

# Второе видео.

## Настройка DNS.

Необходимо установить host (**apt install host**)

Пропишем на всех машинах в папочке **resolv.conf** DNS адреса. На ISP И  
CLI адрес 3.3.3.1(это адрес ISP) а на остальных машинах  
192.168.103.200(это адрес SRV)(при переключении интерфейсов на NAT  
настройки в **resolv.conf** слетают и их надо прописать заного)

### DNS на SRV

☒ Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер:

Альтернативный DNS-сервер:

### DNS на WEB-L

```
GNU nano 5.4
domain int.demo.wsr
search int.demo.wsr
nameserver 192.168.103.200
```

### DNS на RTR-L

```
GNU nano 5.4
domain int.demo.wsr
search int.demo.wsr
nameserver 192.168.103.200
```

### DNS на ISP

```
GNU nano 5.4
domain demo.wsr
search demo.wsr
nameserver 3.3.3.1
```

### DNS на CLI

☐ Получить адрес DNS-сервера автоматически

☒ Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер:

Альтернативный DNS-сервер:

### DNS на RTR-R

```
GNU nano 5.4
domain int.demo.wsr
search int.demo.wsr
nameserver 4.4.4.100
```

### DNS на WEB-R

```
GNU nano 5.4
domain int.demo.wsr
search int.demo.wsr
nameserver 4.4.4.100
```

## Заходим на машину ISP

```
root@ISP:~# apt update
```

Далее устанавливаем пакеты bind9, dnsutils, bind9utils и chrony (пакет на синхрон времени). (важно после установки удалять добавленный интерфейс NAT0)

```
root@ISP:~# apt install bind9 dnsutils bind9utils chrony -y
```

Посмотри статус bind9

```
root@ISP:~# systemctl status named
```

```
• named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2022-05-04 07:08:34 EDT; 1min 2s ago
    Docs: man:named(8)
  Main PID: 1427 (named)
    Tasks: 8 (limit: 1132)
   Memory: 26.9M
      CPU: 77ms
  CGroup: /system.slice/named.service
          └─1427 /usr/sbin/named -f -u bind
```

Далее необходимо отредактировать файл

```
root@ISP:~# nano /etc/bind/named.conf.options
```

Первое это кому мы будем отвечать на вопросы, any означает всем.

```
listen-on { any; };
```

Второе означает что мы не будем никого опрашивать.

```
recursion no;
```

Следующие чьи вопросы мы будем разрешать. (все)

```
allow-query { any; };_
```

Следующий параметр будет проверять является ли данный DNS сервер разрешённым.

```
dnssec-validation no;
```

Последний параметр это будем ли мы отвечать на вопросы ipv6

```
listen-on-v6 { no; };
```

Так должно всё выглядеть

```
//=====
// If BIND logs error messages about the root key being
// you will need to update your keys. See https://www.
//=====
listen-on { any; };
recursion no;
allow-query { any; };
dnssec-validation no;

listen-on-v6 { no; };
```

Перейдём ко второму файлу который отвечает за зоны которые у нас будут описаны.

```
root@ISP:~# nano /etc/bind/named.conf.local
```

Указываем название зоны

```
zone "demo.wsr" {
```

затем указывает тип зоны master т.к. мы являемся хозяином этой зоны.

```
type master;
```

Будем сообщать об этой зоне DNS серверу указываем адрес (4.4.4.100).

```
allow-transfer { 4.4.4.100; };
```

Далее опишем файл где будет описана наша зона demo.wsr.

```
file "/opt/dns/demo.wsr.zone";  
};
```

Конечный вид файла.

```
//  
// Do any local configuration here  
//  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
zone "demo.wsr" {  
    type master;  
    allow-transfer { 4.4.4.100; };  
    file "/opt/dns/demo.wsr.zone";  
};
```

Далее создадим файл который мы ранее описали.

Создаём директорию где будет файл.

```
root@ISP:~# mkdir /opt/dns
```

Копируем шаблон файла чтобы не писать всё руками.

```
root@ISP:~# cp /etc/bind/db.local /opt/dns/demo.wsr.zone
```

Далее необходимо разрешить чтение этого файла системой.(665 даёт права на исполнение и на чтение.)

```
root@ISP:~# chmod 665 /opt/dns/demo.wsr.zone
```

Далее меняем параметры безопасности, нам необходимо добавить право на чтение файла для того что бы наши файлы могли читать приложения.

```
root@ISP:~# nano /etc/apparmor.d/usr.sbin.named
```

Нам необходимо добавить строчку которая будет разрешать чтение и запись во все файлы которые будут в этой директории.

```
/etc/bind/* r,  
/var/lib/bind/* rw,  
/var/lib/bind/ rw,  
/var/cache/bind/* lrw,  
/var/cache/bind/ rw,  
/opt/dns/* rw,
```

Перезапустим апармор.

```
root@ISP:~# service apparmor restart
```

Проверим статус апармора.

```

root@ISP:~# service apparmor status
• apparmor.service - Load AppArmor profiles
  Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; vendor preset: enabled)
  Active: active (exited) since Wed 2022-05-04 07:29:13 EDT; 9s ago
    Docs: man:apparmor(7)
           https://gitlab.com/apparmor/apparmor/wikis/home/
  Process: 1777 ExecStart=/lib/apparmor/apparmor.systemd reload (code=exited, status=0/SUCCESS)
 Main PID: 1777 (code=exited, status=0/SUCCESS)
   CPU: 112ms

```

Далее зайдём наш файл зон.

```

root@ISP:~# nano /opt/dns/demo.wsr.zone

```

Редактируем файл до такого вида.

```

GNU nano 5.4 /opt/dns/demo.wsr.zone
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      demo.wsr. root.demo.wsr. (
                        3      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       demo.wsr.
@         IN      A        3.3.3.1
isp       IN      A        3.3.3.1
www       IN      A        4.4.4.100
www       IN      A        5.5.5.100
internet  IN      CNAME    isp

```

Проверяем работоспособность.

```

root@ISP:~# systemctl status named
• named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2022-05-04 07:42:23 EDT; 1min 3s ago
    Docs: man:named(8)
  Process: 1858 ExecStart=/usr/sbin/named -u named -g named (code=exited, status=0/SUCCESS)
 Main PID: 1858 (code=exited, status=0/SUCCESS)
   CPU: 112ms

May 04 07:42:23 ISP named[1858]: all zones loaded
May 04 07:42:23 ISP named[1858]: running

```

```

root@ISP:~# host www.demo.wsr
www.demo.wsr has address 4.4.4.100
www.demo.wsr has address 5.5.5.100
root@ISP:~# host internet.demo.wsr
internet.demo.wsr is an alias for isp.demo.wsr.
isp.demo.wsr has address 3.3.3.1
root@ISP:~# host isp.demo.wsr
isp.demo.wsr has address 3.3.3.1

```

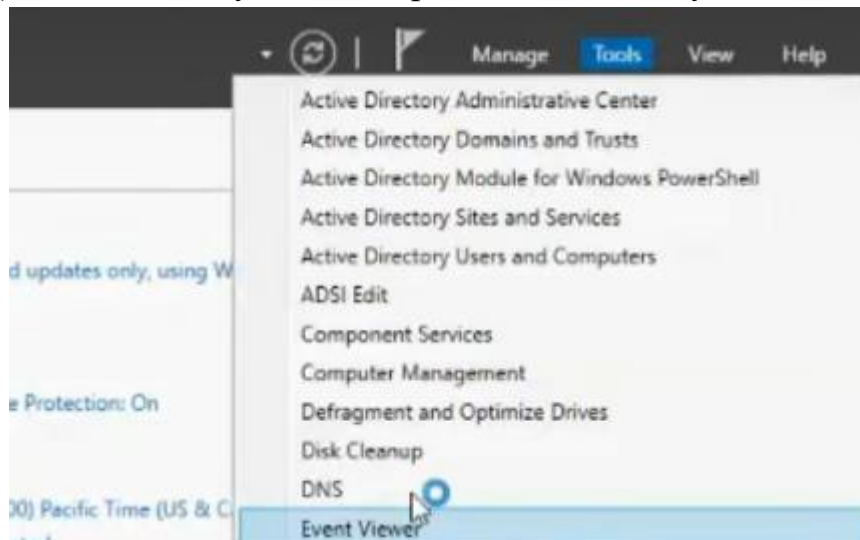
Теперь посмотрим работу со стороны клиента.

```
C:\Users\User>nslookup www.demo.wsr
ТхТхТх: UnKnown
Address: 3.3.3.1

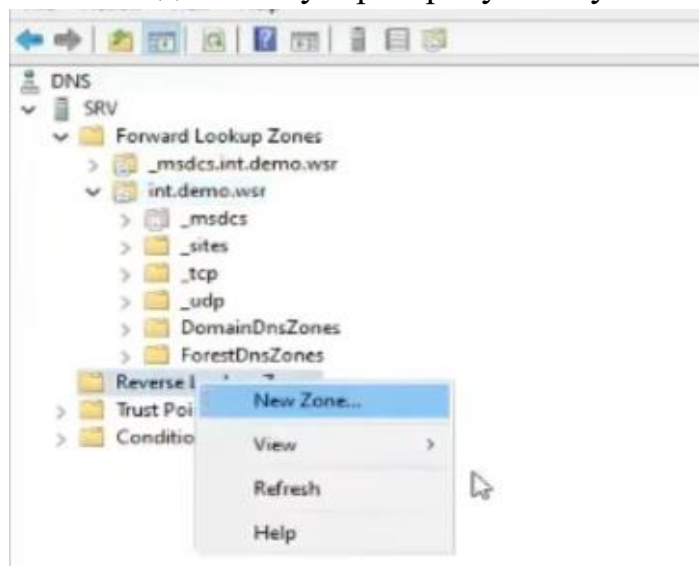
Лб : www.demo.wsr
Addresses: 5.5.5.100
          4.4.4.100
```

## Настройка DNS на SRV.

(Он сказал что у него настроен домен я хз нужен ли он )



Создаём новую реверсную зону.



Всё пропускаем и указываем зону.  
Нам необходимо создать две зоны.

1



New Zone Wizard

**Reverse Lookup Zone Name**  
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:  
[ 192 . 168 . 100 ] .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:  
[ 100.168.192.in-addr.arpa ]

< Back   **Next >**   Cancel

2



New Zone Wizard

**Reverse Lookup Zone Name**  
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:  
[ 172 . 16 . 100 ] .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

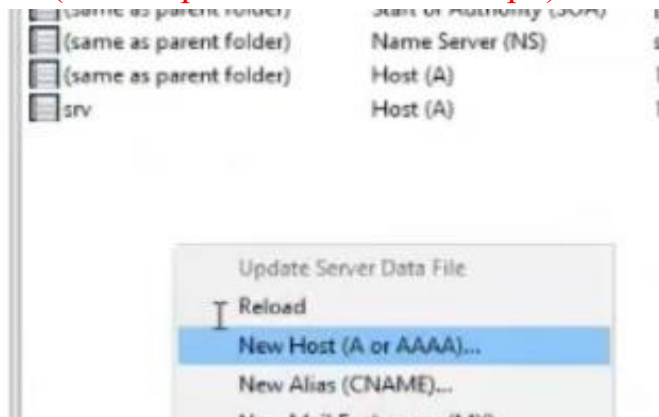
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:  
[ 100.16.172.in-addr.arpa ]

< Back   **Next >**   Cancel

Создадим запись WEB-L и WEB-R так же RTR-L и RTR-R.

(свои адреса 103 важно смотри)



WEV-L

The 'New Host' dialog box is shown with the following fields and options:

- Name (uses parent domain name if blank): web-l
- Fully qualified domain name (FQDN): web-l.int.demo.wsr.
- IP address: 192.168.100.100
- ☒ Create associated pointer (PTR) record
- ☐ Allow any authenticated user to update DNS records with the same owner name
- Buttons: Add Host, Cancel

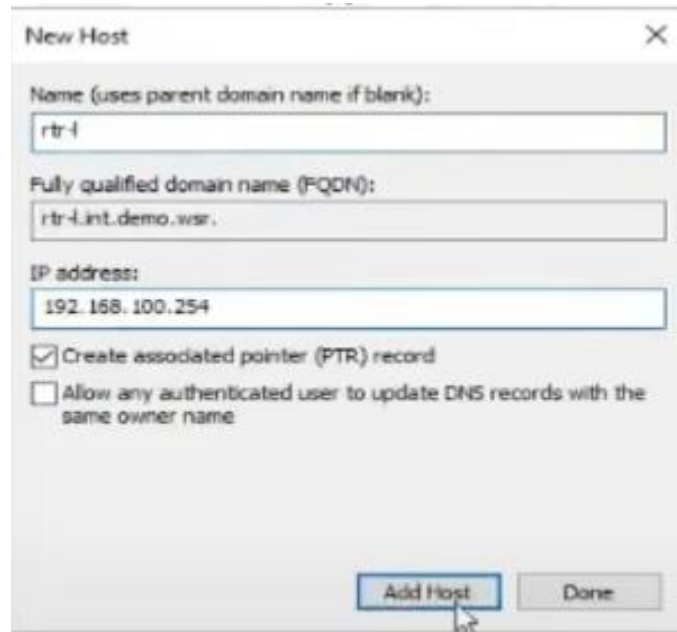
WEV-R

The 'New Host' dialog box is shown with the following fields and options:

- Name (uses parent domain name if blank): web-r
- Fully qualified domain name (FQDN): web-r.int.demo.wsr.
- IP address: 172.16.100.100
- ☒ Create associated pointer (PTR) record
- ☐ Allow any authenticated user to update DNS records with the same owner name
- Buttons: Add Host, Done



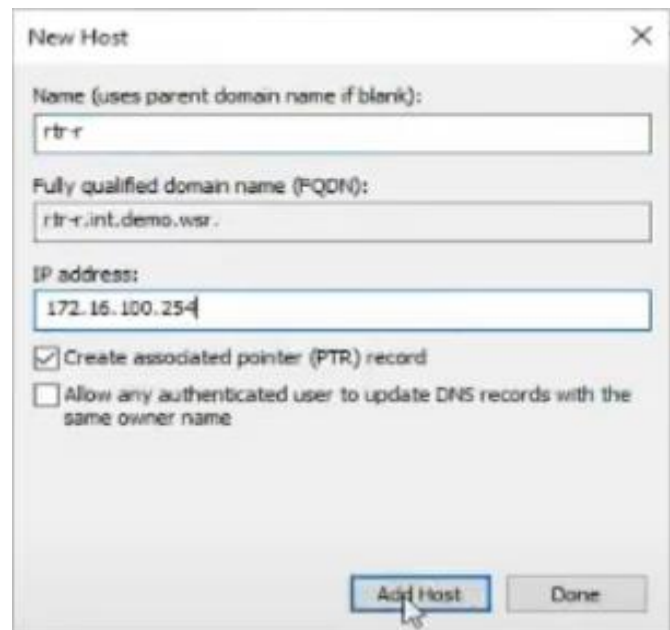
## RTR-L



The 'New Host' dialog box is shown with the following fields and options:

- Name (uses parent domain name if blank):
- Fully qualified domain name (FQDN):
- IP address:
- ☒ Create associated pointer (PTR) record
- ☐ Allow any authenticated user to update DNS records with the same owner name
- Buttons: **Add Host** (highlighted with a mouse cursor), Done

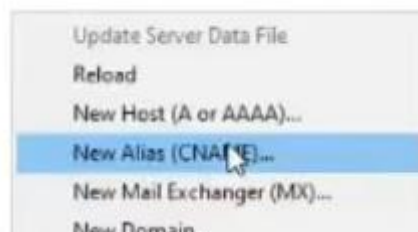
## RTR-R



The 'New Host' dialog box is shown with the following fields and options:

- Name (uses parent domain name if blank):
- Fully qualified domain name (FQDN):
- IP address:
- ☒ Create associated pointer (PTR) record
- ☐ Allow any authenticated user to update DNS records with the same owner name
- Buttons: **Add Host** (highlighted with a mouse cursor), Done

Далее создаём 2 CNAME.



The context menu contains the following options:

- Update Server Data File
- Reload
- New Host (A or AAAA)...
- New Alias (CNAME)...** (highlighted with a mouse cursor)
- New Mail Exchanger (MX)...
- New Domain...



NTP

Должен ссылать на SRV.

New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank):  
ntp

Fully qualified domain name (FQDN):  
ntp.int.demo.wsr

Fully qualified domain name (FQDN) for target host:  
 Browse...

Browse

Look in: DNS

Records:

Name	Type	Data	Timestamp
SRV			

Browse

Look in: SRV

Records:

Name	Type	Data	Timestamp
Forward Lo...			

Browse

Look in: Forward Lookup Zones

Records:

Name	Type	Data	Timestamp
_medcs.int...	Active Dir...	Running	Not Signed
int.demo.wsr	Active Dir...	Running	Not Signed

Browse

Look in: int.demo.wsr

Records:

Name	Type	Data	Timestamp
ForestDnsZ...			
(same as p...	Host (A)	192.168.10...	5/3/2022 ...
srv	Host (A)	192.168.10...	static
web-f	Host (A)	192.168.10...	
web-r	Host (A)	172.16.100...	
rtr-f	Host (A)	192.168.10...	
rtr-r	Host (A)	172.16.100...	

## DNS

Ссылается на SRV.

New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank):

dns

Fully qualified domain name (FQDN):

dns.int.demo.wsr

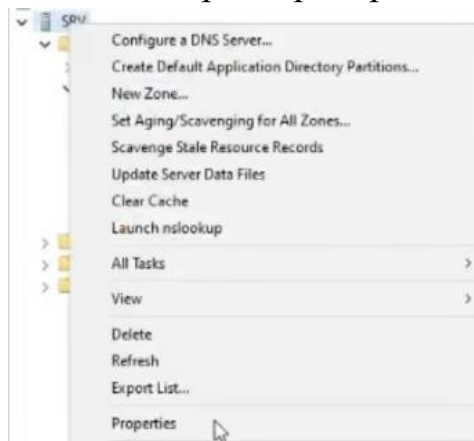
Fully qualified domain name (FQDN) for target host:

srv.int.demo.wsr [Browse...](#)

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel

Смотрим пропортис.

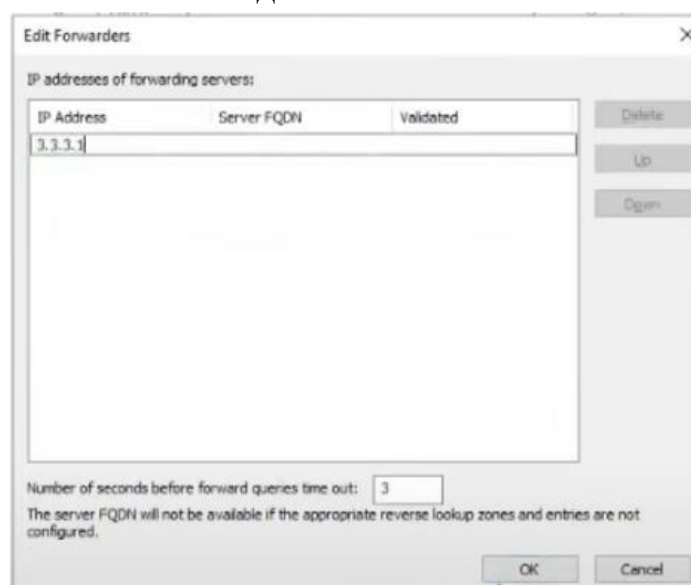


Там смотрим от кого мы будем получать другие зоны.

Записи которые там удаляем.



И создаём свою запись.

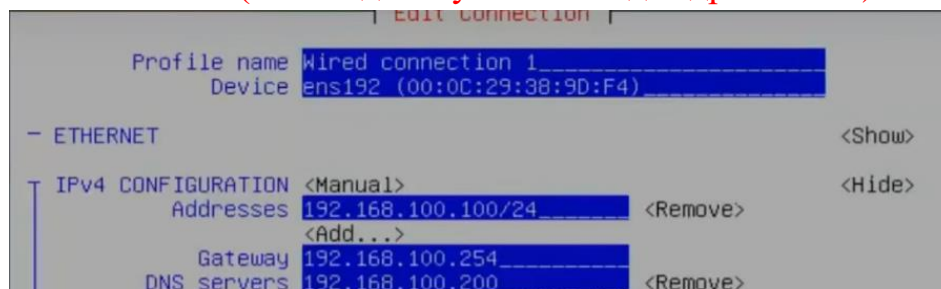


Зайдём на WEB-L и проверим работоспособность.

```
root@WEB-L:~# host www.demo.wsr
www.demo.wsr has address 4.4.4.100
www.demo.wsr has address 5.5.5.100
```

Это означает что всё разрешилось и работает.

Через NMTUI можно проверить какой у нас прописался dns serve. Должно быть так. **(необходимо указать везде адреса DNS)**

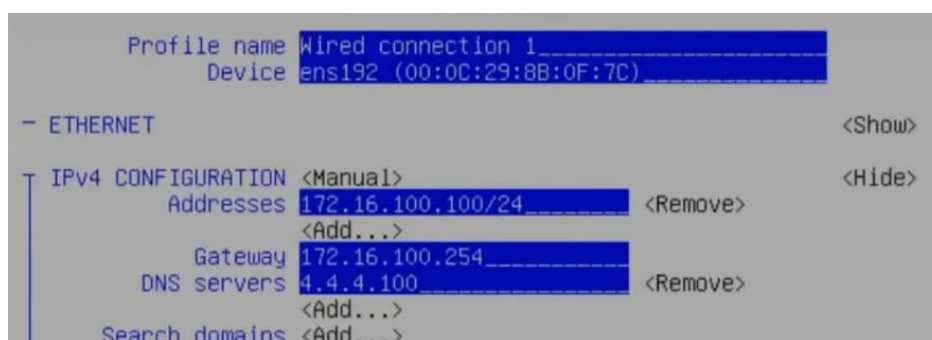


Далее проверим запустится ли SRV,WEB-R,WEB-L.

```
root@WEB-L:~# host srv.int.demo.wsr
srv.int.demo.wsr has address 192.168.100.200
root@WEB-L:~# host web-1.int.demo.wsr
web-1.int.demo.wsr has address 192.168.100.100
root@WEB-L:~# host web-r.int.demo.wsr
web-r.int.demo.wsr has address 172.16.100.100
```

Зайдём на WEB-R и проверим работоспособность.

Через NMTUI можно проверить какой у нас прописался dns serve. Должно быть так.



Далее проверим запустится ли RTR-R,WEB-L

```
root@WEB-R:~# host www.demo.wsr
www.demo.wsr has address 5.5.5.100
www.demo.wsr has address 4.4.4.100
root@WEB-R:~# host web-1.int.demo.wsr
web-1.int.demo.wsr has address 192.168.100.100
root@WEB-R:~# host rtr-r.int.demo.wsr
rtr-r.int.demo.wsr has address 172.16.100.254
```

DNS работает! МБ