Лабораторная работа 10.

Развертывание DHCP сервера на Linux.

1. Теоретическая часть.

1.1 DHCP

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер».

DHCP и BOOTP серверы работают на портах ***TCP и UDP 67 и 68***. BOOTP уже устаревший протокол и позволяет выдавать лишь самые необходимые сетевые настройки хостам. Тем не менее, он отлично подходит для загрузки и работы бездисковых рабочих станций.

Режимы работы DHCP:

1. Ручное распределение адресов. В файле конфигурации администратор сам настраивает привязки MAC-IP, а система уже выдает их, когда к ней обратятся за адресом соответствующие клиенты.
2. Автоматическое распределение адресов. Раздача адресов клиентам выполняется автоматически из доступного пула, адреса выдаются навсегда, то есть, нет времени аренды адреса (по сути так работает протокол BOOTP)
3. Динамическое распределение адресов. Адреса выдаются из пула, но каждая связка имеет время аренды, после которого если клиент не подтверждает связки, адрес освобождается для дальнейшего использования.

1.1.1 Процесс получения IP адреса

Когда клиент подключается к сети, он проходит 4 шага, результатом выполнения которых, является получение IP адреса в аренду.

**Тип пакетов Discover**

В первом шаге, клиент передает широковещательным запросом пакет типа DHCPDISCOVER. DHCPDISCOVER пакет находит серверы протокола динамического выбора хост-машины на сети. Так как хост еще не имеет никакого IP адреса в процессе первоначального подключения к сети, он использует широковещательные пакеты второго и третьего уровней, чтобы связаться с сервером dhcp/bootp и получить IP адрес.

Содержимое пакета DHCPDISCOVER

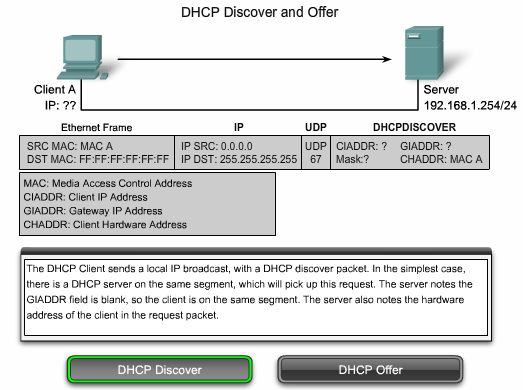


Рисунок 1.

**Тип пакетов OFFER**

Когда сервер DHCP получает пакет DHCDISCOVER, он начинает проверку доступных для выдачи IP адресов, если он его находит, то выдает доступный IP адрес в аренду, создавая у себя в таблице записей выданных адресов, новую запись содержащую MAC адрес компьютера, IP адрес который ему выдался и например имя записи (зависит от типа dhcp). После чего передает данную связку в виде предложения хосту запросившему адрес, в виде пакета DHCPOFFER. DHCPOFFER сообщение посылается как unicast пакет, используя MAC адрес отправителя (MAC адрес сервера dhcp) и MAC адрес получателя (MAC адрес компьютера запросившего получение адреса).

Содержимое пакета DCHPOFFER:

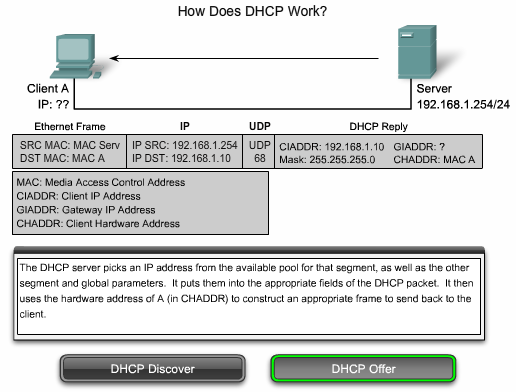


Рисунок 2.

*Обратите внимание: При некоторых обстоятельствах, обмен сообщениями dhcp от сервера к ПК запросившему IP адрес, может передаваться в виде широковещательных пакетов.*

**Тип пакетов Request**

Когда клиент получает DHCPOFFER от сервера, он посылает назад DHCPREQUEST пакет. Это пакет имеет две цели: начало аренды IP адреса или возобновление арендного договора на IP адрес, а так же проверка нахождения компьютера в сети. В случае, когда DHCPREQUEST используется для начало аренды IP адреса, клиент запрашивает сервер, чтобы тот перед окончательным назначением ему IP адреса проверил, не назначался ли предполагаемый для выдачи в пакете IP адрес кому-то другому, если нет, то присвоение адреса происходит высылкой клиенту пакета DHCPACK (являющегося клоном DHCOFFER с незначительными изменениями флагов, сообщающем только то, что это заключительный пакет в процессе выдачи IP адреса).

Пакет DHCPREQUEST, который является ответом от хоста, который готов принять IP адрес с сервера. Так же служит специальным сигналом всем другим серверам, которые могли действовать в данном сегменте сети, что связка IP ---MAC уже привязана к такому-то dhcp серверу (в данном случае адрес этого dhcp сервера, его MAC адрес).

**Тип пакетов Acknowledge**

При получении DHCPREQUEST сообщения, сервер проверяет информацию арендного договора, создает новую запись dhcp для переданного в аренду IP адреса, и отвечает unicast пакетом DHCPACK (MAC получателя тут MAC хоста клиента запросившего себе IP адрес). DHCPACK сообщение является дубликатом пакета DHCPOFFER, имеющего только одно отличие в поле тип сообщения. Когда клиент получает DHCPACK пакет, он регистрирует информацию конфигурации, то есть настраивает свой IP и другие параметры адресов в соответствие с присланными ему dhcp сервером.

На рисунке изображен весь процесс получения адреса с помощью DHCP:

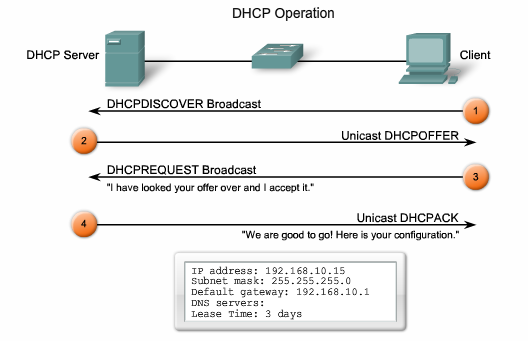


Рисунок 3.

4 параметра, которые обязательно выдаются DHCP и BOOTP сервером DHCP клиенту:

- IP адрес Адрес IP

- Адрес шлюза по умолчанию

- Маска сети

- адрес DNS сервера

1.1.2 Различия между протоколами DHCP и BOOTP:

* BOOTP не умеет выдавать адреса из пула.
* BOOTP не поддерживает механизм аренды адреса, следовательно выдает его навсегда.
* BOOTP может раздавать клиенту только описанные выше, 4-сетевых параметра.
  + 1. Преимущества и недостатки DHCP.

|  |  |
| --- | --- |
| **Преимущества** | **Недостатки** |
| Не надо настраивать каждый компьютер в отдельности, системы Windows по умолчанию настраиваются как клиенты DHCP, при установке систем UNIX указать, что они - клиенты DHCP тоже очень просто. | Если сервер DHCP не доступен, многие из компьютеров сети вообще не смогут начать работу, и через определенное время, связанное с политикой назначения адресов, все компьютеры окажутся "отрезанными" от сети. |
| Все настройки делаются централизованно, при изменении одной настройки (например, адреса основного шлюза сети), нет нужды менять настройки на каждом компьютере. | Сбои DHCP труднее диагностировать, т.к. они проявляются в виде жалоб пользователей (причем не одновременных), на невозможность войти в сеть, а это может быть вызвано дюжинами причин. |
| Можно забыть о настройке параметров сети всех компьютеров, кроме DHCP-сервера, навсегда о них позаботится сервер DHCP. | Использование DHCP усложняет учет событий в сети: ведь в файлы протоколов заносятся IP-адреса компьютеров. Там, где адреса компьютерам выдаются динамически, один и тот же адрес может принадлежать разным компьютерам в разное время. |

1.1.4 Формат cообщения протокола динамического выбора хост-машины

Разработчики DHCP должны были оставить совместимость с BOOTP и для DHCP использовали тот же самый BOOTP формат сообщения. Однако, вследствие того что DHCP имеет больше функциональных возможностей чем BOOTP, к нему добавилось поле с дополнительными DHCP параметрами. При передачи данных сообщений с клиентами умеющими работать только с устаревшим BOOTP, поле дополнительных настроек DHCP хостом-получателем, способным работать только по BOOTP, игнорируется.

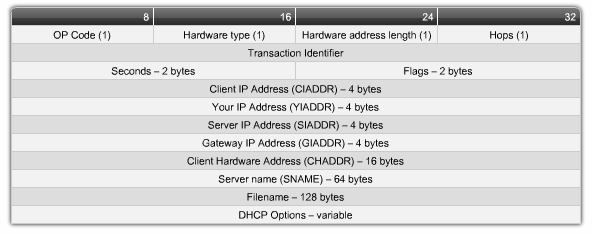


Рисунок 4.

1.1.5 DHCP RELAY

Если dhcp сервер находится за маршрутизаторам, то на маршрутизаторе надо указать релей IP адреса dhcp сервера находящегося за ним, чтобы маршрутизатор знал, куда отправлять запросы типа DHCPDISCOVER, которые приходят на его интерфейсы которые не содержат в своих подсетях dhcp серверы.

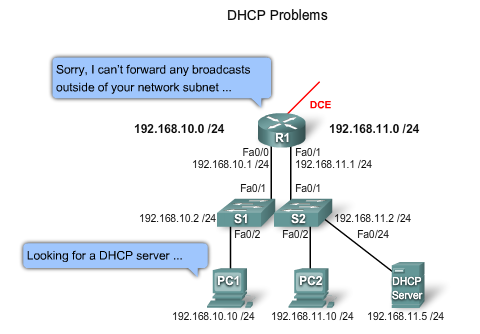


Рисунок 5.

На маршрутизаторе задать DHCP Relay можно командой **ip helper-address**.

Кроме основных сетевых параметров службы dhcp может передать на клиент следующие настройки, так же эти данные могут передаваться и через Relay:

*Port 37: Time*

*Port 49: TACACS*

*Port 53: DNS*

*Port 67: DHCP/BOOTP client*

*Port 68: DHCP/BOOTP server*

*Port 69: TFTP*

*Port 137: NetBIOS name service*

*Port 138: NetBIOS datagram service*

1. Практическая часть.

Задание 1.

Настройка статического IP адреса на DHCP сервере.

1) Обычно в современных дистрибутивах Linux за сетевыми настройки отвечает программа-служба – NetworkManager, как раз значок сети в тулбаре у часов. Так как он не всегда работает должным образом, а серверы обычно вообще запущенны в режиме инициализации init 3, то есть без графического режима, то правильнее будет настроить статический адрес нашего сервера с помощью службы network и текстового конфигурационного файла сетевого интерфейса.

Поэтому первым делом отключим NetworkManager, сделать это можно двумя путями:

1-й используя графическую утилиту управления службами в Linux RedHat, запустить которую можно командой system-config-sevices.

2-й использовать консольную утилиту управления сервисами в Linux RedHat --- chkconfig:

chkconfig --list , покажет нам все службы и их текущие состояние, среди них будет NetworkManager, включенная на уровнях 2-3-5, ее надо отключить командой:

chkconfig NetworkManager off

*Примечение: пример опций chkconfig в приложение 1.*

2) Теперь надо просмотреть информацию о сетевой карте, это можно сделать несколькими способами:

Способ 1 - утилита ifconfig, если сетевая карта отключена, то ifconfig –a покажет все интерфейсы.

Способ 2 – утилита dmesg, если уже известно как она называется, то dmesg |grep ethX

Способ 3 – утилита mii-tool

Способ 4 – утилита lshw, которая показывает развернутую информацио о железе в сервере/ПК, но для сетевой карты можно воспользоваться более коротким выводом, используя команду:

lshw –class network

В данной лабораторной работе надо воспользоваться именно ей, но она не установлена, ее нужно установить:

**yum install lshw**

3) Настроить на ней статический сетевой адрес, ниже приведен универсальный шаблон.

DEVICE=eth0

BOOTPROTO=static

HWADDR=00:01:02:03:04:05

ONBOOT=yes

NM\_CONTROLLED=”no”

DHCP\_HOSTNAME=hostname.my.domain

IPADDR=Ваш.IP.адрес

NETMASK=255.255.255.0

GATEWAY=IP.адрес.шлюза

TYPE=Ethernet

Пока мы не установили службу dhcp понадобится интернет (тип сетевого интерфейса NAT), для этого впишем IP адрес получаемый из dhcp службы сервиса NAT виртуальной платформы VirtualBox:

IP – 10.0.2.15

MASK – 255.255.255.0

GATEWAY – 10.0.2.2 (адрес следующего перелета для маршрута по умолчанию мы можем посмотреть командой route –n)

Осталось только настроить адрес DNS сервера, для чего внести запись в файл /etc/resolv.conf:

Для исп. DNS сервере вуза как основного

nameserver 82.137.178.4

Или адрес 8.8.8.8, чтобы использовать основным DNS сервер компании Google.

Данные настройки надо внести в файл /etc/sysconfig/networking-scripts/ifcfg-ethX. Предварительно сделав резервную копию текущего.

Разумеется MAC адрес должен быть тот, который вы найдете в информации о сетевой карте, **опция NM\_CONTROLLED=”no”** , означает то, что ваша сетевая карте не будет контролироваться NetworkManager, хотя это уже принципе неважно, мы его уже отключили как службу.

Перезапустить сетевую службу network:

/etc/init.d/network restart

С помощью утилиты ifconfig убедится, что сетевой интерфейс получил нужный адрес, а с помощью утилиты ping проверить его доступность с самого сервера.

Задание 2.

Установка и настройка DHCP сервера.

**2.1 Установка dhcp службы:**

Для установки dhcp сервера на ОС Linux CentOS нужно обновить пакет *dhclient* и установить пакет самого dhcp сервера *dhcp*:

**yum update dhclient**

**yum install dhcp**

Примечание: на Linux Ubuntu dhcp сервер ставится так:

**sudo apt-get install isc-dhcp-server**

* 1. Зайти на сетевой диск [\\app.sstu.ru\soft\files](file:///\\app.sstu.ru\soft\files) и скачать файл с примером настройки службы dhcp. Для чего:

- создать точку монтирования сетевого диска – **mkdir /mnt/share**

- смонтировать сетевой диск как сетевой диск windows, для чего использовать тип файловой системы cifs (ранее smbfs):

**mount –t cifs //app.sstu.ru/soft/files /mnt/share –o username=sdsd\test**

И ввести любой пароль.

* 1. Установить статичный адрес, который будет использоваться для интерфейса “Внутренняя сеть”. По аналогии установки IP адреса 10.0.2.15:

IP адрес с=задать следующий: 192.168.100+по журналу.3, IP адрес шлюза 192.168.10X.1, маска 255.255.255.0

**2.2 Знакомство с конфигурационным файлом dhcpd.conf**

После установки в каталоге /etc/dhcp появится файл dhcp.conf, на самом деле он является лишь ссылкой на файл dhcpd.conf.sample с примерами настройки dhcp сервера расположенного в каталоге /usr/share/doc/dhcp-x.x.x/, содержимое этого файла имеет вид, приведенный ниже, зеленым цветом будут выделены части нужные нам для работы DHCP сервера которые возьмем из этого образца и на основе которых будет создан dhcpd.conf файл пример которого будет приведен ниже дефолтового конфига:

# dhcpd.conf

#

# Sample configuration file for ISC dhcpd

#

# option definitions common to all supported networks...

**option domain-name "example.org";**

**option domain-name-servers ns1.example.org, ns2.example.org;**

**default-lease-time 600;**

**max-lease-time 7200;**

# Use this to enble / disable dynamic dns updates globally.

#ddns-update-style none;

# If this DHCP server is the official DHCP server for the local

# network, the authoritative directive should be uncommented.

#authoritative;

# Use this to send dhcp log messages to a different log file (you also

# have to hack syslog.conf to complete the redirection).

log-facility local7;

# No service will be given on this subnet, but declaring it helps the

# DHCP server to understand the network topology.

subnet 10.152.187.0 netmask 255.255.255.0 {

}

# This is a very basic subnet declaration.

subnet 10.254.239.0 netmask 255.255.255.224 {

range 10.254.239.10 10.254.239.20;

option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;

}

# This declaration allows BOOTP clients to get dynamic addresses,

# which we don't really recommend.

subnet 10.254.239.32 netmask 255.255.255.224 {

range dynamic-bootp 10.254.239.40 10.254.239.60;

option broadcast-address 10.254.239.31;

option routers rtr-239-32-1.example.org;

}

# A slightly different configuration for an internal subnet.

**subnet 10.5.5.0 netmask 255.255.255.224 {**

**range 10.5.5.26 10.5.5.30;**

**option domain-name-servers ns1.internal.example.org;**

**option domain-name "internal.example.org";**

**option routers 10.5.5.1;**

**option broadcast-address 10.5.5.31;**

default-lease-time 600;

max-lease-time 7200;

}

# Hosts which require special configuration options can be listed in

# host statements. If no address is specified, the address will be

# allocated dynamically (if possible), but the host-specific information

# will still come from the host declaration.

host passacaglia {

hardware ethernet 0:0:c0:5d:bd:95;

filename "vmunix.passacaglia";

server-name "toccata.fugue.com";

}

# Fixed IP addresses can also be specified for hosts. These addresses

# should not also be listed as being available for dynamic assignment.

# Hosts for which fixed IP addresses have been specified can boot using

# BOOTP or DHCP. Hosts for which no fixed address is specified can only

# be booted with DHCP, unless there is an address range on the subnet

# to which a BOOTP client is connected which has the dynamic-bootp flag

# set.

**host fantasia {**

**hardware ethernet 08:00:07:26:c0:a5;**

**fixed-address fantasia.fugue.com;**

**}**

# You can declare a class of clients and then do address allocation

# based on that. The example below shows a case where all clients

# in a certain class get addresses on the 10.17.224/24 subnet, and all

# other clients get addresses on the 10.0.29/24 subnet.

class "foo" {

match if substring (option vendor-class-identifier, 0, 4) = "SUNW";

}

shared-network 224-29 {

subnet 10.17.224.0 netmask 255.255.255.0 {

option routers rtr-224.example.org;

}

subnet 10.0.29.0 netmask 255.255.255.0 {

option routers rtr-29.example.org;

}

pool {

allow members of "foo";

range 10.17.224.10 10.17.224.250;

}

pool {

deny members of "foo";

range 10.0.29.10 10.0.29.230;

}

}

**2.3 Настройка dhcpd.conf**

Чтобы вам было понятнее привожу 100% рабочий конфигурационный файл dhcpd.conf, который устанавливает время аренды адреса на 28800 секунд, обслуживает зону 192.168.1.0/24, в качестве адреса роутера используется 192.168.1.254, в качестве адреса направленного широковещания 192.168.1.255, в качестве адреса сервера DNS 8.8.8.8

Так же стоит отметить, что данная конфигурация будет раздавать IP адреса всем подключающимся клиентам, без проверки их MAC адреса в диапазоне от 192.168.1.10-192.168.1.128.

authoritative;

ddns-update-style interim;

default-lease-time 28800;

max-lease-time 28800;

subnet 192.168.1.0 netmask 255.255.255.0 {

option routers 192.168.1.254; # default gateway

option subnet-mask 255.255.255.0;

option broadcast-address 192.168.1.255;

option domain-name-servers 8.8.8.8;

option domain-name "mydomain.ru";

pool {

range 192.168.1.10 192.168.1.128;

}

}

По вариантам:

|  |  |
| --- | --- |
| **Номер варианта** | **Сеть для dhcp** |
| 1 | 192.168.1.0/24 |
| 2 | 192.168.2.0/24 |
| 3 | 192.168.3.0/24 |
| 4 | 192.168.4.0/24 |
| 5 | 192.168.5.0/24 |
| 6 | 192.168.6.0/24 |
| 7 | 192.168.7.0/24 |
| 8 | 192.168.8.0/24 |
| 9 | 192.168.9.0/24 |
| 10 | 192.168.10.0/24 |
| 11 | 192.168.11.0/24 |
| 12 | 192.168.12.0/24 |
| 13 | 192.168.13.0/24 |
| 14 | 192.168.14.0/24 |
| 15 | 192.168.15.0/24 |
| 16 | 192.168.16.0/24 |
| 17 | 192.168.17.0/24 |
| 18 | 192.168.18.0/24 |
| 19 | 192.168.19.0/24 |
| 20 | 192.168.20.0/24 |
| 21 | 192.168.21.0/24 |
| 23 | 192.168.22.0/24 |
| 24 | 192.168.23.0/24 |
| 25 | 192.168.24.0/24 |
| 26 | 192.168.25.0/24 |
| 27 | 192.168.26.0/24 |

Разумеется пул выдачи адресов нужно настроить в соответствие с сетью по варинту.

**2.4 Отладка запуска и управление службой dhcp**

Сервис запускается командой **/etc/ini.d/dhcpd start**

Сервис останавливается командой **/etc/ini.d/dhcpd stop**

Проверяется статус сервиса командой **/etc/ini.d/dhcpd status**

Запустить сервис командой /etc/ini.d/dhcpd start , если он не запустится, проверить системный лог файл /etc/log/messages:

**tail –n 1000 /var/log/messages**

Если в выоде лога по старту службы dhcp будет информация о неправильных правах доступа к файлу dhcp.leases

Сообщение о ошибке будет примерно таким:

Nov 15 08:54:45 centos6 dhcpd: Internet Systems Consortium DHCP Server 4.1.1-P1

Nov 15 08:54:45 centos6 dhcpd: Copyright 2004-2010 Internet Systems Consortium.

Nov 15 08:54:45 centos6 dhcpd: All rights reserved.

Nov 15 08:54:45 centos6 dhcpd: For info, please visit https://www.isc.org/software/dhcp/

Nov 15 08:54:45 centos6 dhcpd: Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not specified in the config file

**Nov 15 08:54:45 centos6 dhcpd: Can't open /var/lib/dhcpd/dhcpd.leases for append.**

Nov 15 08:54:45 centos6 dhcpd:

Nov 15 08:54:45 centos6 dhcpd: This version of ISC DHCP is based on the release available

Nov 15 08:54:45 centos6 dhcpd: on ftp.isc.org. Features have been added and other changes

Nov 15 08:54:45 centos6 dhcpd: have been made to the base software release in order to make

Nov 15 08:54:45 centos6 dhcpd: it work better with this distribution.

Nov 15 08:54:45 centos6 dhcpd:

Nov 15 08:54:45 centos6 dhcpd: Please report for this software via the CentOS Bugs Database:

Nov 15 08:54:45 centos6 dhcpd: http://bugs.centos.org/

Nov 15 08:54:45 centos6 dhcpd:

Nov 15 08:54:45 centos6 dhcpd: exiting.

Данная ошибка возникает, если в системе работает служба защиты Selinux, ее надо отключить.

Для чего зайти в каталог /etc/selinux и в файле config:

# This file controls the state of SELinux on the system.

# SELINUX= can take one of these three values:

# enforcing - SELinux security policy is enforced.

# permissive - SELinux prints warnings instead of enforcing.

# disabled - No SELinux policy is loaded.

SELINUX= **enforcing**

# SELINUXTYPE= can take one of these two values:

# targeted - Targeted processes are protected,

# mls - Multi Level Security protection.

SELINUXTYPE=targeted

Исправить параметр enforcing на **disabled**, после чего перезагрузить Linux.

**2.5 Установка автозапуска службы dhcpd**

С помощью команды chkconfig –list проверить настройки службы автозапуска службы dhcpd. Она будет выключена по умолчанию на всех уровнях инициализации.

Включите ее на уровнях 2-3-5 по аналогии с первым заданием:

**chkconfig --level 235 dhcpd on**

Перезагрузить Linux и проверить, что служба запустилась автоматически.

Задание 3

Проверка получения IP адреса DHCP клиентом из пула адресов.

1. Развернуть в качестве клиента ОС Windows 2008 Server или любой дистрибутив Linux, выставить сетевой интерфейс в режим работы “внутренняя сеть”, запустить систему и проверить получение клиентом адреса из пула адресов dhcp сервера, указанного в файле dhcpd.conf.

Задание 4

Настройка получение определённого IP адреса ПК с помощью привязки его к аппаратному адресу сетевого интерфейса.

1. Открыть на редактирование файл /etc/dhcp/dhcpd.conf и добавить в конце файлы строки:

**host test-pk { hardware ethernet 08:00:07:26:c0:a5; fixed-address 192.168.1.129;}**

MAC адрес надо указать MAC клиента, а в качестве IP адреса любой адрес за диапазоном пула, в примере пул заканчивается адресом 192.168.1.128, поэтому укажем адрес 192.168.1.129.

1. После чего сохранить изменения и перезупстить службу dhcp.
2. Зайти на клиент и переполучить IP адрес, для этого:

* На Windows выполнить команды:

ipconfig /release

ipconfig /renew

* На Linux перезапустить сетевую службу командой:

/etc/init.d/network restart

Либо воспользоваться апплетом Network-Manager.

1. Проверить полученный результат. В windows командой ipconfig, в Linux командой ifconfig.
2. Вывод логов на dhcp сервере будет примерно таким:

Dec 3 12:01:44 centos6 dhcpd: **DHCPDISCOVER** from 08:00:27:86:ce:d6 via eth2

Dec 3 12:01:44 centos6 dhcpd: **DHCPOFFER** on 192.168.1.129 to 08:00:27:86:ce:d6 via eth2

Dec 3 12:01:44 centos6 dhcpd: uid lease 192.168.1.12 for client 08:00:27:86:ce:d6 is duplicate on 192.168.1.0/24

Dec 3 12:01:44 centos6 dhcpd: **DHCPREQUEST** for 192.168.1.129 (192.168.1.3) from 08:00:27:86:ce:d6 via eth2

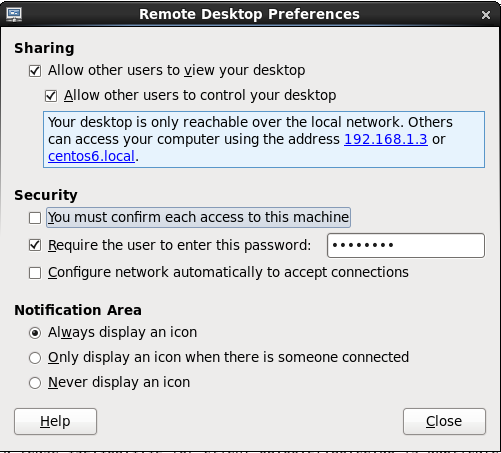
Dec 3 12:01:44 centos6 dhcpd: **DHCPACK** on 192.168.1.129 to 08:00:27:86:ce:d6 via eth2

Синим цветом выделены сообщения от dhcp сервера, красным от dhcp клиента.

Задание 5.

Удаленное управление Linux с помощью службы VNC

1. Запустить приложение Remote Desktop на DHCP сервере из меню System---Preferences или найти данное приложение в поиске.



В его настройках разрешаете удаленный доступ по протоколу VNC и собственно активируйте встроенный в графическую среду Gnome VNC сервер vino. Так же задаете пароль для доступа к VNC сессии.

1. Проверяете доступность удаленного рабочего стола DHCP сервера по протоколу VNC с помощью любого vnc клиента, в котором указываете для подключения IP адрес VNC сервера 192.168.1.3 (в примере). Сам сервер vino вам при его настройке выдает подсказку на какой адрес подключаться.

Если клиентская машина на основе windows, рекомендовано это сделать с помощью vnc клиента tight-vnc.

1. Вопросы к лабораторной работе

1) Чем протокол BOOTP отличается от протокола DHCP?

2) Для чего в современных сетях при настройке DHCP сервера выбирают режим работы совместимый с BOOTP?

3) Какой IP адрес имеет поле IP Address Destination в пакете типа DHCPDISCOVER.

4) Как можно защитить трафик VNC между клиентом и сервером?