TANet無線網路漫遊交換中心

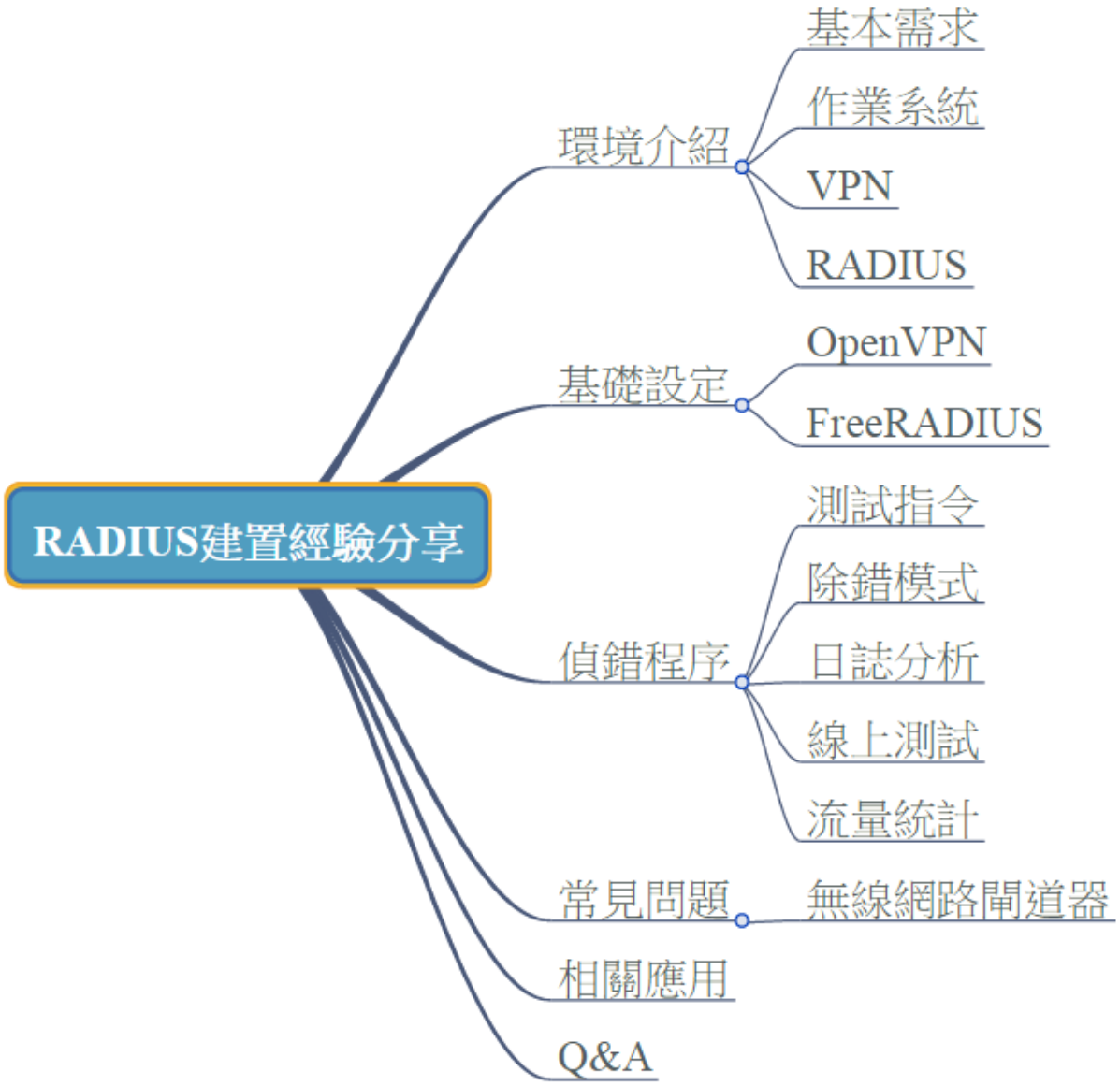
Taiwan Academic Network Roaming Center

無線網路漫遊交換中心
RADIUS 建置經驗分享

江欣鴻

cowman@ems.niu.edu.tw

大綱


RADIUS建置經驗分享
環境介紹
基本需求
作業系統
VPN
RADIUS
基礎設定
OpenVPN
FreeRADIUS
偵錯程序
測試指令
除錯模式
日誌分析
線上測試
流量統計
常見問題
無線網路閘道器
相關應用
Q&A

環境介紹

漫遊成員的基本需求

- 對外的漫遊伺服器
  - VPN
  - RADIUS
- 支援RADIUS協定的無線網路閘道器
  - 無線設備
    - Thin AP
    - Fat AP

作業系統

- Linux
  - CentOS
    - http://www.centos.org/
  - Red Hat
    - http://www.redhat.com/en
  - Ubuntu
    - http://www.ubuntu.com/
  - Debian
    - https://www.debian.org/
- BSD
  - FreeBSD
    - https://www.freebsd.org/
- Windows

VPN

- Virtual Private Network，虛擬私有網路
- 在漫遊環境中採行 SSL VPN 機制，允許雙方在實體網路架構上以一個安全的通道 (Tunnel) 進行資料交換，以確保資料安全性
- 將安裝 OpenVPN 套件
  - https://openvpn.net/

VPN

- CentOS
  - wget http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
  - rpm -Uvh epel-release-6-8.noarch.rpm
  - yum install openvpn
- Ubuntu、Deiban
  - apt-get install openvpn
- FreeBSD
  - cd /usr/ports/security/openvpn/
  - make install clean

RADIUS

- Remote Authentication Dial-in User Service，遠端用戶撥入驗證服務
- 基於AAA協議
  - Authentication 驗證
  - Authorization 授權
  - Accounting 計費
- 利用realm的辨識方式將認證資訊以加密後的訊息轉發至帳戶的認證伺服器中取得帳密認證結果
- 將安裝 FreeRADIUS 套件
  - http://freeradius.org/

RADIUS

- CentOS
  - yum install freeradius freeradius-utils
- Ubuntu、Deiban
  - apt-get install freeradius freeradius-utils
- FreeBSD
  - cd /usr/ports/net/freeradius
  - make install clean

基礎設定

OpenVPN

- 連線設定檔案

clt_009_test.tar.gz
- ca.crt
- ta.key
- client.conf
- clt_009_test.crt
- clt_009_test.csr
- clt_009_test.key

- 程式預設目錄
  - /etc/openvpn

- 啟動openvpn服務
  - service openvpn start

- 設定開機自動啟動
  - chkconfig openvpn on

OpenVPN

- client.conf

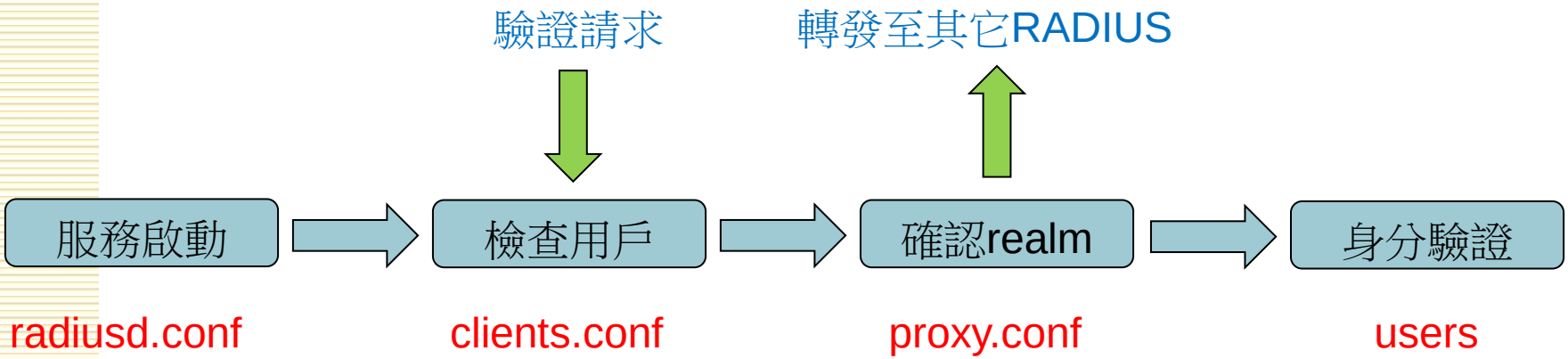
```
client
dev tun
proto tcp
remote 漫遊中心VPN伺服器TANet線路 443
remote 漫遊中心VPN伺服器TWAREN線路 443
float
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert clt_009_test.crt
key clt_009_test.key
tls-auth ta.key 1
comp-lzo
verb 3
log openvpn.log
```

FreeRADIUS

- 程式預設目錄
  - /etc/raddb

- 基本需要設定的檔案
  - radiusd.conf ← FreeRADIUS的基本設定
  - proxy.conf ← 將認證資訊轉送至設定的位置
  - clients.conf ← 設定允許接收認證資訊的來源
  - eap.conf ← 驗證相關設定
  - users ← 帳號相關設定
  - sites-available/default ← 模組的相關設定
  - sites-available/inner-tunnel ← 類似virtual server的相關設定

FreeRADIUS



- proxy.conf
- clients.conf
- users
- eap.conf
- sites-available/default
  - 使用的模組設定檔
- sites-available/inner-tunnel
  - 使用的模組設定檔
- …

FreeRADIUS

- 啟動freeradius服務
  - service radiusd start

- 設定開機自動啟動
  - chkconfig radiusd on

FreeRADIUS

- radiusd.conf

```
<略>

listen {
  type = auth
  ipaddr = *
  port = 0  ← 預設為1812，舊的版本為1645
}

listen {
  ipaddr = *
  port = 0  ← 預設為1813，舊的版本為1646
  type = acct
}

<略>
```

FreeRADIUS

- proxy.conf

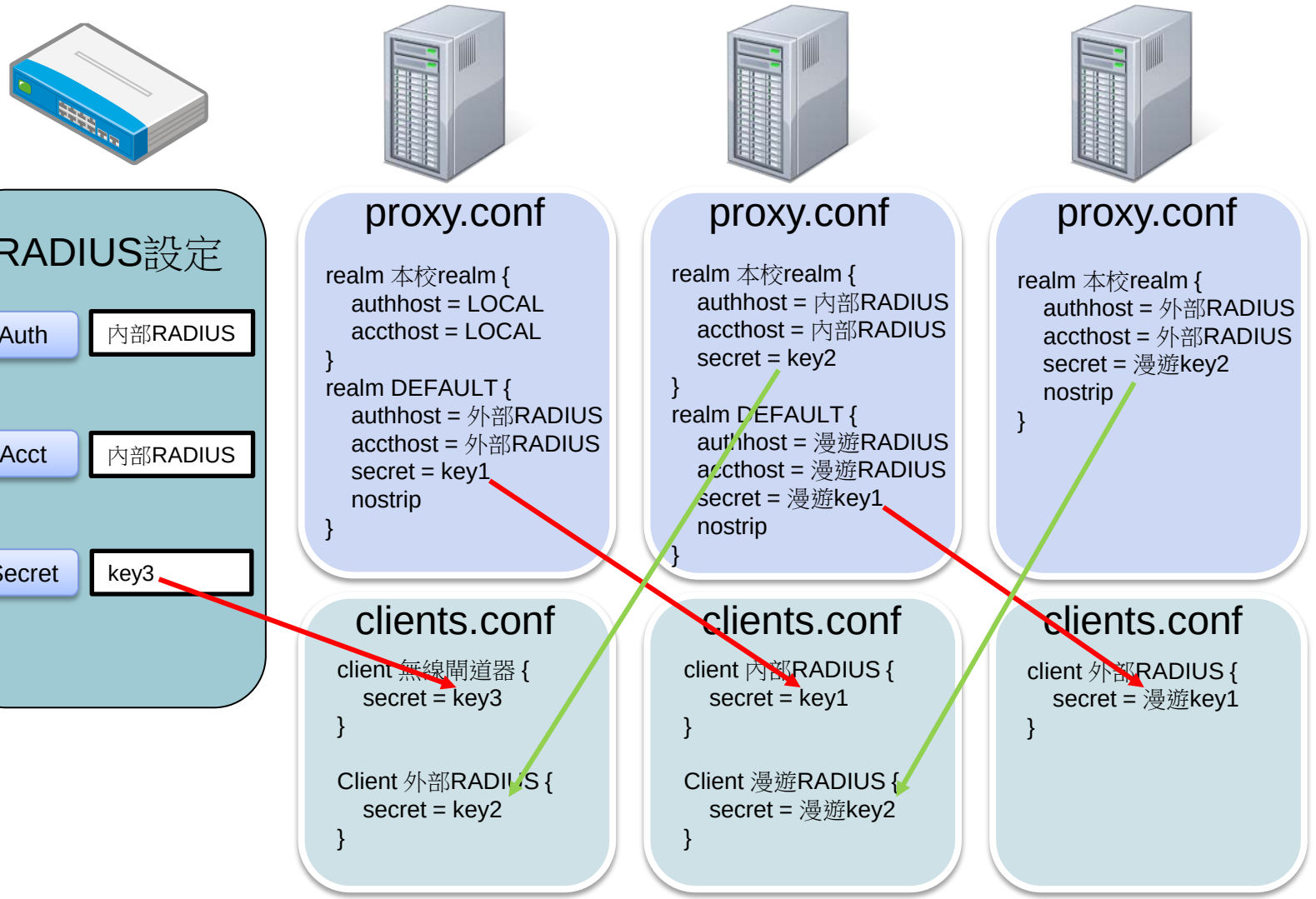
```
# 當遇到帳號並沒有 realm 時的預設動作
realm NULL {
        authhost = LOCAL
        accthost = LOCAL
        secret = 本 RADIUS 主機使用的金鑰字串
}
# 當遇到帳號帶的 realm 是 test.niu.edu.tw 時將認證資訊導至內部認證主機
# 預設情況下，會將realm移除，可以加nostrip不移除
realm test.niu.edu.tw {
        authhost = 宜蘭大學的內部漫遊主機:1812
        accthost = 宜蘭大學的內部漫遊主機:1813
        secret = 宜蘭大學內部使用的金鑰字串
}
# 當遇到帳號有帶 realm 且非 test.niu.edu.tw 時的預設動作，將認證資訊導給漫遊中心
# 且使用nostrip不把realm移除
realm DEFAULT {
        authhost = 漫遊中心 RADIUS 主機 IP:1812
        accthost = 漫遊中心 RADIUS 主機 IP :1813
        secret = 漫遊使用的金鑰字串
        nostrip
}
```

FreeRADIUS

- clients.conf

```
# 本機預設的設定檔
client localhost {
  ipaddr = 127.0.0.1
  netmask = 32
  secret = testing123
  shortname = localhost
  nastype = other
}
# 假設漫遊中心 RADIUS 主機的 IP 是 10.1.0.7
client 10.1.0.7 {
  secret = 漫遊使用的金鑰字串
  shortname = RoamingCenter
}
# 假設宜蘭大學的內部漫遊主機 IP 是 123.123.123.123
client 123.123.123.123 {
  secret = 宜蘭大學內部使用的金鑰字串
  shortname = InsideServer
}
# 假設要允許某一段網路可以進行存取
client 192.168.0.0/24 {
  secret = 內部使用的金鑰字串
  shortname = 內部的應用程式群
}
```

FreeRADIUS


無線閘道器
內部RADIUS
外部RADIUS
漫遊RADIUS
RADIUS設定
Auth
內部RADIUS
Acct
內部RADIUS
Secret
key3
proxy.conf
realm 本校realm {
authhost = LOCAL
accthost = LOCAL
}
realm DEFAULT {
authhost = 外部RADIUS
accthost = 外部RADIUS
secret = key1
nostrip
}
proxy.conf
realm 本校realm {
authhost = 內部RADIUS
accthost = 內部RADIUS
secret = key2
}
realm DEFAULT {
authhost = 漫遊RADIUS
accthost = 漫遊RADIUS
secret = 漫遊key1
nostrip
}
proxy.conf
realm 本校realm {
authhost = 外部RADIUS
accthost = 外部RADIUS
secret = 漫遊key2
nostrip
}
clients.conf
client 無線閘道器 {
secret = key3
}
Client 外部RADIUS {
secret = key2
}
clients.conf
client 內部RADIUS {
secret = key1
}
Client 漫遊RADIUS {
secret = 漫遊key2
}
clients.conf
client 外部RADIUS {
secret = 漫遊key1
}

FreeRADIUS

- 建立本機測試帳號
  - 修改 users 檔案，增加測試帳號 test-account

    “test-account” Cleartext-Password := “test-password”
  - 增加回應訊息

    “test-account” Cleartext-Password := “test-password”

    Reply-Message = "Hello, %{User-Name}"

```
[root@localhost ~]# radtest test-account test-password 127.0.0.1 0 testing123
Sending Access-Request of id 161 to 127.0.0.1 port 1812
        User-Name = "test-account"
        User-Password = "test-password"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=161, length=41
        Reply-Message = "Hello, test-account"
```

FreeRADIUS

- 搭配 MySQL 使用
  - 安裝MySQL套件
    - yum install freeradius-mysql
  - 創建 RADIUS 資料庫
  - 匯入 RADIUS Schema
    - sql/mysql/schema.sql
    - sql/mysql/nas.sql
    - sql/mysql/ippool.sql
    - sql/mysql/wimax.sql
  - 創建 FreeRADIUS 使用的帳號、密碼、權限

FreeRADIUS

– 修改 sql.conf

```
sql {
    database = "mysql"
    driver = "rlm_sql_${database}"
    server = "資料庫位址"
    port = 3306
    login = "帳號"
    password = "密碼"
    radius_db = "radius"
    <略>
    authcheck_table = "radcheck"
    authreply_table = "radreply"
    <略>
    readclients = yes
    nas_table = "nas"
    <略>
}
```

⇦ 取代檔案 users 的設定

⇦ 取代檔案 clients.conf 的設定

FreeRADIUS

- 修改 radiusd.conf
  - 針對使用 sql 的部分取消註解
- 修改 sites-available/default
  - 針對使用 file 的部分加以註解
  - 針對使用 sql 的部分取消註解
- 修改 sites-available/inner-tunnel
  - 針對使用 file 的部分加以註解
  - 針對使用 sql 的部分取消註解
- 影響
  - users ➔ authcheck_table
  - clients.conf ➔ nas_table

FreeRADIUS

- 搭配LDAP使用
  - 安裝LDAP套件
    - yum install freeradius-ldap
  - 修改 sites-available/default
    - 取消對使用 ldap 的註解
  - 修改 sites-available/inner-tunnel
    - 取消對使用 ldap 的註解

FreeRADIUS

– 修改 modules/ldap

```
ldap {
  server = "LDAP IP Address"
  #identity = "cn=admin,o=My Org,c=UA"
  #password = mypass
  basedn = "dc=niu,dc=edu,dc=tw"
```

– LDAP相對應的ACL規則設計需要修正

偵錯程序

測試指令

- 測試服務是否正常

```
[root@Radius ~]# service radiusd status
radiusd (pid  32627) 正在執行...

[root@Radius ~]# service openvpn status
Status written to /var/log/messages
```

測試指令

- 檢查openvpn是否正常取得IP

```
[root@Radius ~]# ifconfig
tun0   Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
       inet addr:10.1.0.9  P-t-P:10.1.0.2  Mask:255.255.255.255
       UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
       RX packets:14994863 errors:0 dropped:0 overruns:0 frame:0
       TX packets:13623795 errors:0 dropped:4063 overruns:0 carrier:0
       collisions:0 txqueuelen:100
       RX bytes:88956905 (84.8 MiB)  TX bytes:2563944855 (2.3 GiB)
```

測試指令

- radtest [帳號] [密碼] [認證位址:認證埠] [NAS port] [secret key]
- 測試本機 RADIUS 服務是否正常

```
[root@Radius ~]# radtest 帳號 密碼 localhost 0 testing123
Sending Access-Request of id 128 to localhost port 1812
        User-Name = “帳號"
        User-Password = “密碼"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host localhost port 1812, id=128, length=20
```

- 測試至其它主機 RADIUS 服務是否正常

```
[root@Radius ~]# radtest 帳號 密碼 伺服器IP 0 金鑰字串
Sending Access-Request of id 128 to 伺服器IP port 1812
        User-Name = “帳號"
        User-Password = “密碼"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 伺服器IP port 1812, id=128, length=20
```

除錯模式

- 使用 FreeRADIUS 除錯模式查詢錯誤資訊
  - radiusd -X

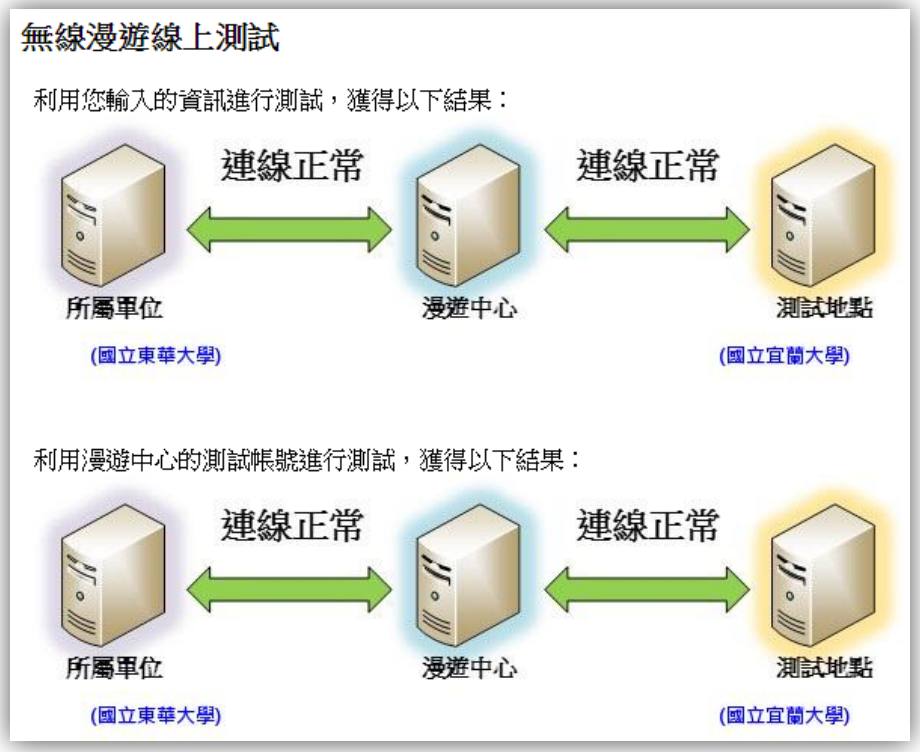
```
< 略 >
radiusd: #### Opening IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
}
listen {
        type = "control"
 listen {
        socket = "/var/run/radiusd/radiusd.sock"
 }
}
listen {
        type = "auth"
        ipaddr = 127.0.0.1
        port = 18120
}
 ... adding new socket proxy address * port 59086
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /var/run/radiusd/radiusd.sock
Listening on authentication address 127.0.0.1 port 18120 as server
inner-tunnel
Listening on proxy address * port 1814
Ready to process requests.
```

日誌分析

- OpenVPN 日誌位置
  - 程式目錄 / openvpn.log
- FreeRADIUS 日誌位置
  - /var/log/radius/radius.log
  - /var/log/radius/radacct/{clients ip}/detail-{年月日}

線上測試

- 漫遊現況 → 無線漫遊線上測試



流量統計

- 計算方式
  - 連線人數
  - 連線次數
- 狀態
  - 紅燈
  - 綠燈
  - 黃燈

常見問題

常見問題

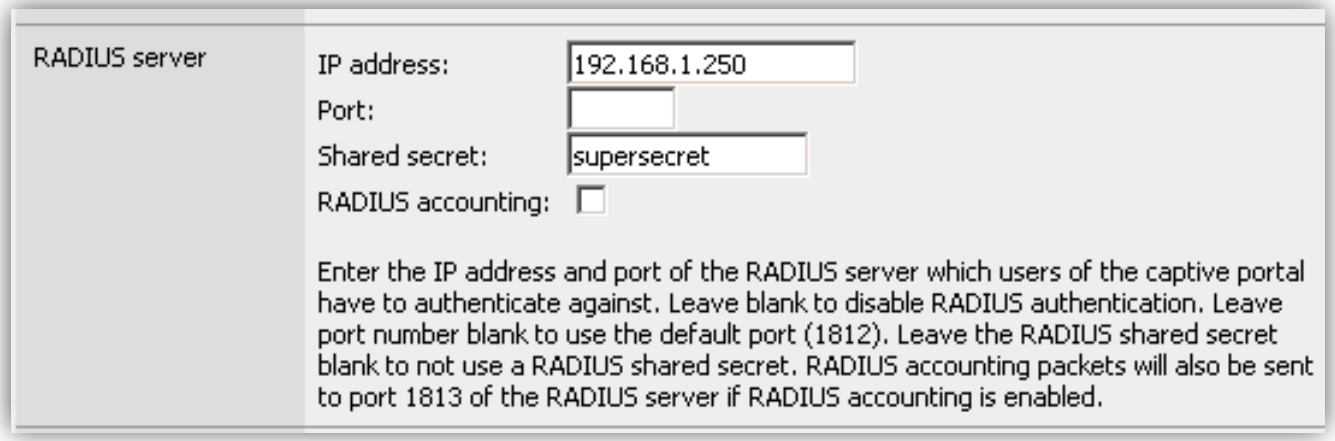
- OpenVPN 無法連線成功
  - 防火牆設定
  - OpenVPN版本過舊
- FreeRADIUS 無法漫遊成功
  - 防火牆設定
- FreeRADIUS 無法順利啟動
  - clients.conf 設定IP出現重覆
  - proxy.conf 設定 realm 出現重複
  - secret 設定錯誤

常見問題

- 認證伺服器不支援RADIUS
  - 查詢支援的外部認證模式，將 FreeRADIUS 安裝套件
- 無線閘道器不支援傳送 Account 封包
  - 更換設備
  - 使用軟體防火牆

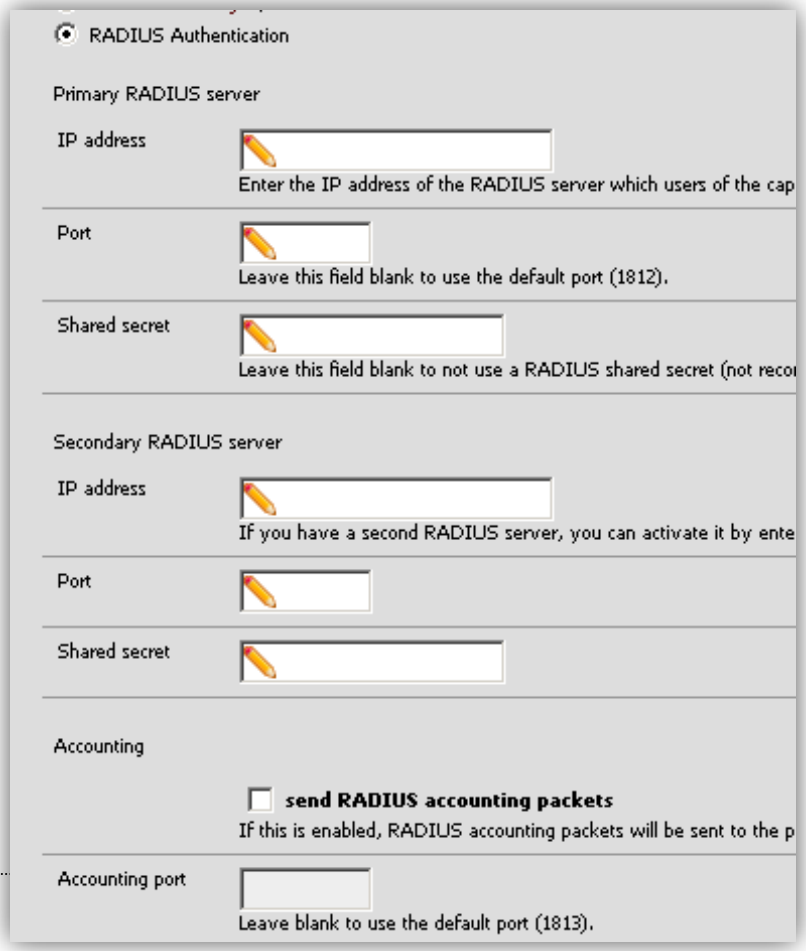
無線網路閘道器

- m0m0wall
  - http://m0n0.ch/wall/
  - 一個完整的嵌入式軟體防火牆
  - 支援 RADIUS Accounting



無線網路閘道器

- pfSense
  - https://www.pfsense.org/
  - 以m0m0wall 為基礎，且具有套件擴充功能的軟體防火牆
  - 支援多線路負載平衡功能
  - 支援 RADIUS Accounting



相關應用

相關應用

- 有線網路存取使用控制
  - 802.1x 架構
  - 需網路設備支援
  - 部分系統需針對有線網路啟用認證機制

- OpenVPN 與 FreeRADIUS 搭配使用
  - 使用 FreeRADIUS 進行驗證，獲得權限使用VPN
  - 安裝 FreeRADIUS 支援 OpenVPN 的套件

相關應用

- 網頁存取認證
  - Apache 安裝支援 RADIUS 的套件
    - mod_auth_radius
    - mod_auth_xradius
  - 設定 RADIUS 相關對應資訊
  - 使用 RADIUS 對使用者進行認證

謝謝您的聆聽與指教

Q&A

聯繫資訊

TANet 無線網路漫遊中心聯繫窗口
電話:(03)931-2047
信箱:pclee@niu.edu.tw
yclu@niu.edu.tw