Wireless Authentication, Authorization and Accounting

Speaker: Chia-Peng Lee

Date: 2019/3/20

MOBILE COMMUNICATIONS NETWORKING Lab, NTU

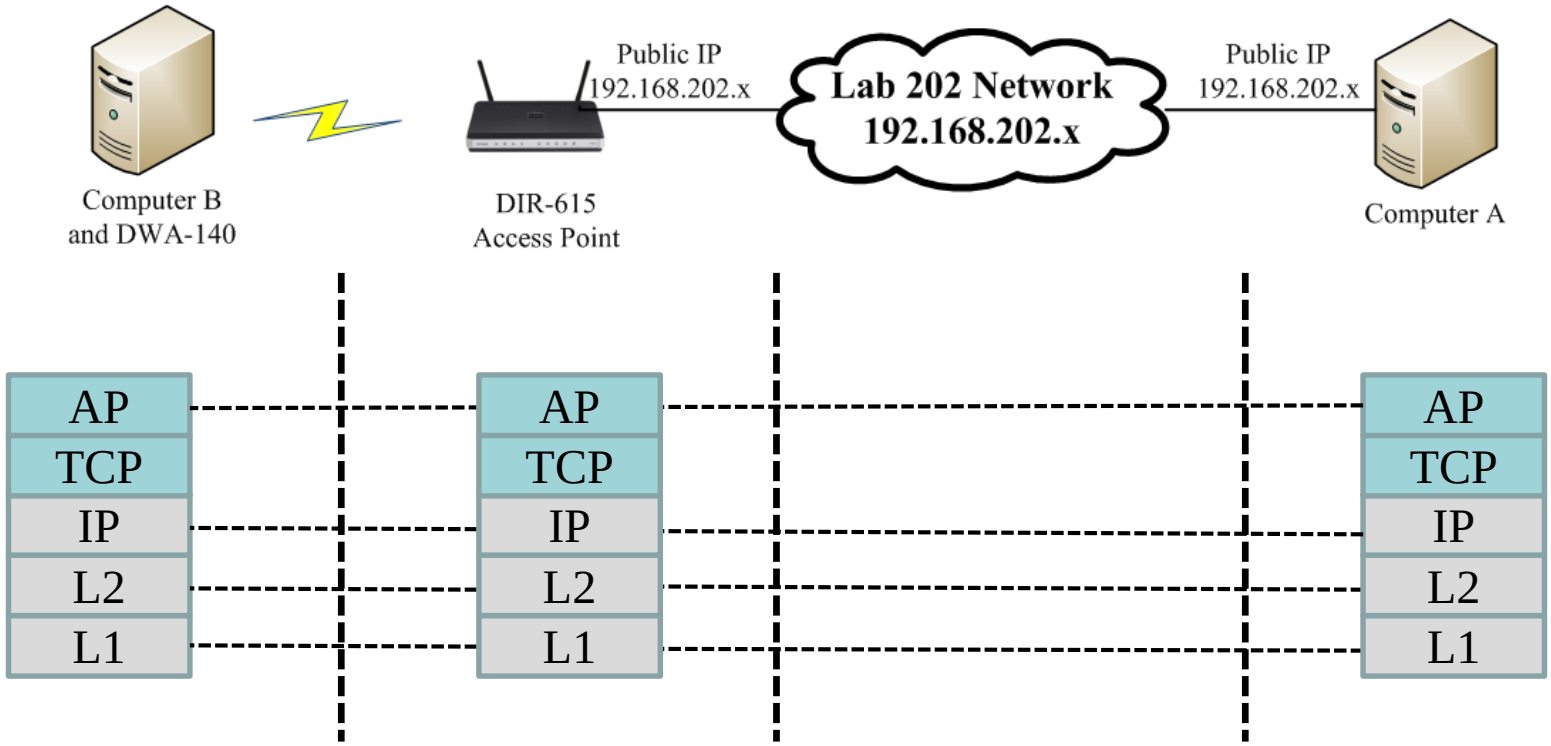
注意事項

- 實驗(二)上機實驗時間 (@ R204)
  - 時間: 2019/3/27 14:20~17:10
- 實驗(二)展演及實驗結報繳交 (@ R204)
  - 時間: 2019/4/10 14:20~17:20
  - 實驗結報繳交方式:
    - 一律使用電子郵件繳交電子檔 (一組只要繳交一份)，
    - 郵件主旨範例如 [CNL實驗(二)結報繳交_組別], 最晚當天繳交完畢。
- 下次上課 (@ R204)
  - 時間: 2019/4/24 14:20~17:10

實驗說明

- 設計一無線區域網路使用者認證機制，可供使用者認證之用，並且統計每個使用者使用此無線區域網路之流量與時間，進以實作流量控管與流量監測。同時也要為這兩項功能寫個供管理者控管及供使用者操作的網頁介面。
- 本次實驗完成下列事項
  - 完成WLAN認證功能
  - 撰寫一個網頁管理介面完成下列功能
    - 流量監測
    - 流量控管
    - 使用者註冊、登入與登出

實驗環境網路架構


Public IP
192.168.202.x
Lab 202 Network
192.168.202.x
Public IP
192.168.202.x
Computer B
and DWA-140
DIR-615
Access Point
Computer A
AP
TCP
IP
L2
L1
AP
TCP
IP
L2
L1
AP
TCP
IP
L2
L1

實驗環境軟體安裝

- 電腦A
  - Apache server
  - RADIUS server
  - MySQL server
- 電腦B (NoteBook)
  - NoteBook
  - PC with wireless card
- 無線基地台
  - DD-WRT
  - ChilliSpot
- 作業系統
  - Ubuntu 16.04.3

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- 安裝LAMP Server (Linux-Apache-MySQL-PHP Server)
  - sudo apt-get install tasksel
  - sudo apt-get update
  - sudo tasksel install lamp-server
- 安裝PHPMyAdmin
  - sudo apt-get install phpmyadmin
- 將PHPMyAdmin的設定檔放到Apache Server中
  - sudo cp /etc/phpmyadmin/apache.conf /etc/apache2/conf.d
- 重啟Apache Server
  - sudo /etc/init.d/apache2 restart
- 瀏覽器測試PHPMyAdmin
  - http://localhost/phpmyadmin

#2019/03/19新增: 若ubuntu版本為16.04.4，此時會出現404 Not Found. 解決方法如下:
1. sudo gedit /etc/apache2/apache2.conf
2. 在最後一行加入: Include /etc/phpmyadmin/apache.conf
3. sudo /etc/init.d/apache2 restart

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- 啟用Apache的SSL功能
  - sudo a2enmod ssl
  - sudo a2ensite default-ssl
  - sudo /etc/init.d/apache2 restart
- 安裝Freeradius
  - sudo apt-get install freeradius
- 安裝Freeradius的MySQL模組
  - sudo apt-get install freeradius-mysql
  - sudo /etc/init.d/freeradius restart

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- 修改Ubuntu中localhost的hotsname混淆問題
  - sudo vim /etc/hosts
  - # ::1 localhost ip6-localhost ip6-loopback (註解)
- 在MySQL中新增radius資料庫
  - mysql –u root –p
  - create database radius;
  - 或者用phpmyadmin新增。

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- 匯入RADIUS資料庫架構到Mysql
  - su root –切換到root
  - cd /etc/freeradius/sql/mysql/
  - mysql -u root -p radius < ippool.sql
  - mysql -u root -p radius < schema.sql
  - mysql -u root -p radius < nas.sql
  - mysql -u root -p radius < admin.sql
    - admin.sql 匯入的話會幫你建立一個 “radius@localhost”的管理者帳號，但是必須修改privilege與密碼。

	帳號	主機名稱	型態	權限	允許授權	動作
☐	debian-sys-maint	localhost	全域	ALL PRIVILEGES	是	編輯權限
☐	radius	localhost	指定資料庫	SELECT	否	編輯權限
☐	root	localhost	全域	ALL PRIVILEGES	是	編輯權限

-->

	帳號	主機名稱	型態	權限	允許授權	動作
☐	debian-sys-maint	localhost	全域	ALL PRIVILEGES	是	編輯權限
☐	radius	localhost	指定資料庫	ALL PRIVILEGES	是	編輯權限
☐	root	localhost	全域	ALL PRIVILEGES	是	編輯權限

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- 修改FreeRADIUS設定，從MySQL讀取使用者帳密
  - su root – 在freeradius資料夾下修改設定要有root的權限。
  - gedit /etc/freeradius/sites-enabled/default
  - 取消 sql 的註解

In the authorize{} module

```
#
#  Look in an SQL database.  The schema of the database
#  is meant to mirror the "users" file.
#
#  See "Authorization Queries" in sql.conf
sql
```

In the accounting{} module

```
#
#  Log traffic to an SQL database.
#
#  See "Accounting queries" in sql.conf
sql
```

Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

In the session{} module

```
session {
        radutmp

        #
        #  See "Simultaneous Use Checking Queries" in sql.conf
        sql
}
```

In the post-auth{} module

```
        #
        #  After authenticating the user, do another SQL query.
        #
        #  See "Authentication Logging Queries" in sql.conf
        sql
```

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- gedit /etc/freeradius/radiusd.conf
- 設定 radius server聽取的埠 (認證埠1812，計量埠1813)

The port for radius server to listen for authentication request is 1812

```
#  Port on which to listen.
#  Allowed values are:
#        integer port number (1812)
#        0 means "use /etc/services for the proper port"
port = 1812
```

Port for accounting is 1813

```
#  This second "listen" section is for listening on the accounting
#  port, too.
#
listen {
        ipaddr = *
#       ipv6addr = ::
        port = 1813
        type = acct
#       interface = eth0
#       clients = per_socket_clients
}
```

Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- gedit /etc/freeradius/radiusd.conf

In the module modules{}

```
        #  Include another file that has the SQL-related configuration.
        #  This is another file only because it tends to be big.
        #
        $INCLUDE sql.conf
```

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- 設定Log資訊

Some settings for logging username, password, etc

```
#  Log the full User-Name attribute, as it was found in the request.
#
# allowed values: {no, yes}
#
stripped_names = yes

#  Log authentication requests to the log file.
#
#  allowed values: {no, yes}
#
auth = yes

#  Log passwords with the authentication requests.
#  auth_badpass  - logs password if it's rejected
#  auth_goodpass - logs password if it's correct
#
#  allowed values: {no, yes}
#
auth_badpass = yes
auth_goodpass = no
```

Copyright owned by NTU MCN Lab. 2015

實驗環境架設
Chillispot + FreeRADIUS + MySQL + Apache

- gedit /etc/freeradius/sql.conf

```
sql {
        #
        #  Set the database to one of:
        #
        #       mysql, mssql, oracle, postgresql
        #
        database = "mysql"

        #
        #  Which FreeRADIUS driver to use.
        #
        driver = "rlm_sql_${database}"

        # Connection info:
        server = "localhost"
        #port = 3306
        login = "radius"
        password = "setupRADIUS"

        # Database table configuration for everyt
        radius_db = "radius"
```

與Mysql的帳密相同

存放User帳密的DataBase

Check the setting that allow FreeRADIUS to read Radius Clients from database

```
# Set to 'yes' to read radius clients from the database ('nas' table)
# Clients will ONLY be read on server startup.  For performance
# and security reasons, finding clients via SQL queries CANNOT
# be done "live" while the server is running.
#
readclients = yes
```

Copyright owned by NTU MCN Lab. 2015

實驗環境架設
Chillispot + FreeRADIUS + MySQL + Apache

- 設定允許連到RADIUS Server的使用者
  - gedit /etc/freeradius/clients.conf

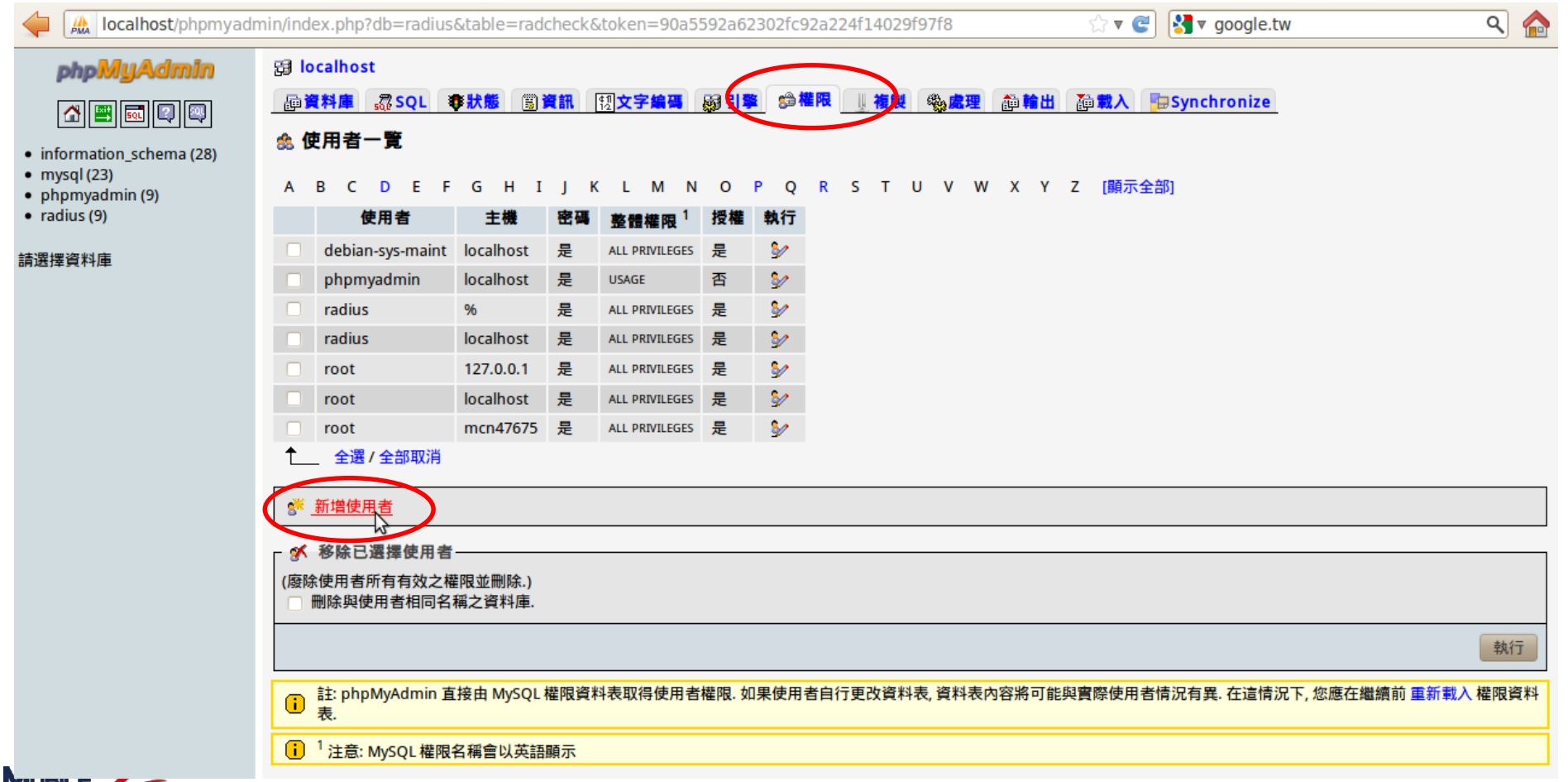
```
client 192.168.202.0/24{        (要包含AP的網路位址)
        secret = (自己的密鑰)
}
```

- 新增RADIUS使用者帳密 (利用PHPMyadmin)
  - 建立MySQL使用者”radius”並允許所有權限
  - 建立DataBase “radius”
  - 新增RADIUS使用者帳密

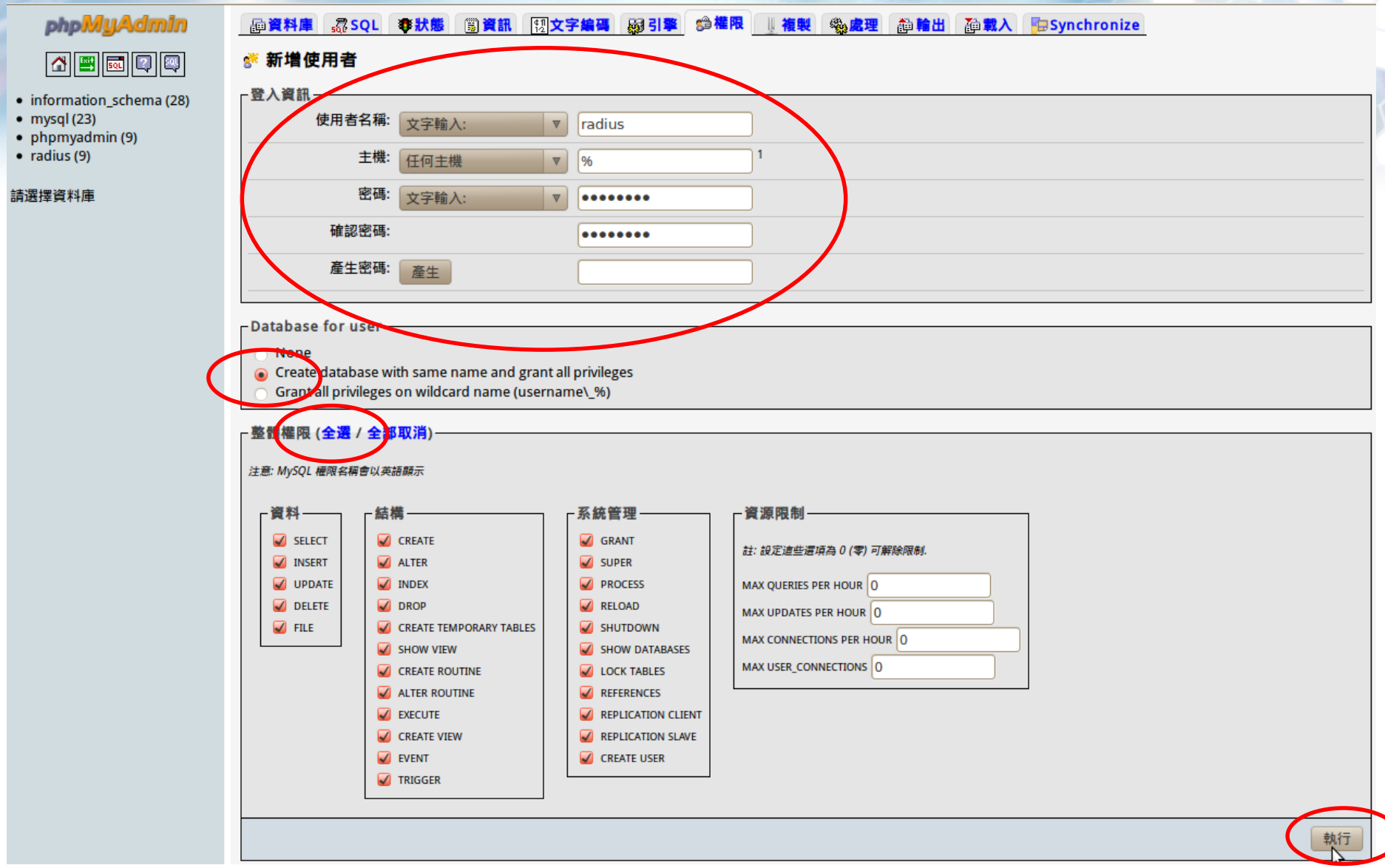
Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache



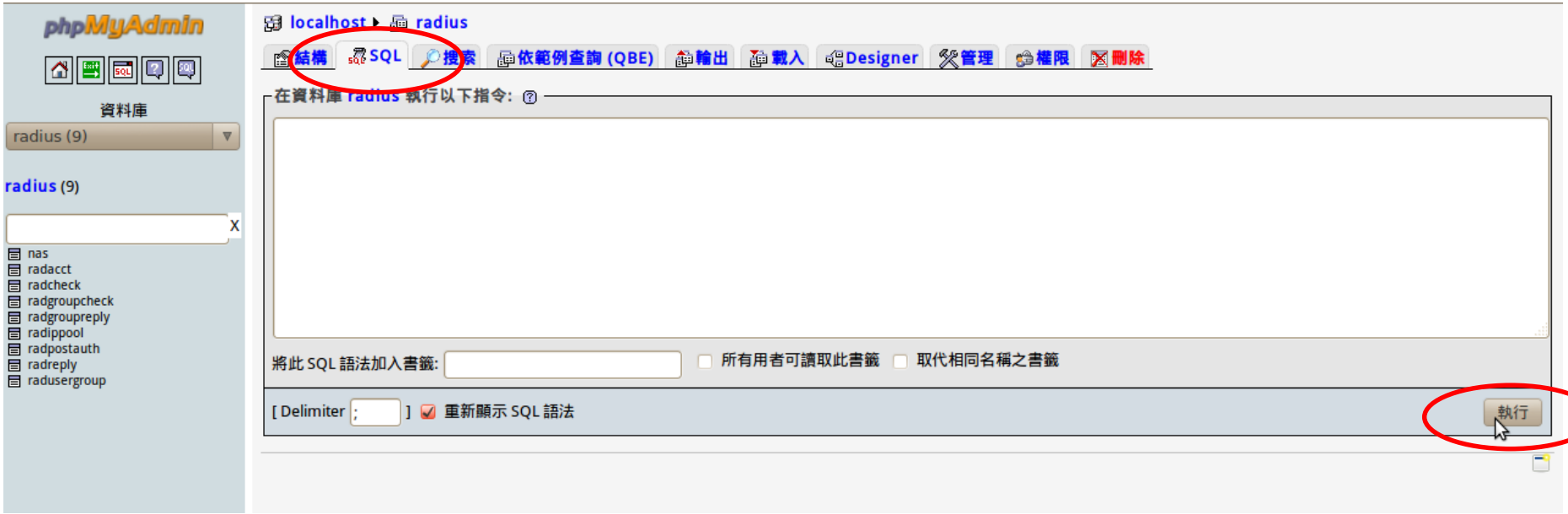
Copyright owned by NTU MCN Lab. 2015



Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache



Copyright owned by NTU MCN Lab. 2015

實驗環境架設
Chillispot + FreeRADIUS + MySQL + Apache

- 首先加入群組資料
  - insert into radgroupreply (groupname,attribute,op,value) values ('user','Auth-Type',':=','CHAP');
  - insert into radgroupreply (groupname,attribute,op,value) values ('user','Service-Type',':=','Framed-User');
- 接著加入測試帳號"ta"
  - insert into radcheck (username,attribute,op,value) values ('ta', 'Cleartext-Password',':=','tatest');
- 最後把帳號加入前面做的群組
  - insert into radusergroup (username,groupname) values ('ta','user');

Mobile Communications Networking Lab, NTU
Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- 之後要加使用者可以透過下面SQL來增加
  - insert into radcheck (username,attribute,op,value) values ('帳號','User-Password',':=','密碼');
  - insert into radusergroup (username,groupname) values ('帳號','user');
- 測試Freeradius
  - radtest ta tatest localhost 1 testing123
  - 成功會顯示request accept

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

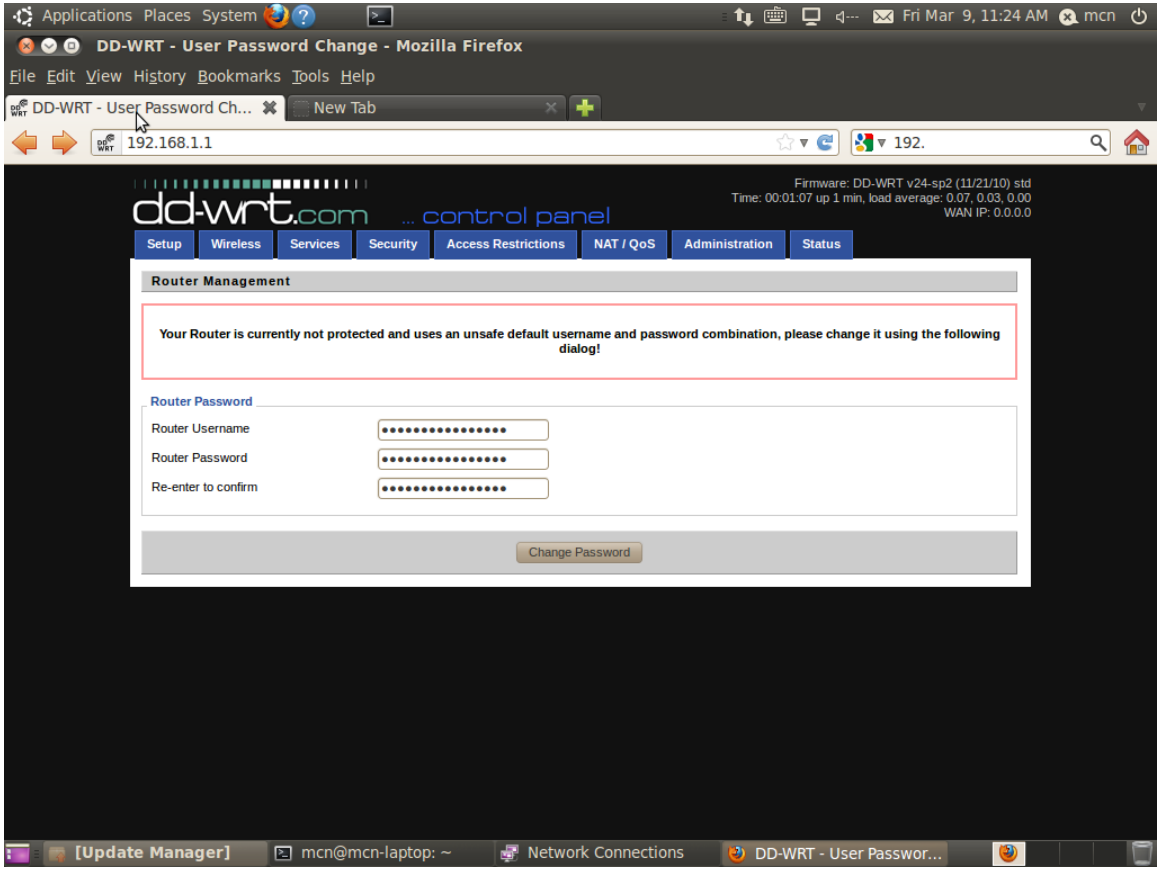
- Freeradius
  - sudo /etc/init.d/freeradius start　　開啟Freeradius
  - sudo /etc/init.d/freeradius stop　　停止Freeradius
  - sudo /etc/init.d/freeradius restart　　重啟Freeradius
- 開啟Freeradius Debug模式
  - sudo /etc/init.d/freeradius stop
  - sudo freeradius -X
- 查看Freeradius Log 檔
  - sudo tail -n 30 /var/log/freeradius/radius.log
  - sudo tail -n 30 /var/log/freeradius/radius.log | grep Error

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

AP設定
進入Web管理介面

- 將網路設定成DHCP或192.168.1.0/24網段。
- 打開瀏覽器輸入192.168.1.1 (DD-WRT與OpenWRT)或192.168.0.1 (D-Link)。



Copyright owned by NTU MCN Lab. 2015

AP設定
進入Web管理介面

- 啟動DD-WRT上的Chillispot服務
  - 進入DD-WRT管理頁面
  - Service -> Hostspot -> Chillispot -> enabled

注意此設定在WAN port是固定IP時有效，若WAN port是虛擬IP時，請將此設為 Disable

要修改成你的Radius server IP

你的Http server的hotspotlogin.php

你的radius server的client secret

與hotspotlogin.php中的uam secret一致

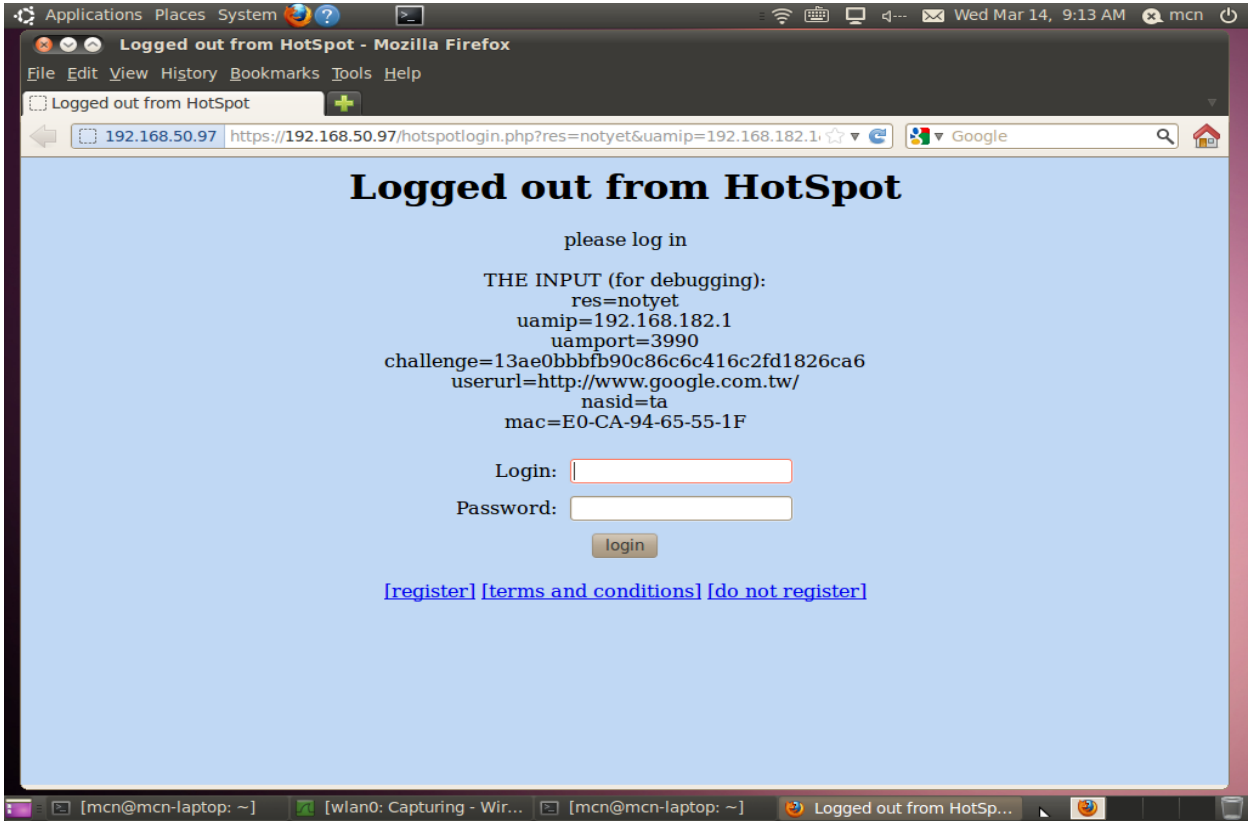
需要Https連線

Copyright owned by NTU MCN Lab. 2015

實驗環境架設

Chillispot + FreeRADIUS + MySQL + Apache

- 將hotspotlogin.php放到 /var/www/中 (10.04.04)
- 將hotspotlogin.php放到 /var/www/html/中 (16.04.4)
- 電腦B使用DHCP協定後開啟瀏覽器



實驗二展演要求

- 架設Chillispot + FreeRADIUS + MySQL + Apache。
  - 實作 Chillispot Redirect 功能(3%)
  - 架設 FreeRADIUS Server (10%)
  - 架設 MySQL server (3%)
  - 架設 Apache HTTP server (4%)
- 實作以下功能在Http server
  - 使用者註冊(3%)
  - 使用者登出(3%)
  - 顯示使用者流量與使用時間的功能(7%)
  - 根據不同的使用者限制流量與使用時間的功能(7%)
    - 超過時間或是超過流量，即時踢掉使用者
- 展示資料庫內容並說明各張 tables 負責的功能，請刪除不需要用到的 table (10%)。

Mobile Communications Networking Lab, NTU
Copyright owned by NTU MCN Lab. 2015

實驗二結報要求

- WLAN Authentication Mechanism (30%)
  1. 說明目前市面上對於無線區域網路所提出之認證機制其優缺點。
  2. 說明提出之認證機制的運作原理。
  3. 說明對於所提出之認證機制其漏洞預防措施為何。
- 網頁介面 (20%)
  1. 說明使用之web介面技術。
  2. 說明你們設計的網頁的運作方式。

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

已知問題

- 1. 含有https or http的網頁無法正確redirect to login webpage.
  - 這是由於伺服器Apache的SSL沒有正常運作，重新安裝SSL模組並重開Apache即可。
  - 或是可以利用下列網址進行轉址:
    - www.ntu.edu.tw

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

參考資料

- RADIUS Introduction
  - http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=1719
- FreeRADIUS + MySQL in Ubuntu 10.04
  - http://www.mydeveloperblog.com/linux-tutorial/radius/radius-servers-installation-guide-freeradius-ubuntu-mysql/
- Chillispot
  - http://www.chillispot.info/
  - http://www.howtoforge.com/ wifi_hotspot_setup
- Coovachilli
  - http://coova.org/CoovaChilli

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

參考資料

- How to build OpenWRT firmware
  - http://www.openwrt.org.cn/bbs/forum.php?mod=viewthread&tid=4217
- OpenWRT with DIR-615
  - http://wiki.openwrt.org/toh/d-link/dir-615
- DD-WRT
  - http://www.dd-wrt.com/site/index

Copyright owned by NTU MCN Lab. 2015

參考資料

- HTML基本教學
  - http://www.w3school.com.cn/html/index.asp
- PHP基本教學
  - http://tw.php.net/
  - http://php.vexp.idv.tw/
  - http://www.jollen.org/php/php_book.html
- PHP與MYSQL
  - http://www.php-mysql-tutorial.com/
- PHP Simple Login Tutorial
  - http://www.knowledgesutra.com/discuss/tlddl-php-simple-login-tutorial-learn-simple-login.html

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

AP韌體安裝
選擇DD-WRT版本

- 根據AP的版本選擇.bin檔
  - 助教的範例用DIR-615 E4版本，所以選 dir615e4-factory-to-ddwrt-firmware.bin
  - 到此下載 .bin 檔並選擇DIR-615 E4版本 http://www.dd-wrt.com/site/support/router-database
- DD-WRT DIR-615詳細解說
  - http://www.dd-wrt.com/wiki/index.php/D-Link_DIR-615_rev_E3

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

AP韌體安裝
DIR-615刷DD-WRT韌體

1. 助教測試使用Win7，瀏覽器為IE8，網路設定如下。
   - IP: 192.168.0.3
   - Netmask: 255.255.255.0
   - Gateway: 192.168.0.1

#若瀏覽器為IE11以上， 打開相容模式即可。

2. 將PC用網路線連接到AP的LAN埠。
3. 開啟AP的緊急模式 (30/30/30 reset) 。
   1. AP插上電源後壓住Reset鍵30秒不放。
   2. 拔掉電源線後繼續壓住Reset鍵30秒不放。
   3. 插上電源線後繼續押住Reset鍵30秒後放開。
   4. 電源燈會變成橘色閃爍，打開IE，在網址輸入192.168.0.1。

Mobile Communications Networking Lab, NTU

Copyright owned by NTU MCN Lab. 2015

AP韌體安裝
DIR-615刷DD-WRT韌體

4. 成功的話會有以下畫面，點選.bin檔。
   - 失敗的話請重複上一步

Copyright owned by NTU MCN Lab. 2015

AP韌體安裝
DIR-615刷DD-WRT韌體

5. 上傳韌體時請耐心等到電源燈由橘色變成綠色為止。
   - 上傳韌體時請不要拔除電源線。
6. 重開AP (拔掉電源線後再插入)
7. 開啟IE輸入192.168.1.1後會看到DD-WRT的管理頁面。

- 此方法適用於刷DD-WRT與原廠韌體。
  - DIR615E4_FW511B43.bin (原廠韌體)
  - dir615e4-factory-to-ddwrt-firmware.bin (DD-WRT)

Mobile Communications Networking Lab, NTU
Copyright owned by NTU MCN Lab. 2015

實驗環境架設
無線網卡

- 官網下載Linux的驅動程式
  - http://www.dlink.com/products/?tab=3.driver&pid=DWA-140&rev=DWA-140_revB
  - 解壓縮後裡面有一個壓縮檔 2010_0413_RT3070_Linux_STA_v2.1.3.0.zip
  - 解壓縮後進入資料夾
  - Make
  - Sudo make install
  - Sudo reboot

Copyright owned by NTU MCN Lab. 2015