

ПРОГРАММА.

МОДУЛЬ 1. ДОБАВЛЕНИЕ МАРШРУТИЗАТОРА

МОДУЛЬ 2. СЕРВИС DHCP

МОДУЛЬ 3. ДОСТУП В INTERNET ЧЕРЕЗ HTTP PROXY

МОДУЛЬ 4. СЕРВИС DNS - РАЗРЕШЕНИЕ ИМЕН

МОДУЛЬ 5. СЕРВИС ТОЧНОГО ВРЕМЕНИ

МОДУЛЬ 6. ФАЙЛОВЫЕ СЕРВИСЫ

МОДУЛЬ 7. СЕРВИС HTTP

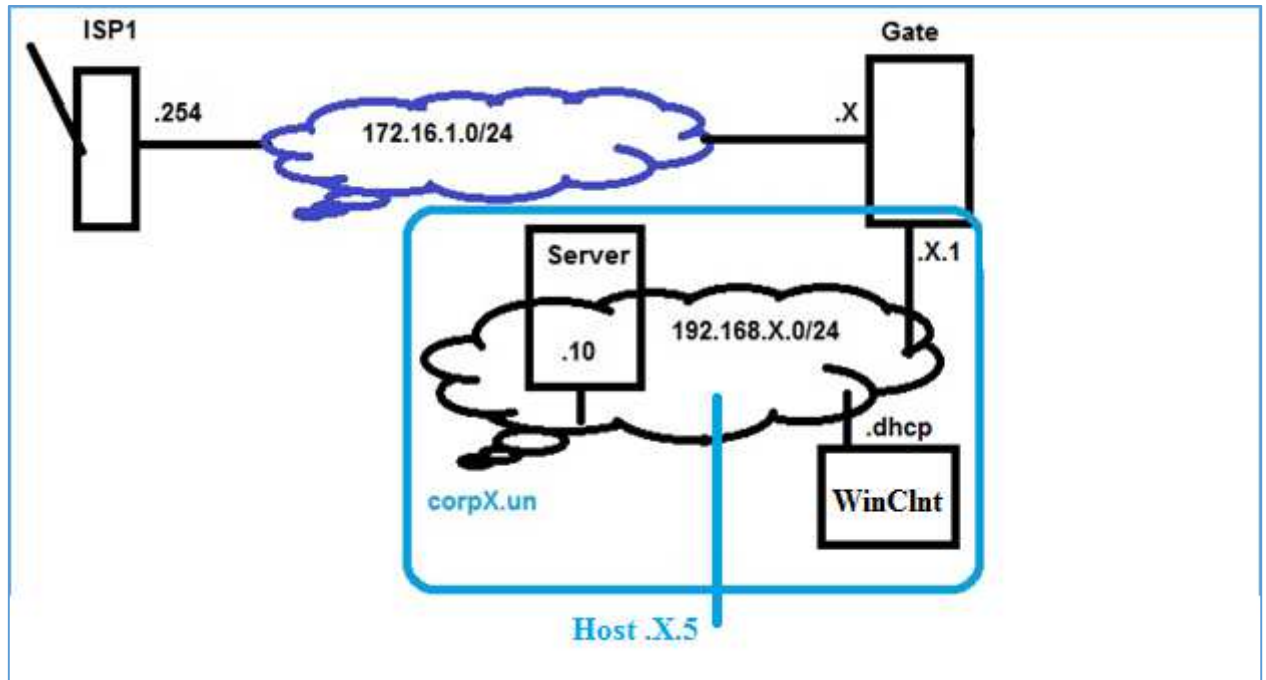
МОДУЛЬ 8. СЕРВЕР ЭЛЕКТРОННОЙ ПОЧТЫ

МОДУЛЬ 9. FIREWALL. ЗАЩИТА СЕТИ

МОДУЛЬ 10. МОНИТОРИНГ ДОСТУПА В ИНТЕРНЕТ ЧЕРЕЗ SQUID

МОДУЛЬ 1. ДОБАВЛЕНИЕ МАРШРУТИЗАТОРА

СХЕМА КЛАССА.



Добавим виртуальную машину Gate.

```
# cat /etc/hostname
```

```
# sed -i 's/X/номер_стенда/g' /etc/hosts
```

```
# sed -i 's/X/номер_стенда/g' /etc/network/interfaces
```

## Модуль 2. Сервис DHCP

### На виртуальной машине Gate:

```
apt-get install isc-dhcp-server  
vi /etc/default/isc-dhcp-server  
INTERFACES="enp0s3"  
vi /etc/dhcp/dhcpd.conf
```

### Настройка dhcp

```
vi /etc/dhcp/dhcpd.conf
```

### В файле dhcpd.conf прописать:

```
-----  
ddns-update-style none;  
log-facility local7;  
subnet 192.168.X.0 netmask 255.255.255.0 {  
    default-lease-time 600;  
    max-lease-time 7200;  
    range 192.168.X.101 192.168.X.199;  
    option routers 192.168.X.1;  
    option domain-name "corpX.un";  
    option domain-name-servers 192.168.X.1;  
  
}
```

### Проверка

```
root@gate:~# dhcpd -t  
root@gate:~# start isc-dhcp-server
```

### Посмотреть результат:

```
# tail -f /var/log/syslog  
# tail -f /var/lib/dhcp/dhcpd.leases
```

### Добавим виртуальную машину WinClient.

Настраиваем LAN-адаптер на автоматическое получение адреса.

Проверяем получение ip

### Модуль 3. Доступ в Internet через HTTP Proxy

#### Установка squid на Ubuntu Server 16.04.02

На виртуальной машине Gate:

```
# apt-get install squid3
```

```
# cd /etc/squid/
```

#### Настройка Squid

```
# vi /etc/squid/squid.conf
```

```
----- squid.conf-----
```

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

```
# Example rule allowing access from your local networks.
```

```
# Adapt localnet in the ACL section to list your (internal) IP networks
```

```
# from where browsing should be allowed
```

```
#http_access allow localnet
```

```
acl our_networks src 192.168.X.0/24
```

```
http_access allow our_networks
```

```
http_access allow localhost
```

```
-----
```

#### Проверка файла конфигурации

```
# squid -k parse
```

```
(squid -k check)
```

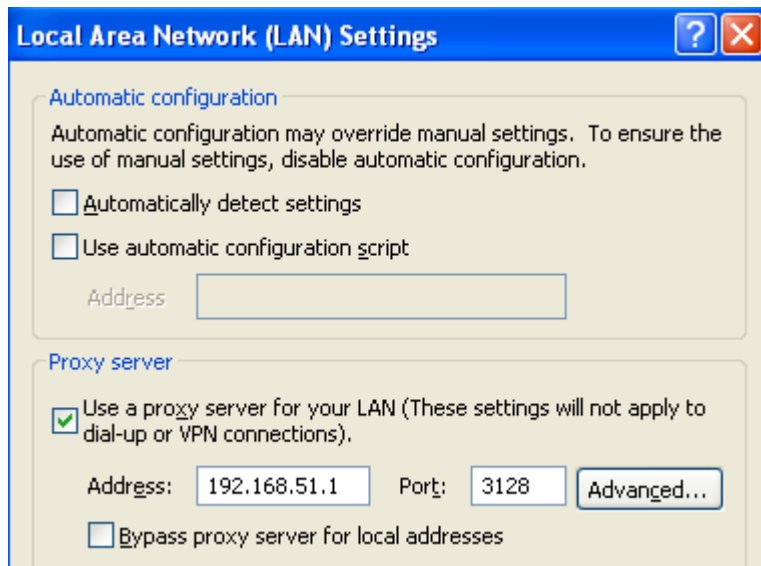
```
# systemctl restart squid
```

```
ps aux |grep squid
```

```
netstat -apnt |grep squid
```

#### Настройка IE в Windows:

3128 port for proxy



Подключимся к яндексу и проверим результат в логе:

```
root@gate:~# tail -f /var/log/squid/access.log
```

### Настройка маршрутизатора

#### Включаем маршрутизацию на Gate:

Убеждаемся, что `sysctl net.inet.ip.forwarding=0`.

Чтобы параметр сохранялся после перезагрузки задаем его в `/etc/sysctl.conf` как `net.ipv4.ip_forward=1`

Чтобы применить без перезагрузки, выполните

```
# sysctl -f
```

## МОДУЛЬ 4. СЕРВИС DNS - РАЗРЕШЕНИЕ ИМЕН

### Настройка рекурсивного, кэширующего DNS сервера

```
gate:~# apt-get install bind9
```

```
# nslookup -q=A www.yandex.ru 127.0.0.1
```

#### Настройка перенаправления.

```
# vi /etc/bind/named.conf.options
```

```
forwarders {  
    172.16.1.254;  
};
```

Проверка файла:

```
# named-checkconf -z
```

Перезапускаем:

```
# service bind9 restart
```

**Перенастроим параметры разрешения имен в /etc/network/interfaces сервера на самого себя:**

```
# dns-nameservers 127.0.0.1
```

### Настройка мастер сервера зоны corpX.un

Файлы мастер зоны лежат в /etc/bind/

Эти файлы подключаются (прописаны в) к центральному файлу конфигурации dns сервера:

```
# vi /etc/bind/named.conf.local
```

В него мы добавим описание нашей мастер-зоны:

```
zone "corpX.un" {
    type master;
    file "/etc/bind/corpX.un";
};
```

файл зоны создадим под именем corpX.un по указанному выше местоположению, в /etc/bind/

```
# vi /etc/bind/corpX.un
```

---

```
$TTL 3h
```

```
@ IN SOA gate. root.gate. (
    199609207 ; serial, todays date + todays serial #
    8H ; refresh, seconds
    2H ; retry, seconds
    4W ; expire, seconds
    1D ) ; min TTL , seconds
```

```
NS gate.
A 192.168.X.10
; MX 1 server
; MX 2 gate
gate IN A 192.168.X.1
server IN A 192.168.X.10
```

---

```
# named-checkconf -z
```

перезагружаем bind:

```
service bind9 restart
```

### Настройка вторичного сервера зоны dns:

```
nslookup -q=AXFR compX.un 172.16.1.254
```

```
gate:~# vim /etc/bind/named.conf.local
```

### В файле пропишем:

```
zone "compX.un" {  
    type slave;  
    file "/var/cache/bind/compX.un";  
    masters {  
        172.16.1.254;  
    };  
};
```

Перезагрузим зоны:

```
gate:~# rndc reload
```

Файл зоны должен появиться в:

```
ls -a /var/cache/bind/
```

### Зона обратного просмотра. PTR записи

Создадим зону обратного просмотра:

```
# vi /var/cache/bind/X.168.192.IN-ADDR.ARPA
```

```
$TTL 3h
```

```
@ SOA ns.corpX.un. root.server.corpX.un. 1 1d 12h 1w 3h
```

```
NS ns.corpX.un.
```

```
1 PTR gate.corpX.un.
```

```
10 PTR server.corpX.un.
```

```
# vi /etc/bind/named.conf.local
```

```
zone "X.168.192.IN-ADDR.ARPA" {  
    type master;
```

```
file "/var/cache/bind/X.168.192.IN-ADDR.ARPA";  
};  
# named-checkconf -z  
# rndc reload  
#####
```

### Настройка динамических обновлений DDNS.

**Прим.** Строки `algorithm hmac-md5`; и

`secret "Q3X9XjqKNpoa1Apnuwf+ng=="`;

взяты из файла `/etc/bind/rndc.key`

На стороне DNS сервера, в файле:

```
# vim /etc/bind/named.conf.local
```

```
-----  
//include "/etc/bind/zones.rfc1918";  
key DHCP_UPDATER {  
    algorithm hmac-md5;  
    secret "Q3X9XjqKNpoa1Apnuwf+ng=="  
};  
zone "corp51.un" {  
    type master;  
    file "/etc/bind/corp51.un";  
    allow-update {192.168.51.0/24;};  
    notify yes;  
};  
-----
```

Отредактировать приведенную ниже строку:

```
vim /etc/apparmor.d/usr.sbin.named
```

```
-----  
...  
# change this string /etc/bind/** r, to:  
/etc/bind/** rw,  
...  
-----
```

Выполнить:

```
# chmod 777 /etc/bind/
```

```
#####
```

На стороне DHCP сервера, в файле:

```
# vim /etc/dhcp/dhcpd.conf
```

```
-----  
ddns-update-style interim;  
ddns-updates on;  
update-static-leases on;  
ddns-domainname "corp51.un";  
key DHCP_UPDATER {  
    algorithm hmac-md5;  
    secret "Q3X9XjqKNpoa1Apnuwf+ng==";  
};  
zone corp51.un {  
    primary 192.168.51.1;  
}  
log-facility local7;  
subnet 192.168.51.0 netmask 255.255.255.0 {  
    default-lease-time 600;  
    max-lease-time 7200;  
    range 192.168.51.101 192.168.51.199;  
    option routers 192.168.51.1;  
    option domain-name "corp51.un";  
    option domain-name-servers 192.168.51.1;  
}  
-----
```

**# reboot**

```
# ls /etc/bind
```

Должен появиться файл:

```
corp51.un.jnl
```