電腦通訊網路

Lab 3 – Network Monitoring over Linux/Windows Using Command Line & Packet Sniffer using Wireshark

實驗目的:

在 Linux/Windows 平台上測試並監控瞭解所在的網路情況，包括

- 利用 Command Line 的方式來除錯與觀察網路。
- 利用 Wireshark 來觀察封包

實驗內容:

A. 熟悉 Linux/Windows Command Line 的用法，包括

1. ifconfig[1] (linux)、ipconfig[1] (Windows)
   查詢電腦網路資訊(包括電腦網路介面、網路 IP、DNS 等設定)。

2. ping[2] (linux/Windows)、 traceroute[3] (linux)、 tracert[3] (Windows)、 pathping[4] (Windows)、mtr(linux)
   偵錯與觀察兩主機溝通與路由路徑。

3. Nslookup
   查詢特定 DNS 伺服器正反解之網路資訊。

4. netstat
   觀察網路對外的連線狀況

B. 熟悉使用 Wireshark，並了解如何觀察封包。

。

實驗設備:

- 一台安裝 Linux/Windows OS 電腦

軟體工具:

1. **ipconfig/ifconfig, ping, tracert/traceroute, pathping/mtr, nslookup , netstat**
2. **Wireshark**

實驗內容及報告:

1. 偵錯與觀察網路：測試自己所屬的區域網路上的狀態。

- 一些常用的例子 (以下皆以 windows 內建網路工具為例子)
  - ifconfig //列出所有 network interface 的詳細資料
  - ping 8.8.8.8 //持續地發送 icmp 封包給 8.8.8.8
  - ping fb.com //發送 icmp 封包給 fb.com
  - traceroute fb.com //追蹤本機端到 fb.com 之間每一個節點的狀況
  - mtr fb.com //回傳從本機到 fb.com 比 tracert 更詳細的節點資訊
  - nslookup www.example.com //查詢 www.example.com 的 ip
  - netstat //觀察網路對外連線狀態

回答以下 6 個問題，以下情境皆在 command line 底下，應該如何使用上述工具以解決以下 6 個問題，請截圖並在圖片上標記協助找出問題的線索，並輔以文字說明。

Q1. 如何獲得自己的 MAC Address 和 IP Address? (hint: ipconfig/ifconfig)

Q2. 如何簡單地確定自己電腦是可以連上網際網路? (hint: ping)

Q3 某網頁載入的速度異常的緩慢，在不考慮本機電腦和網頁伺服器的效能問題情況下，如何找出效能瓶頸的節點? (hint: tracert/traceroute)

Q4. 假設在家裡用筆記型電腦走無線網路上網的時候，想要透過 ip 遠端控制實驗室的電腦但是發現頻繁的斷線，簡單陳述一下該如何鎖定問題(可能問題: 我的電腦故障、家裡無線路由器故障、ISP 端故障、學網故障、學校網路故障、實驗室網路故障、實驗室電腦故障) (hint:pathping/mtr)

Q5. 如何觀察到電腦那些 port 是開啟的?

Q6. 如何去找到網址 www.facebook.com 的 IP 位置?(hint: nslookup)

2. 使用 Wireshark 觀察封包，並根據指示回答問題。

- 請上 *http://www-net.cs.umass.edu/wireshark-labs/*下載 Getting Started, v7.0 這一份 PDF 下來操作。
- 回答上述文件中”What to hand in”以下的四個問題。

Q1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Q2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet- listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)

Q3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

Q4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the "*Selected Packet Only*" and *"Print as displayed"* radial buttons, and then click OK.

每題十分，總分一百分

參考文件:

1. http://linux.vbird.org/linux_server/0140networkcommand.php
2. http://www.techrepublic.com/blog/10-things/10-windows-7-commands-every-administrator-should-know/
3. http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/c8319.htm
4. https://www.linode.com/docs/networking/diagnostics/diagnosing-network-issues-

with-mtr