Hardening MikroTik RouterOS

April 24, 2017
MUM Phnom Penh, Cambodia

By Sarpich RATH (Peter)

About PPIC

- Qualified and Vocational IT Training Center
- Found in late 2013. Offer service in June 2014
- Partners
  - MikroTik Academy
  - Cisco Networking Academy
  - Pearson VUE
  - Prometric

About Me

- Sarpich RATH (Peter)
- First used RouterOS since 2008
- MTCNA, MTCRE, Academy Trainer
- CCNA, CCNA Security, CCNP, Cisco Instructor
- Trainer @PPIC and AEU

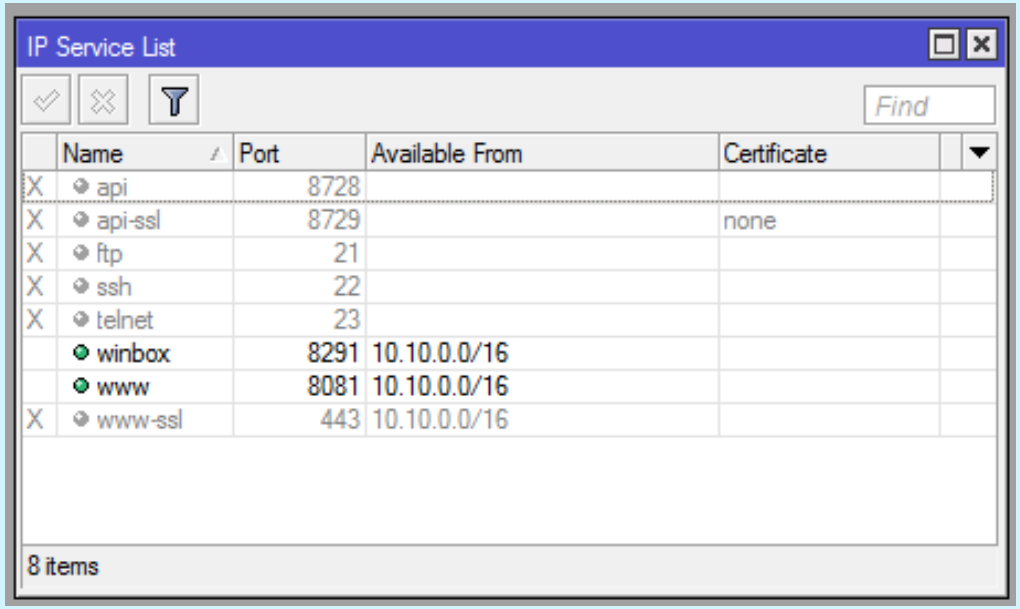
Topic: Hardening MikroTik RouterOS

- Customized RouterOS setting
- RouterOS Firewall
- Recommendation

Customized RouterOS setting

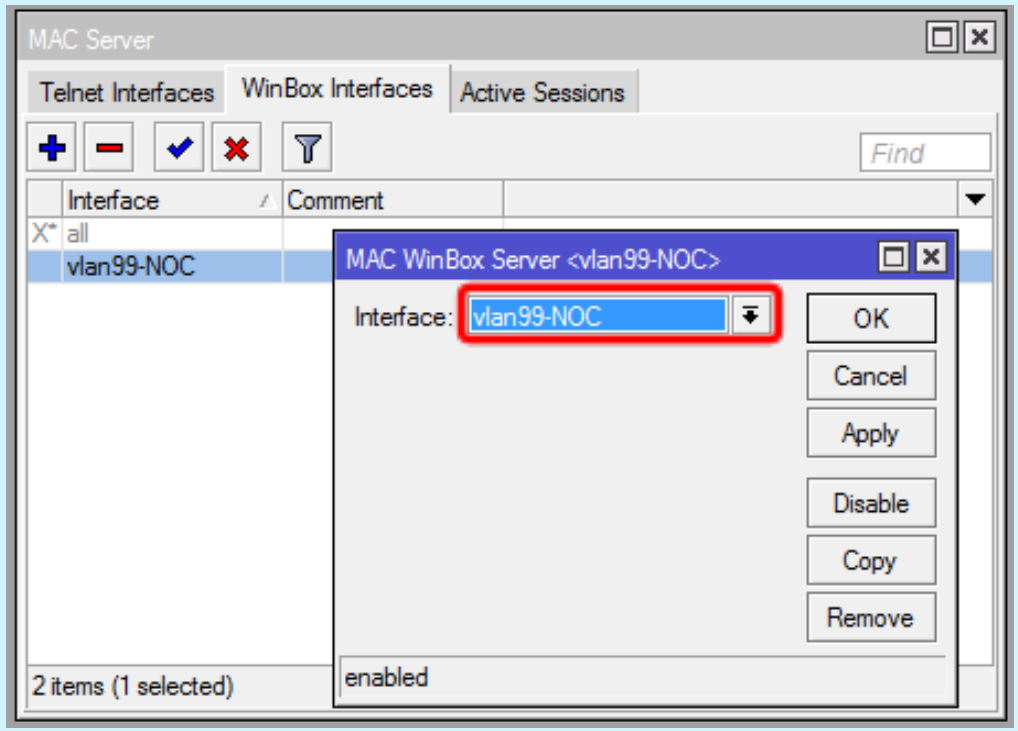
Login Services: IP->Services

- Disable unused services
- Or modify default port
- Limit access from specific network



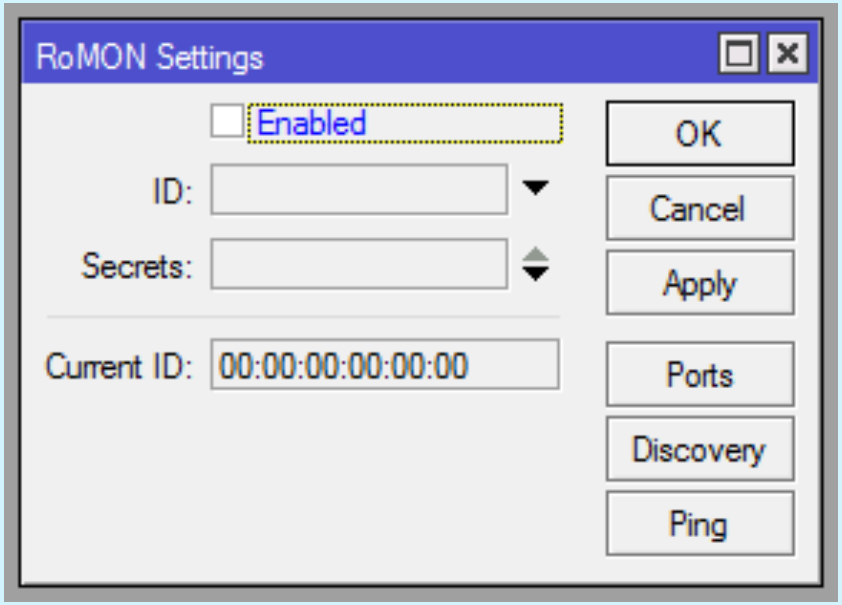
MAC WinBox: Tools->MAC Server

- Disable Allow to login from all interfaces
- Allow from specific interface only



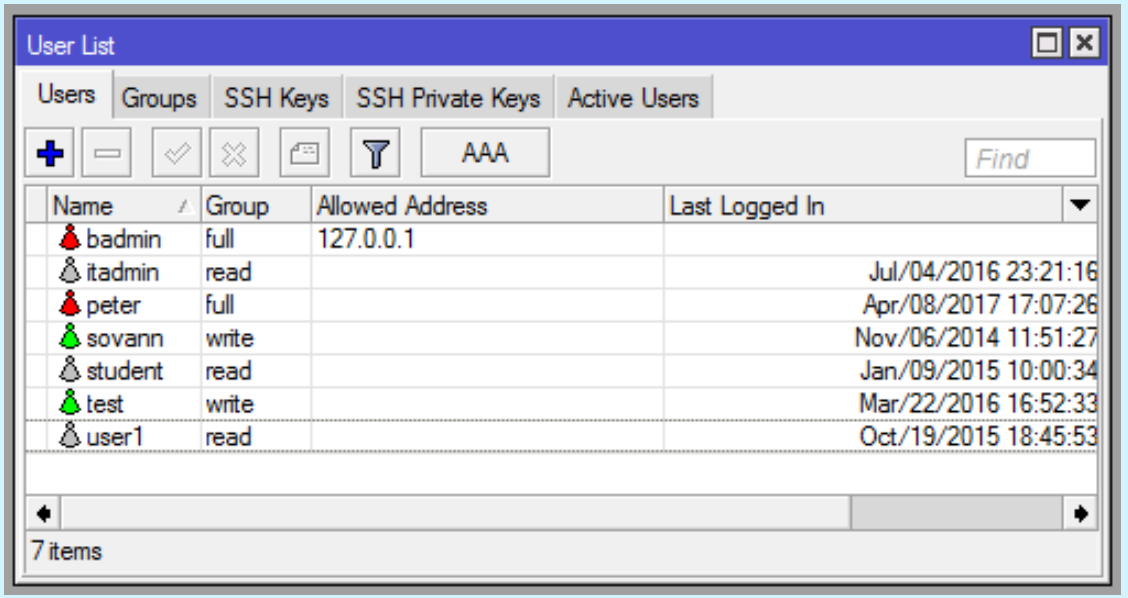
RoMON: Tools->RoMON

- Disable by default
- /tool romon set enabled=no



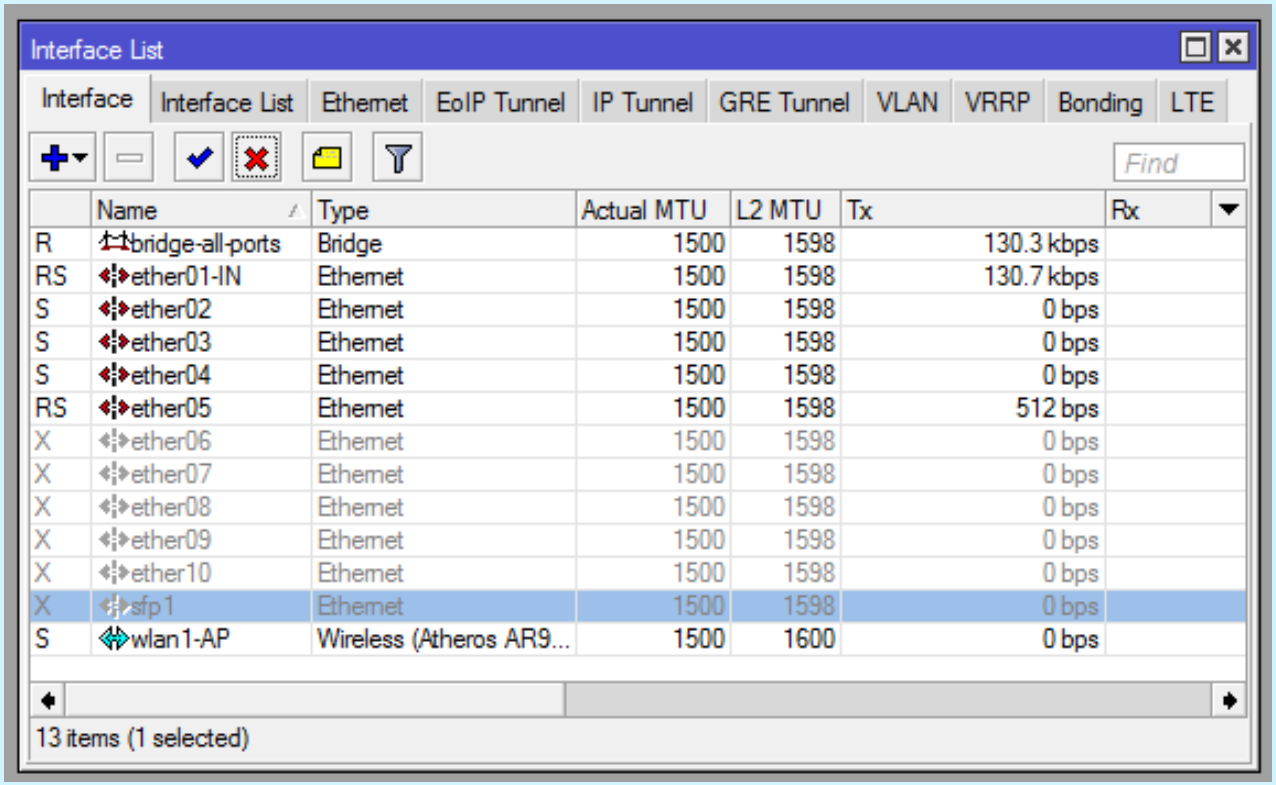
Login Credentials: System->Users

- Rename default admin account
- Strong password policy
- Set the right permission (group) to router users
- Backup login account



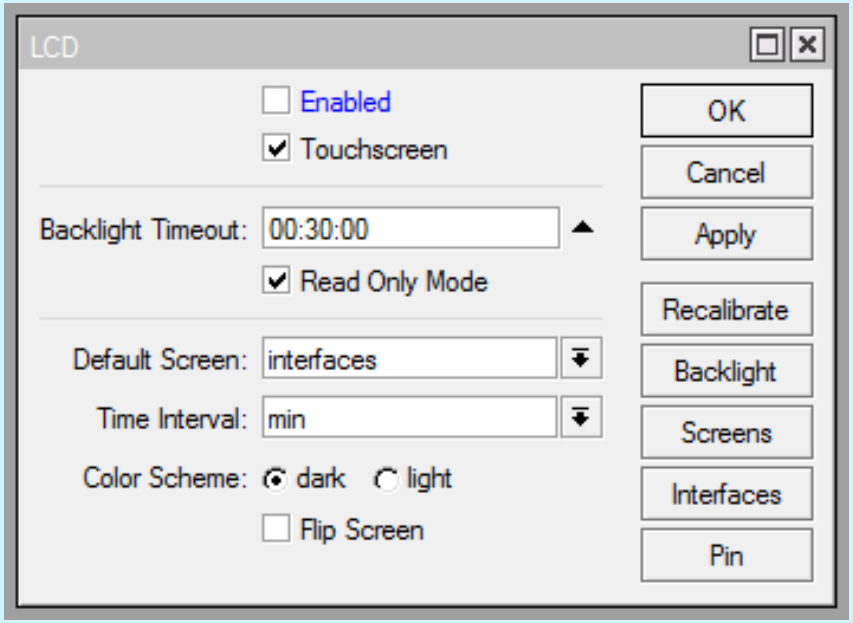
Router Interface

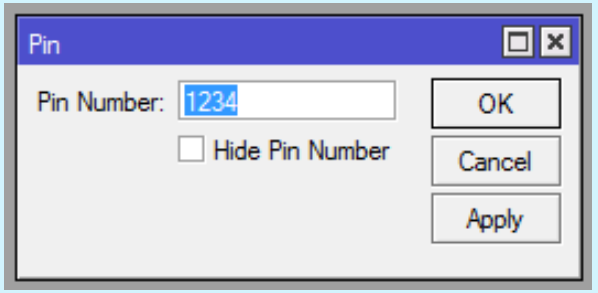
- Disable all unused interfaces on your router, in order to decrease unauthorized access to your router.

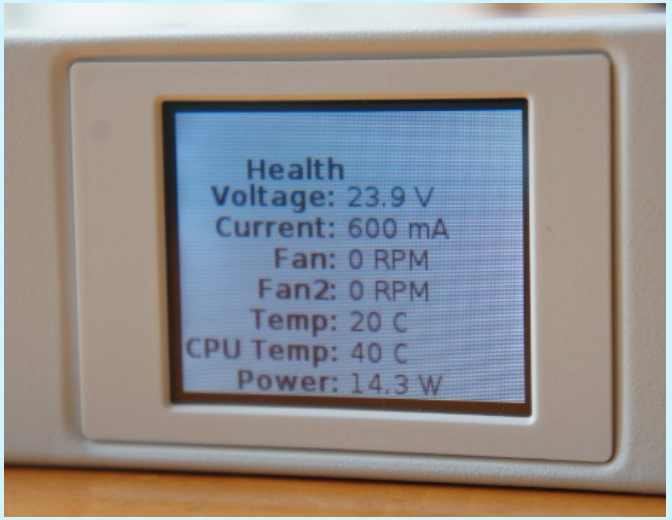


LCD touch screen

- Some RouterBOARDs have LCD module for informational purpose, set pin or disable it.

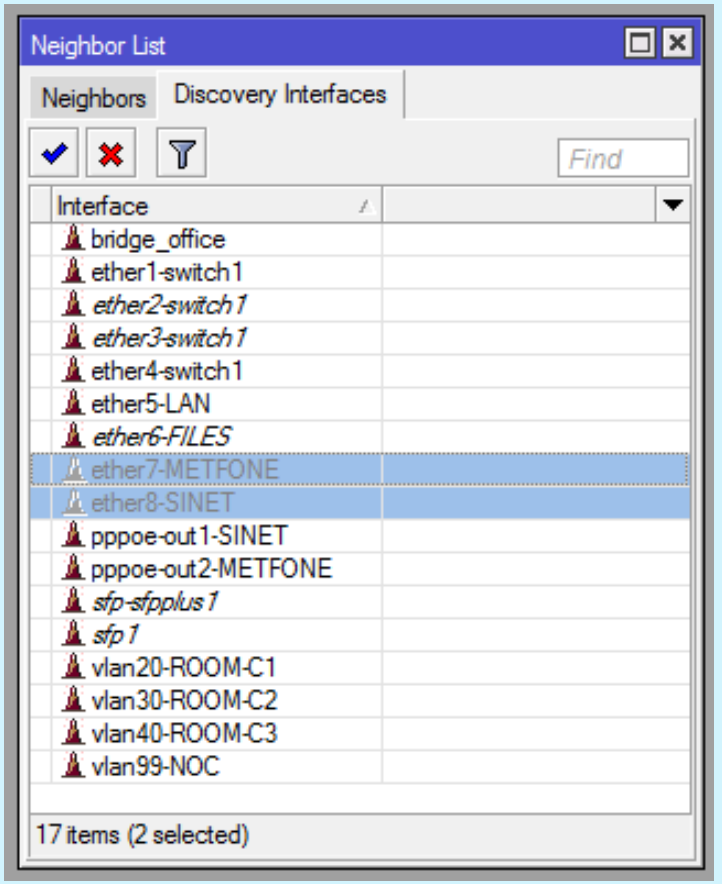




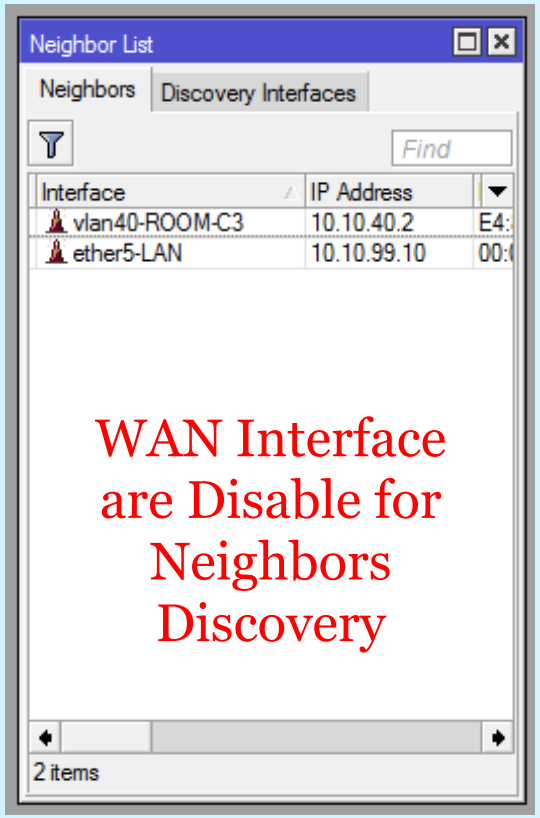


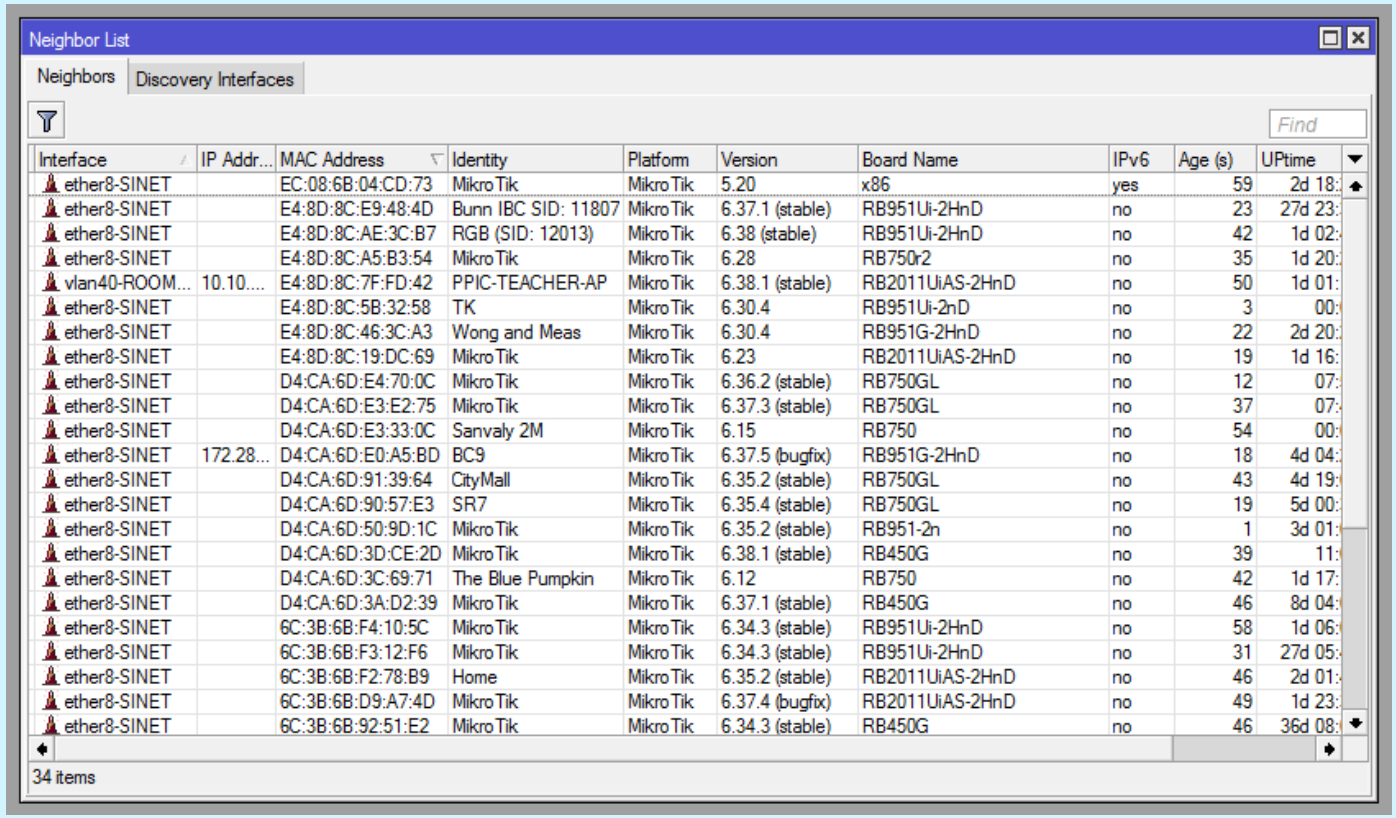
Neighbor Discovery: IP->Neighbors

- Disable Discovery on Interface that connect to Internet



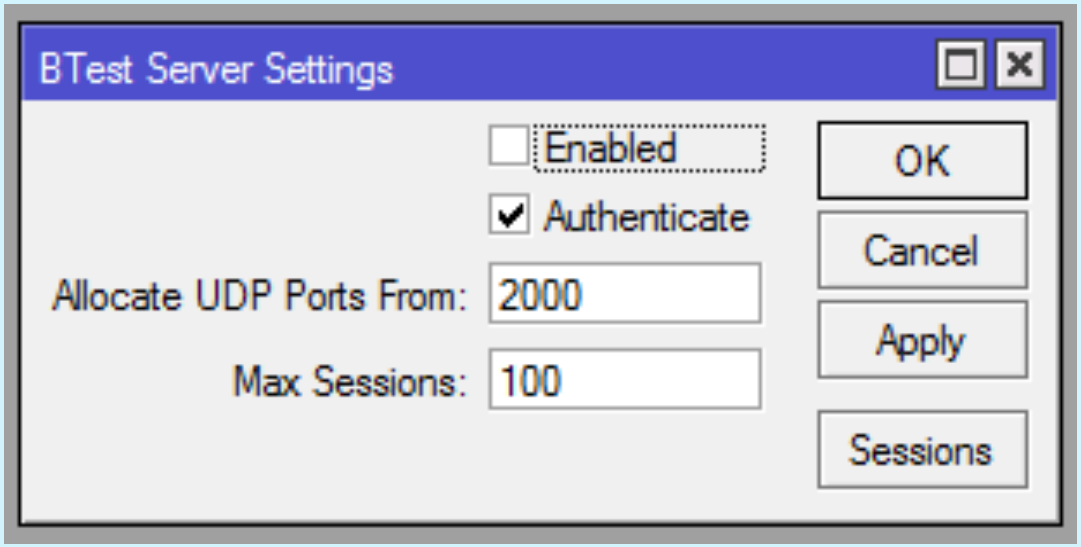
Neighbor Discovery: IP->Neighbors





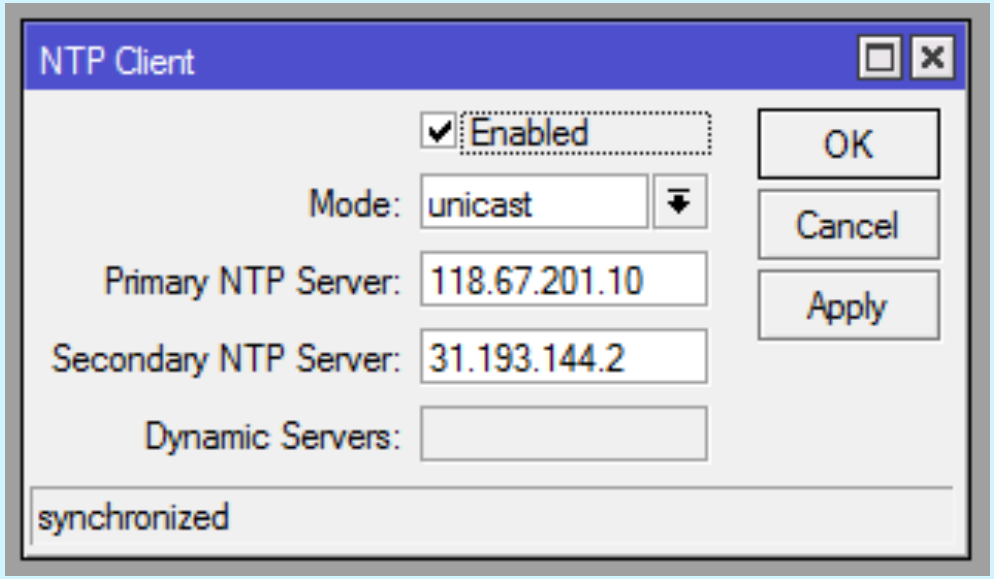
BTest Server: Tools-> Btest Server

- Bandwidth Test
- Disable when not used it



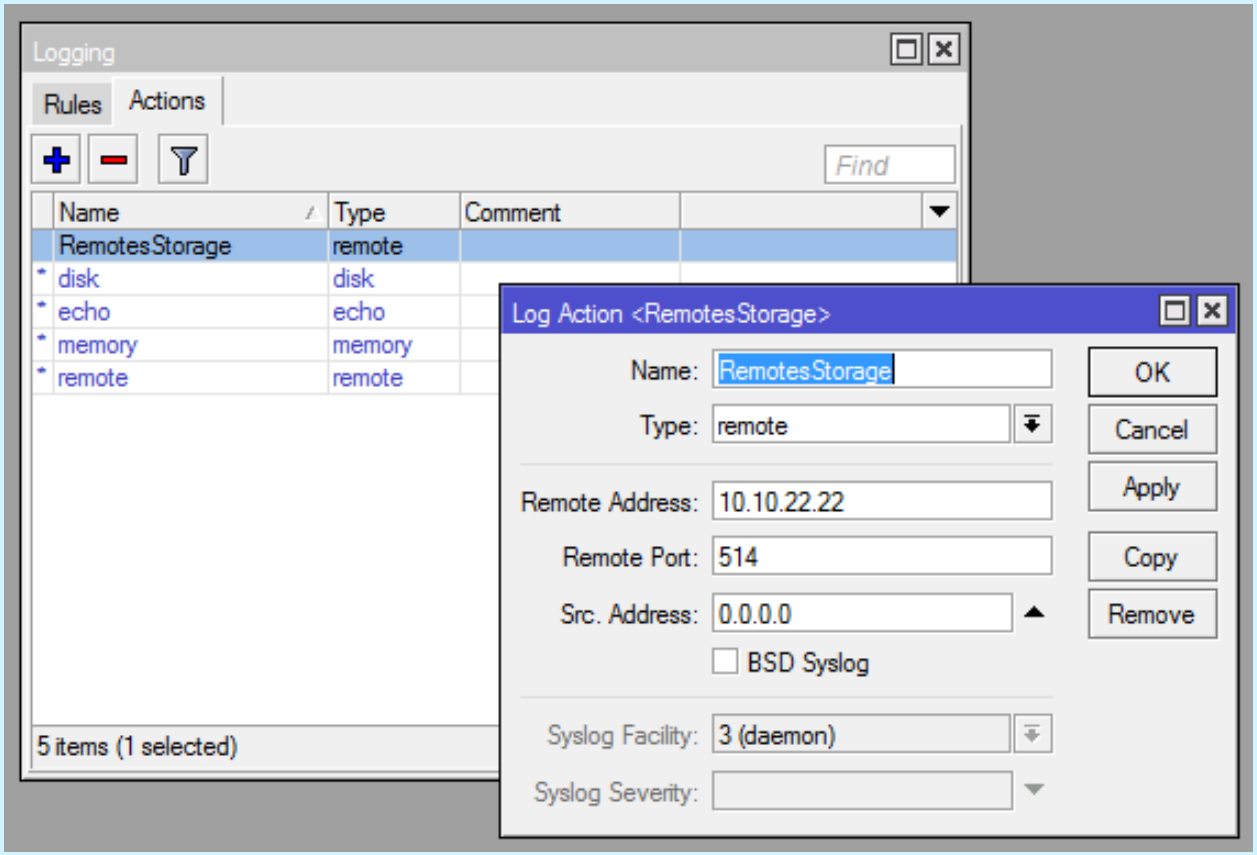
NTP Clock Synchronization

- Keep the router sync with accurate clock
- Server: kh.pool.ntp.org



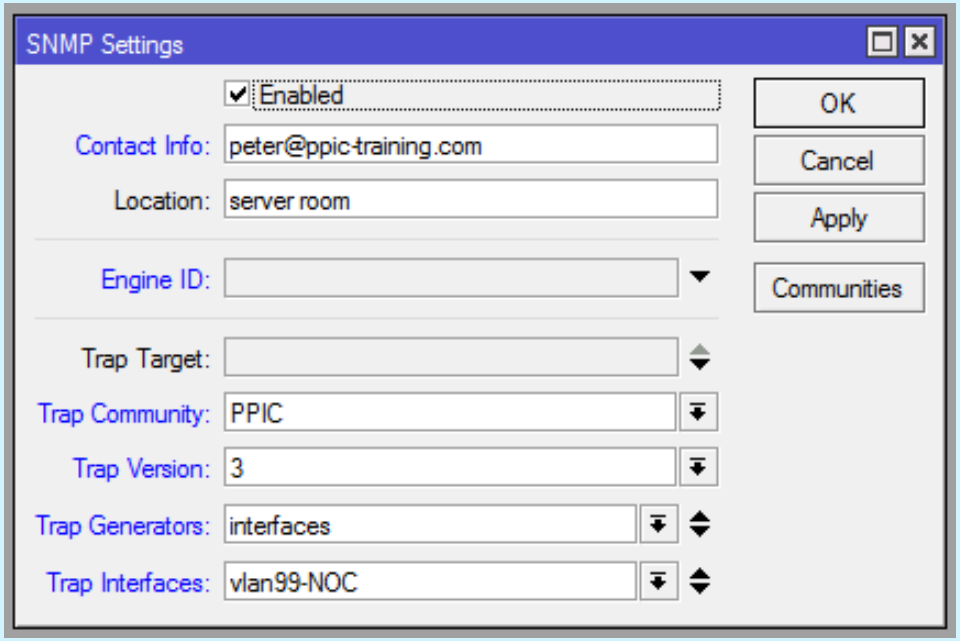
Logging: System->Logging

- Send log message to SysLog Server



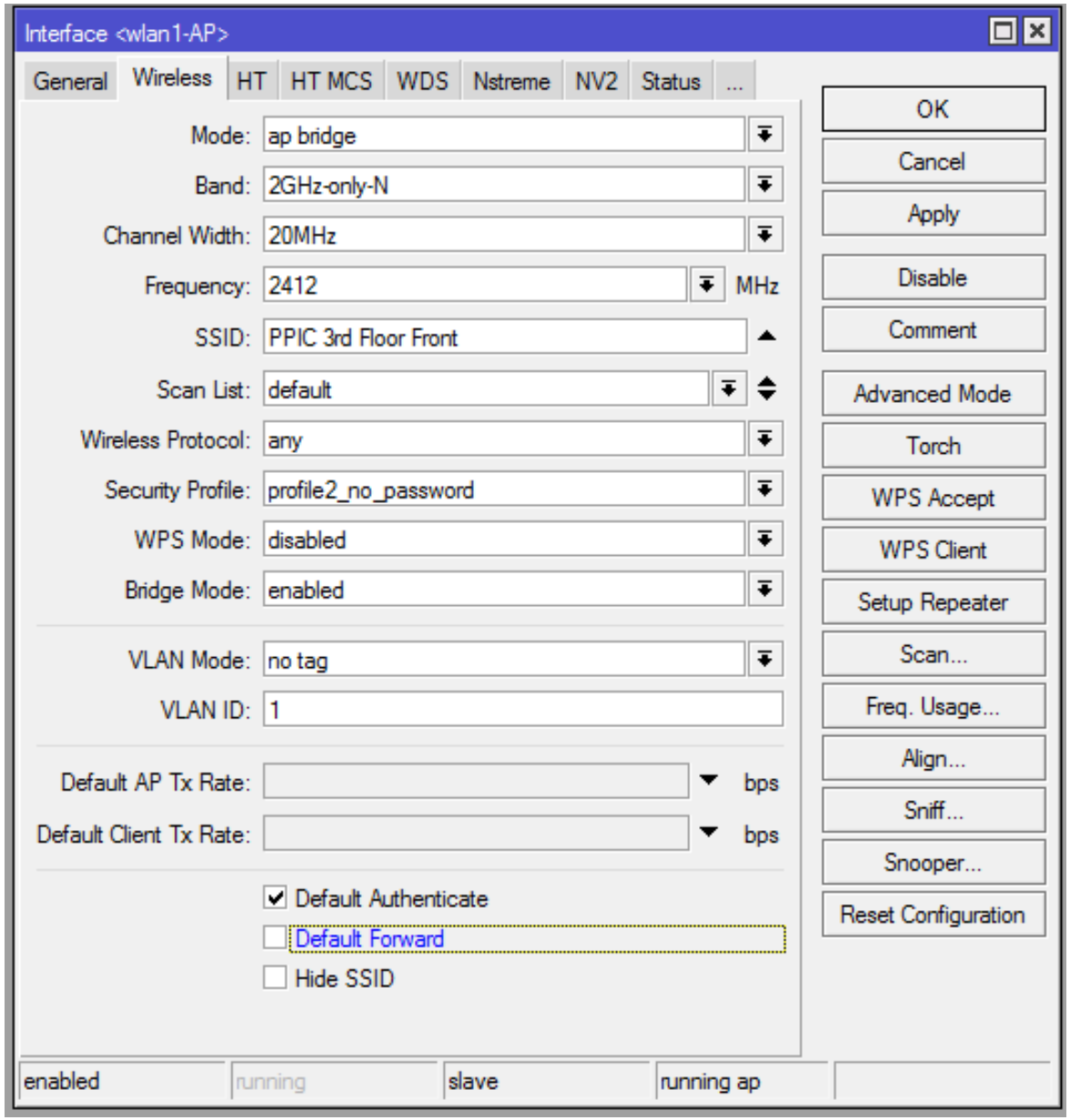
SNMP: IP->SNMP

- Simple Network Management Protocol
- Used to Monitor Bandwidth and resource usages.

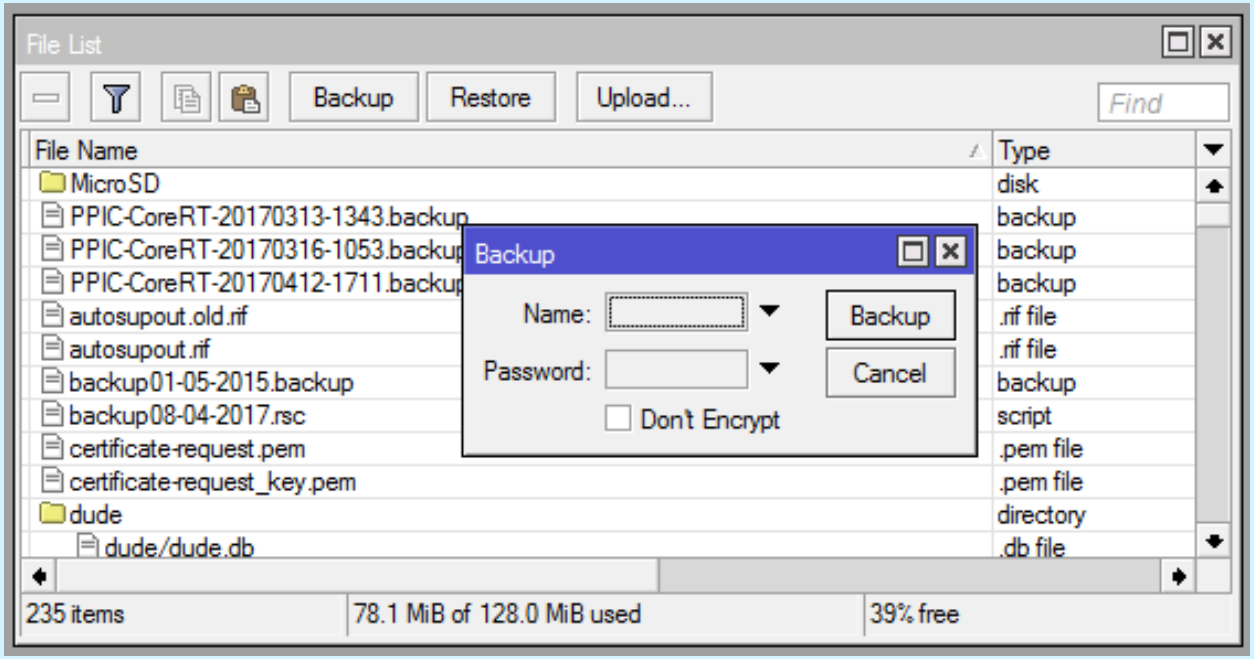


Wireless Client Isolation

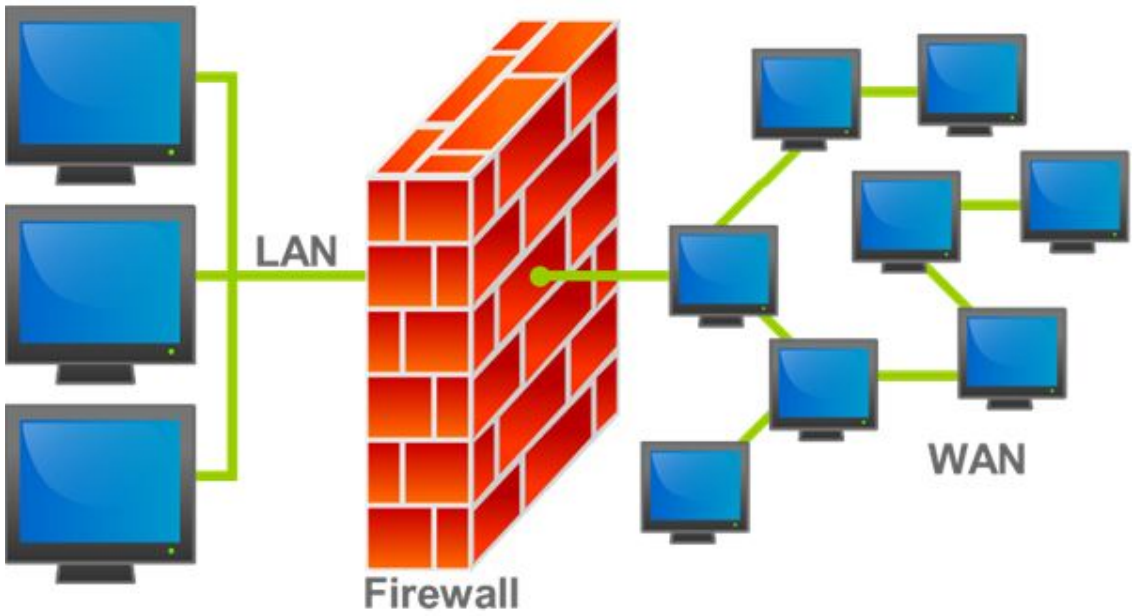
- Allows multiple clients to be on the same network, but not send traffic to each other.
- Attention!!! streaming content to/from other devices such as Chromecast, AppleTV, Ruku, etc… will not work on the same AP.


Interface <wlan1-AP>
General
Wireless
HT
HT MCS
WDS
Nstreme
NV2
Status
...
Mode: ap bridge
Band: 2GHz-only-N
Channel Width: 20MHz
Frequency: 2412 MHz
SSID: PPIC 3rd Floor Front
Scan List: default
Wireless Protocol: any
Security Profile: profile2_no_password
WPS Mode: disabled
Bridge Mode: enabled
VLAN Mode: no tag
VLAN ID: 1
Default AP Tx Rate: bps
Default Client Tx Rate: bps
Default Authenticate
Default Forward
Hide SSID
OK
Cancel
Apply
Disable
Comment
Advanced Mode
Torch
WPS Accept
WPS Client
Setup Repeater
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration
enabled
running
slave
running ap

Configuration Backup



RouterOS Firewall



What is FW used for?

- Preventing unauthorized access to networks
- Protect itself
- Filter for incoming and outgoing traffic.
- Protect and hide the server inside
- etc.

What can RouterOS FW do?

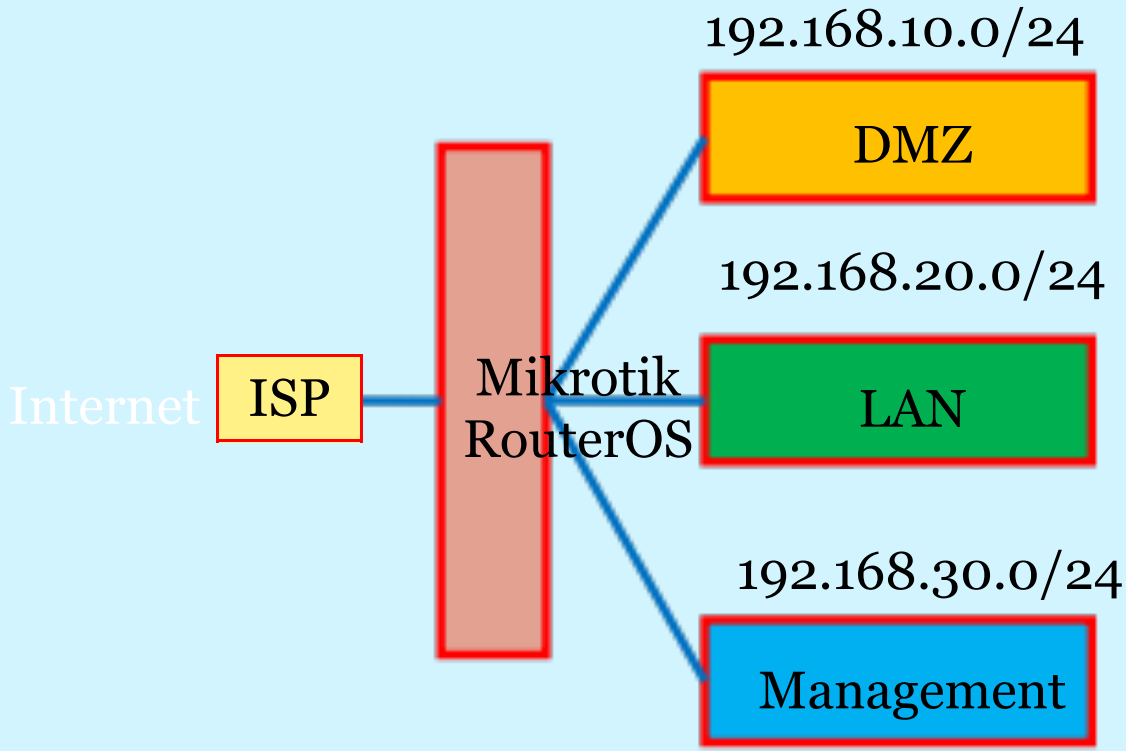
- stateful packet inspection
- Layer-7 protocol detection
- peer-to-peer protocols filtering
- traffic classification by:
  - source MAC address
  - IP addresses (network or list) and address types (broadcast, local, multicast, unicast)
  - port or port range
  - IP protocols
  - interface the packet arrived from or left through
  - internal flow and connection marks
  - packet size
  - packet arrival time
- and much more!

Sample Network design

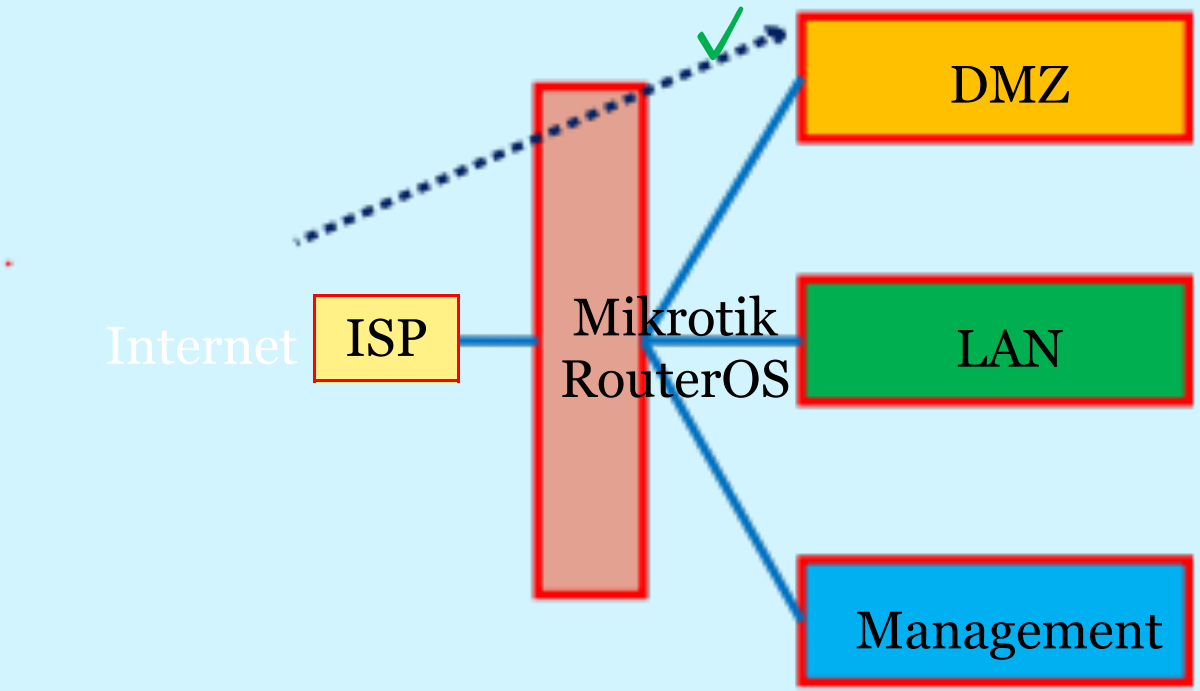
	Outside	Inside		
	ether1	ether2	ether3	ether4
Connect to	Internet	DMZ, Server	LAN	Management
Network	100.1.1.0/30	192.168.10.0/24	192.168.20.0/24	192.168.30.0/24

*** If we don't have enough ports, then can used VLAN for DMZ, LAN and Management network.

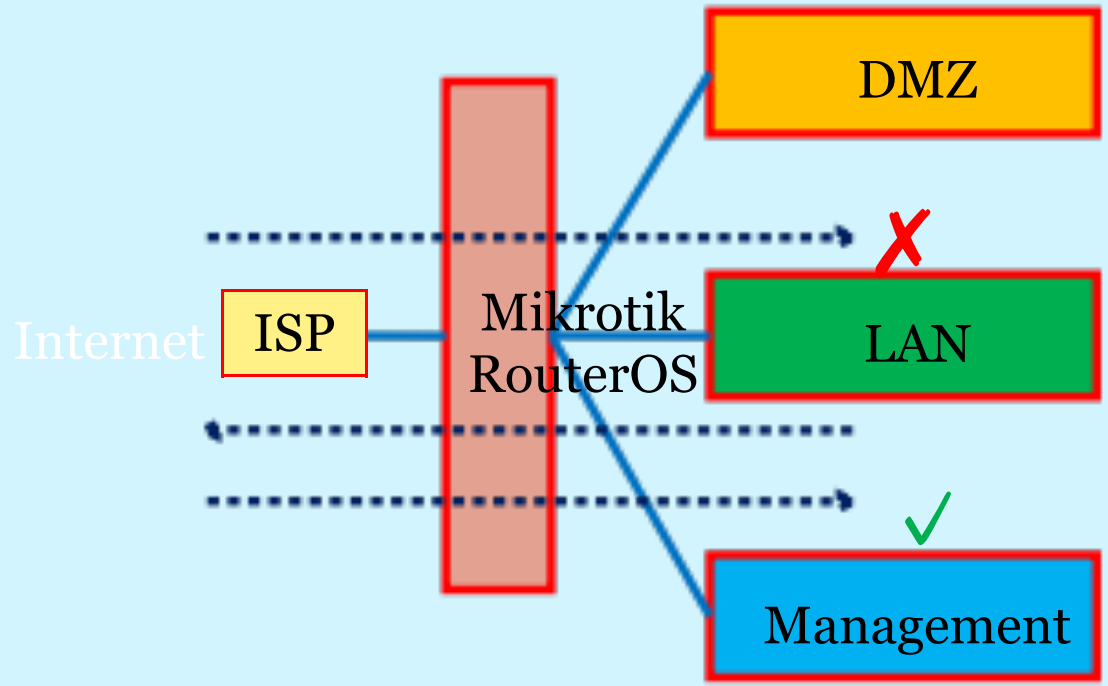
Sample Network design



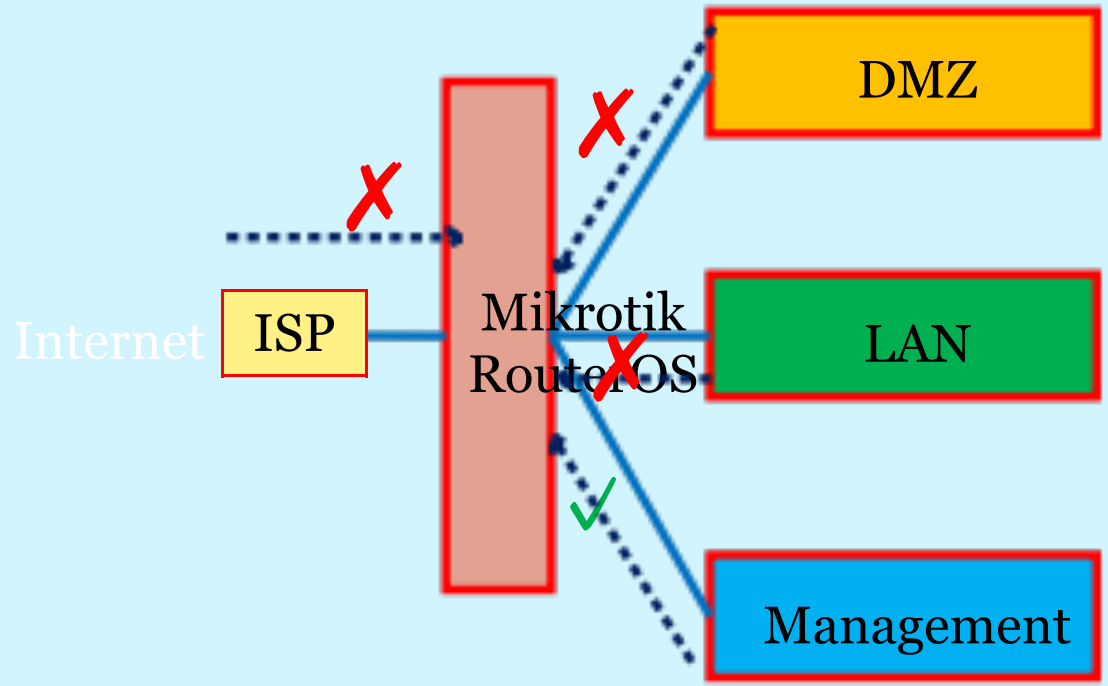
Internet to DMZ



Internet to LAN/Management



Management to Router



IPv4 firewall: Protect the router

- filter with new connections to decrease load on a router;
- create address-list for IP addresses, that are allowed to access your router; example Management
- enable ICMP access (optionally);
- drop everything else, log=yes might be added to log packets that hit the specific rule;

IPv4 firewall: Protect the router

```
/ip firewall filter
add action=accept chain=input comment="default configuration"
   connection-state=established,related
add action=accept chain=input src-address-list=Management
add action=accept chain=input protocol=icmp
.......
add action=drop chain=input

/ip firewall address-list add address=192.168.30.0/24 list=Management
```

IPv4 firewall: Protect the Inside network

- Established/related packets are added to fasttrack for faster data throughput, firewall will work with new connections only;
- drop incoming packets that are not NATed, ether1 is public interface
- drop incoming packets from Internet, which are not public IP addresses, ether1 is public interface
- drop packets from Inside that does not have address from inside address.
- create address-list=Inside to group all inside address
  - 192.168.10.0/24 = DMZ
  - 192.168.20.0/24 = LAN
  - 192.168.30.0/24 = Management

IPv4 firewall: Protect the Inside network

```
/ip firewall filter add action=fasttrack-connection chain=forward comment=FastTrack
    connection-state=established,related
add action=accept chain=forward comment="Established, Related" connection-
    state=established,related
add action=drop chain=forward comment="Drop invalid" connection-state=invalid
add action=drop chain=forward comment="Drop incoming packets that are not NATted"
    connection-nat-state=!dstnat connection-state=new in-interface=ether1
add action=drop chain=forward comment="Drop incoming from internet which is not public
    IP" in-interface=ether1 src-address-list=not_in_internet
```

IPv4 firewall: Protect the Inside network

```
add action=drop chain=forward comment="Drop packets from Inside that do not have Inside
    IP" in-interface=ether2 src-address-list=!Inside
add action=drop chain=forward comment="Drop packets from Inside that do not have Inside
    IP" in-interface=ether3 src-address-list=!Inside
add action=drop chain=forward comment="Drop packets from Inside that do not have Inside
    IP" in-interface=ether4 src-address-list=!Inside

/ip firewall address-list
  add address=192.168.10.0/24 list=Inside
    add address=192.168.20.0/24 list=Inside
  add address=192.168.30.0/24 list=Inside
```

IPv4 firewall: Protect the Inside network

```
/ip firewall address-list
   add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet
   add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet
   add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet
   add address=10.0.0.0/8 comment=RFC6890 list=not_in_internet
   add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
   add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
   add address=224.0.0.0/4 comment=Multicast list=not_in_internet
   add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet
   add address=192.0.0.0/24 comment=RFC6890 list=not_in_internet
   add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
   add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet
   add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
   add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet
   add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet
   add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]" list=not_in_internet
```

*** Modify to meet the requirement

IPv4 firewall: Protect the Server/DMZ

```
WEB-SERVER IP =192.168.10.10

/ip firewall nat
add action=dst-nat chain=dstnat comment=WEB-SERVER dst
   address=100.1.11.2 dst-port=80 in-interface=ether1
 protocol=tcp to-addresses=192.168.10.10 to-ports=80

/ip firewall filter
add action=jump chain=forward comment=WEB-SERVER dst-
   address=192.168.10.10 jump-target=WEB-SERVER
……
add action=accept chain=WEB-SERVER comment=WEB dst-port=80
   protocol=tcp
add action=accept chain=WEB-SERVER comment="accept ssh from NOC" dst-
   port=22 protocol=tcp src-address-list=Management
add action=drop chain=WEB-SERVER comment=DROP
```

More Firewall rules

- https://wiki.mikrotik.com/wiki/Firewall
- SynFlood
- ICMP Flood
- Port Scanner
- Email Spam
- L7 Filter
- DoS attack protection
- Etc.

Recommendation

- Disable unused ports and services on router
- Strong password policy for router users and allow to remote from specific network
- Disable discovery interfaces on outside/WAN ports
- Clock should be accurate synchronize
- Enable SysLog and SNMP for monitoring the router
- Separate network for each LAN and Server
- Used Address list to group all address for used in FW

Recommendation

- Used Action=Jump to organized the FW rules and better performance
- Used FW to protect router itself, inside network and the Servers

Reference

- wiki.mikrotik.com

Question?

Thanks for your Attention ☺

- Upcoming Training: http://ppic-training.com/upcoming-courses/
- Email: info@ppic-training.com
- Facebook: www.facebook.com/PhnomPenhInformaticsCenter

- Mobiel: 077/087 616102
- Please subscribe to our mailing list to receive all update information such as discount and promotion price