H3Cアクセスコントローラ
Comware7 802.1X認証の様々な設定例

内容

例:802.1X CHAPローカル認証の設定

ネットワーク構成

図3に示すように、CHAPを使用してクライアントの802.1Xローカル認証を実行するようにACを構成します。

図3 ネットワーク図

手順

この例では、ローカルユーザーを含む基本的なAAA設定だけを示します。AAAコマンドの詳細については、『User Access and Authentication Command Reference』を参照してください。

1. 802.1Xおよびローカルクライアントの構成:

   # EAP終了を実行し、CHAPを使用するようにACを設定します。

   <AC> system-view

   [AC] dot1x authentication-method chap

   # ユーザー名**chap1**およびパスワード**123456**(プレーンテキスト)のローカルネットワークアクセスユーザーを追加します。

   [AC] local-user chap1 class network

   [AC-luser-network-chap1] password simple 123456

   # サービスタイプを**lan-access**に設定します。.

   [AC-luser-network-chap1] service-type lan-access

   [AC-luser-network-chap1] quit

2. ISPドメインのAAA方式を設定します:

   # **local**という名前のISPドメインを作成します。

   [AC] domain local

   # LANクライアントのローカル認証、ローカル認可、およびローカルアカウンティングを使用するようにISPドメインを設定します。

   [AC-isp-local] authentication lan-access local

   [AC-isp-local] authorization lan-access local

   [AC-isp-local] accounting lan-access local

   [AC-isp-local] quit

3. サービステンプレートを設定する:

   # **wlas_local_chap**という名前のサービステンプレートを作成します。.

   [AC] wlan service-template wlas_local_chap

   # 認証モードを802.1Xに設定します。

   [AC-wlan-st-wlas_local_chap] client-security authentication-mode dot1x

   # サービステンプレートのISPドメイン**local**を指定します。

[AC-wlan-st-wlas_local_chap] dot1x domain local

SSIDを**wlas_local_chap**に設定します。.

[AC-wlan-st-wlas_local_chap] ssid wlas_local_chap

サービステンプレートをイネーブルにします。

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

[AC-wlan-st-wlas_local_chap] quit

4. 手動AP **ap1**を設定し、サービステンプレートをAP無線にバインドします:

ap1を作成し、APモデルとシリアルIDを指定します。

[AC] wlan ap ap1 model WA6638-JP

[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050

チャネル149をAPの無線1の作業チャネルとして設定し、無線1をイネーブルにします。

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel 149

[AC-wlan-ap-ap1-radio-1] radio enable

サービステンプレート**wlas_local_chap**をradio1にバインドします。

[AC-wlan-ap-ap1-radio-1] service-template wlas_local_chap

[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] quit

設定の確認

802.1X構成を確認する.

[AC] display wlan service-template

[AC] display dot1x

#802.1Xクライアントが認証にパスした後にクライアント接続情報を表示します。

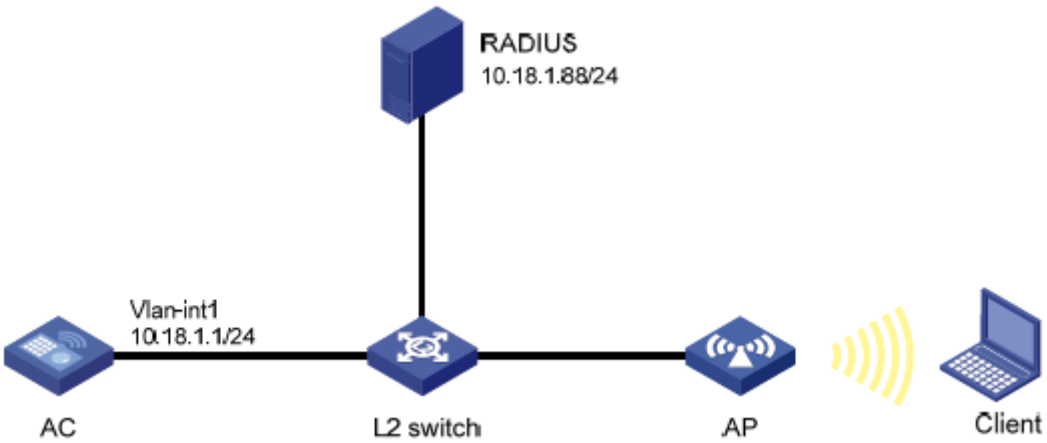
[AC] display dot1x connection

例:802.1X EAP-PEAP RADIUS認証の設定

ネットワーク構成

図4に示すように、EAP-PEAPを使用してクライアントに802.1X RADIUS認証を実行するようにACを設定します。.

図4 ネットワーク図



手順

この例では、RADIUSを含む基本的なAAA設定だけを示します。AAAコマンドの詳細については、『User Access and Authentication Command Reference』を参照してください。

1. ACを次のように設定します。
   a. 802.1XおよびRADIUSスキームを設定します。

      # EAPリレーを使用して802.1Xクライアントを認証するようにACを設定します。

      <AC> system-view

      [AC] dot1x authentication-method eap

      # RADIUSスキームを作成します。

      [AC] radius scheme imc

      # 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ます。

      [AC-radius-imc] primary authentication 10.18.1.88 1812

      [AC-radius-imc] primary accounting 10.18.1.88 1813

      #サーバーとのセキュアな通信のための共有キーをプレーンテキストで12345678に設定します。

      [AC-radius-imc] key authentication simple 12345678

      [AC-radius-imc] key accounting simple 12345678

      # RADIUSサーバーに送信されるユーザー名からドメイン名を除外します。

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

      [AC-radius-imc] quit

   b. ISPドメインのAAA方式を設定します。

      # imcという名前のISPドメインを作成します。

      [AC] domain imc

LANクライアントの認証、認可、およびアカウンティングにRADIUSスキームimcを使用するようにISPドメインを設定します。

[AC-isp-imc] authentication lan-access radius-scheme imc

[AC-isp-imc] authorization lan-access radius-scheme imc

[AC-isp-imc] accounting lan-access radius-scheme imc

[AC-isp-imc] quit

c. サービステンプレートを設定します。

wlas_imc_peapという名前のサービステンプレートを作成します。

[AC] wlan service-template wlas_imc_peap

認証モードを802.1Xに設定します。

[AC-wlan-st-wlas_imc_peap] client-security authentication-mode dot1x

サービステンプレートのISPドメインimcを指定します。

[AC-wlan-st-wlas_imc_peap] dot1x domain imc

SSIDをwlas_imc_peapに設定します。

[AC-wlan-st-wlas_imc_peap] ssid wlas_imc_peap

AKMモードを802.1Xに設定します。

[AC-wlan-st-wlas_imc_peap] akm mode dot1x

CCMP暗号スイートを設定します。

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

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-wlas_imc_peap] 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-wlas_imc_peap] service-template enable

[AC-wlan-st-wlas_imc_peap] quit

d. 手動AP ap1を設定し、サービステンプレートをAP無線にバインドします。:

ap1を作成し、APモデルとシリアルIDを指定します。

[AC] wlan ap ap1 model WA6638-JP

[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050

チャネル149をAPの無線1の作業チャネルとして設定し、無線1をイネーブルにします。

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel 149

[AC-wlan-ap-ap1-radio-1] radio enable

サービステンプレートwlas_imc_peapをradio1にバインドします。

[AC-wlan-ap-ap1-radio-1] service-template wlas_imc_peap

[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] quit

2. RADIUSサーバーを設定します。

この例では、RADIUSサーバーはIMC PLAT7.1およびIMC UAM7.1を実行し、EAP-PEAP証明書がインストールされています。

アクセスデバイスを追加する:

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 Device Management > Access Device**を選択します。

b. **Add**をクリックします。

Add Access Deviceページが表示されます。

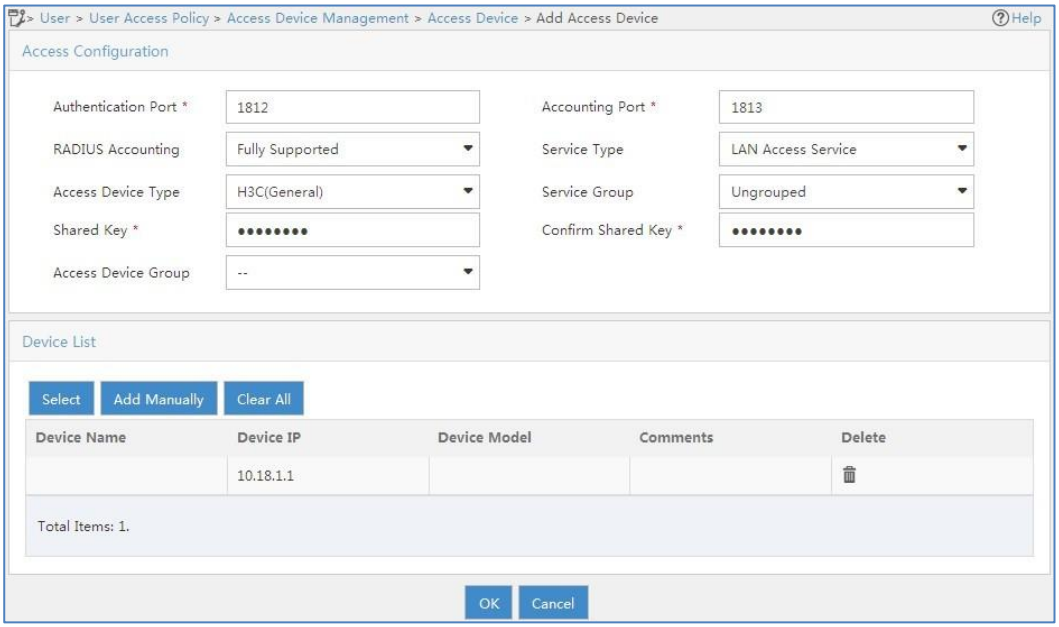
c. **Access Configuration**領域で、図5に示すように、次のパラメーターを設定します。

- Shared KeyフィールドとConfirm Shared Keyフィールドに12345678と入力します。
- 他のパラメーターにデフォルト値を使用します。.

e. Device List領域で、SelectまたはAdd Manuallyをクリックして、10.18.1.1にあるデバイスをアクセスデバイスとして追加します。.

f. OKをクリックします。

図5 アクセス装置の追加



アクセスポリシーを追加する:

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。

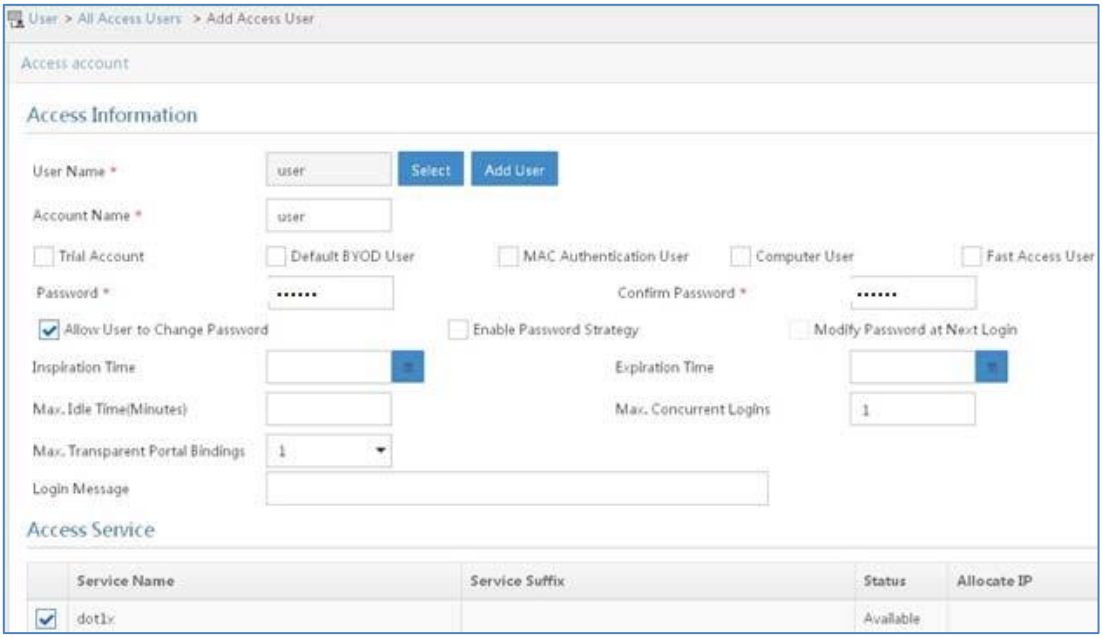
d. 図6に示すように、**Add Access Policy**ページで、次のパラメーターを構成します。:

- Access Policy Nameフィールドにdot1xと入力します。
- Certificate AuthenticationフィールドでEAPを選択します。
- CertificateTypeリストかEAP-PEAPAuthを選択し、CertificateSub-TypeリストかMS-CHAPV2Authを選択します。

iMCサーバーの証明書サブタイプは、クライアントで構成されているID認証方法と同じである必要があります。

e. **OK**をクリックします。

図6 アクセスポリシーの追加



#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 Polic > Access Service**を選択します。

c. **Add**をクリックします。

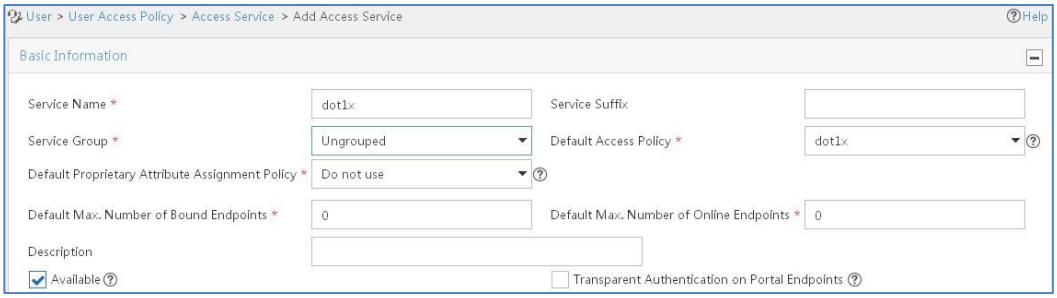
d. **Add Access Service**ページで、図7に示すように、次のパラメーターを設定します。

– **Service Name**フィールドに**dot1x**と入力します。

– **Default Access Policy**リストから**dot1x**を選択します。

e. **OK**をクリックします。

図7 アクセスサービスの追加



#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で、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。

Add Access Userページが表示されます。

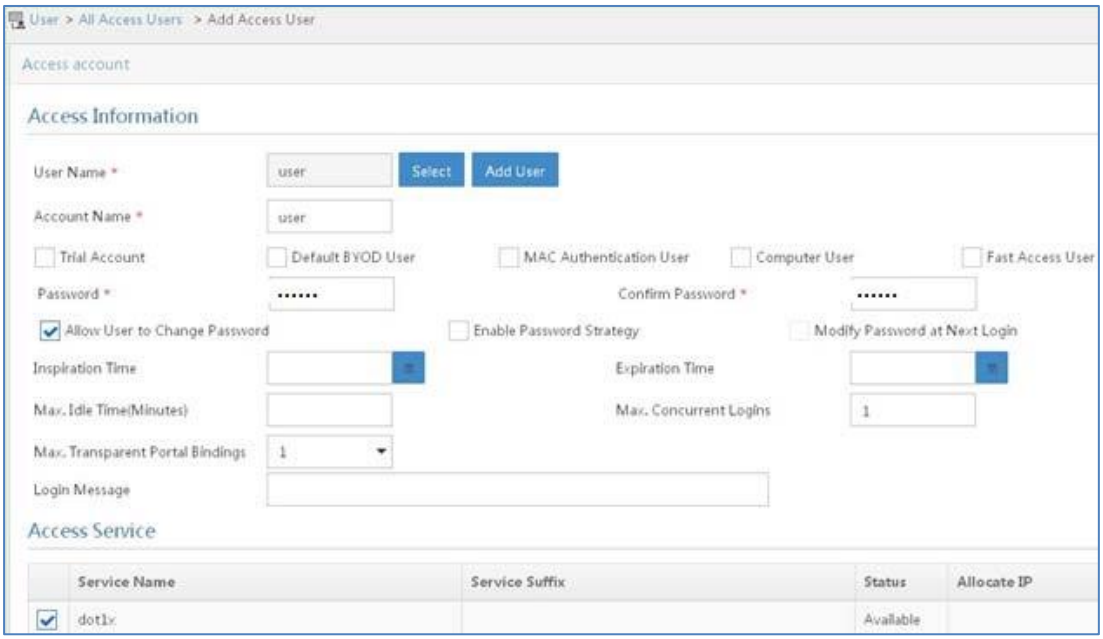
d. Access Information領域で、図8に示すように、次のパラメーターを設定します:

- Select or Add Userをクリックして、ユーザーをIMCプラットフォームユーザーuserに関連付けます。.
- Account Nameフィールドにuserを入力します。.
- PasswordおよびConfirm Passwordフィールドにdot1xと入力します。.

e. Access Service領域で、リストからdot1xを選択します。.

f. OKをクリックします。.

図8 アクセスユーザーカウントの追加



3. WLANクライアントを設定する:

WLANクライアントがEAP-PEAP証明書とともにインストールされている。.

WLANクライアントを設定するには、次のタスクを実行します(詳細は省略)。:

- ID認証にPEAPを選択します。.
- クライアントによるサーバー証明書の検証を無効にします。.
- Windowsのログイン名とパスワードを使用してクライアントが自動的に使用できないようにする.

設定の確認

1. クライアントで、ユーザー名userおよびパスワードdot1xを使用してネットワークにアクセスできることを確認します。(詳細は省略)。

2. ACで次のタスクを実行して、ユーザーが認証にパスし、オンラインになったことを確認します。:

```
# Display online 802.1X client information.
[AC] display dot1x connection
User MAC address        : 0023-8933-2090
AP name                 : ap1
Radio ID                : 1
SSID                    : wlas_imc_peap
BSSID                   : 000f-e201-0003
```

```
User name                    : user
```

Authentication domain : imc
Authentication method :
EAP
Initial VLAN : 1
Authorization VLAN : N/A
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action : Default
Session timeout period : 6001 s
Online from : 2014/04/18 09:25:18
Online duration : 0h 1m 1s

Total connections: 1.
Display WLAN client information.
[AC] display wlan client
Total number of clients : 1

MAC address	Username	AP name	R IP address	
	VLAN0023-8933-2090 user	ap1	1	
10.18.1.100		1		