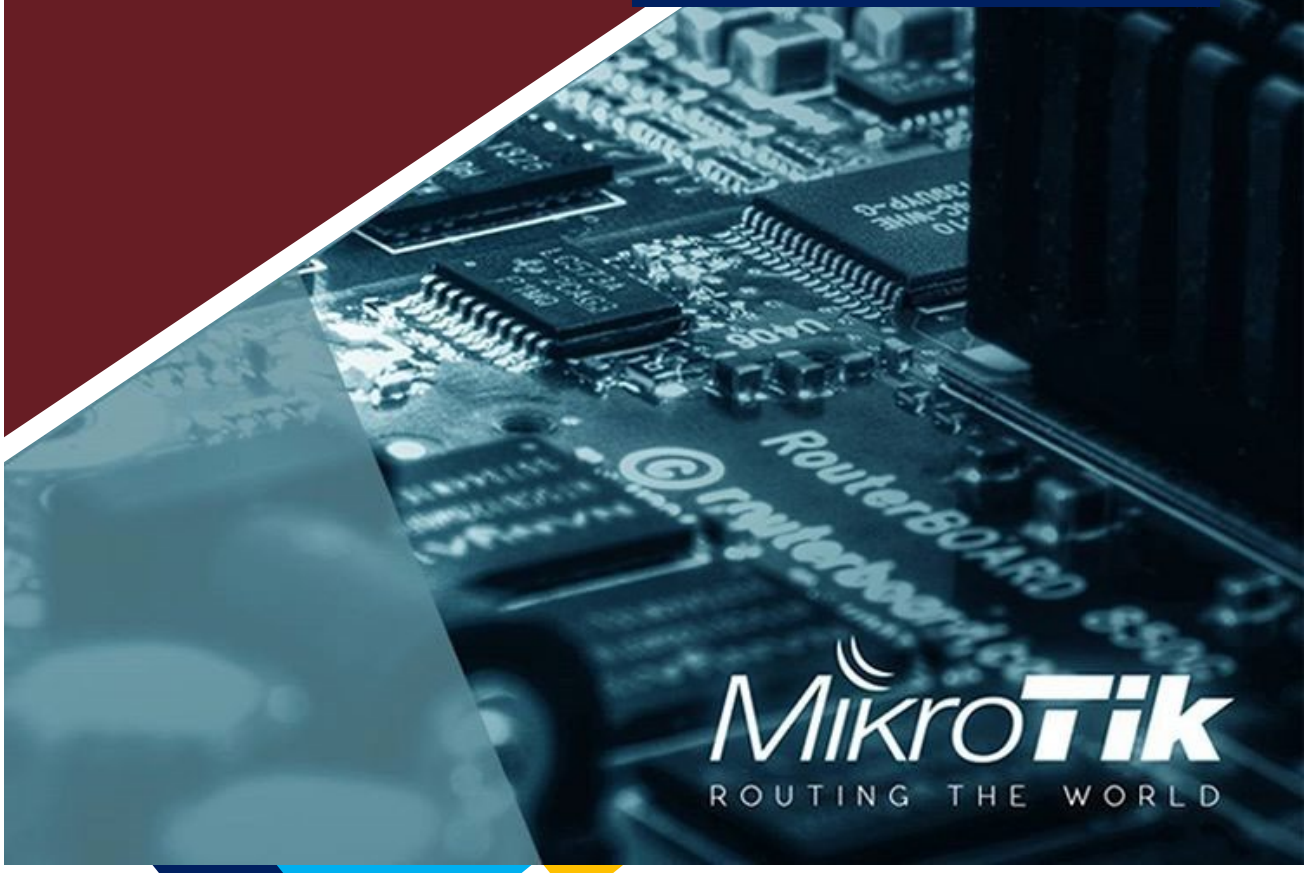
MikroTik ACADEMY

Module 3

Student book version 0.1

Passerelles numériques Cambodia

MTCNA



Passerelles numériques
A Gateway for Life

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

TABLE OF CONTENT

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Passerelles numériques
A Gateway for Life

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

MY COMMITMENT

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 1: INTRODUCTION

OBJECTIVE

After finish, this lesson students will be able to:

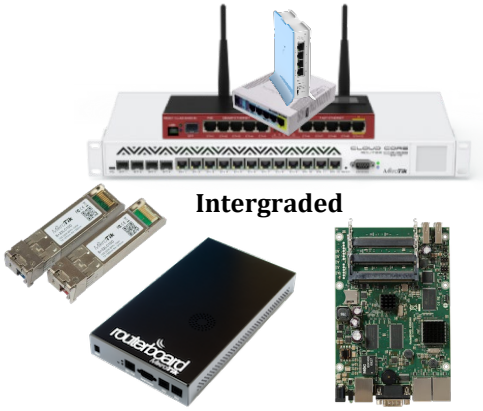
- Describe about MikroTik
- Access to MikroTik Router
- Manage router by basic command line
- Upgrade and downgrade RouterOS
- Managing user and login
- Managing configuration backups
- Reset, reinstall RouterOS
- Understanding licenses

HISTORY OF MIKROTIK

- Location: Riga, Latvia (Northern Europe)
- Produce software and router hardware.
- To make Internet technology cheaper, faster, easier and reliable.
- MikroTik Slogan: Routing the World.
- Founder (1996): John Trully & Arnis Reikstins.
- Website: www.mikrotik.com

MIKROTIK ROUTEROS AND ROUTERBOARD

- RouterOS: is the operating system of MikroTik RouterBOARD hardware. RouterOS is an operating system based on Linux kernel that can also be installed on a PC or as a virtual machine (VM).
- RouterBOARD: is a family of hardware solutions created by MikroTik that run RouterOS. Ranging from small home routers to carrier-class access concentrators.
- Product solution:
  - Integrated solutions: ready to use
  - Boards only: for assembling own system
  - Enclosures: for custom RouterBOARD builds
  - Interfaces: for expanding functionality
  - Accessories



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

MIKROTIK ROUTEROS FEATURES

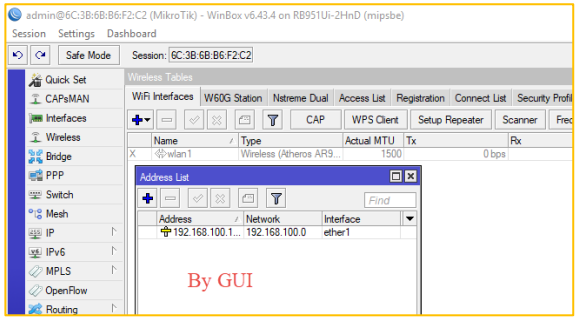
MikroTik has features that more than just a "Router":

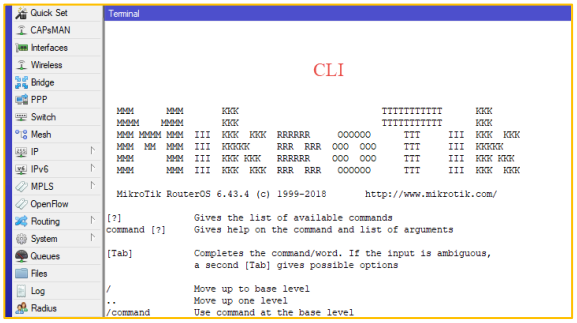
- Firewall and NAT
- Routing (RIP, OSPF, BGP, RIPng, OSPFv3)
- User management (DHCP, Hotspot, Radius).
- QoS / Bandwidth management
- Tunnel (EoIP, PPTP, L2TP, PPPoE, SSTP, OpenVPN)
- Real-time Tools (Torch, Watchdog, Ping, Traceroute
- And many more ..see: www.wiki.mikrotik.com

CONFIGURE MIKROTIK

There are two ways configure MikroTik by GUI and CLI

- GUI: use interface to configure (mostly prefer)
- CLI: use command to configure





MIKROTIK ACCESSING

There are many ways to access MikroTik Router:

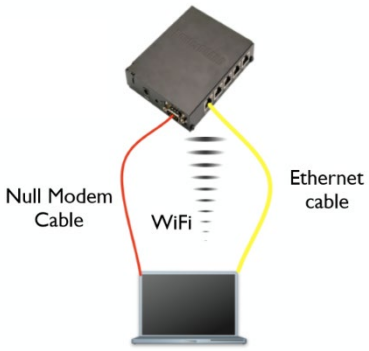
Access	Connection	Text base	GUI	Need IP
Keyboard	Directly into PC	Yes		
Serial Console	Serial Cable	Yes		
Telnet & SSH	Layer 3	Yes		Yes
Winbox	Using OS Windows	Yes	Yes	
FTP	Layer 3	Yes		Yes
API	Socket Programming			Yes
Web(HTTP)	Layer 3		Yes	Yes
MAC-Telnet	Layer 2	Yes		

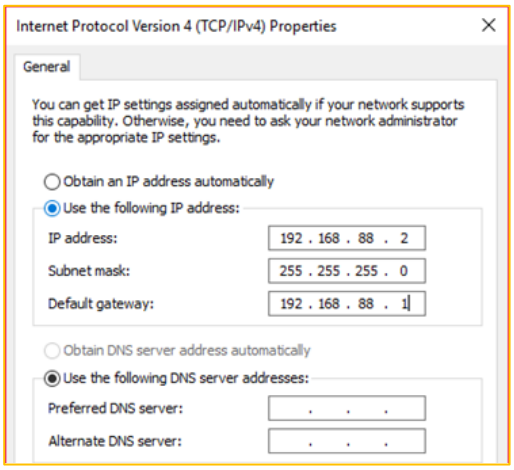
New RouterBOARD, or after reset to default, has a default configuration from the factory:

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

IP Address in Ether 2-5: 192.168.88.1/24

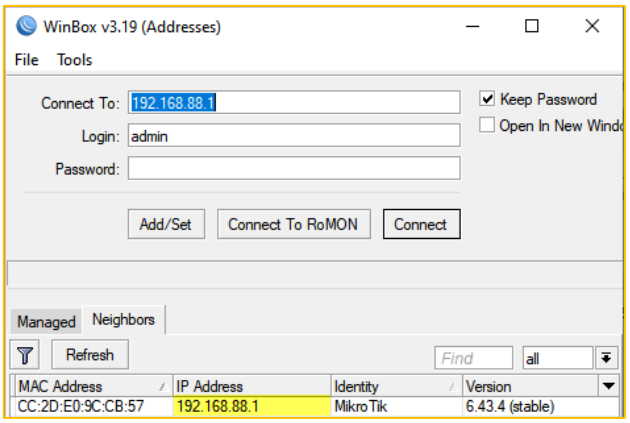
- User name: admin
- Password: no password

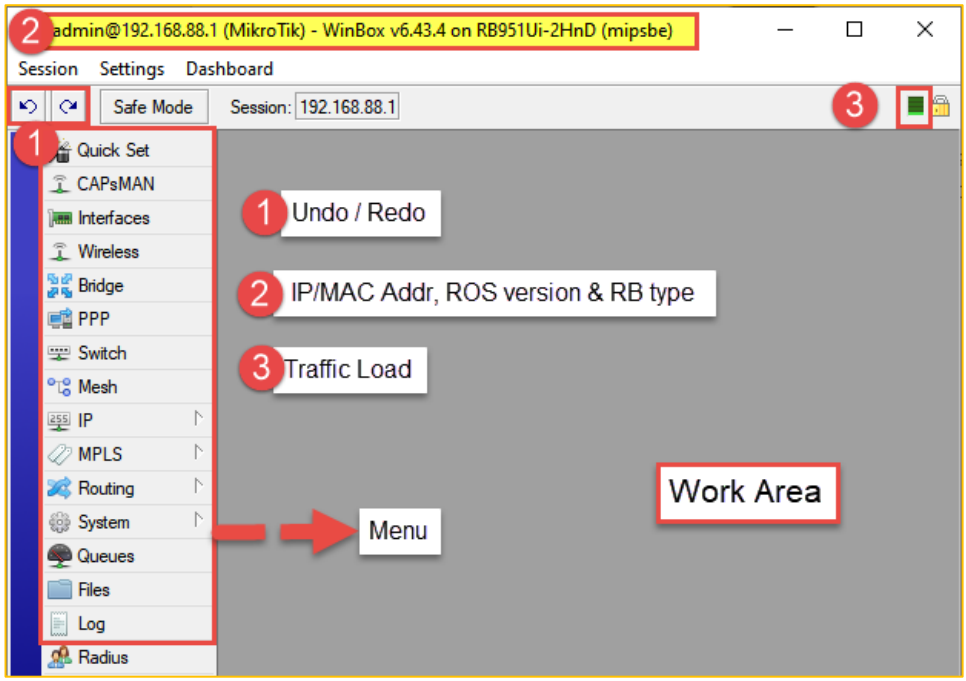




Accessing by WinBox

WinBox is the proprietary software of MikroTik design for specific access to MikroTik devices. You can download from MikroTik website or can download from Webfig. We can access MikroTik router via both IP Address and MAC Address.

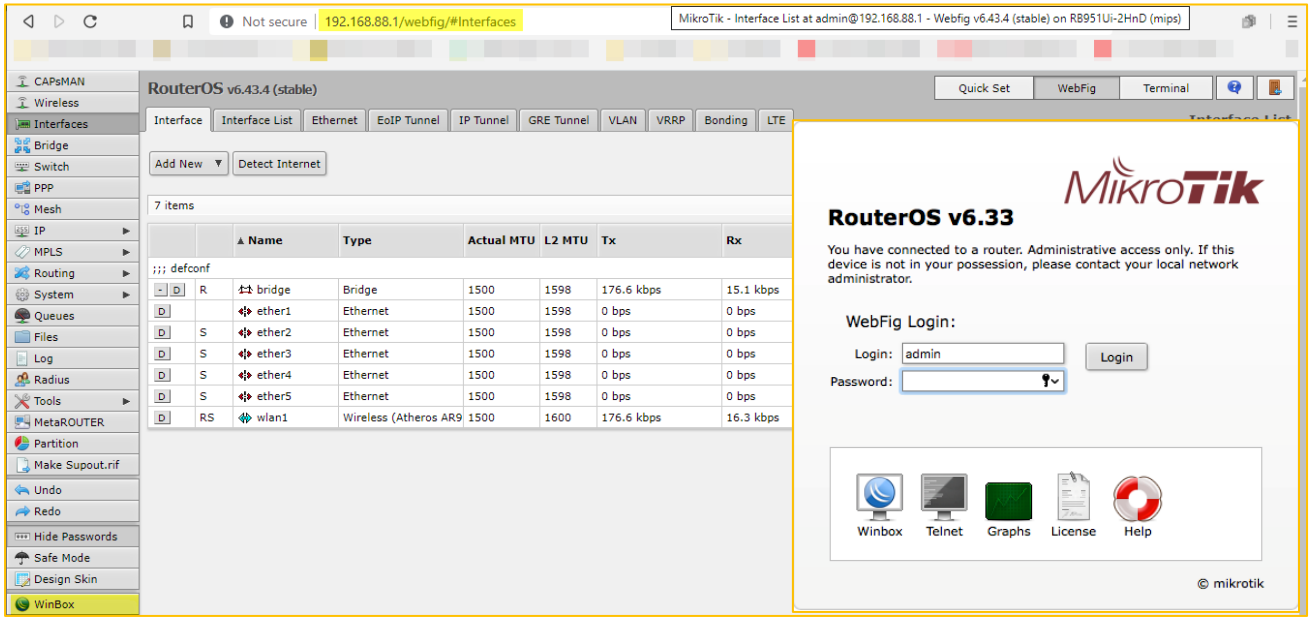




Accessing by Webfig

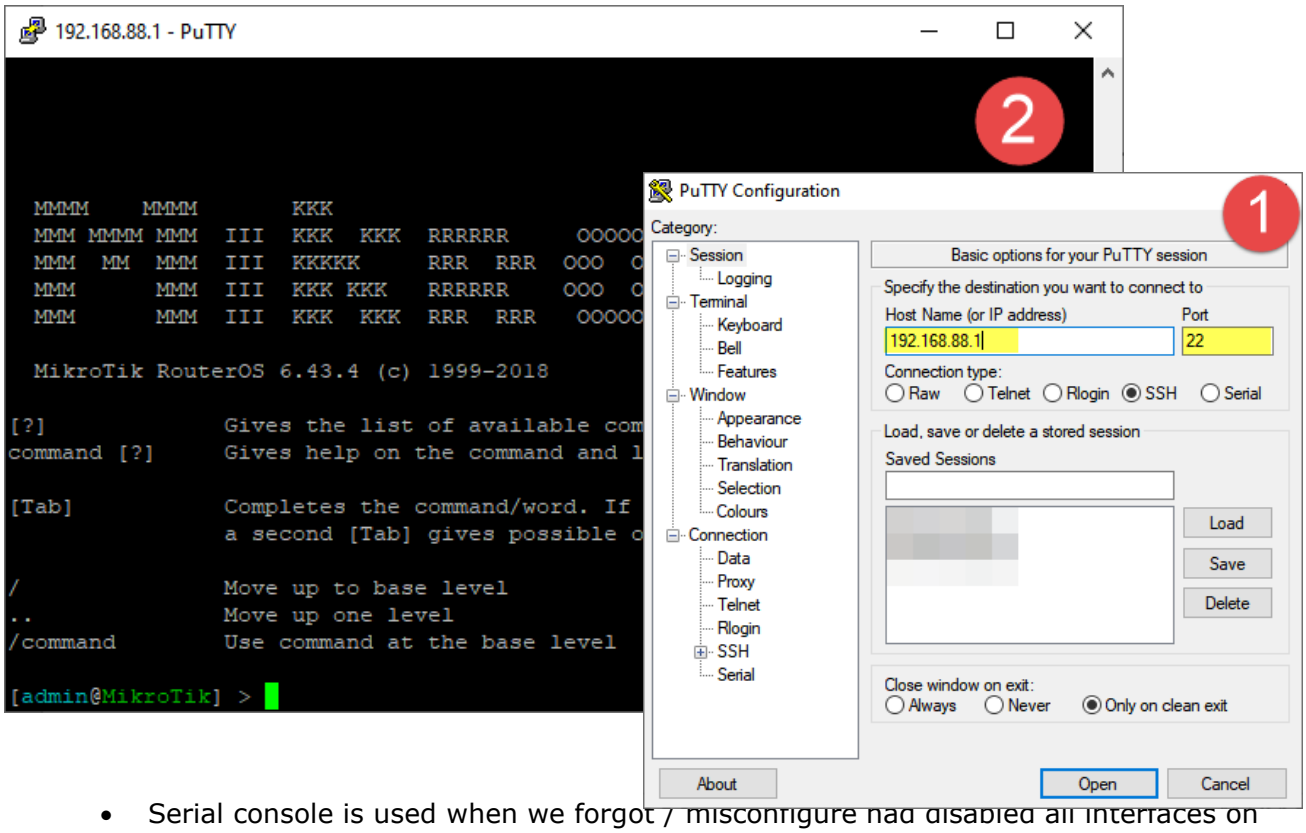
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Accessing router by type ip address (192.168.88.1) of the router on web browser.



Accessing by Terminal

- In some condition, maybe remote configuration via GUI is not possible because of some reasons, such as bandwidth limitations.
- Remote configuration can be done by terminal with the following program:
  - Telnet
  - SSH
  - Serial console (serial cable)



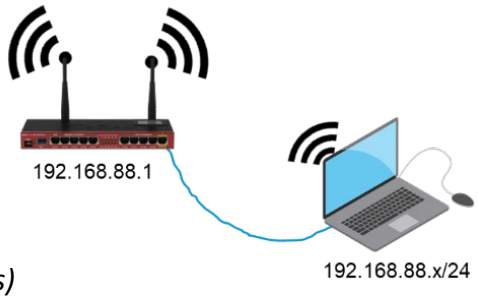
- Serial console is used when we forgot / misconfigure had disabled all interfaces on MikroTik.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

- Serial console is also needed when we use the NetInstall.
- Remote via serial console cable need DB-9 port (or converter USB to DB-9).
- Using the HyperTerminal program.
- It uses 115200 baud rate, 8 data bits, Parity None, stop bits 1, and Flow control none.
- Low end routers do not have a serial port.

1.1-LAB-Connect to Router

- *Change your IP of your laptop to:*
  - *IP Address 192.168.88.x*
  - *Netmask 255.255.255.0*
- *Ping to the RouterBoard (192.168.88.1)*
- *Access to URL of RouterBoard (http://192.168.88.1)*
- *Download winbox the web page.*
- *Remote using winbox to RouterBoard (Mac / IP Address)*
- *Remote by SSH using Putty software*
- *Change identity to your name is easy to identify (system => identity)*



COMMAND LINE INTERFACE

List of keys:

- <tab> completes command
- double <tab> shows available commands
- '?' shows help
- Navigate previous commands with <↑>, <↓> buttons
- Ctrl+C: keyboard interrupt.
- Ctrl+D: log out (if an input line is empty)
- Ctrl+K: clear from the cursor to the end of the line
- Ctrl+A: move thecursor to the beginning of the line. If the cursor is already at the beginning of the line, then go to the beginning of the first line of the current input.
- Ctrl+E: move cursor to the end of the line. If the cursor is already at the end of the line, then move it to the end of the last line of current input.
- Ctrl+L: reset terminal and repaint the screen.
- Hierarchical structure (similar to WinBox menu)
- Ctrl+X: to safe mode. It is sometimes possible to change the router configuration in a way that will make the router inaccessible (except from local console). Usually this is done by accident, but there is no way to undo last change when connection to router is already cut. Safe mode can be used to minimize such risk. To save changes and quit safe mode, press Ctrl+X. To exit without saving the made changes, hit Ctrl+D.
- For more information go to https://wiki.mikrotik.com/wiki/Manual:Console

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Some examples:

List content: print

```
[admin@MikroTik] > ip add print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    192.168.1.1/24     192.168.1.0     ether1
[admin@MikroTik] > _
```

- Change directory path: just put location

```
[admin@MikroTik] > ip
[admin@MikroTik] /ip> address
[admin@MikroTik] /ip address> _
```

```
[admin@MikroTik] >
[admin@MikroTik] > ip address
[admin@MikroTik] /ip address> _
```

```
[admin@MikroTik] /ip address>
[admin@MikroTik] /ip address> /system license
[admin@MikroTik] /system license>
[admin@MikroTik] /system license> print
  software-id: 04S0-0M99
       nlevel: 4
     features:
[admin@MikroTik] /system license> _
```

- Back one path: ..

```
[admin@MikroTik] /system license>
[admin@MikroTik] /system license> ..
[admin@MikroTik] /system> license
[admin@MikroTik] /system license> /
```

- Create User

```
[admin@MikroTik] /user> add name=nakagi password=nakagi group=
full  read  write
[admin@MikroTik] /user> add name=nakagi password=nakagi group=full
[admin@MikroTik] /user> print
Flags: X - disabled
 #    NAME            GROUP           ADDRESS           LAST-LOGGED-IN
 0    ;;; system default user
      admin           full                              dec/27/2018 13:22:18
 1    vuthy           read                              dec/27/2018 15:22:14
 2    nakagi          full
[admin@MikroTik] /user> _
```

- Add IP Address

```
[admin@MikroTik] /ip address> add address=192.168.200.1/24 interface=ether1
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    192.168.200.1/24   192.168.200.0   ether1
[admin@MikroTik] /ip address> _
```

- Help: using question mark " ?" and Tape key to complete command

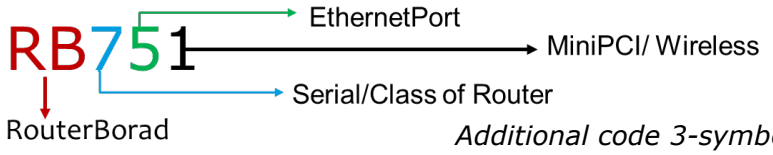
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

```
[admin@MikroTik] /ip address>
IP addresses are given to router to access it remotely and to specify it as a ga
teway for other hosts/routers.

.. -- go up to ip
add -- Create a new item
comment -- Set comment for items
disable -- Disable items
edit --
enable -- Enable items
export -- Print or save an export script that can be used to restore configurati
on
find -- Find items by value
get -- Gets value of item's property
print -- Print values of item properties
remove -- Remove item
set -- Change item properties
```

ROUTER LICENSE

- RouterBoardmodel name, for example:



Additional code 3-symbol name1st symbol stands for series (this can either be a number or a letter)

2nd digit for indicating the number of potential wired interfaces (Ethernet, SFP, SFP+)

3rd digit for indicating the number of potential wireless interfaces (built-in and mPCI and mPCIe slots)

- U= USB port
- A= Advanced, more memory or higher license
- H= High performance, more powerful CPU
- G= Gigabit Ethernet port
- i= Power injector
- 2= 2.4GHz wireless
- N= Support 802.11n wireless
- D= Dual chain antenna

More info: http://wiki.mikrotik.com/wiki/Manual:Product_Naming

Example

Lets decode **RB912UAG-5HPnD** naming:

- RB (RouterBOARD)
- 912 - 9th series board with 1 wired (ethernet) interface and two wireless interfaces (built-in and miniPCIe)
- UAG - has USB port, more memory and gigabit ethernet port
- 5HPnD - has built in 5GHz high power dual chain wireless card with 802.11n support.

RouterOS features are determined by the level of the license attached to the device.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

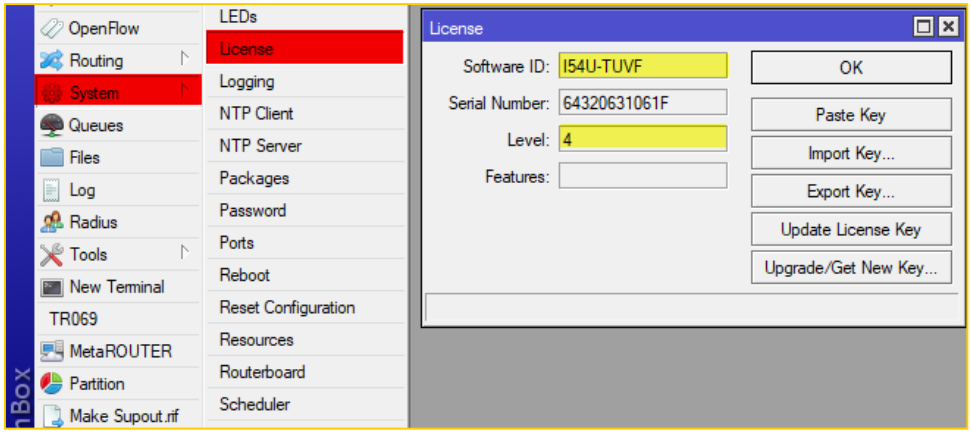
- Level of licenses also determine limits of upgrade version.
- License attached at media storage (ex. HDD, NAND, USB, Compact Flash).
- When the media storage is formatted with non MikroTik software, the license will be lost.

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	volume only	$45	$95	$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	Yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	Unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	Unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	Yes	yes	yes	yes
Queues	24h trial	1	Unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	Yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

LICENSE AND VERSION UPGRADE

License determines which of RouterOS version that can be upgraded in a default installation.

- L3 and L4 allow to upgrade 1 version.
- L5 and L6 allow to upgrade 2 versions.



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

RouterOS version:

- License level is related to the price, higher level of license more expensive.
- Versions is different from license level, version is update or release of the RouterOS
- MikroTik RouterOS features depend on the license level, version, and the packages installed.

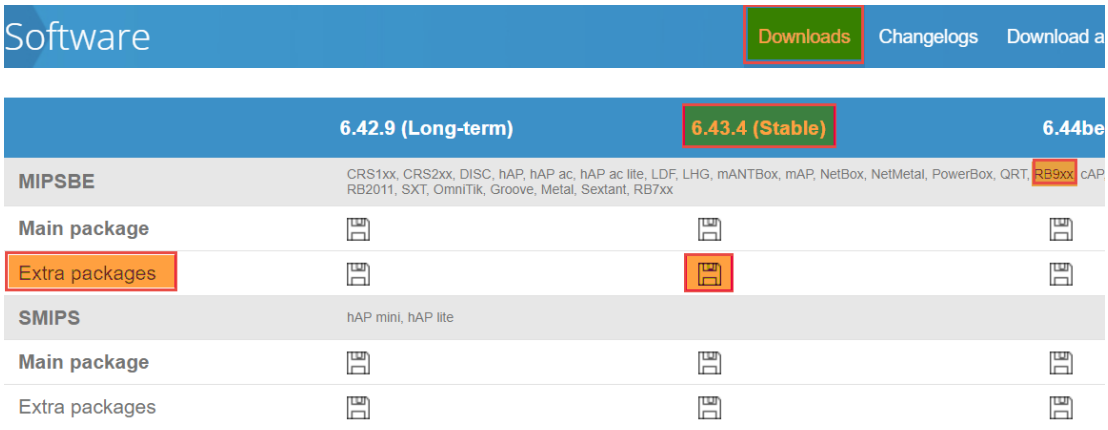
System=> packages (to check version of packages)

Up & Downgrade RouterOS

- Always upgrade your RouterOS to the latest version, for fixing bugs or getting new features.
- Downgrade needed if the hardware does not support the new version or there is a script that can't be run in the new version.
- Upgrade package should consider the rules of your license level.
- Upgrade and downgrade also have to consider the type of hardware architecture.
- Package selection is very important in doing the upgrade/downgrade, different types and hardware architectures have different software packages.
- When we in doubt,see and cross-check at the website of www.MikroTik.com/download.html

mipsbe	RB4xx series, RB7xx series, RB9xx series, RB2011 series, SXT, OmniTik, Groove, METAL, SEXTANT
ppc	RB3xx series, RB600 series, RB800 series, RB1xxx series
x86	PC / X86, RB230 series
mipsle	RB1xx series, RB5xx series, RB Crossroads
tile	CCR series

For example ,**RB951** using **MIPSBE** and the newest version is 6.43.4

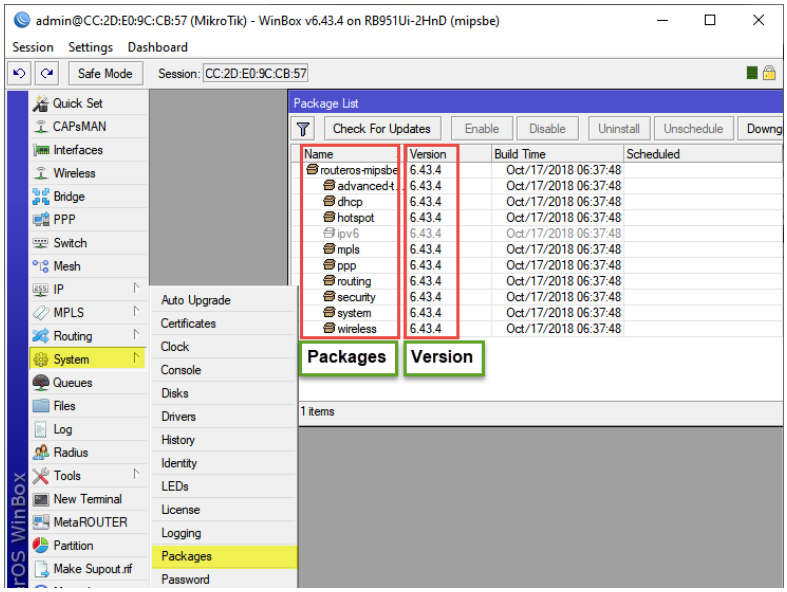


Example Upgrade RouterOS

- Drag and drop all files with extension *.npk from your local folder to
- Winbox We also can use copy paste button
- Reboot the router after finish upload. It will upgrade by itself.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

- Check logs to see if have any errors during the upgrade.



Package	Features
advanced-tools (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	Advanced ping tools (flood-ping, ping-speed), Netwatch, ip-scan, SMS tool, Wake-on-LAN
calea (*mipsle, mipsbe, ppc, x86, mmips, arm*)	Data gathering tool for specific use due to "Communications Assistance for Law Enforcement Act" in USA
dhcp (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	Dynamic Host Control Protocol client and server
gps (*mipsle, mipsbe, ppc, x86, mmips, arm*)	Global Positioning System devices support
hotspot (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	HotSpot captive portal server for user management
ipv6 (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	IPv6 addressing support
lte (*mipsbe*)	Required package only for SXT LTE (RBSXTLTE3-7), which contains drivers for the built-in LTE interface.
mpls (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	Multi Protocol Labels Switching support
multicast (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	Protocol Independent Multicast - Sparse Mode; Internet Group Managing Protocol - Proxy
ntp (*mipsle, mipsbe, ppc, x86, mmips, arm*)	Network protocol server, also includes simplistic client. NTP client is also built into the system package and functions well without this package installed.
openflow (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	Enables OpenFlow support
ppp (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	MIPPP client, PPP, PPTP, L2TP, PPPoE, ISDN PPP clients and servers
routerboard (*mipsle, mipsbe, ppc, x86, mmips, arm*)	accessing and managing RouterBOOT. RouterBOARD specific imformation.
routing (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	dynamic routing protocols like RIP, BGP, OSPF and routing utilities like BFD, filters for routes.
security (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	IPSEC, SSH, Secure WinBox (*necessary for Winbox versions up to v3.14*)
system (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	basic router features like *static routing, ip addresses, sNTP, telnet, API, queues, firewall, web proxy, DNS cache, TFTP, IP pool, SNMP, packet sniffer, e-mail send tool, graphing, bandwidth-test, torch, EoIP, IPIP, bridging, VLAN, VRRP* etc.). Also, for RouterBOARD platform - *MetaROUTER	Virtualization*
tr069 (*mipsbe, ppc, x86, mmips, arm*)	TR069 Client package
ups (*mipsle, mipsbe, ppc, x86, mmips, arm*)	APC ups management interface
user-manager (*mipsle, mipsbe, ppc, x86, mmips, arm*)	MikroTik User Manager server for controlling Hotspot and other service users.
wireless (*mipsle, mipsbe, ppc, x86, mmips, arm, smips*)	wireless interface support. Sometimes sub-types are released, for example **wireless-fp** introduced FastPath support, **wireless-cm2** introduced CAPsMAN v2 and **wireless-rep** introduced Repeater mode. These packages are occasionally released separately, before the new features get merged into the main wireless package.

More detail go to https://wiki.mikrotik.com/wiki/Manual:System/Packages

Note

- Always upgrade your RouterOS to the latest version, for fixing bugs or getting new features.
- Downgrade is needed if the hardware does not support the new version or there is a script that can't be run in the new version.
- Upgrade package should consider the rules of your license level.
- Upgrade and downgrade also have to consider the type of hardware architecture.
- License level 3 can't be an access point, it's function station only
- License binds with HDD.So you can't change the hard disk. If your hdd broken, you have to send hdd to MikroTik to verify.
- Most problems on low-end router when upgrade because of full HDD space, so copy one by one (system packet first).

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

1.2-LAB-Working with packages

- *Disable packages **ipv6***
- *Restart check the package is disabled*
- *Enable **ipv6** package back*
- *Uninstall **mpls** and restart*
- *Check **ipv6** enable back and **mpls** is uninstall*
- *Download packages from " mikrotik website" with your router series.*
- *Upgrade to new version*
- *Check the log to verify there are no problems during the update*

RESET/INSTALL/REINSTALL

Reset Configuration Routers

MikroTik reset configuration required if:

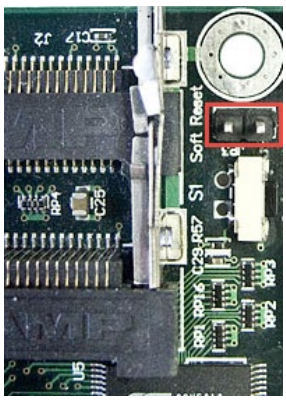
- When forgot username and or password
- When the configuration is too complex and needs to be organized from beginning.

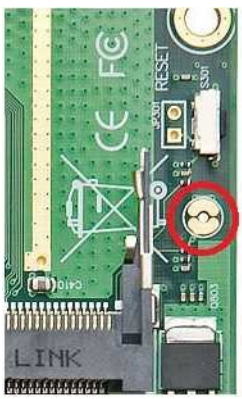
Reset configuration can be done by :

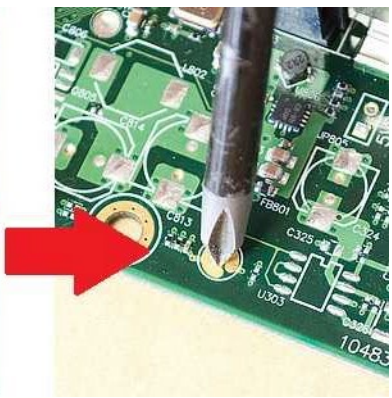
- Hard Reset, reset physically.
- Soft reset, reset by software.
- Reinstall..

Some RouterBoard has reset button in the front of the case, if none, we have to open the case and will see a reset jumper in the circuit board.

Unplug the device



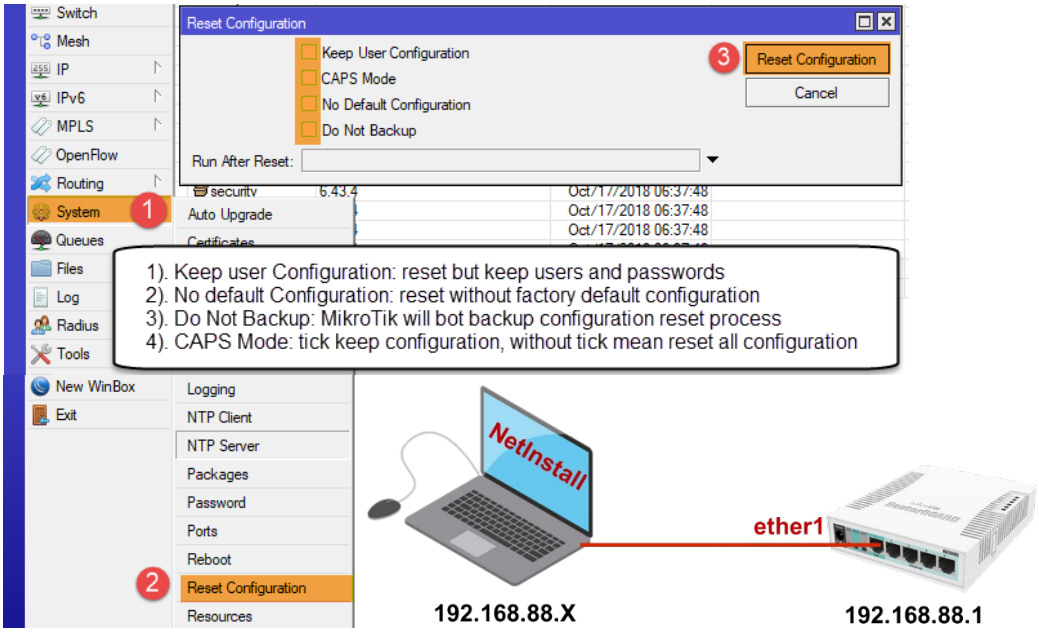




power, hold the button, apply power and wait until LED starts flashing, then release the button to clear configuration.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

If you still be able to accessing MikroTik, reset it by reset menu:



Install / Reinstall MikroTik

- MikroTik can be reinstalled like other operating system
- Reinstall router will make router back to zero config, default configuration, previous config.
- Install can be done using CD or software called **NetInstall**.
- RouterBoard can only be reinstalled using **NetInstall** software.
- RouterBoard must be connected to a laptop / PC via primary Ethernet (ether1)
- Laptop /PC must be running the NetInstall program
- RouterBoard must be set to boot from the network (via ether1), by:
    - Setting via serial console
    - Setting via terminal console
    - Winbox
    - Push reset button for a second

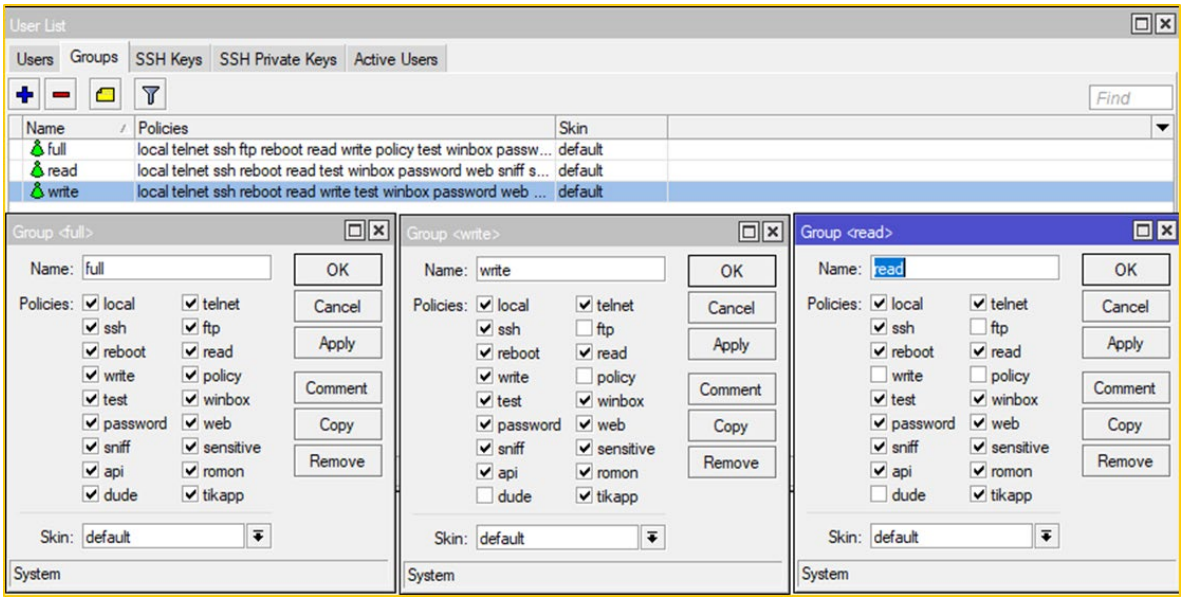
1.3-LAB-Reinstall MikroTik Router

- *Download Netinstall from MikroTik.com*
- *Chose suitable hardware architecture*
- *Connect your laptop with routerBoad on Ether1 and make sure your laptop can communicate with the router. And firewall allows Netinstall application.*

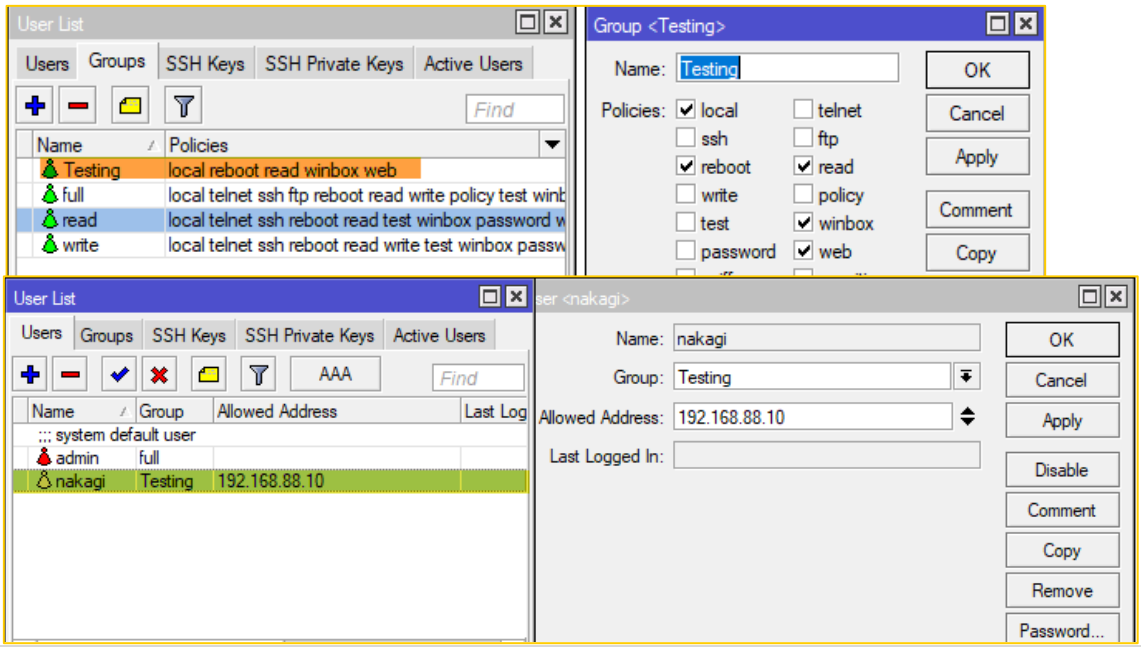
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

USER LOGIN MANAGEMENT

- Access to the router is define by user privilege.
- User management doing by
  - **GROUP** – to make a privilege profile that can be assigned in to user.
  - **USER** – is a router user contain username and password.
- User session that already connect can be seen at "**System>Users>Active Users"**
- User Group is a grouping of privilege / access to be granted to router user.
- There are 3 default privilege in MikroTik, that is **full**, **read** and **write**, but we are allowed to **customize** it.



- User can be restricted based on group
- User can be restricted based on the IP address

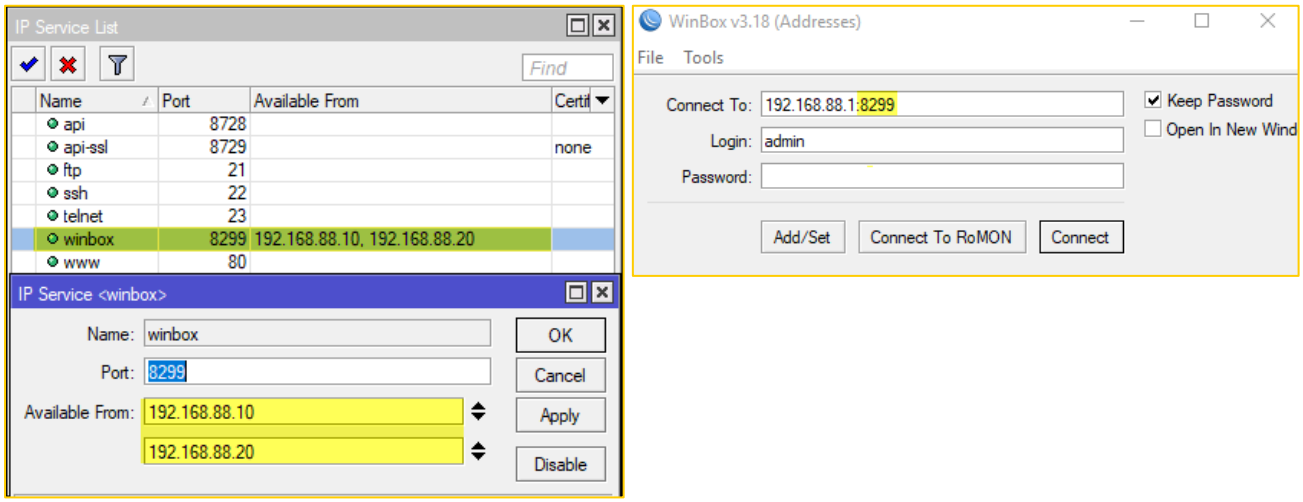


Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

USER LOGIN MANAGEMENT-SERVICE

IP Services use for limit service, which can be accessed by the user

- Configuration settings in the menu **IP>Services**
- For security reason we can permit only IP address or network that can access and also can filter on port access too.



1.4-LAB-User Login Management

- *Create Groups:*
  - *Name: @dminL0 with Permission: Only remote via winbox and reboot only.*
  - *Name: @dminL1 with Permisison: Can remote by winbox, webfix, read and reboot.*
- *Create Users*
  - *Name: Kanitha in group @dminL0*
  - *Name: Sovanna in group @dminL1*
- *Filter only three IP addresses can remote by winbox:8299 and webfix :8099*
- *Testing login and check the permissions that apply.*

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

MIKROTIK NETWORK DISCOVERY PROTOCOL

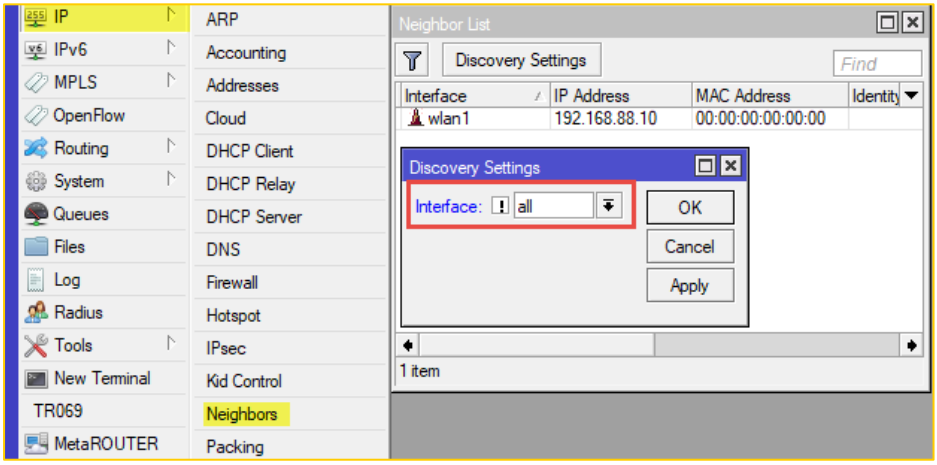
- MNDP is L2 protocol, its generate basic information about router like MAC address, IP address, router-id, platform, etc
- By enabling MNDP mean MikroTik router can discovered by another device that run MNDP too, as long as its in the same network.
- Enable MNDP also allows us to find MikroTik router using Winbox

discovery button MikroTik RouterOS can find another router that also run MNDP and CDP (Cisco Discovery Protocol).

- MNDP can be configured at **IP>Neighbors>Discovery**

To hide your MikrTik so not to appear in Winbox MNDP scan, or could not be found by another network device, MNDP access should be filtered with the following configuration:

- 1- Disable Discovery Interface on **IP** > **neighbors**> **Discovery settings**
- 2- Block UDP port 5678 (MNDP) using **IP Firewall Filter Rule** (for someone try to scan from outside to access from 5678)



BACKUP AND RESTORE

MikroTik router configuration can be backed up and stored for future use. There are 2 types of backup:

1. Binary file (.backup)

- Can not read and edit with text editor.
- To backup all configuration of the router
- Create return point (like snapshot)

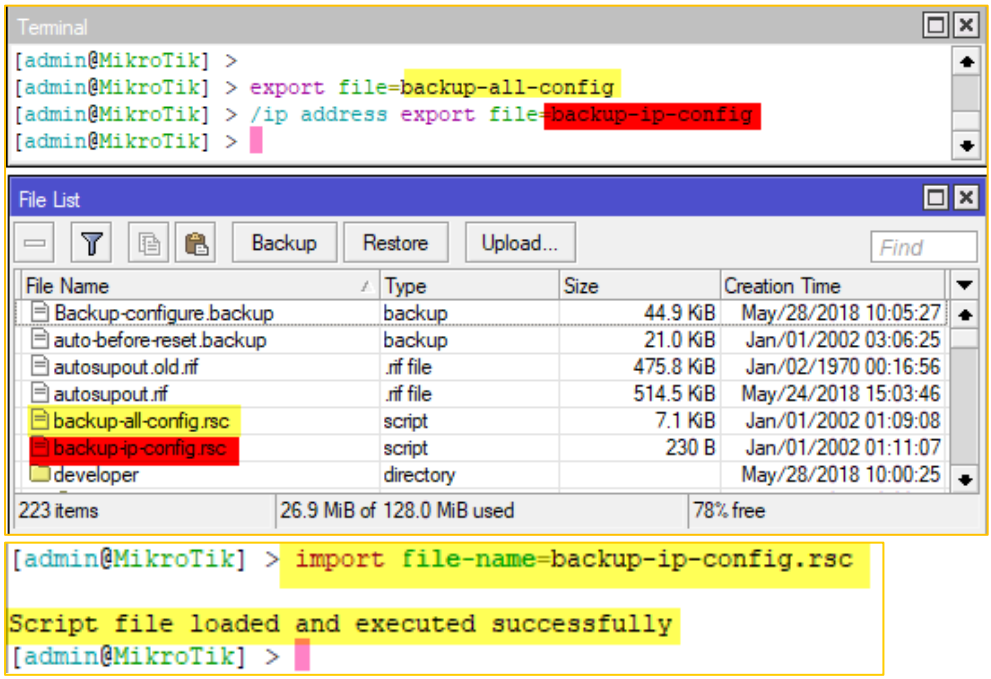
2. Script file (.rsc)

- Can read & edit with text editor.
- To backup a part of configuration of the router.
- Not create return point, just adding the config.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Using script backup

- Backup using script can be done by terminal only with file extension .rsc
- Export do not save username password

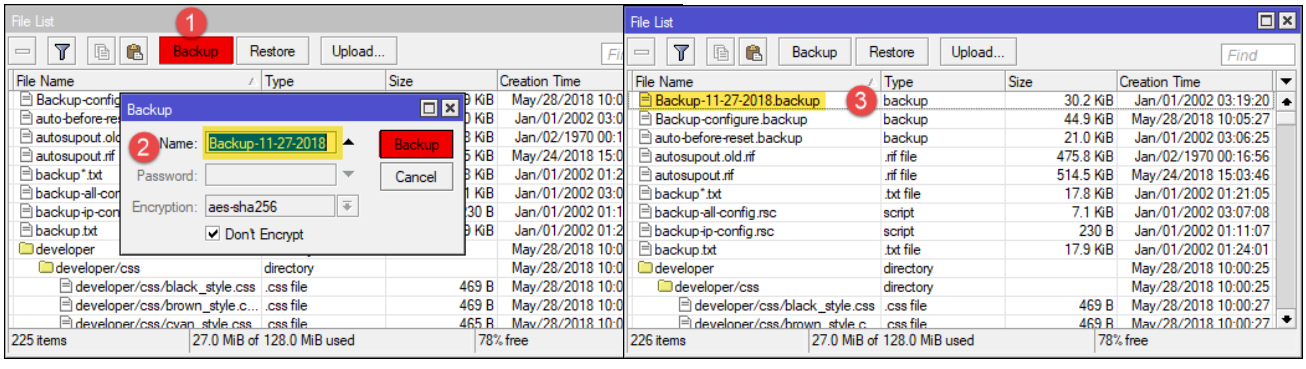


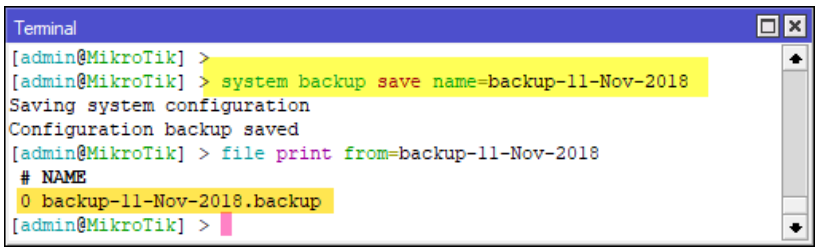
Note: Use export for configuration for edit and analyses by part of configuration.

Using binary backup

Backup using binary can be done by two ways with file extension .backup:

- GUI: File>backup
- CLI (terminal)





Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Different between Export & Backup

CRITERIA	SCRIPT BACKUP	BINARY BACKUP
Command	Export/Import	Backup /Restore
Done by click button menu	No	Yes
Backup all configuration	Yes (but exclude username & password)	Yes
Need reboot to restore	No	Yes
Backup part of configuration	Yes	No
Edit configuration	Yes	No

1.5-LAB-Backup & Restore

- *Backup & Export*
  - *Do backup configuration using:*
    - *"Backup" by GUI for all configuration*
    - *"Export" by terminal for IP configuration*
  - *Download backup file (.backup & .rsc) to your computer*
  - *Try to open, read and edit those files using text editor*
  - *Reset Router to default*
- *Restore & Import*
  - *Restore all configuration back to normal*
  - *Go to delete all users except admin*
  - *Import only users management part*

***Note**:*

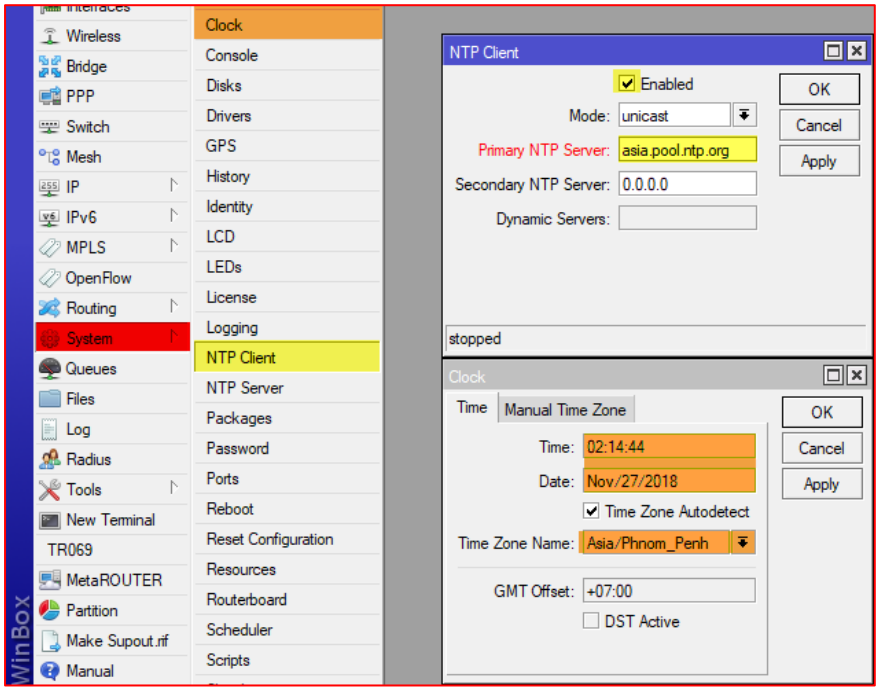
For Export is useful in cast different router version and hardware. If you import = add more, and restore= override. In order to avoid error, you should copy and pass by section into terminal.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

NETWORK TIME PROTOCOL (NTP OR SNTP DEPEND ON ROUTER)

Most of RouterBoard does not have a internal CMOS battery for internal clock (except RB230 and PowerPC)

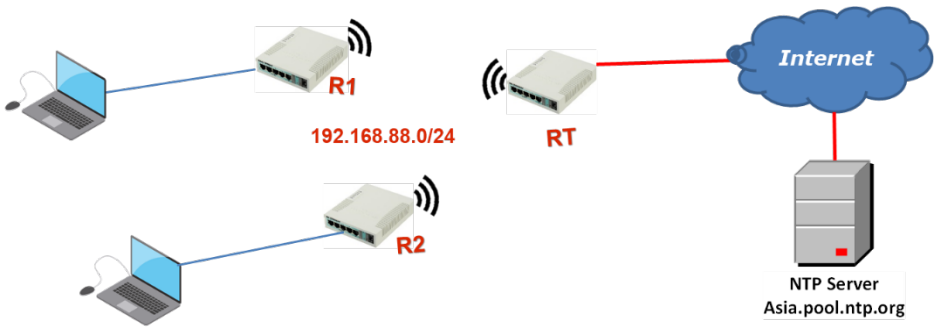
- We need valid time and date to analyze log event correctly.
- Public NTP server list can be found at www.ntp.org
- For example we want to use **asia.pool.ntp.org** and **kh.pool.ntp.org**



1.6-LAB-Network Time Protocol

Configure NTP client on your Router to get the valid time for NTP server using following addresses:

- *Asia.pool.ntp.org*
- *Kh.pool.ntp.org*



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	For static routing functionality, additionally to the RouterOS system package, you will also need routing package.
		2	The license level 0 (demo) is valid 24 hours.
		3	It is impossible to delete admin user on user table MikroTik.
		4	The default baud-rate of currently manufactured RouterBOARDs is 115200.
		5	A backup file from a MikroTik router is store in plain text format.
		6	Netinstall can be used to keep configuration, but reset a lost admin password.
		7	MNDP is L4 protocol, its generate basic information about router like MAC address, IP address, router-id, platform.
		8	The default WinBox port is 8291.
		9	The lisence of MikroTik router store on HDD if you install on PC and we can change HDD if old HDD is broken without notify to MikroTik.
		10	RouterOS base on Linux kernel and has only one main feature is routing.

Answer the Questions

1. What is backup? Why we need to back up?
2. What is your suggestion before you upgrade the MikroTik router?
3. Chose two ways to access MikroTik router and descript briefly.
4. Why is important to manage access to MikroTik Router?
    - Limit access (user)
    - Filter access (Port, firewall..)

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

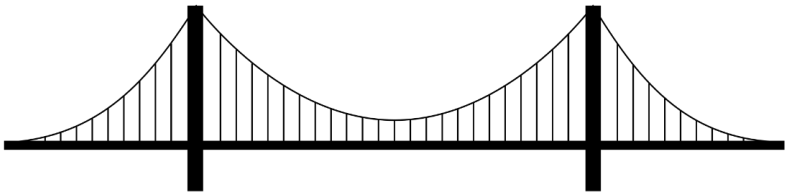
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 2: BRIDGING

OBJECTIVE

After finish, this lesson student will be able to:

1. Bridging Overview
2. Bridge concepts
3. Creating bridges
4. Adding ports to bridges
5. Bridge wireless networks
6. Station bridge
7. STP protocol



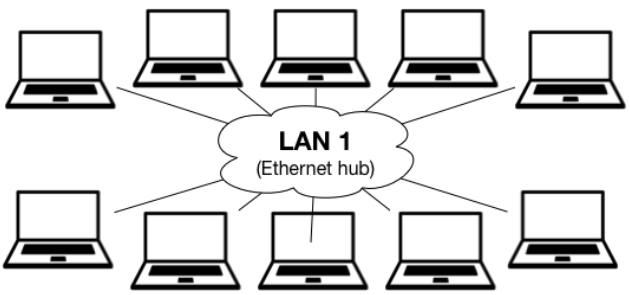
BRIDGE

Some identify of bridge:

- Used to combine two or more interfaces to become one network,
- Bridge can also be run on a wireless network
- Bridge process runs on the data link layer (layer 2) in OSI model
- Bridge interface is a virtual interface, where we can make as much as we want.
- To create bridge is create a new bridge interface and add a physical interface into the port of the bridge.
- If we make the interface bride without adding physical interfaces on the port, the bridge consider as a loopback interface.
- RouterOS implements software bridge
- Ethernet, wireless, SFP and tunnel interfaces can be added to a bridge
- Default configuration SOHO routers

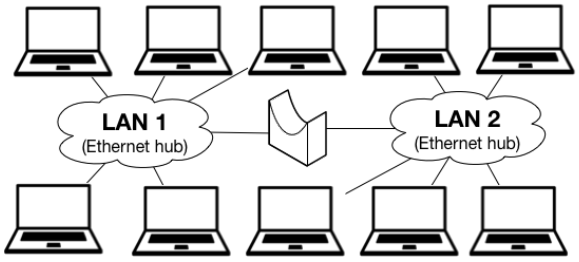
USING BRIDGE

- All hosts still can communicate with each other
- All share the same collision domain



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

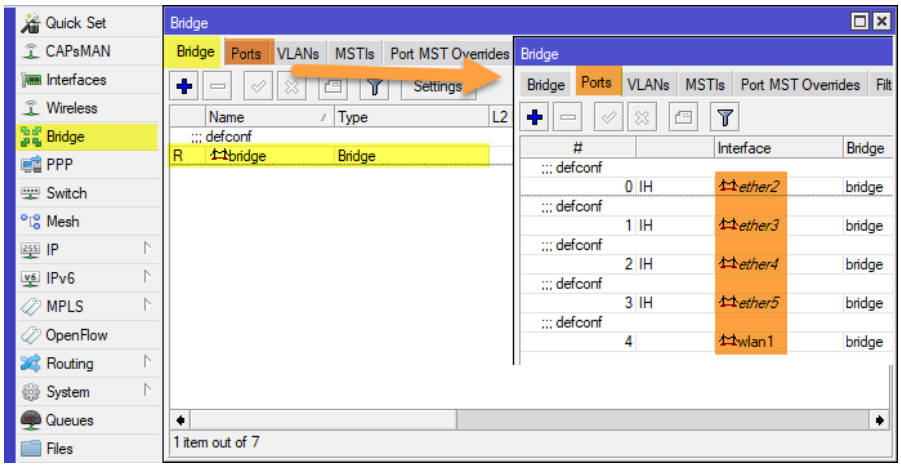
- All hosts still can communicate with each other
- Now there are 2 collision domains



BRIDGE DEFAULT

By default on SOHO RouterBoad:

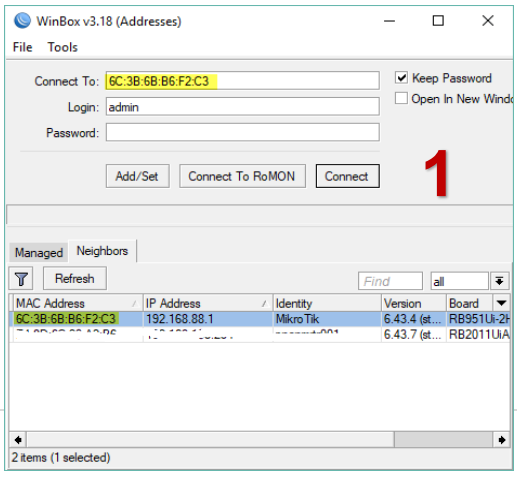
- Port member: ether2-5, Wlan1 (except ether1)
- Bridge name: bridge

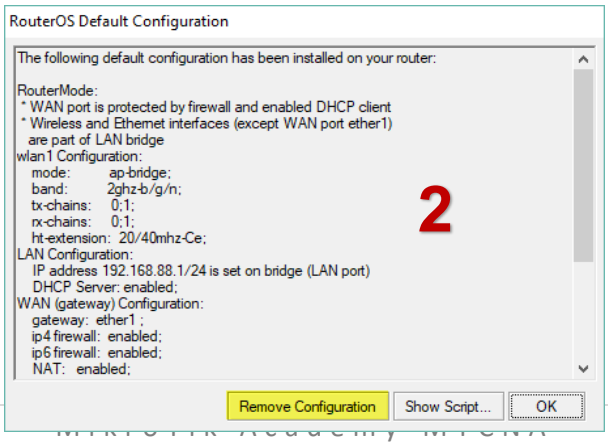


ASSIGN IP ADDRESS

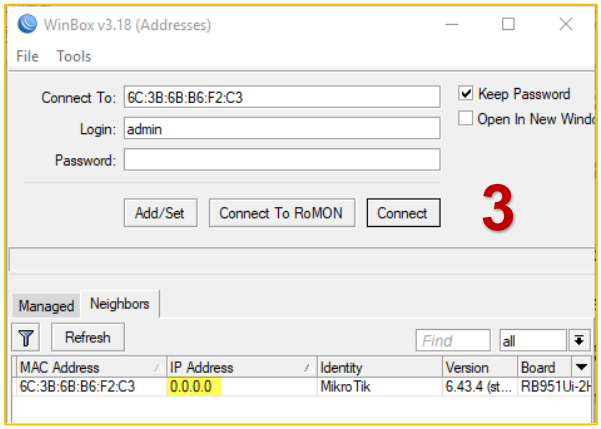
Assign IP Address to interface by remove default configuration. In this cast use for basic assign IP Address.

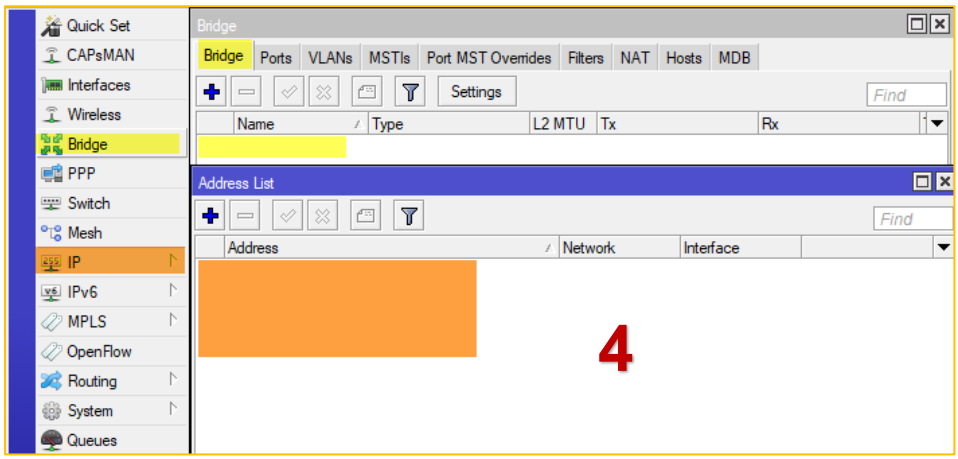
- Connect to router by Mac-address
- Remove all default configuration
- Assign IP address to interfaces or create bridge ask you wish.

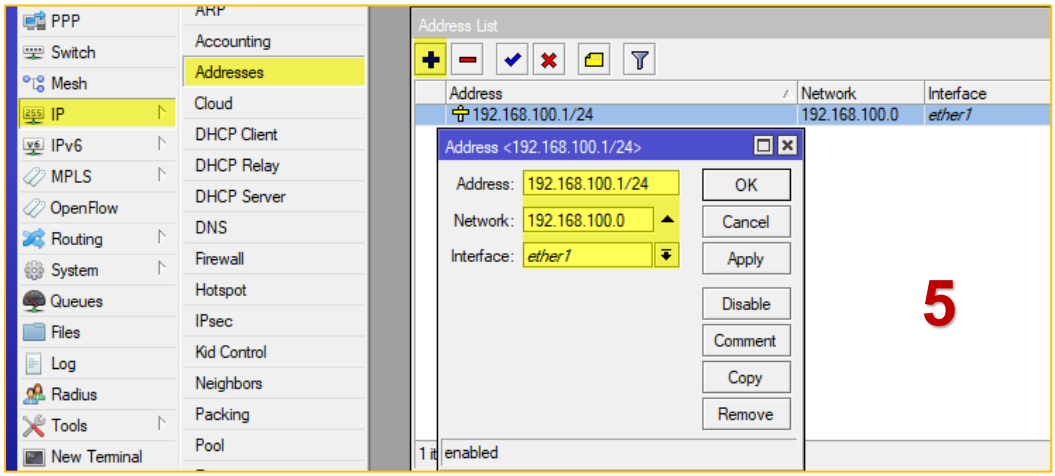


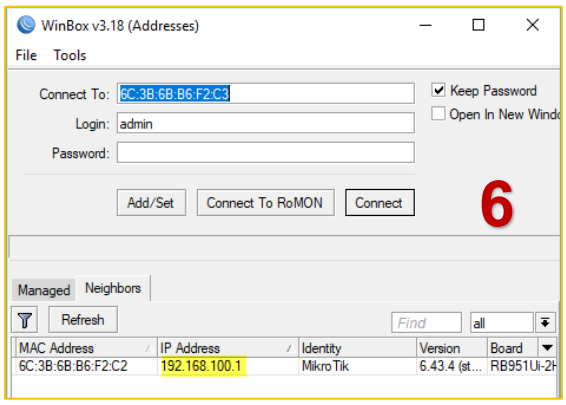


Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org





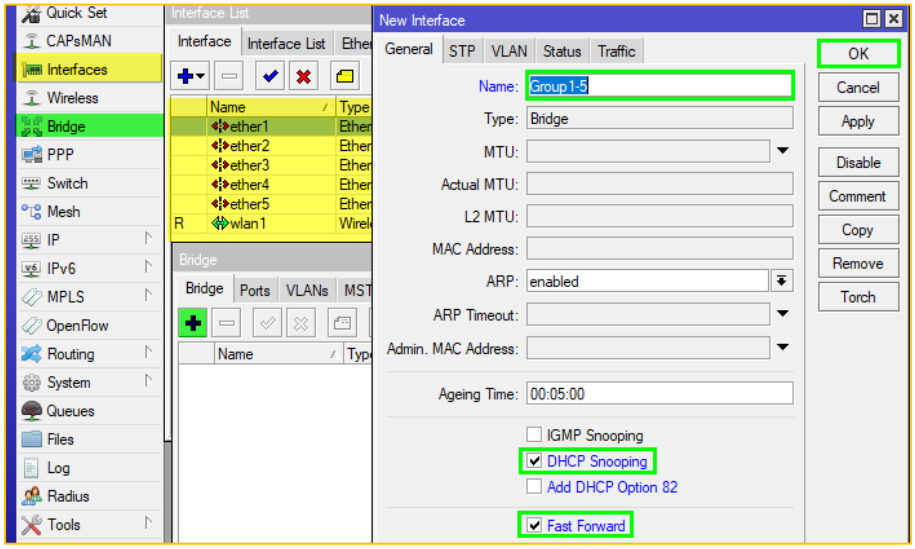




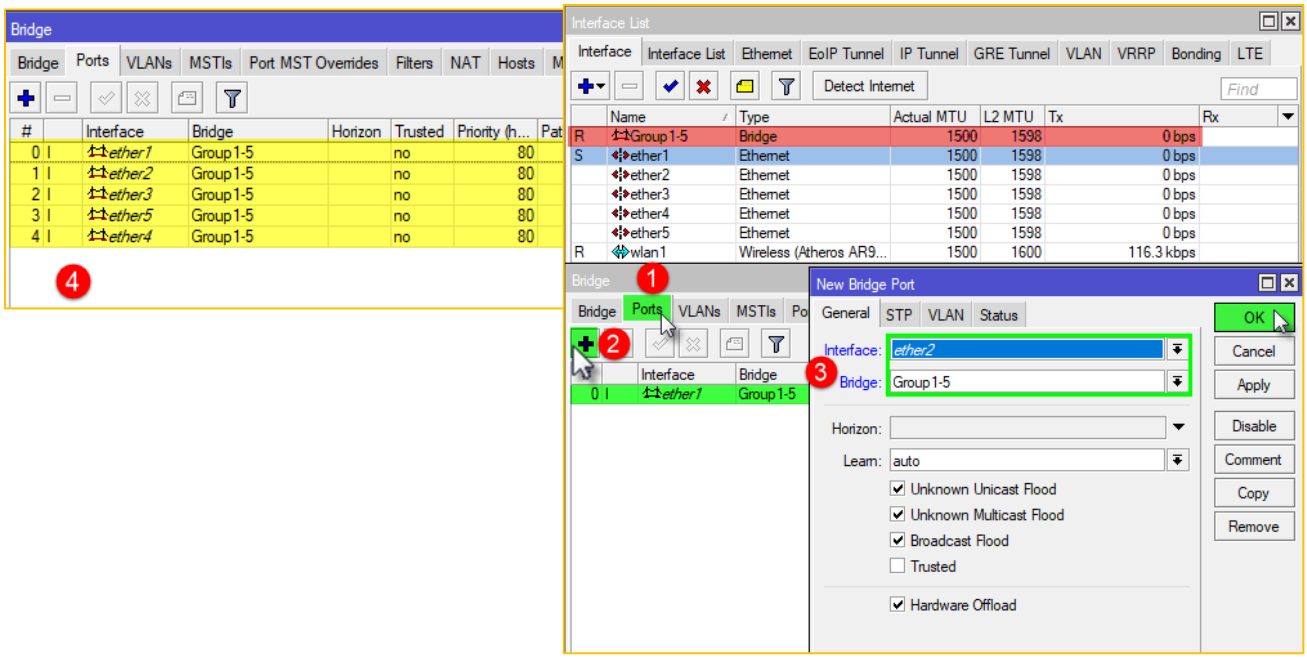
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

WORK WITH BRIDGE

Create bridge by go to Menu => Bridge => Click on + to create bridge



Add Ports to Bridge by select port one by one to add to bridge interface



WIRELESS BRIDGE

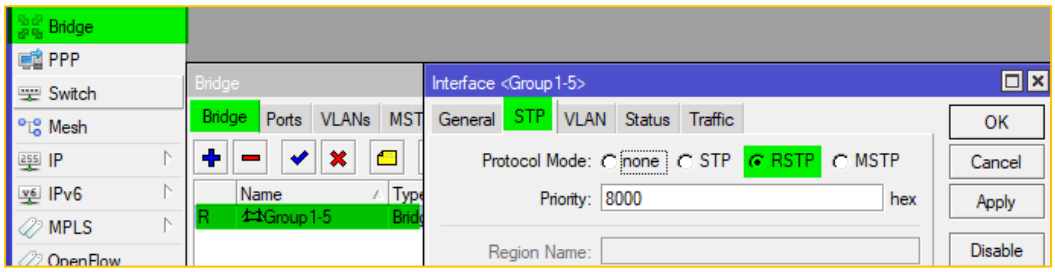
All wireless mode can be bridging, except station mode.

- Station mode can't be bridging, so there is another type of station that can be bridging.
- Station bridge is feature that allows station to be bridging.
- Station bridge will work only on the connection between RouterOS Wireless (version 5 and above).

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SPANNING TREE PROTOCOL (STP)

- Bridge loop occurs when there is more than one path in a network bridge. The impact of this bridge loop is broadcast storms.
- Broadcast storm is sending frames (destination address is not known by the bridge), so the frame keep circling in the network without stopping.
- STP (Spanning Tree Protocol) protocol is used to prevent bridge loops STP can also be used as a fail over system
- RSTP (Rapid Spanning Tree Protocol) is a protocol that has a higher speed failover rather than STP. By default when create bridge it will choose RSTP.



2.1-LAB-Bridge

- *Connect wireless link between AP mode and station bridge mode*
- *Create two bridge port:*
  - *Ethernet 1 with WLAN (both sites)*
  - *Ethernet 2-5*
- *Assign IP addresses to bridge interfaces and computers*
- *Test ping from between laptops (port Ethernet 01)*
- *Test ping between Ethernet port 2 and port 5 in the same router.*

BRIDGE FIREWALL

RouterOS bridge interface supports firewall

Traffic which flows through the bridge can be processed by the firewall

To enable Bridge=> settings=> Use IP firewall

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	The bridge interfaces is physical that can assign IP Address.
		2	No way bridge between Ethernet interface with Wireless interface together.
		3	All wireless mode can be bridging, except station mode.
		4	For SOHO MikroTik router has default Bridge interface that bridge all interfaces.
		5	Bridge can be loop when there is more than one path in a network bridge.
		6	When loop have in MikroTik bridge interface, Rapid PVST+ is the protocol to prevent loop.
		7	STP protocol is enable by default when create the bridge interface.
		8	The bridge interface is the loopback interface when bridge interface without adding physical interface into port.
		9	Bridge process working on the network layer to forward frame between virtual interfaces.
		10	You can't assign IP Address to the member interface of bridge.

Answer the Questions

1. What is Bridge?
2. List the reasons when you have to create Bridge interface.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

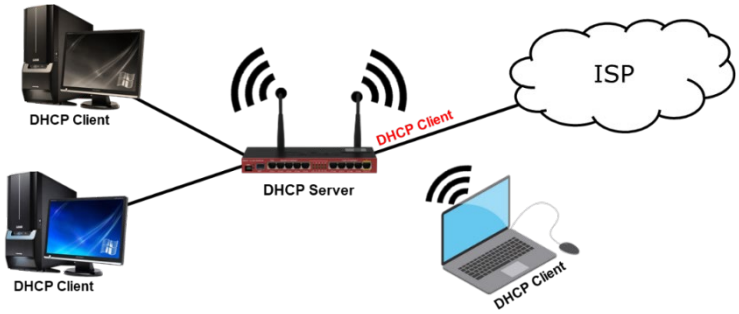
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 3: DHCP

OBJECTIVE

After finish, this lesson student will be able to:

1. DHCP Introduction
2. DHCP Keywords
3. DHCP Server setup
4. Lease management
5. DHCP Client
6. Address Resolution Protocol
    A. ARP mode
    B. ARP table



DHCP INTRODUCTION

The DHCP (Dynamic Host Configuration Protocol) is a protocol used for the distribution of IP addresses automatically in a network when a client request. The MikroTik implementation includes both:

- Client role: The Router acts as a DHCP client when it connects to the ISP (so ISP is the DHCP server). MikroTik SOHO routers by default have DHCP client configured on the ether1 (WAN) interface.
- Server role: The Router acts as a DHCP server for the internal LAN (so the internal PCs are the DHCP clients).

DHCP Keyword

Keywords should know before configure DHCP Server:

- **Pool**: Rank of IP Addresses for provide to Clients
- **Lease Time**: Time for update or lease IP Address to all devices.
- **Reservation** Address: Addresses keep for specific client with client mac-address. Ex. For manager, Director…..
- **Exclude Address**: Addresses exclude for assign static to a specific devices that no need DCHP server. Ex. Printer, Camera, AP,…

Before Configure DHCP Server

- Select ***Network address*** space (192.168.1.0/24)
- Keep ***exclude addresses*** (192.168.1.1-192.168.1.30)
- Select ***reservation addresses***
- ***Create pool address*** (192.168.1.31-192.168.1.254)
- Select ***DNS addresses server*** (8.8.8.8)
- Select ***Interfaces*** (ether1 / wlan)
- ***Lease time*** (3days)
- Don't forget to the choose correct ***default gateway***

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

DHCP CLIENT

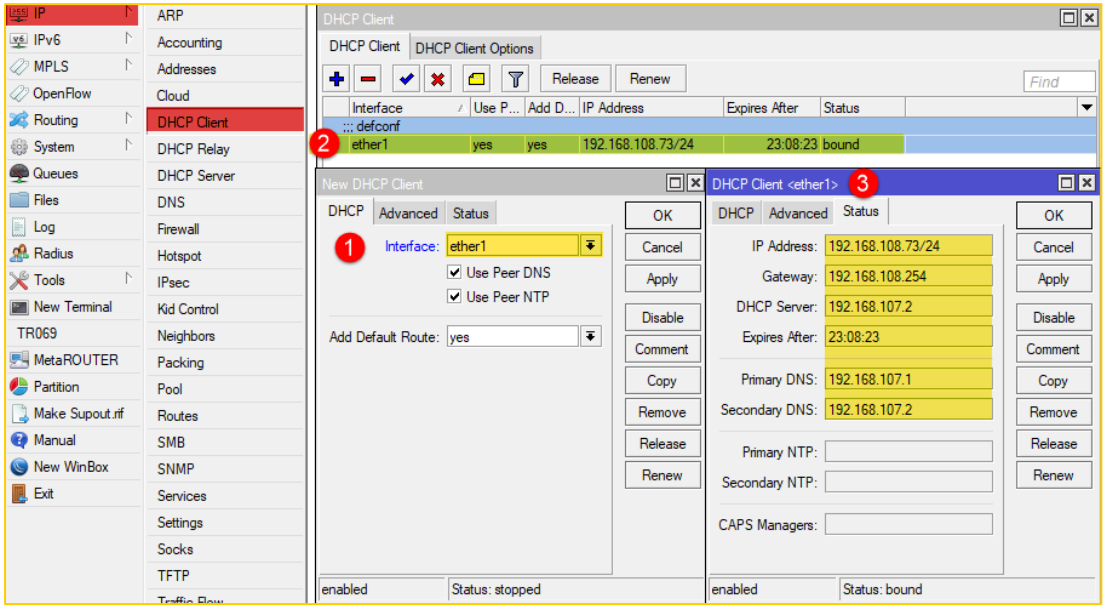
DHCP Client use on interfaces that want to get IP Address automatically from The DHCP server. Example: connect to ISP.

DHCP Client will accept:

- An IP address
- Netmask
- Default gateway
- Two DNS server addresses

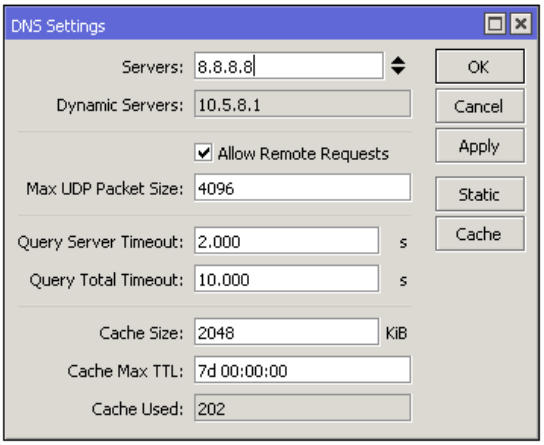
Enable DHCP Client: IP=>DHCP Client =>Chose Interface

Check Status to verify other option (Gateway, DNS..)



DNS

- Client that uses the DNS server will use the cache of the DNS server
- RouterOS can become DNS server, and we can manipulate DNS request
- By default DHCP client asks for a DNS server IP address.
- It can also be entered manually if other DNS server is needed or DHCP is not used.
- RouterOS supports static DNS entries
- By default there's a static DNS A record



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Note: some recommendation about using DNS.

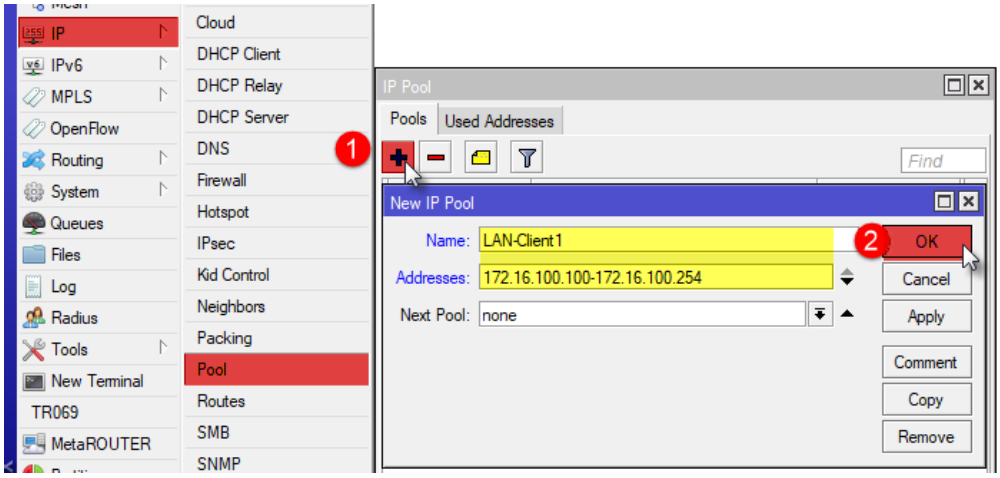
- Use ISP DNS in cast want to have fast update DNS record with service mail … server
- Use Public DNS in the cast have connection more than two ISP connections, so it is the best choice that we use public DNS.
- For the time is not so different if compare between DNS from ISP and Public DNS. Example, if you use ISP DNS, should be 2ms but if use google should be 30ms.So the time is not different and computer also has a cache to save the DNS record.
- For other reason ISP DNS have filter to block some content that we want to access.

DHCP SERVER SETUP

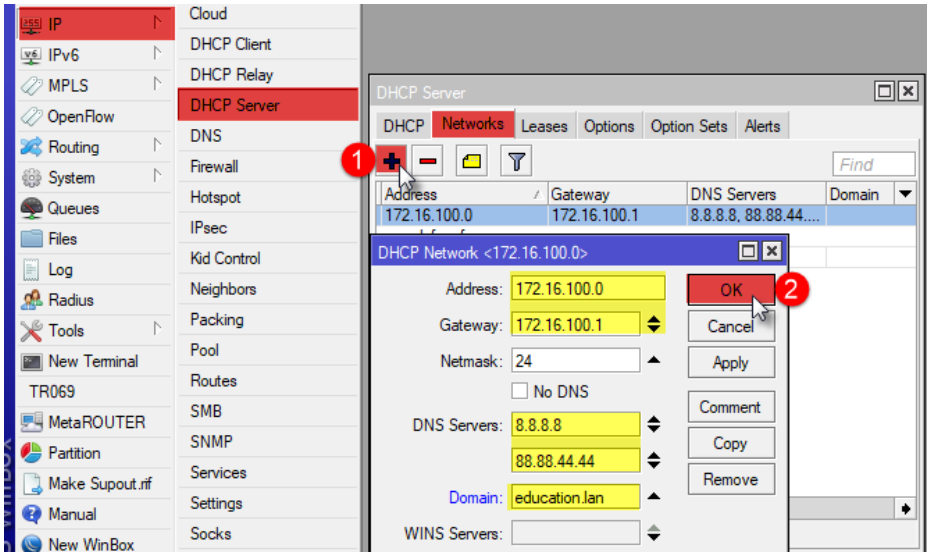
There are two ways to configure DHCP in MikrotTik:

First way:

1. Configure Pool

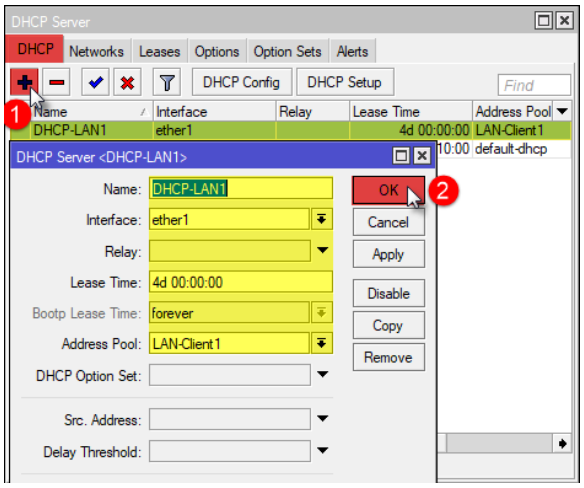


2. Configure Network, gateway, DNS

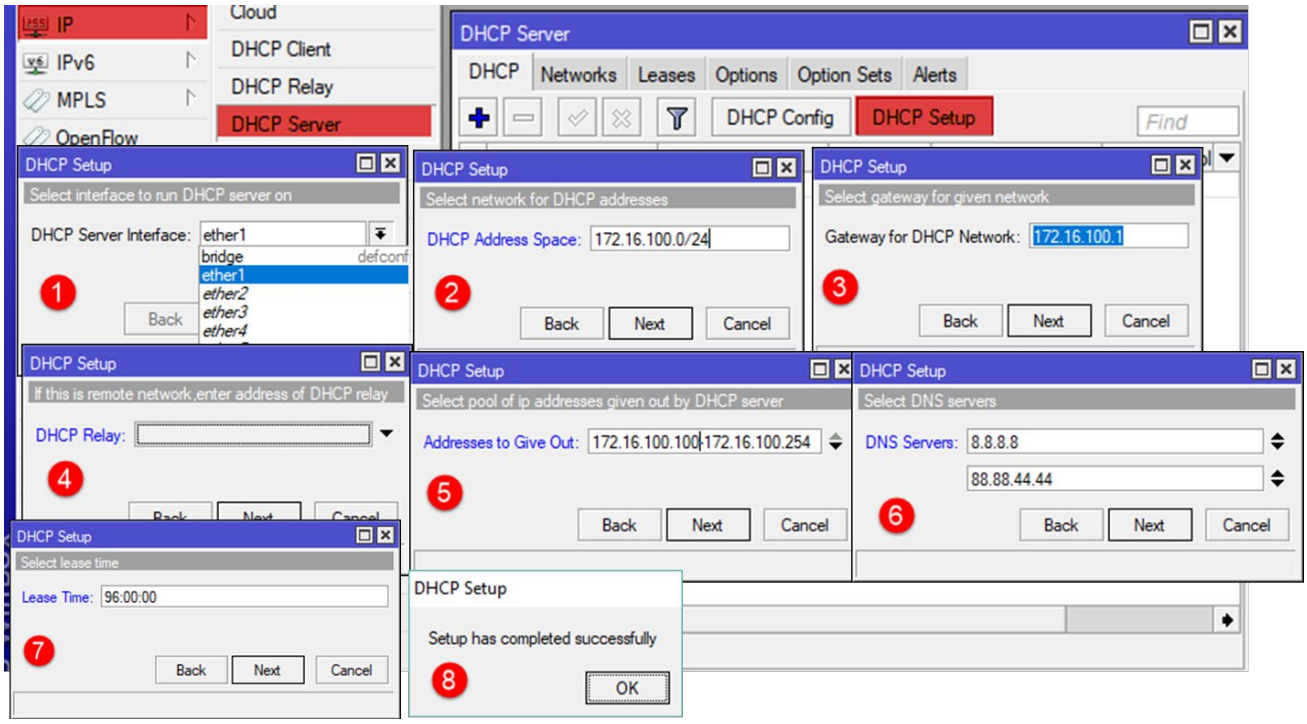


Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

3. Create DHCP Sever



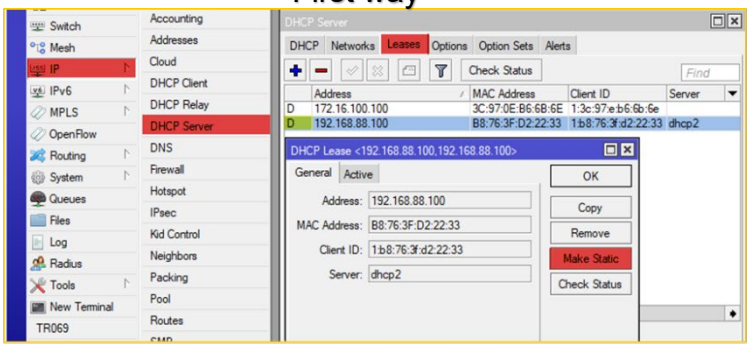
Second way: just click on DHCP Setup and follow step by step to complete the setup process.



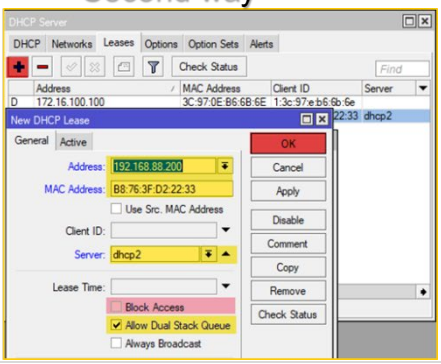
LEASE MANAGEMENT

We can use lease management to reservation address for specific device. Ex. Keep for manager or director. It will be easy to apply policy. It also can block device not allow to access the network.

First way



Second way



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

3.1-LAB-Connect to Internet

Teacher will demo how to do this before student perform doing their lab.

- *Connect your group router to Teacher's Router by WLAN interface*
- *Configure basic NAT to allow your computer can access the Internet.*

3.2-LAB-Configure DHCP Server /Client

- *DHCP Client:*
  - *Connect interface WLAN to TR router and enable DHCP client*
  - *Check to verify that WLAN get an IP address, DNS,..*
- *DHCP Server*
  - *Create Bridge interface name " Bridge-Test"*
  - *Add ports from 2-4 to Bridge-Test*
  - *Exclude IP address 192.168.1.1-192.168.1.100*
  - *Create Pool: name " Test-Pool" with the rest of the IP addresses left*
  - *Create Network: 192.168.1.0/24, DNS: 8.8.8.8, domain: testing.lan*
  - *Create DHCP server: name " DHCP_Testing" chose interface " Bridge-Test", Lease time: 5 days.*
  - *Keep IP address 192.168.1.200 for specific Device.*
  - *Verify with client and make sure all client can ping each other and access to Internet.*

Note:

Routers cannot reach to the outside network.

- Check whether the wireless or cable is connected.
- Check whether it is running a DHCP client and obtain IP

The Router can ping public IP address but cannot ping the domain name.

- Check IP DNS (allow remote request)

Computers cannot ping the router

- Check IP address (make sure subnet /24)

Computers can ping to outside IP but cannot ping the domain => Check IP DNS on the computer.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

ADDRESS RESOLUTION PROTOCOL

- Address Resolution Protocol
- ARP joins together client's IP address with MAC address
- ARP use to mapping Layer 3(IP address) to Layer 2 (MAC Address).
- ARP Operates dynamically, but for some security reasons, ARP can also be manually configured.
- If manually configured, client will not be able to access the Internet if they changed IP address.

ARP

IP= 192.168.100.1 => MAC: B8:76:3F:D2:22:33

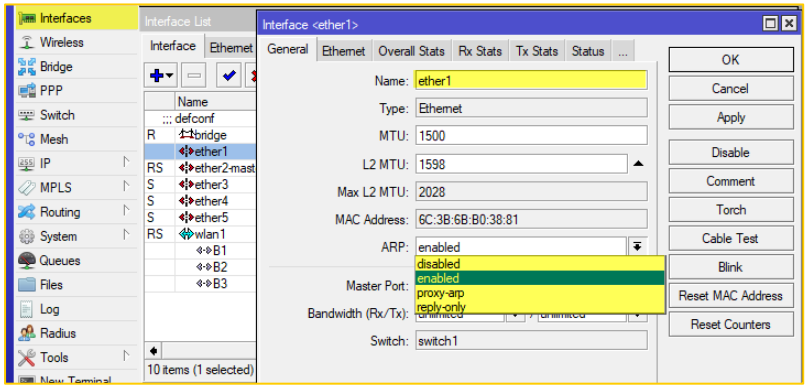
Interface ARP Mode

There are 4 kinds of interface ARP Mode in MikroTik

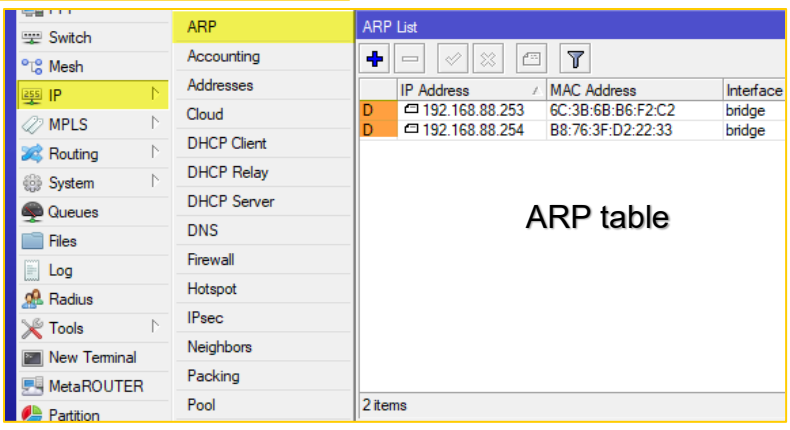
- Enable: default is enabled on all interfaces in MikroTik. All ARPs will be discovered and dynamically added to the ARP table.
- Proxy ARP: Router will act as a transparent proxy ARP between it or more networks are connected directly.
- Reply Only: Routers only allow static ARP reply it was found in the ARP table, router is only accessible by a combination of IP and MAC address found and make static in the ARP table.
- Disable ARP: Requests from clients are not answered by the router. Therefore, staic ARP entry should be added in addition to the side of the router is also client side.

For example: on Windows using the arp command:

C:\> arp –s 192.168.200.1 00-ad-de-ff-a8-1e



ARP mode on interface



ARP table

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

3.3-LAB-ARP Mode

- *Connect your laptop with ether1, and assign IP address of both so that you can ping to router*
- *Set interface ether1 ARP mode is reply-only and try to ping the router from your laptop again.*
  - *Do your computer can reach the router?*
- *Add IP and MAC address manually to ARP list*
- *Test to ping again!*

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

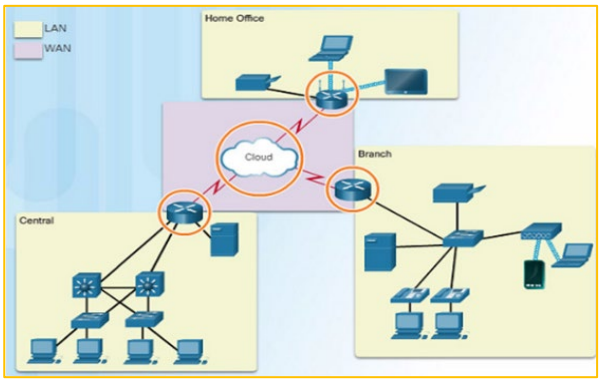
CONCEPTs REVIEW

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 4: ROUTING

OBJECTIVE

1. Routing Overview
    - Routing concepts
    - Route flags
2. Static routing
    - Creating routes
    - Setting default route
    - Managing dynamic routes
    - Implementing static routing in a simple network



WHAT IS ROUTING?

- Routing process to forward the packets from one network to another network using internetwork device (Router, Firewall, Switch layer3...).
- Static routing: Administrator configure route path (best path) in routing table by manually (Static route).
- Dynamic routing: Administrator configure dynamic routing protocol configuration and route path will add automatically to routing table.

CONNECTED ROUTE

- Connected Route formed automatically if we add an IP address on the valid interface (active interface).
- If there are, two IP addresses that belong to the same subnet were assigned to one interface that will only create one connected route.
- If there is 1 IP address was assigned to 2 different interfaces, it will create only one connected route with two gateways, it will make router confuse the gateway (except in point to point interfaces)

STATIC ROUTE

- Static route created by adding route manually in routing table.
- Normally, in static route we only add **destination network** and the **gateway.**
- We can say that we define a route to which network, through which gateway.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

BASIC ROUTING CONCEPT

Router will choose route base on:

- The route must be active
- Most specific destination address
- Smallest Administrative Distance
- Round Robin (random) if there are multiple gateways

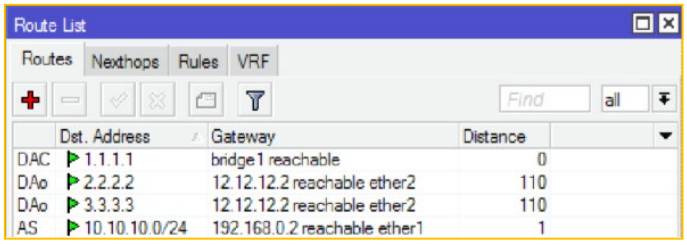
RUTING FLAGS

- D = Dynamic
- A = Active

- C = Connected
- S = Static
- b = BGP
- o = OSPF
- r = RIP

- U = Unreachable
- B = Black hole

Examples:
DAC = Dynamic, Active, Connected
AS = Active, Static



ROUTE PARAMETER

Destination

- Destination address & network mask (ex. 192.168.200.0/23
- 0.0.0.0/0 match to all destination networks

Gateway

- IP Address of gateway, must be IP address that has same subnet of on of IP address that assign in router interfaces.
- Gateway can be filled by an interface if IP address of the gateway is unknown or that is dynamic IP address.

Distance / Administrative Distance

- Use for selection of the best routes to use
- The smaller, the better

Scope & Target Scope

- Use for recursive next hop lookup (gateway of the router in the next hope)

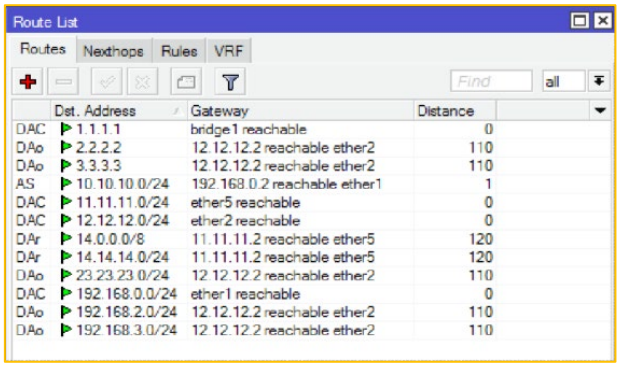
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

BASIC ROUTING CONCEPT

Router will choose route base on:

1. The route must be active
2. Most specific destination address

   (Ex. Destination 192.168.0.128/26 is more specific than 192.168.0.0/24)
3. Smallest Administrative Distance
4. Round Robin (random) if there are multiple gateways



4.1-Activity

For destination 192.168.10.1, which gateway will be chosen as best route?

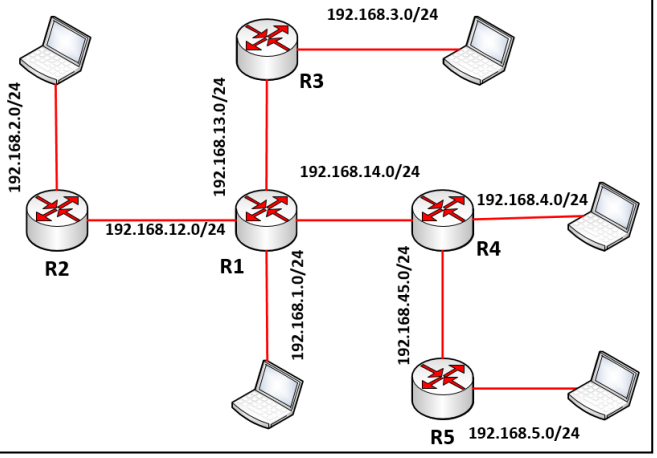
Flag	Destination	Gateway	Distance
AS	192.168.10.0/28	192.168.1.1	1
AS	192.168.10.0/24	192.168.1.2	1
S	192.168.10.0/30	192.168.1.3	1
AS	192.168.10.0/29	192.168.1.4	5
AS	192.168.10.0/29	192.168.1.5	1

4.2-LAB-Static Routing

- *Reset Router configuration to factory with no default configuration*
- *Use the topology and create static routing*
- *Each laptop should be ping each other.*

Try to configure two ways:

- *On interface*
- *On Command line*



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

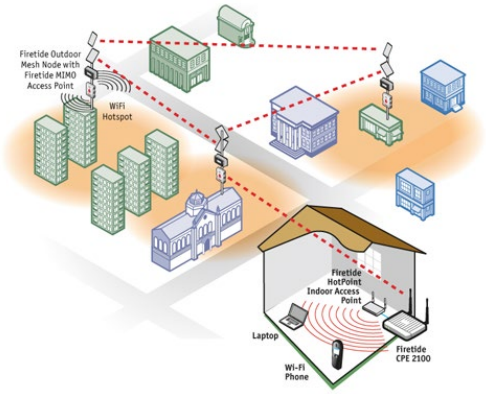
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 5: WIRELESS

OBJECTIVE

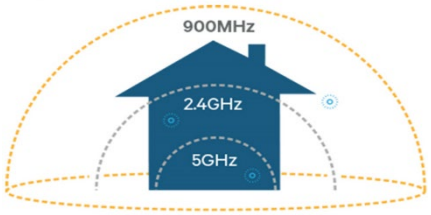
After finish this lesson student will be able to:

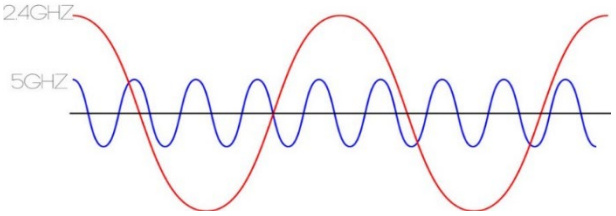
1. 802.11a/b/g/n Concepts
    - Frequencies(bands, channels) data-reates / chains (tx power, rx sensitivity, country regulations)
2. Setup a simple wireless link
    - Access Point configuration
    - Station configuration
    - Wireless security and Encryption



WIRELESS ON ROUTEROS

- RouterOS support wireless card for Wi-Fi (Wireless Fidelity= Full version of WiFi).
- Frequency is the number of complete cycles per second in alternating current direction.
- The standard unit of frequency is the hertz, abbreviated Hz. If a current completes one cycle per second, then the frequency is 1 Hz, if completes 60 cycle per second, then 60 Hz.
- WiFi has specification and standardization IEEE 802.11 and use frequency 2.4GHz and 5GHz.

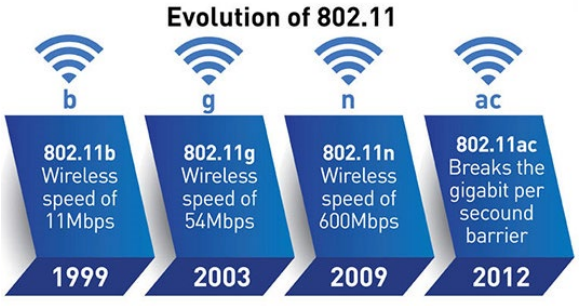




Wireless that supported by RouterOS has IEEE 802.11 a/b/g/n standard:

- 802.11a: frequency 5GHz, 54Mbps.
- 802.11b: frequency 2.4GHz, 11Mbps.
- 802.11g: frequency 2.4GHz, 54Mbps.
- 802.11n: frequency 2.4GHz or 5GHz, up to 600Mbps*
- 802.11ac: frequency 5GHz, up to 1300 Mbps*

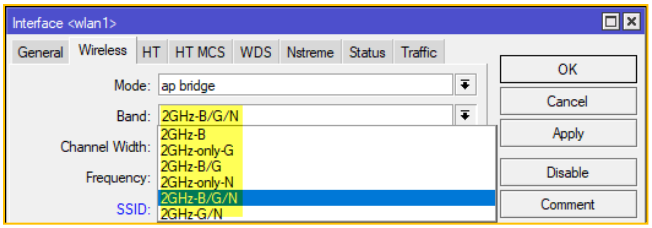
- Depending on RouterBOARD model



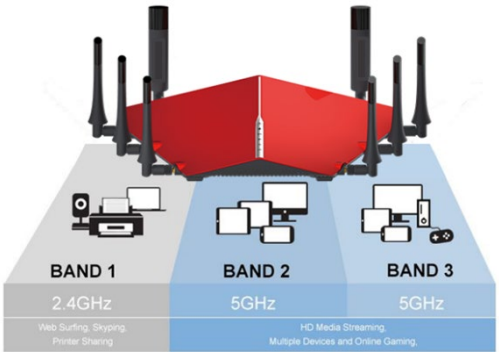
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

WIRELESS –BAND

- **Band** is a working frequency of a wireless device.
- To connect two devices, both of them have to work on the same frequency band.
- Common frequency band in WiFi are 2.4 GHz and 5 GHz.

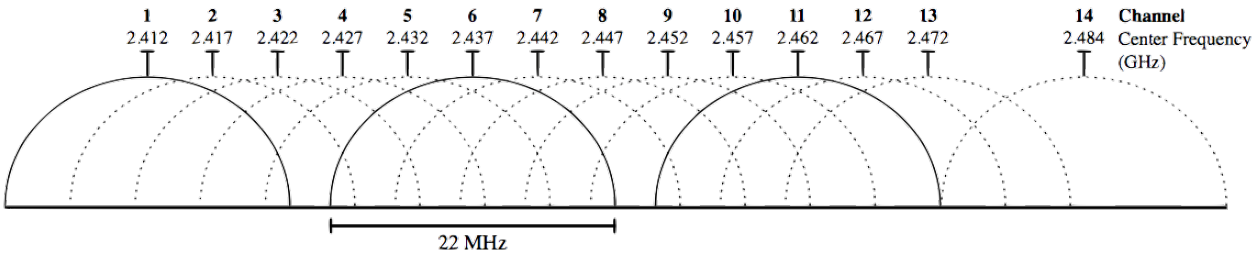


Band on the list is depend on wireless card installed.



WIRELESS –FREQUENCY CHANNEL

- Band frequency divided into Frequency **channel**
- Access Point (AP) will operate at any frequency channel we choose.
- Channel values depend on the selected band, the ability of wireless cards, and rules / regulations frequency of a country
- **2.4GHz Channels**
  - 13x22MHz Channels (most of the world)
  - 3 non-overlapping channels for 2.4GHz (1,6,11), it mean you can put 3 Aps in the same area without interfering.
  - US: 11 channels, 14th Japan-only



- **5GHz Channels**
  - RouterOS supports full range of 5GHz frequencies
  - 5180-5320MHz (channels 36-64)
  - 5500-5720MHz (channels 100-144)
  - 5745-5825MHz (channels 149-165)
  - Varies depending on country regulations

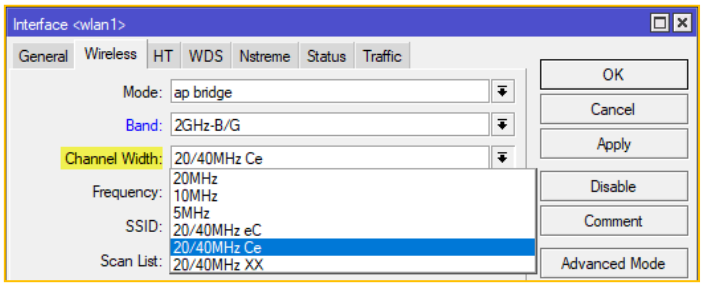
IEEE Standard	Channel Width
802.11a	20MHz
802.11n	20MHz
	40MHz
802.11ac	20MHz
	40MHz
	80MHz
	160MHz

5GHz Band
36 - 5.180
40 - 5.20
44 - 5.220
48 - 5.240
52 - 5.260
56 - 5.280
60 - 5.300
64 - 5.320
149 - 5.745
153 - 5.765
157 - 5.785
161 - 5.805
165 - 5.825

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

WIRELESS –CHANNEL WIDTH

- **Channel width** is the frequency range lower limit and upper limit in 1 channel.
- RouterOS can set how wide the channel to be used.
- The default width of the channel used is 22MHz (written in 20MHz).
- Channel width can be reduced in size (5MHz) reach long distance, or raised (40MHz) to gain greater throughput.
- If you use 2.4 Ghz broadcasting radio, you should use 20 Mhz for the channel width. The simple reason is that 20 Mhz is really a supportive measure for your older devices.
- If you use 5 Ghz broadcasting radio, the chances are that your network is only consisted of the latest devices that support 802.11n. This is when you should use the 40 Mhz bandwidth.
- When You Should Use Combination of 20 / 40 Mhz Combination.
    - 20 MHz - If your network has clients with 802.11b, g and not n or ac.
    - 40 MHz - If your network has clients only with 802.11n or above i.e ac.
    - 20/40MHz - If you have both type of clients.
- How to control Channel
    - For 20 Mhz broadcasting with 2.4 Ghz
        - The best channel band to use are 1, 6, 11
- For 40 Mhz broadcasting with 2.4 Ghz
    - The best channel band to use are 3, 11



- C= Primary control
- e= Addition channel
- X= C or e

20/40MHz Ce = Primary channel is 20MHz and addition channel is 40MHz

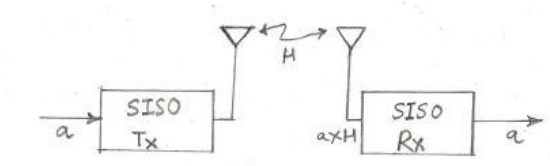
WIRELESS CHAINS

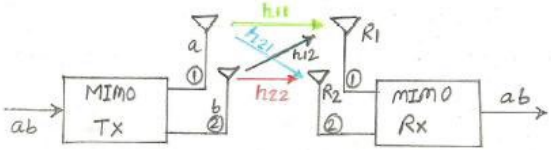
- 802.11n introduced the concept of MIMO (Multiple In and Multiple Out)
- Send and receive data using multiple radios in parallel
- 802.11n with one chain (SISO) can only achieve 72.2Mbps (on legacy cards 65Mbps)

SISO vs MIMO

There are different forms of single / multiple antenna technology:

- SISO - Single Input Single Output
- SIMO - Single Input Multiple output
- MISO - Multiple Input Single Output
- MIMO - Multiple Input multiple Output





Single Input Single Output (SISO) is the antenna technology has only one antenna is used at transmitter and receiver.

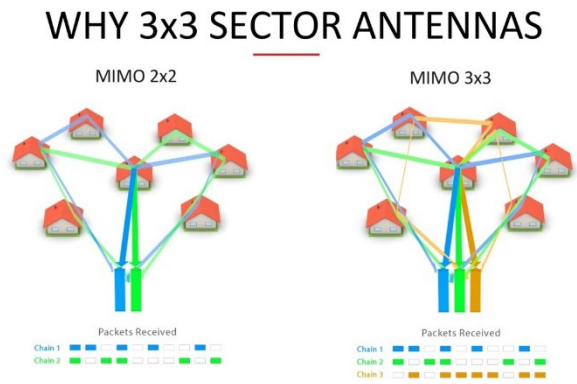
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

MIMO is a wireless technology that uses multiple antennas that are used as source (transmitter) and destination (receiver) to transfer more data at the same time.

Devices with a single antenna and radio are 1x1 MIMO device and are able to communicate via a single stream of transmit or receive. 2x2 MIMO devices with dual antennas and radios communicate via 2 streams of transmit and receive. 3x3 MIMO devices with 3 antennas and radios are capable of transmitting and receiving via 3 streams.

Stream: transmit independent and separately coded data signals use in MIMO

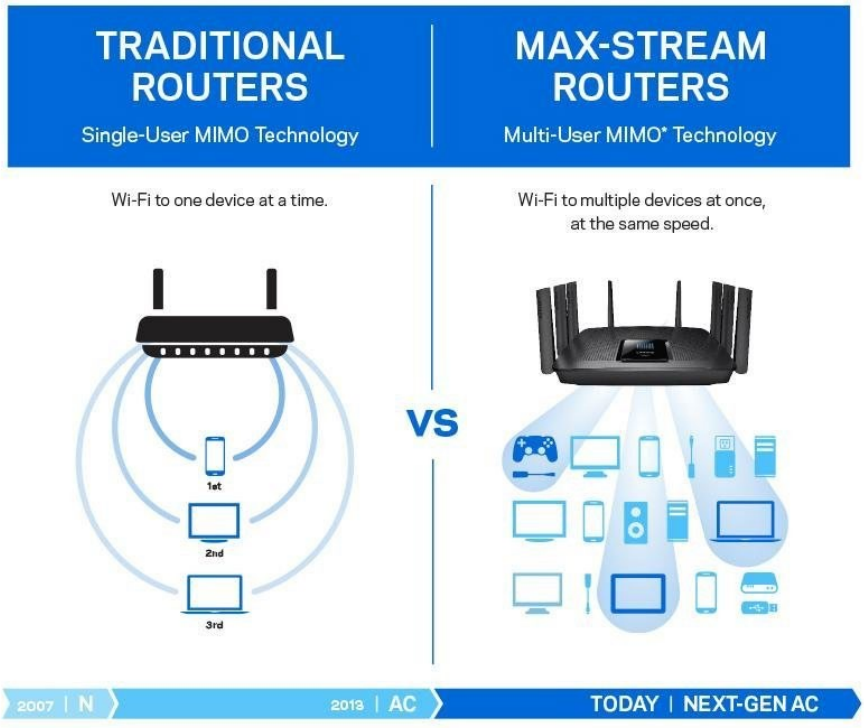
Dual Chain = 2x2 MIMO



SU-MIMO Vs MU-MIMO

Su-MIMO is the technology of antenna that use to transmit and receive data, SU-MIMO serve the device one by one.

MU-MIMO is the technology of antenna that can serve many devices at the same time.



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

COUNTRY REGULTIONS (FREQUENCY REGULATION)

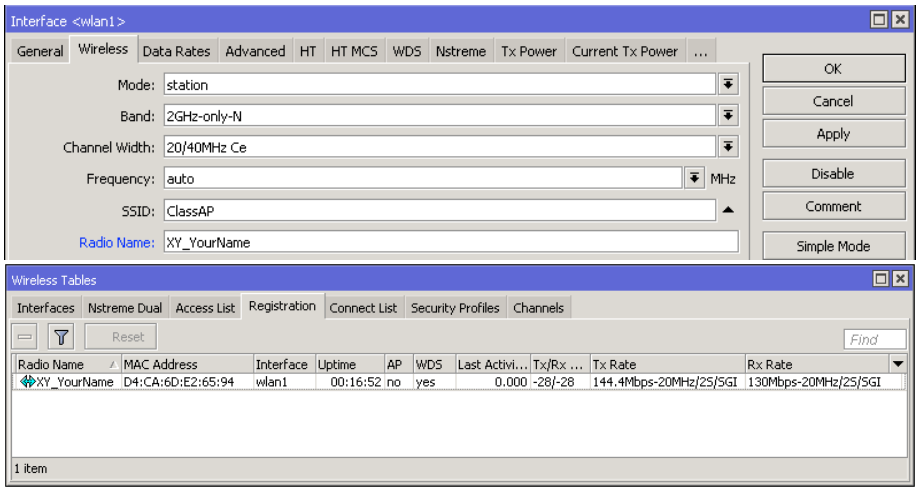
- Each state has certain regulations in terms of frequency for wireless internet carrier.
- Frequency regulation in RouterOS defined in the Wireless "country-regulation".
- However, if it is desirable to open up all the frequencies that can be used by the wireless card, we can use the option "superchannel"

5.1-LAB-Country regulations

- *How many RouterOS default frequency channel in 2.4GHz?*
- *Check in the menu wlan1 Wireless=>Frequency*
- ---
- *How many channels frequency regulation for the country?*
- *Check in the adapter wlan1 to Advanced Mode.*
- ---
- *How many frequency channels if change to Frequency Mode to " supperchannel"?*

RADIO NAME

- Wireless interface "name" use to identify the name of your wireless radio in order easy to connect from AP to other AP.
- RouterOS-RouterOS only
- Can be seen in Wireless tables



5.2-LAB-Radio Name

- *Set the radio name of your wireless interface as follows: Yourname(XY)_Yourname*
- *For example: 23_Nivath*

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

WIRELESS INTERFACE MODE

AP Mode

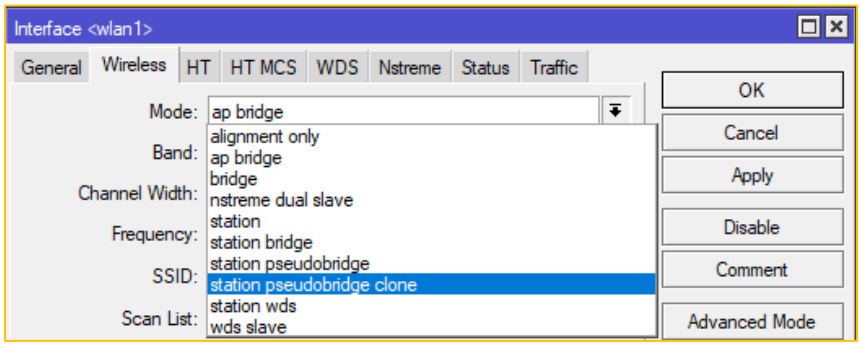
- AP-bridge - work as wireless Access Points.
- Bridge - almost the same as the AP-bridge, but can only be connecting by 1 station / client, this mode is typically used for point-to-point.

Station Mode

- Station -basic station mode. Find and connect to acceptable AP with the same SSID and frequency, in this mode CAN NOT BRIDGING
- station-bridge - the same as the station, this mode is MikroTik proprietary. CAN BE BRIDGING
- Station-wds – Same as station, but create WDS link with AP, using proprietary extension. AP configuration has to allow WDS links with this device. Note that this mode does not use entries in wds.
- Station-pseudobridge – same station, in addition to MAC address translation for the bridge., can be bridging
- Station-pseudobridge-clone – Same as station pseudobridge, using station-bridge-clone-mac address to connect to AP, can be bridging

Special Mode

- Alignment-only – transmit continuously used for antenna positioning.
- nstreme-dual-slave – used for nstreme dual technology
- Wds-slave – this is repeater mode, can connect with AP, another wds-slave, and station.



BASIC CONCEPT OF WIRELESS CONNECTION

- Suitability Mode: AP with Station, AP with Repeater, Repeater with Repeater)
- Same BAND
- Same SSID (0-32 characters): name of WiFi that you see on your device.
- Same encryption and authentication
- Not necessarily, the same frequency of channel, station will automatically follow the frequency channel of AP.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

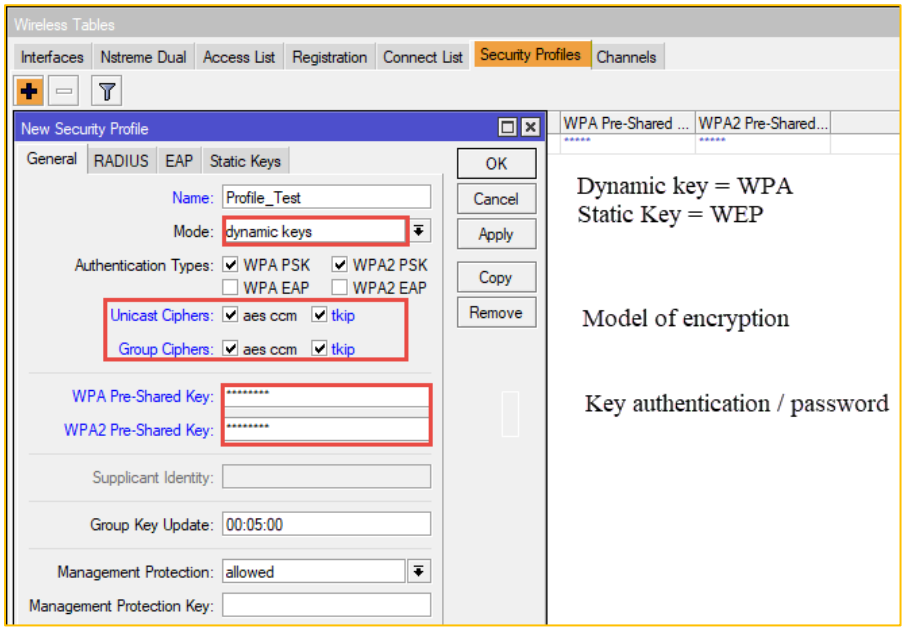
SECURITY

For wireless security connection, not only with the MAC-Filtering enough, because the data through the network can be retrieved and analysed by unauthorized person.

There are other security methods that can be used as following:

- Authentication (WPA-PSK, WPA-AEP)
- Encryption (AES, TKIP, WEP)

All wireless encryption options are on the menu Wireless => Security Profile. Security profiles are given specific names to be implemented in the wireless interface.

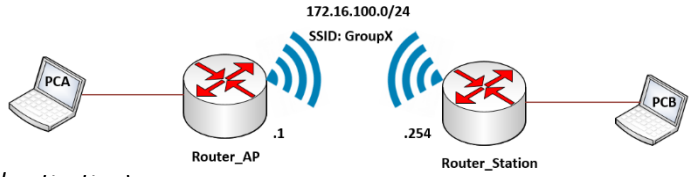


- Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) is a security mechanism used to authenticate and validate users on a wireless LAN or WiFi connection. WPA-PSK configure by passphrase or password of eight to 63 characters and 256-character key is generated, shared and used by both devices for network traffic encryption and decryption. WPA uses TKIP (temporal Key Integrity Protocol) encryption.
- Wi-Fi Protected Access 2 - Pre-Shared Key (WPA2-PSK), and also called WPA2 Personal, is the improved version of WPA but it is capable of using **TKIP** or more advanced **AES** algorithm. Theoretically, WPA2 is hard to hack while WPA is. WPA2 requires more processing power than WPA.
- Temporary Key Integrity Protocol (TKIP) is an encryption method use for WLAN. TKIP is actually an older encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time. TKIP is actually quite similar to WEP encryption. TKIP is no longer considered secure, and is now deprecated. In other words, you shouldn't be using it.
- AES (advanced Encryption standard) is a more secure encryption protocol introduced with WPA2. AES is the latest Wi-Fi encryption standard and latest encryption for Wi-Fi.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

5.3-LAB-Wireless AP & Station

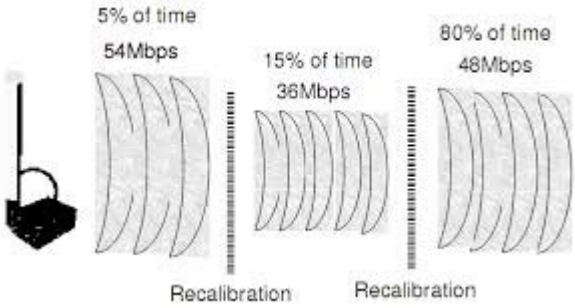
- *There are two routers*
  - *One will be Access Point*
  - *One will be Station*



- *Set with same SSID, and security profile (authentication)*
- *Setting IP Address for wlan interface:*
  - *IP AP=172.16.100.1/24*
  - *IP station=172.16.100.254/24*
- *Make sure Layer 1 connection (wireless) connected, and make sure assign IP address correctly with correct interface.*
- *Test by ping between router*
- *Test by ping between computer client (some necessary configure need)*

RATE FLAPPING

- Data rate is a value that describes how much digital data that can be moved from one location to another in seconds.
- Data rate is influenced by the signal strength
- Rate flapping occurred because up and down of data rate
- Rate flapping can be prevented by choosing a lower data rate in order to link more stable.



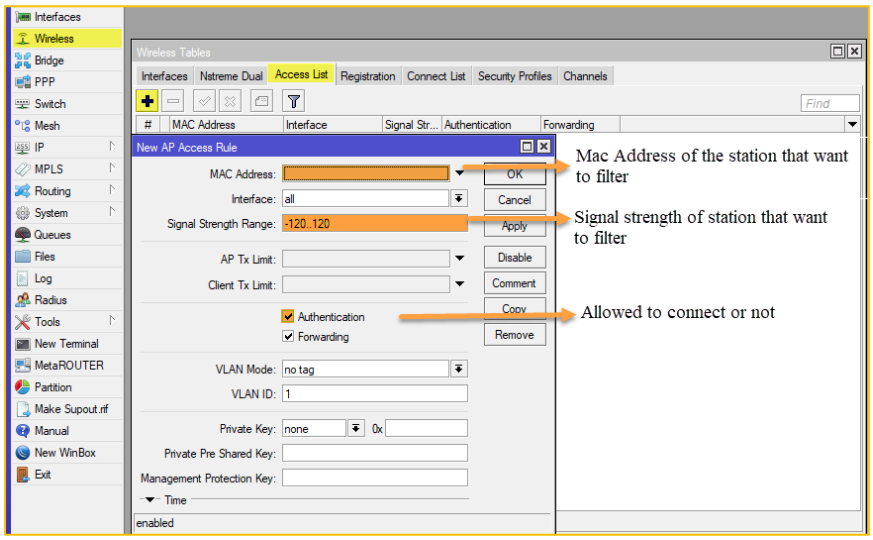
WIRELESS MAC FILTERING

- In Access Point, we can choose which clients can connect to us, and which one can't**.**
- In Station, also can be locked to one Access Point have been determined**.**
- To filter who can connect and who cant connect in wireless link, it uses MAC address filtering
- MAC address filtering in Access point configured in the Access List menu MAC address filtering in Station configured in Connect List.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

ACCESS POINT-ACCESS LIST

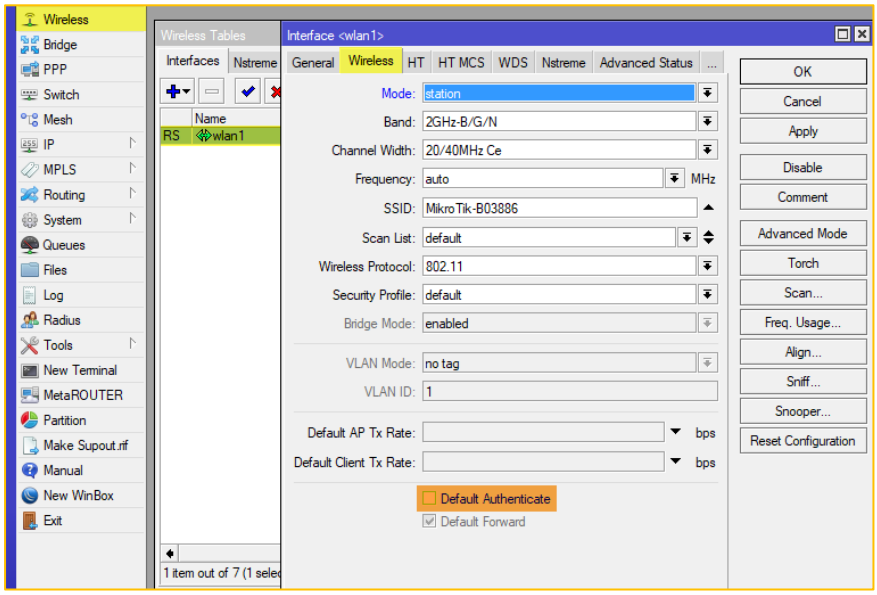
Access List in Access Point, to filter which station allowed connecting:



ACCESS POINT-DEFAULT AUTHENTICATE

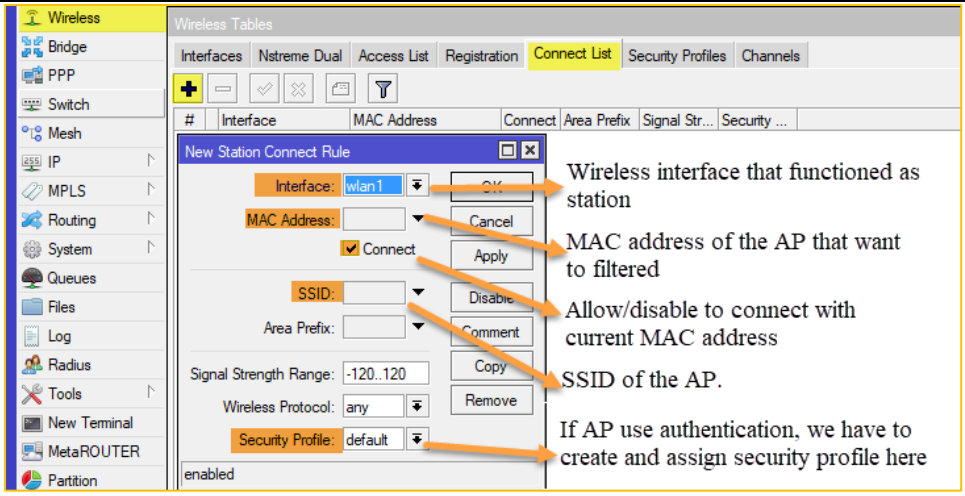
Access List can work if the default authentication in wireless is disable (uncheck).

If it uncheck, by default station will not be able to connect to the AP if not in the allow in the Access List.



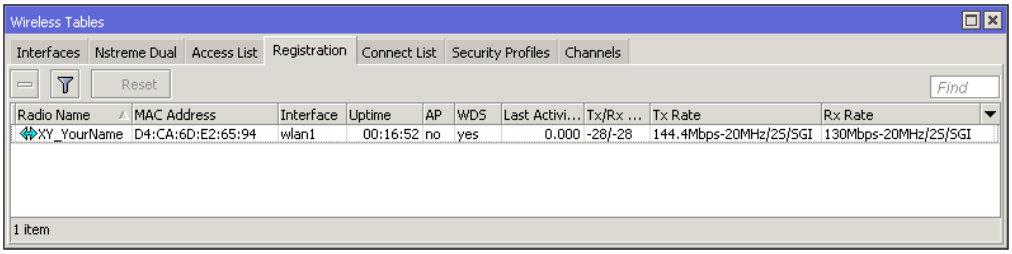
In Station, Connect List can chose which one of AP allow to connect.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org



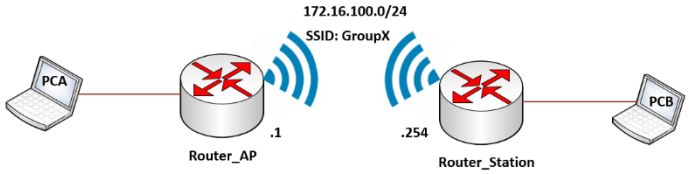
REGISTRATION TABLE

- Used by access point to control allowed connections from stations
- Identify device MAC address
- Configure whether the station can authenticate to the AP
- Limit time of the day when it can connect



5.4-LAB-MAC Filtering

- *Keep configuration from LAB-5.4*
- *Both AP and Station lock connection between your partner by filter MAC Address of AP/Station*
- *For the wireless settings on the AP, the default authentication should be unchecked, so that not all clients can connect automatically.*
- *Test by connect to other group.*



VIRTUAL ACCESS POINT

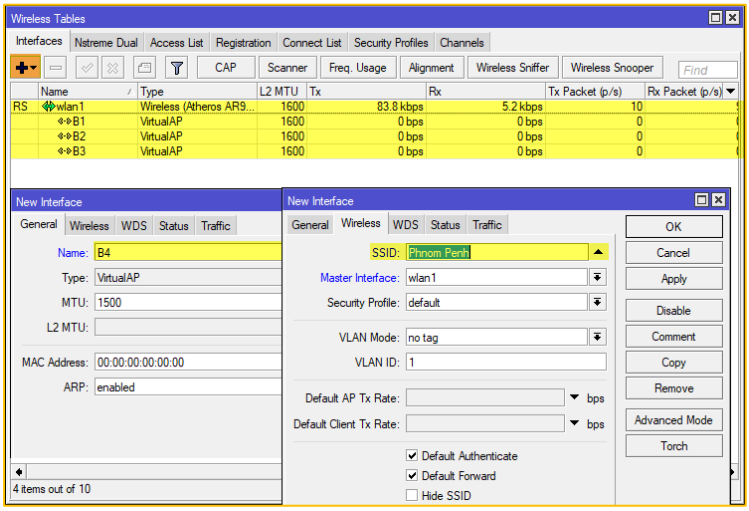
Virtual AP will become child of the wlan1 (real interface). One interface can have multiple virtual APs (maximum 128)

Virtual APs can be set with different SSID, different security profiles and different access lists, but will use the same frequency and band

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Virtual AP is the same as the AP:

- Can be connected to the stations / clients.
- Can function as a DHCP server.
- Can function as a Hotspot server.



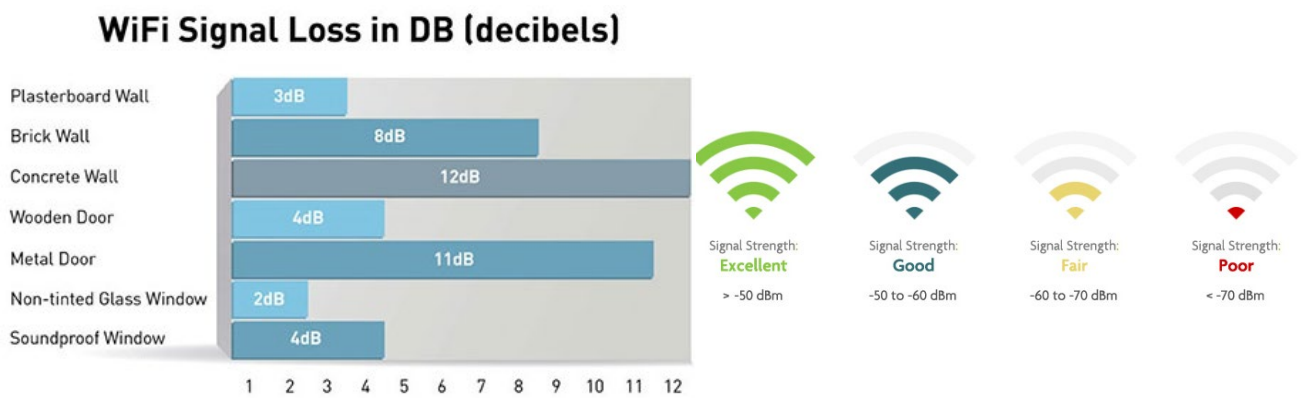
5.5-LAB-Virtual Access Point

- *Connect your WiFi to Teacher Wifi*
- *Create DHCP Server with network 192.168.xx.0/24*
- *Create Virtual WiFi*
  - *SSID: PNCXX*
  - *New security profile*
- *Apply DHCP server to Virtual WiFi*
- *Allow Client get IP address fix : 192.168.xx.100/24*

Factors Affecting Wireless Network Connection (Speed Performance or Coverage)

As wireless signals travel through the atmosphere, they are sensitive to different types of impediments and interference as compared to wired network.

Physical Obstruction:



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

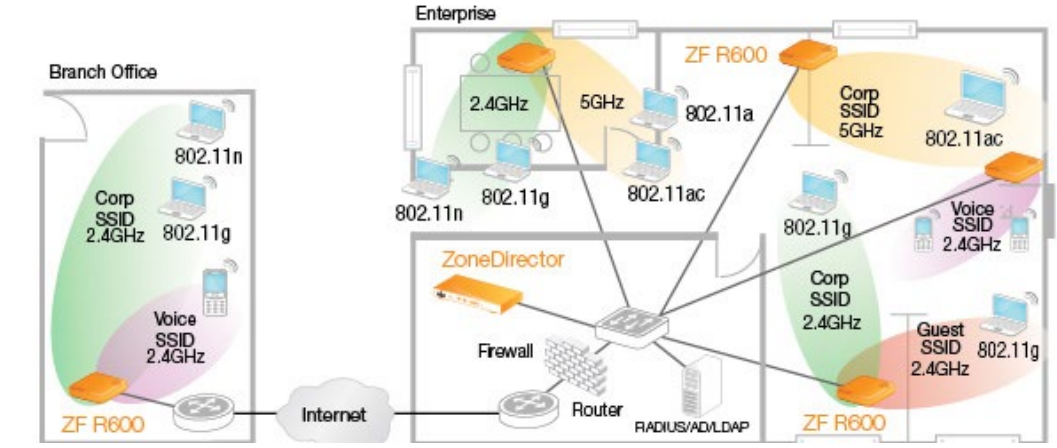
Interference: WiFi network operates at 2.4GHz and 5GHz band, other wireless devices using the same frequencies could cause interferences, resulting poorer WiFi receptions. Microwaves, cordless phones, baby monitors, wireless game controllers and Bluetooth devices all operate on the same wave spectrum of 2.4GHz as WiFi routers.

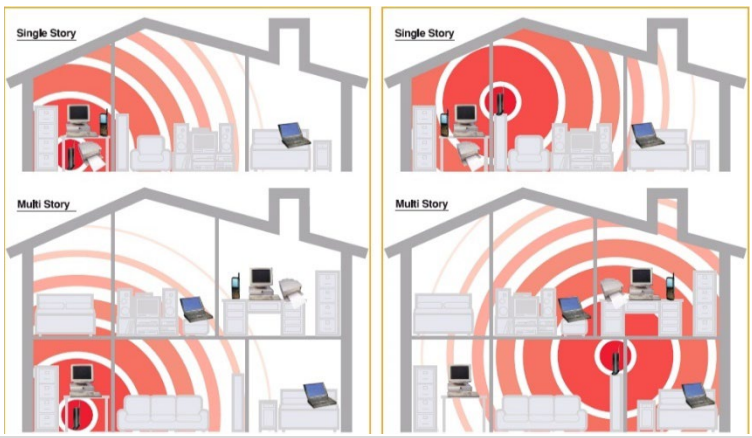
Shared bandwidth: The bandwidth of wireless network is shared among all the wireless users, so the more users you have, the slower the network becomes.

Distance: If you're sitting near a wireless router or access point, you will experience a faster network speed. But if another person is sitting far from the wireless router or access point, the network speed of both computers will drop drastically.

Speed of connected device: The achievable download and upload speed of the device connected to the WiFi network is also dependent on the device itself. A mobile phone with better processor and more advanced antennas and radios design will promise higher download and upload speed.

Location: Where an Access Point or wireless router is placed also makes the difference. Place the devices in higher ground to reduce the impact of physical objects.

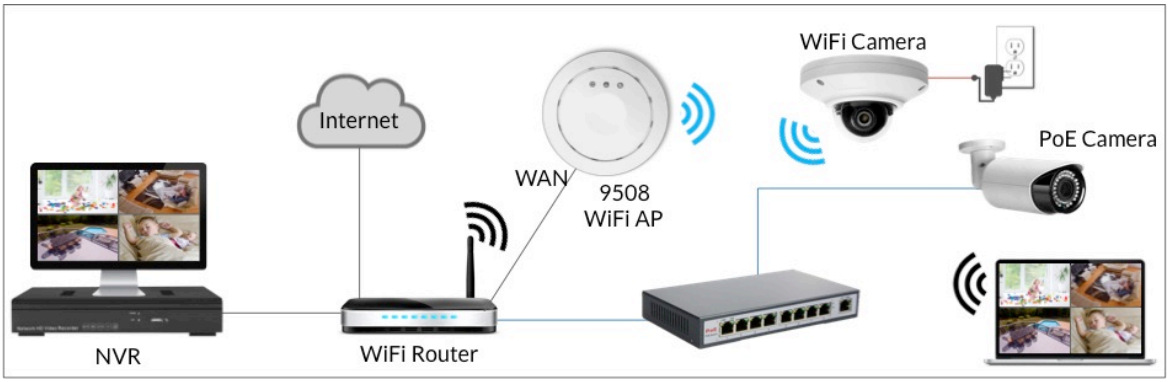




Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

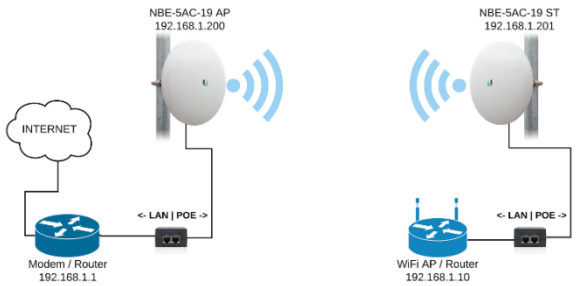
BASIC WIRELESS SCENARIO

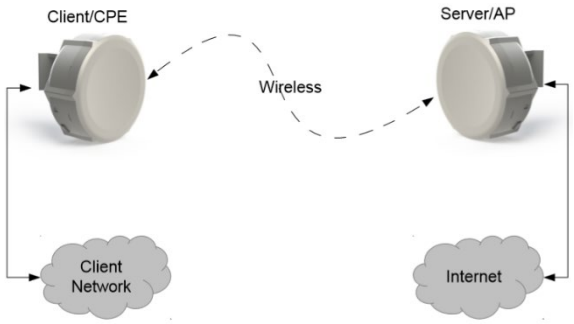
1- Use for share network and Internet connection



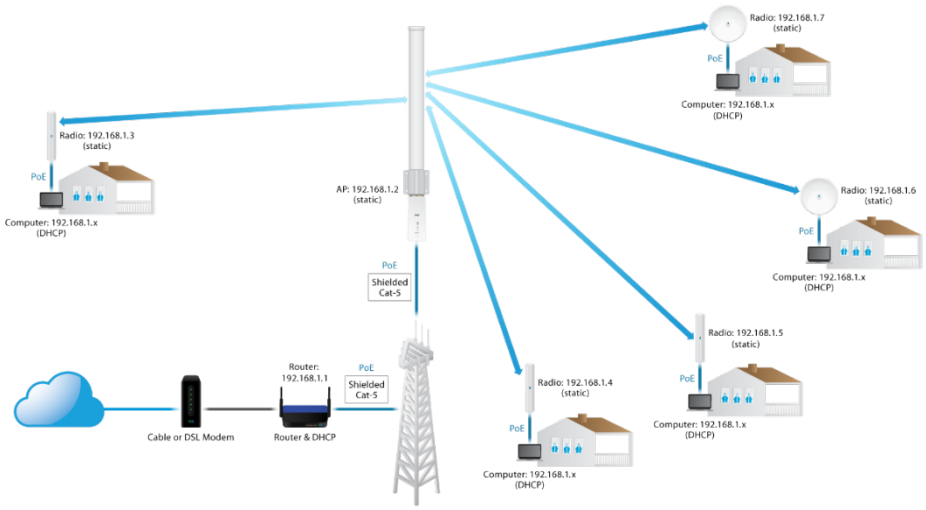
2- Extend connection

Point-to-Point (PTP)





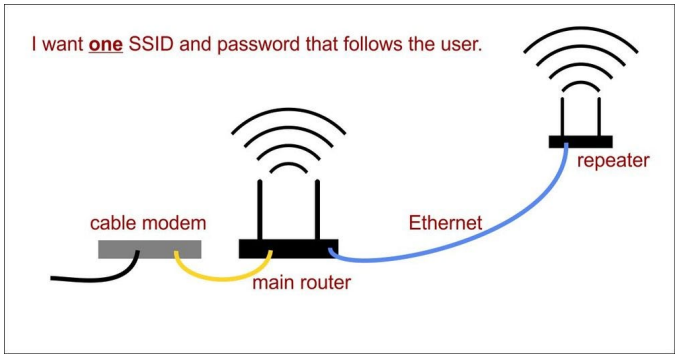
Point to Multi Point (PTMP)

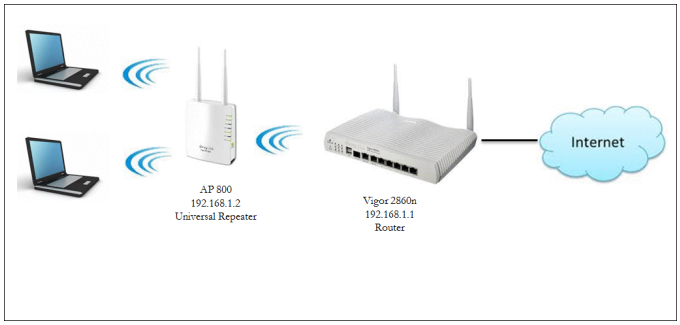


Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

WiFi-Roaming

Wireless Repeater





Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

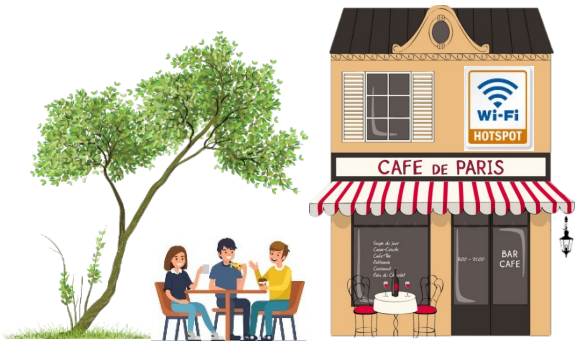
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 6: HOTSPOT

OBJECTIVE

After finish, this lesson student will be able to:

- Hotspot Overview
- Hotspot Benefits
- Hotspot Setup
- Bypass users
- Walled Garden
- Walled Garden IP List
- Limit Speed users Hotspot
- Share Users Hotspot



HOTSPOT OVERVIEW

- Hotspots are used to provide access services (Internet/ Intranet) in the private or public area, using cable or wireless.
- Hotspots provide web services authenticated username and password before access to network (Internet).
- Hotspot can limited by bandwidth, time (time-based) or the amount of data that download / upload.

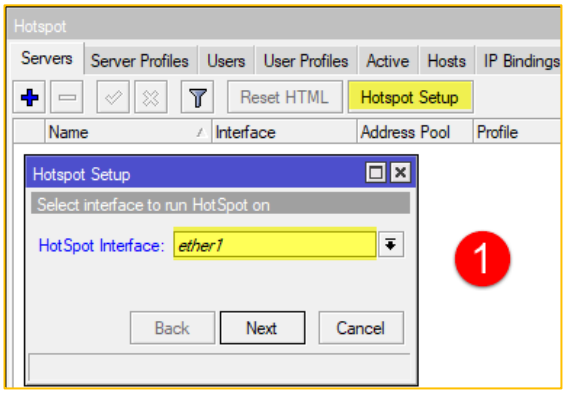
HOTSPOT BENEFITS

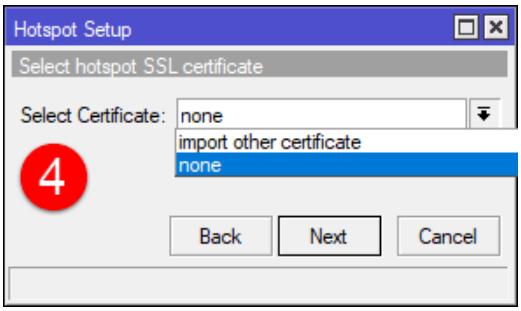
- Require Security login page to internet.
- Provide friendly page login by editing.
- Provide Advertisement own company web page login.
- Provide specific website, bypass the more specific resource at a certain protocol and port.
- Provide bandwidth limitation per user login hotspot.
- Share User Hotspot can access in the same time.
- Interact with other radius server & user---manager in Mikrotik.
- Easy for customize page whatever you like

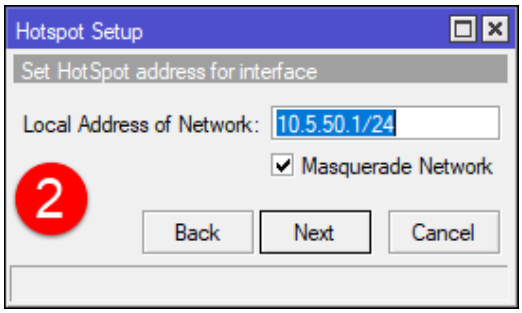
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

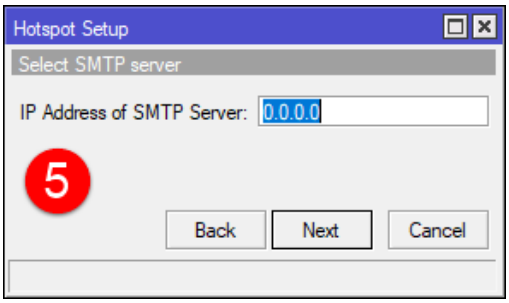
HOTSPOT SETUP

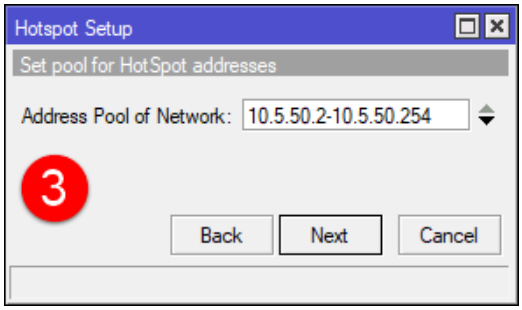
IP=> Hotspot=>Servers=> Hotspot Setup

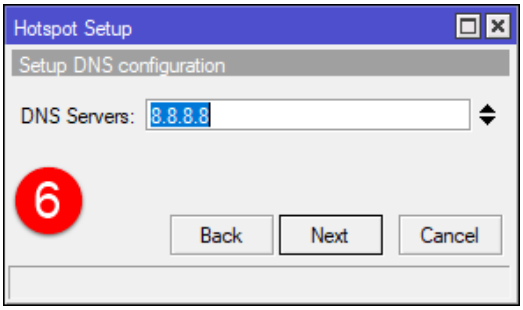


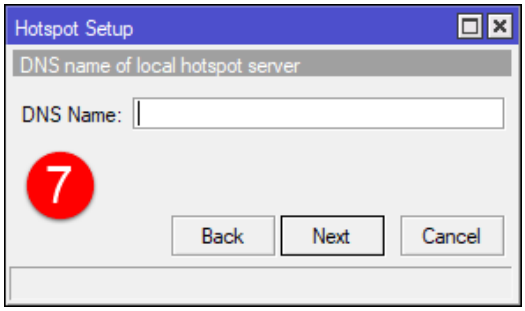


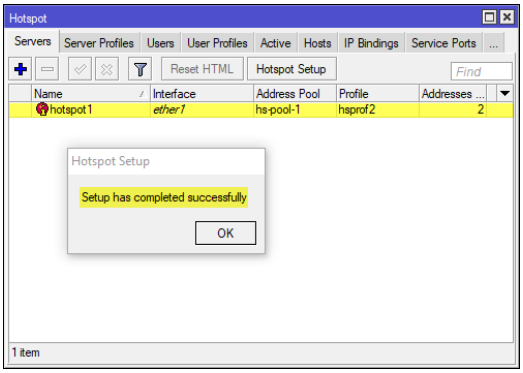












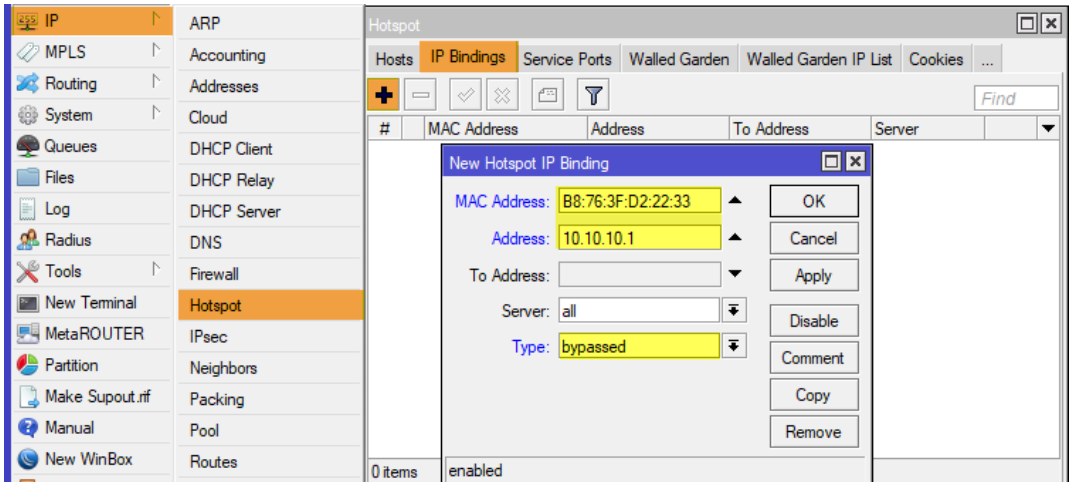
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

1. Choose Interface that provide hotspot to client
2. It will detect network from interface that you choose in first step. If don't have network default it will assign default password. Tick in Masquerade Network, it's mean hotspot will auto create NAT masquerade to allow client that connect hotspot can access to Internet.
3. Address Poll of Network, you can set range network that you wish to provide to hotspot client.
4. Select hotspot SSL certificate, it is related to encryption on hotspot login page. If you have certificate, it mean you can allow client access by https//:
5. Select SMTP server, IP address of the SMTP server, where to redirect HotSpot's network SMTP requests (25 TCP port)
6. DNS server addresses used for HotSpot clients, configuration taken from /ip dns menu of the HotSpot gateway
7. domain name of the HotSpot server, full quality domain name is required, for example www.example.com
8. username of one automatically created HotSpot user, added to */ip hotspot user (default: admin)*

IP BINDINGS

IP-Binding HotSpot menu allows to setup static One-to-One NAT translations, allows to bypass specific HotSpot clients without any authentication, and also allows to block specific hosts and subnets from HotSpot network. Use bypass Printers, IP phones, security Camera….

Configure in menu IP => Hotspot=> IP Binding.



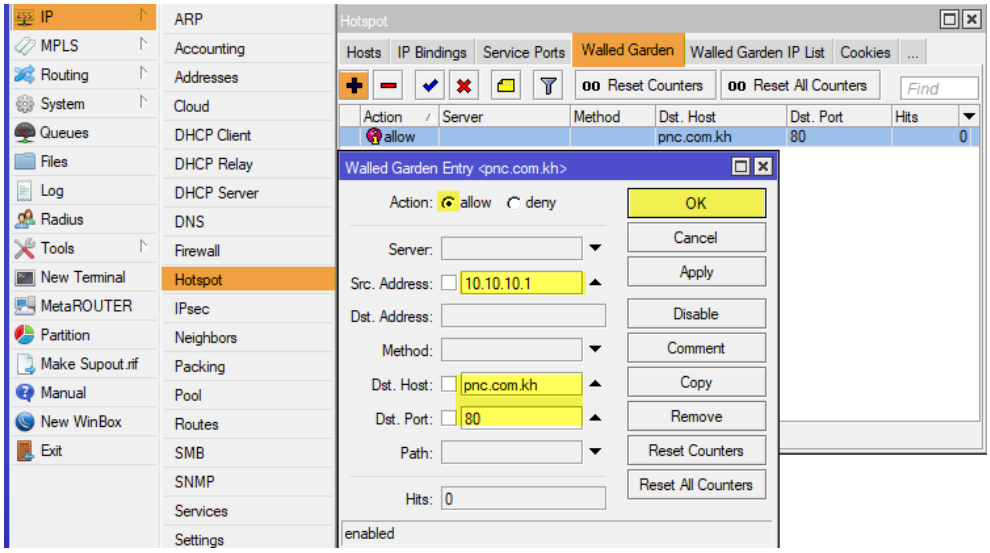
Type of the IP-binding action

- regular - performs One-to-One NAT according to the rule, translates address to to-address
- bypassed - performs the translation, but excludes client from login to the HotSpot
- blocked - translation is not performed and packets from host are dropped

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

WALLED GARDEN

- Allow all users to access specific websites.
- Company website, intranet, internet banking …etc.
- Configure manually by IP => Hotspot => Walled Garden => Src-address => Dst.Host =>Dst.Port=> apply ok



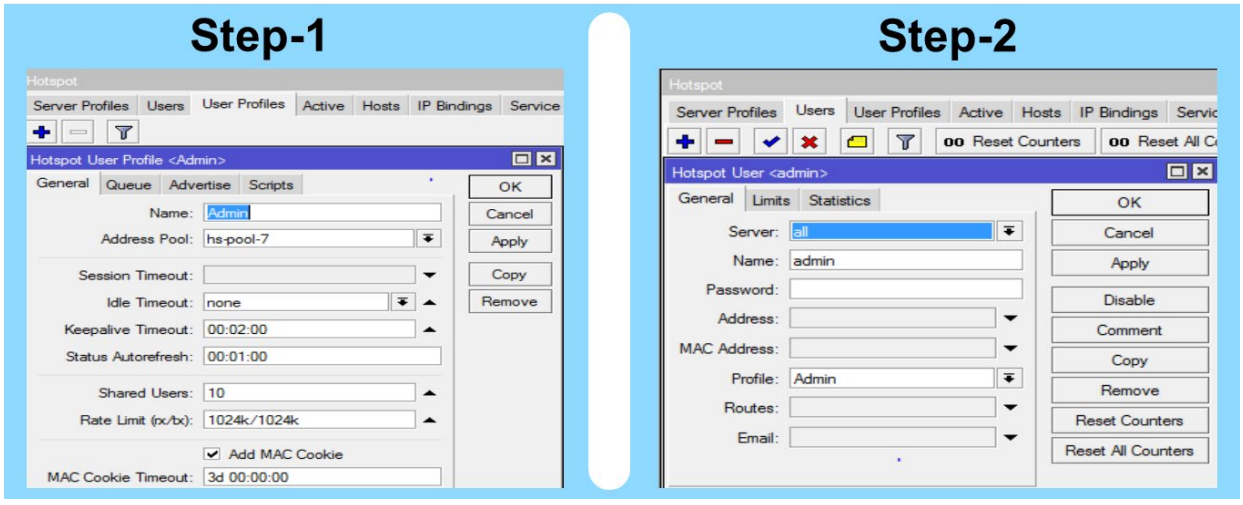
WALLED GARDEN IP LIST

Allow all user access specific protocol

- To bypass HOST/IP with several or ALL services can be accessible from hotspot client without authentication (router, mail server, etc.)
- Configure in menu IP => Hotspot => Walled Garden IP list

LIMIT SPEED USERS HOTSPOT

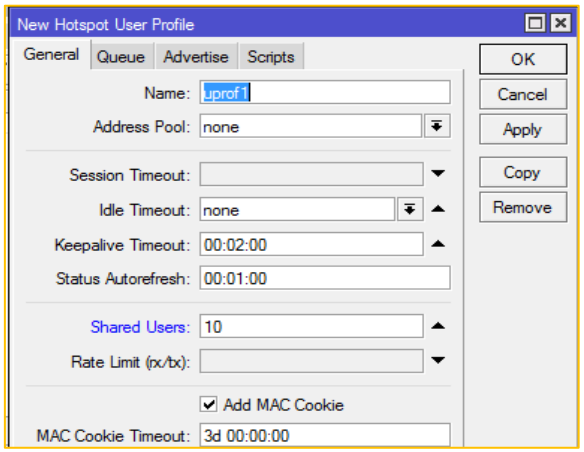
- Limit user bandwidth, using Mikrotik hotspot local user profile.
- Can be set from Hotspot => User Profile
- Configure : General => Rate Limit (rx/tx)



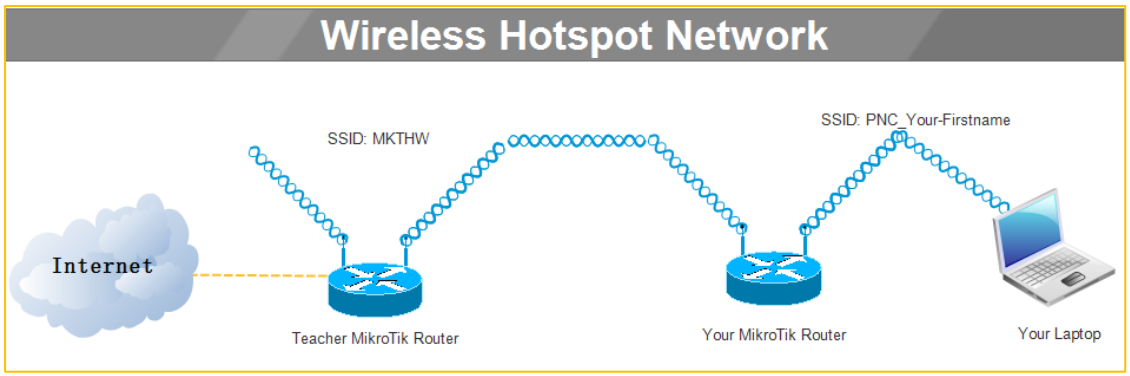
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SHARE USERS HOTSPOT

- One user name can be used more than once, for limit number.
- Set the limit number of user from hotspot☐ User Profile.
- Configuration :
- IP hotspot => Users Profiles => General => Shared User (Set the maximum limit)



6.1-LAB-Hotspot Configuration



I. Connect to MKTHW

a. Login to your MikroTik router and change Password Administrator

b. Bridge interface ether2-3 " Name: Bridge_XX" (XX= your id)

c. Assign IP address to Birdge Interface

d. Connect your router to MKTHW by wireless (password: mikrotik)

e. Enable DHCP client on interface WAN + create default route automatically

i. Test ping to 8.8.8.8

ii. Trace route to Passerellesnumeriques.org and write down the path that access from your compute to passerellesnumeriques.org.

iii. Test speed from your router to MKTHW

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

II. Create Virtual AP

a. Create new security profile allow only AES encryption with strong phrase

b. Create virtual AP by use SSID: PNC_Your-firstname and use your new security profile.

c. Assign IP address to new virtual interface 191.168.xx.1/24 (XX is your ID)

d. Test connect from client to your wireless router and assign IP address static to your computer and ping gateway for testing.

III. Create DHCP Server

a. Create DHCP server name " DHCP-LANClient and provide to interface that connect to client site.

b. Use DNS PNC, and DNS google

c. Pool name " Pool-LANClient" provide range from .100 to 254

d. Test on client to get IP address from DHCP server

e. Set your computer client to get IP address .200 every time it request

f. Test ping to google.com or 8.8.8.8. Does you reach the google website? If yes / no, why it reach or not reach?

g. Repeat the same step to create other DHCP server for Bridge Interface

    i. You can assign any name, address,…. By yourself

IV. Allow LAN Client access Internet

a. Create NAT rule to allow LAN client both by Wireless + Bridge Interface

b. Test access to internet on computer client by wireless connection

c. Test access to internet on computer client by bridge Interface

V. Setup and configure HotSpot

a. Create user use yourname with default profile.

b. Test access to Internet. You can't access to Internet right.

c. Login using your name and password. Test access to Internet.

d. Create user Profiles:

1. Name: LANC20
2. Chose Pool-LANClient
3. Set session Timeout 20 minutes (time for user can access Internet or network) You can test 5 minutes is fast to know result.
4. Allow 10 users can use the same username at the same time
5. Set 1MB upload and 1MB download (For other option keep default.)
6. Create 2 users:

    1. PNC20 and add to Profile LANC20

    2. PNCN and add to Default Profile

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

3. Testing

2. Add client to IP Bidings

    1. Filter Mac Address your computer to bypass without authentication
    2. Borrow your friend computer to connect and block his/her mac not allow to access to internet

3. Allow websites bellow for client can access without authentication in Walled Garden IP List :

    1. www.passerellesnumeriques.org
    2. www.timetables.pnc.passerellesnumeriques.org
    3. www.sms.pnc.passerellesnumeriques.org

Note: Make sure you remove or disable IP binding test in part 7. Because it will allow you to access Internet without authentication.

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

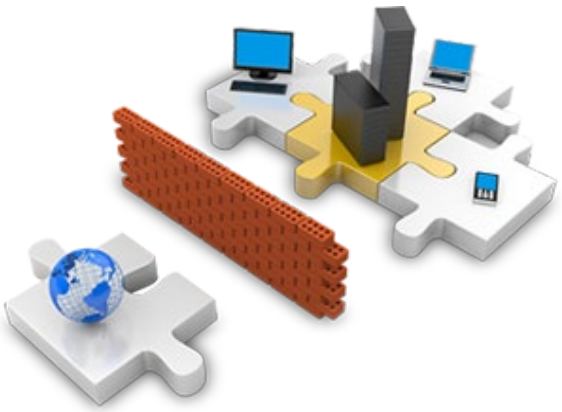
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 7: FIREWALL

OBJECTIVE

After finish, this lesson student will be able to:

- Firewall Principles
  - Connection tracking and states
  - Structure, chains and action
- Firewall Filter in action
  - Filter actions
  - Protecting your router (input)
  - Protection your customers (forward)
- Basic Address-List
- Source NAT
  - Masquerade and src-nat action
- Destination NAT
  - Dst-nat and redirect action
- FastTrack



FIREWALL OVERVIEW

- To protect the router from unauthorized access,
- both originating from the WAN (Internet) or from the LAN (local).
- To protect the network that through the router.
- In RouterOS, firewall has many features that are all included in the IP Firewall menu.
- There are two type of Firewall
  - Hardware Base Firewall
  - Software Base Firewall
- Firewall filtering rules are configured at IP>Firewall>Filter Rule.

HARDWARE FIREWALL

There are two common types of firewall, hardware base firewall and software base firewall.

Hardware base firewall is the device that design to be firewall, it is mean work as firewall,

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Some example common hardware firewalls:


Poloalto


Cisco FirePower


WatchGuard


Juniper


Check Point


ForcePoint


Fortinet FortiGate


Sonicwall

Some example common software firewalls:

IPTABLES untangle pfSense VyOS

IPFire FirewallD OPNsense

FIREWALL RULE

- Each firewall filter rules are organized in a chain and read sequentially.
- Each chain will be read by the router from top to bottom.
- There are 3 default chains (input, forward, output) in Firewall Filter rule.
- In addition to the 3 default chain, we can make chain by yourself as needed

PACKET FLOW

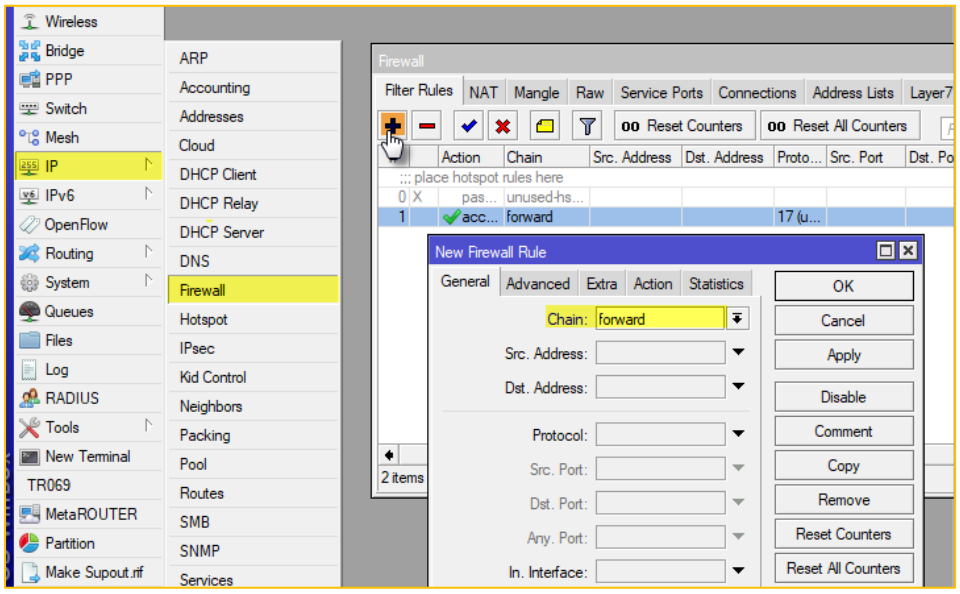
Rules can be placed in three default chains

- input (to router)
- output (from router)
- forward (through the router)

Note: You can create more chain beside default chains.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

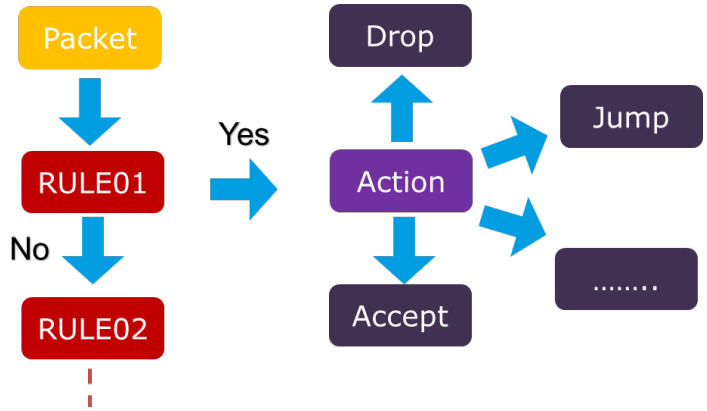
IP => Firewall => Filter Rules



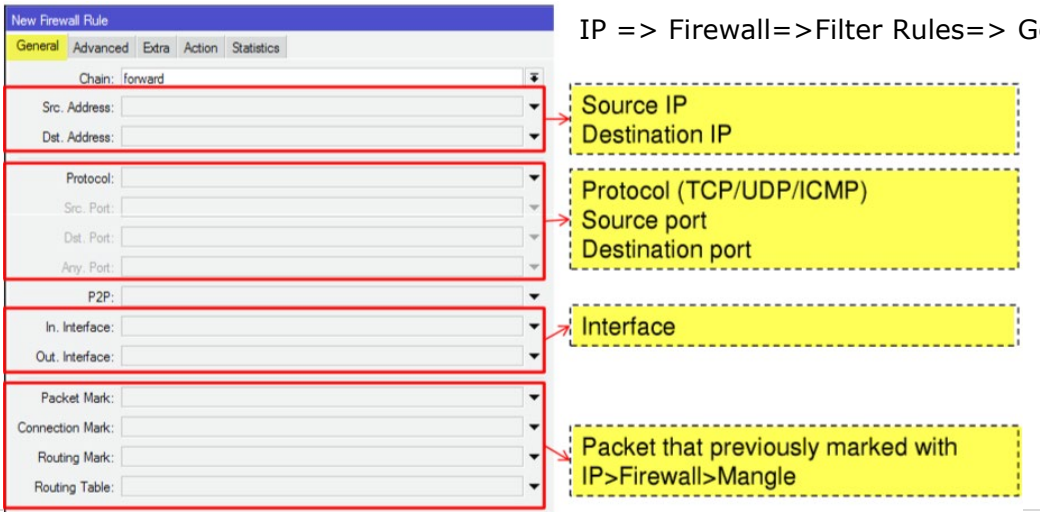
FIEWALL STATEMENT CONCEPT

Rule IF ..... Then .....

IF packet **match** with **Rule** (criteria) **Then** what Firewall will **do** with the packet.



FIEWALL –IF (CONDITION)

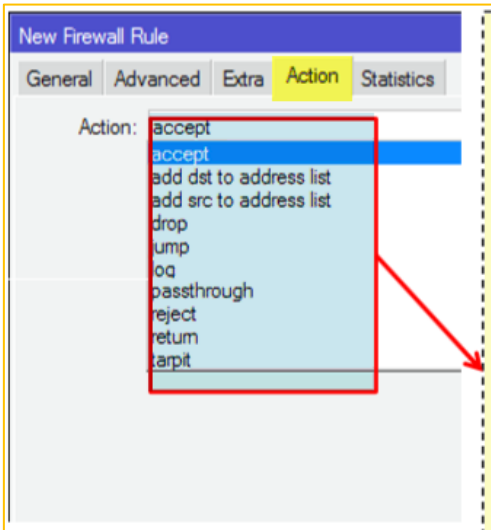


IP => Firewall=>Filter Rules=> General

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

FIEWALL –THEN (ACTION)

IP => Firewall=>Filter Rules =>Action



accept - accept the packet. Packet is not passed to next firewall rule.
add-dst-to-address-list - add destination address to address list specified by address-list parameter
add-src-to-address-list - add source address to address list specified by address-list parameter
drop - silently drop the packet
jump - jump to the user defined chain specified by the value of jump-target parameter
log - add a message to the system log containing following data: in-interface, out-interface, src-mac, protocol, src-ip:port->dst-ip:port and length of the packet. After packet is matched it is passed to next rule in the list, similar as passthrough
passthrough - ignore this rule and go to next one (useful for statistics).
reject - drop the packet and send an ICMP reject message
return - passes control back to the chain from where the jump took place
tarpit - captures and holds TCP connections (replies with SYN/ACK to the inbound TCP SYN packet)

FIEWALL STRATEGY

- A lot of traffic to be filtered, which one allowed (accept) and which one will be rejected (drop)
- There are 2 methods to simplify firewall rule:
  - Drop some, allow others (drop few, accept any)
  - Accept some, discarded others (accept few, drop any)
- By default if there is no any rules in the firewall, all traffic will be accept by the router.

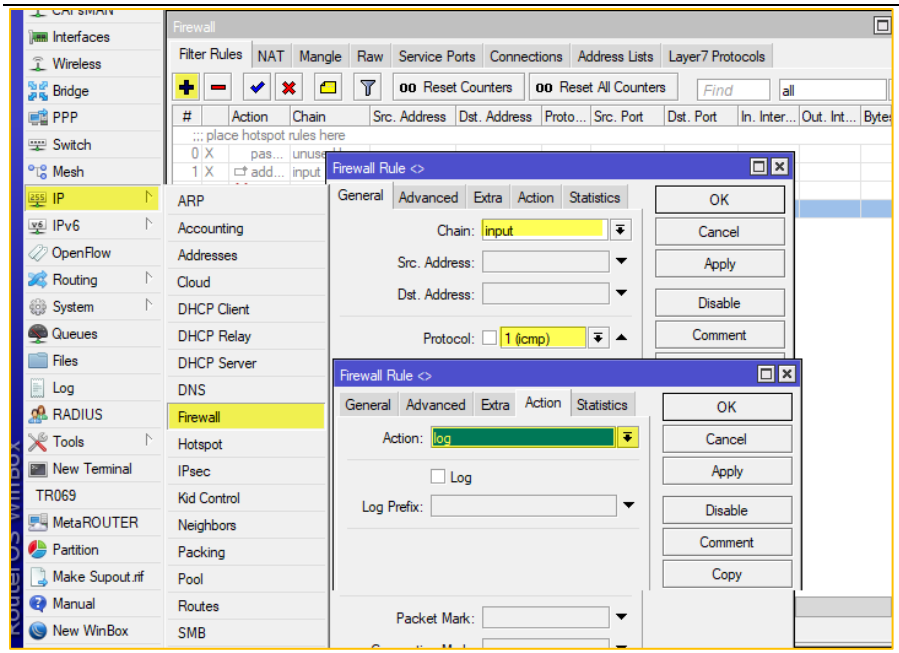
FIREWALL LOG

Firewall Log is a firewall feature to record (displaying in the log) network activities. Each firewall rule can be logged when matched.

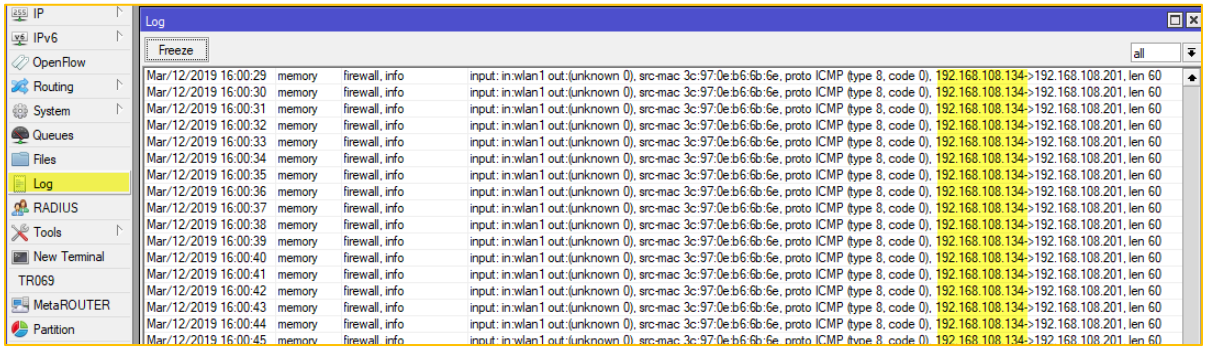
Create a filter rule on the menu IP=> Firewall=>Filter Rules=> Action=>log

Log when have ping packet.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

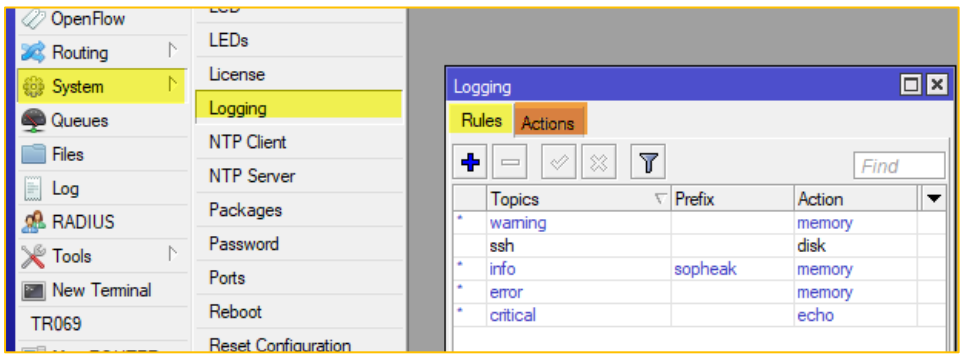


Check log in IP =>log



LOGGING

- We can choose what features will be displayed in the log.
- We can also send logs to a syslog server, by default using protocol UDP port 514
- Logging settings in the menu System=>logging
- There are two taps of Logging:
    - Rules: Create for filter log (condition)
    - Action: Action when the rule match (send to syslog or store in local)



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

There are 3 main point in Rules:

- **action** (*name*; default: **memory**) - specifies one of the system default actions or user specified action listed in **/system logging action**
- **prefix** (*text*) - local log prefix
- **topics** (info | critical | firewall | keepalive | packet | read | timer | write | ddns | hotspot | l2tp | ppp | route | update | account | debug | ike | manager | pppoe | script | warning | async | dhcp | notification | pptp | state | watchdog | bgp | error | ipsec | radius | system | web-proxy | calc | event | isdn | ospf | raw | telephony | wireless | e-mail | gsm | mme | ntp | open | ovpn | pim | radvd | rip | sertcp | ups; default: **info**) - specifies log group or log message type

There are 5 action types:

- disk - logs are saved to the hard drive
- echo - logs are displayed on the console screen
- email - logs are sent by email
- memory - logs are saved to the local memory buffer
- remote - logs are sent to a remote host

Note: You cannot delete or rename default actions.

7.1-LAB-Chain Input

- *Create first firewall rule that allow only your laptop (192.168.XX.200) that can access to your router. Suggest put comment on the rule.*
  - *Test access to your router. Does your PC still access to the router?*
- *Create second rule to deny (drop) all coming traffic to your router. Suggest put comment on the rule.*
  - *There are two rules accept your computer IP address and drop other traffic*
  - *Change your computer IP and test access to your router. Does your PC still access to the router?*
  - *What happened to the Bytes or Packet increasing on each rule?*
- *Create the rule to record who ping to your router.*
  - *Check log to verify that log existing are correct.*
- *Create logging with SSH and target to disk.*

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

ADDRESS LIST

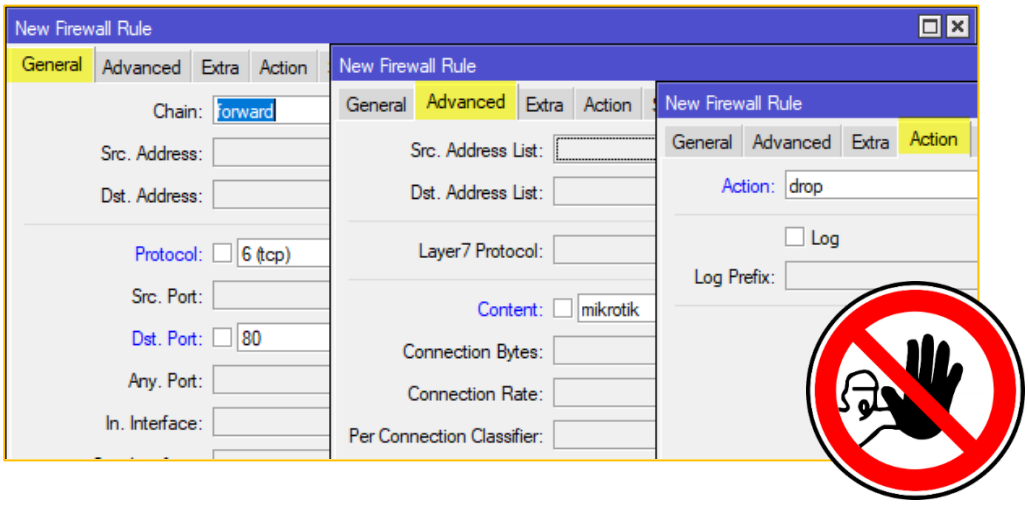
- Address-list is part of the Firewall
- Address-list is used to make group of IP address so will make us easy if we want to filter group of IP address with one rule of Firewall Filter Rule.
- Address-list also can automatically add by firewall filter rule that has action "add src/dst to address-list" permanently or for a while
- One address-list can be single IP, subnet, range or range of IP address.
- One IP address can belong to more than one address list and can be use in different filter rule.

7.2-LAB-Address List

- *Create firewall when the clients ping to your router, client cannot access the Internet for 20 seconds, if client stop pinging router, and client can access the Internet.*
- *Test ping from your computer to gateway and check on router firewall address-list.*

BLOCK CONTENT

- RouterOS has firewall feature to block content
- Firewall will filter on URL that contain the content that filter.
- We can filter all websites that contain the word that want to block. Example: porn, game…



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

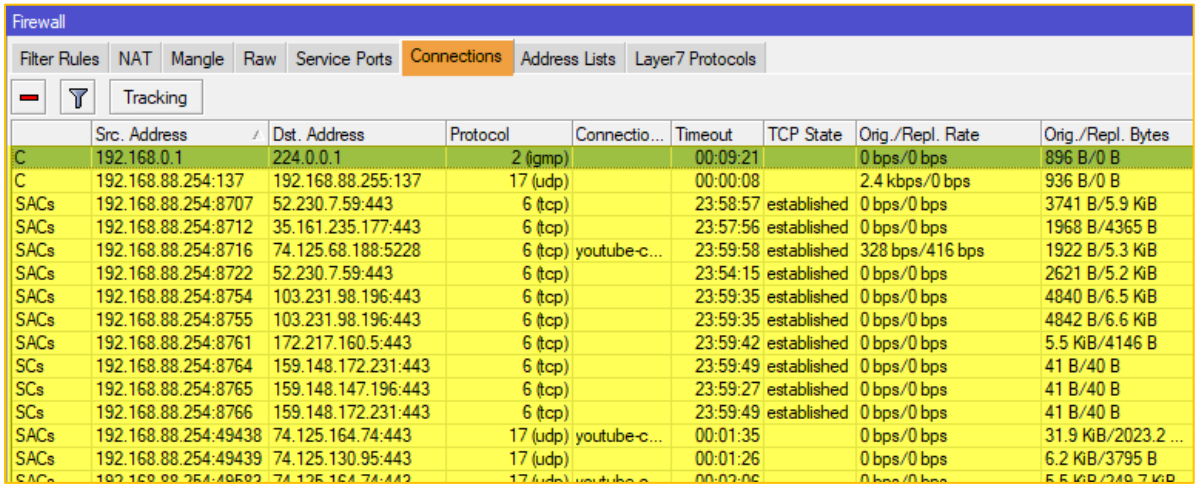
7.3-LAB-Block Content

- *Block client who will access web which contain the word "porn", in the lab we replace word "porn" with word "MikroTik".*

CONNECTION TRACKING

Connection Tracking allow you see what connections are making their way through the router.

Menu " IP => Firewall=> Connection "



	Src. Address	Dst. Address	Protocol	Connectio...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	192.168.0.1	224.0.0.1	2 (igmp)		00:09:21		0 bps/0 bps	896 B/0 B
C	192.168.88.254:137	192.168.88.255:137	17 (udp)		00:00:08		2.4 kbps/0 bps	936 B/0 B
SACs	192.168.88.254:8707	52.230.7.59:443	6 (tcp)		23:58:57	established	0 bps/0 bps	3741 B/5.9 KiB
SACs	192.168.88.254:8712	35.161.235.177:443	6 (tcp)		23:57:56	established	0 bps/0 bps	1968 B/4365 B
SACs	192.168.88.254:8716	74.125.68.188:5228	6 (tcp)	youtube-c...	23:59:58	established	328 bps/416 bps	1922 B/5.3 KiB
SACs	192.168.88.254:8722	52.230.7.59:443	6 (tcp)		23:54:15	established	0 bps/0 bps	2621 B/5.2 KiB
SACs	192.168.88.254:8754	103.231.98.196:443	6 (tcp)		23:59:35	established	0 bps/0 bps	4840 B/6.5 KiB
SACs	192.168.88.254:8755	103.231.98.196:443	6 (tcp)		23:59:35	established	0 bps/0 bps	4842 B/6.6 KiB
SACs	192.168.88.254:8761	172.217.160.5:443	6 (tcp)		23:59:42	established	0 bps/0 bps	5.5 KiB/4146 B
SCs	192.168.88.254:8764	159.148.172.231:443	6 (tcp)		23:59:49	established	0 bps/0 bps	41 B/40 B
SCs	192.168.88.254:8765	159.148.147.196:443	6 (tcp)		23:59:27	established	0 bps/0 bps	41 B/40 B
SCs	192.168.88.254:8766	159.148.172.231:443	6 (tcp)		23:59:49	established	0 bps/0 bps	41 B/40 B
SACs	192.168.88.254:49438	74.125.164.74:443	17 (udp)	youtube-c...	00:01:35		0 bps/0 bps	31.9 KiB/2023.2 ...
SACs	192.168.88.254:49439	74.125.130.95:443	17 (udp)		00:01:26		0 bps/0 bps	6.2 KiB/3795 B

There are some flag to identify the connection:

C = **Confirmed** : Connection is confirmed and a packet is sent out from the device.

S = **Seen-reply** : Destination address has replied to the source address.

A = **Assured**: Indicates that this connection is assured and that it will not be erased if maximum possible tracked connection count is reached.

s = **Srcnat**: Connection is going through SRC-NAT, including packets that were masqueraded through NAT.

Example: SACs= Packet is use masqueraded through NAT, send out from device already reply from destination and it is assured.

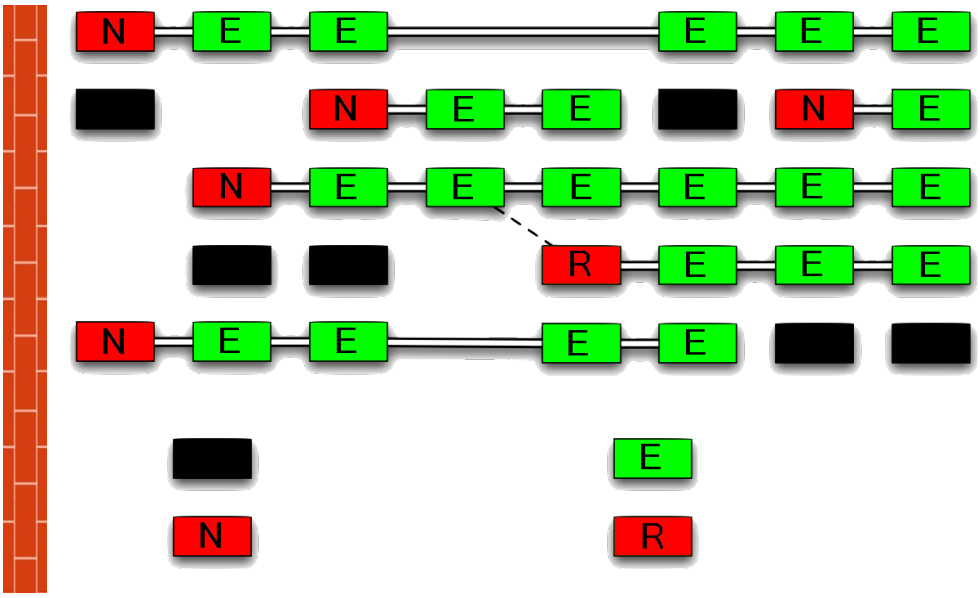
Connection tracking has the ability to see information of connection such as source and destination IP protocol and port and connection state.

Note: if connection tracking is disable, firewall and NAT will not working.

There are 4 kind of connection state:

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

- Established = the packet is part of already known connection.
- New = the packet starts a new connection or belongs to a connection that has not seen packets in both directions yet.
- Related = the packet starts a new connections, but is associated with an existing connection, such as FTP data transfer or ICMP error message.
- Invalid = the packet does not belong to any known connection and, at the same time, does not open a valid new connection



Firewall should proceed only new packets, it is recommended to exclude other types of states

- Connection state new => pass through
- Connection state established => Accept
- Connection state related => Accept
- Connection state invalid => Drop

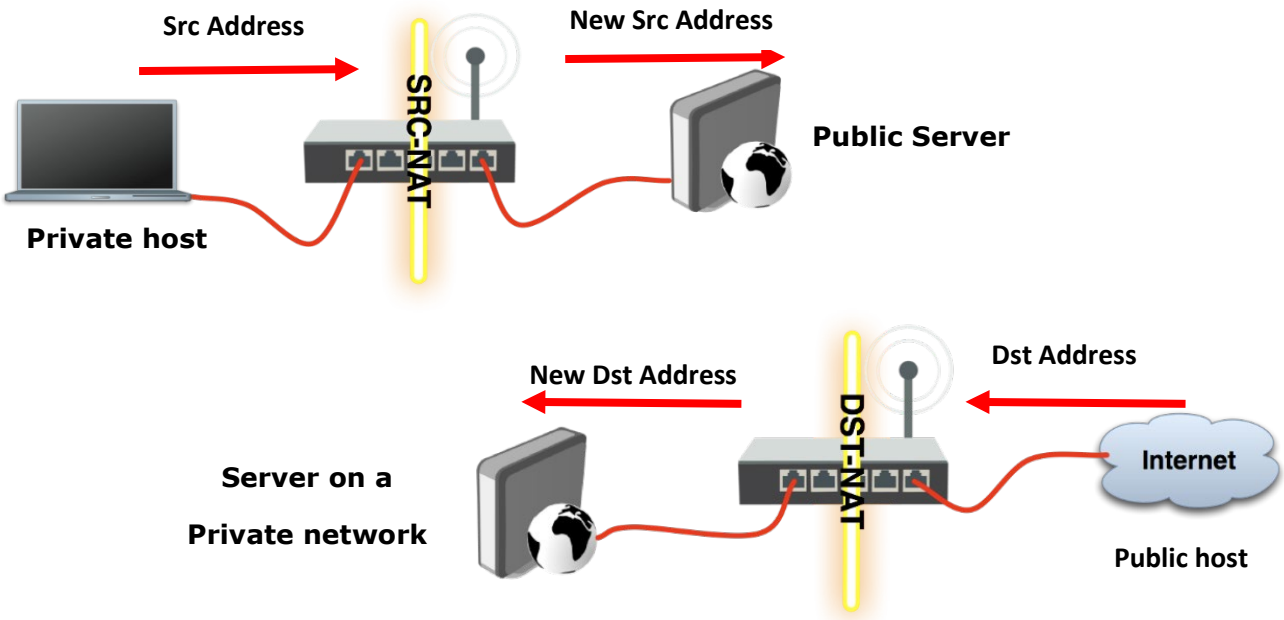
Let Firewall to work with new packets only

NAT

- NAT is a kind of firewall
- NAT configuration in menu IP=>Firewall=>NAT
- RouterOS is able to change Source or Destination address of packets flowing through it.
- Network Address Translation (NAT) is a method of modifying source or destination IP address of a packet
- There are two NAT types - 'source NAT' and 'destination NAT'
- NAT is usually used to provide access to an external network from a one which uses private IPs (src-nat). Src-nat is usually used for masquerade network

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

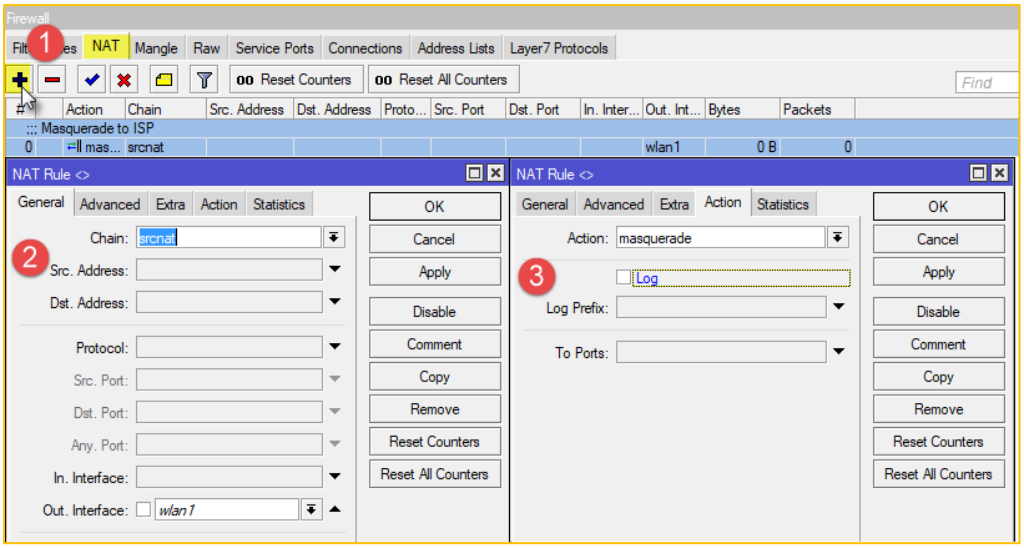
- Or to allow access from an external network to a resource (e.g. web server) on an internal network (dst-nat). Dst-nat is usually used for port forwarding.



NAT-MASQUERADE

- NAT-Masquerade is a method used to connecting multiple computers to the internet by using one or more public IP addresses.
- NAT-Masquerade is used because of the availability of public IP addresses.
- NAT-Masquerade is also used for security reasons, because network that had been NAT not accessible from outside network.

You can configure NAT by: IP => Firewall => NAT



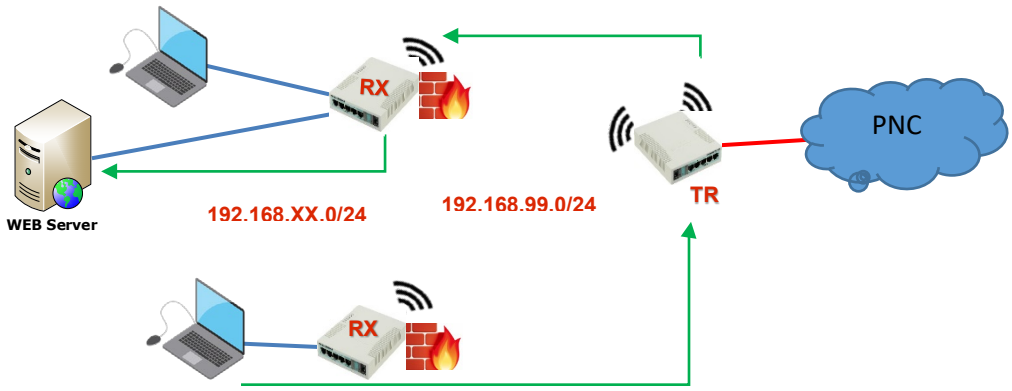
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

NAT-PORT FORWARDING

- Dst-nat changes packet's destination address and port
- It can be used to direct internet users to a server in your private network
- It can be used to direct local user to the router it self
- It also can be used to direct local user to any server

7.4-LAB-Block Content

- *Enable other from outside LAN that access port 81 in public IP address of Router will automatically redirect to WEB server in LAN zone. Ex. http://192.168.99.XX:81 .*



7.5-LAB-Transparent DNS Filtering

- *Redirect DNS request to one of the free filtered DNS server, (example Norton Open DNS: http://dns.norton.com/dnsweb)*

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

FASTTRACK

- A method to accelerate packet flow through the router
- An established or related connection can be marked for fasttrack connection
- Bypasses firewall, connection tracking, simple queue and other features
- Currently supports only TCP and UDP protocols

Without	With
360Mbps	890Mbps
Total CPU usage 100%	Total CPU usage 86%
44% CPU usage on firewall	6% CPU usage on firewall

Tested RB2011 with a single TCP stream. For more information, check FastTrack wiki page

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

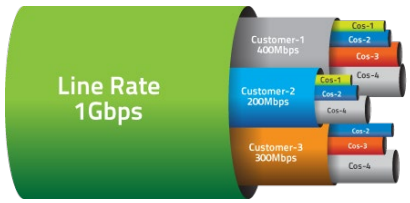
CONCEPTs REVIEW

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 8: BANDWIDTH MANAGEMENT

OBJECTIVE

After finish, this lesson student will be able to:



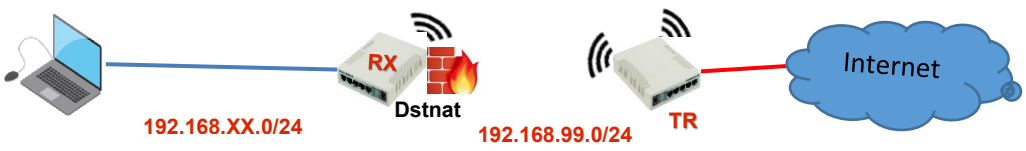
- Simple Queue
  - Target
  - Destinations
  - Max-limit and limit-at
  - Bursting
- One Simple queue for the whole network (PCQ)
  - pcq-rate configuration
  - pcq-limit configuration

SIMPLE QUEUE

- RouterOS implements several QoS methods such as traffic speed limiting (wireless access list, PPP secret and hotspot user), traffic prioritization and other.
- Simple queue is the easiest way to limit bandwidth:
  - Client's download (↓) speed
  - Client's upload (↑)speed
  - Client's total speed (↓ + ↑)
- You must use target-address for simple Queue, target-address is the user's IP address
- Rule order is important for queue rules
- Disable firewall FastTrack rule for simple Queue to work

8.1-LAB-Simple Queue

- *Create simple queue to limit bandwidth of your laptop 64Kb/s and 128Kb/s Download.*
- *Test by use bandwidth test website www.speedtest.net to observe the bandwidth or download file via FTP to access Point.*
- *Check bandwidth status on simple Queue and using tool "Tourch" to observe bandwidth*



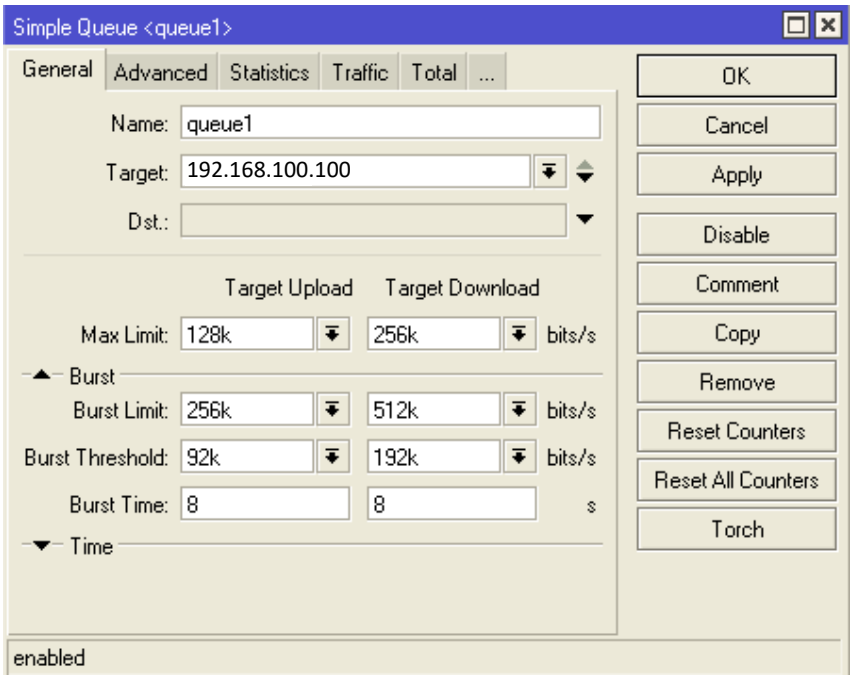
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Note: Queue colors in Winbox:

- 0%-50% available traffic used –**Green**
- 51-75% available traffic used – **Yellow**
- 76%-100% available traffic used – **Red**

BURST

- Used to allow higher data rates for a short period of time
- Useful for HTTP traffic - web pages load faster
- If average data rate is less than burst-threshold, burst is allowed be used (until reach burst-limit)
- Average data rate is calculated from the last burst-time seconds
- Burst:
  - Burst limit - max upload/download data rate that can be reached during the burst
  - Burst time - time (sec), over which the average data rate is calculated (this is NOT the time of actual burst).
  - Burst threshold - when average data rate exceeds or drops below the threshold the burst is switched off or on

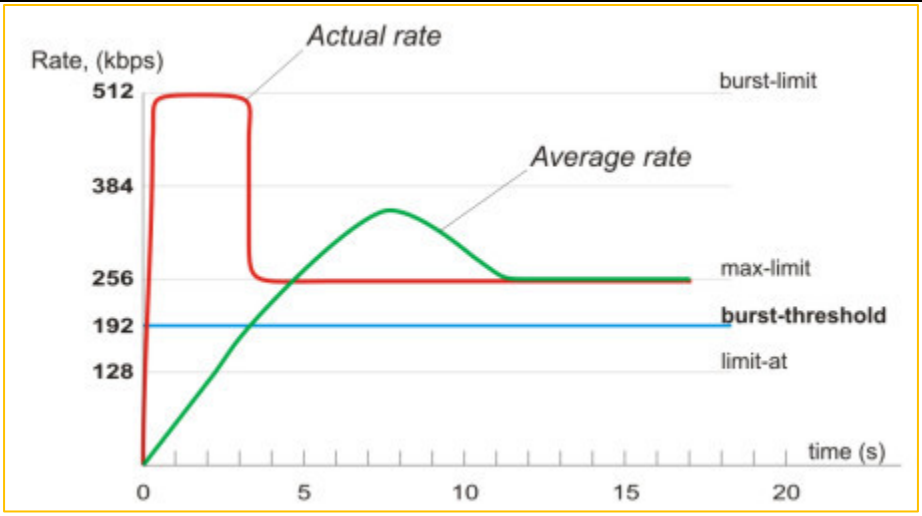


Let's consider the following scenario:

- max-limit=256k
- burst-time=8
- burst-threshold=192k
- burst-limit=512k

The below graph shows the user download activity over time and how RouterOS handles it.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org



Average bandwidth in 1st second: (512+0+0+0+0+0+0+0)/8=64Kb

Average bandwidth in 2nd second: (512+512+0+0+0+0+0+0)/8=128Kb

Average bandwidth in 3rd second: (512+512+512+0+0+0+0+0)/8=192Kb

Average bandwidth in 4th second: (512+512+512+512+0+0+0+0)/8=256Kb

- In 1st second, average bandwidth is 64Kb still lower than threshold 192Kb, still continue to 2nd second (burst limit=512)
- In 2nd second, average bandwidth is 128Kb still lower than threshold 192Kb, still continue to 3rd second (burst limit=512)
- In 3rd second, average bandwidth is 192Kb same with threshold 192Kb, still continue to 4th second (burst limit=512)
- In 4th second, average bandwidth is 256Kb higher than threshold 192Kb, so in 5th second bandwidth not allow to reach burst limit (512Kb), and just can reach max limit (256Kb)

8.2-LAB-Burst Simple Queue

- *Create simple queue with the previously 8.1-lab parameters*
- *Configure burst value like the example.*
- *Test by access some websites or download some file from Internet and monitor in "Queue=>Queue Simple=>Traffic".*

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

MANGLE

- Mangle feature is in IP=>Firewall=>Mangle
- Mangle is used to mark packets
- Separate different types of traffic
- Marks will active within the router, and use to another feature process.
- Marks can't be transmitted to another router
- Used for queue to set different limitation
- Mangle do not change packet structure (except DSCP, TTL specifications)

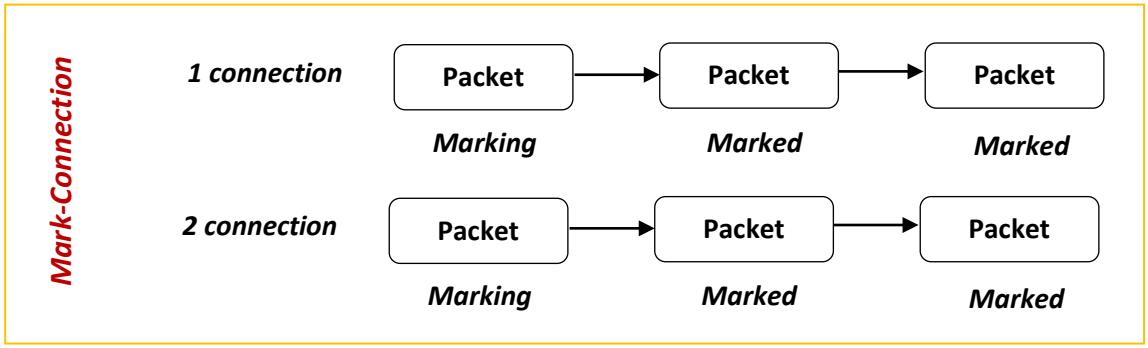
MANGLE ACTION

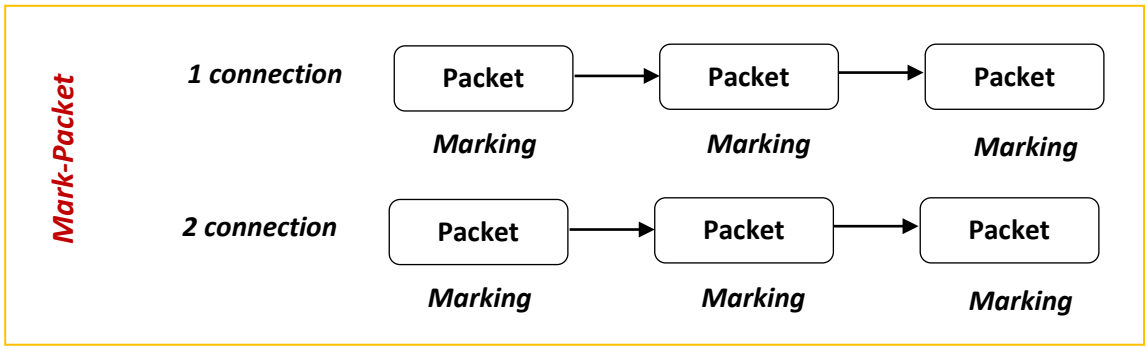
- Mark-connection: uses connection tracking

  Information about new connection added to connection tracking table
- Mark-packet: works with packet directly

  Router follows each packet in connection to apply mark-packet
- Mark-routing: marks traffic with routing-mark for PBR (Policy Based Routing)

At the same time, every packet may have only 1 connection-mark, 1 packet-mark and 1 routing-mark



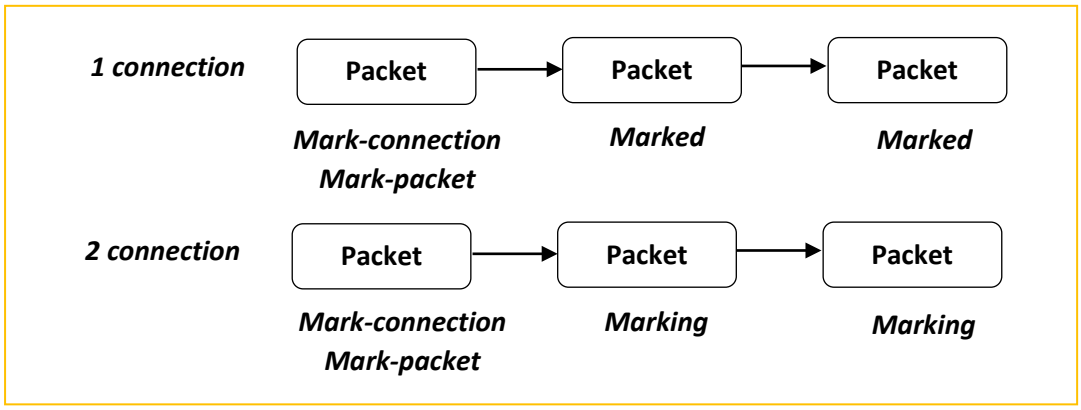


Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

OPTIMAL MANGLE

- Queues have packet-mark option only
- Mark new connection with mark-connection
- Add mark-packet for every mark-connection

Combine Mark-connection and Mark-Packet



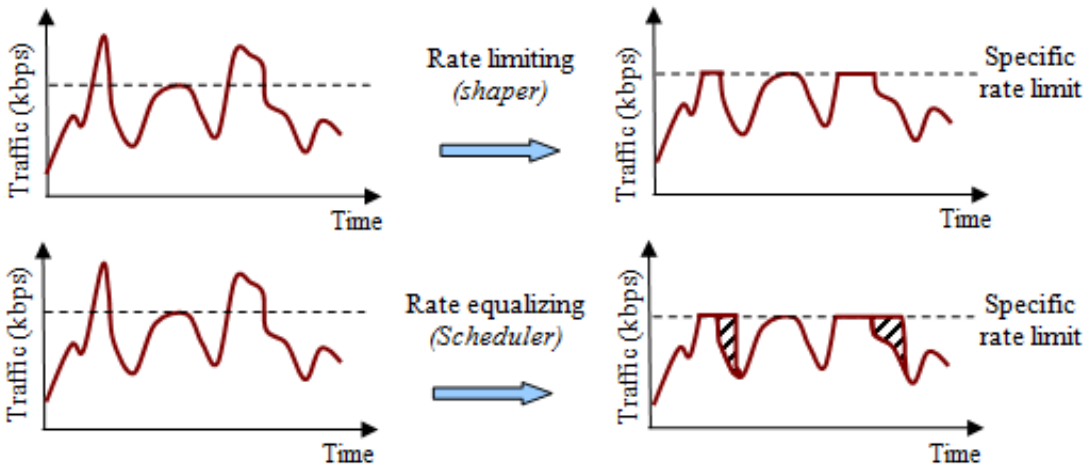
QUEUE KINDS

Scheduler queues: will drop traffic if over bandwidth link

- BFIFO (Bytes First-In First-Out)
- PFIFO (Packets First-In First-Out)
- RED (Random Early Detect)
- SFQ (Stochastic Fairness Queuing)

Shaper Queues: it will delay in queue

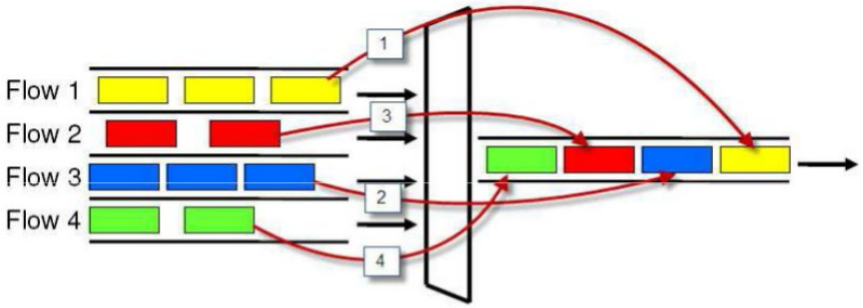
- PCQ (Per Connection Queue)



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

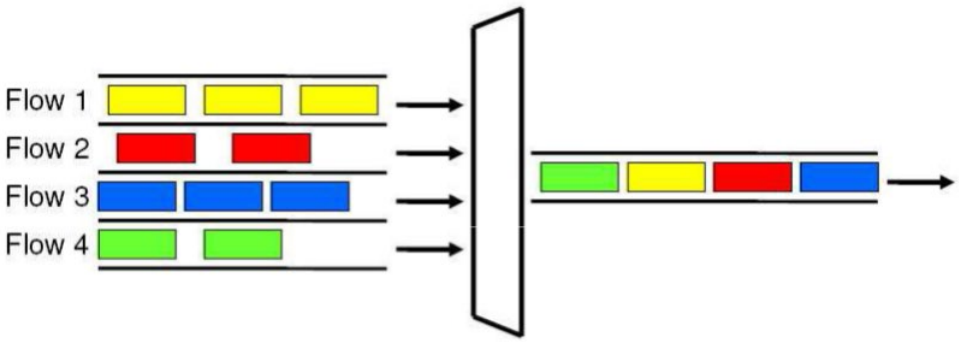
BFIFO/PFIFO

- What come first is handled first, what comes in next waits until the first is finished. Number of waiting unit (packets or bytes) is limited by "queue size" option. If queue is full next unit will be drop
- Large queue sizes can increase latency



RED

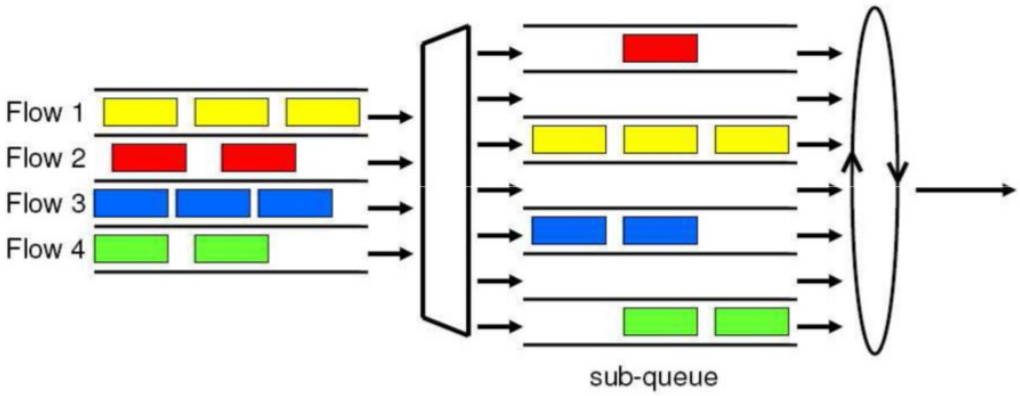
- Random Early Detect (Random Early Drop)
- Doesn't limit the speed indirectly equalizes users data rate when channel is full
- When the average queue size reach min-threshold, RED randomly chooses which arriving packet to drop
- If the average queue size reaches max-threshold, all packets are dropped
- Mainly, RED is used on congested links with high data rates. Work well with TCP protocol, but not so well with UDP



SFQ

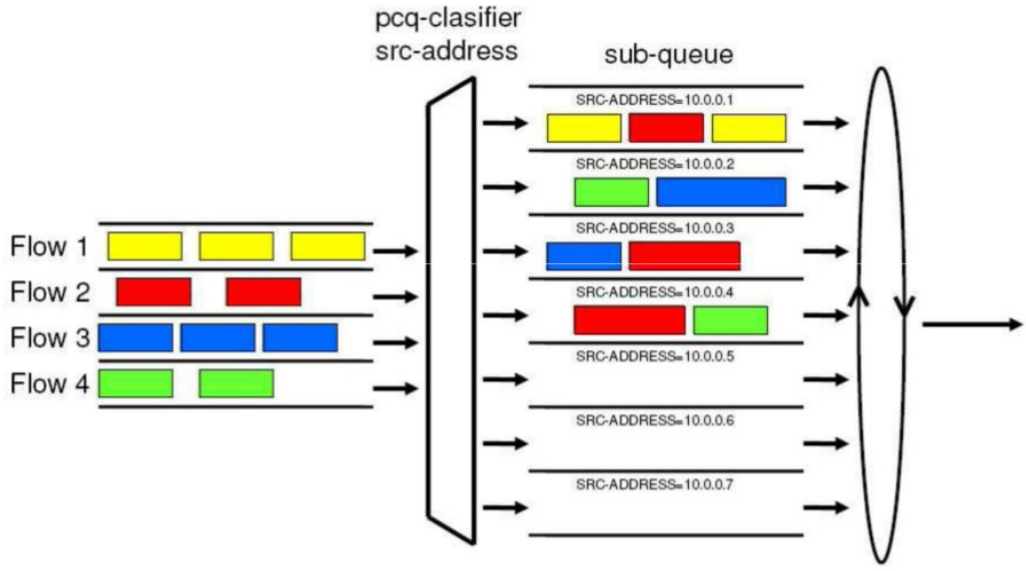
- Based on hash value from source and destination address SFQ divides traffic into 1024 sub-streams Then Round Robin algorithm will distribute equal amount of traffic to each sub-stream
- sfq-perturb(time): How often hash function must be refreshed
- sfq-allot(number): Amount of data in bytes that can be sent in one round-robin round

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

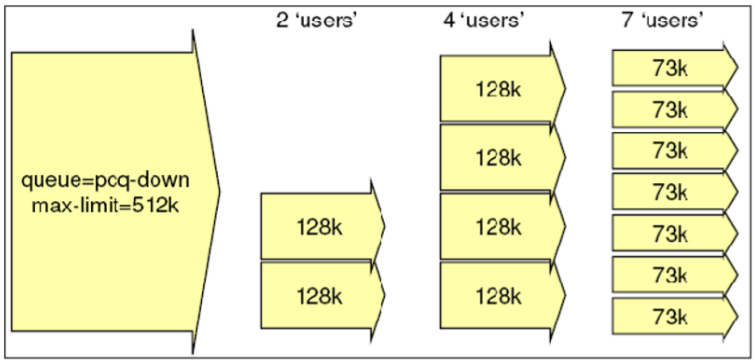


PCQ

- PCQ is advanced Queue type
- PCQ uses classifier to divide traffic (from client point of view; src-address is upload, dst-address is download)
- Replace hundreds of queues with just few
- Set the same limit to any user
- Equalize available bandwidth between users

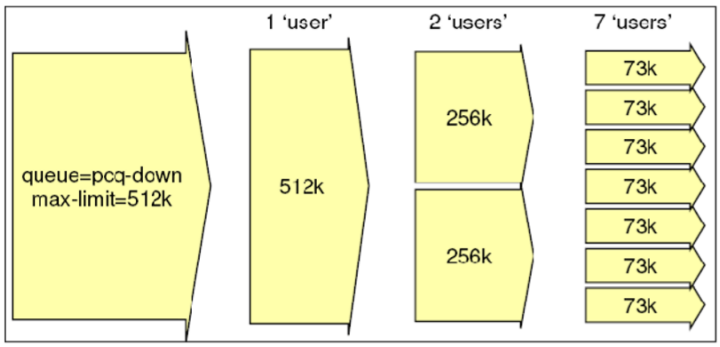


- PCQ Rate = 128k

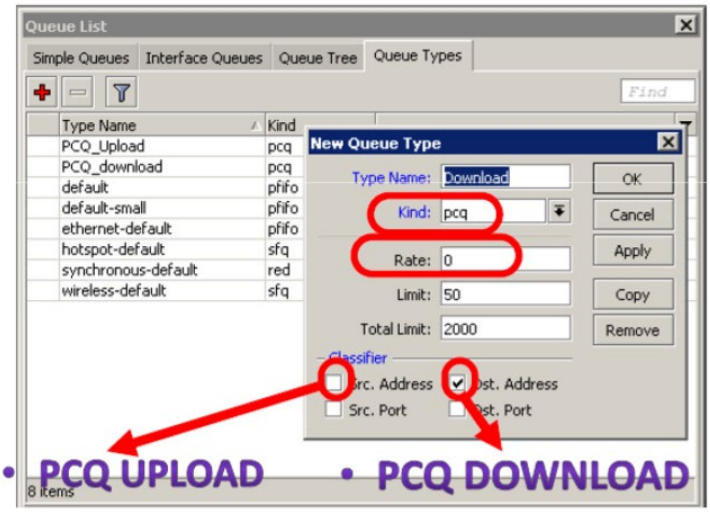


Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

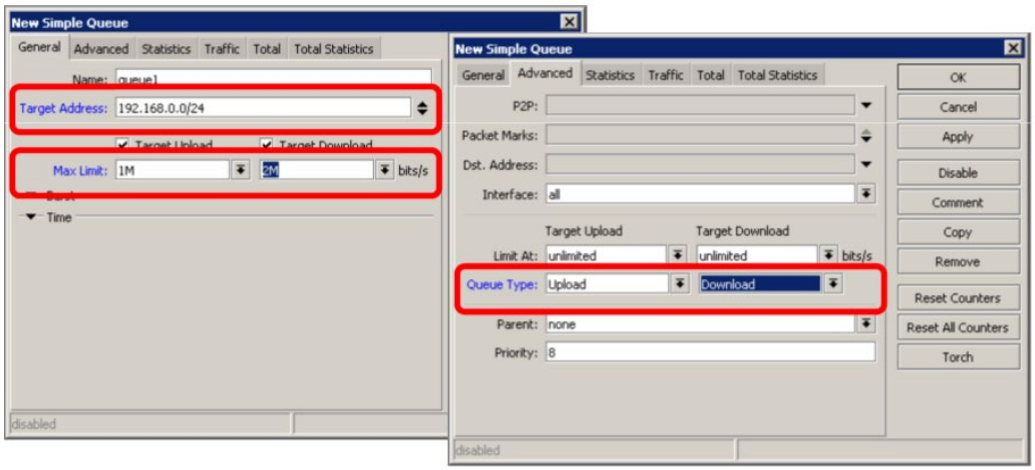
- PCQ Rate = 0



- PCQ allows to set one limit to all users with one queue



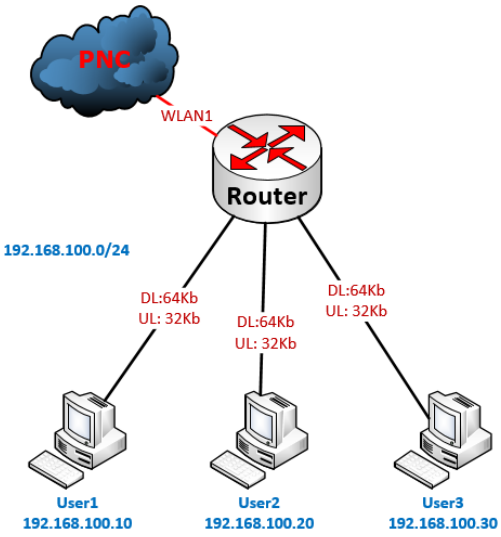
- One limit to all
- 1M upload/2M download is shared between users



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

8.3-LAB-PCQ

- *Make two PCQ queue types for:*
  - *One for Download: 64Kbps*
  - *Other one for Upload : 32Kbps*
- *Make one simple rule queue for all client in one network*
  - *Each user will get DL=64KB, UL=32KB*
- *Test download and upload*



SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

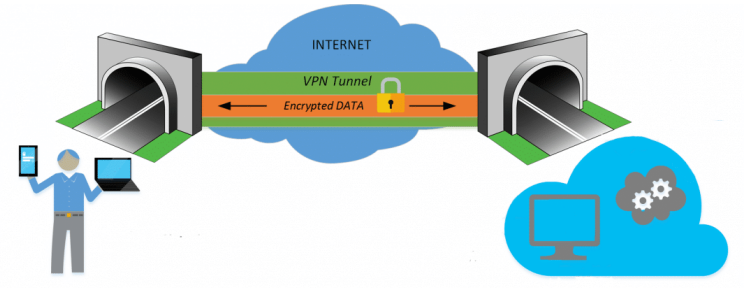
CONCEPTs REVIEW

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 9: TUNNELS

OBJECTIVE

After finish this lesson student will be able to:



- PPP settings
  - PPP profile
  - PPP secret
  - PPP status
- IP pool
  - Creating pool
  - Managing ranges
  - Assigning to a service
- Secure local network
  - PPPoE service-name
  - PPPoE client
  - PPPoE server
- Point-to-point addresses
- Secure remote networks communication
  - PPTP client and PPTP server (Quick Set)
  - SSTP client

TUNNEL OVERVIEW

- Tunnel is a method of encapsulation of data packets in the network.
- Before being transmitted, a data packet having a bit of modification, the addition of the tunnel header
- When data is passed to tunnel and arrived at the destination (end) tunnel, header data packet will be remove.

In MikroTik, there are many tunnel types:

- PPTP, L2TP, PPPOE, EoIP, SSTP, OpenVPN…etc.
- We can see them when we add virtual interface

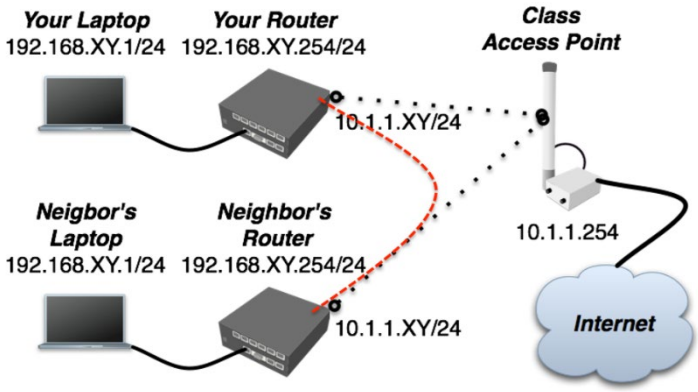
IPIP TUNNEL

- IP protocol 4/IPIP allows to create tunnel by encapsulation IP packets in IP packets and sending over to another router
- IPIP is layer 3 tunnel – It can not be bridged
- RouterOS implements IPIP tunnels according to RFC 2003 – it should be compatible with other vendor IPIP implementations
- To create a tunnel you must specify address of the local and remote router on both sides of the tunnel.

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

9.1-LAB-IPIP Tunnel

- *Create IPIP tunnel that connect between your routers to your neighbor's router.*

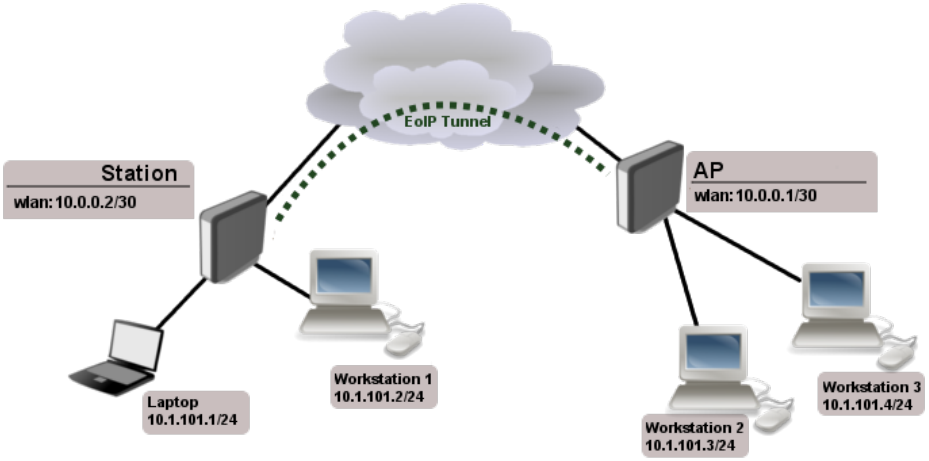


EOIP TUNNEL

- The simplest Tunnel at MikroTikis EoIP (Ethernet over IP)
- EoIP is proprietary MikroTik protocol.
- EoIP possible to bridge 2 network together over internet
- EoIP encapsulation using Generic Routing Encapsulation (GRE, IP Protocol No. 47).
- EoIP not use encryption, so it is not advisable to use for data transmission that requires a high level of security
- EoIP use "Tunnel ID" to identification the peering

9.2-LAB-EoIP Tunnel

- *Create EoIP tunnel between two offices by allow both clients can communicate between internal networks.*
- *For IP public on both routers, check with real situation.*

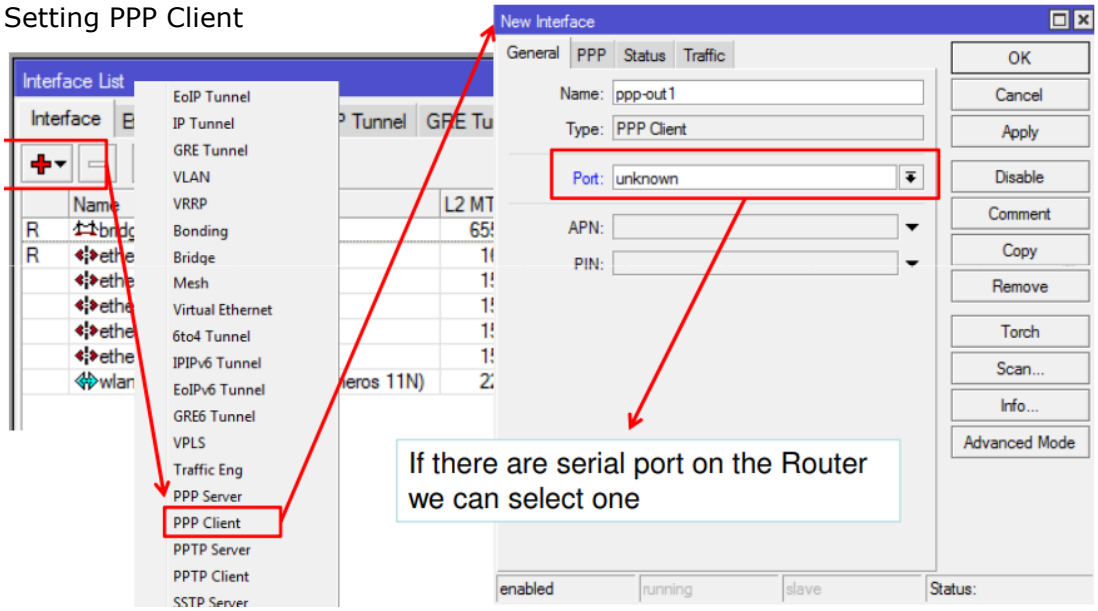


Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

PPP TUNNEL

- PPP (Point-to-Point Protocol) is a layer 2 protocol that is used for serial communication.
- Not like EoIP, PPP is Client-Server tunnel.
- To run a PPP connection, RouterOS must have serial port / serial interface, a RJ11 port telephone line (PSTN), or cellular modem (PCI or PCMCIA)
- To connect server PPP client dial up a specific phone number (ie the number *99 *** 1#).
- Then PPP client virtual interface will get the IP address for the internet connection.
- RouterOS can be used as PPP server and PPP client in the same time

Setting PPP Client



PPTP TUNNEL

- Point to Point Tunnel Protocol provides encrypted tunnels over IP using TCP and GRE (Generic Routing Encapsulation).
- PPTP is secure, because it uses encryption MPPE (Microsoft Point-to-Point Encryption) length 40 and 128 bits encrypts.
- PPTP uses TCP port 1723
- PPTP Client can be run on any Operating System
- PPTP is a client-server type of tunnel, where the PPTP server have to configure for every client who wants to connect

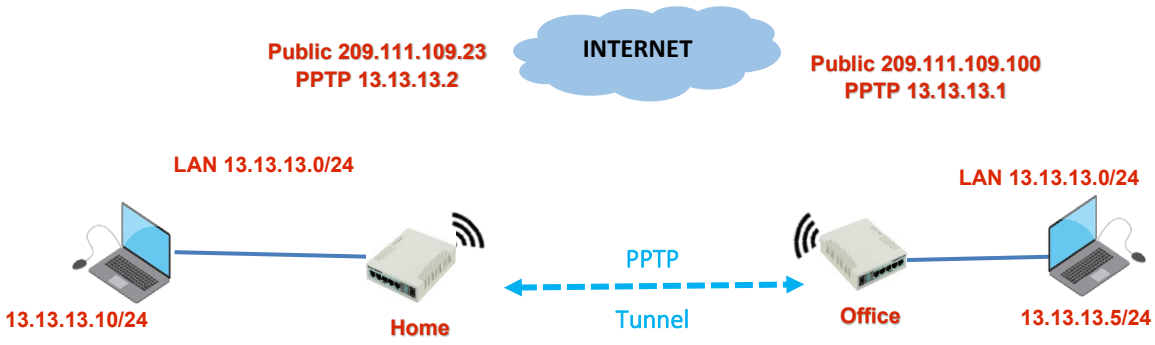
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

PPP SECRET

- All connections that use PPP protocol always involvesthe authentication username and password.
- Locally, username and password is stored and organized in a PPP>Secret menu.
- The username and password can also be stored in a separate RADIUS server.
- PPP Secret is local database store the username and password that will be used by all PPTP clients.
- Besides used for PPTP client, PPP secret is also used for other PPP protocol such as L2TP, OpenVPN, PPPoE, and SSTP.

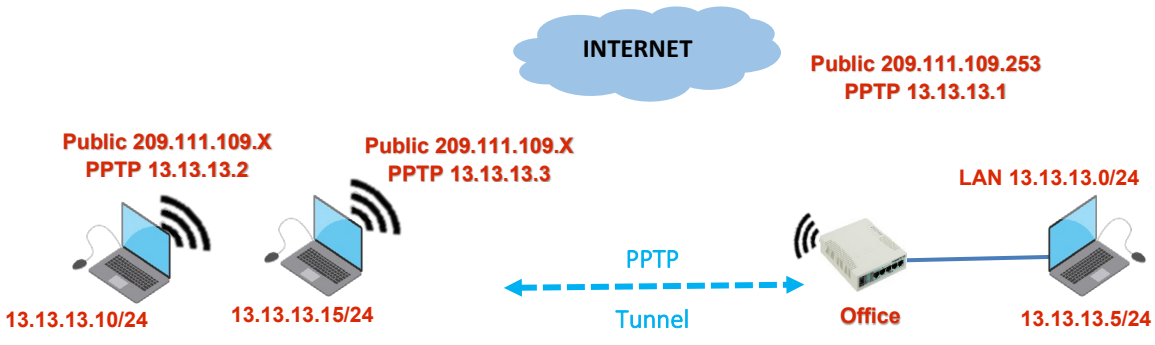
9.3-LAB-PPTP Tunnel (MK to MK)

- *Create PPTP Tunnel between Office (server) to Home (client)*



9.4-LAB-PPTP Tunnel (MK to Laptop)

- *Create PPTP Tunnel between Office (server) to Laptops (client)*



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

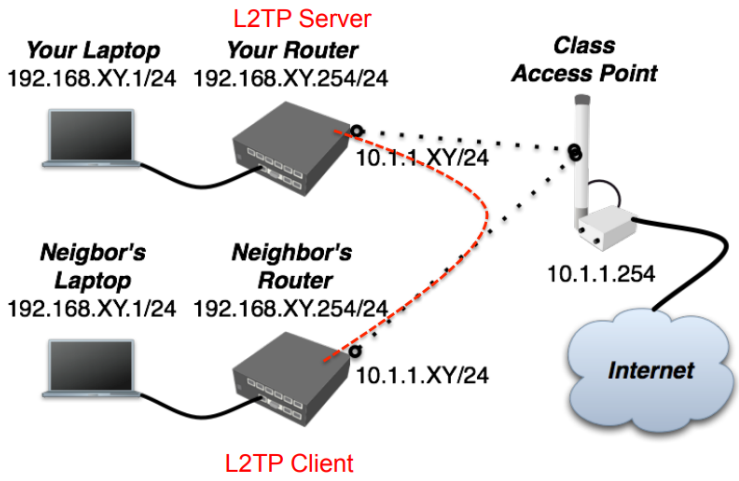
Note: When accessing to Internet via tunneling, the actual traffic is not detected. So that usually tunnel can bypass content firewall. Connection detected as PPTP tunnel using protocol 47 (GRE).

L2TP TUNNEL

- Layer 2 Tunneling Protocol (L2TP) is another type of tunneling and encapsulation for PPP protocol
- L2TP support non-Ethernet protocol like frame relay, ATM and SONET
- L2TP was developed in cooperation between Cisco and Microsoft to combine the features of PPTP with Layer 2 Forwarding, Cisco proprietary protocol
- L2TP does not encrypt packets, for encryption L2TP usually combined with IPsec (but not mandatory)
- L2TP uses UDP port 1701
- L2TP configuration is almost the same as PPTP

9.5-LAB-L2TP

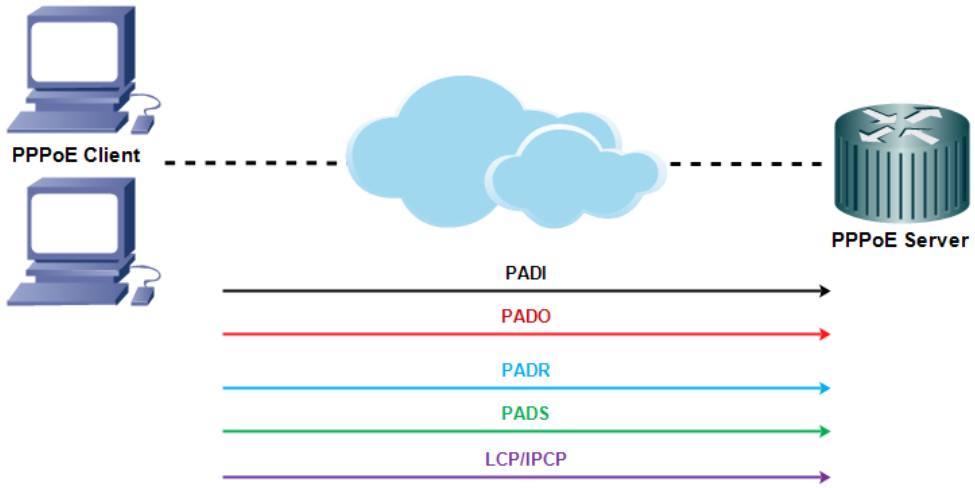
- *Create L2TP Tunnel between Office (server) to Laptops (client)*



PPPOE TUNNEL

- PPPoE encapsula'on Point-to-Point Protocol (PPP) in the Ethernet frame
- PPPoE is typically used for ADSL service.
- PPPoE is Point-to-Point, where there should be one point to one point again. If the first point is our ADSL router, then where is the another point?

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

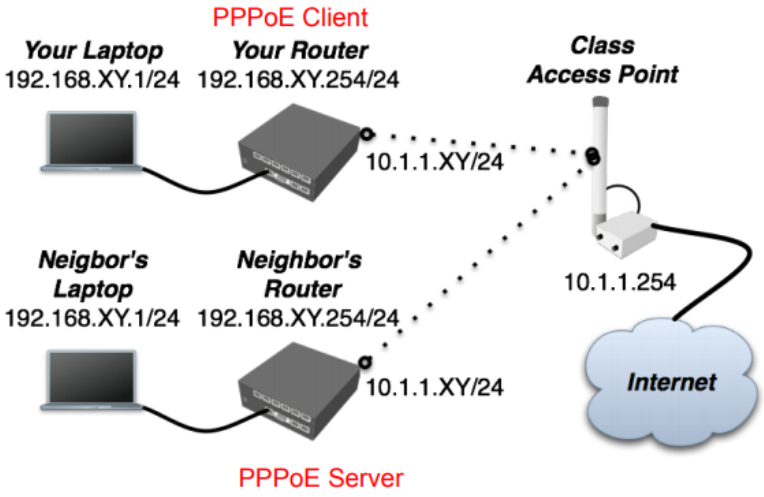


- How PPPoE client in our ADSL modem can find PPPoE server if ADSL provider only give us username and password not IP of PPPoE server

- PADI (PPPoE Active Discovery Initiation), Here PPPoE client sends a broadcast frame to the network, using destination mac address FF:FF:FF::FF::FF:FF
- PADO (PPoE Active Discovery Offer). PADO is a response from one of PPPoE server. PPPoE send PADO with source mac address.
- PADR (PPoE Active Discovery Request), is a confirmation of the PPPoE client to the server. Here PPoE client is able to contact the server using mac address directly (not need broadcast anymore).
- PADS (PPP Active Discovery Session-confirmation), from PPPoE server to the client. At this stage also occurs negotiations username and password then continue with TCP/IP connection.
- PADT (PPP Active Discovery Terminate), can be sent from the server or client, when one of both wants to end the connection.

9.6-LAB-PPPoE

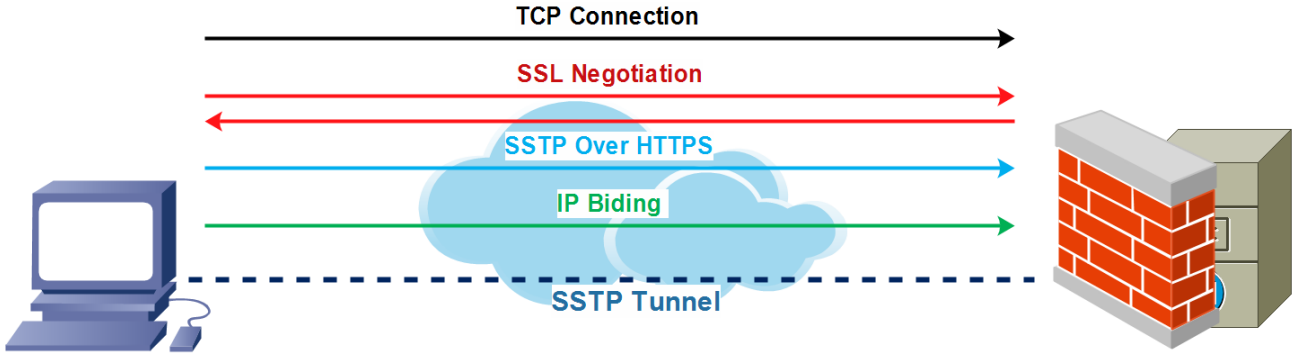
- *Create PPPoE Server and PPPoE client*
- *After connect to PPPoE server, PPPoE will get IP Address automatically and can access to Internet.*



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SSTP TUNNEL

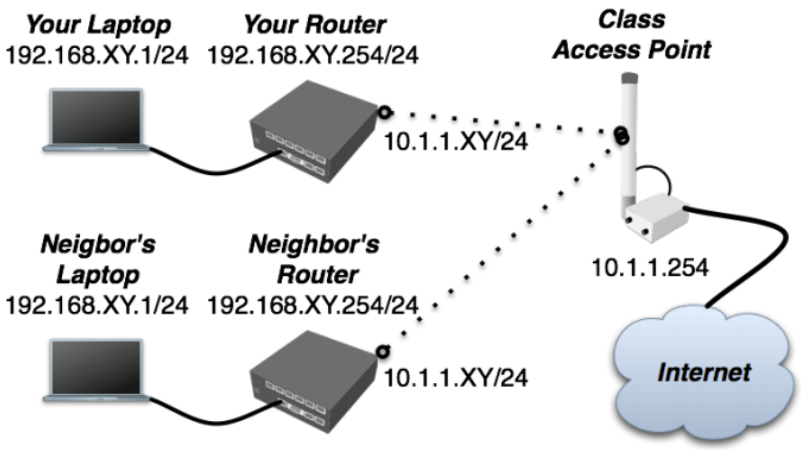
- Secure socket tunneling protocol (SSTP) transport a PPP tunnel over a TLS 1.0 channel
- The use of TLS over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers



1. TCP connection is established from client to server (by default on port 443)
2. SSL validates server certificate. If certificate is valid connection is established otherwise connection is torn down
3. The client send SSTP control packets within the HTTPS session which establishes the SSTP state machine on both sides
4. PPP negotiation over SSTP. Client authenticates to the server and bind IP addresses to SSTP interface
5. SSTP tunnel is now established and packet encapsulation can begin

9.7-LAB-SSTP

- *One of your router will be the SSTP server and other will be SSTP client.*
- *Exchange certificates between SSTP server and Client*



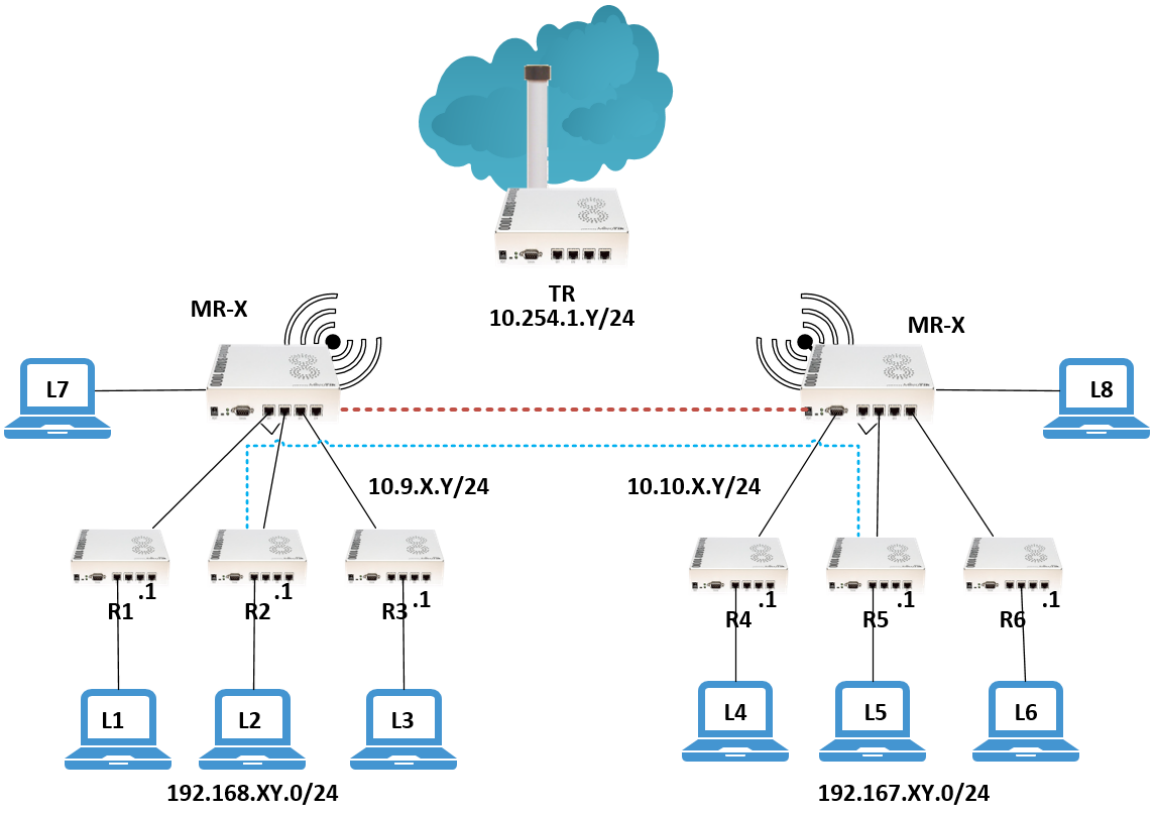
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

DIFFERENT OF TUNNELS

Tunnel	Encryption	Protocol/Port	Notes
EoIP	None	IP no 47 (GRE)	- Proprietary MikroTik - Possible to be bridge
PPTP	MPPE 128 bits	TCP 1723	- Most widely used - PPTP client can run almost in all OS
L2TP	Borrow IPSec 168 bits	UDP 1701	- Not has encryption so borrow IPSec - But Not mandatory using IPSec
SSTP	SSL 2048	TCP 443	- Usually never block by firewall - Very secure
PPPoE	MPPE 128 bit	Frame	- Layer 2 tunnel - Can't pass the router

9.8-LAB-Extra EOIP over PPTP / L2TP

- *Do EOIP tunnel between MR routers*
- *After do PPTP tunnel between RX routers*
- *Restore configuration by do EOIP tunnel between MR routers after do L2TP tunnel between RX routers*



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CHAPTER 10: MISC

OBJECTIVE

After finish this lesson student will be able to:

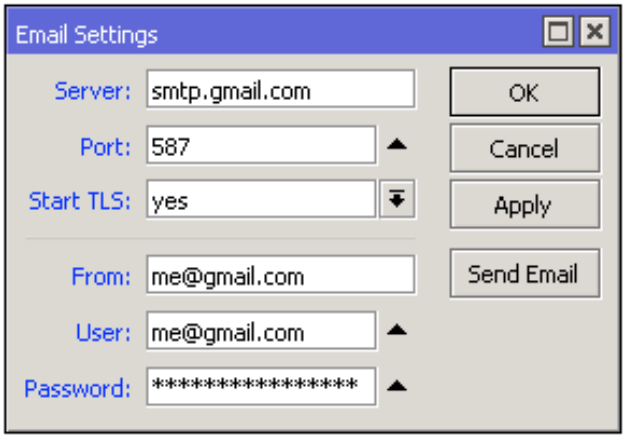
- RouterOS tools
  - E-mail, Netwatch, Ping
  - Traceroute, Profiler (CPU load)
- Monitoring
  - Interface traffic monitor, Torch
  - Graphs, SNMP, The Dude.

ROUTEROS TOOLS

RouterOS provides various utilities that help to administrate and monitor the router more efficiently.

E-mail

- Allows to send e-mails from the router
- For example to send router backup
- Tool => Email



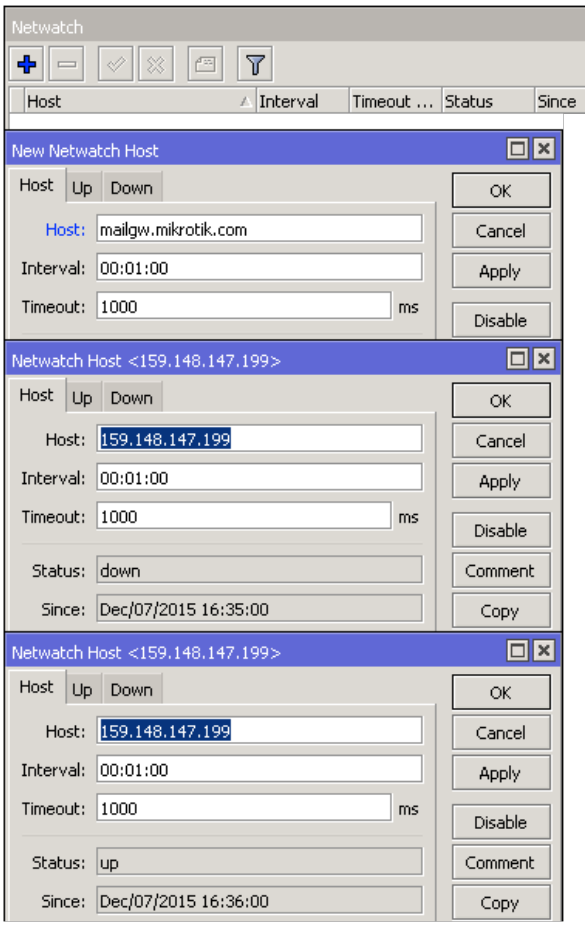
A script to make an export file and send it via e-mail

```
/export file=export
/tool e-mail send to=you@gmail.com\
  subject="$[/system identity get name] export"\
  body="$[/system clock get date]\
  configuration file" file=export.rsc
```

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

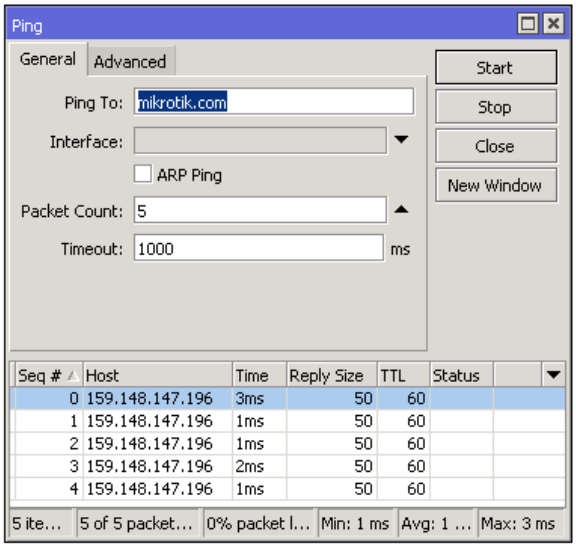
Netwatch

- Monitors state of hosts on the network
- Sends ICMP echo request (ping)
- Can execute a script when a host becomes unreachable or reachable



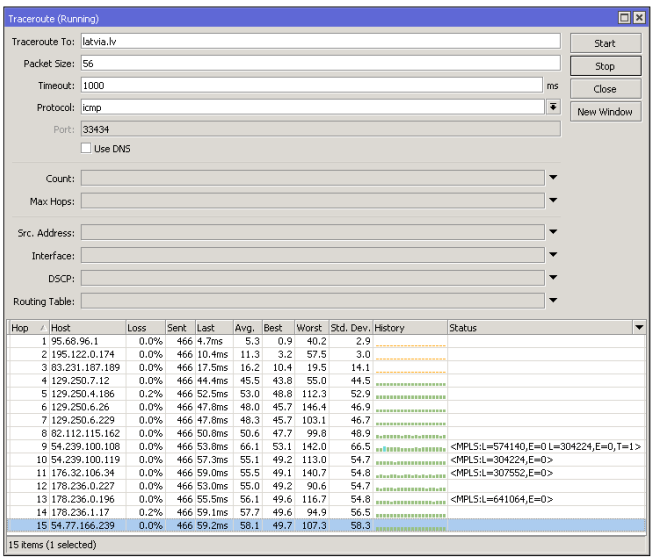
Ping

- Used to test the reachability of a host on an IP network
- To measure the round trip time for messages between source and destination hosts
- Sends ICMP echo request packets



Traceroute

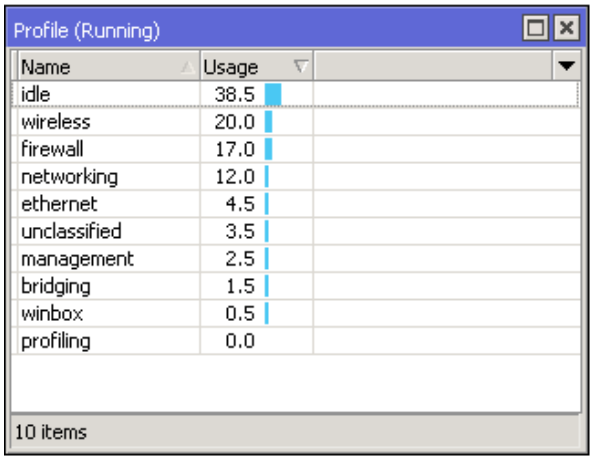
- Network diagnostic tool for displaying route (path) of packets across an IP network
- Can use icmp or udp protocol



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

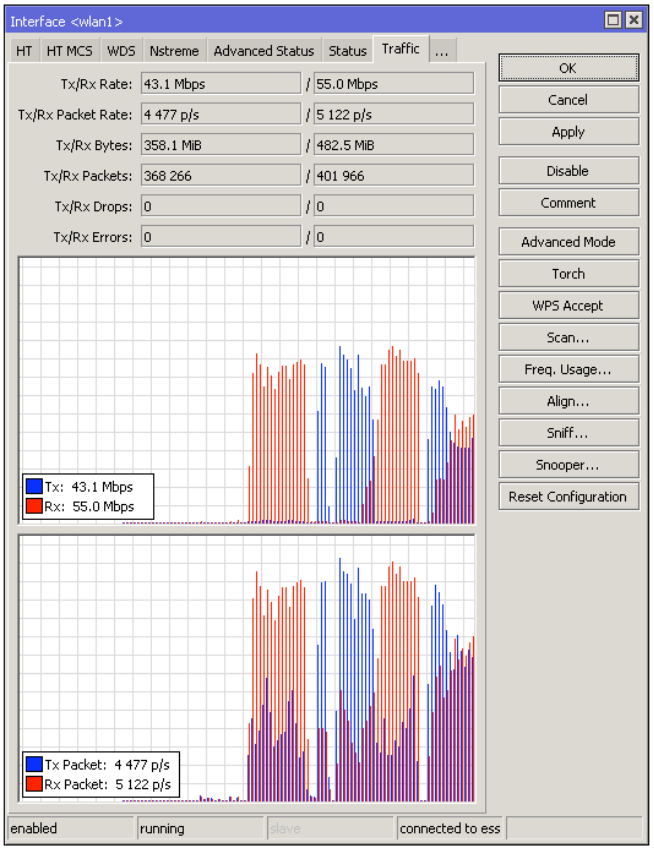
Profile

- Shows CPU usage for each RouterOS running process in real time
- idle - unused CPU resources
- For more info see Profile wiki page



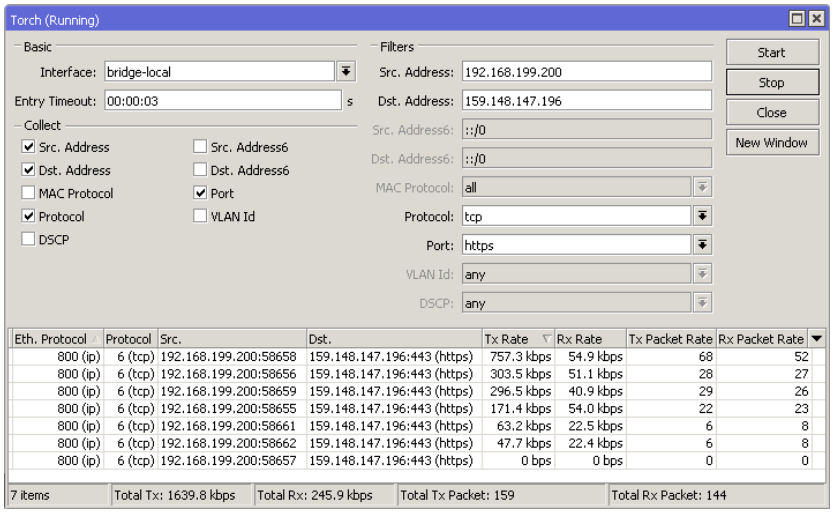
Interface Traffic Monitor

- Real time traffic status
- Available for each interface in traffic tab
- Can also be accessed from both WebFig and command line interface



Torch

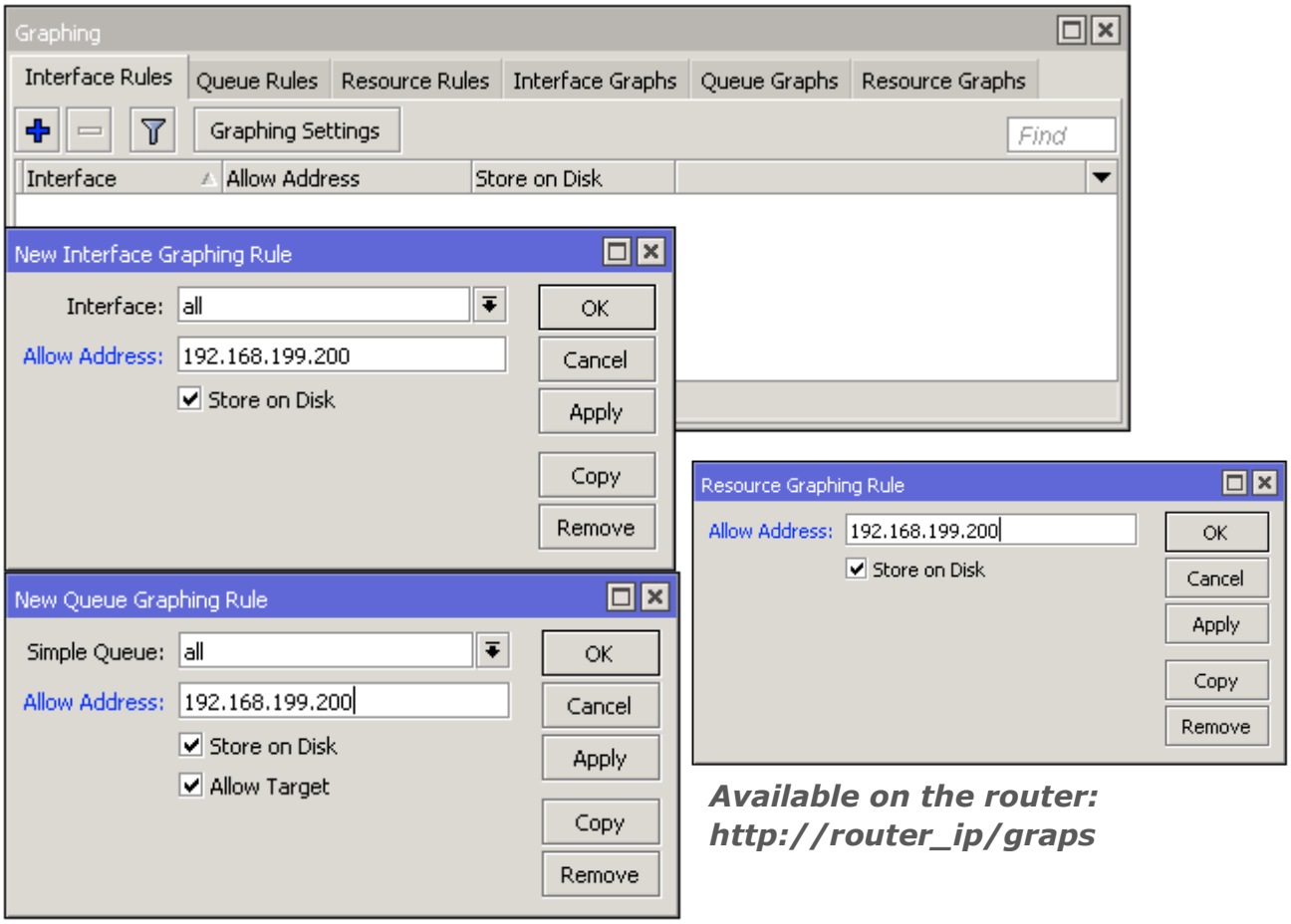
- Real-time monitoring tool
- Can be used to monitor the traffic flow through the interface
- Can monitor traffic classified by IP protocol name, source/destination address (IPv4/ IPv6), port number



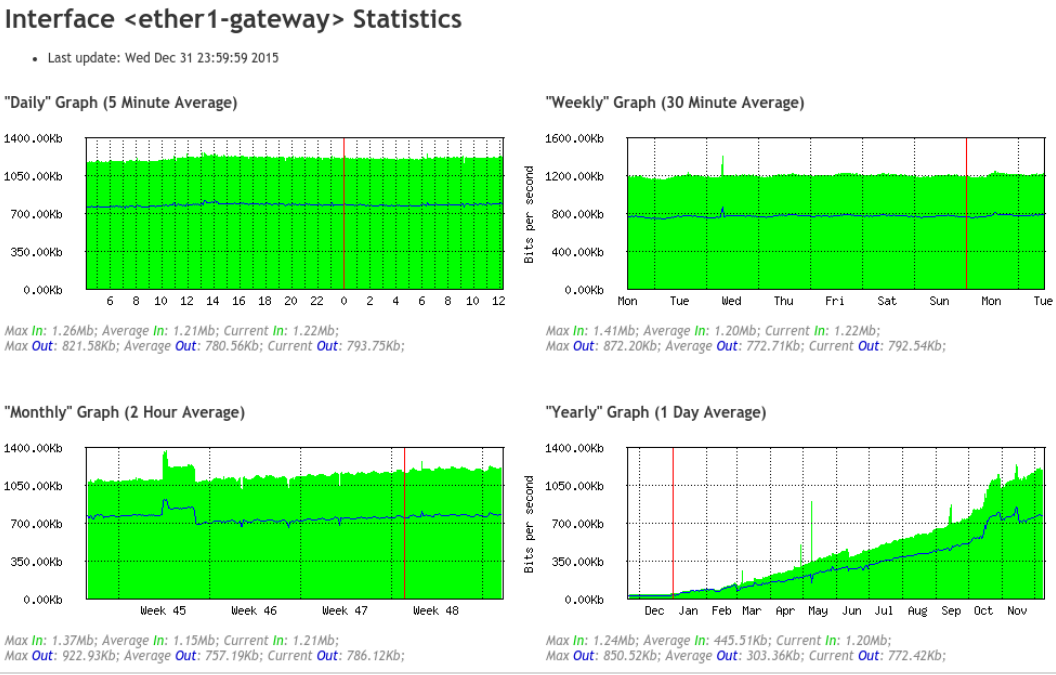
Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

Graph

- RouterOS can generate graphs showing how much traffic has passed through an interface or a queue
- Can show CPU, memory and disk usage
- For each metric there are 4 graphs - daily, weekly, monthly and yearly



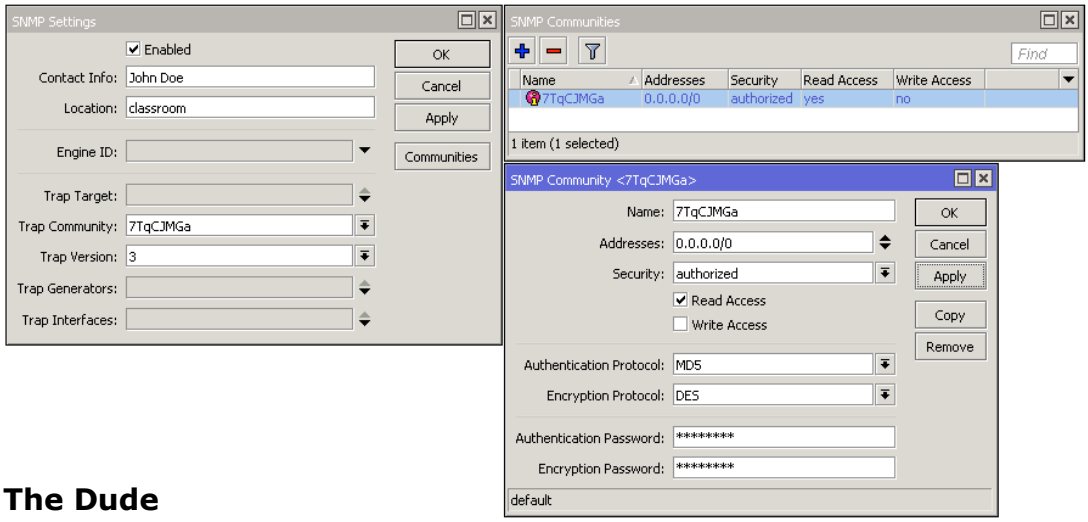
Available on the router: http://router_ip/graps



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

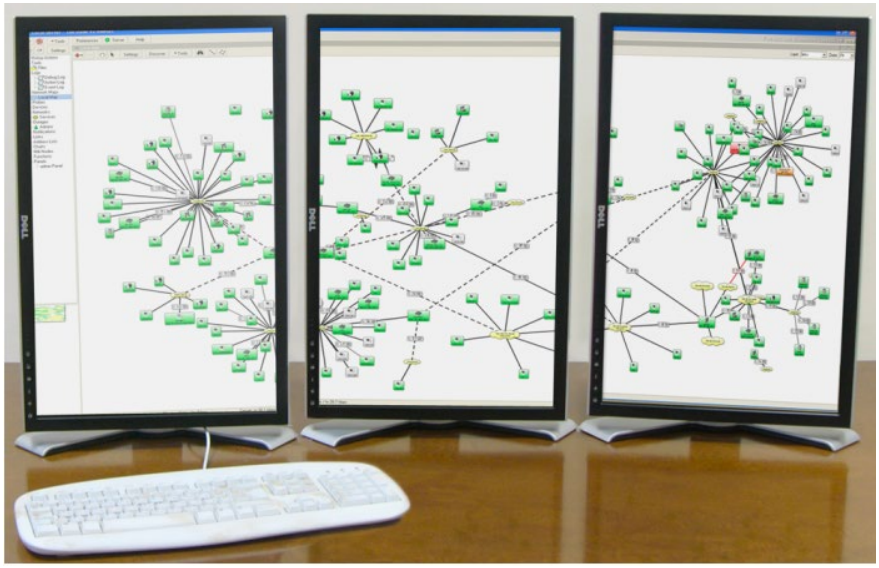
SNMP

- Simple Network Management Protocol (SNMP)
- Used for monitoring and managing devices
- RouterOS supports SNMP v1, v2 and v3
- SNMP write support is available only for some settings



The Dude

- Application by MikroTik which can dramatically improve the way you manage your network environment
- Automatic discovery and layout map of devices
- Monitoring of services and alerting
- Free of charge
- Supports SNMP, ICMP, DNS and TCP monitoring
- Server part runs on RouterOS (CCR, CHR or x86)
- Client on Windows (works on Linux and OS X using Wine)
- For more info see The Dude wiki page



Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

SUMMARY

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW

True False Question

T	F	#	Questions
		1	
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	

Passerelles numériques Cambodia
Street 371 Phum Tropeang Chhuk (Borey Sorla), Sangkat Tek Thla
Khan Sen Sok P.O. Box 511 Phnom Penh, Cambodia
Tel: +855 23.99.55.00
info.cambodia@passerellesnumeriques.org

CONCEPTs REVIEW