ダイナミック認証VLAN

FreeRADIUSを用いて、ダイナミック認証VLANの実現するための設定例です。ダイナミック認証VLANとは、同一ESSID (eduroam) で接続した際に、認証されたユーザごとに異なる定められたVLANに接続する方法のことです。この機能を利用すると、たとえば、教員用ネットワーク、学生用ネットワーク、ビジター用ネットワークの3つを用意しておき、ネットワークに接続するユーザの属性に応じて接続先のネットワークを切り替えることができます。

1) ダイナミックVLAN設定に必要なRADIUSのパラメータ

Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-Id の3つを設定し、アクセスポイントに渡す必要がある。

たとえば以下のような値を渡すことで、認証後に利用者のネットワークが VLAN 100 に接続される。

```
Tunnel-Type = 13
Tunnel-Medium-Type = 6
Tunnel-Private-Group-Id = 100 (VLAN番号)
```

数値を指定する代わりに、数値に対応して定義された文字列をしていることも可能（アクセスポイント側の仕様を確認のこと）。

```
Tunnel-Type = VLAN
Tunnel-Medium-Type = IEEE-802
Tunnel-Private-Group-Id = VLAN100
```

2) テストアカウントの設定

FreeRADIUS であれば、たとえば、raddb/users ファイルに以下のようにユーザを定義することで、テスト用のアカウントとパラメータを定義することができる。

```
test    Cleartext-Password := "Password", Realm == "example.jp"
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id = 100
```

3) パラメータの中継

FreeRADIUSをプロキシサーバとして利用する場合、ダイナミックVLANに関連するパラメータは、デフォルトで「中継」しない設定になっている。もしプロキシサーバにおいてパラメータの中継が必要な場合（組織内でプロキシサーバを多段で運用している等）は、設定の変更が必要である。
（一般的な環境では、このような「中継」の設定は不要。）

raddb/mods-config/attr_filter/post-proxy ファイルの最後にある DEFAULT の定義の中に以下の行を追加する。（継続の "," を忘れずに）

```
DEFAULT
        (略)
        Tunnel-Type =* ANY,
        Tunnel-Medium-Type =* ANY,
        Tunnel-Private-Group-Id =* ANY,
        (略)
```

4) 特定のレルムに対するダイナミックVLANパラメータの追加

通常は、ローカルの認証サーバと連携する際に、ユーザ毎に事前に定義される、利用させたいVLANが受け渡されるように設定を行う。

別の方法として、認証時に、特定のレルムに対してダイナミックVLANを設定したいような場合は、mods-config/attr_filter/post-proxy ファイルに以下のようなレルムの設定を追加する。

```
example.ac.jp
        Tunnel-Type := 13,
        Tunnel-Medium-Type := 6,
        Tunnel-Private-Group-Id := 200, (指定したいVLAN番号)
        Fall-Through = Yes
```

最後の Fall-Through = Yes により、DEFAULT の処理に続ける。（最終行以外は、継続行があることを示す「,」を行末につけることを忘れずに。）

この方法を用いて、教職員と学生を別のVLANに接続したい場合は、教職員と学生とで異なるレルムを利用する。

DEFAULT では、Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-Id の定義は行わない（従って、それ以外のレルムに対してはVLAN番号は設定されない）。

なお、VLAN番号の指定がない場合に、どのVLANに接続するかは、アクセスポイントに設定する。

5) それ以外のレルムに対するダイナミックVLANパラメータの追加

前項 4) に加えて、それ以外のレルムに対してVLAN番号を設定したい場合には、mods-config/attr_filter/post-proxy ファイルにおいて以下のように設定する。

```
example.ac.jp
   ここに元のDEFAULTの内容全部をコピーし、最終行を継続行（","をつける）にする
      Tunnel-Type := 13,
      Tunnel-Medium-Type := 6,
      Tunnel-Private-Group-Id := 200 (指定したいVLAN番号)
（最後の Fall-Through = Yes はここでは不要）

DEFAULT
   (略) 最終行を継続行（","をつける）にして以下を追加する
      Tunnel-Type := 13,
      Tunnel-Medium-Type := 6,
      Tunnel-Private-Group-Id := 300 (指定したいVLAN番号)
```

6) 動作確認

設定内容が意図通りに反映されているかどうかは、実際にアクセスポイントを利用して確認する以外にも、eopol_test などのツールを用いて確認することもできる。

設定ファイルの例

```
network={
    ssid="eduroam"
    eapol_flags=255
    key_mgmt=WPA-EAP
    eap=PEAP
    identity=test@example.jp
    password="Password"
    phase2="autheap=GTC"
}
```

コマンドの実行例

```
eapol_test -c 設定ファイル名 -a RADIUSサーバのアドレス -s RADIUSサーバへのアクセスパスワード
```

アクセスパスワードは、アクセス元のIPアドレス等とともに、FreeRADIUSのclients.confに定義されるものです。