H3Cアクセスコントローラ
Comware7 リモートポータル認証の設定例

内容

はじめに

このドキュメントでは、リモートポータル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。

このドキュメントでは、AAA、ポータル、およびWLANに関する基本的な知識があることを前提としています。

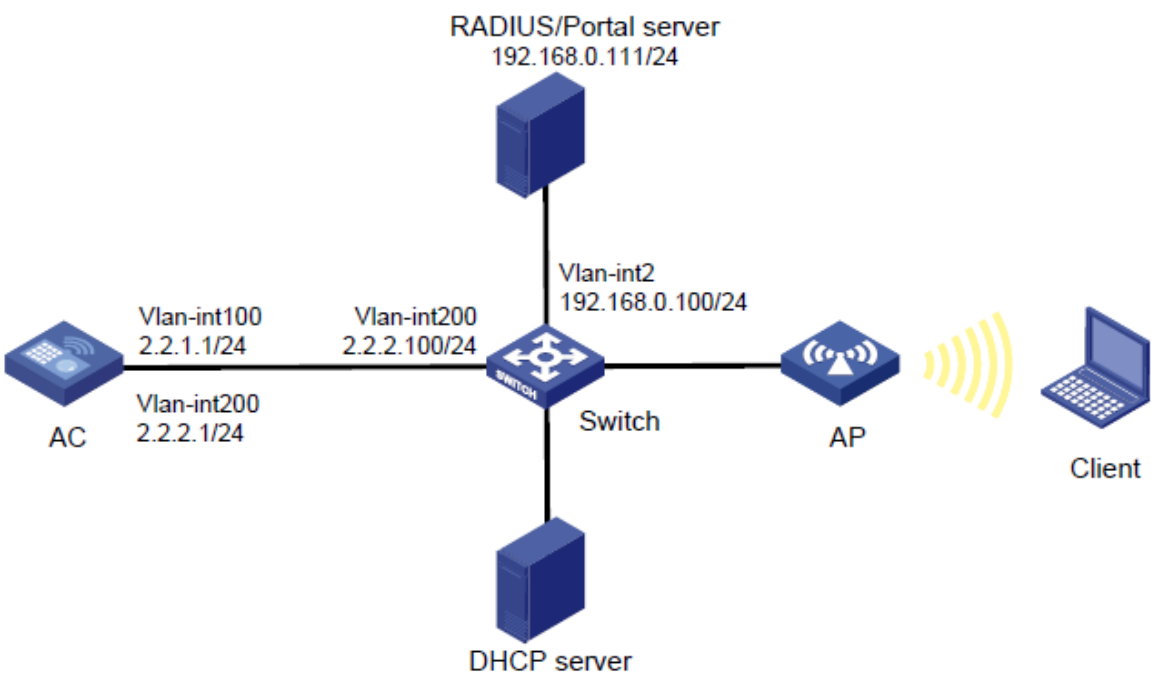
例:リモートポータル認証の設定

ネットワーク構成

図1に示すように、APとクライアントはDHCPサーバーからIPアドレスを取得します。リモートポータル認証を実装するには、次のタスクを実行します。

- 直接ポータル認証を設定します。
- iMCでポータル認証サーバーおよびポータルWebサーバーを設定します。
- RADIUSサーバーを認証サーバーおよびアカウンティングサーバーとして設定します。

図1 ネットワーク図



解析

クライアントがポータルWebサーバーにアクセスできるようにするには、ポータルWebサーバー宛てのトラフィックを許可するポータルフリールールを構成します。

認証されたユーザーがアクセスVLAN内のレイヤ2ポートのネットワークリソースに再認証なしでアクセスできるようにするには、ポータルローミングをイネーブルにします。

ポータルクライアントの頻繁なログインおよびログアウトによって短時間で認証が失敗する可能性を回避するには、ポータルクライアントのRule ARPエントリ機能をディセーブルにします。

RADIUSサーバーがユーザー認可情報を動的に変更したり、ユーザーを強制的に切断したりするには、RADIUSセッション制御機能をイネーブルにします。

制限事項およびガイドライン

リモートポータル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。

- 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。
- ACで指定されたポータル認証サーバーおよびポータルWebサーバーのタイプが、実際に使用されているものと同じであることを確認します(この例ではCMCCサーバーを使用します)。
- デフォルトでは、ユーザーにリダイレクトされるポータルWebサーバーのURLにはパラメータがありません。必要に応じて、リダイレクトURLにパラメータを含めるように構成できます。

手順

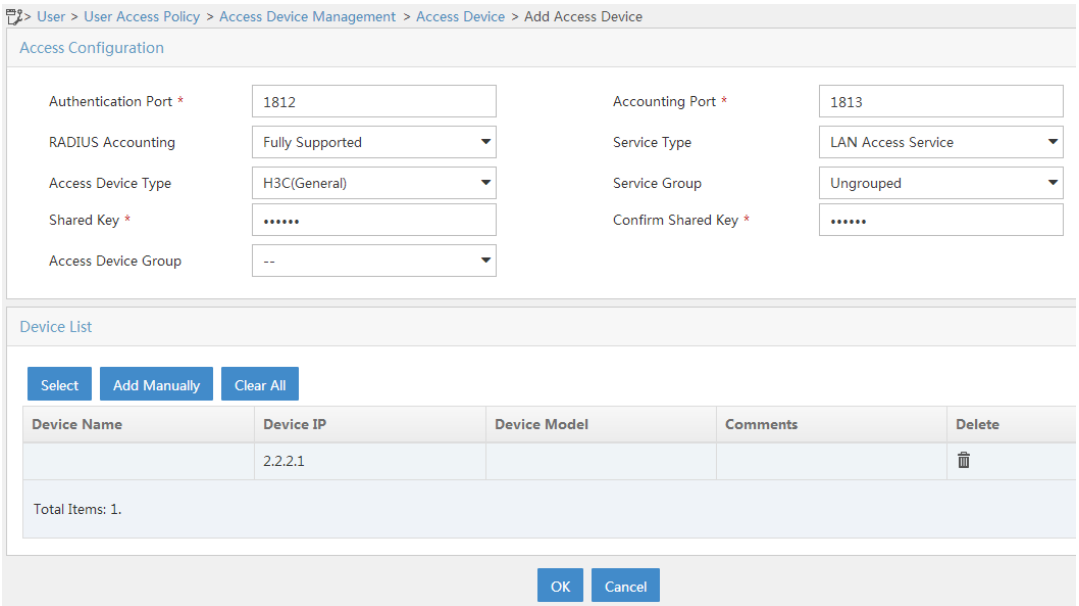
iMCの設定

この例では、iMCサーバーを使用して、RADIUSサーバーおよびポータルサーバーの構成を説明します。iMCサーバーは、iMC PLAT7.1(E0303p13)、iMC EIA7.1(F0302p08)およびiMC EIP7.1(F0302p08)上で稼働します。

RADIUSサーバーの設定

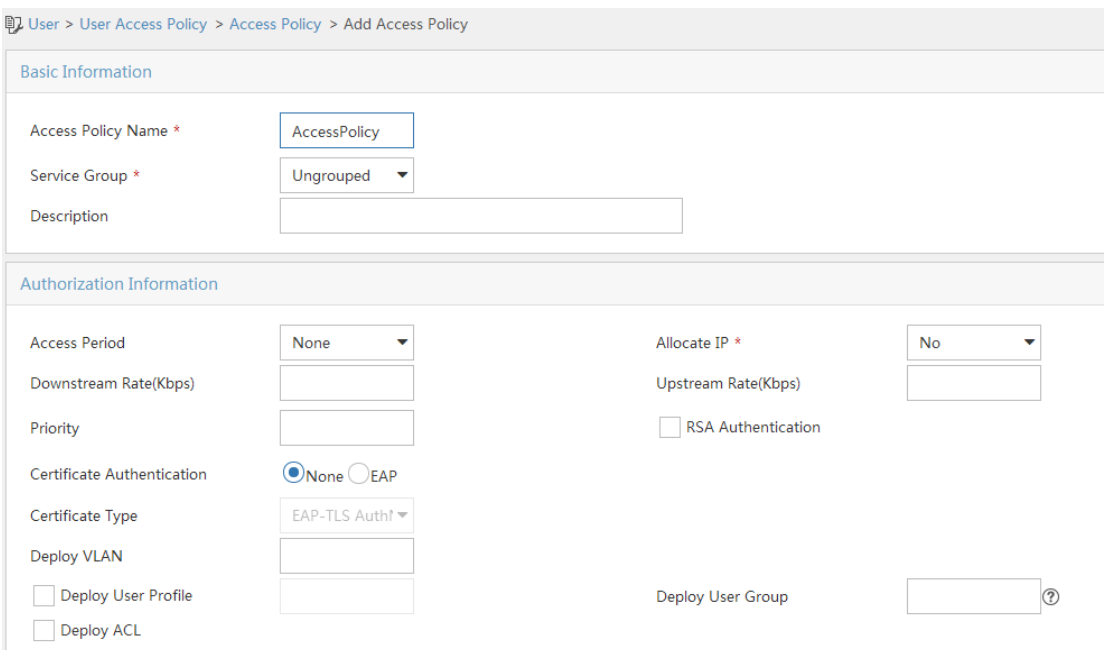
1. アクセスデバイスを追加します。
   a. iMCにログインして、**User**タブをクリックします。
   b. ナビゲーションツリーで、**User Access Policy > Access Device Management > Access Device**を選択します。
   c. 図2に示すように、**Add**をクリックしてページを開きます。
   d. **Device List**領域で、**Add Manually**をクリックして**Add Access Device Manually**を開きます。**Start IP**フィールドに**2.2.2.1**と入力し、**OK**をクリックします。
   e. **Access Configuration**領域で、共有キーを**radius**に設定します。これは、ACで設定されているものと同じである必要があります。
   f. その他のパラメータにはデフォルト設定を使用します。
   g. **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. ナビゲーションツリーで、**User Access Policy > Access Policy**を選択します。
   b. 図3に示すように、**Add**をクリックしてページを開きます。
   c. アクセスポリシー名を入力します。
   d. サービスグループを選択します。
   e. その他のパラメータにはデフォルト設定を使用します

図3 アクセスポリシーの追加

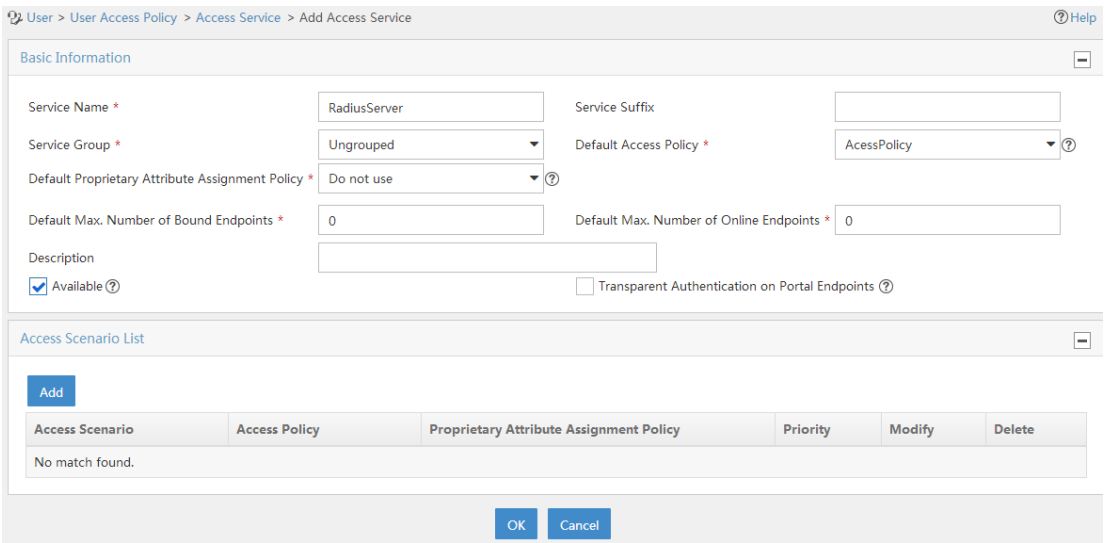


3. アクセスサービスを追加します。
   a. ナビゲーションツリーで、**User Access Policy>Access Service**を選択します。
   b. 図4に示すように、**Add**をクリックしてページを開きます。
   c. サービス名を入力します。

d. その他のパラメータにはデフォルト設定を使用します。

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

b. 図5に示すように、**Add**をクリックしてページを開きます。

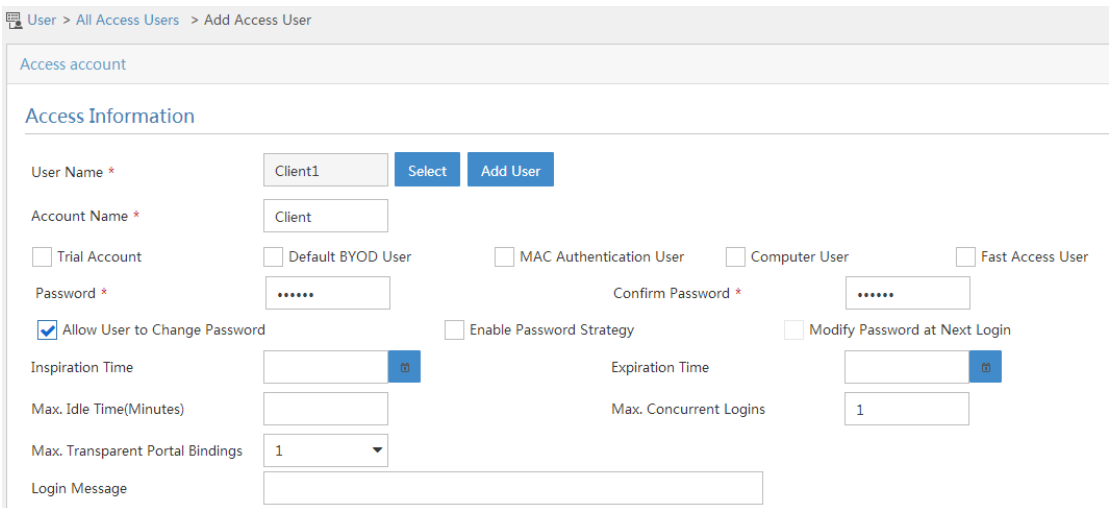
c. 既存のアクセスユーザーを選択するか、**Add User**をクリックして新規アクセスユーザーを追加します。

d. パスワードを設定します。

e. その他のパラメータにはデフォルト設定を使用します。

f. **OK**をクリックします。

図5 アクセスユーザーの追加



ポータルサーバーの構成

1. ポータル認証サービスを構成します。

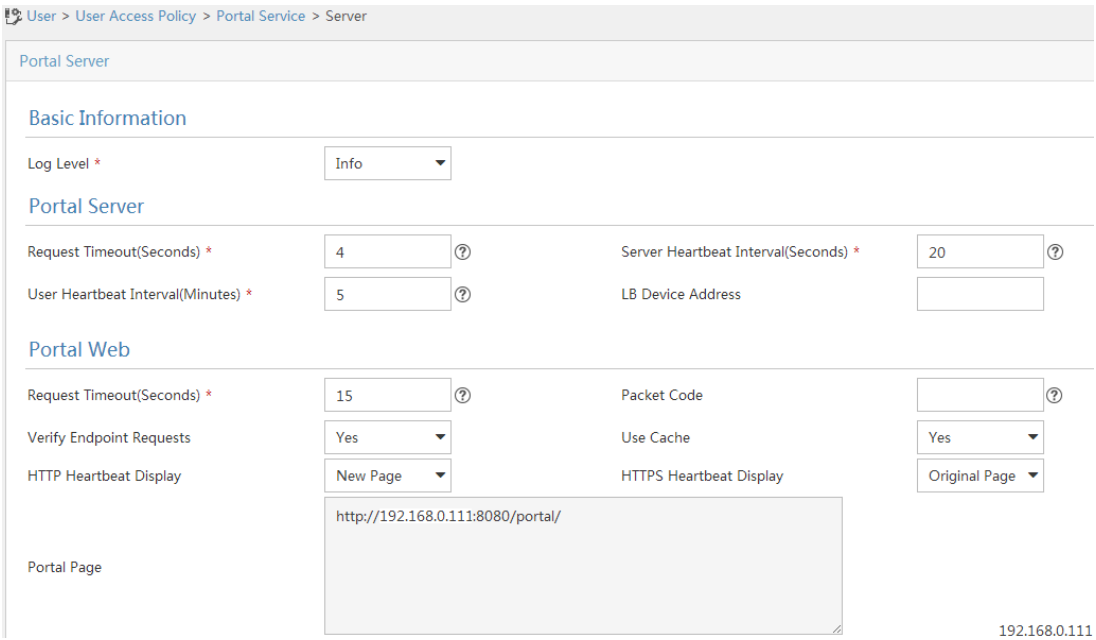
a. 図6に示すように、ナビゲーションツリーから**User Access Policy > Portal Service >**

Serverを選択して、ポータルサーバーの構成ページを開きます。

b. 必要に応じてポータルサーバーパラメータを構成します。この例では、デフォルト設定を使用しています。

c. **OK**をクリックします。

図6 ポータルサーバーの構成



2. 次のようにIPアドレスグループを設定します。

a. ナビゲーションツリーで、**User Access Policy > Portal Service > IP Group**を選択します。

b. 図7に示すように、**Add**をクリックしてページを開きます。

c. IPグループ名を入力します。

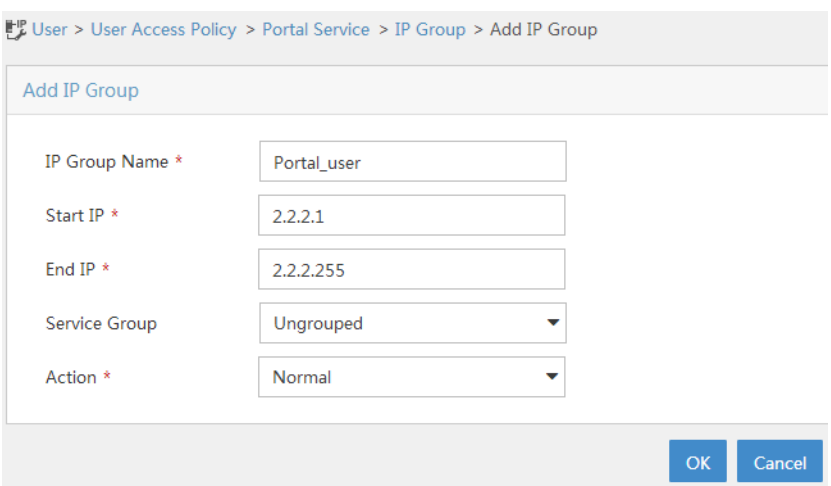
d. IPグループの開始IPアドレスと終了IPアドレスを入力します。クライアントIPアドレスがIPグループに含まれていることを確認してください。

e. サービスグループを選択します。
この例では、既定のグループ**Ungrouped**を使用します。

f. **Action**リストから**Normal**を選択します。

g. **OK**をクリックします。

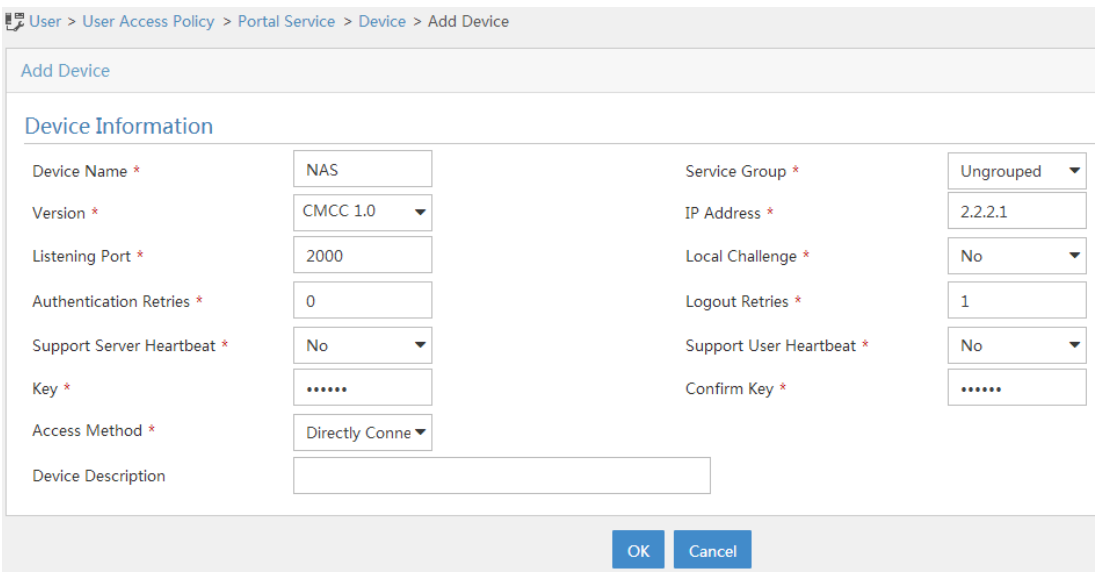
図7 IPアドレスグループの追加



3. ポータルデバイスを追加します。
   a. ナビゲーションツリーで、**User Access Policy > Portal Service > Device**を選択します。
   b. 図8に示すように、**Add**をクリックしてページを開きます。
   c. デバイス名を入力します。
   d. **Version**に**CMCC 1.0**を選択します。
   e. クライアントに接続されているACのインターフェイスのIPアドレスを入力します。
   f. ポータルサーバーのハートビートおよびユーザーのハートビート機能をサポートするかどうかを設定します。

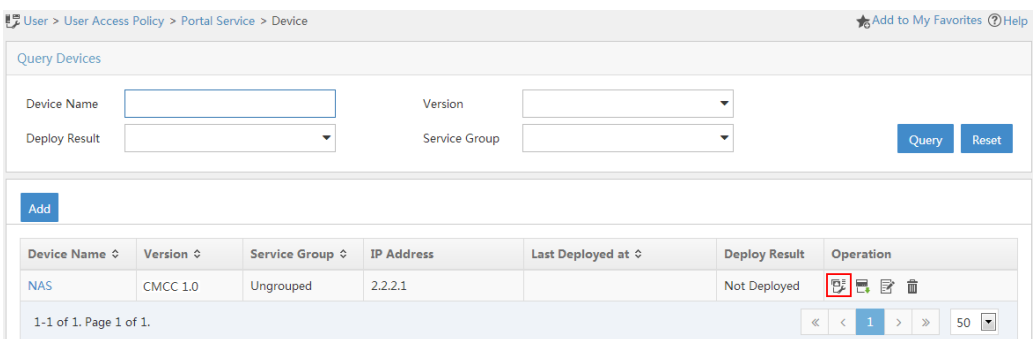
      この例では、**Support Server Heartbeat**と**Support User Heartbeat**の両方に対して**No**を選択します。
   g. キーを入力します。キーは、ACに設定されているキーと同じである必要があります。
   h. **Access Method**で**Directly Connected**を選択します。
   i. その他のパラメータにはデフォルト設定を使用します。
   j. **OK**をクリックします。

図8 ポータルデバイスの追加



4. ポータルデバイスをIPアドレスグループに関連付けます。
   a. 図9に示すように、デバイス**NAS**の**Operation**フィールドで**Port Group**アイコンをクリックします。

図9 デバイスリスト



b. 図10に示すように、**Add**をクリックしてページを開きます。

c. ポートグループ名を入力します。

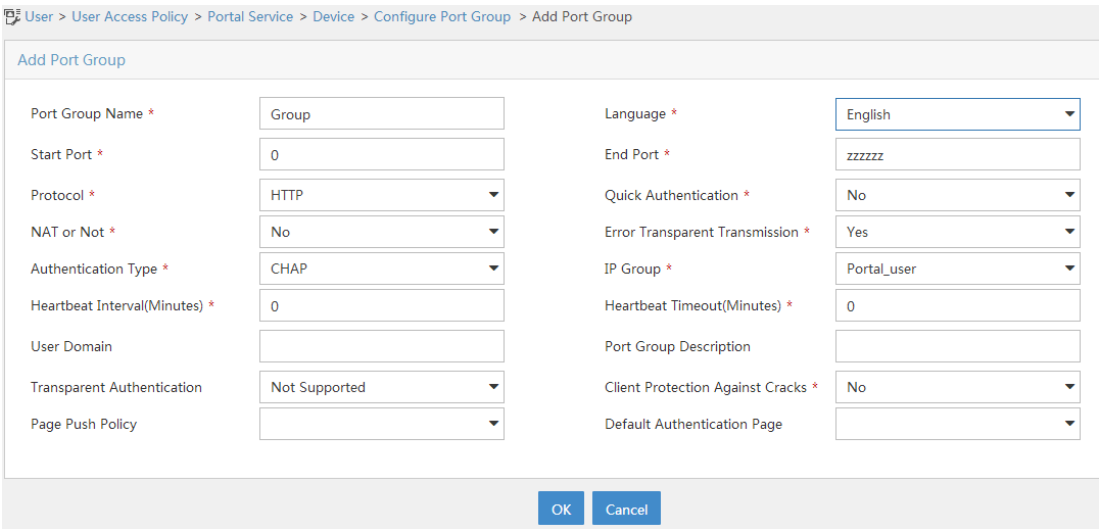
d. 設定済みのIPアドレスグループを選択します。

ユーザーがネットワークにアクセスするために使用するIPアドレスは、このIPアドレスグループ内にある必要があります。

e. その他のパラメータにはデフォルト設定を使用します。

f. **OK**をクリックします。

図10 ポートグループの追加



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-interface100を作成します。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 2.2.1.1 24

[AC-Vlan-interface100] quit

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

[AC] vlan 200

[AC-vlan200] quit

[AC] interface vlan-interface 200

[AC-Vlan-interface200] ip address 2.2.2.1 24

[AC-Vlan-interface200] quit

2. iMCサーバーに到達するためのスタティックルートを設定します。

[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100

3. ワイヤレスサービスを設定します。

#**st1**という名前のサービステンプレートを作成し、そのビューに入ります。

[AC] wlan service-template st1

#サービステンプレート**st1**のSSIDを**service**に設定します。

[AC-wlan-st-st1] ssid service

#サービステンプレート**st1**を介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-service] vlan 200

#ISPドメイン**dm1**をサービステンプレート**st1**上のポータルユーザーの認証ドメインとして指定します。

[AC-wlan-st-st1] portal domain dm1

#サービステンプレート**st1**を有効にします。

[AC–wlan-st-st1] service-template enable

[AC-wlan-st-st1] quit

#モデル**WA560-WW**を使用してofficeという名前のAPを作成し、そのシリアルIDを

219801A1NM8182032235に設定します。

[AC] wlan ap office model WA560-WW

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

#設定ファイル**map.txt**をAPに展開します。

[AC-wlan-ap-office] map-configuration map.txt

#radio2のビューに入ります。

[AC-wlan-ap-office] radio 2

#サービステンプレート**st1**をAP **office** の無線2にバインドします。

[AC-wlan-ap-office-radio-2] service-template st1

#radio2を有効にします。

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

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

[AC-wlan-ap-office] quit

4. RADIUSスキームを設定します。

#**rs1**という名前のRADIUSスキームを作成し、そのビューに入ります。

[AC] radius scheme rs1

#プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

[AC-radius-rs1] primary authentication 192.168.0.111

[AC-radius-rs1] primary accounting 192.168.0.111

[AC-radius-rs1] key authentication simple radius

[AC-radius-rs1] key accounting simple radius

#RADIUSサーバーに送信されるユーザー名からドメイン名を削除するようにACを設定します。

[AC-radius-rs1] user-name-format without-domain

[AC-radius-rs1] quit

#RADIUSセッション制御機能をイネーブルにします。

[Router] radius session-control enable

5. 認証ドメインを構成します。

#**dm1**という名前のISPドメインを作成し、そのビューに入ります。

[AC] domain dm1

#ISPドメインの認証および認可方式をRADIUSに設定し、アカウンティング方式をnoneに設定します。

[AC-isp-dm1] authentication portal radius-scheme rs1

[AC-isp-dm1] authorization portal radius-scheme rs1

[AC-isp-dm1] accounting portal none

#ISPドメイン内のユーザーに対してアイドルカット機能を構成します。ユーザーのトラフィックが15分以内で1024バイトより少なければユーザーをログアウトします。

[AC-isp-dm1] authorization-attribute idle-cut 15 1024

[AC-isp-dm1] quit

6. ポータル認証を構成します。

#newptという名前のポータル認証サーバーを作成し、認証サーバーにIPアドレス192.168.0.111を指定し、リスニングポータルパケットのポート番号として50100を指定します。

[AC] portal server newpt

[AC-portal-server-newpt] ip 192.168.0.111 key simple radius

[AC-portal-server-newpt] port 50100

#ポータル認証サーバーnewptのタイプとしてCMCCを指定します。

[AC-portal-server-newpt] server-type cmcc

[AC-portal-server-newpt] quit

#**newpt**という名前のポータルWebサーバーを作成し、サーバーのURLとして**http://192.168.0.111:8080/portal**を指定します。

[AC] portal web-server newp

[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal

#ポータルWebサーバー**newpt**のURLパラメータ**ssid**、wlanuseripおよび**wlanacname**を構成します。それぞれ**ssid**、**wlanuserip**および**wlanacname**のパラメータの値として、APのSSID、クライアントのIPアドレスおよびACの名前を指定します(パラメータは、CMCCポータルWebサーバーのURLで搬送する必要があります)。

[AC-portal-websvr-newpt] url-parameter ssid ssid

[AC-portal-websvr-newpt] url-parameter wlanuserip source-address

[AC-portal-websvr-newpt] url-parameter wlanacname value AC

#ポータルWebサーバー**newpt**のタイプとしてCMCCを指定します。

[AC-portal-websvr-newpt] server-type cmcc

[AC-portal-websvr-newpt] quit

#宛先ベースのポータルフリー規則番号**0**を設定して、IPアドレス192.168.0.111(ポータルWebサーバー)宛てのトラフィックを許可します。

[AC] portal free-rule 0 destination ip 192.168.0.111 24

#ポータルローミングを有効にします。

[AC] portal roaming enable

#ポータルクライアントのルールARPエントリ機能をディセーブルにします。

[AC] undo portal refresh arp enable

#サービステンプレートst1で直接ポータル認証を有効にします。

[AC] wlan service-template st1

[AC-wlan-st-st1] portal enable method direct

#ISPドメイン**dm1**をポータル認証ドメインとして指定します。

[AC-wlan-st-st1] portal domain dm1

#サービステンプレートst1のポータルWebサーバー**newpt**をポータル認証用に指定します。

[AC-wlan-st-st1] portal apply web-server newpt

#ポータル認証サーバー**newpt**に送信されるポータルパケットのBAS-IPアトリビュートを2.2.2.2に設定します。

[AC-wlan-st-st1] portal bas-ip 2.2.2.1

[AC-wlan-st-st1] 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トンネル上で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を使用してクライアントトラフィックを転送します。

[Switch] vlan 200

[Switch-vlan200] quit

VLAN 2を作成します

[Switch] vlan 2

[Switch-vlan2] quit

#GigabitEthernet1/0/1(ACに接続されているポート)をトランクポートとして設定し、トランクポートをVLAN100およびVLAN200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] port trunk permit vlan 100 200

[Switch-GigabitEthernet1/0/1] quit

#GigabitEthernet1/0/2(APに接続されているポート)をアクセスポートとして設定し、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

アクセスポートのPoEをEnableにします

[Switch-GigabitEthernet1/0/2] poe enable

[Switch-GigabitEthernet1/0/2] quit

#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。

[Switch] interface vlan-interface 200

[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0

[Switch-Vlan-interface200] quit

#VLAN-interface2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。

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0

[Switch-Vlan-interface2] quit

設定の確認

#構成済のユーザー名とパスワードを使用して、クライアント上のWebブラウザを介してポータル認証を実行します。ポータル認証を渡す前に、ユーザーは認証ページ **http://192.168.0.111:8080/portal**にのみアクセスできます。ユーザーからのすべてのWeb要求は認証ページにリダイレクトされます。ポータル認証を渡した後、ユーザーは他のネットワークリソースにアクセスできます。

#すべてのポータルユーザーに関する情報を表示します。

```
[AC] display portal user all
Total portal users: 1
Username: Client
   Portal server: newpt
   State: Online
   VPN instance: N/A
   MAC                 IP              VLAN    Interface
   0021-6330-0933      2.2.2.2         200     Vlan-interface200
   Authorization information:
      DHCP IP pool: N/A
      User profile: N/A
      Session group profile: N/A
      ACL number: N/A
      Inbound CAR: N/A
      Outbound CAR: N/A
```

構成ファイル

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
  portal enable method direct
  portal domain dm1
  portal bas-ip 2.2.2.1
  portal apply web-server newpt
  service-template enable
#
interface Vlan-interface100
  ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.1 255.255.255.0
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
radius scheme rs1
  primary authentication 192.168.0.111
  primary accounting 192.168.0.111
  key authentication cipher $c$3$Sqgqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
  key accounting cipher $c$3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
  user-name-format without-domain
#
domain dm1
  authorization-attribute idle-cut 15 1024
  authentication portal radius-scheme rs1
```

```
  authorization portal radius-scheme rs1
  accounting portal none
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
#
portal roaming enable
undo portal refresh arp enable
#
portal web-server newpt
  url http://192.168.0.111:8080/portal
  server-type cmcc
  url-parameter ssid ssid
  url-parameter wlanacname value AC
  url-parameter wlanuserip source-address
#
portal server newpt
  ip 192.168.0.111 key cipher $c$3$Q82T/9AHq5HT7uFX7nho8K0Y6jziycoJTw==
  server-type cmcc
#
wlan ap office model WA560-WW
  serial-id 219801A1NM8182032235
  radio 1
  radio 2
   radio enable
   service-template st1
#
```

- Switch:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface200
  ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
```

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

関連ドキュメント

- *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*