



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

融合网络无线控制器

第一部分: AireOS漫游



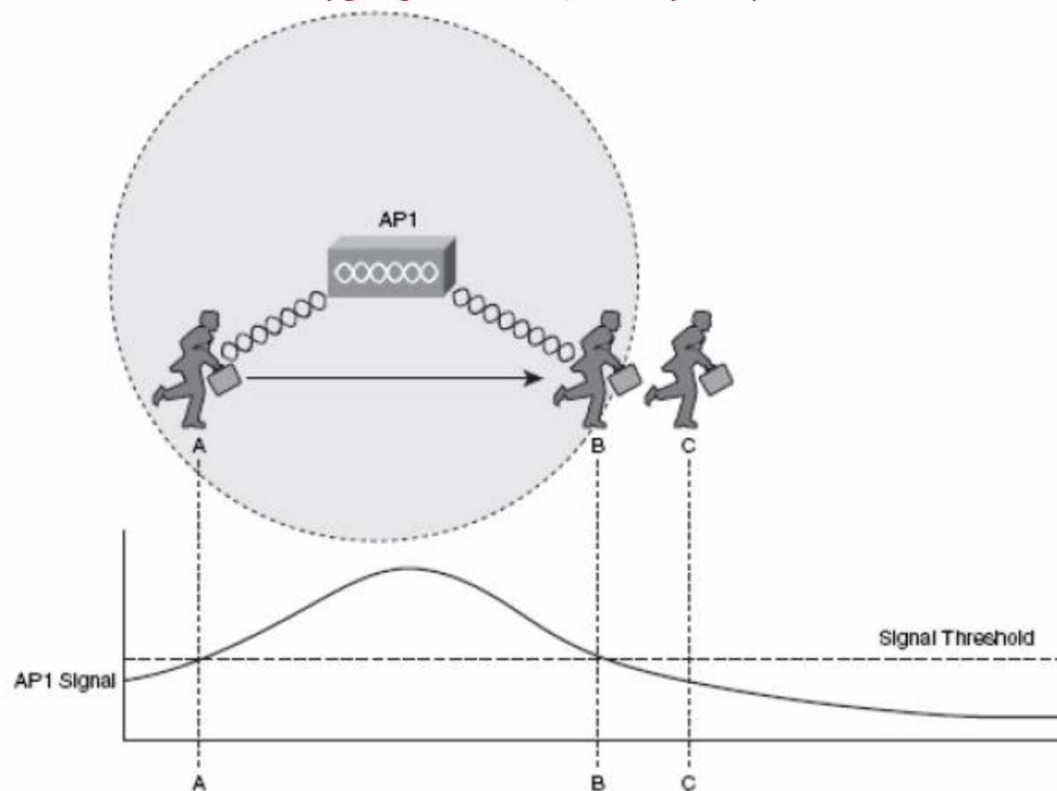
现任明教教主

融合网络无线控制器

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**阈值**,导致客户端失去关联。



漫游

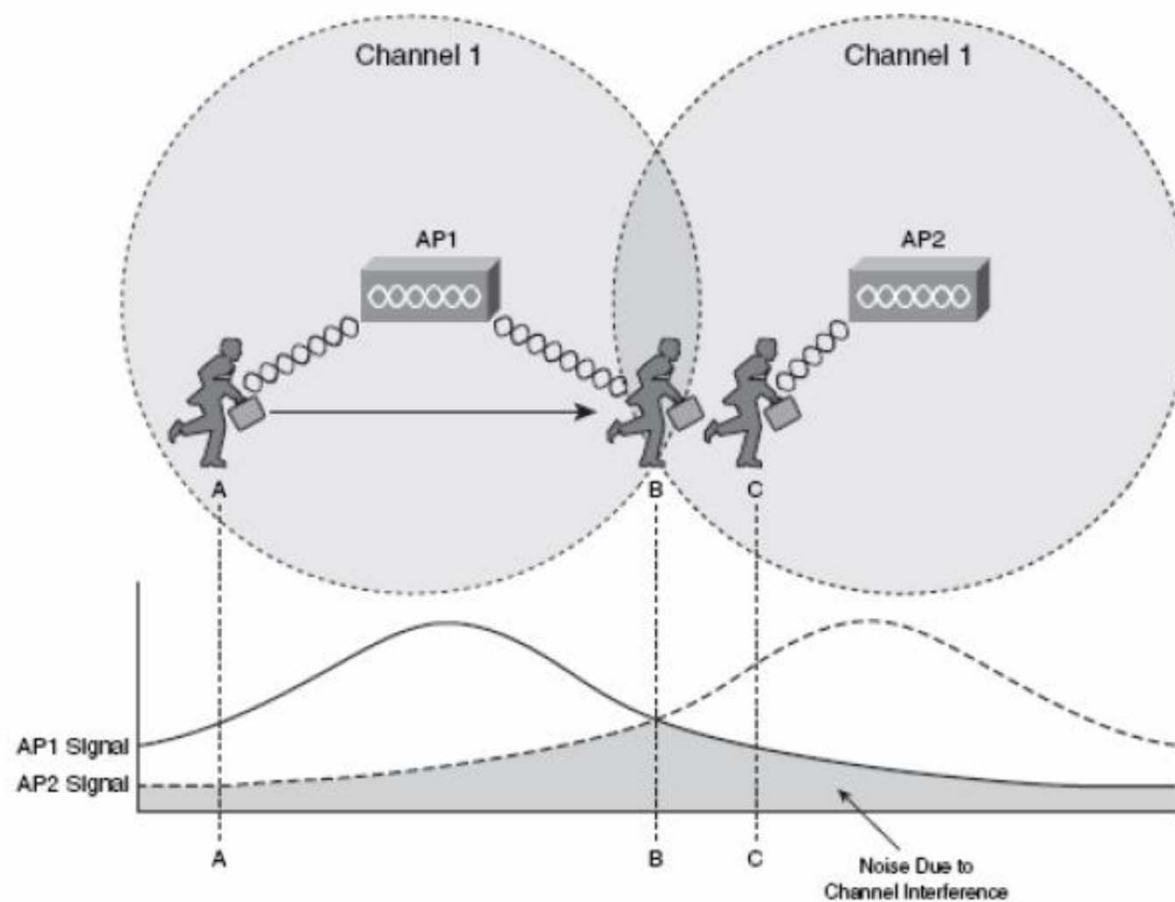
漫游指的是从一个**AP**将关联切换到与另一个**AP**关联，让无线连接在客户端移动时能够保持的过程。

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





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阈值，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

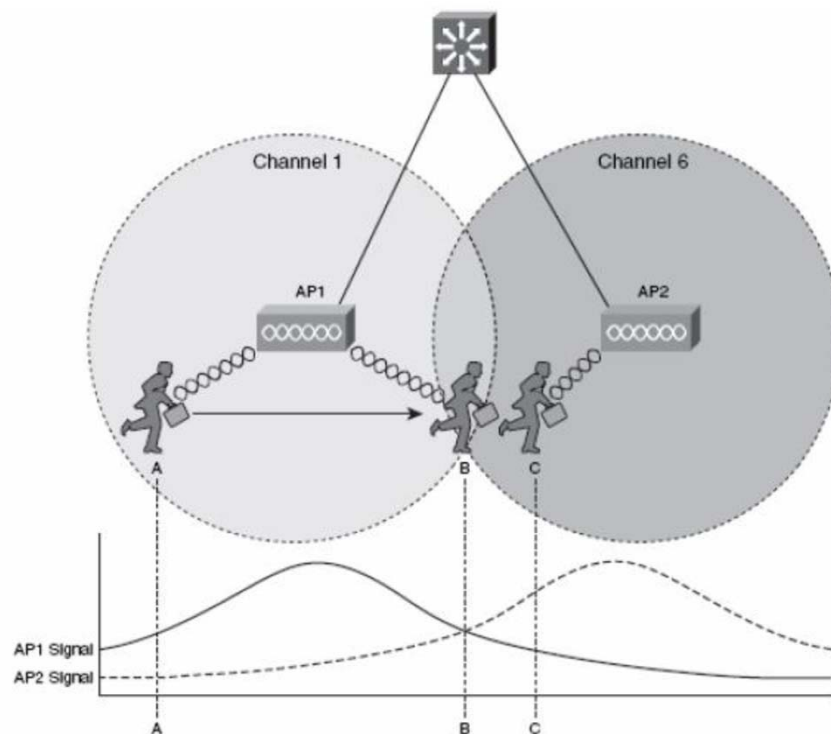
客户端确定应该漫游后，它**首先必须搜索潜在的新AP，这是通过扫描其他信道以找到其他活动AP实现的**，客户端采取两种方法来执行扫描过程：

- **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

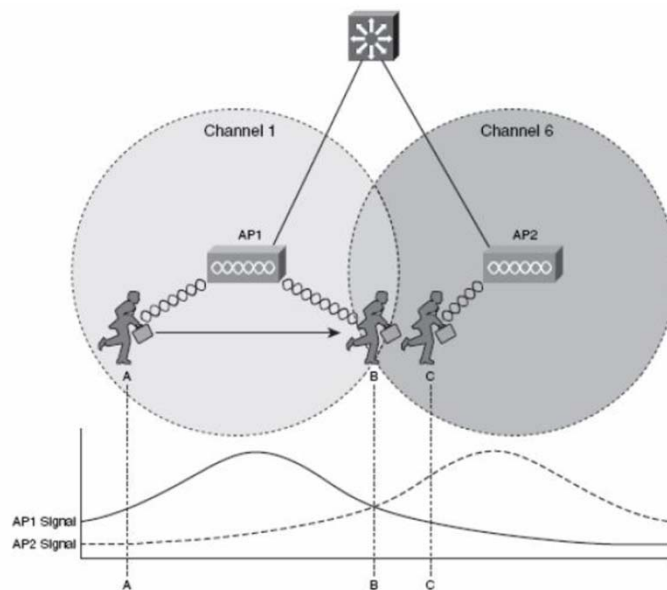
客户端移到位置B附近时, 在各种信道中发送802.11探针请求帧。AP2在信道6中收到探针请求后, 它通过在信道6中发送探针应答来进行响应, 客户端收到探针应答后, 对其进行评估, 以确定同哪个AP关联是最合适的。

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。



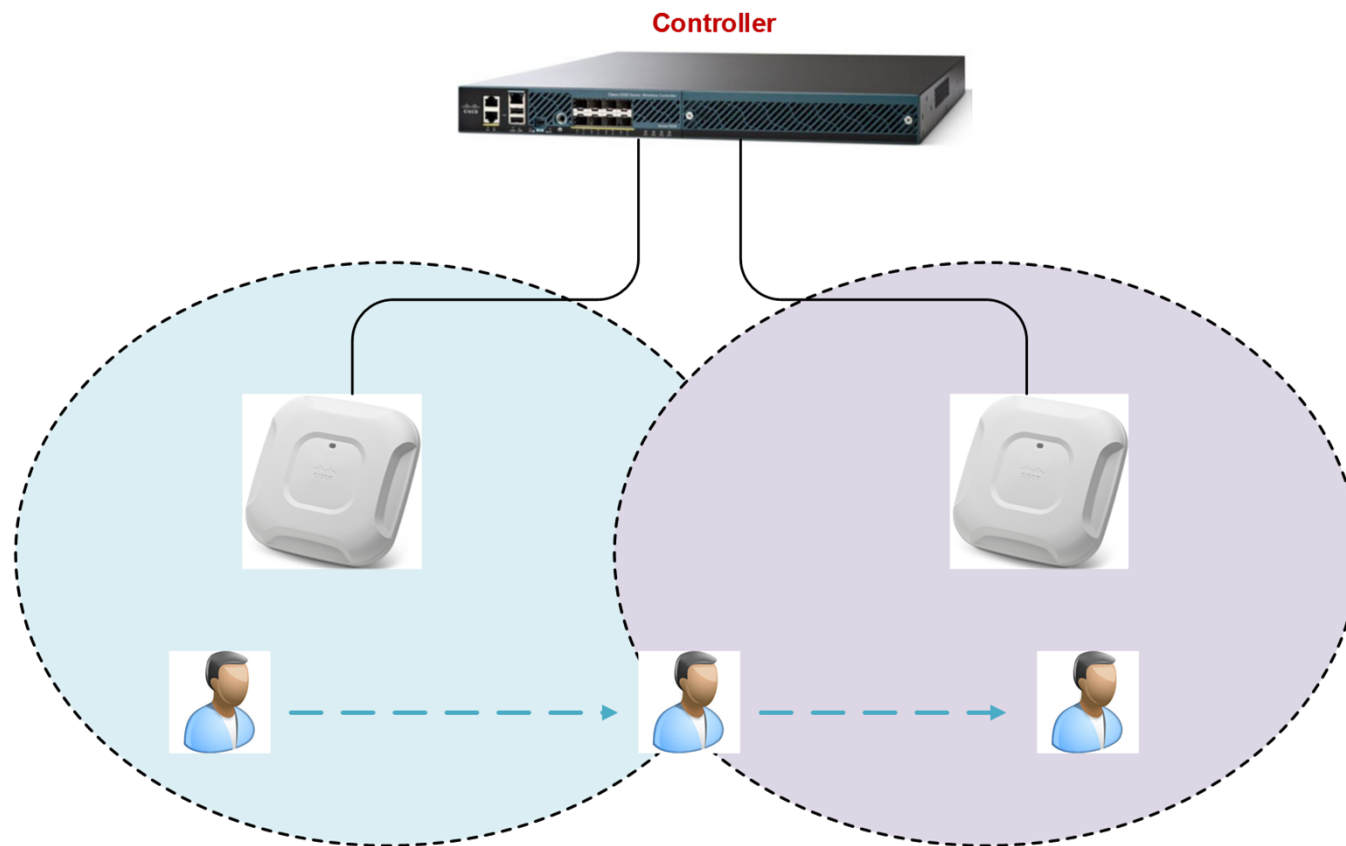
Intra-Controller Roaming

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



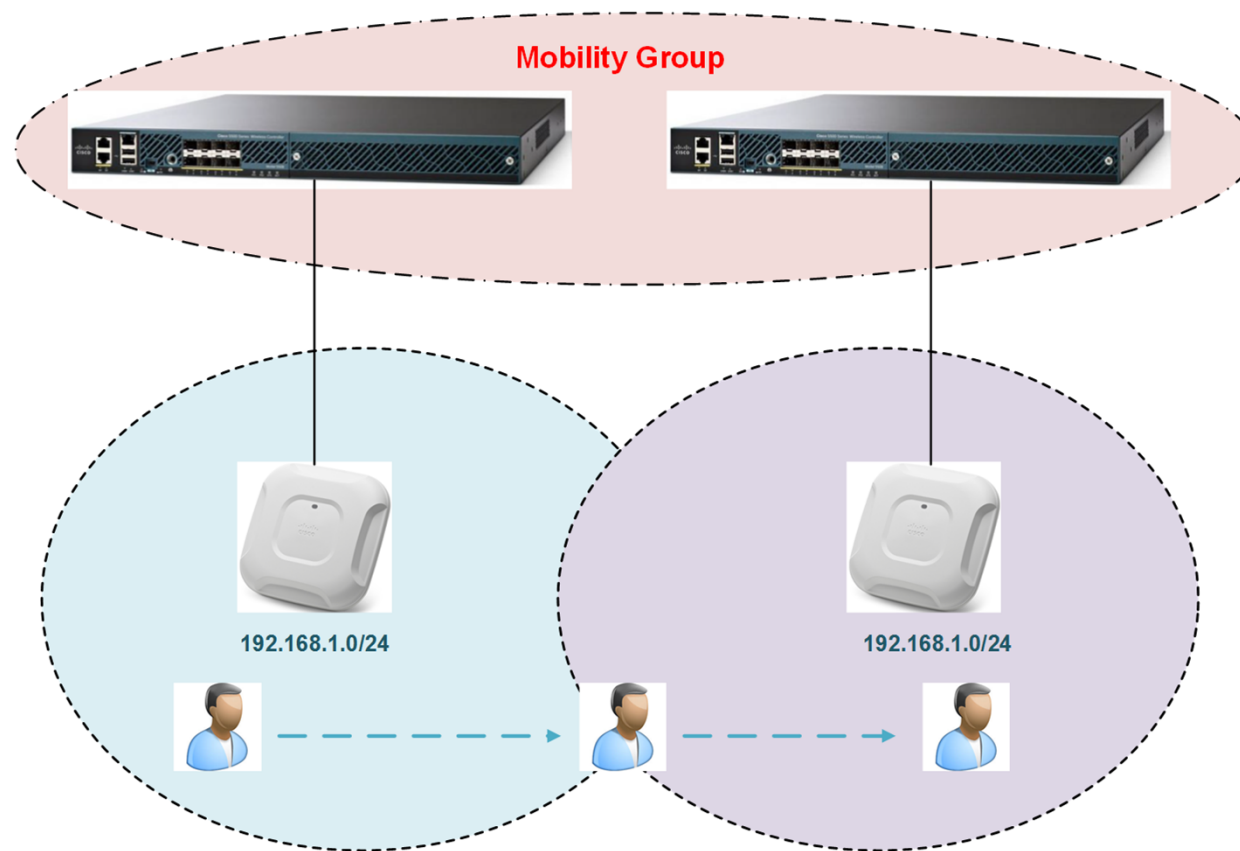


Inter-Controller Roaming

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



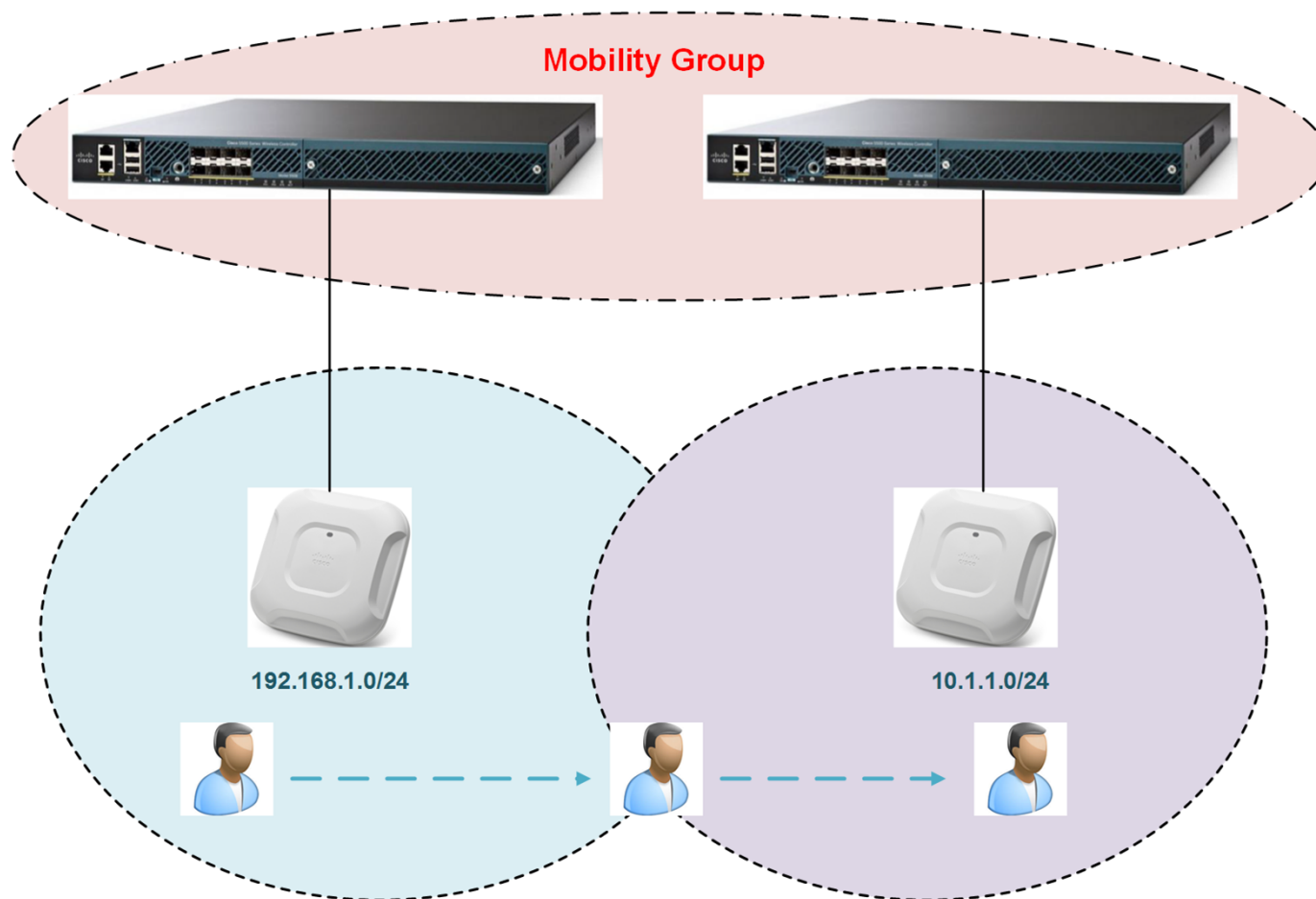


Inter-Subnet Roaming

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.



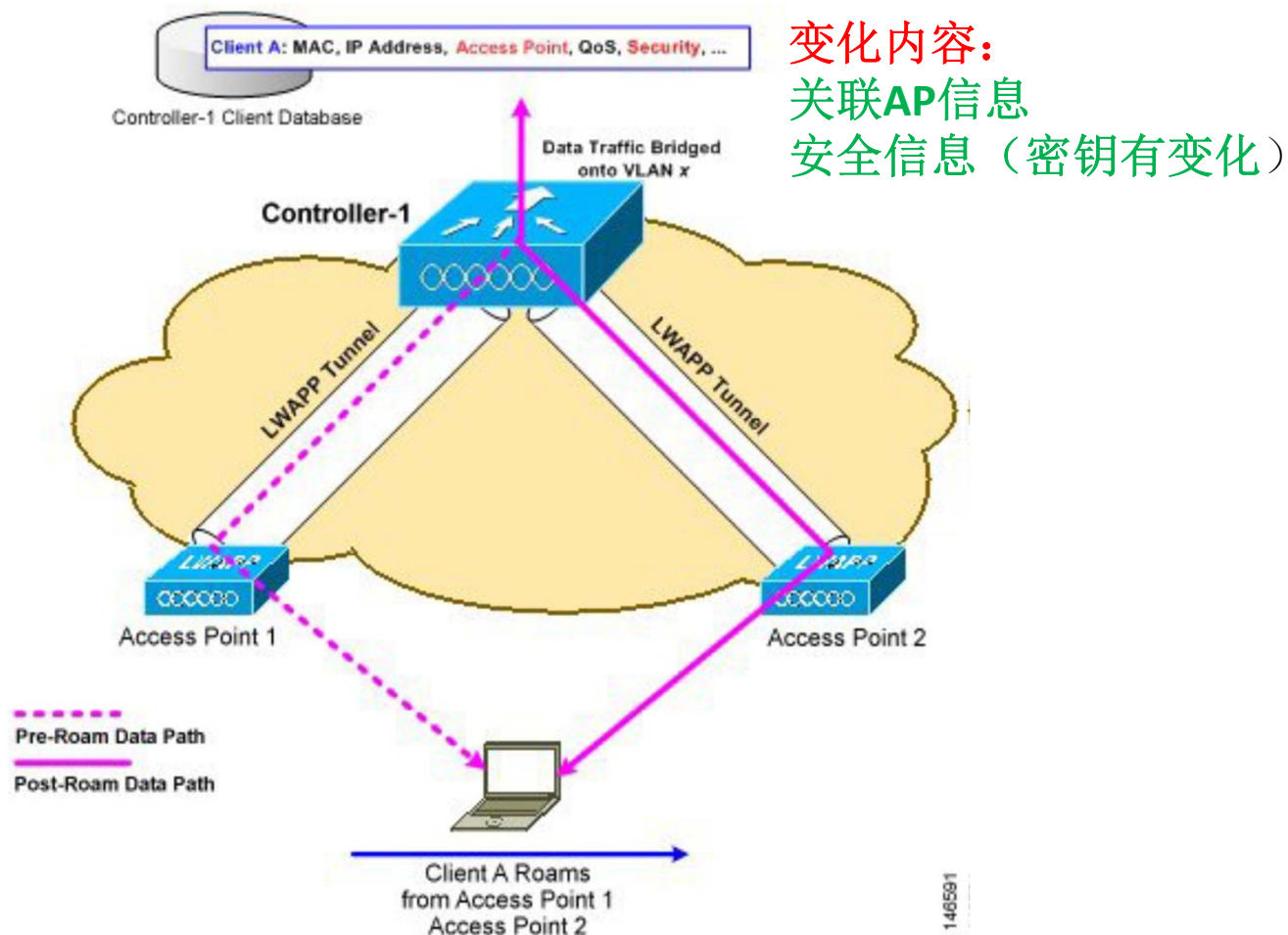
Mobility

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.



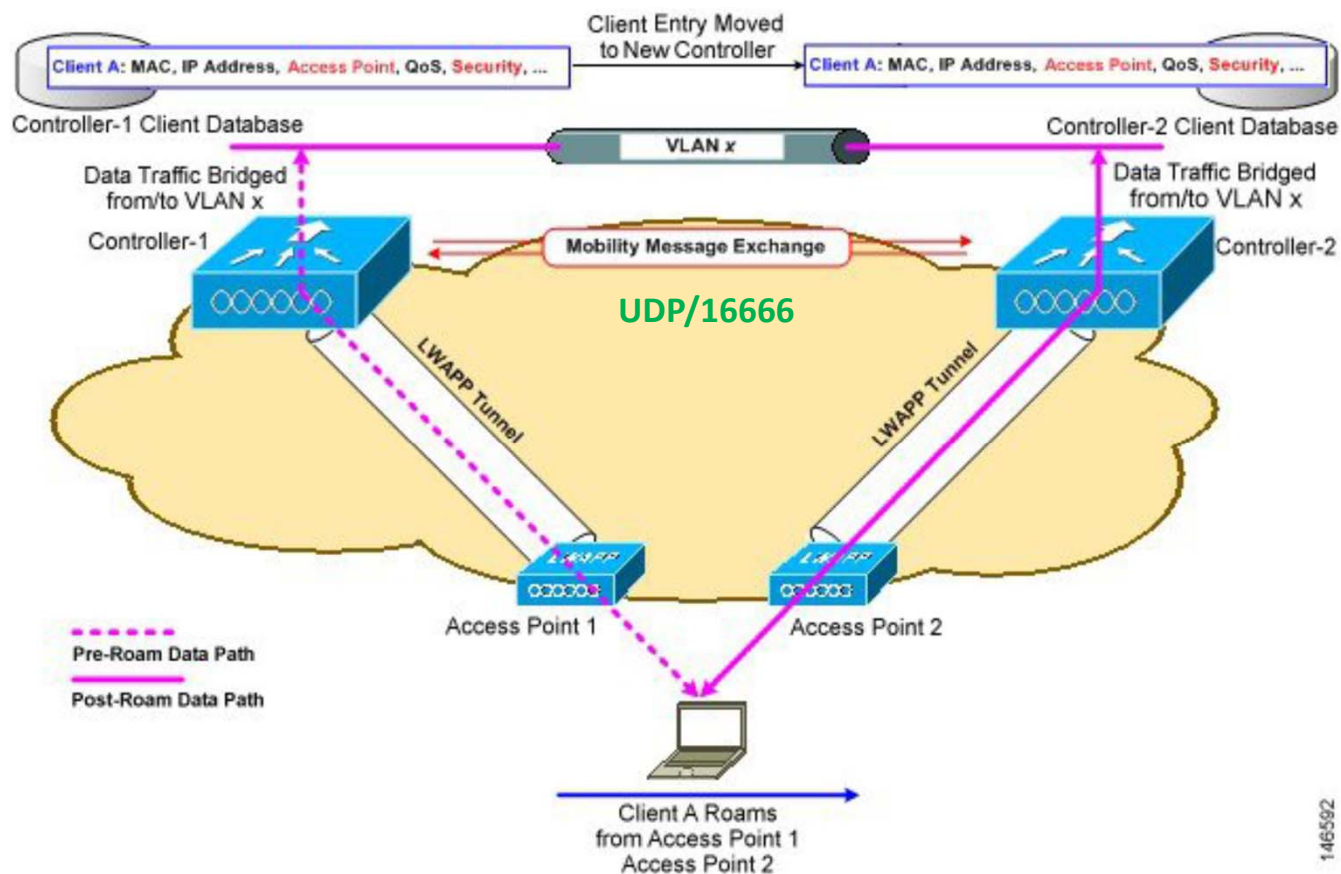
Intra-Controller Roaming





Inter-Controller Roaming

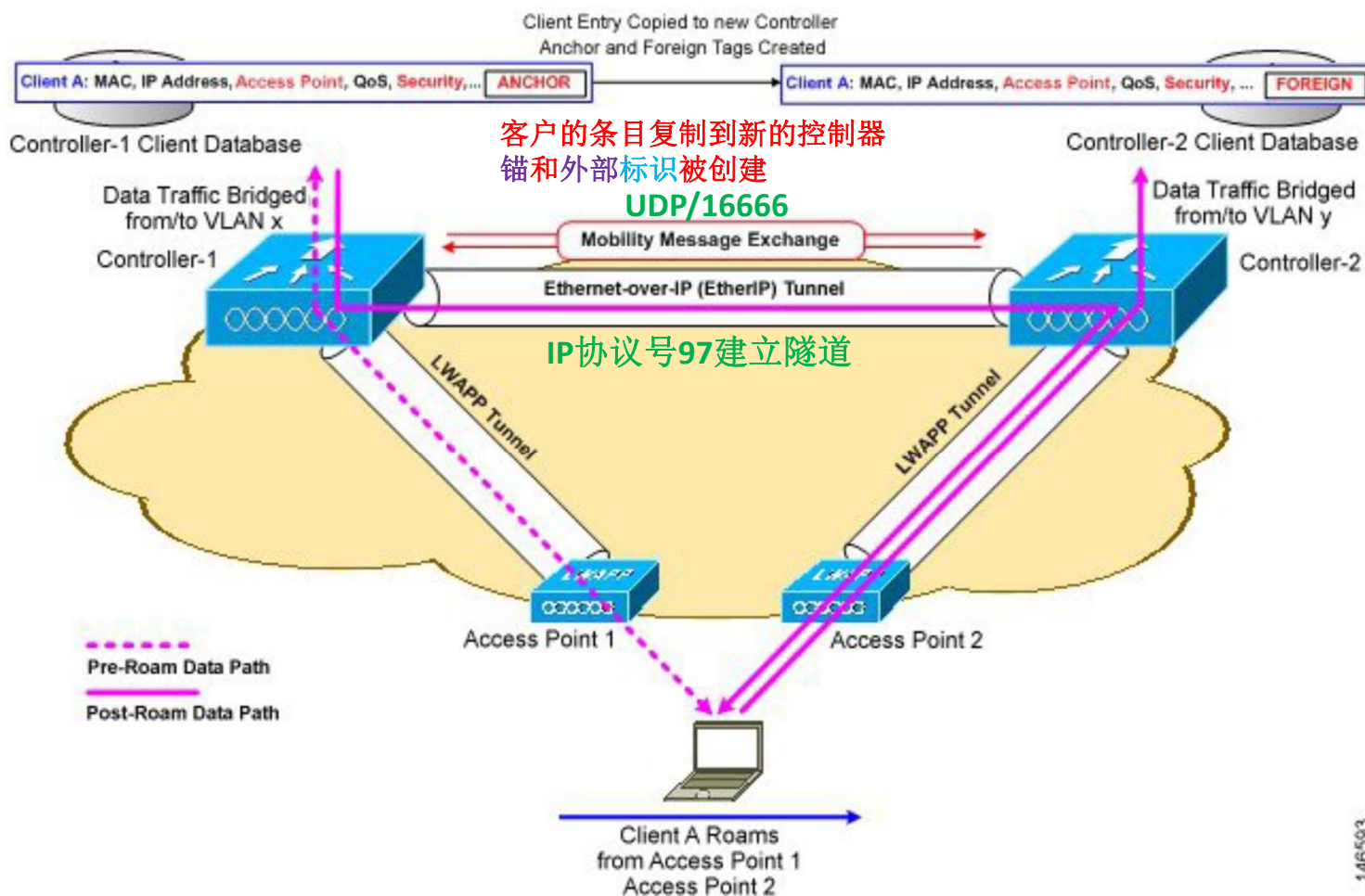
客户的条目移动到新的控制器



146592



Inter-Subnet Roaming





Mobility Group

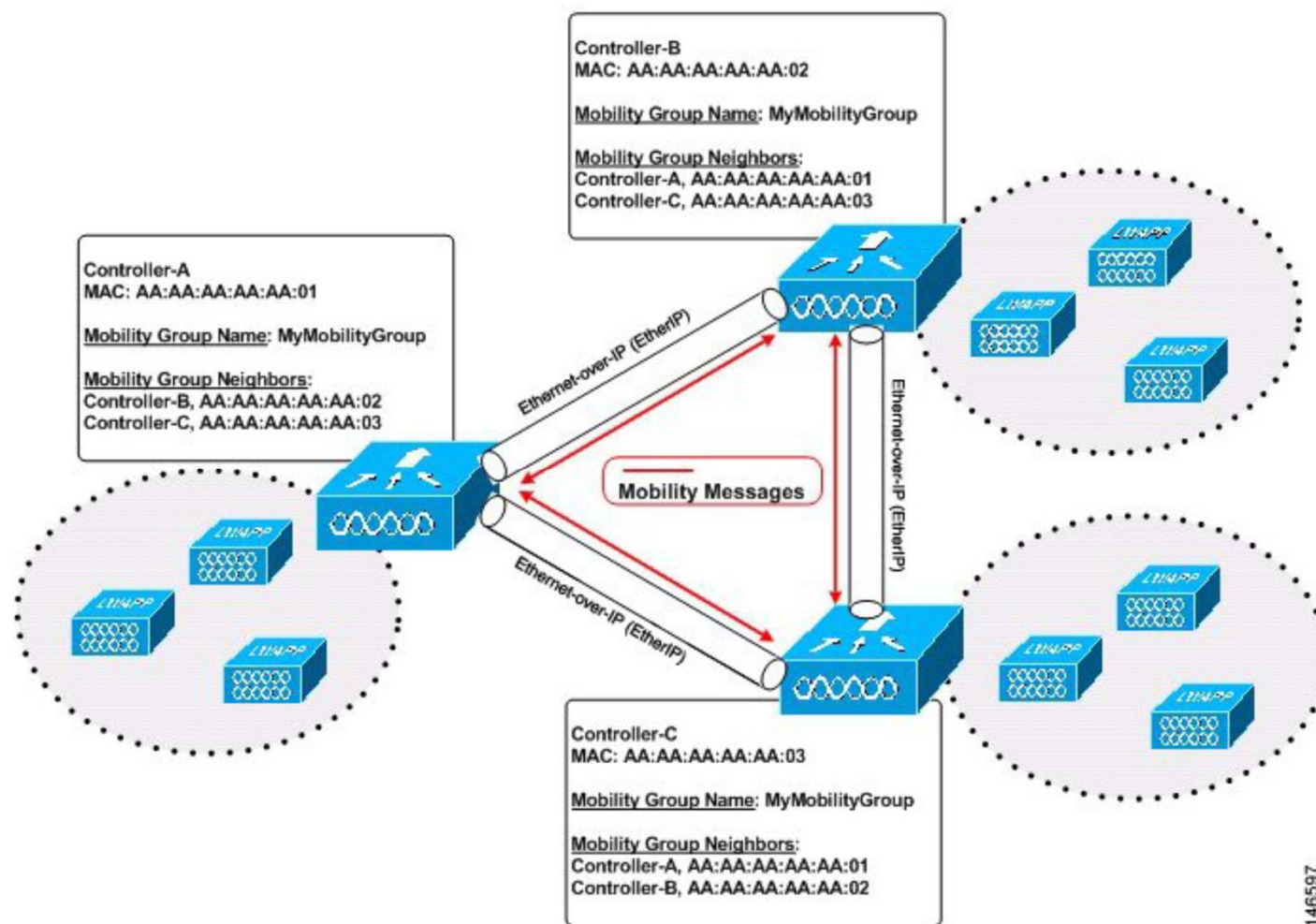
A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients.

(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。)

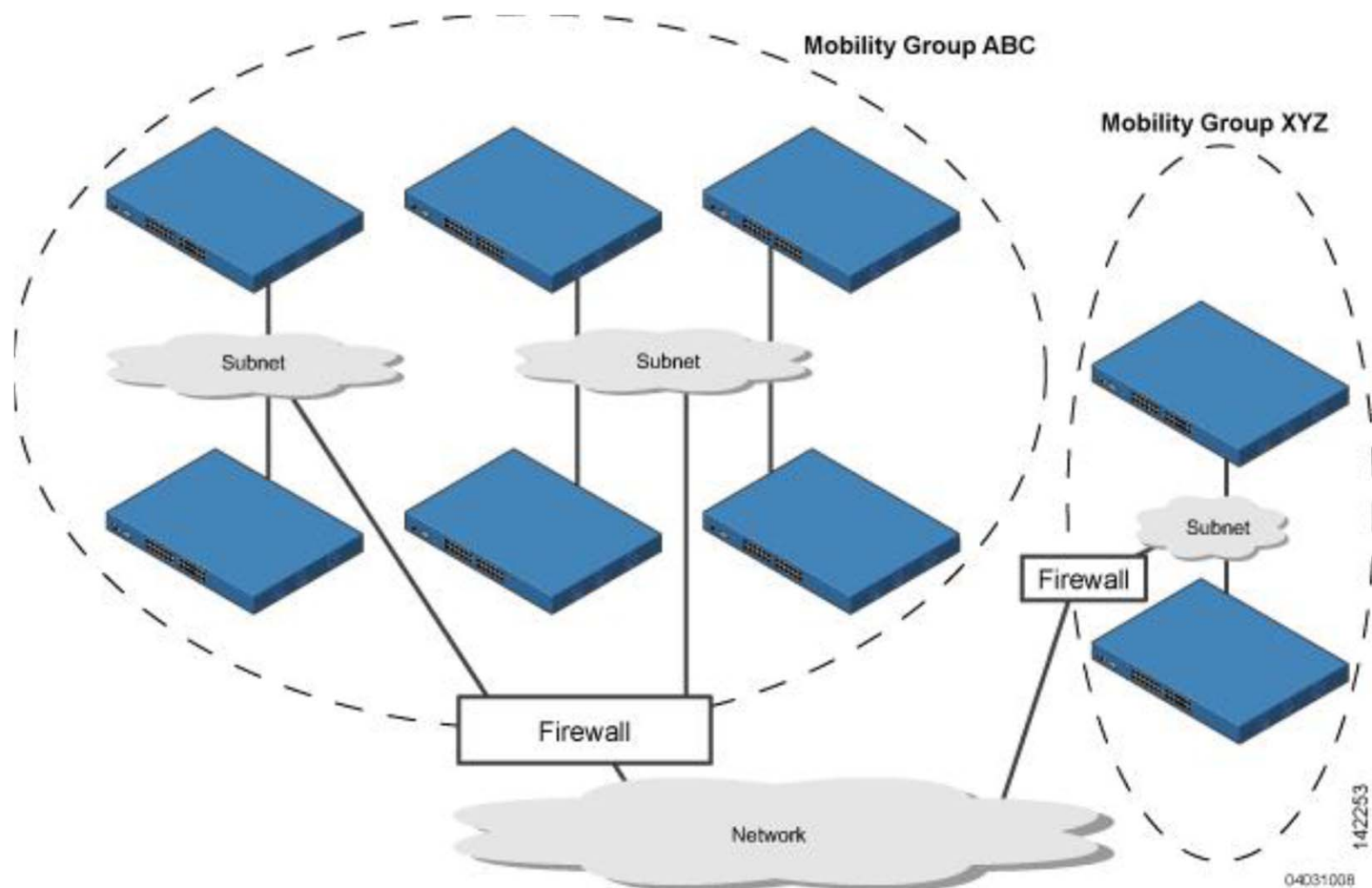


Mobility Group 信息交换





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



Mobility List

The screenshot shows the Cisco AireOS web interface for Mobility Management. The 'CONTROLLER' tab is selected. In the left sidebar, 'Mobility Management' is expanded, and 'Mobility Groups' is highlighted. The main content area shows 'Static Mobility Group Members' with a table of configurations. A 'Local Mobility Group' named 'cisco' is highlighted. The table lists two mobility groups: 'cisco' and 'qytang'.

MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP
58:8d:09:cd:b9:60	10.1.1.100	cisco	0.0.0.0
6c:20:56:65:a6:a0	10.1.1.101	qytang	0.0.0.0



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. (上一頁的圖, 先发**group**內, 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

The screenshot displays the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected and highlighted with a red box and a red circle containing the number '1'. The left sidebar shows the 'Controller' menu with 'Multicast Messaging' highlighted by a red box and a red circle containing the number '2'. The main configuration area is titled 'Mobility Multicast Messaging' and contains two fields: 'Enable Multicast Messaging' with an unchecked checkbox, and 'Local Group Multicast IPv4 Address' with an empty text box. Both fields are enclosed in a red box, and a red circle containing the number '3' is positioned to the right of the text box.



Mobility Group Guideline

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

The screenshot shows the Cisco WLAN configuration interface. The browser address bar displays `https://10.1.1.100/screens/frameset.html`. The navigation bar includes 'MONITOR', 'WLANs', 'ROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' section is active, showing 'Entries 1 - 2 of 2'. A table lists two profiles:

Profile Name	WLAN SSID	Admin Status	Security Policies
qytang	qytang	Enabled	[WPA2][Auth(802.1X)]
Inter-subnet	Inter-subnet	Enabled	[WPA2][Auth(802.1X)]

A context menu is open for the 'Inter-subnet' profile, with 'Mobility Anchors' selected. The menu items are: Remove, Mobility Anchors, 802.11u, Foreign Maps, Service Advertisements, and Hotspot 2.0.



Multiple Anchor

The screenshot displays the Cisco AireOS configuration page for Mobility Anchors. The interface includes a top navigation bar with the Cisco logo and various menu items like MONITOR, WLANs, ROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The main content area is titled 'Mobility Anchors' and features a '< Back' button. A table lists the configuration for a specific anchor:

WLAN SSID	Inter-subnet
Switch IP Address (Anchor)	
local	
Data Path	up
Control Path	up <input checked="" type="checkbox"/>

Below the table, there is a 'Mobility Anchor Create' button and a 'Switch IP Address (Anchor)' dropdown menu set to '10.1.1.101'. Red circles with numbers 1 through 4 highlight key elements: 1. WLANs menu, 2. WLANs sub-menu, 3. WLAN SSID field, and 4. Mobility Anchor Create button.



Multiple Anchor

WLANs

WLANs

Advanced

Mobility Anchors

WLAN SSID Inter-subnet

Switch IP Address (Anchor)	Data Path	Control Path
local	up	up
10.1.1.101	up	up

Mobility Anchor Create

Switch IP Address (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

The screenshot displays the Cisco Wireless LAN Controller configuration interface for a Dynamic Anchor. The configuration is for the WLAN named 'qytang'. The 'Advanced' tab is selected, showing various configuration options. Red circles highlight the following elements:

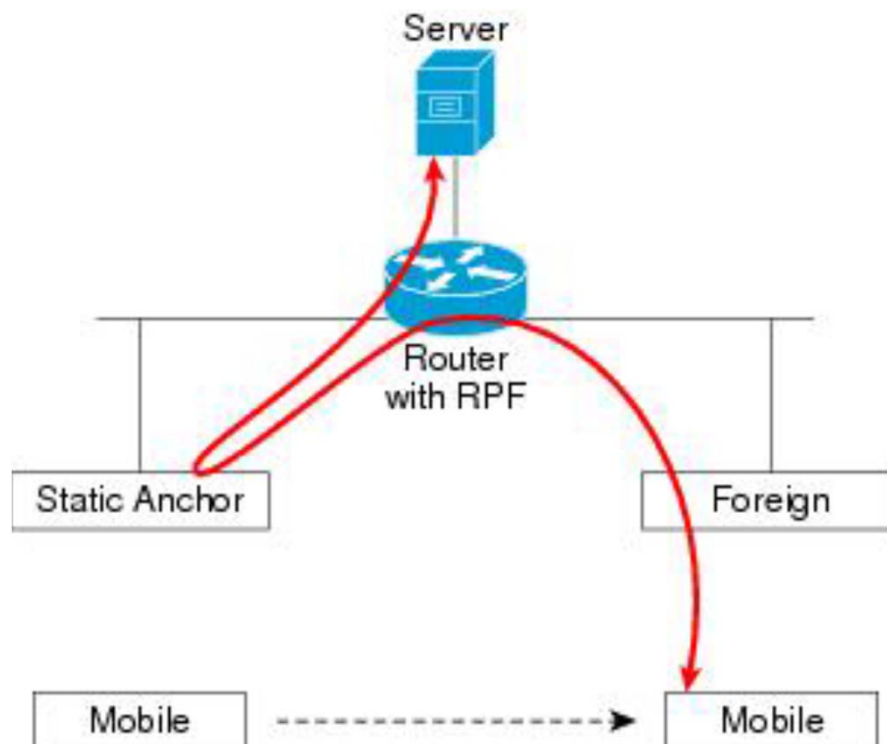
- 1. The 'WLANs' menu item in the top navigation bar.
- 2. The 'WLANs' sub-menu item in the left sidebar.
- 3. The 'Advanced' configuration tab.
- 4. The 'Static IP Tunneling' checkbox, which is currently checked.

Other visible configuration options include:

- Allow AAA Override: Enabled
- Coverage Hole Detection: Enabled
- Enable Session Timeout: 1800 (Session Timeout (secs))
- Aironet IE: Enabled
- Diagnostic Channel: Enabled
- Override Interface ACL: IPv4: None, IPv6: None
- Layer2 Ad: None
- P2P Blocking Action: Disabled
- Client Exclusion: Enabled, 60 (Timeout Value (secs))
- Maximum Allowed Clients: 0
- Static IP Tunneling: Enabled
- Wi-Fi Direct Clients Policy: Disabled
- Maximum Allowed Clients Per AP Radio: 200
- Clear HotSpot Configuration: Enabled
- Client user idle timeout (15 - 10000):
- DHCP: DHCP Server: Override, DHCP Addr. Assignment: Required
- OEAP: Split Tunnel: Enabled
- Management Frame Protection (MFP): MFP Client Protection: Optional
- DTIM Period (in beacon intervals): 802.11a/n (1 - 255): 1, 802.11b/g/n (1 - 255): 1
- NAC: NAC State: None
- Load Balancing and Band Select: (Section header)



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

The screenshot shows the Cisco AireOS configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected and highlighted with a red circle labeled '1'. On the left sidebar, the 'Mobility Management' section is expanded, and 'Mobility Anchor Config' is selected, highlighted with a red circle labeled '2'. The main configuration area, titled 'Mobility Anchor Config', contains the following settings:

Keep Alive Count	<input type="text" value="3"/>
Keep Alive Interval (1-30 seconds)	<input type="text" value="10"/>
Symmetric Mobility Tunneling mode	<input checked="" type="checkbox"/> Enabled 3
DSCP Value	<input type="text" value="0"/>



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

The screenshot shows the Cisco Mobility Anchors configuration page. The interface includes a top navigation bar with 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' menu is highlighted with a red box and a '1' callout. The left sidebar shows 'WLANs' expanded with 'WLANs' and 'Advanced' options, with 'WLANs' highlighted by a red box and a '2' callout. The main content area is titled 'Mobility Anchors' with a '< Back' button and a '3' callout. It displays a table with columns for 'WLAN SSID', 'Switch IP Address (Anchor)', 'Data Path', and 'Control Path'. The table contains two rows: 'local' and '10.1.1.101', both with 'up' in the Data Path and Control Path columns. A 'Remove' button is visible next to the '10.1.1.101' row, with a red box and a '4' callout. Below the table is a 'Mobility Anchor Create' button and a 'Switch IP Address (Anchor)' dropdown menu.

WLAN SSID	Switch IP Address (Anchor)	Data Path	Control Path
Inter-subnet	local	up	up
	10.1.1.101	up	up



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, 需要使用的話需要保存配置并且重启。)



New Mobility Group配置

The screenshot shows the Cisco AireOS configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected and highlighted with a red circle labeled '1'. The left sidebar shows a tree view with 'Mobility Management' expanded, and 'Mobility Configuration' selected, highlighted with a red circle labeled '2'. The main content area shows the 'Global Configuration' page for 'General', with the checkbox 'Enable New Mobility(Converged Access)' selected, highlighted with a red circle labeled '3'.



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:

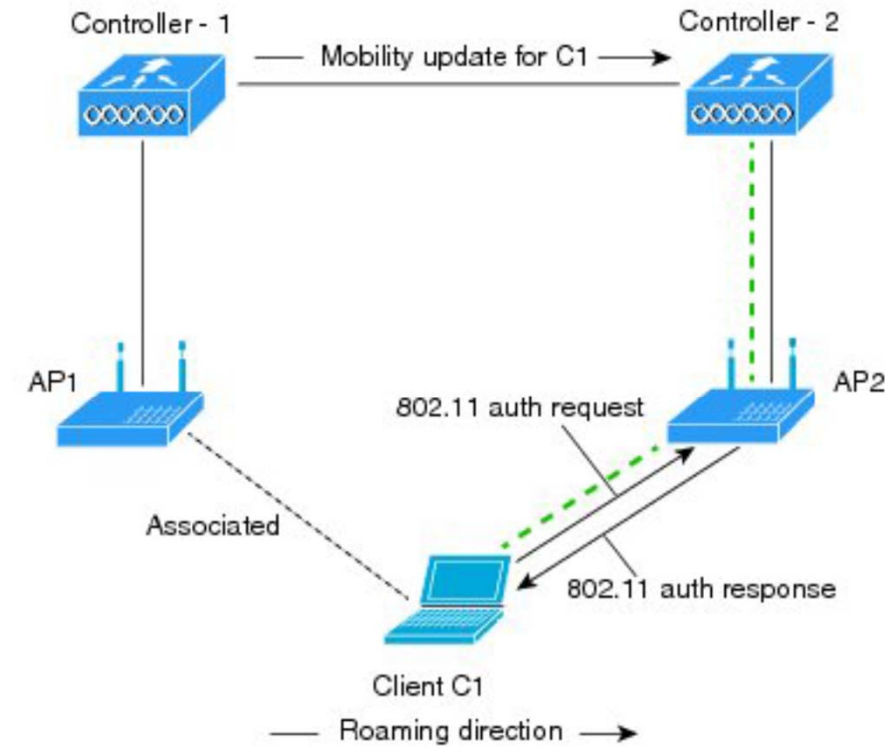
- **Over-the-Air**
- **Over-the-DS (Distribution System)**

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

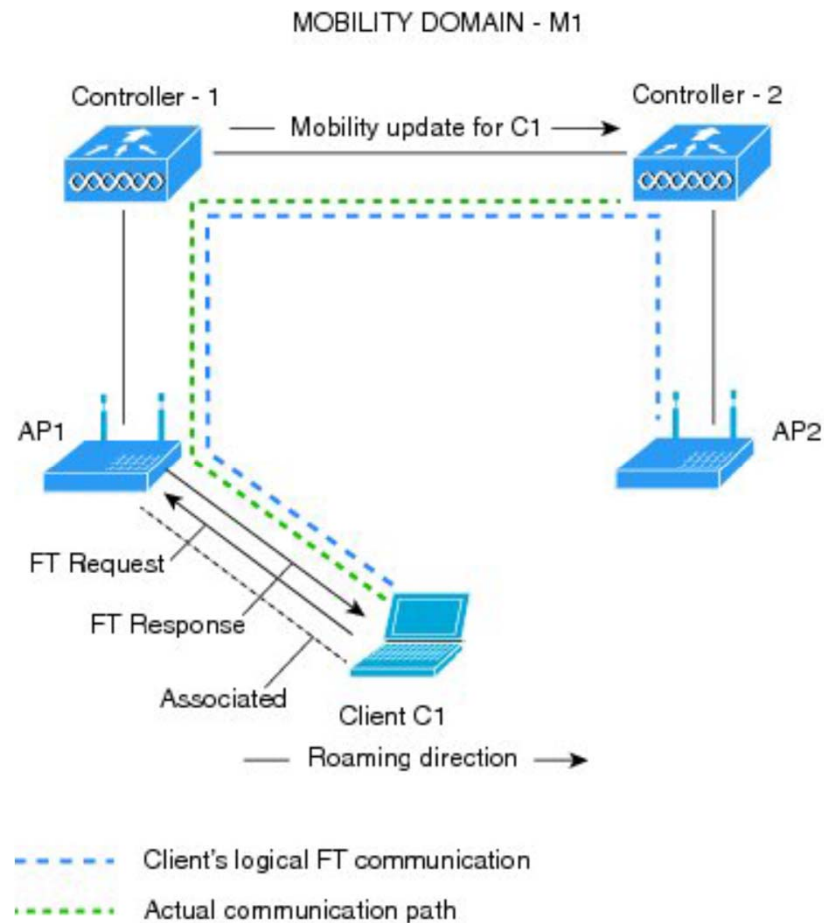
MOBILITY DOMAIN - M1



Actual communication path



Over-the-DS





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)

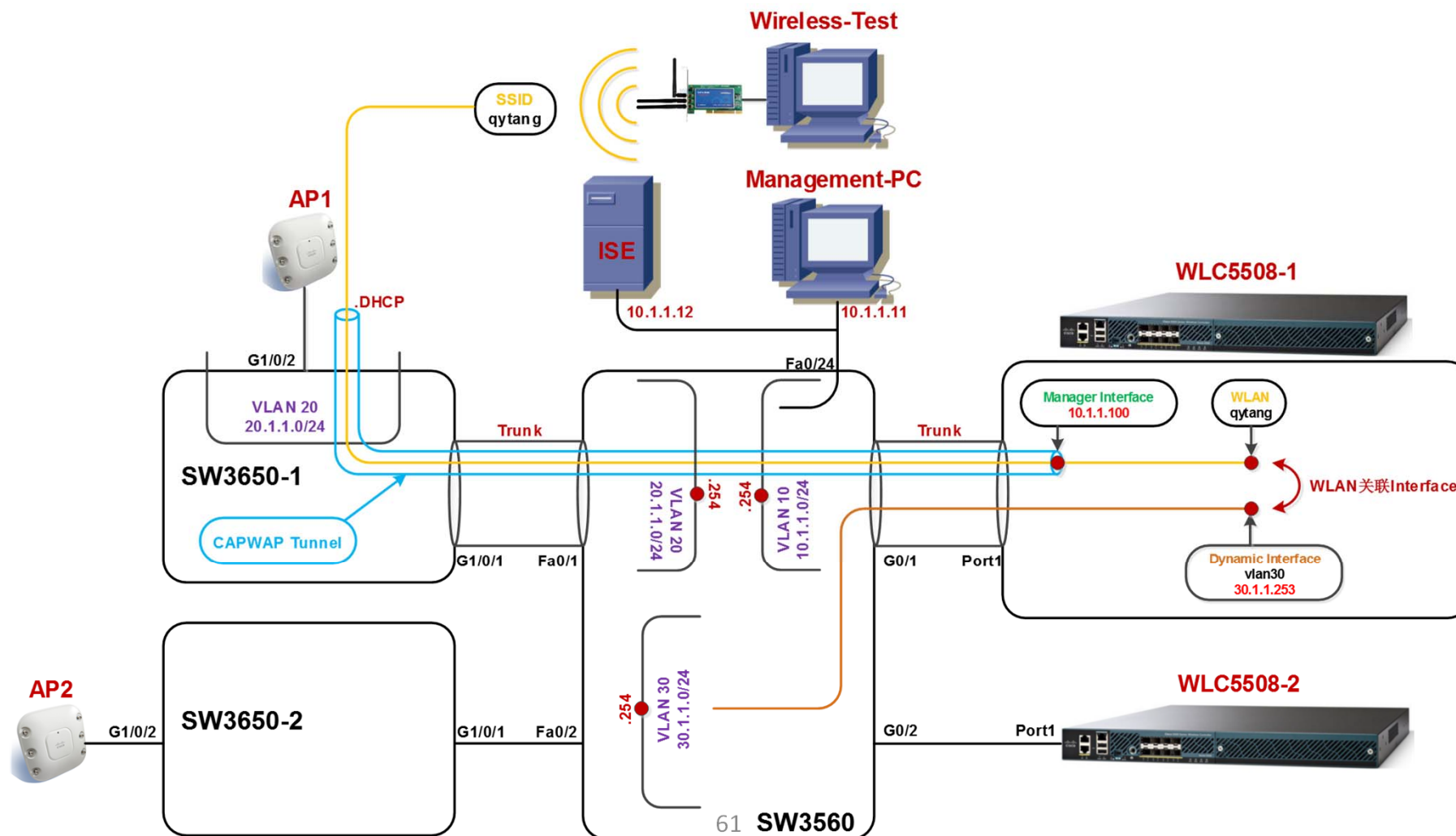


第二部分

Intra-Controller Roaming



实验拓扑





第一部分:AP的控制器的冗余

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
```



第一部分:AP的控制器的冗余

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
```



第一部分:AP的控制器的冗余

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
```




第一部分:AP的控制器的冗余

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



第一部分:AP的控制器的冗余

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



第一部分:AP的控制器的冗余

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



第一部分:AP的控制器的冗余

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



第一部分:AP的控制器的冗余

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



第一部分:AP的控制器的冗余

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

Wireless

All APs Entries 1 - 2 of 2

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

Number of APs: 2

AP Name	IP Address(Ipv4/Ipv6)	AP Model
AP1	20.1.1.1	AIR-CAP1602I-C-K9
AP2	20.1.1.2	AIR-CAP1602I-C-K9

严重确认两个AP
都管理激活状态

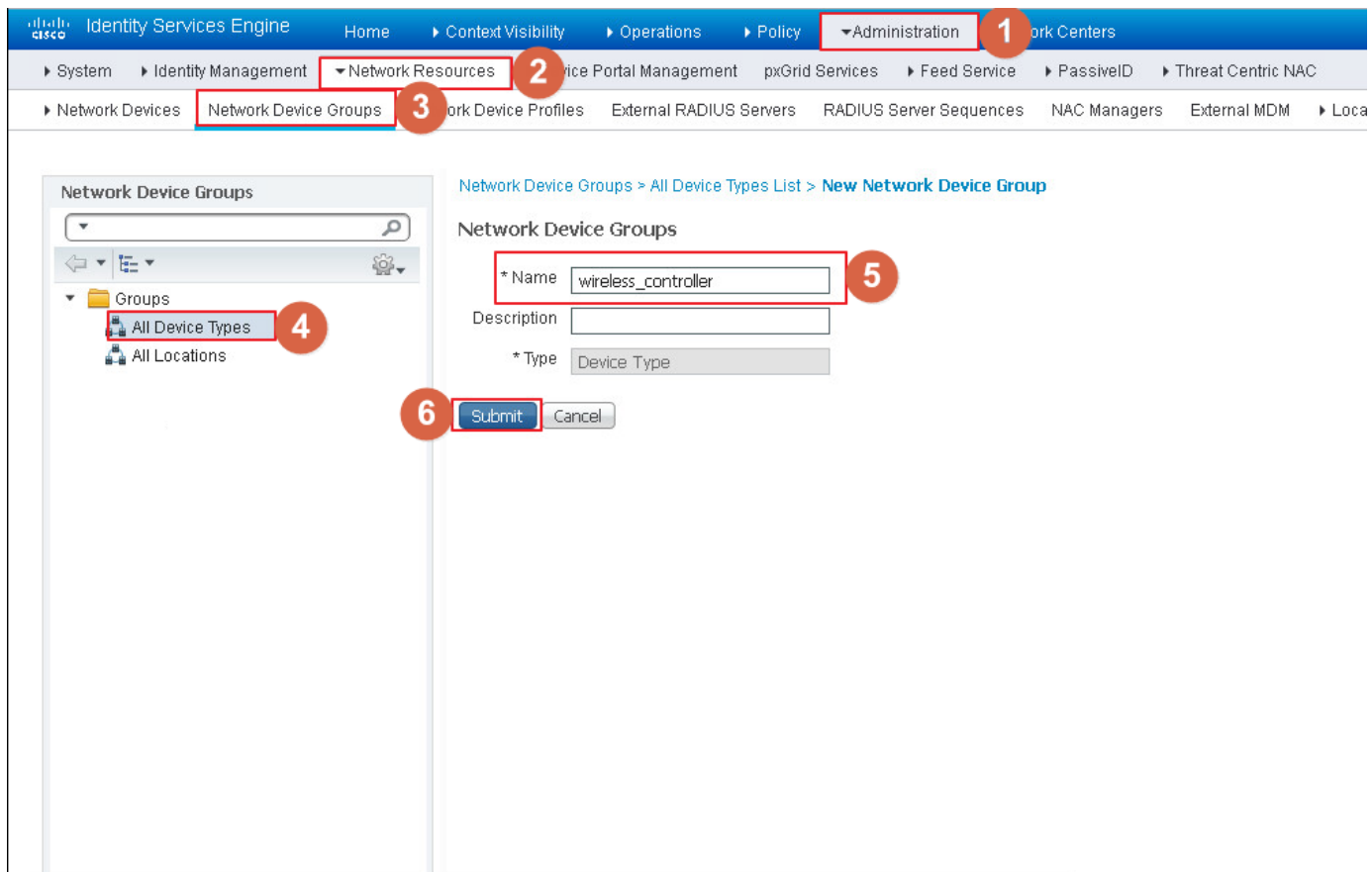


ISE创建NDG

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > Network Resources > Network Device Groups. The interface includes a left-hand navigation pane with a tree view under 'Groups' containing 'All Device Types' and 'All Locations'. The main content area shows the 'Network Device Groups' page with a table that is currently empty, displaying 'No data available'. The table has columns for 'Name', 'Type', and 'Description'. The '+ Add' button is highlighted with a red circle and the number 5. Other buttons like 'Edit', 'Duplicate', and 'Delete' are also visible. The breadcrumb navigation at the top shows the path: Administration > Network Resources > Network Device Groups. The number 1 is placed over the 'Administration' breadcrumb, 2 over 'Network Resources', and 3 over 'Network Device Groups'. The number 4 is placed over the 'All Device Types' item in the left-hand navigation pane.

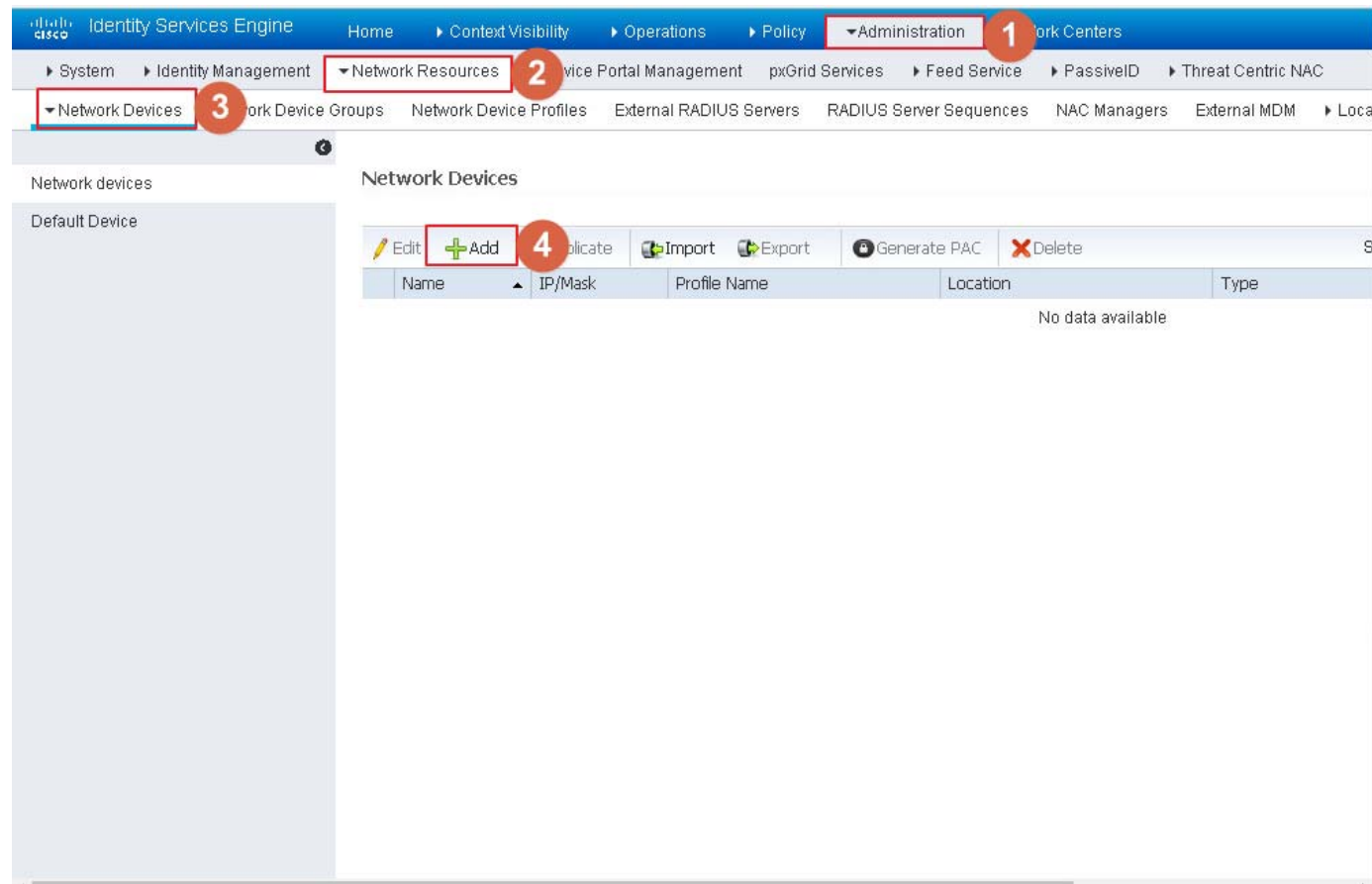


ISE创建NDG





ISE创建WLC5508-1





ISE创建WLC5508-1

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation path is: Administration > Network Resources > Network Devices > New Network Device. The configuration form includes the following fields and actions:

- 1:** Administration menu
- 2:** Network Resources
- 3:** Network Devices
- 4:** * Name: WLC5508-1
- 5:** * IP Address: 10.1.1.100 / 32
- * Device Profile: Cisco
- Model Name: [Dropdown]
- Software Version: [Dropdown]
- * Network Device Group
 - 6:** Device Type: wireless_controller
 - Location: All Locations
 - Set To Default buttons for Device Type and Location
- 7:** Submit button
- Cancel button
- Expansion arrows for RADIUS Authentication Settings and TACACS Authentication Settings



ISE创建WLC5508-1

1 Administration

2 Network Resources

3 Network Devices

4 RADIUS Authentication Settings

5 Submit

密码是cisco



ISE创建WLC5508-2

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is highlighted with red boxes and numbers: 1. Administration, 2. Network Resources, 3. Network Devices, 4. Add button.

Network devices

Default Device

Network Devices

Actions: Edit, Add, Duplicate, Import, Export, Generate PAC, Delete

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> WLC5508-1	10.1.1.100/32	Cisco	All Locations	wireless_controller



ISE创建WLC5508-2

Identity Services Engine Administration > Network Resources > Network Devices > New Network Device

1 Administration

2 Network Resources

3 Network Devices

Network Devices List > **New Network Device**

4 * Name WLC5508-2

Description

5 * IP Address: 10.1.1.101 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

6 * Device Type wireless_controller Set To Default

Location All Locations Set To Default

RADIUS Authentication Settings

TACACS Authentication Settings



ISE创建WLC5508-2

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Administration > Network Resources > Network Devices. The 'RADIUS Authentication Settings' section is expanded, showing the following configuration:

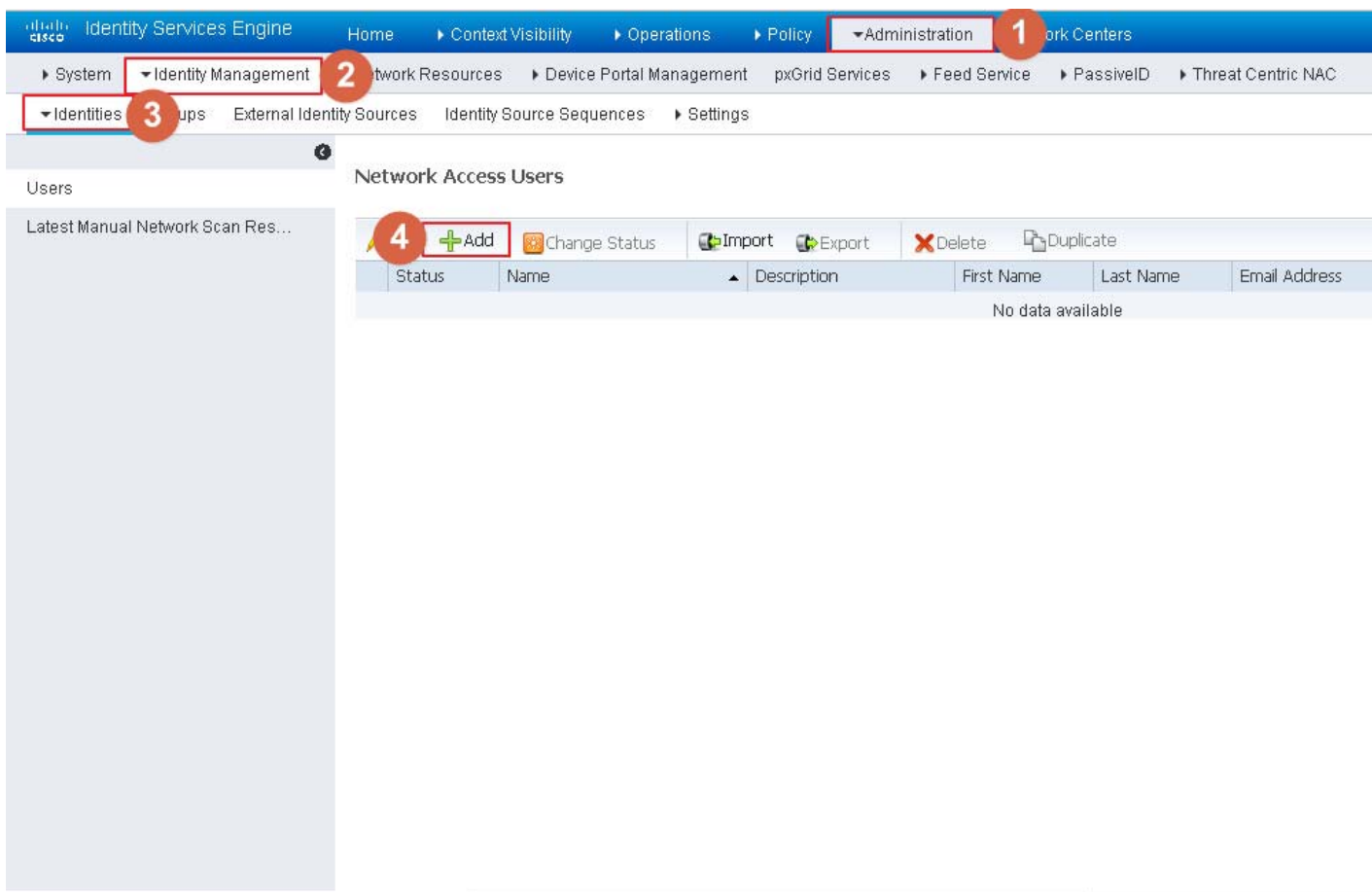
- Enable Authentication Settings:
- Protocol: RADIUS
- * Shared Secret: [masked] (Show button)
- Enable KeyWrap:
- * Key Encryption Key: [masked] (Show button)
- * Message Authenticator Code Key: [masked] (Show button)
- Key Input Format: ASCII HEXADECIMAL
- CoA Port: 1700 (Set To Default button)

At the bottom, there is a 'Submit' button and a 'Cancel' button.

密码是cisco



ISE创建用户名和密码





ISE创建用户名和密码

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration (1) > Identity Management (2) > Identities (3) > Users (4). The 'New Network Access User' form is displayed with the following fields and annotations:

- *Name:** qytang (5)
- Status:** Enabled
- Email:** (empty)
- Password Type:** Internal Users
- *Login Password:** (6) (masked with dots)
- Re-Enter Password:** (masked with dots)
- Generate Password:** (button)
- Enable Password:** (checkbox)
- User Information:** First Name, Last Name (7) (Submit button)
- Account Options:** Description, Change password on next login (checkbox)



创建动态接口(1)

The screenshot shows the Cisco Controller configuration interface. The 'CONTROLLER' tab is selected and highlighted with a red box and the number 1. In the left sidebar, the 'Interfaces' menu item is highlighted with a red box and the number 2. In the top right corner, the 'New...' button is highlighted with a red box and the number 3. The main content area displays a table with the following data:

Interface	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
10.1.1.100	10.1.1.100	Static	Enabled	::/128
0.0.0.0	0.0.0.0	Static	Not Supported	
0.0.0.0	0.0.0.0	Static	Not Supported	
0.0.0.0	0.0.0.0	DHCP	Disabled	::/128
1.1.1.1	1.1.1.1	Static	Not Supported	



创建动态接口(1)

The screenshot shows the Cisco Controller configuration page for creating a new dynamic interface. The interface is titled "Interfaces > New". The configuration fields are as follows:

Interface Name	vlan30
VLAN Id	30

The interface also shows a "Back" button and an "Apply" button. The configuration is highlighted with red boxes and numbered 1 through 5, indicating the steps to create the interface.

- 1: CONTROLLER tab
- 2: Interfaces menu item
- 3: Interfaces > New link
- 4: Interface Name input field
- 5: Apply button



创建动态接口(2)

The screenshot shows the Cisco Controller configuration page for 'Interfaces > Edit'. The page is divided into several sections, with red boxes and numbers highlighting specific configuration steps:

- 1**: The 'CONTROLLER' tab in the top navigation bar.
- 2**: The 'Interfaces' menu item in the left sidebar.
- 3**: The 'Port Number' field in the 'Physical Information' section, set to '1'.
- 4**: The 'Interface Address' section, including 'VLAN Identifier' (30), 'IP Address' (30.1.1.253), 'Netmask' (255.255.255.0), and 'Gateway' (30.1.1.254).
- 5**: The 'DHCP Information' section, including 'Primary DHCP Server' (30.1.1.254), 'Secondary DHCP Server', 'DHCP Proxy Mode' (Global), and 'Enable DHCP Option 82'.
- 6**: The 'Apply' button in the top right corner.



5508-1创建AAA

Security

RADIUS Authentication Servers

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

The screenshot shows the Cisco configuration interface for creating a new RADIUS Authentication Server. The interface includes a navigation menu on the left and a main configuration area on the right. The configuration area is titled "RADIUS Authentication Servers > New" and contains several fields and options. Red boxes and numbers 1 through 5 highlight specific steps in the configuration process:

- 1. The "SECURITY" tab is selected in the top navigation bar.
- 2. The "RADIUS Authentication" option is selected in the left-hand menu.
- 3. The "Shared Secret" field is highlighted, showing a masked password "cisco".
- 4. The "Support for RFC 3576" dropdown menu is set to "Enabled".
- 5. The "Apply" button is highlighted in the top right corner.

Additional configuration details visible in the screenshot include:

- Server Index (Priority): 1
- Server IP Address(Ipv4/Ipv6): 10.1.1.12
- Shared Secret Format: ASCII
- Confirm Shared Secret: cisco
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- IPSec: Enable

密码: cisco



5508-1创建SSID

The screenshot displays the Cisco AireOS configuration interface for creating a WLAN profile. The interface is titled "WLANs > Edit 'Intra-controller'". The left sidebar shows the "WLANs" menu with "WLANs" and "Advanced" options. The main content area shows the configuration for the "Intra-controller" profile. The "General" tab is selected, and the "Status" checkbox is checked, indicating the profile is enabled. The "Interface/Interface Group" is set to "vlan30". The "Security Policies" are set to "[WPA2][Auth(802.1X)]". The "Radio Policy" is set to "All". The "Broadcast SSID" checkbox is checked, and the "NAS-ID" is set to "none".

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode



5508-1修改认证方式

WLANs > Edit 'Intra-controller'

General Security **3** Policy-Mapping Advanced

Layer 2 **4** Layer 3 AAA Servers

Fast Transition

Fast Transition

Over the DS **5** 启用802.11r的快速漫游

Reassociation Timeout: 20 Seconds

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy:

WPA2 Policy-AES:

Authentication Key Management

802.1X: Enable

CCKM: Enable

PSK: Enable

FT 802.1X: Enable **6** 应该启用FT 802.1x

FT PSK: Enable

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
3 When client exclusion is enabled, Timeout Value of zero means infinity. It will require administrative override to reset excluded



不启用FT配置

WLANs > Edit 'Inter-controller'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Fast Transition

Fast Transition 1

Protected Management Frame

PMF Disabled

WPA+ WPA2 Parameters

WPA Policy

WPA2 Policy-AES

Authentication Key Management

802.1X Enable 2

CCKM Enable

PSK Enable

FT 802.1X Enable

FT PSK Enable

WPA gtk-randomize State [14](#) Disable

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

The screenshot shows the Cisco AireOS configuration interface for a WLAN named 'Inter-controller'. The 'Advanced' tab is selected, and the 'Layer 3' sub-tab is active. Under the 'Authentication Key Management' section, the 'CCKM' option is checked and highlighted with a red circle and the number '1'. Other options like '802.1X', 'PSK', 'FT 802.1X', and 'FT PSK' are also visible with their respective enable/disable checkboxes. The 'Protected Management Frame' (PMF) is set to 'Disabled'. The 'WPA+WPA2 Parameters' section shows 'WPA Policy' disabled and 'WPA2 Policy-AES' enabled. The 'Fast Transition' option is also disabled.

思科私有解决方案，需要思科CCX客户端，不推荐使用

本页仅为展示保留FT设置



5508-1指定AAA服务器

WLANs > Edit 'Intra-controller'

General Security Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Radius Server Overwrite interface Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	<input checked="" type="checkbox"/> Enabled IP: 10.1.1.12, Port: 1812	<input checked="" type="checkbox"/> Enabled None	Enable <input type="checkbox"/>
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

Radius Server Accounting

Interim Update Interim Interval 0

LDAP Servers

Server 1	None
Server 2	None

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
3 When client exclusion is enabled, Timeout Value of zero means infinity (will require administrative override to reset excluded)

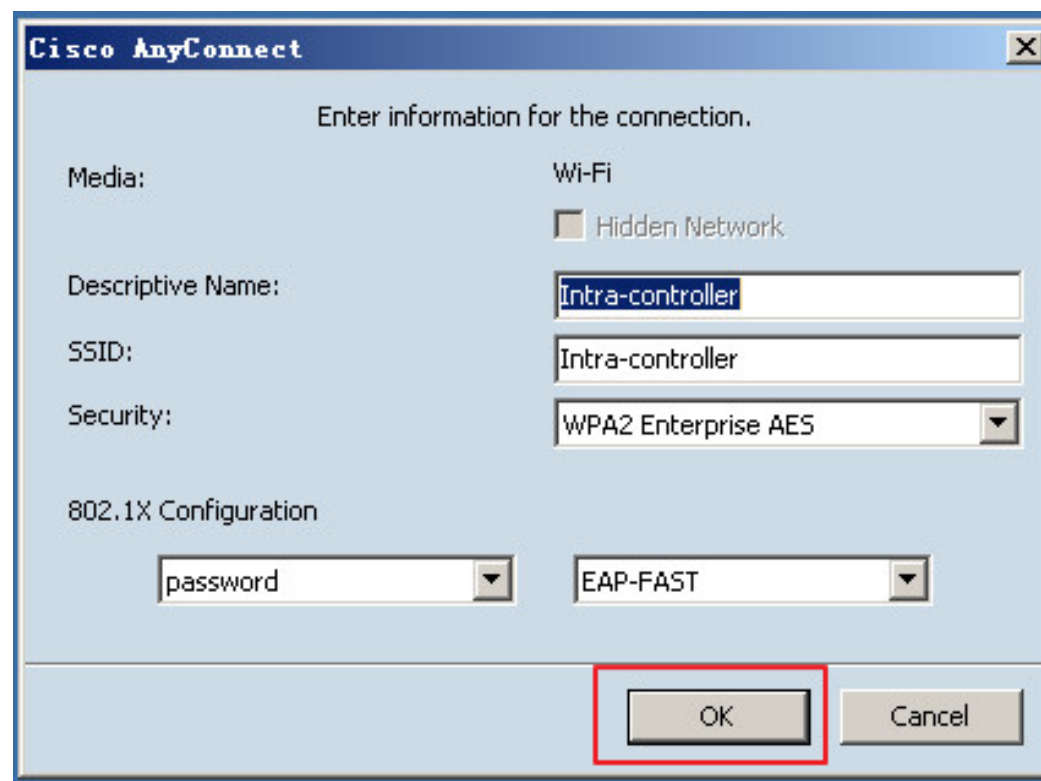
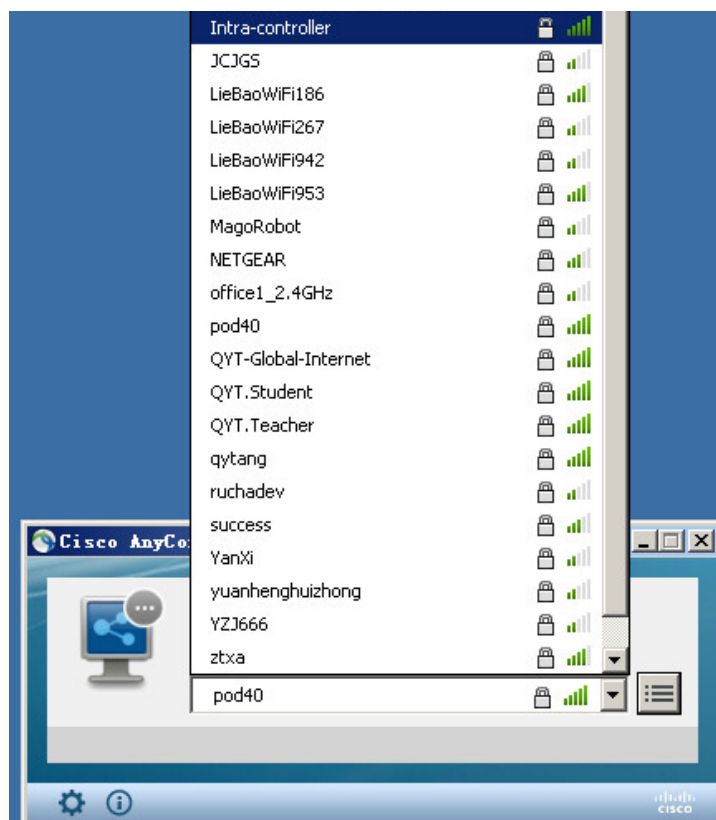


5508-1指定AAA override

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'intra-controller'. The 'Advanced' tab is selected, and the 'Allow AAA Override' checkbox is checked and highlighted with a red box and a '4' in a red circle. Other configuration options include Coverage Hole Detection (checked), Session Timeout (1800), Aironet IE (checked), Diagnostic Channel (unchecked), Override Interface ACL (IPv4: None, IPv6: None), Layer2 Ad (None), P2P Blocking Action (Disabled), Client Exclusion (checked, 60), Maximum Allowed Clients (0), Static IP Tunneling (unchecked), Wi-Fi Direct Clients Policy (Disabled), and Maximum Allowed Clients Per AP Radio (200). On the right side, DHCP, OEAP, Management Frame Protection (MFP), DTIM Period, and NAC settings are visible.

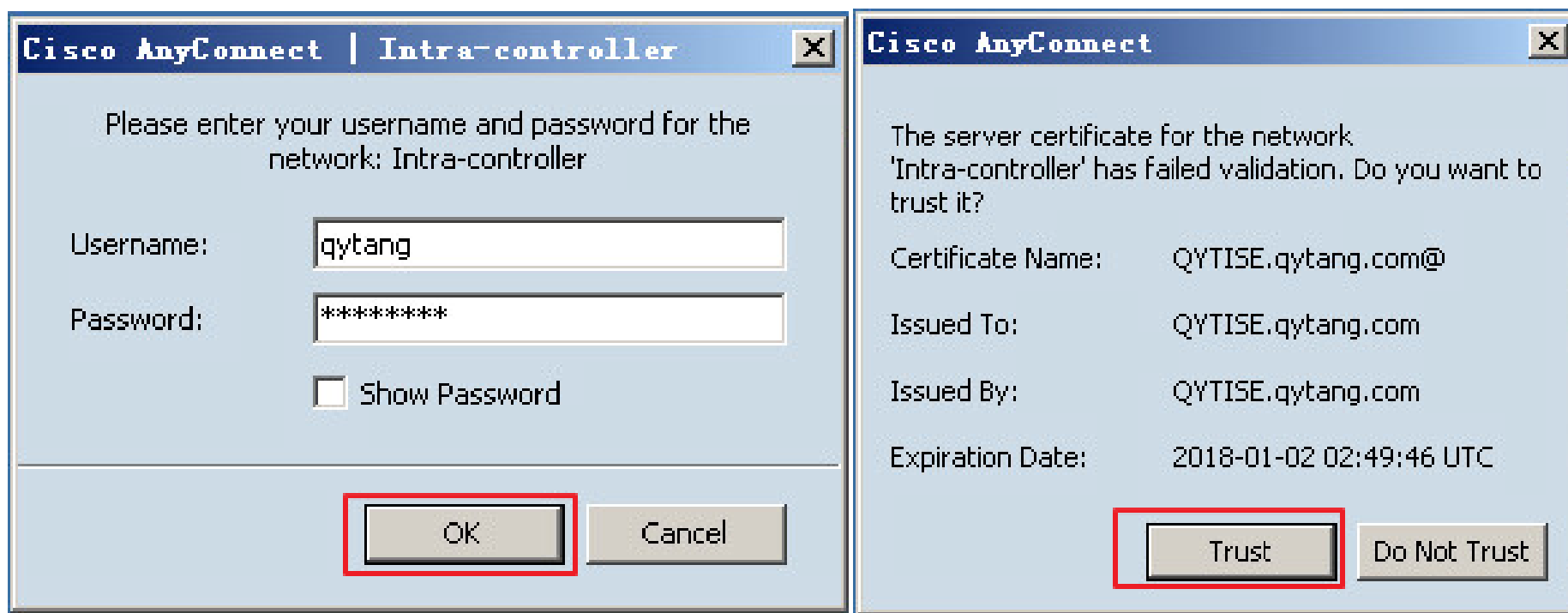


Test-PC创建无线认证





Test-PC连接无线





Test-PC连接无线

The screenshot displays a Windows command prompt window on the left and the Cisco AnyConnect Secure Mobility Client interface on the right. The command prompt shows the configuration of network interfaces and a successful ping test to 10.1.1.254.

```
连接特定的 DNS 后缀 . . . . . :  
本地连接 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-BAE03FA5426> :  
  
媒体状态 . . . . . : 媒体已断开  
连接特定的 DNS 后缀 . . . . . :  
  
隧道适配器 6T04 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>ipconfig
```

The Cisco AnyConnect Secure Mobility Client interface shows the network status as "Network: Connected (30.1.1.1)" and the connection mode as "Intra-controller".



查看ISE认证

Identity Services Engine Home Context Visibility Operations 1 Policy Administration Work Centers

RADIUS 2 RADIUS 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 Last

Reset Repeat Counts Export To

Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentica...	Authorizati...	Authorizati...	IP Address	Network Devi...
	Identity	Endpoint ID	Endpoint Prof	Authenticator	Authorization	Authorization	IP Address	Network Devi...
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

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=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=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=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

The screenshot displays the Cisco WLC GUI. The top navigation bar includes 'MONITOR' (1), 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'Monitor' section with 'Clients' (2) selected. The main content area shows the 'Clients' page with a table of client information:

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN
a0:63:91:bb:d3:b2	30.1.1.1	AP1 (3)	Intra



关闭两个控制器的2.4G信号

The screenshot shows the Cisco Wireless configuration interface for 802.11b/g Global Parameters. The left sidebar shows the navigation tree with '802.11b/g/n Network' selected. The main content area shows the 'General' section with the following parameters:

- 802.11b/g Network Status: Enabled (3)
- 802.11g Support: Enabled (4)
- Beacon Period (millisecs): 100
- Short Preamble: Enabled
- Fragmentation Threshold (bytes): 2346
- DTPC Support: Enabled
- Maximum Allowed Clients: 200
- RSSI Low Check: Enabled
- RSSI Threshold (-60 to -90 dBm): -80

The 'Data Rates**' section shows the following rates and their status:

Data Rate	Status
1 Mbps	Mandatory
2 Mbps	Mandatory
5.5 Mbps	Mandatory
11 Mbps	Mandatory

The 'CCX Location Measurement' section shows the Mode set to Enabled.

** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate. The actual data rates that are supported depend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. But in reality, the AP will pick the next lower data rate allowed for that channel if the chosen data rate is not supported.



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
 802.11a/n Cisco APs > Configure

Note: Changing any of the parameters causes i 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

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

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

The screenshot shows the Cisco Identity Services Engine (ISE) Operations page. The navigation bar includes Home, Context Visibility, Operations (1), Policy, Administration, and Work Centers. The breadcrumb trail is RADIUS (2) > RADIUS Live Logs > TACACS > Reports > Troubleshoot > Adaptive Network Control. The sub-menu is Live Logs (3) > Sessions. The summary cards show 0 for Misconfigured Supplicants, Misconfigured Network Devices, RADIUS Drops, Client Stopped Responding, and Repeat Counter. The filters are Refresh (Every 1 minute), Show (Latest 20 records), and Within (Last 24 hours). The table below shows two log entries for user 'qytang' with endpoint ID 'A0:63:91:BB:D3:B2' and network device 'WLC5508-1'. A red box highlights these two entries, and a red circle with the number 4 is next to the second entry.

Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentica...	Authorizati...	Authorizati...	IP Address	Network Device
04:07:34.875 PM	✓	🔒	qytang	A0:63:91:BB:D3:B2	Netgear-De...	Default >> D...	Default >> B...	PermitAccess		WLC5508-1
03:58:32.744 PM	✓	🔒	qytang	A0:63:91:BB:D3:B2		Default >> D...	Default >> B...	PermitAccess		WLC5508-1

Last Updated: Tue Sep 19 2017 16:16:18 GMT+0800 (中国标准时间) Records Shown: 2

每一次漫游都会多一次认证信息



查看客户端关联AP

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
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

The screenshot shows the Cisco Wireless Controller configuration interface. The navigation menu at the top includes MONITOR, WLANs, CONTROLLER, WIRELESS (1), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the configuration tree with 'All APs' (2) selected under 'Access Points'. The main content area is titled 'All APs > Details for AP2' (3) and has 'Apply' and '< Back' buttons. The 'High Availability' (4) tab is active, showing a table for controller associations:

	Name	Management IP Address(Ipv4/Ipv6)
Primary Controller	WLC5508-2	10.1.1.101 (5)
Secondary Controller		
Tertiary Controller		

Below the table, the 'AP Failover Priority' is set to 'Low'.



查看AP2 关联WLC5508-2

The screenshot shows the Cisco WLC WebUI interface. The browser address bar (1) displays `https://10.1.1.101/screens/frameset.html`. The navigation menu (2) has **WIRELESS** selected. The left sidebar (3) shows **Access Points** expanded. The main content area shows **All APs** with a table listing one AP:

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AI
AP2	20.1.1.2	AIR-CAP1602I-C-K9	f0



5508-2 创建动态接口

The screenshot shows the Cisco Controller configuration interface. The 'CONTROLLER' tab is selected. The left sidebar shows the 'Interfaces' menu item. The main content area displays a table of interfaces with the following data:

Interface	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
10.1.1.101	10.1.1.101	Static	Enabled	::/128
0.0.0.0	0.0.0.0	Static	Not Supported	
0.0.0.0	0.0.0.0	Static	Not Supported	
0.0.0.0	0.0.0.0	DHCP	Disabled	::/128
1.1.1.1	1.1.1.1	Static	Not Supported	



5508-2创建动态接口

The screenshot shows the Cisco Controller configuration page for creating a new dynamic interface. The interface is titled "Interfaces > New". The "Interface Name" field is set to "vlan30" and the "VLAN Id" field is set to "30". The "Apply" button is highlighted. The navigation menu on the left includes "General", "Inventory", "Interfaces", "Interface Groups", "Multicast", "Network Routes", "Redundancy", "Internal DHCP Server", "Mobility Management", "Ports", "NTP", "CDP", "PMIPv6", "IPv6", "mDNS", and "Advanced". The "CONTROLLER" tab is selected in the top navigation bar.

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER 1 WIRELESS 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 4

VLAN Id: 30



5508-2创建动态接口

The screenshot shows the Cisco Controller configuration interface for creating a dynamic interface. The page is titled "Interfaces > Edit". The left sidebar shows the navigation menu with "Interfaces" highlighted (callout 2). The main content area is divided into several sections:

- General Information:** Interface Name is set to "vlan30" (callout 3). MAC Address is "6c:20:56:65:a6:a0".
- Configuration:** Guest Lan, Quarantine, and Quarantine Vlan Id are unchecked. NAS-ID is set to "none".
- Physical Information:** Port Number is set to "1" (callout 4). Backup Port is "0", Active Port is "0", and Enable Dynamic AP Management is unchecked.
- Interface Address:** WLAN Identifier is "30", IP Address is "30.1.1.252", Netmask is "255.255.255.0", and Gateway is "30.1.1.254" (callout 5).
- DHCP Information:** Primary DHCP Server is "30.1.1.254" (callout 6). Secondary DHCP Server is empty, and DHCP Proxy Mode is set to "Global".



5508-2创建AAA

Security

RADIUS Authentication Servers

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

The screenshot displays the Cisco configuration page for creating a new RADIUS Authentication Server. The page is titled "RADIUS Authentication Servers > New" and includes a navigation menu on the left and a main configuration area on the right. The configuration area contains the following fields and options:

- Server Index (Priority):** A dropdown menu set to "1".
- Server IP Address(Ipv4/Ipv6):** A text input field containing "10.1.1.12".
- Shared Secret Format:** A dropdown menu set to "ASCII".
- Shared Secret:** A text input field containing "*****".
- Confirm Shared Secret:** A text input field containing "*****".
- Key Wrap:** A checkbox labeled "(Designed for FIPS customers and requires a key wrap compliant RADIUS server)" which is unchecked.
- Port Number:** A text input field containing "1812".
- Server Status:** A dropdown menu set to "Enabled".
- Support for RFC 3576:** A dropdown menu set to "Enabled".
- Server Timeout:** A text input field containing "2" followed by "seconds".
- Network User:** A checkbox labeled "Enable" which is checked.
- Management:** A checkbox labeled "Enable" which is checked.
- IPSec:** A checkbox labeled "Enable" which is unchecked.

The interface also includes a "Security" sidebar on the left with a tree view showing "AAA" > "RADIUS" > "Authentication" selected. At the top right, there are buttons for "Save Configuration", "Ping", "Logout", and "Refresh". At the bottom right, there are buttons for "< Back" and "Apply".



5508-2创建SSID

The screenshot displays the Cisco AireOS configuration interface for creating a WLAN profile. The interface is titled "WLANs > Edit 'Inter-controller'". The configuration is divided into several tabs: General, Security, QoS, Policy-Mapping, and Advanced. The "General" tab is selected, and the following fields are visible:

- Profile Name: Inter-controller
- Type: WLAN
- SSID: Inter-controller
- Status: Enabled
- Security Policies: [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface/Interface Group(G): vlan30
- Multicast Vlan Feature: Enabled
- Broadcast SSID: Enabled
- NAS-ID: none

Red boxes and numbers 1 through 6 highlight specific steps in the configuration process:

1. The "WLANs" menu item in the top navigation bar.
2. The "WLANs" dropdown menu in the left sidebar.
3. The "WLANs > Edit 'Inter-controller'" page title.
4. The "General" tab in the configuration area.
5. The Profile Name, Type, SSID, and Status fields.
6. The Radio Policy and Interface/Interface Group(G) fields.

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, Timeout Value of zero means infinity (will require administrative override to reset excluded)



5508-2修改认证方式

WLANs > Edit 'Inter-controller'

General Security Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Fast Transition

Fast Transition

Over the DS

Reassociation Timeout: 20 Seconds

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy-AES

Authentication Key Management

802.1X Enable

CCKM Enable

PSK Enable

FT 802.1X Enable

FT PSK Enable

Foot Notes

1 Web Policy cannot be used in combination with IPsec

2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode

3 When client exclusion is enabled, Timeout Value of zero means infinity, will require administrative override to reset excluded



5508-2修改认证服务器

The screenshot displays the Cisco WLC configuration interface for editing the 'Inter-controller' WLAN. The 'Security' tab is active, and the 'AAA Servers' sub-tab is selected. The 'Authentication Servers' section is expanded, showing a table of servers. The first server is configured with the IP address '10.1.1.12' and port '1812'. The 'Radius Server Accounting' section is also visible, with 'Interim Update' checked and 'Interim Interval' set to 0. The 'LDAP Servers' section shows two servers set to 'None'. The page includes a 'Foot Notes' section at the bottom with several technical notes.

Server	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	IP:10.1.1.12, Port:1812	None	Enable
Server 2	None	None	None
Server 3	None	None	None
Server 4	None	None	None
Server 5	None	None	None
Server 6	None	None	None



5508-2启用AAA-Override

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'Inter-controller'. The 'Advanced' tab is selected, and the 'Allow AAA Override' checkbox is checked and highlighted with a red box and the number 4. Other configuration options include Coverage Hole Detection (checked), Enable Session Timeout (1800), Aironet IE (checked), Diagnostic Channel (disabled), Override Interface ACL (IPv4: None, IPv6: None), Layer2 Ad (None), P2P Blocking Action (Disabled), Client Exclusion (checked, 60), and Maximum Allowed Clients (0). The DHCP, OEAP, Management Frame Protection (MFP), DTIM Period, and NAC sections are also visible. The 'Apply' button is highlighted with a red box and the number 6. The breadcrumb path 'WLANs > Edit 'Inter-controller'' is highlighted with a red box and the number 3. The 'WLANs' menu is highlighted with a red box and the number 2. The 'Advanced' tab is highlighted with a red box and the number 5.

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded)



5508-1创建SSID

The screenshot displays the Cisco WLC configuration interface for creating a WLAN profile. The browser address bar shows `https://10.1.1.100/screens/frameset.html`. The navigation bar includes 'MONITOR', 'WLANs', 'ROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The main content area is titled 'WLANs > Edit 'Inter-controller'' and features a 'Back' button and an 'Apply' button. The configuration is organized into tabs: 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is active, showing the following fields:

- Profile Name: Inter-controller
- Type: WLAN
- SSID: Inter-controller
- Status: Enabled
- Security Policies: [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface/Interface Group(G): vlan30
- Multicast Vlan Feature: Enabled
- Broadcast SSID: Enabled
- NAS-ID: none

Foot Notes:

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity. It will require administrative override to react excluded.



5508-1修改认证方式

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'Inter-controller'. The 'Security' tab is selected, and the 'AAA Servers' sub-tab is active. The following settings are highlighted with red boxes and numbered:

- 1: WLANs menu
- 2: WLANs sub-menu
- 3: WLANs > Edit 'Inter-controller'
- 4: Security tab
- 5: Fast Transition section, including 'Fast Transition' (checked), 'Over the DS' (checked), and 'Reassociation Timeout' (20 Seconds).
- 6: Authentication Key Management section, including '802.1X' (checked), 'CCKM' (unchecked), 'PSK' (unchecked), 'FT 802.1X' (checked), and 'FT PSK' (unchecked).

Other visible settings include 'Protected Management Frame' (PMF Disabled) and 'WPA+ WPA2 Parameters' (WPA Policy unchecked, WPA2 Policy-AES checked).

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity. It will require administrative override to reset excluded.



5508-1修改认证服务器

The screenshot shows the Cisco WLC configuration interface for the 'Inter-controller' WLAN. The configuration is divided into several sections: General, Security, Policy-Mapping, and Advanced. The 'Security' section is active, and the 'AAA Servers' tab is selected. The 'Authentication Servers' section is expanded, showing a table of servers. The first server is configured with IP: 10.1.1.12 and Port: 1812. The 'Radius Server Accounting' section is also visible, with 'Interim Update' checked and 'Interim Interval' set to 0. The 'LDAP Servers' section shows two servers set to 'None'. The 'Foot Notes' section at the bottom provides additional information about the configuration.

1. WLANs menu
2. WLANs > Edit 'Inter-controller'
3. Security tab
4. AAA Servers tab
5. Authentication Servers section
6. Server 1 IP: 10.1.1.12, Port: 1812

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, Timeout Value of zero means infinity. It will require administrative override to reset excluded



5508-1启用AAA-Override

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'Inter-controller'. The 'Advanced' tab is selected, and the 'Allow AAA Override' checkbox is checked and highlighted with a red box and the number 4. Other configuration options include Coverage Hole Detection (checked), Enable Session Timeout (1800), Aironet IE (checked), Diagnostic Channel (disabled), Override Interface ACL (IPv4: None, IPv6: None), Layer2 Ad (None), P2P Blocking Action (Disabled), Client Exclusion (checked, 60), and Maximum Allowed Clients (0). The DHCP, OEAP, Management Frame Protection (MFP), DTIM Period, and NAC sections are also visible. The 'Apply' button is highlighted with a red box and the number 6. The breadcrumb path 'WLANs > Edit 'Inter-controller'' is highlighted with a red box and the number 3. The 'WLANs' menu item is highlighted with a red box and the number 2. The 'MONITOR' tab is highlighted with a red box and the number 1.

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded)



5508-1添加5508-2到Mobility Group

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

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER 1 LESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

3 New... EditAll

Name	Multicast IP	Status	Hash Key
	0.0.0.0	Up	none



5508-1添加5508-2到Mobility Group

Controller

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** 2
 Mobility Configuration
 Mobility Groups 3
 Mobility Anchor Config
 Multicast Messaging
Ports
▶ NTP
▶ CDP
▶ PMIPv6
▶ IPv6
▶ mDNS
▶ Advanced

Mobility Group Member > New

< Back Apply 5

Member IP Address(ipv4/ipv6) 10.1.1.101
Member MAC Address 6c:20:56:65:a6:a0 4
Group Name qytang
Hash none

1. Hash is not supported for IPv6 members

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



5508-2添加5508-1到Mobility Group

The screenshot shows the Cisco Controller GUI. The 'CONTROLLER' tab is selected (1). The 'New...' button is highlighted (3). The 'Mobility Groups' menu item is highlighted (2). The table below shows the existing Mobility Groups configuration:

Name	Multicast IP	Status	Hash Key
	0.0.0.0	Up	none



5508-2添加5508-1到Mobility Group

Controller

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

Mobility Group Member > New

< Back | Apply

Member IP Address(Ipv4/Ipv6)	10.1.1.100
Member MAC Address	58:8d:09:cd:b9:60
Group Name	qytang
Hash	none

1. Hash is not supported for IPv6 members

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



5508-1 查看mobility list状态

Static Mobility Group Members

Local Mobility Group	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
qytang	58:8d:09:cd:b9:60	10.1.1.100	qytang	0.0.0.0	Up
	6c:20:56:65:a6:a0	10.1.1.101	qytang	0.0.0.0	Up

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

Static Mobility Group Members

Local Mobility Group				
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	qytang	0.0.0.0	Up

严重注意一定要查看状态为“UP”



Ping测试

The screenshot shows the Cisco AireOS Controller configuration interface. The left sidebar lists various configuration categories, with 'Multicast' selected under 'Interface Groups'. The main content area displays a table of Multicast configurations:

Group Name	Multicast IP	Status	Hash Key
qytang	0.0.0.0	Up	none
qytang	0.0.0.0	Up	none

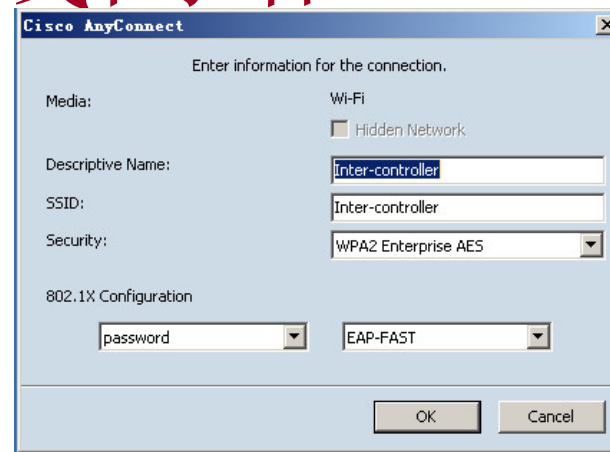
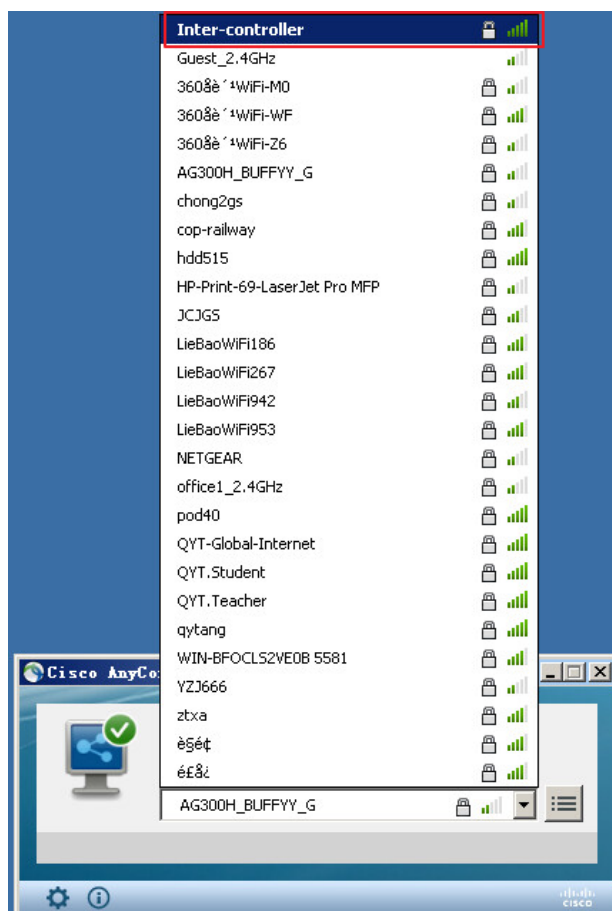
A 'Ping' button is visible next to the second entry. A dialog box is open, showing the results of a ping test to 10.1.1.101:

```
10.1.1.101 显示:  
Reply received from Mobility Peer 10.1.1.100 : (send count = 3,  
receive count = 3)
```

The dialog box also includes a checkbox for '禁止此页再显示对话框。' (Prevent this page from displaying this dialog box again) and a '确定' (OK) button.



Test-PC连接无线网络



用户名: qytang
密码: Cisc0123



查看ISE认证

The screenshot shows the Cisco Identity Services Engine (ISE) Live Logs interface. The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > RADIUS > Live Logs. The 'Live Logs' section is selected, and the 'Sessions' tab is active. The interface displays a table of authentication records with columns for Status, Details, Repeat Counts, Identity, Endpoint ID, Endpoint Profile, Authentication, Authorization, IP Address, and Network Device. The table shows three successful authentication records for user 'qytang' from endpoint 'A0:63:91:BB:D3:B2' on device 'WLC5508-1'. A red box highlights the first two rows, and a red circle with the number '4' is placed next to the 'WLC5508-1' device name in the second row.

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
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

The screenshot shows the Cisco AireOS Monitor interface. The top navigation bar includes 'MONITOR' (highlighted with a red box and a '1' in a circle), 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar contains a 'Monitor' menu with options: Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Clients (highlighted with a red box and a '2' in a circle), Sleeping Clients, Multicast, Applications, and Local Profiling. The main content area is titled 'Clients' and shows a table with one entry. The table has columns: Client MAC Addr, IP Address(Ipv4/Ipv6), AP Name, WLAN Profile, WLAN SSID, and User. The entry shows Client MAC Addr 'a0:63:91:bb:d3:b2', IP Address '30.1.1.1', AP Name 'AP1' (highlighted with a red box and a '3' in a circle), WLAN Profile 'Inter-controller', WLAN SSID 'Inter-controller', and User 'qyta'. The top right of the main area shows 'Entries 1 - 1 of 1'. The bottom of the interface has links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'.

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	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
 802.11a/n Cisco APs > Configure

Note: Changing any of the parameters causes i 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

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

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=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 1 > Policy > Administration > Work Centers

RADIUS 2 > RADIUS 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 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
			Identity	Endpoint ID	Endpoint Prof	Authenticator	Autho	Authorization	IP Address	Network Device
7 03:45:27.912 PM		0	qytang	A0:63:91:BB:D3:B2	Netgear-De...	Default >> D...	Def...	PermitAccess		
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			qytang	A0:63:91:BB:D3:B2	Netgear-De...	Default >> D...	Def...	PermitAccess		WLC5508-1



查看WLC5508-2

The screenshot shows the Cisco WLC Monitor interface. The top navigation bar includes 'MONITOR' (highlighted with a red box and a '1' in a circle), 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar has 'Monitor' selected, with sub-items like 'Summary', 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', 'Rogues', 'Clients' (highlighted with a red box and a '2' in a circle), 'Sleeping Clients', 'Multicast', 'Applications', and 'Local Profiling'. The main content area is titled 'Clients' and shows a table with one entry. The entry is highlighted with a red box and a '3' in a circle. The table columns are 'Client MAC Addr', 'IP Address (Ipv4/Ipv6)', 'AP Name', 'WLAN Profile', 'WLAN SSID', and 'User'. The entry shows 'a0:63:91:bb:d3:b2' for MAC, '30.1.1.1' for IP, 'AP2' for AP Name, 'Inter-controller' for both WLAN Profile and WLAN SSID, and 'qyta' for User.

Client MAC Addr	IP Address (Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User
a0:63:91:bb:d3:b2	30.1.1.1	AP2	Inter-controller	Inter-controller	qyta



3.1

组播漫游消息



WLC5508-1配置组播消息

The screenshot shows the Cisco WLC5508-1 configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER (highlighted with a red circle 1), ELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar menu includes: Controller, General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Redundancy, Internal DHCP Server, Mobility Management (expanded), Mobility Configuration, Mobility Groups, Mobility Anchor Config, Multicast Messaging (highlighted with a red circle 2), Ports, NTP, CDP, PMIPv6, IPv6, mDNS, and Advanced. The main content area is titled "Mobility Multicast Messaging" and contains the following configuration options: "Enable Multicast Messaging" (checked, highlighted with a red circle 3), and "Local Group Multicast IPv4 Address" (239.1.1.1, highlighted with a red circle 3). Below these options is a section for "Mobility Group".



WLC5508-1删除单播配置

The screenshot shows the Cisco WLC5508-1 configuration page for Static Mobility Group Members. The page is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: Controller, General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Redundancy, Internal DHCP Server, Mobility Management (expanded), Ports, NTP, CDP, PMIPv6, IPv6, mDNS, and Advanced. The main content area is titled "Static Mobility Group Members" and displays a table with the following data:

Local Mobility Group	qytang				
MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key
58:8d:09:cd:b9:60	10.1.1.100	qytang	239.1.1.1	Up	none



WLC5508-2配置组播消息

The screenshot displays the Cisco WLC5508-2 configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'ELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected and highlighted with a red circle '1'. The left sidebar shows the 'Mobility Management' section expanded, with 'Multicast Messaging' selected and highlighted with a red circle '2'. The main content area shows the 'Mobility Multicast Messaging' configuration page. The 'Enable Multicast Messaging' checkbox is checked and highlighted with a red circle '3'. The 'Local Group Multicast IPv4 Address' field contains the value '239.1.1.1' and is also highlighted with a red circle '3'. Below this, the 'Mobility Group' section is visible.



WLC5508-2删除单播配置

The screenshot shows the Cisco WLC5508-2 configuration interface. The left sidebar contains a navigation menu with categories like Controller, General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Redundancy, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, PMIPv6, IPv6, mDNS, and Advanced. The main content area is titled 'Static Mobility Group Members' and displays a table with the following data:

Local Mobility Group	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key
qytang	10.1.1.101	qytang	239.1.1.1	Up	none



3.2 锚测试



测试默认没有锚的漫游效果

The screenshot shows the Cisco WLC5508-2 configuration interface for Access Control Lists. The 'Security' tab is active, and the 'Access Control Lists > Edit' page is displayed. The 'General' section shows the 'Access List Name' as 'deny-icmp' and 'Deny Counters' as '0'. A table below lists the ACL rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Deny	0.0.0.0 /	0.0.0.0 /	ICMP	Any	Any	Any	Any	0
2	Permit	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	0

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

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

Network Routes

Redundancy

Internal DHCP Server

Mobility Management

Ports

NTP

CDP

PMIPv6

IPv6

mDNS

Advanced

Guest Lan

Quarantine

Quarantine Vlan Id

NAS-ID

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier 1

IP Address

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

DHCP Proxy Mode

Enable DHCP Option 82

Access Control List

ACL Name 2

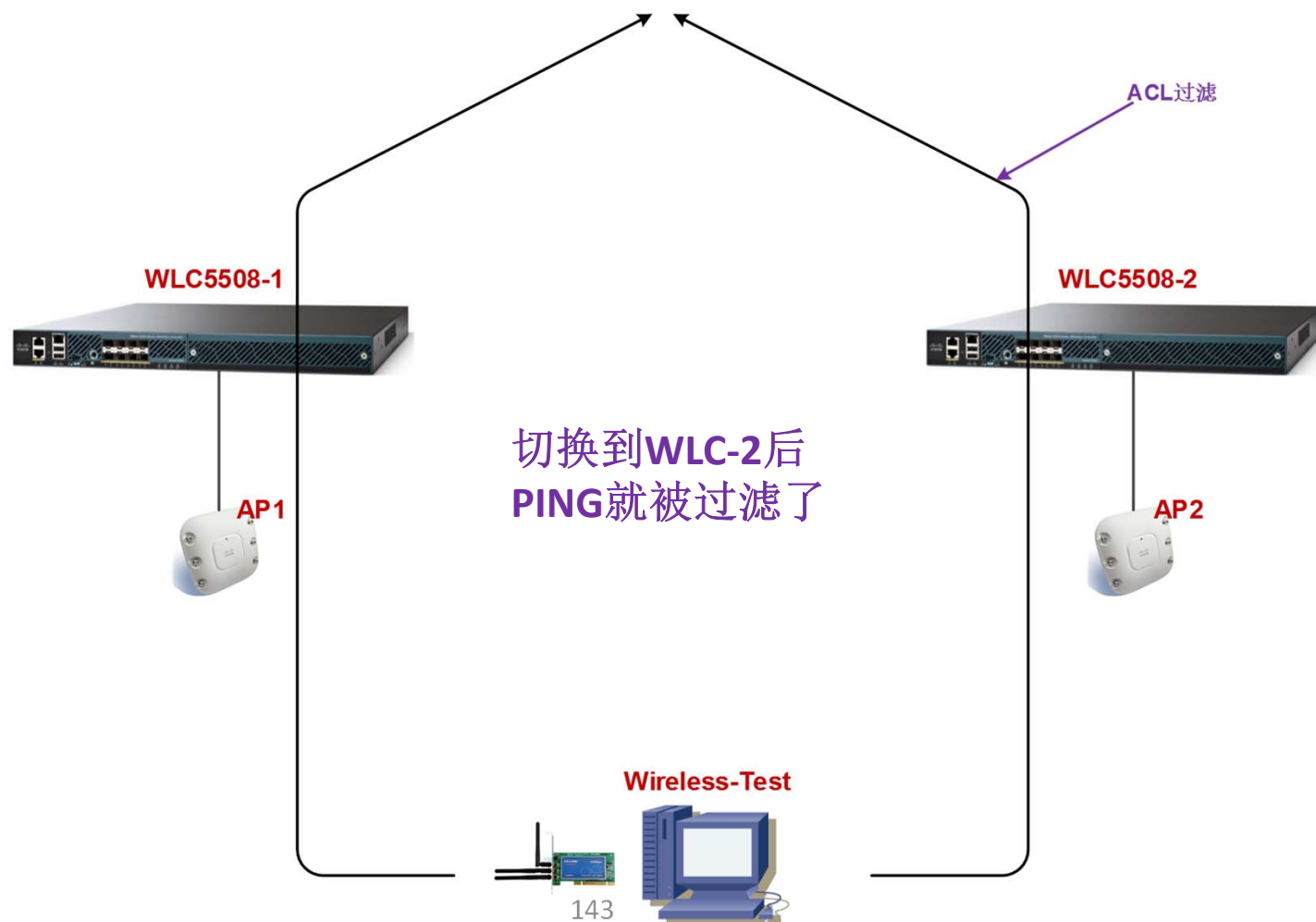
mDNS

mDNS Profile

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



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)

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar lists various configuration categories, with 'Mobility Management' expanded to show 'Mobility Groups'. The main content area is titled 'Static Mobility Group Members' and displays a table with the following data:

Local Mobility Group	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
qytang	58:8d:09:cd:b9:60	10.1.1.100	qytang	239.1.1.1	Up
	6c:20:56:65:a6:a0	10.1.1.101	qytang	239.1.1.1	Up



恢复漫游组静态成员 (WLC-2)

The screenshot shows the Cisco WLC configuration interface. The left sidebar contains a navigation menu with categories like General, Inventory, Interfaces, Network Routes, Redundancy, Internal DHCP Server, Mobility Management, Ports, and Advanced. The main content area is titled 'Static Mobility Group Members' and shows a table with columns for MAC Address, IP Address(Ipv4/Ipv6), Group Name, Multicast IP, and Status. Two rows are visible, both with a status of 'Up'.

Local Mobility Group	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
qytang	6c:20:56:65:a6:a0	10.1.1.101	qytang	239.1.1.1	Up
qytang	58:8d:09:cd:b9:60	10.1.1.100	qytang	239.1.1.1	Up



WLC5508-1配置锚

The screenshot shows the Cisco WLC5508-1 configuration interface. The top navigation bar includes 'MONITOR', 'WLANs' (highlighted with a red box and a '1' in a red circle), 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The main content area displays a table of WLAN configurations. A context menu is open over the second row, with 'Mobility Anchors' highlighted and a red box and '2' in a red circle next to it.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	qytang	qytang	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Inter-controller	Inter-controller	Enabled	[WPA2][Auth(802.1X)]



WLC5508-1配置锚

The screenshot displays the Cisco WLC5508-1 configuration interface for Mobility Anchors. The interface includes a navigation menu at the top with options like MONITOR, WLANs, TROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The main configuration area is titled 'Mobility Anchors' and features a table with columns for 'Switch IP Address (Anchor)', 'Data Path', and 'Control Path'. The 'Switch IP Address (Anchor)' is set to 'local', 'Data Path' is 'up', and 'Control Path' is 'up'. A 'Mobility Anchor Create' button is located below the table. The interface also includes a 'Back' button in the top right corner.

Switch IP Address (Anchor)	Data Path	Control Path
local	up	up



WLC5508-2配置锚

Save Configuration | Ping | Logout | Refresh

MONITOR **WLANs** 1 CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs 2

Advanced

Mobility Anchors < Back

WLAN SSID Inter-controller 3

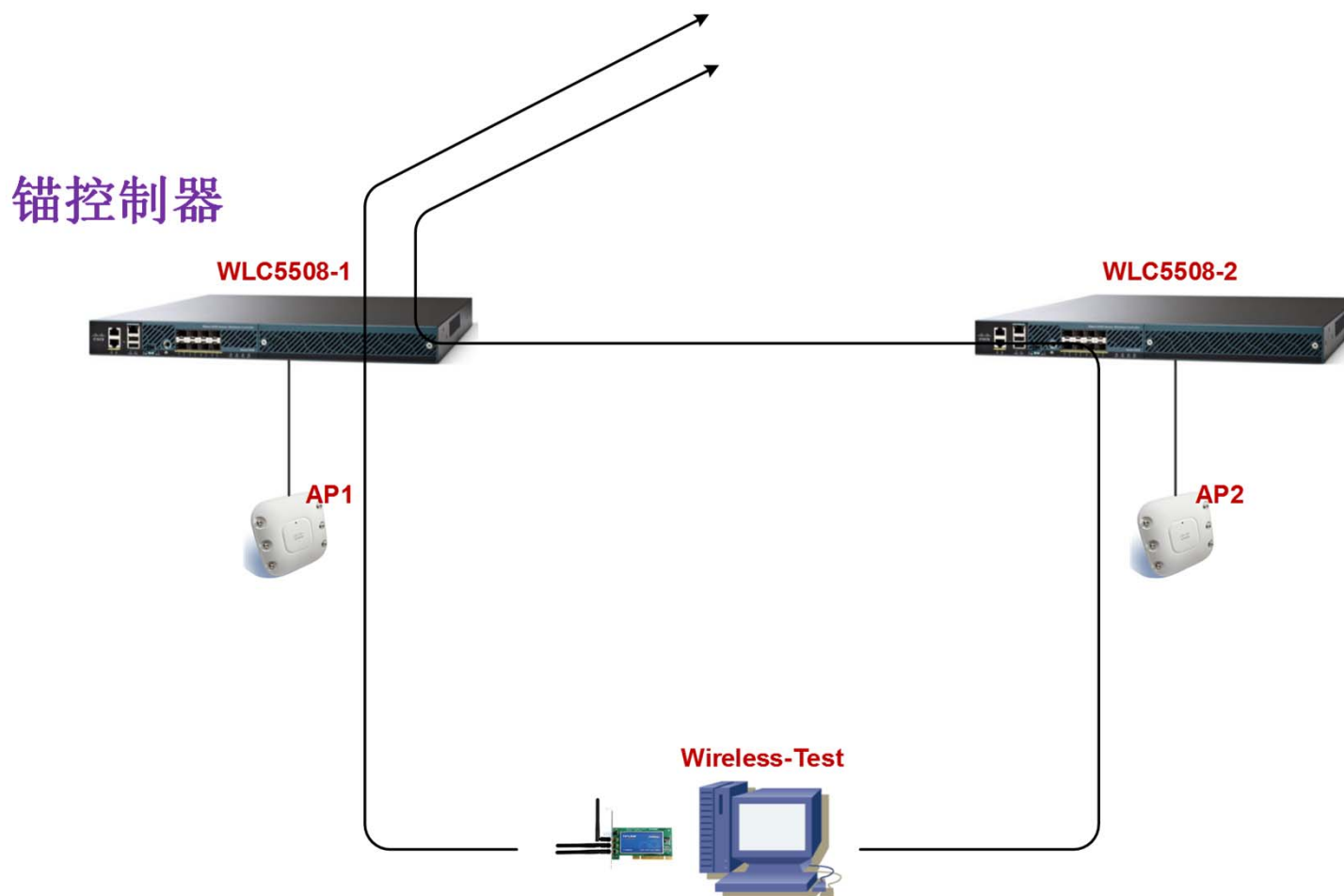
Switch IP Address (Anchor)	Data Path	Control Path
10.1.1.100 4	up	up

Mobility Anchor Create

Switch IP Address (Anchor) local



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

Static Mobility Group Members

Local Mobility Group	qytang			
MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
58:8d:09:cd:b9:60	10.1.1.100	qytang	0.0.0.0	Up

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

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

注意删除所有锚链接配置
删除老的WLAN配置



WLC5508-1修改Group 组

The screenshot shows the Cisco WLC5508-1 configuration interface. The 'CONTROLLER' tab is selected, and the 'General' sub-tab is active. The 'Default Mobility Domain Name' field is highlighted with a red circle and the number 3, containing the value 'cisco'. Other settings include Name (WLC5508-1), 802.3x Flow Control Mode (Disabled), LAG Mode on next reboot (Disabled), Broadcast Forwarding (Disabled), AP Multicast Mode (Unicast), AP IPv6 Multicast Mode (Unicast), AP Fallback (Enabled), CAPWAP Preferred Mode (ipv4), Fast SSID change (Disabled), Link Local Bridging (Disabled), User Idle Timeout (300), ARP Timeout (300), Web Radius Authentication (PAP), Operating Environment (Commercial), Internal Temp Alarm Limits (0 to 65 C), WebAuth Proxy Redirection Mode (Disabled), WebAuth Proxy Redirection Port (0), Global IPv6 Config (Enabled), Web Color Theme (Default), and HA SKU secondary unit (Disabled). A note at the bottom states: '1. Multicast is not supported with FlexConnect on this platform.'

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

Static Mobility Group Members

Local Mobility Group	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
cisco	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	Up

取消组播配置

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



WLC5508-2 删除组WLC5508-1

Static Mobility Group Members

Local Mobility Group	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
qytang	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	Up

取消组播配置

WLC5508-1 MAC:
58:8d:09:cd:b9:60



WLC5508-1 创建vlan40

The screenshot displays the Cisco WLC configuration interface for creating a new interface. The 'CONTROLLER' tab is selected, and the 'Interfaces > Edit' configuration page is shown. The 'General Information' section is expanded, showing 'Interface Name' as '1'. The 'DHCP Information' section is also expanded, showing 'Primary DHCP Server' as '40.1.1.254'. The 'Physical Information' section is expanded, showing 'Port Number' as '1'. The 'Interface Address' section is expanded, showing 'VLAN Identifier' as '40', 'IP Address' as '40.1.1.253', 'Netmask' as '255.255.255.0', and 'Gateway' as '40.1.1.254'. Red boxes and numbers 1, 2, 3, and 4 highlight specific configuration fields.



WLC5508-1 创建 Inter-subnet

The screenshot displays the Cisco WLC5508-1 configuration interface for creating an Inter-subnet WLAN. The interface is divided into several sections:

- Navigation:** The top navigation bar includes 'MONITOR', 'WLANs' (highlighted with a red box and '1'), 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' menu is expanded, showing 'WLANs' (highlighted with a red box and '2') and 'Advanced'.
- Configuration Page:** The main configuration area is titled 'WLANs > Edit 'Inter-subnet''. It features a 'General' tab (highlighted with a red box and '3') and other tabs: 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab contains the following fields:
 - Profile Name:** Inter-subnet
 - Type:** WLAN (highlighted with a red box and '4')
 - SSID:** Inter-subnet
 - Status:** Enabled
 - Security Policies:** [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
 - Radio Policy:** All (highlighted with a red box and '5')
 - Interface/Interface Group(G):** vlan40
 - Multicast Vlan Feature:** Enabled
 - Broadcast SSID:** Enabled
 - NAS-ID:** none
- Foot Notes:** A section at the bottom provides additional information:
 - 1 Web Policy cannot be used in combination with IPsec
 - 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
 - 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
 - 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
 - 3 When client exclusion is enabled, Timeout (value of zero means infinity) will require administrative override to re-associate



WLC5508-1 创建 Inter-subnet

The screenshot displays the Cisco WLC5508-1 configuration interface for creating an Inter-subnet WLAN. The interface is divided into several sections:

- WLANs > Edit 'Inter-subnet'**: The main configuration page.
- General**, **Security**, **Policy-Mapping**, **Advanced**: Configuration tabs.
- Layer 2**, **Layer 3**, **AAA Servers**: Sub-sections under the Security tab.
- Fast Transition**: Includes checkboxes for **Fast Transition** and **Over the DS**, and a **Reassociation Timeout** field set to 20 Seconds.
- Protected Management Frame**: Includes a **PMF** dropdown menu set to Disabled.
- WPA+WPA2 Parameters**: Includes checkboxes for **WPA Policy** and **WPA2 Policy-AES**.
- Authentication Key Management**: Includes checkboxes for **802.1X**, **CCKM**, **PSK**, **FT 802.1X**, and **FT PSK**.

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity. (will require administrative override to reset excluded...



WLC5508-1 创建 Inter-subnet

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'Inter-subnet'. The interface is divided into several sections:

- General**: Contains tabs for Layer 2, Layer 3, AAA Servers, Policy-Mapping, and Advanced.
- Security**: Contains a table for AAA Servers.
- Radius Server Accounting**: Contains a checkbox for Interim Update and a text field for Interim Interval.
- LDAP Servers**: Contains a table for LDAP Servers.

The AAA Servers table is as follows:

Server	Authentication Servers	Accounting Servers
Server 1	IP:10.1.1.12, Port:1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

The Radius Server Accounting section is configured with Interim Update checked and Interim Interval set to 0.

The LDAP Servers section is currently empty.

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded)



WLC5508-1 创建 Inter-subnet

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'Inter-subnet'. The 'Advanced' tab is selected, and several settings are highlighted with red boxes and numbered callouts:

- 1:** The 'WLANs' menu item in the top navigation bar.
- 2:** The 'WLANs' menu item in the left sidebar.
- 3:** The 'Advanced' tab in the configuration pane.
- 4:** The 'Allow AAA Override' checkbox, which is checked and set to 'Enabled'.
- 5:** The 'Apply' button in the top right corner of the configuration pane.

Other visible settings in the 'Advanced' tab include:

- Coverage Hole Detection: Enabled
- Enable Session Timeout: 1800 (Session Timeout in secs)
- Aironet IE: Enabled
- Diagnostic Channel: 18
- Override Interface ACL: IPv4: None, IPv6: None
- Layer2 Acl: None
- P2P Blocking Action: Disabled
- Client Exclusion: Enabled, 60 (Timeout Value in secs)
- Maximum Allowed Clients: 0
- DHCP: DHCP Server (Override), DHCP Addr. Assignment (Required)
- OEAP: Split Tunnel (Enabled)
- Management Frame Protection (MFP): MFP Client Protection (Optional)
- DTIM Period (in beacon intervals): 802.11a/n (1 - 255): 1, 802.11b/g/n (1 - 255): 1
- NAC: NAC State (None)
- Load Balancing

Foot Notes:

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, 3 Timeout Value of zero means infinity (will require administrative override to reset excluded)



WLC5508-2 创建 Inter-subnet

The screenshot displays the Cisco WLC5508-2 configuration interface for creating an Inter-subnet WLAN. The interface is titled "WLANs > Edit 'Inter-subnet'" and includes a navigation bar with "MONITOR", "WLANs", "ROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", "HELP", and "FEEDBACK". The "WLANs" menu is highlighted with a red box and a circled "1". The "WLANs" dropdown menu is also highlighted with a red box and a circled "2". The "General" tab is selected, highlighted with a red box and a circled "3". The configuration fields are as follows:

- Profile Name: Inter-subnet
- Type: WLAN
- SSID: Inter-subnet
- Status: Enabled
- Security Policies: [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface/Interface Group(G): vlan30
- Multicast Vlan Feature: Enabled
- Broadcast SSID: Enabled
- NAS-ID: none

The "Radio Policy" and "Interface/Interface Group(G)" dropdowns are highlighted with a red box and a circled "5". The "Profile Name", "Type", "SSID", and "Status" fields are highlighted with a red box and a circled "4".

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client authentication is enabled, the Timeout Value of new session (infinite) will result in Authentication timeout. As a result, the client will not be able to connect to the network.



WLC5508-2 创建 Inter-subnet

The screenshot shows the Cisco WLC configuration page for 'Inter-subnet'. The interface includes a navigation menu with 'WLANs' highlighted (1). On the left, 'WLANs' is selected in the sidebar (2). The 'Security' tab is active (3). Under the 'Layer 2' sub-tab (4), the 'Fast Transition Over the DS' checkbox is checked (5), and the 'Reassociation Timeout' is set to 20 seconds. In the 'Authentication Key Management' section, '802.1X' and 'FT 802.1X' are both checked and set to 'Enable' (6). The 'Protected Management Frame' section shows 'PMF' is set to 'Disabled'. The 'WPA+WPA2 Parameters' section shows 'WPA Policy' is disabled and 'WPA2 Policy-AES' is checked. The 'Foot Notes' section at the bottom provides additional context for the configuration.



WLC5508-2 创建 Inter-subnet

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'Inter-subnet'. The configuration is divided into several tabs: General, Security, Policy-Mapping, and Advanced. The Security tab is active, and the AAA Servers sub-tab is selected. The configuration includes a table for AAA Servers with columns for Authentication Servers and Accounting Servers. The first server is configured with IP: 10.1.1.12, Port: 1812. The Interim Update checkbox is checked, and the Interim Interval is set to 0.

Server	Authentication Servers	Accounting Servers
Server 1	IP: 10.1.1.12, Port: 1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Radius Server Accounting: Interim Update Interim Interval 0



WLC5508-2 创建 Inter-subnet

The screenshot displays the Cisco WLC5508-2 configuration page for a WLAN named 'Inter-subnet'. The interface is divided into several sections:

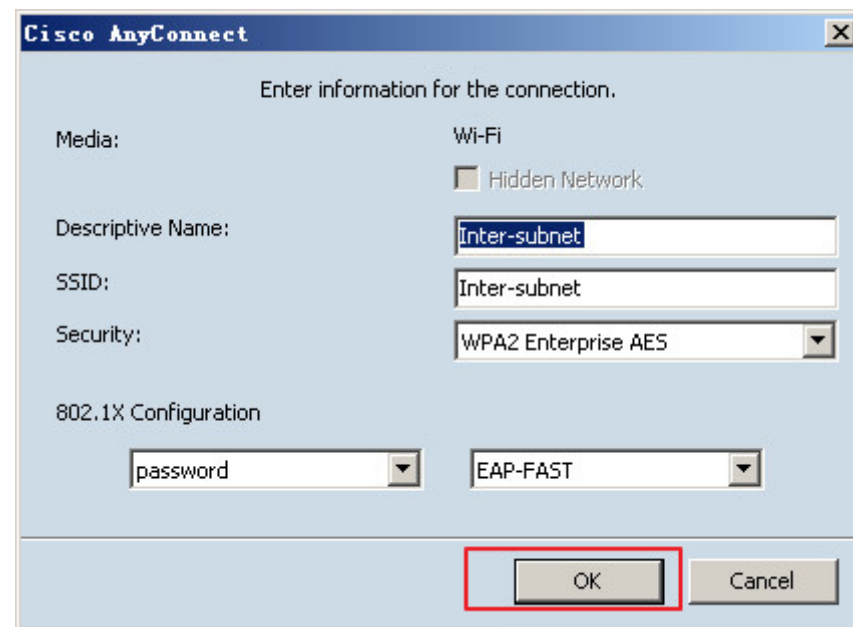
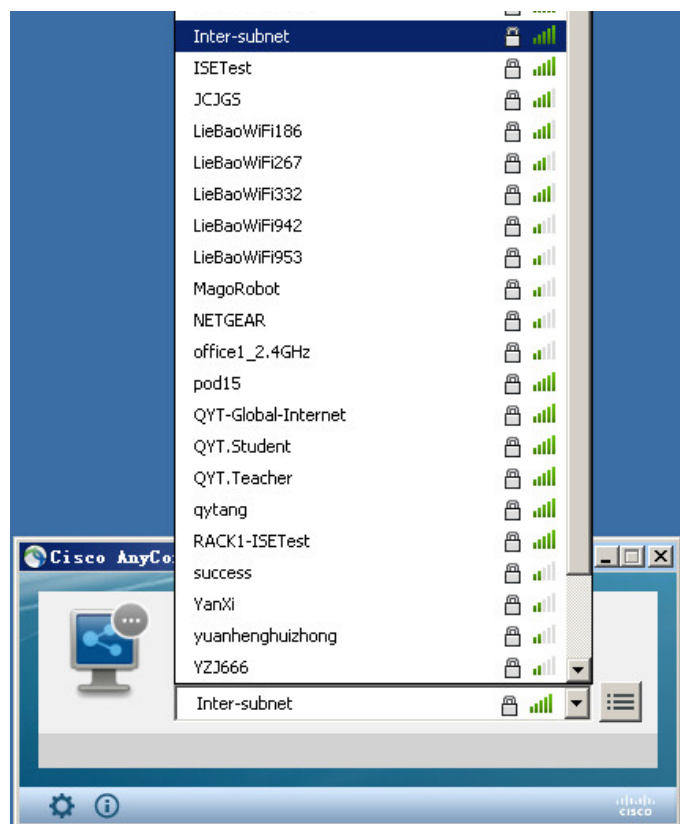
- WLANs:** A sidebar menu with 'WLANs' (2) and 'Advanced' (2) options.
- WLANs > Edit 'Inter-subnet':** The main configuration area with tabs for General, Security, QoS, Policy-Mapping, and Advanced (3).
- Advanced Tab:** Contains various settings:
 - Allow AAA Override:** Checked (4).
 - Coverage Hole Detection:** Checked.
 - Enable Session Timeout:** Checked, with a value of 1800.
 - Aironet IE:** Checked.
 - Diagnostic Channel:** 18.
 - Override Interface ACL:** IPv4: None, IPv6: None.
 - Layer2 Ad:** None.
 - P2P Blocking Action:** Disabled.
 - Client Exclusion:** Checked (3), with a Timeout Value of 60.
 - Maximum Allowed Clients:** 0.
 - DHCP:** DHCP Server (Override), DHCP Addr. Assignment (Required).
 - OEAP:** Split Tunnel (Enabled).
 - Management Frame Protection (MFP):** MFP Client Protection (4) set to Optional.
 - DTIM Period (in beacon intervals):** 802.11a/n (1 - 255) set to 1, 802.11b/g/n (1 - 255) set to 1.
 - NAC:** NAC State set to None.
 - Load Balancing:** (Section header).
- Buttons:** '< Back' and 'Apply' (5) buttons are visible at the top right.

Foot Notes:

- Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity. It will require administrative override to re-act excluded

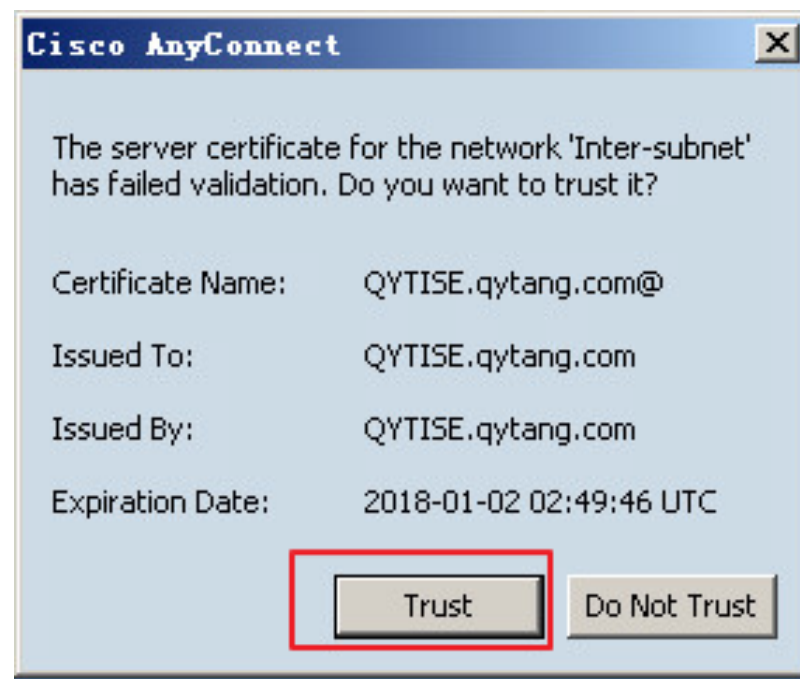
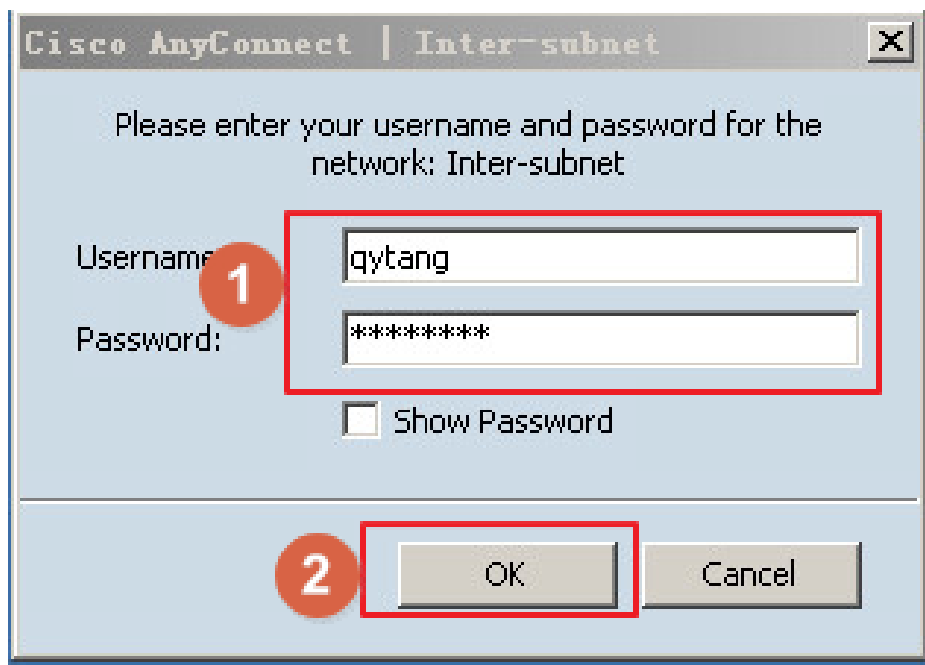


客户端测试: Inter-subnet





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:fab: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-B0BE03FA5426>:

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

隧道适配器 6T04 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-Interfaces:

    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:
10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
10.1.1.254 的回复: 字节=32 时间=88ms TTL=255
10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
10.1.1.254 的回复: 字节=32 时间=3ms TTL=255
10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
10.1.1.254 的回复: 字节=32 时间=4ms TTL=255
10.1.1.254 的回复: 字节=32 时间=1ms TTL=255
10.1.1.254 的回复: 字节=32 时间=2ms TTL=255
```

Cisco AnyConnect Secure Mobility Client

Network: Connected (40.1.1.1)

Inter-subnet



WLC 5508-1查看关联

The screenshot shows the Cisco WLC Monitor interface. The 'MONITOR' tab is selected (1). In the left sidebar, the 'Clients' link is highlighted (2). The main content area displays a table of clients with the following data:

Client MAC Addr	IP Address (IPv4/IPv6)	AP Name	WLAN
a0:63:91:bb:d3:b2	40.1.1.1	AP1	Inter

The IP address '40.1.1.1' is highlighted with a red box and a circled '3'.



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

802.11a/n Cisco APs > Configure

Note: Changing any of the parameters causes i 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

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

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

```
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

Monitor

MONITOR 1

CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

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	WL#
a0:63:91:bb:d3:b2	40.1.1.1	AP2	3

3

两边都有
关联信息

注意登陆
WLC5508-2



控制器验证测试效果

Monitor

MONITOR 1

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
a0:63:91:bb:d3:b2	40.1.1.1	10.1.1.101	Inter

3

两边都有
关联信息

注意登陆
WLC5508-1



三层漫游效果





WLC 5508-1 关闭AP1

The screenshot shows the Cisco WLC 5508-1 configuration interface. The 'WIRELESS' menu is selected (1). In the left sidebar, 'All APs' is selected (2). The 'General' tab is active (3). The 'Admin Status' dropdown is set to 'Disable' (4).

General		Versions	
AP Name	AP1	Primary Software Version	8.0.140.0
Location	default location	Backup Software Version	0.0.0.0
AP MAC Address	fc:5b:39:37:1a:98	Predownload Status	None
Base Radio MAC	68:99:cd:06:5f:30	Predownloaded Version	None
Admin Status	Disable	Predownload Next Retry Time	NA
AP Mode	local	Predownload Retry Count	NA
AP Sub Mode	None	Boot Version	15.2.2.0
Operational Status	REG	IOS Version	15.3(3)1A10\$
Port Number	1	Mini IOS Version	0.0.0.0
Venue Group	Unspecified	IP Config	
Venue Type	Unspecified	CAPWAP Preferred Mode	Ipv4 (Global Cor
Venue Name		DHCP Ipv4 Address	20.1.1.2
Language		Static IP (Ipv4/Ipv6)	<input type="checkbox"/>
Network Spectrum Interface Key	C3C482749862E8EE7277FB2D6C786160	Time Statistics	
GPS Location		UP Time	0 d, 01 h 09 m 4
GPS Present	No	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

The screenshot shows the Cisco Wireless LAN Controller GUI. The top navigation bar includes 'MONITOR' (highlighted with a red box and a '1' in a red circle), 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'Monitor' section with 'Clients' highlighted (marked with a red box and a '2' in a red circle). The main content area displays a table with the following columns: WLAN Profile, WLAN SSID, User Name, Protocol, Status, Auth, Port, Slot Id, PMIPv6, WGB, and Device Type. A single entry is shown with values: Inter-subnet, Inter-subnet, qytang, 802.11(Mobile), Associated, Yes, 1, 0, No, No, and Unk. A context menu is open over the 'Unk' cell, with 'Remove' highlighted (marked with a red box and a '3' in a red circle). Other menu items include LinkTest, Disable, 802.11aTSM, and 802.11b/gTSM. The top right corner of the GUI has links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'.

WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	PMIPv6	WGB	Device Type
Inter-subnet	Inter-subnet	qytang	802.11(Mobile)	Associated	Yes	1	0	No	No	Unk



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               . . . . . : 00-63-91-BB-D3-B2
   DHCP 已启用            . . . . . : 是
   自动配置已启用        . . . . . : 是
   本地连接 IPv6 地址 . . . . . : fe80::c0e0:fab: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 IAD            . . . . . : 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
   TCP/IP 上的 NetBIOS    . . . . . : 已启用

隧道适配器 isatap.<?F06461E-C4A6-4E5C-8AFC-BABE03FA5426>:

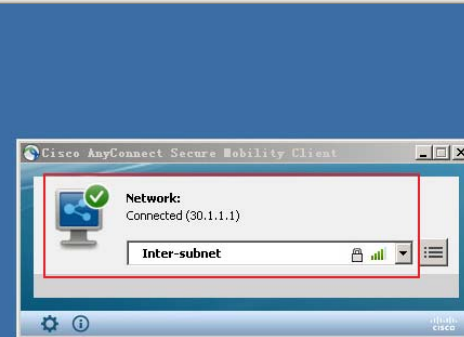
   媒体状态               . . . . . : 媒体已断开
   连接特定的 DNS 后缀   . . . . . :
   描述                   . . . . . : Microsoft ISATAP Adapter
   物理地址               . . . . . : 00-00-00-00-00-00-E0
   DHCP 已启用            . . . . . : 否
   自动配置已启用        . . . . . : 是

隧道适配器 6T04 Adapter:

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

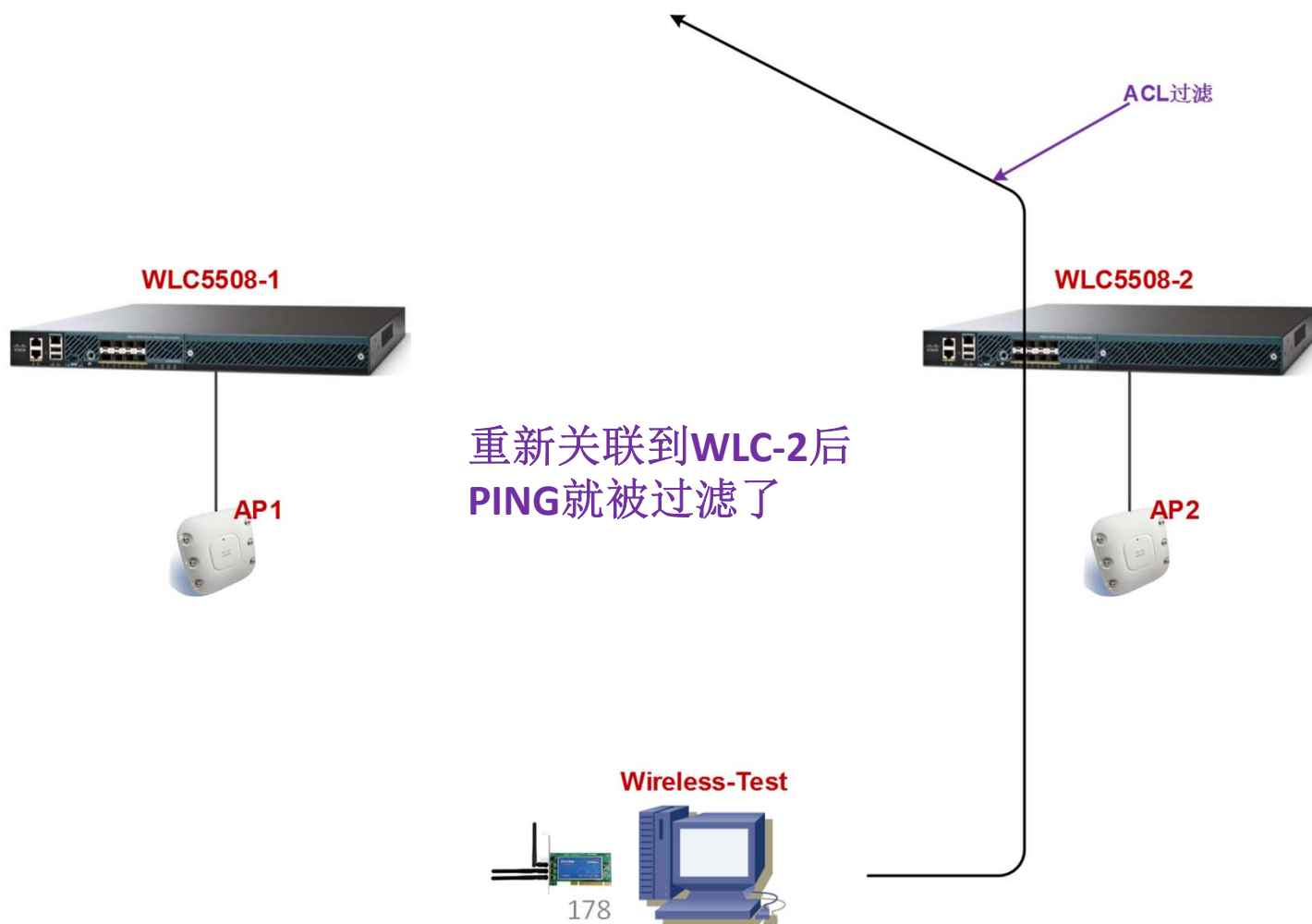
```
管理员: C:\Windows\system32\cmd.exe - ping 30.1.1.254 -t

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.
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





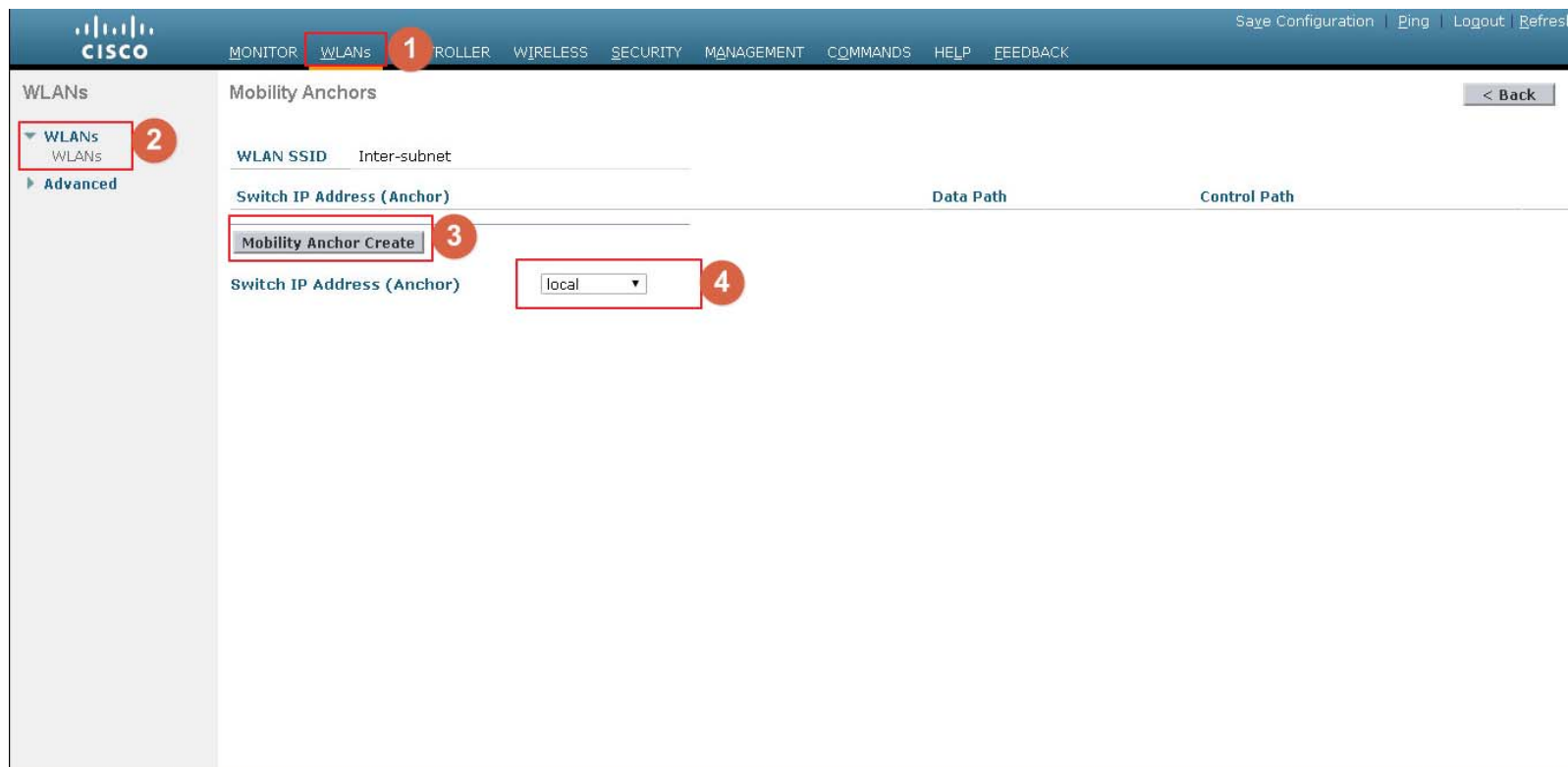
WLC5508-1 配置锚

The screenshot shows the Cisco WLC configuration interface for WLANs. The 'WLANs' tab is selected and highlighted with a red box and the number '1'. In the left sidebar, the 'WLANs' menu item is expanded and highlighted with a red box and the number '2'. The main content area displays a table with one entry: WLAN ID 1, Type WLAN, Profile Name Inter-subnet, WLAN SSID Inter-subnet, Admin Status Enabled, and Security Policies [WPA2][Auth(802.1X)][Auth(FT 802.1X)]. A context menu is open over the entry, with 'Mobility Anchors' highlighted and marked with a red box and the number '3'. The table has columns: WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. The table contains one row with the following data: 1, WLAN, Inter-subnet, Inter-subnet, Enabled, [WPA2][Auth(802.1X)][Auth(FT 802.1X)].

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Inter-subnet	Inter-subnet	Enabled	[WPA2][Auth(802.1X)][Auth(FT 802.1X)]



WLC5508-1 配置锚



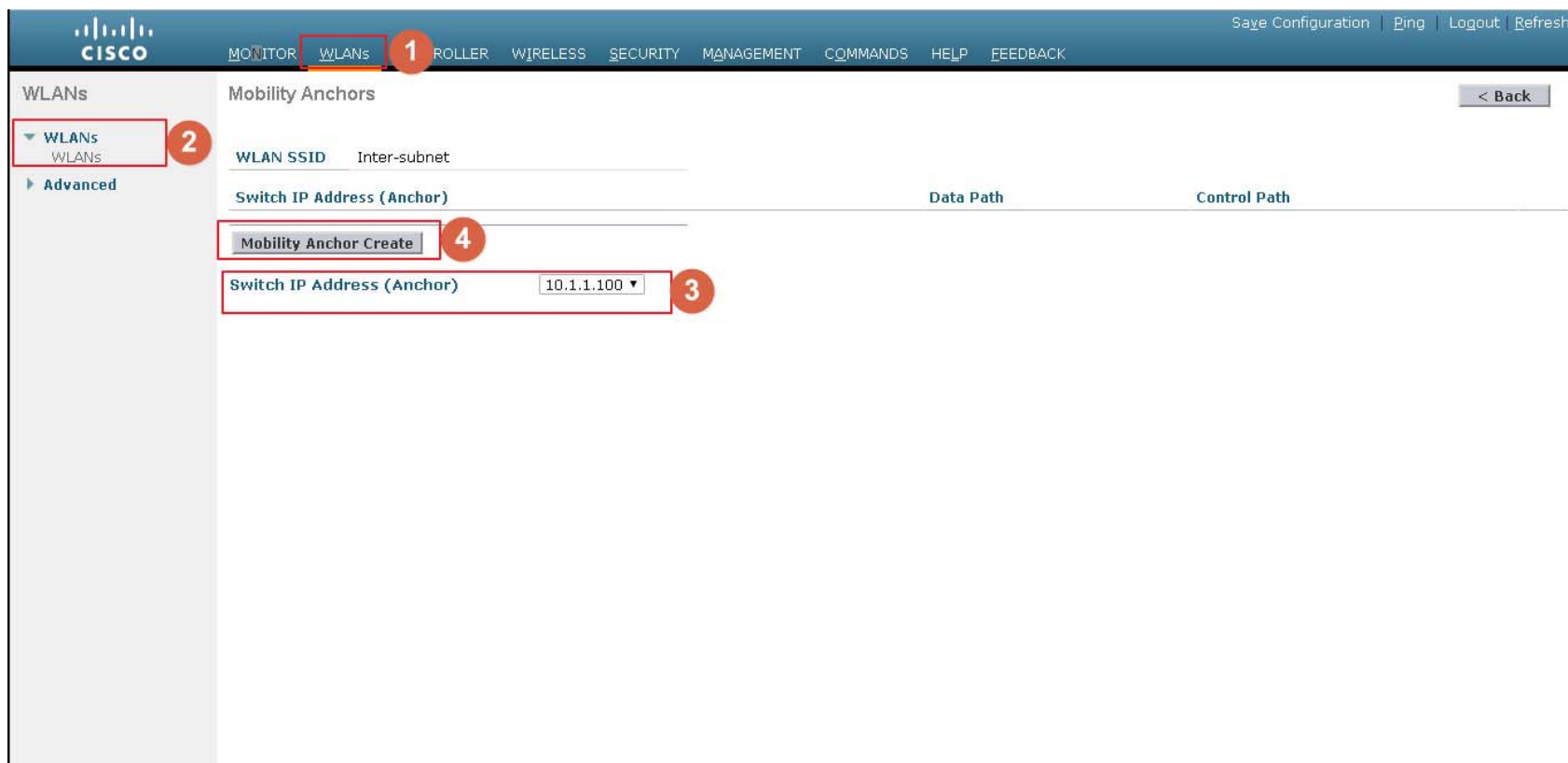


WLC5508-2 配置锚

The screenshot shows the Cisco WLC5508-2 configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'ROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' tab is selected and highlighted with a red box and a red circle containing the number '1'. On the left sidebar, the 'WLANs' menu is expanded, and the 'WLANs' sub-item is highlighted with a red box and a red circle containing the number '2'. The main content area displays a table of WLANs with the following columns: 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'. A single entry is shown with 'WLAN ID' 1, 'Type' WLAN, 'Profile Name' Inter-subnet, 'WLAN SSID' Inter-subnet, 'Admin Status' Enabled, and 'Security Policies' [WPA2][Auth(802.1X)][Auth(FT 802.1X)]. A context menu is open over the 'Security Policies' column, with the 'Mobility Anchors' option highlighted in blue and a red box and a red circle containing the number '3'. Other options in the menu include 'Remove', '802.11u', 'Foreign Maps', 'Service Advertisements', and 'Hotspot 2.0'. The bottom of the page shows a small JavaScript snippet: `javascript: actionAnchorClicked(0);`



WLC5508-2 配置锚





Test-PC 重新获取新的网段

```
自动配置已启用 . . . . . : 是
本地连接 IPv6 地址 . . . . . : fe80::c0e0:fafb:1174:9380%15<首选>
IPv4 地址 . . . . . : 40.1.1.1<首选>
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2017年9月23日 16:55:37
租约过期的时间 . . . . . : 2017年9月24日 16:55:38
默认网关 . . . . . : 40.1.1.254
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 . . . . . : fe0:0:0:ffff::1%1
                       fe0:0:0:ffff::2%1
                       fe0:0:0:ffff::3%1

TCP/IP 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-E0
DHCP 已启用 . . . . . : 否
自动配置已启用 . . . . . : 是

隧道适配器 6T04 Adapter:

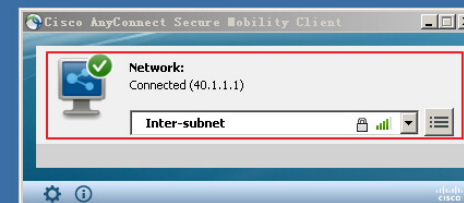
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Microsoft 6to4 Adapter
物理地址 . . . . . : 00-00-00-00-00-00-E0
DHCP 已启用 . . . . . : 否
自动配置已启用 . . . . . : 是
IPv6 地址 . . . . . : 2002:2801:101::2801:101<首选>
默认网关 . . . . . :
DNS 服务器 . . . . . : fe0:0:0:ffff::1%1
                       fe0:0:0:ffff::2%1
                       fe0:0:0:ffff::3%1

TCP/IP 上的 NetBIOS . . . . . : 已禁用

隧道适配器 Teredo Tunneling Pseudo-Interface:

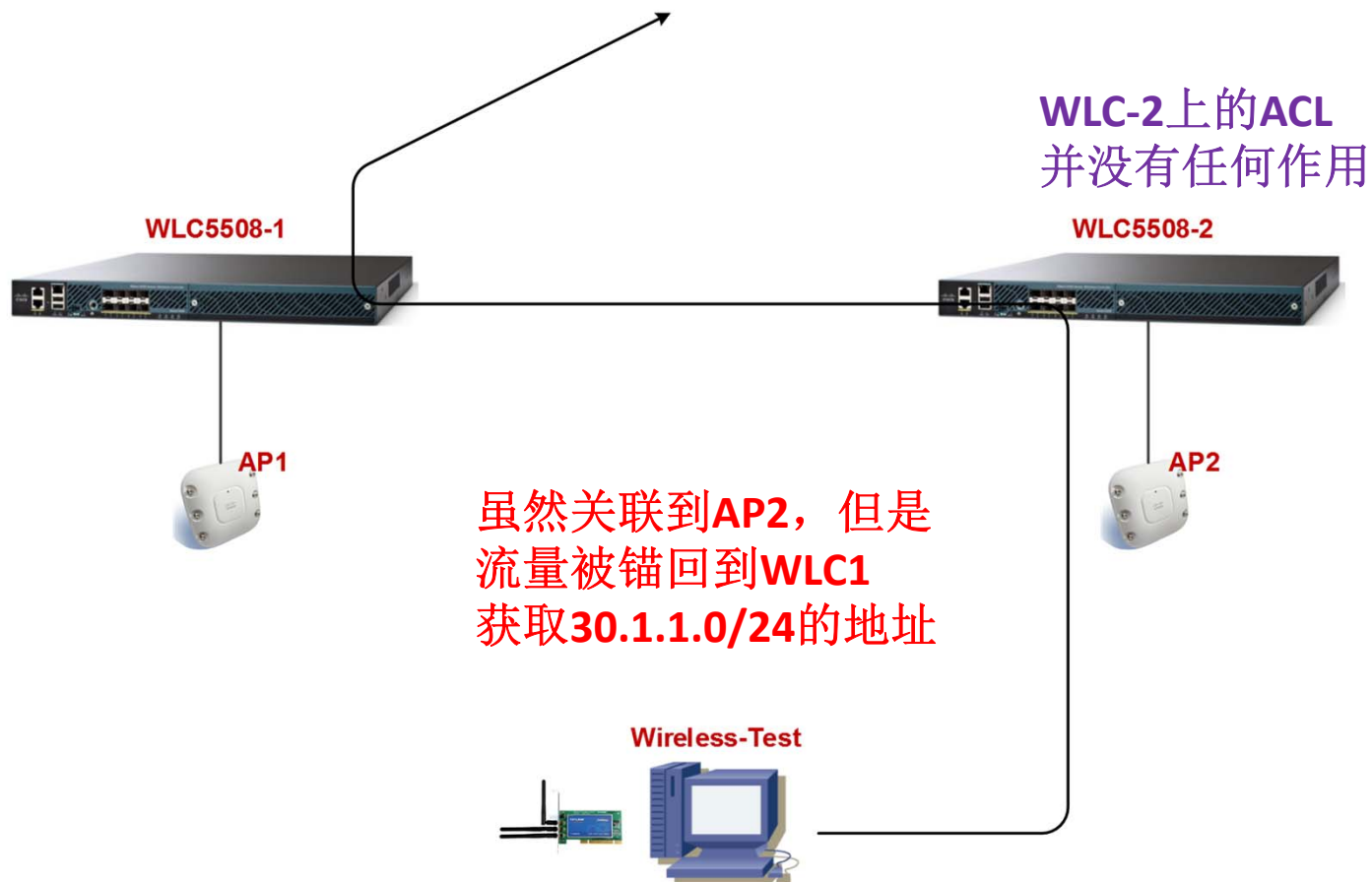
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Teredo Tunneling Pseudo-Interface
物理地址 . . . . . : 00-00-00-00-00-00-E0
DHCP 已启用 . . . . . : 否
自动配置已启用 . . . . . : 是

C:\Users\Administrator>
```





三层锚效果



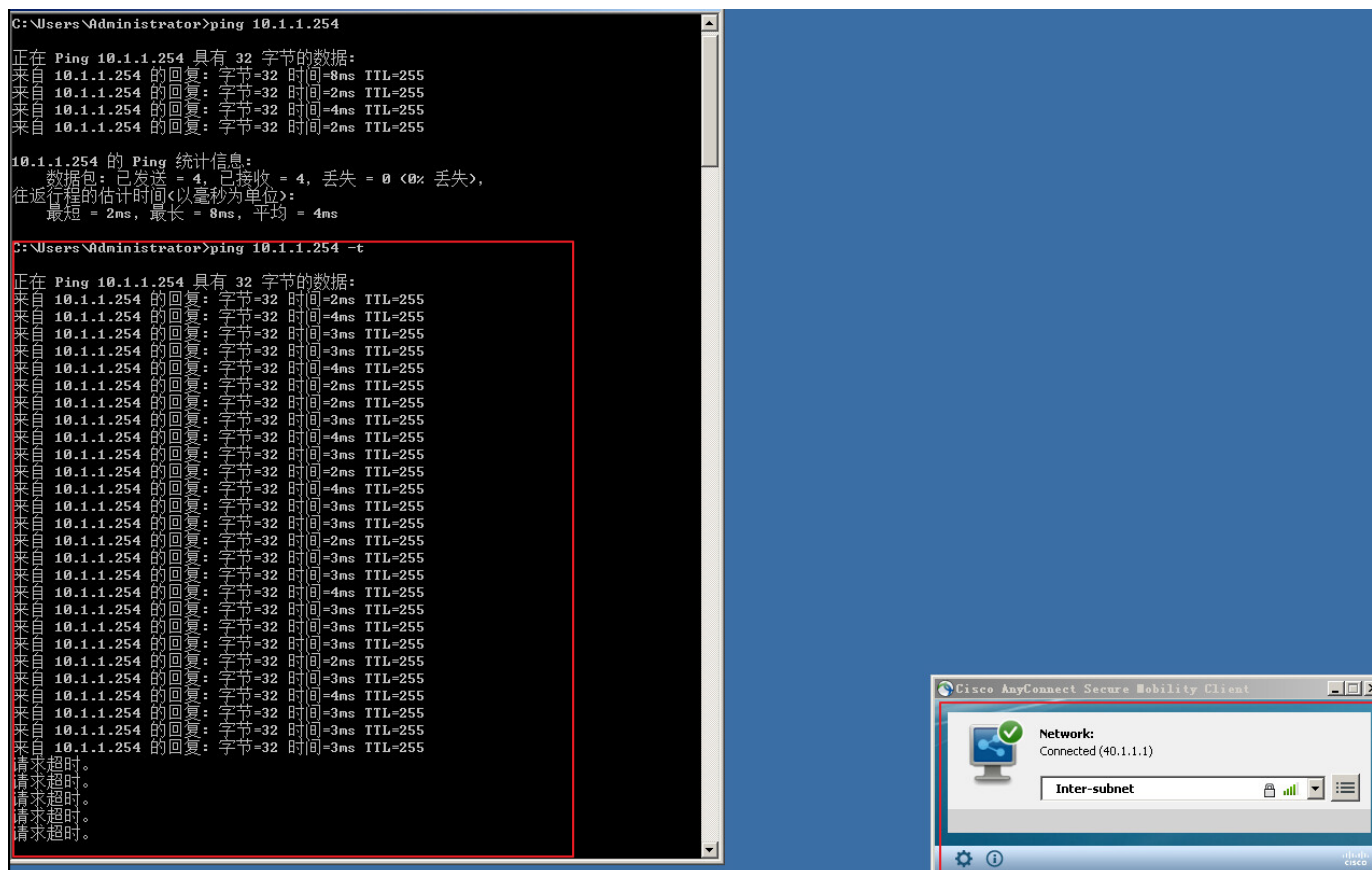


SW3560 设置列表

```
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





数据路径Down

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar lists various configuration categories, with 'Mobility Management' expanded to show 'Mobility Groups'. The main content area is titled 'Static Mobility Group Members' and contains a table with the following data:

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

The image shows a terminal window on the left and a Cisco AnyConnect client interface on the right. The terminal window displays a series of ping commands to 10.1.1.254, with each line showing a successful response (字节=32, 时间=...ms, TTL=255). A red box highlights the first few lines of the terminal output, with a red circle containing the number '1' next to it. The Cisco AnyConnect client interface on the right shows a 'Network' section with a green checkmark and the text 'Connected (40.1.1.1)'. Below this, there is a dropdown menu showing 'Inter-subnet'. A red box highlights the 'Network' section, with a red circle containing the number '2' next to it.

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

The screenshot shows the Cisco AireOS Controller GUI. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'LESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected and highlighted with a red box and a '1' in a red circle. The left sidebar shows a navigation menu with 'Mobility Management' expanded, and 'Mobility Groups' highlighted with a red box and a '2' in a red circle. The main content area displays 'Static Mobility Group Members' for the 'Local Mobility Group' 'cisco'. A table lists members with columns for MAC Address, IP Address (Ipv4/Ipv6), Group Name, Multicast IP, and Status. The second row, representing MAC 6c:20:56:65:a6:a0 and IP 10.1.1.101, is highlighted with a red box and a '3' in a red circle, showing a status of 'Control Path Down'.

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



测试动态锚

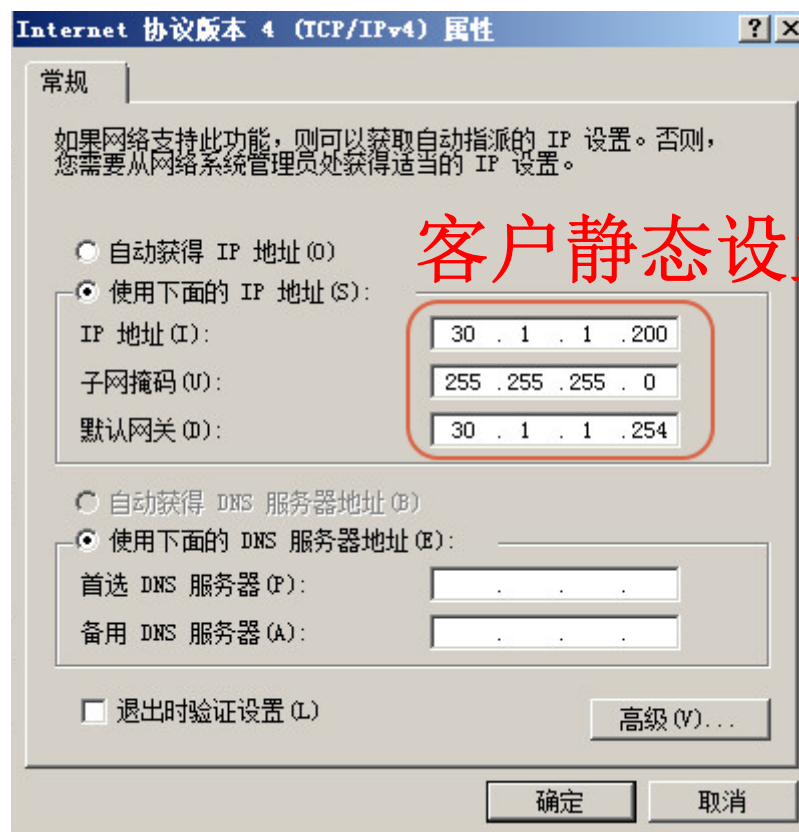
The screenshot shows the Cisco Wireless Management interface. The 'Wireless' section is active, and the 'All APs' view is selected. The 'Current Filter' is set to 'None'. The 'Number of APs' is 1. A table lists the APs, with 'AP2' highlighted. The 'Admin Status' for 'AP2' is 'Disabled', which is circled in red. The interface includes a navigation menu on the left and a top navigation bar with options like 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'.

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status
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

The screenshot displays a Windows desktop environment. On the left, a Command Prompt window titled '管理员: C:\Windows\system32\cmd.exe - ping 30.1.1.254 -t' shows a continuous stream of failed ping attempts to the IP address 30.1.1.254. The output for each attempt is: '来自 30.1.1.200 的回复: 无法访问目标主机。' (Reply from 30.1.1.200: Cannot access target host). On the right, the Cisco AnyConnect Secure Mobility Client window is open, showing a green checkmark and the text 'Network: Connected (30.1.1.200)'. Below this, it displays 'Inter-subnet' with a lock icon and a signal strength indicator. The Windows taskbar at the bottom shows the system tray with the date '2017/9/24' and time '17:10'.

虽然关联但是并不能
访问网络



测试动态锚

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'Inter-subnet'. The 'Advanced' tab is selected, and the 'Static IP Tunneling' option is checked and highlighted with a red circle and the number '2'. A red callout box with the number '1' points to the 'Advanced' tab itself. The page also features a large red text overlay: '两个控制器都激活动态锚技术 (static IP tunneling)'.

两个控制器都激活动态锚技术 (static IP tunneling)



测试动态锚

已经能正常访问网络

The screenshot displays a Windows desktop environment. On the left, a command prompt window titled '管理员: C:\Windows\system32\cmd.exe - ping 30.1.1.254 -t' shows a continuous stream of ping results. Each line indicates a successful response from 30.1.1.254 with a 32-byte payload, a time of approximately 1-4ms, and a TTL of 255. On the right, the Cisco AnyConnect Secure Mobility Client window is open, showing a green checkmark and the text 'Network: Connected (30.1.1.200)'. Below this, a dropdown menu is set to 'Inter-subnet'. The system tray at the bottom right shows the time as 17:13 on 2017/9/24.



测试动态锚

WLC-1信息, 客户端
关联到AP1

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name
a0:63:91:bb:d3:b2	30.1.1.200	AP1	Inter-subnet	Inter-subnet	qytang

WLC-2信息, 客户端
被动态锚到了AP2

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name
a0:63:91:bb:d3:b2	30.1.1.200	10.1.1.100	Inter-subnet	Inter-subnet	Unknown



测试动态锚

Monitor Clients > Detail

Max Number of Records 10 Clear AVC Stats

General	AVC Statistics
Port Number	1
Interface	vlan40
VLAN ID	40
CCX Version	CCXv5
E2E Version	Not Supported
Mobility Role	Export Foreign
Mobility Peer IP Address	10.1.1.101
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	200

WLC-1信息,
为外部标记

Monitor Clients > Detail

Max Number of Records 10 Clear AVC Stats

General	AVC Statistics
Client Type	Regular
User Name	
Port Number	1
Interface	vlan30
VLAN ID	30
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Export Anchor
Mobility Peer IP Address	10.1.1.100
Policy Manager State	RUN

WLC-2信息,
为锚标记