



# 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



# 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

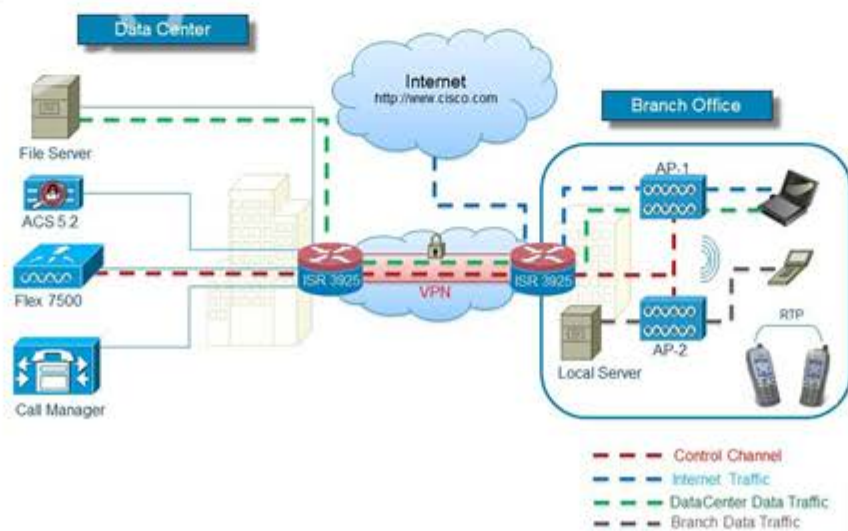


# 统一访问：一种架构，多种部署选项



# 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 对客户端进行身份认证)
- **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，切换到 FlexConnect 模式，AP 不会重启。

The screenshot shows the Cisco Wireless Configuration Manager interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WIRELESS' menu is highlighted with a red box and the number 1. On the left sidebar, 'Wireless' is expanded to 'Access Points', and 'All APs' is selected with a red box and the number 2. The main content area shows 'Details for AP1' with tabs for 'General', 'Credentials', 'Interfaces', 'High Availability', 'Inventory', 'FlexConnect', and 'Advanced'. The 'General' tab is active, showing fields for AP Name (AP1), 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 (FlexConnect), Operational Status, Port Number, Venue Group, and Venue Type. The 'AP Mode' dropdown menu is open, showing options: local, FlexConnect (highlighted with a red box and the number 3), monitor, Rogue Detector, Sniffer, Bridge, Flex+Bridge, SE-Connect, and Sensor. The 'Versions' section shows software and boot versions. The 'IP Config' section shows CAPWAP Preferred Mode (Ipv4 (Global Config)) and DHCP Ipv4 Address (20.1.1.1). A red box and the number 4 highlight the 'Apply' button in the top right corner.

# 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。

The screenshot shows the Cisco FlexConnect configuration interface for a WLAN named 'QYT\_FlexConnect'. The 'Advanced' tab is selected, and the 'FlexConnect Local Switching' option is checked and set to 'Enabled'. Other options like 'FlexConnect Local Auth', 'Learn Client IP Address', and 'Lync Server' are also visible.

Section	Option	Status
FlexConnect	FlexConnect Local Switching	Enabled
	FlexConnect Local Auth	Enabled
	Learn Client IP Address	Enabled
	Man 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
	Neighbor List Dual Band	Enabled

Additional configuration options visible on the right side of the page include:

- DHCP Profiling:
- HTTP Profiling:
- Local Client Profiling:
- PMIP:
- PMIP Mobility Type:
- PMIP NAI Type: Hexadecimal
- PMIP Profile: None
- PMIP Realm:
- Universal AP Admin Support:
- 11v BSS Transition Support:
- BSS Transition:
- Optimized Roaming Disassociation Timer (0 to 40 TBTT): 40
- BSS Max Idle Service:



# 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)

The screenshot shows the Cisco Prime Infrastructure configuration interface for an AP. The page title is "All APs > Details for AP1". The navigation menu includes "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", "HELP", and "FEEDBACK". The "FlexConnect" tab is selected and highlighted with a red box and a circled "1". The "VLAN Support" checkbox is checked and highlighted with a red box and a circled "2". The "Native VLAN ID" is set to "1". The "VLAN Mappings" button is visible. The "Apply" button is highlighted with a red box and a circled "3".

# 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)

Wireless

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | Home

All APs > Details for AP1

General | Credentials | Interfaces | High Availability | Inventory | FlexConnect | Advanced

VLAN Support

Inheritance Level AP-Specific

Native VLAN ID 20

VLAN Mappings

```
interface GigabitEthernet1/0/2
switchport trunk native vlan 20
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

# SSID to VLAN Mapping - 1

- 点击 VLAN Mappings

The screenshot shows the Cisco FlexConnect configuration interface for AP1. The page is titled "All APs > Details for AP1" and has tabs for General, Credentials, Interfaces, High Availability, Inventory, FlexConnect, and Advanced. The FlexConnect tab is active. In the FlexConnect section, the "VLAN Support" checkbox is checked, and the "Make VLAN AP Specific" dropdown is set to "Make VLAN AP Specific". A "Go" button is next to it. Below this, the "Inheritance Level" is set to "AP-Specific". The "Native VLAN ID" is set to "20". A red box highlights the "VLAN Mappings" link, which is indicated by a red circle with the number "1".

# SSID to VLAN Mapping - 2

- 将 SSID 映射到本地的 VLAN

The screenshot shows the Cisco FlexConnect configuration page for AP1. The breadcrumb navigation is "All APs > AP1 > VLAN Mappings". The page title is "All APs > AP1 > VLAN Mappings". There are navigation buttons for "< Back" and "Apply".

**AP Information:**

- 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	20	no	Wlan-specific

**Centrally switched Wlans:**

WLAN Id	SSID	VLAN ID
---------	------	---------

Annotations: A red box highlights the "Apply" button (labeled with a red circle containing the number 2). Another red box highlights the "20" in the "VLAN ID" column of the mapping table (labeled with a red circle containing the number 1).



## 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

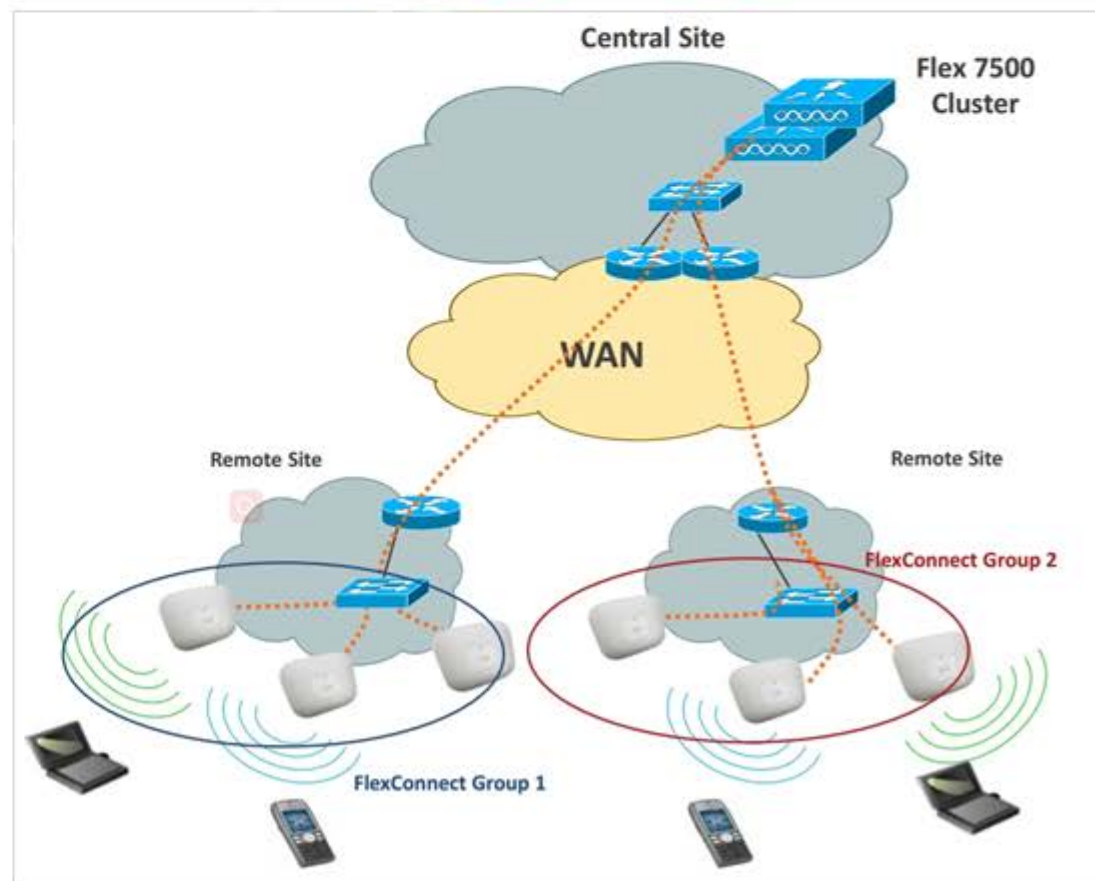


# FlexConnect Group 介绍

- 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

The screenshot displays the Cisco FlexConnect Groups configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'FlexConnect Groups' option selected. The main content area shows a table with one entry: 'default-flex-group' with 1 AP. A 'New...' button is visible in the top right. Below the table is a 'New' form with a 'Group Name' field containing 'FlexConnect\_Shanghai\_Site'. The 'Apply' button is highlighted in the bottom right.

Group Name	Number of APs
<a href="#">default-flex-group</a>	1

FlexConnect Groups > New

Group Name:

< Back Apply

# 添加 AP 到 FlexConnect Group

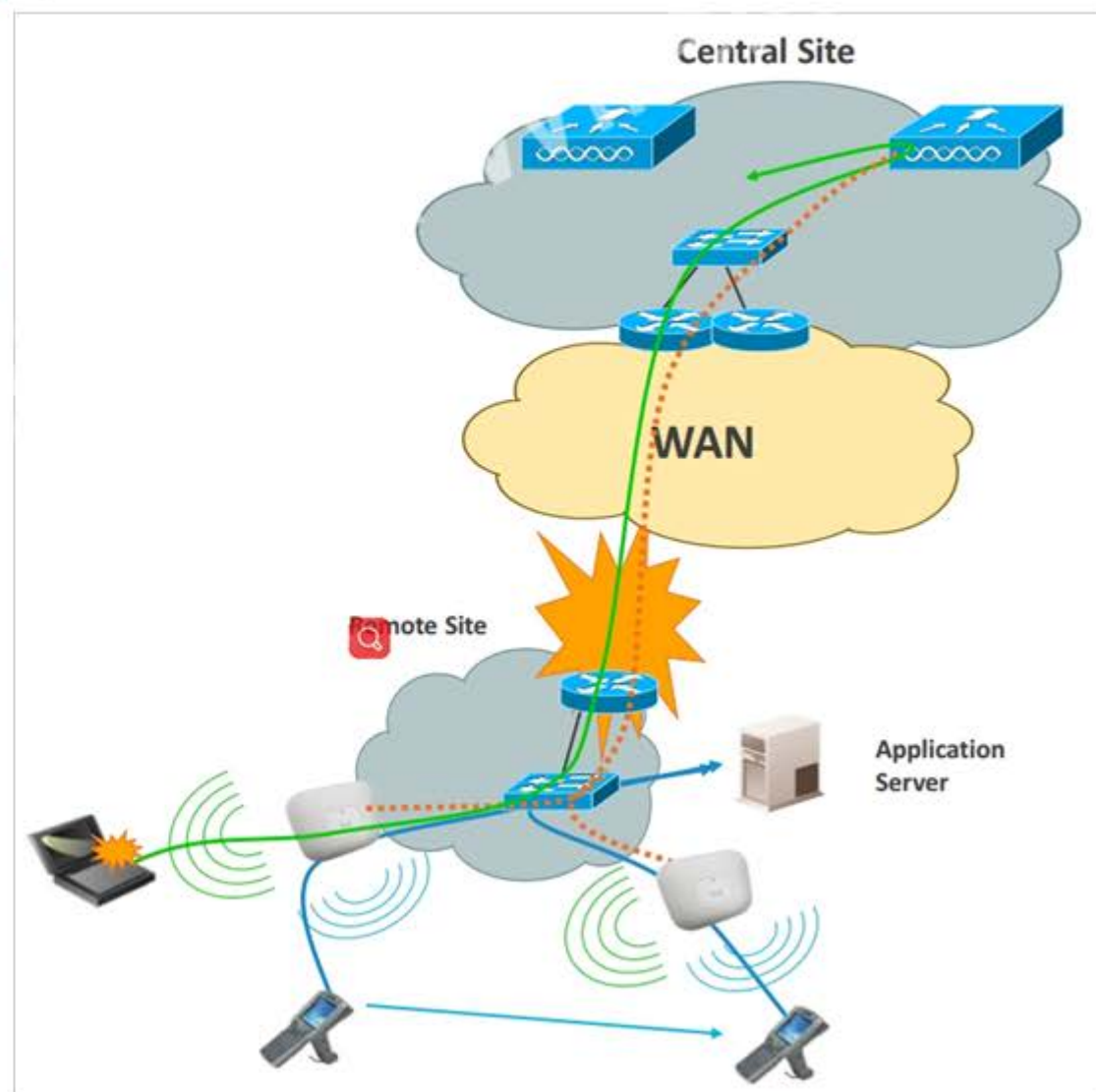
- AP 默认属于 default-flex-group, 将 AP 移动到新建的 FlexConnect Group。

The screenshot shows the Cisco FlexConnect Groups configuration page. The left sidebar shows the navigation menu with 'FlexConnect Groups' selected. The main content area is titled 'FlexConnect Groups > Edit 'default-flex-group''. The 'WLAN AVC mapping' tab is active, showing the 'Group Name' as 'default-flex-group' and 'VLAN Template Name' as 'none'. A red box highlights the 'FlexConnect AP' link. Below this, the 'New Group Name' dropdown is set to 'FlexConnect\_Shanghai\_Site', and a red box highlights the 'Move' button. At the bottom, a table lists the APs associated with the group.

MAC Address	AP Name	Status	Type	Conflict with PnP	
<input checked="" type="checkbox"/>	fc:5b:39:37:1a:98	AP1	Associated	Manual	Yes

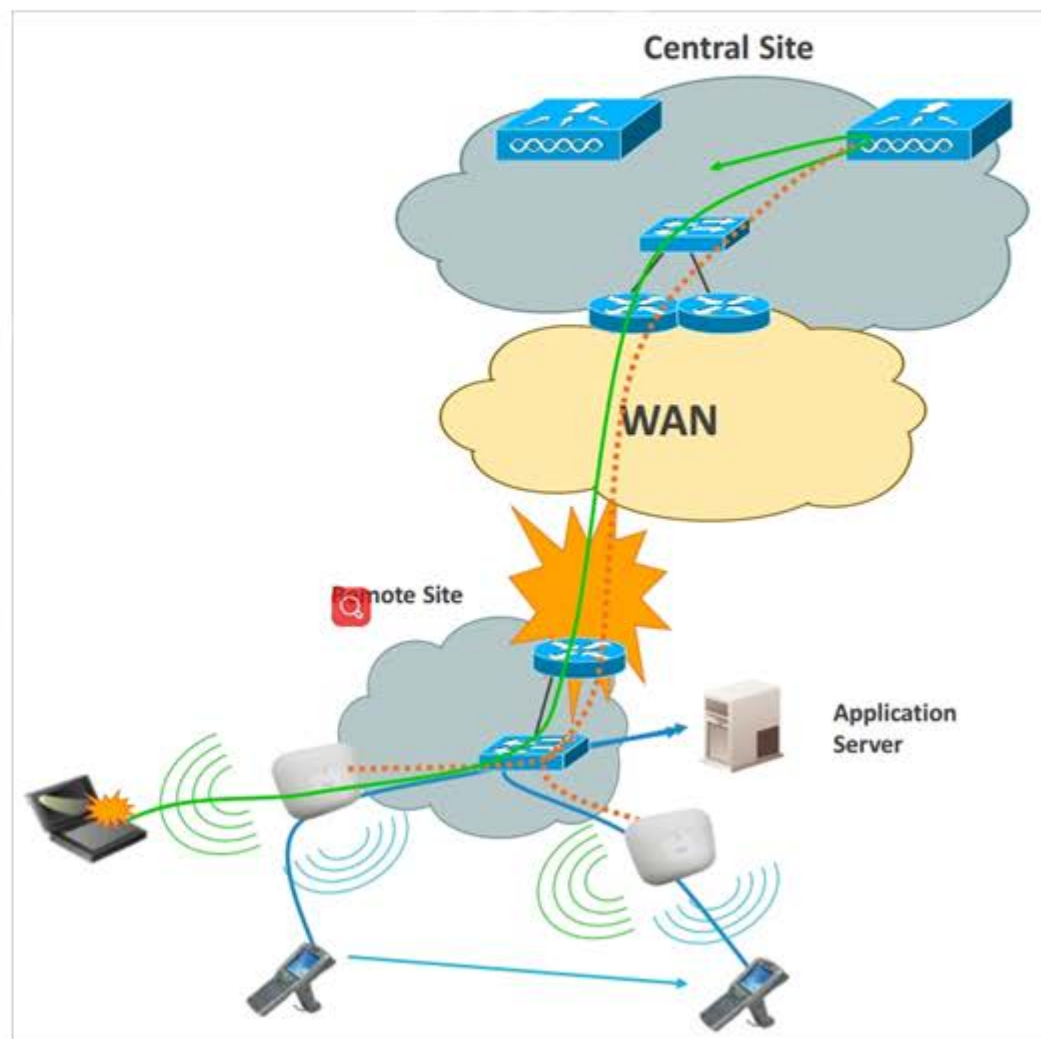
# FlexConnect 备份情景 — WAN Failure

- 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



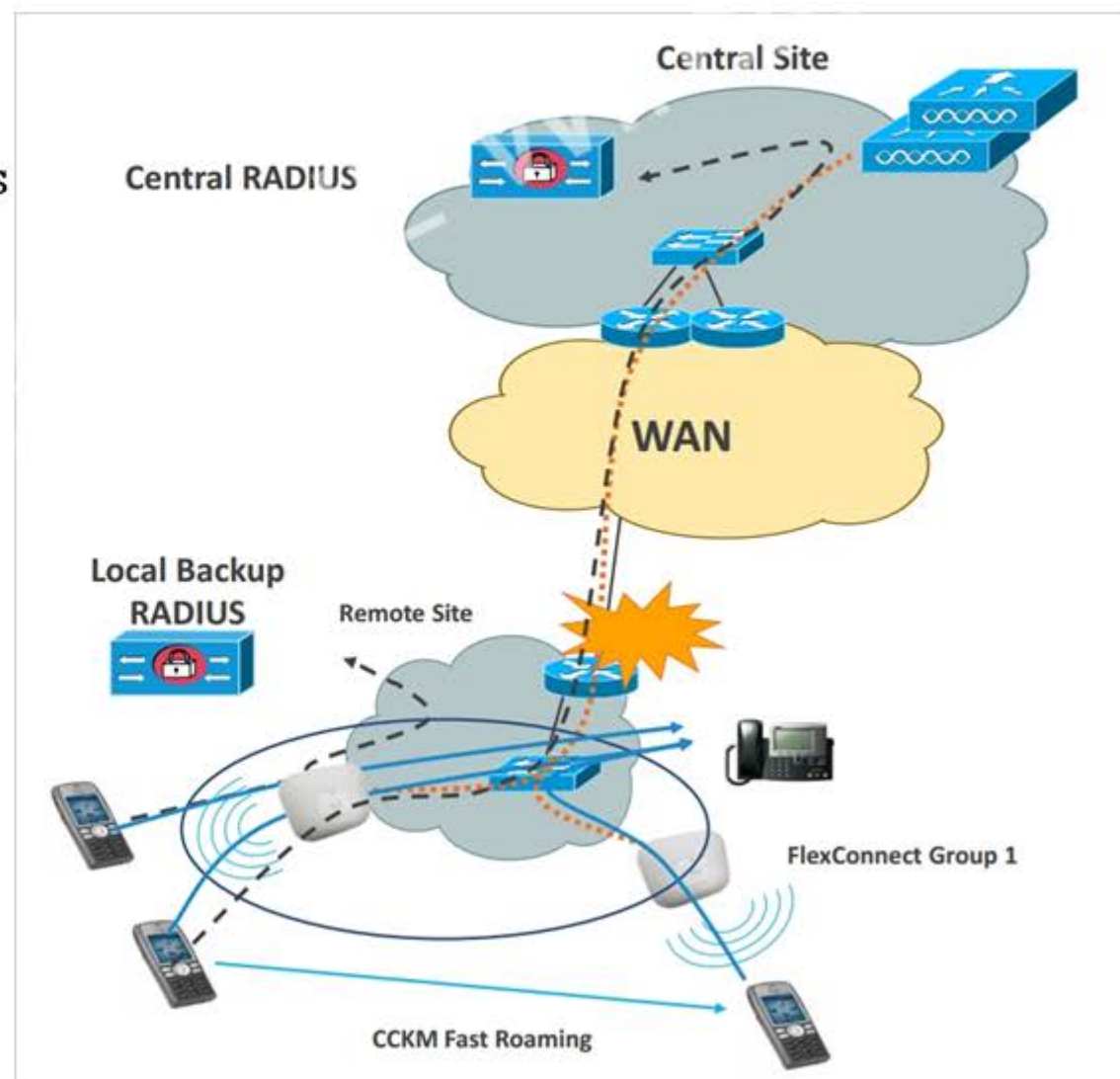
# FlexConnect 备份情景 — WLC Failure

- 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

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration Ping Logout Refresh Home

Wireless FlexConnect Groups > Edit 'FlexConnect\_Shanghai\_Site' Apply

**1** **General** Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC mapping

**2** **FlexConnect Groups**

**Group Name** FlexConnect\_Shanghai\_Site  
**VLAN Template Name** none  
**Enable AP Local Authentication**

**FlexConnect AP**

**HTTP-Proxy**  
**Ip Address** 0.0.0.0  
**Port** 0  
Add

**AAA**

**Server Ip Address** 10.1.1.11  
**Server Type** Secondary  
**Shared Secret** .....  
**Confirm Shared Secret** .....  
**Port Number** 1812  
Add

Server Type	Address	Port	
Primary	10.1.1.12	1812	<input checked="" type="checkbox"/>
UnConfigured	Unconfigured	0	<input checked="" type="checkbox"/>

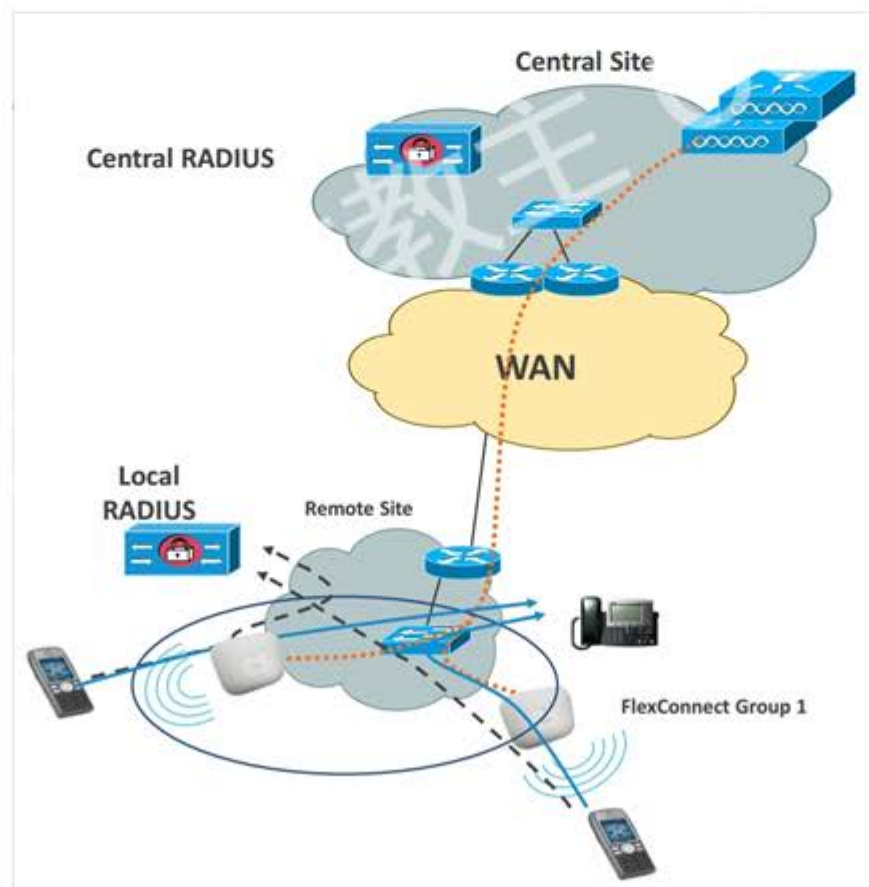
**3** **AAA**  
**Server Ip Address** 10.1.1.12  
**Server Type** Primary  
**Shared Secret** .....  
**Confirm Shared Secret** .....  
**Port Number** 1812  
Add

**4** **AAA**



# 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)

The screenshot shows the Cisco FlexConnect Groups configuration interface. The page title is "FlexConnect Groups > Edit 'FlexConnect\_Shanghai\_Site'". The "Local Authentication" tab is active. The "Group Name" is "FlexConnect\_Shanghai\_Site". The "VLAN Template Name" is set to "none". The "Enable AP Local Authentication" checkbox is checked and highlighted with a red box. Below this, there are sections for "FlexConnect AP" and "HTTP-Proxy". The "HTTP-Proxy" section has fields for "Ip Address" (0.0.0.0) and "Port" (0).

# FlexConnect Group 配置 AP 本地认证 - 2

- 8.3 版本支持的本地认证协议。

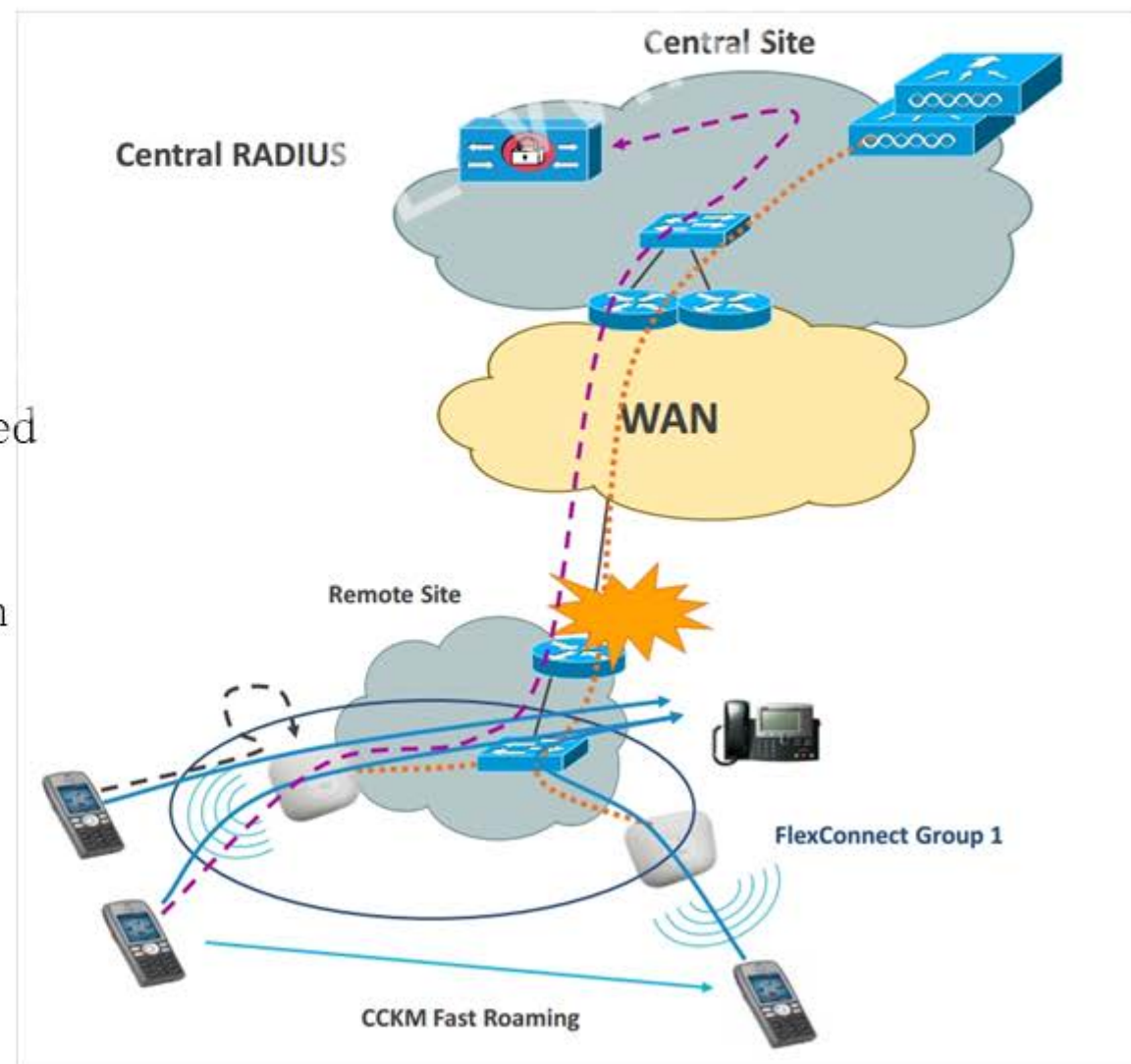
The screenshot displays the Cisco FlexConnect Groups configuration interface for the 'FlexConnect\_Shanghai\_Site'. The 'Local Authentication' tab is active, and the 'Local Use' sub-tab is selected. The 'Protocols' section is highlighted with a red box, showing the following configuration:

- LEAP**
  - Enable LEAP Authentication<sup>2</sup>
- EAP Fast**
  - Enable EAP Fast Authentication<sup>2</sup>
  - Server Key (in hex)   Enable Auto key generation
  - (Confirm server key)
  - Authority ID (in hex)
  - Authority Info
  - PAC Timeout (2 to 4095 days)
- PEAP**
  - Enable PEAP Authentication<sup>2</sup>
- EAP TLS**
  - Enable EAP TLS Authentication<sup>2</sup>
  -

# Local Backup Authentication

- Normal authentication is done centrally
- On WAN failure, AP authenticates new clients with 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 <b>New</b>



# Local Authentication

The screenshot shows the Cisco FlexConnect configuration interface for a WLAN named 'QYT\_FlexConnect'. The 'Advanced' tab is selected, and the 'FlexConnect Local Auth' option is highlighted with a red box and a circled '3'. Other options like 'FlexConnect Local Switching' and 'Learn Client IP Address' are also enabled. The right side of the page shows various other configuration options like 'Local Client Profiling', 'PMIP', and '11v BSS Transition Support'.

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

WLANs > Edit 'QYT\_FlexConnect' < Back Apply

**2** General Security QoS Policy-Mapping **Advanced**

**3** FlexConnect Local Auth  Enabled

FlexConnect Local Switching  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

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

Directed Multicast Service



# 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

The screenshot shows the Cisco FlexConnect configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'SECURITY' menu is highlighted with a red box and the number 1. The left sidebar shows the 'Security' menu with 'Access Control Lists' expanded, and 'FlexConnect ACLs' highlighted with a red box and the number 2. The main content area is titled 'FlexConnect Access Control Lists' and shows 'Entries 0 - 0 of 0'. A 'New...' button is highlighted with a red box and the number 3. Below this, the 'Access Control Lists > New' form is shown. The 'Access Control List Name' field is highlighted with a red box and the number 4, containing the text 'FlexConnect\_ACL'. Below the form, the 'General' section shows the 'Access List Name' as 'FlexConnect\_ACL'. A table below the 'General' section shows the configuration for the ACL rule:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any

# FlexConnect ACL per AP - 1

The screenshot shows the Cisco FlexConnect configuration interface for an AP. The 'FlexConnect' tab is selected and highlighted with a red box and a '1' in a red circle. The 'VLAN Mappings' link is highlighted with a red box and a '2' in a red circle. The 'Native VLAN ID' is set to 20. The 'FlexConnect Group Name' is 'FlexConnect\_Shanghai\_Site'.

Wireless

All APs > Details for AP1

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support  Make VLAN AP Specific Go

Inheritance Level AP-Specific

Native VLAN ID 20 **VLAN Mappings**

FlexConnect Group Name FlexConnect\_Shanghai\_Site

[WLAN AVC Mapping](#)





# FlexConnect ACL per AP - 2

Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

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

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	20	no	AP-specific

Centrally switched Wlans

WLAN Id	SSID	VLAN ID

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
20	FlexConnect_ACL	FlexConnect_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.

< Back **Apply**

```

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

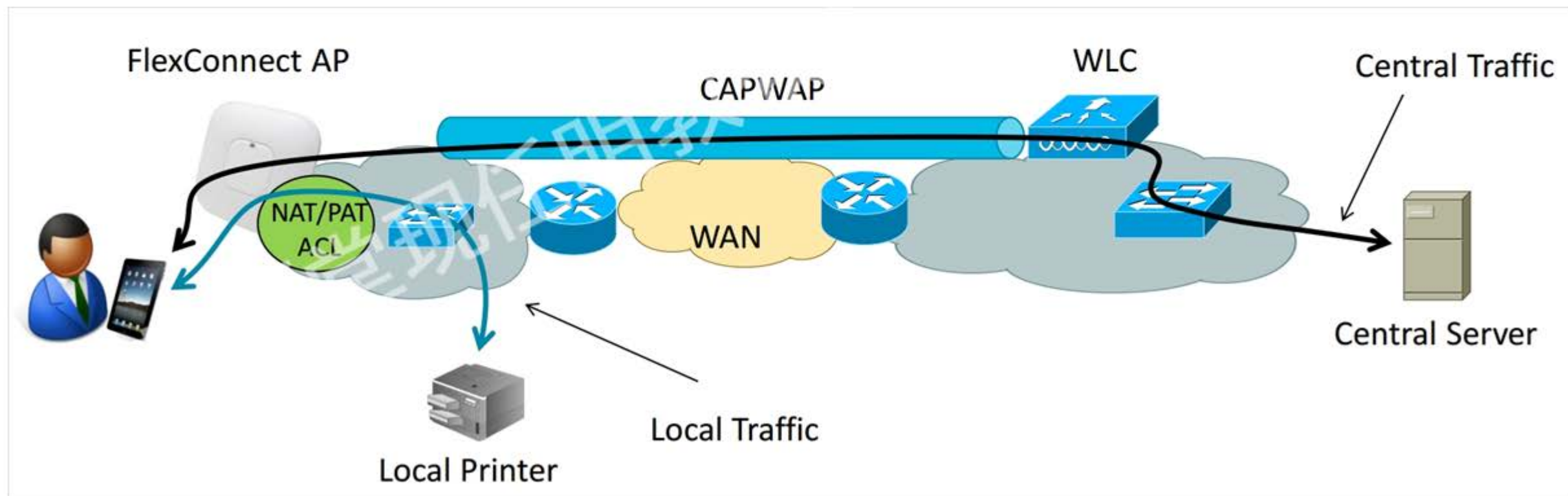
- AAA VLAN-ACL mapping 还有一个作用：做 per-user vlan 的时候需要 AP 本地有对应的 vln (子接口)，此时又不想多创建一个 SSID，可以创建 AAA VLAN-ACL mapping，不关联 ACL。

The screenshot shows the Cisco Wireless Configuration Manager interface for editing a FlexConnect Group named 'FlexConnect\_Shanghai\_Site'. The 'ACL Mapping' tab is selected, and the 'AAA VLAN-ACL mapping' sub-tab is active. The configuration shows a mapping for Vlan Id 30 with Ingress and Egress ACLs set to FlexConnect\_ACL. A table below shows the mapping for Vlan Id 30 with Ingress and Egress ACLs set to FlexConnect\_Group\_ACL.

Vlan Id	Ingress ACL	Egress ACL
30	FlexConnect_Group_ACL	FlexConnect_Group_ACL

# FlexConnect ACL - Split Tunneling

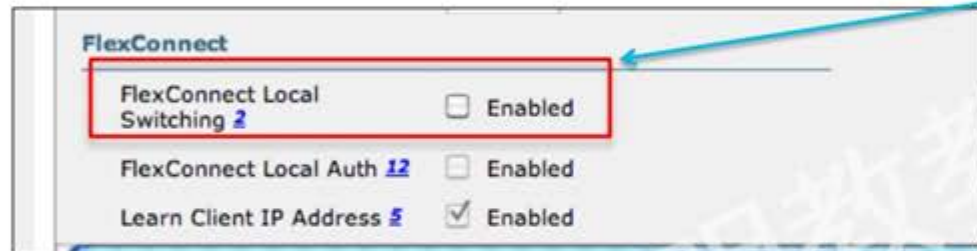
- Split tunneling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunneling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunneling is using the AP IP@ for the NAT/PAT feature



# Split Tunneling 配置 - 1

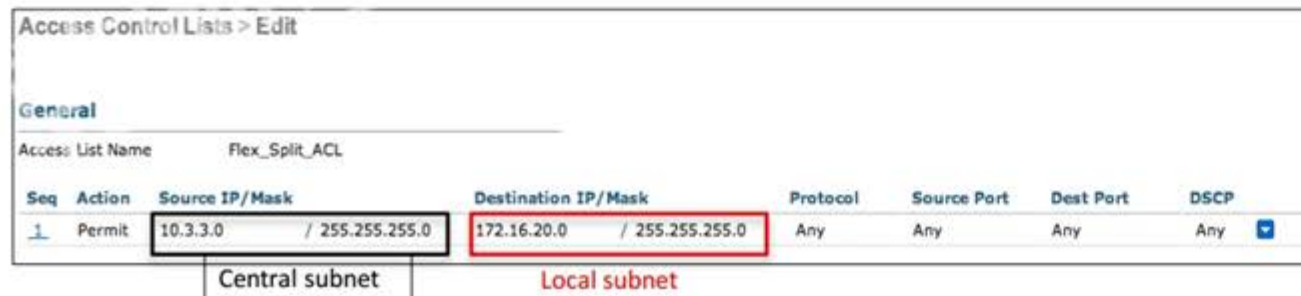
- 这个WLAN就不能本地转发了

- Create a centrally switched WLAN



Flex Local switching should not be checked

- Define Flex ACL to match traffic to be locally switched



# Split Tunneling 配置 - 2

All APs > Details for AP-3600-A

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID 52 **VLAN Mappings**

FlexConnect Group Name FlexConnect-Site-1

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#)

**[Local Split ACLs](#)**

[Central DHCP Processing](#)

All APs > AP-3600-A > ACL Mappings

AP Name AP-3600-A

Base Radio MAC 64:d9:89:43:4f:50

WLAN ACL Mapping

WLAN Id 1

Local-Split ACL Flex\_Split\_ACL

**Add**

WLAN Id	WLAN Profile Name	Local-Split ACL
1	RackMobility	Flex_Split_ACL <input checked="" type="checkbox"/>

# Split Tunneling FlexConnect Group 配置

FlexConnect Groups > Edit 'FlexConnect-Site-1'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP

AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies

**Web Auth ACL Mapping**

WLAN Id   
WebAuth ACL FlexConnect-Ad-1

**Local Split ACL Mapping**

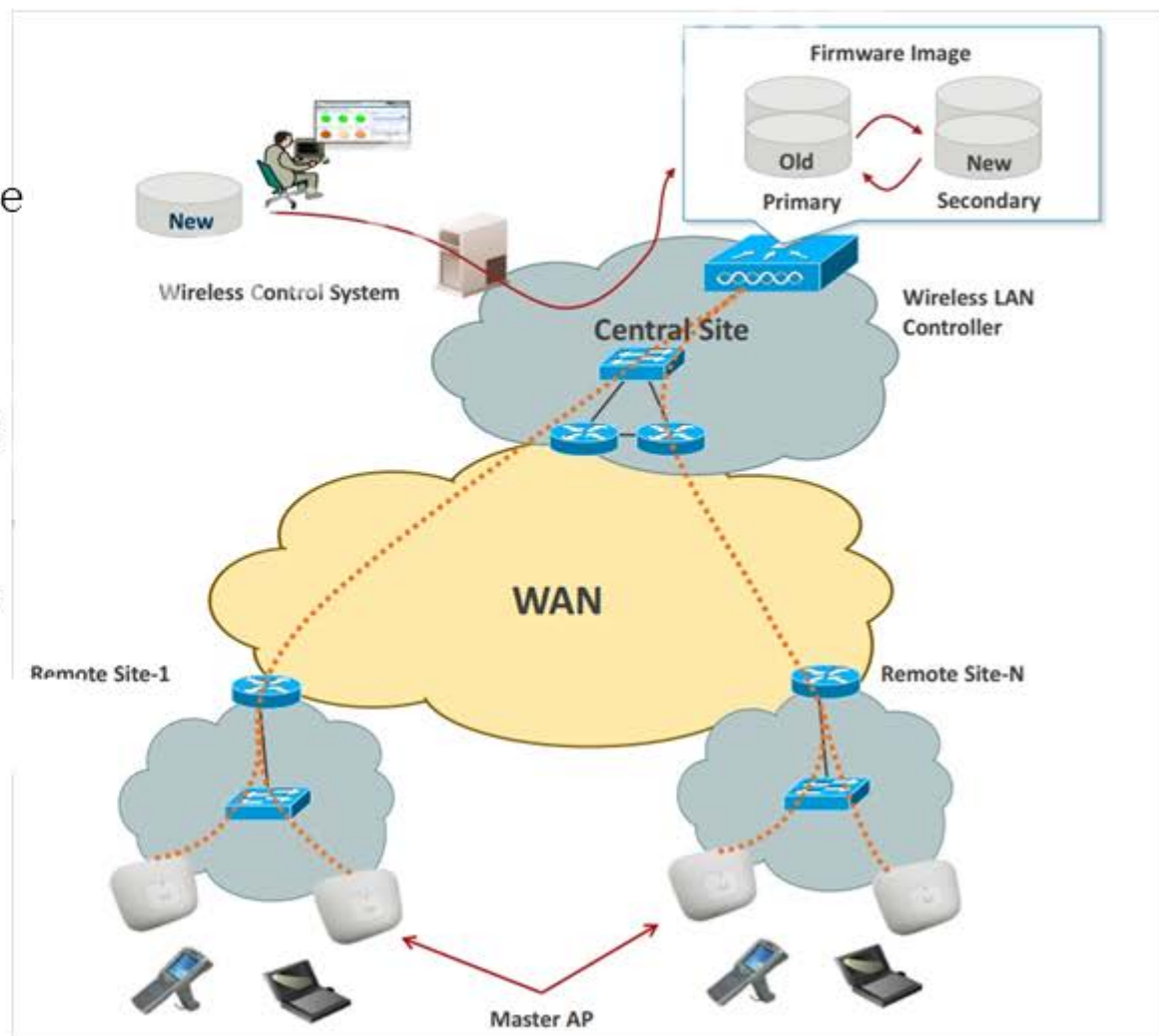
WLAN Id   
Local Split ACL Flex\_Split\_ACL

WLAN Id	WLAN Profile Name	WebAuth ACL	WLAN Id	WLAN Profile Name	LocalSplit ACL
			1	RackMobility	Flex_Split_ACL <input type="button" value="Add"/>

# 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)



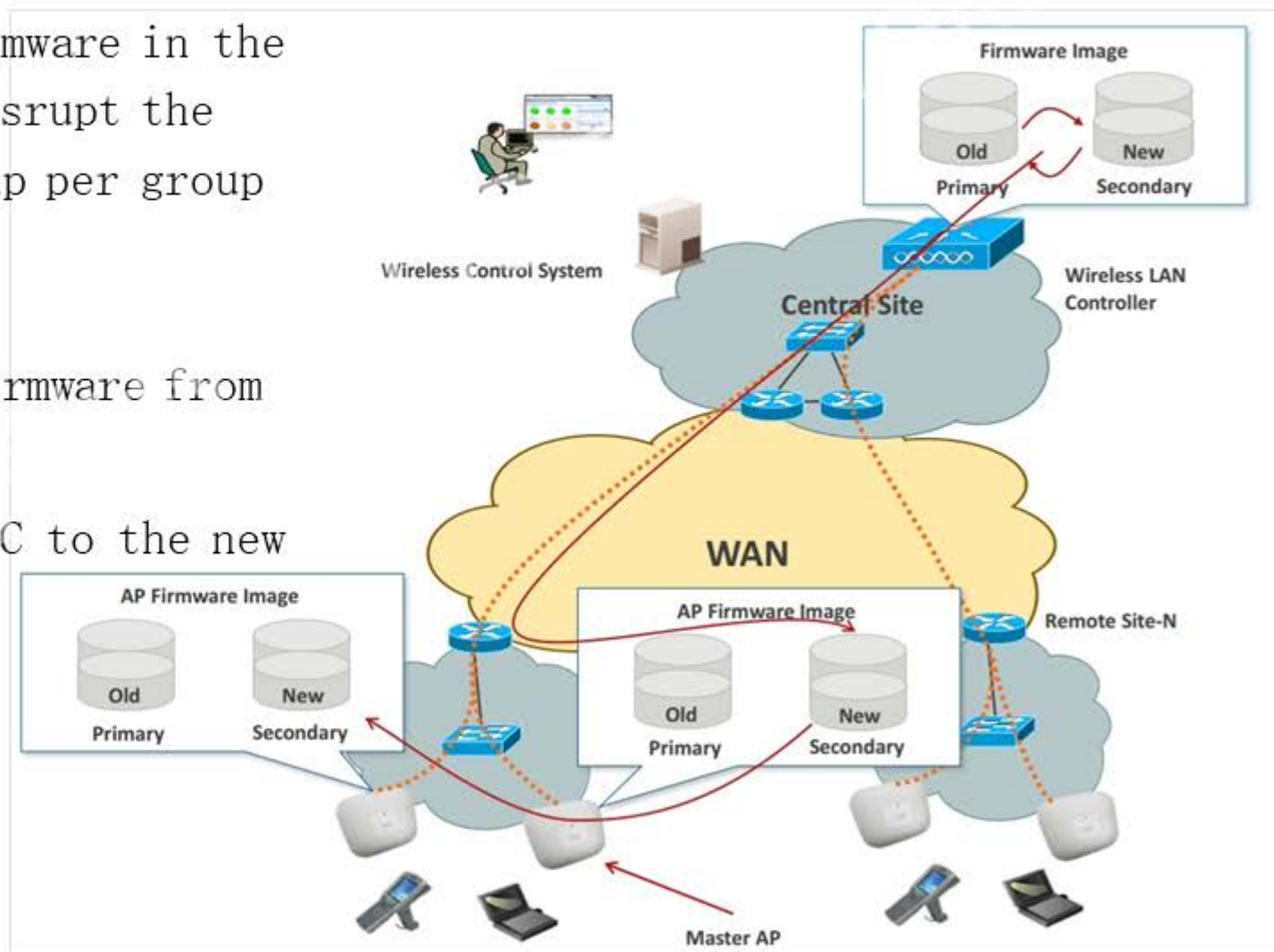
# FlexConnect Smart AP Image Upgrade -2

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 AP firmware 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

Wireless

FlexConnect Groups > Edit 'FlexConnect\_Shanghai\_Site'

General Local Authentication **Image Upgrade** ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count: 44

Upgrade Image: Primary

FlexConnect Master APs

AP Name:

Master AP Name	AP Model	Manual
----------------	----------	--------

# 配置 - 2

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

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WIRELESS' tab is selected and highlighted with a red box. On the left sidebar, 'Global Configuration' is also highlighted with a red box. The main content area is titled 'AP Image Pre-download' and contains four buttons: 'Download Primary', 'Download Backup', 'Interchange Image', and 'Abort Predownload'. To the right, there are several configuration sections: 'Flexconnect Ethernet Fallback', 'Global Telnet SSH', 'Global IPv6 UDP Lite', 'Hyperlocation Config Parameters', and 'BLE Beacon Config Parameters'. Each section contains various settings, checkboxes, and input fields.



3

# FlexConnect Group 实验





## 3.1

# WLAN-VLAN 映射继承顺序

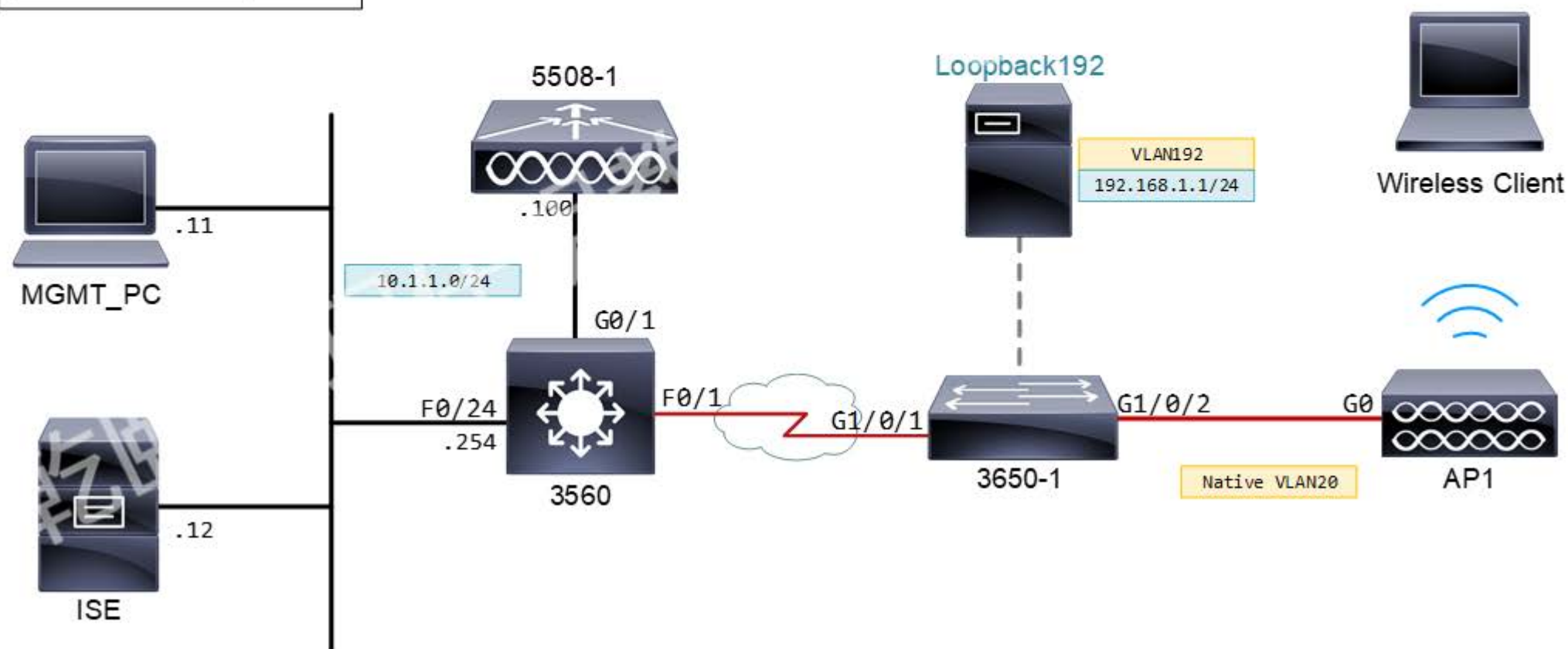


# 拓扑图

图例:

Trunk Links

Access Links



## 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

The screenshot shows the Cisco WLC configuration interface for AP1. The 'FlexConnect' tab is selected, and the 'AP Mode' is set to 'FlexConnect'. The 'Apply' button is highlighted, indicating the configuration is being saved.

**General Tab Configuration:**

- 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
- Network Spectrum Interface Key: 44AEA62298C887B4685D78ED1E2F006F
- 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)D11S
- 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):

**Time Statistics:**

- UP Time: 0 d, 00 h 18 m 39 s
- Controller Associated Time: 0 d, 00 h 04 m 55 s
- Controller Association Latency: 0 d, 00 h 13 m 43 s

**Hardware Reset:**

- Perform a hardware reset on this AP:

**Set to Factory Defaults:**

- Clear configuration on this AP and reset it to factory defaults:

# WLC 新建 Interface - 1

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER' (highlighted with a red box), 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. On the right, there are links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh', along with a 'Home' button. The left sidebar shows a tree view with 'Controller' selected, and 'Interfaces' highlighted with a red box. The main content area displays a table of interfaces with the following data:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
<a href="#">management</a>	10	10.1.1.100	Static	Enabled	::/128
<a href="#">redundancy-management</a>	10	0.0.0.0	Static	Not Supported	
<a href="#">redundancy-port</a>	untagged	0.0.0.0	Static	Not Supported	
<a href="#">service-port</a>	N/A	0.0.0.0	DHCP	Disabled	::/128
<a href="#">virtual</a>	N/A	1.1.1.1	Static	Not Supported	

At the top right of the interface list, it says 'Entries 1 - 5 of 5' and a 'New...' button is highlighted with a red box.

# WLC 新建 Interface - 2

The screenshot shows the Cisco WLC configuration page for creating a new interface. The page has a blue header with the Cisco logo and navigation tabs: MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the right of the header, there are links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh', along with a 'Home' button. A left sidebar contains a 'Controller' menu with options: General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Redundancy, and Internal DHCP Server. The main content area is titled 'Interfaces > New'. It contains two input fields: 'Interface Name' with the value 'deadnet' and 'VLAN Id' with the value '999'. A red box highlights the 'Interface Name' field, and a red circle with the number '1' is placed above it. In the top right corner of the main area, there are '< Back' and 'Apply' buttons. The 'Apply' button is highlighted with a red box, and a red circle with the number '2' is placed above it.

# WLC 新建 Interface - 3

The screenshot shows the Cisco WLC configuration page for a new interface named 'deadnet'. The interface is configured with a MAC address of 58:8d:09:cd:b9:60. The configuration is divided into several sections:

- Configuration:** Guest Lan, Quarantine, Quarantine Vlan Id (0), and NAS-ID (none).
- Physical Information:** Port Number (1), Backup Port (0), Active Port (0), and Enable Dynamic AP Management (unchecked).
- Interface Address:** VLAN Identifier (999), IP Address (9.9.9.9), Netmask (255.255.255.0), Gateway (9.9.9.254), IPv6 Address (::), Prefix Length (128), IPv6 Gateway (::), and Link Local IPv6 Address (fe80::5a8d:9ff:febd:b960/64).
- DHCP Information:** Primary DHCP Server (9.9.9.254) and Secondary DHCP Server (empty).

The values 1, 999, 9.9.9.9, 255.255.255.0, 9.9.9.254, and 9.9.9.254 are highlighted with red boxes in the original image.

# WLC 新建 Interface - 4

The screenshot shows the Cisco WLC configuration page for creating a new interface. The page title is "Interfaces > New". The "Interface Name" field is set to "vlan20" and the "VLAN Id" field is set to "20". Both fields are highlighted with a red box. The left sidebar shows the "Controller" menu with options: General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Redundancy, and Internal DHCP Server. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK, Save Configuration, Ping, Logout, Refresh, and Home.

Interface Name	vlan20
VLAN Id	20

# WLC 新建 Interface - 5

The screenshot displays the Cisco WLC configuration interface for a new interface named 'vlan20'. The configuration is organized into several sections:

- General:** Interface Name: vlan20, MAC Address: 58-8d:09:cd-b9:60.
- Configuration:** Guest Lan, Quarantine, and Quarantine Vlan Id (0) are disabled. NAS-ID is set to none.
- Physical Information:** Port Number is 1, Backup Port is 0, and Active Port is 0. Enable Dynamic AP Management is checked.
- Interface Address:** VLAN Identifier is 20, IP Address is 20.1.1.252, Netmask is 255.255.255.0, and Gateway is 20.1.1.253. IPv6 Address, Prefix Length (128), and IPv6 Gateway are all set to ::.
- DHCP Information:** Primary DHCP Server is 20.1.1.253, and the Secondary DHCP Server is empty.

Red boxes highlight the following fields: Port Number (1), VLAN Identifier (20), IP Address (20.1.1.252), Netmask (255.255.255.0), Gateway (20.1.1.253), and Primary DHCP Server (20.1.1.253).

# WLC 创建 WLAN - 1

The screenshot shows the Cisco WLC configuration page for creating a new WLAN. The page title is "WLANs > New". The configuration fields are as follows:

Type	WLAN
Profile Name	QYT_FlexConnect_PSK
SSID	QYT_FlexConnect_PSK
ID	1

Navigation buttons: < Back, Apply (highlighted with a red box).

Page navigation: Save Configuration | Ping | Logout | Refresh | Home



# WLC 创建 WLAN - 2

The screenshot shows the Cisco WLC configuration interface for editing the WLAN profile 'QYT\_FlexConnect\_PSK'. The 'Security' tab is selected, and the 'Advanced' sub-tab is active. Two red circles with numbers 1 and 2 highlight specific configuration items: the SSID field and the 'Interface/Interface Group(s)' dropdown menu.

**WLANs**

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | Save Configuration | Ping | Logout | Refresh | Home

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: All (2)

Interface/Interface Group(s): deadnet (2)

Multicast Man Feature:  Enabled

Broadcast SSID:  Enabled

NAS-ID: none

# WLC 创建 WLAN - 3

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'QYT\_FlexConnect\_PSK'. The 'Security' tab is selected, and the 'Authentication Key Management' section is expanded. The following table summarizes the configuration options shown:

Option	Enabled
WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/>
WPA2 Encryption (AES)	<input checked="" type="checkbox"/>
WPA2 Encryption (TKIP)	<input type="checkbox"/>
WPA2 Encryption (CCMP256)	<input type="checkbox"/>
WPA2 Encryption (GCMP128)	<input type="checkbox"/>
WPA2 Encryption (GCMP256)	<input type="checkbox"/>
OSEN Policy	<input type="checkbox"/>
802.1X	<input type="checkbox"/>
CKM	<input type="checkbox"/>
PSK	<input checked="" type="checkbox"/>
FT 802.1X	<input type="checkbox"/>
FT PSK	<input type="checkbox"/>
SUITEB-1X	<input type="checkbox"/>
SUITEB192-1X	<input type="checkbox"/>

Additional configuration details:

- PMF: Disabled
- Authentication Key Management: 19
- PSK Format: ASCII
- PSK Key: [Redacted]

# WLC 创建 WLAN - 4

WLANs > Edit 'QYT\_FlexConnect\_PSK'

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration Ping Logout Refresh Home

WLANs

- WLANs
- Advanced

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

< Back Apply

# 客户端连接测试



```
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 . . . . . :
    本地连接 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

The screenshot shows the Cisco Wireless configuration page for a FlexConnect Group named 'default-flex-group'. The interface includes a navigation menu on the left and a main configuration area with several tabs: General, Local Authentication, Image Upgrade, ACL Mapping, Control DHCP, WLAN VLAN mapping, and WLAN AVC mapping. The 'WLAN VLAN mapping' tab is selected and highlighted with a red box and a circled '3'. In the left navigation menu, 'FlexConnect Groups' is highlighted with a red box and a circled '2'. The 'WLAN Support' section has a checked box and a 'Native VLAN ID' field set to '20', both highlighted with a red box and a circled '4'. An 'Apply' button is highlighted with a red box and a circled '5'. The 'WLAN VLAN Mapping' section contains input fields for 'WLAN Id' (1) and 'Vlan Id' (1), with an 'Add' button below them. A table below shows columns for 'WLAN Id', 'WLAN Profile Name', and 'Vlan'.

Wireless

FlexConnect Groups > Edit 'default-flex-group'

MONITOR WLANS CONTROL WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration | Ping | Logout | Refresh

Home

Access Points

Advanced

Mesh

ATF

2 Flex 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 Local Authentication Image Upgrade ACL Mapping Control DHCP 3 WLAN VLAN mapping 5 Apply WLAN AVC mapping

VLAN Support 4  Native VLAN ID 20

Override VLAN on AP

WLAN VLAN Mapping

WLAN Id 1

Vlan Id 1

Add

WLAN Id	WLAN Profile Name	Vlan
---------	-------------------	------

# 配置 WLAN VLAN 映射 - 2

Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | Home

Wireless

- Access Points
- 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

FlexConnect Groups > Edit 'default-flex-group' Apply

General | Local Authentication | Image Upgrade | ACL Mapping | Central DHCP | **WLAN VLAN mapping** | WLAN AVC mapping

VLAN Support  Native VLAN ID: 20

Override VLAN on AP

WLAN VLAN Mapping

WLAN Id: 1  
Vlan Id: 10  
Add

WLAN Id	WLAN Profile Name	Vlan
1	QYT_FlexConnect_PSK	10

```

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
GigabitEthernet0.10 unassigned      YES  unset    up          up
GigabitEthernet0.20 unassigned      YES  unset    up          up
  
```

# 客户端连接测试



```

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

The screenshot displays the Cisco configuration interface for an AP. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROL', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WIRELESS' tab is selected and highlighted with a red box and a circled '1'. The left sidebar shows the 'Wireless' menu with 'Access Points' selected and 'All APs' highlighted with a red box and a circled '2'. The main content area is titled 'All APs > Details for AP1' and features a 'FlexConnect' tab highlighted with a red box and a circled '3'. Within the FlexConnect configuration, the 'VLAN Support' checkbox is checked, and the 'Make VLAN AP Specific' dropdown is set to 'Make VLAN AP Specific'. The 'Inheritance Level' is set to 'Group-Specific'. The 'Native VLAN ID' is set to '20', and the 'VLAN Mappings' link is highlighted with a red box and a circled '4'. Other fields include 'FlexConnect Group Name' (default-flex-group) and 'VLAN Template Name' (none).



# AP 下直接修改报错

Save Configuration | Ping | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK 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

10.1.1.100 显示:

20 Native vlan should be AP specific

3 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.

< Back Apply

# Make VLAN AP Special

The screenshot shows the Cisco Wireless LAN Controller configuration interface for AP1. The 'Advanced' tab is selected, and the 'Make VLAN AP Specific' option is highlighted with a red box and a circled '1'. The 'Go' button is also highlighted with a red box and a circled '2'. The 'Native VLAN ID' is set to 20. The 'VLAN Support' checkbox is checked. The 'Inheritance Level' is set to 'Group-Specific'. The 'FlexConnect Group Name' is 'default-flex-group'. The 'VLAN Template Name' is 'none'. The 'VLAN Mappings' button is visible next to the 'Native VLAN ID' field.

Wireless

All APs > Details for AP1

< Back Apply

General Credentials Interfaces High Availability Inventory FlexConnect Advanced

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](#)

# AP 下将 WLAN 映射到 VLAN20

Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

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**

AP Name AP1

Base Radio MAC 68:99:cd:06:5f:30

#### WLAN VLAN Mapping

Make AP Specific

WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance	
<input type="checkbox"/>	1	QYT_FlexConnect_PSK	20	no	AP-specific

#### Centrally switched Wlans

WLAN Id	SSID	VLAN ID

#### AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
20	none	none

#### Group level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL

Foot Notes

1. Vlan does not take effect for NAT-PAT enabled WLANs.

# 客户端连接测试



```
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

Wireless

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Save Configuration | Ping | Logout | Refresh

Home

FlexConnect Groups > Edit 'default-flex-group'

1 Apply

2

General | Local Authentication | Image Upgrade | ACL Mapping | Central DHCP | **WLAN VLAN mapping** | WLAN AVC mapping

VLAN Support  Native VLAN ID 20

Override VLAN on AP

WLAN VLAN Mapping

WLAN Id 1

Vlan Id 1

Add

```
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
```

WLAN Id	WLAN Profile Name	Vlan
1	QYT_FlexConnect_PSK	30

3

4

1 Profiles

**FlexConnect Groups**

FlexConnect ACLs

FlexConnect VLAN Templates

OEAP ACLs

Network Lists

802.11a/n/ac

802.11b/g/n

Media Stream

# 启用“Override VLAN on AP”

Save Configuration | Ping | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Wireless FlexConnect Groups > Edit 'default-flex-group' 2 Apply

General Local Authentication Image Upgrade ACL Mapping Central DHCP **WLAN VLAN mapping** WLAN AVC mapping

VLAN Support 1  Native VLAN ID 20

Override VLAN on AP

WLAN VLAN Mapping

WLAN Id  Vlan Id

```

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
  
```

WLAN Id	WLAN Profile Name	Vlan
1	QYT_FlexConnect_PSK	30 <input checked="" type="checkbox"/>

# 客户端连接测试



```
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 . . . . . :
    本地连接 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

10.1.1.100 显示:

20. Native vlan should be AP specific.

确定

< Back Apply

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



# 查看报错

The screenshot shows the Cisco Meraki configuration interface for 'All APs > Details for AP1'. The 'Advanced' tab is selected, and the 'VLAN Support' checkbox is checked. A dropdown menu is set to 'Make VLAN AP Specific' (marked with a red circle 1), and a 'Go' button is highlighted (marked with a red circle 2). The 'Native VLAN ID' is set to 20. A modal error message is displayed, titled '10.1.1.100 显示:', containing the following text:

```
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.
```

The error message has a '确定' (OK) button at the bottom right.



3.2

# VLAN Override



# WLC 添加 Radius 服务器 - 1

The screenshot displays the Cisco WLC configuration page for adding a new RADIUS Accounting Server. The left sidebar shows the navigation menu with 'AAA' expanded and 'Accounting' selected. The main content area is titled 'RADIUS Accounting Servers > New' and contains the following configuration fields:

- Server Index (Priority): 1
- Server IP Address(Ipv4/Ipv6): 10.1.1.12
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Port Number: 1813
- Server Status: Enabled
- Server Timeout: 2 seconds
- Network User:  Enable
- Tunnel Proxy:  Enable
- IPSec:  Enable

At the top right of the configuration area, there are buttons for '< Back' and 'Apply'. The 'Apply' button is highlighted with a red box and a callout '4'. Other callouts include '1' for the 'Accounting' menu item, '2' for the 'Server Index (Priority)' dropdown, and '3' for the 'Shared Secret' and 'Confirm Shared Secret' text input fields.



# WLC 添加 Radius 服务器 - 2

The screenshot shows the Cisco WLC configuration page for adding a new RADIUS authentication server. The interface includes a top navigation bar with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted with a red box and '1'), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a 'Security' sidebar has 'Authentication' highlighted with a red box and '2'. The main area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

- Server Index (Priority): 1 (highlighted with a red box and '3')
- Server IP Address(Ipv4/Ipv6): 10.1.1.12 (highlighted with a red box and '3')
- Shared Secret Format: ASCII (highlighted with a red box and '4')
- Shared Secret: [Redacted with dots] (highlighted with a red box and '4')
- Confirm Shared Secret: [Redacted with dots] (highlighted with a red box and '4')
- Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled (highlighted with a red box and '5')
- Support for CoA: Enabled (highlighted with a red box and '5')
- Server Timeout: 2 seconds
- Network User:  Enable
- Management:  Enable
- Management Retransmit Timeout: 2 seconds
- Tunnel Proxy:  Enable
- IPSec:  Enable

At the top right, there are links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'. At the bottom right, there are '< Back' and 'Apply' buttons, with 'Apply' highlighted by a red box and '6'.

# WLC 新建 WLAN - 1



The screenshot displays the Cisco WLC configuration interface for creating a new WLAN. The page title is "WLANs > New". The configuration fields are as follows:

Field	Value
Type	WLAN
Profile Name	QYT_FlexConnect_Dot1x
SSID	QYT_FlexConnect_Dot1x
ID	2

The Profile Name and SSID fields are highlighted with a red box. The interface includes a navigation menu on the left with "WLANs" and "Advanced" options. The top navigation bar includes "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", "HELP", and "FEEDBACK". The top right corner has "Save Configuration", "Ping", "Logout", and "Refresh" links. The bottom right corner has "< Back" and "Apply" buttons.

# WLC 新建 WLAN - 2

The screenshot shows the Cisco WLC configuration interface for editing a WLAN profile named 'QYT\_FlexConnect\_Dot1x'. The 'Security' tab is selected, and several fields are highlighted with red boxes:

- Status:**  Enabled
- Interface/Interface Group(G):** deadnet

Other configuration details include:

- Profile Name: QYT\_FlexConnect\_Dot1x
- Type: WLAN
- SSID: QYT\_FlexConnect\_Dot1x
- Security Policies: [WPA2][Auth(802.1X)]
- Radio Policy: All
- Multicast Man Feature:  Enabled
- Broadcast SSID:  Enabled
- NAS-ID: none

# WLC 新建 WLAN - 3

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'QYT\_FlexConnect\_Dot1x'. The 'Security' tab is selected, and the 'AAA Servers' sub-tab is active. The configuration includes:

- General:** Security, QoS, Policy-Mapping, Advanced
- Layer 2:** Layer 3, AAA Servers
- AAA Servers:** Select AAA servers below to override use of default servers on this WLAN
- RADIUS Servers:**
  - RADIUS Server Overwrite interface:  Enabled
  - Authentication Servers:  Enabled
  - Accounting Servers:  Enabled
  - EAP Parameters: Enable
  - Server 1: IP: 10.1.1.12, Port: 1812 (selected)
  - Server 2: None
  - Server 3: None
  - Server 4: None
  - Server 5: None
  - Server 6: None
- RADIUS Server Accounting:** Interim Update  Interim Interval 0 Seconds
- LDAP Servers:**

# WLC 新建 WLAN - 4

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'QYT\_FlexConnect\_Dot1x'. The 'Advanced' tab is selected and highlighted with a red box. The 'Allow AAA Override' checkbox is also checked and highlighted with a red box. Other configuration options include Coverage Hole Detection (Enabled), Session Timeout (1800 secs), Aironet IE (Enabled), Diagnostic Channel (Enabled), Override Interface ACL (IPv4: None, IPv6: None), Layer2 Ad (None), URL ACL (None), P2P Blocking Action (Disabled), Client Exclusion (Enabled, 60 secs), Maximum Allowed Clients (0), Static IP Tunneling (Disabled), Wi-Fi Direct Clients Policy (Disabled), Maximum Allowed Clients Per AP Radio (200), and Clear HotSpot Configuration (Enabled). On the right side, DHCP settings (Server, Addr. Assignment, Override, Required), OEAP Split Tunnel (Enabled), Management Frame Protection (MFP) Client Protection (Optional), DTIM Period (802.11a/n: 1, 802.11b/g/n: 1), and NAC State (None) are visible.





# WLC 新建 WLAN - 5

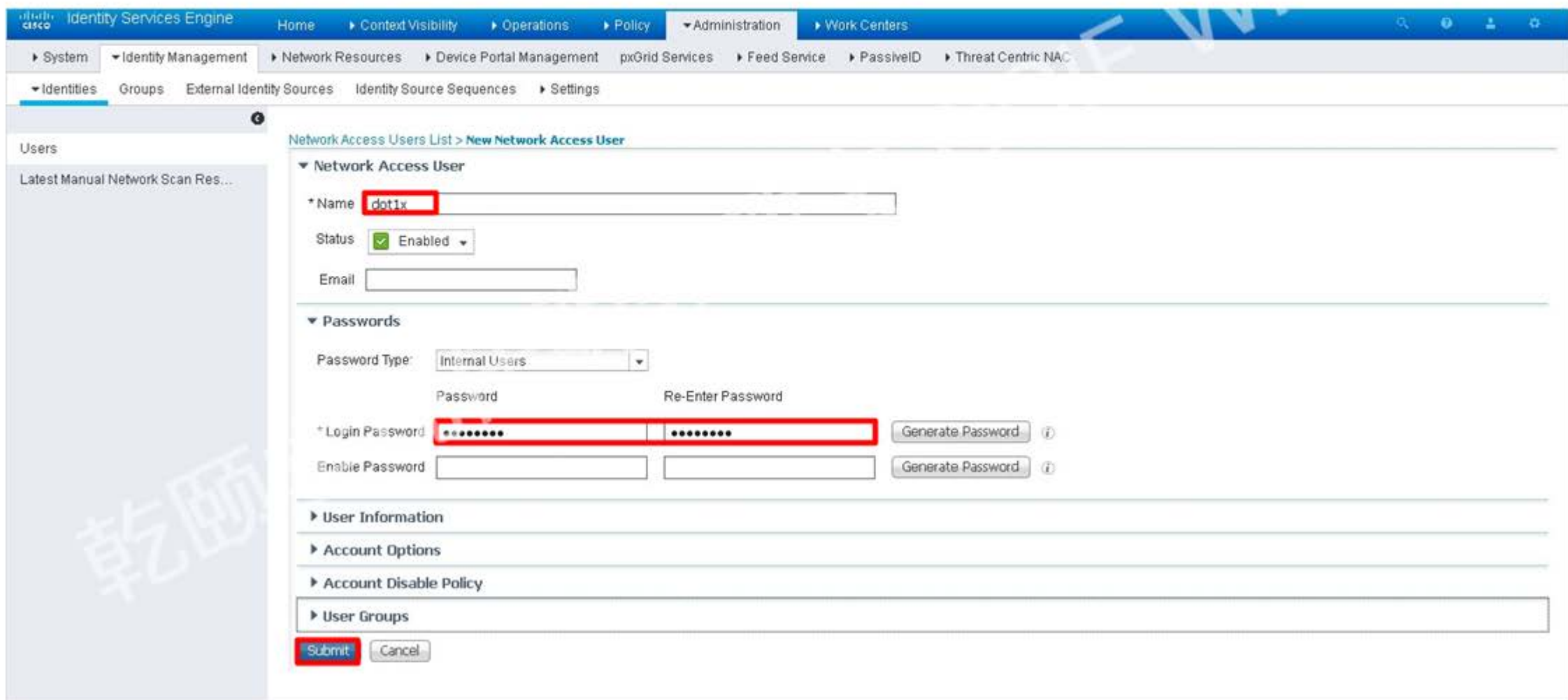
The screenshot shows the Cisco WLC configuration interface for a WLAN named 'QYT\_FlexConnect\_Dot1x'. The 'Advanced' tab is selected, and the 'FlexConnect' section is expanded. A red box highlights the 'FlexConnect Local Switching' checkbox, which is checked and labeled with a '1'. Another red box highlights the 'Apply' button in the top right corner, labeled with a '2'. Other settings include 'FlexConnect Local Auth', 'Learn Client IP Address', 'Vlan based Central Switching', 'Central DHCP Processing', 'Override DNS', 'NAT-PAT', 'Central Assoc', 'Lync Server' (Disabled), 'Neighbor List' (Enabled), and 'Neighbor List Dual Band' (Enabled). The right side of the page shows sections for 'Local Client Profiling', 'PMIP', 'Universal AP Admin Support', and '11v BSS Transition Support'.

# ISE 创建 Network Device

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > Network Devices. The 'Network Devices' menu item is highlighted with a red box. The main content area is titled 'Network Devices List > New Network Device'. The form contains the following fields and values:

- Name: WLC (highlighted with a red box)
- Description: (empty)
- IP Address: 10.1.1.100 / 32 (highlighted with a red box)
- Device Profile: Cisco (dropdown menu)
- Model Name: (dropdown menu)
- Software Version: (dropdown menu)
- Network Device Group: (empty)
- Device Type: All Device Types (dropdown menu) with a 'Set To Default' button
- Location: All Locations (dropdown menu) with a 'Set To Default' button
- RADIUS Authentication Settings (checked):
  - Enable Authentication Settings: (checked)
  - Protocol: RADIUS
  - Shared Secret: Cisc0123 (highlighted with a red box) with a 'Hide' button
  - Enable KeyWrap:  (unchecked)

# ISE 创建用户



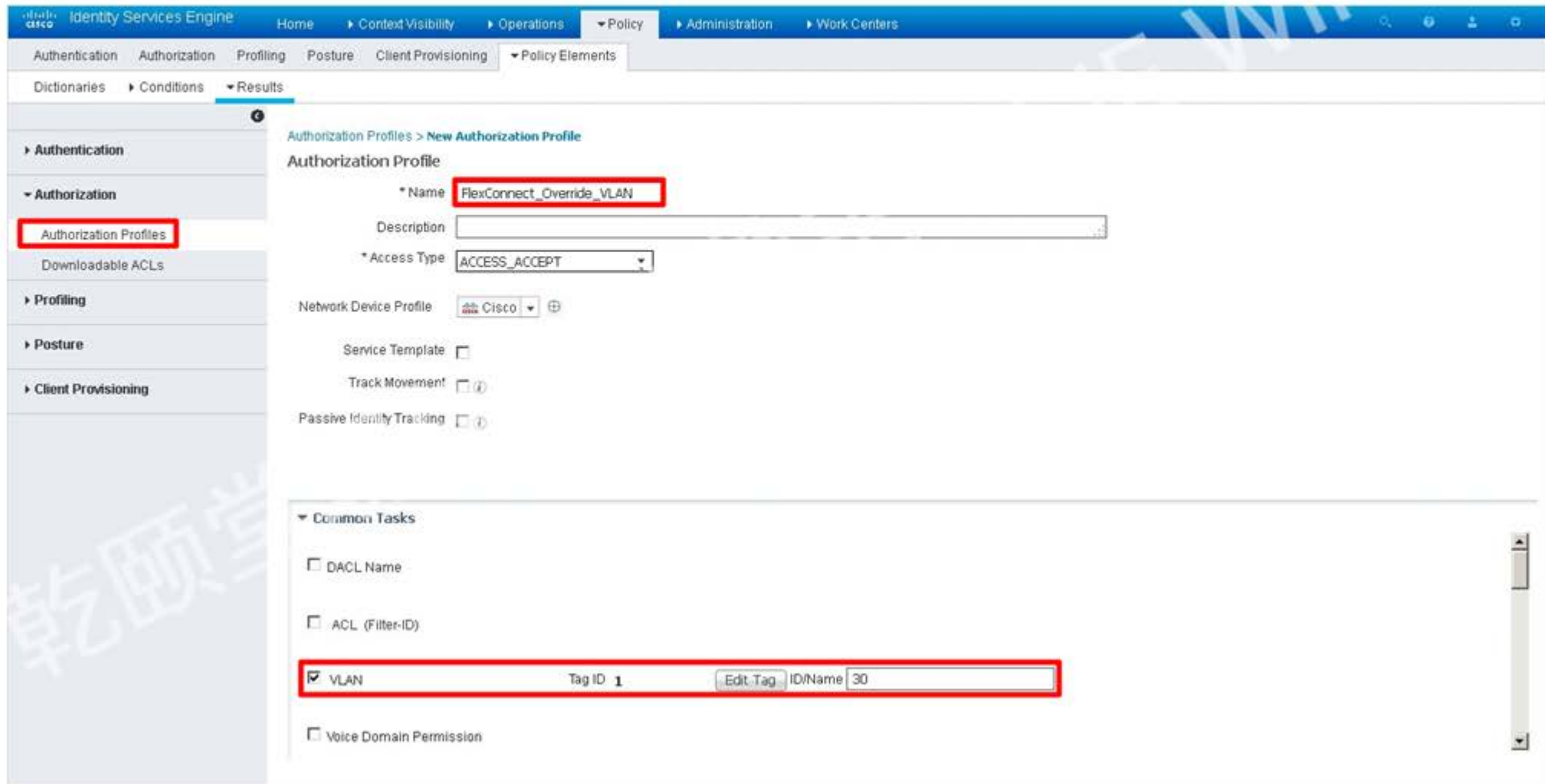
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Identities' selected. The main content area is titled 'Network Access Users List > New Network Access User'.

The configuration form includes the following sections:

- Network Access User**
  - \* Name: dot1x
  - Status:  Enabled
  - Email: [Empty field]
- Passwords**
  - Password Type: Internal Users
  - Fields for Password and Re-Enter Password, with the Login Password field highlighted in red.
  - Buttons: Generate Password (i)
- User Information**
- Account Options**
- Account Disable Policy**
- User Groups**

At the bottom of the form are 'Submit' and 'Cancel' buttons.

# ISE 创建授权 Profile



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, and Client Provisioning. Under Authorization, the 'Authorization Profiles' option is selected and highlighted with a red box. The 'New Authorization Profile' configuration page is displayed, with the following fields and options:

- Name:** FlexConnect\_Override\_VLAN (highlighted with a red box)
- Description:** (empty text field)
- Access Type:** ACCESS\_ACCEPT (dropdown menu)
- Network Device Profile:** Cisco (dropdown menu)
- Service Template:**
- Track Movement:**
- Passive Identity Tracking:**

Under the 'Common Tasks' section, the 'VLAN' checkbox is checked and highlighted with a red box. The configuration for this task is as follows:

<input checked="" type="checkbox"/> VLAN	Tag ID 1	Edit Tag	ID/Name 30
--	----------	----------	------------

Other options in the 'Common Tasks' section include 'DAACL Name', 'ACL (Filter-ID)', and 'Voice Domain Permission', all of which are unchecked.



# 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](#)

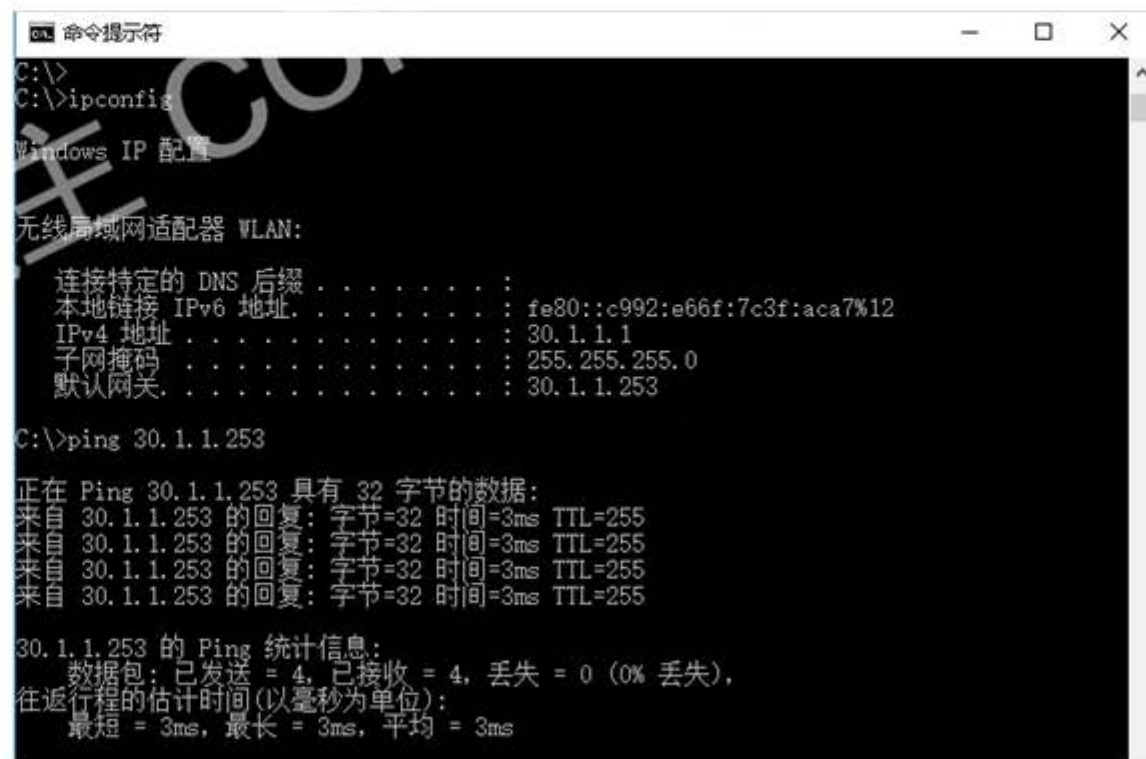
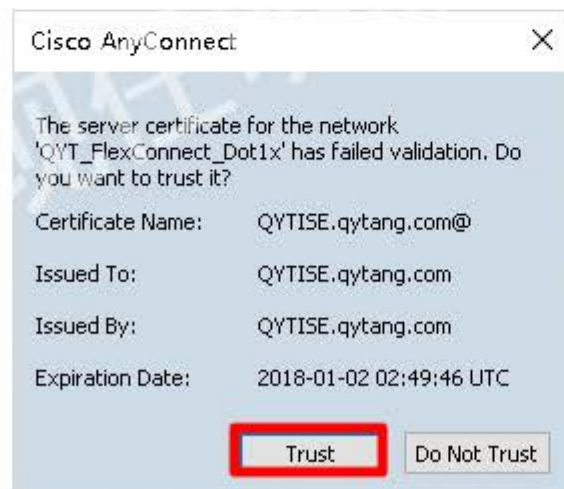
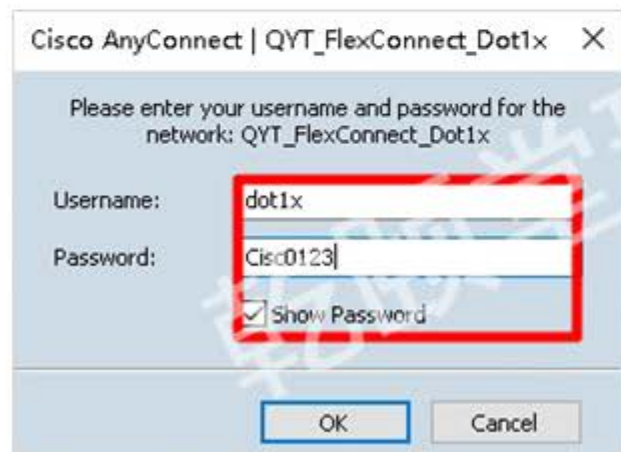
First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	WLC_FlexConnect_Dot1x	(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



# 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
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

The screenshot shows the Cisco WLC Monitor interface. The left sidebar contains navigation options like Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Clients, Sleeping Clients, Multicast, Applications, Lync, and Local Profiling. The main content area is divided into 'General' and 'AVC Statistics' tabs. Under 'AVC Statistics', there are two sections: 'Client Properties' and 'AP Properties'. In the 'Client Properties' section, the 'VLAN ID' field is highlighted with a red box and contains the value '30'. In the 'AP Properties' section, the 'Data Switching' and 'Authentication' fields are highlighted with a red box, showing 'Local' and 'Central' respectively.

Client Properties		AP Properties	
MAC Address	a0:63:91:a6:b5:fb	AP Address	68:99:cd:06:5f:30
IPv4 Address	30.1.1.1	AP Name	AP1
IPv6 Address		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

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, and Client Provisioning. The 'Results' sub-menu is active. The left sidebar shows the navigation tree with 'Authorization' expanded to 'Authorization Profiles'. The main content area displays the configuration for the 'FlexConnect\_Override\_VLAN' authorization profile. The 'Name' field is 'FlexConnect\_Override\_VLAN', 'Access Type' is 'ACCESS\_ACCEPT', and 'Network Device Profile' is 'Cisco'. The 'Common Tasks' section is expanded, showing a table of tasks. The 'VLAN' task is checked and highlighted with a red box. The 'Tag ID' is '1' and the 'ID/Name' is '10'. Other tasks like 'DAACL Name', 'ACL (Filter-ID)', and 'Voice Domain Permission' are unchecked.

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

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > FlexConnect\_Override\_VLAN

Authorization Profile

Name FlexConnect\_Override\_VLAN

Description

Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DAACL Name

ACL (Filter-ID)

VLAN Tag ID 1 Edit Tag ID/Name 10

Voice Domain Permission



# AP 没有授权 VLAN

```
AP1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status
BVI1	20.1.1.1	YES	DHCP	up
GigabitEthernet0	unassigned	NO	unset	up
GigabitEthernet0.20	unassigned	YES	unset	up
GigabitEthernet0.30	unassigned	YES	unset	up

# 查看 AP 信息

The screenshot displays the Cisco WLC Monitor interface. The top navigation bar includes 'MONITOR' (highlighted with a red box and a '1' in a circle), 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'Monitor' menu with 'Clients' highlighted (marked with a red box and a '2' in a circle). The main content area is divided into 'General' and 'AVC Statistics' tabs. Under 'Client Properties', the 'Client Properties' section shows the following details:

Client Properties	Value
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

The 'AP Properties' section shows the following details for AP1:

AP Properties	Value
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

The 'VLAN ID' field in the Client Properties section is highlighted with a red box, indicating the VLAN override configuration.

# AP 添加 VLAN (子接口)



Wireless

FlexConnect Groups > Edit 'default-flex-group'

MONITOR WLANs CONTROL WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Ping Logout Refresh Home

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

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping WLAN AVC mapping

**AAA VLAN-ACL mapping** WLAN-ACL mapping Policies

AAA VLAN ACL Mapping

Vlan Id **10**  
Ingress ACL none  
Egress ACL none  
**Add**

```

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
  
```

Vlan Id	Ingress ACL	Egress ACL
10	none	none

# 客户连接测试



```
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 . . . . . :
    本地连接 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)

The screenshot shows the Cisco configuration interface for FlexConnect Groups. The page title is "FlexConnect Groups > Edit 'default-flex-group'". The "ACL Mapping" tab is selected, and the "AAA VLAN-ACL mapping" sub-tab is active. The "AAA VLAN ACL Mapping" section contains a table with the following data:

Vlan Id	Ingress ACL	Egress ACL	
0	none	none	
10	none	none	<a href="#">Remove</a>

The "Remove" button for the entry with Vlan Id 10 is highlighted with a red box. The left sidebar shows the navigation menu with "FlexConnect Groups" expanded.



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

The screenshot shows the Cisco WLAN configuration interface for the WLAN 'QYT\_FlexConnect\_Dot1x'. The 'Advanced' tab is selected, and the 'Vlan based Central Switching' option is checked and highlighted with a red box and a '2' in a circle. The 'Policy-Mapping' tab is also highlighted with a red box and a '1' in a circle. The 'Apply' button is highlighted with a red box and a '3' in a circle. The interface includes a navigation menu on the left with 'WLANs' and 'Advanced' options. The main configuration area is divided into sections: FlexConnect, Lync, 11k, Local Client Profiling, PMIP, Universal AP Admin Support, and 11v BSS Transition Support. The 'FlexConnect' section includes options for Local Switching, Local Auth, Learn Client IP Address, Vlan based Central Switching, Central DHCP Processing, Override DNS, NAT-PAT, and Central Assoc. The 'Lync' section has a Lync Server dropdown set to 'Disabled'. The '11k' section has options for Neighbor List and Neighbor List Dual Band. The 'Local Client Profiling' section has options for DHCP and HTTP Profiling. The 'PMIP' section has options for PMIP Mobility Type, PMIP NAI Type (Hexadecimal), PMIP Profile (None), and PMIP Realm. The 'Universal AP Admin Support' section has a checkbox for Universal AP Admin. The '11v BSS Transition Support' section has options for BSS Transition, Optimized Roaming Disassociation Timer (set to 40), and BSS Max Idle Service.

# ISE 授权 VLAN10

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The current page is 'Authorization Profiles > FlexConnect\_Override\_VLAN'. The 'Authorization Profile' configuration is shown with the following fields:

- \* Name: FlexConnect\_Override\_VLAN
- Description: (empty)
- \* Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Passive Identity Tracking:

Under the 'Common Tasks' section, the 'VLAN' checkbox is checked, and the 'Tag ID' is set to 1 and 'ID/Name' is set to 10. This configuration is highlighted with a red box.

# 客户连接测试



```
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 . . . . . :
    本地连接 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

The screenshot displays the Cisco WLC GUI interface. The top navigation bar includes 'MONITOR', 'WLAN', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows a 'Monitor' menu with options like 'Summary', 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', 'Rogues', 'Clients', 'Sleeping Clients', 'Multicast', 'Applications', 'Lync', and 'Local Profiling'. The main content area is divided into 'General' and 'AVC Statistics' tabs. The 'Client Properties' section shows the following details:

Property	Value
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

The 'AP Properties' section shows the following details:

Property	Value
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

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, and Client Provisioning. The 'Policy Elements' sub-menu is expanded to show 'Results'. The left sidebar has sections for Authentication, Authorization (selected), Profiling, Posture, and Client Provisioning. The 'Authorization' section is further expanded to show 'Authorization Profiles' and 'Downloadable ACLs'. The main content area is titled 'Authorization Profiles > FlexConnect\_Override\_VLAN' and 'Authorization Profile'. It contains the following fields:

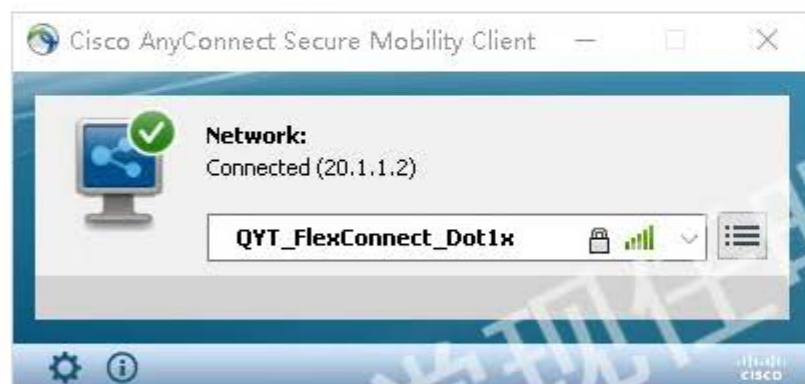
- \* Name: FlexConnect\_Override\_VLAN
- Description: (empty text box)
- \* Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Passive Identity Tracking:

Below these fields is the 'Common Tasks' section, which includes a list of tasks with checkboxes and input fields:

- DACL Name
- ACL (Filter-ID)
- VLAN Tag ID 1 Edit Tag ID/Name 20
- Voice Domain Permission

The 'VLAN' task is highlighted with a red box, indicating it is the active configuration point for VLAN 20.

# 客户连接测试



```

命令提示符
C:\>ipconfig

C:\>ipconfig

Windows IP 配置

无线局域网适配器 WLAN:

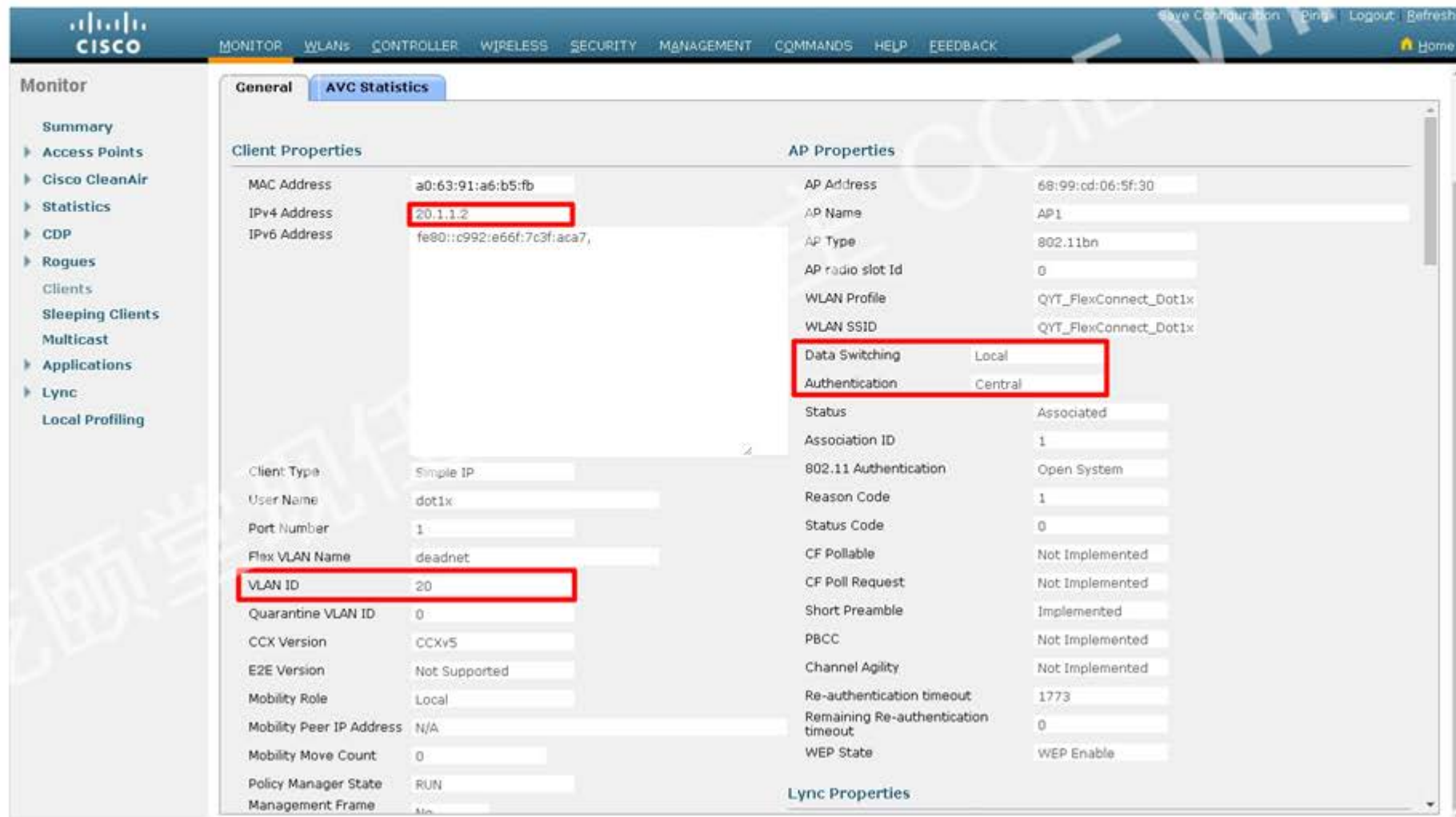
    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址 . . . . . : fe80::c992:e66f:7c3f:aca7%12
    IPv4 地址 . . . . . : 20.1.1.2
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 20.1.1.253

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



The screenshot displays the Cisco WLC GUI, specifically the 'AVC Statistics' page under the 'Monitor' tab. The page is divided into several sections: 'Client Properties', 'AP Properties', and 'Lync Properties'. The 'Client Properties' section shows the following information:

Property	Value
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	No

The 'AP Properties' section shows the following information:

Property	Value
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

The 'Lync Properties' section is currently empty.

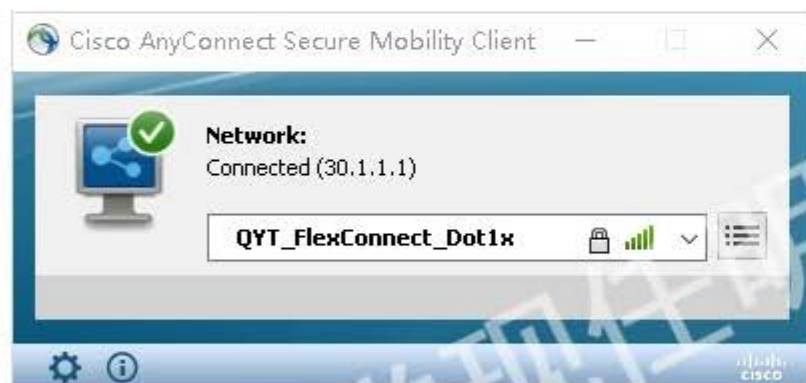
# ISE 授权 VLAN30

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with Authentication, Authorization (selected), Profiling, Posture, and Client Provisioning. Under Authorization, there are links for Authorization Profiles and Downloadable ACLs. The main content area is titled 'Authorization Profiles > FlexConnect\_Override\_VLAN' and shows the configuration for an Authorization Profile. The fields are: Name: FlexConnect\_Override\_VLAN, Description: (empty), Access Type: ACCESS\_ACCEPT, Network Device Profile: Cisco, Service Template: (unchecked), Track Movement: (unchecked), and Passive Identity Tracking: (unchecked). Below these fields is a 'Common Tasks' section with a table of tasks. The 'VLAN' task is checked and highlighted with a red box. The table has columns for the task name, Tag ID, and ID/Name.

Task Name	Tag ID	ID/Name
<input checked="" type="checkbox"/> VLAN	1	30
<input type="checkbox"/> Voice Domain Permission		



# 客户连接测试



```
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

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK 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	

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

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

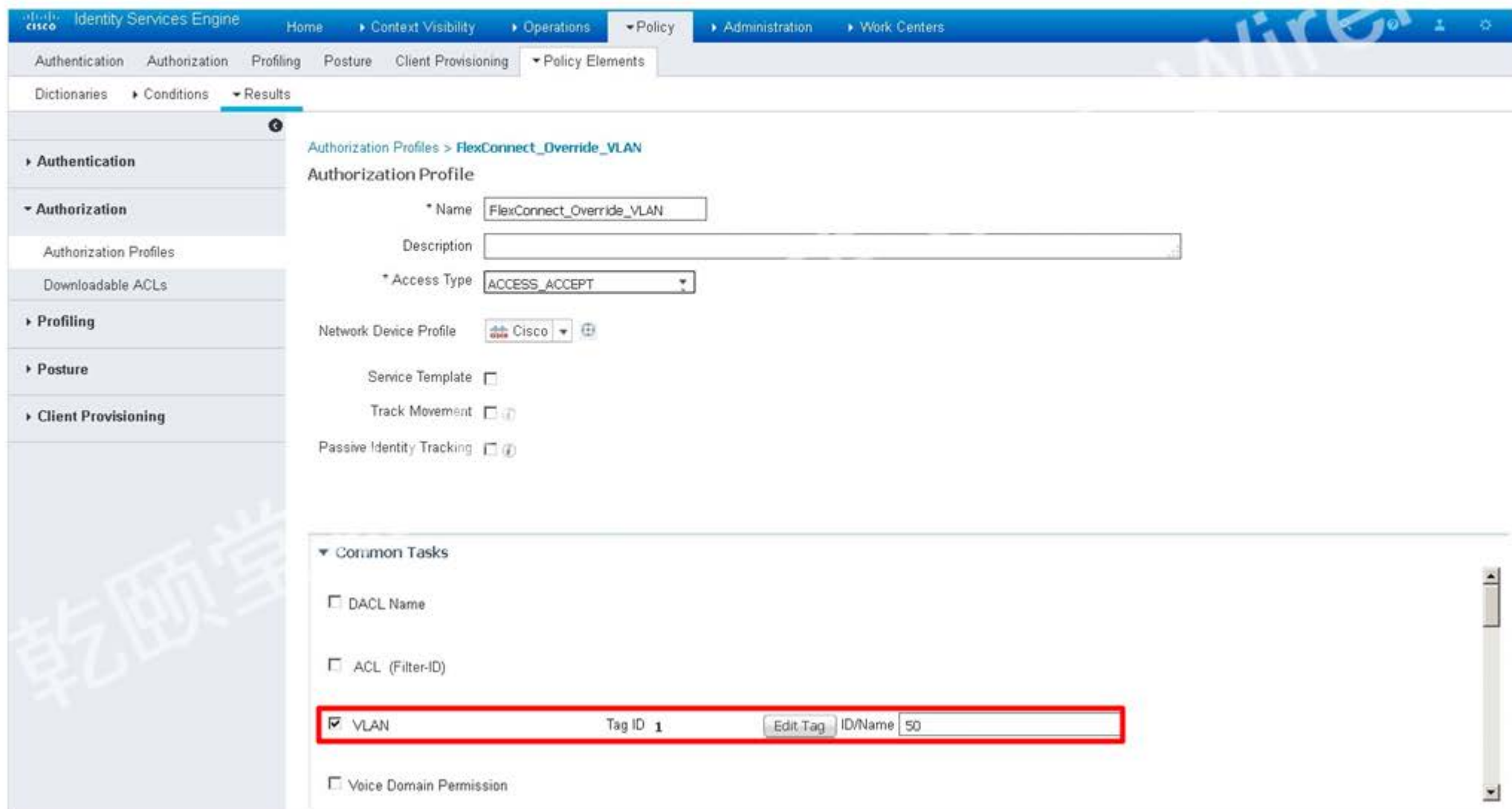
Mobility Move Count: 0

Policy Manager State: RUN

Management Frame: No

Lync Properties

# ISE 授权 VLAN50



The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The navigation menu on the left includes Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > FlexConnect\_Override\_VLAN' and shows the configuration for an Authorization Profile. The 'Name' field is set to 'FlexConnect\_Override\_VLAN', and the 'Access Type' is set to 'ACCESS\_ACCEPT'. The 'Network Device Profile' is set to 'Cisco'. The 'Common Tasks' section is expanded, and the 'VLAN' checkbox is checked, with the 'Tag ID' set to '1' and the 'ID/Name' set to '50'. A red box highlights the 'VLAN' checkbox and its associated fields.

Authorization Profiles > FlexConnect\_Override\_VLAN

Authorization Profile

\* Name FlexConnect\_Override\_VLAN

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

ACL (Filter-ID)

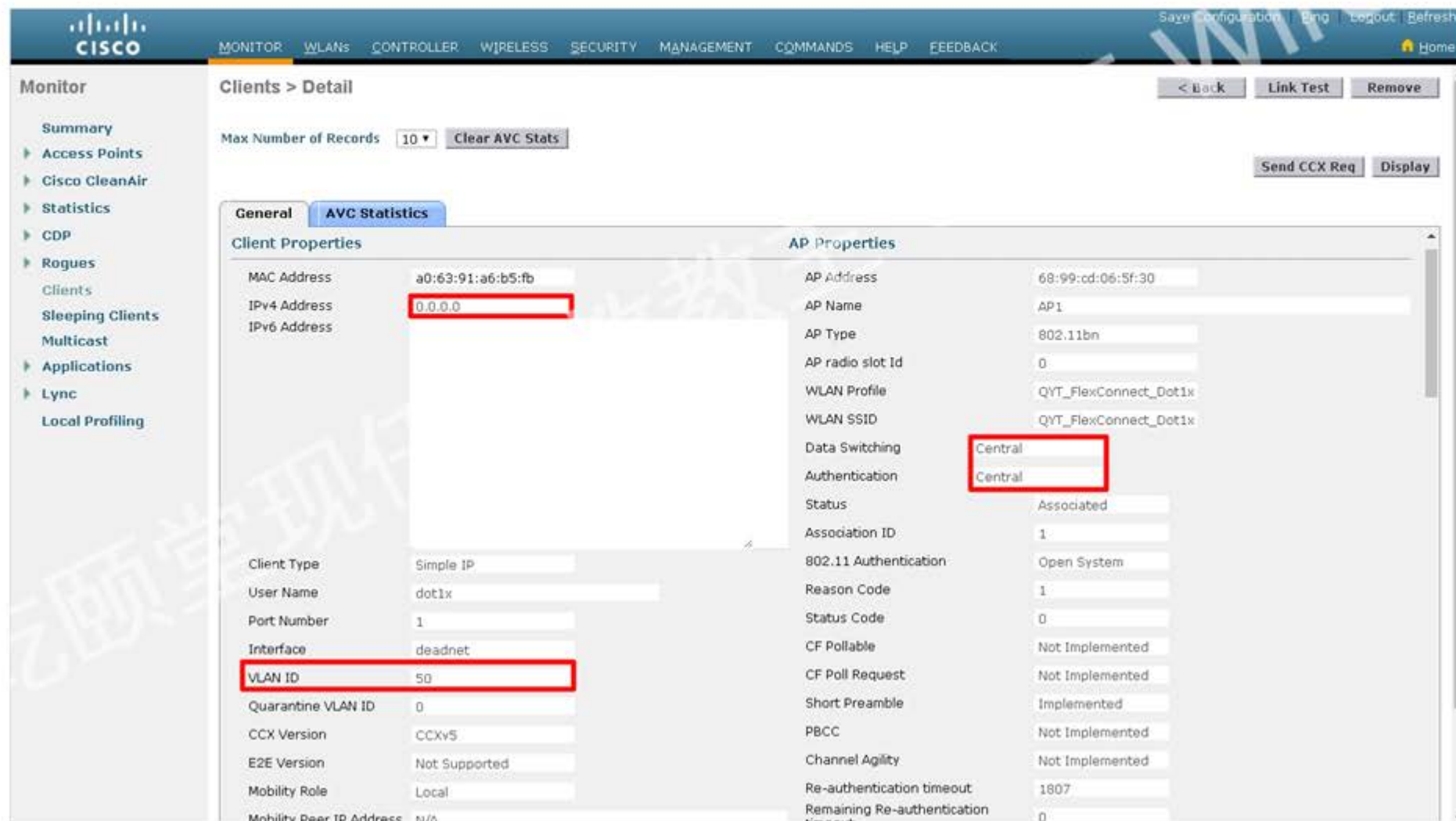
VLAN Tag ID 1 ID/Name 50

Voice Domain Permission

# 客户连接测试



# 查看客户端信息



The screenshot displays the Cisco ISE GUI for monitoring clients. The main content area is titled "Clients > Detail" and shows the "AVC Statistics" tab for a specific client. The client's IP address is 0.0.0.0, and it is associated with the 'dot1x' user name on the 'deadnet' interface, with a VLAN ID of 50. The client is connected to AP1, which is configured for Central switching and authentication.

Client Properties		AP Properties	
MAC Address	a0:63:91:a6:b5:fb	AP Address	68:99:cd:06:5f:30
IPv4 Address	0.0.0.0	AP Name	AP1
IPv6 Address		AP Type	802.11bn
Client Type	Simple IP	AP radio slot Id	0
User Name	dot1x	WLAN Profile	QYT_FlexConnect_Dot1x
Port Number	1	WLAN SSID	QYT_FlexConnect_Dot1x
Interface	deadnet	Data Switching	Central
VLAN ID	50	Authentication	Central
Quarantine VLAN ID	0	Status	Associated
CCX Version	CCXv5	Association ID	1
E2E Version	Not Supported	802.11 Authentication	Open System
Mobility Role	Local	Reason Code	1
Mobility Peer IP Address	N/A	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 timeout	0

# ISE 不授权 VLAN

Identity Services Engine Home Context Visibility

Authentication Authorization Profiling Posture Client Provisioning

Dictionary Conditions Results

Authorization Profiles > FlexConnect\_Override\_VLAN

Authorization Profile

\* Name: FlexConnect\_Override\_VLAN

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

- DACL Name
- ACL (Filter-ID)
- VLAN
- Voice Domain Permission

Disabling VLAN will disable the VLAN common task that is referenced in Authorization Profiles

CCIE WIL

乾颐堂现任明教教主

# 客户连接测试



# 查看客户端信息

The screenshot displays the Cisco WLC GUI with the following details:

- Client Properties:**
  - MAC Address: a0:63:91:a6:b5:fb
  - IPv4 Address: 0.0.0.0
  - IPv6 Address: (empty)
  - 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: (empty)
- 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



# AP 修改静态地址

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration Log 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
- Country
- Timers
- Netflow
- QoS

All APs > Details for AP1

< Back Apply

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 Name

Network Spectrum Interface Key: 44AEA6229BC887B4685D78ED1E2F006F

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)D11F  
 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 RADIUS 服务器

Wireless

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Save Configuration | Bing | Logout | Refresh

Home

FlexConnect Groups > Edit 'default-flex-group'

Apply

2

1

3

4

5

General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC mapping

Group Name default-flex-group

VLAN Template Name none

Enable AP Local Authentication

FlexConnect AP

AAA

Server Ip Address 10.1.1.12

Server Type Primary

Shared Secret .....

Confirm Shared Secret .....

Port Number 1812

Add

Server Type	Address	Port
UnConfigured	Unconfigured	0
UnConfigured	Unconfigured	0
Primary	10.1.1.12	1812
UnConfigured	Unconfigured	0

External Module Configuration

FlexConnect Local Switching

# ISE 为 AP 添加 Network Device

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassivID Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device:

Network Devices List > New Network Device

Network Devices

\* Name **AP1**

Description

\* IP Address: **20.1.1.1** / 32

\* Device Profile AlcatelWired

Model Name

Software Version

\* Network Device Group

Device Type All Device Types Set To Default

Location All Locations Set To Default

RADIUS Authentication Settings

Enable Authentication Settings

Protocol RADIUS

\* Shared Secret **Cisc0123** Hide



# ISE 为 AP 添加授权策略

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   ▼
✓	AP_FlexConnect_Dot1x	if Radius:NAS-IP-Address EQUALS 20.1.1.1 AND Radius:Called-Station-ID ENDS_WITH QYT_FlexConnect_Dot1x )	then FlexConnect_Override_VLAN	Edit   ▼

## 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

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The 'Results' sub-menu is selected under Policy Elements.

The main content area displays the configuration for the Authorization Profile 'FlexConnect\_Override\_VLAN'. The fields are as follows:

- Name: FlexConnect\_Override\_VLAN
- Description: (empty)
- Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Passive Identity Tracking:

Under the 'Common Tasks' section, the 'VLAN' checkbox is checked. The configuration for this task is shown in a table:

<input checked="" type="checkbox"/>	VLAN	Tag ID 1	Edit Tag	ID/Name 30
-------------------------------------	------	----------	----------	------------

Other options in the 'Common Tasks' section include 'DAACL Name', 'ACL (Filter-ID)', and 'Voice Domain Permission', all of which are unchecked.

# 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

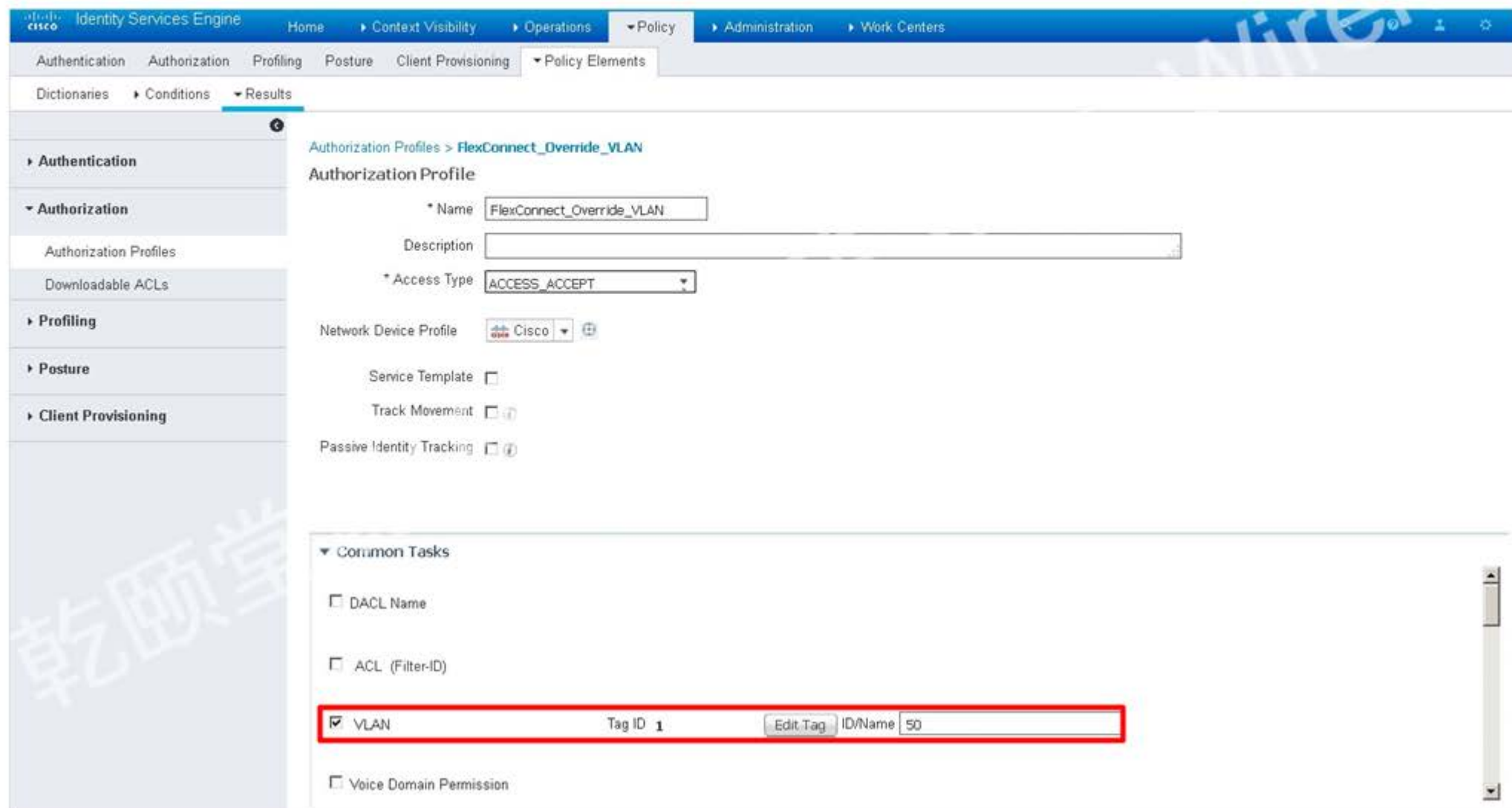
Refresh: Every 1 minute | Show: Latest 20 records | Within: Last 24 hours

Refresh | Reset Repeat Counts | Export To | Filter | Settings

Time	Status	Details	Repeat...	Identity	Endpoint ID	Endpoint Profile	Authenticati...	Authorization P...	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



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu on the left includes Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area shows the configuration for an Authorization Profile named "FlexConnect\_Override\_VLAN".

**Authorization Profile Configuration:**

- Name: FlexConnect\_Override\_VLAN
- Description: (Empty field)
- Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Passive Identity Tracking:

**Common Tasks:**

- DACL Name
- ACL (Filter-ID)
- VLAN Tag ID 1 ID/Name 50
- Voice Domain Permission

The "VLAN" option is highlighted with a red box, indicating the selected configuration.

# 客户连接测试



# ISE 不授权 VLAN

Identity Services Engine Home Context Visibility

Authentication Authorization Profiling Posture Client Provisioning

Dictionary Conditions Results

Authorization Profiles > FlexConnect\_Override\_VLAN

Authorization Profile

\* Name: FlexConnect\_Override\_VLAN

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

- DACL Name
- ACL (Filter-ID)
- VLAN
- Voice Domain Permission

Disabling VLAN will disable the VLAN common task that is referenced in Authorization Profiles

CCIE WILSON

乾颐堂现任明教教主

# 客户连接测试





# 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

The screenshot displays the Cisco WLC configuration interface. The top navigation bar includes the Cisco logo and menu items: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted with a red box and number 1), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the right side of the navigation bar, there are links for Save Configuration, Ping, Logout, Refresh, and Home.

The left sidebar shows the Security menu with the following options: AAA, Local EAP, Advanced EAP, Priority Order, Certificate, Access Control Lists (expanded), Access Control Lists, PU Access Control Lists, FlexConnect ACLs (highlighted with a red box and number 2), Layer2 ACLs, URL ACLs, Wireless Protection Policies, Web Auth, TrustSec SXP, Local Policies, and Advanced.

The main content area is titled 'FlexConnect Access Control Lists' and shows 'Entries 0 - 0 of 0'. A 'New...' button (highlighted with a red box and number 3) is located in the top right corner. The 'Access Control List Name' field (highlighted with a red box and number 4) contains the text 'Deny\_ICMP\_11'.

# WLC 创建 FlexConnect ACL - 2

The screenshot shows the Cisco WLC configuration page for creating a new Access Control List (ACL) rule. The page is titled "Access Control Lists > Rules > New". The left sidebar shows the "Security" menu with "Access Control Lists" expanded. The main content area contains the following configuration fields:

- Sequence: 1
- Source: Any
- Destination: IP Address (dropdown), IP Address: 10.1.1.11, Netmask: 255.255.255.255
- Protocol: ICMP
- DSCP: Any
- Action: Deny

Four red circles with numbers 1, 2, 3, and 4 are overlaid on the interface to highlight specific elements: 1 points to the Source dropdown, 2 points to the Protocol dropdown, 3 points to the Action dropdown, and 4 points to the Apply button. A red box highlights the Destination section (IP Address dropdown, IP Address field, and Netmask field).

Navigation buttons include "< Back" and "Apply". The top navigation bar includes "MONITOR", "WLANS", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", "HELP", "FEEDBACK", "Home", "Save Configuration", "Ping", "Logout", and "Refresh".



# WLC 创建 FlexConnect ACL - 3

The screenshot shows the Cisco WLC configuration page for creating a new Access Control List (ACL) rule. The page is titled "Access Control Lists > Rules > New". The left sidebar shows the "Security" menu with "Access Control Lists" expanded. The main content area displays the configuration fields for the new rule:

- Sequence: 2
- Source: Any
- Destination: Any
- Protocol: Any
- DSCP: Any
- Action: Permit

Red boxes and numbers highlight the "Permit" action in the "Action" field (labeled with a red circle containing the number 1) and the "Apply" button in the top right corner (labeled with a red circle containing the number 2). The "Apply" button is highlighted with a red border.

Navigation links at the top right include: Save Configuration, Ping, Logout, Refresh, Home, and a Home icon.

Navigation links at the top center include: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK.

# WLC 创建 FlexConnect ACL - 4

Save Configuration | Ping | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Security

- ▶ AAA
- ▶ Local EAP
- Advanced EAP
- ▶ Priority Order
- ▶ Certificate
- ▼ Access Control Lists
  - Access Control Lists
  - CPU Access Control Lists
  - FlexConnect ACLs
  - Layer2 ACLs
  - URL ACLs
- ▶ Wireless Protection Policies
- ▶ Web Auth
- TrustSec SXP
- Local Policies
- ▶ Advanced

Access Control Lists > Edit < Back Add New Rule

General

Access List Name Deny\_ICMP\_11

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
<u>1</u>	Deny	0.0.0.0 / 0.0.0.0	10.1.1.11 / 255.255.255.255	ICMP	Any	Any	Any <input checked="" type="checkbox"/>
<u>2</u>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any <input checked="" type="checkbox"/>

# WLC 创建 FlexConnect ACL - 5

Save Configuration | Ping | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Security

- ▶ AAA
- ▶ Local EAP
- ▶ Advanced EAP
- ▶ Priority Order
- ▶ Certificate
- ▼ Access Control Lists
  - Access Control Lists
  - CPU Access Control Lists
  - FlexConnect ACLs
  - Layer2 ACLs
  - URL ACLs
- ▶ Wireless Protection Policies
- ▶ Web Auth
- ▶ TrustSec SXP
- ▶ Local Policies
- ▶ Advanced

Access Control Lists > Edit < Back Add New Rule

General

Access List Name Deny\_ICMP\_12

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Deny	0.0.0.0 / 0.0.0.0	10.1.1.12 / 255.255.255.255	ICMP	Any	Any	Any <input checked="" type="checkbox"/>
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any <input checked="" type="checkbox"/>

# WLC 创建 VLAN-ACL 映射

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Wireless

FlexConnect Groups > Edit 'default-flex-group'

Apply

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping WLAN AVC mapping

**AAA VLAN-ACL mapping** WLAN-ACL mapping Policies

AAA VLAN ACL Mapping

Vlan Id **30**

Ingress ACL Deny\_ICMP\_11

Egress ACL Deny\_ICMP\_11

Add

Vlan Id Ingress ACL Egress ACL

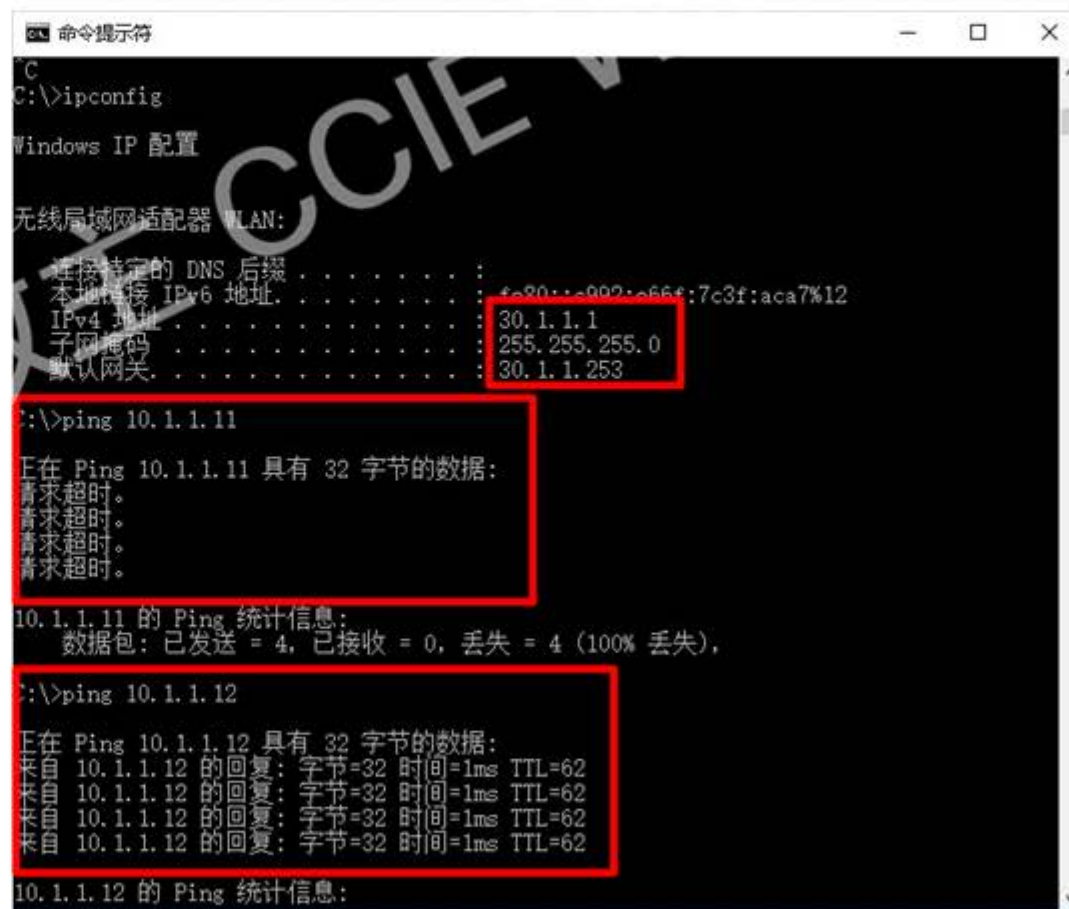
**30** Deny\_ICMP\_11 Deny\_ICMP\_11

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

# 客户端连接测试 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 Policies 推送 ACL

The screenshot shows the Cisco WLC configuration interface for FlexConnect Groups. The 'ACL Mapping' tab is selected, and the 'Policies' section is highlighted. A dropdown menu for 'Policy ACL' is open, showing 'Deny\_ICMP\_12' and an 'Add' button. A terminal window shows the output of 'AP1#sh access-lists'.

**Policy Access Control Lists**

Policy ACL	ACL
Deny_ICMP_12	10 deny icmp any host 10.1.1.11 (6 matches) 20 permit ip any any (246 matches)
Deny_ICMP_12	10 deny icmp any host 10.1.1.12 20 permit ip any any

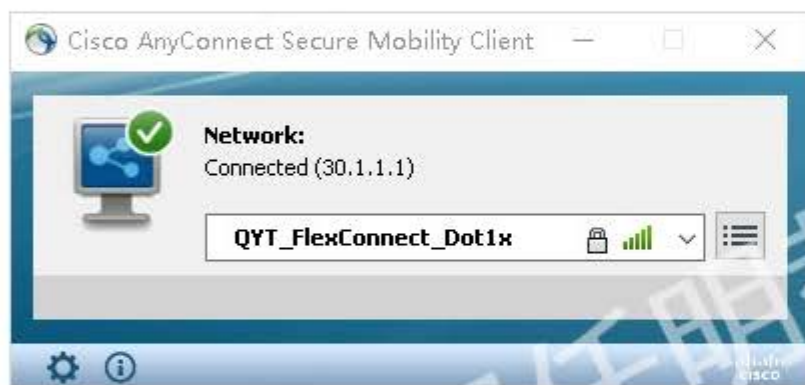
```

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

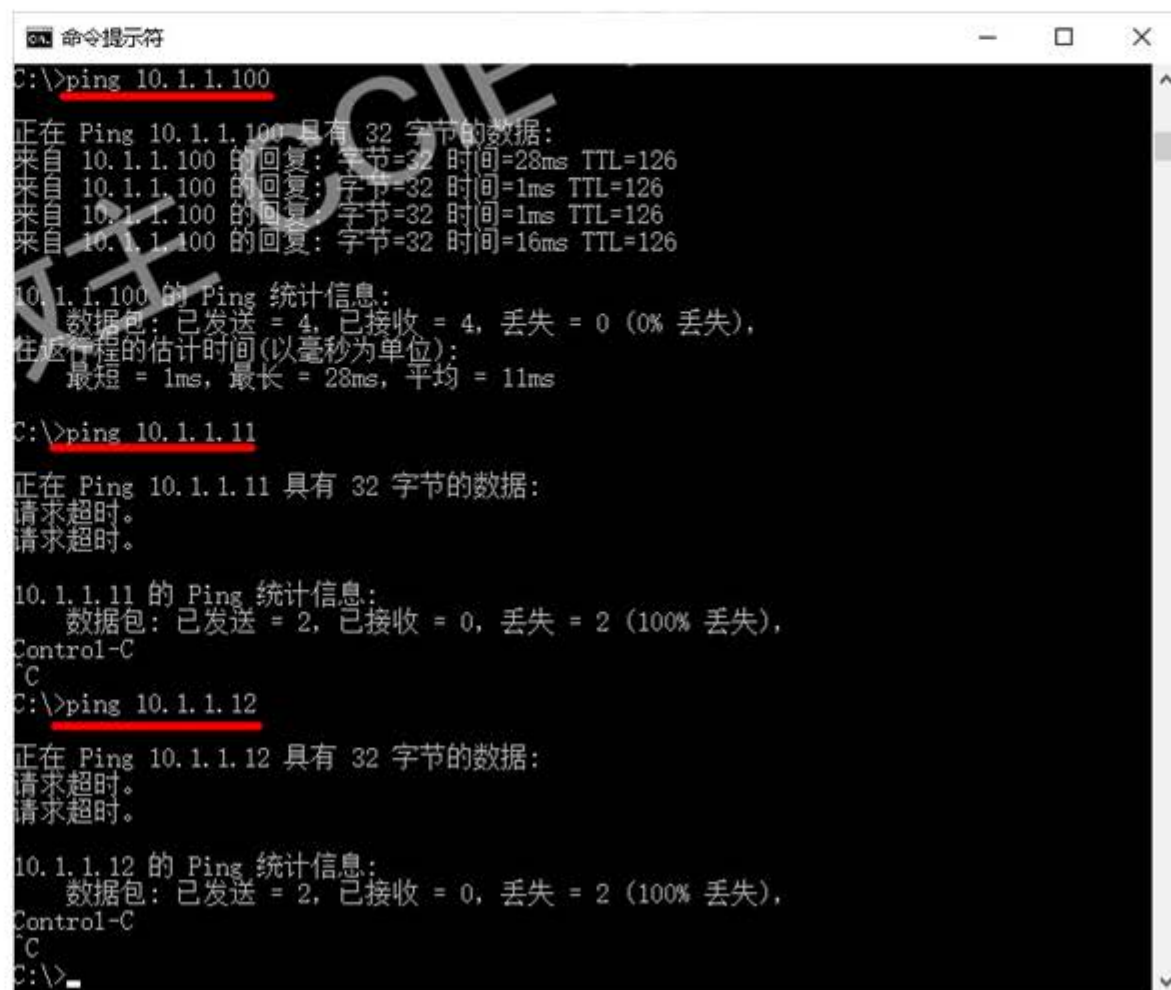
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation at the top reads: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation bar includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with categories: Authentication, Authorization (selected), Profiling, Posture, and Client Provisioning. Under Authorization, the following items are listed: Authorization Profiles, Downloadable ACLs, and Results (selected). The main content area is titled "Passive Identity Tracking" and contains several sections: "Common Tasks" with checkboxes for "Web Authentication (Local Web Auth)", "Airespace ACL Name" (checked and highlighted with a red box and a red circle containing the number 1), "ASA VPN", and "AVC Profile Name"; "Advanced Attributes Settings"; and "Attributes Details" which displays a list of attributes: Access Type = ACCESS\_ACCEPT, Tunnel-Private-Group-ID = 1:30, Tunnel-Type = 1:13, Tunnel-Medium-Type = 1:6, and Airespace-ACL-Name = Deny\_ICMP\_12. At the bottom of the configuration area, there are "Save" and "Reset" buttons, with the "Save" button highlighted by a red box and a red circle containing the number 2.

# 客户端连接测试 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)
  
```



```

命令提示符
C:\>ping 10.1.1.100

正在 Ping 10.1.1.100 具有 32 字节的数据:
来自 10.1.1.100 的回复: 字节=32 时间=28ms TTL=126
来自 10.1.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 10.1.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 10.1.1.100 的回复: 字节=32 时间=16ms TTL=126

10.1.1.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    在运行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 28ms, 平均 = 11ms

C:\>ping 10.1.1.11

正在 Ping 10.1.1.11 具有 32 字节的数据:
请求超时。
请求超时。

10.1.1.11 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 0, 丢失 = 2 (100% 丢失),
Control-C
^C
C:\>ping 10.1.1.12

正在 Ping 10.1.1.12 具有 32 字节的数据:
请求超时。
请求超时。

10.1.1.12 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 0, 丢失 = 2 (100% 丢失),
Control-C
^C
C:\>
  
```



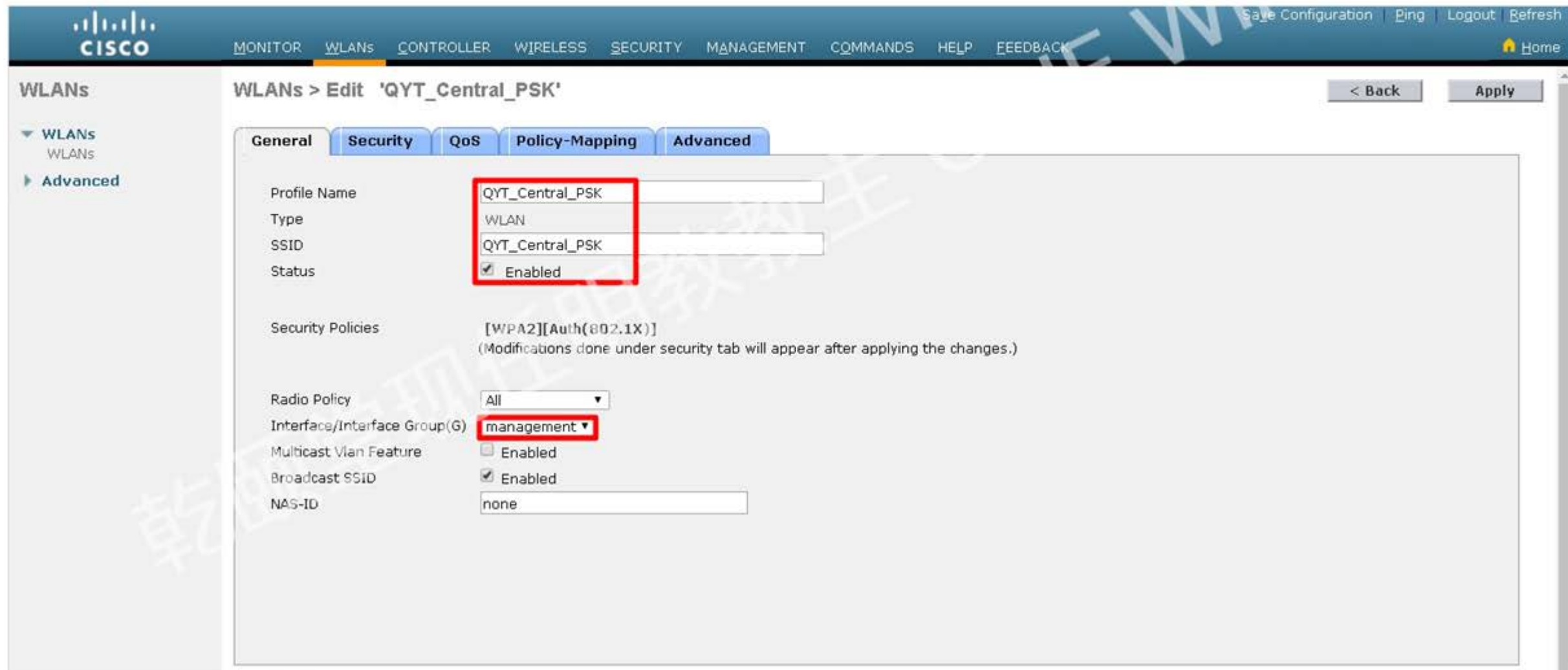


3.

# Split Tunneling



# WLC 创建 WLAN -1

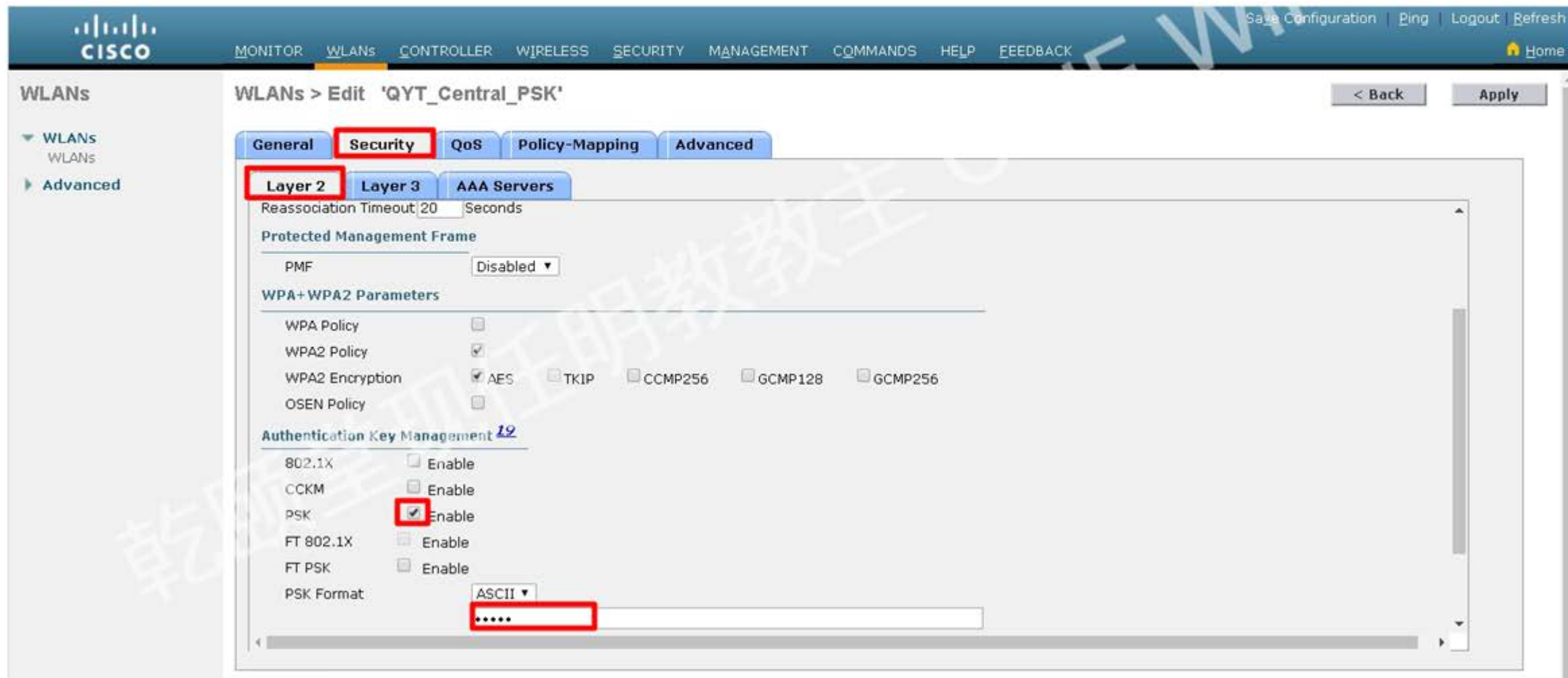


The screenshot shows the Cisco WLC configuration interface for editing a WLAN profile named 'QYT\_Central\_PSK'. The 'General' tab is selected, and the 'Advanced' sub-tab is active. The configuration fields are as follows:

Field	Value
Profile Name	QYT_Central_PSK
Type	WLAN
SSID	QYT_Central_PSK
Status	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none

Navigation buttons: < Back, Apply

# WLC 创建 WLAN -2



The screenshot shows the Cisco WLC configuration interface for editing a WLAN named 'QYT\_Central\_PSK'. The interface is divided into several sections:

- General**: Contains tabs for General, Security, QoS, Policy-Mapping, and Advanced. The Security tab is selected.
- Layer 2**: Contains tabs for Layer 2, Layer 3, and AAA Servers. The Layer 2 tab is selected.
- Protected Management Frame**: Contains a PMF dropdown menu set to Disabled.
- WPA+WPA2 Parameters**: Contains checkboxes for WPA Policy, WPA2 Policy, WPA2 Encryption (AES, TKIP, CCMP256, GCMP128, GCMP256), and OSEN Policy.
- Authentication Key Management**: Contains checkboxes for 802.1X, CCKM, PSK, FT 802.1X, and FT PSK. The PSK checkbox is checked.
- PSK Format**: Contains a dropdown menu set to ASCII and a text input field containing six dots.

The interface also includes a navigation menu on the left, a top navigation bar with links like 'Save Configuration', 'Ping', 'Logout', and 'Refresh', and a bottom navigation bar with 'Back' and 'Apply' buttons.

# WLC 创建 WLAN -3

Save Configuration | Ping | Logout | Refresh

MONITOR **WLANS** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

WLANS

WLANS > Edit 'QYT\_Central\_PSK' < Back **Apply**

**1** **Advanced**

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  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

# WLC 创建 FlexConnect

Security

- ▶ AAA
- ▶ Local EAP
- ▶ Advanced EAP
- ▶ Priority Order
- ▶ Certificate
- ▼ Access Control Lists
  - Access Control Lists
  - CPU Access Control Lists
  - FlexConnect ACLs
  - Layer2 ACLs
  - URL ACLs
- ▶ Wireless Protection Policies
- ▶ Web Auth
- TrustSec SXP
- Local Policies
- ▶ Advanced

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration | Ping | Logout | Refresh Home

## Access Control Lists > Edit

< Back Add New Rule

General

Access List Name **To\_LocalServer**

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
<u>1</u>	Permit	0.0.0.0 / 0.0.0.0	192.168.1.0 / 255.255.255.0	ICMP	Any	Any	Any

# 将列表关联到中心交换的 WLAN

The screenshot shows the Cisco FlexConnect Groups configuration page for 'default-flex-group'. The 'ACL Mapping' tab is selected, and the 'WLAN-ACL mapping' sub-tab is active. The configuration includes:

- Web Auth ACL Mapping:** WLAN Id: 0, WebAuth ACL: Deny\_ICMP\_11.
- Local Split Mapping:** WLAN Id: 3, Local Split ACL: To\_LocalServer.

A table below shows the mapping for WLAN Id 3:

WLAN Id	WLAN Profile Name	LocalSplit ACL
3	QYT_Central_PSK	To_LocalServer

At the bottom, a terminal output shows the command and its result:

```
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:
```

```
.....
```

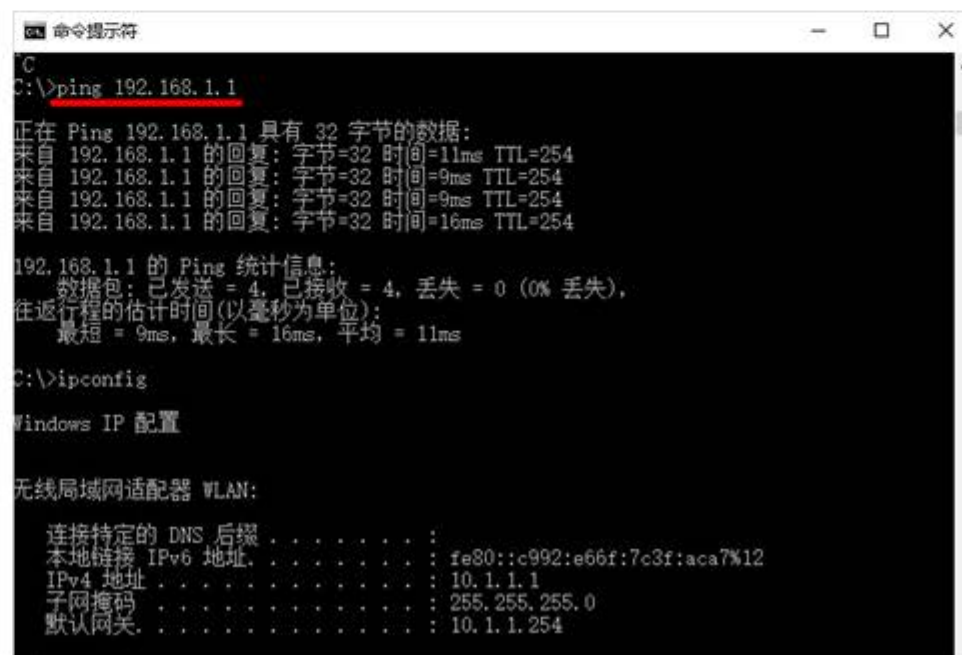
```
Success rate is 0 percent (0/5)
```

# 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