10 Wireless Network

- Беспроводные сети обладают гибкостью при конфигурации и расширении. Могут служить как добавлением, так и заменой проводных сетей при построении сетевой инфраструктуры
- Пользователи могут свободно перемещаться, т.к. беспроводные сети обеспечивают доступ к сетевым ресурсам компании из любого места.
- Беспроводные сети не только обеспечивают мобильный доступ, но и сами мобильны, т.к. можно легко переместить сеть в другое место. Быстрая и лёгкая инсталляция.

Сферы применения беспроводных сетей

- Сети провайдеров Интернет
- Расширение сети провайдеров Интернет: подключение клиентов там, где нет возможности протянуть кабель
- Внутриофисные сети (+гостевой доступ)
- Домашние сети
- Выставочные комплексы и конференц-залы
- Доступ к Интернет в гостиницах, кафе, библиотеках, аэропортах, парках и т.д. (Hot Spot)
- и т.д.

Семейство стандартов беспроводных сетей IEEE 802.11

Стандарт IEEE 802.11 входит в серию стандартов IEEE 802.X, относящихся к сетям и коммуникациям, сюда также входят такие стандарты, как 802.3 Ethernet, 802.5 Token Ring и т.д.

Таким образом, стандарт IEEE 802.11 определяет компоненты и характеристики сети на физическом уровне передачи данных и на уровне доступа к среде с учетом беспроводного способа передачи данных и возможности взаимодействия с существующими сетями.

Семейство стандартов беспроводных сетей IEEE 802.11

IEEE 802.11 – канальная скорость до 2Мбит/с (2,4 Ггц, 1997г)
IEEE 802.11a – канальная скорость до 54Мбит/с (5 Ггц, 1999г)
IEEE 802.11b – канальная скорость до 11Мбит/с (2,4 Ггц, 1999г)
IEEE 802.11g – канальная скорость до 54Мбит/с (2,4 Ггц, 2003г)
IEEE 802.11n – канальная скорость до 300Мбит/с (2,4 Ггц и 5Ггц, 2009г)

IEEE 802.11b+
IEEE 802.11G Turbo (Super) – канальная скорость до 108Мбит/с

MikroTik - Nstream
MikroTik - Nstream Dual

Стандарты беспроводных сетей - IEEE 802.11b

- Распространенный стандарт, совместим с предыдущим стандартом IEEE 802.11
- Работает на частоте 2,4 ГГц
- Используется метод прямой последовательности с разнесением сигнала по широкому диапазону (DSSS)
- Поддерживает скорость соединения 1, 2, 5.5, **11 Мбит/с** (**реальная скорость передачи данных от 4 до 6 Мбит/с**), автоматический или фиксированный выбор скорости
- Защита данных при помощи шифрования WEP

Стандарты беспроводных сетей - IEEE 802.11a

- Более сложная передовая технология
- Работает на частоте 5 ГГц
- Используется метод мультиплексирования с ортогональным делением частот (OFDM)
- Поддерживает скорость соединения до **54 Мбит/с** (48, 36, 24, 18, 12, 9 и 6 Мбит/с), **реальная скорость передачи данных от 20 - 24 Мбит/с**
- 12 одновременно доступных для работы каналов
- Защита данных при помощи шифрования WEP,WPA,802.1x

Стандарты беспроводных сетей - IEEE 802.11g

- Обратная совместимость с устройствами стандарта IEEE 802.11b
- Работает на частоте 2.4 ГГц
- Используется метод прямой последовательности с разнесением сигнала по широкому диапазону (DSSS) и метод мультиплексирования с ортогональным делением частот (OFDM)
- Скорость соединения до **54 Мбит/с**, реальная скорость передачи данных от **20 - 24 Мбит/с**
- автоматический или фиксированный выбор скорости
- Защита данных при помощи WPA (Wi Fi Protected Access), 802.1x

802.11n

Особенности стандарта

- Возможность использования двух диапазонов – 2,4 Гц или 5 ГГц;
- Возможность использования каналов с шириной 20 и 40МГц;
- Обратная совместимость с предыдущими стандартами WiFi при работе с модуляциями CCK и OFDM в канале шириной 20МГц;

Преимущества 802.11n

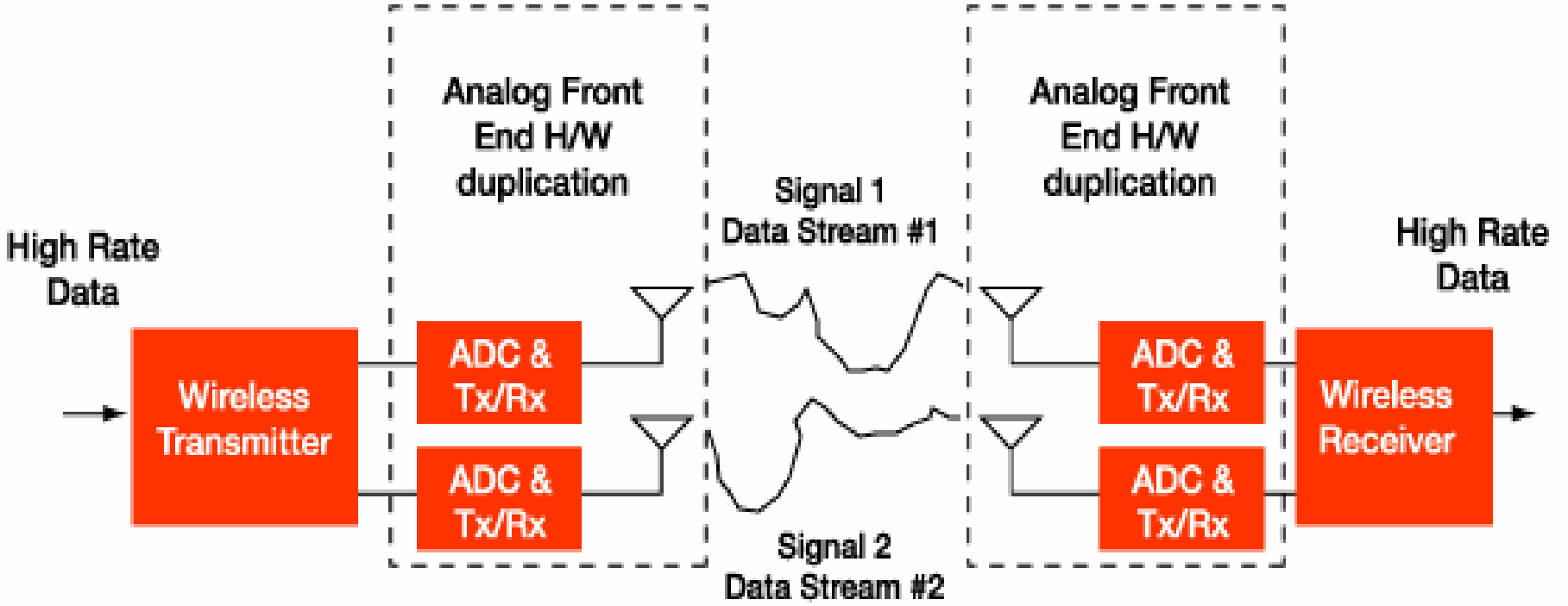
a. Высокий уровень безопасности
b. Поддержка 2x диапазонов (2.4GHz и 5GHz)
c. Меньше подвержен помехам
d. Использование MIMO повышает скорость передачи данных

Maximum Theoretical Application-Level Throughput *

	Modulation	Maximum Link Rate	Maximum TCP Rate	Maximum UDP Rate
802.11b	CCK	11Mbps	5,9Mbps	7,1Mbps
802.11g (with 11b)	OFDM/CCK	54Mbps	14,4Mbps	19,5Mbps
802.11g (11g-only mode)	OFDM/CCK	54Mbps	24,4Mbps	30,5Mbps
802.11a	OFDM	54Mbps	24,4Mbps	30,5Mbps
802.11a TURBO™	OFDM	108Mbps	42,9Mbps	54,8Mbps

* По данным компании Atheros™ Communications

Технология MIMO



Скорость

Более высокая скорость улучшает пропускную способность

Более низкая скорость увеличивает дистанцию и надежность

Автоматический или фиксированный выбор скорости

REC7003E

Regulatory parameters related to Annex 3

	Frequency Band	Power	Duty cycle	Channel spacing	ECC/ERC Decision	Notes
a	2400.0-2483.5 MHz	100 mW e.i.r.p.	No Restriction	No spacing	ERC/DEC/(01)07	For wide band modulations other then FHSS (e.g. DSSS, OFDM, ..), the maximum e.i.r.p. density is limited to 10 mW/1 MHz
b	5150 -5250 MHz	200 mW Max mean	No Restriction		ECC/DEC/(04)08	Restricted to indoor use. The maximum mean e.i.r.p. density shall b limited to 0.25 mW/25 kHz in any 25 kHz band.
c	5250 – 5350 MHz	200 mW Max mean	No Restriction		ECC/DEC/(04)08	Restricted to indoor use. The maximum mean e.i.r.p. density shall b limited to 10 mW/MHz in any 1 MHz band
d	5470 – 5725 MHz	1 W Max mean	No Restriction		ECC/DEC/(04)08	Indoor as well as outdoor use allowed. The maximum mean e.i.r.p. density shall b restricted to 50 mW/MHz in any 1 MHz band.
e	17.1 - 17.3 GHz	100 mW e.i.r.p.	No Restriction	No spacing		

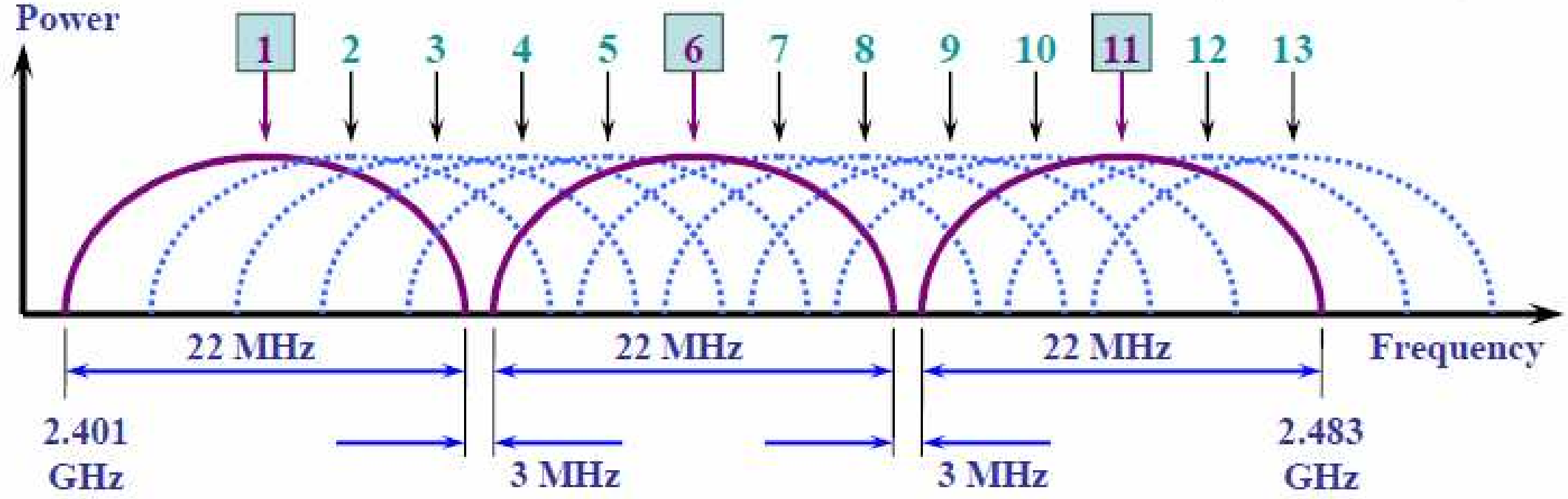
Кол-во каналов для стран (2,4Ггц) REC7003E

Европа (за исключением Франции и Испании)	2.412 - 2.472 ГГц	13
Франция и Испания	2.457 - 2.472 ГГц	4
США и Канада	2.412 - 2.462 ГГц	11
Япония	2.412 - 2.484 ГГц	14
Корея	2.412 - 2.472 ГГц	13
Чили	2.412 - 2.472 ГГц	13
Австралия	2.412 - 2.472 ГГц	13
Южная Африка	2.412 - 2.472 ГГц	13
Юго-Восточная Азия (включая Сингапур, Малайзию, Таиланд)	2.412 - 2.472 ГГц	13

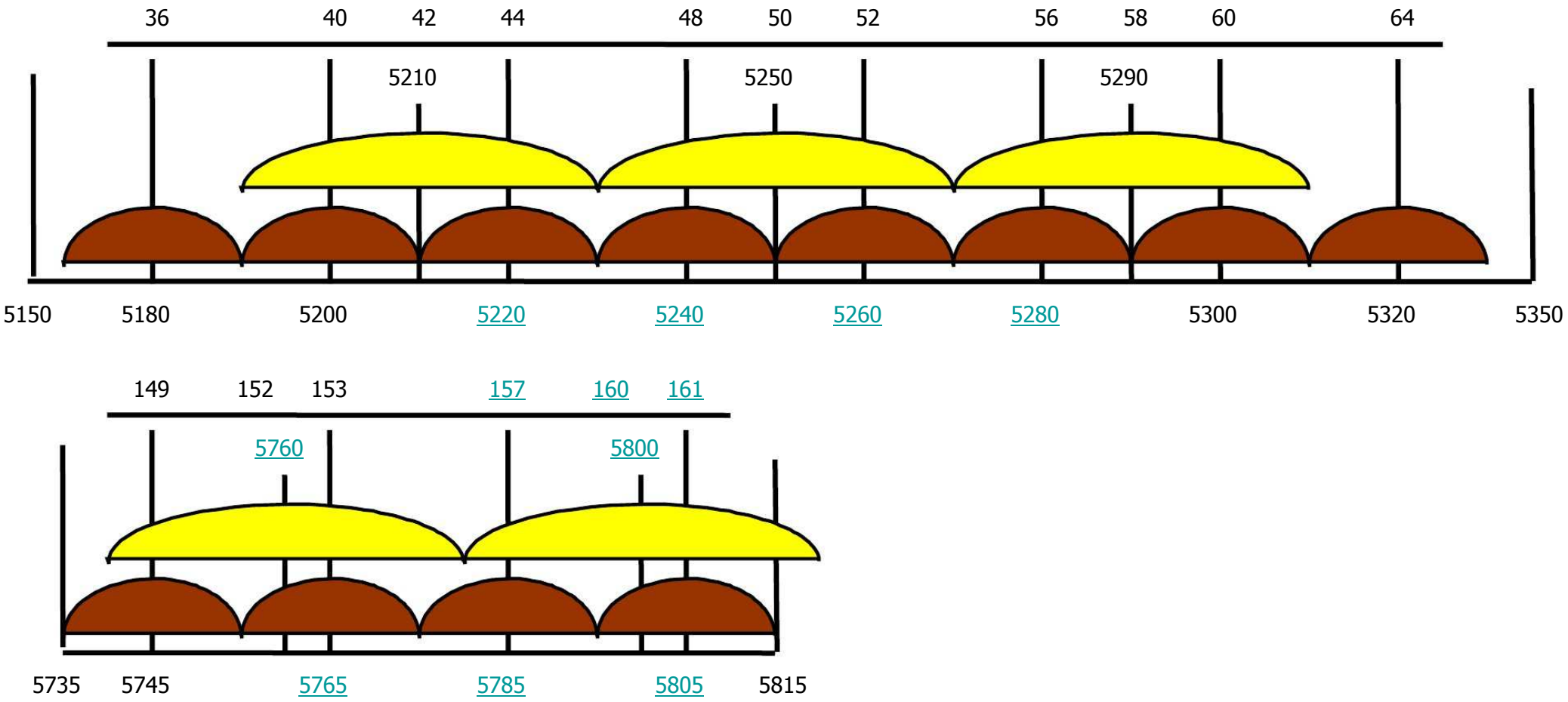
Частоты каналов

Каждый канал занимает частотный диапазон в 22 МГц.
Например, канал 1 работает в диапазоне
от 2,401ГГц до 2,423ГГц, т.е 2,412ГГц ±11МГц.

Канал	Частота
1	2,412 ГГц
2	2,417 ГГц
3	2,422 ГГц
4	2,427 ГГц
5	2,432 ГГц
6	2,437 ГГц
7	2,442 ГГц
8	2,447 ГГц
9	2,452 ГГц
10	2,457 ГГц
11	2,462 ГГц
12	2,467 ГГц
13	2,472 ГГц

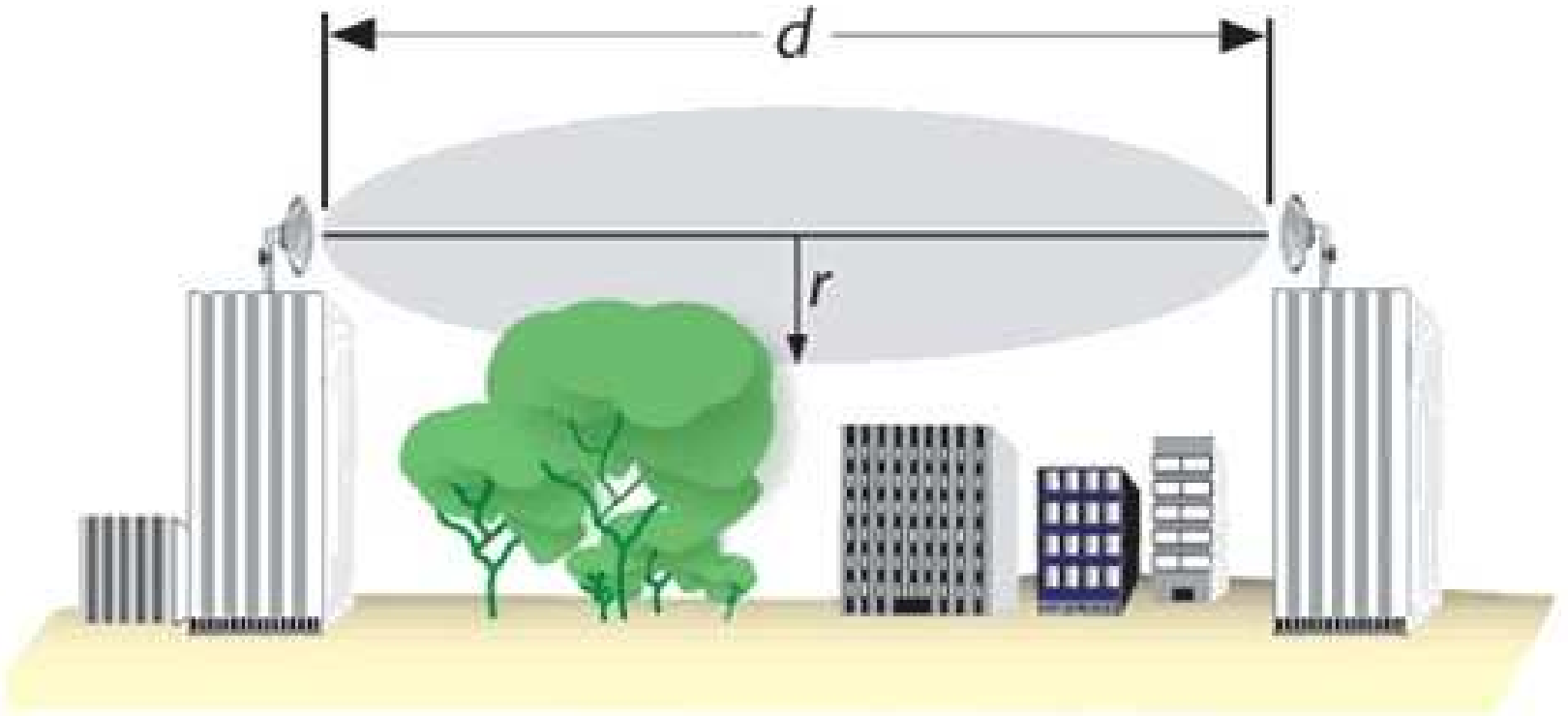


802.11a Channels



- (12) 20 MHz wide channels
- (5) 40MHz wide turbo channels

Зона Френеля



Радиоволна в процессе распространения в просторные занимает объем в виде эллипсоида обращения с максимальным радиусом в середине пролета, который называют зоной Френеля.

Естественные (земля, горбы, деревья) и искусственные (здания, столбы) препятствия, которые попадаются в это

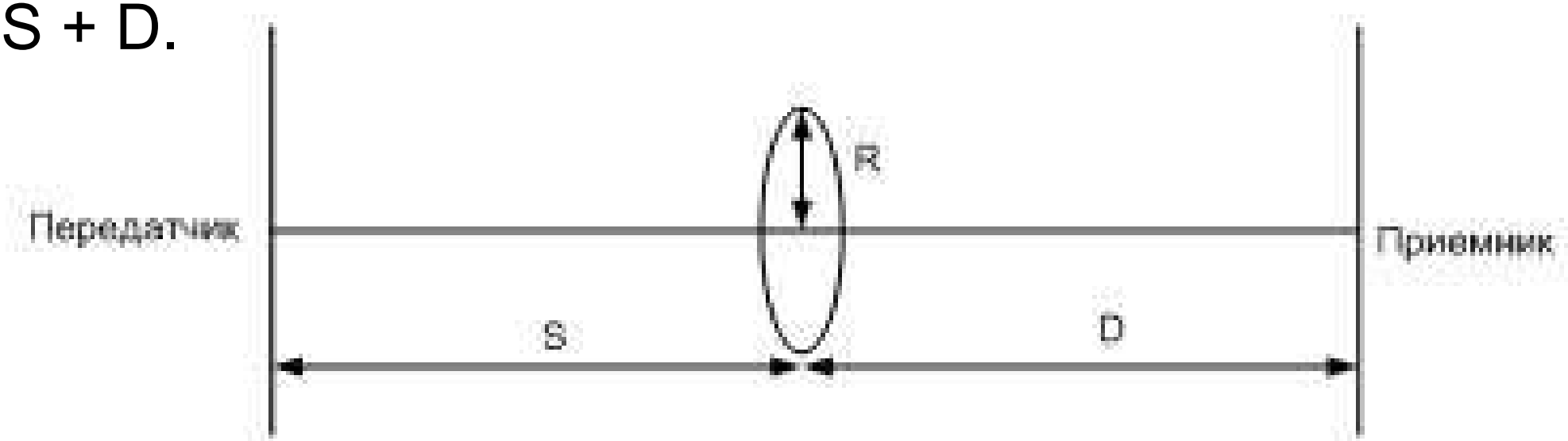
Зона Френеля

Понятие зон Френеля основано на принципе **Гюйгенса,** согласно которому **каждая точка среды до которой доходит возмущение, сама становится источником вторичных волн**, и поле излучения может рассматриваться как суперпозиция всех вторичных волн.

На основе этого принципа можно показать, что объекты лежащие внутри концентрических окружностей, проведенных вокруг линии прямой видимости двух трансиверов, могут влиять на качество как положительно, так и отрицательно. Все препятствия, попадающие внутрь первой окружности, первой зоны Френеля, оказывают наиболее негативное влияние.

Зона Френеля

Рассмотрим точку, находящуюся на прямом тракте между передатчиком и приемником, причем расстояние от точки до передатчика равно S, а расстояние от точки до приемника равно D, т.е. расстояние между передатчиком и приемником равно S + D.



Зона Френеля

радиус первой зоны Френеля в этой точке:

$$R = \sqrt{\frac{\lambda SD}{S+D}}$$

где R, S и D измеряются в одних и тех же единицах, а ? обозначает длину волны сигнала вдоль тракта. Для удобства формулу можно переписать следующим образом:

$$R_M = 17{,}3\sqrt{\frac{1}{f_{ГГц}}\frac{S_{КМ}D_{КМ}}{S_{КМ}+D_{КМ}}}$$

где R выражается в метрах, два остальных расстояния - в километрах, а частота сигнала - в

Безопасность в беспроводных сетях

Для обеспечения безопасности в беспроводных сетях используется несколько средств:

- Контроль за подключением к точке доступа на основе MAC-адресов и имени сети
- Шифрование на основе протокола WEP, WPA,WPA2
- Контроль за доступом к среде передачи на основе протокола 802.1x
- Настройка VPN поверх беспроводного соединения
- Вынос беспроводной сети за межсетевой экран, как сети с низким доверием

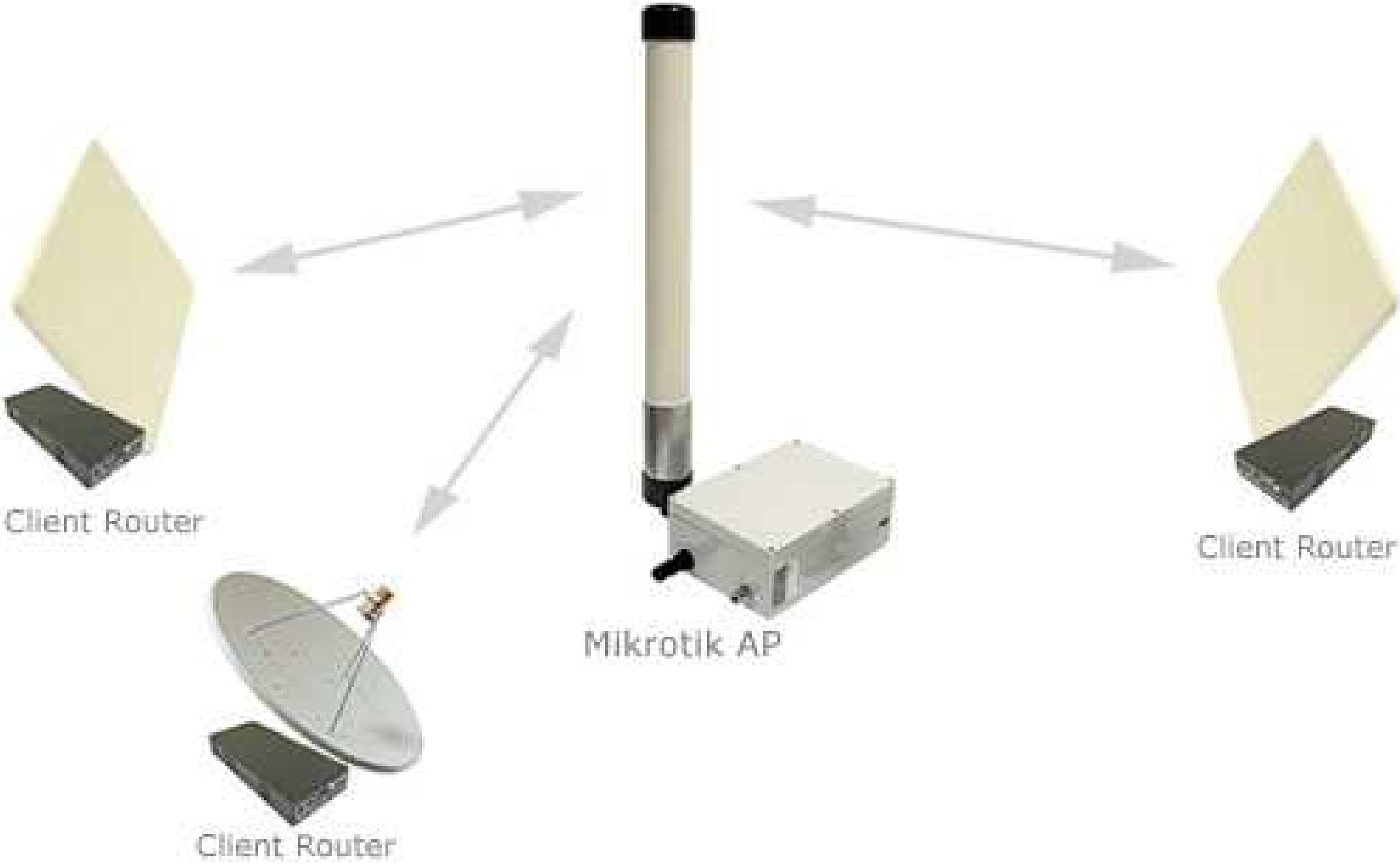
Поддерживаемые частоты MikroTik RouterOS

- 2.4GHz: 2312 - 2499 MHz
- 5GHz: 4920 - 6100 MHz

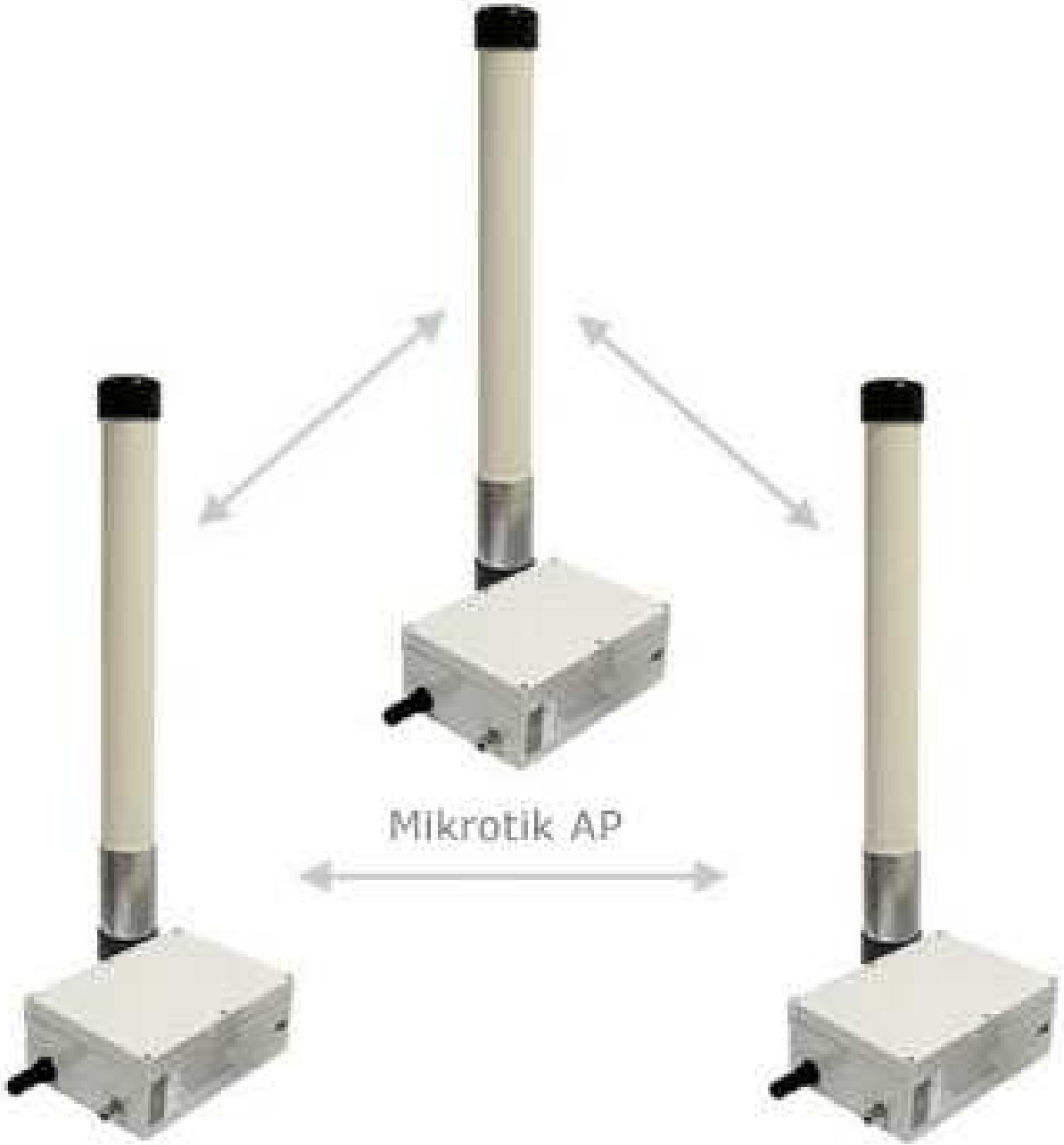
В зависимости от региона

Рассматриваемые режимы wireless MTCNA

Point-to-multipoint



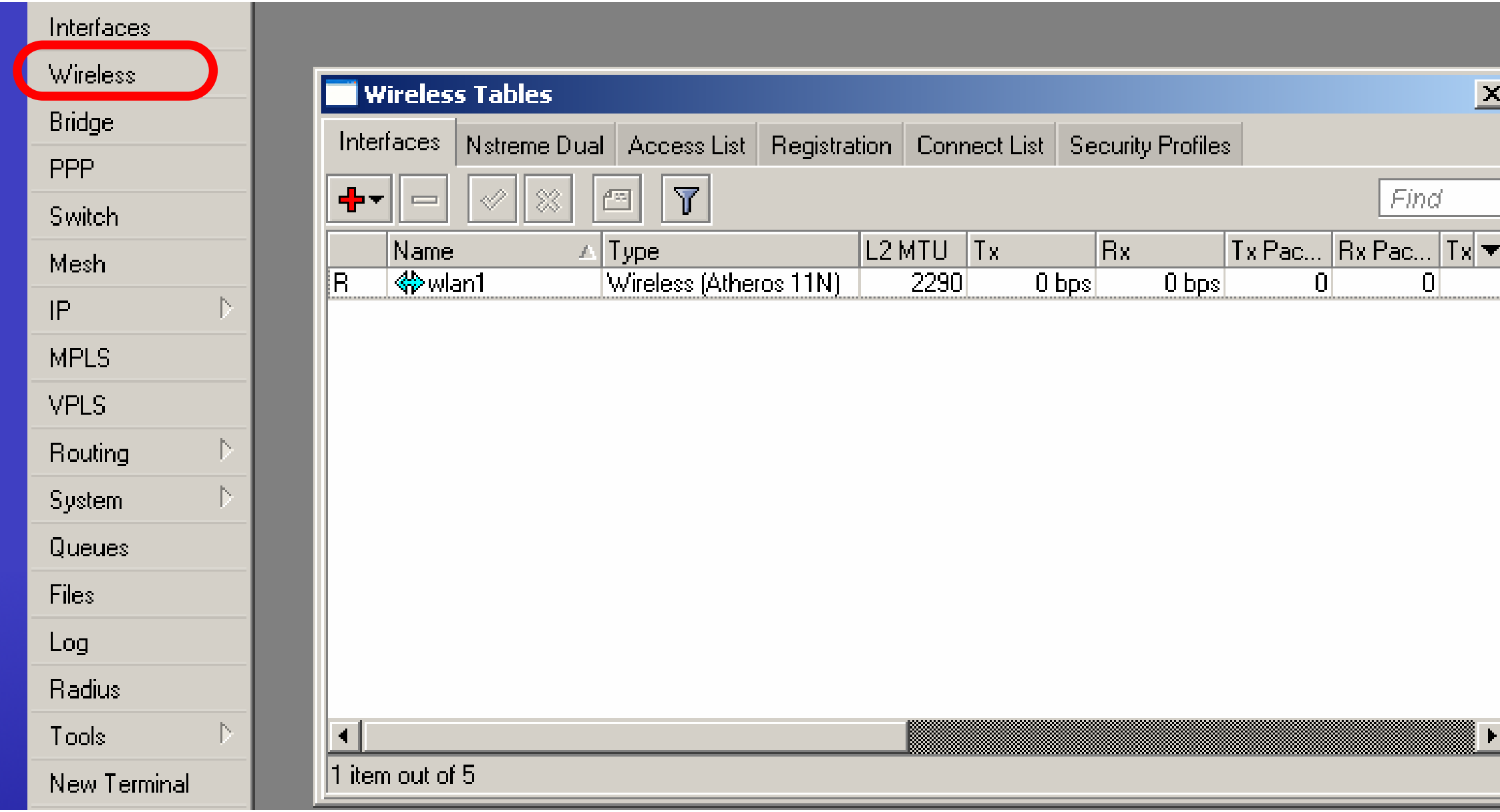
WDS



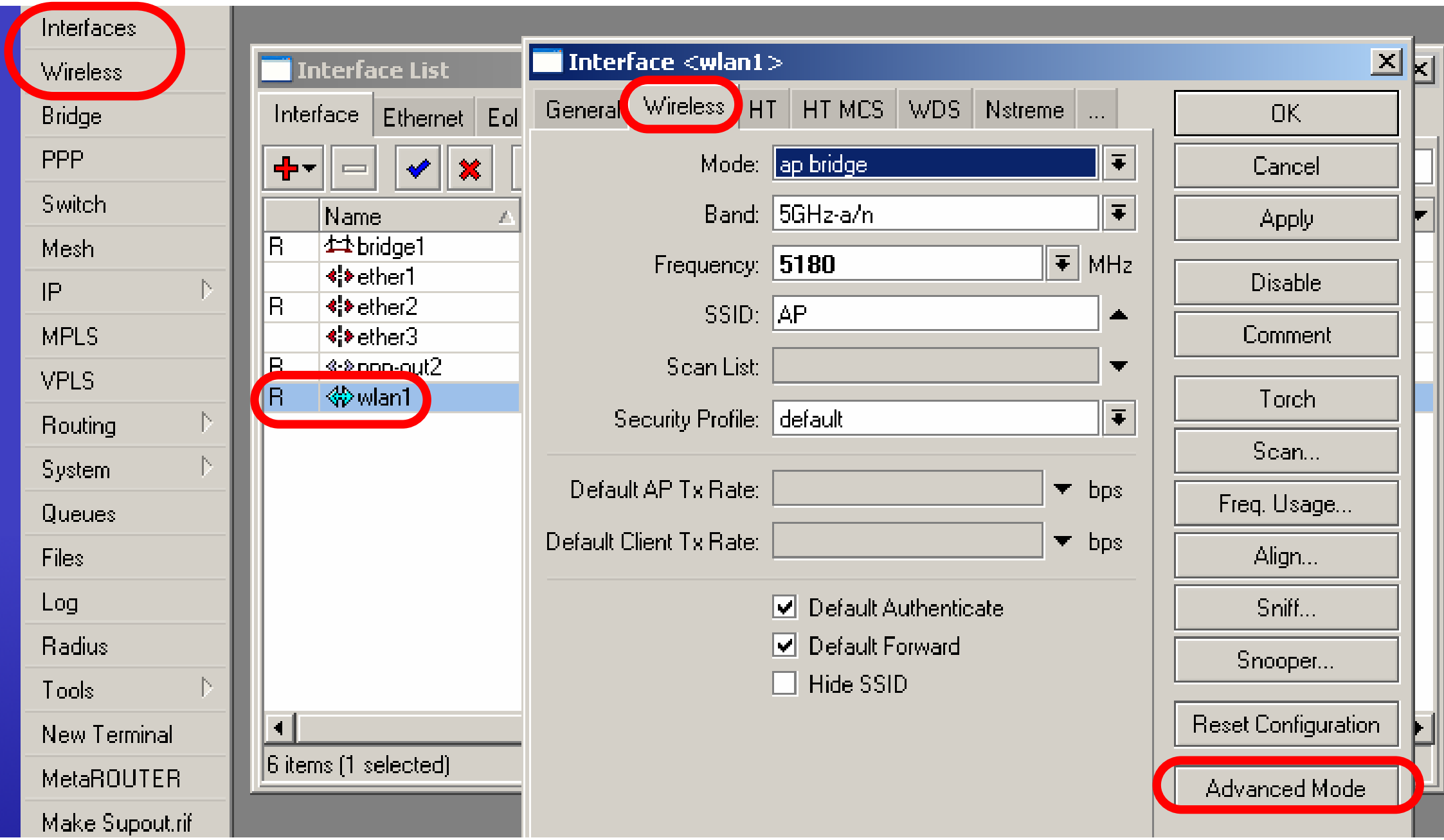
Point-to-point

Общие настройки

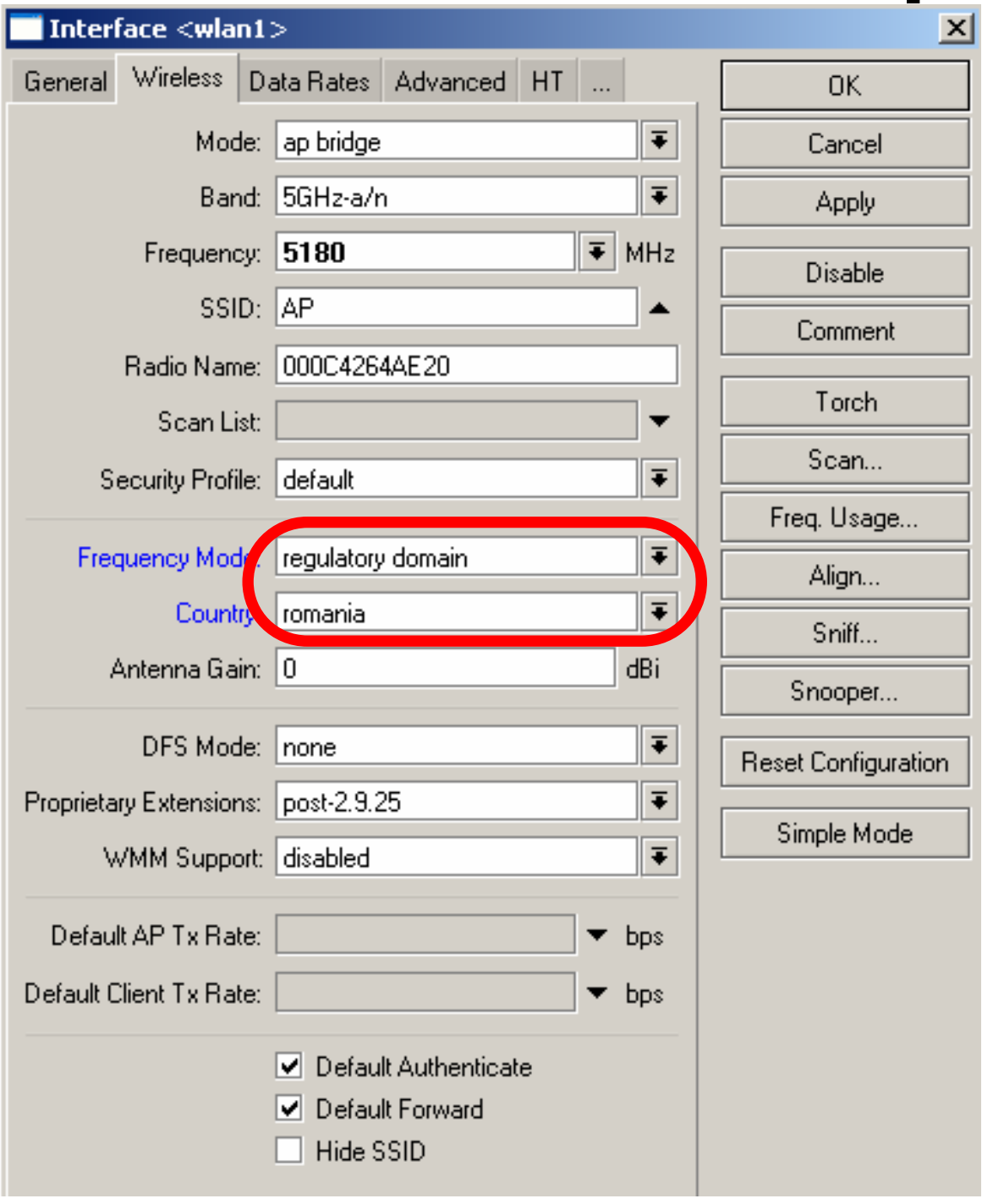
Wireless Configuration



Выбор региональных настроек



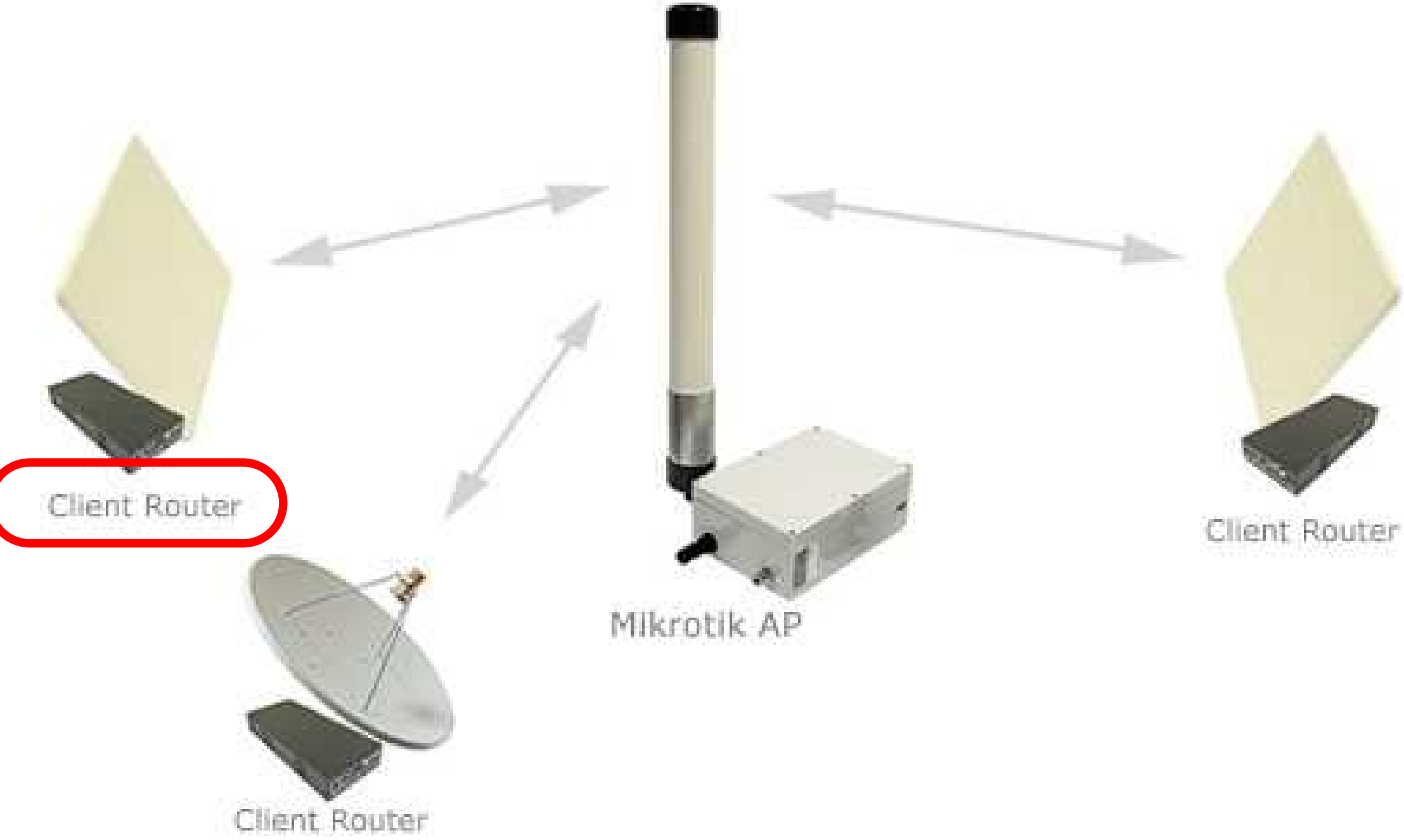
Выбор региональных настроек



RADIO Name

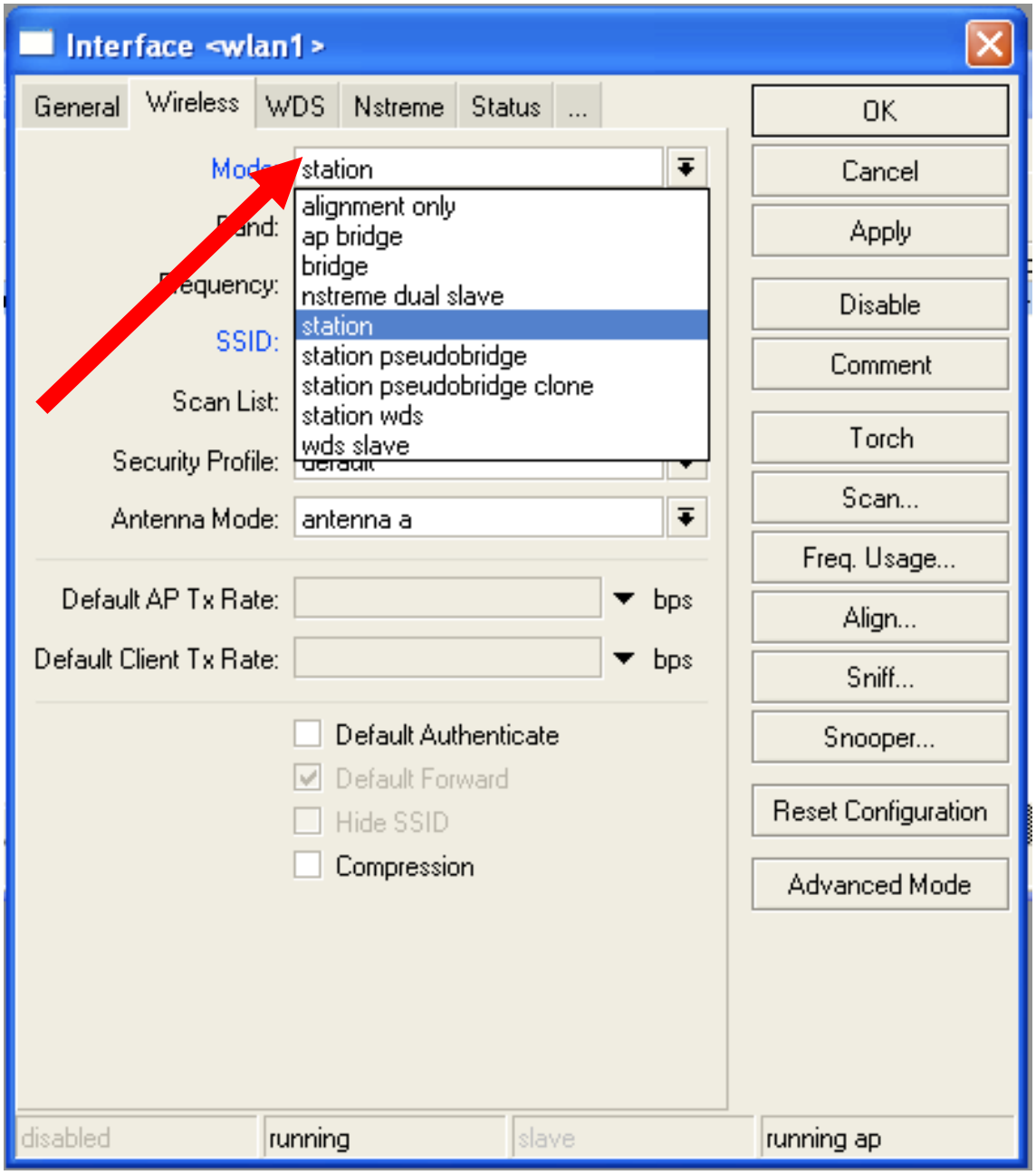
- Мы будем использовать RADIO Name для тех же целей что и использовали router identity
- Установите RADIO Name : **Ваш номер(X) + Ваше имя**

Настройка роутера как клиент (station)



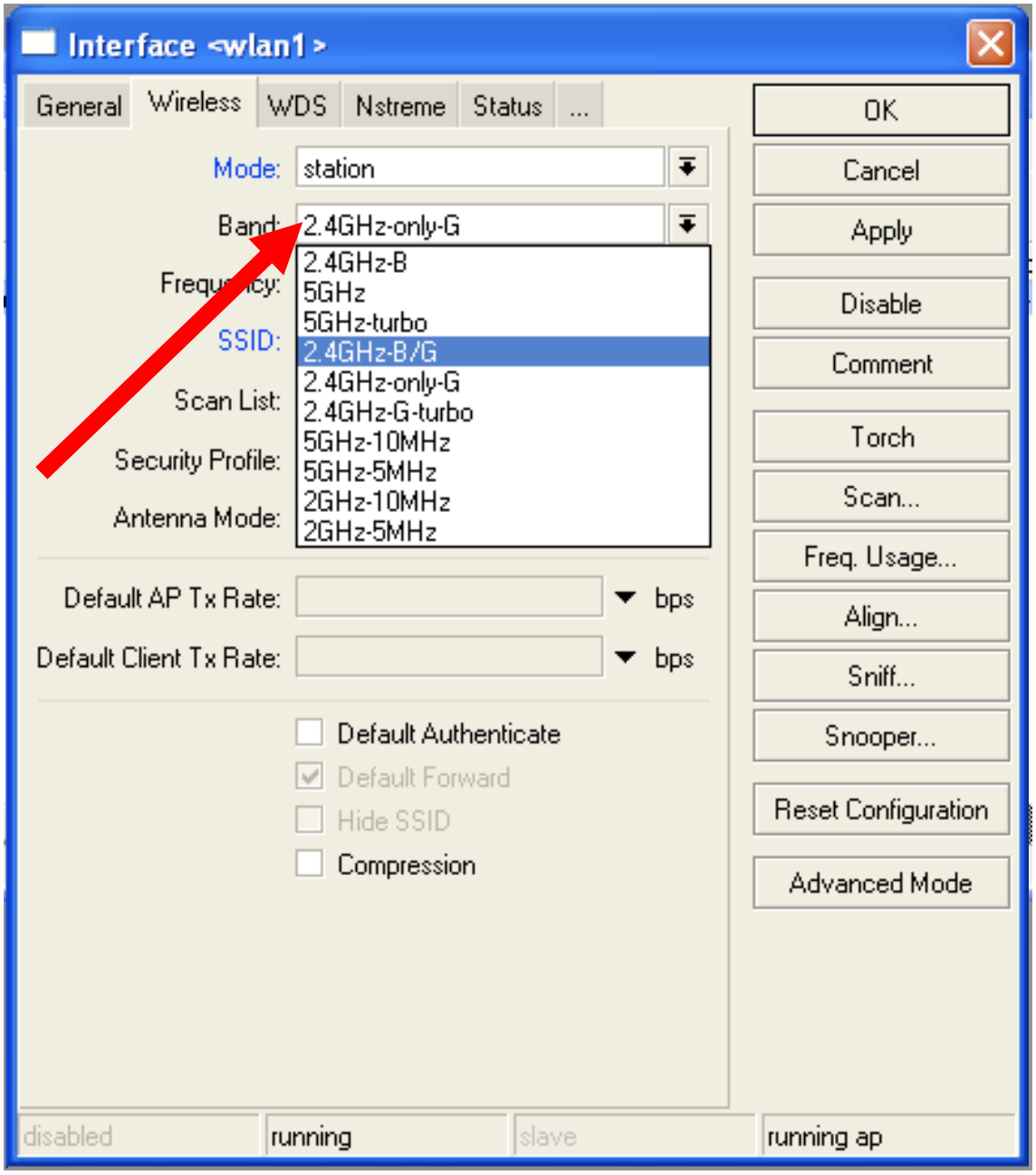
Настройка клиента (Station)

- Установите интерфейс **mode=station**
- Укажите **band (частоту)**
- Укажите **SSID**, Wireless Network Identity
- Указание частоты не является необходимым полем, так же как SSID, потому что можно использовать **scan-list**



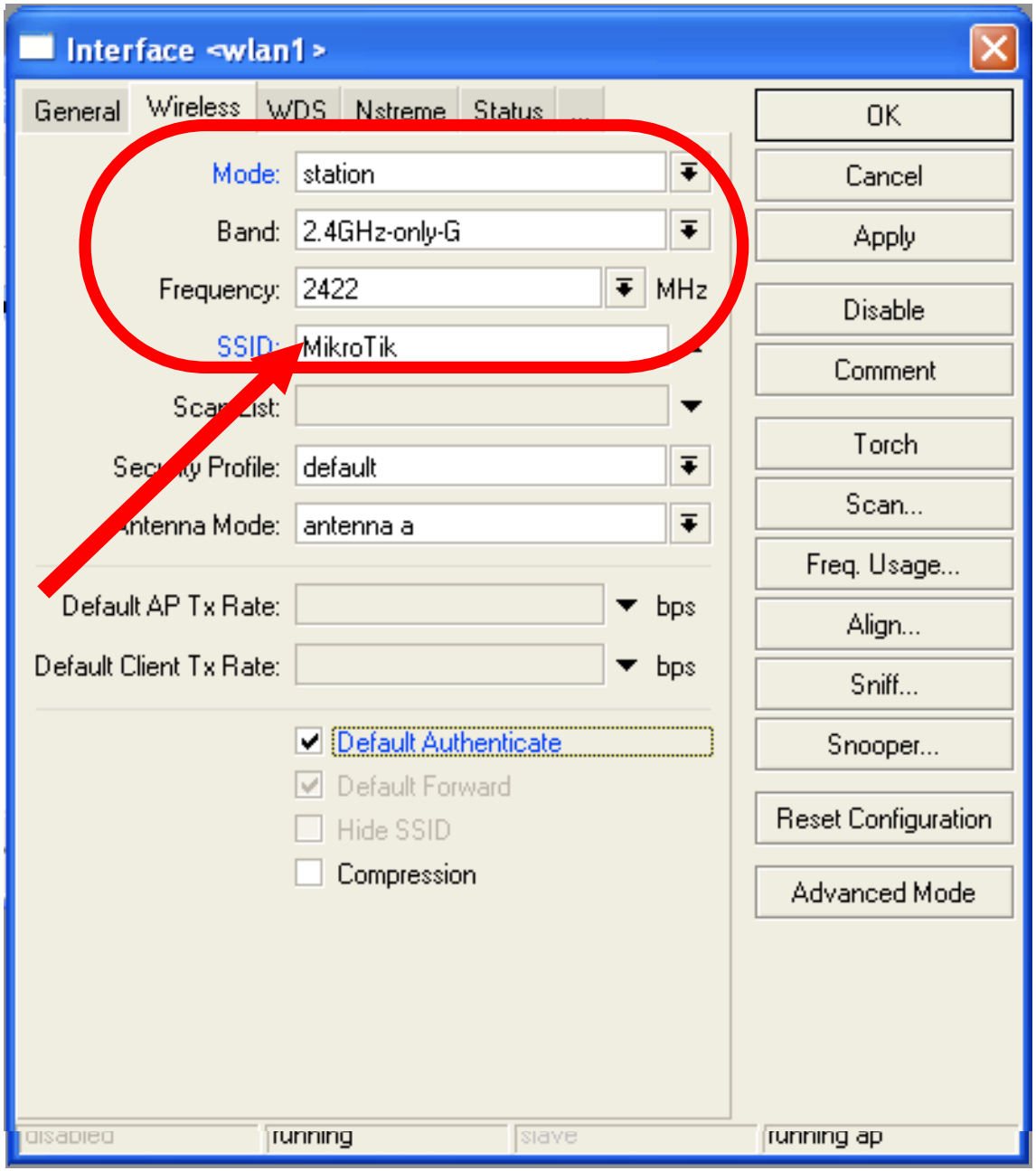
Настройка клиента (Station)

- Установите интерфейс **mode=station**
- Укажите **band (частоту)**
- Укажите **SSID**, Wireless Network Identity
- Указание частоты не является необходимым полем, так же как SSID, потому что можно использовать **scan-list**



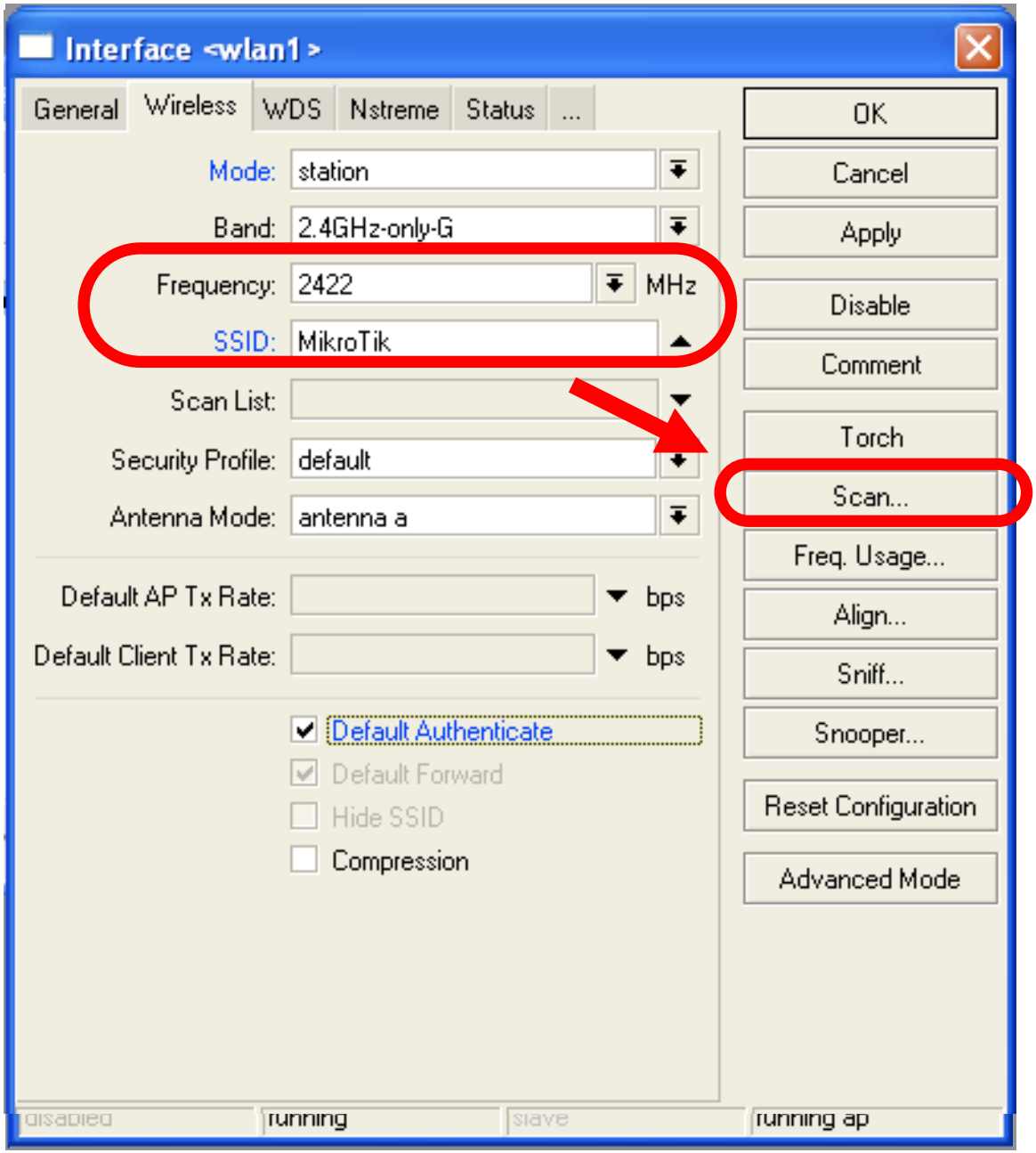
Настройка клиента (Station)

- Установите интерфейс **mode=station**
- Укажите **band (частоту)**
- Укажите **SSID**, Wireless Network Identity
- Указание частоты не является необходимым полем, так же как SSID, потому что можно использовать **scan-list**

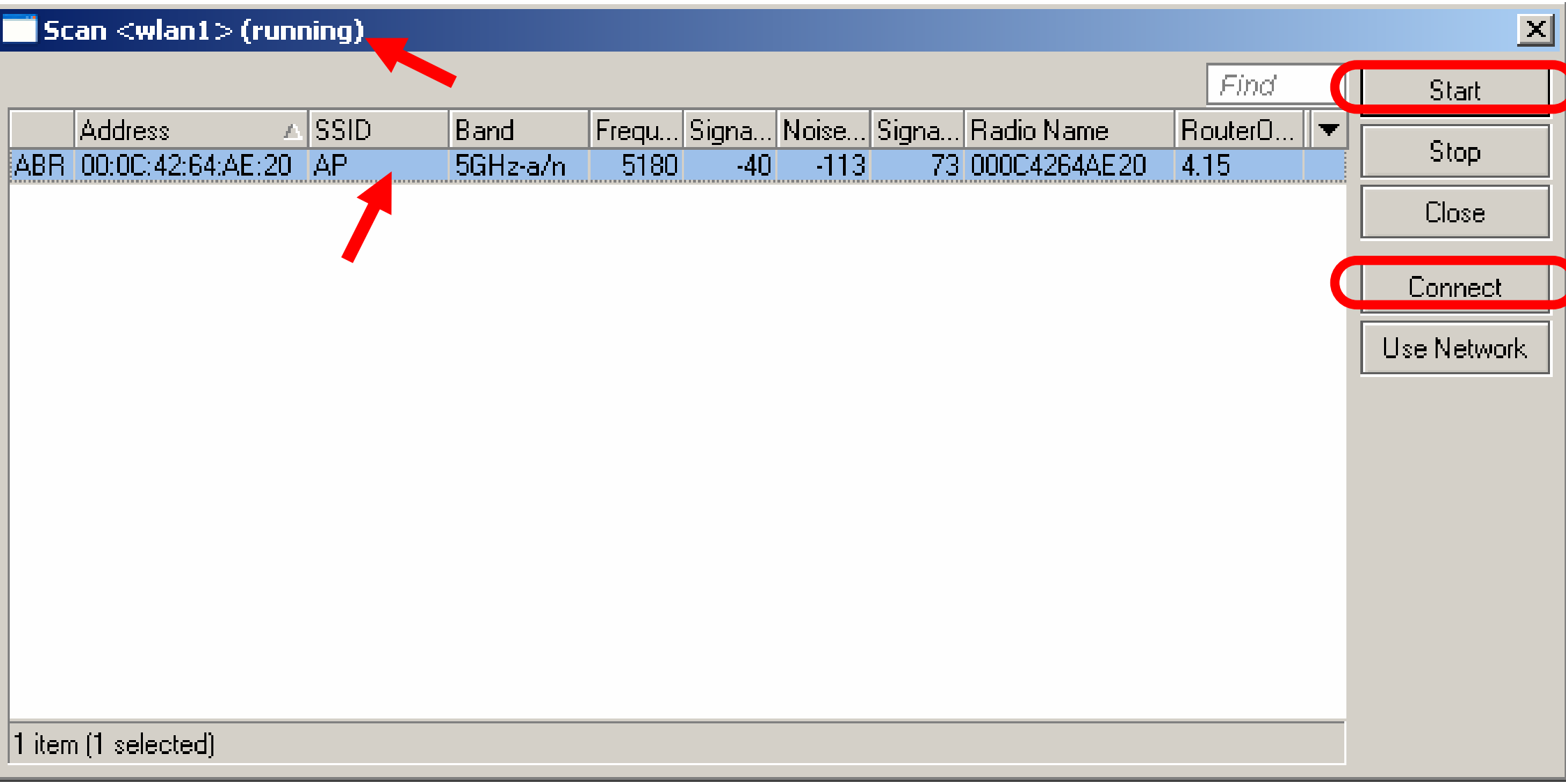


Настройка клиента (Station)

- Установите интерфейс **mode=station**
- Укажите **band (частоту)**
- Укажите **SSID**, Wireless Network Identity
- Указание частоты не является необходимым полем, так же как SSID, потому что можно использовать **scan-list**



Station Configuration - scan



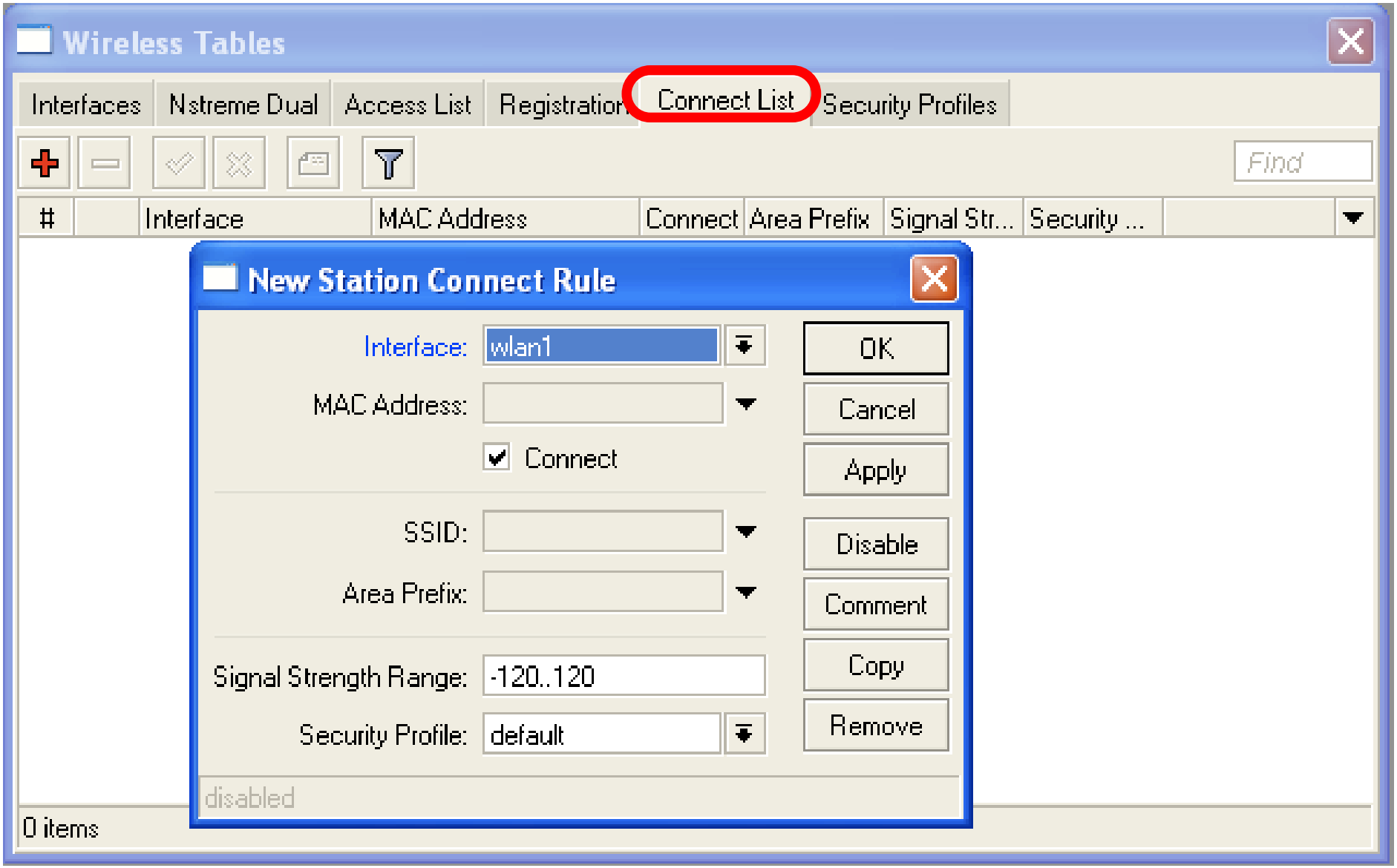
Во время сканирования беспроводной интерфейс потеряет соединение (отключится)

Station Configuration Lab

LAB

- Подключитесь к Trainers точки доступа (AP) используя утилиту поиска сетей **Scan**
- Убедитесь что соединение установлено (**R)**

Connect List



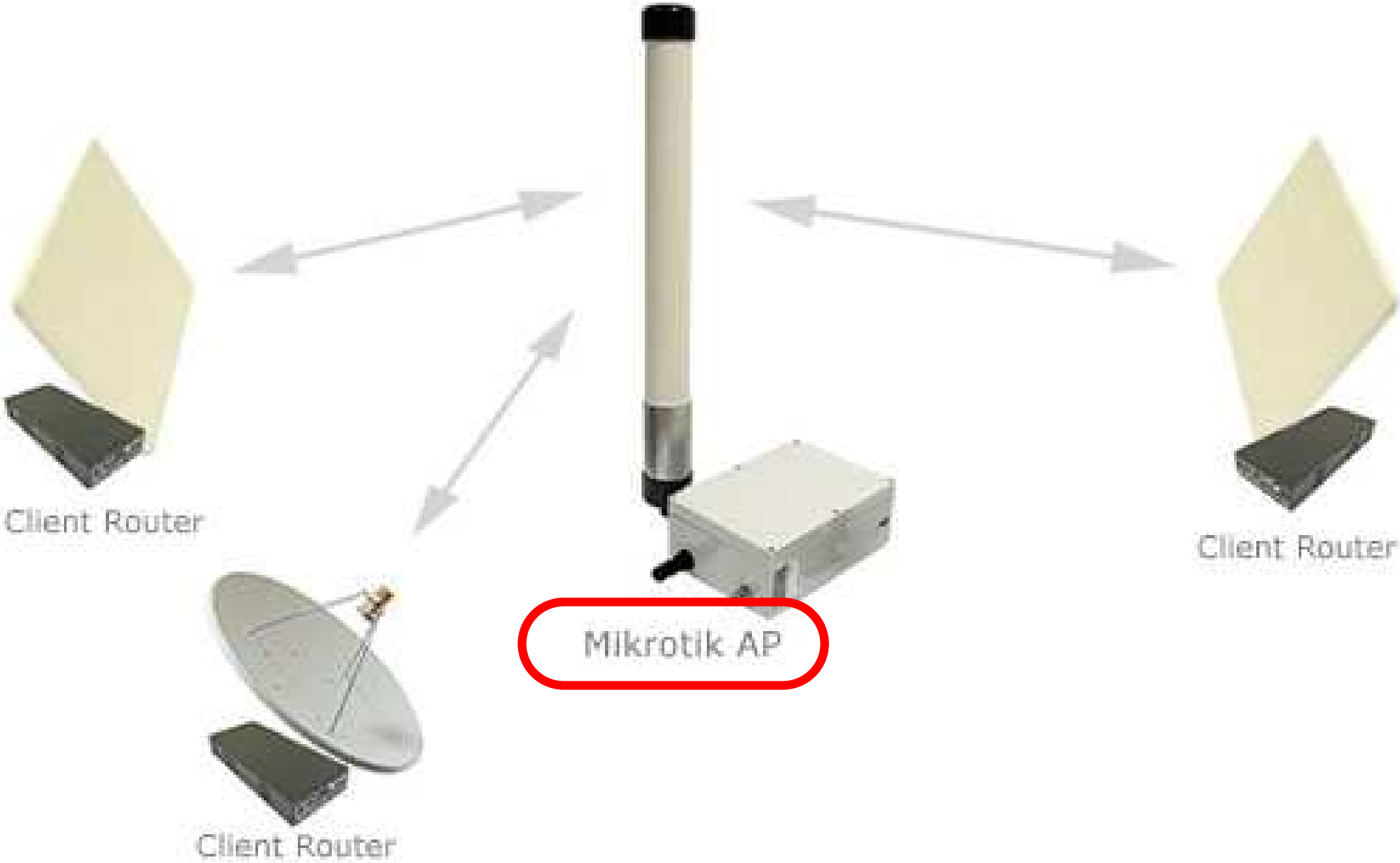
- Создание правил для подключения к точкам доступа (access-point)

Connect List Lab

LAB

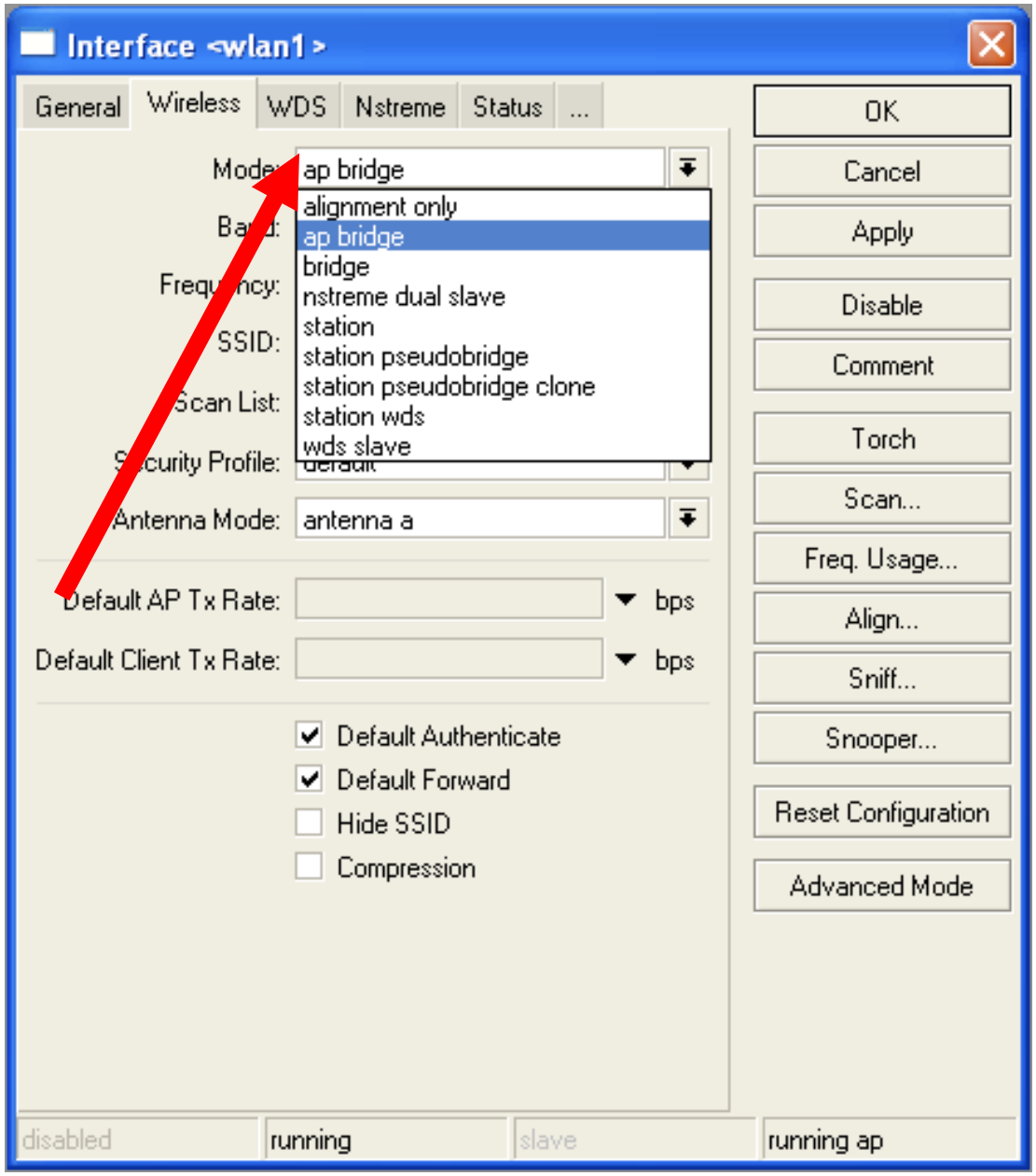
- Сейчас ваш роутер подключен к трейнерской точке доступа (access-point)
- Сделайте правило которое отключит вас от точки доступа
- Используйте для этого connect-list

Настройка роутера как точку доступа (Access point)



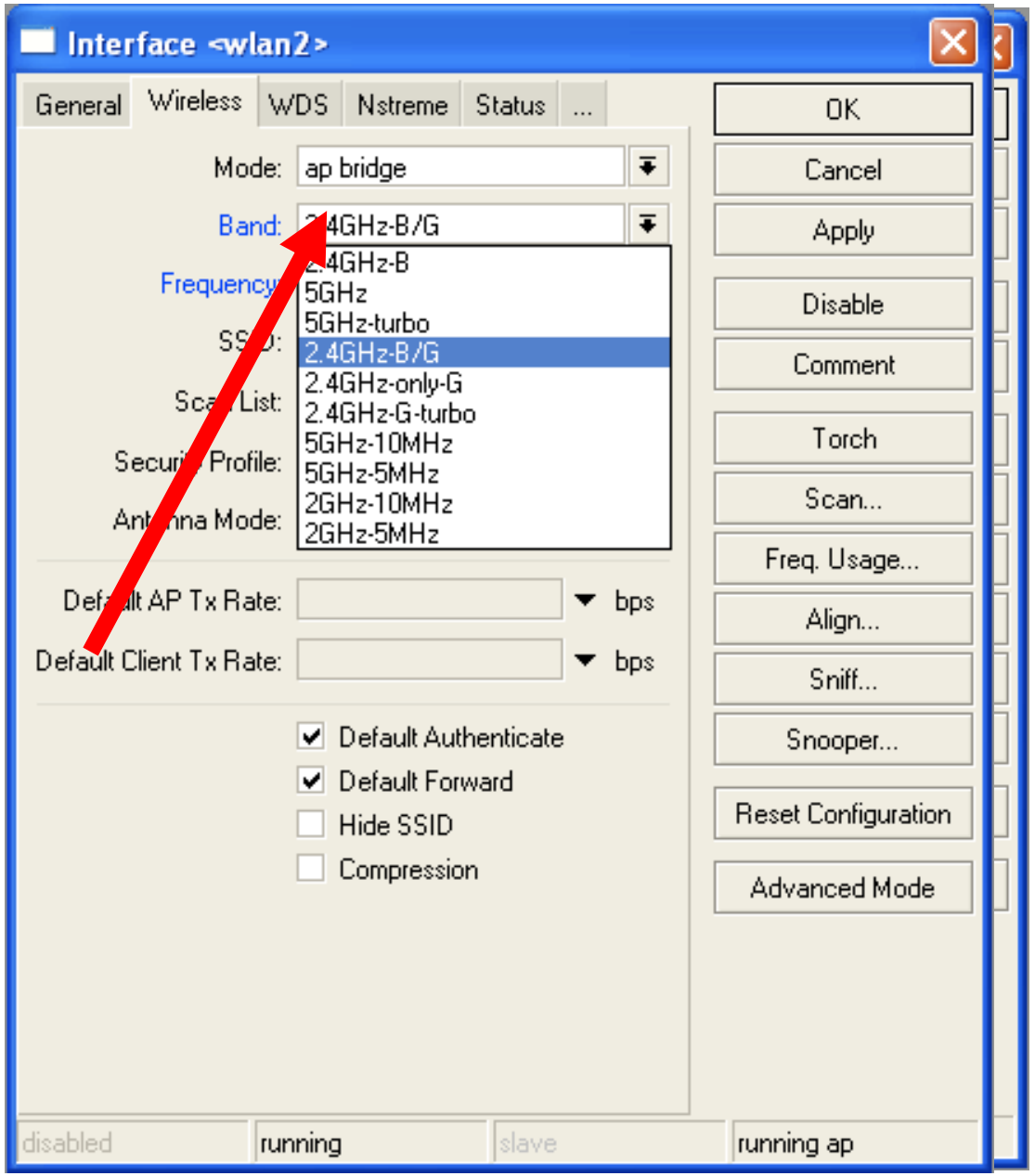
Access Point Configuration
Настойка точки доступа

- Установите интерфейс **mode=ap-bridge**
- Select **band**
- Укажите **SSID**, Wireless Network Identity
- Установите **Frequency**



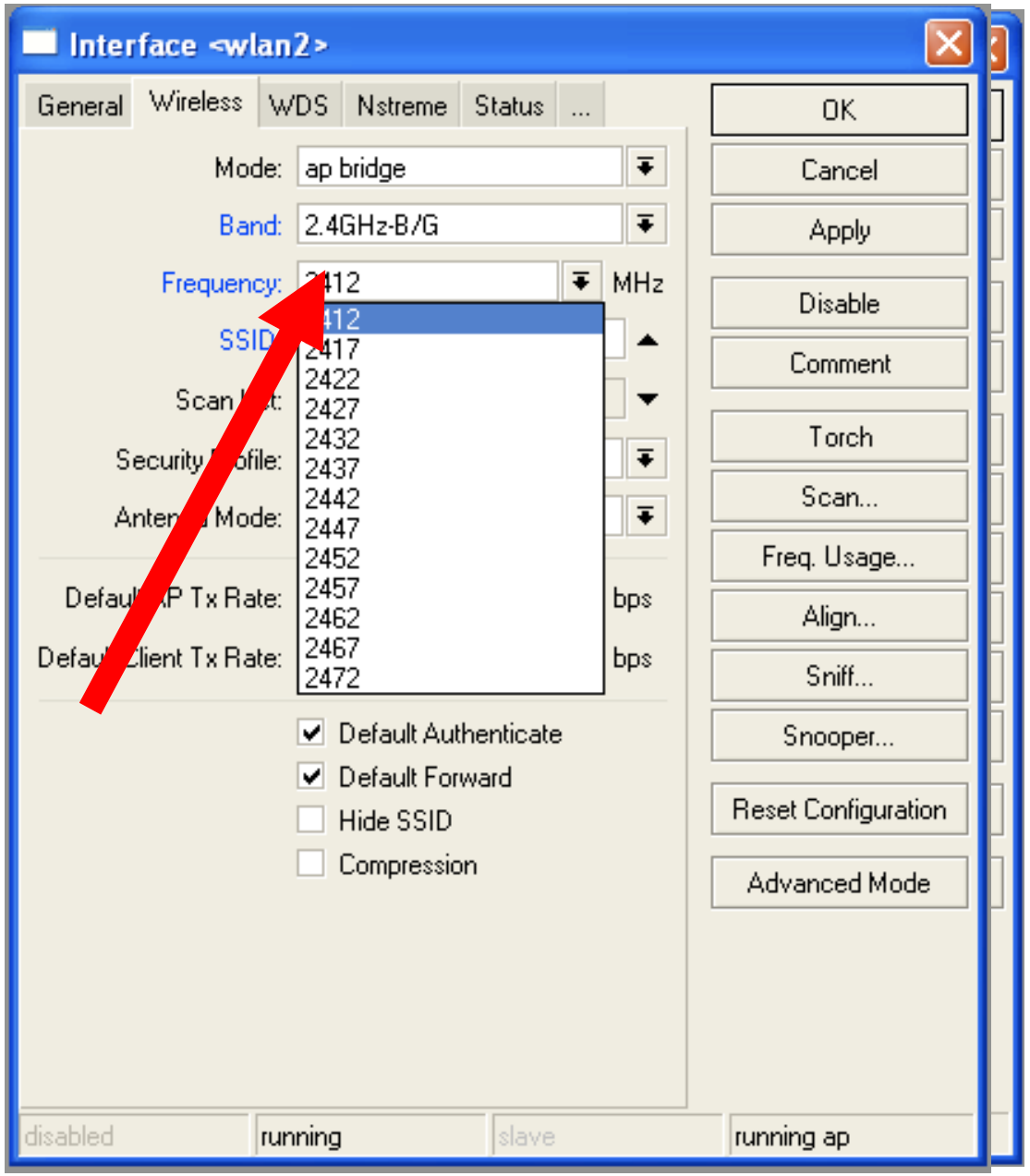
Access Point Configuration
Настойка точки доступа

- Установите интерфейс **mode=ap-bridge**
- Select **band**
- Укажите **SSID**, Wireless Network Identity
- Установите **Frequency**



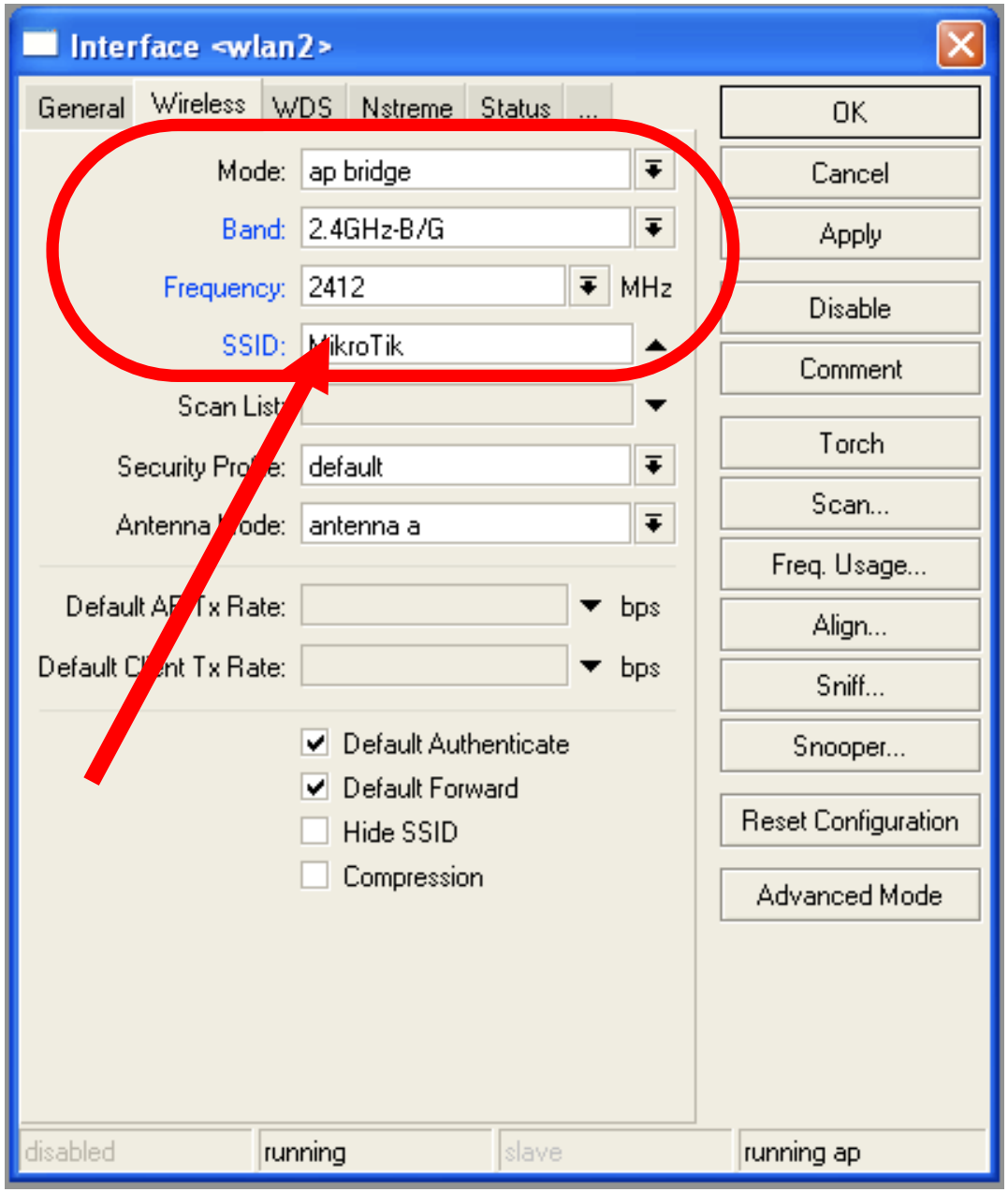
Access Point Configuration
Настойка точки доступа

- Установите интерфейс **mode=ap-bridge**
- Select **band**
- Укажите **SSID**, Wireless Network Identity
- Установите **Frequency**



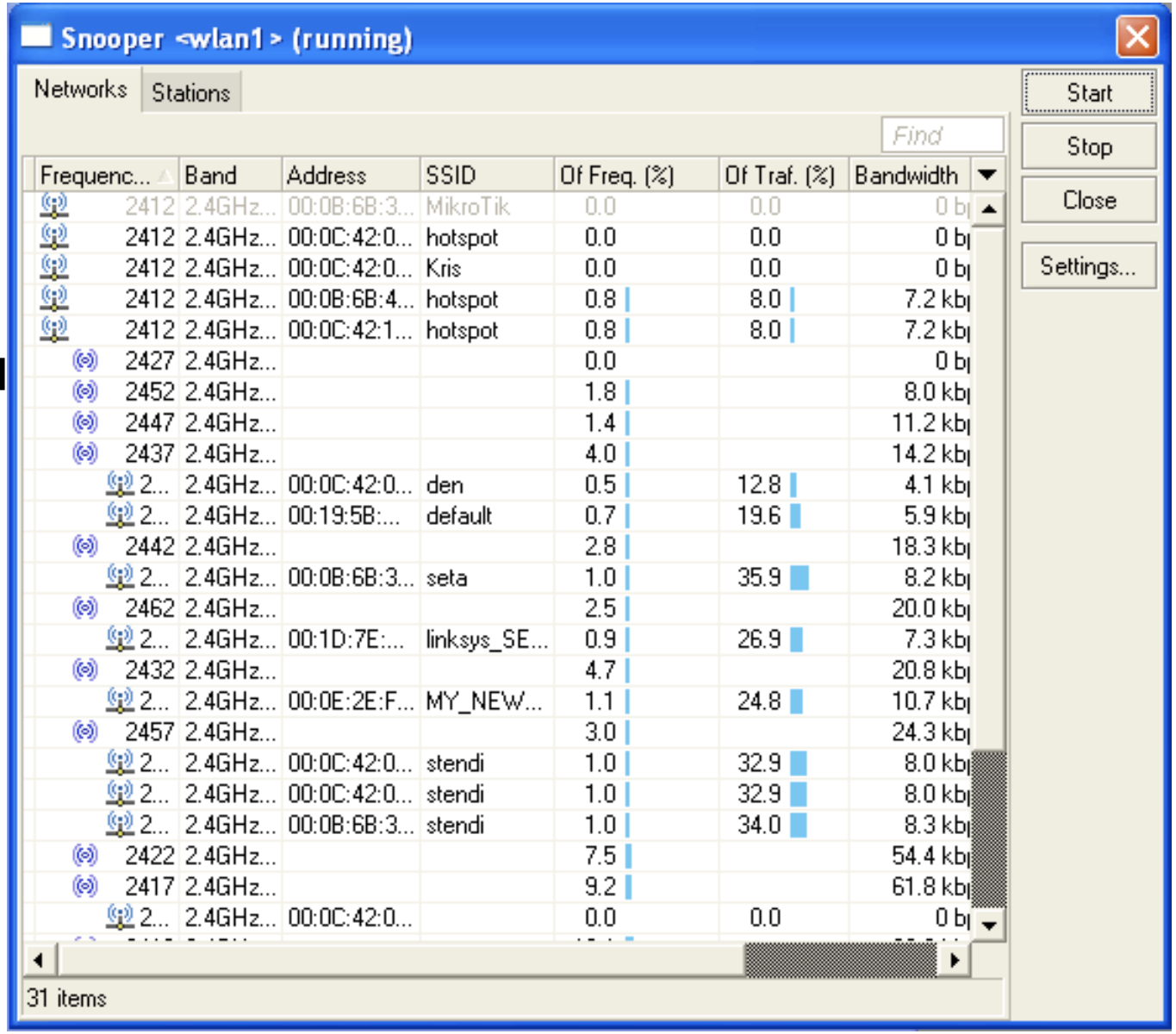
Access Point Configuration
Настойка точки доступа

- Установите интерфейс **mode=ap-bridge**
- Select **band**
- Укажите **SSID**, Wireless Network Identity
- Установите **Frequency**



Snooper wireless monitor

- Используйте Snooper, чтобы получить общее представление о беспроводных сетях, и используемых частотах
- В это время беспроводной интерфейс отключится

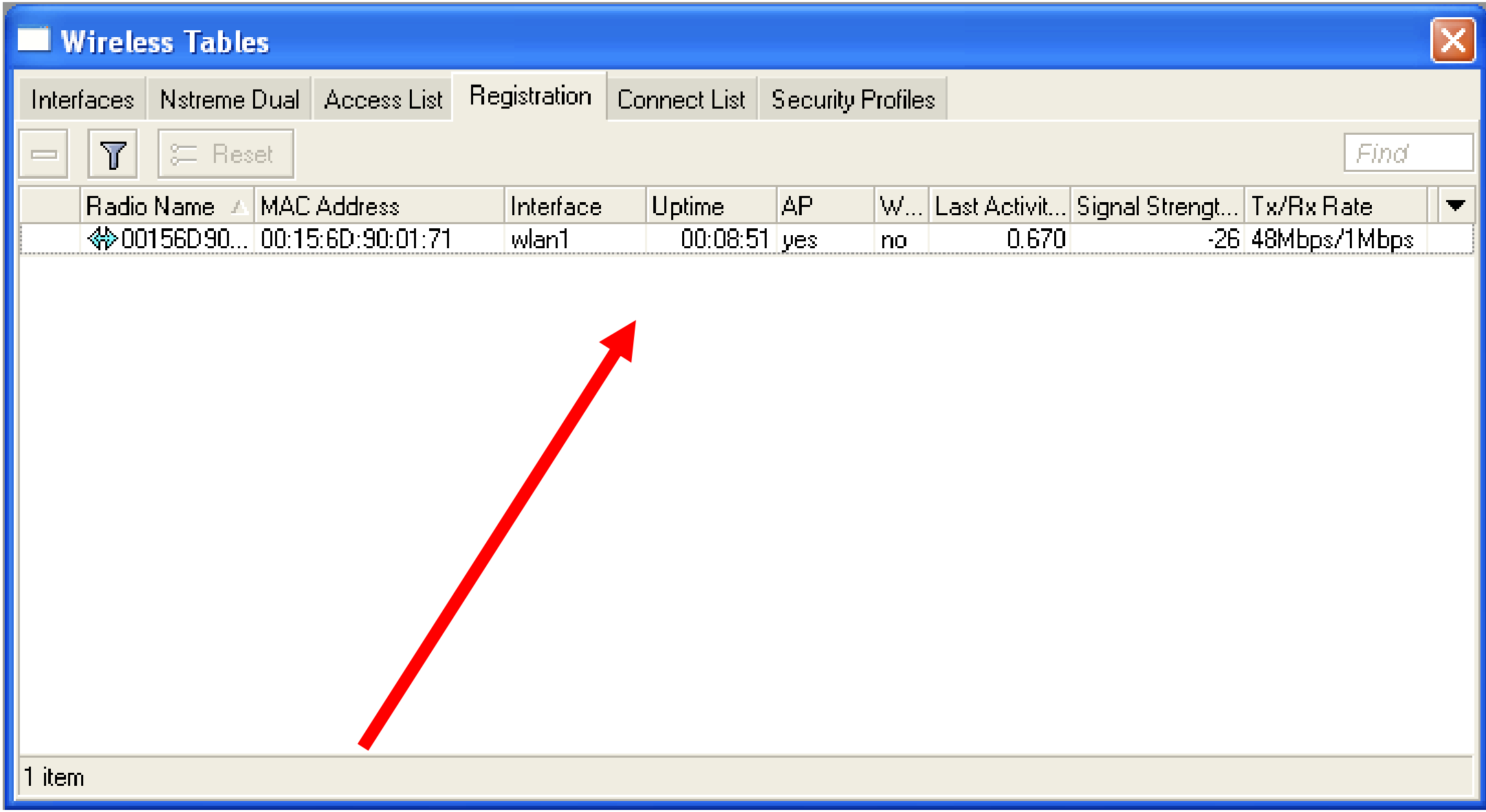


Wireless AP(точка доступа) and Station

LAB

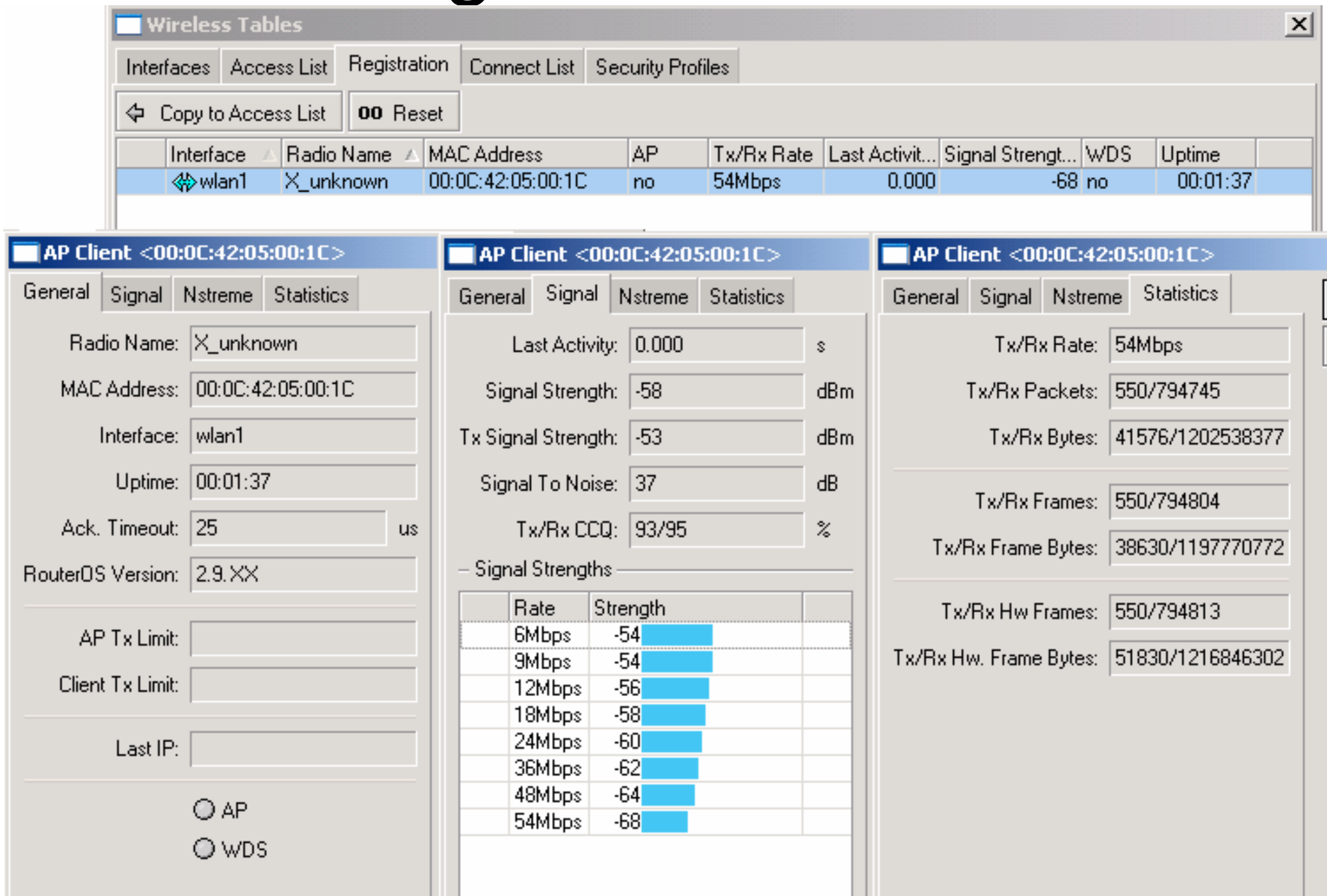
- Работа в группе где один из группы сделает из своего роутера точку доступа (AP), а остальные члены группы к ней подключатся
- Один из группы создайте точку доступа на беспроводном интерфейсе wlan1, работающую на 2Ghz, с SSID “AP_Y_X, где Y номер вашей группы, а X ваш личный номер.
- Остальные члены группы настройте на своем роутере интерфейс wlan1 как station и подключитесь к точке доступа своего соседа в вашей группе.

Registration Table

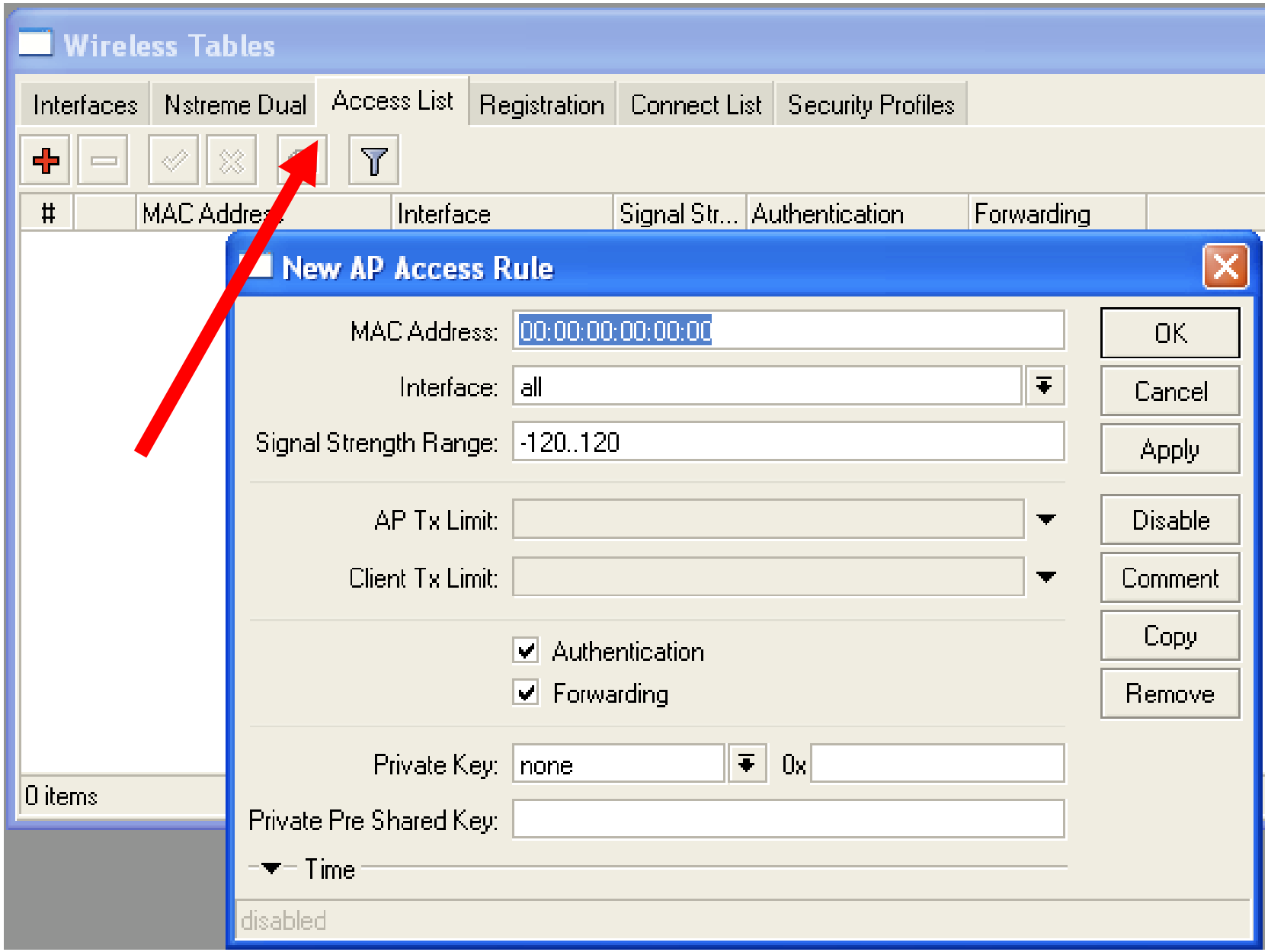


- Показывает всех подключенных к беспроводному интерфейсу

Registration Table



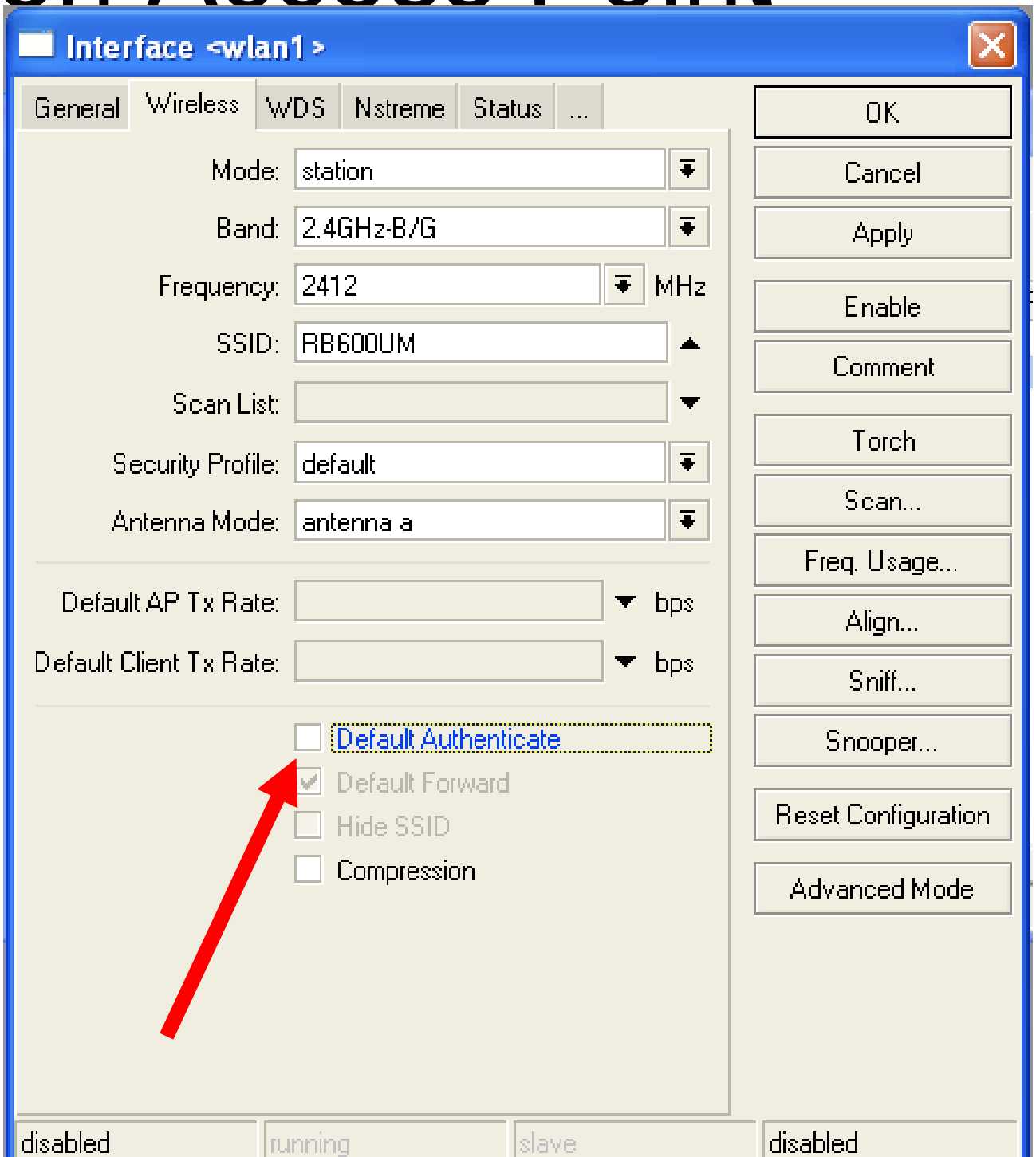
Security on Access Point



- **Access-list** используется для фильтрации клиентов по **MAC-address**

Security on Access Point

- Отключите **Default-Authentication** что бы разрешить доступ к точке только устройствам прописанным в Access-list



Default Authentication

- **Yes,** правила Access-List проверяются, пользователи могут подключаться если нет запрещающего правила
- **No,** доступ к точке только по правилам Access-List

Access-List Lab

LAB

- Сконфигурируйте свои роутеры в режим station и подключитесь к тренерской точки доступа SSID “AP_Trainers”
- Отключим только определенных клиентов
- Разрешим доступ определенным клиентам

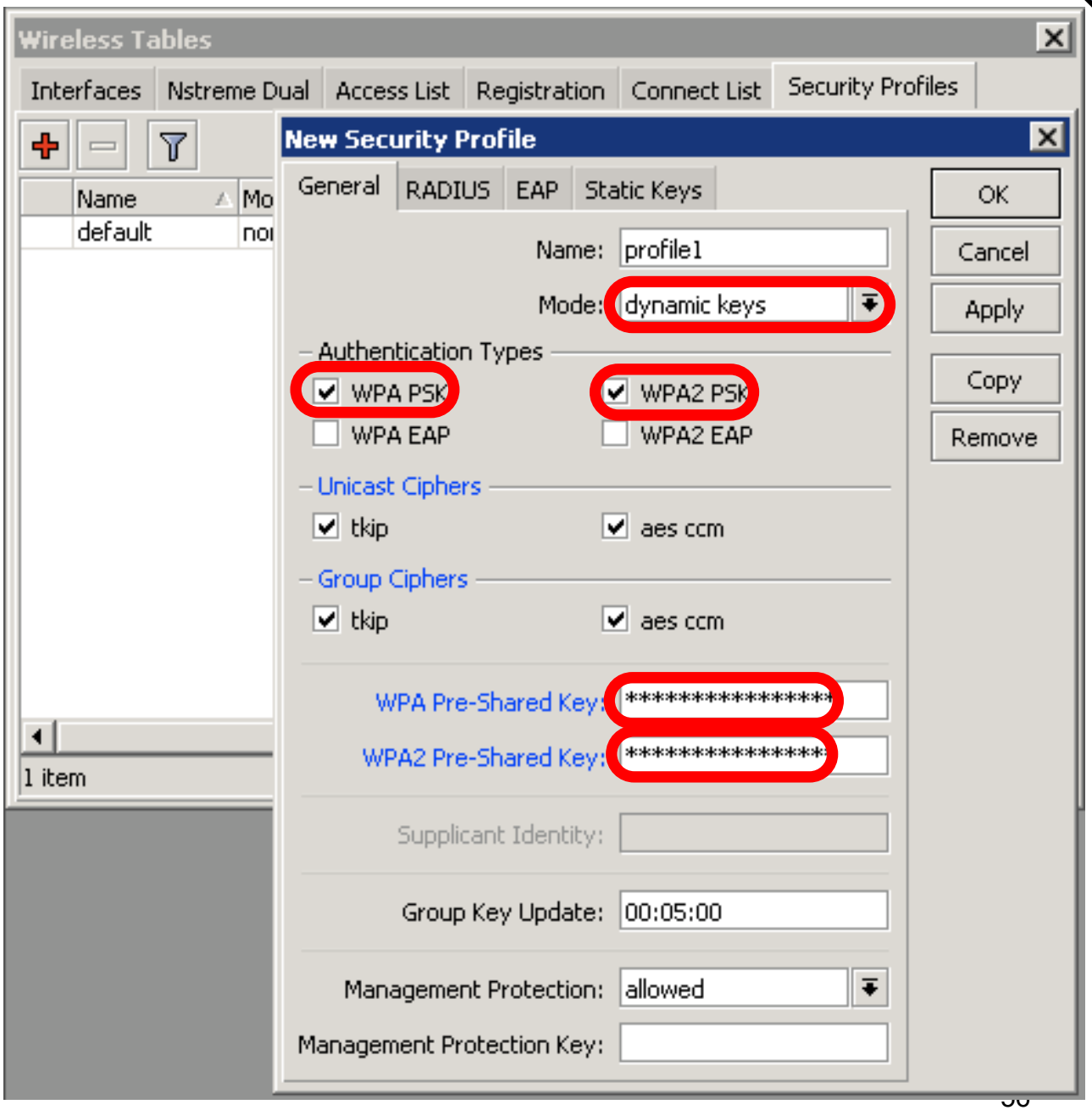
Security

- Сейчас мы включим шифрование для нашей беспроводной сети
- Вы должны использовать WPA или WPA2 шифрование
- Все устройства в сети должны иметь одинаковые параметры безопасности

Security

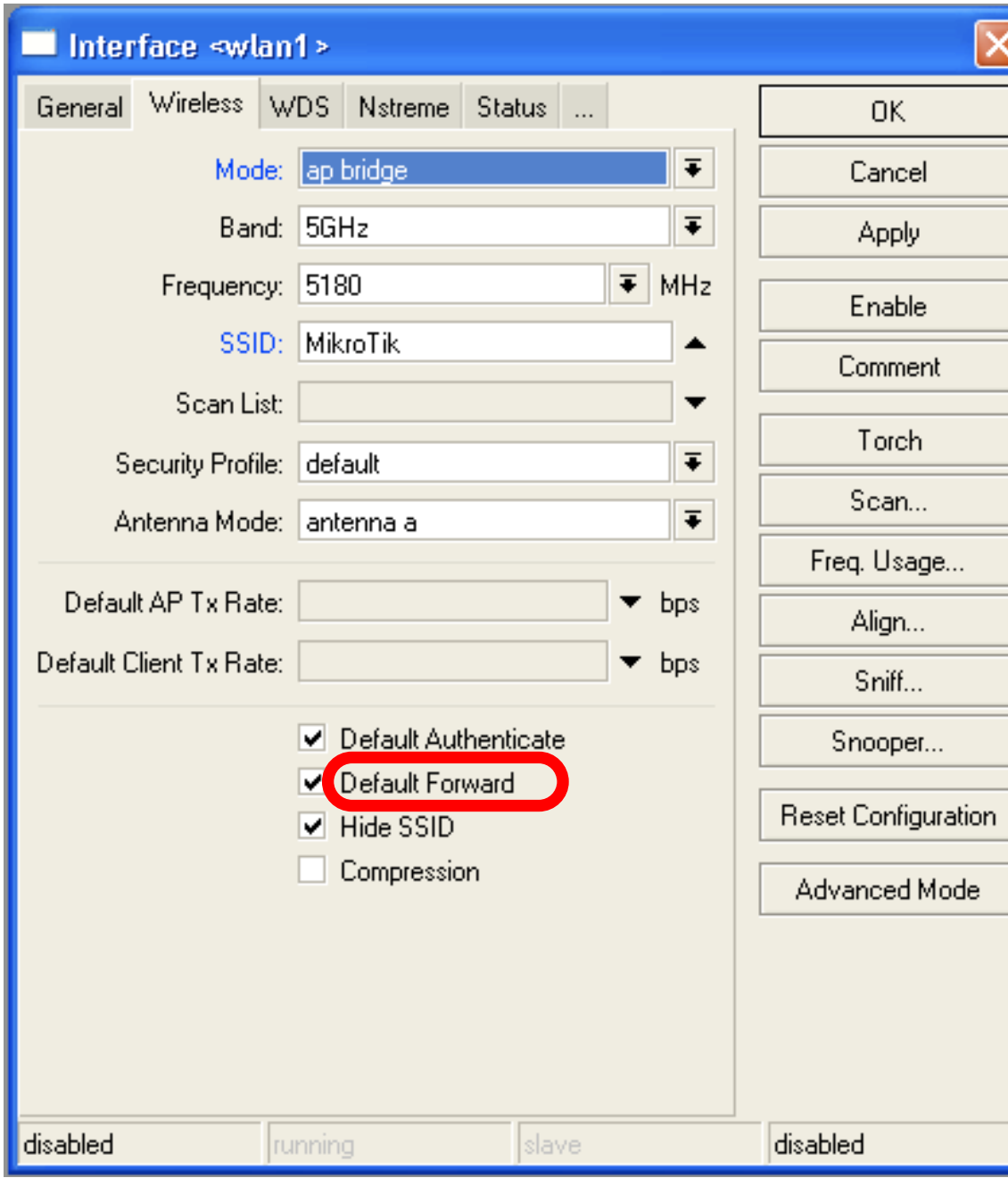
LAB

- Сейчас мы включим шифрование WPA для нашей беспроводной сети
- WPA Pre-Shared Key будет **mikrotiktraining**



Блокировка соединения между клиентами

- **Default-Forwarding** используется для отключения связи между клиентами подключенных к одной и той же точки доступа



Default Forwarding

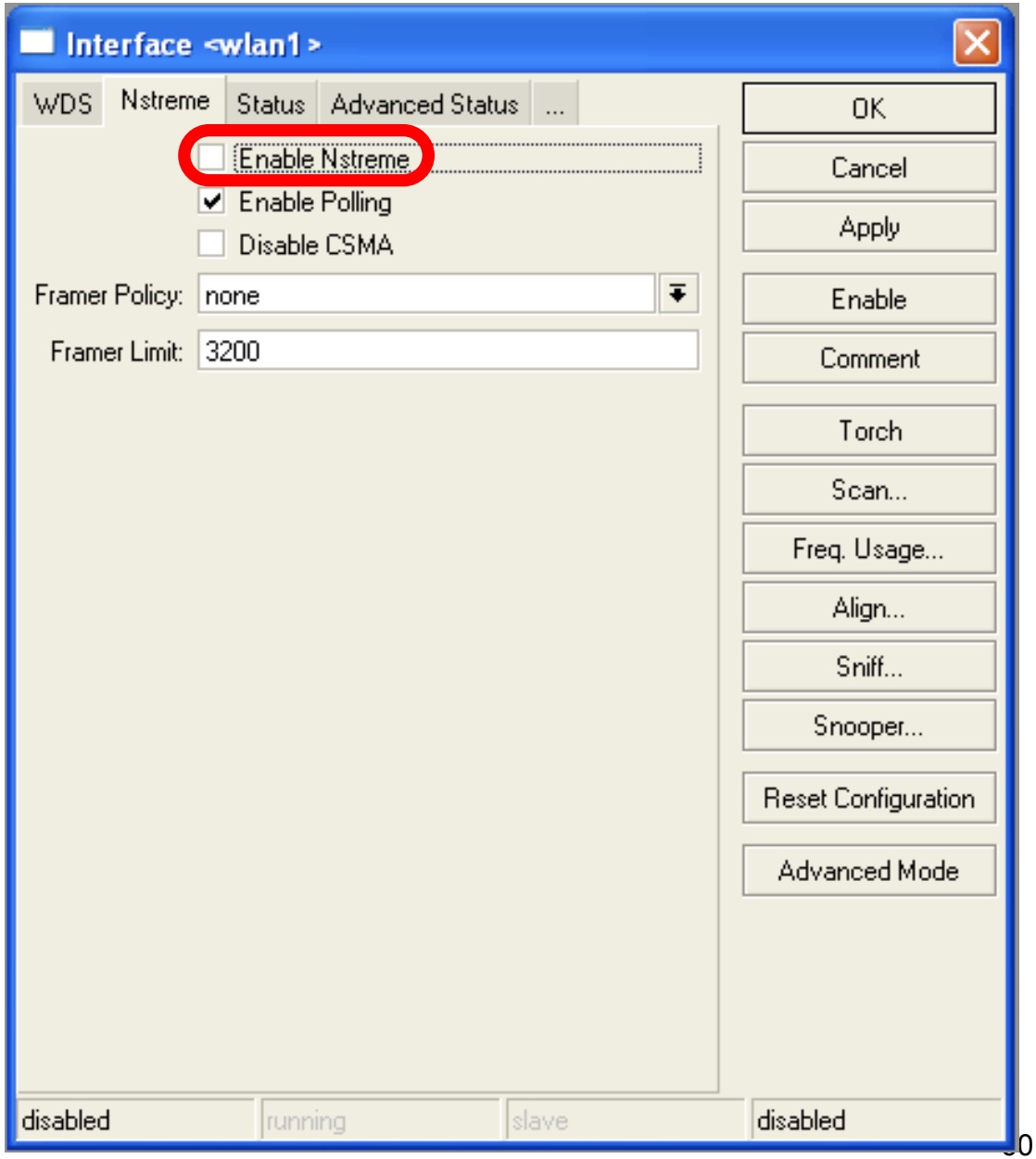
- Правила Access-List имеют высший приоритет
- Если между клиентами есть связь, то проверьте правила в access-list

Nstreme

- Собственный протокол беспроводной связи MikroTik
- Улучшает качество беспроводной связи, увеличивается пропускная способность, увеличивается дальность линков
- Чтобы использовать в вашей сети, включите данный протокол на всех беспроводных устройствах в вашей сети

Nstreme Lab

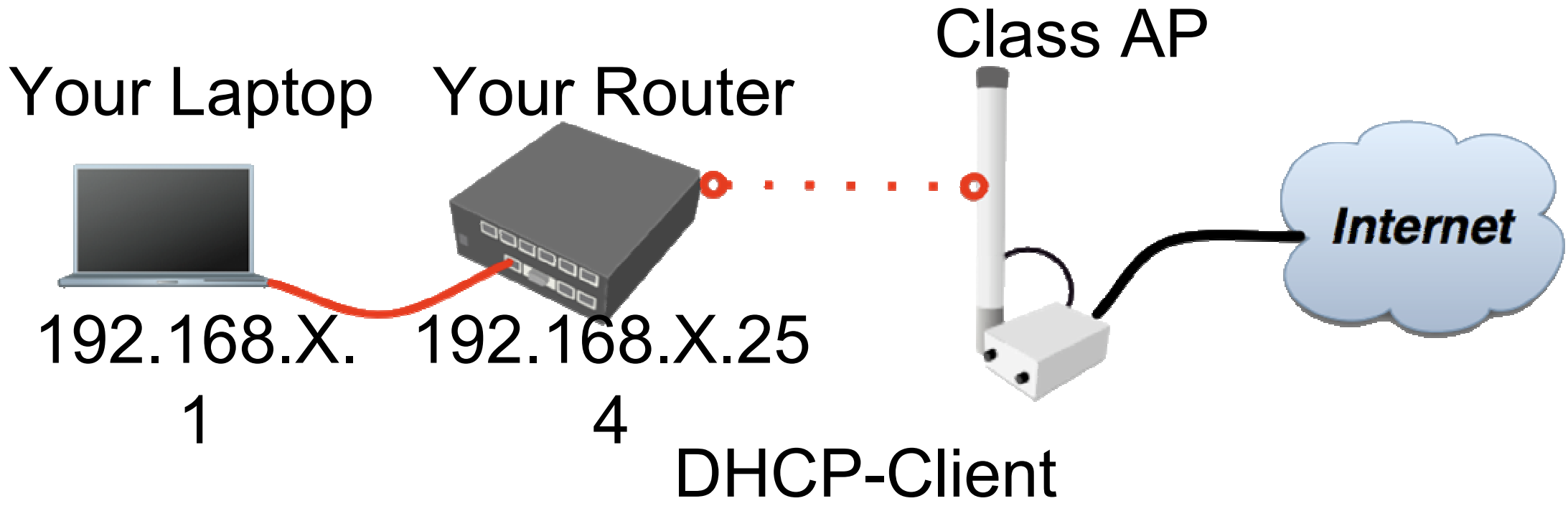
- Включите Nstreme на вашем роутере
- **Nstreme** должен быть включен на обоих(всех) роутерах



Summary

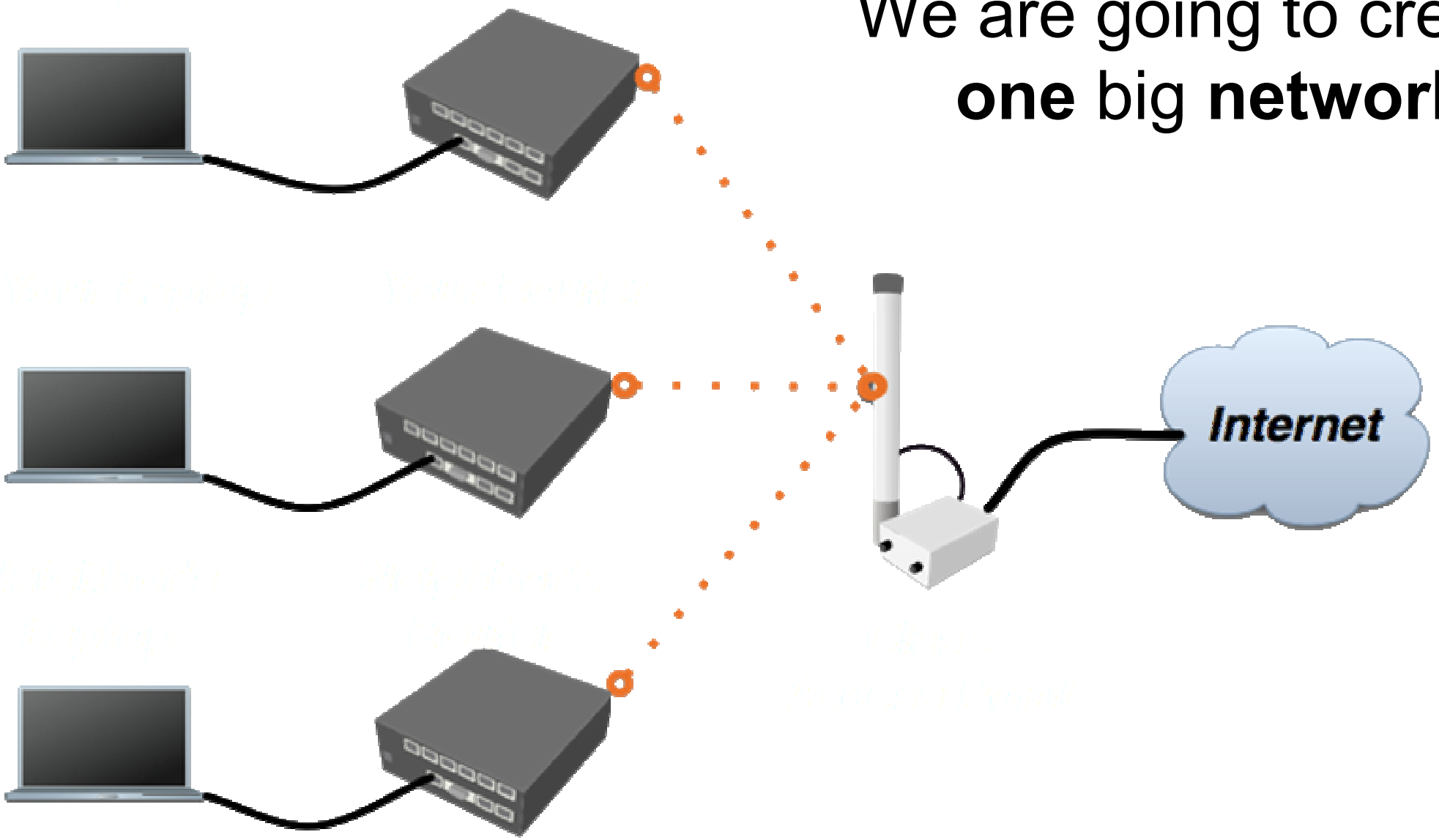
Bridging

Bridge Wireless Network

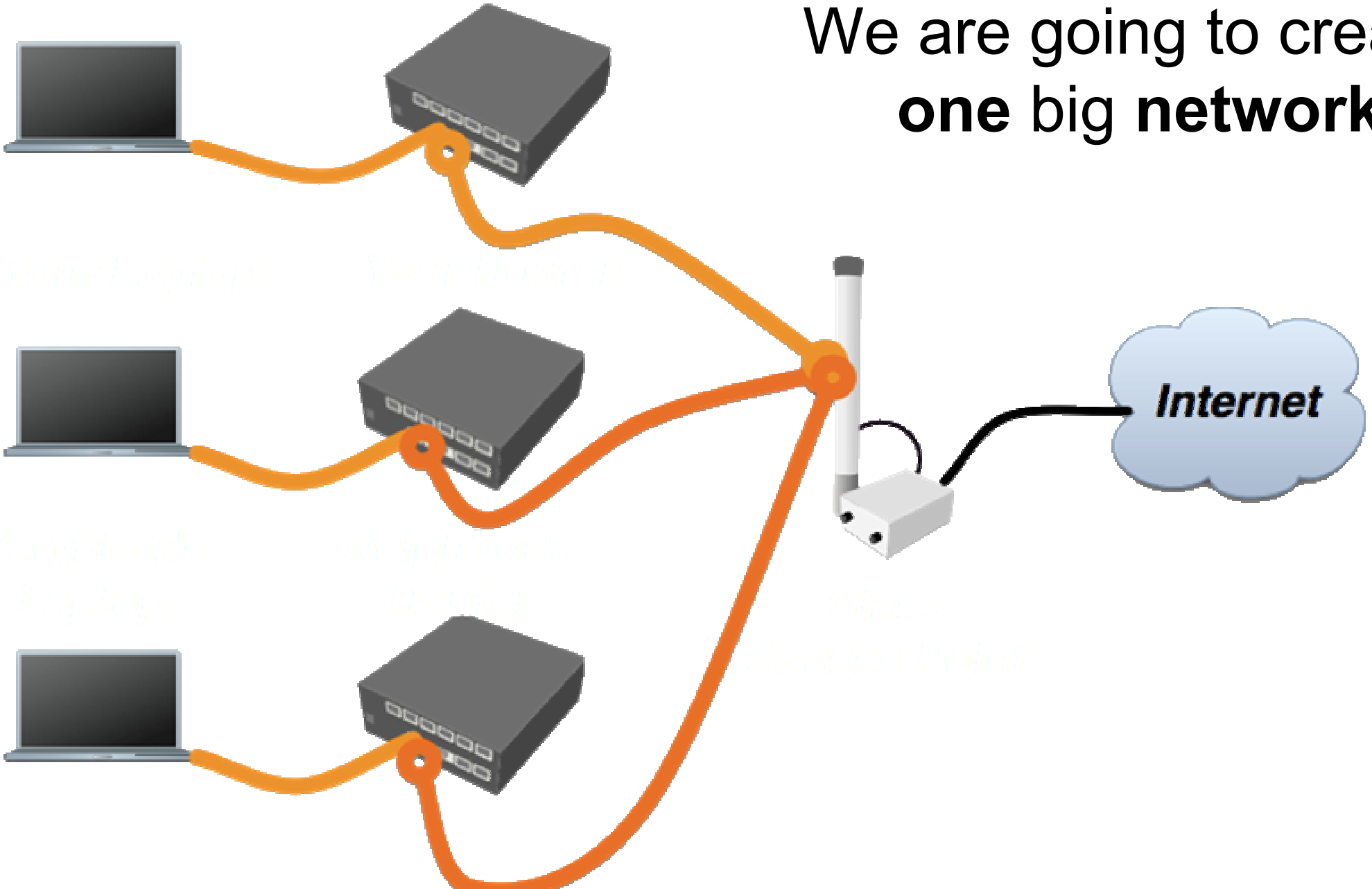


- Let's get back to our configuration

Bridge Wireless Network



Bridge Wireless Network



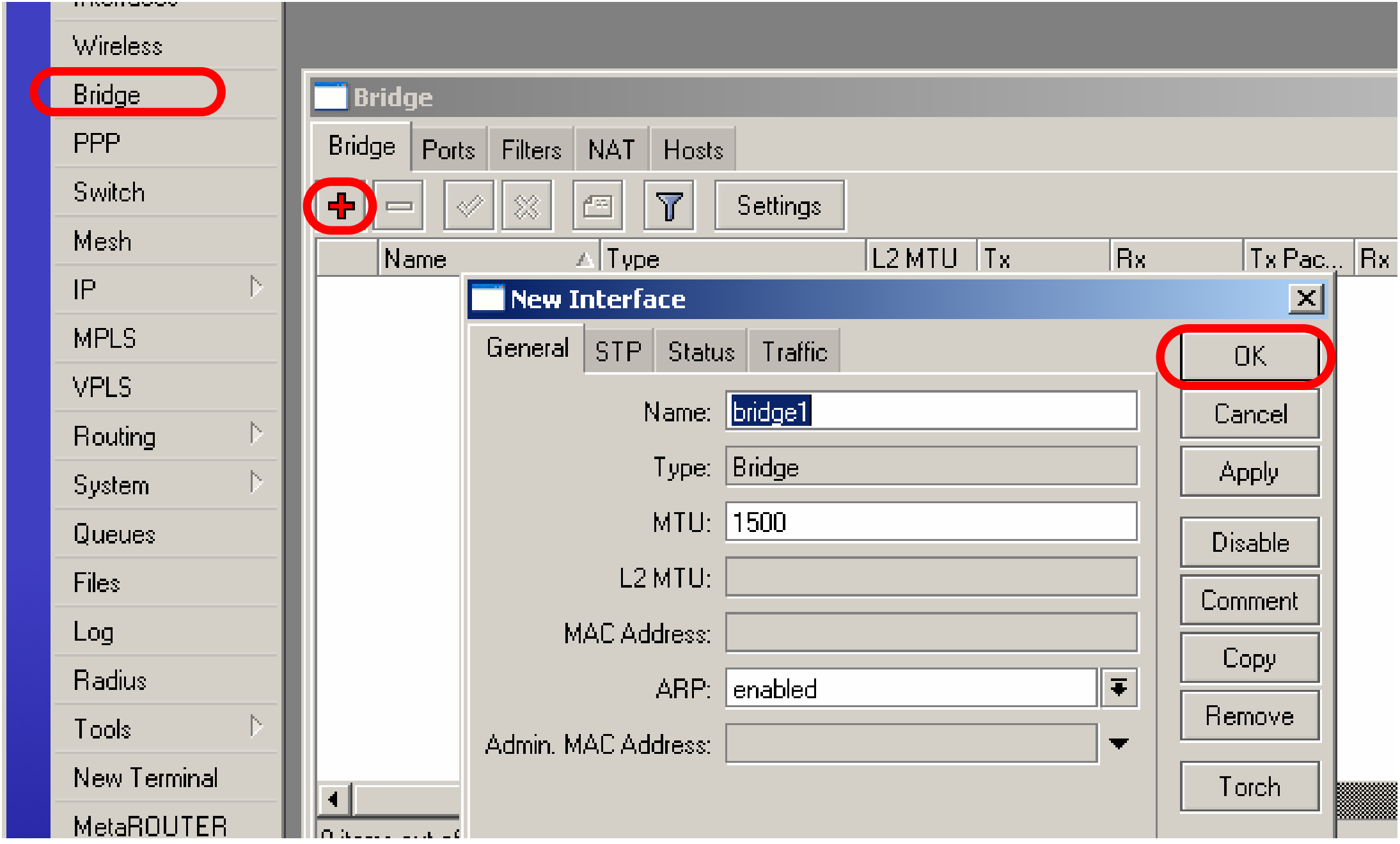
Bridge

- Мы сделаем bridge локального интерфейса с беспроводным интерфейсом
- Все ваши ноутбуки будут в одной сети

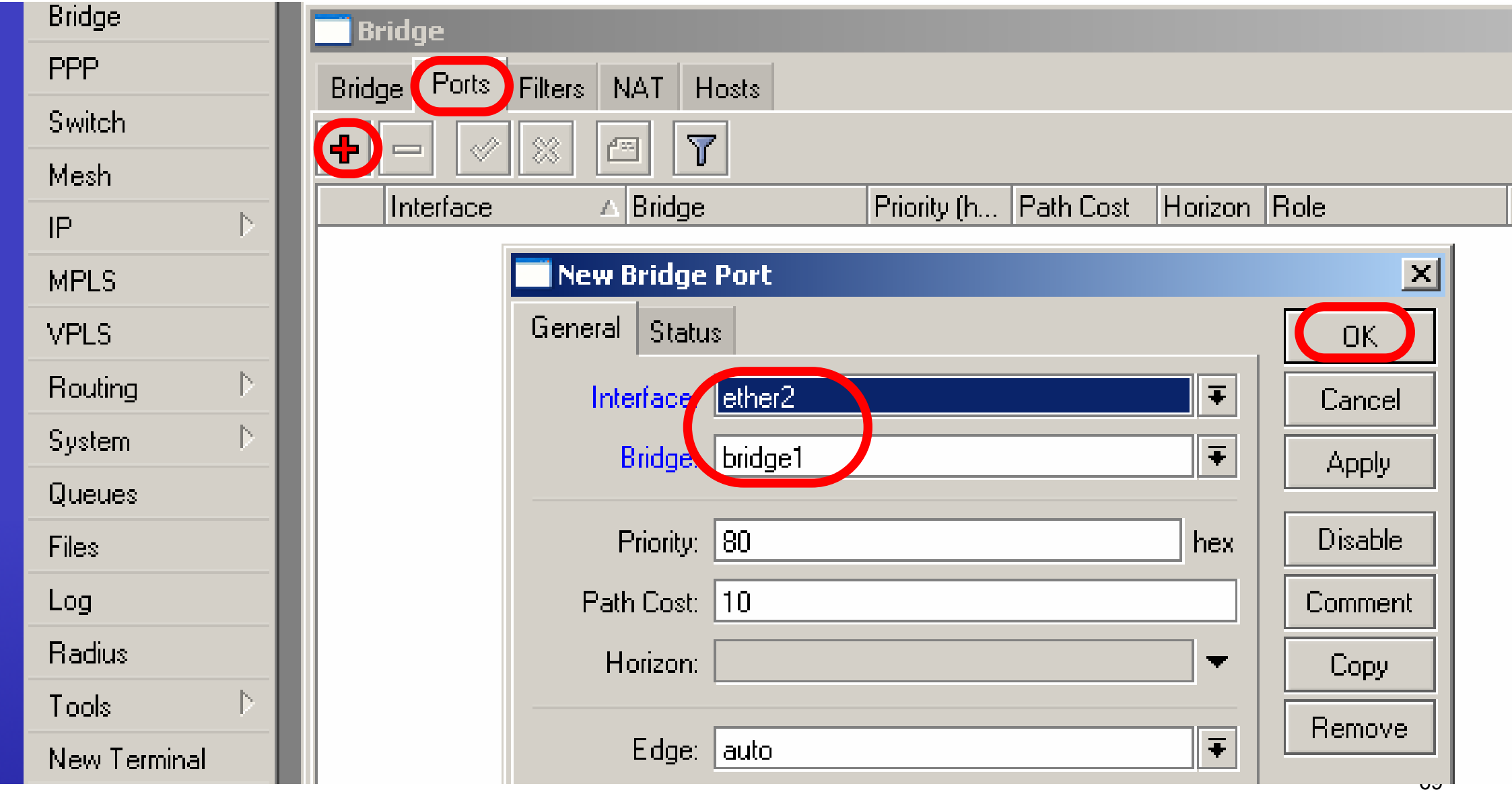
Bridge

- Для создания bridge вам необходимо создать bridge интерфейс
- И добавить интерфейсы в bridge ports

Bridge


Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
VPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Bridge
Bridge
Ports
Filters
NAT
Hosts
Settings
Name
Type
L2 MTU
Tx
Rx
Tx Pac...
Rx
New Interface
General
STP
Status
Traffic
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Name:
bridge1
Type:
Bridge
MTU:
1500
L2 MTU:
MAC Address:
ARP:
enabled
Admin. MAC Address:

Bridge - demo


Bridge
PPP
Switch
Mesh
IP
MPLS
VPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Bridge
Bridge
Ports
Filters
NAT
Hosts
Interface
Bridge
Priority (h...
Path Cost
Horizon
Role
New Bridge Port
General
Status
Interface:
ether2
Bridge:
bridge1
Priority:
80
hex
Path Cost:
10
Horizon:
Edge:
auto
OK
Cancel
Apply
Disable
Comment
Copy
Remove

Bridge

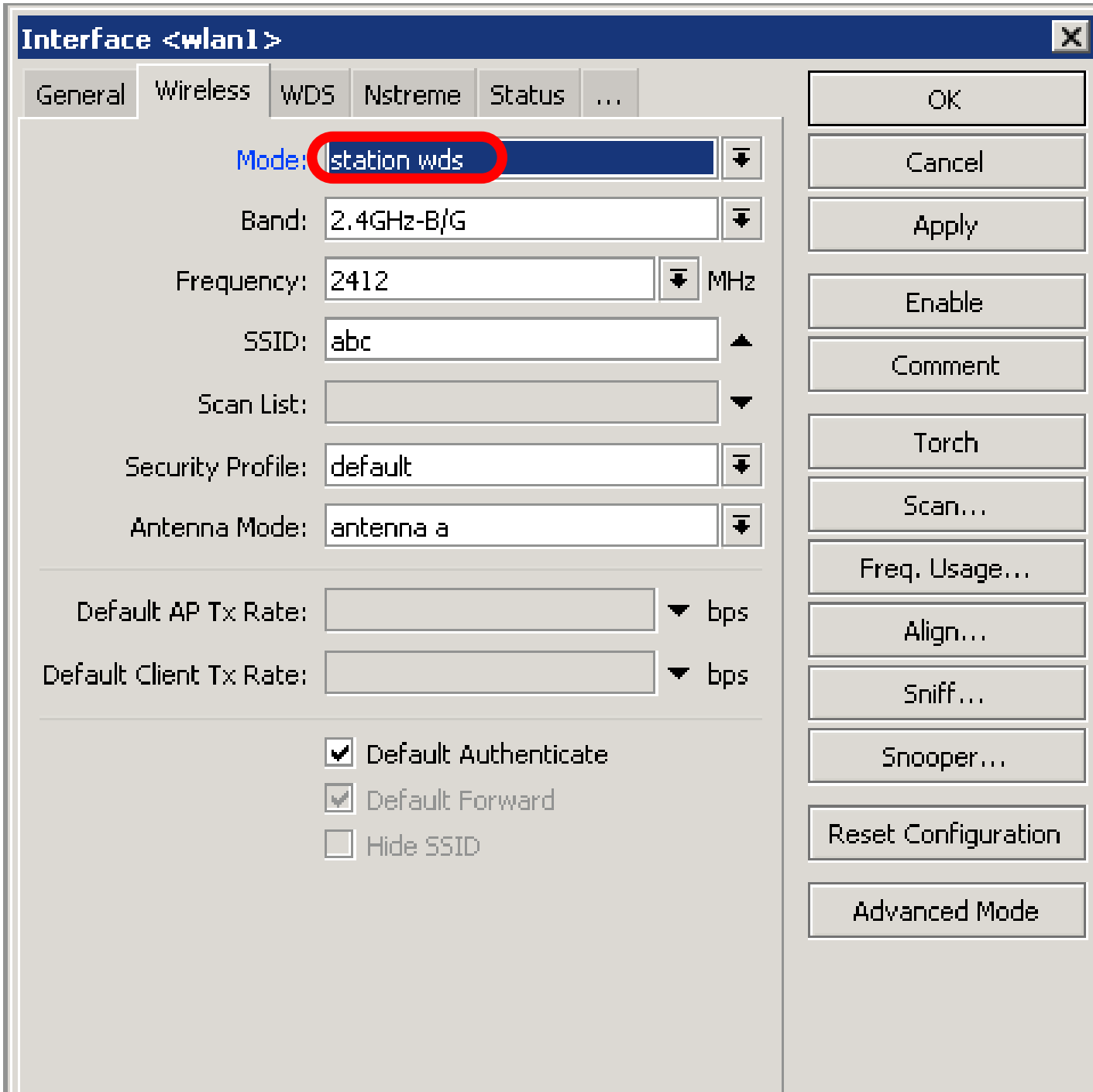
- Нет проблем забриджживать Ethernet интерфейсы
- Wireless Clients (**mode=station**) не поддерживает **bridging** это ограничение стандарта 802.11

Bridge Wireless

- **WDS** позволяет добавить клиентов wireless в **bridge**
- WDS (Wireless Distribution System) позволяет построить связь между Access Point и Access Point

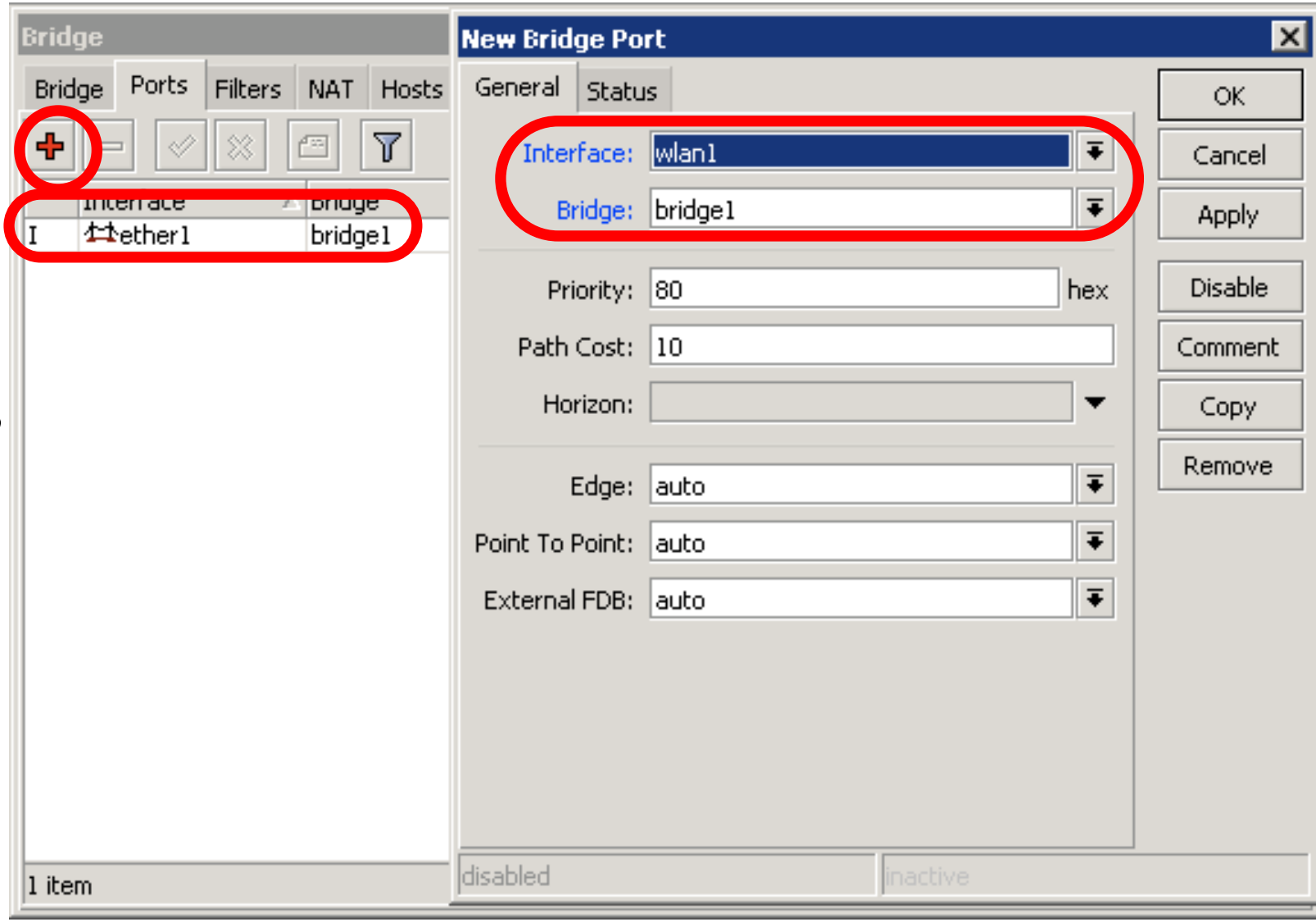
Установка режима WDS

- **Station-wds** это специальный клиентский режим с поддержкой WDS



Add Bridge Ports

- Добавьте публичный и локальный интерфейсы в bridge
- Ether1 (local), wlan1 (public)

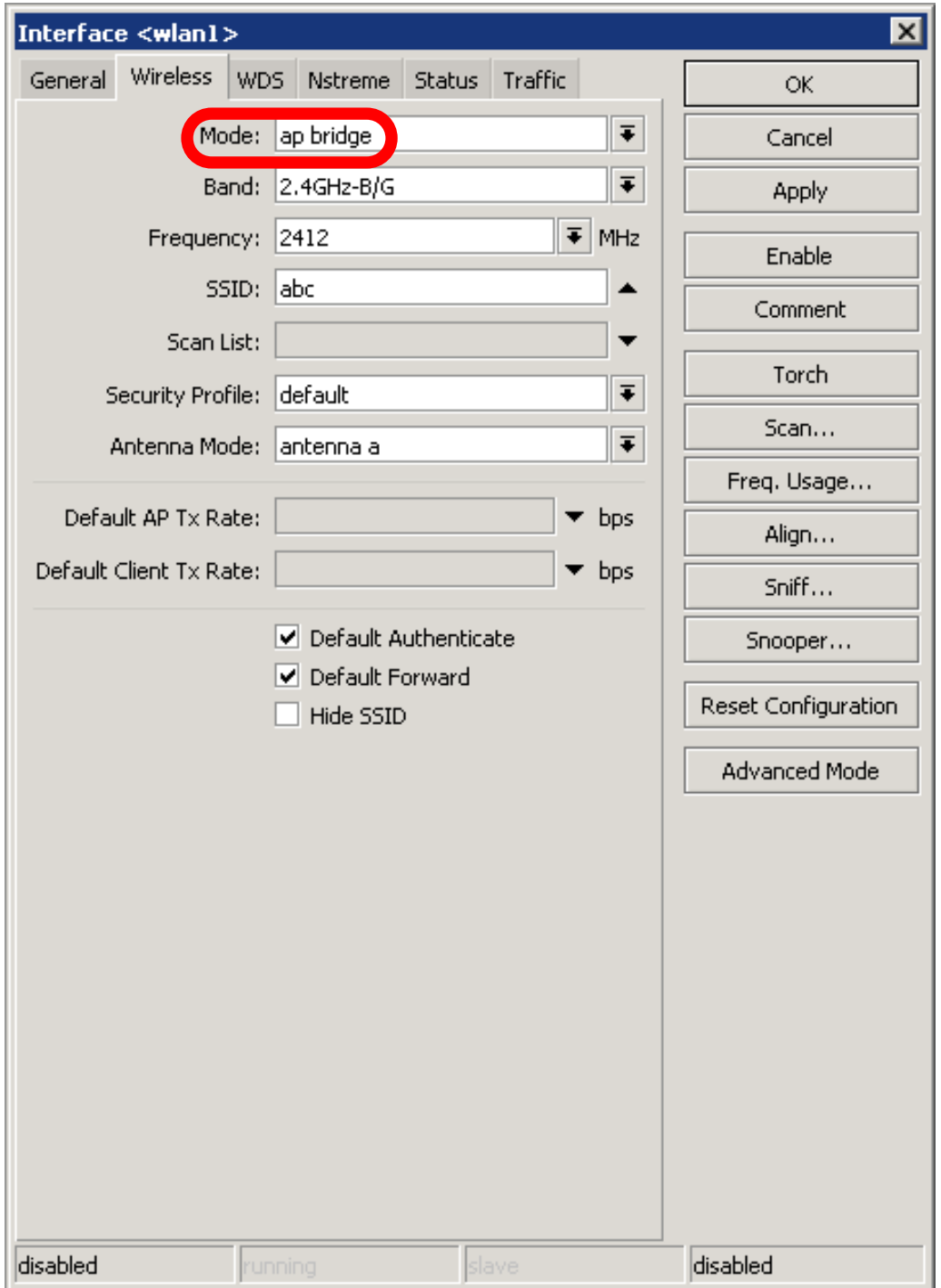


Access Point WDS

- Для включения WDS на AP-bridge, используйте режим mode=dynamic-mesh
- WDS интерфейсы будут создаваться на лету
- Use default bridge for WDS interfaces
- Добавит Wireless интерфейс Interface в Bridge

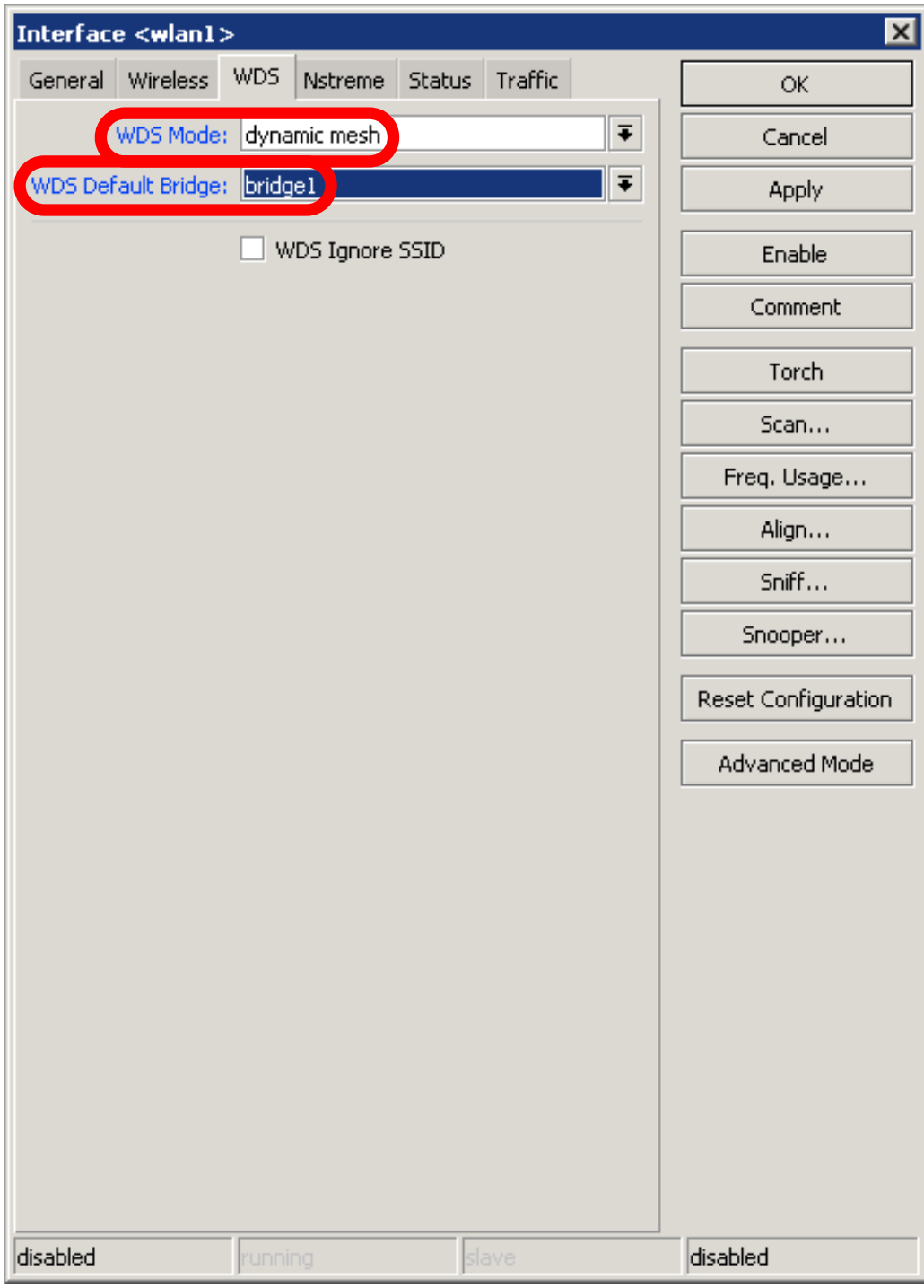
AP-bridge

- Set AP-bridge settings
- Add Wireless interface to **bridge**



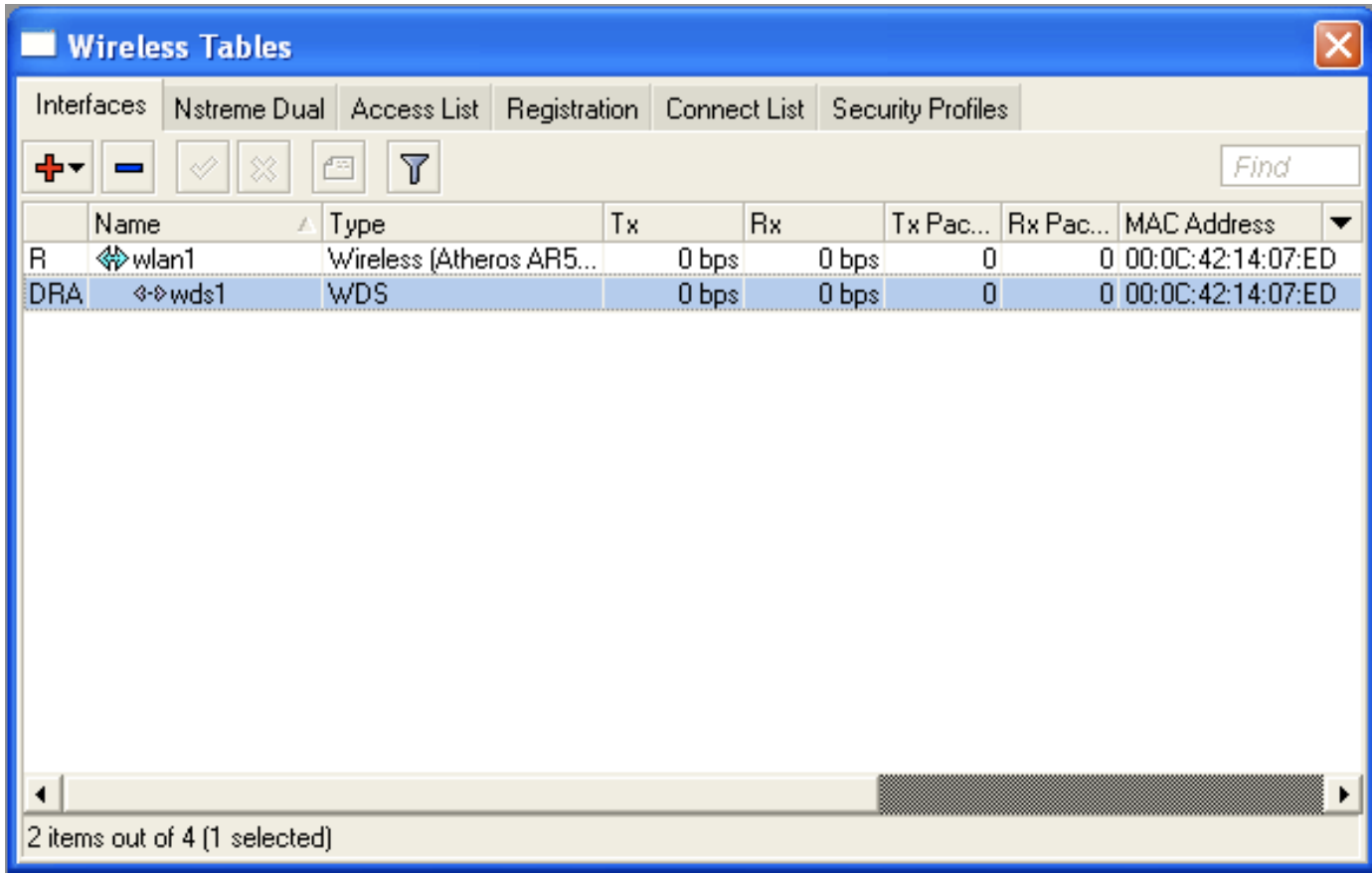
WDS configuration

- Use **dynamic-mesh** WDS mode
- WDS interfaces are created on the fly
- Others AP should use **dynamic-mesh** too



WDS

- WDS link is established
- Dynamic interface is present



WDS Lab

LAB

- Отключите правило **masquerade**
- Отключите **DHCP-client** на вашем роутере на wlan1 интерфейсе
- Используйте режим mode=**station-wds** на вашем роутере для подключения к Тренерской точки доступа
- Включите DHCP на вашем ноутбуке
- Теперь вы можете пинговать ваших соседей, вы в одной сети 192.168.111.0/24