H3Cアクセスコントローラ
Comware7 MAC認証およびPSK認証の設定例

内容

はじめに

このドキュメントでは、PSK認証およびMAC認証の設定例について説明します。

前提条件

この文書は、Comware7ベースのアクセスコントローラおよびアクセスポイントに適用されます。例の手順および情報は、アクセスコントローラおよびアクセスポイントのソフトウェアまたはハードウェアのバージョンによって若干異なる場合があります。

このドキュメントの設定例は、ラボ環境で作成および検証されたものであり、すべてのデバイスは工場出荷時のデフォルト設定で開始されています。ライブネットワークで作業している場合は、ネットワークに対するすべてのコマンドの潜在的な影響を理解していることを確認してください。

このマニュアルでは、AAA、MAC認証、WLAN認証、およびWLANアクセスに関する基本的な知識があることを前提としています。

例:MAC認証およびPSK認証の設定

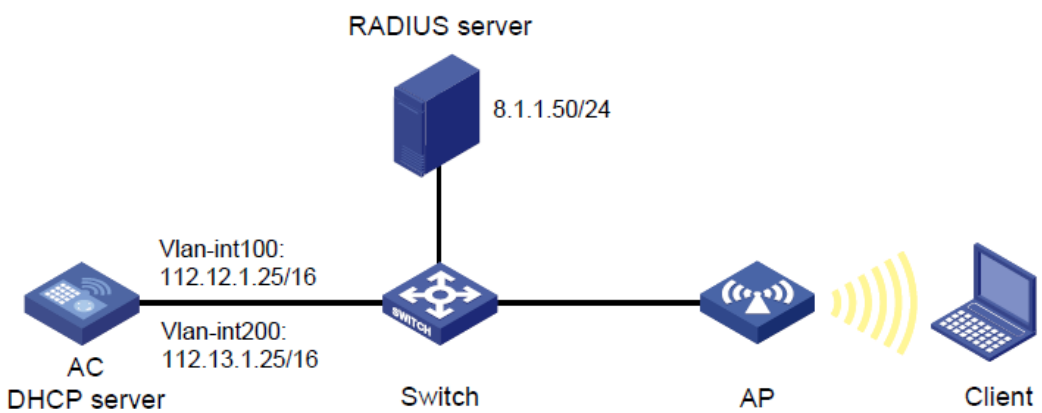
ネットワーク構成

図1に示すように、ACはDHCPサーバとして機能し、APおよびクライアントにIPアドレスを提供します。ACはクライアントトラフィックを中央に転送します。

クライアントのネットワークリソースへのアクセスを制御するには、次のタスクを実行します。

- VLAN200をクライアントのアクセスVLANとして設定します。
- RADIUSサーバを使用してクライアントのMAC認証を実行するようにACを設定します。
- AKMモードをPSKに設定して、クライアントとAP間のデータ伝送を保護します。

図1 ネットワーク図



制限事項およびガイドライン

無線クライアントにPSK AKMモードでMAC認証を設定する場合は、次の制約事項およびガイドラインに従ってください。

- ACで、MAC認証用のユーザアカウント形式を指定します。この例では、クライアントのMACアドレスがユーザ名とパスワードとして使用されます。RADIUSサーバのユーザ名とパスワードの設定が、ACの設定と一致していることを確認してください。
- APの背面パネルに表示されているシリアルIDを使用して、APを指定します。
- VLAN1のパケット数が多すぎる場合は、ACをAPに接続するポートをVLAN1から削除します。

手順

ACの設定

1. ACのインターフェイスを設定します。

#VLAN100およびVLANインターフェイス100を作成し、VLANインターフェイスにIPアドレスを割り当てます。ACはこのIPアドレスを使用して、APとのCAPWAPトンネルを確立します。

<AC> system-view

[AC] vlan 100

[AC-vlan100] quit

[AC] interface vlan-interface 100

[AC-Vlan-interface100] ip address 112.12.1.25 16

[AC-Vlan-interface100] quit

#VLAN200およびVLAN-interface200を作成し、VLANインターフェイスにIPアドレスを割り当てます。VLAN200はクライアントアクセスに使用されます。

[AC] vlan 200

[AC-vlan200] quit

[AC] interface vlan-interface 200

[AC-Vlan-interface200] ip address 112.13.1.25 16

[AC-Vlan-interface200] quit

#GigabitEthernet1/0/1(ACとスイッチを接続するポート)をトランクポートとして設定します。

VLAN1からポートを削除し、ポートをVLAN100および200に割り当てます。

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port link-type trunk

[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1

[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200

Set the PVID of GigabitEthernet 1/0/1 to VLAN 100.

[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1

GigabitEthernet1/0/1のPVIDをVLAN100に設定します。

[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100

[AC-GigabitEthernet1/0/1] quit

2. DHCPの設定:

#DHCPを有効にします。

[AC]dhcp enable

#vlan100という名前のDHCPアドレスプールを作成し、DHCPアドレスプールにサブネット112.12.0.0/16およびゲートウェイIPアドレス112.12.1.25を指定します。

[AC] dhcp server ip-pool vlan100

[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0

[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25

[AC-dhcp-pool-vlan100] quit

#vlan200という名前のDHCPアドレスプールを作成し、サブネット112.13.0.0/16を指定します。

DHCPアドレスプールのゲートウェイIPアドレス112.13.1.25。

[AC] dhcp server ip-pool vlan200

[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0

[AC-dhcp-pool-vlan200] gateway-list 112.13.1.30

[AC-dhcp-pool-vlan200] quit

3. RADIUSベースのMAC認証を設定します。

#officeという名前のRADIUSスキームを作成し、そのビューを入力します。

[AC] radius scheme office

#プライマリ認証およびアカウンティングRADIUSサーバのIPアドレスを指定します。

[AC-radius-office] primary authentication 8.1.1.50

[AC-radius-office] primary accounting 8.1.1.50

#RADIUS認証およびアカウンティング用の共有キーを指定します。

[AC-radius-office] key authentication simple 123456789

[AC-radius-office] key accounting simple 123456789

#RADIUSサーバに送信されるユーザ名からISPドメイン名を除外します。

[AC-radius-office] user-name-format without-domain

#発信RADIUSパケットの送信元IPアドレスとしてIPアドレス112.12.1.25を指定します。

[AC-radius-office] nas-ip 112.12.1.25

[AC-radius-office] quit

#office1という名前のISPドメインを作成し、そのビューを入力します。

[AC] domain office1

#RADIUSスキームオフィスをISPドメインオフィス1に適用して、LANユーザの認証、認可、およびアカウンティングを行います。

[AC-isp-office1] authentication lan-access radius-scheme office

[AC-isp-office1] authorization lan-access radius-scheme office

[AC-isp-office1] accounting lan-access radius-scheme office

#ISPドメインoffice1のクライアントにアイドルカット機能を設定します。

[AC-isp-office1] authorization-attribute idle-cut 15 1024

[AC-isp-office1] quit

#MACベースのアカウントを使用するようにMAC認証を設定します。各MACアドレスは#MACベースのアカウントを使用するようにMAC認証を設定します。各MACアドレスはハイフンなしの16進

数表記で、文字は小文字です。

[AC] mac-authentication user-name-format mac-address without-hyphen lowercase

4. ワイヤレスサービスを設定します。

#1という名前のサービステンプレートを作成し、そのビューを入力します。

[AC] wlan service-template 1

#サービステンプレート1のSSIDをserviceとして設定します。

[AC-wlan-st-1] ssid service

#サービステンプレートを使用してオンラインになるクライアントをVLAN200に割り当てます。

[AC-wlan-st-1] vlan 200

#認証モードをMAC認証に設定します。

[AC-wlan-st-1] client-security authentication-mode mac

#ISPドメインoffice1をMAC認証ドメインとして指定します。

[AC-wlan-st-1] mac-authentication domain office1

5. サービステンプレートのAKMモードを設定します。

#AKMモードをPSKに設定します。

[AC-wlan-st-1] akm mode psk

#プレーンテキスト文字列123456789をPSKとして設定します。

[AC-wlan-st-1] preshared-key pass-phrase simple 123456789

#CCMPを暗号スイートとして設定し、ビーコンおよびプローブ応答でRSN IEをイネーブルにします。

[AC-wlan-st-1]cipher-suite ccmp

[AC-wlan-st-1]security-ie rsn

#サービステンプレートをイネーブルにします。

[AC-wlan-st-1] service-template enable

[AC-wlan-st-1] quit

6. 手動AP officeapを設定し、サービステンプレート1をAP無線にバインドします。

#officeapという名前の手動APを作成し、APのモデルとシリアルIDを指定します。

[AC] wlan ap officeap model WA560-WW

[AC-wlan-ap-officeap] serial-id 219801A1NM8182032235

#radio2のビューを入力し、サービステンプレート1をradio2にバインドします。

[AC-wlan-ap-officeap] radio 2

[AC-wlan-ap-officeap-radio-2] service-template 1

#radio2を有効にします。

[AC-wlan-ap-officeap-radio-2] radio enable

[AC-wlan-ap-officeap-radio-2] quit

[AC-wlan-ap-officeap] quit

スイッチの設定

VLAN100を作成します。スイッチはこのVLANを使用して、ACとAP間のCAPWAPトンネル上のトラフィックを転送します。

<Switch> system-view

[Switch] vlan 100

[Switch-vlan100] quit

#VLAN200を作成します。スイッチはこのVLANを使用して、ワイヤレスクライアントにパケットを転送します。

[Switch] vlan 200

[Switch-vlan200] quit

#GigabitEthernet1/0/1(スイッチとACを接続するポート)をトランクポートとして設定し、VLAN1からポートを削除して、トランクポートをVLAN100に割り当てます。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port link-type trunk

[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1

[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100

#GigabitEthernet1/0/1のPVIDをVLAN100に設定します。

[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100

[Switch-GigabitEthernet1/0/1] quit

#GigabitEthernet1/0/2 1(スイッチとAPを接続するポート)をアクセスポートとして設定します。アクセスポートをVLAN100に割り当てます。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] port link-type access

[Switch-GigabitEthernet1/0/2] port access vlan 100

GigabitEthernet1/0/2でPoEをイネーブルにします。

[Switch-GigabitEthernet1/0/2] poe enable

[Switch-GigabitEthernet1/0/2] quit

RADIUSサーバの設定

この例では、RADIUSサーバはiMC PLAT7.1(E0303P10)およびiMC UAM7.1(E0303P10)を実行します。こ

1. アクセスデバイスを追加します
   a. IMCにログインして、**User**タブをクリックします。
   b. ナビゲーションツリーで、**User Access Policy > Access Device Management > Access Device**を選択します。
   c. **Add**をクリックします。

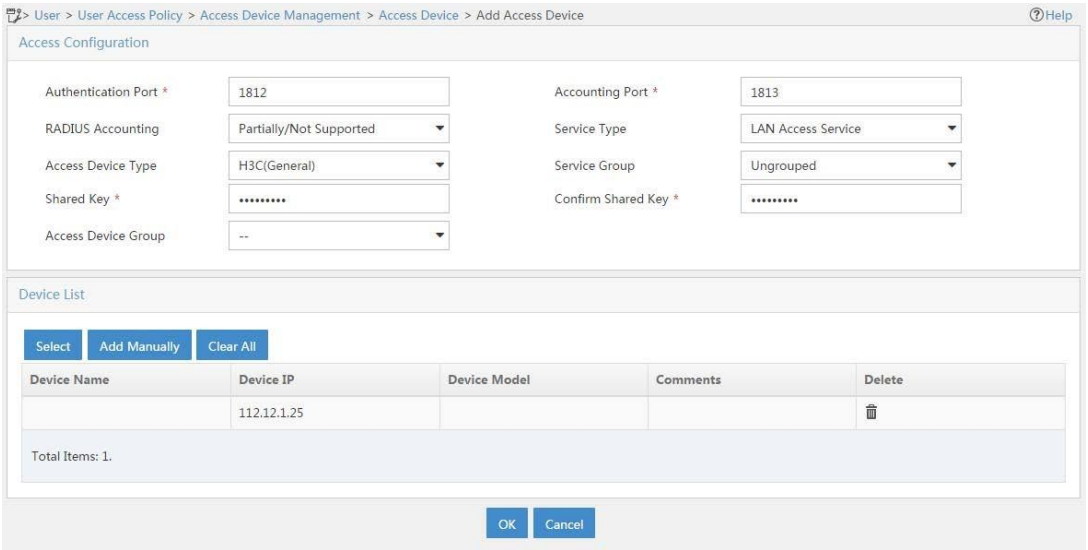
      Add Access Deviceページが開きます。
   d. **Device List**領域で、**Add Manually**をクリックして、**112.12.1.25**にあるデバイスをアクセスデバイスとして追加します。このIPアドレスは、発信RADIUSパケットのACで指定された送

信元IPアドレスです。

e. **Access Configuration**領域で、図2に示すように、次のパラメータを設定します
   - **Shared Key**および**Confirm Shared Key**フィールドに**123456789**を入力します。キーは、ACに構成されている共有キーと一致しています。
   - 他のパラメータにはデフォルト値を使用します。

f. **OK**をクリックします。

図2 アクセスデバイスの追加



2. アクセスポリシーを追加します。

   a. **User**タブをクリックします

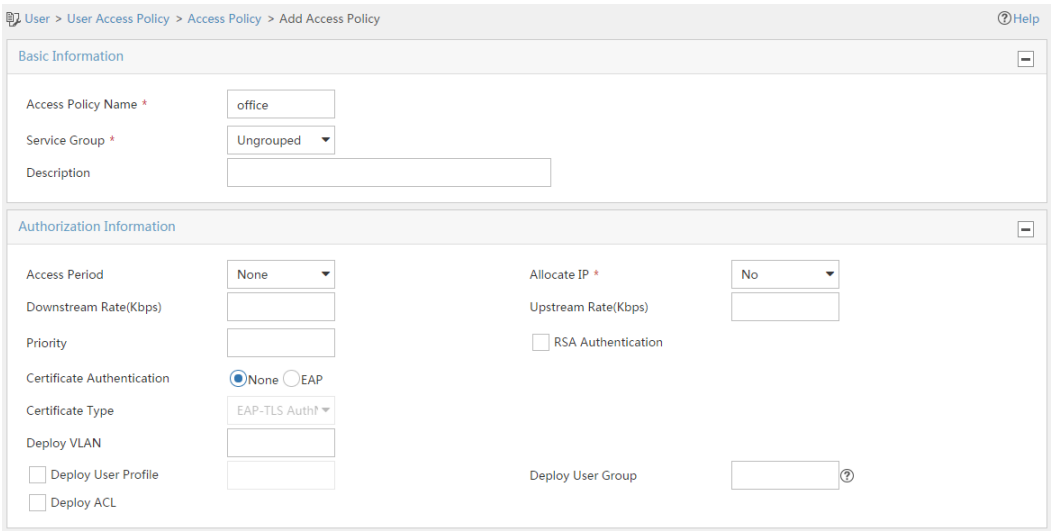
   b. ナビゲーションツリーで、**User Access Policy > Access Policy**を選択します。

   c. **Add**をクリックします。

   d. **Add Access Policy**ページで、図3に示すように、次のパラメータを設定します。
      - **Access Policy Name**フィールドに**office**と入力します。
      - 他のパラメータにはデフォルト値を使用します。

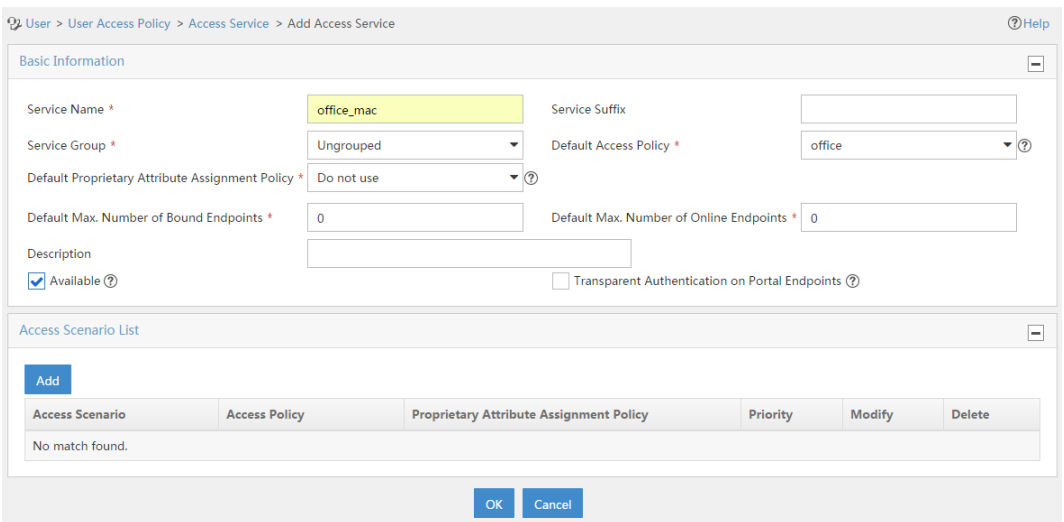
   e. **OK**をクリックします。

図3 アクセスポリシーの追加



3. アクセスサービスを追加します。
   a. **User**タブをクリックします
   b. ナビゲーションツリーで、**User Access Policy > Access Service**を選択します。
   c. **Add**をクリックします。
   d. **Add Access Service**ページで、図4に示すように、次のパラメータを設定します。
      - **Service Name**フィールドに**office_mac**と入力します。
      - **Default Access Policy**リストから**office**を選択します。
      - 他のパラメータにはデフォルト値を使用します。
   e. **OK**をクリックします。

図4 アクセスサービスの追加



4. アクセスユーザーを追加します。
   a. **User**タブをクリックします。
   b. ナビゲーションツリーから**Access User > All Access Users**を選択します。

アクセスユーザーリストが表示されます。

c. **Add**をクリックします。

Access User pageページが開きます。

d. **Access Information**領域で、図5に示すように、ユーザを追加します

- **Add User**をクリックします。
- 表示されたダイアログボックスでUser Nameフィールドと**Identity Number**フィールドに**adm_office_mac**と入力します。
- Usernameとidentity numberの正当性を調べるために**Check Availability**をクリックします。
- **OK**をクリックします。

e. **Access Information**領域で、図6に示すように、次のパラメータを設定します。

a. Account Nameフィールドに**3891d5833b20**と入力します。

b. **Password**フィールドと**Confirm Password**フィールドに**3891d5833b20**と入力します。

f. **Access Service**領域で、リストから**office_mac**を選択します。

g. **OK**をクリックします。

図5 ユーザーの追加

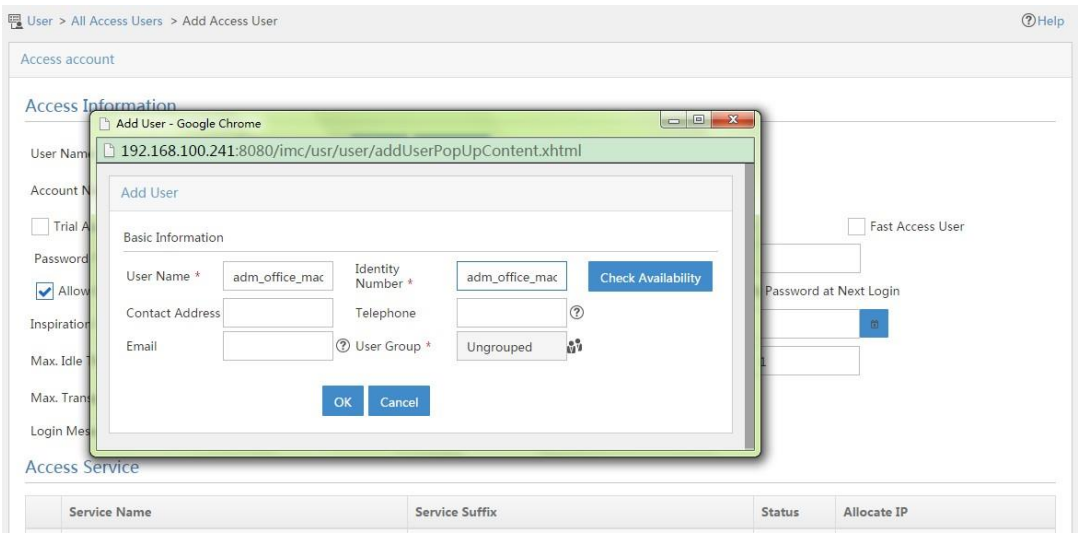
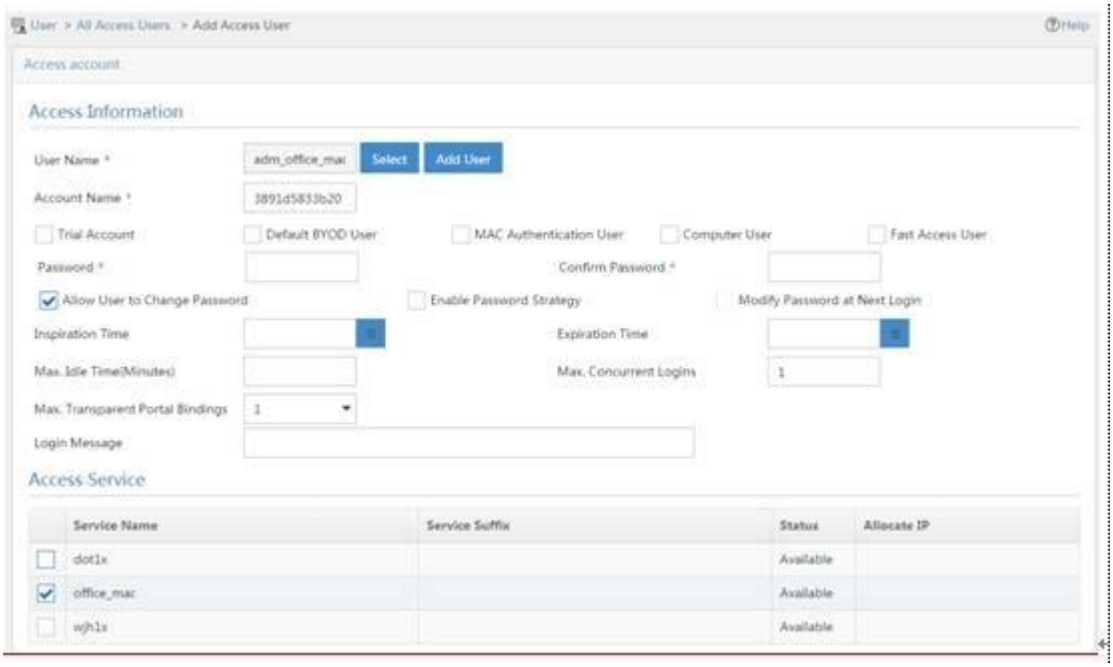


図6 アクセスユーザーアカウントの追加



設定の確認

クライアントはネットワークへのアクセスを要求します。

#ACで、ワイヤレスクライアントがMAC認証およびPSK認証にパスし、VLAN200でオンラインになることを確認します。

[AC] display wlan client

Total number of clients : 1

MAC address	Username	AP name	RID	IP address	IP address	VLAN
3891-d583-3b20	3891d5833b20	officeap	2	112.13.0.2	N/A	200

設定ファイル

- AC:

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
  gateway-list 112.12.1.25
  network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
```

```
  gateway-list 112.13.1.25
  network 112.13.0.0 mask 255.255.0.0
#
wlan service-template 1
  ssid service
  vlan 200
  akm mode psk
  preshared-key pass-phrase cipher
  $c$3$heDUT35pq2/Zmsuy18nxS3vSHAeolC6kobTrDA==
  cipher-suite ccmp
  security-ie rsn
  client-security authentication-mode mac
  mac-authentication domain office1
  service-template enable
#
interface Vlan-interface100
  ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
  ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200
  port trunk pvid vlan 100
#
radius scheme office
  primary authentication 8.1.1.50
  primary accounting 8.1.1.50
  key authentication cipher
  $c$3$o/3Ueu4pLSdJ0r1kLdAwzJU/AaBGCxnGuBXHmQ==
  key accounting cipher $c$3$oKqS/GRbPQc8AG+Vp+bJO4ZPKlk5+ceFuye/tQ==
  user-name-format without-domain
  nas-ip 112.12.1.25
#
domain office1
  authorization-attribute idle-cut 15 1024
  authentication lan-access radius-scheme office
  authorization lan-access radius-scheme office
  accounting lan-access radius-scheme office
#
wlan ap officeap model WA560-WW
  serial-id 219801A1NM8182032235
  vlan 1
  radio 1
  radio 2
    radio enable
    service-template 1
```

- Switch:

```
#
vlan 1
#
```

```
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port access vlan 100
  poe enable
#
```

関連ドキュメント

- *Layer 3—IP Services Command Reference in H3C Access Controllers Command References*
- *Layer 3—IP Services Configuration Guide in H3C Access Controllers Configuration Guides*Layer 3—IP Services Configuration Guide in H3C Access Controllers Configuration GuidesLayer 3—IP Services Configuration Guide in H3C Access Controllers Configuration Guides*Layer 3—IP Services Configuration Guide in H3C Access Controllers Configuration Guides*
- *Security Command Reference in H3C Access Controllers Command References*Security Command Reference in H3C Access Controllers Command ReferencesSecurity Command Reference in H3C Access Controllers Command References*Security Command Reference in H3C Access Controllers Command References*
- *Security Configuration Guide in H3C Access Controllers Configuration Guides*Security Configuration Guide in H3C Access Controllers Configuration GuidesSecurity Configuration Guide in H3C Access Controllers Configuration Guides*Security Configuration Guide in H3C Access Controllers Configuration Guides*
- *WLAN Command Reference in H3C Access Controllers Command References*WLAN Command Reference in H3C Access Controllers Command ReferencesWLAN Command Reference in H3C Access Controllers Command References*WLAN Command Reference in H3C Access Controllers Command References*
- *WLAN Configuration Guide in H3C Access Controllers Configuration Guides*WLAN Configuration Guide in H3C Access Controllers Configuration GuidesWLAN Configuration Guide in H3C Access Controllers Configuration Guides*WLAN Configuration Guide in H3C Access Controllers Configuration Guides*