H3Cアクセスコントローラ
Comware7 リモート802.1X認証の設定例

内容

はじめに

このドキュメントでは、ワイヤレスクライアントにリモート802.1X認証を設定する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、WLANアクセス、WLANセキュリティ、WLAN認証、および802.1X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802.1X認証の設定

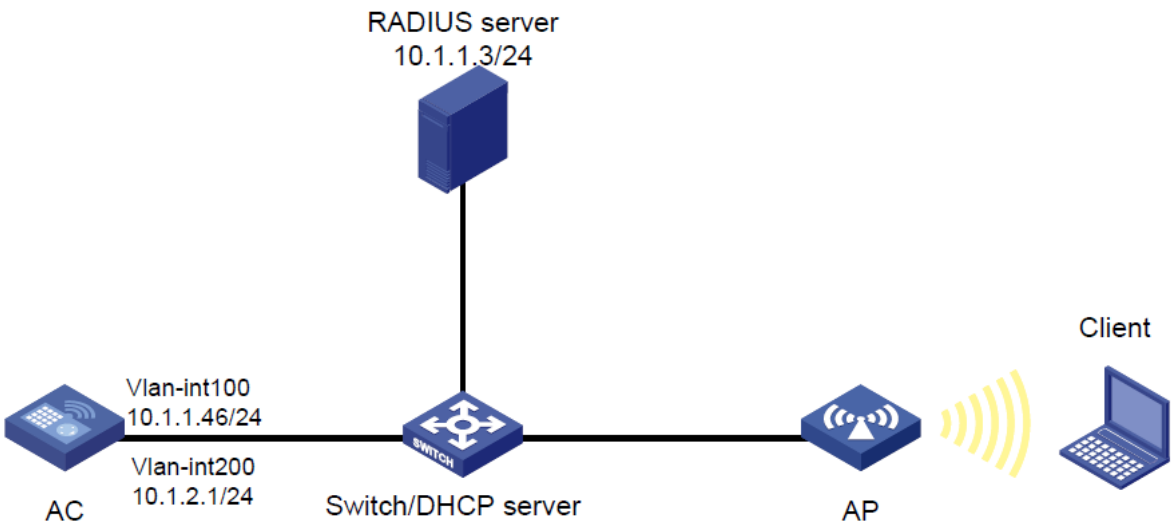
ネットワーク構成

図1に示すように、スイッチはAPおよびクライアントにIPアドレスを割り当てるDHCPサーバとして機能します。

次の要件を満たすように、AC、クライアント、スイッチ、およびRADIUSサーバを設定します。

- ACはRADIUSサーバを使用して、ワイヤレスクライアントの802.1X認証を実行します。
- ACは、データリンク層でクライアントにオープンシステム認証を使用します。これはデフォルトの認証方法です。
- ACは802.1X AKMモードを使用して、クライアントとAP間のデータ伝送を保護します。
- 暗号スイートはCCMPである。

図1:ネットワーク図



制限事項およびガイドライン

ワイヤレスクライアントにリモート802.1X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。
- クライアントがオンラインになったときにダイナミック認可が失敗しないようにするには、RADIUS DAS機能を設定します。

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 10.1.1.46 24

   [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 10.1.2.1 24

   [AC-Vlan-interface200] quit

2. RADIUSスキームを設定します。

#radius1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 radius1

#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-radius1] primary authentication 10.1.1.3

[AC-radius-radius1] primary accounting 10.1.1.3

#サーバとの安全な通信のために、プレーンテキストで共有キーを12345に設定します。

[AC-radius-radius1] key authentication simple 12345

[AC-radius-radius1] key accounting simple 12345

#発信RADIUSパケットの送信元IPアドレスとしてIPアドレス10.1.2.1を指定します。

[AC-radius-radius1] nas-ip 10.1.2.1

[AC-radius-radius1] quit

#dom1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 dom1

#RADIUSスキームradius1をISPドメインdom1に適用して、LANユーザの認証、認可、アカウンティングを行います。

[AC-isp-dom1] authentication lan-access radius-scheme radius1

[AC-isp-dom1] authorization lan-access radius-scheme radius1

[AC-isp-dom1] accounting lan-access radius-scheme radius1

[AC-isp-dom1] quit

#RADIUSセッション制御機能をイネーブルにします。

[AC] radius session-control enable

#RADIUS DAS機能を有効にして、RADIUS DASビューを入力します。

[AC] radius dynamic-author server

#RADIUSサーバをDACとして10.1.1.3に指定し、RADIUSサーバからのDAEパケットを検証するための共有キーをプレーンテキストで12345に設定します。

[AC-radius-da-server] client ip 10.1.1.3 key simple 12345

[AC-radius-da-server] quit

3. 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] dot1x authentication-method eap

4. ワイヤレスサービスを設定します。

#service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 service

#サービステンプレートのSSIDをserviceとして設定します。

[AC-wlan-st-service] 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-service] vlan 200

#AKMモードを802.1Xに設定します。

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

#暗号スイートをCCMPに設定します。

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

#認証モードを802.1Xに設定します。

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

#802.1Xクライアントを認証するためのISPドメインdom1を指定します。

[AC-wlan-st-service] dot1x domain dom1

#サービステンプレートを有効にします。

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

[AC-wlan-st-service] quit

5. 手動APを設定します。

#office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 office model WA560-WW

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

#radio1のビューを入力します。

[AC-wlan-ap-office] radio 1

#service template serviceをradio1にバインドし、radio1をイネーブルにします。

[AC-wlan-ap-office-radio-1] service-template service

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

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

[AC-wlan-ap-office] 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、トランクポートをVLAN100および200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(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、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

#VLAN-interface100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 100

[Switch-Vlan-interface100] ip address 10.1.1.47 24

[Switch-Vlan-interface100] 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 10.1.2.2 24

[Switch-Vlan-interface200] quit

#APにIPアドレスを割り当てるようにDHCPプール100を設定します。

[Switch] dhcp server ip-pool 100

[Switch-dhcp-pool-100] network 10.1.1.0 mask 255.255.255.0

[Switch-dhcp-pool-100] gateway-list 10.1.1.46

[Switch-dhcp-pool-100] quit

#クライアントにIPアドレスを割り当てるようにDHCPプール200を構成します。

[Switch] dhcp server ip-pool 200

[Switch-dhcp-pool-200] network 10.1.2.0 mask 255.255.255.0

[Switch-dhcp-pool-200] gateway-list 10.1.2.1

[Switch-dhcp-pool-200] quit

#DHCPを有効にします。

[Switch] dhcp enable

WLANクライアントの設定

クライアントにEAP-PEAP証明書がインストールされていることを確認します。

ワイヤレスNICの設定、ワイヤレスネットワークサービスの作成、およびワイヤレスネットワークのプロパティの設定を行います(詳細は省略)。

設定の確認

1. クライアントで、クライアントが認証をパスし、APとアソシエートし、ワイヤレスネットワークにアクセスできることを確認します(詳細は表示されません)。
2. ACで次のタスクを実行して、ユーザが認証にパスし、オンラインになったことを確認します。

   #詳細なWLANクライアント情報を表示します。

   [AC]display wlan client verbose

   Numbers of client:1
   MAC address: cc3a-61a8-fb8c
   IPv4 address: 10.1.2.3
   IPv6 address: N/A
   Username: dot1x

   AID: 1
   AP ID: 3
   AP name: office
   Radio ID: 1
   SSID: service
   BSSID: 741f-4ad4-1fe0
   VLAN ID: 200

   Sleep count: 0
   Wireless mode: 802.11ac
   Channel bandwidth: 80MHz
   SM power save: Disabled
   Short GI for 20MHz: Supported
   Short GI for 40MHz: Supported
   Short GI for 80MHz: Supported
   Short GI for 160/80+80MHz: Not supported
   STBC RX capability: Not supported
   STBC TX capability: Not supported
   LDPC RX capability: Not supported
   SU beamformee capability: Not supported
   MU beamformee capability: Not supported
   Beamformee STS capability: N/A
   Block Ack: N/A
   Supported VHT-MCS set: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
   Supported HT MCS set: 0, 1, 2, 3, 4, 5, 6, 7
   Supported rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
   QoS mode: WMM
   Listen interval: 10
   RSSI: 0

Rx/Tx rate: 0/0
Authentication method: Open system
Security mode: RSN
AKM mode: 802.1X
Cipher suite: CCMP
User authentication mode: 802.1X

Authorization ACL ID: N/A
Authorization user profile: N/A
Roam status: N/A
Key derivation: SHA1
PMF status: N/A
Forwarding policy name: N/A
Online time: 0days 0hours 0minutes 15seconds
FT status: Inactive

#オンラインの802.1Xクライアント情報を表示します。
[AC] display dot1x connection Total
connections: 1

User MAC address: cc3a-61a8-fb8c
AP name: office
Radio ID: 1
SSID: service
Username: dot1x
BSSID: 741f-4ad4-1fe0
Authentication domain: dom1 IPv4 address
: 10.1.2.3
Authentication method
: EAP Initial
VLAN
: 200
Authorization VLAN
: 200
Authorization ACL number
: N/A
Authorization user profile
: N/A
Termination action
: Default
Session timeout period: 36000001 s
Online from: 2015/12/21 11:27:11
Online duration: 0h 1m 1s

設定ファイル

- AC:

```
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain dom1
 service-template enable
#
interface Vlan-interface100
 ip address 10.1.1.46 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
radius scheme radius1
 primary authentication 10.1.1.3
 primary accounting 10.1.1.3
 key authentication cipher $c$3$Bb61SHV2ZsVYPJU2+RFB/8ntk0uCQkmxdA==
 key accounting cipher $c$3$w03NfxnBmfDuedv9/xo7ESnoxKjowmmX9A==
 nas-ip 10.1.2.1
#
radius dynamic-author server
 client ip 10.1.1.3 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
radius session-control enable
#
domain dom1
```

```
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap office model WA560-WW
 serial-id 219801A1NM8182032235
 radio 1
 radio enable
 service-template service
#
```

- PoEスイッチ:

```
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 network 10.1.1.0 mask 255.255.255.0
 gateway-list 10.1.1.46
#
dhcp server ip-pool 200
 network 10.1.2.0 mask 255.255.255.0
 gateway-list 10.1.2.1
#
interface Vlan-interface100
 ip address 10.1.1.47 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port access vlan 100
 poe enable
```

関連ドキュメント

- *Security Command Reference* in *H3C Access Controllers Command References*
- *Security Configuration Guide in H3C Access Controllers Configuration Guides*
- *WLAN Command Reference in H3C Access Controllers Command References*
- *WLAN Configuration Guide in H3C Access Controllers Configuration Guides*