МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное автономное образовательное учреждение высшего образования

«Санкт–Петербургский государственный университет  
аэрокосмического приборостроения»

ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ОТЧЕТ

ЗАЩИЩЕН С ОЦЕНКОЙ

РУКОВОДИТЕЛЬ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| преподаватель |  |  |  | И. В. Козлов |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ ПО ЛАБОРАТОРНЫМ РАБОТАМ  по дисциплине МДК 02.01. Администрирование сетевых операционных систем |
|  |
|  |
|  |
|  |

РАБОТУ ВЫПОЛНИЛИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТЫ ГР. № | С342 |  |  |  | Б. И. Глаголевский,  Е. Ю. Барабаш |
|  |  |  | подпись, дата |  | инициалы, фамилия |

**ОГЛАВЛЕНИЕ**

[Практическая работа №1: Реализация DHCP 3](#_Toc199288854)

[Практическая работа №2: Создание и настройка области DHCP 7](#_Toc199288855)

[Практическая работа №3: Устранение неполадок DNS 13](#_Toc199288856)

[Практическая работа №4: Установка роли DNS-сервера 16](#_Toc199288857)

[Практическая работа №5. Создание AD-интегрированной зоны. 18](#_Toc199288858)

[Лабораторная работа 6.1: Реализация DHCP 23](#_Toc199288859)

[Лабораторная работа №6.2: Реализация DNS 30](#_Toc199288860)

# Практическая работа №1: Реализация DHCP

Для настройки DHCP-сервера на SVR1 выполним следующую последовательность действий. Первоначально требуется авторизоваться в системе под учетной записью с правами администратора, что обеспечит необходимый уровень привилегий для установки и настройки серверных ролей.

После успешного входа следует запустить "Диспетчер серверов" - стандартный инструмент управления ролями и функциями Windows Server. В основном меню диспетчера необходимо выбрать раздел "Управление", а затем пункт "Добавить роли и компоненты", который запускает соответствующий мастер установки.

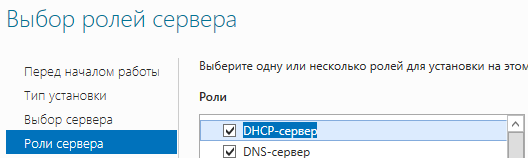


Рисунок 1 – Выбор ролей сервера.

В открывшемся мастере установки ролей и компонентов нужно последовательно пройти все этапы, уделяя особое внимание разделу выбора серверных ролей. В списке доступных ролей необходимо найти и отметить пункт "DHCP-сервер". При выборе данной роли система автоматически предложит установить дополнительные компоненты управления, включая консоль администрирования DHCP и инструменты командной строки, которые рекомендуется включить для полноценного управления службой.

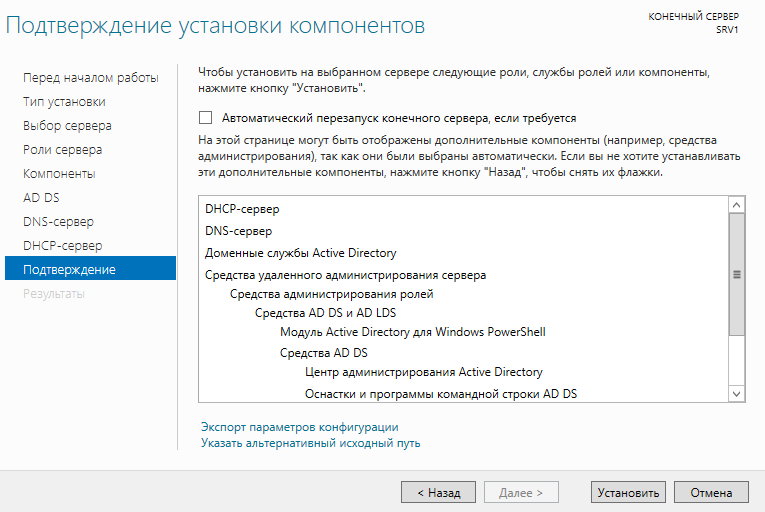


Рисунок 2 – Подтверждение установки компонентов.

После подтверждения выбора DHCP-сервера мастер отобразит краткое описание службы и ее функциональных возможностей. На следующем этапе будет показан список устанавливаемых компонентов, где следует проверить наличие всех необходимых элементов. Система автоматически проведет проверку зависимостей и предварительных требований перед началом установки.

Процесс установки DHCP-сервера может занять несколько минут в зависимости от производительности системы. По завершении установки мастер выведет уведомление об успешном выполнении операции, после чего можно будет приступать к последующей настройке службы DHCP через соответствующую оснастку в "Диспетчере серверов".

Для применения всех изменений может потребоваться перезагрузка сервера, хотя в большинстве случаев это не обязательно. После установки роли DHCP-сервер будет готов к детальной конфигурации, включая создание областей, настройку параметров аренды адресов и определение дополнительных опций.

На сервере SRV2 выполняется аналогичная процедура установки роли DHCP-сервера. Авторизация производится под учетной записью администратора домена или локальной административной учетной записью с соответствующими правами.

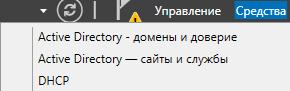


Рисунок 3 – DHCP.

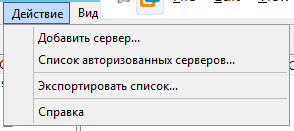


Рисунок 4 – Авторизовать сервер.

После установки роли DHCP-сервера на SRV2 необходимо выполнить процедуру авторизации сервера в Active Directory. Для этого в оснастке DHCP следует выполнить следующие действия.

Открываем оснастку DHCP через меню "Администрирование" или из "Диспетчера серверов". В левой части интерфейса выбираем узел с именем текущего сервера (SRV2). В верхнем меню оснастки переходим во вкладку "Действие", где выбираем пункт "Список авторизированных серверов".

В открывшемся диалоговом окне отобразится перечень уже авторизованных в домене DHCP-серверов. Для добавления нового сервера нажимаем кнопку "Авторизовать". В появившемся поле вводим IP-адрес или полное доменное имя сервера SRV2, затем подтверждаем выбор.

Система выполнит проверку доступности сервера и его соответствия требованиям домена. После успешной авторизации сервер SRV2 появится в общем списке разрешенных DHCP-серверов. Это гарантирует, что служба DHCP будет работать корректно и не вызовет конфликтов в доменной среде.

Авторизация DHCP-сервера в Active Directory является важным этапом настройки, так как предотвращает появление несанкционированных DHCP-серверов в сети. Только авторизованные серверы могут обслуживать клиентов в домене, что обеспечивает безопасность и стабильность сетевой инфраструктуры.

После завершения процедуры можно приступать к созданию областей (scopes) и настройке параметров DHCP для обслуживания клиентских устройств. Рекомендуется проверить статус сервера в оснастке DHCP, где он должен отображаться с зеленой иконкой, свидетельствующей о нормальной работе службы.

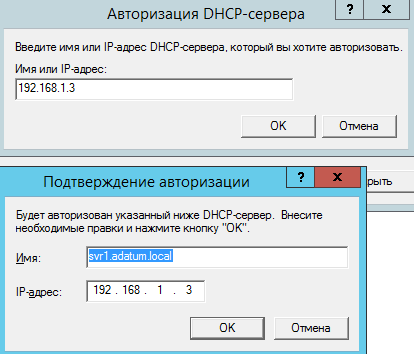


Рисунок 5 – Авторизация сервера.

После ввода IP-адреса или доменного имени сервера SRV2 в соответствующее поле диалогового окна и нажатия кнопки подтверждения система начинает процесс авторизации DHCP-сервера в доменной среде. Этот процесс включает автоматическую проверку доступности сервера, прав учетной записи и отсутствия конфликтов с существующей инфраструктурой.

При успешном прохождении всех проверок сервер SRV2 добавляется в централизованный список авторизованных DHCP-серверов домена. В оснастке DHCP это отражается изменением статуса сервера с "Не авторизован" на активное состояние, что визуально подтверждается специальным значком.

Авторизация обеспечивает серверу полномочия для создания и управления областями адресов, обработки клиентских запросов и участия в распределенном обслуживании сети. Для проверки результата следует обновить представление данных в оснастке, проверить журнал системных событий на предмет возможных ошибок и убедиться в работоспособности соответствующей службы.

После успешного завершения процедуры можно приступать к настройке конкретных параметров DHCP. Важно учитывать возможную задержку распространения изменений по домену из-за особенностей репликации Active Directory. Рекомендуется выждать некоторое время перед проверкой доступности новых настроек на других контроллерах домена

.

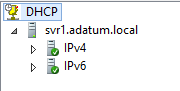


Рисунок 6 – Зеленые галочки.

После авторизации DHCP-сервера в Active Directory в оснастке DHCP должны отображаться зеленые индикаторы статуса для IPv4 и IPv6. Эти индикаторы свидетельствуют о корректной работе соответствующих протоколов и успешной интеграции сервера в доменную инфраструктуру.

Появление зеленых индикаторов подтверждает несколько важных аспектов. Во-первых, сервер успешно прошел процедуру авторизации в Active Directory. Во-вторых, служба DHCP активна и готова к обработке клиентских запросов. В-третьих, отсутствуют конфликты с другими серверами в сети.

# Практическая работа №2: Создание и настройка области DHCP

1. Настройка области DHCP в графическом интерфейсе (LON-SVR1)

Нажимаем правой кнопкой на IPv4 и выбираем «Создать область»

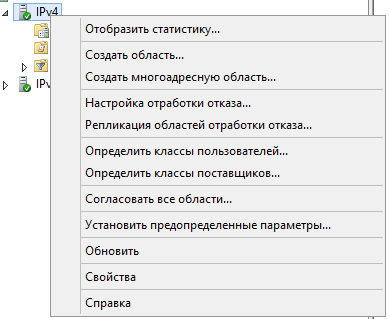


Рисунок 7 – Создание области.

Для настройки области DHCP на сервере LON-SVR1 через графический интерфейс необходимо выполнить следующие действия. В оснастке DHCP следует развернуть дерево конфигурации, найти и выделить узел IPv4. После этого нужно вызвать контекстное меню правой кнопкой мыши и выбрать пункт "Создать область".

Это действие запустит мастер создания новой области, который проведет через процесс пошаговой настройки. В первом окне мастера потребуется ввести имя и описание создаваемой области, которые помогут идентифицировать ее в дальнейшем. На следующем этапе необходимо указать диапазон IP-адресов, включая начальный и конечный адрес, а также определить маску подсети.

В мастере создания области вводим имя «Branch Office», Диапазон IP 172.16.0.100 – 172.16.0.200, Маска подсети 255.255.0.0, Исключения 172.16.0.190 – 172.16.0.200

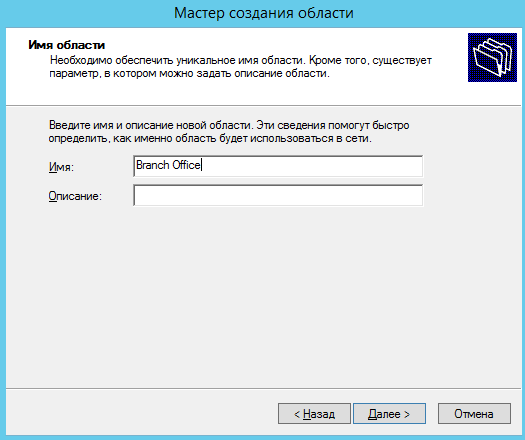


Рисунок 8 – Имя области.

На данном шаге, в качестве имени области, следует использовать «Branch Office».

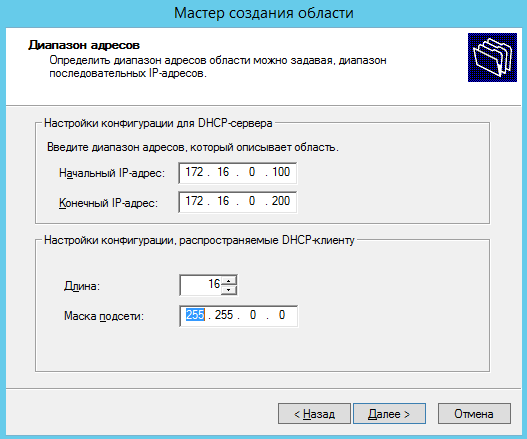


Рисунок 9 – Диапазон адресов.

На данном шаге, в качестве диапазона адресов необходимо указать 172.16.0.100 – 172.16.0.200.

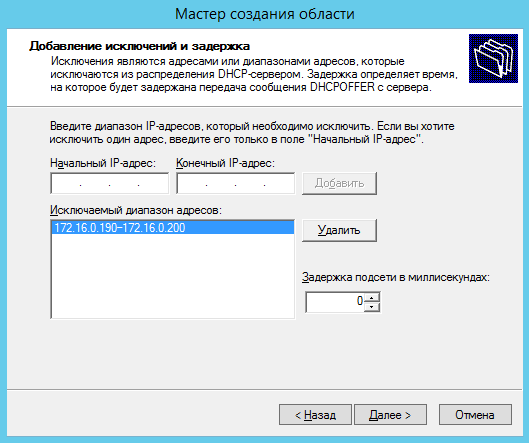


Рисунок 10 – Добавление и исключение адресов.

На данном шаге определяются адреса, которые будут исключены из DHCP-пула. В данном случае, под исключения попадают адреса 172.16.0.190 – 172.16.0.200.

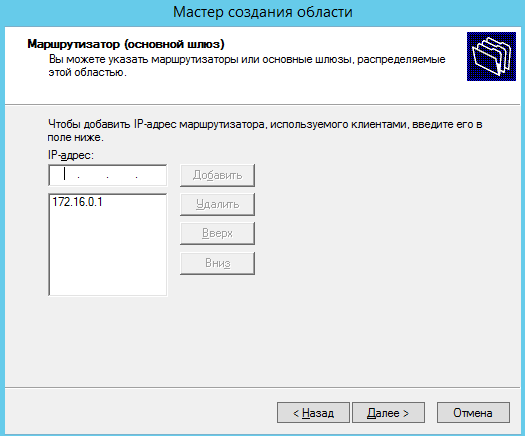


Рисунок 11 – Основной шлюз.

На данном шаге необходимо указать адрес, который будет выполнять роль шлюза по умолчанию.

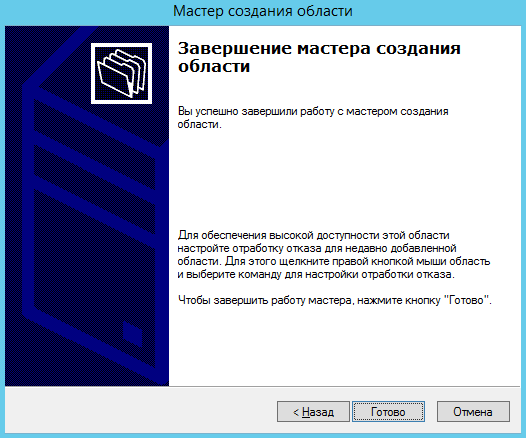


Рисунок 12 – Завершение мастера создания области.

На данном шаге можно наблюдать успешное завершение работы с мастером создания области.

2. Настройка области DHCP в PowerShell (LON-SVR2)



Рисунок 13 – Powershell.

На сервере SVR2 необходимо выполнить следующие действия для создания новой области DHCP с использованием PowerShell. Открываем консоль PowerShell с правами администратора, что обеспечит необходимый уровень доступа для изменения конфигурации DHCP-сервера.

В командной строке PowerShell вводим команду создания области, указав все требуемые параметры. Основные параметры включают имя области, которое служит для ее идентификации в оснастке DHCP, диапазон распределяемых адресов и маску подсети. Команда должна быть введена полностью в одной строке, без разрывов.

После выполнения команды система создаст новую область с указанными характеристиками. Для проверки результата можно использовать команду Get-DhcpServerv4Scope, которая выведет список всех областей на сервере, включая только что созданную. В выводе должны присутствовать указанные параметры: имя области, диапазон адресов и маска подсети.

Важно убедиться, что указанный диапазон адресов не пересекается с существующими областями и статическими назначениями в сети. Также следует проверить, что маска подсети соответствует реальной сетевой конфигурации. После завершения настройки можно протестировать работу новой области, подключив клиентское устройство и проверив получение адреса из заданного диапазона.

Для обеспечения отказоустойчивости рекомендуется аналогичным образом настроить область на втором DHCP-сервере, если в сети используется распределенная DHCP-инфраструктура. Это позволит клиентам продолжать получать адреса при недоступности одного из серверов.



Рисунок 14 – Powershell.

Для исключения диапазона адресов в области DHCP на сервере SVR2 используется команда Add-DhcpServerv4ExclusionRange. В данном случае необходимо указать идентификатор области ScopeID, соответствующий подсети 10.10.0.0, а также начальный и конечный адреса исключаемого диапазона. Полная команда выглядит следующим образом: Add-DhcpServerv4ExclusionRange -ScopeId 10.10.0.0 -StartRange 10.10.0.190 -EndRange 10.10.0.200.

После выполнения команды рекомендуется проверить результат с помощью Get-DhcpServerv4ExclusionRange, указав тот же ScopeId. Это позволит убедиться, что указанный диапазон адресов действительно исключен из автоматического распределения.

Исключение адресов используется для резервирования определенных IP-адресов под устройства, которым требуется статическая адресация, такие как серверы, сетевые принтеры или другое оборудование. Важно убедиться, что исключаемый диапазон не пересекается с уже зарезервированными или статически назначенными адресами в сети.



Рисунок 15 – Powershell.

Для настройки параметров DHCP на сервере SVR2 выполняем следующие команды в PowerShell с правами администратора. Первая команда устанавливает основной шлюз для клиентов DHCP. В данном случае шлюзом назначается адрес 10.10.0.1. Команда выглядит следующим образом: Set-DhcpServerv4OptionValue -Router 10.10.0.1.

Вторая команда активирует область DHCP с идентификатором 10.10.0.0, если она была ранее создана, но находилась в неактивном состоянии. Команда для активации области: Set-DhcpServerv4Scope -ScopeID 10.10.0.0 -State Active.

После выполнения этих команд клиенты, получающие адреса из данной области DHCP, будут автоматически настраивать указанный шлюз по умолчанию в своих сетевых параметрах. Активация области необходима для того, чтобы сервер начал обслуживать запросы клиентов на получение адресов из этого диапазона.

Для проверки результатов выполненных изменений можно использовать команду Get-DhcpServerv4OptionValue, которая покажет текущие установленные параметры DHCP, включая адрес маршрутизатора. Состояние области можно проверить командой Get-DhcpServerv4Scope, где в выводе будет указано, что область активна.

Важно убедиться, что указанный адрес шлюза действительно соответствует реальному сетевому оборудованию в данной подсети. Также рекомендуется проверить связность между клиентскими устройствами и указанным шлюзом после применения новых параметров DHCP.

Эти настройки являются базовыми для работы DHCP-сервера. В дальнейшем при необходимости можно добавить другие параметры, такие как адреса DNS-серверов, доменное имя или другие опции, используя аналогичные команды Set-DhcpServerv4OptionValue с соответствующими параметрами.

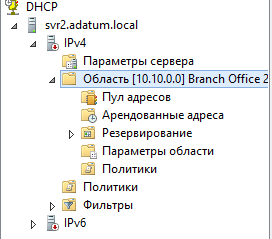


Рисунок 16 – Консоль DHCP.

Для проверки созданной области DHCP в оснастке управления DHCP выполните следующие действия. Откройте консоль DHCP через меню "Администрирование" или из "Диспетчера серверов". В дереве навигации слева раскройте узел сервера, затем разверните раздел IPv4.

Среди списка областей можно наблюдать созданную область с именем "Branch Office 2" и идентификатором 10.10.0.0.

# Практическая работа №3: Устранение неполадок DNS

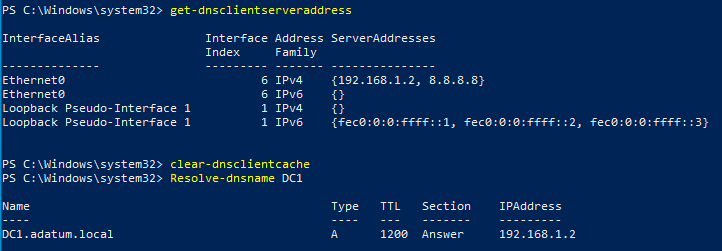


Рисунок 17 – Команды диагностики DNS.

На контроллере домена DC1 выполняем последовательность команд для диагностики DNS. Первой выполняется команда Get-DnsClientServerAddress, которая отображает текущие DNS-серверы, назначенные сетевым интерфейсам. В выводе будут показаны IP-адреса всех настроенных DNS-серверов для каждого активного сетевого адаптера.

Следующая команда Clear-DnsClientCache очищает локальный DNS-кэш на сервере. Это полезно при устранении проблем с разрешением имен, так как удаляет устаревшие или некорректные записи, заставляя систему выполнять новые DNS-запросы. Команда не выводит результатов при успешном выполнении.

Завершающая команда Resolve-DnsName DC1 проверяет возможность разрешения имени контроллера домена в IP-адрес. В выводе будет показана подробная информация о DNS-записи, включая полученный IP-адрес, тип записи и TTL. Это позволяет убедиться, что основная функциональность DNS работает корректно.

После выполнения этих команд можно сделать вывод о состоянии DNS-клиента на контроллере домена. Если все команды выполнены без ошибок, это свидетельствует о правильной базовой настройке DNS. При наличии проблем следует проверить сетевые подключения, настройки DNS-серверов в свойствах сетевых адаптеров и состояние службы DNS на самом контроллере домена.

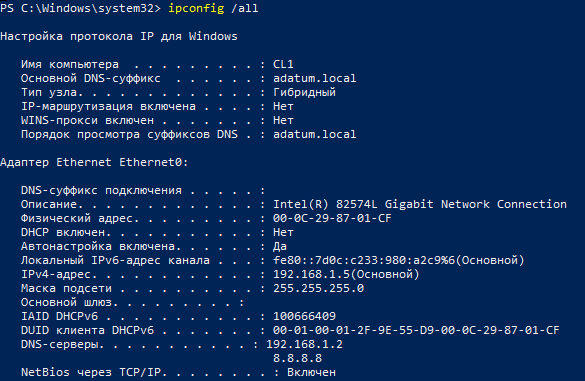


Рисунок 18 – Проверка сетевых настроек.

Для проверки сетевых настроек на CL1 необходимо выполнить команду ipconfig /all в командной строке. Эта команда выводит детальную информацию о конфигурации всех сетевых интерфейсов системы. В результате отображаются параметры каждого сетевого адаптера, включая физический адрес (MAC-адрес), назначенные IP-адреса (как IPv4, так и IPv6), способ получения адреса (DHCP или статический), маску подсети, основной шлюз, DNS-серверы с порядком их опроса, суффикс DNS и дополнительные параметры подключения.

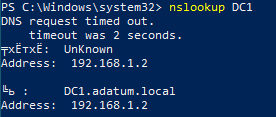


Рисунок 19 – Проверка работы DNS.

Для проверки работы DNS выполняется команда nslookup DC1. Она отправляет запрос к DNS-серверу для разрешения имени контроллера домена. В ответе будет указан используемый DNS-сервер и соответствующий IP-адрес DC1. Успешный ответ подтверждает корректность DNS-записи и доступность сервера. Если возникает ошибка, нужно проверить: настройки DNS в ipconfig /all, наличие записи DC1 в DNS-зоне и доступность DNS-сервера через ping. Для углубленной проверки можно в интерактивном режиме nslookup указать конкретный DNS-сервер командой server [IP], затем запросить DC1. Дополнительно стоит проверить обратное преобразование и SRV-записи, важные для AD.

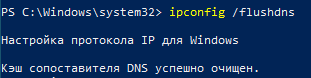


Рисунок 20 – Очищение кэша.

Для очистки DNS-кэша используется команда ipconfig /flushdns. После ее выполнения система удаляет все сохраненные DNS-записи, что полезно при проблемах с разрешением имен. Успешное выполнение команды подтверждается сообщением "Кэш DNS успешно очищен".

Очистка кэша особенно полезна после изменений в DNS-зонах или при переходе ресурсов на новые IP-адреса. Это стандартная процедура диагностики, которая часто решает проблемы с доступом к сетевым ресурсам.

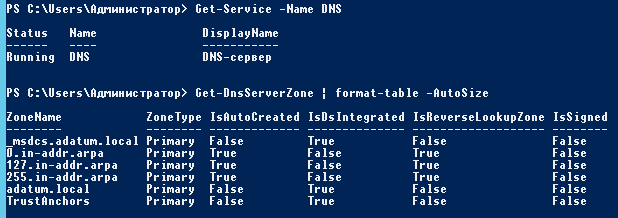


Рисунок 21 – Проверка состояния службы.

На DC1 проверяем состояние службы DNS. Для этого выполняем команду Get-Service -Name DNS, которая выводит текущий статус службы DNS-сервера. В результате отображается информация о состоянии службы (работает/остановлена), тип запуска и имя службы. Убеждаемся, что статус показывает "Running", что означает корректную работу DNS-сервера.

Далее проверяем зоны DNS с помощью команды Get-DnsServerZone | Format-Table -AutoSize. Эта команда выводит список всех зон DNS, настроенных на сервере, в компактном табличном формате. В выводе проверяем наличие основных зон: прямую (обычно соответствует доменному имени) и обратную (in-addr.arpa). Для каждой зоны отображается ее имя, тип (Primary, Secondary, Stub), статус и другие параметры.

Особое внимание уделяем зонам, связанным с Active Directory. Проверяем, что зона домена (например, domain.local) имеет тип "ActiveDirectory", что означает интеграцию с AD. Также убеждаемся в наличии и корректности обратных зон для используемых подсетей.

Если какие-то зоны отсутствуют или имеют неправильный тип, потребуется дополнительная настройка DNS. Для проверки записей в конкретной зоне можно использовать Get-DnsServerResourceRecord -ZoneName "имя\_зоны".

После проверки рекомендуется также удостовериться в правильности настроек передачи зон и обновлений, особенно если в инфраструктуре несколько DNS-серверов. Это можно сделать через Get-DnsServerZoneTransfer -Name "имя\_зоны".

Все команды выполняются в PowerShell с правами администратора. Полученные данные помогают оценить корректность конфигурации DNS-сервера и его готовность к обслуживанию запросов в доменной среде.

# Практическая работа №4: Установка роли DNS-сервера



Рисунок 22 – Powershell SRV1.

На сервере SVR1 выполняем настройку основной зоны DNS с заданными параметрами. В PowerShell с правами администратора вводим команду создания первичной зоны: Add-DnsServerPrimaryZone -Name fabrikam.com -DynamicUpdate Secure -ReplicationScope Domain.

Команда создает новую первичную зону DNS с именем fabrikam.com, которая будет интегрирована с Active Directory. Параметр DynamicUpdate Secure разрешает безопасное динамическое обновление записей, что позволяет клиентам автоматически регистрировать свои имена в DNS с проверкой подлинности. Параметр ReplicationScope Domain обеспечивает репликацию данных зоны на все DNS-серверы домена, что важно для поддержания согласованности данных в распределенной среде.

После выполнения команды система создает новую зону и настраивает ее согласно указанным параметрам. Для проверки результата можно использовать команду Get-DnsServerZone -Name fabrikam.com, которая отобразит свойства созданной зоны. Убеждаемся, что в выводе присутствует созданная зона с правильным типом репликации и параметрами обновления.

Особое внимание следует уделить проверке безопасности зоны. Так как указан безопасный режим обновлений, необходимо убедиться, что соответствующие разрешения установлены корректно. Это можно проверить через DNS-менеджер или командлет Get-DnsServerResourceRecord -ZoneName fabrikam.com.

Для завершения настройки рекомендуется проверить возможность динамической регистрации записей, подключив тестовое клиентское устройство к домену и убедившись, что его запись появляется в зоне fabrikam.com. Также стоит проверить репликацию зоны на другие контроллеры домена, выполнив на них Get-DnsServerZone и убедившись в наличии созданной зоны с одинаковыми параметрами.

Эта конфигурация подходит для доменных сред, где требуется обеспечить безопасное и согласованное хранение DNS-записей с автоматическим обновлением данных. При необходимости можно дополнительно настроить делегирование зоны или трансферы для вторичных серверов.

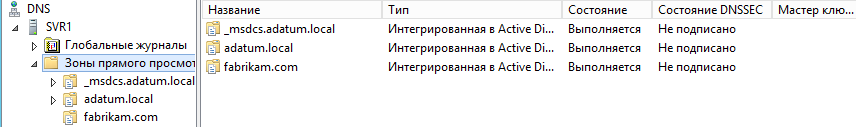


Рисунок 23 – Проверка зоны.

Успешное создание подтверждается наличием зоны в списке (проверить все зоны можно через Get-DnsServerZone без параметров).

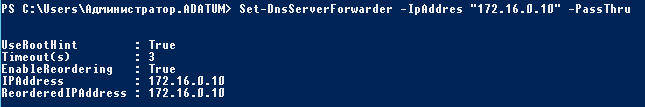


Рисунок 24 – PowerShell.

Для настройки переадресации DNS-запросов на сервере DC1 выполняется команда Set-DnsServerForwarder -IPAddress 172.16.0.10 -PassThru. Эта команда задает указанный IP-адрес в качестве DNS-форвардера, куда будут направляться запросы для внешних доменов, если локальный сервер не может их разрешить.

Параметр -PassThru обеспечивает вывод результата выполнения команды, позволяя сразу убедиться в применении изменений. После выполнения следует проверить настройки командой Get-DnsServerForwarder, которая должна отобразить добавленный IP-адрес форвардера.

Перед применением важно убедиться в доступности указанного DNS-сервера (172.16.0.10) через ping или Test-NetConnection. Также рекомендуется проверить, что брандмауэр не блокирует DNS-запросы на порт 53.

Настроенный форвардер ускоряет разрешение внешних DNS-запросов и снижает нагрузку на локальный сервер. Однако для доменных зон (например, связанных с Active Directory) запросы будут обрабатываться локально без переадресации.

Для комплексной проверки можно выполнить nslookup для внешнего домена (например, example.com) и убедиться, что запрос корректно обрабатывается через форвардер. При проблемах следует проверить журнал DNS-сервера и настройки сетевых интерфейсов.

# Практическая работа №5. Создание AD-интегрированной зоны.

1. Повышение LON-SVR1 до контроллера домена:

Для повышения LON-SVR1 до контроллера домена выполните следующие шаги. Сначала откройте Диспетчер серверов. В меню выберите Управление, затем Добавить роли и компоненты. В мастере установки перейдите к выбору ролей сервера. Отметьте Active Directory Domain Services (AD DS) и подтвердите добавление необходимых компонентов. Нажмите Далее и запустите установку.

После установки роли в Диспетчере серверов появится уведомление о необходимости повышения до контроллера домена. Нажмите на это уведомление для запуска мастера настройки AD DS. В мастере выберите "Добавить контроллер домена в существующий домен". Укажите имя домена и введите учетные данные администратора домена.

На этапе настройки параметров отметьте установку DNS-сервера (обязательно) и Глобального каталога (рекомендуется). Задайте пароль для Режима восстановления служб каталогов (DSRM). Продолжите установку, после чего сервер автоматически перезагрузится. После перезагрузки LON-SVR1 станет полноправным контроллером домена.

Для проверки успешности выполнения откройте оснастку "Пользователи и компьютеры Active Directory" и убедитесь, что сервер появился в списке контроллеров домена. Также можно использовать команду Get-ADDomainController в PowerShell для подтверждения роли сервера.

2. Создание зоны contoso.com:

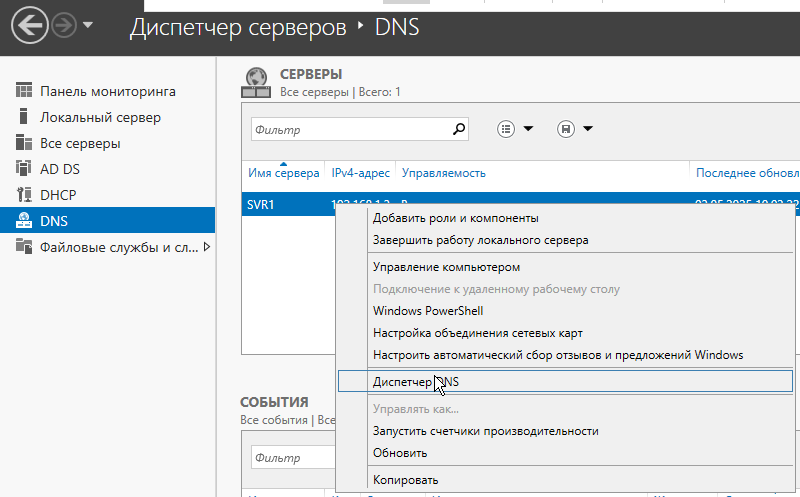


Рисунок 25 – Открытие диспетчера серверов.

Для работы с DNS в Диспетчере серверов необходимо выполнить следующие действия. Сначала открываем Диспетчер серверов через меню Пуск или поиск в системе. В левой части интерфейса находим и выбираем раздел DNS. Далее нажимаем правой кнопкой мыши на имя нужного DNS-сервера (например, LON-DC1) и выбираем пункт "Диспетчер DNS" из контекстного меню. Это откроет оснастку управления DNS, где можно просматривать и изменять зоны DNS, проверять записи, настраивать параметры сервера. В открывшемся Диспетчере DNS будет отображаться древовидная структура со списком всех настроенных зон (прямых и обратных), параметрами сервера и другими элементами конфигурации. Для работы с конкретной зоной нужно развернуть соответствующий узел в дереве консоли. Все изменения вносятся через контекстное меню или панель действий. После выполнения необходимых настроек оснастку можно закрыть - изменения сохраняются автоматически.

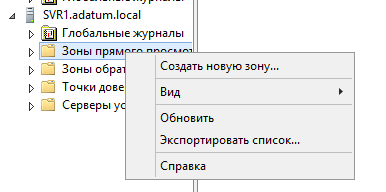


Рисунок 26 – Создание новой зоны прямого просмотра.

Для создания новой зоны прямого просмотра в Диспетчере DNS на сервере SVR1.adatum.local выполните следующие действия. Сначала разверните узел сервера SVR1.adatum.local в левой части окна Диспетчера DNS. Найдите и разверните раздел "Зоны прямого просмотра". Щелкните правой кнопкой мыши по этому разделу и выберите пункт "Создать зону" в контекстном меню.

Запустится мастер создания новой зоны. На первом этапе выберите тип создаваемой зоны - рекомендуется выбрать "Основная зона". На следующем шаге укажите, что зона должна храниться в Active Directory для обеспечения репликации между контроллерами домена. Затем введите полное имя новой зоны.

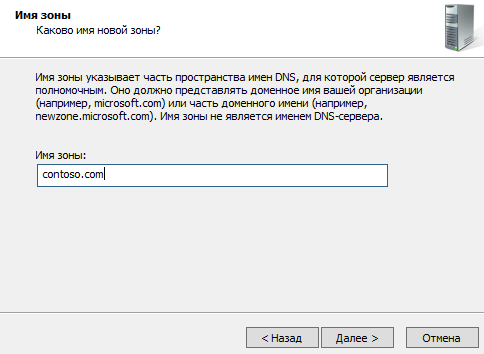


Рисунок 27 – Имя зоны.

Важным параметром является настройка динамического обновления. Для безопасности выберите вариант "Разрешить только безопасное динамическое обновление". Это позволит клиентам автоматически регистрировать свои записи в DNS, но только после аутентификации в домене.

После завершения работы мастера новая зона появится в списке зон прямого просмотра. Система автоматически создаст необходимые начальные записи: SOA (Start of Authority) и NS (Name Server). Для проверки правильности создания зоны можно использовать команду nslookup в командной строке, указав имя новой зоны.

При необходимости в созданную зону можно добавлять новые записи вручную: A-записи для узлов, MX для почтовых серверов, CNAME для псевдонимов и другие. Все изменения будут автоматически реплицированы на другие DNS-серверы домена благодаря интеграции с Active Directory.

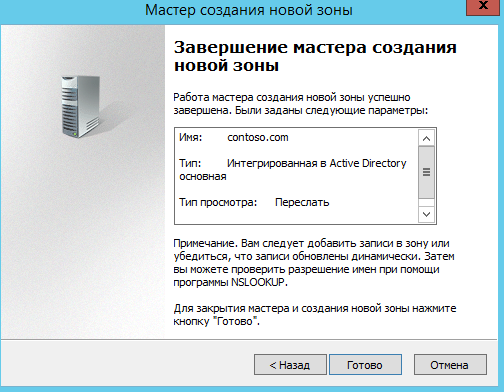


Рисунок 28 – Завершение создания новой зоны.

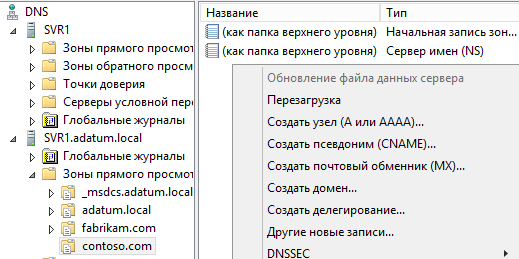


Рисунок 29 – Создание узла.

Для добавления записи www в новую зону DNS выполните следующие шаги. Откройте Диспетчер DNS и перейдите к созданной ранее зоне прямого просмотра. В контекстном меню зоны выберите пункт создания новой записи типа А. В открывшемся окне укажите имя узла как www и соответствующий IP-адрес 172.16.0.100. Подтвердите создание записи.

Дополнительно можно проверить наличие созданной записи непосредственно в оснастке DNS, где она должна отображаться в списке ресурсных записей зоны. Убедитесь, что запись имеет правильный тип (А) и назначенный адрес.

Все изменения в DNS следует вносить аккуратно, так как они могут повлиять на работу сетевых служб и приложений, использующих доменные имена для доступа к ресурсам. После внесения изменений рекомендуется провести тестирование работы всех зависимых сервисов.

3. Проверка репликации на LON-SVR1.

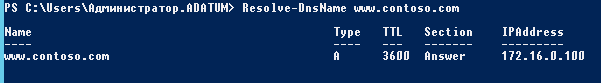


Рисунок 30 – Проверка репликации.

Проверка репликации DNS на сервере SVR1 выполняется с помощью команды Resolve-DnsName. В PowerShell вводится команда Resolve-DnsName www.contoso.com -Server SVR1 для проверки разрешения имени через указанный сервер. В случае успешной репликации зоны contoso.com команда должна вернуть IP-адрес 172.16.0.100, который был назначен записи www.contoso.com.

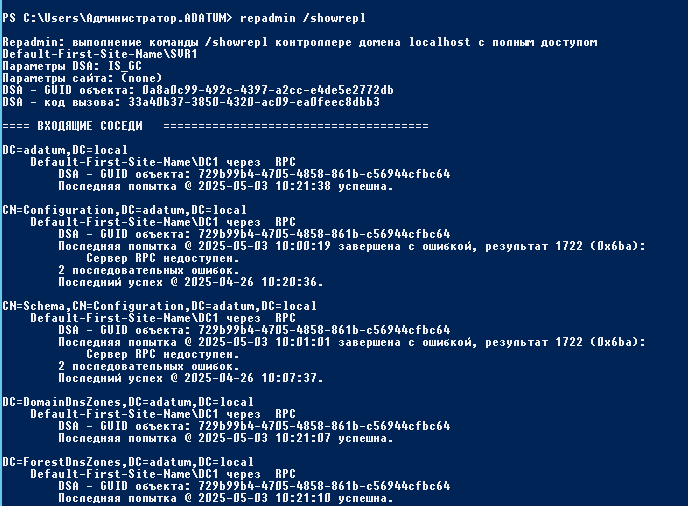


Рисунок 31 – Проверка репликации.

# Лабораторная работа 6.1: Реализация DHCP

Упражнение 1: Настройка DHCP

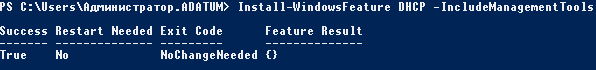


Рисунок 32 – Установка роли DHCP.



Рисунок 33 – Завершение настройки.

На сервере SVR1 выполняется установка роли DHCP-сервера. Процедура осуществляется через PowerShell с правами администратора. Используется командлет Install-WindowsFeature с указанием имени роли DHCP и необходимых компонентов управления.

Полная команда для установки: Install-WindowsFeature DHCP -IncludeManagementTools. После выполнения система проведет установку необходимых компонентов. Процесс может занять несколько минут в зависимости от производительности сервера.

По завершении установки требуется зарегистрировать сервер в Active Directory. Это выполняется командой Add-DhcpServerInDC, которая добавляет сервер в список авторизованных DHCP-серверов домена. Без этой процедуры сервер не сможет обслуживать клиентов в доменной среде.

После регистрации необходимо перезагрузить сервер для применения всех изменений. Далее можно приступать к созданию областей (scopes) и настройке параметров DHCP. Проверить успешность установки можно командой Get-WindowsFeature, которая отобразит список установленных ролей с отметкой о состоянии DHCP.



Рисунок 34 – Powershell.

На сервере SVR1 создается новая область DHCPv4 с помощью команды PowerShell. Выполняется следующая команда: Add-DhcpServerv4Scope -Name "BranchOffice" -StartRange 192.168.1.100 -EndRange 192.168.1.200 -SubnetMask 255.255.255.0 -State Active. Эта команда создает активную область с именем BranchOffice, которая будет распределять адреса из диапазона 192.168.1.100-192.168.1.200 с маской подсети 255.255.255.0.

После выполнения команды рекомендуется проверить созданную область. Это можно сделать с помощью командлета Get-DhcpServerv4Scope, который выведет список всех областей на сервере. Созданная область должна отображаться в списке с указанными параметрами: именем, диапазоном адресов, маской подсети и состоянием "Active".

Для полноценной работы области необходимо дополнительно настроить параметры, такие как шлюз по умолчанию, DNS-серверы и другие опции. Это выполняется отдельными командами, например: Set-DhcpServerv4OptionValue -Router 192.168.1.1 для указания шлюза по умолчанию.

Перед вводом области в эксплуатацию следует убедиться, что указанный диапазон адресов не пересекается с другими областями DHCP в сети и не включает адреса, назначенные статически. Также рекомендуется проверить доступность адресов из диапазона с помощью ping перед началом использования области.



Рисунок 35 – Powershell.

На сервере SVR1 выполняется настройка исключений в созданной области DHCP BranchOffice. Применяется команда: Add-DhcpServerv4ExclusionRange -ScopeId 192.168.1.0 -StartRange 192.168.1.1 -EndRange 192.168.1.99. Данная команда резервирует диапазон адресов с 192.168.1.1 по 192.168.1.99, исключая их из автоматического распределения DHCP-сервером.

Исключение указанного диапазона необходимо для резервирования адресов под устройства, требующие статической IP-настройки, такие как сетевые принтеры, серверы или другое оборудование. После выполнения команды DHCP-сервер не будет назначать эти адреса клиентам автоматически.

Для проверки созданного исключения используется команда: Get-DhcpServerv4ExclusionRange -ScopeId 192.168.1.0. Она отобразит все исключенные диапазоны в указанной области. Убедитесь, что новый диапазон 192.168.1.1-192.168.1.99 присутствует в выводе команды.



Рисунок 36 – Powershell.

На сервере SVR1 выполняется настройка параметров DHCP для области BranchOffice. Используется команда Set-DhcpServerv4OptionValue с указанием ScopeId 192.168.1.0 и параметра Router 192.168.1.1. Эта команда устанавливает основной шлюз для клиентов, получающих адреса из данной области DHCP.

После выполнения команды клиентские устройства при получении IP-адреса из диапазона 192.168.1.100-192.168.1.200 будут автоматически настраивать указанный шлюз 192.168.1.1 в своих сетевых параметрах. Это обеспечит корректную маршрутизацию трафика за пределы локальной подсети.

Для проверки примененных настроек можно использовать команду Get-DhcpServerv4OptionValue -ScopeId 192.168.1.0, которая отобразит все установленные параметры для указанной области. В выводе должен присутствовать параметр Router со значением 192.168.1.1.

Рекомендуется дополнительно проверить доступность указанного шлюза с клиентских устройств после получения ими новых сетевых настроек. Это можно сделать командой ping 192.168.1.1 с любого клиента в подсети.

Все изменения применяются немедленно и затрагивают только новые запросы на получение адреса. Уже подключенные клиенты получат новые параметры при следующем обновлении аренды адреса.



Рисунок 37 – Установка DNS-сервера.

На сервере SVR1 выполняется настройка DNS-серверов для области DHCP BranchOffice с идентификатором 192.168.1.0. Применяется команда: Set-DhcpServerv4OptionValue -ScopeId 192.168.1.0 -DnsServer 192.168.1.2,192.168.1.2. Данная команда назначает DNS-сервер с адресом 192.168.1.2 в качестве основного и дополнительного для клиентов, получающих адреса из указанной области.

После выполнения команды все клиентские устройства, запрашивающие настройки сети через DHCP, будут получать указанный DNS-сервер в своих сетевых параметрах. Важно отметить, что адрес 192.168.1.2 указан дважды, что означает его использование как первичного и вторичного DNS-сервера. В рабочих средах обычно указывают разные DNS-серверы для обеспечения отказоустойчивости.



Рисунок 38 – Установка доменного имени.

На сервере SVR1 выполняется конфигурация доменного суффикса для DHCP-клиентов в области BranchOffice с идентификатором 192.168.1.0. Используется командлет Set-DhcpServerv4OptionValue с параметрами ScopeId 192.168.1.0 и DnsDomain adatum.com. Данная команда назначает доменный суффикс adatum.com для всех устройств, получающих сетевые настройки через указанную область DHCP.

После выполнения команды клиентские системы будут автоматически использовать указанный доменный суффикс при разрешении имен и регистрации в DNS. Это позволяет упростить доступ к ресурсам домена, используя короткие имена вместо полных доменных имен.

На клиентских устройствах изменения вступят в силу после обновления DHCP-аренды. Для проверки работоспособности на клиенте следует освободить и обновить IP-адрес (ipconfig /release + ipconfig /renew), затем проверить применение доменного суффикса через ipconfig /all. Дополнительно рекомендуется проверить разрешение имен внутри домена и возможность регистрации клиента в DNS.

Упражнение 2: Настройка агента ретрансляции DHCP

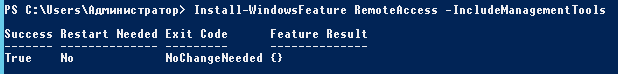


Рисунок 39 - Установка службы маршрутизации

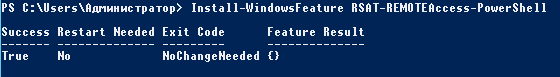


Рисунок 40 – Установка подкомпонента.

Установка службы маршрутизации на сервере выполняется через добавление соответствующей роли. Для этого в PowerShell с правами администратора используется команда Install-WindowsFeature Routing -IncludeManagementTools. Данная команда устанавливает компоненты службы маршрутизации и удаленного доступа, включая необходимые инструменты управления.

После установки требуется дополнительная настройка через оснастку "Маршрутизация и удаленный доступ". В консоли управления сервером выбирается пункт "Добавить роли и компоненты", где в разделе "Роли сервера" отмечается "Служба удаленного доступа". В составе этой роли выбирается подкомпонент "Маршрутизация".

Завершив установку, необходимо перейти к настройке службы. В оснастке "Маршрутизация и удаленный доступ" через мастер настройки сервера выбирается вариант "Особая конфигурация" и далее "Маршрутизация LAN". Мастер проведет через процесс настройки, после чего потребуется завершить конфигурацию и запустить службу.

После успешной установки и настройки можно приступать к конфигурации конкретных параметров маршрутизации: добавлению статических маршрутов, настройке протоколов маршрутизации или определению политик пересылки пакетов. Все изменения рекомендуется тестировать перед вводом в эксплуатацию.

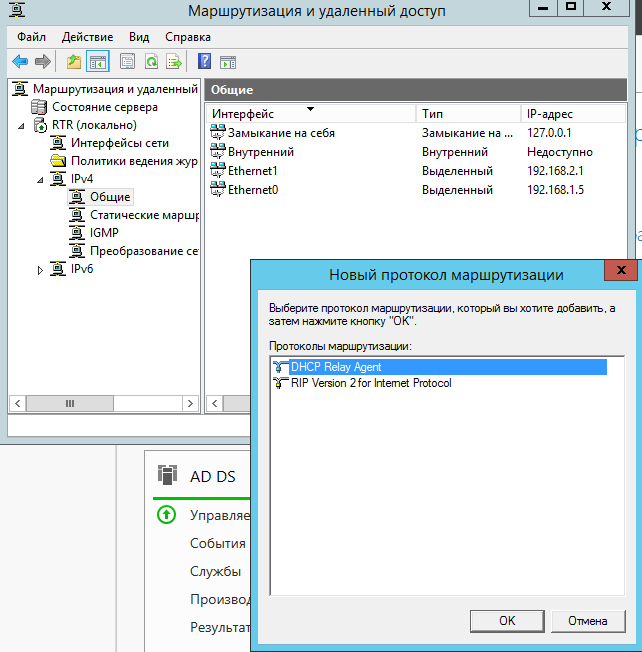


Рисунок 41 – Маршрутизация и удаленный доступ.

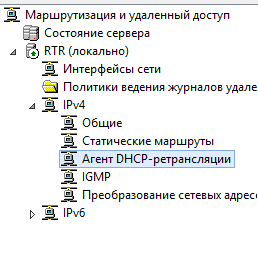


Рисунок 42 – Список «Маршрутизация и удаленный доступ.»

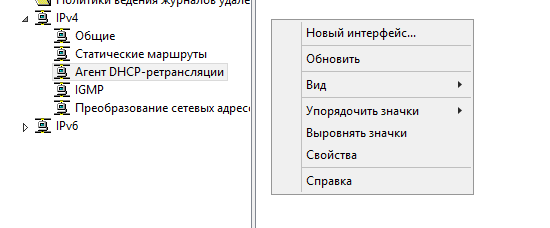


Рисунок 43 – Добавление нового интерфейса.

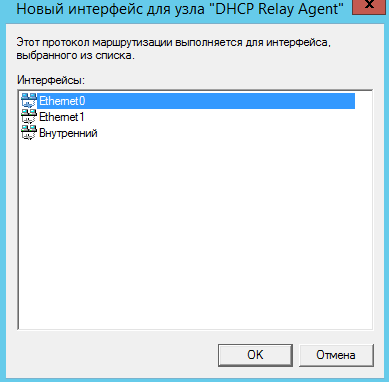


Рисунок 44 – Реализация нового интерфейса.

Настраивается DHCP-ретрансляция на сервере с установленной ролью маршрутизации. Процедура выполняется через оснастку "Маршрутизация и удаленный доступ". В дереве консоли выбирается раздел IPv4, затем пункт DHCP-ретранслятор. Через свойства данного компонента задаются адреса целевых DHCP-серверов, куда будут перенаправляться запросы клиентов.

Для работы ретранслятора необходимо добавить сетевые интерфейсы, которые будут принимать запросы от клиентов. Для каждого интерфейса настраиваются параметры hop-count (максимальное количество переходов) и boot threshold (задержка перед пересылкой запроса). Типичные значения - 4 перехода и 2 секунды задержки соответственно.

После настройки проверяется работоспособность: клиент в удаленной подсети запрашивает адрес через ipconfig /renew, при этом DHCP-сервер должен зарегистрировать новую аренду. Для диагностики используются журналы событий DHCP-сервера и утилиты мониторинга трафика.

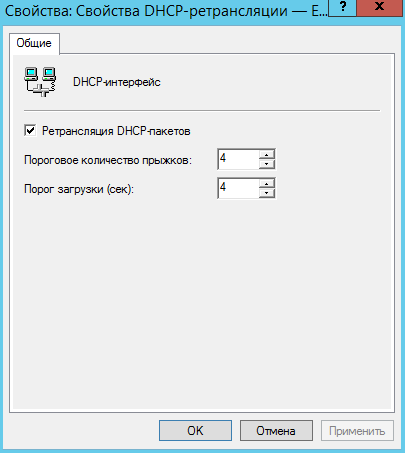


Рисунок 45 – Свойства DHCP-ретрансляции.

Необходимо, чтобы в свойствах DHCP-ретрансляции была включена ретрансляция DHCP-пакетов и далее как на «Рисунке 45».

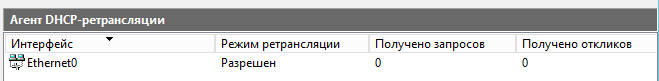


Рисунок 46 – Агент DHCP-ретрансляции.

# Лабораторная работа №6.2: Реализация DNS

Упражнение 1: Установка и настройка DNS на DC1

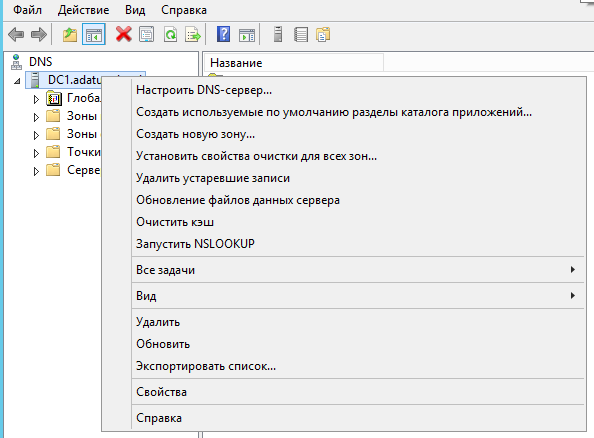


Рисунок 47 – Переход во свойства.

Для проверки и настройки параметров DNS на локальном сервере выполняем следующие действия. Открываем Диспетчер серверов через меню Пуск или поиск в системе. В левой панели выбираем раздел DNS. Развертываем дерево серверов и находим наш локальный сервер. Кликаем правой кнопкой мыши на имени сервера и выбираем пункт "Свойства" в контекстном меню.

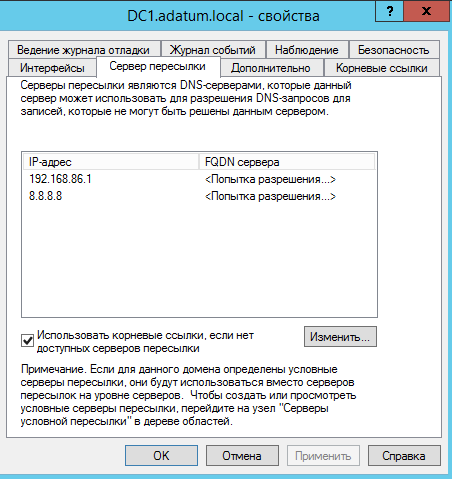


Рисунок 48 – Свойства DC1.

Переходим в свойства DNS-сервера через Диспетчер серверов. В открывшемся окне выбираем вкладку "Сервер пересылки". Нажимаем кнопку "Изменить" для настройки параметров переадресации DNS-запросов. В поле ввода добавляем IP-адрес 8.8.8.8, который является публичным DNS-сервером Google. Подтверждаем добавление нажатием кнопки "Добавить". Завершаем процесс нажатием "Применить" для сохранения изменений и "OK" для закрытия окна свойств.

После выполнения этих действий DNS-сервер будет перенаправлять запросы, которые не может разрешить локально, на указанный публичный DNS-сервер. Это обеспечит корректное разрешение интернет-доменов при сохранении локальной обработки запросов для внутренних зон.

Упражнение 2: Создание А-записей

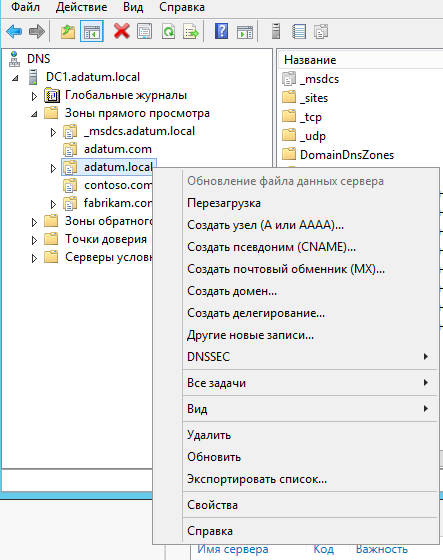


Рисунок 49 – Создание узла.

Переходим в оснастку управления DNS через Диспетчер серверов. В дереве консоли раскрываем узел "Зоны прямого просмотра", где отображаются все созданные прямые зоны DNS. Находим и выбираем нужный домен (в данном случае adatum.local), кликнув по нему левой кнопкой мыши.

После выбора зоны adatum.local в правой панели отображается список всех существующих DNS-записей этой зоны. Здесь можно просматрить, добавлять, изменять или удалять записи различных типов (A, MX, CNAME и другие). Для создания новой записи используется контекстное меню (правая кнопка мыши на зоне или в пустом месте правой панели), где выбирается соответствующий тип создаваемой записи.

При работе с зоной домена Active Directory (adatum.local) особое внимание следует уделить системным записям, которые автоматически создаются контроллерами домена. Эти записи критически важны для работы служб Active Directory, их случайное удаление или изменение может привести к проблемам в работе домена.

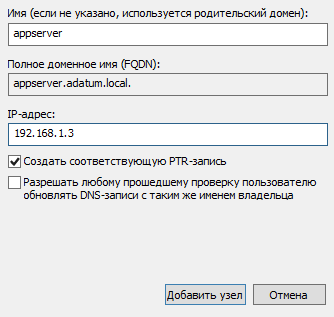


Рисунок 50 – Создание узла.

В оснастке Диспетчер DNS на сервере SVR1 выполняется создание новой записи типа А для узла appserver в зоне adatum.local. Для этого необходимо открыть зону прямого просмотра adatum.local, затем в контекстном меню выбрать пункт создания нового узла (записи типа А). В открывшемся окне указывается имя узла - appserver и соответствующий IP-адрес сервера SVR1.

После заполнения полей и подтверждения создается новая DNS-запись, которая связывает имя appserver.adatum.local с указанным IP-адресом.

Важно убедиться, что указанный IP-адрес действительно соответствует серверу SVR1 и доступен в сети. Также рекомендуется проверить возможность разрешения созданного имени с других узлов сети для подтверждения репликации DNS-записи на все серверы домена.

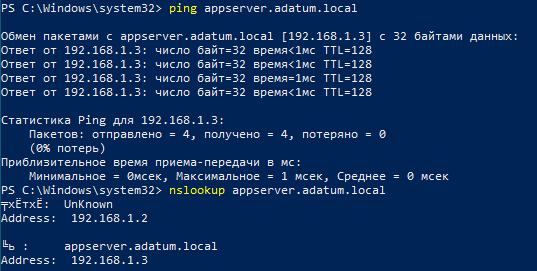


Рисунок 51 – Проверка с помощью ping.

На клиентском компьютере CL1 выполняем проверку работы DNS и доступности сервера appserver. В командной строке вводим команду ping appserver.adatum.local для проверки сетевой связности. Эта команда отправляет ICMP-запросы к указанному узлу и должна получить ответ от IP-адреса, соответствующего A-записи в DNS.

Затем выполняем команду nslookup appserver.adatum.local для проверки корректности разрешения доменного имени. Эта команда отправляет запрос к DNS-серверу и должна вернуть IP-адрес, указанный в записи для данного узла.

Все команды выполняются в стандартной командной строке Windows без необходимости повышенных прав. Результаты проверки помогают убедиться в корректности работы DNS и сетевой инфраструктуры домена. При обнаружении проблем следует последовательно проверить настройки DNS, сетевые параметры и конфигурацию брандмауэра на всех участвующих узлах.

Упражнение 3: Управление кэшем DNS

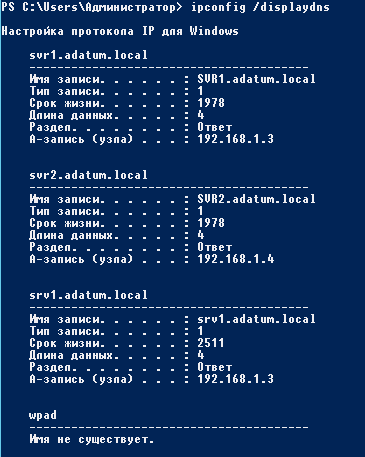


Рисунок 52 – Просмотр DNS-кэша.

На контроллере домена DC1 выполняется проверка содержимого DNS-кэша. Для этого необходимо открыть командную строку с повышенными привилегиями (от имени администратора) и выполнить команду ipconfig /displaydns. Данная команда выводит полный список DNS-записей, сохраненных в кэше операционной системы.

В результате выполнения команды отображается подробная информация о каждой кэшированной записи, включая доменное имя, соответствующий IP-адрес, тип записи (A, AAAA, CNAME и другие), время жизни записи (TTL) и другие параметры. Записи сортируются в хронологическом порядке, начиная с последних использованных.

Для очистки DNS-кэша используется команда ipconfig /flushdns, выполняемая также с правами администратора. После очистки кэша новые DNS-запросы будут обрабатываться сервером заново, без использования сохраненных данных.

Проверка DNS-кэша полезна при диагностике проблем с разрешением имен, когда требуется убедиться в актуальности получаемых клиентом DNS-записей или выявить возможные несоответствия между кэшированными и актуальными данными на сервере.

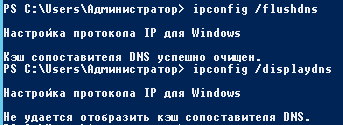


Рисунок 53 – Очистка кэша.

На контроллере домена DC1 выполняется очистка DNS-кэша с использованием команды ipconfig /flushdns. Для выполнения данной операции необходимо открыть командную строку с правами администратора. После ввода команды система производит полную очистку временных DNS-записей, сохраненных в локальном кэше.

Команда не требует дополнительных параметров и выполняет немедленное удаление всех кэшированных данных. Успешное выполнение операции подтверждается сообщением "Кэш DNS успешно очищен". Это означает, что последующие DNS-запросы будут обрабатываться заново, без использования ранее сохраненной информации.

Очистка DNS-кэша является стандартной процедурой при устранении проблем с разрешением имен, особенно после внесения изменений в DNS-зону или при возникновении конфликтов записей. Рекомендуется выполнять эту операцию при следующих ситуациях: изменение IP-адресов серверов, проблемы с доступом к сетевым ресурсам, необходимость принудительного обновления DNS-информации.

После очистки кэша для проверки можно использовать команды nslookup или ping к целевым доменным именам, чтобы убедиться в корректности их разрешения. Также можно повторно выполнить ipconfig /displaydns для подтверждения отсутствия старых записей в кэше.

Важно отметить, что очистка DNS-кэша влияет только на локальный компьютер и не затрагивает записи на DNS-серверах. Для полного обновления DNS-информации в домене могут потребоваться дополнительные действия на серверах DNS.

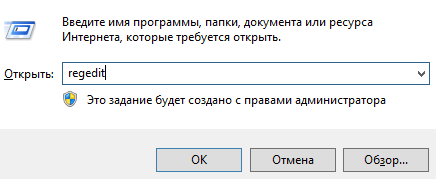


Рисунок 54 – Открытие редактора реестра.

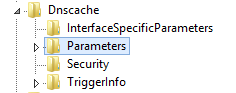
****

Рисунок 55 – Редактор реестра.

Для отключения кэширования DNS на сервере DC1 выполняем следующие действия. Открываем редактор реестра путем нажатия комбинации клавиш Win+R и ввода команды regedit в диалоговом окне "Выполнить". В открывшемся редакторе реестра переходим по следующему пути: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters.

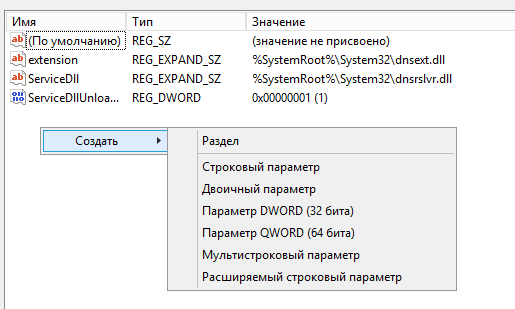
****

Рисунок 56 – Создание параметра DWORD.

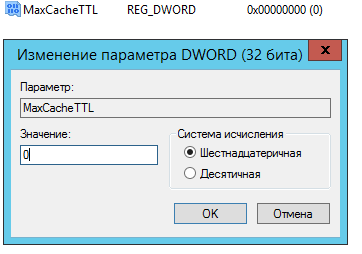
****

Рисунок 57 Изменение MaxCache в 0.

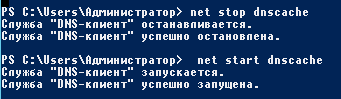
****

Рисунок 58 – Перезапуск DNS.

В данном разделе необходимо создать или изменить параметр DWORD с именем MaxCacheTTL. Устанавливаем значение 0, что полностью отключает кэширование DNS. Также рекомендуется создать или изменить параметр MaxNegativeCacheTTL, также установив значение 0, чтобы отключить кэширование отрицательных ответов.

После внесения изменений в реестр требуется перезагрузка сервера для применения новых параметров. Альтернативно можно перезапустить службу DNS-клиента (Dnscache) через командную строку с повышенными привилегиями, выполнив команды: net stop dnscache и net start dnscache.

Важно понимать, что отключение DNS-кэширования может увеличить нагрузку на DNS-серверы, так как все запросы будут обрабатываться заново. Данную настройку следует применять только в диагностических целях или в специфических сценариях, когда актуальность DNS-записей критически важна.