IWR 工業 LTE GPS 路由器

使用手冊

版本: 3.0

日期: Oct 1，2018

修訂記錄

版本	日期	改變
1.0	08/22/2018	首次發布 IWR 使用手冊
2.0	09/12/2018	依韌體 Ver1359 Wed Sep 12 09:12:57 UTC 2018 編修 IWR 使用手冊
3.0	10/01/2018	JMHUANG - 加入各功能及細部功能介紹

目錄

修訂記錄 **2**

1. 產品概述 **5**

1.1 介紹 5
1.2 硬體規格 6
1.3 軟體規格 7
1.4 無線規格 7
1.5 I/O 規格 8
1.6 外觀尺寸(CASING DIMENSION) 8
1.7 重啟為出廠預設值 9
1.8 LED 顯示定義 9
1.9 包裝內容 10

2. 快速安裝及使用 **12**

3. 狀態功能設定 **14**

3-1 STATUS 狀態資訊 16
3-2 FIREWALL 防火牆 19
3-3 ROUTES 路由 21
3-4 SYSTEM LOG 系統日誌 22
3-5 KERNEL LOG 核心日誌 22
3-6 REALTIME GRAPHS 即時圖表 23

4. 系統功能設定 **24**

4-1 SYSTEM 系統 24
4-2 ADMINISTRATOR 管理員 26
4-3 BACKUP / FLASH FIRMWARE 備份還原設定值/更新韌體 27
4-4 REBOOT 重啟 29

5. 服務功能設定 **29**

5-1 GPS GW 全球定位功能 29
5-2 BEACON GW 設定(選配) 31
5-3 UHTTPD 服務器 32
5-4 SERIAL GW 序列閘道 33

6.網路功能設定 **34**

6-1 INTERFACE OVERVIEW 介面狀態 34

6-2 WIRELESS 無線設置 37
6-3 SWITCH 開關設置 42
6-4 DHCP & DNS 43
6-5 HOSTNAMES 主機名稱 46
6-6 STATIC ROUTES 靜態路由 47
6-7 FIREWALL 防火牆 48
6-8 DIAGNOSTICS 診斷 52
6-9 QOS 服務質量 53
6-A LOAD BALANCING 負載平衡 54

7. 快速無線 4G 上網/APN 設定 60

1. 產品概述

1.1 介紹

IWR 是一個帶有 LTE、WiFi 與 GPS 的工業物聯網路由器,它可從各種物聯網設備感應器收集數據資料,如行動軌跡、溫度、濕度、氣壓、電力、G sensor、陀螺儀、燈光、Modbus PLC 等等.IWR 工業物聯網路由器可轉換不同介面與設備的協議到物聯網伺服器,如 Http 伺服器,MOTT 伺服器.

IWR 系列工業無線路由器是一種物聯網無線通信路由器,利用公用營運商網路為用戶提供
無線長距離數據傳輸. IWR 採用高性能的工業級 32 位通信處理器和工業級無線模塊，以嵌入式操作系統為軟體支撐平台,同時提供 2 個乙太網 LAN(其中一個可配置為 WAN),同時連接串口設備,乙太網設備,實現數據透明傳傳輸和路由功能.

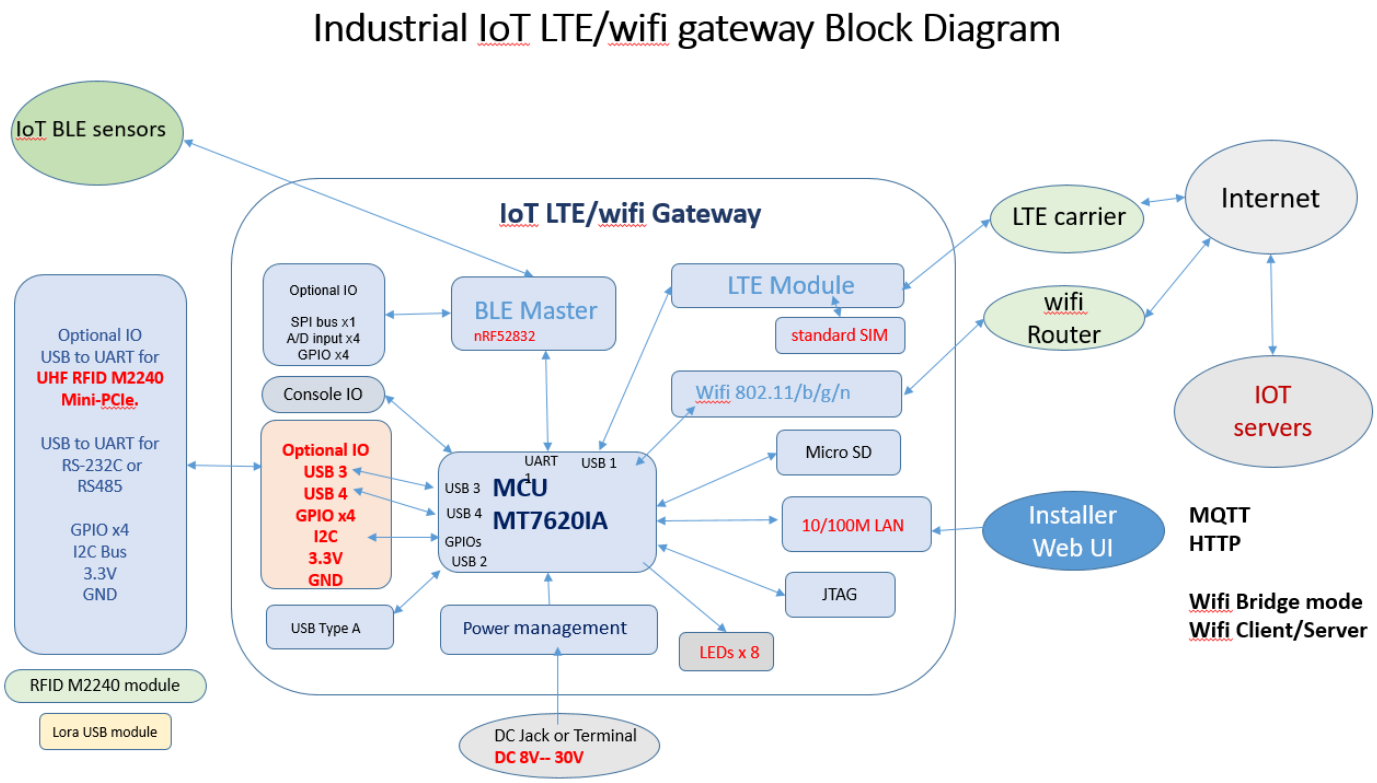
IWR 已廣泛應用於物聯網產業鏈中的 M2M 行業,如智能電網,智能交通,智能家居,移動 POS 終端,供應鏈自動化,工業自動化,智能建築,消防,公共安全,環境保護,氣象,數字化醫療,遙感勘測，軍事,空間探索,農業,林業,水資源,煤礦,石化等領域.

1.2 硬體規格

- 中央處理器: MT7620IA
- 同步動態隨機存取記憶體: 64MB ~256MB
- 快閃記憶體: 8MB ~ 16MB
- MT7620IA工作溫度範圍: -40° C ~ +85° C
- 功率範圍: DC8V~DC30V /1A
- 濕度範圍: 10% ~ 90% non-condensing

天線:

- 可拆卸SMA WiFi天線 x 2
- 可拆卸SMA LTE天線 x 2
- 可拆卸SMA GPS天線 x 1
- 導軌套件
- 壁掛套件



1.3 軟體規格

- Internet access over Ethernet WAN (support DHCP，Static IP，PPPoE) or Internal LTE
  Failover from Ethernet WAN to LTE
- 防火牆
  IP and MAC Filter
  Virtual Server and DMZ
  NAT (Network Address Translation)
- VPN
  PPTP，L2TP pass through
- 通訊協議 (Communication Protocols)
  IP，NAT，DHCP，PAP，CHAP，PPP，TCP，UDP，HTTP，NTP

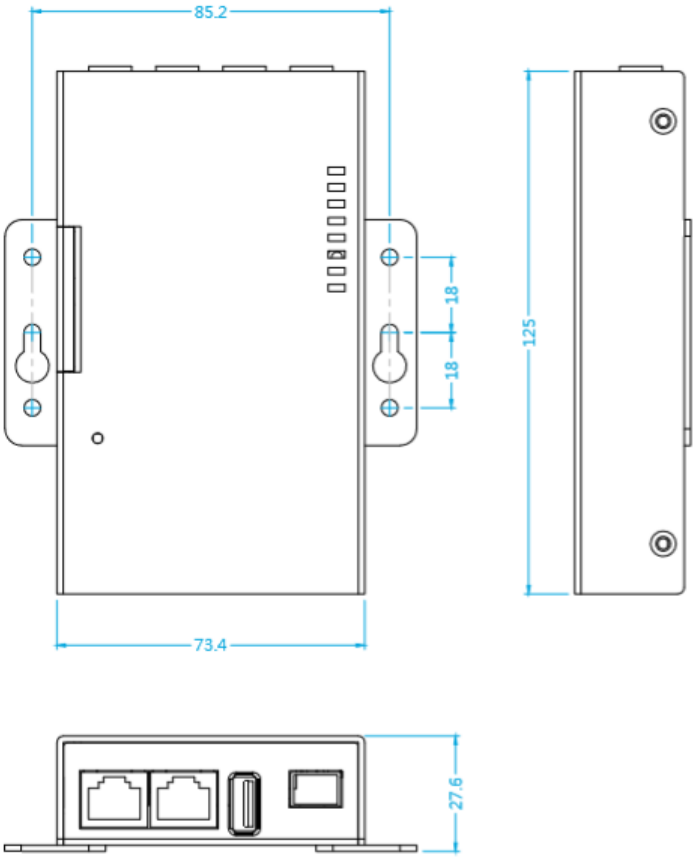
1.4 無線規格

- WiFi Specification (2T2R 802.11n)
  Output Power (WiFi)
  802.11n:11 dBm
  802.11g:13 dBm
  802.11b:15 dBm
- Sensitivity (WiFi):
  802.11n : -68 dBm
  802.11g : -68 dBm
  802.11b : -85 dBm
- WiFi Frequencies
  2,4 - 2,462 GHz，CCK / OFDM (Modulation Range Coverage)
- WiFi Distances
  Indoor: approximately 30 to 50 meters
  Outdoor: 80 to 100 meters

1.5 I/O 規格

- 10/100M LAN x1
- 10/100M WAN or LAN
- USB Type A x 1
- LED x 8
- Reset button x 1
- Micro SD Card x 1
- Standard SIM Card x 1
- WiFi SMA Antenna x 2
- LTE SMA Antenna x 2
- GPS SMA Antenna x 1
- DC Jack x1 (DC 8V ~ 30V input)
- DC 5mm terminal Jack x1.

1.6 外觀尺寸(Casing dimension)

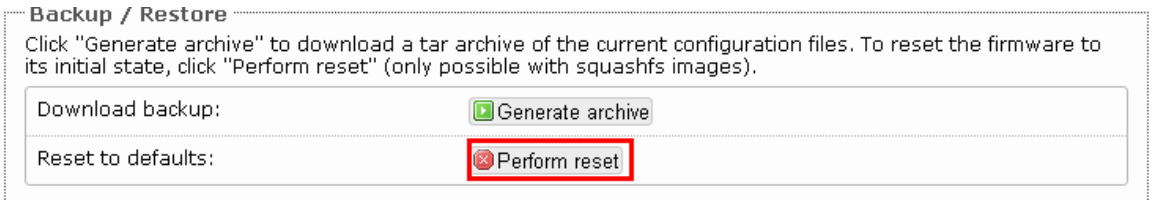


1.7 重啟為出廠預設值

重啟為出廠預設值方式(特殊需求時，如…忘記當初修改的設定值或更新最新韌體)

方式 1:設備啟動後，請等待約 45 秒，按壓 Reset 按鈕，直到 LED 3(LTE),4(CSQ),7(RUN)閃爍

方式 2:登錄網頁後，請按下重置按鈕> 5--10 秒，LED 3(LTE),4(CSQ),7(RUN)閃爍



步驟 3: 等待系統重啟（設備將恢復為出廠預設值）

注意：重啟為出廠預設值過程中，請勿關閉電源。

1.8 LED 顯示定義

LED1: LAN 2 狀態顯示

LED2: WAN / LAN 1 狀態顯示

LED3. LTE 工作狀態顯

LED4. LTE CSQ 顯示，閃爍速度（高，中，低）

LED5. WiFi 802.11 b / g / n 工作狀態顯示

LED6. BLE 工作狀態顯示

LED7. SYS(重啟按鈕顯示和 SD 工作狀態顯示）

LED8 : 開機顯示

正常工作狀態

LED 1閃爍（連接到PC LAN端口之後）

LED 2熄滅（預設為WAN端口設定）

LED 3閃爍（設備連接到4G運營商和數據上傳或下載）

LED 4快速閃爍意味著CSQ> 20（低速閃爍意味著CSQ <10 ..）

LED 5閃爍（WiFi RF開啟，數據上傳或下載）

LED 6關閉（保留給BLE應用）

LED 7關閉（重啟按鈕狀態顯示）

LED 8亮起

1.9 包裝內容

標準配件

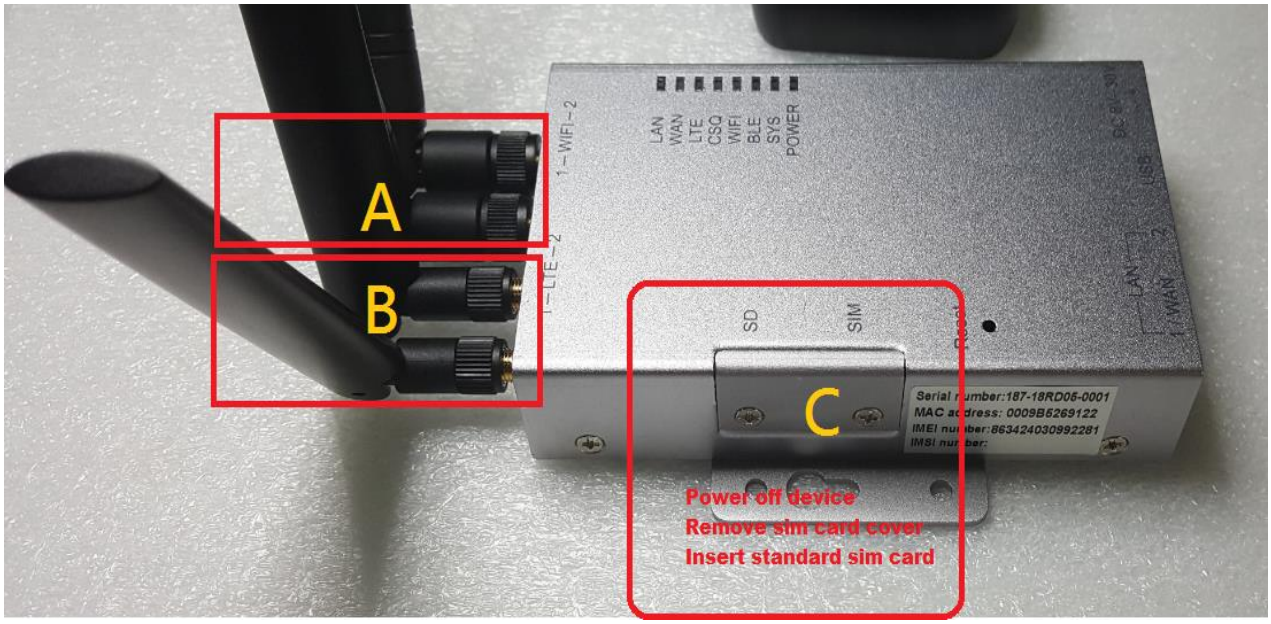
- IWR x 1
- 電源(DC_12V /1A) x 1
- LTE Antenna x 2
- WiFi Antenna x 2
- GPS Antenna x 1
- IP CAM1 x 1(選配)

1 – LTE – 2
1 – WIFI – 2
LAN
WAN
LTE
CSQ
WIFI
BLE
SYS
POWER
SD
SIM
Reset
LAN
1 / WAN
2
USB
DC 8V--30V
--- +

可選擇其他相關配件

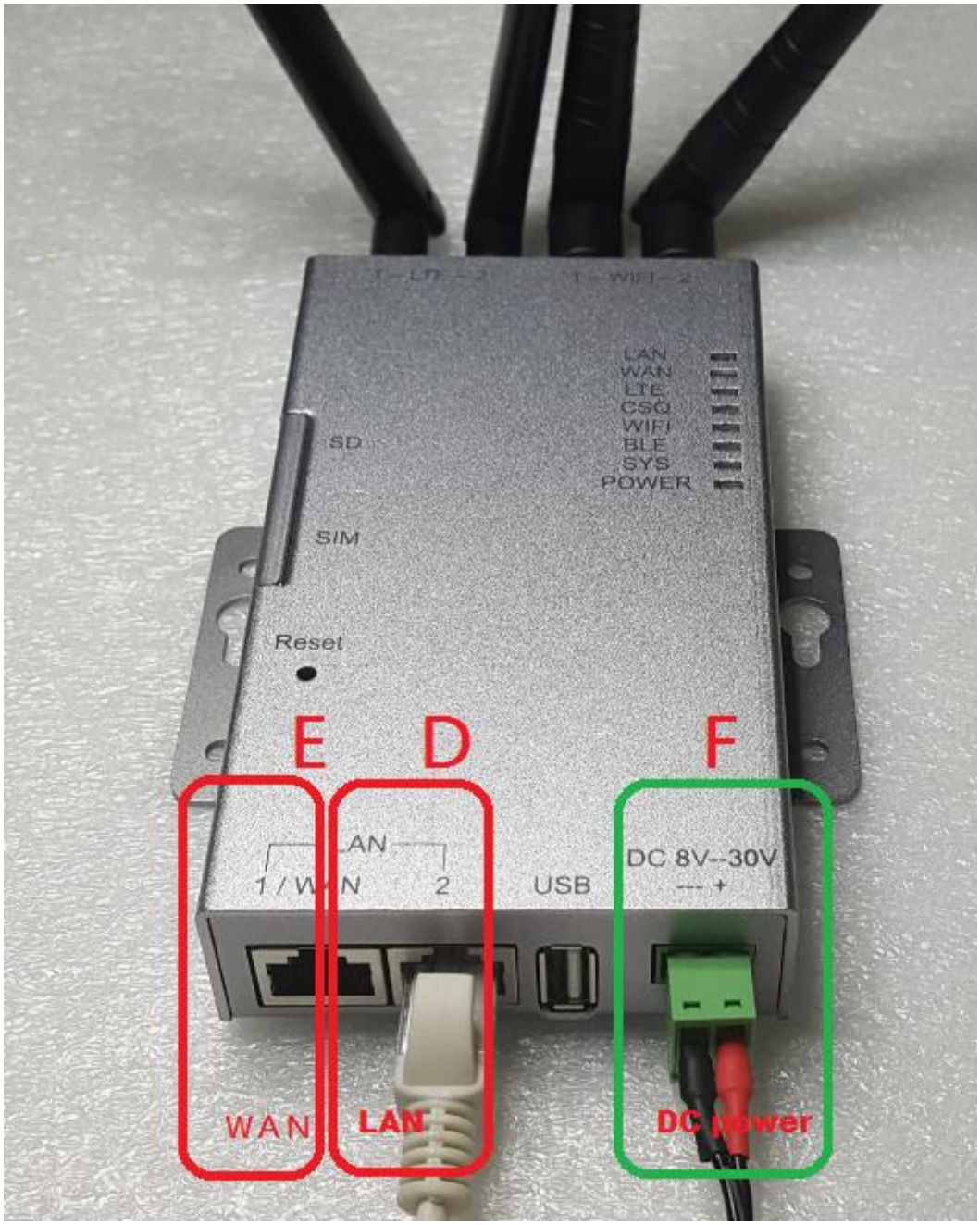
2. 快速安裝及使用

1. 首先接上 wifi 天線*2（下圖 A ）及 4G 天線*2（下圖 B ）
2. 接著將 SIM/SD 卡座外蓋（下圖 C ）二個螺絲卸下後取下外蓋，並置入 4G SIM CARD
3. 再蓋回卡座外蓋（下圖 C ）後再鎖回二個螺絲



4. 於 LAN2 接口接上與電腦連接之網路線（下圖 D ），若有需要接 WAN(有線外網下圖 E ）)時，請於電源啟動 30 秒後再行插入 WAN 網路線

5. 最後再接上電源接頭（下圖 F)，以啟動開機程序

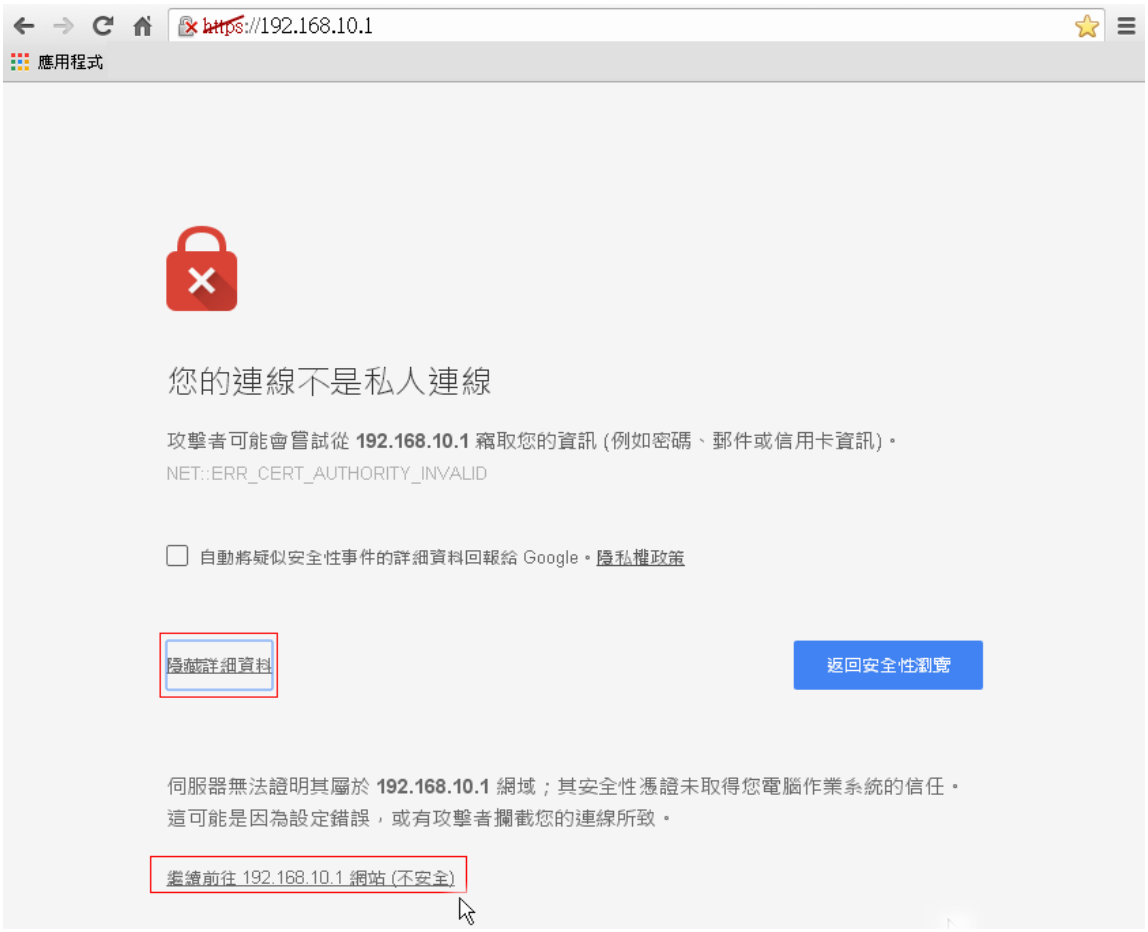


6. 開啟電腦瀏覽器軟體，於網址列鍵入 Router 功能設定首頁的 IP 地址為 https://192.168.10.1

3. 狀態功能設定

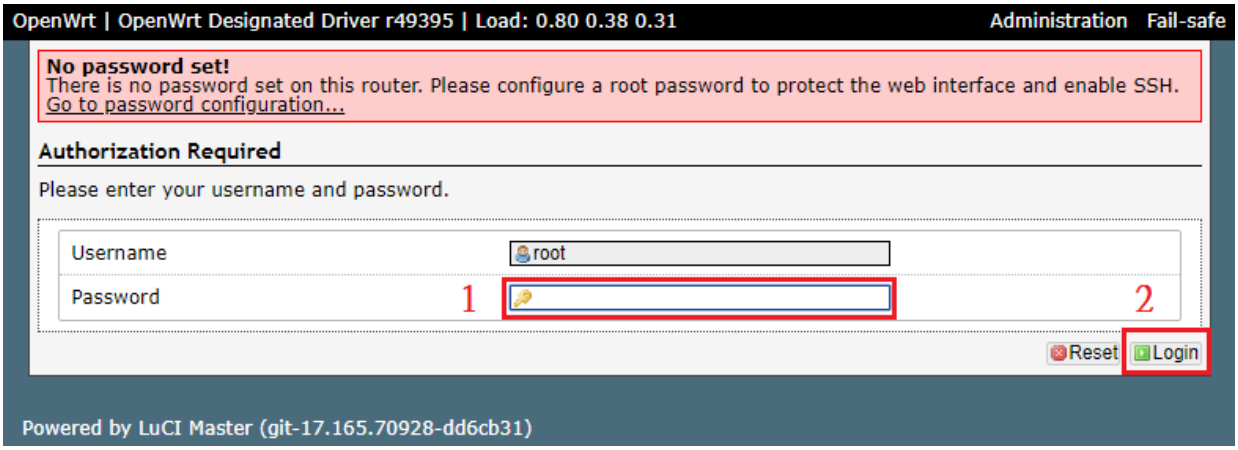
• 登入：Router 功能設定首頁的 IP 地址為 https://192.168.10.1

注意：如果出現警告頁面，請先點選進入"進階"→繼續前往 192.168.10.1 網站（不安全），這只會出現在您有做還原預設值的動作(按壓 Reset 按鍵)第一次進入設定頁面時或您的韌體為舊版時會出現。斷電重啟後，接下來您都可以用 https://192.168.10.1 或 http://192.168.10.1 網址進入 IWR 路由器的設定頁面，不會再出現繼續前往 192.168.10.1 網站（不安全)的警告畫面，以下是以 https://192.168.10.1 為範例。

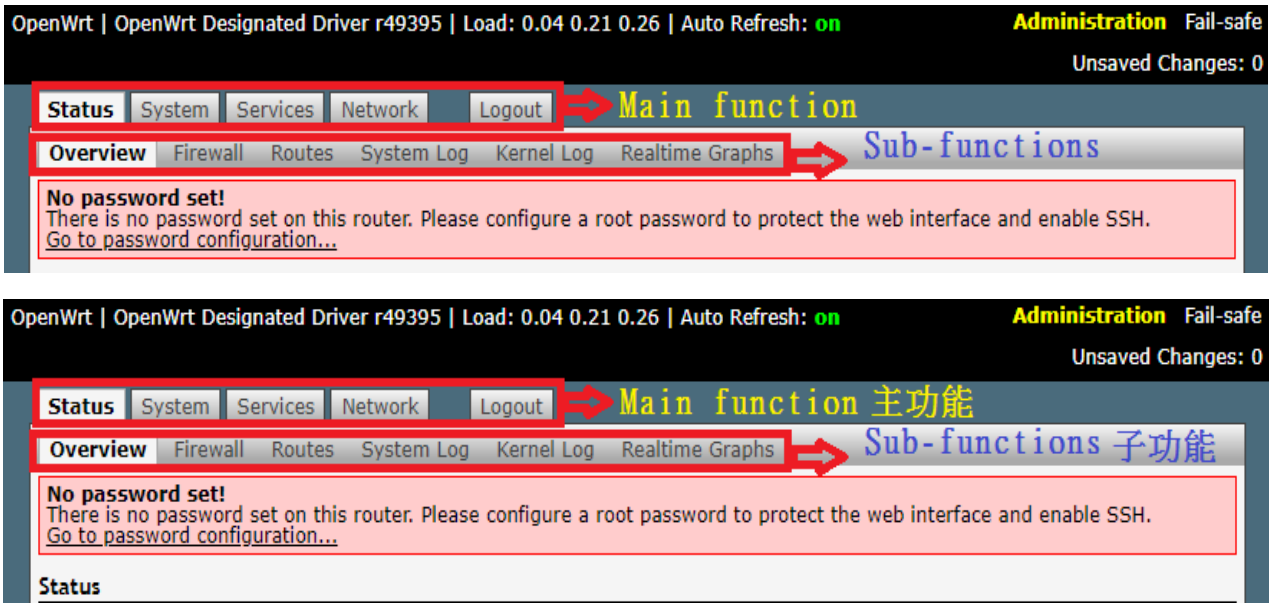


步驟 1: 選擇 Administration。

步驟 2:輸入使用者名稱（預設為 root）及密碼（預設無需 password)後再按 login。



• 主功能：包含狀態資訊設定、系統功能設定、服務功能設定及網路相關功能設定（如下圖）。



步驟 3: 檢查數據機信號品質 CSQ 值、SIM CARD 狀態、網路註冊資訊與其他網路狀態訊息。.

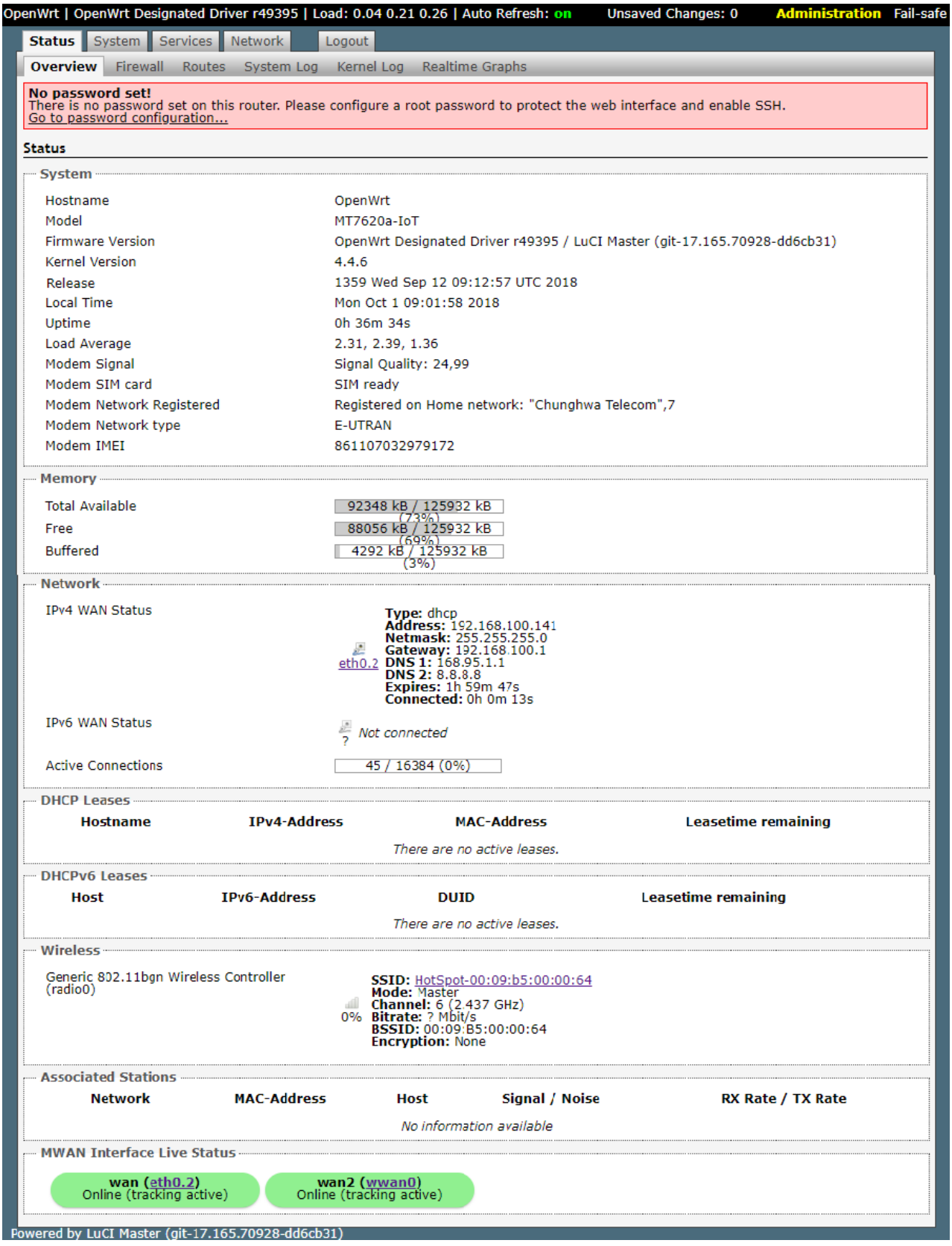
https://192.168.10.1/cgi-bin/luci/admin/status

當 CSQ<10 時表示信號品質不佳(檢視 4G 天線是否銜接妥當）CSQ>20 時表示信號品質很好.

3-1 Status 狀態資訊

Overview ➔IWR Router 狀態資訊

包含：System / Memory / Network / DHCP Leases / DHCPv6 Leases / Wireless / Associated Stations / MWAN Interface Live Status 等資訊。



• System 系統資訊

Hostname ： 顯示 IWR Router 主機名稱

Model: 顯示 IWR Router 型號

Firmware Version：韌體版本資訊

Kernel Version：核心版本資訊

Release：系統釋出的韌體版本資訊

Local Time：本地時間顯示（星期 月日 時 分 秒 年）

Uptime：IWR Router 開機後已工作時間

Load Average：負載平均值

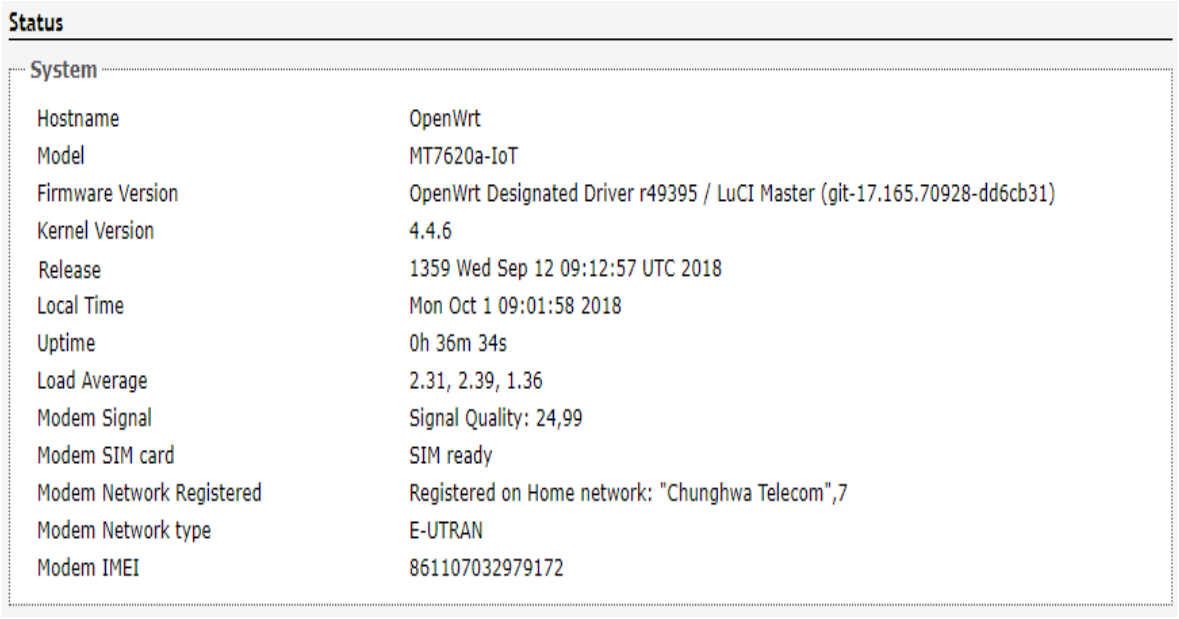
Modem Signal：模組 CSQ 訊號值

Modem SIM card：SIM card 狀能

Modem Network Registered：SIM card 業者基地台註冊狀能

Modem Network type：顯示 4G LTE 網路連接模式

Modem IMEI：顯示 4G 模組的 IMEI 號碼

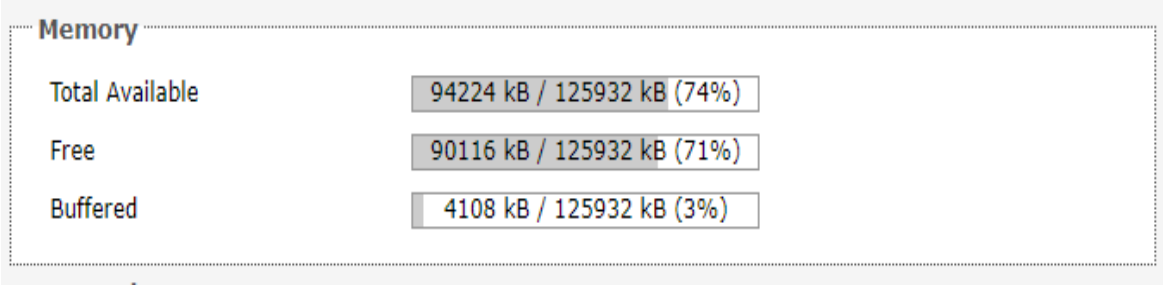


• Memory 記憶體使用資訊

Total Available

Free

Buffered

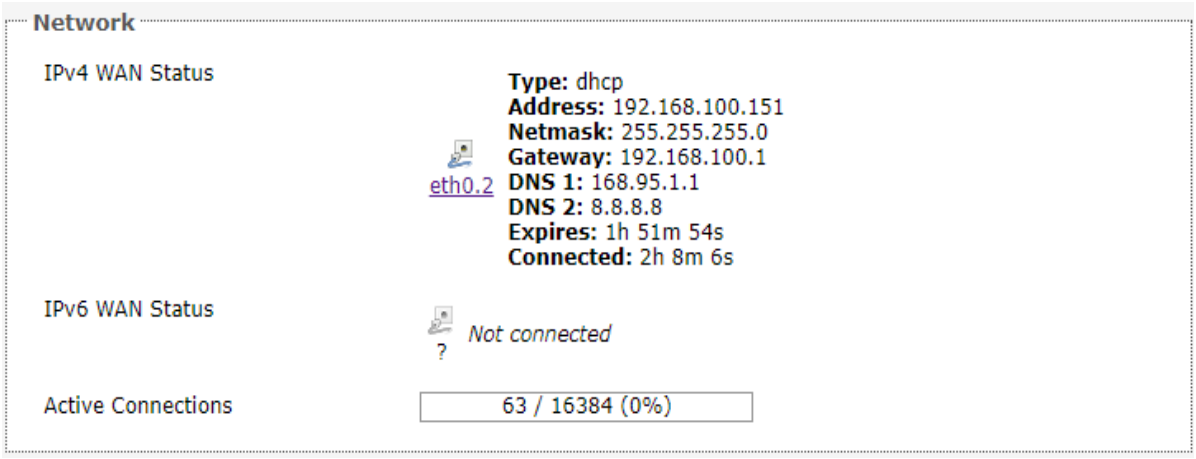


・Network 網路資訊

IPv4 WAN Status 顯示目前 IPv4 外網連線資訊，包含 IP 及 IP 取得方式等

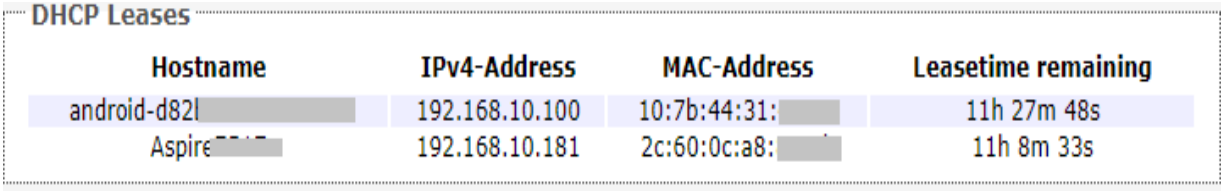
IPv6 WAN Status 顯示目前 IPv6 外網連線資訊，目前尚未開放

Active Connections　顯示目前活動連接數資訊。



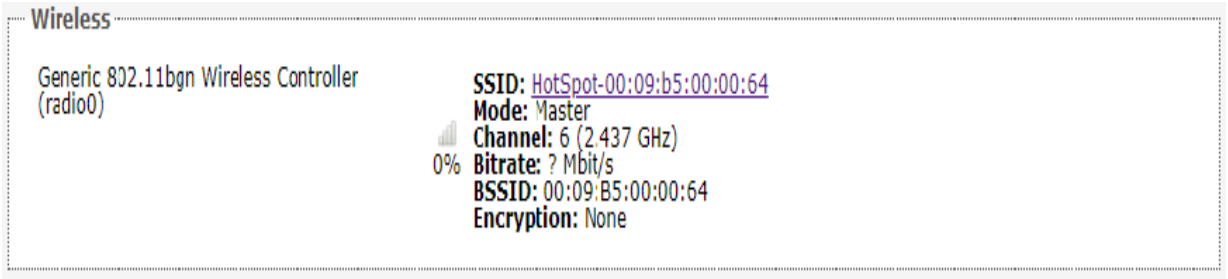
・DHCP Leases 租約資訊

顯示目前 DHCPv4 使用的資訊(DHCPv6 未開放)，包含主機名稱、IP 位置、MAC Address、已使用租約時間等。



・Wireless 無線網路資訊

顯示目前無線網路的資訊，包含 SSID、連接模式、頻道、Bitrate、MAC、加密方式等。



・MWAN Interface Live Status 外網接口即時狀態

顯示目前 WAN 網路即時狀態的資訊。

3-2 Firewall 防火牆

Firewall Status ➔IWR Router 防火牆狀態資訊
為路由器的最小防火牆配置通常由一個的默認部分，至少兩個區（lan 和 wan）和一個轉發，以允許從 lan 到 wan。（當不超過兩個區域時，不嚴格要求轉發部分，因為該規則可以設置為該區域的“全局默認”。）

defaults 默認
該 defaults 部分聲明了不屬於特定區域的全局防火牆設置

zone 區
zone 節組的一個或多個接口，並且用作源或目的地為 forwardings，規則和重定向。

Forwardings 轉發
這些 forwarding 部分控制區域之間的交通流量，並且可以針對特定方向啟用 MSS 箝位。
forwarding 規則只涵蓋一個方向。

區域的 INPUT 規則描述了試圖通過該區域中的接口到達路由器本身的流量會發生什麼。
區域的 OUTPUT 規則描述了源自路由器本身通過該區域中的接口的流量會發生什麼。
區域的 FORWARD 規則描述了在該區域中不同接口之間傳遞的流量會發生什麼。

Redirects 重定向
端口轉發（DNAT）由 redirect 部分定義。指定源區域上與給定規則匹配的所有傳入流量將定向到指定的內部主機。
重定向通常也稱為“端口轉發”和“虛擬服務器”。

Rules 規則
該類型的部分 rule 可用於定義基本的接受或拒絕規則，以允許或限制對特定端口或主機的訪問。

Chain *INPUT* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
10975	937.56 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for input */
8353	755.15 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate RELATED,ESTABLISHED
23	920.00 B	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate INVALID
20	1.02 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 tcp flags:0x17/0x02
2599	181.52 KB	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_wan_input	all	wwan0	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_wan_input	all	eth0.2	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *FORWARD* (Policy: *DROP*, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
199024	45.73 MB	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for forwarding */
195439	45.43 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate RELATED,ESTABLISHED
75	3.20 KB	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate INVALID
3510	309.37 KB	zone_lan_forward	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_wan_forward	all	wwan0	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_wan_forward	all	eth0.2	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	reject	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *OUTPUT* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	ACCEPT	all	*	lo	0.0.0.0/0	0.0.0.0/0	ID:66773300
10271	1.19 MB	output_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for output */
3971	723.54 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate RELATED,ESTABLISHED
0	0.00 B	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate INVALID
0	0.00 B	zone_lan_output	all	*	br-lan	0.0.0.0/0	0.0.0.0/0	ID:66773300
6300	496.34 KB	zone_wan_output	all	*	wwan0	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_wan_output	all	*	eth0.2	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *reject* (References: 5)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 reject-with tcp-reset
0	0.00 B	REJECT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 reject-with icmp-port-unreachable

Chain *syn_flood* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
20	1.02 KB	RETURN	tcp	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 tcp flags:0x17/0x02 limit: avg 25/sec burst 50
0	0.00 B	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_lan_dest_ACCEPT* (References: 5)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	ACCEPT	all	*	br-lan	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_lan_forward* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
3510	309.37 KB	forwarding_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for forwarding */
3510	309.37 KB	zone_vpn_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* forwarding lan -> vpn */
3510	309.37 KB	zone_wan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* forwarding lan -> wan */
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate DNAT /* Accept port forwards */
0	0.00 B	zone_lan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_lan_input* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
2599	181.52 KB	input_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for input */
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate DNAT /* Accept port redirections */
2599	181.52 KB	zone_lan_src_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_lan_output* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	output_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for output */
0	0.00 B	zone_lan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_lan_src_ACCEPT* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
2599	181.52 KB	ACCEPT	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_vpn_forward* (References: 0)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	forwarding_vpn_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for forwarding */
0	0.00 B	zone_lan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* forwarding vpn -> lan */
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate DNAT /* Accept port forwards */
0	0.00 B	zone_vpn_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_vpn_input* (References: 0)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	input_vpn_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for input */
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate DNAT /* Accept port redirections */
0	0.00 B	zone_vpn_src_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_vpn_output* (References: 0)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	output_vpn_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for output */
0	0.00 B	zone_vpn_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_wan_dest_ACCEPT* (References: 2)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
9810	805.71 KB	ACCEPT	all	*	wwan0	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	ACCEPT	all	*	eth0.2	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_wan_dest_REJECT* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	reject	all	*	wwan0	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	reject	all	*	eth0.2	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_wan_forward* (References: 2)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	MINIUPNPD	all	*	*	0.0.0.0/0	0.0.0.0/0	-
0	0.00 B	forwarding_wan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for forwarding */
0	0.00 B	zone_lan_dest_ACCEPT	esp	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* @rule[7] */
0	0.00 B	zone_lan_dest_ACCEPT	udp	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 udp dpt:500 /* @rule[8] */
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate DNAT /* Accept port forwards */
0	0.00 B	zone_wan_dest_REJECT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Table: NAT

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 669, Traffic: 43.88 KB)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
4408	312.89 KB	prerouting_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for prerouting */
4408	312.89 KB	zone_lan_prerouting	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_wan_prerouting	all	wwan0	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_wan_prerouting	all	eth0.2	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *POSTROUTING* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
7932	634.35 KB	postrouting_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for postrouting */
0	0.00 B	zone_lan_postrouting	all	*	br-lan	0.0.0.0/0	0.0.0.0/0	ID:66773300
7932	634.35 KB	zone_wan_postrouting	all	*	wwan0	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_wan_postrouting	all	*	eth0.2	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_lan_postrouting* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	postrouting_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for postrouting */

Chain *zone_lan_prerouting* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
4408	312.89 KB	prerouting_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for prerouting */

Chain *zone_vpn_postrouting* (References: 0)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	postrouting_vpn_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for postrouting */
0	0.00 B	MASQUERADE	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Chain *zone_vpn_prerouting* (References: 0)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	prerouting_vpn_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for prerouting */

Chain *zone_wan_postrouting* (References: 2)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
7932	634.35 KB	MINIUPNPD-POSTROUTING	all	*	*	0.0.0.0/0	0.0.0.0/0	-
7932	634.35 KB	postrouting_wan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for postrouting */
7932	634.35 KB	MASQUERADE	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

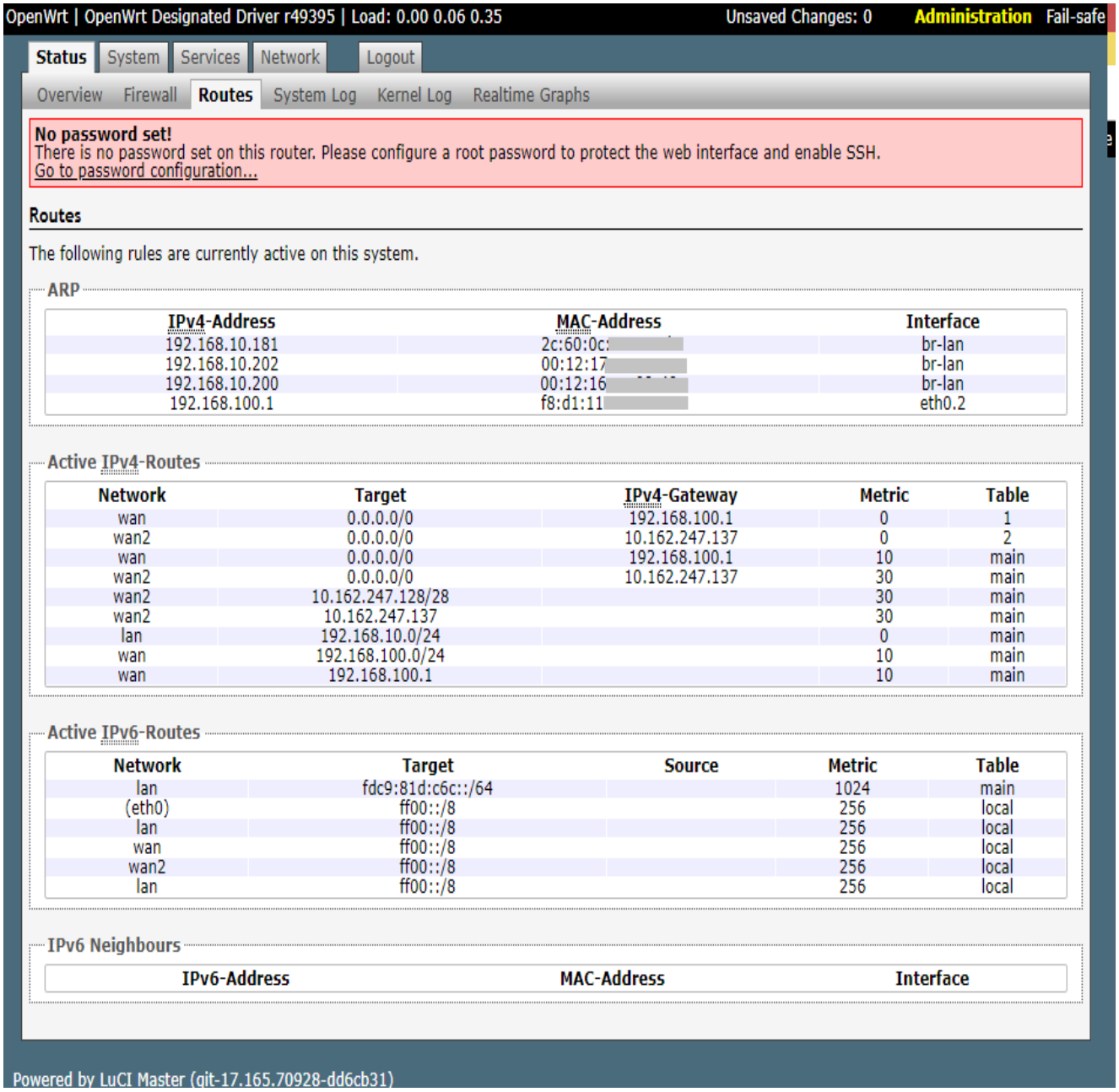
Chain *zone_wan_prerouting* (References: 2)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	MINIUPNPD	all	*	*	0.0.0.0/0	0.0.0.0/0	-
0	0.00 B	prerouting_wan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for prerouting */

3-3 Routes 路由

Routes 路由: Status➔Routes

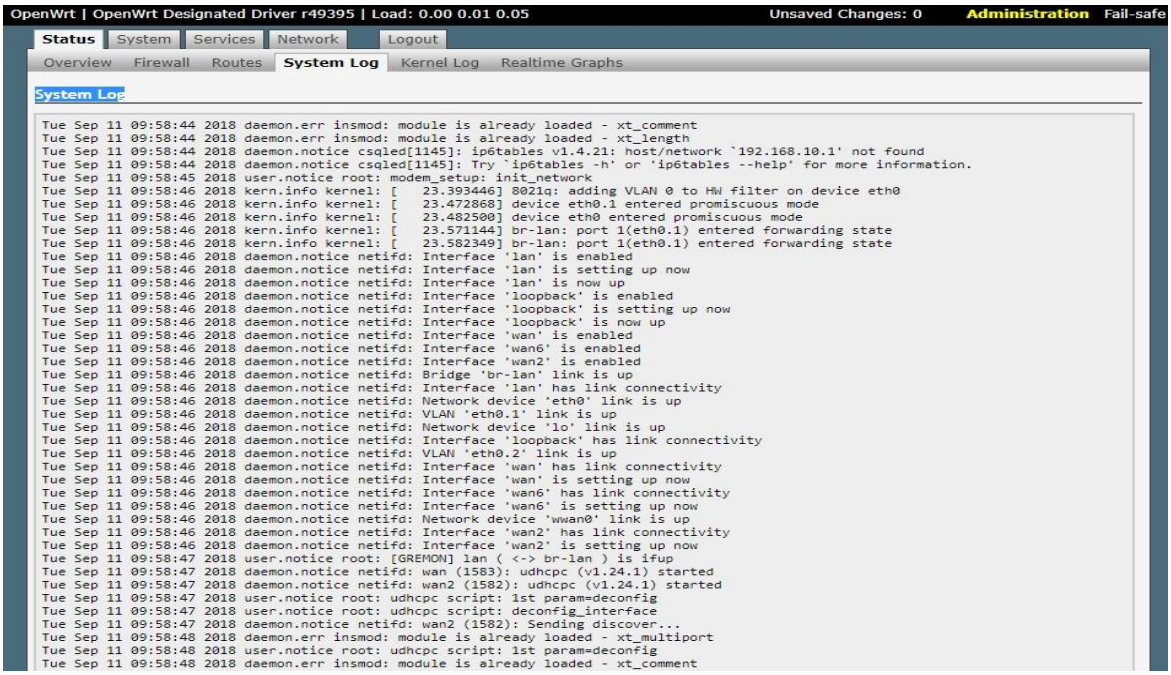
顯示依所例規則及 Interface 在這個系統上當前的活動狀態，包括 Lan 端使用者 IP 及 MAC/WAN 及 WAN2 等資訊，是選擇網絡中用於發送網絡流量的路徑的過程。有幾種路由協議可以或多或少地自動發生。為此，我們將使用靜態路由。路由由內核的組件處理，



3-4 System Log 系統日誌

System Log 系統日誌 : Status➔System Log

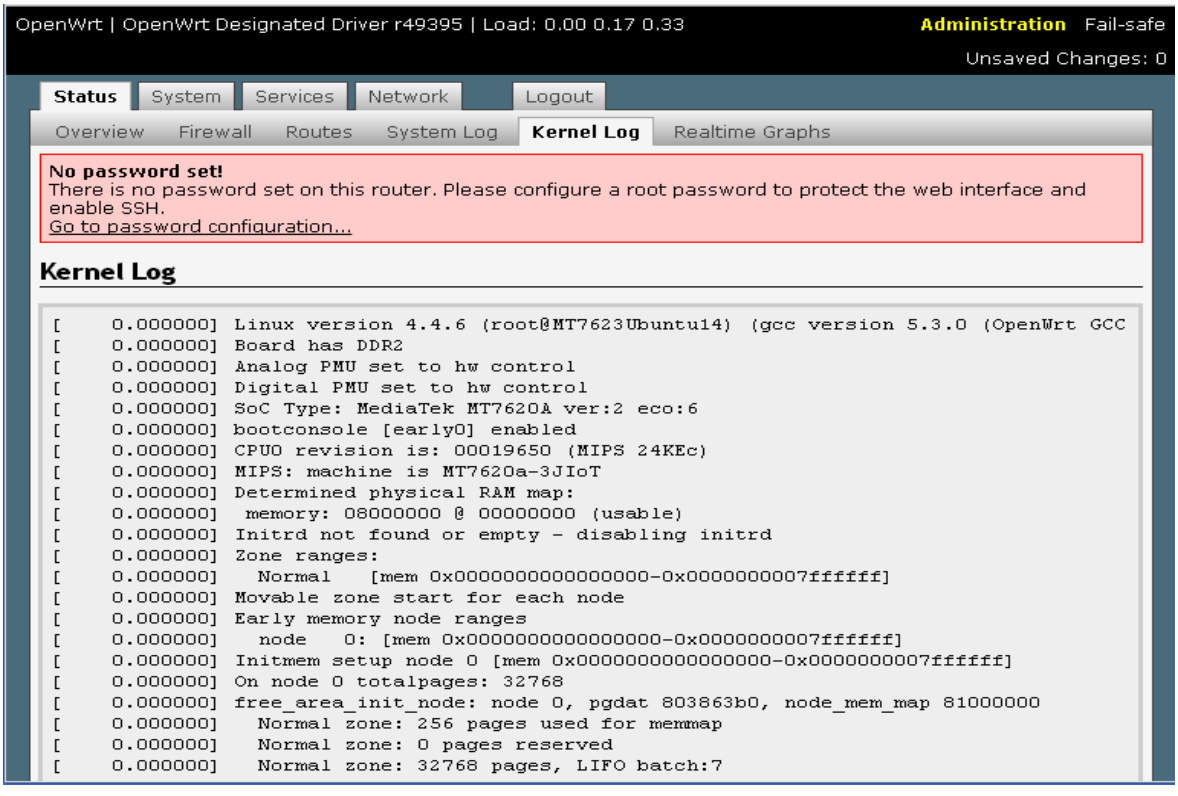
系統運行日誌記錄



3-5 Kernel Log 核心日誌

Kernel log 核心日誌：Status➔Kernel Log

核心運行日誌記錄

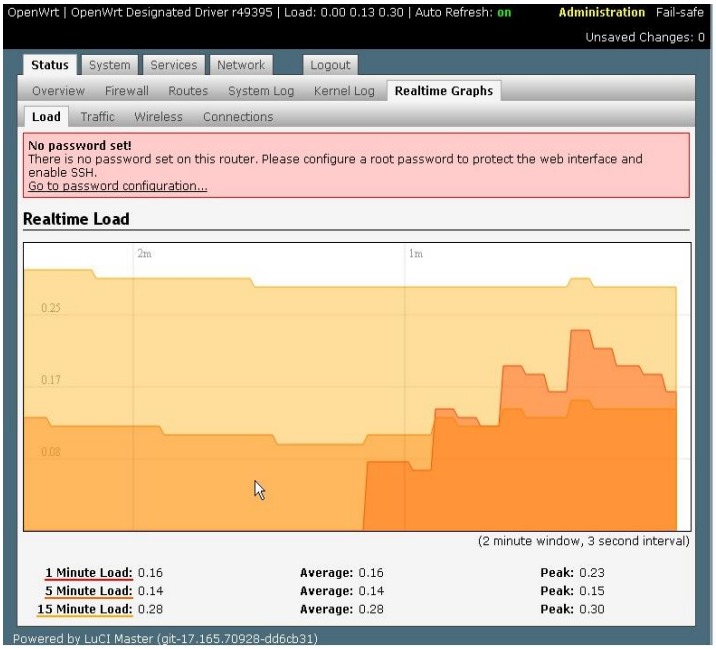


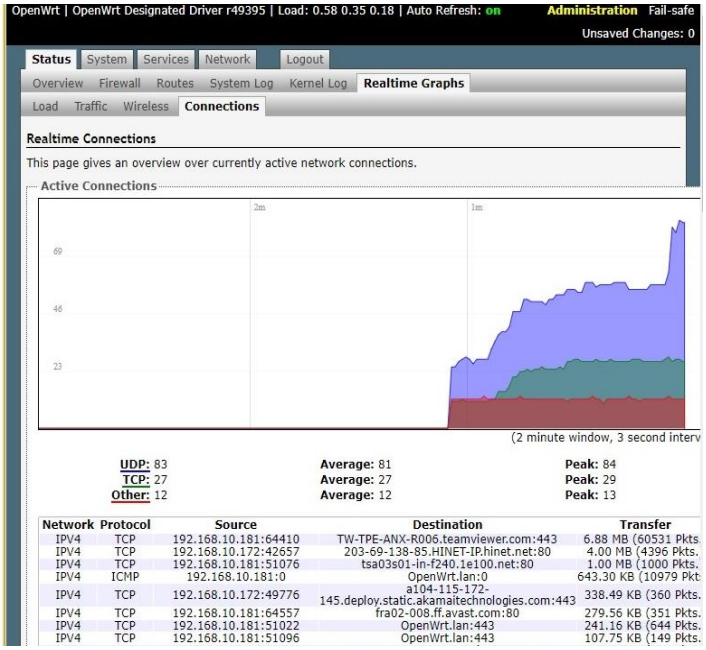
3-6 Realtime Graphs 即時圖表

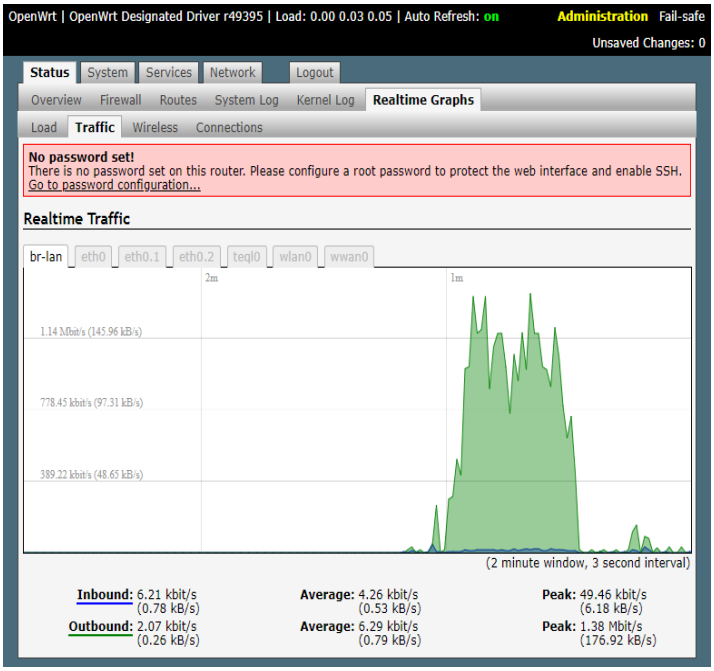
Realtime Graphs 即時圖表：Status➔ Realtime Graphs

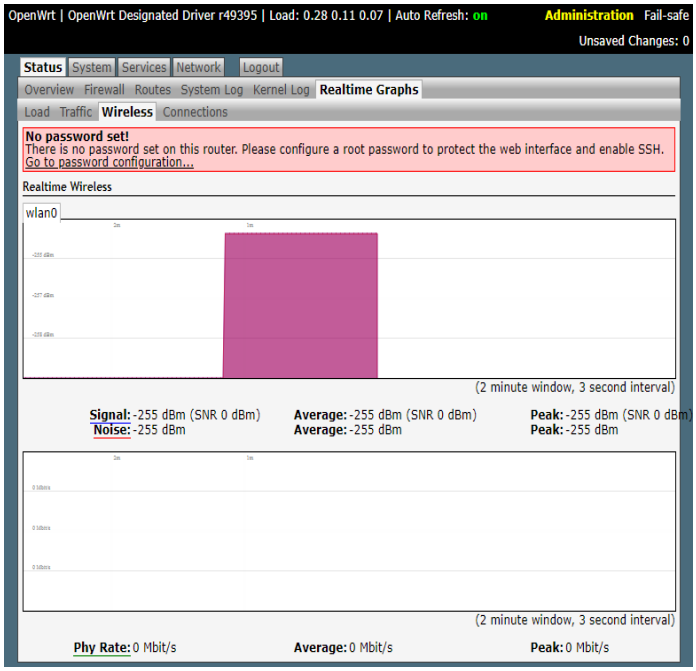
類似 MRTGK 的即時圖型資訊，包含

Load 即時負載/即時連接 Connections/即時流量 Traffic/即時無線流量 Wireless









4. 系統功能設定

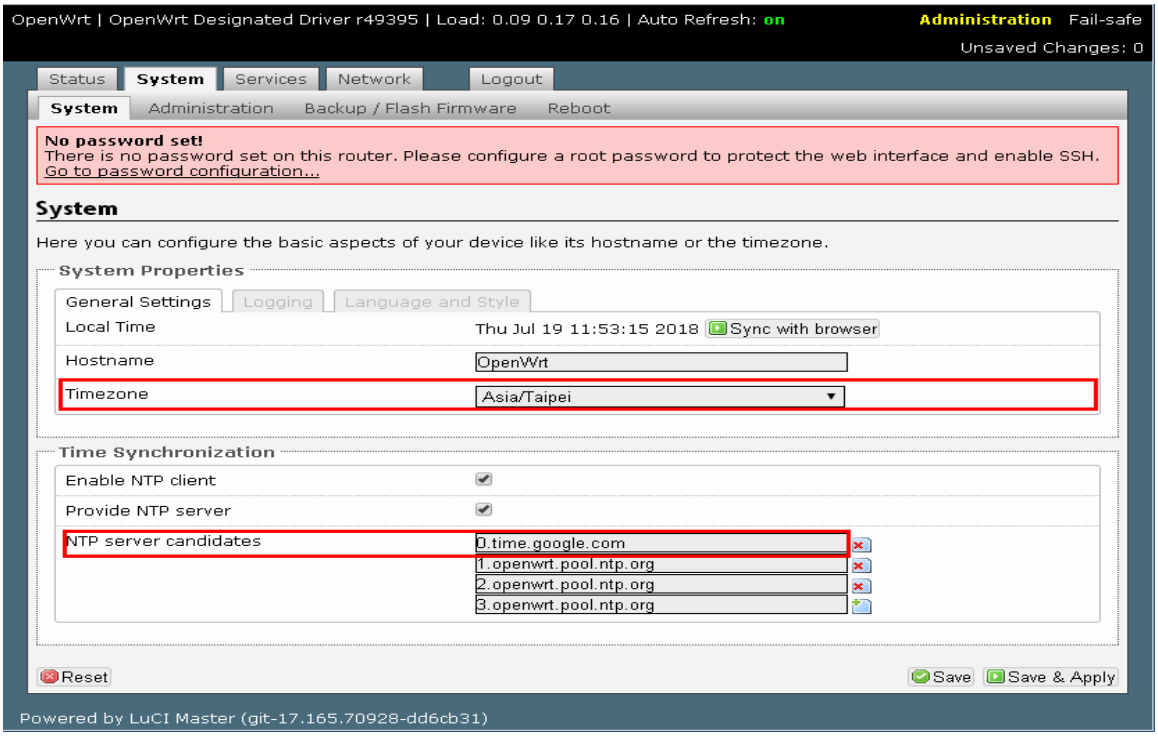
4-1 System 系統

System 系統：System➔System

可設定 IWR 路由器的時間/時區，記錄 log 的儲存及語系等設置。

General Settings 基本設置

選擇您所要的 Timezone 時區，如 Asia/Taipei or UTC 與可自定多個 NTP 網路校時伺服器可設定 time.google.com，設定好後按下 Save & Apply 鍵。



Logging 記錄設置

System log buffer size:設置記錄檔 buffer 容量大小

External system log server: 記錄檔儲存到遠端伺服器的 IP 位置

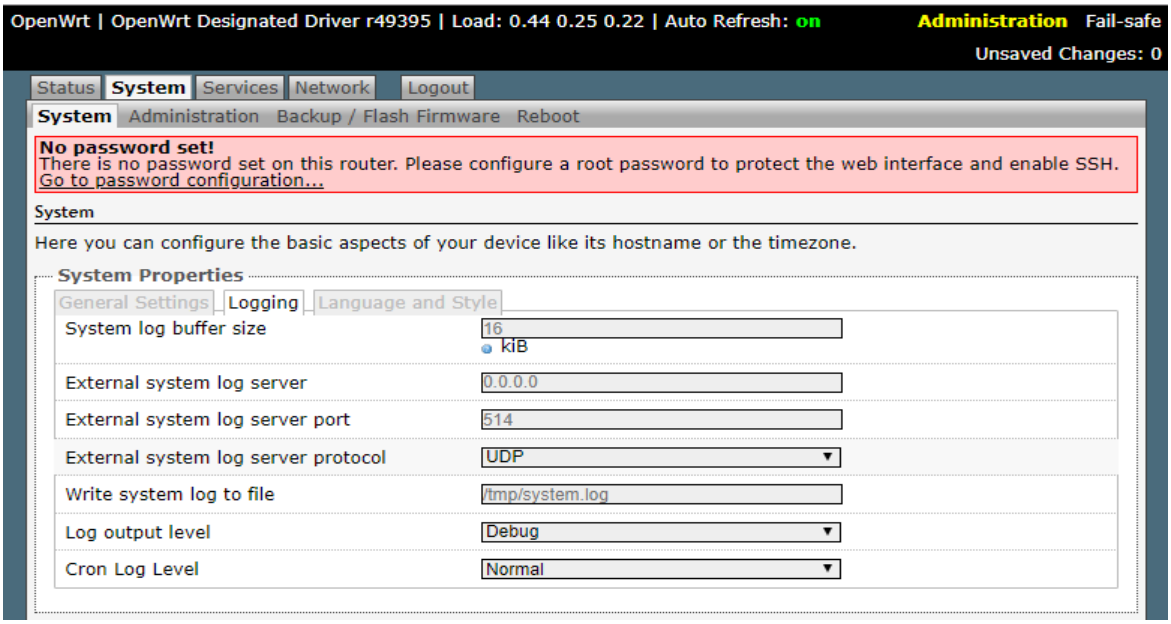
External system log server Port: 記錄檔儲存到遠端伺服器的 Port

External system log server protocol: 記錄檔儲存到遠端伺服器的通訊協定

Write system log to file: 記錄檔儲存成檔案

Log output level：記錄檔輸出的級別或分類

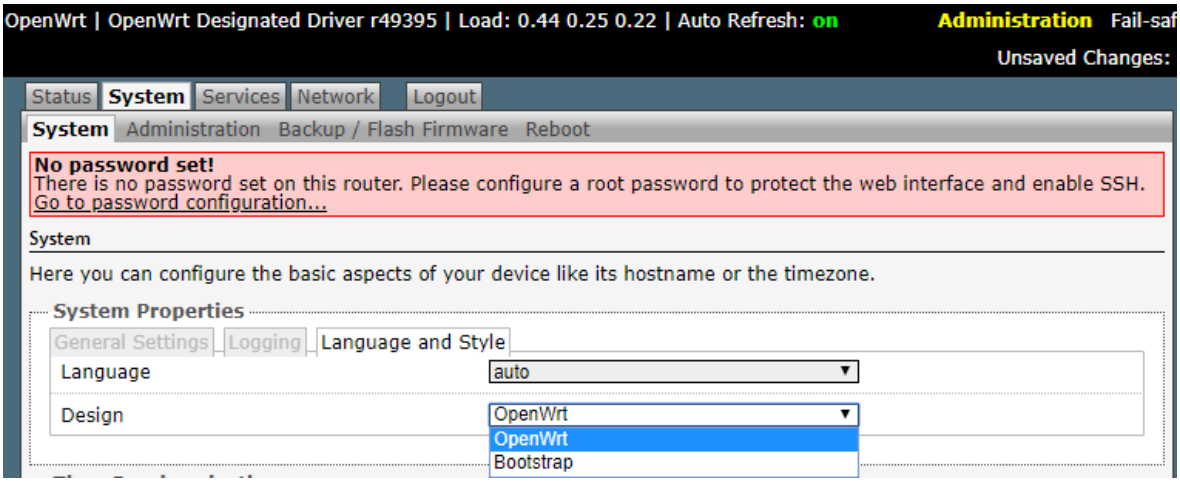
Cron Log Level：



Language and Style 語言和風格

Language 預設為 Auto

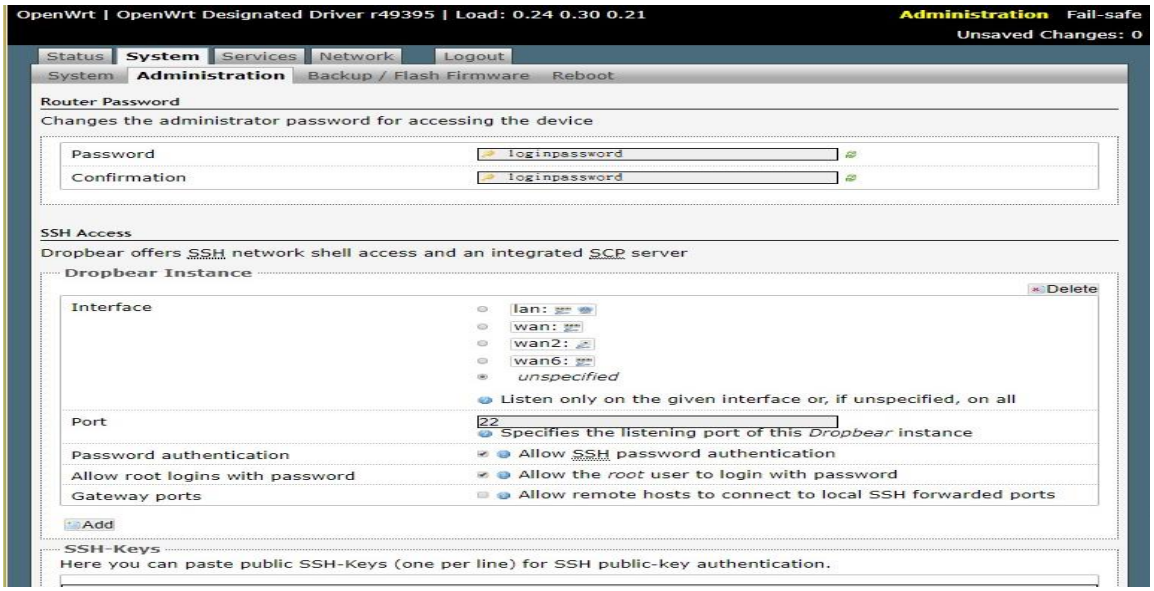
Style 預設為 OpenIWR



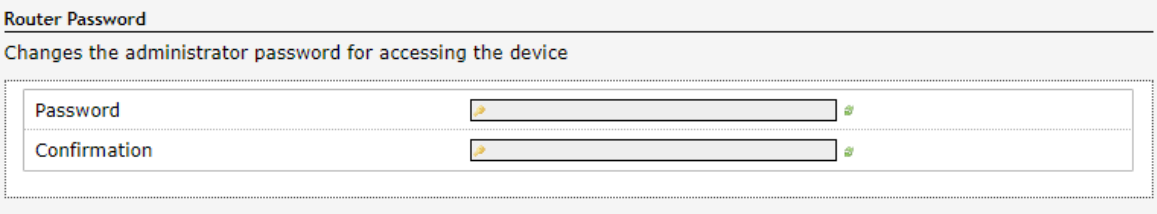
4-2 Administrator 管理員

Router Password & SSH Access 本地登入密碼 &遠端登入：System➔Administration

可自行變更最高權限 Login 密碼/設定 SSH 遠端登入 Router



更改用於訪問設備的管理員密碼：在 Password 與 Confirmation 欄位內鍵入欲變更的密碼後再按下 Save & Apply



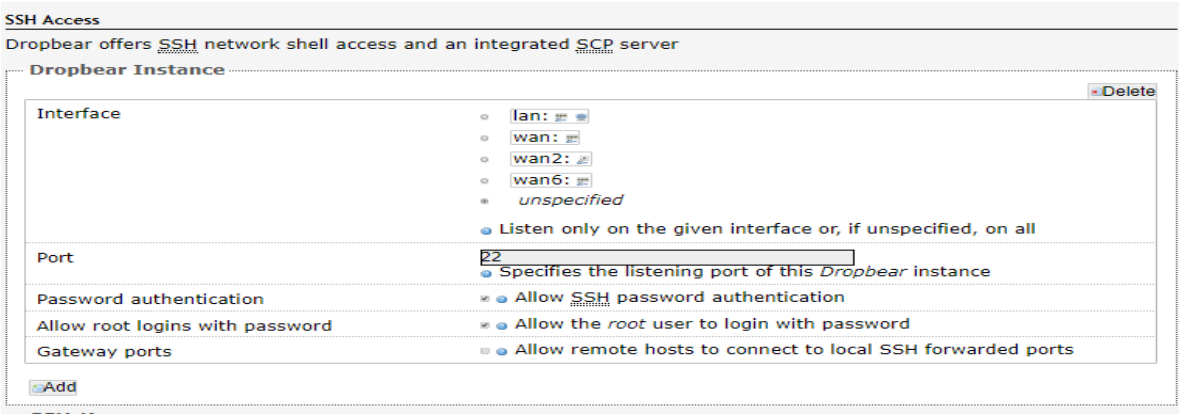
設定 SSH Access:SSH 遠端登入 Router 提供 Dropbear SSH 網絡 shell 訪問和集成的 SCP 服務器供遠端登入，類似 Telnet

Interface: 告訴 dropbear 只在指定的界面上監聽　　Port:要收聽的端口號

Password authentication: 是否使用密碼進行身份驗證

Allow root logins with password: 是否使用 root 密碼驗證

Gateway ports: 是否允許遠程主機連接到本地 SSH 轉發端口



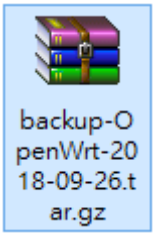
提供 SSH 網絡 shell 訪問和集成的 SCP 服務器供遠端登入，類似 Telnet

4-3 Backup / Flash firmware 備份還原設定值/更新韌體

Backup /Restore 備份及還原: System➔Backup / Flash Firmware➔Actions

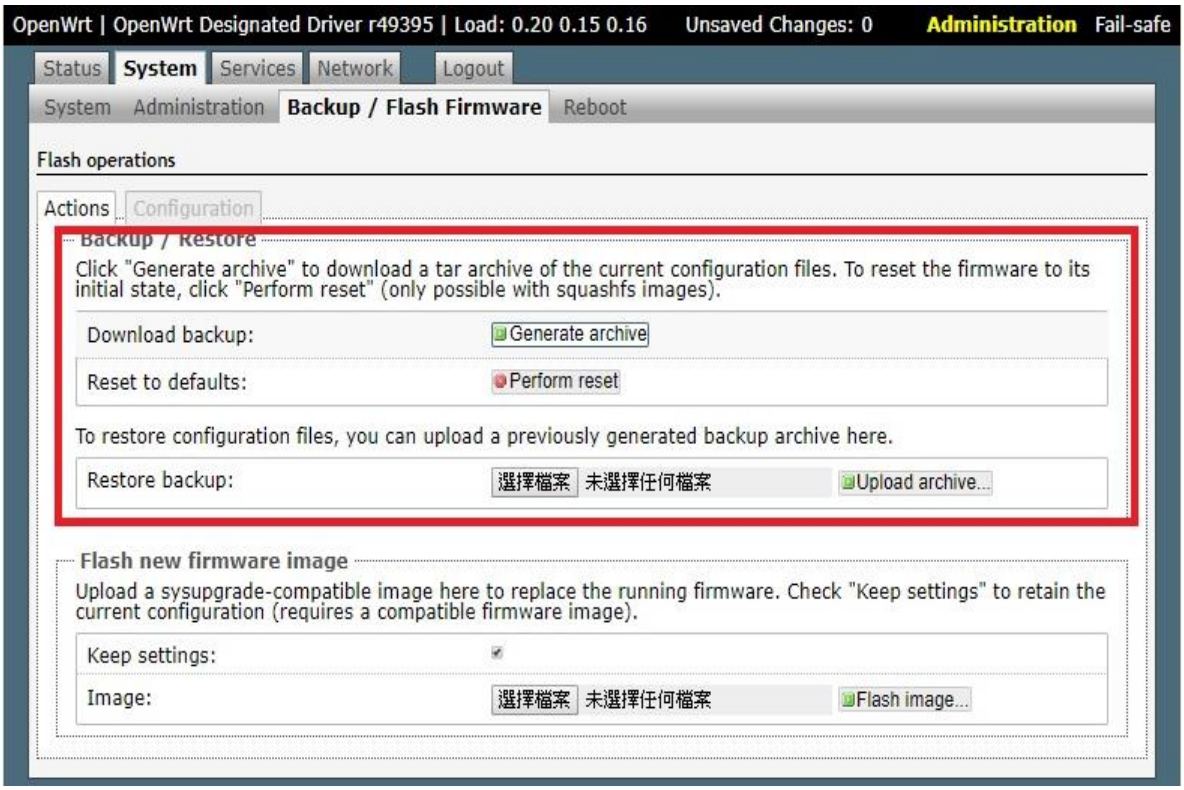
此功能為(1)備份 Router 系統設定值（Download backup）:

按下”Generate archive”即將現所有設定值成一壓縮檔，如下圖。



(2)載入 Router 系統 設定值(Restore backup)：選擇檔案位置後按”Upload archive”

(3)還原出廠預設值(Reset to defaults)：按下”Perform reset”過程中勿中斷電源



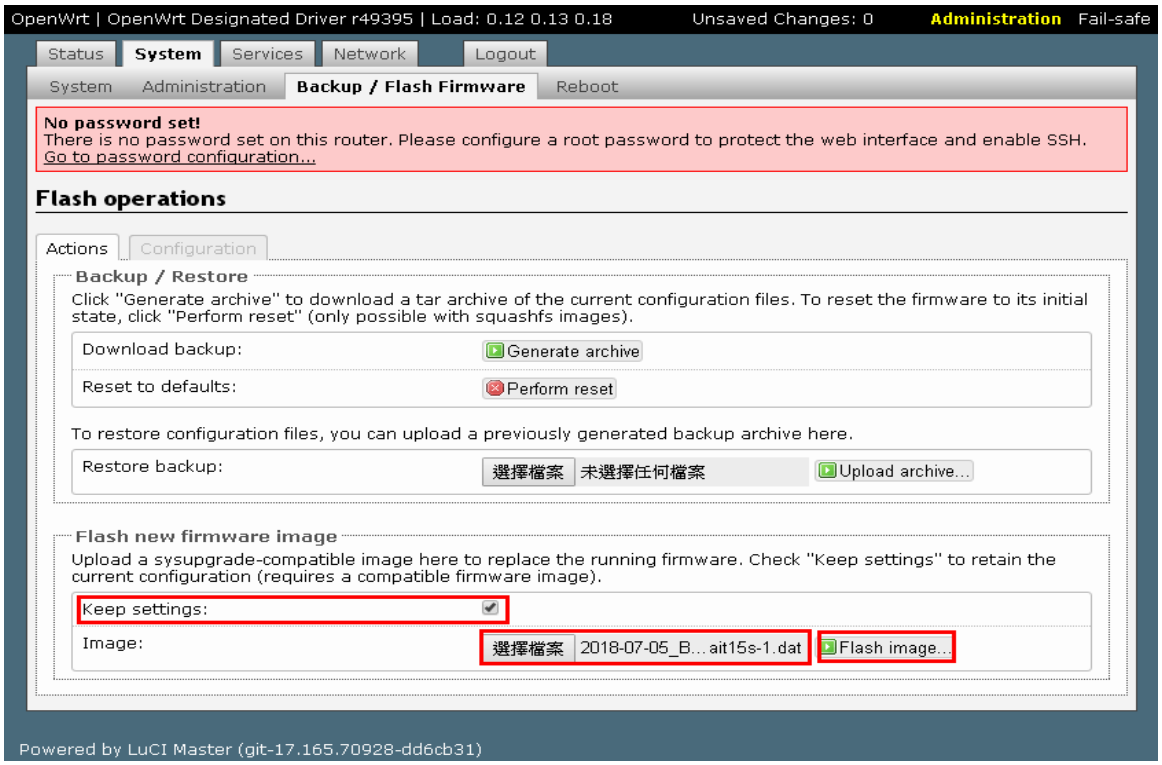
(4) Flash new firmware image 韌體更新

System➔Backup / Flash Firmware➔Flash new firmware image

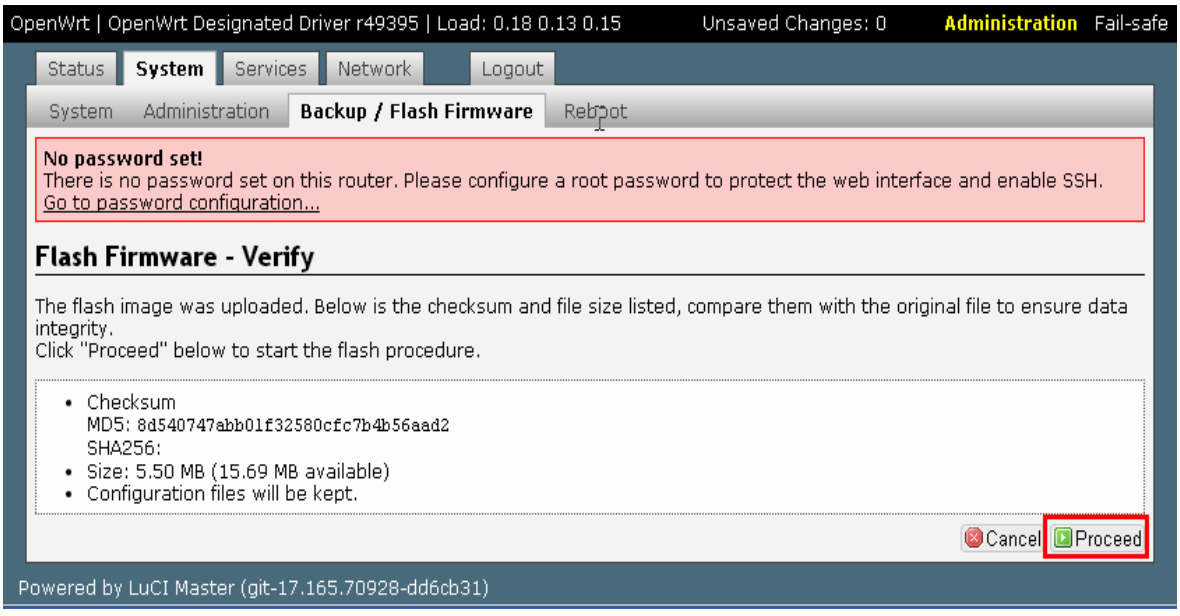
選擇更新韌體檔案(路徑)以進行更新流程，如果要保留當前主要設定值，請在 Keep settings 打勾。點擊 Flash image…，待出現提示畫面後，點擊 Proceed 開始更新流程並等待系統重啟。強烈建議更新韌體後請再次執行"1.7 重啟為出廠預設值"的動作並進行相關設定值的設定。

【注意：更新韌體到重新進入系統前，請勿關閉電源】

4.3.1 載入韌體檔案並上傳到系統



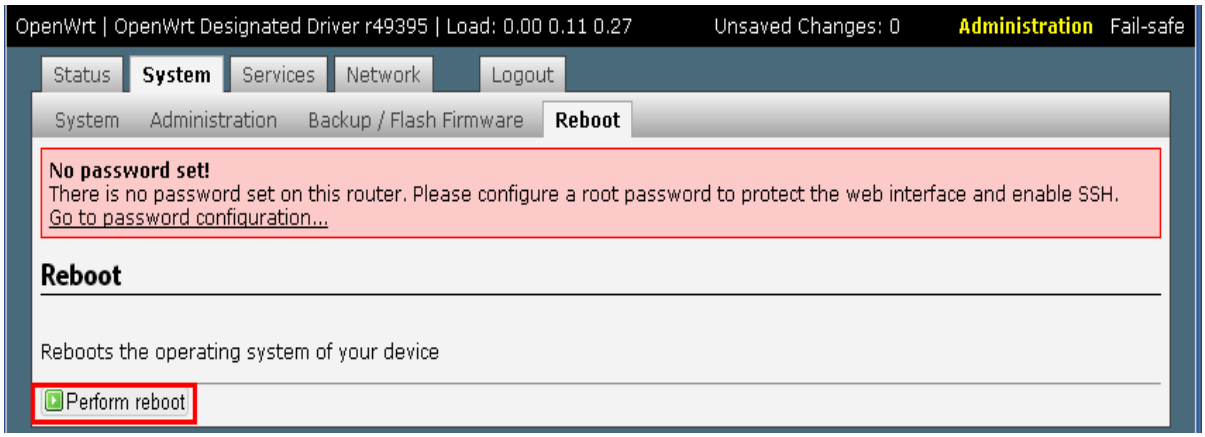
4.3.2 Flash 更新檔已上傳， 下圖列出了校驗和和文件大小，請單擊下面的“繼續”以啟動更新。



4-4 Reboot 重啟

Reboot 重新啟動：System➔Reboot

重新啟動設備的操作系統



5. 服務功能設定

Services 服務 ：Services

包含 GPS GW / Beacon GW / uHTTPd / Serial GW 等功能。

5-1 GPS GW 全球定位功能

Services➔GPS GW

1. Start GPS GateWay service:

是否啟用，如果需要此功能，請將 Start GPS GateWay service 選項打勾。

GPS Report interval(3 ~ 65535 seconds)：GPS 間隔紀錄依個人需要設並定。

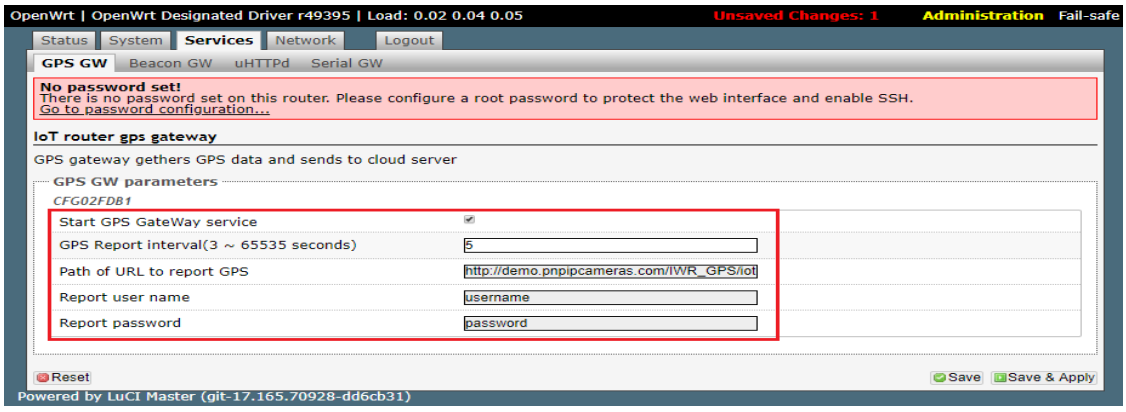
Path of URL to report GPS:

紀錄網址路徑 http://demo.pnpipcameras.com/IWR_GPS/iotcurlgps.php

Report user name & password:

設定個人的 Report user name 與 Report user password(目前不需要設定)。

設定好 GPS 相關設定後套用，按下 Save & Apply 鍵



2 檢視 GPS 路徑報告

2.1 打開 GPS 路徑紀錄網址 http://demo.pnpipcameras.com.tw/IWR_GPS/

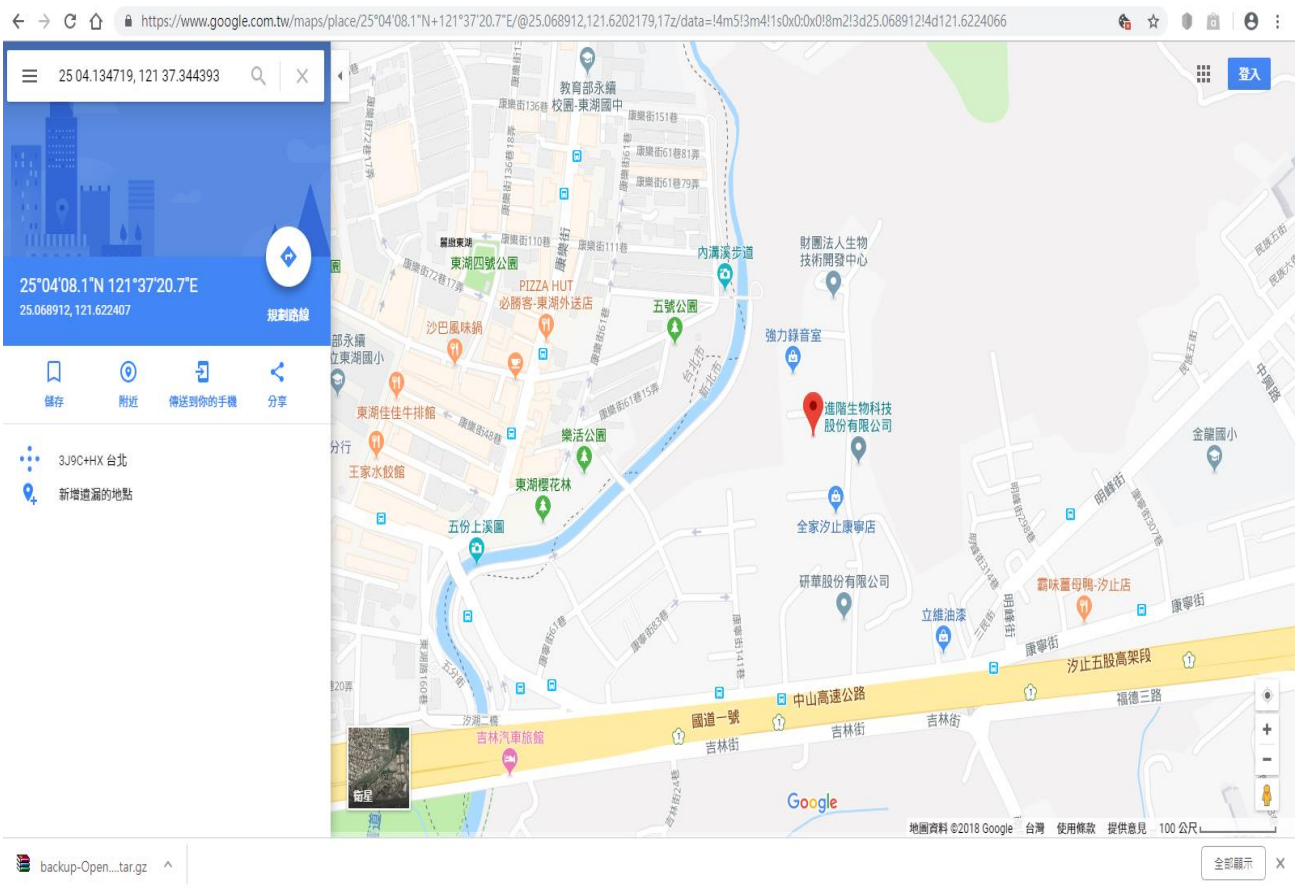
GPS

Searcher

Get Total Rows : 8

MAC	IMEI	Date Time (DDMMYY HHMMSS)	GPS address	Map link
00:09:b5	861107031320121	200718 040633	2504.134719,N, 12137.344393,E	Click Map
00:09:b5	861107035028035	220818 074546	2504.123576,N, 12137.328417,E	Click Map
00:09:b5	861107036162627	170918 034349	2503.583186,N, 12132.661951,E	Click Map
00:09:b5	861107037130920	240818 103439	2504.154933,N, 12137.354538,E	Click Map
00:09:b5	863424030864548	180718 015810	2503.586610,N, 12132.648894,E	Click Map
00:09:b5	863424030864803	160718 084200	2503.581382,N, 12132.677074,E	Click Map
00:09:b5	863424030866329	310718 033527	2504.132246,N, 12137.347423,E	Click Map
00:09:b5	866758040407070	170918 013307	2504.139912,N, 12137.356030,E	Click Map

2.2 根據您 IWR 路由器外殼上的貼紙資訊(4G 模組的 IMEI 號碼或 Mac Address)來點擊 Click Map 檢視您所需要的 GPS 路徑圖。注意：時間可能因為是 https://192.168.10.1/cgi-bin/luci/admin/system 設定在 UTC 而有所不同。



5-2 Beacon GW 設定(選配)

Services➔Beacon GW

為雲端 MQTT 伺服器啟動接收 Beacon 數據之服務

如果需要此功能，請將 Start Beacon GateWay service 選項打勾後按下 Save & Apply 鍵。

Beacon MQTT Server URL ： 雲端 MQTT 伺服器位置為 61.56.193.66.

MQTT Server port ： 雲端 MQTT 伺服器連接埠為 1883

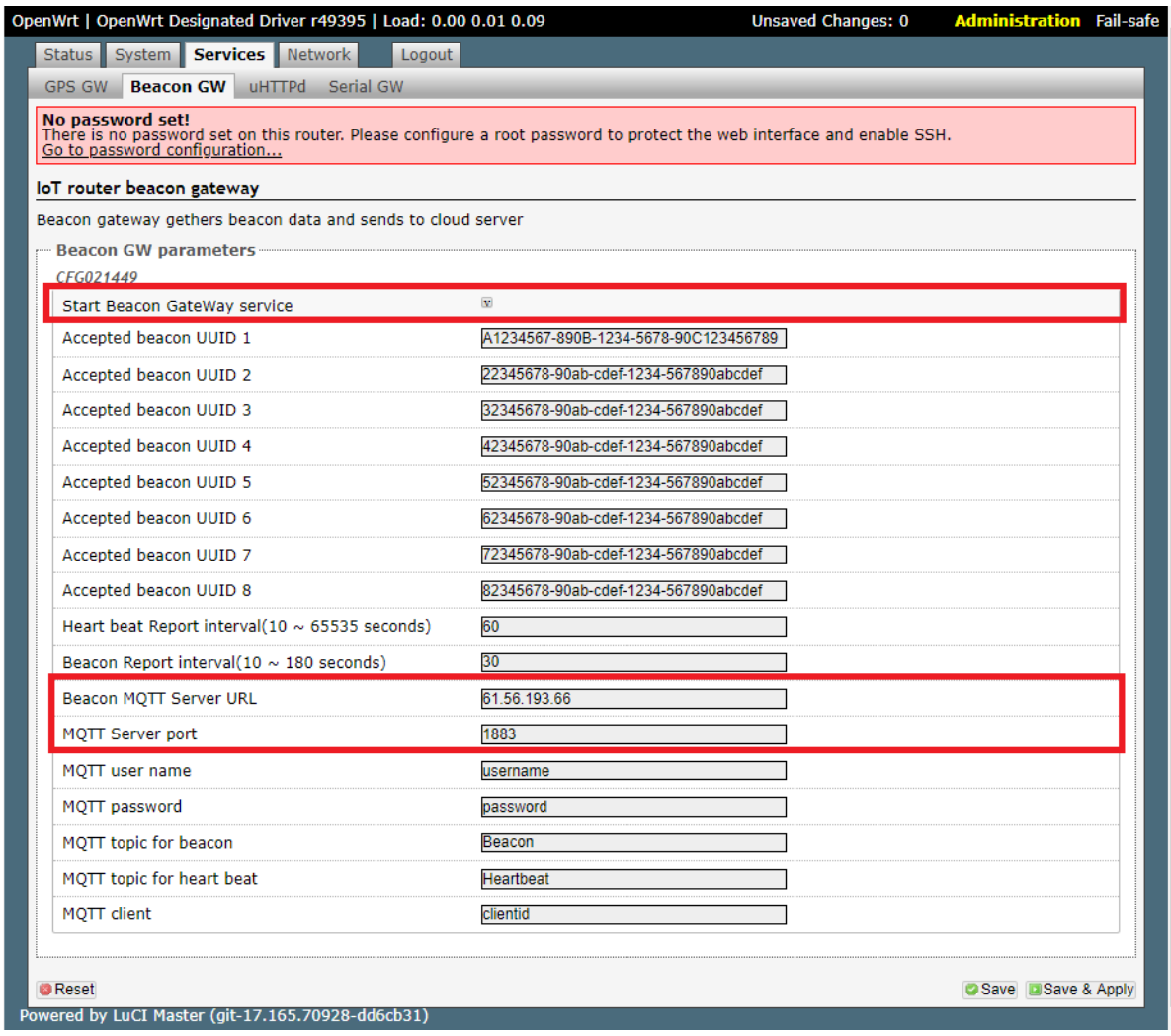
MQTT user name ： 使用者

MQTT password ：密碼

MQTT topic for beacon ：伺服器主題

MQTT topic for heart beat：MQTT **在線訊號**

MQTT client ： 伺服器角色



5-3 uHTTPd 服務器

Services➔uHTTPd

A lightweight single-threaded HTTP(S) server， uHTTPd 是 OpenIWR 的標準 HTTP 服務器，但本處目前僅開放做 HTTPS 轉址 HTTP 使用。

General Settings

HTTP listeners ： 設定 HTTP 監聽位址及埠，指定要偵聽純 HTTP 訪問的端口和地址。如果僅給出端口號，則服務器將嘗試同時提供 IPv4 和 IPv6 請求。用於 0.0.0.0:80 僅在 IPv4 接口上綁定端口 80 或[::]:80 僅用於 IPv6。要在多個接口上運行，指定每個接口，您可以列出每行一個接口（或接口：端口）

HTTPS listener：指定要偵聽加密 HTTPS 訪問的監聽位址及埠，格式同 HTTP

Redirect all HTTP to HTTPS :設定將所有 HTTP 重定向到 HTTPS

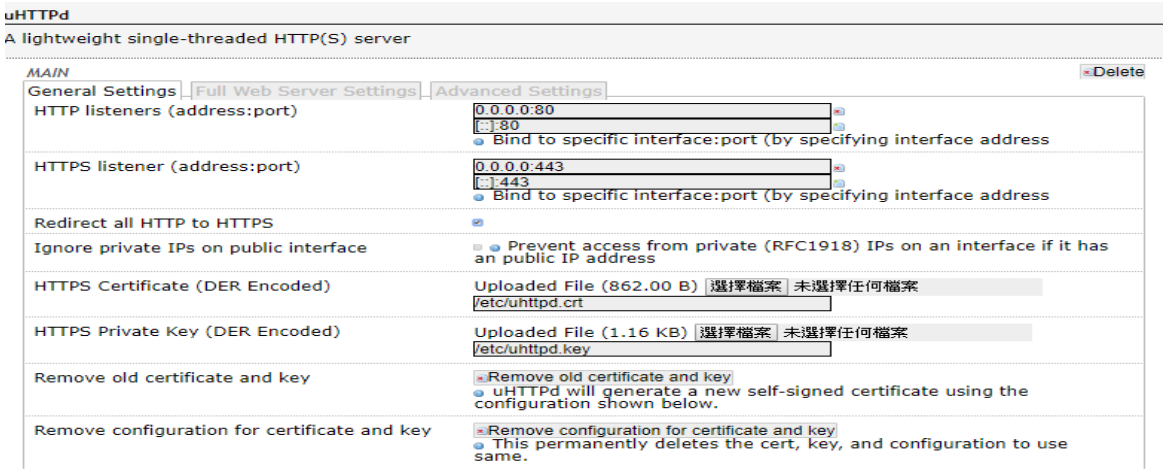
Ignore private IPs on public interface：忽略在公用界面上的私有 IPs

HTTPS Certificate：用於提供 HTTPS 連接的 ASN.1 / DER 證書的文件路徑

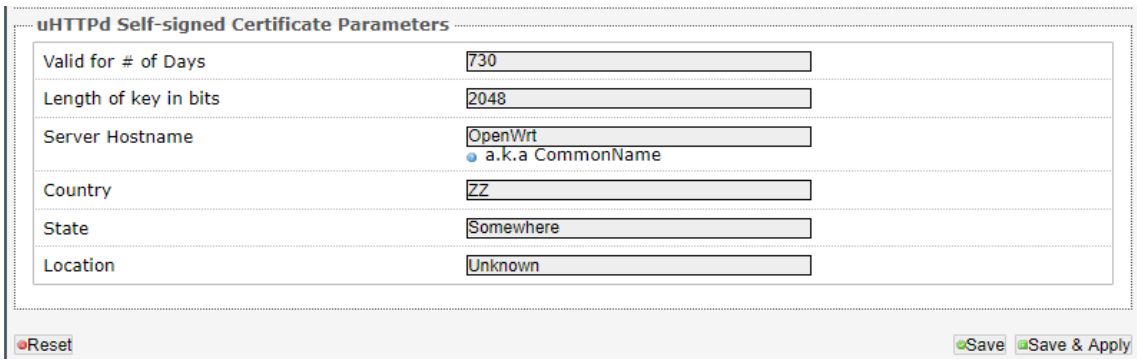
HTTPS Private Key：用於提供 HTTPS 連接的 ASN.1 / DER 私鑰的文件路徑

Remove old certificate and key：刪除舊的 DER 證書和 DER 私鑰

Remove configuration for certificate and key：刪除 DER 證書和 DER 私鑰的配置



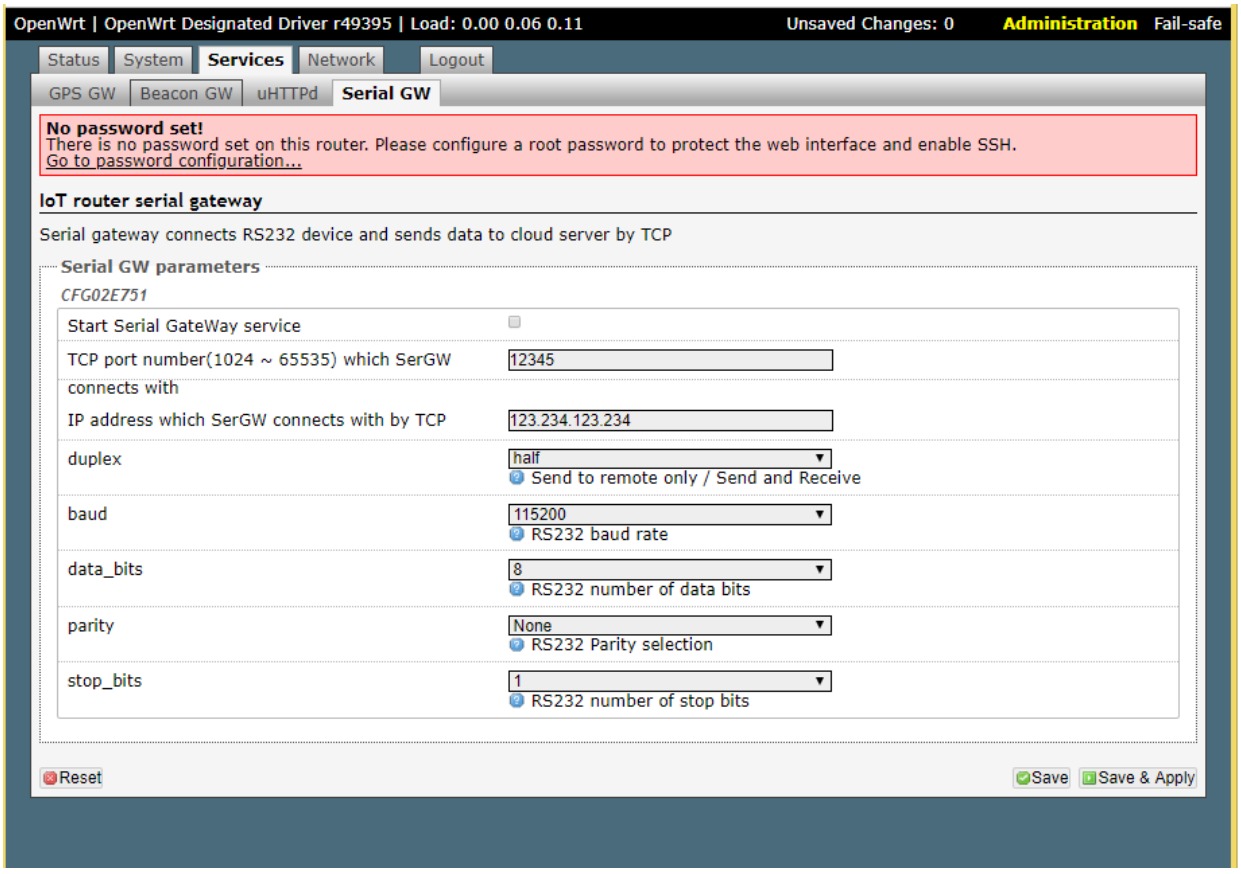
uHTTPd Self-signed Certificate Parameters：uHTTPd 自簽名證書參數



5-4 Serial GW 序列閘道

Services➔Serial GW 物聯網路由器 serial gateway
Serial GateWay 通過 TCP 連接 RS232 設備並將數據發送到雲服務器

Start Serial GateWay service：勾選啟用此服務
TCP port number(1024 ~ 65535) which SerGW：設定連接雲端伺服器的連接 Port 號
IP address which SerGW connects with by TCP：設定連接雲端伺服器的 IP 位置
Duplex：工作模式採 全雙工 or 半雙工
Baud：設定 RS232 baud rate
data_bits：設定 RS232 data bits
parity：RS232 Parity selection
stop_bits：RS232 number of stop bits

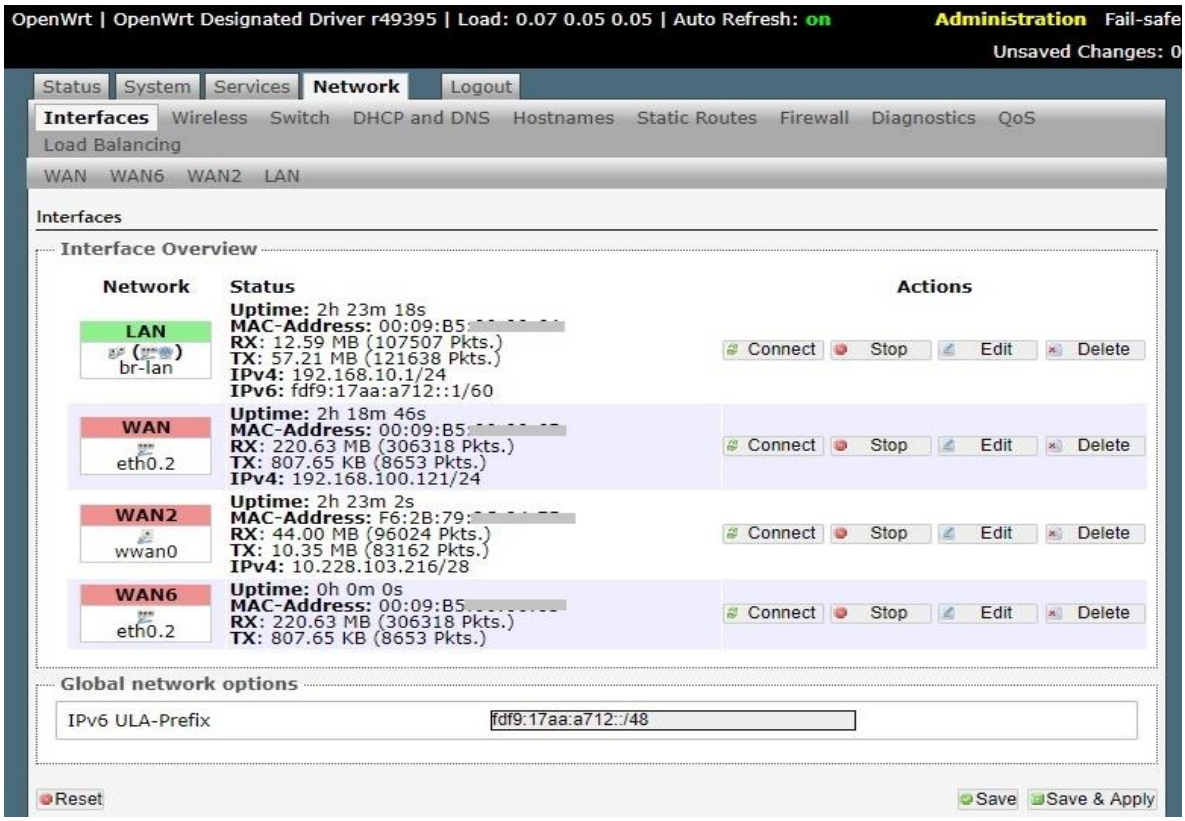


6.網路功能設定

6-1 Interface Overview 介面狀態

Interface Overview 各網路介面狀態：Network➔Interface

此處可查閱及設定各網路介面狀態

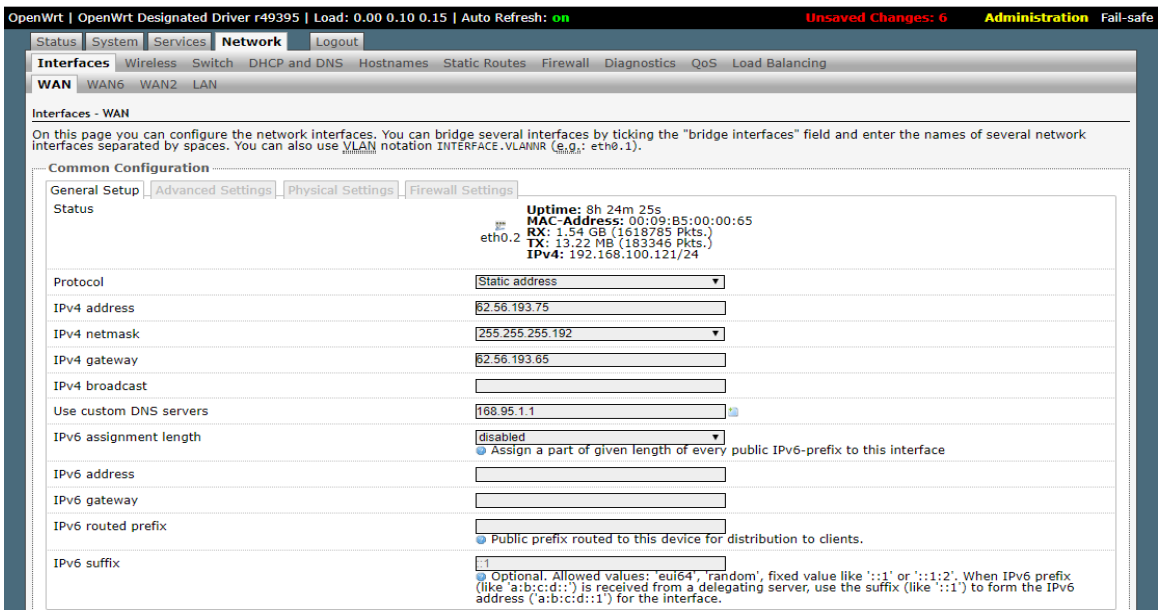


包含 WAN(IPV4)/WAN6(IPV6)/WAN2(4G)/LAN 的各細項設定，下列以 WAN 做說明。

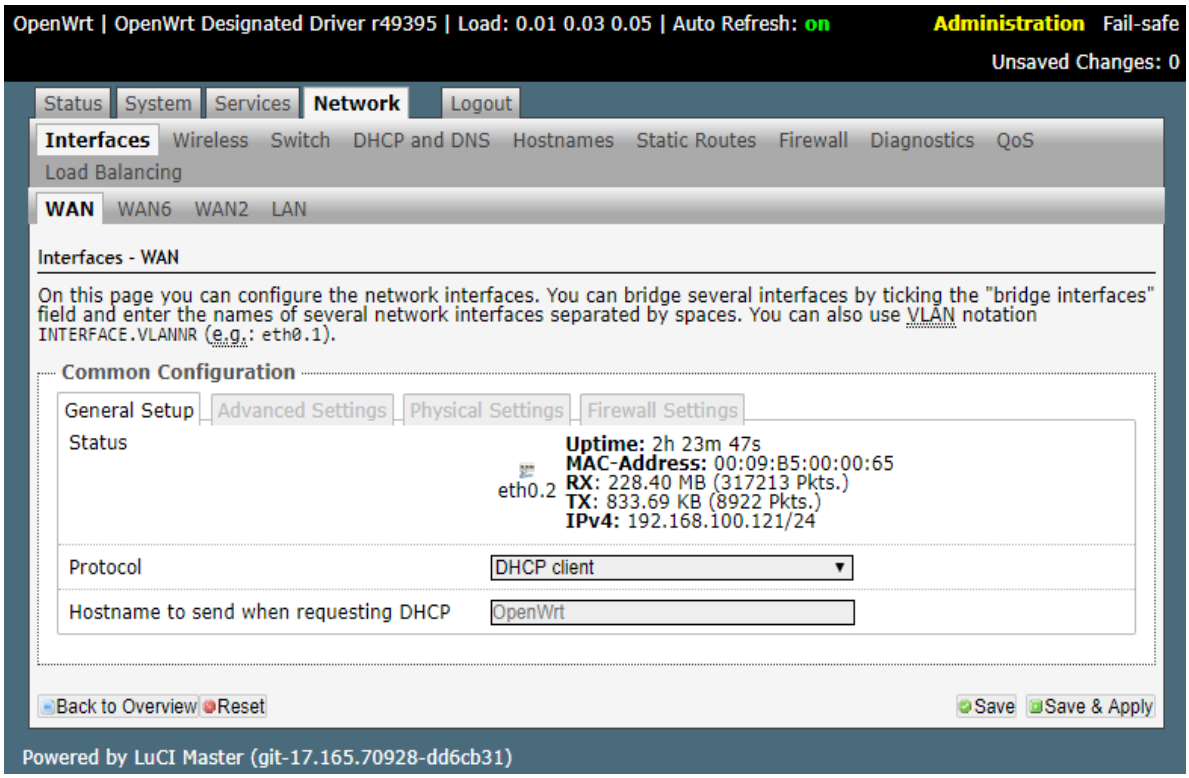
WAN(IPV4)➔General setup ：

可設定 WAN IP 取得的方式：靜態 IP/DHCP/PPPoE

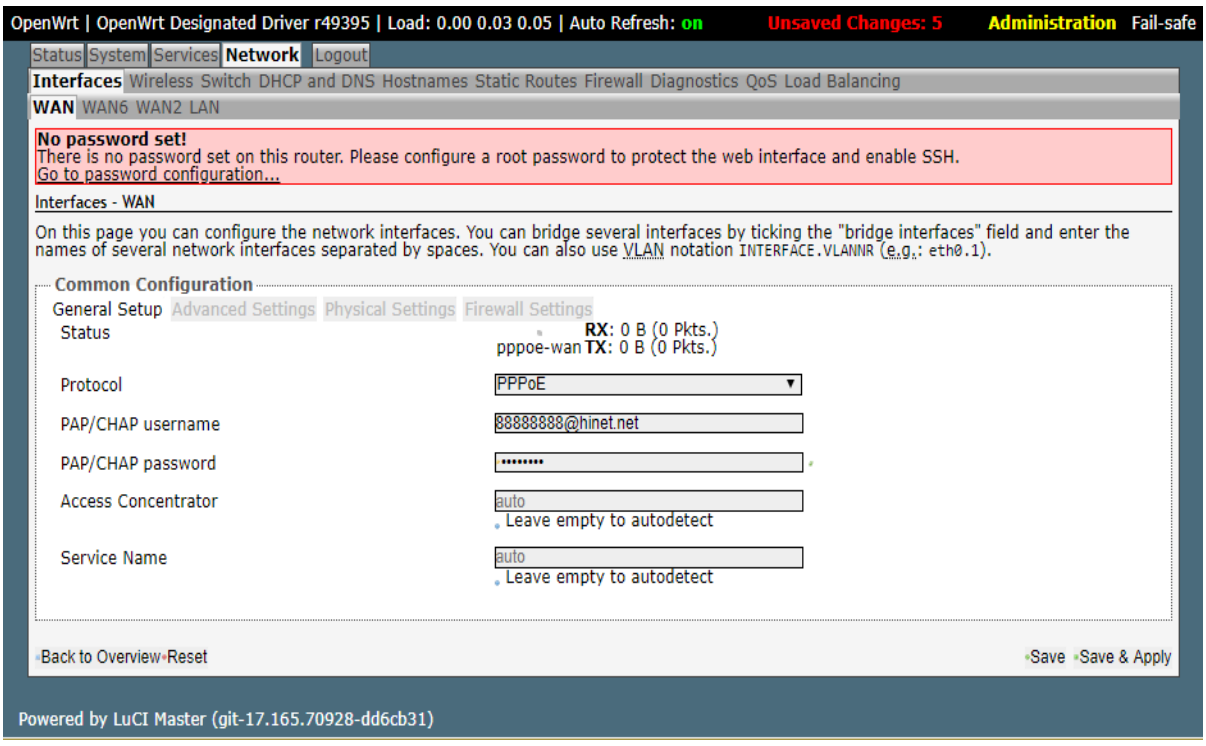
靜態 IP 設定：設定 IP Address / netmask / Geteway / DNS



DHCP 設定：自動取得 IP



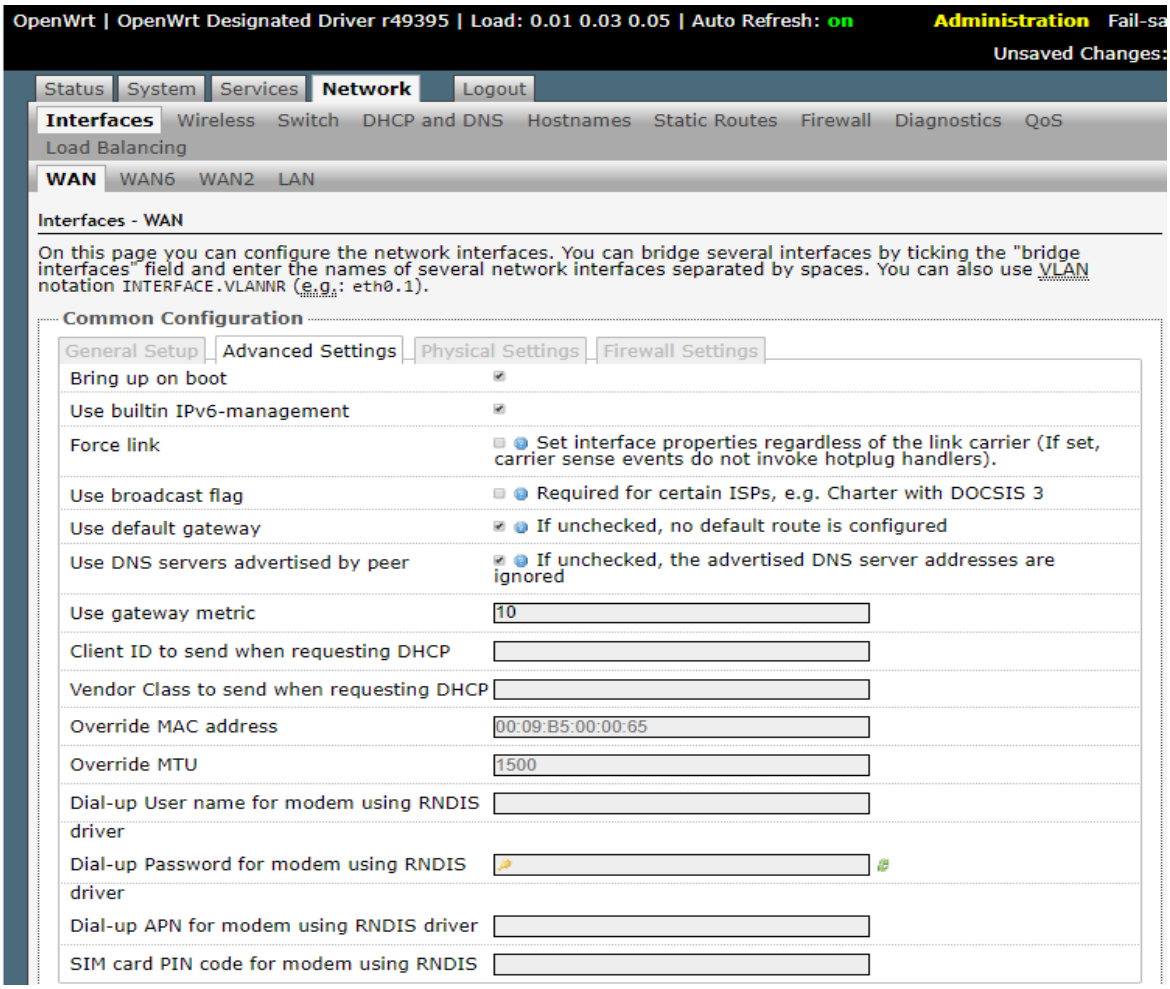
PPPoE 設定：使用您 ISP 所提供之帳號及密碼撥接



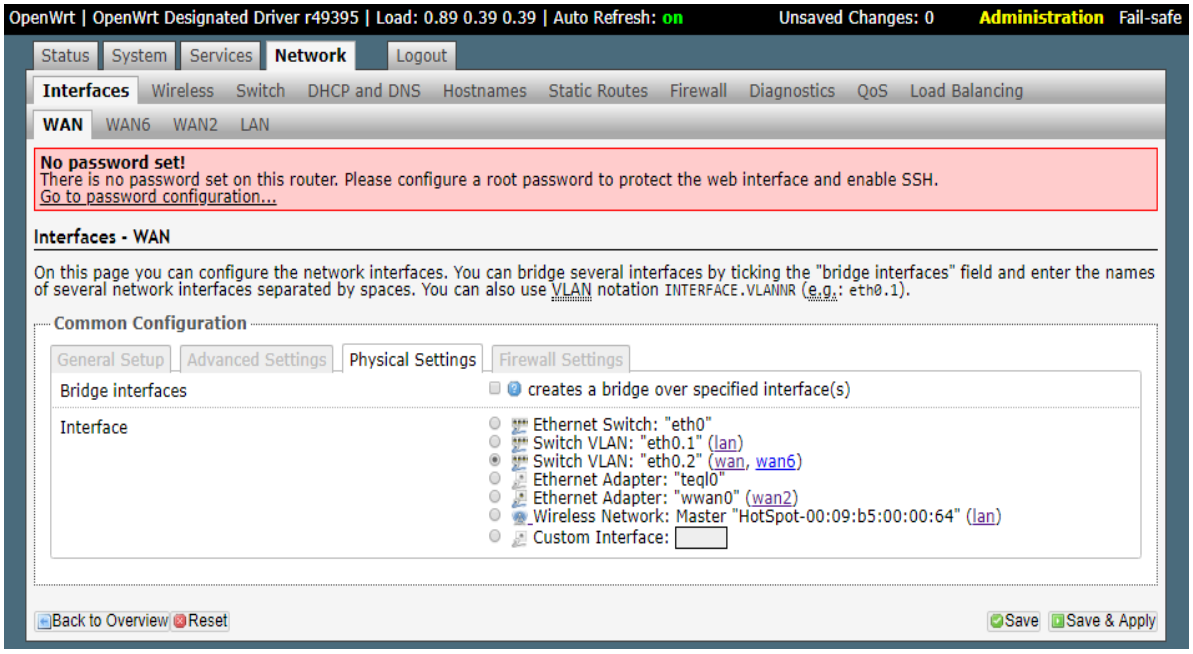
PPPoE Advanced Settings：此項內之設定請保留原廠預設值

WAN(IPV4)➔Advanced Settings：WAN 的進階設定，包含 Bring up on boot/ Use builtin IPv6-management/ Use default gateway/MAC address…

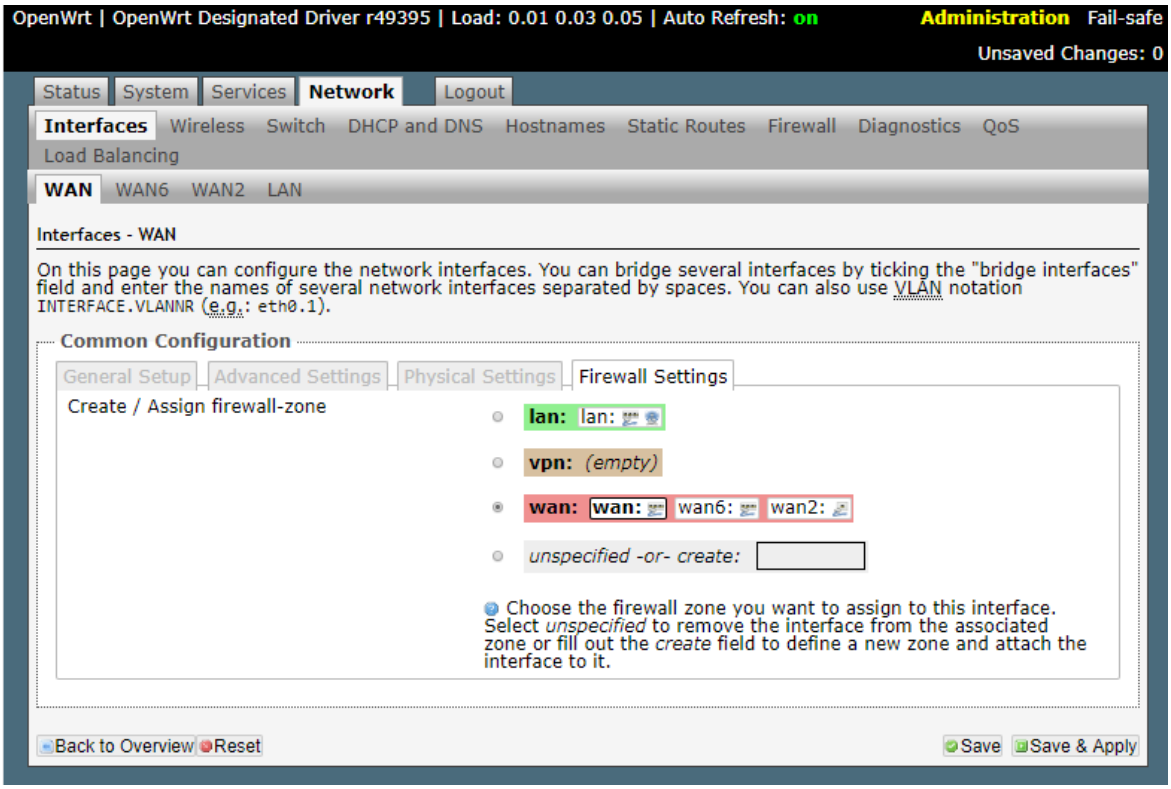
此進階設定內之設定值請保留原廠初始值



WAN(IPV4)➔Physical Settings：creates a bridge over specified interface

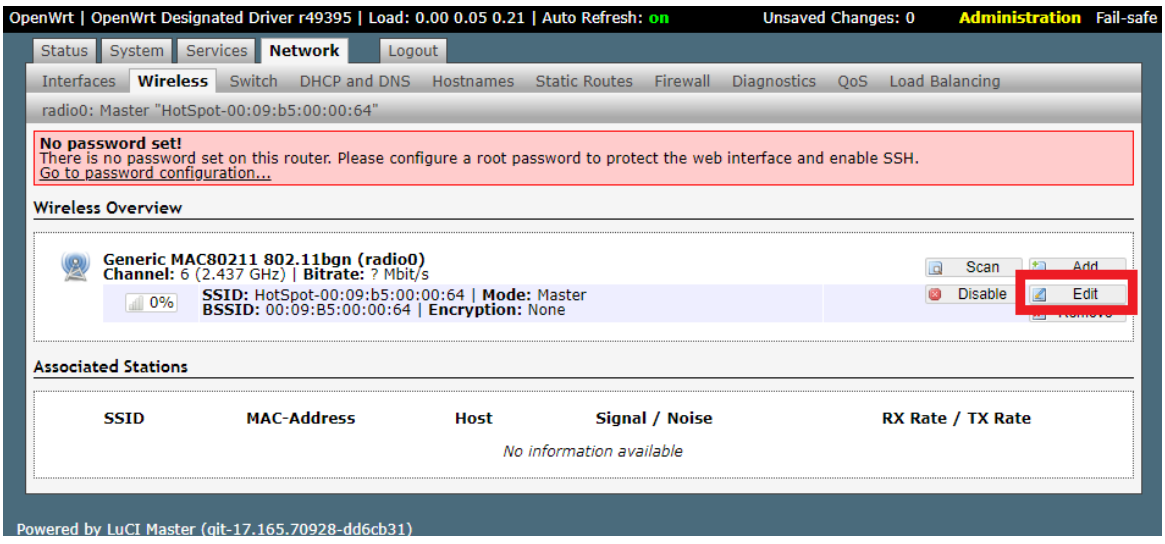


WAN(IPV4)➔Firewall Settings：Create / Assign firewall-zone



6-2 Wireless 無線設置

Wireless 無線設定：Network➔Wireless



預設 SSID 為 HotSpot-00:09:b5:00:00:64(MAC 則會依各主機號略有不同)

預設 WiFi 密碼是關閉的

Device Configuration

General setup ：Network➔Wireless➔Edit

基本設定中 Status 為顯示目前各項設定值的狀態

Wireless network is enabled 開啟或關閉無線網路

Operating frequency 調整模式 Mode 及頻道 Channel、頻寬 Width 等

Transmit Power 調整發射功率

ESSID/MODE 變更 SSID / 連線模式

Advanced Settings：Network➔Wireless➔edit➔ Advanced Settings

Country Code：指定國家/地區代碼，影響可用的通道和傳輸功率，802.11 工作組劃分了 4 個獨立的頻段：2.4 GHz、3.6 GHz、4.9 GHz 和 5.8 GHz[1]，每個頻段又劃分為若干頻道，每個國家自己制定了政策訂出如何使用這些頻段，例如最大的發射功率和配製方式等。

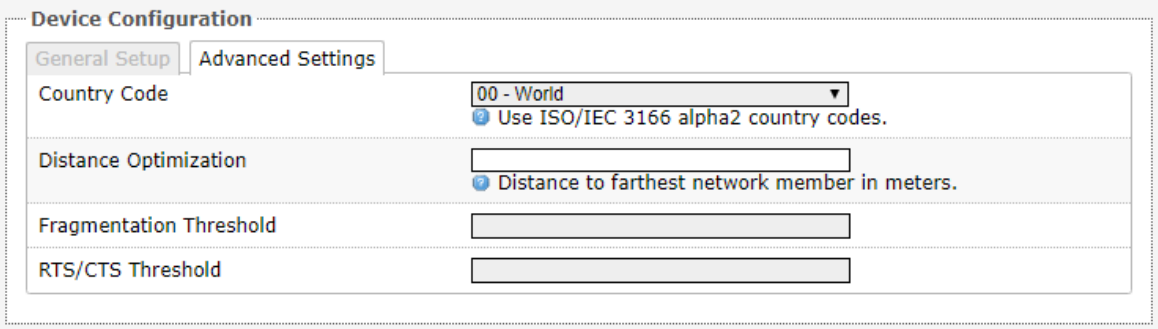
Distance Optimization ：距離优化指 ap 與最遠客戶間距離，以米為單位

Fragmentation Threshold：分段閾值

RTS/CTS Threshold：

RTS /CTS 功用同跟一般有線網路的 CSMA/CA 載波偵測

假設有二個 wireless client 同時跟一個基地台做資料傳輸.二個 wireless client 之間又有距離無法知道對方也在搶著講話,這時會產生碰撞狀況.所以基地台和 wireless client 可以設定多少大小 frame ,才使用 rts/cts 功能,rts/cts 如非必要 不要用會影響到效能 .因為 wlan frame 最大 2304+8 wep byte=2312 所以訂 2312 -到 2346 等於是"不啟用 "RTS/ CTS ，使用時機是能（1）當 wireless client 端很散亂分布（2）rf 頻譜干擾嚴重時



Interface Configuration

General setup ：Network➔Wireless➔edit➔ Interface Configuration

ESSID：修改 WiFi 名稱

Mode：設置無線模式，包含橋接器 Access Point、APClient 模式、Ad-Hoc 、802.11S、WDS…等

Network：選擇要附加到此無線接口的網絡，或填寫“新建”以定義新網絡

Hide ESSID：啟用隱藏 ESSID

啟用了隱藏 SSID 選項，所以無線用戶端無法掃描到其 SSID。

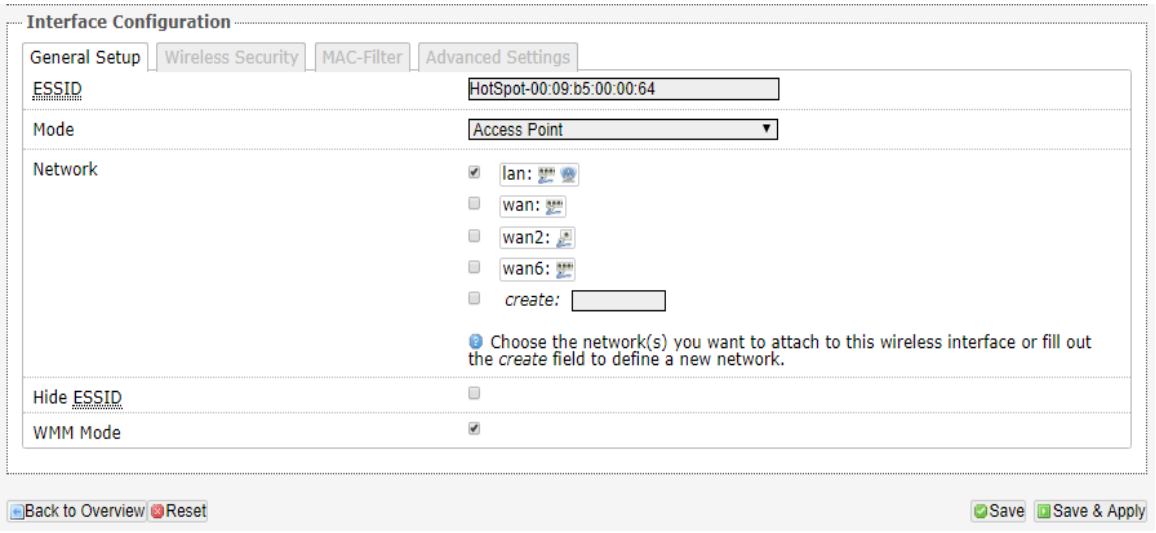
1. 請點選變更進階設定，進入無線網路內容

2. 點選新增，設定無線網路

3. 手動輸入網路名稱（ SSID ）並將資料加密停用

4. 由網路連線-> 無線網路-> 內容可發現無線網路連線已成功

WMM Mode：啟用 Wi-Fi 多媒體（WMM），是基於 IEEE 802.11e 標準的 Wi-Fi 聯盟互操作性認證，它為 IEEE 802.11 網絡提供基本的 QoS 功能，用於 RF 媒體之間的無線 QoS

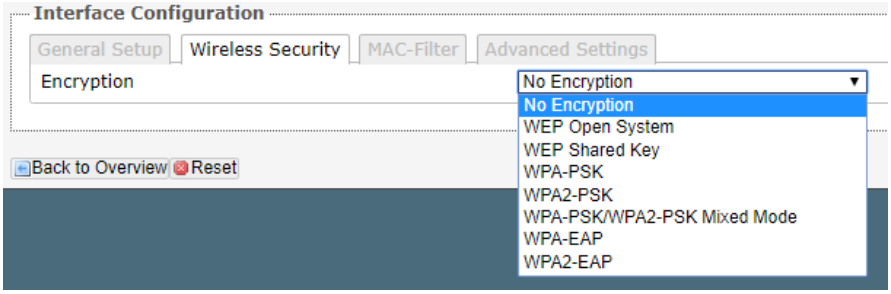


Wireless Security：Network➔Wireless➔edit➔Interface Configuration

設定 WiFi 密碼，選擇 Wireless Security 進行相關加密設定，設定完後請按 Save & Apply。

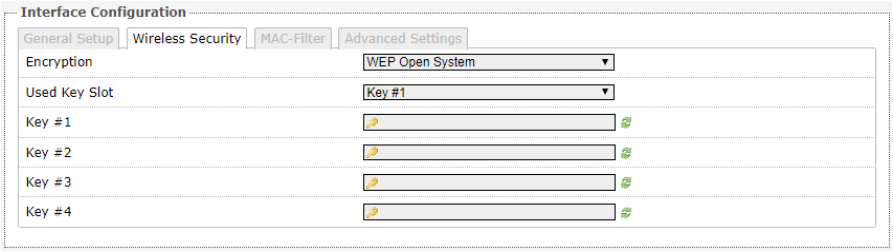
Encryption：設定無線加密方式

在無線安全方面，密碼只是成功的一半。選擇適當的加密級別同樣重要，正確的選擇將決定您的無線局域網是否是稻草屋或堡壘，大多數無線接入點都能夠選擇三種無線加密標準：有線等效保密（WEP），Wi-Fi 保護訪問（WPA）或 WPA2



No Encryption：不加密，為系統預設值

WEP：WEP 為有線等效加密（Wired Equivalent Privacy），又稱無線加密協議（Wireless Encryption Protocol），屬於為早期採用的加密技術，易破解不太建議使用，可設最少四組



WPA：WPA 具有適用於企業用戶和個人用途的離散模式，企業模式 WPA-EAP 使用更嚴格的 802.1x 身份驗證和可擴展身份驗證協議（EAP）。個人模式 WPA-PSK 使用預共享密鑰，以便在消費者和小型辦公室之間實現更簡單的實施和管理。企業模式需要使用身份驗證服務器，WPA 包括：

WPA-PSK: WPA 預共享金鑰個人模式

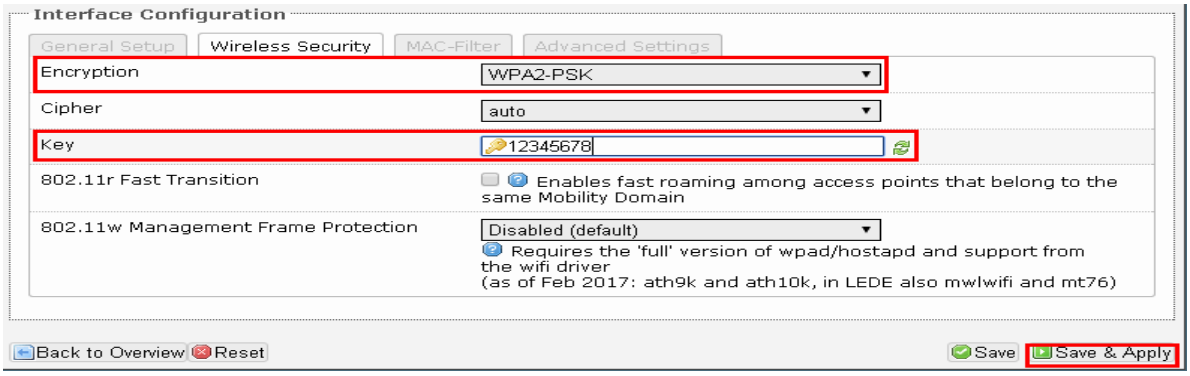
WPA2-PSK:WPA2 預共享金鑰個人模式

WPA-PSK/ WPA2-PSK Mixed Mode: WPA2 / WPA 混合模式中可以與 WPA（TKIP）和 WPA2（AES）客戶端連接

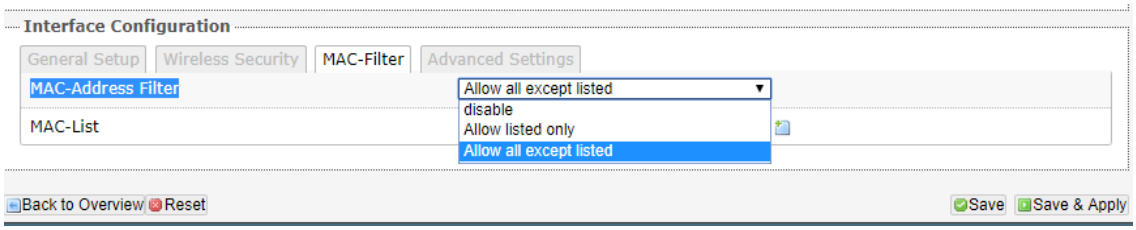
WPA-EAP: WPA 預共享金鑰企業模式

WPA2-EAP: WPA2 預共享金鑰企業模式

Cipher：設定無線加密技術，WPA 加密分為 2 種安全加密技術，分別為 TKIP 與 AES，這也是目前無線路由器所會看到的 2 種選擇方案。其中 AES 比 TKIP 採用更高級的加密技術，而如果採用 TKIP 的話，網路的傳輸速度就會被限制在 54 Mbps 以下



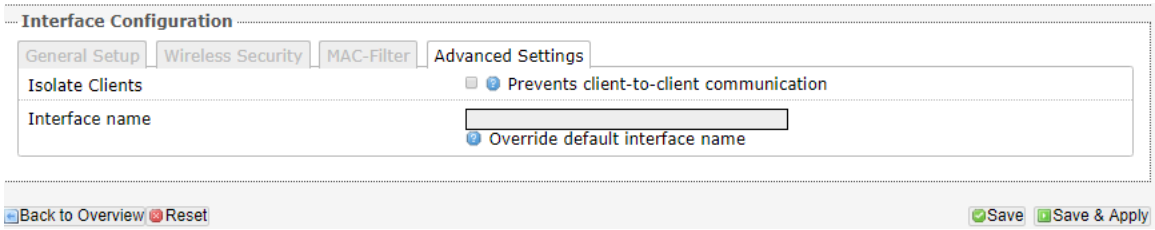
MAC-Address Filter： MAC-Address 過濾器，設定項有關閉/同意列出的 MAC 通過/除列出的 MAC 外全都同意



Advanced Settings：Network➔Wireless➔edit➔ Interface Configuration ➔Advanced Settings

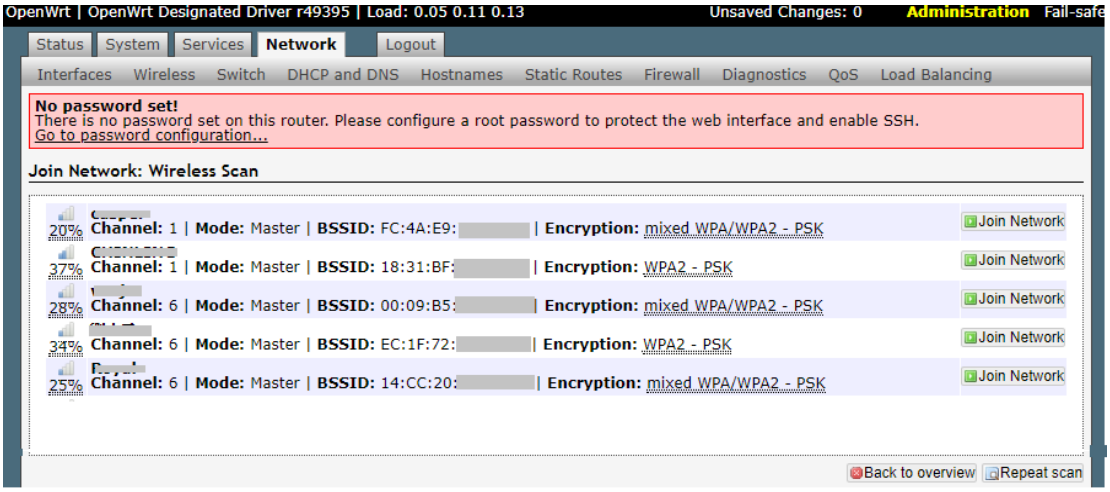
Isolate Clients：防止客戶端到客戶端的通信

Interface name：覆蓋默認接口名稱



Join Network: Wireless Scan：Network➔Wireless➔Scan

周圍的無線裝置掃描，掃描結果會顯示周圍有那些無線網路，包含訊號強度、SSID、Channel、Mode、MAC Address、加密方式等



6-3 Switch 開關設置

SWITCH 網路開關：Network➔Switch

此設備上的網絡端口可以組合到多個 VLAN，電腦可以在這些 VLAN 之間直接相互通信。

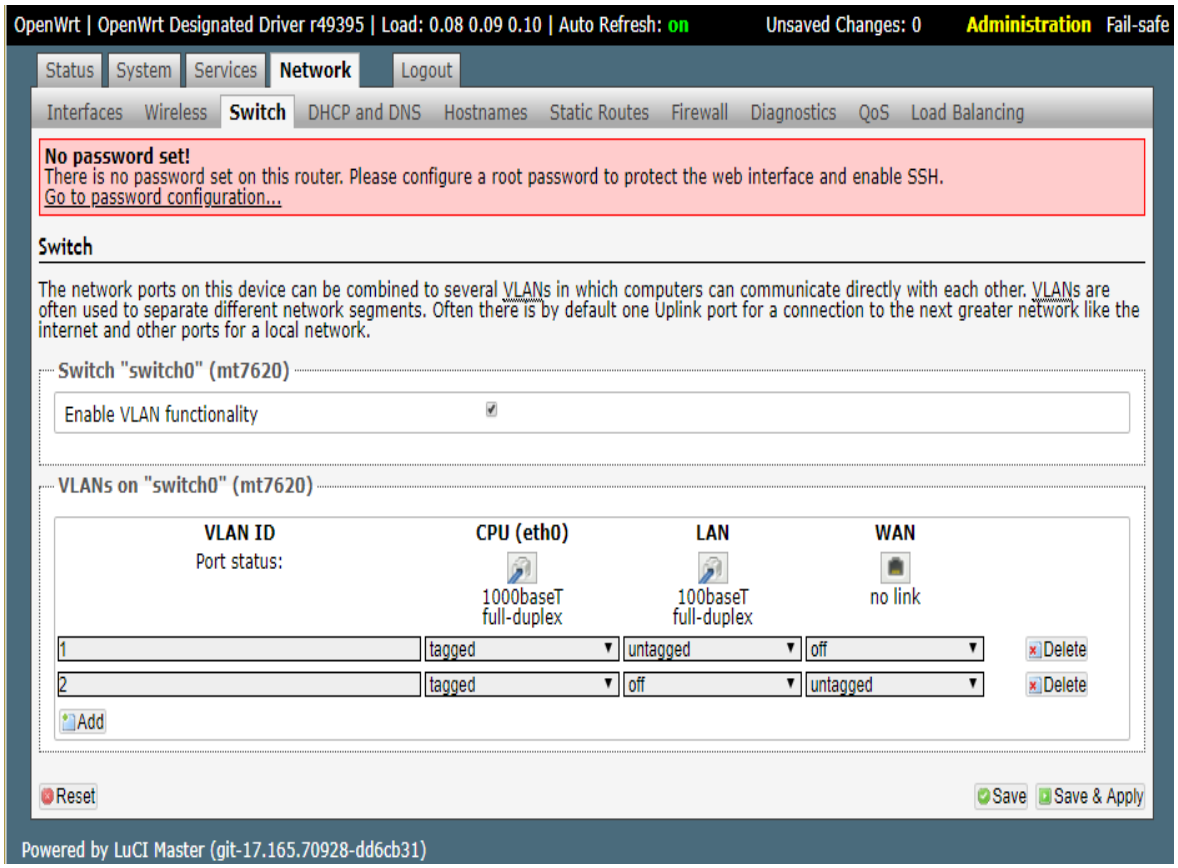
VLAN 通常用於分隔不同的網段，通常默認情況下有一個上行鏈路端口用於連接到下一個更大的網絡，如互聯網和本地網絡的其他端口。

Enable VLAN functionality：勾選啟用此功能

Add：增加新的 VLAN1 設定

Delete：刪除 VLAN1 設定

Save / Save & Apply：儲存及套用



6-4 DHCP & DNS

DHCP & DNS：Network➔DHCP and DNS

是設定 DHCP 服務器和 DNS 透過 NAT 轉發通過防火牆

6-4.1 General setup 一般設置

Domain required：勾選表示不要在沒有 DNS 名稱的情況下轉發 DNS 請求

Authoritative：勾選表示這是本地網絡中唯一的 DHCP

Local server：規範與此域匹配的名稱永遠不會轉發，只能從 DHCP 或主機文件中解析

Local domain：附加到 DHCP 名稱和主機文件條目

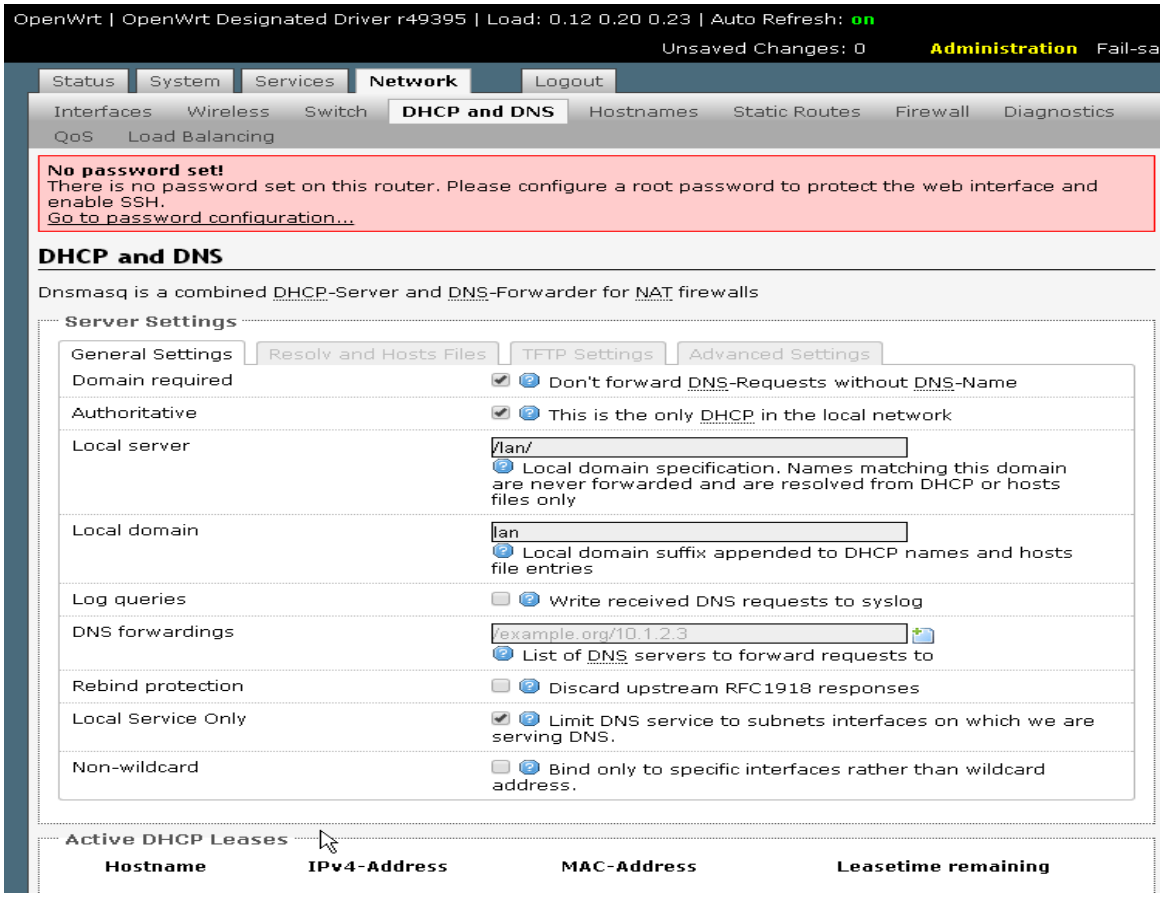
Log queries：是否將收到的 DNS 請求寫入 syslog

DNS forwardings：請求轉發到的 DNS 服務器列表

Rebind protection：丟棄上層 RFC1918 回應重新綁定保護

Local Service Only：限制 DNS 服務只提供給 subnets interfaces

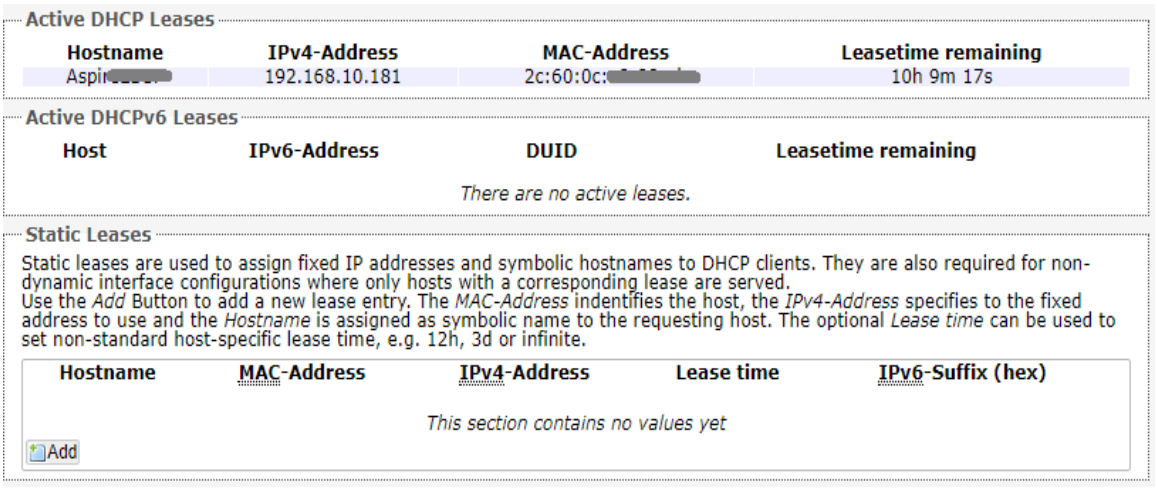
Non-wildcard：僅綁定到特定接口



Active DHCP Leases：顯示 ipv4 現已取得 DHCP 租約的電腦名稱、IP、MAC、租約時間

Active DHCPv6 Leases：顯示 ipv6 現已取得 DHCP 租約的電腦名稱、IP、MAC、租約時間

Static Leases：顯示靜態租約，為 DHCP 客戶端分配固定 IP 地址和主機名稱



6-4.2 Resolv and Hosts Files 解析和託管文件

Use /etc/ethers：勾選讀取 / etc / ethers 以配置 DHCP 服務器

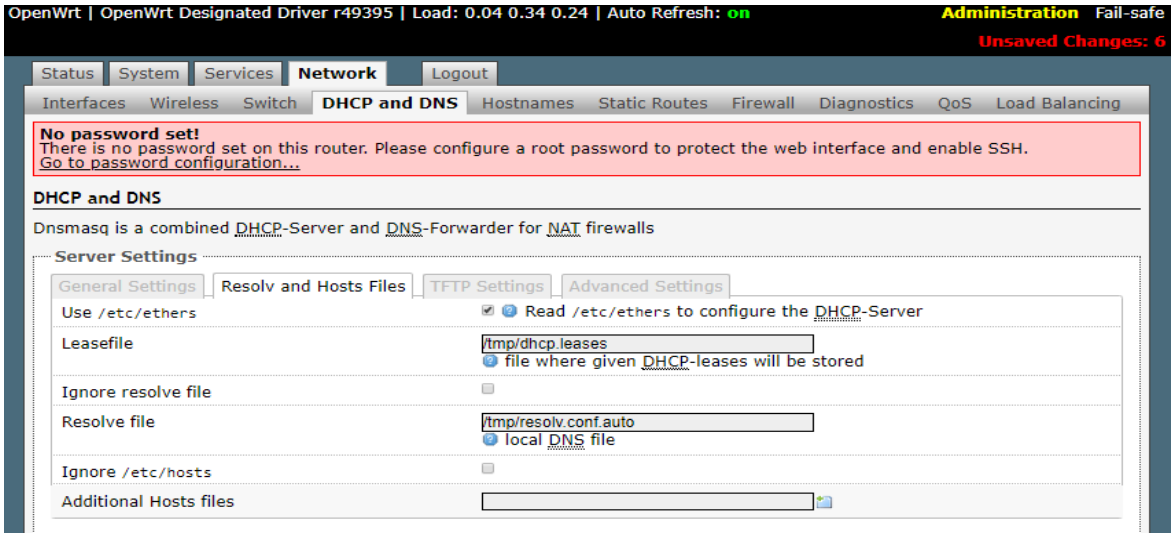
Leasefile：將存儲存給定 DHCP 租約的文件

Ignore resolve file：勾選則忽略解析文件

Resolve file：本地 DNS 解析文件所在位置

Ignore /etc/hosts：忽略/ etc / hosts

Additional Hosts files：設定其他主機文件



6-4.3 TFTP Settings TFTP 設置：略

6-4.4 Advanced Settings 高級設置

Suppress logging：設定是否禁止記錄這些協定日常的日誌

Allocate IP sequentially：設定是否從最低可用地址開始按順序分配 IP 地址

Filter private：設定是否過濾私密，不要轉發從本地網絡來的反向查找

Localise queries：設定是否使用本地化查詢，如果有多個 IP 可用，則根據請求的子網本地化主機名

Expand hosts：設定是否擴充主機，增加從 hosts 文件提供的名稱

No negative cache：沒有負面緩存，不要緩存否定回答，例如 對於不存在的域

Additional servers file：其他服務器文件，此文件可能包含“server = / domain / 1.2.3.4”或“server = 1.2.3.4”等行，用於特定於域或完整的上層 DNS 服務器。

Strict order：設定是否 DNS 服務器將在 resolvfile 的順序進行查詢

Bogus NX Domain Override：設定是否提供虛假 NX 域結果的主機列表

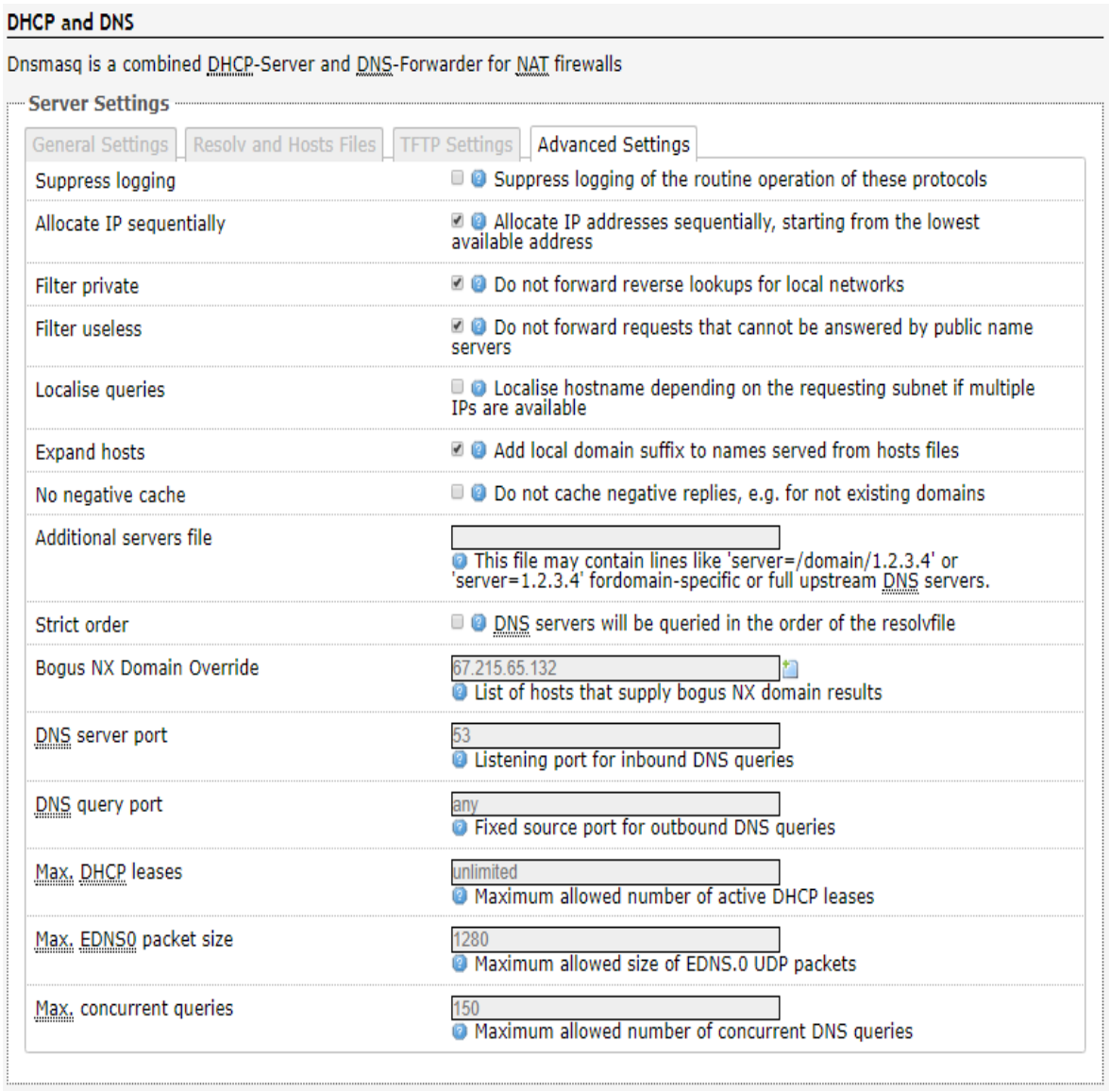
DNS server port：設定 DNS 伺服器連接埠

DNS query port：設定 DNS 伺服器查詢埠

Max. DHCP leases：設定 DHCP 最大租約

Max. EDNS0 packet size：設定 DHCP 最大允計的 UDP 封包大小

Max. concurrent queries：設定允許發送的最大 DNS 查詢數

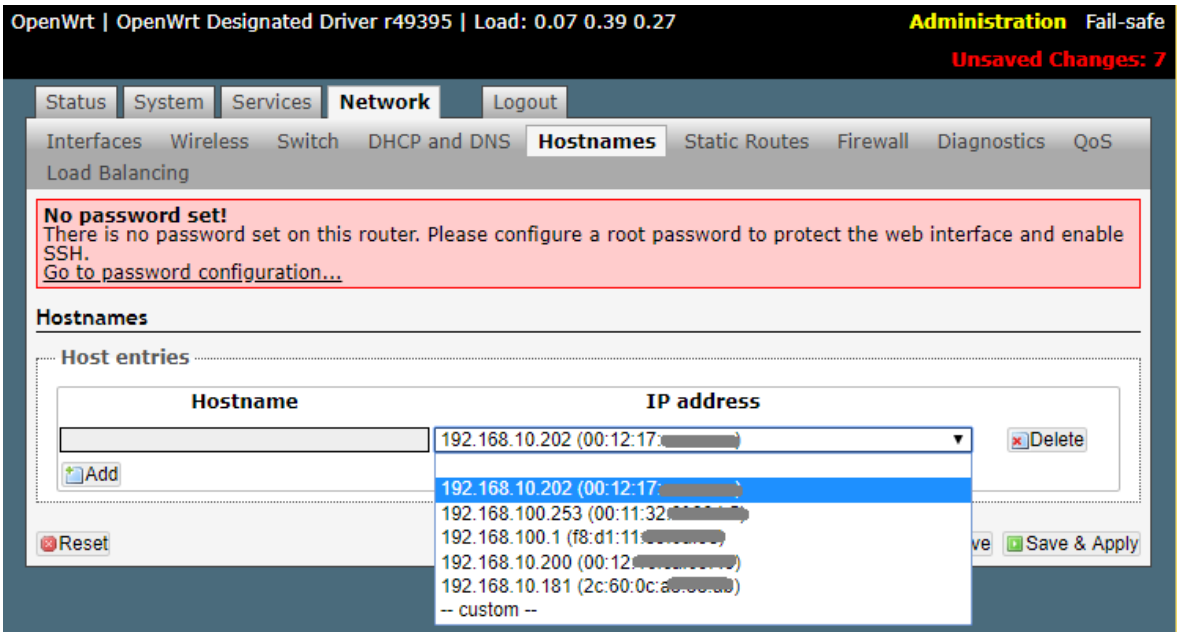


6-5 Hostnames 主機名稱

Hostnames 主機名：Network➔Hostnames

設定LAN 端使用者之主機名稱

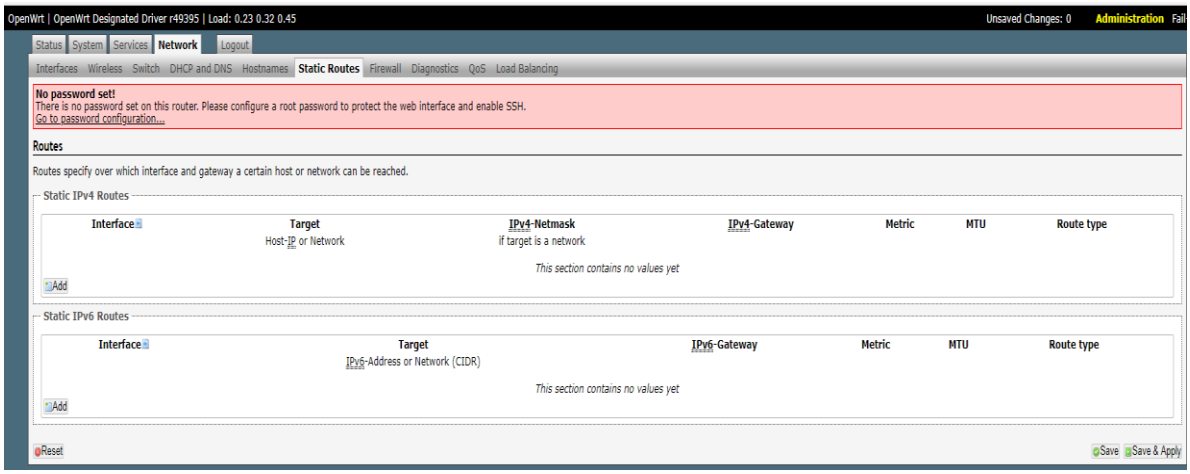
可自行新增主機名稱給 DHCP　　租約下或自定之 IP 位置



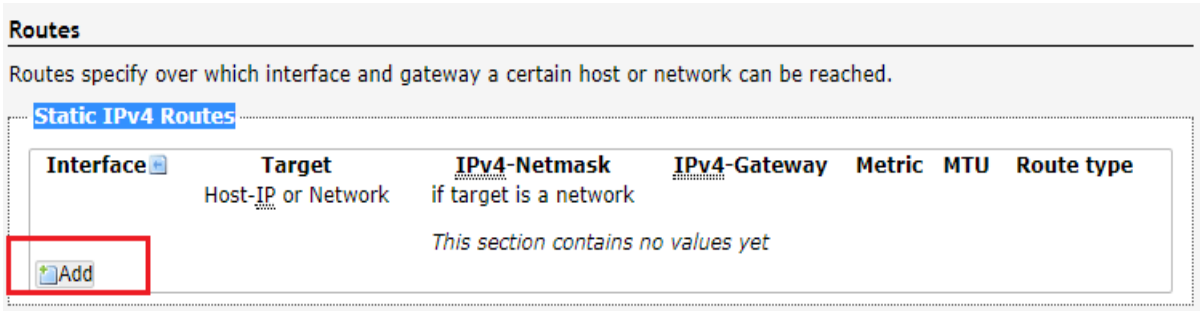
6-6 Static Routes 靜態路由

Static Routes 靜態路由：Network➔Static Routes

顯示及設定路由指定可以到達某個主機或網絡的接口（interface）和通訊閘（gateway）

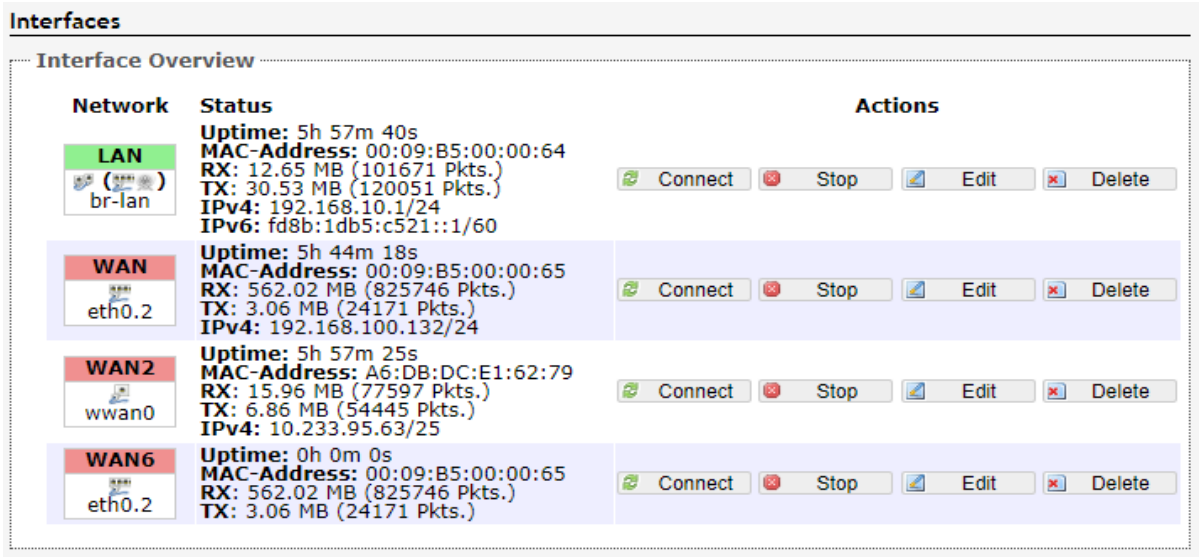


Add Static IPv4 Routes：新增一 IPv4 靜態路由

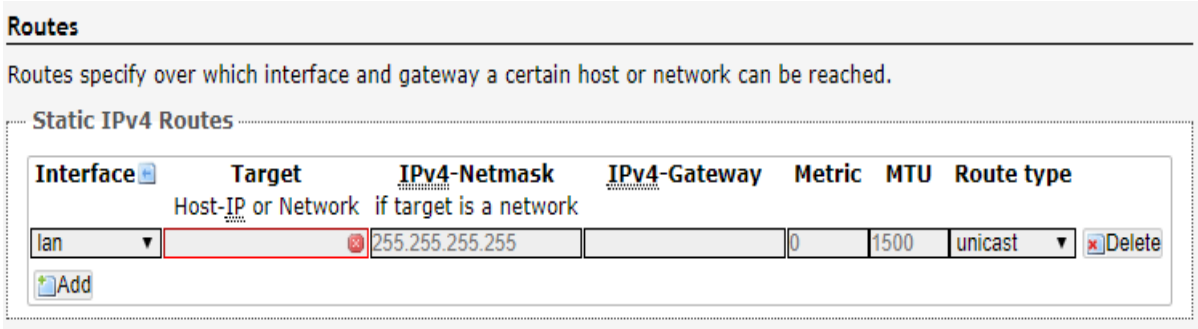


Interface：選擇要新增加的靜態路由是那個網路界面

接口（interface）所指如下圖所示



Tarage：新增目標，指定主機 IP or 網路
IPv4-Netmask：指定一個子網路遮罩
IPv4-Gateway：指定一個閘道器
Metric：權值，預設權值為 0
MTU：最大傳輸單位(Maximum Transmission Unit) 一般的網路介面預設值 1500
Route type：指定路由類型



6-7 Firewall 防火牆

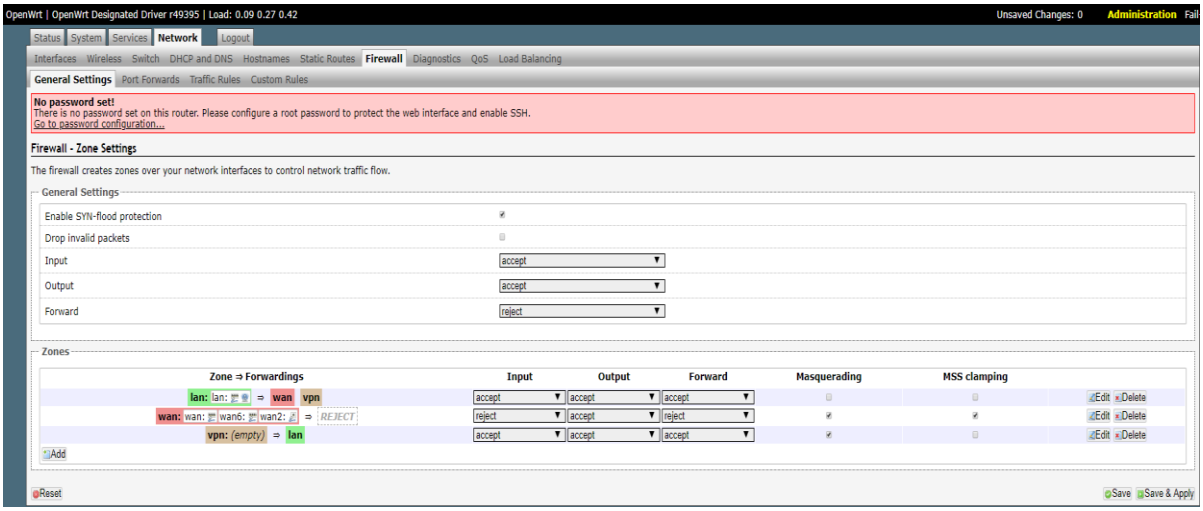
Firewall 防火牆：Network➔Firewall

設定網路的連入/連出及轉發，包含 Port forwarding/Traffic Rules/Custom Rules

6-7.1 General setup 一般設置

Enable SYN-flood protection：設定是否啟用 SYN-flood 保護
是一種阻斷服務攻擊，起因於攻擊者傳送一系列的 SYN 請求到目標系統，企圖消耗服務器資源，使系統無法響應合法的通信請求

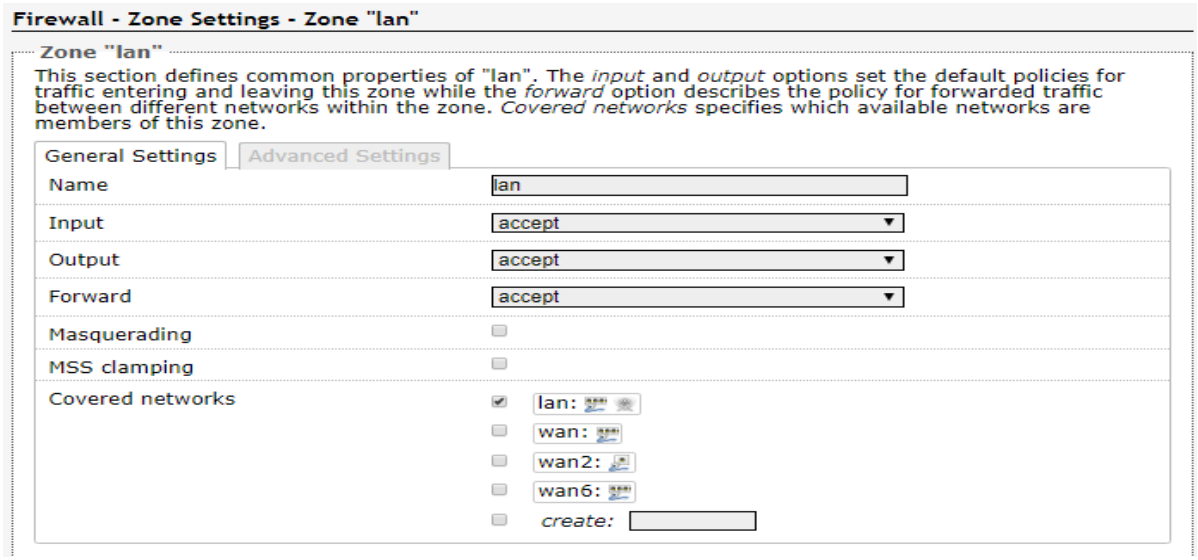
Drop invalid packets：設定是否丟棄無效數據包(封包)
Input：對進入之數據包做設定，丟棄/接受/拒絕
Output：對出去之數據包做設定，丟棄/接受/拒絕
Forward：對轉發之數據包做設定，丟棄/接受/拒絕



Masquerading：設定偽裝

MSS clamping：設定 MSS 箝位

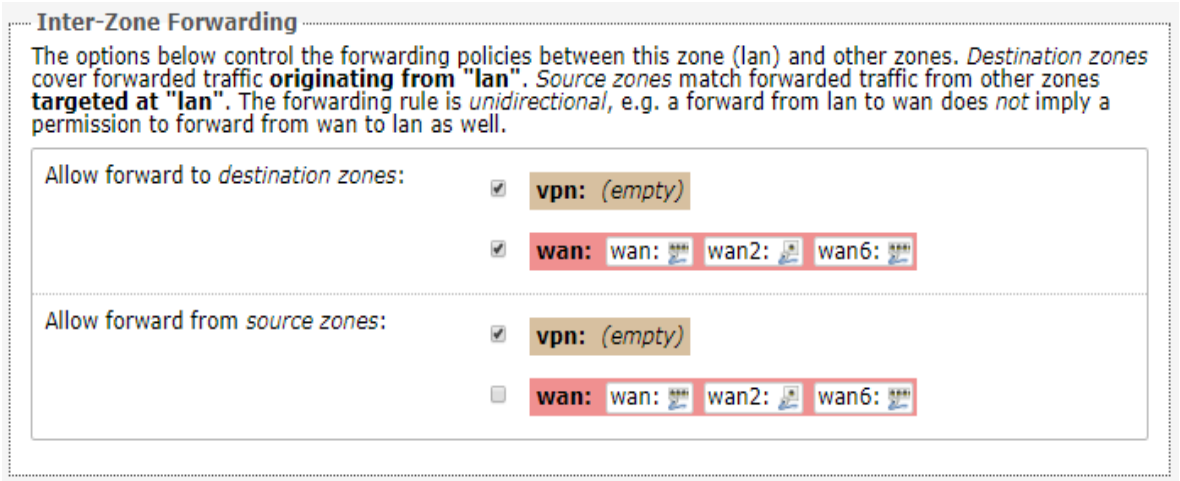
Covered networks：設定涵蓋那些網絡



Inter-Zone Forwarding 區域間轉發

Allow forward to destination zones: 允許轉發到目標區域

Allow forward from source zones: 允許自來源區域轉發



6-7.2 Advanced Settings 高級設置

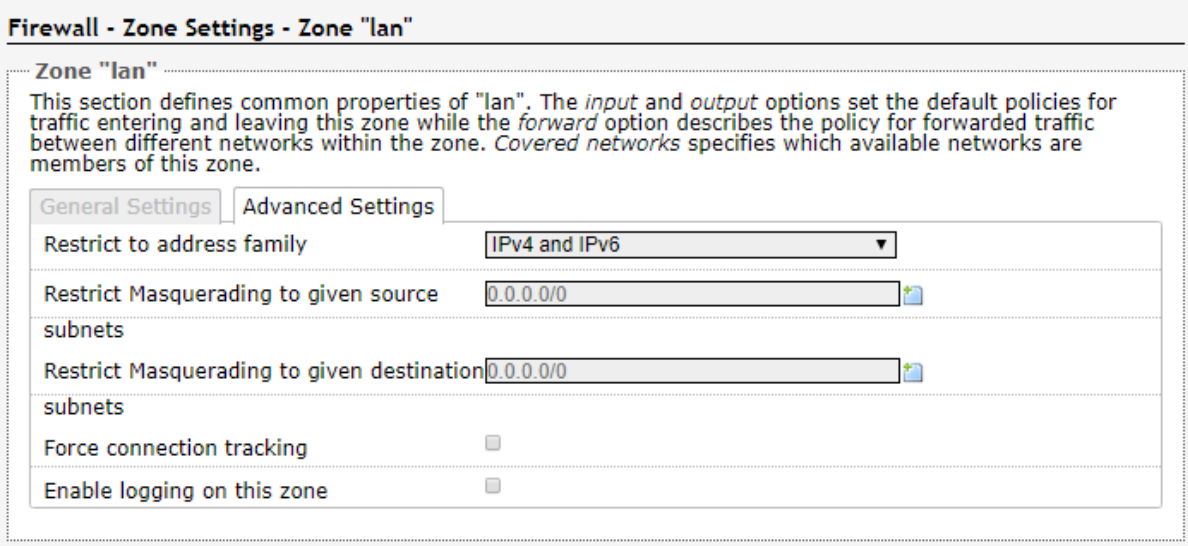
Restrict to address family：設定選擇限制位走址類型為 IPv4 / IPv6 / 二者皆是

Restrict Masquerading to given source：限制偽裝來源 IP

Restrict Masquerading to given destination：限制偽裝目的地 IP

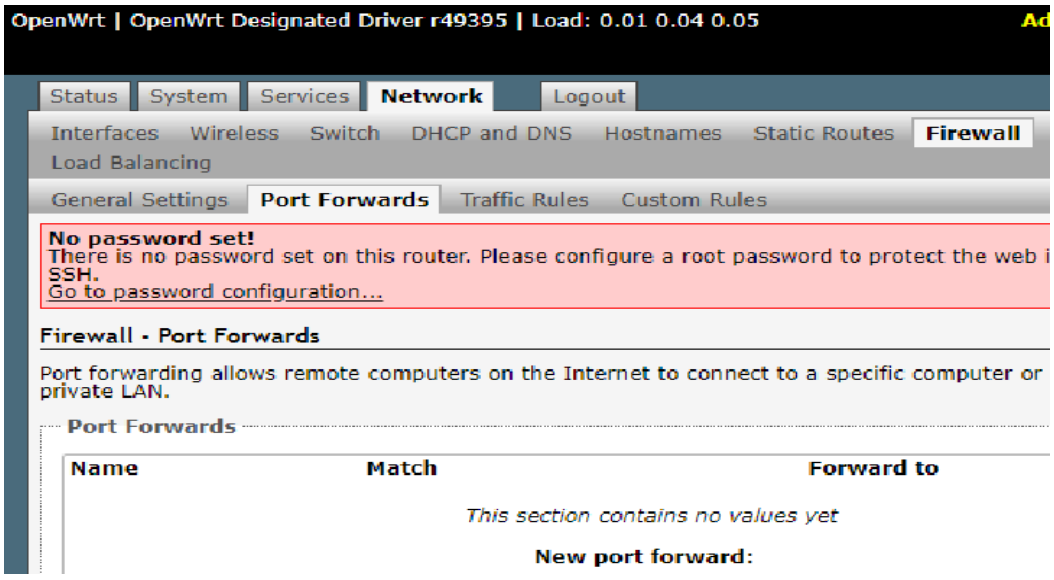
Force connection tracking：強制連接跟踪

Enable logging on this zone：啟用此區域的日誌記錄



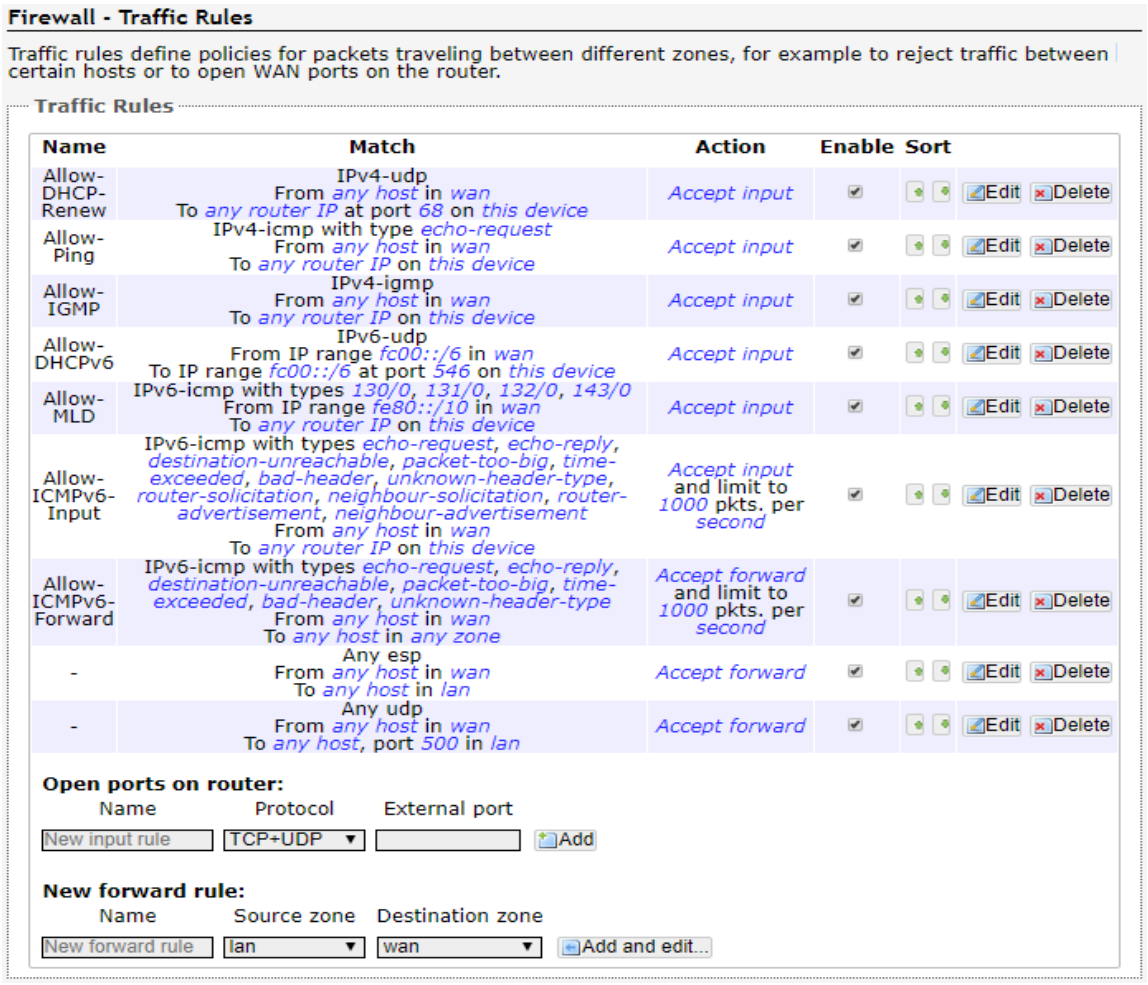
6-7.3 Port Forwards 埠轉發

允許 Internet 上的遠程計算機連接到專用 LAN 內的特定計算機或服務，最常用於通過將通信的目標 IP 地址和端口號重新映射到駐留在網關（外部網絡）相對端的主機上的受保護或偽裝（內部）網絡上的主機上進行服務



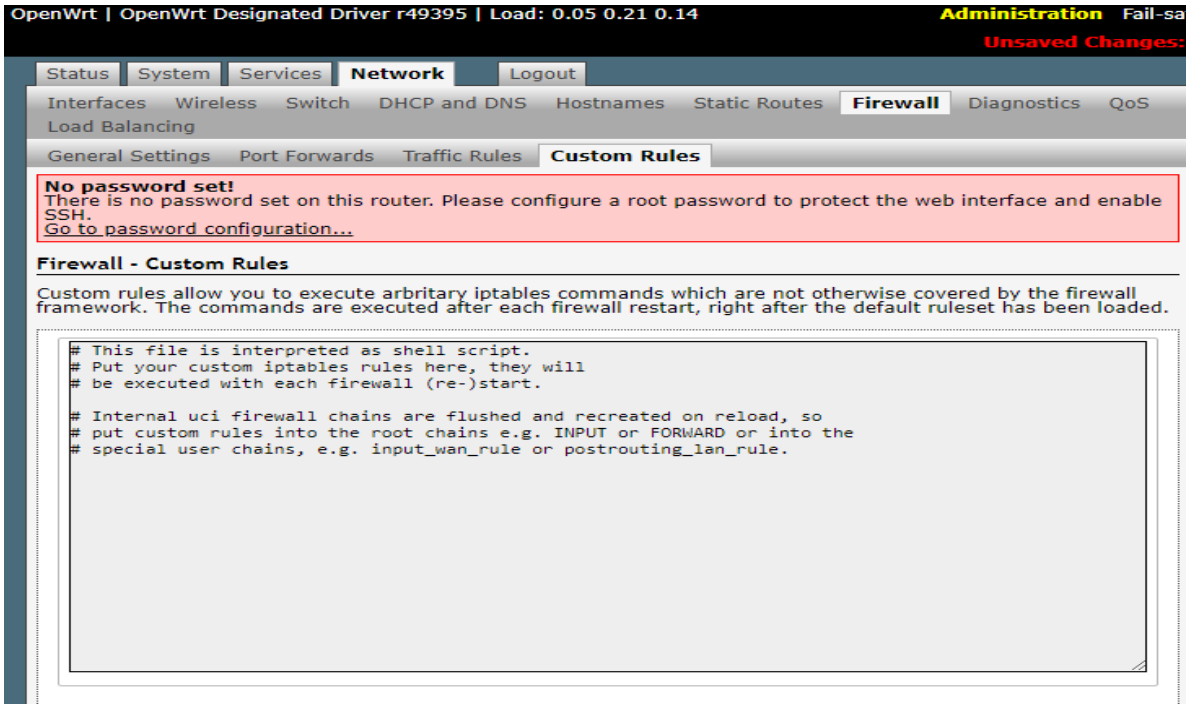
6-7.4 Traffic Rules 流量傳送規則

流量傳送規則定義在不同區域之間傳輸的數據包的策略，例如拒絕某些主機之間的流量或打開路由器上的 WAN 端口。



6-7.5 Custom Rules 自定義規則

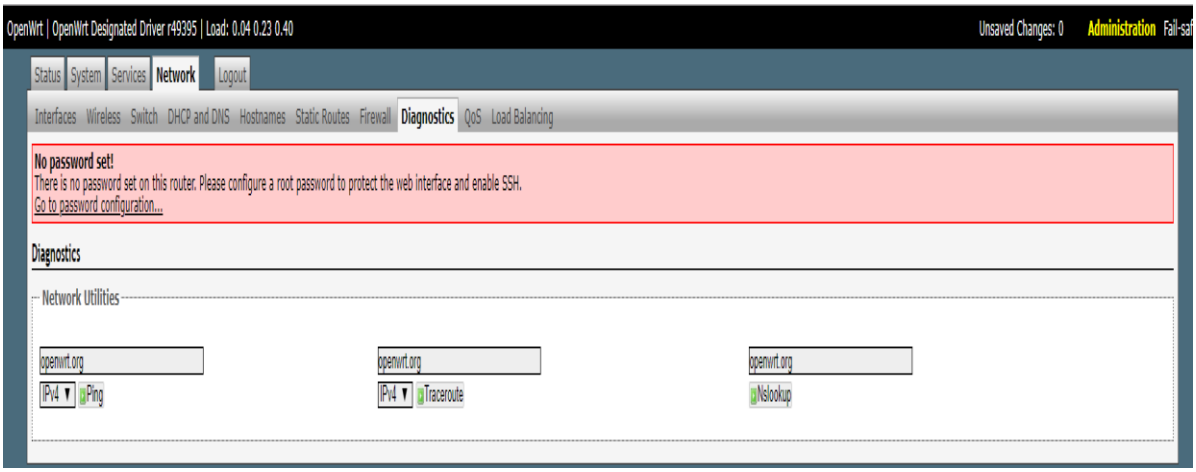
自定義規則允許您執行防火牆框架未涵蓋的 arbritary iptables 命令，在每個防火牆重新啟動後，在加載默認規則集後立即執行這些命令。



6-8 Diagnostics 診斷

Diagnostics 診斷：Network➔Diagnostics

可設置遠端主機透過網路工具（Ping /Traceroute/Nslookup）來診斷網狀況



Ping

```
PING openwrt.org (139.59.209.225): 56 data bytes
64 bytes from 139.59.209.225: seq=0 ttl=44 time=270.137 ms
64 bytes from 139.59.209.225: seq=1 ttl=44 time=269.737 ms
64 bytes from 139.59.209.225: seq=2 ttl=44 time=286.656 ms
64 bytes from 139.59.209.225: seq=3 ttl=44 time=267.156 ms
64 bytes from 139.59.209.225: seq=4 ttl=44 time=266.836 ms

--- openwrt.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 266.836/272.104/286.656 ms
```

Traceroute

```
traceroute to openwrt.org (139.59.209.225), 30 hops max, 38 byte packets
 1  *
 2  10.156.65.41  14.580 ms
 3  10.156.67.103  14.679 ms
 4  10.156.67.113  13.960 ms
 5  210.65.126.162  19.320 ms
 6  220.128.3.190  23.340 ms
 7  220.128.26.77  15.399 ms
 8  220.128.7.41  19.300 ms
 9  220.128.7.45  21.820 ms
10  80.231.200.78  241.897 ms
11  80.231.200.78  378.435 ms
12  195.219.87.18  247.556 ms
13  195.219.50.90  272.657 ms
14  139.59.209.225  275.136 ms
```

Nslookup

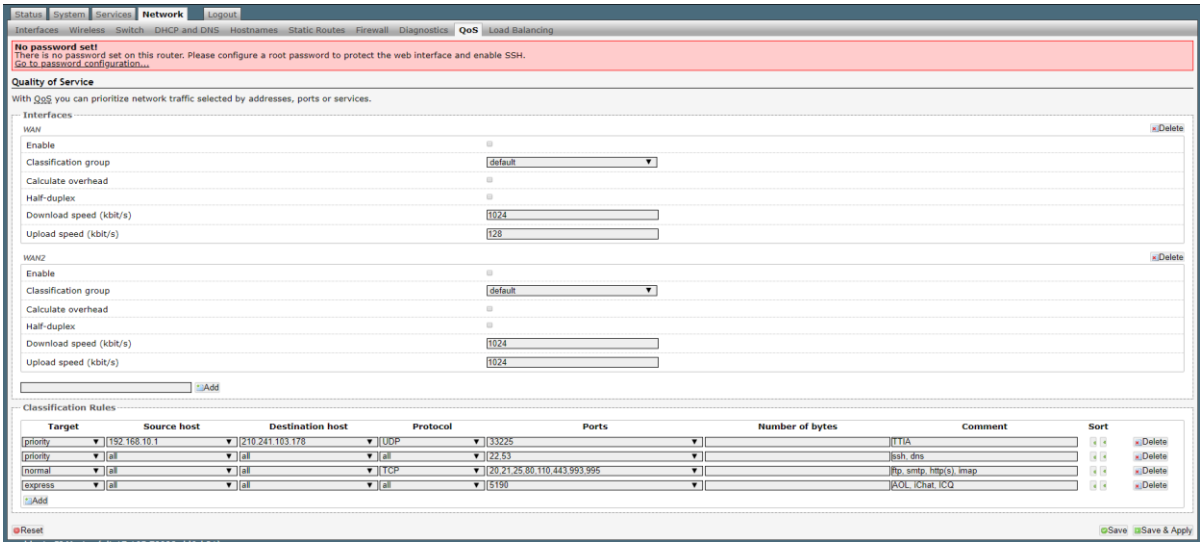
```
nslookup: can't resolve '(null)': Name does not resolve

Name:      openwrt.org
Address 1: 139.59.209.225 wiki-01.infra.lede-project.org
Address 2: 2a03:b0c0:3:d0::1af1:1 wiki-01.infra.lede-project.org
```

6-9 QoS 服務質量

QoS 服務質量(流量控制)：Network➔QoS

QoS 的英文全稱為 Quality of Service，中文名為服務質量。QoS 是網路的一種安全機制，是用來解決網路延遲和阻塞等問題的一種技術。在正常情況下，如果網路只用於特定的無時間限制的應用系統，並不需要 QoS，如 Web 應用或 E-mail 設置等，但是對關鍵應用和多媒體應用就十分必要。當網路過載或擁塞時，QoS 能確保重要業務量不受延遲或丟棄，同時保證網路的高效運行，進行帶寬限制、帶寬保證、優先順序控制，從而使關鍵業務能得到充分的服務質量保證。

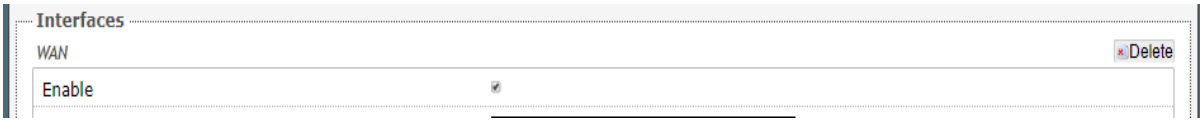


用戶可針對 interfaces(WAN/WAN2)自定義 QoS 規則

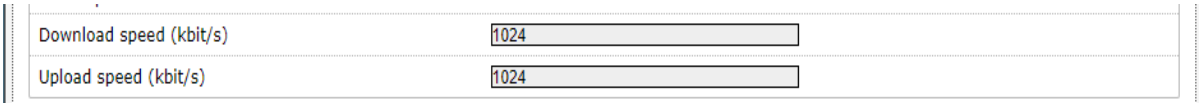
QoS 為您提供了進階的配置項，包括端口，協議和傳輸。QoS 目標類別的切換可為每個客戶端設置優先 Priority/快速 Express/正常 Nomal/低 Low 等級之設置。

[如何設定 QoS]

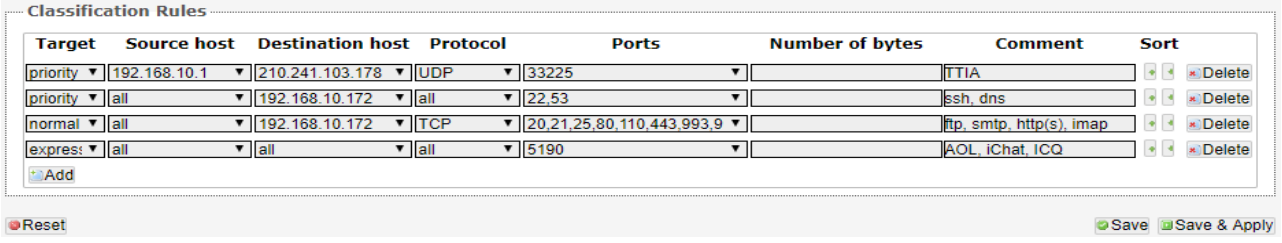
1. 啟用 QoS



2. 設定限制您的上傳、下載的頻寬(kbit/s)



3. 自定義分類規則，用戶可依优先等級及端口，協議，來源，目的，傳輸來自行定義流量控制



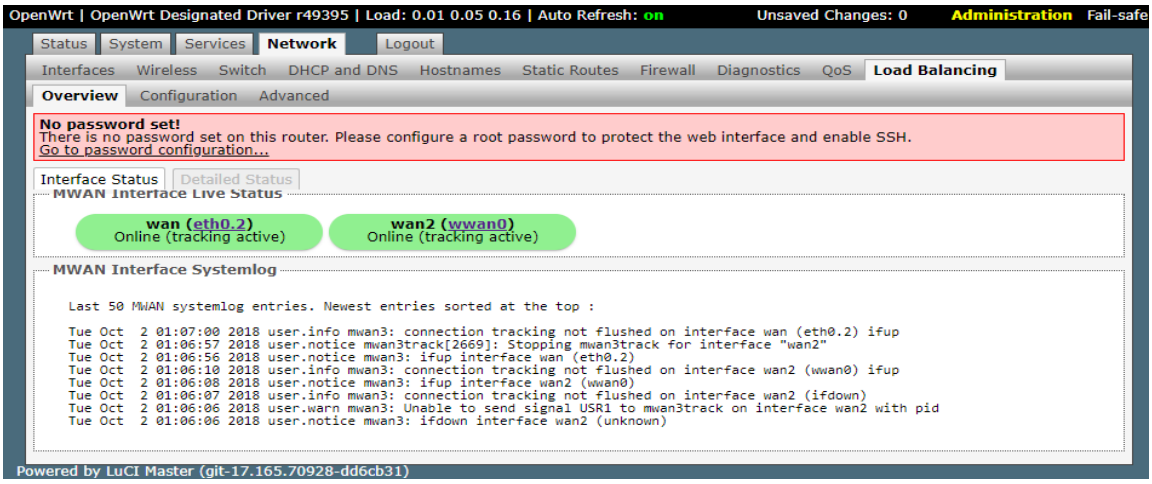
4. 點選[儲存&應用](Save & Apply)來儲存設定。

6-A Load Balancing 負載平衡

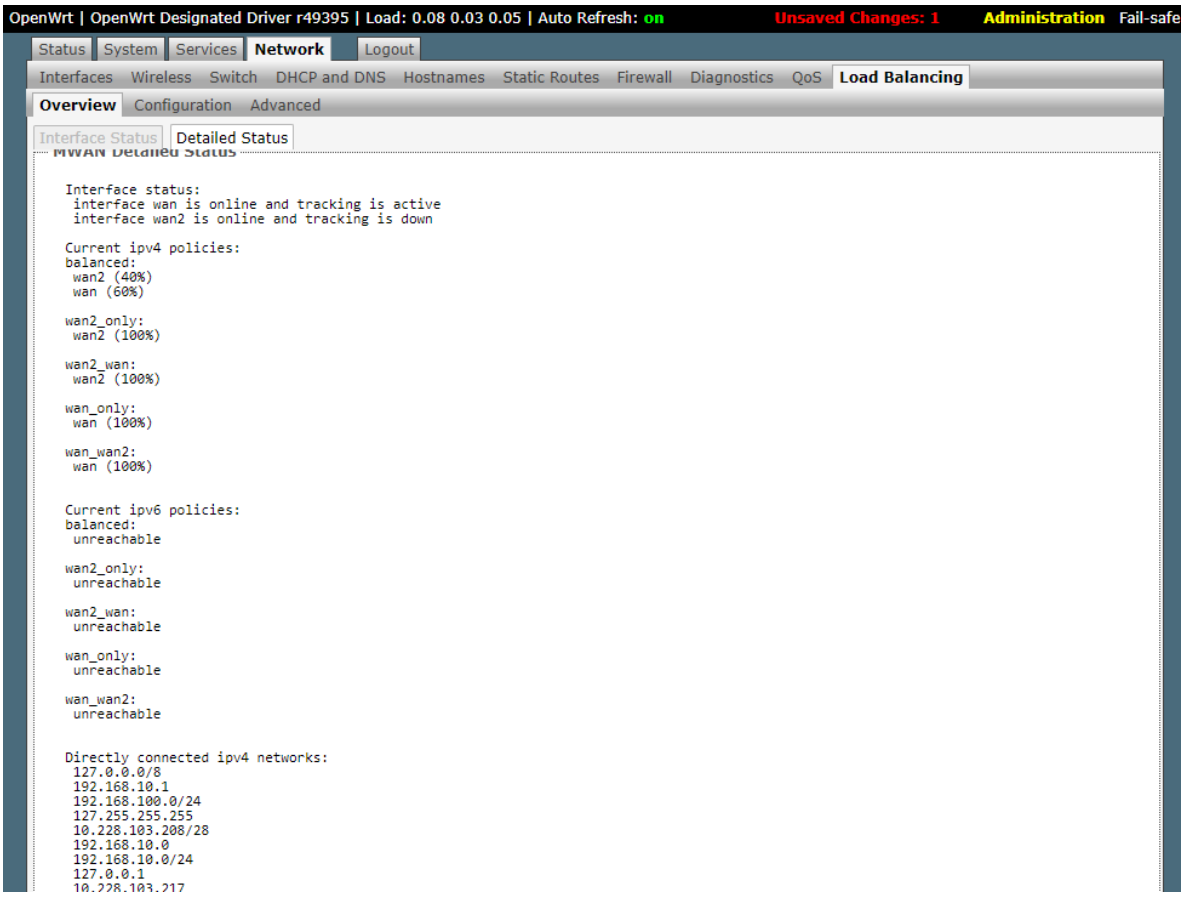
Load Balancing 負載平衡：Network➔Load Balancing

WAN Load Balance，當 Router 對外線路有兩種（Wlan/4G）以上的時候，WLB 就可以擔負起網際網路（Internet）與內部網路（Intranet）之間多條連外線路流量平衡的工作，有助於調整、控制封包的進出順序。可以在使用多條線路的情況下動態分配內網的數據流量，動態的實現帶寬匯聚的功能。

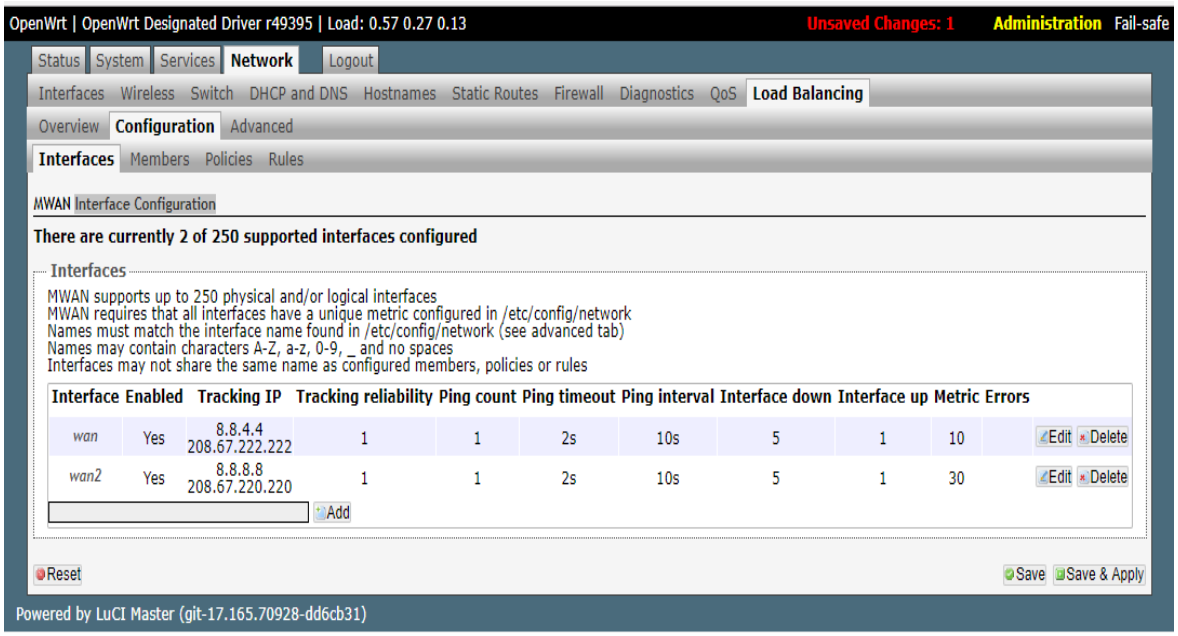
界面即時狀態 Interface Live Status：



詳細狀態 Detailed Status：

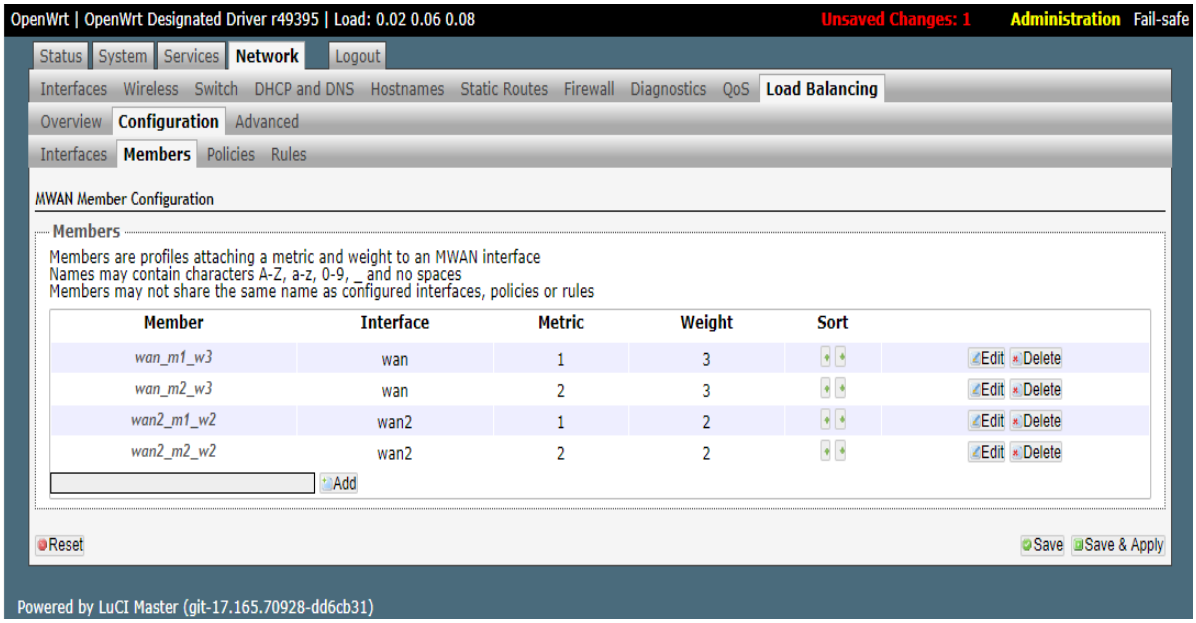


界面接口配置 Interface Configuration：最多支持 250 個物理和/或邏輯接口



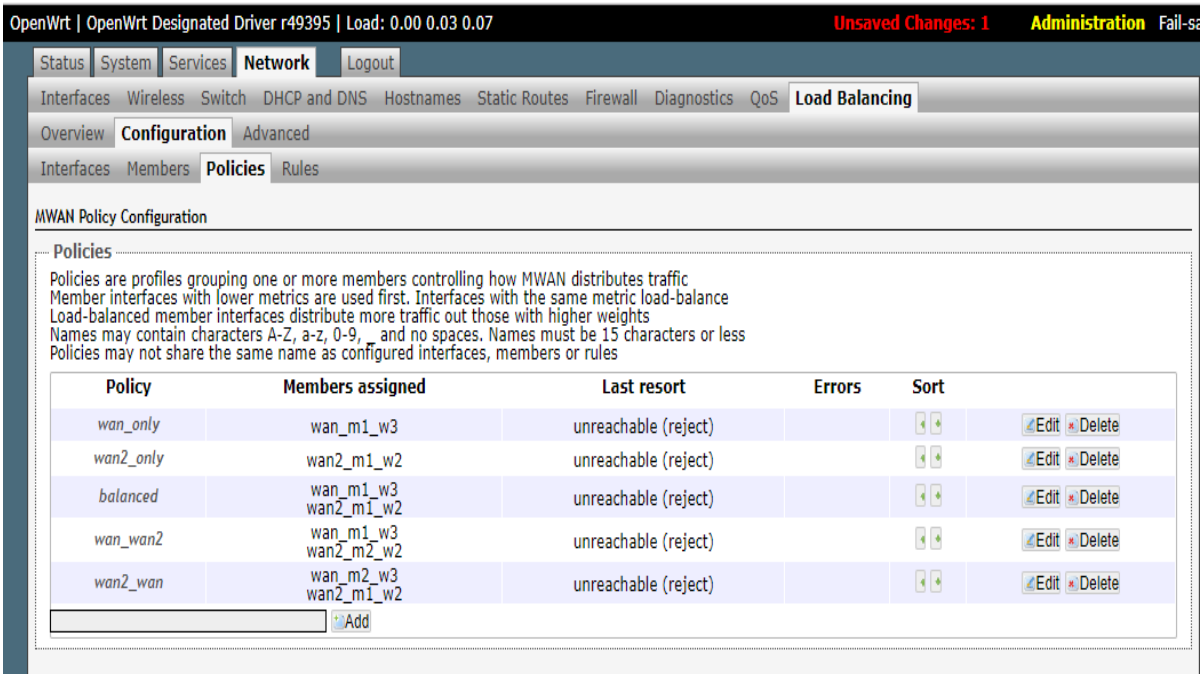
會員配置 Member Configuration：

是將 Metric 和 Weight 附加到 MWAN 接口的配置



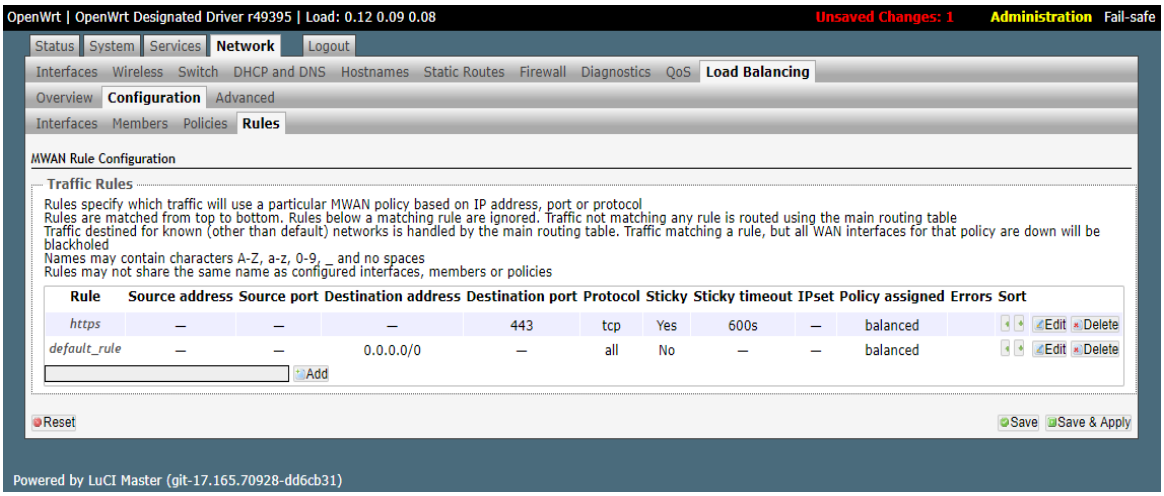
策略配置 Policy Configuration：

是對控制 MWAN 如何分配流量的一個或多個成員進行分組的配置



規則配置 Rule Configuration：

指定哪些流量將使用於 IP 地址，端口或協議的特定 MWAN 策略



高級設置 advanced：**＊本部分非專業人員，建議勿修改＊**

Hotplug Script

本部分允許您修改/etc/hotplug.d/iface/16-mwancustom 的內容

基於接口 ifup 或 ifdown hotplug 事件運行系統命令

MWAN Config

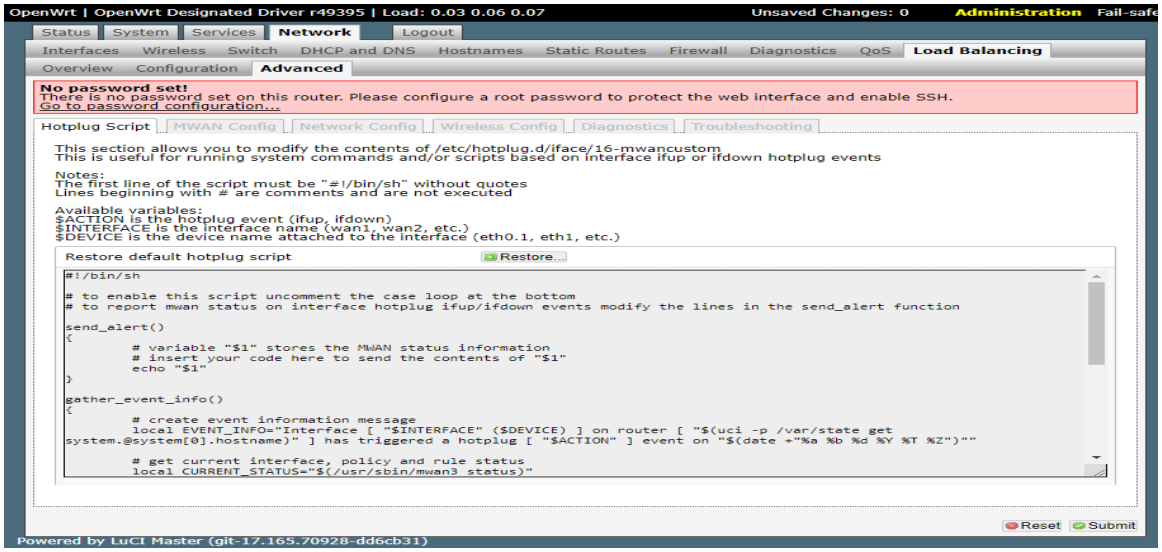
本部分允許您修改/ etc / config / mwan3 的內容

Network Config

本部分允許您修改/ etc / config / network 的內容

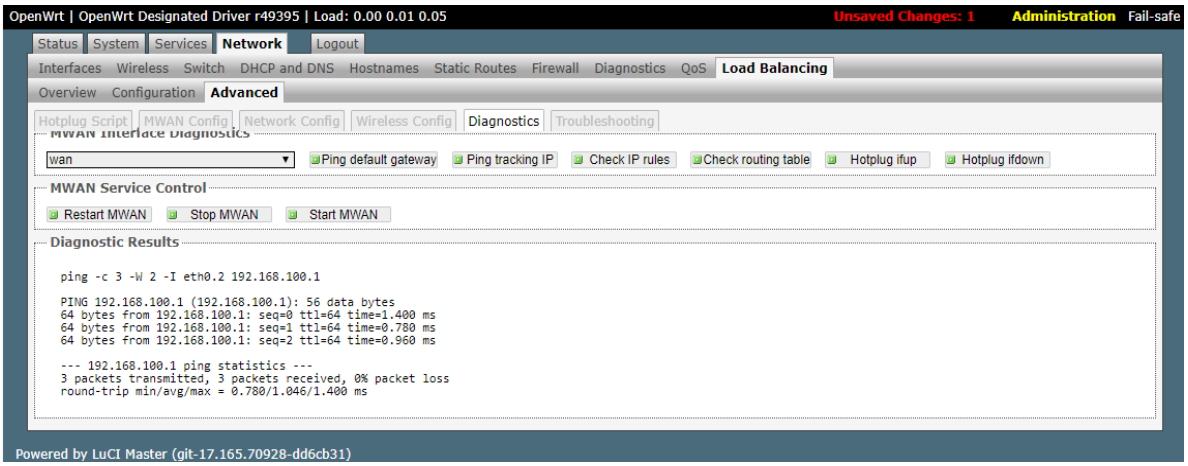
Wireless Config

本部分允許您修改/etc/config/wireless 的內容

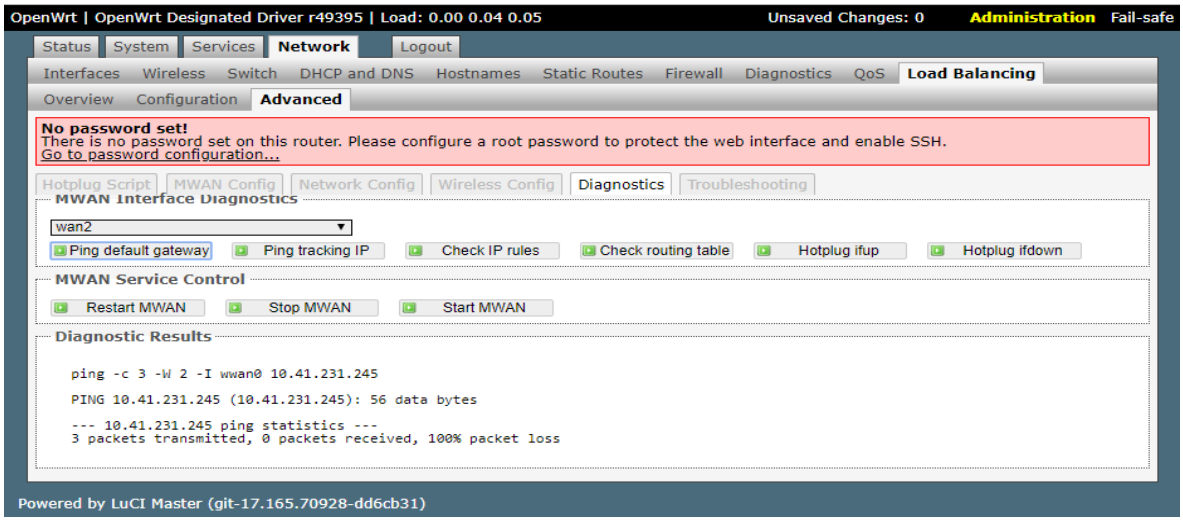


界面接口診斷 Interface Diagnostics：

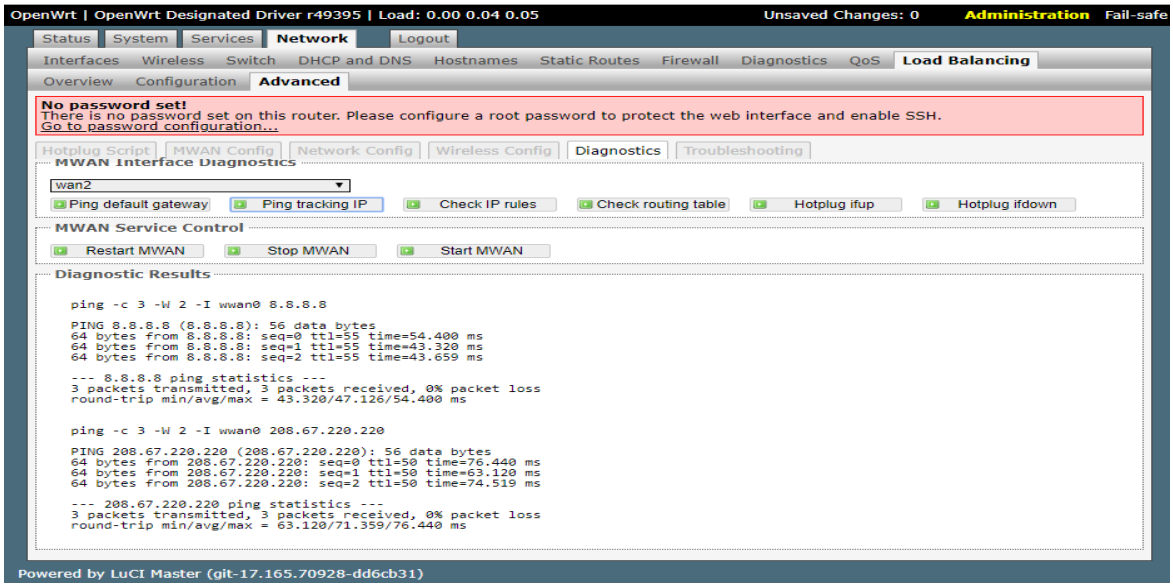
界面接口診斷包含（Ping default gateway/ Ping tracking IP/ Check IP nles/ Check routingtable 等等…）及界面服務的控制



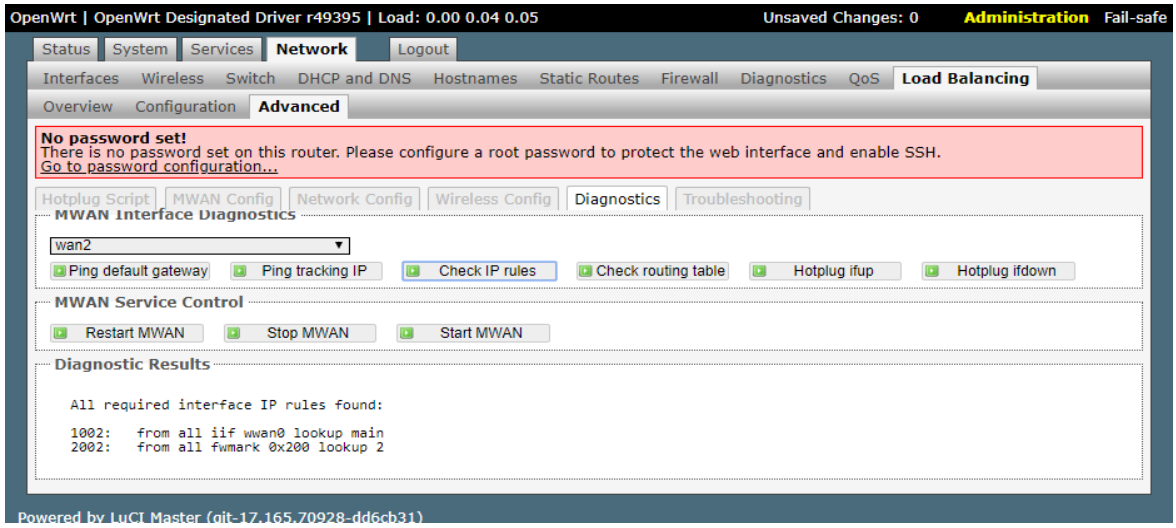
Ping default gateway



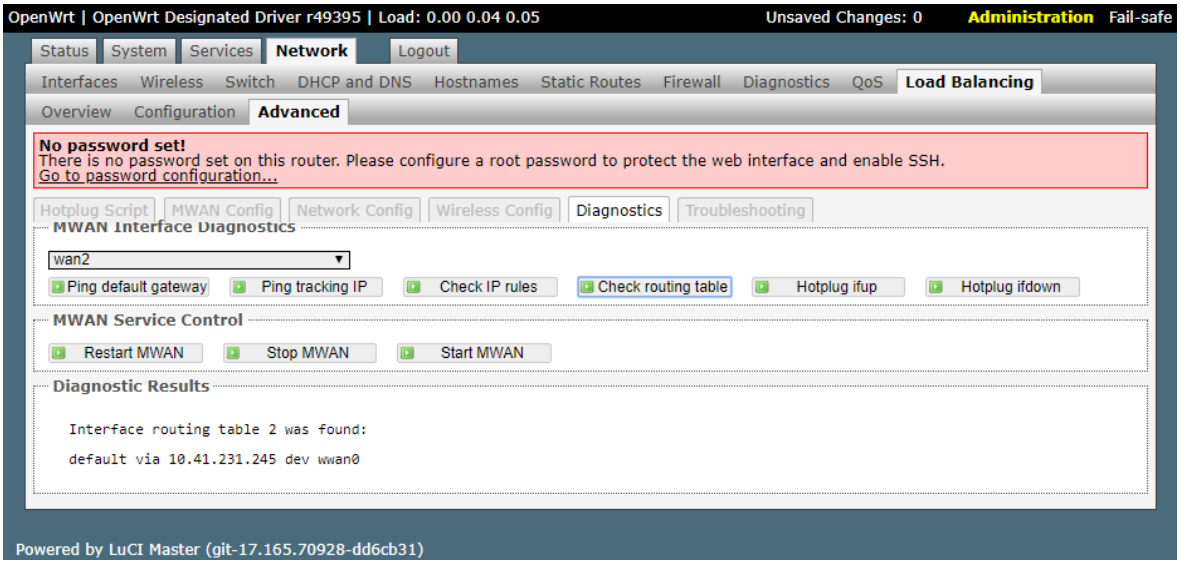
Ping tracking IP



Check IP nles

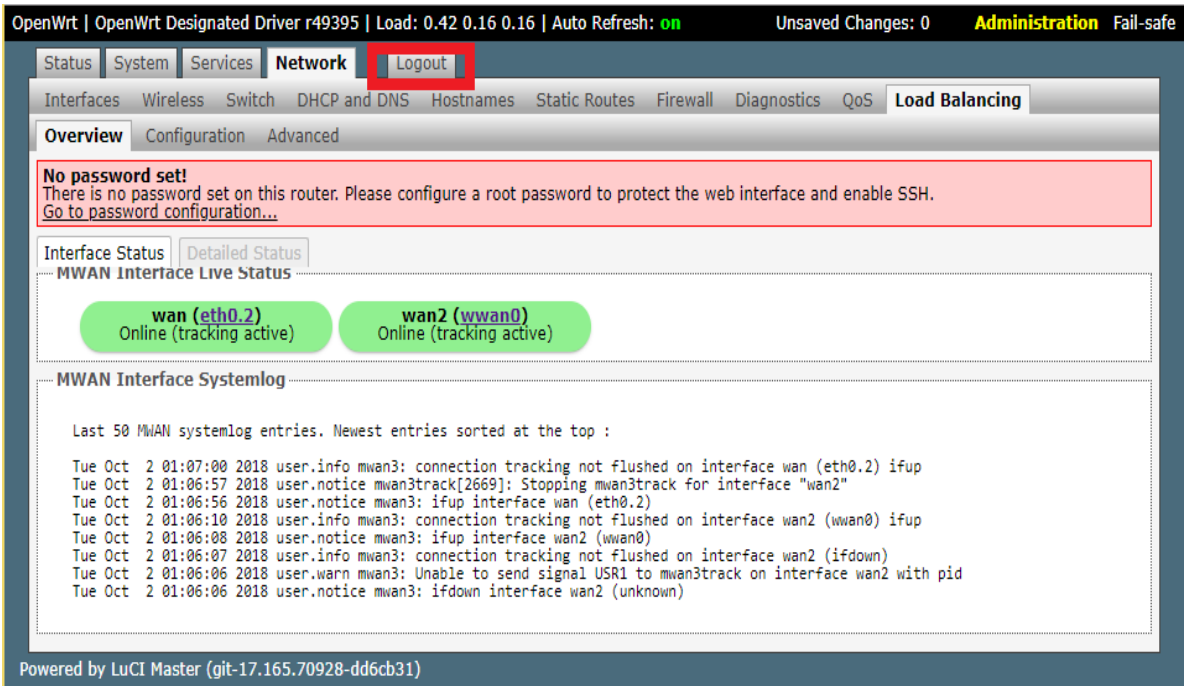


Check routingtable



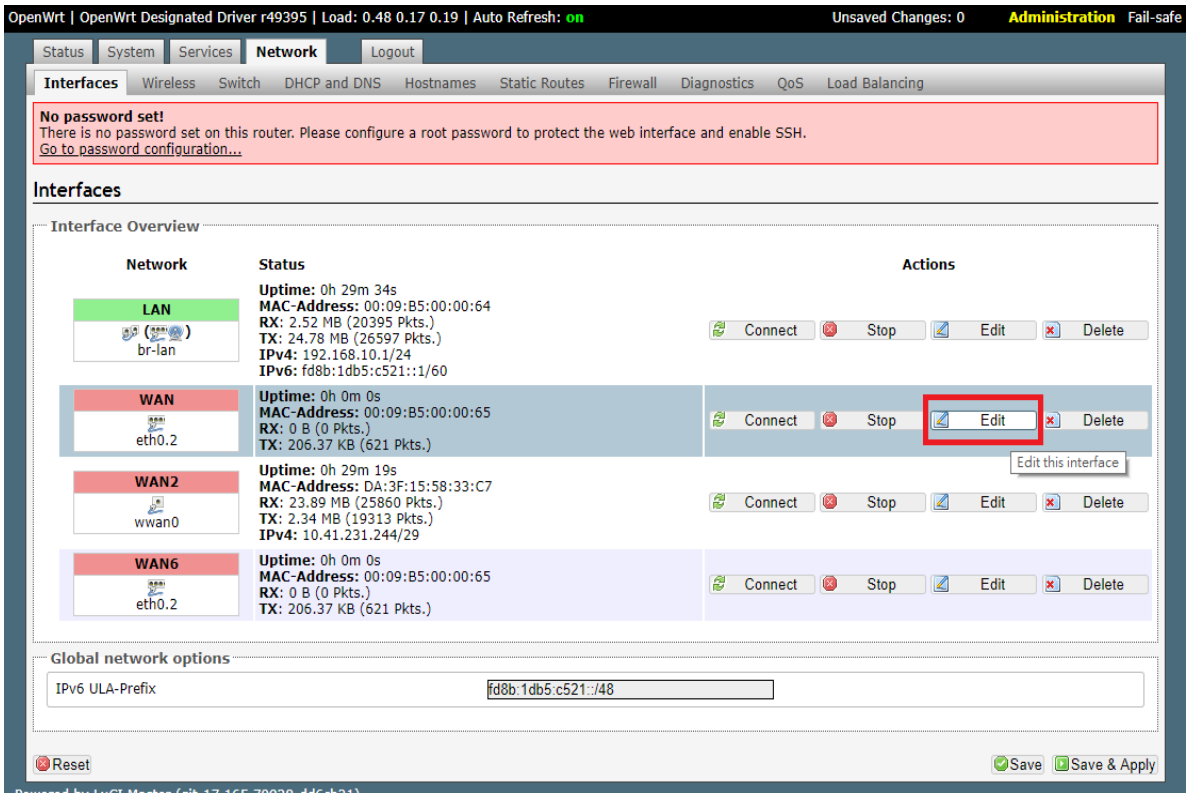
登出 Logout：

離開設定頁面

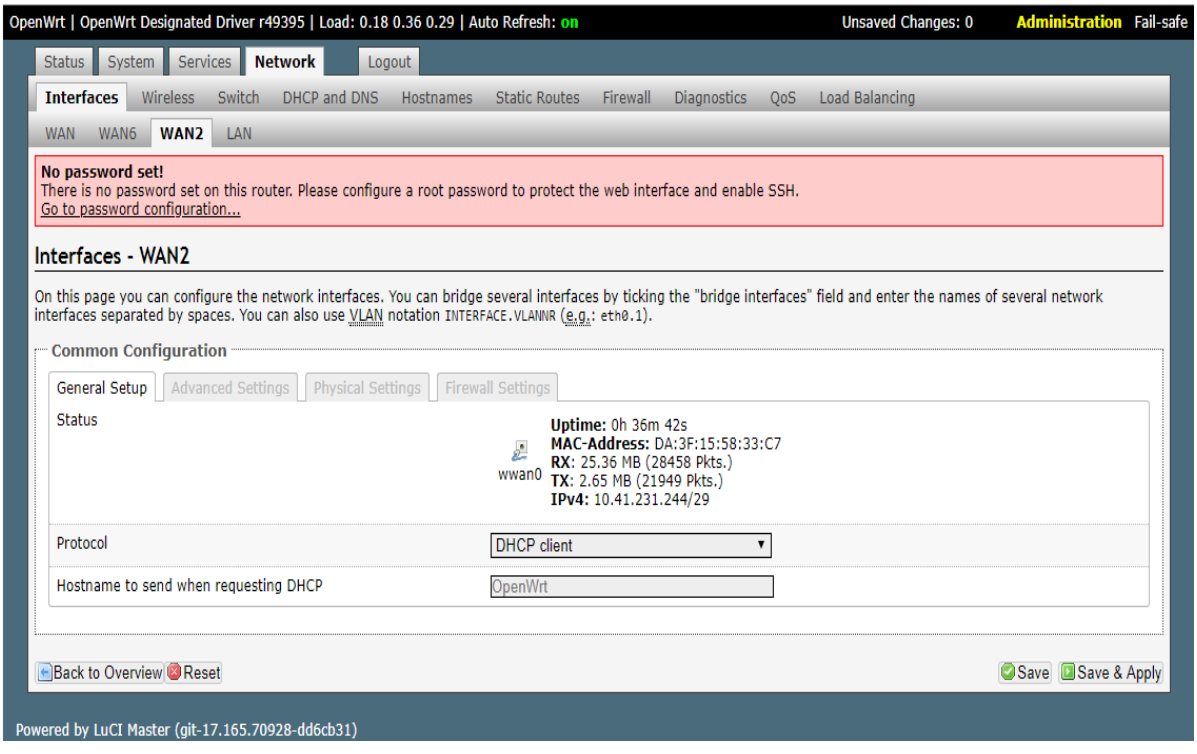


7. 快速無線 4G 上網/APN 設定

Network➔Interfaces ： 選擇 WAN2 的 Edit

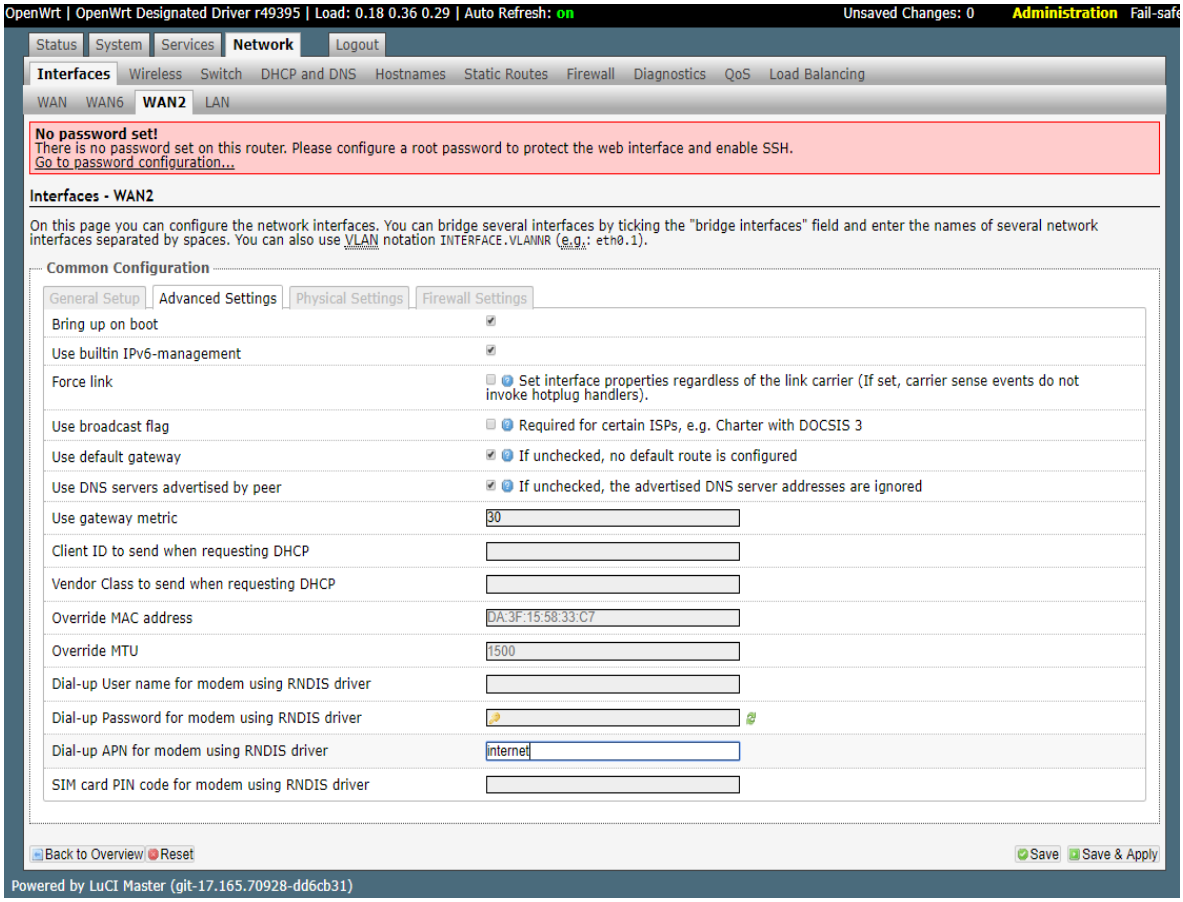


General Setup➔Protocol：選擇連線模式，4G SIM Card 連線為需選 DHCP.



進入 Advanced Settings 作相關設定

如：User name、Password、PIN Code、Dial-up、.....等等

如果是使用中華電信之 SIM CARD，請設置 APN 為 internet，無需設置用戶名和密碼

其他電信業者請參考各電信業者的相關設定，設置完成後，請按 Save & Apply 並重新啟動系統。