利用MadWiFi實作WDS

彰化師大資工所

李宏杰

101.01.02

WDS

Q：什麼是WDS (Wireless Distribution System)？

A：WDS 就是一台AP(a)透過另一台AP(b)連到原來(a)所不能連到的地方。

一般的無線AP都號稱距離可達50-100公尺，但是會受到建築物的影響而有所減少，如果使用者位於超過AP的發射距離而連外只有一條ADSL又不想另外拉線，WDS就可以派上用場。

達成WDS的必要條件

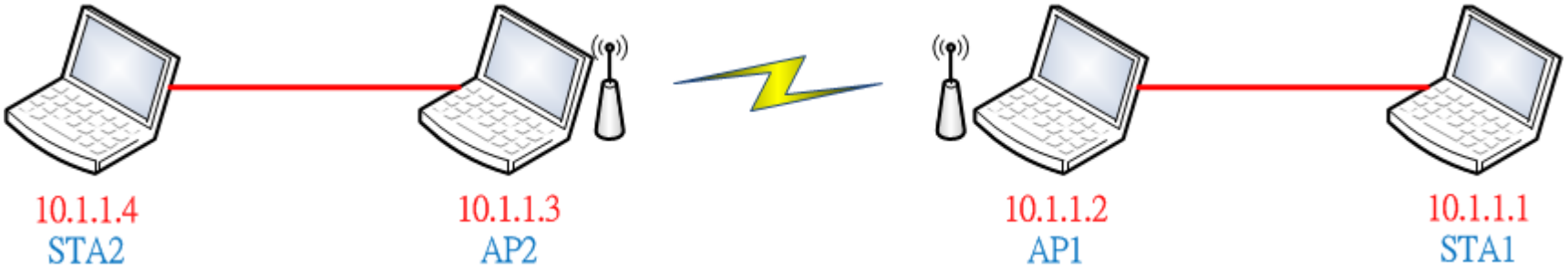
1. 兩個具有WDS功能的AP
2. 兩個AP的SSID要相同
3. 兩個AP使用的無線網路頻道必須相同
4. 兩個AP啟動WDS，並互設對方wireless MAC address
5. 兩個AP的安全機制必須相同

實驗環境

- **硬體：**
  (1)4台NB - Acer 4830TG * 1 - STA1
  Acer 4720 * 2 - AP1 & AP2
  Asus A8FM * 1 - STA2
  (2)2張D-Link DWL-G650無線網卡
- **作業系統：**
  Acer 4830TG(STA1) - Ubuntu 10.04
  Acer 4720(AP1) & (AP2) - Fedora core 6
  AP1 MAC：00:0f:3d:de:1d:d7
  AP2 MAC：00:0f:3d:de:1d:d0
  Asus A8FM(STA2) - WinXP(只是為了證明任何系統都可成功)

實驗目標

- 在WDS裡，橋接兩端的AP，藉由無線傳輸連接，即是從兩邊有線的乙太網路(802.3)，透過中間的無線傳輸(802.11)來進行溝通使得雙方能夠互ping。
- **實驗拓樸**



實際實驗拓樸

10.1.1.4 STA2

10.1.1.3 AP2

10.1.1.2 AP1

10.1.1.1 STA1

實作WDS

要安裝Bridge控制套件

如果一開始安裝時沒點選到此套件，

Fedora core 6光碟有

在->Fedora->RPMS->bridge-utils-1.1-2.i386(依你的系統版本而定，我是灌i386)

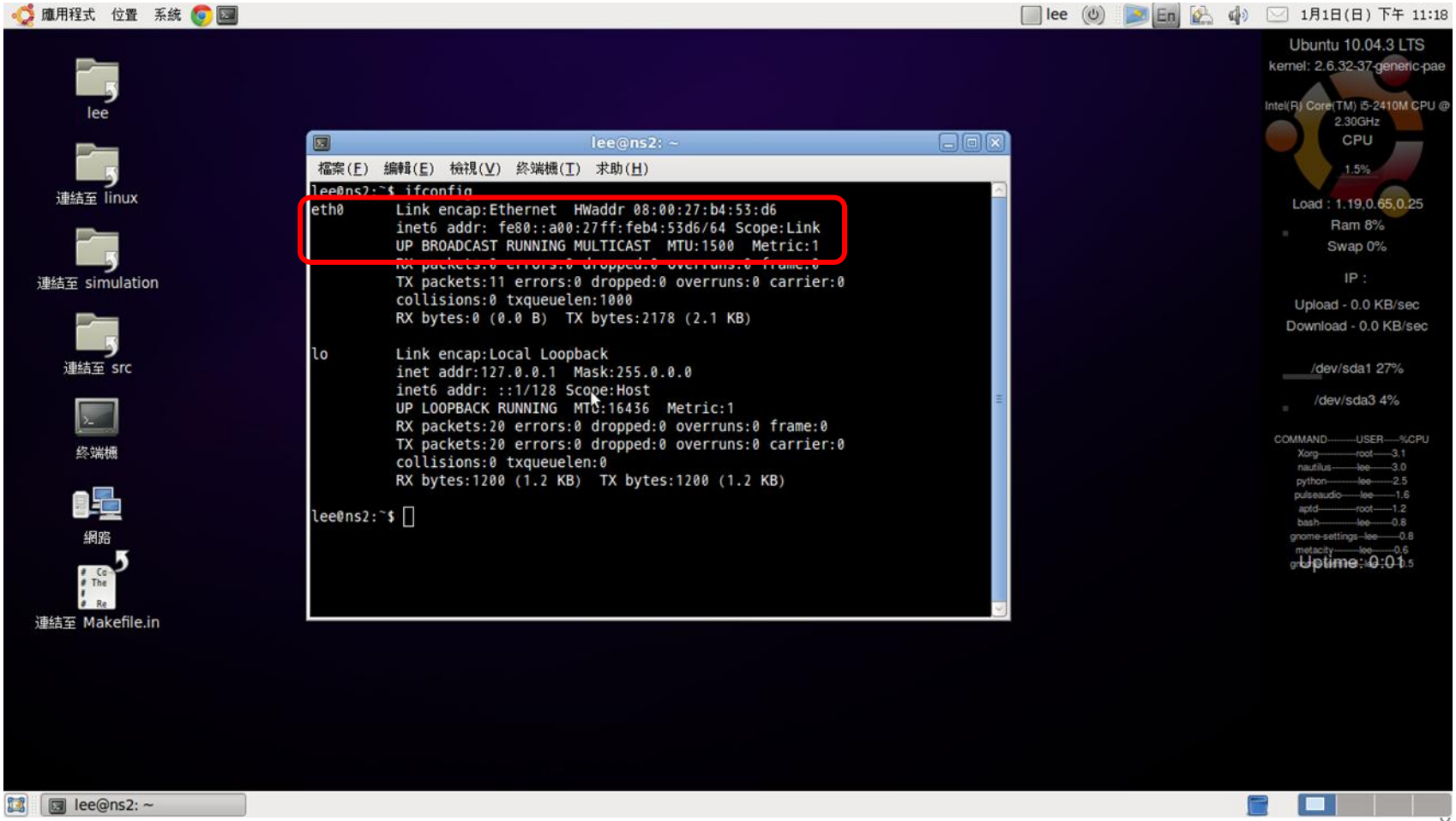
抓出來之後，執行安裝

#rpm -ivh bridge-utils-1.1-2.i386

必須安裝此套件才能使用brctl command

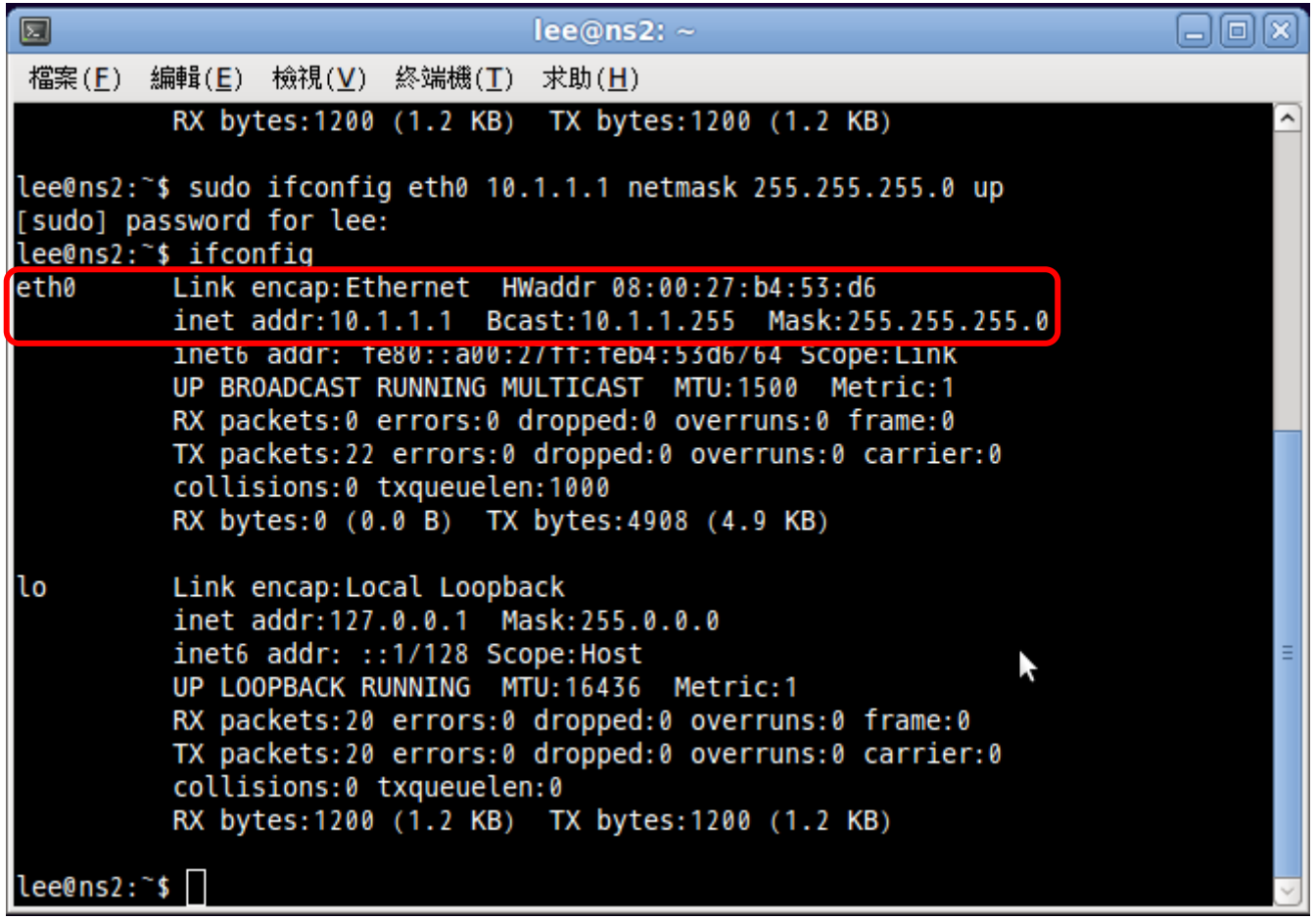
STA1的設定與運作情形

- 初始狀態，eth0無任何IP設定



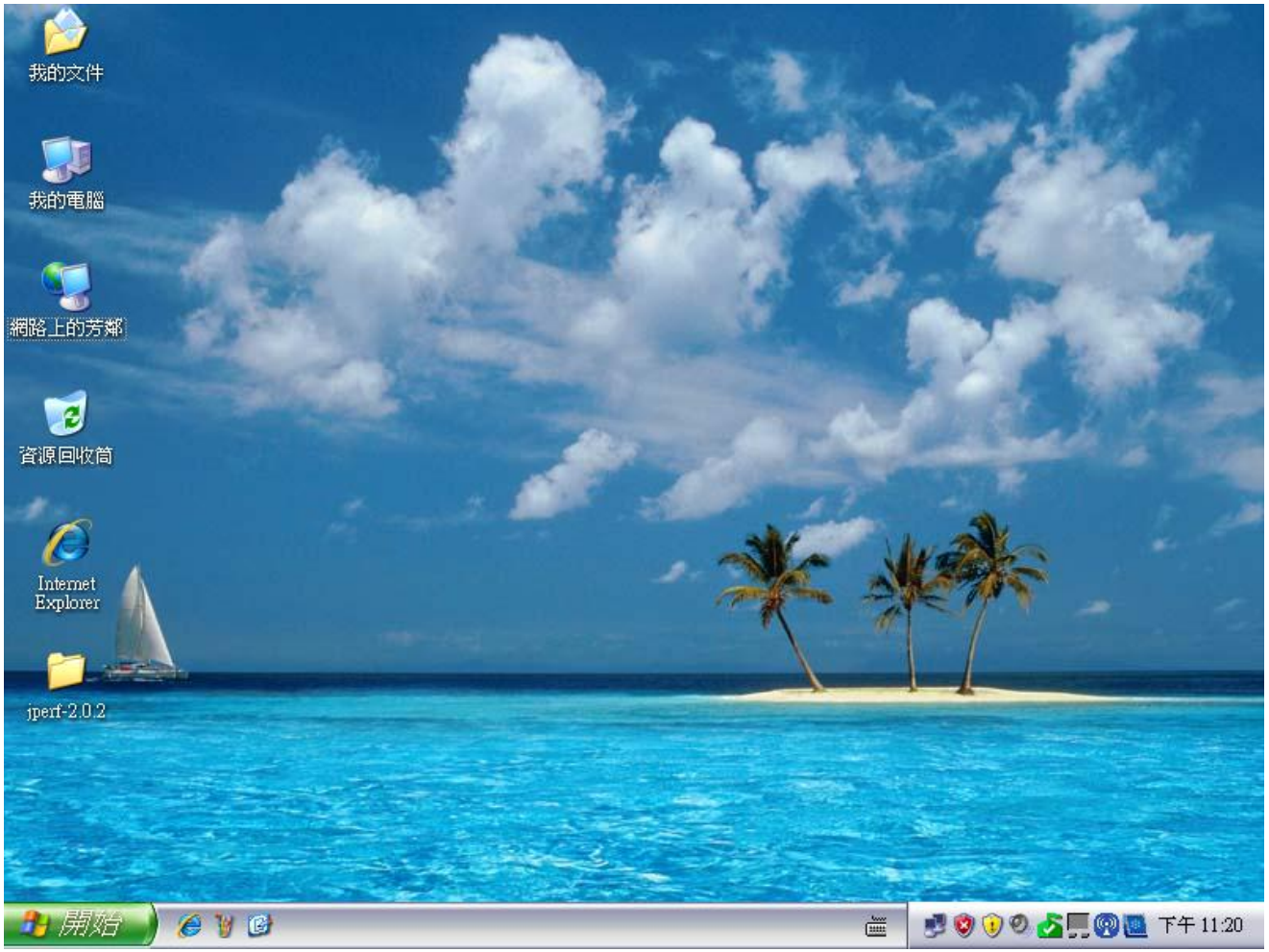
STA1的設定與運作情形

- #sudo ifconfig eth0 10.1.1.1 netmask 255.255.255.0 up



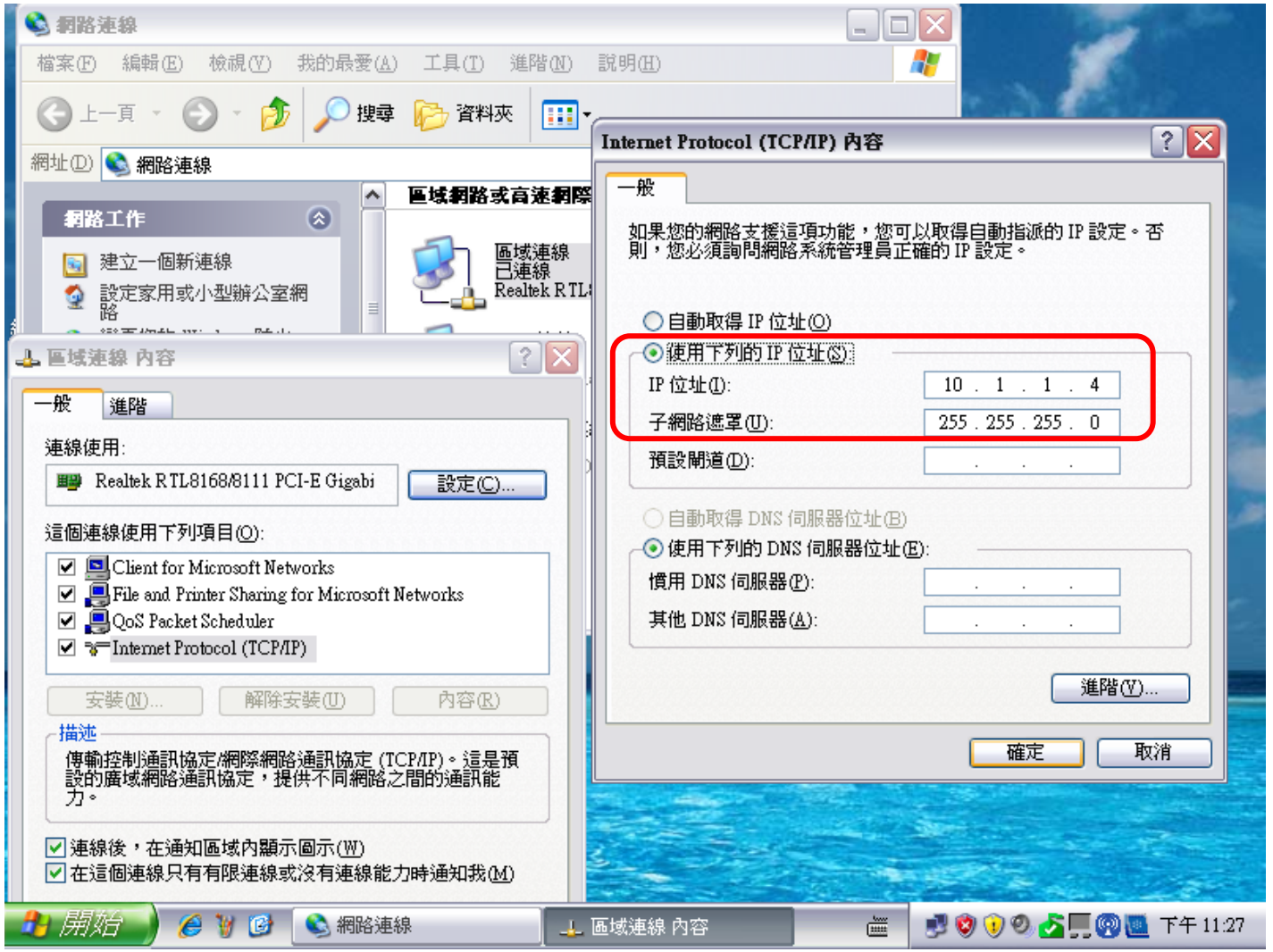
STA2的設定與運作情形

- 初始狀態



STA2的設定與運作情形

- 設定WinXP IP，想必大家都會



AP1的設定與運作情形(1/12)

編寫設定檔

```
#vim final_ap1.sh or #gedit final_ap1.sh
echo "br0 down “
ifconfig br0 down
sleep 3
echo "ath0 down “
ifconfig ath0 down
sleep 3
echo "wdsath0 down “
ifconfig wdsath0 down
sleep 3
echo "wlanconfig ath0 destroy “
wlanconfig ath0 destroy
sleep 3
echo "wlanconfig wdsath0 destroy “
```

AP1的設定與運作情形(2/12)

```
wlanconfig wdsath0 destroy
sleep 3
echo "delbr br0 “
brctl delbr br0
sleep 3
echo "rmmod -w ath_pci “
rmmod -w ath_pci
sleep 3
```

//以上為執行第二次以上才有作用，為device重置的意思，初次執行會無此裝置是沒關係的

#設定ath0無線相關設定

```
echo "modprobe ath_pci “
modprobe ath_pci
sleep 3
echo "wlanconfig ath0 destroy “
```

AP1的設定與運作情形(3/12)

```
wlanconfig ath0 destroy
sleep 3
echo "wlanconfig ath0 create wlandev wifi0 wlanmode ap “
wlanconfig ath0 create wlandev wifi0 wlanmode ap
sleep 3
echo "ifconfig ath0 down “
ifconfig ath0 down
sleep 3
echo "iwconfig ath0 essid honjie “
iwconfig ath0 essid honjie
sleep 3
echo "iwconfig ath0 channel 10 “
iwconfig ath0 channel 10
sleep 3
echo "wlanconfig wdsath0 create wlandev wifi0 wlanmode wds “
```

AP1的設定與運作情形(4/12)

```
wlanconfig wdsath0 create wlandev wifi0 wlanmode wds
sleep 3
echo "ifconfig wdsath0 down “
ifconfig wdsath0 down
sleep 3
echo "iwpriv wdsath0 wds_add 00:0f:3d:de:1d:d0 “
iwpriv wdsath0 wds_add 00:0f:3d:de:1d:d0
sleep 3
echo "iwpriv wdsath0 wds 1 “
iwpriv wdsath0 wds 1
sleep 3
echo "ifconfig ath0 0.0.0.0 up “
ifconfig ath0 0.0.0.0 up
sleep 3
echo "ifconfig wdsath0 0.0.0.0 up “
```

AP1的設定與運作情形(5/12)

```
ifconfig wdsath0 0.0.0.0 up
sleep 3
echo "ifconfig eth0 0.0.0.0 up “
ifconfig eth0 0.0.0.0 up
sleep 3
# 建立虛擬的br0—Bridge介面
echo "brctl addbr br0 “
brctl addbr br0
sleep 3
echo "brctl addif br0 ath0 “
brctl addif br0 ath0
sleep 3
echo "brctl addif br0 wdsath0 “
brctl addif br0 wdsath0
sleep 3
```

AP1的設定與運作情形(6/12)

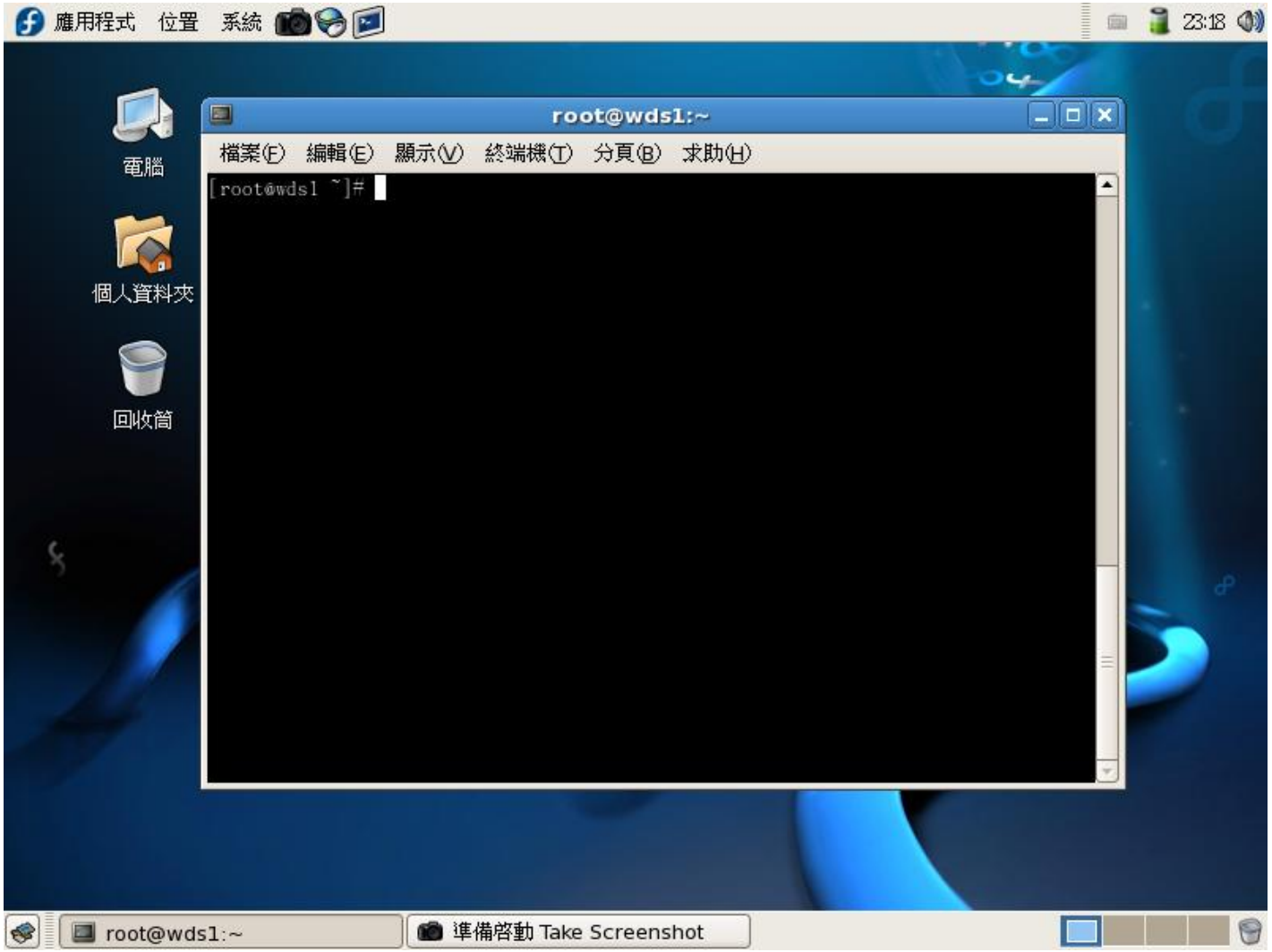
```
echo “brctl addif br0 eth0 “
brctl addif br0 eth0
sleep 3
echo "echo 1 > /proc/sys/net/ipv4/ip_forward “
echo 1 > /proc/sys/net/ipv4/ip_forward
sleep 3
#設定bridge的Network資訊，並將此bridge啟動
echo "ifconfig br0 10.1.1.2 netmask 255.255.255.0 up “
ifconfig br0 10.1.1.2 netmask 255.255.255.0 up
//以上WDS之相關設定與bridge橋接均完成
```

存檔並執行

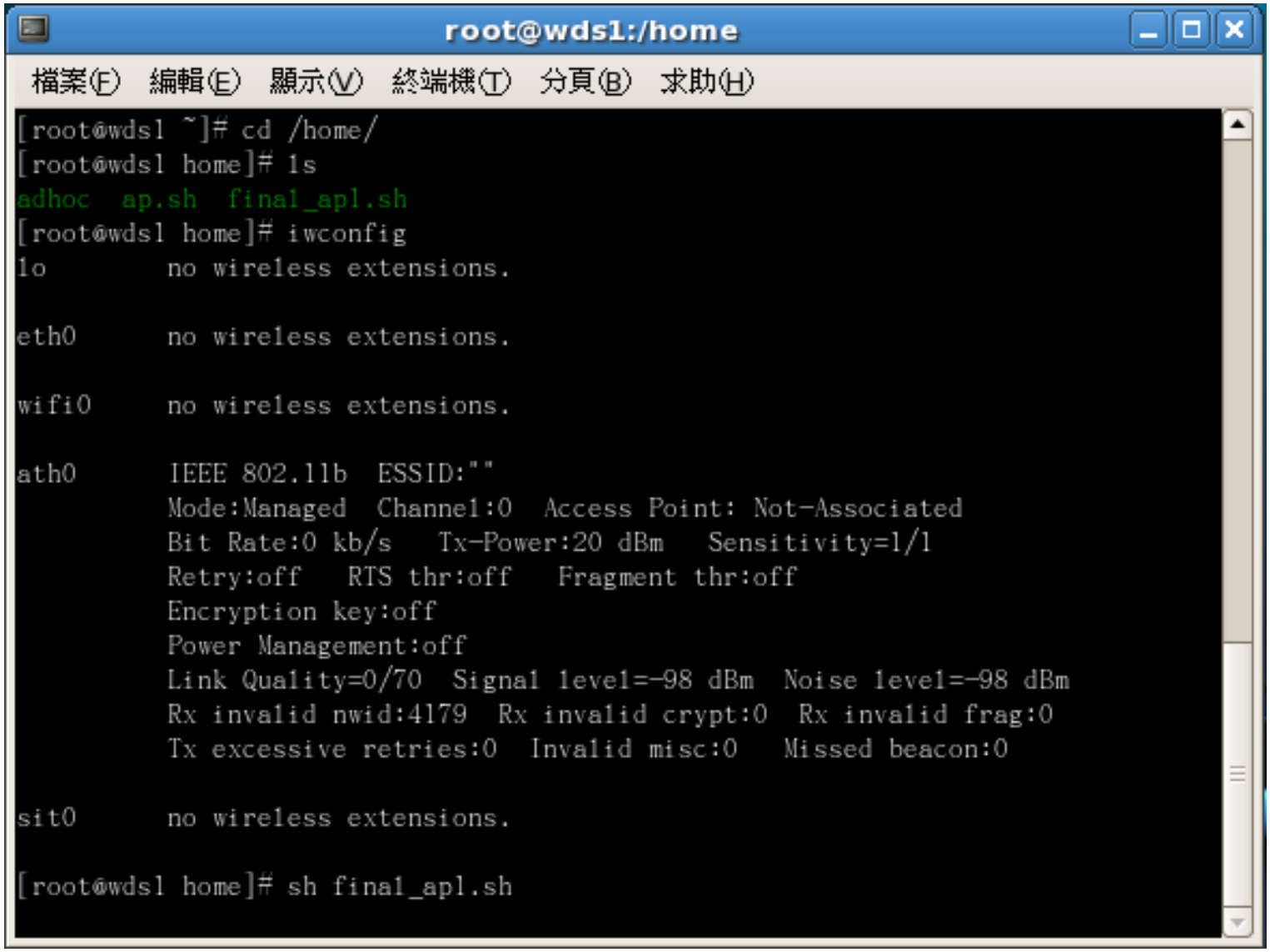
```
#chmod 755 final_ap1.sh
#sh final_ap1.sh
```

AP1的設定與運作情形(7/12)

- 初始狀態

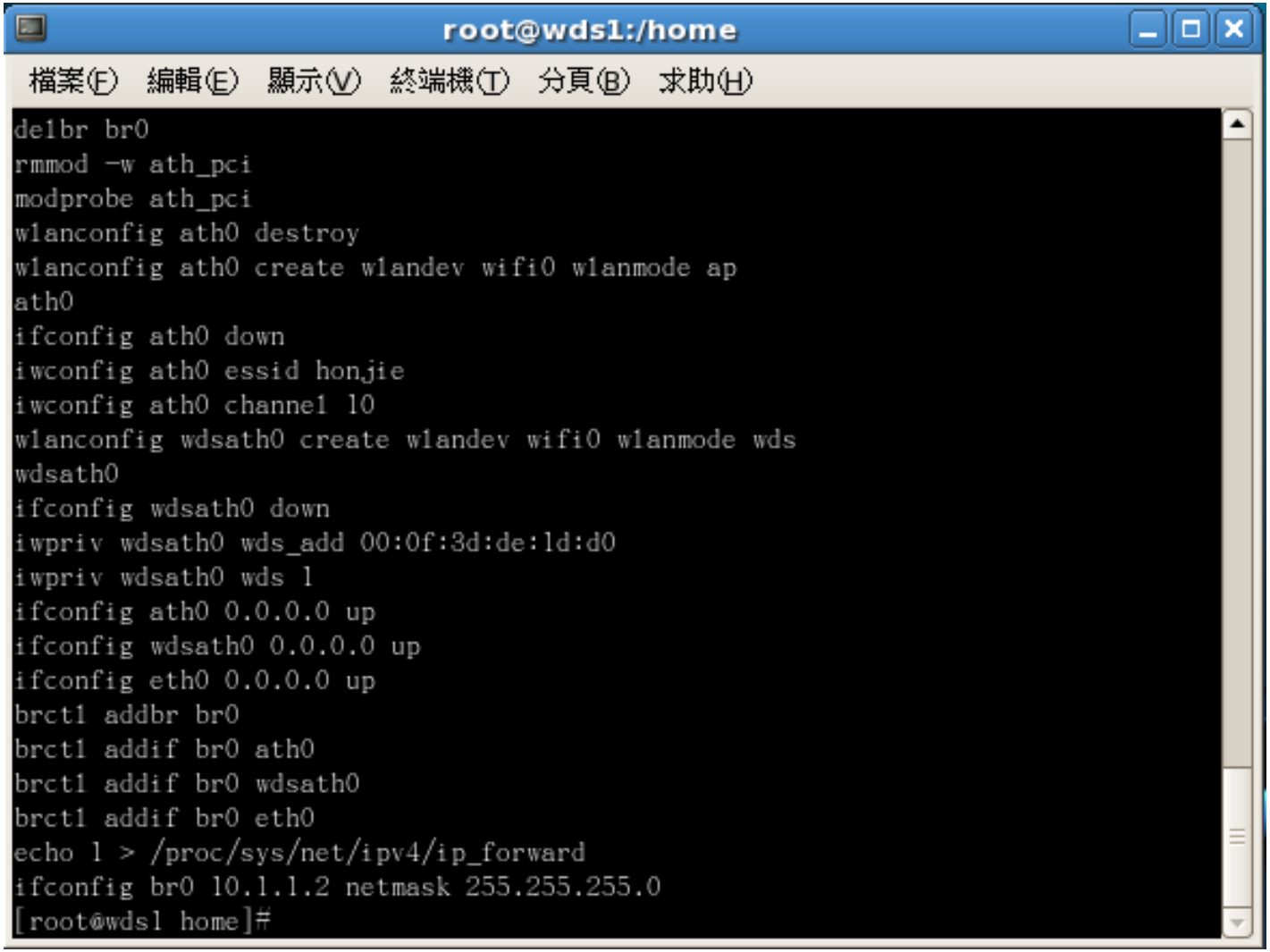


AP1的設定與運作情形(8/12)



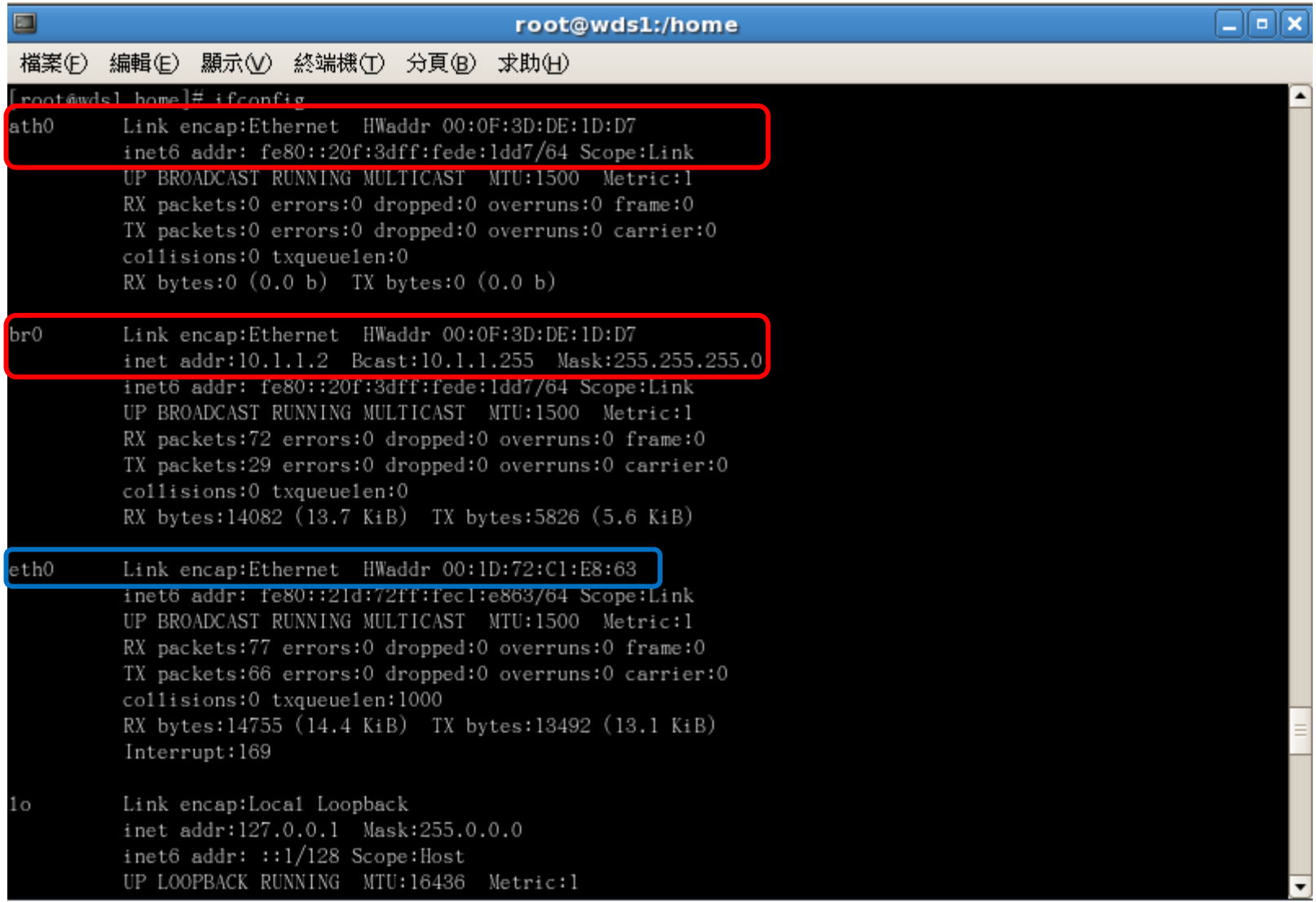
AP1的設定與運作情形(9/12)

執行後結果

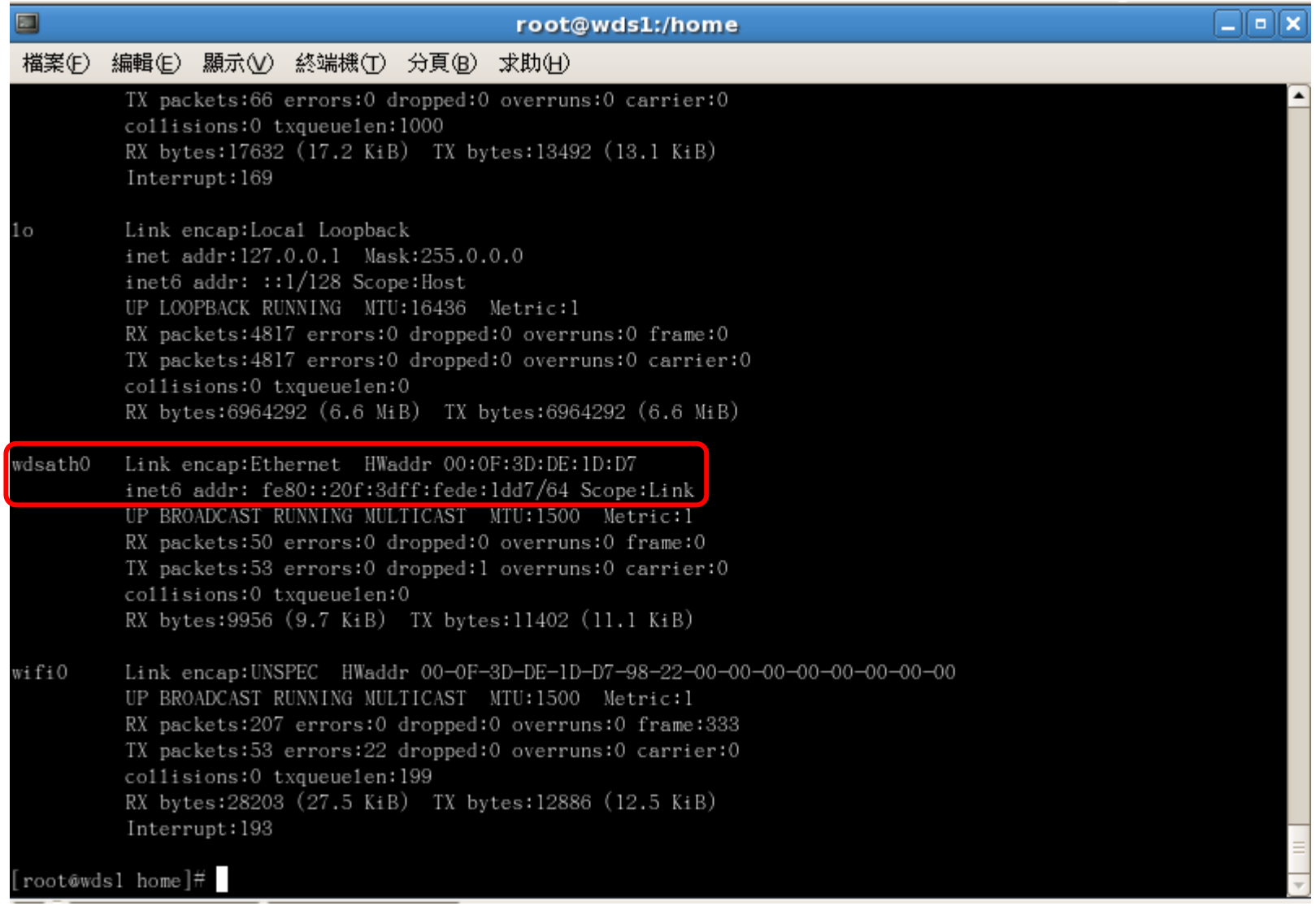


AP1的設定與運作情形(10/12)

觀看網路相關設定，#ifconfig

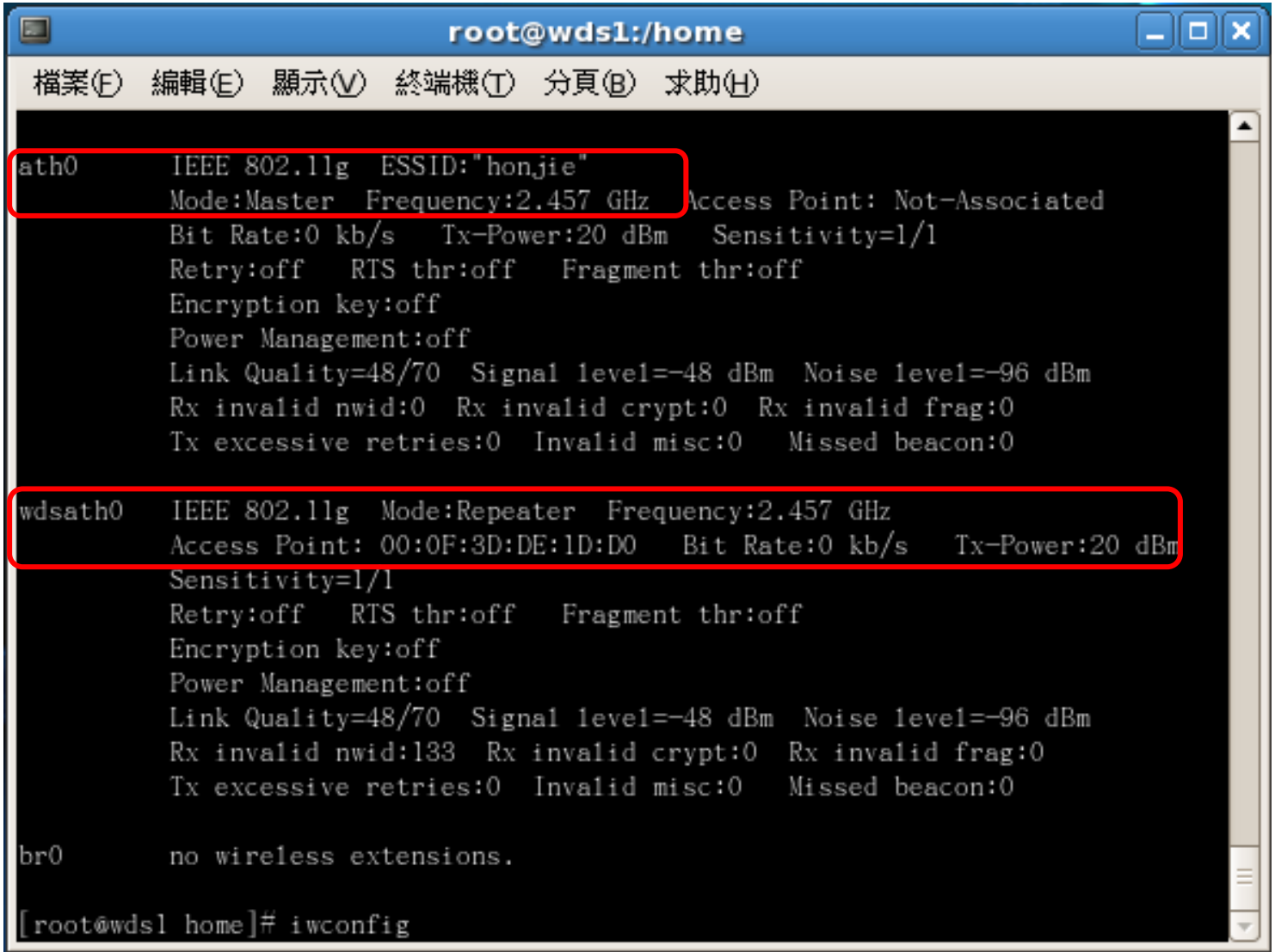


AP1的設定與運作情形(11/12)



AP1的設定與運作情形(12/12)

觀看無線網卡相關設定， #iwconfig



AP2的設定與運作情形(1/7)

編寫設定檔，大致上都跟AP1一樣，只須改綠色部分，將

```
echo "iwpriv wdsath0 wds_add 00:0f:3d:de:1d:d0 “
iwpriv wdsath0 wds_add 00:0f:3d:de:1d:d0
```

改成

```
echo "iwpriv wdsath0 wds_add 00:0f:3d:de:1d:d7 “
iwpriv wdsath0 wds_add 00:0f:3d:de:1d:d7
```

並將

```
echo "ifconfig br0 10.1.1.2 netmask 255.255.255.0 up “
ifconfig br0 10.1.1.2 netmask 255.255.255.0 up
```

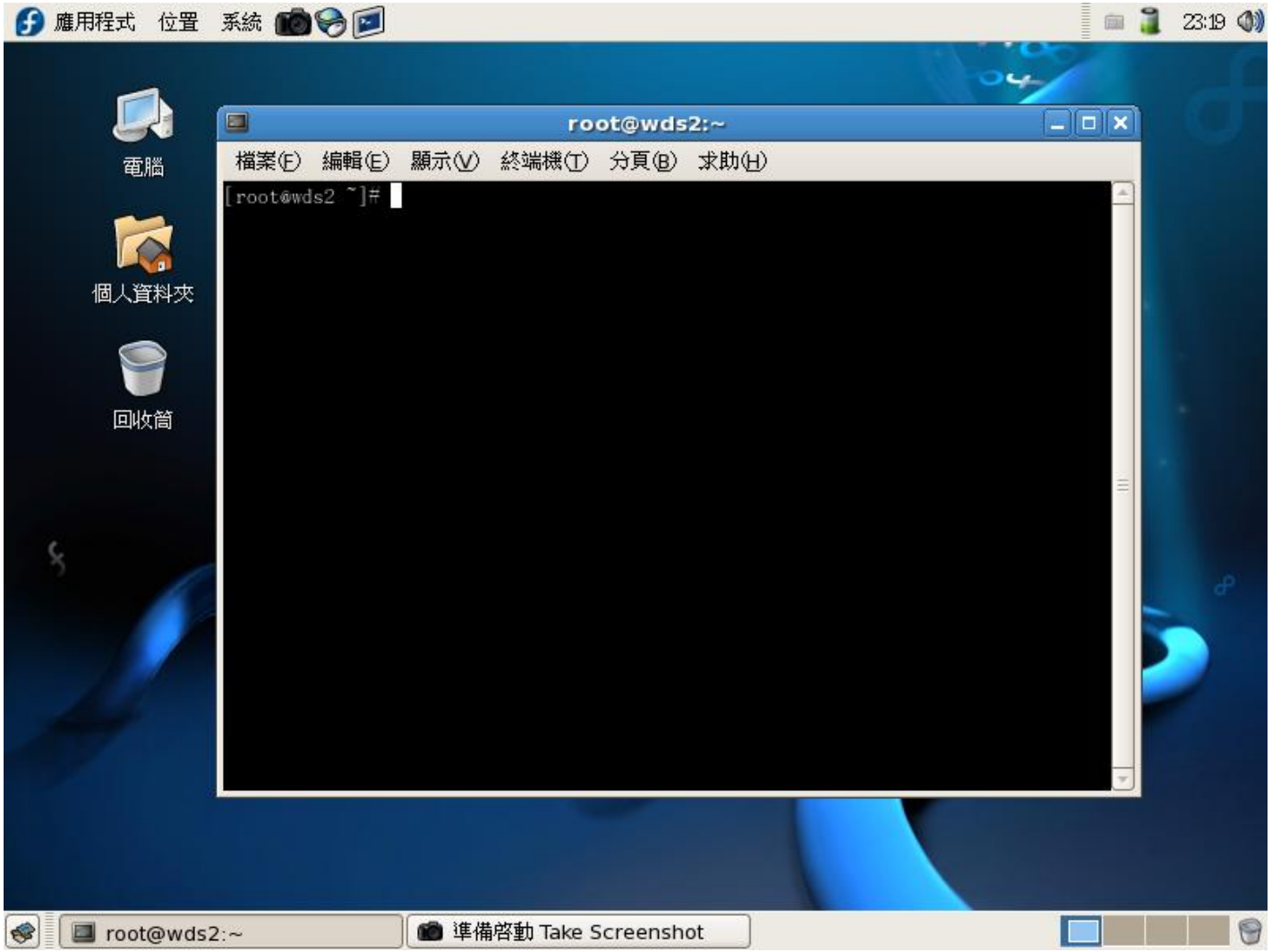
改成

```
echo "ifconfig br0 10.1.1.3 netmask 255.255.255.0 up “
ifconfig br0 10.1.1.3 netmask 255.255.255.0 up
```

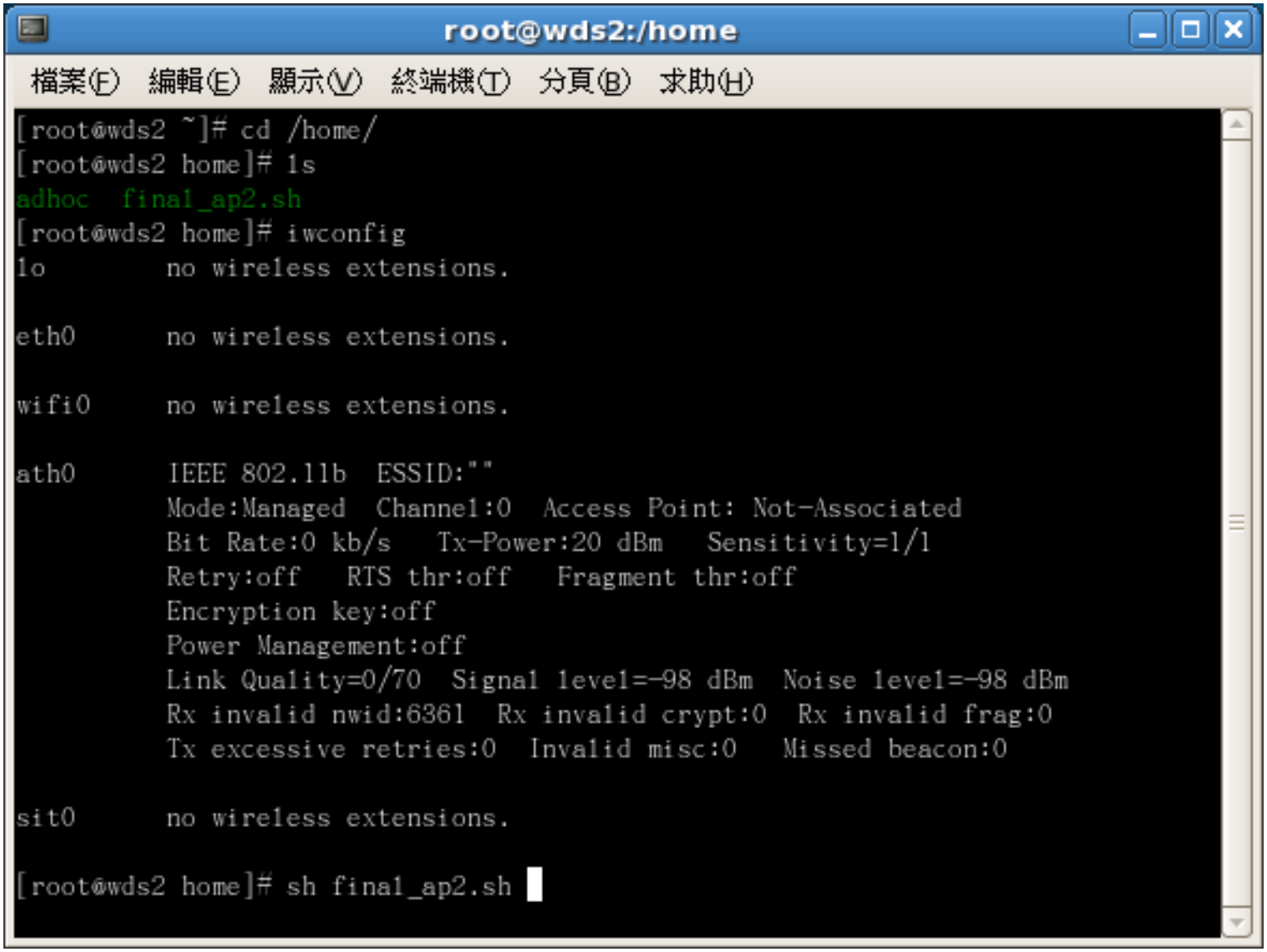
改藍字部分之後存檔執行。

AP2的設定與運作情形(2/7)

- 初始狀態

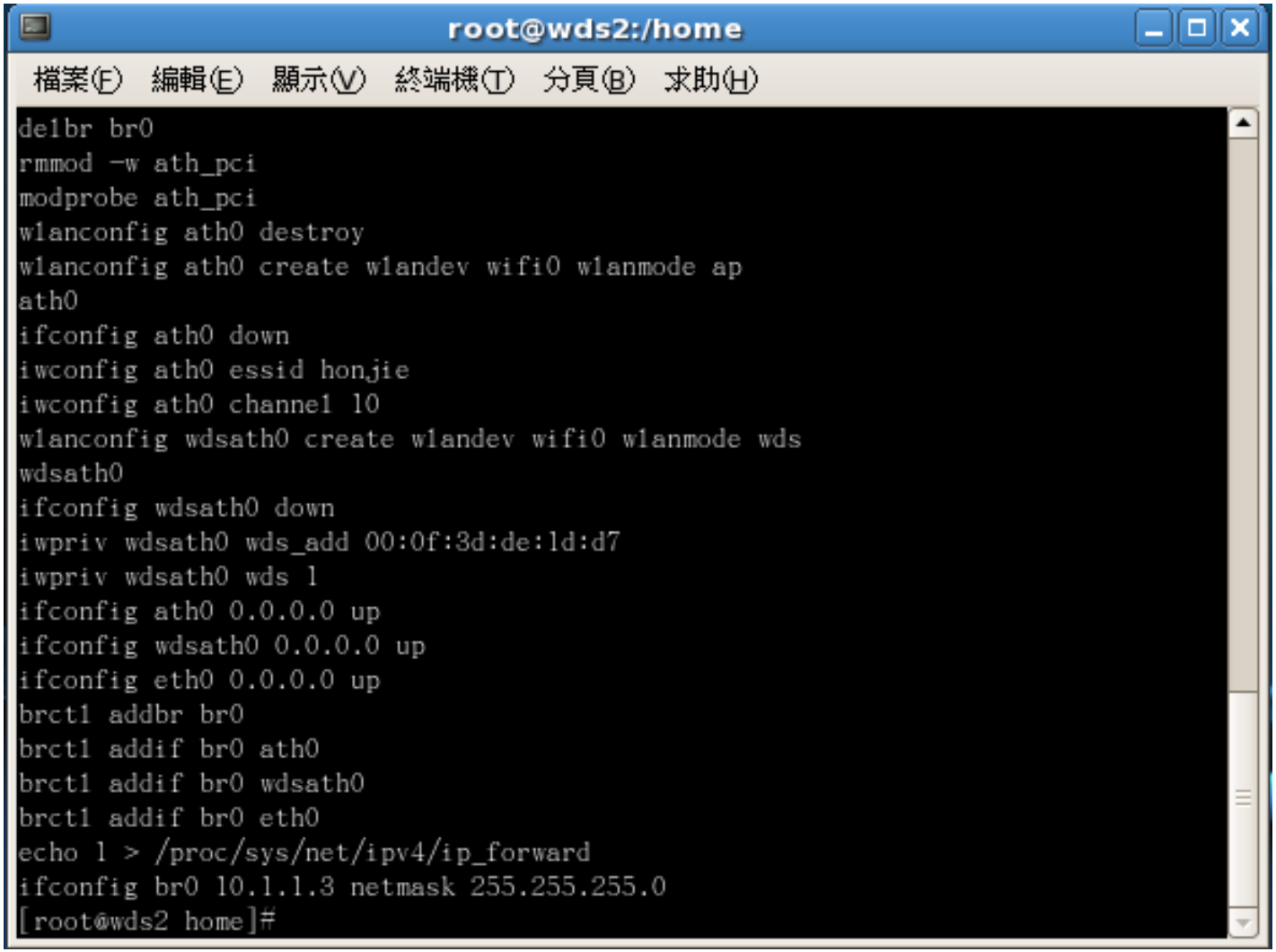


AP2的設定與運作情形(3/7)



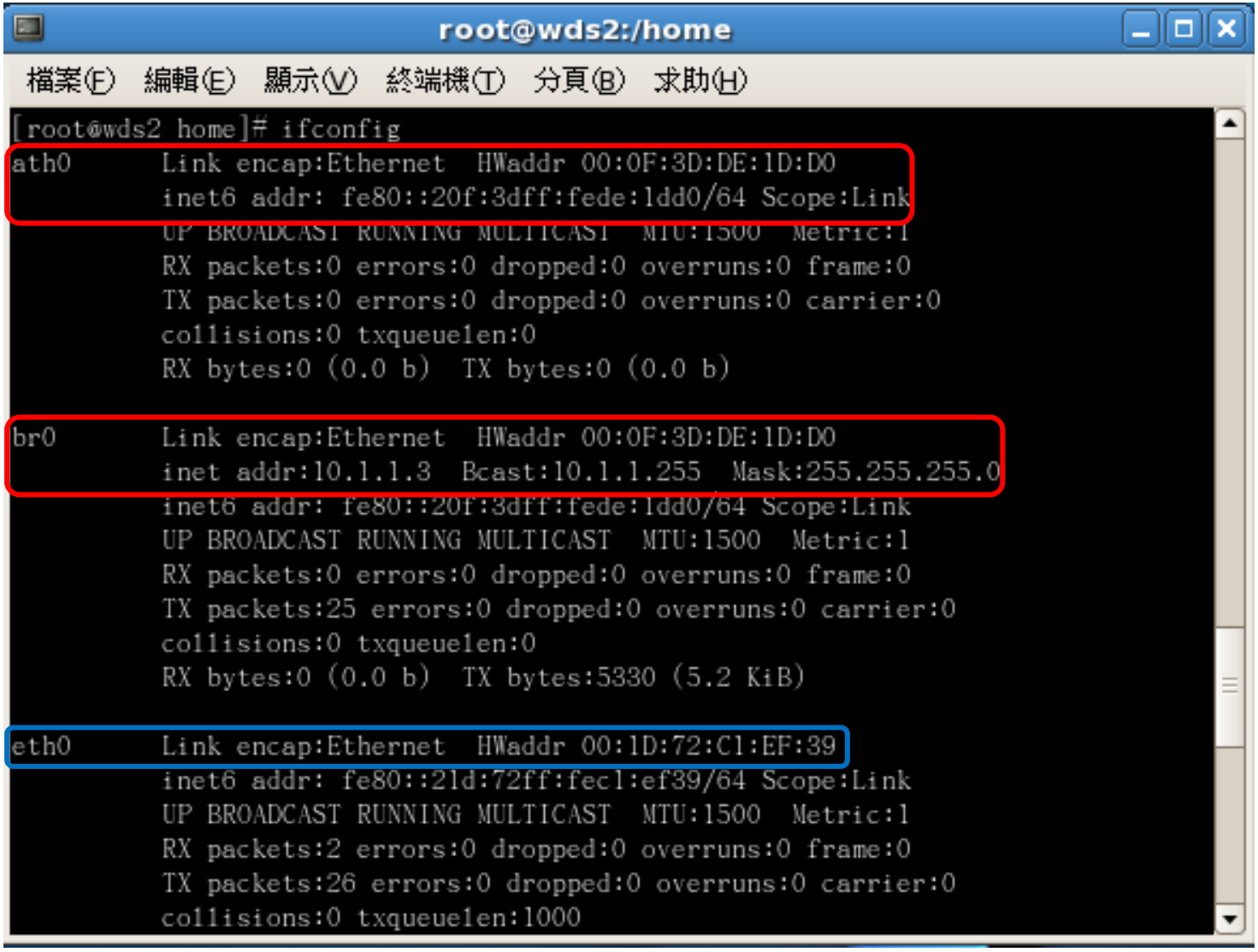
AP2的設定與運作情形(4/7)

執行後結果

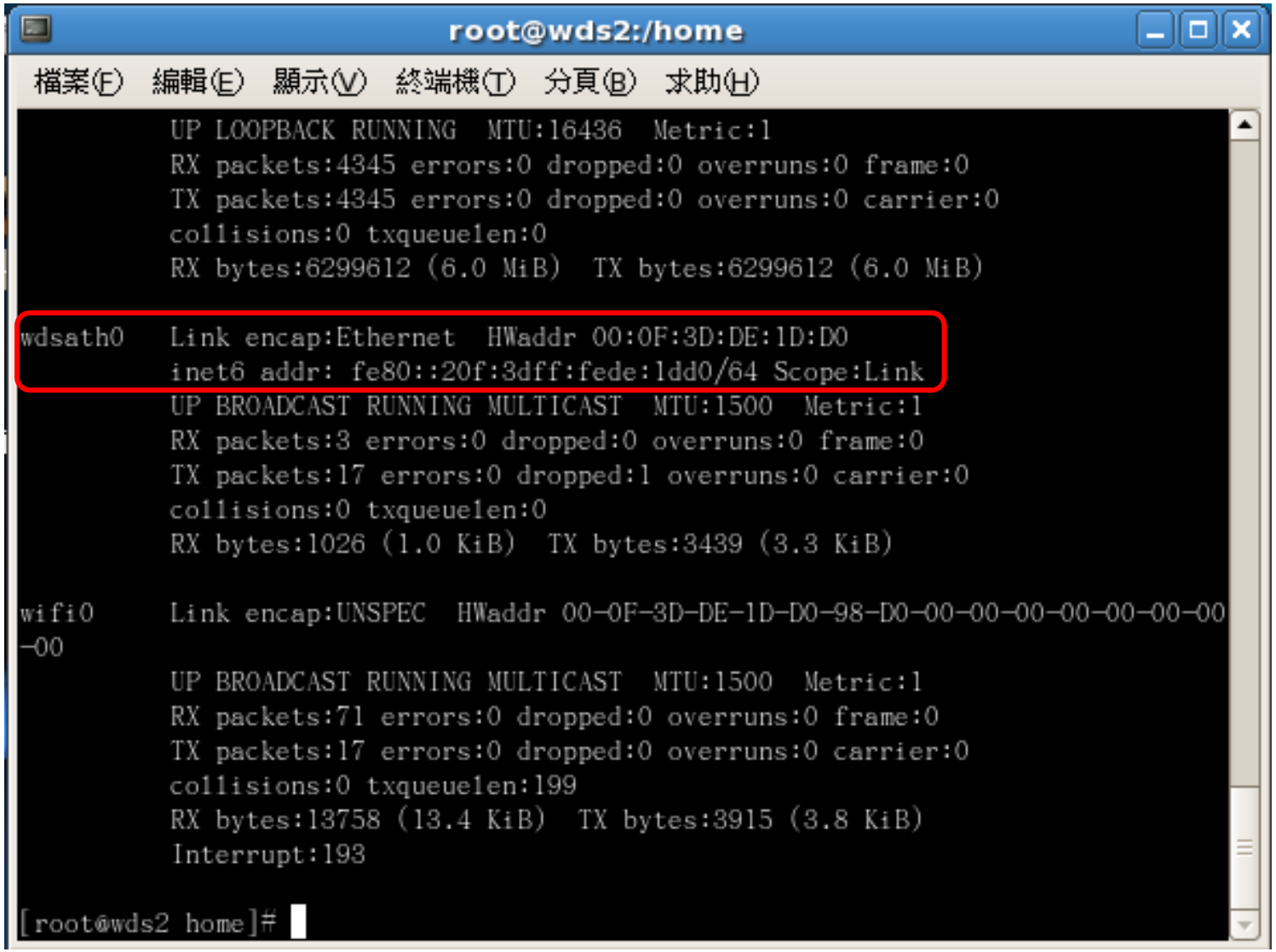


AP2的設定與運作情形(5/7)

觀看網路相關設定，#ifconfig

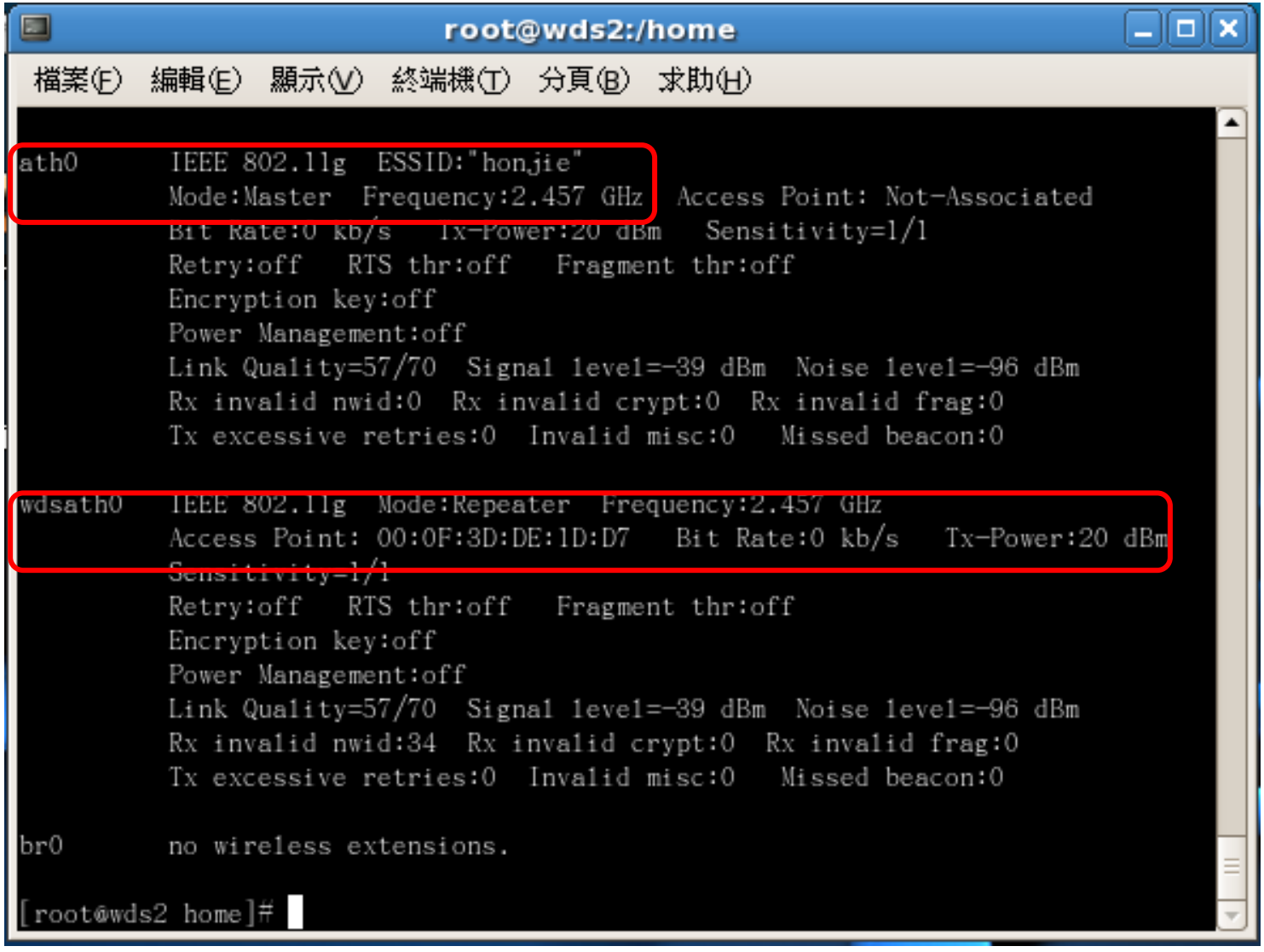


AP2的設定與運作情形(6/7)



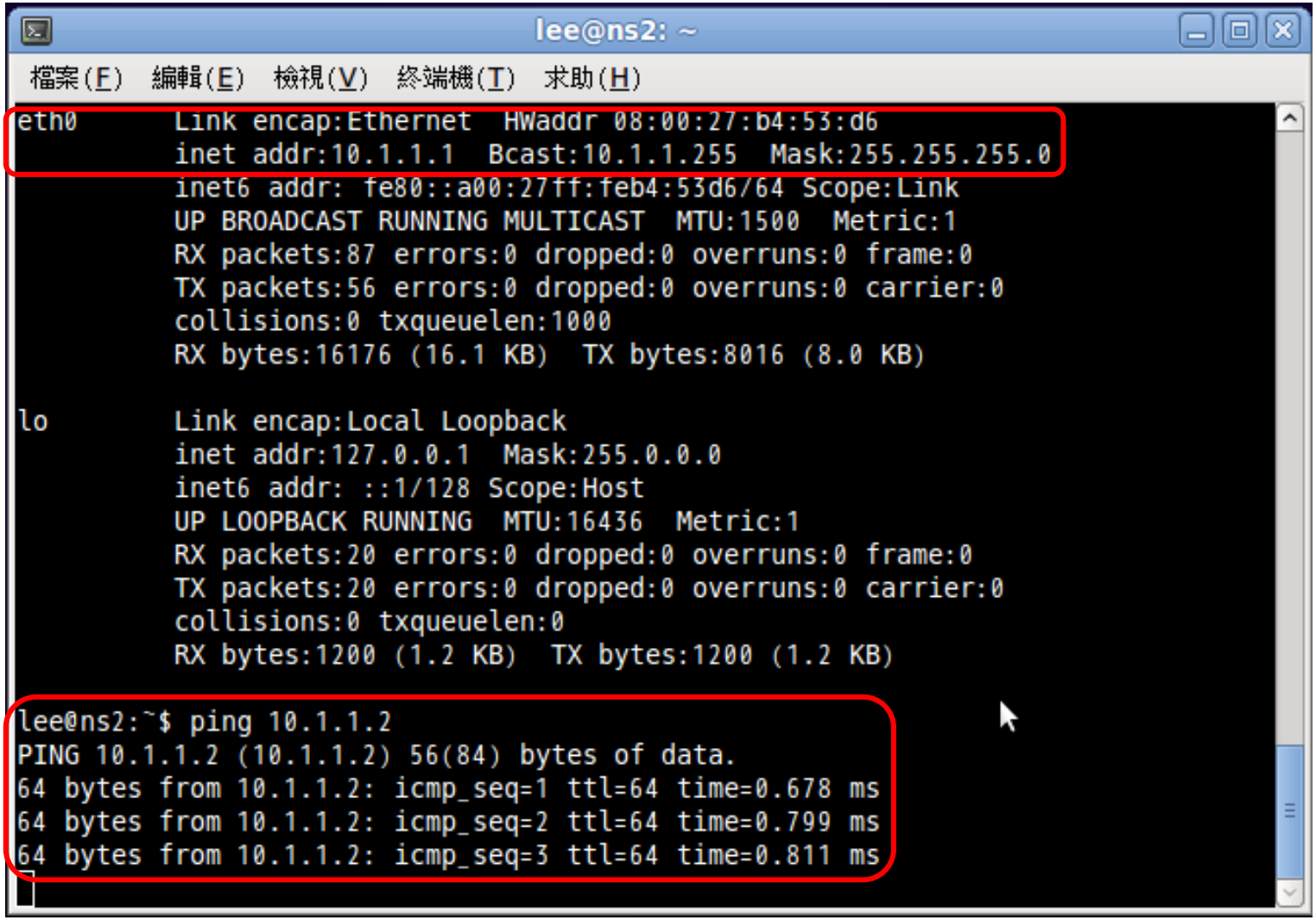
AP2的設定與運作情形(7/7)

觀看無線網卡相關設定， #iwconfig



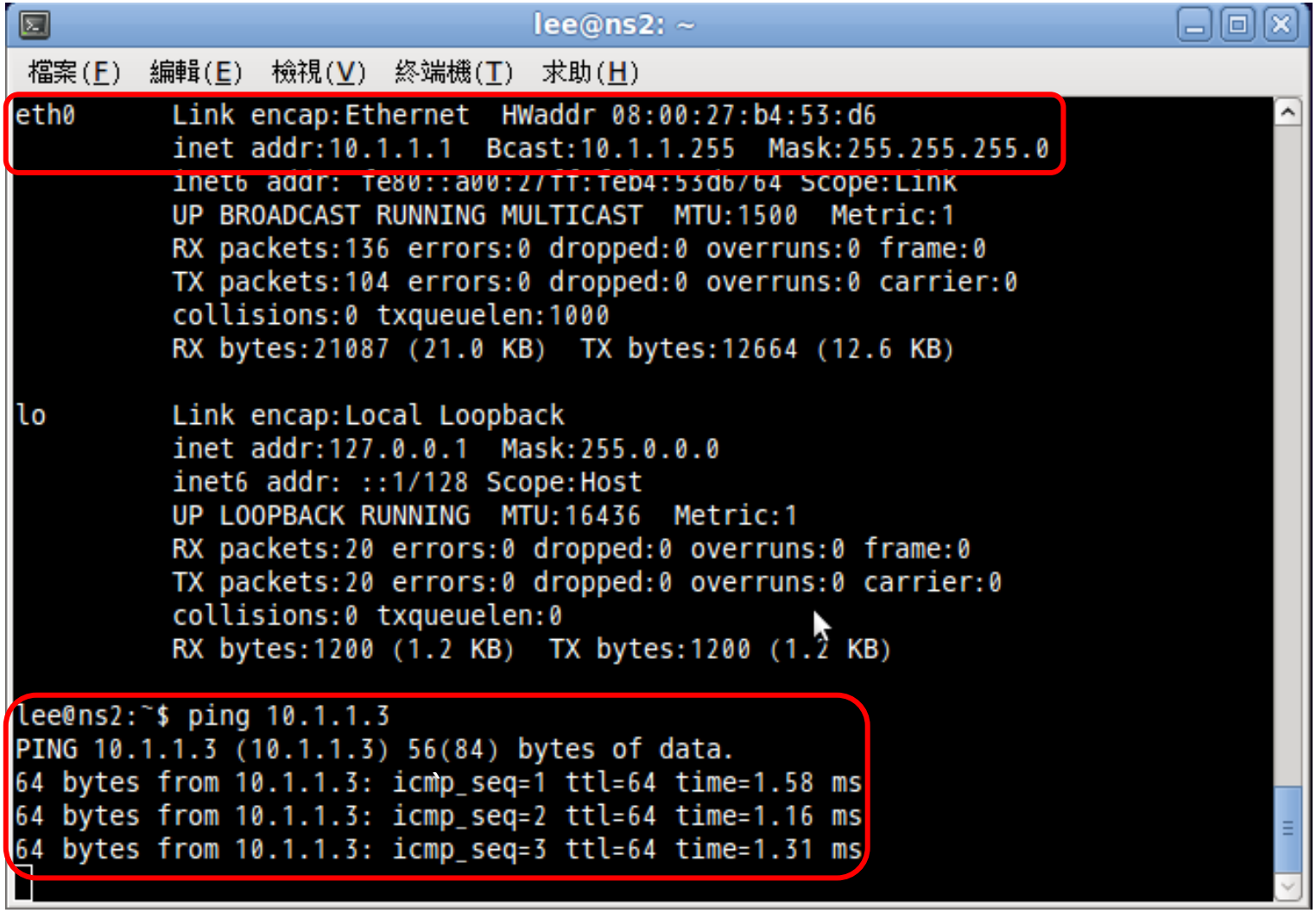
實驗結果(1/13)

- STA1(10.1.1.1) ping AP1(10.1.1.2)



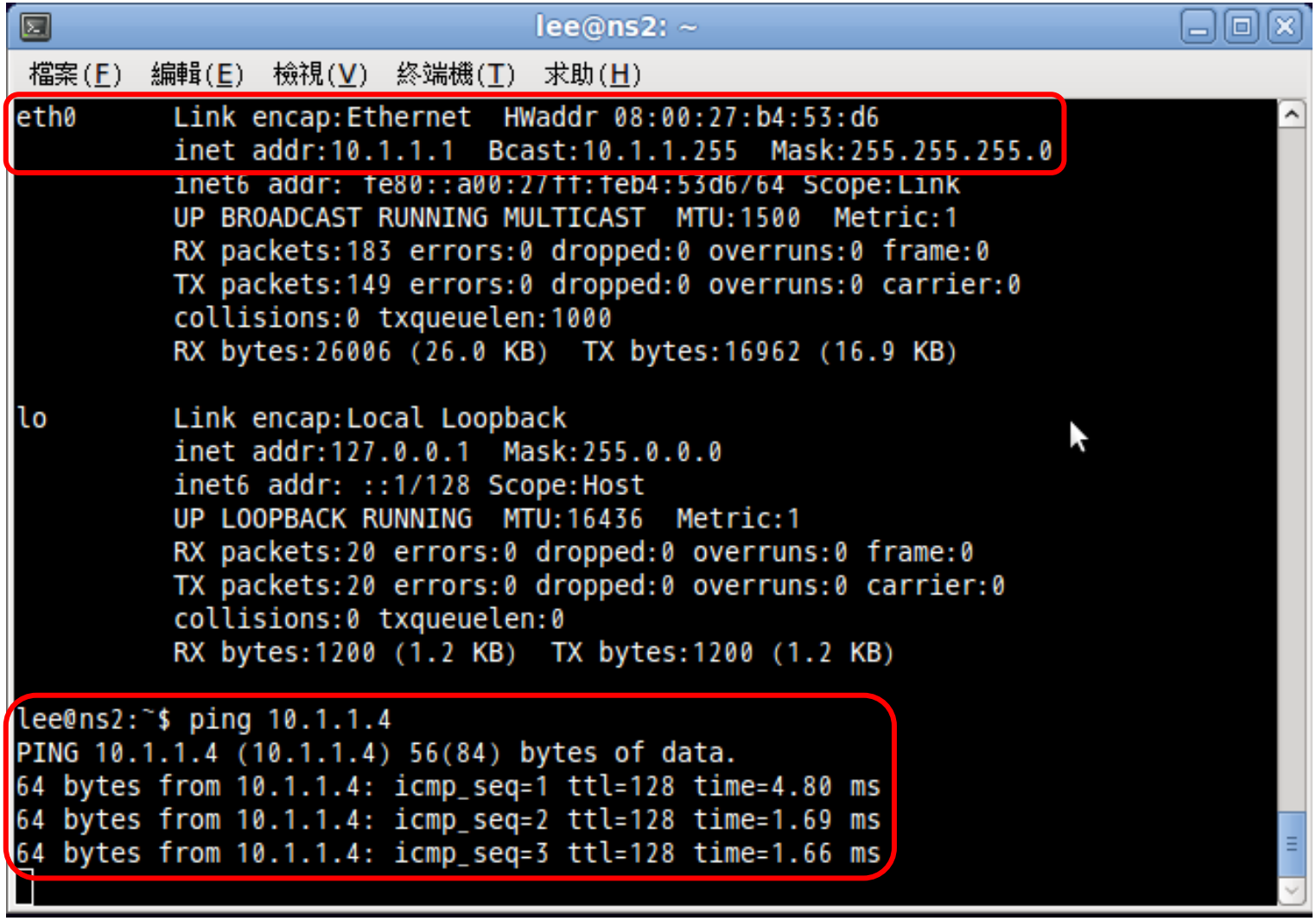
實驗結果(2/13)

- STA1(10.1.1.1) ping AP2(10.1.1.3)



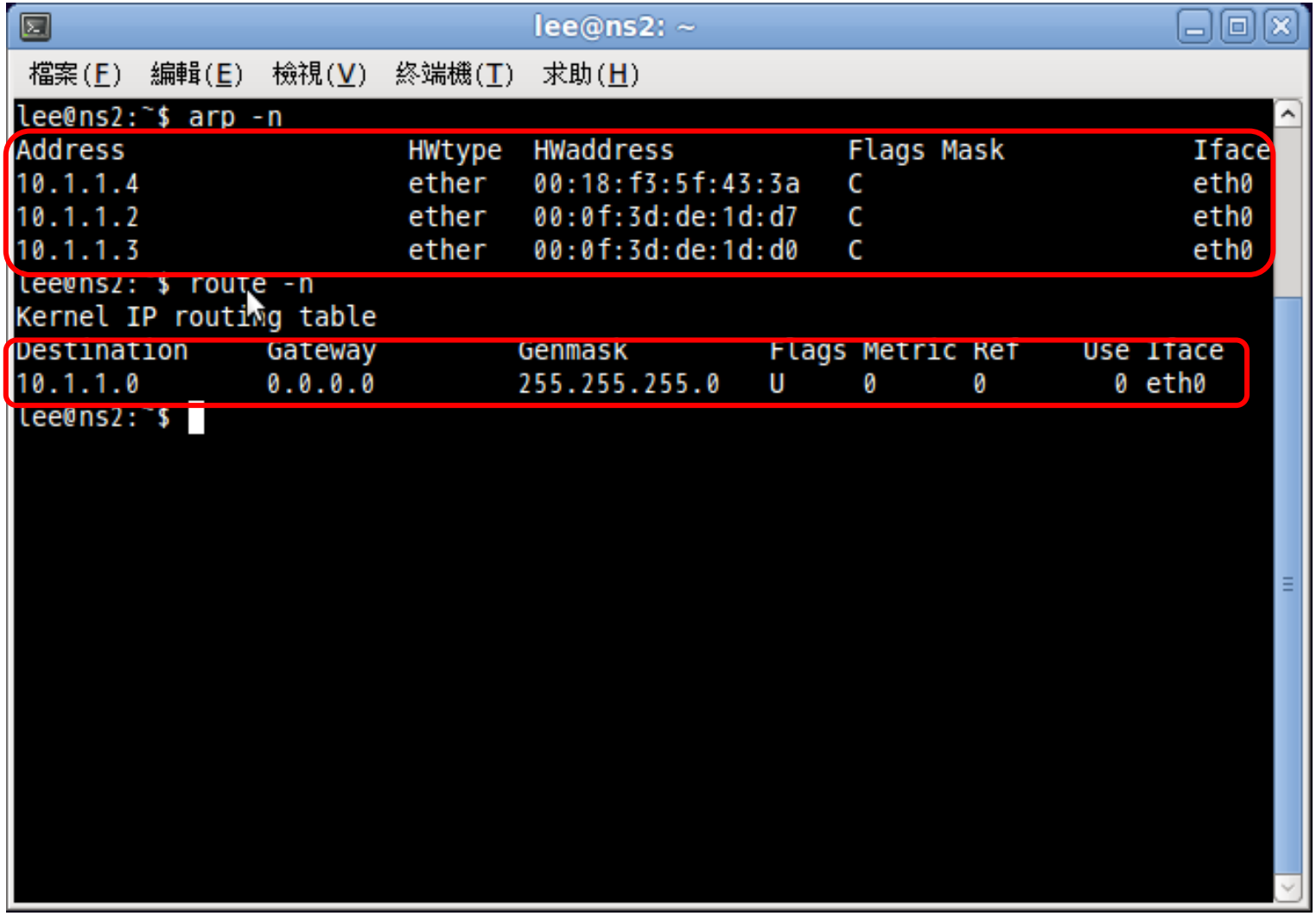
實驗結果(3/13)

- STA1(10.1.1.1) ping STA2(10.1.1.4)



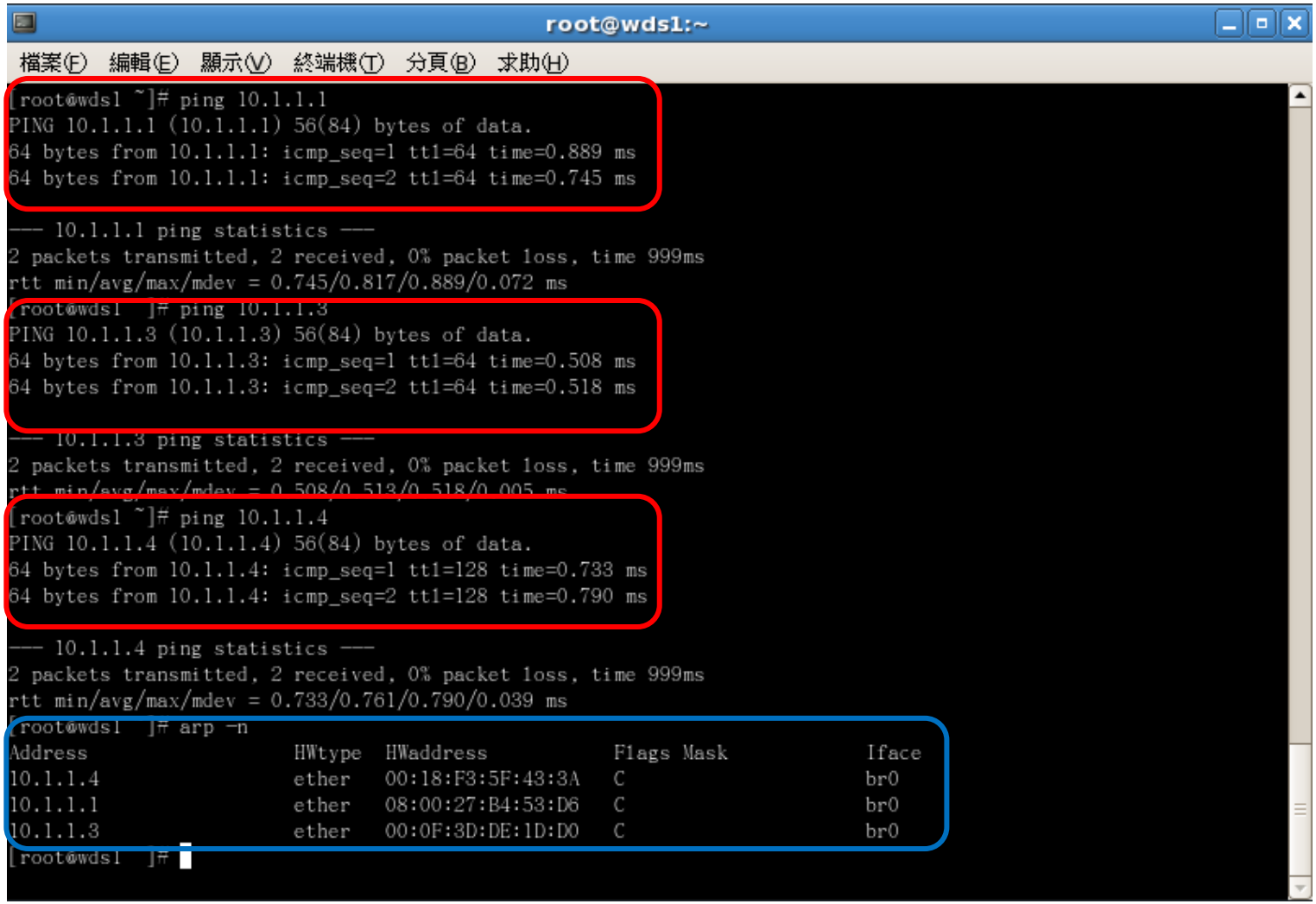
實驗結果(4/13)

- STA1(10.1.1.1) arp 與 route table



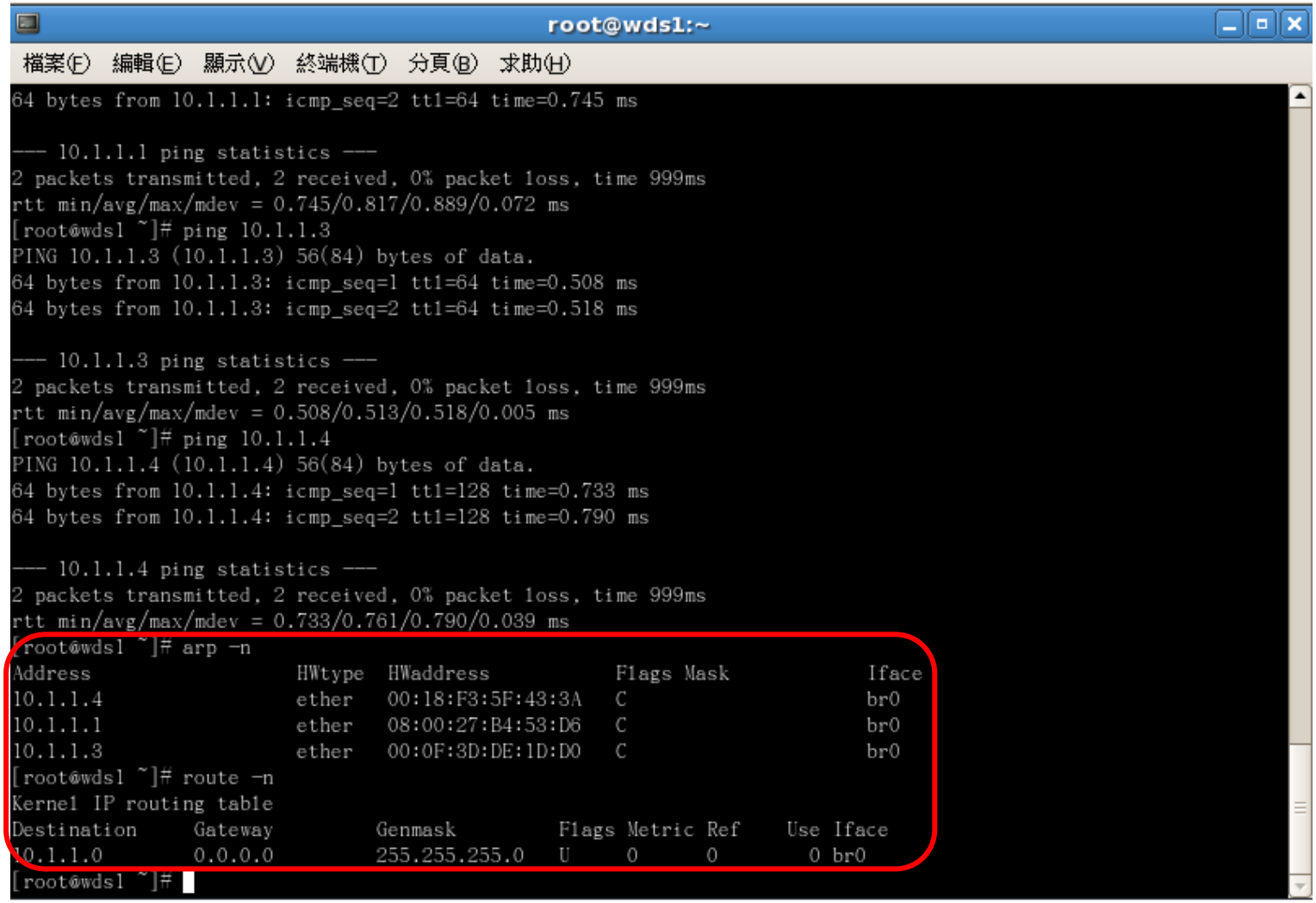
實驗結果(5/13)

- AP1(10.1.1.2) ping STA1(10.1.1.1)
- AP1(10.1.1.2) ping AP2(10.1.1.3)
- AP1(10.1.1.2) ping STA2(10.1.1.4)



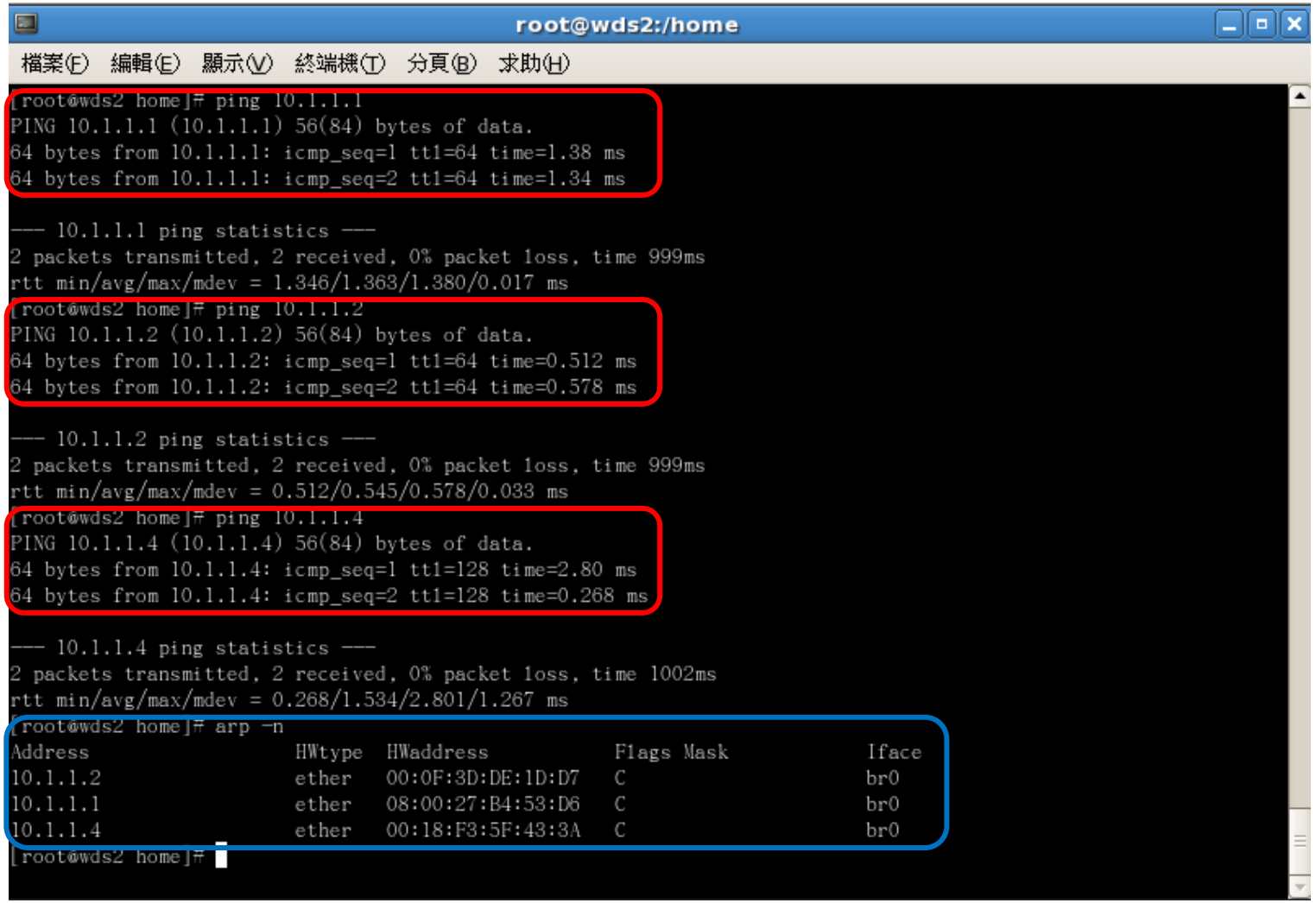
實驗結果(6/13)

- AP1(10.1.1.2) arp 與 route table



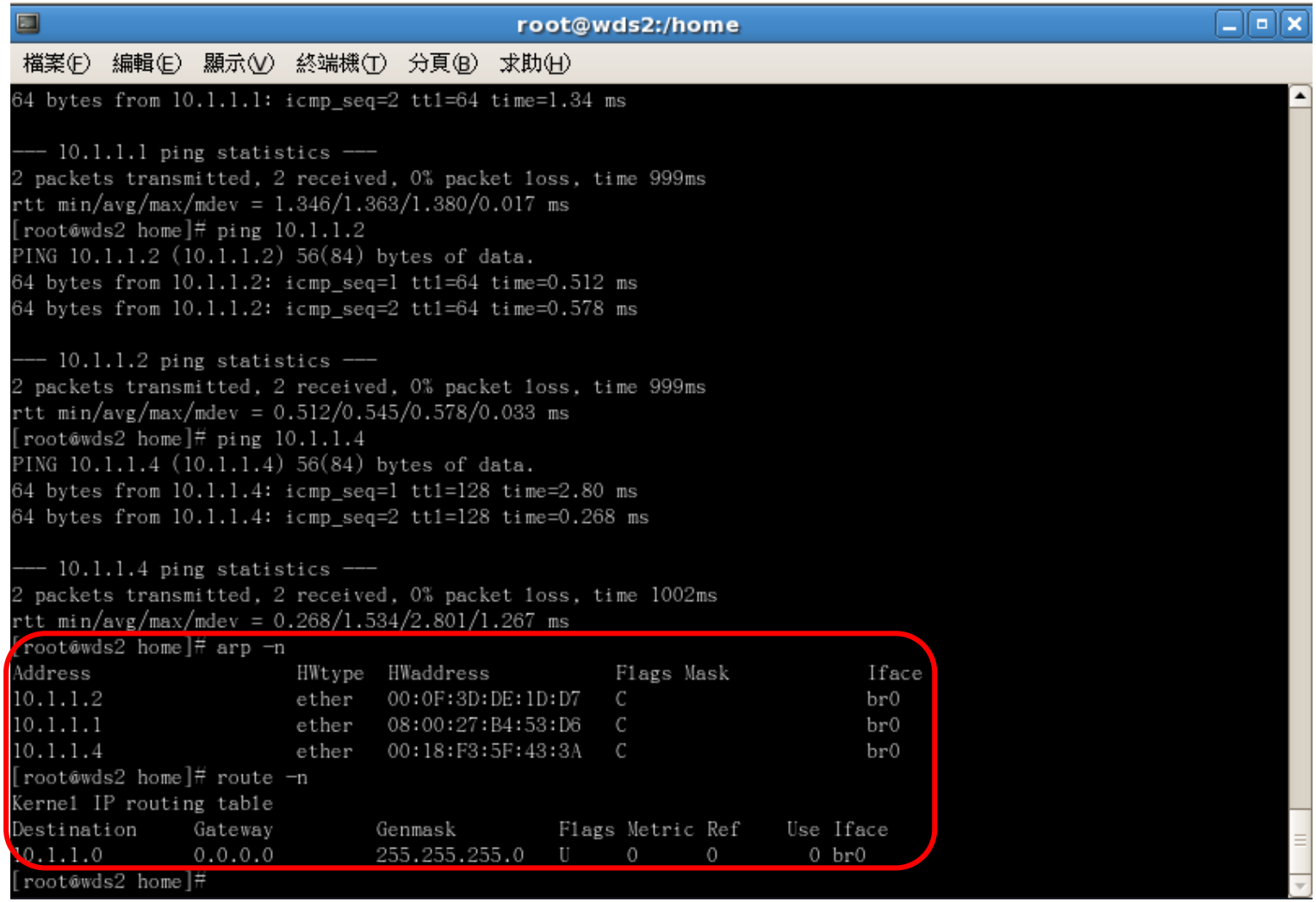
實驗結果(7/13)

- AP2(10.1.1.3) ping STA1(10.1.1.1)
- AP2(10.1.1.3) ping AP1(10.1.1.2)
- AP2(10.1.1.3) ping STA2(10.1.1.4)



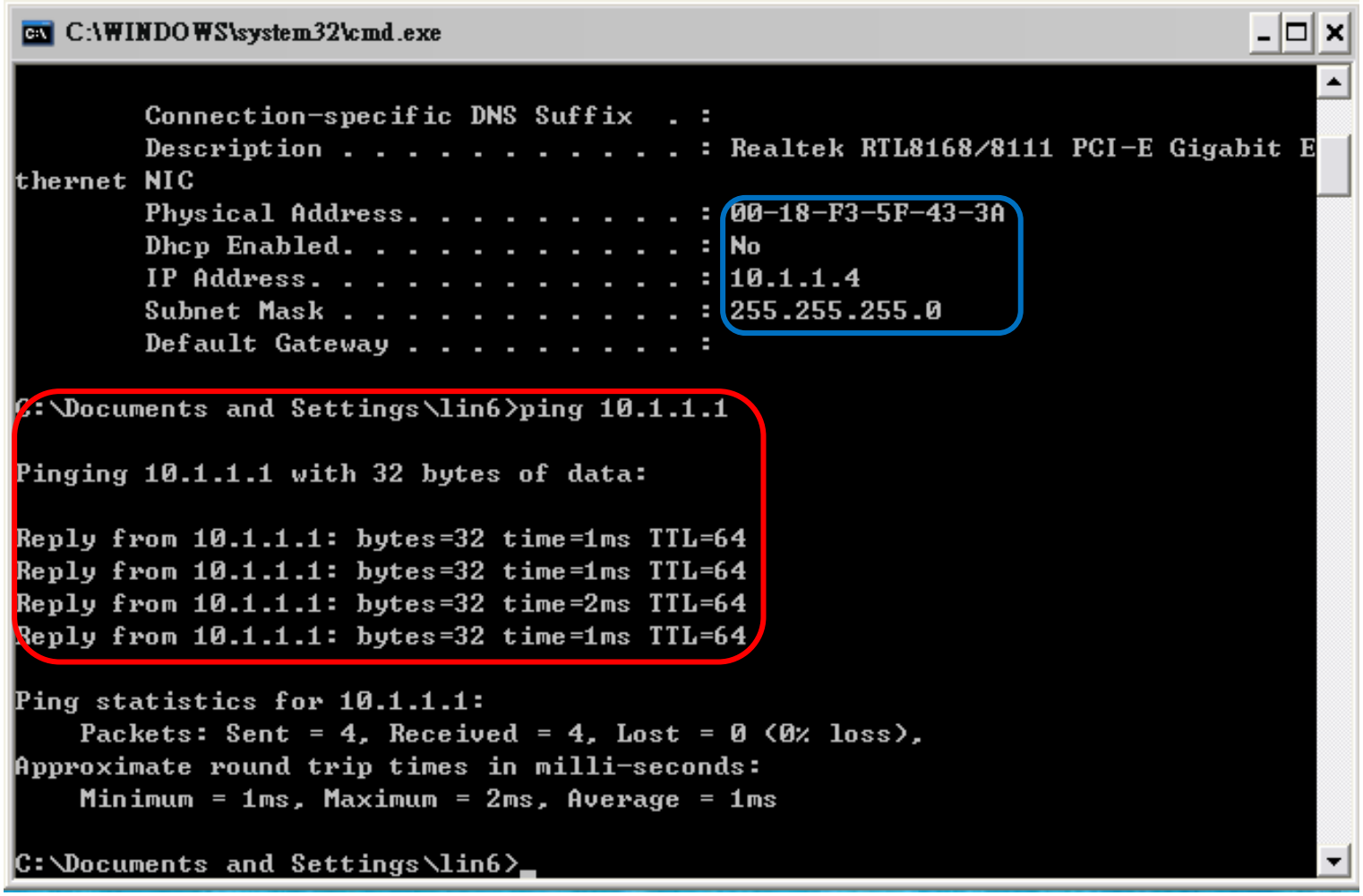
實驗結果(8/13)

- AP2(10.1.1.3) arp 與 route table



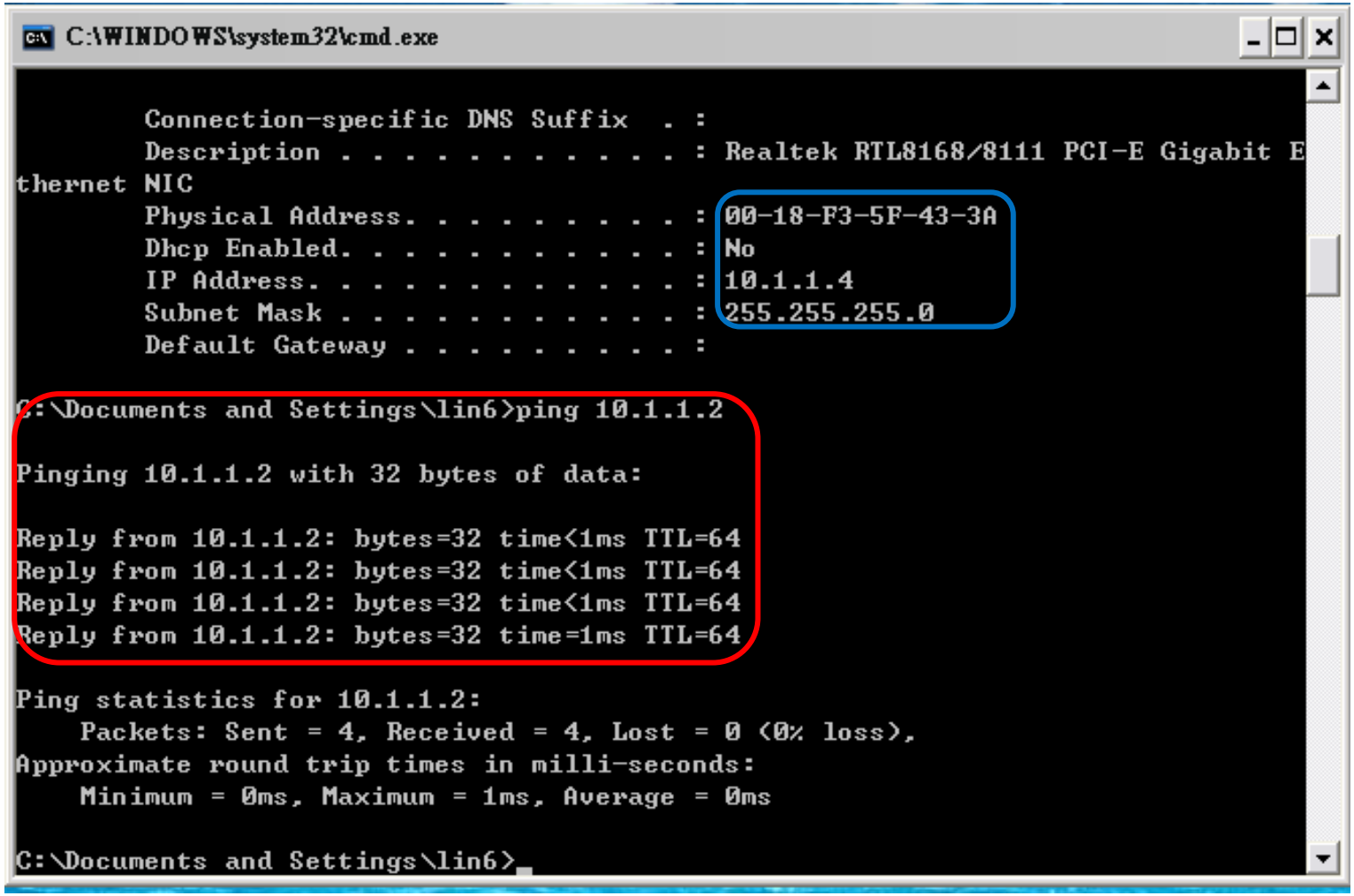
實驗結果(9/13)

- STA2(10.1.1.4) ping STA1(10.1.1.1)



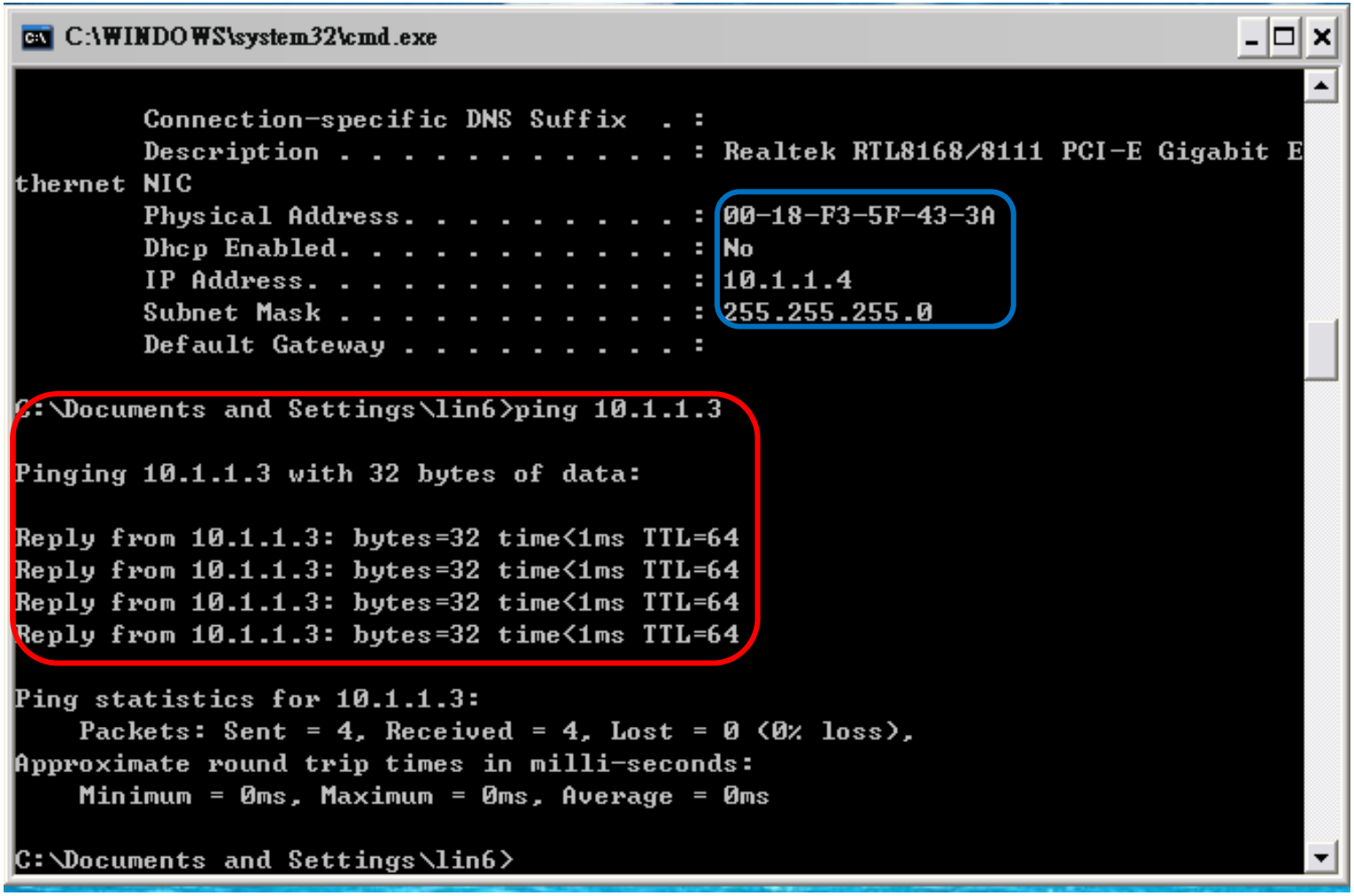
實驗結果(10/13)

- STA1(10.1.1.4) ping AP1(10.1.1.2)



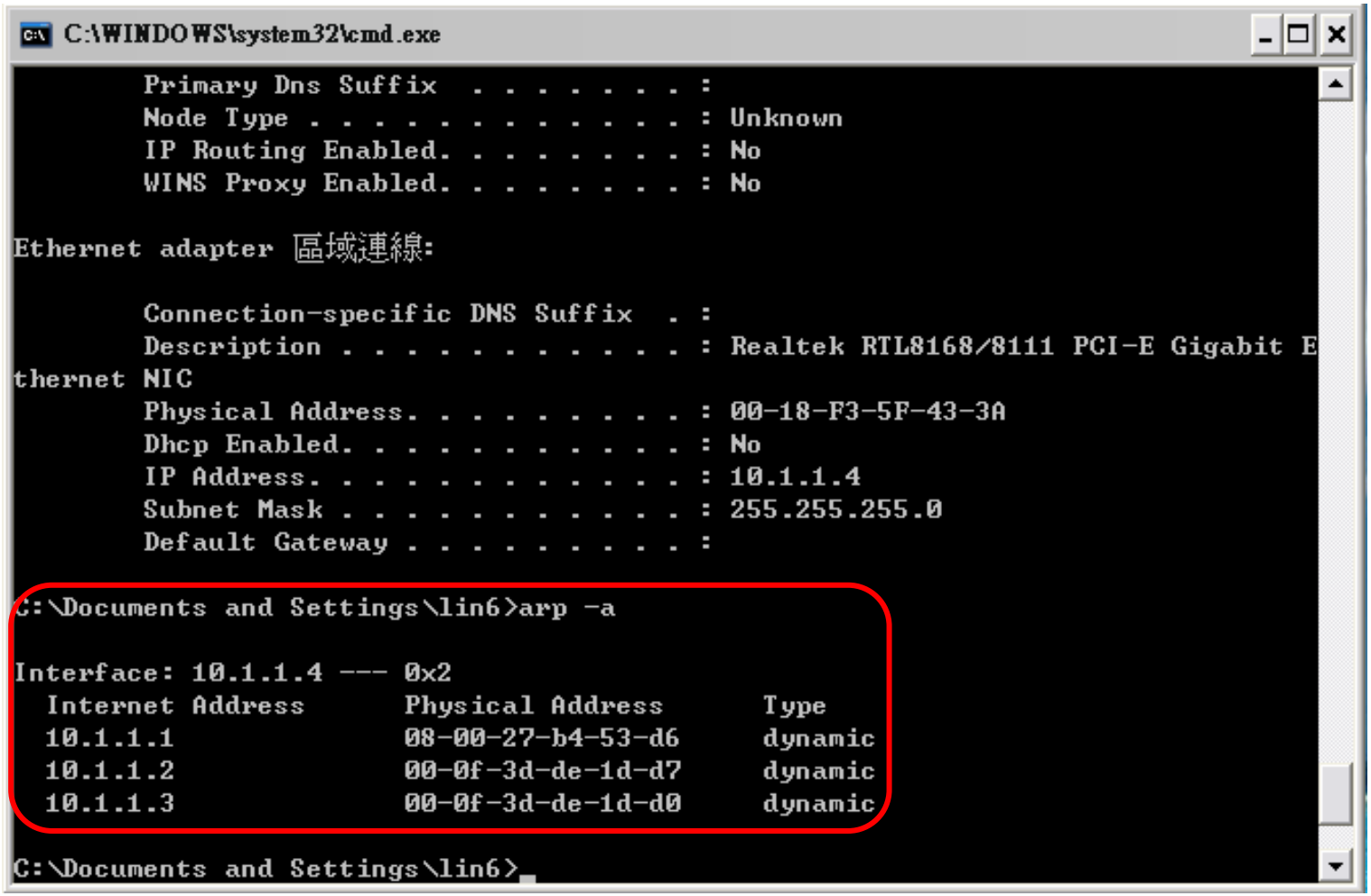
實驗結果(11/13)

- STA2(10.1.1.4) ping AP2(10.1.1.3)



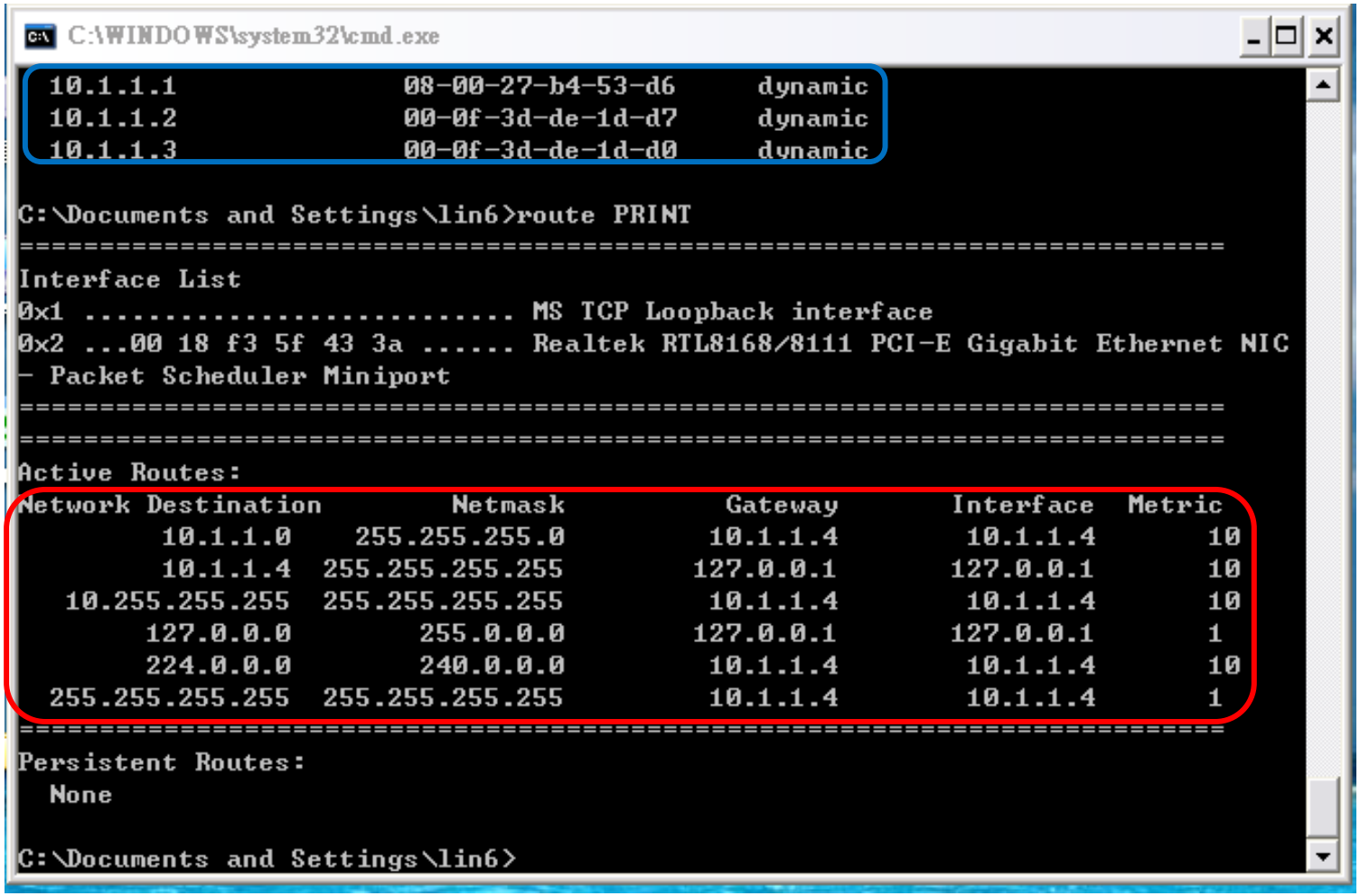
實驗結果(12/13)

- STA2(10.1.1.4) arp table



實驗結果(13/13)

- STA2(10.1.1.4) route table



注意事項(1/4)

- AP1設定檔裡提到//以上為執行第二次以上才有作用，為device重置的意思，初次執行會無此裝置是沒關係的，因為不一定執行一次就會成功，故所以加入這一段，執行第二次以上後就會清除所有設定，重新寫入，也就是重置裝置的意思
- 基本上，本次實驗都是使用802.11g居多，WiFi(802.11b & 802.11g)有11個無線頻道(channel)，由1~11所組成，他們的頻段為ISM Band 2.4GHz。在同一個地方可能有許多台AP，由於11個channel的頻率其實蠻接近的，為了讓彼此AP降低干擾，而理想的頻道間隔應該為5，也就是在同一區域如果有3人各自架設自己的AP提供自己人上網使用，那麼最好的選擇將會是channel 1 & channel 6 & channel 11，此為最理想狀況(頻率間隔越大，彼此間干擾越低)，所以請盡量避免channel在2.4GHz的設備之間架設AP(ex:微波爐…等等)，除非你們是使用WiFi其他的規格(ex:802.11a就在5GHz…等等)

注意事項(2/4)

- 基於以上第2點，所以如果我們能避開相同或是鄰近的channel，那麼AP & WDS實驗的成功性必將提高許多，所以我們可以先使用無線網卡來掃瞄無線AP的channel與SSID跟一些相關訊息，利用這些訊息來避開實驗選擇相同或是鄰近的channel，以降低干擾，提升成功率。
- 插入無線網卡，輸入以下指令

  #ifconfig ath0 up

  #wlanconfig ath0 list scan

  我在NETLAB scan，結果如下圖

注意事項(3/4)

- 我檔案裡有寫echo ”” ，此為print出目前執行到哪一個指令動作，不一定要寫，只是為了方便debug哪一行出錯。另外sleep 3-sleep功能是讓他執行程序後等待一段時間再度執行下一行指令，避免機器當機狀態，或是沒有執行指令就跳過。建議寫比較保險，不然當機就飽了(以上是我試多種Linux Distribution實作adhoc & AP實驗心得)，故我之後都會加 “sleep 3”
- 如果station一端是Windows用戶，建議關閉防火牆，不然無法ping到，先前實驗都是用Linux Distribution，所以無此問題(此為我這次實作所遇到的問題)
- 此次實驗STA1其實是使用我的NB Win7底下灌Virtualbox掛載Ubuntu，但是其實不影響結果，我試過了station端不管是WinXP、Win7、Fedora、CentOS、Ubuntu都可以成功互ping

注意事項(4/4)

- 先前WDS實驗是在Ubuntu底下架設成功，但是也是一直在try and error許久之後才革命成功，印象試了N次才成功1次，已記不得了。經由再次實做WDS實驗，我覺得也許在Fedora底下會比較容易成功，我執行1~2次就成功了，頂多3次，已驗證關機重開機再試，驗證10次的成功取樣
- 如果堅持要在Ubuntu底下實作WDS，他的ath0無線網卡mac開頭會改成06:XX:XX:XX:XX:XX，你要啟動WDS，要加入對方AP MAC時，也許改成06:XX:XX:XX:XX:XX，才會成功。
- 其實有興趣的同學也可以參考The MadWiFi project網站，有更多詳細的MadWiFi介紹，可以玩看看加密機制的AP…等等，經由實作adhoc & AP & WDS想必同學對網路運作觀念與原理更加確實了解，Good luck！

参考文献

[1] **The MadWifi project**

http://madwifi-project.org/wiki