



Wireless Tools & Configuration



Certified Mikrotik Training Advance Wireless Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



Training Outline

- Wireless Tools
 - Scan
 - Frequency Usage
 - Spectral Scan/History
 - Snooper
 - Align
 - Sniffer
- Basic Configuration

Scan & Frequency Usage

- Kedua tool Scan dan Frequency Usage sama-sama menggunakan Scanlist untuk parameter range frequency yang digunakan.
- Interface menjadi terdisable jika menggunakan tool ini.
- Scan akan memperlihatkan AP mana saja yang aktif di sekitar perangkat.
- Frequency Usage menampilkan penggunaan atau load dari tiap frequency.

Scan

Scanner (Running)

Interface: wlan1

Start

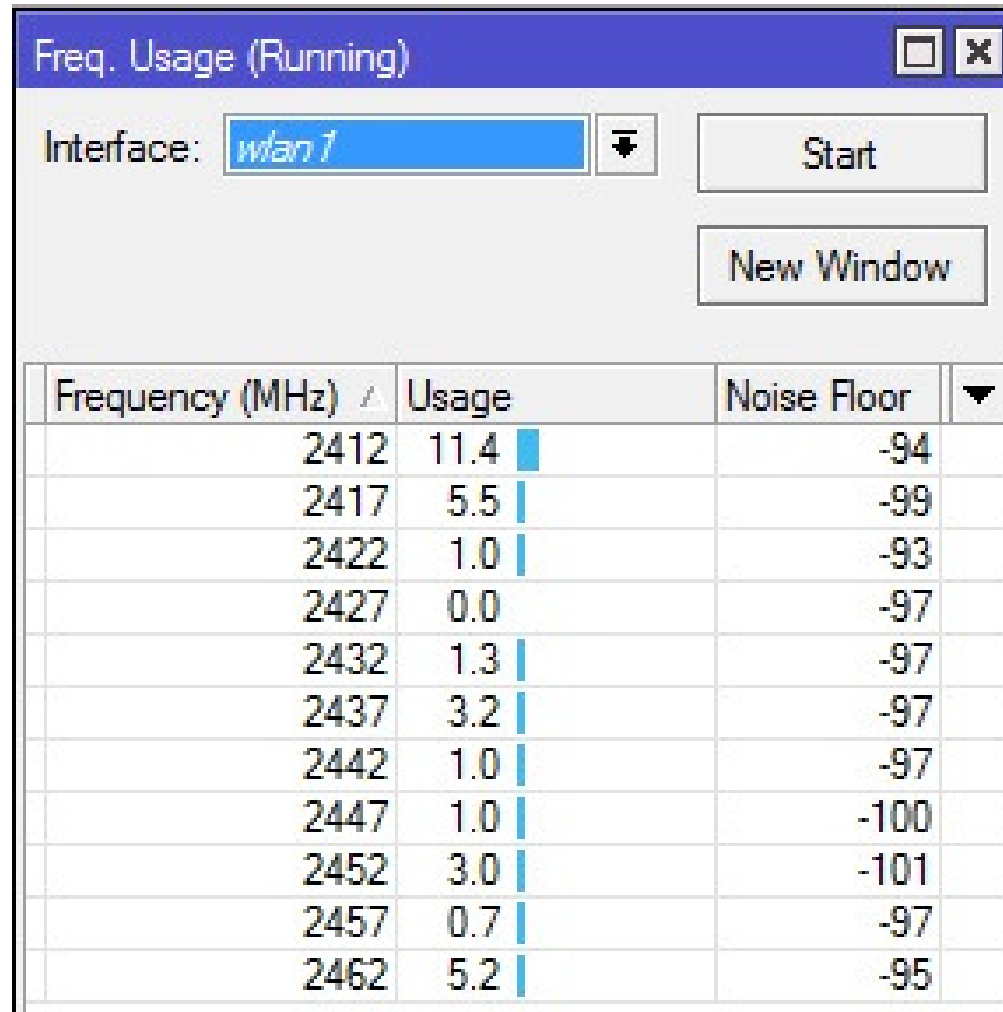
New Window

Connect

Use Network

| | Address | SSID | Band | Frequ... | Signal Strength | Noise Floor | Signal To Noise | Radio Name | Router(|
|-----|-------------------|---------------------|----------|----------|-----------------|-------------|-----------------|--------------|----------|
| ABR | 00:0C:42:23:C5:13 | Private | 2.4GHz-G | 2412 | -70 | -95 | 25 | 000C4223C513 | 5.0beta5 |
| ABR | 00:0C:42:68:8C:60 | RND-A1 | 2.4GHz-G | 2412 | -45 | -95 | 50 | 000C42688C60 | 4.10 |
| ABP | 02:0C:42:23:C5:14 | test2 | 2.4GHz-G | 2412 | -71 | -95 | 24 | 000C4223C513 | 5.0beta5 |
| ABP | 02:0C:42:23:C5:13 | | 2.4GHz-G | 2412 | -71 | -95 | 24 | 000C4223C513 | 5.0beta5 |
| ABP | 00:08:9F:0D:F1:54 | DW INDONESIA | 2.4GHz-G | 2412 | -82 | -95 | 13 | | |
| ABR | 00:0C:42:61:22:DF | tester | 2.4GHz-G | 2437 | -23 | -97 | 74 | 000C426122DF | 5.0beta5 |
| ABP | 00:25:9C:BB:62:89 | Linksys_Npn | 2.4GHz-G | 2437 | -90 | -97 | 7 | | |
| AP | A2:38:59:0E:38:C4 | aink | 2.4GHz-G | 2462 | -77 | -95 | 18 | | |
| ABP | 00:90:4C:91:00:01 | Sekretariat - APJII | 2.4GHz-G | 2462 | -68 | -95 | 27 | | |
| BR | 00:0C:42:61:1A:17 | Kipli23 | 2.4GHz-G | 2412 | -88 | -95 | 7 | 000C42611A17 | 4.3 |
| BR | 00:80:48:7F:CA:D0 | cctra | 2.4GHz-G | 2417 | -87 | -99 | 12 | 0080487FCAD0 | 3.28 |

Frequency Usage



Spectral Scan / History

- Tool ini hanya bisa digunakan di Chipset Atheros terbaru yaitu Atheros Merlin 802.11n wireless cards
- Range frequency yang ditampilkan
 - 2ghz, 5ghz, current-channel, range
- Value yang didapatkan
 - avg, avg-peak, interference, max, min
- Classify-samples (gangguan dari interferensi)
 - wifi, bluetooth, microwave-oven, etc



Spectral History

- Berbentuk Plot spectrogram.
- Perbedaan warna menunjukkan variasi dari power perangkat atau kekuatan signal.
- Terdapat opsi untuk menggunakan indikator Beep pada router untuk mendeskripsikan tiap baris hasil scan.
 - Nilai scan akan dibaca dari kiri ke kanan, semakin tinggi frequency suara menunjukkan nilai yang tinggi nilai scan pada spectrogram.

Spectral History

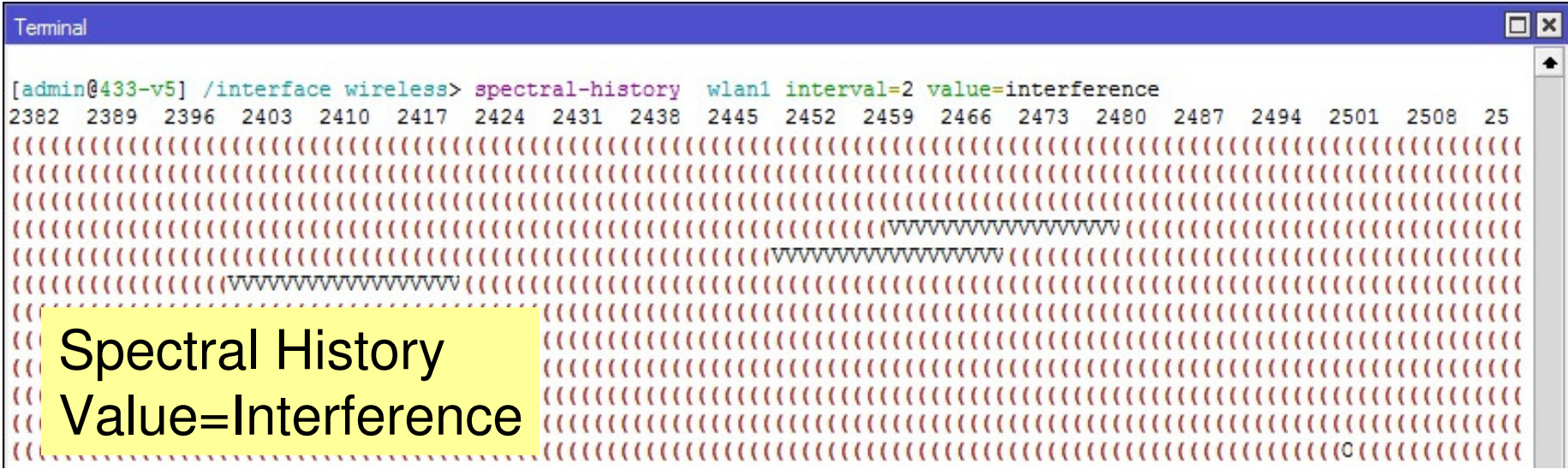
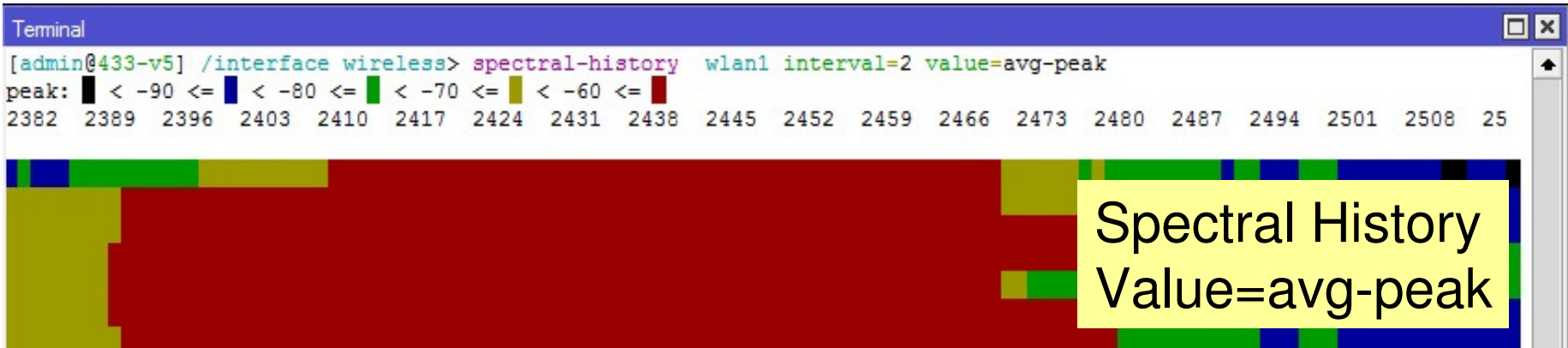




Spectral History

- Spectral History Command :
/interface wireless spectral-scan wlan1
- **Buckets** – lebar kolom tiap frequency
- **Duration** – durasi lama scanning
- **Audible** – opsi penggunaan beeper
- **Interval** – lama interfal menampilkan tiap baris hasil scan
- **Range** – pilihan range frequency yang akan di scan
 - 2.4ghz - scan whole 2.4ghz band
 - 5ghz - scan whole 5ghz band
 - current-channel - scan current channel only (20 or 40 mhz wide)
- **Samples** – sampling yang akan digunakan untuk menentukan nilai rata-rata pada saat melakukan scanning.
- **Value** – pilihan untuk menentukan tampilan dari plot spectogram

Spectral History





Spectral Scan

- Secara kontinu memonitor data spectral
- Setiap baris menampilkan data dari spectogram scan :
 - Frequency
 - Numeric value of power average
 - Character graphic bar
 - average power value - ':'
 - average peak hold - '.'
 - maximum lone floating - ':'
- Menampilkan opsi Interferensi lebih detail

Spectral Scan

```
Terminal
[admin@433-v5] /interface wireless> spectral-scan wlan1
FREQ DBM GRAPH
2386 -80 .....
2395 -61 .....
2404 -61 .....
2413 -60 .....
2422 -34 .....
2432 -18 .....
2441 -13 .....
2450 -22 .....
2459 -67 .....
2468 -67 .....
2477 -70 .....
2486 -78 .....
2495 -74 .....
2505 -73 .....
2514 -90 .....
└─ [Q quit|D dump|C-z pause|down]
```


Spectral Scan & Interference

```
Terminal
[admin@433-v5] /interface wireless> spectral-scan wlan1 show-interference=yes
FREQ INTERFERENCE      DBM  GRAPH
2386 none              -82  .....
2394 none              -80  .....
2403 none              -63  .....
2411 wifi:-78          -60  .....
2420 wifi:-78          -63  .....
2428 wifi:-78          -57  .....
2437 none              -64  .....
2446 none              -18  .....
2454 none              -39  .....
2463 none              -42  .....
2471 none              -67  .....
2480 none              -72  .....
2488 none              -80  .....
2497 none              -74  .....
2506 none              -84  .....
2514 none              -91  .....
-- [Q quit|D dump|C-z pause|down]
```

Spectral scan
Show-Interference=yes

Wireless Snooper Tool

- o Dengan menggunakan Snooper tool maka bisa diketahui load dan besar traffic tiap frekuensi.

```
Terminal
[admin@433-v5] /interface wireless snooper> snoop wlan1
BAND      FREQ      USE      BW          NET-COUNT NOISE-FLOOR STA-COUNT
2.4ghz-b/g 2412MHz 15.1% 116.0kbps 5          -96          7
2.4ghz-b/g 2417MHz 7.3%  59.7kbps  0          -99          0
2.4ghz-b/g 2422MHz 1.3%  9.7kbps  0          -94          1
2.4ghz-b/g 2427MHz 1.1%  9.6kbps  0          -97          0
2.4ghz-b/g 2432MHz 2.1%  14.3kbps 0          -97          0
2.4ghz-b/g 2437MHz 1.9%  15.8kbps 2          -97          2
2.4ghz-b/g 2442MHz 2.2%  10.1kbps 0          -97          0
2.4ghz-b/g 2447MHz 1.5%  6.9kbps  0          -100         0
2.4ghz-b/g 2452MHz 0.2%  1656bps  0          -101         0
2.4ghz-b/g 2457MHz 1.1%  4.7kbps  0          -98          0
2.4ghz-b/g 2462MHz 3%    24.0kbps 2          -97          4
- [Q quit|D dump|C-z pause|n networks|s stations]
```

Wireless Alignment

Alignment <wlan1> (running)

| | Address | SSID | Rx Qu... | Avg. Rx ... | Last Rx | Tx Qu... | Last Tx | Corre |
|---|-------------------|--------|----------|-------------|---------|----------|---------|-------|
| A | 00:0C:42:61:22:DF | tester | -27 | -25 | 0.03 | | 0.00 | |
| A | 00:0C:42:68:8C:60 | RND-A1 | -74 | -73 | 0.07 | | 0.00 | |
| | 00:19:7E:3B:D1:42 | | -49 | -49 | 16.57 | | 0.00 | |
| | 00:19:7E:3B:E4:13 | | -74 | -67 | 20.28 | | 0.00 | |
| | 00:19:7E:3B:E7:34 | | -60 | -54 | 0.20 | | 0.00 | |
| | 00:1A:73:BD:FA:44 | | -63 | -64 | 29.01 | | 0.00 | |
| | 00:22:66:81:C5:C3 | | -74 | -73 | 19.01 | | 0.00 | |
| | 0C:EE:E6:86:39:9F | | -67 | -67 | 21.01 | | 0.00 | |

Wireless Alignment Settings

Frame Size: 300

Active Mode

Receive All

Filter MAC Address: 00:00:00:00:00:00

SSID All

Frames per Second: 25

Audio Monitor: 00:00:00:00:00:00

Audio Min: -100

Audio Max: -20

OK

Cancel

Apply

Audio Monitor :

adalah opsi mac-address dari Perangkat sisi lawan untuk Dimonitor Menggunakan indikator audible beep

Wireless Sniffer

The image displays the Mikrotik Wireless Sniffer interface. The main window, titled "Sniffer <wlan 1>", shows various statistics and control buttons. The statistics include:

- Processed Packets: 0
- Memory Size: 0 B
- Memory Saved Packets: 0
- Memory Over Limit Packets: 0
- File Size: 0 B
- File Saved Packets: 0
- File Overlimit Packets: 0
- Stream Dropped Packets: 0
- Stream Sent Packets: 0
- File Limit: 0 KiB
- Memory Limit: 0 KiB

Control buttons include Start, Stop, Save, Set, and Pause. A "Sniffer Settings" dialog box is overlaid on the main window, showing the following configuration options:

- Multiple Channels
- Only Headers
- Receive Errors
- Channel Time: 00:00:00.20 s
- Memory Limit: 10 KiB
- File Name: [Empty field]
- File Limit: 10 KiB
- Streaming Enabled
- Streaming Server: 0.0.0.0
- Streaming Max. Rate: [Empty field] p/s

Buttons for OK, Cancel, and Apply are also visible in the dialog box.



Wireless Sniffer

- Dengan menggunakan wireless Sniffer maka bisa dilakukan sniffing packet data dari jaringan wireless.
 - **channel-time** – Berapa lama waktu yang digunakan untuk sniff tiap channel jika opsi “multiple channel” diaktifkan.
 - **file-limit** – Batas besar file yang akan digunakan untuk menyimpan data sniffer.
 - **file-name** – nama file yang akan digunakan untuk menyimpan data sniffer dan akan disimpan di storage Router (PCAP format).
 - **memory-limit** – besar memory yang akan digunakan untuk tool sniffer.

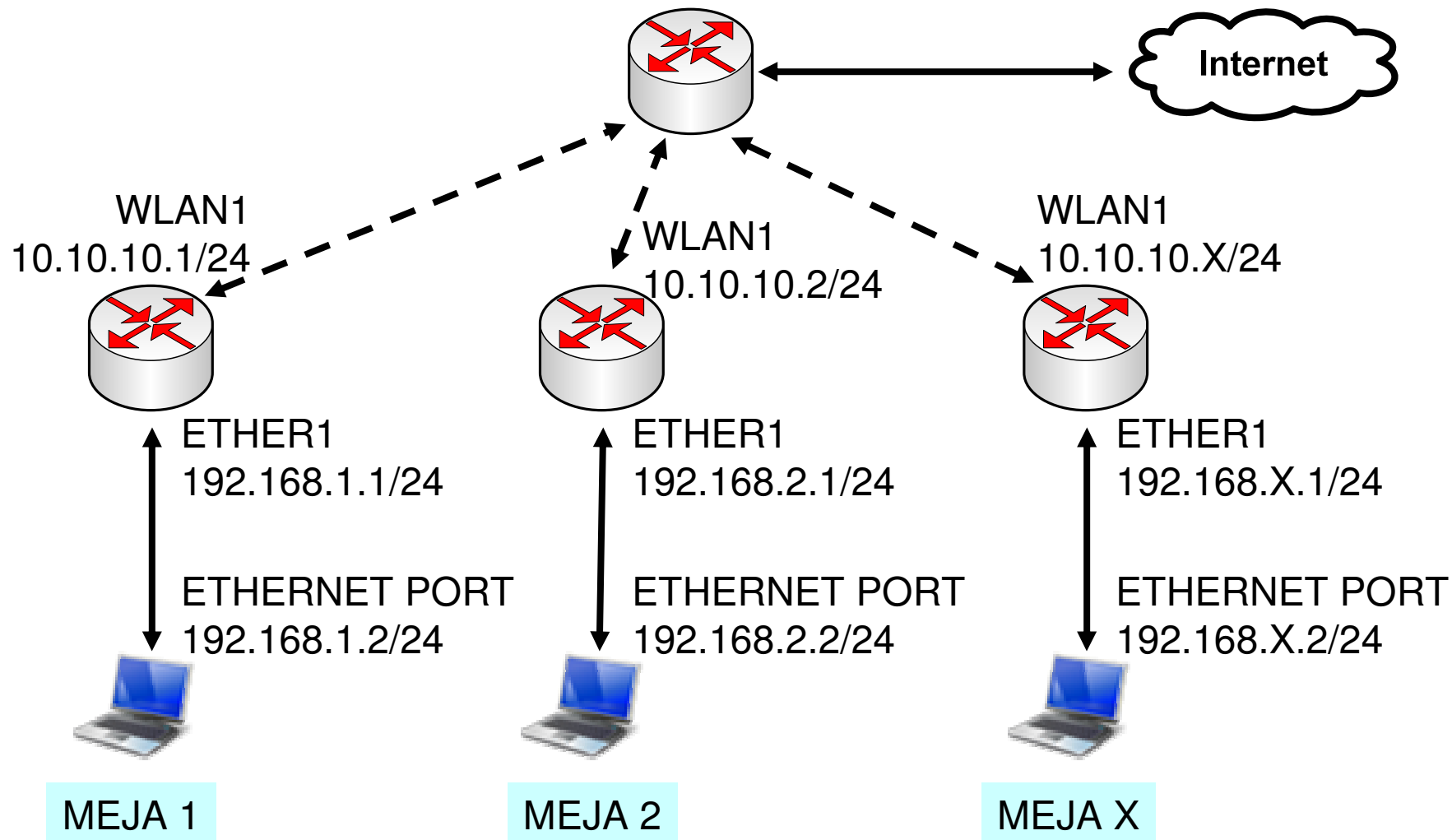
Wireless Sniffer

- **multiple-channels** – opsi jika ingin melakukan sniffing di multi channel atau tidak.
 - **no** - wireless sniffer sniffs only one channel in frequency that is configured in /interface wireless
 - **yes** - sniff in all channels that are listed in the scan-list in /interface wireless
- **only-headers** – opsi untuk melakukan sniffing terhadap seluruh paket data atau hanya paket header.
- **streaming-enabled** – opsi jika ingin melakukan pengiriman data sniffing ke sebuah server tertentu (TZSP format).
- **streaming-max-rate** – batas maksimal paket data (pps) yang akan diterima oleh router.
 - 0 - no packet per second limitation
- **streaming-server** – alamat ip dari server yang menerima data sniffing.

[LAB-1] Wireless Tools

- Aktifkan Wireless Router :
 - Lakukan scan dan snoop untuk mendapatkan gambaran dari kondisi wireless disekitar perangkat.
 - Scan / Snoop di band 2.4Ghz dan 5Ghz.
 - Gunakan Spectral Tool (Scan dan History) untuk mendapatkan gambaran lebih detail terhadap interferensi.
 - Aktifkan audible

• • • [LAB-2] Konfigurasi Dasar





IP Configuration

Lab-2 adalah sebuah simulasi konfigurasi dasar sebuah Router Mikrotik yang akan digunakan di jaringan local seperti warnet, office, kampus atau bahkan di RT/RW-NET

X = nomor peserta

Routerboard Setting

WAN IP : 10.10.10.x/24

Gateway : 10.10.10.100

LAN IP : 192.168.x.1/24

DNS : 10.100.100.1

Src-NAT and DNS Server

Laptop Setting

IP Address : 192.168.x.2/24

Gateway : 192.168.x.1

DNS : 192.168.x.1

Basic Configuration

- Parameter Untuk konfigurasi minimal
 - Mode
 - Band
 - Frequency
 - SSID
 - Scan-List

Interface <wlan1>

General Wireless HT WDS Nstreme Status ...

Mode: station

Band: 5GHz

Frequency: 5180 MHz

SSID: tester

Scan List:

Wireless Protocol: any

Security Profile: default

TDMA Period Size: 2 ms

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

Wireless Mode Station

- **Station modes:**
 - **station** – Mode Client paling sederhana
 - **station-wds** – mode station yang mengaktifkan WDS bridge
 - **station-pseudobridge** – mode station tetapi ditambahkan fungsi MAC translation sehingga interface wireless bisa dimasukkan ke dalam bridge.
 - **station-pseudobridge-clone** – mode station yang menggunakan fungsi station-bridge-clone-mac address



Wireless Mode Access Point

- **AP modes:**
 - **ap-bridge** – mode standard untuk Access Point.
 - **bridge** – sama seperti mode ap-bridge tetapi hanya menerima satu client.
 - **wds-slave** – mode ap-bridge tetapi mampu untuk melakukan scan terhadap AP yang memiliki SSID yang sama dan membangun WDS link ke AP tersebut. Jika terputus maka akan dilakukan scanning ulang dan akan terkoneksi kembali.



Wireless Mode – Special

- **Special modes:**
 - **alignment-only** – mengaktifkan mode align transmit untuk digunakan sebagai membantu pointing antenna.
 - **nstreme-dual-slave** – digunakan jika ingin menggunakan Dual-Nstreme

Wireless Band – 2.4Ghz

- **band** – Opsi untuk menentukan standard wireless yang ingin digunakan
 - **2.4ghz-b** – menggunakan standard IEEE 802.11b
 - **2.4ghz-b/g** - IEEE 802.11g (supports also legacy IEEE 802.11b protocol).
 - **2.4ghz-g-turbo** - IEEE 802.11g menggunakan double channel yang kecepatan teoritisnya adalah hingga 108 Mbit.
 - **2.4ghz-onlyg** – hanya menggunakan standard IEEE 802.11g
 - **2ghz-10mhz** – variasi dari IEEE 802.11g dengan menggunakan setengah dari lebar band standard (air rate of up to 27Mbit)
 - **2ghz-5mhz** - variasi dari IEEE 802.11g dengan menggunakan seperempat dari lebar band standard (air rate of up to 13.5Mbit)

Wireless Band – 5Ghz

- **5ghz** – menggunakan standard IEEE 802.11a 54 Mbit
 - **5ghz-turbo** - IEEE 802.11a menggunakan double channel yang kecepatan teoritisnya adalah hingga 108 Mbit.
 - **5ghz-10mhz** - variasi dari IEEE 802.11a dengan menggunakan setengah dari lebar band standard (air rate of up to 27Mbit)
 - **5ghz-5mhz** - variasi dari IEEE 802.11a dengan menggunakan seperempat dari lebar band standard (air rate of up to 13.5Mbit)

Frequency, SSID & Scan-List

- **frequency** – Frequency yang digunakan untuk AP. Parameter ini akan diabaikan jika pada perangkat diaktifkan mode “client”.
- **ssid** (text) – Sebagai identitas dari jaringan wireless.
- **scan-list** – nilai default adalah channel ISM (standard channel) sesuai dengan band yang digunakan. Scan list bisa berupa range, list dari channel yang dipisahkan dengan tanda comma atau bisa juga gabungan dari keduanya.
 - Example: **scan-list=default,2222,2312-2362**
 - Dari scan list tersebut perangkat akan melakukan scan di default channel dan beberapa range frequency custom.
 - Penggunaan custom channel bergantung dari setting “**channel-mode**”

Default TX & RX Limit

- **default-ap-tx-limit** (integer; default: 0) – adalah limit traffic rate untuk pengiriman data dari AP ke tiap client (bps).
 - 0 – berarti tanpa limit
- **default-client-tx-limit** (integer; default: 0) – adalah limit traffic rate untuk pengiriman data dari tiap client ke AP (bps). Hanya bekerja jika client sama-sama menggunakan mikrotik.
 - 0 – berarti tanpa limit

Interface <wlan1>

General Wireless HT WDS Nstreme Status ...

Mode: station

Band: 5GHz

Frequency: 5180 MHz

SSID: tester

Scan List:

Wireless Protocol: any

Security Profile: default

TDMA Period Size: 2 ms

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

Default Authenticate & Forward

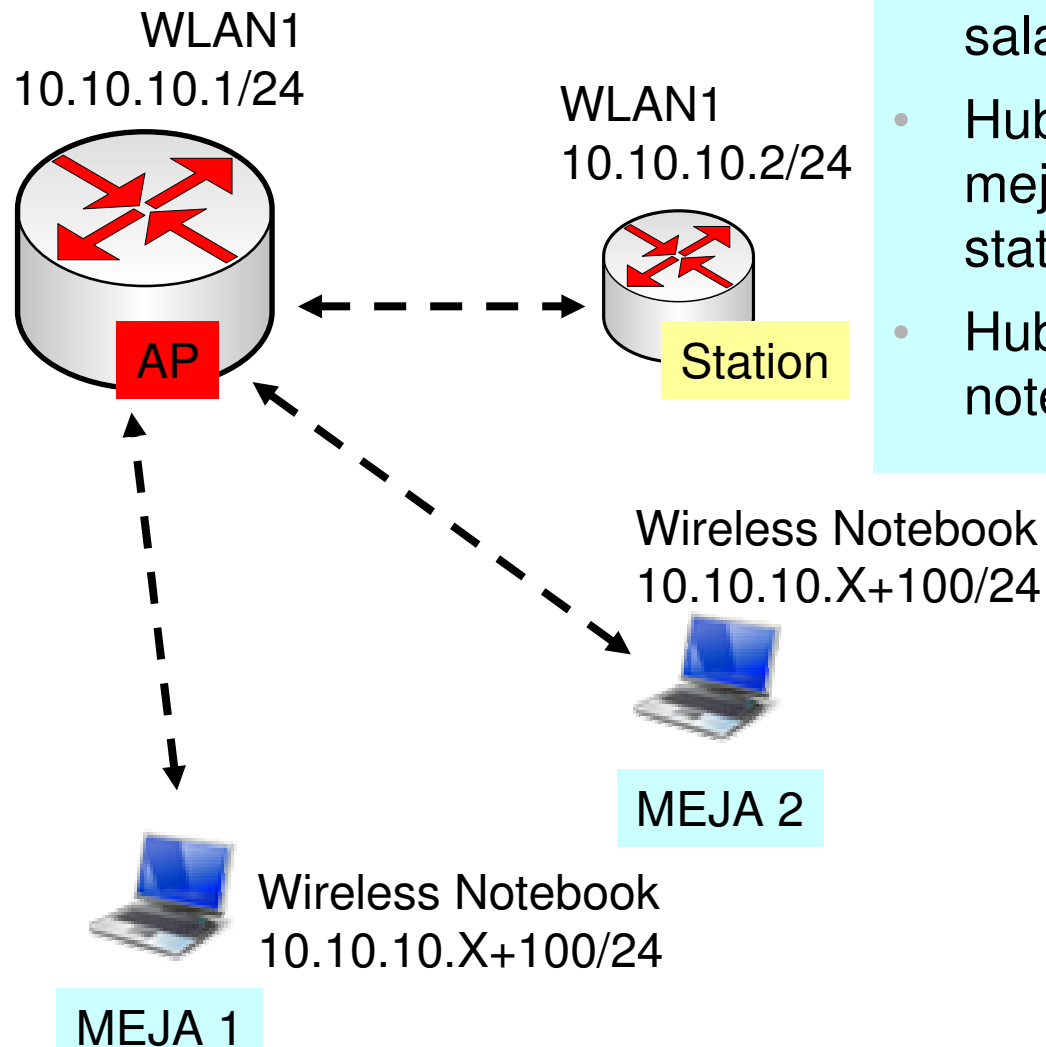
- **default-authentication** (default value: yes) :
 - Jika digunakan mode AP maka semua client yang tidak dibatasi di **access-list** akan diautentikasi dan bisa terkoneksi.
 - Jika digunakan di mode station maka wireless bisa terkoneksi ke AP manapun yang tidak dibatasi di **connect-list**.
- **default-forwarding** (default value: yes) :
 - Adalah parameter yang digunakan untuk forwarding traffic dari client ke client yang lain dalam AP yang sama. Bisa dibatasi lebih spesifik per clientnya di access-list.



Hide SSID

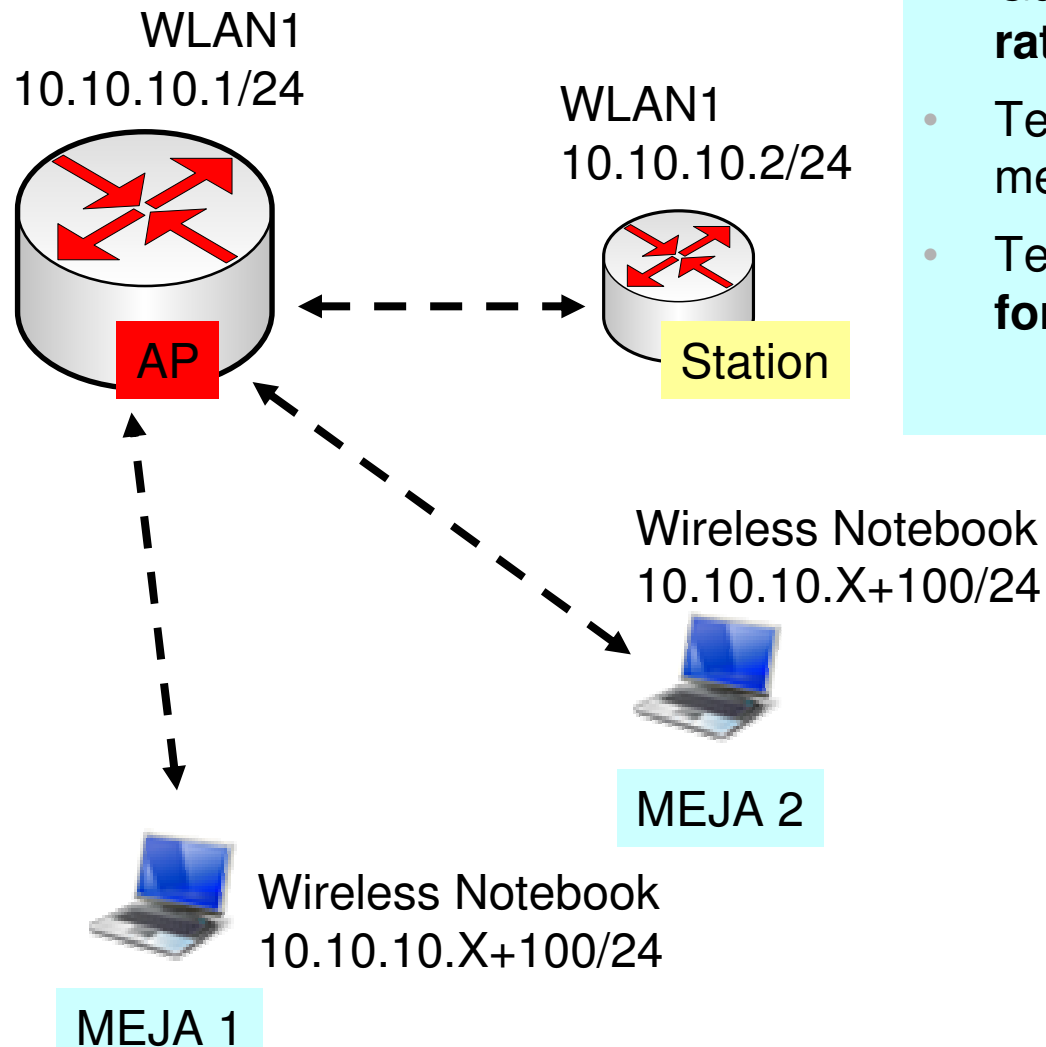
- **hide-ssid** (default value: no) :
 - **yes** – jika diaktifkan maka AP tidak akan memasukkan informasi SSID pada beacon frame dan tidak akan memberikan frame balasan berisi informasi SSID jika ada permintaan informasi SSID.
 - **no** – AP akan memasukkan informasi SSID pada frame beacon dan akan memberikan informasi SSID jika ada permintaan informasi SSID.
- Setting ini hanya berpengaruh jika menggunakan mode AP, sebenarnya tidak berpengaruh banyak pada security karena informasi SSID tetap dimasukkan pada frame yang lain (bukan beacon frame).

[LAB-3] Wireless Setup



- Aktifkan mode ap-bridge pada salah satu router (Router meja1).
- Hubungkan router kedua (Router meja 2) menggunakan mode station.
- Hubungkan juga wireless tiap notebook untuk terkoneksi ke AP.

[LAB-4] Wireless Limit



- Gunakan parameter **default ap tx rate** dan **default client tx rate**.
- Test performancinya menggunakan bandwidth test.
- Test traffic antar client jika **default forward** di non-aktifkan.