H3Cアクセスコントローラ
LDAPサーバーを介したComware7
ローカル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、認証のために無線ユーザー情報をLDAPサーバーに送信するように、AC上のローカルポータルサービスを設定する例を示します。

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。実際のネットワーク環境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。

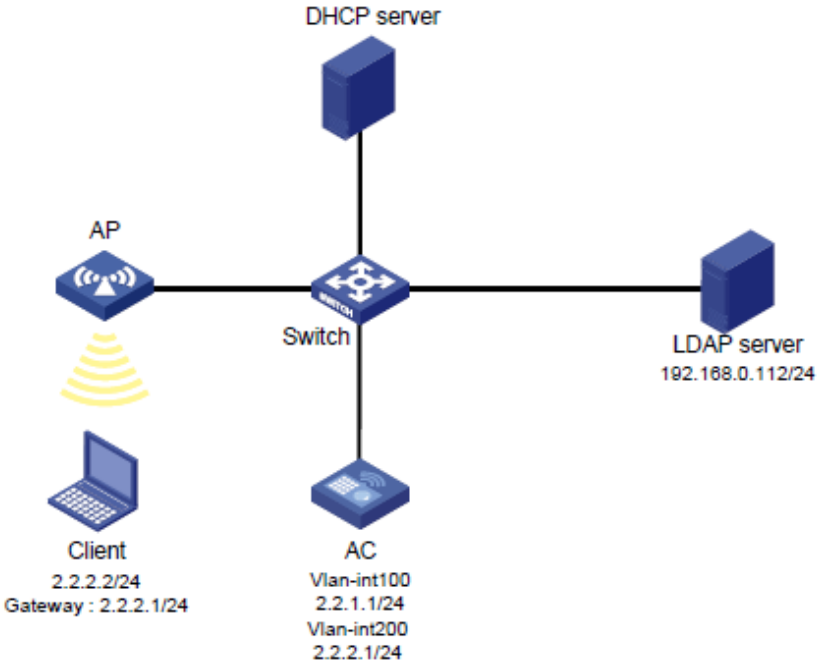
例:LDAPサーバーを介したローカルポータル認証の設定

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。構成要件は次のとおりです。

- クライアントに認証ページを提供するように、ACのローカルポータルサービスを設定します。
- LDAPサーバーを使用してクライアントを認証します。

図1:ネットワーク図



制限事項およびガイドライン

LDAPサーバーを使用してローカル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。

- デバイスが相互に到達できるようにルーティングを設定します。
- 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。
- 認証ページを編集し、.zipファイルに圧縮し(この例ではabc.zipを使用)、ACの記憶媒体のルートディレクトリにファイルをアップロードします。ACでは、このファイルをデフォルトの認証ページファイルとして指定する必要があります。
- デフォルトの認証ページファイルを変更するには、最初にundoを実行する必要があります。default-logon-pageコマンドを使用して、新しいデフォルト認証ページファイルを指定します。

手順

ACの設定

1. VLANおよびインターフェイスの設定:

   #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。このVLANはワイヤレス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 2.2.2.1 24
[AC-Vlan-interface200] quit
#GigabitEthernet1/0/1(スイッチに接続されているポート)をトランクポートとして
設定します。ポートをVLAN100およびVLAN200に設定します。
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit

2. LDAPスキームを構成します。
#ldapという名前のLDAPサーバーを作成し、そのビューに入ります。
[AC] ldap server ldap
#管理者のDNを指定します。
[AC-ldap-server-ldap] login-dn cn=administrator,cn=users,dc=ldap,dc=com
#ユーザー検索のベースDNを指定します。
[AC-ldap-server-ldap] search-base-dn dc=ldap,dc=com
#LDAPサーバーのIPアドレスを指定します。
[AC-ldap-server-ldap] ip 192.168.0.112
#管理者パスワードを指定します。
[AC-ldap-server-ldap] login-password simple 123456
[AC-ldap-server-ldap] quit
#ldapという名前のLDAPスキームを作成し、そのビューを入力します。
[AC] ldap scheme ldap
#ldapをLDAP認証サーバーとして指定します。
[AC-ldap-ldap] authentication-server ldap
[AC-ldap-ldap] quit
#ldap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 ldap
#ISPドメインldap内のポータルユーザーに対して、認証方式をLDAPとして設定し、
認証およびアカウンティング方式をnoneとして設定します。
[AC-isp-ldap] authentication portal ldap-scheme ldap
[AC-isp-ldap] authorization portal none
[AC-isp-ldap] accounting portal none
#ISPドメインldapのユーザーに対してidle-cut機能を構成します。ユーザーの
トラフィックが15分間で1024バイト未満の場合は、ユーザーをログアウトします。
[AC-isp-ldap] authorization-attribute idle-cut 15 1024
[AC-isp-ldap] quit

3. ポータル認証を構成します。
#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を
次のように指定します。
[AC] portal web-server newpt
[AC-portal-websvr-newpt] url http://2.2.2.1/portal
[AC-portal-websvr-newpt] quit
#ローカルポータルサービスを有効にして、HTTPベースのローカルポータルWeb
サービスビューを開始します。

[AC] portal local-web-server http
#デフォルトの認証ページファイルをabc.zipとして指定します(このファイルは、
ACの記憶媒体のルートディレクトリにすでに存在している必要があります)。
[AC–portal-local-websvr-http] default-logon-page abc.zip
[AC–portal-local-websvr-http] quit

4. # 宛先ベースのポータルフリー規則1および2を設定して、ポータルユーザーが認証無しにDNSにアクセスできるようにします。
[AC] portal free-rule 1 destination ip any udp 53
[AC] portal free-rule 2 destination ip any tcp 53
5. ワイヤレスサービスを次のように設定します。
st1という名前のサービステンプレートを作成し、そのビューを入力します。
[AC] wlan service-template st1
#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-st1] 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-st1] vlan 200
#ポータルの直接認証を有効にします。
[AC-wlan-st-st1] portal enable method direct
#ポータル認証ドメインをldapとして構成します。
[AC-wlan-st-st1] portal domain ldap
#サービステンプレートでポータルWebサーバーnewptを指定します。
[AC-wlan-st-st1] portal apply web-server newpt
#サービステンプレートを有効にします。
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit
#officeapという名前のアクセスポイントを作成します。アクセスポイントのモデルと
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のビューに入ります。
[AC-wlan-ap-officeap] radio 2
サービステンプレートst1をradio2にバインドします。
[AC-wlan-ap-officeap-radio-2] service-template st1
[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、ワイヤレスクライアント
のトラフィックを転送します。
[Switch] vlan 200
[Switch-vlan200] 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ま。
トランクポートをVLAN100およびVLAN200に割り当てます。
[Switch] interface gigabitethernet1/0/1

[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ます。
#アクセスポートをVLAN100に割り当てます。
[Switch] interface gigabitethernet1/0/2
[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 を有効にする。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit

client forwarding-location apの場合の注意点

デフォルトでは、デバイスはARPエントリのみに従ってワイヤレスポータルクライアントの有効性をチェックします。APがクライアントトラフィックを転送するワイヤレスネットワークでは、ACにはクライアントのARPエントリがありません。したがって、ACはARPエントリを使用してポータルクライアントの有効性を確認できません。有効なユーザーがポータル認証を実行できるようにするには、ACでワイヤレスクライアントの有効性チェックを有効にする必要があります。
この機能により、ACは、WLANスヌーピングテーブル、DHCPスヌーピングテーブル、およびARPテーブルでクライアント情報を検索することにより、クライアントを検証できます。クライアント情報が存在する場合、ACはクライアントがポータル認証に有効であると判断します。この機能を有効にするには以下のコマンドを入力します。

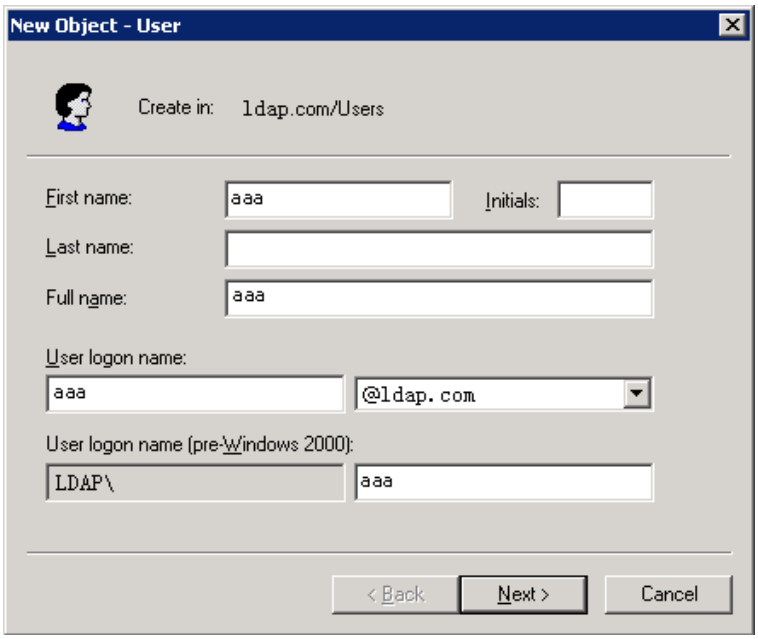
コマンド:
[AC] **portal host-check enable**

LDAPサーバーの設定

この例では、Microsoft Windows2003Server Active Directoryを使用して、LDAPサーバー上の構成を示します。

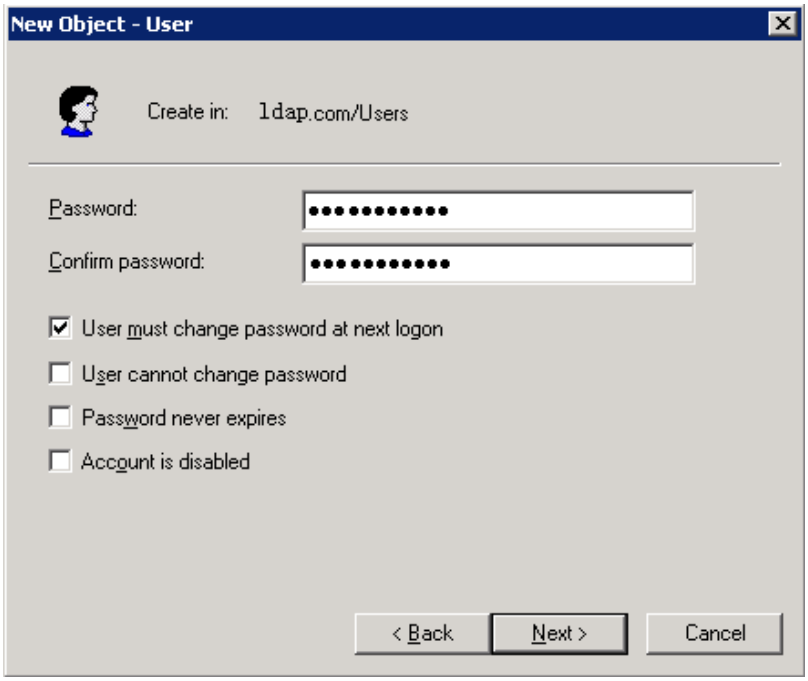
1. aaaという名前のユーザーを追加します。
   a. LDAPサーバーで、Start > Control Panel > Administrative Toolsの順に選択します。
   b. Active Directory Users and Computersをダブルクリックします。
      Active Directory Users and Computersウィンドウが開きます。
   c. ナビゲーションツリーで、ldap.comノードの下のUserをクリックします。
   d. メニューからStart > Control Panel > Administrative Toolを選択して、ユーザーを追加するためのダイアログボックスを開きます。
   e. ログオン名としてaaaと入力し、Nextをクリックします。

図2 ユーザーaaaの追加



f. ダイアログボックスで、passwordに123456と入力し、必要に応じてオプションを選択して、Nextをクリックします。

図3 ユーザーのパスワードの設定



g. OKをクリックします。

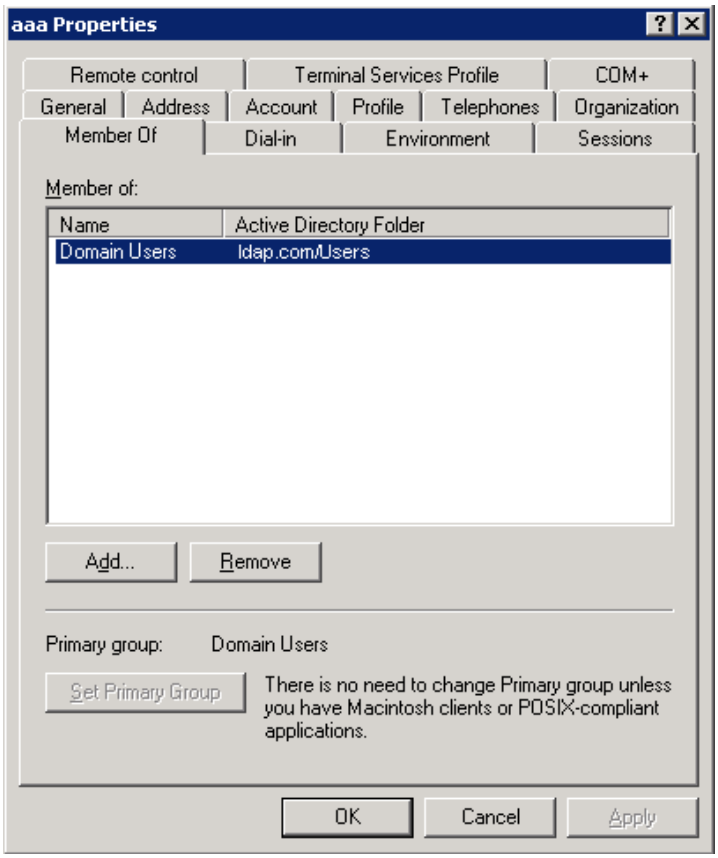
2. ユーザーaaaをユーザーグループUsersに追加します。

a. ナビゲーションツリーで、ldap.comノードの下のUsersをクリックします。

b. 右ペインで、ユーザーaaaを右クリックし、Propertiesを選択します。

c. ダイアログボックスで、memberタブをクリックし、Addをクリックします。

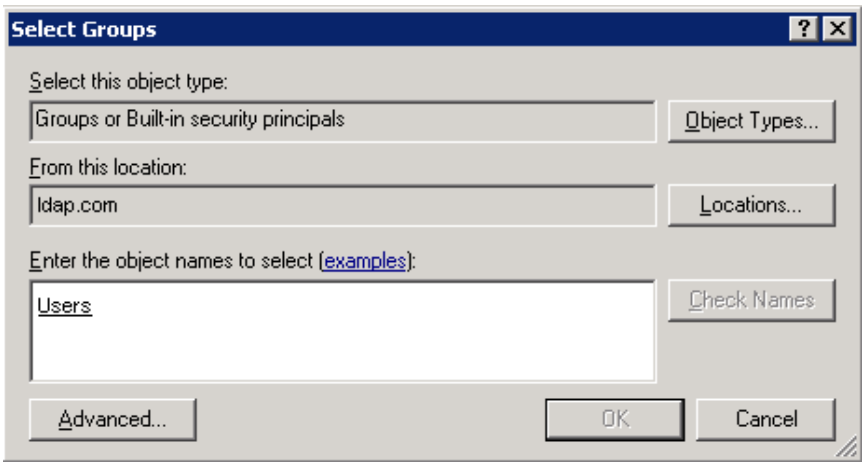
図4 ユーザープロパティの変更



d. Select Groupsダイアログボックスで、Users in the Enter the object namesフィールドにUsersと入力しOKをクリックします。

ユーザーaaaがグループUsersに追加されます。

図5 Usersグループへのユーザーaaaの追加



3. 管理者パスワードを設定します。

a. 右側のペインで、ユーザーAdministratorを右クリックし、Set Passswordを選択します。

b. ダイアログボックスで、管理者パスワードを入力します(詳細は省略します)。

設定の確認

#ワイヤレスクライアントでIEなどのWebブラウザを開きます。アドレスバーにIPアドレスを
#入力し、Enterキーを押します。ポータル認証ページが開きます。ユーザー名aaaと
パスワード123456を入力し、Logonをクリックします。ユーザーaaaは認証に成功しました。
#オンラインポータルユーザーをACに表示します。
<AC> display portal user all Total portal users: 1 Username: aa
AP name: officeap Radio ID: 2 SSID: service
Portal server: newpt State: Online
VPN instance: N/A

MAC	IP	VLAN	Interface
2477-0341-f118	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: 3777

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 ldap
 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
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
ldap server ldap
```

```
 login-dn cn=administrator,cn=users,dc=ldap,dc=com
 search-base-dn dc=ldap,dc=com
 ip 192.168.0.112
 login-password cipher
 $c$3$CEz2vKCnA2/51D8rFc/+nTNtOx8Gan+81Q==
#
ldap scheme ldap
 authentication-server ldap
#
domain ldap
 authorization-attribute idle-cut 15 1024
 authentication portal ldap-scheme ldap
 authorization portal none
 accounting portal none
#
portal web-server newpt
 url http://2.2.2.1/portal
#
portal local-web-server http
 default-logon-page abc.zip
#
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
wlan ap officeap model WA560-WW
 serial-id 219801A1NM8182032235
 radio 2
  radio enable
  service-template st1
#
```

- Switch:

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

関連文書

- *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*

付録. 標準のログイン画面用設定ファイル (flash:/defaultfile.zip)

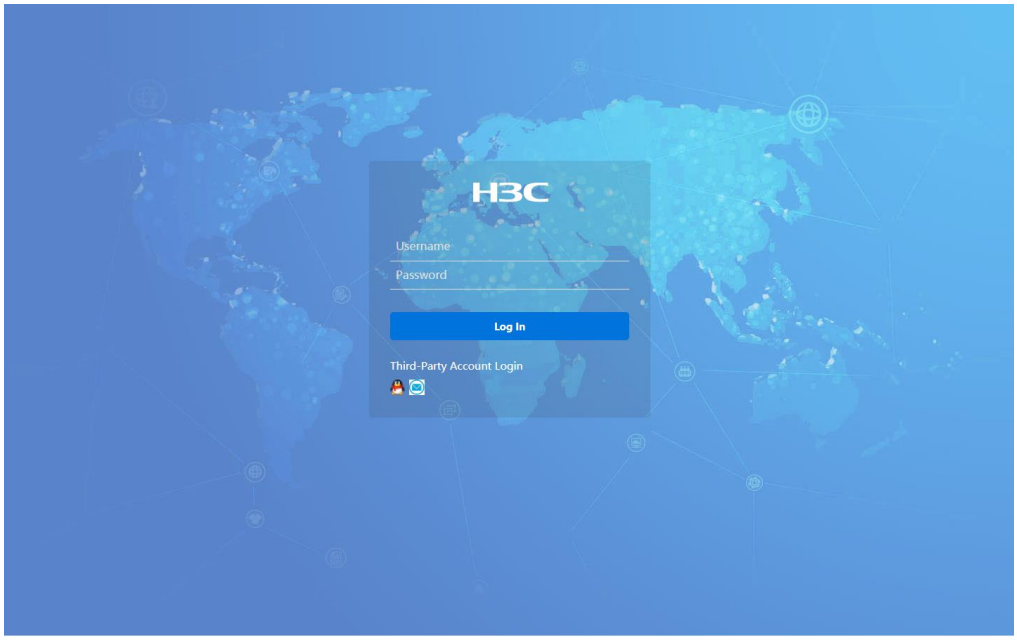
WX1840HのFlashフォルダーのファイル例（ここにdefaultfile.zipがデフォルトで入っております）

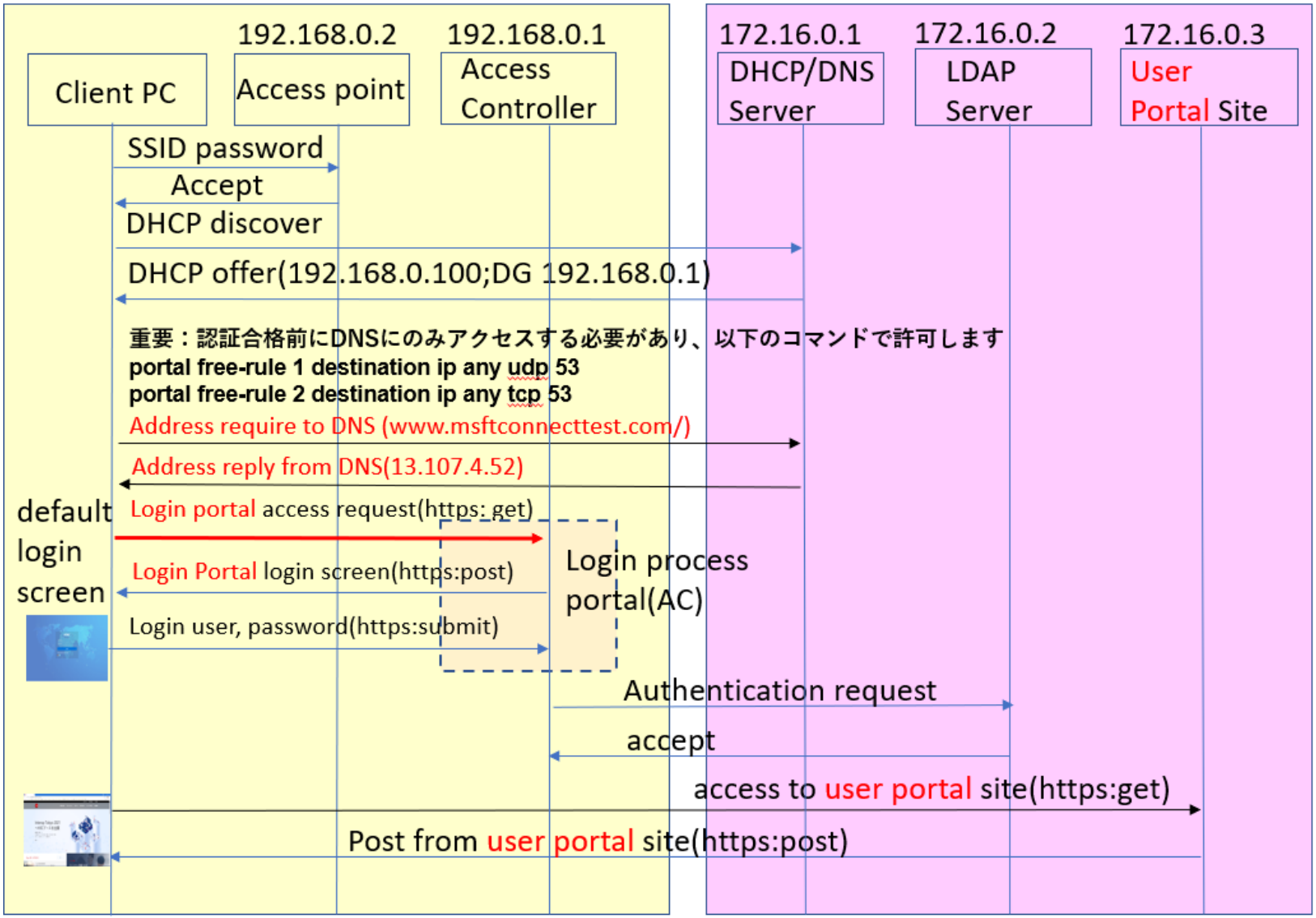
```
<WX1840H>dir
Directory of flash:
   0 -rw-   148520960 Jun 04 2021 21:53:10   WX1840H-CMW710-
R5441P02.ipe
   1 drw-           - Jul 07 2021 16:19:41   apimge
   2 -rw-     6417408 Jul 07 2021 16:13:55   boot.bin
   3 drw-           - Jul 04 2020 01:01:19   command
   4 drw-           - Mar 28 2021 14:18:05   core
   5 -rw-      261508 Jul 07 2021 20:55:48   defaultfile.zip
   6 drw-           - Nov 05 2019 22:01:41   diagfile
   7 -rw-      262878 Jul 07 2021 20:55:48   facebook.zip
   8 -rw-     1463296 Apr 08 2021 23:45:29   freeradius.bin
   9 -rw-         735 Jul 04 2020 00:54:13   hostkey
  10 -rw-         349 Jul 07 2021 20:54:54   ifindex.dat
  11 -rw-      259026 Jul 07 2021 20:55:48   ise.zip
  12 drw-           - Jan 27 2020 18:25:01   license
  13 drw-           - Jan 27 2020 18:20:33   logfile
  14 -rw-         913 Mar 18 2021 12:12:25   map_config.cfg
  15 drw-           - Aug 05 2021 20:59:12   pdt_reserve
  16 drw-           - Nov 05 2019 22:03:09   pki
  17 drw-           - Nov 05 2019 22:01:41   seclog
  18 -rw-         591 Jul 04 2020 00:54:13   serverkey
  19 -rw-        7598 Apr 09 2021 00:49:16   startup.cfg
  20 -rw-      196346 Apr 09 2021 00:49:16   startup.mdb
  21 -rw-    90874880 Jul 07 2021 16:16:25   system.bin
  22 -rw-           0 Dec 18 2020 21:43:24   topology.dba
  23 -rw-    60545024 Jul 07 2021 20:47:27   wa6600.ipe

1048576 KB total (649108 KB free)

<WX1840H>
```

defaultfile.zipを解凍したもの

- logo-white-small.png
- logo-red-small.png
- logonFail.htm
- logon.htm
- Busy.htm
- background-logon.jpg
- logonFail.js
- js
- online.htm
- logonSuccess.htm
- logoffSuccess.htm
- emailLogon.htm
- logonSuccess.js
- favicon.ico
- common.css
- mail.png
- Connect_logo_1.png

デフォルトのログイン画面




192.168.0.2
192.168.0.1
172.16.0.1
172.16.0.2
172.16.0.3
Client PC
Access point
Access Controller
DHCP/DNS Server
LDAP Server
User Portal Site
SSID password
Accept
DHCP discover
DHCP offer(192.168.0.100;DG 192.168.0.1)
重要：認証合格前にDNSにのみアクセスする必要があり、以下のコマンドで許可します
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
Address require to DNS (www.msftconnecttest.com/)
Address reply from DNS(13.107.4.52)
default login screen
Login portal access request(https: get)
Login Portal login screen(https:post)
Login user, password(https:submit)
Login process portal(AC)
Authentication request
accept
access to user portal site(https:get)
Post from user portal site(https:post)