

窮人的 Cisco,高CP值網路設備 MikroTik 簡介與基本操作

2020/08/25 顯赫資訊股份有限公司 吳漢璋 Kasper



課程大綱- MikroTik RouterOS



- ❖ RouterOS 基本功能與模擬器說明
- ❖ RouterOS 防火牆、認證網頁功能CWP解說與實做
- ❖RouterOS 8大網管工具介紹



現代人沒有網路行嗎?



過去

馬斯洛的人類生存需求理論

自我

實現需求

完全發揮個人潛能

尊重需求

獲得聲望、成就感

社交需求

<u>友誼、親密關係、歸屬感</u>

安全需求

人身安全、生活穩定、健康保障

生理需求

食物、空氣、水、睡眠



現在

自我

實現需求

完全發揮個人潛能

尊重需求

獲得聲望、成就感

社交需求

<u></u>友誼、親密關係、歸屬感

安全需求

人身安全、生活穩定、健康保障

生理需求

食物、空氣、水、睡眠

網路需求



現在

自我

實現需求

完全發揮個人潛能

尊重需求

獲得聲望、成就感

社交需求

<u>友誼、親密關係、歸屬感</u>

安全需求

人身安全、生活穩定、健康保障

生理需求

食物、空氣、水、睡眠

網路需求

電池



關於 MikroTik



- ❖ 1996年 成立於拉脫維亞(Latvia)首都里加(Riga),主要從事「路由器」和「無線ISP系統」開發
- ❖ 1997年 推出RouterOS軟體路由器 RouterOS是一套低成本高性能的路 由器作業系統

(http://www.mikrotik.com/download)

- ❖ 2002年 推出RouterBOARD硬體路 由器(http://routerboard.com)
- ❖ 企業口號: Routing the World





歐洲知名品牌MikroTik在145個國家或地區中有五百多家經銷商和代理商,它們提供了產品銷售支援及MikroTik相關解決方案



MikroTik 用戶見面會(MUM)





❖會議內容主要是在介紹MikroTik RouterOS軟體和RouterBOARD硬體

- ❖參與者提出問題、聆聽簡報與專家交談並觀看 MikroTik最新技術展示。
- ❖全世界到目前為止已經辦了150多場MikroTik 用戶會議。最大的活動有3000多名人員參加。
- https://mum.mikrotik.com

MikroTik 學院





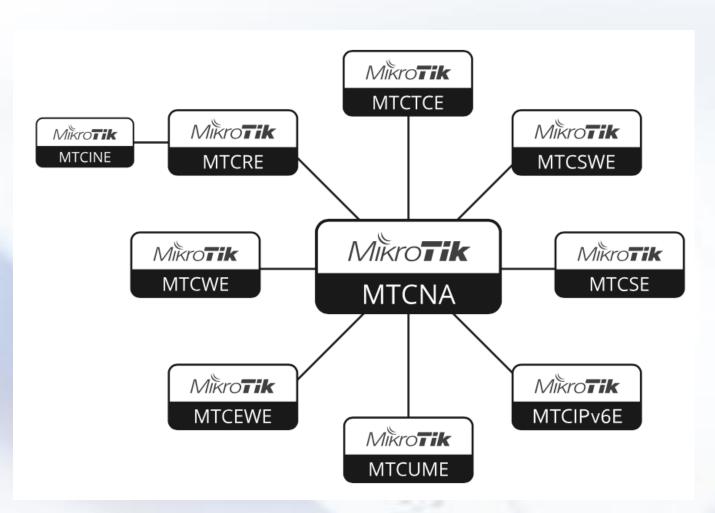


❖適用於大學、技術學校、學院、職業學校和其他 教育單位等教育機構的計劃

❖全球已有500多所大學和750名培訓講師加入

MikroTik 國際認證介紹





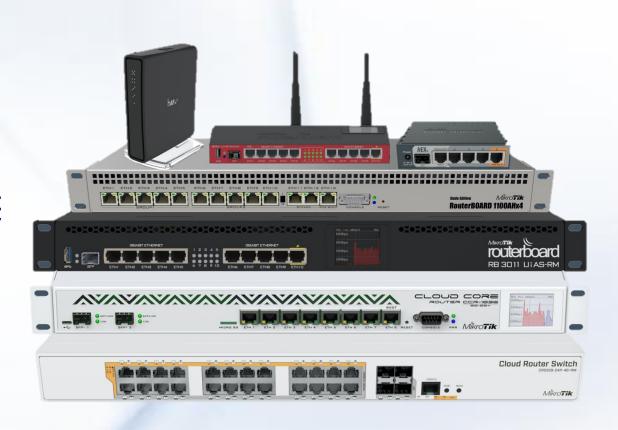
MikroTik 國際認證課程:

- · MTCNA-網路助理
- · MTCRE-路由工程師
- MTCINE-網路互連工程師
- MTCWE-無線工程師
- MTCTCE-流量控制工程師
- · MTCUME-用戶管理工程師
- MTCIPv6E-IPv6工程師
- MTCSE-安全工程師 New
- MTCSWE-交換器工程師 New
- MTCEWE-企業無線工程師 New

為什麼要選擇使用MikroTik?



- ❖ 最佳價格及效能
- ❖ 耗電量低
- ❖ 數千頁的文件、範例,應用說明和指南
- ❖ RouterOS軟體支援大多數常見功能, 產品會不斷依客戶需求來新增新功能
- ❖ 數以百萬RouterOS網路設備正在環遊 全世界
- ❖ 擁有23年的網路軟體和硬體開發經驗
- ❖ 全球超過13萬個RouterOS網路認證 工程師



Cisco v.s. MikroTik 產品比較



產品比較	Cisco	MikroTik
支援	有SMARTnet 支援 ,但必須付費	官方支援(回覆約1至3個工作日) 討論區/社群支援 Free~
效能	支援更高階需求	網路吞吐量最快80Gbps
價格	較貴	便宜
功能	功能取決於型號及啟動的授權	所有型號共享相同的功能, 只是硬體規格容量不同
管理	內建CLI,對初學者不易操作	CLI、GUI、內建網頁、 更多友善操作方式
測試	實體設備要做實驗(Lab)通常無法 負擔起費用	x86版的授權可免費試用24小時,如需獲得實體設備上所有功能, 只需付便宜費用即可獲得。
市場	數據中心/網路服務供應商	家裡辦公、小型辦公(SOHO)及中小型企業
證照	證照大家都知道	證照比較不知名

教育體系應用案例



❖H縣教育網路中心

學校端L3 路由器、防火牆及L2 Switch、The Dude應用

❖ Y縣教育網路中心

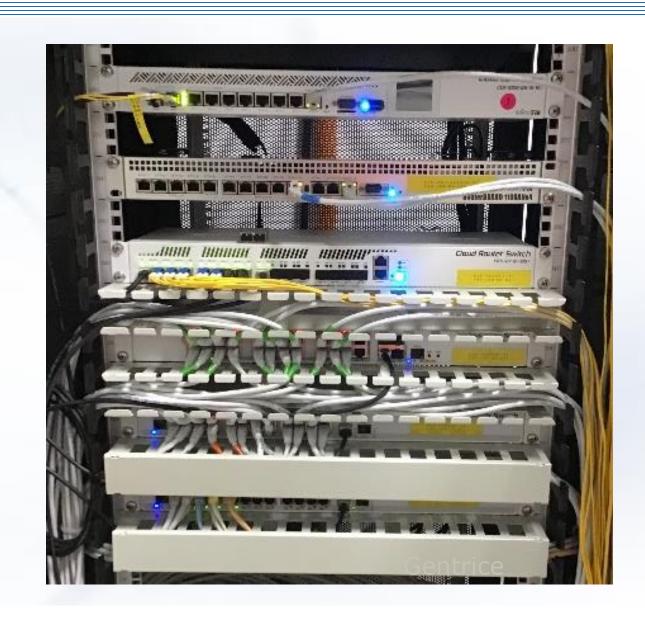
中心端NAT Server 及學校端 L3 路由器應用

❖C縣教育網路中心

學校端IPv4/IPv6防火牆、NAT、無線網路存取閘道器應用

❖ I縣教育網路中心

各校IPv4/IPv6防火牆、NAT、無線網路存取閘道器應用





MikroTik主要產品分成二部份

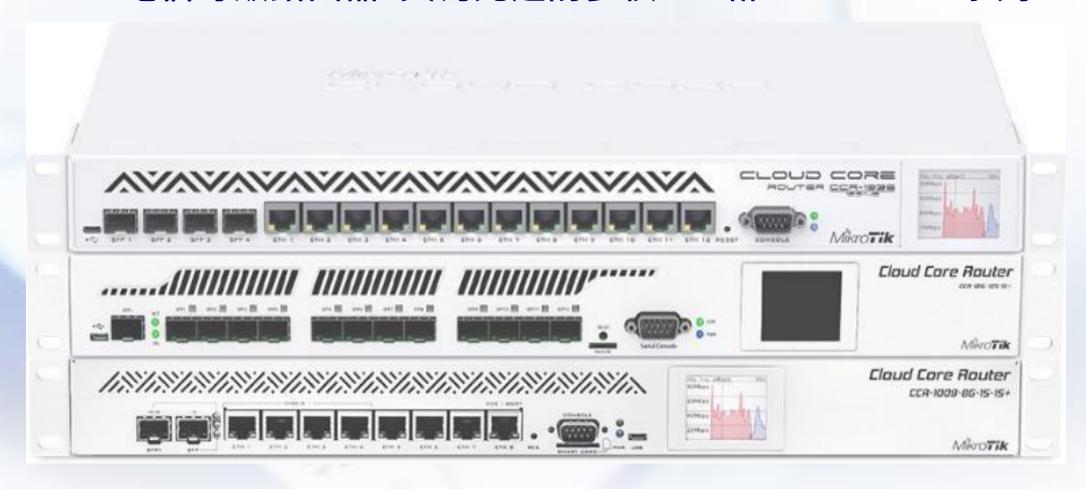
- 1. 硬體:
- · 由MikroTik 及合作夥伴設計製造
- · 獨特功能: 雙電源輸入、內建RouterOS

2.軟體:

- RouterOS
- Swos
- The Dude



一、電信等級路由器: 具有先進的多核CPU和Smart Switch系列





電信等級路由器(Cloud Core Router)



CCR2004-1G-12S+2XS NEW

The Connectivity Router - your best companion when it comes to SFP, SFP+ and SFP28 management! 1, 10 and 25 Gbps ports in a single device to make your life easier.



CCR1036-8G-2S+EM

1U rackmount, 8x Gigabit Ethernet, 2xSFP+ cages, LCD, 36 cores x 1.2GHz CPU, 8GB RAM, 41.5mpps fastpath, Up to 28Gbit/s throughput, RouterOS L6, Dual PSU



CCR1072-1G-8S+



1U rackmount, 1x Gigabit Ethernet, 8xSFP+ cages, LCD, 72 cores x 1GHz CPU, 16GB RAM, up to 120 million packets per second, 80Gbps throughput, RouterOS L6



CCR1016-12S-1S+

1U rackmount, 12xSFP cage, 1xSFP+ cage, 16 cores x 1.2GHz CPU, 2GB RAM, LCD panel, Dual Power supplies, RouterOS L6

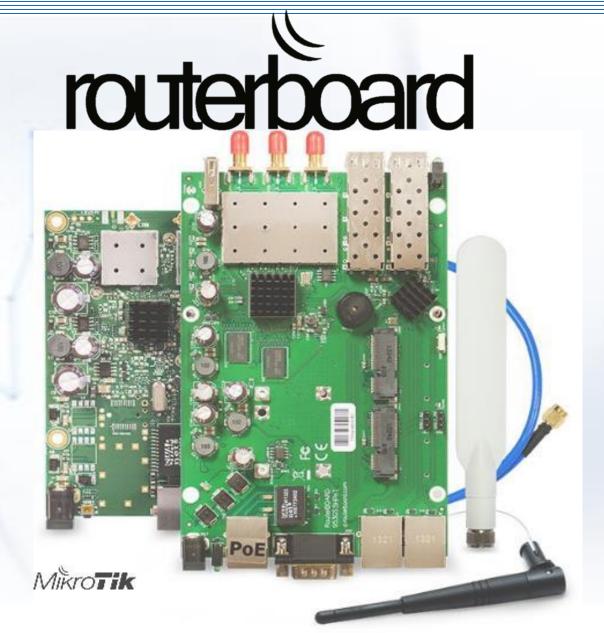


CCR1009-7G-1C-1S+

1U rackmount, 7x Gigabit Ethernet, 1x Combo port (SFP or Gigabit Ethernet), 1xSFP+ cage, 9 cores x 1.2GHz CPU, 2GB RAM, LCD panel, Dual Power supplies, SmartCard slot, RouterOS L6



二、RouterBOARD系列:可依需求搭配列:可依需求搭配模組及配件組裝成一台路由器



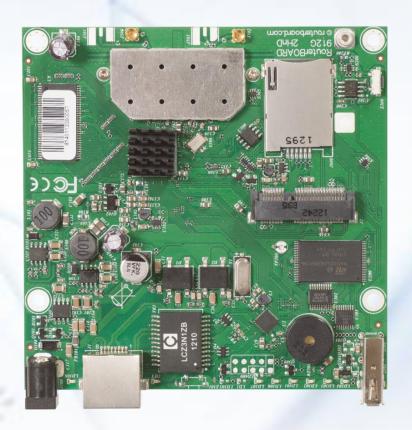
RouterBOARD 硬體外觀



❖右圖片為

RB912 RB953 RouterBOARD

❖更多型號
https://routerboard.com







RouterBOARD 型號介紹



- ❖RouterBOARD型號命名方式有幾種,最常看到是使用
- ❖3位數字來做命名。
- 1. 數字第一碼: 系列代號
- 2. 數字第二碼: 有線埠數
- 3. 數字第三碼:無線介面數(含內建mPCI和mPCIe插槽數)
- ❖直接用名稱命名:例如:OmniTIK, Groove, SXT, SEXTANT, Metal, LHG, DynaDish, cAP, wAP
- ❖特殊型號:像是MikroTik RouterBoard 600, 800, 1000, 1100, 1200, 2011

RouterBOARD 型號介紹



以3位數字命名後面的代號介紹

- ❖ U: USB埠
- ❖ P: 電源Power簡稱P,多個以上的PoE Out埠 (有控制器)
- ❖ i:乙太網路電源供應連接器injector 簡稱 i, 單一PoE埠 (無控制器)
- ❖ A: 配置較多的記憶體或是License 等級比較高的機型
- ❖ H: 配置高效能的CPU
- ❖ G: 千兆乙太網路埠(通常會跟 "U", "A", "H"搭配)
- ❖ L: 精簡版
- ❖ S: SFP光纖傳輸模組埠
- ❖ e: PCIe 擴充介面卡
- ❖ x <N>: "N" 代表CPU核心數 (x2, x16, x36)
- ❖ R MiniPCI or MINIPCIe 插槽

RouterBOARD 型號介紹



例如: RB912UAG-5HPnD

* **RB**: RouterBOARD

❖ 9: 9 系列

❖ 1:1個有線網路埠

❖ 2: 1個WiFi 介面及1個內建 miniPCIe插槽

❖ U: USB 埠

* A: license level 4

❖ G: 千兆乙太網埠

❖ 5: 內建5GHz

* HP: High Power

❖ n: WiFi 802.11n

❖ D: 雙天線



三、無線產品:提供戶外室內用戶端設備(CPE)及AP解決方案

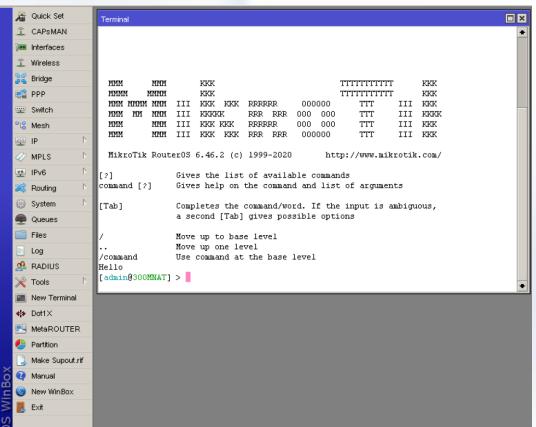


產品介紹-軟體 RouterOS



RouterOS





產品介紹-軟體 RouterOS CHR虛擬機版本



RouterOS CHR (Cloud Hosted Router)

- ❖「虚擬機器」專用
- ❖ 支援x86 64bit 架構
- ❖支援多種版本虛擬伺服器,例如:VMWare、Hyper-V、VirtualBox、KVM等
- ❖ CHR 擁有完整的RouterOS預設功能

產品介紹-軟體 MikroTik SwOS



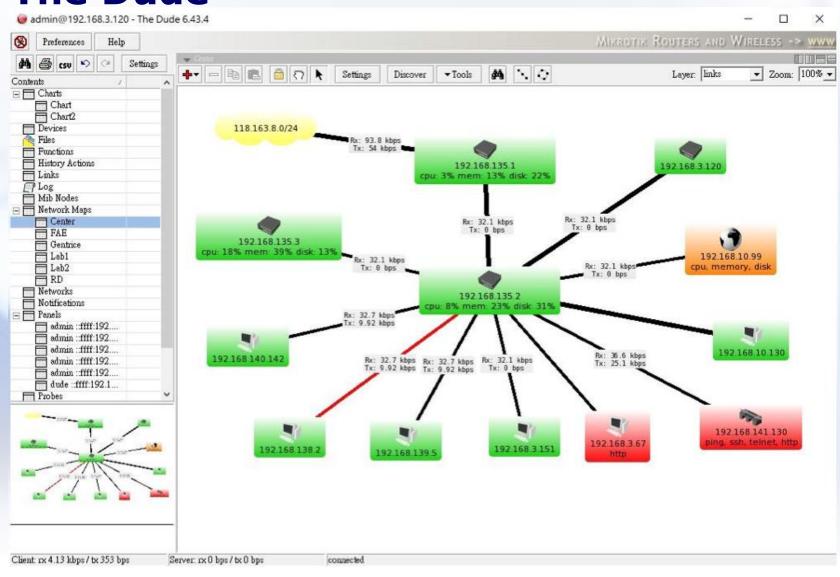
SwtichOS (SwOS)

MikroTik SwOS					
Link SFP Port Isolation LAG	Forwarding RSTP Stats Errors Hist VLAN VLANs Hosts IGMP SNMP ACL System Upgrade				
General					
Address Acquisition	DHCP with fallback 🗸				
Static IP Address	192.168.88.1				
Identity	MikroTik				
Allow From					
Allow From Ports					
Allow From VLAN					
Watchdog					
Independent VLAN Lookup					
IGMP Snooping					
Mikrotik Discovery Protocol					
MAC Address	64:d1:54:c7:3a:58				
Serial Number	763C076756AE				
Board Name	CRS326-24G-2S+				
Uptime	00:08:17				

產品介紹-軟體 MikroTik the Dude



The Dude



MikroTik 產品該如何選?



- ❖埠數及介面種類
- ❖ 運用效能PPS、網路吞吐量Throghput
- ❖價格預算

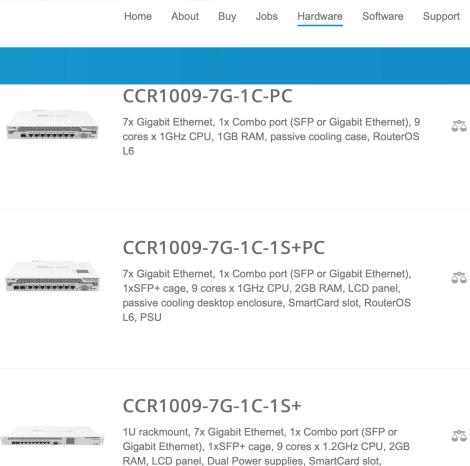
產品介紹



目前提供160多種不同的產品 https://mikrotik.com/products



MikroTik Products **Product categories** Ethernet routers Wireless systems Wireless for home and office Data over Powerlines



RouterOS L6



一、RouterOS 基本功能與模擬器

MikroTik RouterOS 基本功能介紹



MikroTik RouterOS™是一套軟體路由器系統,可將一般PC或MikroTik RouterBOARD™硬體變成專用路由器

RouterOS 重要的功能如下:

- Firewall & NAT (封包控制).
- Routing (RIP, OSPF, BGP, RIPng, OSPF V3)
- VPN & Tunnel (EoIP, PPTP, L2TP, PPPoE, SSTP, OpenVPN)
- Wireless (802.11 a/b/g/n/ac, 2.4/5Ghz)
- DHCP、Hotspot、Radius (用戶端管理)
- QoS & Bandwidth limiter (頻寬管理)
- Proxy (Web Proxy)
- Tools (Torch, MAC-Ping, MRTG, Packet Sniffer)



RouterOS一般版的軟體授權



❖RouterOS一般版的軟體授權等級分成 Level 0~6

等級	0 (試用模式)	1 (免費展示)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
價格	無金鑰	需要至官網註冊	大量授權	\$45美元	\$95美元	\$250美元
初始設定支援	-	-	-	15 日	30 日	30 日
Wireless AP	試用24小時	-	-	支援	支援	支援
Wireless Client 及 Bridge	試用24小時	-	支援	支援	支援	支援
RIP, OSPF, BGP 協定	試用24小時	-	支援(*)	支援	支援	支援
EoIP tunnels	試用24小時	1	不限	不限	不限	不限
PPPoE tunnels	試用24小時	1	200	200	500	不限
PPTP tunnels	試用24小時	1	200	200	500	不限
L2TP tunnels	試用24小時	1	200	200	500	不限
OVPN tunnels	試用24小時	1	200	200	不限	不限
VLAN 介面	試用24小時	1	不限	不限	不限	不限
HotSpot 線上使用數限制	試用24小時	1	1	200	500	不限
RADIUS 客戶端	試用24小時	-	支援	支援	支援	支援
Queues 佇列	試用24小時	1	不限	不限	不限	不限
Web proxy網頁代理	試用24小時	-	支援	支援	支援	支援
User manager 活動session數	試用24小時	1	10	20	50	不限
KVM guests數量	無	1	不限	不限	不限	不限

^{(*) -} BGP功能僅包含在等級3授權的RouterBOARD中,對於其他設備需要等級4或更高級別授權才能擁有BGP功能。

MikroTik RouterOS CHR虛擬機版本授權



CHR(Cloud Hosted Router) 版本授權等級分成四級:

- **❖Free** 免費
- **❖p1** (perpetual-1) \$45美元
- **❖p10** (perpetual-10) \$95美元
- ❖ p-unlimited (perpetual-unlimited) \$250美元

授權等級	網路速度限制	價格(美元)
Free	1Mbit	免費
P1	1Gbit	\$45
P10	10Gbit	\$95
P-Unlimited	無限制	\$250



想了解RouterOS設定沒有實體機怎麼辦?

想練習RouterOS設定沒有實體機怎麼辦?



❖方法一、MikroTik 官方提供二個網址展示 http://demo.mt.lv http://demo2.mt.lv

❖方法二、直接在PC上裝模擬器



RouterOS搭配GNS3 模擬器介紹

RouterOS搭配GNS3 模擬器介紹



GNS3 全名為「Graphical Network Simulator」是一款具有圖型化界面的網路模擬器,可透過模擬的Router和Switch來建立複雜網路測試環境。



- **❖GNS3-all-in-one software (GUI)** 安裝於本機PC(Windows, MAC, Linux)
- The GNS3 virtual machine (VM)

用裝於VMServer





RouterOS搭配GNS3 模擬器介紹



使用GNS3的優點:

- ❖免費工具 Free
- ❖開源軟體 (Open Source)
- ❖無需月費或年費授權(License)
- ❖模擬裝置數量無限制(需依硬體等級CPU及記體決定)
- ❖即時(Real-time)網路模擬
- ❖ 跨平台系統及多種網路設備廠商裝置支援
- ❖模擬各種網路架構及測試
- ❖驗證網路概念
- ❖GNS3模擬器可以連到外面真實的網路

GNS3 模擬器與Packet Tracer比較



Cisco Packet Tracer

- ❖非免費軟體(需要註冊於網路學院師生及註冊學校用戶才能使用)
- ❖ 專利程式碼非開源軟體Open source
- ❖ 只能模擬Cisco 裝置不支援其他設備商。
- ❖不支援部分設備的完整指令集。
- ❖只限軟體內部模擬無法整合實體網路裝置連出外網。
- ❖不支援MacOS

GNS3模擬器軟體安裝設定



安裝檔下載位置:

https://github.com/GNS3/gns3-gui/releases

以下使用Windows 版為安裝範例,先找到 GNS3-x.x.x-all-in-one.exe

GNS3-2.2.12-all-in-one.exe	84.9 MB
GNS3-2.2.12-all-in-one.exe.sha256	93 Bytes
⇔ GNS3-2.2.12.dmg	73.6 MB
→ GNS3-2.2.12.dmg.sha256	82 Bytes
♦ GNS3-2.2.12.source.zip	15.4 MB
♦ GNS3-2.2.12.source.zip.sha256	89 Bytes
♦ GNS3.VM.Hyper-V.2.2.12.zip	735 MB
♦ GNS3.VM.Hyper-V.2.2.12.zip.sha256	93 Bytes
♦ GNS3.VM.KVM.2.2.12.zip	655 MB
♦ GNS3.VM.KVM.2.2.12.zip.sha256	89 Bytes
♦ GNS3.VM.VirtualBox.2.2.12.zip	664 MB
♦ GNS3.VM.VirtualBox.2.2.12.zip.sha256	96 Bytes
♦ GNS3.VM.VMware.ESXI.2.2.12.zip	709 MB
♦ GNS3.VM.VMware.ESXI.2.2.12.zip.sha256	97 Bytes
♦ GNS3.VM.VMware.Workstation.2.2.12.zip	709 MB
♦ GNS3.VM.VMware.Workstation.2.2.12.zip.sha256	104 Bytes
Source code (zip)	
Source code (tar.gz)	



下載 MikroTik CHR(Cloud Hosted Router) image

網址: http://www.mikrotik.com/download

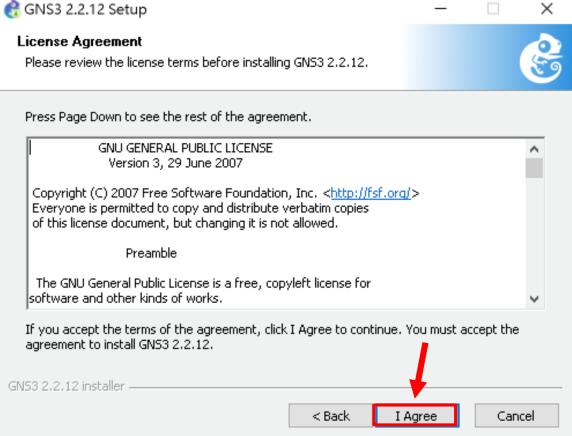
找到 CHR-> Raw disk image->stable 下載

Cloud Hosted Router

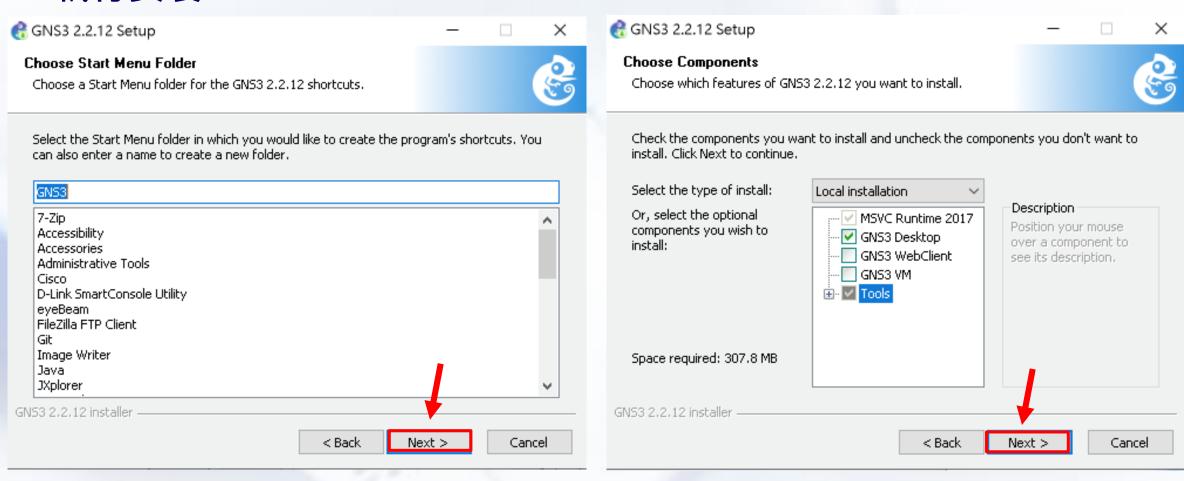
	6.45.9 (Long-term)	6.47.1 (Stable)	6.48beta12 (Testing)
Images	vmdk, vhdx, vdi, ova, img		
Main package			
VHDX image			
VMDK image			
VDI image			
OVA template			
Raw disk image			
Extra packages			
The Dude server			
The Dude client			
Changelog	∷	≣	: :
Checksum	\checkmark	\checkmark	~



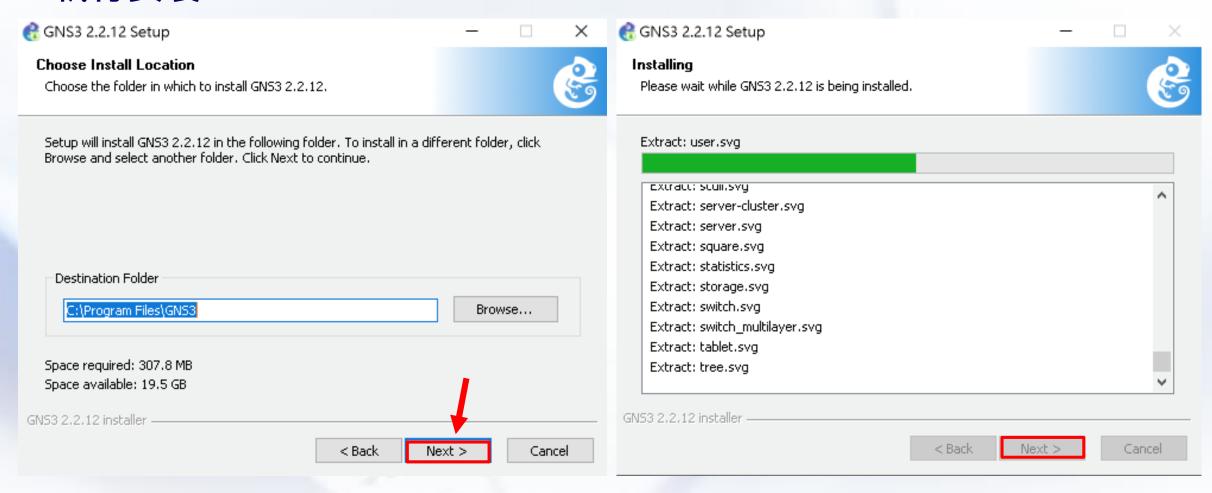




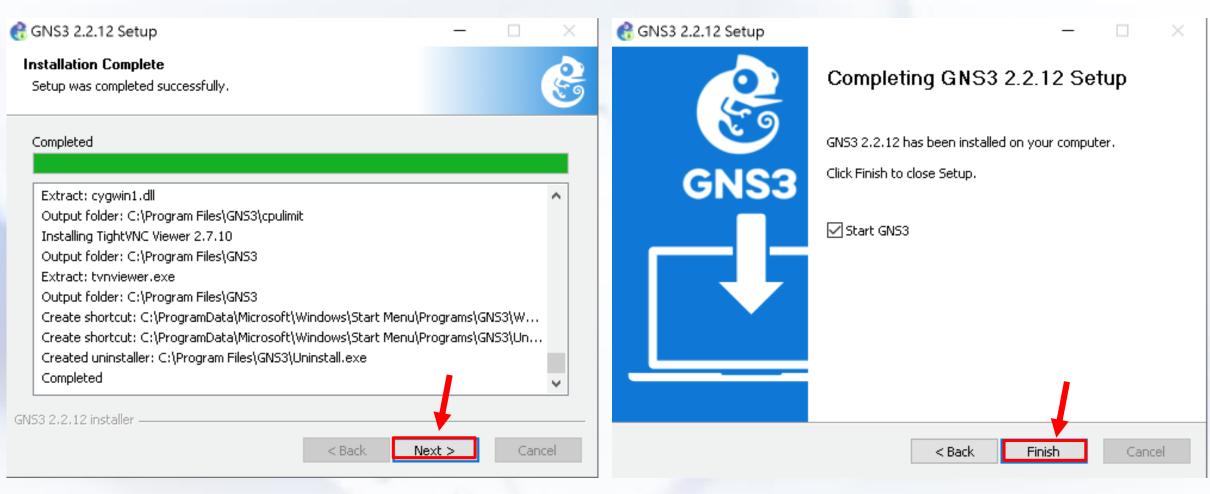






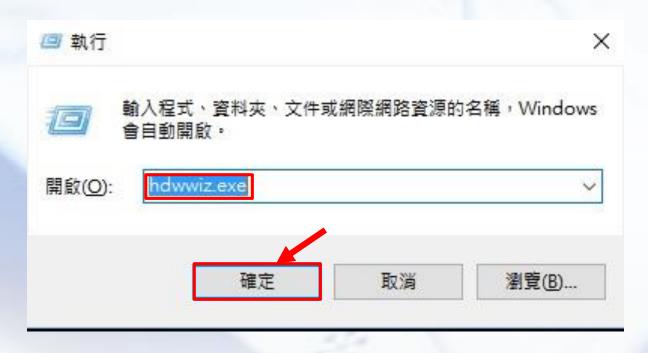








- ❖為了連結Internet 我們需要建立Loopback 網路介面
- 1. Windows鍵+R 呼叫「執行」輸入hdwwiz.exe





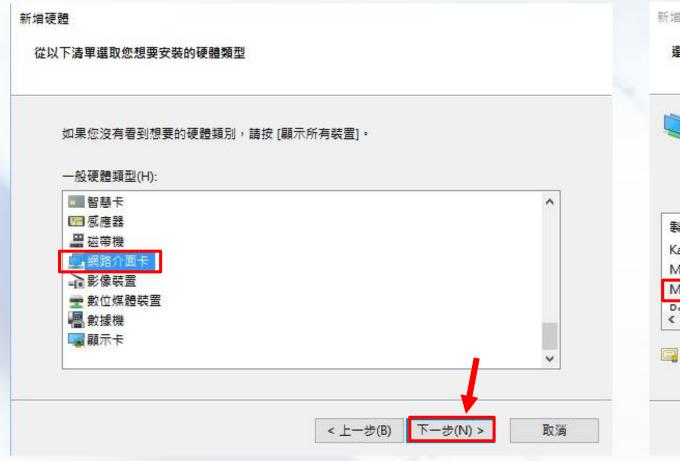
❖建立Loopback 網路介面







❖建立Loopback 網路介面



新增硬體 選取您要為這個硬體安裝的裝置驅動程式 請選擇您的硬體裝置製造商和機型,然後按 [下一步]。如果您想從磁片安裝其他驅動程式,請 按 [從磁片安裝]。 製造商 型號 Kaspersky Security Data Escort Microsoft IP-HTTPS Platform Adapter Microsoft ISATAP Adapter Mellanox Technologies Ltd. Microsoft Microsoft KM-TEST Loopback Adapter Microsoft Teredo Tunneling Adapter Darollale 驅動程式已數位簽章。 從磁片安裝(H)... 告訴我為什麼驅動程式簽章很重要 < 上一步(B) 下一步(N) > 取消



❖為了連上Internet 需建立Loopback 網路介面

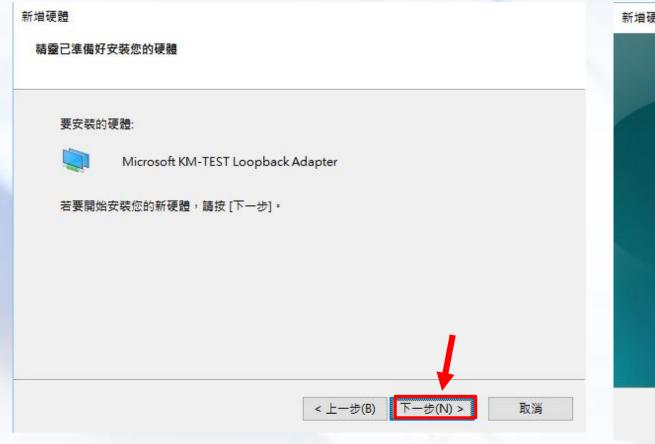
注意:安裝後需重開機才生效

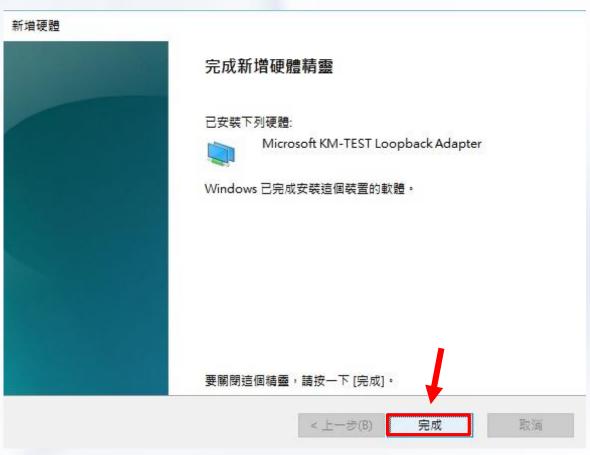




❖為了連上Internet 需建立Loopback 網路介面

注意:安裝後需重開機才生效





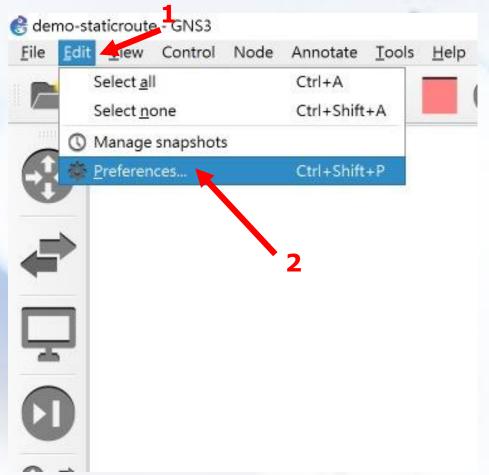


❖檢查Loopback 網路介面是否新增成功

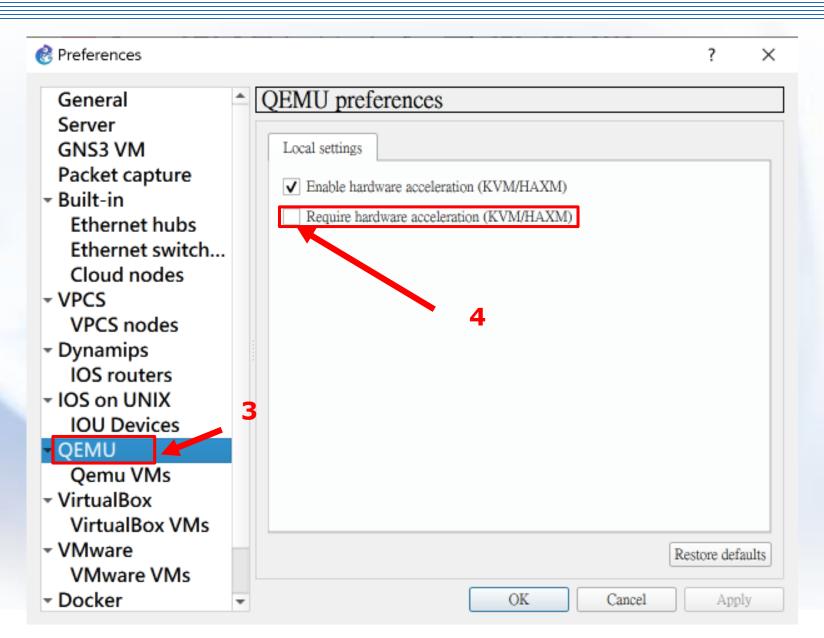




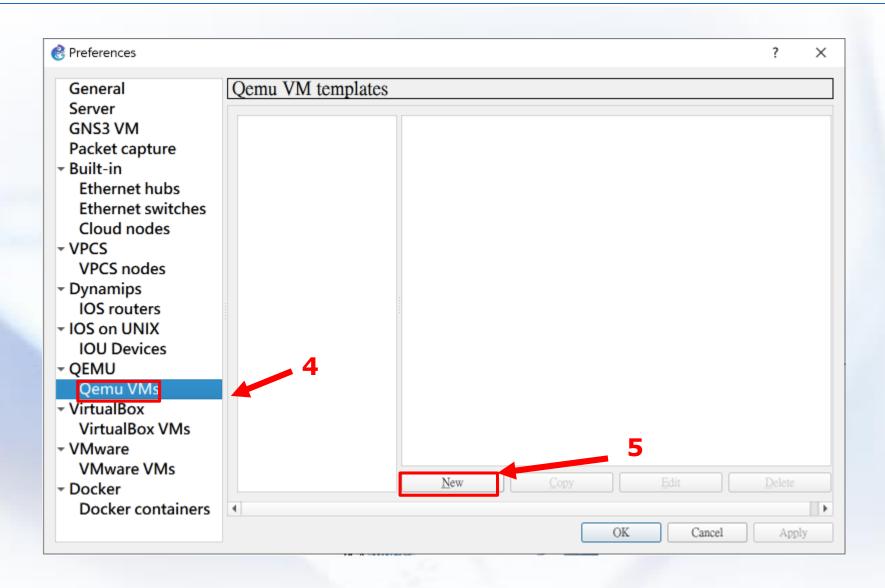
- ❖ 啟動GNS3後,我們需要先製作RouterOS 映像檔
- GNS3->Edit->Preferences



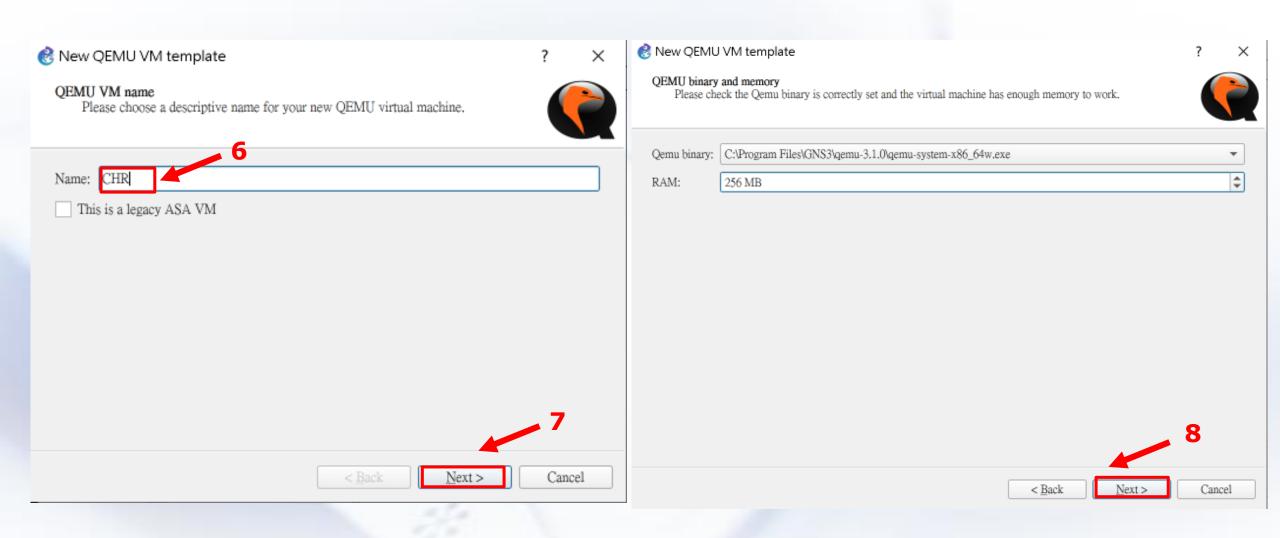




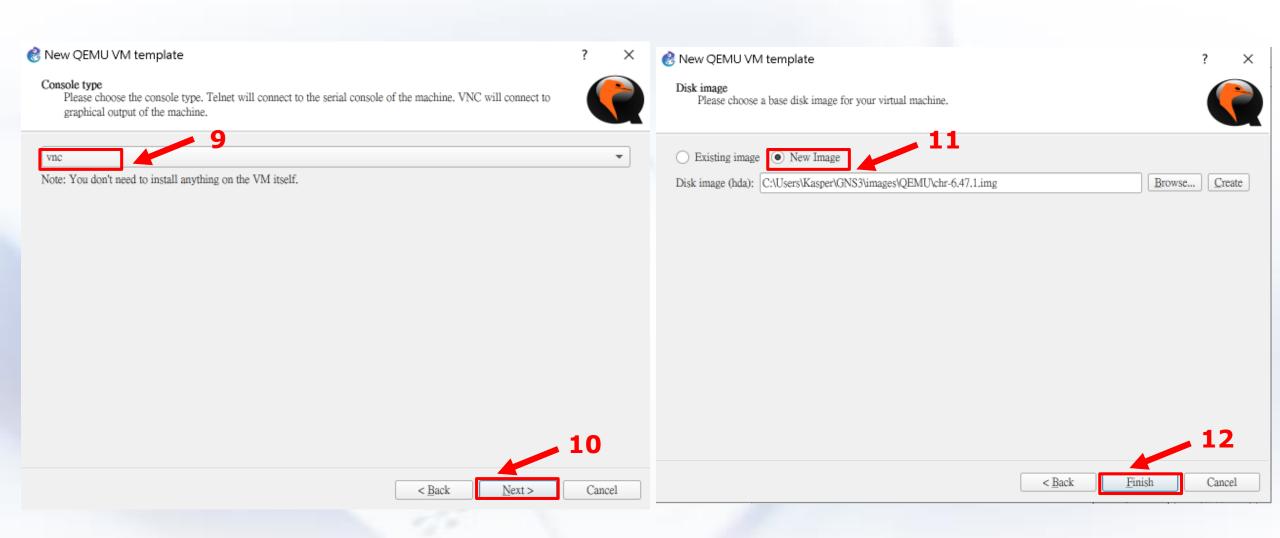




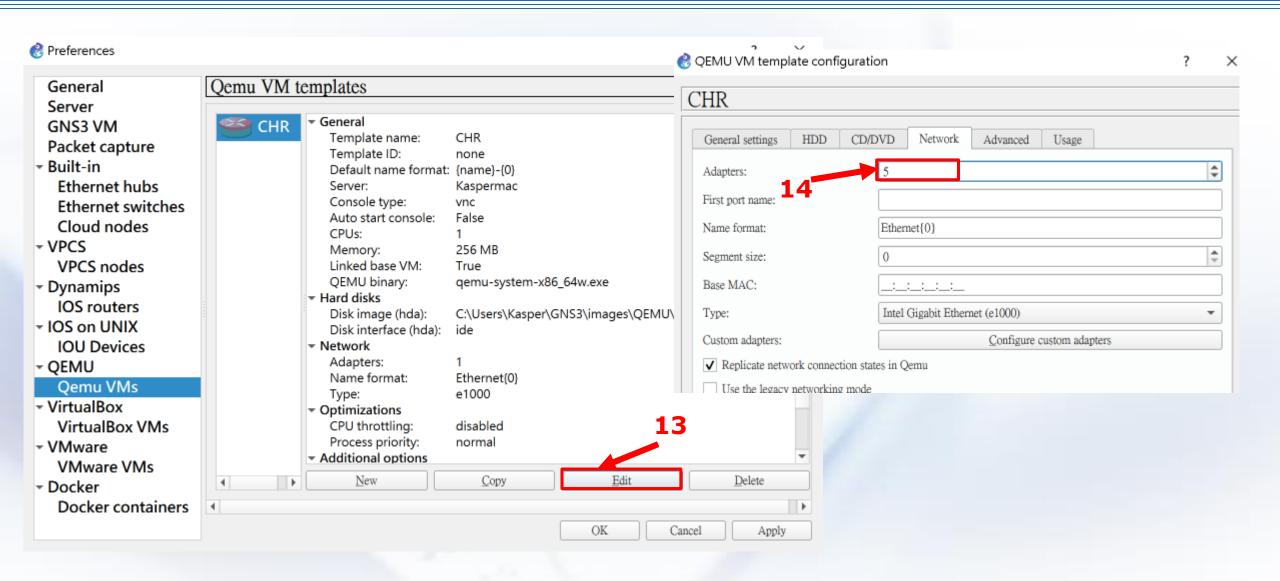




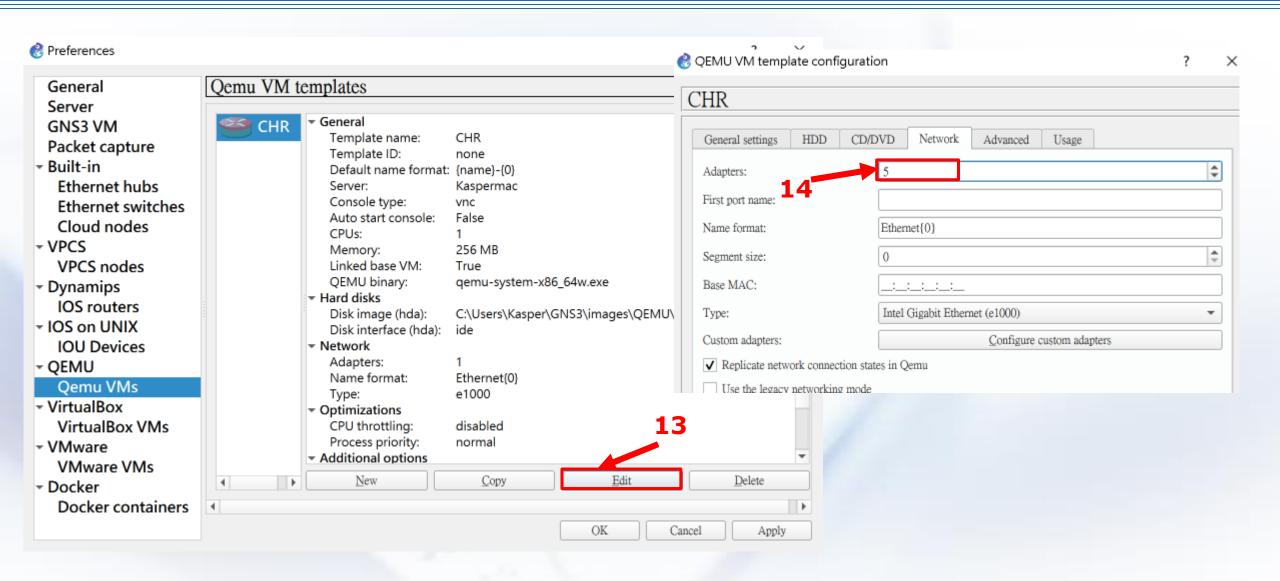






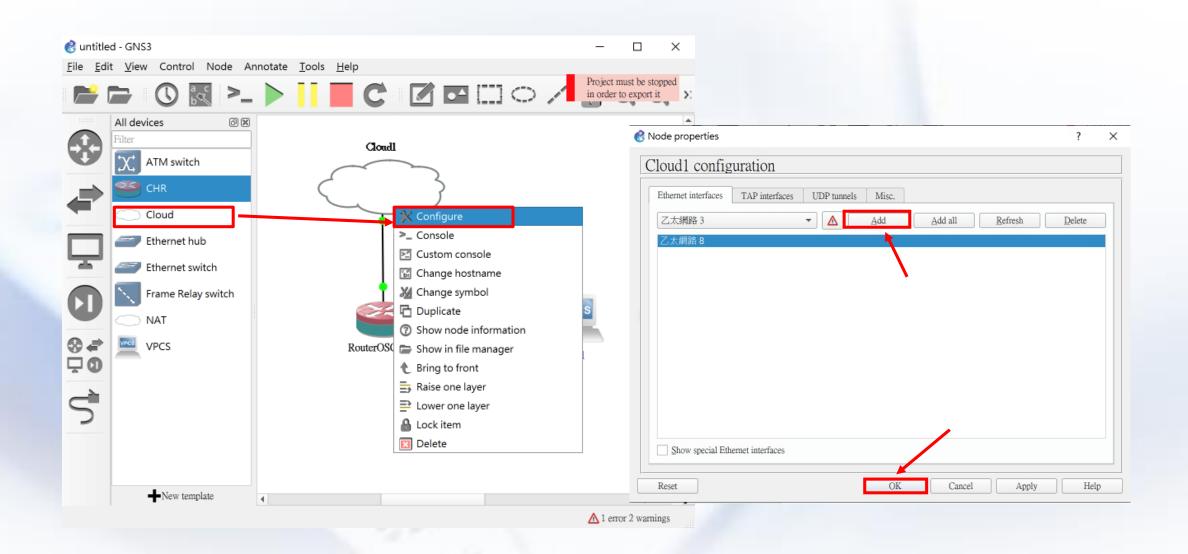






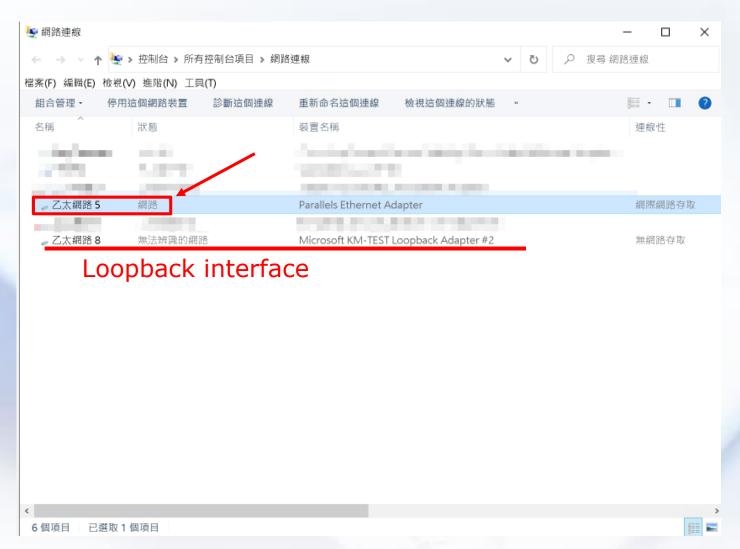
設定Cloud 網路

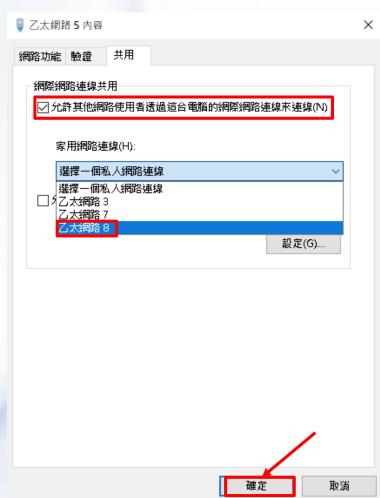




設定網路共用

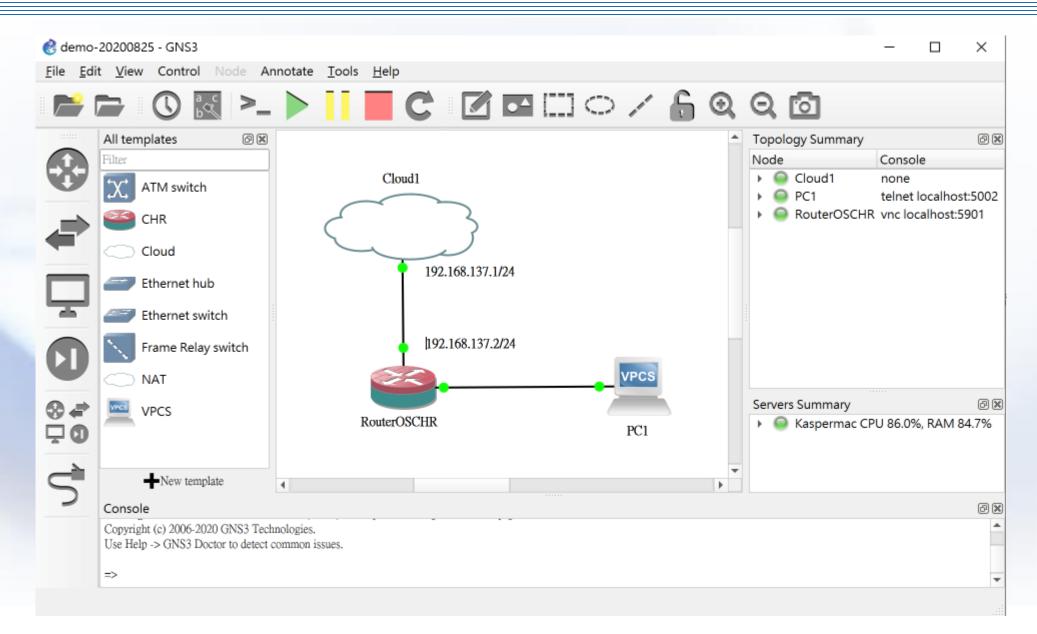






RouterOS 模擬器測試





RouterOS 連線管理



RouterOS 常用連線及管理方式:

- **∜Web**
- **SSH**
- ***** Telnet
- **⋄WinBox**
- MikroTik mobile app
- * QuickSet

RouterOS 使用Web連線



❖ Web登入 http://192.168.88.1

出廠預設值 IP: 192.168.88.1 帳號:admin 密碼:空白

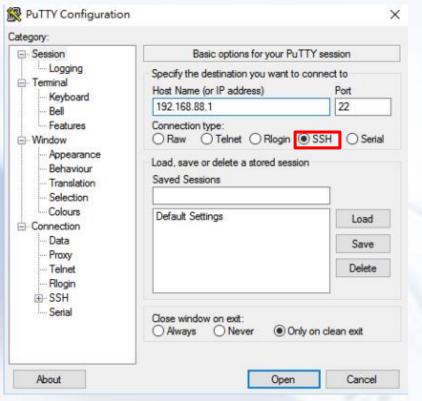


RouterOS 使用SSH



SSH

下載位置 http://www.putty.org/



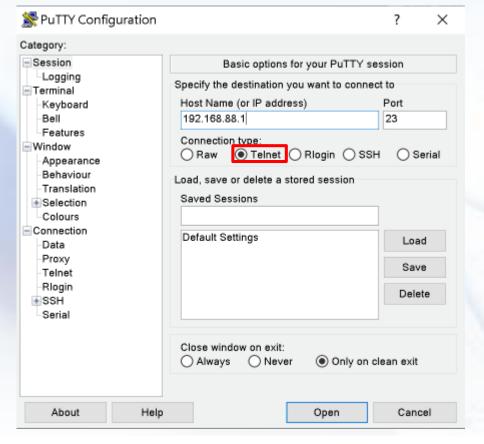
```
MMM
           MMM
                       KKK
                                                      TTTTTTTTTT
                                                                         KKK
           MMMM
                       KKK
                                                                         KKK
  MMMM
                                                      TTTTTTTTTT
                      KKK
                           KKK
                                                          TTT
                                                                        KKK KKK
  MMM MMMM MMM
                 III
                                 RRRRRR
                                             000000
                                                                   III
                 III
                      KKKKK
                                  RRR
                                                 000
                                                          TTT
                                                                        KKKKK
  \mathsf{MMM}
       MM
           MMM
                                      \mathbf{R}\mathbf{R}\mathbf{R}
                                            000
                      KKK KKK
                                 RRRRRR
                                            000
                                                 000
                                                          TTT
                                                                        KKK KKK
  MMM
            \mathsf{MMM}
                                                          TTT
  MMM
            MMM
                      KKK KKK
                                 RRR RRR
                                             000000
                                                                   III
                                                                        KKK KKK
  MikroTik RouterOS 6.47.1 (c) 1999-2020
                                                   http://www.mikrotik.com/
                 Gives the list of available commands
[?]
command [?]
                 Gives help on the command and list of arguments
[Tab]
                 Completes the command/word. If the input is ambiguous,
                 a second [Tab] gives possible options
                 Move up to base level
                 Move up one level
                 Use command at the base level
∕command
[admin@MikroTik] >
```

RouterOS 使用SSH



***Telnet**

下載位置 http://www.putty.org/



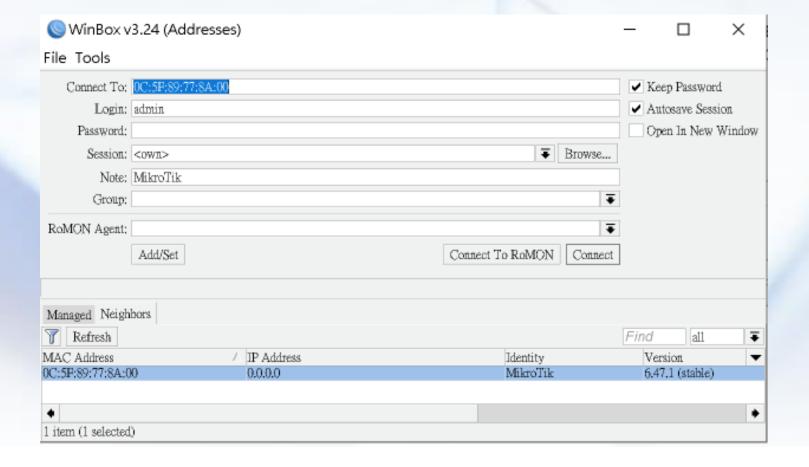
```
MMM
                      KKK
                                                     TTTTTTTTTT
                                                                      KKK
  MMM
                      KKK
                                                                      KKK
  MMMM
           MMMM
                      KKK
                           KKK
                                RRRRRR
                                                         TTT
                                                                      KKK KKK
  MMM MMMM MMM
                                            000000
                 III
                                                                 III
                                                         TTT
                      KKKKK
                                 RRR
                                     RRR
                                           000
                                                000
                                                                      KKKKK
  MMM
       MM
           MMM
                      KKK KKK
                                                000
                                                         TTT
                                                                      KKK KKK
  \mathsf{MMM}
            MMM
                 III
                                 RRRRRR
                                           000
                     KKK KKK
                                RRR RRR
                                            000000
                                                         TTT
                                                                 III KKK
                                                                           KKK
  \mathsf{MMM}
            MMM
                                                 http://www.mikrotik.com/
  MikroTik RouterOS 6.47.1 (c) 1999-2020
                 Gives the list of available commands
[?]
command [?]
                 Gives help on the command and list of arguments
[Tab]
                 Completes the command/word. If the input is ambiguous,
                 a second [Tab] gives possible options
                 Move up to base level
                 Move up one level
                 Use command at the base level
/command
[adminOMikroTik] > _
```

RouterOS 使用WinBox連線



❖WinBox管理工具

http://www.mikrotik.com/download



RouterOS 使用MikroTik 行動APP



- ❖可透過MikroTik 行動APP管理系統
- ❖ 支援Android和iOS操作系統



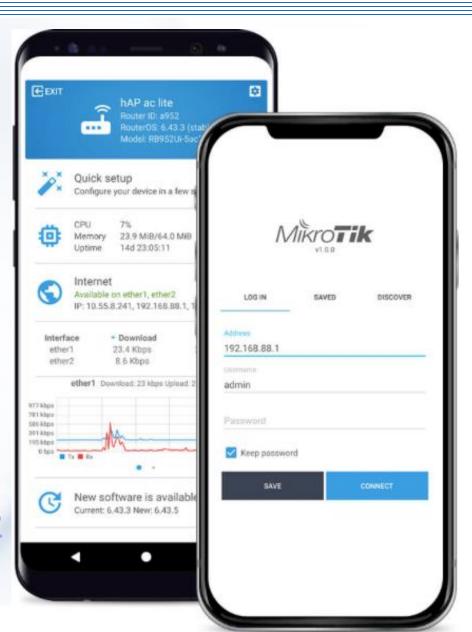
❖iOS下載位置

https://apps.apple.com/app/id1323064830



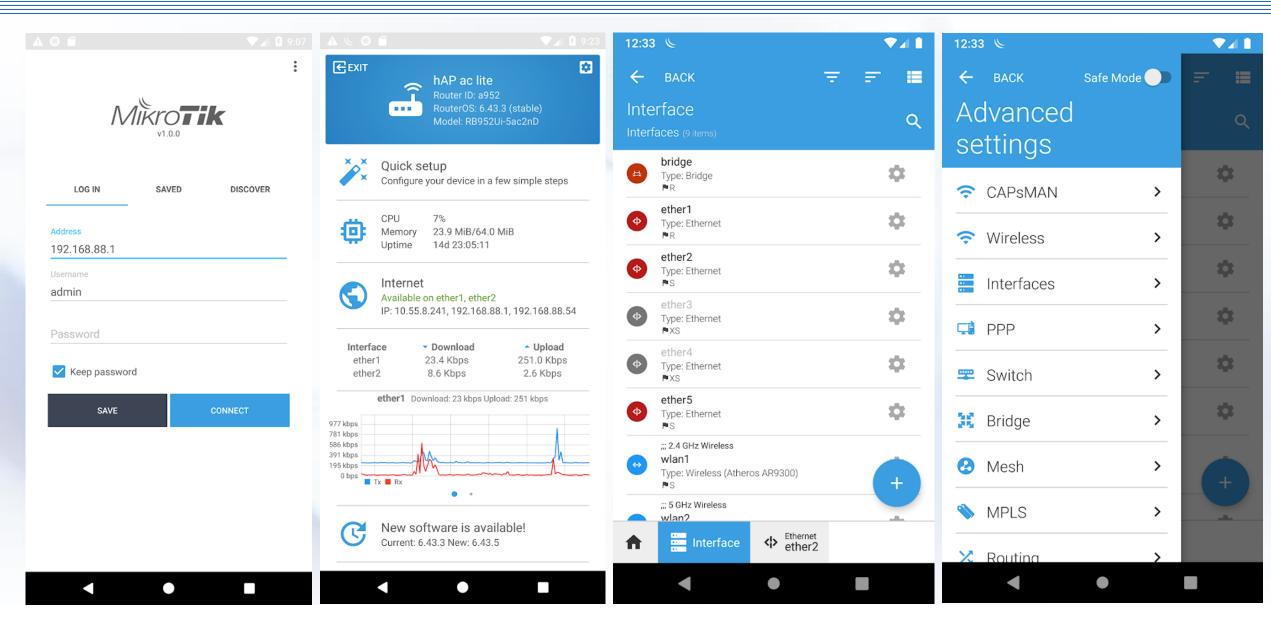
❖Android 下載位置

https://play.google.com/store/apps/details?
id=com.mikrotik.android.tikapp



RouterOS 使用MikroTik 行動APP

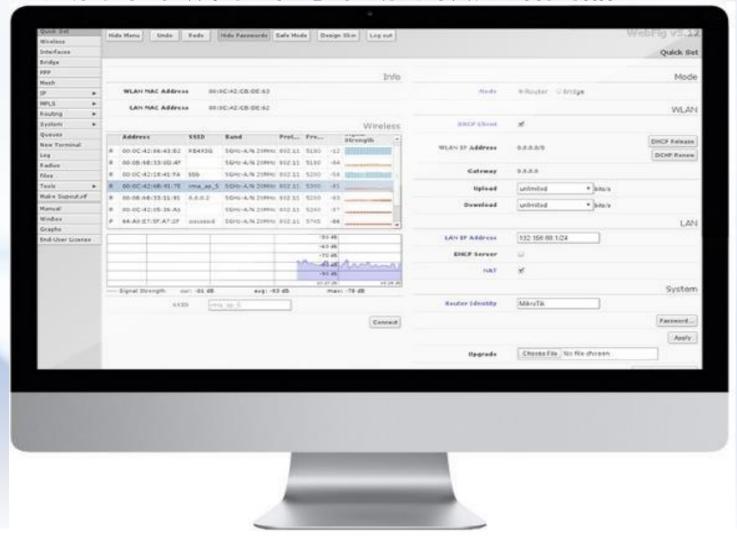




QuickSet 快速設定工具

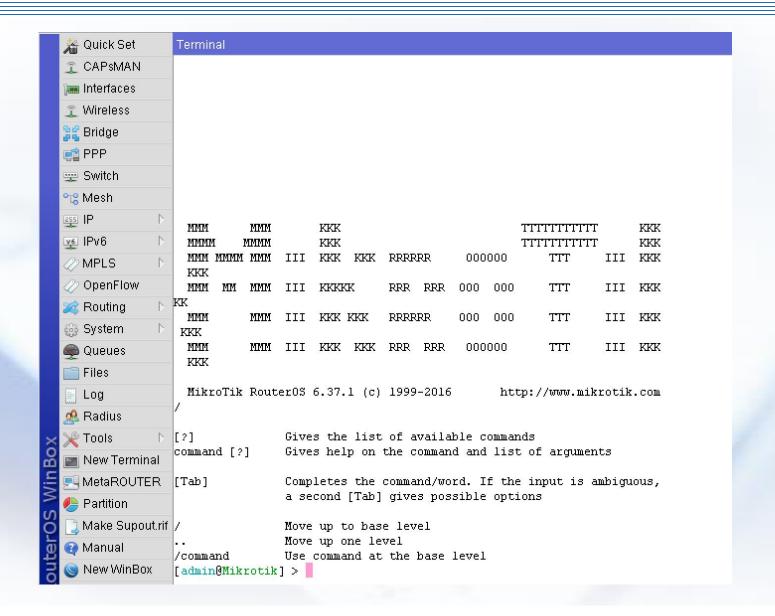


只需單擊幾下即可幫助您設定路由器!



RouterOS New Terminal 介紹





RouterOS 指令



❖具階層式架構,例如:/ip route

```
[admin@MikroTik] > ip route
[admin@MikroTik] ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
                         PREF-SRC
       DST-ADDRESS
                                        G GATEWAY
                                                         DIS INTE...
0 A S 0.0.0.0/0
                                        r 10.0.3.1
                                                             bridge1
1 ADC 1.0.1.0/24
                     1.0.1.1
                                                             bridge1
2 ADC 1.0.2.0/24 1.0.2.1
                                                         0 ether3
3 ADC 10.0.3.0/24 10.0.3.144
                                                             bridge1
4 ADC 10.10.10.0/24
                                                             wlan1
                       10.10.10.1
[admin@MikroTik] ip route>
```

❖回上一層:「..」

[admin@MikroTik] ip route> ..
[admin@MikroTik] ip>

❖回根目錄: 「/」

```
[admin@MikroTik] ip route> /
[admin@MikroTik] >
```

RouterOS 指令



❖善用[TAB]提示

```
[admin@MikroTik] > interface set e[Tab]_
[admin@MikroTik] > interface set ether[Tab]_
[admin@MikroTik] > interface set ether[Tab]_
ether1 ether5
[admin@MikroTik] > interface set ether_
```

❖縮寫指令功能

```
[admin@MikroTik] > pi 10.1 c 3 si 100
等同於
```

[admin@MikroTik] > ping 10.0.0.1 count 3 size 100

RouterOS 指令



❖常用指令:

add, edit, find, move, print, remove, set

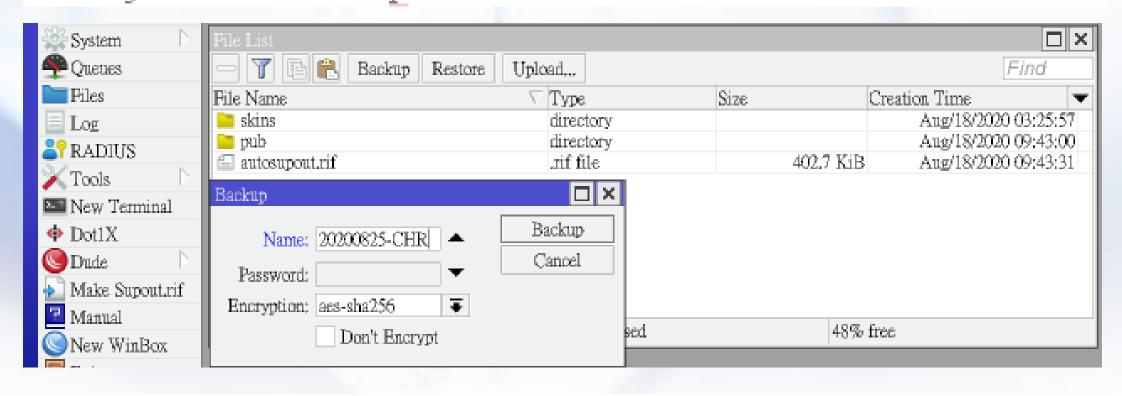
```
[admin@MikroTik] > interface print
Flags: X - disabled, D - dynamic, R - running
      NAME
                            TYPE
                                             MTU
    R ether1
                            ether
                                             1500
    R ether2
                            ether
                                             1500
   R ether3
                            ether
                                             1500
  3 R ether4
                            ether
                                             1500
[admin@MikroTik] > interface set 0,1,2 mtu=1460
[admin@MikroTik] > interface print
Flags: X - disabled, D - dynamic, R - running
      NAME
                            TYPE
                                             MTU
    R ether1
                            ether
                                             1460
    R ether2
                            ether
                                             1460
    R ether3
                            ether
                                             1460
    R ether4
                            ether
                                             1500
[admin@MikroTik] >
```

RouterOS 設定檔備份



❖/system backup save name=存檔檔名

[admin@MikroTik] > /system backup save name=20200825-CHR Saving system configuration Configuration backup saved



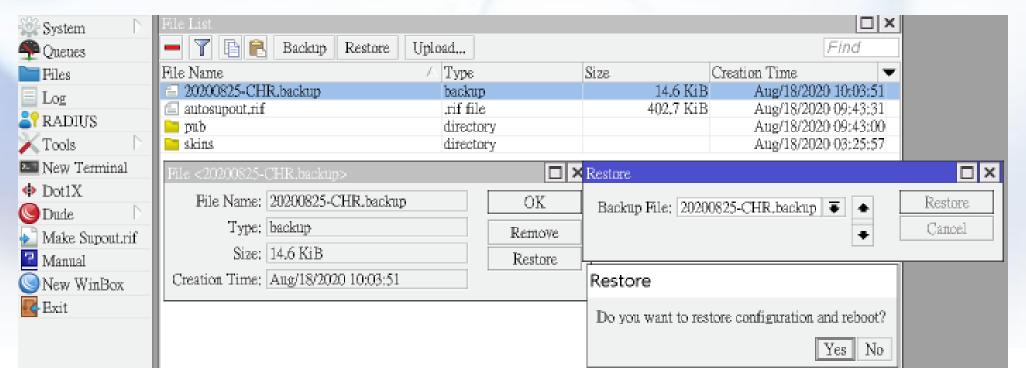
RouterOS 設定檔備份



❖/system backup load name=存檔檔名

[admin@MikroTik] > /system backup load name=20200825-CHR.backup password:
Restore and reboot? [y/N]:

Y
Restoring system configuration
System configuration restored, rebooting now



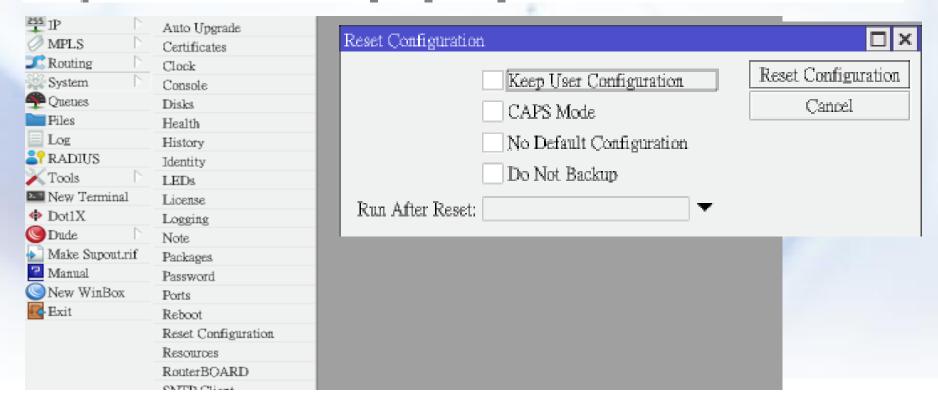
RouterOS 還原出廠預設值說明



RouterOS 還原出廠預設值:

/system reset-configuration

[admin@MikroTik] > /system reset-configuration Dangerous! Reset anyway? [y/N]:



RouterOS 使用者密碼變更說明



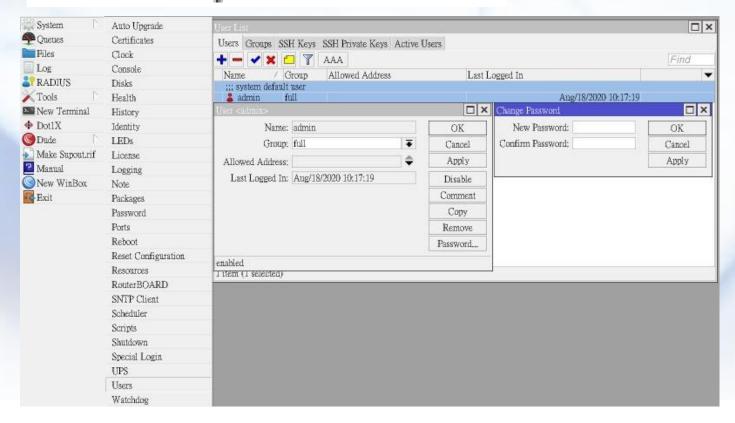
使用者密碼變更指令: /password

[admin@MikroTik] > /password

old-password:

new-password: *****

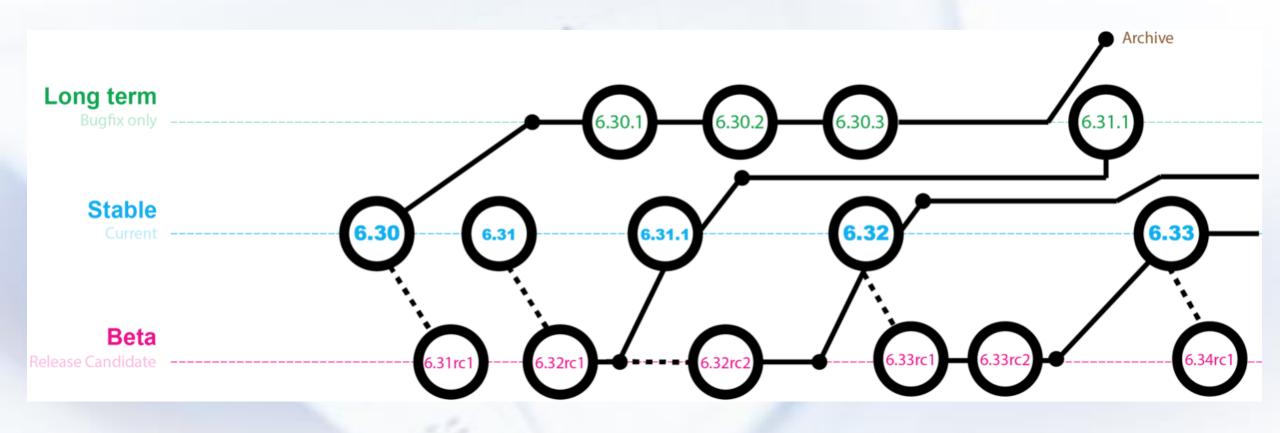
confirm-new-password: *****



RouterOS 常用功能設定介紹



❖ RouterOS 套件版本管理



RouterOS 常用功能設定介紹



RouterOS 基本設定:

- ***IP Address**
- Default Gateway
- **DNS**
- ***DHCP Server**
- **❖NTP Client**

Question

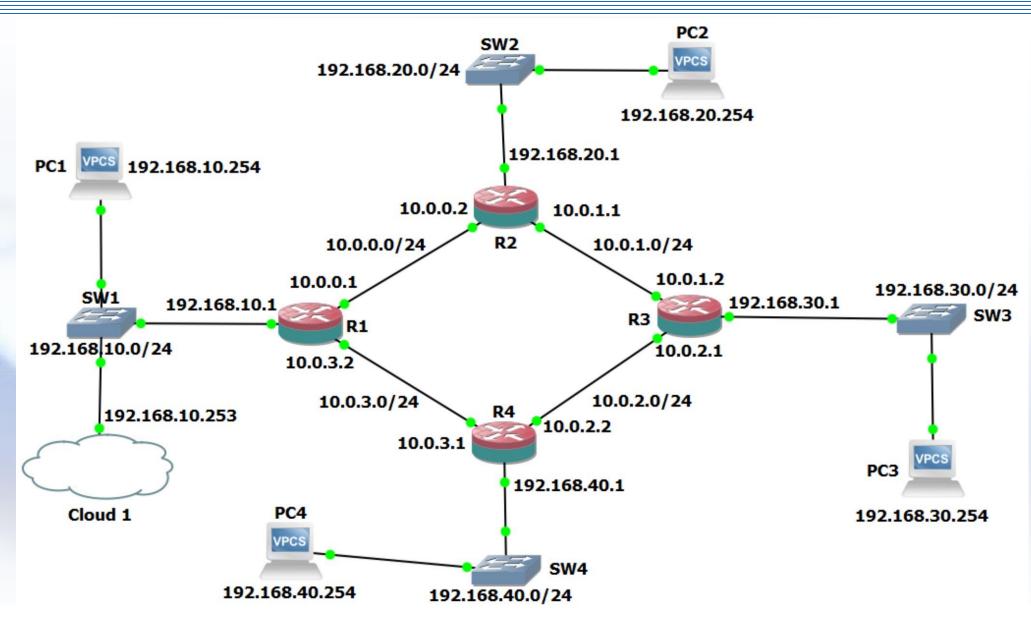


- Q1:如何使用指令設定下列呢?
- **❖IP -> Address**
- **❖IP -> Route**
- **♦IP-> DNS**
- **❖IP-> DHCP Server**
- **♦ System -> SNTP Client**
- **♦ System -> Packages**
- **❖System -> Routerboard**

Q2:如何設定非法的DHCP Server 呢?

Lab: Static Route





Lab1: Static Route 範例下載



❖範例下載: <u>https://0rz.tw/6Ea5v</u>

*QRCODE



Lab1: Static Route



R1

```
/ip address add address=192.168.10.1/24 interface=ether3 add address=10.0.0.1/24 interface=ether1 add address=10.0.3.2/24 interface=ether2 /ip route add distance=1 dst-address=192.168.20.0/24 gateway=10.0.0.2 add distance=1 dst-address=192.168.30.0/24 gateway=10.0.0.2 add distance=1 dst-address=192.168.40.0/24 gateway=10.0.3.1
```

☆ R2

```
/ip address
add address=192.168.20.1/24 interface=ether3
add address=10.0.1.1/24 interface=ether1
add address=10.0.0.2/24 interface=ether2
/ip route
add distance=1 dst-address=192.168.10.0/24 gateway=10.0.0.1
add distance=1 dst-address=192.168.30.0/24 gateway=10.0.1.2
add distance=1 dst-address=192.168.40.0/24 gateway=10.0.1.2
```

* R3

```
/ip address add address=192.168.30.1/24 interface=ether3 add address=10.0.1.2/24 interface=ether2 add address=10.0.2.1/24 interface=ether1 /ip route add distance=1 dst-address=192.168.10.0/24 gateway=10.0.1.1 add distance=1 dst-address=192.168.20.0/24 gateway=10.0.1.1 add distance=1 dst-address=192.168.40.0/24 gateway=10.0.2.2
```



```
/ip address
add address=192.168.40.1/24 interface=ether3
add address=10.0.2.2/24 interface=ether2
add address=10.0.3.1/24 interface=ether1
/ip route
add distance=1 dst-address=192.168.10.0/24 gateway=10.0.3.2
add distance=1 dst-address=192.168.20.0/24 gateway=10.0.3.2
add distance=1 dst-address=192.168.30.0/24 gateway=10.0.2.1
```



_ MikroTik RouterOS 防火牆

什麼是「防火牆」?



- ❖嘗試將「受保護程度較低」的外部區域與「受保護程度較高」 的內部區域隔離開來。
- ❖安全是一個過程,「防火牆」只是其中的一部分
- ❖ 不太安全的因素存在鍵盤和椅子之間



L1 防火牆







RouterOS 防火牆到底是在那裡呢?



參與L2的防守,不僅只有MAC Address而已...

❖ 硬體:Switch晶片上的ACL

❖軟體:Bridge介面上的ACL

RouterOS 防火牆是在那裡呢?



❖Layer2 防火牆

- Bridge → Filter
- Switch → Rule 或 Access List 及其他

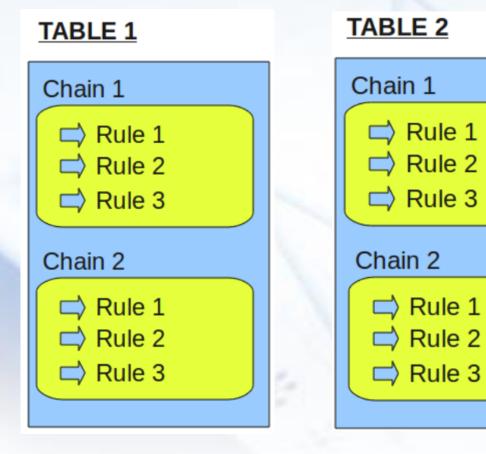
❖Layer3 (及以上)的 IPv4防火牆

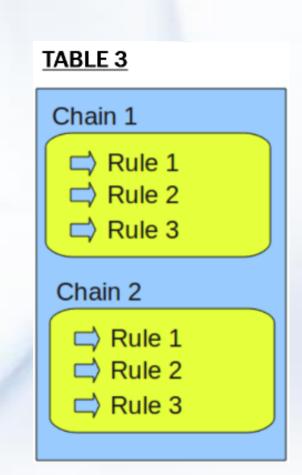
- IP → Firewall
- IP → Web Proxy
- **❖Layer3** 防火牆 IPv6
- IPv6 → Firewall

防火牆架構及基本防火牆簡介設定說明



❖L3 防火牆組成主要是由表(table)、鏈(chain)和規則 (rule)組成





防火牆架構及基本防火牆簡介設定說明



防火牆 Filter 中常用的三個鏈(chain):

* input

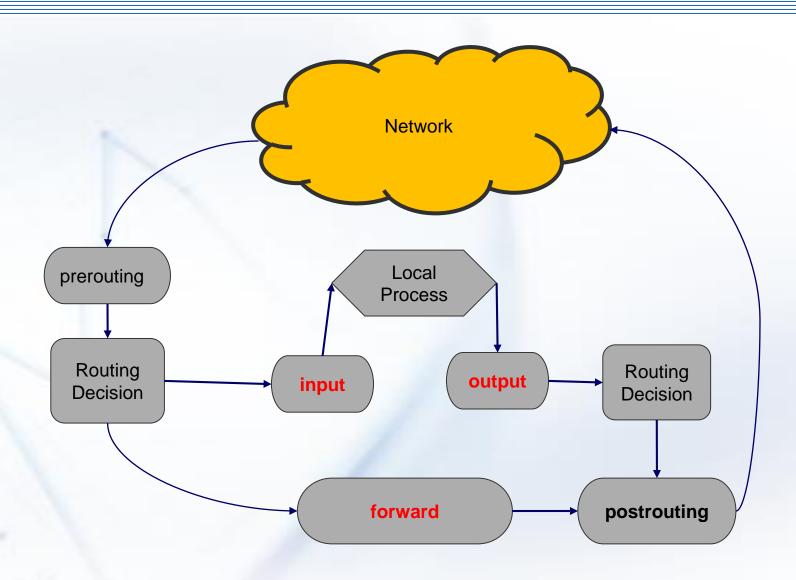
通過路由表後目的地為本 機封包

forward

通過路由表後目的地不是 本機的封包

output

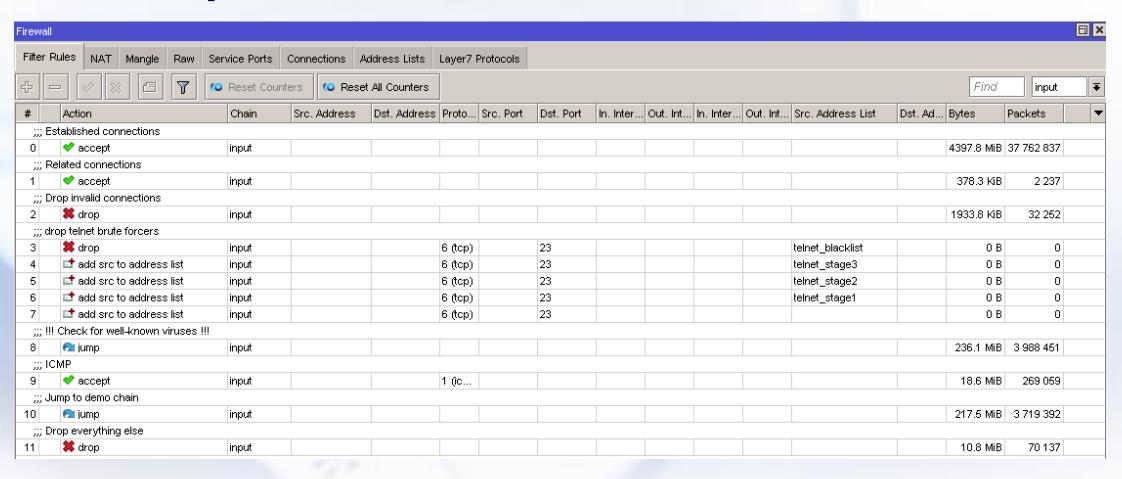
來自本機的封包向外傳送



啟動防火牆過濾Filter Rules Chain: Input



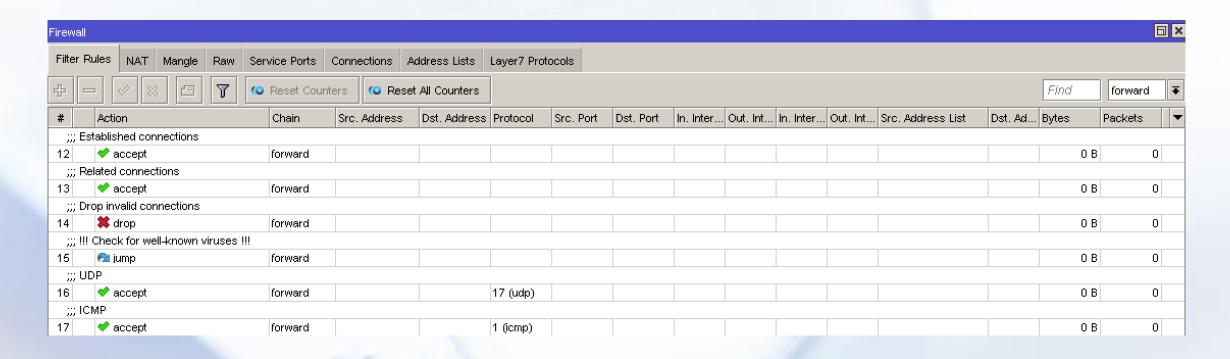
♦ Chain: Input



啟動防火牆過濾Filter Rules Chain: Forward



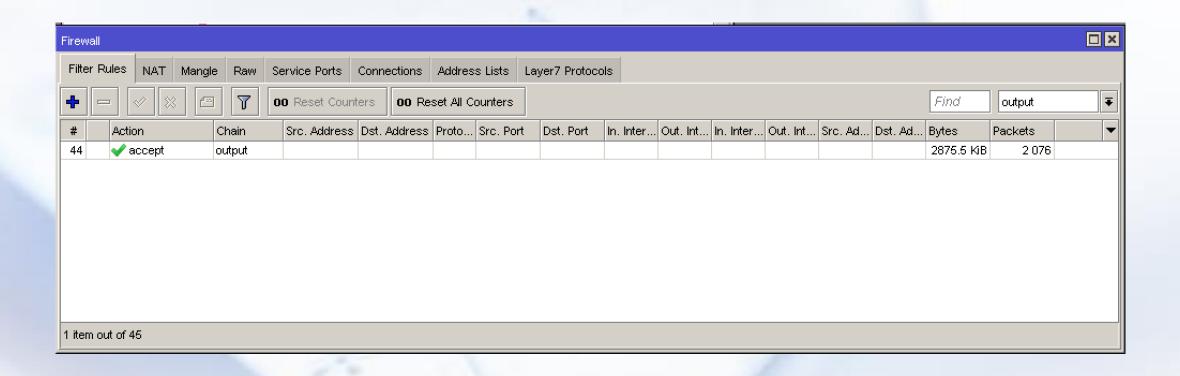
Chain: Forward



啟動防火牆過濾Filter Rules Chain: Output

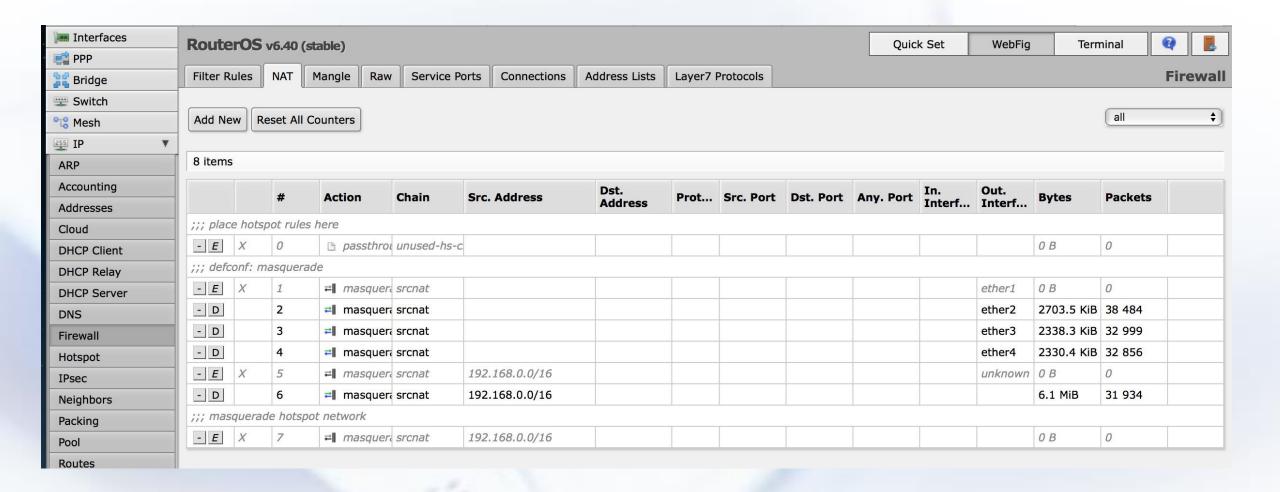


♦ Chain: Output



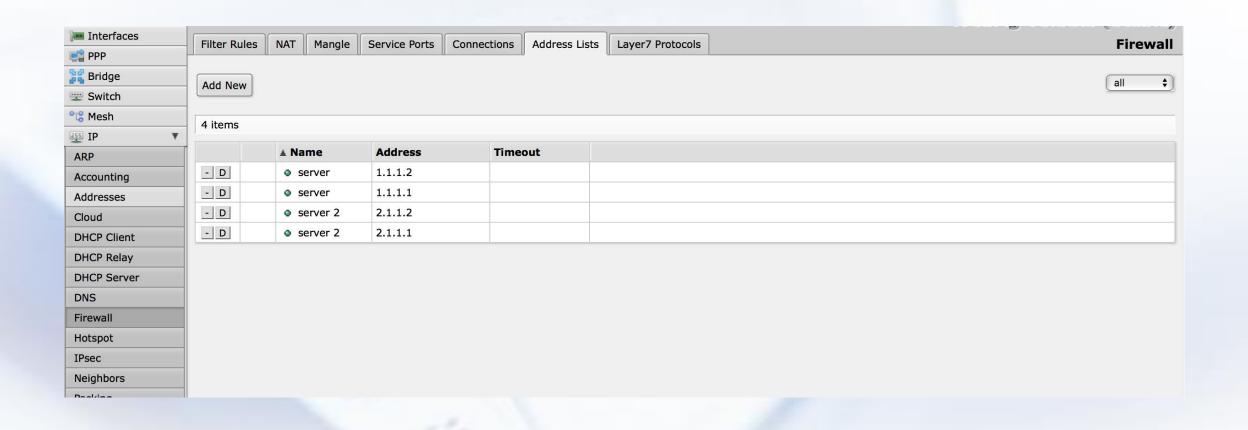
NAT 設定





Address-List





防火牆連線狀態追蹤Connection tracking



Fite	Rules NAT Mangle	Service Ports Conne	ctions Address Lists La	yer7 Protocols							
	Tracking		A Company of the Comp	CONTRACTOR CONTRACTOR						Find	
	Src. Address	Dst. Address	Reply Src. Address	Protocol	Connecti	Connecti	P2P	Timeout	TCP State	ICMP Type	
A.	10.5.8.208.58337	66.228.113.24.8291	66.228.113.24.8291	6 (tcp)	100000000000000000000000000000000000000		1	00:04:23	established		
1	10.10.0.3	224.0.0.5	224.0.0.5	89 (ospf)				00:09:17			
1	10.10.0.3:47445	66.228.113.24:161	66.228.113.24:161	17 (udp)				00:02:23			
	10.10.0.3:51186	66.228.113.24:23	66.228.113.24:23	6 (tcp)				00:00:05	close		
1	10.10.0.3.51997	66.228.113.24:80	66.228.113.24:80	6 (top)				00:00:03	time wat		
	10.10.0.3:55102	66.228.113.24.8291	66.228.113.24.8291	6 (cp)				23:59:20	established		
1	10.10.0.3.56727	66.228.113.24.22	66.228.113.24.22	6 (tcp)				00:00:04	close		
1	10.10.0.3.59423	66.228.113.24.21	66.228.113.24:21	6 (tcp)				00:00:06	time wat		
j	66.228.113.24	224.0.0.5	224.0.0.5	89 (ospf)				00:09:24			
J	66.228.113.24:22	159.148.172.205:1631	159.148.172.205:1631	6 (top)				07:41:27	established		
J	66.228.113.24:23	159.148.172.205.4566	159.148.172.205.4566	6 (top)					established		
1	66.228.113.24:80	61.247.26.243.1177	61.247.26.243:1177	6 (tcp)				21:59:32	established		
1		41.234.95.3:12701	41.234.95.3:12701	6 (tcp)					established		
1	66.228.113.24:80	58.96.34.68:4304	58.96.34.68:4304	6 (cp)				and the second s	established		
1	66.228.113.24:80		41.234.129.149:13058	6 (tcp)					established		
J	1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		125.160.169.179.51566	6 (top)					established		
J	66.228.113.24:80	77.48.235.215.8530	77.48.235.215.8530	6 (tcp)				05:49:42	established		
1	66.228.113.24:80	41.234.95.3:12700	41.234.95.3:12700	6 (tcp)				06:52:46	established		
J	66.228.113.24:80	A Principle and the second of	217.52.99.170.3269	6 (tcp)					established		
J	66.228.113.24:80	65.5.222.47.50726	65.5.222.47:50726	6 (tcp)				10:42:12	established		
J	66.228.113.24:8291	41.233.48.14.50087	41.233.48.14:50087	6 (top)					established		
1	66.228.113.24:8291	189.58.32.236.1484	189.58.32.236:1484	6 (top)					established		
1	66.228.113.24:8291	41.236.252.35.52727	41.236.252.35.52727	6 (top)					established		
1		189.58.32.236.1478	189.58.32.236:1478	6 (tcp)					established		
1	66.228.113.25	224.0.0.5	224.0.0.5	89 (cspf)				00:09:24			
A	80.93.248.214:2050	66.228.113.24.8291	66.228.113.24:8291	6 tcp)					established		
1	The second secon	66.228.113.24.8291	66.228.113.24:8291	6 (cp)					established		
	80.93.249.97:3687	66.228.113.24.8291	66.228.113.24:8291	6 (cp)				M.7177, 127	established		
	159.148.172.205:3160		66.228.113.24:161	17 (udp)				00:02:24			
1	159.148.172.205:4177		66.228.113.24.23	6 (cp)				00:00:00			
	159 148 172 205:4336	Commission of the Commission o	66 228 113 24:22	6 (cp)				00:00:02			
	159 148 172 205:4403	Control of the Contro	66.228.113.24:21	6 (cp)				00:00:04			
1	159.148.172.205:4512	CO PER SON CONTRACTOR DE LA CONTRACTOR D	66.228.113.24:80	6 (tcp)	the second secon				time wat		
	159.148.172.205:4939	700 01 000 01 1 1 1 1 1 1 1 1 1 1 1 1 1	66.228.113.24.8291	6 (cp)					established		
A	193.189.117.122:42		66.228.113.24:161	17 (udp)				00:01:40			
A	193.189.117.122:42		66.228.113.24:161	17 (udp)				00:01:40			
9 te			Max Entries: 9830					20000			-

防火牆Layer7 Protocols





Question



Q1: 如何利用防火牆擋臉書 Facebook?

A1: MikroTik Facebook Block Script:

/ip firewall layer7-protocol add name=facebook regexp="^.+(facebook.com).*\$"
/ip firewall filter add chain=forward protocol=tcp dst-port=80,443 layer7-protocol=facebook action=drop comment="Block Facebook"

❖Q2: 如何利用防火牆擋住UDP 139,445 Port?

A2: MikroTik Block UDP 139,445 Script:

/ip firewall filter add chain=forward protocol=udp dst-port=139,445 action=drop

Q3: 如何利用防火牆做NAT位址轉換(118.163.8.254:53->192.168.10.20:514)

呢?

A3: MikroTik NAT mapping Script:

/ip firewall nat add chain=dstnat action=dst-nat to-addresses=192.168.10.20 to-ports=514 protocol=udp dst-address=118.163.8.254 dst-port=53



MikroTik RouterOS 認證網頁功能CWP



圖片來源:

endlessorigami.com

基本生存需求

以前



- ・食物・飲水
- ・庇護・衣物

現在



・網路

·水·庇護·衣物(可選)

真實新聞事件





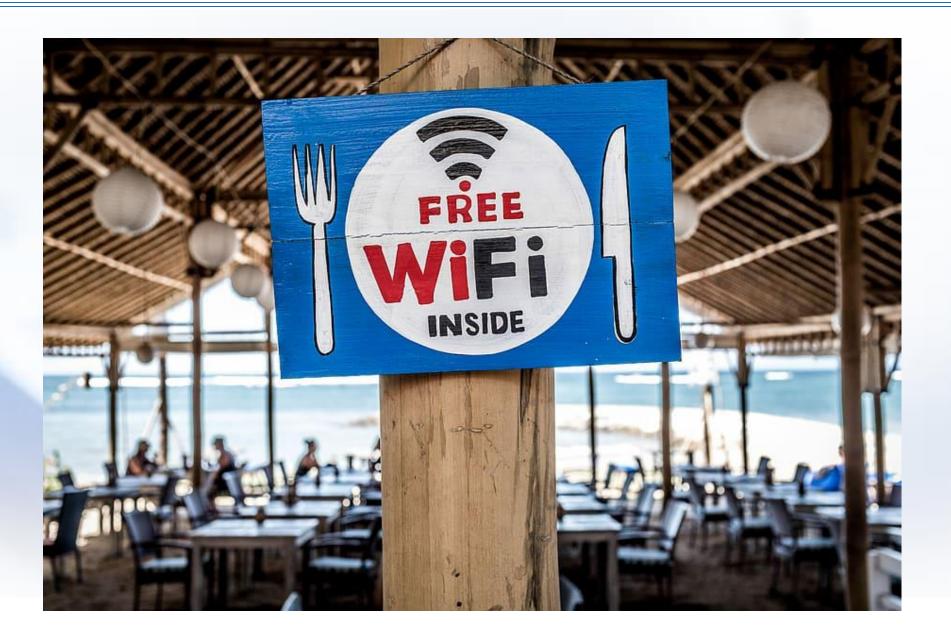
圖片來源: Mobilisation Nationale Wakashio

2020年7月25日一艘日本貨輪「若潮號」 偏離航道最後在非洲 東南方的「模里西斯」 外海擱淺並造成原油 外洩。

發生原因: 船員為了 要連陸地上的WiFi

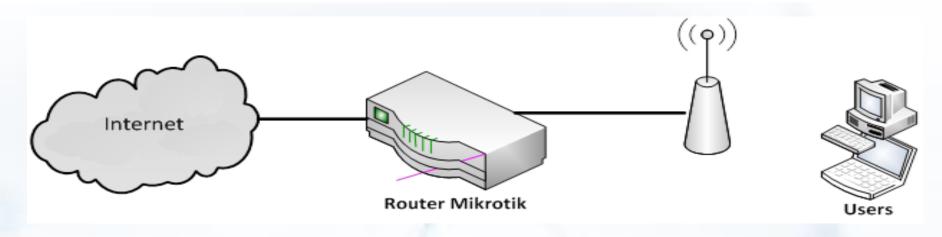






認證網頁功能CWP(Captive Web Portal)





MikroTik 內建的Hotspot 有那些功能呢?

- 1. 頻寬限制(網路速度限制或流量配額限制)
- 2. Hotspot Server多種認證方法
- 3. 可排除不需要認證的裝置或IP
- 4. 自訂Hotspot網頁
- 5. 廣告系統
- 6. 與社群網站API整合



❖ 適用地方:旅館





❖ 適用地方:學生宿舍





❖ 適用地方:公車





❖ 適用地方:公車站牌



認證網頁功能CWP



適用地方:機場



認證網頁功能CWP

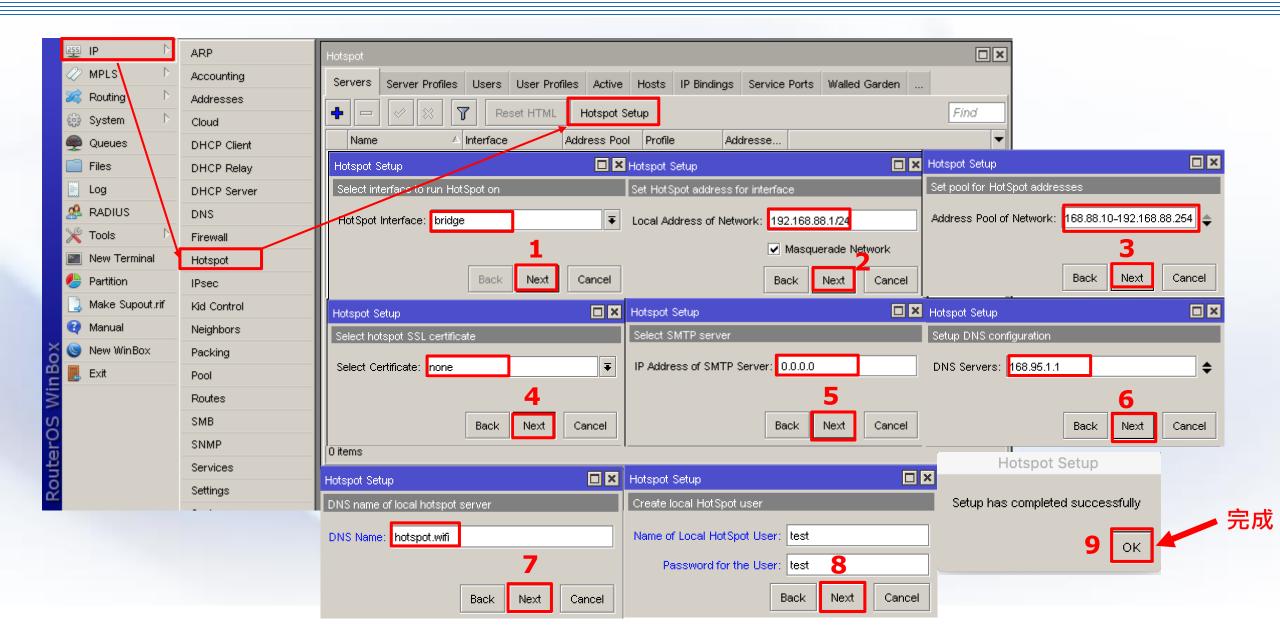


❖ 適用地方:遊客中心



認證網頁功能CWP-Hotspot 快速設定



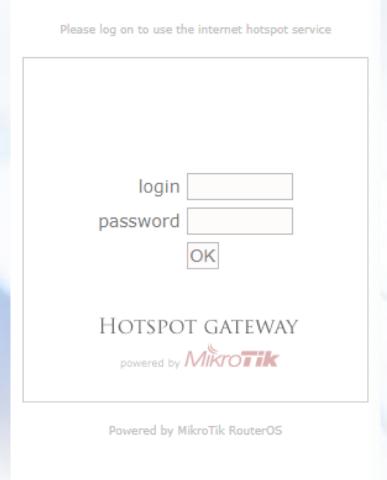


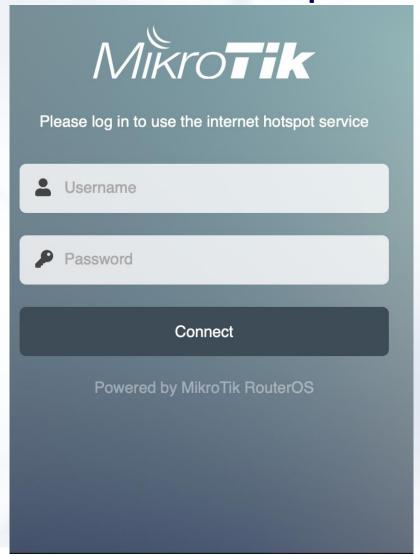
認證網頁功能CWP-預設登入頁面



RouterOSv6.47版以前的Hotspot預設登入頁面

RouterOSv6.47版以上Hotspot預設登入頁面





認證網頁功能CWP-登入頁面自訂





登入 取消

為提升服務品質



English

熱點查詢 使用說明

iTaiwan無線上網服務使 用條款

您好,歡迎使用iTaiwan無線上網服務(以下簡稱本服務)。

為保障您的使用權益,請於使用本服務之前,詳細閱覽iTaiwan無線上網服務使用條款(以下簡稱本條款)內容。一旦您接受並點選開始上網者,即表示同意本服務規範及以下所有條款內容。

一、使用者行為規範

我同意&免費上網

客服電話:0800-081-051

國家發展委員會 版權所有 ©copyright 2011 無線上網服務規章 聯絡我們

認證網頁功能CWP-登入頁面自訂







三、MikroTik RouterOS 8大網管工具介紹

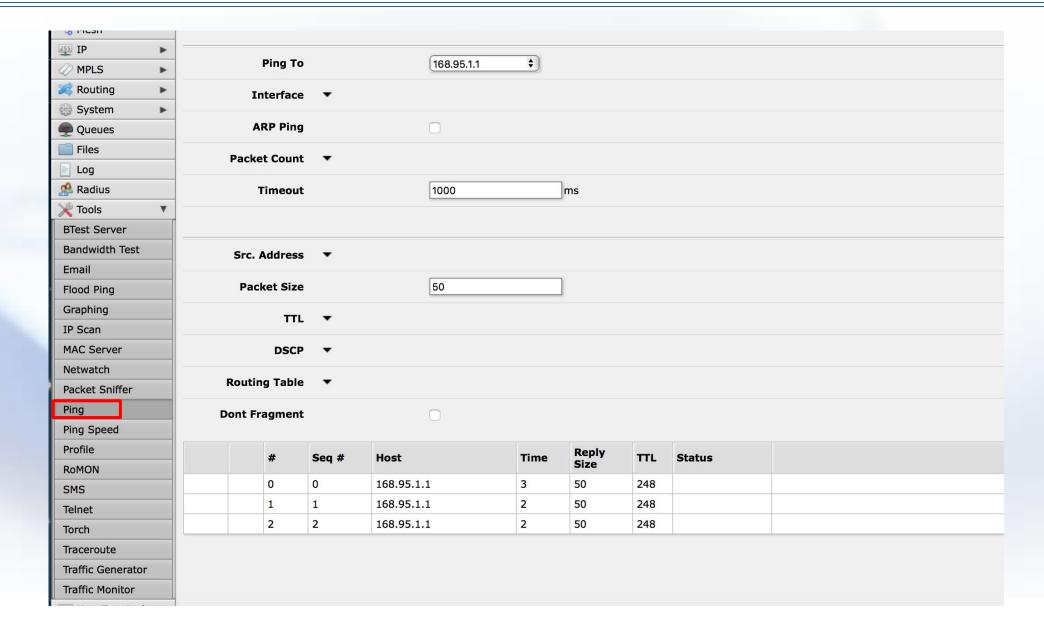
RouterOS 工具 **Traceroute**



Interfaces		Start Sto		Close											
Bridge		Start Sto	<u>ір</u>	Close											
Switch Switch								1							
PPP PPP		Tracero	ute To			0.0.0.0									
ଂଞ୍ଜ Mesh		Packe	et Size			56		1							
255 IP	>							-							
Ø MPLS	•	Ti			1000 ms										
Routing	>	Pr	otocol			icmp \$									
⊕ System	>		OLOCO.			Tomp 4									
Queues			Port			33434									
Files															
Log		US	e DNS												
A Radius			Count	•											
× Tools	*														
BTest Server		Max	Hops	•											
Bandwidth Test		Src. Ac	ddroee	~											
Email		SIC. A	uui CSS	•											
Flood Ping		Int	erface	•											
Graphing															
IP Scan			DSCP	•											
MAC Server		Routing Table		•											
Netwatch		_													
Packet Sniffer			#	Нор	Host		Loss	Sent	Last	Avg.	Best	Wors			
Ping				1	1							1.0.0			
Ping Speed															
Profile															
RoMON															
SMS															
Telnet															
Torch															
Traceroute															

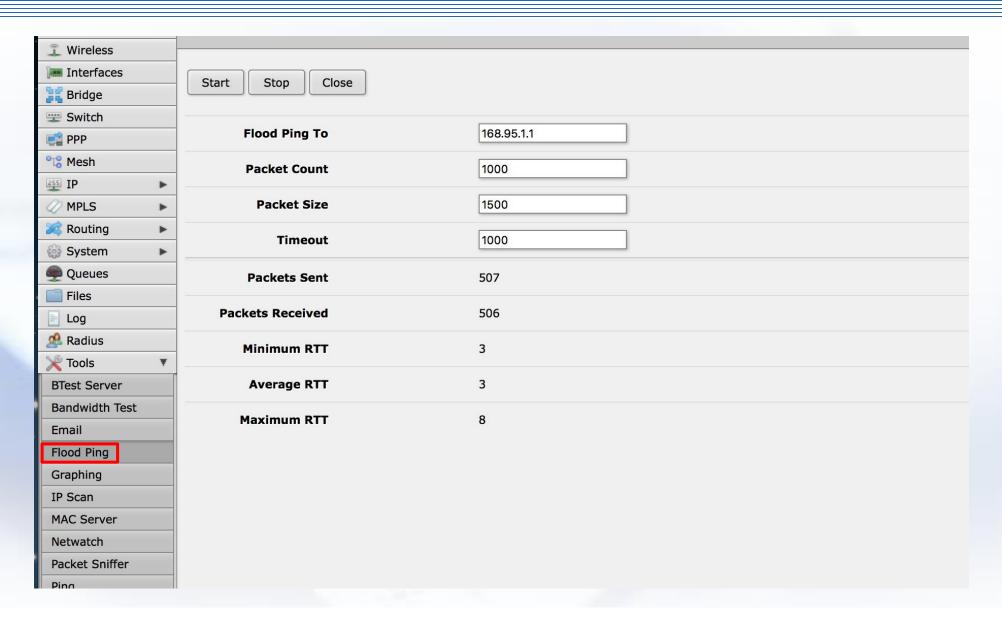
RouterOS 工具 Ping





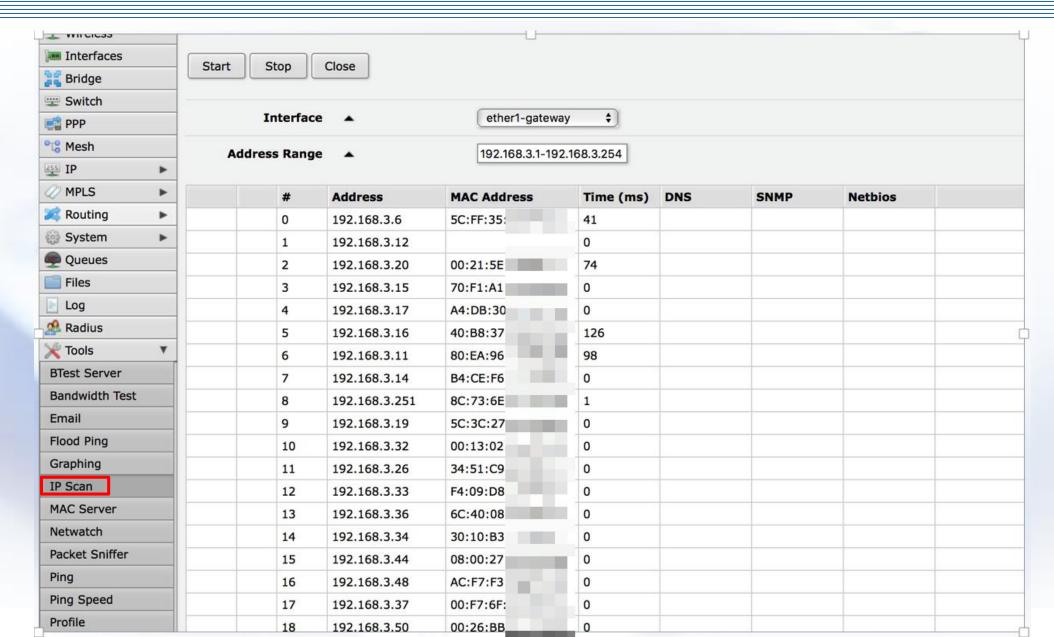
RouterOS 工具 Ping、Flood Ping





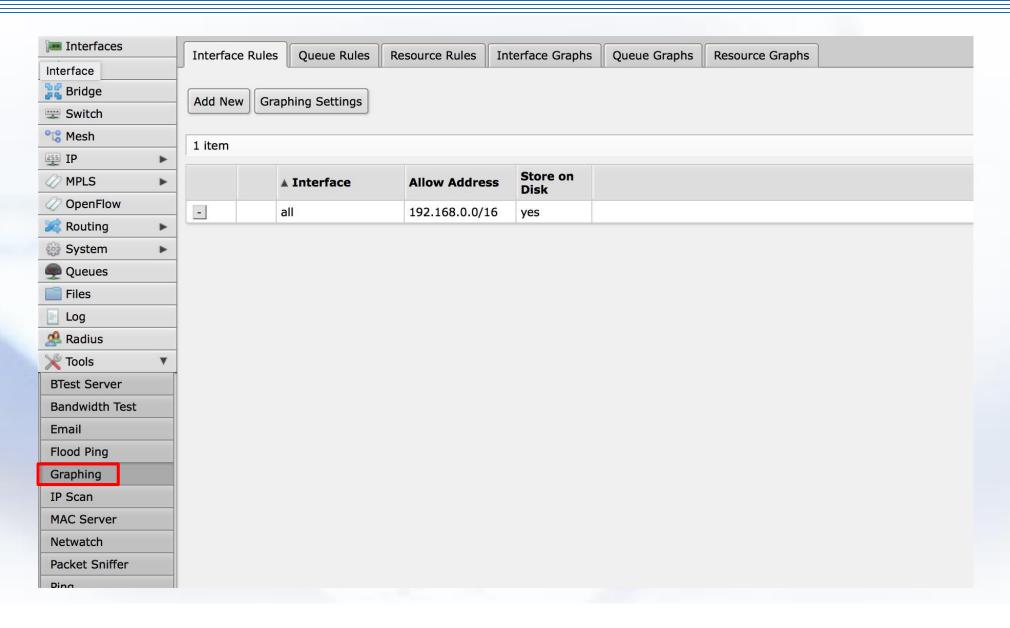
RouterOS 工具 IPScan





RouterOS 工具 Graphing





RouterOS 工具 Profiler



Rridge		Start	Stop	Close		
Switch		Start	Этор	Close		
™ Mesh						
255 IP	-		#	Name	▼ Usage	
Ø MPLS	•		4	idle	94.0	
OpenFlow			5	profiling	5.0	
🤾 Routing	-		0	www	0.5	
System	-		3	management	0.5	
Queues			1	firewall	0.0	
Files			2	networking	0.0	
Log						
🤼 Radius						
× Tools	*					
BTest Server						
Bandwidth Test						
Email						
Flood Ping						
Graphing						
IP Scan						
MAC Server						
Netwatch						
Packet Sniffer						
Ping						
Ping Speed						
Profile						
RoMON						

RouterOS 工具 Torch



Mesh								Basic								Filters
<u>≥55</u> IP	Interface			athor1		<u> </u>		Src. Address		0.0	0.0.0.0/0		7			
Ø MPLS ▶	Interrace			ether1 💠						310. 7	o.o.o.o/0					
Routing	Entry Timeout		: [00:00:03 s			Dst.		Dst. A	Dst. Address 0.0.0.0/0		.0.0/0				
System >										Suc Ac	droce	/	\		7	
Queues								Collect		Src. Ad	dress6	::/0)			
Files			· ·	Src. Ac	ldress		Dst. Addres	ss		Dst. Ad	dress6	::/0)			
Log Radius																
E LCD				Src. Ac	ldress6		Dst. Addres	ss6		MAC P	rotocol	all		*)		
¥ Tools ▼				MAC Pr	otocol		Protocol			Р	rotocol	any	/	†)		
BTest Server																
Bandwidth Test				Port			VLAN Id				Port	lany	/	\$)		
Email				DSCP						V	LAN Id	any	/	*		
Flood Ping																
Graphing											DSCP	any	/-	(
IP Scan																
MAC Server		#	Eth. Protocol	Pro	Src.		Dst.		VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Packet	Rx Packet		
Netwatch			Protocoi						Iu				Rate	Rate		
Packet Sniffer																
Ping																
Ping Speed																
Profile																
RoMON																
SMS																
Telnet																
Torch																
Traceroute																
Traffic Generator																
Traffic Monitor																

RouterOS 工具Packet Sniffer



Interfaces		Apply Start St	Stop Packets Connections Hosts Protocols	
PPP PPP		Apply	Tackets Connections Noses 110cccols	
Bridge		stopped		
Switch		заорреа		
°t Mesh				General
255 IP	•			
Ø MPLS	•	Memory Limit	100000 kb	
Routing	•	Only Headers		
System	•			
Queues		File Name	raidus.pcap	
Files		Pila I imia	400000	
Log		File Limit	100000 kb	
A Radius			c	Streaming
E LCD				, cr carriing
× Tools	•	Streaming Enabled		
BTest Server		Server	0.0.0.0	
Bandwidth Test				
Email		Filter Stream		
Flood Ping				
Graphing				Filter
IP Scan		Interfaces	▼ (all •) ▲	
MAC Server				
Netwatch		MAC Address	▼	
Packet Sniffer		MAC Protocol	•	
Ping				
Ping Speed		IP Address	▼	
Profile		IP Protocol	▼	
RoMON		IP Protocor	·	
SMS		Port	▼	
Telnet				
Torch		Direction	any 💠	



簡報完畢 敬請指教

顯 赫 資 訊 股 份 有 限 公 司

Gentrice technology Company Limited

地址:新北市中和區中正路738號15樓之5

Email: service@gentrice.net

電話:02-8226-9200