

### Лабораторная работа 3. Службы DNS. Установка и настройка в ОС Windows.

#### Задание.

Используя виртуальные машины из предыдущих лабораторных работ настроить и протестировать работу служб DNS. Установить на Windows Server 2019 роль DNS-сервер. Создать на DNS-сервере зону прямого просмотра. В зоне прямого просмотра настроить несколько записей различного типа: начальную запись зоны (SOA), Сервер имен (NS), узел (A), псевдоним (CNAME). Создать зону обратного просмотра для текущей сети сервера с несколькими записями указателя (PTR). Проверить работу клиента DNS, протестировать механизм работы кэша DNS и срока жизни записи DNS (TTL).

#### Этапы выполнения.

- 1) Установить на Windows Server 2019 роль DNS-сервер.
- 2) Изменить настройки сетевого подключения, указать в качестве DNS-сервера loopback адрес - 127.0.0.1. (рис.1).

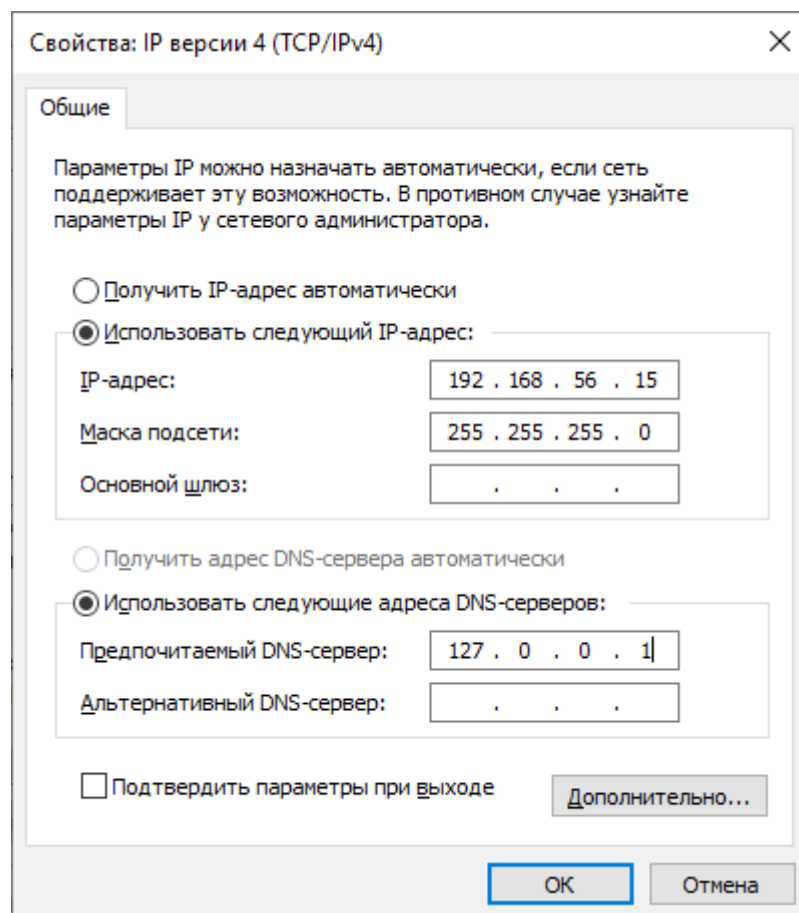


Рис.1. Настройка сетевого подключения.

- 3) Запустить Диспетчер DNS в Диспетчере серверов.

4) В Диспетчере DNS создать основную зону прямого просмотра с произвольным доменным именем (например, example.edu) (рисунки 2,3,4). Остальные параметры создания зона оставить в значениях по умолчанию.

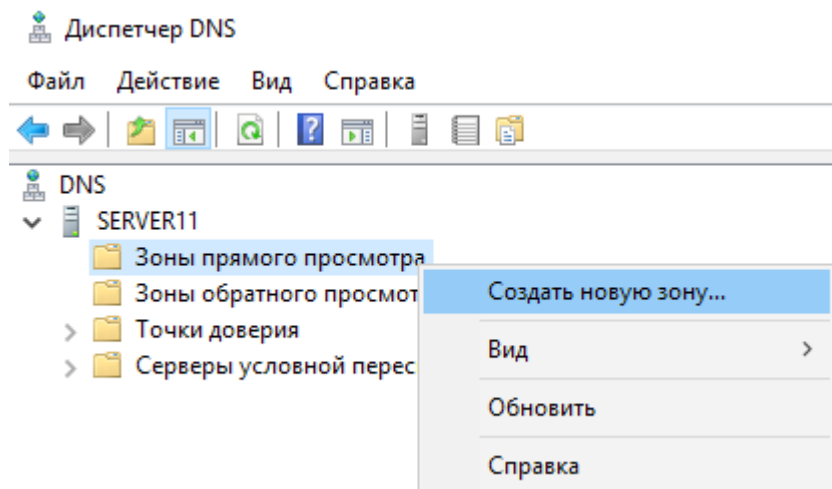


Рис.2. Создание новой зоны DNS.

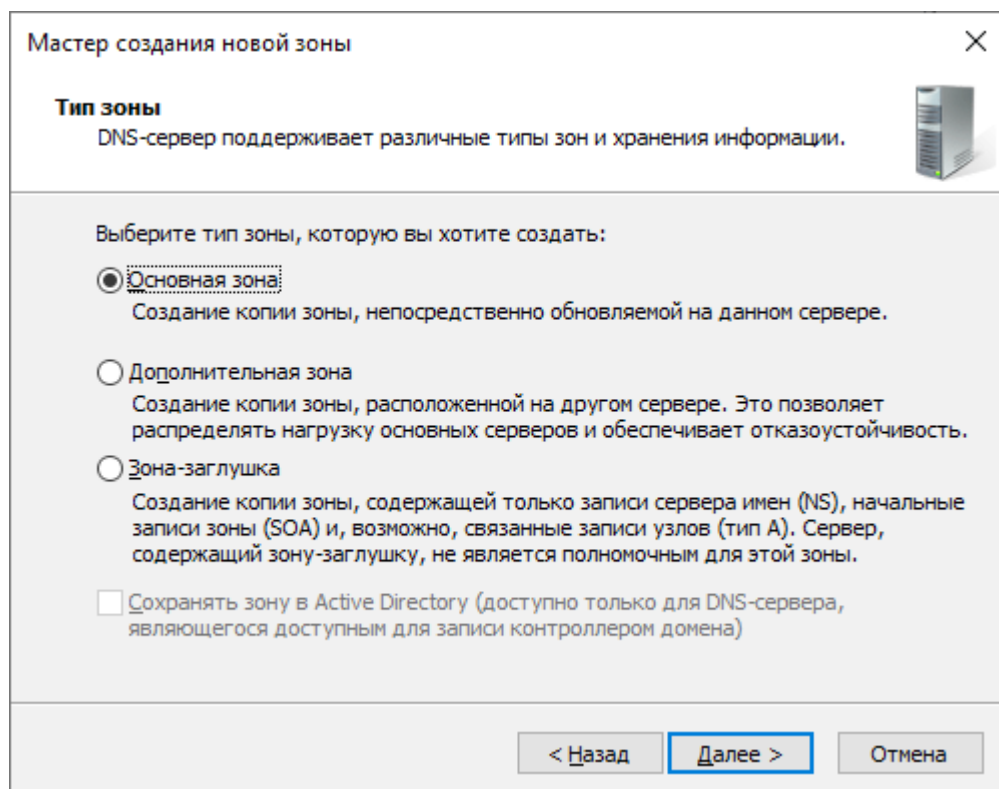


Рис.3. Выбор типа зоны.

Мастер создания новой зоны

**Имя зоны**  
Каково имя новой зоны?

Имя зоны указывает часть пространства имен DNS, для которой сервер является полномочным. Оно должно представлять доменное имя вашей организации (например, microsoft.com) или часть доменного имени (например, newzone.microsoft.com). Имя зоны не является именем DNS-сервера.

Имя зоны:  
example.edu

< Назад    Далее >    Отмена

Рис.4. Имя зоны (доменное имя).

5) В созданной зоне прямого просмотра создать запись типа А (узел), в которой указать имя и IP-адрес сервера Windows Server 2019 (рисунки 5, 6).

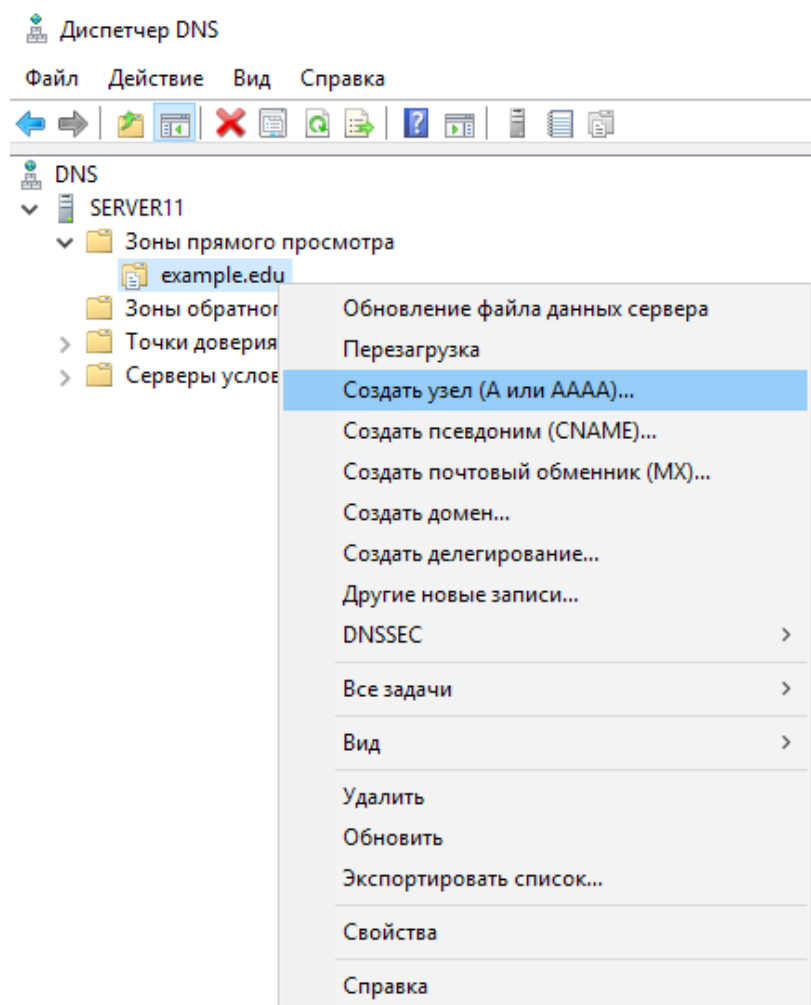


Рис.5. Создание записи.

Новый узел

Имя (если не указано, используется родительский домен):  
server11

Полное доменное имя (FQDN):  
server11.example.edu.

IP-адрес:  
192.168.56.15

☐ Создать соответствующую PTR-запись

Добавить узел    Отмена

Рис.6. Параметры записи узла.

6) Изменить «Начальную запись зоны (SOA)» (рис.7) - в качестве основного сервера указать полное доменное имя сервера (например, server01.example.edu).

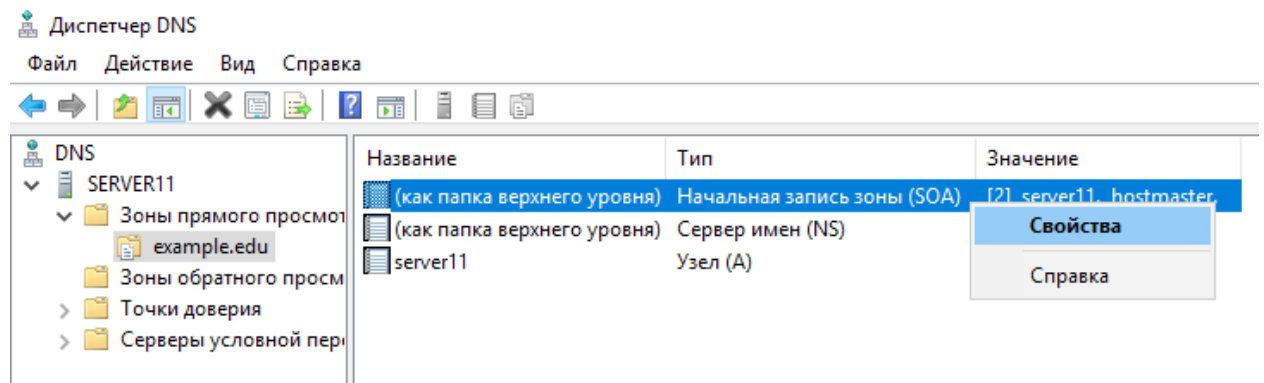


Рис.7. Изменение записи.

7) Изменить запись «Сервер имен (NS)» - изменить имя сервера на полное доменное имя.

8) Создать запись типа CNAME (Псевдоним) – указать псевдоним «test» для сервера, используя полное доменное имя из созданной записи типа A (узел) (например, server01.example.edu) (рис.8).

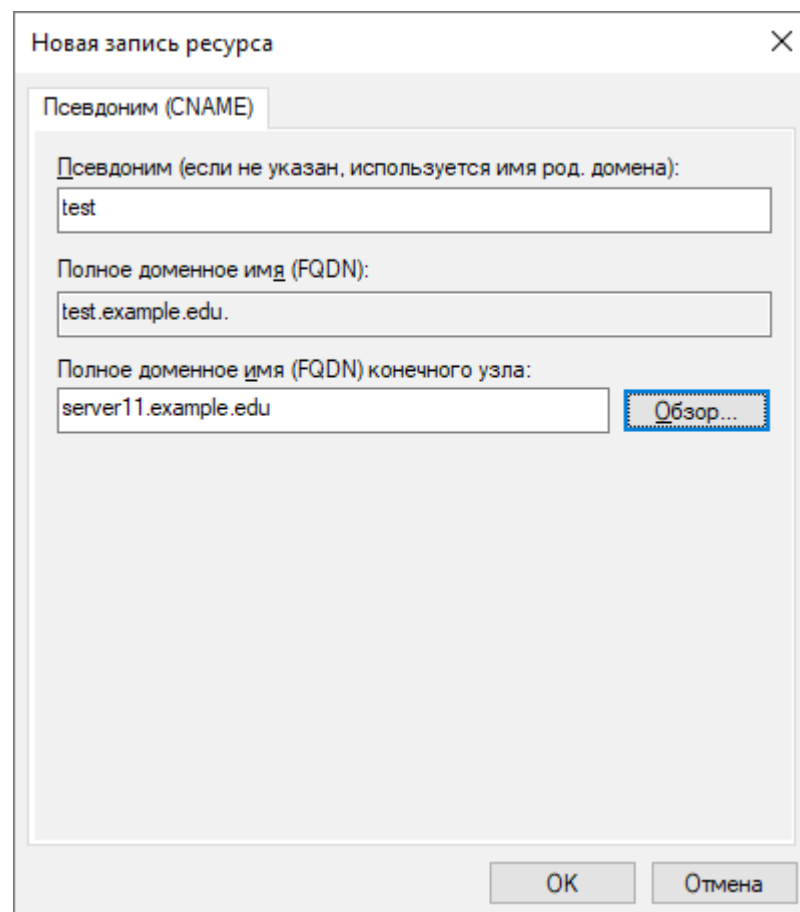


Рис.8. Создание псевдонима.

9) Создать основную зону обратного просмотра для IPv4 адресов в текущей сети сервера. Идентификатор сети указать в формате, изображенном на рис.9 (пример для сети 192.168.56.0/24). Остальные параметры оставить в значениях по умолчанию.

Мастер создания новой зоны

**Имя зоны обратного просмотра**  
Зона обратного просмотра преобразует IP-адреса в DNS-имена.

Можно задать зону обратного просмотра, указав идентификатор сети или имя этой зоны.

☒ Идентификатор сети:  
192 .168 .56| .

Идентификатор сети - это часть IP-адресов, которые принадлежат данной зоне. Введите идентификатор сети в обычном (не в обратном) порядке.

При явном использовании нуля в идентификаторе сети он появится в имени зоны. Например, идентификатор сети '10' будет соответствовать зоне '10.in-addr.arpa', а идентификатор сети '10.0' будет соответствовать зоне '0.10.in-addr.arpa'.

☐ Имя зоны обратного просмотра:  
56.168.192.in-addr.arpa

< Назад    Далее >    Отмена

Рис.9. Создание зоны обратного просмотра.

10) В зоне обратного просмотра создать PTR запись (указатель) для текущего сервера (имя узла указать в формате FQDN) (рисунки 10,11).

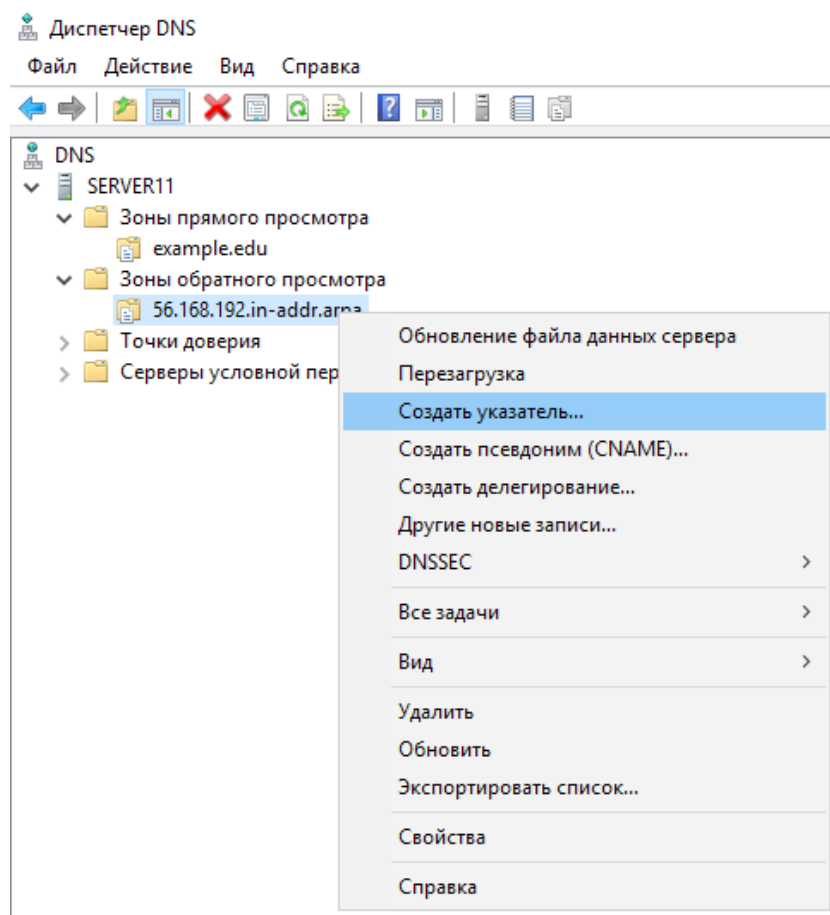


Рис.10. Создание записи в зоне обратного просмотра.

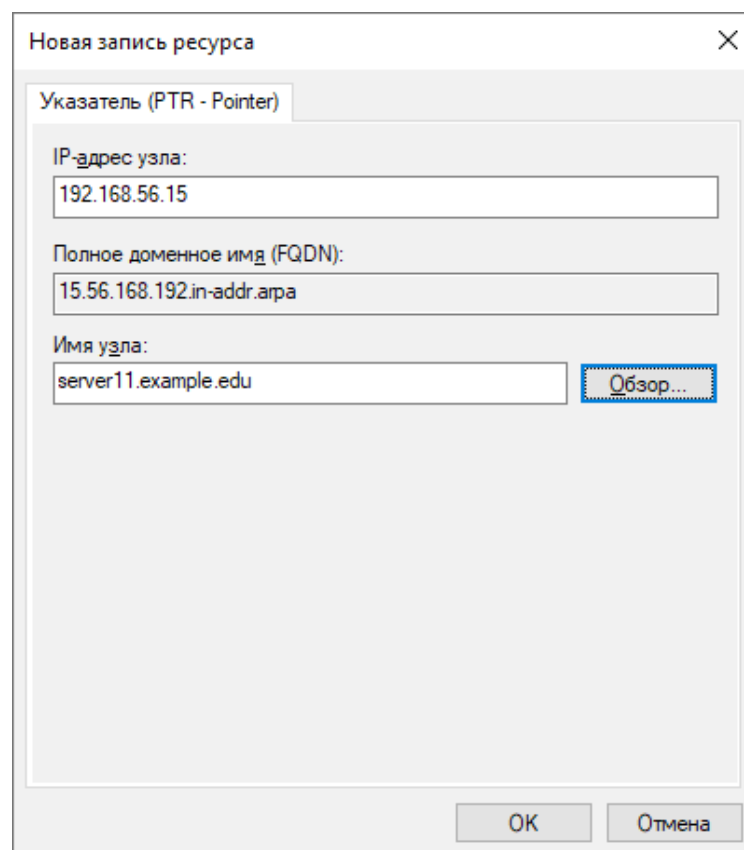


Рис.11. Создание указателя (PTR).

11) В зоне прямого просмотра создать еще одну запись типа A (узел), в которой указать имя «host» и IP-адрес системы-хоста – по умолчанию 192.168.56.1. При создании отметить параметр «Создать соответствующую PTR-запись».

12) На Windows 10 проверить настройки DNS – адрес DNS сервера и DNS суффикс должны быть получены по протоколу DHCP или настроены вручную.

13) На Windows 10 проверить работу клиента DNS. С помощью утилиты nslookup в командной строке узнать IP-адрес сервера Windows Server 2019 по основному имени (A) и имени псевдонима (CNAME). Примеры команд:

```
nslookup server01
```

если не настроен DNS суффикс, указать полное имя (FQDN):

```
nslookup server01.example.edu
```

узнать IP-адрес по псевдониму:

```
nslookup test
```

Узнать имя узла по IP-адресу:

```
nslookup 192.168.56.1
```

Альтернатива разрешения имени узла по IP-адресу:

```
ping -a 192.168.56.1
```

Просмотр информации о начальной записи зоны DNS (SOA):

```
nslookup -type=SOA example.edu
```

Снимки результатов выполнения nslookup – в отчет.

14) В зоне прямого просмотра DNS создать еще одну запись типа A (узел), указать произвольное имя узла (например, testportal) и произвольный незанятый IP-адрес (например, 10.1.2.3).

Снимок Диспетчера DNS с записями в зоне прямого просмотра и снимок с записями в зоне обратного просмотра – в отчет.

15) На Windows 10 проверить механизм работы кэша DNS и срока жизни записи DNS (TTL):

- выполнить ping до созданного узла, чтобы DNS имя узла и IP-адрес попали в кэш клиента DNS:

```
ping testportal
```

- проверить кэш клиента DNS и убедиться, что узел добавлен в кэш:



```
ipconfig /displaydns
```

Снимок результата выполнения команды – в отчет.

На сервере DNS:

- в Диспетчере DNS изменить запись для узла (testportal) – сменить IP-адрес (например, на 10.1.2.4).

На Windows 10:

- выполнить ping до тестового узла и убедиться в том, что IP-адрес берется из кэша клиента DNS (например, 10.1.2.3):

```
ping testportal
```

- не дожидаясь окончания срока жизни (TTL) записи (по умолчанию – 1 час), выполнить команду очистки кэша:

```
ipconfig /flushdns
```

- выполнить ping до созданного узла (testportal), убедиться в том, что подставляется актуальный IP-адрес (например, 10.1.2.4):

```
ping testportal
```

- повторно проверить кэш DNS:

```
ipconfig /displaydns
```

Снимок результата повторной проверки – в отчет.

**Отчет:**

- снимки результатов работы утилиты nslookup на этапе 13.
- снимок Диспетчера DNS с записями в зоне прямого просмотра;
- снимок Диспетчера DNS с записями в зоне обратного просмотра;
- снимки результатов выполнения команд на этапе 15.