คู่มือการติดตั้ง Radius server สำหรับบริการ eduroam
สำหรับการเปนผูใหบริการหลัก (Main Realm) ของสถาบัน

บทนำ

ขั้นตอนการติดตั้ง จะประกอบดวย ๓ ขั้นตอนหลัก กับ ๒ ทางเลือก ประกอบดวย

1. การติดตั้งและทดสอบพื้นฐาน
   สามารถทำให Radius server ทำงานไดดวยตัวเอง ใชบัญชีผูใชที่มีอยูในไฟลของโปรแกรม
2. การติดตั้งใชงานรวมกับ eduroam-TH
3. การเชื่อมตอกับเครื่องใหบริการยอย (Sub-Realm) ของสถาบัน
4. การเลือกใชฐานขอมูลบัญชีผูใชจากระบบภายนอก เปนการกำหนดให Radius server ใชบัญชีผูใชจากฐานขอมูลภายนอก ประกอบดวย ๓ ทางเลือก
   - การติดตั้งโดยมี LDAP Server เปนฐานขอมูลบัญชีผูใช
   - การติดตั้งโดยมี Microsoft Active Directory เปนฐานขอมูลบัญชีผูใช
   - การติดตั้งโดยมี MySQL เปนฐานขอมูลบัญชีผูใช

วิธีการติดตั้ง เปนการแนะนำคำสั่งในการดำเนินการอยางเปนลำดับ พรอมตัวอยางคำสั่งที่ตรงกับสภาพแวดลอมของ เครื่องมากที่สุด เชรน การติดตั้งแพคเกจ การแกไขไฟล การทดสอบการทำงาน เปนตน โดยคุณสมบัติของโปรแกรม เกือบทั้งหมด เปนการนำไฟลสำเร็จรูปที่ผานการปรับรูปแบบเพื่อไมใหซ้ำกับไฟลคุณสมบัติเดิมของโปรแกรม นำมาติดตั้ง ดำเนินการแกไขเนื้อหาในไฟลใหเหมาะสม และใชงาน

เพื่อใหการติดตั้งมีความถูกตองและสามารถทำงานไดอยางไมมีขอผิดพลาด จำเปนตองดำเนินการตามลำดับขั้นโดยละเอียด ยกเวนการเลือกใชฐานขอมูลบัญชีผูใชที่สามารถเลือกไดอยางใดอยางหนึ่ง

หัวขอ การตรวจวิเคราะหและตรวจสอบการทำงานของ Radius server เปนสวนของการแนะนำการปรับแตงคุณสมบัติ เพื่อให Radius server ทำงานที่แตกตางหรือเพิ่มเติมจากการติดตั้งนี้ รวมถึงการตรวจสอบกิจกรรมที่เกิดขึ้นที่บันทึกไวในไฟล Log
หัวขอ การติดตั้ง Wireless Controller หรือ Anonymous Access Point รวมกับ Radius server แนะนำวิธีการกำหนดคุณสมบัติของ Radius server และอุปกรณ WLC หรือ AP ใหทำงานรวมกัน

ลักษณะเดนของการกำหนดคุณสมบัติในการติดตั้งนี้คือ สามารถเปดโอกาสใหสมาชิกภายในองคกรใชบริการเครือขายภายในองคกรได ประโยชนก็เพื่อใหสมาชิกดำเนินการกำหนดคุณสมบัติการเชื่อมตอจากเครือขายภายในใหสำเร็จกอน แกปญหาใหเสร็จกอน จากนั้นจึงจะไปใชบริการจากผูใหบริการอื่นได้ทันที

รุนของระบบปฏิบัติการ และโปรแกรม freeradius ที่ใชทดลองติดตั้ง

คำสั่งและไฟลจะอางอิงตามระบบปฏิบัติการและโปรแกรม freeradius จึงควรเลือกใชคำสั่งอยางถูกตอง ดังนี้

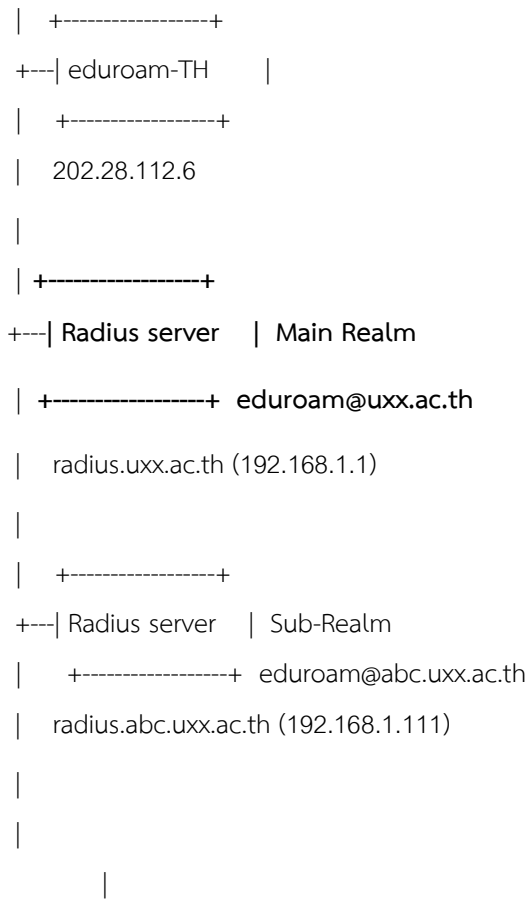
- Debian 9.8 (stretch)

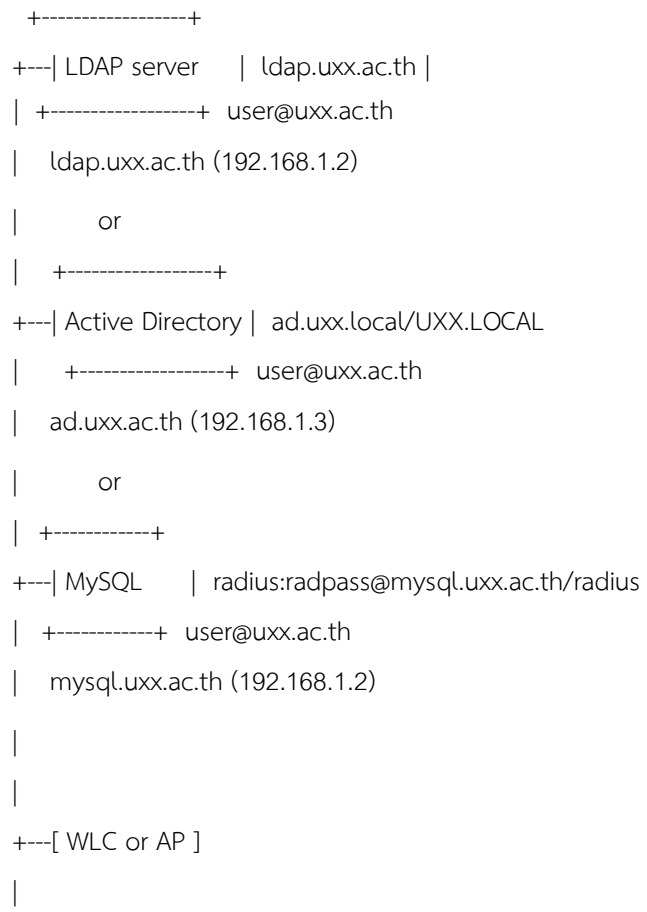
  cat /etc/debian_version

- Freeradius 3.0

  freeradius -v

โครงสรางเครือขายประกอบการติดตั้ง





== Hosts Account/Password ==

Linux: root/asdf

Windows: Administrator/Asdf1234

<u>การติดตั้งและทดสอบขั้นพื้นฐาน</u>

เปนการติดตั้งและกำหนดคุณสมบัติพื้นฐานให Radius server สามารถทำงานไดดวยตัวเอง ประกอบดวยการติดตั้งโปรแกรม ติดตั้งแพคเกจพื้นฐาน ติดตั้งแพคเกจสนับสนุน ติดตั้งโปรแกรมสำหรับทดสอบ แกไขคุณสมบัติพื้นฐาน และทดสอบการทำงาน โดยการทดสอบจะนำข่อมูลผูใชแบบไฟลข่อความที่มีอยูไฟล user-eduroam.conf มาใชงาน

๑. อัพเกรดแพคเกจลาสุดและแพคเกจพื้นฐาน

apt update apt upgrade -y

อาจตองรีบูท

apt install ntp -y

service ntp restart

๒. ติดตั้งแพคเกจ freeradius และแพคเกจสนับสนุน

apt install freeradius -y

apt install easy-rsa -y

apt install wget -y

update-rc.d freeradius enable

๓. ดาวนโหลดและคอมไพลเครื่องมือสำหรับทดสอบ

เปนเครื่องมือหรือโปรแกรมสำหรับใชทดสอบการทำงานไปยัง radius server โดยสามารถทดสอบกับ radius server เกี่ยวกับ WPA-Enterprise ถึงขั้น phase-2 ได

```
apt install gcc make libssl-dev -y

cd /etc/freeradius/3.0

wget \
http://www.rmuti.ac.th/user/prakai/p/2019-05-freeradius-test-t ool.tar.gz

tar vxfz 2019-05-freeradius-test-tool.tar.gz

cd tool/wpa_supplicant-2.6/wpa_supplicant

cp -f defconfig .config
  nano .config
        --------
        ...
        CONFIG_EAPOL_TEST=y
```

...

#CONFIG_DRIVER_NL80211=y

...

make eapol_test cp eapol_test ../../bin

ref: http://deployingradius.com/scripts/eapol_test

๔. ดาวนโหลดชุดไฟลคุณสมบัติสำเร็จรูป

เปนไฟลคุณสมบัติสำเร็จรูปจะไดรับการปรับแตงคาตัวแปรบางสวนไวแลว

cd /etc/freeradius/3.0

wget \

http://www.rmuti.ac.th/user/prakai/p/2019-05-freeradius-๓-debi an-eduroam.tar.gz

๕. แตกไฟลคุณสมบัติสำเร็จรูป

แตกไฟลคุณสมบัติสำเร็จรูป โดยไฟลคุณสมบัติสำเร็จรูปมีหลายไฟล ไดรับการปรับแตงคาตัวแปรบางสวนไวแลว รวมถึงไดตัดคำอธิบาย (comment) ออกไป เพื่อใหเนื้อหาในไฟลมีความกระชับขึ้น

tar vxfz 2019-05-freeradius-๓-debian-eduroam.tar.gz

รายการไฟลคุณสมบัติสำเร็จรูปมีดังนี้

- คุณสมบัติหลักของ freeradius 3.0 ใชดูเพื่อเทียบสำหรับแกไขไฟลปจจุบัน radiusd-eduroam.conf
- การคัดกรองบัญชีผูใชหรือ realm ที่ไมถูกตอง
  eduroam-realm-checks.conf eduroam-mon-checks.conf
- ประกาศไซตหรือการบริการของ freeradius สำหรับ eduroam แบบ Main realm หรือ Sub-realm
  sites-available/eduroam-main
  sites-available/eduroam-sub
  sites-available/eduroam-inner-tunnel
  sites-available/eduroam-status
- การเชื่อมตอกับ radius เครื่องอื่น เชน NRO, Main realm หรือ Sub-realm
  proxy-eduroam-main.conf
  proxy-eduroam-sub.conf

clients-eduroam-main.conf
clients-eduroam-sub.conf

- คุณสมบัติโมดูล EAP และ attr_filter
  mods-available/eap-eduroam
  mods-config/attr_filter/pre-proxy
- บัญชีผู้ใชแบบไฟล
  mods-available/files-eduroam
  mods-config/files-eduroam/accounting
  mods-config/files-eduroam/pre-proxy
  mods-config/files-eduroam/authorize
- บัญชีผู้ใชจาก LDAP server
  mods-available/ldap-eduroam
- บัญชีผู้ใชจาก Microsoft Active Directory
  mods-available/mschap-eduroam
- บัญชีผู้ใชจาก MySQL server
  mods-available/sql-eduroam
  mods-config/sql/main/mysql/queries-eduroam.conf

๖. แกไขไฟล radiusd.conf

โดยปรับแกเฉพาะจุดโดยเทียบจากไฟล radiusd-eduroam.conf

cd /etc/freeradius/3.0

nano radiusd.conf

```
--------
# Change some configurations in radiusd.conf as show below

# PROXY CONFIGURATION
#
proxy_requests  = yes
$INCLUDE proxy.conf
#  eduroam
$INCLUDE proxy-eduroam.conf
```

```
...

# CLIENTS CONFIGURATION
#
$INCLUDE clients.conf
#  eduroam
$INCLUDE clients-eduroam.conf
```

๗. สำเนาไฟลสำหรับการเปนผูใหบริการหลัก (Main Realm) ของสถาบัน

เลือกใชไฟลสำหรับ Main Realm

```
cd /etc/freeradius/3.0

cp proxy-eduroam-main.conf  proxy-eduroam.conf
cp clients-eduroam-main.conf  clients-eduroam.conf
cp sites-available/eduroam-main  sites-available/eduroam
```

๘. แกไขไฟล proxy-eduroam.conf

ปรับแกในไฟลเฉพาะจุดที่ต่องแกไข

```
cd /etc/freeradius/3.0

nano proxy-eduroam.conf
        --------
        #
        #  realm for local service
        #
        realm uxx.ac.th {
                auth_pool = localhost
                nostrip
        }
        realm ~.uxx.ac.th {
                virtual_server = auth-reject
                nostrip
        }
```

๙. แก้ไขไฟล sites- available/eduroam

ปรับแก้ในไฟลเฉพาะจุดที่ต่องแก้ไข

```
cd /etc/freeradius/3.0

nano sites-available/eduroam
        --------
        authorize {

        # Change realm to be LOCAL for local user
        if( ("%{Realm}" =~ /uxx.ac.th$$/) ) {
            if( ("%{Realm}" =~ /^uxx.ac.th$$/) ) {
                    update control {
                            Proxy-To-Realm := LOCAL
                        }
                }
               ...
        }
         ...
        pre-proxy {

         # Update Operator-Name to IdP
        if ("%{Operator-Name}" == "") {
                    update proxy-request {
                            Operator-Name := "1uxx.ac.th"
                                }
                }
               ...
        }
```

๑๐. ยกเลิกไซตเดิม และเปดใชไซตใหม

```
cd /etc/freeradius/3.0/sites-enabled

rm -f default
rm -f inner-tunnel
```

```
ln -s ../sites-available/eduroam
ln -s ../sites-available/eduroam-inner-tunnel
ln -s ../sites-available/eduroam-status
cd ..
```

๑๑. เปดใชโมดูล eap-eduroam และ files-eduroam

```
cd /etc/freeradius/3.0/mods-enabled

ln -s ../mods-available/eap-eduroam
ln -s ../mods-available/files-eduroam
cd ..
```

๑๒. สรางไฟล Certificates

ปรับแกในไฟลเฉพาะจุดที่ต่องแกไข

```
cd /etc/freeradius/3.0/certs
 rm *
cp /usr/share/doc/freeradius/examples/certs/* .
  nano ca.cnf
        --------
        [ CA_default ] :
             default_days                    = 3650

        :

  [certificate_authority]
 countryName = TH
 stateOrProvinceName = Bangkok
 localityName = -
```

organizationName = XX University

emailAddress = eduroam@uxx.ac.th

commonName = "UXX Wi-Fi Certificate Authority"

nano server.cnf

```
--------
[ CA_default ]
:
default_days                    = 3650
:

[server]
countryName                     = TH
stateOrProvinceName             = Bangkok
localityName                    = -
organizationName                = XX University
emailAddress                    = eduroam@uxx.ac.th
commonName                      = "UXX Wi-Fi Certificate"
```

nano client.cnf

```
--------
[ CA_default ]
:
default_days                    = 3650
:

[client]
countryName                     = TH
stateOrProvinceName             = Bangkok
localityName                    = -
```

organizationName = XX University
emailAddress = eduroam@uxx.ac.th
commonName = eduroam@uxx.ac.th

nano Makefile --------

```
dh:
	openssl dhparam -dsaparam -out dh $(DH_KEY_SIZE)
```

./bootstrap
cd ..

๑๓. เปลี่ยนสิทธิ์หรือเจาของของไฟล

chown -R freerad:freerad /etc/freeradius/3.0

๑๔. ทดสอบการทำงานแบบพื้นฐาน

บัญชีผูใชสำหรับการทดสอบอยูในไฟล

mods-config/files-eduroam/authorize

หนาจอที่ ๑

service freeradius stop
freeradius -X
(stop debugging with CTRL+C)

หนาจอที่ ๒

cd /etc/freeradius/๓.๐/tool

```
./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
                -u  'eduroam@uxx.ac.th' \
                -p 'TESTING-PASSWORD' \
                -v  -m IEEE8021X \
```

-s eduroam -e PEAP -2 MSCHAPV2

-------- access-accept; 0

RADIUS message: code=2 (Access-Accept) identifier=8

length=187

Attribute 27 (Session-Timeout) length=6

Value: 600

Attribute 1 (User-Name) length=21

Value: 'eduroam@uxx.ac.th'

Attribute 79 (EAP-Message) length=6

Value: 03080004

Attribute 80 (Message-Authenticator) length=18

Value: 6668fe5c30e59946dc91ad7200c0a810

การติดตั้งใชงานรวมกับ eduroam-TH

๑๕. แกไขไฟล radiusd.conf

โดยปรับแกเฉพาะจุดโดยเทียบจากไฟล radiusd-eduroam.conf

```
cd /etc/freeradius/3.0

nano radiusd.conf
        --------
        # Change some configurations in radiusd.conf as show below

        # PROXY CONFIGURATION
        #
        proxy_requests  = yes
        $INCLUDE proxy.conf
        #  eduroam
        $INCLUDE proxy-eduroam.conf

        # CLIENTS CONFIGURATION
        #
        $INCLUDE clients.conf
        #  eduroam
        $INCLUDE clients-eduroam.conf
```

๑๖. แกไขไฟล proxy-eduroam.conf

ปรับแกในไฟลเฉพาะจุดที่ต่องแกไข

```
cd /etc/freeradius/3.0

nano proxy-eduroam.conf
        --------
        #
        #  realm for local service
        #
        realm uxx.ac.th {
              auth_pool = localhost
              nostrip
```

```
}
home_server eduroam-NRO-a {
        type = auth+acct
        ipaddr = 202.28.112.6
        port = 1812
        secret = XXXXXXXXXXXXXXXX
        #src_ipaddr = xxx.xxx.xxx.xxx
        status_check = status-server
        require_message_authenticator = yes
}
```

๑๗. แก้ไขไฟล clients-eduroam.conf

ปรับแก้ในไฟลเฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano clients-eduroam.conf
        --------
        #
        #  eduroam server (NRO)
        #
        client eduroam-NRO-a {
                ipaddr = 202.28.112.6 #UniNet
                secret = XXXXXXXXXXXXXXXX
                require_message_authenticator = no
                shortname = eduroam-NRO
                #virtual_server = eduroam
        }
```

๑๘. ทดสอบการทำงานดวยผูใช eduroam จาก IdP อื่น

หนาจอที่ ๑

```
service freeradius stop
freeradius -X
```

(stop debugging with CTRL+C)

หนาจอที่ ๒

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
        -u 'eduroam@uni.net.th' \
        -p 'AskToUniNet' \
        -v -m IEEE8021X \
        -s eduroam -e PEAP -2 MSCHAPV2
           -------- access-accept; 0
           RADIUS message: code=๒ (Access-Accept) identifier=๘ length=187
             Attribute ๒๗ (Session-Timeout) length=6
            Value: 600
             Attribute 1 (User-Name) length=21
            Value: 'eduroam@uni.net.th'
             Attribute 79 (EAP-Message) length=6
            Value: 03080004
             Attribute 80 (Message-Authenticator) length=18
            Value: 4f334b7622ec20537163ac31c1926d84
```

การเชื่อมตอกับเครื่องใหบริการยอย (Sub-Realm) ของสถาบัน

๑๙. แกไขไฟล radiusd.conf

โดยปรับแกเฉพาะจุดโดยเทียบจากไฟล radiusd-eduroam.conf

```
cd /etc/freeradius/3.0

nano radiusd.conf
        --------
        # Change some configurations in radiusd.conf as show below

        # PROXY CONFIGURATION
```

```
#
proxy_requests  = yes
$INCLUDE proxy.conf
#  eduroam
$INCLUDE proxy-eduroam.conf

# CLIENTS CONFIGURATION
#
$INCLUDE clients.conf
#  eduroam
$INCLUDE clients-eduroam.conf
```

๒๐. แก้ไขไฟล proxy-eduroam.conf

ปรับแก้ในไฟลเฉพาะจุดที่ต่องแก้ไข

```
cd /etc/freeradius/3.0

nano proxy-eduroam.conf
--------
#
#  home server for ABC.UXX.AC.TH
#
home_server abc-uxx-ac-th {
        type = auth+acct
        ipaddr = xxx.xxx.xxx.xxx # 192.168.1.111
        port = 1812
        secret = XXXXXXXXXXXXXXXX
        #src_ipaddr = xxx.xxx.xxx.xxx
        status_check = status-server
        require_message_authenticator = yes
}
#
#  home server pool for ABC.UXX.AC.TH
#
home_server_pool abc-uxx-ac-th-pool {
```

```
        type = fail-over
        home_server = abc-uxx-ac-th
    }
    #
    #  realm for ABC.UXX.AC.TH
    #
    realm abc.uxx.ac.th {
        auth_pool = abc-uxx-ac-th-pool
        nostrip
    }
```

๒๑. แก้ไขไฟล clients-eduroam.conf

ปรับแก้ในไฟลเฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano clients-eduroam.conf
    --------
    #
    #  ABC.UXX.AC.TH server -- Sub-Realm
    #
    client abc-uxx-ac-th {
     ipaddr = xxx.xxx.xxx.xxx # 192.168.1.111
     netmask = 32  secret = XXXXXXXXXXXXXXXX
    require_message_authenticator = no  shortname = abc-uxx-ac-th
    nastype = other
    }
```

๒๒. ทดสอบการทำงานดวยผูใช eduroam จากเครื่องใหบริการยอย (Sub-Realm) ของสถาบัน

บัญชีผูใชสำหรับการทดสอบอยูใน **ไฟลที่เครื่องใหบริการยอยของสถาบัน**

mods-config/files-eduroam/authorize

หนาจอที่ 1

```
service freeradius stop
freeradius -X
(stop debugging with CTRL+C)
```

หนาจอที่ 2

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
                    -u 'eduroam@abc.uxx.ac.th' \
                    -p 'TESTING-PASSWORD' \
                    -v -m IEEE8021X \
                    -s eduroam -e PEAP -2 MSCHAPV2
-------- access-accept; 0
RADIUS message: code=2 (Access-Accept) identifier=8
length=187
  Attribute 27 (Session-Timeout) length=6
 Value: 600
  Attribute 1 (User-Name) length=21
 Value: 'eduroam@abc.xx.ac.th'
  Attribute 79 (EAP-Message) length=6
 Value: 03080004
  Attribute 80 (Message-Authenticator) length=18
```

Value: 4f334b7622ec20537163ac31c1926d84

การติดตั้งโดยมี LDAP Server เปนฐานขอมูลบัญชีผูใช

เปนการติดตั้งและกำหนดคุณสมบัติพื้นฐานให Radius server สามารถทำงานกับ LDAP server (OpenLDAP) เพื่อใชบัญชีผูใชจากฐานขอมูล LDAP ข่อมูลบัญชีผูใชควรมีการเก็บรหัสผานในรูปแบบ NT/LM Hash (NT-Password, LM-Password)

การทำงานของ Radius server จะติดตอโดยตรงไปยัง LDAP server ผานโมดูลที่มีอยูใน Radius server

๒๓. โครงสรางขอมูลใน LDAP Server

โครงสรางหลักโดยยอของข่อมูลผูใชใน LDAP Server

```
dn: dc=uxx,dc=ac,dc=th
objectClass: top
objectClass: organization
dc: u

dn: ou=People,dc=uxx,dc=ac,dc=th
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Group,dc=uxx,dc=ac,dc=th
ou: Group
objectClass: top
objectClass: organizationalUnit

dn: cn=Users,ou=Group,dc=uxx,dc=ac,dc=th
cn: Users
objectClass: posixGroup
gidNumber: 1001
description: Group of Users on Unix System

dn: uid=user,ou=People,dc=uxx,dc=ac,dc=th
cn: User
sn: User
objectClass: top
```

objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
uid: user
uidNumber: ๑๐๐๑
gidNumber: ๑๐๐๑
loginShell: /bin/bash
homeDirectory: /home/user
gecos: User User
description: User User
displayName: User User
sambaAcctFlags: [U]
sambaLMPassword: C๘DFD๕AC๐๕๔๖E๙๕DFF๑๗๓๖๕FAF๑FFE๘๙
sambaNTPassword: ๒C๔๗AA๙B๕AC๐๒๓๖๐๔๗๓ECE๘๗B๖๘๐๐๙๒๐ sambaSID: ...
sambaPrimaryGroupSID: ...
userPassword::
e๑NTSEF๙Y๐F๑dXBVNURlbVFhakxxaDFSU๒VVTHl๕Wi๙NQ๑dlSXM=

๒๔. ติดตั้งแพคเกจ freeradius-ldap

ติดตั้ง module เสริม เพื่อให้ freeradius เขาถึงข้อมูลจาก LDAP ได

```
apt install freeradius-ldap -y
```

๒๕. แก้ไขไฟล sites-available/eduroam-inner-tunnel

ปรับแก้ในไฟลเฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano sites-available/eduroam-inner-tunnel
        --------
        authorize {
                ...
                group {
                        #  Read the 'users-eduroam' file
                        files-eduroam {
```

```
                        # return if match
                        ok = return
                        update = return
                }
                #
                # for LDAP
                ldap-eduroam {
                        # return if match
                        ok = return
                        update = return
                }
                # for Active Directory
                #mschap-eduroam {
                #       # return if match
                #         ok = return
                #         update = return
                #}
                # for MySQL
                #sql-eduroam {
                #       # return if match
                #         ok = return
                #         update = return
                #}
                 ...
        }
         ...
}
authenticate {
# PAP Authentication
   Auth-Type PAP {
      pap
   } ...
 #
 # MSCHAP Authentication
 # for file-eduroam and/or LDAP and/or MySQL
        Auth-Type MS-CHAP {
                mschap
        }

        # MSCHAP Authentication
```

```
        # for Active Directory
        #Auth-Type MS-CHAP {
        #       mschap-eduroam
        #}

        # Allow EAP authentication.
        eap-eduroam
}
...
```

๒๖. แก้ไขไฟล modules/ldap-eduroam

โดยปรับแกทุกจุดใหถูกตอง สัมพันธกับ LDAP server

```
cd /etc/freeradius/3.0

nano mods-available/ldap-eduroam
        --------
        ldap ldap-eduroam {

        # server = "your-ldap-server-host-name" # ldap.uxx.ac.th
          server = "your-ldap-server-host-ip" # 192.168.1.2

        # port = 398

        # identity = "cn=admin,dc=uxx,dc=ac,dc=th"
        # password = mypass
         basedn = "dc=uxx,dc=ac,dc=th "
            update {
                control:Password-With-Header += 'userPassword'
        #       control:NT-Password          := 'ntPassword'
                control:NT-Password          := 'sambaNTPassword'
```

```
        ...
    } ...
        user {
                ...
                filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
                ...
                access_attribute = 'uid'
                ...
        }
 ...
}
```

๒๗. เปดใชงานโมดูล ldap-eduroam

```
cd /etc/freeradius/3.0/mods-enabled

ln -s ../mods-available/ldap-eduroam
```

๒๘. เปลี่ยนสิทธิ์หรือเจาของของไฟล

```
chown -R freerad:freerad /etc/freeradius/3.0
```

๒๙. ทดสอบการทำงานดวยผูใชจาก LDAP Server

หนาจอที่ 1

```
service freeradius stop
freeradius -X
(stop debugging with CTRL+C)
```

หนาจอที่ 2

```
cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
        -u  'user@uxx.ac.th' -p 'Asdf๑๒๓๔' \
        -v  -m IEEE8021X \
                -s eduroam -e PEAP -2 MSCHAPV2
 -------- access-accept; 0
 RADIUS message: code=2 (Access-Accept) identifier=8 length=187
    Attribute 27 (Session-Timeout) length=6
                Value: 600
    Attribute 1 (User-Name) length=21
   Value: 'user@uxx.ac.th'
    Attribute 79 (EAP-Message) length=6
    Value: 03080004
    Attribute 80 (Message-Authenticator) length=18
   Value: 4f334b7622ec20537163ac31c1926d84
```

การติดตั้งโดยมี Microsoft Active Directory เปนฐานขอมูลบัญชีผูใช

เปนการติดตั้งและกำหนดคุณสมบัติพื้นฐานให Radius server สามารถทำงานรวมกับ Microsoft Active Directory เพื่อตรวจสอบผูใชจากบัญชีผูใชใน Active Directory

การทำงานของ Radius server จะตรวจสอบตัวตนของผูใชผานโปรแกรมภายนอก คือ samba หรือ winbind จึงจำเปนตองกำหนดคุณสมบัติของ samba หรือ winbind ใหสามารถติดตอกับ Active Directory เสียกอน

๓๐. แกไขไฟล /etc/resolv.conf

ปรับแกในไฟลเฉพาะจุดที่ตองแกไข

nano /etc/resolv.conf

...

search uxx.local

nameserver <dc_server_address> # 192.168.1.3

nameserver <other_dns_server> # 8.8.8.8

๓๑. แก้ไขไฟล /etc/hosts

ปรับแก้ในไฟลเฉพาะจุดที่ต้องแก้ไข

nano /etc/hosts

-------- ...

<dc_server_address> ad.uxx.local ad.uxx.ac.th ad

#192.168.1.3 ad.uxx.local ad.uxx.ac.th ad

๓๒. ติดตั้งแพคเกจสนับสนุนเกี่ยวกับ samba, krb๕ และ winbind

apt install samba winbind krb๕-user krb๕-config -y

Default Kerberos version ๕ realm:

UXX.LOCAL

Kerberos servers for your realm:

ad.uxx.local

Administrative server for your Kerberos realm:

ad.uxx.local

ถาไมพบหนาจอการตั้งคา สามารถกำหนดคุณสมบัติอีกครั้ง

```
dpkg-reconfigure -plow krb5-config
```

๓๓. แก้ไขไฟล /etc/samba/smb.conf

ปรับแกในไฟลเฉพาะจุดที่ต้องแกไข และเพิ่ม

nano /etc/samba/smb.conf

```
--------
[global]

# Change this to the workgroup/NT-domain name ...
        workgroup = UXX

# Add new all lines below to this location
        security = ADS
        realm = UXX.LOCAL
        encrypt passwords = yes
        client use spnego = yes

idmap config *:backend = tdb
idmap config *:range = 1000-9999
idmap config UXX:backend = ad
idmap config UXX:schema_mode = rfc2307
idmap config UXX:range = 10000-99999

winbind nss info = rfc๒๓๐๗
winbind trusted domains only = no
winbind use default domain = yes
winbind enum users  = yes
```

winbind enum groups = yes

winbind refresh tickets = yes

...

๓๔. แก้ไขไฟล /etc/krb๕.conf

ปรับแก้ในไฟลเฉพาะจุดที่ต่องแก้ไข

nano /etc/krb5.conf

-------- [libdefaults]

default_realm = UXX.LOCAL

dns_lookup_realm = false

dns_lookup_kdc = true

forwardable = true

[realms]

UXX.LOCAL = {

kdc = ad.uxx.local

admin_server = ad.uxx.local

}

[domain_realm]

.uxx.local = UXX.LOCAL

uxx.local = UXX.LOCAL

๓๕. รีสตารตโปรแกรม samba

/etc/init.d/samba restart

๓๖. Join เครื่อง Radius server ไปเปนสมาชิกของ Active Directory Domain

net ads join -U Administrator

Enter Administrator's password: <Administrator’s password>

Using short domain name -- UXX

Joined 'YOUR-RADIUS-SERVER' to dns domain 'UXX.LOCAL'

๓๗. รีสตารตโปรแกรม samba และ winbind

/etc/init.d/samba restart

/etc/init.d/winbind restart

๓๘. ทดสอบผลการ Join เครื่อง Radius server ไปเปนสมาชิกของ Active Directory Domain

---

wbinfo -u --------

administrator

user

and other users

หากไมไดผล โดยมั่นใจวา Active Directory ทำงาน และไฟลคุณสมบัติถูกตอง ใหดำเนินการซ้ำในขอ ๓๕-๓๗

๓๙. ทดสอบใชบัญชีผูใชจาก Active Directory

/usr/bin/ntlm_auth --domain=UXX.LOCAL --username=user \

--password=Asdf1234

NT_STATUS_OK: Success (0x0)

๔๐. เพิ่มสิทธิ์ใหผูใชที่รันโพรเซส Radius server เขาในกลุมของผูใชที่รันโปรเซส winbind

---

chown root:winbindd_priv /var/lib/samba/winbindd_privileged

usermod -a -G winbindd_priv freerad

๔๑. แกไขไฟล modules/mschap-eduroam

ปรับแกในไฟลเฉพาะจุดที่ตองแกไข

```
cd /etc/freeradius/3.0
        nano modules/mschap-eduroam
        --------
        mschap mschap-eduroam {
                use_mppe = yes

                require_encryption = yes
                require_strong = yes

                ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key
                        --domain=UXX.LOCAL --username=%{Stripped-User-Name}
                        --challenge=%{mschap:Challenge:-00}
                        --nt-response=%{mschap:NT-Response:-00}"

                #ntlm_auth_timeout = 10
                ...
        }
```

๔๒. แก้ไขไฟล sites-available/eduroam-inner-tunnel

ปรับแก้ในไฟลเฉพาะจุดที่ต้องแก้ไข

```
nano sites-available/eduroam-inner-tunnel
        --------
        authorize {
           ...
           group {
                   #  Read the 'users-eduroam' file
                files-eduroam {
                        # return if match
                        ok = return
                        updated = return
                   }
```

```
        #
        # for LDAP
        #ldap-eduroam {
        #       # return if match
        #       ok = return
        #       updated = return
        #}
        # for Active Directory
        mschap-eduroam {
            # return if match
            ok = return
           updated = return
        }
        # for MySQL
        #sql- eduroam {
          #                    # return if match
          #                ok = return
        #       updated = return
        #}
         ...
    }
    ...
}
     authenticate {
            # PAP Authentication
            Auth-Type PAP {
                              pap
             }

            # MSCHAP Authentication
            # for file-eduroam and/or LDAP and/or MySQL
```

```
        #Auth-Type MS-CHAP {
        #    mschap
        #}

        # MSCHAP Authentication
        # for Active Directory
        Auth-Type MS-CHAP {
            mschap-eduroam
        }

        eap-eduroam
    }
    ...
```

๔๓. เปดใชงานโมดูล mschap-eduroam

```
cd /etc/freeradius/3.0/mods-enabled
ln -s ../mods-available/mschap-eduroam
```

๔๔. เปลี่ยนสิทธิ์หรือเจาของของไฟล

```
chgrp -R freerad /etc/freeradius
```

๔๕. ทดสอบการทำงานดวยผูใชจาก Active Directory

หนาจอที่ 1

```
service freeradius stop
freeradius -X
(stop debugging with CTRL+C)
```

หนาจอที่ ๒

```
cd /etc/freeradius/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \
                        -u  'user@uxx.ac.th' \
                        -p 'Asdf๑๒๓๔' \
                        -v  -m IEEE8021X \
                        -s eduroam -e PEAP -2 MSCHAPV2
------- access-accept; 0
RADIUS message: code=2 (Access-Accept) identifier=8
length=187
   Attribute 27 (Session-Timeout) length=6
    Value: 600
   Attribute 1 (User-Name) length=21
    Value: 'user@uxx.ac.th'
   Attribute 79 (EAP-Message) length=6
    Value: 03080004
   Attribute 80 (Message-Authenticator) length=18
    Value: 4f334b7622ec20537163ac31c1926d84
```

การติดตั้งโดยมี MySQL เปนฐานขอมูลบัญชีผูใช

เปนการติดตั้งและกำหนดคุณสมบัติพื้นฐานให Radius server สามารถทำงานโดยเขาถึงฐานขอมูลผูใชที่เก็บไวใน เซิรฟเวอร MySQL

ขอมูลบัญชีผูใชที่เก็บในรูปแบบของฐานขอมูลนั้น สามารถมีโครงสรางใดก็ได ขึ้นอยูกับมหาวิทยลัยออกแบบและจัดเก็บ แตในคูมือนี้ จะอางอิงรูปแบบการจัดเก็บขอมูลตามวิธีการพื้นฐานของ freeradius-mysql

๔๖. โครงสรางขอมูลใน MySQL Server

องคประกอบพื้นฐานที่สุดของการจัดเก็บขอมูลบัญชีผูใช ตามรูปแบบของ freeradius-mysql นั้น ขอมูลผูใชจะเก็บไวในตาราง ชื่อ radcheck มีรูปแบบของขอมูลผูใช ดังนี้

```
mysql> select * from radcheck;
+----+----------+-------------------+----+----------+
| id | username | attribute         | op | value    |
+----+----------+-------------------+----+----------+
|  1 | user     | Cleartext-Password | := | Asdf1234 |
+----+----------+-------------------+----+----------+

mysql> select * from radcheck;
+----+----------+------------+----+---------------------
+
| id | username | attribute   | op | value
|
+----+----------+------------+----+--------------------+
|  1 | user     | NT-Password | := | 2C47AA9B5AC02360473.. |
|  2 | user     | LM-Password | := | C8DFD5AC0546E95DFF1.. |
+----+----------+------------+----+---------------------
+
```

๔๗. ติดตั้งแพคเกจ freeradius-mysql

ติดตั้ง module เสริม เพื่อให้ freeradius เขาถึงข้อมูลจาก MySQL ได

```
apt-get install freeradius-mysql -y
```

๔๘. แก้ไขไฟล sites-available/eduroam-inner-tunnel

ปรับแก้ในไฟลเฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano sites-available/eduroam-inner-tunnel
        --------
```

```
authorize {
        ...
    group {
        #  Read the 'users-eduroam' file        files-eduroam {
                # return if match
                ok = return
                updated = return
        }
        #
        # for LDAP
        #ldap-eduroam {
        #    # return if match
        #    ok = return
        #    updated = return
        #}
        # for Active Directory
        #mschap-eduroam {
        #    # return if match
        #    ok = return
        #    updated = return
        #}
        # for MySQL
        sql- eduroam {
            # return if match
            ok = return
            updated = return
        }
        ...
    }
    ...
}
```

```
authenticate {

    # PAP Authentication
    Auth-Type PAP {
        pap     }
   ...
    # MSCHAP Authentication
    # for file-eduroam and/or LDAP and/or MySQL
    Auth-Type MS-CHAP {
        mschap
    }

    # MSCHAP Authentication
    # for Active Directory
    #Auth-Type MS-CHAP {
    #    mschap-eduroam
    #}

    eap-eduroam
  }
...
```

๔๙. แก้ไขไฟล mods-available/sql-eduroam

ปรับแก้ในไฟลเฉพาะจุดที่ต้องแก้ไข

```
cd /etc/freeradius/3.0

nano mods-available/sql-eduroam
        --------
        sql sql-eduroam {
```

```
...
#
driver = "rlm_sql_mysql"
dialect = "mysql"
...
 # Connection info:
server = "<mysql_server_host_address>" # 192.168.1.2
#port = 3306
login = "radius"
password = "radpass"
radius_db = "radius"
acct_table๑ = "radacct"
acct_table๒ = "radacct"
...
}
```

๕๐. แก้ไขไฟล mods-config/sql/main/mysql/queries-eduroam.conf

ปรับแก้ในไฟลเฉพาะจุดที่ต่องแก้ไข

กรณีมีฐานข่อมูลบัญชีผู้ใชที่ไมเปนไปตามรูปแบบของ freeradius-mysql จำเปนตองแก้ไขคำสั่ง SQL เพื่อให เหมาะสมกับโครงสรางขอมูลนั้น

```
cd /etc/freeradius/3.0

nano mods-config/sql/main/mysql/queries-eduroam.conf
--------
...
#  Query config:  Username
...
sql_user_name = "%{%{Stripped-User-Name}:-%{%{User-Name}:-DEFAULT}}"
```

```
        #sql_user_name = "%{User-Name}"
        ...
        #  Authorization Queries
        ...
        authorize_check_query = "\
                SELECT id, username, attribute, value, op \
                FROM ${authcheck_table} \
                WHERE username = '%{SQL-User-Name}' \
                ORDER BY id"
authorize_reply_query = "\
                SELECT id, username, attribute, value, op \
                FROM ${authreply_table} \
                WHERE username = '%{SQL-User-Name}' \
                ORDER BY id"
        ...
        #group_membership_query = "\
        #       SELECT groupname \
        ...
        #       ORDER BY priority"

        #authorize_group_check_query = "\
        #       SELECT id, groupname, attribute, \
        ...
        #       ORDER BY id"

        #authorize_group_reply_query = "\
        #       SELECT id, groupname, attribute, \
        ...
        #       ORDER BY id"
        ...
```

๕๑. เปดใชงานโมดูล ldap-eduroam

cd /etc/freeradius/3.0/mods-enabled

ln -s ../mods-available/sql-eduroam

๕๒. เปลี่ยนสิทธิ์หรือเจาของของไฟล

chown -R freerad:freerad /etc/freeradius/3.0

๕๓. ทดสอบการทำงานดวยผูใชจาก MySQL

หนาจอที่ 1

service freeradius stop freeradius -X

(stop debugging with CTRL+C)

หนาจอที่ 2

cd /etc/freeradius/3.0/tool

./rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 \

-u 'user@uxx.ac.th' -p 'Asdf1234' \

-v -m IEEE๘๐๒๑X \

-s eduroam -e PEAP -2 MSCHAPV2

---

access-accept; 0

RADIUS message: code=2 (Access-Accept) identifier=8 length=187

Attribute 27 (Session-Timeout) length=6

Value: 600

Attribute 1 (User-Name) length=21

Value: 'user@uxx.ac.th'

Attribute 79 (EAP-Message) length=6

Value: 03080004

Attribute 80 (Message-Authenticator) length=18

Value: 4f334b7622ec20537163ac31c1926d84

การติดตั้ง Wireless Controller หรือ Anonymous Access Point รวมกับ Radius server

Radius server: แก้ไขไฟล clients.conf หรือ clients-eduroam.conf

เพิ่ม IP address หรือเครือขายของ Anonymous Access Point

```
cd /etc/freeradius/3.0

nano clients.conf --------
        client <ip_or_network_of_access_point_or_wlc> {
                secret = testing123
                shortname  = my_access_point
        }
        client 172.16.11.8 { secret = secret_for_172_16_11_8 shortname =
                ap_172_16_11_8
        }
        client 192.168.0.0/24 { secret = secret_for_net_192_168_0_0_24 shortname =
        ap_in_net_192_168_0_0_24 }
```

Cisco Wireless Controller

๑. Add/Edit RADIUS profile

SECURITY > AAA > RADIUS > Authentication > [New...] or Edit

Server IP Address(Ipv๔/Ipv๖): <radius_server_ip_address>

Shared Secret Format: ASCII

Shared Secret: <secret_shared_with _radius_server>

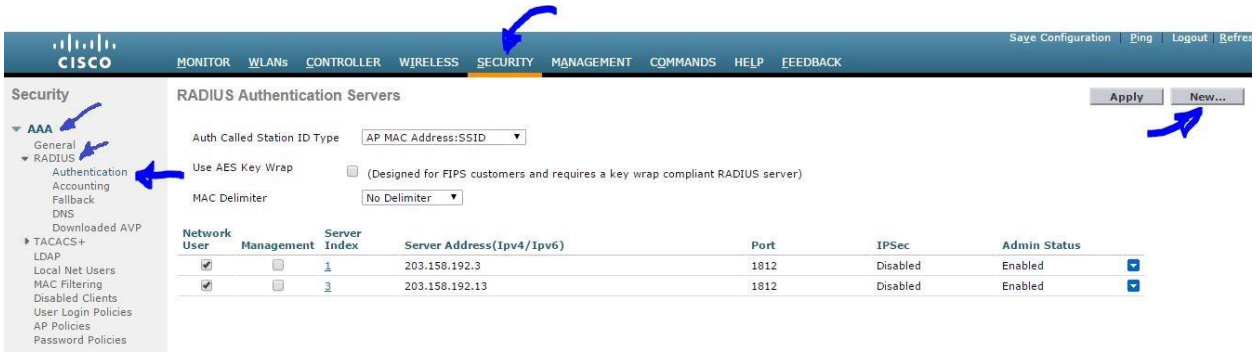
Confirm Shared Secret: <secret_shared_with _radius_server>

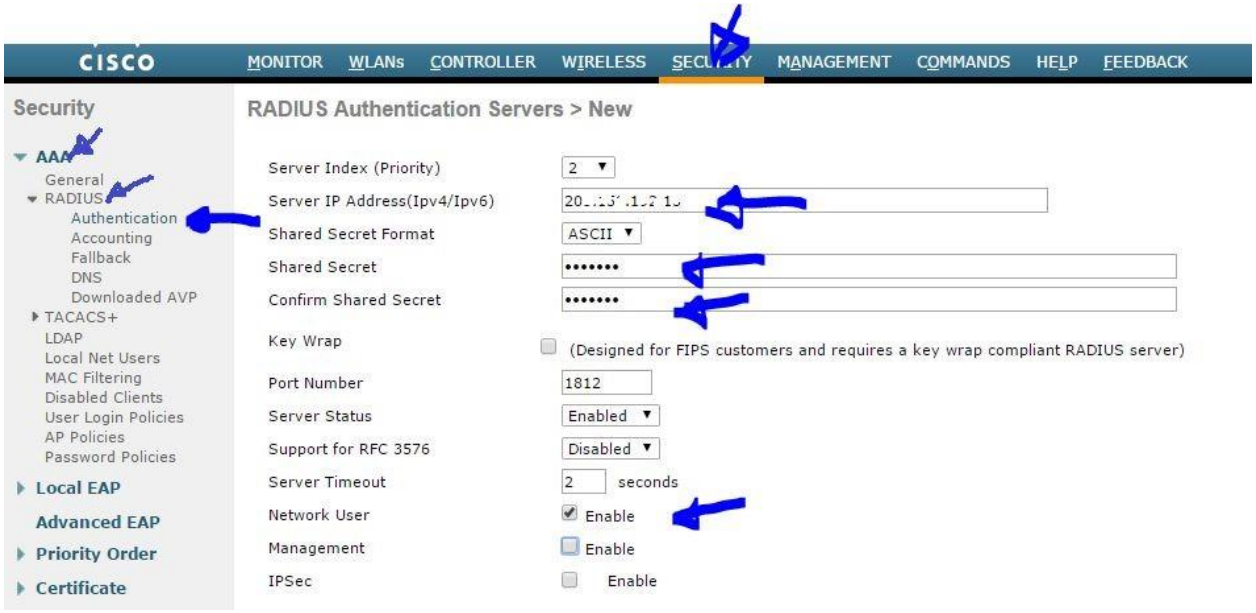
Key Wrap: [ ]

Port Number: 1812

Server Status: Enabled

Network User: [/] Enable





SECURITY > AAA > RADIUS > Accounting > [New...] or Edit

Server IP Address(Ipv๔/Ipv๖): <radius_server_ip_address>

Shared Secret Format: ASCII

Shared Secret: <secret_shared_with _radius_server>

Confirm Shared Secret: <secret_shared_with _radius_server>

Port Number: 1813

Server Status: Enabled

Network User: [/] Enable

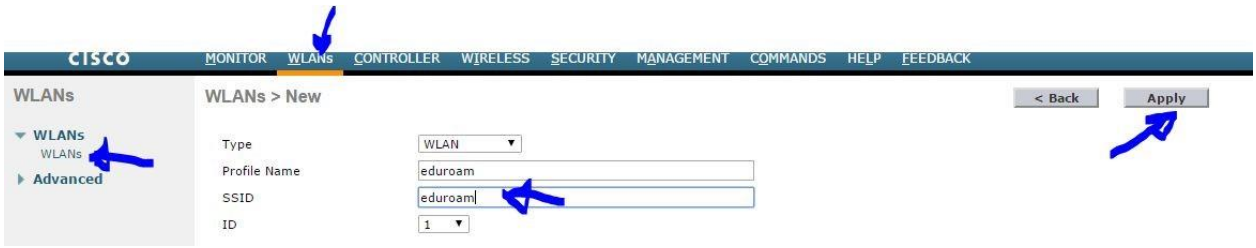
๒. Add/Edit Wireless LAN profile

WLANs > WLANs > WLANs > [Create new...] or Edit

Type: [WLAN]

Profile Name: <wlan_profile>

SSID: <wlan_ssid>



WLANs > WLANs > WLANs > [wlan_profile] > Security > Layer 2

Layer 2 Security: WPA+WPA2

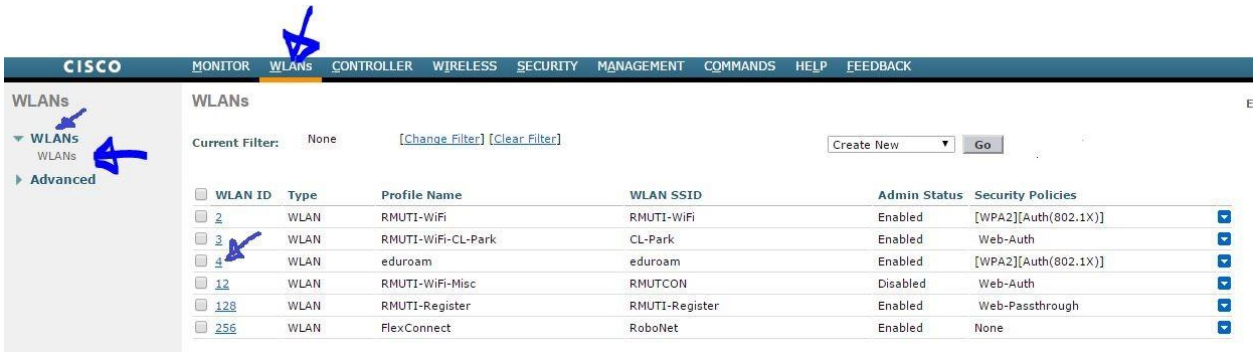
WPA+WPA๒ Parameters

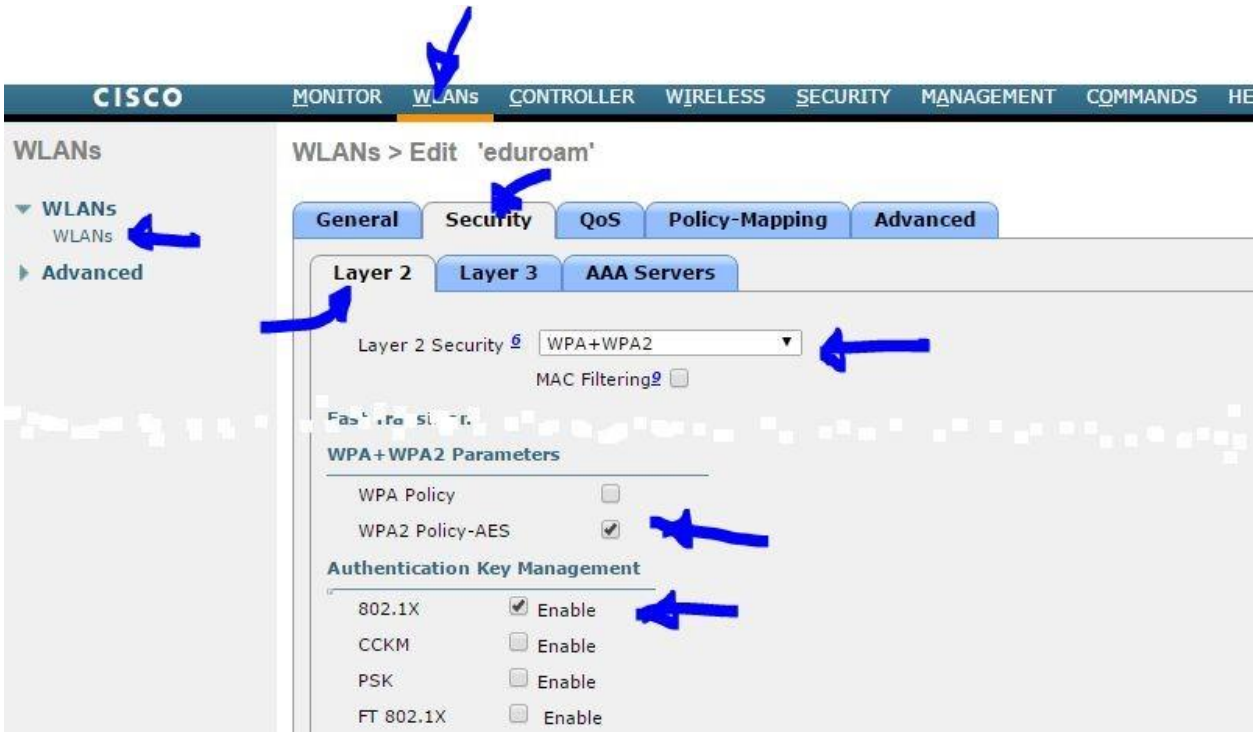
WPA Policy: [ ]

WPA๒ Policy-AES: [/]

Authentication Key Management

802.1X: [/] Enable





WLANs > WLANs > WLANs > [wlan_profile] > Security > AAA Server

Authentication Servers Accounting Servers

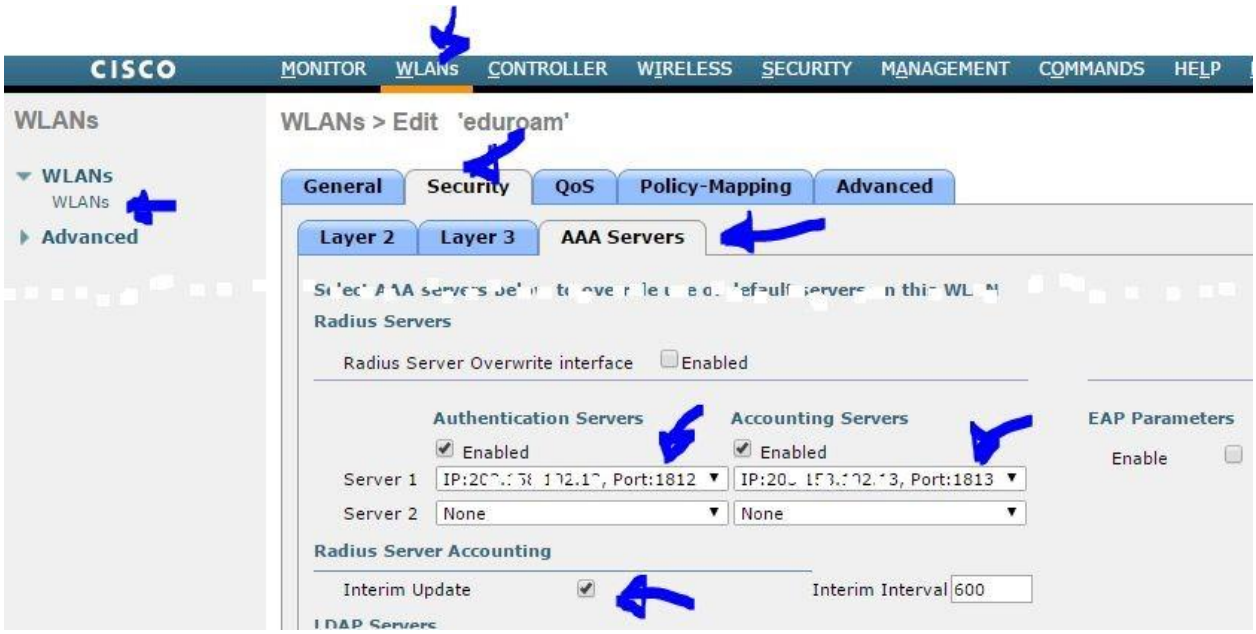
[/] Enabled [/] Enabled

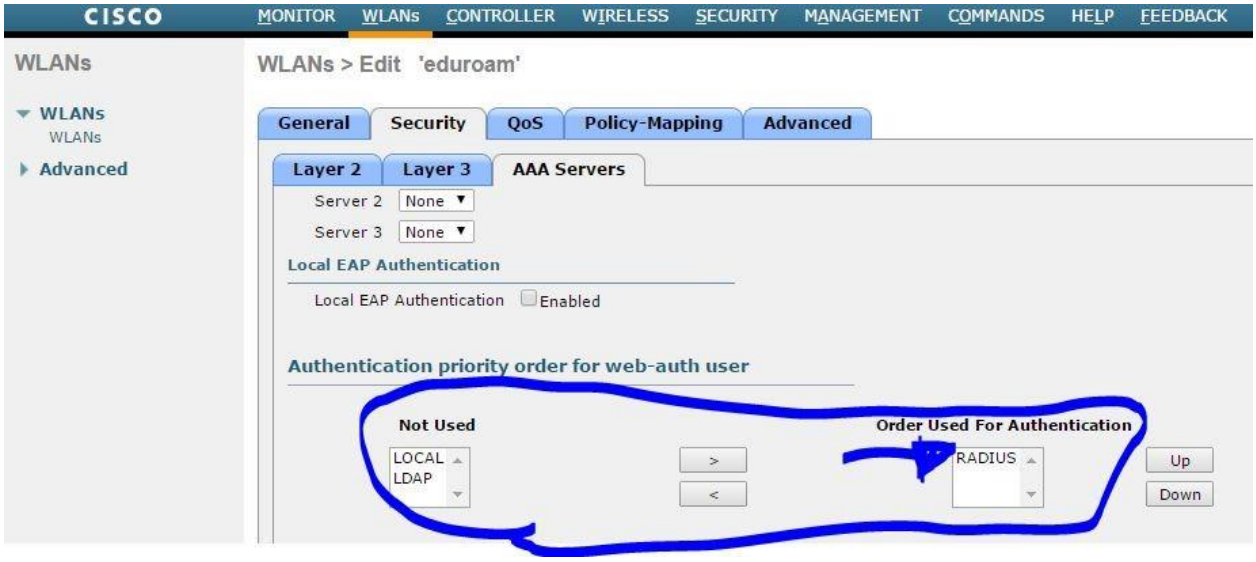
Server 1 [auth_radius_ip:port]

[acct_radius_ip:port]

Radius Server Accounting

Interim Update: [/]





Aruba Wireless Controller

1. Create Radius Server profile

   Configuration > Security > Authentication > Servers > RADIUS Server

2. Edit Radius Server profile

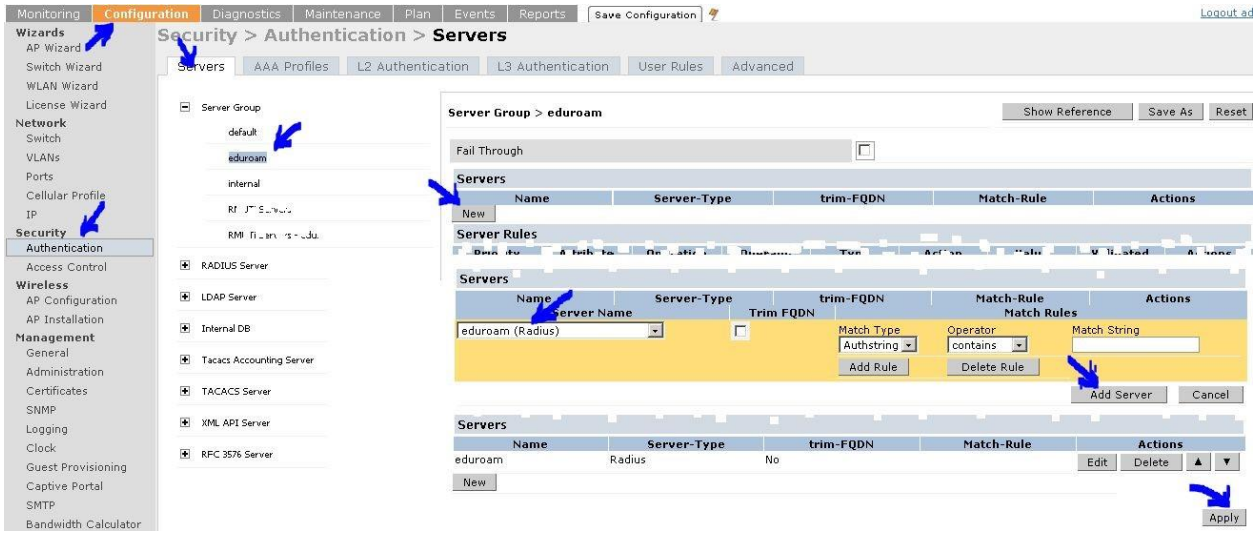
Configuration > Security > Authentication > Servers > RADIUS Server > eduroam

3. Create Server Group profile

Configuration > Security > Authentication > Servers > Server Group

4. Add RADIUS to Server Group profile

Configuration > Security > Authentication > Servers > Server Group > eduroam

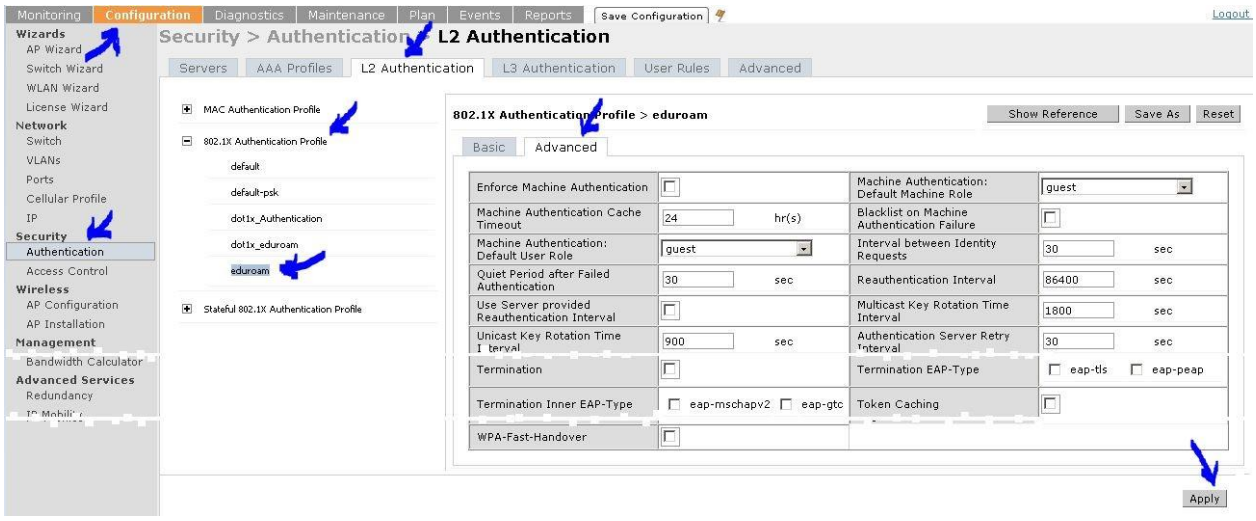


5. Create L๒ Authentication profile

Configuration > Security > Authentication > L๒ Authentication > ๘๐๒.๑X Authenticaion Profiles

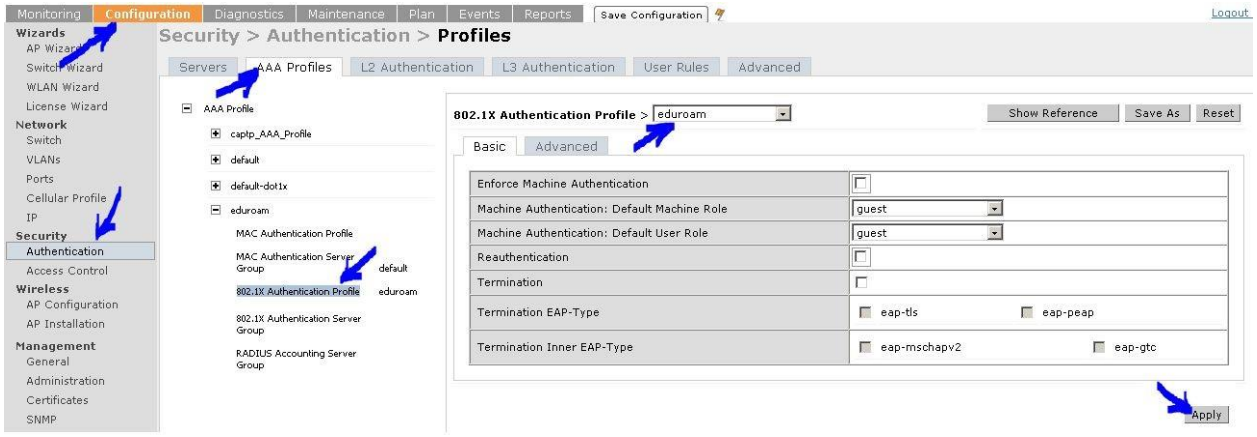
6. Edit L๒ Authentication profile

Configuration > Security > Authentication > L๒ Authentication > ๘๐๒.๑X Authenticaion Profiles > eduroam



7. Create AAA Authentication profile

Configuration > Security > Authentication > AAA Authentication

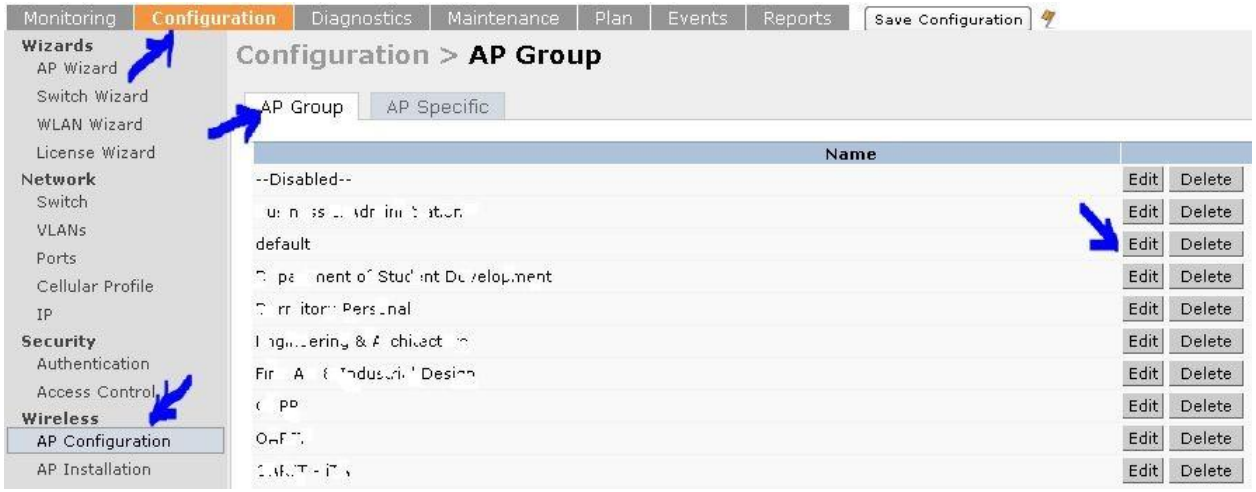


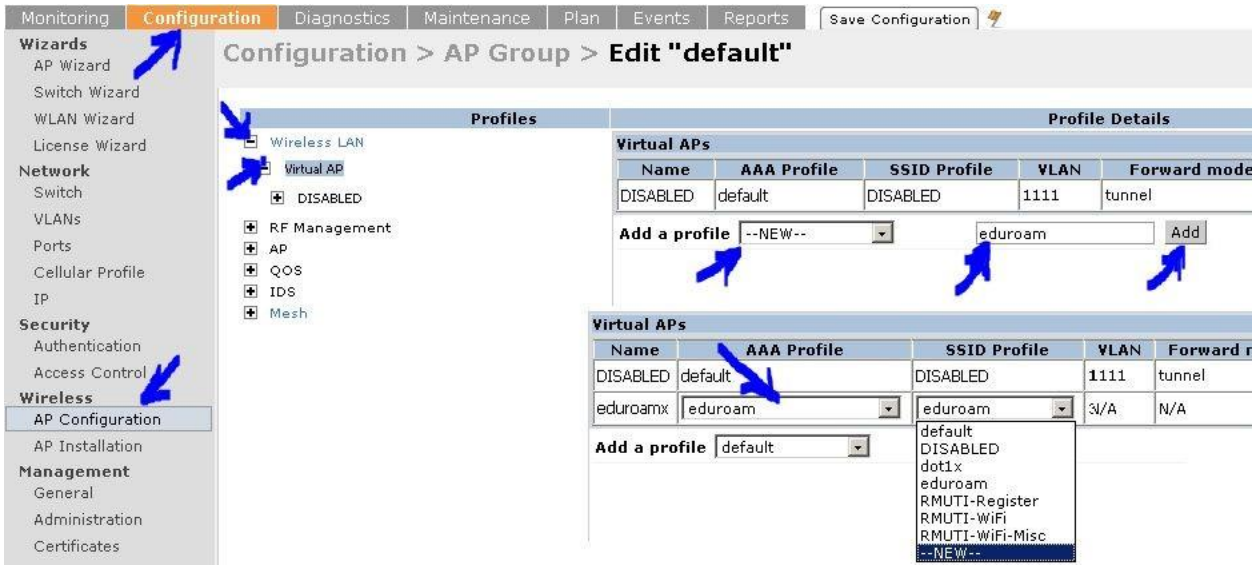
8. Modify Advanced Authentication

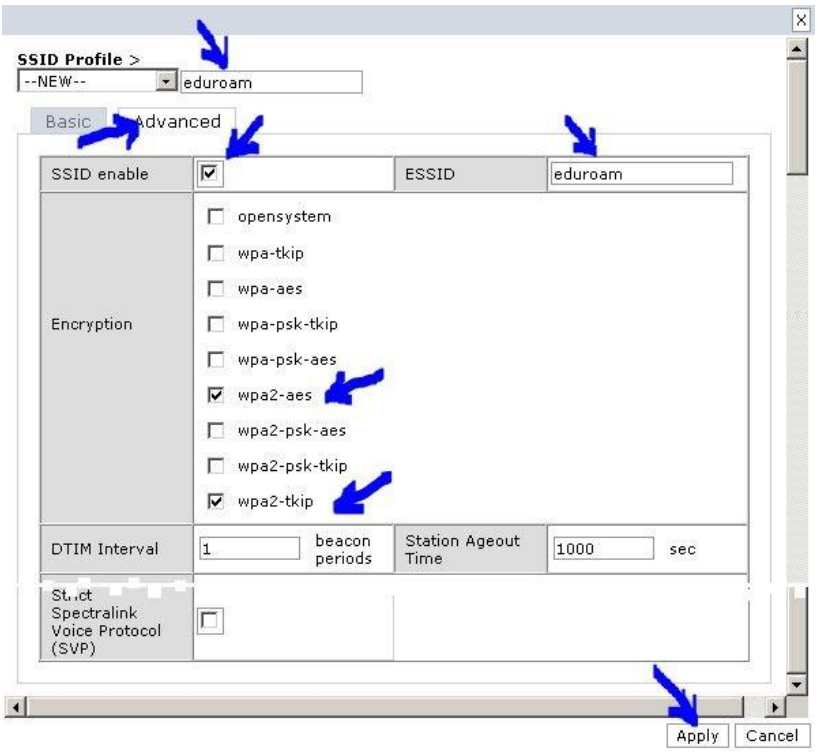
Configuration > Security > Authentication > Advanced

9. Modify AP Configuration

Configuration > Wireless > AP Configuration > AP Group


Monitoring
Configuration
Diagnostics
Maintenance
Plan
Events
Reports
Save Configuration
Wizards
AP Wizard
Switch Wizard
WLAN Wizard
License Wizard
Network
Switch
VLANs
Ports
Cellular Profile
IP
Security
Authentication
Access Control
Wireless
AP Configuration
AP Installation
Configuration > AP Group
AP Group
AP Specific
Name
--Disabled--
default
Edit
Delete


Monitoring
Configuration
Diagnostics
Maintenance
Plan
Events
Reports
Save Configuration
Wizards
AP Wizard
Switch Wizard
WLAN Wizard
License Wizard
Network
Switch
VLANs
Ports
Cellular Profile
IP
Security
Authentication
Access Control
Wireless
AP Configuration
AP Installation
Management
General
Administration
Certificates
Configuration > AP Group > Edit "default"
Profiles
Wireless LAN
Virtual AP
DISABLED
RF Management
AP
QOS
IDS
Mesh
Profile Details
Virtual APs
Name
AAA Profile
SSID Profile
VLAN
Forward mode
DISABLED
default
DISABLED
1111
tunnel
Add a profile
--NEW--
eduroam
Add
eduroamx
N/A
default
DISABLED
dot1x
eduroam
RMUTI-Register
RMUTI-WiFi
RMUTI-WiFi-Misc
--NEW--



<u>การตรวจวิเคราะหและตรวจสอบการทำงานของ Radius server</u>

การทำงานของ Radius server นั้น จะมีการรับข่อมูลการรองขอการเขาถึง (Access-Request) จากภายนอก และสงตอเปนลำดับขั้นการทำงานตามลำดับที่ประกาศไวในไฟลคุณสมบัติ โดยลำดับขั้นสำคัญจะอยูในไฟลไซตที่ประกาศใช ประกอบดวยไฟล sites-enabled/eduroam และไฟล sites-enabled/eduroam-inner-tunnel

เมื่อ Radius server ไดรับการรองขอ จะนำขอมูลการรองขอเข่าไปประมวลผลตามขั้นตอนในไฟล sites-enabled/eduroam เปนไฟลแรก และอาจสงตอไปยังการประมวลผลภายในในไฟล sites-enabled/eduroam-inner-tunnel หรือสงตอไปยัง Radius server เครื่องถัดไป

๑. การเขียนภาษา unlang ใชใน Radius server

ผูใชสามารถเขียนภาษา unlang เพื่อประมวลผลข่อมูลและตัดสินใจการทำงานได เชน เขียนเพื่อการตรวจสอบรูปแบบบัญชีผูใชใหเหมาะสม หรือเปนไปตามกฎของการใชบริการ eduroam เปนตน

รูปแบบของภาษา unlang จะใกลเคียงกับภาษา C สามารถเขียนใหมีการตรวจสอบคาหรือตัวแปร กำหนดเสนทางการทำงานตามรูปแบบของภาษาโปรแกรม และกำหนดผลการทำงาน สามารถเขียนภาษา unlang ไดในสวนการประมวลข่อมูล เชน authrize {}, authenticate {} เปนตน

ตัวแปรของภาษา unlang จะเปนตัวแปรภายใน ไมสามารถประกาศขึ้นเองได ตัวแปรที่เกิดขึ้น จะขึ้นกับ ๓ สวน คือ สวนของการทำงานของโมดูล จากการกำหนดเปน Attribute ในไฟล dictionary และสิ่งที่ลูกขายสงเขามาขณะร่องขอบริการ

การกำหนดคาใหตัวแปร ใชใน section ชื่อ update ใน 3 ตำแหนง control, request และ response ตัวอยาง เชน

```
update request {
        User-Name := "login_name"
}
update control {
        Proxy-To-Realm := "LOCAL"
}
update response {
        Operator-Name := "๑abc.ac.th"
}
```

การอางถึงตัวแปร ใชรูปแบบ %{Variable-Name} เชน ไมตองดำเนินการใน section ใดๆ เชน

```
if( "%{Realm}" =~ /rmuti.ac.th$$/ ) { reject
}
```

ตัวกระทำในภาษา unlang มีเชนเดียวกับโปรแกรมภาษา C แตมีความยืดหยุนกวา เชน การเปรียบเทียบ

(!foo) Negation

(foo || bar) Or

(foo && bar) And

(foo == bar) Equal

(foo != bar) Not equal

(foo =~ bar) Regular expression (match)

(foo !~ bar) Negate regular expression (not match)

(foo < bar) Less than

(foo > bar) More than

การกำหนดคา

foo = “value” Add the attribute to the list, if and only if an attribute of the same name is not already present in that list.

foo := “value” Add the attribute to the list. If any attribute of the same name is already present in that list, its value is replaced with the value of the current attribute.

foo += “value” Add the attribute to the tail of the list, even if attributes of the same name are already present in the list. When the right hand side of the expression resolves to multiple values, it means add all values to the tail of the list.

ตัวอยางตัวแปรที่มักมีการอางถึง สามารถดูไดจากการรันโปรแกรมแบบ Debug เชน

การรองขอ (Request)

Received Access-Request Id 0 from 127.0.0.1:59868 to ...

User-Name = 'user@rmuti.ac.th'

NAS-IP-Address = 127.0.0.1

Calling-Station-Id = '70-6F-6C-69-73-68'

Framed-MTU = 1400

NAS-Port-Type = Wireless-802.11

การตอบกลับ (Response)

Sending Access-Challenge Id ๐ from 127.0.0.1:1812 to ...

```
        EAP-Message = 0x010100061920
      Message-Authenticator = 0x000000000000000000...

Sending Access-Accept Id 9 from 127.0.0.1:1812 to ...
        User-Name := 'user@rmuti.ac.th'
        EAP-Message = 0x03090004
      Message-Authenticator = 0x000000000000000000...
```

การกำหนดเสนทางการไหลของโปรแกรม สามารถใชการกระทำแบบเลือกทางพื้นฐาน คือ if else elseif ได เชน

```
if( "%{Realm}" =~ /rmuti.ac.th$$/ ) {
        update control {
                Proxy-To-Realm := LOCAL
        }
}
else {
        update request {
                Realm := "eduroam"
        }
}
```

๒. การคัดกรองบัญชีผูใชที่ไมเหมาะสม

เพื่อคัดกรองบัญชีที่ผิดปกติ จำเปนตองเขียนภาษา unlange เพิ่มเขาไปในไซต ตัวอยางชื่อบัญชีที่ไมเหมาะสม คือ บัญชีที่ไมมี realm หรือไมมี @xxxx หรือบัญชีที่เกิดจากการทำงานโดยอัตโนมัติของบางระบบปฏิบัติการ เชน ๓gppnetwork.org เปนตน

ในการติดตั้งนี้ ไดมีการเขียนภาษา unlang เพื่อคัดกรองบัญชีที่ไมเหมาะสมตามที่ไดรวบรวมไวแลว ไวในไฟล eduroam-realm-checks.conf และไดนำไฟลนี้ไปประกอบเปนสวนหนึ่งของไฟลไซต sites-enabled/eduroam

```
sites-enabled/eduroam
        --------
        authorize {
                $INCLUDE ${confdir}/eduroam-realm-checks.conf
        }
```

๓. การกำหนดเครือขายใหเหมาะสมกับผูใชที่ตางกัน

หากตองการผูใชตางการถูกทำใหเชื่อมตอเขากับเครือขายที่ตางกัน สามารถทำไดโดยการสงขอมูลหมายเลข VLAN จาก Radius server ไปยัง Wireless Controller (WLC) หรือ Access Point (AP) ได ทั้งนี้ ที่ WLC หรือ AP จะตองประกาศ VLAN ดวยหมายเลขที่ตรงกับที่ตอบกลับโดย Radius server ตัวอยางเชน ตองการแยกระหวางอาจารย (User-Name: txxxxxx) กับนักศึกษา (User-Name: sxxxxxx) ใหใชเครือขายที่ตางกันดังผังเครือขาย

```
                                +-- Teacher
+---------------+    +-----------+ VID:๑๐๐ for Teachers .++.
| Radius server |----| L2 device |======================|AP|
+---------------+    +-----------+ VID:๒๐๐ for Students +--+
                               +-- Student
```

```
sites-enabled/eduroam
--------
post-auth {
        update reply {
            Tunnel-Type := "VLAN"
            Tunnel-Medium-Type := "IEEE-802"
        }
                if( "%{User-Name}" =~ /^t*/ ) {
                        update reply {
                                Tunnel-Private-Group-Id := 100
                        }
                }
                elseif( "%{User-Name}" =~ /^s*/ ) {
                        update reply {
                                Tunnel-Private-Group-Id := 200
                        }
                }
                else {
```

```
        }
    }
```

๔. การดูกิจกรรมการทำงานของโปรแกรมโดยละเอียด (Full debuging)

การตรวจสอบการทำงานของโปรแกรม Radius server วาทำงานอยางถูกตองหรือไมนั้น วิธีที่ดีที่สุดคือการสั่งรันโปรแกรมแบบ full debuging โปรแกรมจะพิมพผลการทำงาน หรือกิจกรรมที่เกิดขึ้นโดยละเอียดออกทางจอภาพในเครื่องหนึ่งเครื่องจะสามารถรันโปรแกรม Radius server ไดเพียงหนึ่งโปรแกรม ดังนั้น หากจะรันโปรแกรม แบบ full debuging จะต่องปดโปรแกรมเดิมกอน และสิ้นสุดดวยการพิมพ CTRL+C การดำเนินการเปนดังนี้

```
service freeradius
stop freeradius -X
```

หรือการบันทึกผลการทำงานไวในไฟล

```
freeradius -X > text.txt
```

๕. การบันทึกกิจกรรมใน Log

คุณสมบัติเกี่ยวกับการบันทึกกิจกรรมการทำงานที่กำหนดไวการติดตั้งนี้ ใชไฟลโมดูลเดิม และมีตำแหนงการบันทึกตามคาดั้งเดิมของ Radius server ประกอบดวย

```
sites-enabled/eduroam -------- authorize {
        # get request from local user and NRO (as IdP and SP)
        # config: ${configdir}/(modules or mods-enabled)/detail.log
        # log:
        ${logdir}/radacct/<client_ip>/auth-detail-<date>
        auth_log
    }
    accounting {
        # accouting request from local user and NRO (as IdP and SP)
        # config: ${configdir}/(modules or mods-enabled)/detail
        # log: ${logdir}/radacct/<client_ip>/detail-<date>
        detail
```

```
}
 post-auth {
        # get result after authentication process (as IdP)
        # config: ${configdir}/(modules or mods-enabled)/detail.log
        # log:
        ${logdir}/radacct/<client_ip>/reply-detail-<date>
        reply_log
}
pre-proxy {
        # process and forward request to NRO (as SP)
        # config: ${configdir}/(modules or mods-enabled)/detail.log
        # log:
        ${logdir}/radacct/<client_ip>/pre-proxy-detail-<date>
        pre_proxy_log
}
post-proxy {
        # get response from NRO (as SP)
        # config: ${configdir}/(modules or mods-enabled)/detail.log
        # log:
        ${logdir}/radacct/<client_ip>/post-proxy-detail-<date>
        post_proxy_log
}
```

ตัวอยางเนื้อหาในไฟล auth-detail

```
Fri Oct 23 22:39:14 2015
Packet-Type = Access-Request
  User-Name = "eduroam@rmuti.ac.th"
NAS-IP-Address = 127.0.0.1
        Calling-Station-Id = "70-6F-6C-69-73-68"
Stripped-User-Name = "eduroam"
  NAS-Port-Type = Wireless-802.11
```

Realm = "rmuti.ac.th"

ตัวอยางเนื้อหาในไฟล reply-detail

Sat Oct 24 02:01:00 2015

Packet-Type = Access-Accept

Session-Timeout = 600

User-Name = "eduroam@rmuti.ac.th"

ตัวอยางเนื้อหาในไฟล pre-proxy-detail

Sat Oct 24 00:05:49 2015

Packet-Type = Access-Request

User-Name = "eduroam@rmuti.ac.th"

NAS-IP-Address = 127.0.0.1

Calling-Station-Id = "70-6F-6C-69-73-68"

Realm = "eduroam"

Proxy-State = 0x30

ตัวอยางเนื้อหาในไฟล post-proxy-detail

Mon Oct 26 15:33:43 2015

Packet-Type = Access-Accept

Session-Timeout = 600 User-Name = "eduroam@rmuti.ac.th"

Proxy-State = 0x39

อางอิง

- https://www.eduroam.us/node/๘๙
- http://confluence.diamond.ac.uk/display/PAAUTH/Using+Active+Directory+as+authentication+source
- https://wiki.samba.org/index.php/Setup_a_Samba_AD_Member_Server
- http://freeradius.org/radiusd/man/unlang.html
- https://www.tobtu.com/lmntlm.php -

จัดทำโดย สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet)

Version ๑

๑๕/๑/๒๕๖๗