Severay. Works Different

Запуск сети на **YotaArena**

Трудности и их решения

Severay. Works Different

Об авторе

Александр Кокшаров. Москва, Россия

Сертификаты Mikrotik
MTCNA, MTCTCE, MTCWE, MTCRE
MUM 2017,Россия

Severay. Works Different

О компании

14
лет в бизнесе
56
компаний партнеров
231
внедренных решений
61
выполненных проектов

Наша компания ориентирована на разработку и реализацию комплексных решений в области, ИТ и строительства инновационных объектов в крупнейших города России.

Основная задача компании - создание высококачественных комплексных решений "под ключ", представляющих собой единый законченный продукт, максимально соответствующий требованиям и задачам клиента.

Деятельность Severay - это прежде всего предоставление комплексного решения для каждого из Заказчиков, рассчитанного на основании нашего опыта, стандартов и качества.

Severay. Works Different

Требования к сети

Требования к WAN и LAN

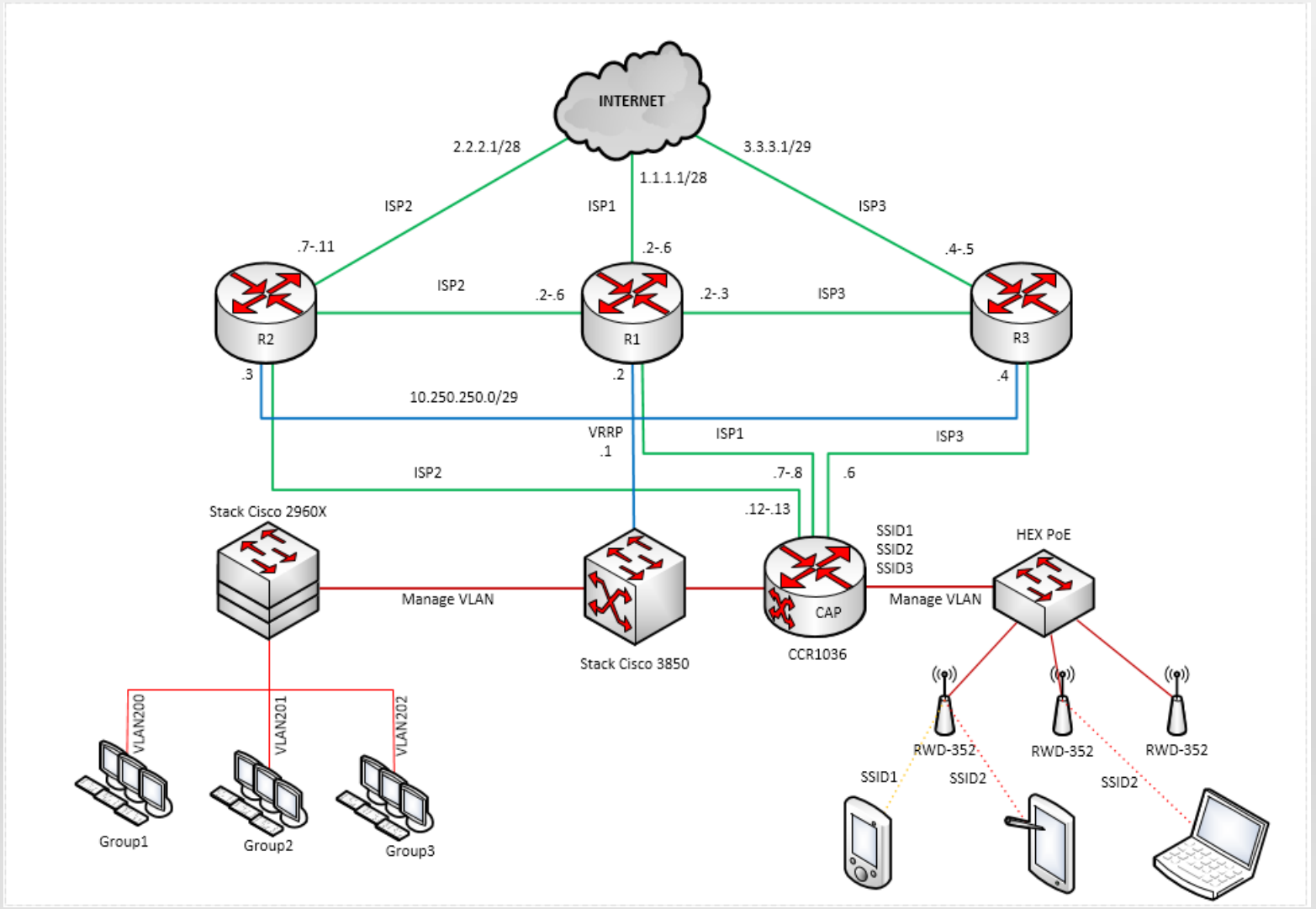
- обеспечение бесперебойной работы пользователей в локальной сети и интернет.
- два-три независимых ISP канала с суммарной пропускной способностью до 10Гб/с с «горячим» резервированием.
- распределение нагрузки между внешними каналами на уровне source IP
- защита от внешних DDoS и других атак.

Требования к WiFi

- иметь централизованное управление точками через контроллер
- поддерживать не менее 2 SSID
- поддерживать бесшовность
- поддерживать внешнюю авторизацию (для реализации идентификации абонента посредством SMS)
- обеспечивать в пиковой нагрузке достаточно комфортное пользование в размере не менее 4-5 мегабит на клиента.
- обслуживать одновременно до 600 подключений.

Severay. Works Different

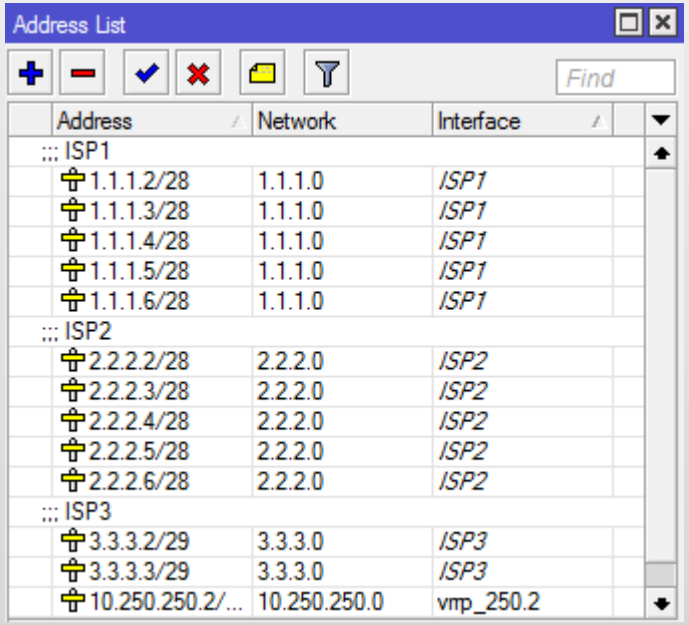
Логическая схема сети **YotaArena**



Severay. Works Different

Настройка маршрутизаторов CCR1072

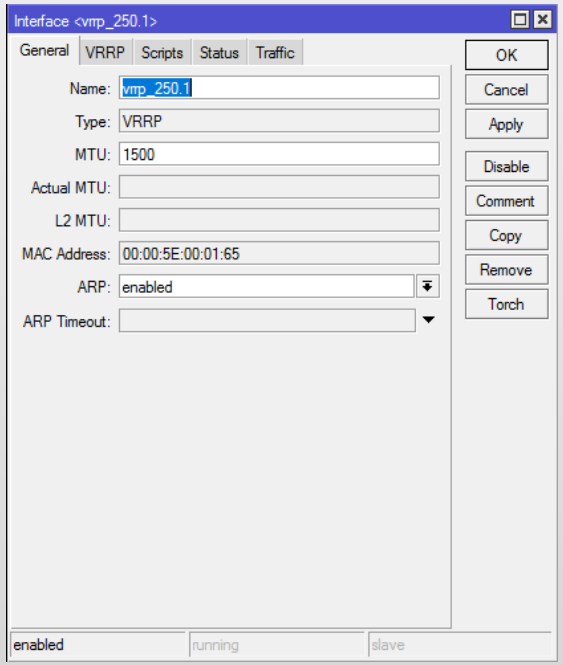
R1 (master)

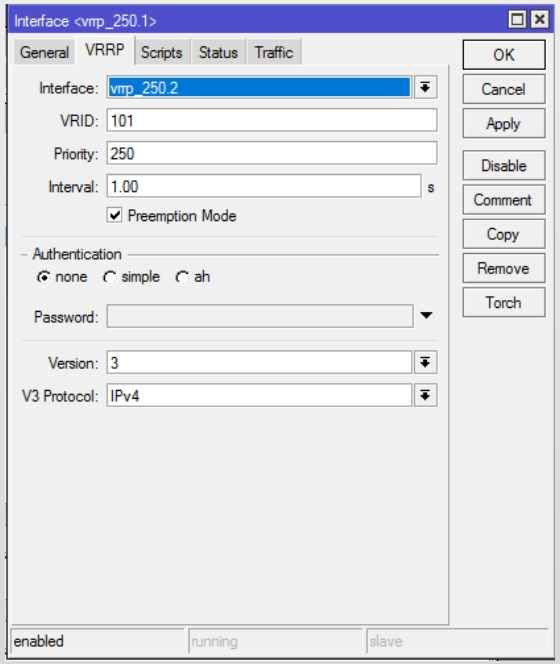



```
/ip address
add address=1.1.1.2/28 comment=ISP1 interface=ISP1 network=1.1.1.0
add address=1.1.1.3/28 interface=ISP1 network=1.1.1.0
add address=1.1.1.4/28 interface=ISP1 network=1.1.1.0
add address=1.1.1.5/28 interface=ISP1 network=1.1.1.0
add address=1.1.1.6/28 interface=ISP1 network=1.1.1.0
add address=2.2.2.2/28 comment=ISP2 interface=ISP2 network=2.2.2.0
add address=2.2.2.3/28 interface=ISP2 network=2.2.2.0
add address=2.2.2.4/28 interface=ISP2 network=2.2.2.0
add address=2.2.2.5/28 interface=ISP2 network=2.2.2.0
add address=2.2.2.6/28 interface=ISP2 network=2.2.2.0
add address=3.3.3.2/29 comment=ISP3 interface=ISP3 network=3.3.3.0
add address=3.3.3.3/29 interface=ISP3 network=3.3.3.0
add address=10.250.250.2/29 interface=vrrp_250.2 network=10.250.250.0
```

- Назначаем несколько IP-адресов из пула подключенного провайдера: 1.1.1.0/29, 2.2.2.0/28, 3.3.3.0/29 на внешние интерфейсы R1
- Назначаем IP-адрес 10.250.250.2 на внутренний интерфейс «vrrp_250.2»

R1 (master)

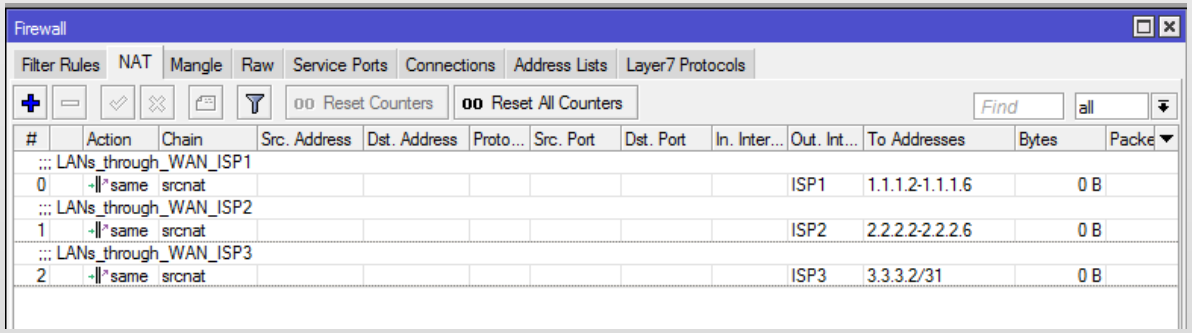





```
/interface vrrp
add interface=vrrp_250.2 name=vrrp_250.1 priority=250 vrid=101
/ip address
add address=10.250.250.1/29 interface=vrrp_250.1 network=10.250.250.0
```

- Создаем виртуальный VRRP интерфейс VRRP_250.1 с приоритетом 250, и VRID 101. Применяем его к внутреннему интерфейсу «vrrp_250.2». Preemption Mode оставляем включенным.
- Назначаем новому интерфейсу vrrp_250.1 IP-адрес 10.250.250.1

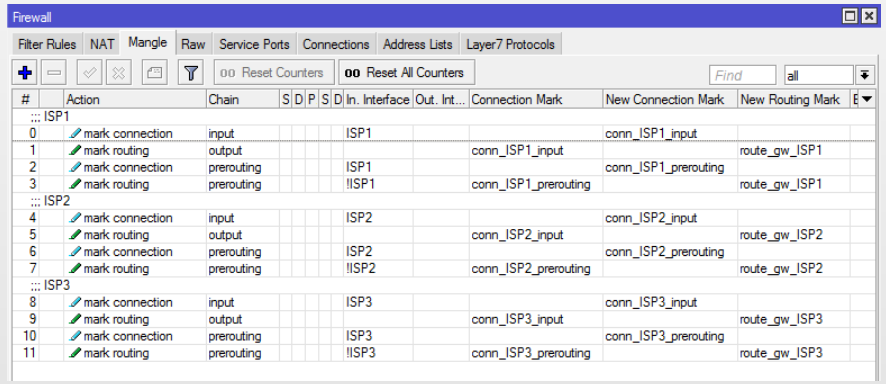
R1 (master)




```
/ip firewall nat
add action=same chain=srcnat comment=LANs_through_WAN_ISP1 out-interface=ISP1 \
    same-not-by-dst=no to-addresses=1.1.1.2-1.1.1.6
add action=same chain=srcnat comment=LANs_through_WAN_ISP2 out-interface=ISP2 \
    same-not-by-dst=no to-addresses=2.2.2.2-2.2.2.6
add action=same chain=srcnat comment=LANs_through_WAN_ISP3 out-interface=ISP3 \
    same-not-by-dst=no to-addresses=3.3.3.2-3.3.3.3
```

- Для распределения исходящих соединений при настройке SRC-NAT в поле Action выбираем «same», а в поле «To Addresses» вносим назначенные на внешние интерфейсы IP-адреса: 1.1.1.2-1.1.1.6, 2.2.2.2-2.2.2.6, 3.3.3.2-3.3.3.3

R1 (master)




```
add action=mark-connection chain=input comment=ISP1 in-interface=ISP1 new-connection-mark=conn_ISP1_input passthrough=yes
add action=mark-routing chain=output connection-mark=conn_ISP1_input new-routing-mark=route_gw_ISP1 passthrough=no
add action=mark-connection chain=prerouting in-interface=ISP1 new-connection-mark=conn_ISP1_prerouting passthrough=yes
add action=mark-routing chain=prerouting connection-mark=conn_ISP1_prerouting in-interface=!ISP1 new-routing-mark=route_gw_ISP1 passthrough=no
add action=mark-connection chain=input comment=ISP2 in-interface=ISP2 new-connection-mark=conn_ISP2_input passthrough=yes
add action=mark-routing chain=output connection-mark=conn_ISP2_input new-routing-mark=route_gw_ISP2 passthrough=no
add action=mark-connection chain=prerouting in-interface=ISP2 new-connection-mark=conn_ISP2_prerouting passthrough=yes
add action=mark-routing chain=prerouting connection-mark=conn_ISP2_prerouting in-interface=!ISP2 new-routing-mark=route_gw_ISP2 passthrough=no
add action=mark-connection chain=input comment=ISP3 in-interface=ISP3 new-connection-mark=conn_ISP3_input passthrough=yes
add action=mark-routing chain=output connection-mark=conn_ISP3_input new-routing-mark=route_gw_ISP3 passthrough=no
add action=mark-connection chain=prerouting in-interface=ISP3 new-connection-mark=conn_ISP3_prerouting passthrough=yes
add action=mark-routing chain=prerouting connection-mark=conn_ISP3_prerouting in-interface=!ISP3 new-routing-mark=route_gw_ISP3 passthrough=no
```

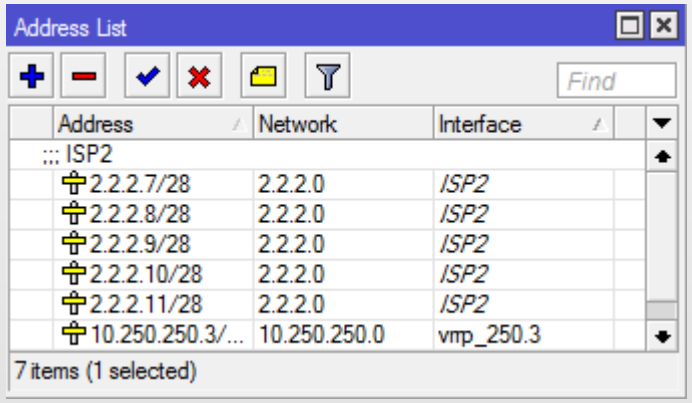
- Включаем маркировку входящих-исходящих соединений и пакетов в Mangle для дальнейшей маршрутизации.

R1 (master)

```
/ip route
add check-gateway=arp distance=1 gateway=1.1.1.1
add check-gateway=arp distance=2 gateway=2.2.2.1
add check-gateway=arp distance=3 gateway=3.3.3.1
add check-gateway=arp distance=1 gateway=1.1.1.1 routing-mark=route_gw_ISP1
add check-gateway=arp distance=1 gateway=2.2.2.1 routing-mark=route_gw_ISP2
add check-gateway=arp distance=1 gateway=3.3.3.1 routing-mark=route_gw_ISP3
```

- Добавляем в таблицу маршрутизации новые записи

R2 и R3 (slave)



R2

/ip address

add address=2.2.2.7/28 comment=ISP2 interface=ISP2 network=2.2.2.0

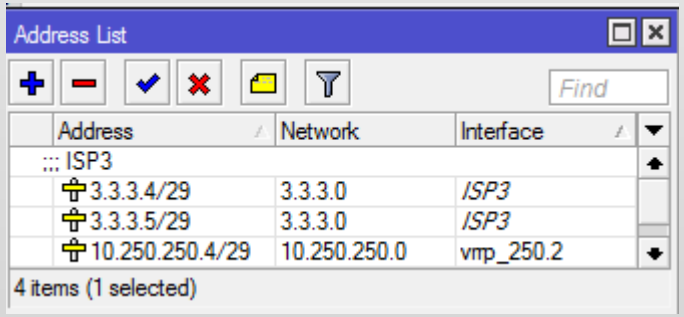
add address=2.2.2.8/28 interface=ISP2 network=2.2.2.0

add address=2.2.2.9/28 interface=ISP2 network=2.2.2.0

add address=2.2.2.10/28 interface=ISP2 network=2.2.2.0

add address=2.2.2.11/28 interface=ISP2 network=2.2.2.0

add address=10.250.250.3/29 interface=vrrp_250.3 network=10.250.250.0



R3

/ip address

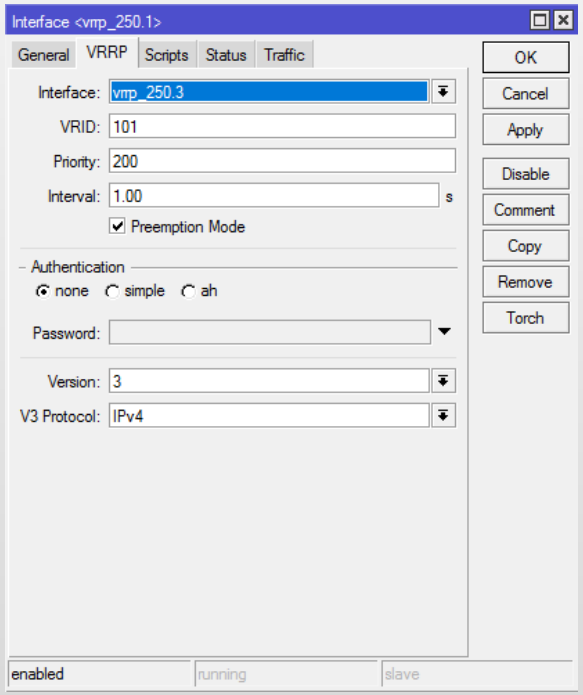
add address=3.3.3.4/29 comment=ISP3 interface=ISP3 network=3.3.3.0

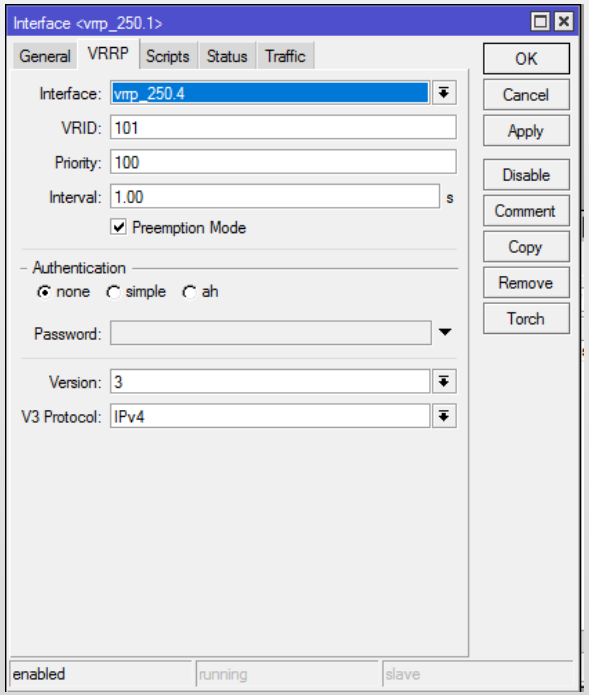
add address=3.3.3.5/29 interface=ISP3 network=3.3.3.0

add address=10.250.250.4/29 interface=vrrp_250.4 network=10.250.250.0

- Назначаем несколько IP-адресов из пула подключенного провайдера: 2.2.2.0/28, 3.3.3.0/29 на внешние интерфейсы R2 и R3
- На R2 добавляем IP-адрес 10.250.250.3 на внутренний интерфейс «vrrp_250.3»
- На R3 добавляем IP-адрес 10.250.250.4 на внутренний интерфейс «vrrp_250.4»

R2 и R3 (slave)





R2

/interface vrrp

add interface=vrrp_250.3 name=vrrp_250.1 priority=200 vrid=101

/ip address

add address=10.250.250.1/29 interface=vrrp_250.1 network=10.250.250.0

R3

/interface vrrp

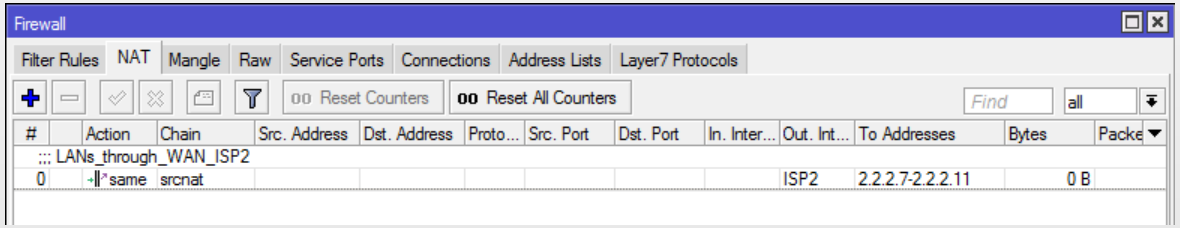
add interface=vrrp_250.4 name=vrrp_250.1 priority=100 vrid=101

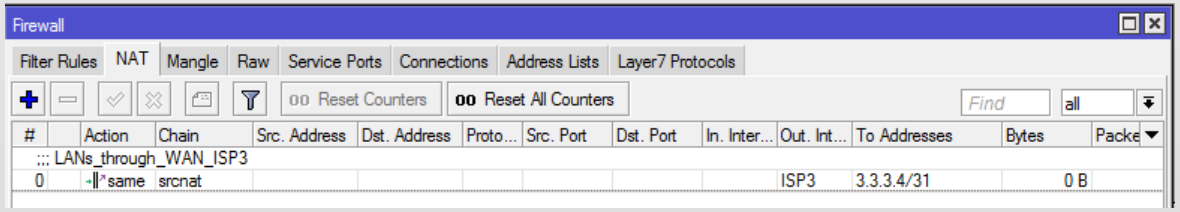
/ip address

add address=10.250.250.1/29 interface=vrrp_250.1 network=10.250.250.0

- На R2 создаем виртуальный VRRP интерфейс VRRP_250.1 с приоритетом 200, и VRID 101. Применяем его к внутреннему интерфейсу «vrrp_250.3».
- На R3 создаем виртуальный VRRP интерфейс VRRP_250.1 с приоритетом 100, и VRID 101. Применяем его к внутреннему интерфейсу «vrrp_250.4».
- Назначаем новому интерфейсу vrrp_250.1 IP-адрес 10.250.250.1

R2 и R3 (slave)





R2

/ip firewall nat

add action=same chain=srcnat comment=LANs_through_WAN_ISP2 out-interface=ISP2 \

same-not-by-dst=no to-addresses=2.2.2.7-2.2.2.11

R2

/ip route

add check-gateway=arp distance=2 gateway=2.2.2.1

R3

add action=same chain=srcnat comment=LANs_through_WAN_ISP3 out-interface=ISP3 \

same-not-by-dst=no to-addresses=3.3.3.4-3.3.3.5

R3

/ip route

add check-gateway=arp distance=3 gateway=3.3.3.1

- Для распределения исходящих соединений при настройке SRC-NAT в поле Action выбираем «same», а в поле «To Addresses» вносим назначенные на внешние интерфейсы IP-адреса: R2 2.2.2.7-2.2.2.11, R3 3.3.3.4-3.3.3.5
- Добавляем маршрутизацию по умолчанию

Severay. Works Different

Развертывание сети **WiFi**

Радиообследование

На любом строящемся а так же эксплуатируемом объекте, где предполагается использование корпоративных беспроводных Wi-Fi сетей необходимо еще на стадии проектирования проводить радиообследование объекта.

Радиообследование поможет получить информацию по распространению, а так же затуханию сигнала внутри помещения с учетом всех особенностей объекта.
Проведение обследования поможет выявить места источников шумов и помех, которые в дальнейшем при эксплуатации могут мешать правильному функционированию сети.

На основании полученного результата можно добиться оптимальной расстановки Wi-Fi точек на объекте и после правильной настройки, получить эффективную работоспособную сеть, которая будет соответствовать требуемым характеристикам.

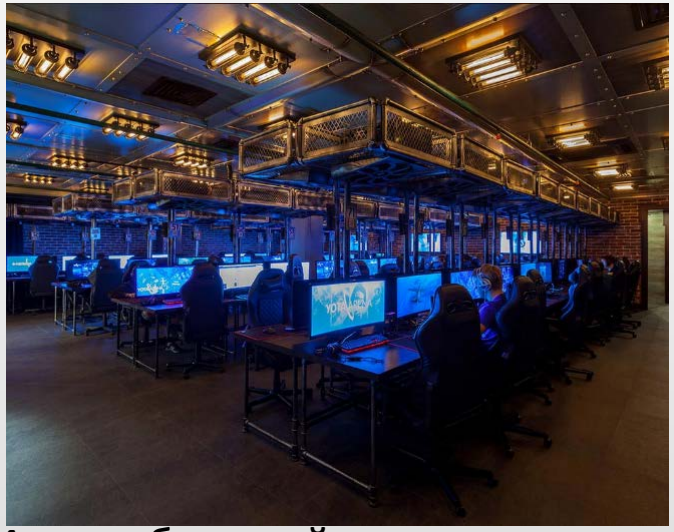
Проектные и фактические места установки точек WiFi

- Проектные места установки (после радиообследования)

- Фактические места установки

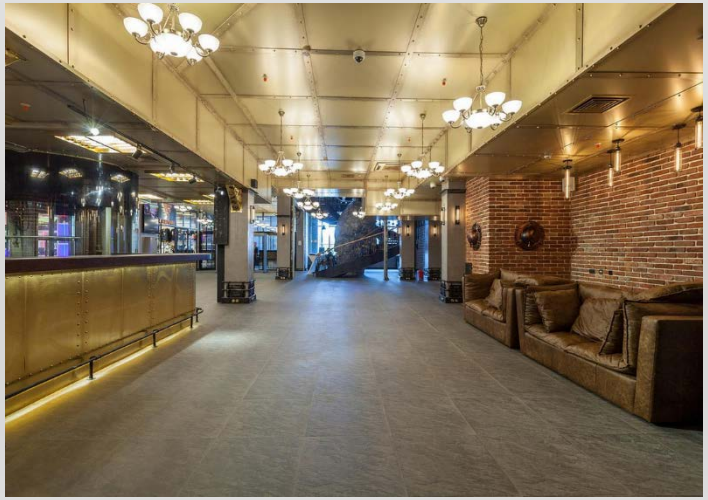
Severay. Works Different

Развертывание сети WiFi



«Подводные камни»

- Места с большой плотностью клиентов



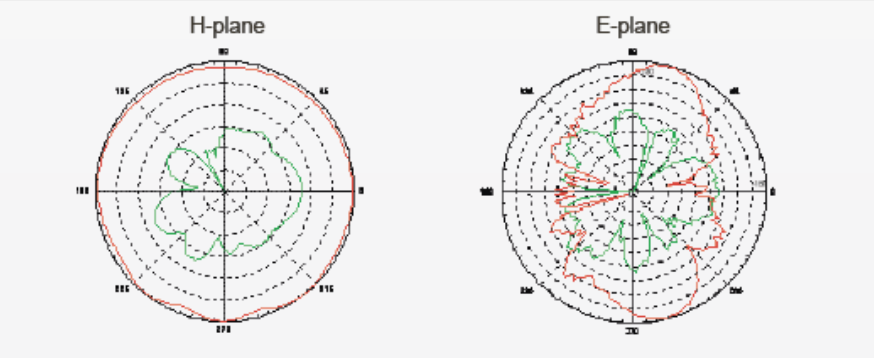
- Стены и потолок выполнены из радио-отражающего материала (латунь)

- Большое количество помех на пути прохождения радиосигнала

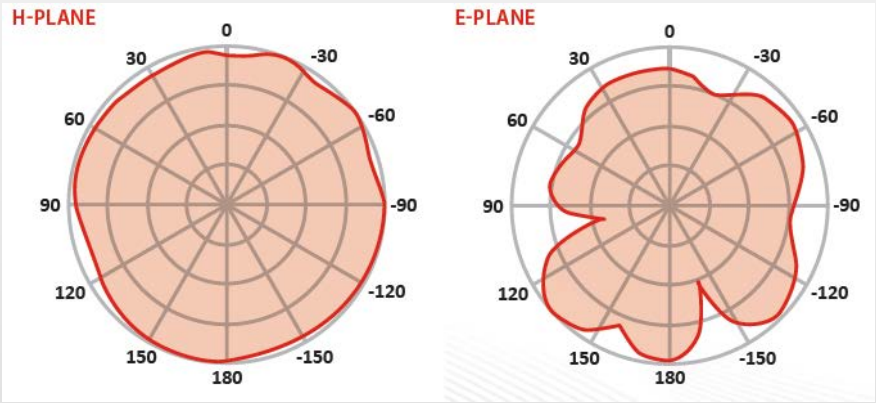
- Требуется стабильная работа WiFi в двух диапазонах 2.4Ггц и 5 Ггц на всем объекте

- Одновременная работа до 600 клиентов

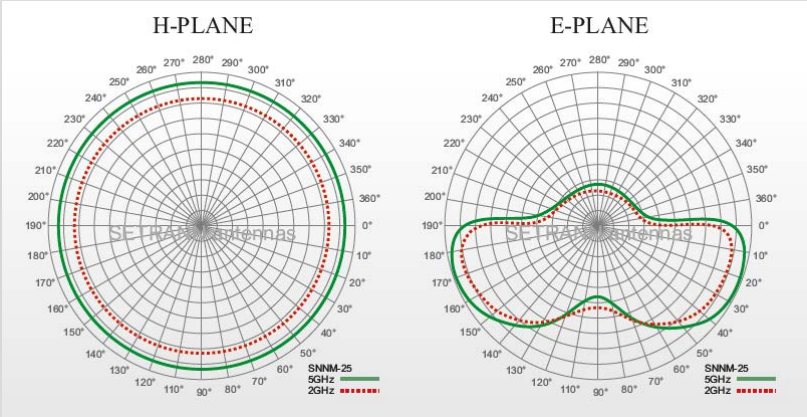
Диаграмма направленности распространения радиосигнала антенн



Mikrotik 2.4Ghz 5dBi Dipole antenna

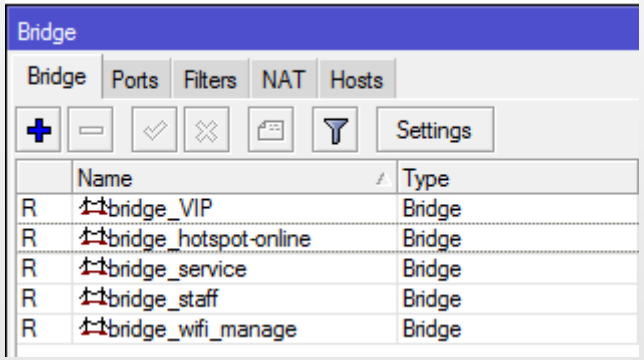


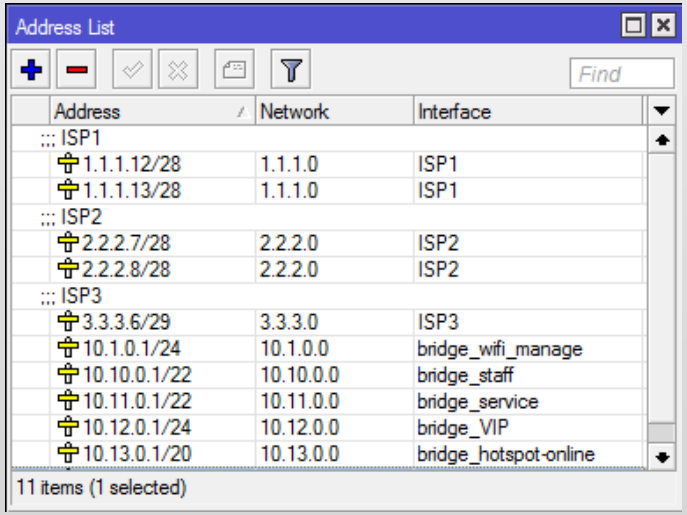
RF elements Omni Antenna 2.4/5 Ghz 2/3dBi



Antenna STYX 2.4/5 Ghz 3/5dBi
(используемая в САР)

Настройка CAPsMAN





/interface bridge

add arp=reply-only fast-forward=no name=bridge_VIP

add arp=reply-only fast-forward=no name=bridge_hotspot-online protocol-mode=none

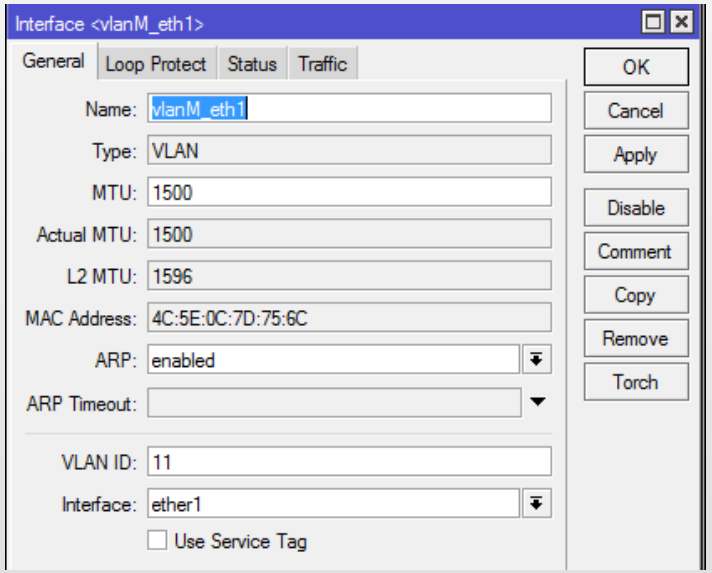
add arp=reply-only fast-forward=no name=bridge_service

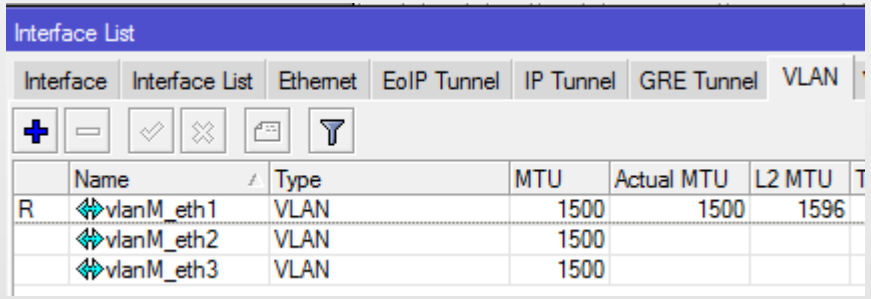
add arp=reply-only fast-forward=no name=bridge_staff

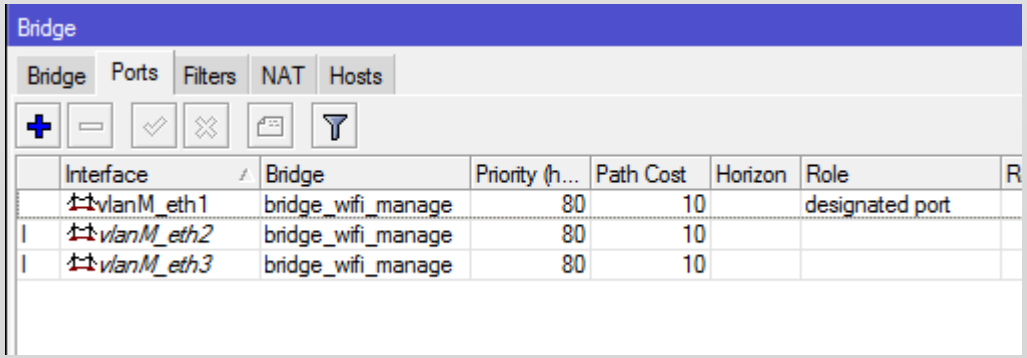
/ip address
add address=1.1.1.12/28 comment=ISP1 interface=ISP1 network=1.1.1.0
add address=1.1.1.13/28 interface=ISP1 network=1.1.1.0
add address=2.2.2.7/28 comment=ISP2 interface=ISP2 network=2.2.2.0
add address=2.2.2.8/28 interface=ISP2 network=2.2.2.0
add address=3.3.3.6/29 comment=ISP3 interface=ISP3 network=3.3.3.0
add address=10.1.0.1/24 interface=bridge_wifi_manage network=10.1.0.0
add address=10.10.0.1/22 interface=bridge_staff network=10.10.0.0
add address=10.11.0.1/22 interface=bridge_service network=10.11.0.0
add address=10.12.0.1/24 interface=bridge_VIP network=10.12.0.0
add address=10.13.0.1/20 interface=bridge_hotspot-online network=10.12.0.0

- Создаем необходимое количество Bridge-интерфейсов
- Добавляем режим работы arp=reply-only, чтобы у клиента не было возможности работать в WiFi сети с IP-адресом введенным вручную.
- Назначаем несколько IP-адресов из пула подключенного провайдера: 1.1.1.0/29, 2.2.2.0/28, 3.3.3.0/29 на внешние интерфейсы CAP
- Назначаем IP-адреса на внутренних Bridge-интерфейсах

Настройка CAPsMAN



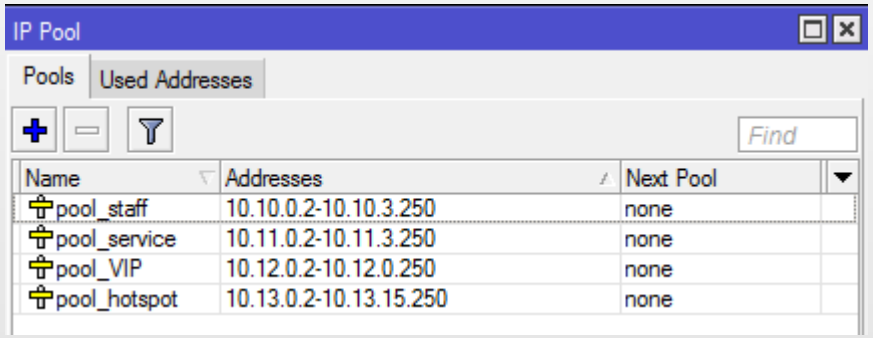


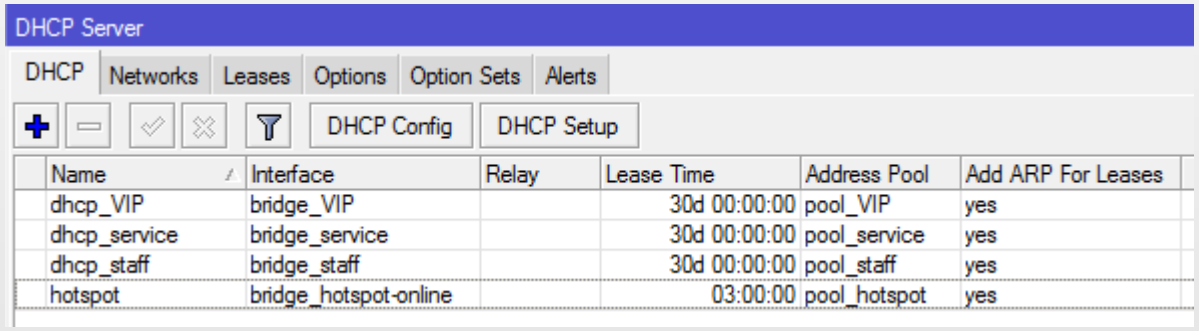


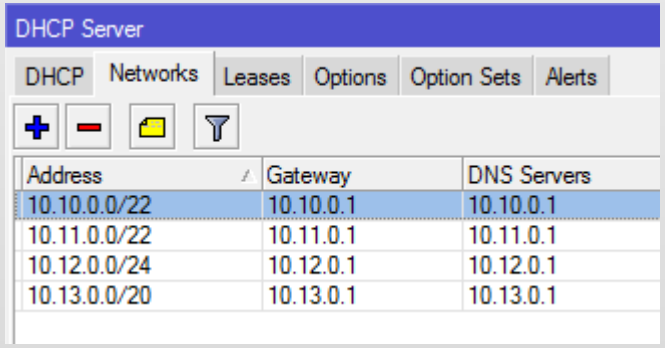

```
/interface vlan
add interface=ether1 name=vlanM_eth1 vlan-id=11
add interface=ether2 name=vlanM_eth2 vlan-id=11
add interface=ether3 name=vlanM_eth3 vlan-id=11

/interface bridge port
add bridge=bridge_wifi_manage interface=vlanM_eth1
add bridge=bridge_wifi_manage interface=vlanM_eth2
add bridge=bridge_wifi_manage interface=vlanM_eth3
```

- Для изоляции служебного сетевого трафика от AP к CAP, создаем VLAN 11 «Management LAN»
- Добавляем VLAN интерфейсы к физическим интерфейсам внутренней сети
- Объединяем интерфейсы Management LAN в Bridge_wifi_manage

Настройка CAPsMAN



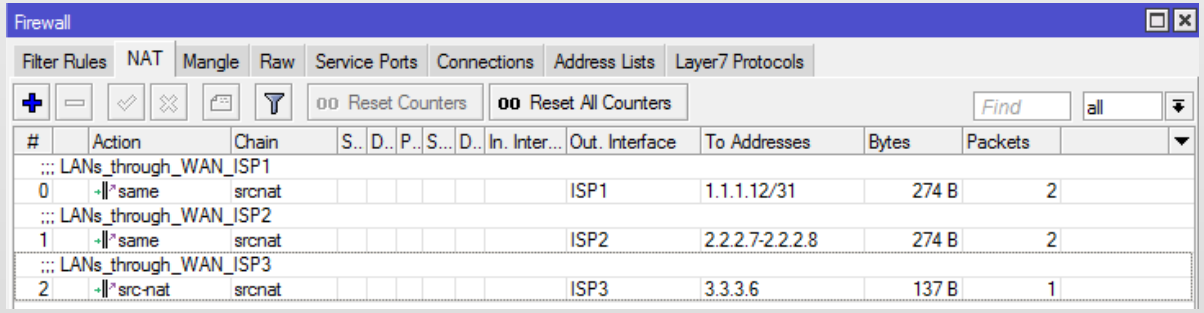





```
/ip pool
add name=pool_staff ranges=10.10.0.2-10.10.3.250
add name=pool_hotspot ranges=10.13.0.2-10.13.15.250
add name=pool_service ranges=10.11.0.2-10.11.3.250
add name=pool_VIP ranges=10.12.0.2-10.12.0.250
/ip dhcp-server
add add-arp=yes address-pool=pool_staff disabled=no interface=bridge_staff lease-time=4w2d name=dhcp_staff
add add-arp=yes address-pool=pool_service disabled=no interface=bridge_service lease-time=4w2d name=dhcp_service
add add-arp=yes address-pool=pool_VIP disabled=no interface=bridge_VIP lease-time=4w2d name=dhcp_VIP
add add-arp=yes address-pool=pool_hotspot disabled=no interface=bridge_hotspot-online lease-time=3h name=hotspot
```

- Создаем DHCP сервера и пулы для клиентов WiFi, при создании не забываем установить флажок на «Add ARP For Leases», для того, чтобы клиенты прописались в таблицу ARP и получили доступ к сети.

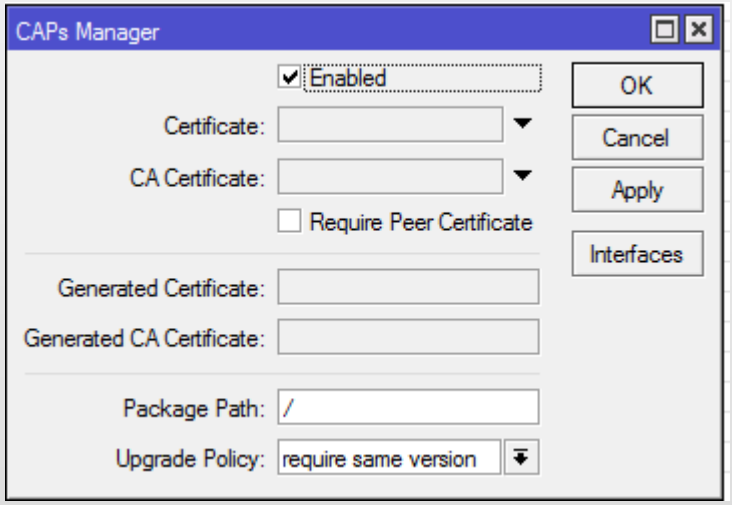
Настройка CAPsMAN




```
/ip firewall nat
add action=same chain=srcnat comment=LANs_through_WAN_ISP1 out-interface=ISP1 \
same-not-by-dst=no to-addresses=1.1.1.12-1.1.1.13
add action=same chain=srcnat comment=LANs_through_WAN_ISP2 out-interface=ISP2 \
same-not-by-dst=no to-addresses=2.2.2.7-2.2.2.8
add action=src-nat chain=srcnat comment=LANs_through_WAN_ISP3 out-interface=ISP3 \
to-addresses=3.3.3.6
```

- Для распределения исходящих соединений при настройке SRC-NAT в поле Action выбираем «same», а в поле «To Addresses» вносим назначенные на внешние интерфейсы IP-адреса R1-R2: 1.1.1.12-1.1.1.13, 2.2.2.7-2.2.2.8
- Т.к. ISP3 только один IP-адрес, выбираем в Action выбрать «src-nat». В поле «To Address» вносим IP-адрес 3.3.3.6

Настройка CAPsMAN



/caps-man manager

set enabled=yes package-path=/ upgrade-policy=require-same-version

- Переходим в раздел CAPsMAN и включаем управление AP на контроллере WiFi
- В поле «Package Path» прописываем директорию, откуда при необходимости AP будут брать обновленные прошивки
- Для автоматического обновления AP после обновления CAP, в поле «Upgrade Policy» выбираем режим «suggest same version» или «require same version» (советовать или требовать обновления AP)

Настройка CAPsMAN

CAPsMAN

CAP Interface | Provisioning | Configurations | Channels | Datapaths | Security Cfg.

Name	Frequency	Control Channel ...	Band
channel1	2412	20Mhz	2ghz-onlyn
channel4	2427	20Mhz	2ghz-onlyn
channel5	2432	20Mhz	2ghz-onlyn
channel8	2447	20Mhz	2ghz-onlyn
channel9	2452	20Mhz	2ghz-onlyn
channel11	2437	20Mhz	2ghz-onlyn
channel13	2472	20Mhz	2ghz-onlyn
channel36	5180	20Mhz	5ghz-a/n/ac
channel40	5200	20Mhz	5ghz-a/n/ac
channel44	5220	20Mhz	5ghz-a/n/ac
channel48	5240	20Mhz	5ghz-a/n/ac
channel52	5260	20Mhz	5ghz-a/n/ac
channel56	5280	20Mhz	5ghz-a/n/ac
channel60	5300	20Mhz	5ghz-a/n/ac
channel64	5320	20Mhz	5ghz-a/n/ac

CAPsMAN

CAP Interface | Provisioning | Configurations | Channels | Datapaths | Security Cfg. | A

Name	Bridge	Bridge Horizon	Local For...	Client To ...
datapath_hotspot	bridge_hotspot-online	10	no	no
datapath_service	bridge_service		no	no
datapath_staff	bridge_staff		no	yes
datapath_vip	bridge_VIP		no	no

CAPsMAN

CAP Interface | Provisioning | Configurations | Channels | Datapaths | Security Cfg. | Access List | Rates | Remote CAP | Ra

Name	Authentication Type	Encryption	Group Encryption	Group Key Update	Passphrase
security_service	WPA PSK WPA2 ...	aes ccm tkip	aes ccm		12312312
security_staff	WPA PSK WPA2 ...	aes ccm	aes ccm		1234567800
security_vip	WPA PSK WPA2 ...	aes ccm tkip	aes ccm		11112222

CAP Interface | Provisioning | Configurations | Channels | Datapaths | Security Cfg. | Access List | Rates | Remote CAP

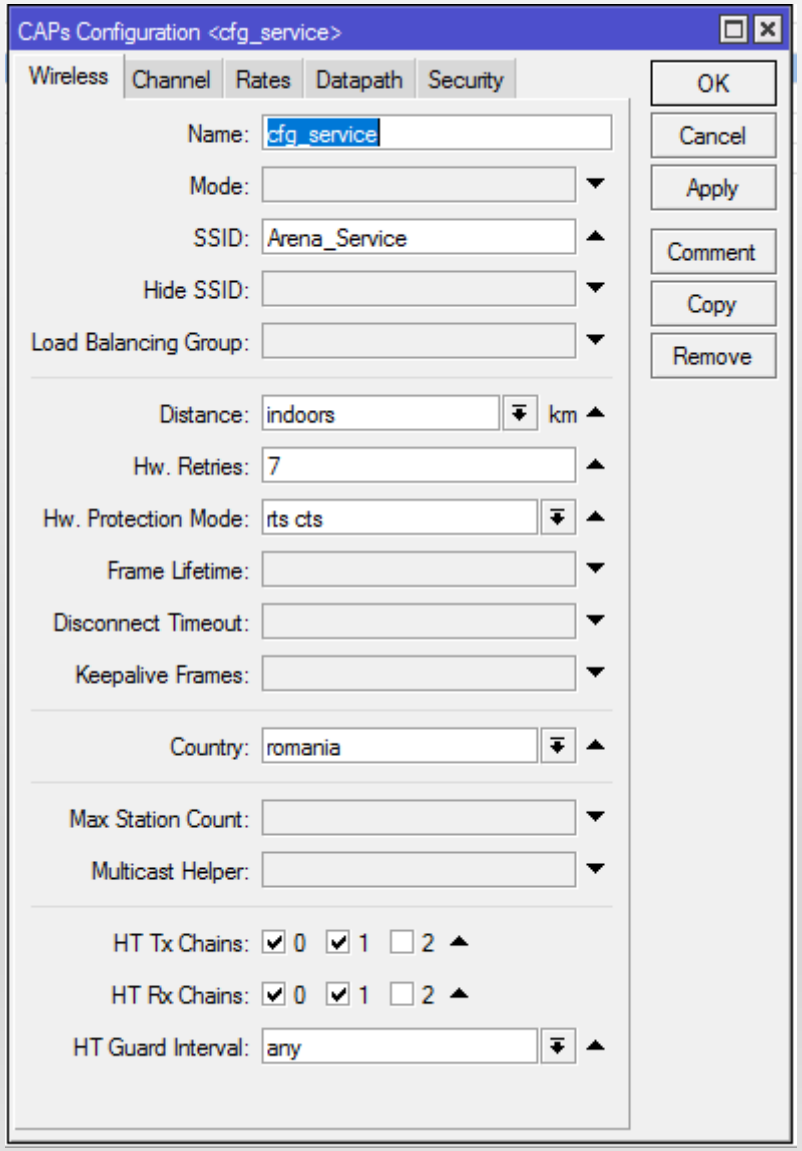
#	MAC Address	MAC Mask	Interface	SSID Regexp	Signal Ra...	Action
0					-80..-30	accept
1					-120..-81	reject

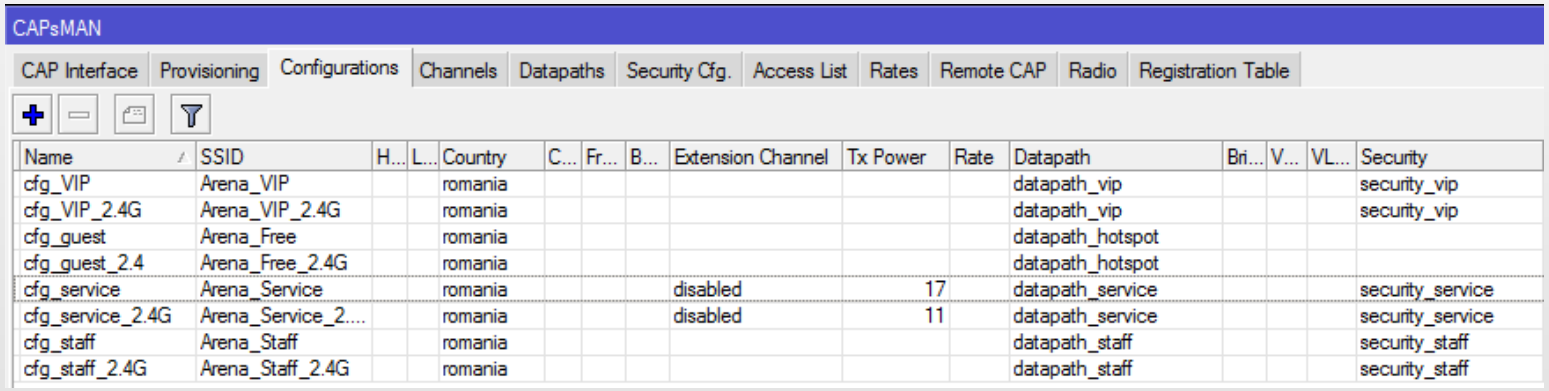
- Во вкладке **Channels** создаем каналы 2,4 и 5Ггц на которых будет работать наша WiFi сеть. Указываем в каком стандарте 802.11 будут работать созданные каналы
- Во вкладке **Datapaths** указываем необходимый Bridge, отключаем «Local forwarding», чтобы маршрутизацией занимался только CAP, для гостевых сетей отключаем передачу от клиента к клиенту «Client To Client Forwarding». Для изоляции гостевых клиентов устанавливаем в поле «Bridge Horizon» цифровое значение «10»
- В **Security** добавляем способы авторизации, алгоритмы шифрования и пароли к сети.
- В **Access List** добавляем два правила для отключения клиентов со слабым сигналом

Настройка CAPsMAN

```
/caps-man channel
add band=2ghz-onlyn control-channel-width=20mhz frequency=2412 name=channel1
add band=2ghz-onlyn control-channel-width=20mhz frequency=2432 name=channel5
add band=2ghz-onlyn control-channel-width=20mhz frequency=2452 name=channel9
add band=5ghz-a/n/ac control-channel-width=20mhz frequency=5180 name=channel36
add band=5ghz-a/n/ac control-channel-width=20mhz frequency=5200 name=channel40
add band=2ghz-onlyn control-channel-width=20mhz frequency=2472 name=channel13
add band=5ghz-a/n/ac control-channel-width=20mhz frequency=5220 name=channel44
add band=5ghz-a/n/ac control-channel-width=20mhz frequency=5240 name=channel48
add band=5ghz-a/n/ac control-channel-width=20mhz frequency=5260 name=channel52
add band=5ghz-a/n/ac control-channel-width=20mhz frequency=5280 name=channel56
add band=5ghz-a/n/ac control-channel-width=20mhz frequency=5300 name=channel60
add band=2ghz-onlyn control-channel-width=20mhz frequency=2437 name=channel11
add band=2ghz-onlyn control-channel-width=20mhz frequency=2427 name=channel4
add band=2ghz-onlyn control-channel-width=20mhz frequency=2447 name=channel8
add band=5ghz-a/n/ac control-channel-width=20mhz frequency=5320 name=channel64
/caps-man datapath
add bridge=bridge_staff client-to-client-forwarding=yes local-forwarding=no   name=datapath_staff
add bridge=bridge_hotspot-online bridge-horizon=10 client-to-client-forwarding=no local-forwarding=no name=datapath_free
add bridge=bridge_service client-to-client-forwarding=yes local-forwarding=no name=datapath_service
add bridge=bridge_VIP bridge-horizon=20 client-to-client-forwarding=no local-forwarding=no name=datapath_vip

/caps-man security
add authentication-types=wpa-psk,wpa2-psk encryption=aes-ccm group-encryption=aes-ccm name=security_staff passphrase=1234567800
add authentication-types=wpa-psk,wpa2-psk encryption=aes-ccm,tkip group-encryption=aes-ccm name=security_service passphrase=12312312
add authentication-types=wpa-psk,wpa2-psk encryption=aes-ccm,tkip group-encryption=aes-ccm name=security_vip passphrase=11112222
```

Настройка CAPsMAN





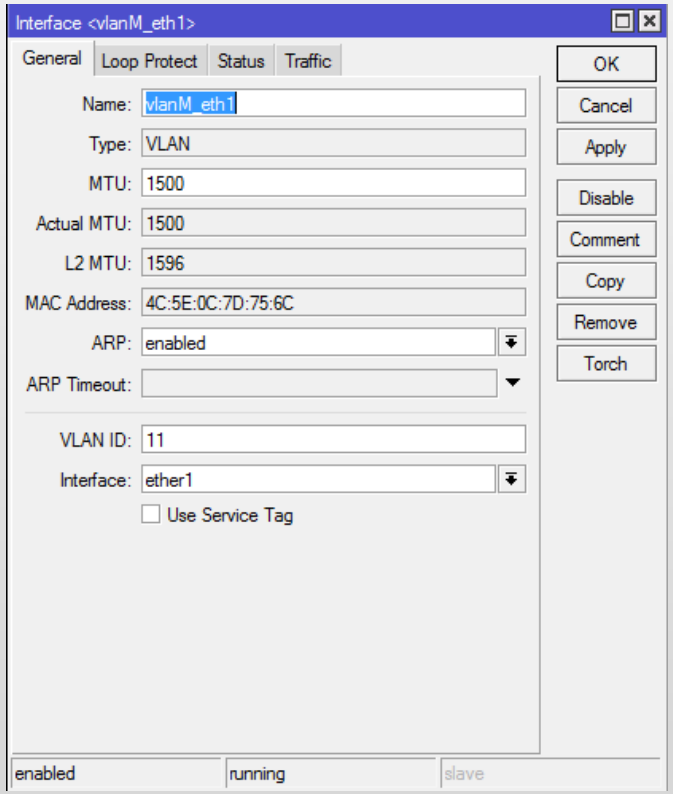
Name	SSID	H...	L...	Country	C...	Fr...	B...	Extension Channel	Tx Power	Rate	Datapath	Bri...	V...	VL...	Security
cfg_VIP	Arena_VIP			romania							datapath_vip				security_vip
cfg_VIP_2.4G	Arena_VIP_2.4G			romania							datapath_vip				security_vip
cfg_guest	Arena_Free			romania							datapath_hotspot				
cfg_guest_2.4	Arena_Free_2.4G			romania							datapath_hotspot				
cfg_service	Arena_Service			romania				disabled	17		datapath_service				security_service
cfg_service_2.4G	Arena_Service_2....			romania				disabled	11		datapath_service				security_service
cfg_staff	Arena_Staff			romania							datapath_staff				security_staff
cfg_staff_2.4G	Arena_Staff_2.4G			romania							datapath_staff				security_staff

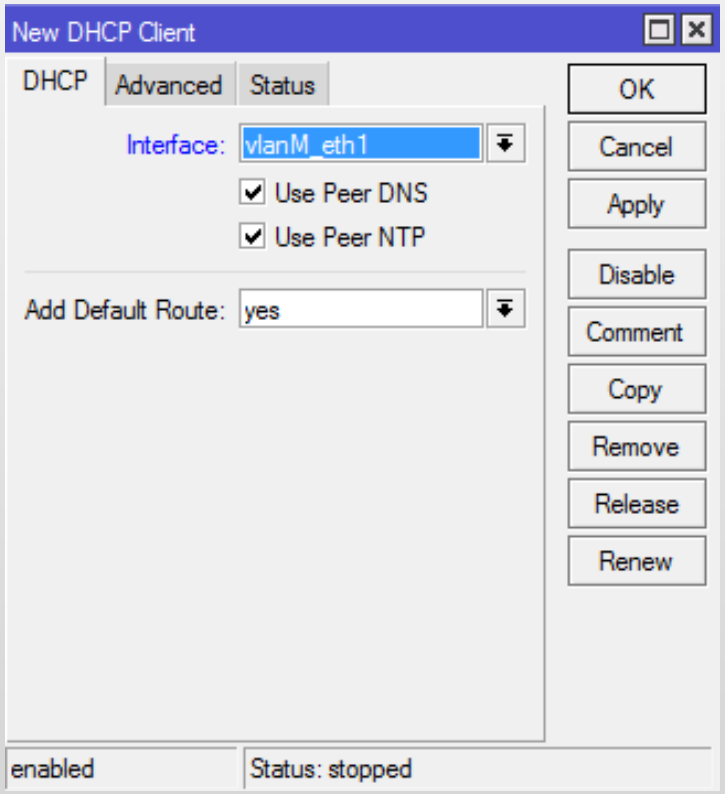
- Создаем конфигурации будущих WiFi-сетей, разделяя 2.4 и 5 Ггц

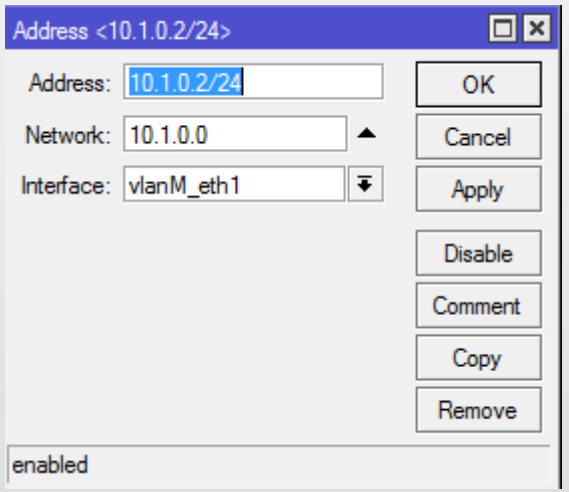
Из основных настроек:

- прописываем SSID
- устанавливаем режим Hw.Protection Mode «rts cts», для защиты от «скрытого узла»
- выбираем два канала 0 и 1 в HT Tx Chains и HT Rx Chains, чтобы точка работала в режиме MIMOx2
- Выбираем какая из конфигураций будет «основной» и прописываем в ней все необходимые настройки в закладке «Channel»
- Выбираем Datapaths под создаваемую конфигурацию
- Выбираем созданный ранее Security профиль авторизации SSID.

Настройка CAP



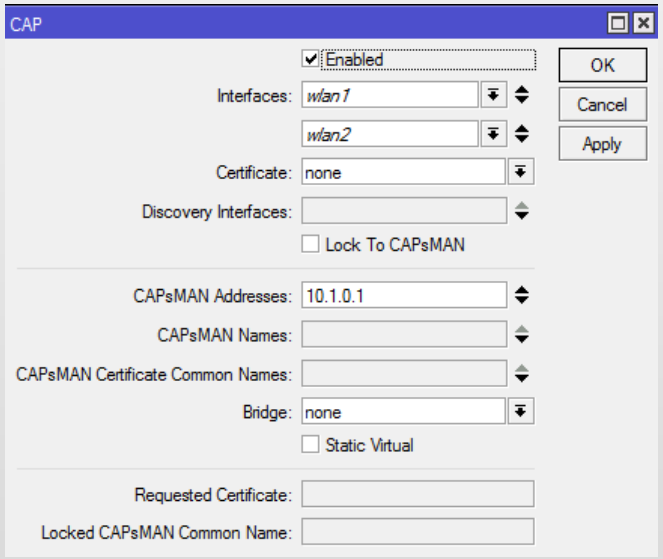


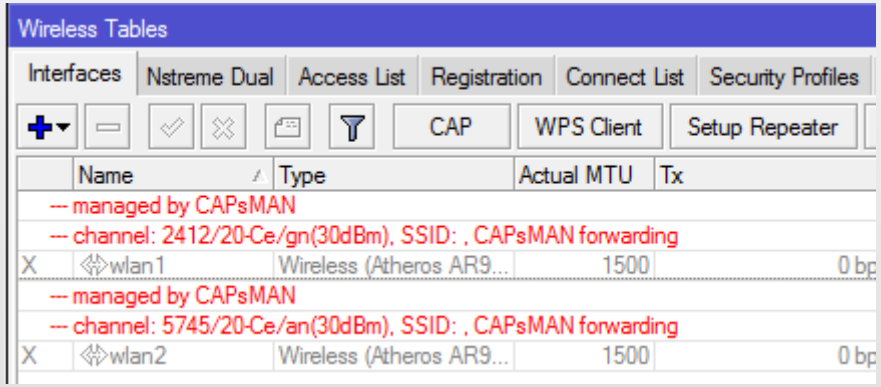



```
/interface vlan
add interface=ether1 name=vlanM_eth1 vlan-id=11
/ip address
add address=10.1.0.2/24 interface=vlanM_eth1 network=10.1.0.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=vlanM_eth1
```

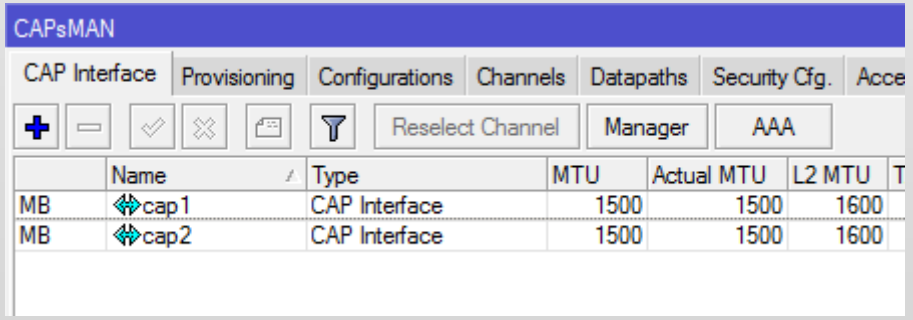
- Для подключения к CAP через Management LAN , создаем VLAN-интерфейс «vlanM_eth1» и применяем его к интерфейсу «ether1».
- На VLAN интерфейсе «vlanM_eth1» назначаем IP-адрес из Management LAN, либо получаем по DHCP

Подключение CAP к CAPsMAN





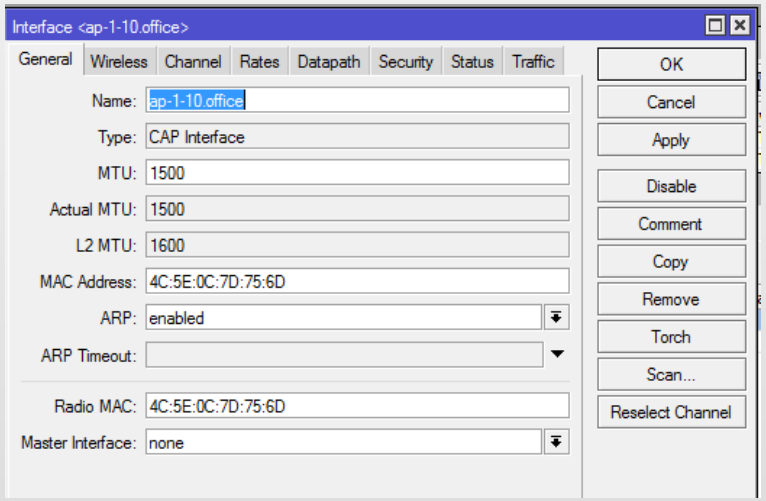
Успешное соединение с CAPsMAN со стороны CAP

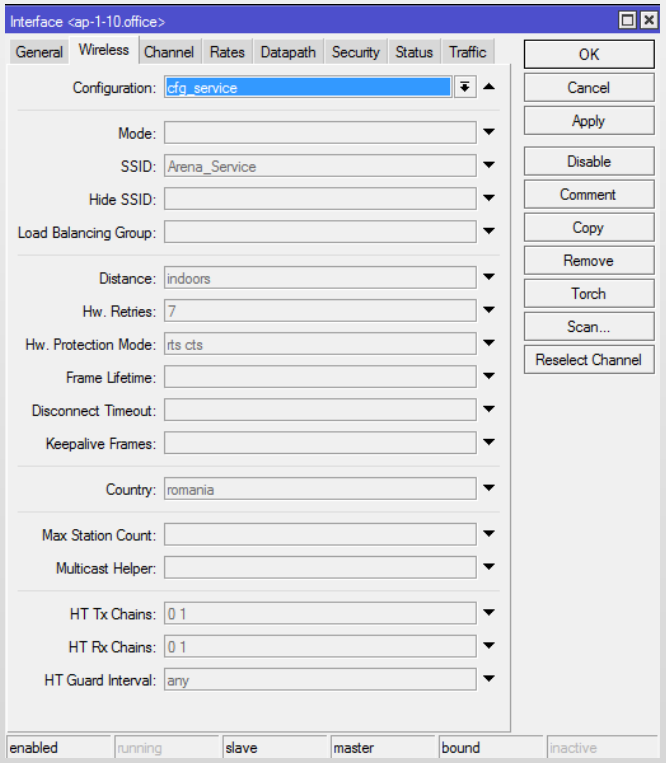


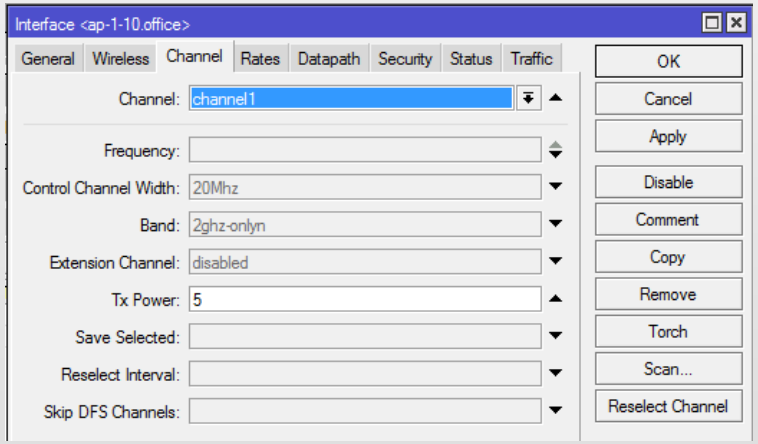
Успешное соединение с CAP со стороны CAPsMAN

- В разделе Wireless на вкладке Interfaces заходим в CAPsMAN
- В Interfaces выбираем беспроводные интерфейсы, которые хотим подключить к CAPsMAN
- В CAPsMAN Addresses вписываем IP-адрес нашего CAP -10.1.0.1
- Ставим «галочку» Enable, для подключения CAP к CAPsMAN

Подкючение AP к CAP

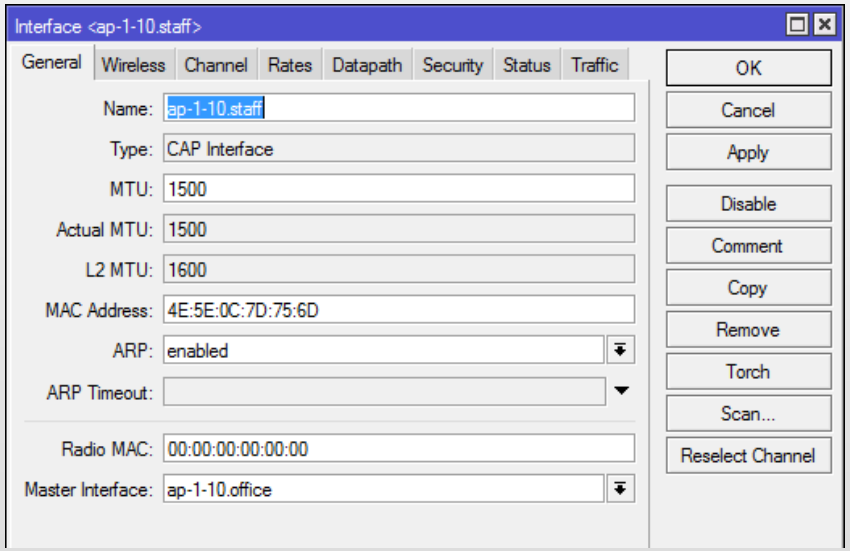


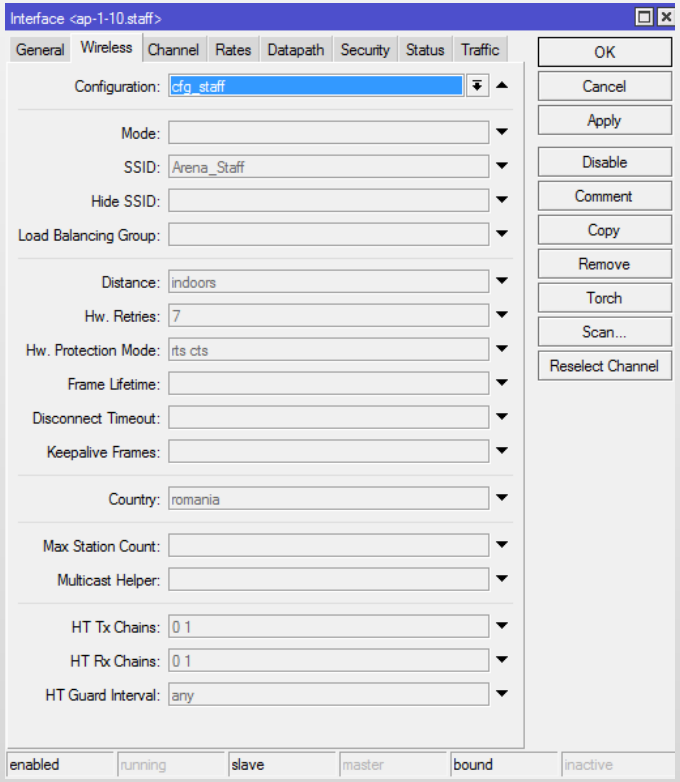


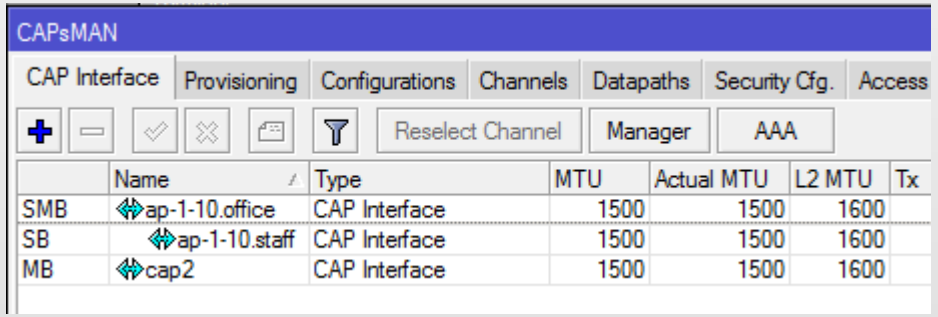


- Настраиваем на CAPsMAN подключившиеся физические интерфейсы AP:
- На вкладке General указываем имя
- На вкладке Wireless указываем основную конфигурацию
- На вкладке Channel указываем частоту на которой будет работать AP

Подключение AP к CAP

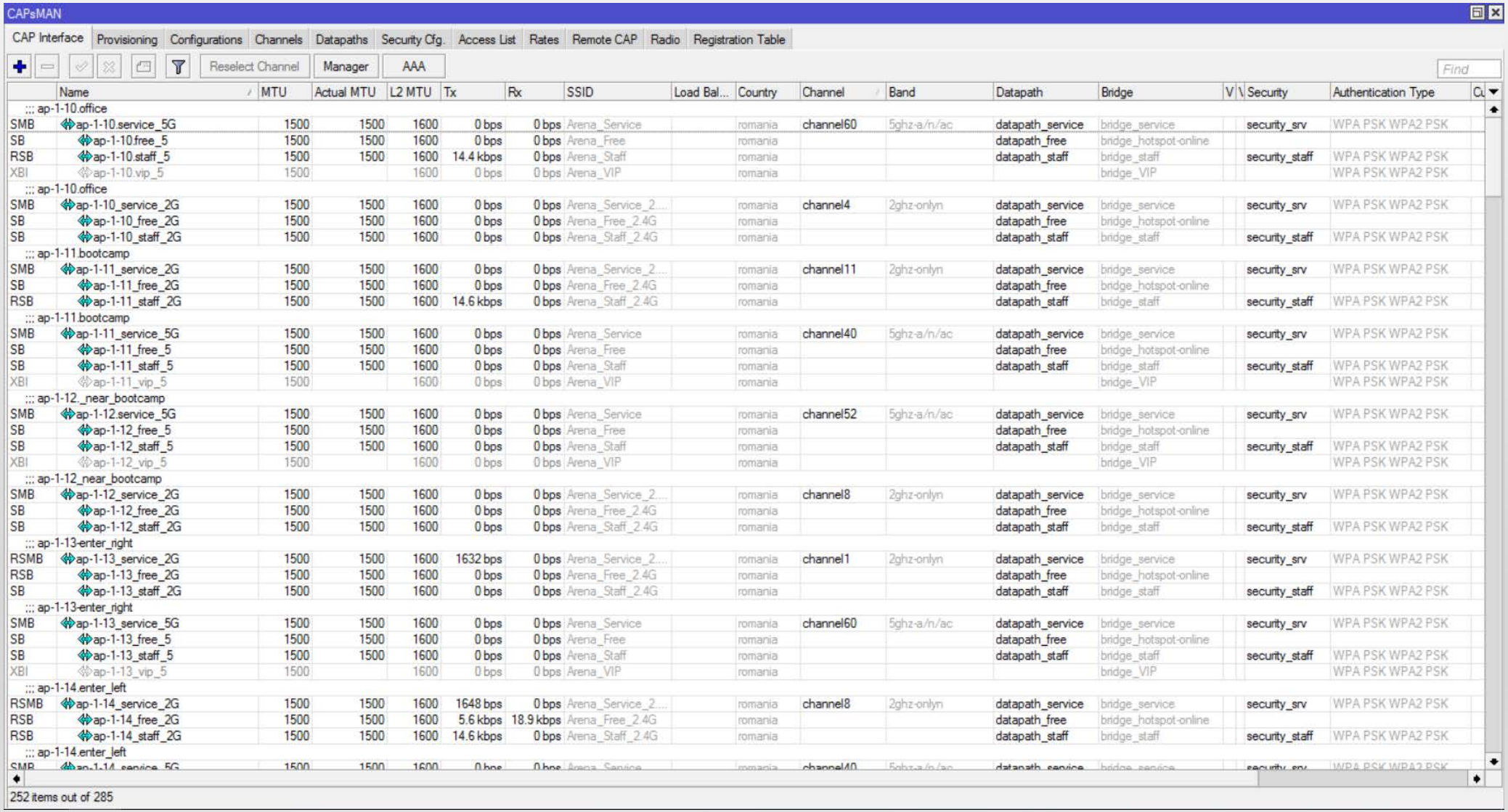






- Для подключения более одного SSID, необходимо создать VirtualAP
- Создав VirtualAP в поле Master interface указываем физический интерфейс подключенной AP
- На вкладке Wireless указываем дополнительную конфигурацию
- Частоту канала можно не выставлять т.к. данный параметр, как и ряд других, на VirtualAP не работает. Дополнительные параметры VirtualAP берет от «родительской» конфигурации. ☺

Конечный результат:



CAPsMAN

CAP Interface | Provisioning | Configurations | Channels | Datapaths | Security Cfg. | Access List | Rates | Remote CAP | Radio | Registration Table

Reselect Channel | Manager | AAA | Find

	Name	MTU	Actual MTU	L2 MTU	Tx	Rx	SSID	Load Bal...	Country	Channel	Band	Datapath	Bridge	V	Security	Authentication Type	Cu
	;;; ap-1-10.office																
SMB	ap-1-10.service_5G	1500	1500	1600	0 bps	0 bps	Arena_Service		romania	channel60	5ghz-a/n/ac	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
SB	ap-1-10.free_5	1500	1500	1600	0 bps	0 bps	Arena_Free		romania			datapath_free	bridge_hotspot-online				
RSB	ap-1-10.staff_5	1500	1500	1600	14.4 kbps	0 bps	Arena_Staff		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
XBI	ap-1-10.vip_5	1500		1600	0 bps	0 bps	Arena_VIP		romania				bridge_VIP			WPA PSK WPA2 PSK	
	;;; ap-1-10.office																
SMB	ap-1-10_service_2G	1500	1500	1600	0 bps	0 bps	Arena_Service_2....		romania	channel4	2ghz-onlyn	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
SB	ap-1-10_free_2G	1500	1500	1600	0 bps	0 bps	Arena_Free_2.4G		romania			datapath_free	bridge_hotspot-online				
SB	ap-1-10_staff_2G	1500	1500	1600	0 bps	0 bps	Arena_Staff_2.4G		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
	;;; ap-1-11.bootcamp																
SMB	ap-1-11_service_2G	1500	1500	1600	0 bps	0 bps	Arena_Service_2....		romania	channel11	2ghz-onlyn	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
SB	ap-1-11_free_2G	1500	1500	1600	0 bps	0 bps	Arena_Free_2.4G		romania			datapath_free	bridge_hotspot-online				
RSB	ap-1-11_staff_2G	1500	1500	1600	14.6 kbps	0 bps	Arena_Staff_2.4G		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
	;;; ap-1-11.bootcamp																
SMB	ap-1-11_service_5G	1500	1500	1600	0 bps	0 bps	Arena_Service		romania	channel40	5ghz-a/n/ac	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
SB	ap-1-11_free_5	1500	1500	1600	0 bps	0 bps	Arena_Free		romania			datapath_free	bridge_hotspot-online				
SB	ap-1-11_staff_5	1500	1500	1600	0 bps	0 bps	Arena_Staff		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
XBI	ap-1-11_vip_5	1500		1600	0 bps	0 bps	Arena_VIP		romania				bridge_VIP			WPA PSK WPA2 PSK	
	;;; ap-1-12._near_bootcamp																
SMB	ap-1-12.service_5G	1500	1500	1600	0 bps	0 bps	Arena_Service		romania	channel52	5ghz-a/n/ac	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
SB	ap-1-12_free_5	1500	1500	1600	0 bps	0 bps	Arena_Free		romania			datapath_free	bridge_hotspot-online				
SB	ap-1-12_staff_5	1500	1500	1600	0 bps	0 bps	Arena_Staff		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
XBI	ap-1-12_vip_5	1500		1600	0 bps	0 bps	Arena_VIP		romania				bridge_VIP			WPA PSK WPA2 PSK	
	;;; ap-1-12_near_bootcamp																
SMB	ap-1-12_service_2G	1500	1500	1600	0 bps	0 bps	Arena_Service_2....		romania	channel8	2ghz-onlyn	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
SB	ap-1-12_free_2G	1500	1500	1600	0 bps	0 bps	Arena_Free_2.4G		romania			datapath_free	bridge_hotspot-online				
SB	ap-1-12_staff_2G	1500	1500	1600	0 bps	0 bps	Arena_Staff_2.4G		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
	;;; ap-1-13-enter_right																
RSMB	ap-1-13_service_2G	1500	1500	1600	1632 bps	0 bps	Arena_Service_2....		romania	channel1	2ghz-onlyn	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
RSB	ap-1-13_free_2G	1500	1500	1600	0 bps	0 bps	Arena_Free_2.4G		romania			datapath_free	bridge_hotspot-online				
SB	ap-1-13_staff_2G	1500	1500	1600	0 bps	0 bps	Arena_Staff_2.4G		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
	;;; ap-1-13-enter_right																
SMB	ap-1-13_service_5G	1500	1500	1600	0 bps	0 bps	Arena_Service		romania	channel60	5ghz-a/n/ac	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
SB	ap-1-13_free_5	1500	1500	1600	0 bps	0 bps	Arena_Free		romania			datapath_free	bridge_hotspot-online				
SB	ap-1-13_staff_5	1500	1500	1600	0 bps	0 bps	Arena_Staff		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
XBI	ap-1-13_vip_5	1500		1600	0 bps	0 bps	Arena_VIP		romania				bridge_VIP			WPA PSK WPA2 PSK	
	;;; ap-1-14.enter_left																
RSMB	ap-1-14_service_2G	1500	1500	1600	1648 bps	0 bps	Arena_Service_2....		romania	channel8	2ghz-onlyn	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	
RSB	ap-1-14_free_2G	1500	1500	1600	5.6 kbps	18.9 kbps	Arena_Free_2.4G		romania			datapath_free	bridge_hotspot-online				
RSB	ap-1-14_staff_2G	1500	1500	1600	14.6 kbps	0 bps	Arena_Staff_2.4G		romania			datapath_staff	bridge_staff		security_staff	WPA PSK WPA2 PSK	
	;;; ap-1-14.enter_left																
SMB	ap-1-14_service_5G	1500	1500	1600	0 bps	0 bps	Arena_Service		romania	channel40	5ghz-a/n/ac	datapath_service	bridge_service		security_srv	WPA PSK WPA2 PSK	

252 items out of 285