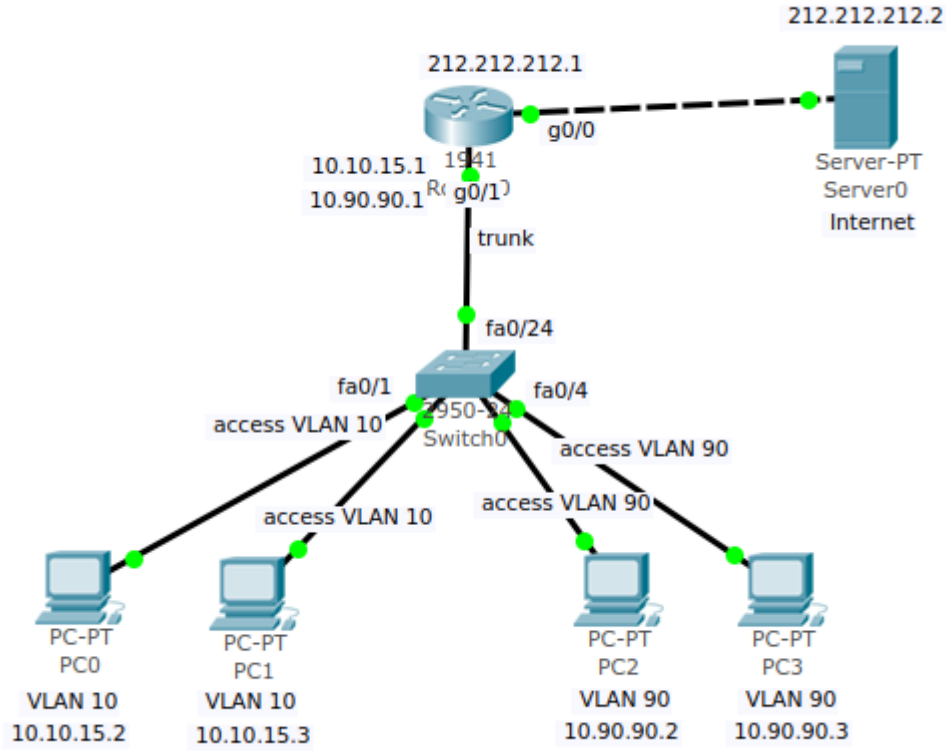
DHCP на VLAN-ах



Задача разбить сеть на VLAN и поднять каждому DHCP-server

VLAN

Создаем vlan по образу и подобию.

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp5s9.10
VLAN=yes
DEVICE=enp5s9.10
PHYSDEV=enp5s9
ONBOOT=yes
BOOTPROTO="static"
IPADDR=10.10.15.1
PREFIX=24
```

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp5s9.90
VLAN=yes
DEVICE=enp5s9.90
PHYSDEV=enp5s9
ONBOOT=yes
```

```
BOOTPROTO="static"
IPADDR=10.90.90.1
PREFIX=24
```

DHCP

If more than one network interface is attached to the system, but the DHCP server should only be started on one of the interfaces, configure the DHCP server to start only on that device. In /etc/sysconfig/dhcpd, add the name of the interface to the list of DHCPDARGS:

```
# Command line options here
DHCPDARGS="enp5s9.10 enp5s9.90"
```

По умолчанию dhcpd пишет два основных log файла, /var/lib/dhcpd/dhcpd.leases – список выданных адресов и /var/log/messages – ошибки и все остальное, проблема в том что в /var/log/messages хранятся логи не только dhcpd но и все остальные, что делает поиск проблем очень сложной задачей. Для того что бы нам перенаправить поток логов в нужный файл и не зацепить лишнего мы используем параметр log-facility который указывали в настройках DHCP-сервера.

Создать папку в которой будут храниться наши лог-файлы:

```
# mkdir /var/log/dhcp
```

Создать файл logrotate дабы все не хранилось в одном файле и периодически очищалось, для этого в папке /etc/logrotate.d/ создаем файл dhcpd в котором следующее содержимое

```
# cat /etc/logrotate.d/dhcpd
/var/log/dhcp/dhcpd.log {
    rotate 4
    missingok
    daily
    sharedscripts
    create 0644 root root
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null`
2> /dev/null || true
```

```
    endscript
}
```

Ну и последнее наше действие в файле /etc/rsyslog.conf добавляем параметр с комментарием, который и будет перенаправлять все наши логи в нужный нам файл.

```
# DHCPD Log file
local5.*
/var/log/dhcp/dhcpd.log
```

В данном случае local5 служит в качестве маркера, по которому можно направить поток логов в нужное русло, всего таких маркеров 7 и если это занять вы будете использовать любой из local1-7.

Копируем образцы

```
# cp /usr/share/doc/dhcp*/dhcpd.conf.example /etc/dhcp/
```

Приводим к такому виду dhcp.conf:

```
option domain-name "my.server.com";
option domain-name-servers 192.168.113.1, 8.8.8.8;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local5;

## START Потом отключить
subnet 10.10.5.0 netmask 255.255.255.0 {
}
## END

## VLAN 10 Pool
subnet 10.10.15.0 netmask 255.255.255.0 {
range 10.10.15.20 10.10.15.100;
option routers 10.10.15.1;
option domain-name "my.server.com";
option domain-name-servers 192.168.113.1, 8.8.8.8;
option broadcast-address 10.10.15.255;
default-lease-time 600;
```

```
max-lease-time 7200;
}

## VLAN 90 Pool
subnet 10.90.90.0 netmask 255.255.255.0 {
range 10.90.90.40 10.90.90.100;
option domain-name "my.server.com";
option domain-name-servers 192.168.113.1, 8.8.8.8;
option broadcast-address 10.90.90.255;
option routers 10.90.90.1;
default-lease-time 600;
max-lease-time 7200;
}
```

После того как все параметры заданы и все файлы заполнены нужной информацией, можно запустить DHCP-сервер, поставить его на автозапуск при включении и проверить все ли у нас работает правильно

```
systemctl start dhcpd
systemctl enable dhcpd
```

Маршрутизация между VLAN

По умолчанию ПК из разных VLAN не видят друг друга. Но бывают ситуации, когда это нужно.

```
# vim /etc/sysctel.conf
net.ipv4.ip_forward=1

# sysctl -p
# service network restart
```

Add these two lines (place them according to your iptables file configuration):

```
if_lan10="enp5s9.10"
if_lan90="enp5s9.90"

-A FORWARD -i $if_lan10 -o $if_lan90 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i $if_lan90 -o $if_lan10 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
```