
CISCO
50.Cisco FlexConnect
教主技术进化论
翻越下一座技术的高峰
主讲人：现任明教教主
PPT制作：刘强龙、现任明教教主
Ciscolive!
BRKEWN-2013
© 2017 Cisco and/or its affiliates. All rights reserved.
Cisco Public
1

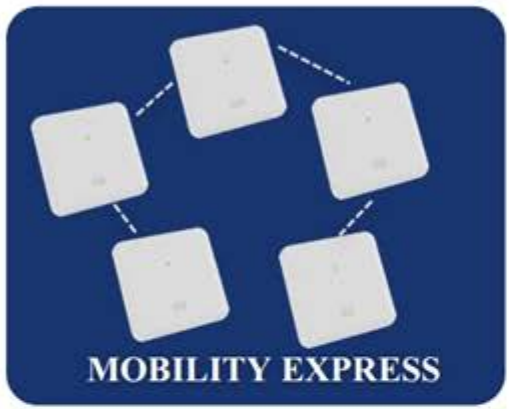
内容简介

1. FlexConnect 介绍
2. FlexConnect Group 介绍
3. FlexConnect Group 实验
   - 3.1 WLAN-VLAN 映射继承顺序
   - 3.2 VLAN Override
   - 3.3 VLAN Based Central Switching
   - 3.4 FlexConnect ACL
   - 3.5 Split Tunneling

1

FlexConnect 介绍

统一访问：一种架构，多种部署选项



Small Network

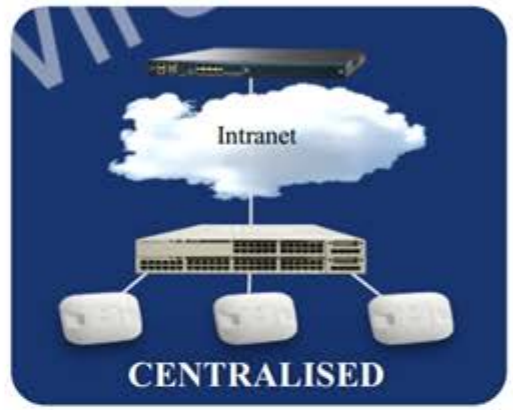
- Single site network
- Low IT footprints
- SP hotspots
- Virtual controller option AP
- [illegible]

Branch

- Distributed network
- Highly scalable
- First in class for distributed networks
- Controllers
  - New 8540 Controller
  - New 5520 Controller
  - or other Cisco Wireless Controllers

Small Campus / Branch

- Simplified Campus/Branch
- Consistent Wired/Wireless
- Common OS
- Controllers
  - Integrated 3650/3850/Sup 8E



Large Campus

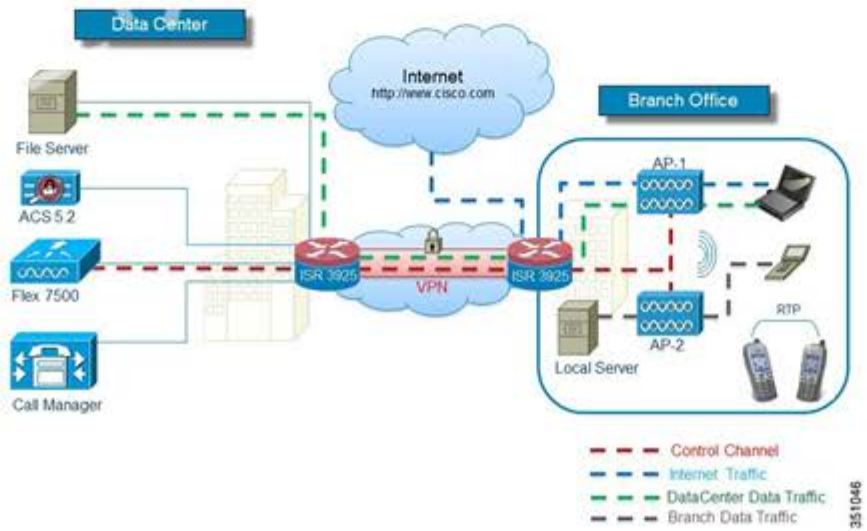
- Data centre hosted controller
- Distributed enterprises
- Controllers
  - New 8540 Controller
  - New 5520 Controller
  - or other Cisco Wireless Controllers

Aironet Access Points
11ac Wave2 : 3800/2800/1800
11ac: 3700/2700/1700
11n: 3600/ 2600/ 1600/ 700i/700w

Prime Infrastructure, Identity Service Engine, Connected Mobile Experiences

FlexConnect 介绍

- FlexConnect is a wireless solution for branch office and remote office deployments. （FlexConnect 是分支机构和远程办公室部署的无线解决方案。）
- It enables you to configure and control APs in a branch or remote office from the corporate office through a WAN link without the deployment of a controller in each office. （它使你能够通过 WAN链路在公司配置和控制分支机构的 AP，而无需在每个分支部署控制器）
- The FlexConnect APs can switch client data traffic locally and perform client authentication locally. （FlexConnect AP 可以在本地交换客户端数据流量，并在本地执行客户端身份验证）
- When they are connected to the controller, they can also send traffic back to the controller. （当AP连接到控制器时，也可以将流量发送回控制器）



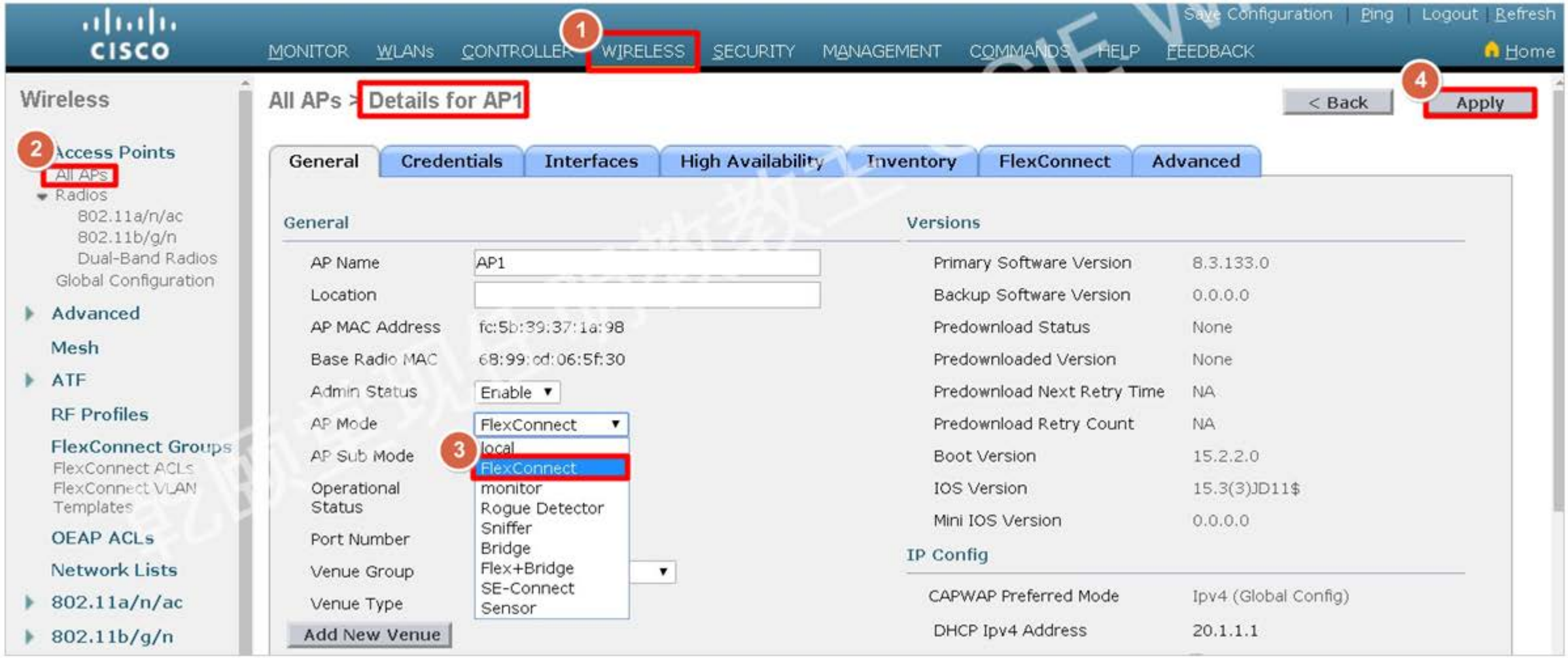
FlexConnect 术语

- **Connected Mode（连接模式）** - When FlexConnect can reach Controller (connected state),it gets help from controller to complete client authentication.（WLC 对客端进行身份认证）
- **Standalone mode（独立模式）** - When controller is not reachable by FlexConnect, it goes into standalone state and does client authentication by itself.（AP 对客户进行身份认证）

- **Local Switching** - Data traffic switched onto local VLANs for an SSID（数据流量通过本地有线接口直接进入本地交换网络）
- **Central Switching** - Data traffic tunneled back to WLC for an SSID（数据流量通过CAPWAP隧道传回到 WLC 进行转发）

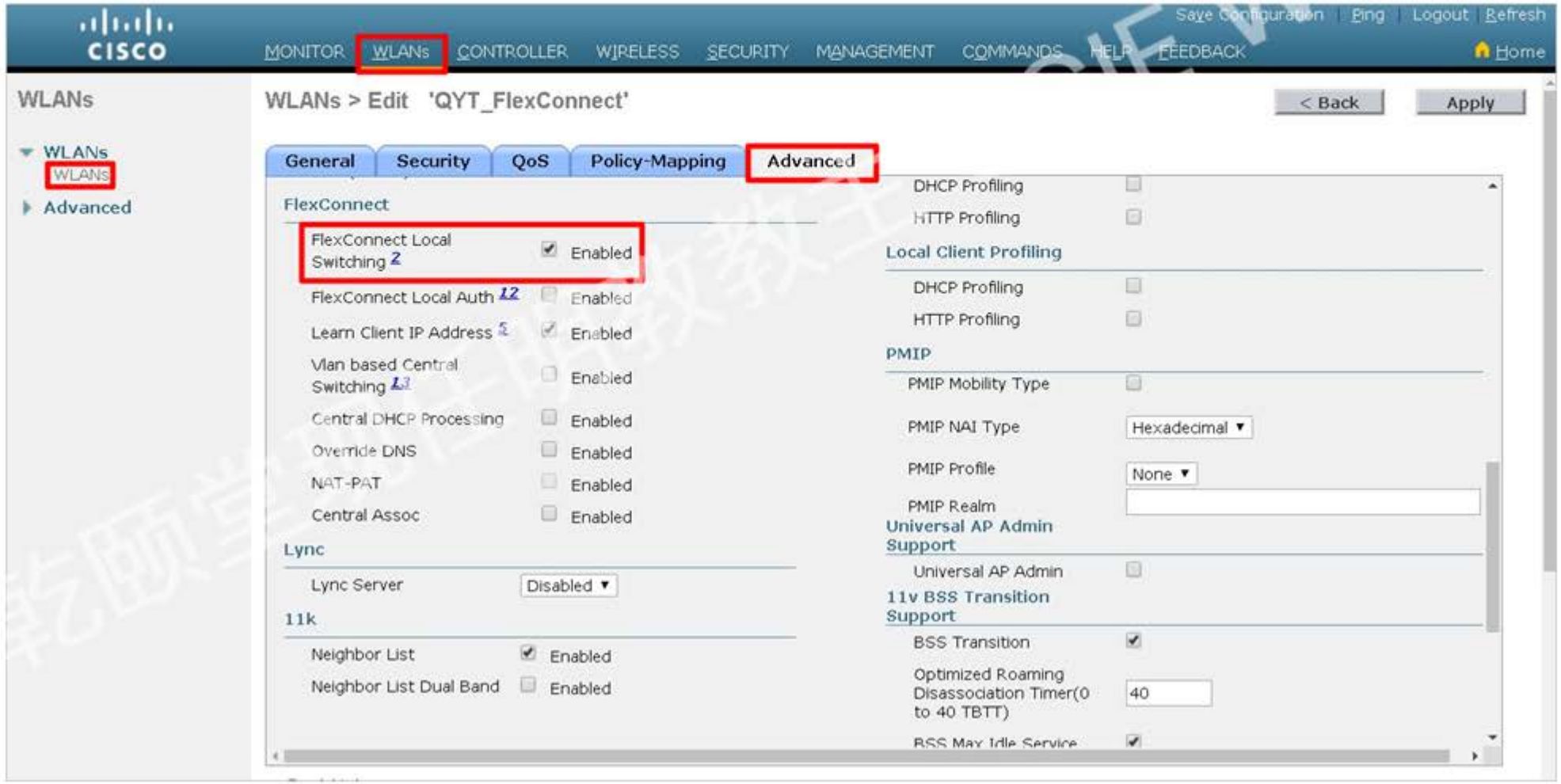
AP 配置 FlexConnect 模式

- AP 默认为 Local 模式，切换成 FlexConnect 模式，AP 不会重启。



FlexConnect 配置本地交换

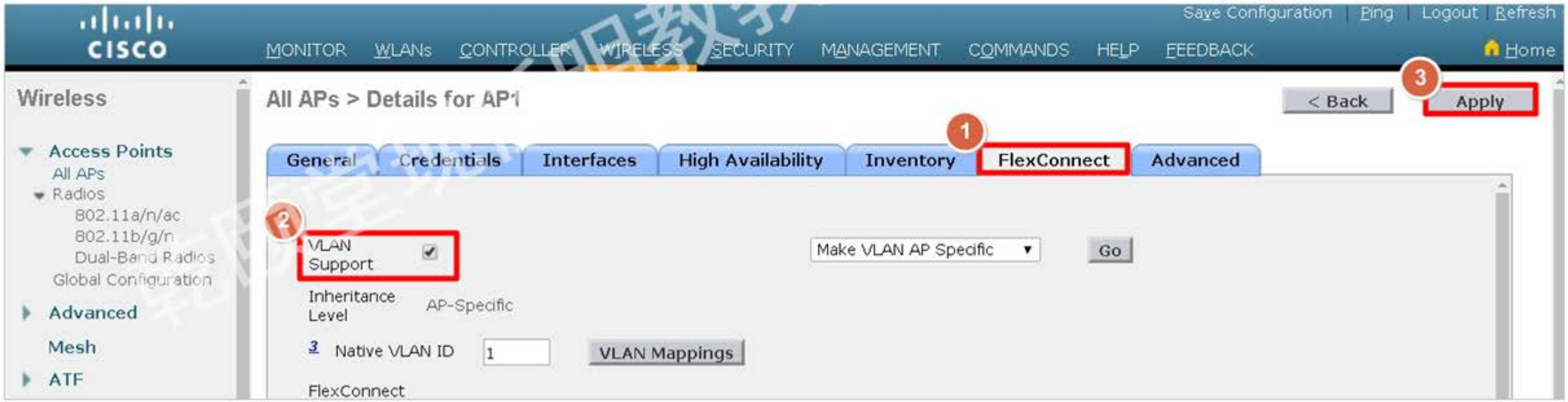
- 只有在 WLAN 下激活“FlexConnect Local Switching”，数据流量才会在本地交换。



FlexConnect VLAN Mapping

- FlexConnect AP can be connected on an access port or connected to a 802.1Q trunk port (using the native VLAN)（FlexConnect AP 可以连接到 access 接口或连接到 802.1Q 中继端口（使用 Native VLAN））

- VLAN mapping can be performed per AP configuration on WLC and/or by AP groups using Cisco Prime Infrastructure templates（可以使用 Cisco PI 模板在 WLC 上和/或 AP 组上按 AP 配置执行 VLAN 映射）

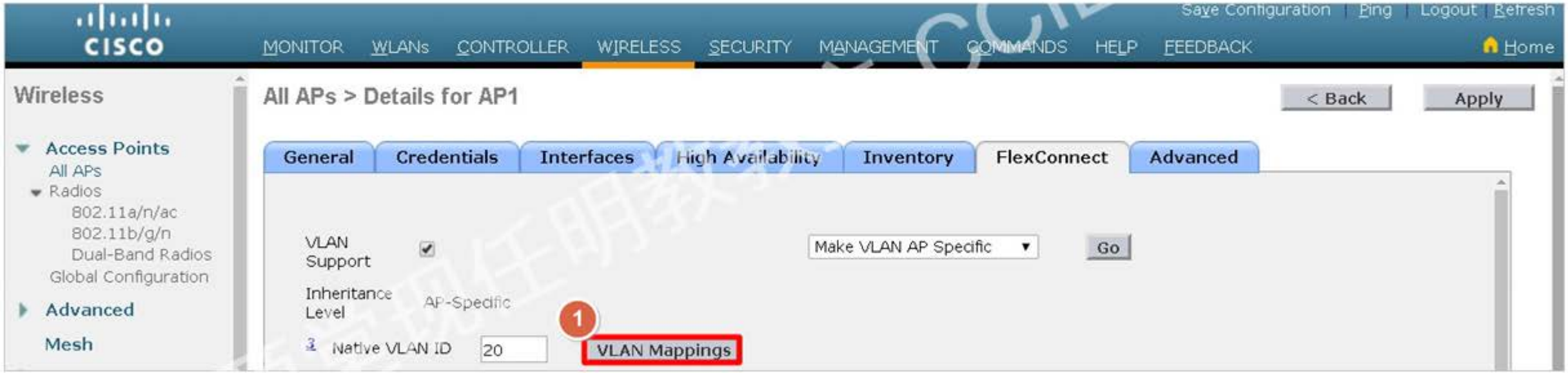


FlexConnect Native VLAN

- When connecting with Native VLAN on AP, L2 switchport must also match with corresponding Native VLAN configuration（在 AP 上连接 Native VLAN 时，2 层接口也必须设置响应的 Native VLAN）
- Each corresponding SSID that is allowed to be locally switch should be allowed on the corresponding switchport（应该在本地交换机接口上放行 SSID 映射的 VLAN 流量）

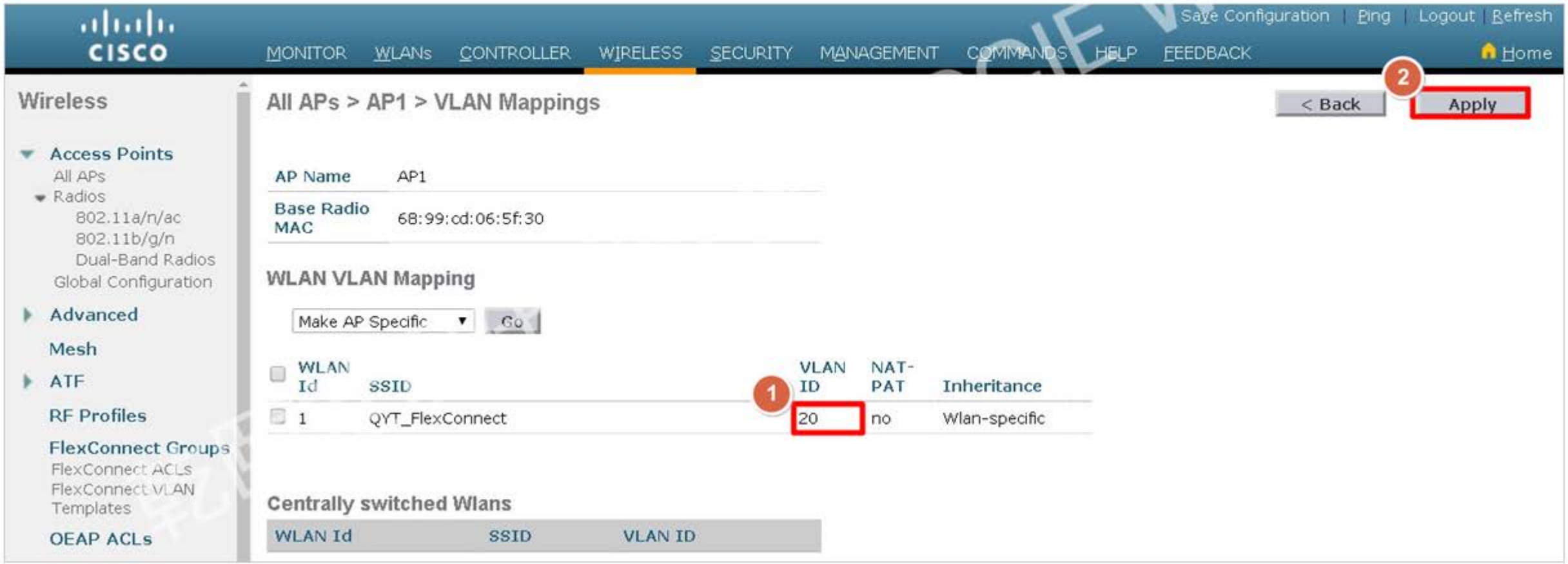
SSID to VLAN Mapping – 1

- 点击 VLAN Mappings



SSID to VLAN Mapping – 2

- 将 SSID 映射到本地的 VLAN



WAN 应用限制

Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	Max APs per Branch	Max Clients per Branch
Data	128 kbps	300 ms	5	25
Data+Voice	128 kbps	100 ms	5	25
Data	128 kbps	1 sec	1	1
Monitor	128 kbps	2 sec	5	N/A
Data	1.44 Mbps	1 sec	50	1000
Data+Voice	1.44 Mbps	100 ms	50	1000
Monitor	1.44 Mbps	2 sec	50	1000

FlexConnect 应用限制

- Some features are not available in standalone mode or in local switching mode
  - MAC/Web Auth in Standalone Mode（Web 认证需要 WLC 弹出 Portal，如果AP 是 Connected Mode 是可以支持的。）
  - VideoStream
  - IPv6 L3 Mobility
  - SXP TrustSec （8.4 版本以后可以支持）
  - See full list in «FlexConnect Feature Matrix »

  https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/112042-technote-wlc-00.html

FlexConnect 历史

- The **REAP** feature is supported up to WLC Release 3.2.215.（只支持本地交换，不支持多vlan，独立模式下只能发布一个 SSID）
- From WLC Release 4.0.155.5, this functionality is called Hybrid REAP（**H-REAP 混合远程边缘接入点**）with few enhancements until 7.0.x.x.（不支持 Pre-User 的授权）
- From 7.2.103 release, this feature is called **FlexConnect**.

FlexConnect 特性更新

7.2

- Smart AP Image Upgrade
- ACL's on FlexConnect AP
- AAA Over-ride of VLAN - dynamic VLAN assignment for locally switched clients
- H-REAP -> FlexConnect Re-branding
- Fast Roaming for Voice Clients
- Peer to Peer Blocking

7.3 & 7.4

Flex 7500 Scale Update

VLAN Based Central Switching

Split Tunneling

Central DHCP Processing

WGB/uWGB Support with local switching

Bidirectional Rate Limiting

Support for ISE BYOD Registration & Provisioning

7.5, 7.6 & 8.0

PEAP and EAP-TLS Support (7.5)

FlexConnect Group specific WLAN-VLAN mapping (7.5)

AAA Client ACL (7.5)

Ethernet Fallback (7.6)

Videostream for Local switching (8.0)

Faster time to deploy (8.0)

Flex with Mesh deployment support (8.0)

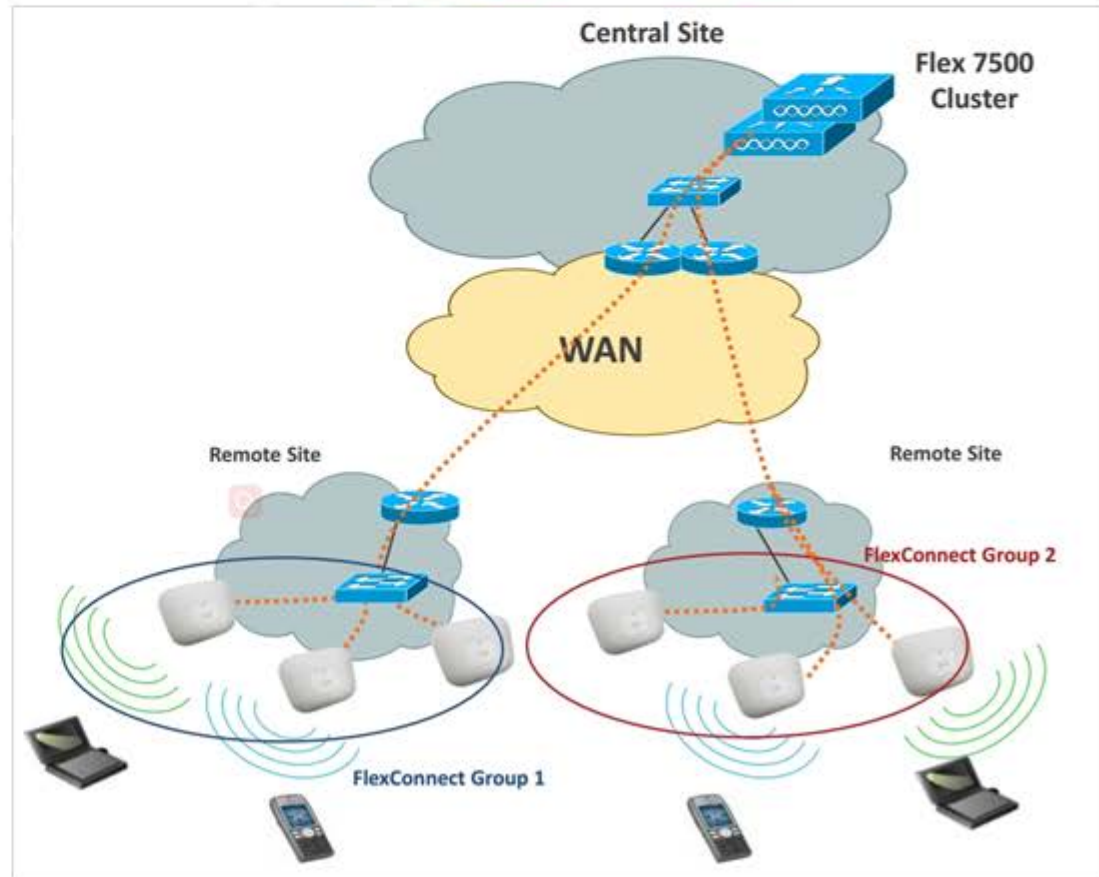
2

FlexConnect Group 介绍

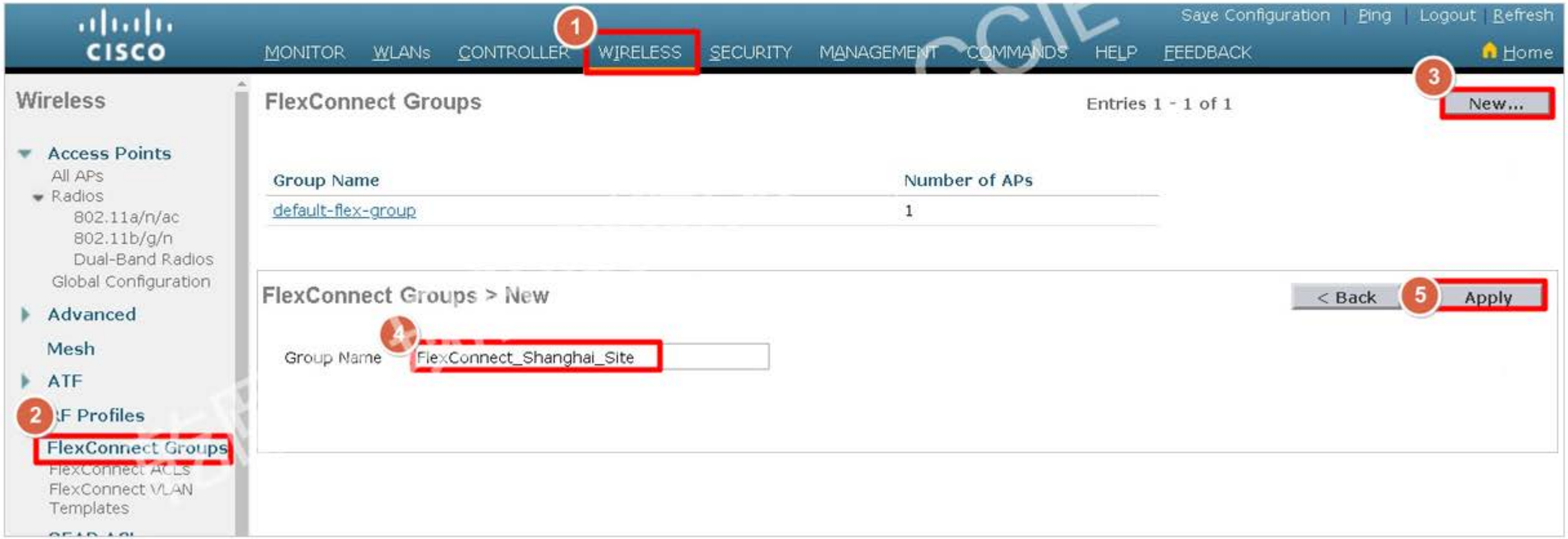
FlexConnect Group 介绍

- FlexConnect groups allow sharing of:
  - CCKM/OKC fast roaming keys（WLC 推送 key 到 FlexConnect Group）
  - Local/backup RADIUS servers IP/keys（需要在 FlexConnect Group 下配置 3A 服务器）
  - Local user authentication
  - Local EAP authentication
  - AAA-Override for Local Switching
  - Smart Image Upgrade
- 扩展信息

Scaling	Flex 7500	CT-5508	WiSM2	CT-2504
FlexConnect Groups	2000	100	100	20

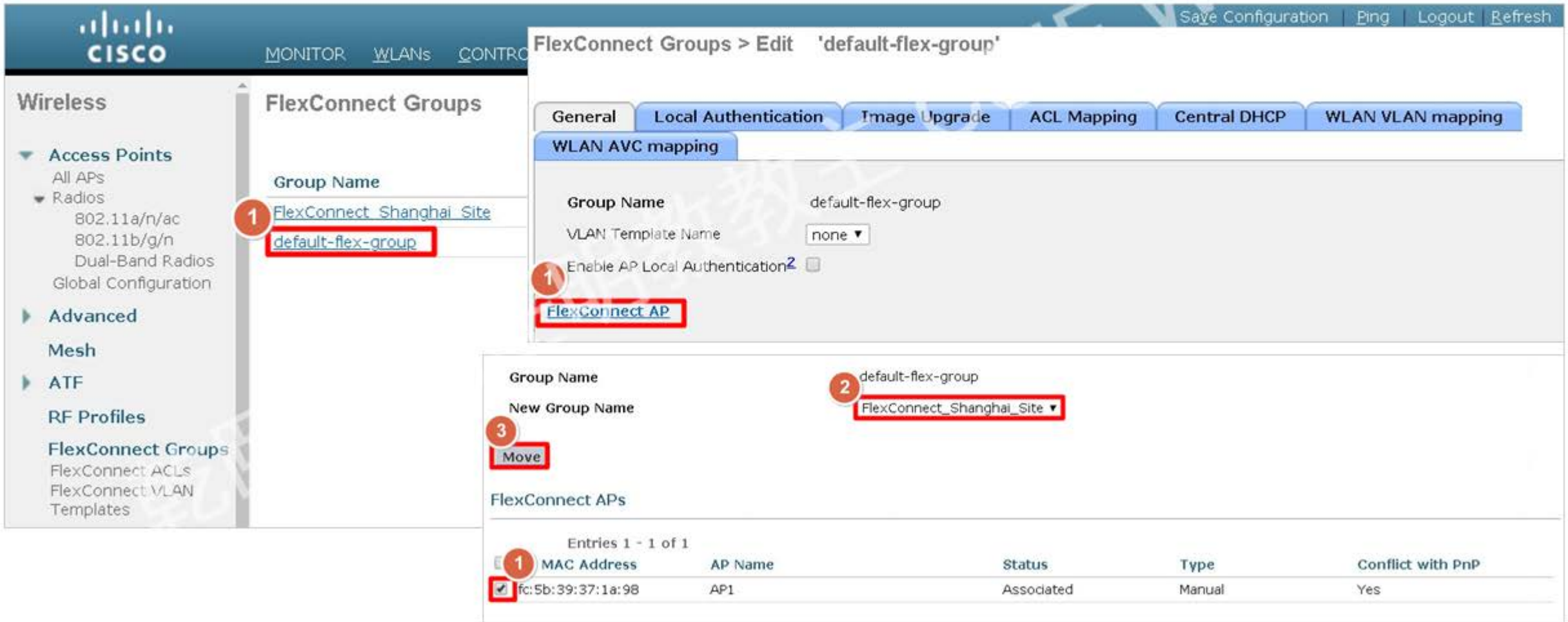


创建 FlexConnect Group



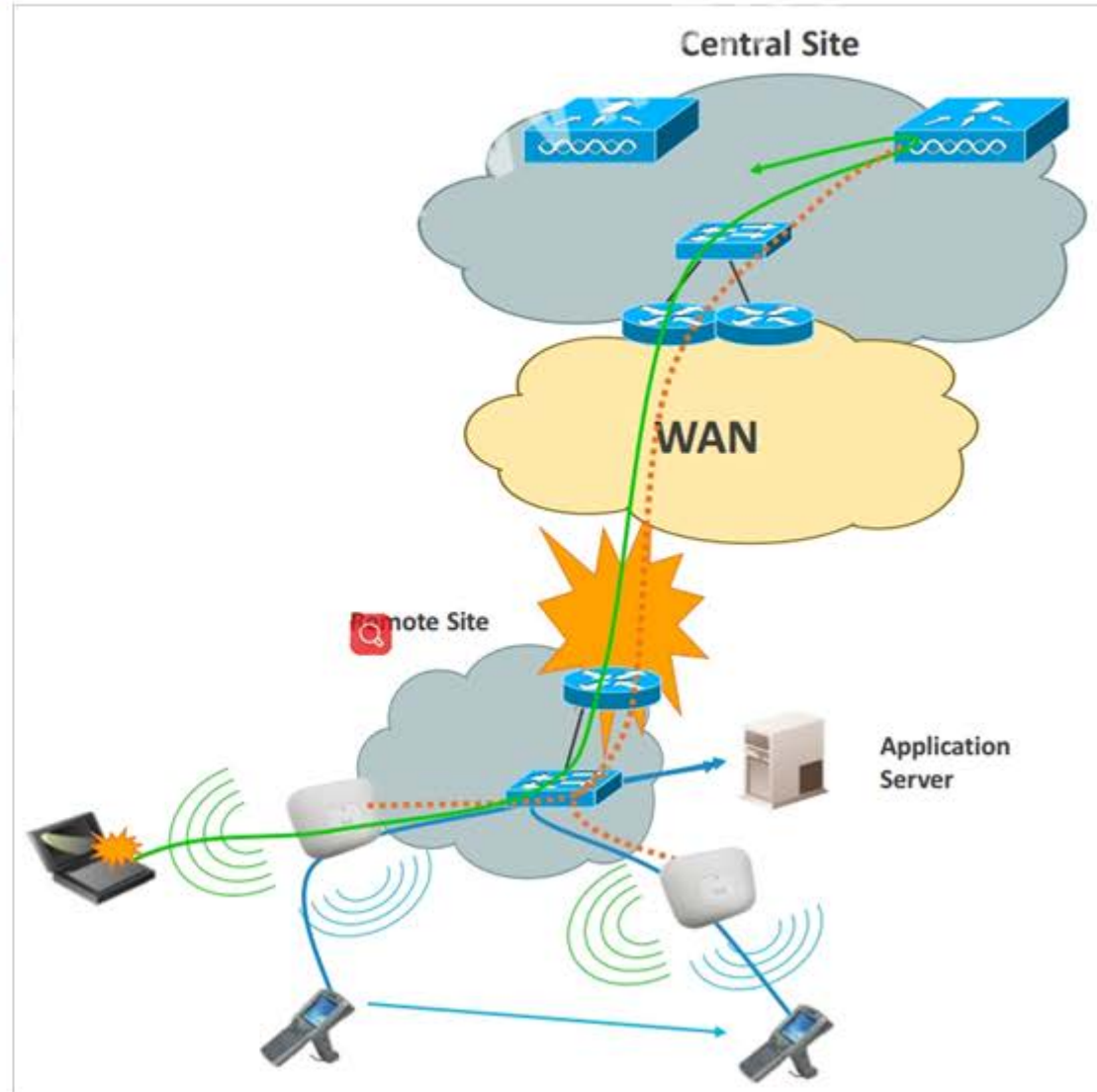
添加 AP 到 FlexConnect Group

- AP 默认属于 default-flex-group，将 AP 移动到新建的 FlexConnect Group。



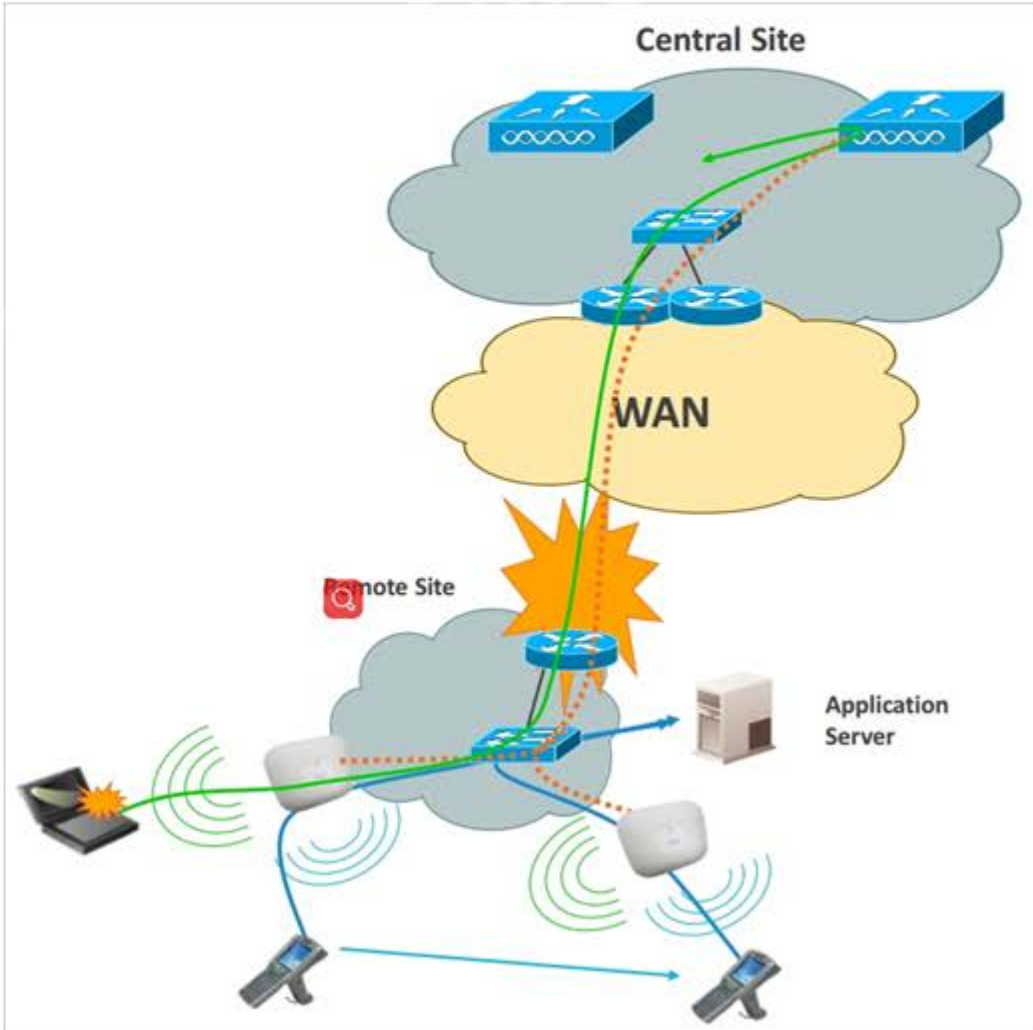
FlexConnect 备份情景 — WAN Failure

- FlexConnect will backup on local switched mode
  - No impact for locally switched SSIDs（本地交换的 SSID 没有影响）
  - Disconnection of centrally switched SSIDs clients（中心交换机的 SSID 会断开连接）
- Static authentication keys are locally stored in FlexConnect AP
- Lost features
  - RRM, WIDS, location, other AP modes
  - Web authentication, NAC



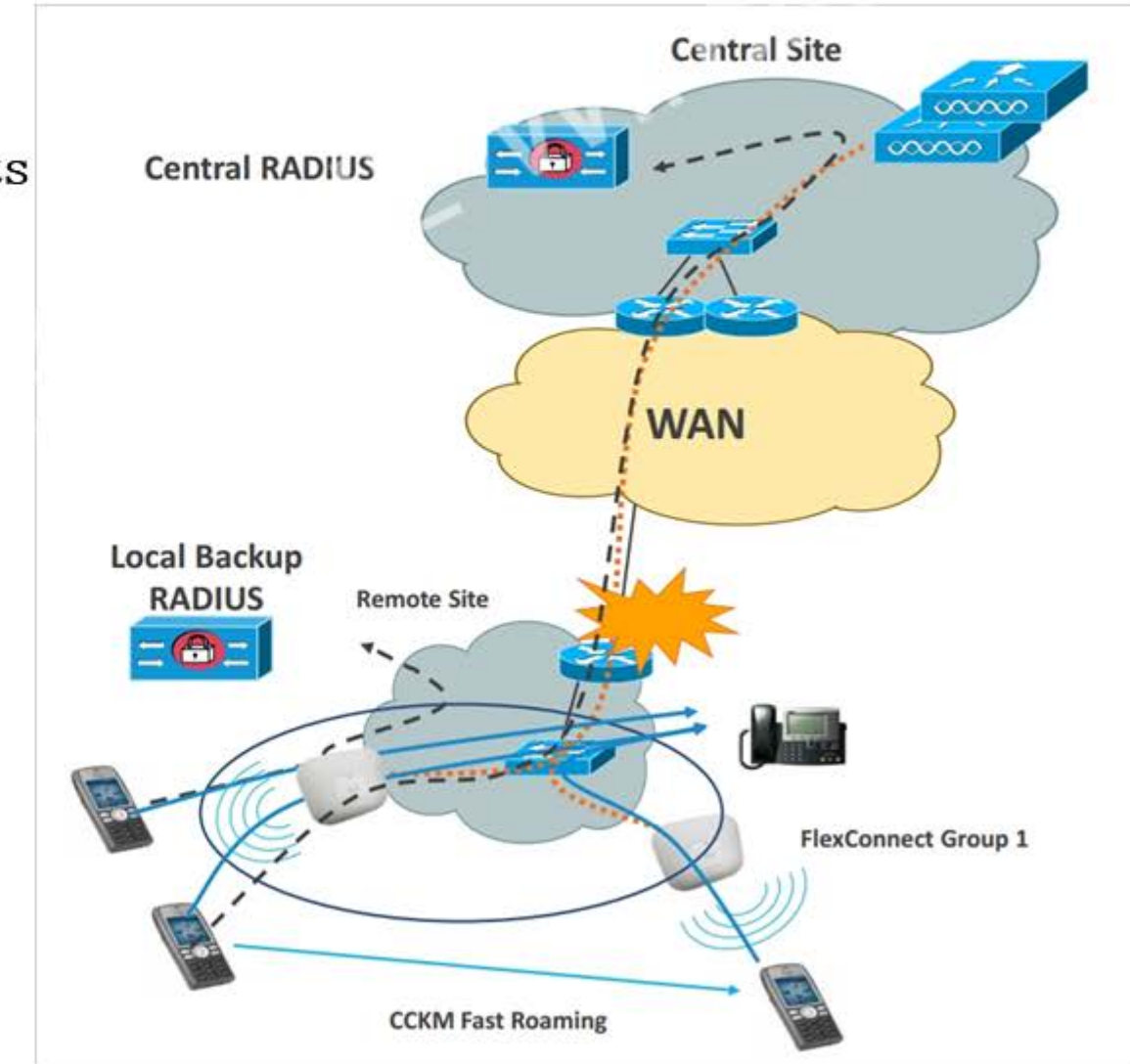
FlexConnect 备份情景 — WLC Failure

- FlexConnect will first backup on local switched mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- CCKM roaming allowed in FlexConnect group
- FlexConnect AP will then search for backup WLC; when backup WLC is found, FlexConnect AP will resync with WLC and resume client sessions with central traffic.
- Client sessions with Local Traffic are not impacted during resync with Backup WLC

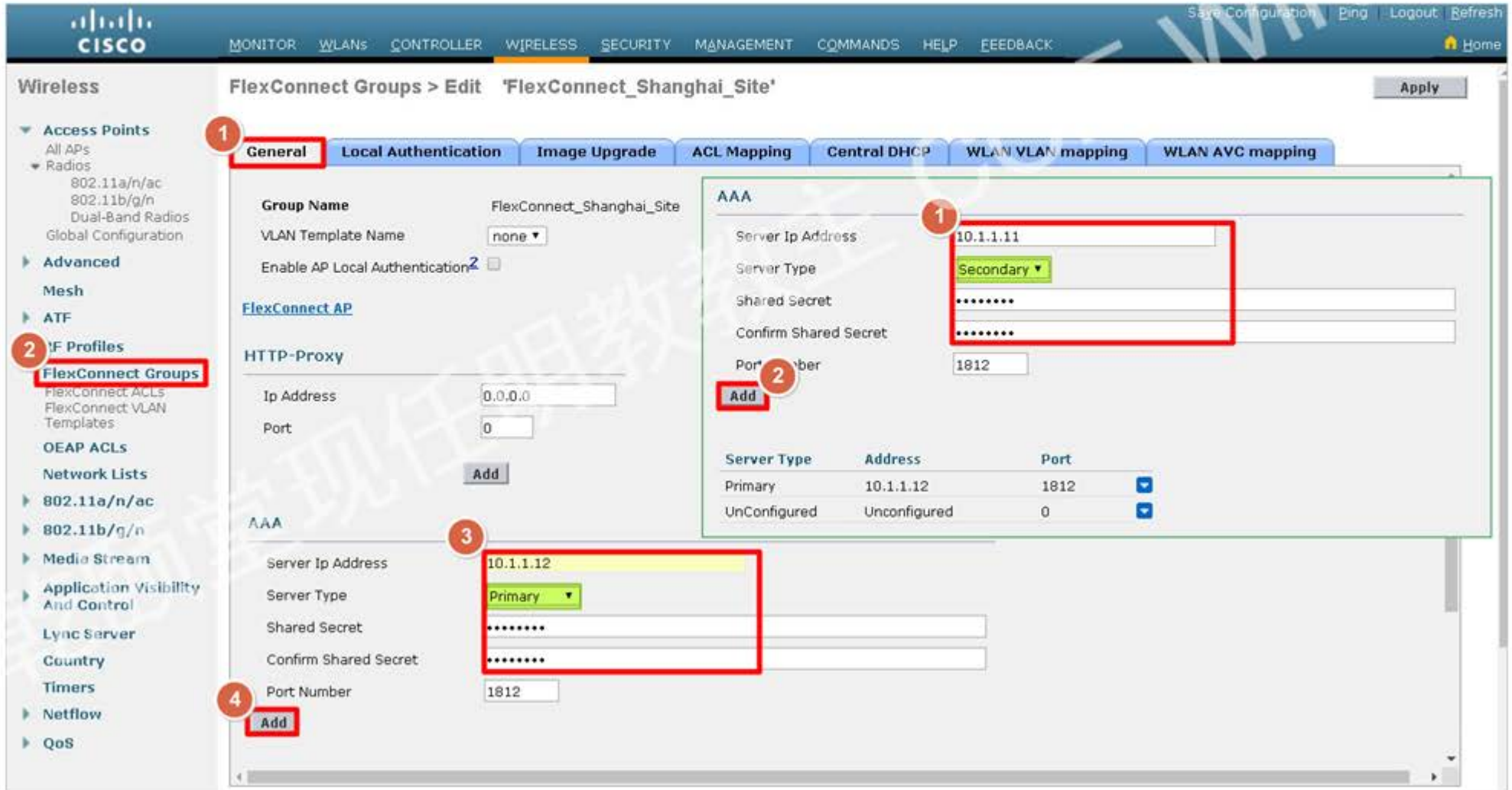


FlexConnect 备份情景 — Local Backup Radius

- Normal authentication is done centrally
- On WAN failure, AP authenticates new clients with locally defined RADIUS server
- Existing connected clients stay connected
- Clients can roam with
  - CCKM fast roaming, or
  - Reauthentication

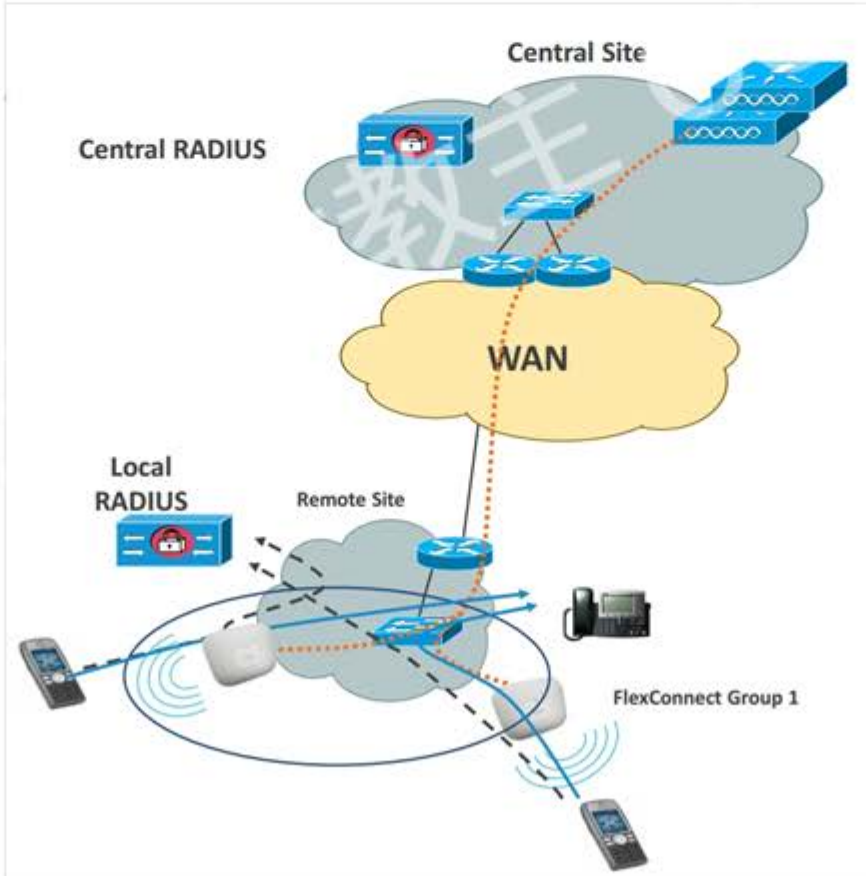


FlexConnect Group 配置主备 Radius



AP Local Authentication

- By default FlexConnect AP authenticates clients through central controller
- Local Authentication allow use of local RADIUS server directly from the FlexConnect AP

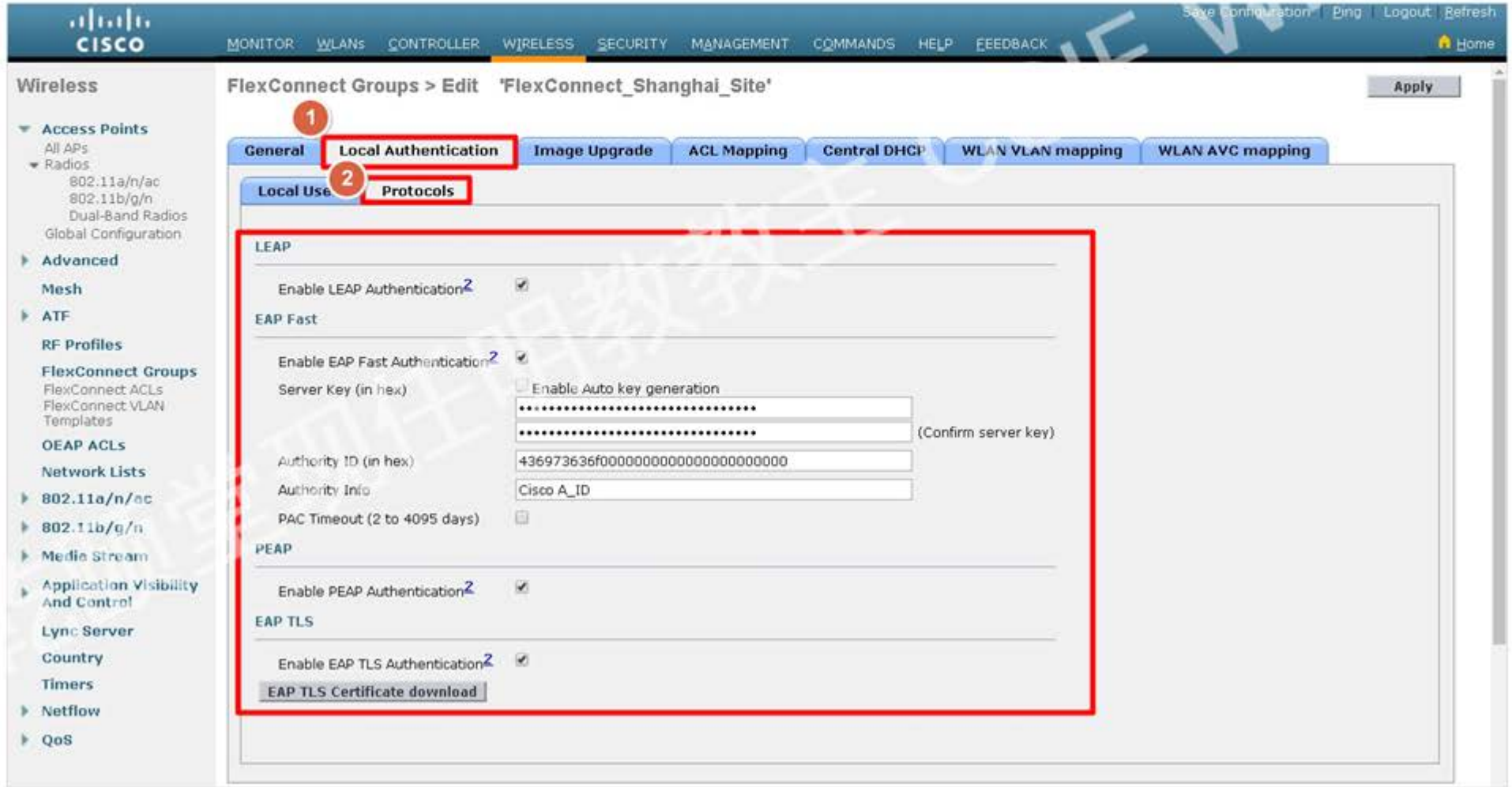


FlexConnect Group 配置 AP 本地认证 - 1

- LEAP/EAP-fast/PEAP/EAP-TLS authentication can be configured only when AP local authentication is configured（要配置 AP 本地认证，需要先激活这个选项）

FlexConnect Group 配置 AP 本地认证 - 2

- 8.3 版本支持的本地认证协议。

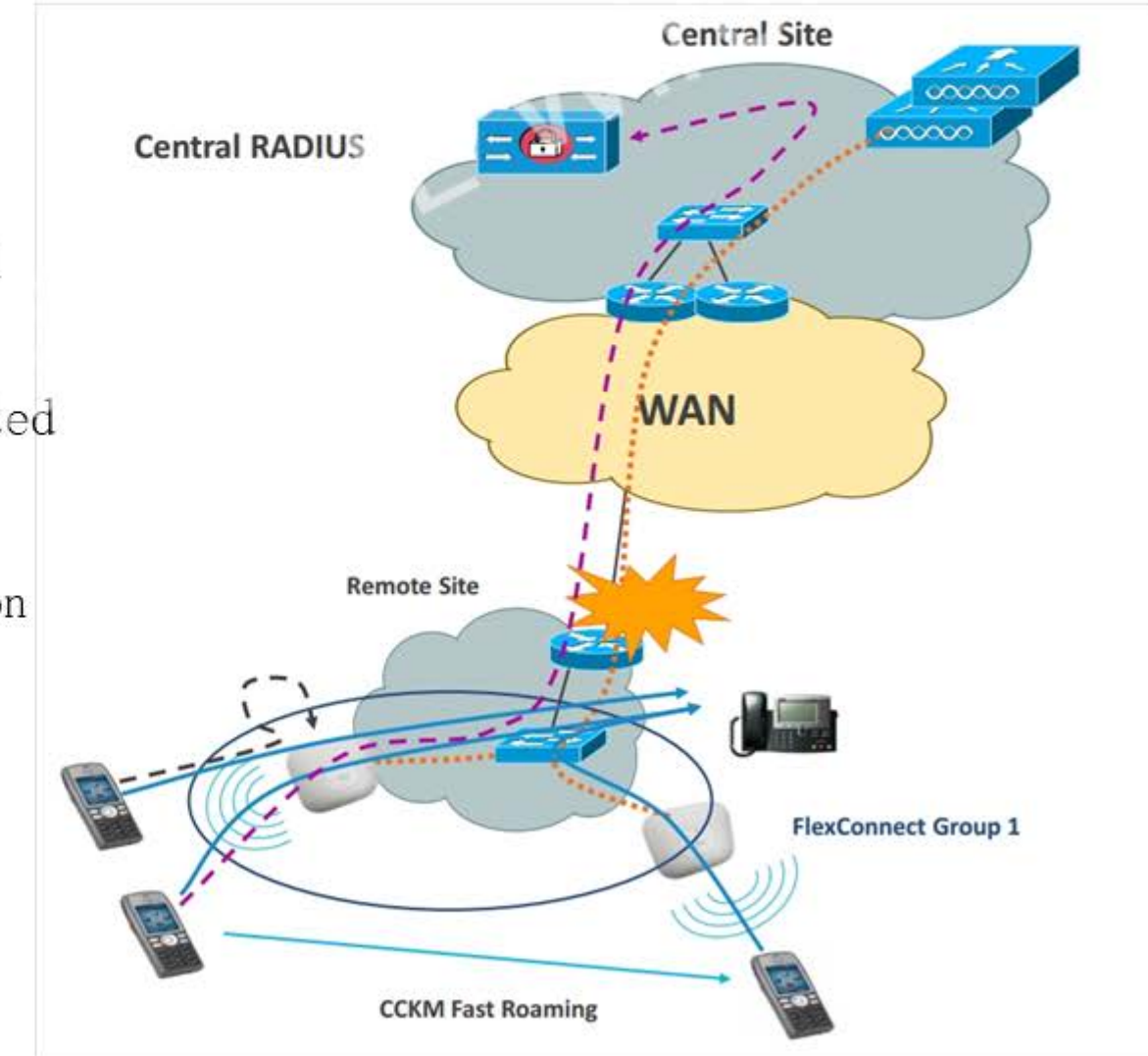


Local Backup Authentication

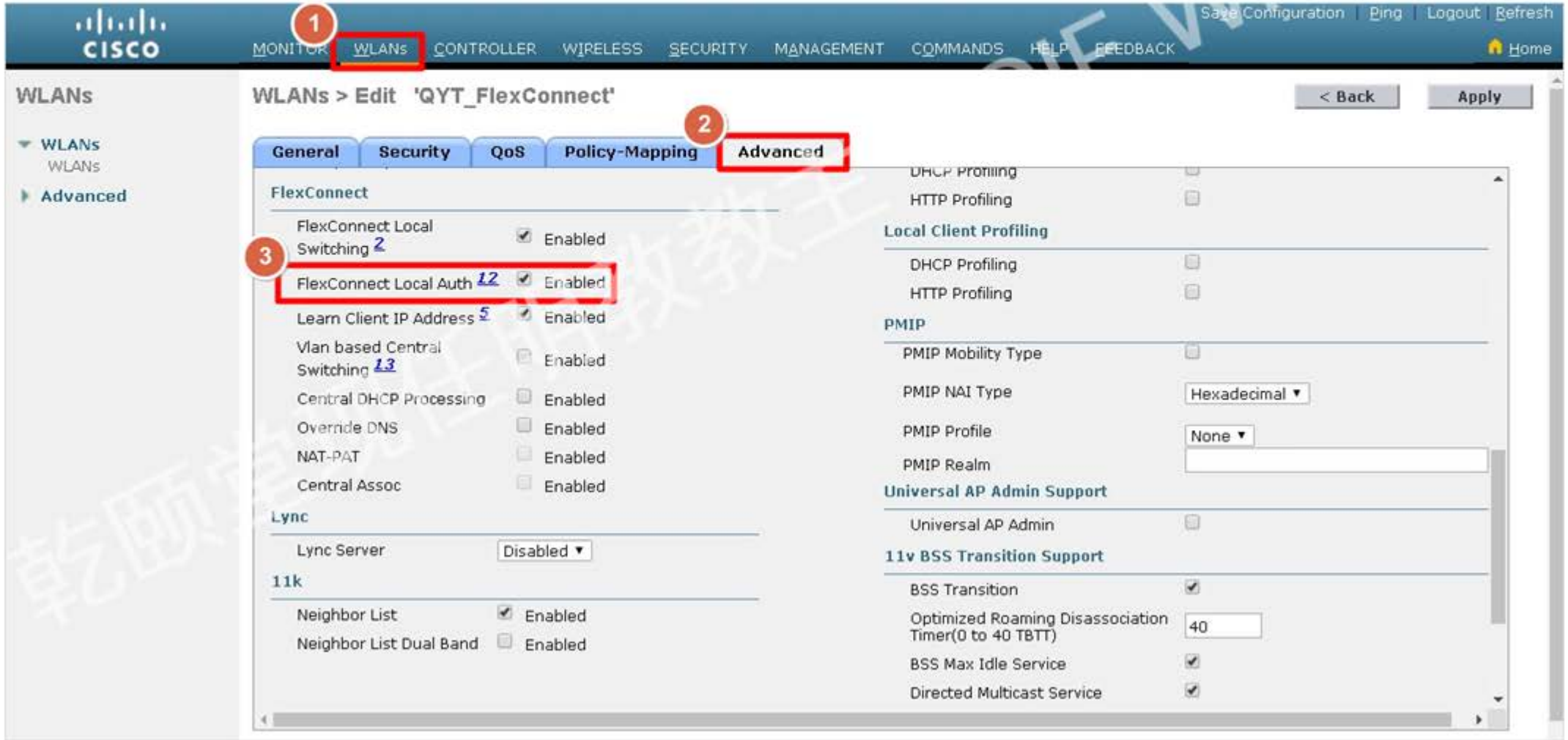
- Normal authentication is done centrally
- On WAN failure, AP authenticates new clientswith its local database
- Each FlexConnect AP has a copy of the local user DB
- Existing authenticated clients stay connected
- Clients can roam with:
  - CCKM fast roaming, or Local re-authentication

Supported Security Types	Release Version
LEAP	6.0
EAP-FAST	6.0
PEAP	7.5
EAP-TLS	7.5

New



Local Authentication

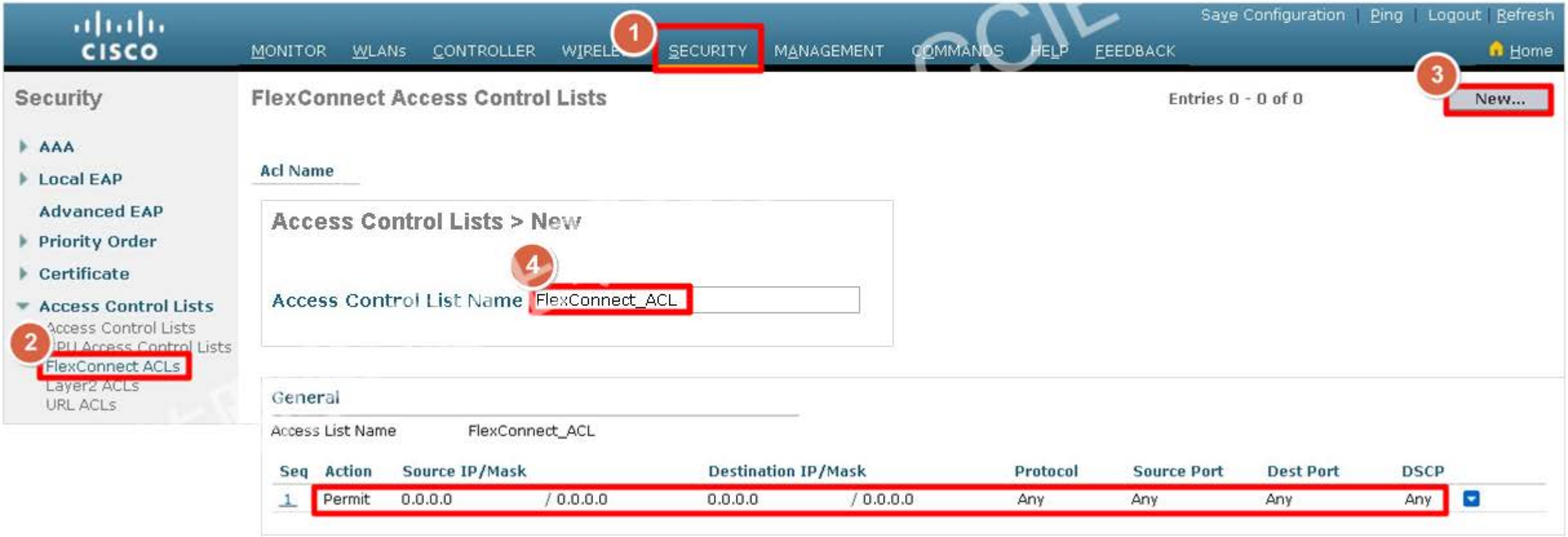


FlexConnect Access Lists

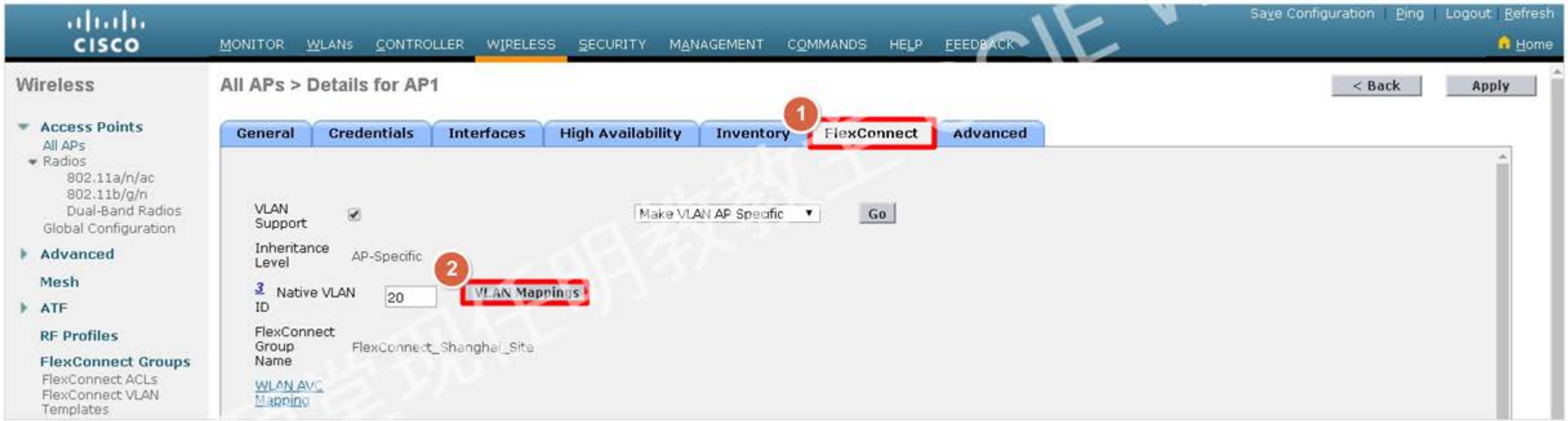
- FlexConnect ACL are ACL that are applied at the FlexConnect AP level
- 4 FlexConnect ACL usages :
  - ACL mapped to local VLAN per AP or FlexConnect Group
  - ACL used for NAT/PAT Split tunneling
  - ACL used for External WebAuthentication
  - ACL used for Web Policies (ISE policies)
- 512 FlexConnect ACL per WLC
- 16 ingress ACL & 16 egress ACL per AP
- 64 ACL rules per ACL
- No IPv6 AC

创建 FlexConnect ACL

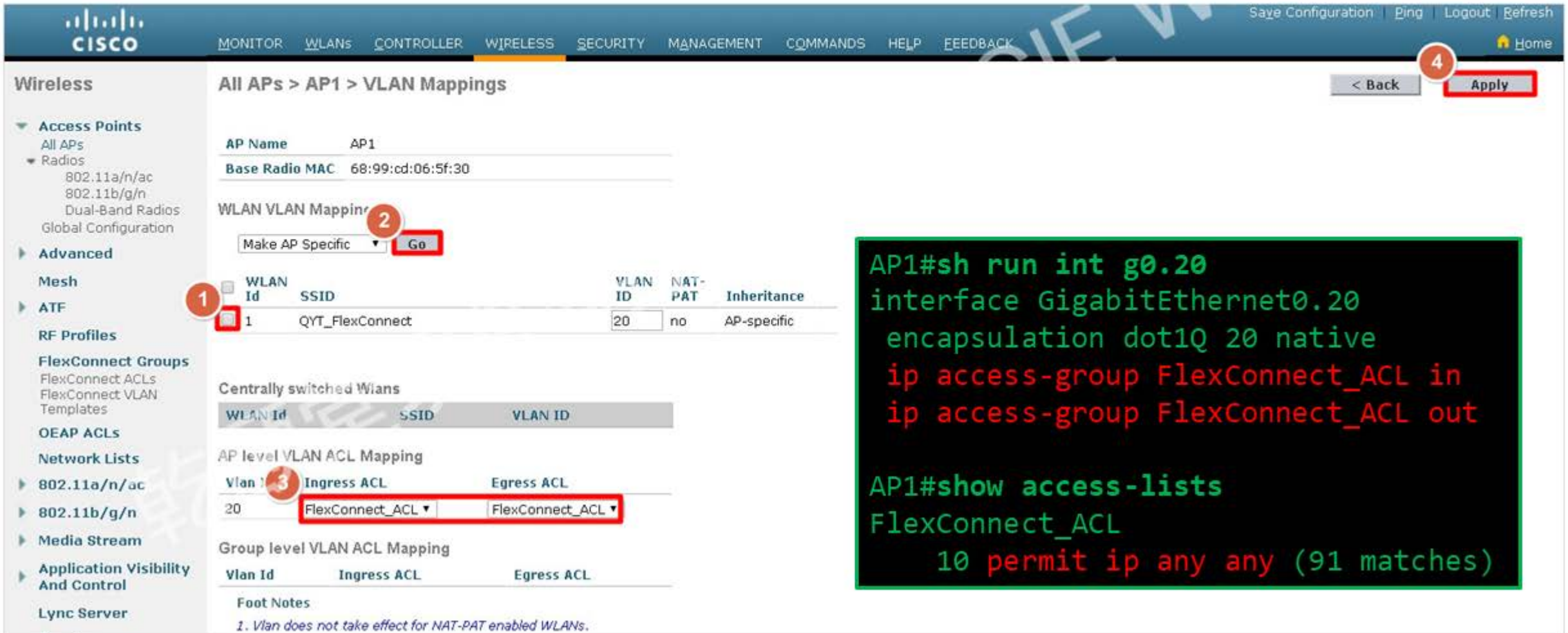
- FlexConnect ACL are not the same as ACL for Local Mode AP
- FlexConnect ACL rule creation is similar to rule creation for Local Mode AP



FlexConnect ACL per AP – 1



FlexConnect ACL per AP – 2



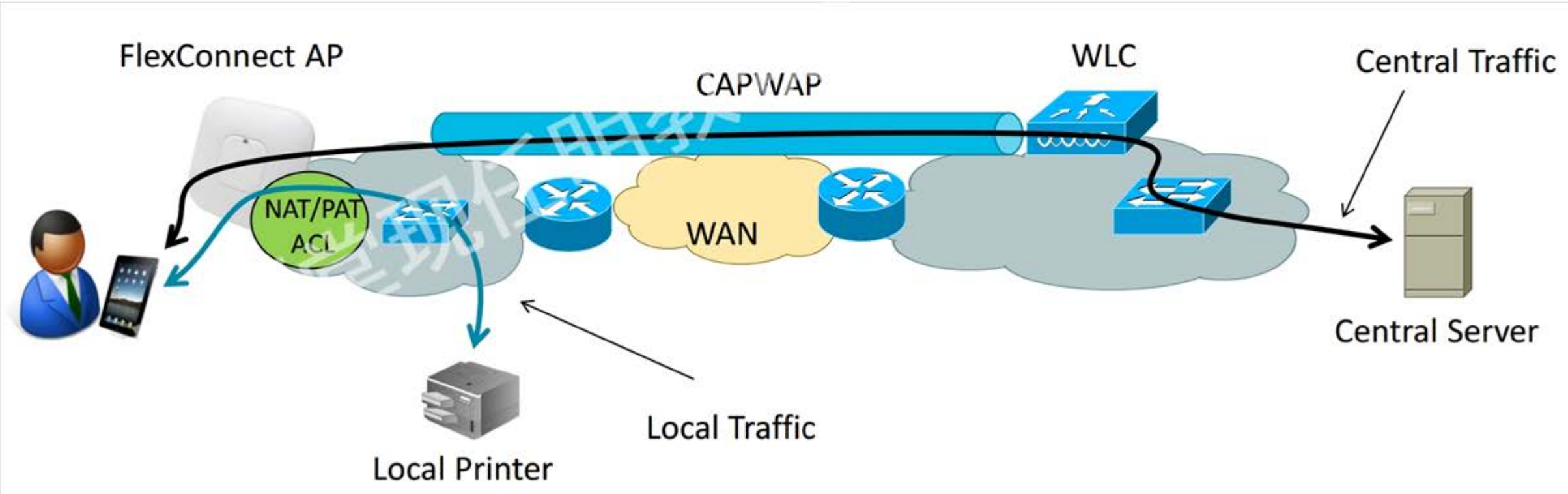

```
AP1#sh run int g0.20
interface GigabitEthernet0.20
 encapsulation dot1Q 20 native
 ip access-group FlexConnect_ACL in
 ip access-group FlexConnect_ACL out

AP1#show access-lists
FlexConnect_ACL
    10 permit ip any any (91 matches)
```

FlexConnect ACL per FlexConnect Group

- AAA VLAN-ACL mapping 还有一个作用：做 per-user vlan 的时候需要 AP 本地有对应的 valn（子接口），此时又不想多创建一个 SSID，可以创建 AAA VLAN-ACL mapping，不关联 ACL。

FlexConnect ACL - Split Tunneling

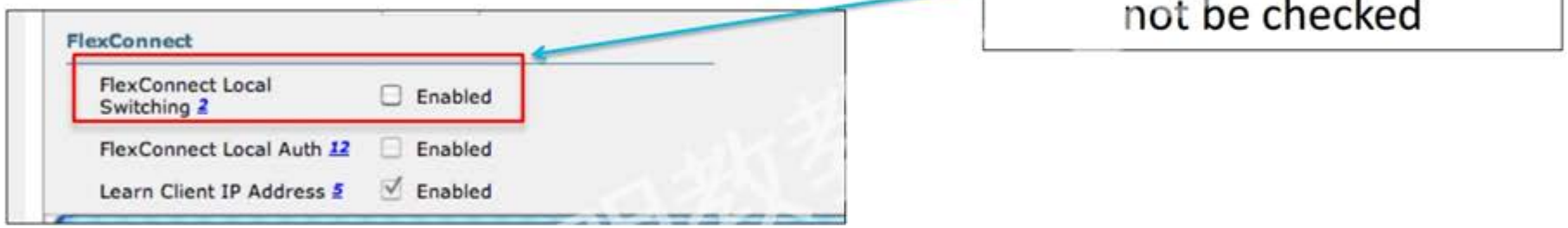
- Split tunneling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunneling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunneling is using the AP IP@ for the NAT/PAT feature



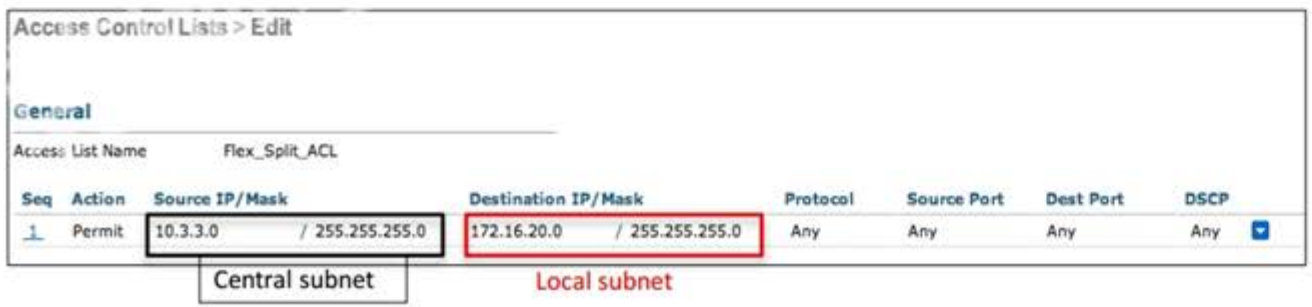
Split Tunneling 配置 - 1

- 这个WLAN就不能本地转发了

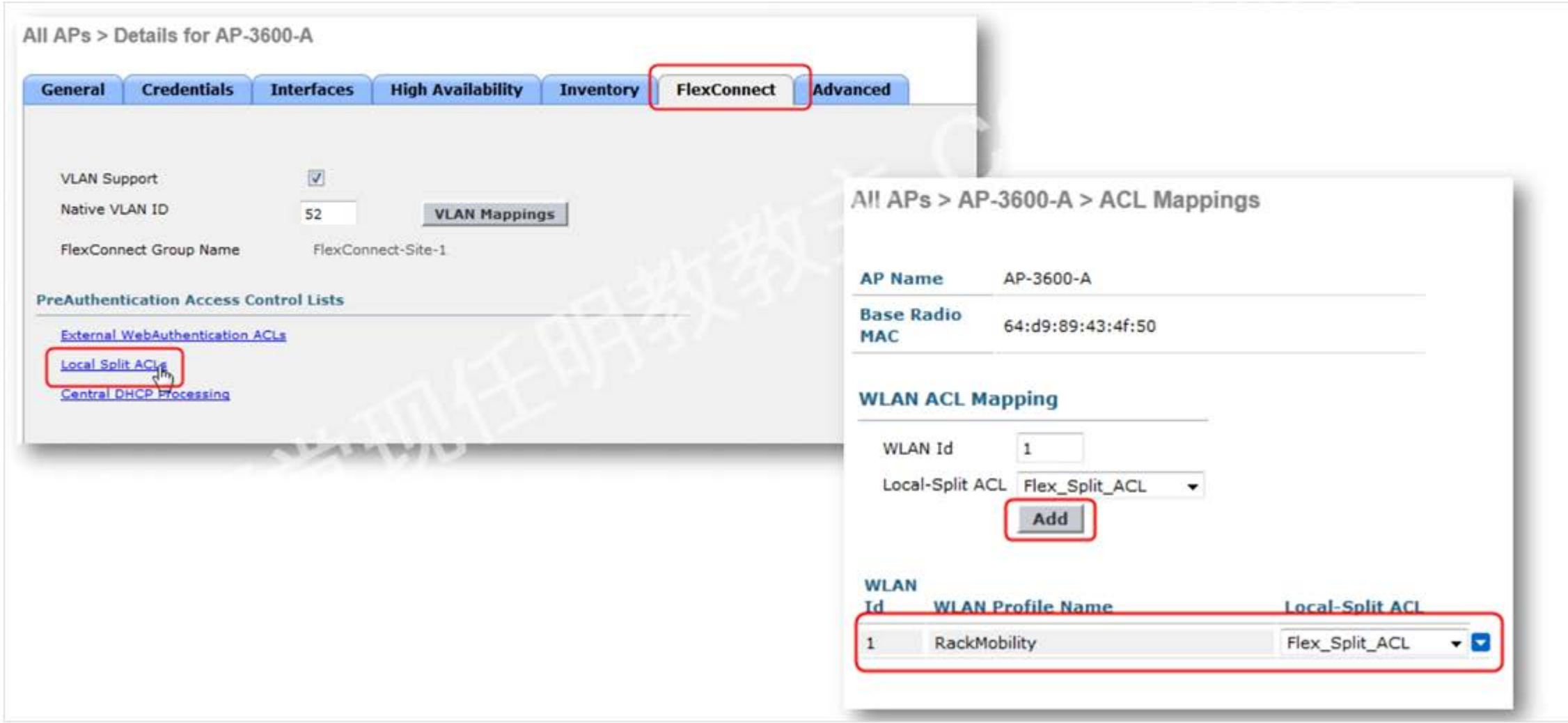
- Create a centrally switched WLAN



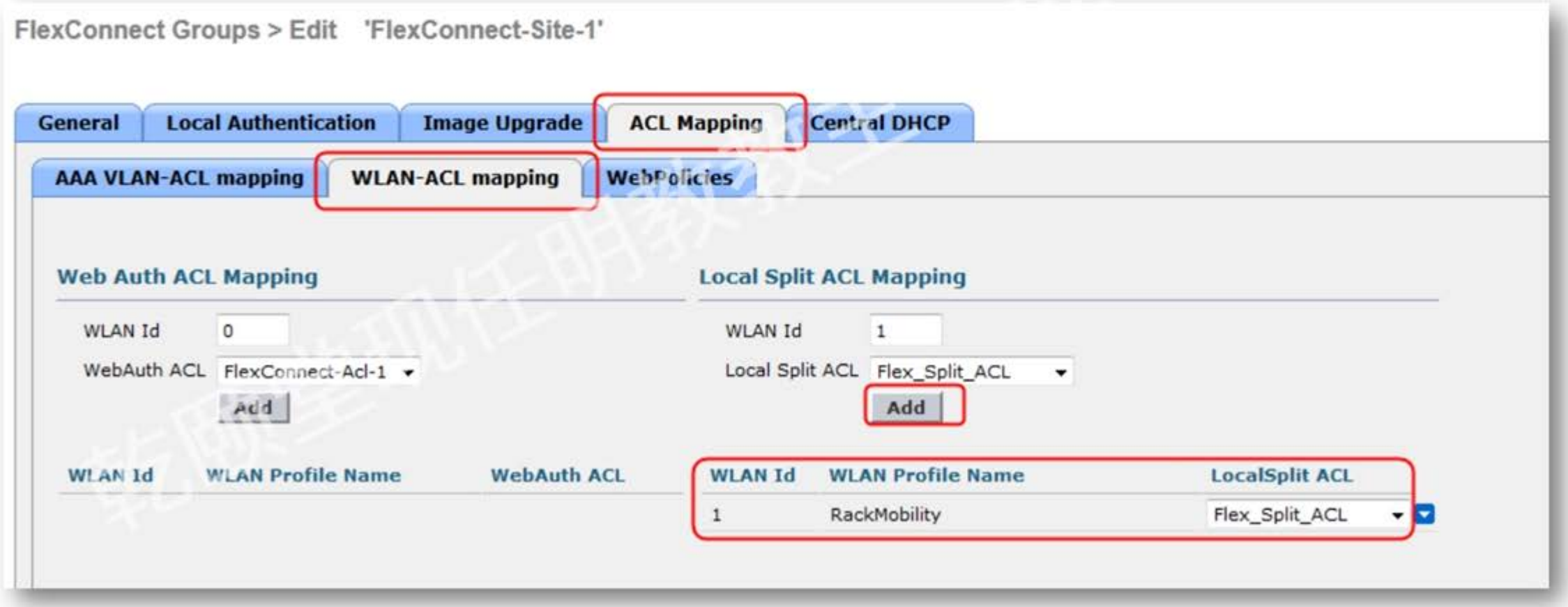
- Define Flex ACL to match traffic to be locally switched



Split Tunneling 配置 - 2



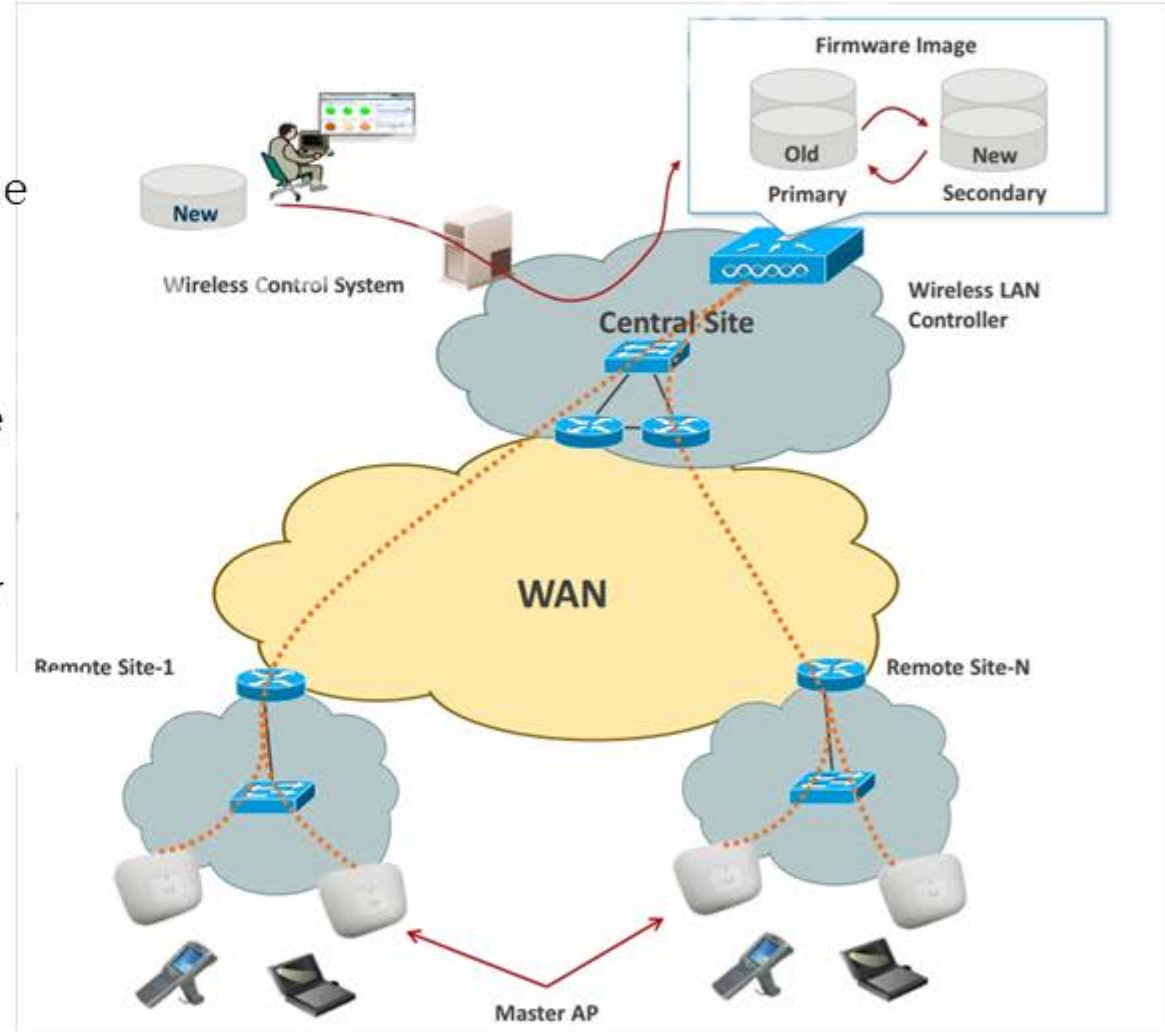
Split Tunneling FlexConnect Group 配置



FlexConnect Smart AP Image Upgrade -1

Smart AP Image Upgrade use a «master » AP in each FlexConnect Group to download the code. Other FlexConnect AP download the code from the master locally

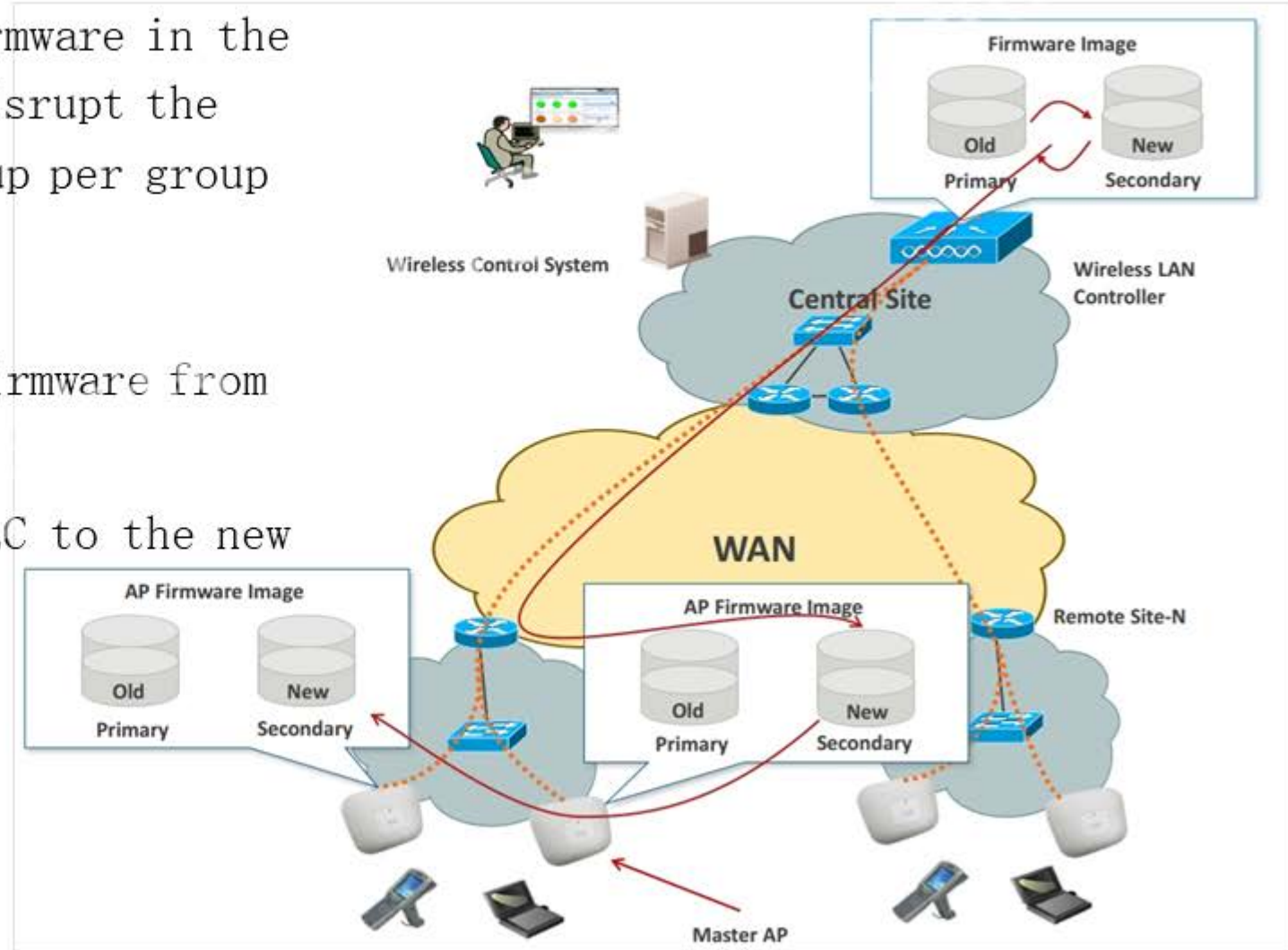
1. Download WLC upgraded firmware (will become primary)
2. Force the «boot image » to be the secondary (and not the newly upgraded one) to avoid parallel download of all AP in case of unexpected WLC reboot
3. WLC elect a master AP in each FlexConnect Group (can be also set manually)



FlexConnect Smart AP Image Upgrade -2

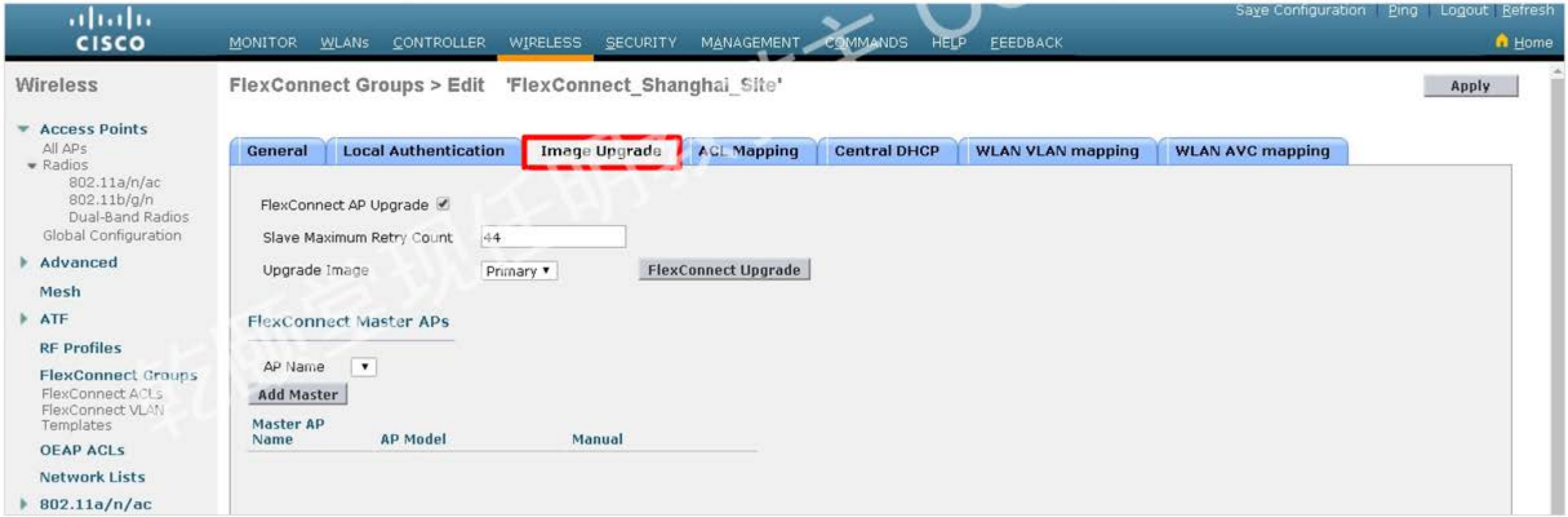
Master AP «Pre-download » the AP firmware in the secondary «boot image » (will not disrupt the actual service)—Can be started group per group to limit WAN exhaust

5. Slave AP «Pre-download » the APfirmware from the Master AP
6. Change the «bootimage » of the WLC to the new image
7. Reboot the controller



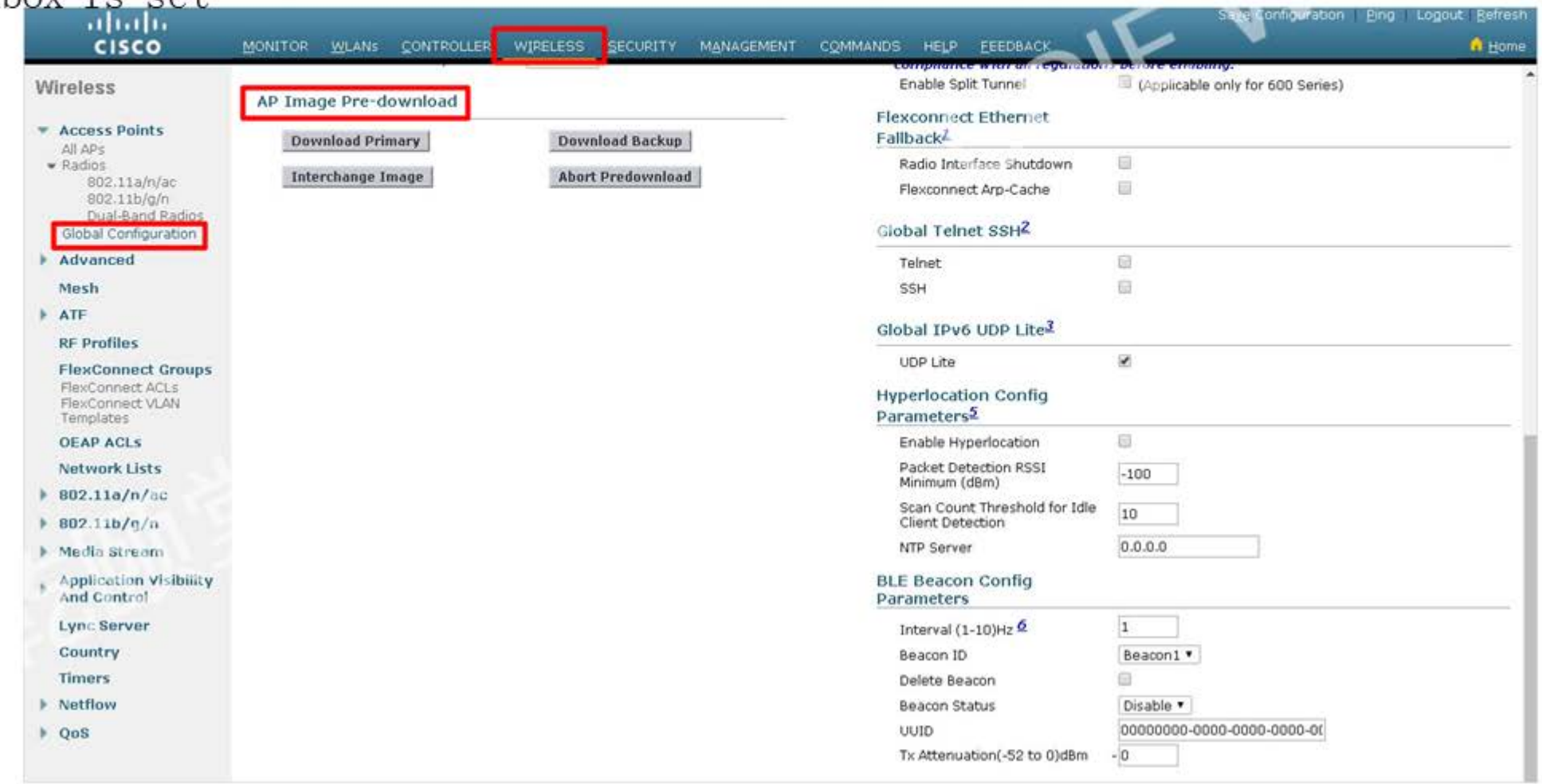
配置 - 1

- “FlexConnect AP Upgrade” checkbox has to be enabled for each FlexConnect Group.
- By default, Master AP for each FlexConnect Group is selected using Lower-MAC algorithm.
- One Master select per AP type



配置 – 2

- Upgrade across all Branches or FlexConnect Groups whose “FlexConnect AP Upgrade” checkbox is set



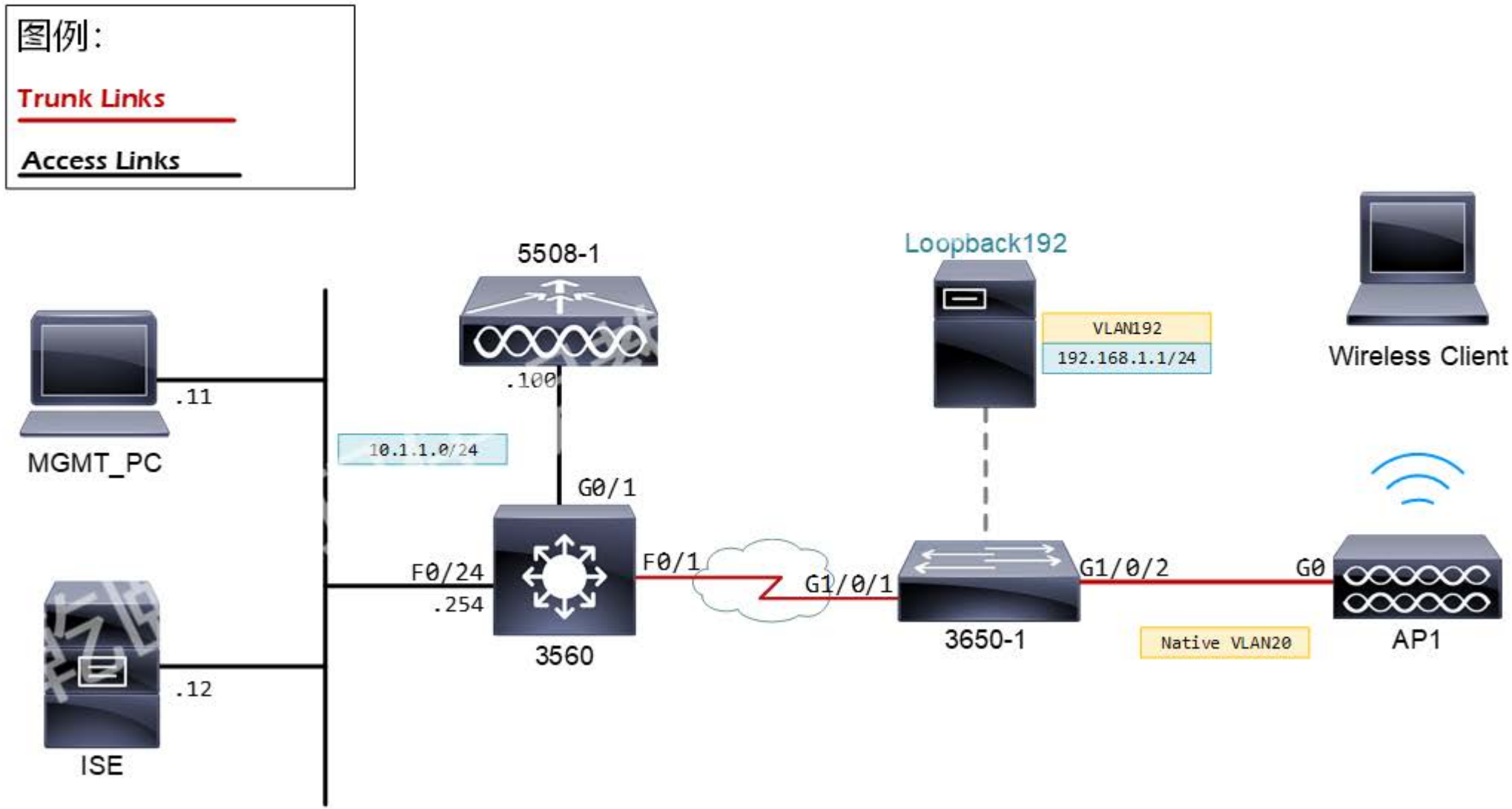
3

FlexConnect Group 实验

3.1

WLAN-VLAN 映射继承顺序

拓扑图


图例:
Trunk Links
Access Links
5508-1
.100
Loopback192
VLAN192
192.168.1.1/24
Wireless Client
.11
MGMT_PC
10.1.1.0/24
G0/1
F0/24
.254
F0/1
G1/0/1
3560
3650-1
G1/0/2
G0
Native VLAN20
AP1
.12
ISE

WLC5508-1 初始化 - 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]: 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

Enable HA [yes][NO]: no

Virtual Gateway IP Address: 192.0.2.1

Mobility/RF Group Name: qytang
Network Name (SSID): qytang
```

WLC5508-1 初始化 - 2

```
Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: yes

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
Enable Auto-RF [YES][no]: YES

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

Configuration saved!
Resetting system with new configuration...
```

3560 预配

```
hostname SW3560
!
ip routing
!
vlan 10
 name management
vlan 20
 name for-ap1
!
interface range FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
!
interface range GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
```

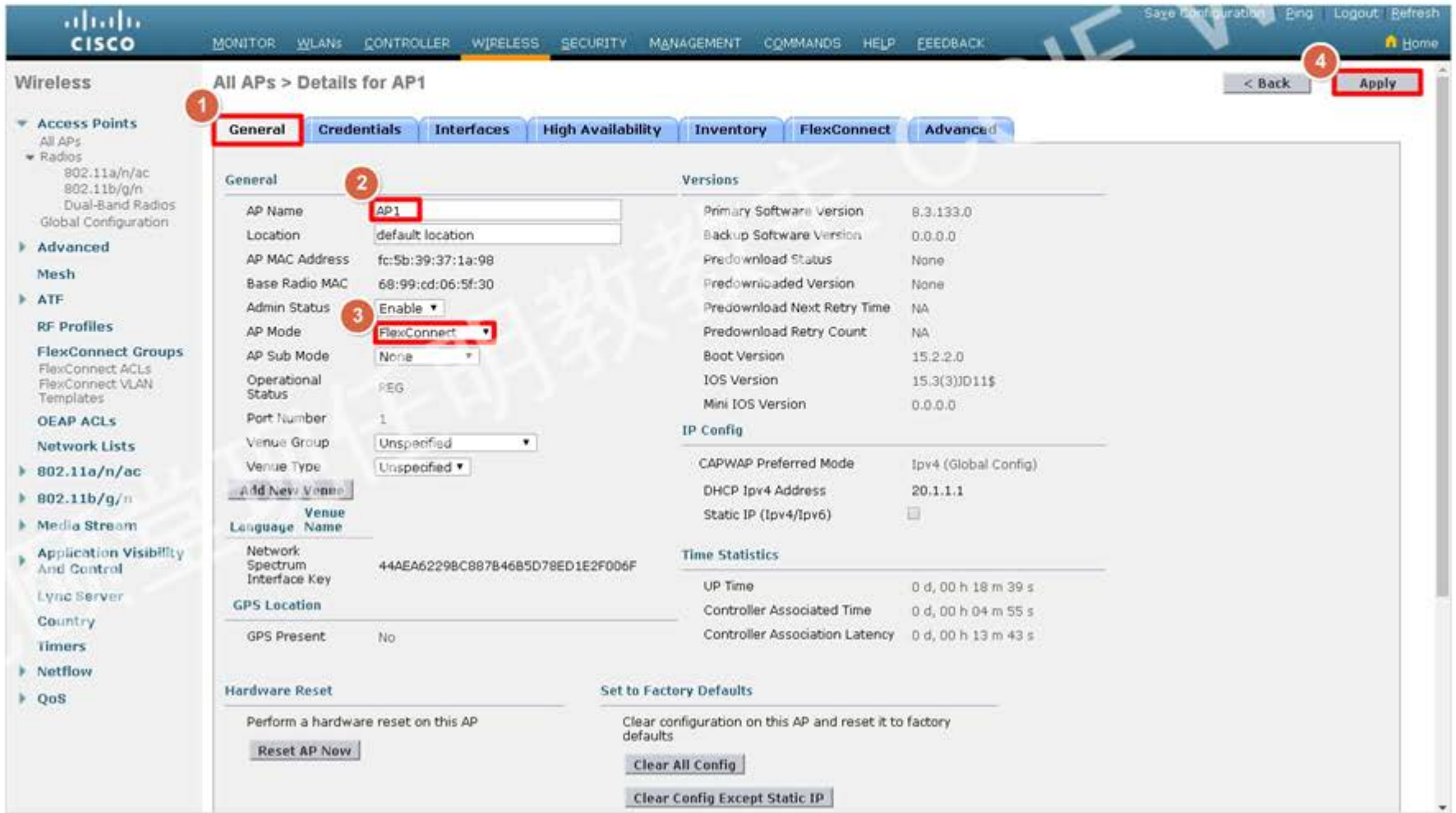
```
interface FastEthernet0/24
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
ip dhcp pool vlan10
   network 10.1.1.0 255.255.255.0
   default-router 10.1.1.254
!
interface Vlan10
 ip address 10.1.1.254 255.255.255.0
!
interface Vlan20
 ip address 20.1.1.254 255.255.255.0
!
ip route 30.1.1.0 255.255.255.0 20.1.1.253
```

3650-1 预配

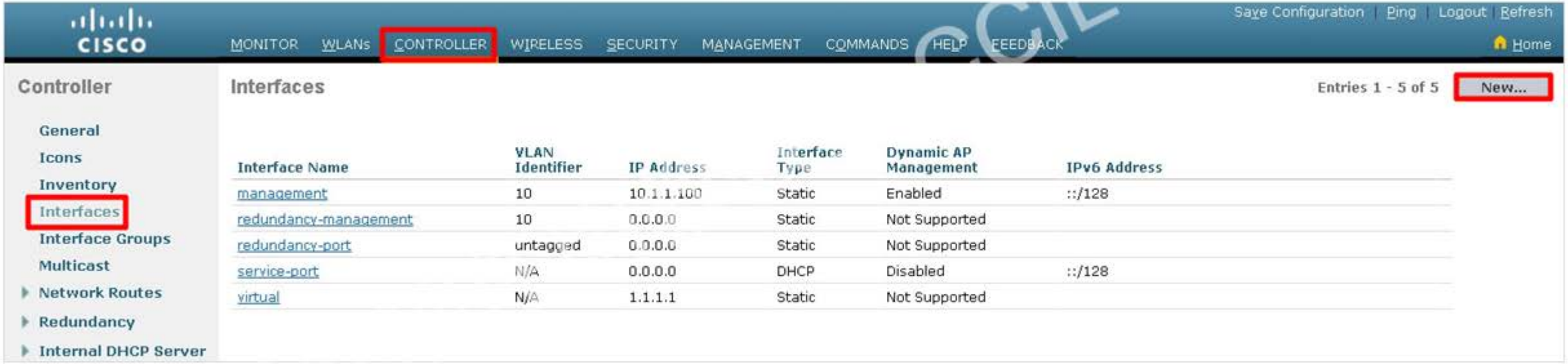
```
hostname SW3650-1
!
ip routing
!
vlan 10
 name management
!

vlan 20
 name for-ap1
!
vlan 30
 name for-client
!
vlan 192
 name for-server
!
interface GigabitEthernet1/0/1
switchport mode trunk
!
```

```
interface GigabitEthernet1/0/2
 switchport trunk native vlan 20
 switchport mode trunk

ip dhcp pool for-ap2
   network 20.1.1.0 255.255.255.0
   default-router 20.1.1.253
   option 43 hex f104.0a01.0164
!
ip dhcp pool for-client
   network 30.1.1.0 255.255.255.0
   default-router 30.1.1.253
!
interface Vlan20
ip address 20.1.1.253 255.255.255.0
!
interface Vlan30
ip address 30.1.1.253 255.255.255.0
!
interface Vlan192
 ip address 192.168.1.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 20.1.1.254
```

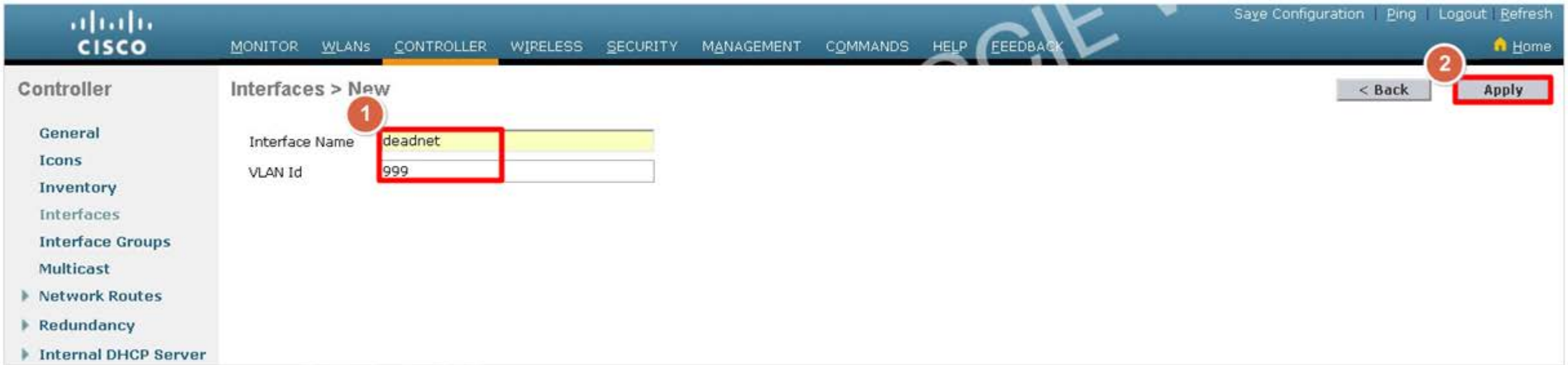
AP1 切换为 FlexConnect 模式



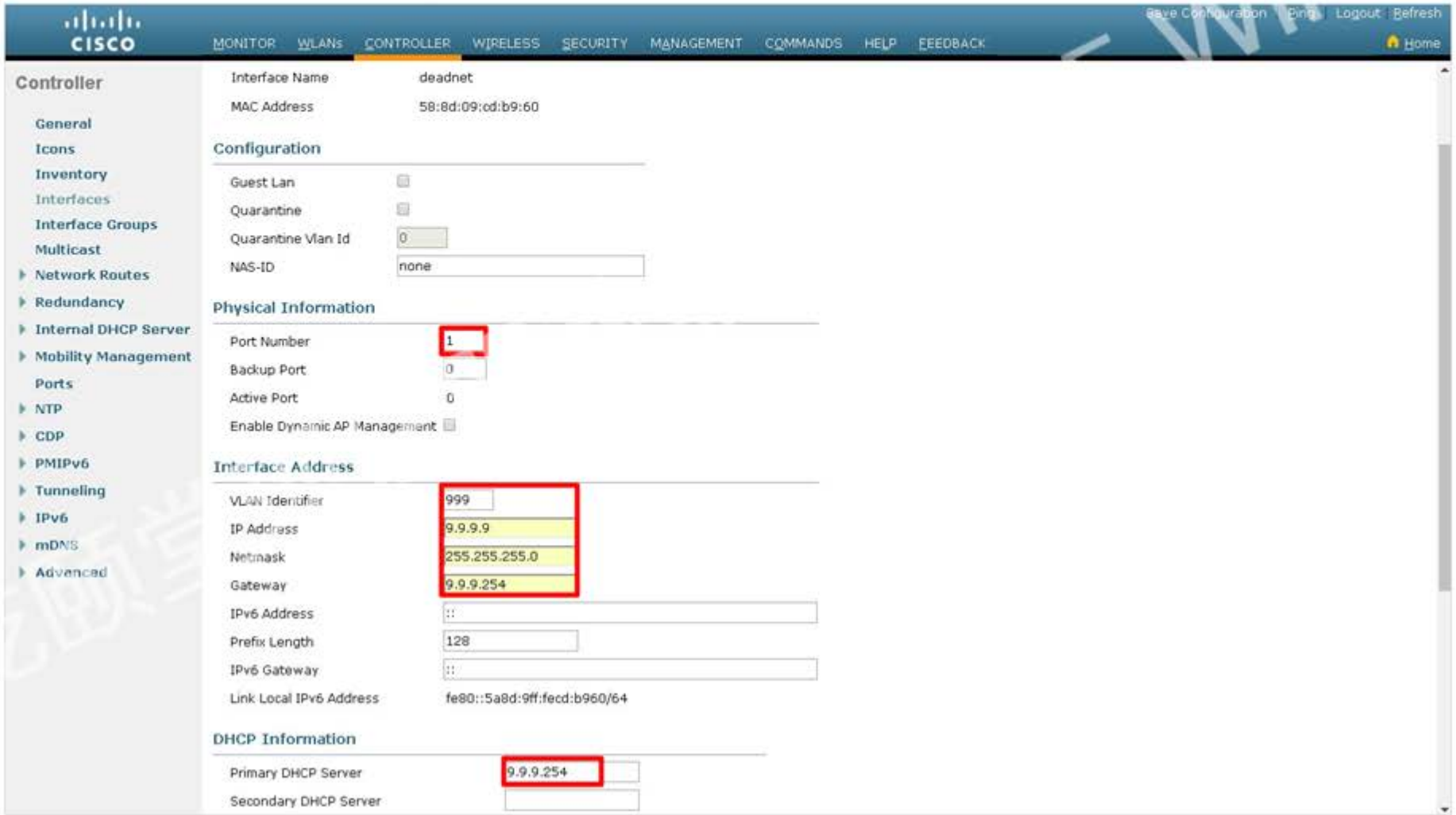
WLC 新建 Interface - 1



WLC 新建 Interface - 2

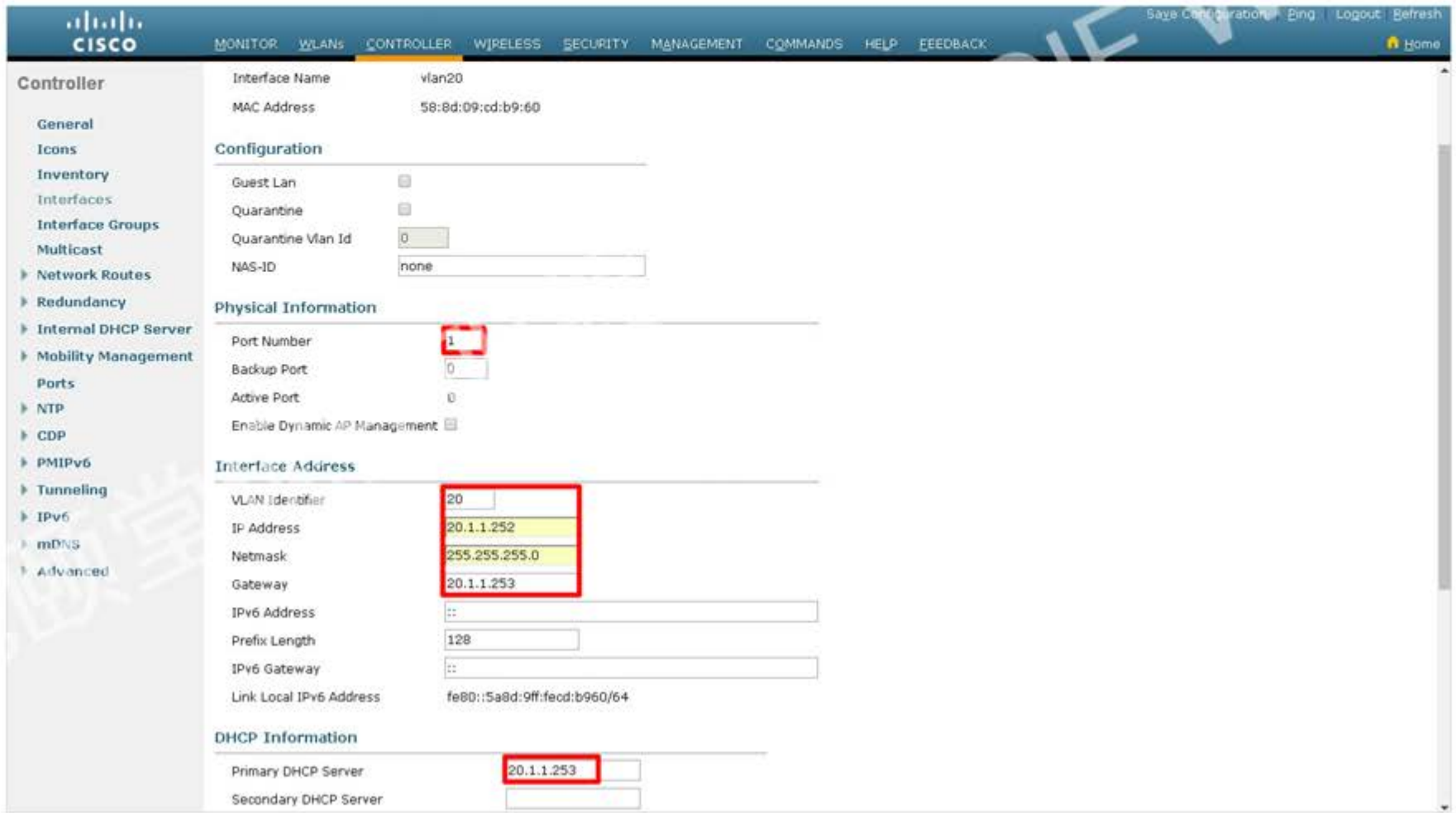


WLC 新建 Interface - 3

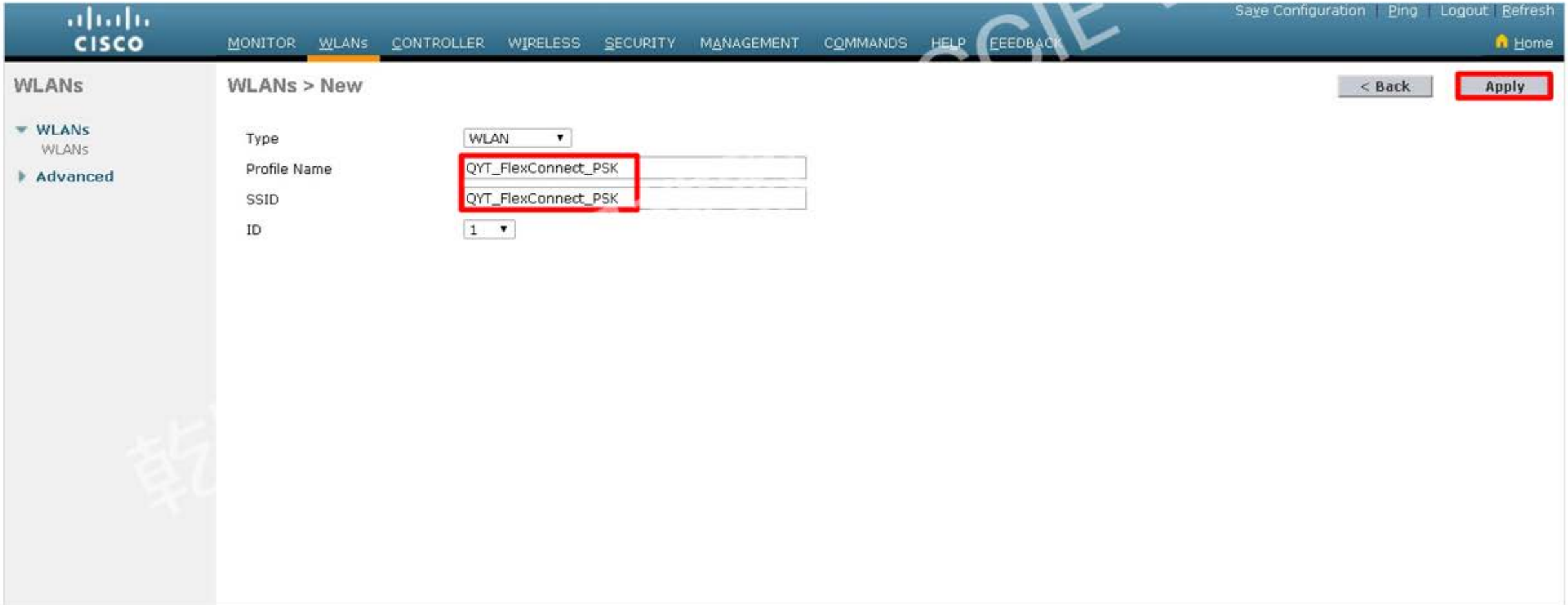


WLC 新建 Interface - 4

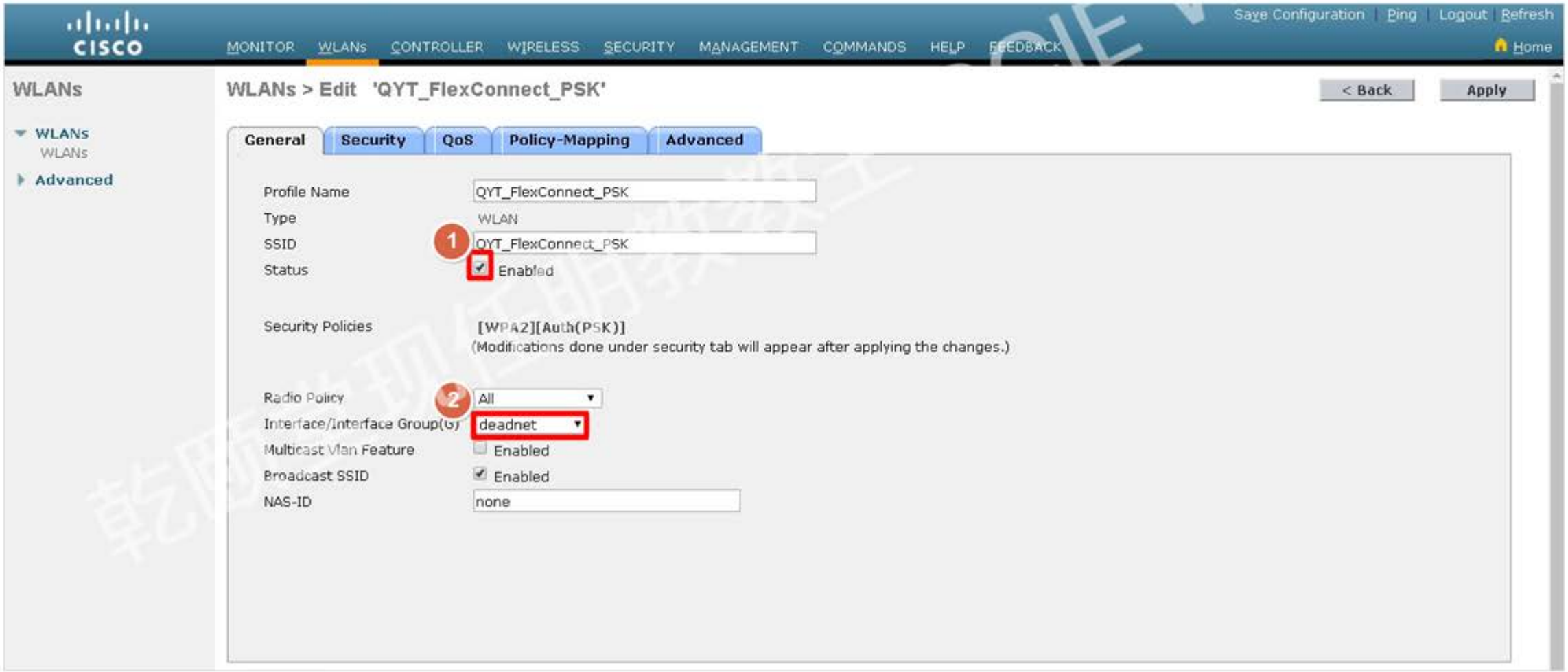
WLC 新建 Interface - 5



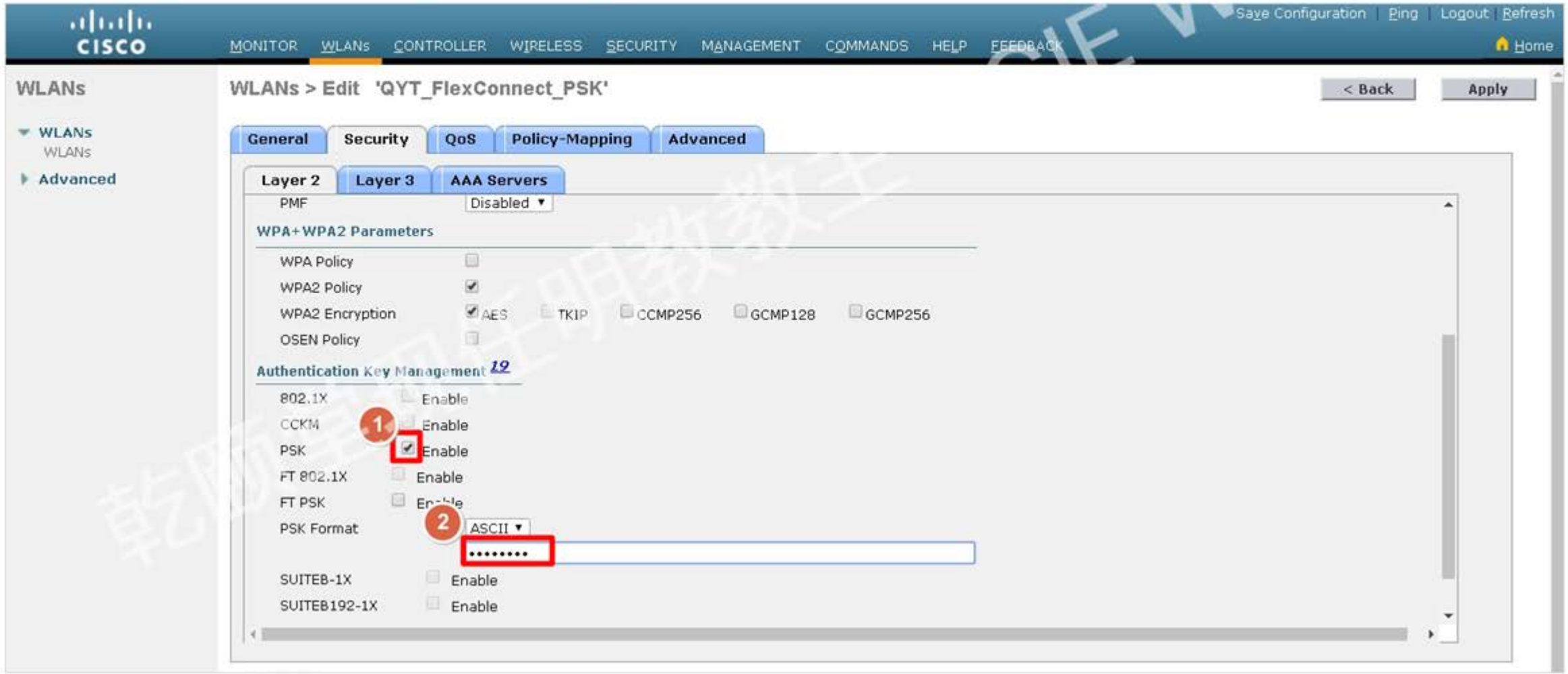
WLC 创建 WLAN - 1


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > New
< Back
Apply
WLANs
WLANs
Advanced
Type
WLAN
Profile Name
QYT_FlexConnect_PSK
SSID
QYT_FlexConnect_PSK
ID
1

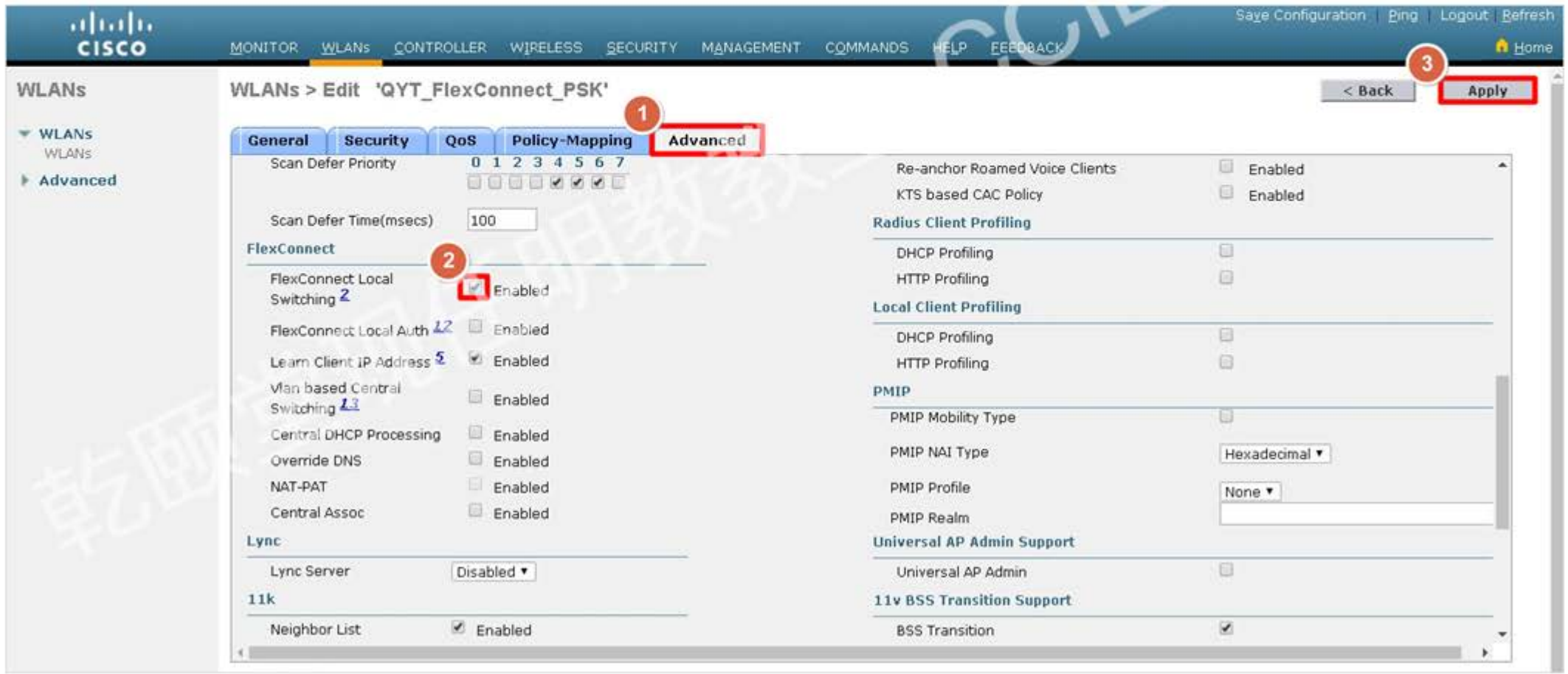
WLC 创建 WLAN - 2


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs
Advanced
WLANs > Edit 'QYT_FlexConnect_PSK'
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
QYT_FlexConnect_PSK
Type
WLAN
SSID
QYT_FlexConnect_PSK
1
Status
Enabled
Security Policies
[WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
2
All
Interface/Interface Group(G)
deadnet
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none

WLC 创建 WLAN - 3


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > Edit 'QYT_FlexConnect_PSK'
< Back
Apply
WLANs
WLANs
Advanced
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management 19
802.1X
Enable
CCKM
Enable
PSK
Enable
FT 802.1X
Enable
FT PSK
PSK Format
ASCII
SUITEB-1X
Enable
SUITEB192-1X
Enable
1
2

WLC 创建 WLAN - 4

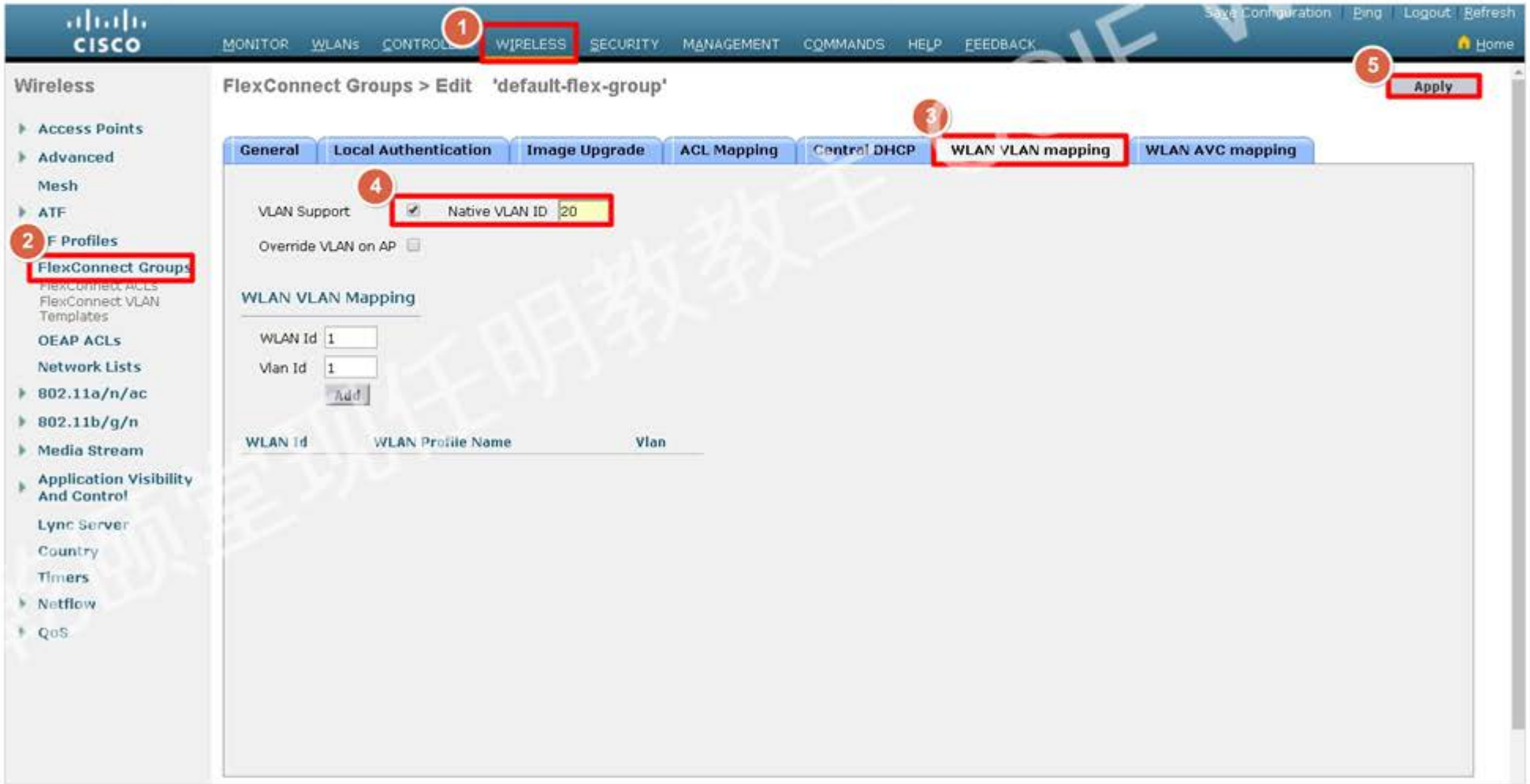

CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs
Advanced
WLANs > Edit 'QYT_FlexConnect_PSK'
< Back
Apply
1
2
3
General
Security
QoS
Policy-Mapping
Advanced
Scan Defer Priority
0 1 2 3 4 5 6 7
Scan Defer Time(msecs)
100
FlexConnect
FlexConnect Local Switching
Enabled
FlexConnect Local Auth
Enabled
Learn Client IP Address
Enabled
Vlan based Central Switching
Enabled
Central DHCP Processing
Enabled
Override DNS
Enabled
NAT-PAT
Enabled
Central Assoc
Enabled
Lync
Lync Server
Disabled
11k
Neighbor List
Enabled
Re-anchor Roamed Voice Clients
Enabled
KTS based CAC Policy
Enabled
Radius Client Profiling
DHCP Profiling
HTTP Profiling
Local Client Profiling
DHCP Profiling
HTTP Profiling
PMIP
PMIP Mobility Type
PMIP NAI Type
Hexadecimal
PMIP Profile
None
PMIP Realm
Universal AP Admin Support
Universal AP Admin
11v BSS Transition Support
BSS Transition

客户端连接测试

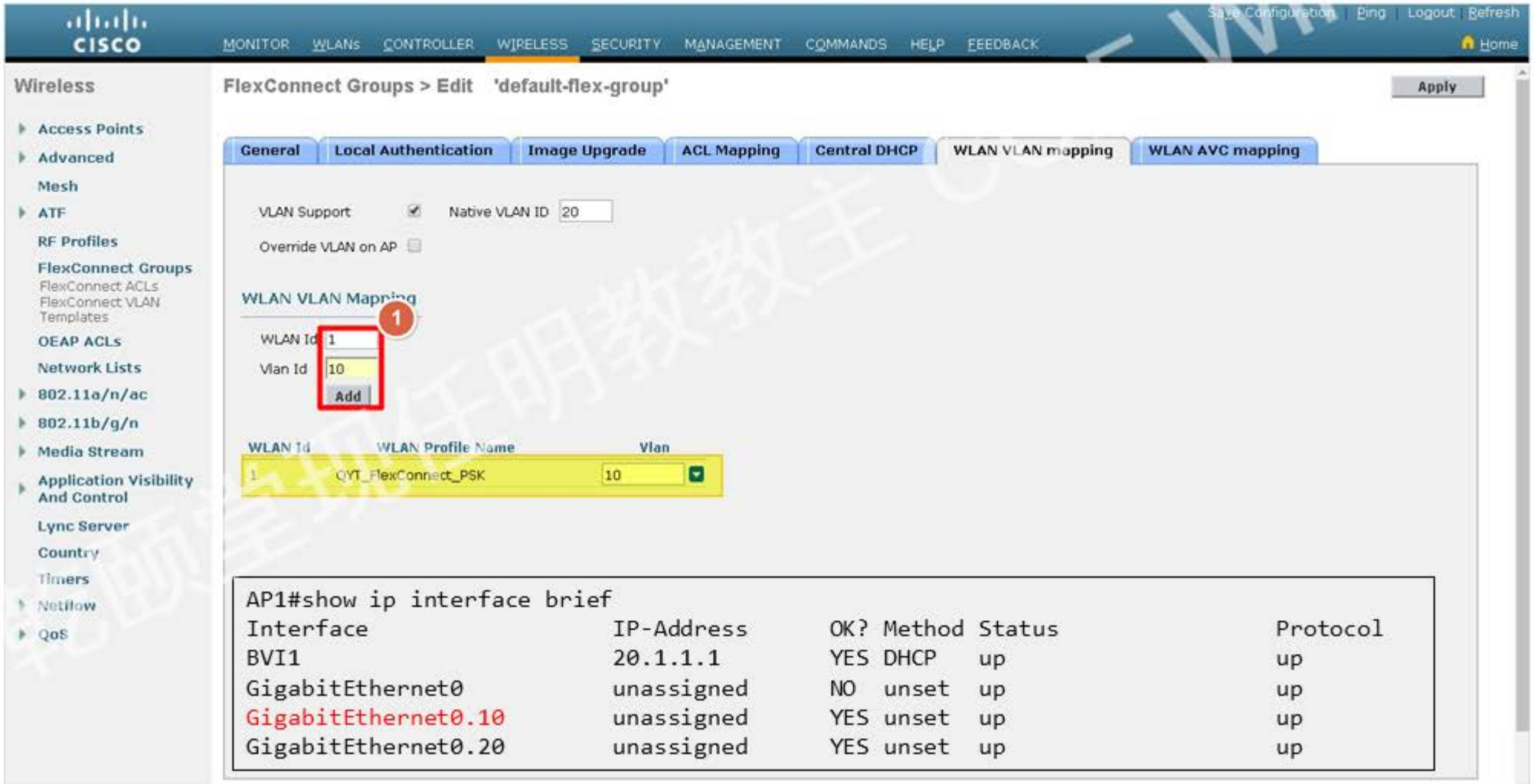

Cisco AnyConnect Secure Mobility Client
Network:
Connected (20.1.1.2)
QYT_FlexConnect_PSK


命令提示符
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 20.1.1.2
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 20.1.1.253
C:\>
C:\>ping 20.1.1.253
正在 Ping 20.1.1.253 具有 32 字节的数据:
来自 20.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=3ms TTL=255
20.1.1.253 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 = 3ms, 最长 = 3ms, 平均 = 3ms
C:\>

配置 WLAN VLAN 映射 - 1

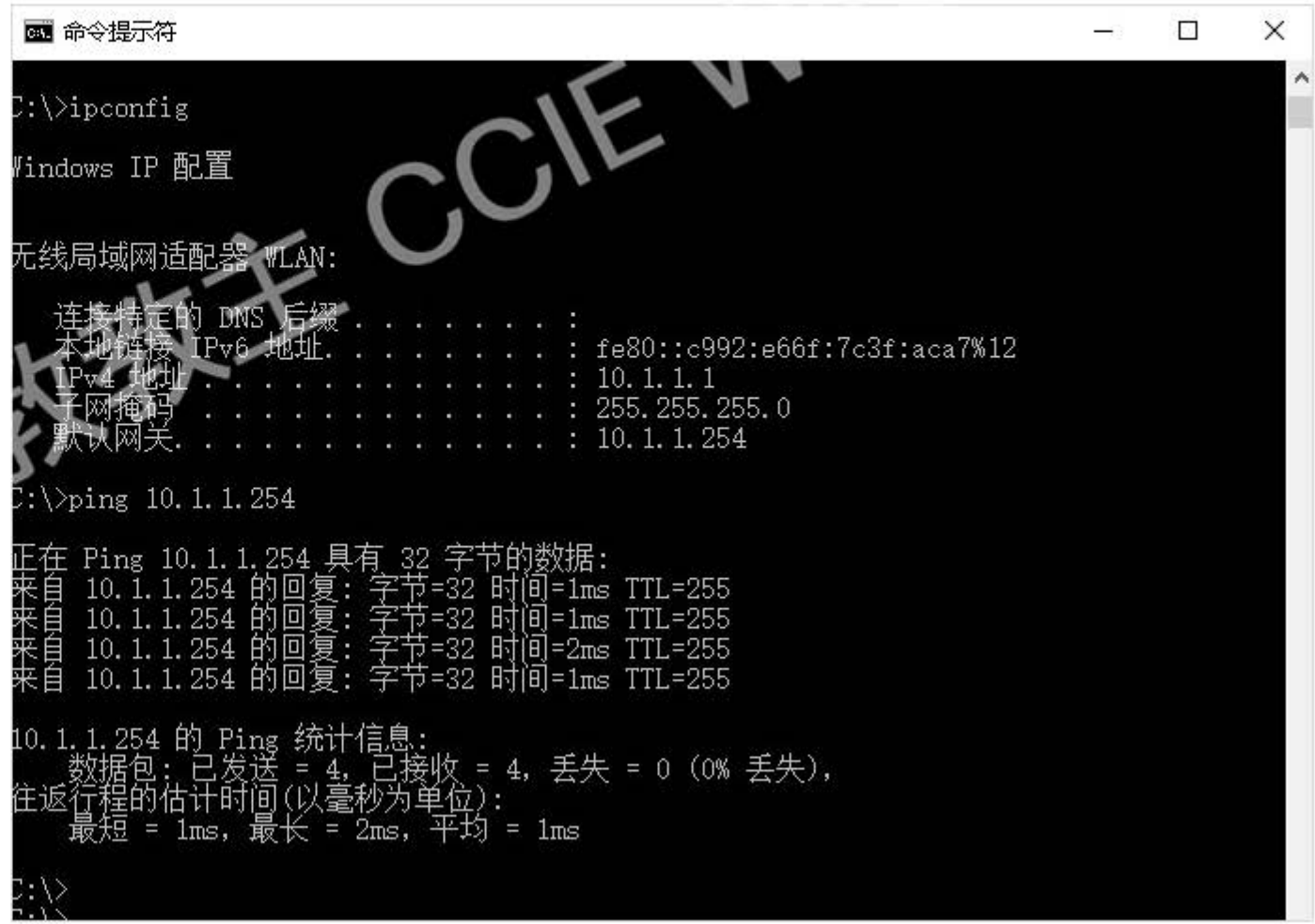


配置 WLAN VLAN 映射 - 2

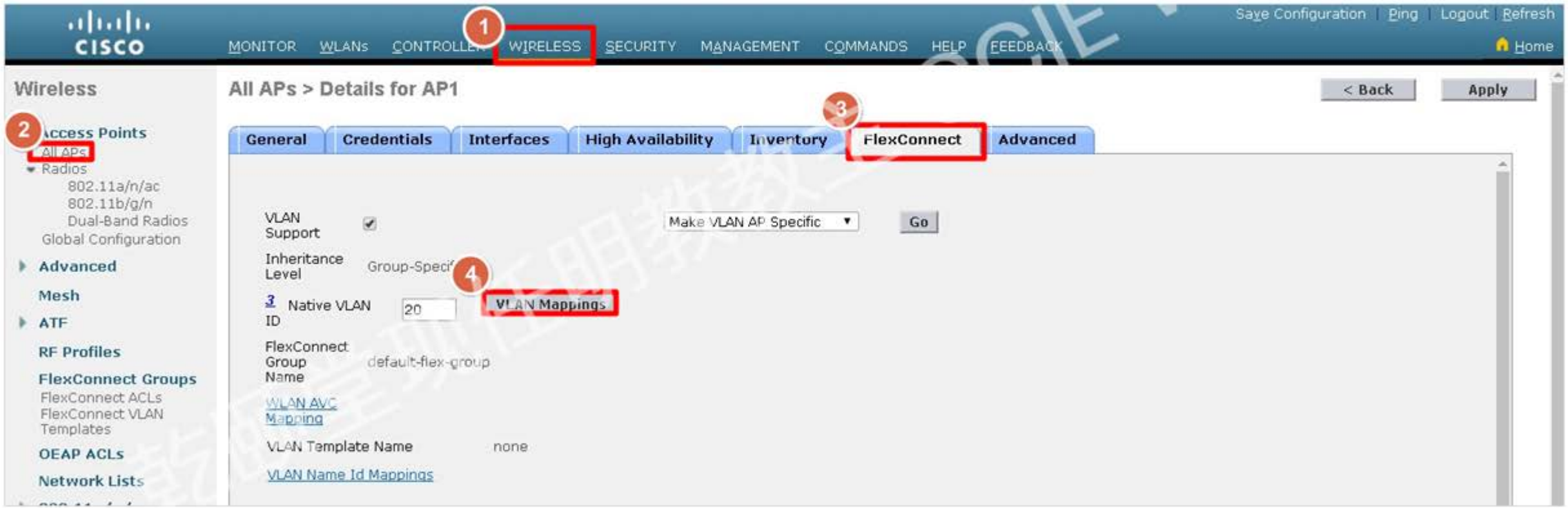


客户端连接测试

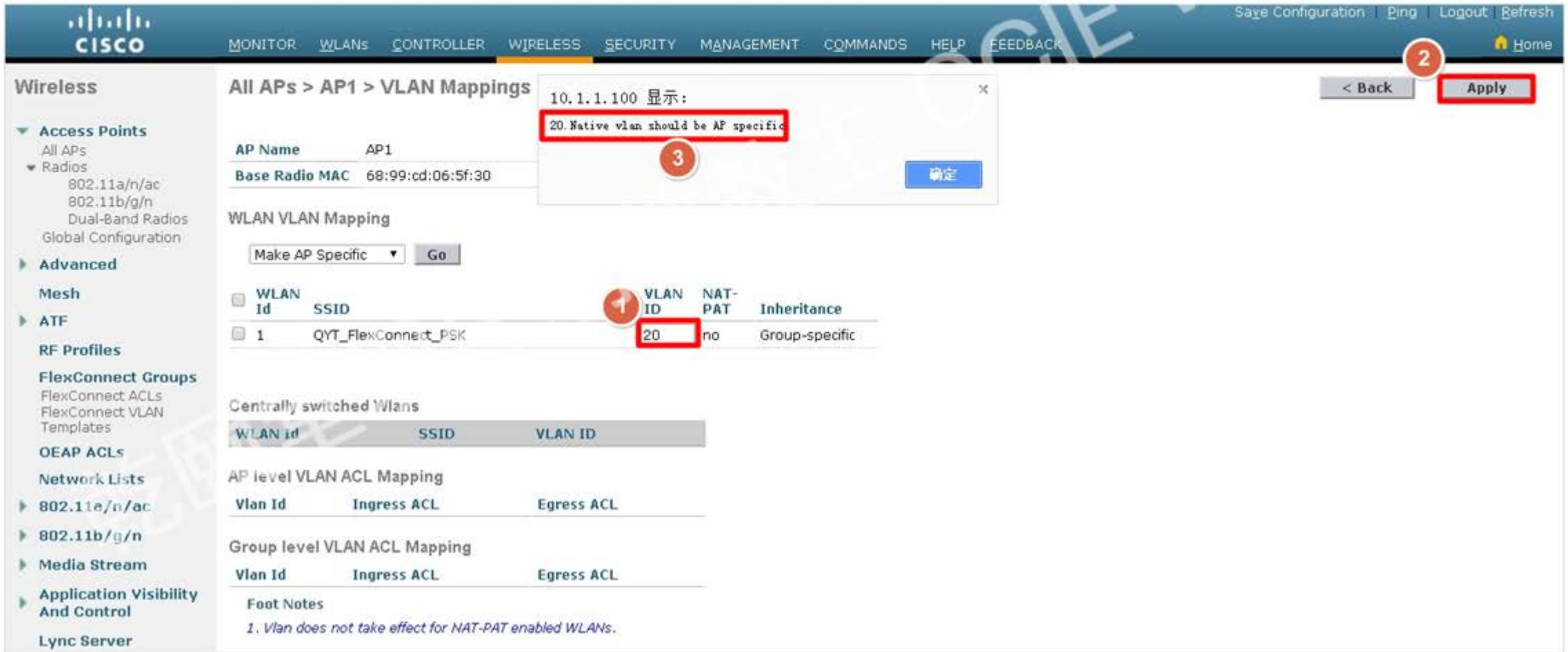

Cisco AnyConnect Secure Mobility Client
Network:
Connected (10.1.1.1)
QYT_FlexConnect_PSK


命令提示符
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 10.1.1.1
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 10.1.1.254
C:\>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=1ms 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=1ms 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:\>

AP 下面修改 VLAN 映射

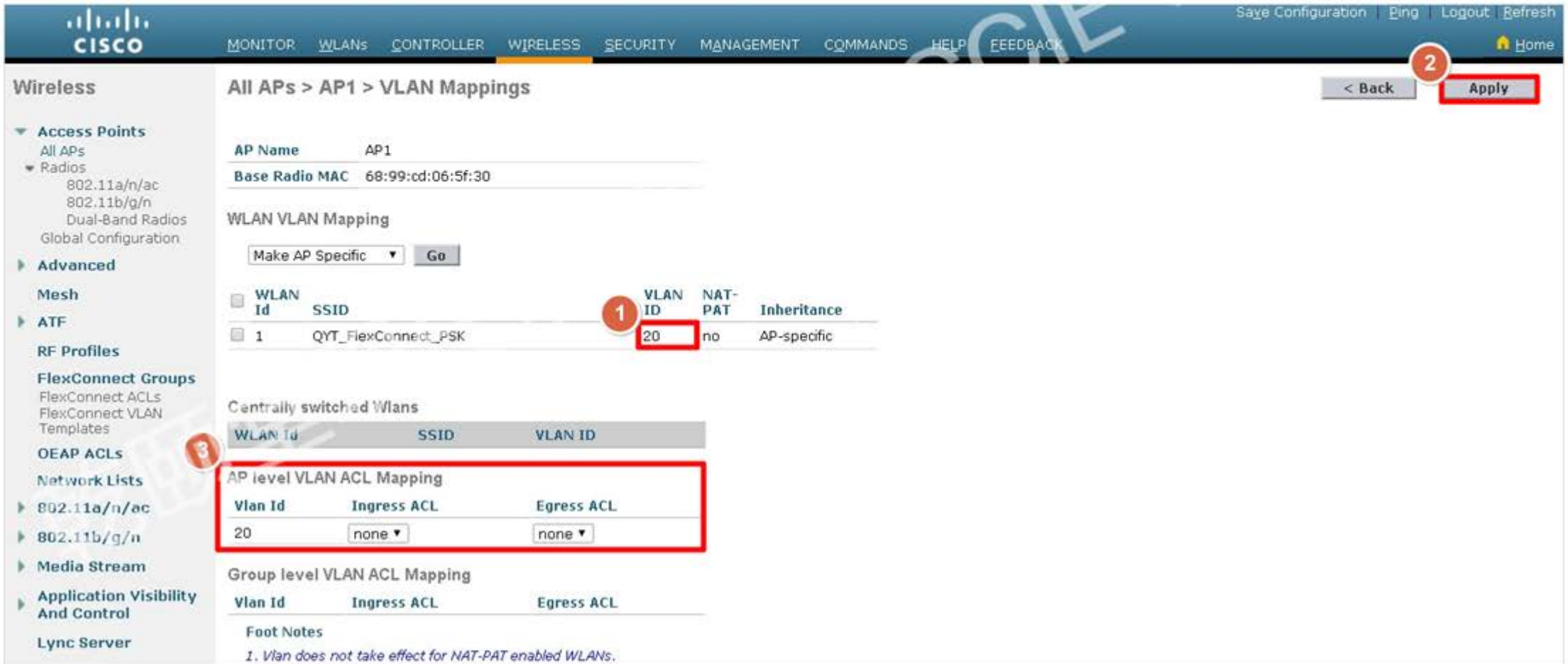


AP 下直接修改报错


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates
OEAP ACLs
Network Lists
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Lync Server
All APs > AP1 > VLAN Mappings
< Back
Apply
10.1.1.100 显示:
20.Native vlan should be AP specific
确定
AP Name AP1
Base Radio MAC 68:99:cd:06:5f:30
WLAN VLAN Mapping
Make AP Specific
Go
WLAN Id
SSID
VLAN ID
NAT-PAT
Inheritance
1
QYT_FlexConnect_PSK
20
no
Group-specific
Centrally switched Wlans
WLAN id
SSID
VLAN ID
AP level VLAN ACL Mapping
Vlan Id
Ingress ACL
Egress ACL
Group level VLAN ACL Mapping
Vlan Id
Ingress ACL
Egress ACL
Foot Notes
1. Vlan does not take effect for NAT-PAT enabled WLANs.

Make VLAN AP Special

AP 下将 WLAN 映射到 VLAN20



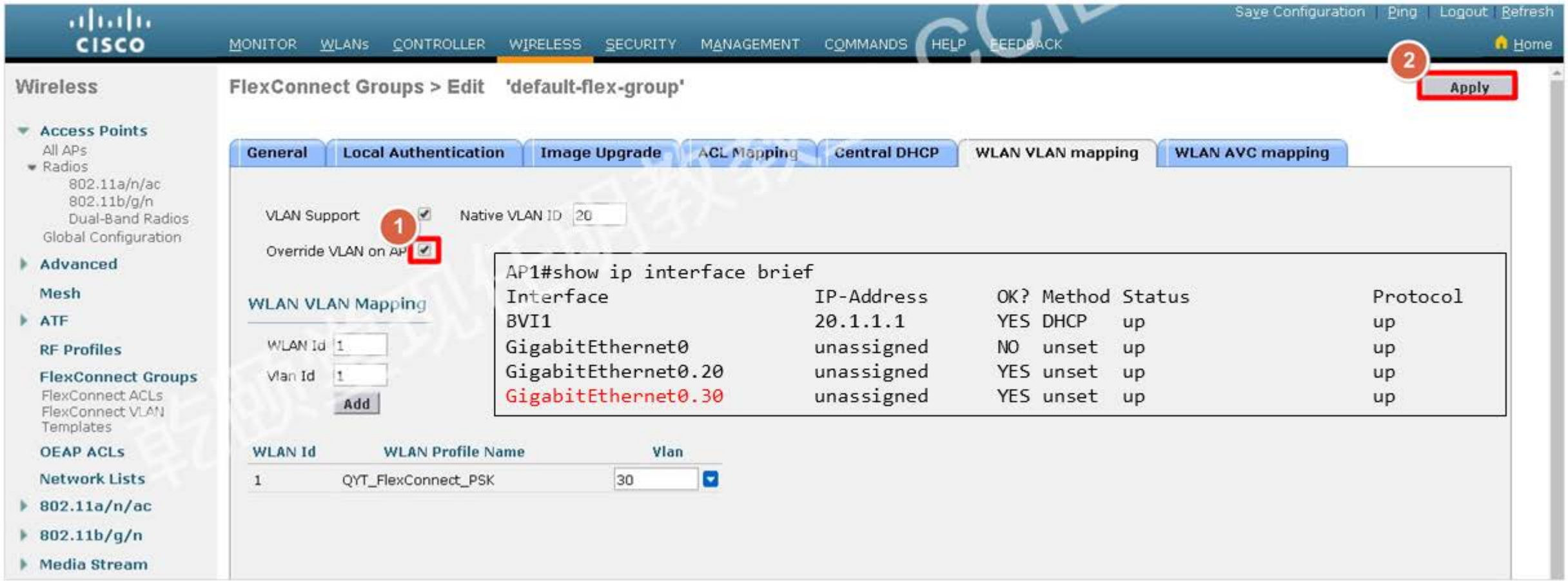
客户端连接测试


Cisco AnyConnect Secure Mobility Client
Network:
Connected (20.1.1.2)
QYT_FlexConnect_PSK


命令提示符
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 20.1.1.2
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 20.1.1.253
C:\>ping 20.1.1.253
正在 Ping 20.1.1.253 具有 32 字节的数据:
来自 20.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=3ms TTL=255
20.1.1.253 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 = 3ms, 最长 = 3ms, 平均 = 3ms

Group 下直接修改映射失败

启用“Override VLAN on AP”



客户端连接测试


Cisco AnyConnect Secure Mobility Client
Network:
Connected (30.1.1.1)
QYT_FlexConnect_PSK


命令提示符
C:\>
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 30.1.1.1
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 30.1.1.253
C:\>ping 30.1.1.253
正在 Ping 30.1.1.253 具有 32 字节的数据:
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
30.1.1.253 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 = 3ms, 最长 = 3ms, 平均 = 3ms

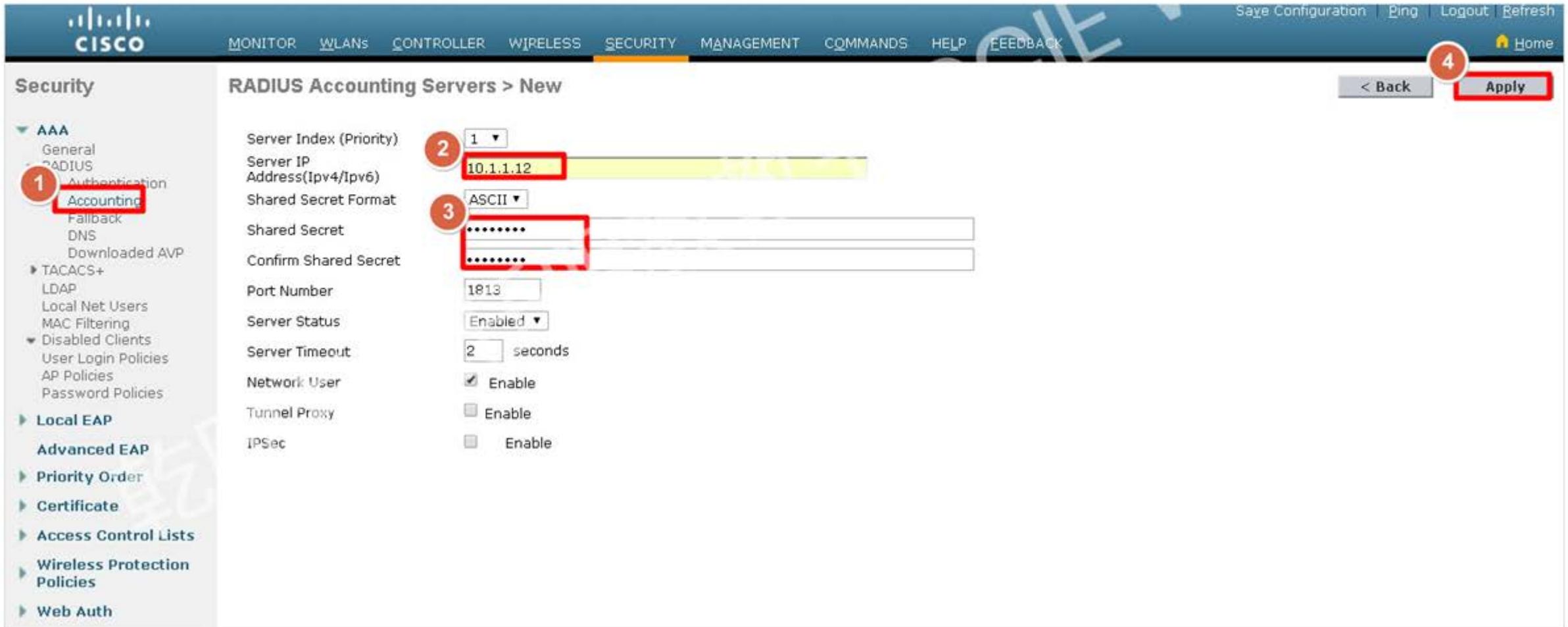
此时 AP 下无法修改映射

查看报错

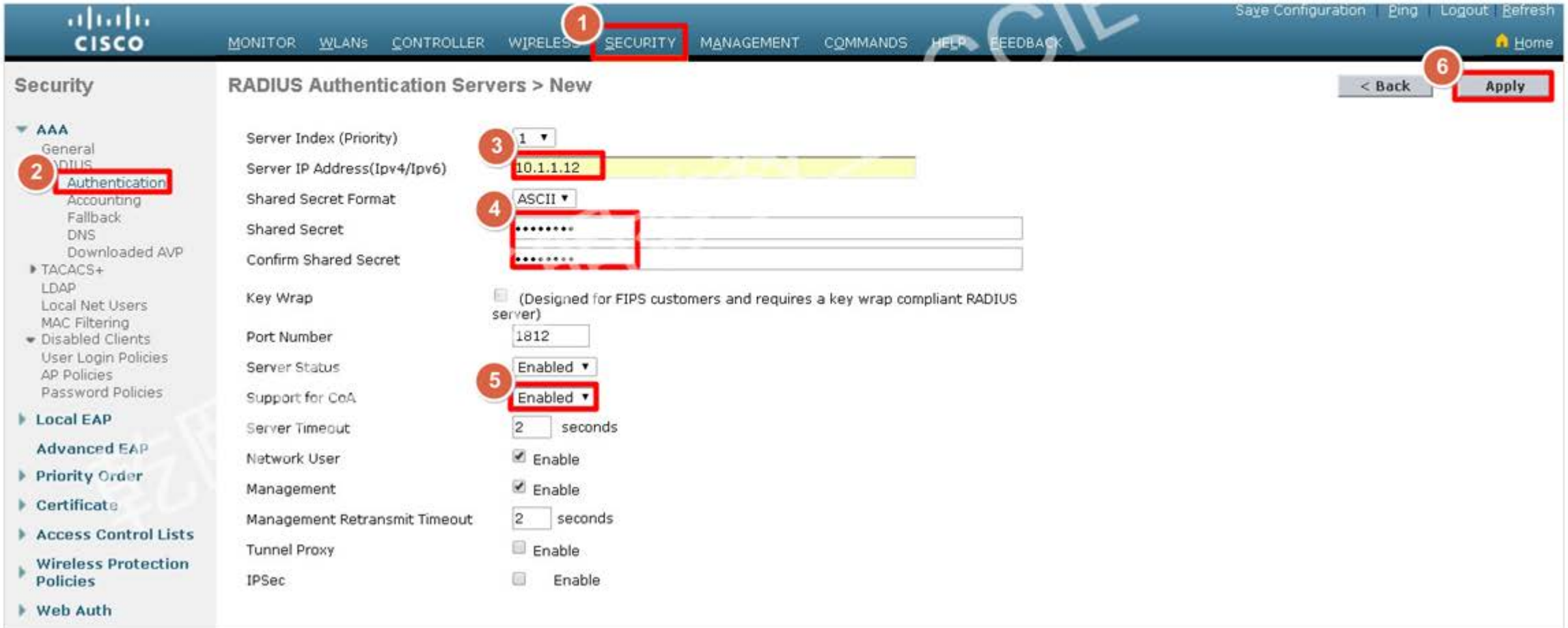

CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates
OEAP ACLs
Network Lists
All APs > Details for AP1
< Back
Apply
General
Credentials
Interfaces
High Availability
Inventory
FlexConnect
Advanced
1
2
Make VLAN AP Specific
Go
VLAN Support
Inheritance Level
Group-Specific
3
Native VLAN ID
20
VLAN Mappings
FlexConnect Group Name
default-flex-group
WLAN AVC Mapping
VLAN Template Name
none
VLAN Name Id Mappings
10.1.1.100 显示:
Failed to set VLAN Support.
Request failed: Override flag is enabled at the flexconnect group.
Failed to set FlexConnect Native VLAN ID.Override flag is enabled on the flexconnect group.
确定

3.2
VLAN Override

WLC 添加 Raidus 服务器 - 1



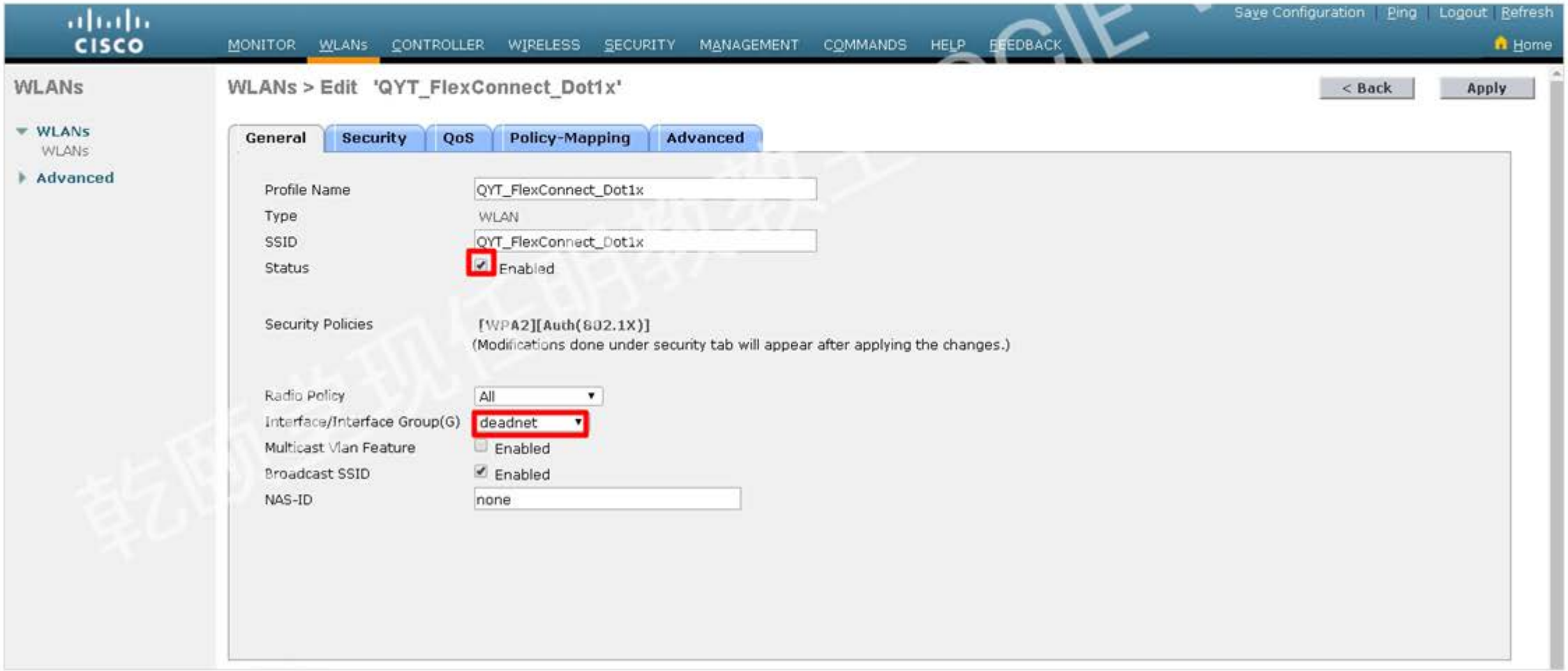
WLC 添加 Raidus 服务器 - 2



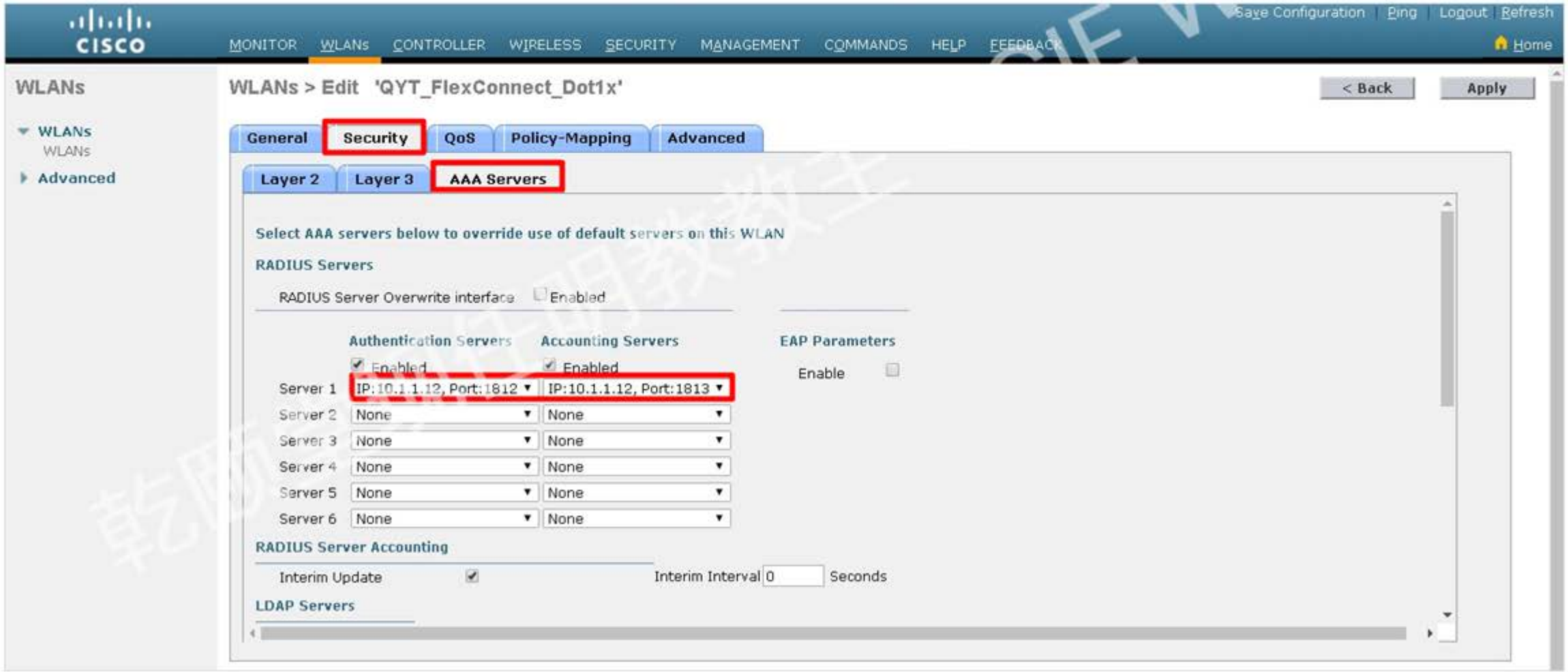
WLC 新建 WLAN - 1


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > New
< Back
Apply
WLANs
WLANs
Advanced
Type
WLAN
Profile Name
QYT_FlexConnect_Dot1x
SSID
QYT_FlexConnect_Dot1x
ID
2

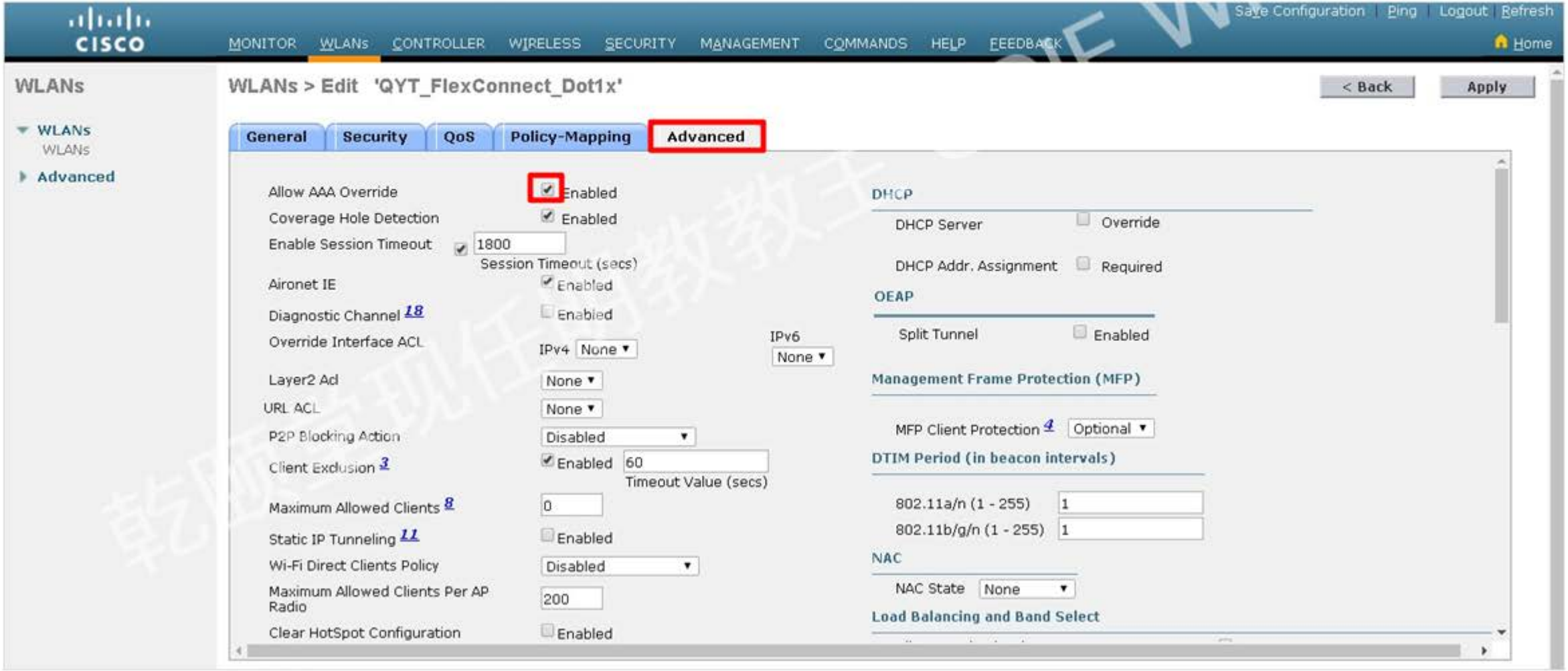
WLC 新建 WLAN - 2


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs
Advanced
WLANs > Edit 'QYT_FlexConnect_Dot1x'
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
QYT_FlexConnect_Dot1x
Type
WLAN
SSID
QYT_FlexConnect_Dot1x
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)
deadnet
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none

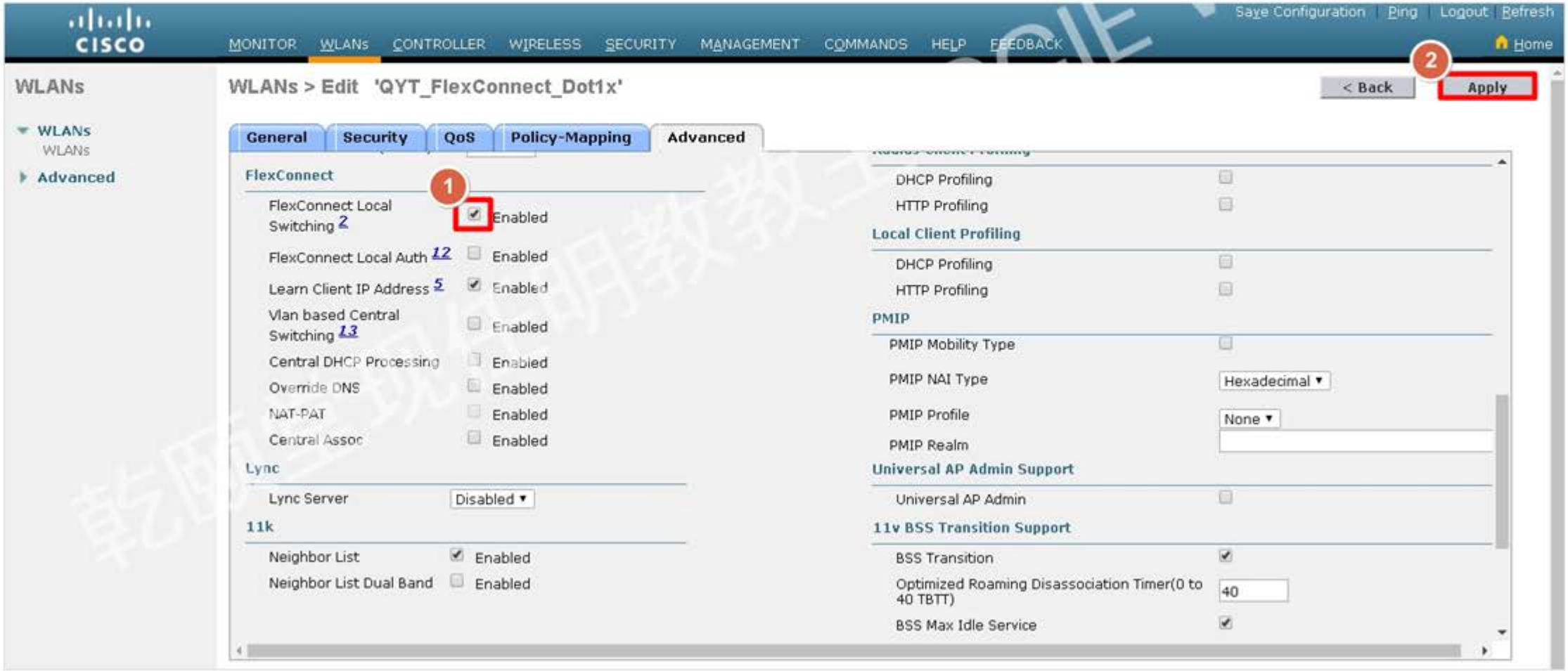
WLC 新建 WLAN - 3


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs
Advanced
WLANs > Edit 'QYT_FlexConnect_Dot1x'
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Select AAA servers below to override use of default servers on this WLAN
RADIUS Servers
RADIUS Server Overwrite interface
Enabled
Authentication Servers
Accounting Servers
EAP Parameters
Enabled
Enabled
Enable
Server 1
IP:10.1.1.12, Port:1812
IP:10.1.1.12, Port:1813
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
Seconds
LDAP Servers

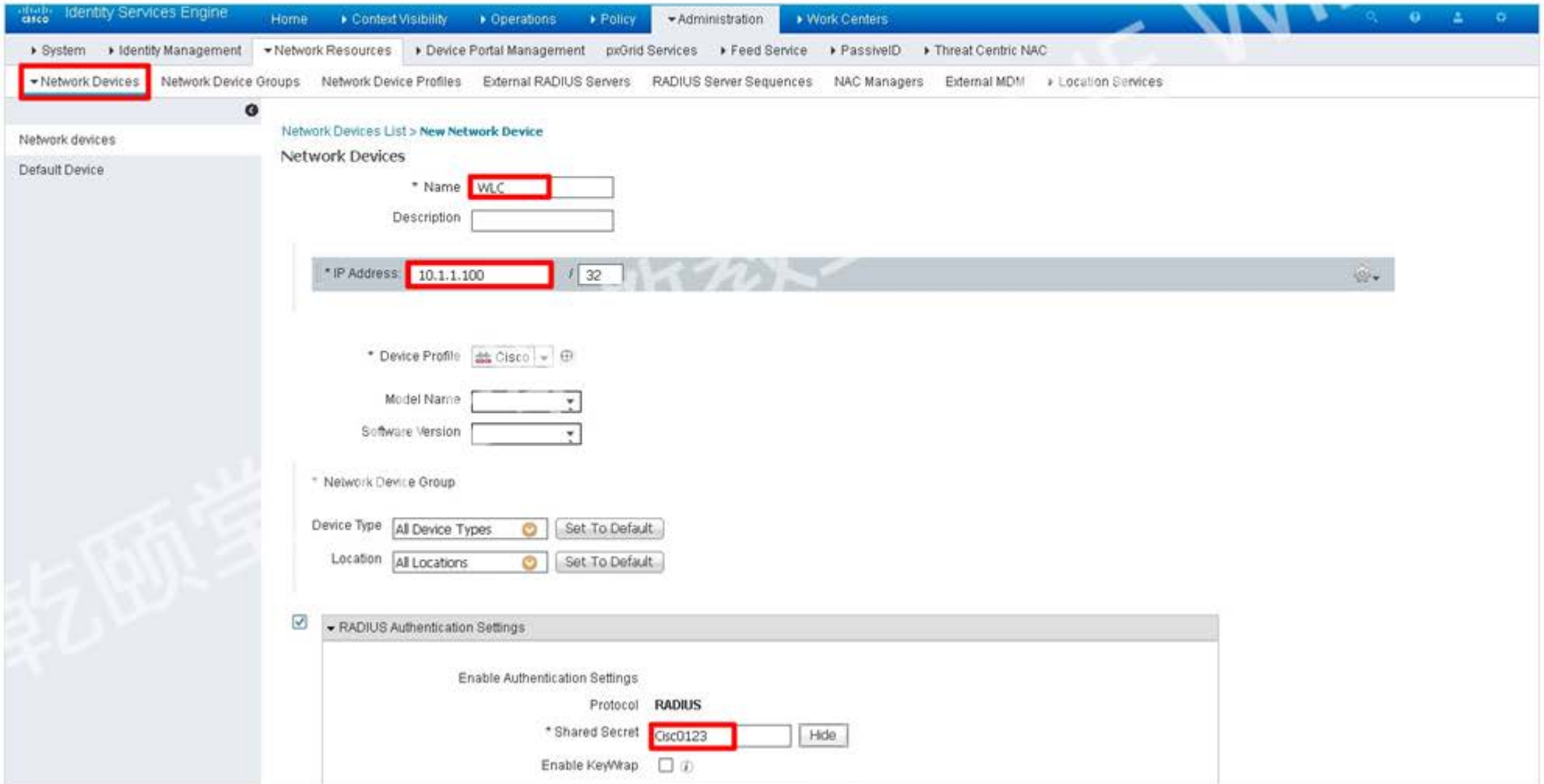
WLC 新建 WLAN - 4


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > Edit 'QYT_FlexConnect_Dot1x'
< Back
Apply
WLANs
WLANs
Advanced
General
Security
QoS
Policy-Mapping
Advanced
Allow AAA Override
Enabled
Coverage Hole Detection
Enabled
Enable Session Timeout
1800
Session Timeout (secs)
Aironet IE
Enabled
Diagnostic Channel 18
Enabled
Override Interface ACL
IPv4 None
IPv6 None
Layer2 Acl
None
URL ACL
None
P2P Blocking Action
Disabled
Client Exclusion 3
Enabled
60
Timeout Value (secs)
Maximum Allowed Clients 8
0
Static IP Tunneling 11
Enabled
Wi-Fi Direct Clients Policy
Disabled
Maximum Allowed Clients Per AP Radio
200
Clear HotSpot Configuration
Enabled
DHCP
DHCP Server
Override
DHCP Addr. Assignment
Required
OEAP
Split Tunnel
Enabled
Management Frame Protection (MFP)
MFP Client Protection 4
Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255)
1
802.11b/g/n (1 - 255)
1
NAC
NAC State
None
Load Balancing and Band Select

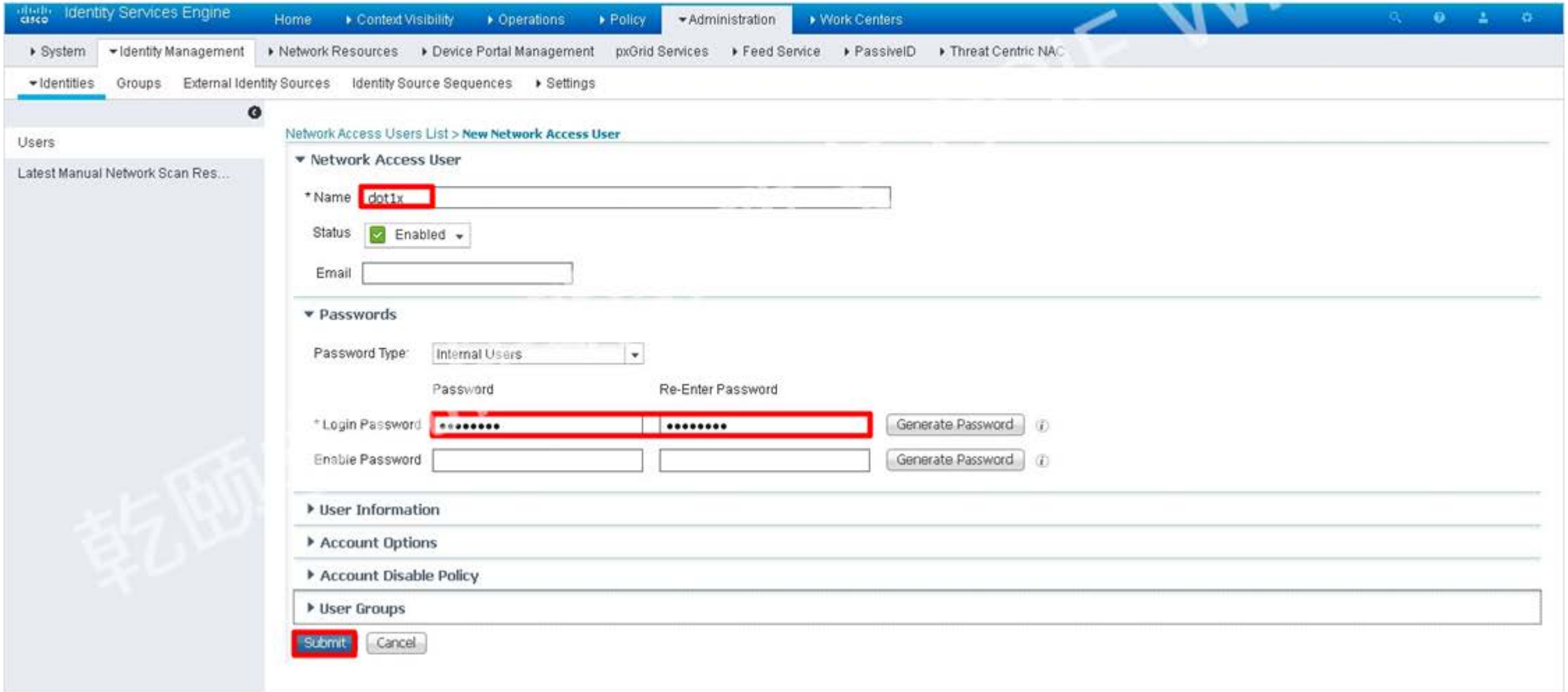
WLC 新建 WLAN - 5


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs > Edit 'QYT_FlexConnect_Dot1x'
< Back
Apply
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
FlexConnect
FlexConnect Local Switching 2
Enabled
FlexConnect Local Auth 12
Enabled
Learn Client IP Address 5
Enabled
Vlan based Central Switching 13
Enabled
Central DHCP Processing
Enabled
Override DNS
Enabled
NAT-PAT
Enabled
Central Assoc
Enabled
Lync
Lync Server
Disabled
11k
Neighbor List
Enabled
Neighbor List Dual Band
Enabled
DHCP Profiling
HTTP Profiling
Local Client Profiling
DHCP Profiling
HTTP Profiling
PMIP
PMIP Mobility Type
PMIP NAI Type
Hexadecimal
PMIP Profile
None
PMIP Realm
Universal AP Admin Support
Universal AP Admin
11v BSS Transition Support
BSS Transition
Optimized Roaming Disassociation Timer(0 to 40 TBTT)
40
BSS Max Idle Service

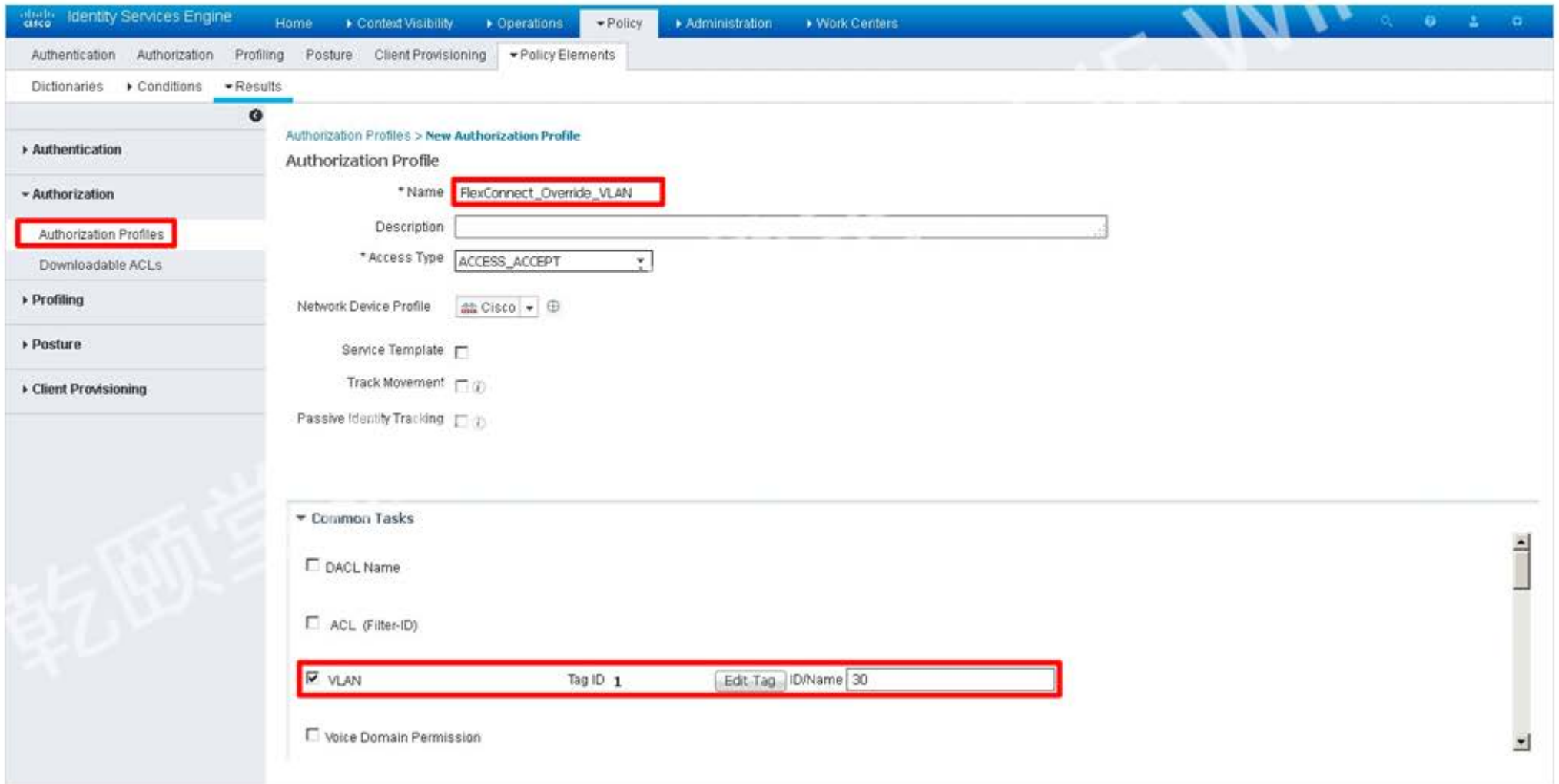
ISE 创建 Network Device



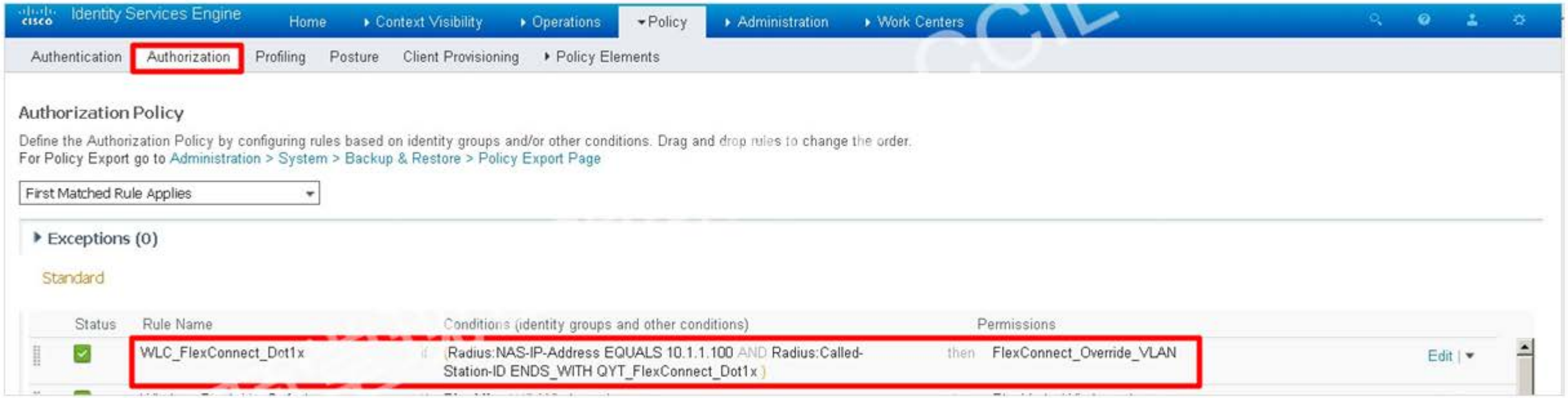
ISE 创建用户


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
PassiveID
Threat Centric NAC
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...
Network Access Users List > New Network Access User
Network Access User
*Name dot1x
Status Enabled
Email
Passwords
Password Type: Internal Users
Password
Re-Enter Password
*Login Password
Generate Password
Enable Password
Generate Password
User Information
Account Options
Account Disable Policy
User Groups
Submit
Cancel

ISE 创建授权 Profile

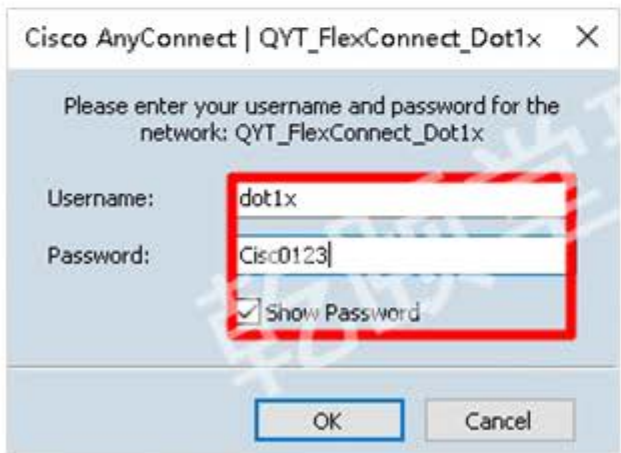


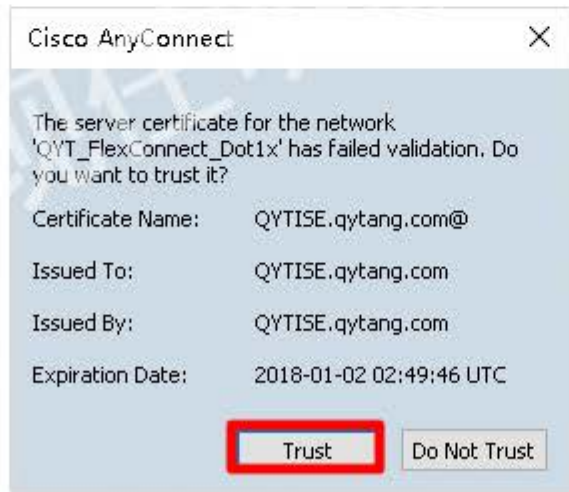
ISE 创建授权策略

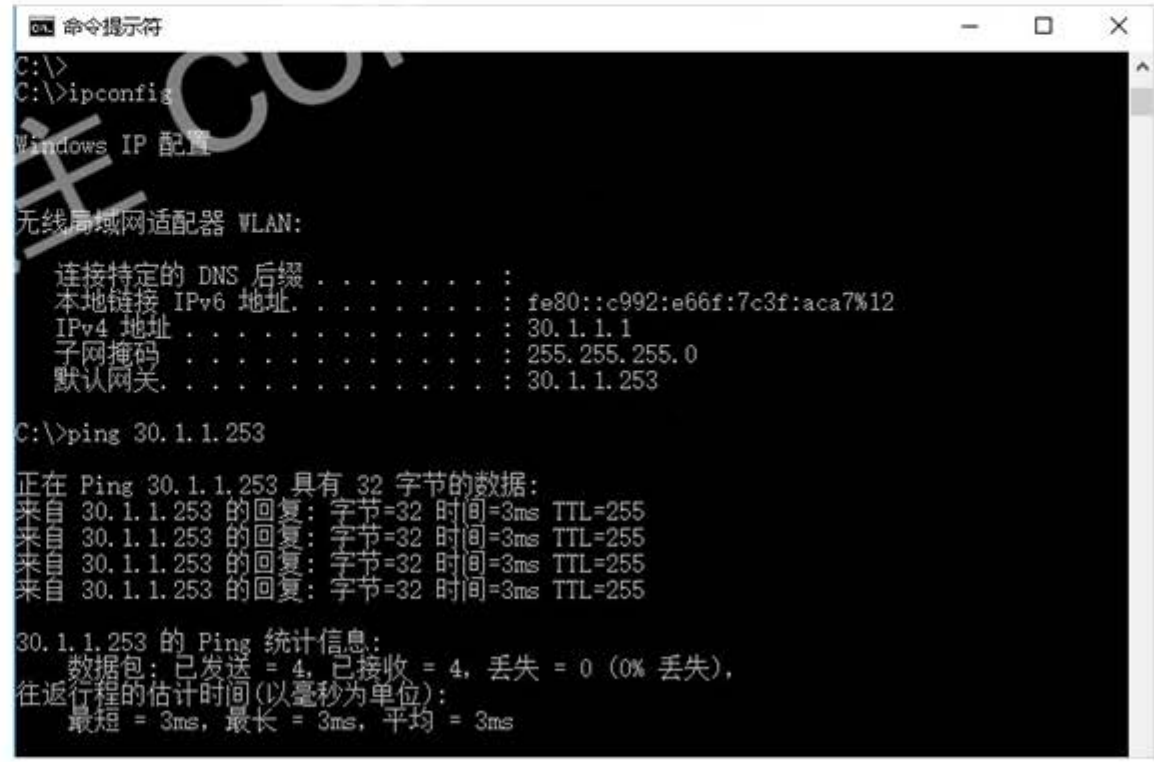

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Authentication
Authorization
Profiling
Posture
Client Provisioning
Policy Elements
Authorization Policy
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page
First Matched Rule Applies
Exceptions (0)
Standard
Status
Rule Name
Conditions (identity groups and other conditions)
Permissions
WLC_FlexConnect_Dot1x
if
(Radius:NAS-IP-Address EQUALS 10.1.1.100 AND Radius:Called-Station-ID ENDS_WITH QYT_FlexConnect_Dot1x)
then
FlexConnect_Override_VLAN
Edit

客户端连接测试

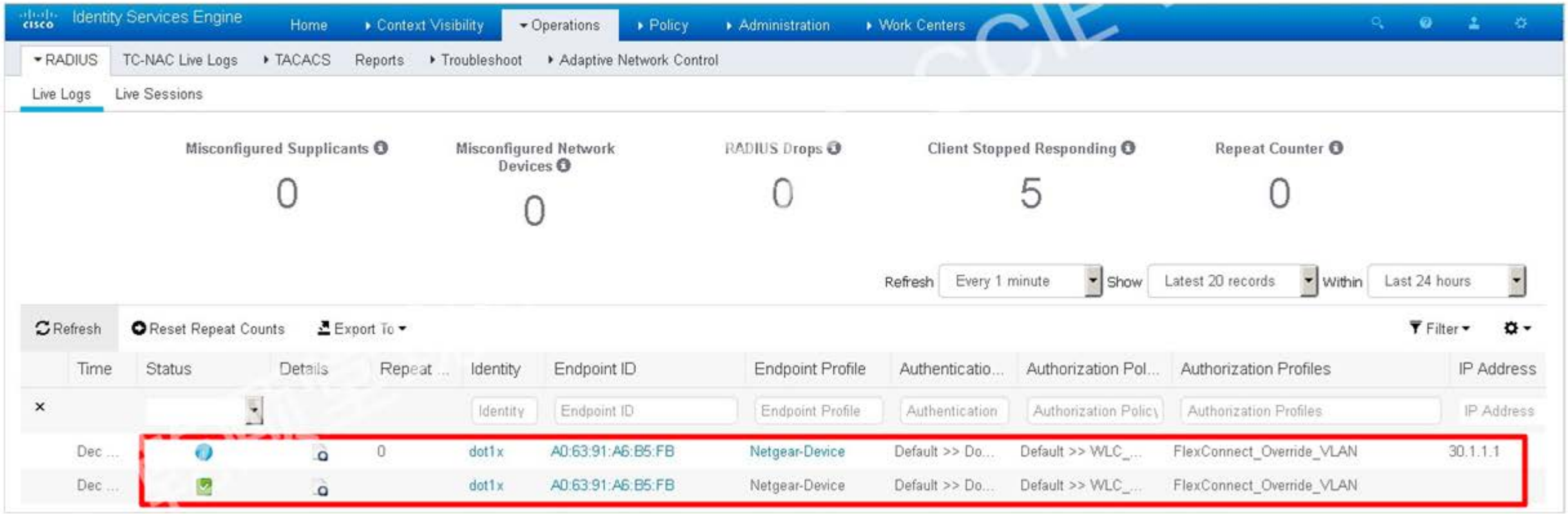

Cisco AnyConnect Secure Mobility Client
Network:
Authenticating
QYT_FlexConnect_Dot1x


Cisco AnyConnect | QYT_FlexConnect_Dot1x
Please enter your username and password for the network: QYT_FlexConnect_Dot1x
Username:
dot1x
Password:
Cisc0123
Show Password
OK
Cancel

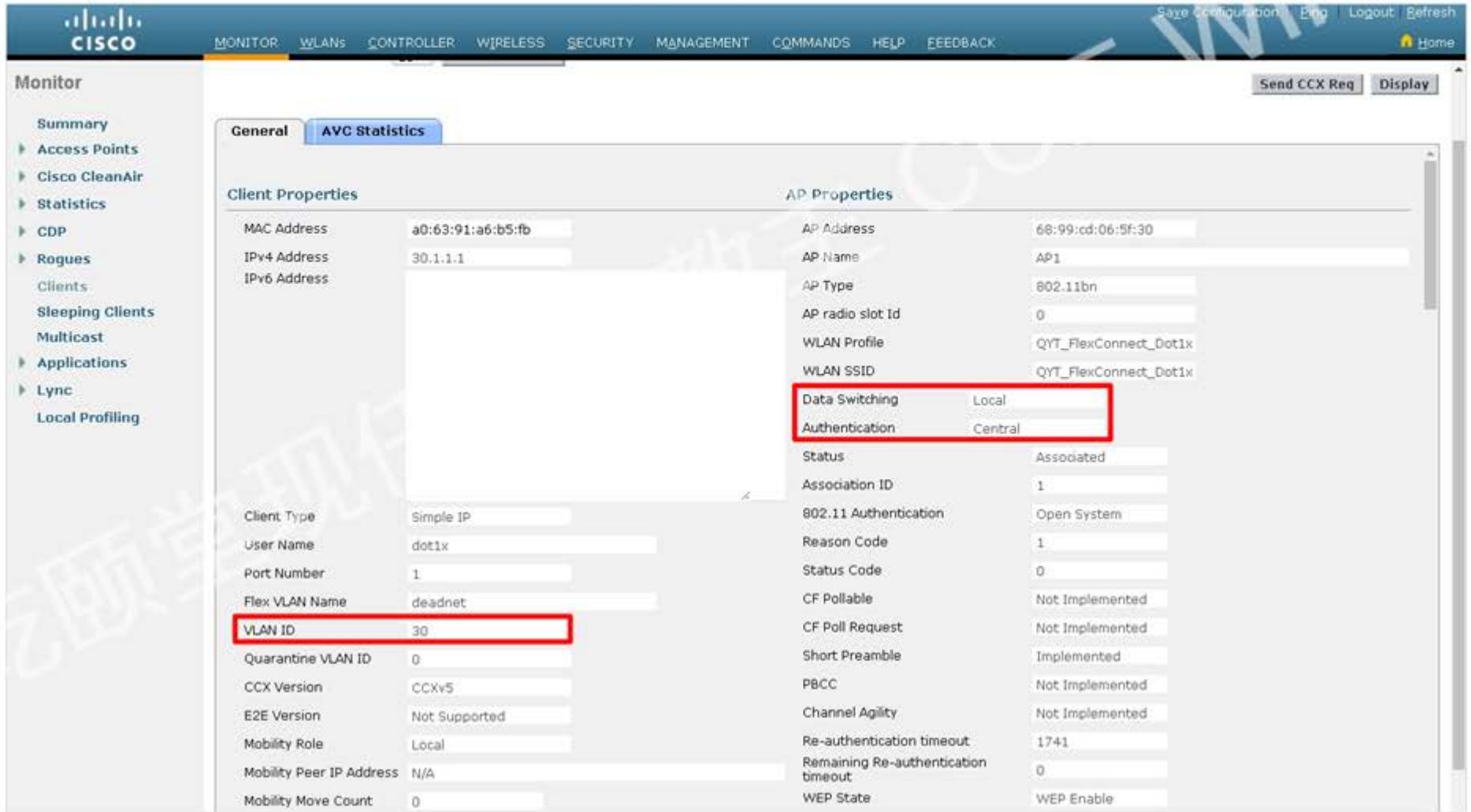

Cisco AnyConnect
The server certificate for the network 'QYT_FlexConnect_Dot1x' has failed validation. Do you want to trust it?
Certificate Name: QYTISE.qytang.com@
Issued To: QYTISE.qytang.com
Issued By: QYTISE.qytang.com
Expiration Date: 2018-01-02 02:49:46 UTC
Trust
Do Not Trust


命令提示符
C:\>
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 30.1.1.1
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 30.1.1.253
C:\>ping 30.1.1.253
正在 Ping 30.1.1.253 具有 32 字节的数据:
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
30.1.1.253 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 = 3ms, 最长 = 3ms, 平均 = 3ms

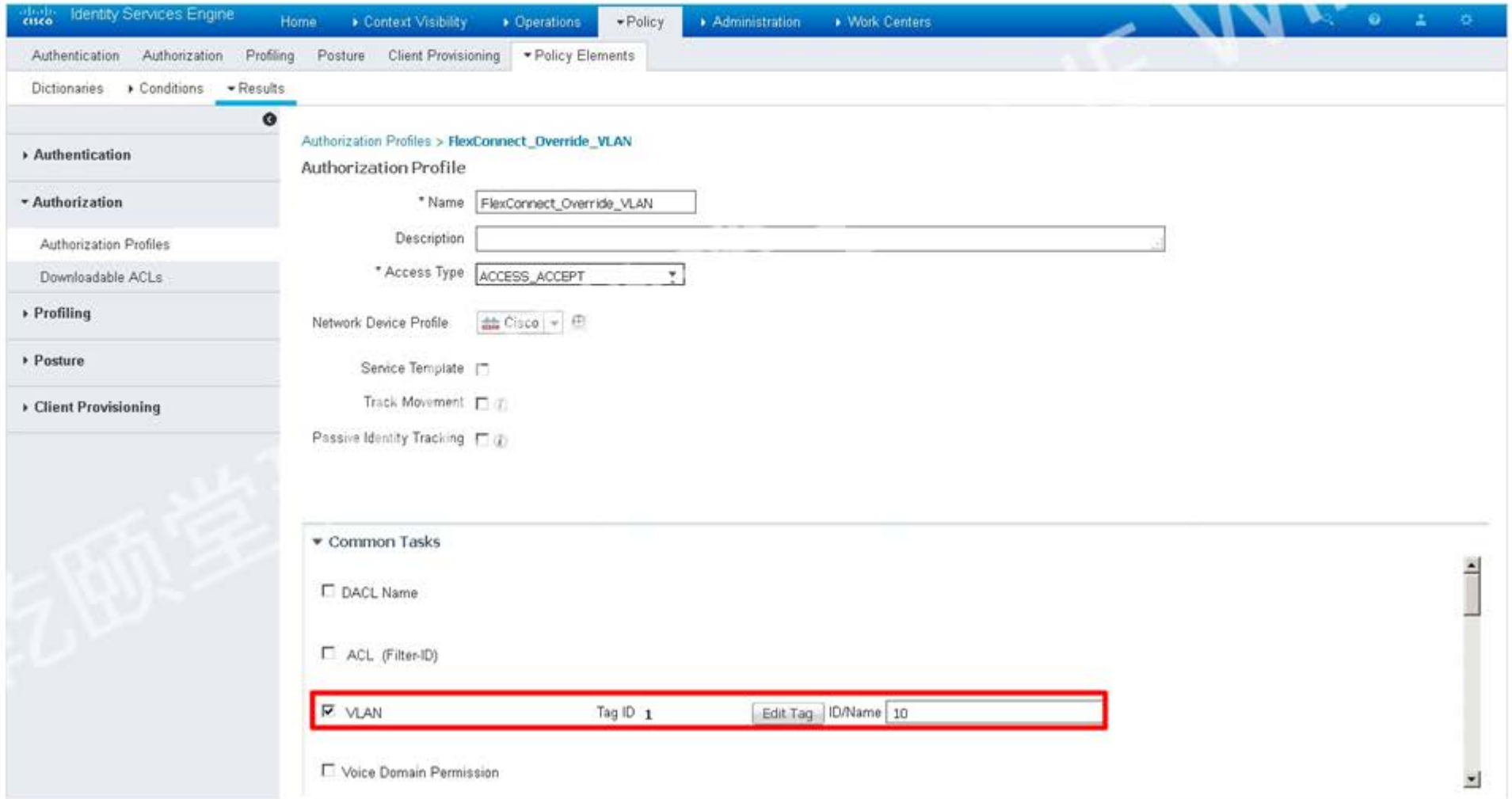
ISE 查看认证日志


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
RADIUS
TC-NAC Live Logs
TACACS
Reports
Troubleshoot
Adaptive Network Control
Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
5
Repeat Counter
0
Refresh
Every 1 minute
Show
Latest 20 records
Within
Last 24 hours
Refresh
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repeat ...
Identity
Endpoint ID
Endpoint Profile
Authenticatio...
Authorization Pol...
Authorization Profiles
IP Address
Identity
Endpoint ID
Endpoint Profile
Authentication
Authorization Policy
Authorization Profiles
IP Address
Dec ...
0
dot1x
A0:63:91:A6:B5:FB
Netgear-Device
Default >> Do...
Default >> WLC_...
FlexConnect_Override_VLAN
30.1.1.1
Dec ...
dot1x
A0:63:91:A6:B5:FB
Netgear-Device
Default >> Do...
Default >> WLC_...
FlexConnect_Override_VLAN

WLC 查看客户端信息


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
Send CCX Req
Display
General
AVC Statistics
Client Properties
MAC Address a0:63:91:a6:b5:fb
IPv4 Address 30.1.1.1
IPv6 Address
Client Type Simple IP
User Name dot1x
Port Number 1
Flex VLAN Name deadnet
VLAN ID 30
Quarantine VLAN ID 0
CCX Version CCXv5
E2E Version Not Supported
Mobility Role Local
Mobility Peer IP Address N/A
Mobility Move Count 0
AP Properties
AP Address 68:99:cd:06:5f:30
AP Name AP1
AP Type 802.11bn
AP radio slot Id 0
WLAN Profile QYT_FlexConnect_Dot1x
WLAN SSID QYT_FlexConnect_Dot1x
Data Switching Local
Authentication Central
Status Associated
Association ID 1
802.11 Authentication Open System
Reason Code 1
Status Code 0
CF Pollable Not Implemented
CF Poll Request Not Implemented
Short Preamble Implemented
PBCC Not Implemented
Channel Agility Not Implemented
Re-authentication timeout 1741
Remaining Re-authentication timeout 0
WEP State WEP Enable

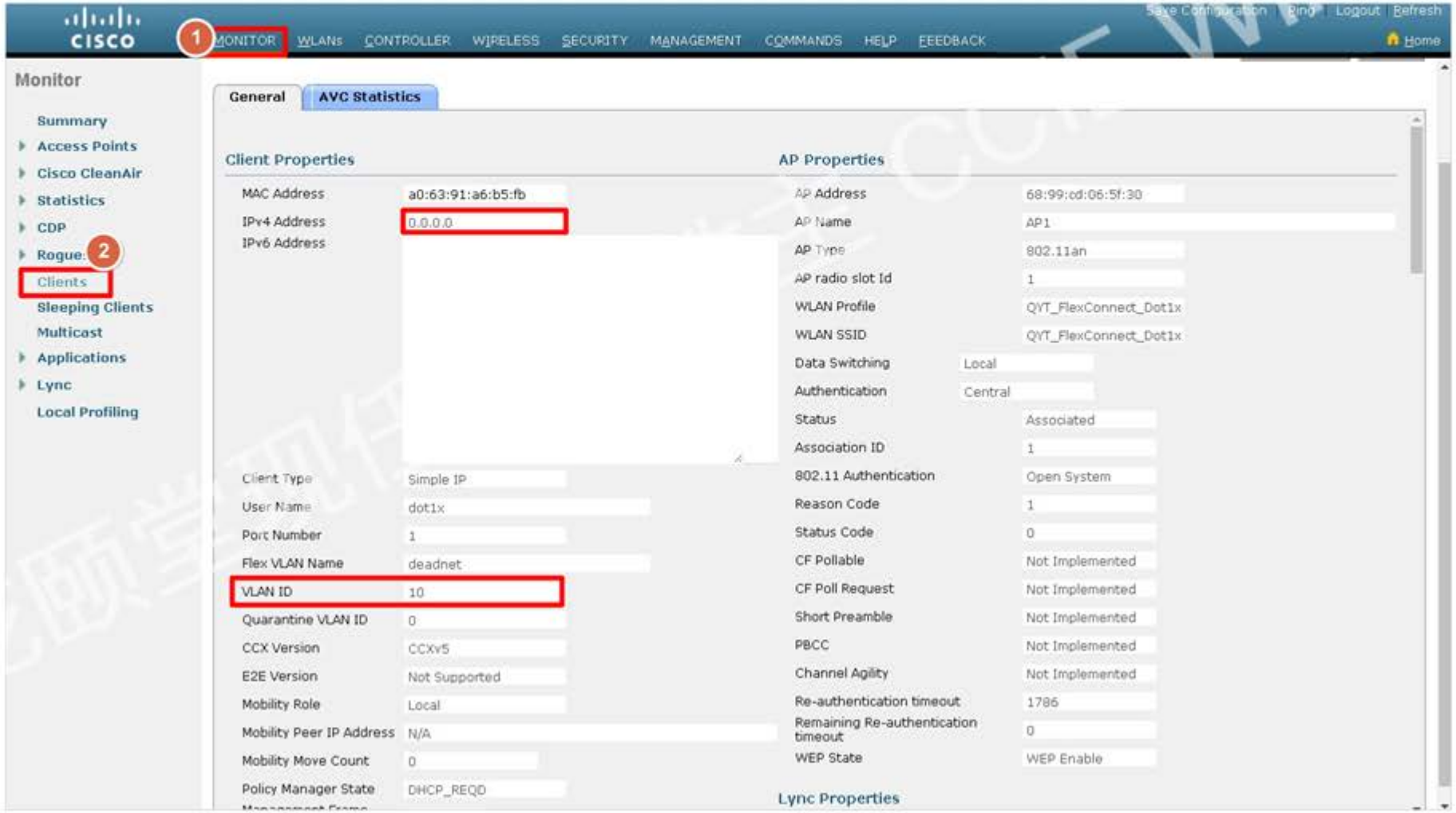
修改授权为 VLAN10



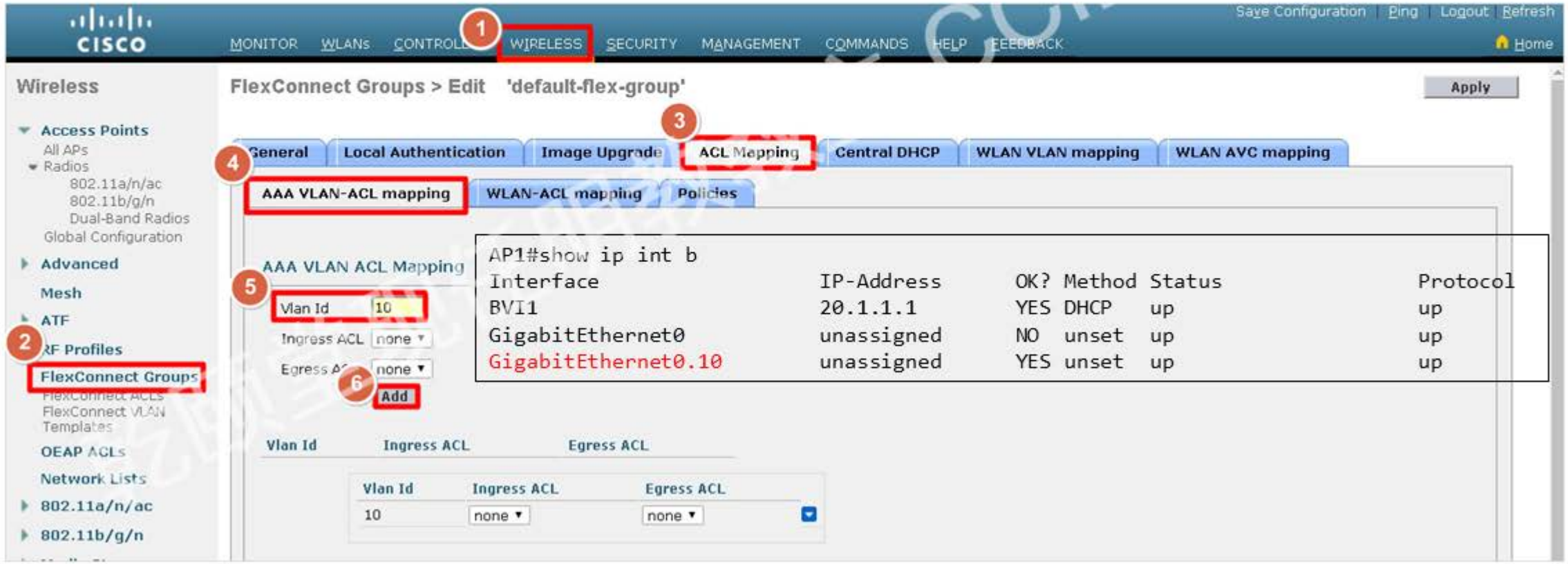
AP 没有授权 VLAN

```
AP1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
BVI1                       20.1.1.1        YES DHCP   up                    up
GigabitEthernet0           unassigned      NO  unset  up                    up
GigabitEthernet0.20        unassigned      YES unset  up                    up
GigabitEthernet0.30        unassigned      YES unset  up                    up
```

查看 AP 信息


CISCO
1
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
EEEDBACK
Save Configuration
Ping
Logout
Refresh
Home
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
2
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
General
AVC Statistics
Client Properties
MAC Address a0:63:91:a6:b5:fb
IPv4 Address 0.0.0.0
IPv6 Address
Client Type Simple IP
User Name dot1x
Port Number 1
Flex VLAN Name deadnet
VLAN ID 10
Quarantine VLAN ID 0
CCX Version CCXv5
E2E Version Not Supported
Mobility Role Local
Mobility Peer IP Address N/A
Mobility Move Count 0
Policy Manager State DHCP_REQD
AP Properties
AP Address 68:99:cd:06:5f:30
AP Name AP1
AP Type 802.11an
AP radio slot Id 1
WLAN Profile QYT_FlexConnect_Dot1x
WLAN SSID QYT_FlexConnect_Dot1x
Data Switching Local
Authentication Central
Status Associated
Association ID 1
802.11 Authentication Open System
Reason Code 1
Status Code 0
CF Pollable Not Implemented
CF Poll Request Not Implemented
Short Preamble Not Implemented
PBCC Not Implemented
Channel Agility Not Implemented
Re-authentication timeout 1786
Remaining Re-authentication timeout 0
WEP State WEP Enable
Lync Properties

AP 添加 VLAN（子接口）



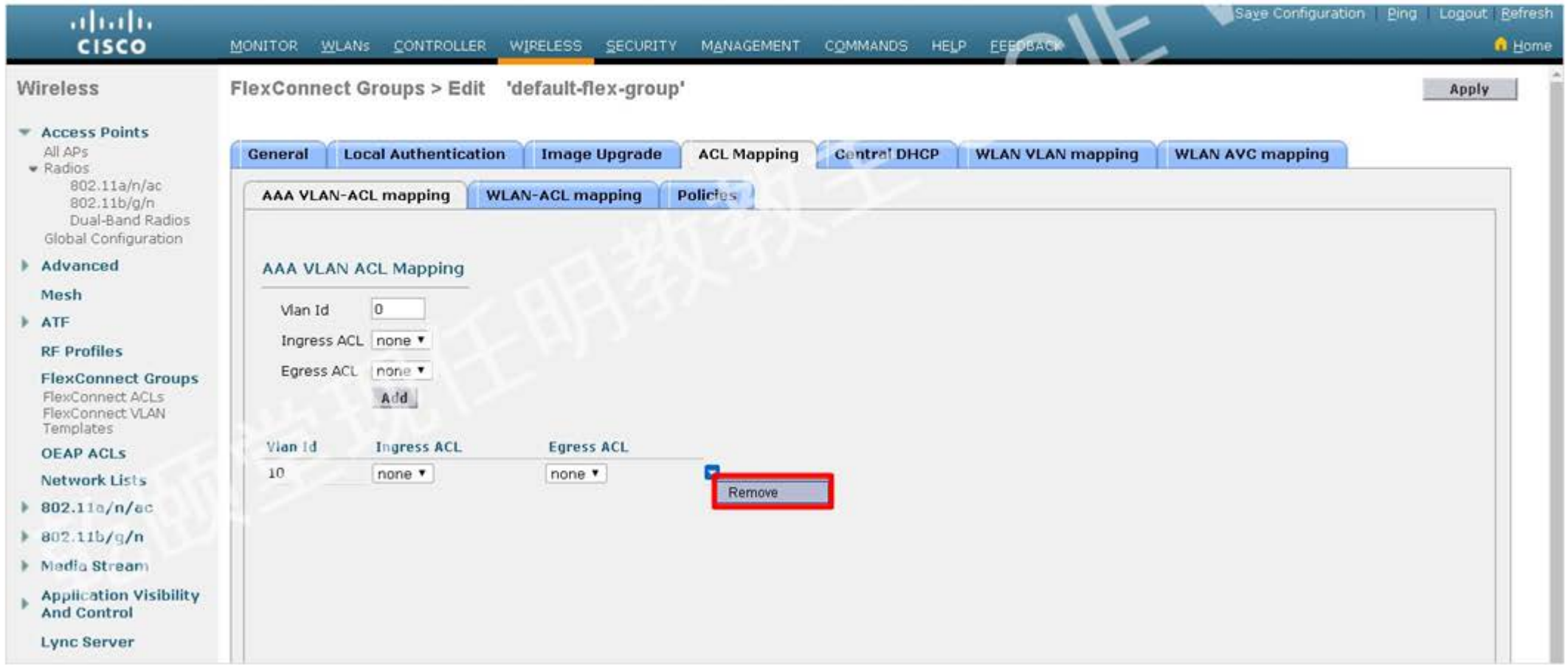

```
AP1#show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
BVI1                       20.1.1.1        YES DHCP   up                    up
GigabitEthernet0           unassigned      NO  unset  up                    up
GigabitEthernet0.10        unassigned      YES unset  up                    up
```

客户连接测试


Cisco AnyConnect Secure Mobility Client
Network:
Connected (10.1.1.1)
QYT_FlexConnect_Dot1x


命令提示符
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 10.1.1.1
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 10.1.1.254
C:\>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=1ms 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=1ms 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 = 3ms, 平均 = 1ms

AP 删除 VLAN10（子接口）

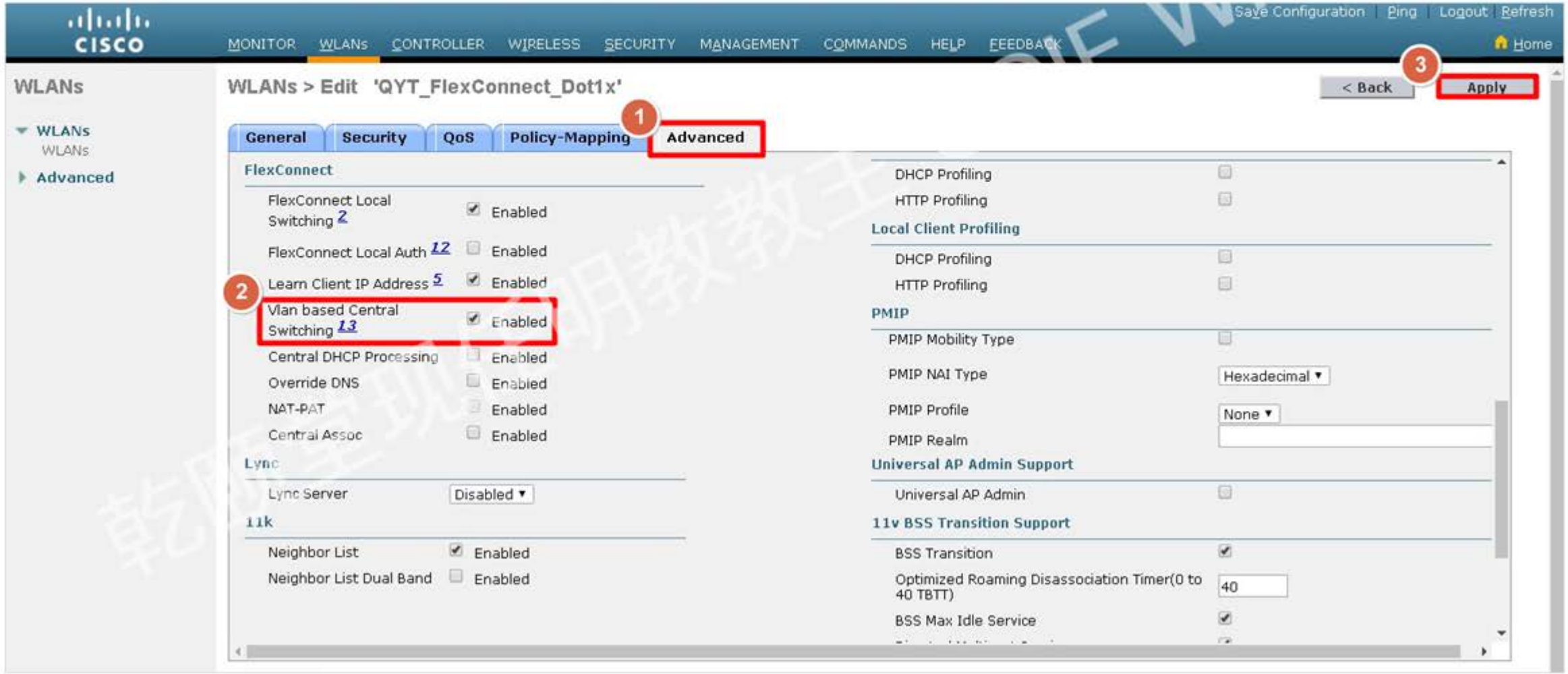


3.3 VLAN Based Central Switching

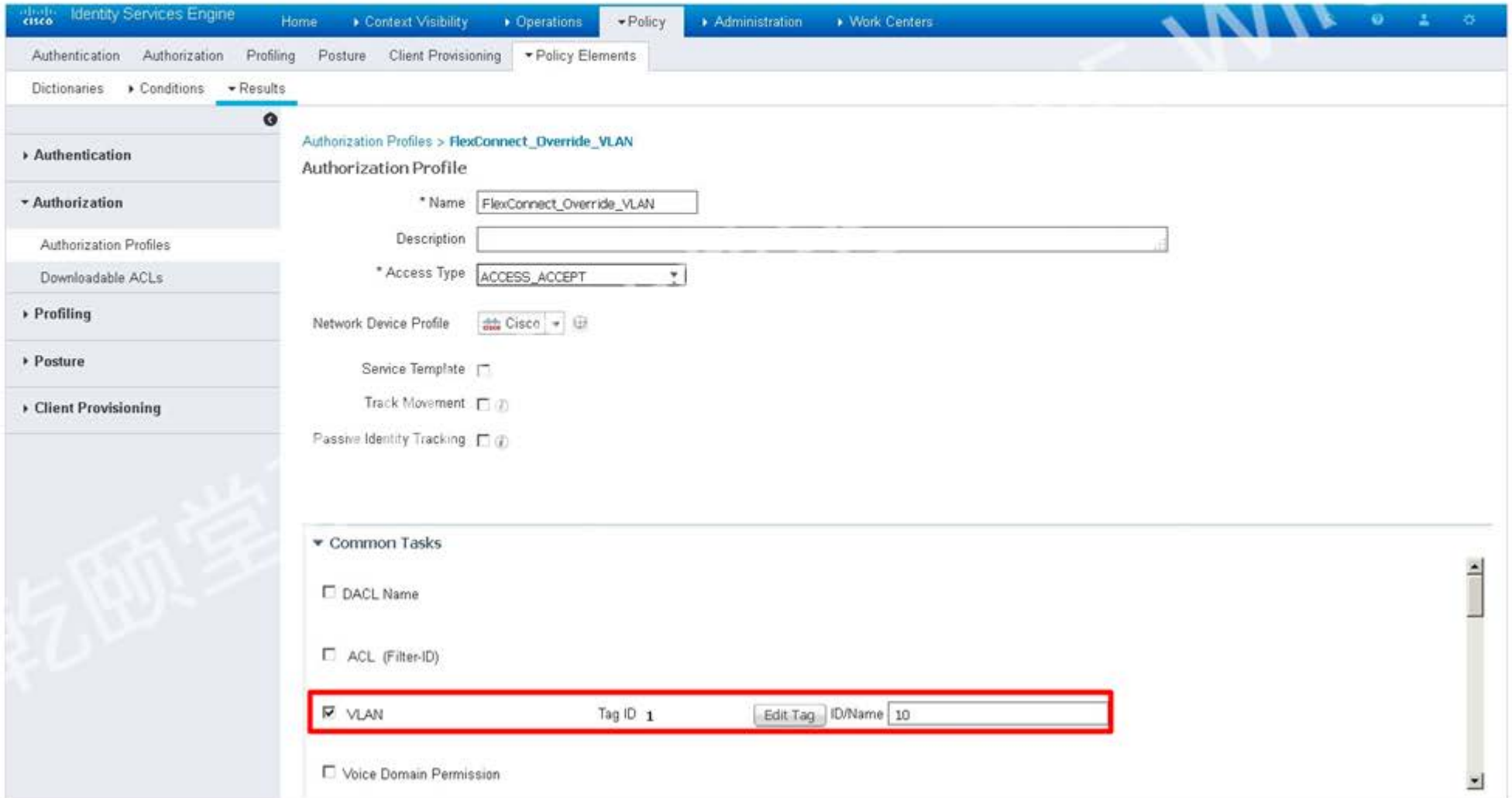
VLAN Base Central Switching 所有情况

FlexConnect模式	序号	WLC可达性	RADIUS可达性	WLC本地VLAN	AP本地VLAN	RADIUS授权VLAN	WLAN关联VLAN	实际转发VLAN	认证者	认证	转发位置
连接模式	1	√	√	10,20	20,30	10	999（deadnet）	10	WLC	中心	中心
	2	√	√	10,20	20,30	20	999（deadnet）	20	WLC	中心	本地
	3	√	√	10,20	20,30	30	999（deadnet）	30	WLC	中心	本地
	4	√	√	10,20	20,30	50	999（deadnet）	999（deadnet）	WLC	中心	中心
	5	√	√	10,20	20,30	不授权vlan	999（deadnet）	999（deadnet）	WLC	中心	本地
独立模式	6	×	√	不可用	20,30	30	999（deadnet）	30	AP	中心	本地
	7	×	√	不可用	20,30	50	999（deadnet）	999（deadnet）	AP	中心	本地
	8	×	√	不可用	20,30	不授权vlan	999（deadnet）	999（deadnet）	AP	中心	本地

开启 VLAN base Central Switching



ISE 授权 VLAN10

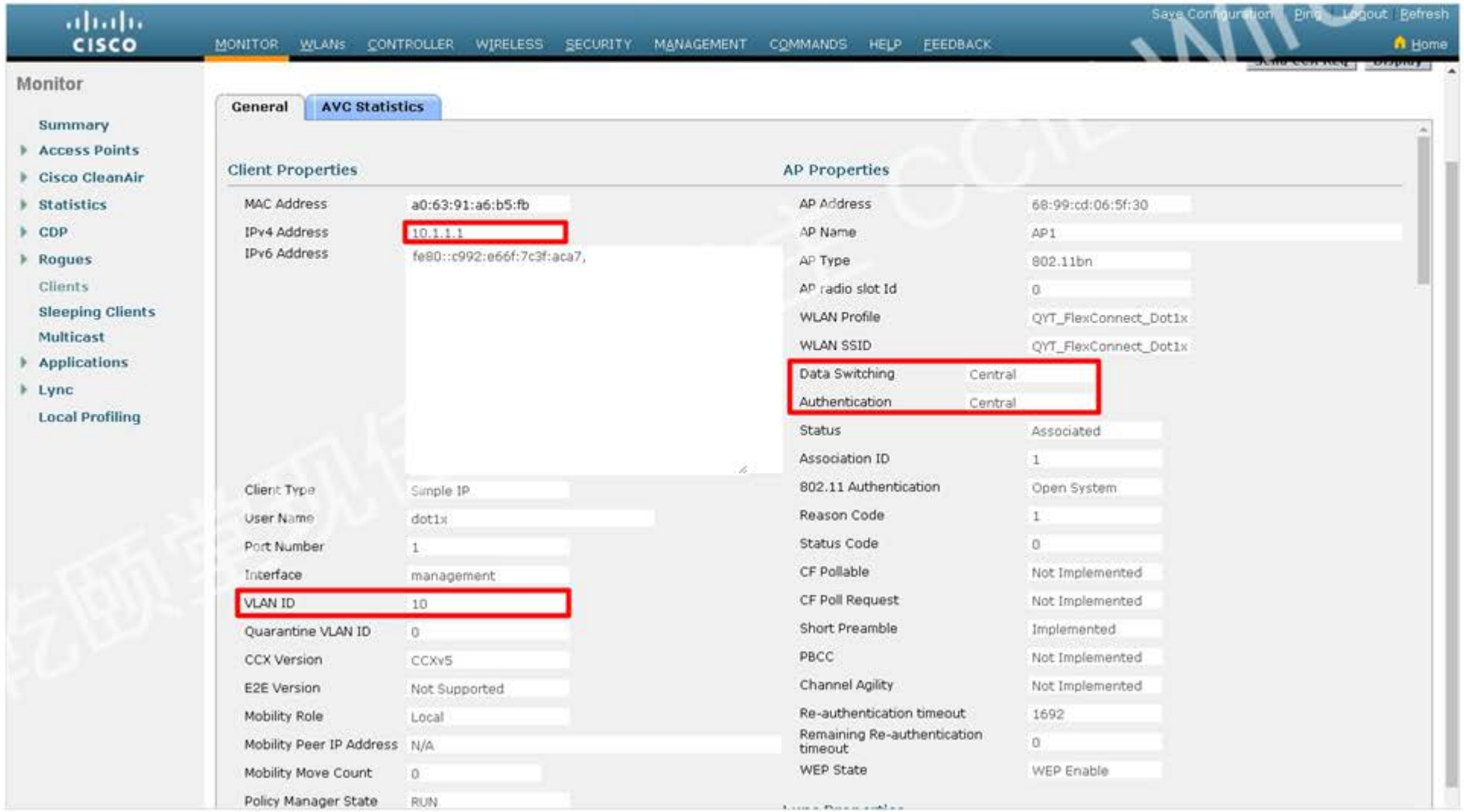


客户连接测试

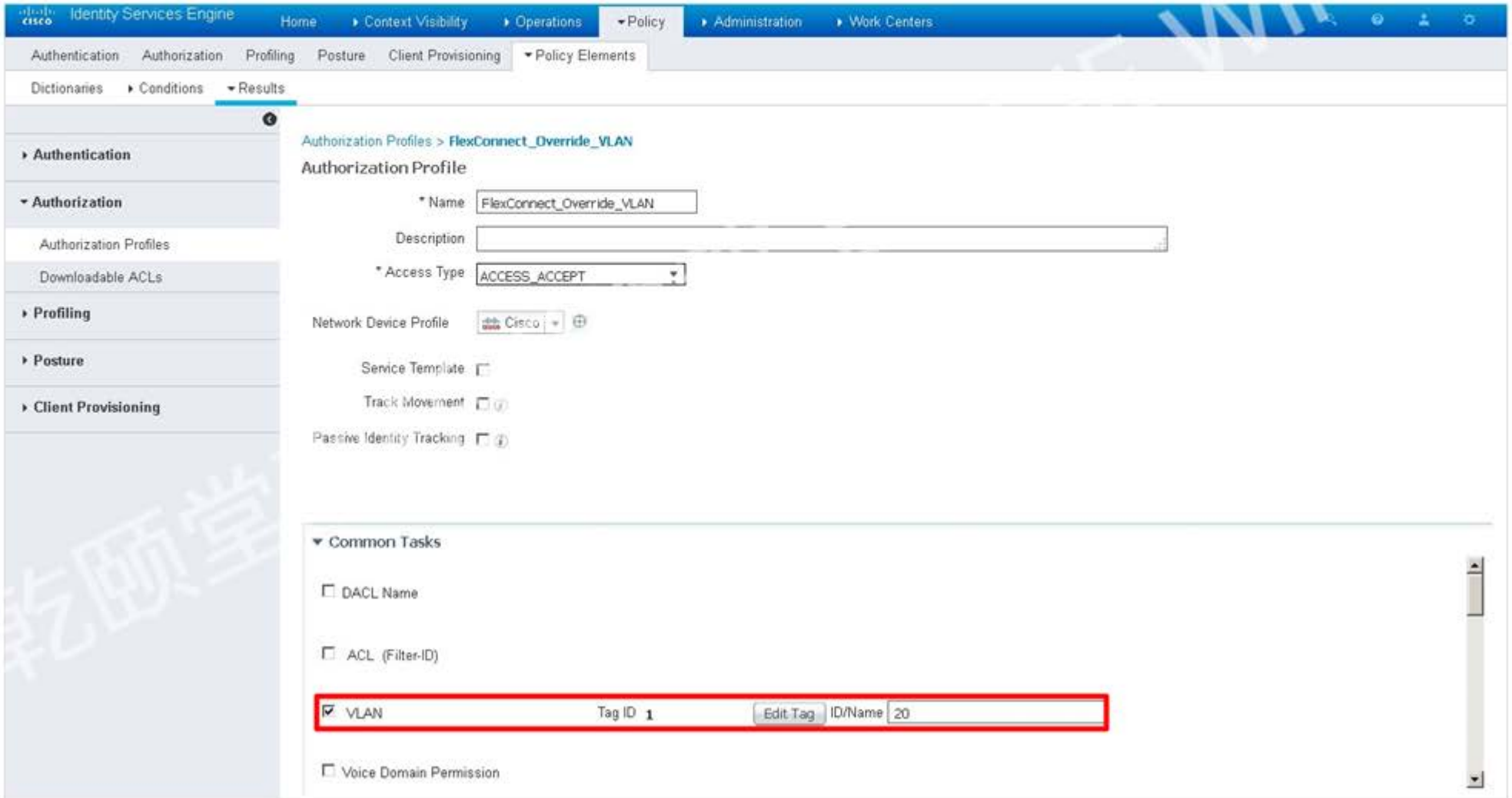

Cisco AnyConnect Secure Mobility Client
Network:
Connected (10.1.1.1)
QYT_FlexConnect_Dot1x


命令提示符
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 10.1.1.1
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 10.1.1.254
C:\>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=1ms 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=1ms 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 = 3ms, 平均 = 1ms

查看客户端信息

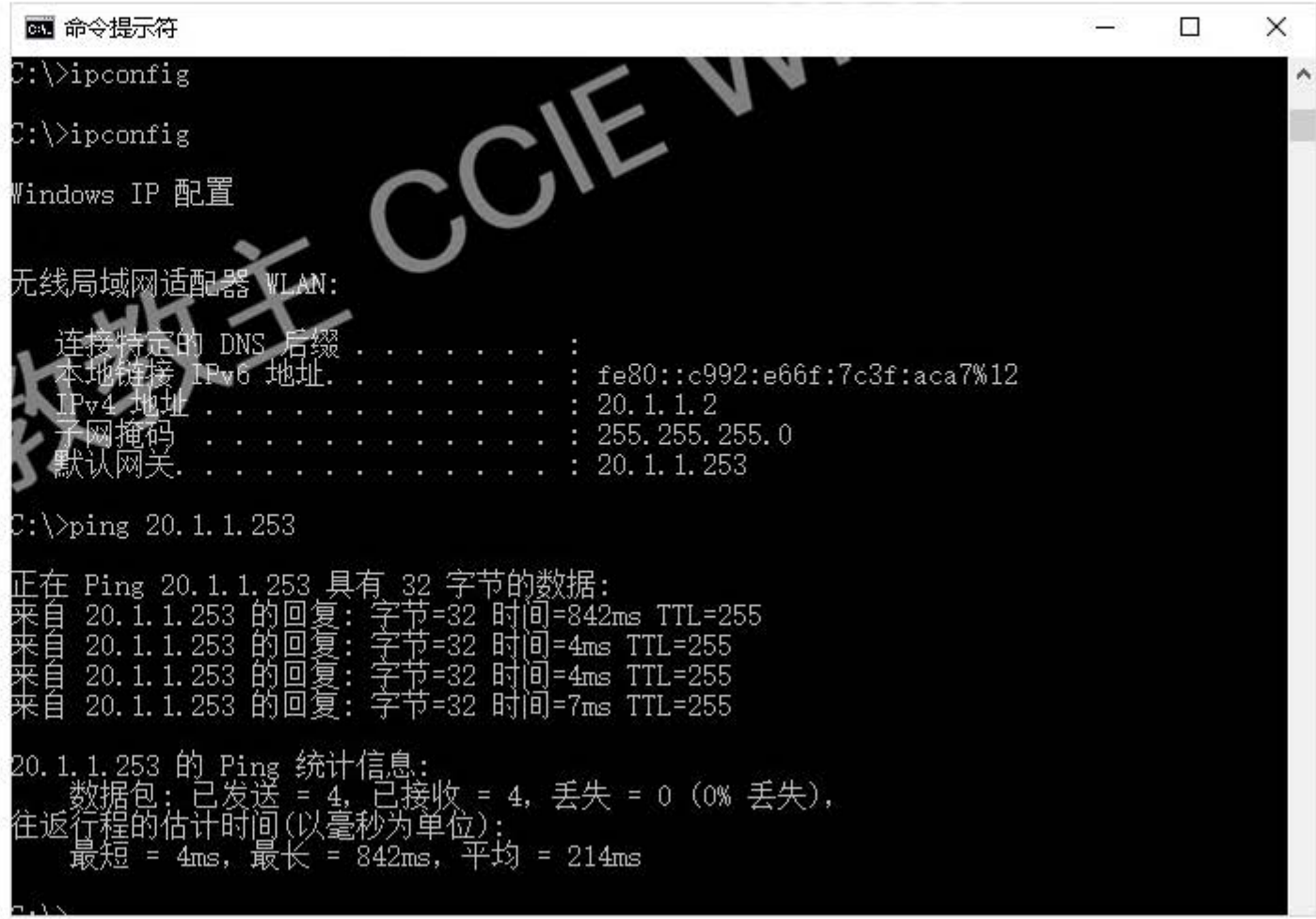

CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
General
AVC Statistics
Client Properties
MAC Address a0:63:91:a6:b5:fb
IPv4 Address 10.1.1.1
IPv6 Address fe80::c992:e66f:7c3f:aca7,
Client Type Simple IP
User Name dot1x
Port Number 1
Interface management
VLAN ID 10
Quarantine VLAN ID 0
CCX Version CCXv5
E2E Version Not Supported
Mobility Role Local
Mobility Peer IP Address N/A
Mobility Move Count 0
Policy Manager State RUN
AP Properties
AP Address 68:99:cd:06:5f:30
AP Name AP1
AP Type 802.11bn
AP radio slot Id 0
WLAN Profile QYT_FlexConnect_Dot1x
WLAN SSID QYT_FlexConnect_Dot1x
Data Switching Central
Authentication Central
Status Associated
Association ID 1
802.11 Authentication Open System
Reason Code 1
Status Code 0
CF Pollable Not Implemented
CF Poll Request Not Implemented
Short Preamble Implemented
PBCC Not Implemented
Channel Agility Not Implemented
Re-authentication timeout 1692
Remaining Re-authentication timeout 0
WEP State WEP Enable

ISE 授权 VLAN20

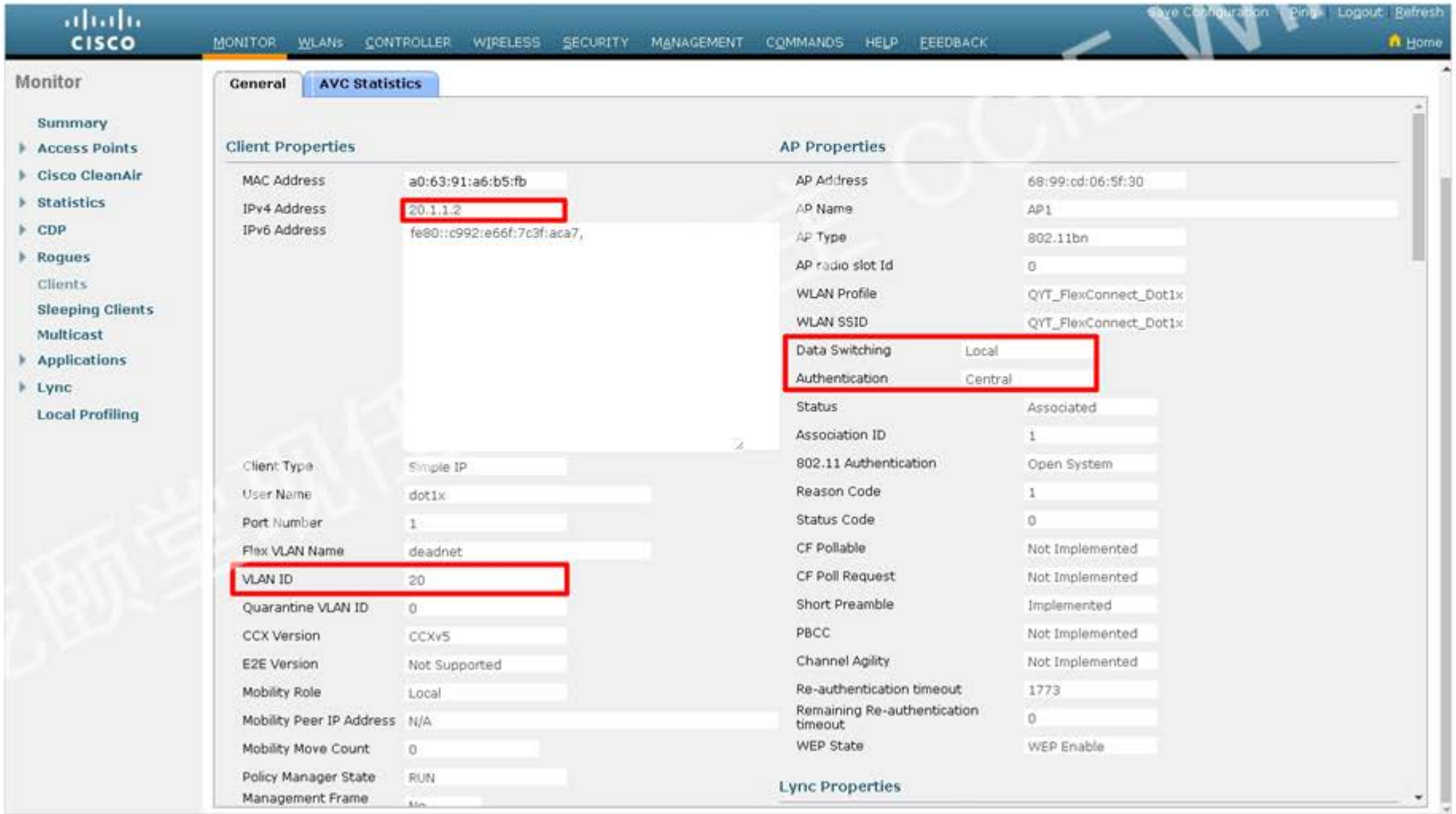


客户连接测试

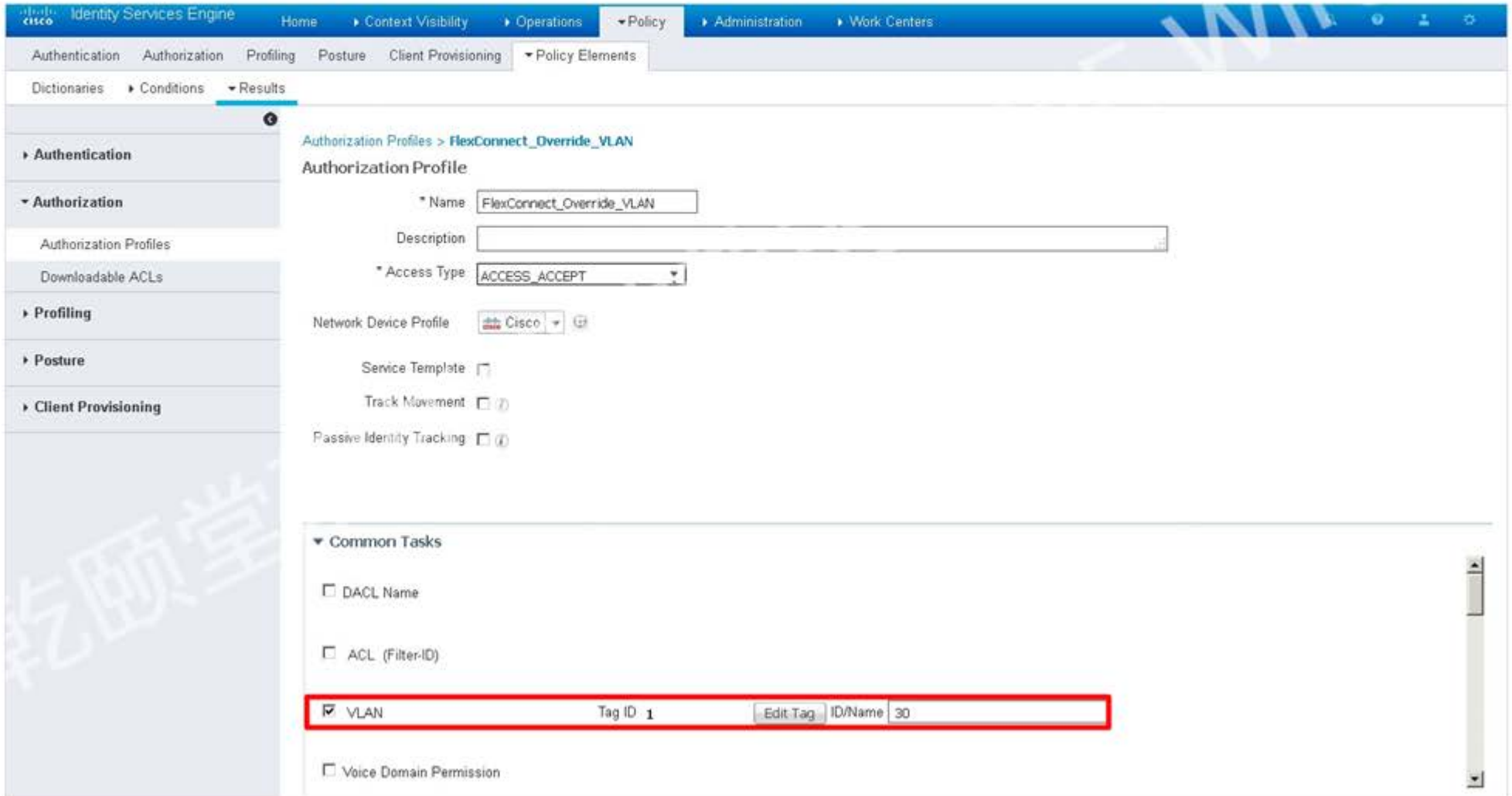

Cisco AnyConnect Secure Mobility Client
Network:
Connected (20.1.1.2)
QYT_FlexConnect_Dot1x


命令提示符
C:\>ipconfig
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 20.1.1.2
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 20.1.1.253
C:\>ping 20.1.1.253
正在 Ping 20.1.1.253 具有 32 字节的数据:
来自 20.1.1.253 的回复: 字节=32 时间=842ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=4ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=4ms TTL=255
来自 20.1.1.253 的回复: 字节=32 时间=7ms TTL=255
20.1.1.253 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 = 4ms, 最长 = 842ms, 平均 = 214ms

查看客户端信息


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
General
AVC Statistics
Client Properties
MAC Address a0:63:91:a6:b5:fb
IPv4 Address 20.1.1.2
IPv6 Address fe80::c992:e66f:7c3f:aca7,
Client Type Simple IP
User Name dot1x
Port Number 1
Flex VLAN Name deadnet
VLAN ID 20
Quarantine VLAN ID 0
CCX Version CCXv5
E2E Version Not Supported
Mobility Role Local
Mobility Peer IP Address N/A
Mobility Move Count 0
Policy Manager State RUN
Management Frame
AP Properties
AP Address 68:99:cd:06:5f:30
AP Name AP1
AP Type 802.11bn
AP radio slot Id 0
WLAN Profile QYT_FlexConnect_Dot1x
WLAN SSID QYT_FlexConnect_Dot1x
Data Switching Local
Authentication Central
Status Associated
Association ID 1
802.11 Authentication Open System
Reason Code 1
Status Code 0
CF Pollable Not Implemented
CF Poll Request Not Implemented
Short Preamble Implemented
PBCC Not Implemented
Channel Agility Not Implemented
Re-authentication timeout 1773
Remaining Re-authentication timeout 0
WEP State WEP Enable
Lync Properties

ISE 授权 VLAN30

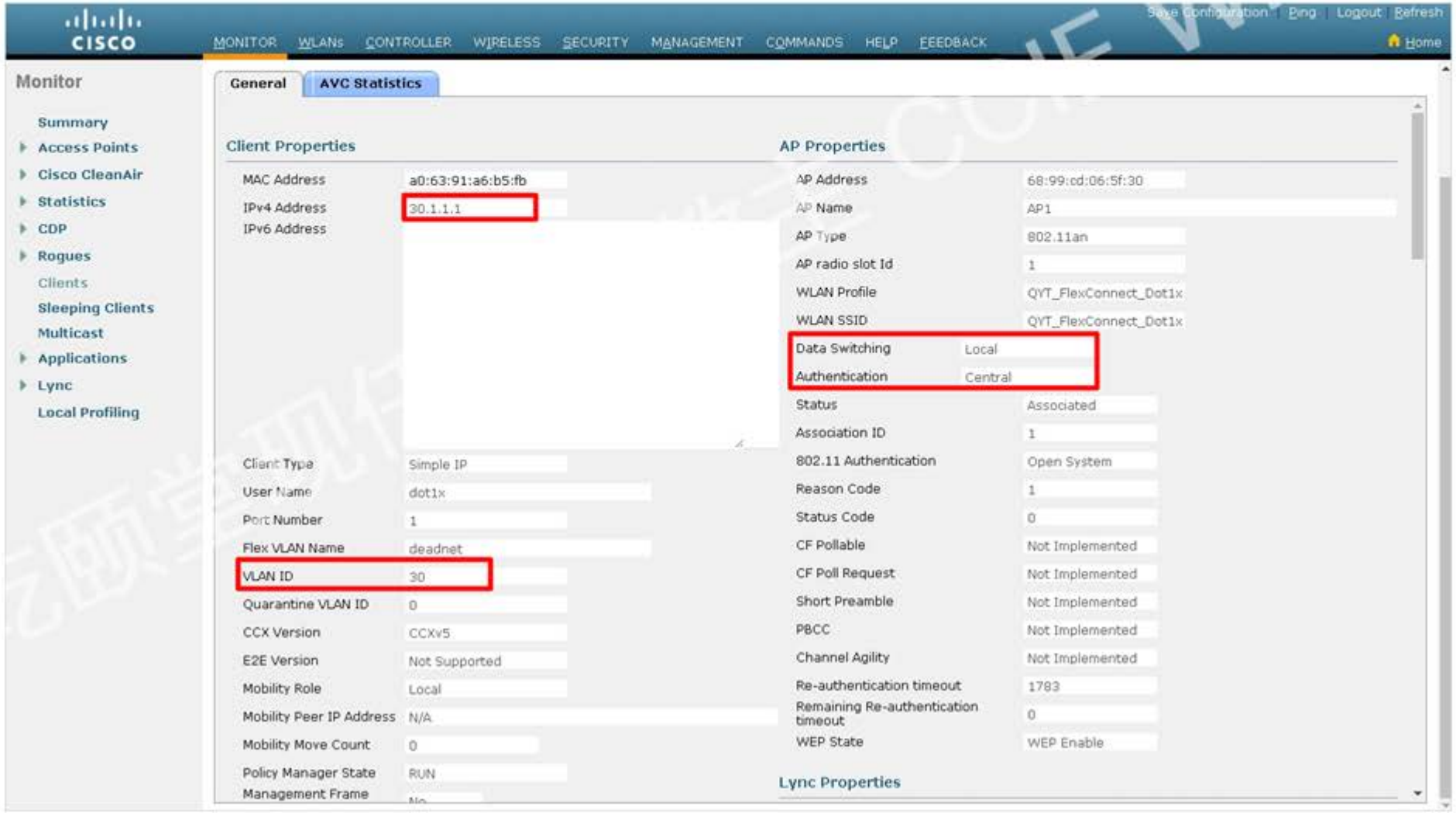


客户连接测试

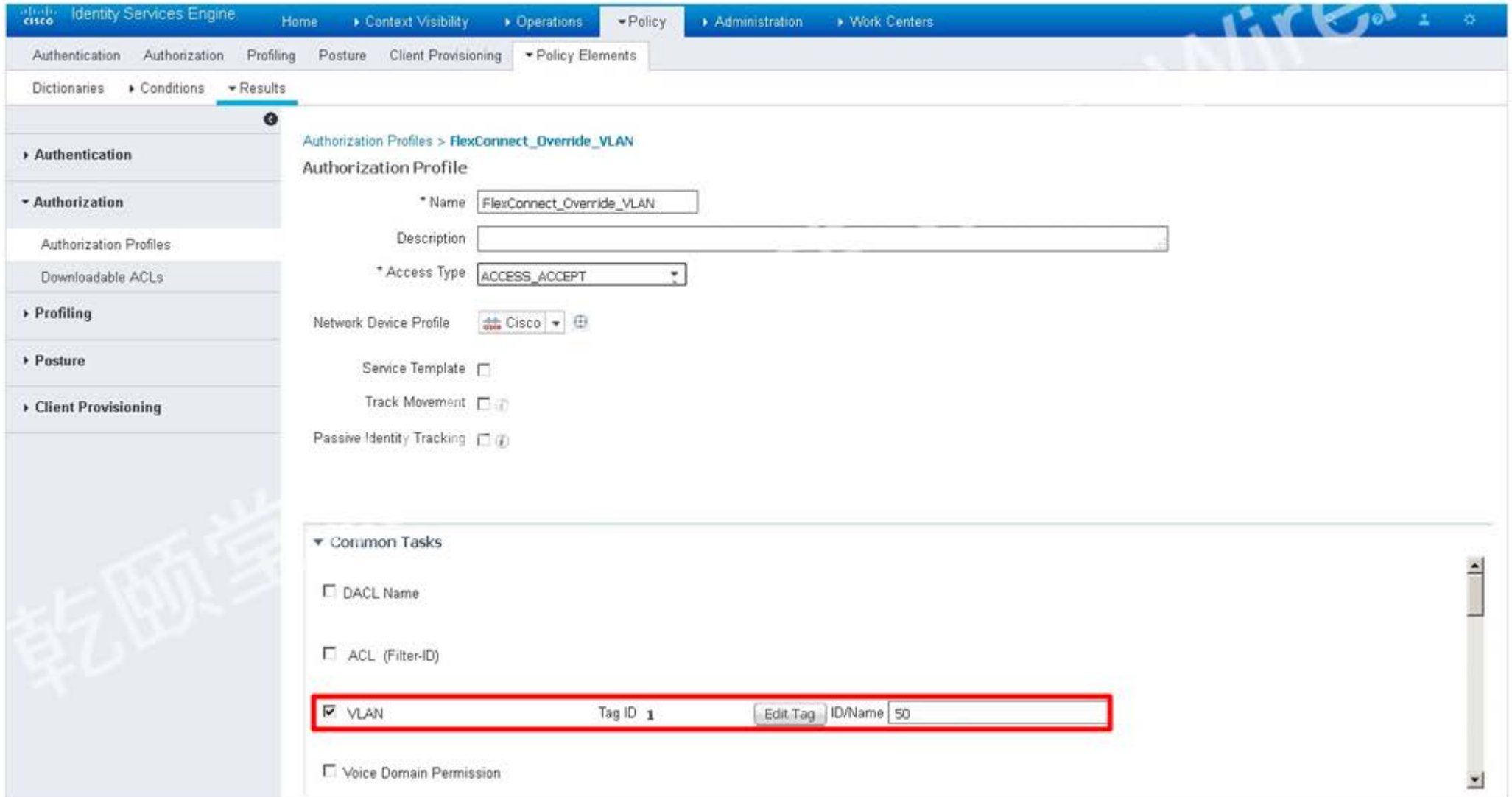

Cisco AnyConnect Secure Mobility Client
Network:
Connected (30.1.1.1)
QYT_FlexConnect_Dot1x


命令提示符
C:\>ipconfig
Windows IP 配置
无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::c992:e66f:7c3f:aca7%12
IPv4 地址 . . . . . : 30.1.1.1
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 30.1.1.253
C:\>ping 30.1.1.253
正在 Ping 30.1.1.253 具有 32 字节的数据:
来自 30.1.1.253 的回复: 字节=32 时间=4ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=4ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=24ms TTL=255
来自 30.1.1.253 的回复: 字节=32 时间=3ms TTL=255
30.1.1.253 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 = 3ms, 最长 = 24ms, 平均 = 8ms
C:\>

查看客户端信息


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
General
AVC Statistics
Client Properties
MAC Address a0:63:91:a6:b5:fb
IPv4 Address 30.1.1.1
IPv6 Address
Client Type Simple IP
User Name dot1x
Port Number 1
Flex VLAN Name deadnet
VLAN ID 30
Quarantine VLAN ID 0
CCX Version CCXv5
E2E Version Not Supported
Mobility Role Local
Mobility Peer IP Address N/A
Mobility Move Count 0
Policy Manager State RUN
Management Frame
AP Properties
AP Address 68:99:cd:06:5f:30
AP Name AP1
AP Type 802.11an
AP radio slot Id 1
WLAN Profile QYT_FlexConnect_Dot1x
WLAN SSID QYT_FlexConnect_Dot1x
Data Switching Local
Authentication Central
Status Associated
Association ID 1
802.11 Authentication Open System
Reason Code 1
Status Code 0
CF Pollable Not Implemented
CF Poll Request Not Implemented
Short Preamble Not Implemented
PBCC Not Implemented
Channel Agility Not Implemented
Re-authentication timeout 1783
Remaining Re-authentication timeout 0
WEP State WEP Enable
Lync Properties

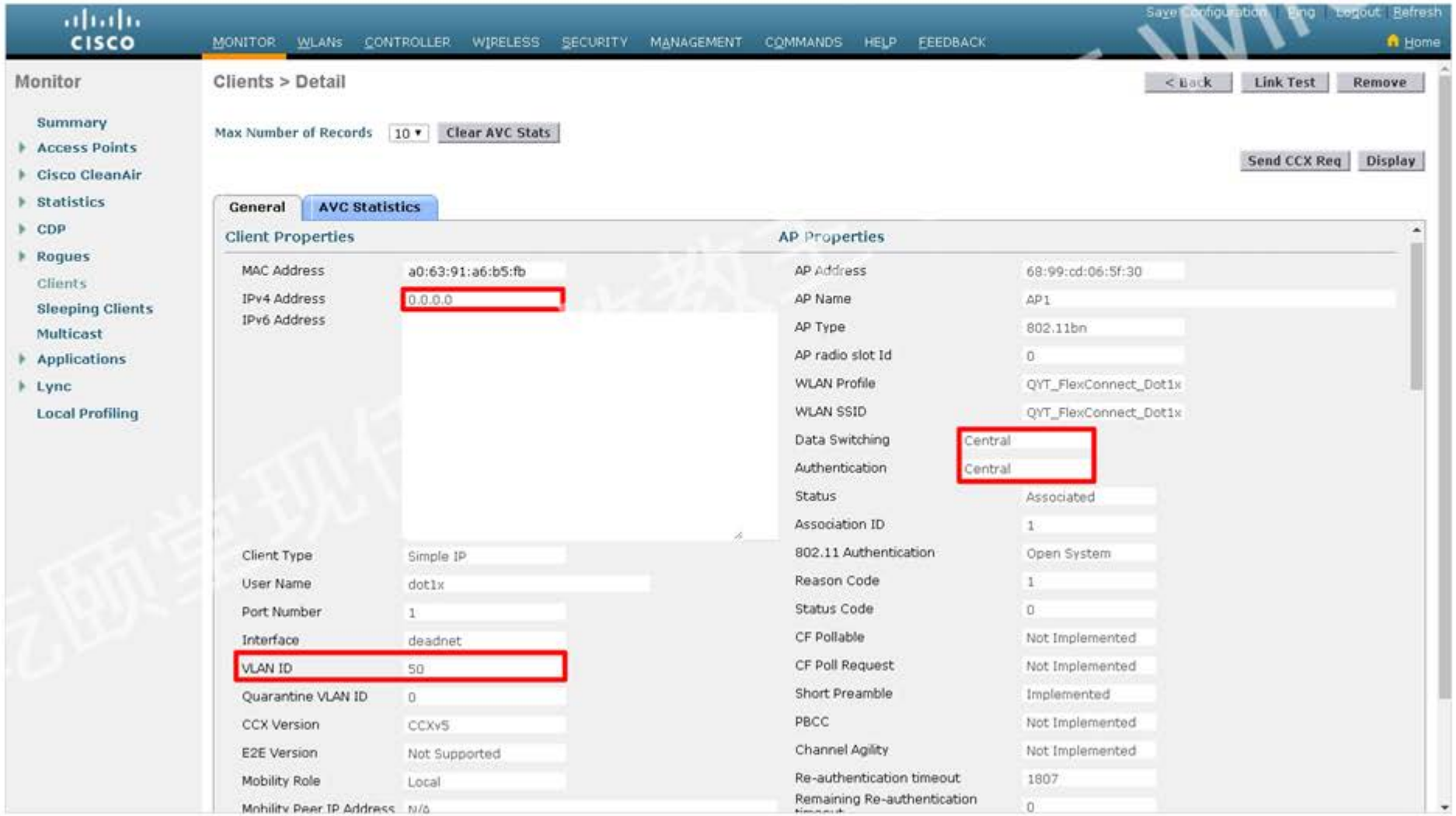
ISE 授权 VLAN50



客户连接测试


Cisco AnyConnect Secure Mobility Client
Network:
Limited or no connectivity
QYT_FlexConnect_Dot1x

查看客户端信息

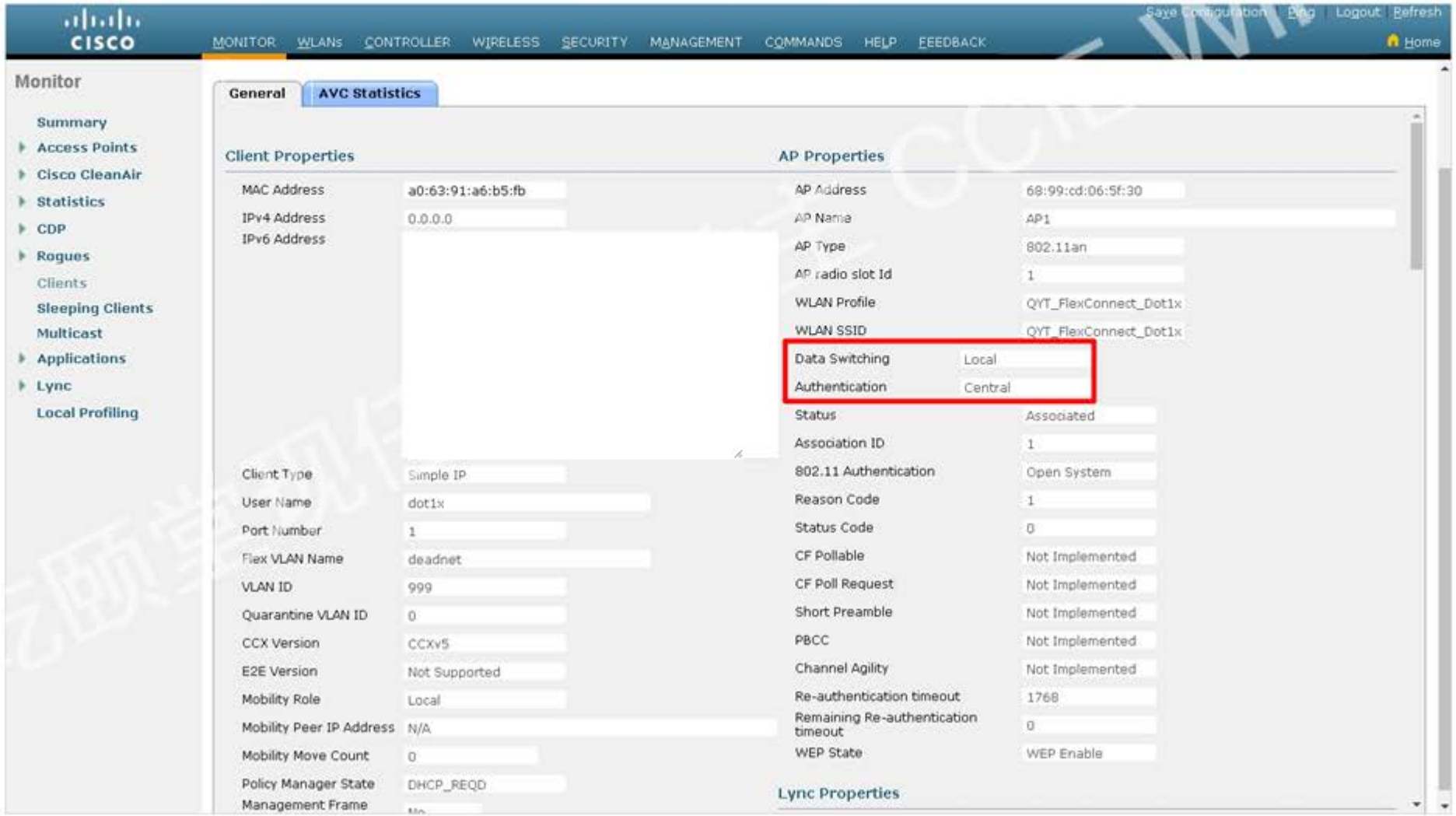

CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
Clients > Detail
< Back
Link Test
Remove
Max Number of Records
10
Clear AVC Stats
Send CCX Req
Display
General
AVC Statistics
Client Properties
MAC Address a0:63:91:a6:b5:fb
IPv4 Address 0.0.0.0
IPv6 Address
Client Type Simple IP
User Name dot1x
Port Number 1
Interface deadnet
VLAN ID 50
Quarantine VLAN ID 0
CCX Version CCXv5
E2E Version Not Supported
Mobility Role Local
Mobility Peer IP Address N/A
AP Properties
AP Address 68:99:cd:06:5f:30
AP Name AP1
AP Type 802.11bn
AP radio slot Id 0
WLAN Profile QYT_FlexConnect_Dot1x
WLAN SSID QYT_FlexConnect_Dot1x
Data Switching Central
Authentication Central
Status Associated
Association ID 1
802.11 Authentication Open System
Reason Code 1
Status Code 0
CF Pollable Not Implemented
CF Poll Request Not Implemented
Short Preamble Implemented
PBCC Not Implemented
Channel Agility Not Implemented
Re-authentication timeout 1807
Remaining Re-authentication 0

ISE 不授权 VLAN

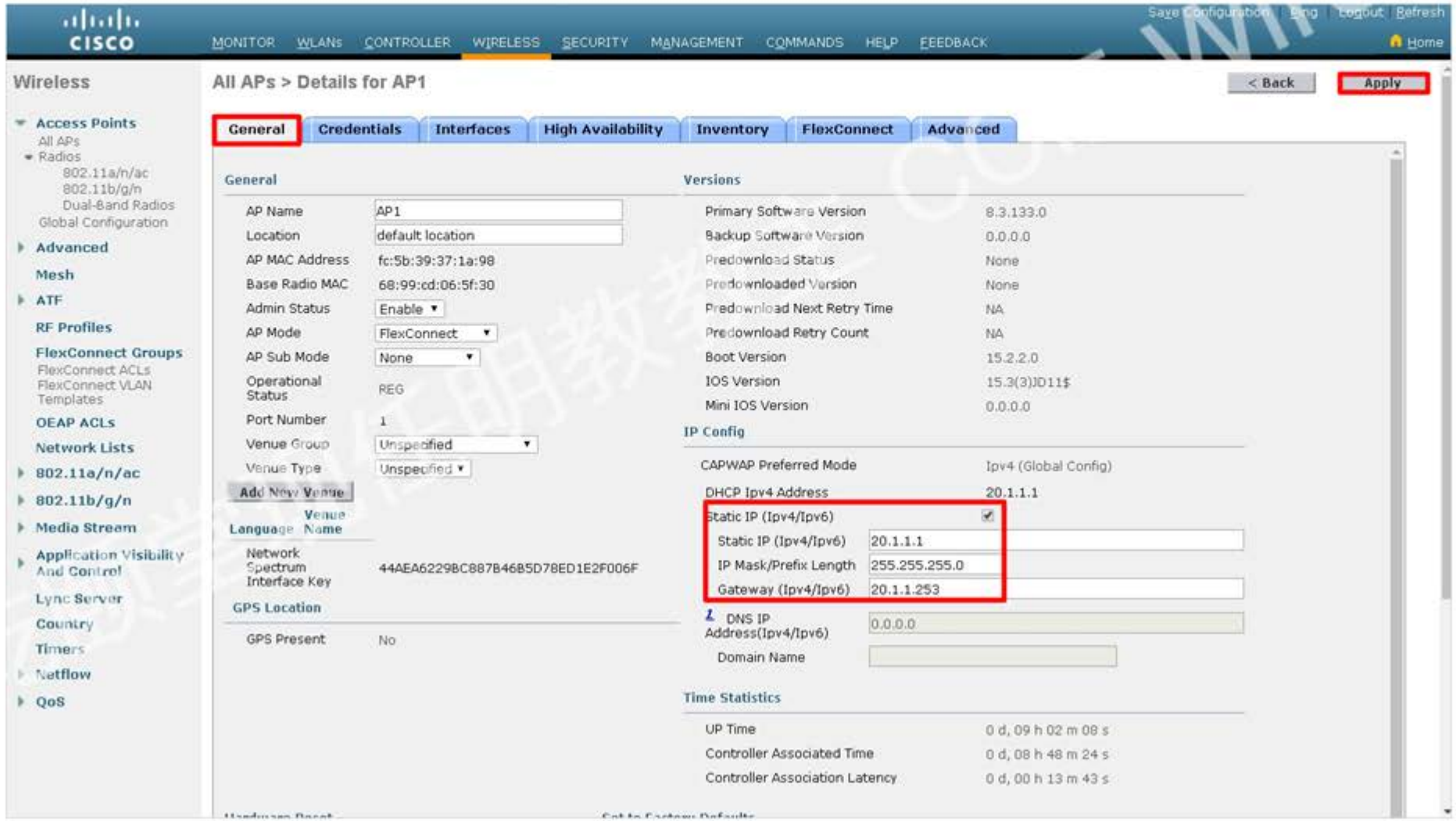
客户连接测试


Cisco AnyConnect Secure Mobility Client
Network:
Limited or no connectivity
QYT_FlexConnect_Dot1x

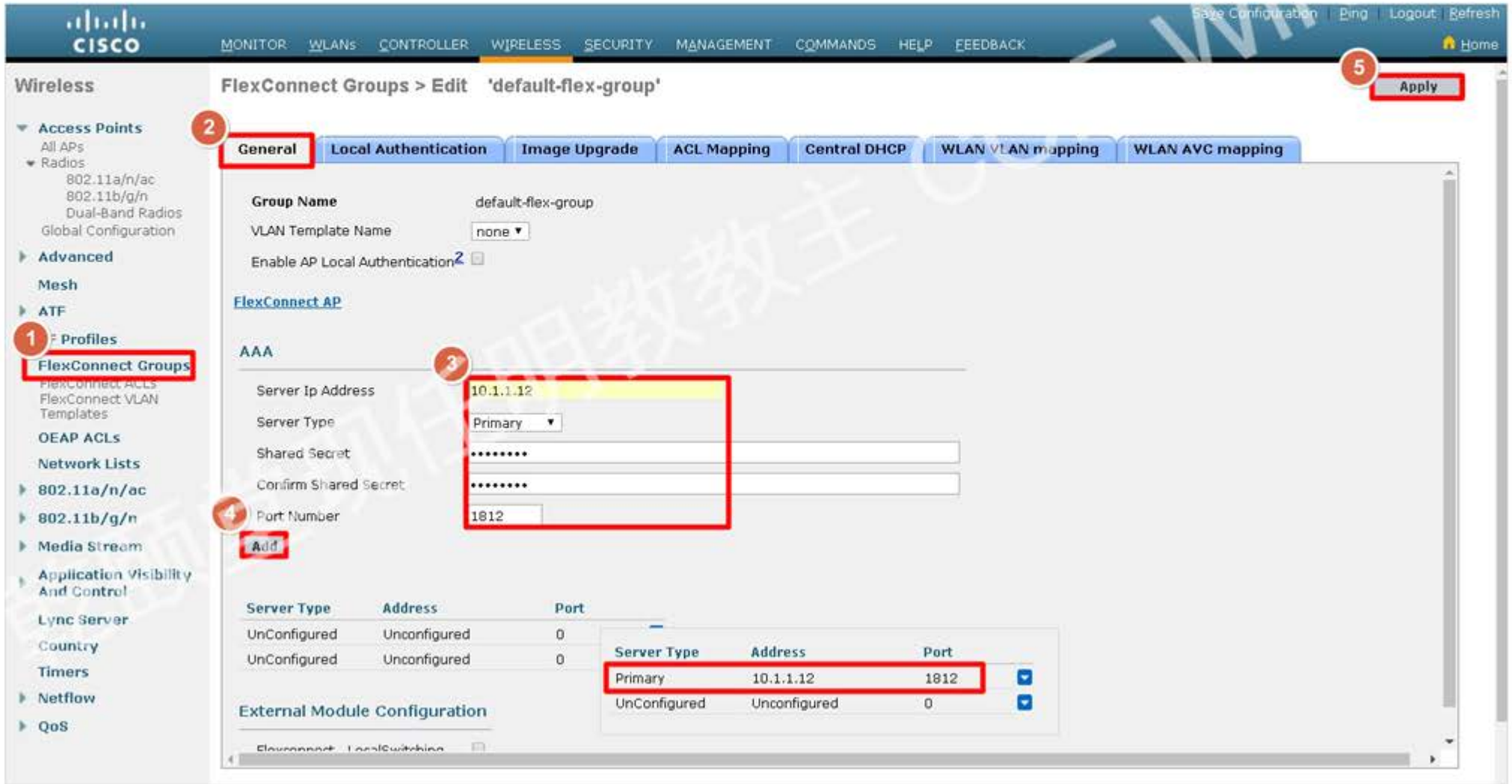
查看客户端信息


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
General
AVC Statistics
Client Properties
MAC Address a0:63:91:a6:b5:fb
IPv4 Address 0.0.0.0
IPv6 Address
Client Type Simple IP
User Name dot1x
Port Number 1
Flex VLAN Name deadnet
VLAN ID 999
Quarantine VLAN ID 0
CCX Version CCXv5
E2E Version Not Supported
Mobility Role Local
Mobility Peer IP Address N/A
Mobility Move Count 0
Policy Manager State DHCP_REQD
Management Frame
AP Properties
AP Address 68:99:cd:06:5f:30
AP Name AP1
AP Type 802.11an
AP radio slot Id 1
WLAN Profile QYT_FlexConnect_Dot1x
WLAN SSID QYT_FlexConnect_Dot1x
Data Switching Local
Authentication Central
Status Associated
Association ID 1
802.11 Authentication Open System
Reason Code 1
Status Code 0
CF Pollable Not Implemented
CF Poll Request Not Implemented
Short Preamble Not Implemented
PBCC Not Implemented
Channel Agility Not Implemented
Re-authentication timeout 1768
Remaining Re-authentication timeout 0
WEP State WEP Enable
Lync Properties

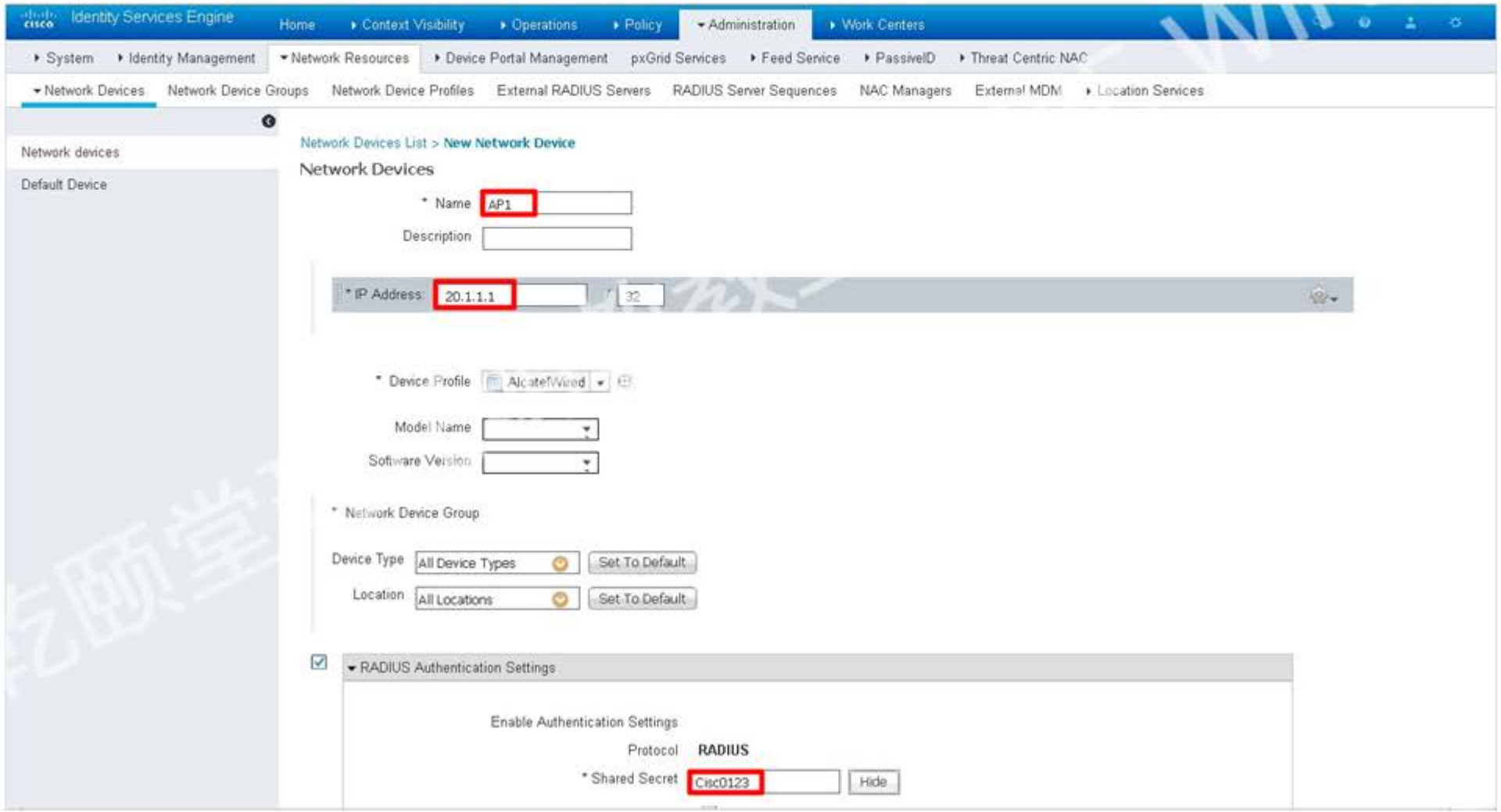
AP 修改静态地址


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
Wireless
All APs > Details for AP1
< Back
Apply
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
ATF
RF Profiles
FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates
OEAP ACLs
Network Lists
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Lync Server
Country
Timers
Netflow
QoS
General
Credentials
Interfaces
High Availability
Inventory
FlexConnect
Advanced
General
AP Name AP1
Location default location
AP MAC Address fc:5b:39:37:1a:98
Base Radio MAC 68:99:cd:06:5f:30
Admin Status Enable
AP Mode FlexConnect
AP Sub Mode None
Operational Status REG
Port Number 1
Venue Group Unspecified
Venue Type Unspecified
Add New Venue
Venue Language Name
Network Spectrum Interface Key 44AEA6229BC887B46B5D78ED1E2F006F
GPS Location
GPS Present No
Versions
Primary Software Version 8.3.133.0
Backup Software Version 0.0.0.0
Predownload Status None
Predownloaded Version None
Predownload Next Retry Time NA
Predownload Retry Count NA
Boot Version 15.2.2.0
IOS Version 15.3(3)JD11$
Mini IOS Version 0.0.0.0
IP Config
CAPWAP Preferred Mode Ipv4 (Global Config)
DHCP Ipv4 Address 20.1.1.1
Static IP (Ipv4/Ipv6)
Static IP (Ipv4/Ipv6) 20.1.1.1
IP Mask/Prefix Length 255.255.255.0
Gateway (Ipv4/Ipv6) 20.1.1.253
DNS IP Address(Ipv4/Ipv6) 0.0.0.0
Domain Name
Time Statistics
UP Time 0 d, 09 h 02 m 08 s
Controller Associated Time 0 d, 08 h 48 m 24 s
Controller Association Latency 0 d, 00 h 13 m 43 s

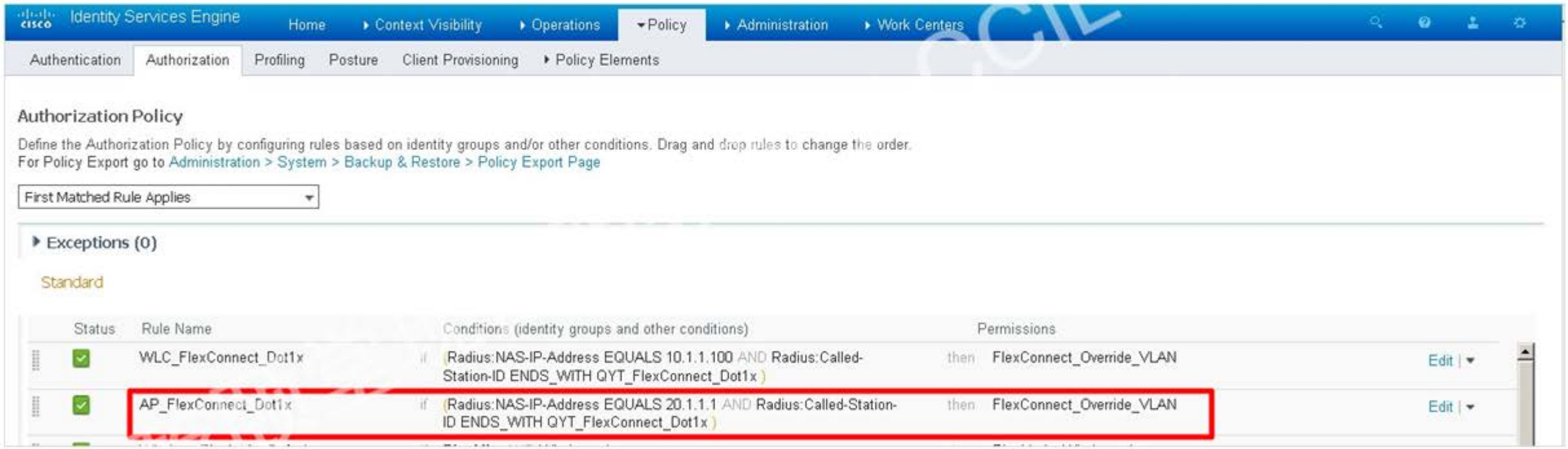
AP 指定主用 Raidus 服务器



ISE 为 AP 添加 Network Device



ISE 为 AP 添加授权策略

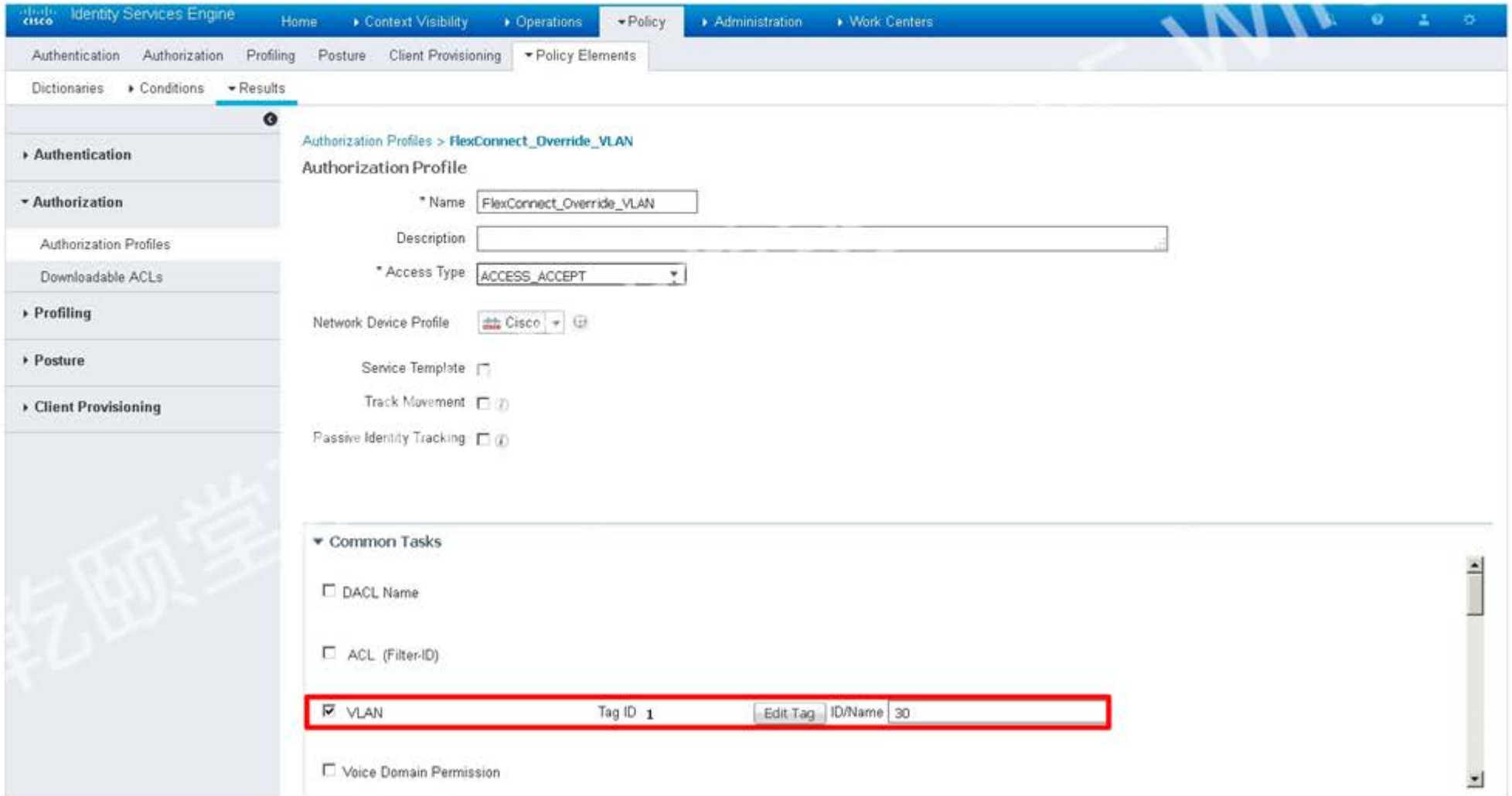


断开 WLC，让 AP 进入独立模式

```
SW3560(config)#interface g0/1
SW3560(config-if)#shutdown
```

```
*Dec 18 01:08:02.447: %EVT-4-WRN: Write of flash:/event.capwap done
*Dec 18 01:08:02.463: %LWAPP-3-CLIENTERRORLOG: Switching to Standalone mode
*Dec 18 01:08:02.479: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 10.1.1.100:5246
*Dec 18 01:08:02.855: %WIDS-6-DISABLED: IDS Signature is removed and disabled.
Not in Bound state.
*Dec 18 01:11:08.365: %CAPWAP-3-DHCP_RENEW: Could not discover WLC. Either IP address is not assigned or assigned
IP is wrong. Renewing DHCP IP.
*Dec 18 01:11:13.377: %LWAPP-3-LWAPP_INTERFACE_GOT_IP_ADDRESS: Interface BVI1 obtained IP from DHCP...
*Dec 18 01:11:13.489: %DHCP-6-ADDRESS_ASSIGN: Interface BVI1 assigned DHCP address 20.1.1.4, mask 255.255.255.0,
hostname AP1
*Dec 18 01:11:13.489: %LWAPP-3-LWAPP_INTERFACE_GOT_IP_ADDRESS: Interface BVI1 obtained IP from DHCP...
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)
*Dec 18 01:11:19.369: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.1.1.100 obtained through DHCP


AP1#sh ip int b
Interface                  IP-Address      OK? Method Status                Protocol
BVI1                       20.1.1.4        YES DHCP   up                    up
```

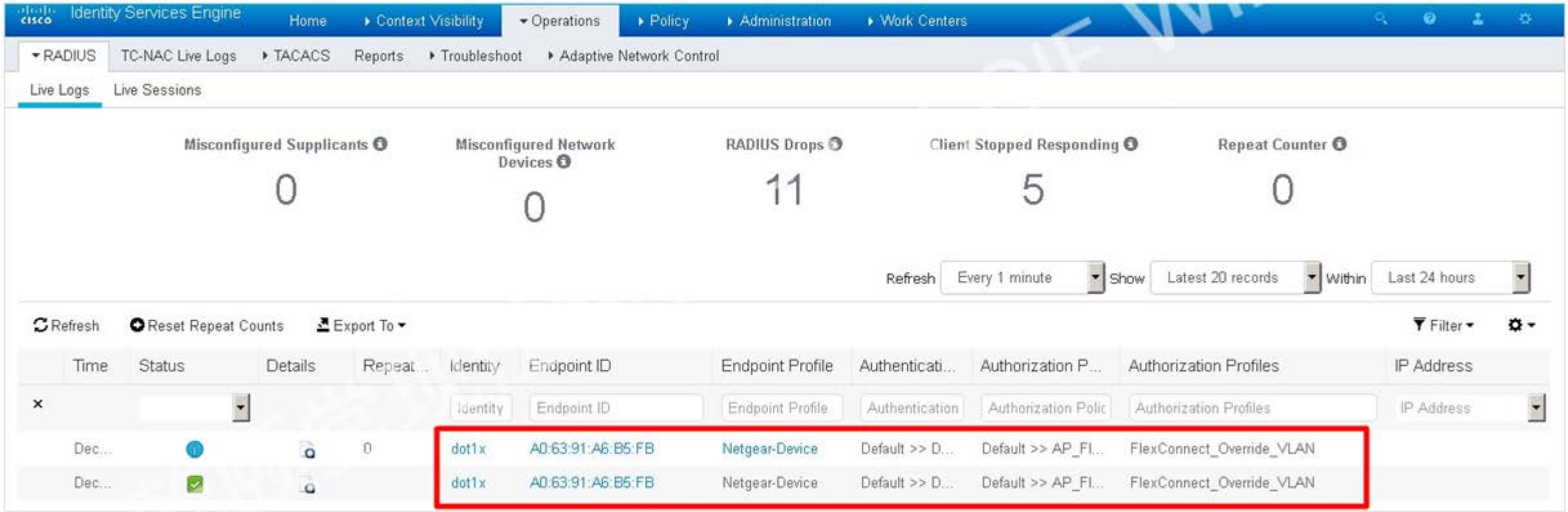
ISE 授权 VLAN30



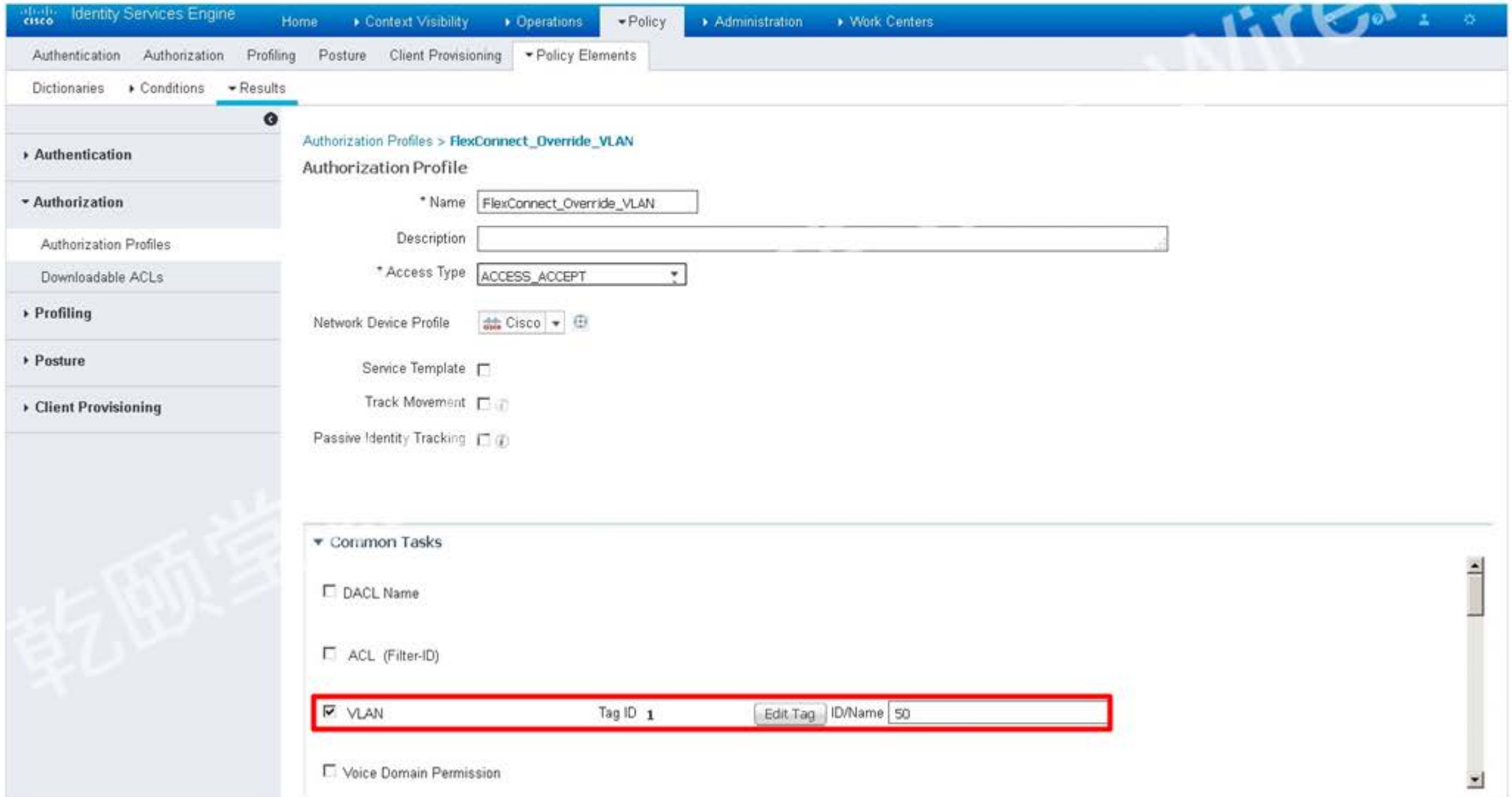
客户连接测试

```
*Dec  6 07:25:36.858: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.1.1.12:1812,1000 is being marked alive.
*Dec  6 07:25:36.858: %RADIUS-6-SERVERALIVE: Group radius: Radius server 10.1.1.12:1812,1000 is
responding again (previously dead).
```

查看 ISE 认证日志


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
RADIUS
TC-NAC Live Logs
TACACS
Reports
Troubleshoot
Adaptive Network Control
Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
11
Client Stopped Responding
5
Repeat Counter
0
Refresh
Every 1 minute
Show
Latest 20 records
Within
Last 24 hours
Refresh
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repeat...
Identity
Endpoint ID
Endpoint Profile
Authenticati...
Authorization P...
Authorization Profiles
IP Address
Identity
Endpoint ID
Endpoint Profile
Authentication
Authorization Polic
Authorization Profiles
IP Address
Dec...
0
dot1x
A0:63:91:A6:B5:FB
Netgear-Device
Default >> D...
Default >> AP_FI...
FlexConnect_Override_VLAN
Dec...
dot1x
A0:63:91:A6:B5:FB
Netgear-Device
Default >> D...
Default >> AP_FI...
FlexConnect_Override_VLAN

ISE 授权 VLAN50



客户连接测试


Cisco AnyConnect Secure Mobility Client
Network:
Limited or no connectivity
QYT_FlexConnect_Dot1x


Cisco AnyConnect Secure Mobility Client
Network:
Acquiring IP Address
QYT_FlexConnect_Dot1x

ISE 不授权 VLAN

客户连接测试


Cisco AnyConnect Secure Mobility Client
Network:
Limited or no connectivity
QYT_FlexConnect_Dot1x


Cisco AnyConnect Secure Mobility Client
Network:
Acquiring IP Address
QYT_FlexConnect_Dot1x

test

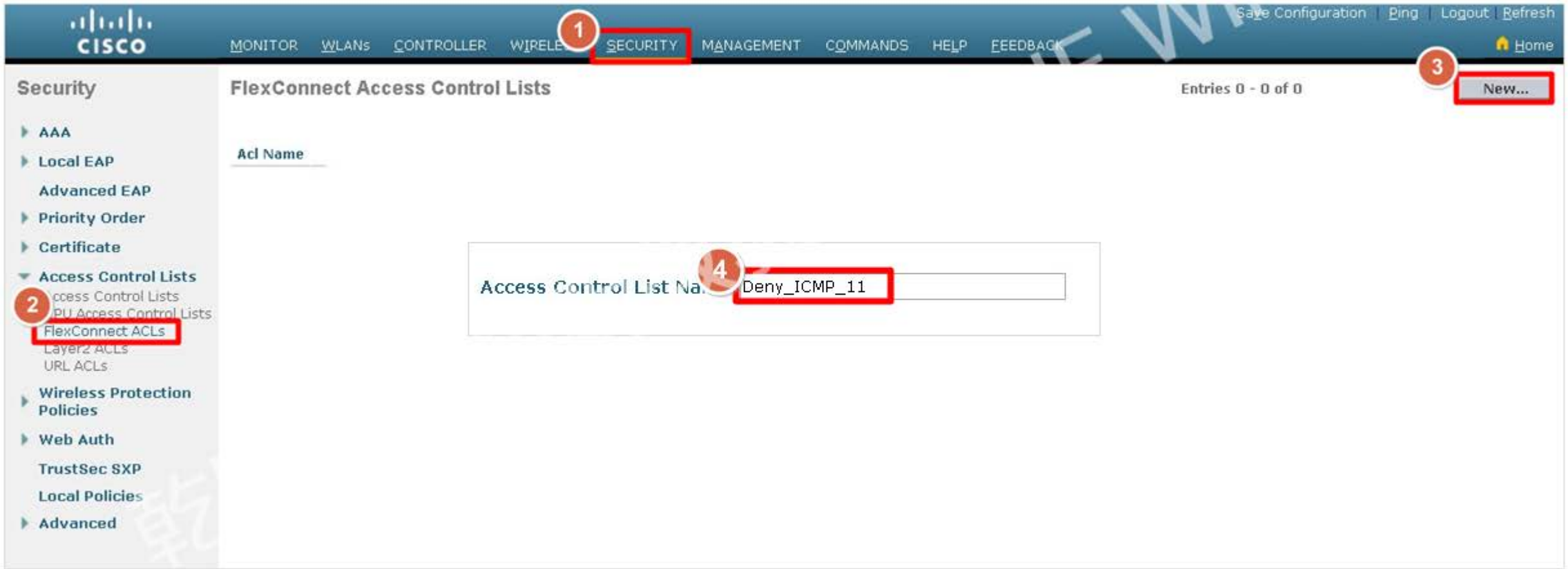
```
SW3560(config-if)#no shutdown
```

```
*Dec  6 07:32:01.955: AP has SHA2 MIC certificate - Using SHA2 MIC certificate for DTLS.

*Dec 18 01:34:38.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.1.1.100 peer_port: 5246
*Dec 18 01:34:38.323: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 10.1.1.100 peer_port:
5246
*Dec 18 01:34:38.323: %CAPWAP-5-SENDJOIN: sending Join Request to 10.1.1.100
*Dec 18 01:34:39.983: %LWAPP-4-CLIENTEVENTLOG: OfficeExtend Localssid saved in AP flash
*Dec 18 01:34:40.543: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller WLC-5508-1WLAN id 1, SSID
QYT_FlexConnect_PSK, L2ACL , L2ACL AP
WLAN id 2, SSID QYT_FlexConnect_Dot1x, L2ACL , L2ACL AP

*Dec 18 01:34:40.679: %LWAPP-3-CLIENTERRORLOG: Switching to Connected modecapwap_delete_all_l2Acls_in_nacl_list:336.
Deleting all L2Acls in AP config

*Dec 18 01:34:42.303: %WIDS-6-ENABLED: IDS Signature is loaded and enabled
*Dec 18 01:34:44.271: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
```

3.4

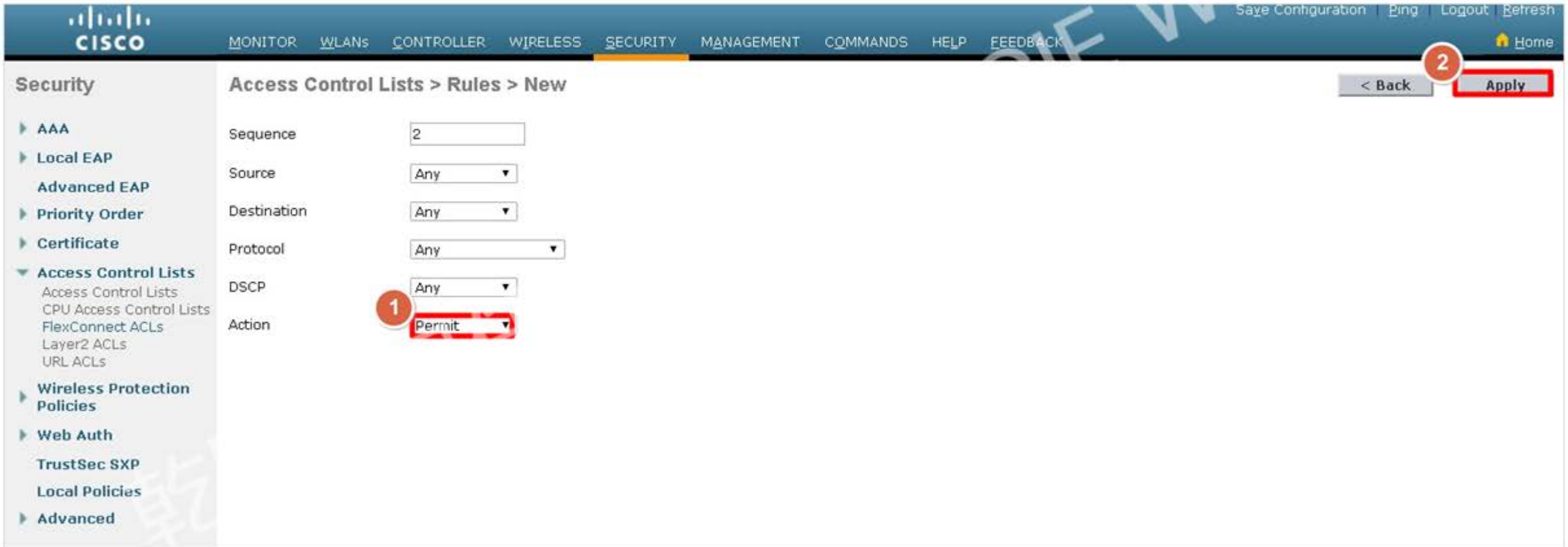
FlexConnect ACL

WLC 创建 FlexConnect ACL - 1

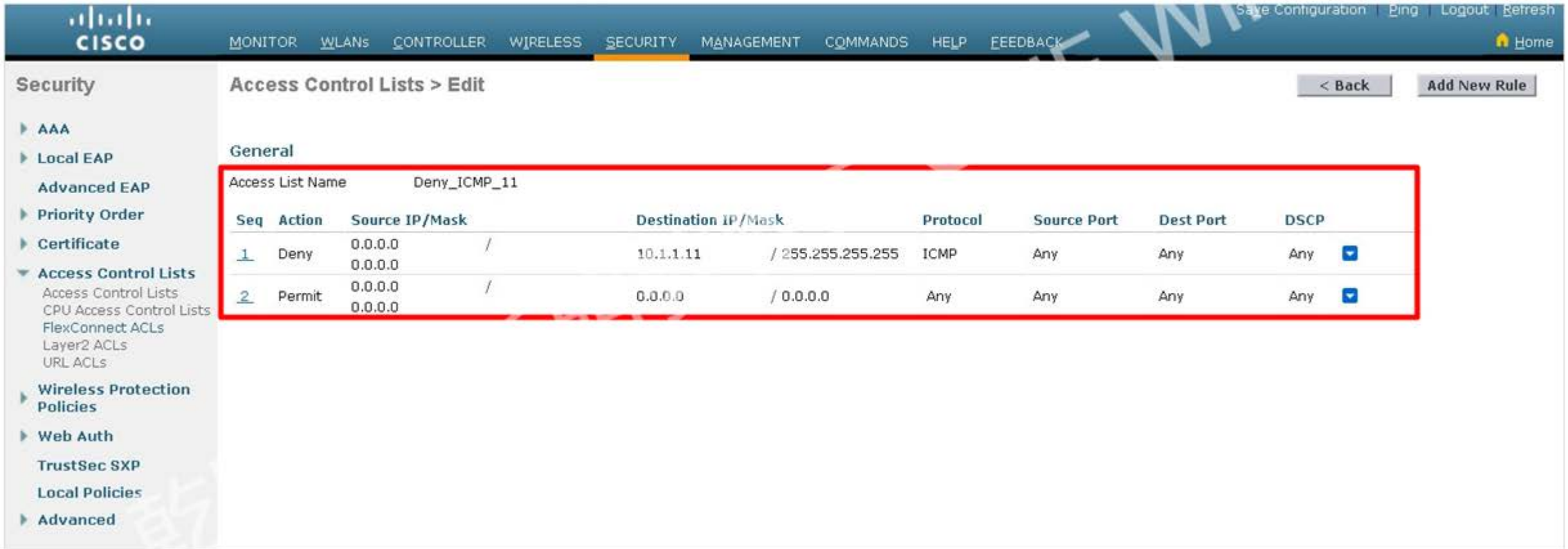


WLC 创建 FlexConnect ACL - 2

WLC 创建 FlexConnect ACL - 3

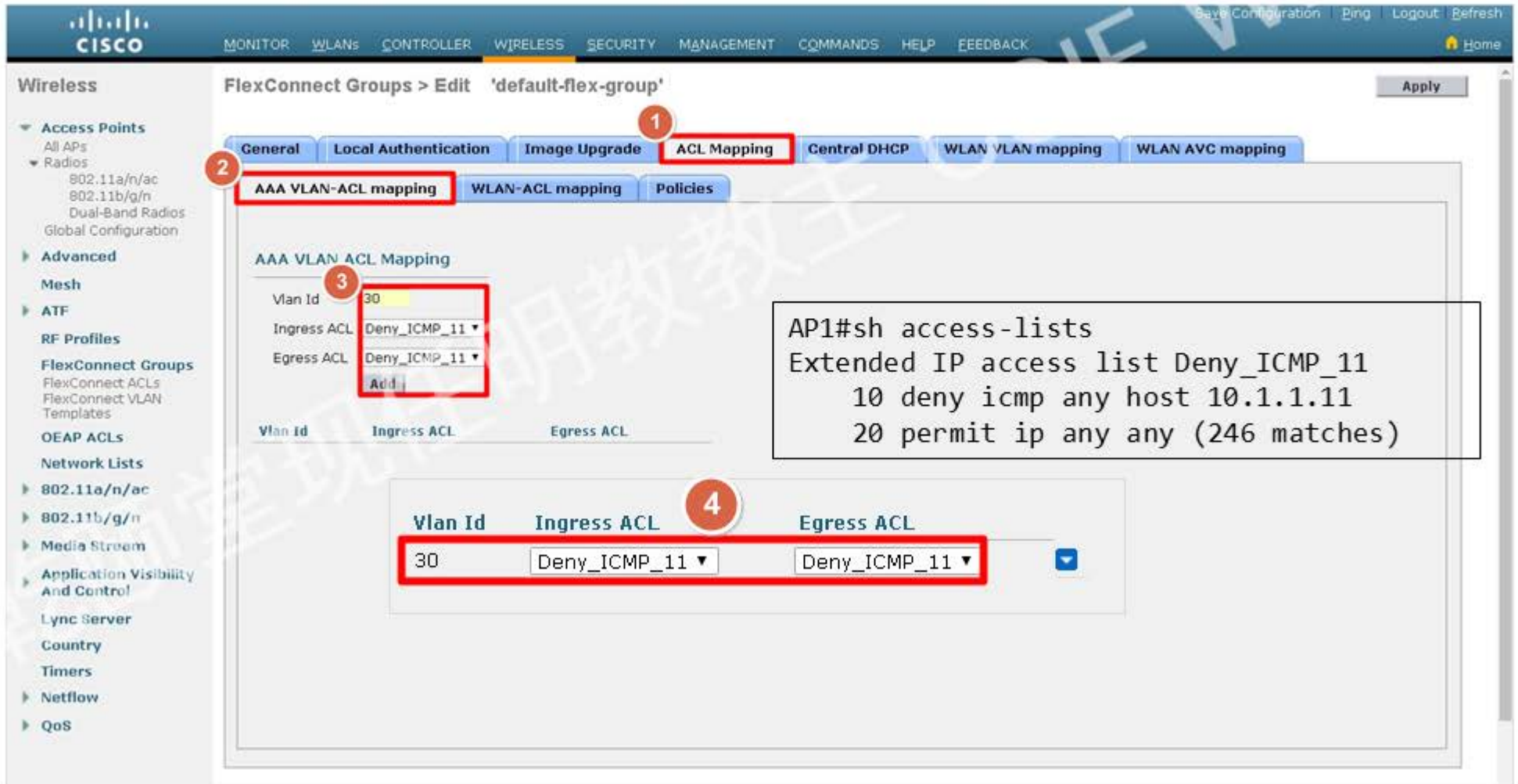


WLC 创建 FlexConnect ACL - 4



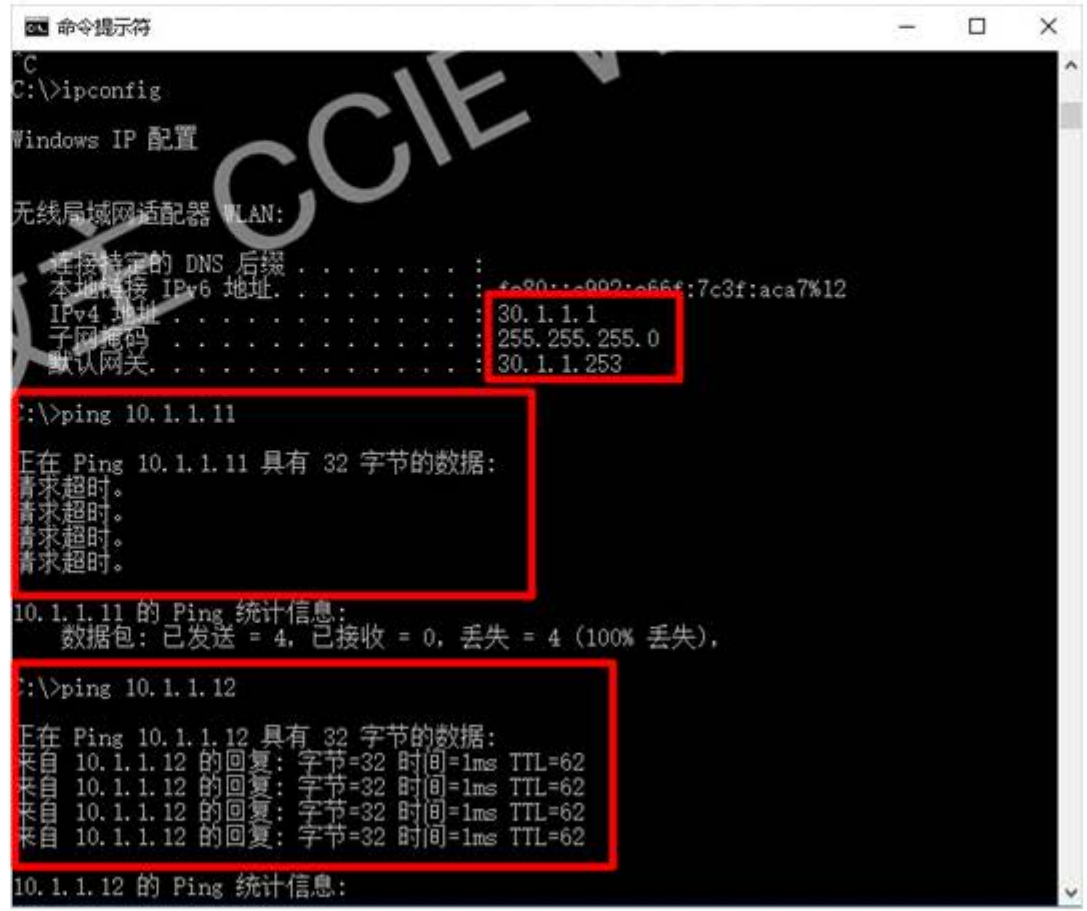
WLC 创建 FlexConnect ACL - 5

WLC 创建 VLAN-ACL 映射

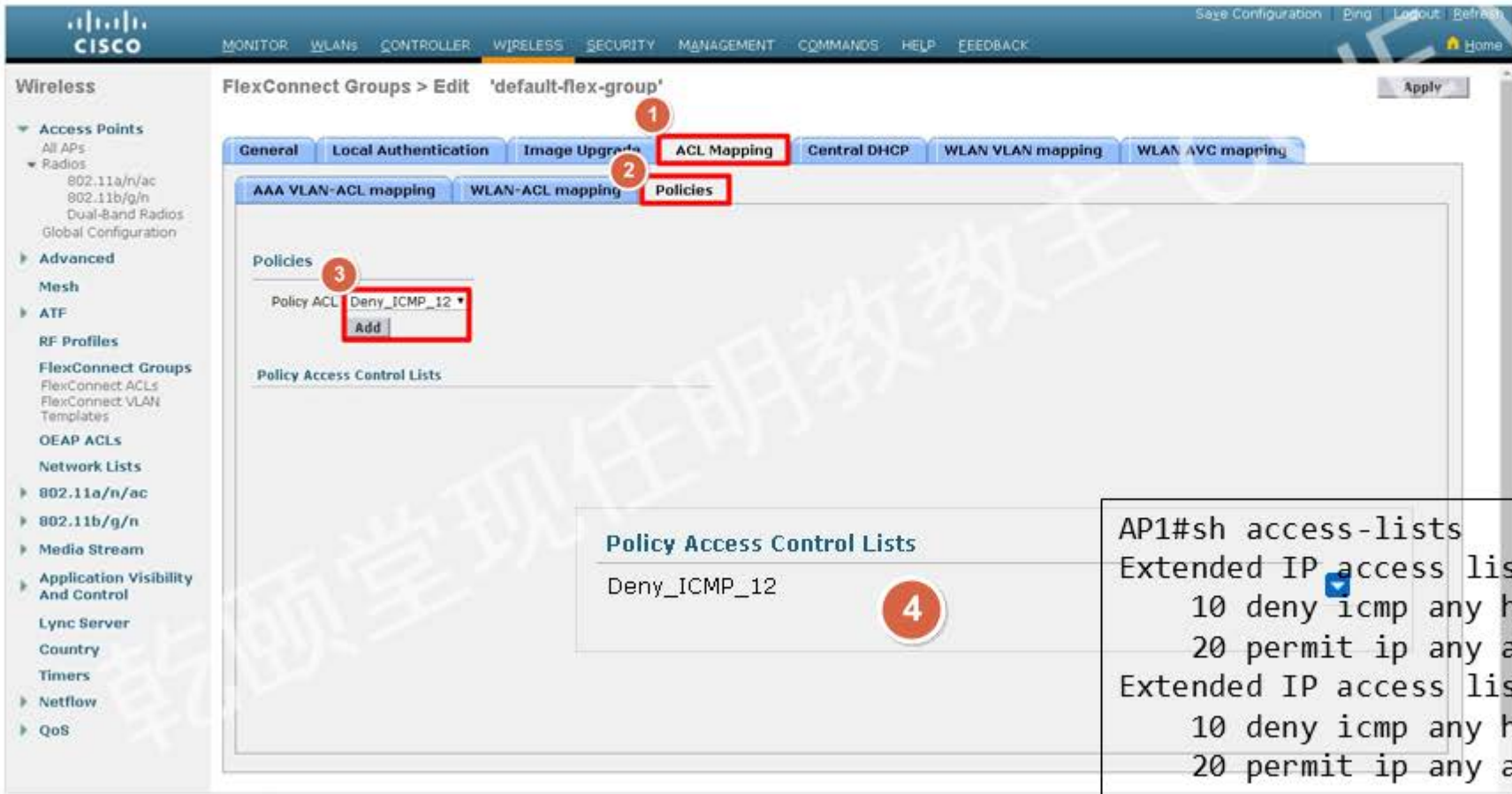


客端户连接测试 ACL 作用


```
AP1#sh access-lists
Extended IP access list Deny_ICMP_11
    10 deny icmp any host 10.1.1.11 (6 matches)
    20 permit ip any any (246 matches)
```

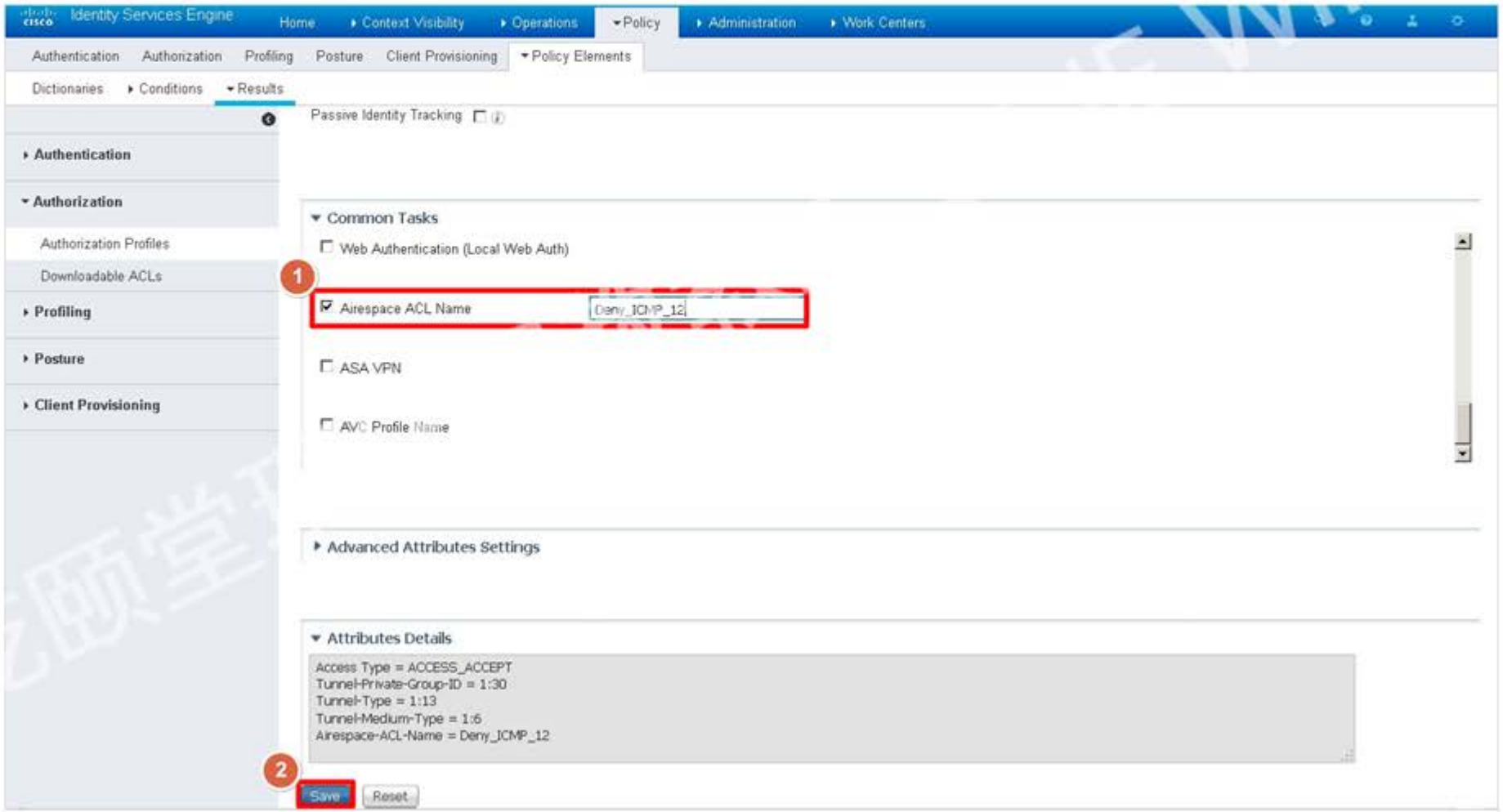


WLC 通 Polices 推送 ACL

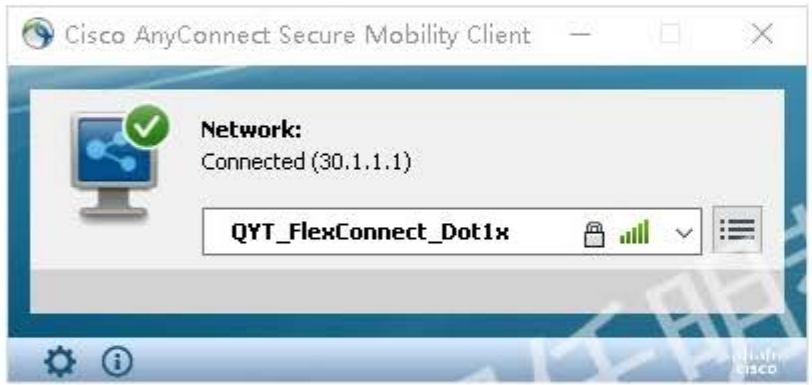



```
AP1#sh access-lists
Extended IP access list Deny_ICMP_11
    10 deny icmp any host 10.1.1.11 (6 matches)
    20 permit ip any any (246 matches)
Extended IP access list Deny_ICMP_12
    10 deny icmp any host 10.1.1.12
    20 permit ip any any
```

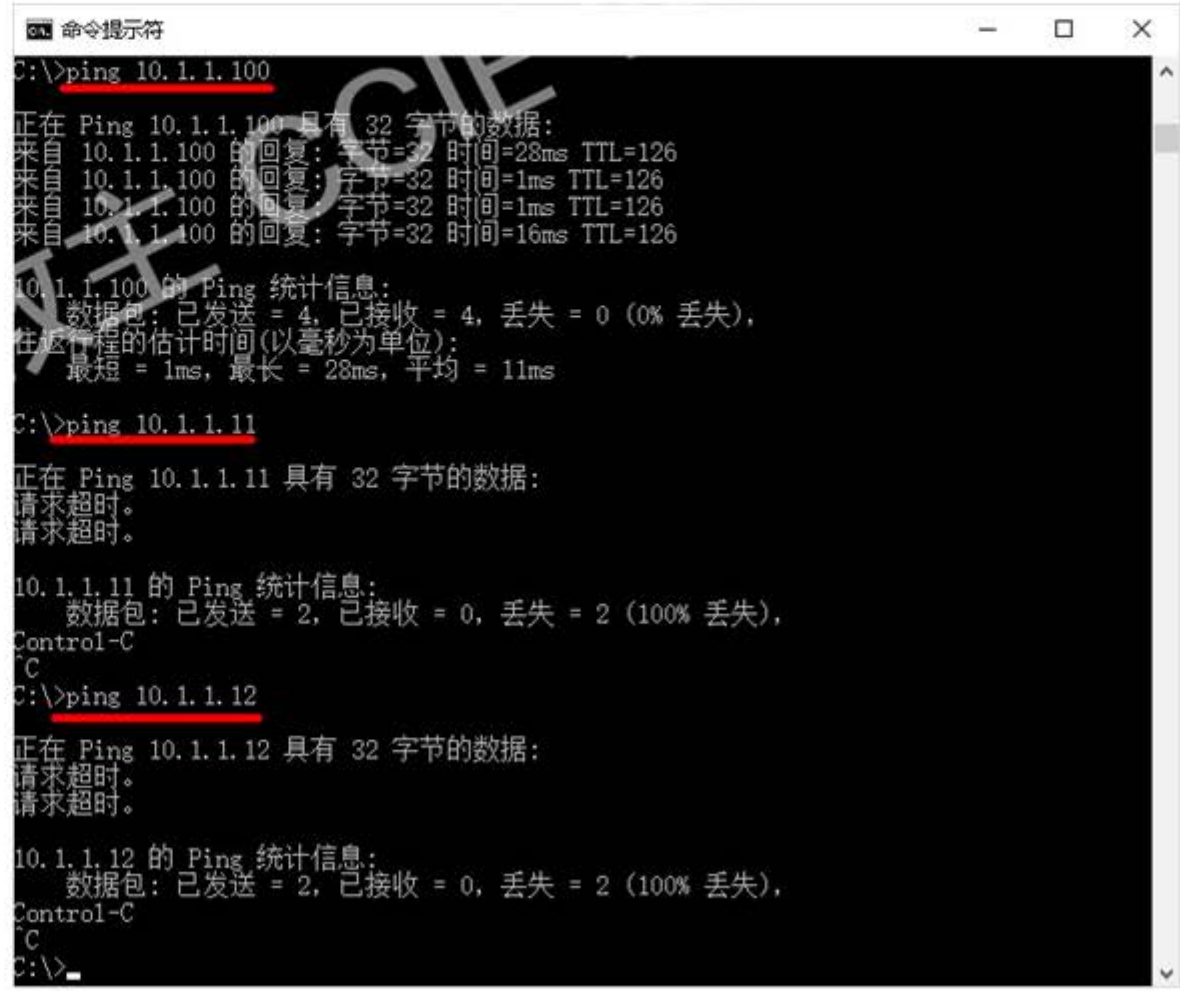
ISE 授权 Airspace ACL Nmae



客端户连接测试 ACL 权限

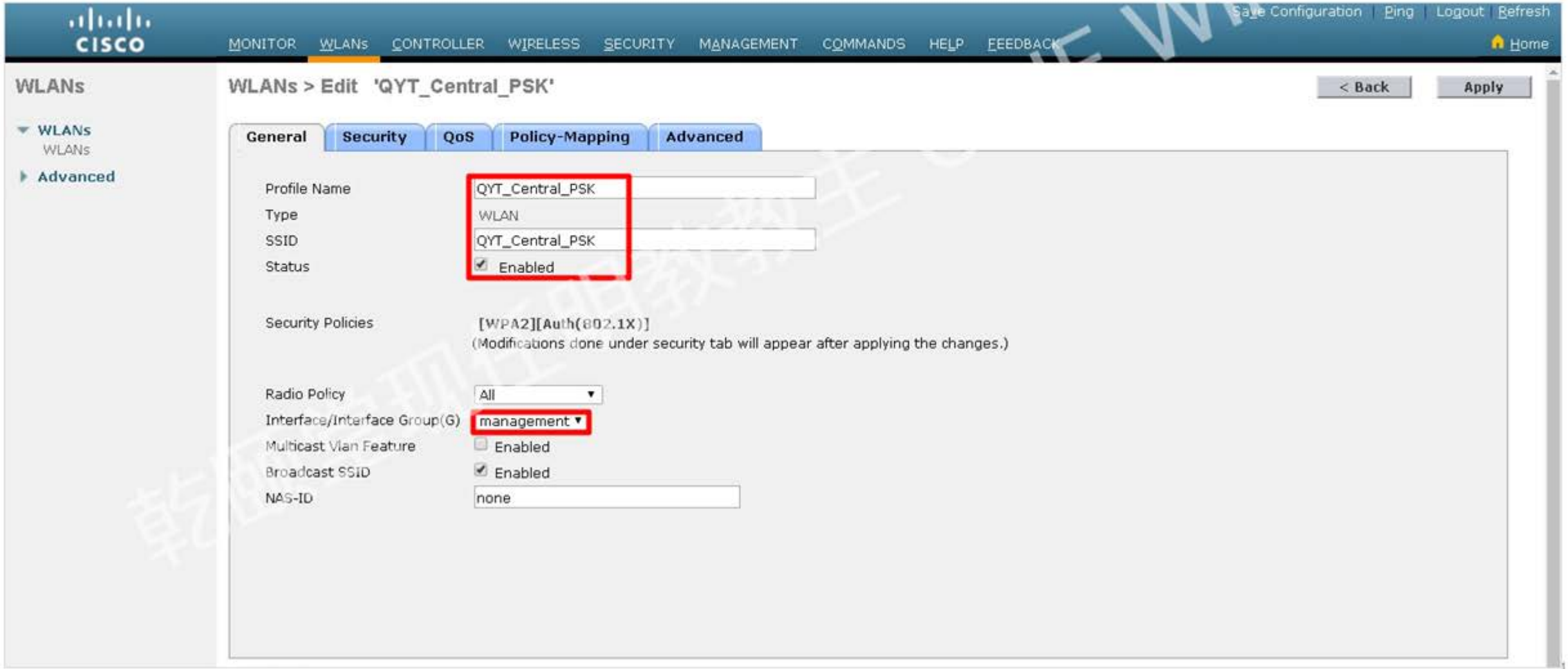



```
AP1#sh access-lists
Extended IP access list Deny_ICMP_11
    10 deny icmp any host 10.1.1.11 (14 matches)
    20 permit ip any any (474 matches)
Extended IP access list Deny_ICMP_12
    10 deny icmp any host 10.1.1.12 (5 matches)
    20 permit ip any any (236 matches)
```

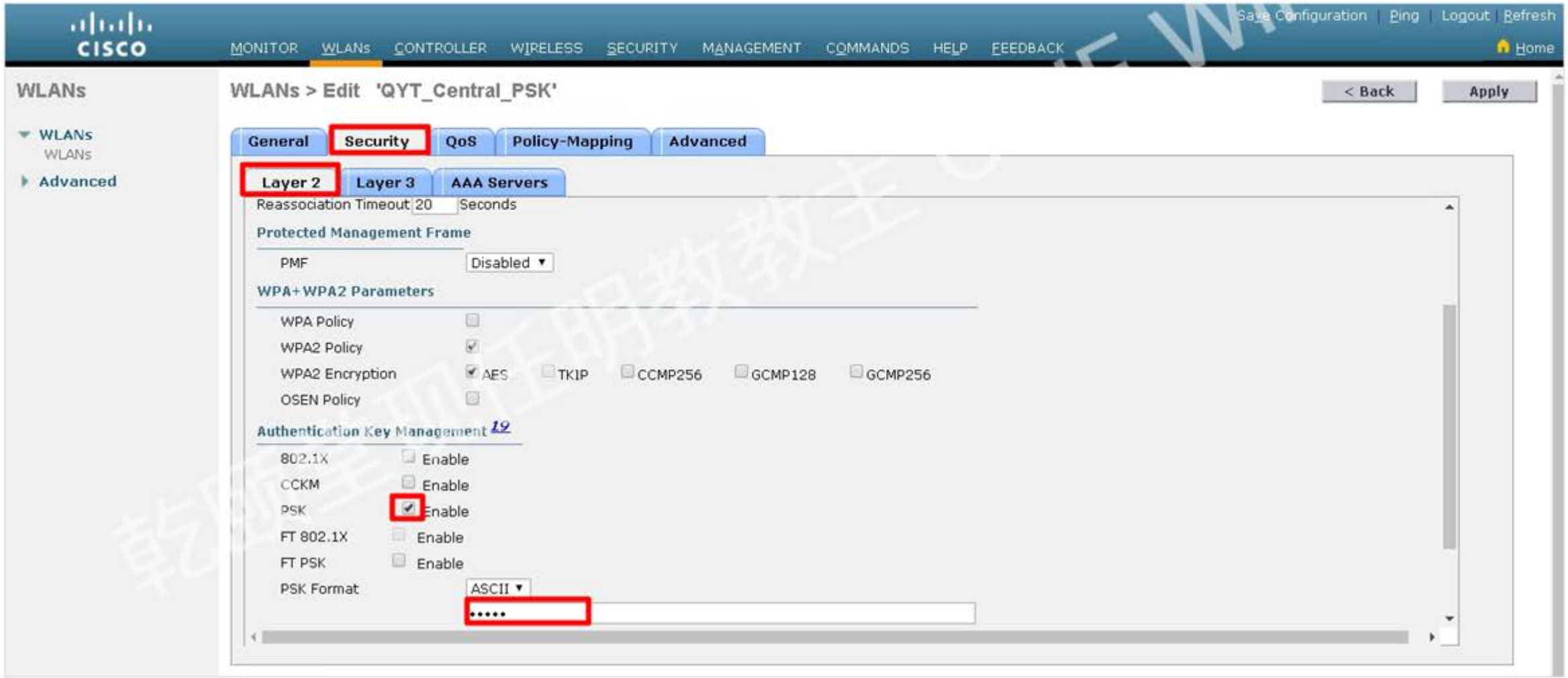


3.5 Split Tunneling

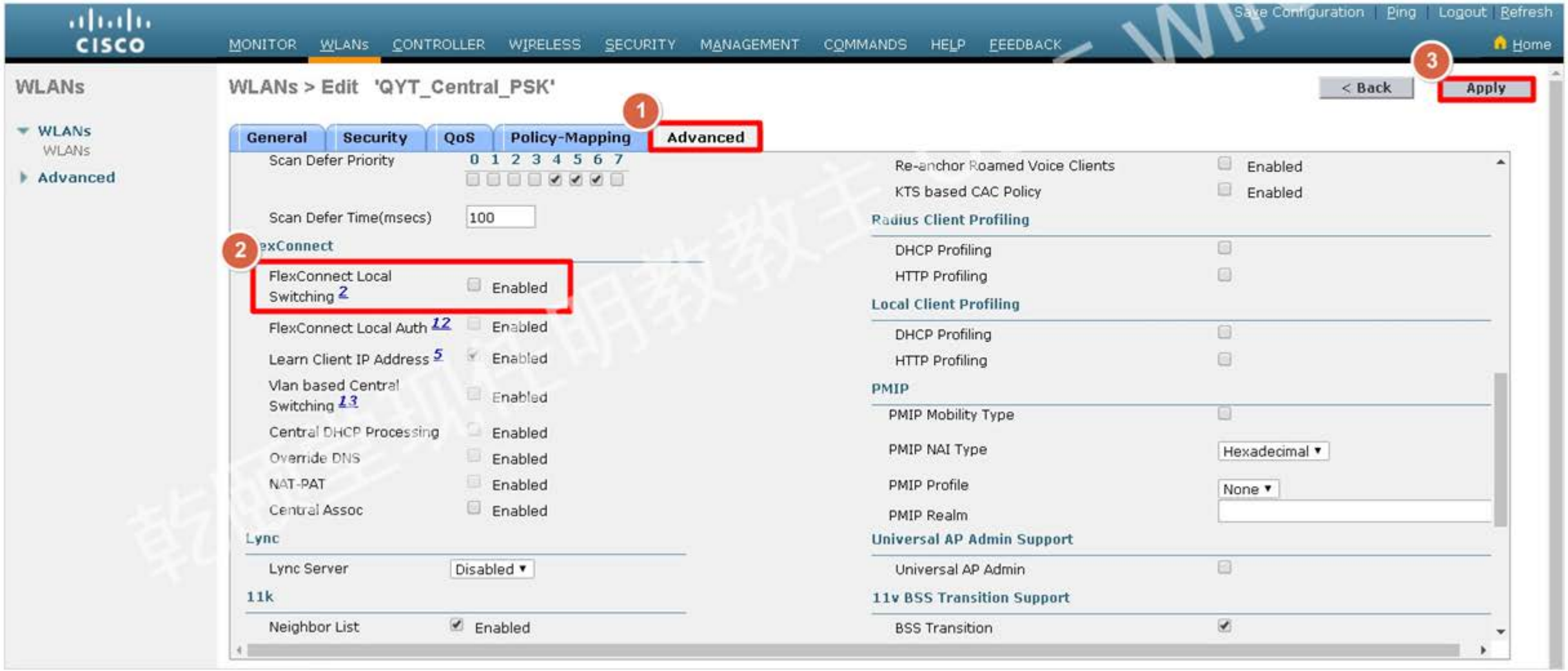
WLC 创建 WLAN -1


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > Edit 'QYT_Central_PSK'
< Back
Apply
WLANs
WLANs
Advanced
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
QYT_Central_PSK
Type
WLAN
SSID
QYT_Central_PSK
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)
management
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none

WLC 创建 WLAN -2


Save Configuration | Ping | Logout | Refresh
Home
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'QYT_Central_PSK'
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Reassociation Timeout 20 Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management 19
802.1X
Enable
CCKM
Enable
PSK
Enable
FT 802.1X
Enable
FT PSK
Enable
PSK Format
ASCII
•••••

WLC 创建 WLAN -3


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs
Advanced
WLANs > Edit 'QYT_Central_PSK'
< Back
Apply
1
General
Security
QoS
Policy-Mapping
Advanced
Scan Defer Priority
0 1 2 3 4 5 6 7
Scan Defer Time(msecs)
100
2
FlexConnect
FlexConnect Local Switching 2
Enabled
FlexConnect Local Auth 12
Enabled
Learn Client IP Address 5
Enabled
Vlan based Central Switching 13
Enabled
Central DHCP Processing
Enabled
Override DNS
Enabled
NAT-PAT
Enabled
Central Assoc
Enabled
Lync
Lync Server
Disabled
11k
Neighbor List
Enabled
Re-anchor Roamed Voice Clients
Enabled
KTS based CAC Policy
Enabled
Radius Client Profiling
DHCP Profiling
HTTP Profiling
Local Client Profiling
DHCP Profiling
HTTP Profiling
PMIP
PMIP Mobility Type
PMIP NAI Type
Hexadecimal
PMIP Profile
None
PMIP Realm
Universal AP Admin Support
Universal AP Admin
11v BSS Transition Support
BSS Transition

WLC 创建 FlexConnect

将列表关联到中心交换的 WLAN

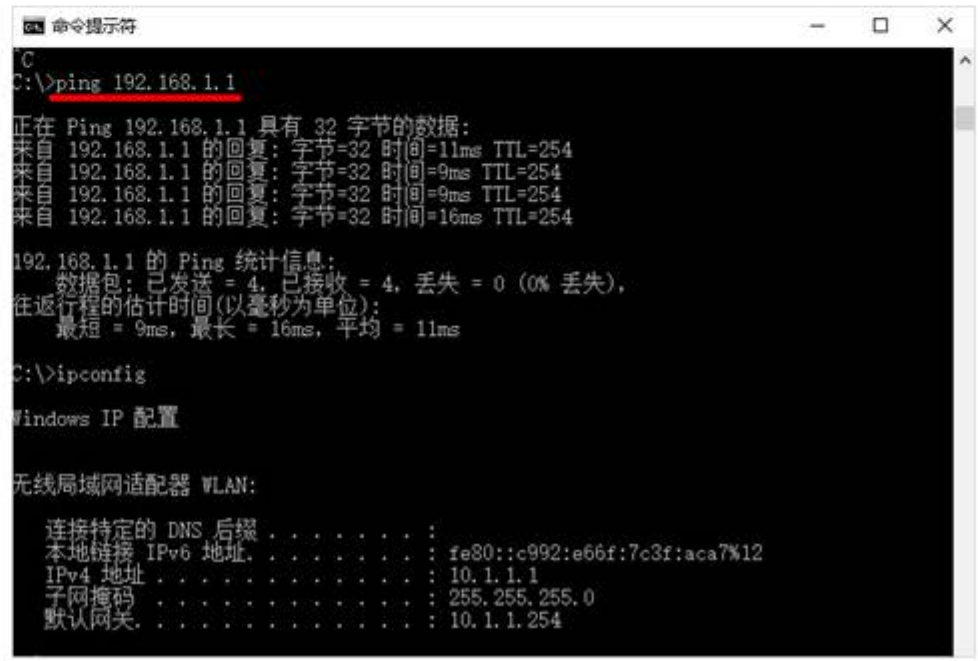

```
AP1#show access-lists
Extended IP access list To_LocalServer
    10 permit icmp any 192.168.1.0 0.0.0.255
```

中心交换机无法访问分支服务器

```
SW3560#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

客户端连接测试

```
SW3650-1# debug ip icmp
*Dec 16 02:57:55.244: ICMP: echo reply sent, src 192.168.1.1, dst 20.1.1.1, topology BASE, dscp 0
topoid 0
*Dec 16 02:57:55.643: ICMP: redirect sent to 20.1.1.1 for dest 10.1.1.100, use gw 20.1.1.254
*Dec 16 02:57:56.496: ICMP: redirect sent to 20.1.1.1 for dest 10.1.1.100, use gw 20.1.1.254
*Dec 16 02:57:57.071: ICMP: redirect sent to 20.1.1.1 for dest 10.1.1.100, use gw 20.1.1.254
*Dec 16 02:57:57.827: ICMP: redirect sent to 20.1.1.1 for dest 10.1.1.100, use gw 20.1.1.254
```



查看 AP 配置

```
AP1#show access-lists
Extended IP access list Deny_ICMP_11
    10 deny icmp any host 10.1.1.11 (14 matches)
    20 permit ip any any (1730 matches)
Extended IP access list Deny_ICMP_12
    10 deny icmp any host 10.1.1.12 (5 matches)
    20 permit ip any any (1595 matches)
Extended IP access list To_LocalServer
    10 permit icmp any 192.168.1.0 0.0.0.255 (4 matches)
Extended IP access list reap_local_central_acl
    10 permit ip 10.1.1.0 0.0.0.255 any (1 match)
```

```
AP1#show derived-config

interface BVI1
 mac-address fc5b.3937.1a98
 ip address 20.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
!
interface BVI2
 mac-address 6899.cd06.5f30
 ip address 10.1.1.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly in

ip nat inside source list reap_local_central_acl
interface BVI1 overload


ip access-list extended To_LocalServer
 permit icmp any 192.168.1.0 0.0.0.255
ip access-list extended reap_local_central_acl
 permit ip 10.1.1.0 0.0.0.255 any
```

AP1#show derived-config .txt