

在Catalyst 9800 WLC上配置OEAP和RLAN

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[AP在NAT后加入](#)

[配置](#)

[验证](#)

[登录OEAP并配置个人SSID](#)

[在9800 WLC上配置RLAN](#)

[故障排除](#)

简介

本文档说明如何在9800 WLC上配置Cisco OfficeExtend接入点(OEAP)和远程局域网(RLAN)。

Cisco OfficeExtend接入点(OEAP)提供从控制器到远程位置的Cisco AP的安全通信，通过互联网将公司WLAN无缝扩展到员工住所。用户在家庭办公室的体验与企业办公室的体验完全相同。接入点和控制器之间的数据报传输层安全(DTLS)加密可确保所有通信都具有最高级别的安全性。

远程LAN(RLAN)用于使用控制器对有线客户端进行身份验证。有线客户端成功加入控制器后，LAN端口会在中央或本地交换模式之间交换流量。来自有线客户端的流量被视为无线客户端流量。接入点(AP)中的RLAN发送身份验证请求以对有线客户端进行身份验证。RLAN中有线客户端的身份验证类似于中央身份验证的无线客户端。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800 WLC
- 对无线控制器和接入点的命令行界面(CLI)访问

使用的组件

本文档中的信息基于以下软件和硬件版本：

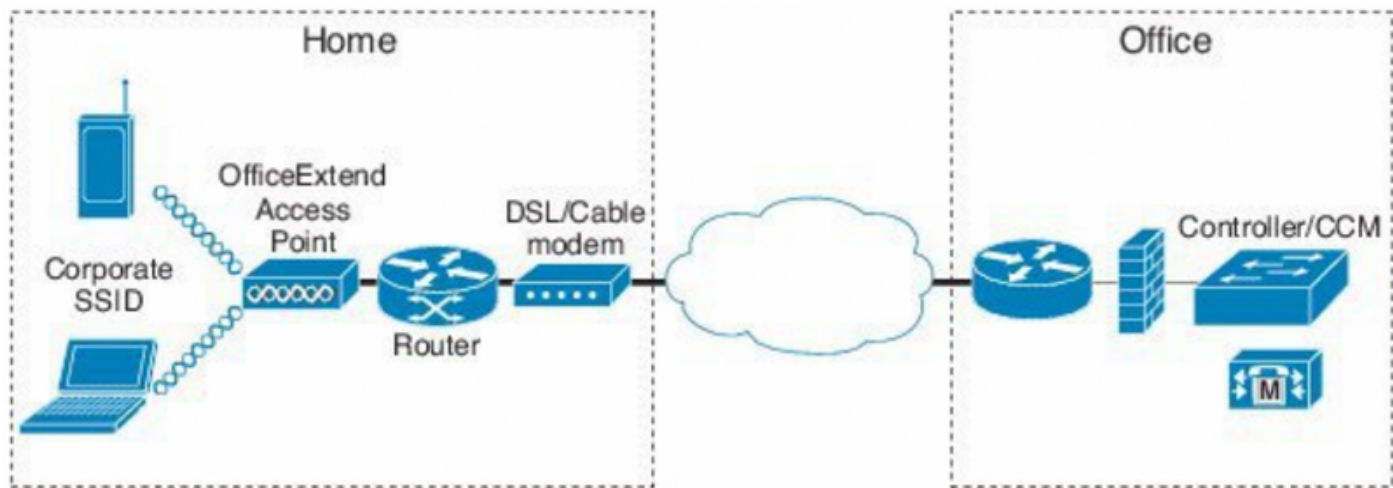
- Catalyst 9800 WLC版本17.02.01
- 1815/1810系列AP

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



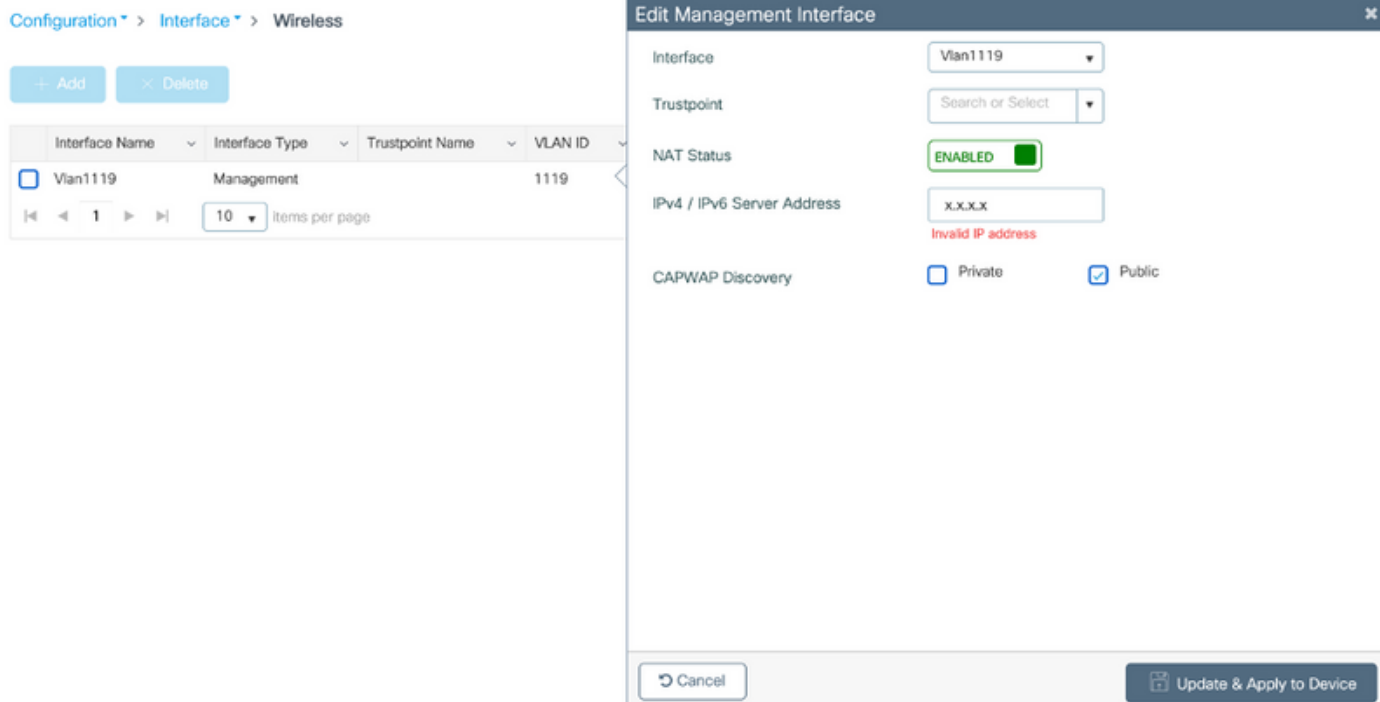
AP在NAT后加入

在16.12.x代码中，您需要从CLI配置NAT IP地址。没有可用的GUI选项。您还可以通过公共或专用IP选择CAPWAP发现。

```
(config)#wireless management interface vlan 1114 nat public-ip x.x.x.x
(config-nat-interface)#capwap-discovery ?
  private  Include private IP in CAPWAP Discovery Response

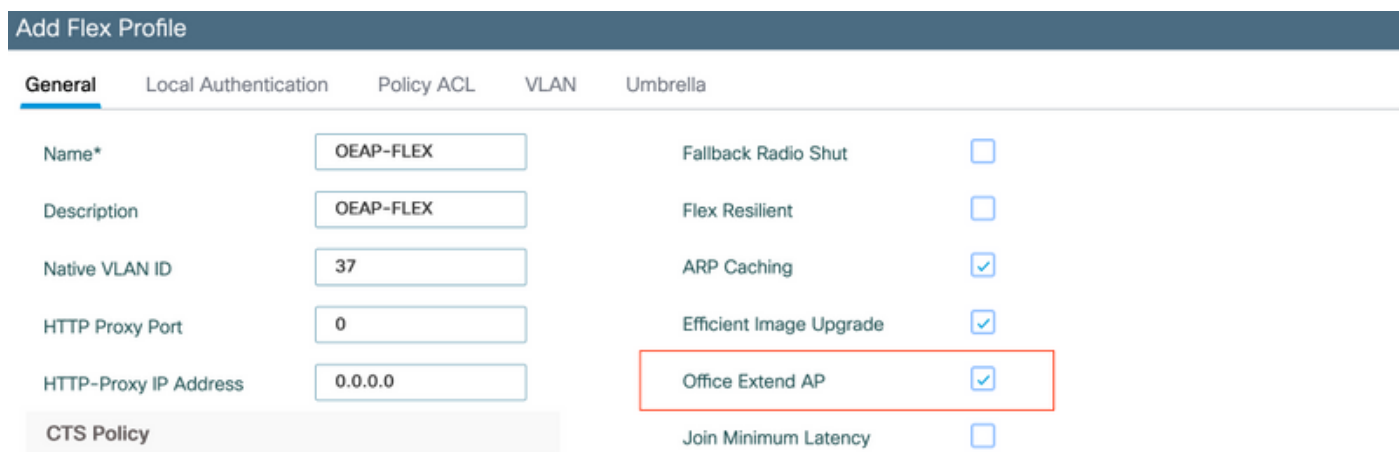
  public   Include public IP in CAPWAP Discovery Response
```

在17.x代码中，导航至**Configuration > Interface > Wireless**，然后单击**Wireless Management Interface**，从GUI中配置NAT IP和CAPWAP发现类型。



配置

1. 要创建Flex配置文件，请启用Office Extend AP并导航至Configuration > Tags & Profiles > Flex。



2. 要创建站点标签并映射Flex Profile，请导航至配置>标签和配置文件>标签。

Add Site Tag

Name*

Home-Office

Description

Enter Description

AP Join Profile

default-ap-profile ▼

Flex Profile

OEAP-FLEX| ▼

Control Plane Name

▼

Enable Local Site

Cancel

3. 导航至使用 Configuration > Wireless Setup > Advanced > Tag APs 创建的 Site Tag (站点标签) 标记 1815 AP。

Tag APs



Tags

Policy

default-policy-tag ▼

Site

Home-Office ▼

RF

default-rf-tag ▼

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel



Apply to Device

验证

1815 AP重新加入WLC后，验证以下输出：

```
vk-9800-1#show ap name AP1815 config general
```

```
Cisco AP Name      : AP1815
```

```
=====
Cisco AP Identifier      : 002c.c8de.3460
Country Code            : Multiple Countries : IN,US
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-ABDN
AP Country Code         : US - United States
Site Tag Name          : Home-Office
RF Tag Name             : default-rf-tag
Policy Tag Name         : default-policy-tag
AP join Profile         : default-ap-profile
Flex Profile          : OEAP-FLEX
Administrative State    : Enabled
Operation State         : Registered
AP Mode                 : FlexConnect
AP VLAN tagging state   : Disabled
AP VLAN tag             : 0
CAPWAP Preferred mode   : IPv4
CAPWAP UDP-Lite         : Not Configured
AP Submode              : Not Configured
Office Extend Mode    : Enabled
Dhcp Server             : Disabled
Remote AP Debug         : Disabled
```

```
vk-9800-1#show ap link-encryption
```

| | Encryption | Dnstream | Upstream | Last |
|---------|-------------------|----------|----------|-------------------|
| AP Name | State | Count | Count | Update |
| ----- | | | | |
| N2 | Disabled | 0 | 0 | 06/08/20 00:47:33 |

when you enable the OfficeExtend mode for an access point DTLS data encryption is enabled automatically.

```
AP1815#show capwap client config
```

```
AdminState           : ADMIN_ENABLED(1)
Name                  : AP1815
Location              : default location
Primary controller name : vk-9800-1
ssh status            : Enabled
ApMode                : FlexConnect
ApSubMode             : Not Configured
Link-Encryption      : Enabled
OfficeExtend AP     : Enabled
Discovery Timer       : 10
Heartbeat Timer       : 30
Syslog server         : 255.255.255.255
Syslog Facility       : 0
Syslog level          : informational
```

注意：您可以使用ap link-encryption命令为特定接入点或所有接入点启用或禁用DTLS数据加密

```
vk-9800-1(config)#ap profile default-ap-profile
```

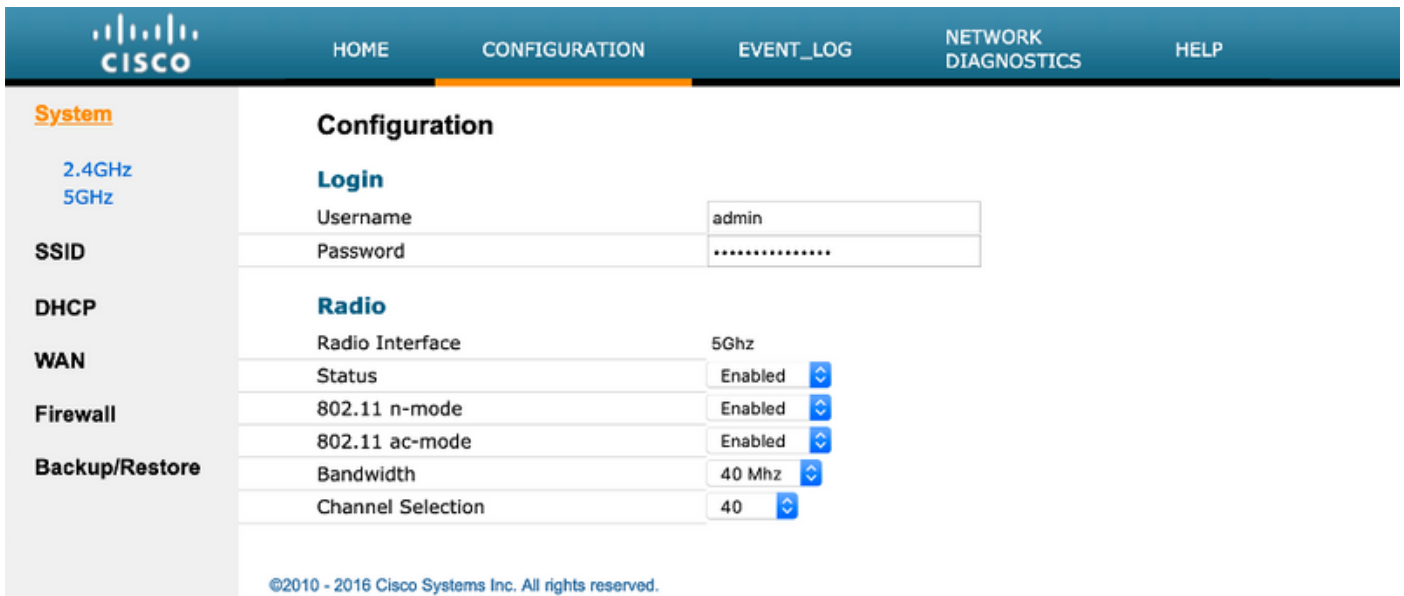
```
vk-9800-1(config-ap-profile)#no link-encryption
```

Disabling link-encryption globally will reboot the APs with link-encryption.

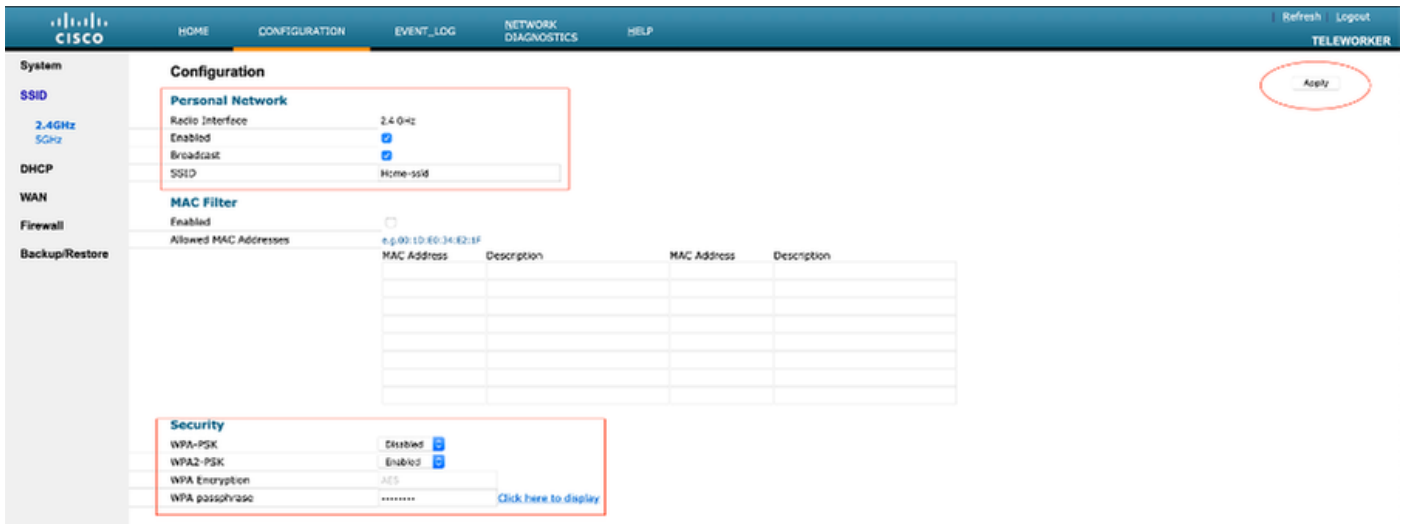
```
Are you sure you want to continue? (y/n) [y]:y
```

登录OEAP并配置个人SSID

- 1.您可以使用IP地址访问OEAP的Web界面。要登录的默认凭证是admin和admin。
- 2.出于安全原因，建议更改默认凭据。



3. 导航至 Configuration > SSID > 2.4GHz/5GHz 以配置个人 SSID。



4. 启用无线电接口。

5. 输入 SSID 并启用广播

6. 对于加密，请选择 WPA-PSK 或 WPA2-PSK 并输入相应安全类型的口令。

7. 单击“应用”以使设置生效。

8. 默认情况下，连接到个人 SSID 的客户端从 10.0.0.1/24 网络获取 IP 地址。

9. 家庭用户可以使用相同的 AP 连接供家庭使用，并且流量不通过 DTLS 隧道传输。

10. 要检查 OEAP 上的客户端关联，请导航至“主页”>“客户端”。您可以看到与 OEAP 关联的本地客户端和公司客户端。

| Cisco | | | | | | |
|---|-----------------------------------|---------------|----------------|-----------|------------------|-------------|
| HOME CONFIGURATION EVENT_LOG NETWORK DIAGNOSTICS HELP Refresh Logout TELEWORKER | | | | | | |
| AP Info | Association Show all | | | | | |
| SSID | | | | | | |
| Client | Local Clients | | | | | |
| | Client MAC | Client IP | WLAN SSID | Radio/LAN | Association Time | Pkts In/Out |
| | 00:17:7C:88:13:D8 | 10.0.0.59 | Home-ssid | 2.4Ghz | 00d:00h:24m:55s | 332/101 |
| | Corporate Clients | | | | | |
| | Client MAC | Client IP | WLAN SSID | Radio/LAN | Association Time | Pkts In/Out |
| | 50:3E:AA:B7:0F:F4 | 10.106.37.115 | corporate-ssid | 2.4Ghz | 00d:00h:07m:09s | 499/269 |

To clear personal ssid from office-extend ap

```
ewlc#ap name cisco-ap clear-personalssid-config
```

clear-personalssid-config Clears the Personal SSID config on an OfficeExtend AP

在9800 WLC上配置RLAN

远程LAN(RLAN)用于使用控制器对有线客户端进行身份验证。有线客户端成功加入控制器后，LAN端口会在中央或本地交换模式之间交换流量。来自有线客户端的流量被视为无线客户端流量。接入点(AP)中的RLAN发送身份验证请求以对有线客户端进行身份验证的。

RLAN中有线客户端的身份验证类似于中央身份验证的无线客户端。

注意：本例中，本地EAP用于RLAN客户端身份验证。WLC上必须存在本地EAP配置才能配置以下步骤。它包括aaa authentication & authorization方法、本地EAP配置文件和本地凭证。

[Catalyst 9800 WLC上的本地EAP身份验证配置示例](#)

1. 要创建RLAN配置文件，请导航至**Configuration > Wireless > Remote LAN**，然后输入RLAN配置文件的Name和RLAN ID，如下图所示。

2. 导航至**Security > Layer2**，为了为RLAN启用802.1x，请将802.1x状态设置为Enabled，如下图所示

示。

The screenshot shows the 'Edit RLAN Profile' configuration page. The 'Security' tab is selected, and the 'Layer2' sub-tab is active. The configuration includes:

- 802.1x:** A toggle switch labeled 'ENABLED' with a green square, indicating it is turned on.
- MAC Filtering:** A dropdown menu showing 'Not Configured' with a downward arrow.
- Authentication List:** A dropdown menu showing 'default' with a downward arrow.

3. 导航至 **Security > AAA**，将 Local EAP Authentication 设置为 enabled，然后从下拉列表中选择所需的 EAP Profile Name，如此图所示。

The screenshot shows the 'Edit RLAN Profile' configuration page. The 'Security' tab is selected, and the 'AAA' sub-tab is active. The configuration includes:

- Local EAP Authentication:** A toggle switch labeled 'ENABLED' with a green square, indicating it is turned on.
- EAP Profile Name:** A dropdown menu showing 'Local-EAP' with a downward arrow.

4. 要创建 RLAN 策略，请导航至 **Configuration > Wireless > Remote LAN**，然后在“Remote LAN”页面上，单击 **RLAN Policy** 选项卡，如下图所示。

Edit RLAN Policy ✕

General Access Policies Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this policy.

| | | | |
|--------------|---|------------------------------|---|
| Policy Name* | RLAN-Policy | RLAN Switching Policy | |
| Description | Enter Description | Central Switching | ENABLED <input checked="" type="checkbox"/> |
| Status | ENABLED <input checked="" type="checkbox"/> | Central DHCP | ENABLED <input checked="" type="checkbox"/> |
| PoE | <input type="checkbox"/> | | |
| Power Level | 4 ▼ | | |

导航至访问策略并配置VLAN和主机模式并应用设置。

Edit RLAN Policy ✕

General **Access Policies** Advanced

| | | | |
|-----------------------|--------------------------|-----------|--------------|
| Pre-Authentication | <input type="checkbox"/> | Host Mode | singlehost ▼ |
| VLAN | VLAN0039 ▼ | | |
| Remote LAN ACL | | | |
| IPv4 ACL | Not Configured ▼ | | |
| IPv6 ACL | Not Configured ▼ | | |

5.要创建策略标记并将RLAN配置文件映射到RLAN策略，请导航至Configuration > Tags & Profiles > Tags。

Add Policy Tag



Name*

RLAN-TAG

Description

Enter Description

WLAN-POLICY Maps: 0

RLAN-POLICY Maps: 0

+ Add

× Delete

| Port ID | RLAN Profile | RLAN Policy Profile |
|---------------------|--------------|---------------------|
| No items to display | | |

Map RLAN and Policy

Port ID*

3

RLAN Profile*

RLAN-TEST

RLAN Policy Profile*

RLAN-Policy



Cancel

Apply to Device

Add Policy Tag ✕

Name*

Description

➤ WLAN-POLICY Maps: 0

▼ RLAN-POLICY Maps: 1

| | Port ID | RLAN Profile | RLAN Policy Profile |
|--------------------------|---------|--------------|---------------------|
| <input type="checkbox"/> | 3 | RLAN-TEST | RLAN-Policy |

⏪ ◀ 1 ▶ ⏩ items per page 1 - 1 of 1 items

6. 启用LAN端口并在AP上应用策略标记。导航至 **Configuration > Wireless > Access Points**，然后单击AP。

Edit AP

| | | | |
|---|---|--------------------------------|-------------------------------|
| Location* | default location | Predownloaded Status | N/A |
| Base Radio MAC | 0042.5ab7.8f60 | Predownloaded Version | N/A |
| Ethernet MAC | 0042.5ab6.4ab0 | Next Retry Time | N/A |
| Admin Status | ENABLED <input checked="" type="checkbox"/> | Boot Version | 1.1.2.4 |
| AP Mode | Local ▼ | IOS Version | 17.2.1.11 |
| Operation Status | Registered | Mini IOS Version | 0.0.0.0 |
| Fabric Status | Disabled | IP Config | |
| LED State | <input type="checkbox"/> DISABLED | CAPWAP Preferred Mode | Not Configured |
| LED Brightness Level | 8 ▼ | DHCP IPv4 Address | 10.106.39.198 |
| Tags | | Static IP (IPv4/IPv6) | <input type="checkbox"/> |
| <p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.</p> | | | |
| Policy | RLAN-TAG ▼ | Time Statistics | |
| Site | default-site-tag ▼ | Up Time | 0 days 13 hrs 33 mins 40 secs |
| RF | default-rf-tag ▼ | Controller Association Latency | 20 secs |

应用设置，AP重新加入WLC。单击AP，然后选择**Interfaces**并启用LAN端口。

Edit AP

General **Interfaces** High Availability Inventory ICap Advanced

Radio Interfaces

| Slot No | Interface | Band | Admin Status | Operation Status | Spectrum Admin Status | Spectrum Operation Status | Regulatory Domain |
|---------|-------------------|------|--------------|------------------|-----------------------|---------------------------|-------------------|
| 0 | 802.11n - 2.4 GHz | All | Enabled | | Disabled | | -A |
| 1 | 802.11ac | All | Enabled | | Disabled | | -D |

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode

PoE Pre-Standard Switch: Disabled

PoE Power Injector MAC Address: Disabled

LAN Port Settings

| Port ID | Status | VLAN ID | PoE | Power Level | RLAN |
|---------|-------------------------------------|---------|--------------------------|-------------|------|
| LAN1 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | NA | |
| LAN2 | <input type="checkbox"/> | 0 | NA | NA | |
| LAN3 | <input checked="" type="checkbox"/> | 39 | NA | NA | |

10 items per page 1 - 3 of 3 items

应用设置并验证状态。

Edit AP

General **Interfaces** High Availability Inventory ICap Advanced

Radio Interfaces

| Slot No | Interface | Band | Admin Status | Operation Status | Spectrum Admin Status | Spectrum Operation Status | Regulatory Domain |
|---------|-------------------|------|--------------|------------------|-----------------------|---------------------------|-------------------|
| 0 | 802.11n - 2.4 GHz | All | Enabled | | Disabled | | -A |
| 1 | 802.11ac | All | Enabled | | Disabled | | -D |

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode

PoE Pre-Standard Switch: Disabled

PoE Power Injector MAC Address: Disabled

LAN Port Settings

| Port ID | Status | VLAN ID | PoE | Power Level | RLAN |
|---------|-------------------------------------|---------|--------------------------|-------------|------|
| LAN1 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | NA | |
| LAN2 | <input type="checkbox"/> | 0 | NA | NA | |
| LAN3 | <input checked="" type="checkbox"/> | 39 | NA | NA | |

10 items per page 1 - 3 of 3 items

7.将PC连接到AP的LAN3端口。PC将通过802.1x进行身份验证，并从已配置的VLAN获取IP地址。

导航至**监控>无线>客户端**以检查客户端状态。

Delete



Total Client(s) in the Network: 2

Number of Client(s) selected: 0

| <input type="checkbox"/> | Client MAC Address | IPv4 Address | IPv6 Address | AP Name | SSID | WLAN ID | State | Protocol | User Name | Device Type | Role |
|--------------------------|--------------------|---------------|--------------------------|---------|----------------|---------|-------|----------|-----------|-------------|-------|
| <input type="checkbox"/> | 503e.aab7.0ff4 | 10.106.39.227 | 2001::c | AP1815 | corporate-ssid | 3 | Run | 11n(2.4) | | N/A | Local |
| <input type="checkbox"/> | b496.9126.dd6c | 10.106.39.191 | fe80::d8cax582:2703:f24e | AP1810 | RLAN-TEST | 1 | Run | Ethernet | vinodh | N/A | Local |

1 - 2 of 2 clients

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Call Statistics

Client Properties

AP Properties

Security Information

Client Statistics

QOS Properties

EoGRE

Session Manager

| | |
|-------------------------|--------------------------|
| IIF ID | 0x9000000C |
| Authorized | TRUE |
| Common Session ID | 00000000000000E79E8C7A9A |
| Acct Session ID | 0x00000000 |
| Auth Method Status List | |
| Method | Dot1x |
| SM State | AUTHENTICATED |
| SM Bend State | IDLE |

vk-9800-1#show wireless client summary

Number of Clients: 2

| MAC Address | AP Name | Type | ID | State |
|-------------|---------|------|----|-------|
|-------------|---------|------|----|-------|

Protocol Method Role

```
-----
503e.aab7.0ff4 AP1815 WLAN 3 Run
11n(2.4) None Local
b496.9126.dd6c AP1810 RLAN 1 Run
Ethernet Dot1x Local
```

Number of Excluded Clients: 0

故障排除

常见问题:

- 仅本地SSID的工作，WLC上配置的SSID未被广播：检查AP是否已正确加入控制器。
- 无法访问OEAP GUI:检查ap是否具有IP地址并检验连通性（防火墙、ACL等网内）
- 集中交换无线或有线客户端无法验证或获取IP地址：获取RA跟踪，始终在跟踪等。

有线802.1x客户端的始终在线跟踪示例：

```
[client-orch-sm] [18950]: (note): MAC: <client-mac> Association received. BSSID 00b0.e187.cfc0,
old BSSID 0000.0000.0000, WLAN test_rlan, Slot 2 AP 00b0.e187.cfc0, Ap_1810
```

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_INIT -> S_CO_ASSOCIATING

[dot11-validate] [18950]: (ERR): MAC: <client-mac> Failed to dot11 determine ms physical radio type. Invalid radio type :0 of the client.

[dot11] [18950]: (ERR): MAC: <client-mac> Failed to dot11 send association response. Encoding of assoc response failed for client reason code: 14.

[dot11] [18950]: (note): MAC: <client-mac> Association success. AID 1, Roaming = False, WGB = False, llr = False, llw = False AID list: 0x1| 0x0| 0x0| 0x0

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-auth] [18950]: (note): MAC: <client-mac> L2 Authentication initiated. method DOT1X, Policy VLAN 1119,AAA override = 0 , NAC = 0

[ewlc-infra-evq] [18950]: (note): Authentication Success. Resolved Policy bitmap:11 for client <client-mac>

[client-orch-sm] [18950]: (note): MAC: <client-mac> Mobility discovery triggered. Client mode: Local

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS

[mm-client] [18950]: (note): MAC: <client-mac> Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Previous BSSID MAC: 0000.0000.0000 Client IFID: 0xa0000003, Client Role: Local PoA: 0x90000012 PoP: 0x0

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS

[dot11] [18950]: (note): MAC: <client-mac> Client datapath entry params - ssid:test_rlan,slot_id:2 bssid ifid: 0x0, radio_ifid: 0x90000006, wlan_ifid: 0xf0404001

[dpath_svc] [18950]: (note): MAC: <client-mac> Client datapath entry created for ifid 0xa0000003

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [18950]: (note): MAC: <client-mac> Client IP learn successful. Method: DHCP IP: <Client-IP>

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Get ATF policy name from WLAN profile:: Failed to get wlan profile. Searched wlan profile test_rlan

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name

[apmgr-bssid] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name from WLAN profile name: No such file or directory

[client-orch-sm] [18950]: (ERR): Failed to get client ATF policy name: No such file or directory

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition:

S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN