

MTRB for Home Lab



Multi-Purpose Mikrotik Router Board

for ... XaaS use

MikroTiK User Meeting

first-most MUM

Yangon, Myanmar

Speaker Brief

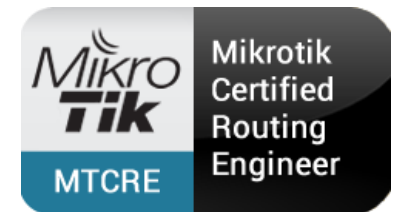
BroNaing – Senior Core Network Engineer, YTP ISP
Yatanarpon Teleport Public Company Ltd.

- fresh MTCNA, MTCRE just 2015 Aug; thanks to Phyo & Makito
- MCITP Server Admin
- MCSA +Security +Messaging since 2008
- CCNA, ECSA/CEH, RHCSA, RHCE candidate
- various Linux, FOSS and NOS user since 2001
- + familiar with sort of Virtualizations and Hypervisors

*** end users in any Industry, SOHO, MNC to ISP Core, IXP traffic flow is our concern ***



MikroTik Certified Network Associate



Speaker Background

- 15 years in ICT industry, *just simple end user actually*
- 7+ years in Service Provider, Solution Design, Procurement + Troubleshooting & Support
- DNS, Mail and other ISP Application Admin
 - Routing, Switching, Firewall, Security Engineer
 - Application Development, SE & QC, Scripting, ...
 - Linux, DBMS, FOSS System Deployments
- ***WHY*** server, App, Sec, R&S guy ***into MikroTik(s) ?***



MTRB for Everybody

- **For Home** starting with my very first little step into MTRB
- **Everyday SOHO, SME, Enterprise Use Cases**
 - **Router**, Switch Equipment @ effortable budget
 - DHCP, local DNS cache, web proxy, ...
 - WiFi **HotSpot** manager, billing solutions
 - Stateful Firewall, NAT, VPN gateway, ...
 - BlackHole, Bogons, attack & route filters
 - SNMP ready, NTP and SysLog, ... further analysis

MTRB Day #1 HOWTO

- grab my first MTik unit, then, START until satisfied
 - RB750G (no WiFi.. Oops! yet like its HW spec:
5x 10/100/1000 eth ports, 680MHz CPU MIPS-BE, 32MB RAM, 1x PoE in)
 - http://wiki.mikrotik.com/wiki/Manual:Product_Naming
- Discovered how user friendly & easy to manage
 - WinBox or web GUI + ssh /telnet, even handhelds
 - login by **MAC** address, console OR **192.168.88.1**
 - got many WINE based clients for Mac OSx
- my next Mikrotiks... ???
 - VM, next ones with 3G, RB800, 951, CCR, CRS, microSD/SSD caches ...

Understanding MTRB Model and Naming

growing interest on models, features, ... (**naming convention**)

RB750G

Series RB 7 ; 5 ports ; G for gigabit port

<board name> <board features>-<build-in wireless> <wireless card features>-<connector type>
-<enclosure type>

RB 95 1 Ui – 2 HnD (widely used here)

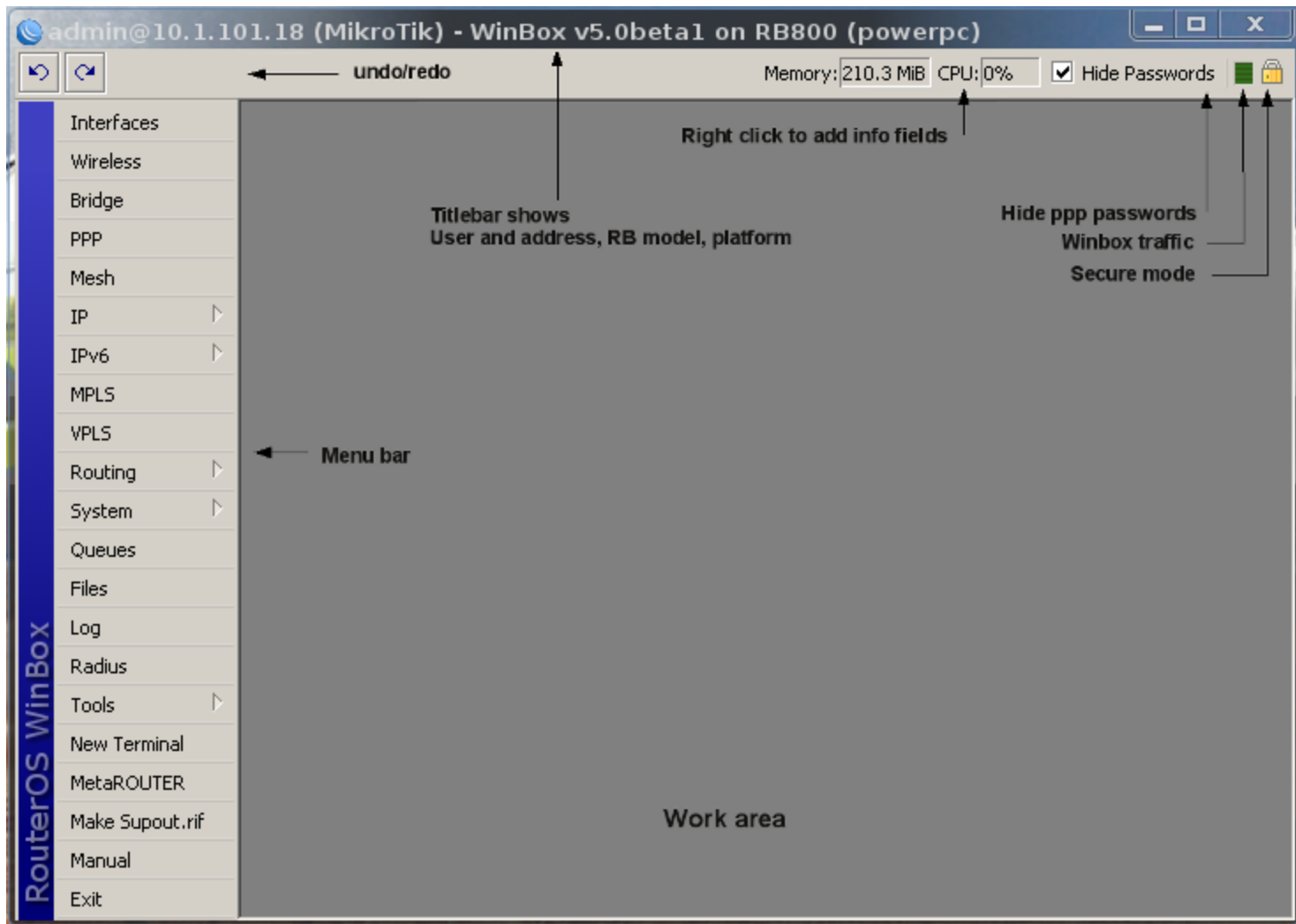
USB port, **i** = Power injector, **n** = 802.11n WiFi

H high performance CPU, **A** adv in RAM, license

2 for 2.4GHz wireless, **D** dual chain antenna

Ref: http://wiki.mikrotik.com/wiki/Manual:Product_Naming

WinBox



- Be sure to config with comments for better documentation :P
<http://wiki.mikrotik.com/wiki/Manual:Winbox>

<http://wiki.mikrotik.com/wiki/Manual:Quickset>

admin@D4:CA:6D:02:B5:65 (m750n) - WinBox v6.32.1 on RB750 (mipsbe)

Sessions Settings Dashboard

Safe Mode Session: D4:CA:6D:02:B5:65

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit

Firewall

Filter Rules

#	Action
0	dst
1 X	acc
2	dst
...	default con
3 X	ma
4	ma

5 items

Ethernet Quick Set

Configuration

Mode: ☒ Router ☐ Bridge

Internet

Address Acquisition: ☒ Static ☐ Automatic ☐ PPPoE

IP Address: 192.168.2.22

Netmask: 255.255.255.0 (/24)

Gateway: 192.168.2.1

DNS Servers: 10.10.10.10
10.10.10.11
8.8.4.4

MAC Address: D4:CA:6D:02:B5:61

Local Network

IP Address: 192.168.4.4

Netmask: 255.255.255.0 (/24)

☐ Bridge All LAN Ports
☐ DHCP Server
☐ NAT

VPN

☐ VPN Access

VPN Address: 467802dfd017.sn.mynetname.net

Src. Port	Dst. Port	In. Inter...	Out. Interface	Bytes	Packets
	80			0 B	0
	80			0 B	0
	80			1819.7 KB	33 255
			ether1-gateway	0 B	0
			ether1-gateway	1832.8 KB	28 797

No Joke! RB system with/without wireless wizards may be a bit different.

See! : more QuickSets with hAP Lite

admin@192.168.3.166 (MikroTik) - WinBox v6.32.2 on hAP lite (smips)

Sessions Settings Dashboard

Safe Mode Session: 192.168.3.166

Quick Set

WISP AP Quick Set

Configuration

Mode: ☒ Router ☐ Bridge

Internet

Address Acquisition: ☐ Static ☒ Automatic ☐ PPPoE

IP Address: Renew Release

Netmask:

Gateway:

MAC Address: 4C:5E:0C:F0:B8:2B

Local Network

IP Address: 192.168.3.166

Netmask: 255.255.255.0 (/24)

☐ DHCP Server

☒ NAT

Enable CAPsMAN Support

VPN

☐ VPN Access

VPN Address: 5b320480a8fc.sn.mynetname.net

System

Router Identity: MikroTik

Network Name: mtH1

Frequency: auto MHz

Band: 2GHz-B/G/N

Channel Width: 20/40MHz Ce

Country: thailand

MAC Address: 4C:5E:0C:F0:B8:2F

☐ Use Access List (ACL)

Security: ☐ WPA ☐ WPA2

Wireless Clients

MAC Address	In ACL	Last IP	Uptime	Sign
-------------	--------	---------	--------	------

Enjoying my first hour with MT, as a real dummy user!! Cheers, well done, Mikrotik!

mum

Myanmar 2015 Oct

Plan, Plug, Config, Monitor, Tune, ...

- Be sure to config with comments for better documentation :P and easy future use
- Follow usual deployment cycle
 - Use
 - Monitor
 - Modify/tune
 - loop that
- Stay in communities, forums, study from MIK Experts' best and usual practices + samples ...
- Passing my requirements /objectives here, my TIK Seniors & experts would present details:

MTRB Home Labs

- QuickSet Wizard (really my dummy approach)
- discovering MNDP/mac, reset to default,...
- Switch, Router, Bridge, vLANs, ... WOOOW!
 - all done with single Router Board OS
 - Full feature without much limitations to series/models
 - Any port can be your WANx, LAN, bridge ports, ...
 - Enjoy power of your gateway box by level of license
 - wow... up to BGP, OSPF, RIP, ISIS, MPLS support, + IPv6, ...
 - Incredible +++ ;
highly versatile, cost effective, customizable, extendable, ..

RB750 played at home lab

- Feel it is like a Linux box,
better than traditional dummy NAT routers
at MIK's same or ½ price 😊
- No Wi-Fi with RB750, so, using TP-Link and LinkSys
DWRT on LAN ports as my Wi-Fi AP 😞
- Definitely enjoying power of HotSpot functions and
customization in RB 750 +++ 😊

haP Lite played at home lab

- Easy HotSpot config & built-in Wi-Fi system 😊
 - Its Wi-Fi usable capacity 😞 , License Level 😞
 - Yet, enough for my ~25 household gadgets/PC 😊
 - Can integrate with existing AP and Repeaters wirelessly ???
???? ; I always need help on Radio/wireless distribution
 - better than DWRT 😊
-
- *++ Not needed complex, expensive, power and space consuming platforms for Wi-Fi hotspot; no giant server, nor external DB/ AD/LDAP/radius needed.*
- Home 802.1X/EAP Auth, all simply done by Mikrotik 😊**
- <http://www.mikrotik.com/testdocs/ros/3.0/pnp/hotspot.php> and Google

x86 VM Mikrotik + PfSense gw Proxy

- got ADSL; and vPro, 8GB RAM with 250G + 1T HDD refurbished operational HP workstation
 - Installed ESXi6 VMWare Hypervisor on it /**Existing Infra**/
 - Installed Slackware **SinkHole DNS** resolver VM (1G vRAM)
 - Installed PfSense BSD gateway, Squid 3 and Dansguardian (with 300G caching HDD space and 6G vRAM)
 - ** Installed Mikrotik x86 VM appliance with 512M RAM
- Config the systems, VM and all basic Network, management and right data traffic flow for above servers in a DMZ before distributing to an external switch and dummy WiFi-AP...
- *** **MT is the Boss/Joker here finishing Home Wi-Fi HotSpot**

x86 Mikrotik HotSpot VM+ PfSense gw Proxy

192.168.2.9 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Inventory Inventory

192.168.2.9

- betaDev
 - ut_7-2
- ProD
 - gpfs2
 - mk620a
 - pfs1_7-77
 - sDNS1_
 - siDNS

e2 VMware ESXi, 6.0.0, 2494585

Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Users Events Permissions

Configuration Issues

ESXi Shell for the host has been enabled
SSH for the host has been enabled

General

Manufacturer:	Hewlett-Packard
Model:	HP Compaq dc7800p Small ...
CPU Cores:	2 CPUs x 2.327 GHz
Processor Type:	Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz
License:	VMware vSphere 6 Hypervisor - Licensed for 1 physical CP...
Processor Sockets:	1
Cores per Socket:	2
Logical Processors:	2
Hyperthreading:	Inactive
Number of NICs:	3
State:	Connected
Virtual Machines and Templates:	6
vMotion Enabled:	N/A
VMware EVC Mode:	Disabled

Resources

CPU usage: **2384 MHz** Capacity 2 x 2.327 GHz

Memory usage: **5998.00 MB** Capacity 8111.21 MB

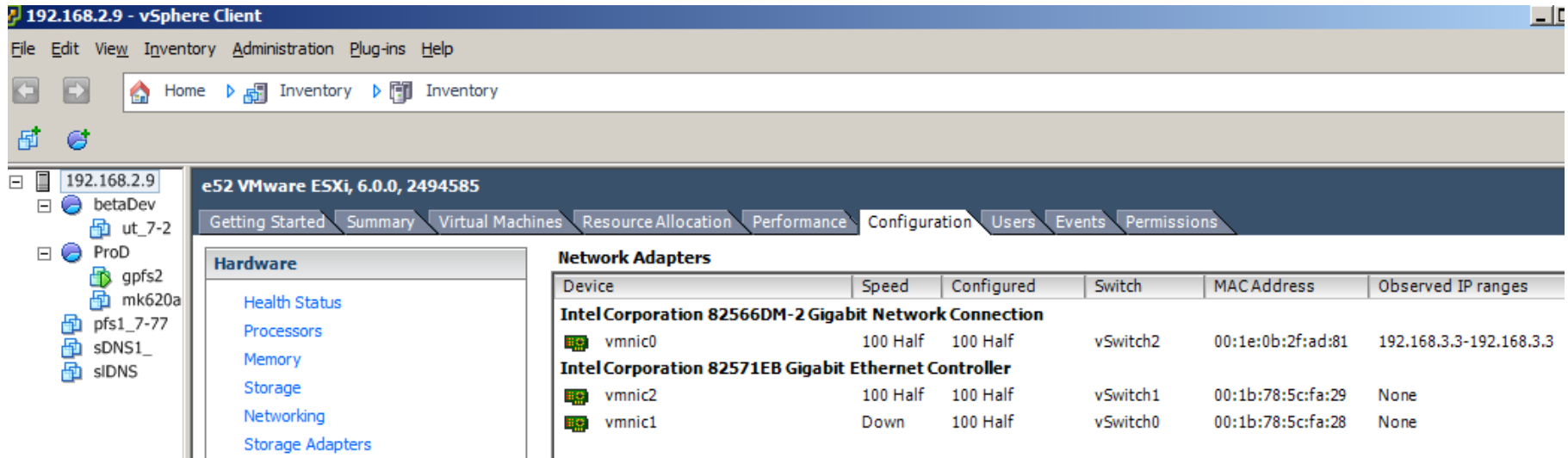
Storage	Drive Type	Capacity	Free
datastore1	Non-SSD	225.25 GB	22%
dt2	Non-SSD	815.25 GB	69%

Network	Type
VMtestNet	Standard port group
vn2_xDSL	Standard port group
cWiFi	Standard port group

Fault Tolerance

HotSpot in a Can, powered by VMWare and Mikrotik

x86 Mikrotik HotSpot VM+ PfSense gw Proxy ..



192.168.2.9 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Inventory Inventory

192.168.2.9

betaDev
ut_7-2
ProD
gpfs2
mk620a
pfs1_7-77
sDNS1_
sIDNS

e52 VMware ESXi, 6.0.0, 2494585

Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Users Events Permissions

Hardware

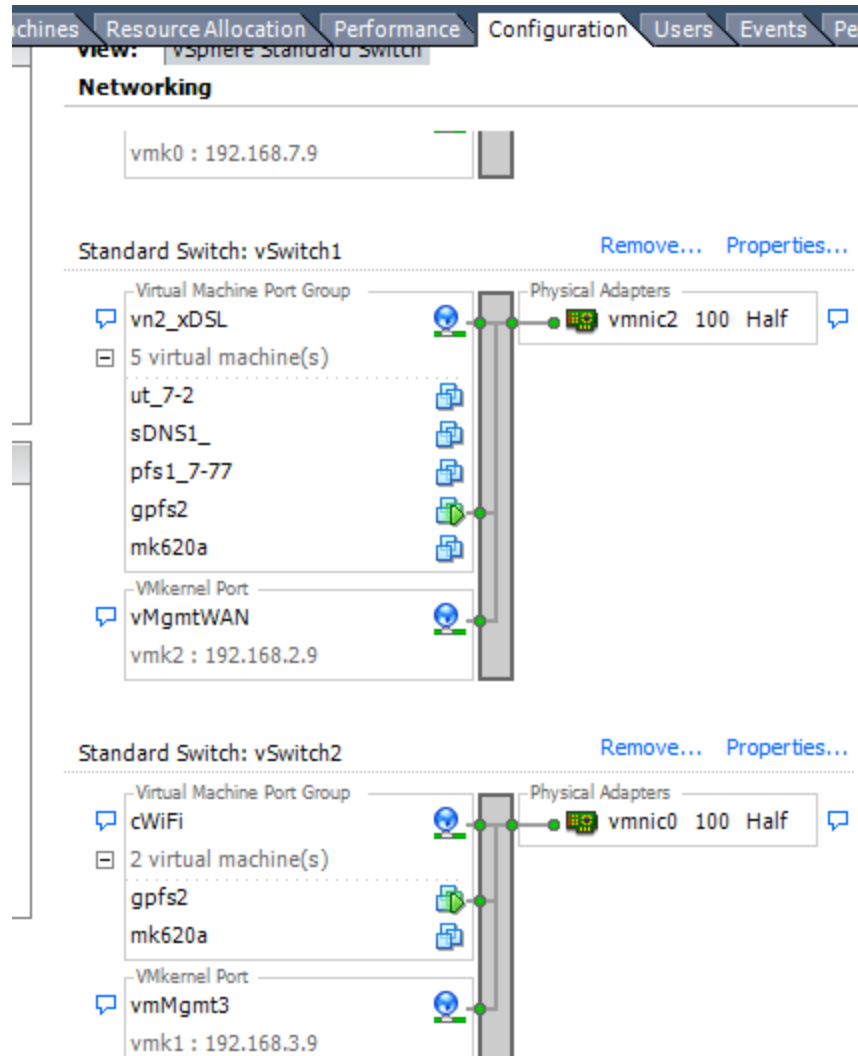
- Health Status
- Processors
- Memory
- Storage
- Networking
- Storage Adapters

Network Adapters

Device	Speed	Configured	Switch	MAC Address	Observed IP ranges
Intel Corporation 82566DM-2 Gigabit Network Connection					
vmnic0	100 Half	100 Half	vSwitch2	00:1e:0b:2f:ad:81	192.168.3.3-192.168.3.3
Intel Corporation 82571EB Gigabit Ethernet Controller					
vmnic2	100 Half	100 Half	vSwitch1	00:1b:78:5c:fa:29	None
vmnic1	Down	100 Half	vSwitch0	00:1b:78:5c:fa:28	None

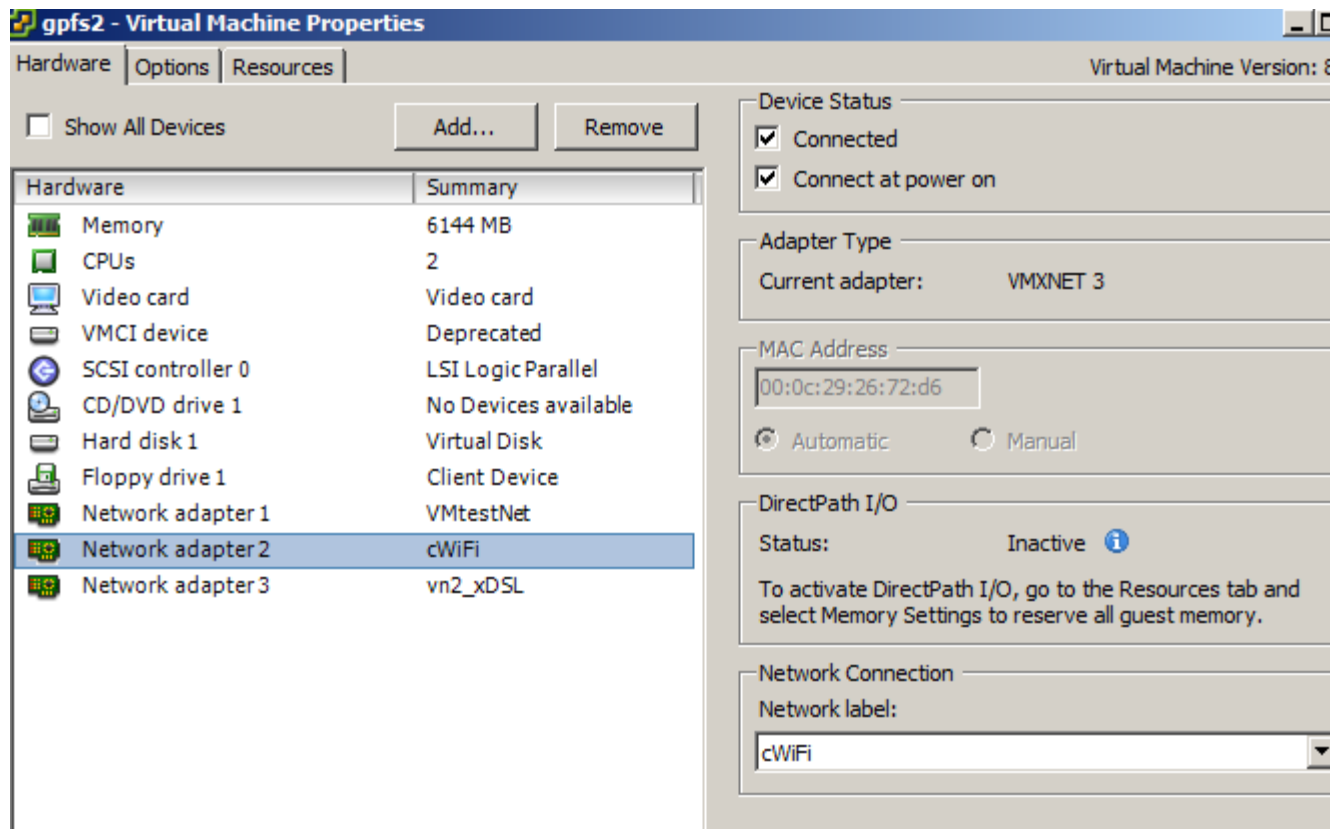
Added 2 ports PCIE NIC card and config VMnet

x86 Mikrotik HotSpot VM+ PfSense gw Proxy ..



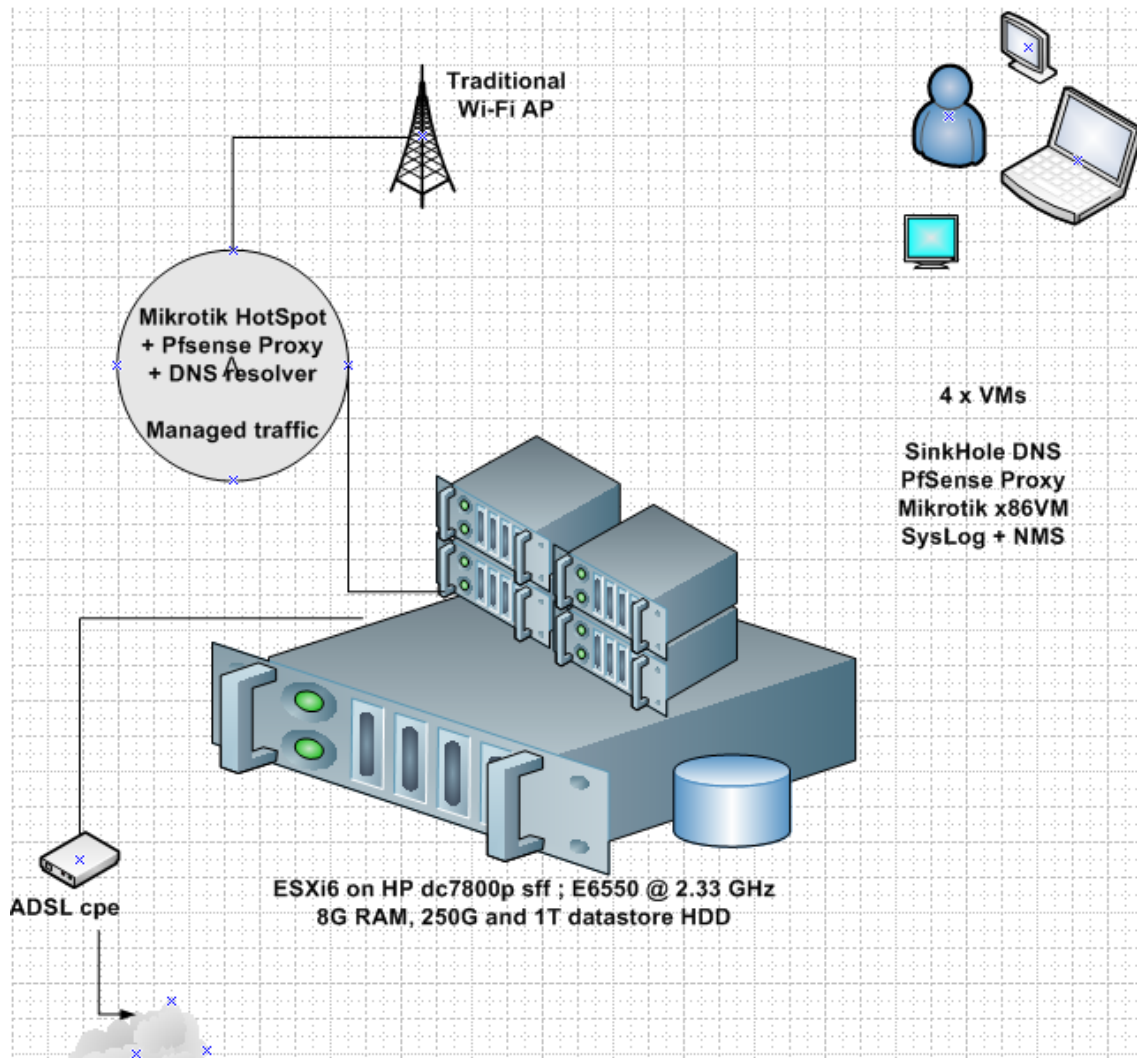
Configure and Connect VMs in Host

x86 Mikrotik HotSpot VM+ PfSense gw Proxy ..



PfSense Server with 6G RAM, 3NIC

x86 Mikrotik HotSpot VM+ PfSense gw Proxy ..



Basic Home HotSpot in a CAN

Home Lab with MT + PfS Proxy + external DNS

- Production Use for now ; took 4 evenings of config time
- MT vm take HotSpot role + DHCP for tablets, handsets and laptops connected through dummy AP
- For non http port 80 traffic,
 - esp: CoC, https, torrents forward to ADSL gateway/WAN
 - For port 80, HTTP traffic, it forward to PfSense **caching** (can get additional web filter and usage reporting here)
 - Port 53, DNS servers assigned during DHCP lease is handled by separate **SinkHole DNS** VMs, which already filter my own and world known blacklisted malicious sites.
 - MT hotspot & all servers send syslog to another centralized log server.
- **MT masters HotSpot performance with managed DNS+ Proxy**

MTRB for Home Lab

- This MT HotSpot in a CAN is based on resources especially from
- **Example #2,B** of Using Caching Server (5 Main Idea's)
- http://wiki.mikrotik.com/wiki/Examples_for_Use_Caching_Server_%285_Main_Idea%E2%80%99s%29

and

- <http://wiki.mikrotik.com/wiki/Manual:IP/Proxy>

MTRB for xxx

- Further Customizations Labs @home
 - Packet Filtering – Deny garbage traffic, Virus suspect ports, ...
 - Content Filtering – Parental Control, porno, ADs, blacklisted CnC sites, ...
 - fair use policies – throttle heavy bandwidth users/apps/sessions
 - QoS and control – queues, prioritize live traffic of specific IP/user/application demand
 - VPN Server @ overseas and operation management net/test DMZ
 - Backend user Authentication by external Radius/DB [not MT local/built-in]
 - R-Pi based deployments
 - MT models with Bigger storage / caches ; SSD, Micro-SD, ...
(http://wiki.mikrotik.com/wiki/Proxy_on_RouterBOARD's_external_drive)

MTRB for xxx

- All other Advanced Topics already DONE by our seniors with more of hands-on Mikrotik experience & solution Projects
- my Next Intensions/Labs
 - Tunnels, EoIP,
 - PBR, Policy based Routing
 - Load Balancing & Fail Over, Multi WAN solutions /may be/
 - MPLS TE self study before next CERTs
with little hands-on PCC, ECMP Load Balancing Scenarios

Useful Links

- Nomenclature

[http://wiki.mikrotik.com/wiki/Manual:First time startup](http://wiki.mikrotik.com/wiki/Manual:First_time_startup)

- License Levels and our demanded sizing, ...

[http://wiki.mikrotik.com/wiki/Manual:License#License Levels](http://wiki.mikrotik.com/wiki/Manual:License#License_Levels)

- Exams & Certifications @ Training + LABs
with basic principle and foundation study on Network, IP, ...

- +++

Thanks! and....

any Questions?

for suggestions, advices,
feel free to pass / email to:
BroNaing@ymail.com

