

教育部「5G行動寬頻人才培育跨校教學聯盟計畫」

5G行動網路協定與核網技術聯盟中心

課程:5G垂直應用網路

實驗一

開源碼小基站實驗平台 之建置與量測

副教授：吳俊興

助教：胡詠翔

國立高雄大學 資訊工程學系

Outline

- 實驗目的及實驗內容
- 背景知識
- 實驗環境
- Stage 1: 環境架設
- Stage 2: srsLTE 及 ZeroMQ 編譯安裝
- Stage 3: srsLTE 執行及測試
- Stage 4: srsLTE 封包觀測
- 總結及問題

實驗目的

- 建置開源碼小基站及小核網系統
- 建置UE及設定5G電腦裝置並安裝應用程式以熟悉連線量測工具

實驗內容

- 環境架設
 - 進行 Ubuntu 的系統架設以熟悉 Linux 環境
 - 進行 Linux NAT 架設及路由設定以符合實驗環境
- srsLTE 及 ZeroMQ 編譯安裝
- srsLTE 執行及測試
 - 設定及啟動 srsLTE
 - 進行 Downlink 及 Uplink 的 ICMP 與 TCP 測試
- srsLTE 封包觀測
 - 使用 Wireshark 進行 S1-MME 控制平面的封包觀測
 - 使用 Wireshark 進行 S1-U 及 SGi 使用者平面的封包觀測

Outline

- 實驗目的及實驗內容
- 背景知識
 - srsLTE
 - ZeroMQ
 - TUN device
 - SCTP
 - NAS
 - GTP
- srsLTE 實驗環境
- Stage 1: 環境架設
- Stage 2: srsLTE 及 ZeroMQ 編譯安裝
- Stage 3: srsLTE 執行及測試
- Stage 4: srsLTE 封包觀測
- 總結及問題

背景知識 - srsLTE

- srsLTE為一開源的LTE系統，包含EPC、eNB及UE的實作
 - srsEPC 實作的單元有MME、HSS、S-GW及P-GW
 - eNB實作了如MAC、RLC、PDCP、RRC、NAS、S1AP及GW等協定層
 - eNB及UE間的無線電連線可以選用如USRP B210等SDR或是ZeroMQ
 - eNB及UE皆支援eMBMS
- 本實驗使用srsLTE作為EPC、eNB及UE的執行軟體

背景知識 - ZeroMQ

- ZeroMQ是一個 Messaging Library
 - 使用ZeroMQ Message Transport Protocol作為傳輸層協定
 - ZMTP的底層可以是TCP、UDP或是IPC
 - 支援多種傳輸模式，如REQ-REP、PUB-SUB、PUSH-PULL等
- 本實驗使用ZeroMQ作為srsLTE的無線電訊號傳送媒介
- srsLTE 預設採用 REQ-REP 模式的 ZeroMQ socket
 - REQ 用於無線電訊號的 Rx，會發送請求給 Tx
 - REP 用於無線電訊號的 Tx，接受 Rx 的請求後回覆無線電訊號的 Sample
 - REP 並不一定要在 REQ 建立前建立好
 - 若 REQ 無法連線到指定的 REP，則 REQ 會重新嘗試連線

背景知識 – TUN Device

- 為 Linux 下的一種 L3 虛擬網路裝置, 具有IP位址。
 - 任何送進 TUN 的封包皆可被連接在該裝置上的 Process 讀取
 - 通常用在 VPN 裡, 將原始的 IP 流量封裝入 VPN 協定內後再透過實體網路介面傳送出去, 如 OpenVPN
- srsLTE用TUN來將其內部的通訊協定層封裝為一個L3網路裝置, 使得從UE的應用層看起來為一通往 Internet 的 IP Gateway
- 本實驗會對srsLTE產生的TUN裝置進行使用者平面的資料收送, 也會設定NAT使其能與實體網路介面連接

背景知識 – SCTP

- Stream Control Transmission Protocol, 流控制傳輸協定
- 與 TCP、UDP 一樣為傳輸層協定
 - 訊息導向的傳輸層協定
 - 提供可靠且有序的高速傳輸
 - 從 PSTN 的 SS7 演化而來
 - 可以進行 Selective ACK
 - 多重聯外線路的支援使其得以進行網路容錯
- srsLTE 的 S1-MME 使用 SCTP 作為傳輸層協定
- 本實驗會看到 SCTP 如何建立及銷毀連線，也會看到 eNB 及 MME 如何透過 SCTP 確認連線仍然存在

背景知識 – NAS

- Non-access stratum, 非接入層
 - UE和MME間的控制層
- 本實驗會看到的NAS層功能
 - UE連接處理
 - UE身分驗證
 - UE認證
 - 安全協商與控制
 - EMM 訊息傳遞
 - UE離線處理

背景知識 – S1AP

- S1 Application Protocol, S1應用協定
 - S1的控制層協定
- 本實驗會看到的S1AP功能
 - eNB和MME間的信令傳遞
 - S1介面的建立
 - 傳遞NAS的信令
 - UE Context 的建立及銷毀

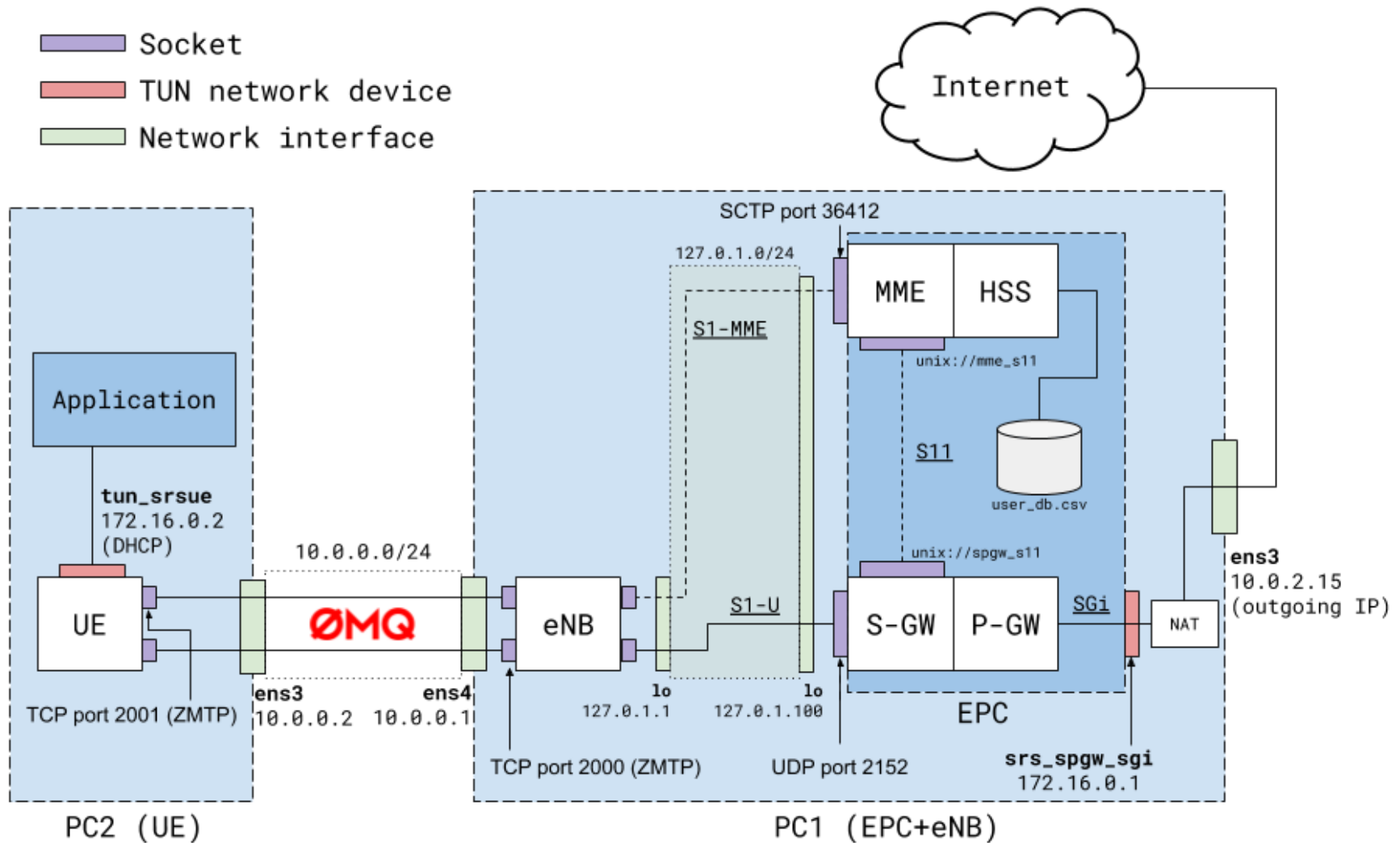
背景知識 – GTP-U

- GTP-User Data Tunneling, GPRS隧道協定-使用者資料隧道
 - 為eNB和S-GW間以及S-GW和P-GW間的使用者平面隧道
 - 透過隧道封裝資料來達成移動性
- 本實驗會看到S1-U所傳送的使用者平面封包使用GTP-U封裝，並在P-GW離開GTP-U的隧道同時還原成原始資料

Outline

- 實驗目的及實驗內容
- 背景知識
- 實驗環境
 - 開源碼小基站實驗架構
 - 軟硬體環境-硬體
 - 軟硬體環境-軟體
- Stage 1: 環境架設
- Stage 2: srsLTE 及 ZeroMQ 編譯安裝
- Stage 3: srsLTE 執行及測試
- Stage 4: srsLTE 封包觀測
- 總結及問題

開源碼小基站實驗架構



軟硬體環境—硬體

*eNB與UE以乙太網路相接

名稱	規格	數量	目的
EPC+ eNB	電腦型號： ASUS VivoMini UN65H	1	啟動 MME,HSS,S- GW,P-GW,eNB
	乙太網路卡	2	讓 eNB 透過 ZeroMQ 與 UE 溝通
UE	電腦型號： ASUS NB M580V	1	模擬 UE
	乙太網路卡	1	讓 UE 透過 ZeroMQ 與 eNB 溝通

軟硬體環境—軟體

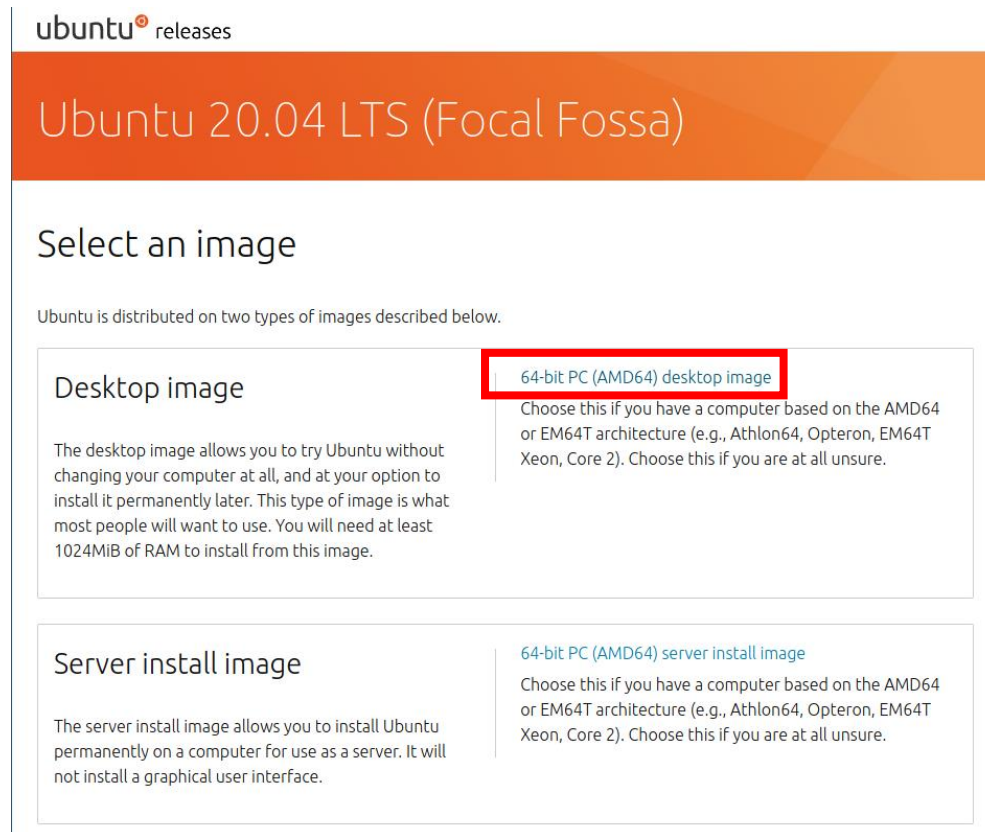
名稱	軟體	版本
EPC+ eNB	OS : Ubuntu	Ubuntu 20.04
	srsLTE	srsLTE 20.04.1 c892ae56be5302eaae5ca00e270efc7a5ce6fbb2
UE	OS : Ubuntu	Ubuntu 20.04
	srsLTE	srsLTE 20.04.1 c892ae56be5302eaae5ca00e270efc7a5ce6fbb2

Outline

- 實驗目的及實驗內容
- 背景知識
- 實驗環境
- Stage 1: 環境架設
 - Step1: Ubuntu 安裝
 - Step2: Ubuntu 設定
 - Step3: Ubuntu 初次使用
 - Step4: 軟體安裝
 - Step5: 網路設定
- Stage 2: srsLTE 及 ZeroMQ 編譯安裝
- Stage 3: srsLTE 執行及測試
- Stage 4: srsLTE 封包觀測
- 總結及問題

Step1-1 Ubuntu 安裝(下載映像檔)

至 <https://releases.ubuntu.com/20.04/> 點選 64-bit PC (AMD64) desktop image 下載 Ubuntu 20.04 Desktop 映像檔



ubuntu[®] releases

Ubuntu 20.04 LTS (Focal Fossa)

Select an image

Ubuntu is distributed on two types of images described below.

<h4>Desktop image</h4> <p>The desktop image allows you to try Ubuntu without changing your computer at all, and at your option to install it permanently later. This type of image is what most people will want to use. You will need at least 1024MiB of RAM to install from this image.</p>	64-bit PC (AMD64) desktop image <p>Choose this if you have a computer based on the AMD64 or EM64T architecture (e.g., Athlon64, Opteron, EM64T Xeon, Core 2). Choose this if you are at all unsure.</p>
<h4>Server install image</h4> <p>The server install image allows you to install Ubuntu permanently on a computer for use as a server. It will not install a graphical user interface.</p>	64-bit PC (AMD64) server install image <p>Choose this if you have a computer based on the AMD64 or EM64T architecture (e.g., Athlon64, Opteron, EM64T Xeon, Core 2). Choose this if you are at all unsure.</p>

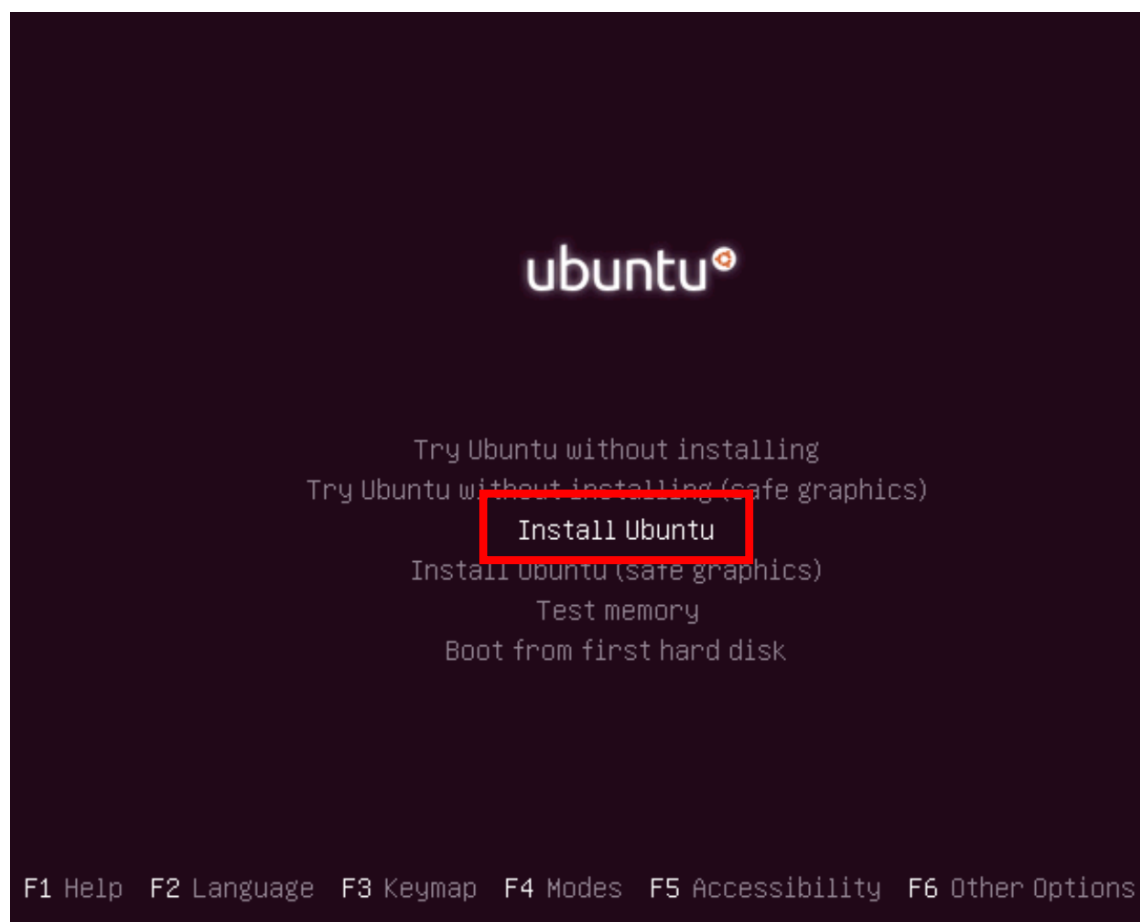
Step1-2 Ubuntu 安裝(語言選單)

使用映像檔開機後在語言選單選擇“English”



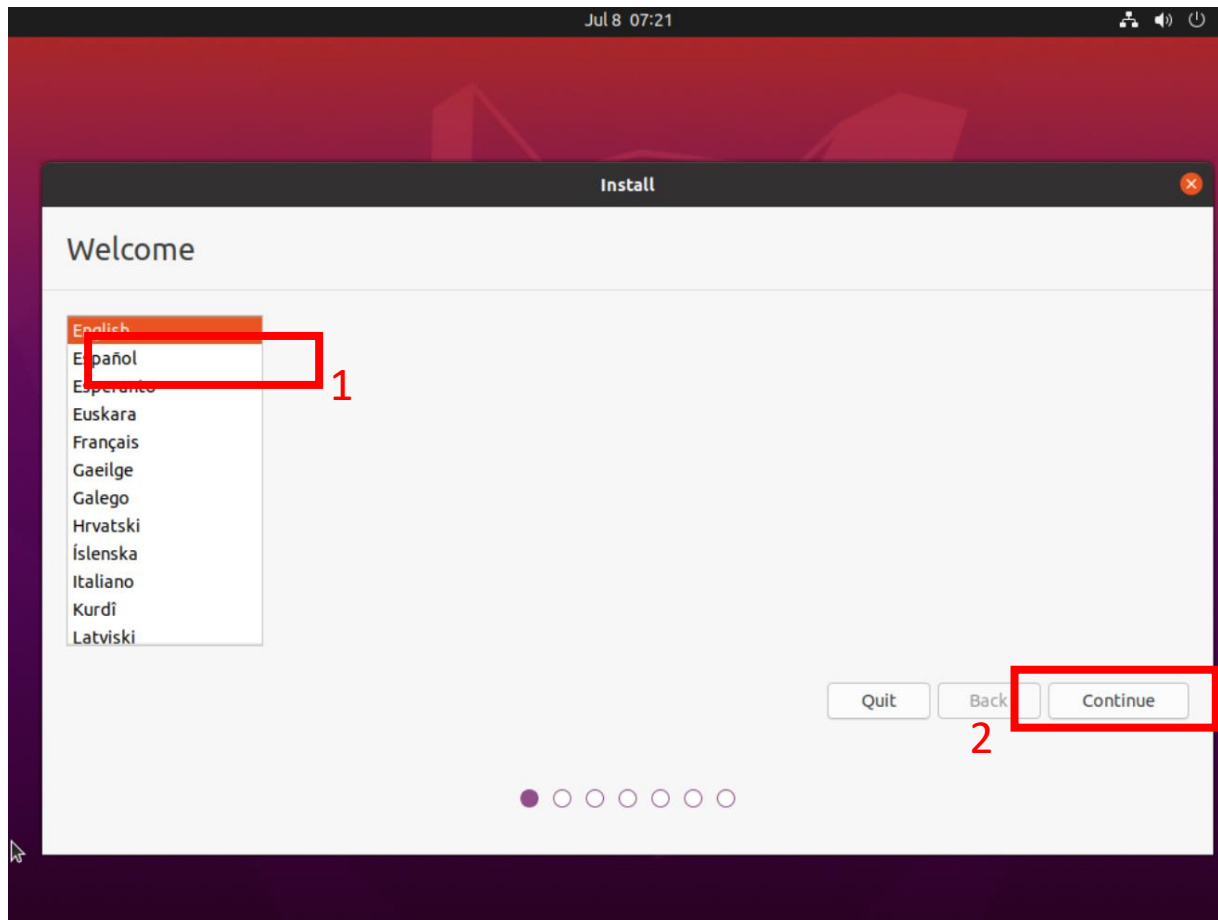
Step1-3 Ubuntu 安裝(開機選單)

在開機選單選擇“Install Ubuntu”



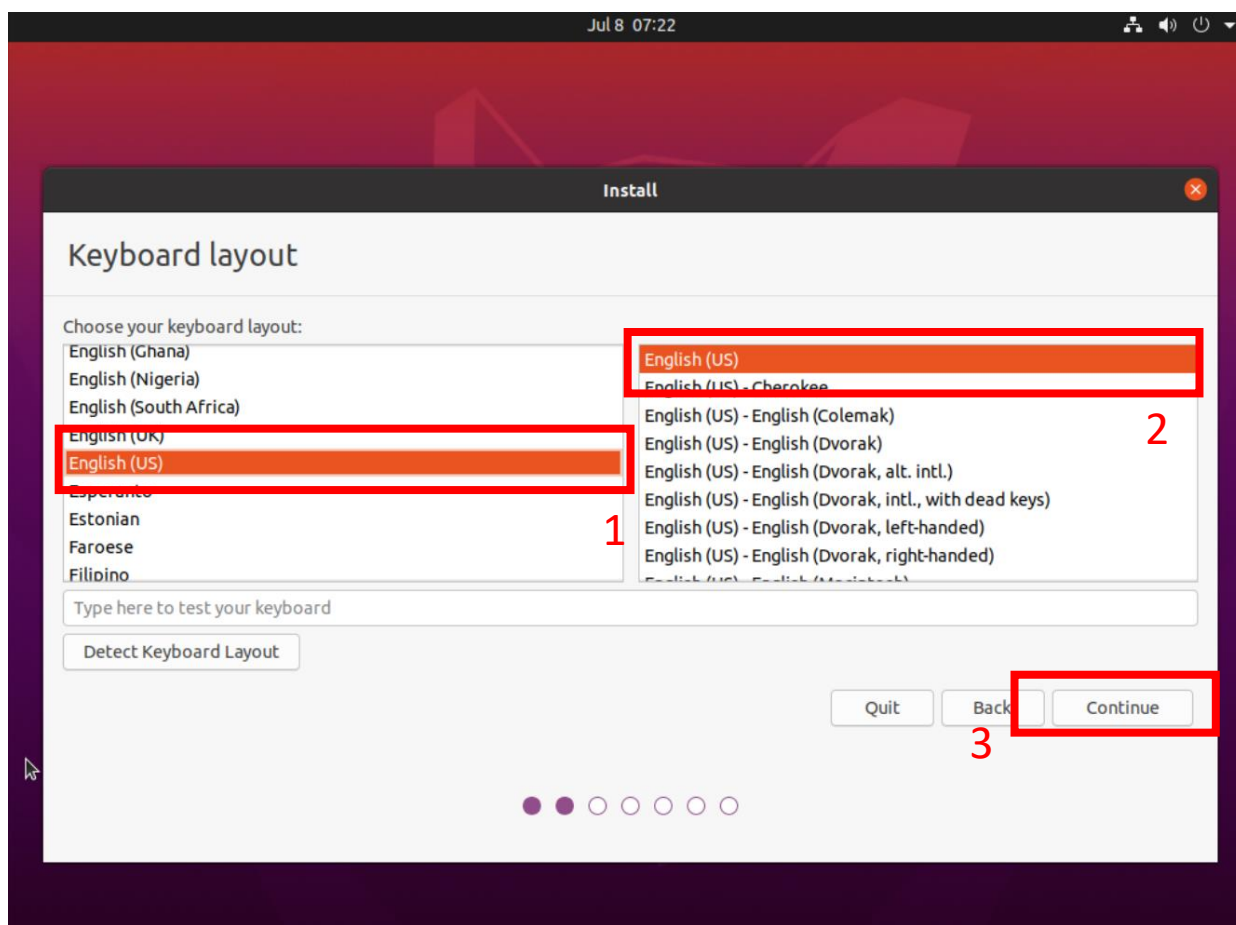
Step1-4 Ubuntu 安裝(語言選擇)

在系統語言選單選擇“English”後點選“Continue”



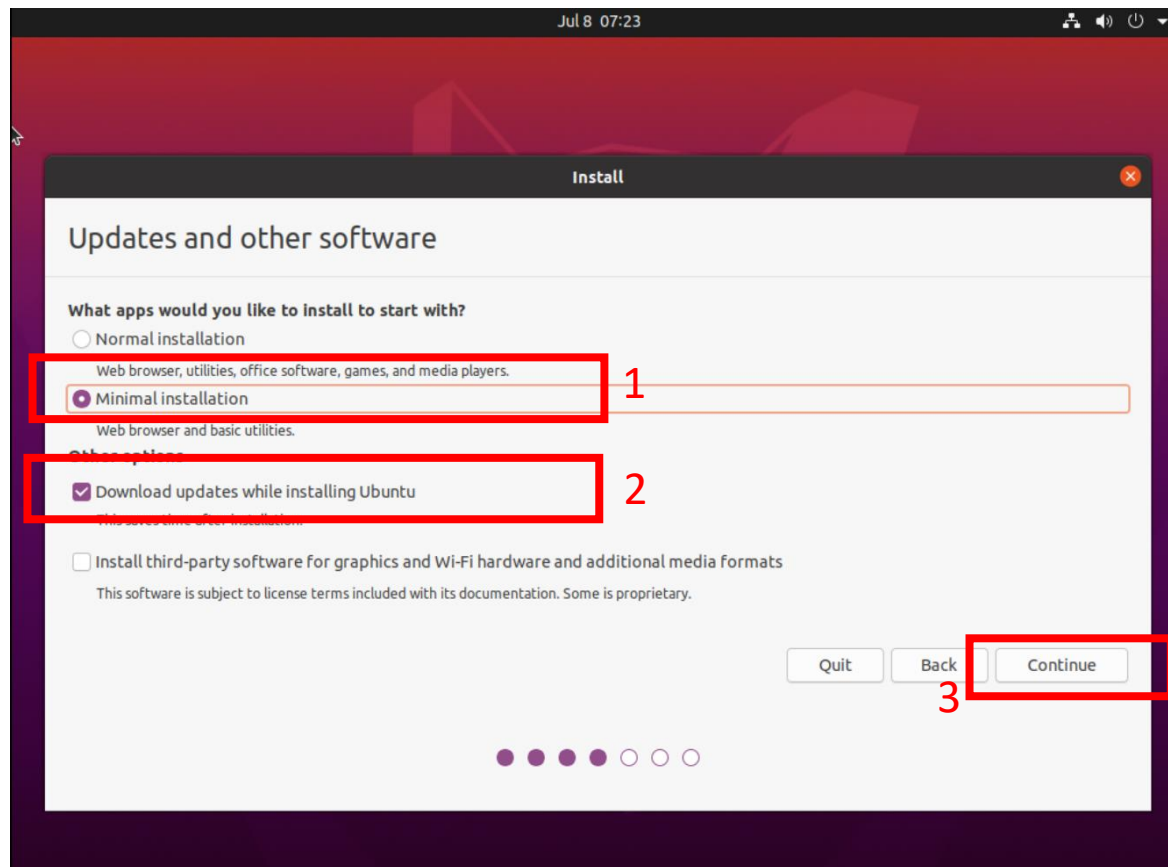
Step1-5 Ubuntu 安裝(鍵盤配置)

在鍵盤配置選單選擇“English(US)”後點選“Continue”



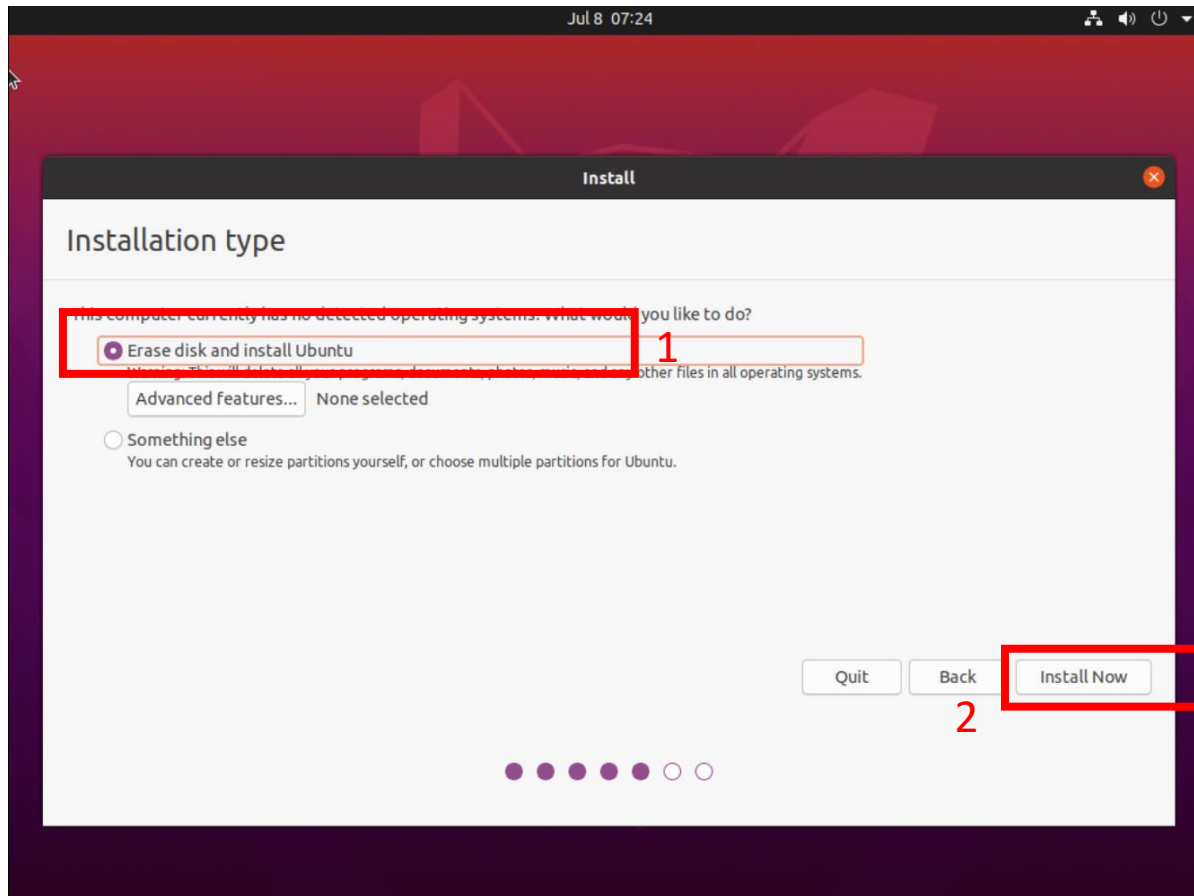
Step1-6 Ubuntu 安裝(套件選擇)

在套件選單選擇“Minimal Installation”及“Download updates while installing Ubuntu”後點選“Continue”



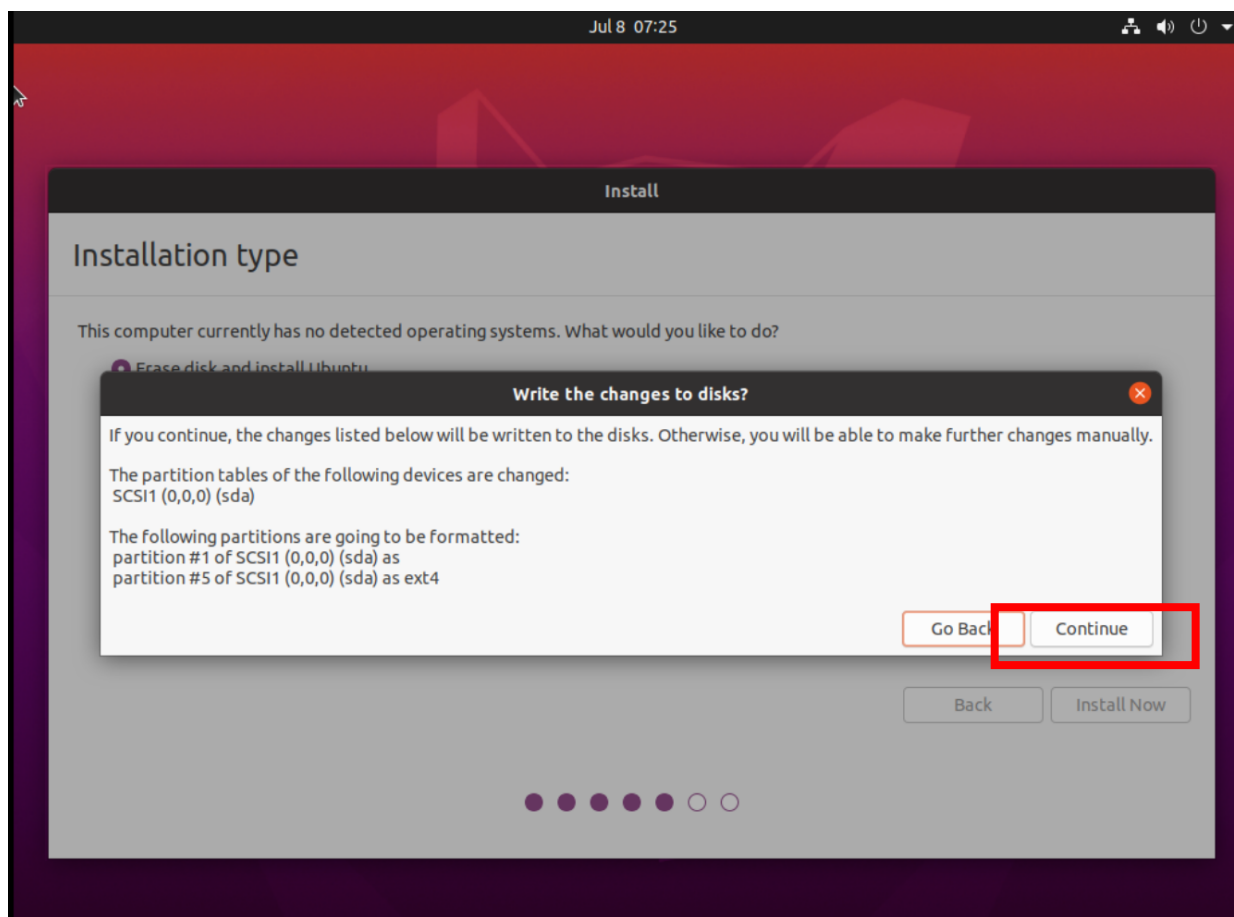
Step2-1 Ubuntu 設定(磁碟分區)

在磁碟分區選單選擇“Erase disk and install Ubuntu”後點選
“Install Now”



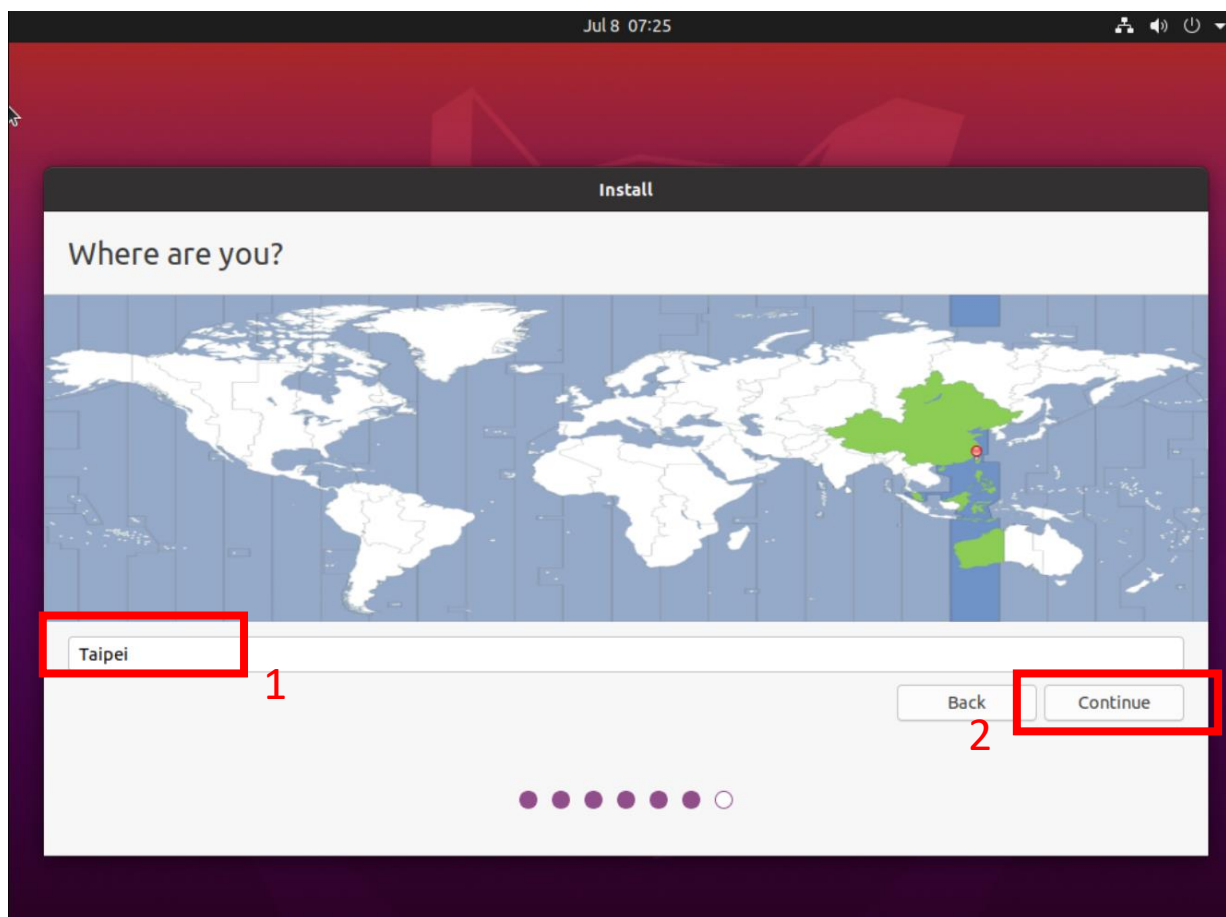
Step2-2 Ubuntu 設定(確認分區)

於彈出的提示框中點選“Continue”



Step2-3 Ubuntu 設定(時區設定)

在時區選單中選擇“Taipei”後點選“Continue”



Step2-4 Ubuntu 設定(使用者設定)

在使用者設定表單中填入途中的資料後點選“Continue”

*註:本範例的密碼為123456

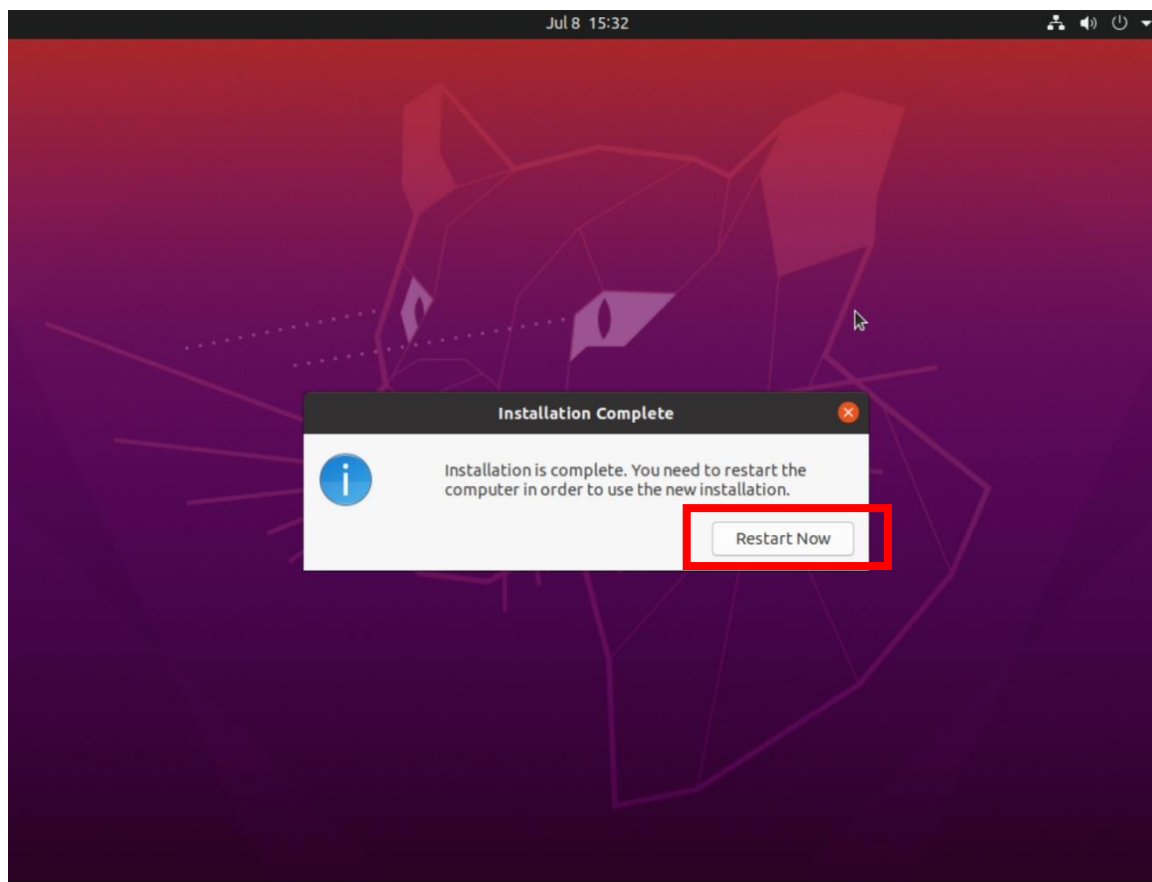
The screenshot shows the 'Who are you?' screen in the Ubuntu installer. The form is titled 'Who are you?' and contains the following fields and options:

- Your name: user (with a green checkmark)
- Your computer's name: Lab01 (with a green checkmark). Below this is the text: 'The name it uses when it talks to other computers.'
- Pick a username: user (with a green checkmark)
- Choose a password: (with a green checkmark and the text 'Fair password')
- Confirm your password: (with a green checkmark)
- Log in automatically (selected with a radio button)
- Require my password to log in (unselected with a radio button)

The 'Continue' button is highlighted with a red box and the number 2. A red box labeled 1 encloses the entire form area.

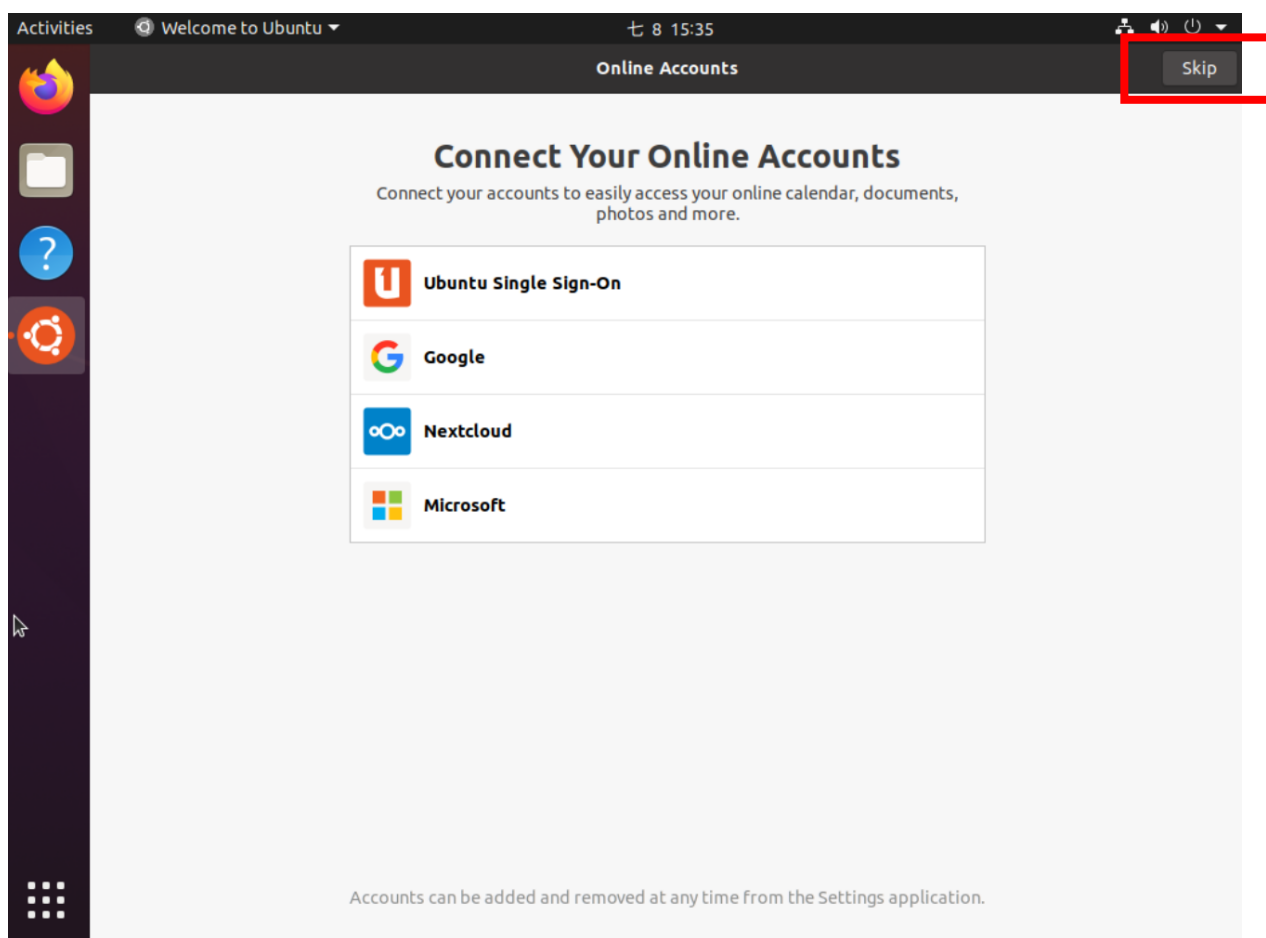
Step3-1 Ubuntu 初次使用(重啟)

等待安裝完畢後點選“Restart Now”重新啟動電腦並移除安裝媒介，由硬碟開機。



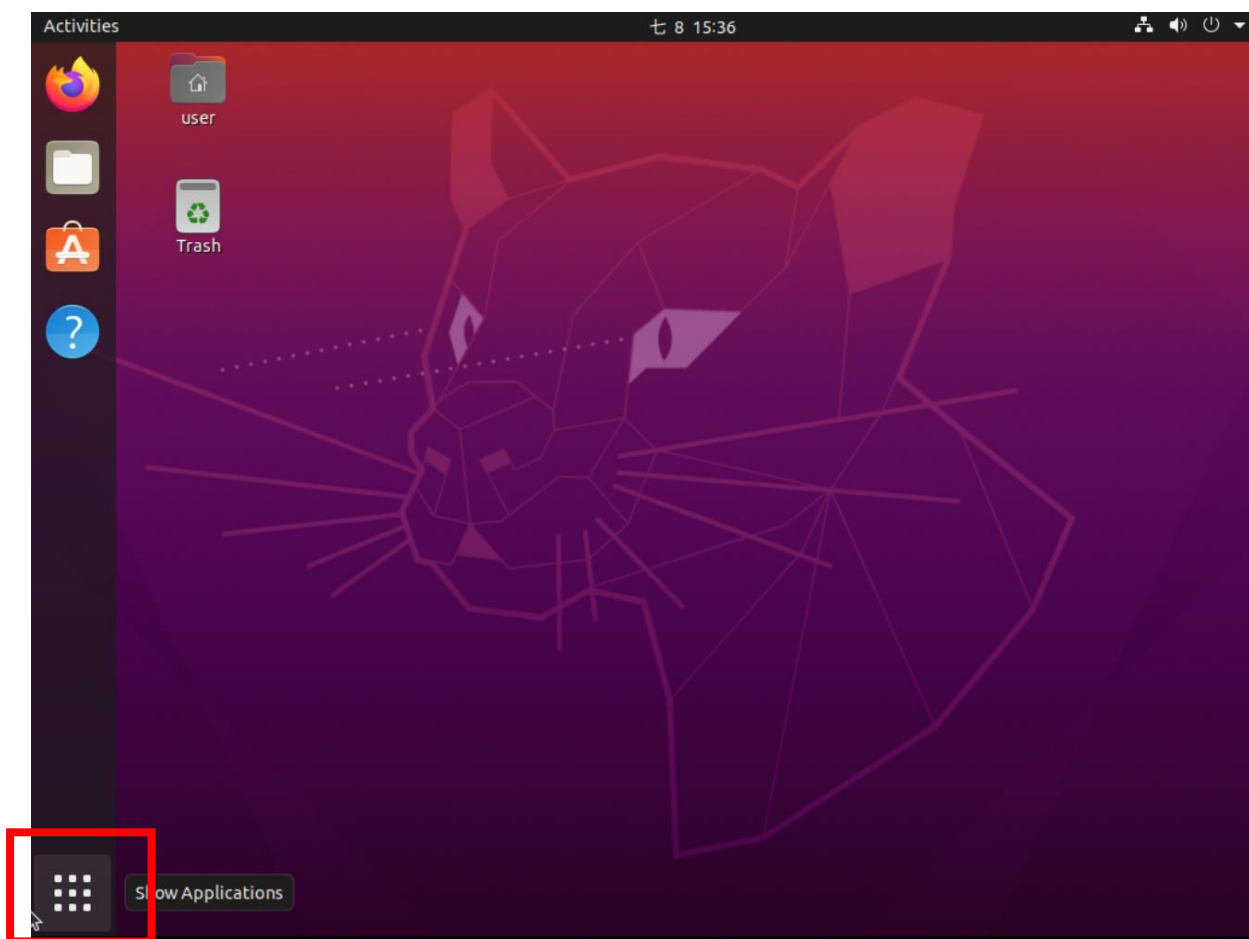
Step3-2 Ubuntu 初次使用(介面)

重新啟動完後應會自動登入，登入後點選“Skip”



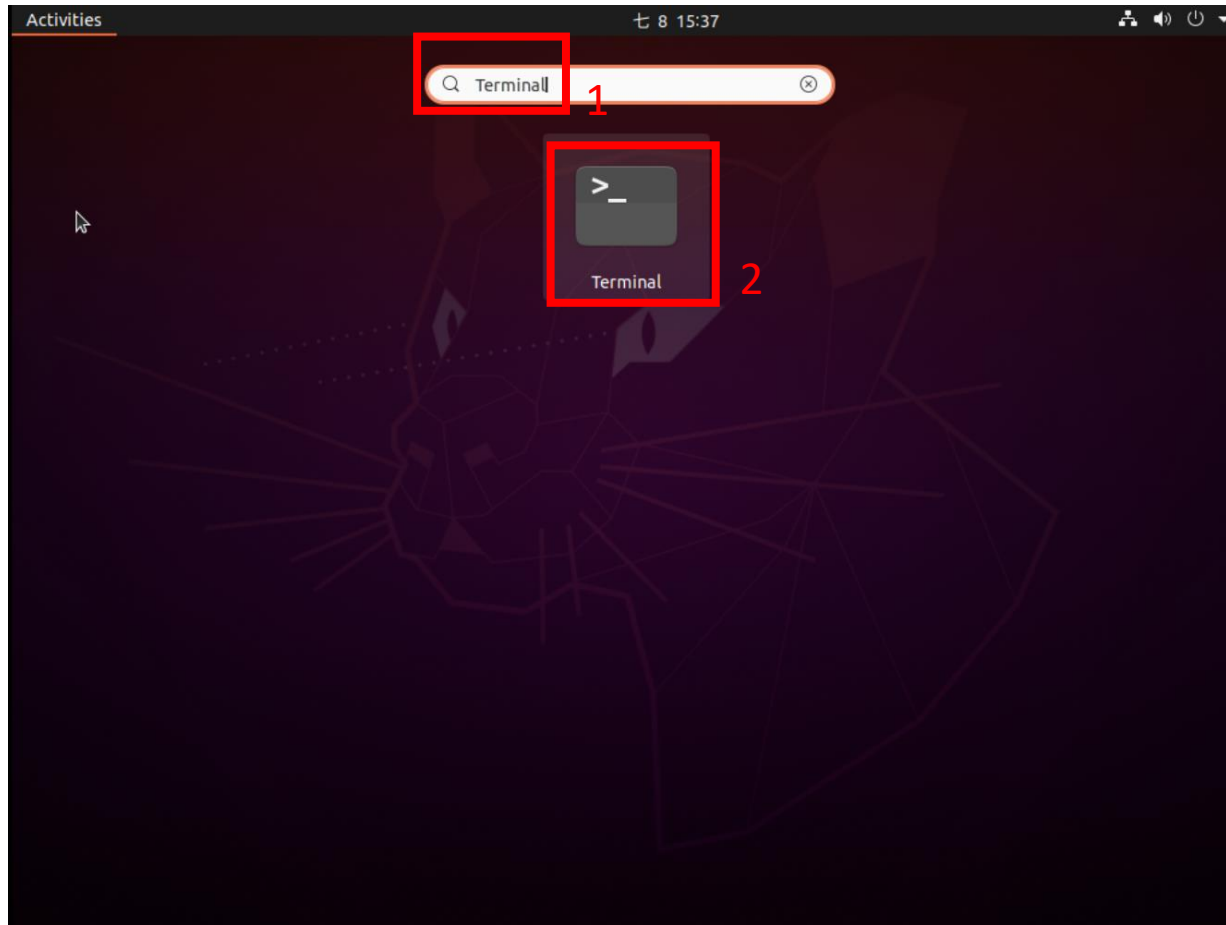
Step3-3 Ubuntu 初次使用(選單)

點選左下角的圖示



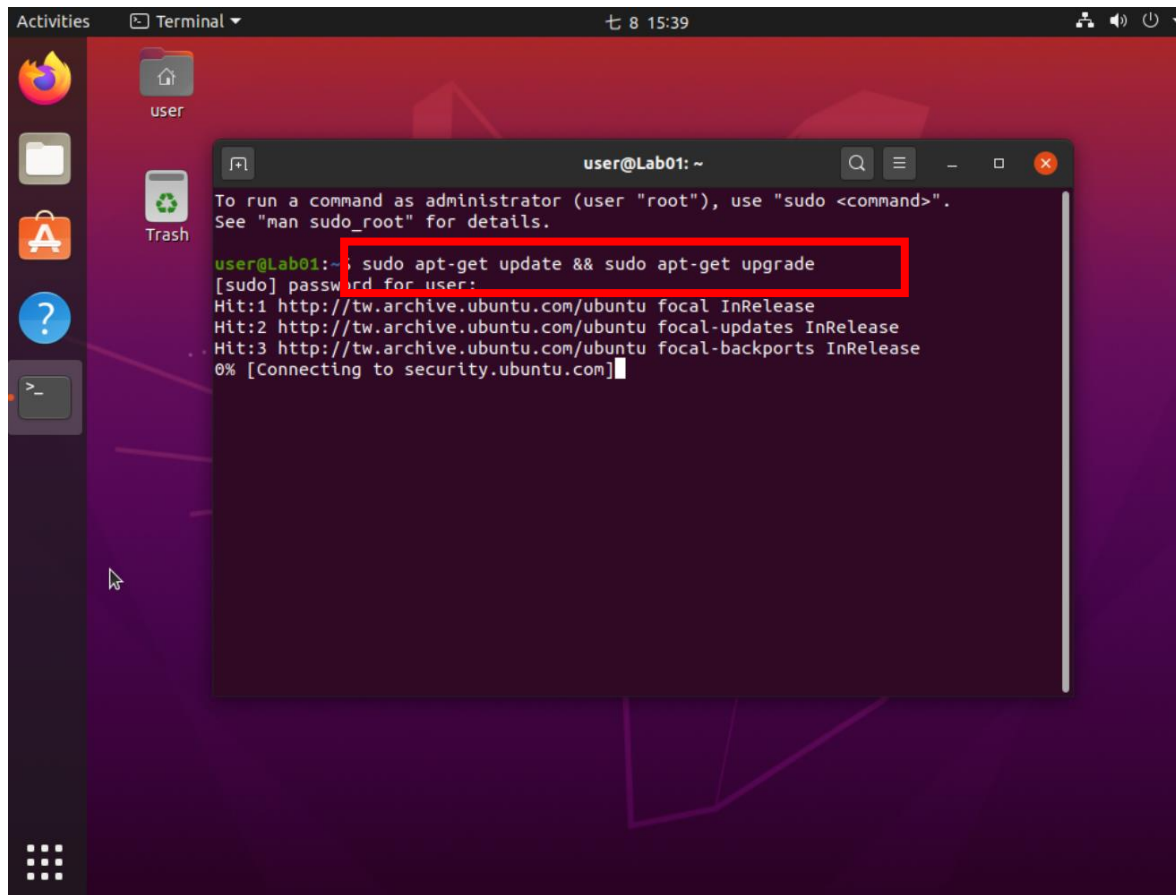
Step3-4 Ubuntu 初次使用(終端機)

輸入“Terminal”之後點選終端機的圖示



Step4-1 軟體安裝(更新系統軟體)

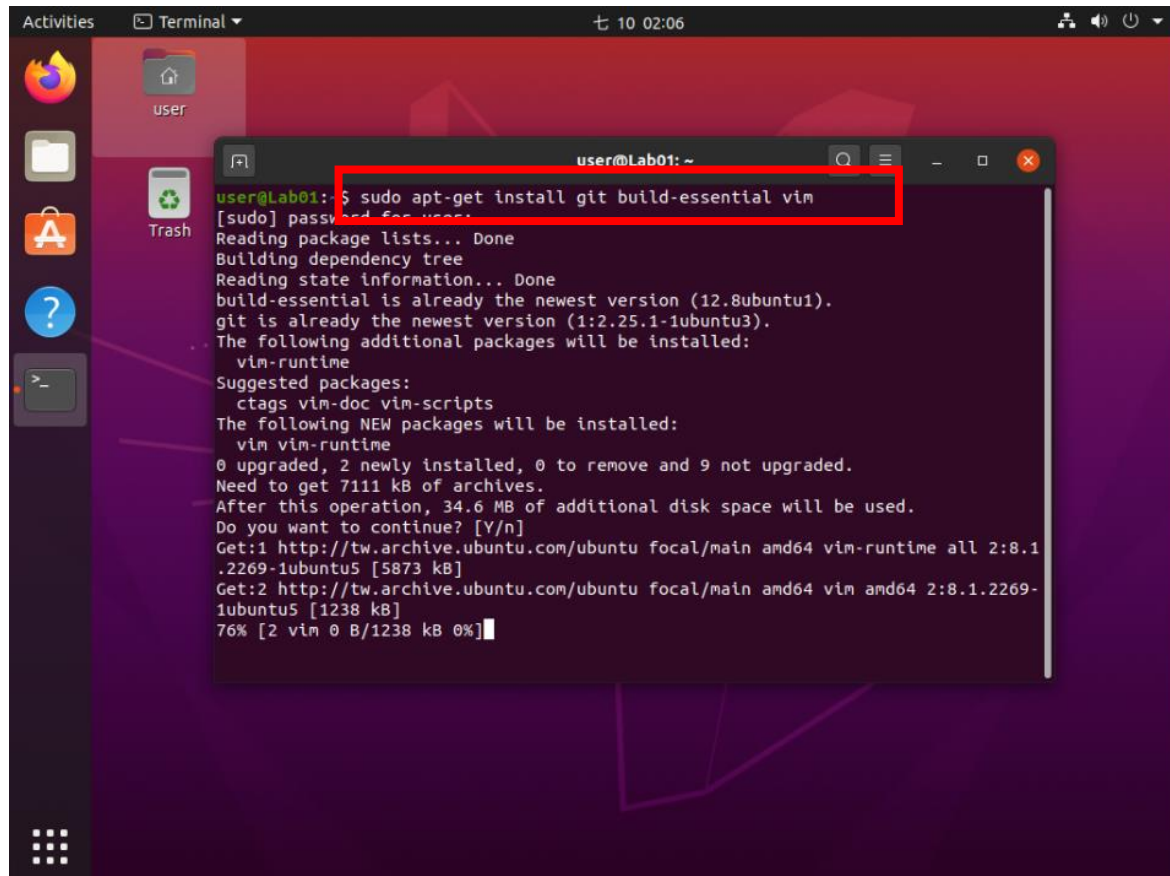
輸入 `sudo apt-get update && sudo apt-get upgrade` 並輸入密碼，若有新更新可安裝請輸入“y”安裝

A screenshot of a Linux desktop environment with a terminal window open. The terminal window title is 'user@Lab01: ~'. It shows the command 'sudo apt-get update && sudo apt-get upgrade' being entered. The prompt '[sudo] password for user:' is visible, followed by three 'Hit' messages indicating updates for 'focal', 'focal-updates', and 'focal-backports'. The terminal output is as follows:

```
user@Lab01:~$ sudo apt-get update && sudo apt-get upgrade
[sudo] password for user:
Hit:1 http://tw.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://tw.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://tw.archive.ubuntu.com/ubuntu focal-backports InRelease
0% [Connecting to security.ubuntu.com]
```

Step4-2 軟體安裝(安裝必要軟體)

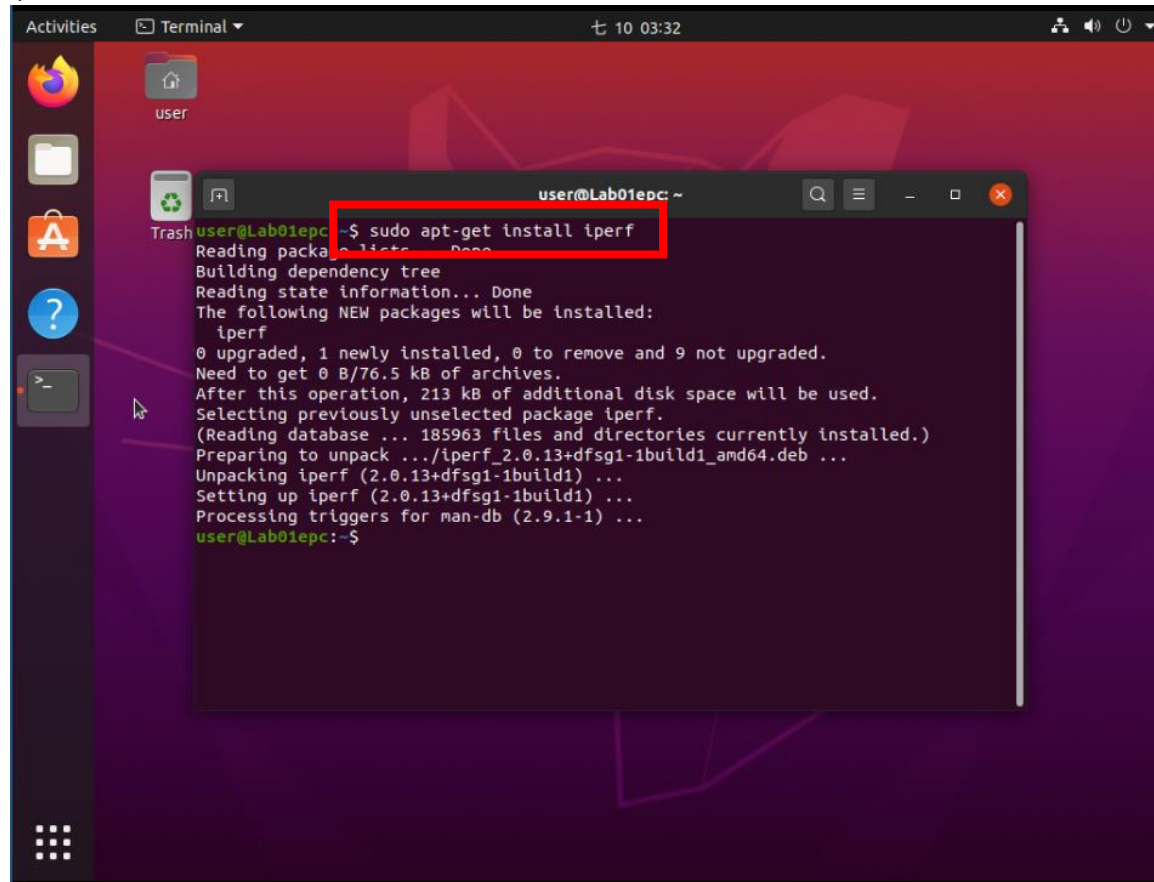
輸入`sudo apt-get install git build-essential vim`並輸入密碼，等待提示後請輸入“y”安裝



```
user@Lab01: ~  
user@Lab01:~$ sudo apt-get install git build-essential vim  
[sudo] password for user:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
build-essential is already the newest version (12.8ubuntu1).  
git is already the newest version (1:2.25.1-1ubuntu3).  
The following additional packages will be installed:  
  vim-runtime  
Suggested packages:  
  ctags vim-doc vim-scripts  
The following NEW packages will be installed:  
  vim vim-runtime  
0 upgraded, 2 newly installed, 0 to remove and 9 not upgraded.  
Need to get 7111 kB of archives.  
After this operation, 34.6 MB of additional disk space will be used.  
Do you want to continue? [Y/n]  
Get:1 http://tw.archive.ubuntu.com/ubuntu focal/main amd64 vim-runtime all 2:8.1  
.2269-1ubuntu5 [5873 kB]  
Get:2 http://tw.archive.ubuntu.com/ubuntu focal/main amd64 vim amd64 2:8.1.2269-  
1ubuntu5 [1238 kB]  
76% [2 vim 0 B/1238 kB 0%]
```

Step4-3 軟體安裝(安裝測試軟體)

輸入`sudo apt-get install iperf`並輸入密碼，等待提示後請輸入“y”安裝



The screenshot shows a terminal window titled "user@Lab01epc: ~" with the command `sudo apt-get install iperf` entered. The command is highlighted with a red box. The terminal output shows the package list being read, the dependency tree being built, and the state information being read. It then lists the new packages to be installed: `iperf`. It indicates that 0 packages are upgraded, 1 is newly installed, 0 are to be removed, and 9 are not upgraded. It also shows the disk space requirements and the selection of the `iperf` package. The installation process is then shown, including unpacking and setting up the package. The terminal ends with the prompt `user@Lab01epc:~$`.

```
user@Lab01epc:~$ sudo apt-get install iperf
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  iperf
0 upgraded, 1 newly installed, 0 to remove and 9 not upgraded.
Need to get 0 B/76.5 kB of archives.
After this operation, 213 kB of additional disk space will be used.
Selecting previously unselected package iperf.
(Reading database ... 185963 files and directories currently installed.)
Preparing to unpack .../iperf_2.0.13+dfsg1-1build1_amd64.deb ...
Unpacking iperf (2.0.13+dfsg1-1build1) ...
Setting up iperf (2.0.13+dfsg1-1build1) ...
Processing triggers for man-db (2.9.1-1) ...
user@Lab01epc:~$
```

Step5-1 網路設定(檢查EPC介面)

在EPC上輸入`sudo ip link show`並輸入密碼以檢查網路介面
本範例之 EPC 有二網路介面，ens3 為連結 Internet 之介面，
ens4 為連接 UE 之介面。

```
user@Lab01epc:~$ sudo ip link show
[sudo] password for user:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
   group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
   DEFAULT group default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
   DEFAULT group default qlen 1000
    link/ether 52:54:00:12:34:57 brd ff:ff:ff:ff:ff:ff
user@Lab01epc:~$
```


Step5-2 網路設定(設定EPC IP位址)

在EPC上輸入`sudo ip addr add 10.0.0.1/24 dev ens4`並輸入密碼以設定IP位址

設定完後可使用`ip addr show`檢查所設置位址是否正確

```
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute ens3
        valid_lft 86180sec preferred_lft 86180sec
    inet6 fec0::885f:e4a1:2a9a:c266/64 scope site temporary dynamic
        valid_lft 86182sec preferred_lft 14182sec
    inet6 fec0::21d1:81aa:6b57:7479/64 scope site dynamic mngtmpaddr noprefixroute
        valid_lft 86182sec preferred_lft 14182sec
    inet6 fe80::acea:8a2b:a6a8:7c28/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:12:34:57 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 scope global ens4
        valid_lft forever preferred_lft forever
```


Step5-3 網路設定(檢查UE介面)

在UE上輸入`sudo ip link show`並輸入密碼以檢查網路介面
本範例之 UE 有一網路介面 `ens3` 為連結 EPC 之介面。

```
user@Lab01ue:~$ sudo ip link show
[sudo] password for user:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
```

Step5-4 網路設定(設定UE IP位址)

在UE上輸入`sudo ip addr add 10.0.0.2/24 dev ens3`並輸入密碼以設定IP位址

設定完後可使用`ip addr show`檢查所設置位址是否正確

```
user@Lab01ue:~$ sudo ip addr add 10.0.0.2/24 dev ens3
user@Lab01ue:~$ sudo ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/24 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::acea:8a2b:a6a8:7c28/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Stage 1 Check List

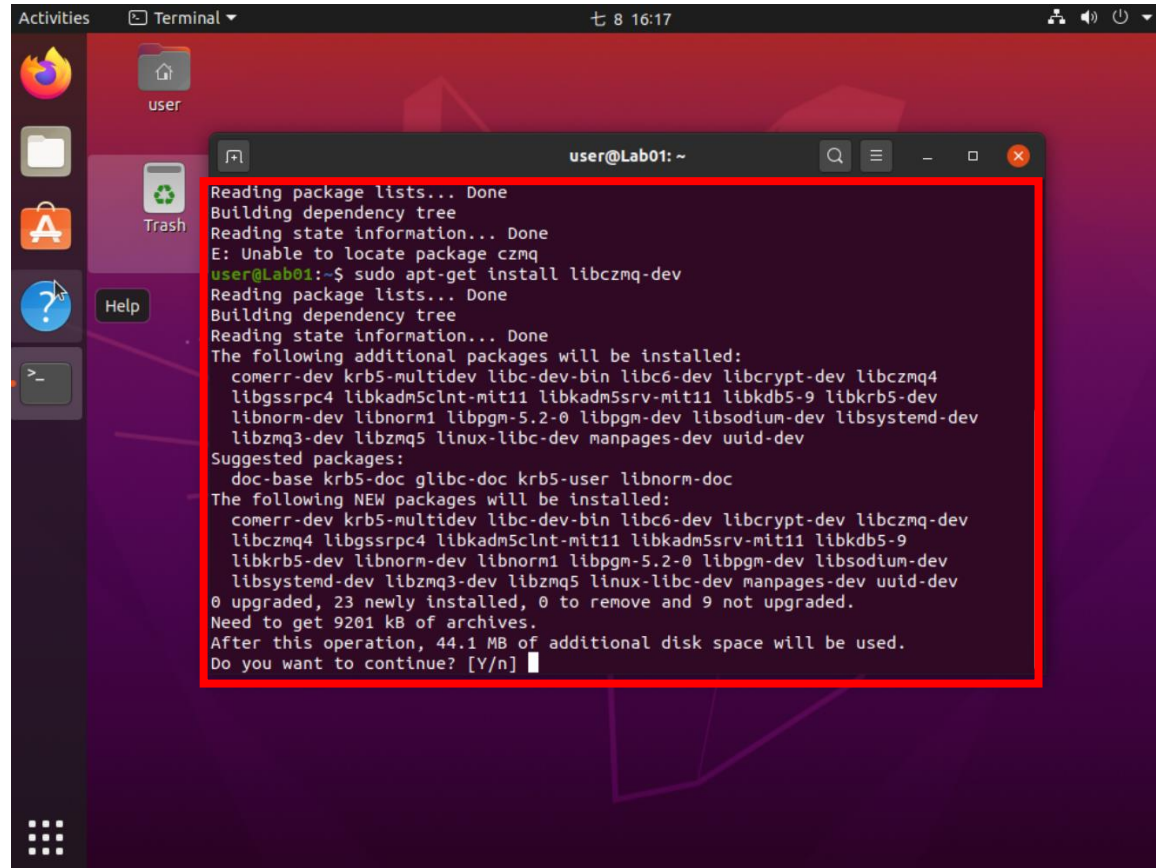
項目	內容
確認更新到最新	<code>sudo apt-get update</code>
確認iperf有安裝	<code>iperf --version</code>
確認 EPC 及 UE 之網路介面名稱	<code>ip link show</code> 本範例 EPC 之對外網路介面名稱為 ens3，對內與 UE 連接的網路介面編號為 ens4。 本範例 UE 與 EPC 連接的網路介面為 ens3。
確認 EPC 及 UE 之 IP 位址設定正確	<code>ip addr show</code> 確認 EPC 對內介面的 IP 位址為 10.0.0.1。 確認 UE 介面的 IP 位址為 10.0.0.2。
確認 EPC 與 UE 是否能互相通訊	在 EPC 上： <code>ping 10.0.0.2 -c 10</code> 在 UE 上： <code>ping 10.0.0.1 -c 10</code> 若沒出現任何錯誤訊息即為成功。

Outline

- 實驗目的及實驗內容
- 背景知識
- 實驗環境
- Stage 1: 環境架設
- Stage 2: srsLTE 及 ZeroMQ 編譯安裝
 - Step1: 安裝依賴套件
 - Step2: 下載 srsLTE 原始碼
 - Step3: 編譯 srsLTE
 - Step4: 安裝 srsLTE 執行檔
 - Step5: 安裝 srsLTE 預設設定檔
 - Step6: 更新 ld 路徑
- Stage 3: srsLTE 執行及測試
- Stage 4: srsLTE 封包觀測
- 總結及問題

Step1-1 安裝依賴套件(ZeroMQ)

輸入 `sudo apt-get install libczmq-dev` 並輸入密碼，等待提示後輸入“y”安裝 libczmq

A screenshot of a Linux desktop environment with a terminal window open. The terminal shows the command `sudo apt-get install libczmq-dev` being executed. The output lists additional packages to be installed, suggested packages, and new packages to be installed. The prompt `Do you want to continue? [Y/n]` is visible at the bottom of the terminal output.

```
user@Lab01: ~  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
E: Unable to locate package czmq  
user@Lab01:~$ sudo apt-get install libczmq-dev  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  comerr-dev krb5-multidev libc-dev-bin libc6-dev libcrypt-dev libczmq4  
  libgssrpc4 libkadm5clnt-mit11 libkadm5srv-mit11 libkdb5-9 libkrb5-dev  
  libnorm-dev libnorm1 libpgm-5.2-0 libpgm-dev libsodium-dev libsystemd-dev  
  libzmq3-dev libzmq5 linux-libc-dev manpages-dev uuid-dev  
Suggested packages:  
  doc-base krb5-doc glibc-doc krb5-user libnorm-doc  
The following NEW packages will be installed:  
  comerr-dev krb5-multidev libc-dev-bin libc6-dev libcrypt-dev libczmq-dev  
  libczmq4 libgssrpc4 libkadm5clnt-mit11 libkadm5srv-mit11 libkdb5-9  
  libkrb5-dev libnorm-dev libnorm1 libpgm-5.2-0 libpgm-dev libsodium-dev  
  libsystemd-dev libzmq3-dev libzmq5 linux-libc-dev manpages-dev uuid-dev  
0 upgraded, 23 newly installed, 0 to remove and 9 not upgraded.  
Need to get 9201 kB of archives.  
After this operation, 44.1 MB of additional disk space will be used.  
Do you want to continue? [Y/n]
```


Step1-2 安裝依賴套件(srsLTE)

輸入 `sudo apt-get install cmake libfftw3-dev libmbedtls-dev libboost-program-options-dev libconfig++-dev libsctp-dev` 並輸入密碼，等待提示後輸入“y”

```
libboost-graph-parallel1.71-dev libboost-iostreams1.71-dev
libboost-locale1.71-dev libboost-log1.71-dev libboost-math1.71-dev
libboost-mpi1.71-dev libboost-mpi-python1.71-dev libboost-numpy1.71-dev
libboost-python1.71-dev libboost-random1.71-dev libboost-regex1.71-dev
libboost-serialization1.71-dev libboost-stacktrace1.71-dev
libboost-system1.71-dev libboost-test1.71-dev libboost-thread1.71-dev
libboost-timer1.71-dev libboost-type-erasure1.71-dev libboost-wave1.71-dev
libboost1.71-tools-dev libmpfr++-dev libntl-dev libfftw3-doc libmbedtls-doc
lksctp-tools libstdc++-7-doc make-doc
The following NEW packages will be installed:
binutils binutils-common binutils-x86-64-linux-gnu cmake cmake-data gcc
gcc-7-base gcc-8-base gcc-9 libasan4 libasan5 libatomic1 libbinutils
libboost-program-options-dev libboost-program-options1.71-dev
libboost-program-options1.71.0 libboost1.71-dev libcilkrts5 libconfig++-dev
libconfig++9v5 libconfig-dev libconfig-doc libconfig9 libctf-nobfd0 libctf0
libcurl4 libfftw3-bin libfftw3-dev libfftw3-double3 libfftw3-long3
libfftw3-quad3 libgcc-7-dev libgcc-9-dev libitm1 libjsoncpp1 liblsan0
libmbedcrypto3 libmbedtls-dev libmbedtls12 libmbedx509-0 libmpx2
libquadmath0 librtmp0 libsctp-dev libsctp1 libstdc++-7-dev libtsan0
libubsan0 libubsan1 make
0 upgraded, 50 newly installed, 0 to remove and 9 not upgraded.
Need to get 39.1 MB/39.4 MB of archives.
After this operation, 295 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Step2-1 下載 srsLTE 原始碼(下載)

輸入 `git clone https://github.com/srsLTE/srsLTE.git` 下載 srsLTE 原始碼

```
Get:3 http://tw.archive.ubuntu.com/ubuntu focal/main amd64 git amd64 1:2.25.1-1u
buntu3 [4554 kB]
Fetched 5464 kB in 1s (5312 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 183192 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17029-1_all.deb ...
Unpacking liberror-perl (0.17029-1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a2.25.1-1ubuntu3_all.deb ...
Unpacking git-man (1:2.25.1-1ubuntu3) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.25.1-1ubuntu3_amd64.deb ...
Unpacking git (1:2.25.1-1ubuntu3) ...
Setting up liberror-perl (0.17029-1) ...
Setting up git-man (1:2.25.1-1ubuntu3) ...
Setting up git (1:2.25.1-1ubuntu3) ...
Processing triggers for man-db (2.9.1-1) ...
user@Lab01:~$ git clone https://github.com/srsLTE/srsLTE.git
Cloning into 'srsLTE'...
remote: Enumerating objects: 76402, done.
remote: Total 76402 (delta 0), reused 0 (delta 0), pack-reused 76402
Receiving objects: 100% (76402/76402), 34.05 MiB | 256.00 KiB/s, done.
Resolving deltas: 100% (57370/57370), done.
user@Lab01:~$
```

Step2-2 下載 srsLTE 原始碼(改版本)

輸入以下指令以將 srsLTE 版本改為 20.04.1

```
cd srsLTE; git fetch --all --tags;  
git checkout tags/release_20_04_1
```

```
user@Lab01:~$ cd srsLTE/  
user@Lab01:~/srsLTE$ git fetch --all --tags  
Fetching origin  
user@Lab01:~/srsLTE$ git checkout tags/release_20_04_1  
Note: switching to 'tags/release_20_04_1'.  
  
You are in 'detached HEAD' state. You can look around, make experimental  
changes and commit them, and you can discard any commits you make in this  
state without impacting any branches by switching back to a branch.  
  
If you want to create a new branch to retain commits you create, you may  
do so (now or later) by using -c with the switch command. Example:  
  
    git switch -c <new-branch-name>  
  
Or undo this operation with:  
  
    git switch -  
  
Turn off this advice by setting config variable advice.detachedHead to false  
  
HEAD is now at c892ae56b rrc_cell_cfg: fix potential div by zero  
user@Lab01:~/srsLTE$
```


Step3-1 編譯 srsLTE (cmake)

輸入 `mkdir build; cd build; cmake ../` 並檢查過程中是否出現 `found libZEROMQ: ...`

```
-- No package 'libbladerf' found
-- libbladerf not found.
-- FINDING SOAPY.
-- Checking for module 'SoapySDR'
-- No package 'SoapySDR' found
-- libSOAPYSDR not found.
-- FINDING ZEROMQ.
-- Checking for module 'ZeroMQ'
-- No package 'ZeroMQ' found
-- Found libZEROMQ: /usr/include, /usr/lib/x86_64-linux-gnu/libzmq.so
-- Found Boost: /usr/lib/x86_64-linux-gnu/cmake/Boost-1.71.0/BoostConfig.cmake (
found suitable version "1.71.0", minimum required is "1.35") found components: p
rogram_options
-- SRSGUI_LIBRARIES SRSGUI_LIBRARIES-NOTFOUND
-- SRSGUI_INCLUDE_DIRS SRSGUI_INCLUDE_DIRS-NOTFOUND
-- Could NOT find SRSGUI (missing: SRSGUI_LIBRARIES SRSGUI_INCLUDE_DIRS)
-- Performing Test HAVE_WNO_UNUSED_BUT_SET_VARIABLE
-- Performing Test HAVE_WNO_UNUSED_BUT_SET_VARIABLE - Success
-- Performing Test HAVE_SSE
-- Performing Test HAVE_SSE - Success
-- SSE4.1 is enabled - target CPU must support it
-- Performing Test HAVE_AVX
-- Performing Test HAVE_AVX - Failed
-- Performing Test HAVE_AVX2
-- Performing Test HAVE_AVX2 - Failed
```

Step3-2 編譯 srsLTE (make)

輸入 `make -j8` 並等待編譯完成

```
Scanning dependencies of target srslte_mimo
Scanning dependencies of target srslte_phch
Scanning dependencies of target srslte_sync
[ 1%] Building C object lib/src/phy/agc/CMakeFiles/srslte_agc.dir/agc.c.o
[ 1%] Building C object lib/src/phy/common/CMakeFiles/srslte_phy_common.dir/phy_common.c.o
[ 1%] Building C object lib/src/phy/mimo/CMakeFiles/srslte_mimo.dir/layermap.c.o
[ 1%] Building C object lib/src/phy/enb/CMakeFiles/srslte_enb.dir/enb_dl.c.o
[ 1%] Building C object lib/src/phy/ch_estimation/CMakeFiles/srslte_ch_estimation.dir/chest_common.c.o
[ 1%] Building C object lib/src/phy/fec/CMakeFiles/srslte_fec.dir/cbsegm.c.o
[ 1%] Building C object lib/src/phy/sync/CMakeFiles/srslte_sync.dir/cfo.c.o
[ 1%] Building C object lib/src/phy/phch/CMakeFiles/srslte_phch.dir/cqi.c.o
[ 2%] Building C object lib/src/phy/fec/CMakeFiles/srslte_fec.dir/convcoder.c.o
[ 2%] Built target srslte_agc
[ 2%] Building C object lib/src/phy/sync/CMakeFiles/srslte_sync.dir/cp.c.o
Scanning dependencies of target srslte_utils
[ 2%] Building C object lib/src/phy/ch_estimation/CMakeFiles/srslte_ch_estimation.dir/chest_dl.c.o
[ 2%] Building C object lib/src/phy/mimo/CMakeFiles/srslte_mimo.dir/precoding.c.o
[ 3%] Building C object lib/src/phy/utils/CMakeFiles/srslte_utils.dir/bit.c.o
```

Step4 安裝 srsLTE 執行檔

輸入 `sudo make install` 並輸入密碼

```
-- Installing: /usr/local/include/srslte/phy/channel/ch_awgn.h
-- Installing: /usr/local/include/srslte/phy/channel/channel.h
-- Installing: /usr/local/include/srslte/phy/channel/fading.h
-- Installing: /usr/local/include/srslte/phy/mimo
-- Installing: /usr/local/include/srslte/phy/mimo/layermap.h
-- Installing: /usr/local/include/srslte/phy/mimo/precoding.h
-- Installing: /usr/local/lib/librslte_rf.so
-- Installing: /usr/local/include/srslte/version.h
-- Installing: /usr/local/share/srslte/ue.conf.example
-- Installing: /usr/local/bin/srsue
-- Set runtime path of "/usr/local/bin/srsue" to ""
-- Installing: /usr/local/share/srslte/enb.conf.example
-- Installing: /usr/local/share/srslte/drb.conf.example
-- Installing: /usr/local/share/srslte/rr.conf.example
-- Installing: /usr/local/share/srslte/sib.conf.example
-- Installing: /usr/local/bin/srsenb
-- Set runtime path of "/usr/local/bin/srsenb" to ""
-- Installing: /usr/local/share/srslte/epc.conf.example
-- Installing: /usr/local/share/srslte/mbms.conf.example
-- Installing: /usr/local/share/srslte/user_db.csv.example
-- Installing: /usr/local/bin/srsepc_if_masq.sh
-- Installing: /usr/local/bin/srsepc
-- Installing: /usr/local/bin/srsmbms
user@Lab01:~/srsLTE/build$
```

Step5 安裝 srsLTE 預設設定檔

輸入 `sudo srslte_install_configs.sh service --force` 並輸入密碼

```
-- Installing: /usr/local/share/srslte/sib.conf.example
-- Installing: /usr/local/bin/srsenb
-- Set runtime path of "/usr/local/bin/srsenb" to ""
-- Installing: /usr/local/share/srslte/epc.conf.example
-- Installing: /usr/local/share/srslte/mbms.conf.example
-- Installing: /usr/local/share/srslte/user_db.csv.example
-- Installing: /usr/local/bin/srsepc_if_masq.sh
-- Installing: /usr/local/bin/srsepc
-- Installing: /usr/local/bin/srsmbms
user@Lab01:~/srsLTE/build$ sudo srslte_install_configs.sh service --force
Force overwrite called. Overwriting any existing configuration files.
Is this OK? [y/n]: y
Installing srsLTE configuration files:
- Creating srsLTE config folder /etc/srslte
- Installing ue.conf.example in /etc/srslte/ue.conf
- Installing enb.conf.example in /etc/srslte/enb.conf
- Installing sib.conf.example in /etc/srslte/sib.conf
- Installing rr.conf.example in /etc/srslte/rr.conf
- Installing drb.conf.example in /etc/srslte/drb.conf
- Installing epc.conf.example in /etc/srslte/epc.conf
- Installing mbms.conf.example in /etc/srslte/mbms.conf
- Installing user_db.csv.example in /etc/srslte/user_db.csv
Done.
user@Lab01:~/srsLTE/build$
```

Step6-1 更新 ld 路徑(更改設定檔)

輸入 **sudo vim /etc/ld.so.conf.d/locallib.conf** 並輸入密碼，出現文字編輯器後輸入**i**並輸入**/usr/local/lib** 後按 **Esc**、**:wq**儲存離開。

```
/usr/local/lib
```

```
-- INSERT --
```

```
1,15 All
```

Step6-2 更新 ld 路徑(執行更新)

輸入 `sudo ldconfig` 並輸入密碼以更新 ld 搜尋路徑。

利用 `ld --verbose | grep SEARCH_DIR` 確認 `/usr/local/lib` 是否在搜尋目錄中。

```
user@Lab01epc:~$ sudo vim /etc/ld.so.conf.d/ldconfig.conf
[sudo] password for user:
user@Lab01epc:~$ sudo ldconfig
user@Lab01epc:~$ ld --verbose | grep SEARCH_DIR
SEARCH_DIR("/usr/local/lib/x86_64-linux-gnu"); SEARCH_DIR("/lib/x86_64-linux-g
nu"); SEARCH_DIR("/usr/lib/x86_64-linux-gnu"); SEARCH_DIR("/usr/lib/x86_64-lin
ux-gnu64"); SEARCH_DIR("/usr/local/lib64"); SEARCH_DIR("/lib64"); SEARCH_DIR("
=/usr/lib64"); SEARCH_DIR("/usr/local/lib"); SEARCH_DIR("/lib"); SEARCH_DIR("=
/usr/lib"); SEARCH_DIR("/usr/x86_64-linux-gnu/lib64"); SEARCH_DIR("/usr/x86_64
-linux-gnu/lib");
user@Lab01epc:~$
```


Stage 2 Check List

項目	內容
確認有偵測到 ZeroMQ	在使用 cmake 產生 srsLTE 的 makefile 時檢查是否出現 <code>found libZEROMQ:</code>
確認 srsepc、srenb 及 srsue 安裝成功	<code>sudo ls /usr/local/bin grep srs</code> 確認 srsepc、srsenb 及 srsue 有出現在該目錄中。
確認設定檔安裝成功	<code>sudo ls -alh /etc/srslte</code> 確認 ue.conf、enb.conf、sib.conf、rr.conf、drb.conf、epc.conf、mbms.conf 及 user_db.csv 檔案存在於 /etc/srslte 目錄下。
確認 ld 路徑正確	<code>ld --verbose grep SEARCH_DIR</code> 確認 /usr/local/lib 在 ld 的搜尋路徑中。

Outline

- 實驗目的及實驗內容
- 背景知識
- 實驗環境
- Stage 1: 環境架設
- Stage 2: srsLTE 及 ZeroMQ 編譯安裝
- Stage 3: srsLTE 執行及測試
 - Step1: 啟動實驗平台
 - Step2: 虛擬介面觀察
 - Step3: 連線測試
 - Step4: 外連設定
 - Step5: 測試能否連到 Internet
- Stage 4: srsLTE 封包觀測
- 總結及問題

Step1-1 啟動實驗平台(EPC)

輸入 `sudo srsepc` 並輸入密碼啟動srsepc

```
user@Lab01epc:~$ sudo srsepc
[sudo] password for user:

Built in Release mode using commit c892ae56b on branch HEAD.

--- Software Radio Systems EPC ---

Reading configuration file /etc/srslte/epc.conf...
HSS Initialized.
MME S11 Initialized
MME GTP-C Initialized
MME Initialized. MCC: 0xf001, MNC: 0xff01
SPGW GTP-U Initialized.
SPGW S11 Initialized.
SP-GW Initialized.
```

I

Step1-2 啟動實驗平台(eNB)

開啟新終端機視窗並輸入

```
sudo srsenb \  
  --rf.device_name=zmq \  
  --rf.device_args=" \  
    fail_on_disconnect=true, \  
    tx_port=tcp://*:2000, \  
    rx_port=tcp://10.0.0.2:2001, \  
    id=enb, \  
    base_srate=23.04e6" \  
--expert.nof_phy_threads=1  
並確認eNB是否連上EPC
```

```
#以root身分啟動srsenb  
#使用ZeroMQ作為RF裝置  
#設定ZeroMQ相關參數  
#在中斷連線時產生錯誤  
#將tx port綁定至tcp://*:2000  
#指定rx port連接至UE  
#將id設定為“enb”  
#設定基礎取樣率為23.04MHz  
#僅以一個執行續運作PHY層
```

eNB 啟動結果

eNB啟動後應會自動連上EPC，EPC的終端機也會顯示對應訊息。

```
user@Lab01epc:~$ sudo srsepc
[sudo] password for user:

B Files in Release mode using commit c892ae56b on branch HEAD.

--- Software Radio Systems EPC ---

Reading configuration file /etc/srslte/epc.conf...
HSS Initialized.
MME S11 Initialized
MME GTP-C Initialized
MME Initialized. MCC: 0xf001, MNC: 0xff01
SPGW GTP-U Initialized.
SPGW S11 Initialized.
SP-GW Initialized.
Received S1 Setup Request.
S1 Setup Request - eNB Name: srsenb01, eNB id: 0x19b
S1 Setup Request - MCC:001, MNC:01, PLMN: 61712
S1 Setup Request - TAC 0, B-PLMN 0
S1 Setup Request - Paging DRX v128
Sending S1 Setup Response
```

EPC

```
user@Lab01epc:~$ sudo srsenb --rf.device_name=zmq -
-rf.device_args="fail_on_disconnect=true,tx_port=tc
p://*:2000,rx_port=tcp://10.0.0.2:2001,id=enb,base_
stave=23.04e6" --expert.nof_phy_threads=1
[sudo] password for user:
--- Software Radio Systems LTE eNodeB ---

Reading configuration file /etc/srslte/enb.conf...
Built in Release mode using commit c892ae56b on branch HEAD.

Opening 1 channels in RF device=zmq with args=fail_
on_disconnect=true,tx_port=tcp://*:2000,rx_port=tcp
://10.0.0.2:2001,id=enb,base_stave=23.04e6
CHx id=enb
Current sample rate is 1.92 MHz with a base rate of
23.04 MHz (x12 decimation)
CH0 rx_port=tcp://10.0.0.2:2001
CH0 tx_port=tcp://*:2000
CH0 fail_on_disconnect=true
Current sample rate is 11.52 MHz with a base rate o
f 23.04 MHz (x2 decimation)
Current sample rate is 11.52 MHz with a base rate o
f 23.04 MHz (x2 decimation)
Setting frequency: DL=2685.0 Mhz, UL=2565.0 Mhz for
cc_idx=0

==== eNodeB started ====
Type <t> to view trace
```

eNB

Step1-3 啟動實驗平台(UE)

開啟新終端機視窗並輸入

```
sudo srsue \  
  --rf.device_name=zmq \  
  --rf.device_args=" \  
    fail_on_disconnect=true, \  
    tx_port=tcp://*:2001, \  
    rx_port=tcp://10.0.0.1:2000, \  
    id=ue, \  
    base_srate=23.04e6"
```

並確認UE是否連上eNB及EPC

```
#以root身分啟動srsue  
#使用ZeroMQ作為RF裝置  
#設定ZeroMQ相關參數  
#在中斷連線時產生錯誤  
#將tx port綁定至tcp://*:2001  
#指定rx port連接至eNB  
#將id設定為“ue”  
#設定基礎取樣率為23.04MHz
```

UE啟動結果

UE啟動後應會自動連上eNB，並顯示EMM訊息中的
Software Radio System LTE。

```
Built in Release mode using commit c892ae56b on branch HEAD.

Opening 1 channels in RF device=zmq with args=tx_port=tcp://*:2001,rx_port=tcp://10.0.0.1:2000,id=ue,base_srate=23.04e6
CHx base_srate=23.04e6
CHx id=ue
Current sample rate is 1.92 MHz with a base rate of 23.04 MHz (x12 decimation)
CH0 rx_port=tcp://10.0.0.1:2000
CH0 tx_port=tcp://*:2001
Waiting PHY to initialize ... done!
Attaching UE...
Current sample rate is 1.92 MHz with a base rate of 23.04 MHz (x12 decimation)
Current sample rate is 1.92 MHz with a base rate of 23.04 MHz (x12 decimation)
.
Found Cell: Mode=FDD, PCI=1, PRB=50, Ports=1, CF0=-0.2 KHz
Current sample rate is 11.52 MHz with a base rate of 23.04 MHz (x2 decimation)
Current sample rate is 11.52 MHz with a base rate of 23.04 MHz (x2 decimation)
Found PLMN: Id=00101, TAC=7
Random Access Transmission: seq=0, ra-rnti=0x2
Random Access Complete.      c-rnti=0x46, ta=0
RRC Connected
Network attach successful. IP: 172.16.0.2
Software Radio Systems LTE (srsLTE)
```


UE啟動結果(EPC)

下圖為UE成功連線時，eNB及EPC的畫面

```
Authentication Response -- IMSI 001010123456789
UE Authentication Accepted.
Generating KeNB with UL NAS COUNT: 0
Downlink NAS: Sending NAS Security Mode Command.
UL NAS: Received Security Mode Complete
Security Mode Command Complete -- IMSI: 001010123456789
Getting subscription information -- QCI 7
Sending Create Session Request.
Creating Session Response -- IMSI: 1010123456789
Creating Session Response -- MME control TEID: 1
Received GTP-C PDU. Message type: GTPC_MSG_TYPE_CREATE_SESSION_REQUEST
SPGW: Allocated Ctrl TEID 1
SPGW: Allocated User TEID 1
SPGW: Allocate UE IP 172.16.0.2
Received Create Session Response
Create Session Response -- SPGW control TEID 1
Create Session Response -- SPGW S1-U Address: 127.0.1.100
SPGW Allocated IP 172.16.0.2 to IMSI 001010123456789
Adding attach accept to Initial Context Setup Request
Sent Initial Context Setup Request. E-RAB id 5
Received Initial Context Setup Response
E-RAB Context Setup. E-RAB id 5
E-RAB Context -- eNB TEID 0x460003; eNB GTP-U Address 127.0.1.1
UL NAS: Received Attach Complete
Unpacked Attached Complete Message. IMSI 1010123456789
Unpacked Activate Default EPS Bearer message. EPS Bearer id 5
Received GTP-C PDU. Message type: GTPC_MSG_TYPE MODIFY_BEARER_REQUEST
Sending EMM Information
[ ]
```

```
user@Lab01epc:~$ sudo srsenb --rf.device_name=zmq --rf.device_args="fail_on_disconnect=true,tx_port=tcp://*:2000,rx_port=tcp://10.0.0.2:2001,id=enb,base_stay=23.04e6" --expert.nof_phy_threads=1
[sudo] password for user:
--- Software Radio Systems LTE eNodeB ---

Reading configuration file /etc/srslte/enb.conf...

Built in Release mode using commit c892ae56b on branch HEAD.

Opening 1 channels in RF device=zmq with args=fail_on_disconnect=true,tx_port=tcp://*:2000,rx_port=tcp://10.0.0.2:2001,id=enb,base_stay=23.04e6
CHx id=enb
Current sample rate is 1.92 MHz with a base rate of 23.04 MHz (x12 decimation)
CH0 rx_port=tcp://10.0.0.2:2001
CH0 tx_port=tcp://*:2000
CH0 fail_on_disconnect=true
Current sample rate is 11.52 MHz with a base rate of 23.04 MHz (x2 decimation)
Current sample rate is 11.52 MHz with a base rate of 23.04 MHz (x2 decimation)
Setting frequency: DL=2685.0 Mhz, UL=2565.0 Mhz for cc_idx=0

==== eNodeB started ====
Type ctrl to view trace
RACH: tti=181, preamble=0, offset=0, temp_crnti=0x46
User 0x46 connected
[ ]
```

EPC

eNB

Step2-1 虛擬介面觀察(EPC)

保持EPC及eNB開啟的狀態下開啟第三個終端機並輸入
sudo ip link show 應會看到一名為srs_spgw_sgi的TUN裝置

```
user@Lab01epc:~$ sudo ip link
[sudo] password for user:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    DEFAULT group default qlen 1000
    link/ether 52:54:00:12:34:57 brd ff:ff:ff:ff:ff:ff
4: srs_spgw_sgi: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    state UNKNOWN mode DEFAULT group default qlen 500
    link:none
user@Lab01epc:~$
```

Step2-2 虛擬介面觀察(UE)

保持UE開啟的狀態下開啟第二個終端機並輸入`sudo ip link show` 應會看到一名為tun_srsue的TUN裝置

```
user@Lab01ue:~$ sudo ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noque
ue state UNKNOWN mode DEFAULT group default qlen 10
00
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00
:00:00
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc fq_codel state UP mode DEFAULT group default
qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff
:ff
3: tun_srsue: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER
_UP> mtu 1500 qdisc fq_codel state UNKNOWN mode DEF
AULT group default qlen 500
    link/none
user@Lab01ue:~$
```


Step3-1 連線測試(Downlink ICMP)

在EPC空間的終端機輸入 `ping 172.16.0.2 -c 10` 測試
Downlink ICMP 能不能正常運作

```
user@Lab01epc:~$ ping 172.16.0.2 -c 10
PING 172.16.0.2 (172.16.0.2) 56(84) bytes of data.
64 bytes from 172.16.0.2: icmp_seq=1 ttl=64 time=73.9 ms
64 bytes from 172.16.0.2: icmp_seq=2 ttl=64 time=101 ms
64 bytes from 172.16.0.2: icmp_seq=3 ttl=64 time=64.3 ms
64 bytes from 172.16.0.2: icmp_seq=4 ttl=64 time=53.5 ms
64 bytes from 172.16.0.2: icmp_seq=5 ttl=64 time=68.4 ms
64 bytes from 172.16.0.2: icmp_seq=6 ttl=64 time=85.6 ms
64 bytes from 172.16.0.2: icmp_seq=7 ttl=64 time=102 ms
64 bytes from 172.16.0.2: icmp_seq=8 ttl=64 time=86.1 ms
64 bytes from 172.16.0.2: icmp_seq=9 ttl=64 time=32.9 ms
64 bytes from 172.16.0.2: icmp_seq=10 ttl=64 time=66.8 ms

--- 172.16.0.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 32.937/73.438/102.432/20.196 ms
user@Lab01epc:~$
```

Step3-2 連線測試(Downlink TCP)

在 UE 輸入 `sudo iperf -s` 並在 EPC 空間的終端機輸入 `iperf -c 172.16.0.2 -w 100M -t 10 -i 10 -r` 測試 Downlink TCP 能不能正常運作

```
user@Lab01epc:~$ iperf -c 172.16.0.2 -w 100M -t 10 -i 10 -r
-----
Server listening on TCP port 5001
TCP window size: 416 KByte (WARNING: requested 100 MByte)
-----
Client connecting to 172.16.0.2, TCP port 5001
TCP window size: 416 KByte (WARNING: requested 100 MByte)
-----
[ 3] local 172.16.0.1 port 37060 connected with 172.16.0.2 port 5001
[ ID] Interval      Transfer      Bandwidth
[ 3] 0.0-10.0 sec  10.6 MBytes  8.91 Mbits/sec
[ 3] 0.0-10.0 sec  10.6 MBytes  8.90 Mbits/sec
[ 3] local 172.16.0.1 port 5001 connected with 172.16.0.2 port 39364
[ 3] 0.0-10.0 sec   3.96 MBytes  3.33 Mbits/sec
[ 3] 0.0-13.0 sec   5.12 MBytes  3.30 Mbits/sec
[SUM] 0.0-13.0 sec   9.09 MBytes  5.85 Mbits/sec
user@Lab01epc:~$
```

Step3-3 連線測試(Uplink ICMP)

在UE輸入 `ping 172.16.0.1 -c 10` 測試 Uplink ICMP 能不能正常運作

```
user@Lab01ue:~$ ping 172.16.0.1 -c 10
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=55
.6 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=64 time=35
.1 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=64 time=83
.0 ms
64 bytes from 172.16.0.1: icmp_seq=4 ttl=64 time=47
.0 ms
64 bytes from 172.16.0.1: icmp_seq=5 ttl=64 time=60
.0 ms
64 bytes from 172.16.0.1: icmp_seq=6 ttl=64 time=75
.0 ms
64 bytes from 172.16.0.1: icmp_seq=7 ttl=64 time=90
.3 ms
64 bytes from 172.16.0.1: icmp_seq=8 ttl=64 time=36
.6 ms
64 bytes from 172.16.0.1: icmp_seq=9 ttl=64 time=86
.0 ms
64 bytes from 172.16.0.1: icmp_seq=10 ttl=64 time=6
3.9 ms

--- 172.16.0.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss
, time 9010ms
rtt min/avg/max/mdev = 35.128/63.268/90.326/19.008
ms
user@Lab01ue:~$
```

Step3-4 連線測試(Uplink TCP)

在EPC空間的終端機輸入 `sudo iperf -s` 並在 UE 輸入 `iperf -c 172.16.0.1 -w 100M -t 10 -i 10 -r` 測試 Uplink TCP 能不能正常運作

```
user@Lab01ue:~$ iperf -c 172.16.0.1 -w 100M -t 10
-i 10 -r
-----
Server listening on TCP port 5001
TCP window size: 416 KByte (WARNING: requested 10
0 MByte)
-----
-----
Client connecting to 172.16.0.1, TCP port 5001
TCP window size: 416 KByte (WARNING: requested 10
0 MByte)
-----
-----
[ 3] local 172.16.0.4 port 50326 connected with 17
2.16.0.1 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0-10.0 sec  4.12 MBytes 3.46 Mbits/sec
[ 3] 0.0-10.1 sec  4.12 MBytes 3.44 Mbits/sec
[ 3] local 172.16.0.4 port 5001 connected with 172
.16.0.1 port 57180
[ 3] 0.0-10.0 sec  10.2 MBytes 8.58 Mbits/sec
[ 3] 0.0-11.1 sec  11.4 MBytes 8.58 Mbits/sec
[SUM] 0.0-11.1 sec  21.6 MBytes 16.3 Mbits/sec
user@Lab01ue:~$
```

Step4-1 外連設定(封包轉送)

在 EPC 空間的終端機輸入

`echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward` 以開啟 Linux 核心的封包轉送功能

```
user@Lab01epc:~$ sudo echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
[sudo] password for user:
1
user@Lab01epc:~$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
1
user@Lab01epc:~$
```


Step4-2 外連設定(NAT規則)

在 EPC空間的終端機輸入 `sudo iptables -A POSTROUTING -t nat -o ens3 -s 172.16.0.0/24 -j MASQUERADE` 以進行 NAT 規則設定，可使用 `sudo iptables -L POSTROUTING -t nat` 來檢查

```
user@Lab01epc:~$ sudo iptables -L POSTROUTING -t nat
Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
user@Lab01epc:~$ sudo iptables -A POSTROUTING -t nat -o ens3 -s 172.16.0.0/24 -j MASQUERADE
user@Lab01epc:~$ sudo iptables -L POSTROUTING -t nat
Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  172.16.0.0/24          anywhere
user@Lab01epc:~$
```

Step4-3 外連設定(UE路由)

在UE的終端機輸入 `sudo ip route add default via 172.16.0.1 dev tun_srsue` 以設定 default gateway，可使用 `sudo ip route show` 來檢查

```
user@Lab01ue:~$ sudo ip route add default via 172.16.0.1 dev tun_srsue
user@Lab01ue:~$ sudo ip route show
default via 172.16.0.1 dev tun_srsue
default via 10.0.0.1 dev ens3 proto static metric 20100
10.0.0.0/24 dev ens3 proto kernel scope link src 10.0.0.2 metric 100
169.254.0.0/16 dev ens3 scope link metric 1000
172.16.0.0/24 dev tun_srsue proto kernel scope link src 172.16.0.3
user@Lab01ue:~$
```

Step5 測試能否連到Internet

在UE的終端機輸入 `ping 8.8.8.8 -c 10` 以測試使否能正確連到 Internet

```
user@Lab01ue:~$ ping 8.8.8.8 -c 10
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=254 time=262
ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=254 time=115
ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=254 time=241
ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=254 time=189
ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=254 time=172
ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=254 time=276
ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=254 time=117
ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=254 time=218
ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=254 time=345
ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=254 time=97.
8 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss
, time 901ms
rtt min/avg/max/mdev = 97.784/203.261/345.141/76.16
3 ms
```


Stage 3 Check List

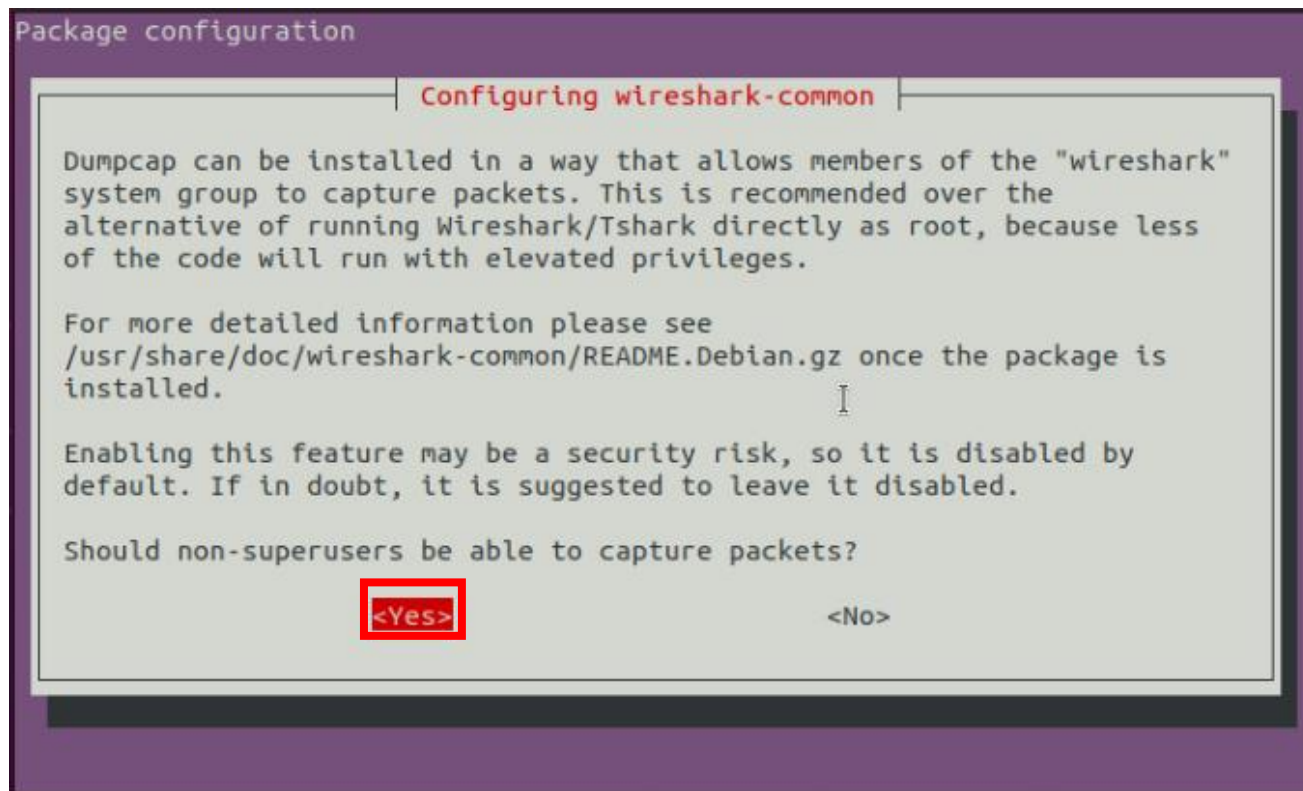
項目	內容
srsepc	確認 srsepc 之視窗沒有任何錯誤訊息，且SPGW順利核發 IP 給新連入之 UE。
srsenb	確認 srsenb 之視窗沒有任何錯誤訊息，且順利與 UE 建立連線。
srsue	確認 srsue 之視窗沒有任何錯誤訊息，且順利連上 eNB。
Uplink 連線是否正常	UE 能順利對 EPC 執行 ping 及 iperf
Downlink 連線是否正常	EPC 能順利對 UE 執行 ping 及 iperf
UE 能否連上 Internet	UE 是否能順利 ping Internet 上的主機，如 8.8.8.8

Outline

- 實驗目的及實驗內容
- 背景知識
- 實驗環境
- Stage 1: 環境架設
- Stage 2: srsLTE 及 ZeroMQ 編譯安裝
- Stage 3: srsLTE 執行及測試
- Stage 4: srsLTE 封包觀測
 - Step1: 安裝 Wireshark 及介面介紹
 - Step2: 介面及觀測過濾器設定
 - Step3: 觀測eNB啟動流程
 - Step4: 觀測UE連接流程
 - Step5: 觀測使用者平面
 - Step6: 觀測UE離線流程
 - Step7: 觀測eNB關閉流程
- 總結及問題

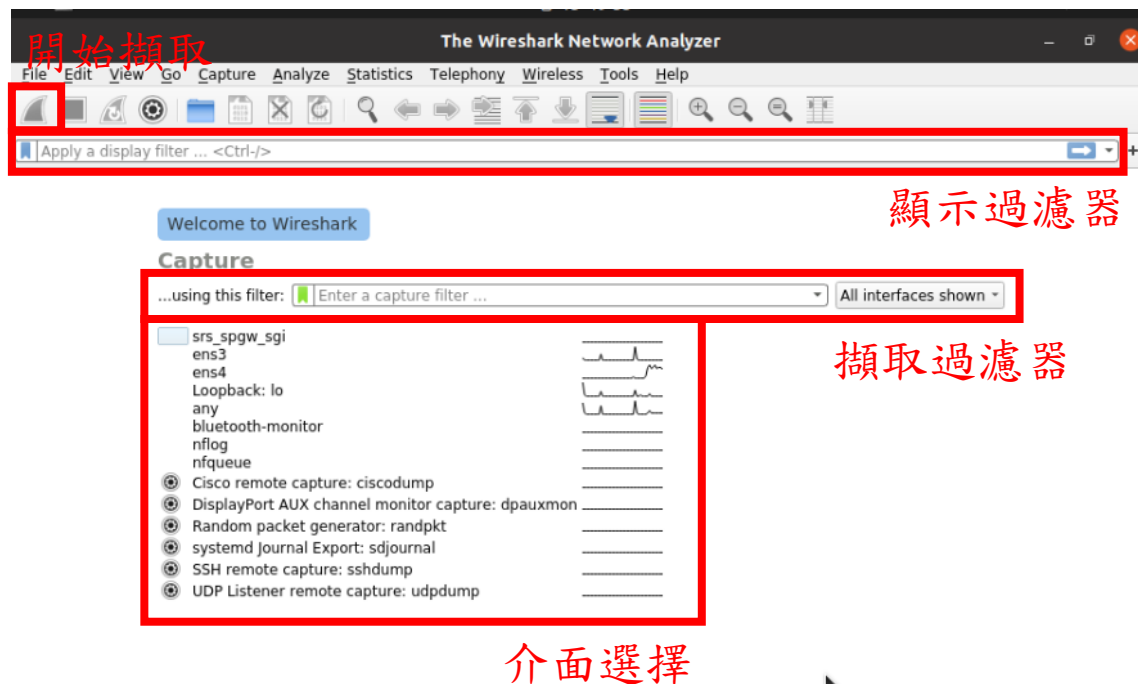
Step1-1 安裝 Wireshark

在EPC的終端機輸入 `sudo add-apt-repository ppa:wireshark-dev/stable && sudo apt update && sudo apt-get -y install wireshark` 以安裝 Wireshark，若出現以下畫面請選擇yes



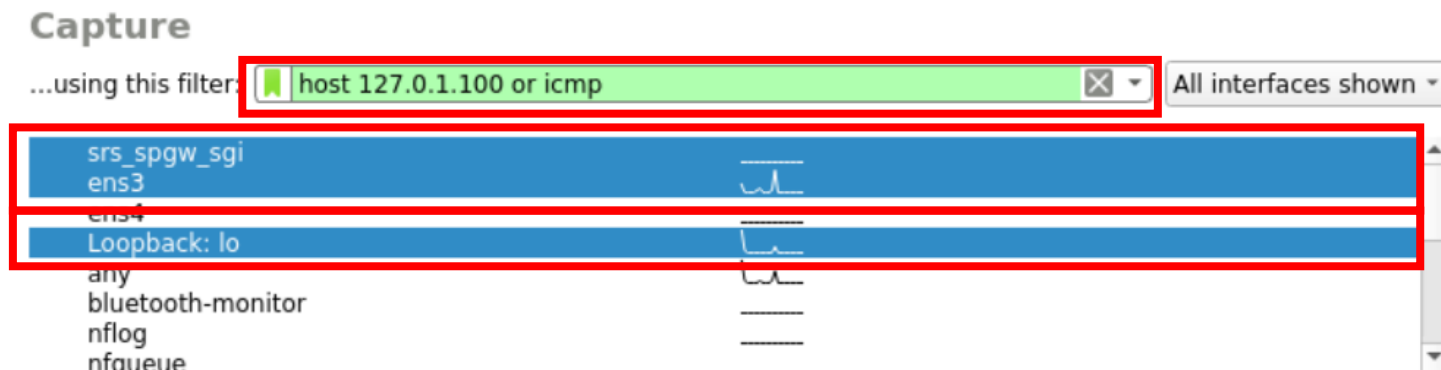
Step1-2 Wireshark 介面介紹

在EPC的終端機輸入 `sudo wireshark` 以啟動 Wireshark，其介面介紹如圖所示



Step2 介面及觀測過濾器設定

開啟 EPC 後在 Wireshark 按住 Shift 選擇 **lo**、**ens3** 及 **srs_spgw_sgi** 介面並將擷取過濾器設定為 **host 127.0.1.100 or icmp** 後按下 Enter 即可開始擷取



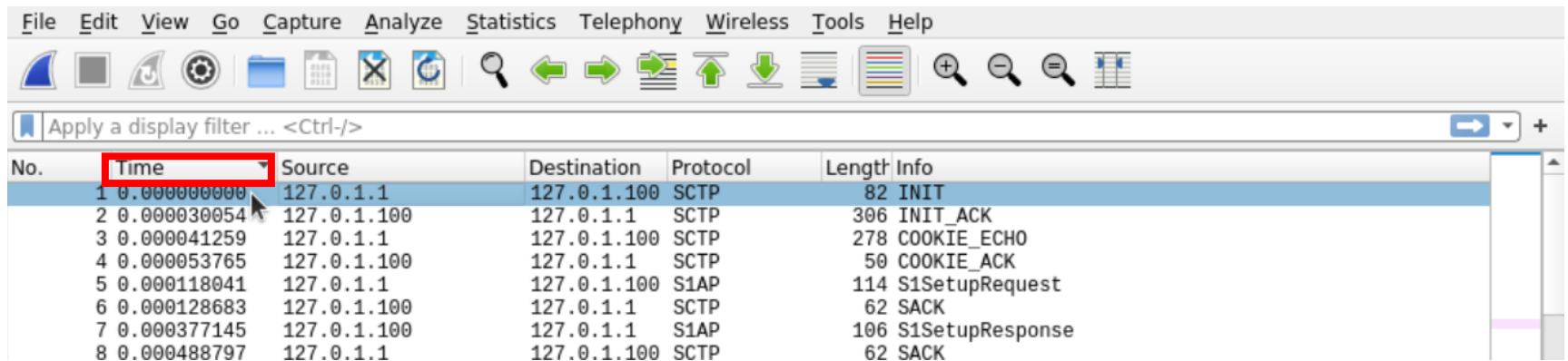
Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.2.4 (Git v3.2.4 packaged as 3.2.4-1~ubuntu20.04.0+wiresharkdevstable1).

Step3-1 觀測eNB啟動流程

點選Time欄位以時間進行排序後再按照Stage3的步驟啟動eNB後應可看到Wireshark上出現如下8個封包。其中S1AP通訊協定的S1SetupRequest及S1SetupResponse為本次觀察重點。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	127.0.1.1	127.0.1.100	SCTP	82	INIT
2	0.000030054	127.0.1.100	127.0.1.1	SCTP	306	INIT_ACK
3	0.000041259	127.0.1.1	127.0.1.100	SCTP	278	COOKIE_ECHO
4	0.000053765	127.0.1.100	127.0.1.1	SCTP	50	COOKIE_ACK
5	0.000118041	127.0.1.1	127.0.1.100	S1AP	114	S1SetupRequest
6	0.000128683	127.0.1.100	127.0.1.1	SCTP	62	SACK
7	0.000377145	127.0.1.100	127.0.1.1	S1AP	106	S1SetupResponse
8	0.000488797	127.0.1.1	127.0.1.100	SCTP	62	SACK

Step3-2 S1SeutpRequest

點選 **S1SetupRequest** 封包以檢視其詳細內容，比對 **macroENB-ID** 欄位扣除尾端4位元的padding後是否與eNB設定檔(/etc/srslte/enb.conf)相符合。

1	0.000000000	127.0.1.1	127.0.1.100	SCTP	82	INIT
2	0.000030054	127.0.1.100	127.0.1.1	SCTP	306	INIT_ACK
3	0.000041259	127.0.1.1	127.0.1.100	SCTP	278	COOKIE_ECHO
4	0.000053765	127.0.1.100	127.0.1.1	SCTP	50	COOKIE_ACK
5	0.000118041	127.0.1.1	127.0.1.100	S1AP	114	S1SetupRequest
6	0.000128683	127.0.1.100	127.0.1.1	SCTP	62	SACK
7	0.000237445	127.0.1.100	127.0.1.1	S1AP	106	S1SetupResponse

▶ Transmission sequence number: 1721475745
 Stream identifier: 0x0000
 Stream sequence number: 0
 Payload protocol identifier: S1 Application Protocol (S1AP) (18)
 Chunk padding: 000000

▼ S1 Application Protocol
 ▼ S1AP-PDU: initiatingMessage (0)
 ▼ initiatingMessage
 procedureCode: id-S1Setup (17)
 criticality: reject (0)
 ▼ value
 ▼ S1SetupRequest
 ▼ protocolIEs: 4 items
 ▼ Item 0: id-Global-ENB-ID
 ▼ ProtocolIE-Field
 id: id-Global-ENB-ID (59)
 criticality: reject (0)
 ▼ value
 ▼ Global-ENB-ID
 plmnIdentity: 00f110
 mobileCountryCode: Mobile Country Code (MCC): Unknown (1)
 mobileNetworkCode: Mobile Network Code (MNC): Unknown (01)
 ▼ eNB-ID: id-eNB-ID (10)
 macroENB-ID: 0019b0 [b] t length 20, 4 LSB pad bits, 0000 0000 0001 1001 1011 decimal va...

▼ Item 1: id-eNBname
 ▼ ProtocolIE-Field
 id: id-eNBname (60)
 criticality: ignore (1)
 ▼ value
 ENBname: rsrenb01

▼ Item 2: id-SupportedTAs
 ▼ Item 3: id-DefaultPagingDRX

```

[enb]
enb_id = 0x19B
mcc = 001
mnc = 01
mme_addr = 127.0.1.100
gtp_bind_addr = 127.0.1.1
s1c_bind_addr = 127.0.1.1
n_prb = 50
#tm = 4
#nof_ports = 2
        
```

Step3-3 S1SetupResponse

點選**S1SetupResponse**封包以檢視其詳細內容，比對**MME-Code**欄位否與EPC設定檔(/etc/srslte/epc.conf)相符合。

The image shows a Wireshark packet capture of an S1SetupResponse message. The packet list on the left shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000053765	127.0.1.100	127.0.1.1	SCTP	50	COOKIE_ACK
5	0.000118041	127.0.1.1	127.0.1.100	S1AP	114	S1SetupRequest
6	0.000128683	127.0.1.100	127.0.1.1	SCTP	62	SACK
7	0.000377145	127.0.1.100	127.0.1.1	S1AP	106	S1SetupResponse
8	0.000488797	127.0.1.1	127.0.1.100	SCTP	62	SACK
9	8.758144213	127.0.1.1	127.0.1.100	S1AP/NAS-EPS	150	

The details pane for the selected S1SetupResponse packet (packet 7) shows the following structure:

- S1SetupResponse
 - protocolIEs: 3 items
 - Item 0: id-MMENAME
 - ProtocolIE-Field
 - id: id-MMENAME (61)
 - criticality: ignore (1)
 - value
 - MMENAME: srsme01
 - Item 1: id-ServedGUMMEIs
 - ProtocolIE-Field
 - id: id-ServedGUMMEIs (105)
 - criticality: reject (0)
 - value
 - ServedGUMMEIs: 1 item
 - Item 0
 - ServedGUMMEIsItem
 - servedPLMNs: 1 item
 - Item 0
 - PLMNIdentity: 00f110
 - Mobile Country Code (MCC): Unknown
 - Mobile Network Code (MNC): Unknown (01)
 - servedGroupIDs: 1 item
 - Item 0
 - MME-Group-ID: 256 (0x0100)
 - servedMMECs: 1 item
 - Item 0
 - MME-Code: 26 (0x1a)
 - Item 2: id-RelativeMMECapacity
 - ProtocolIE-Field
 - id: id-RelativeMMECapacity (87)
 - criticality: ignore (1)
 - value
 - RelativeMMECapacity: 255

The hex data pane on the right shows the following values:

```
[mme]
mme_code = 0x1a
mme_group = 0x0001
tac = 0x0007
mcc = 001
mnc = 01
mme_bind_addr = 127.0.1.100
apn = srsapn
dns_addr = 8.8.8.8
encryption_algo = EEA0
integrity_algo = EIA1
paging_timer = 2
```


Step3-4 HEARTBEAT

當eNB連上EPC後應可以在Wireshark看到MME和eNB兩者每隔30秒透過SCTP向對方傳送一次HEARTBEAT的訊號以確認連線依然存在。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------|-------------|----------|--------|---------------|
| 71 | 40.487776978 | 127.0.1.1 | 127.0.1.100 | SCTP | 98 | HEARTBEAT |
| 72 | 40.487781200 | 127.0.1.100 | 127.0.1.1 | SCTP | 98 | HEARTBEAT |
| 73 | 40.487826286 | 127.0.1.100 | 127.0.1.1 | SCTP | 98 | HEARTBEAT_ACK |
| 74 | 40.487829818 | 127.0.1.1 | 127.0.1.100 | SCTP | 98 | HEARTBEAT_ACK |

| |
|---|
| ▶ Frame 71: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface lo, id 2 |
| ▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00) |
| ▶ Internet Protocol Version 4, Src: 127.0.1.1, Dst: 127.0.1.100 |
| ▼ Stream Control Transmission Protocol, Src Port: 56763 (56763), Dst Port: 36412 (36412) |
| Source port: 56763 |
| Destination port: 36412 |
| Verification tag: 0xa70a7d59 |
| [Association index: 65535] |
| Checksum: 0x00000000 [unverified] |
| [Checksum Status: Unverified] |
| ▼ HEARTBEAT chunk (Information: 48 bytes) |
| ▼ Chunk type: HEARTBEAT (4) |
| 0... .. = Bit: Stop processing of the packet |
| .0.. .. = Bit: Do not report |
| Chunk flags: 0x00 |
| Chunk length: 52 |
| ▶ Heartbeat info parameter (Information: 44 bytes) |

Step4-1 觀測UE連接流程

按照Stage3的步驟啟動UE後應可在Wireshark上觀察到如下的封包，由於本實驗並無觀測 UE 和 eNB 間的介面訊息，因此來源位址為127.0.1.1且通訊協定為S1AP/NAS-EPS的封包即為來自UE的訊息。

可以觀察到UE和MME間控制平面所使用的通訊協定主要為NAS，且在UE連接的過程中主要分為連接請求、身分確認、認證、安全模式協商、連接完成五大步驟。

| | | | | | |
|----|-------------|------------------------|-------------|--------------|---|
| 9 | 8.758144213 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 150 InitialUEMessage, Attach request, PDN connectivi... |
| 10 | 8.758462515 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 106 DownlinkNASTransport, Identity request |
| 11 | 8.821400180 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 UplinkNASTransport, Identity response |
| 12 | 8.822030712 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 138 DownlinkNASTransport, Authentication request |
| 13 | 8.888152139 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 UplinkNASTransport, Authentication response |
| 14 | 8.888777001 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 118 DownlinkNASTransport, Security mode command |
| 15 | 8.962884415 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 134 UplinkNASTransport, Security mode complete |
| 16 | 8.963699314 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 258 InitialContextSetupRequest, Attach accept, Activ... |
| 17 | 9.107242720 | 127.0.1.1 | 127.0.1.100 | S1AP | 118 InitialContextSetupResponse |
| 18 | 9.301305514 | fe80::12f:7da2:1412... | ff02::2 | GTP <ICMPv6> | 98 Router Solicitation |
| 19 | 9.310699739 | 127.0.1.100 | 127.0.1.1 | SCTP | 62 SACK |
| 20 | 9.310809283 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 122 UplinkNASTransport, Attach complete, Activate de... |
| 21 | 9.311462607 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 146 DownlinkNASTransport, EMM information |
| 22 | 9.514689233 | 127.0.1.1 | 127.0.1.100 | SCTP | 62 SACK |

Step4-2 連接請求

點選**InitialUEMessage**, **Attach request**封包以檢視其詳細內容，記錄其中的**ENB-UE-S1AP-ID** 以便後續識別連線內容。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|--------------|--------|---|
| 7 | 0.000377145 | 127.0.1.100 | 127.0.1.1 | S1AP | 106 | S1SetupResponse |
| 8 | 0.000488797 | 127.0.1.1 | 127.0.1.100 | SCTP | 62 | SACK |
| 9 | 8.758144213 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 150 | InitialUEMessage, Attach request, PDN connectivi... |
| 10 | 8.758462515 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 106 | DownlinkNASTransport, Identity request |
| 11 | 8.821400180 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Identity response |
| 12 | 8.822030712 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 138 | DownlinkNASTransport, Authentication request |
| 13 | 8.808152120 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Authentication response |

| |
|--|
| ▼ S1 Application Protocol |
| ▼ S1AP-PDU: initiatingMessage (0) |
| ▼ initiatingMessage |
| procedureCode: id-initialUEMessage (12) |
| criticality: ignore (1) |
| ▼ value |
| ▼ InitialUEMessage |
| ▼ protocolIEs: 6 items |
| ▼ Item 0: id-eNB-UE-S1AP-ID |
| ▼ ProtocolIE-Field |
| id: id-eNB-UE-S1AP-ID (8) |
| criticality: reject (0) |
| ▼ value |
| ENB-UE-S1AP-ID: 1 |
| ▼ Item 1: id-NAS-PDU |
| ▼ ProtocolIE-Field |
| id: id-NAS-PDU (26) |
| criticality: reject (0) |
| ▼ value |
| NAS-PDU: 1746262ec7030741010bf600f11000011a2d408ba002f070... |
| ▼ Non-Access-Stratum (NAS)PDU |
| 0001 = Security header type: Integrity protected (1) |
| 0111 = Protocol discriminator: EPS mobility management messages (0x7) |
| Message authentication code: 0x46262ec7 |
| Sequence number: 3 |
| 0000 = Security header type: Plain NAS message, not security protected (0) |
| 0111 = Protocol discriminator: EPS mobility management messages (0x7) |
| NAS EPS Mobility Management Message Type: Attach request (0x41) |
| 0... = Type of security context flag (TSC): Native security context (for KSIasme) |
| .000 = NAS key set identifier: (0) |
| 0... = Spare bit(s): 0x00 |
|001 = EPS attach type: EPS attach (1) |
| ▼ EPS mobile identity |

Step4-3 身分確認(Identity request)

點選**DownlinkNASTransport, Identity request**封包以檢視其詳細內容，記錄其中的**MME-UE-S1AP-ID** 以便後續識別連線內容。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|--------------|--------|---|
| 7 | 0.000377145 | 127.0.1.100 | 127.0.1.1 | S1AP | 106 | S1SetupResponse |
| 8 | 0.000488797 | 127.0.1.1 | 127.0.1.100 | SCTP | 62 | SACK |
| 9 | 8.758144213 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 150 | InitialUEMessage, Attach request, PDN connectivi... |
| 10 | 8.758462515 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 106 | DownlinkNASTransport, Identity request |
| 11 | 8.821400180 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Identity response |
| 12 | 8.822030712 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 138 | DownlinkNASTransport, Authentication request |
| 13 | 8.888452120 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Authentication response |

| |
|---|
| ▼ S1 Application Protocol |
| ▼ S1AP-PDU: initiatingMessage (0) |
| ▼ initiatingMessage |
| procedureCode: id-downlinkNASTransport (11) |
| criticality: ignore (1) |
| ▼ value |
| ▼ DownlinkNASTransport |
| ▼ protocolIEs: 3 items |
| ▼ Item 0: id-MME-UE-S1AP-ID |
| ▼ ProtocolIE-Field |
| id: id-MME-UE-S1AP-ID (0) |
| criticality: reject (0) |
| ▼ value |
| MME-UE-S1AP-ID: 1 |
| ▼ Item 1: id-eNB-UE-S1AP-ID |
| ▼ ProtocolIE-Field |
| id: id-eNB-UE-S1AP-ID (8) |
| criticality: reject (0) |
| ▼ value |
| eNB-UE-S1AP-ID: 1 |

Step4-3 身分確認(Identity response)

點選UplinkNASTransport, Identity response封包以檢視其詳細內容，確認其中的 **IMSI** 欄位與 UE 設定檔 (/etc/srslte/ue.conf)相符合。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|--------------|--------|---|
| 7 | 0.000377145 | 127.0.1.100 | 127.0.1.1 | SIAP | 106 | SISetupResponse |
| 8 | 0.000488797 | 127.0.1.1 | 127.0.1.100 | SCTP | 62 | SACK |
| 9 | 8.758144213 | 127.0.1.1 | 127.0.1.100 | SIAP/NAS-EPS | 150 | InitialUEMessage, Attach request, PDN connectivi... |
| 10 | 8.758462515 | 127.0.1.100 | 127.0.1.1 | SIAP/NAS-EPS | 106 | DownlinkNASTransport, Identity request |
| 11 | 8.821400180 | 127.0.1.1 | 127.0.1.100 | SIAP/NAS-EPS | 138 | UplinkNASTransport, Identity response |
| 12 | 8.822030712 | 127.0.1.100 | 127.0.1.1 | SIAP/NAS-EPS | 138 | DownlinkNASTransport, Authentication request |
| 13 | 8.880453420 | 127.0.1.1 | 127.0.1.100 | SIAP/NAS-EPS | 138 | UplinkNASTransport, Authentication response |

▼ S1 Application Protocol

▼ SIAP-PDU: initiatingMessage (0)

▼ initiatingMessage

procedureCode: id-uplinkNASTransport (13)

criticality: ignore (1)

▼ value

▼ UplinkNASTransport

protocolIEs: 5 items

Item 0: id-MME-UE-S1AP-ID

▼ ProtocolIE-Field

id: id-MME-UE-S1AP-ID (0)

criticality: reject (0)

value

MME-UE-S1AP-ID: 1

Item 1: id-eNB-UE-S1AP-ID

▼ ProtocolIE-Field

id: id-eNB-UE-S1AP-ID (8)

criticality: reject (0)

value

eNB-UE-S1AP-ID: 1

Item 2: id-NAS-PDU

▼ ProtocolIE-Field

id: id-NAS-PDU (26)

criticality: reject (0)

value

NAS-PDU: 0756080910101032547698

▼ Non-Access-Stratum (NAS)PDU

0000 = Security header type: Plain NAS message, not security protected (0)

.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)

NAS EPS Mobility Management Message type: Identity response (0x56)

Mobile identity - IMSI (001010123456789)

Item 3: id-EUTRAN-Cell-ID

▼ ProtocolIE-Field

```
[usin]
mode = soft
algo = xor
#opc = 63BFA50EE6523365FF14C1F45F88737D
k = 00112233445566778899aabbccddeeff
imsi = 001010123456789
imei = 353490069873319
#reader =
#pin = 1234
```

Step4-4 認證(Request)

點選 **DownlinkNASTransoprt, Authentication request** 以檢視其詳細內容，可以觀察到MME對UE傳送了EPS challenge 的訊息。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|--------------|--------|--|
| 10 | 8.758462515 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 106 | DownlinkNASTransport, Identity request |
| 11 | 8.821400180 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Identity response |
| 12 | 8.822030712 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 138 | DownlinkNASTransport, Authentication request |
| 13 | 8.888152139 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Authentication response |
| 14 | 8.888777001 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 118 | DownlinkNASTransport, Security mode command |

protocolIEs: 3 items

Item 0: id-MME-UE-S1AP-ID

ProtocolIE-Field

id: id-MME-UE-S1AP-ID (0)

criticality: reject (0)

value

MME-UE-S1AP-ID: 1

Item 1: id-eNB-UE-S1AP-ID

ProtocolIE-Field

id: id-eNB-UE-S1AP-ID (8)

criticality: reject (0)

value

eNB-UE-S1AP-ID: 1

Item 2: id-NAS-PDU

ProtocolIE-Field

id: id-NAS-PDU (26)

criticality: reject (0)

value

NAS-PDU: 075200f3395c38b260f055cd01f0ea3dd5216b100bf63596...

Non-Access-Stratum (NAS)PDU

0000 = Security header type: Plain NAS message, not security protected (0)

.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)

NAS EPS Mobility Management Message Type: Authentication request (0x52)

0000 = Spare half octet: 0

.... 0... = Type of security context flag (TSC): Native security context (for KSIasme)

0000 = NAS key set identifier: (0) ASME

Authentication Parameter RAND - EPS challenge

RAND value: f3395c38b260f055cd01f0ea3dd5216b

Authentication Parameter AUTN (UMTS and EPS authentication challenge) - EPS challenge

Length: 16

AUTN value: 0bf6359631c59001f3287e0be5b50623

SQN xor AK: 0bf6359631c5

AMF: 9001

MAC: f3287e0be5b50623

Step4-4 認證(Response)

點選UplinkNASTransprt, Authentication response以檢視其詳細內容，可以觀察到UE透過EPS challenge的訊息及自身的USIM算出challenge的結果並回傳給MME，若此訊息正確MME才會進一步處理連接請求。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|--------------|--------|--|
| 10 | 8.758462515 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 106 | DownlinkNASTransport, Identity request |
| 11 | 8.821490180 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Identity response |
| 12 | 8.822030712 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 138 | DownlinkNASTransport, Authentication request |
| 13 | 8.888152139 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Authentication response |
| 14 | 8.888777001 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 118 | DownlinkNASTransport, Security mode command |

UplinkNASTransport

protocolIEs: 5 items

Item 0: id-MME-UE-S1AP-ID

ProtocolIE-Field

id: id-MME-UE-S1AP-ID (0)

criticality: reject (0)

value

MME-UE-S1AP-ID: 1

Item 1: id-eNB-UE-S1AP-ID

ProtocolIE-Field

id: id-eNB-UE-S1AP-ID (8)

criticality: reject (0)

value

eNB-UE-S1AP-ID: 1

Item 2: id-NAS-PDU

ProtocolIE-Field

id: id-NAS-PDU (26)

criticality: reject (0)

value

NAS-PDU: 075308f3287e0bf6359622

Non-Access-Stratum (NAS) PDU

0000 = Security header type: Plain NAS message, not security protected (0)

.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)

NAS EPS Mobility Management Message Type: Authentication response (0x53)

Authentication response parameter

RES: f3287e0bf6359622

Item 3: id-EUTRAN-CGI

ProtocolIE-Field

id: id-EUTRAN-CGI (100)

criticality: ignore (1)

value

EUTRAN-CGI

PLMNidentity: 00f110

Step4-5 安全模式協商 (Command)

點選DownlinkNASTransport, Security mode command封包以檢視其詳細內容，可以觀察到MME在本次連接中選擇了EEA0作為加解密演算法，同時也選擇了128-EIA1作為資料完整性演算法，此二者皆可於MME的設定檔設定。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|--------------|--------|---|
| 13 | 8.888152139 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Authentication |
| 14 | 8.888777001 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 118 | DownlinkNASTransport, Security mode command |
| 15 | 8.962884415 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 134 | UplinkNASTransport, Security mode complete |
| 16 | 8.963699314 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 258 | InitialContextSetupRequest |
| 17 | 9.107242720 | 127.0.1.1 | 127.0.1.100 | S1AP | 118 | InitialContextSetupResponse |

| | |
|--|--|
| value | NAS-PDU: 3701d5717500075d010002f070 |
| Non-Access-Stratum (NAS)PDU | |
| 0011 | = Security header type: Integrity protected with new EPS security |
| 0111 | = Protocol discriminator: EPS mobility management messages |
| Message authentication code: 0x01d57175 | |
| Sequence number: 0 | |
| 0000 | = Security header type: Plain NAS message, not security protected |
| 0111 | = Protocol discriminator: EPS mobility management messages |
| NAS EPS Mobility Management Message Type: Security mode command (0x5d) | |
| NAS security algorithms - Selected NAS security algorithms | |
| 0... .. | = Spare bit(s): 0x00 |
| .000 ... | = Type of ciphering algorithm: EPS encryption algorithm EEA0 |
| 0... | = Spare bit(s): 0x00 |
|001 | = Type of integrity protection algorithm: EPS integrity algorithm 128-EIA1 (1) |
| 0000 | = Spare half octet: 0 |
| 0... | = Type of security context flag (TSC): Native security context (for KSIasme) |
|000 | = NAS key set identifier: (0) ASME |
| UE security capability - Replayed UE security capabilities | |

[mme]
mme_code = 0x1a
mme_group = 0x0001
tac = 0x0007
mcc = 001
mnc = 01
mme_bind_addr = 127.0.1.100
apn = srsapn
dns_addr = 8.8.8.8
encryption_algo = EEA0
integrity_alao = EIA1
paging_timer = 2

Step4-5 安全模式協商 (Complete)

點選UplinkNASTransport, Security mode complete封包以檢視其詳細內容，UE同意MME所選擇的安全套件並回傳Security mode compete。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|--------------|--------|---|
| 13 | 9.491063500 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Authentication response |
| 14 | 9.492305195 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 118 | DownlinkNASTransport, Security mode command |
| 15 | 9.573489495 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 134 | UplinkNASTransport, Security mode complete |
| 16 | 9.574934563 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 258 | InitialContextSetupRequest, Attach accept, Activ... |
| 17 | 0.702769506 | 127.0.1.1 | 127.0.1.100 | S1AP | 118 | InitialContextSetupResponse |

| |
|---|
| ▼ initiatingMessage |
| procedureCode: id-uplinkNASTransport (13) |
| criticality: ignore (1) |
| ▼ value |
| ▼ UplinkNASTransport |
| ▼ protocolIEs: 5 items |
| ▼ Item 0: id-MME-UE-S1AP-ID |
| ▼ ProtocolIE-Field |
| id: id-MME-UE-S1AP-ID (0) |
| criticality: reject (0) |
| ▼ value |
| MME-UE-S1AP-ID: 1 |
| ▼ Item 1: id-eNB-UE-S1AP-ID |
| ▼ ProtocolIE-Field |
| id: id-eNB-UE-S1AP-ID (8) |
| criticality: reject (0) |
| ▼ value |
| ENB-UE-S1AP-ID: 1 |
| ▼ Item 2: id-NAS-PDU |
| ▼ ProtocolIE-Field |
| id: id-NAS-PDU (26) |
| criticality: reject (0) |
| ▼ value |
| NAS-PDU: 475eb9d83300075e |
| ▼ Non-Access-Stratum (NAS)PDU |
| 0100 = Security header type: Integrity protected and ciphered with new EPS security context (4 |
| 0111 = Protocol discriminator: EPS mobility management messages (0x7) |
| Message authentication code: 0x5eb9d833 |
| Sequence number: 0 |
| 0000 = Security header type: Plain NAS message, not security protected (0) |
| 0111 = Protocol discriminator: EPS mobility management messages (0x7) |
| NAS EPS Mobility Management Message Type: Security mode complete (0x5e) |
| ▼ Item 3: id-ECM-MO |
| ▼ ProtocolIE-Field |

Step4-6 連接完成(Attach Accept)

點選InitialContextSetupRequest, Attach accept封包以檢視其詳細內容，確認其中的 **MME-UE-S1AP-ID** 與 **ENB-UE-S1AP-ID** 相符合，若出現此訊息表示MME接受UE的連接請求。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|------------------------|-------------|--------------|--------|---|
| 13 | 8.888152139 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 138 | UplinkNASTransport, Authentication response |
| 14 | 8.888777001 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 118 | DownlinkNASTransport, Security mode command |
| 15 | 8.962884415 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 134 | UplinkNASTransport, Security mode complete |
| 16 | 8.963699314 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 258 | InitialContextSetupRequest, Attach accept, Activ... |
| 17 | 9.107242720 | 127.0.1.1 | 127.0.1.100 | S1AP | 118 | InitialContextSetupResponse |
| 18 | 9.301305514 | fe80::12f:7da2:1412... | ff02::2 | GTP <ICMPv6> | 98 | Router Solicitation |
| 19 | 9.310600720 | 127.0.1.100 | 127.0.1.1 | ICMPv6 | 62 | ACK |

| |
|---|
| ▼ S1 Application Protocol |
| ▼ S1AP-PDU: initiatingMessage (0) |
| ▼ initiatingMessage |
| procedureCode: id-InitialContextSetup (9) |
| criticality: reject (0) |
| ▼ value |
| ▼ InitialContextSetupRequest |
| ▼ protocolIEs: 6 items |
| ▼ Item 0: id-MME-UE-S1AP-ID |
| ▼ ProtocolIE-Field |
| id: id-MME-UE-S1AP-ID (0) |
| criticality: reject (0) |
| ▼ value |
| MME-UE-S1AP-ID: 1 |
| ▼ Item 1: id-ENB-UE-S1AP-ID |
| ▼ ProtocolIE-Field |
| id: id-eNB-UE-S1AP-ID (8) |
| criticality: reject (0) |
| ▼ value |
| ENB-UE-S1AP-ID: 1 |
| ▼ Item 2: id-AggregateMaximumBitrate |

Step4-6 連接完成(Attach Complete)

點選UplinkNASTransport, Attach complete封包以檢視其詳細內容，確認其中的 **MME-UE-S1AP-ID** 與 **ENB-UE-S1AP-ID** 相符合，若出現此訊息表示UE已順利連接。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|------------------------|-------------|--------------|--------|---|
| 16 | 8.963699314 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 258 | InitialContextSetupRequest, Attach accept, Activ... |
| 17 | 9.107242720 | 127.0.1.1 | 127.0.1.100 | S1AP | 118 | InitialContextSetupResponse |
| 18 | 9.301305514 | fe80::12f:7da2:1412... | ff02::2 | GTP <ICMPv6> | 98 | Router Solicitation |
| 19 | 9.310699739 | 127.0.1.100 | 127.0.1.1 | SCTP | 62 | SACK |
| 20 | 9.310809283 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 122 | UplinkNASTransport, Attach complete, Activate de... |
| 21 | 9.311462607 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 146 | DownlinkNASTransport, EMM information |
| 22 | 9.514600222 | 127.0.1.1 | 127.0.1.100 | SCTP | 62 | SACK |

▶ Stream Control Transmission Protocol, Src Port: 58987 (58987), Dst Port: 36412 (36412)

▼ S1 Application Protocol

- ▼ S1AP-PDU: initiatingMessage (0)
 - ▼ initiatingMessage
 - procedureCode: id-uplinkNASTransport (13)
 - criticality: ignore (1)
 - ▼ value
 - ▼ UplinkNASTransport
 - ▼ protocolIEs: 5 items
 - ▼ Item 0: id-MME-UE-S1AP-ID
 - ▼ ProtocolIE-Field
 - id: id-MME-UE-S1AP-ID (0)
 - criticality: reject (0)
 - ▼ value
 - MME-UE-S1AP-ID: 1**
 - ▼ Item 1: id-ENB-UE-S1AP-ID
 - ▼ ProtocolIE-Field
 - id: id-ENB-UE-S1AP-ID (8)
 - criticality: reject (0)
 - ▼ value
 - ENB-UE-S1AP-ID: 1**
 - ▼ Item 2: id-NAS-PDU

Step4-6 連接完成(EMM Information)

連接完成後 MME 會向 UE 傳送 EMM 訊息，點選 **DownlinkNASTransport, EMM Information** 封包以檢視其內容，此訊息包含連入網路的名稱。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------|-------------|--------------|--------|---|
| 19 | 9.310699739 | 127.0.1.100 | 127.0.1.1 | SCTP | 62 | SACK |
| 20 | 9.310809283 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 122 | UplinkNASTransport, Attach complete, Activate de... |
| 21 | 9.311462607 | 127.0.1.100 | 127.0.1.1 | S1AP/NAS-EPS | 146 | DownlinkNASTransport, EMM information |
| 22 | 9.514689233 | 127.0.1.1 | 127.0.1.100 | SCTP | 62 | SACK |
| 24 | 25.928462486 | 172.16.0.2 | 8.8.8.8 | GTP <ICMP> | 134 | Echo (ping) request id=0x0006, seq=1/256, ttl=6... |
| 23 | 25.928603312 | 172.16.0.2 | 8.8.8.8 | ICMP | 84 | Echo (ping) request id=0x0006, seq=1/256, ttl=6... |
| 25 | 25.928700022 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0006, seq=1/256, ttl=2... |

ENB-UE-S1AP-ID: 1

Item 2: id-NAS-PDU

ProtocolIE-Field

id: id-NAS-PDU (26)

criticality: reject (0)

value

NAS-PDU: 27d95f27f6020761431882d3b7997e0fcbcb2069989c7e83...

Non-Access-Stratum (NAS)PDU

0010 = Security header type: Integrity protected and ciphered (2)

.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)

Message authentication code: 0xd95f27f6

Sequence number: 2

0000 = Security header type: Plain NAS message, not security protected (0)

.... 0111 = Protocol discriminator: EPS mobility management messages (0x7)

NAS EPS Mobility Management Message Type: EMM information (0x61)

Network Name - Full name for network

Element ID: 0x43

Length: 24

1... = Extension: No Extension

.000 = Coding Scheme: Cell Broadcast data coding scheme, GSM default alphabet, language uns

.... 0... = Add CI: The MS should not add the letters for the Country's Initials to the text str

.... .010 = Number of spare bits in last octet: bits 7 and 8 are spare and set to '0' in octet n

Text String: Software Radio Systems LTE

Network Name - Short Name

Element ID: 0x45

Length: 7

1... = Extension: No Extension

.000 = Coding Scheme: Cell Broadcast data coding scheme, GSM default alphabet, language uns

.... 0... = Add CI: The MS should not add the letters for the Country's Initials to the text str

.... .110 = Number of spare bits in last octet: bits 3 to 8(inclusive) are spare and set to '0' :

Text String: srsLTE

Step5-1 觀測使用者平面(流量產生)

在UE的終端機輸入 **ping 8.8.8.8** 以持續產生觀測流量，隨即應可在EPC上的Wireshark看到許多如下圖所示的GTP-U及ICMP的封包，若排序混亂的話可再點擊Time欄位以時間進行排序。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|------------|-------------|------------|--------|--|
| 25 | 32.828883368 | 172.16.0.2 | 8.8.8.8 | GTP <ICMP> | 134 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 27 | 32.828905660 | 172.16.0.2 | 8.8.8.8 | ICMP | 84 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 23 | 32.828928150 | 10.0.2.15 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 24 | 32.836061129 | 8.8.8.8 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| 28 | 32.836079463 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| 26 | 32.836148729 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| 33 | 33.796304765 | 172.16.0.2 | 8.8.8.8 | GTP <ICMP> | 134 | Echo (ping) request id=0x0008, seq=2/512, ttl=6... |
| 29 | 33.796327581 | 172.16.0.2 | 8.8.8.8 | ICMP | 84 | Echo (ping) request id=0x0008, seq=2/512, ttl=6... |
| 31 | 33.796337838 | 10.0.2.15 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x0008, seq=2/512, ttl=6... |
| 32 | 33.803376499 | 8.8.8.8 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply id=0x0008, seq=2/512, ttl=2... |
| 30 | 33.803388423 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0008, seq=2/512, ttl=2... |
| 34 | 33.803461911 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0008, seq=2/512, ttl=2... |
| 35 | 34.788515149 | 172.16.0.2 | 8.8.8.8 | GTP <ICMP> | 134 | Echo (ping) request id=0x0008, seq=3/768, ttl=6... |
| 39 | 34.788537390 | 172.16.0.2 | 8.8.8.8 | ICMP | 84 | Echo (ping) request id=0x0008, seq=3/768, ttl=6... |
| 37 | 34.788547286 | 10.0.2.15 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x0008, seq=3/768, ttl=6... |
| 38 | 34.795496362 | 8.8.8.8 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply id=0x0008, seq=3/768, ttl=2... |
| 40 | 34.795509095 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0008, seq=3/768, ttl=2... |
| 36 | 34.795895537 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0008, seq=3/768, ttl=2... |
| 45 | 35.816815338 | 172.16.0.2 | 8.8.8.8 | GTP <ICMP> | 134 | Echo (ping) request id=0x0008, seq=4/1024, ttl=... |
| 41 | 35.816839114 | 172.16.0.2 | 8.8.8.8 | ICMP | 84 | Echo (ping) request id=0x0008, seq=4/1024, ttl=... |
| 43 | 35.816848910 | 10.0.2.15 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x0008, seq=4/1024, ttl=... |
| 44 | 35.823862906 | 8.8.8.8 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply id=0x0008, seq=4/1024, ttl=... |
| 42 | 35.823874495 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0008, seq=4/1024, ttl=... |
| 46 | 35.823988971 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0008, seq=4/1024, ttl=... |

Step5-2 觀測使用者平面(GTP-U)

點擊其中任意一個GTP-U封裝的ICMP request封包以檢視其內容，可以觀察到此GTP-U封包的底層IP來源為127.0.1.1且目的UDP port為2152，表示有封包透過GTP隧道從eNB傳送至S-GW，此隧道可以以TEID識別。

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|------------|-------------|------------|--------|--|
| → 25 | 32.828883368 | 172.16.0.2 | 8.8.8.8 | GTP <ICMP> | 134 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 27 | 32.828905660 | 172.16.0.2 | 8.8.8.8 | ICMP | 84 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 23 | 32.828928150 | 10.0.2.15 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 24 | 32.836061129 | 8.8.8.8 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| 28 | 32.836079463 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| ← 26 | 32.836148729 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |

| | |
|---|--|
| ▶ Frame 25: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface lo, id 2 | |
| Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00) | |
| Internet Protocol Version 4, Src: 127.0.1.1, Dst: 127.0.1.100 | |
| User Datagram Protocol, Src Port: 2152, Dst Port: 2152 | |
| GPRS Tunneling Protocol | |
| Flags: 0x30 | |
| 001. = Version: GTP release 99 version (1) | |
| ...1 = Protocol type: GTP (1) | |
| 0... = Reserved: 0 | |
|0.. = Is Next Extension Header present?: No | |
|0. = Is Sequence Number present?: No | |
|0 = Is N-PDU number present?: No | |
| Message Type: T-PDU (0xff) | |
| Length: 84 | |
| TEID: 0x00000001 (1) | |
| ▶ Internet Protocol Version 4, Src: 172.16.0.2, Dst: 8.8.8.8 | |
| Internet Control Message Protocol | |

Step5-3 觀測使用者平面(SGi)

點擊前步驟所述之GTP-U封包的下一個封包，可以觀察到GTP-U Tunnel的部分已經被移除，且其流經的介面為srs_spgw_sgi。以此可以確定封包在P-GW順利離開GTP隧道並透過SGi介面離開EPC。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|------------|-------------|------------|--------|--|
| 25 | 32.828883368 | 172.16.0.2 | 8.8.8.8 | GTP <ICMP> | 134 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 27 | 32.828905660 | 172.16.0.2 | 8.8.8.8 | ICMP | 84 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 23 | 32.828928150 | 10.0.2.15 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 24 | 32.836061129 | 8.8.8.8 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| 28 | 32.836079463 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| 26 | 32.836148729 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |

▶ Frame 27: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface srs_spgw_sgi, id 0

Raw packet data

▶ Internet Protocol Version 4 Src: 172.16.0.2, Dst: 8.8.8.8

▼ Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x65c3 [correct]

[Checksum Status: Good]

Identifier (BE): 8 (0x0008)

Identifier (LE): 2048 (0x0800)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

[Response frame: 28]

Timestamp from icmp data: Jul 16, 2020 18:58:24.000000000 CST

[Timestamp from icmp data (relative): 138.325938180 seconds]

▼ Data (48 bytes)

Data: e6ce0c0000000000101112131415161718191a1b1c1d1e1f...

[Length: 48]

Step5-4 觀測資料平面(外連)

點擊前步驟所述之SGi封包的下一個封包，其來源IP位置已由srsLTE的172.16.0.2內部IP透過NAT轉換成對外的10.0.2.15並由ens3介面傳送出去，以此可以驗證從EPC與外部的連線沒有問題。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|------------|-------------|------------|--------|--|
| 25 | 32.828883368 | 172.16.0.2 | 8.8.8.8 | GTP <ICMP> | 134 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 27 | 32.828905660 | 172.16.0.2 | 8.8.8.8 | ICMP | 84 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 23 | 32.828928150 | 10.0.2.15 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x0008, seq=1/256, ttl=6... |
| 24 | 32.836061129 | 8.8.8.8 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| 28 | 32.836079463 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |
| 26 | 32.836148729 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0008, seq=1/256, ttl=2... |

| | |
|---|---|
| ▶ | Frame 23: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens3, id 1 |
| ▶ | Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02) |
| ▶ | Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8 |
| ▼ | Internet Control Message Protocol |
| | Type: 8 (Echo (ping) request) |
| | Code: 0 |
| | Checksum: 0x65c3 [correct] |
| | [Checksum Status: Good] |
| | Identifier (BE): 8 (0x0008) |
| | Identifier (LE): 2048 (0x0800) |
| | Sequence number (BE): 1 (0x0001) |
| | Sequence number (LE): 256 (0x0100) |
| | [Response frame: 24] |
| | Timestamp from icmp data: Jul 16, 2020 18:58:24.000000000 CST |
| | [Timestamp from icmp data (relative): 138.325960670 seconds] |
| ▼ | Data (48 bytes) |
| | Data: e6ce0c0000000000101112131415161718191a1b1c1d1e1f... |
| | [Length: 48] |

Step6-1 觀測UE離線流程(Request)

在執行UE的終端機中按下Ctrl-C結束UE後應可看到如下圖中的訊息，點選UplinkNASTransport, Detach request後確認MME-UE-S1AP-ID是否與Step5一致以驗證是否真的為該UE所發送的訊息，亦可至執行EPC的終端機上確認。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------|-------------|--------------|--------|---|
| 68 | 55.647115580 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0007, seq=1/256, ttl=2... |
| 70 | 55.647195283 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0007, seq=1/256, ttl=2... |
| 71 | 60.556730332 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 130 | UplinkNASTransport, Detach request (EPS detach /... |
| 72 | 60.557500894 | 127.0.1.100 | 127.0.1.1 | S1AP | 98 | UEContextReleaseCommand [NAS-cause=normal-releas... |
| 73 | 60.557649108 | 127.0.1.1 | 127.0.1.100 | S1AP | 98 | UEContextReleaseComplete |
| 74 | 60.758713471 | 127.0.1.100 | 127.0.1.1 | SCTP | 62 | SACK |
| 75 | 70.105195417 | 127.0.1.1 | 127.0.1.100 | SCTP | 54 | SHUTDOWN |

Frame 71: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface lo, id 1

- Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.1.1, Dst: 127.0.1.100
- Stream Control Transmission Protocol, Src Port: 58987 (58987), Dst Port: 58987 (58987)
- S1 Application Protocol
 - S1AP-PDU: initiatingMessage (0)
 - initiatingMessage
 - procedureCode: id-uplinkNASTransport (13)
 - criticality: ignore (1)
 - value
 - UplinkNASTransport
 - protocolIEs: 5 items
 - Item 0: id-MME-UE-S1AP-ID
 - ProtocolIE-Field
 - id: id-MME-UE-S1AP-ID (0)
 - criticality: reject (0)
 - value
 - MME-UE-S1AP-ID: 1

```
Create Session Response -- SPGW control TEID 1
Create Session Response -- SPGW S1-U Address: 127.0.1.100
SPGW Allocated IP 172.16.0.2 to IMSI 001010123456789
Adding attach accept to Initial Context Setup Request
Sent Initial Context Setup Request. E-RAB id 5
Received Initial Context Setup Response
E-RAB Context Setup. E-RAB id 5
E-RAB Context -- eNB TEID 0x460003; eNB GTP-U Address 127.0.1.1
UL NAS: Received Attach Complete
Unpacked Attached Complete Message. IMSI 1010123456789
Unpacked Activate Default EPS Bearer message. EPS Bearer id 5
Received GTP-C PDU. Message type: GTPC_MSG_TYPE_MODIFY_BEARER_REQUEST
Sending RMM Information
UL NAS: Detach Request
Detach request -- IMSI 001010123456789
Received GTP-C PDU. Message type: GTPC_MSG_TYPE_DELETE_SESSION_REQUEST
Received UE context release complete. MME-UE-S1AP-ID: 1
There are active E-RABs, send release access bearers request
UE Context Release Completed.
SCTP Association Shutdown. Association: 6
Deleting eNB context. eNB Id: 0x19ba
Releasing UEs context
No UEs to be released
```

Step6-2 觀測UE離線流程(Release)

點選**UEContextReleaseCommand**以觀測其詳細內容，此訊息代表MME要求eNB釋放有關該UE的所有資源，可以觀察到封包內容中有本次釋放命令的原因“normal-release”。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------|-------------|--------------|--------|---|
| 68 | 55.647115580 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0007, seq=1/256, ttl=2... |
| 70 | 55.647195283 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0007, seq=1/256, ttl=2... |
| 71 | 60.556730332 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 130 | UplinkNASTransport, Detach request (EPS detach /... |
| 72 | 60.557500894 | 127.0.1.100 | 127.0.1.1 | S1AP | 98 | UEContextReleaseCommand [NAS-cause=normal-releas... |
| 73 | 60.557649108 | 127.0.1.1 | 127.0.1.100 | S1AP | 98 | UEContextReleaseComplete |
| 74 | 60.758713471 | 127.0.1.100 | 127.0.1.1 | SCTP | 62 | SACK |
| 75 | 70.105195417 | 127.0.1.1 | 127.0.1.100 | SCTP | 54 | SHUTDOWN |

```

> Frame 72: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface lo, id 1
> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.1.100, Dst: 127.0.1.1
> Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 58987 (58987)
> S1 Application Protocol
  > S1AP-PDU: initiatingMessage (0)
    > initiatingMessage
      procedureCode: id-UEContextRelease (23)
      criticality: reject (0)
      > value
        > UEContextReleaseCommand
          > protocolIEs: 2 items
            > Item 0: id-UE-S1AP-IDs
              > ProtocolIE-Field
                id: id-UE-S1AP-IDs (99)
                criticality: reject (0)
                > value
                  > UE-S1AP-IDs: uE-S1AP-ID-pair (0)
                    > uE-S1AP-ID-pair
                      mME-UE-S1AP-ID: 1
                      eNB-UE-S1AP-ID: 1
            > Item 1: id-Cause
              > ProtocolIE-Field
                id: id-Cause (2)
                criticality: ignore (1)
                > value
                  Cause: nas (2)
                  nas: normal-release (0)

```

Step6-3 觀測UE離線流程(Complete)

點選**UEContextReleaseComplete**以觀測其詳細內容，此訊息代表eNB已按照MME要求釋放有關該UE的所有資源，核對**MME-UE-S1AP-ID**以確認正確釋放UE，同時EPC的終端機也應顯示出相應訊息。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------|-------------|--------------|--------|---|
| 68 | 55.647115580 | 8.8.8.8 | 172.16.0.2 | ICMP | 84 | Echo (ping) reply id=0x0007, seq=1/256, ttl=2... |
| 70 | 55.647195283 | 8.8.8.8 | 172.16.0.2 | GTP <ICMP> | 134 | Echo (ping) reply id=0x0007, seq=1/256, ttl=2... |
| 71 | 60.556730332 | 127.0.1.1 | 127.0.1.100 | S1AP/NAS-EPS | 130 | UplinkNASTransport, Detach request (EPS detach /... |
| 72 | 60.557500894 | 127.0.1.100 | 127.0.1.1 | S1AP | 98 | UEContextReleaseCommand [NAS-cause=normal-releas... |
| 73 | 60.557649108 | 127.0.1.1 | 127.0.1.100 | S1AP | 98 | UEContextReleaseComplete |
| 74 | 60.758713471 | 127.0.1.100 | 127.0.1.1 | SCTP | 62 | SACK |
| 75 | 70.105195417 | 127.0.1.1 | 127.0.1.100 | SCTP | 54 | SHUTDOWN |

Frame 73: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface lo, id 1

Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 127.0.1.1, Dst: 127.0.1.100

Stream Control Transmission Protocol, Src Port: 58987 (58987), Dst Port: 58987 (58987)

S1 Application Protocol

- S1AP-PDU: successfulOutcome (1)
 - successfulOutcome
 - procedureCode: id-UEContextRelease (23)
 - criticality: reject (0)
 - value
 - UEContextReleaseComplete
 - protocolIEs: 2 items
 - Item 0: id-MME-UE-S1AP-ID
 - ProtocolIE-Field
 - id: id-MME-UE-S1AP-ID (0)
 - criticality: ignore (1)
 - value
 - Item 1: id-eNB-UE-S1AP-ID
 - ProtocolIE-Field
 - id: id-eNB-UE-S1AP-ID (8)
 - criticality: ignore (1)
 - value
 - ENB-UE-S1AP-ID: 1

Create Session Response -- SPGW control TEID 1

Create Session Response -- SPGW S1-U Address: 127.0.1.100

SPGW Allocated IP 172.16.0.2 to IMSI 001010123456789

Adding attach accept to Initial Context Setup Request

Sent Initial Context Setup Request. E-RAB id 5

Received Initial Context Setup Response

E-RAB Context Setup. E-RAB id 5

E-RAB Context -- eNB TEID 0x460003; eNB GTP-U Address 127.0.1.1

UL NAS: Received Attach Complete

Unpacked Attached Complete Message. IMSI 1010123456789

Unpacked Activate Default EPS Bearer message. EPS Bearer id 5

Received GTP-C PDU. Message type: GTPC_MSG_TYPE_MODIFY_BEARER_REQUEST

Sending EMM Information

UL NAS: Detach Request

Detach request -- IMSI 001010123456789

Received S1-MME PDU: Message type: S1-MME_MSG_TYPE_DELETE_SESSION_REQUEST

Received UE Context Release Complete. MME-UE S1AP Id 1

There are active E-RABs, send release access bearers request

UE Context Release Completed.

Deleting eNB context. eNB Id: 0x19ba

Releasing UEs context

No UEs to be released

Step7-1 觀測eNB關閉流程(請求)

在執行eNB的終端機按下Ctrl-C以結束eNB，同時Wireshark中應會出現eNB關閉時所傳送的訊息，點選**SHUTDOWN**以觀測其詳細內容，此訊息為eNB透過SCTP告知MME即將關閉連線，同時EPC的終端機畫面上也會顯示出相關訊息。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------|-------------|----------|--------|--------------------------|
| 73 | 60.557649108 | 127.0.1.1 | 127.0.1.100 | S1AP | 98 | UEContextReleaseComplete |
| 74 | 60.758713471 | 127.0.1.100 | 127.0.1.1 | SCTP | 62 | SACK |
| 75 | 70.105195417 | 127.0.1.1 | 127.0.1.100 | SCTP | 54 | SHUTDOWN |
| 76 | 70.105211538 | 127.0.1.100 | 127.0.1.1 | SCTP | 50 | SHUTDOWN_ACK |
| 77 | 70.105217106 | 127.0.1.1 | 127.0.1.100 | SCTP | 50 | SHUTDOWN_COMPLETE |

▶ Frame 75: 54 bytes on wire (432 bits), 54 bytes captured on interface 0 (eth0) from 127.0.1.1 to 127.0.1.100

▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

▶ Internet Protocol Version 4, Src: 127.0.1.1, Dst: 127.0.1.100

▼ Stream Control Transmission Protocol, Src Port: 58987, Dst Port: 36412

Source port: 58987

Destination port: 36412

Verification tag: 0x7694b862

[Association index: 65535]

Checksum: 0x00000000 [unverified]

[Checksum Status: Unverified]

▼ SHUTDOWN chunk (Cumulative TSN ack: 996260459)

▶ Chunk type: SHUTDOWN (7)

Chunk flags: 0x00

Chunk length: 8

Cumulative TSN Ack: 996260459

Create Session Response -- SPGW control TEID 1

Create Session Response -- SPGW S1-U Address: 127.0.1.100

SPGW Allocated IP 172.16.0.2 to IMSI 001010123456789

Adding attach accept to Initial Context Setup Request

Sent Initial Context Setup Request. E-RAB id 5

Received Initial Context Setup Response

E-RAB Context Setup. E-RAB id 5

E-RAB Context -- eNB TEID 0x460003; eNB GTP-U Address 127.0.1.1

UL NAS: Received Attach Complete

Unpacked Attach Complete Message. IMSI 1010123456789

Unpacked Activate Default EPS Bearer message. EPS Bearer id 5

Received GTP-C PDU. Message type: GTPC_MSG_TYPE_MODIFY_BEARER_REQUEST

Sending EMM Information

UL NAS: Detach Request

Detach request -- IMSI 001010123456789

Received GTP-C PDU. Message type: GTPC_MSG_TYPE_DELETE_SESSION_REQUEST

Received UE Context Release Complete. MME-UE S1AP Id 1

There are active E-RABs, send release access bearers request

UE Context Release Completed

SCTP Association Shutdown. Association: 6

Deleting eNB context. eNB Id: 0x19ba

Releasing UEs context

No UEs to be released

Step7-2 觀測eNB關閉流程(完成)

點選**SHUTDOWN_COMPLETE**以觀測其詳細內容，此訊息為eNB透過SCTP告知MME已完成連線關閉的工作。若收到此訊息即表示eNB已正確被關閉。

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------|-------------|----------|--------|--------------------------|
| 73 | 60.557649108 | 127.0.1.1 | 127.0.1.100 | SIAP | 98 | UEContextReleaseComplete |
| 74 | 60.758713471 | 127.0.1.100 | 127.0.1.1 | SCTP | 62 | SACK |
| 75 | 70.105195417 | 127.0.1.1 | 127.0.1.100 | SCTP | 54 | SHUTDOWN |
| 76 | 70.105211538 | 127.0.1.100 | 127.0.1.1 | SCTP | 50 | SHUTDOWN_ACK |
| 77 | 70.105217106 | 127.0.1.1 | 127.0.1.100 | SCTP | 50 | SHUTDOWN_COMPLETE |

▶ Frame 77: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface lo, id 1

▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

▶ Internet Protocol Version 4, Src: 127.0.1.1, Dst: 127.0.1.100

▼ Stream Control Transmission Protocol, Src Port: 58987 (58987), Dst Port: 36412 (36412)

Source port: 58987

Destination port: 36412

Verification tag: 0x7694b862

[Association index: 65535]

Checksum: 0x00000000 [unverified]

[Checksum Status: Unverified]

▼ SHUTDOWN_COMPLETE chunk

▼ Chunk type: SHUTDOWN_COMPLETE (14)

0... = Bit: Stop processing of the packet

.0... = Bit: Do not report

▼ Chunk flags: 0x00

.... ...0 = T-Bit: Tag not reflected

Chunk length: 4

Stage 4 Check List

| 項目 | 內容 |
|------------------------|---|
| 已安裝 Wireshark | wireshark --version |
| 觀測 S1-MME 在 eNB 啟動時的行為 | 應要看到 S1SetupRequest 即 S1SetupResponse 兩個訊息 |
| 觀測 S1-MME 在 UE 連接時的行為 | 應要觀察到有連接請求、身分確認、認證、安全模式協商、連接完成五大步驟 |
| 觀測使用者平面 | S1-U 中出現以 GTP-U 封裝過的 UE 封包並在 SGi 出現 UE 所傳送的原始封包 |
| 觀測 S1-MME 在 UE 離線時的行為 | 應要觀察到 Detach request、UEContextRelease 等相關訊息 |
| 觀測 S1-MME 在 eNB 關閉時的行為 | 應要觀察到 SHUTDOWN 等相關訊息 |

Outline

- 實驗目的及實驗內容
- 背景知識
- 實驗環境
- Stage 1: 環境架設
- Stage 2: srsLTE 及 ZeroMQ 編譯安裝
- Stage 3: srsLTE 執行及測試
- Stage 4: srsLTE 封包觀測
- 總結及問題

總結

- 進行 Linux NAT 架設及路由設定以符合實驗環境
- 進行 srsLTE 及 ZeroMQ 編譯安裝
- srsLTE 執行及測試
 - 了解如何設定及啟動 srsLTE
 - 進行 Downlink 及 Uplink 的 ICMP 與 TCP 測試
- srsLTE 封包觀測
 - 觀測eNB啟動流程的SCTP 及 S1AP 封包
 - 觀測UE連接流程的 S1AP 及 NAS 封包
 - 觀測使用者平面的封包流向及 GTP-U 的封裝情形
 - 觀測UE離線流程的 NAS 及 S1AP 封包
 - 觀測eNB關閉流程的 SCTP 封包

問題

在UE上使用瀏覽器開啟www.google.com然後觀察

1. S1-U 的封包內容
2. SGi 的封包內容
3. 繪製 HTTP 請求經過 UE、eNB、SPGW、Internet 時封包內容為何(多了什麼/被封裝在什麼協定內)並配上 Wireshark 截圖。