H3Cアクセスコントローラ

Comware7 802.1X認証の様々な設定例

Copyright©2019New H3C Technologies Co.,Ltd.All rights reserved.

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の事前の書面による同意なしには、いかなる形式または手段によっても複製または変更することはできません。

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されている商標は、それぞれの所有者の所有物です。

本ドキュメントの情報は、予告なく変更されることがあります。

内容

例:802.1X CHAPローカル認証の設定	. 3
例:802.1X EAP-PEAP RADIUS認証の設定	. 5

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
 [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。.





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

5

#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] guit

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[こ設定します。
[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
[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。

Authentication Port *	1812		Accounting Port *	1813		
RADIUS Accounting	Fully Supported	-	Service Type	LAN Access Servi	ce 💌	
Access Device Type	H3C(General)	•	Service Group	Ungrouped	•	
Shared Key *	•••••		Confirm Shared Key *	•••••		
Access Device Group	220	-				
vice List						
vice List Select Add Manually	Clear Ali					
vice List Select Add Manually Device Name	Clear All Device IP	Device Model	Comment	s I	Delete	
vice List Select Add Manually Device Name	Clear All Device IP 10.18.1.1	Device Model	Comment	s I	Delete	

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

User > All Access Users > Add Acc	ess User			
Access account				
Access Information				
User Name *	user	Add User		
Account Name *	user			
Trial Account	Default BYOD User	MAC Authentication User	Computer User	Fast Access User
Password *		Confirm Passwor	* • • • • • •	
Allow User to Change Passwor	d	Enable Password Strategy	Modify Password	at Next Login
Inspiration Time		Expiration Time		- 10
Max. Idle Time(Minutes)		Max. Concurrent	Logins 1	
Max. Transparent Portal Bindings	1 .			
Login Message				
Access Service				
Service Name		Service Suffix	Status	Allocate IP
dotlx.			Available	

#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

User > User Access Policy > Access Service > Add	Access Service				(?) Help
Basic Information					-
Service Name *	dot1×		Service Suffix		
Service Group *	Ungrouped	•	Default Access Policy *	dot1×	• ?
Default Proprietary Attribute Assignment Policy *	Do not use	•	0		
Default Max. Number of Bound Endpoints *	0		Default Max. Number of Online Endpoints *	0	
Description					
✓ Available ⑦			Transparent Authentication on Portal End	dpoints 🕐	

#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

User > All Access Users > Add Acc	ess User					
Access account						
Access Information						
User Name *	user	Select	Add User			
Account Name *	user					
Trial Account	Default BYOD U	ser	MAC Authentication User	Computer User		Fast Access Use
Password *			Confirm Password *			
Allow User to Change Passwor	d		Enable Password Strategy	Modif	Password a	t Next Login
Inspiration Time			Expiration Time	[7
Max. Idle Time(Minutes)			Max. Concurrent Log	gins	1	
Max. Transparent Portal Bindings	1 •					
Login Message						
Access Service						
Service Name			Service Suffix		Status	Allocate IP
dotlx.					Available	

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 do	omain	: imc						
Authentication m	ethod	:						
EAP								
Initial VLAN		: 1						
Authorization VL/	AN	: N/A						
Authorization AC	L number	: N/A						
Authorization use	er profile : N/	Ά						
Termination actio	n	: Default						
Session timeout	period	: 6001 s						
Online from		: 2014/04/18 09:25:18	}					
Online duration		: 0h 1m 1s						
Total connections	s: 1.							
# Display WLAN	client informa	ation.						
[AC] display wlan	client							
Total number of o	clients	: 1						
MAC address	Jsername	AP name	R IP address					
N	/LAN0023-8	933-2090 user	ap1	1				
10.18.1.100		1						