簡易網路流量統計系統建置方案

范修維　　廖鴻圖　　伍啟錄

世新大學資訊管理學系　　世新大學資訊管理學系　　世新大學電算中心

fan@cc.shu.edu.tw　　htliaw@cc.shu.edu.tw　　rick@cc.shu.edu.tw

摘要

教育部目前正積極推動新世代寬頻骨幹網路，使各級學校以更高速的頻寬連接至 TANet 骨幹。為了有效利用新世代寬頻骨幹，防止不當的網路行為，要求各級學校在申請加入之前，都必須完成網路流量統計排行榜的要求。目前大專院校幾乎都使用 Cisco 網路設備，許多網路流量統計軟體也都是建構在其專屬的 netflow 機制上。對於規模較小的中小學而言，它們沒有 Cisco 設備所提供的 netflow 機制，所以這些軟體也都無法使用。如果採用市售的流量統計軟體，高昂的價格也成為沈重的負擔。再者，大部分的流量統計軟體都需要資料庫的輔助，所以也需要功能較強的電腦才能勝任。為了解決這些學校的流量統計需求，我們開發了一套網路流量統計系統，它不需要太高的電腦效能即可完成簡易的流量排行工作，也不需要使用 netflow 的功能來搭配就可獨立完成，並且這套系統完全不需要資料庫，僅需要作業系統及網頁伺服器即可運作，因此幾乎所有常見的系統 (Linux、FreeBSD、Solaris、Window 98/2000) 都可以使用。本文中，我們除了說明整個系統的開發架構外，也說明如何將此系統用於實際的流量統計。對於一些急欲加入新世代寬頻骨幹的學校，只要按照本文的說明進行網路流量統計系統的建置，即可達成教育部所訂定的要求。

關鍵字：網路流量、流量統計。

1. 前言

為了提昇台灣學術網路的速度，並且希望能以較低的成本獲得更高的頻寬，教育部放棄了原先的 ATM 網路架構，改採 Gigabit Ethernet 為主的 MAN 網路架構。其目標為大專院校都能以 Gigabit Ethernet 的方式直接連上 TANet，而中小學亦能以 Fast Ethernet 的方式連接。網路速度的提昇固然得以節省使用者的傳輸時間，獲得更大的使用效能，但相對地也更容易地傳遞不當資訊，產生不當的網路行為。為了有效利用新世代寬頻骨幹，防止不當的網路行為，教育部訂定了一些使用規範及要求，各級學校必須完成這些規範及要求才得以申請加入新世代網路骨幹。這個使用規範之立意非常好，但是其中有二個要求卻不容易作到：一是防治不當網路資訊，二是完成網路流量前三十名統計排行。

對於教育部所訂定的要求，如果有具體的作法或準則，各級學校都非常樂意配合。但是當此要求是一項困難、甚至沒有完善的解決方案時，這個要求只不過是增加各級學校網管人員的負擔罷了。例如：對於不當網路資訊的防治，至今都沒有完善的解決方案，也沒有徹底杜絕的可能。目前雖然已有一些防治色情資訊的網路管制設備問市，但是這些設備仍是以 URL 為主的過濾器，只能防治網頁的瀏覽，對於一些非標準協定 (Port 80) 的地下網站，就沒有過濾的效果。再者，如果沒有定時更新 URL 的資料庫，也無法杜絕新增的色情網站。當然，最大的問題仍然是經費的考量，這類商品的價格大約都在數十萬元左右，對於中小學仍是個沈重的負擔。如果僅是針對 URL 的過濾，其實是不必採購這類的商品，只要使用 Squid Guard[6] 就可以達到相同的功能，但哪些 URL 必須過濾、哪些 URL 可以放行，這卻是問題所在。若是教育部能提供不當資訊的網址，以及建置過濾機制的步驟，相信各級學校都能完全配合。

同樣地，對於網路流量的統計，這個問題教育部也沒有提供一個參考建置方案，必須讓各級學校自行找尋解決辦法。目前已有部分大專院校完成了網路流量的統計，也提供了網路流量統計的程式，但是這些流量統計都是建立於一個前題下：使用 Cisco 的網路設備並且使用專屬的 netflow 機制作統計。如果學校沒有採用 Cisco 網路設備或者該網路設備不提供 netflow 數據統計，這些程式就沒有任何幫助。如果能提供一種簡單、通用的流量統計建置方案供各級學校使用，相信各級學校也一定樂於配合。

在 TANet 2001 研討會中，我們曾提出了一種網路流量統計的建置策略[1]，該流量統計的前題就是以通用為主要考量，不限定於 Cisco 的網路設備，也不需要 netflow 的支援，一般的網路設備都能使用。除了通用的考量外，歷史的追溯能力、任意的統計區間、即時的報表產生是另外的訴求重點，所以整個系統就變得較為複雜。如果只要完成校內流量前三十名的統計排行，使用該程式的部分

功能就得以完成。

我們把原來的系統作了大幅的簡化，僅針對主機流量排行作統計，並且放棄了即時運算的能力，改採背景定時計算、定時報表產生的方式，使得整個系統變得非常單純。簡化後的系統對於硬體的要求也更低，相對地也減低了建置成本。

為了讓中小學在進行網路流量的統計排行時，能夠有個建置的參考依據，我們提供了一套簡易型的網路流量統計建置機制，不僅提供整個系統的原始程式，同時也提供各種平台的可執行檔。各級學校只要按照本文的說明進行建置，都可以完成流量排行的統計工作。

在接下來的章節裡，我們將說明建置網路流量統計所採用的網路架構。整個程式的開發重點，我們將在第三節說明，對於有興趣作進一步研究或開發的人員得以更順利地接續工作。在第四節中，我們將一步步地說明系統設定步驟以及參考的設定範例，網管人員只要按此步驟就可以完成網路流量的統計排行。最後，我們在第五節中作簡單的結論。

2. 網路架構

我們的網路流量統計系統是採用封包擷取的方式，計算出實際的網路流量。這種方式與傳統的網路監聽技術一樣，都需要將封包擷取系統直接連接在網路上。如果要統計學校對外的網路流量時，就必須放置於學校對外出入口。一般中小學典型的網路架構如圖 1 所示，此時可以加裝集線器以 T 接的方式接上封包擷取系統 (如圖 2)。或者，如果所使用的 Core Switch 具有 Span (Switched Port ANalyzer) 功能時，也可以利用 Span 功能將封包重導至 Monitor Port，讓封包擷取系統直接讀取網路封包 (如圖 3)。

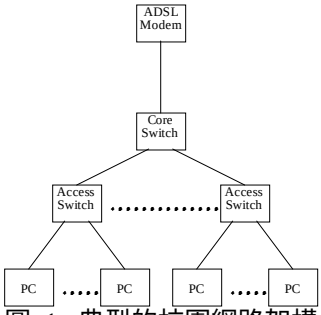

圖 1. 典型的校園網路架構

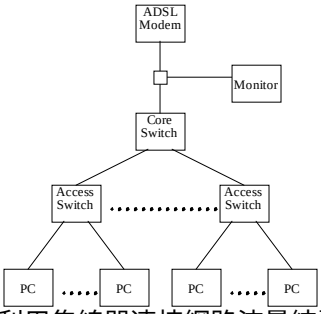

圖 2. 利用集線器連接網路流量統計系統

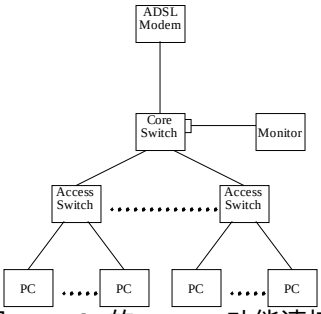

圖 3. 利用 Switch 的 SPAN 功能連接網路流量統計系統

須注意的是，圖 2 的連接方式一定要使用集線路，不可以改用 Switch，否則網路流量統計系統將無法讀取網路傳輸封包。

擔任網路流量統計系統的電腦硬體要求並不高，只要一般等級的電腦加上一張網路卡即可。軟體方面也只需要安裝一般的作業系統 (Linux、FreeBSD、Solaris、Windows98/2000) 及網頁伺服軟體 (如 Apache)。記憶體的需求也不大，64MB 應已足夠一般中小學的使用環境 (如果校內大量使用 Private IP，則需要較大的記憶體)。至於硬碟的容量，如果只保持七天的記錄資料，一顆 3GB 的硬碟都已足夠放置整個系統及統計資料。

我們的系統共分為二部分，一個是封包擷取系統，隨時監聽網路傳輸，並且以一分鐘為一個統計單位，將每分鐘的統計結果寫入硬碟的檔案中。另一個是資料統計系統，以定時的方式在背景計算，將置於硬碟的統計資料作累計及排序，再將結果以 HTML 格式的檔案置於網頁目錄中。

3. 系統架構

要從網路上擷取封包並不是件困難的事，只要利用 libpcap[2] 程式庫即可輕易達成。該程式庫原先是在 Unix 系統發展，現在也已經移植到 Windows 平台[3]，使得封包擷取系統的開發變得更為容易，也具有更高的可移植性。

抓取到網路封包後，我們就應該針對 Layer 2、Layer 3、Layer 4 的通訊協定進行封包分析：

1. Layer 2 封包分析：

由於我們只關心學校至 TANet 的網路封包，而這些封包絕大部分的型態都是 Ethernet Version 2，所以我們只需要把 Type 0800 的封包讀取即可。至於 ARP、RARP 封包並不會造成 TANet 的流量，可不予理會。

2. Layer 3 封包分析：
   在絕大部分的情形下，學校至 TANet 的網路封包都是 TCP/IP 傳輸協定，為了簡化問題，我們也只讀取這部分的封包。在分析之後，可以得知該封包的型態 (TCP、UDP、ICMP) 以及來源位址 (SrcIP) 與目的位址 (DstIP)。
3. Layer 4 封包分析：
   如果所得到的封包是 TCP 或 UDP 封包，就可以再進一步取得該協定的通訊埠號 (SrcPort、DstPort)。

根據上述封包的分析，我們可以整理出下列的表格 (如表 1)：

表 1. 網路流量統計表

流水號	封包型態	校內電腦 IP	校內電腦 Port	校外電腦 IP	校外電腦 Port	流入量 Bytes	流出量 Bytes	流入量 Pkts	流出量 Pkts
1									
2									
3									
…									

每當我們抓取一個網路封包時，就將結果填入表格：

1. 封包型態可區分為 ICMP、TCP 及 UDP，其它型態的封包則可以忽略。
2. 按照學校所分配的網路位址作為範圍，若網路封包的來源位址或目的位址屬於學校所配置的位址範圍，即視為校內電腦，否則即為校外電腦。
3. 每一個封包都會產生一個 Packet 的流量及若干 Bytes 的流量，至於該流量屬於流入量還是流出量，就按照封包來源位址及目的位址作判斷：
   (1) 若來源位址是校內電腦且目的位址是校外電腦，屬於流出量。
   (2) 若來源位址是校外電腦且目的位址是校內電腦，屬於流入量。
   (3) 若來源位址與目的位址均屬於校內電腦，此屬於內部流量，可不予計算。
   (4) 若來源位址與目的位址均屬於校外電腦，此情形不應該發生 (亦不予計算)。
4. 填入資料時，按照封包型態、校內電腦 IP、校內電腦 Port、校外電腦 IP 及校外電腦 Port 作依據，若五個欄位都相同時，則把流量加入相對的欄位，否則就建立一筆新的資料項。

上述表格會隨著時間而增長，為了保持良好的效能以及統計的精確度，最好不要將統計時間拉得太長。建議可以以一分鐘為單位，將每分鐘的統計結果寫入檔案中，這樣統計的表格就不會過大。由於我們完全不使用資料庫，所以上述表格必須以 C 語言的「結構」或 Pascal 語言的「紀錄」留存於記憶體中。為了提高效能，建議採用「高度平衡二元樹」作為表格的增加與累計。

如果要簡化程式，也可以將表一作些刪減 (如表 2)：

表 2. 簡化後的網路流量統計表

流水號	校內電腦 IP	流入量 Bytes	流出量 Bytes	流入量 Packets	流出量 Packets
1					
2					
3					
…					

簡化後的表格只保留校內電腦 IP 位址作為索引欄位。由於學校所分配到的 IP 位址不多，表格的處理也變得非常容易，只要建構一個固定大小的陣列，每個校內電腦 IP 位址都配置一個資料項，就可以快速地將統計資料累計到表格中。如此即可省去「高度平衡二元樹」的撰寫，又可提高整個程式的執行效能。

至於要採用表一標準型式的流量統計方式，還是要採用表二簡化後的流量統計方式，則有不同的考量重點。簡化後的統計方式可以讓程式變得非常簡單，開發時程可以縮短，也可以使用更低階的電腦來執行，但是缺點是所提供的訊息較少，只能完成校內電腦的流量排行。如果僅要完成教育部所指定的要求，使用這項簡化後的統計方式就已足夠。反之，使用標準的統計方式需要花費較多的時間開發程式，困難度也比較高，但相對地可以提供較多的資訊，不僅可以提供校內電腦的流量排行，也可以提供網路協定分佈、校內外主機互傳排行…等重要資訊。

我們可以利用系統的 Cron Table 以定時的方式啟動資料統計系統，把先前所收集到的資料作整理與統計，再將結果以 HTML 的格式輸出。

統計時，只需給予統計的起訖時間，統計程式就自動到檔案堆裡讀取相對應的統計檔，並進行表格的合併。由於這部分屬於背景程式，沒有 Real-Time 運算的壓力，所以可以很單純地一個個檔案進行累加。這種統計方法雖然不是很理想，但是對於每日排行、甚至每週排行都已足夠。

4. 建置範例

按照上述的原理，我們撰寫了二支程式：recorder 與 reporter，分別用來處理封包的擷取及資料的統計。在使用彈性的考量下，我們提供了一個設定檔以滿足不同的使用需求。為了方便系統的安裝，我們也提供了各種平台的 tar ball 檔案，供使用者直接安裝。以下，我們就以 Linux 系統為例，說明如何建置一套簡易型的網路流量系統。

4.1 系統安裝

系統安裝非常簡單，只需要在 /usr/local/nm-lite/ 目錄下解開 tar ball 即可，參考指令如下：

```
mkdir -p /usr/local/nm-lite
cd /usr/local/nm-lite
lynx
http://cc.shu.edu.tw/~nm/download/nm-lite-linux-1.1.1.tar.gz
tar -xvzf nm-lite-linux-1.1.1.tar.gz
```

4.2 系統設定

在 /usr/local/nm-lite/etc/config.nm 檔案中具有許多設定項目，其參考內容如下：

```
[global]
recording_dev        = eth0
log_dir              = /usr/local/nm-lite/log
raw_dir              = /usr/local/nm-lite/spool/raw
realm                = 10.0.0.0     ~ 10.255.255.255
realm                = 172.16.0.0   ~ 172.31.255.255
realm                = 192.168.0.0  ~ 192.168.255.255
realm                = 192.192.148.0 ~ 192.192.159.255
vip                  = 10.0.0.0     ~ 10.255.255.255
vip                  = 172.16.0.0   ~ 172.16.255.255
umask_dir            = 0700
umask_file           = 0600
TopN                 = 30
field_inbyte         = on
field_outbyte        = on
field_totalbyte      = off
field_inpacket       = on
field_outpacket      = on
field_totalpacket    = off
field_avg_inbyte     = on
field_avg_outbyte    = on
field_avg_totalbyte  = off
table_sort_inbyte    = on
table_sort_outbyte   = on
table_sort_totalbyte = off
table_sort_inpacket  = off
table_sort_outpacket = off
table_sort_totalpacket     = off
table_sort_ip = off
report_title  = <head>
report_title  = <title>世新大學網路流量統計</title>
report_title  = <meta http-equiv="Content-Type"
content="text/html; charset=big5">
     report_title    =      <link    rel="stylesheet"
type="text/css" href="style.css">
     report_title    = </head>
     report_title    = <h1>網 路 流 量 統 計
     report_title    = <img
src="http://cc.shu.edu.tw/cgi-bin/Count.cgi?df=nm-lite-general.dat|comma=T|chcolor=T"
align=abscenter></h1>
```

現在針對各項參數作細部說明：

1. recording_dev
   指定抓取封包的網路卡介面名稱。這個介面卡的名稱就是由 ifconfig 指令所顯示出來的界面 (不含 ip-alias 虛擬界面)。在 Linux 系統中，第一張網路卡名稱即為 eth0。
2. log_dir
   指定系統紀錄檔的目錄。程式執行時如果遇到問題 (如檔案毀損)，就會將結果輸出於這個目錄中。
3. raw_dir
   指定原始紀錄的存放目錄。這個目錄也就是封包擷取程式所產生的統計資料檔，會按照「年、月、日、時」的方式建立子目錄，再把每分鐘的統計檔案放在相對應的目錄中。
4. realm
   指定學校所使用的 IP 範圍。如果學校所配置的 IP 位址不是連續的範圍，就以多個敘述來指定。若學校校內同時啟動 Private IP，本程式也可以將其紀錄下來。
5. vip
   指定不列入統計項目的 IP 範圍。或許某些特別人物或某些特定因素不能將某些 IP 列入統計時，就利用此參數把該 IP 位址的流量過濾掉。
6. umask_dir
   指定資料目錄的存取權限。在產生原始紀錄檔案時，建立目錄所使用的 umask。
7. umask_file
   指定資料檔案的存取權限。同上，但此處為檔案的 umask。
8. TopN
   指定報表的輸出量。也就是產生排行榜的數量 (0 代表無限制)。
9. field_xxxxxx
   指定各欄位的輸出與否。我們提供了 Bytes、Packets 的統計，包含流入、流出及總量、平均量等資訊。
10. table_xxxxxx
    指定各表格的輸出與否。這是按照不同欄位排序後的輸出結果。
11. report_title
    可修改輸出報表的表頭。利用這個功能，可以讓報表具有不同的背景或外觀。

4.3 啟動封包擷取系統

啟動封包擷取系統的方法非常簡單，只要鍵入「/usr/local/nm-lite/bin/recorder -b」即可。其中 -b

參數代表以 daemon 執行。為了讓系統開機後也能自動載入執行，請將上述指令加入 /etc/rc.d/rc.local 檔案尾端。

4.4 啟動資料統計系統

在 /usr/local/nm-lite/bin/ 目錄下的 reporter 程式可以將流量紀錄檔整理成 html 檔案輸出，可以使用「reporter [5min | 10min | hour | day | week | month | year]」來統計最近五分鐘、十分鐘、一小時、一日、一週、一個月、一年的統計結果，也可以使用「reporter starting_time ending_time」來指定統計的起訖時間。

我們可以利用「crontab -e」來編輯 Cron Table，讓系統固定每五分鐘、一小時、一日、一星期都更新一次，其內容如下：

```
1,6,11,16,21,26,31,36,41,46,51,56 * * * *
/usr/local/nm-lite/bin/reporter hour >
/usr/local/nm-lite/html/hour.html 2>&1
1 * * * * /usr/local/nm-lite/bin/reporter hour
> /usr/local/nm-lite/html/last-hour.html 2>&1
1 * * * * /usr/local/nm-lite/bin/reporter day >
/usr/local/nm-lite/html/today.html 2>&1
1 0 * * * /usr/local/nm-lite/bin/reporter day >
/usr/local/nm-lite/html/yesterday.html 2>&1
1 0 * * * /usr/local/nm-lite/bin/reporter week
> /usr/local/nm-lite/html/week.html 2>&1
1 0 * * 0 /usr/local/nm-lite/bin/reporter week
> /usr/local/nm-lite/html/last-week.html 2>&1
```

4.5 建立流量網頁

請在系統的網頁目錄下，以 symbolic link 在主網頁目錄下建立 lite 鏈結，指向 /usr/local/nm-lite/html 目錄，然後在該目錄下建立 index.html 檔，內容如下：

```
<head>
<meta                    http-equiv=Content-Type
content="text/html; charset=big5">
<title>世 新 大 學 網 路 流 量 排 行 榜</title>
</head>
<body bgcolor=#EBC79E>
<h1>世 新 大 學 網 路 流 量 排 行 榜</h1>
<ul>
<li><a
href="http://nm.shu.edu.tw/lite/hour.html">最
近 一 小 時 排 行 榜</a>   (每 五 分 鐘 更 新)
<li><a
href="http://nm.shu.edu.tw/lite/last-hour.htm
l">前 小 時 排 行 榜</a>   (每 小 時 更 新)
<li><a
href="http://nm.shu.edu.tw/lite/today.html">
最 近 一 日 排 行 榜</a>   (每 小 時 更 新)
<li><a
href="http://nm.shu.edu.tw/lite/yesterday.htm
l">昨 日 排 行 榜</a>            (每 日 更 新)
<li><a
href="http://nm.shu.edu.tw/lite/week.html">最
近 一 週 排 行 榜</a>            (每 日 更 新)
<li><a
href="http://nm.shu.edu.tw/lite/last-week.htm
l">上 週 排 行 榜</a>            (每 週 更 新)
</ul>
```

4.6 系統測試

在啟動封包擷取系統之後，於 /usr/local/nm-lite/spool/raw/ 目錄下就會產生「年、月、日、時」的子目錄，並且在最底層的子目錄會以每分鐘的速率產生流量統計檔案。另外，在 /usr/local/nm-lite/html/ 目錄內也會以五分鐘的速率更新網頁檔案。在產生網頁檔案後，就可以使用瀏覽器去觀察流量統計的結果 (如圖 4)。

由於我們的流量統計系統採用封包擷取的方式進行統計，或多或少都會有封包漏失的情形，只要封包漏失的情形不算大，都算是合理的範圍。若要測試封包的漏失量，可以使用另一台電腦以 Sniffer[5] 軟體進行比較，以判斷其資料的差異性。或者，也可以使用 MRTG[4] 的流量統計圖作為比較，看看流量大小的曲線是否合理。

在進行比較時，須瞭解不同系統的一些差異性，例如：我們的系統只統計校內通往校外的交互流量，校內電腦互傳所產生的流量不納入統計。如果使用 Sniffer 或 MRTG 的流量統計，則可能將所有的網路流量都納入計算。另外，不同系統對於網路封包的長度計算方式可能也不太一樣，例如：是否以 Layer 2 的封包長度作計量，還是以 Layer 3 的封包長度作計量？若以 Layer 2 的封包長度作計量，其封包表頭及表尾的 CRC 檢查碼是否納入計算？若以 Layer 3 的封包長度作計量，是否只計算 Payload 長度，還是連同表頭一起計算？不同計算的基準都會造成計算上的差異。

本校目前使用一台 Pentium III 700MHz 的電腦作為流量統計系統，該電腦主要負責即時的流量統計運算，所以系統效能要求比較高，配有 1GB 的記憶體及 70G * 2 的硬碟。我們在該電腦上順便執行這套簡易型的網路流量統計系統，一切都非常順利。本校所配置的 IP 範圍共有 12 個 Class C 網段，並同時啟用 16 個 Class B 網段，所以 IP 範圍並不算小。

目前我們僅完成 T1 的連接測試，並且已正試上線使用，更高的速率則因為缺乏適當的環境無法進行。但是根據使用的經驗判斷，這樣的系統就算用於 Fast Ethernet 的環境下仍是游刃有餘。至於在 Gigabit Ethernet 的環境是否仍能正常的運作，這就是個未知數。如果真的無法應付，我們將考慮採用階層式的統計架構來解決這個統計問題。

圖 4. 簡易的網路流量統計結果

4.7 歷史回溯與系統維護

由封包擷取系統所產生的每分鐘統計資料會存放於 /usr/local/nm-lite/spool/raw/ 目錄下，這些資料並不會自動刪除。保留這些資料的主要目的是為了提供歷史回溯的功能。如果網管人員有需要，隨時可以使用 reporter 程式對歷史資料進行統計。除了流量統計之外，網管人員還可以利用這些資料作進一步的分析，以得到更多、更有用的資訊。當然，如果網管人員不需要保留歷史資料，也可以自行設定 Cron Table，定時將過期的資料刪除。

5. 結論

我們所開發的簡易網路流量統計系統只需要使用一台普通的個人電腦就得以完成，其硬體配備也不用太高，非常適合於中小學的校園環境使用。網管人員只要按照本文的建置範例進行建置，就可以完成教育部所訂定的網路流量統計排行的要求。對於有進一步研究興趣的人員，我們也提供了系統開發的相關資料，並且提供原始程式[7]，相關人員可以藉由這些資訊作更進一步的探討。

參考文獻

1. 范修維、廖鴻圖、邱孟佑、伍啟錄，“網路流量分析系統之建置及應用”，TANet 2001 台灣區網際網路研討會，pp. 419-424，2001 年。
2. http://ftp.ee.lbl.gov/
3. http://netgroup-serv.polito.it/winpcap/
4. http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
5. http://www.sniffer.com/
6. http://www.squidguard.org/
7. http://cc.shu.edu.tw/~nm/