Most Common Mistake on MikroTik configuration

Paul Darius

MikroTik User Meeting
Kuala Lumpur – Malaysia
June 12, 2019

About me

Name: Paul Darius

MikroTik Certification :

- MTCNA (2011)
- MTCTCE
- MTCUME
- MTCRE
- MTCINE
- MTCWE
- MTCSE
- TRAINER (TR0606)

Work :

- Company: ATS / Asia Teknologi Solusi
- Assignment: NOC

MikroTik Certified Consultant

Padang to Kuala Lumpur

West Sumatra

About ATS

- PT Asia Teknologi Solusi
- Established since 1998
- Data center since 2006
- Internet Service Provider since 2014
- Coverage area:
  - East Tangerang
  - Jakarta
  - North Depok
  - Bekasi
  - Kerawang
  - Purwakarta
- MikroTik Training Center

ATS Coverage Area

ATS Services

- Dedicated Internet Connection
- Broadband Internet Connection
- Interconnection
- Local-loop
- Server Hosting / Colocation
- WEB & Email hosting
- Managed Services
- Etc.

How to reach us ?

- Asia Teknologi Solusi
  Sentra Niaga Blok N-17
  Green Lake City, Duri Kosambi
  West Jakarta – 11750 – Indonesia
- Phone: (62-21) 225 242 012
- Homepage : https://www.ats-com.net
- email sales@ats-com.net

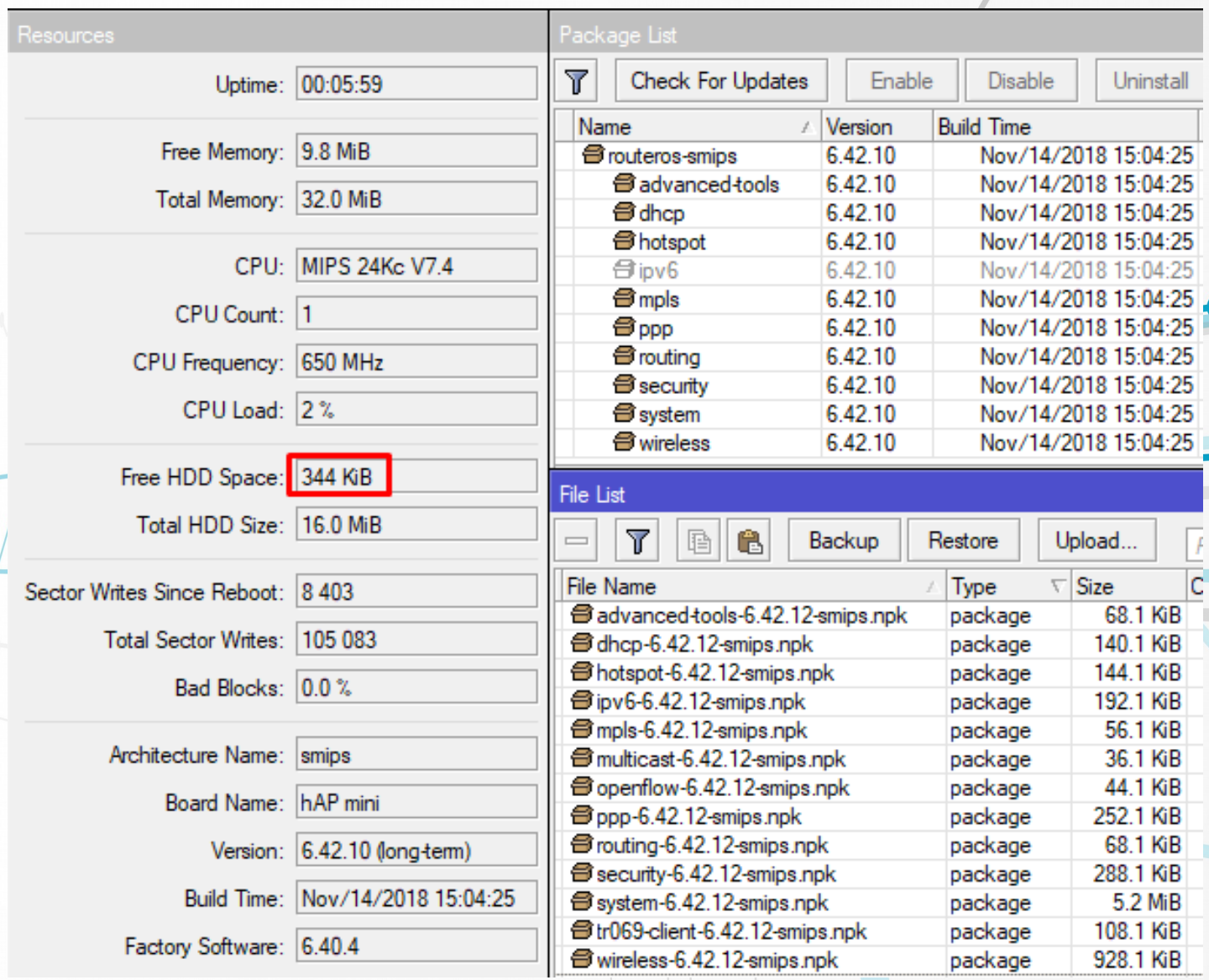
Objective

- To help you understand and diagnose most common RouterOS configurations issues
- Show the proper application of RouterOS features to avoid configurations issues
- Encourage you to use latest RouterOS versions and newest features

Presentation Material

- This presentation will consist of the most popular problems compiled sent to mikrotik forum discussion and groups.
- Examples are compressed / combined / simplified for presentation purposes
- The presentation will show configuration issues and improved configuration

NAND router FULL



Problem Analysis

- Problem:
  - NAND on the router FULL and an error message appears on the LOG router
- Diagnosis:
  - “System Resouce” show Free Space about 0.5MB
  - “System Package” show almost all package installed even if never been used.
- Reson:
  - Packages that do not use (although have been disabled) still need space on the NAND router

Package Management

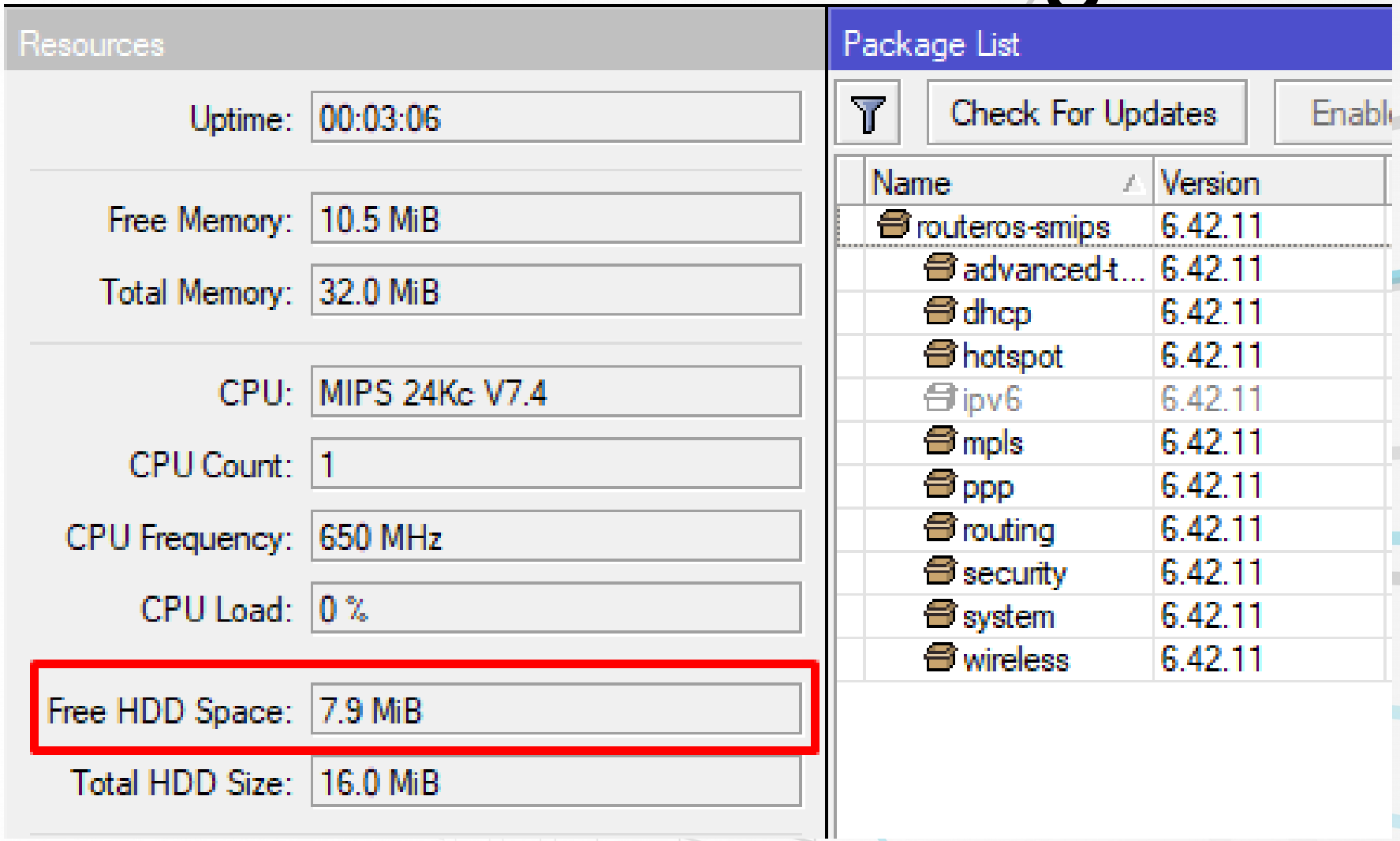
Paket	Fungsi
advance-tool	Advanced ping tools, Netwatch, ip-scan, SMS tool, Wake-on-LAN
calea	Communications Assistance for Law Enforcement Act
dhcp	Dynamic Host Control Protocol client and server
hotspot	HotSpot captive portal server for user management
ipv6	IPv6 addressing support
mpls	Multi Protocol Labels Switching support, Traffic engineering
ntp	Network protocol server
ppp	PPP, PPTP, L2TP, PPPoE, PPP servers and clients
routing	Dynamic routing: RIP, BGP, OSPF
security	Secure WinBox, SSH, IPsec
system	Basic features: static routing, firewall, bridging, etc.
wireless	802.11 a/b/g/n/ac support, CAPsMAN v2
user-manager	User Manager support

Correct Implementation

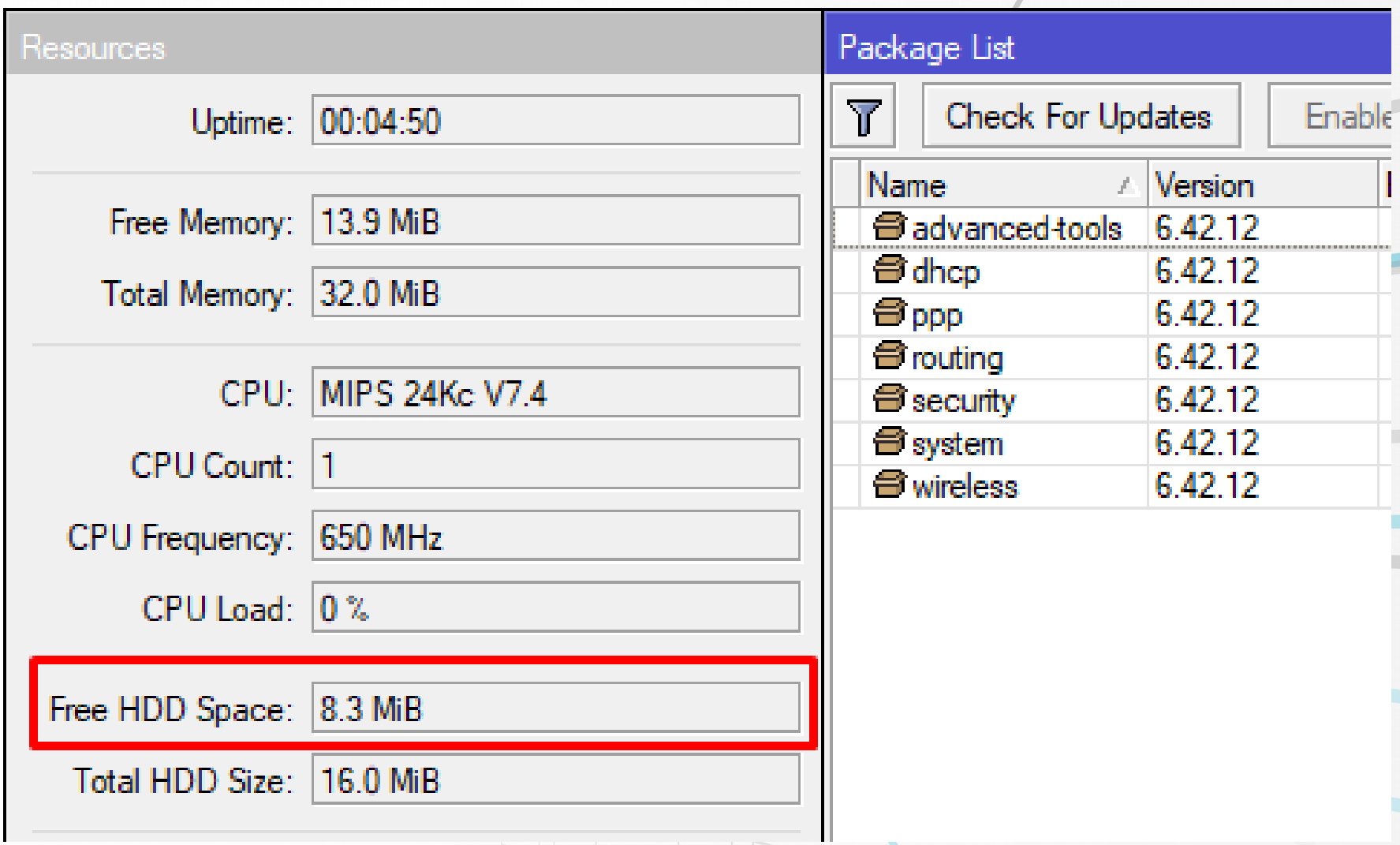
- Remove unneeded packages like calea, gps, ipv6, mpls, ntp, openflow, tr069, and other packages that are likely not to be used.
- Don't use bundled packages like:
  - routeros-mipsbe-6.42.12.npk
  - routeros-smips-6.42.12.npk
  - routeros-mmips-6.42.12.npk
  - routeros-ppc-6.42.12.npk
  - routeros-tile-6.42.12.npk
  - routeros-arm-6.42.12.npk
  - routeros-x86-6.42.12.npk

  Because the individual packages that are included in the above bundled package cannot be deleted, they can only be disabled so that it still occupies space in storage / NAND
- It strongly recommend that you use an Extra Package because we can add and or delete each individual package that we use.

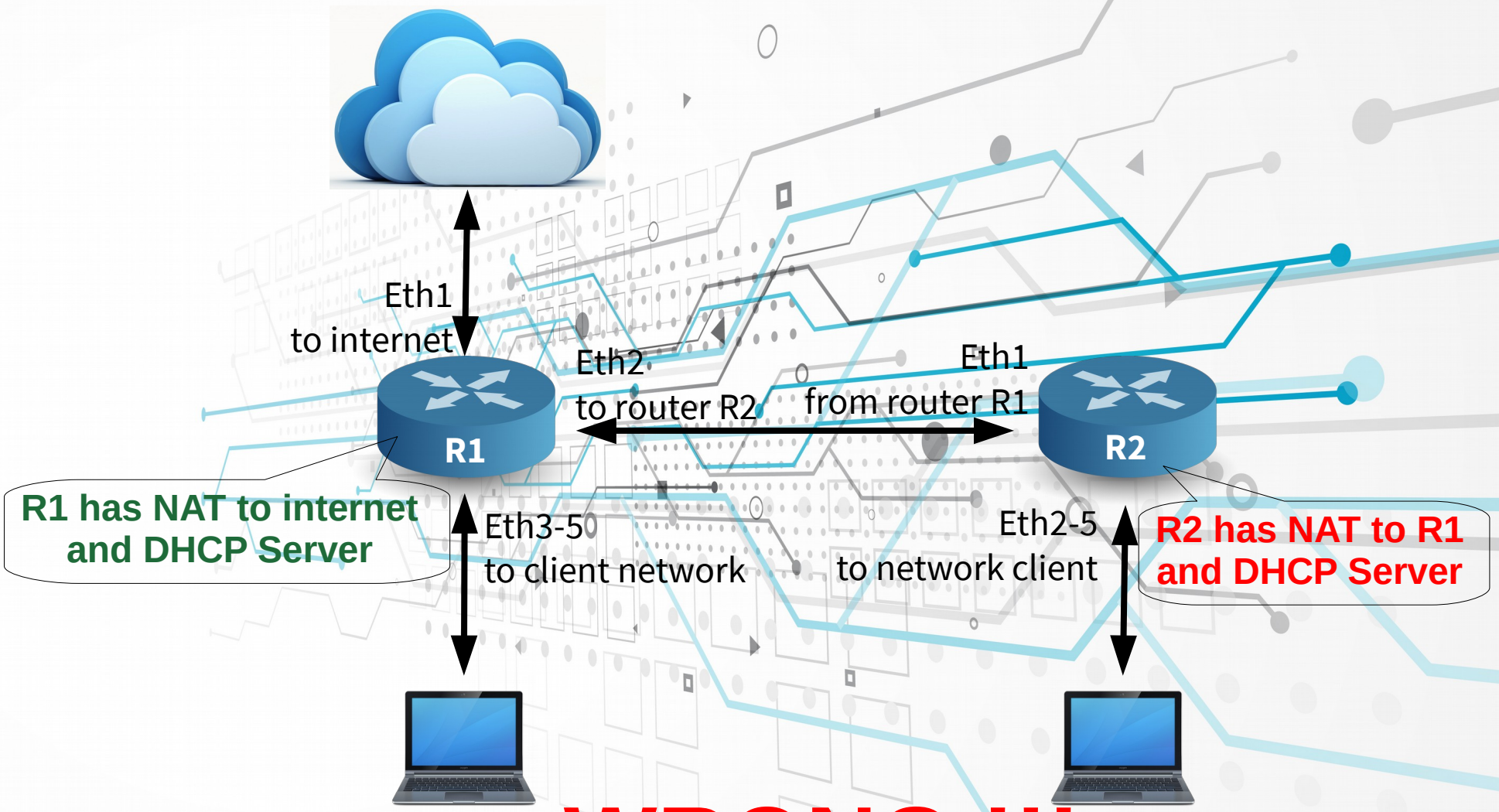
Bundled Package



Extra Package



Double or Triple NAT



WRONG !!!

Problem Analysis

- Computer that connected to R1 will not be able to do P2P communicatin to computer that connected to R2
- Separate DHCP server between R1 and R2
- Cannot be a firewall on R1 for computers connected to R1 and R2; unless the same firewall are installed again on R2. So it's double effort.

Correct Impelementation

- Take-out ether2 on R1 from bridge
- Alocate P2P ip address from ether2 @ R1 to ether1 @ R2
- Put static routing from R1 to R2
- Add DHCP-Relay from R1 to R2 so DHCP Lease at R1 will contain all leased both on R1 and R2
- The firewall configuration is only on R1.

Wireless

/interface wireless

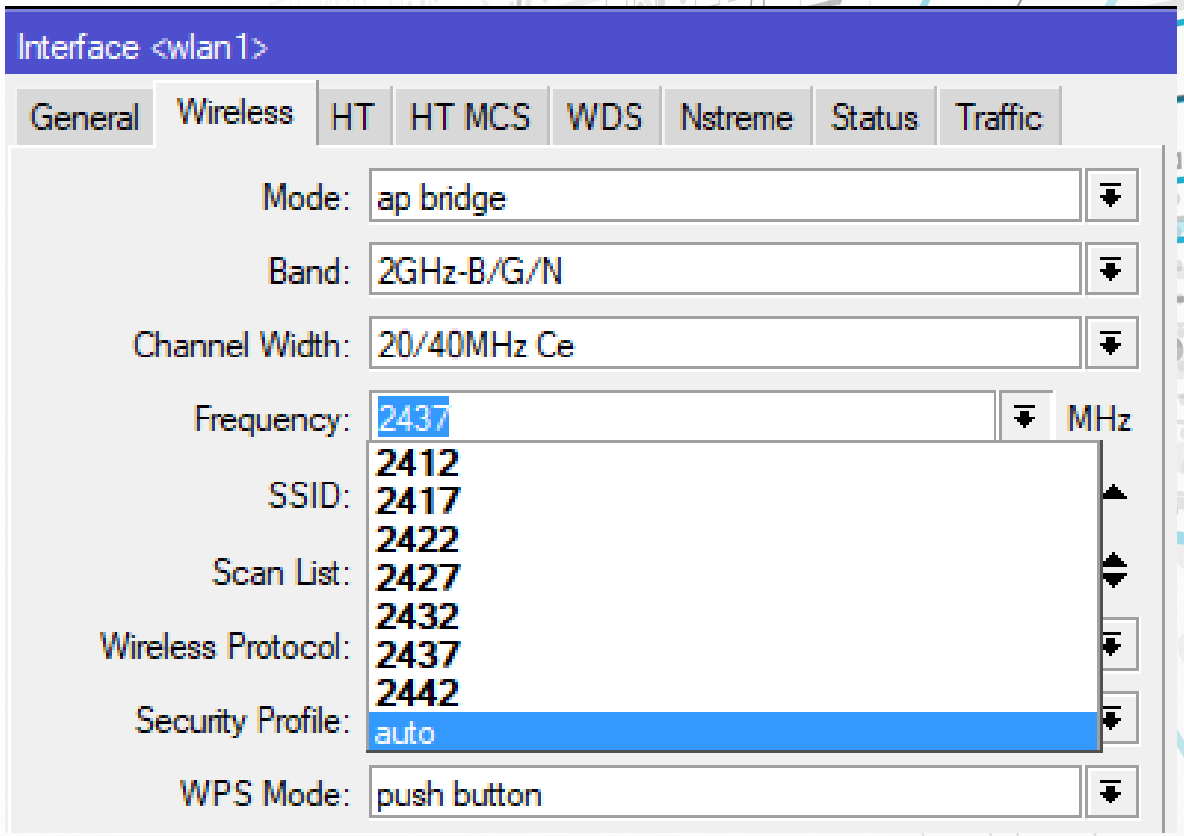
set [find default-name=wlan1] mode=ap-bridge band=2ghz-b/g/n \
channel-width=20/40mhz-Ce frequency=2437 ssid=Office

Apakah ada yang salah dengan configurasi di atas ???

WRONG !!!

Problem Analisys (1)

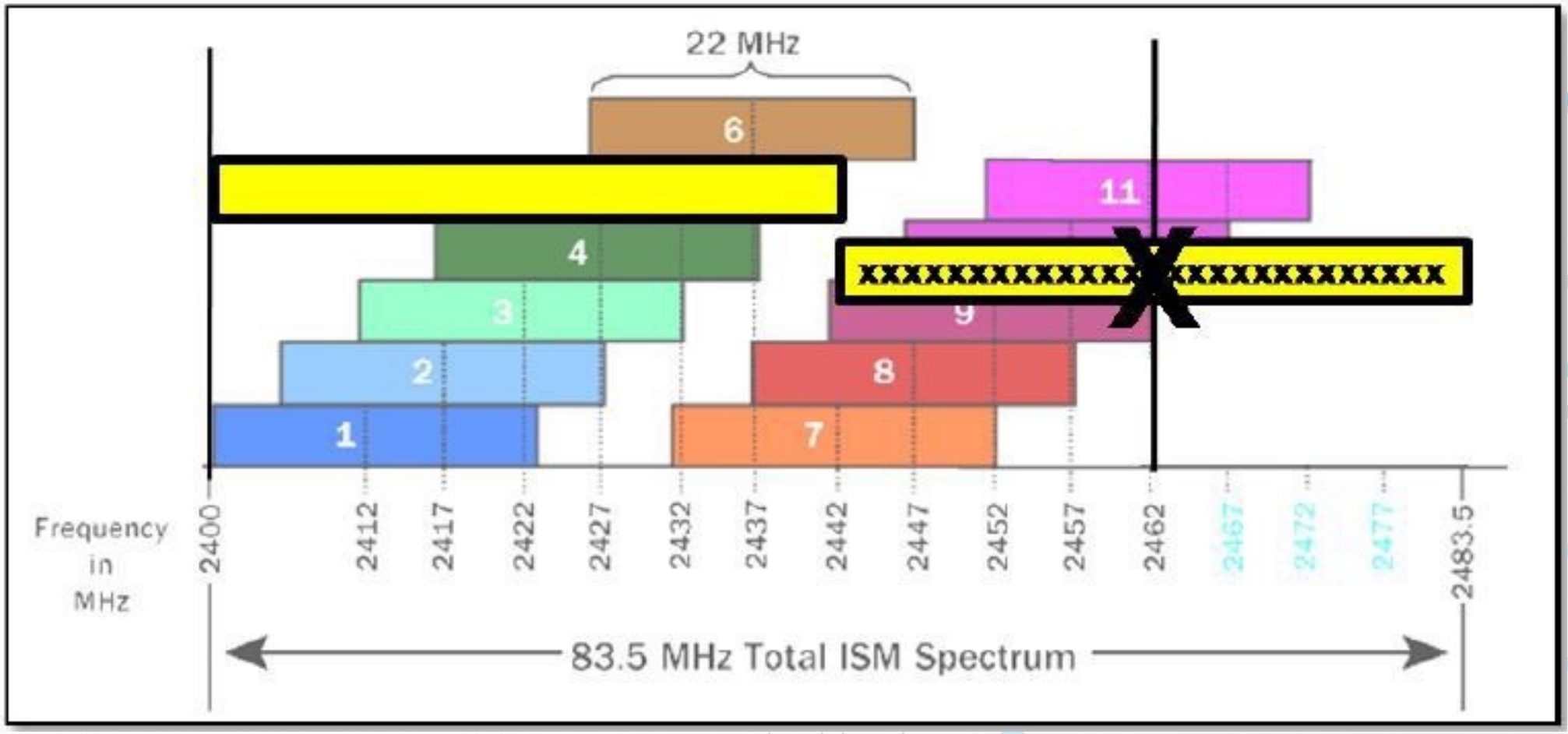
- By using 20 / 40MHz band, the available channel are only 7; not 11.
- Most of the client devices does not support 40MHz band



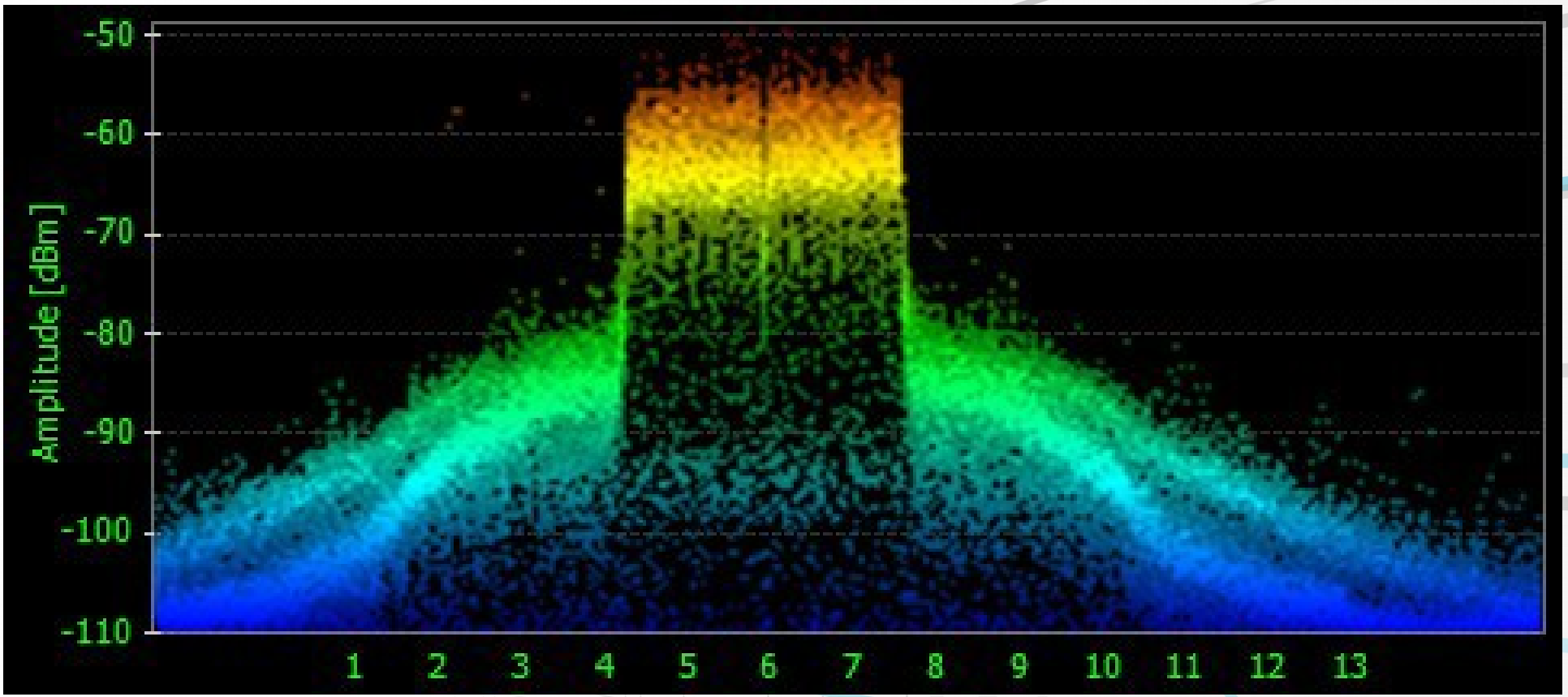
- If all clients use 40Mhz and then thre is one client connects with 20Mhz, then everyone will be 20Mhz

Problem Analisys (2)

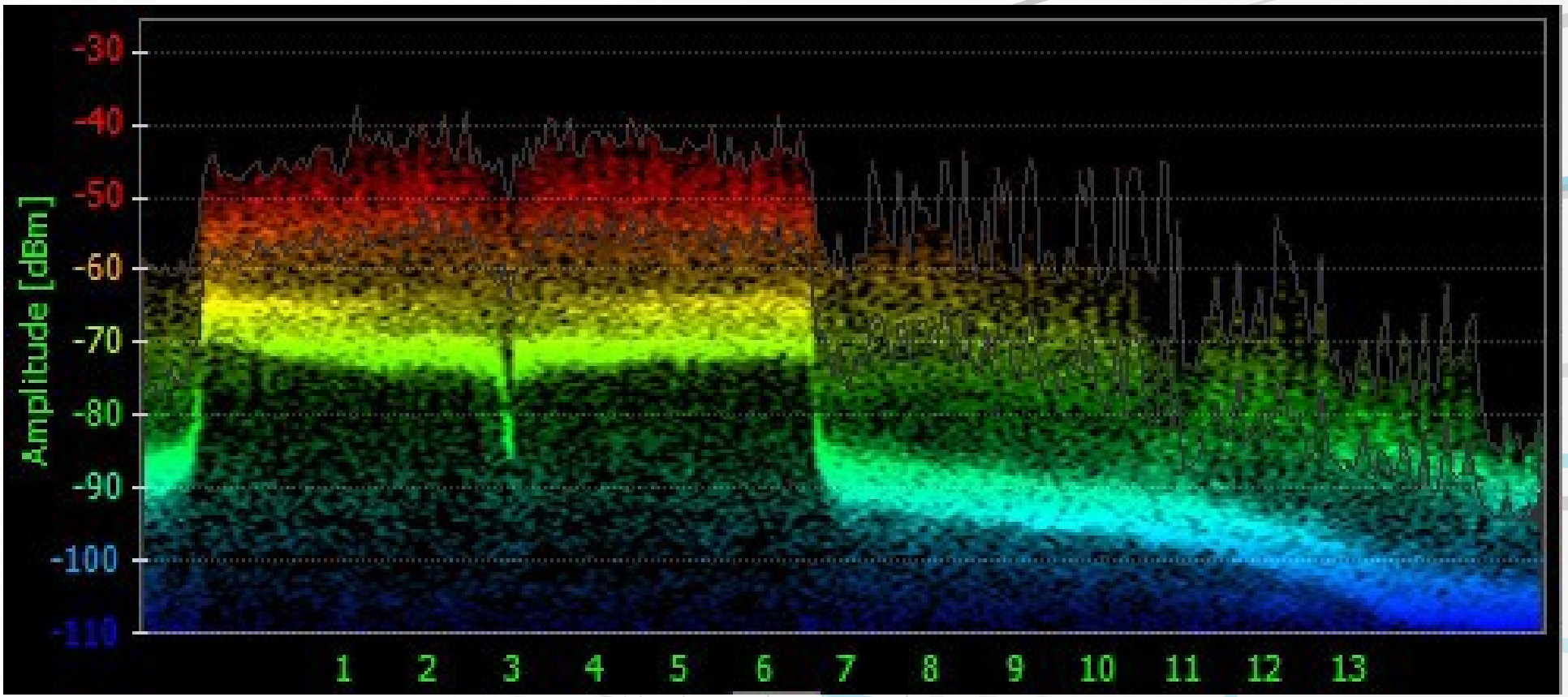
- By using 20 / 40Mhz then only 1 non overlapping channels available



Spectrum 20Mhz @ 2.4GHz



Spectrum 40Mhz @ 2.4GHz



Problem Analisys (3)

- Standard 802.11 wireless network uses CSMA / CA (Carrier-sense multiple access with collision avoidance)
- Standard wireless 802.11 b uses a 22Mhz channel width
- Standard wireless 802.11 a and 802.11 g use a of 20 MHz channel width
- Standard wireless 802.11 n standard uses a 20/40 Mhz channel width

Correct Implementation

```
/interface wireless

set [ find default-name=wlan1 ] mode=ap-bridge band=2ghz-g/n \
   channel-width=20mhz frequency=2437
```

- Use g-only atau g/n if the connected client device is not an old device from the early 2000s.
- Use channel-width 20mhz (disable extended channel on capsman) to get a better choice of non-overlapping channels.
- If the distance between APs is close enough, reduce tx-power to force the client to move AP.

L7 => High CPU Load

```
/ip firewall layer7-protocol
add name=youtube regexp="^.+(youtube).*\$"
add name=facebook regexp="^.+(facebook).*\$"
/ip firewall filter
add action=drop chain=forward layer7-protocol=facebook
add action=drop chain=forward layer7-protocol=youtube
```

WRONG !!!

Problem Analisys

- Problem:
  - High CPU load, increased latency, packet loss, jitter, youtube and facebook is not blocked
- Diagnosis:
  - “/tool profile” high layer7 load
- Reason:
  - Each connection is rechecked over and over again
  - Layer7 is checked in the wrong place and against all traffic

Layer 7

- Layer7-protocol is a method of searching for patterns in ICMP/ TCP/UDP streams
- On trigger Layer7 collects next 10 packets or 2KB of a connection and searches for the pattern in the collected data
- All Layer7 patterns available on the Internet are designed to work only for the first 10 packets or 2KB of a connection.

Correct Implementation

/ip firewall mangle

add action=mark-connection chain=prerouting protocol=udp dst-port=53 **connection-mark=no-mark** layer7-protocol=youtube **new-connection-mark**=youtube_conn passthrough=yes

add action=mark-packet chain=prerouting connectionmark=youtube_conn new-packet-mark=youtube_packet

/ip firewall filter
add action=drop chain=forward packet-mark=youtube_packet
add action=drop chain=input packet-mark=youtube_packet

(and do the same set for facebook and others)


Q&A

Wanna to reach me ?

- Email: paul@ranahminang.net
- Twitter: https://twitter.com/PaulDarius67
- Instagram https://www.instagram.com/prawir67

References

- Common MikroTik WiFi mistakes and how to avoid them by Ron Touw – MUM UK 2018
- Most underused and overused RouterOS tools and features by Janis Megis – MUM US 2017
- https://wiki.mikrotik.com