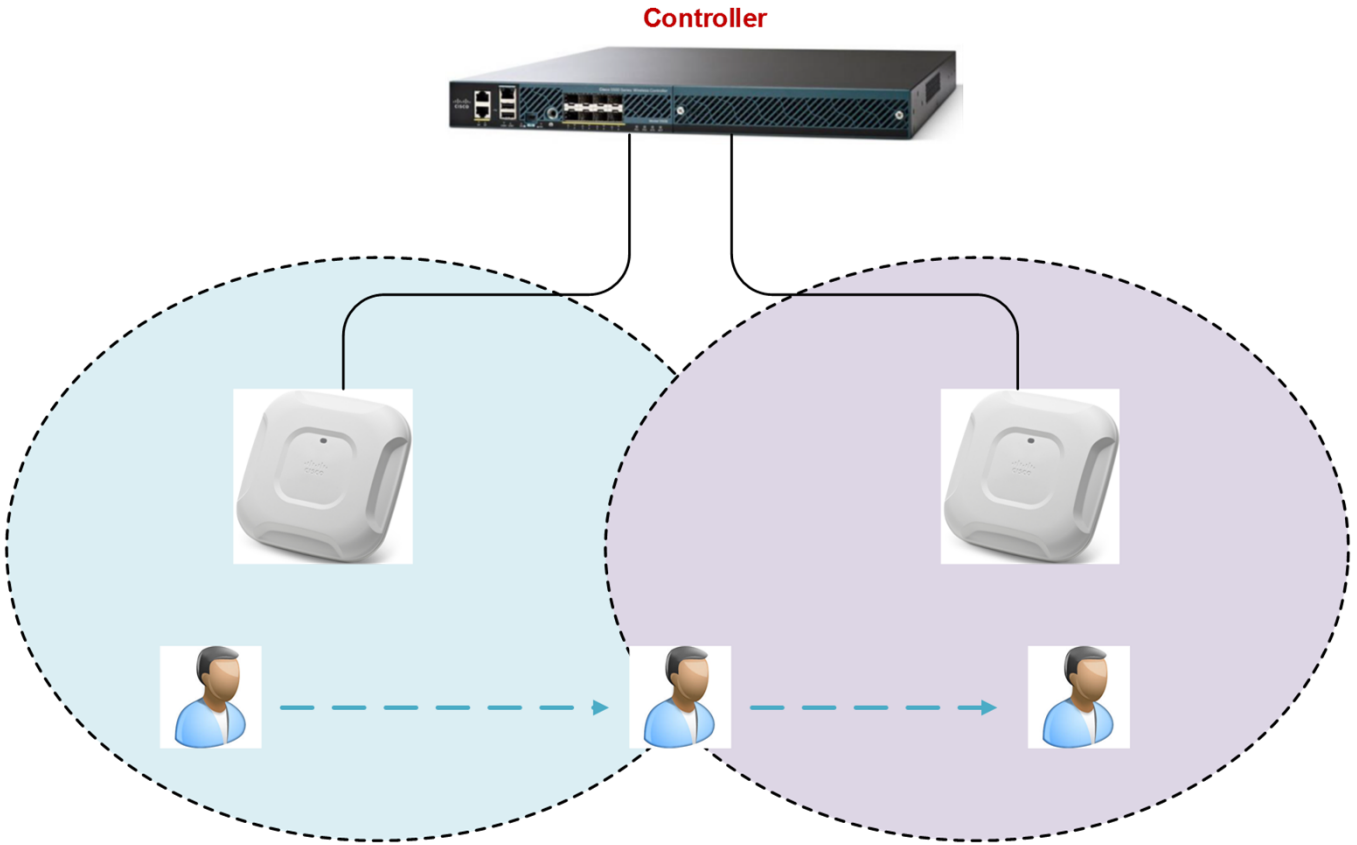
有时候，在WLAN的规模很大时，最好增加新的IP子网和VLAN。应将大型园区网划分成多个交换模块，以免出现跨越整个园区网的VLAN，对WLAN来说也如此，因为它实际上只是对交换型网络的扩展。

如果WLAN被划分成多个VLAN和子网，无线客户端漫游时可能跨越第3层边界，在这些边界上漫游时，客户端的IP地址可能发生变化，在这种情况下，漫游不仅需要发送802.11探针和关联请求，客户端还需要请求并获得新的IP地址，因此离线时间将更长。

Intra-Controller Roaming

Each controller supports **same-controller client roaming across access points managed by the same controller.**（漫游发生在一个控制器的几个**AP**之间。）
This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address. The controller provides DHCP functionality with a relay function. **Same-controller roaming is supported in single-controller deployments and in multiple-controller deployments.**
（在一个控制器部署和多个控制器部署的时候都支持）

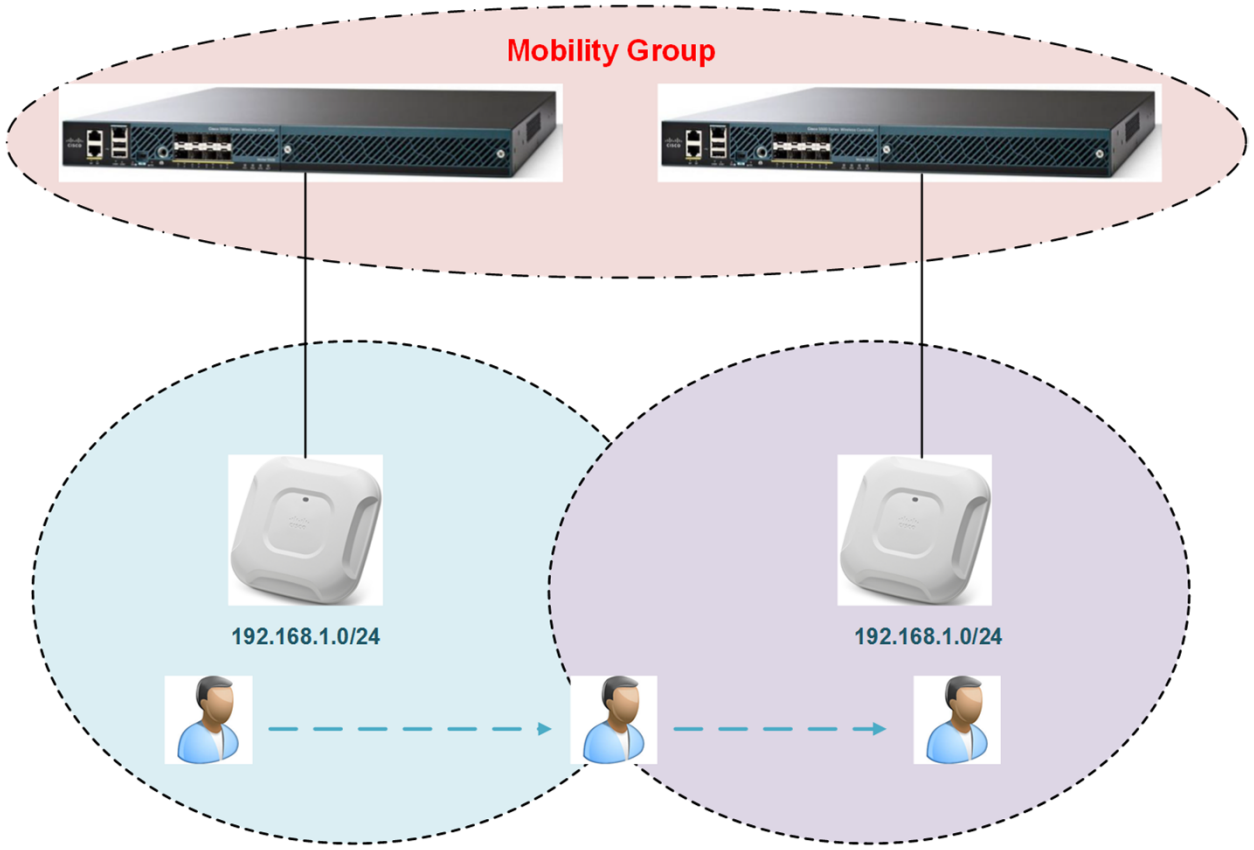
Intra-Controller Roaming



Inter-Controller Roaming

Multiple-controller **deployments support client roaming across access points managed by controllers in the same mobility group and on the same subnet.**（客户端漫游组中进行漫游，并且漫游在同一个网段。）This roaming is also transparent to the client because the **session is sustained and a tunnel between controllers** allows the client to continue using the same DHCP- or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate **when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set session timeout is exceeded.**（隧道会**down**，并且客户需要重新认证，当客户发送一个**DHCP Discover**，使用**0.0.0.0**的客户**ip**地址，或者一个**169.254.*.***的客户自动**IP**地址，或者设置的会话超时时间超过）

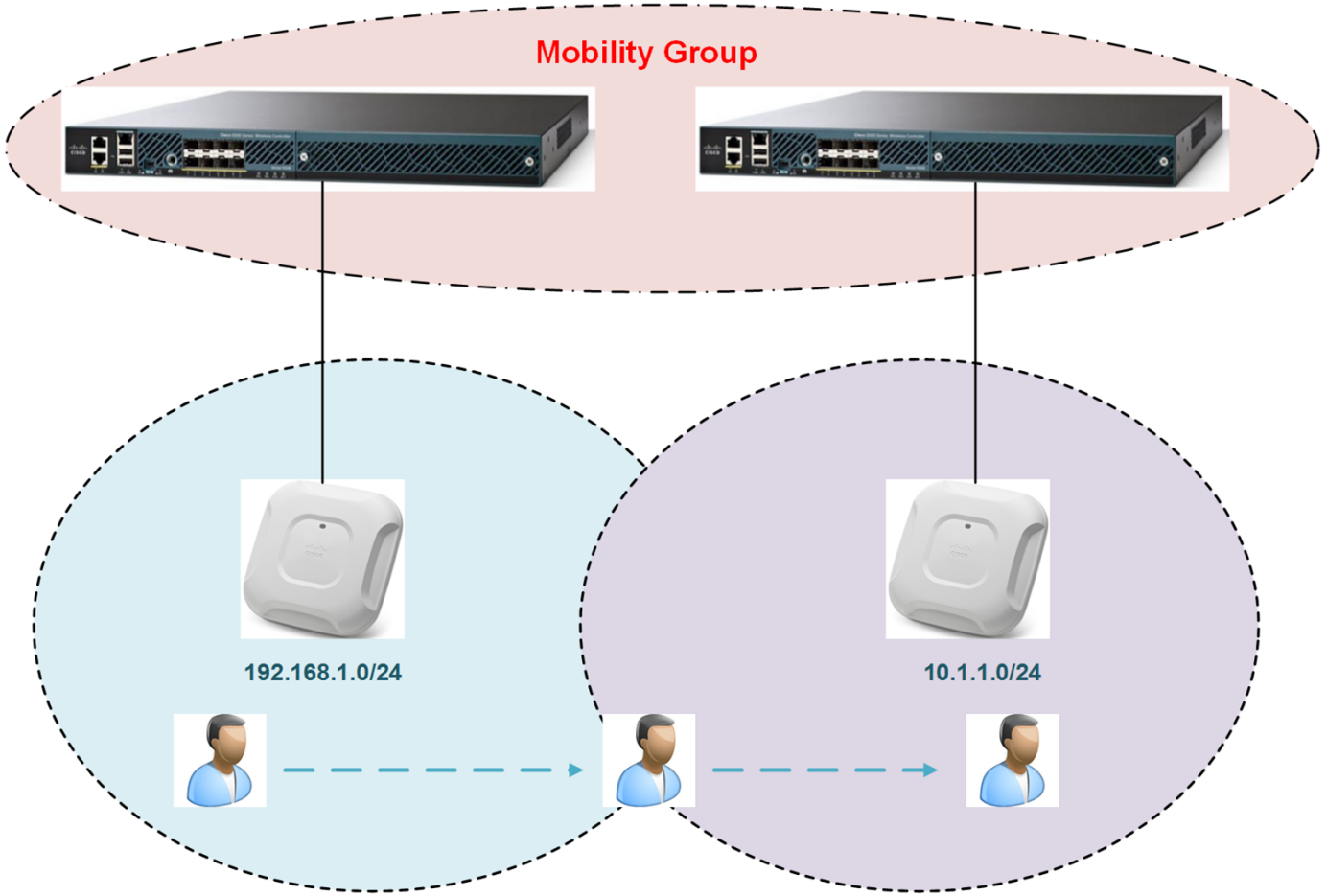
Inter-Controller Roaming



Inter-Subnet Roaming

Multiple-controller deployments support **client roaming across access points managed by controllers in the same mobility group on different subnets.**（客户端在漫游组中的不同网段间漫游。） This roaming is transparent to the client because the **session is sustained and a tunnel between the controllers** allows the client to continue using the same DHCP-assigned or client-assigned IP address as long **as the session remains active**.（当会话是**Active**状态的时候，客户端不需要重新更新地址。） The tunnel is torn down, and the client **must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set user timeout is exceeded.**

Inter-Subnet Roaming



CCX Layer2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements （**CCX的网卡才支持的**）

- Access point assisted roaming（**AP辅助漫游**）
- Enhanced neighbor list （增强的邻居列表）
- Enhanced neighbor list request (E2E) （增强的邻居列表请求）
- Roam reason report （漫游原因报告）
- Directed roam request （直接漫游请求）

CCX Layer2 Client Roaming

Access point assisted roaming—This feature helps clients save scanning time.（这个特性可以减少客户端的扫描时间） When a **CCXv2** client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point.（当CCXv2的客户端连接到新的AP上时，CCXv2客户端会把之前他连接AP的一些属性信息发送到新的AP上。） Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association.（漫游时间将会减少，当这个客户识别和使用一个AP清单，这个清单是客户端以前关联AP的信息，这个清单会在每一个客户关联的时候通过单播的方式发送给客户端） The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.（这个AP的清单会包含信道，BSSID和那些现在支持的SSID，还有AP从原来AP取消关联的时间。）**{便于返回以前的AP}**

CCX Layer2 Client Roaming

- **Enhanced neighbor list**—This feature focuses on improving a **CCXv4** client's roam experience and network edge performance, especially when servicing voice applications. **The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.**（**AP**会以单播的形式给客户端更新**AP**关联的客户端信息，和**AP**的邻居信息。）（需要**CCXv4**的支持）

- **Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience.(**是**cisco**和**intel**协同接口，定义一个新的协议和接口来提高语音和漫游体验**) It applies only to Intel clients in a CCX environment.**（只支持**CCX**的**intel**的网卡） **Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.**（当**intel**的客户端需要的时候，发送邻居清单请求，**AP**转发这个请求到控制器，控制器回应可以**CCX**漫游的邻居**AP**的子列表）

CCX Layer2 Client Roaming

- **Roam reason report—This feature enables CCXv4 clients to report the reason why they roamed to a new access point.（让CCXv4的客户端报告为什么他需要漫游到一个新的AP）**It also allows network administrators to build and monitor a roam history.

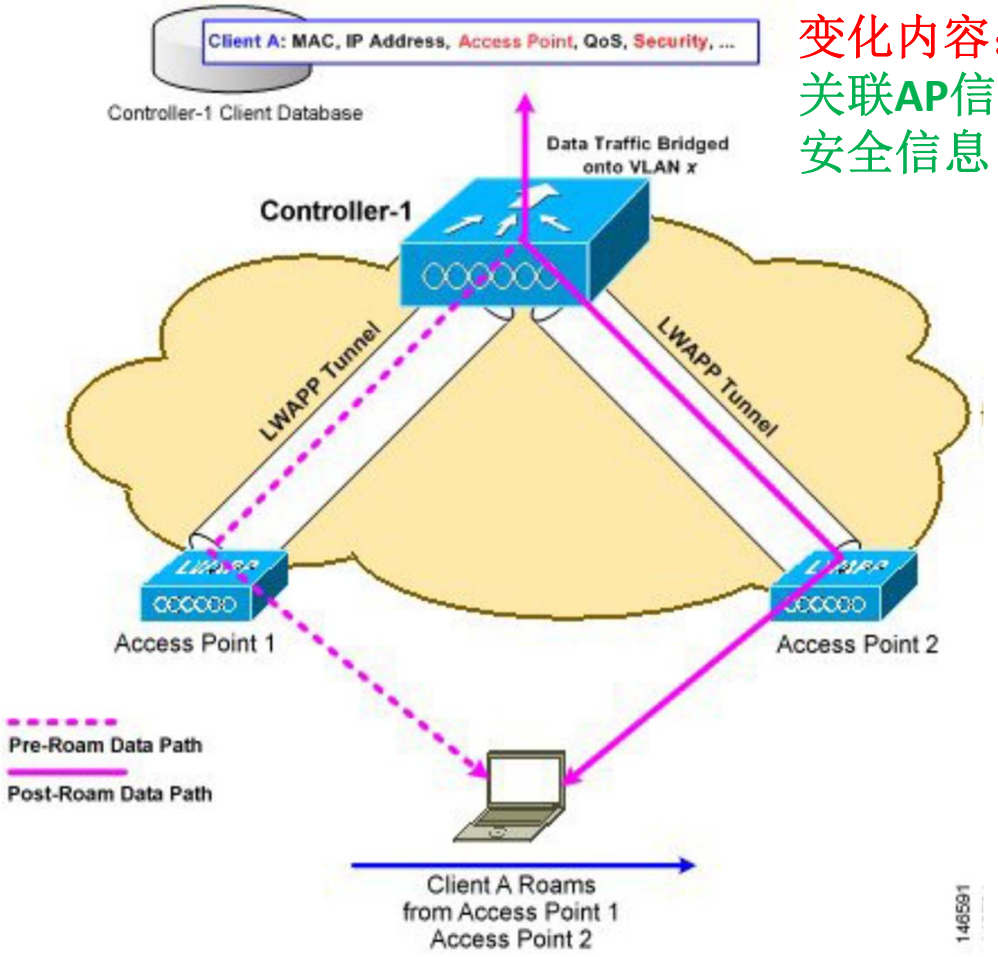
- **Directed roam request—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated.(这个特性让控制器可以直接让客户端漫游到更适合他的AP上去)** In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. **Non-CCX clients and clients running CCXv3 or below must not take any action.（低于CCXv3的不会采取行动）** No configuration is required for this feature.

Mobility

Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible.（移动，或者漫游，是无线网络客户端的一种能力，能够从一个**AP**安全的，低延时的漫游到另外一个**AP**上，并且保持关联状态）

When a wireless client associates and authenticates to an access point, the access point's controller places an entry for that client in its client database（关联后，控制器会为客户维护一个数据库条目）. **This entry includes the client's MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated access point.**（记录包含**MAC**地址，**ip**地址，安全的信息，**QOS**，和客户端关联的**AP**和**WLAN**）The controller uses this information to forward frames and manage traffic to and from the wireless client.

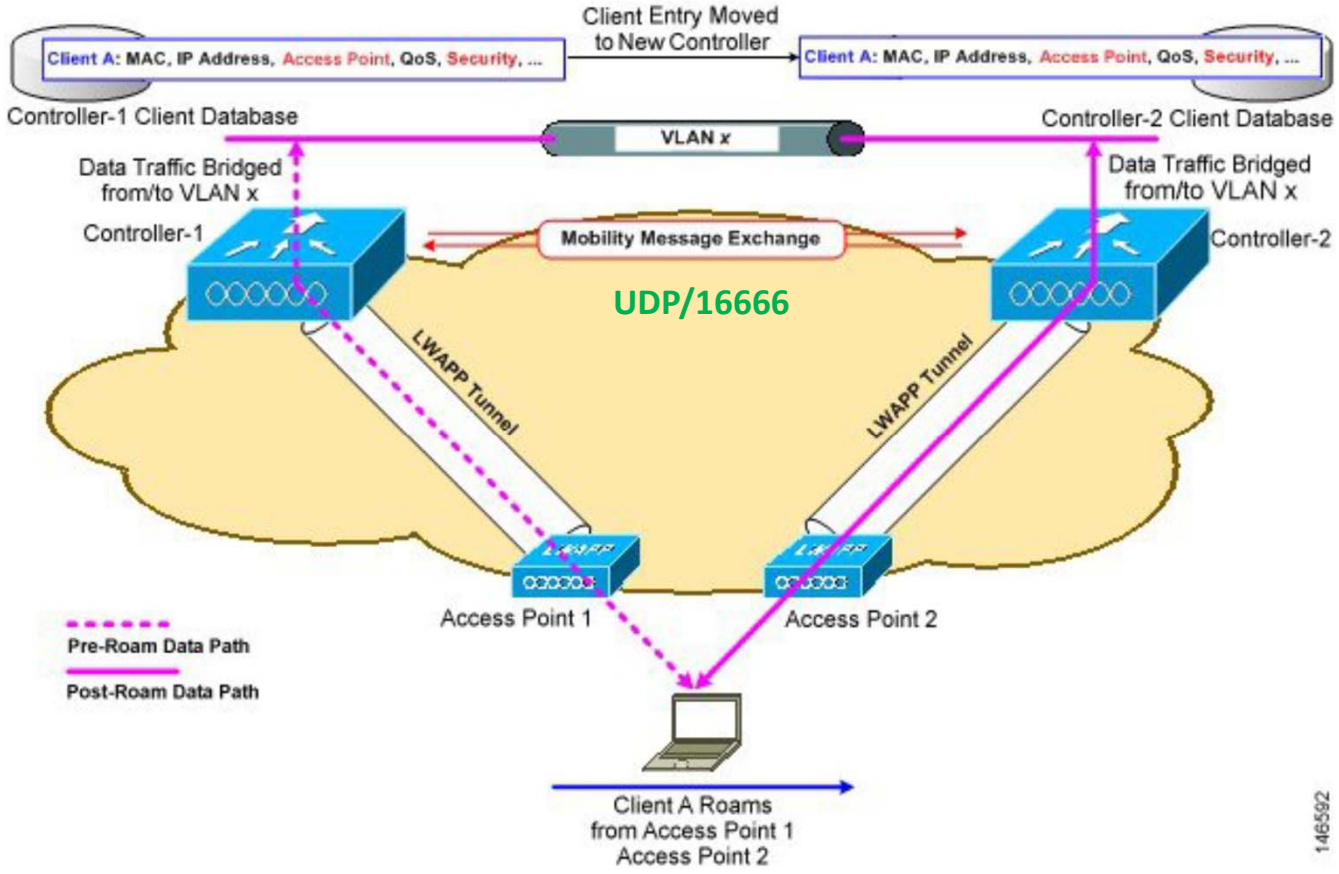
Intra-Controller Roaming



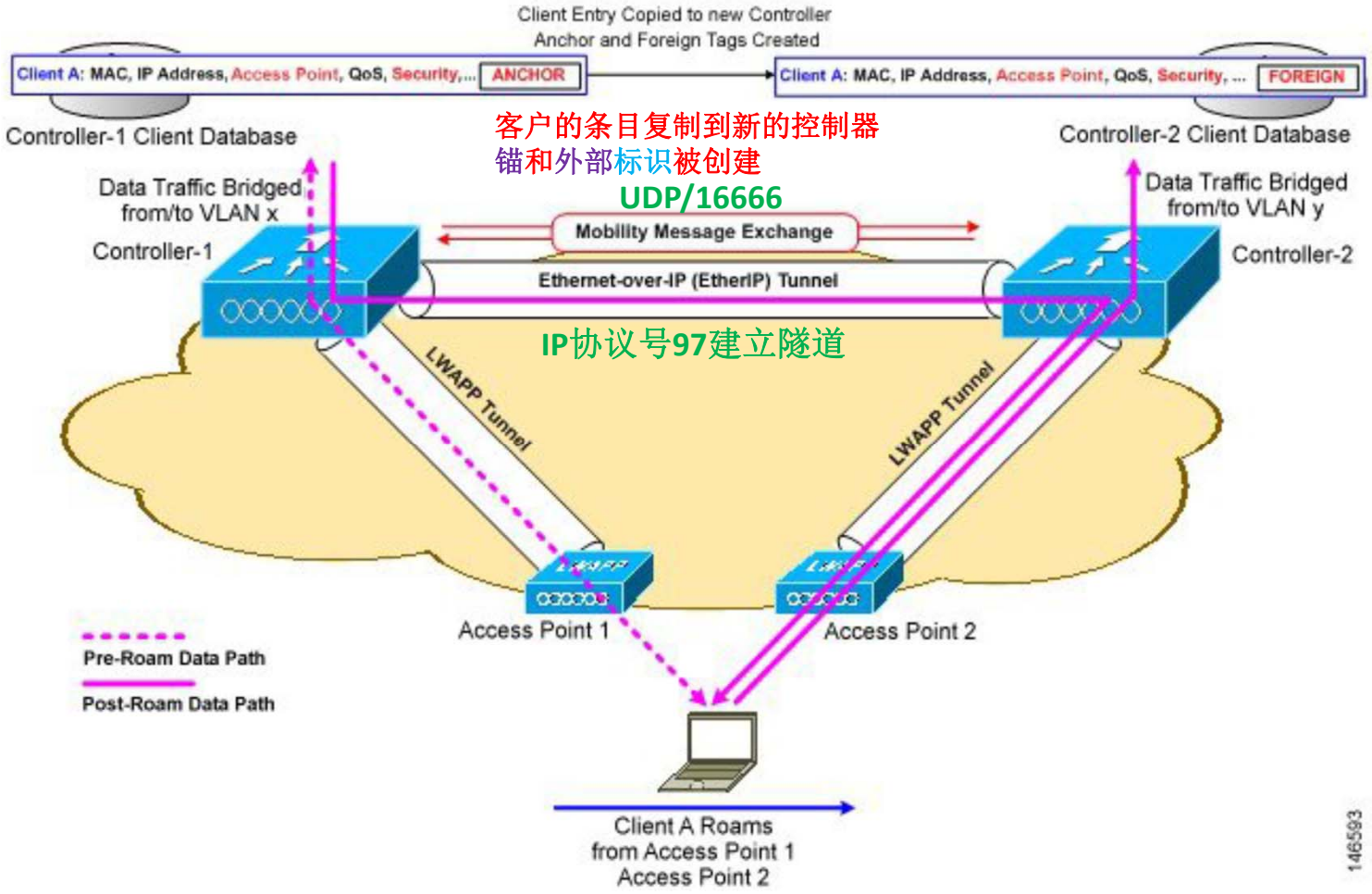
变化内容：
关联AP信息
安全信息（密钥有变化）

Inter-Controller Roaming

客户的条目移动到新的控制器



Inter-Subnet Roaming

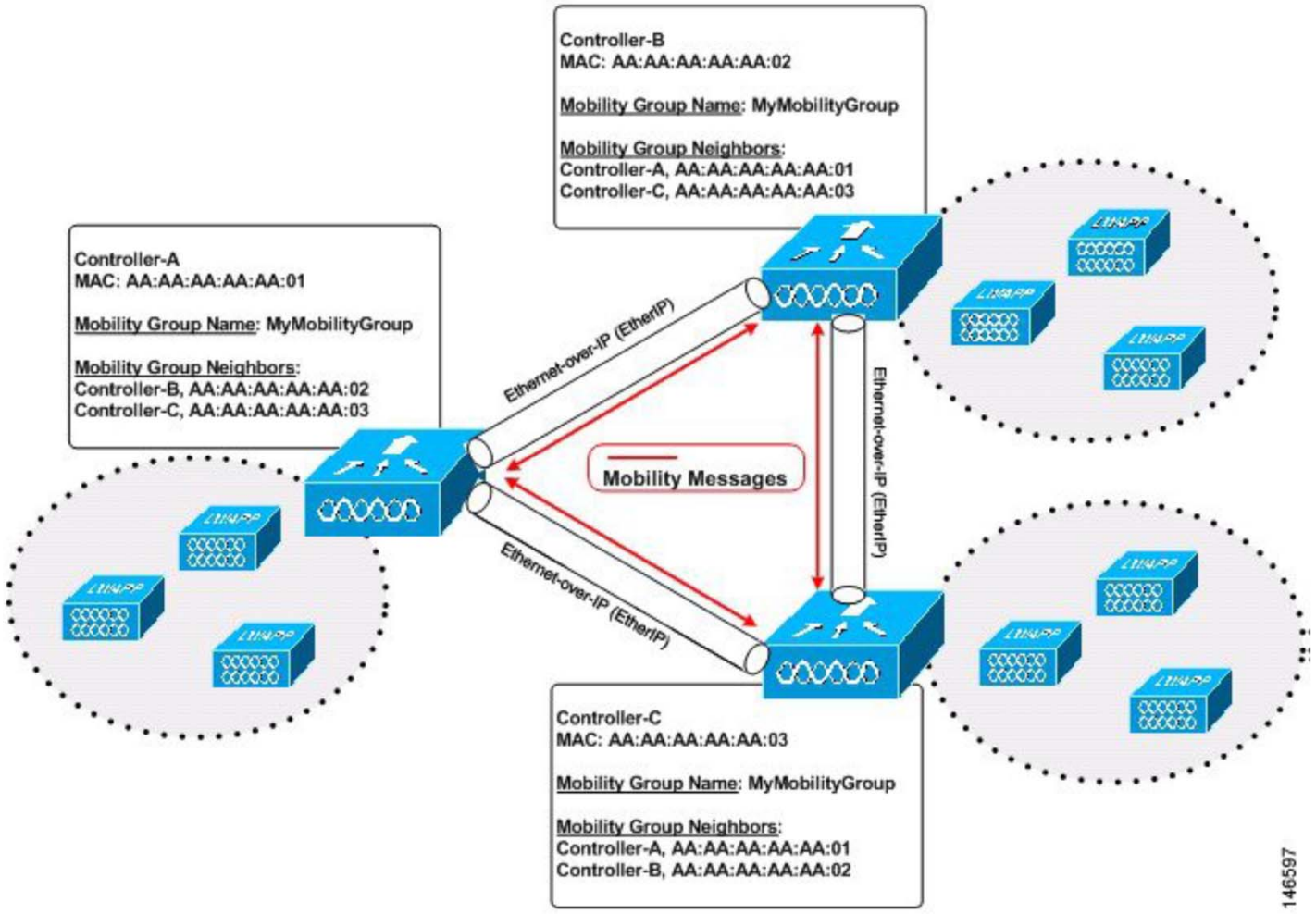


Mobility Group

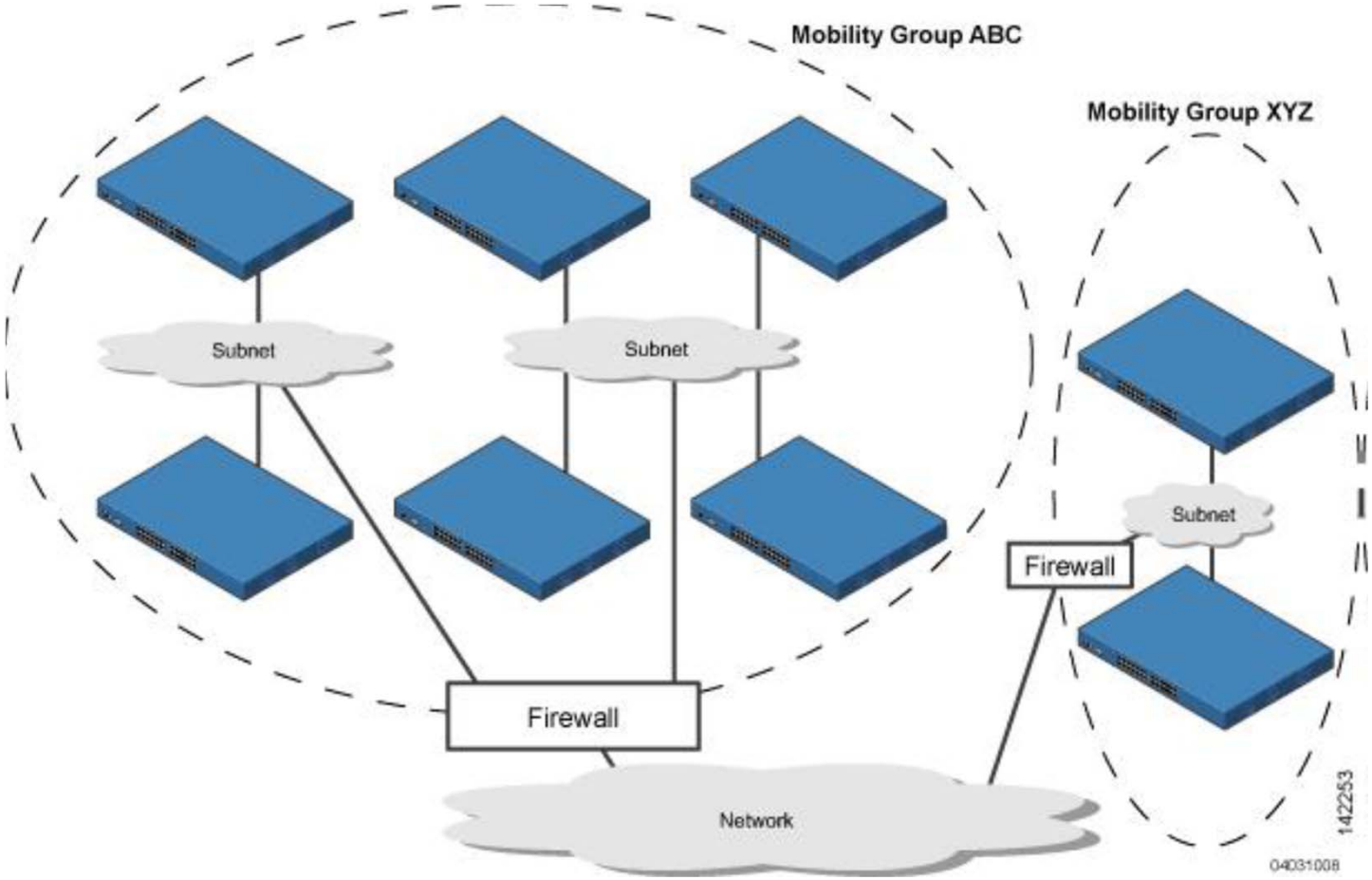
A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients.（一个移动组是由多个控制器设置相同的组名组成的，为无线客户端提供一个无缝漫游的区域）By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. **Controllers in the same mobility group can share the context and state of client devices as well as their list of access points**（一个漫游组中的控制器会共享他们保存的客户信息和**AP**清单） so that they do not consider each other's access points as rogue devices. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

Controllers do not have to be of the same model to be a member of a mobility group. Mobility groups can be comprised of any combination of controller platforms.(Mobility Group的成员可以是不同型号和平台的控制器。**)**

Mobility Group信息交换



Mobility Group信息交换

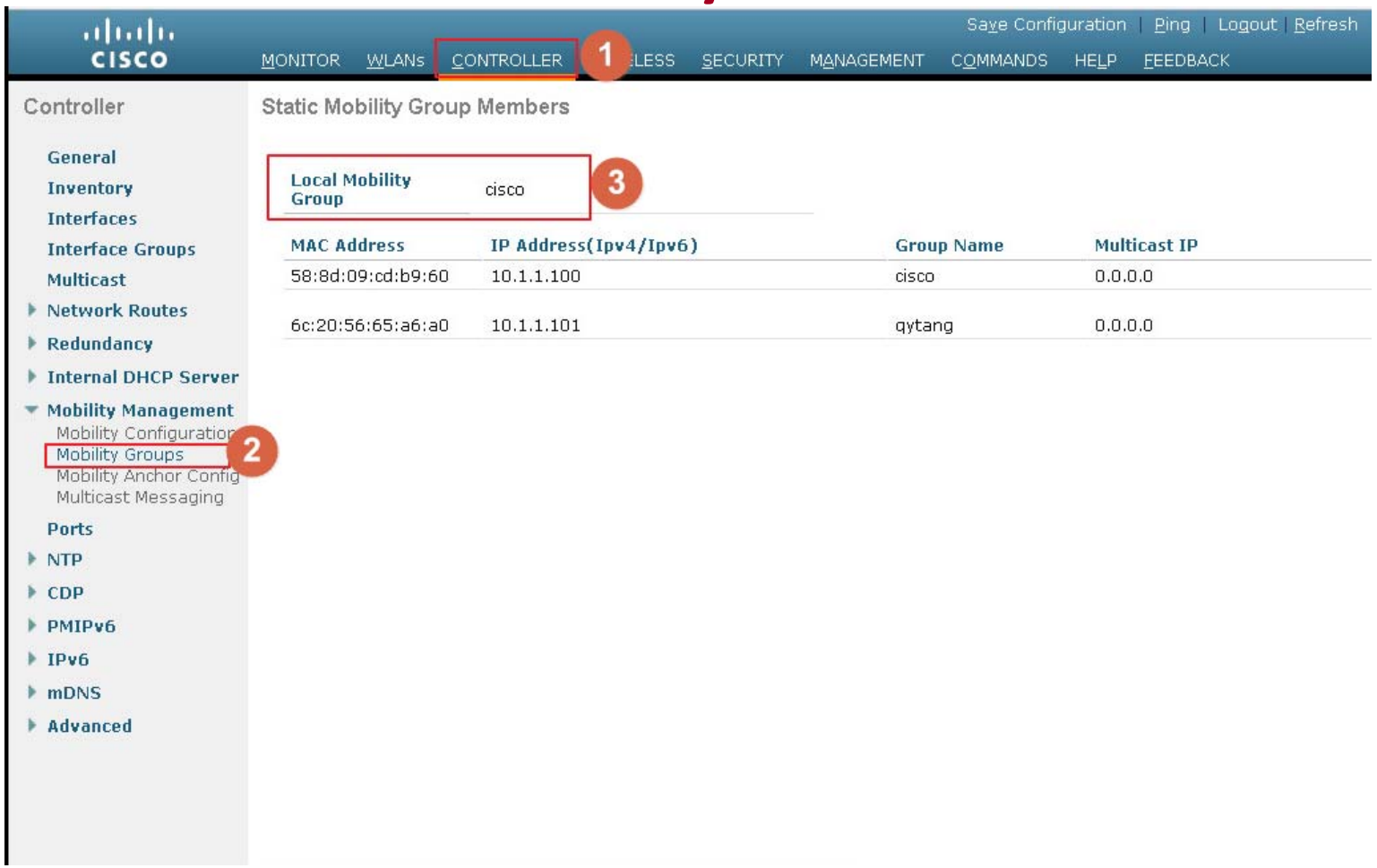


Mobility List

Every controller maintains information about its peer controllers in a mobility list. **（每个控制器会维护他的邻居漫游列表中的信息。）** **Controllers can communicate across mobility groups and clients may roam between access points in different mobility groups if the controllers are included in each other's mobility lists.** （不同移动组中的控制器可以直接通信，客户也可以在不同漫游组之间进行漫游，前提是这个控制器在其他控制器的漫游清单中）In the following example, controller 1 can communicate with either controller 2 or 3, but controller 2 and controller 3 can communicate only with controller 1 and not with each other. Similarly, clients can roam between controller 1 and controller 2 or between controller 1 and controller 3 but not between controller 2 and controller 3.

Controller 1 Mobility group: A	Controller 2 Mobility group: A	Controller 3 Mobility group: C
Mobility list:	Mobility list:	Mobility list:
Controller 1 (group A)	Controller 1 (group A)	Controller 1 (group A)
Controller 2 (group A)	Controller 2 (group A)	Controller 3 (group C)
Controller 3 (group C) ?		

Mobility List



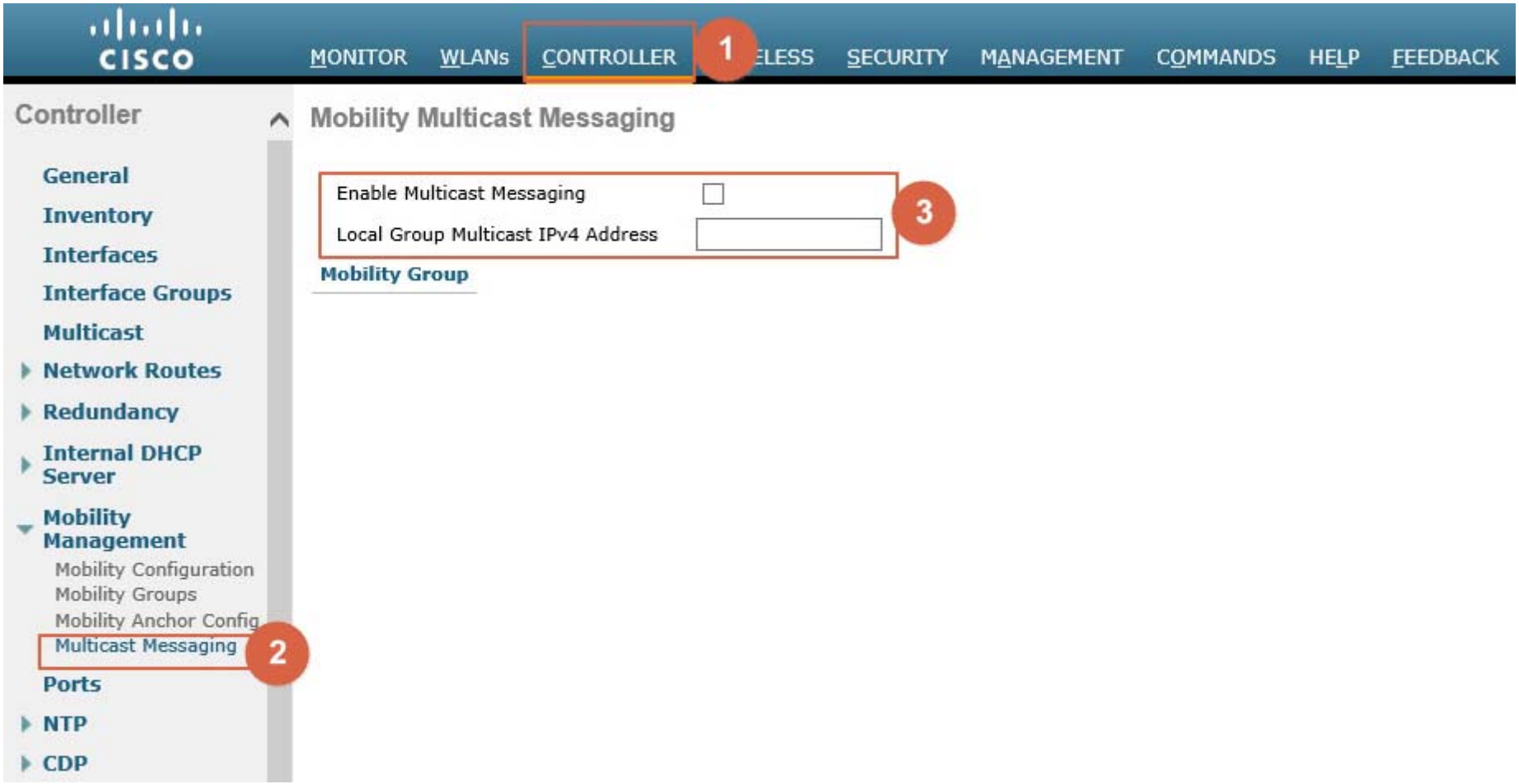
Message Among Mobility Groups

The controller **provides inter-subnet mobility** for clients by sending mobility messages to other member controllers.（不同子网中的漫游是需要发送信息的）

- **The controller sends a Mobile Announce message to members in the mobility list each time that a new client associates to it.**（当有客户端关联的时候，控制器会发送移动通知信息到所有的**mobility**列表中的控制器） The controller sends the message only to those members that are in the same group as the controller (the local group) and then includes all of the other members while sending retries.（上一页的图，先发**group**内，再发**list**）

- You can configure the controller to use **multicast** to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group that contains all the mobility members. **To derive the maximum benefit from multicast messaging, we recommend that it be enabled on all group members.**（推荐用组播地址来更新）

组播配置


CISCO
MONITOR
WLANs
CONTROLLER
1
ELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Mobility Configuration
Mobility Groups
Mobility Anchor Config
Multicast Messaging
2
Ports
NTP
CDP
Mobility Multicast Messaging
Enable Multicast Messaging
Local Group Multicast IPv4 Address
3
Mobility Group

Mobility Group Guildline

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- IP connectivity must exist between the management interfaces of all controllers.（所有的 控制器要**IP**可达）
- When controllers in the mobility list use **different software versions, Layer 2 or Layer 3 clients have limited roaming support. (**如果控制器版本不一样，漫游功能将被限制**)**Layer 2 or Layer 3 client roaming is supported only between controllers that use the same version.
- All controllers must be configured with the **same virtual interface IP address**（要有相同的虚拟地址）.
- **You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group.**（你需要把**ip**地址和**mac**地址在漫游组的每个控制器上都保存一份。）This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.
- When you configure mobility groups using a third-party firewall, for example, Cisco PIX, or Cisco ASA, **you must open port 16666, and IP protocol 97.**（需要放行**16666**端口和**97**号协议号 ）
- For inter-controller CAPWAP data and control traffic, **you must open the ports 5247 and 5246**.

Auto-Anchor Mobility

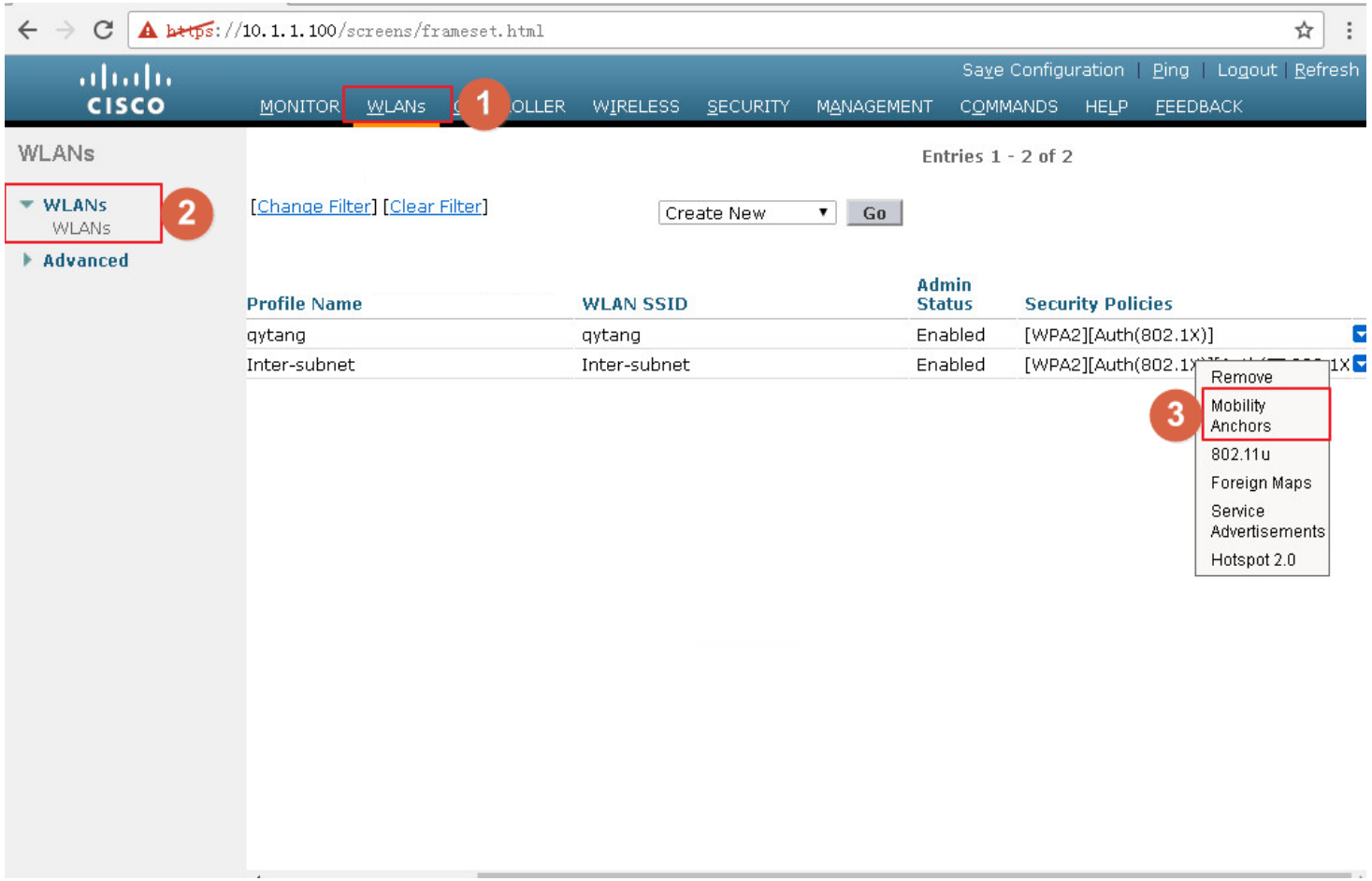
You can use auto-anchor mobility (also called guest tunneling) to improve load balancing and security for roaming clients on your wireless LANs. **Under normal roaming conditions, client devices join a wireless LAN and are anchored to the first controller that they contact.**（在一般情况下，客户端会认为第一个控制器是**anchor**） **If a client roams to a different subnet, the controller to which the client roamed sets up a foreign session for the client with the anchor controller**（当客户端漫游到不同的网段，流量会回送到**anchor**控制器转发）. **However, when you use the auto-anchor mobility feature, you can specify a controller or set of controllers as the anchor points for clients on a wireless LAN.**（当你启用**auto-anchor**的时候，你为特定**WLAN**指派一个或者一系列特定的控制器为锚）

In auto-anchor mobility mode, a subset of a mobility group is specified as the anchor controllers for a WLAN. **You can use this feature to restrict a WLAN to a single subnet, regardless of a client's entry point into the network**. Clients can then access a guest WLAN throughout an enterprise but still be restricted to a specific subnet. Auto-anchor mobility can also **provide geographic load balancing** because the WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on), effectively creating a set of home controllers for a WLAN. **Instead of being anchored to the first controller that they happen to contact, mobile clients can be anchored to controllers that control access points in a particular vicinity.(**客户端可以被**anchor**到在他附近的控制器上，而不是第一个连接的控制器。**)**

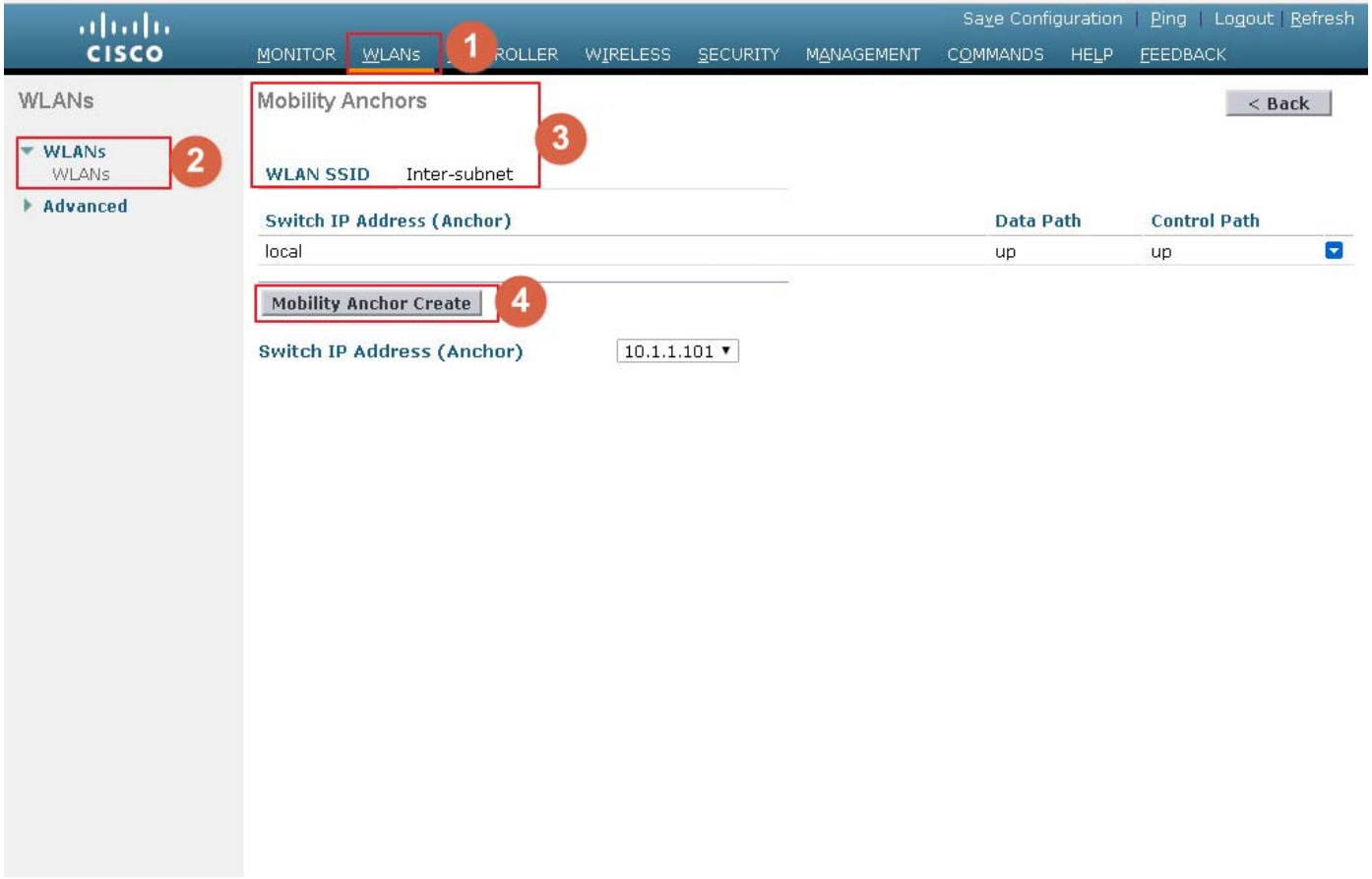
Multiple Anchor

If multiple controllers are added as mobility anchors for a particular WLAN on a foreign controller, the foreign controller internally sorts the controller by their IP address. (如果你在一个WLAN添加了多个anchor，那么他会基于IP地址来循环) The controller with **the lowest IP address is the first anchor（地址最小的是最先的Anchor）**. For example, a typical ordered list would be 172.16.7.25, 172.16.7.28, 192.168.5.15. If the first client associates to the foreign controller's anchored WLAN, the client database entry is sent to the first anchor controller in the list, the second client is sent to the second controller in the list, and so on, until the end of the anchor list is reached. The process is repeated starting with the first anchor controller. **If any of the anchor controller is detected to be down, all the clients anchored to the controller are deauthenticated, and the clients then go through the authentication/anchoring process again in a round-robin manner with the remaining controller in the anchor list.（如果列表中的一个anchor控制器被删除，连接到这个anchor的客户端会被取消关联，再进行认证，并且在现有的锚列表中循环选择一个） This functionality is also extended to regular mobility clients through mobility failover. This feature enables mobility group members to detect failed members and reroute clients.（这个特性也可以理解为高可用性，让漫游组的成员检测失败的客户端并且重新路由这些客户端）**

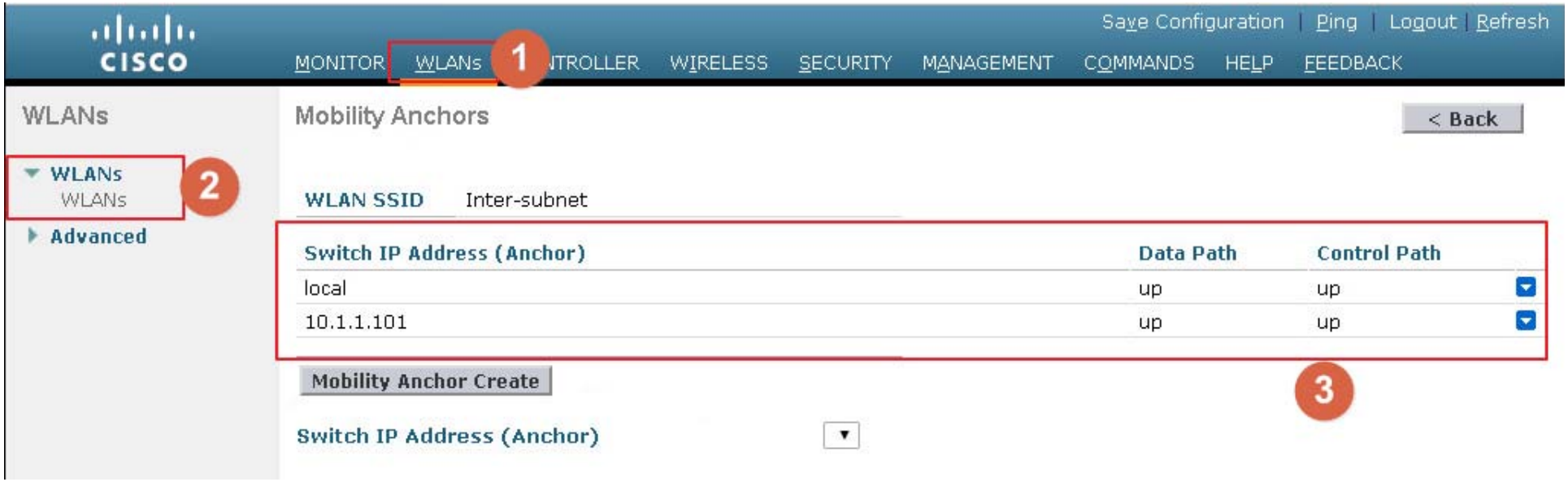
Multiple Anchor



Multiple Anchor



Multiple Anchor



Auto-Anchor的限制

- **You must add controllers to the mobility group member list** before you can designate them as mobility anchors for a WLAN.
- **You can configure multiple controllers as mobility anchors for a WLAN.（你可以配置多个控制器作为一个WLAN的锚）**
- **Auto-anchor mobility supports web authentication but does not support other Layer 3 security types.（auto-anchor在三层只支持webauth）**
- **You must configure the WLANs on both the foreign controller and the anchor controller with mobility anchors.（anchor信息需要在本地控制器和远程控制器上都配置）** On the anchor controller, configure the anchor controller itself as a mobility anchor. On the foreign controller, configure the anchor as a mobility anchor.
- Auto-anchor mobility is **not supported for use with DHCP option 82(auto-anchor不支持option82)**. **For Layer 3 RADIUS authentication, the RADIUS requests for authentication are sent by the anchor controller.（像radius发送请求的是anchor控制器）**
- **The mobility anchor is not supported on virtual wireless LAN controllers.（vWLC不支持anchor）**

Dynamic-Anchor for static address

At times you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they could try associating with other controllers. **If the clients try to associate with a controller that does not support the same subnet as the static IP, the clients fail to connect to the network. You can now enable dynamic tunneling of clients with static IP addresses.**

Dynamic anchoring of static IP clients with static IP addresses can be associated with other controllers where the client's subnet is supported by tunneling the traffic to another controller in the same mobility group. (在动态anchor的时候，静态的IP地址可以被tunnel到能转发这个流量的anchor控制器上去)This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses.（这个特性可以让一个WLAN同时为静态IP地址进行服务。）

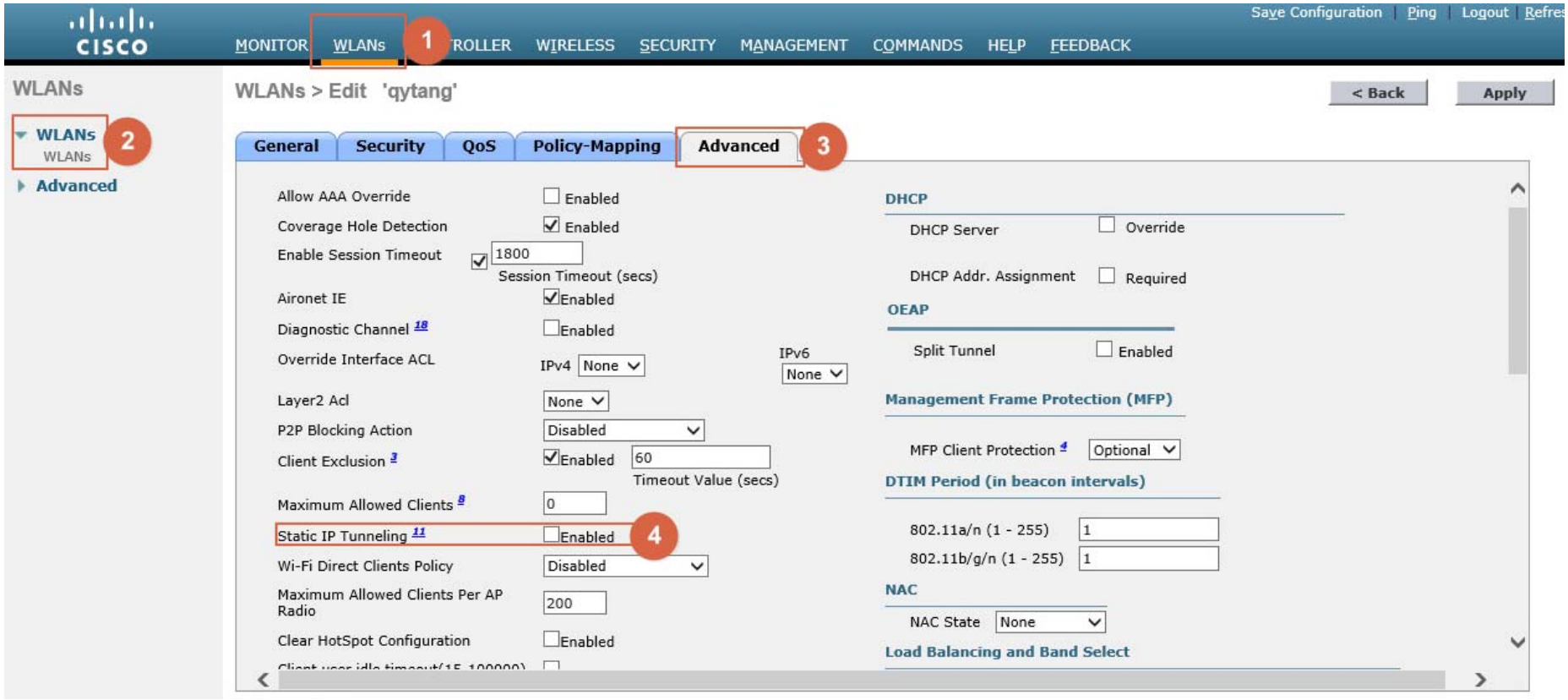
Dynamic-Anchor工作方式

1. When a client associates with a controller, for example, WLC-1, it performs a mobility announcement. **If a controller in the mobility group responds (for example WLC-2), the client traffic is tunneled to the controller WLC-2.** **（当有控制器回应的时候，客户端的流量会被tunnel到这个anchor控制器）** **As a result, the controller WLC 1 becomes the foreign controller and WLC-2 becomes the anchor controller.** **（这个时候，WLC1是外部控制器而WLC2变成anchor的控制器）**

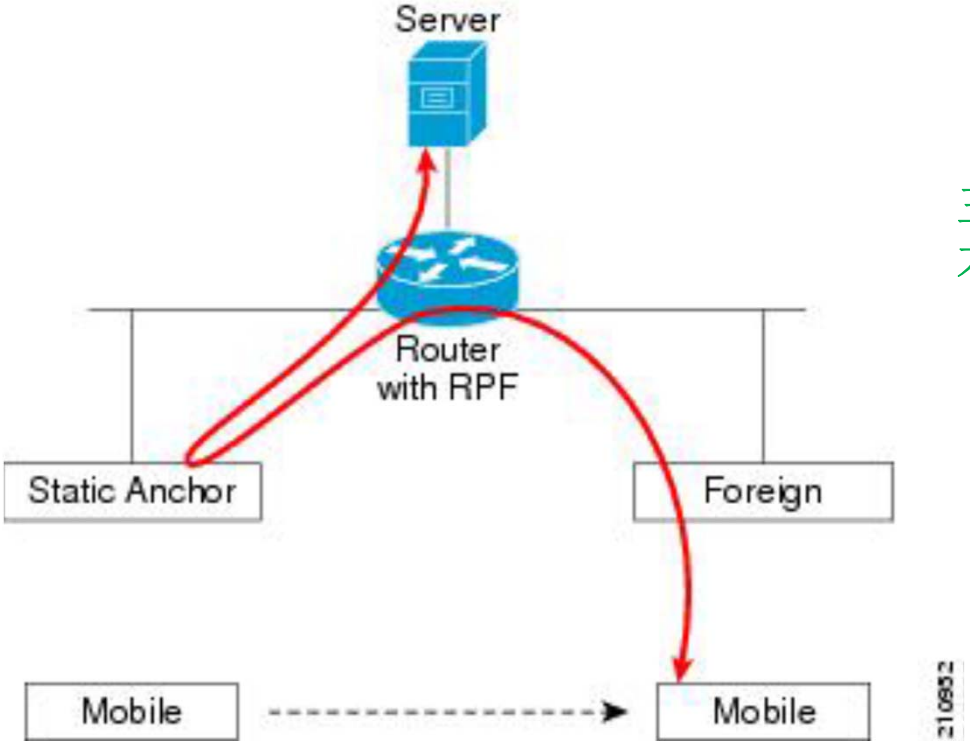
2. **If none of the controllers responds, the client is treated as a local client and authentication is performed.** **（如果没有人回应这个包，控制器就自己处理这个客户端。）** The IP address for the client is updated either through an orphan packet handling or an ARP request processing. **If the IP subnet of the client is not supported in the controller (WLC-1), WLC-1 sends another static IP mobile announce and if a controller (for example WLC-3) that supports the client's subnet responds to that announcement, the client traffic is tunneled to that controller** **（如果WLC1不支持这个客户端的IP网段，就会再发送另一个宣告，如果WLC3给了回应，就回把数据tunnel到WLC3上去）**, that is WLC-3. As a result, the controller WLC 1 becomes the export foreign controller and WLC-3 becomes the export anchor controller.

3. Once the acknowledgment is received, the client traffic is tunneled between the anchor and the controller (WLC-1).

Dynamic-Anchor配置



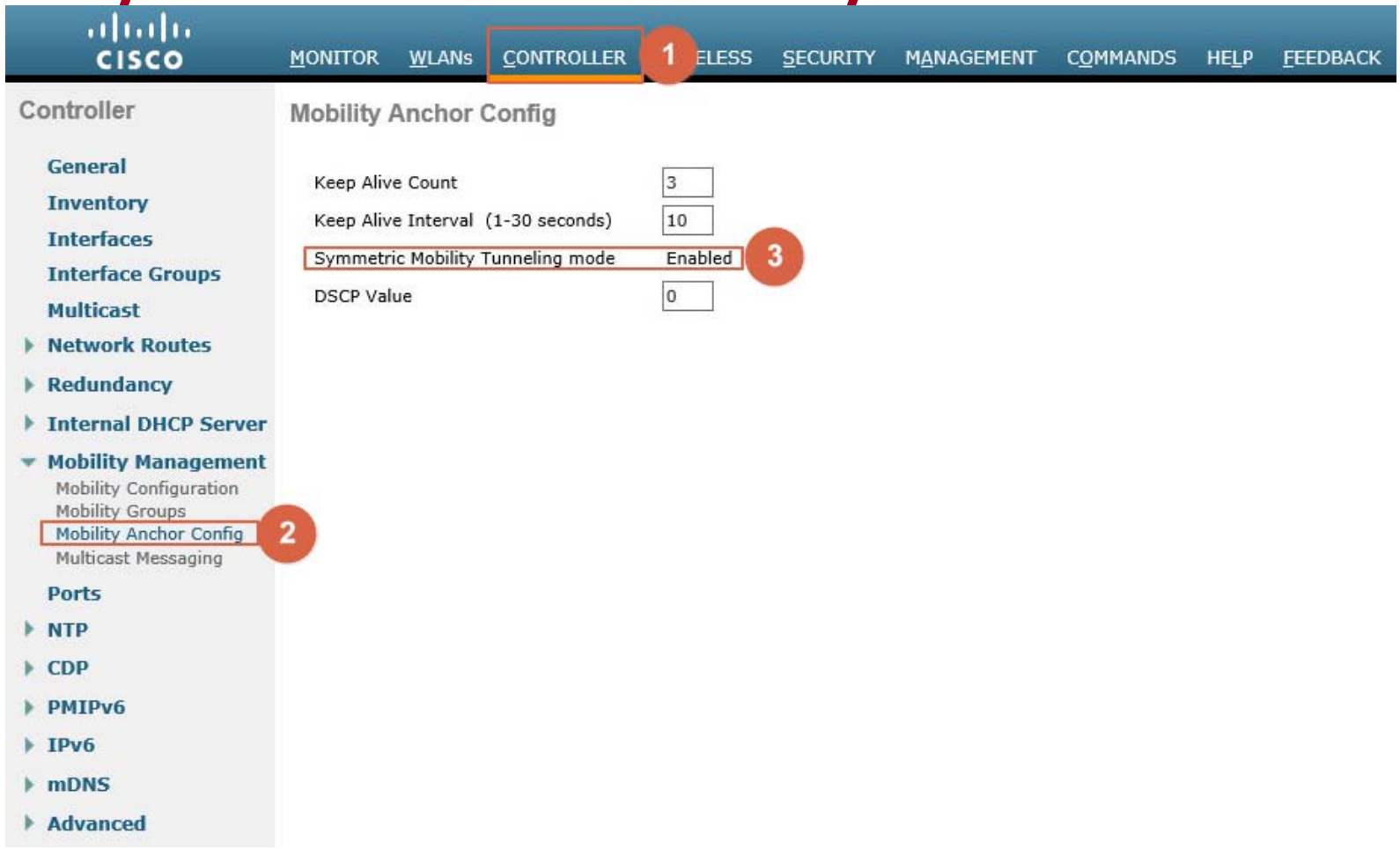
Symmetric Mobility Tunnel



三层漫游
才有必要

When symmetric mobility tunneling is enabled, all client traffic is sent to the anchor controller and can then successfully pass the RPF check. (默认情况下是开启的。)

Symmetric Mobility Tunnel配置



Mobility Ping Test

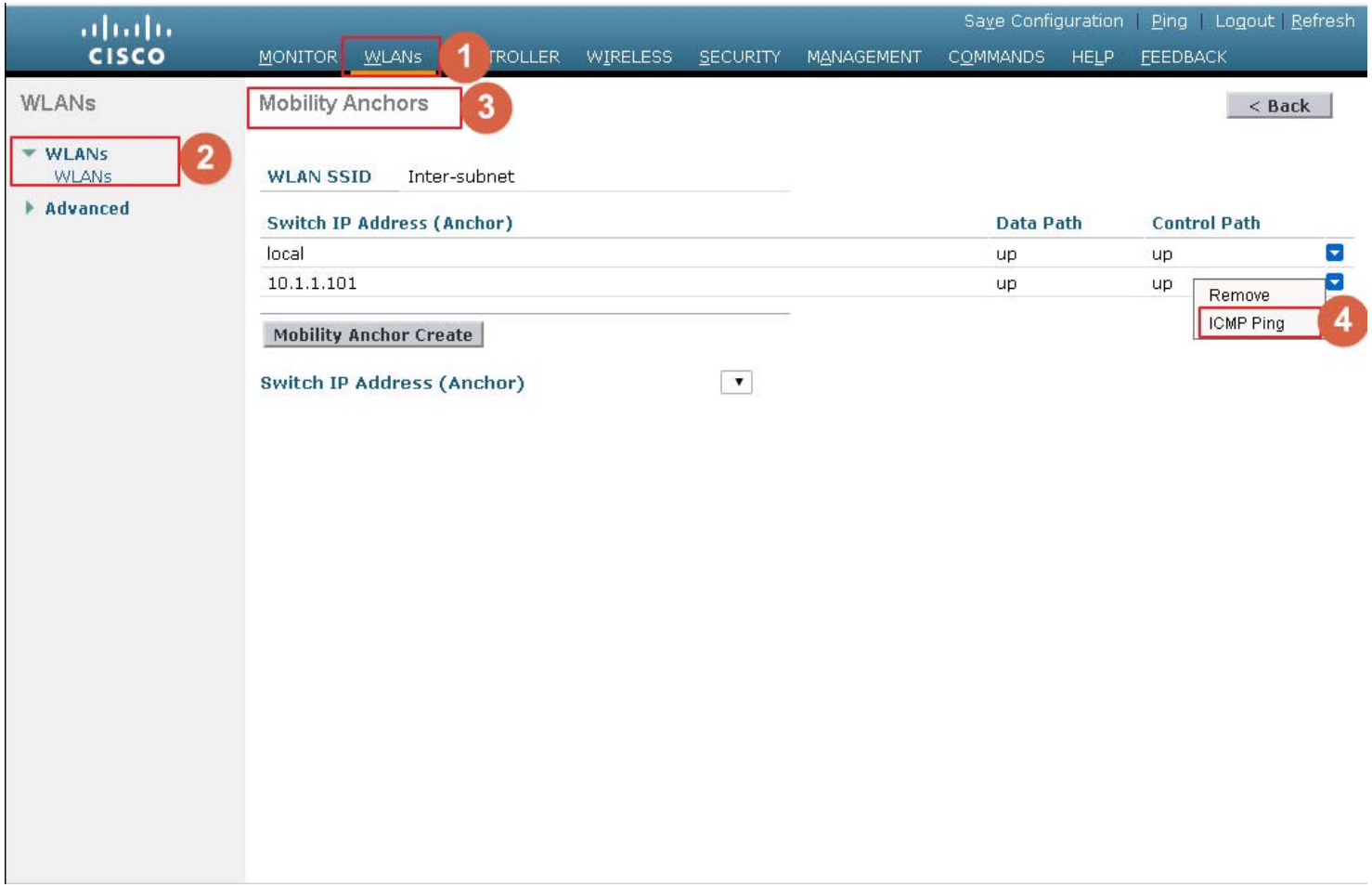
Controllers in a mobility list communicate with each other by controlling information over a well-known UDP port and exchanging data traffic through an Ethernet-over-IP (EoIP) tunnel. **Because UDP and EoIP are not reliable transport mechanisms, there is no guarantee that a mobility control packet or data packet will be delivered to a mobility peer.**（由于UDP和EoIP都是无连接的协议，所以不能确保控制报文和数据报文能够成功的传输 到对端）Mobility packets may be lost in transit due to a firewall filtering the UDP port or EoIP packets or due to routing issues.

Controller enable you to test the mobility communication environment by performing mobility ping tests.（控制器允许来用ping来测试漫游设备的通信环境） These tests may be used to validate connectivity between members of a mobility group (including guest controllers). Two ping tests are available:

- **Mobility ping over UDP**—This test runs over mobility **UDP port 16666**. **It tests whether the mobility control packet can be reached over the management interface.**（测试控制报文能够正常到达对端的管理接口）

- **Mobility ping over EoIP**—This test runs over EoIP. **It tests the mobility data traffic over the management interface.**（测试数据流量能够正常的到达对端的管理接口）

Mobility Ping Test

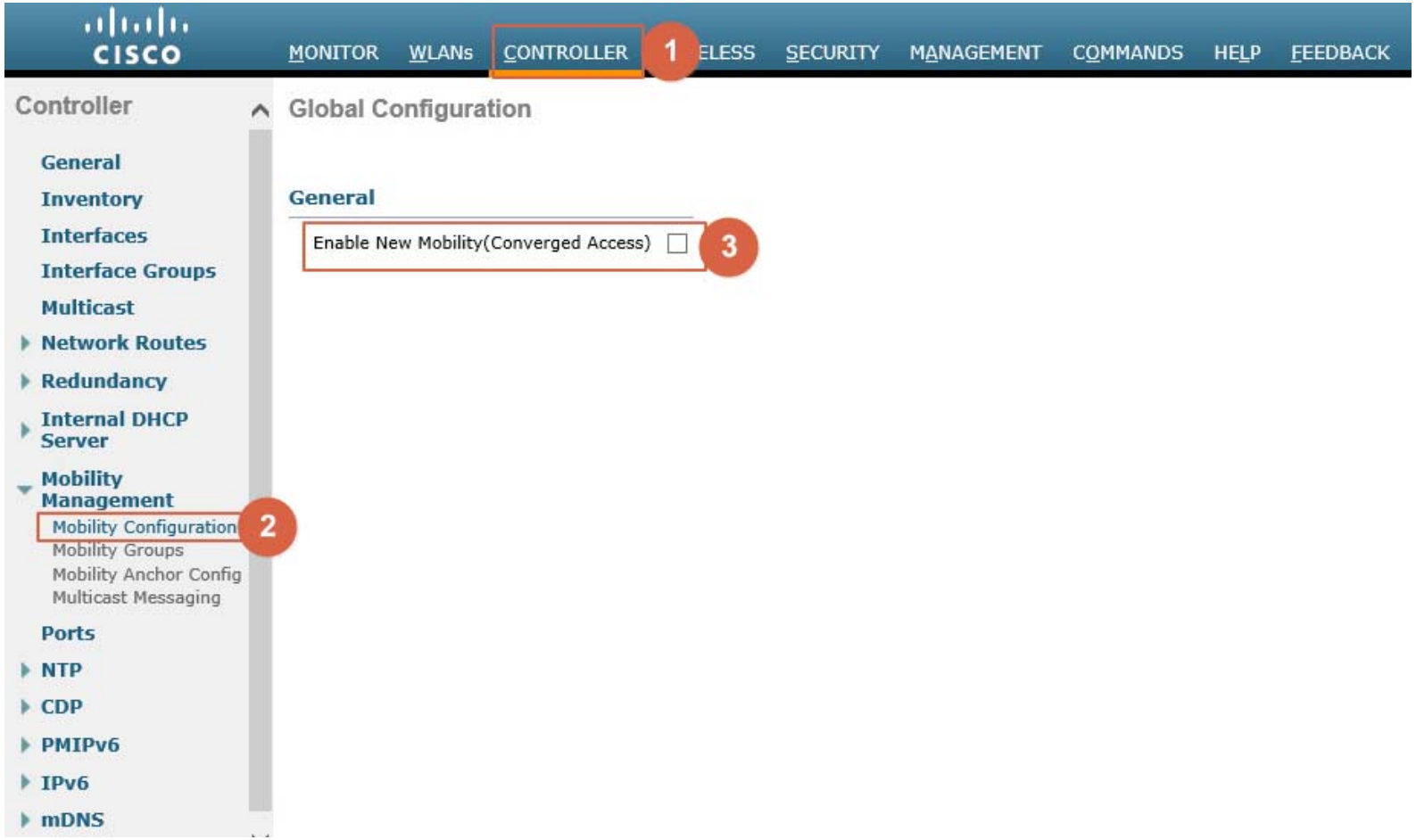


New Mobility Group

New Mobility enables Cisco WLCs to be compatible with converged access controllers with Wireless Control Module (WCM)（新的漫游组是为了兼容**IOS-XE**系统的控制器） such as the Cisco Catalyst 3850 Series Switches and the Cisco 5760 Series Wireless LAN Controllers. **New Mobility provides the ability to run Mobility Controller (MC) functionality on a Cisco WLC in the Converged Access mode with a Catalyst 3850 mobility agent (MA)**（新的漫游组让**WLC**作为**MC**,而**IOS-XE**的系统作为**MA**）

By default, New Mobility is disabled. When you enable or disable new mobility, you must save the configuration and reboot the controller.（这个功能默认是关闭的，需要使用的话需要保存配置并且重启。）

New Mobility Group配置



快速漫游的由来

Handoffs are already supported under the preexisting standard. The fundamental architecture for handoffs is identical for 802.11 with and without 802.11r: **the mobile device is entirely in charge of deciding when to handoff and to which access point it wishes to handoff.**（漫游设备会决定什么时候去交互，和哪个他期望的**AP**交互）In the early days of 802.11, handoff was a much simpler task for the mobile device. **Only four messages were required for the device to establish a connection with a new access point** (five if you count the optional "I'm leaving" message (Deauthentication / Disassociation packet) the client could send to the old access point). **However, as additional features were added to the standard, including 802.11i with 802.1x authentication and 802.11e or WMM with admission control requests, the number of messages required went up dramatically.**（由于新的功能被加入到**802.11**的标准中，客户端域**AP**交互的数据戏剧性的增长）During the time these additional messages are being exchanged, the mobile device's traffic, including that from voice calls, cannot proceed, and the loss experienced by the user could amount to several seconds. **Generally, the highest amount of delay or loss that the edge network should introduce into a voice call is 50 ms.**

802.11r was launched to attempt to undo the added burden that security and quality of service added to the handoff process, and restore it to the original four-message exchange.（**802.11r**是用来不让客户端在漫游的时候多做多余的交付过程，恢复原始的**4**个包交互）

CCKM

Cisco Centralized Key Management (CCKM) is the first fast secure roaming method developed by Cisco for enterprise WLANs, **as the solution to mitigate roaming delays when 802.1X/EAP security is enabled on a WLAN.**（在启用**802.1X**安全的**WLAN**上减少漫游的延迟） As this is a **Cisco proprietary protocol**（思科私有协议）**, it is only supported by Cisco and third-party clients that are Cisco Compatible Extension (CCX) compatible.**（只支持思科和第三方支持**CCX**的设备）

CCKM can be implemented with all of the different encryption methods available for WLANs including WEP, TKIP, and AES（**CCKM**支持所有的**WLAN**上的加密方式）**. It is also supports multiple EAP methods (dependent upon the CCX version supported by the client devices).**（基于**CCX**的版本，你可以支持多重的**EAP**的方式）

(CCKM的功能是CCXv4支持。)

CCKM 工作原理

With CCKM, the initial association to the WLAN is similar to WPA/WPA2,（开启了CCKM，初始化的关联和WPA的方式是一样的） where an MSK (also known here as the Network Session Key) is mutually derived from a successful authentication with a RADIUS server. **This master key is sent from the server to the WLC after a successful authentication, and is cached as the basis for derivation of all subsequent keys for the lifetime of the client session**（当认证成功之后，主key从服务器发送到WLC，衍生出所有后续key来完成客户端的整个会话）. The WLC and client derive the seed information that is used for fast secure roaming based on CCKM, performing a 4-way handshake (similar to WPA/WPA2), in order to derive the unicast (PTK) and multicast/broadcast (GTK) encryption keys.

When a CCKM client roams to a new AP, it sends a single Reassociation Request frame to the CAPWAP AP (including an MIC and a sequentially incrementing Random Number), and provides enough information (including the new BSSID MAC address) in order to derive the new PTK.（当CCKM的客户端漫游到新的客户端的时候，他只需要发送一个重新关联的请求包含MIC和随机数，并且提供新的AP的BSSID的MAC地址来生成一个PTK）**With this Reassociation Request, the WLC and new AP also have enough information in order to derive the new PTK, so they simply respond with a Reassociation Response, avoiding both the EAP authentication and 4-way handshake.**（WLC和新的AP有足够的信息来生成新的PTK，所以就会回复重新关联请求，避免产生新的EAP而只需要4此握手就可以。）

CCKM Summary

- Is supported by Cisco and third-party clients that **are CCX compatible.（CCXv4）**
- **Supports different encryption and EAP methods** (depending on CCX version).
- Fast roaming is performed by avoiding the 802.1X/EAP authentications and 4-way handshakes.
- Supported for both **Centralized and FlexConnect** deployments (locally or centrally switched)**(支持本地和中心转发)**
  - Centralized – Works across APs and WLCs in the same Mobility group
  - FlexConnect – Works across APs in the same FlexConnect group
- FlexConnect WLANs can be configured for local or centralized authentication using central or local switching.
- FlexConnect APs are supported in connected or standalone modes – **however there are restrictions as to how the MSK is shared in standalone mode.(虽然在standalone模式下MSK的共享是有些限制)**

802.11r

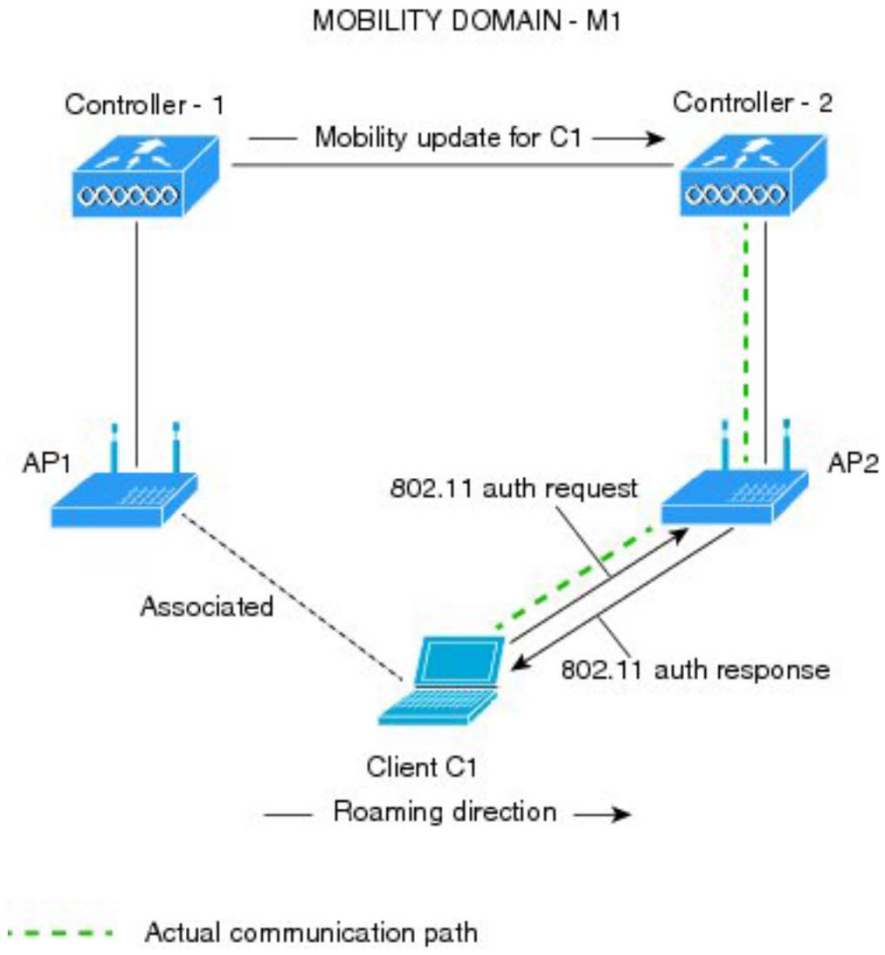
802.11r, which is the IEEE standard for fast roaming,（802.11r是公有的） introduces a new concept of **roaming where the initial handshake with the new AP is done even before the client roams to the target AP**（在客户端没有漫游到目标AP的时候，初始化的握手已经完成）, which is called Fast Transition (FT). **The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance.**（初始化握手允许客户端在没有关联到AP之前协商好PTK） **These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.**（在客户端和新的AP重新关联的时候就直接应用PTK）

802.11r provides two methods of roaming:

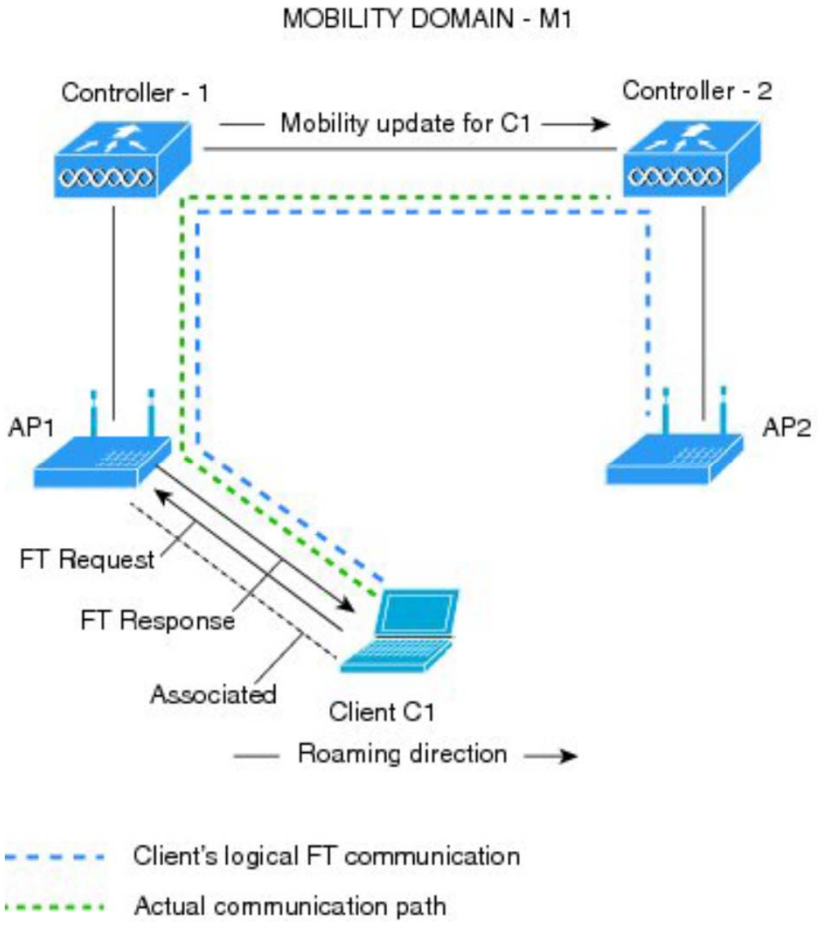
- **Over-the-Air**
- **Over-the-DS (Distribution System)**

The FT key hierarchy is designed to **allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP.**（允许客户端在BSS内的AP进行快速漫游不需要在每个AP重新认证） **WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).**（FT是一个新的认证KEY管理类型）

Over-the-air


MOBILITY DOMAIN - M1
Controller - 1
Mobility update for C1
Controller - 2
AP1
802.11 auth request
AP2
Associated
802.11 auth response
Client C1
Roaming direction
Actual communication path
351714

Over-the-DS


MOBILITY DOMAIN - M1
Controller - 1
Mobility update for C1
Controller - 2
AP1
AP2
FT Request
FT Response
Associated
Client C1
Roaming direction
Client's logical FT communication
Actual communication path

802.11r summary

1. Only supported on WPA2 WLANs using **PSK or 802.1X key management**.

2. Fast roaming is performed by avoiding 802.1X/EAP authentications and 4-way handshakes during a roam.

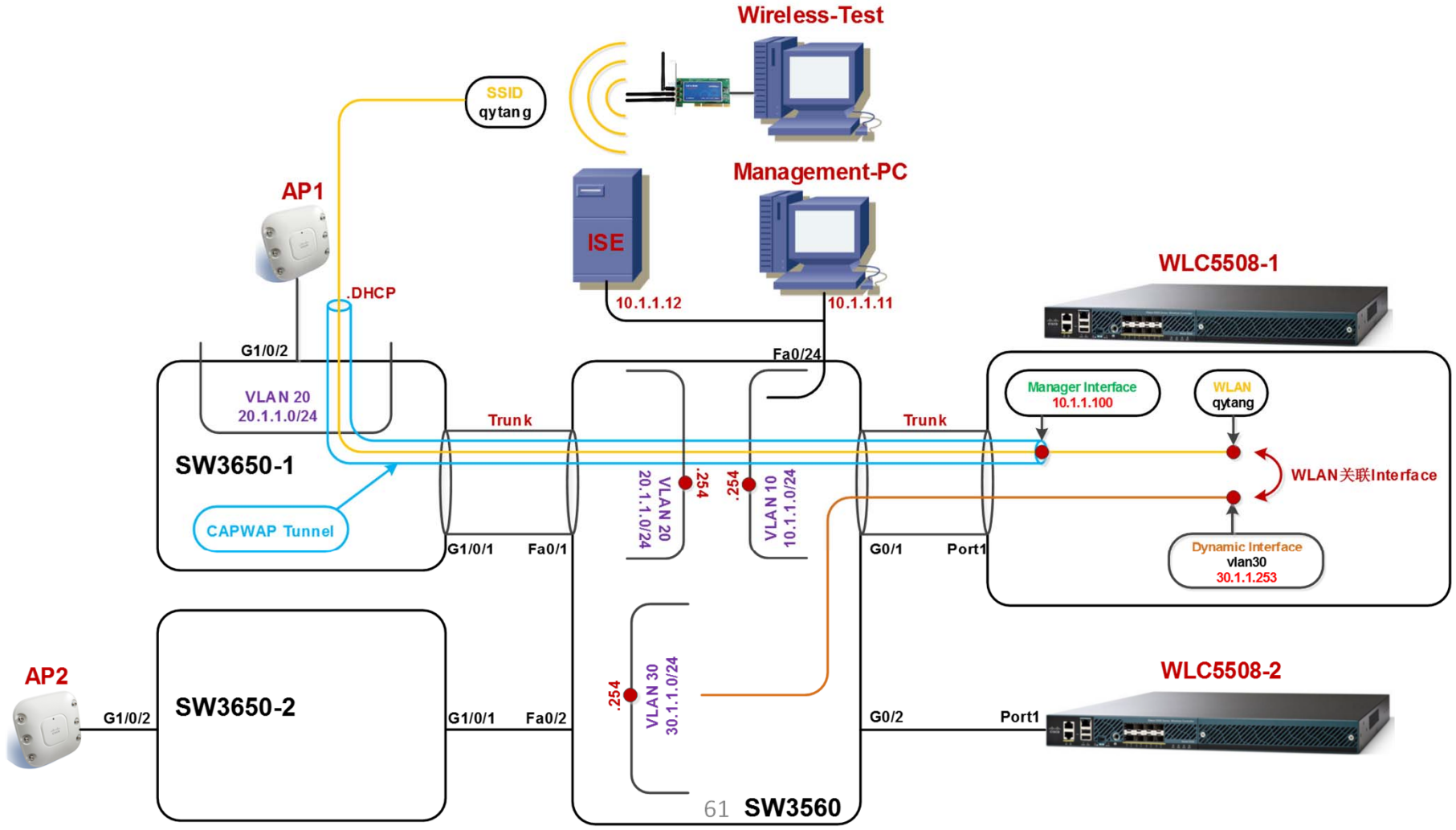
3. Supported for both **Centralized and FlexConnect** (centralized or locally switched) deployments:
   - Centralized – Works across WLCs in the same Mobility group.
   - FlexConnect – Works across APs in the same FlexConnect group.

4. FlexConnect requires WLANs to be configured for centralized authentication, **local authentication is not supported. (本地认证是不支持的)**Fast secure roaming is **not supported on FlexConnect APs operating in standalone mode.（standalone也是不支持的）**

第二部分
Intra-Controller Roaming

现任明教教主
融合网络CCNA

实验拓扑



SW3560配置

```
hostname SW3560
!
ip routing
!
vlan 10
 name management
vlan 20
 name ap_network
vlan 30
 name client
!
interface range FastEthernet0/1 - 2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
!
interface range GigabitEthernet0/1 -2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
!
interface FastEthernet0/24
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface Vlan10
 ip address 10.1.1.254 255.255.255.0
!
interface Vlan20
 ip address 20.1.1.254 255.255.255.0
!
interface Vlan30
 ip address 30.1.1.254 255.255.255.0
!
ip dhcp pool for-client
   network 30.1.1.0 255.255.255.0
   default-router 30.1.1.254
!
ip dhcp pool for-ap
   network 20.1.1.0 255.255.255.0
   default-router 20.1.1.254
option 43 hex f104.0a01.0164
```

SW3650-1配置

```
hostname SW3650-1
!
ip routing
!
vlan 20
 name ap_network
!
interface GigabitEthernet1/0/1
 switchport mode trunk
 no shutdown
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
 no shutdown
```

SW3650-2配置

```
hostname SW3650-2
!
ip routing
!
vlan 20
 name ap_network
!
interface GigabitEthernet1/0/1
 switchport mode trunk
 no shutdown
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
 no shutdown
```

初始化5508-1（1）

System Name [Cisco_65:a6:a4] (31 characters max): WLC5508-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): Cisc0123
Re-enter Administrative Password : Cisc0123
Service Interface IP Address Configuration [static][DHCP]:

Enable Link Aggregation (LAG) [yes][NO]:

Management Interface IP Address: 10.1.1.100
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.1.1.254
Cleaning up Provisioning SSID
Management Interface VLAN Identifier (0 = untagged): 10
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.1.1.254

初始化5508-1（2）

Enable HA [yes][NO]:

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: qytang

Network Name (SSID): qytang

Configure DHCP Bridging Mode [yes][NO]:

Allow Static IP Addresses [YES][no]:

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: CN

初始化5508-1（3）

Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time is set.
Please see documentation for more details.

Would you like to configure IPv6 parameters[YES][no]: no

Configuration correct? If yes, system will save it and reset. [yes][NO]: **yes**

初始化5508-2（1）

System Name [Cisco_65:a6:a4] (31 characters max): WLC5508-2
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): Cisc0123
Re-enter Administrative Password : Cisc0123
Service Interface IP Address Configuration [static][DHCP]:

Enable Link Aggregation (LAG) [yes][NO]:

Management Interface IP Address: 10.1.1.101
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.1.1.254
Cleaning up Provisioning SSID
Management Interface VLAN Identifier (0 = untagged): 10
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.1.1.254

初始化5508-2（2）

Enable HA [yes][NO]:

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: qytang

Network Name (SSID): qytang

Configure DHCP Bridging Mode [yes][NO]:

Allow Static IP Addresses [YES][no]:

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: CN

初始化5508-2（3）

Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time is set.
Please see documentation for more details.

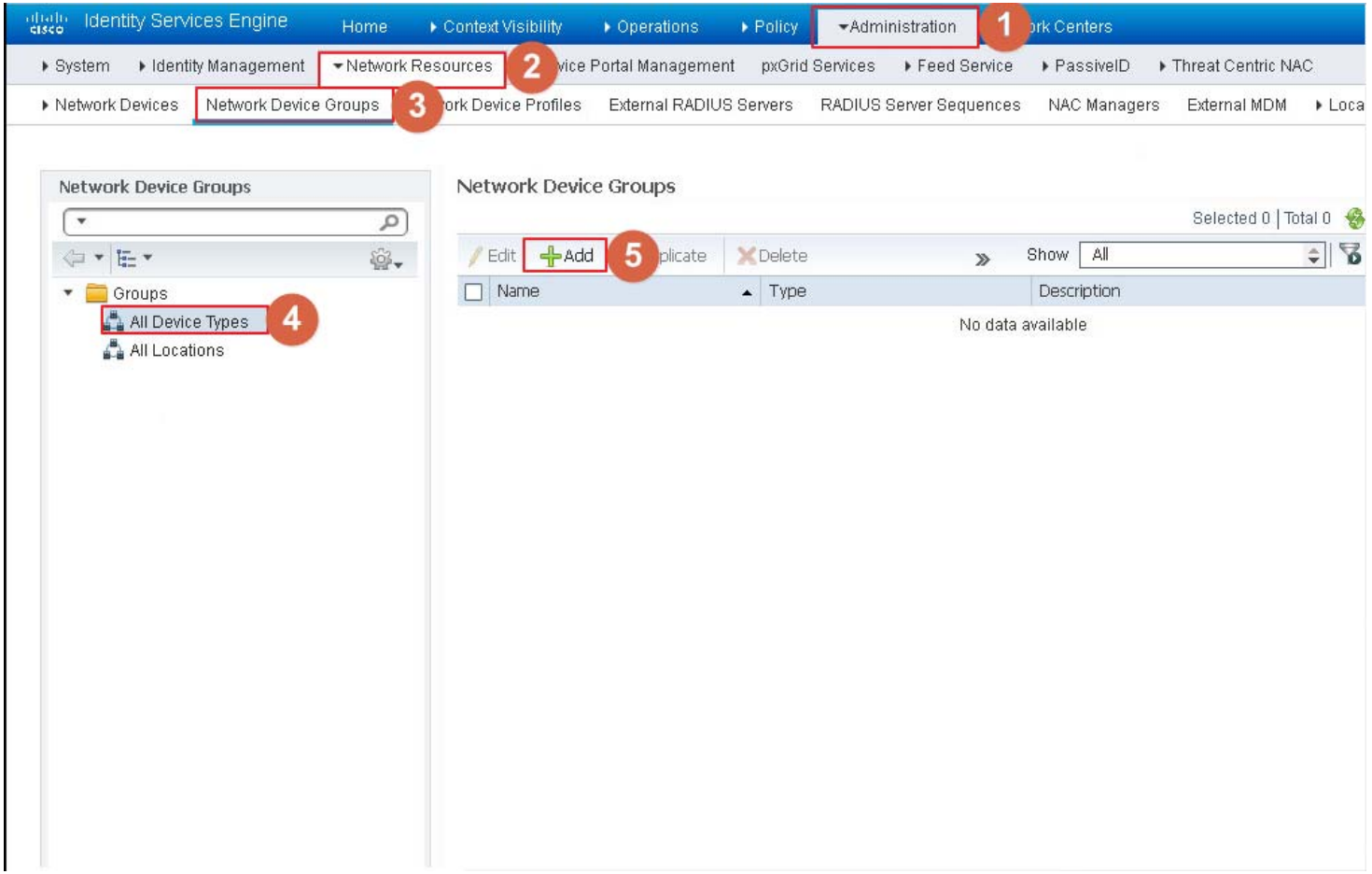
Would you like to configure IPv6 parameters[YES][no]: no

Configuration correct? If yes, system will save it and reset. [yes][NO]: **yes**

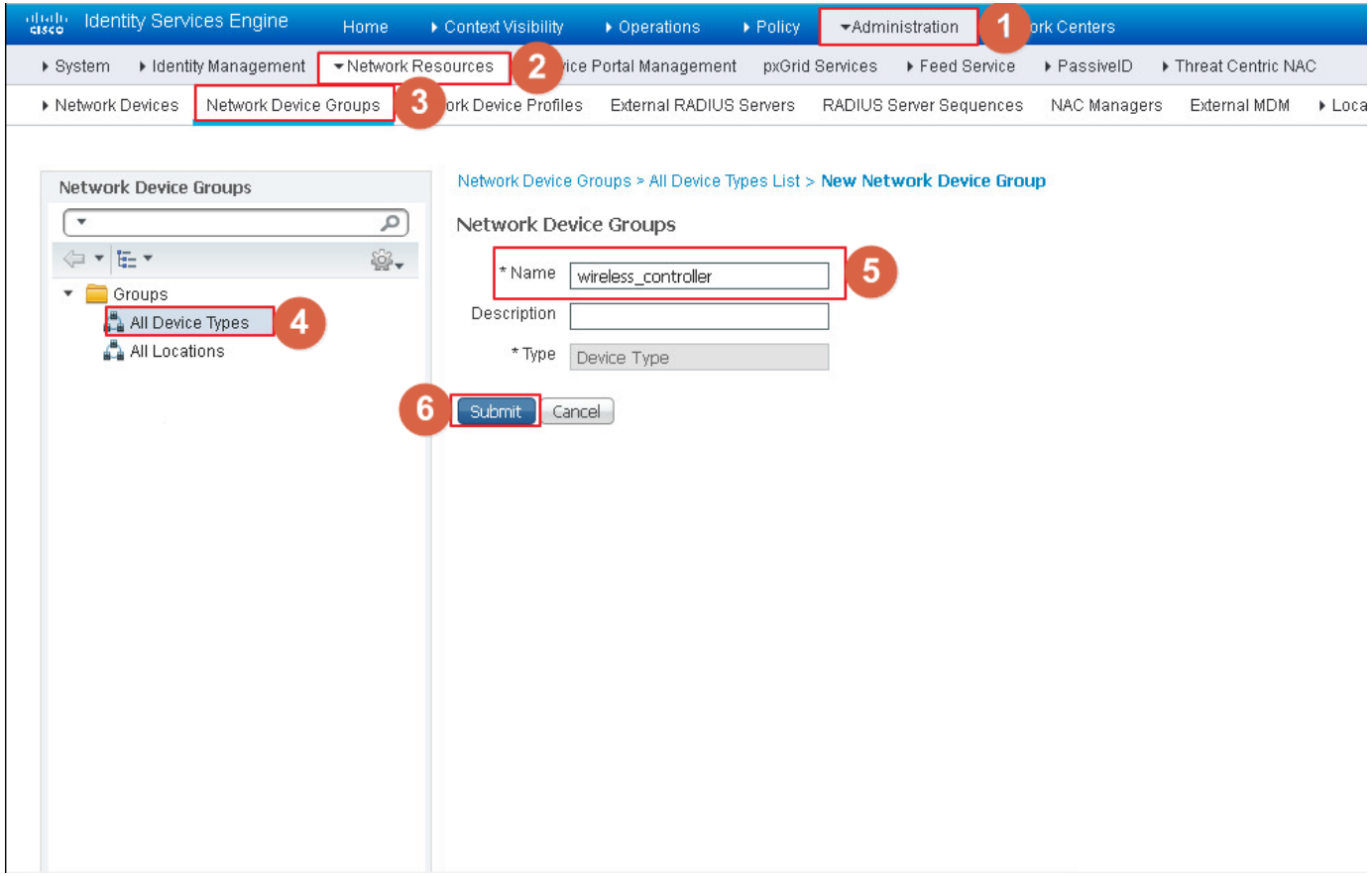
5508-1查看AP关联状态

严重确认两个AP
都管理激活状态

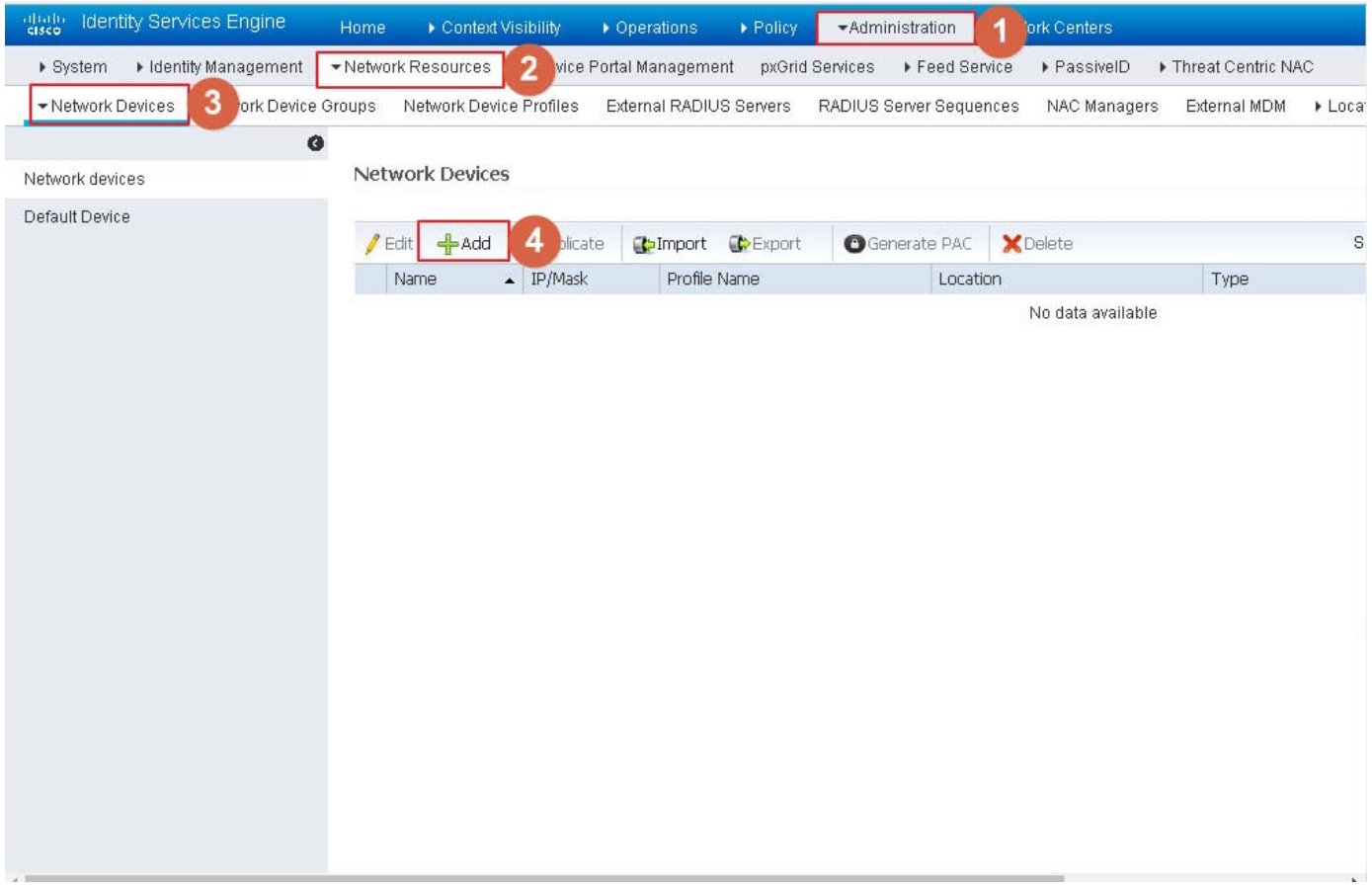
ISE创建NDG


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
1
System
Identity Management
Network Resources
2
pxGrid Services
Feed Service
PassiveID
Threat Centric NAC
Network Devices
Network Device Groups
3
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Network Device Groups
Groups
All Device Types
4
All Locations
Network Device Groups
Selected 0 | Total 0
Edit
Add
5
Delete
Show
All
Name
Type
Description
No data available

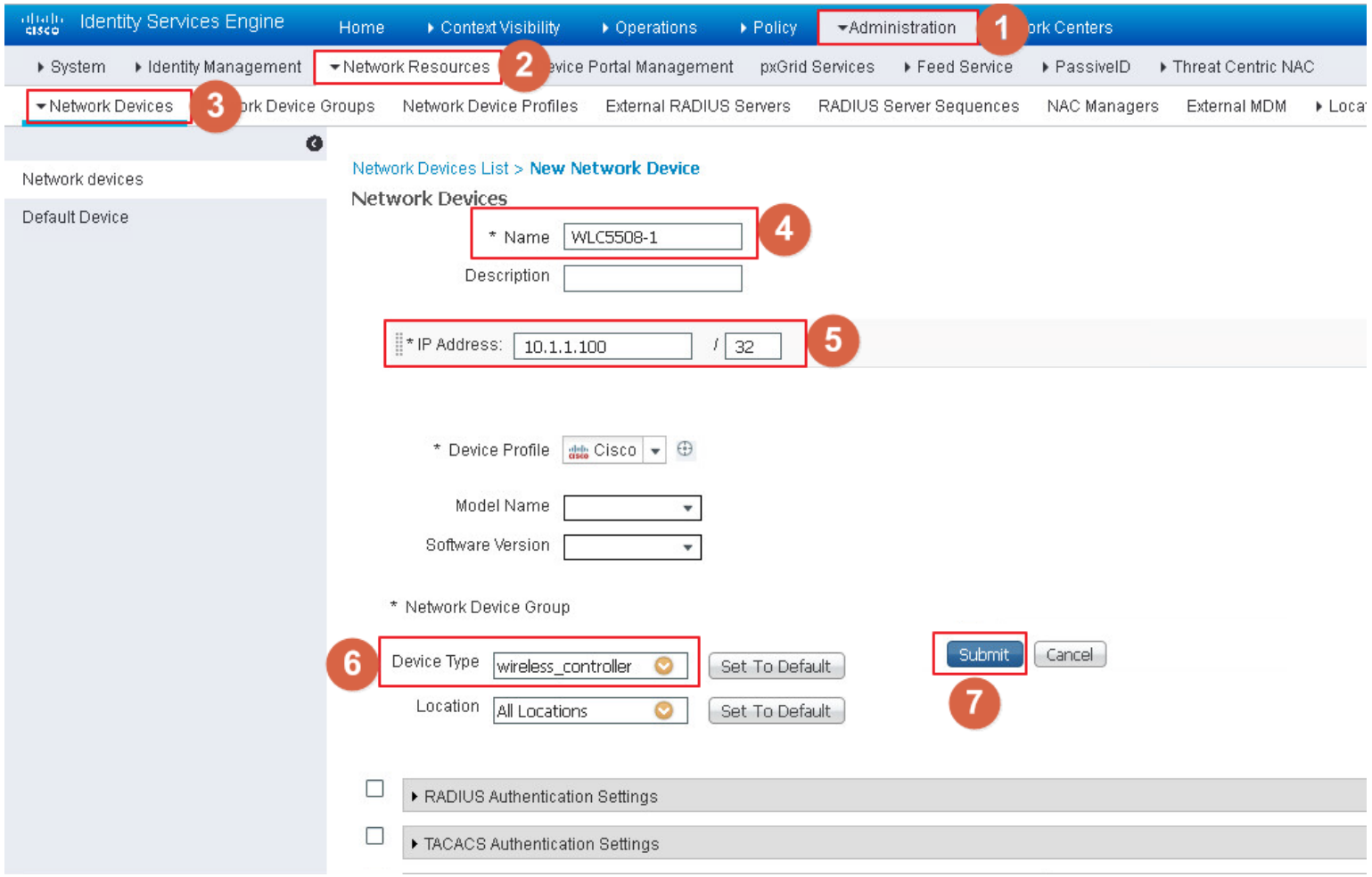
ISE创建NDG


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
1
System
Identity Management
Network Resources
2
pxGrid Services
Feed Service
PassiveID
Threat Centric NAC
Network Devices
Network Device Groups
3
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Network Device Groups
Groups
All Device Types
4
All Locations
Network Device Groups > All Device Types List > New Network Device Group
Network Device Groups
* Name
wireless_controller
5
Description
* Type
Device Type
6
Submit
Cancel

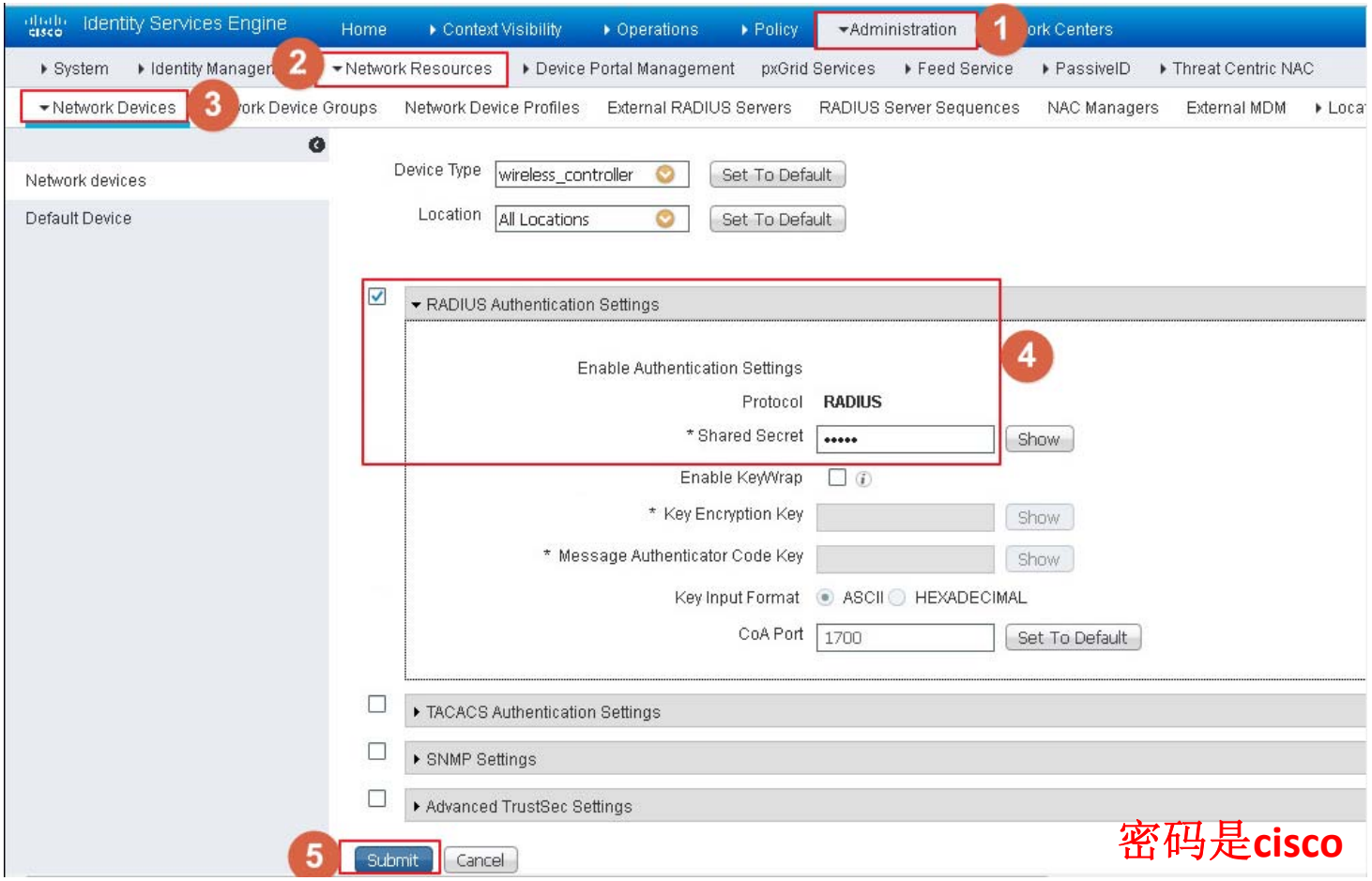
ISE创建WLC5508-1



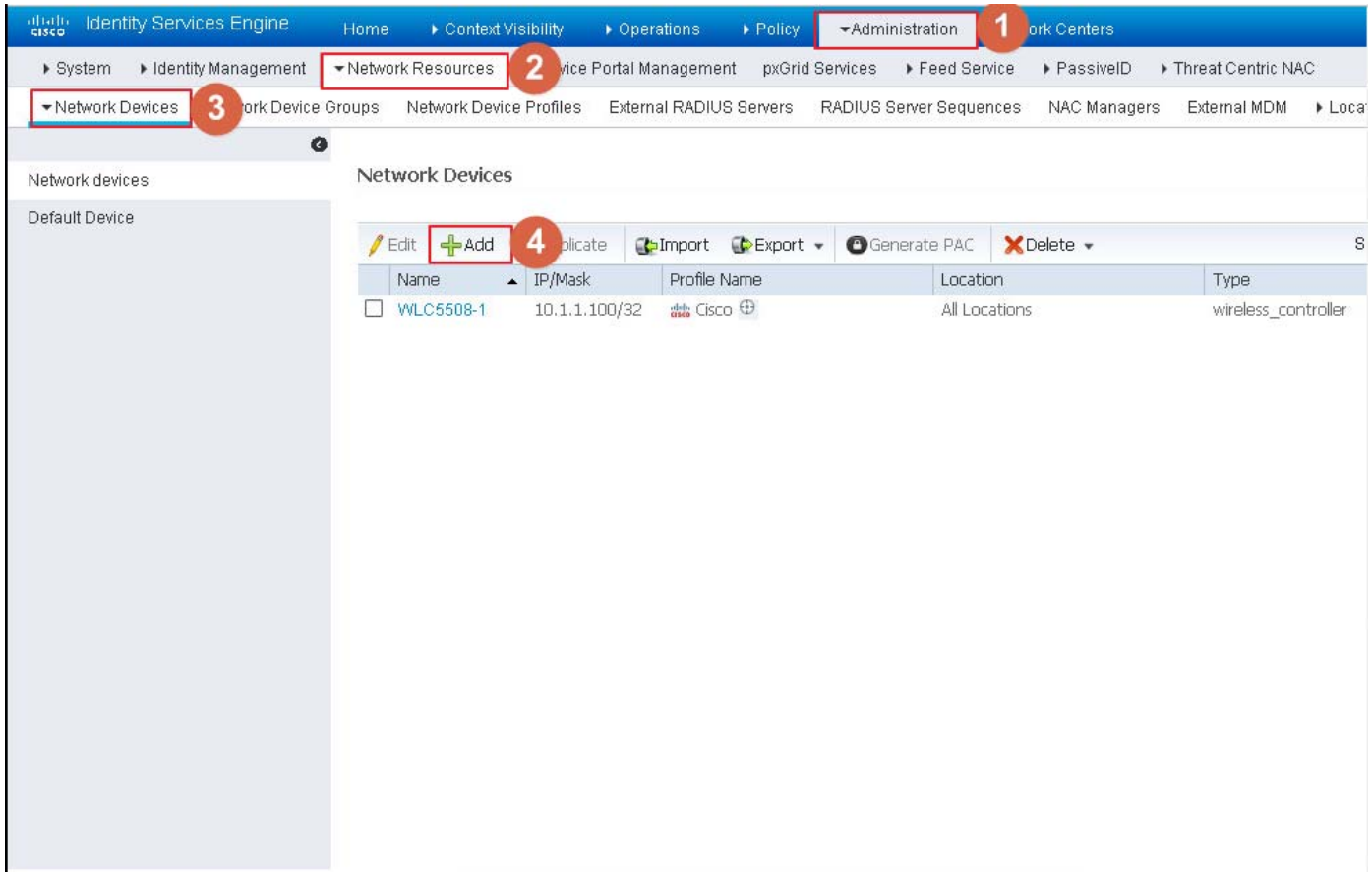
ISE创建WLC5508-1



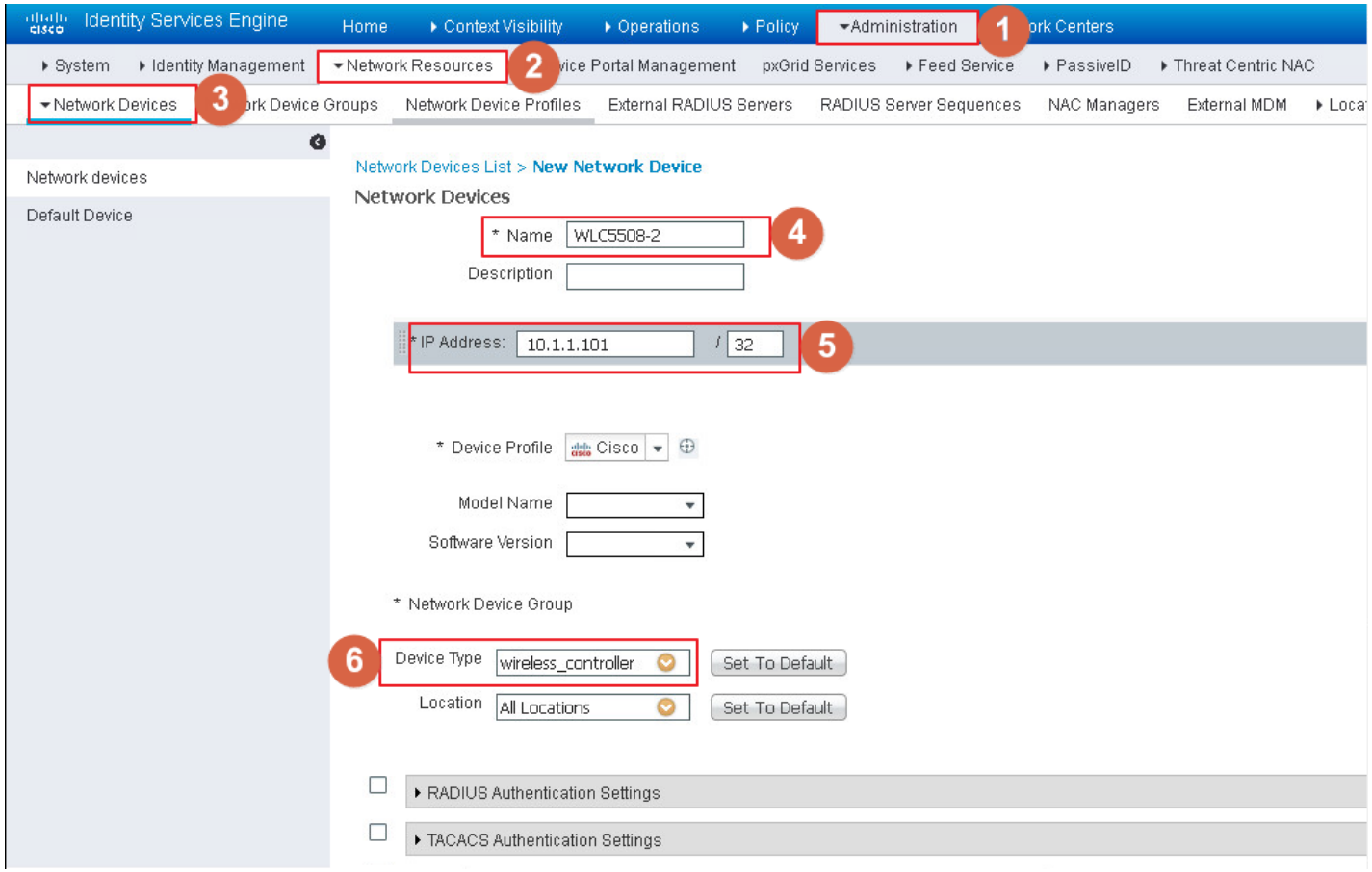
ISE创建WLC5508-1



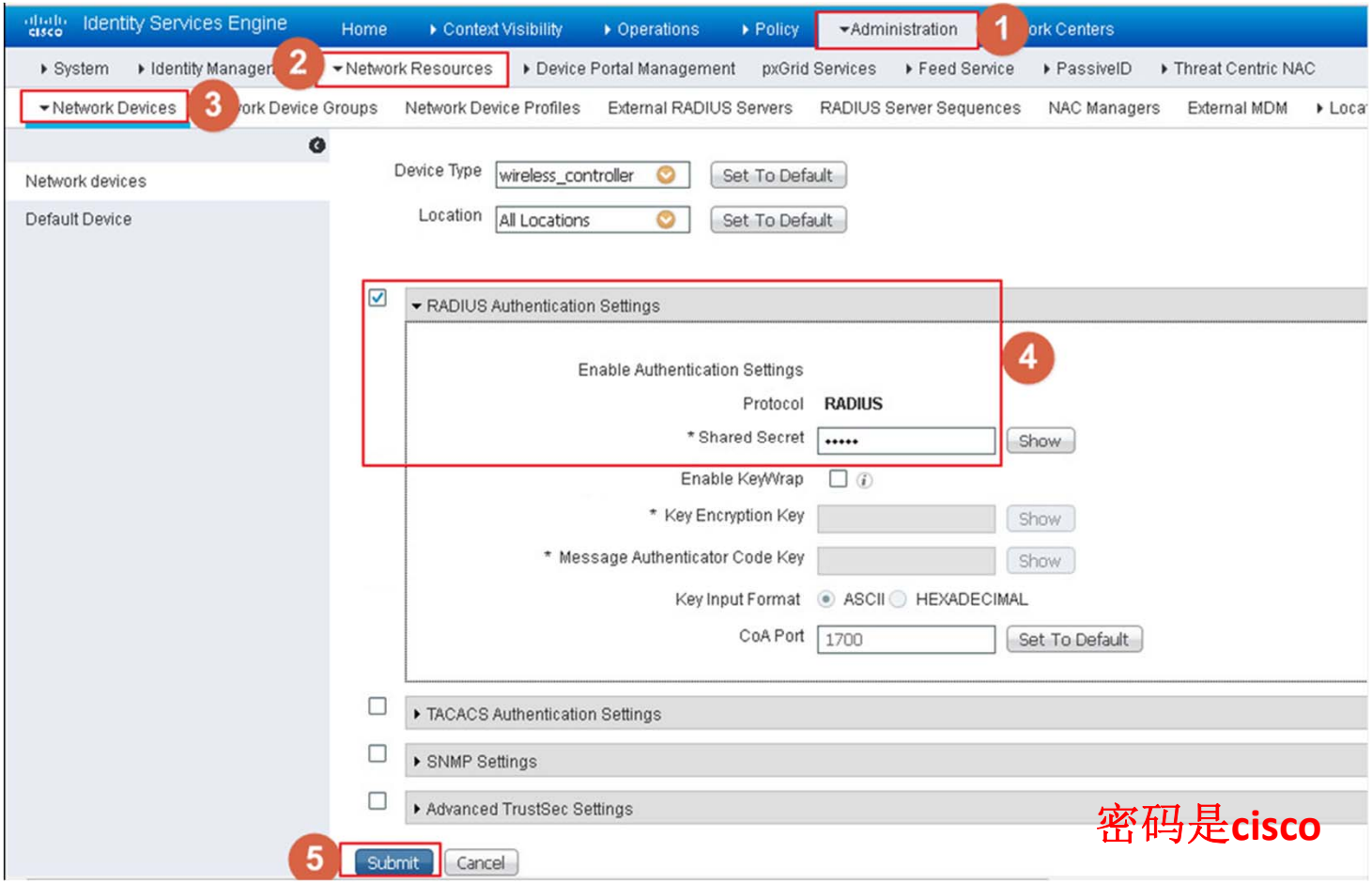
ISE创建WLC5508-2



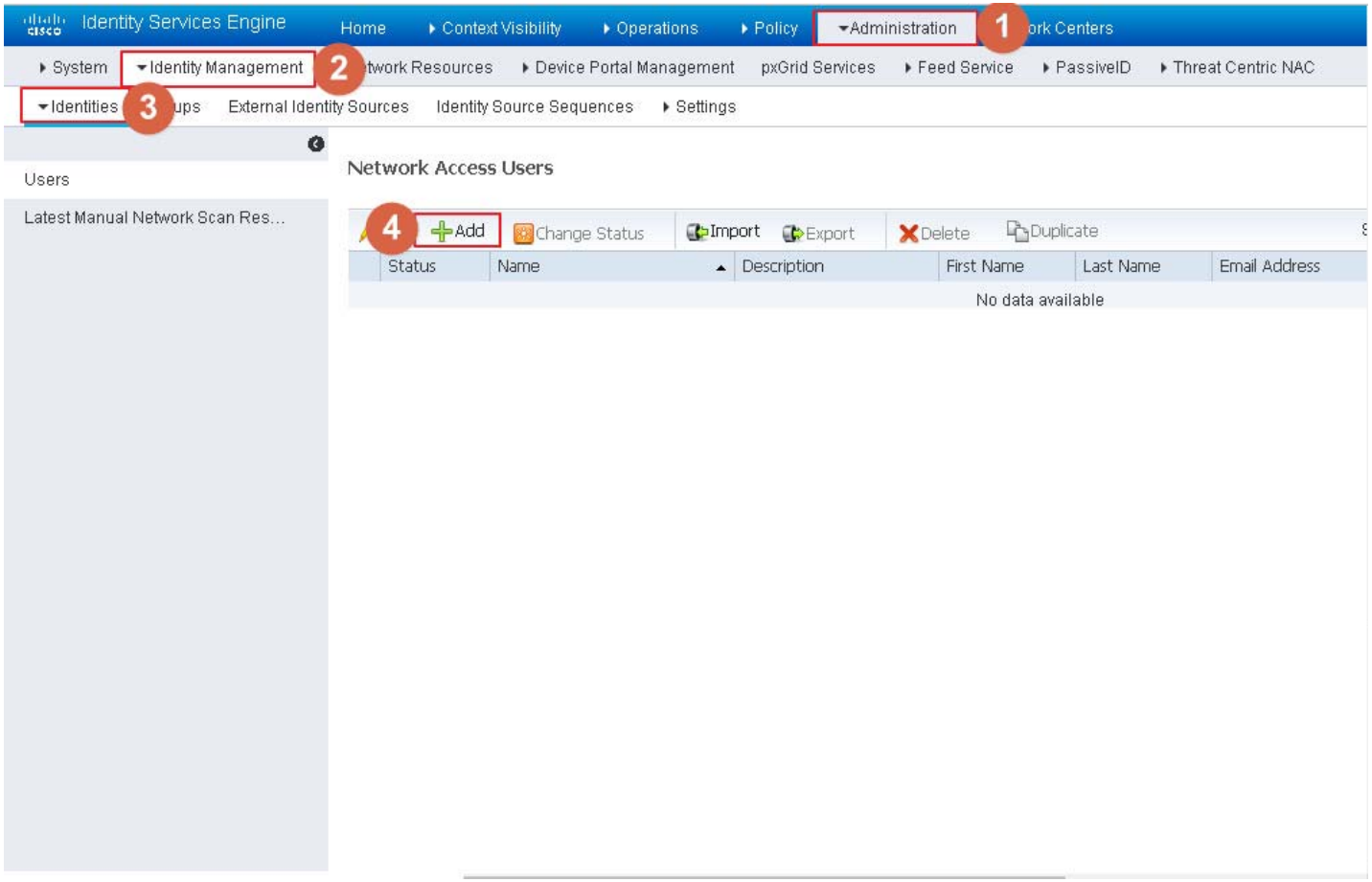
ISE创建WLC5508-2



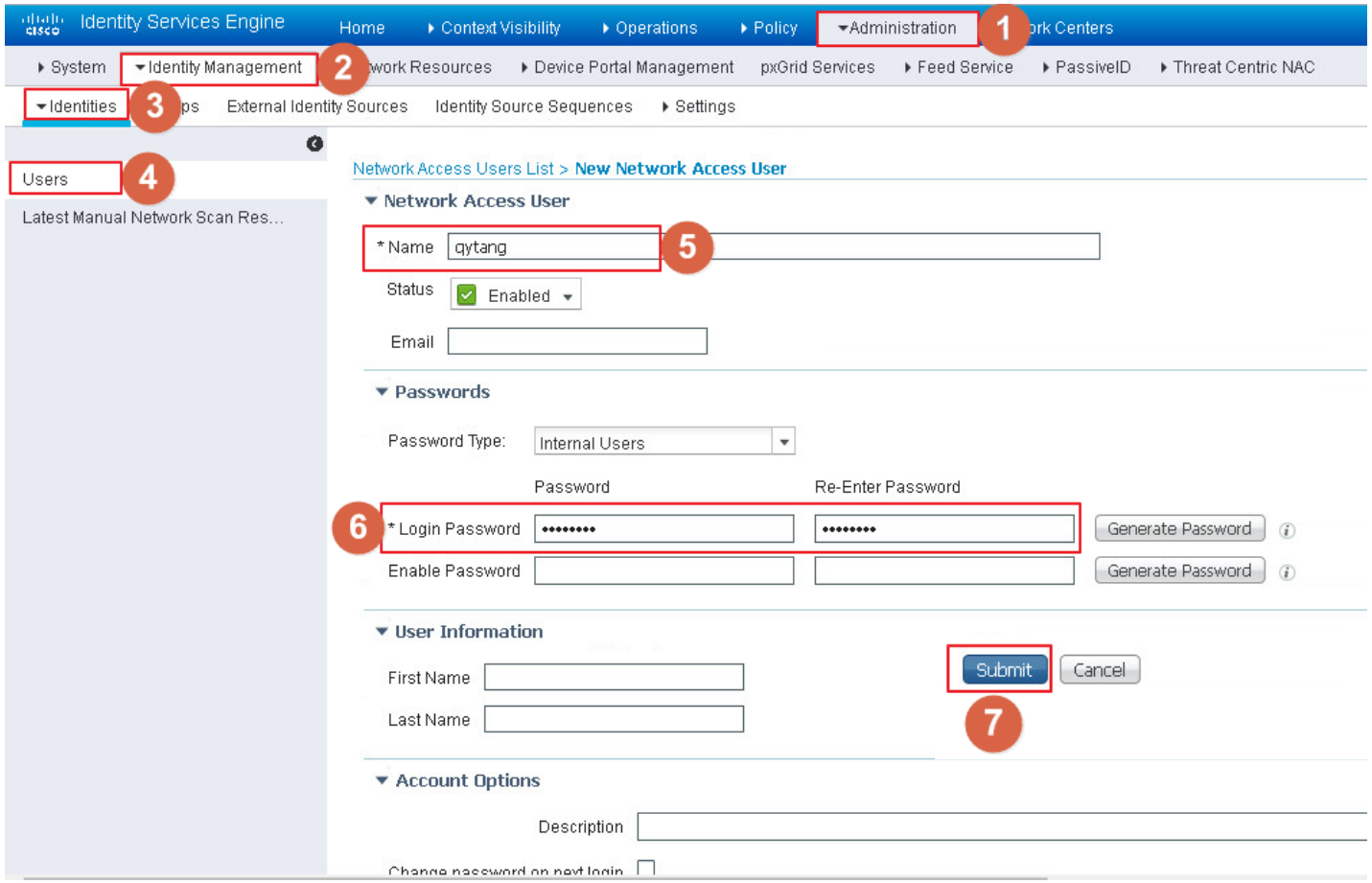
ISE创建WLC5508-2



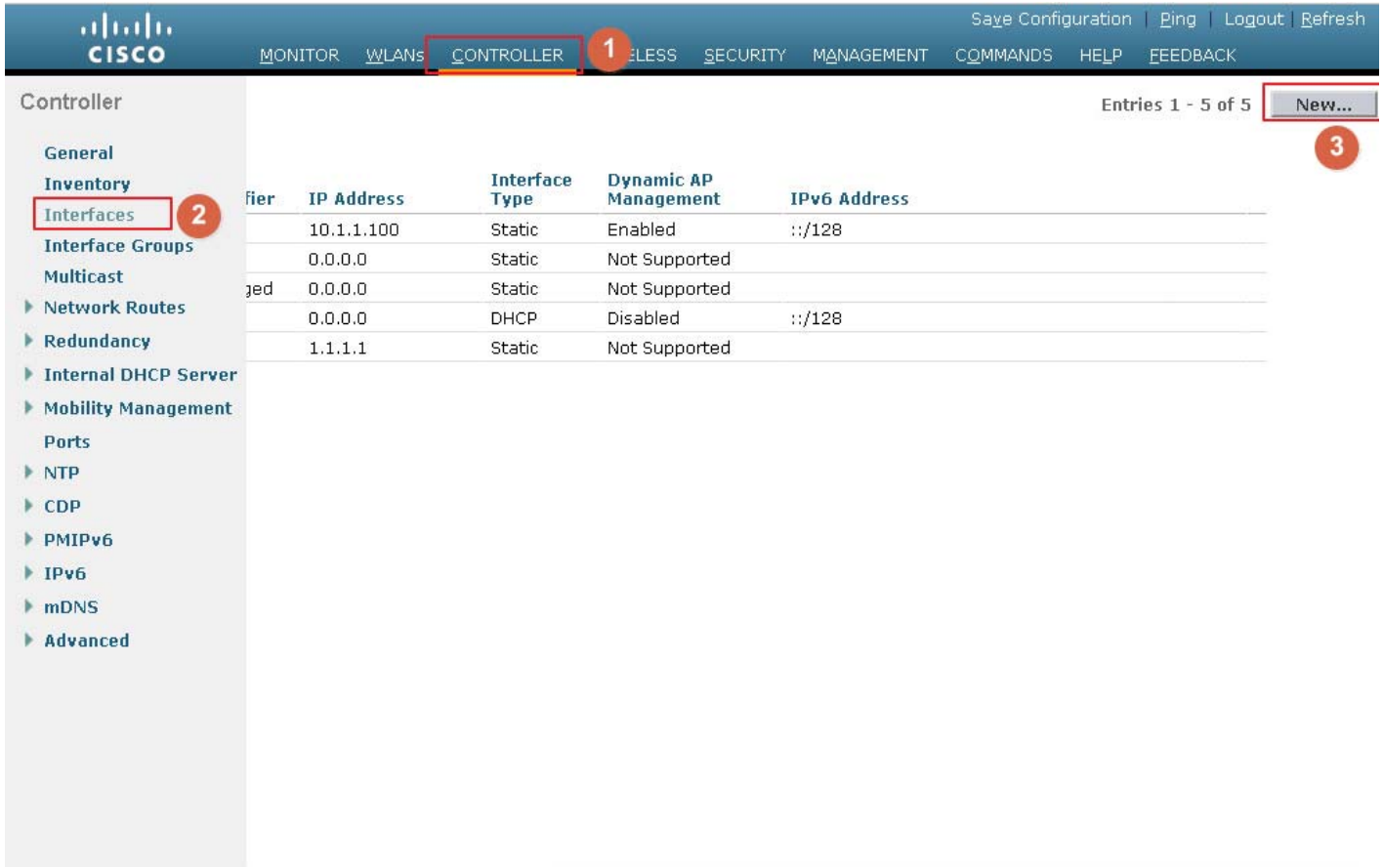
ISE创建用户名和密码



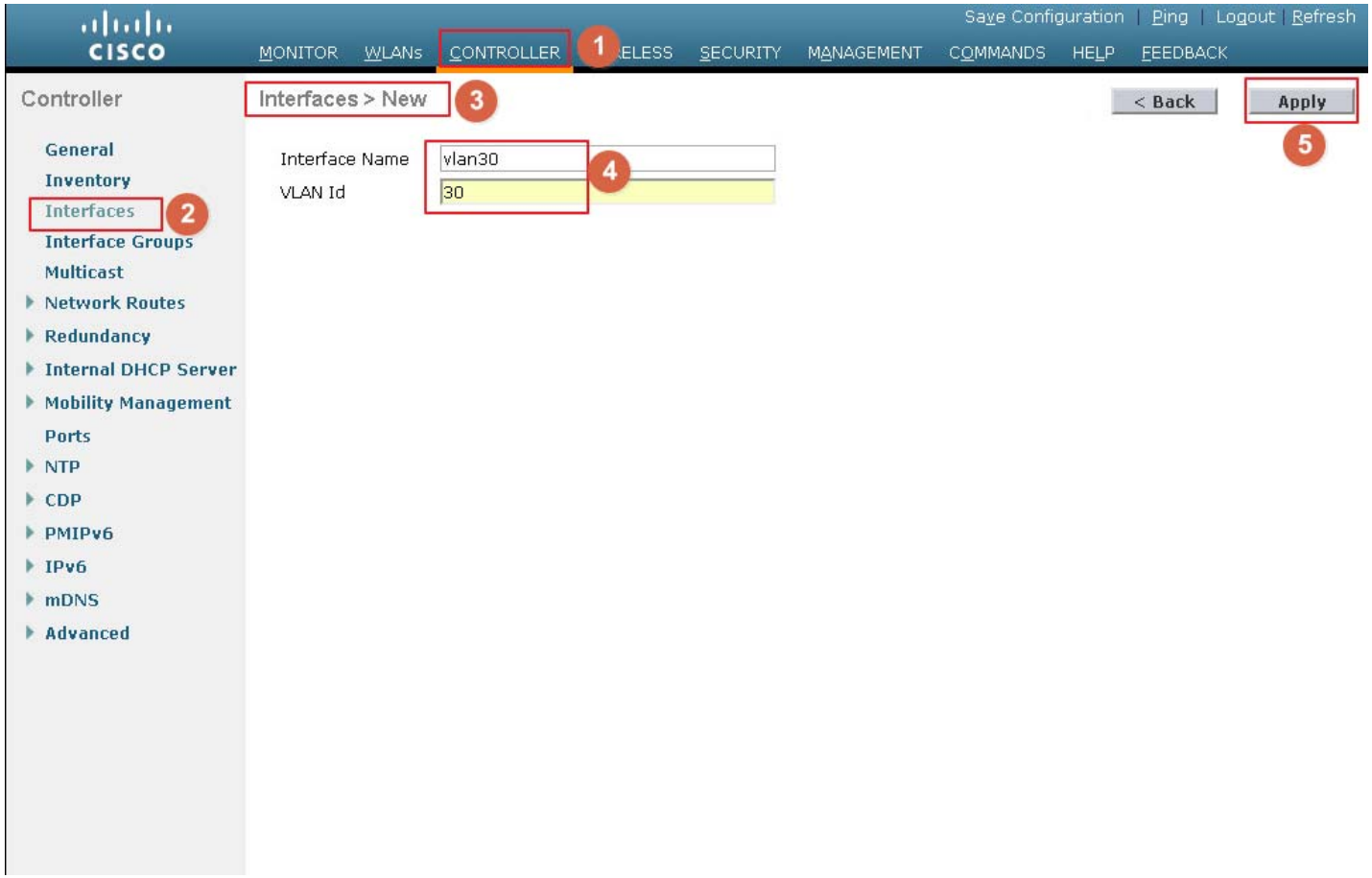
ISE创建用户名和密码



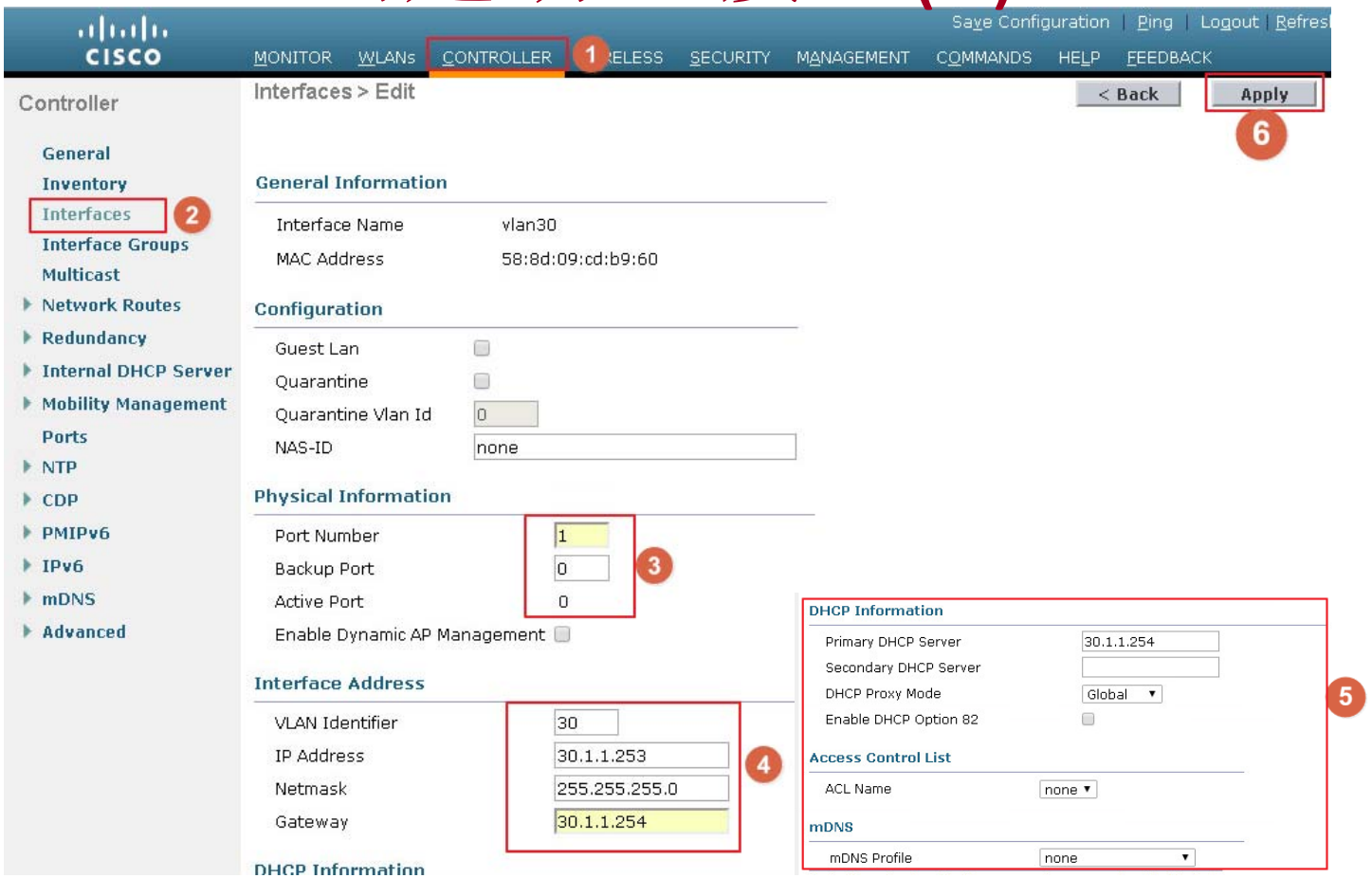
创建动态接口(1)


Save Configuration | Ping | Logout | Refresh
MONITOR
WLANs
CONTROLLER
1
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Controller
General
Inventory
Interfaces
2
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
PMIPv6
IPv6
mDNS
Advanced
Entries 1 - 5 of 5
New...
3
IP Address
Interface Type
Dynamic AP Management
IPv6 Address
10.1.1.100 Static Enabled ::/128
0.0.0.0 Static Not Supported
0.0.0.0 Static Not Supported
0.0.0.0 DHCP Disabled ::/128
1.1.1.1 Static Not Supported

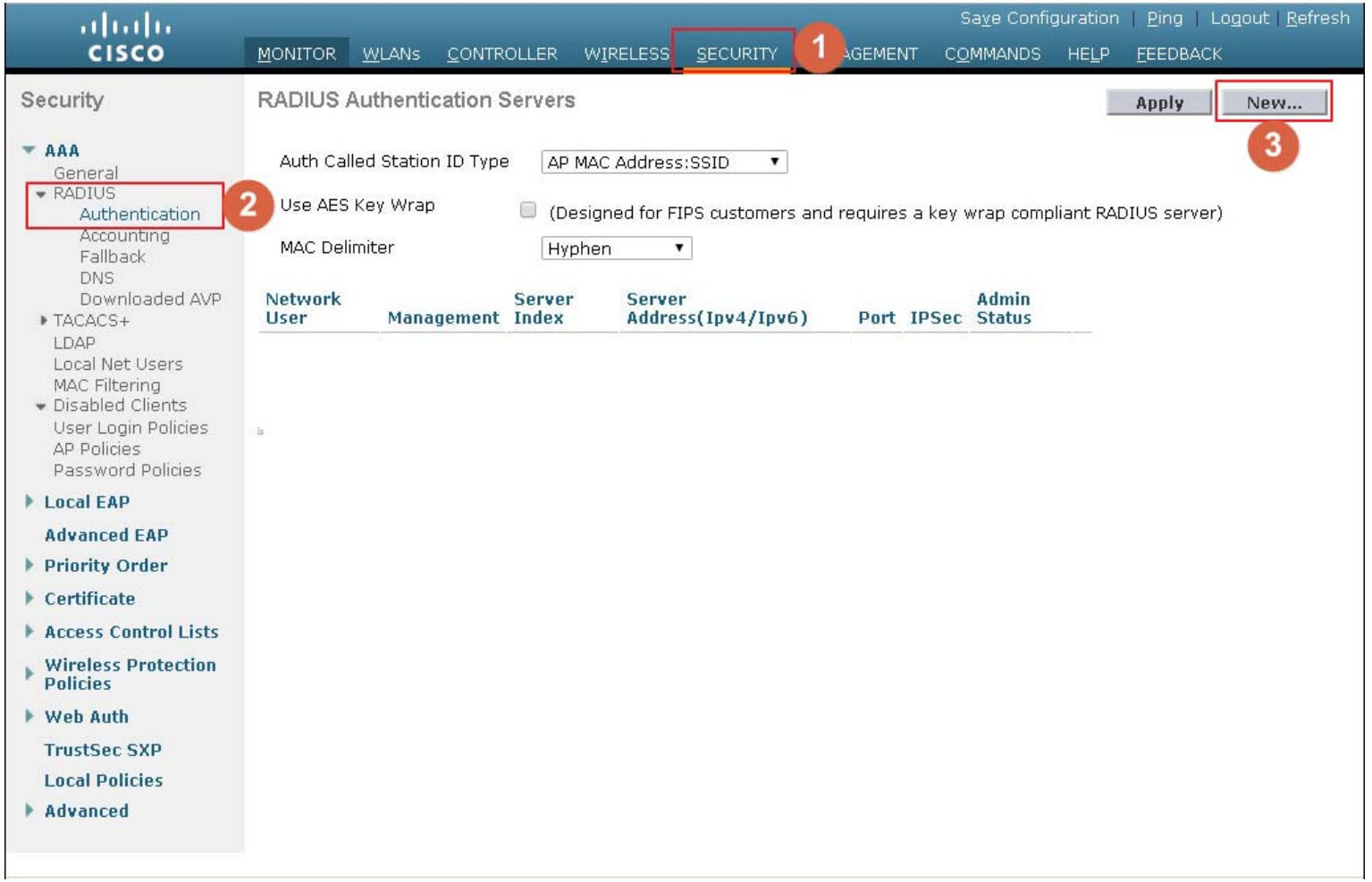
创建动态接口(1)


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER 1 ELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller
Interfaces > New 3
< Back
Apply 5
General
Inventory
Interfaces 2
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
PMIPv6
IPv6
mDNS
Advanced
Interface Name vlan30
VLAN Id 30 4

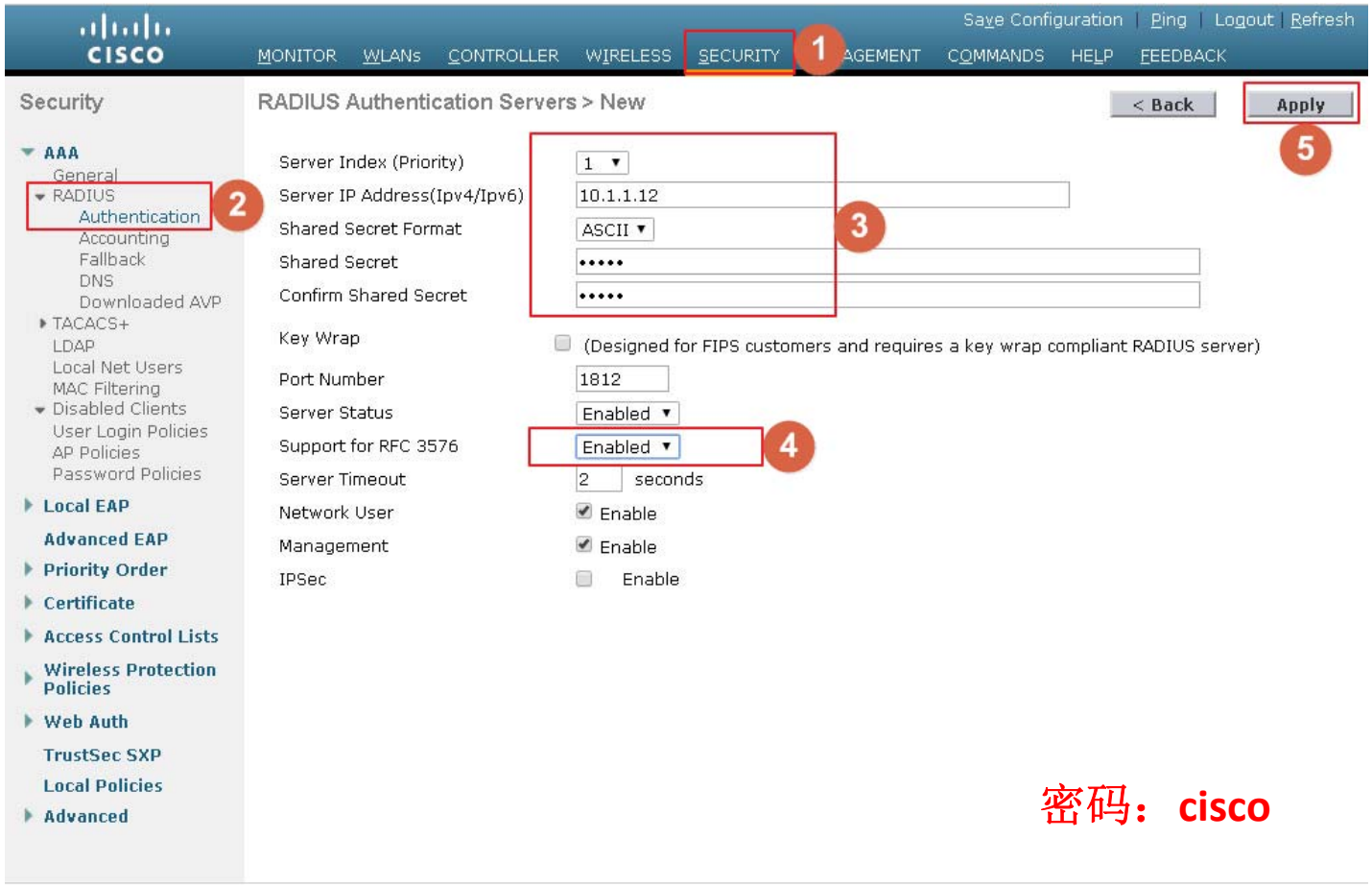
创建动态接口(2)


Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER 1 RELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller
General
Inventory
Interfaces 2
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
PMIPv6
IPv6
mDNS
Advanced
Interfaces > Edit
< Back
Apply
6
General Information
Interface Name vlan30
MAC Address 58:8d:09:cd:b9:60
Configuration
Guest Lan
Quarantine
Quarantine Vlan Id 0
NAS-ID none
Physical Information
Port Number 1
Backup Port 0
Active Port 0
3
Enable Dynamic AP Management
Interface Address
VLAN Identifier 30
IP Address 30.1.1.253
Netmask 255.255.255.0
Gateway 30.1.1.254
4
DHCP Information
Primary DHCP Server 30.1.1.254
Secondary DHCP Server
DHCP Proxy Mode Global
Enable DHCP Option 82
5
Access Control List
ACL Name none
mDNS
mDNS Profile none

5508-1创建AAA

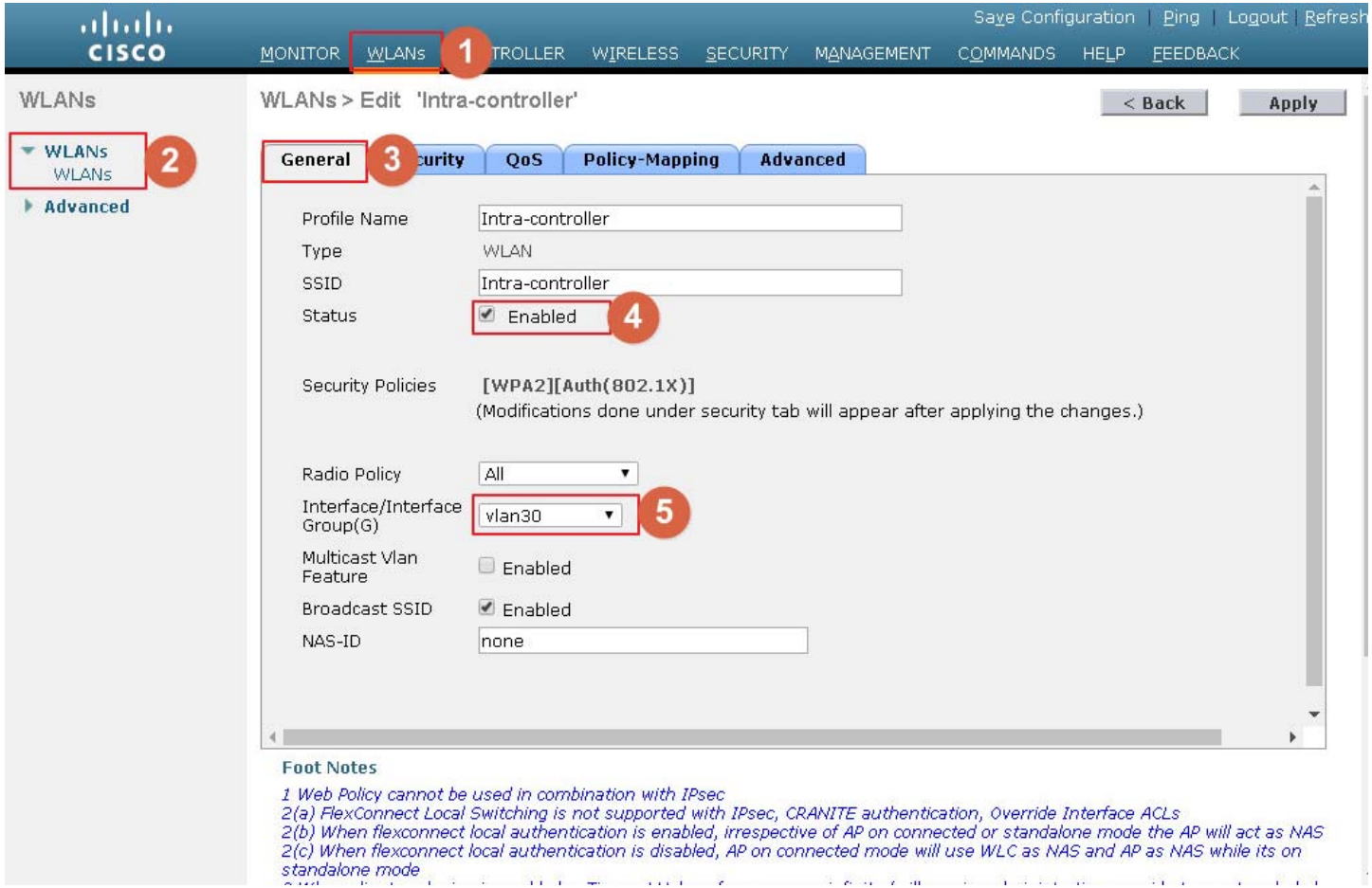

cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY 1 AGEMENT COMMANDS HELP FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec SXP
Local Policies
Advanced
2
RADIUS Authentication Servers
Apply
New...
3
Auth Called Station ID Type
AP MAC Address:SSID
Use AES Key Wrap
(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Delimiter
Hyphen
Network User
Management
Server Index
Server Address(Ipv4/Ipv6)
Port
IPSec
Admin Status

5508-1创建AAA

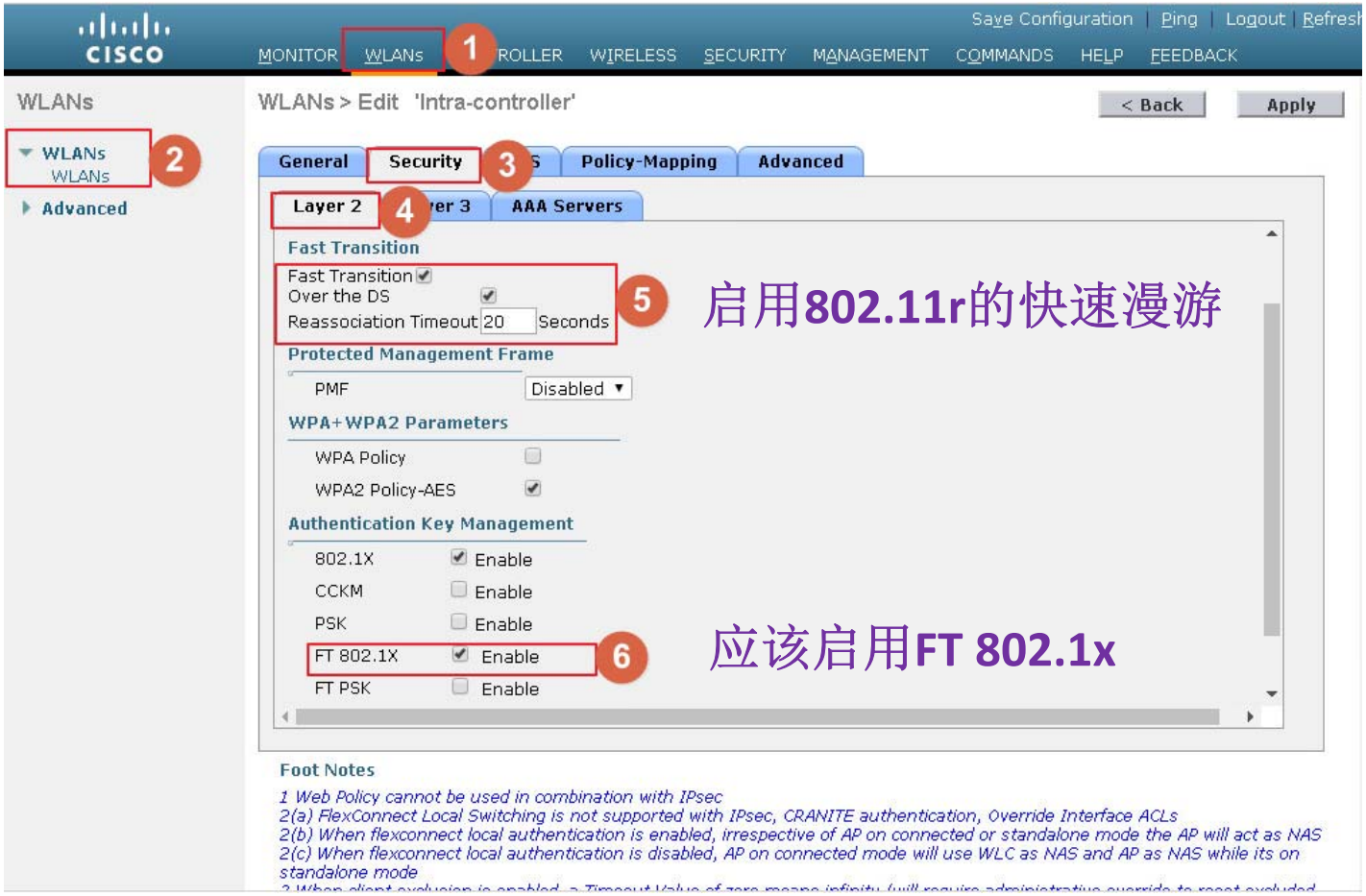


密码： cisco

5508-1创建SSID



5508-1修改认证方式



不启用FT配置

传统配置，包比FT多，效率更低，但是人很难感受到

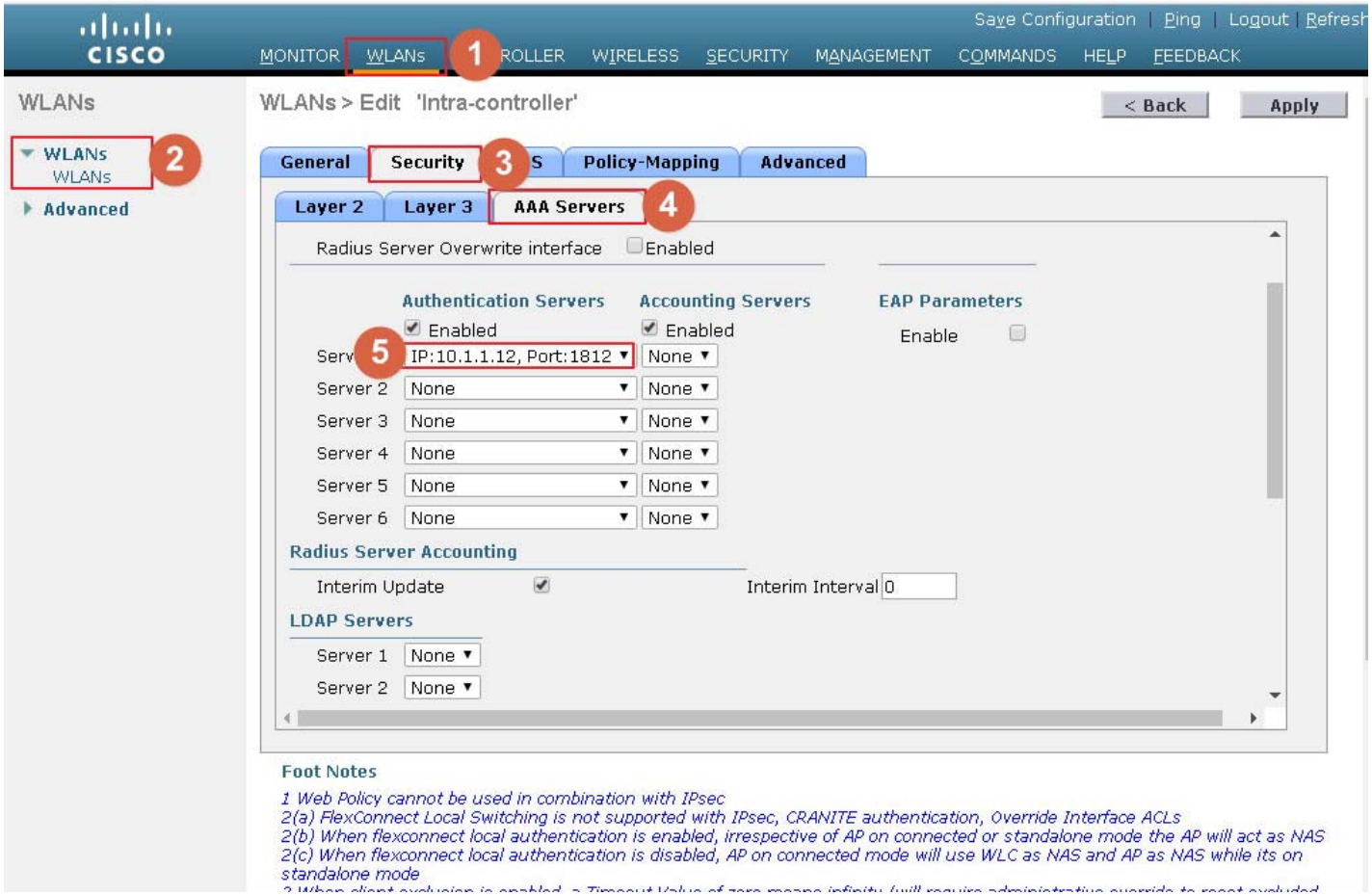
本页仅仅为展示保留FT设置

CCKM配置

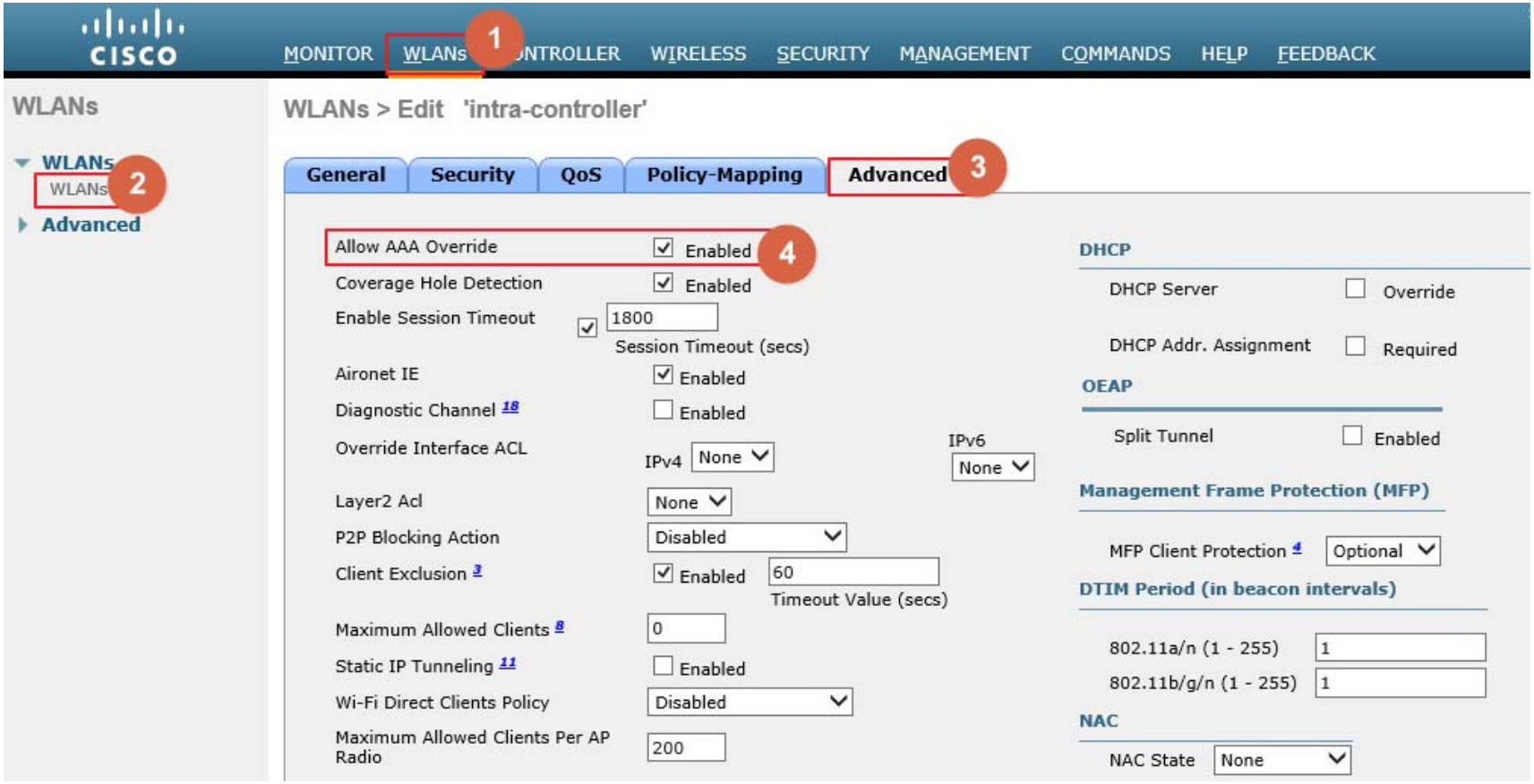
思科私有解决方案，需要思科CCX客户端，不推荐使用

本页仅仅为展示
保留FT设置

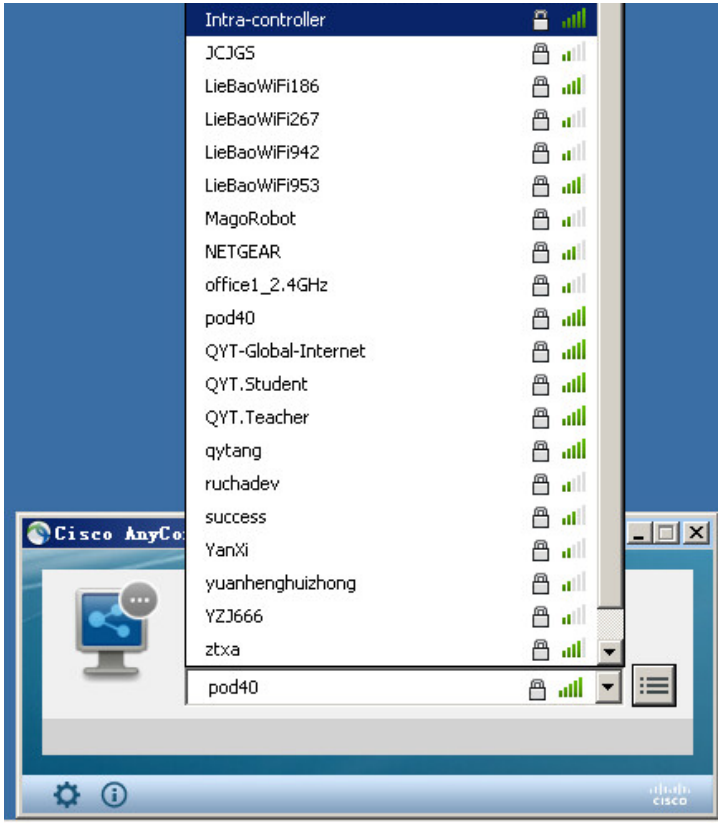
5508-1指定AAA服务器

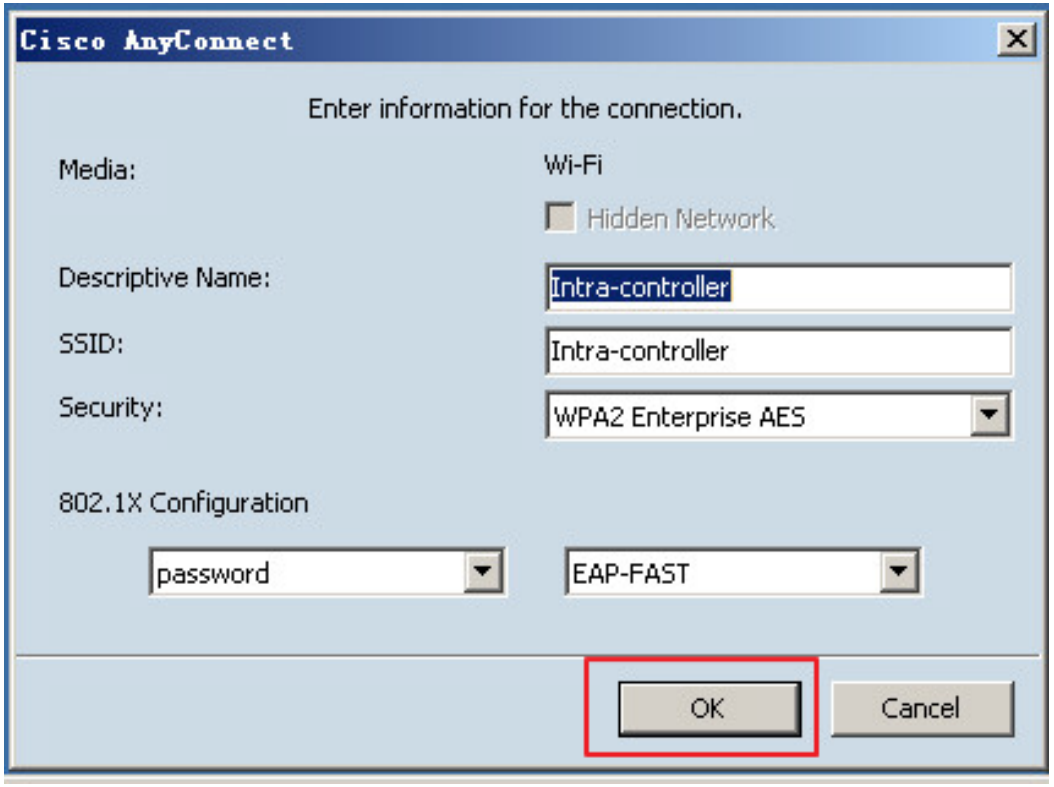


5508-1指定AAA override

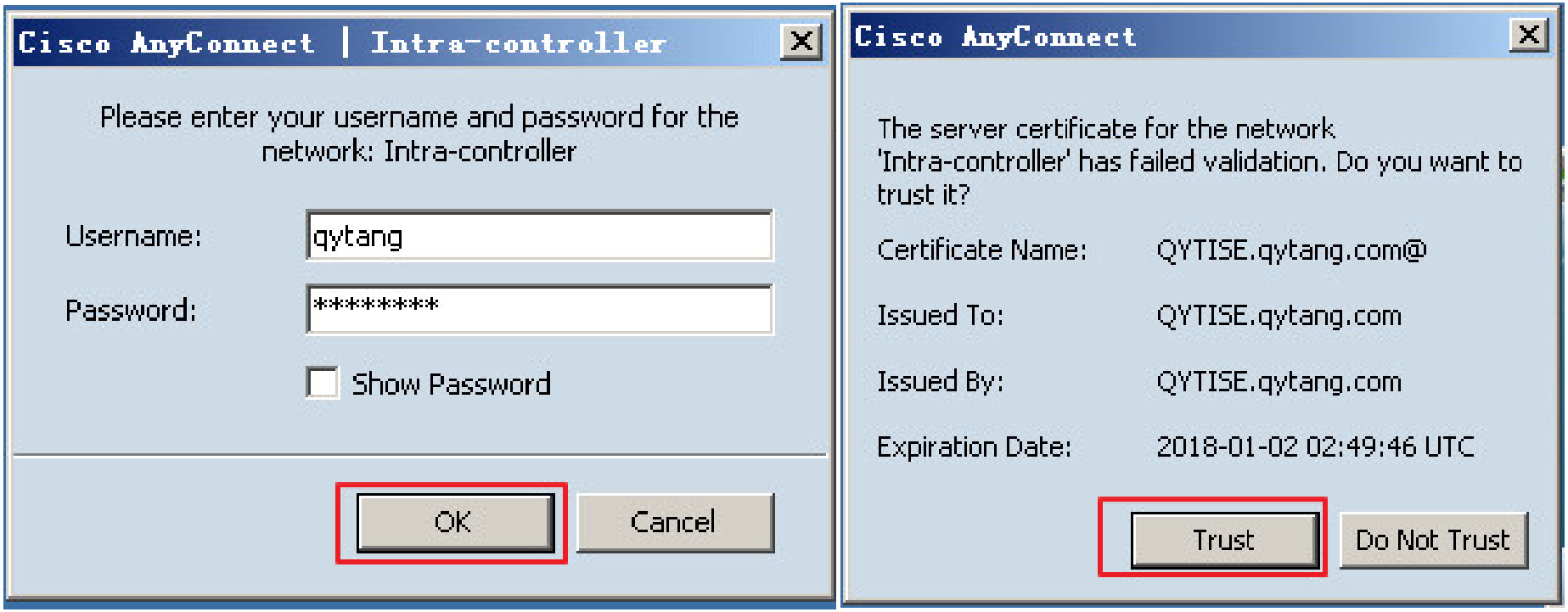


Test-PC创建无线认证





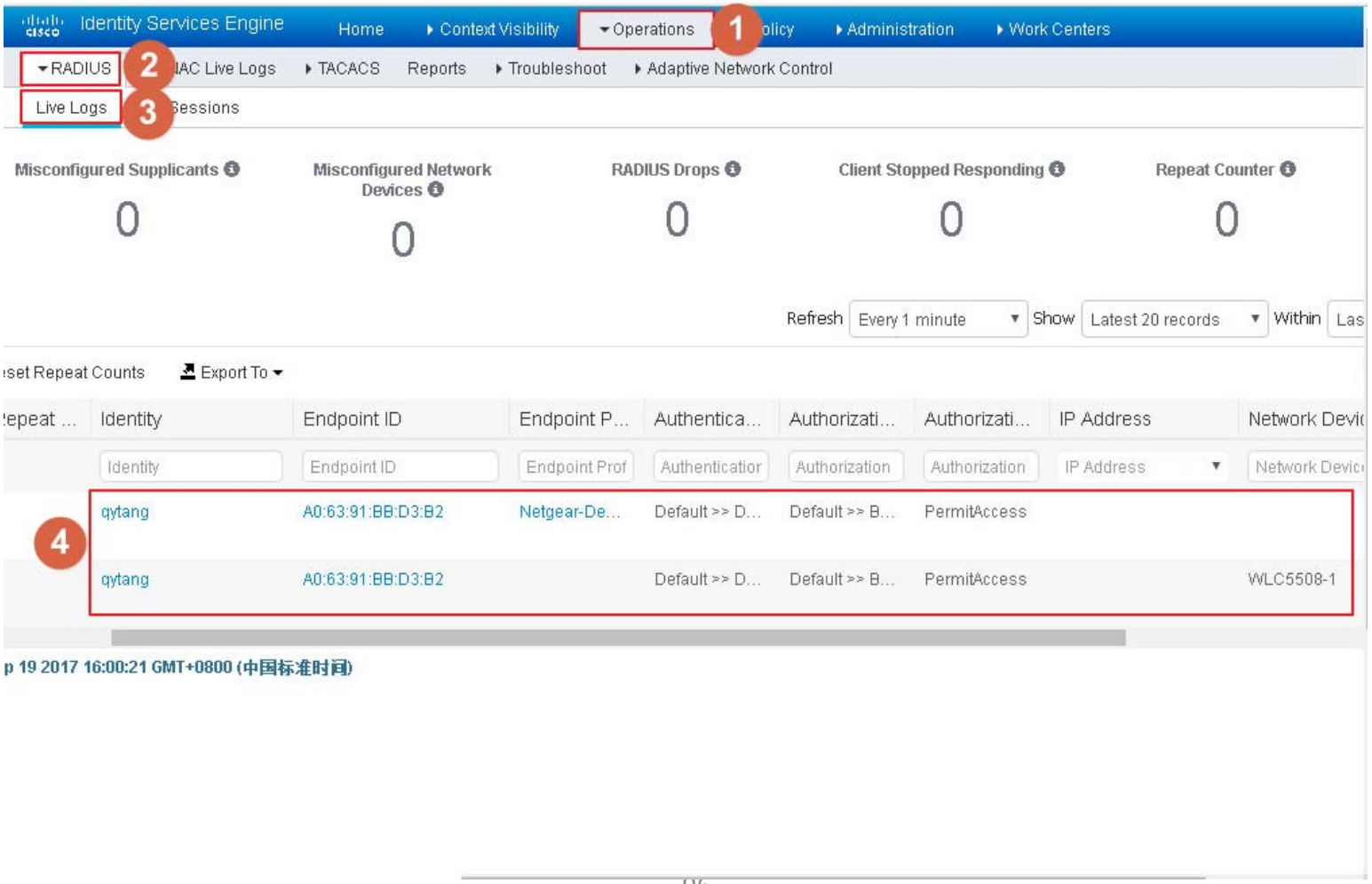
Test-PC连接无线


Cisco AnyConnect | Intra-controller
Please enter your username and password for the network: Intra-controller
Username:
qytang
Password:
****
Show Password
OK
Cancel
Cisco AnyConnect
The server certificate for the network 'Intra-controller' has failed validation. Do you want to trust it?
Certificate Name:
QYTISE.qytang.com@
Issued To:
QYTISE.qytang.com
Issued By:
QYTISE.qytang.com
Expiration Date:
2018-01-02 02:49:46 UTC
Trust
Do Not Trust

Test-PC连接无线

```
   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::c0e0:fafb:1174:9380%15
   IPv4 地址 . . . . . . . . . . . . : 30.1.1.1
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 30.1.1.254

隧道适配器 isatap.{7F06461E-C4A6-4E5C-8AFC-BABE03FA5426}:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

隧道适配器 6TO4 Adapter:

   连接特定的 DNS 后缀 . . . . . . . :
   IPv6 地址 . . . . . . . . . . . . : 2002:1e01:101::1e01:101
   默认网关. . . . . . . . . . . . . :

隧道适配器 Teredo Tunneling Pseudo-Interface:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

C:\Users\Administrator>ping 10.1.1.254

正在 Ping 10.1.1.254 具有 32 字节的数据:
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255

10.1.1.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 2ms, 平均 = 1ms

C:\Users\Administrator>AA
```

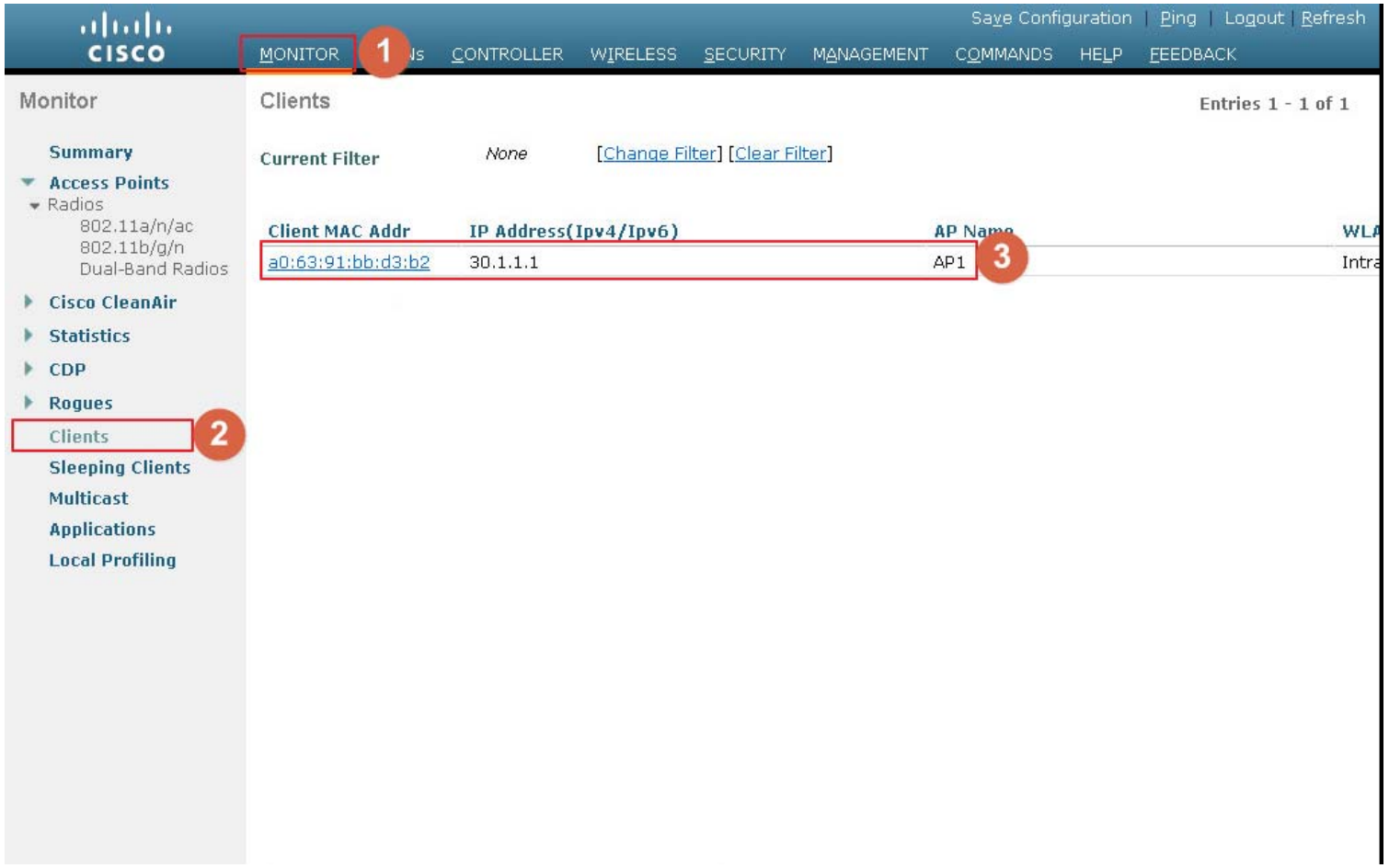
查看ISE认证


Identity Services Engine
Home
Context Visibility
Operations
1
olicy
Administration
Work Centers
RADIUS
2
IAC Live Logs
TACACS
Reports
Troubleshoot
Adaptive Network Control
Live Logs
3
Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Repeat Counter
0
Refresh
Every 1 minute
Show
Latest 20 records
Within
Las
set Repeat Counts
Export To
epeat ...
Identity
Endpoint ID
Endpoint P...
Authentica...
Authorizati...
Authorizati...
IP Address
Network Devi
Identity
Endpoint ID
Endpoint Prof
Authenticatior
Authorization
Authorization
IP Address
Network Devic
4
qytang
A0:63:91:BB:D3:B2
Netgear-De...
Default >> D...
Default >> B...
PermitAccess
qytang
A0:63:91:BB:D3:B2
Default >> D...
Default >> B...
PermitAccess
WLC5508-1
p 19 2017 16:00:21 GMT+0800 (中国标准时间)

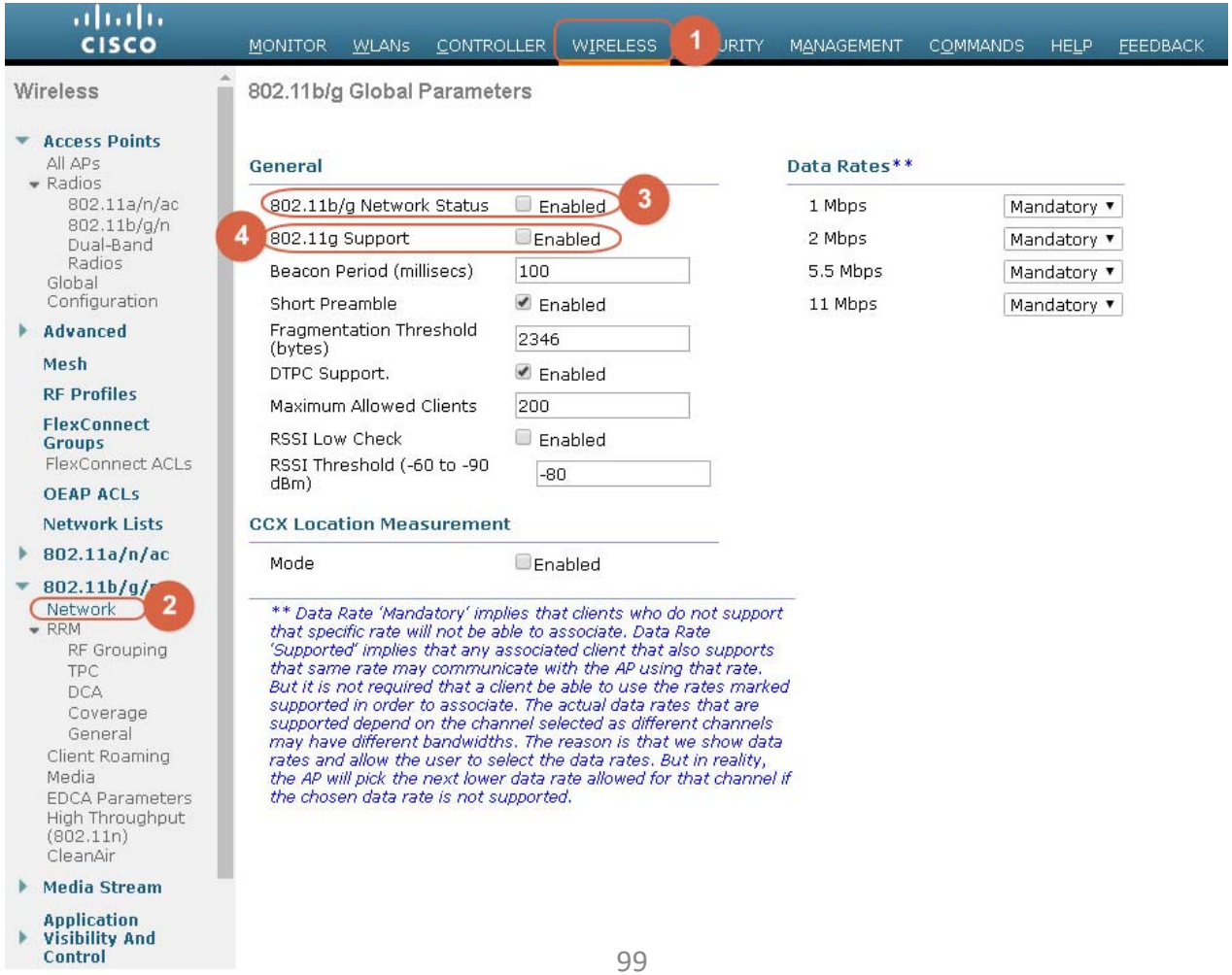
测试漫游

```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping 10.1.1.254 -t

正在 Ping 10.1.1.254 具有 32 字节的数据:
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
```

查看客户端关联AP


Save Configuration | Ping | Logout | Refresh
MONITOR
1
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Monitor
Summary
Access Points
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Cisco CleanAir
Statistics
CDP
Rogues
Clients
2
Sleeping Clients
Multicast
Applications
Local Profiling
Clients
Entries 1 - 1 of 1
Current Filter
None
[Change Filter] [Clear Filter]
Client MAC Addr
IP Address(Ipv4/Ipv6)
AP Name
a0:63:91:bb:d3:b2
30.1.1.1
AP1
3

关闭两个控制器的2.4G信号



天线与型号强度调整

802.11a/n Cisco APs > Configure

General

AP Name	AP2
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☐ C ☐

RF Channel Assignment

Current Channel	161
Channel Width *	20 MHz

** Channel width can be configured only when channel configuration is in custom mode*

Assignment Method	Global / Custom

Tx Power Level Assignment

Current Tx Power Level	6
Assignment Method	Global / Custom 6

Performance Profile

View and edit Performance Profile for this AP

Performance Profile

Note: Changing any of the parameters causes … disabled and thus may result in loss of connect

送出端

信号调整到最小（6）
天线只留A

接收端

信号调整到最大（1）
天线A B C全部打开

802.11a/n Cisco APs > Configure

General

AP Name	AP1
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel	149
Channel Width *	20 MHz

** Channel width can be configured only when channel configuration is in custom mode*

Assignment Method	Global / Custom

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	Global / Custom 1

Performance Profile

View and edit Performance Profile for this AP

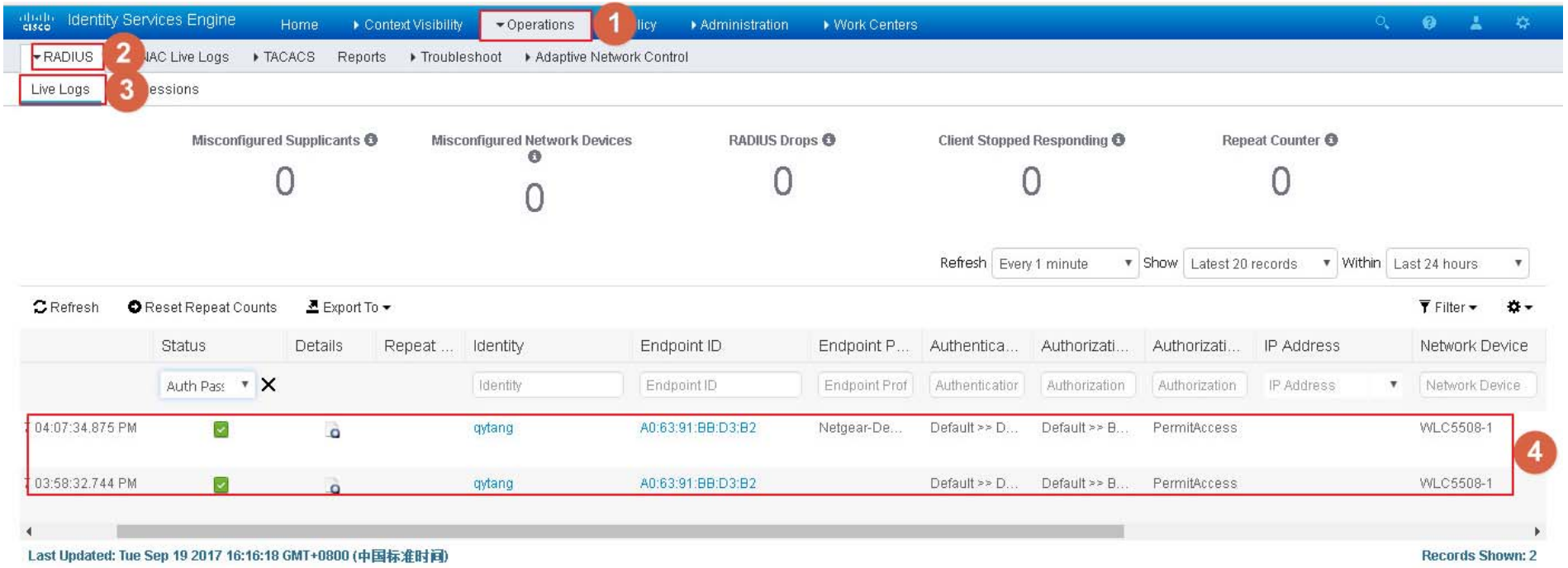
Performance Profile

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

查看实验现象

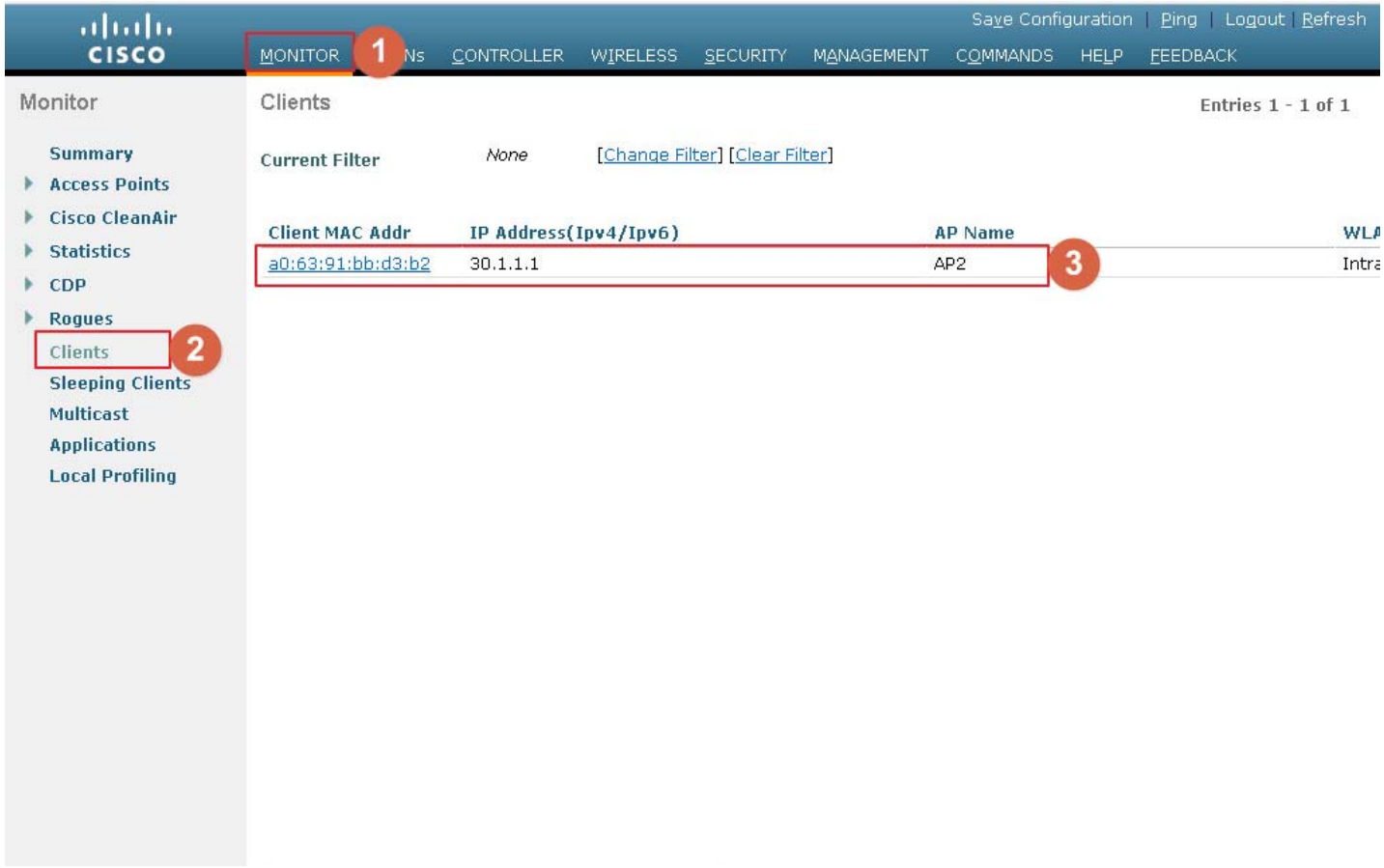
```
来自 10.1.1.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=15ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=13ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=10ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=254
请求超时。
来自 10.1.1.254 的回复: 字节=32 时间=24ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=11ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=19ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=39ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
```

查看ISE现象



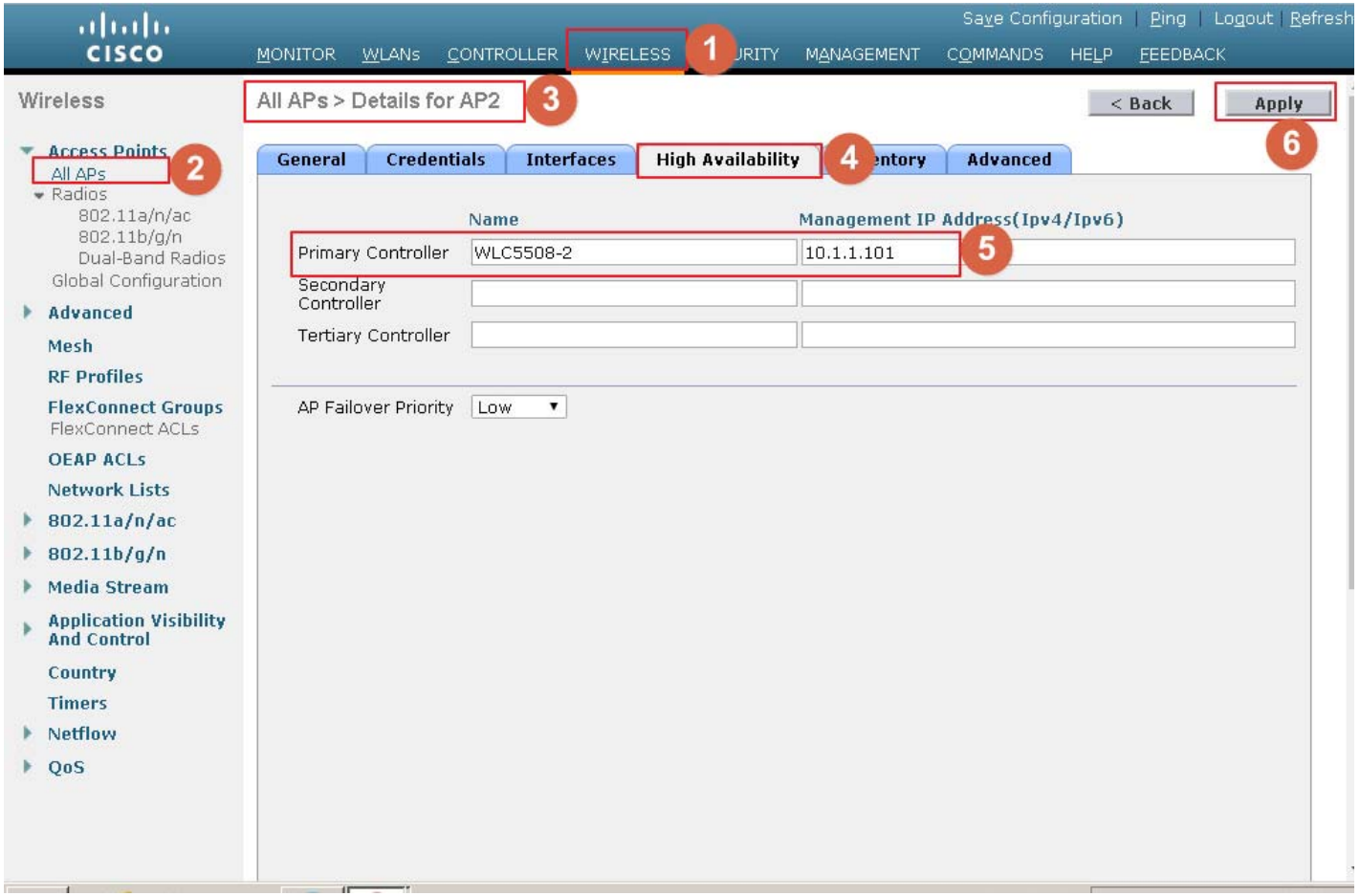
每一次漫游都会多一次认证信息

查看客户端关联AP

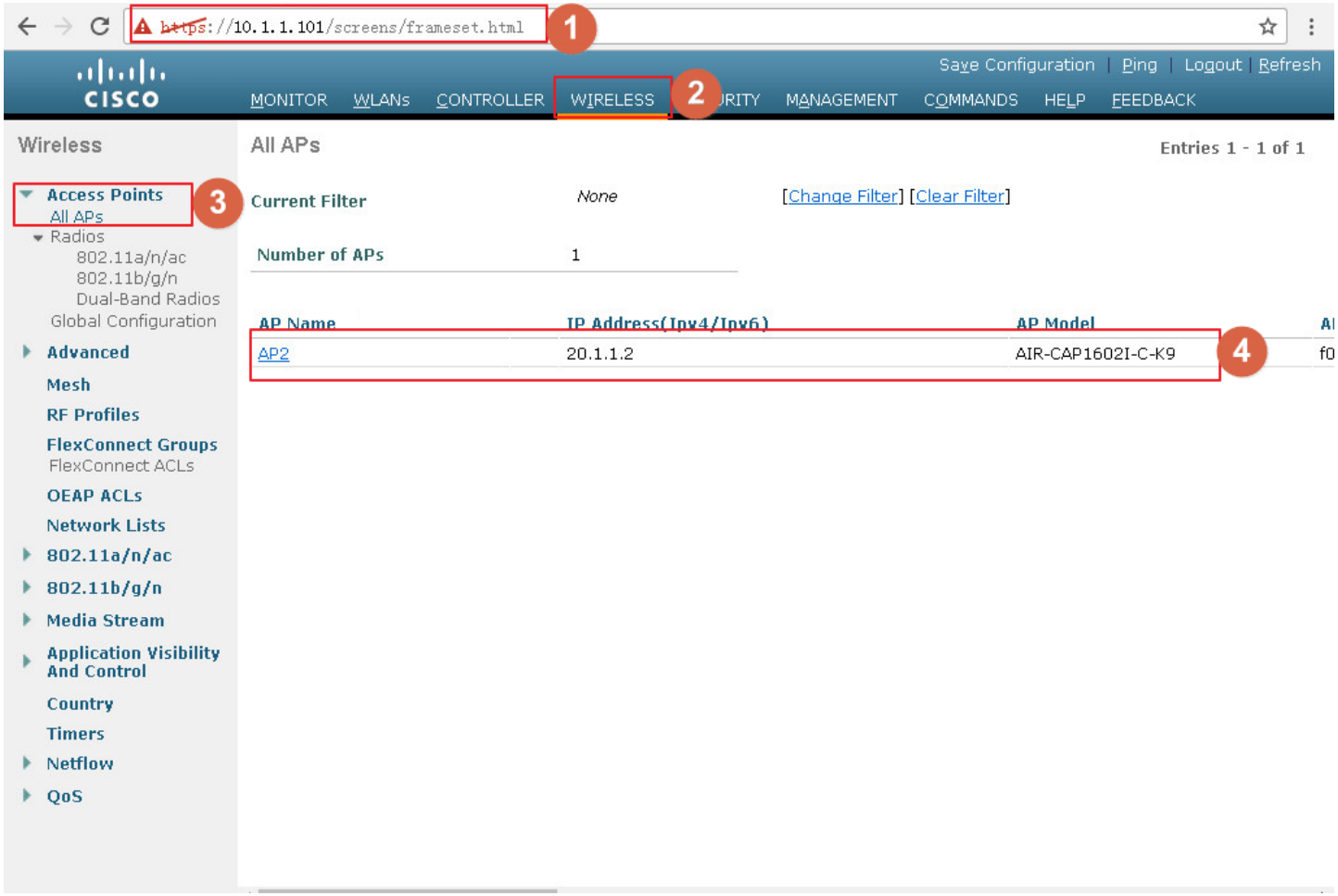

cisco
Save Configuration | Ping | Logout | Refresh
MONITOR
1
Ns
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
2
Sleeping Clients
Multicast
Applications
Local Profiling
Clients
Entries 1 - 1 of 1
Current Filter
None
[Change Filter] [Clear Filter]
Client MAC Addr
IP Address(Ipv4/Ipv6)
AP Name
WLA
a0:63:91:bb:d3:b2
30.1.1.1
AP2
3
Intra

第三部分
Inter-Controller Roaming

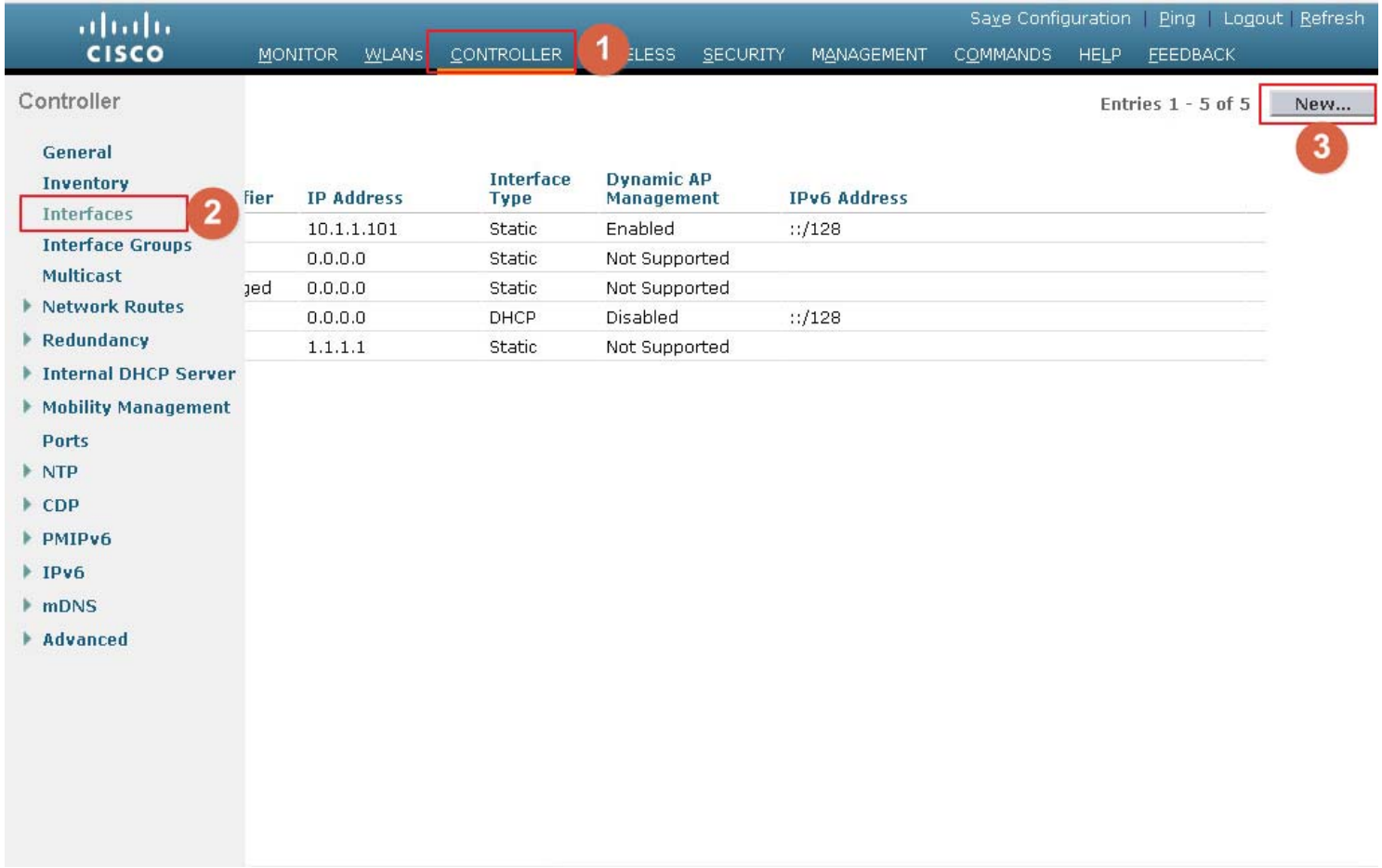
将AP2 关联WLC5508-2



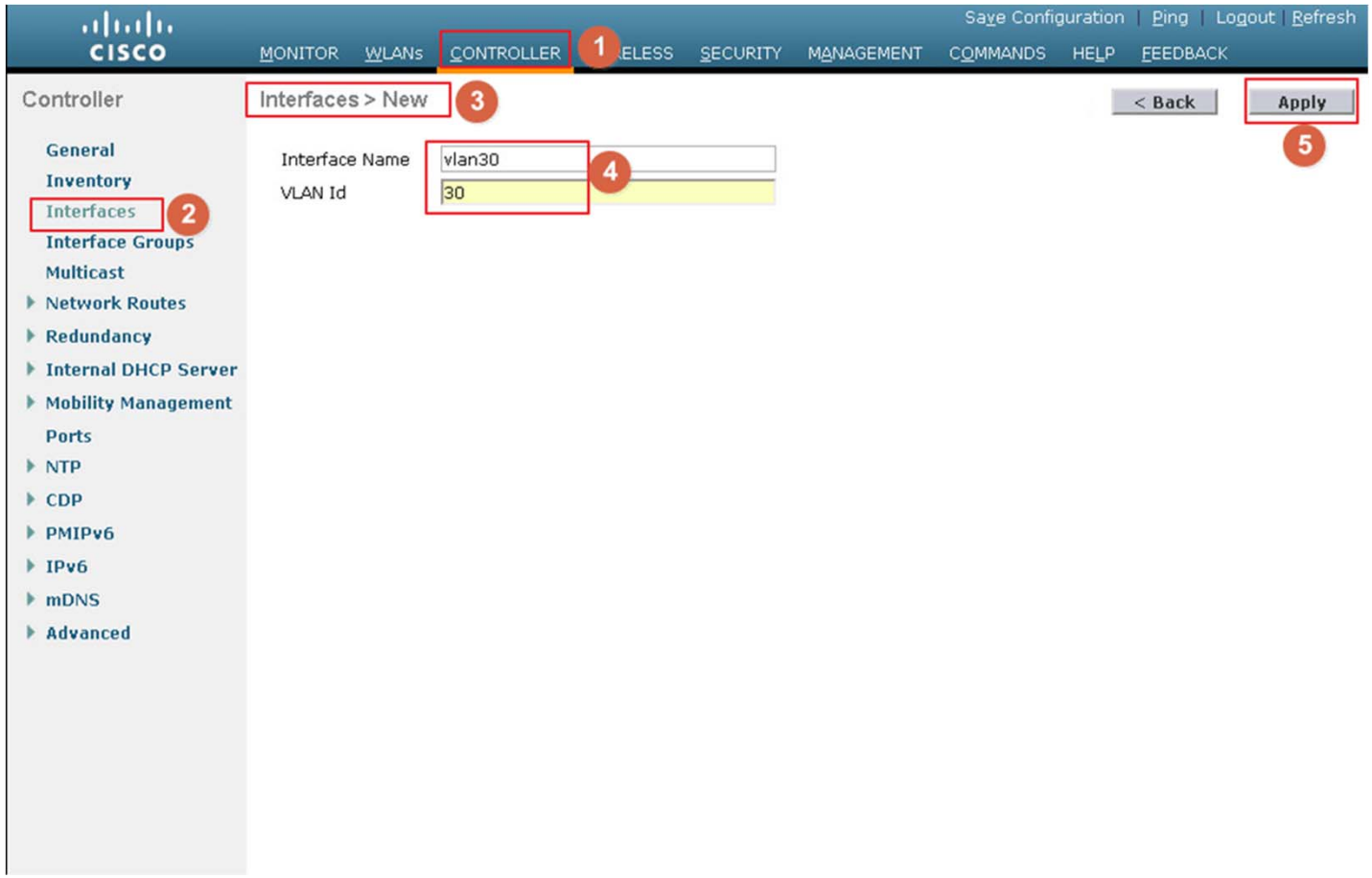
查看AP2 关联WLC5508-2



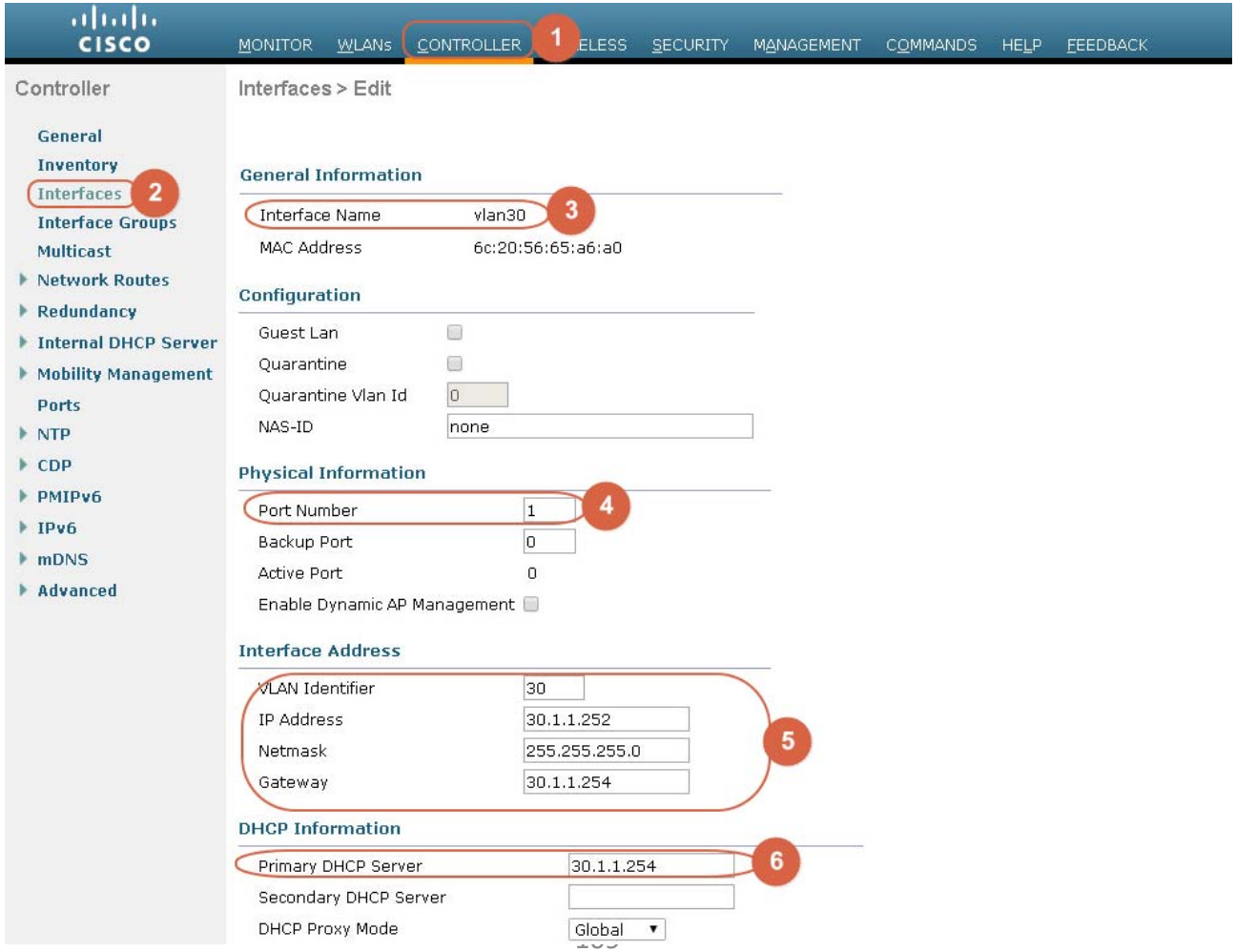
5508-2 创建动态接口



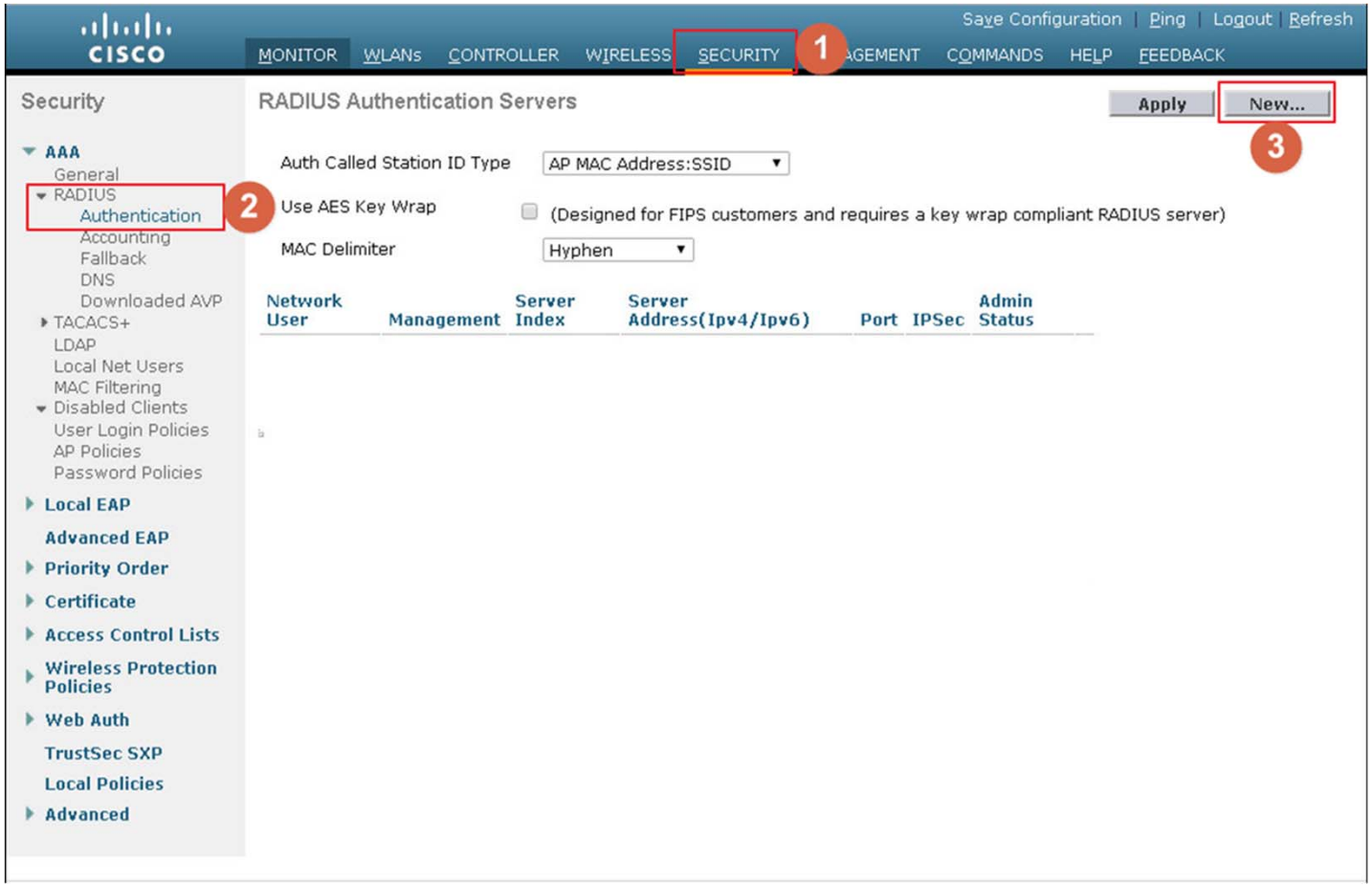
5508-2创建动态接口



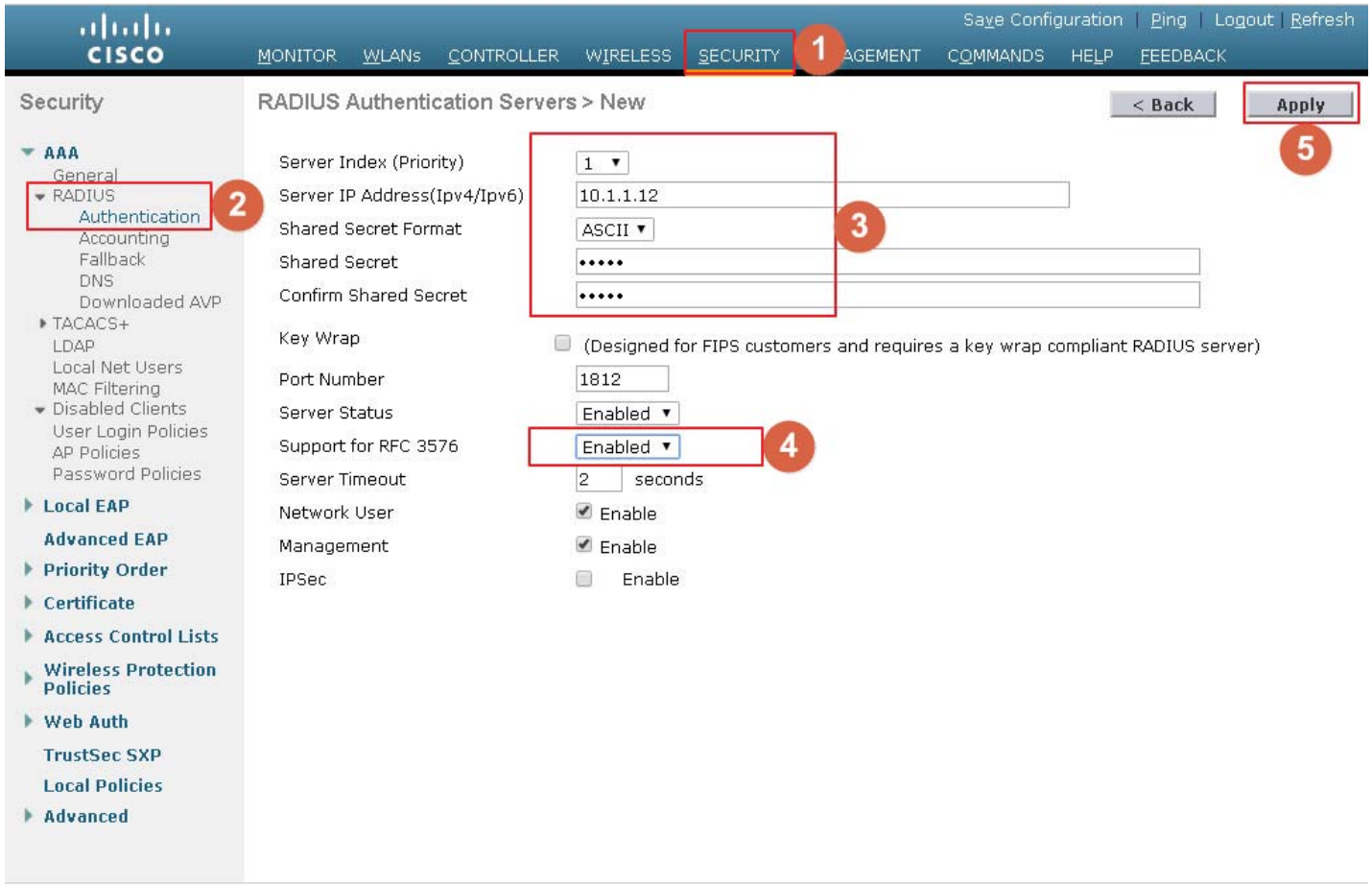
5508-2创建动态接口



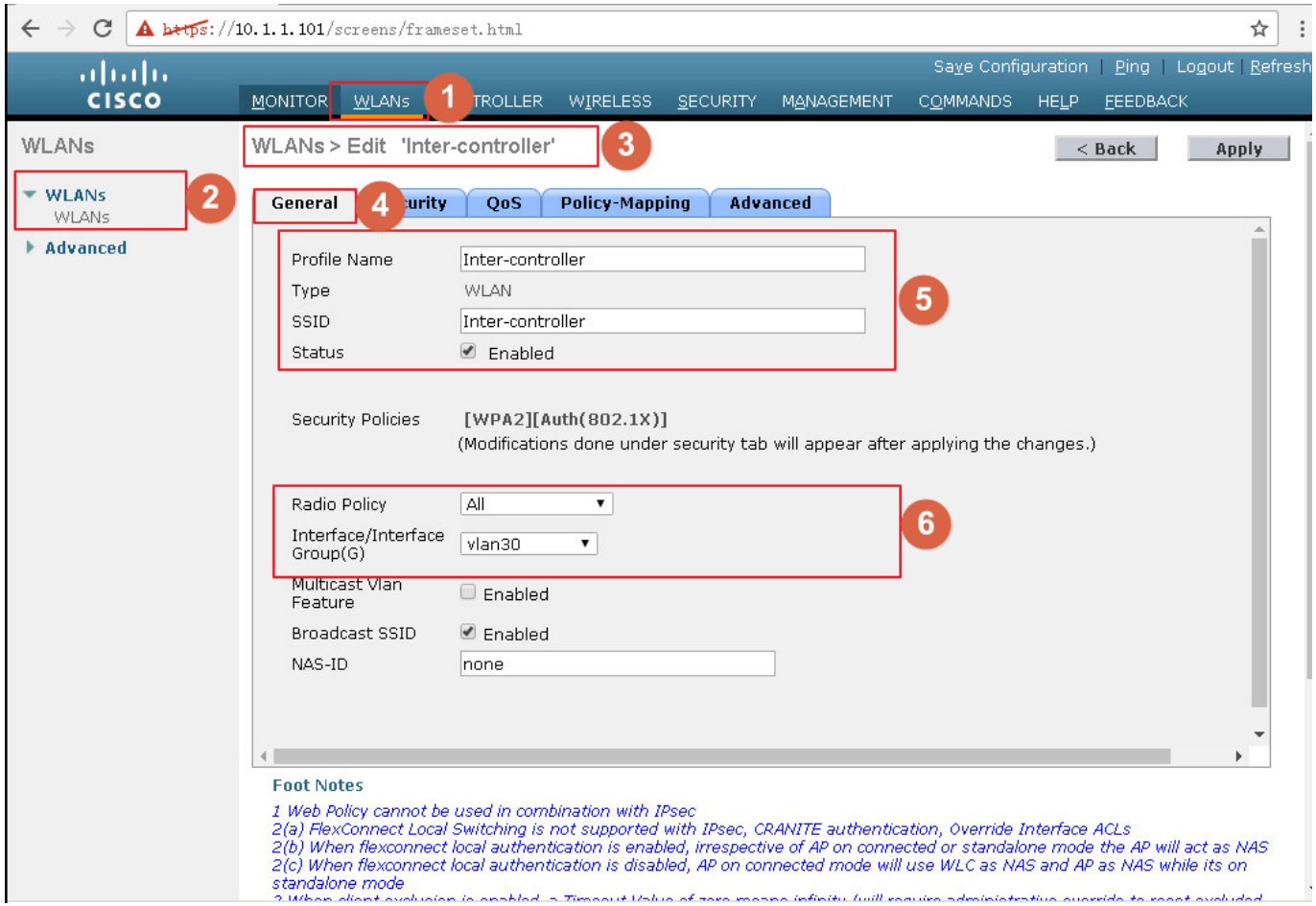
5508-2创建AAA


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY 1 AGEMENT COMMANDS HELP FEEDBACK
Security
RADIUS Authentication Servers
Apply
New...
3
AAA
General
RADIUS
Authentication
2
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec SXP
Local Policies
Advanced
Auth Called Station ID Type
AP MAC Address:SSID
Use AES Key Wrap
(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Delimiter
Hyphen
Network User
Management
Server Index
Server Address(Ipv4/Ipv6)
Port
IPSec
Admin Status

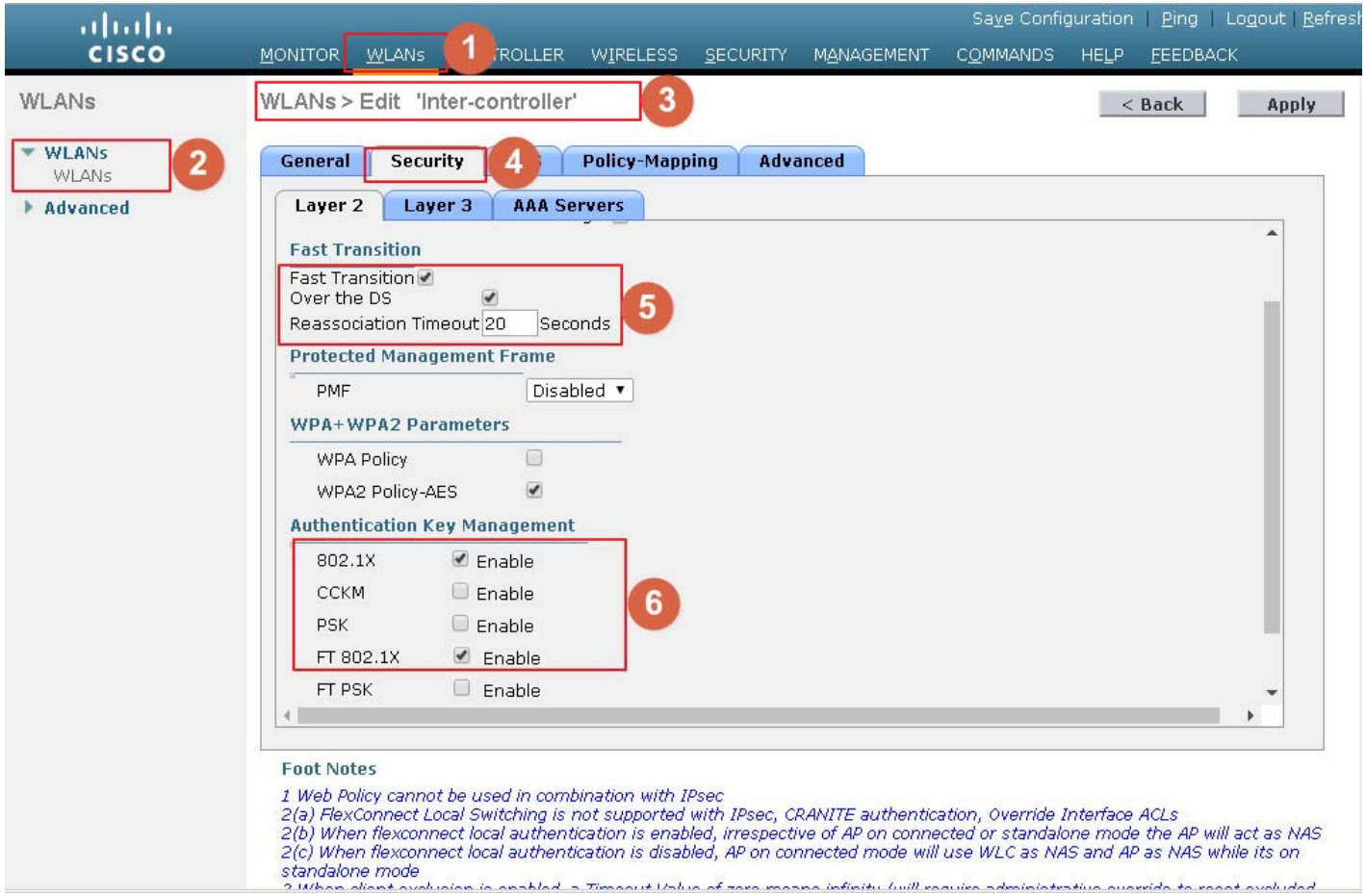
5508-2创建AAA


cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY 1 AGEMENT COMMANDS HELP FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec SXP
Local Policies
Advanced
2
RADIUS Authentication Servers > New
< Back
Apply
5
Server Index (Priority) 1
Server IP Address(Ipv4/Ipv6) 10.1.1.12
Shared Secret Format ASCII
Shared Secret
Confirm Shared Secret
3
Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number 1812
Server Status Enabled
Support for RFC 3576 Enabled
4
Server Timeout 2 seconds
Network User Enable
Management Enable
IPSec Enable

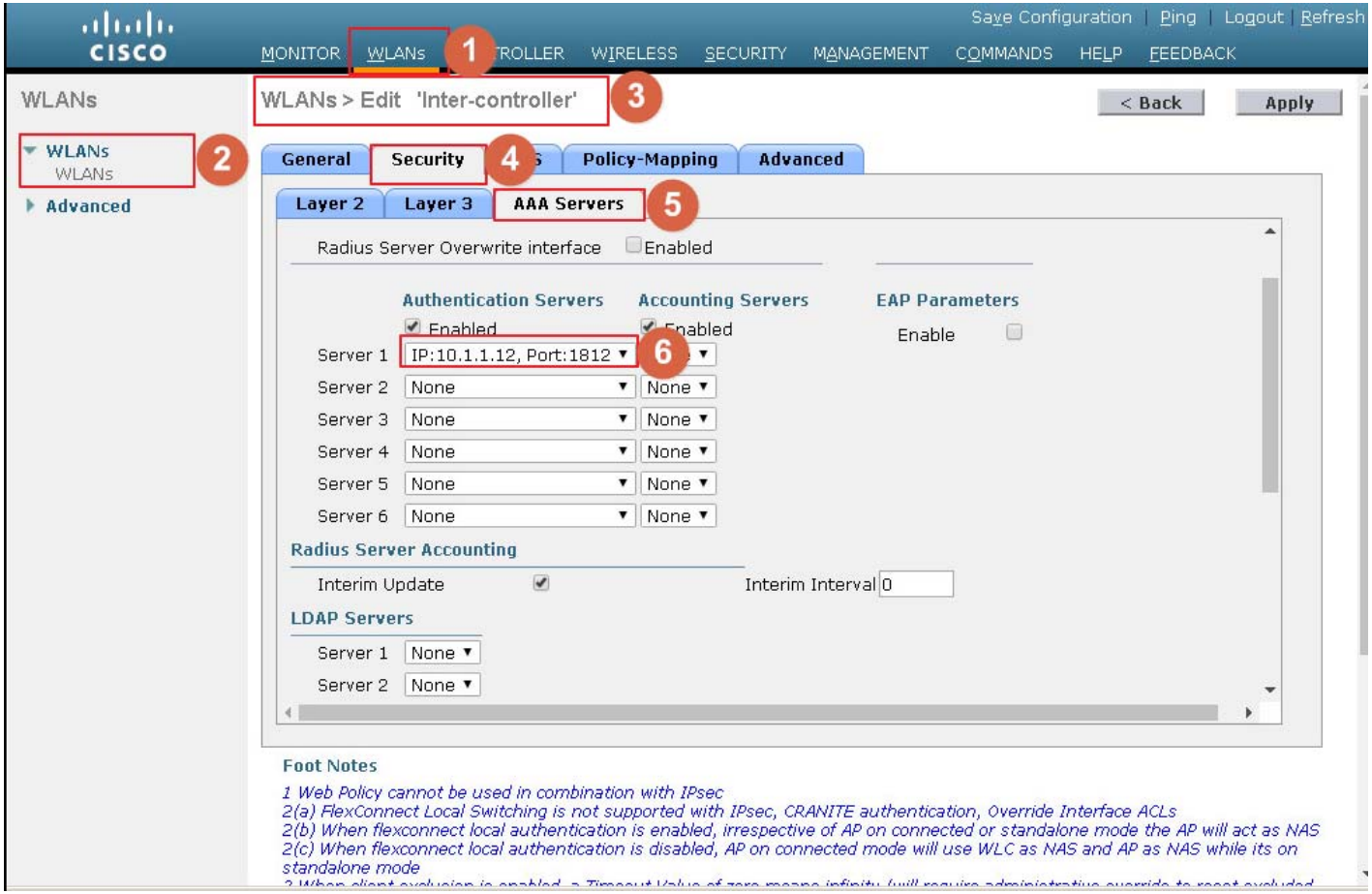
5508-2创建SSID



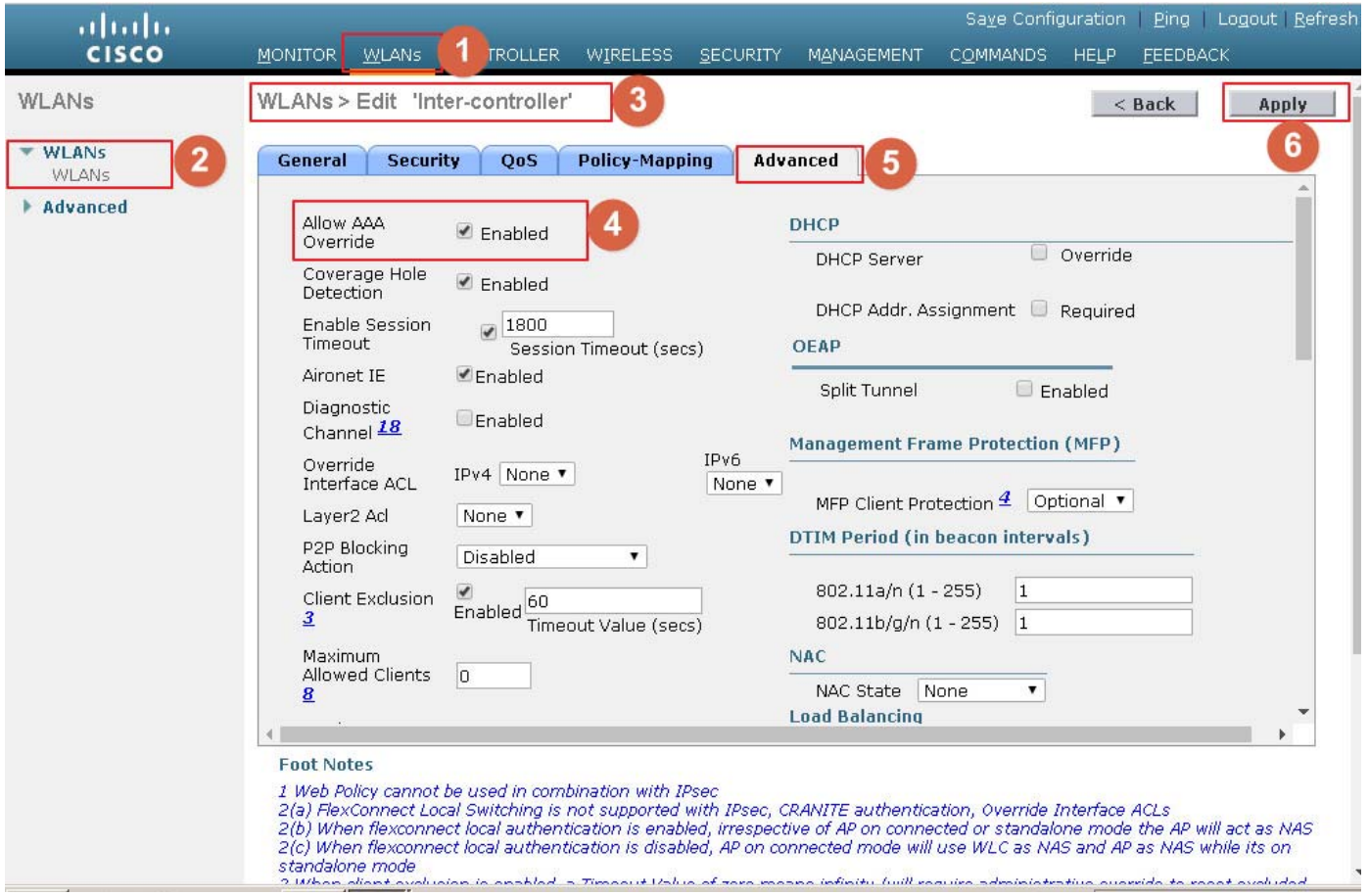
5508-2修改认证方式



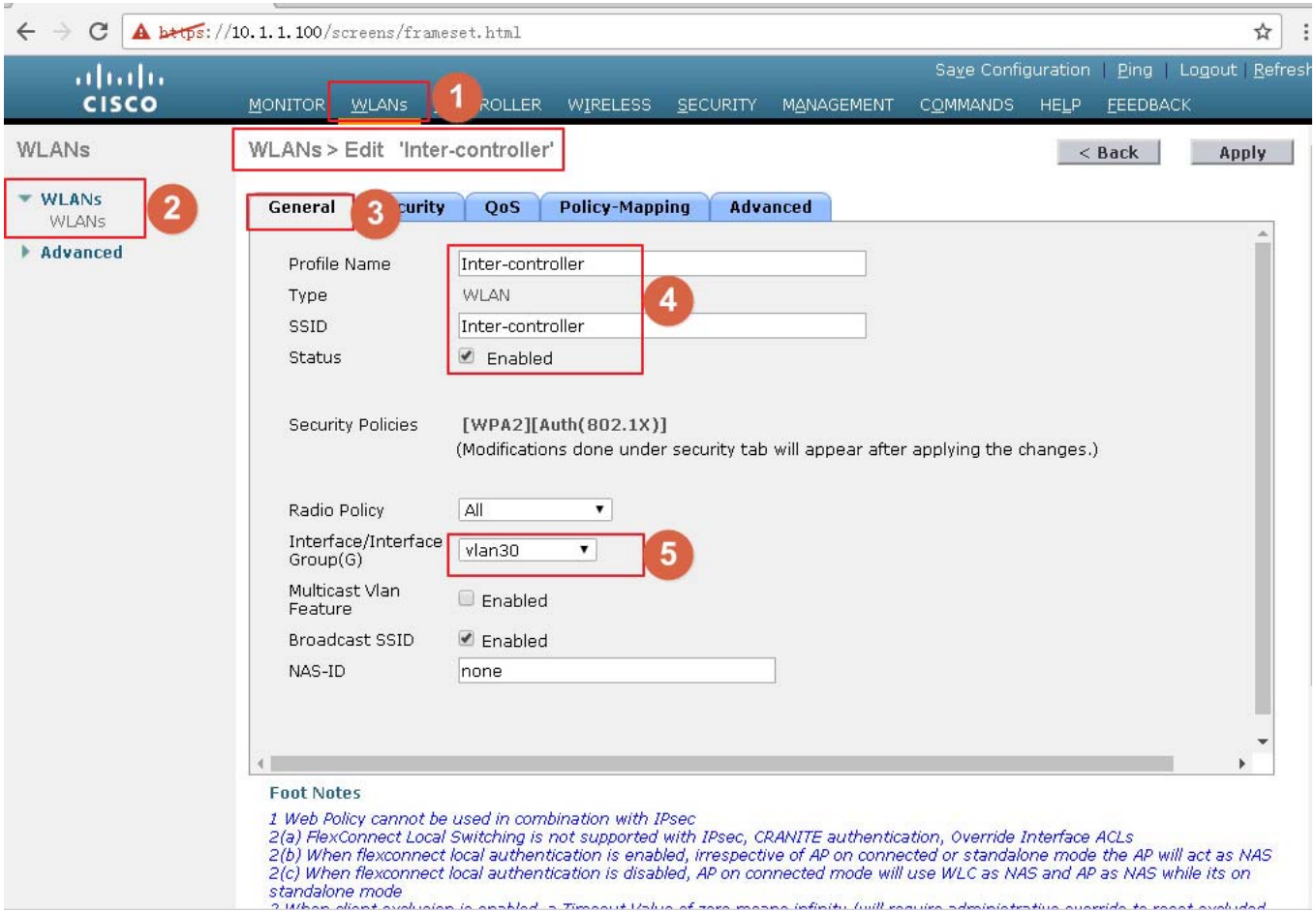
5508-2修改认证服务器



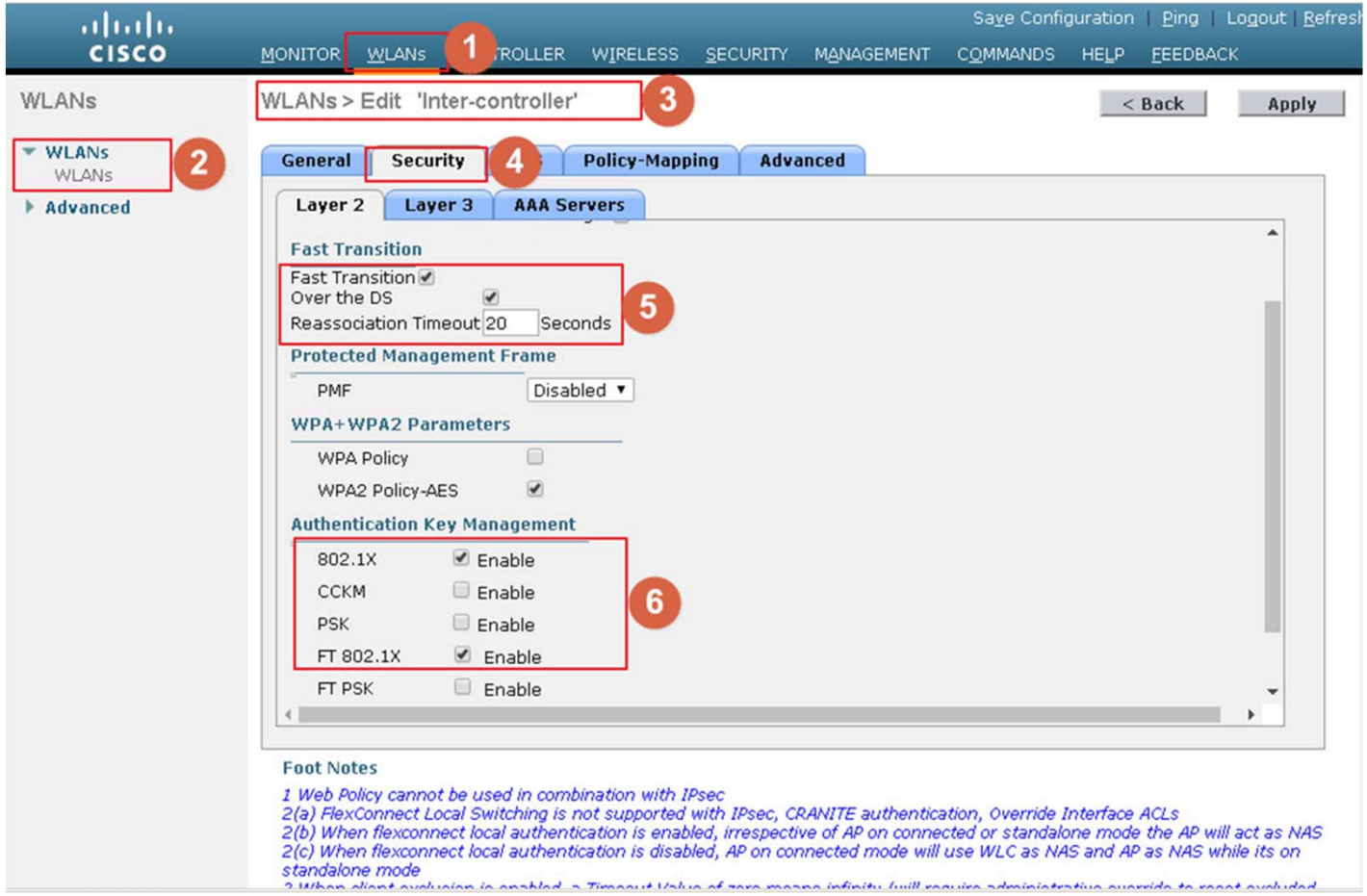
5508-2启用AAA-Override



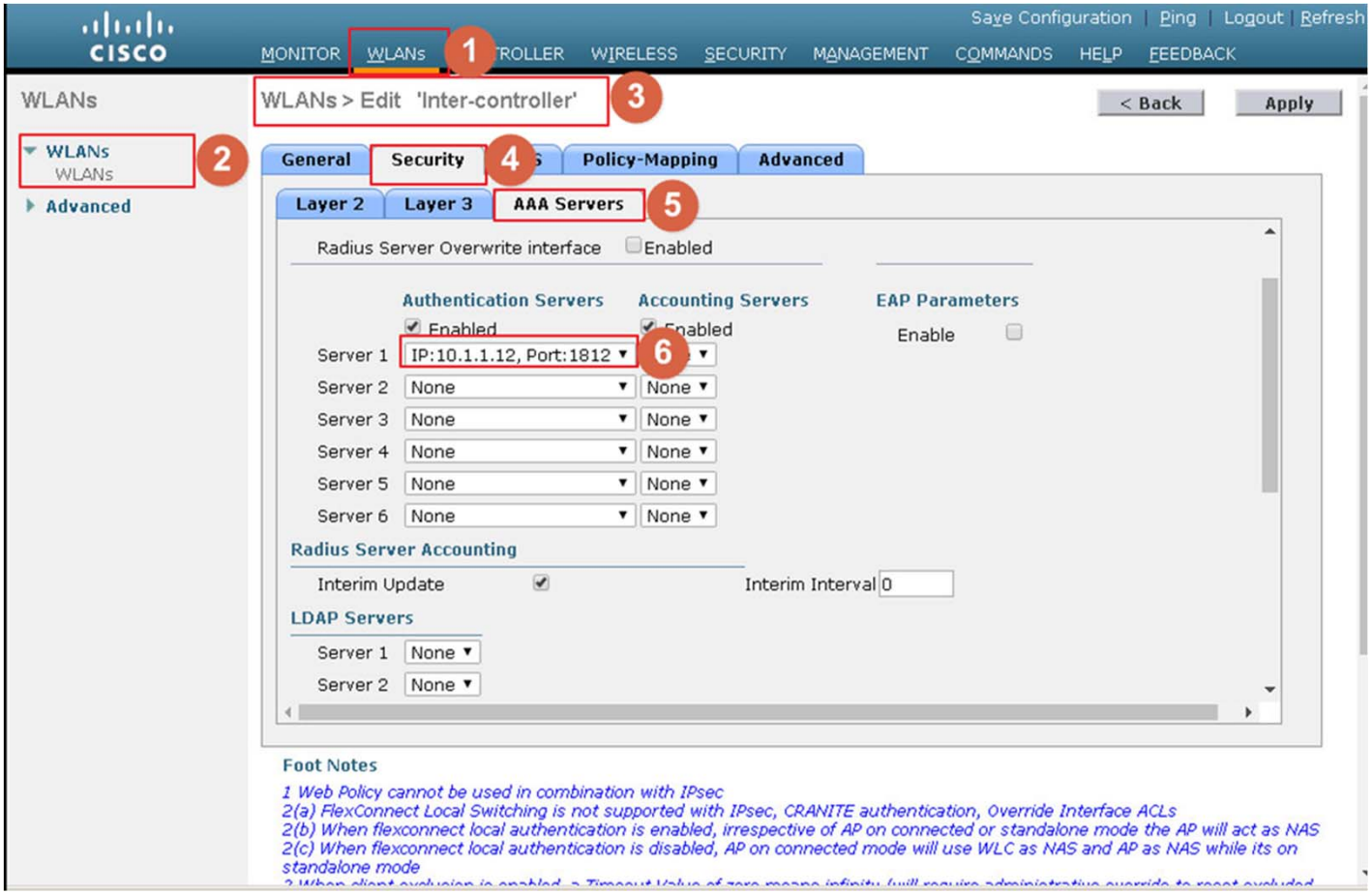
5508-1创建SSID



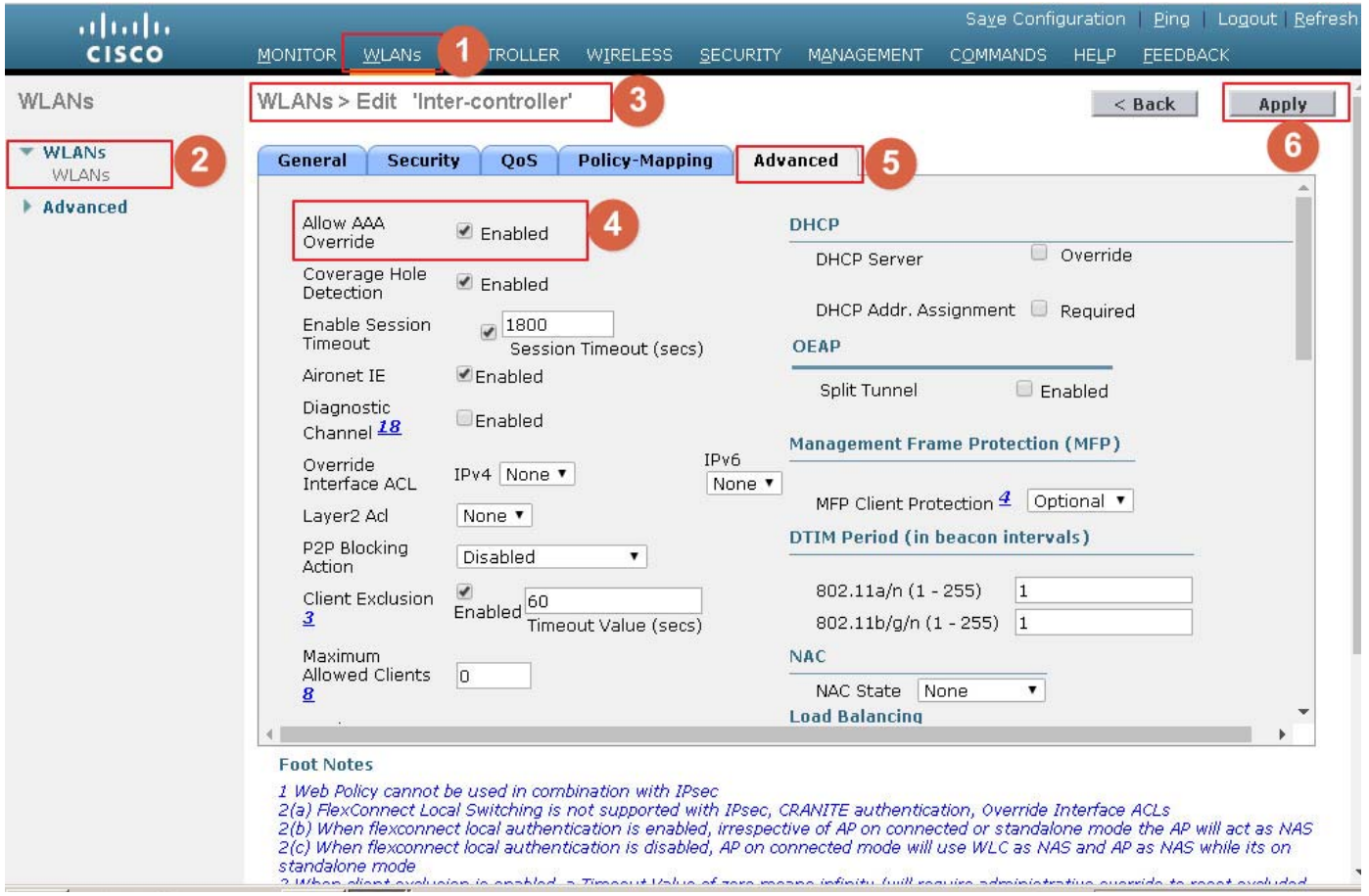
5508-1修改认证方式



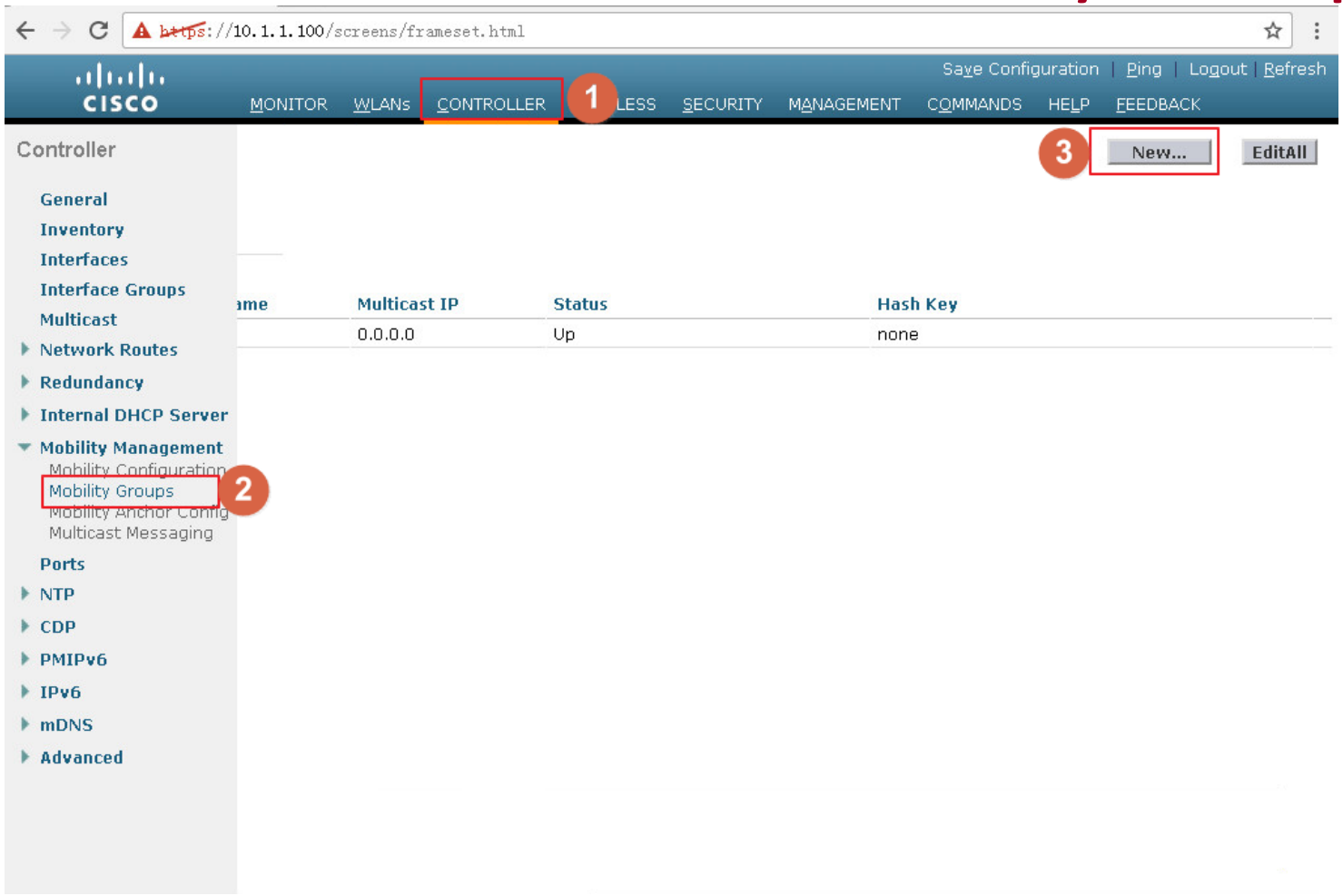
5508-1修改认证服务器



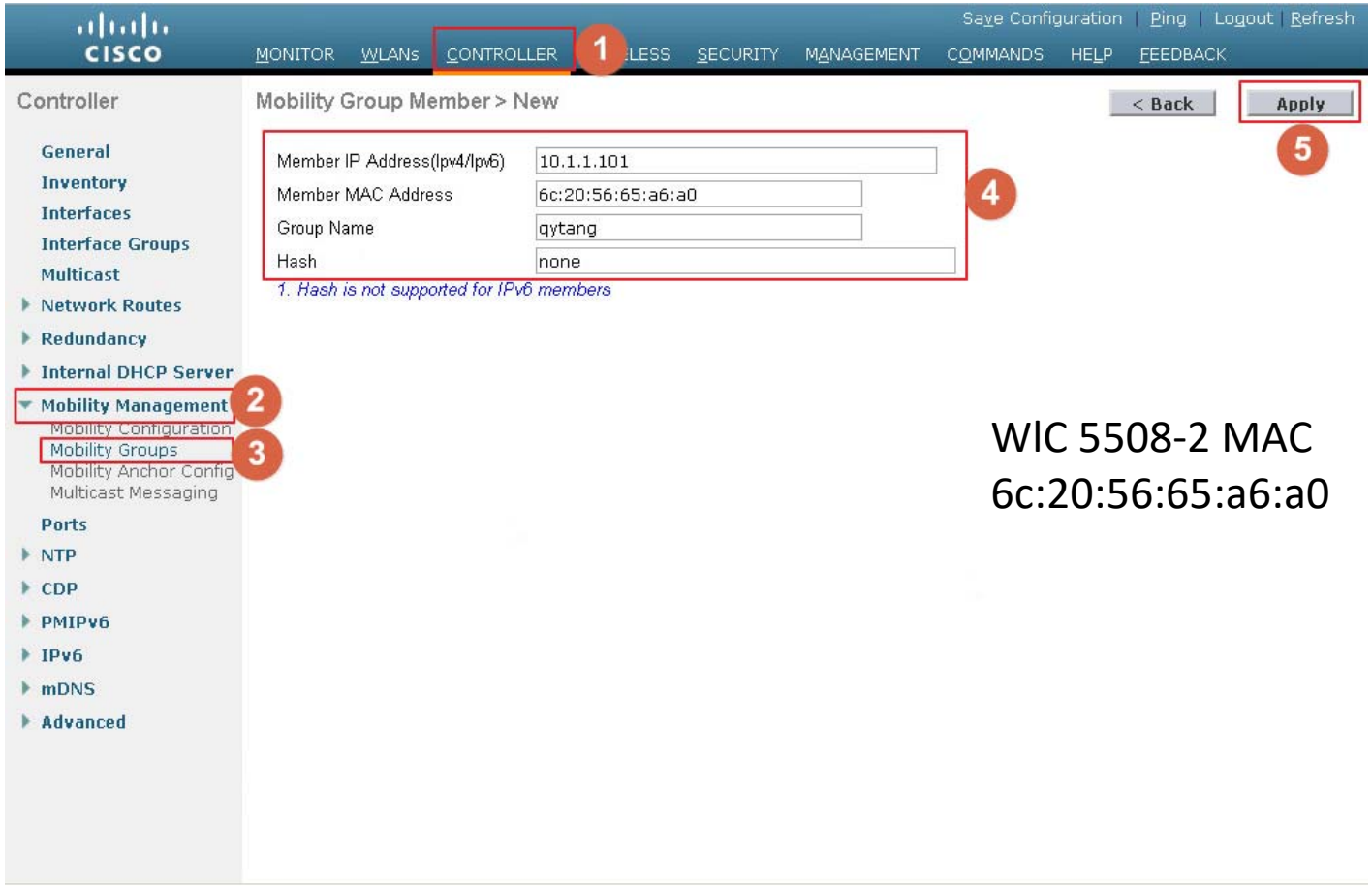
5508-1启用AAA-Override



5508-1添加5508-2到Mobility Group

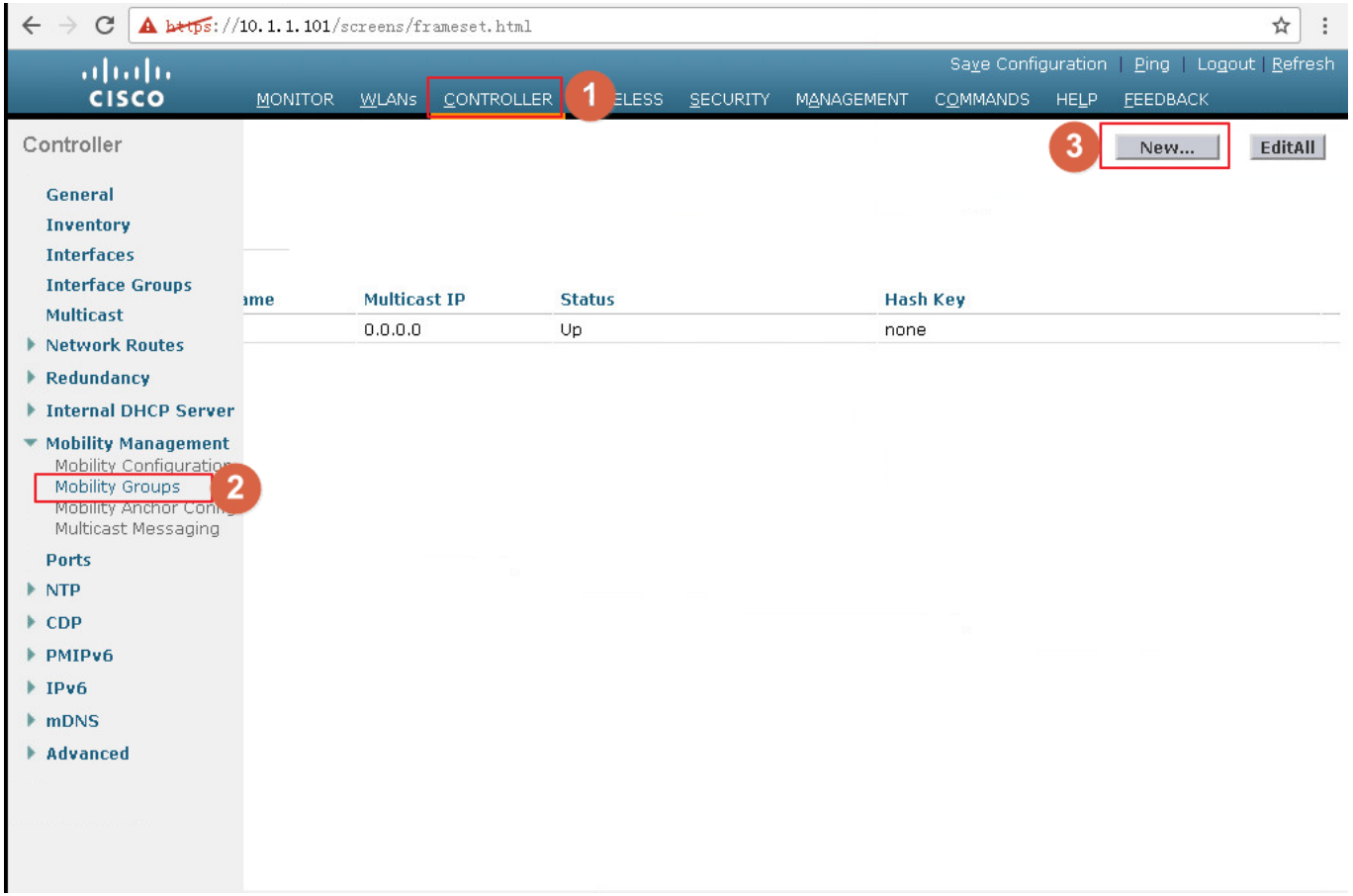


5508-1添加5508-2到Mobility Group

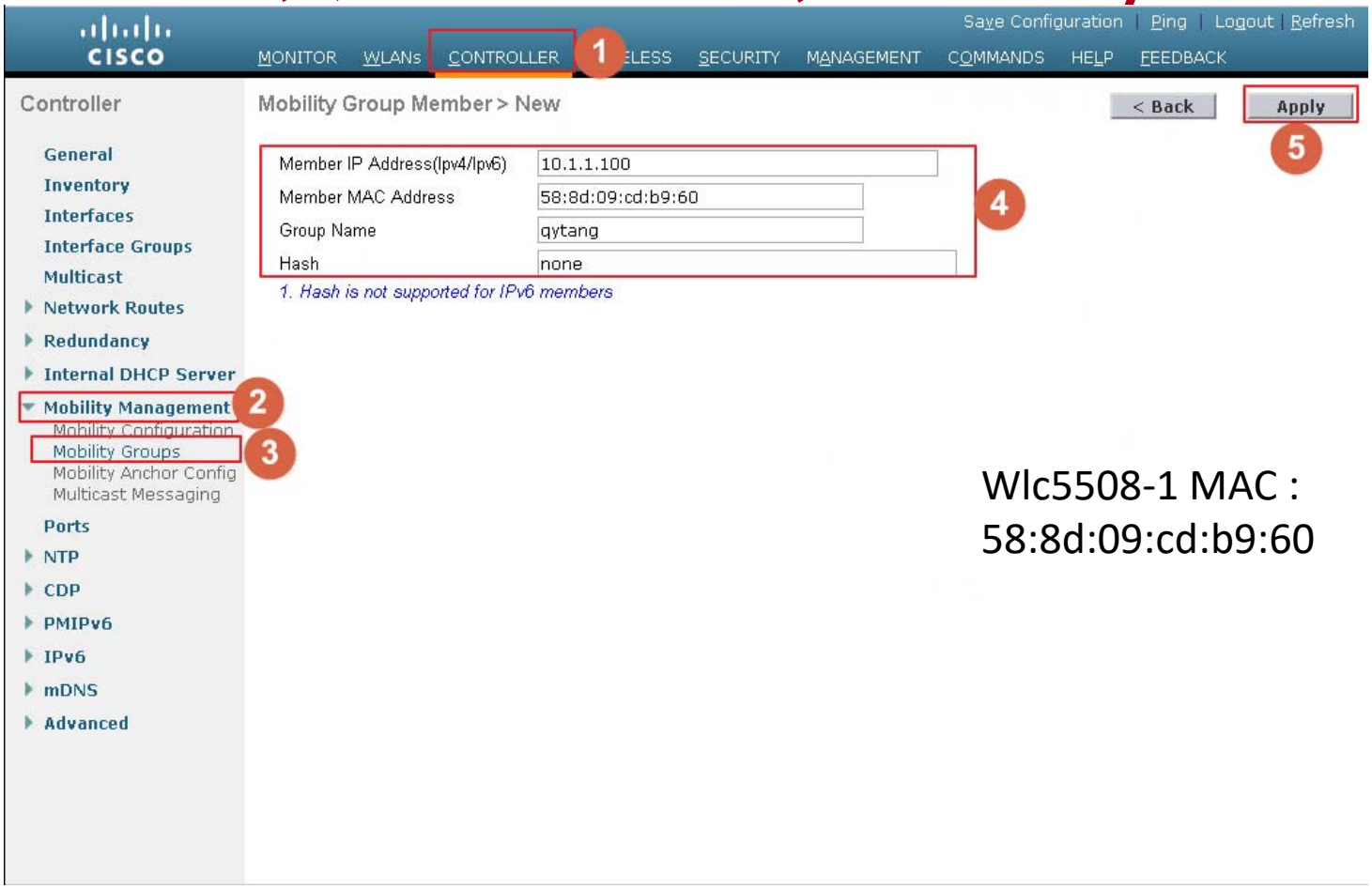


WlC 5508-2 MAC
6c:20:56:65:a6:a0

5508-2添加5508-1到Mobility Group



5508-2添加5508-1到Mobility Group



Wlc5508-1 MAC :
58:8d:09:cd:b9:60

5508-1查看mobility list状态

严重注意一定要查看状态为“UP”

数据层面为IP 97
控制层面为UDP/16666

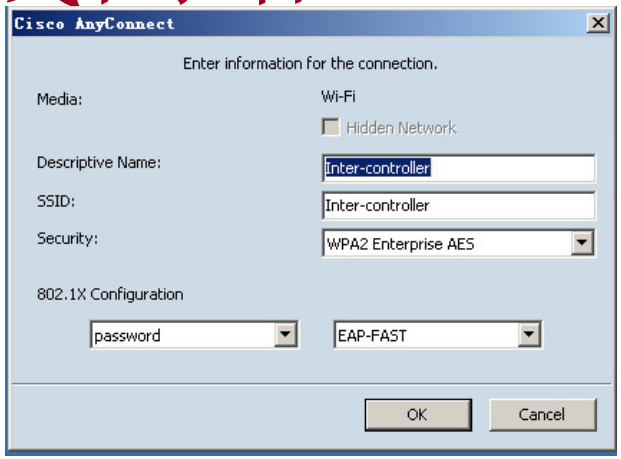
5508-2查看mobility list状态

严重注意一定要查看状态为“UP”

Ping测试

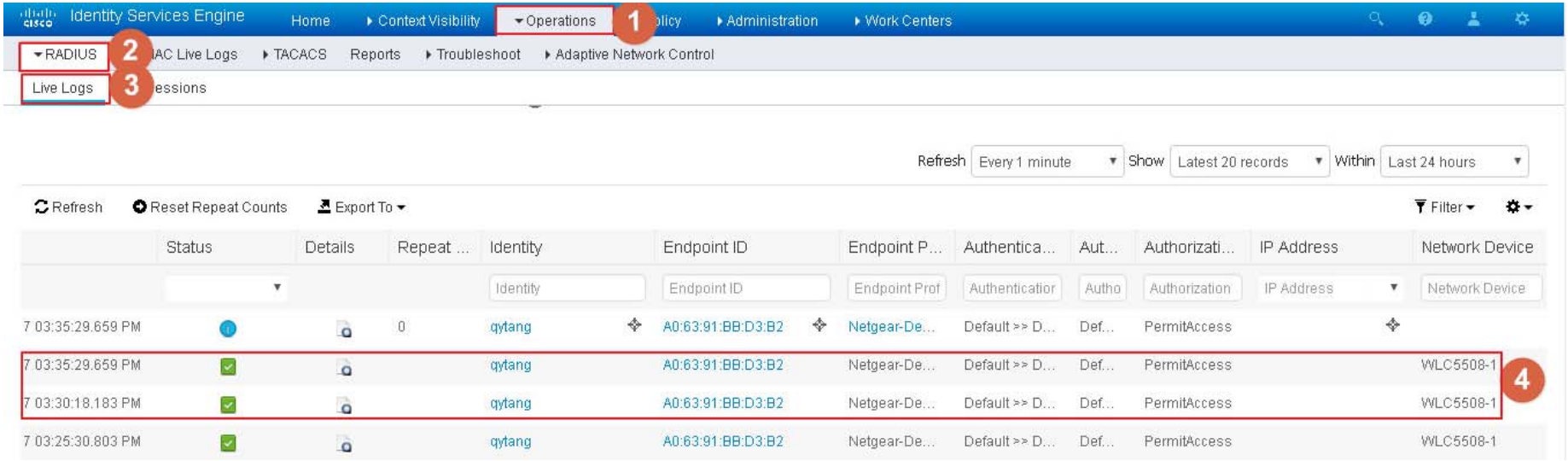

CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Mobility Configuration
Mobility Groups
Mobility Anchor Config
Multicast Messaging
Ports
NTP
CDP
PMIPv6
IPv6
mDNS
Advanced
New...
EditAll
v4/Ipv6)
Group Name
Multicast IP
Status
Hash Key
qytang
0.0.0.0
Up
none
qytang
0.0.0.0
Up
none
Remove
Ping
10.1.1.101 显示:
Reply received from Mobility Peer 10.1.1.100 : (send count = 3, receive count = 3)
禁止此页再显示对话框。
确定

Test-PC连接无线网络



用户名：**qytang**
密码：**Cisc0123**

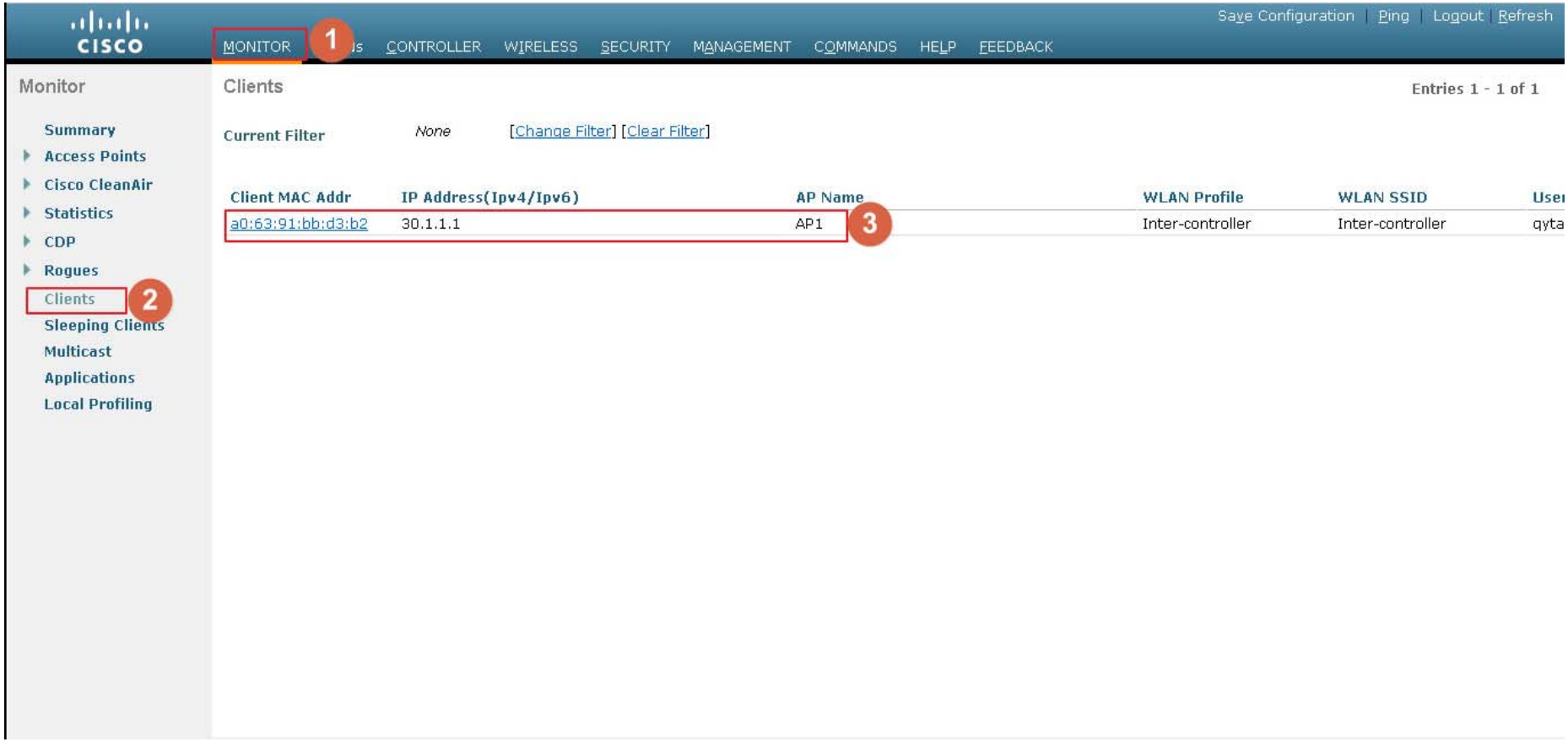
查看ISE认证


Identity Services Engine
Home
Context Visibility
Operations
1
Administration
Work Centers
RADIUS
2
TACACS
Reports
Troubleshoot
Adaptive Network Control
Live Logs
3
Refresh
Every 1 minute
Show
Latest 20 records
Within
Last 24 hours
Refresh
Reset Repeat Counts
Export To
Filter
Status
Details
Repeat ...
Identity
Endpoint ID
Endpoint P...
Authentica...
Aut...
Authorizati...
IP Address
Network Device
7 03:35:29.659 PM
0
qytang
A0:63:91:BB:D3:B2
Netgear-De...
Default >> D...
Def...
PermitAccess
7 03:35:29.659 PM
qytang
A0:63:91:BB:D3:B2
Netgear-De...
Default >> D...
Def...
PermitAccess
WLC5508-1
4
7 03:30:18.183 PM
qytang
A0:63:91:BB:D3:B2
Netgear-De...
Default >> D...
Def...
PermitAccess
WLC5508-1
7 03:25:30.803 PM
qytang
A0:63:91:BB:D3:B2
Netgear-De...
Default >> D...
Def...
PermitAccess
WLC5508-1

测试漫游

```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>
C:\Users\Administrator>ping 10.1.1.254 -t

正在 Ping 10.1.1.254 具有 32 字节的数据:
来自 10.1.1.254 的回复: 字节=32 时间=12ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=10ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
```

查看客户端关联AP


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
1
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
2
Sleeping Clients
Multicast
Applications
Local Profiling
Clients
Entries 1 - 1 of 1
Current Filter
None
[Change Filter] [Clear Filter]
Client MAC Addr
IP Address(Ipv4/Ipv6)
AP Name
WLAN Profile
WLAN SSID
User
a0:63:91:bb:d3:b2
30.1.1.1
AP1
3
Inter-controller
Inter-controller
qyta

天线与型号强度调整

802.11a/n Cisco APs > Configure

General

AP Name	AP2
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☐ C ☐

RF Channel Assignment

Current Channel	161
Channel Width *	20 MHz

** Channel width can be configured only when channel configuration is in custom mode*

Assignment Method	Global / Custom

Tx Power Level Assignment

Current Tx Power Level	6
Assignment Method	Global / Custom 6

Performance Profile

View and edit Performance Profile for this AP

Performance Profile

Note: Changing any of the parameters causes … disabled and thus may result in loss of connect

送出端

信号调整到最小（6）
天线只留A

接收端

信号调整到最大（1）
天线A B C全部打开

802.11a/n Cisco APs > Configure

General

AP Name	AP1
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel	149
Channel Width *	20 MHz

** Channel width can be configured only when channel configuration is in custom mode*

Assignment Method	Global / Custom

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	Global / Custom 1

Performance Profile

View and edit Performance Profile for this AP

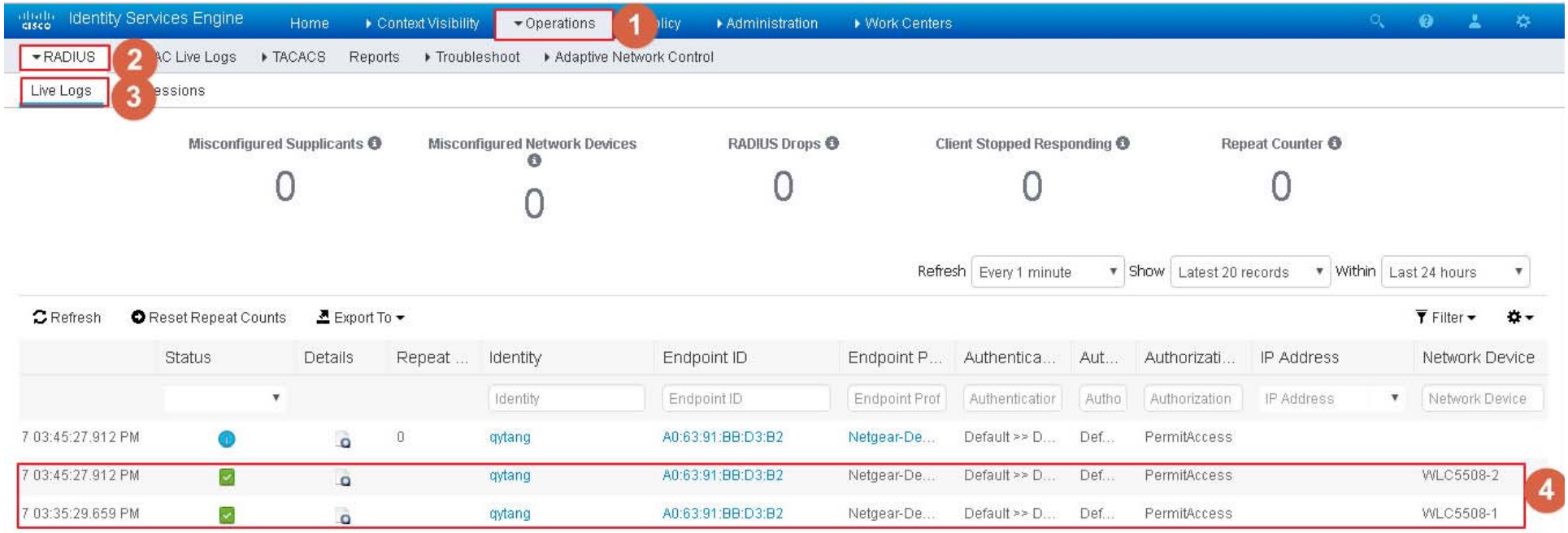
Performance Profile

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

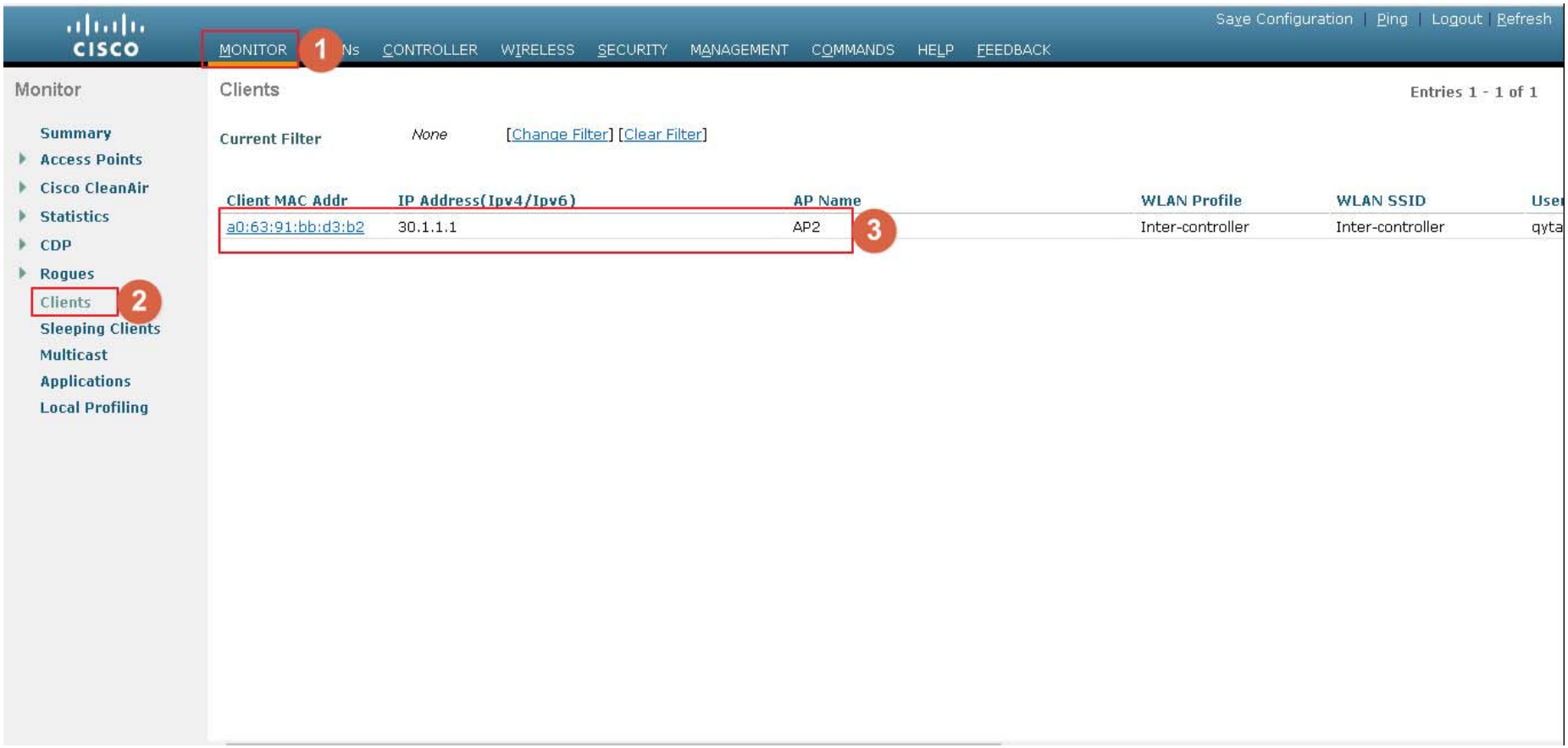
查看漫游现象

```
来自 10.1.1.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=10ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=7ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=9ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=15ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=8ms TTL=254
请求超时。
来自 10.1.1.254 的回复: 字节=32 时间=25ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=39ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=6ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=10ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=14ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=8ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=18ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=33ms TTL=254
来自 10.1.1.254 的回复: 字节=32 时间=18ms TTL=254
```

查看ISE现象

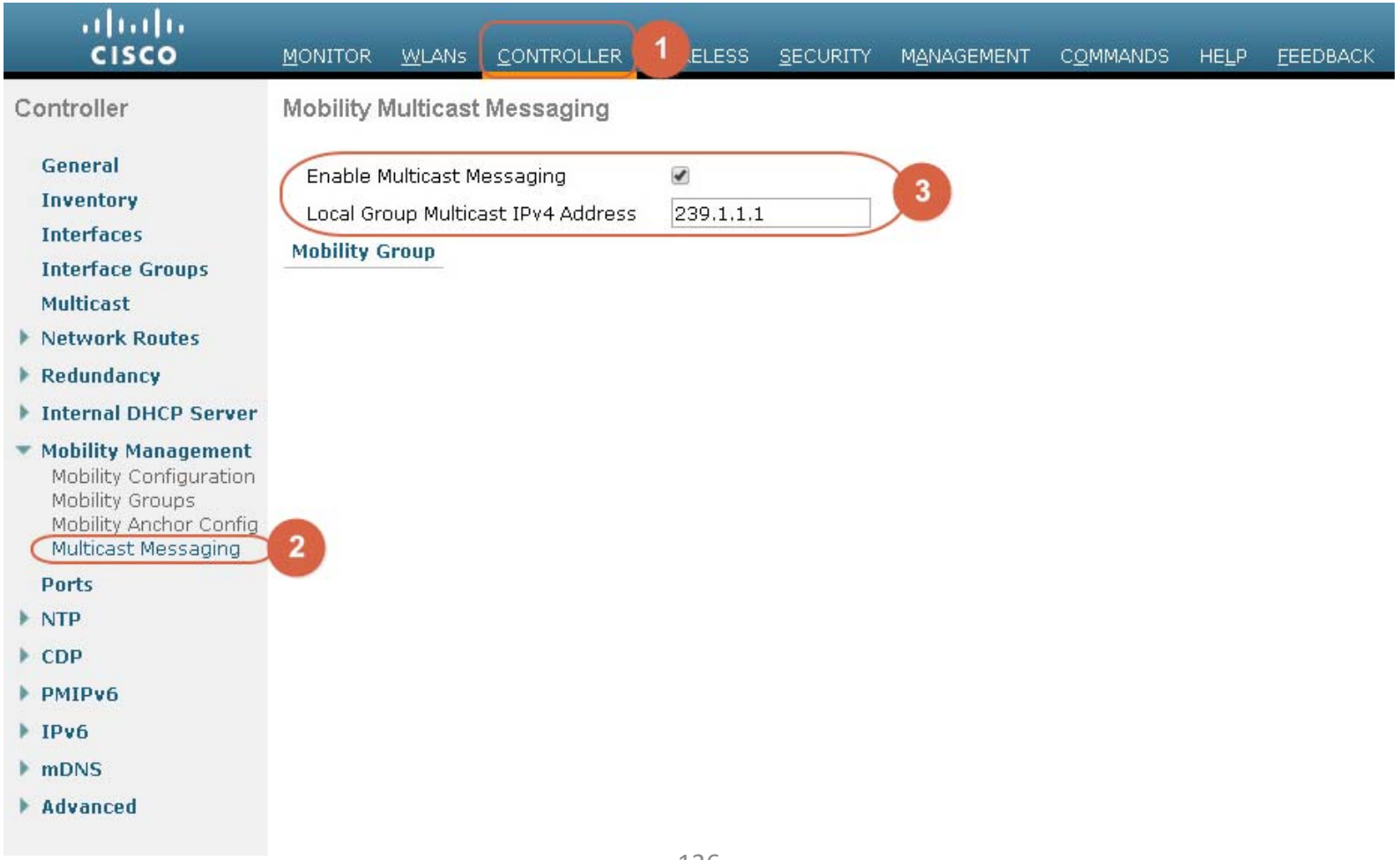

Identity Services Engine
Home
Context Visibility
Operations
Administration
Work Centers
RADIUS
TACACS
Reports
Troubleshoot
Adaptive Network Control
Live Logs
Misconfigured Supplicants
Misconfigured Network Devices
RADIUS Drops
Client Stopped Responding
Repeat Counter
0
Refresh
Every 1 minute
Show
Latest 20 records
Within
Last 24 hours
Reset Repeat Counts
Export To
Filter
Status
Details
Repeat ...
Identity
Endpoint ID
Endpoint P...
Authentica...
Aut...
Authorizati...
IP Address
Network Device
7 03:45:27.912 PM
qytang
A0:63:91:BB:D3:B2
Netgear-De...
Default >> D...
Def...
PermitAccess
WLC5508-2
7 03:35:29.659 PM
WLC5508-1
1
2
3
4

查看WLC5508-2

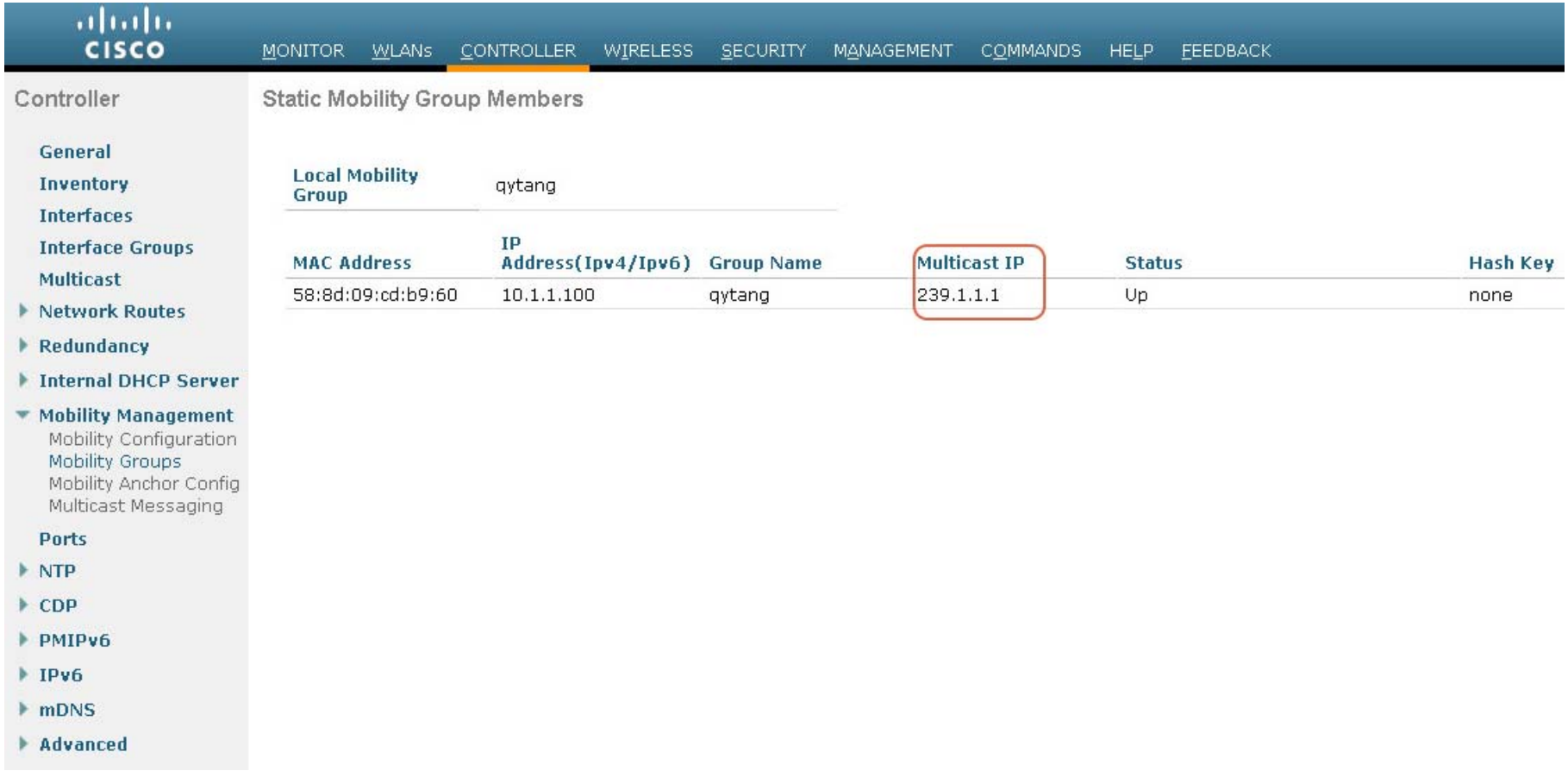

cisco
Save Configuration | Ping | Logout | Refresh
MONITOR
1
Ns
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
2
Sleeping Clients
Multicast
Applications
Local Profiling
Clients
Entries 1 - 1 of 1
Current Filter
None
[Change Filter] [Clear Filter]
Client MAC Addr
IP Address(Ipv4/Ipv6)
AP Name
WLAN Profile
WLAN SSID
a0:63:91:bb:d3:b2
30.1.1.1
AP2
3
Inter-controller
Inter-controller

3.1
组播漫游消息

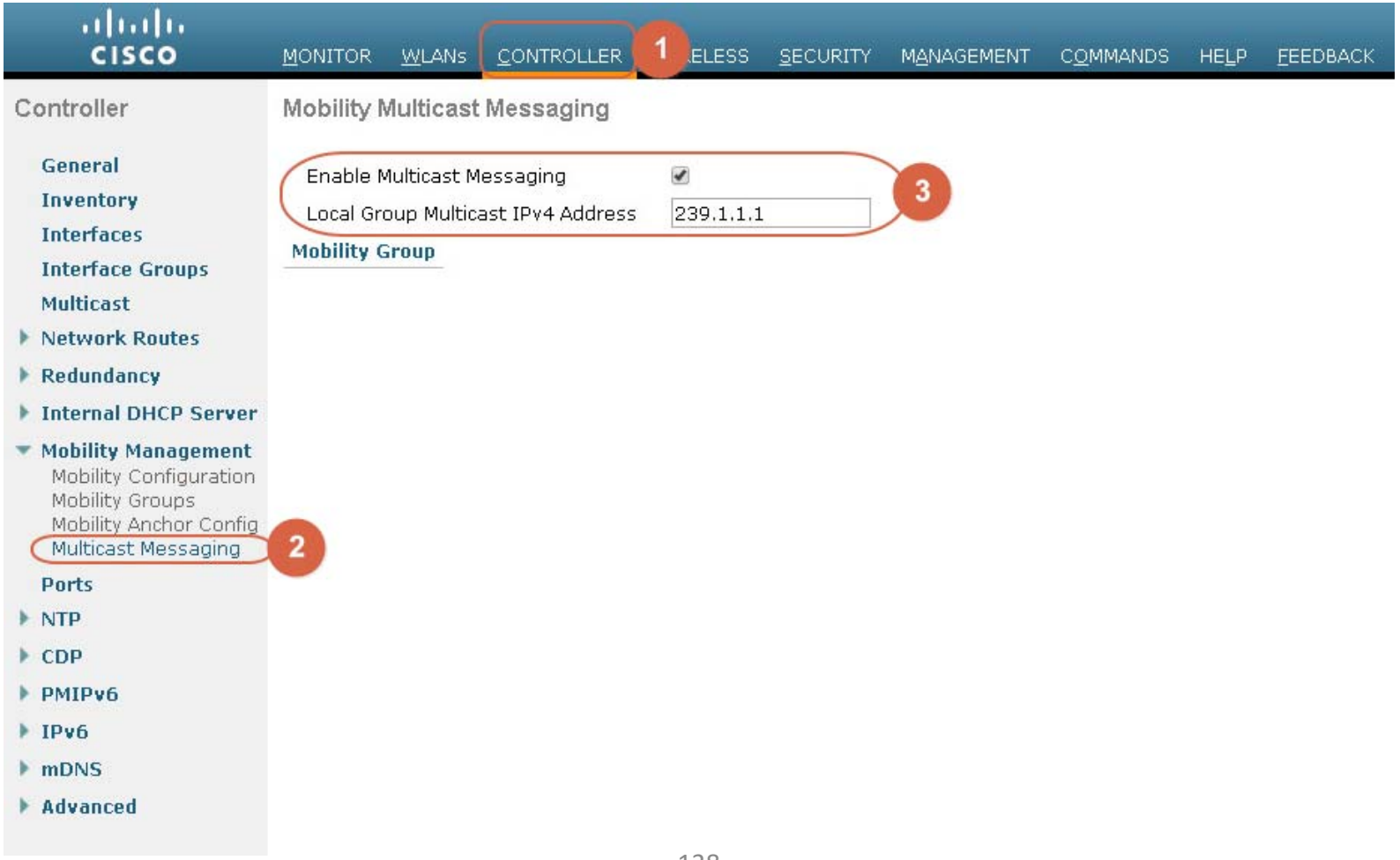
WLC5508-1配置组播消息



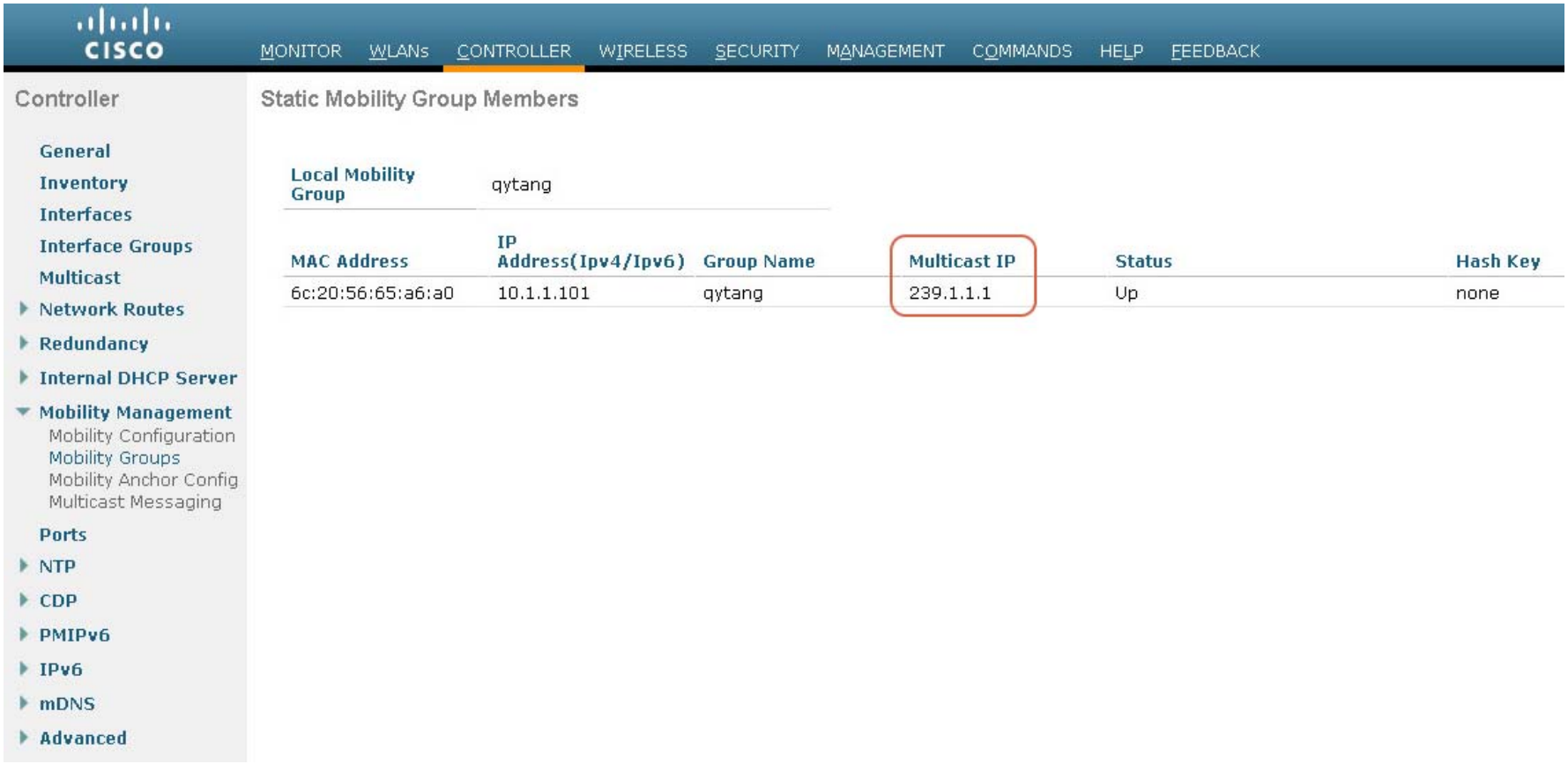
WLC5508-1删除单播配置



WLC5508-2配置组播消息



WLC5508-2删除单播配置



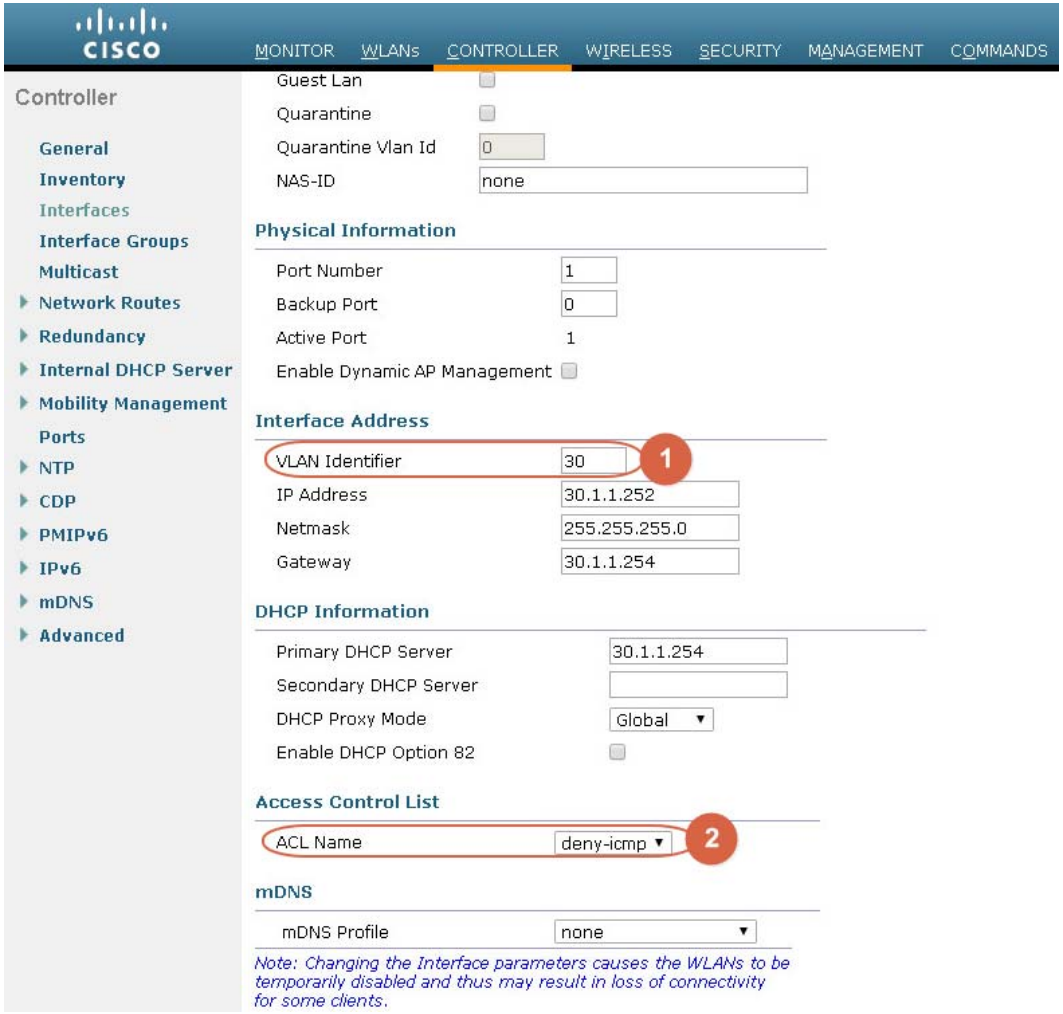
3.2
锚测试

测试默认没有锚的漫游效果

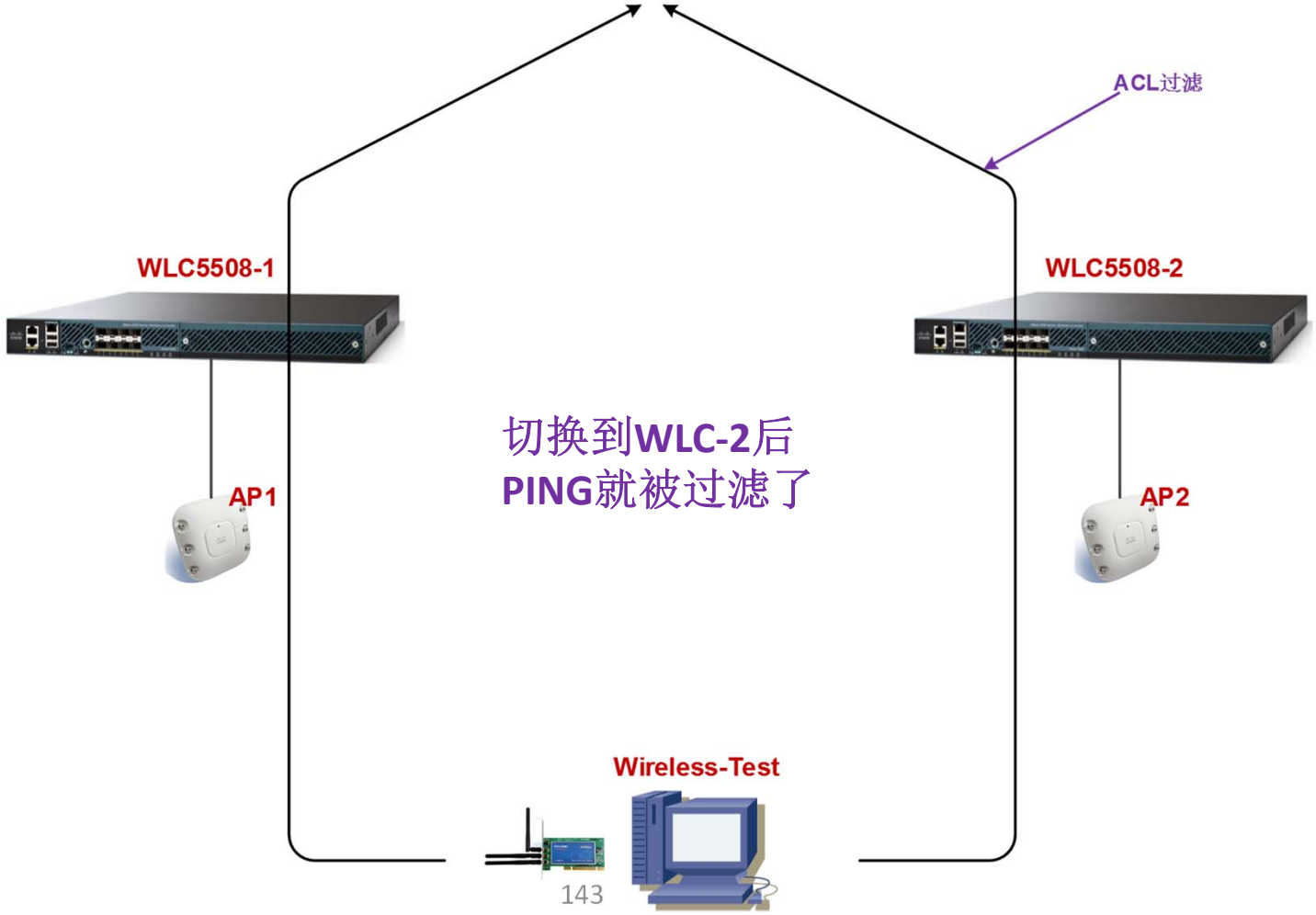
WLC5508-2
ACL Deny ICMP流量

测试默认没有锚的漫游效果

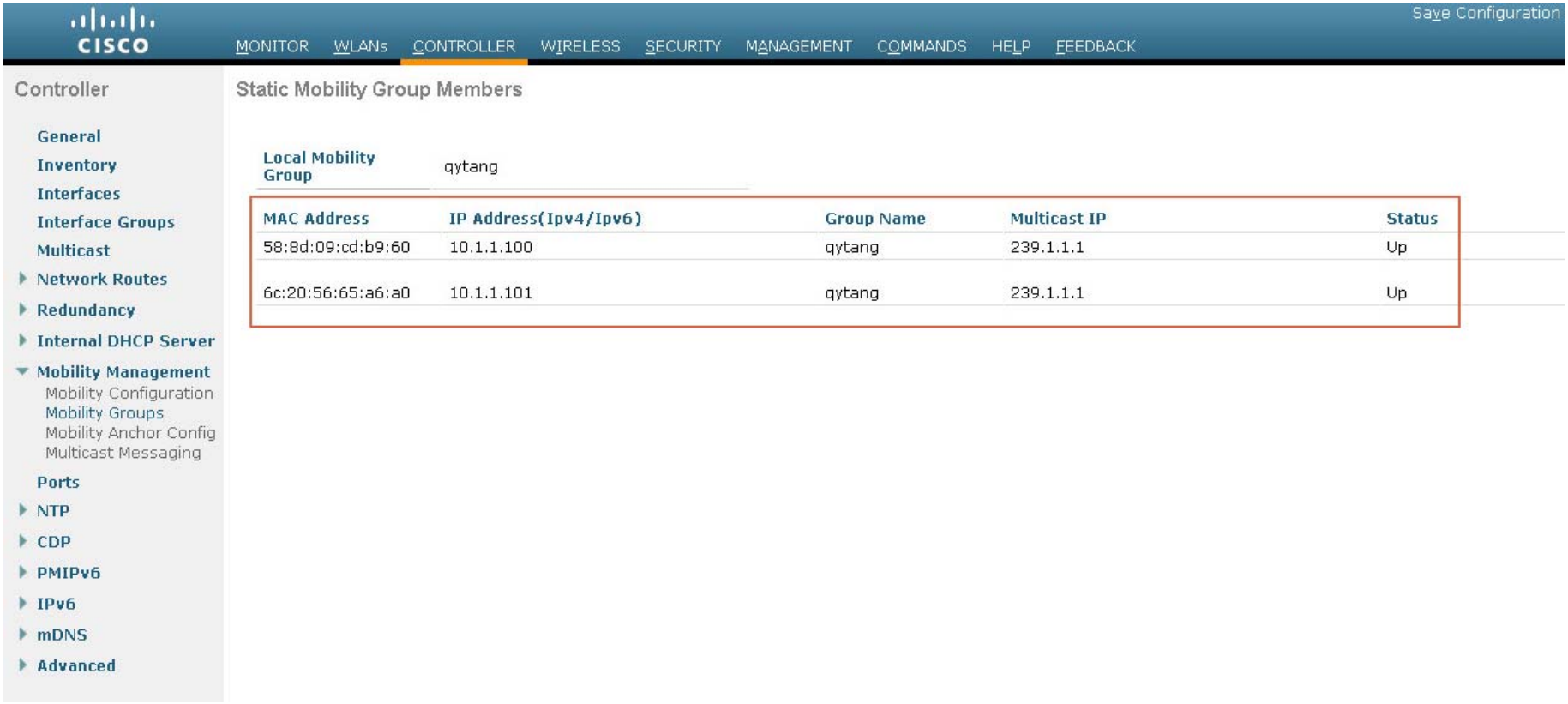
控制器WLC5508-2的VLAN30接口调用ACL



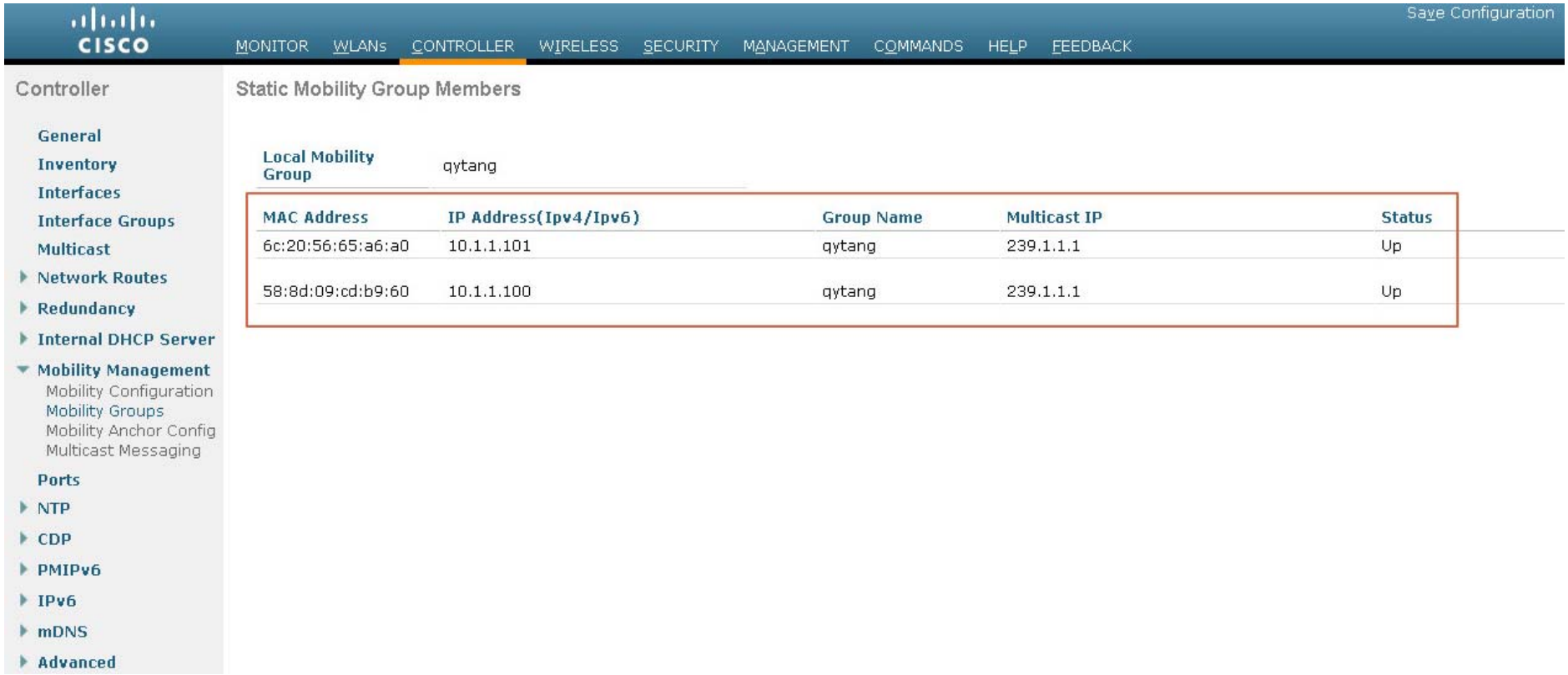
二层漫游默认没有锚的漫游效果



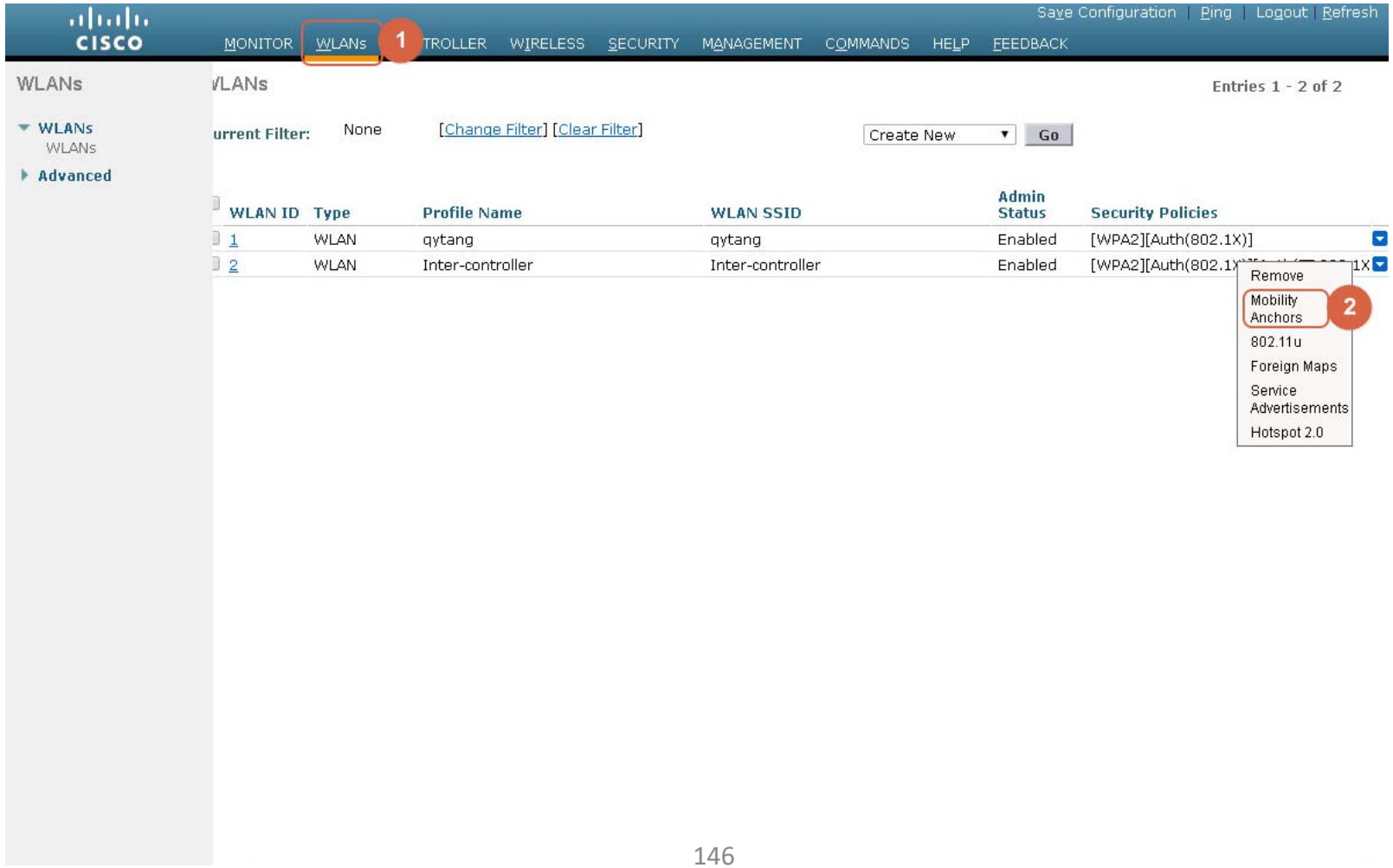
恢复漫游组静态成员（WLC-1）



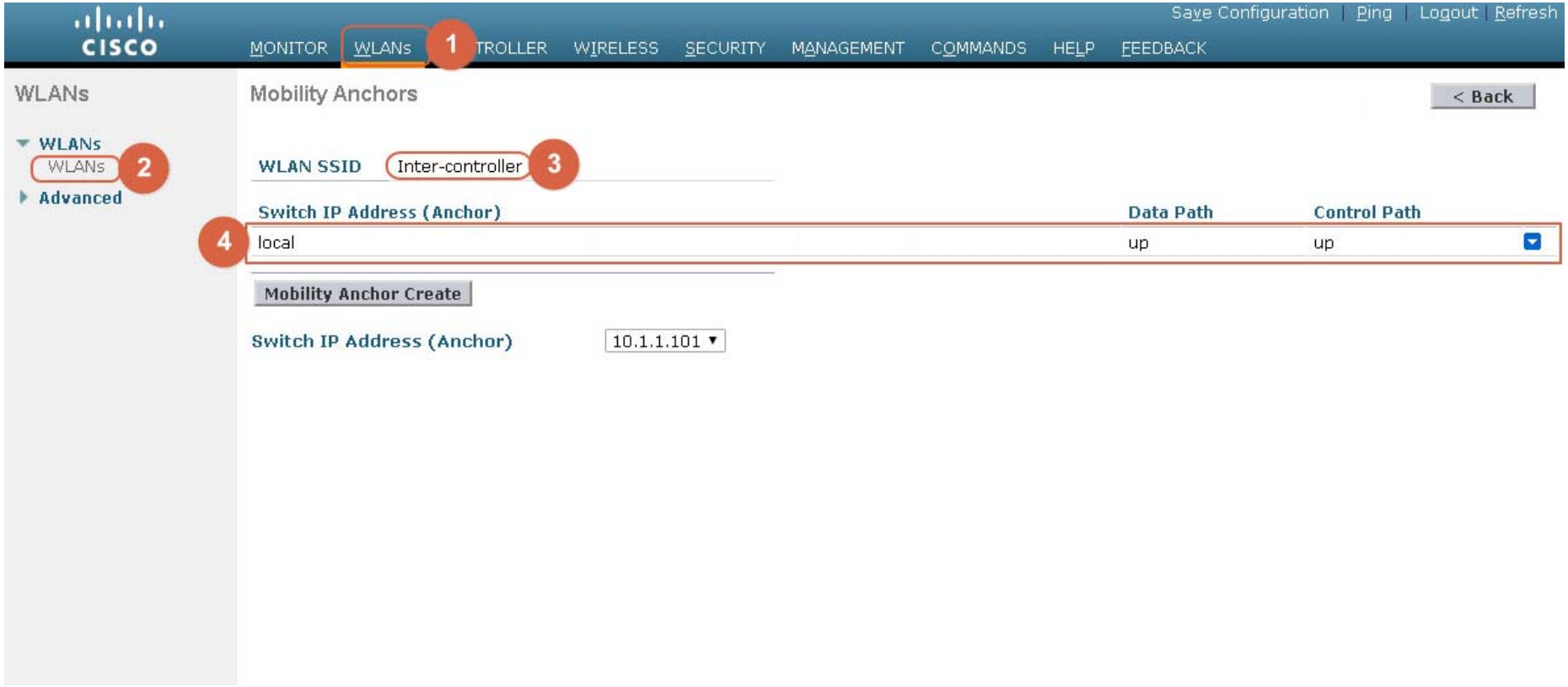
恢复漫游组静态成员（WLC-2）



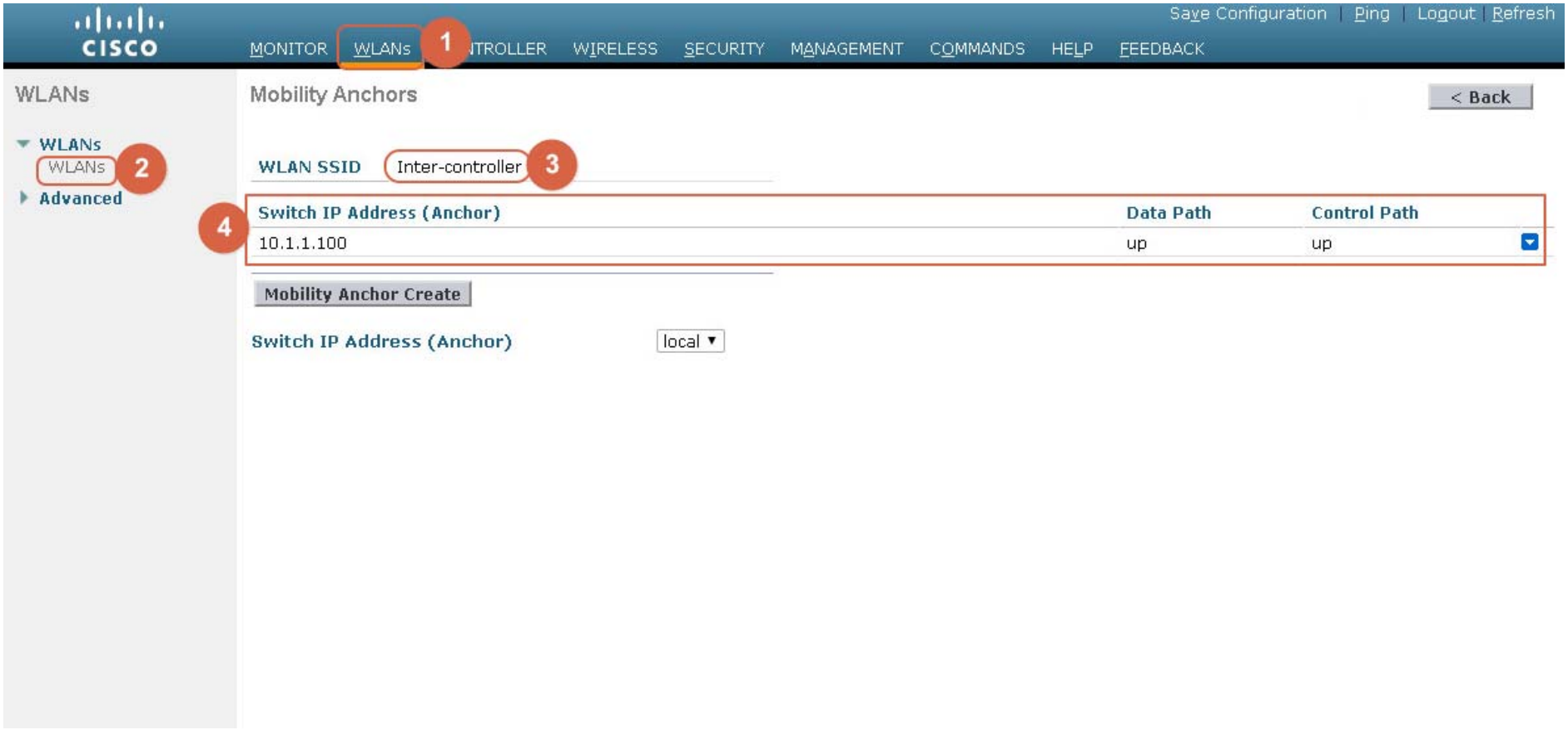
WLC5508-1配置锚



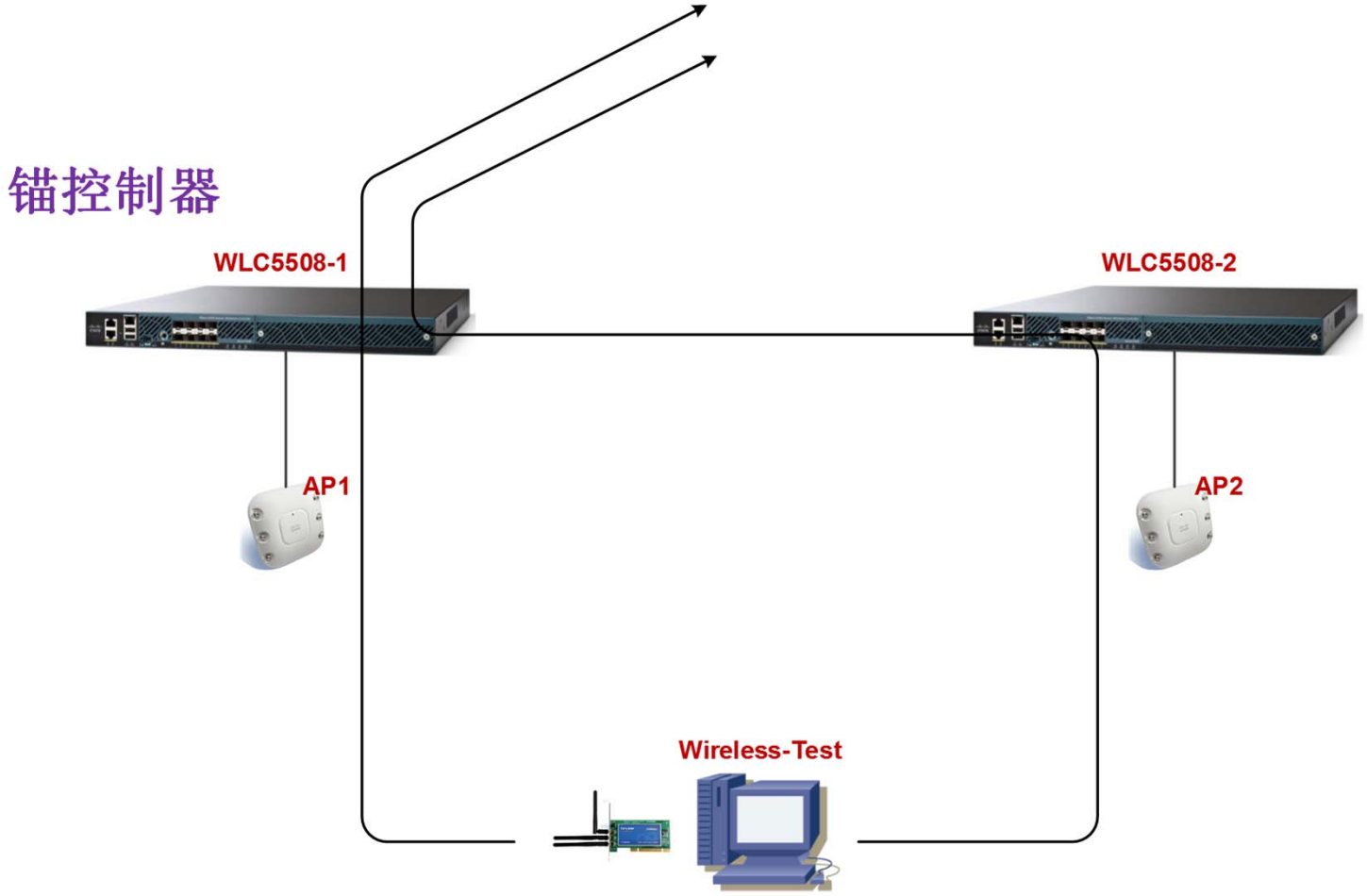
WLC5508-1配置锚



WLC5508-2配置锚



设置锚（WLC5508-1）的漫游效果

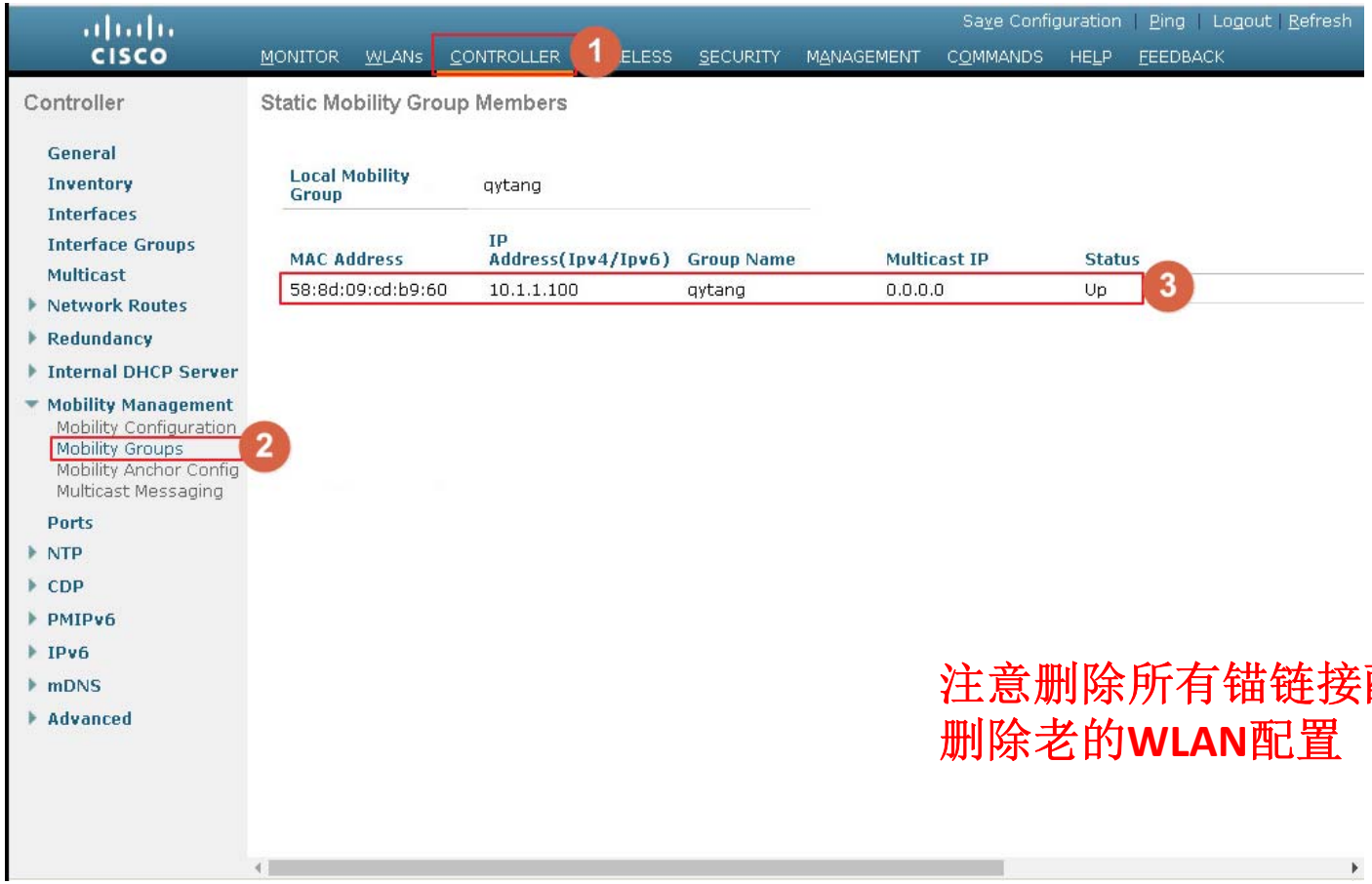


第四部分
Inter-Subnet Roaming

SW3560 配置

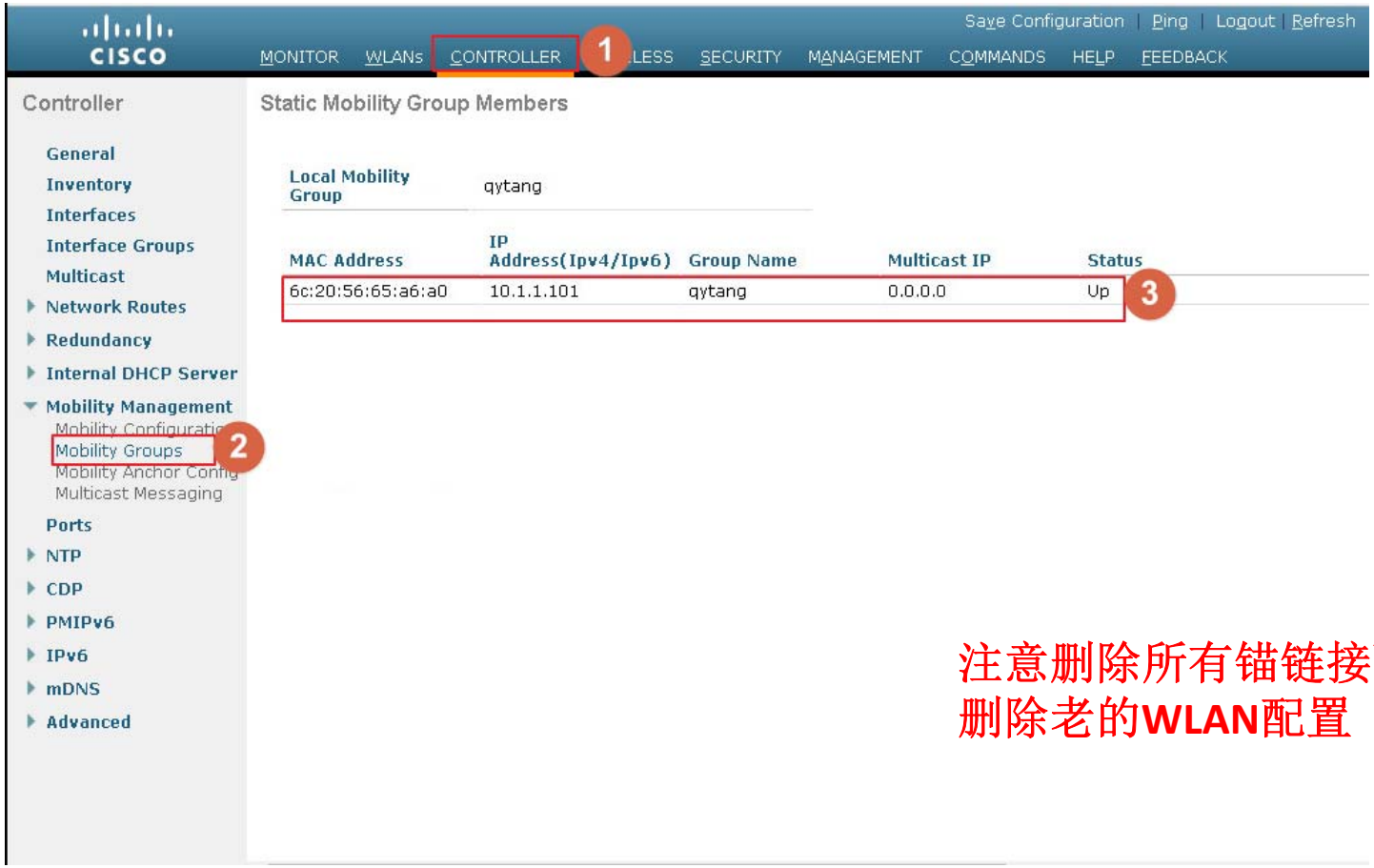
```
vlan 40
!
interface Vlan40
 ip address 40.1.1.254 255.255.255.0
!
ip dhcp pool Inter-subnet
   network 40.1.1.0 255.255.255.0
   default-router 40.1.1.254
```

WLC5508-1 删除组WLC5508-2



注意删除所有锚链接配置
删除老的**WLAN**配置

WLC5508-2 删除组WLC5508-1



注意删除所有锚链接配置
删除老的**WLAN**配置

WLC5508-1修改Group 组

删除之前所有创建的SSID， 或者关闭所有的WLAN FT 功能

WLC5508-1重新指定WLC5508-2

取消组播配置

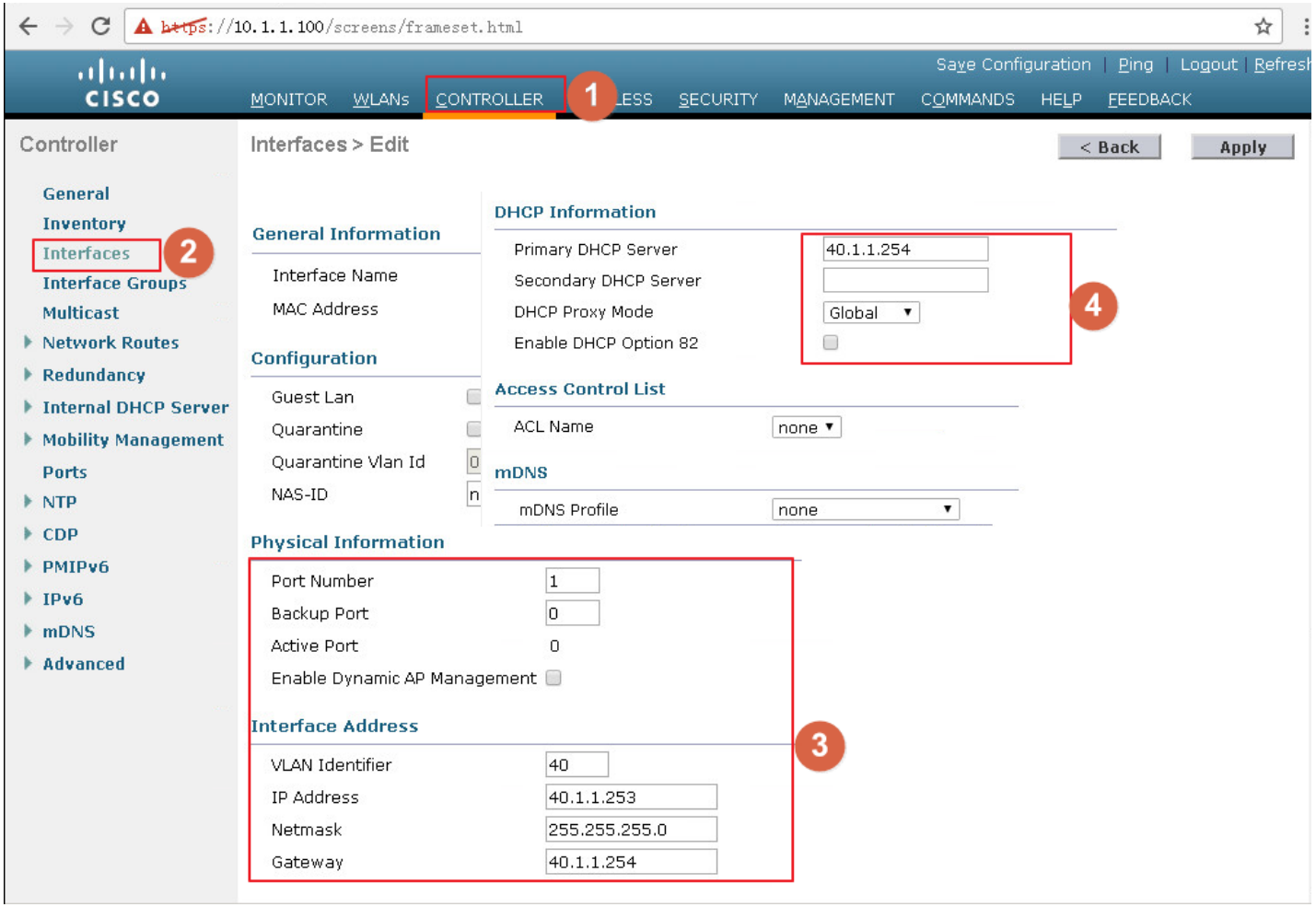
WLC 5508-2 MAC
6c:20:56:65:a6:a0

WLC5508-2 删除组WLC5508-1

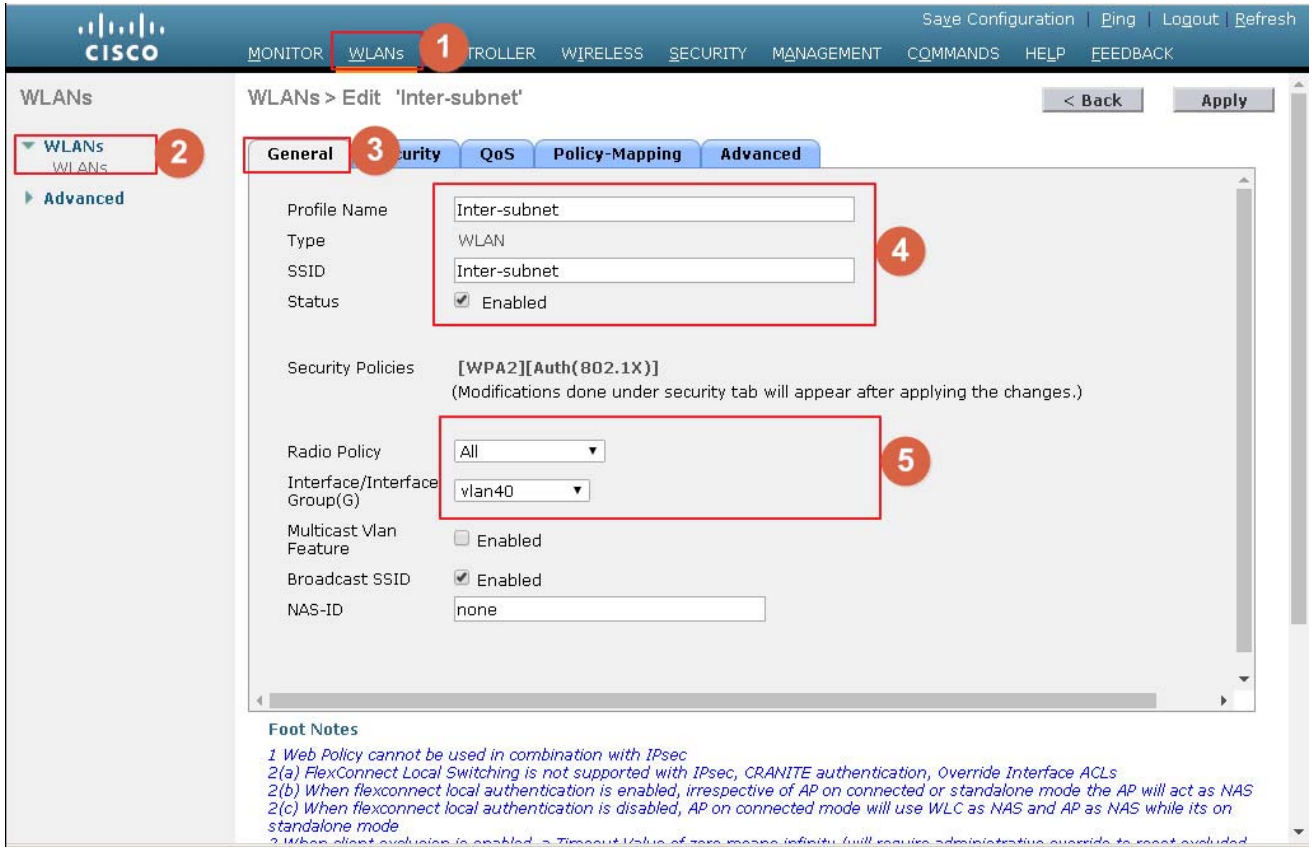
取消组播配置

WLC5508-1 MAC：
58:8d:09:cd:b9:60

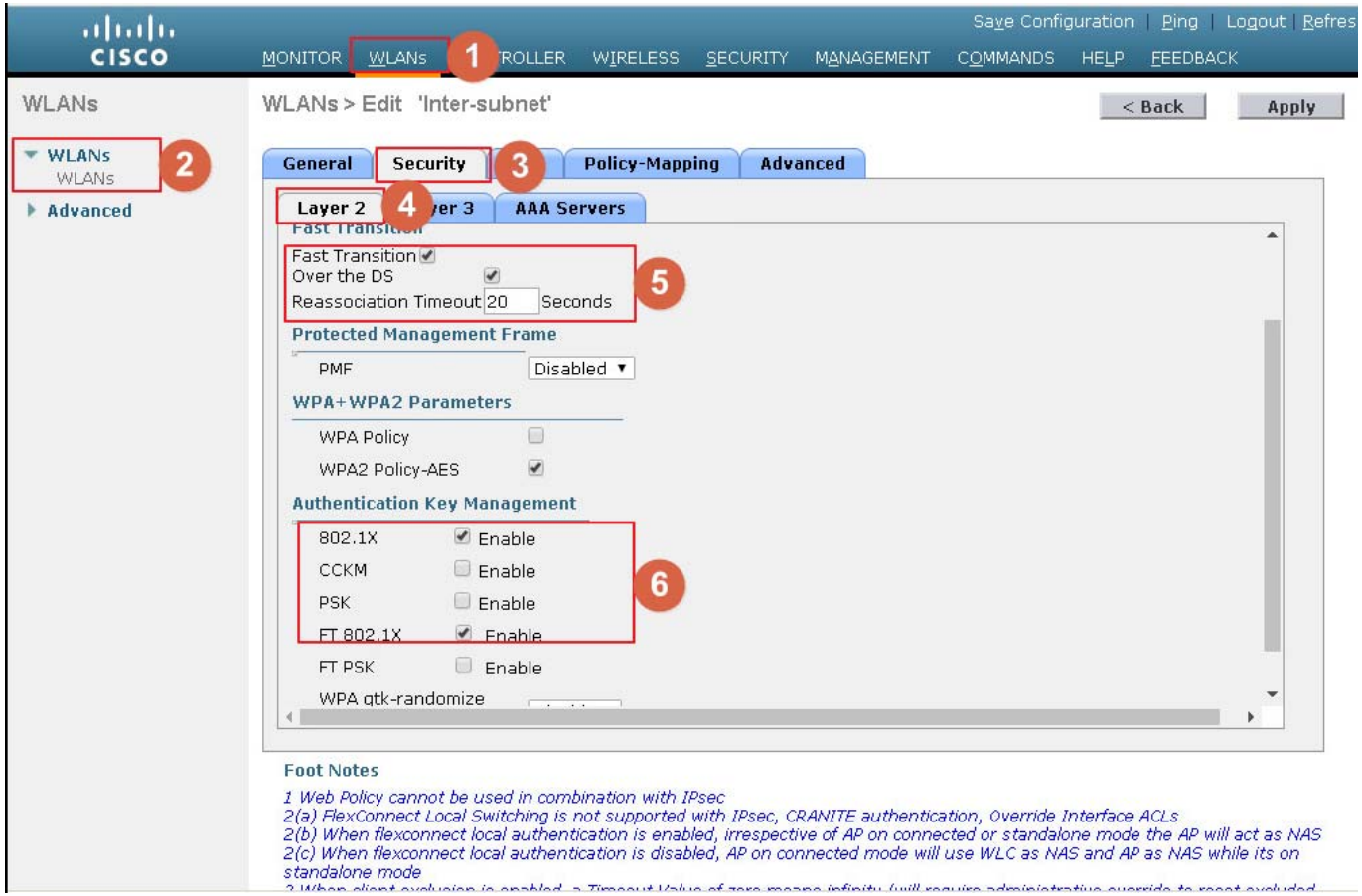
WLC5508-1 创建vlan40



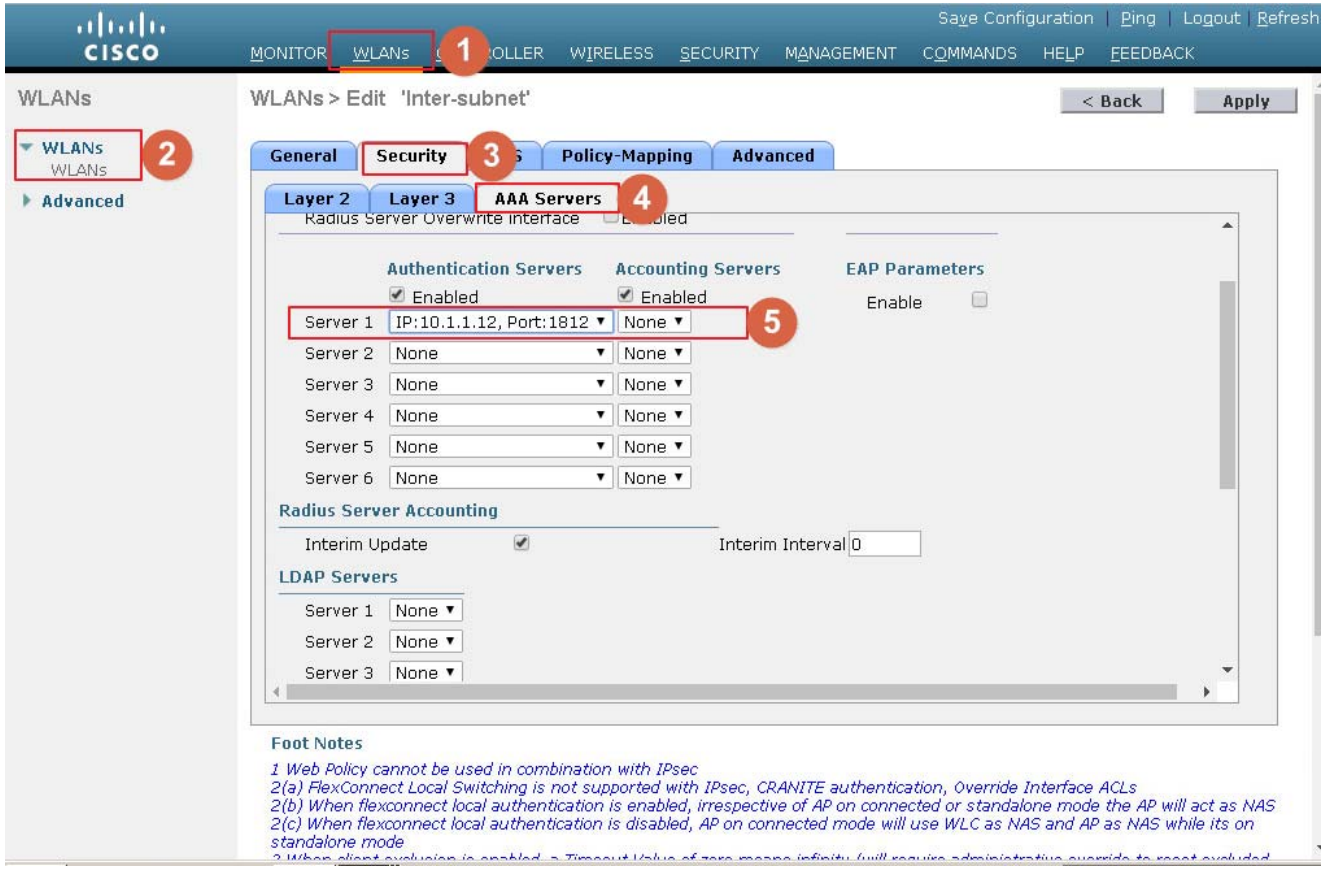
WLC5508-1 创建 Inter-subnet



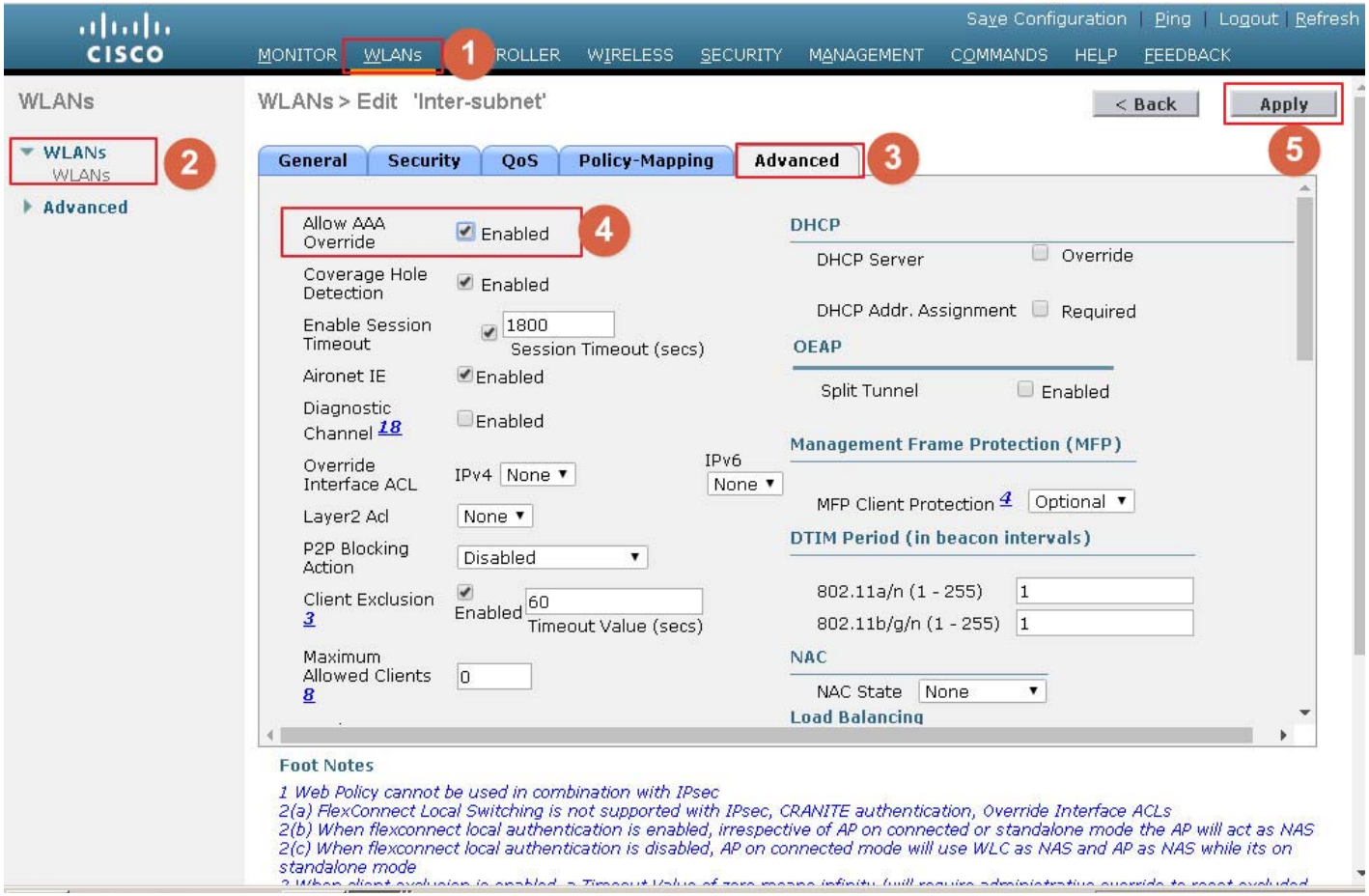
WLC5508-1 创建 Inter-subnet



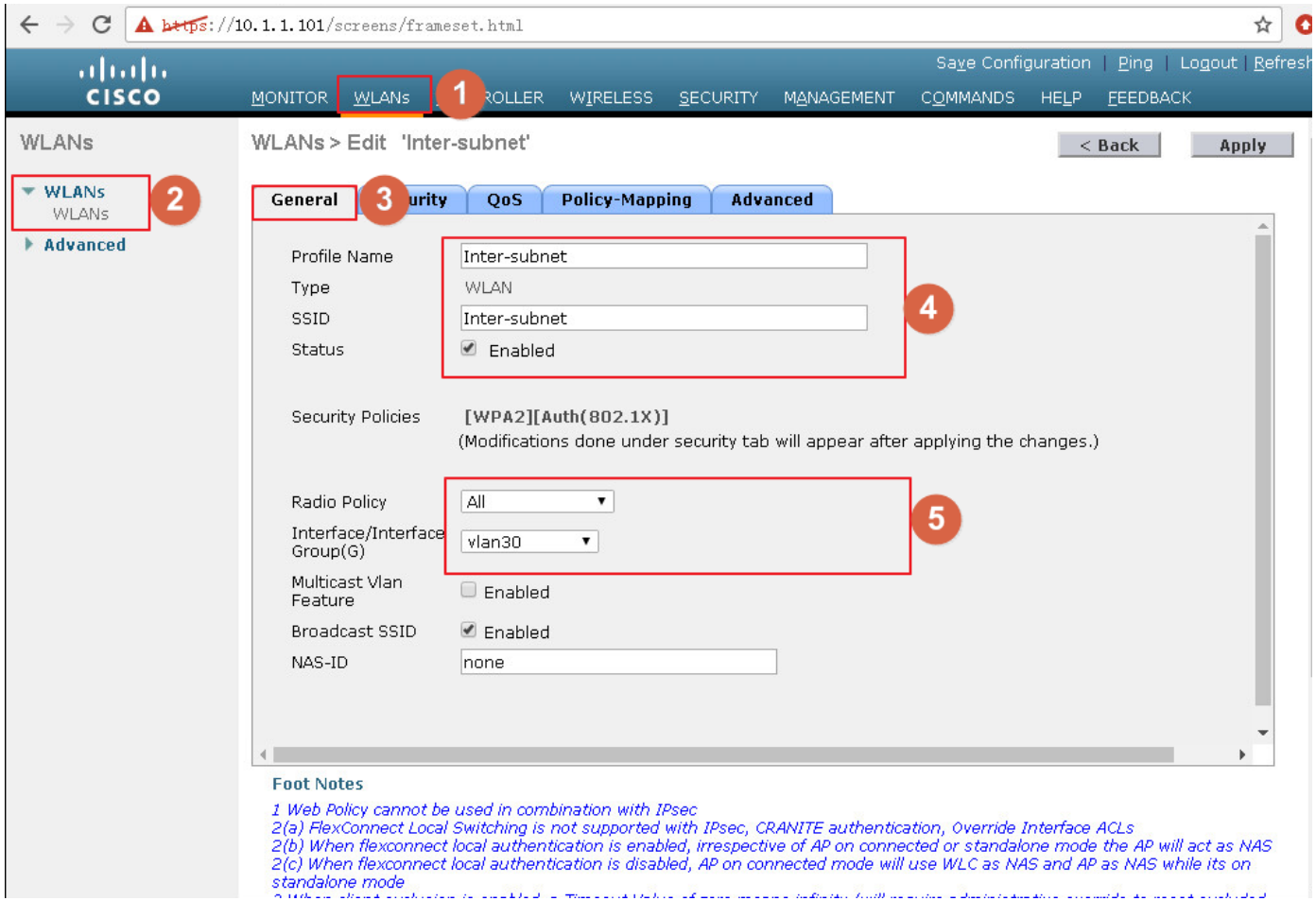
WLC5508-1 创建 Inter-subnet



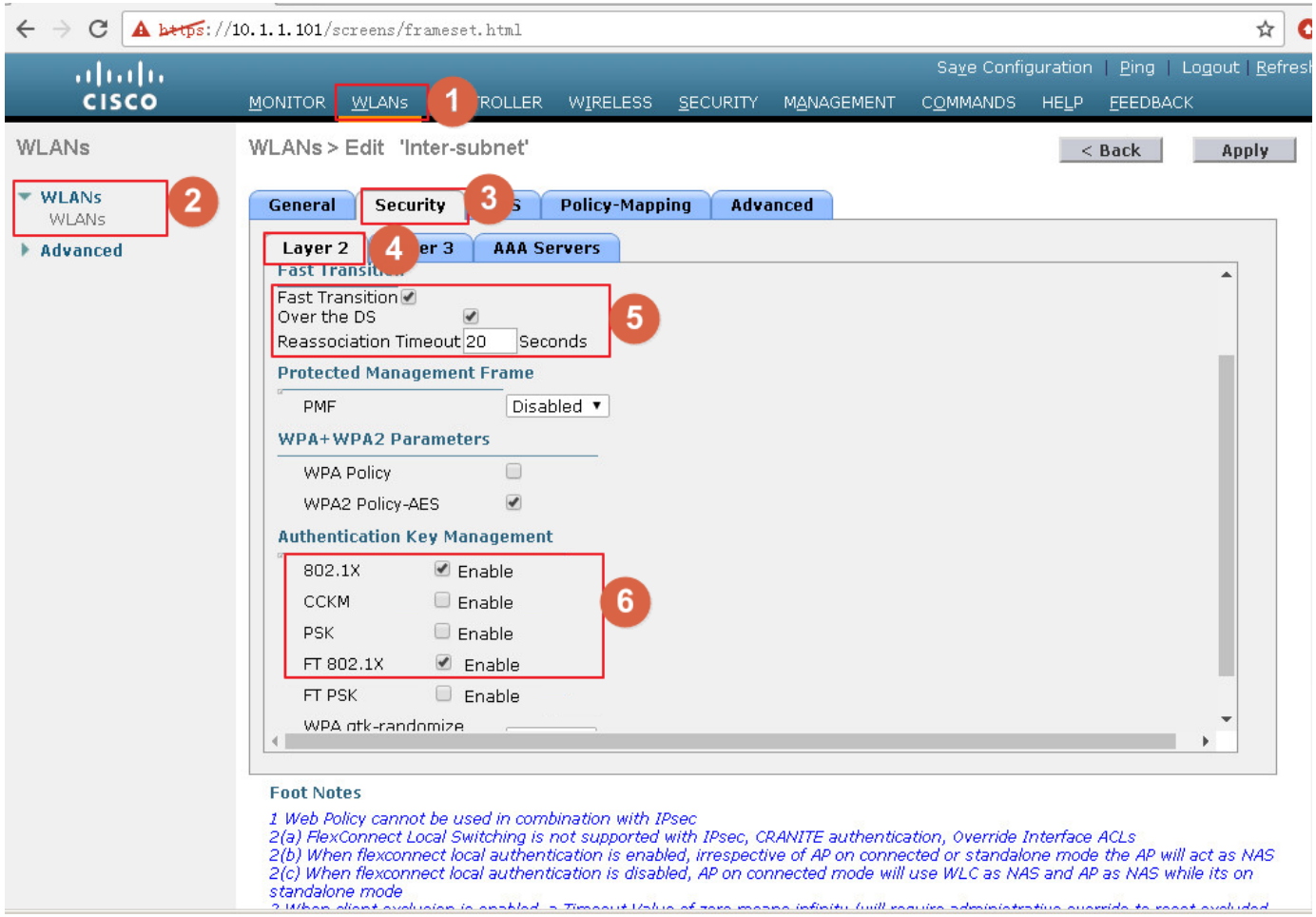
WLC5508-1 创建 Inter-subnet



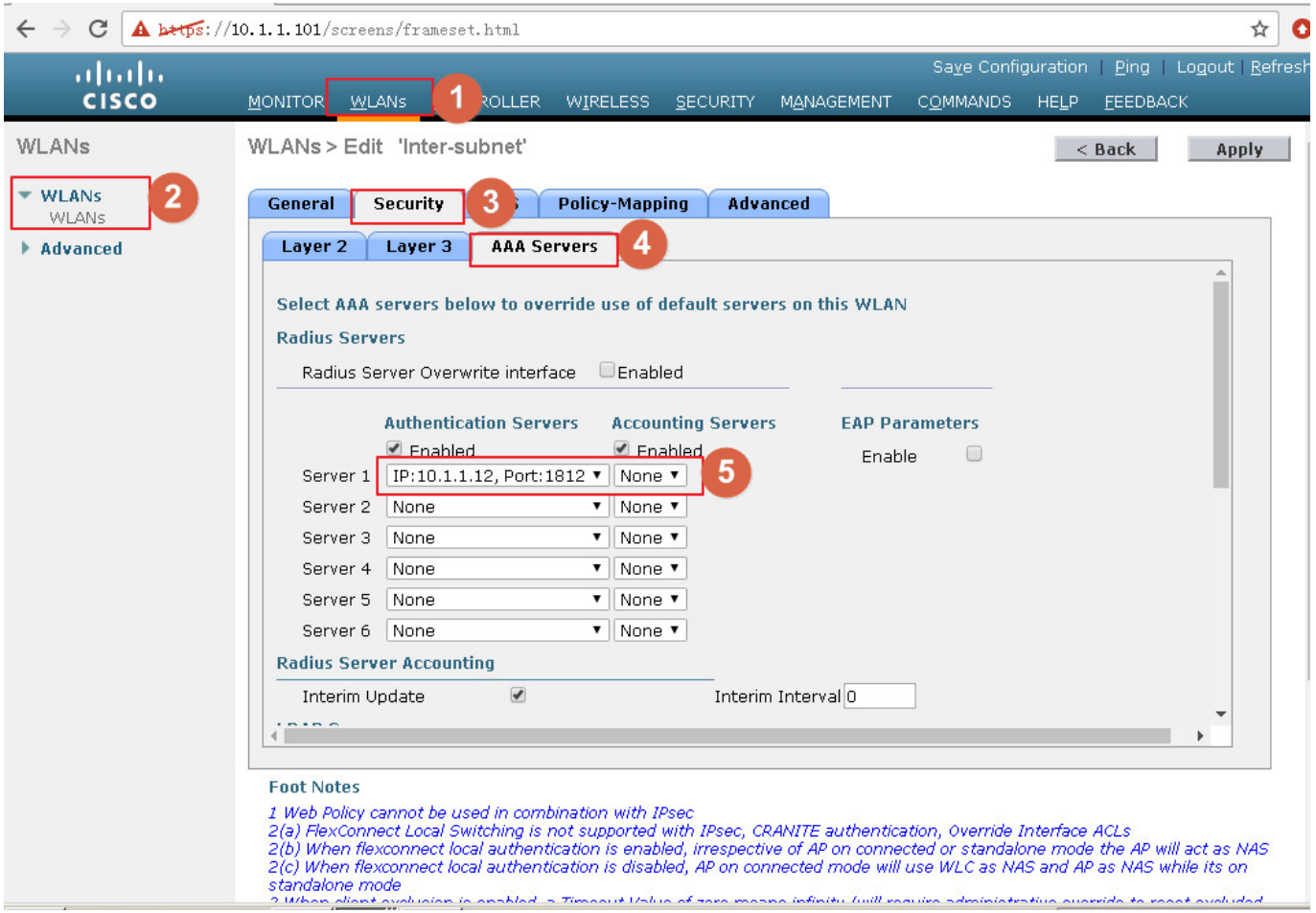
WLC5508-2 创建 Inter-subnet



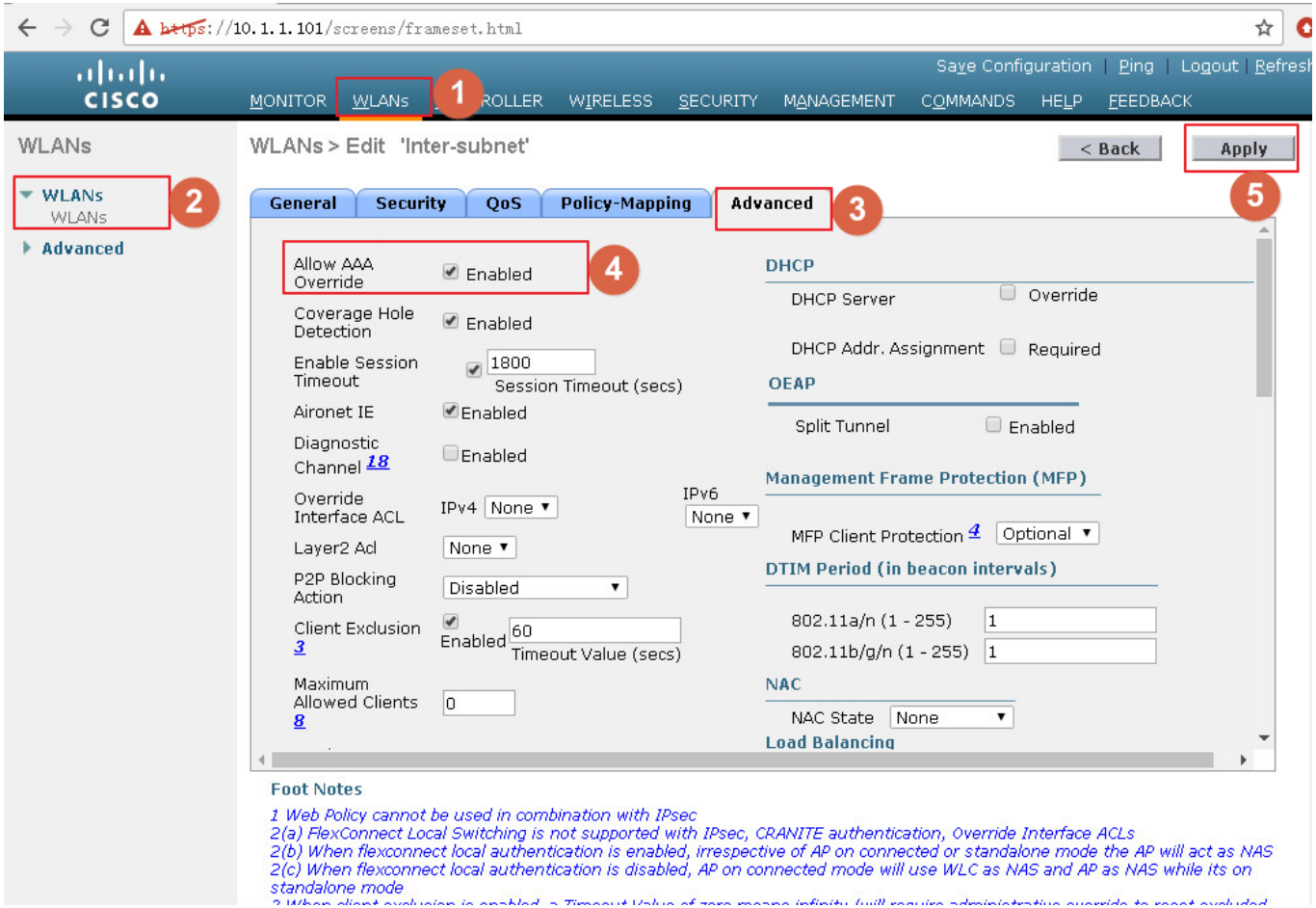
WLC5508-2 创建 Inter-subnet



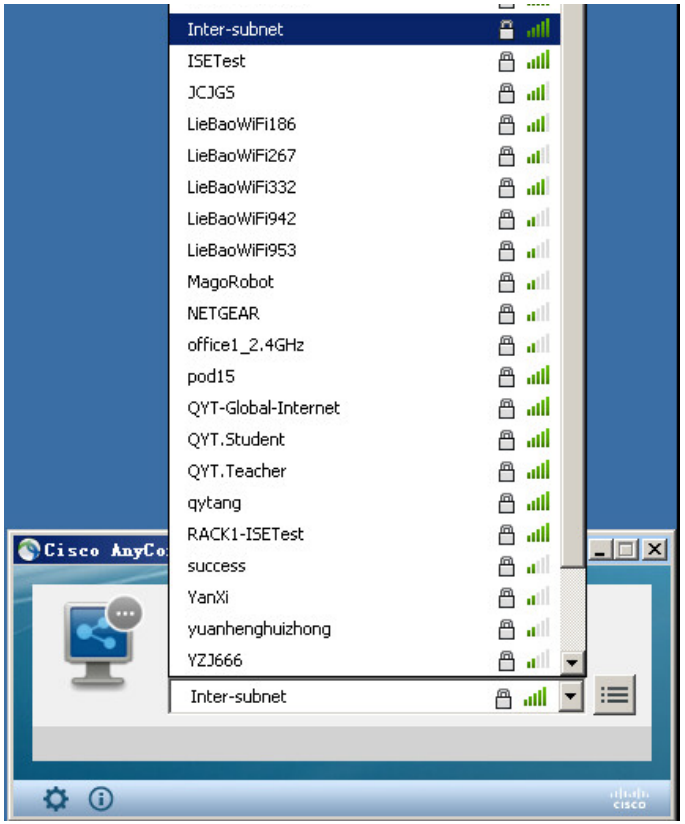
WLC5508-2 创建 Inter-subnet

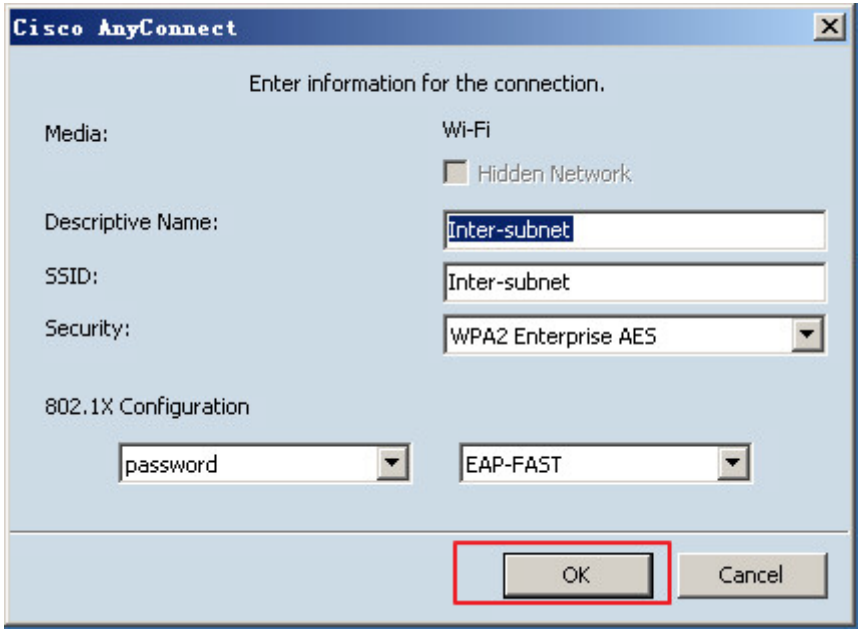


WLC5508-2 创建 Inter-subnet

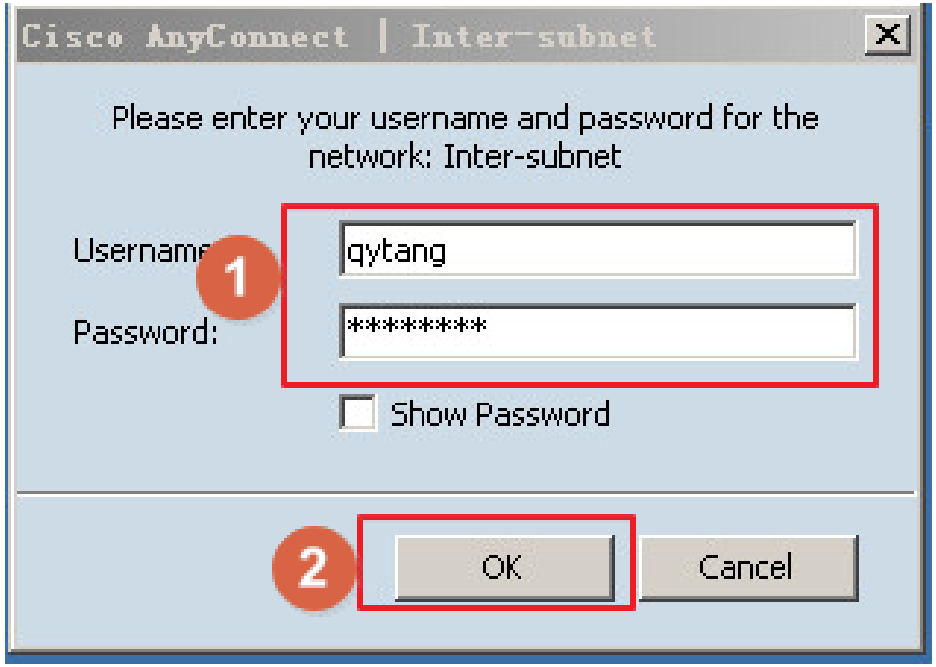


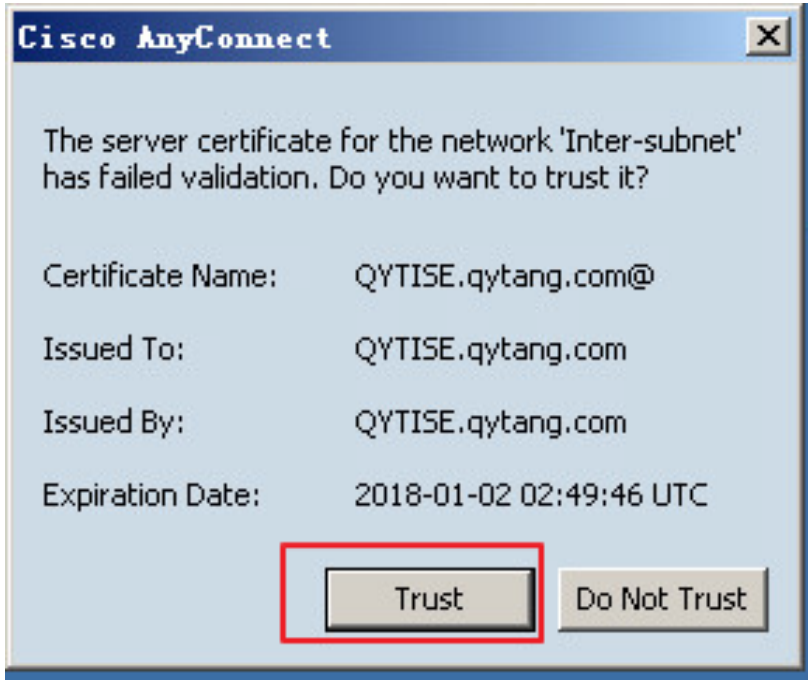
客户端测试: Inter-subnet





客户端测试: Inter-subnet

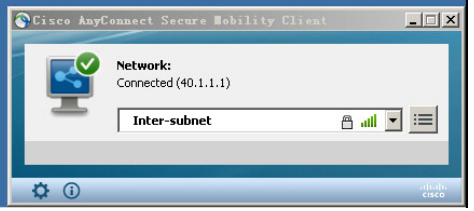




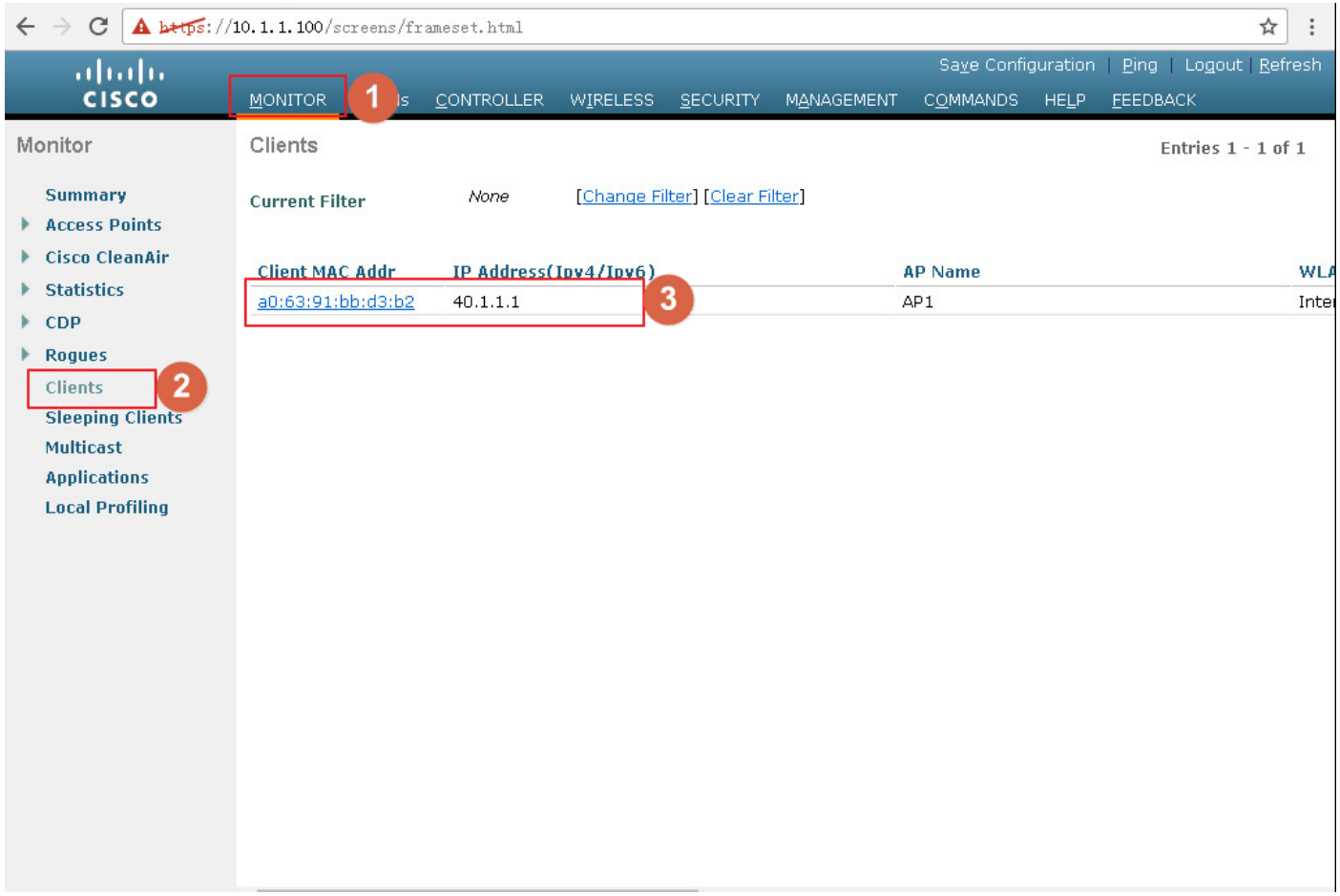
用户名：**qytang**
密码：**Cisc0123**

客户端测试: Inter-subnet

```
C:\Users\Administrator>ipconfig

Windows IP 配置

无线局域网适配器 无线网络连接:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::c0e0:fafb:1174:9380%15
   IPv4 地址 . . . . . . . . . . . . : 40.1.1.1
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 40.1.1.254

隧道适配器 isatap.{7F06461E-C4A6-4E5C-8AFC-BABE03FA5426}:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

隧道适配器 6TO4 Adapter:

   连接特定的 DNS 后缀 . . . . . . . :
   IPv6 地址 . . . . . . . . . . . . : 2002:2801:101::2801:101
   默认网关. . . . . . . . . . . . . :

隧道适配器 Teredo Tunneling Pseudo-Interface:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

C:\Users\Administrator>ping 10.1.1.254 -t

正在 Ping 10.1.1.254 具有 32 字节的数据:
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=88ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
```



WLC 5508-1查看关联



天线与型号强度调整

802.11a/n Cisco APs > Configure

General

AP Name	AP2
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☐ C ☐

RF Channel Assignment

Current Channel	161
Channel Width *	20 MHz

** Channel width can be configured only when channel configuration is in custom mode*

Assignment Method	Global / Custom

Tx Power Level Assignment

Current Tx Power Level	6
Assignment Method	Global / Custom 6

Performance Profile

View and edit Performance Profile for this AP

Performance Profile

Note: Changing any of the parameters causes … disabled and thus may result in loss of connect

送出端

信号调整到最小（6）
天线只留A

接收端

信号调整到最大（1）
天线A B C全部打开

802.11a/n Cisco APs > Configure

General

AP Name	AP1
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel	149
Channel Width *	20 MHz

** Channel width can be configured only when channel configuration is in custom mode*

Assignment Method	Global / Custom

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	Global / Custom 1

Performance Profile

View and edit Performance Profile for this AP

Performance Profile

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

客户端测试效果

管理员: C:\Windows\system32\cmd.exe

```
C:\Users\Administrator>ping 10.1.1.254 -t

正在 Ping 10.1.1.254 具有 32 字节的数据:
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
请求超时。
来自 10.1.1.254 的回复: 字节=32 时间=5ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
```

控制器验证测试效果

两边都有
关联信息

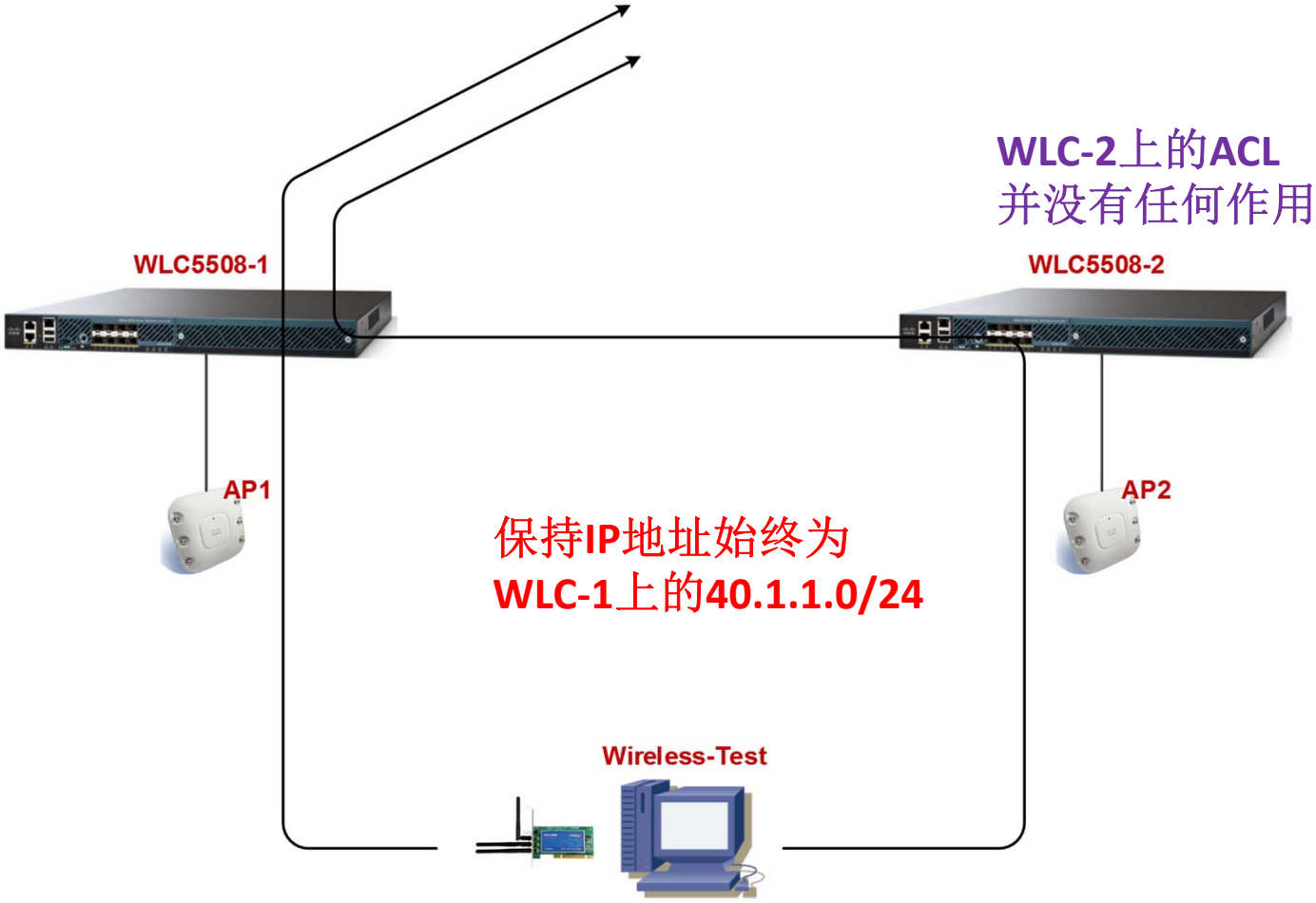
注意登陆
WLC5508-2

控制器验证测试效果

两边都有
关联信息

注意登陆
WLC5508-1

三层漫游效果


WLC-2上的ACL
并没有任何作用
WLC5508-1
WLC5508-2
AP1
AP2
保持IP地址始终为
WLC-1上的40.1.1.0/24
Wireless-Test

WLC 5508-1 关闭AP1

https://10.1.1.100/screens/frameset.html

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS 1 URITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

- Access Poi
  - All APs 2
  - Radios
    - 802.11a/n/ac
    - 802.11b/g/n
    - Dual-Band Radios
  - Global Configuration
- Advanced
- Mesh
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- OEAP ACLs
- Network Lists
- 802.11a/n/ac
- 802.11b/g/n
- Media Stream
- Application Visibility And Control
- Country
- Timers
- Netflow
- QoS

All APs > Details for AP1 < Back Apply

General 3 dentials Interfaces High Availability Inventory Advanced

General

AP Name	AP1
Location	default location
AP MAC Address	fc:5b:39:37:1a:98
Base Radio MAC	68:99:cd:06:5f:30
Admin Status	Disable 4
AP Mode	local
AP Sub Mode	None
Operational Status	REG
Port Number	1
Venue Group	Unspecified
Venue Type	Unspecified
Venue Name	
Language	
Network Spectrum Interface Key	C3C482749862E8EE7277FB2D6C786160

GPS Location

GPS Present	No

Versions

Primary Software Version	8.0.140.0
Backup Software Version	0.0.0.0
Predownload Status	None
Predownloaded Version	None
Predownload Next Retry Time	NA
Predownload Retry Count	NA
Boot Version	15.2.2.0
IOS Version	15.3(3)JA10$
Mini IOS Version	0.0.0.0

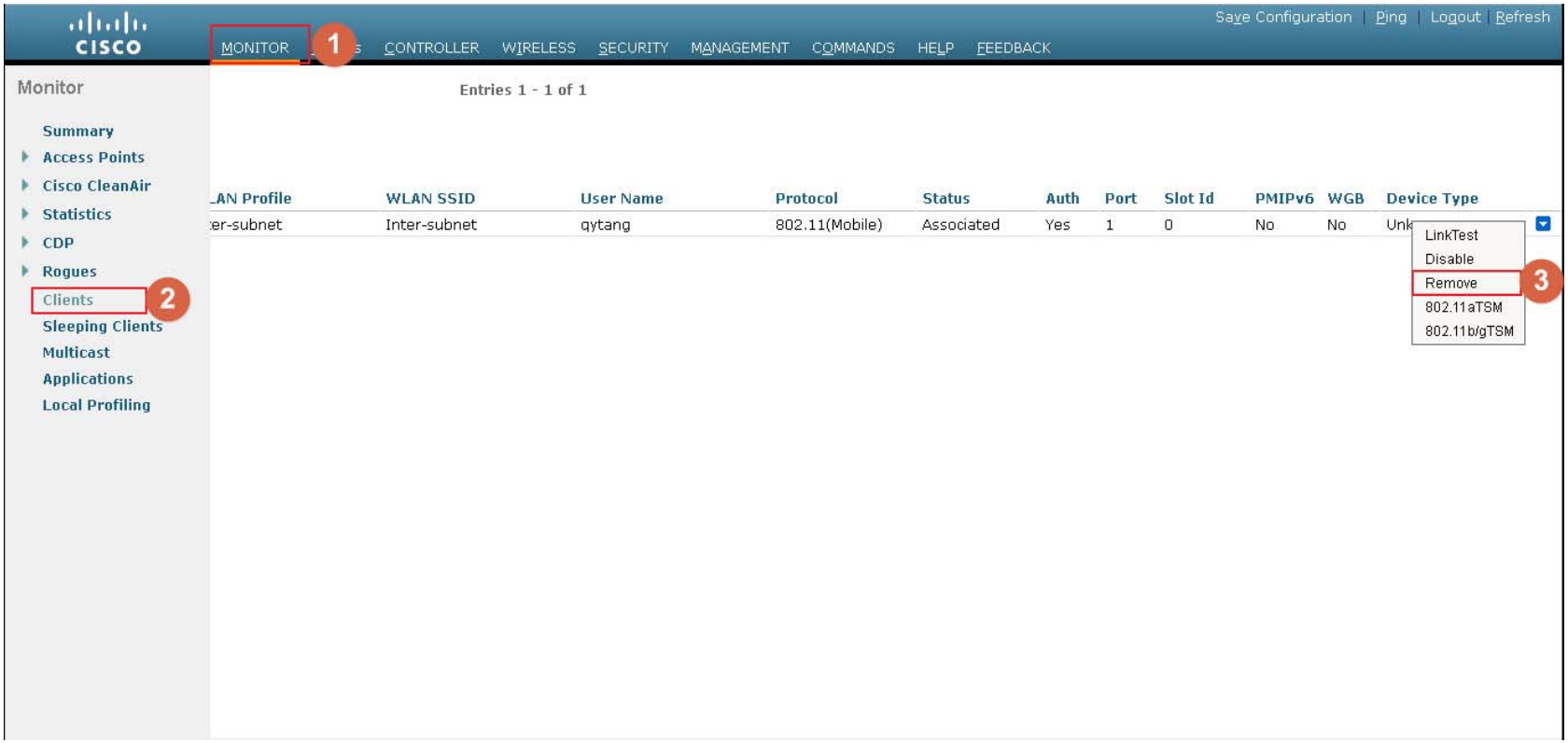
IP Config

CAPWAP Preferred Mode	Ipv4 (Global Cor
DHCP Ipv4 Address	20.1.1.2
Static IP (Ipv4/Ipv6)	

Time Statistics

UP Time	0 d, 01 h 09 m 4
Controller Associated Time	0 d, 01 h 03 m 2
Controller Association Latency	0 d, 00 h 06 m 1

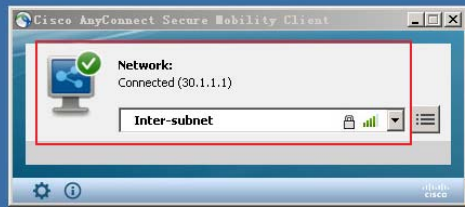
删除两个控制的关联


cisco
MONITOR
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Save Configuration | Ping | Logout | Refresh
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Local Profiling
Entries 1 - 1 of 1
LAN Profile
WLAN SSID
User Name
Protocol
Status
Auth
Port
Slot Id
PMIPv6
WGB
Device Type
er-subnet
Inter-subnet
qytang
802.11(Mobile)
Associated
Yes
1
0
No
No
LinkTest
Disable
Remove
802.11aTSM
802.11b/gTSM
1
2
3

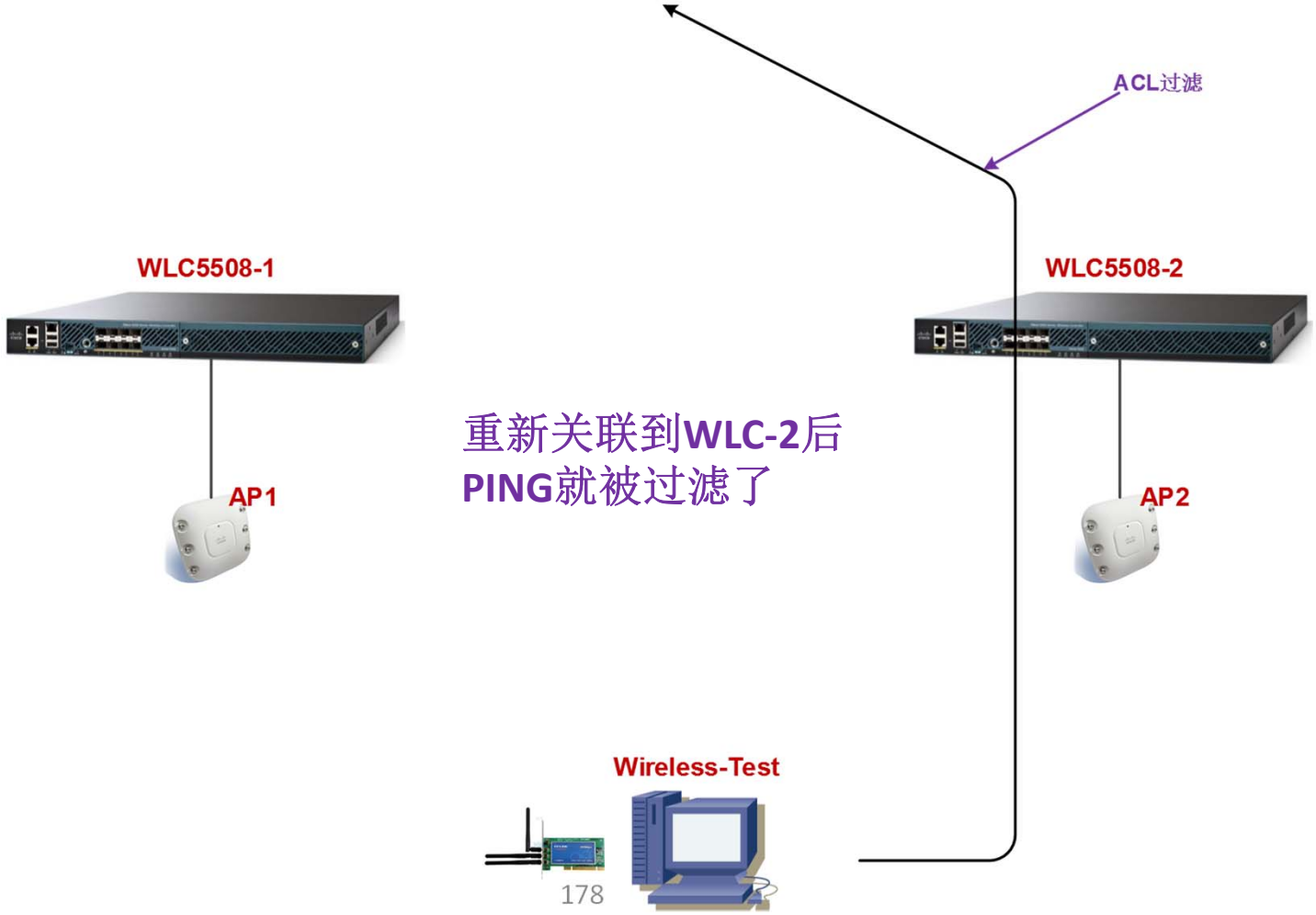
Test-PC 重新获取IP地址

```
C:\Users\Administrator>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : WIRMGMTPC
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型 . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否

无线局域网适配器 无线网络连接:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : NETGEAR A6210 WiFi USB3.0 Adapter
   物理地址. . . . . . . . . . . . . : A0-63-91-BB-D3-B2
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::c0e0:fafb:1174:9380%15(首选)
   IPv4 地址 . . . . . . . . . . . . : 30.1.1.1(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2017年9月23日 16:45:07
   租约过期的时间  . . . . . . . . . : 2017年9月24日 16:45:07
   默认网关. . . . . . . . . . . . . : 30.1.1.254
   DHCP 服务器 . . . . . . . . . . . : 1.1.1.1
   DHCPv6 IAID . . . . . . . . . . . : 362832785
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-20-29-74-EF-00-50-56-B2-DF-C3

   DNS 服务器  . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

隧道适配器 isatap.{7F06461E-C4A6-4E5C-8AFC-BABE03FA5426}:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft ISATAP Adapter
   物理地址. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是

隧道适配器 6TO4 Adapter:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft 6to4 Adapter
   物理地址. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
```

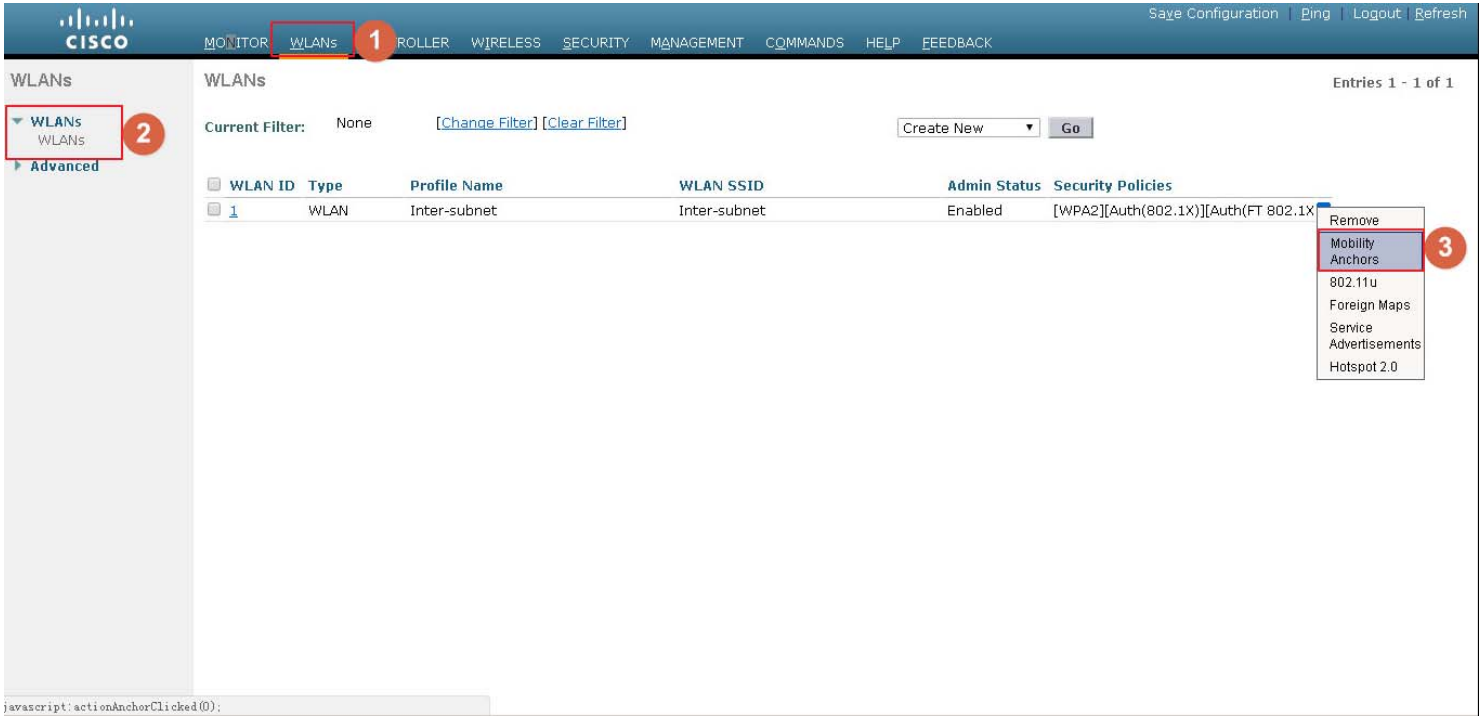
```
管理员: C:\Windows\system32\cmd.exe - ping  30.1.1.254 -t
来自 30.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=3ms TTL=255
请求超时。
请求超时。
来自 40.1.1.1 的回复: 无法访问目标主机。
一般故障。
PING: 传输失败。General failure.
PING: 传输失败。General failure.
PING: 传输失败。General failure.
PING: 传输失败。General failure.
PING: 传输失败。General failure.
PING: 传输失败。General failure.
PING: 传输失败。General failure.
PING: 传输失败。General failure.
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
```



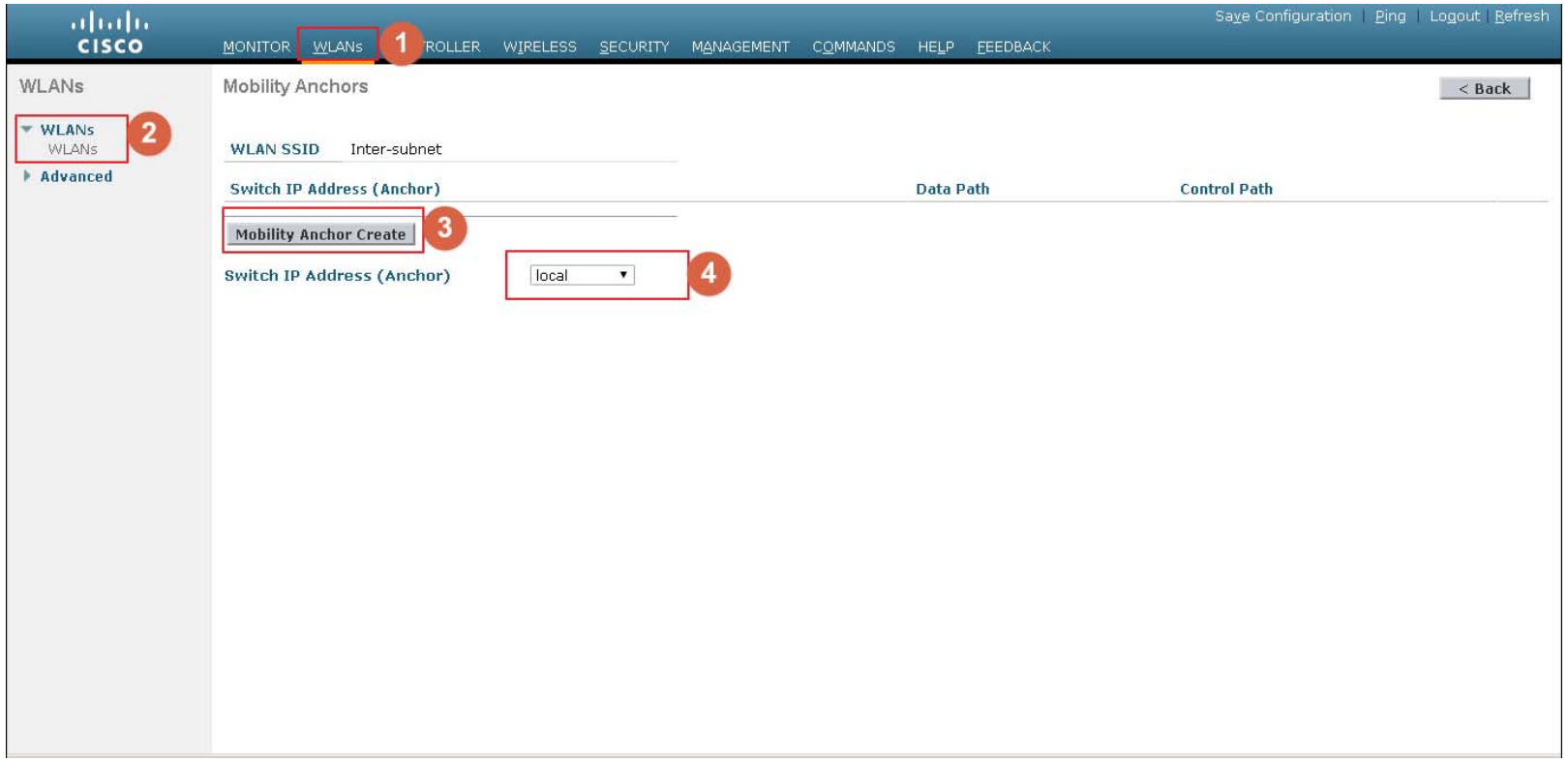
三层漫游效果


ACL过滤
WLC5508-1
WLC5508-2
AP1
AP2
重新关联到WLC-2后
PING就被过滤了
Wireless-Test

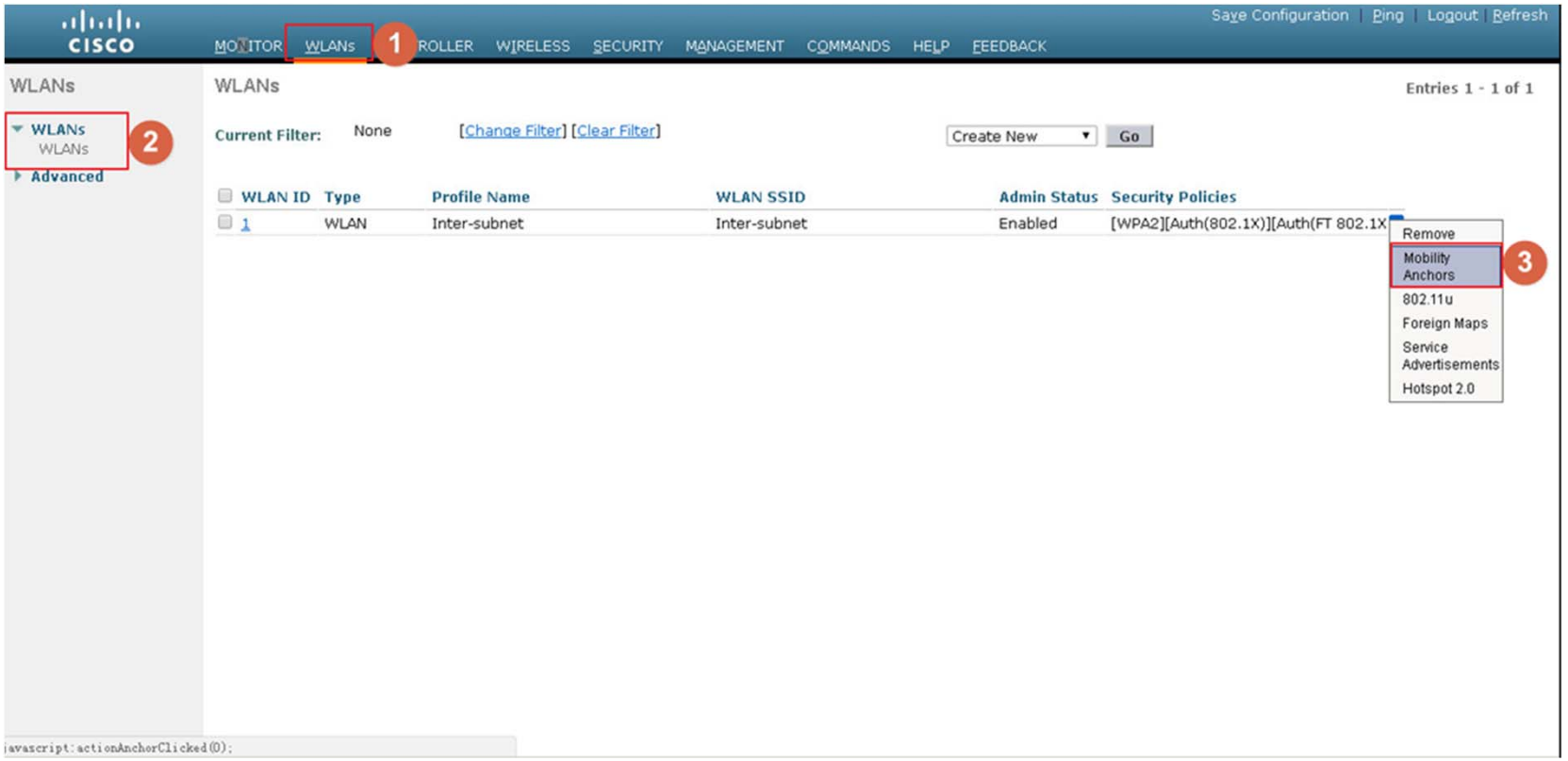
WLC5508-1 配置锚



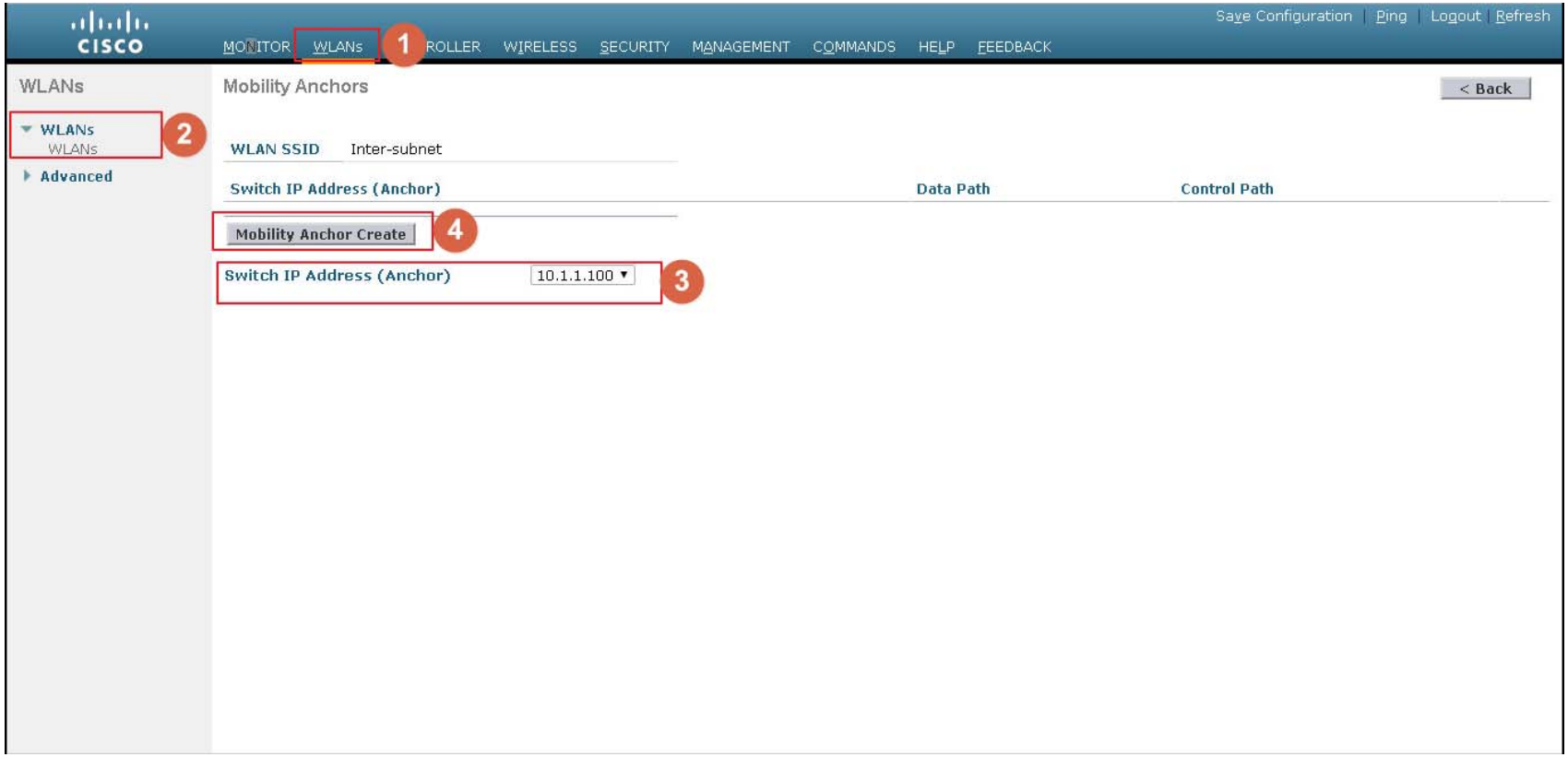
WLC5508-1 配置锚



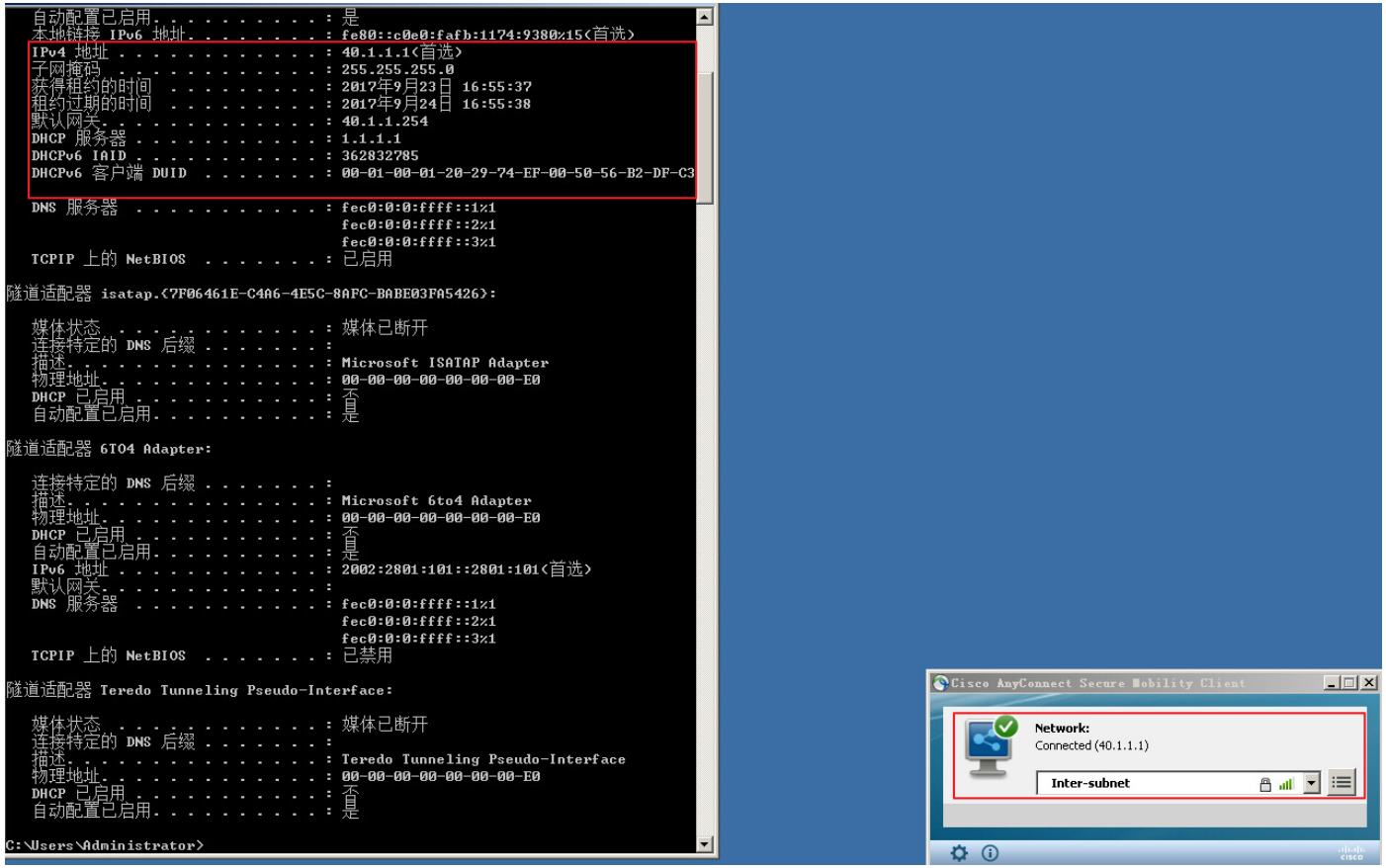
WLC5508-2 配置锚



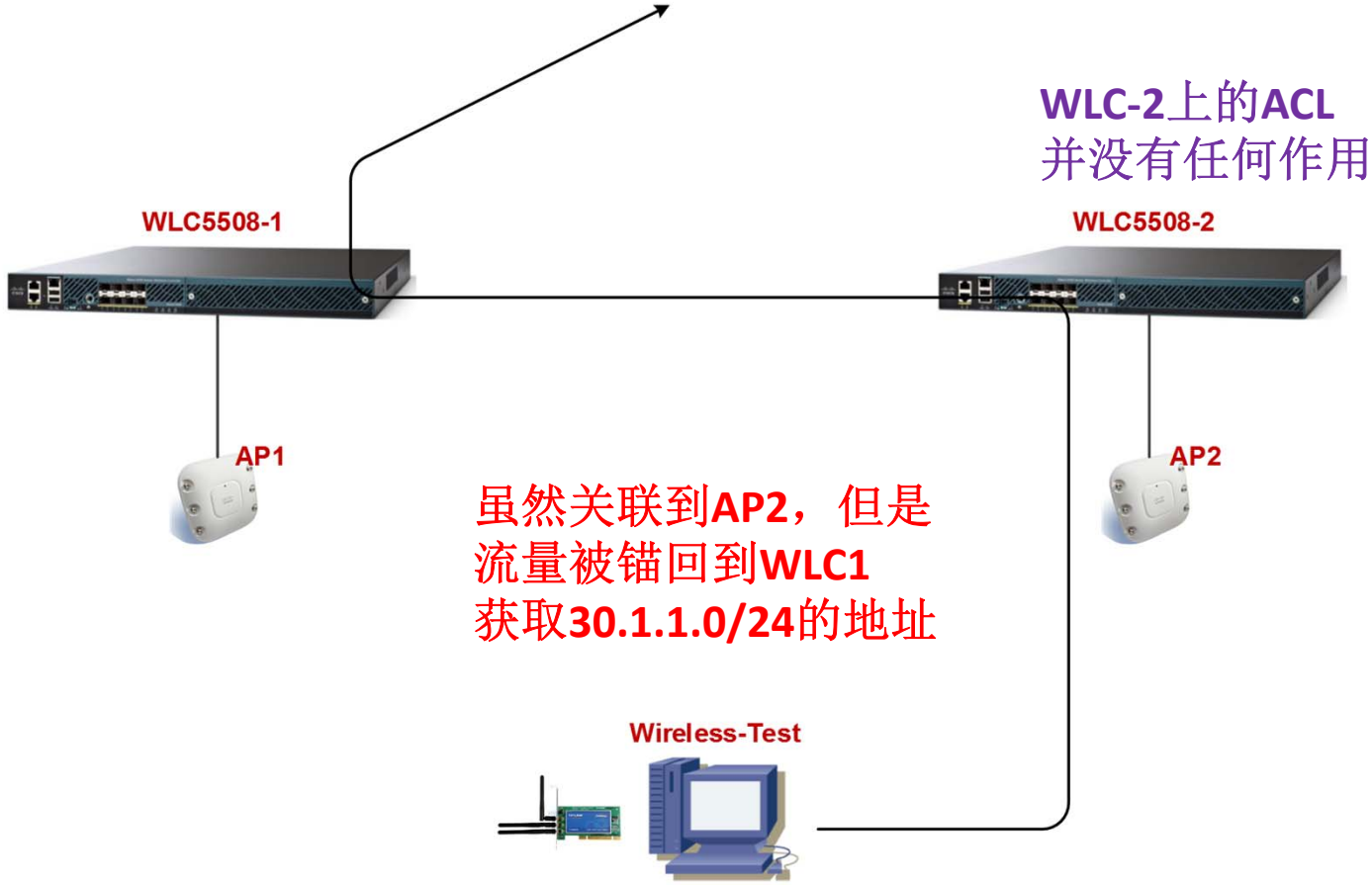
WLC5508-2 配置锚



Test-PC 重新获取新的网段



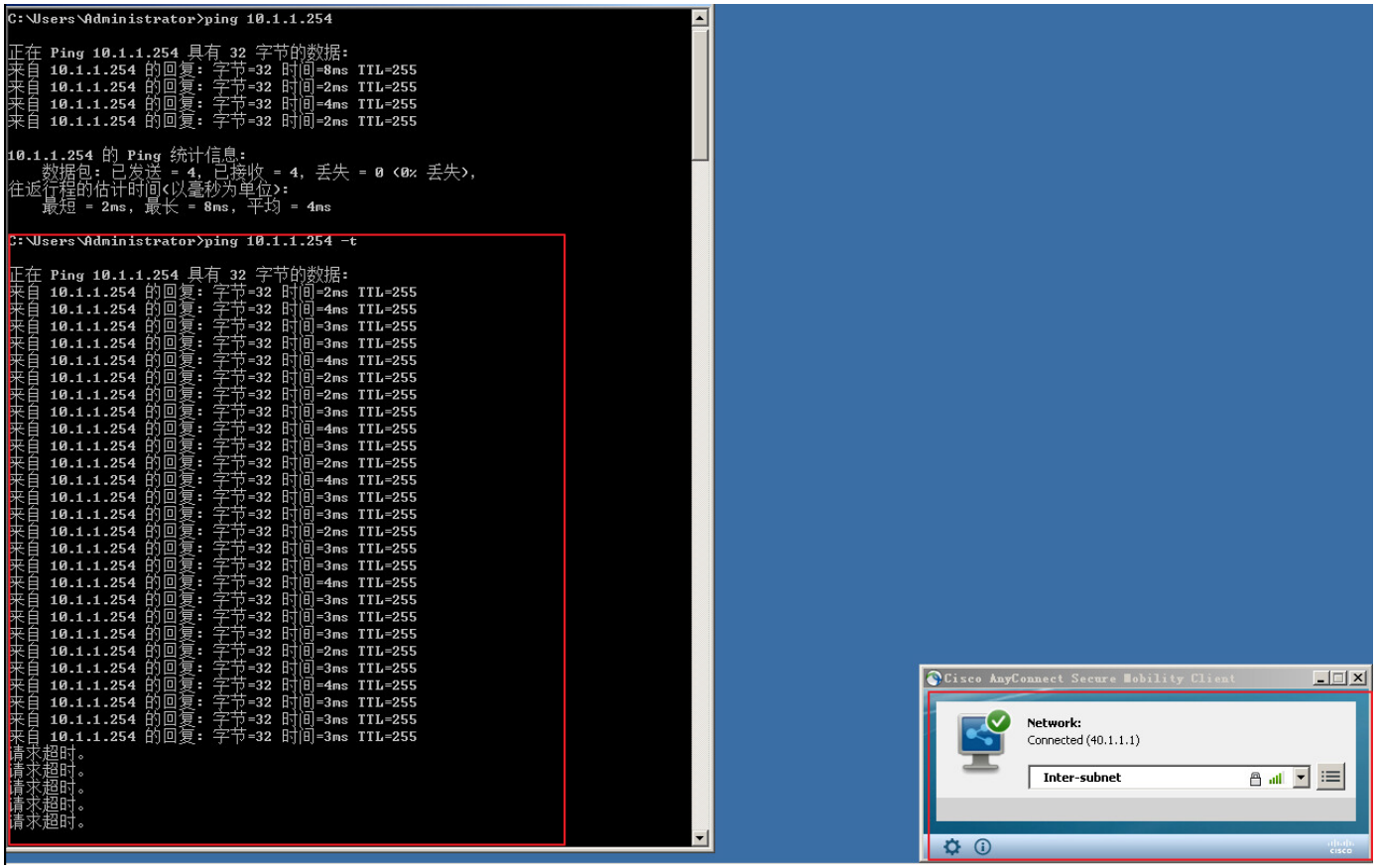
三层锚效果


WLC-2上的ACL
并没有任何作用
WLC5508-1
WLC5508-2
AP1
AP2
虽然关联到AP2，但是
流量被锚回到WLC1
获取30.1.1.0/24的地址
Wireless-Test

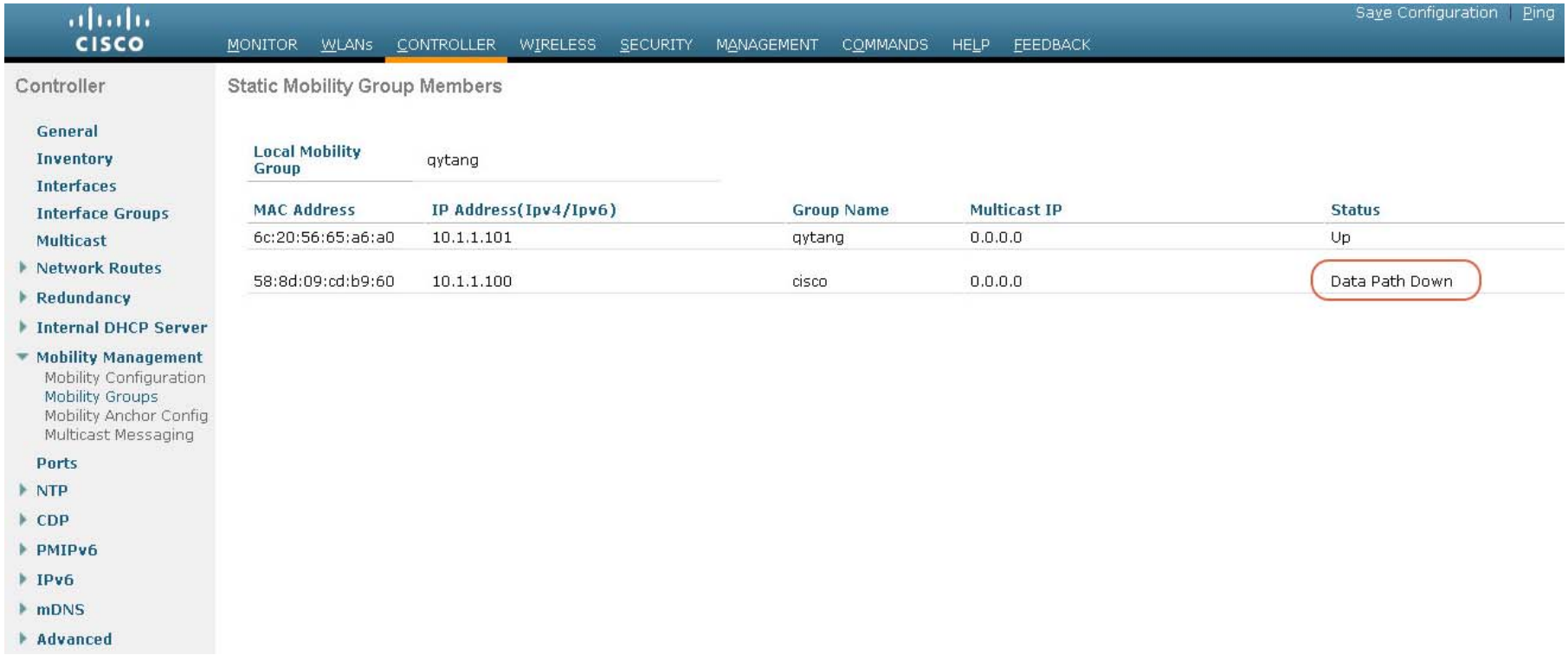
SW3560 设置列表

```
SW3560(config)#access-list 100 deny   97 any any
SW3560(config)#access-list 100 permit ip any any
SW3560(config)#int g0/1
SW3560(config-if)#ip access-group 100 in
```

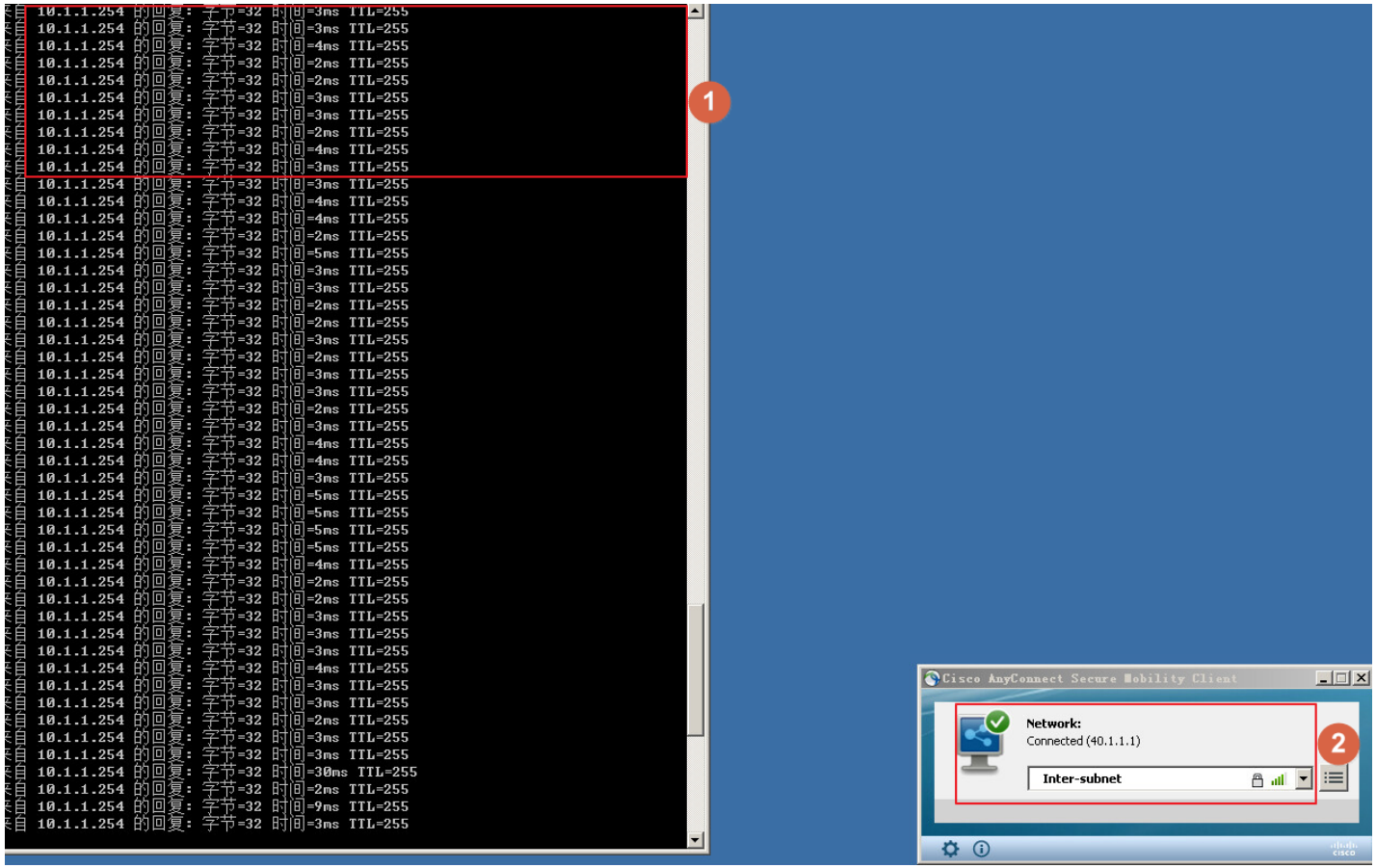
Test-PC 测试效果


C:\Users\Administrator>ping 10.1.1.254
正在 Ping 10.1.1.254 具有 32 字节的数据:
来自 10.1.1.254 的回复: 字节=32 时间=8ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
10.1.1.254 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 2ms, 最长 = 8ms, 平均 = 4ms
C:\Users\Administrator>ping 10.1.1.254 -t
正在 Ping 10.1.1.254 具有 32 字节的数据:
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
Cisco AnyConnect Secure Mobility Client
Network:
Connected (40.1.1.1)
Inter-subnet

数据路径Down


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Mobility Configuration
Mobility Groups
Mobility Anchor Config
Multicast Messaging
Ports
NTP
CDP
PMIPv6
IPv6
mDNS
Advanced
Static Mobility Group Members
Local Mobility Group
qytang
MAC Address
IP Address(Ipv4/Ipv6)
Group Name
Multicast IP
Status
6c:20:56:65:a6:a0
10.1.1.101
qytang
0.0.0.0
Up
58:8d:09:cd:b9:60
10.1.1.100
cisco
0.0.0.0
Data Path Down

删除列表 Test-PC 测试效果

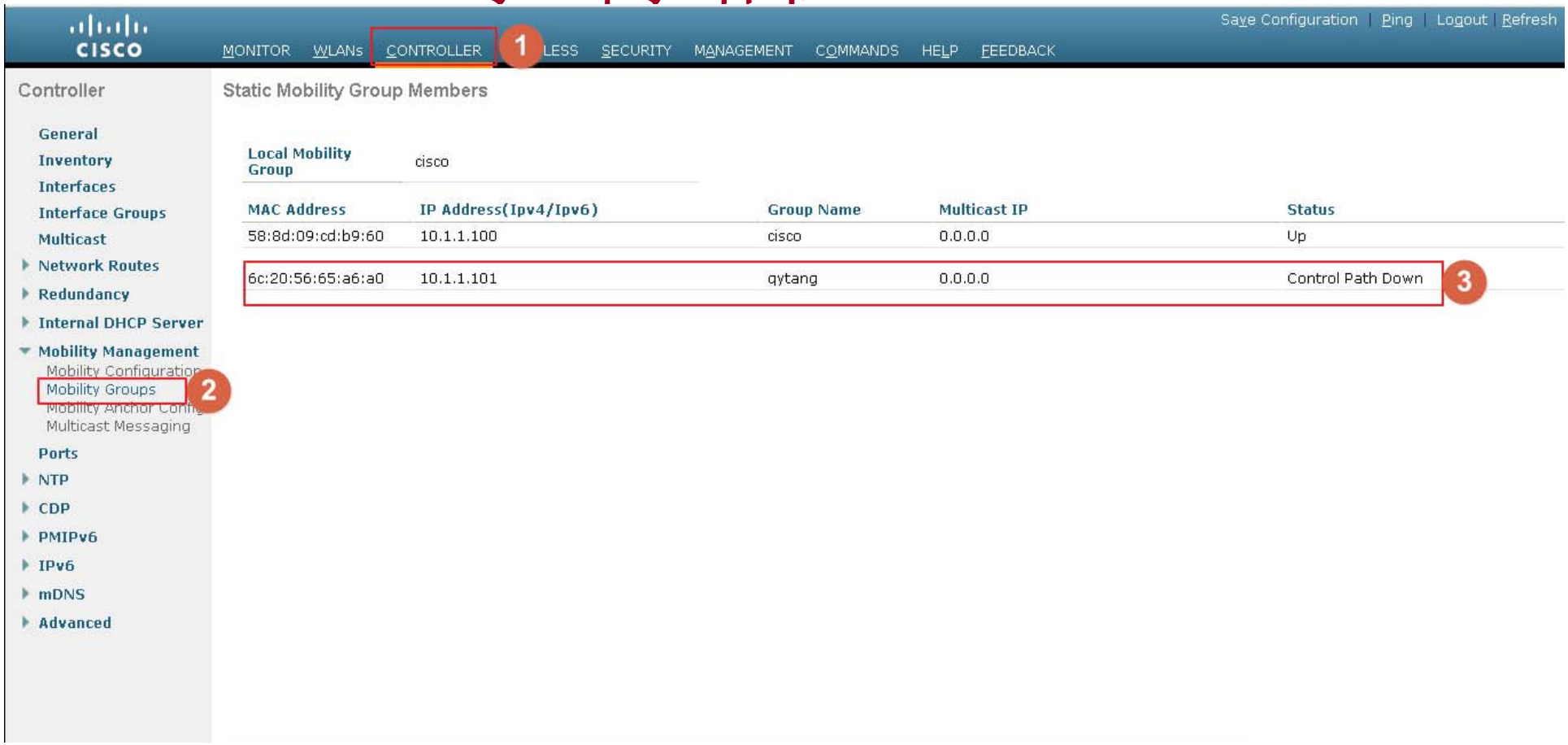


SW3560(config-if)#no ip access-group 100 in

SW3560 配置列表

```
SW3560(config)#access-list 101 deny   udp any any eq 16666
SW3560(config)#access-list 101 permit ip any any
SW3560(config)#interface  g0/1
SW3560(config-if)#ip access-group 101 in
```

控制路径Down

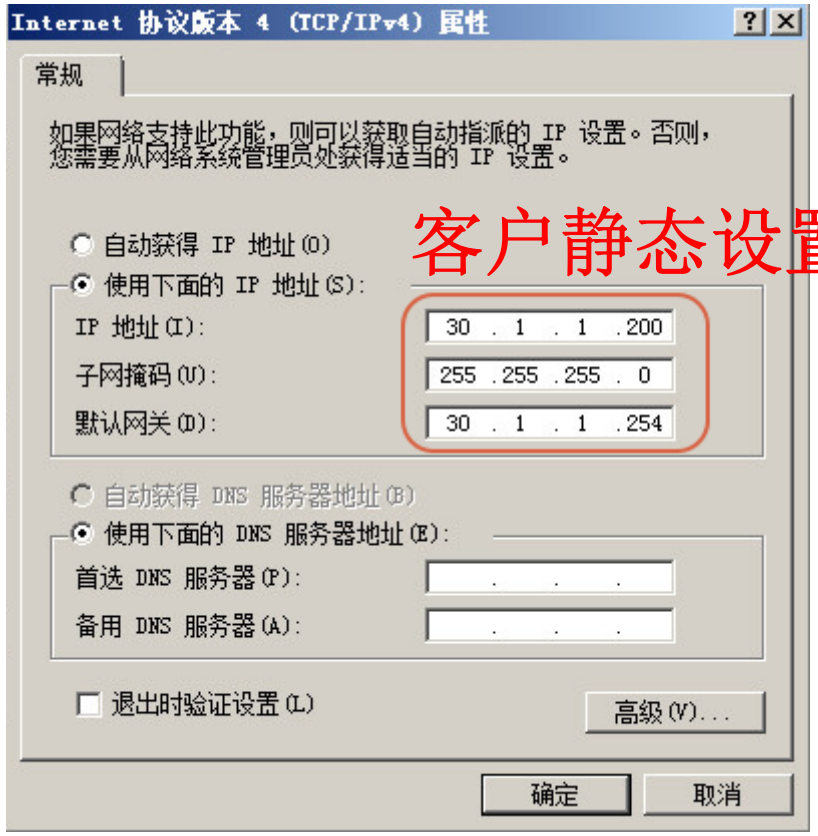

cisco
MONITOR
WLANs
CONTROLLER
1
LESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Save Configuration | Ping | Logout | Refresh
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Mobility Configuration
Mobility Groups
2
Multicast Messaging
Ports
NTP
CDP
PMIPv6
IPv6
mDNS
Advanced
Static Mobility Group Members
Local Mobility Group
cisco
MAC Address
IP Address(Ipv4/Ipv6)
Group Name
Multicast IP
Status
58:8d:09:cd:b9:60
10.1.1.100
cisco
0.0.0.0
Up
6c:20:56:65:a6:a0
10.1.1.101
qytang
0.0.0.0
Control Path Down
3

测试动态锚


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
OEAP ACLs
Network Lists
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
All APs
Entries 1 - 1 of 1
Current Filter
None
[Change Filter] [Clear Filter]
Number of APs
1
AP Name
IP Address(Ipv4/Ipv6)
AP Model
AP MAC
AP Up Time
Admin Stat
AP2
20.1.1.8
AIR-CAP1602I-C-K9
f0:7f:06:f0:97:d5
0 d, 05 h 43 m 26 s
Disabled

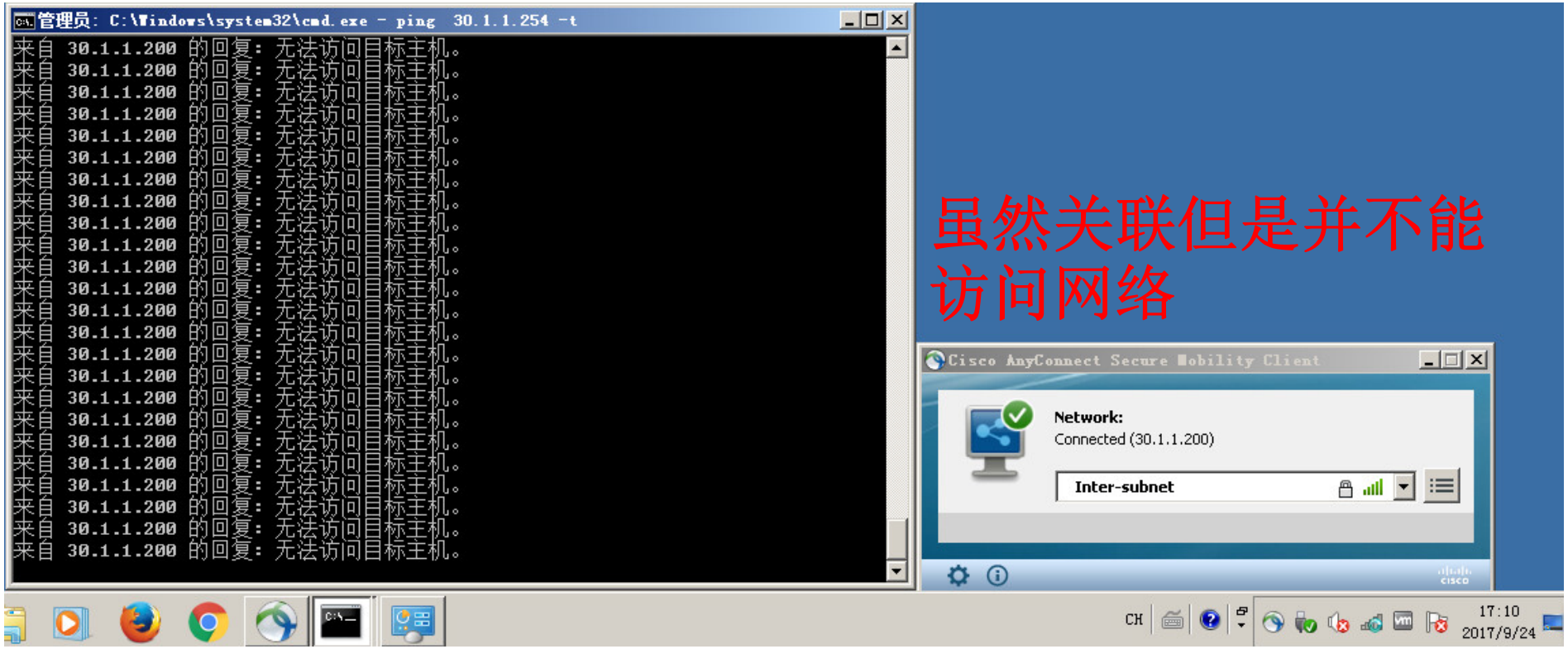
关闭AP2

测试动态锚

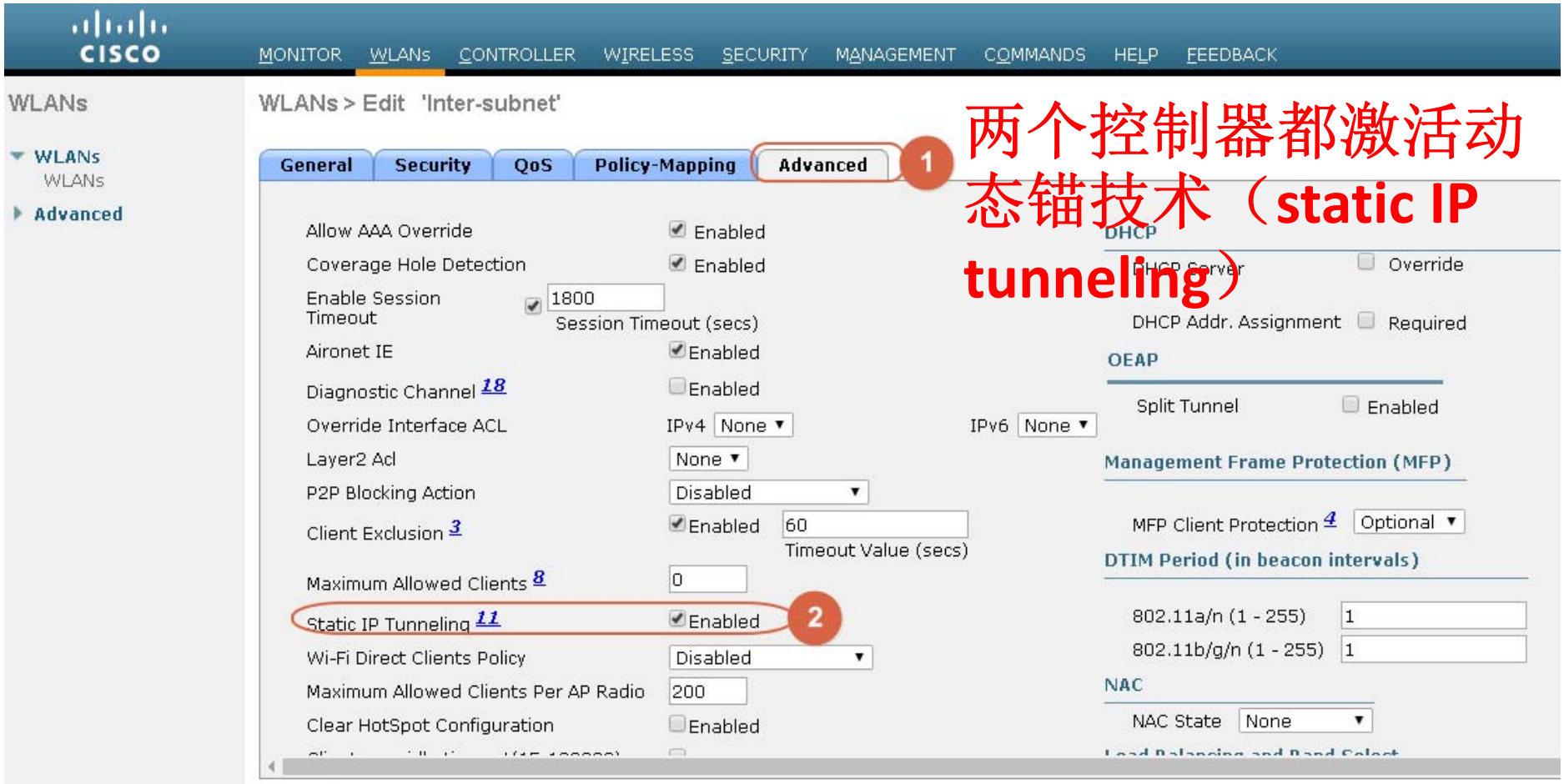


客户静态设置IP地址

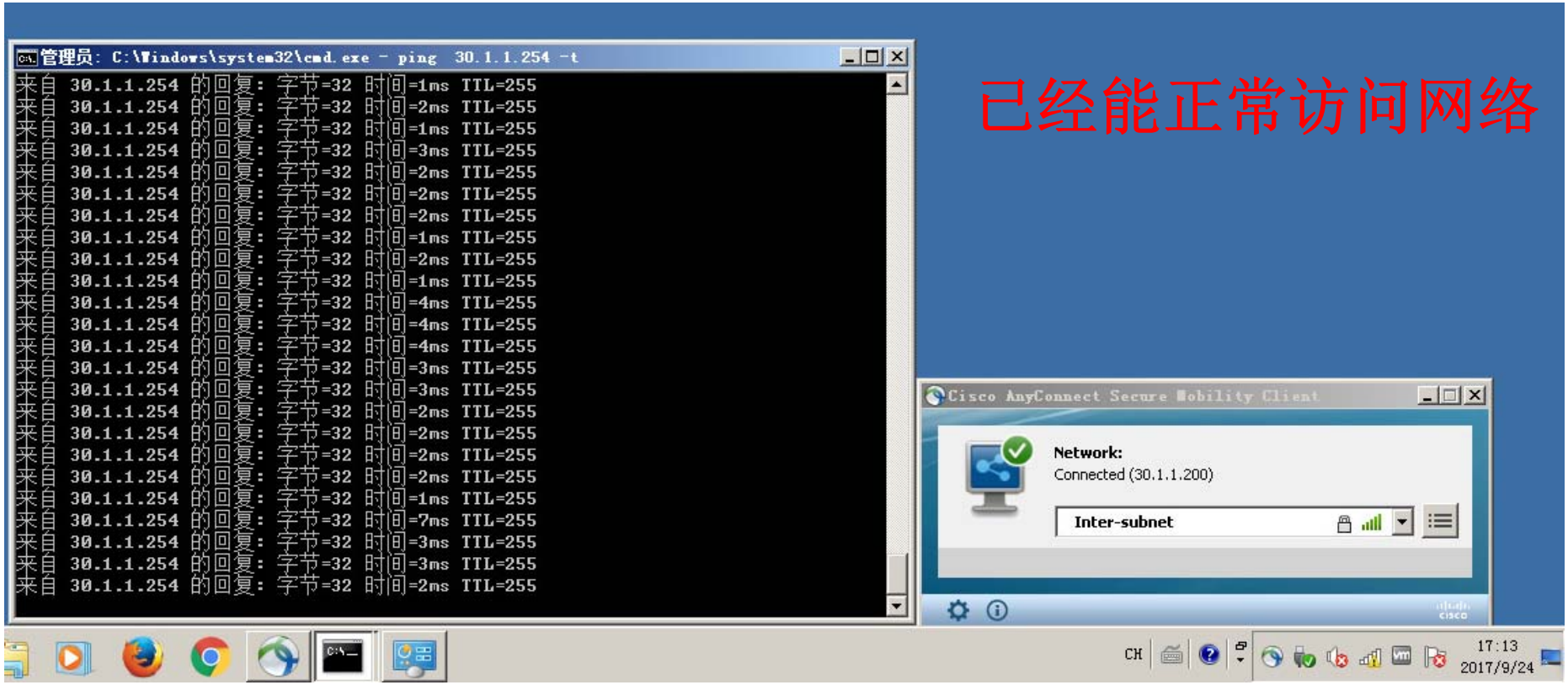
测试动态锚


管理员: C:\Windows\system32\cmd.exe - ping 30.1.1.254 -t
来自 30.1.1.200 的回复: 无法访问目标主机。
虽然关联但是并不能访问网络
Cisco AnyConnect Secure Mobility Client
Network:
Connected (30.1.1.200)
Inter-subnet
CH
17:10
2017/9/24

测试动态锚


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'Inter-subnet'
General Security QoS Policy-Mapping Advanced
1
两个控制器都激活动态锚技术（static IP tunneling）
Allow AAA Override Enabled
Coverage Hole Detection Enabled
Enable Session Timeout 1800 Session Timeout (secs)
Aironet IE Enabled
Diagnostic Channel 18 Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
P2P Blocking Action Disabled
Client Exclusion 3 Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 Enabled
2
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration Enabled
DHCP
DHCP Server Override
DHCP Addr. Assignment Required
OEAP
Split Tunnel Enabled
Management Frame Protection (MFP)
MFP Client Protection 4 Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1
NAC
NAC State None

测试动态锚


管理员: C:\Windows\system32\cmd.exe - ping 30.1.1.254 -t
来自 30.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=4ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=1ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=7ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.254 的回复: 字节=32 时间=2ms TTL=255
已经能正常访问网络
Cisco AnyConnect Secure Mobility Client
Network:
Connected (30.1.1.200)
Inter-subnet
CH
17:13
2017/9/24

测试动态锚

WLC-1信息，客户端关联到AP1

WLC-2信息，客户端被动态锚到了AP2

测试动态锚

WLC-1信息，为外部标记

WLC-2信息，为锚标记