

Настройка VLAN на Микротик

 mikrotiklab.ru/nastrojka/artga-vlan.html

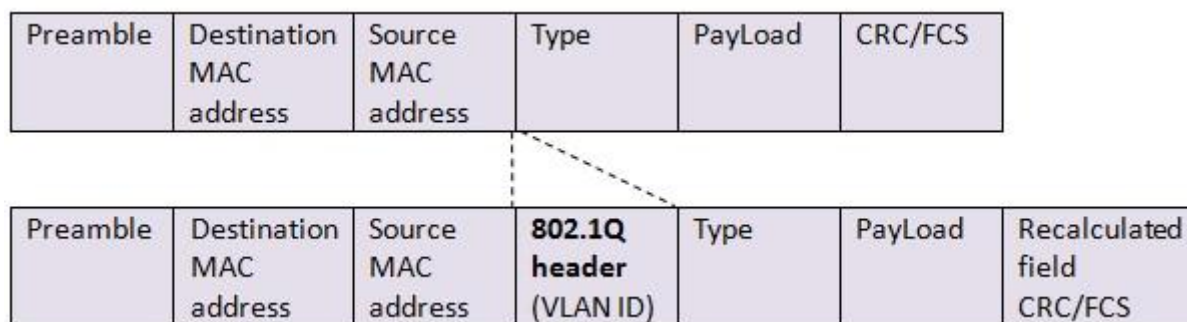
March 14, 2020

Самая непонятная, сложная и странная тема в нашем обзоре – настройка VLAN на Mikrotik. Вы можете найти миллион статей в интернете, но как на зло, ни одна из них не объяснит, как же все-таки настраивается эта технология. Честно признаться, я сам иногда задумываюсь «Как же устроен мозг того разработчика, который реализовал это именно таким образом?».

На курсах Mikrotik не особо уделяют этому время (понять можно, за 3-ех дневной тренинге роутинга особо не расскажешь про данную технологию), и в большинстве случаев, не сразу улавливаешь суть. В голове простого человека сразу же начинают возникать кучу вопросов – как? откуда? Кто роутер? Кто свитч? и т.д. Подливает масло в огонь следующее – реализация отличается на разных железках. «Куда мир катится?» — и я с вами соглашусь. Существует 2 способа реализации на трех типах устройствах. Но обо всем по порядку.

Немного теории

VLAN – виртуальная локальная сеть, которая реализуется на роутерах и свитчах на втором уровне модели OSI путем расширения стандартного кадра Ethernet 4-ех байтовым полем. 3 бита выделены под Priority, 1 под CFI и 12 бит на VID.



VID – это VLAN ID, идентификатор который может принимать до 4096 значений. В отличие от устройств компании, чье название начинается с Cisco, на Mikrotik можно задавать любое значение от 0 до 4095. Т.е. эта та штука, которая делит одну плоскую широковещательную сеть на разные.

Наша команда рекомендует изучить [Наша команда рекомендует изучить углубленный курс по администрированию сетевых устройств MikroTik](#) В курсе много лабораторных работ по итогам которых вы получите обратную связь. После обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [ТУТ](#).

Порты – существует 2 вида в понятии Mikrotik. Tagged и Untagged. Или проще говоря Tagged – транковые или же uplink, смотрящие на роутеры и свитчи. Untagged – порты доступа (принтеры, компьютеры, серверы) т.е. конечные устройства.

Ранее я говорил, что есть два вида реализации на трех типах устройств. Первая – программная реализация она везде одинакова и настраивается в bridge, вторая – аппаратная. В первом случае, обработка трафика идет через центральный процессор, во втором – обработкой трафика занимается свитч чип. Но в свитчах 3XX серии настройка именно через меню Bridge.

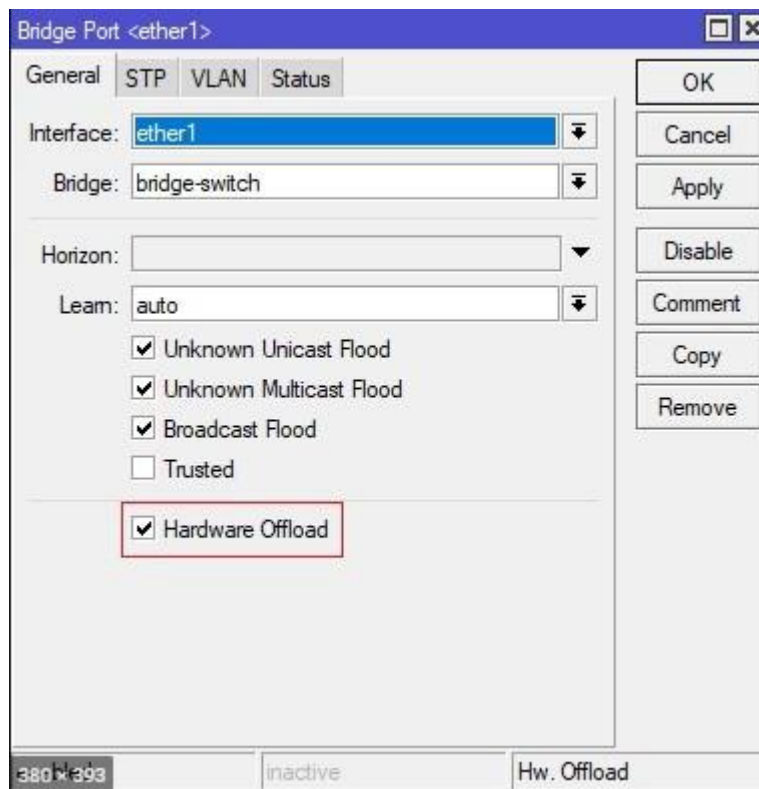
Из-за того, что чипов много и разных, существуют 3 подхода к реализации:

- Роутеры и SOHO устройства – это устройства на чипах Atheros 8227, Atheros 8327 и не только, в которых аппаратная реализация находится в меню Switch. Подробнее можно ознакомиться [тут](#)
- CRS1XX/2XX серии – устройства с 24-мя портами на борту, в которых аппаратная реализация находится в меню Ознакомьтесь с функциями чипа можно [тут](#)
- CRS3XX серии – устройства с мощным чипом коммутации, в котором аппаратная реализация находится в bridge. Ознакомьтесь с функциями чипа можно [тут](#)

Важный нюанс. С версии прошивки 6.41 изменился подход к реализации. Абсолютно все устройства настраиваются через Bridge. Появилось понятие Hardware Offload – аппаратная разгрузка, означает, что трафик обрабатывается свитч чипом, а не процессором. Параметр выставляется при добавлении порта в бридж. Но если вы имеете в вашей схеме сети в качестве роутера Har Lite, hAP AC lite или любое устройство из первого и второго пунктов, а также не планируется на этом же устройстве делать порты доступа, создавать и добавлять порты в бридж не нужно.

Вышесказанное может сбить с толку. В первом и втором типе, порты нужно добавлять в Bridge, а настраивать в меню Switch. Но если у вас один порт, который используется для tagged трафика, то добавлять не нужно, просто вешаете на него VLAN-ы. Здесь подразумевается, что это устройство скорее всего роутер. Но если вы добавили все порты в Bridge, и настраиваете в меню Bridge, то вы отключите HW Offload и задействуется ЦП. В третьем типе, все настраивается в Bridge и это будет аппаратная реализация.

Всегда следите за аппаратной разгрузкой, если вы включили функционал, который не поддерживается чипом, разгрузка выключится и трафик побежит через процессор.



В данной инструкции мы остановимся на свитчах третьей серии и будем настраивать Mikrotik VLAN через Bridge для нескольких сценариях:

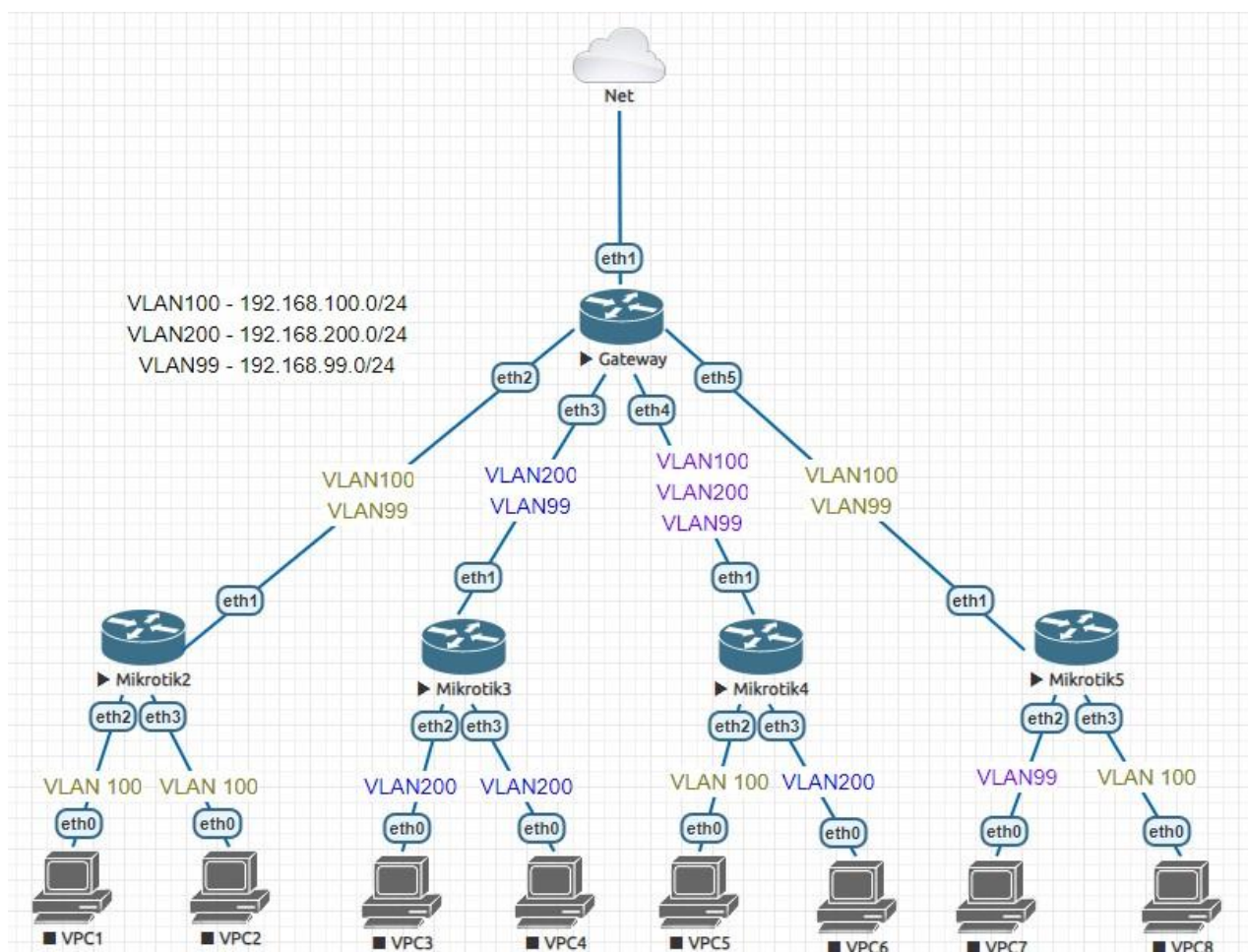
- Только VLAN100 и все порты подключены в него;
- Только VLAN200 и все порты подключены в него;
- На коммутаторе VLAN100 и VLAN200;
- Управления VLAN99 и VLAN.



Схема сети

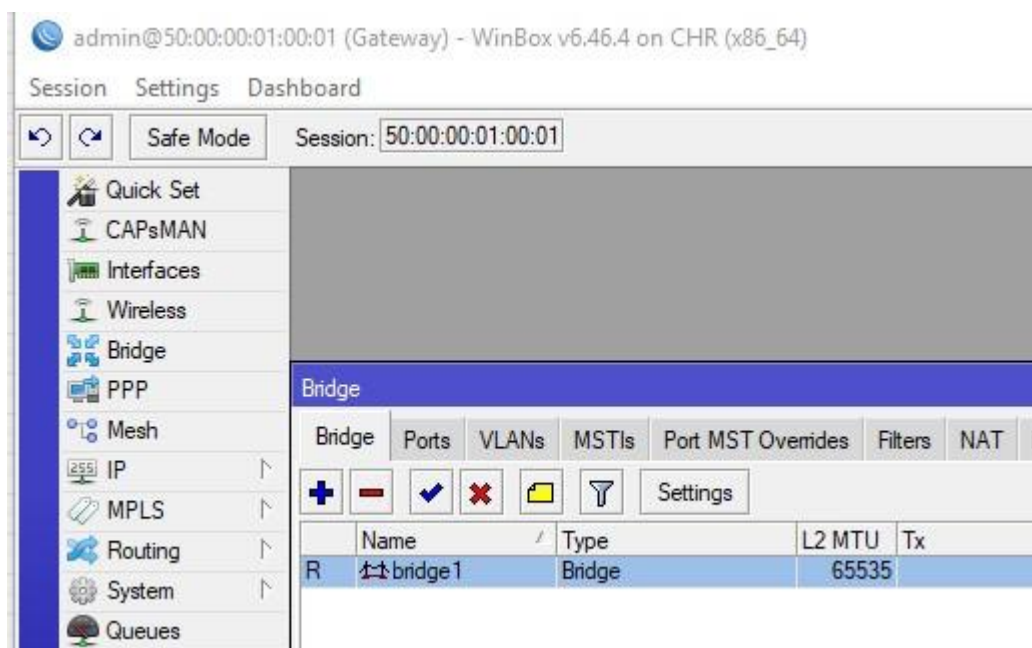
Мы имеем:

- VLAN100 – 192.168.100.0/24 – для ПК и принтеров;
- VLAN200 – 192.168.200.0/24 – для ПК и принтеров;
- VLAN99 – 192.168.99.0/24 – management сеть;
- Gateway – выполняет роль роутера и имеет доступ во все сети;
- Mikrotik2-5 – коммутаторы;
- VPC7 – админский ПК, полный доступ;
- RouterOS версии 6.46.4.



Настройка роутера

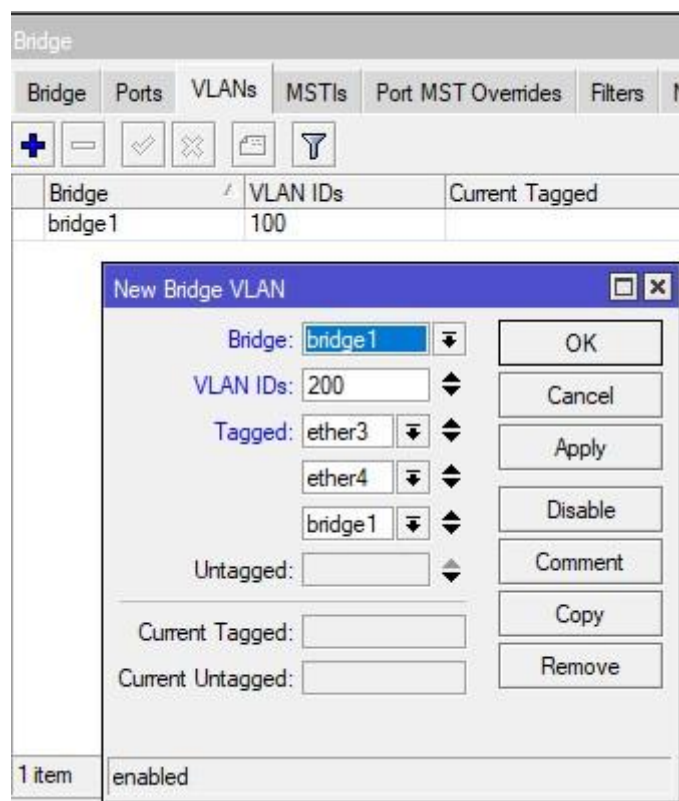
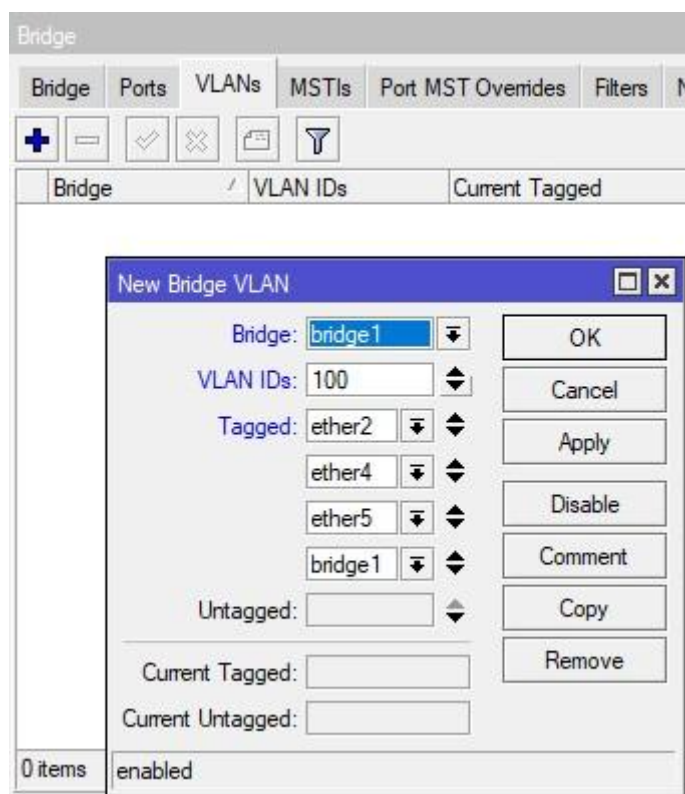
Роутер на то и роутер чтобы управлять трафиком через firewall. Но мы не будем настраивать правила фильтрации в данной статье. Так же у нас не будет включена Hardware Offload т.к. мы используем лабораторный стенд и отсутствуют какие-либо чипы коммутации. Чипы коммутации отсутствуют на RouterBoard серии CCR и виртуалок CHR. Первым делом создадим bridge и добавим в него ether2-5.

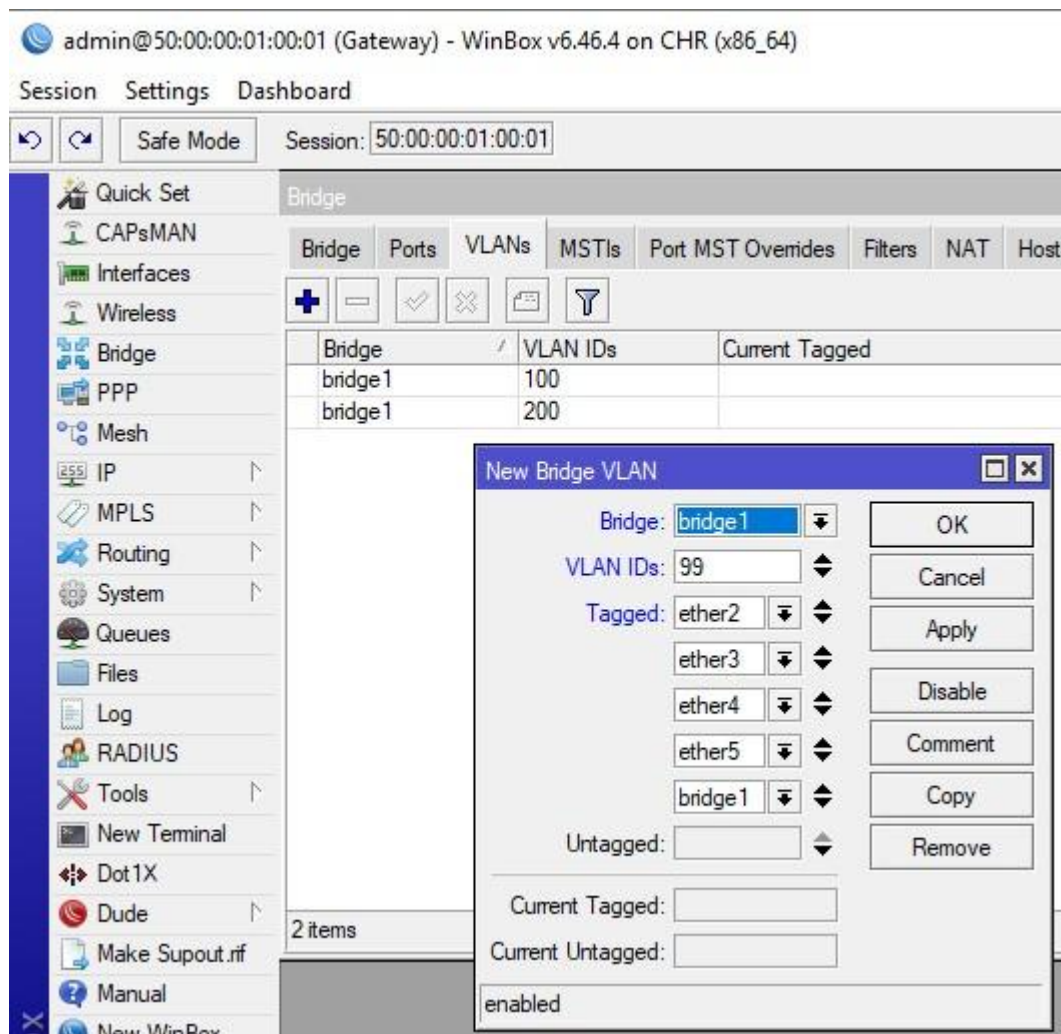


На вкладке VLANs укажем сети.

Согласно схеме коммутации, у нас есть ПК в VLAN100 за Mikrotik2, Mikrotik4, Mikrotik5, в связи с этим указываем соответствующие Tagged интерфейсы. Добавляем бридж в бридж, это так сказать некий порт, между роутером и сетью который позволяет понимать трафик в определенном VLAN. Прodelываем аналогично для 200-ой сети.

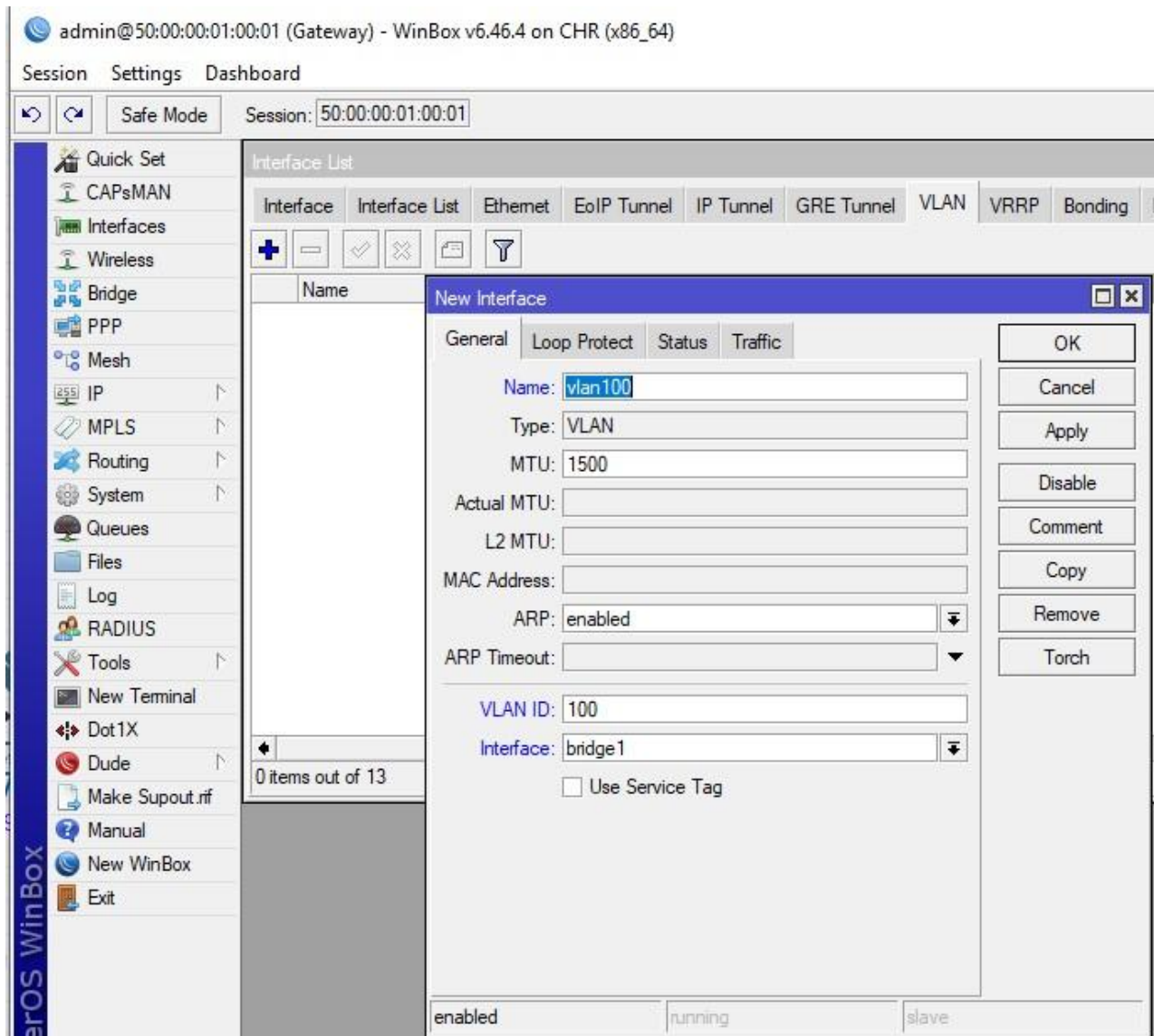
Далее настроим сеть управления, в которой будут коммутаторы и роутер, а также ПК VPC7.



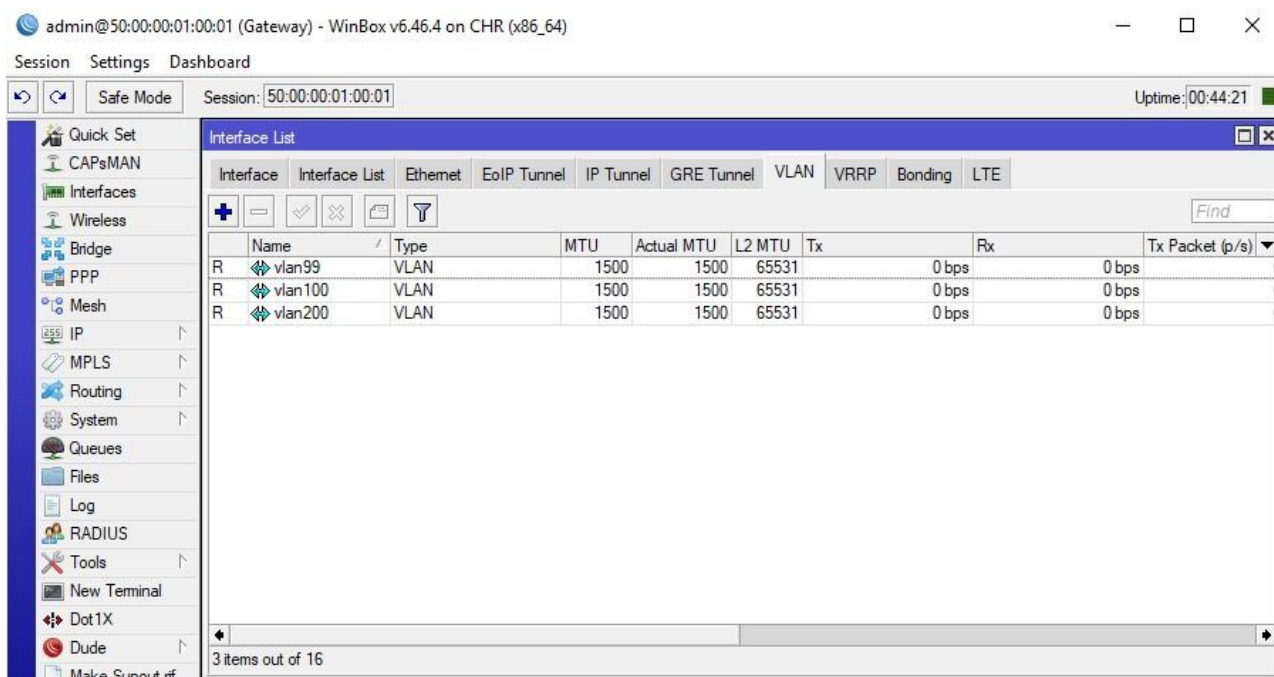


«Почему так?» —спросите вы. Потому что данный тег нужно передавать на все коммутаторы, чтобы ими управлять, принимая его на устройствах.

Далее создадим VLAN интерфейсы и укажем на них адреса. В Interfaces создадим новый указав понятное название и VID. Обязательно указываем bridge1, т.к. повесить метку на физический интерфейс не получится, в связи с тем, что он находится в slave режиме (зависит от bridge).

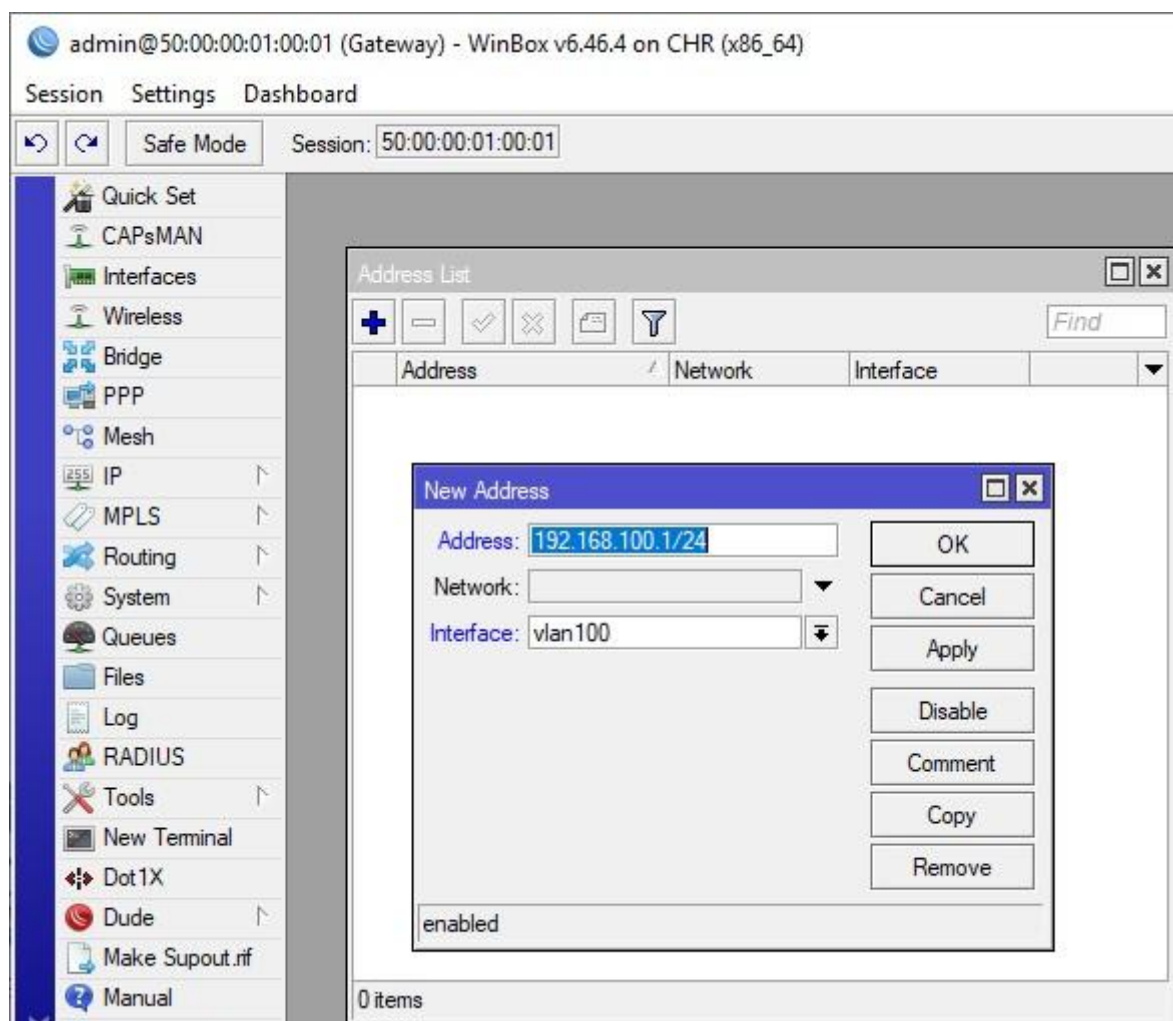


Создаем по аналогии для меток 200 и 99.

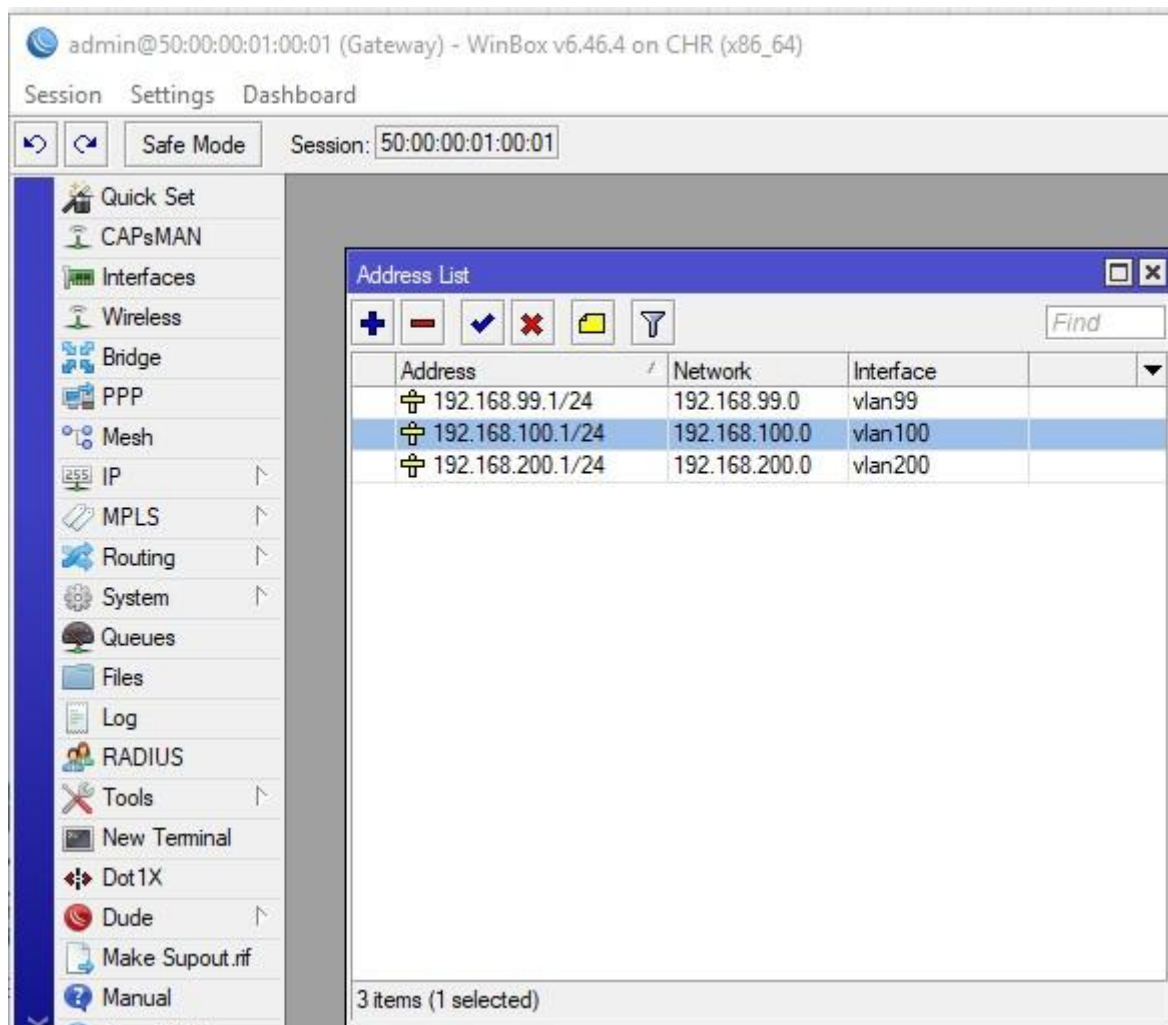


Далее задаем адреса на интерфейсы:

- VLAN100 – 192.168.100.1/24;
- VLAN200 – 192.168.200.1/24;
- VLAN99 – 192.168.99.1/24.



По аналогии добавляем адреса для сетей 200 и 99 выбрав соответствующее интерфейсы.



Все что мы сделали выше – подготовительные работы. Еще ничего не работает, метки не бегают, адреса фейковые. Обязательно все перепроверим и только после этого, открываем свойства bridge1 и включаем VLAN Filtering. Все начинает работать, до этой галочки – нет.

Safe Mode Session: 50:00:00:01:00:01

Bridge

Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB

+ - ✓ ✗ 📁 🔍 Settings

	Name	Type	L2 MTU	Tx	Rx
R	bridge1	Bridge	65535	0 bps	0 bps

Interface <bridge1>

General STP VLAN Status Traffic

☒ VLAN Filtering

EtherType: 0x8100

PVID: 1

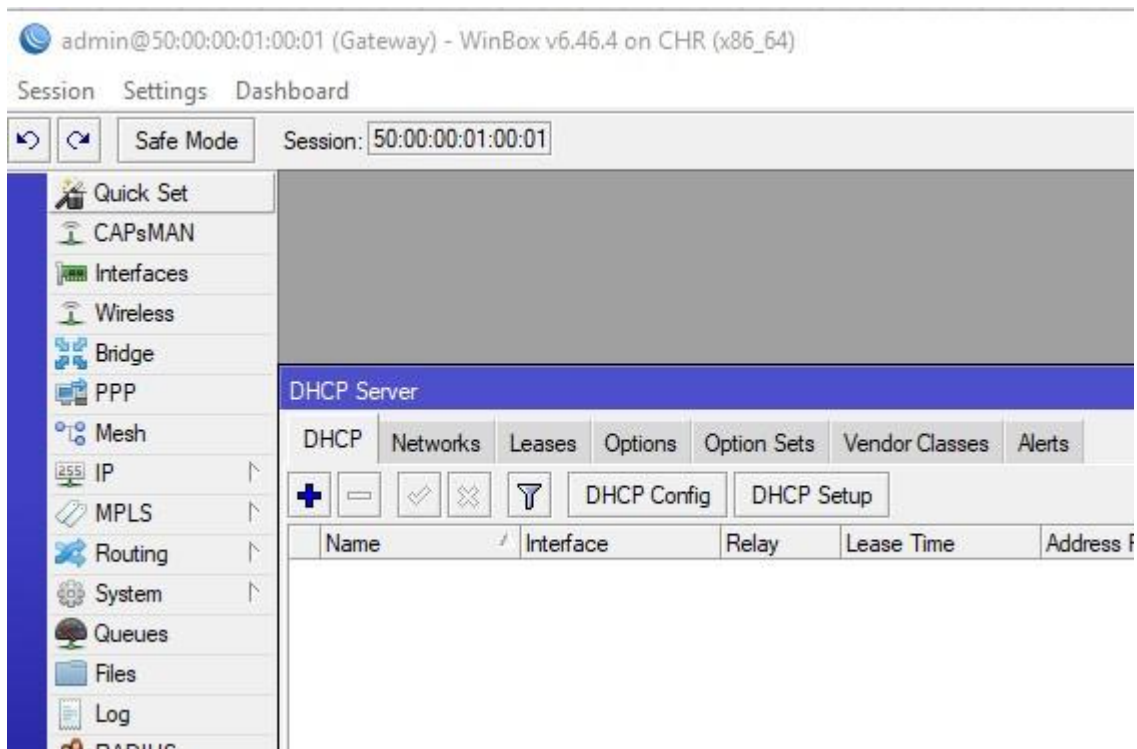
Frame Types: admit all

☐ Ingress Filtering

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

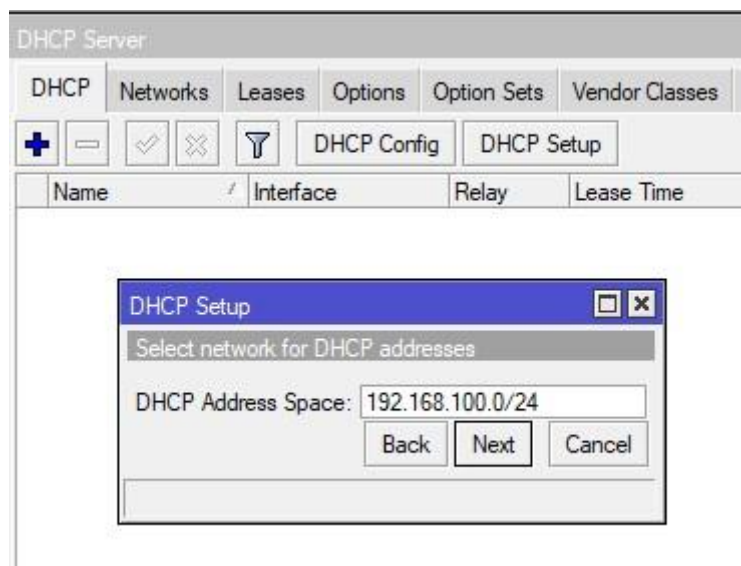
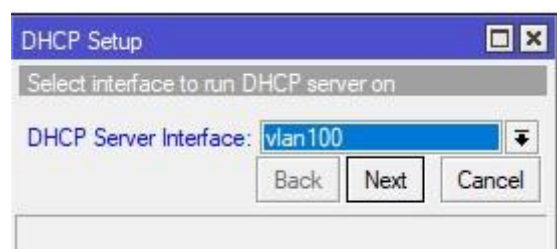
Сохраняем и перейдем к созданию DHCP серверов для Vlan сетей на нашем микротике Открываем IP – DHCP Server и жмем DHCP Setup.

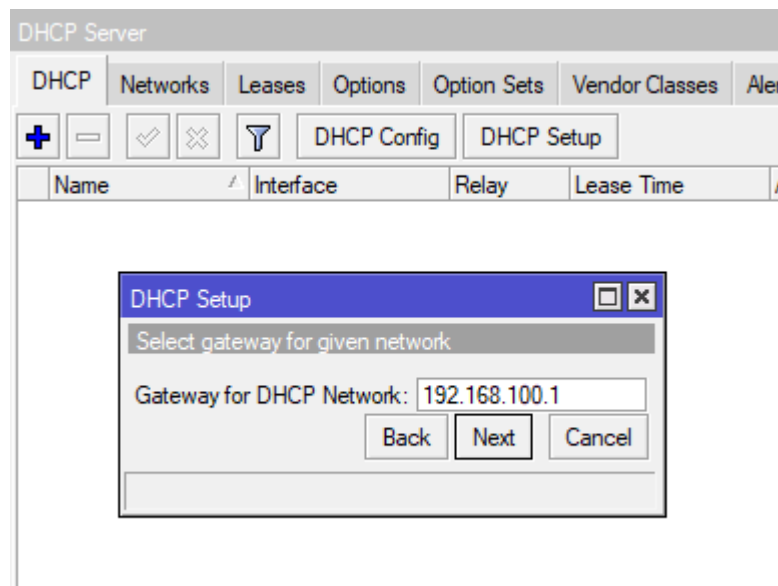


Выбираем интерфейс, на котором будет работать служба DHCP.

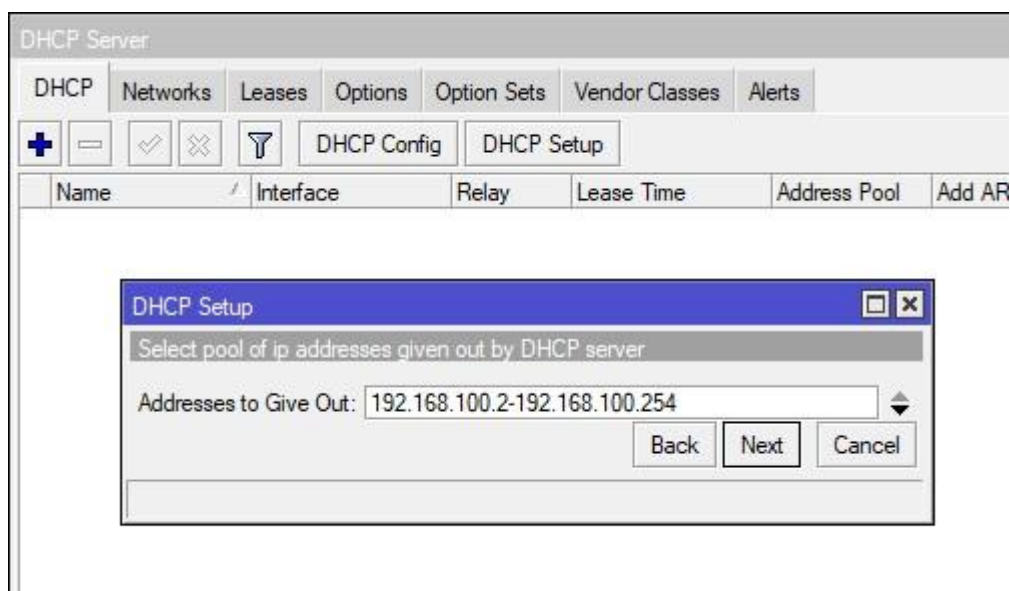
На следующем шаге ничего не меняем.

Следом необходимо указать шлюз. В данном случае будет 192.168.100.1

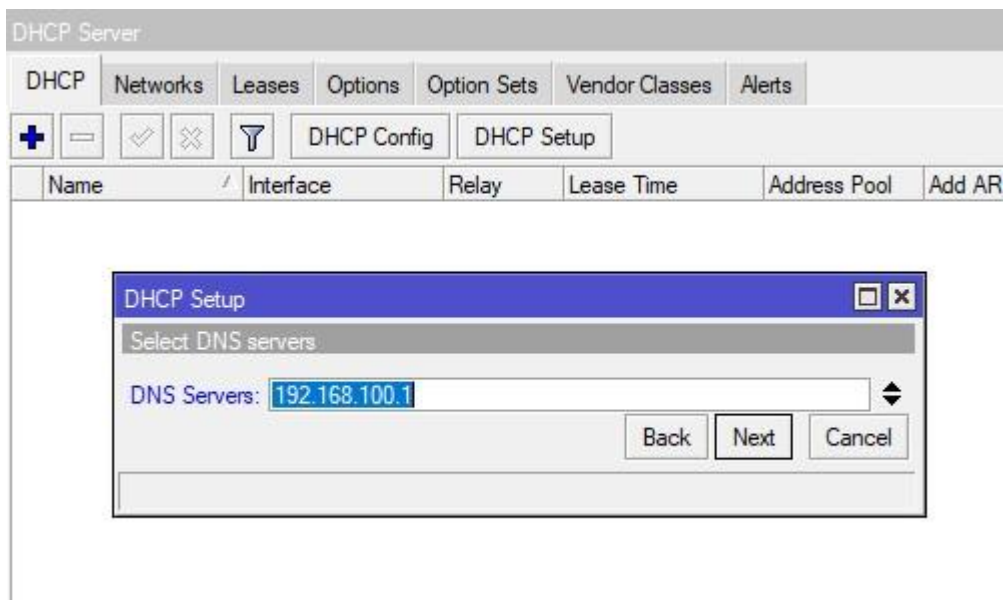




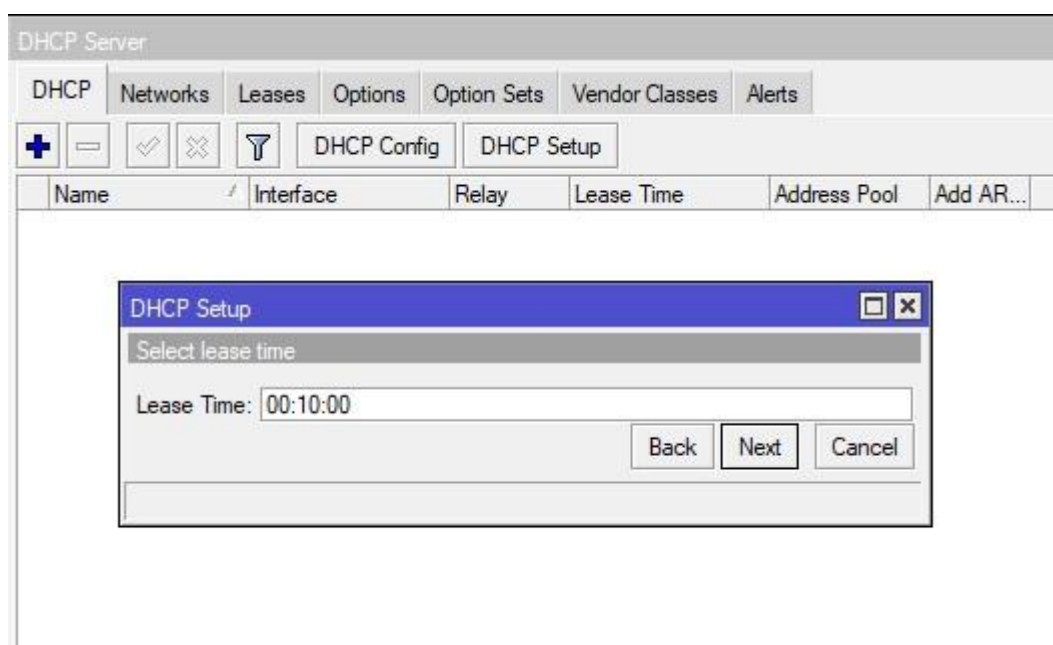
Далее нам предлагают указать выдаваемый пул адресов.



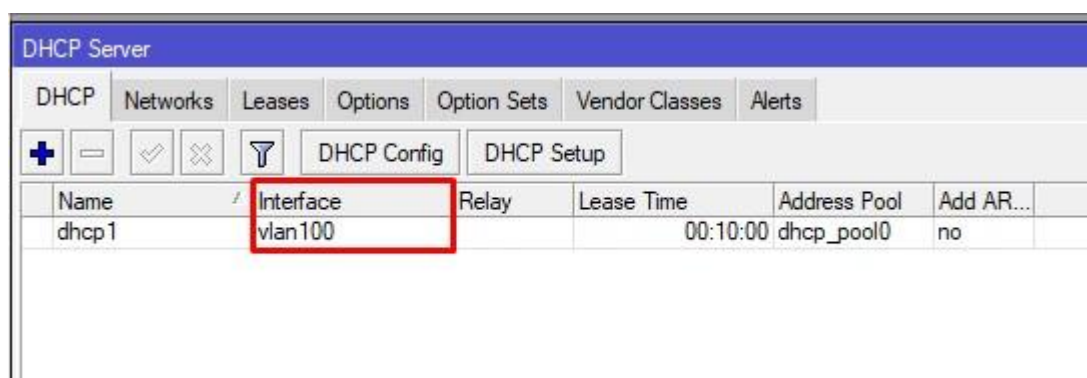
DNS-сервер. В нашей инсталляции будет свой на каждый VLAN, т.е. 192.168.100.1. Если у вас уже есть DNS сервера, можете указать их.



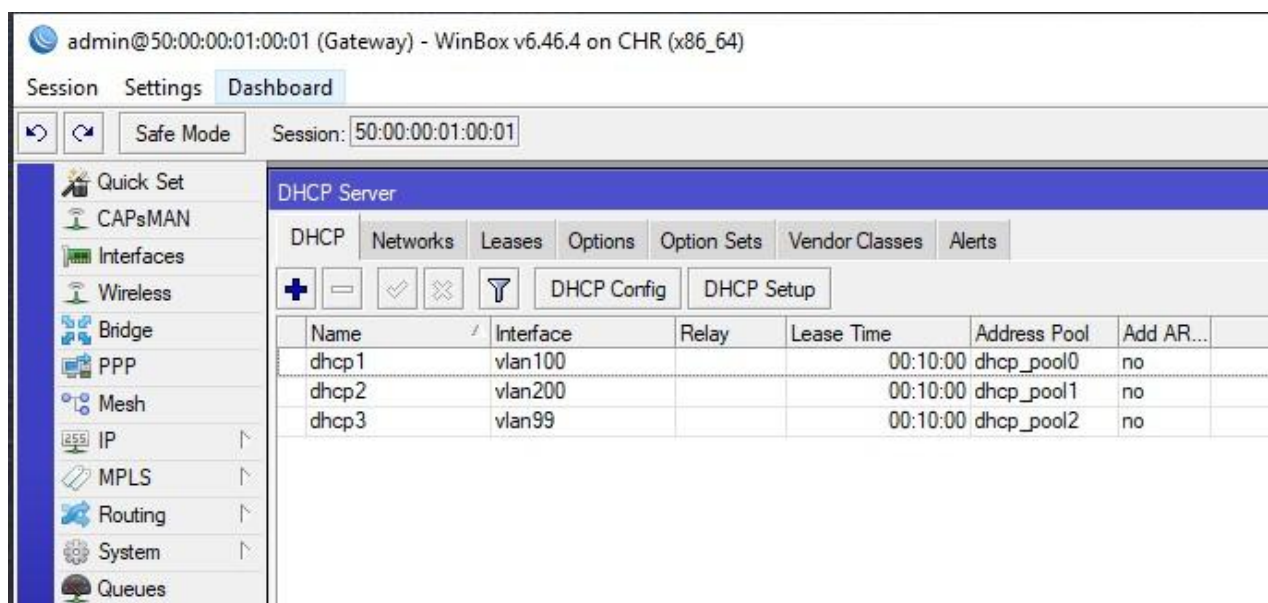
И последнее – время аренды. Оставим по умолчанию.



После создания проверим, на верном ли интерфейсе у нас работает служба.



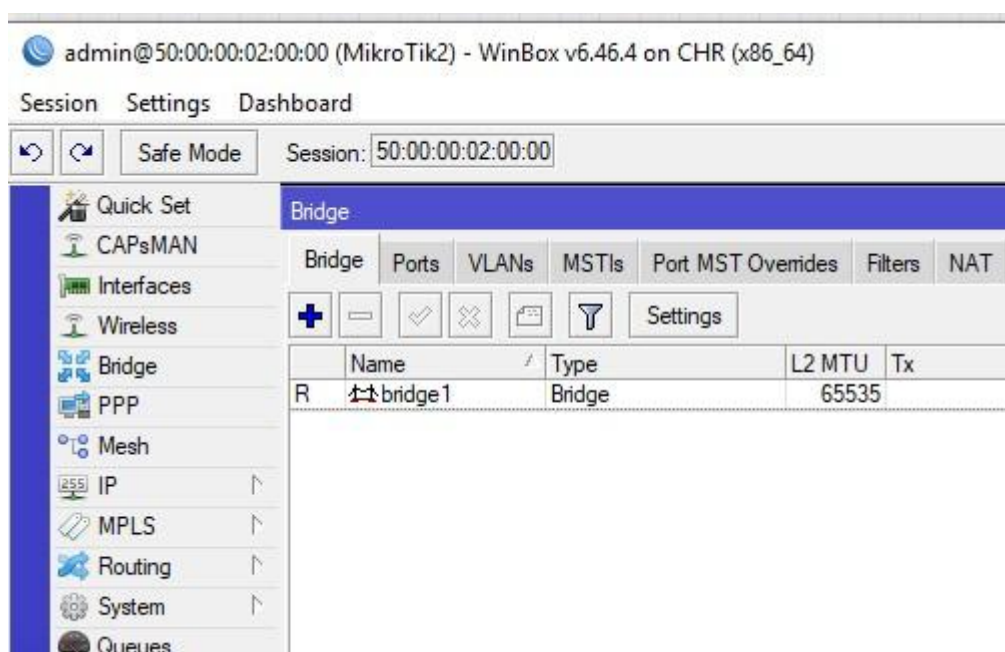
По аналогии создаем для 200 и 99.



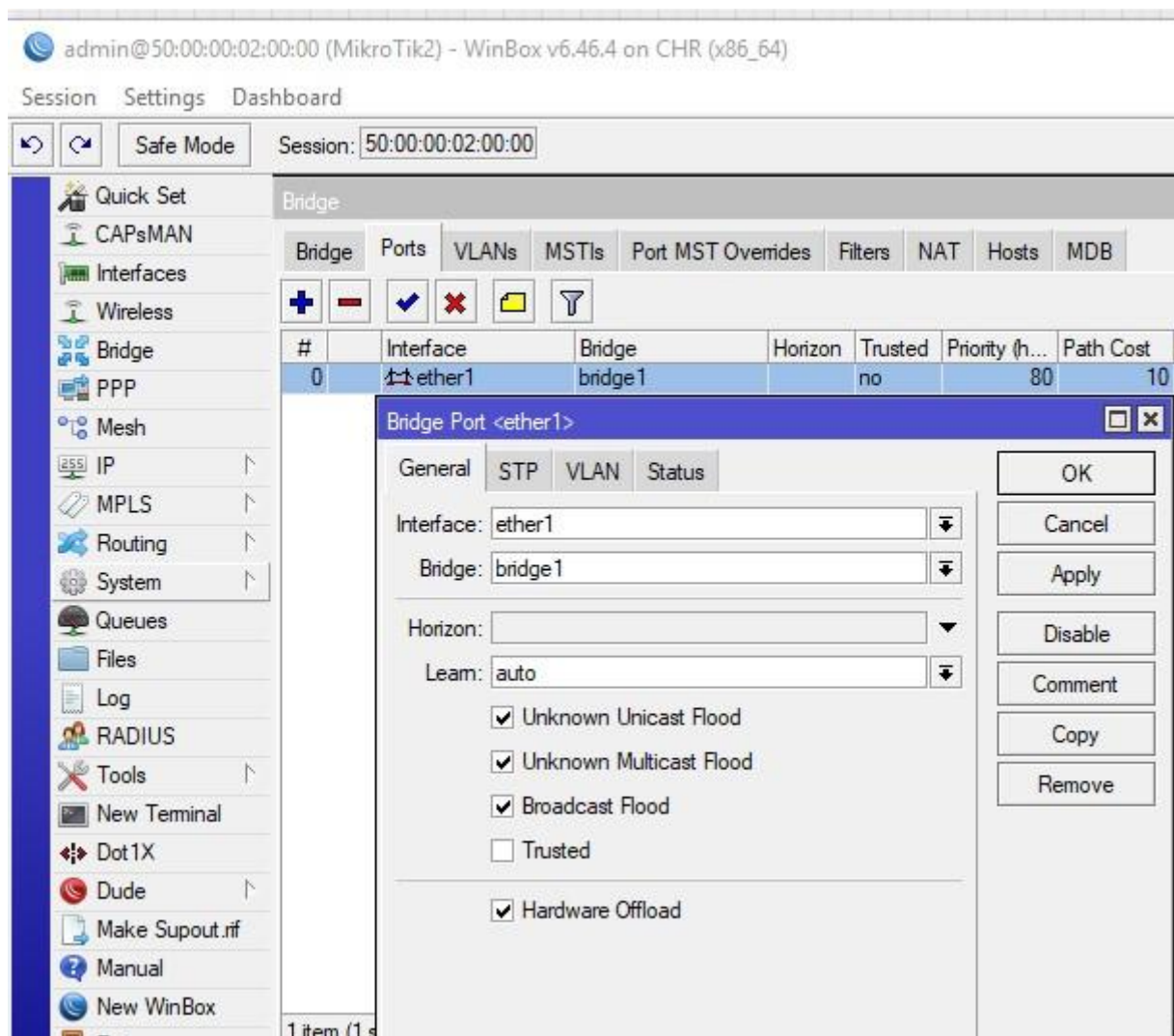
На этом базовая настройка шлюза завершена.

Настройка VLAN100, все порты подключены в него.

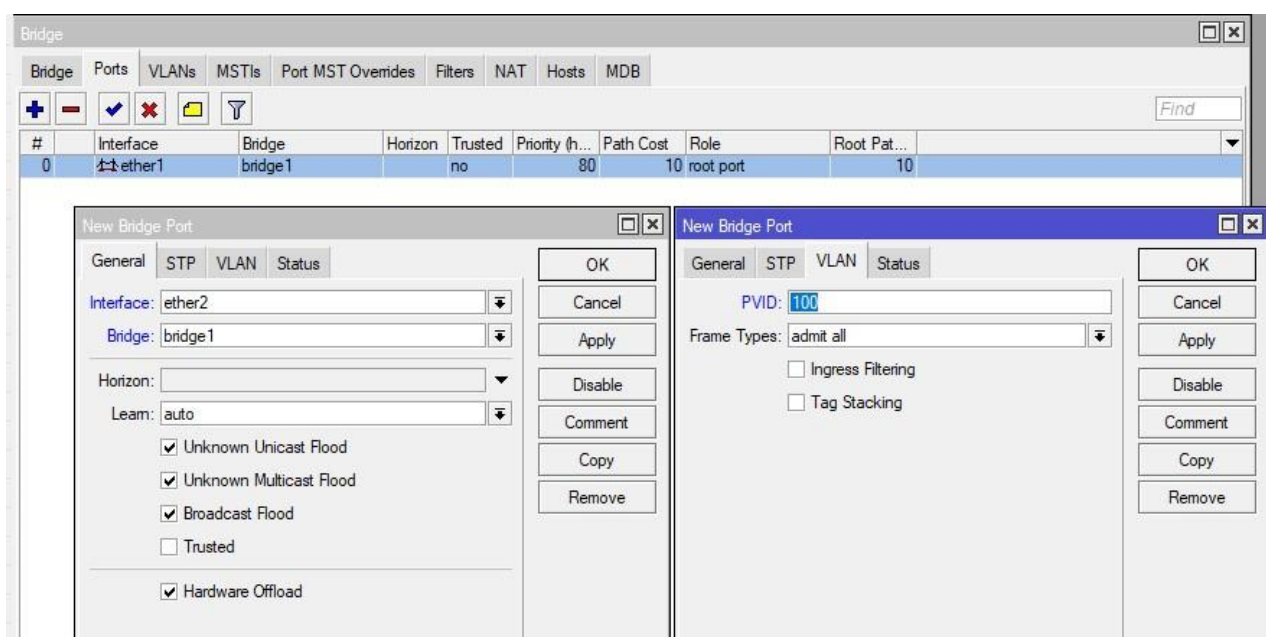
Согласно нашей схеме, нам нужно принять два тега: 100 и 99. Первый для ПК, второй для управления самим коммутатором (service tag). Создадим bridge.



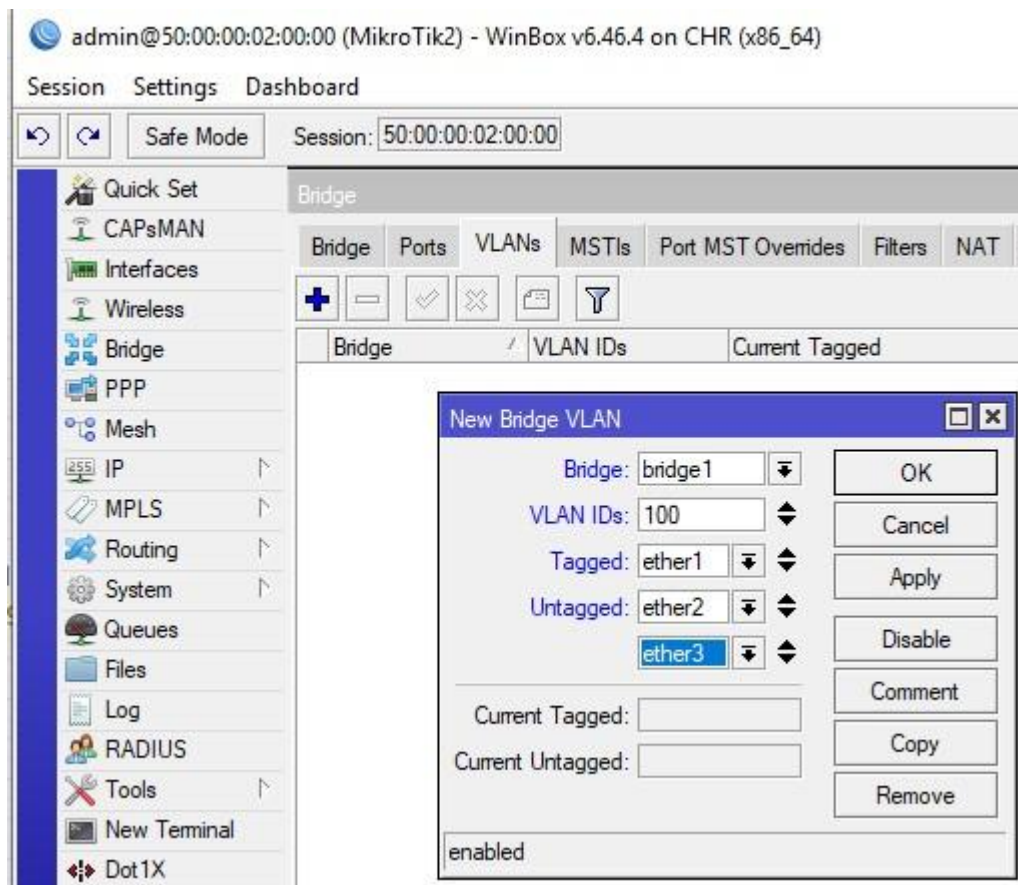
Добавим в него tagged ether1.



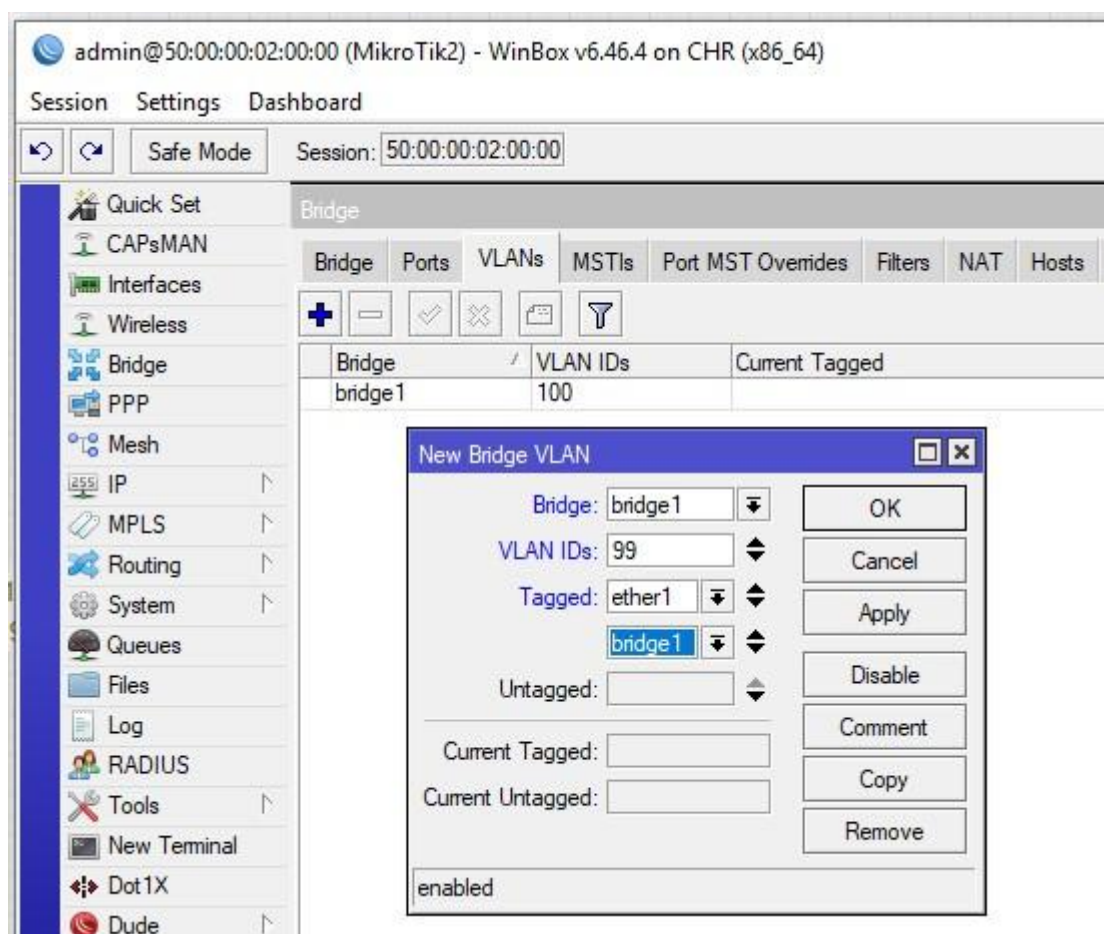
Untagged ether2, ether3. Указав PVID 100 на вкладке VLAN.



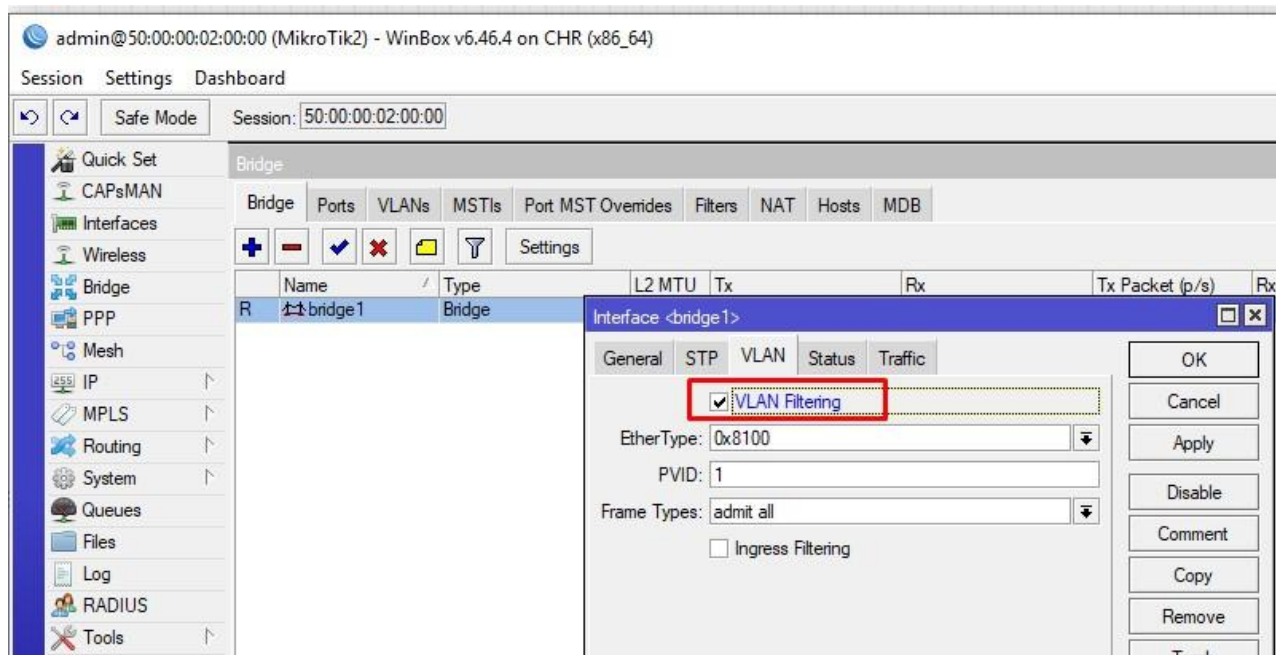
Переходим в вкладку VLANs бриджа. Указываем тегированные и не тегированные порты. В нашем случае tagged ether1, untagged ether2 и ether3.



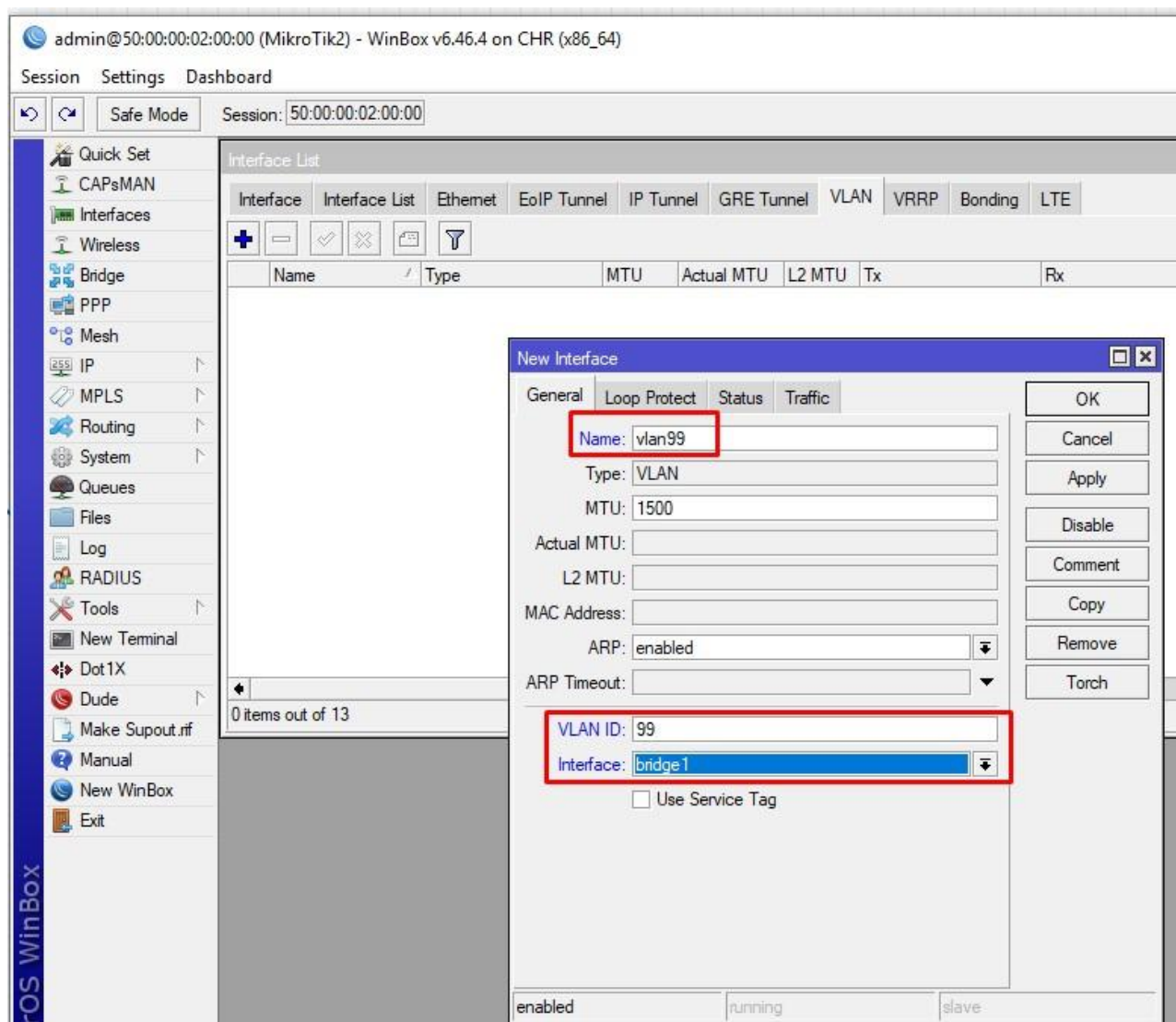
Добавляем VLAN для управления.



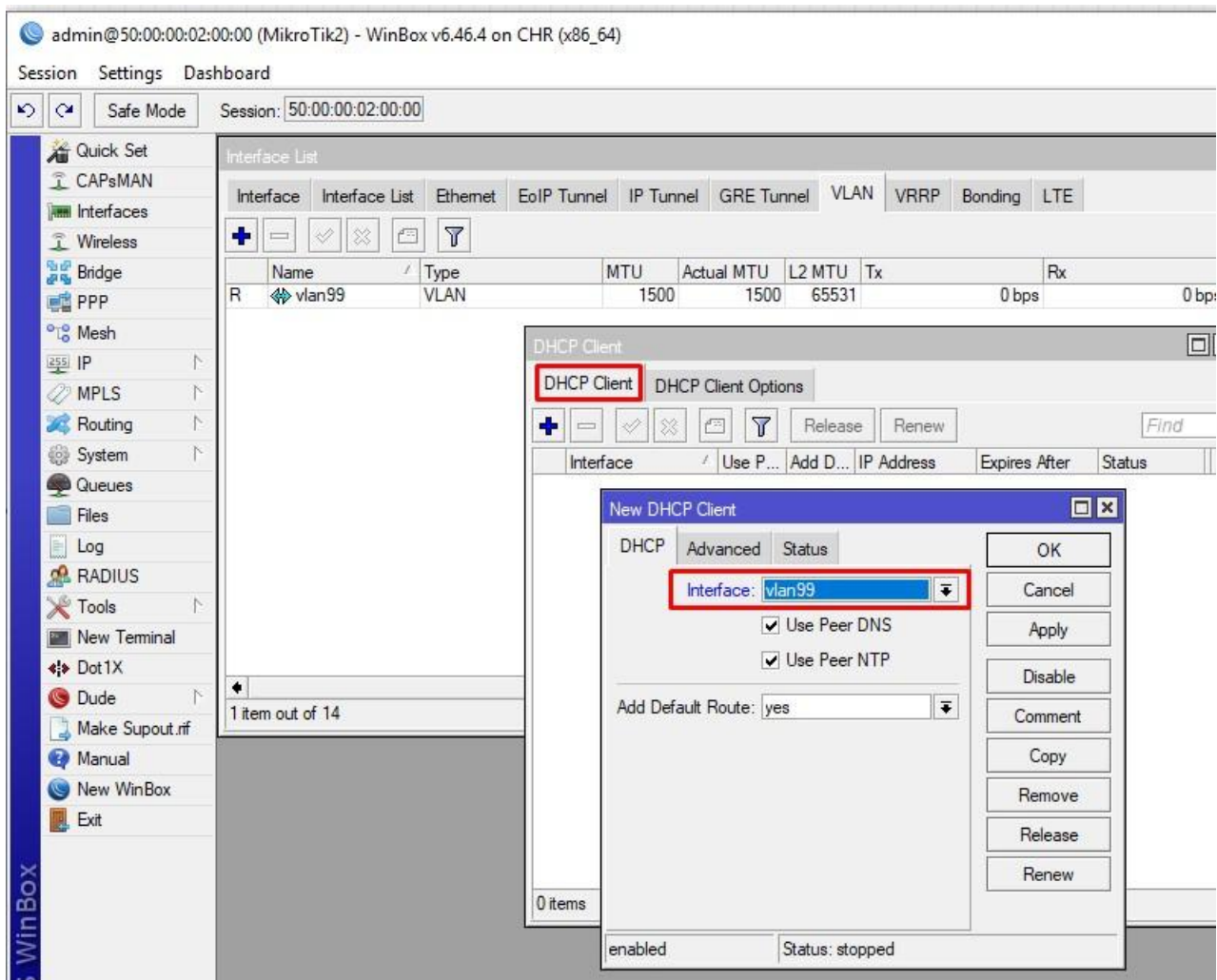
Перепроверив, включаем фильтрацию.



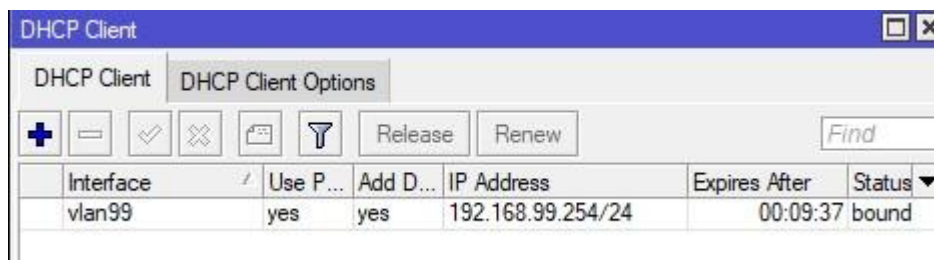
Далее нужно получить адрес из сети управления.



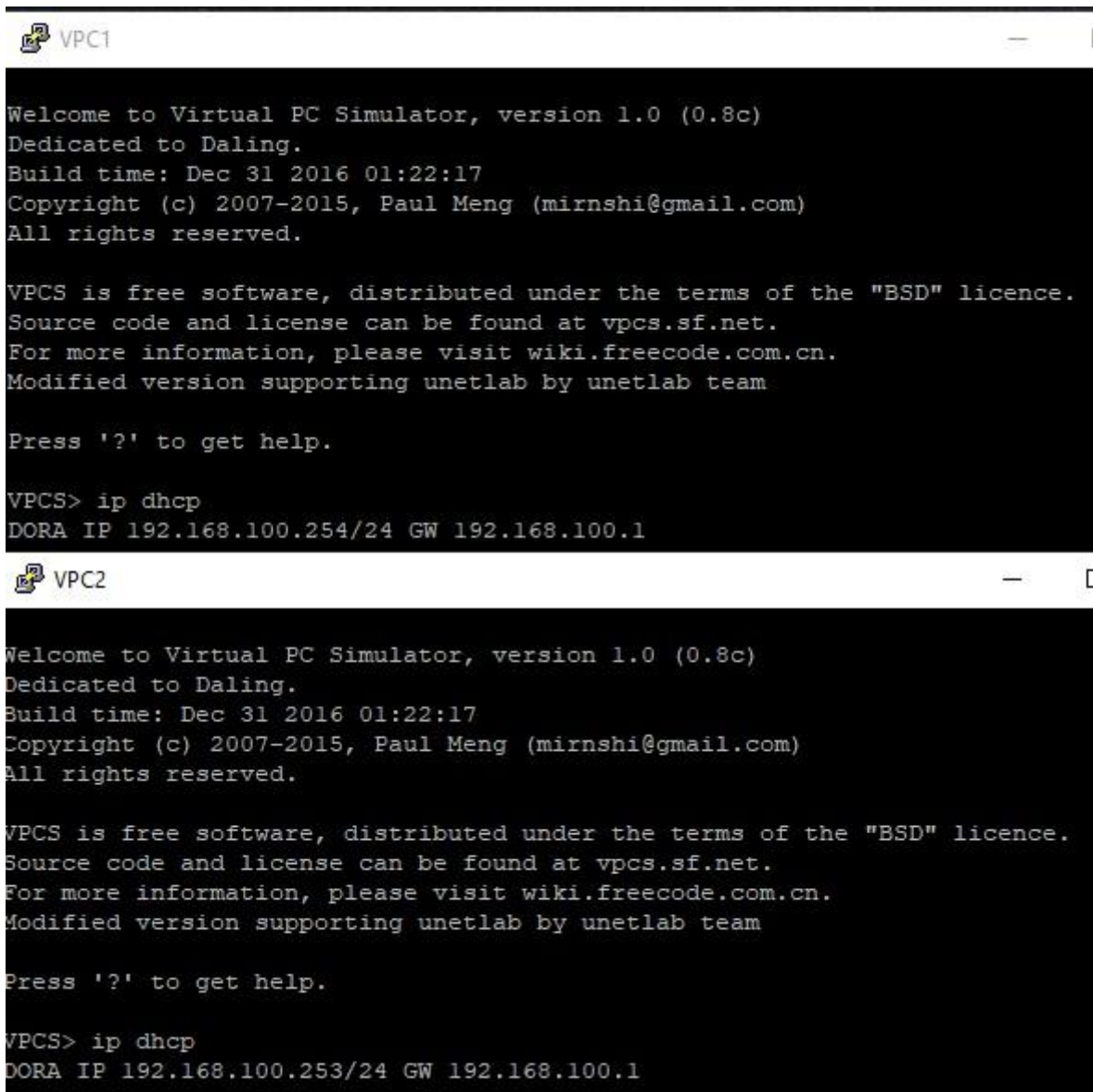
Повесим DHCP-Client на него.



После чего мы удачно получили адрес.



Далее нам нужно включить наши ПК и проверить какие адреса мы получили на них.



```
VPC1

Welcome to Virtual PC Simulator, version 1.0 (0.8c)
Dedicated to Daling.
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS> ip dhcp
DORA IP 192.168.100.254/24 GW 192.168.100.1

VPC2

Welcome to Virtual PC Simulator, version 1.0 (0.8c)
Dedicated to Daling.
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS> ip dhcp
DORA IP 192.168.100.253/24 GW 192.168.100.1
```

Настройка VLAN200, все порты подключены в него.

Настройка будет аналогична предыдущему примеру, за исключением номеров тэгов. В бридже на интерфейсах доступа укажем PVID 200.

#	Interface	Bridge	Horizon	Trusted	Priority (h...	Path Cost	Role	Root Pat...
0	ether1	bridge1		no	80	10	root port	10
1	ether3	bridge1		no	80	10	designated port	
2	ether2	bridge1		no	80	10	designated port	

Bridge Port <ether3>

General STP VLAN Status

PVID: 200

Frame Types: admit all

☐ Ingress Filtering

☐ Tag Stacking

Bridge Port <ether2>

General STP VLAN Status

PVID: 200

Frame Types: admit all

☐ Ingress Filtering

☐ Tag Stacking

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Укажем порты и сеть управления.

После, создаем интерфейс в Interfaces, вешаем на бридж и включаем DHCP-Client.

New Bridge VLAN

Bridge: bridge1

VLAN IDs: 200

Tagged: ether1

Untagged: ether2

ether3

Current Tagged:

Current Untagged:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Bridge VLAN <99>

Bridge: bridge1

VLAN IDs: 99

Tagged: ether1

bridge1

Untagged:

Current Tagged: bridge1

ether1

Current Untagged:

enabled

OK

Cancel

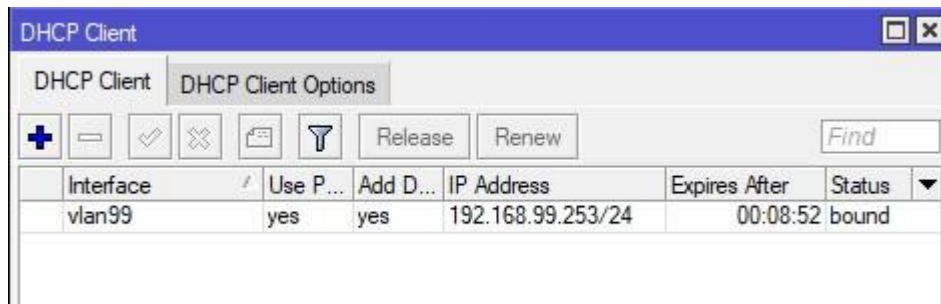
Apply

Disable

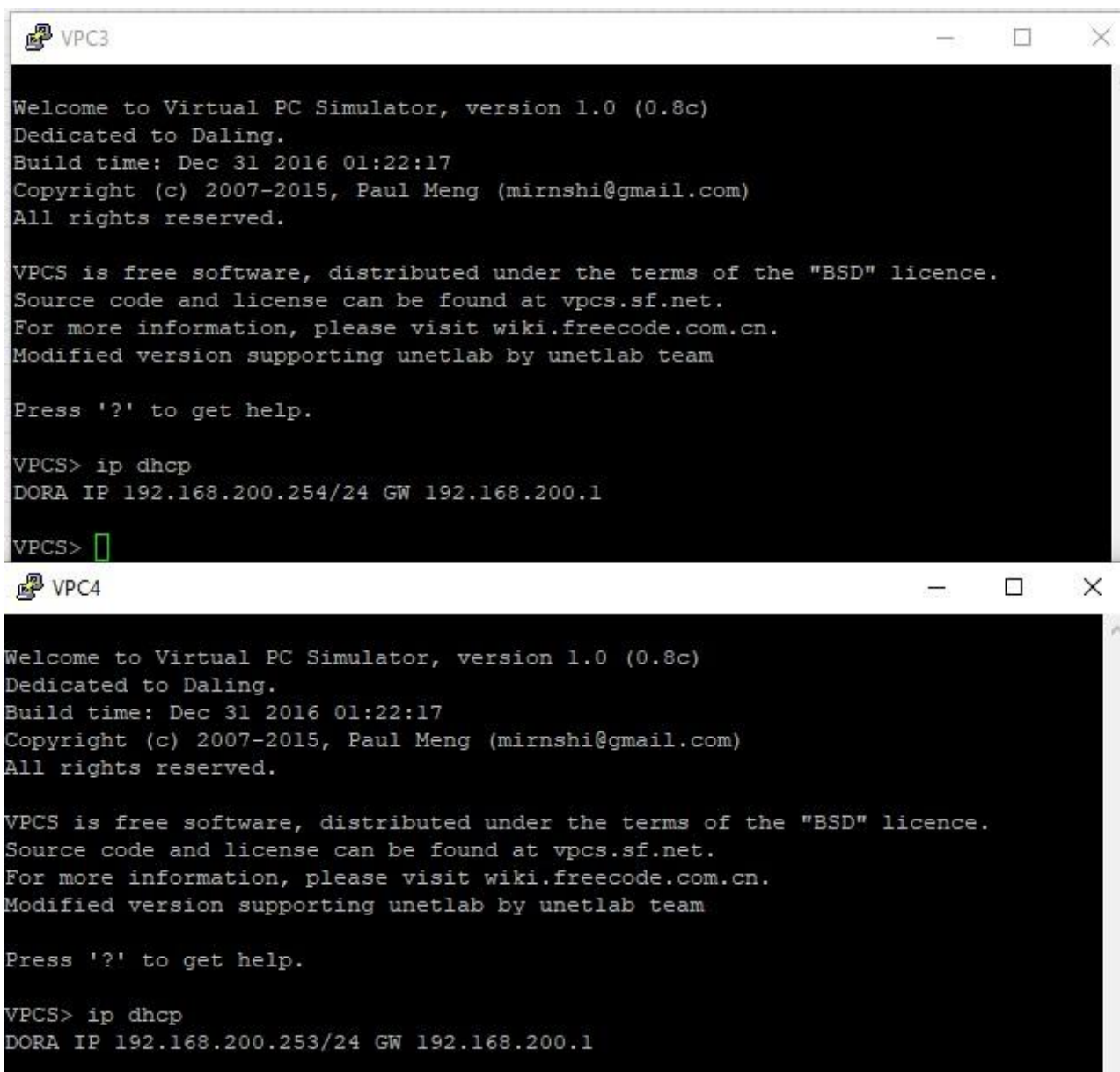
Comment

Copy

Remove



Включаем ПК и принимаем адреса.



Проверим связь между VPC4 и VPC1

```
VPC4
Dedicated to Daling.
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS> ip dhcp
DORA IP 192.168.200.253/24 GW 192.168.200.1

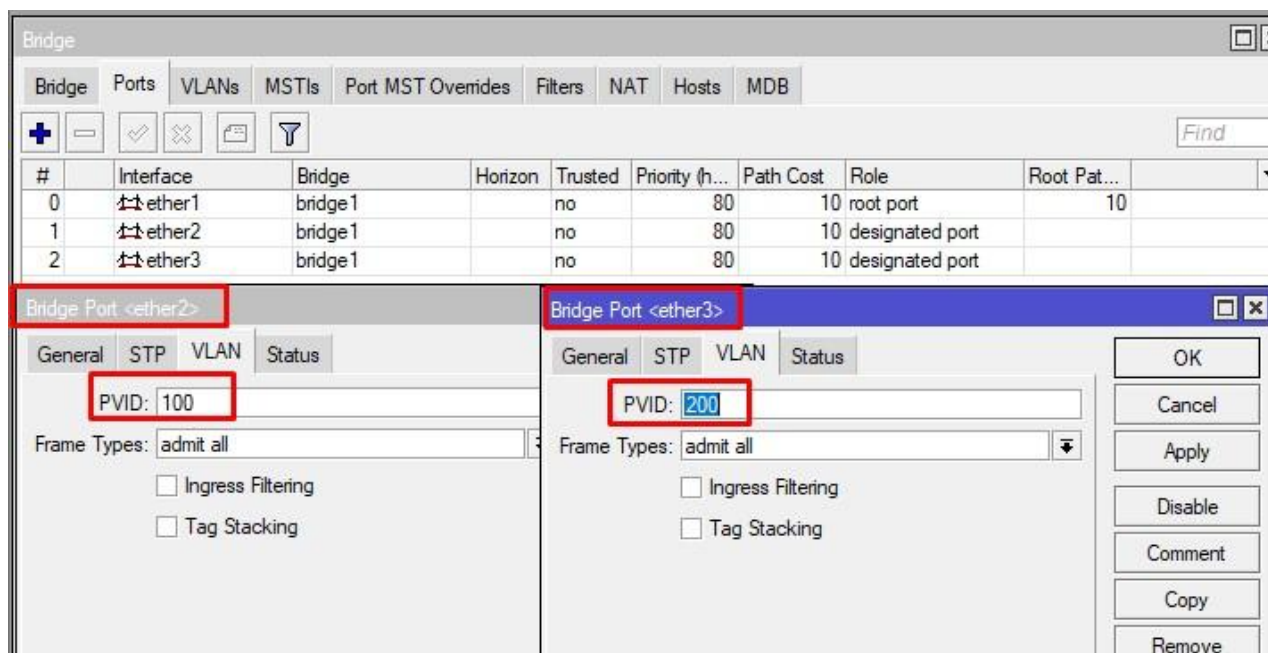
VPCS> ping 192.168.100.254

84 bytes from 192.168.100.254 icmp_seq=1 ttl=63 time=38.393 ms
84 bytes from 192.168.100.254 icmp_seq=2 ttl=63 time=39.990 ms
84 bytes from 192.168.100.254 icmp_seq=3 ttl=63 time=49.049 ms
84 bytes from 192.168.100.254 icmp_seq=4 ttl=63 time=47.192 ms
84 bytes from 192.168.100.254 icmp_seq=5 ttl=63 time=19.088 ms

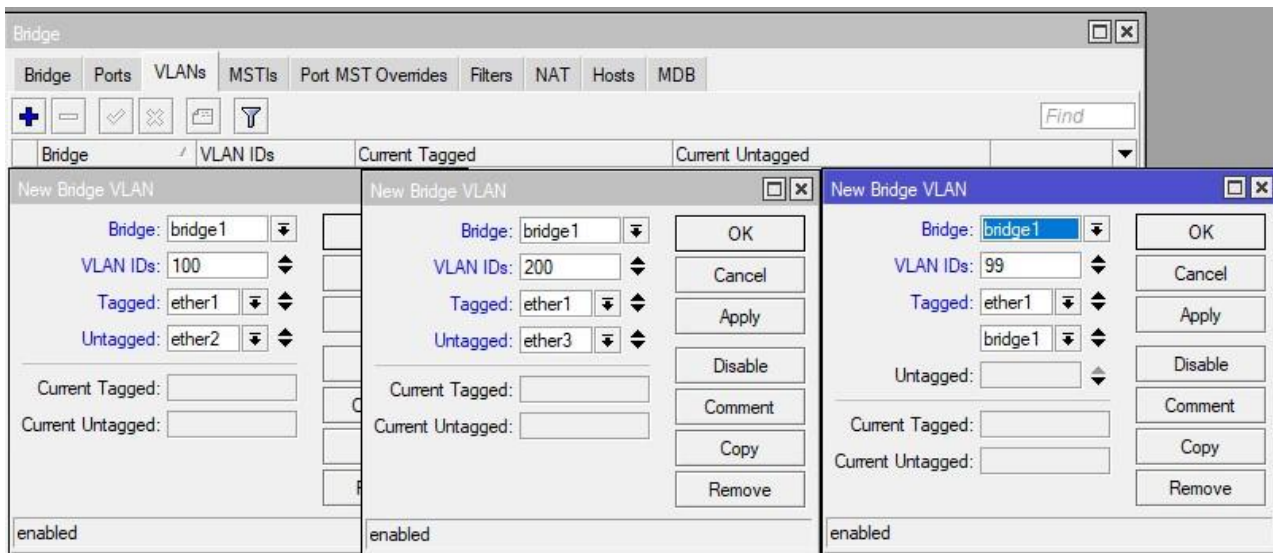
VPCS>
```

VLAN100 и VLAN200

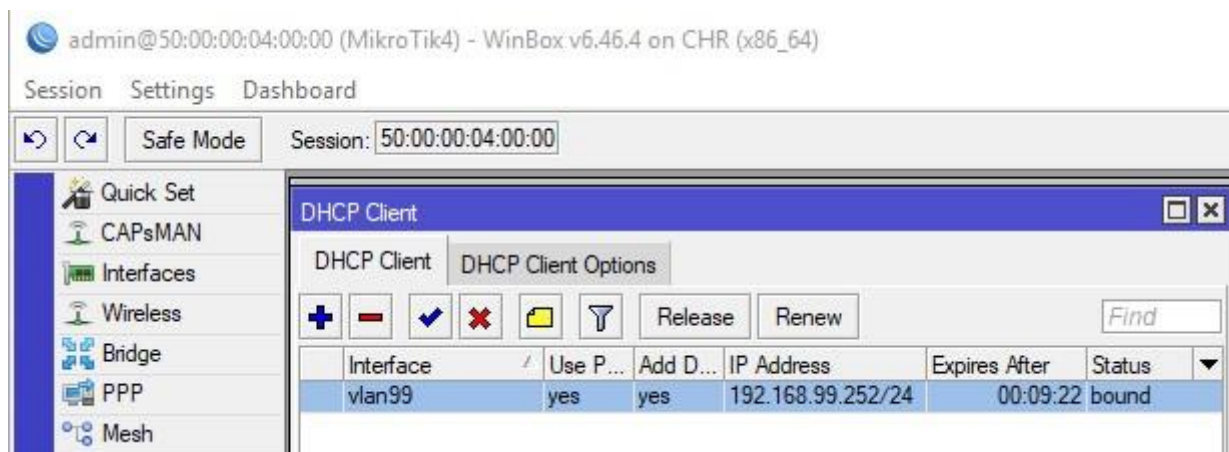
В предыдущих двух примерах мы настраивали свитчи только под определенные метки. А что, если на одном свитче живут разные сети. После создания бриджа на этапе добавления интерфейсов нужно указать соответствующее PVID. В нашем случае ether2 – 100, ether3 – 200.



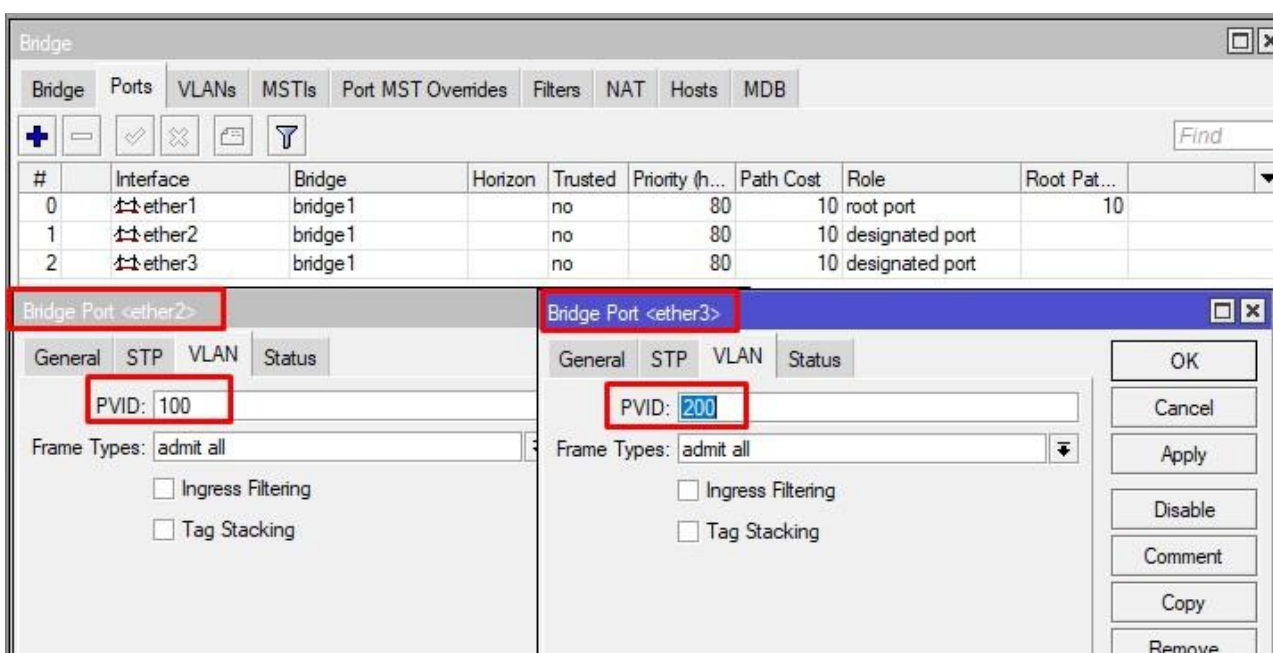
Настраиваем порты.



Не забываем включить фильтрацию и проверим что коммутатор получил адрес из нужной сети.

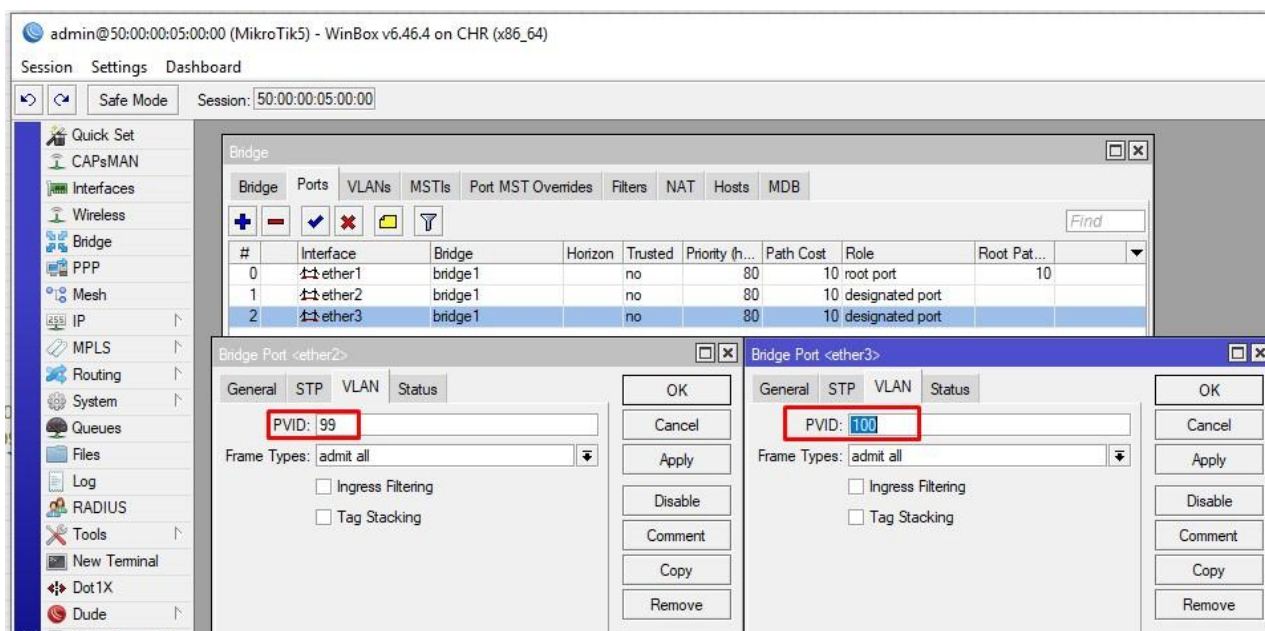


Включим рабочие станции.

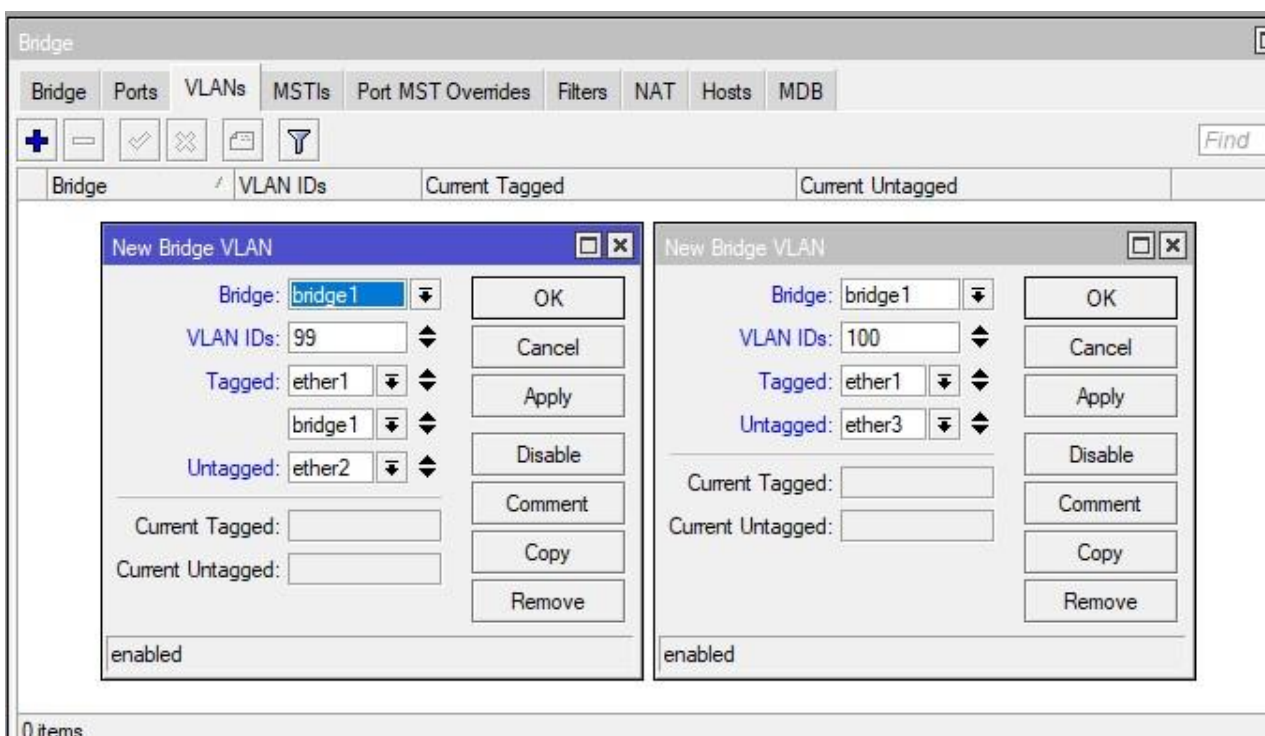


Сеть управления VLAN99

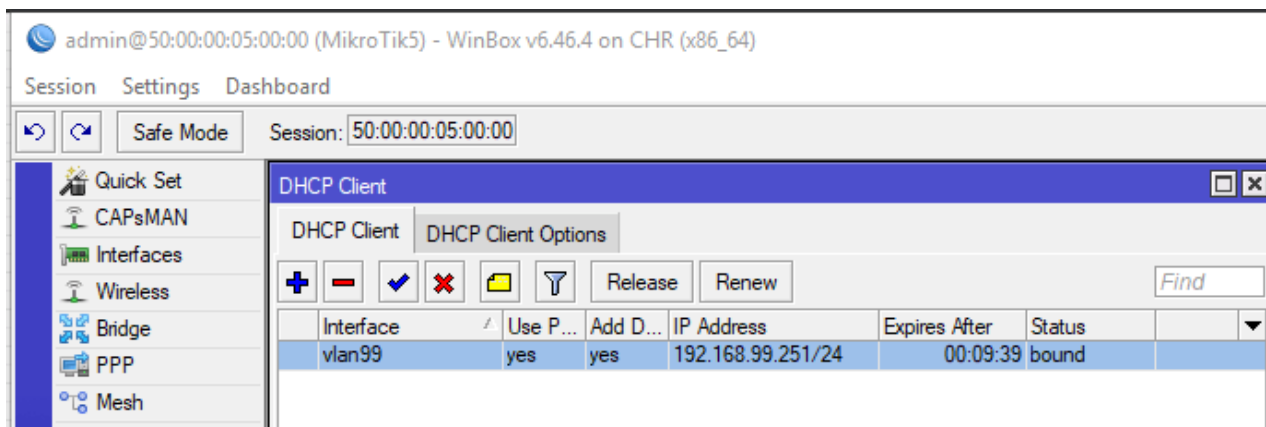
Ну и напоследок представим, что в одном коммутаторе доступа есть ПК административного персонала, за которыми работают администраторы, а также обычные пользователи. Посмотрим на PVID для интерфейсов.



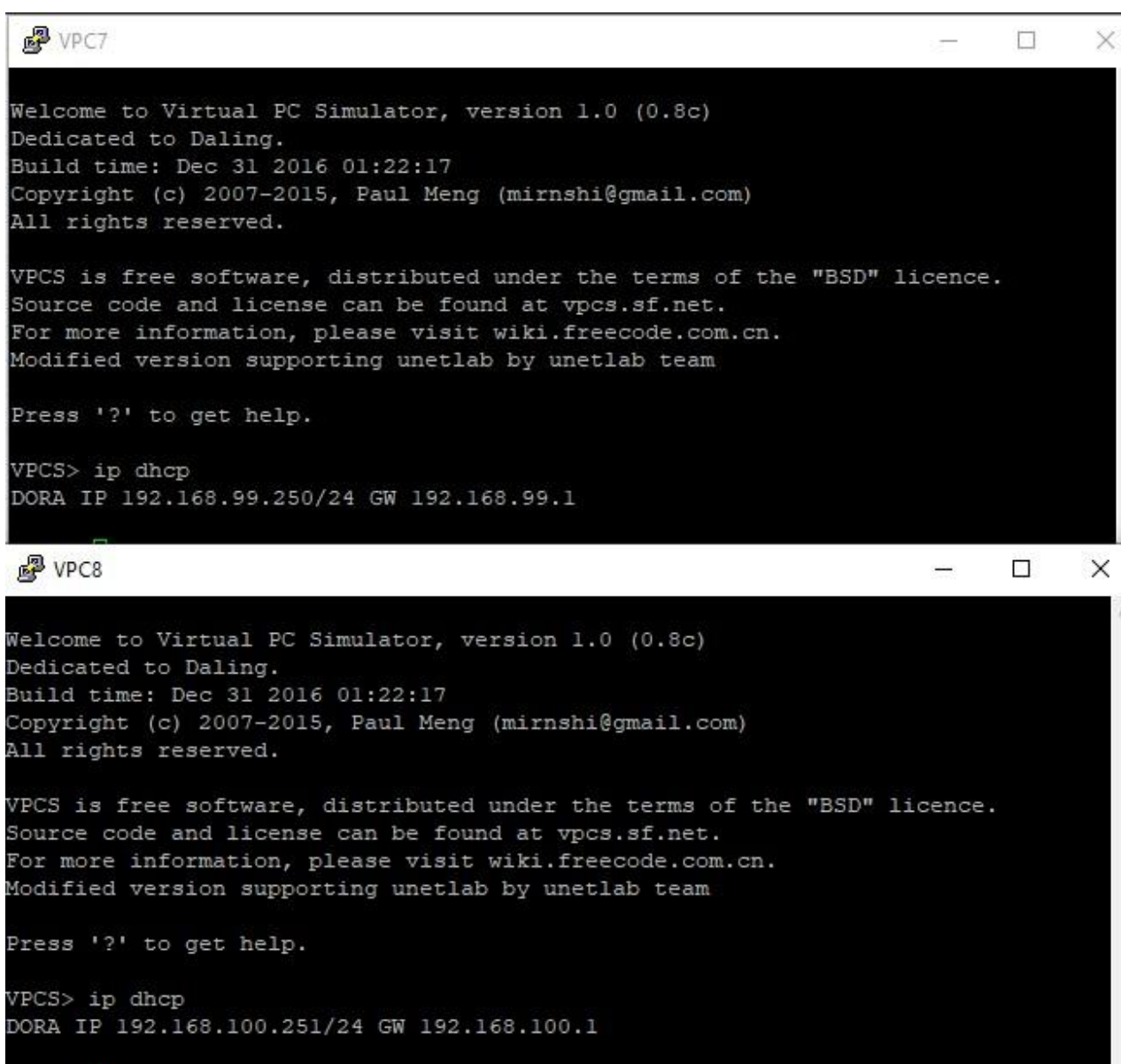
Т.к. нам нужно чтобы ПК администратора VP7 был в одной сети с коммутаторами и роутером, сделаем его untagged.



Получим адрес управления.



Включим оба ПК.



Попробуем проверить связь с коммутаторами и ПК.

```
VPCS> ping 192.168.99.1

84 bytes from 192.168.99.1 icmp_seq=1 ttl=64 time=2.541 ms
84 bytes from 192.168.99.1 icmp_seq=2 ttl=64 time=2.218 ms
84 bytes from 192.168.99.1 icmp_seq=3 ttl=64 time=2.303 ms
^C
VPCS> ping 192.168.99.254

84 bytes from 192.168.99.254 icmp_seq=1 ttl=64 time=4.089 ms
84 bytes from 192.168.99.254 icmp_seq=2 ttl=64 time=3.957 ms
84 bytes from 192.168.99.254 icmp_seq=3 ttl=64 time=4.062 ms
^C
VPCS> ping 192.168.99.253

84 bytes from 192.168.99.253 icmp_seq=1 ttl=64 time=4.435 ms
84 bytes from 192.168.99.253 icmp_seq=2 ttl=64 time=4.024 ms
84 bytes from 192.168.99.253 icmp_seq=3 ttl=64 time=3.636 ms
^C
VPCS> ping 192.168.99.252

84 bytes from 192.168.99.252 icmp_seq=1 ttl=64 time=4.303 ms
84 bytes from 192.168.99.252 icmp_seq=2 ttl=64 time=3.928 ms
84 bytes from 192.168.99.252 icmp_seq=3 ttl=64 time=3.596 ms
^C
VPCS> ping 192.168.99.251

84 bytes from 192.168.99.251 icmp_seq=1 ttl=64 time=1.012 ms
84 bytes from 192.168.99.251 icmp_seq=2 ttl=64 time=0.669 ms
84 bytes from 192.168.99.251 icmp_seq=3 ttl=64 time=0.779 ms
^C
VPCS> ping 192.168.100.254

84 bytes from 192.168.100.254 icmp_seq=1 ttl=63 time=8.971 ms
84 bytes from 192.168.100.254 icmp_seq=2 ttl=63 time=5.522 ms
84 bytes from 192.168.100.254 icmp_seq=3 ttl=63 time=4.679 ms
^C
VPCS> ping 192.168.200.254

84 bytes from 192.168.200.254 icmp_seq=1 ttl=63 time=8.645 ms
84 bytes from 192.168.200.254 icmp_seq=2 ttl=63 time=31.161 ms
84 bytes from 192.168.200.254 icmp_seq=3 ttl=63 time=12.657 ms
^C
VPCS> █
```

Взглянем на DHCP сервер.

admin@50:00:00:01:00:01 (Gateway) - WinBox v6.46.4 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 50:00:00:01:00:01 Uptime: 01:52:32

Quick Set

CAPsMAN

Interfaces

Wireless

Bridge

PPP

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

RADIUS

Tools

New Terminal

Dot1X

Dude

Make Snapshot

DHCP Server

DHCP

Networks

Leases

Options

Option Sets

Vendor Classes

Alerts

Check Status

Find

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host	Expires After	Status
D	192.168.99.250	00:50:79:66:68:0C	1:0:50:79:66:68:c	dhcp3	192.168.99.250	00:50:79:66:68:0C	VPCS1	00:06:32	bound
D	192.168.99.251	50:00:00:05:00:00	1:50:0:0:5:0:0	dhcp3	192.168.99.251	50:00:00:05:00:00	MikroTik5	00:05:34	bound
D	192.168.99.252	50:00:00:04:00:00	1:50:0:0:4:0:0	dhcp3	192.168.99.252	50:00:00:04:00:00	MikroTik4	00:08:02	bound
D	192.168.99.253	50:00:00:03:00:00	1:50:0:0:3:0:0	dhcp3	192.168.99.253	50:00:00:03:00:00	MikroTik3	00:08:15	bound
D	192.168.99.254	50:00:00:02:00:00	1:50:0:0:2:0:0	dhcp3	192.168.99.254	50:00:00:02:00:00	MikroTik2	00:08:09	bound
D	192.168.100.251	00:50:79:66:68:0D	1:0:50:79:66:68:d	dhcp1	192.168.100....	00:50:79:66:68:0D	VPCS1	00:06:41	bound
D	192.168.100.252	00:50:79:66:68:0A	1:0:50:79:66:68:a	dhcp1	192.168.100....	00:50:79:66:68:0A	VPCS1	00:08:28	bound
D	192.168.100.253	00:50:79:66:68:07	1:0:50:79:66:68:7	dhcp1	192.168.100....	00:50:79:66:68:07	VPCS1	00:09:59	bound
D	192.168.100.254	00:50:79:66:68:06	1:0:50:79:66:68:6	dhcp1	192.168.100....	00:50:79:66:68:06	VPCS1	00:06:31	bound
D	192.168.200.252	00:50:79:66:68:0B	1:0:50:79:66:68:b	dhcp2	192.168.200....	00:50:79:66:68:0B	VPCS1	00:08:30	bound
D	192.168.200.253	00:50:79:66:68:09	1:0:50:79:66:68:9	dhcp2	192.168.200....	00:50:79:66:68:09	VPCS1	00:05:13	bound
D	192.168.200.254	00:50:79:66:68:08	1:0:50:79:66:68:8	dhcp2	192.168.200....	00:50:79:66:68:08	VPCS1	00:05:01	bound

12 items

Далее мы можем создавать interface-list и управлять трафиком через firewall. На этом настройка VLAN Bridge на роутере MikroTik под управлением routeros завершена, спасибо за внимание.

Вы хорошо разбираетесь в Микротиках? Или впервые недавно столкнулись с этим оборудованием и не знаете, с какой стороны к нему подступиться? В обоих случаях вы найдете для себя полезную информацию в углубленном курсе «[Администрирование сетевых устройств MikroTik](#)». В курсе много практических лабораторных работ по результату выполнения которых вы получите обратную связь. После окончания обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [тут](#).