РОСЖЕЛДОР
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный университет путей сообщения»
(ФГБОУ ВО РГУПС)

Соколова О.И., Бондаренко А.Д.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ЛАБОРАТОРНЫХ РАБОТ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

ОП.05 «КОМПЬЮТЕРНЫЕ СЕТИ»

для специальности
09.02.09 Веб-разработка

Ростов-на-Дону
2025

СОДЕРЖАНИЕ

Введение

Методические указания к лабораторным работам и по выполнению самостоятельной работы студентов составлены в соответствии с ФГОС СПО и рабочей программой профессионального модуля ОП.05 «Компьютерные сети», которые являются частью программы подготовки специалистов среднего звена специальности 09.02.09 Веб-разработка.

Рабочей программой дисциплины ОП.05 «Компьютерные сети» предусмотрено на выполнение лабораторных работ – 42 часа и самостоятельной работы студентов – 36 часов.

При выполнении лабораторных работ и при организации самостоятельной работы студентов используются активные и интерактивные формы обучения - просмотр и обсуждение учебных видеофильмов, групповая дискуссия, лекция - консультация, моделирование производственных процессов и ситуаций, обсуждение в группах, тренинг, кейс-метод, защита практических и лабораторных работ и другие.

Цель методических рекомендаций - оказание методической помощи студентам в выполнении лабораторных работ и в организации их самостоятельной работы по изучению учебного материала, для расширения, углубления и закрепления знаний и умений, а также формирования профессиональных (ПК) компетенций.

Код и содержание компетенции	Уметь	Знать
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.	Анализировать сетевую проблему (потери пакетов, отсутствие связи) и выбирать оптимальный способ её решения из нескольких возможных.	Принципы сетевой диагностики и основные методы устранения неполадок на разных уровнях модели OSI/TCP-IP.
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.	Находить и критически оценивать техническую информацию по сетевым технологиям (настройки, протоколы, уязвимости).	Основные источники профессиональной информации: RFC-стандарты, документация вендоров, технические форумы, базы знаний.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.	Применять специализированное ПО для проектирования, эмуляции, мониторинга и администрирования сетей.	Современное программное обеспечение для работы с сетевой инфраструктурой.
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Настраивать и использовать сетевое окружение для решения профессиональных задач (настройка сервисов, удалённое управление).	Основы сетевого взаимодействия, принципы работы клиент-серверных приложений, нормы информационной безопасности.
ПК 1.1. Проектировать информационные ресурсы.	Рассчитывать длины и выбирать типы кабелей, разрабатывать план размещения оборудования и трассировки кабельных трасс.	Стандарты структурированных кабельных систем (СКС), характеристики кабелей (витая пара, оптоволокно), правила монтажа.
ПК 2.3. Настраивать права пользователей в соответствии с функциональными задачами (ролями) и на основании информации о поведенческих факторах.	Настраивать и администрировать основные сетевые службы: DHCP, DNS, файловые, веб-серверы, каталоги (Active Directory).	Архитектуру, принципы работы и протоколы ключевых сетевых служб; основы системного администрирования.
ПК 2.4. Применять программные средства обеспечения безопасности информации веб-приложений.	Использовать средства мониторинга для сбора данных, анализировать трафик и журналы событий для оценки производительности и диагностики проблем.	Методы и средства мониторинга сетевого оборудования и трафика; ключевые показатели производительности сети (KPI).

ПК 4.1. Администрировать среды и платформы разработки информационных ресурсов.	Настраивать базовые механизмы защиты: брандмауэры (файрволы), политики доступа, VPN, безопасную беспроводную сеть.	Основные сетевые угрозы и уязвимости; принципы и технологии защиты информации в сетях (шифрование, аутентификация).

1 ПЛАН РАСПРЕДЕЛЕНИЯ УЧЕБНОЙ НАГРУЗКИ

Объем дисциплины в академических часах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.

Вид учебной работы	**Объем часов**
Объем образовательной программы учебной дисциплины	**108**
в том числе:	
Лекции (теоретическое обучение)	28
Лабораторные работы	42
Самостоятельная работа	36
Промежуточная аттестация (в форме зачета)	**2**

Содержание дисциплины

Наименование лекционных занятий	**Трудоемкость аудиторной работы, часы**
Раздел № 1 Введение в компьютерные сети. Базовые понятия и модели.	
1.1 Назначение, классификация и топологии сетей. Аппаратные компоненты (NIC, хабы, свитчи, маршрутизаторы).	2
1.2 Сетевая модель OSI и стек TCP/IP.	2
Раздел № 2 Передача данных по сети. Физический и канальный уровни. Локальные сети (LAN).	
2.1 Среды передачи. Технология Ethernet. MAC-адресация. Протокол ARP.	2
2.2 Коммутаторы. Виртуальные сети (VLAN): концепция и базовые настройки.	2
Раздел № 3 Передача данных по сети. Сетевой уровень. IP-адресация и маршрутизация.	
3.1 Протокол IPv4. Бесклассовая адресация (CIDR). Расчёт подсетей.	4
3.2 Основы маршрутизации. Статическая маршрутизация. Протоколы RIP/OSPF.	2
Раздел № 4 Передача данных по сети. Транспортный уровень.	

Наименование лекционных занятий	Трудоемкость аудиторной работы, часы
4.1 Протоколы TCP и UDP. Понятие порта. Анализ сегментов.	2
4.2 Программные средства обеспечения безопасности функционирования веб-приложений. Виды организации контроля доступа к системам и способы распределения прав.	2
Раздел № 5 Передача данных по сети. Сеансовый, представительный и прикладной уровни. Сетевые службы.	
5.1 Управление диалогом (RPC, PPTP). Перевод данных (SSL/TLS)	2
5.3 DNS: архитектура, типы записей. DHCP: принцип работы.	2
5.2 Сетевые службы и интерфейсы для пользователя.	2
Раздел № 6 Основы сетевой безопасности.	
6.1 Угрозы и базовые меры защиты. Межсетевые экраны (ACL).	2
6.2 Виртуальные частные сети (VPN). Безопасность Wi-Fi.	2

Лабораторные работы

Наименование лабораторных работ	Трудоемкость аудиторной работы, часы
Раздел № 1 Введение в компьютерные сети. Базовые понятия и модели.	
1.1 Сопоставление сетевых протоколов, устройств и единиц данных уровням модели OSI	2
1.2 Знакомство с анализатором трафика Wireshark	2
Раздел № 2 Передача данных по сети. Физический и канальный уровни. Локальные сети (LAN).	
2.1 Обжим витой пары по стандартам TIA/EIA-568A/B, проверка кабельным тестером.	2
2.1 Изучение MAC-адресов сетевых интерфейсов и таблицы коммутатора.	2
2.2 Разделение одной физической сети на несколько логических (VLAN) для изоляции трафика.	2

Наименование лабораторных работ	Трудоемкость аудиторной работы, часы
Раздел № 3 Передача данных по сети. Сетевой уровень. IP-адресация и маршрутизация.	
3.1 Работа с масками переменной длины.	2
3.2 Настройка IPv4-адресов на компьютерах и маршрутизаторах в симуляторе.	2
3.3 Конфигурация статических маршрутов на нескольких маршрутизаторах.	2
3.4 Наблюдение за автоматическим построением таблиц маршрутизации.	2
Раздел № 4 Передача данных по сети. Транспортный уровень.	
4.1 Захват и сравнение сегментов TCP и датаграмм UDP в Wireshark.	2
4.2 Анализ трёхстороннего рукопожатия.	2
4.3 Использование утилит для диагностики соединений	2
Раздел № 5 Передача данных по сети. Сеансовый, представительный и прикладной уровни. Сетевые службы.	
5.1 Анализ handshake-процесса HTTPS на уровне представления	2
5.2 Развертывание и настройка локального DNS-сервера	2
5.3 Настройка DHCP-сервера для автоматической раздачи IP-параметров	2
5.4 Удаленное управление сетевым устройством по протоколу SSH	2
5.5 Установка и настройка веб-сервера	2
Раздел № 6 Основы сетевой безопасности.	
6.1 Создание правил фильтрации трафика	2
6.2 Настройка безопасности портов коммутатора	2
6.3 Настройка VPN-клиента и проверка шифрования трафика	2
6.4 Конфигурация точки доступа	2

Самостоятельное изучение учебного материала (самоподготовка)

Номер раздела данной дисциплины	Наименование тем, вопросов, вынесенных для самостоятельного изучения	Трудоемкость внеаудиторной работы, часы
1	Установка Wireshark	6
2	Установка и настройка PNETLab	6

Номер раздела данной дисциплины	Наименование тем, вопросов, вынесенных для самостоятельного изучения	Трудоемкость внеаудиторной работы, часы
3	Установка и настройка серверной операционной системы	6
4	Установка и настройка VMware Workstation	6
5	Консольные утилиты настройки сетевых компонентов в MS Windows	6
6	Настройка удаленного доступа к компьютеру	6

Лабораторная работа № 1 «Сопоставление сетевых протоколов, устройств и единиц данных уровням модели OSI»

Теоретические сведения

Модель взаимодействия открытых систем (Open Systems Interconnection, OSI) - это эталонная семиуровневая архитектура, разработанная ISO в 1984 году для стандартизации сетевых коммуникаций. Её фундаментальная ценность заключается в:

1 Абстрагировании сложных сетевых процессов через декомпозицию на логические уровни.

2 Обеспечении совместимости продуктов разных производителей.

3 Создании универсальной терминологии для проектирования и диагностики сетей.

4 Разделении ответственности между уровнями с чётко определёнными интерфейсами.

Таблица 1.1 Характеристика уровней модели

Уровень	Наименование	Ключевая функция	Принцип работы	Критерий идентификации
7	Прикладной (Application)	Предоставление сетевых услуг конечным пользователям и приложениям	Интерфейс между сетевыми службами и пользовательскими процессами	Работа с данными в формате, понятном человеку (URL, команды, файлы)
6	Представительный (Presentation)	Преобразование данных между сетевым и прикладным форматами	Шифрование, сжатие, кодирование, преобразование протоколов	Изменение представления данных без изменения их смысла
5	Сеансовый (Session)	Организация и управление диалогом между приложениями	Установление, поддержание, синхронизация и завершение сеансов связи	Управление диалогом (полудуплекс / дуплекс), контроль точек синхронизации
4	Транспортный (Transport)	Гарантированная или негарантированная доставка данных от процесса к процессу	Сегментация, управление потоком, контроль ошибок, мультиплексирование портов	Использование номеров портов, обеспечение end-to-end доставки
3	Сетевой (Network)	Логическая адресация и маршрутизация между различными сетями	Определение оптимальных путей, фрагментация, межсетевое взаимодействие	Работа с логическими адресами (IP-адресация), функционирование между разными средами

Уровень	Наименование	Ключевая функция	Принцип работы	Критерий идентификации
2	Канальный (Data Link)	Организация надежной передачи данных в пределах одной среды передачи	Формирование кадров, физическая адресация, контроль доступа к среде, обнаружение ошибок	Работа с MAC-адресами, обеспечение связи "узел-узел" в одной подсети
1	Физический (Physical)	Передача битовых потоков по физической среде	Кодирование сигналов, передача электрических/оптических/радиосигналов	Работа с физическими характеристиками: разъёмы, кабели, уровни напряжения, модуляция

Каждый уровень оперирует специфическими блоками данных:

1 Данные (Data) — уровни 7-5
2 Сегмент (Segment) — TCP, уровень 4
3 Дейтаграмма (Datagram) — UDP, уровень 4
4 Пакет (Packet) — IP, уровень 3
5 Кадр (Frame) — Ethernet, уровень 2
6 Биты (Bits) — уровень 1

Инкапсуляция в модели OSI — это процесс добавления служебной информации (заголовков и иногда концевиков) к данным на каждом уровне стека протоколов при их движении от верхних уровней к нижним (отправитель) и их удаления при обратном движении (получатель), чтобы обеспечить корректную передачу и обработку информации, где каждый уровень добавляет свою порцию данных, формируя PDU (Protocol Data Unit)

Процесс передачи данных от приложения к сети происходит через последовательную инкапсуляцию:

1 Данные приложения (уровень 7) передаются вниз по стеку.

2 Каждый уровень добавляет свой заголовок (а на уровне 2 также добавляется трейлер).

3 На физическом уровне данные передаются как последовательность битов.

4 На принимающей стороне происходит обратный процесс декапсуляции.

Устройства и их уровень функционирования:

1. Уровень 1 (физический) - работа с сигналами

– Концентратор (Hub). Регенерация и широковещательная передача электрического/оптического сигнала на все порты. Создает общий домен коллизий, делит полосу пропускания. Устарел, заменен коммутаторами.

– Повторитель (Repeater). Усиление сигнала для преодоления ограничений по длине кабеля. Работает на физическом уровне, не анализирует данные.

– Медиаконвертер. Преобразование сигналов между разными средами (медь↔оптика, Ethernet↔Wi-Fi). Прозрачный мост между физическими технологиями.

– Сетевая карта (уровень 1) (NIC). Преобразование битов↔сигналы, кодирование/декодирование. Аппаратный интерфейс между компьютером и средой.

2. Уровень 2 (канальный) - работа с кадрами и mac-адресацией

– Коммутатор (уровень 2) (Switch). Интеллектуальная пересылка кадров на основе MAC-адресов. Построение таблицы MAC-адресов, целевая отправка. Может использовать VLAN, агрегацию каналов (LACP), STP.

– Мост (Bridge). Фильтрация трафика между сетевыми сегментами (2-4 порта). Аналогичен коммутатору, но программная реализация. Исторический предшественник коммутатора.

– Точка доступа Wi-Fi (AP). Организация беспроводной сети. Трансляция между беспроводными и проводными кадрами. Поддерживает режимы: AP, Bridge, Repeater, WDS.

– Сетевая карта (NIC) (уровень 2) – Формирование/анализ кадров, проверка CRC, управление доступом к среде. Адресация по MAC, контроль ошибок. Реализация протоколов ARP, LLDP.

3. Уровень 3 (сетевой) - работа с пакетами и ip-адресацией

– Маршрутизатор (Router). Маршрутизация между разными сетями, определение оптимальных путей. Статика и динамика (RIP, OSPF, BGP), таблицы маршрутизации. Разделяет широковещательные домены, NAT.

– Коммутатор (уровень 3). Высокоскоростная маршрутизация между VLAN внутри одного устройства. Аппаратная маршрутизация (ASIC), маршрутизация на скорости коммутации. "Маршрутизатор в коробке коммутатора".

– Межсетевой экран (уровни 3 и 4). Фильтрация трафика по IP/порт, отслеживание состояния сессий (Stateful). ACL (Access Control Lists), State Table. Базовый уровень сетевой безопасности.

4. Уровни 4-7 (транспортный, сеансовый, представительный, прикладной)

– Балансировщик нагрузки (Load Balancer) (уровень 4, реже уровень 7). Распределение запросов между серверами, отказоустойчивость. Может быть аппаратным (F5)и программным (nginx, HAProxy).

– Прокси-сервер (Proxy). (уровень 7). Посредник между клиентом и сервером, кэширование, фильтрация.

– VPN-шлюз (уровени 2,3,7). Создание зашифрованных туннелей через публичные сети. На разных уровнях может иметь разные реализации: IPsec (уровень 3), SSL-VPN (уровень 7), PPTP/L2TP (уровень 2).

– Шлюз (Gateway) (Все уровни). Преобразование между разными протоколами/сетями.

– IDS/IPS (уровни 4-7).Обнаружение/предотвращение вторжений по сигнатурам.

Задания к лабораторной работе

Для каждого варианта выполнить:

1 Заполнить таблицу сопоставления

2 Ответить на контрольные вопросы

Таблица 1.2 Пример таблицы для отчета

№	Объект анализа	Уровень OSI	Обоснование выбора
1	…	…	…
…	…	…	…

Варианты заданий:

Вариант 1:

Объекты для анализа:

- TCP (протокол управления передачей)
- Концентратор (Hub)
- Сегмент (Segment) как PDU
- Протокол HTTP
- Маршрутизатор (Router)
- Витая пара категории 6
- MAC-адресация
- SSL/TLS шифрование
- IP (Internet Protocol)

Вариант 2:

Объекты для анализа:

- Ethernet (IEEE 802.3)
- Коммутатор L2 (Switch)
- Кадр (Frame) как PDU
- Порт 80 (веб-сервисы)
- Сетевая карта (Network Interface Card)
- Волоконно-оптический кабель
- ARP (Address Resolution Protocol)
- SSH (Secure Shell)
- DHCP (Dynamic Host Configuration)

Вариант 3:

Объекты для анализа:

- Wi-Fi (IEEE 802.11)
- Точка доступа (Access Point)
- Пакет (Packet) как PDU
- DNS (Domain Name System)
- Межсетевой экран (Firewall)

– Радиоволна 2.4 ГГц
– WPA2-шифрование
– Прокси-сервер
– UDP (User Datagram Protocol)

Вариант 4:
Объекты для анализа:
– OSPF (протокол маршрутизации)
– Маршрутизатор L3
– Дейтаграмма (Datagram) как PDU
– FTP (File Transfer Protocol)
– Модем (Modulator-Demodulator)
– Коаксиальный кабель
– VLAN (Virtual LAN)
– VPN (Virtual Private Network)
– ICMP (Internet Control Message Protocol)

Вариант 5:
Объекты для анализа:
– HTTPS
– Брандмауэр уровня приложений
– Заголовок TCP (структура)
– SMTP (Simple Mail Transfer Protocol)
– Коммутатор управляемый
– Разъём RJ-45
– Шлюз (Gateway)
– PPP (Point-to-Point Protocol)
– TCP (Transmission Control Protocol)

Вариант 6:
Объекты для анализа:
– DNS-сервер
– Сетевой мост (Bridge)
– Заголовок IP (структура)
– Telnet
– Повторитель (Repeater)
– Инфракрасный канал
– NAT (Network Address Translation)
– RDP (Remote Desktop Protocol)
– ARP (Address Resolution Protocol)

Вариант 7:
Объекты для анализа:

– BGP (Border Gateway Protocol)
– Load Balancer (балансировщик нагрузки)
– MTU (Maximum Transmission Unit)
– SNMP (Simple Network Management Protocol)
– Патч-панель
– Радиоканал Bluetooth
– QoS (Quality of Service)
– SIP (Session Initiation Protocol)
– HTTP/1.1

Вариант 8:
Объекты для анализа:
– VLAN tagging (802.1Q)
– Гипервизор сетевой
– Jumbo frames
– NTP (Network Time Protocol)
– Медиаконвертер
– Оптический патч-корд
– VXLAN (Virtual Extensible LAN)
– LDAP (Lightweight Directory Access Protocol)
– Ethernet (стандарт IEEE 802.3)

Вариант 9:
Объекты для анализа:
– IGMP (Internet Group Management Protocol)
– Multicast-маршрутизатор
– Широковещательный домен
– TFTP (Trivial File Transfer Protocol)
– Трансивер (Transceiver)
– Электрическая витая пара
– STP (Spanning Tree Protocol)
– VoIP (Voice over IP)
– DNS (Domain Name System)

Вариант 10:
Объекты для анализа:
– SNMP trap
– Контроллер SDN
– Заголовок UDP (структура)
– Syslog
– Пассивный сетевой тестер
– Беспроводной мост
– MPLS (Multiprotocol Label Switching)

– Kerberos
– SSL/TLS (Secure Sockets Layer/Transport Layer Security)

Контрольные вопросы

1 Какой процесс описывает термин «инкапсуляция» и на каком этапе сетевого взаимодействия он происходит

2 Почему коммутатор считается устройством канального уровня, а маршрутизатор — сетевого?

3 Какие функции уровней представления и сеансового реализованы в современных протоколах?

4 Как модель OSI помогает в диагностике сетевых проблем?

5 В чем практическое отличие между сегментом TCP и дейтаграммой UDP с точки зрения модели OSI?

Лабораторная работа № 2 «Знакомство с анализатором трафика Wireshark»

Теоретические сведения

Wireshark — это мощный кроссплатформенный сетевой анализатор трафика с открытым исходным кодом. Программа позволяет:

– Захватывать (сниффить) сетевые пакеты в реальном времени
– Декодировать более 3000 протоколов
– Анализировать сетевой трафик на разных уровнях модели OSI
– Диагностировать сетевые проблемы и уязвимости

Основные компоненты интерфейса Wireshark

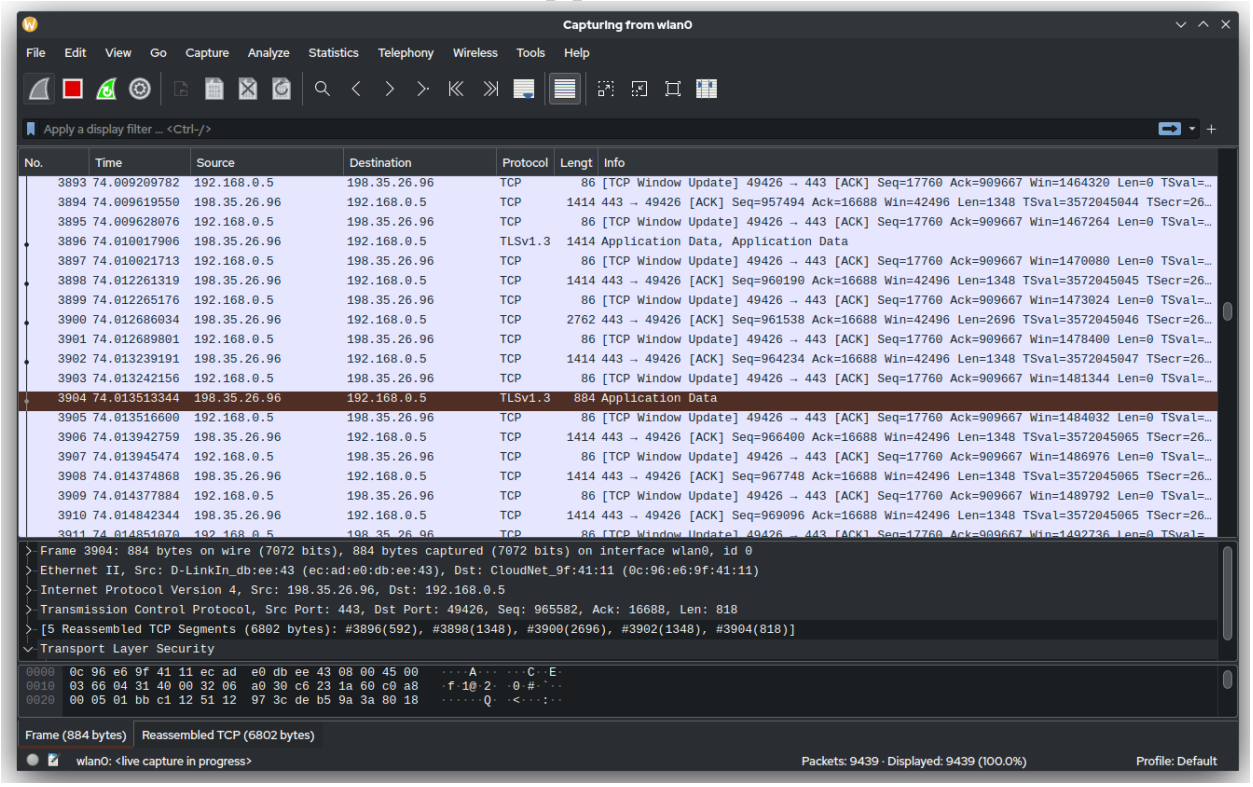

Рисунок 2.1 - Интерфейс Wireshark

Главное окно программы:

– Строка меню. Доступ ко всем функциям: файл, захват, анализ, статистика.

– Панель инструментов. Быстрый доступ к частым операциям: старт/стоп захвата, открытие файла.

– Панель фильтров. Задание фильтров отображения: http, ip.addr=192.168.1.1.

– Список пакетов. Хронологический список захваченных пакетов и выбор пакета для детального анализа.

– Детали пакета. Иерархическое представление заголовков пакета, а ткже анализ на уровне протоколов.

– Байтовое представление. Шестнадцатеричный дамп пакета. Анализ бинарных данных

Ключевые колонки в списке пакетов:

- № — порядковый номер пакета
- Time — временная метка относительно начала захвата
- Source — IP-адрес источника
- Destination — IP-адрес назначения
- Protocol — протокол верхнего уровня
- Length — длина пакета в байтах
- Info — краткая информация о содержимом

Типы фильтров в Wireshark

1. Фильтры захвата (Capture Filters). Применяются ДО захвата пакетов, имеют синтаксис Berkeley Packet Filter (BPF). Примеры:

- host 192.168.1.1 — только трафик с/на указанный хост
- tcp port 80 — только HTTP (80 порт) трафик
- not arp — исключить ARP пакеты

2. Фильтры отображения (Display Filters). Применяются ПОСЛЕ захвата и имеют более гибкий и мощный синтаксис. Примеры:

- ip.addr == 192.168.1.1 — трафик с участием адреса
- tcp.port == 443 — HTTPS трафик
- http.request.method == "GET" — только GET запросы
- dns — только DNS пакеты
- tcp.flags.syn == 1 — пакеты с флагом SYN

Методология анализа сетевого трафика

Правило трёх панелей:

1. Список пакетов — поиск аномалий по времени, адресам, протоколам
2. Детали пакета — анализ конкретного протокола и его полей
3. Байтовое представление — проверка целостности данных

Ключевые индикаторы проблем:

- Красные строки — ошибки протоколов
- Чёрные фоновые строки — повторно передаваемые пакеты
- Необычные протоколы в колонке Protocol
- Резкий рост RTT (Round Trip Time)

Таблица 2.1 Основные сетевые протоколы в Wireshark

Протокол	Уровень OSI	Ключевые поля для анализа	Цвет в Wireshark
Ethernet	L2	Source/Dest MAC, Type	Голубой
ARP	L2/L3	Opcode, Sender/Target IP/MAC	Розовый
IP	L3	Version, TTL, Protocol, Src/Dst IP	Зелёный
TCP	L4	Src/Dst Port, Flags, Seq/Ack Numbers	Светло-голубой
UDP	L4	Src/Dst Port, Length	Фиолетовый
HTTP	L7	Method, URI, Status Code, Headers	Светло-зелёный
DNS	L7	Query/Response, Type, Answer	Тёмно-синий

Задания к лабораторной работе

Общая структура задания для всех вариантов:

1. Подготовительный этап: Установка и настройка Wireshark
2. Захват трафика: Выполнение сетевых операций по сценарию
3. Анализ: Применение фильтров, изучение пакетов
4. Отчет: Ответы на вопросы, скриншоты, выводы

Вариант 1: Анализ DNS-трафика

Сценарий захвата:

1. Очистите кэш DNS (ipconfig /flushdns в Windows)
2. Начните захват трафика в Wireshark
3. Откройте браузер и перейдите на google.com
4. Остановите захват через 10 секунд

Задания для анализа:

– Сколько DNS-запросов было отправлено? Какие типы записей запрашивались?

– Найдите пакет с первым DNS-запросом. Какие поля заголовка IP присутствуют?

– Определите время отклика DNS-сервера (разница между запросом и ответом)

– Примените фильтр dns и экспортируйте все DNS-пакеты в отдельный файл

– Найдите рекурсивный DNS-запрос и объясните его структуру

Контрольные вопросы:

1. Почему DNS использует UDP, а не TCP?
2. Какой порт используется для DNS-запросов?
3. Что означает поле "Transaction ID" в DNS-заголовке?

Вариант 2: Исследование ARP-протокола

Сценарий захвата:

1. Начните захват трафика
2. Выполните команду arp -d * (очистка ARP-кэша)
3. Выполните ping на IP-адрес шлюза по умолчанию
4. Остановите захват

Задания для анализа:

– Найдите ARP-запрос (Request). Какие MAC и IP адреса в нём указаны?

– Найдите ARP-ответ (Reply). Как изменились адреса?

– Определите длину ARP-пакета. Почему именно такая длина?

– Примените фильтр arp и подсчитайте количество ARP-пакетов

– Найдите gratuitous ARP (если есть) и объясните его назначение

Контрольные вопросы:

1. Почему ARP работает на канальном уровне, хотя использует IP-адреса?
2. Какова структура ARP-таблицы в операционной системе?
3. Что такое ARP-spoofing и как его можно обнаружить?

Вариант 3: Анализ HTTP-соединения

Сценарий захвата:

1. Начните захват трафика
2. Откройте браузер в режиме инкогнито
3. Перейдите на http://httpbin.org/get
4. Остановите захват

Задания для анализа:

– Найдите TCP handshake (SYN, SYN-ACK, ACK). Какие порты используются?

– Определите начальные номера последовательности (Sequence numbers)

– Найдите HTTP GET-запрос. Какие заголовки присутствуют?

– Найдите HTTP-ответ. Какой код статуса?

– Проанализируйте процесс завершения TCP-соединения (FIN-пакеты)

Контрольные вопросы:

1. Почему HTTP использует порт 80?
2. Как происходит установление TCP-соединения (three-way handshake)?
3. Что означают TCP-флаги SYN, ACK, FIN?

Вариант 4: Исследование ICMP (ping/traceroute)

Сценарий захвата:

1. Начните захват трафика
2. Выполните ping -n 4 8.8.8.8
3. Выполните tracert 8.8.8.8
4. Остановите захват

Задания для анализа:

– Найдите ICMP Echo Request. Какие поля ICMP присутствуют?

– Найдите соответствующий ICMP Echo Reply. Сравните Identifier и Sequence Number

– Проанализируйте пакеты traceroute. Почему TTL последовательно увеличивается?

– Определите тип ICMP-сообщения для "Time exceeded"

– Рассчитайте среднее время RTT (Round Trip Time)

Контрольные вопросы:

1. Какие типы ICMP-сообщений вы обнаружили?
2. Как работает механизм TTL в IP-пакетах?

3. Почему traceroute показывает разные маршруты для разных провайдеров?

Вариант 5: Сравнение TCP и UDP

Сценарий захвата:

1. Начните захват трафика
2. Выполните nslookup google.com (DNS over UDP)
3. Выполните curl http://httpbin.org/get (HTTP over TCP)
4. Остановите захват

Задания для анализа:

– Найдите DNS-пакет (UDP). Какая длина заголовка UDP?

– Найдите TCP-соединение для HTTP. Сравните заголовки TCP и UDP

– Определите, какой протокол создает больше служебного трафика

– Проанализируйте контрольную сумму UDP. Как она рассчитывается?

– Сравните номера портов для клиентских приложений

Контрольные вопросы:

1. Какие преимущества TCP перед UDP?
2. Когда следует использовать UDP вместо TCP?
3. Почему DNS может использовать и TCP, и UDP?

Вариант 6: Анализ сетевого взаимодействия браузера

Сценарий захвата:

1. Начните захват трафика
2. Откройте новую вкладку в браузере
3. Введите example.com и нажмите Enter
4. Подождите полной загрузки страницы
5. Остановите захват

Задания для анализа:

– Определите все этапы загрузки страницы: DNS, TCP, HTTP, TLS (если есть)

– Найдите TCP handshake для каждого соединения

– Определите, сколько отдельных TCP-соединений было установлено

– Проанализируйте заголовки HTTP Request и Response

– Найдите пакеты с передачей контента (изображения, CSS, JS)

Контрольные вопросы:

1. Почему браузер устанавливает несколько TCP-соединений к одному серверу?
2. Какой контент загружается первым при открытии страницы?
3. Что такое "pipelining" в HTTP/1.1?

Вариант 7: Исследование SSL/TLS handshake

Сценарий захвата:

1. Начните захват трафика
2. Перейдите на https://www.google.com
3. Остановите захват после полной загрузки

Задания для анализа:

– Найдите Client Hello сообщение. Какие шифры поддерживает клиент?
– Найдите Server Hello. Какой шифр выбран сервером?
– Проанализируйте Certificate сообщение. Кто выдал сертификат?
– Найдите Finished сообщение. Что оно подтверждает?
– Определите, используется ли TLS 1.2 или TLS 1.3

Контрольные вопросы:

1. Какие этапы включает TLS handshake?
2. Почему важно проверять сертификаты сервера?
3. Что такое forward secrecy в контексте TLS?

Вариант 8: Анализ широковещательного трафика

Сценарий захвата:

1. Начните захват трафика
2. Подождите 60 секунд без активных действий
3. Остановите захват

Задания для анализа:

– Определите все типы широковещательных пакетов в захвате
– Найдите ARP-запросы. Какие адреса запрашиваются?
– Обнаружьте NetBIOS или LLMNR пакеты (если есть)
– Проанализируйте DHCP-пакеты (если есть обновление аренды)
– Подсчитайте процент широковещательного трафика от общего

Контрольные вопросы:

1. Почему широковещательный трафик важен для работы сети?
2. Какие проблемы может вызвать избыточный широковещательный трафик?
3. Как коммутаторы обрабатывают широковещательные кадры?

Вариант 9: Сравнение IPv4 и IPv6

Сценарий захвата:

1. Убедитесь, что система имеет IPv6-адрес
2. Начните захват трафика
3. Выполните ping -6 google.com (если поддерживается)
4. Выполните ping -4 google.com
5. Остановите захват

Задания для анализа:

– Найдите IPv6-пакеты. Сравните структуру заголовка с IPv4
– Проанализируйте адресацию: какие типы IPv6-адресов используются?
– Сравните ICMPv6 и ICMPv4 сообщения

– Определите, используется ли Neighbor Discovery вместо ARP
– Найдите разницу в TTL (IPv4) и Hop Limit (IPv6)

Контрольные вопросы:

1. Какие преимущества IPv6 перед IPv4?
2. Почему IPv6 не требует NAT?
3. Как работает автоматическая конфигурация адресов в IPv6?

Вариант 10: Диагностика сетевой проблемы

Сценарий захвата:

1. Начните захват трафика
2. Попытайтесь подключиться к несуществующему серверу: telnet 192.0.2.1 80
3. Выполните ping на несуществующий IP в локальной сети
4. Остановите захват

Задания для анализа:

– Найдите TCP SYN-пакет к несуществующему серверу. Что происходит?
– Проанализируйте ICMP-сообщения о недостижимости порта/хоста
– Определите, сколько попыток делает система перед отказом
– Найдите ARP-запросы для несуществующих хостов
– Проанализируйте временные интервалы между повторными попытками

Контрольные вопросы:

1. Какие ICMP-сообщения указывают на разные типы проблем?
2. Как система определяет, что хост недоступен?
3. Что такое "exponential backoff" в TCP?

Лабораторная работа № 3 «Обжим витой пары по стандартам TIA/EIA-568A/B, проверка кабельным тестером»

Теоретические сведения

Витая пара (Twisted Pair) — самый распространенный тип кабеля для локальных сетей, состоящий из одной или нескольких пар изолированных проводников, скрученных между собой с определенным шагом. Скручивание уменьшает электромагнитные помехи и перекрестные наводки.

Таблица 3.1 Классификация витой пары

Категория	Частота, МГц	Скорость передачи	Применение
Cat 5	100	до 100 Мбит/с	Устаревшие сети
Cat 5e	100	до 1 Гбит/с	Базовые сети (самая распространенная)
Cat 6	250	до 10 Гбит/с (до 55 м)	Современные офисы
Cat 6a	500	до 10 Гбит/с (до 100 м)	ЦОД, высокоскоростные сети
Cat 7	600	до 10 Гбит/с	Специализированные приложения

Также существует разделение в зависимости от конструктивных особенностей:

– UTP (Unshielded) — неэкранированная витая пара (наиболее распространена)

– FTP (Foiled) — с общим экраном из фольги

– STP (Shielded) — с экранированием каждой пары

– S/FTP — с экранированием каждой пары и общим экраном

Стандарт TIA/EIA-568 определяет порядок расположения проводников в 8P8C-разъемах (RJ-45) для обеспечения совместимости и правильной работы сетей Ethernet. Он также подразделяется на стандарты 568A и 568B

Таблица 3.2 Сравнение стандартов 568A и 568B

Контакт RJ-45	Цвет по 568A	Цвет по 568B	Назначение (100BASE-TX)
1	Бело-зеленый	Бело-	TX+ (Передача +)

Контакт RJ-45	Цвет по 568A	Цвет по 568B	Назначение (100BASE-TX)
		оранжевый	
2	Зеленый	Оранжевый	TX- (Передача -)
3	Бело-оранжевый	Бело-зеленый	RX+ (Прием +)
4	Синий	Синий	Не используется*
5	Бело-синий	Бело-синий	Не используется*
6	Оранжевый	Зеленый	RX- (Прием -)
7	Бело-коричневый	Бело-коричневый	Не используется*
8	Коричневый	Коричневый	Не используется*

*Для Gigabit Ethernet (1000BASE-T) используются ВСЕ 4 пары

Типы кабелей по назначению:

1. Прямой (Straight-through) кабель:

Оба конца обжаты по одному стандарту (оба 568A или оба 568B)

Применение: Соединение разнородных устройств

Примеры: Компьютер ↔ Коммутатор, Коммутатор ↔ Маршрутизатор

2. Перекрестный (Crossover) кабель:

Один конец — 568A, другой — 568B

Применение: Соединение однородных устройств

Примеры: Компьютер ↔ Компьютер, Коммутатор ↔ Коммутатор, Маршрутизатор ↔ Маршрутизатор

3. Консольный кабель (Rollover):

Полная инверсия пар (1↔8, 2↔7, 3↔6, 4↔5)

Применение: Подключение к консольному порту сетевого оборудования

Важно: Современное оборудование с поддержкой Auto-MDIX автоматически определяет тип кабеля, но понимание различий обязательно для диагностики!

Также при работе обжиме требуется соблюдать правила монтажа и безопасности:

1. Технические требования:

– Максимальная длина сегмента: 100 метров (90 м постоянная линия + 10 м патч-корды).

– Минимальный радиус изгиба: 4× внешнего диаметра кабеля.

– Удаленность от источников помех: не менее 30 см от силовых кабелей.
– Температурный режим: от 0°C до +60°C при эксплуатации.
2. Электрическая безопасность:
– Работа с обесточенным оборудованием.
– Проверка отсутствия напряжения на кабелях.
– Использование изолированного инструмента.
3. Производственная безопасность:
– Защита глаз от обрезков проволоки.
– Использование перчаток при работе с металлическими элементами.
– Правильное хранение инструмента.

Задания к лабораторной работе

Задание 1: Изготовление прямого кабеля (Straight-through) по стандарту 568B

Последовательность действий:

1. Подготовка кабеля:
– Отрежьте ровный отрезок кабеля длиной 1 метр
– Наденьте защитный колпачок на кабель (со стороны будущего разъема)
– С помощью стриппера снимите внешнюю изоляцию на 20-25 мм
– ВАЖНО: Не повредите изоляцию внутренних проводников!
2. Раскладка проводников:
– Расплетите пары до длины 12-15 мм
– Расправьте проводники и расположите их в следующем порядке (568B):

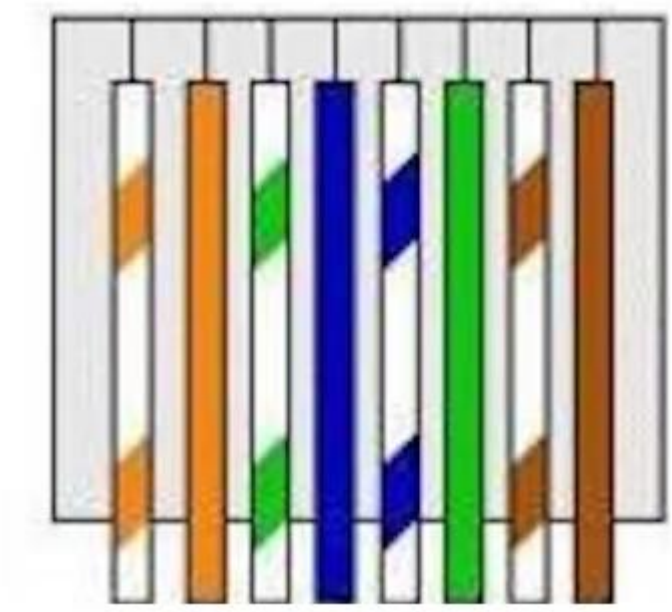

Рисунок 3.1 - TIA/EIA-568B

1. Бело-оранжевый
2. Оранжевый
3. Бело-зеленый
4. Синий
5. Бело-синий
6. Зеленый
7. Бело-коричневый
8. Коричневый

– Выровняйте концы проводников, обрежьте их до длины 12-13 мм
– Концы должны быть ровными и находиться на одном уровне

3. Обжим разъема:

– Вставьте проводники в разъем RJ-45 до упора
– Убедитесь, что внешняя изоляция заходит в разъем на 5-6 мм, все проводники дошли до конца контактов, порядок проводников не нарушен
– Вставьте разъем в соответствующее гнездо кримпера
– Плавно, но сильно сожмите рукоятки до характерного щелчка

4. Повторите операцию для второго конца кабеля, используя ТОТ ЖЕ стандарт 568B

Задание 2: Изготовление перекрестного кабеля (Crossover)

1. Изготовьте первый конец кабеля по стандарту 568B (как в задании 1)
2. Изготовьте второй конец кабеля по стандарту 568A:

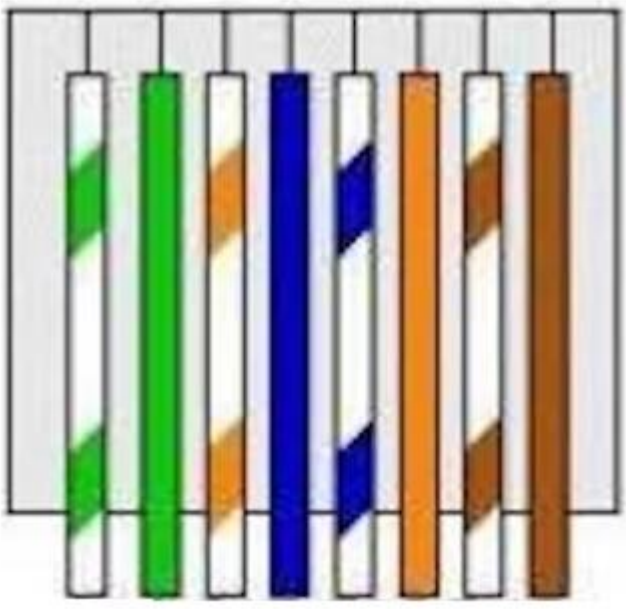

Рисунок 3.1 - TIA/EIA-568A

1. Бело-зеленый

2. Зеленый
3. Бело-оранжевый
4. Синий
5. Бело-синий
6. Оранжевый
7. Бело-коричневый
8. Коричневый

Задание 3: Проверка кабелей тестером

1. Подготовка тестера:
– Установите батареи (если требуется)
– Подключите передатчик (master) к одному концу кабеля
– Подключите приемник (remote) к другому концу
2. Проверка прямого кабеля (568B ↔ 568B):
– Включите тестер
– Наблюдайте последовательное загорание светодиодов 1→2→3→4→5→6→7→8→G
– Правильный результат: Светодиоды загораются попарно в одинаковой последовательности на обоих модулях
3. Проверка перекрестного кабеля (568B ↔ 568A):

Ожидаемая последовательность:
– Передатчик (568B): 1-2-3-4-5-6-7-8
– Приемник (568A): 3-6-1-4-5-2-7-8

Контрольные вопросы

1. В чем различие между стандартами TIA/EIA-568A и 568B?
2. Для чего нужен перекрестный кабель? Приведите 3 примера использования.
3. Какие инструменты необходимы для обжима витой пары?
4. Как определить обрыв провода с помощью кабельного тестера?
5. Почему при обжиме важно, чтобы внешняя изоляция заходила в разъем?

Лабораторная работа № 4 «Изучение MAC-адресов сетевых интерфейсов и таблицы коммутатора»

Теоретические сведения

MAC-адрес (Media Access Control Address) — это уникальный 48-битный (6-байтный) идентификатор сетевого интерфейса, записанный в его ПЗУ (ROM). Это "физический" адрес устройства на канальном уровне модели OSI.

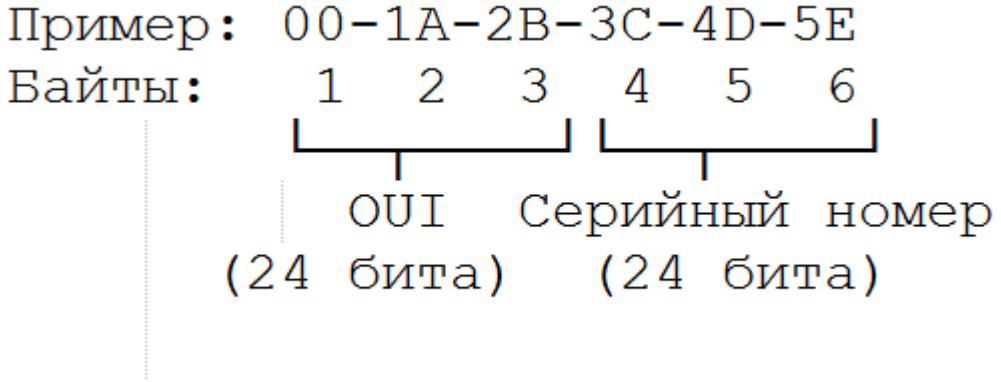

Рисунок 4.1 - Структура MAC-адреса

Первые 3 байта это OUI (Organizationally Unique Identifier) присваиваются IEEE производителям оборудования, например: Cisco (00-00-0C), Intel (00-90-27), Apple (00-03-93). По OUI можно определить производителя устройства

Последние 3 байта это уникальный серийный номер он назначается производителем и гарантирует уникальность в сочетании с OUI.

Также существуют специальные MAC-адреса:

– Широковещательный: FF-FF-FF-FF-FF-FF (все устройства в сети)
– Мультикаст IPv4: 01-00-5E-00-00-00 до 01-00-5E-7F-FF-FF
– STP (Spanning Tree): 01-80-C2-00-00-00

Коммутатор (Switch) — устройство канального уровня, которое принимает решения о пересылке кадров на основе MAC-адресов.

Его ключевыми функциями являются:

1. Обучение (Learning):
– Коммутатор анализирует исходный MAC-адрес входящих кадров
– Создает/обновляет таблицу соответствия: MAC-адрес → порт
– Пример: Кадр от MAC A пришел на порт 1 → запись: A → порт 1
2. Пересылка (Forwarding):
– Анализ MAC-адреса назначения
– Если адрес известен (есть в таблице) → отправка только на нужный порт
– Если адрес неизвестен → флуд (flooding) на все порты, кроме источника
– Широковещательный адрес → флуд на все порты, кроме источника

3. Фильтрация (Filtering):

– Не пересылает кадры обратно на порт-источник

– Изоляция доменов коллизий

Команды для работы с MAC-адресами в различных ОС:

1. Windows:

ipconfig /all *# Основная информация, включая MAC*
getmac /v *# Детальная информация о MAC-адресах*
arp –a *# ARP таблица (соответствие IP→MAC)*
netsh interface show interface *# Список интерфейсов*

2. Linux:

ifconfig –a *# Информация о сетевых интерфейсах*
ip link show *# Современная альтернатива ifconfig*
cat /sys/class/net//address* *# Только MAC-адреса*
arp –n *# ARP таблица*

3. macOS:

ifconfig *# Информация о сетевых интерфейсах*
networksetup –listallhardwareports *# Список оборудования*
arp –a *# ARP таблица*

КАК РАБОТАТЬ В PNETLab

Шаг 1: Добавление устройств

– На панели слева выберите устройство

– Кликните на рабочую область

– Повторите для всех устройств

Шаг 2: Соединение устройств

– Нажмите на иконку кабеля

– Кликните на первое устройство → выберите порт

– Кликните на второе устройство → выберите порт

Шаг 3: Включение устройств

– Нажмите кнопку "Start" на каждом устройстве

– Ждите, пока загорится зеленый свет

Шаг 4: Настройка компьютеров

– Кликните на компьютер

– Вкладка "Desktop" → "IP Configuration"

– Введите IP-адрес и маску

Задания к лабораторной работе

Задание 1:

1. С помощью команд ОС определите MAC-адреса всех сетевых интерфейсов вашего компьютера.

2. Для каждого MAC-адреса определите производителя сетевой карты.

Задание 2:

1. Запустите PNETLab и создайте новый проект
2. Добавьте на рабочую область:

– 1 коммутатор (Cisco 2960)
– компьютера

3. Соедините устройства кабелями
4. Включите все устройства
5. На компьютерах настройте IP-адреса:

– PC1: 192.168.1.10/24
– PC2: 192.168.1.20/24

6. Проверьте связь: PC1 → ping PC2

Задание 3:

Узнайте MAC-адреса компьютеров:

1. В PNETLab кликните на компьютер
2. Перейдите на вкладку "Desktop"
3. Откройте "Command Prompt"
4. Введите: *ipconfig /all* (Windows) или *ifconfig* (Linux)
5. Найдите строку "Physical Address" или "HWaddr"

Задание 4:

1. На коммутаторе введите:

– enable
– show mac address-table

2. Если таблица пустая выполните:

– С PC1: ping на PC2
– Снова проверьте таблицу MAC
– С PC2: ping на PC1
– Проверьте таблицу MAC еще раз

3. Если таблица заполнена подождите 5 минут (в реальности, в PNETLab можно ускорить) и снова проверьте таблицу MAC.

Контрольные вопросы

1. Что делает команда ping?
2. Что такое MAC-адрес и зачем он нужен?
3. Почему не все MAC-адреса на коммутаторе видны сразу?
4. Что такое широковещательный адрес и как он выглядит?
5. Почему коммутатору нужна таблица MAC-адресов?

Лабораторная работа № 5 «Разделение одной физической сети на несколько логических (VLAN) для изоляции трафика»

Теоретические сведения

VLAN (Virtual Local Area Network) — это технология работающая на канальном уровне модели OSI, которая позволяет разделить одну физическую сеть на несколько логических (виртуальных) сетей. Она создает независимые широковещательные домены в рамках одной физической инфраструктуры.

Представьте большой офис (одна физическая сеть). С помощью перегородок (VLAN) вы создаете отдельные комнаты:

- Бухгалтерия (VLAN 10)
- Отдел продаж (VLAN 20)
- IT-отдел (VLAN 30)

Использование VLAN позволяет, разделять хосты на логические группы (сервера, пользователи, оборудование), изолировать трафик, локализовать проблемы, легче управлять группами.

Технический принцип: Коммутатор добавляет VLAN ID (12-битный тег, значения 1-4094) к заголовку кадра Ethernet при передаче между коммутаторами. Этот тег определяет принадлежность кадра к определенному VLAN.

Типы портов и их функции:

1. Access Port (Порт доступа). Используется для подключение конечных устройств (компьютеров, принтеров, IP-телефонов). Принимает нетегированные кадры от устройства, добавляет VLAN тег при передаче внутрь коммутатора и удаляет VLAN тег при отправке кадра на устройство.
2. Trunk Port (Магистральный порт) соединяет коммутаторы между собой. Передает тегированные кадры, при этом может переносить трафик нескольких VLAN одновременно.
3. Особый случай: Voice VLAN. Поддержка IP-телефонии. Один физический порт обслуживает два VLAN:

- Данные (Data VLAN) — для компьютера
- Голос (Voice VLAN) — для IP-телефона

КАК РАБОТАТЬ С VLAN В PNETLab

Базовые команды для VLAN:

1. Создание VLAN:

```
configure terminal          # войти в режим настройки
vlan 10                     # создать VLAN 10
name Accounting             # дать имя
exit                        # выйти
```

2. Настройка порта как access:

```
interface fastEthernet 0/1          # выбрать порт 1
```

switchport mode access *# режим access*
switchport access vlan 10 *# назначить VLAN 10*
no shutdown *# включить порт*
exit *# выйти*

3. Настройка порта как trunk:

interface fastEthernet 0/24 *# выбрать порт 24*
switchport mode trunk *# режим trunk*
switchport trunk allowed vlan 10,20 *# разрешить VLAN*
no shutdown *# включить порт*
exit *# выйти*

4. Посмотреть все VLAN:

show vlan brief

5. Посмотреть настройку порта:

show interface fastEthernet 0/1 switchport

6. Посмотреть текущую конфигурацию:

show running-config

Задания к лабораторной работе

Задание 1:

Создайте две отдельные группы компьютеров в одной физической сети.

1. Создайте сеть: 1 коммутатор, 4 компьютера
2. На коммутаторе создайте VLAN 10 и VLAN 20:

configure terminal
vlan 10
name Accounting
exit
vlan 20
name Sales
exit

3. Настройте порты:

Порт 1-2 → VLAN 10 (компьютеры 1-2)
Порт 3-4 → VLAN 20 (компьютеры 3-4)
interface range fastEthernet 0/1-2
switchport mode access
switchport access vlan 10
no shutdown
exit

4. Настройте IP-адреса:

PC1-2: 192.168.10.x (VLAN 10)
PC3-4: 192.168.20.x (VLAN 20)

5. Проверка:

PC1 → ping PC2 ✓ (работает)

PC1 → ping PC3 ✗ (не работает)
PC3 → ping PC4 ✓ (работает)

Задание 2:
Соедините два коммутатора так, чтобы VLAN проходили между ними.
1. Создайте VLAN 10 и 20 на обоих коммутаторах
2. Настройте access порты для компьютеров

Switch1
Порт 1 → VLAN 10 (PC1)
Порт 2 → VLAN 20 (PC3)
Switch2
Порт 1 → VLAN 10 (PC2)
Порт 2 → VLAN 20 (PC4)

3. Настройте trunk между коммутаторами:

interface fastEthernet 0/24
switchport mode trunk
switchport trunk allowed vlan 10,20
no shutdown

4. Проверка:

PC1 (Switch1) → ping PC2 (Switch2) ✓ (работает)
PC3 (Switch1) → ping PC4 (Switch2) ✓ (работает)
PC1 → ping PC3 ✗ (не работает)

Контрольные вопросы

1. Что такое VLAN?
2. Могут ли компьютеры из разных VLAN общаться?
3. Какая команда показывает все VLAN?
4. Что такое trunk порт?
5. Зачем изолировать трафик?

Лабораторная работа № 6 «Работа с масками переменной длины.»

Теоретические сведения

IP-адрес (Internet Protocol Address) — уникальный числовой идентификатор устройства в сети. Это как «почтовый адрес» для компьютера в сети.

Существует две версии:

– IPv4 содержащий 32 бита (4 байта), например: 192.168.1.1

– IPv6 содержащий 128 бит (16 байт), например: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Маска подсети определяет, какая часть IP-адреса относится к сети, а какая — к устройству.

Пример классической маски:

IP-адрес: 192.168.1.1

Маска: 255.255.255.0

Результат: Сеть: 192.168.1.0, Устройство: .1

Зачем нужны маски переменной длины?

Раньше сети делили на 3 размера:

Большие (A) (16 млн устройств) — слишком много

Средние (B) (65 тыс устройств) — часто много

Маленькие (C) (254 устройства) — часто мало

У вас магазин с 10 компьютерами. По старым правилам вы получали сеть на 254 устройства. 244 адреса пропадают зря. Маски переменной длины позволяют создавать сети любого размера.

Существует две формы записи маски:

1. Старая форма: 255.255.255.0
2. Новая форма (CIDR): /24

Всего в IP-адресе 32 бита

/24 значит: 24 бита для сети, 8 бит для устройств

/24 = 255.255.255.0 = 11111111.11111111.11111111.00000000

Сетевая маска	Инверсия	Префикс	Используется	Размер
0.0.0.0	255.255.255.255	/0	4,294,967,294	весь интернет
128.0.0.0	127.255.255.255	/1	2,147,483,646	128 классов ‘a’
192.0.0.0	63.255.255.255	/2	1,073,741,822	64 класса ‘a’
224.0.0.0	31.255.255.255	/3	536,870,910	32 класса ‘a’
240.0.0.0	15.255.255.255	/4	268,435,454	16 классов ‘a’
248.0.0.0	7.255.255.255	/5	134,217,726	8 классов ‘a’
252.0.0.0	3.255.255.255	/6	67,108,862	4 класса ‘a’
254.0.0.0	1.255.255.255	/7	33,554,430	2 класса ‘a’
255.0.0.0	0.255.255.255	/8	16,777,214	1 класс ‘a’
255.128.0.0	0.127.255.255	/9	8,388,606	128 классов ‘b’
255.192.0.0	0.63.255.255	/10	4,194,302	64 класса ‘b’
255.224.0.0	0.31.255.255	/11	2,097,150	32 класса ‘b’
255.240.0.0	0.15.255.255	/12	1,048,574	16 классов ‘b’
255.248.0.0	0.7.255.255	/13	524,286	8 классов ‘b’
255.252.0.0	0.3.255.255	/14	262,142	4 класса ‘b’
255.254.0.0	0.1.255.255	/15	131,07	2 класса ‘b’
255.255.0.0	0.0.255.255	/16	65,534	1 класс ‘b’
255.255.128.0	0.0.127.255	/17	32,766	128 классов ‘c’
255.255.192.0	0.0.63.255	/18	16,382	64 класса ‘c’
255.255.224.0	0.0.31.255	/19	8,19	32 класса ‘c’
255.255.240.0	0.0.15.255	/20	4,094	16 классов ‘c’
255.255.248.0	0.0.7.255	/21	2,046	8 классов ‘c’
255.255.252.0	0.0.3.255	/22	1,022	4 класса ‘c’
255.255.254.0	0.0.1.255	/23	510	2 классов ‘c’
255.255.255.0	0.0.0.255	/24	254	1 класс ‘c’
255.255.255.128	0.0.0.127	/25	126	128 хостов
255.255.255.192	0.0.0.63	/26	62	64 хоста
255.255.255.224	0.0.0.31	/27	30	32 хоста
255.255.255.240	0.0.0.15	/28	14	16 хостов
255.255.255.248	0.0.0.7	/29	6	8 хостов
255.255.255.252	0.0.0.3	/30	2	4 хоста
255.255.255.254	0.0.0.1	/31	0	2 хоста
255.255.255.255	0.0.0.0	/32	1	1 хост

Рисунко 6.1 – Таблица соответствий

Простой расчет количества устройств
Формула: *2^(32 - n) - 2*
Где n — число после /
Примеры:
/24: 2^(8) - 2 = 256 - 2 = 254 устройства
/25: 2^(7) - 2 = 128 - 2 = 126 устройств
/26: 2^(6) - 2 = 64 - 2 = 62 устройства
Почему минус 2:

- Один адрес — адрес сети (например, 192.168.1.0)
- Один адрес — широковещательный (например, 192.168.1.255)

Эти адреса нельзя давать устройствам!

Как определить границы сети:
Дано: 192.168.1.64/26

1. Расчет:

Шаг 1: Определяем размер блока

/26 → 32-26=6 бит на устройства

2^6 = 64 адреса в блоке

Шаг 2: Находим границы

Адрес сети: 192.168.1.64 (первый адрес)

Широковещательный: 192.168.1.127 (последний адрес)

Устройства могут быть: 192.168.1.65 — 192.168.1.126

2. Простой метод:

Запомнить "магические числа": 128, 192, 224, 240, 248, 252

Для /26 → 192 в последнем октете

256 - 192 = 64 (шаг сетей)

Сети: .0, .64, .128, .192

VLSM (Variable Length Subnet Mask) — создание сетей РАЗНОГО размера в одной большой сети.

Пример задачи:

У вас сеть 192.168.1.0/24 (254 устройства). Нужно создать:

- Отдел А: 100 компьютеров
- Отдел Б: 50 компьютеров
- Связь между маршрутизаторами: 2 устройства

Решение:

1. Отдел А (100 устройств):
- Нужно: 100+2=102 адреса
- Ближайшая степень двойки: 128
- Маска: 32-7=25 → /25
- Подсеть: 192.168.1.0/25 (диапазон: .1-.126)
2. Отдел Б (50 устройств):
- Нужно: 50+2=52 адреса
- Ближайшая степень двойки: 64
- Маска: 32-6=26 → /26
- Следующая свободная подсеть: 192.168.1.128/26 (диапазон: .129-.190)
3. Связь (2 устройства):
- Используем /30
- Следующая свободная: 192.168.1.192/30 (диапазон: .193-.194)

<u>Правила, которые нельзя нарушать!!!:</u>

1. Всегда начинай с самых больших сетей
2. Сети не должны пересекаться

Плохо: Сеть А (.0-.127) и Сеть Б (.64-.191) — пересекаются!

Хорошо: Сеть А (.0-.127) и Сеть Б (.128-.255)

3. Два специальных адреса в каждой сети:

Адрес сети (первый) — нельзя для устройств

Широковещательный (последний) — нельзя для устройств

Задания к лабораторной работе

Задание 1:
Разбейте сеть 192.168.1.0/24 на 4 равные подсети.
Шаги:
1. Определите новую маску:
Было: /24 (255.255.255.0)
2. Рассчитайте подсети:
Подсеть 1: 192.168.1.*/*
Подсеть 2: 192.168.1.*/*
Подсеть 3: 192.168.1.*/*
Подсеть 4: 192.168.1.*/*
3. Для каждой подсети определите:
Адрес сети
Первый доступный адрес
Последний доступный адрес
Широковещательный адрес

Задание 2:
Для сети 10.0.0.0/24 создайте подсети для:
- Отдел А: 60 хостов
- Отдел В: 30 хостов
- Связь между маршрутизаторами: 2 хоста

Контрольные вопросы

Чем отличается адресация IPv6 от IPv4?
Как определить подсеть по IP и маске?
Почему устройства в разных подсетях не могут общаться напрямую?
Почему из максимального числа хостов подсети вычитается 2?
Какая самая широкая маска?

Лабораторная работа № 7 «Настройка IPv4-адресов на компьютерах и маршрутизаторах в симуляторе»

Теоретические сведения

IPv4-адрес — это как «номер телефона» для компьютера в сети. Без него компьютер не может общаться с другими устройствами.

Формат IPv4 это 4 числа от 0 до 255 разделены точками. Примеры правильных адресов:

- 10.0.0.1
- 172.16.0.100
- 192.168.100.50

Кроме IP также обычно настраиваются:

1. Маска подсети:
- Определяет, кто в одной сети с вами
- Чаще всего: 255.255.255.0
- Пример: Если маска 255.255.255.0, то компьютеры 192.168.1.1 и 192.168.1.2 в одной сети

2. Шлюз по умолчанию:
- «Выход» из вашей сети
- Обычно это адрес маршрутизатора
- Пример: 192.168.1.1

3. DNS-сервер:
- Переводчик имен (например, google.com → 142.250.185.14)
- Можно использовать 8.8.8.8 (Google DNS) или 77.88.8.8 (Яндекс DNS)

Основные правила настройки:

Правило 1: Все компьютеры в одной сети должны иметь:

- Одинаковую маску подсети
- Разные IP-адреса
- Одинаковый шлюз (если есть)

Правило 2: Адреса, которые НЕЛЬЗЯ использовать:

- Первый адрес в сети (например, 192.168.1.0)
- Последний адрес в сети (например, 192.168.1.255)
- Адрес шлюза (например, 192.168.1.1) — уже занят!

Пример правильной настройки для сети 192.168.1.0/24:

Маршрутизатор (шлюз): 192.168.1.1
Компьютер 1: 192.168.1.10
Компьютер 2: 192.168.1.11
Компьютер 3: 192.168.1.12
Маска у всех: 255.255.255.0
Шлюз у всех: 192.168.1.1

Порядок работы в PNETLab:

1. Настройка компьютера:

– Шаг 1: Кликните на компьютер в PNETLab
– Шаг 2: Перейдите на вкладку "Desktop"
– Шаг 3: Выберите "IP Configuration"
– Шаг 4: Заполните:

IP Address: *192.168.1.10*
Subnet Mask: *255.255.255.0*
Default Gateway: *192.168.1.1*
DNS Server: *8.8.8.8*

– Шаг 5: Нажмите "FastEthernet0" чтобы применить

2. Настройка маршрутизатора:
– Шаг 1: Кликните на маршрутизатор
– Шаг 2: Перейдите на вкладку "CLI" (командная строка)
– Шаг 3: Введите команды:

```
enable                          # войти в режим настройки
configure terminal              # начать настройку
interface GigabitEthernet0/0    # выбрать интерфейс
ip address 192.168.1.1 255.255.255.0 # настроить IP
no shutdown                     # включить интерфейс
exit                            # выйти
```

3. Проверка настройки на компьютере:
– Откройте "Command Prompt"
– Введите: ping 192.168.1.1
– Если видите "Reply" — всё работает.
4. Проверка настройки на маршрутизаторе:

show ip interface brief *# посмотреть все IP*
ping 192.168.1.10 *# проверить связь с компьютером*

Задания к лабораторной работе

Задание 1: Настройте сеть с маршрутизатором.
1. Настройка:
– Маршрутизатор: 192.168.1.1/24
– Компьютер: 192.168.1.10/24, шлюз = 192.168.1.1
2. Проверка:
– Компьютер → ping 192.168.1.1
– Маршрутизатор → ping 192.168.1.10

Зачем компьютеру шлюз?
Сколько интерфейсов у маршрутизатора?
Что делает команда no shutdown?

Задание 2: Настройте сеть, где 2 компьютера общаются через маршрутизатор.
1. Настройка:

- Маршрутизатор интерфейс 1: 192.168.1.1/24
- Маршрутизатор интерфейс 2: 192.168.2.1/24
- Компьютер 1: 192.168.1.10/24, шлюз 192.168.1.1
- Компьютер 2: 192.168.2.10/24, шлюз 192.168.2.1

2. Проверка:
- PC1 → ping 192.168.1.1 (работает)
- PC2 → ping 192.168.2.1 (работает)
- PC1 → ping 192.168.2.10 (не работает без маршрутизации)

Контрольные вопросы

1. Что будет, если поставить одинаковые IP?
2. Зачем компьютеру шлюз?
3. Что делает команда no shutdown?
4. Зачем маршрутизатору несколько IP-адресов?
5. Что делает команда show ip interface brief?

Лабораторная работа № 8 «Конфигурация статических маршрутов на нескольких маршрутизаторах»

Теоретические сведения

Протоколы маршрутизации - это правила, по которым осуществляется обмен информации о путях передачи пакетов между маршрутизаторами. Протоколы характеризуются временем сходимости, потерями и масштабируемостью. В настоящее время используется несколько протоколов маршрутизации.

Одна из главных задач маршрутизатора состоит в определении наилучшего пути к заданному адресату. Маршрутизатор определяет пути (маршруты) к адресатам или из статической конфигурации, введённой администратором, или динамически на основании маршрутной информации, полученной от других маршрутизаторов. Маршрутизаторы обмениваются маршрутной информацией с помощью протоколов маршрутизации.

Маршрутизатор хранит таблицы маршрутов в оперативной памяти. Таблица маршрутов это список наилучших известных доступных маршрутов. Маршрутизатор использует эту таблицу для принятия решения куда направлять пакет.

В случае статической маршрутизации администратор вручную определяет маршруты к сетям назначения.

В случае динамической маршрутизации – маршрутизаторы следуют правилам, определяемым протоколами маршрутизации для обмена информацией о маршрутах и выбора лучшего пути.

Статические маршруты не меняются самим маршрутизатором. Динамические маршруты изменяются самим маршрутизатором автоматически при получении информации о смене маршрутов от соседних маршрутизаторов. Статическая маршрутизация потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Для настройки маршрута используется команда *ip route [СЕТЬ] [МАСКА] [КУДА]*

Где [КУДА]:

- IP-адрес next-hop: 192.168.1.2
- Имя интерфейса: GigabitEthernet0/0

Next-hop (следующий прыжок) это IP-адрес следующего маршрутизатора на пути к цели.

Для проверки настроек можно использовать команду *show ip route* которая покажет все настроенные маршруты.

Пошаговая настройка:

- Шаг 1: Настройте IP-адреса на всех интерфейсах
- Шаг 2: Проверьте, что соседние маршрутизаторы пингуются.

– Шаг 3: Добавьте статические маршруты
– Шаг 4: Проверьте таблицу маршрутизации

Задания к лабораторной работе

Проведем настройку статической маршрутизации с помощью PNETLab.

Создайте схему сети, представленную на рисунке 8.1

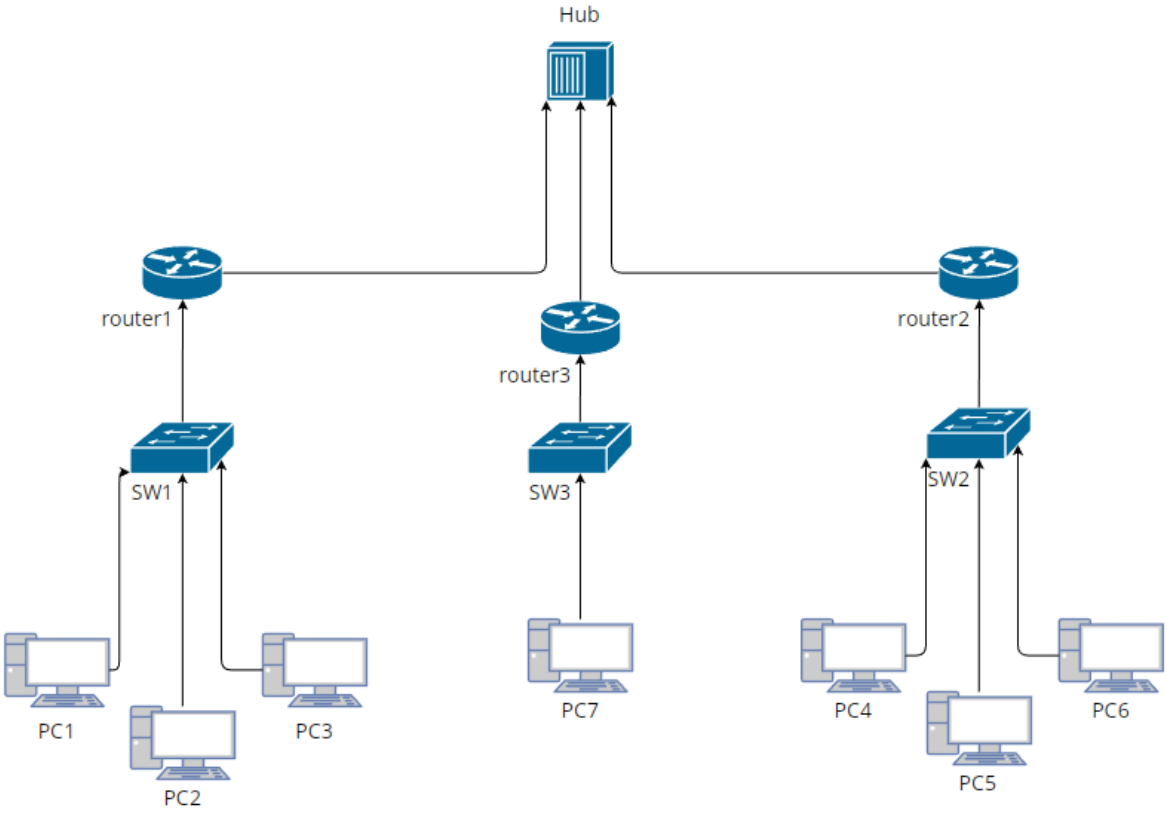

Рисунок 8.1 – Схема сети

На данной схеме представлена корпоративная сеть, состоящая из следующих компонентов:

1. Сеть 1 – на SW1 замыкается сеть первой организации (таблица 5.1):

Таблица 5.1. Сеть первой организации.

Компьютер	IP адрес
PC1	192.168.1.2/24
PC2	192.168.1.3/24
PC3	192.168.1.4/24

Шлюз в сети – 192.168.1.1/24.

2. Сеть 2 – на SW2 замыкается сеть второй организации (таблица 5.2):

Таблица 5.2. Сеть второй организации.

Компьютер	IP адрес
PC4	10.0.0.5/8
PC5	10.0.0.6/8
PC6	10.0.0.7/8

Шлюз в сети – 10.0.0.1/8.

3. Сеть 3 – на Hub замыкается сеть 200.200.200.0/24.

4. Сеть 4 – маршрутизатор Router3 выводит сеть в интернет через коммутатор SW3 (сеть 210.210.210.0/24). На PC7 IPадрес 210.210.210.8/24, шлюз 210.210.210.3/24.

Маршрутизаторы имеют по два интерфейса:

Router1 – 192.168.1.1/24 и 200.200.200.1/24.

Router2 – 10.0.0.1/8и 200.200.200.2/24.

Router3 – 210.210.210.3/24 и 200.200.200.3/24.

Задача:

1. Настроить сети организаций.
2. Настроить статические таблицы маршрутизации на роутерах.
3. Проверить работу сети – на каждом из компьютеров.

Контрольные вопросы

1. Что такое статическая маршрутизация и чем она отличается от динамической?
2. В каких случаях рекомендуется использовать статические маршруты?
3. Какая команда используется для добавления статического маршрута на маршрутизаторе Cisco?
4. Адрес чего использовать в next-hop?
5. Почему next-hop не может быть своим адресом?

Лабораторная работа № 9 «Наблюдение за автоматическим построением таблиц маршрутизации»

Теоретические сведения

Протоколы маршрутизации - это правила, по которым осуществляется обмен информации о путях передачи пакетов между маршрутизаторами. Протоколы характеризуются временем сходимости, потерями и масштабируемостью. В настоящее время используется несколько протоколов маршрутизации.

Одна из главных задач маршрутизатора состоит в определении наилучшего пути к заданному адресату. Маршрутизатор определяет пути (маршруты) к адресатам или из статической конфигурации, введённой администратором, или динамически на основании маршрутной информации, полученной от других маршрутизаторов. Маршрутизаторы обмениваются маршрутной информацией с помощью протоколов маршрутизации.

Маршрутизатор хранит таблицы маршрутов в оперативной памяти. Таблица маршрутов это список наилучших известных доступных маршрутов. Маршрутизатор использует эту таблицу для принятия решения куда направлять пакет.

В случае статической маршрутизации администратор вручную определяет маршруты к сетям назначения.

В случае динамической маршрутизации – маршрутизаторы следуют правилам, определяемым протоколами маршрутизации для обмена информацией о маршрутах и выбора лучшего пути.

Статические маршруты не меняются самим маршрутизатором. Динамические маршруты изменяются самим маршрутизатором автоматически при получении информации о смене маршрутов от соседних маршрутизаторов. Статическая маршрутизация потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Задания к лабораторной работе

Выполните самостоятельно следующую работу, схема сети для которой представлена на рисунке 9.1.

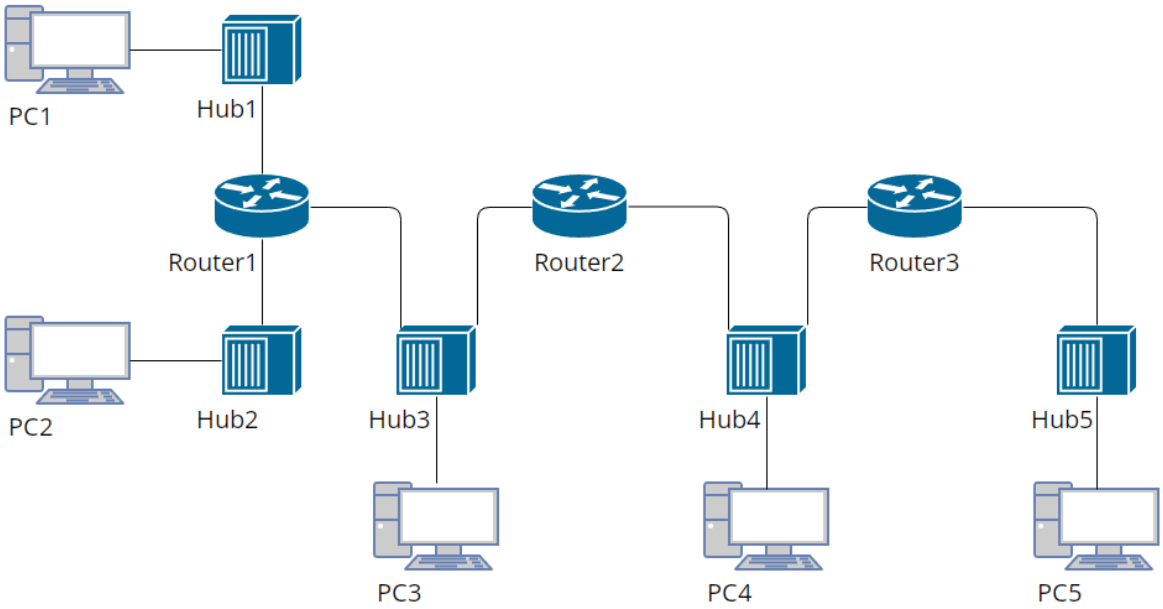

Рисунок 9.1 – Схема сети

Пять концентраторов представляют следующие пять сетей:
Hub1 – сеть 11.0.0.0
Hub2 – сеть 12.0.0.0
Hub3 – сеть 13.0.0.0
Hub4 – сеть 14.0.0.0
Hub5 – сеть 15.0.0.0

Все компьютеры имеют произвольные IP адреса со шлюзами своих роутеров.

Интерфейсы роутеров определяются сетью на концентраторе и номером роутера. Например для Router3: 15.0.0.3 и 14.0.0.3

С PC4 должны быть доступны все остальные компьютеры

После настройки и проверки доступа посмотреть таблицу маршрутизации командой *show ip route*

Контрольные вопросы

1. Что такое динамическая маршрутизация и чем она принципиально отличается от статической?
2. Какой командой можно посмотреть маршруты?
3. Если в таблице маршрутизации есть и статический, и динамический маршрут к одной сети, какой будет использоваться и почему?
4. Как проверяется работоспособность маршрутов после настройки?
5. Какие преимущества и недостатки динамической маршрутизации?

Лабораторная работа № 10 «Захват и сравнение сегментов TCP и датаграмм UDP в Wireshark»

Теоретические сведения

Транспортный уровень (Уровень 4 модели OSI) — это мост между сетевыми приложениями и сетью. Он обеспечивает сквозную (end-to-end) доставку данных между процессами на разных хостах.

Протокол TCP (Transmission Control Protocol) надёжный, ориентированный на соединение протокол транспортного уровня.

Ключевые особенности:

– Установка соединения (Three-way handshake): Перед обменом данными происходит процесс SYN -> SYN-ACK -> ACK.

– Надёжность: Использует подтверждения (ACK), тайм-ауты и повторные передачи для гарантированной доставки.

– Управление потоком: Механизм «скользящего окна» предотвращает переполнение буфера получателя.

– Управление перегрузкой: Динамически изменяет размер окна перегрузки для эффективного использования сети.

– Сегментация: Поток данных от приложения делится на сегменты.

Структура заголовка (20+ байт): Важные поля: Source/Destination Port, Sequence Number, Acknowledgment Number, Flags (SYN, ACK, FIN, RST), Window Size.

Протокол UDP (User Datagram Protocol) менее надёжный, не ориентированный на соединение (дейтаграммный) протокол.

Ключевые особенности:

– Отсутствие соединения: Данные отправляются без предварительной установки сеанса.

– Минимальные задержки: Нет накладных расходов на установку соединения, подтверждения и контроль потока.

– Нет гарантий доставки: Датаграммы могут быть потеряны, продублированы или прийти не по порядку.

– Неизменность данных границ: Сохраняет границы сообщений, отправленных приложением.

Структура заголовка (всего 8 байт): Поля: Source/Destination Port, Length, Checksum.

Таблица 10.1 – Сравнение протоколов

Характеристика	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Соединение	С установлением соединения (connection-oriented)	Без установления соединения (connectionless)
Надёжность	Гарантированная доставка, контроль ошибок, повторная передача	Без гарантий
Порядок	Сохранение порядка пакетов	Порядок не гарантируется
Контроль потока	Динамическое окно, предотвращение перегрузок	Отсутствует
Заголовок	20-60 байт (сложный)	8 байт (простой)
Примеры использования	HTTP, HTTPS, FTP, SSH, электронная почта	DNS, VoIP, видеостриминг, онлайн-игры

Задания к лабораторной работе

Задание 1:

1. Запустите Wireshark и выберите активный сетевой интерфейс.
2. Примените отображающий фильтр Wireshark: *tcp.port == 80*.
3. Начните захват пакетов.
4. Откройте в браузере простую HTTP-страницу (не HTTPS).
5. Остановите захват через 10 секунд и проанализируйте полученные пакеты.

Задание 2:

1. Примените отображающий фильтр Wireshark: *udp.port == 53*.
2. Начните захват пакетов.
3. В командной строке выполните команду nslookup example.com или откройте сайт по имени.
4. Остановите захват через 10 секунд и проанализируйте полученные пакеты.

Задание 3:

1. Примените отображающий фильтр Wireshark: *dns*.
2. Начните захват пакетов.
3. Запустите nslookup. Сначала запросите nslookup -type=A example.com, затем nslookup -type=MX example.com.
4. Остановите захват через 10 секунд и проанализируйте полученные пакеты.
5. Сравните процессы обмена для UDP и TCP: наличие handshake, количество пакетов, общий объем переданных данных.

Контрольные вопросы

1. В чем ключевые отличия TCP и UDP?
2. Почему UDP не нуждается в рукопожатии?
3. Какие преимущества у UDP перед TCP?
4. Когда используют UDP вместо TCP?
5. Какой фильтр в Wireshark покажет только TCP-трафик на порт 80?

Лабораторная работа № 11 «Анализ трёхстороннего рукопожатия»

Теоретические сведения

TCP (Transmission Control Protocol) — это протокол, который гарантирует доставку данных. Он работает как заказное письмо с уведомлением — вы знаете, что письмо дошло.

Трёхстороннее рукопожатие (Three-way Handshake) — это процесс из трёх шагов для установления надёжного соединения между двумя устройствами (клиентом и сервером) в сети по протоколу TCP, включающий отправку запроса (SYN), подтверждение (SYN-ACK) и финальное подтверждение (ACK) для синхронизации параметров и гарантии, что обе стороны готовы к обмену данными, предотвращая путаницу со старыми пакетами

Ключевые состояния при установлении соединения:

Со стороны клиента:

1. CLOSED: Начальное состояние
2. SYN_SENT: Отправил SYN, ждёт SYN-ACK
3. ESTABLISHED: Получил SYN-ACK, отправил ACK

Со стороны сервера:

1. CLOSED: Начальное состояние
2. LISTEN: Готов принимать соединения
3. SYN_RECEIVED: Получил SYN, отправил SYN-ACK
4. ESTABLISHED: Получил ACK

Флаги — это специальные биты в заголовке TCP, которые показывают тип пакета:

Таблица 11.1 – Флаги TCP

Флаг	Название	Что означает
SYN	Synchronize	начало соединения
ACK	Acknowledge	подтверждение
FIN	Finish	завершение
RST	Reset	аварийное завершение
PSH	Push	не жди буфера
URG	Urgent	приоритетные

Порядок работы в Wireshark:

Шаг 1: Откройте Wireshark

Шаг 2: Выберите сетевой интерфейс (Wi-Fi или Ethernet)

Шаг 3: Начните захват (кнопка "акула")

Шаг 4: Выполните действие, которое создаст TCP соединение:

- Откройте сайт в браузере
- Выполните telnet или ssh
- Используйте любое приложение, работающее по TCP

Шаг 5: Остановите захват через 10-15 секунд

Поиск рукопожатия в захваченном трафике

Метод 1: Фильтр по порту

tcp.port == 80 # HTTP
tcp.port == 443 # HTTPS
tcp.port == 22 # SSH

Метод 2: Фильтр по флагам

tcp.flags.syn == 1 # Ищем SYN пакеты
tcp.flags.ack == 1 # Ищем ACK пакеты
tcp.flags.syn == 1 and tcp.flags.ack == 1 # Ищем SYN-ACK

Метод 3: Фильтр потока

Выберите любой TCP пакет → правой кнопкой → Follow → TCP Stream

После чего на вкладке "Packet Details" можно найти подробности пакета. Ключевые поля:

- Sequence number: Начальный номер последовательности
- Acknowledgment number: Номер подтверждения
- Flags: Какие флаги установлены
- Window size: Размер окна (сколько данных можно отправить без подтверждения)
- MSS (Maximum Segment Size): Максимальный размер сегмента

Задания к лабораторной работе

Задание 1: Захватить и проанализировать рукопожатие при открытии сайта.

Шаги:

1. Откройте Wireshark, начните захват
2. Откройте в браузере: *http://example.com*
3. Остановите захват

Найдите трёхстороннее рукопожатие (SYN → SYN-ACK → ACK)

Для каждого пакета определите:

- Исходный и целевой порты
- Установленные флаги
- Sequence number
- Acknowledgment number

Задание 2: Проанализировать ситуацию, когда рукопожатие не удалось.

Метод: Попробуйте подключиться к несуществующему серверу:

telnet 192.168.1.999 80

1. Что происходит вместо SYN-ACK?
2. Сколько SYN отправляет клиент перед сдачей?
3. Какие таймауты наблюдаете?

Контрольные вопросы

Что такое трёхстороннее рукопожатие (three-way handshake) в TCP и зачем оно нужно?

Назовите и объясните назначение двух ключевых флагов TCP, используемых в рукопожатии.

Сколько времени занимает рукопожатие (время между SYN и ACK)?

Как клиент понимает, что соединение не установится?

Перечислите три пакета трёхстороннего рукопожатия в правильной последовательности.

Лабораторная работа № 12 «Использование утилит для диагностики соединений»

Теоретические сведения

Целью устранения неисправностей в настройке TCP/IP является восстановление нормальной работы сети. Для поиска неисправностей можно использовать специальные диагностические утилиты, предназначенные для проверки конфигурации стека TCP/IP и тестирования сетевого соединения. Список некоторых утилит приведен в таблице 1.

Таблица 12.1 – Диагностические утилиты.

Утилита	Применение
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу).
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

Задания к лабораторной работе

Задание 1: Получение справочной информации по командам.

Выведите на экран справочную информацию по всем рассмотренным утилитам. Для этого в командной строке введите имя утилиты без параметров и дополните /?.

Сохраните справочную информацию в отдельном файле.

Изучите ключи, используемые при запуске утилит.

Задание 2: Получение имени хоста.

Выведите на экран имя локального хоста с помощью команды hostname. Сохраните результат в отдельном файле.

Задание 3: Изучение утилиты ipconfig.

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	

Задание 4: Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.
3. Проверьте возможность установления соединения с удаленным хостом.
4. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте rgups.ru) и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

Задание 5: Определение пути IP-пакета.

С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Изучите ключи команды.

a) rgups.ru

b) portal.rgups.ru

c) dlearn.rgups.ru

Задание 6: Просмотр ARP-кэша.

С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

Внести в кэш локального компьютера любую статическую запись.

Задание 7: Просмотр локальной таблицы маршрутизации.

С помощью утилиты route просмотреть локальную таблицу маршрутизации.

Задание 8: Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы

1. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
2. Каким образом команда ping проверяет соединение с удаленным хостом?
3. Какие могут быть причины неудачного завершения ping и tracert?
4. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
5. Всегда ли можно узнать символьное имя узла по его ip-адресу?

Лабораторная работа № 13 «Анализ handshake-процесса HTTPS на уровне представления»

Теоретические сведения

HTTPS (HyperText Transfer Protocol Secure) — это не самостоятельный протокол, а результат наслоения стандартного HTTP на протокол шифрования TLS (или его устаревшего предшественника SSL). Безопасность обеспечивается именно TLS, который работает между транспортным протоколом (TCP) и прикладным протоколом (HTTP).

В изучаемом процессе задействуется сразу 3 уровня модели OSI:

– Транспортный уровень (4): TCP. Обеспечивает надежную доставку сегментов. Handshake HTTPS начинается с TCP handshake (SYN, SYN-ACK, ACK).

– Сеансовый уровень (5): TLS. Установление, управление и завершение защищённого сеанса связи.

– Уровень представления (6): TLS. Преобразование данных — шифрование, дешифрование, аутентификация, проверка целостности (коды аутентичности сообщений — MAC).

После установки TCP-соединения происходит диалог TLS, состоящий из обмена специальными записями (TLS Records):

1. *Client Hello*: Клиент отправляет серверу:

– Поддерживаемые версии TLS (например, TLS 1.2, 1.3).

– Случайное число (Client Random).

– Список поддерживаемых шифр-наборов (Cipher Suites) — комбинаций алгоритмов для ключеого обмена, аутентификации, шифрования и контроля целостности.

– Список поддерживаемых методов сжатия (часто не используется).

– При необходимости — расширения (SNI для указания имени виртуального хоста и др.).

2. *Server Hello*: Сервер отвечает:

– Выбранную версию TLS.

– Случайное число (Server Random).

– Выбранный шифр-набор из предложенного клиентом списка.

– Свой цифровой сертификат (цепочку сертификатов), содержащий открытый ключ сервера.

– Запрос на аутентификацию клиента (опционально, редко для веба).

3. Client Key Exchange (для TLS 1.2 и ранее): Клиент проверяет сертификат сервера (срок действия, доверие УЦ, доменное имя). После успешной проверки:

– Генерирует Pre-Master Secret (Премьер-секрет).

– Шифрует его открытым ключом сервера из сертификата и отправляет серверу.

– Для TLS 1.3: Этот этап кардинально изменён (обмен ключами по Диффи-Хеллману).

4. Создание ключей: И сервер, и клиент независимо, используя Client Random, Server Random и Pre-Master Secret, вычисляют одинаковый Master Secret. Из него генерируются сессионные ключи для симметричного шифрования трафика и вычисления кодов аутентичности (MAC).

5. Change Cipher Spec (Смена алгоритмов): Уведомление о том, что все последующие сообщения будут шифроваться выбранными алгоритмами.

6. Finished (Завершено): Первое зашифрованное сообщение, содержащее дайджест всех предыдущих handshake-сообщений для проверки целостности процесса.

Задания к лабораторной работе

Предварительная настройка системы:

1. Создайте на рабочем столе или в удобной папке пустой текстовый файл и назовите его, например, *sslkeys.log*. Запомните его полный путь (например, *C:\Users\ВашеИмя\Desktop\sslkeys.log*).

2. Настройка системы (Windows)

– Нажмите Win + R, введите *sysdm.cpl* и нажмите Enter.

– Перейдите на вкладку «Дополнительно» и нажмите кнопку «Переменные среды…».

– В нижней части («Переменные среды пользователя») нажмите «Создать…».

– В поле «Имя переменной» введите: SSLKEYLOGFILE

– В поле «Значение переменной» введите полный путь к созданному файлу (например, *C:\Users\ВашеИмя\Desktop\sslkeys.log*).

– Нажмите ОК во всех открытых окнах.

– ВАЖНО: Для вступления изменений в силу необходимо полностью закрыть все окна браузера (Chrome, Firefox, Edge) и перезапустить их.

– Для Linux/macOS: Экспорт переменной в терминале перед запуском браузера: *export SSLKEYLOGFILE=~/sslkeys.log*

3. Настройка Wireshark для использования файла ключей

– Откройте Wireshark.

– Перейдите в меню: Edit (Правка) -> Preferences (Настройки).

– В левом списке разверните узел Protocols и найдите (или введите в поиск) протокол TLS.

– В правой панели найдите поле *(Pre)-Master-Secret log filename*.

– Нажмите кнопку Browse... и выберите тот самый файл sslkeys.log, который вы создали.

– Нажмите OK. Теперь Wireshark будет автоматически расшифровывать TLS-трафик из браузеров.

Задание 1: Процесс захвата и анализа трафика

1. Запустите Wireshark от имени администратора (чтобы были доступны все сетевые интерфейсы).

2. В списке интерфейсов выберите тот, через который осуществляется выход в интернет (обычно это Wi-Fi-адаптер или Ethernet). Подсказка: нужный интерфейс будет показывать активный всплеск трафика (зеленая полоска).

3. Сразу примените фильтр захвата (Capture Filter):

– Нажмите на шестеренку рядом с выбранным интерфейсом.

– В поле Capture Filter введите: host <IP_адрес_целевого_сайта>.

– Пример для google.com: Сначала узнайте IP через ping google.com в командной строке. Допустим, IP 142.250.185.78. Тогда фильтр: host 142.250.185.78.

– Это нужно чтобы захватить только трафик к нужному сайту, избежав тысяч лишних пакетов. Если IP неизвестен, можно использовать фильтр port 443, но будет больше шума.

4. Нажмите кнопку Start Capture (синяя акула) в Wireshark.

5. В браузере: Очистите кэш и куки для чистоты эксперимента (Ctrl+Shift+Del). Откройте новую вкладку.

6. Введите в адресную строку *https://www.example.com* и нажмите Enter.

7. Дождитесь полной загрузки страницы.

8. Переключитесь обратно в Wireshark и нажмите кнопку Stop Capture (красный квадрат).

Задание 2: Фильтрация и базовый анализ в Wireshark

1. В поле «Apply a display filter» (строка над списком пакетов) введите: tls и нажмите Enter. Вы увидите только TLS-трафик.

2. Найдите первый пакет TLSv1.2 или TLSv1.3 типа *Client Hello*.

3. Просмотр деталей: Щелкните на пакете *Client Hello*. В средней панели разверните структуру:

– Frame (общая информация о кадре).

– Ethernet II (кадр канального уровня).

– Internet Protocol Version 4 (IP-заголовок).

– Transmission Control Protocol (TCP-заголовок, порты).

– Transport Layer Security – это то, что нам нужно! Разверните это дерево:

– TLSv1.2 Record Layer: Handshake Protocol: Client Hello

– Внутри Handshake Protocol: Client Hello найдите ключевые поля: Version, Random, Cipher Suites, Extensions.

Задание 3: Анализ полного handshake

1. Найдите TCP handshake: Примените фильтр tcp.flags.syn==1 or tcp.flags.ack==1. Убедитесь, что перед Client Hello идут пакеты SYN, SYN-ACK, ACK.

2. Верните фильтр tls. Пронумеруйте ключевые сообщения TLS:

– Пакет 1: Client Hello

– Пакет 2: Server Hello (часто в одном TCP-сегменте с Certificate и Server Key Exchange/Server Hello Done)

– Пакет 3: Certificate (сертификат сервера, может быть несколько).

– Пакет 4: Client Key Exchange (для TLS 1.2), Change Cipher Spec, Encrypted Handshake Message (Finished).

– Пакет 5: New Session Ticket (если есть), Change Cipher Spec, Encrypted Handshake Message (Finished) от сервера.

3. Анализ Application Data: После handshake идут пакеты Application Data. Если настройка с sslkeys.log прошла успешно, Wireshark расшифрует их, и вы увидите внутри HTTP/2 или TLSv1.2 Application Data -> HyperText Transfer Protocol 2 (или HTTP/1.1). Щелкните правой кнопкой по такому пакету -> Follow -> TLS Stream (или HTTP2 Stream), чтобы увидеть весь диалог в удобном виде.

Контрольные вопросы

1. Какие два протокола лежат в основе HTTPS?
2. Каковы основные цели протокола TLS, поверх которого работает HTTPS?
3. Опишите последовательность сообщений в полном TLS 1.2 handshake.
4. Где в процессе handshake клиент получает открытый ключ сервера, чтобы начать с ним безопасно общаться?
5. По каким признакам в списке пакетов Wireshark вы сразу найдёте начало TLS handshake?

Лабораторная работа № 14 «Развертывание и настройка локального DNS-сервера»

Теоретические сведения

DNS (Domain Name System «система доменных имён») — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене (SRV-запись).

Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

Основой DNS является представление об иерархической структуре имени и зонах. Каждый сервер, отвечающий за имя, может передать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Начиная с 2010 года в систему DNS внедряются средства проверки целостности передаваемых данных, называемые DNS Security Extensions (DNSSEC). Передаваемые данные не шифруются, но их достоверность проверяется криптографическими способами. Внедряемый стандарт DANE обеспечивает передачу средствами DNS достоверной криптографической информации (сертификатов), используемых для установления безопасных и защищённых соединений транспортного и прикладного уровней.

DNS обладает следующими характеристиками:

– Распределённость администрирования. Ответственность за разные части иерархической структуры несут разные люди или организации.

– Распределённость хранения информации. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности, и (возможно) адреса корневых DNS-серверов.

– Кэширование информации. Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.

– Иерархическая структура, в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегировать (передавать) их другим узлам.

– Резервирование. За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

DNS важна для работы Интернета, так как для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать

буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например, HTTP-серверы, различая их по имени запроса. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла hosts, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом Сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

Ключевыми понятиями DNS являются:

– Домéн (domain «область») — узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), то есть именованная ветвь или поддерево в дереве имён. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо от младших доменов к доменам высшего уровня (в порядке повышения значимости): вверху находится корневой домен (имеющий идентификатор «.»(точка)), ниже идут домены первого уровня (доменные зоны), затем — домены второго уровня, третьего и т. д. (например, для адреса ru.wikipedia.org. домен первого уровня — org, второго — wikipedia, третьего — ru). DNS позволяет не указывать точку корневого домена.

– Поддомен (subdomain) — подчинённый домен (например, wikipedia.org — поддомен домена org, а ru.wikipedia.org — домена wikipedia.org). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имён используют более строгие ограничения. Например, если у вас есть домен вида mydomain.ru, вы можете создать для него различные поддомены вида mysite1.mydomain.ru, mysite2.mydomain.ru и т. д.

– Ресурсная запись — единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определённому доменному имени, узлу в дереве имён), тип и поле данных, формат и содержание которого зависит от типа.

– Зона — часть дерева доменных имён (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имён (DNS-сервере, см. ниже), а чаще — одновременно на нескольких серверах (см. ниже). Целью выделения части дерева в отдельную зону является передача ответственности (см. ниже) за соответствующий домен другому лицу или организации. Это называется делегированием (см. ниже). Как связная часть дерева, зона внутри тоже представляет собой дерево. Если рассматривать пространство имён DNS как структуру из зон, а не отдельных узлов/имён, тоже получается дерево; оправданно говорить о родительских и дочерних зонах, о старших и подчинённых. На практике большинство зон 0-го и 1-го уровня ('.', ru, com, …) состоят из единственного узла, которому непосредственно подчиняются дочерние зоны. В больших корпоративных

доменах (2-го и более уровней) иногда встречается образование дополнительных подчинённых уровней без выделения их в дочерние зоны.

– Делегирование — операция передачи ответственности за часть дерева доменных имён другому лицу или организации. За счёт делегирования в DNS обеспечивается распределённость администрирования и хранения. Технически делегирование выражается в выделении этой части дерева в отдельную зону, и размещении этой зоны на DNS-сервере (см. ниже), управляемом этим лицом или организацией. При этом в родительскую зону включаются «склеивающие» ресурсные записи (NS и A), содержащие указатели на DNS-сервера дочерней зоны, а вся остальная информация, относящаяся к дочерней зоне, хранится уже на DNS-серверах дочерней зоны.

– DNS-сервер — специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.

– DNS-клиент — специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

– Авторитетность (authoritative) — признак размещения зоны на DNS-сервере. Ответы DNS-сервера могут быть двух типов: авторитетные (когда сервер заявляет, что сам отвечает за зону) и неавторитетные (Non-authoritative), когда сервер обрабатывает запрос, и возвращает ответ других серверов. В некоторых случаях вместо передачи запроса дальше DNS-сервер может вернуть уже известное ему (по запросам ранее) значение (режим кеширования).

– DNS-запрос (DNS query) — запрос от клиента (или сервера) серверу. Запрос может быть рекурсивным или нерекурсивным.

Система DNS содержит иерархию DNS-серверов, соответствующую иерархии зон. Каждая зона поддерживается как минимум одним авторитетным сервером DNS (authoritative — авторитетный), на котором расположена информация о домене.

Имя и IP-адрес не тождественны — один IP-адрес может иметь множество имён, что позволяет поддерживать на одном компьютере множество веб-сайтов (это называется виртуальный хостинг). Обратное тоже справедливо — одному имени может быть сопоставлено множество IP-адресов: это позволяет создавать балансировку нагрузки.

Для повышения устойчивости системы используется множество серверов, содержащих идентичную информацию, а в протоколе есть средства, позволяющие поддерживать синхронность информации, расположенной на разных серверах. Существует 13 корневых серверов, их адреса практически не изменяются.

Протокол DNS использует для работы TCP- или UDP-порт 53 для ответов на запросы. Традиционно запросы и ответы отправляются в виде

одной UDP-датаграммы. TCP используется, когда размер данных ответа превышает 512 байт, и для AXFR-запросов.

DNS используется в первую очередь для преобразования символьных имён в IP-адреса, но он также может выполнять обратный процесс. Для этого используются уже имеющиеся средства DNS. Дело в том, что с записью DNS могут быть сопоставлены различные данные, в том числе и какое-либо символьное имя. Существует специальный домен in-addr.arpa, записи в котором используются для преобразования IP-адресов в символьные имена. Например, для получения DNS-имени для адреса 11.22.33.44 можно запросить у DNS-сервера запись 44.33.22.11.in-addr.arpa, и тот вернёт соответствующее символьное имя. Обратный порядок записи частей IP-адреса объясняется тем, что в IP-адресах старшие биты расположены в начале, а в символьных DNS-именах старшие (находящиеся ближе к корню) части расположены в конце.

Задания к лабораторной работе

1. В диспетчере серверов выбрать пункт «Добавить роли и компоненты».

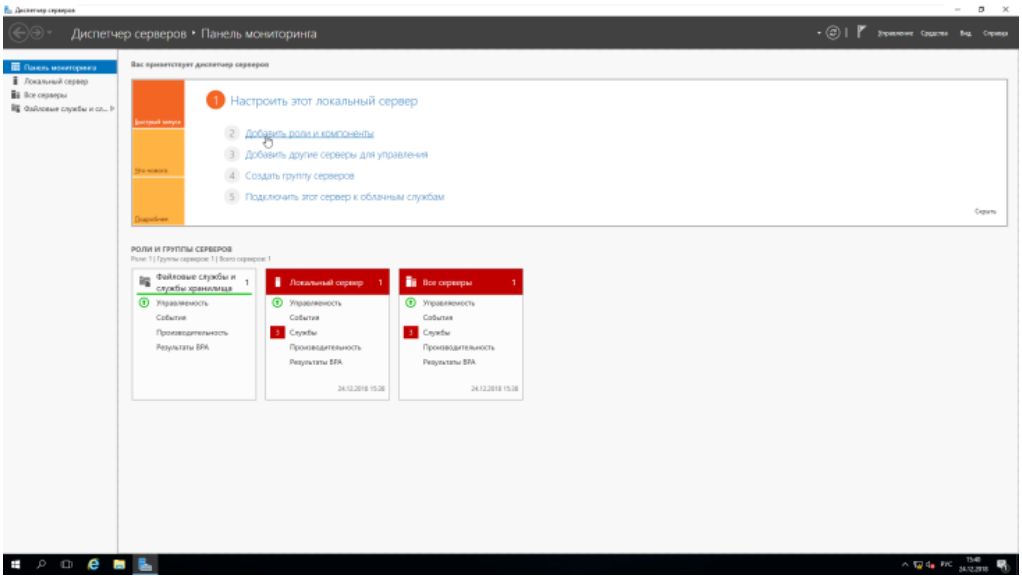

Рисунок 14.1 – Диспетчер сервера

2. В открывшемся окне мастера нажать далее.

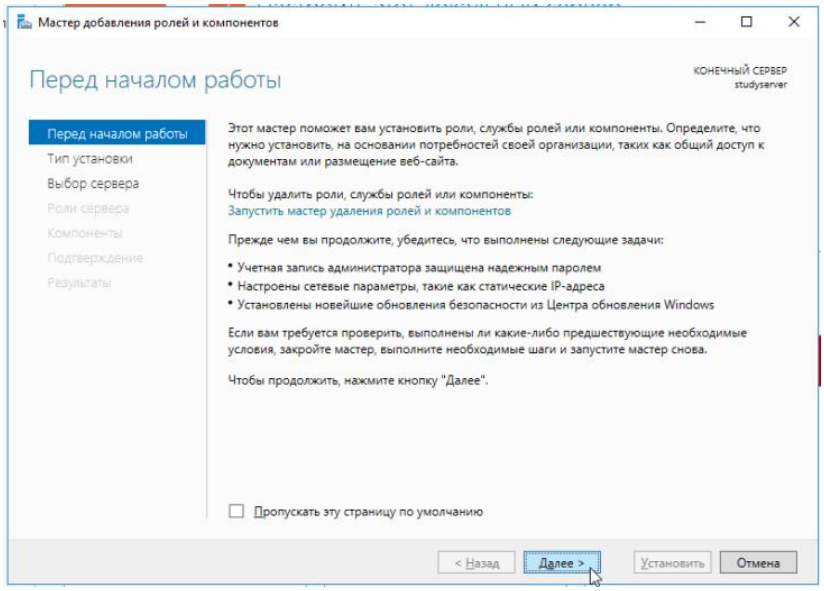

Рисунок 14.2 – Мастер добавления ролей

3. Выбрать пункт: «Установка ролей и компонентов».

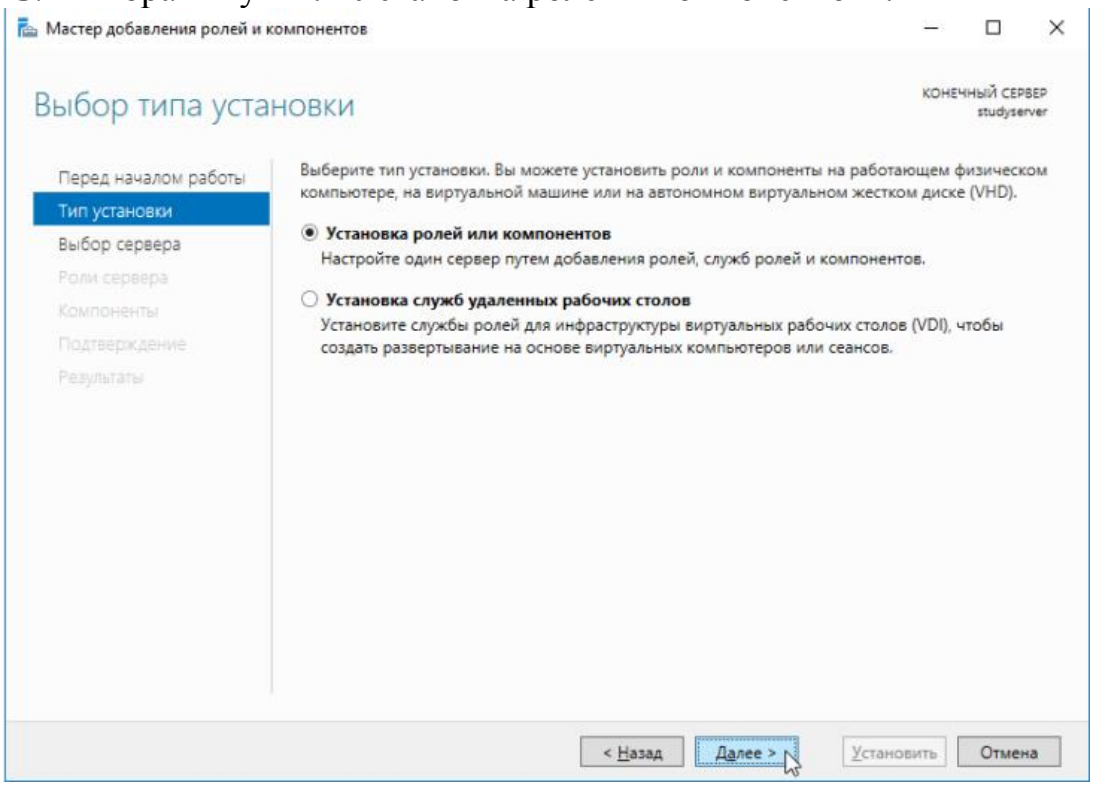

Рисунок 14.3 – Тип установки

4. Выбрать сервер из списка.

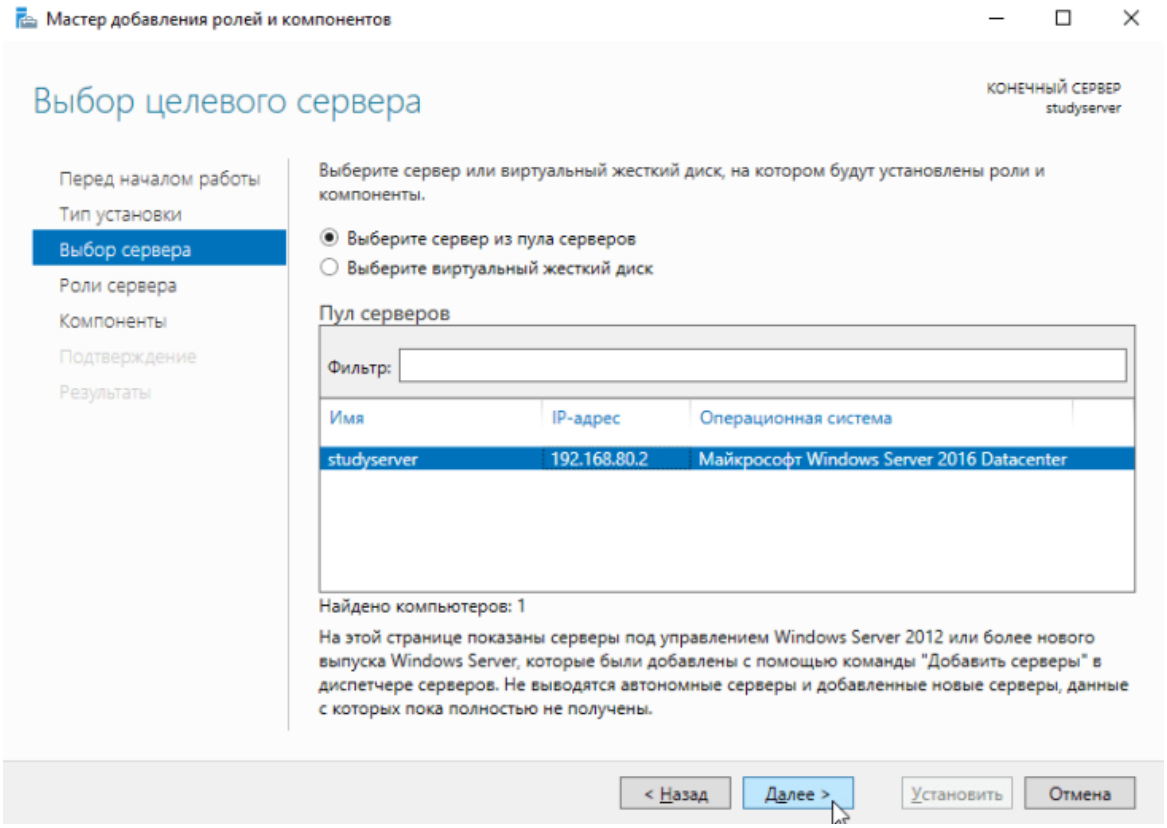

Рисунок 14.4 – Выбор сервера

5. Выбрать роль «DNS-сервер».

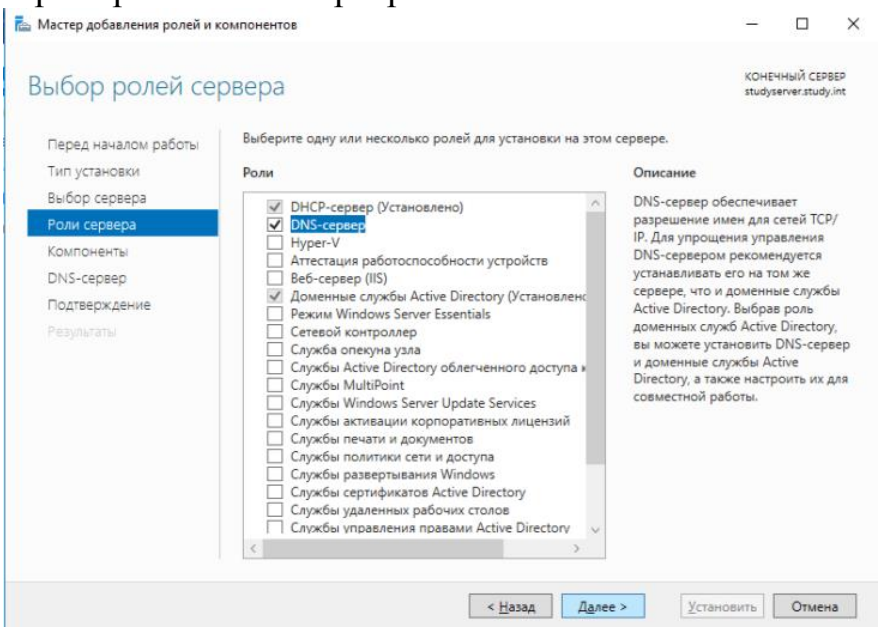

Рисунок 14.5 – Выбор ролей

6. В появившемся окне предлагают установить необходимые для продолжения компоненты. Нажать «Добавить компоненты».

7. В окне выбора компонентов нажать «Далее», поскольку необходимые компоненты были выбраны в предыдущем пункте.

8. В следующем окне приведена краткая информация о роли DNS — сервера. Ознакомиться с ней и нажать «Далее».

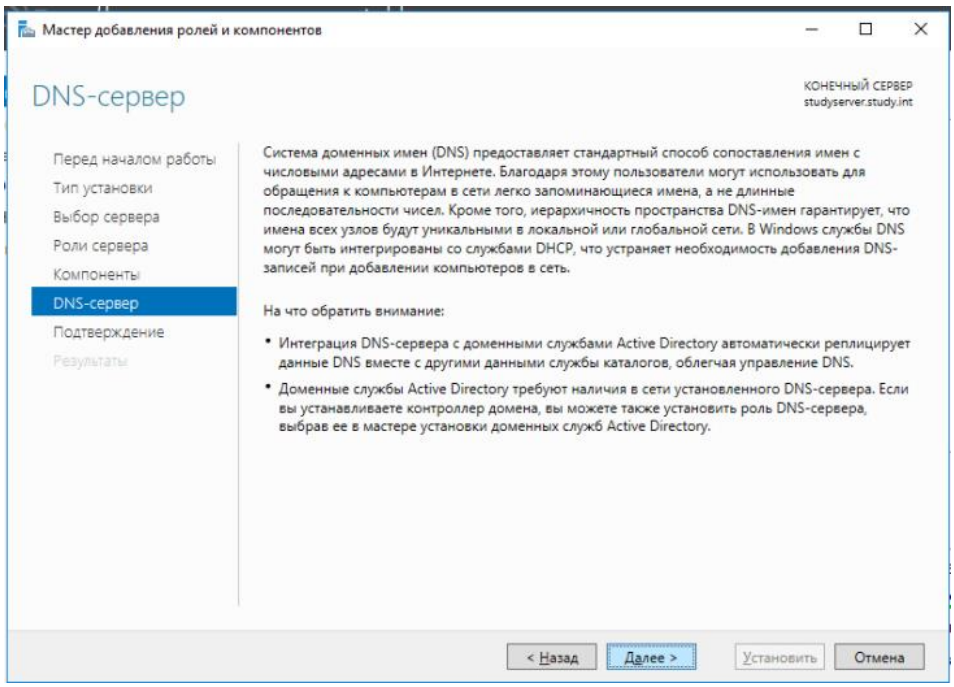

Рисунок 14.6 – Информация

9. Ознакомиться со списком устанавливаемых компонентов и нажать «Установить».

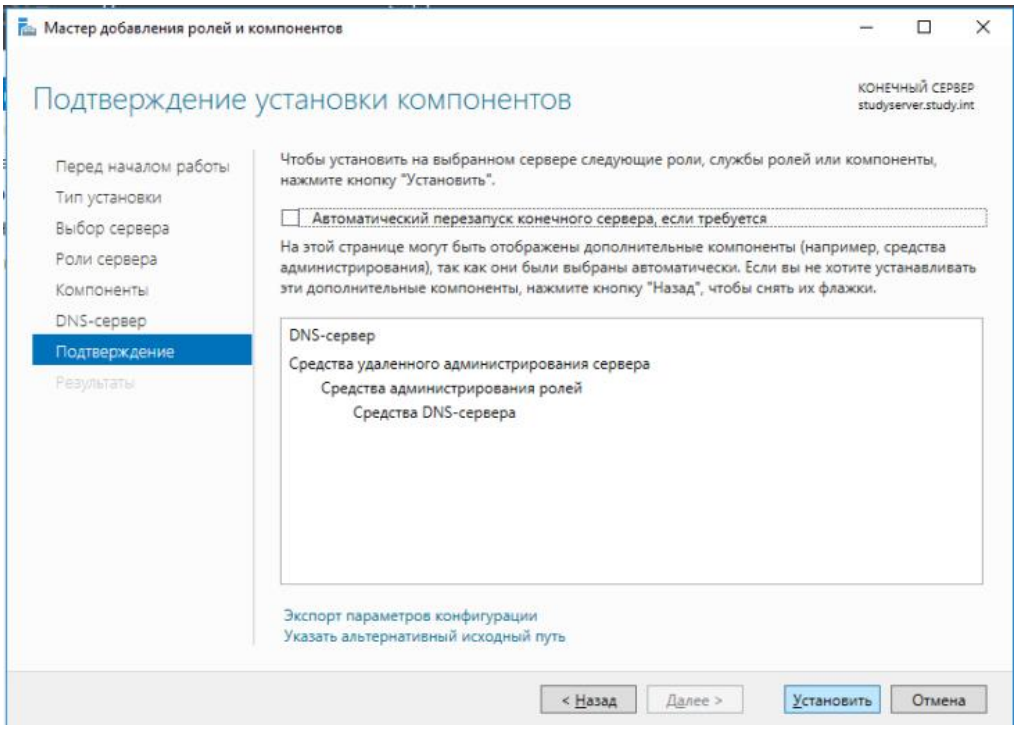

Рисунок 14.7 – Подтверждение

10. По окончании установки, закрыть мастер.

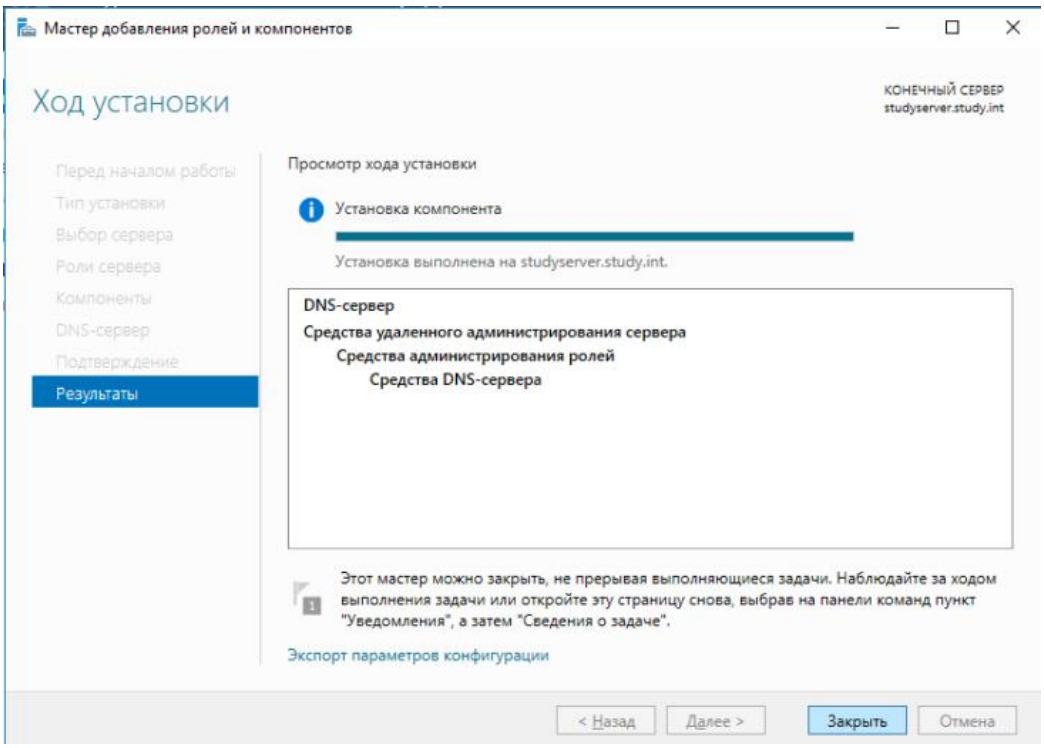

Рисунок 14.8 – Окончание установки

11. В диспетчере серверов, в пункте «Средства», выбрать DNS.

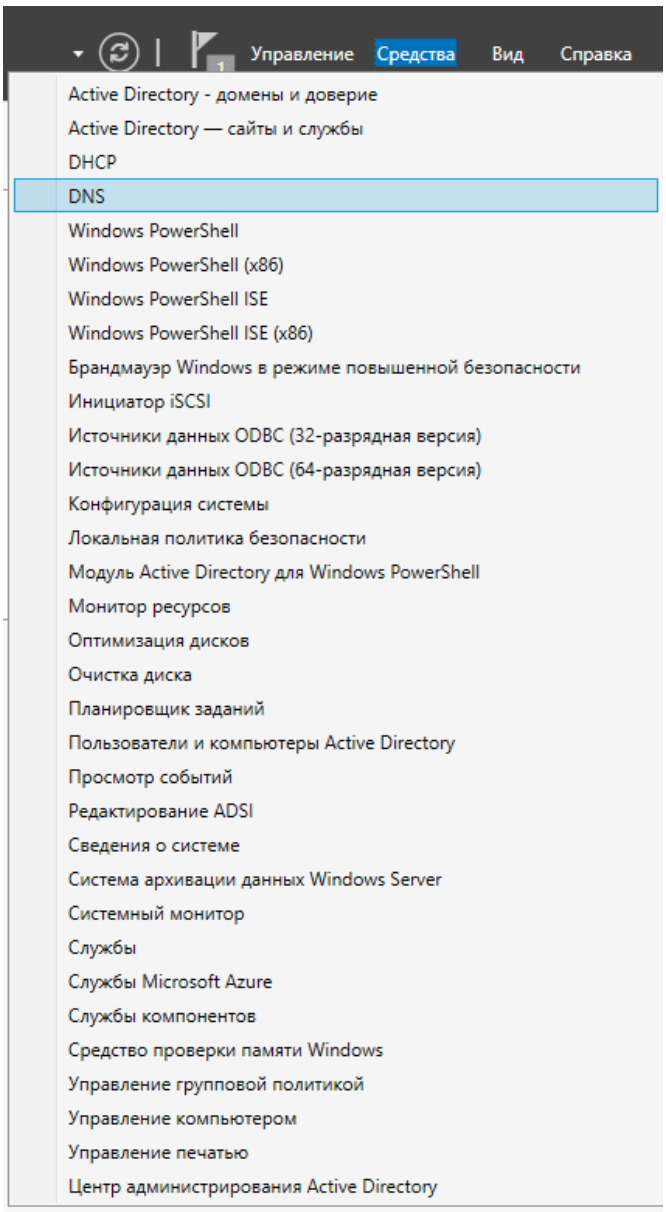

Рисунок 14.9 – Выбор компонента

12. В открывшемся диспетчере DNS видно созданный сервер.

Примечание: в некоторых случаях, зона прямого промотора создается автоматически (присутствует на изображении) её можно удалить или оставить как есть. В дальнейшем, рассматривается вариант, когда зона не создана или удалена.

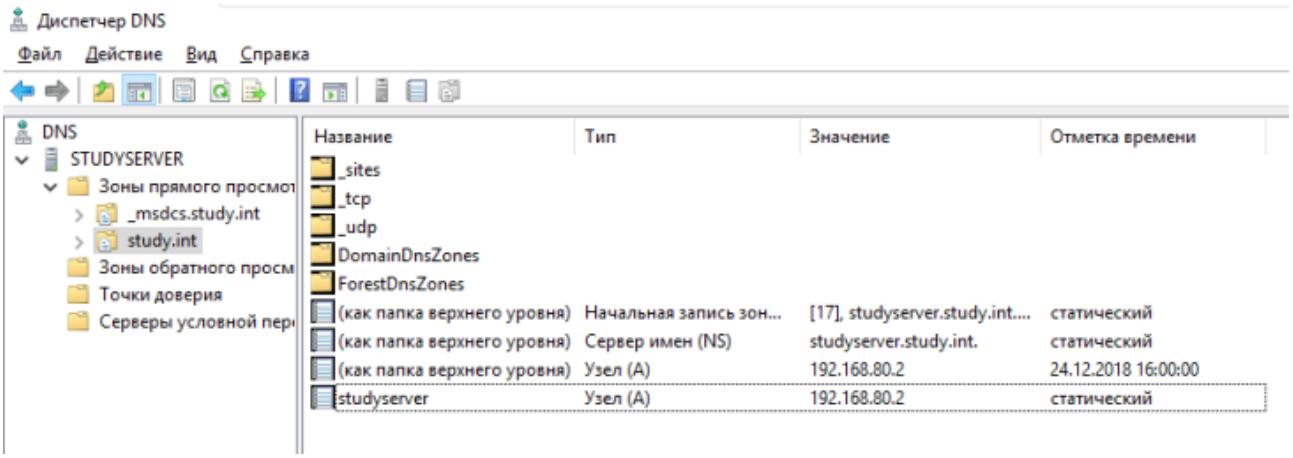

Рисунок 14.10 – Диспетчер DNS

13. На группе «Зоны прямого просмотра» щелчком правой кнопкой мыши вызвать контекстное меню и выбрать «Создать новую зону».

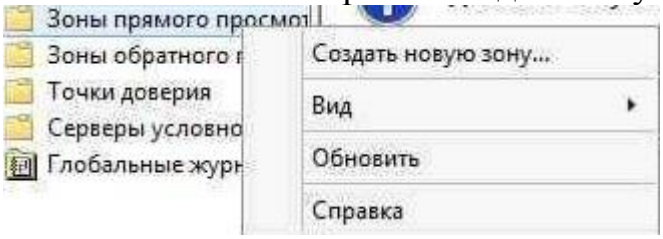

Рисунок 14.11 – Создание новой зоны

14. В открывшемся мастере, нажать «Далее».

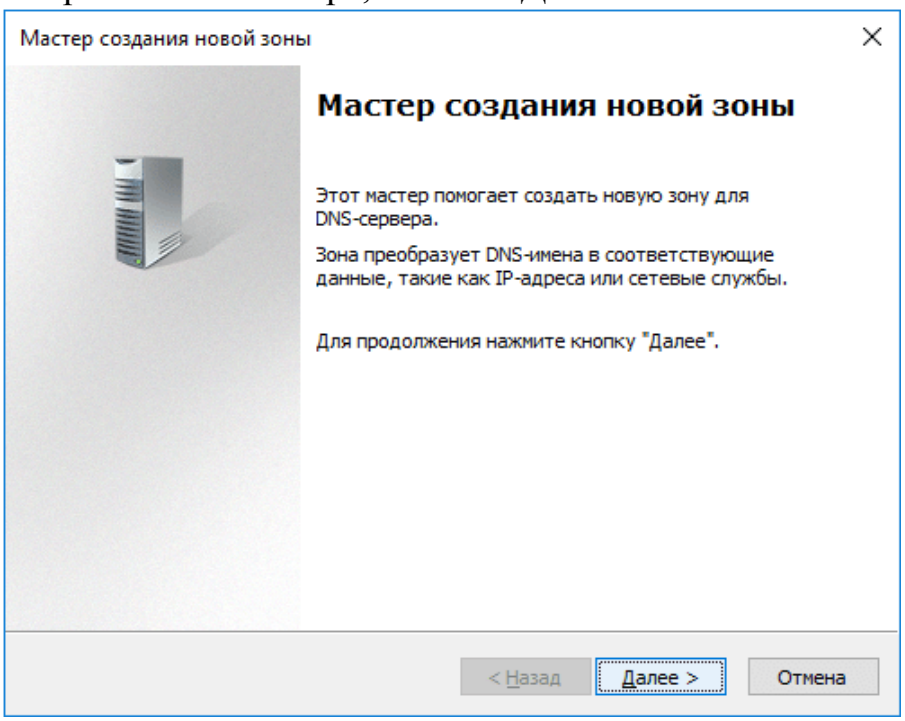

Рисунок 14.12 – Мастер создания

15. Выбрать тип зоны — «Основная».

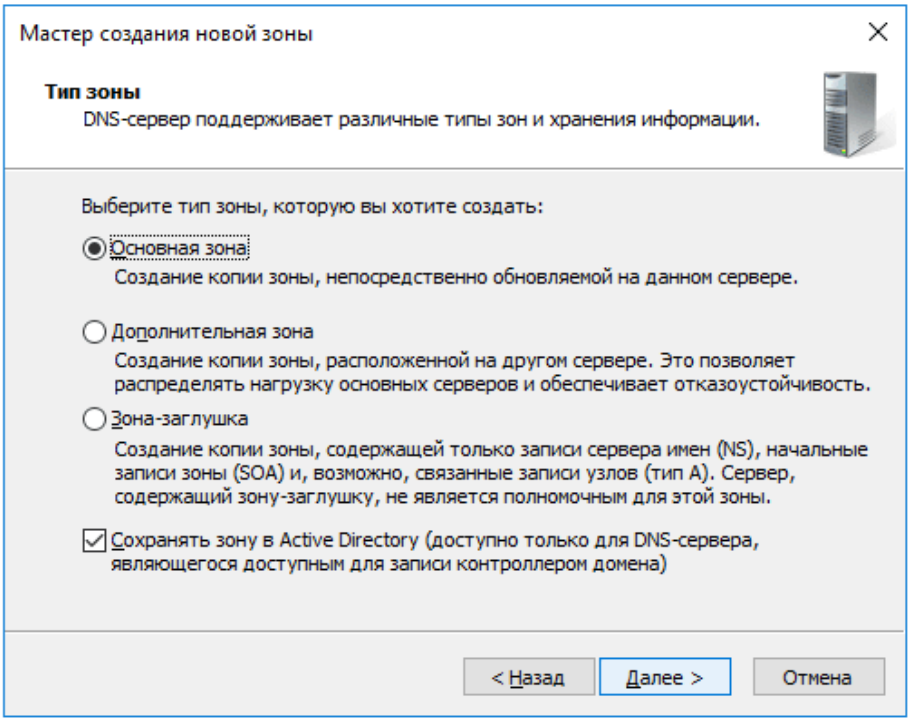

Рисунок 14.13 – Выбор типа зоны

16. Выбрать область репликации.

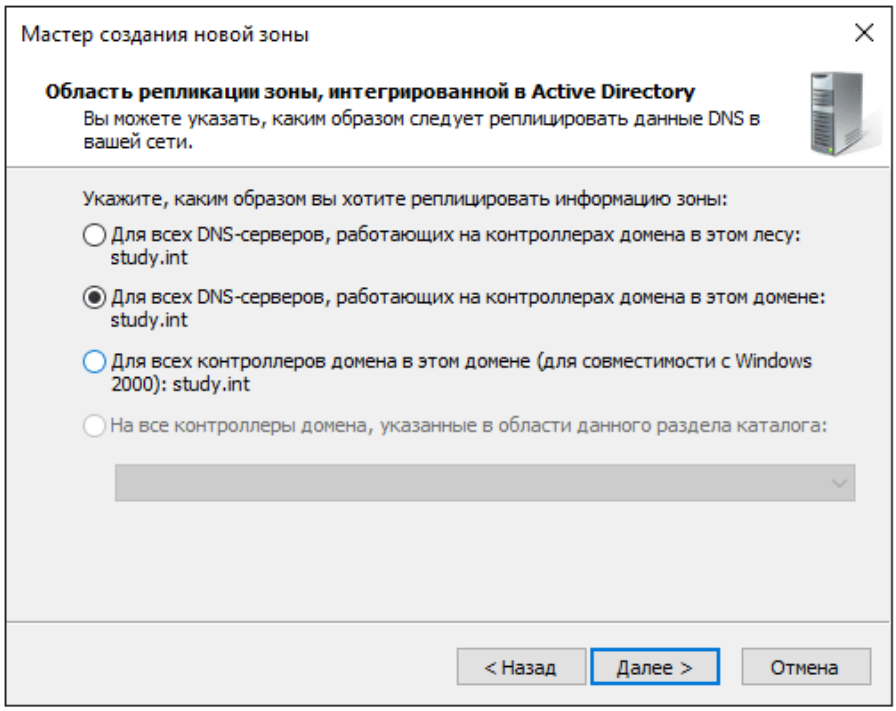

Рисунок 14.14 – Выбор области репликации

17. Ввести имя зоны.

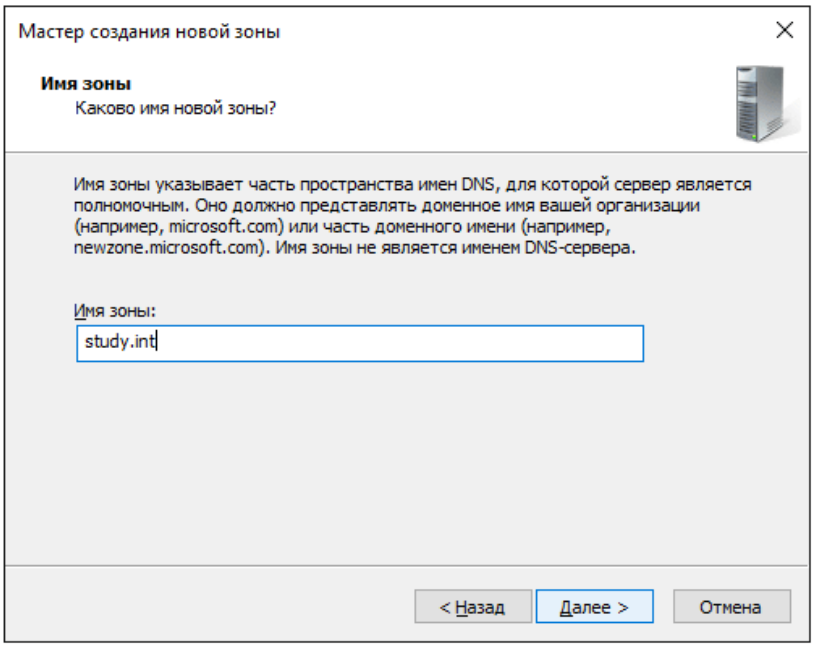

Рисунок 14.15 – Имя зоны

18. Выбрать настройки динамического обновления.

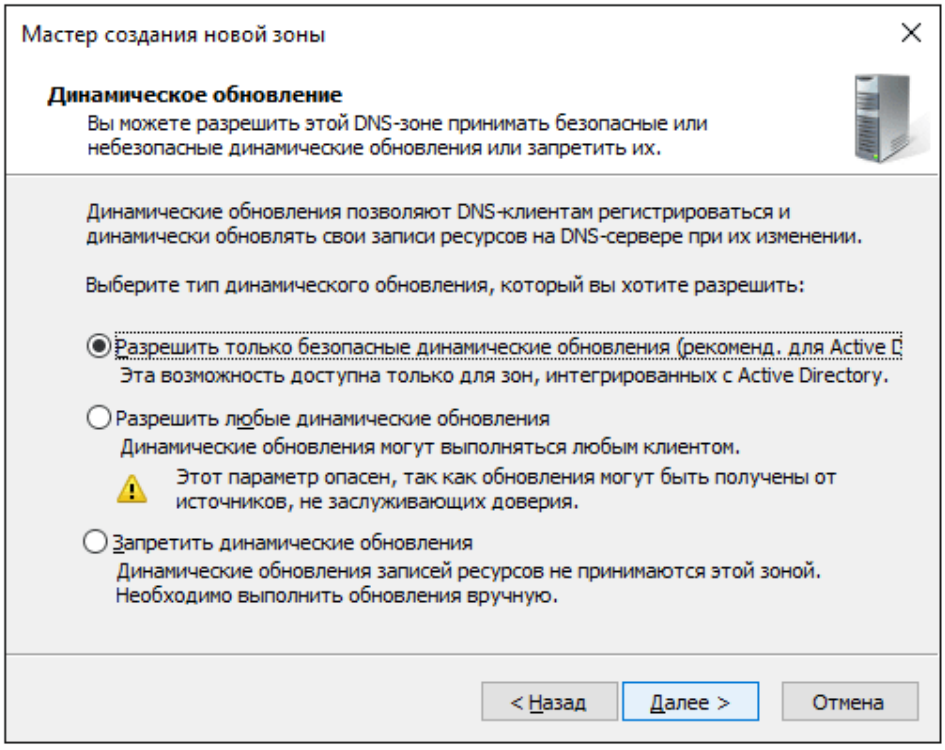

Рисунок 14.16 – Настройки обновления

19. По завершении работы, мастер выведет сообщение, что зона создана.

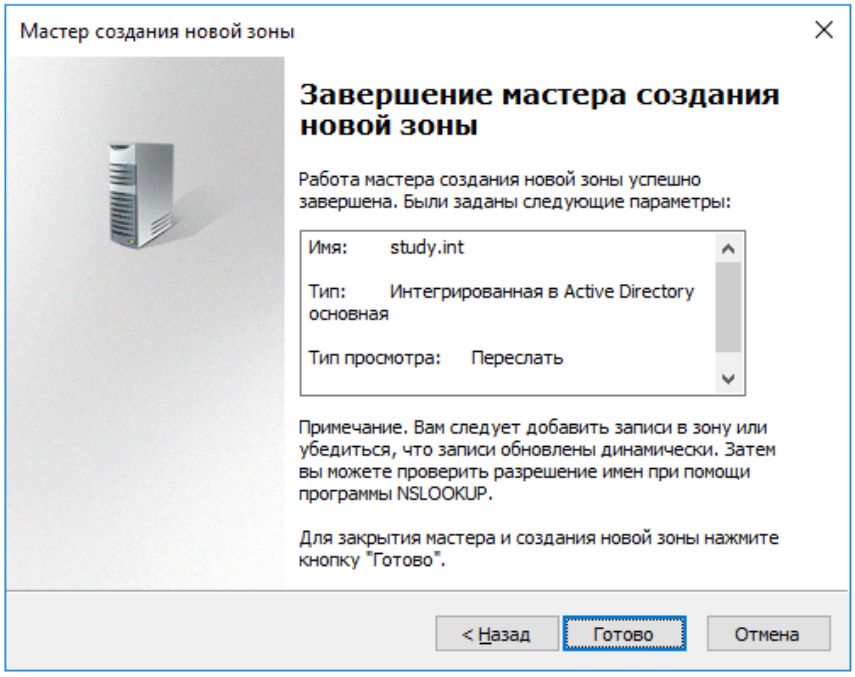

Рисунок 14.17 – Завершение создания зоны

20. Также нужно создать узел в этой зоне, например, текущий сервер. Для этого, щелкнуть правой кнопкой мыши в зоне и нажать — «Создать узел (A или AAAA)…».

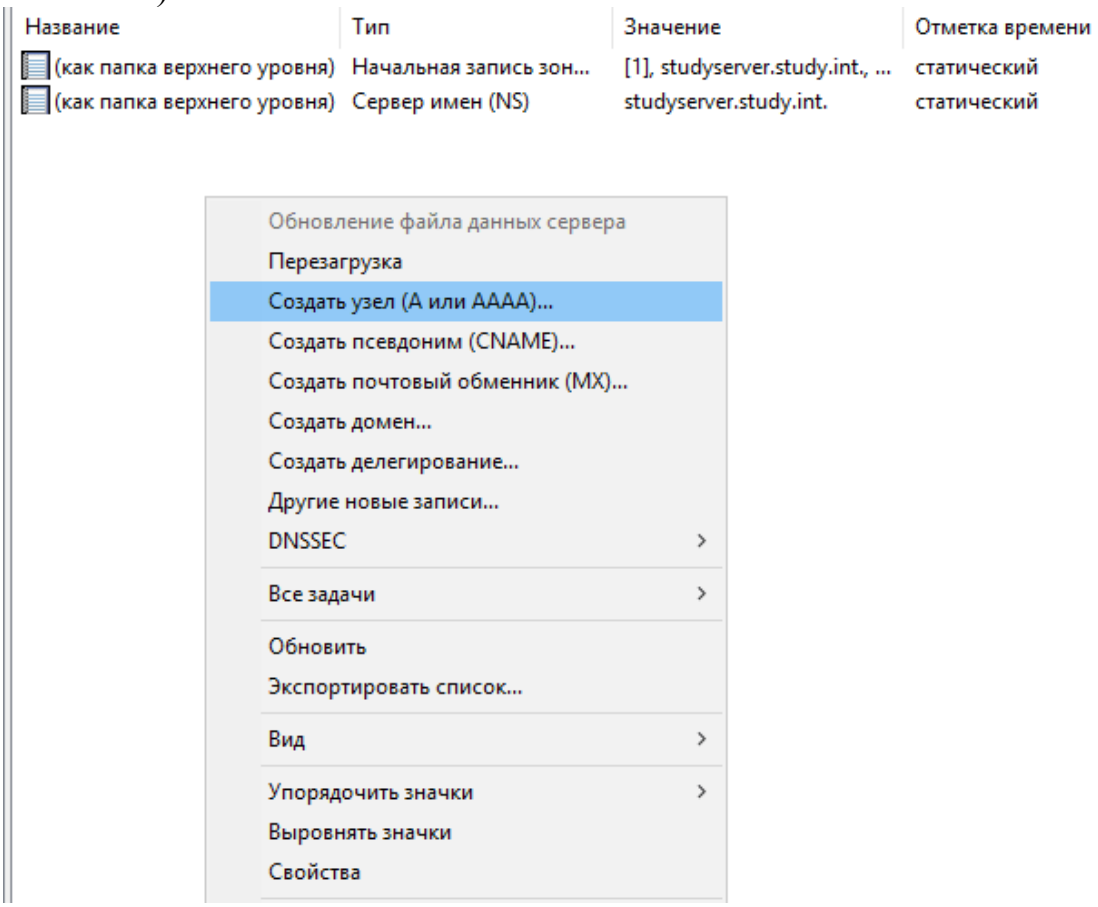

Рисунок 14.18 – Создание узла

21. Ввести имя узла и его адрес и нажать «Добавить узел».

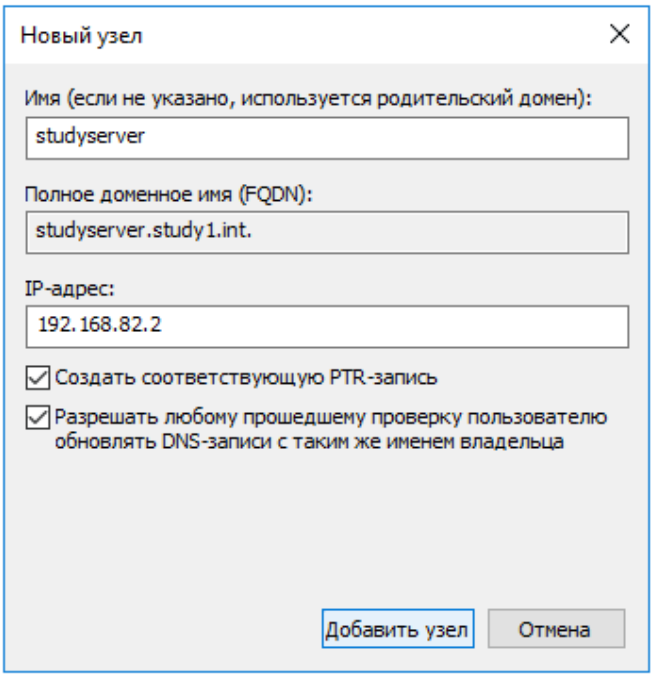

Рисунок 14.19 – Настройки узла

Так зона должна выглядеть в диспетчере DNS.

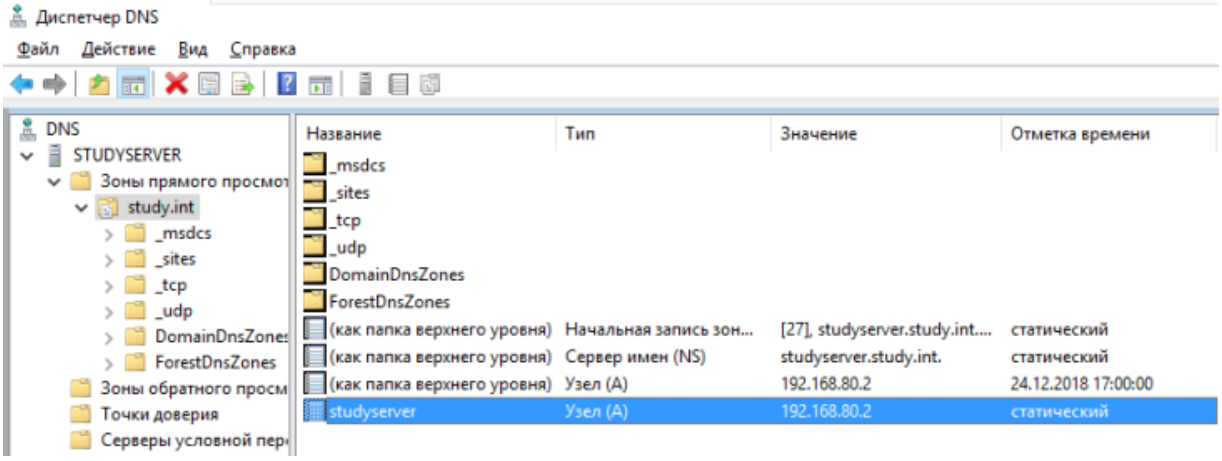

Рисунок 14.20 – Вид зоны

Также нужно создать зону обратного просмотра. Мастер запускается аналогичным образом.

22. В открывшемся мастере, нажать «Далее».

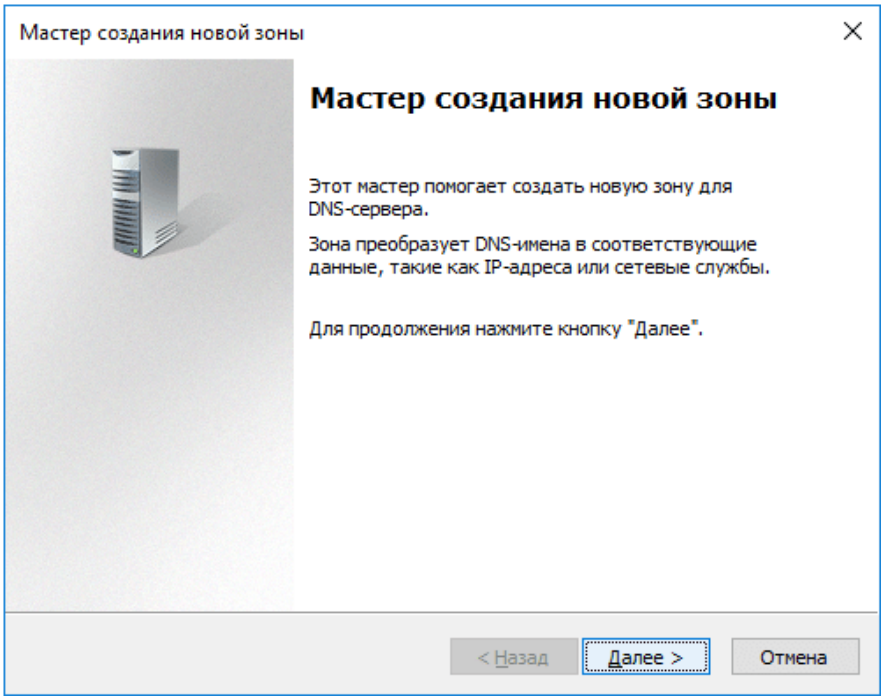

Рисунок 14.21 – Создание зоны обратного просмотра

23. Выбрать тип зоны — «Основная».

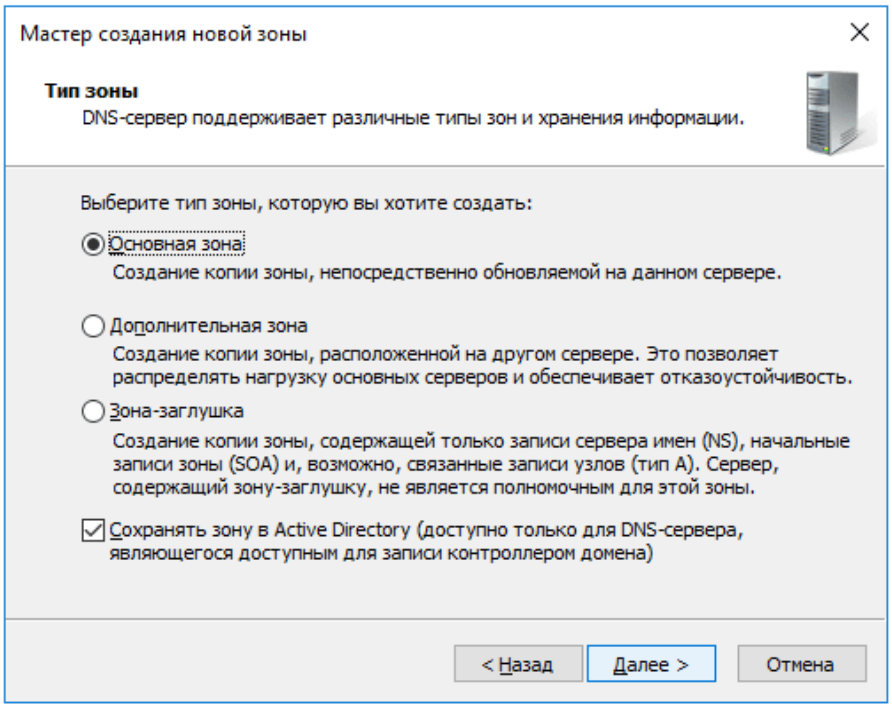

Рисунок 14.22 – Выбор типа зоны

24. Выбрать область репликации.

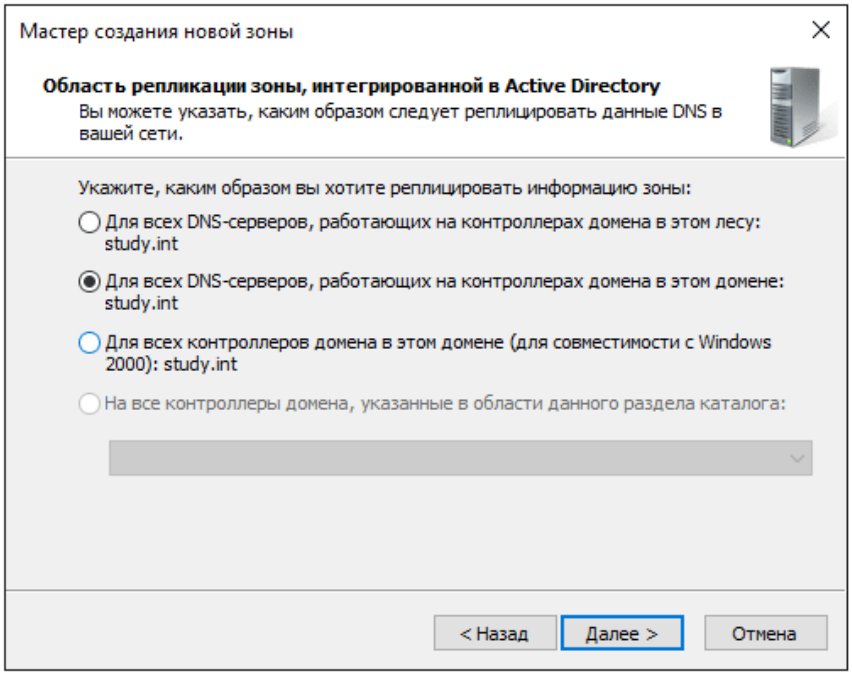

Рисунок 14.23 – Выбор области репликации

25. Выбрать тип зоны обратного просмотра IPv4.

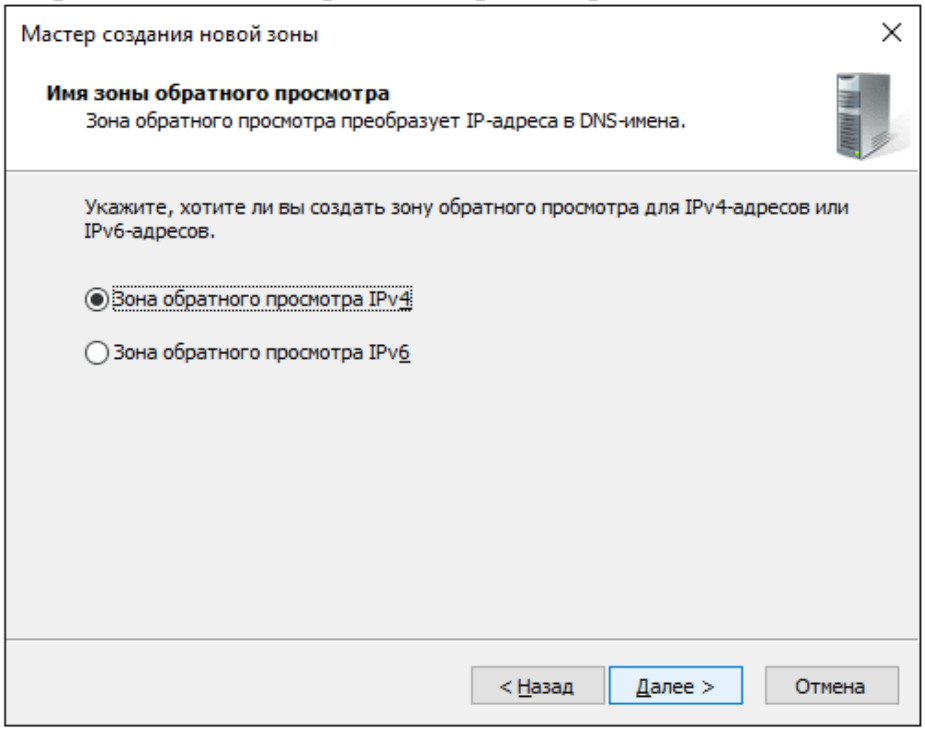

Рисунок 14.24 – Выбор зоны обратного просмотра

26. Задать идентификатор текущей сети.

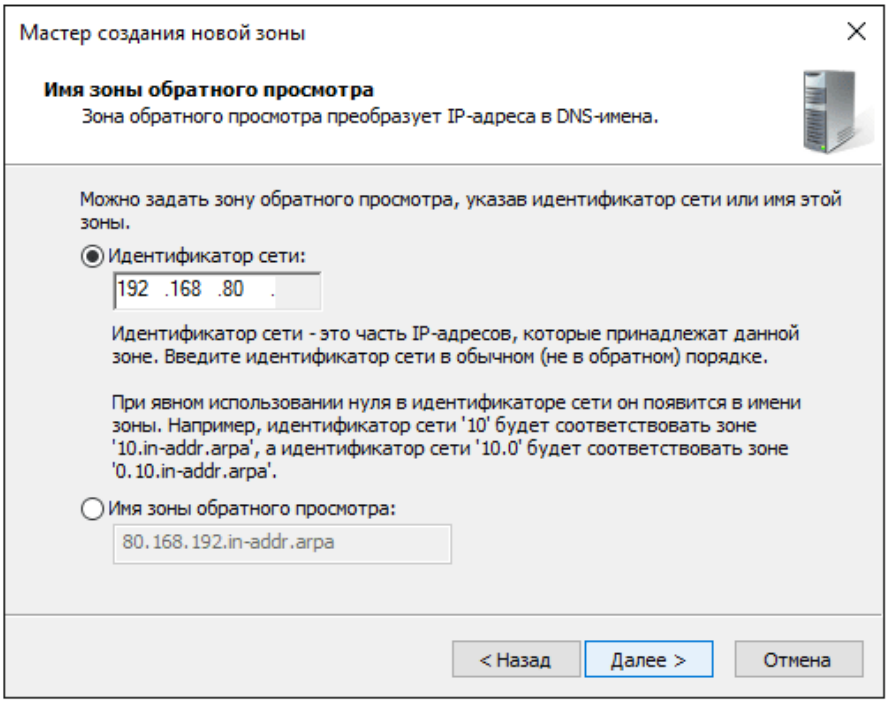

Рисунок 14.25 – Идентификатор сети

27. Выбрать настройки обновления.

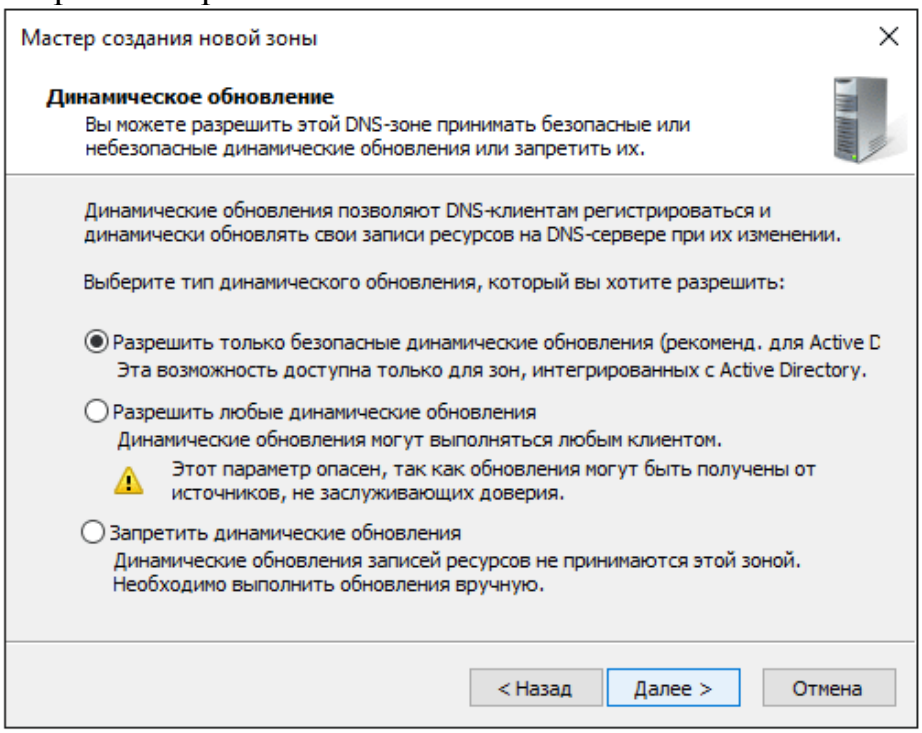

Рисунок 14.26 – Настройка обновлений

28. Завершить работу мастера, нажав «Готово».

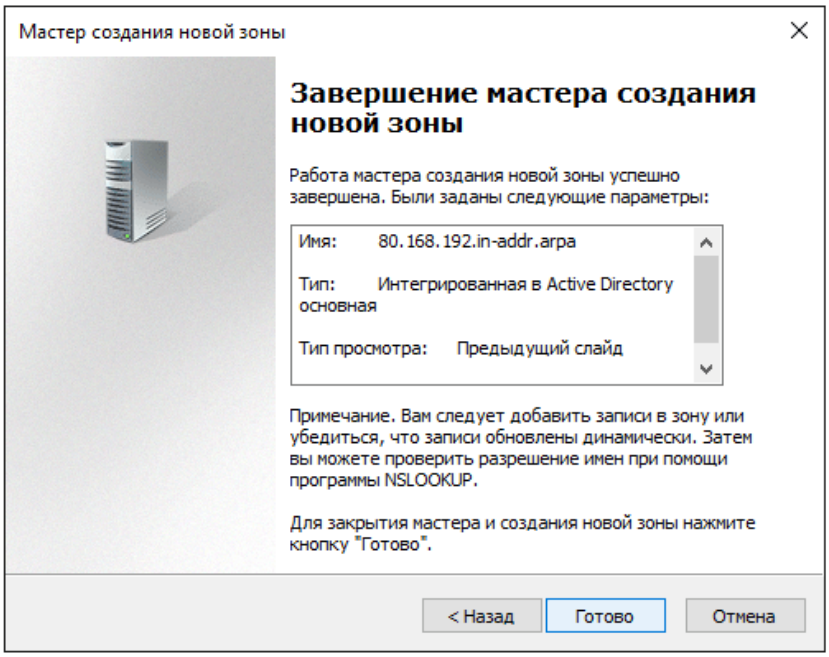

Рисунок 14.27 – Завершение создания зоны

Проверить корректность настройки, можно введя в командной строке команду nslookup <IP-адрес>

В ответе должен быть похожий результат.

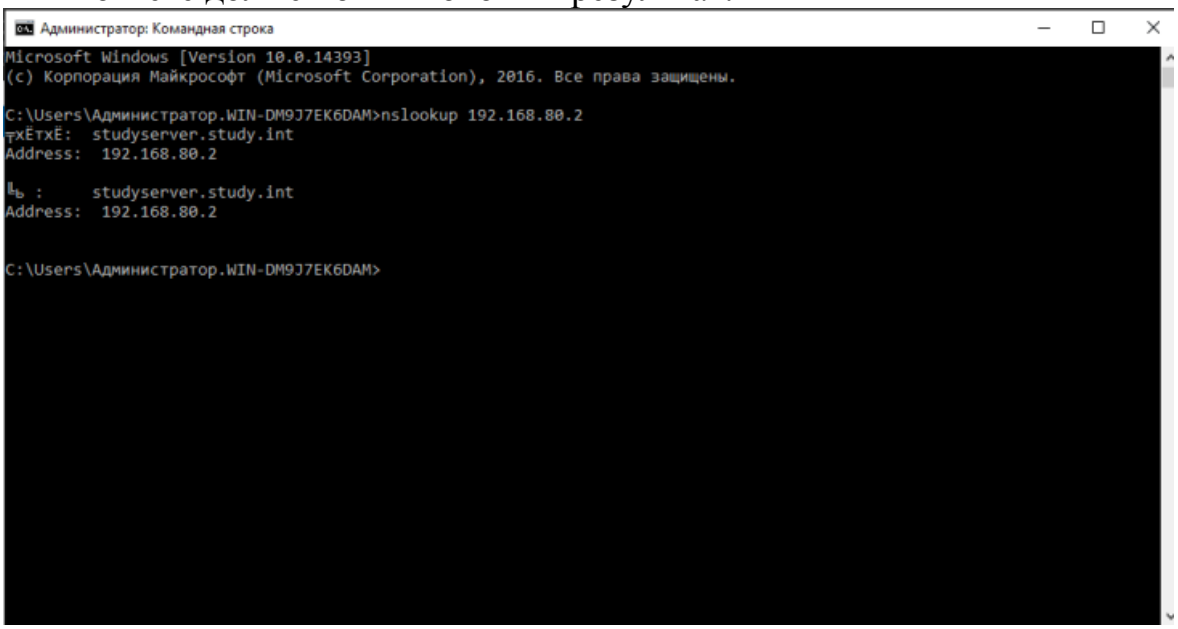

Рисунок 14.28 – Проверка работоспособности

Контрольные вопросы

1. Что делает DNS-сервер?
2. Какой утилитой из командной строки можно отправить тестовый DNS-запрос?
3. Что такое «зона» в терминологии DNS?
4. Зачем нужна зона прямого просмотра?
5. Зачем нужна зона обратного просмотра?

Лабораторная работа № 15 «Настройка DHCP-сервера для автоматической раздачи IP-параметров»

Теоретические сведения

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической настройки узла) — прикладной протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

Распределение IP-адресов

Протокол DHCP предоставляет три способа распределения IP-адресов:

– Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet-сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

– Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.

– Динамическое распределение. Этот способ аналогичен автоматическому распределению за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов. Это производится при помощи протокола обновления DNS, описанного в RFC 2136.

Опции DHCP

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети.

Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132.

Некоторыми из наиболее часто используемых опций являются:

– IP-адрес маршрутизатора по умолчанию;
– маска подсети;
– адреса серверов DNS;
– имя домена DNS.

Некоторые поставщики программного обеспечения могут определять собственные, дополнительные опции DHCP.

Задания к лабораторной работе

1. В диспетчере серверов выбрать пункт «Добавить роли и компоненты».

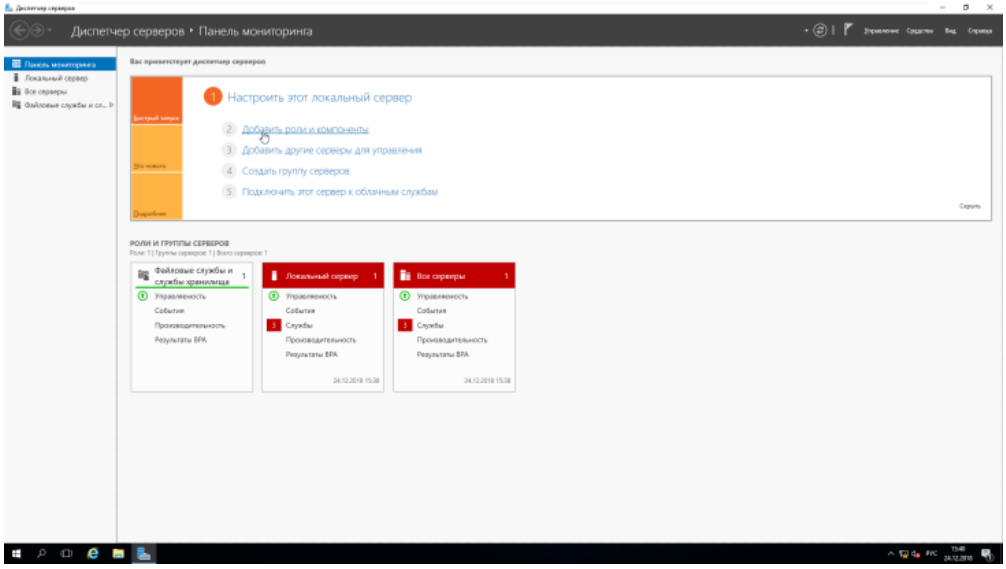

Рисунок 15.1 – Добавление роли

2. В открывшемся окне мастера нажать далее.

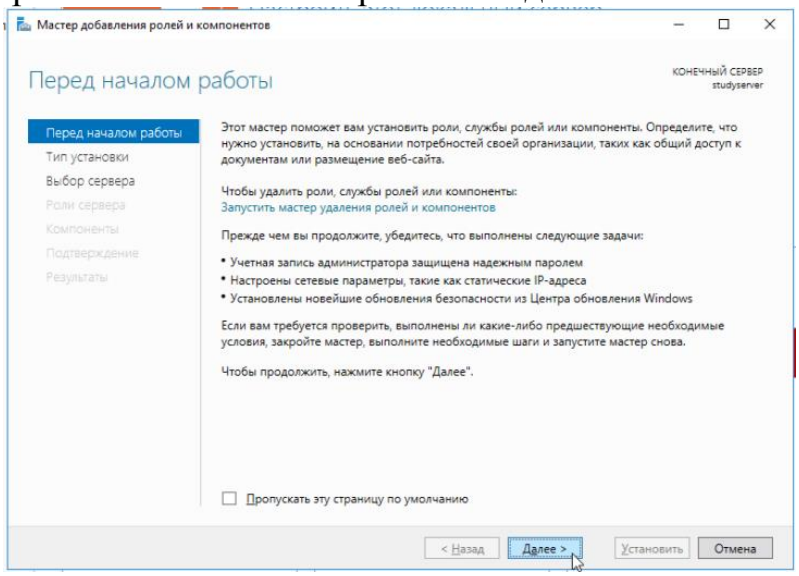

Рисунок 15.2 – Мастер добавления родей

3. Выбрать пункт: «Установка ролей и компонентов».

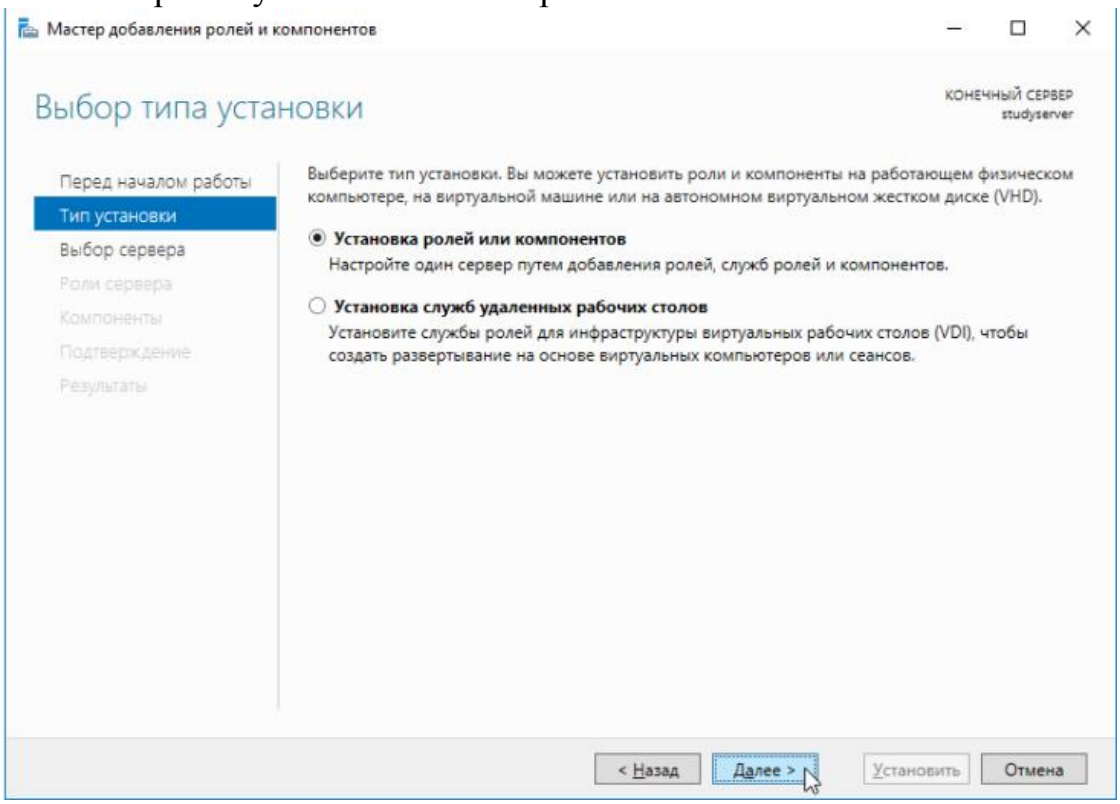

Рисунок 15.3 – Выбор типа установки

4. Выбрать сервер из списка.

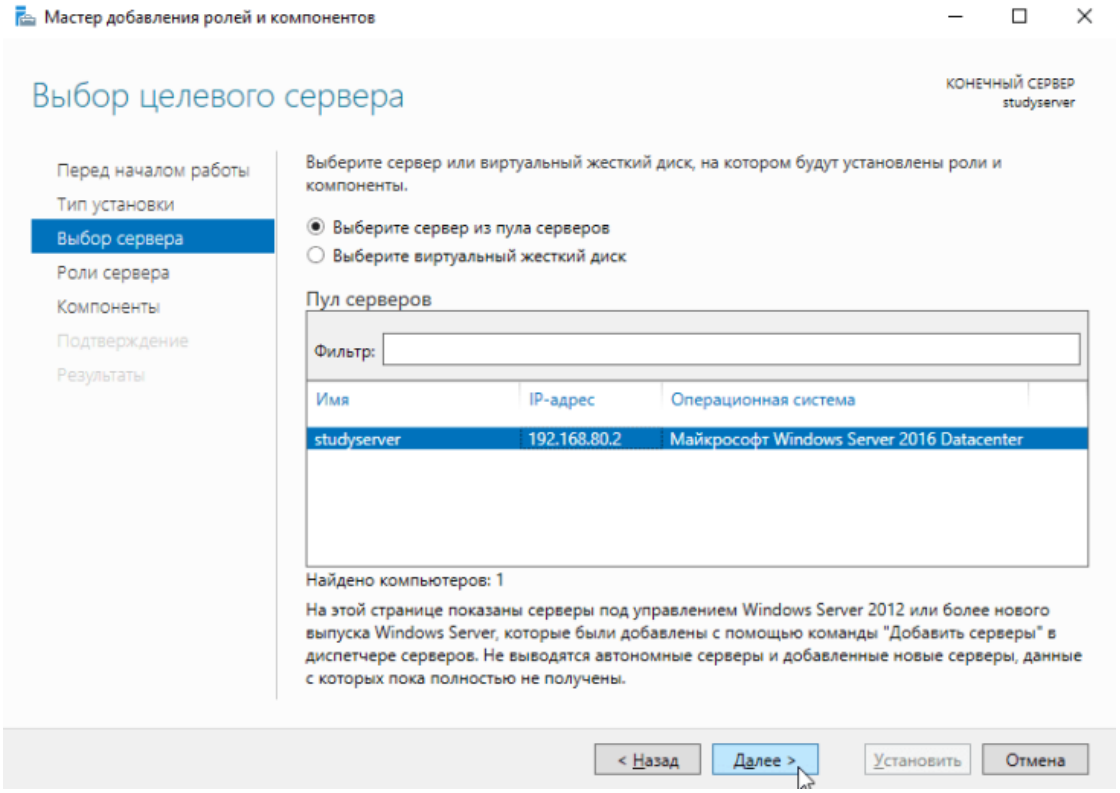

Рисунок 15.4 – Выбор сервера

5. Выбрать роль «DHCP-сервер».

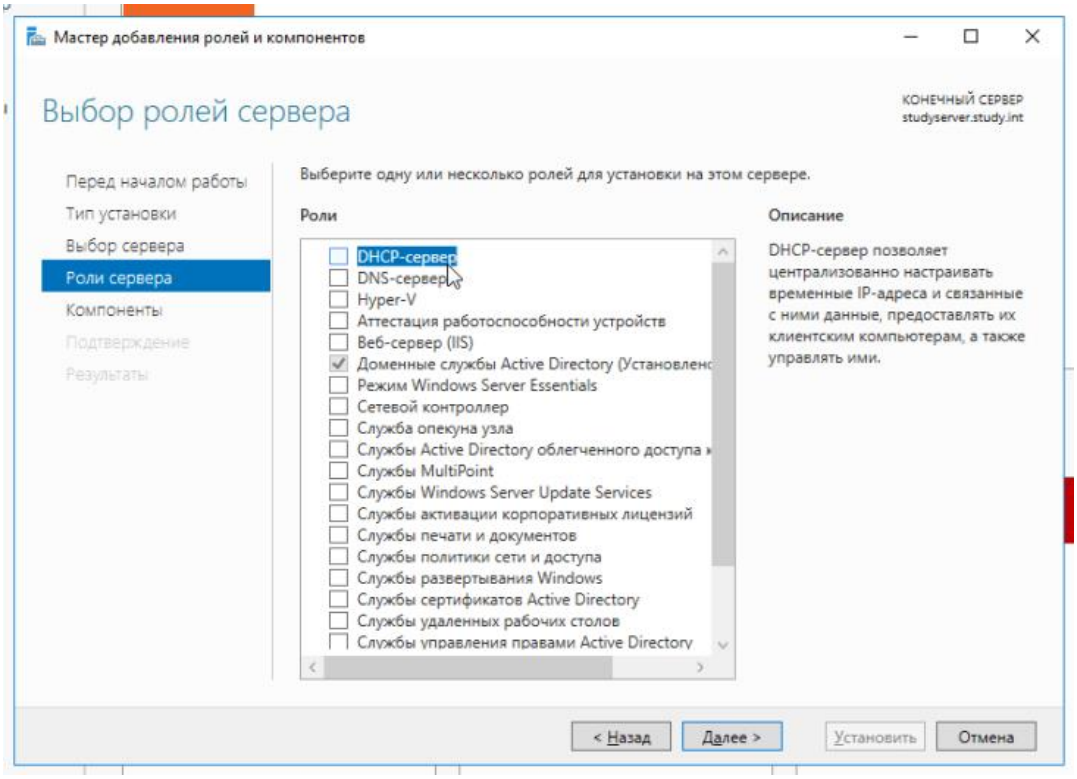

Рисунок 15.5 – Роль сервера

6. В появившемся окне предлагают установить необходимые для продолжения компоненты. Нажать «Добавить компоненты».

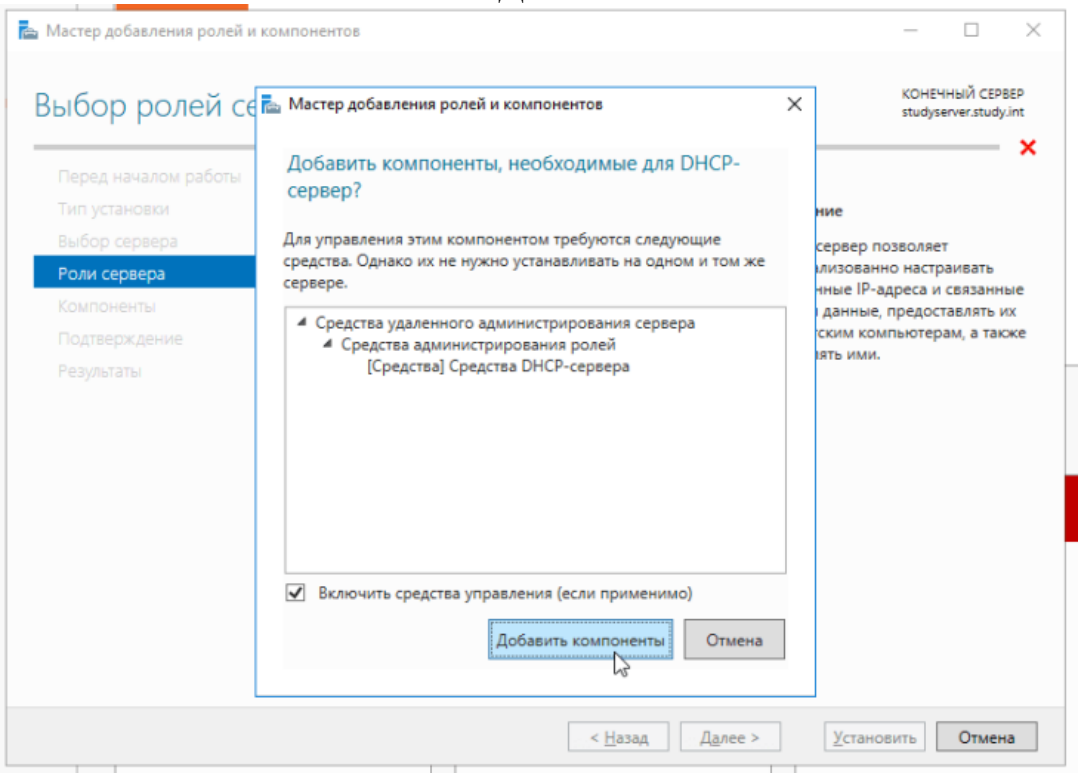

Рисунок 15.6 – Добавление компонентов

7. В окне выбора компонентов нажать «Далее», поскольку необходимые компоненты были выбраны в предыдущем пункте.

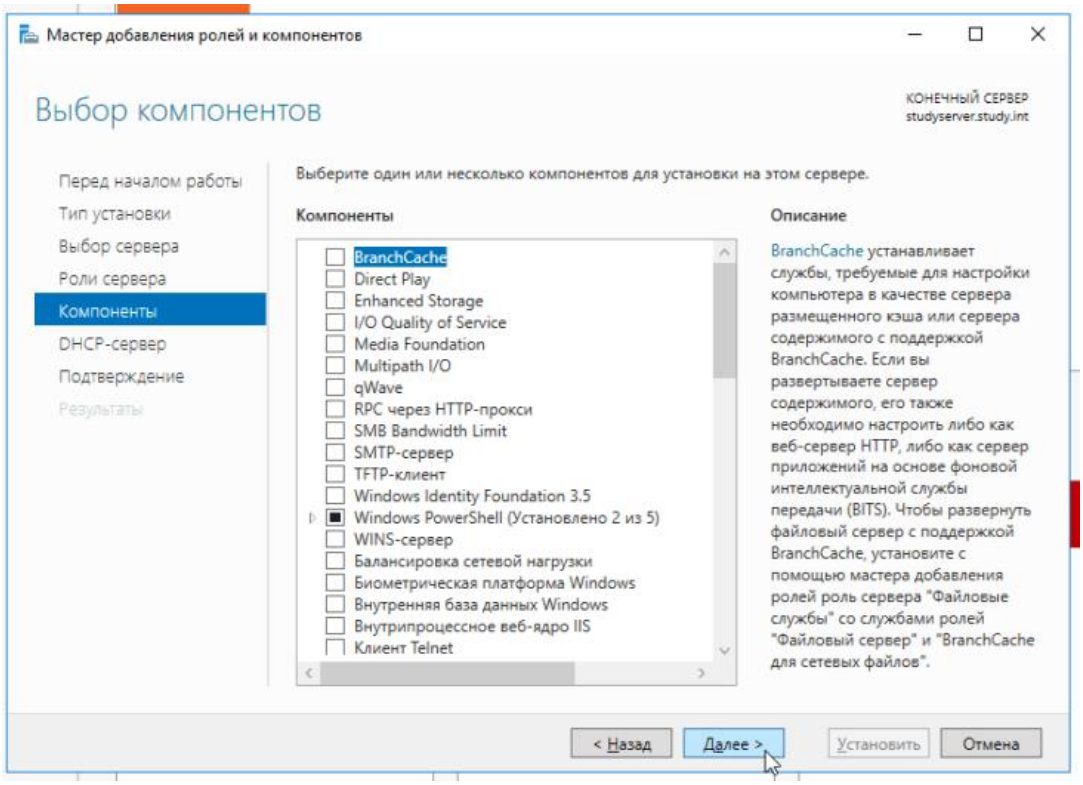

Рисунок 15.7 – Выбор компонентов

8. В следующем окне приведена краткая информация о роли DHCP — сервера. Ознакомиться с ней и нажать «Далее».

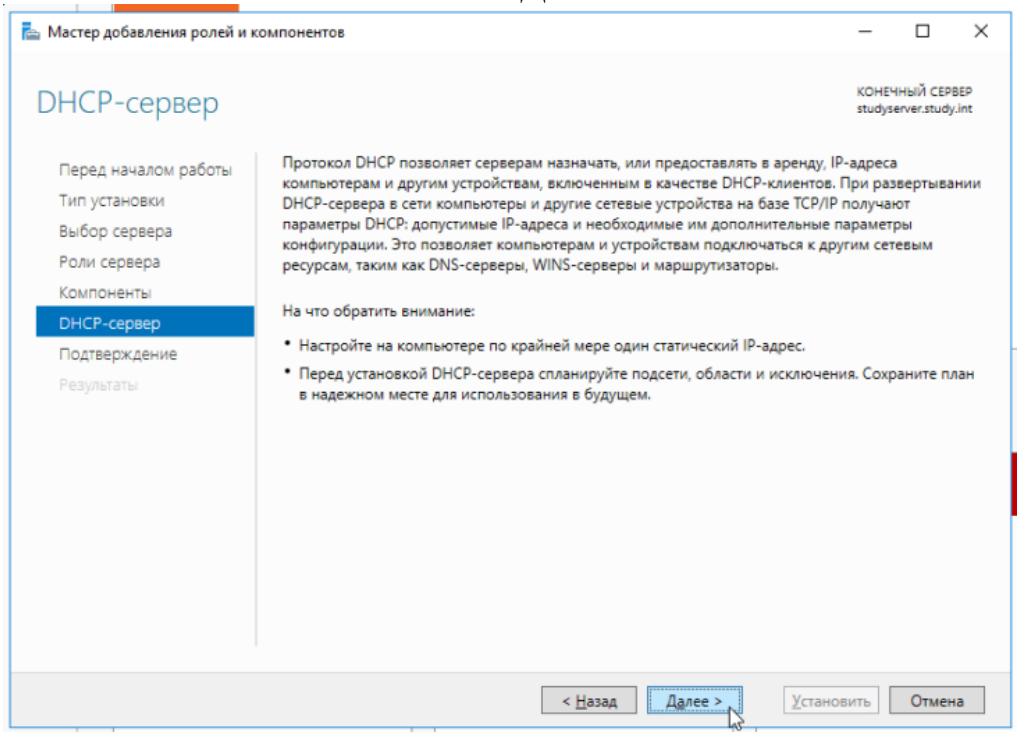

Рисунок 15.8 – Информация о роли

9. Ознакомиться со списком устанавливаемых компонентов и нажать «Установить».

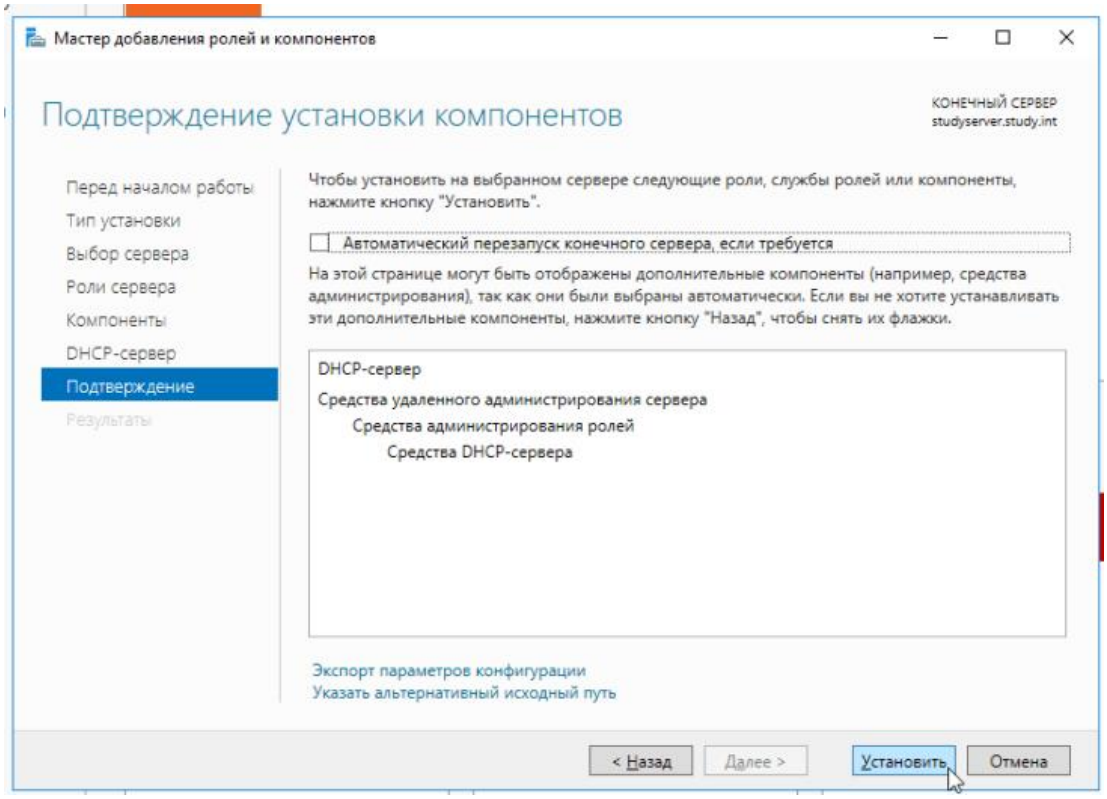

Рисунок 15.9 - Подтверждение

10. Выбрать пункт «Завершение настройки DHCP», для того чтобы настроить сервер DHCP.

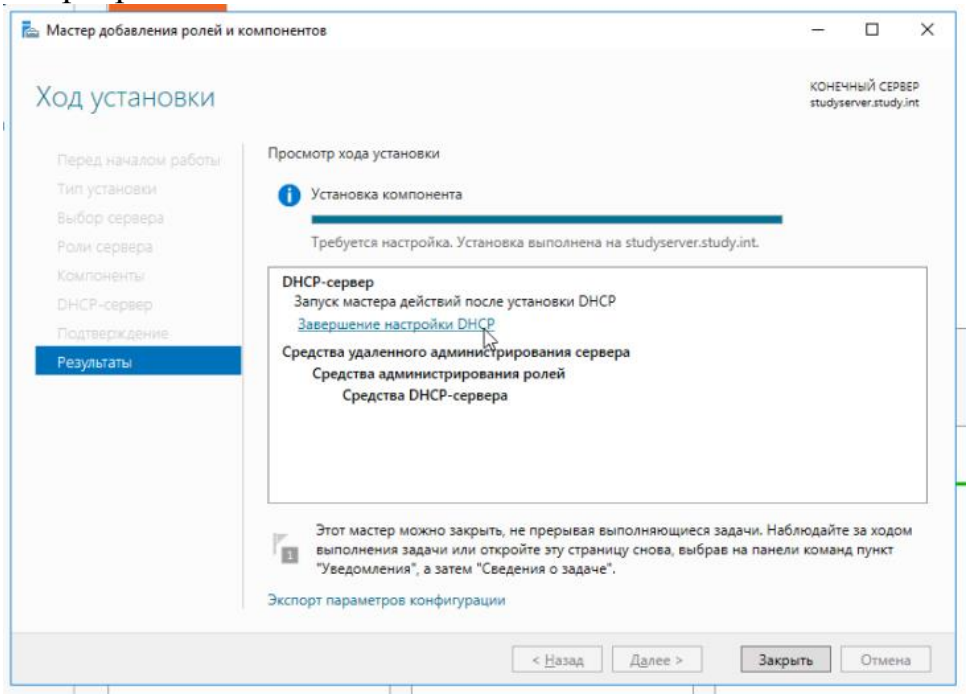

Рисунок 15.10 – Завершение установки

11. Появляется уведомление о том, что далее будут созданы две локальные группы безопасности для управления доступом к серверу DHCP, а затем будет произведена авторизация сервера DHCP в Active Directory. Нажать кнопку «Далее».

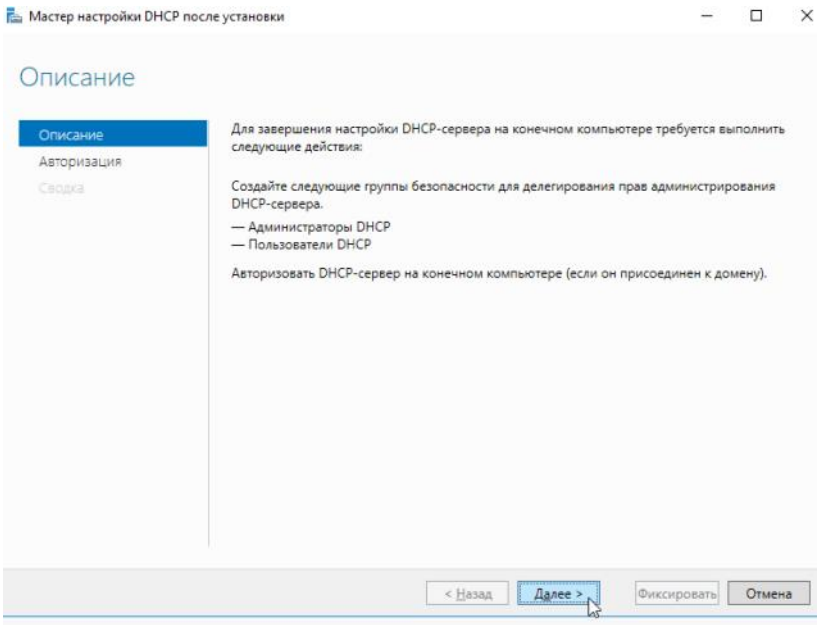

Рисунок 15.11 – Мастер настройки DHCP

12. В разделе «Авторизация», в пункте «Использовать учетные данные следующего пользователя» указываем учетную запись с правами администратора домена. Нажать на кнопку «Фиксировать».

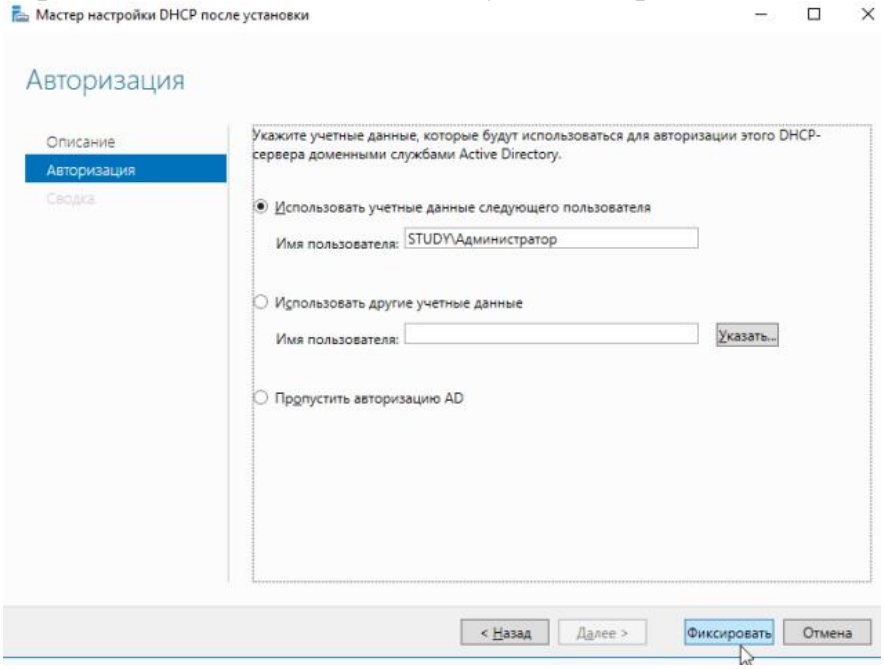

Рисунок 15.12 - Авторизация

13. Теперь DHCP-сервер авторизован в Active Directory, а также созданы необходимые группы безопасности для управления доступом к DHCP. Нажать на кнопку «Закрыть».

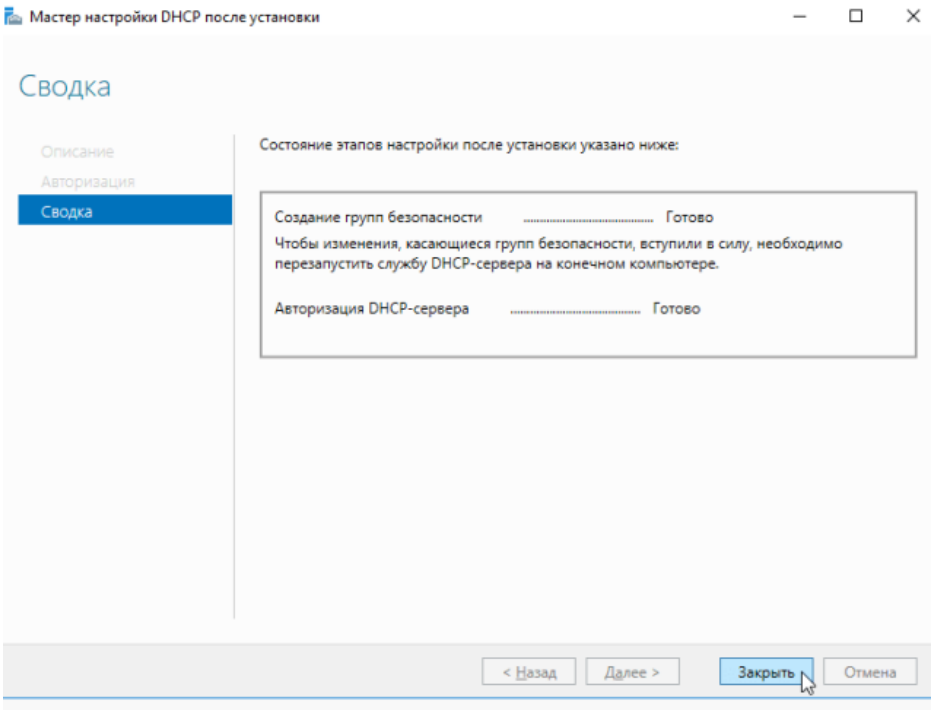

Рисунок 15.13 – Завершение авторизации

14. В мастере настройке ролей, также нажать «Закрыть».

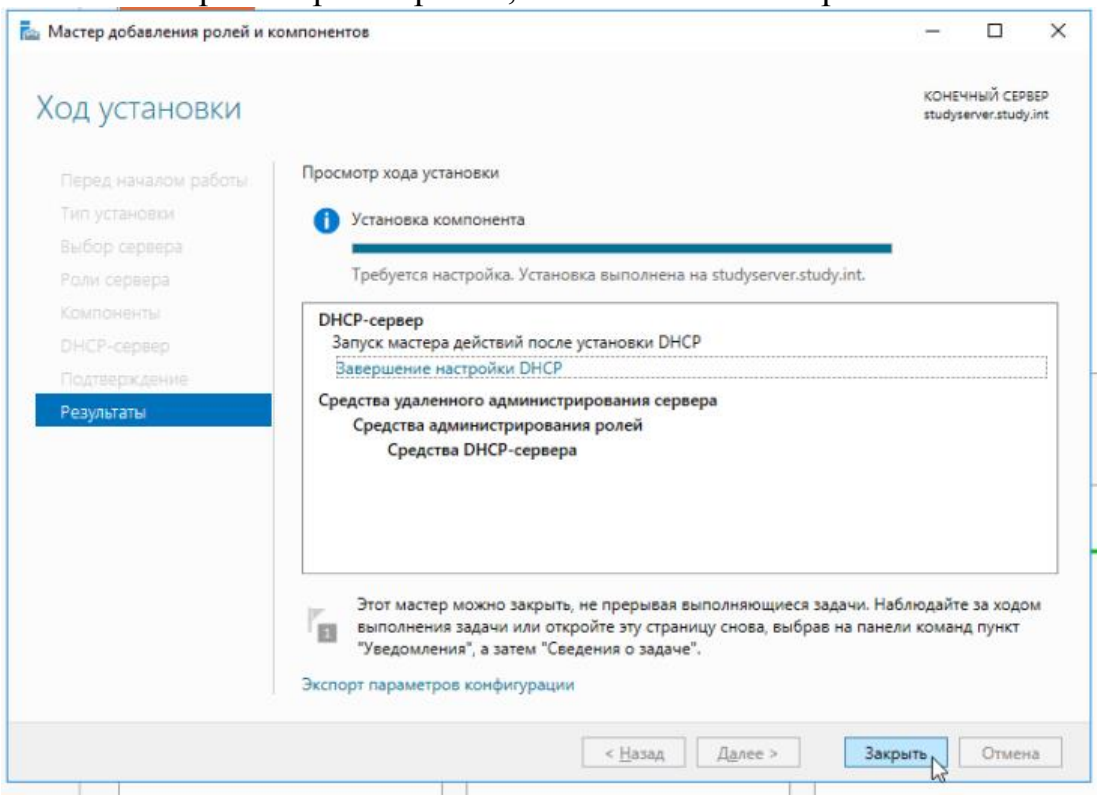

Рисунок 15.14 – Закрытие установки

Настройка DHCP-сервера

15. В диспетчере серверов, в пункте «Средства», выбрать DHCP.

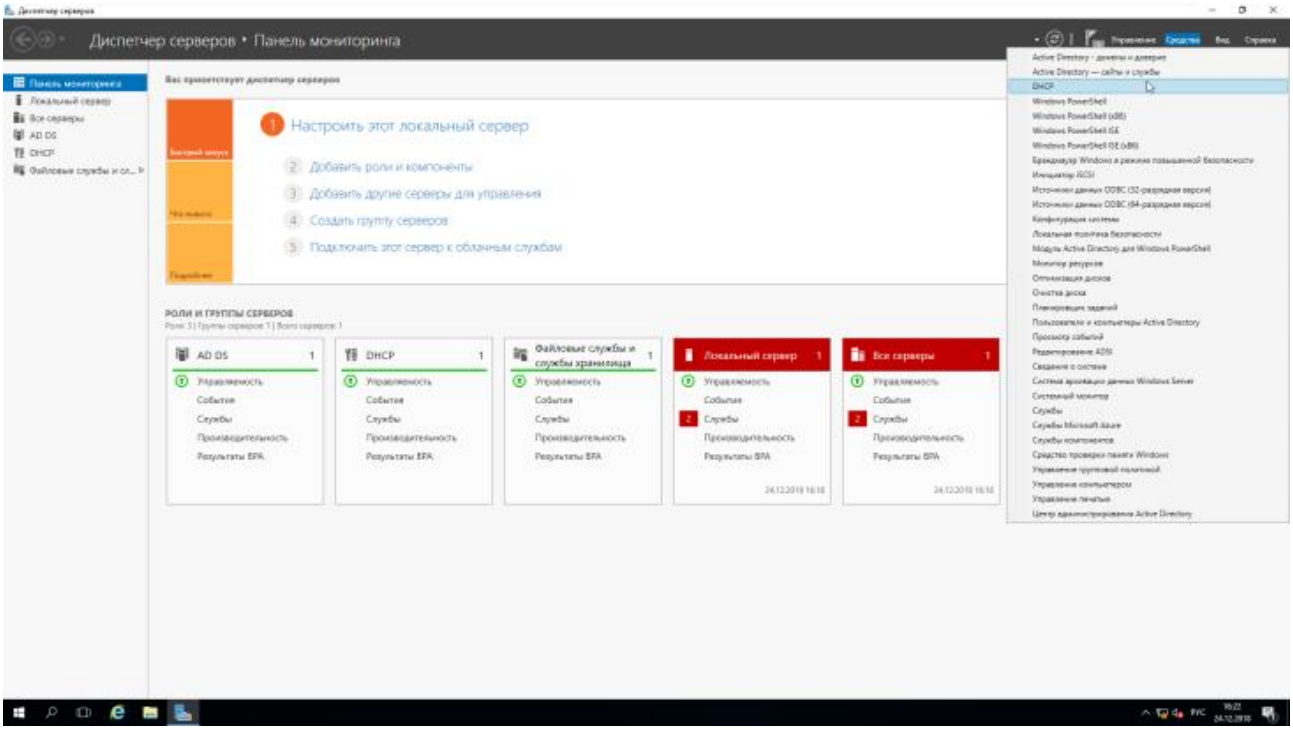

Рисунок 15.15 – Выбор DHCP сервера

16. В открывшемся окне настройки, выбрать созданный сервер и на вкладке IPv4, щелчком правой кнопки мыши открыть контекстное меню, в котором выбрать пункт «Создать область».

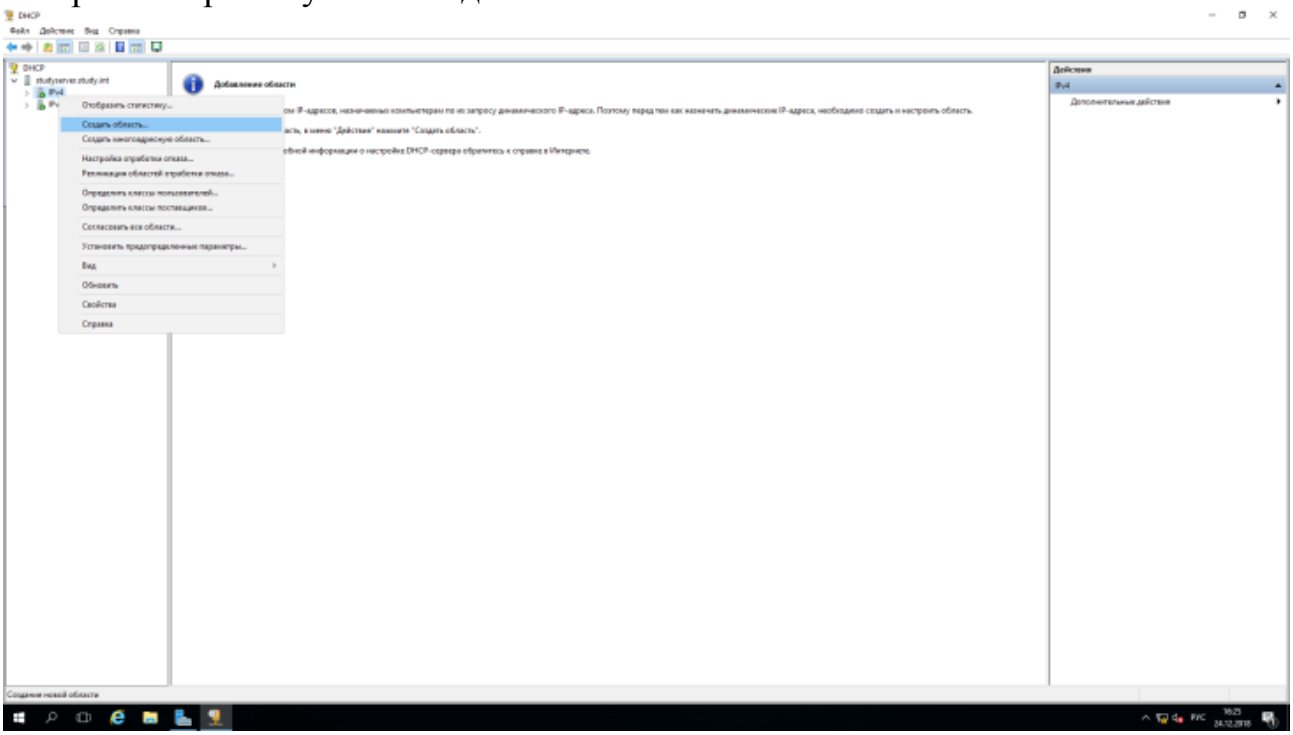

Рисунок 15.16 – Создание области

17. Открывается «Мастер создания областей». В поле «Имя», указать имя для нового диапазона адресов.

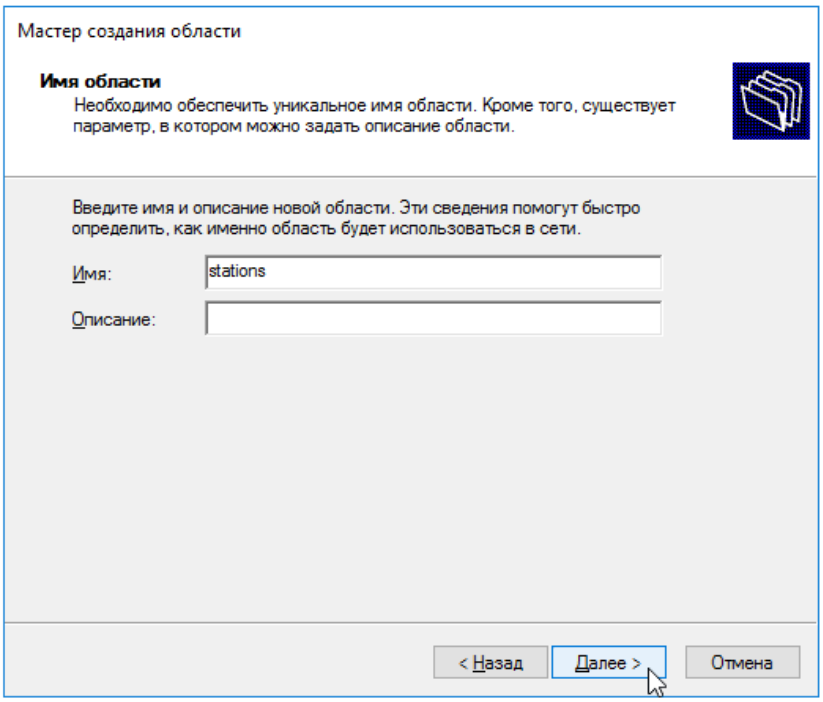

Рисунок 15.17 – Мастер создания области

18. Указать маску подсети и диапазон адресов, из которого сервер DHCP будет раздавать IP-адреса для устройств в локальной сети. Нажать на кнопку «Далее».

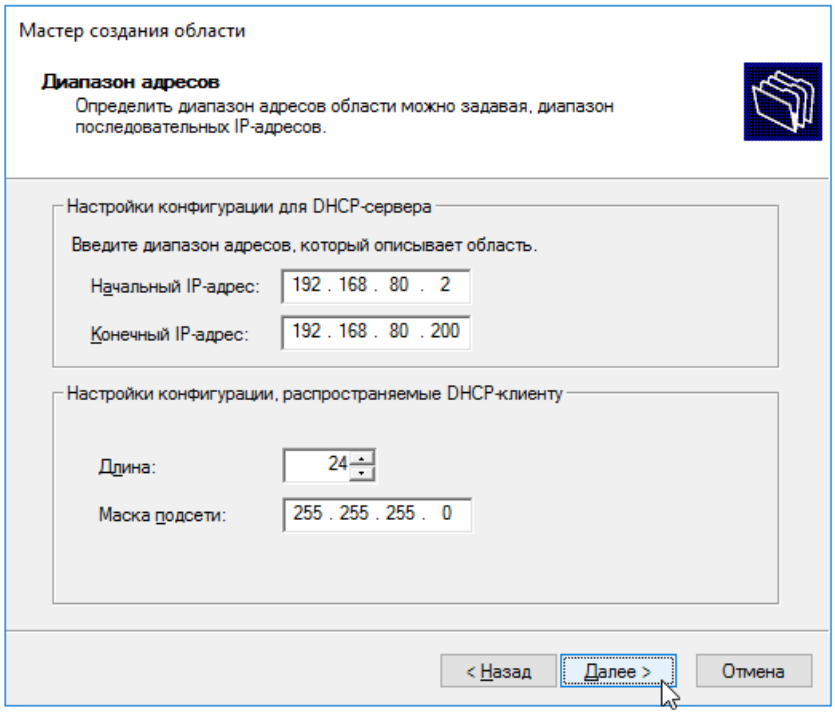

Рисунок 15.18 – Диапазон адресов

19. Следует указать диапазон, для которого сервер DHCP не будет раздавать настройки.

Это может пригодиться, если вы знаете, что в определенном диапазоне адресов находятся сервера, принтеры или другие устройства, которым уже

присвоен статический IP-адрес. В таком случае нужно исключить эту часть диапазона, так как IP-адреса из него уже используются. Также нужно исключить IP-адрес, который присвоен шлюзу.

Чтобы исключить один IP-адрес достаточно заполнить только поле «Начальный IP-адрес».

Указать часть диапазона, которую нужно исключить, и нажать на кнопку «Добавить».

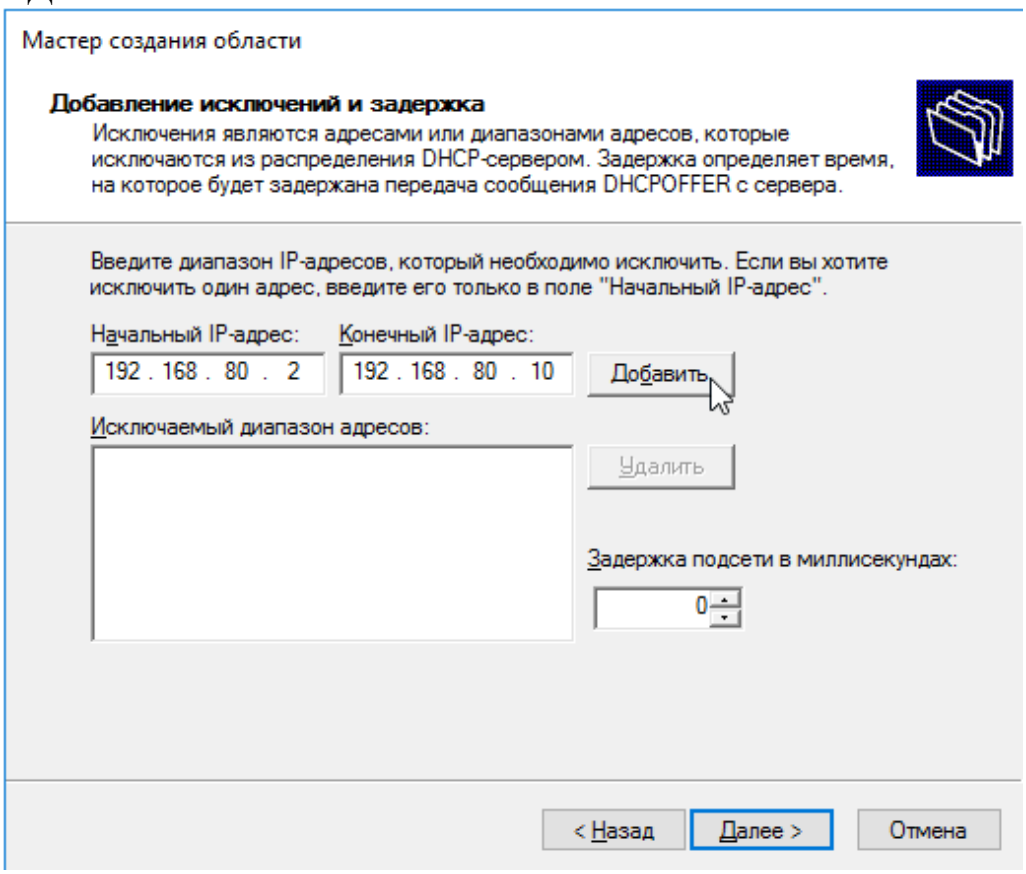

Рисунок 15.19 – Настройка исключений

20. Далее можно выбрать на какое время IP-адреса будут выдаваться устройствам в аренду. Можно оставить настройки без изменений и нажать на кнопку «Далее».

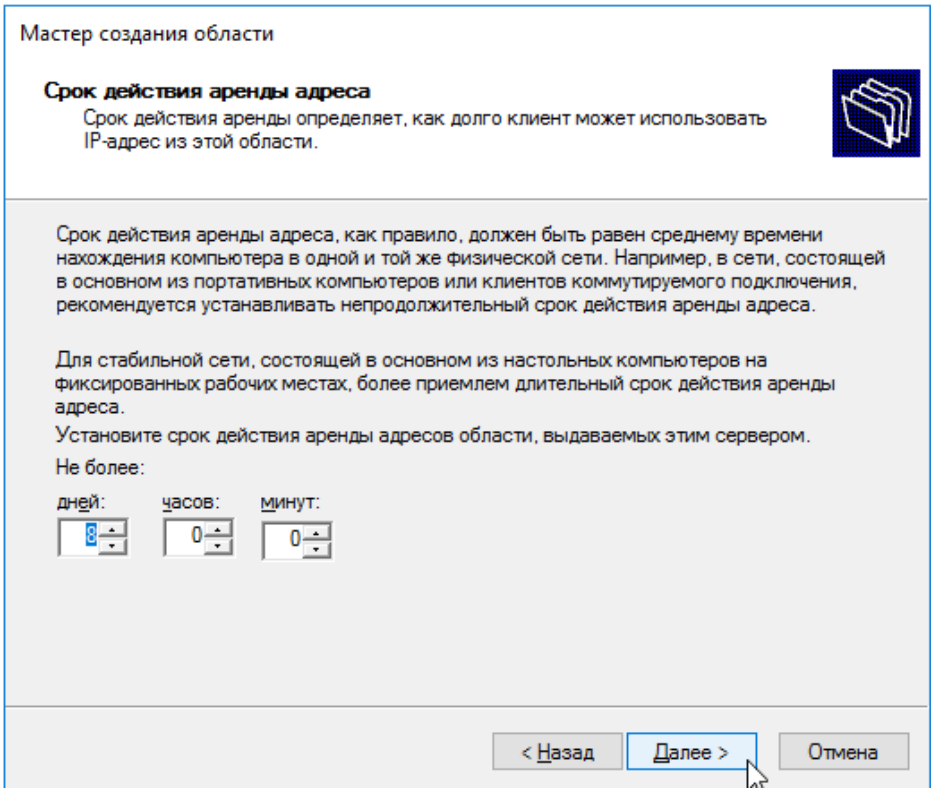

Рисунок 15.20 – Настройка срока аренды

21. Необходимо указать сетевые настройки (шлюз, DNS), которые сервер DHCP будет раздавать для устройств в локальной сети. Выбрать пункт «Да, настроить эти параметры сейчас».

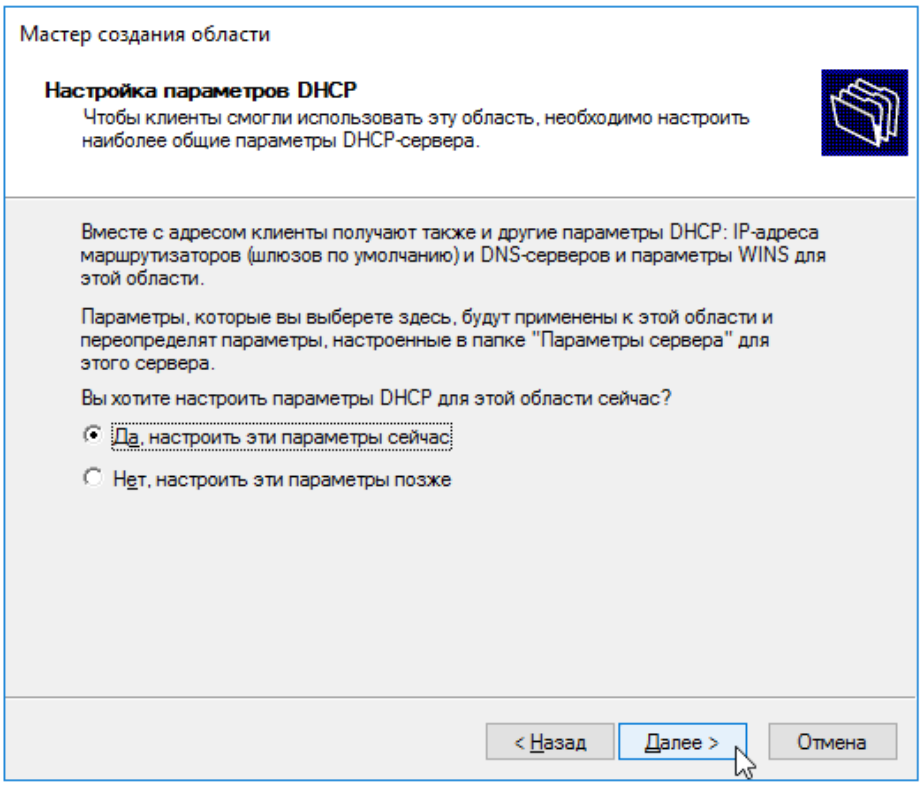

Рисунок 15.21 – Настройка параметров

22. В поле «IP-адрес» указать IP-адрес вашего шлюза (в данном цикле лабораторных работ это адрес машины, на которой устанавливается сервер) и нажать на кнопку «Добавить». Затем нажать «Далее».

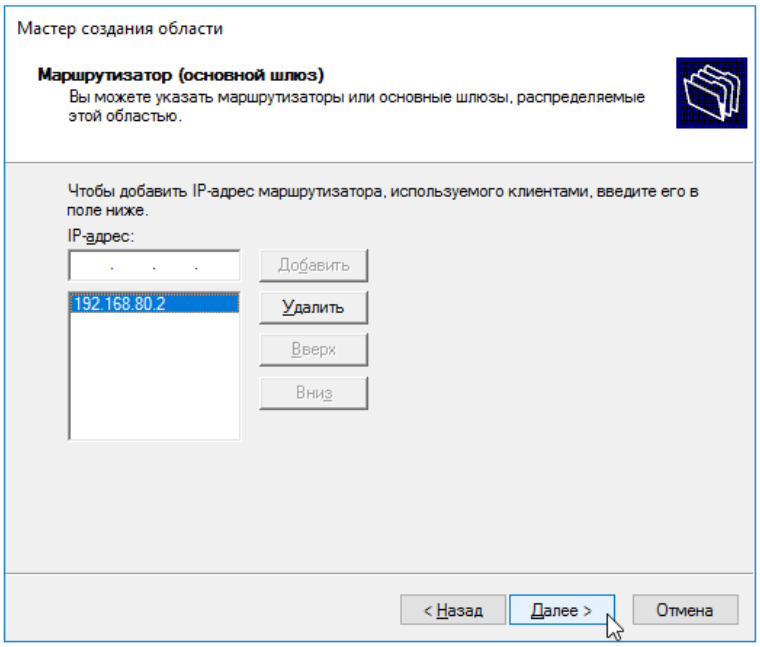

Рисунок 15.22 – Настройка шлюза

23. В поле «Родительский домен» указать имя домена, созданного в предыдущей лабораторной работе. В поле «IP-адрес» указать IP-адрес сервера DNS (указать так же адрес текущей машины). Нажать на кнопку «Далее».

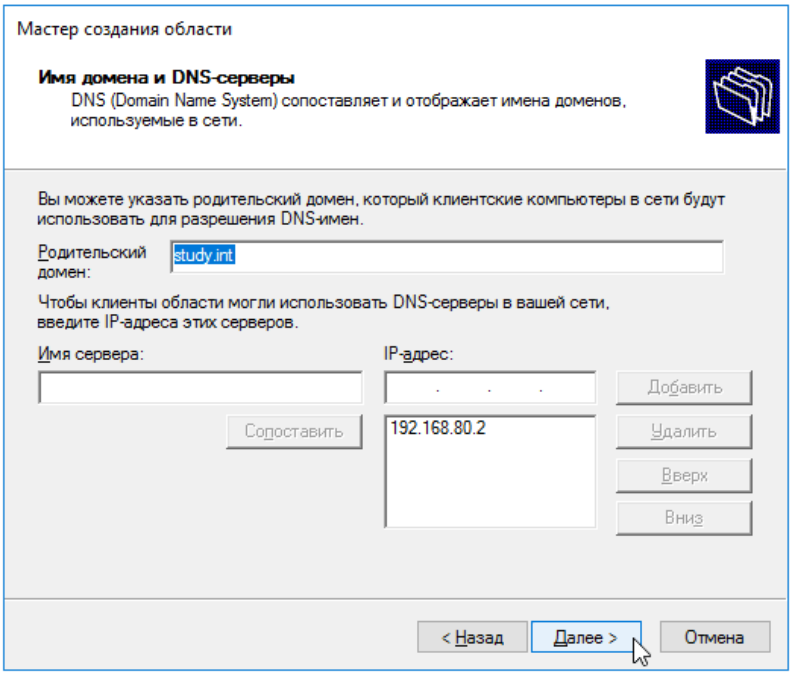

Рисунок 15.23 – Настройка домена и DNS

24. WINS-сервер в данном случае использоваться не будет, поэтому нажать — «Далее».

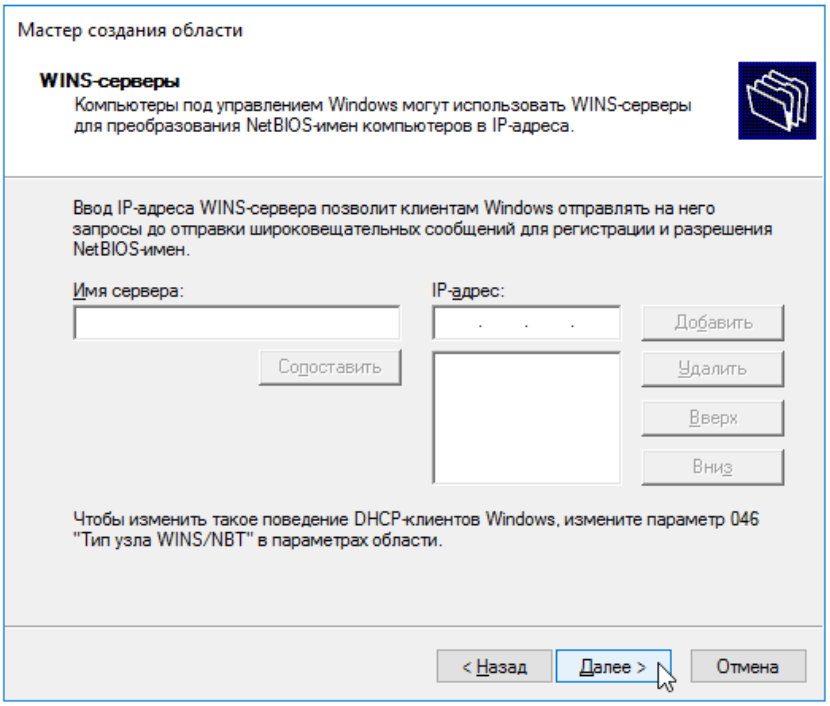

Рисунок 15.24 – Настройка WINS-сервера

25. Активировать созданную область, выбрав пункт «Да, я хочу активировать эту область сейчас» и нажать «Далее».

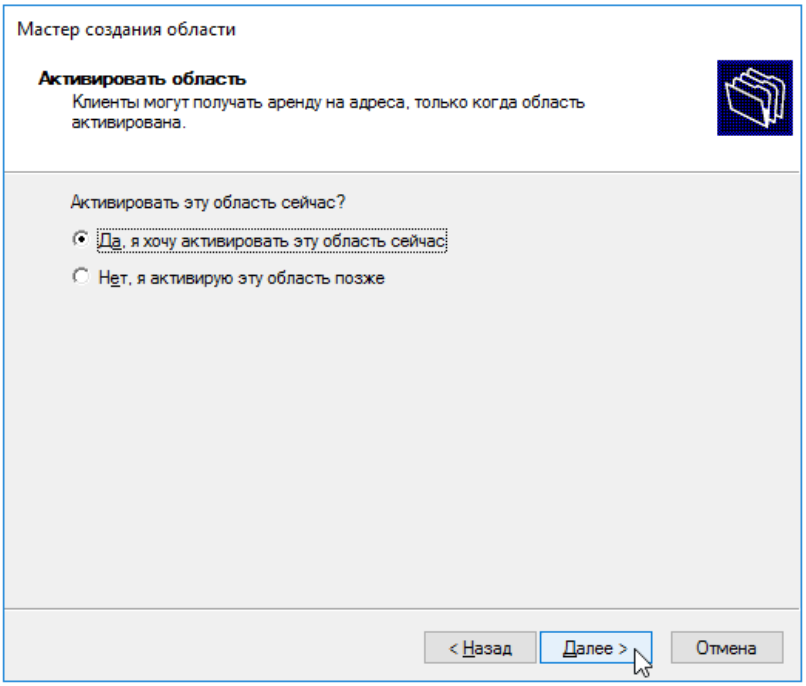

Рисунок 15.25 – Активация области

26. Настройка сервера DHCP завершена. Теперь все устройства, подключаемые к локальной сети, будут получать сетевые настройки (IP-адрес, маска подсети, шлюз, DNS) и смогут взаимодействовать друг с другом. Нажать на кнопку «Готово».

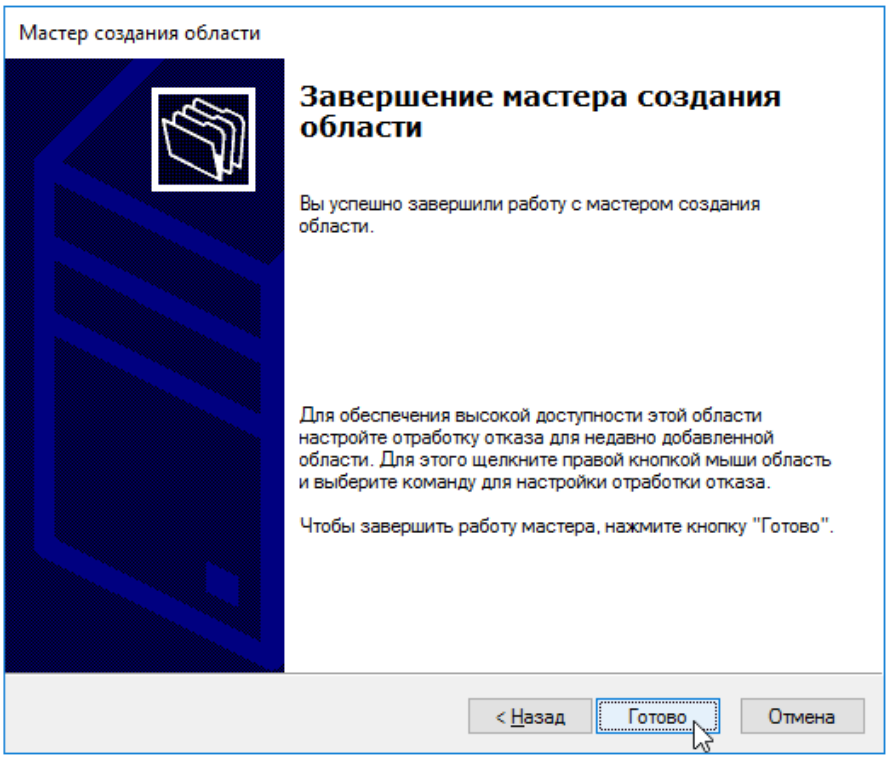

Рисунок 15.26 – Завершение настройки

Контрольные вопросы

1. Каковы основные цели и задачи протокола DHCP?
2. Что такое «аренда адреса» и какова её роль?
3. В чём разница между статическим, автоматическим и динамическим выделением IP-адресов?
4. Помимо IP-адреса и маски сети, какие ещё параметры может передать DHCP-сервер?
5. Как интеграция DHCP-сервера может упростить управление сетью?

Лабораторная работа № 16 «Удаленное управление сетевым устройством по протоколу SSH»

Теоретические сведения

SSH (Secure Shell) — криптографический сетевой протокол прикладного уровня, предназначенный для безопасного удаленного управления операционной системой и туннелирования TCP-соединений.

Удаленный доступ - это частный случай соединения компьютеров через глобальные связи. От обычных вариантов с использованием мостов и маршрутизаторов удаленный доступ отличается тем, что одной из взаимодействующих сторон является не локальная сеть, а отдельный компьютер без сетевого адаптера. Кроме того, удаленный доступ обычно использует низкоскоростные соединения по коммутируемым телефонным аналоговым сетям. Реже используются сети ISDN или X.25.

Компоненты удаленного доступа

Большинство решений для удаленного доступа базируются на тех же основных компонентах, что и обычные локальные сети:

– некоторое количество машин, работающих в качестве информационных серверов,

– большое количество клиентских машин или ноутбуков, имеющих доступ к разделяемым данным, хранящимся на серверах,

– программная и аппаратная инфраструктура, обеспечивающая взаимодействие серверных и клиентских машин.

Однако в то время, как в локальных сетях инфраструктура передачи данных обычно состоит из сетевых адаптеров, кабелей и маршрутизаторов, системы удаленного доступа добавляют к ним модемы, телефонные линии, возможно, некоторое количество выделенных линий, а также специальное программное и аппаратное обеспечение удаленного доступа.

Ключевые особенности и преимущества SSH:

– Шифрование всего трафика: Защита от перехвата и анализа (сниффинга).

– Аутентификация: Проверка подлинности как сервера для клиента, так и клиента для сервера.

– Целостность данных: Обнаружение подмены или искажения передаваемой информации.

– Сжатие данных: Повышение эффективности на медленных каналах связи.

Протокол состоит из трех основных уровней:

1. Транспортный уровень (Transport Layer):

– Обеспечивает первоначальное согласование версий, обмен ключами, шифрование, сжатие и целостность.

– Происходит аутентификация сервера на основе его открытого ключа (проверка "отпечатка" — fingerprint).

– Создается безопасный канал поверх TCP.

2. Уровень аутентификации пользователя (User Authentication Layer):

– Происходит аутентификация клиента на сервере.

– Основные методы:

– По паролю: Простой, но уязвимый к brute-force атакам.

– По открытому ключу (Public Key): Наиболее безопасный и рекомендуемый метод. Клиент использует свой закрытый ключ, а сервер проверяет соответствующий открытый ключ.

– По Kerberos, по host-based ключам и др.

3. Уровень соединения (Connection Layer):

– Управляет интерактивными сессиями, портами и туннелями внутри установленного безопасного канала.

– Мультиплексирует несколько логических каналов (сессий) в одном SSH-соединении.

Базовые криптографические понятия SSH:

– Асимметричное шифрование (RSA, ECDSA, Ed25519): Используется для аутентификации (серверной и клиентской) и обмена сессионными ключами.

– Симметричное шифрование (AES, ChaCha20): Используется для шифрования всего трафика сессии после handshake. Ключ генерируется для каждой сессии.

– Хеш-функции (SHA-2): Используются для обеспечения целостности.

– Ключевая пара: Открытый (публичный) ключ (id_rsa.pub) и закрытый (приватный) ключ (id_rsa). Приватный ключ хранится в секрете и защищен парольной фразой (passphrase). Публичный клюк копируется на сервер.

Таблица 16.1 - Ключевые команды SSH

Действие	**Команда (на Client, если не указано иное)**	**Пояснение**
Подключение	*ssh user@host*	Базовое подключение
Подключение к нестандартному порту	*ssh -p 2222 user@host*	Порт указывается флагом -p
Генерация ключа (Ed25519)	*ssh-keygen -t ed25519 -a 100 -C "ваш комментарий"*	-a — число циклов KDF (усиливает стойкость)
Копирование ключа на сервер	*ssh-copy-id -p 2222 user@host*	Автоматически добавляет ключ в ~/.ssh/authorized_keys
Ручное копирование ключа	*cat ~/.ssh/id_ed25519.pub | ssh user@host 'cat >> .ssh/authorized_keys'*	Если ssh-copy-id недоступен
Проверка подключения по ключу	*ssh -o PasswordAuthentication=no user@host*	Проверяет, работает ли только ключ
Создание локального туннеля	*ssh -L 33306:localhost:3306 user@host*	Проброс порта с сервера на клиент
Создание удаленного туннеля	*ssh -R 8080:localhost:80 user@host*	Проброс порта с клиента на сервер
Копирование файла НА сервер	*scp -P 2222 file.txt user@host:/путь/*	scp использует -P (заглавная) для порта
Копирование файла С сервера	*scp user@host:/путь/file.txt .*	Точка означает текущую директорию клиента

Продолжение Таблицы 16.1 - Ключевые команды SSH

Действие	**Команда (на Client, если не указано иное)**	**Пояснение**
Запуск ssh-agent	*eval "$(ssh-agent -s)"*	Запуск и настройка переменных окружения
Добавление ключа в агент	*ssh-add ~/.ssh/id_ed25519*	Запрос парольной фразы и кэширование
Просмотр логов сервера (в реальном времени)	*sudo tail -f /var/log/auth.log*	Выполнять на Server!

Задания к лабораторной работе

Предварительная подготовка:

1. Разверните две виртуальные машины (или используйте физический хост и виртуальную машину): одна будет SSH-сервером (например, Ubuntu Server), вторая — SSH-клиентом (например, Ubuntu Desktop).

2. Убедитесь, что машины находятся в одной сети и могут обмениваться ICMP-пакетами (ping).

3. На сервере убедитесь, что установлен и запущен пакет openssh-server (sudo systemctl status ssh).

Первичная настройка сети и определение IP-адресов:

1. На Server:

– Войдите под пользователем.

– Узнайте IP-адрес.

2. На Client:

– Войдите в систему.

– Узнайте свой IP-адрес.

– Проверьте связь с сервером: Выполните ping <адрес_сервера> (например, ping 192.168.56.101). Должны приходить ответы.

Установка необходимого ПО:

1. На ВМ Server (в терминале):

sudo apt update *# Обновление списка пакетов*

sudo apt install openssh-server –y *# Установка SSH-сервера*

sudo systemctl status ssh *# Проверка, что служба запущена*

Должна быть зелёная надпись active (running).

2. На ВМ Client: SSH-клиент уже предустановлен в Ubuntu Desktop. Для Windows можно использовать PowerShell (встроенный ssh) или Putty.

Первое подключение по SSH (с паролем):

1. На ВМ Client откройте терминал.
2. Введите команду: ssh labuser@<адрес_сервера>.
3. Пример: ssh labuser@192.168.56.101
4. Внимание! Вы увидите сообщение:

The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.

ECDSA key fingerprint is SHA256:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

Are you sure you want to continue connecting (yes/no/[fingerprint])?

5. Это нормально. Сервер впервые представляет клиенту свой открытый ключ. Введите yes и нажмите Enter.
6. Система попросит пароль пользователя на сервере. Введите пароль.
7. Если всё правильно, приглашение командной строки изменится. Теперь вы находитесь в терминале сервера, управляя им удалённо.
8. Выполните команду hostname — она покажет имя серверной машины.
9. Выполните whoami — покажет вашего пользователя на сервере.
10. Выйти из сессии можно командой exit или нажав Ctrl+D.

Контрольные вопросы

1. Опишите трехуровневую архитектуру протокола SSH.
2. Какие основные методы аутентификации пользователя поддерживаются в SSH?
3. Какой командой публичный ключ клиента передаётся на сервер для настройки входа без пароля?
4. Какой командой проверить, запущен ли SSH-сервер?
5. Как безопасно выйти из SSH-сессии?

Лабораторная работа № 17 «Установка и настройка веб-сервера»

Теоретические сведения

Веб-сервер — это программное обеспечение, которое принимает HTTP/HTTPS-запросы от клиентов (браузеров, мобильных приложений) и возвращает им ответы, обычно — HTML-страницы, изображения, CSS, JS файлы и другие веб-ресурсы. Основная функция это обработка запросов по протоколу HTTP(S) и обслуживание веб-сайтов.

Архитектура «Клиент-Сервер» в вебе:

1. Клиент (браузер) отправляет HTTP-запрос (GET /index.html HTTP/1.1).
2. Веб-сервер принимает запрос, анализирует его (метод, URI, заголовки).
3. Сервер находит запрашиваемый ресурс на диске или генерирует его динамически (с помощью PHP, Python и т.д.).
4. Сервер формирует и отправляет HTTP-ответ, содержащий статус-код (например, 200 OK), заголовки и тело ответа (контент).

Обзор популярных веб-серверов:

1. Apache HTTP Server:

– Статус: Один из самых первых и распространённых (с 1995 г.).

– Архитектура: Мультипроцессная (MPM — Multi-Processing Module). Может работать в режиме prefork (по процесс на соединение) или worker (потоки).

– Конфигурация: Централизованный файл httpd.conf или разбитый на части в /etc/apache2/ (Ubuntu). Настройка через .htaccess-файлы на уровне директорий (гибкость для хостинга).

– Сильные стороны: Мощность, гибкость, огромное количество модулей (.htaccess, mod_rewrite, mod_php), отличная документация.

– Слабые стороны: Выше потребление памяти при большой нагрузке по сравнению с Nginx.

2. Nginx (Engine-X):

– Статус: Современный высокопроизводительный сервер (с 2004 г.).

– Архитектура: Асинхронная, событийно-ориентированная (event-driven). Один мастер-процесс управляет несколькими рабочими процессами, которые обслуживают тысячи соединений в каждом.

– Конфигурация: Централизованная, директивная. Основной файл /etc/nginx/nginx.conf. Нет аналога .htaccess, все настройки делаются в основном конфиге (лучшая производительность и безопасность).

– Сильные стороны: Высочайшая производительность при статическом контенте и как reverse proxy, низкое потребление памяти, эффективная работа с большим числом одновременных соединений.

– Слабые стороны: Меньше встроенных модулей, динамические модули сложнее подключать.

Задания к лабораторной работе

Задание 1: Установка веб-сервера apache на linux

Установка Apache на CentOS:

1. Откройте окно терминала и обновите списки пакетов репозитория, введя следующее: sudo yum update
2. Теперь вы можете установить Apache с помощью команды: sudo yum –y install httpd

httpd - это имя службы Apache в CentOS. Опция *–y* автоматически отвечает да на запрос подтверждения.

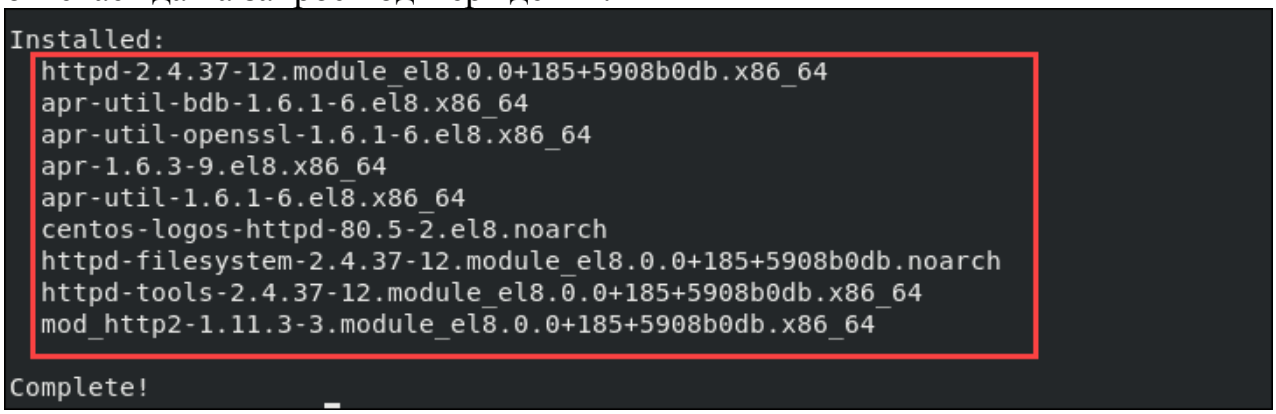

Рисунок 17.1 - Установка Apache на CentOS

3. Готово, Apache установлен.

Установка Apache на Ubuntu и Debian

1. В Ubuntu и Debian пакет и служба Apache называются apache2.
2. Сначала также обновите инструмент управления пакетами: *sudo apt update*
3. Теперь устанавливаем Apache: *sudo apt install apache2*

Задание 2: Запуск и управление веб-сервером Apache

Apache - это сервис, работающий в фоновом режиме. В Debian и Ubuntu он автоматически запустится после установки, а в CentOS его нужно запустить вручную.

Не забывайте что в командах в CentOS нам нужно использовать httpd, а в Debian и Ubuntu apache2

1. Запустите службу Apache, введя следующее: *sudo systemctl start httpd*

Система не возвращает вывод, если команда выполняется правильно.

2. Чтобы настроить автозагрузку Apache при запуске используйте команду: *sudo systemctl enable httpd*

3. Чтобы проверить состояние службы Apache: *sudo systemctl status httpd*

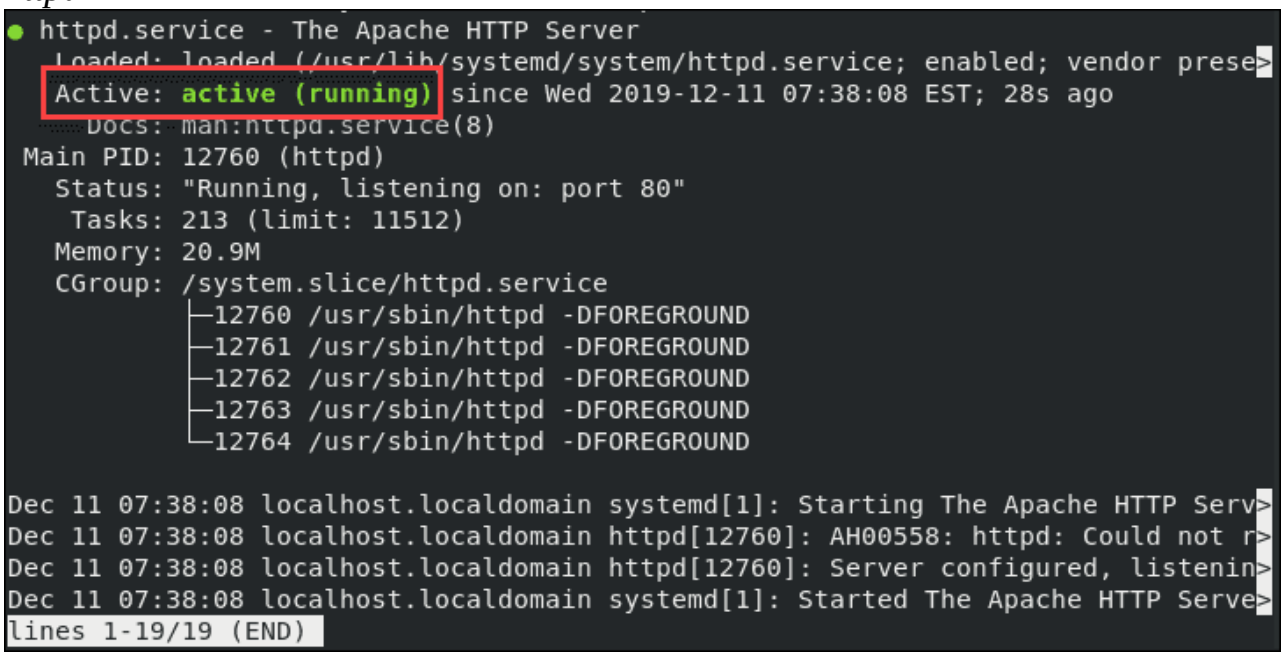

Рисунок 17.2 – Проверка состояния Apache

4. Чтобы перезагрузить Apache (перезагрузит файлы конфигурации, чтобы применить изменения): *sudo systemctl reload httpd*

5. Чтобы перезапустить весь сервис Apache: *sudo systemctl restart httpd*

6. Чтобы остановить Apache: *sudo systemctl stop httpd*

7. Чтобы отключить Apache при запуске системы: *sudo systemctl disable httpd*

Задание 3: проверьте тестовую страницу Apache

1. В окне терминала узнайте IP-адрес вашей системы одной из команд:

– *hostname -I | awk '{print $1}'*

– *ip addr show*

– *ifconfig*

2. Откройте веб-браузер и введите IP-адрес, отображаемый в выводе. Система должна показать тестовую страницу HTTP-сервера Apache.

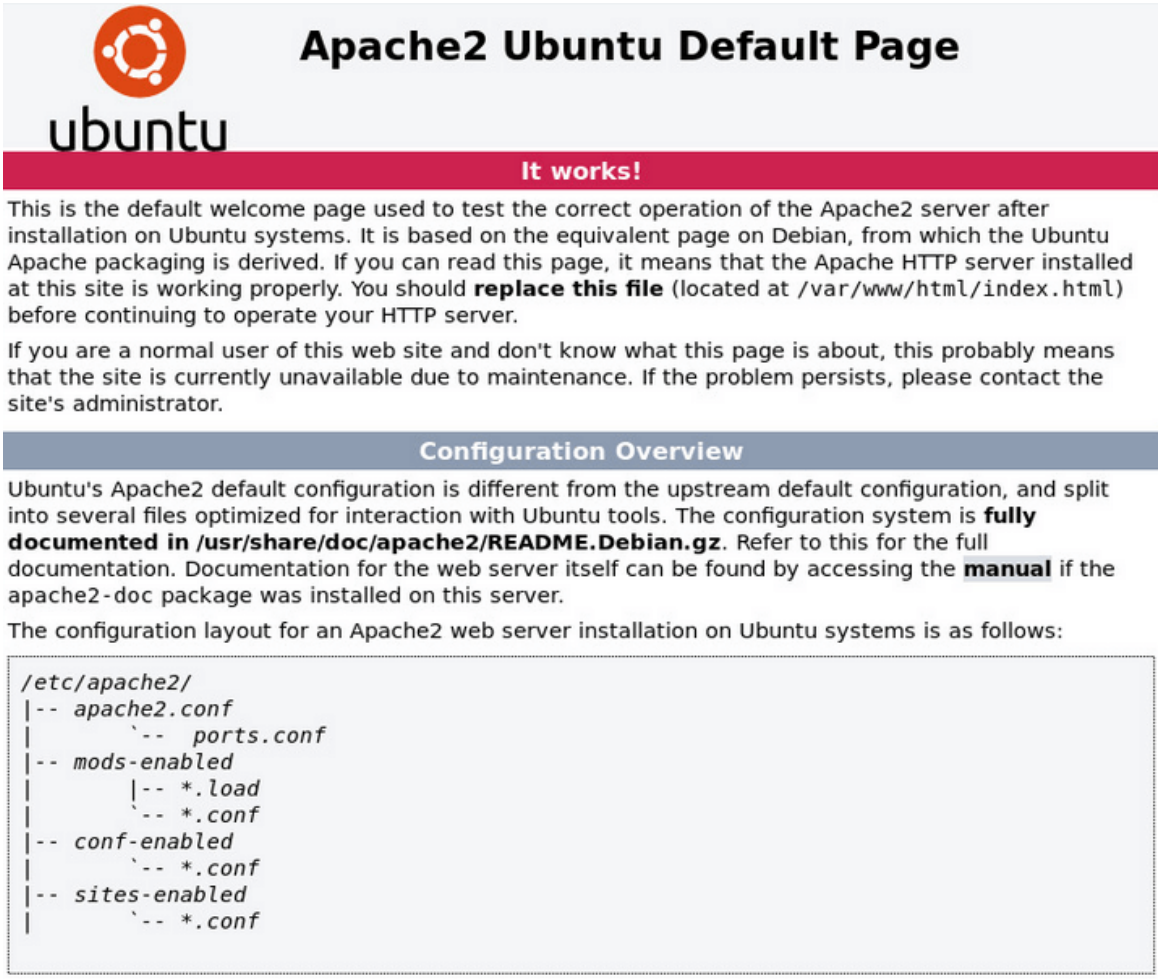

Рисунок 17.3 – Тестовая страница Apache

Контрольные вопросы

1. Какова основная задача веб-сервера?
2. Каковы основные функции веб-сервера в модели клиент-серверного взаимодействия?
3. Опишите путь HTTP-запроса от браузера до получения HTML-страницы.
4. Назовите два самых популярных веб-сервера с открытым кодом.
5. Опишите последовательность команд для установки и запуска Apache.

Лабораторная работа № 18 «Создание правил фильтрации трафика»

Теоретические сведения

Брандмауэр Защитника Windows (Windows Defender Firewall) это встроенный в Windows хост-брандмауэр (host-based firewall), который контролирует входящий и исходящий сетевой трафик на основе правил. Его основные задачи:

- Защита от несанкционированного доступа из сети.
- Контроль исходящих соединений приложений.
- Предотвращение сетевых атак и распространения вредоносного ПО.
- Изоляция компьютера в публичных сетях.

WFP — это набор API и системных служб в Windows, предоставляющих платформу для создания фильтров сетевого трафика. Ключевые компоненты:

- Фильтры (Filters): Основные правила, определяющие судьбу пакета. Содержат условия и действие.
- Слои (Layers): Точки в сетевом стеке, где применяются фильтры (например, уровень авторизации подключений, уровень IP-трафика).
- Провайдеры (Providers): Источники правил (Брандмауэр Windows, сторонние антивирусы).
- Подслои (Sublayers): Позволяют упорядочивать фильтры внутри слоя (весовые коэффициенты).

Правила фильтрации можно применять к одному, нескольким профилям стандартным профили сети (Network Profiles):

- Доменный (Domain): Когда компьютер присоединен к домену Active Directory.
- Частный (Private): Для доверенных сетей (домашняя, рабочая).
- Общедоступный (Public): Для ненадежных сетей (кафе, аэропорт). Самые строгие правила по умолчанию.

Основные элементы каждого правила фильтрации правил:

1. Направление (Direction): Inbound (входящий) или Outbound (исходящий) трафик.
2. Действие (Action): Allow (разрешить) или Block (заблокировать). При блокировке можно уведомлять пользователя.
3. Условия (Conditions):

- Программа (Program): Путь к исполняемому файлу (.exe).
- Порт (Port): Номер TCP/UDP порта и протокол.

– Предопределенное правило (Predefined): Для известных служб (например, "Удаленный рабочий стол").

– Настраиваемое (Custom): Любые параметры (протокол, IP-адреса, интерфейсы, пользователи).

4. Типы правил:

– Правила для программ: Контролируют доступ конкретного приложения.

– Правила для портов: Контролируют доступ к определенным портам независимо от приложения.

Способы управления правилами фильтрации:

– Графический интерфейс: Брандмауэр Защитника Windows (wf.msc).

– PowerShell: Модуль NetSecurity (команды New-NetFirewallRule, Get-NetFirewallRule, Set-NetFirewallRule, Remove-NetFirewallRule).

– Командная строка: Утилита netsh advfirewall.

Правила брандмауэра могут централизованно управляться через групповые политики. Такой способ управления имеет приоритет перед локальными правилами.

Задания к лабораторной работе

Подготовка:

1. Используйте виртуальную машину или физический компьютер с Windows.
2. Запустите PowerShell от имени администратора.
3. Включите брандмауэр (по умолчанию включен): *Set-NetFirewallProfile -All -Enabled True*
4. Определите активный сетевой профиль: *Get-NetConnectionProfile*

Задание: Блокировка Edge (ключевые моменты)

1. Найдите точный путь к Edge в PowerShell: *Get-Process msedge | Select-Object Path*
2. Или найдите вручную: обычно C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe.
3. Создайте блокирующее правило. Критически важно указать полный путь в кавычках: *New-NetFirewallRule -DisplayName "Block Edge Outbound" -Direction Outbound -Program "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -Action Block*
4. Закройте все окна Edge.
5. Запустите Edge → попробуйте открыть google.com.

6. Результат: Должна быть ошибка "Подключение не установлено" или "Нет подключения к интернету".

7. Важно: Откройте Firefox (если есть) — он должен работать, так как правило касается только Edge.

8. После проверки на забудте удалить правлило командой: *Remove-NetFirewallRule -DisplayName " Block Edge Outbound "*

Контрольные вопросы

1. Каковы основные функции Брандмауэра Защитника Windows?
2. Объясните понятие «Профили сети» в Windows.
3. Что такое Windows Filtering Platform (WFP)?
4. Какие основные типы правил брандмауэра существуют?
5. Как полностью отключить брандмауэр для всех профилей с помощью PowerShell?

Лабораторная работа № 19 «Настройка безопасности портов коммутатора»

Теоретические сведения

Основные угрозы безопасности на уровне коммутатора:

1. Атака на переполнение CAM-таблицы (MAC Flooding)

– Принцип: Злоумышленник генерирует огромное количество фреймов с разными поддельными MAC-адресами.

– Результат: CAM-таблица коммутатора заполняется, коммутатор переходит в режим хаба (broadcast для неизвестных MAC-адресов), что позволяет прослушивать трафик.

– Защита: Port Security.

2. MAC Spoofing (подмена MAC-адреса)

– Принцип: Атакующий подменяет MAC-адрес своего устройства на MAC-адрес легитимного устройства.

– Цель: Перехват трафика, обход фильтрации по MAC, атаки "человек посередине".

– Защита: Port Security с привязкой MAC-адресов.

3. Атаки на протоколы верхних уровней через коммутатор

– DHCP Spoofing (Starvation): Злоумышленник истощает пул адресов DHCP-сервера или внедряет rogue DHCP-сервер.

– ARP Spoofing (Poisoning): Отправка поддельных ARP-ответов для перенаправления трафика.

– Защита: DHCP Snooping + Dynamic ARP Inspection (DAI).

Технология Port Security. Основные концепции:

1. Фиксация MAC-адресов: Порту разрешено изучать и использовать только определённые MAC-адреса.

2. Типы безопасных MAC-адресов:

– Static (Статические): Вручную сконфигурированные администратором (switchport port-security mac-address XXXX.XXXX.XXXX).

– Dynamic (Динамические): Автоматически изученные коммутатором из трафика на порту. Хранятся только в рабочей конфигурации (теряются при перезагрузке).

– Sticky (Липкие): Автоматически изученные, но затем сохранённые в конфигурации (записываются в startup-config).

3. Violation Mode (Режим реакции на нарушение): Действие при попытке подключения неразрешённого устройства:

– protect: Фреймы с неразрешённых MAC-адресов отбрасываются, но нет логирования.

– restrict: Фреймы отбрасываются, генерируется syslog-сообщение, счётчик нарушений увеличивается.

– shutdown (по умолчанию): Порт переводится в err-disable состояние (отключается), требуется ручное включение или настройка err-disable recovery.

Ключевые команды настройки (Cisco IOS):

Switch(config-if)# switchport mode access // Порт в режим доступа

Switch(config-if)# switchport port-security // Включение Port Security

Switch(config-if)# switchport port-security maximum 2 // Макс. кол-во MAC-адресов

Switch(config-if)# switchport port-security violation restrict // Режим реакции

Switch(config-if)# switchport port-security mac-address sticky // Липкие MAC

Задания к лабораторной работе

Настроить и протестировать Port Security с разными типами MAC-адресов.

Топология в PNETLab:

Swich1: Fa0/1 → PC1, Fa0/2 → PC2, Fa0/3 → PC3

Настройка адресов на PC1 и PC2

PC1> ip 192.168.1.10/24 192.168.1.1

PC2> ip 192.168.1.11/24 192.168.1.1

Настройка коммутатора:

enable

configure terminal

1. Создание VLAN

vlan 10

name SECURITY_LAB

exit

2. Настройка интерфейсов

interface range fastEthernet 0/1-3

switchport mode access

switchport access vlan 10

exit

3. Port Security на Fa0/1 (Static MAC)

interface fastEthernet 0/1
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address 0000.1111.2222 ! MAC PC1
switchport port-security violation restrict
exit

4. Port Security на Fa0/2 (Dynamic)

interface fastEthernet 0/2
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
exit

5. Port Security на Fa0/3 (Sticky)

interface fastEthernet 0/3
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit

Тестирование в PNETLab:

1. На PC3 измените MAC-адрес и попробуйте подключиться к Fa0/1
2. Проверьте логи: show logging
3. Покажите статистику: show port-security
4. Команды для проверки PNETLab:

– show port-security
– show port-security address
– show mac address-table
– show interface status

Контрольные вопросы

1. Покажите полную последовательность команд для настройки Port Security с sticky MAC-адресами на порту Fa0/5.
2. Какие команды используются для мониторинга нарушений безопасности в реальном времени?
3. Объясните принцип ARP Spoofing (Poisoning) атаки.
4. Какие три типа безопасных MAC-адресов поддерживает Port Security?
5. Что происходит с портом при срабатывании режима shutdown?

Лабораторная работа № 20 «Настройка VPN-клиента и проверка шифрования трафика»

Теоретические сведения

VPN (Virtual Private Network) — виртуальная частная сеть, создающая защищённое соединение поверх публичной сети (Интернет).

Ключевые функции:

– Конфиденциальность: Шифрование всего трафика

– Целостность: Гарантия, что данные не были изменены

– Аутентификация: Подтверждение подлинности участников

– Неотрекаемость: Невозможность отказаться от отправленных данных

Типы VPN:

1. По уровню OSI:

– SSL/TLS VPN (Уровень приложений): OpenVPN, WireGuard, AnyConnect

– IPsec VPN (Сетевой уровень): L2TP/IPsec, IKEv2/IPsec

2. По архитектуре:

– Remote Access VPN: Удалённый доступ для отдельных пользователей

– Site-to-Site VPN: Постоянное соединение между сетями

Протоколы VPN:

1. IPsec (Internet Protocol Security). Режимы:

– Transport Mode: Шифрует только полезную нагрузку (данные)

– Tunnel Mode: Шифрует весь IP-пакет (заголовок + данные)

Его основными компонентами являются:

– IKE (Internet Key Exchange): Протокол установления безопасного канала

– ESP (Encapsulating Security Payload): Шифрование и аутентификация

– AH (Authentication Header): Только аутентификация (редко используется)

2. OpenVPN:

– Основан на SSL/TLS

– Гибкая настройка, кроссплатформенность

– Использует порт 1194 UDP/TCP по умолчанию

3. WireGuard:

– Современный, высокопроизводительный

– Простая конфигурация, малый кодовая база
– Использует UDP-порт 51820

4. L2TP/IPsec. L2TP (Layer 2 Tunneling Protocol) + IPsec для шифрования, встроен в большинство ОС.

Криптографические компоненты:

1. Алгоритмы шифрования:
– Симметричные: AES (128, 192, 256 бит), ChaCha20
– Асимметричные: RSA, ECC (Elliptic Curve Cryptography)
2. Алгоритмы аутентификации:
– Хеш-функции: SHA-1, SHA-256, SHA-512
– Коды аутентичности: HMAC (Hash-based MAC)
3. Обмен ключами:
– Diffie-Hellman: Безопасный обмен ключами по открытому каналу
– ECDH: Версия на эллиптических кривых (современнее)

Этапы установки VPN-соединения:

1. Аутентификация клиента
2. Обмен ключами (IKE Phase 1)
3. Установка безопасного канала (IKE Phase 2)
4. Передача данных через туннель
5. Разрыв соединения

Задания к лабораторной работе

Задание 1: Настройка VPN-сервера на Windows Server

Откройте Диспетчер серверов → Добавить роли

Роли:

– Удалённый доступ

Службы ролей:

– Маршрутизация
– DirectAccess и VPN (RRAS)

Настройка RRAS через PowerShell:

1. Установка роли:

Install-WindowsFeature -Name RemoteAccess -IncludeManagementTools
Install-WindowsFeature -Name Routing

2. Настройка RRAS

Install-RemoteAccess -VpnType VpnS2S

3. Перезагрузка

Restart-Computer -Force

Настройка через графический интерфейс:

Откройте "Маршрутизация и удаленный доступ"

Правой кнопкой на сервере → "Настроить и включить маршрутизацию и удаленный доступ"

Выберите "Специальная конфигурация" → "Доступ к виртуальной частной сети (VPN)"

Настройка пула адресов:

Set-VpnIPAddressRange -IPAddressRangeStart 10.0.0.100 `

-IPAddressRangeEnd 10.0.0.200 `

-RoutingDomain "."

Задание2: Создание пользователей VPN

1. Создайте пользователя:

New-LocalUser -Name "vpnuser" -Password (ConvertTo-SecureString "P@ssw0rd123" -AsPlainText -Force)

Add-LocalGroupMember -Group "Пользователи удаленного рабочего стола" -Member "vpnuser"

2. Настройка политики доступа:

Откройте "Панель управления" → "Администрирование" → "Политика безопасности"

Политики Windows → Параметры безопасности → Политики учетных записей

"Пользователи удаленного доступа" → Добавить пользователя

Задание 3: Настройка VPN-подключения

Откройте настройки VPN:

1. Через PowerShell

Add-VpnConnection -Name "SSTP-Lab" `

-ServerAddress "192.168.100.10" `

-TunnelType "Sstp" `

-EncryptionLevel "Required" `

-AuthenticationMethod MSChapv2 `

-SplitTunneling $false `

-RememberCredential $true

2. Альтернативно через GUI:

Параметры → Сеть и Интернет → VPN

"Добавление VPN-подключения"

Параметры:

- Поставщик услуг VPN: Windows (встроенные)
- Имя подключения: SSTP-Lab
- Имя или адрес сервера: 192.168.100.10
- Тип VPN: SSTP

– Тип данных для входа: Имя пользователя и пароль

Настройка параметров безопасности

1. Изменение свойств подключения:

```
Set-VpnConnection -Name "SSTP-Lab" `
        -AuthenticationMethod MSChapv2 `
        -EncryptionLevel Required `
        -TunnelType Sstp
```

2. Просмотр настроек:

```
Get-VpnConnection -Name "SSTP-Lab" | Format-List *
```

Подключение и тестирование

1. Подключение

```
rasdial "SSTP-Lab" vpnuser P@ssw0rd123
```

2. Проверка состояния

```
Get-VpnConnection -Name "SSTP-Lab"
```

3. Проверка сети:

```
ipconfig /all
route print
ping 10.0.0.1  # Внутренний адрес VPN
```

Контрольные вопросы

1. Опишите этапы установки соединения.
2. Объясните разницу между туннельным и транспортным режимами IPsec.
3. Какой порт по умолчанию использует OpenVPN?
4. Какой протокол использует WireGuard?
5. Какой инструмент используется для анализа сетевого трафика?

Лабораторная работа № 21 «Конфигурация точки доступа»

Теоретические сведения

Точка доступа (Access Point, AP) — устройство, обеспечивающее подключение беспроводных клиентов к проводной сети и управляющее их взаимодействием. Ключевые характеристики:

1. Стандарты Wi-Fi: 802.11a/b/g/n/ac/ax (Wi-Fi 6/6E)
2. Частотные диапазоны: 2.4 ГГц и 5 ГГц
3. Скорость передачи: Зависит от стандарта и ширины канала
4. Зона покрытия: Определяется мощностью передатчика и антеннами

Архитектура беспроводных сетей

1. Режимы работы точки доступа:

– Режим точки доступа (AP Mode): Стандартный режим

– Режим клиента (Client Mode): Подключение к другой точке как клиент

– Режим моста (Bridge Mode): Соединение двух сетей

– Режим повторителя (Repeater Mode): Расширение зоны покрытия

2. Типы беспроводных сетей:

– Инфраструктурная сеть: Клиенты → Точка доступа → Проводная сеть

– Ad-hoc сеть: Прямое соединение клиентов без точки доступа

– Mesh-сеть: Самоорганизующаяся сеть из нескольких точек доступа

Параметры конфигурации точки доступа:

1. Основные настройки:

– SSID (Service Set Identifier): Имя сети (максимум 32 символа)

– Канал (Channel): Номер частотного канала

– Ширина канала: 20/40/80/160 МГц

– Мощность передатчика: От 1 до 100% (или dBm)

2. Режимы безопасности:

– WEP (Wired Equivalent Privacy): Устаревший, ненадёжный

– WPA (Wi-Fi Protected Access): TKIP шифрование

– WPA2 (WPA второе поколение): AES-CCMP шифрование

– WPA3 (WPA третье поколение): Современный стандарт

3. Типы аутентификации:

– PSK (Pre-Shared Key): Общий ключ для всех

– Enterprise: Индивидуальная аутентификация (RADIUS)

– Captive Portal: Веб-аутентификация

Технологии управления и оптимизации:

1. Управление перегрузкой:
– Client Limiting: Ограничение количества клиентов
– Bandwidth Control: Ограничение скорости
– Load Balancing: Балансировка нагрузки между точками
2. Расширенные функции:
– VLAN: Виртуальные сети для разных групп
– QoS (Quality of Service): Приоритезация трафика
– Guest Network: Гостевая изолированная сеть
– WPS (Wi-Fi Protected Setup): Быстрая настройка
– Mesh Networking: Ячеистая сеть
3. Мониторинг и диагностика:
– Сигнал/шум (RSSI/SNR): Качество соединения
– Retransmissions: Повторные передачи
– Channel Utilization: Загрузка канала

Протоколы управления:
– HTTP/HTTPS: Веб-интерфейс управления
– SSH/Telnet: Удалённое управление
– SNMP (Simple Network Management Protocol): Мониторинг
– TR-069: Удалённое управление провайдером

Задания к лабораторной работе

Задание: Базовая настройка точки доступа

Физическое подключение:
1. Подключите точку доступа к сети через LAN-порт
2. Настройте ПК с IP 192.168.0.100/24
3. Откройте веб-интерфейс (192.168.0.1)

Базовая конфигурация:
1. Параметры:
– SSID: Student-<ВашаФамилия>
– Режим работы: Точка доступа
– Канал: Авто (2.4 ГГц), 36 (5 ГГц)
– Ширина канала: 20/40 МГц (2.4 ГГц), 80 МГц (5 ГГц)
2. Настройка безопасности:
– Безопасность: WPA2-Personal
– Шифрование: AES
– Пароль: ComplexPass2024!
– Скрыть SSID: Нет

– Фильтрация по MAC: Отключена

Проверка работы:

1. Подключите 2 устройства
2. Проверьте скорость соединения

Контрольные вопросы

1. Объясните разницу между режимами работы точки доступа.
2. Что такое SSID и какие рекомендации существуют по его настройке?
3. Что такое QoS в беспроводных сетях?
4. Какие параметры влияют на производительность Wi-Fi?
5. Какие частотные диапазоны используются в Wi-Fi?

2 ОБЩАЯ ХАРАКТЕРИСТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа - целенаправленная, планируемая в рамках учебного плана деятельность студентов, которая осуществляется по заданию, при методическом руководстве и контроле преподавателя, но без его непосредственного участия. Самостоятельная работа студентов является одной из важнейших составляющих образовательного процесса.

В учебном процессе учебного заведения выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная — планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Целью самостоятельной работы студентов является:

- систематизация и закрепление полученных теоретических знаний и практических умений;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов, творческой инициативы, самостоятельности, ответственности, организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации;
- формирование общих и профессиональных компетенций.

Самостоятельная работа студентов должна быть хорошо спланирована и организована. При планировании такой работы необходимо учитывать условия, обеспечивающие её успешное выполнение:

- чёткое определение преподавателем объёма и содержания самостоятельной работы;
- определение видов консультативной помощи;
- постановка цели самостоятельной работы и критерии её оценки;
- виды и формы контроля её выполнения.

Выполняя самостоятельную работу под контролем преподавателя, студент должен:

- освоить минимум знаний;
- планировать свою самостоятельную работу в соответствии разработанным графиком;
- выполнять самостоятельную работу и отчитываться по ее результатам в соответствии с графиком представления результатов, видами и сроками отчетности по самостоятельной работе студентов.

В процессе самостоятельной работы студент приобретает навыки самоорганизации, самоконтроля, самоуправления, саморефлексии и становится активным самостоятельным субъектом учебной деятельности.

Таким образом, самостоятельная работа студентов оказывает важное влияние на формирование личности будущего специалиста.

Самостоятельная работа студентов является обязательной для каждого студента, объем ее определяется учебным планом в соответствии с требованиями Государственных образовательных стандартов.

При изучении тем дисциплины студенты выполняют следующие виды самостоятельной работы:

- проработка конспектов занятий, учебных изданий и специальной технической литературы;
- составление конспекта, тематических схем, таблиц;
- подготовка к лабораторным работам и практическим занятиям с использованием методических рекомендаций преподавателя;
- оформление отчетов по лабораторным работам и практическим занятиям, подготовка к их защите;
- моделирование и решение производственных процессов и ситуационных задач;
- подготовка презентаций;
- работа с электронными ресурсами в сети Интернет;
- подготовка к семинару;
- подготовка к зачетам, экзаменам.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов образовательного учреждения. Материально-техническое и информационно - техническое обеспечение самостоятельной работы студентов включает в себя:

- библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами;
- учебно-методическую базу учебных кабинетов, лабораторий и методического центра;
- компьютерные классы с возможностью работы в Интернет;
- базы практики в соответствии с заключенными договорами;
- аудитории для консультационной деятельности;
- учебную и учебно-методическую литературу, разработанную с учетом увеличения доли самостоятельной работы студентов, и иные методические материалы.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж по выполнению задания, в котором указывает цель задания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Во время выполнения студентами внеаудиторной самостоятельной работы и при необходимости преподаватель может проводить консультации. Самостоятельная работа может осуществляться

индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся.

3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Общие методические рекомендации студенту при изучении тем дисциплины.

Большая часть самостоятельной работы выполняется студентом вне учебных занятий при подготовке домашних заданий. Общие требования к выполнению этого вида самостоятельной работы заключаются в следующем:

- активно работать на уроке, усваиваю основную часть нового материала;
- если что-то непонятно, не стесняться задавать вопросы преподавателю;
- большое задание необходимо разбивать на части и работать над каждой из них в отдельности;
- выполняя домашнее задание, надо не просто думать, что надо сделать, а еще и решать, с помощью каких средств и приемов этого можно добиться;
- в процессе приготовления домашнего задания необходимо делать перерывы;
- готовиться к докладам, рефератам, защите курсовых работ и проектов, практических и лабораторных занятий надо заранее, равномерно распределяя нагрузку, а не оставлять такую ответственную работу на последний день;
- изучая заданный материал, сначала надо его понять, а уже потом запомнить;
- научиться находить интересующую нужную информацию с помощью компьютера;
- не стесняться обращаться за помощью к взрослым и однокурсникам;
- надо составлять план устного ответа и проверять себя;
- на письменном столе должно лежать только то, что необходимо для выполнения одного задания. После его завершения со стола убираются уже использованные материалы, и кладутся те учебные принадлежности, которые необходимы для выполнения следующего задания;
- нужно решить, в какой последовательности лучше выполнять задания и сколько времени понадобится на каждое из них;
- трудный материал урока лучше повторить в тот же день, чтобы сразу закрепить его и запомнить;
- читая учебник, надо задавать самому себе вопросы по тексту.

Подготовка тематических сообщений, докладов, рефератов

Реферат доклад, сообщение (от латинского refero - передаю, сообщаю) - краткое письменное изложение материала по определенной теме с целью привития студентам навыков самостоятельного поиска и анализа информации, формирования умения подбора и изучения литературных источников, используя при этом дополнительную научную, методическую и периодическую литературу.

Тема реферата выбирается по желанию студента из списка, предлагаемого преподавателем. Тема может быть сформулирована студентом самостоятельно.

Выбранная тема согласовывается с преподавателем.

После выбора темы требуется:

- составить план реферата;
- подобрать необходимую информацию;
- изучить подобранную информацию;
- составить текст реферата.

План реферата должен включать в себя введение, основной текст и заключение. Во введении аргументируется актуальность выбранной темы, указываются цели и задачи исследования. В нем также отражается методика исследования и структура работы. Основная часть работы предполагает освещение материала в соответствии с планом. В заключении излагаются основные выводы и рекомендации по теме исследования.

Реферат оформляется согласно требованиям, установленным в учебном заведении. Он должен содержать: титульный лист, оглавление и список использованной литературы. На титульном листе указываются: название учебного заведения, название профессионального модуля, междисциплинарного курса, тема работы, курс, группа, фамилии, имена, отчества студента и руководителя работы, название города, в котором находится учебное заведение, год написания данной работы. Реферат может содержать приложения в форме схем, образцов документов и другие изображения в соответствии с темой исследования. Все страницы работы, включая оглавление и список литературы, нумеруются по порядку с титульного листа (на нем цифра не ставится) до последней страницы без пропусков и повторений. Введение, заключение, новые главы, список использованных источников и литературы должны начинаться с нового листа. Подбор литературы производится студентом из предложенного преподавателем списка литературы. Текст реферата необходимо набирать на компьютере на одной стороне листа. Размер левого поля 30 мм, правого - 15 мм, верхнего - 20 мм, нижнего - 20 мм. Шрифт - Times New Roman, размер - 14, межстрочный интервал - 1,5. Фразы, начинающиеся с новой строки, печатаются с абзацным отступом от начала строки (1,25 см). Реферат, выполненный небрежно, неразборчиво, без соблюдения требований по оформлению, возвращается студенту без проверки с указанием причин возврата на титульном листе.

Критерии оценки:

- знание и понимание проблемы;
- умение систематизировать и анализировать материал, четко и обоснованно формулировать выводы;
- «трудозатратность» (объем изученной литературы, добросовестное отношение к анализу проблемы);

- самостоятельность, способность к определению собственной позиции по проблеме и к практической адаптации материала, недопустимость плагиата;

- выполнение необходимых формальностей (точность в цитировании и указании источника текстового фрагмента, аккуратность оформления).

Проработка занятий, учебных изданий и специальной технической литературы

Работа с конспектом лекций по темам междисциплинарных курсов заключается в том, что студент после рассмотрения темы на учебных занятиях в период между очередными лекциями изучает материал конспекта. При этом непонятные положения конспекта необходимо выяснять у преподавателя на консультациях или при чтении основной и дополнительной литературы.

При работе с книгой необходимо научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги. Правильный подбор учебников рекомендуется преподавателем. Необходимая литература может быть также указана в методических разработках. Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и определения (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода). Полезно составлять опорные конспекты. При изучении материала по учебнику, полезно в тетради (на специально отведенных полях) дополнять конспект лекций, написанный на учебных занятиях. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем. Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при пропитывании записей лучше запоминались. Различают два вида чтения; первичное и вторичное. Первичное - эти внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятного слова. Содержание не всегда может быть понятно после первичного чтения. Задача вторичного чтения - полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

Чтение научного текста является частью познавательной деятельности. Ее цель - извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия. Выделяют четыре основные установки в чтении научного текста:

- информационно-поисковая, задача которой - найти, выделить искомую информацию;

- усваивающая, при которой усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения, излагаемые автором, так и всю логику его рассуждений;
- аналитико-критическая - читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему;
- творческая, создающая у читателя готовность в том или ином виде использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке.

Самостоятельная работа при чтении учебной литературы начинается с изучения конспекта материала, полученного при слушании лекций преподавателя. Полученную информацию необходимо осмыслить. При необходимости, в конспект лекций могут быть внесены схемы, эскизы рисунков, другая дополнительная информация.

Составление конспекта, тематических схем, таблиц

При изучении нового материала, как правило, составляется конспект. Конспект - изложение текста, которому присущи краткость, связность и последовательность. При этом максимально точно записываются формулы, определения, схемы, трудные для запоминания места.

При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре текста. Для уточнения и дополнения необходимо оставлять поля. Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

Классификация конспектов:

- плановый конспект, для чего сначала нужно написать план текста, а затем на пункты плана делаются комментарии: свободно изложенный текст либо цитаты;
- обзорный конспект - краткое изложение данной темы с использованием нескольких источников;
- текстуальный конспект состоит из цитат одного текста;
- свободный конспект предполагает цитаты текста и собственные формулировки прочитанного текста;
- сложный - конспект, в котором отражается определенная тема или вопрос;
- хронологический конспект отражает последовательность событий;
- опорный конспект, в котором излагается информация в виде опорных знаков, слов, сигналов.

Методические рекомендации по составлению конспекта:

- определить цель написания конспекта;
- внимательно прочитать текст, уточнить в справочной литературе непонятные слова;

- выделить основные смысловые части текста;
- определить главное, составить план;
- кратко сформулировать основные положения текста, отметить аргументацию автора;
- составить текст конспекта, изложив информацию кратко и своими словами, четко следуя пунктам плана, записи следует вести четко, ясно;
- грамотно записывать цитаты, учитывая лаконичность, значимость мысли;
- в тексте конспекта желательно приводить не только тезисные положения, но и их доказательства.

При составлении тематических схем, таблиц необходимо внимательно прочитать текст соответствующий параграф учебника. Продумать «конструкцию» таблицы или схемы, расположение порядковых номеров, терминов, примеров и пояснений (и прочего). Начертить схему или таблицу и заполнить ее графы необходимым содержимым.

Подготовка к лабораторным работам и практическим занятиям, оформление отчетов по лабораторным работам и практическим занятиям, подготовка к их защите

Программы профессиональных модулей предусматривают выполнение практических и лабораторных занятий.

Лабораторное занятие - форма учебного занятия, ведущей дидактической целью которого является экспериментальное подтверждение и проверка существующих теоретических положений (законов, зависимостей), формирование учебных и профессиональных практических умений и навыков.

Практическое занятие - это одна из форм учебной работы, которая ориентирована на закрепление изученного теоретического материала, его более глубокое усвоение и формирование умения применять теоретические знания в практических целях. Особое внимание на практических занятиях уделяется выработке учебных или профессиональных навыков. Такие навыки формируются в процессе выполнения конкретных заданий - упражнений, задач - под руководством и контролем преподавателя.

Подготовка к практическим и лабораторным занятиям заключается в работе с конспектом лекций по данной теме, в изучении соответствующего раздела учебника или учебного пособия, в просмотре дополнительной литературы. Этапы подготовки к практическому или лабораторному занятию заключаются в следующем: освежить в памяти теоретические сведения, полученные на лекциях и в процессе самостоятельной работы, подобрать необходимую учебную и справочную литературу. Отобрать те материалы, которые позволят в полной мере реализовать цели и задачи предстоящей работы. Еще раз проверить соответствие отобранного материала. Студент должен прийти на лабораторное или практическое занятие подготовленным по данной теме.

При выполнении заданий практического или лабораторного занятия студент должен быть ознакомлен преподавателем с целью и ходом выполнения задания и, по необходимости, с правилами техники безопасности. Если у студентов во время выполнения заданий возникают вопросы, то преподаватель консультирует студентов. Порядок выполнения того или иного задания излагается в инструкционных картах или рабочих тетрадях.

После проведения занятия студент представляет письменный отчет, который оформляется в соответствие с принятыми в образовательном учреждении правилами. Отчеты оформляются на листах писчей бумаги формата А4 или в специальных рабочих тетрадях, разработанных преподавателем. Содержание отчета указано в инструкционных картах или рабочих тетрадях.

При подготовке к защите практических и лабораторных занятий студент должен ответить на контрольные вопросы, указанные также в инструкционных картах или рабочих тетрадях, проштудировав при этом конспект лекций, учебную литературу.

Моделирование и решение производственных процессов и ситуационных задач

При изучении дисциплины очень часто студенту приходится сталкиваться с профессиональными задачами и ситуациями, которые необходимо решить самостоятельно, как во время аудиторной работы, так и во время внеаудиторной. При решении таких задач необходимо:

- провести анализ ситуации для определения проблемы в целом; представить ситуацию и себя в качестве действующего в ней лица; проанализировать ошибочные или правильные действия всех участников ситуации;
- определить проблемные узлы - возможные причины и прогнозируемые последствия развития данной ситуации;
- рассмотреть условное прогнозирование развития ситуации: определить окончательную гипотезу, представить обоснованный и доказательный прогноз вероятностного развития ситуации; предложить варианты действий, обоснованные теоретически и, по возможности, подкрепленные практическим личным опытом, опираясь на принципы профессиональной этики; определить способы и методы воздействия на предлагаемую ситуацию;
- сформулировать итоговые выводы, используя профессиональные термины, доказательства правильности своего решения.

Подготовка презентаций

Подготовка презентации позволит студенту логически выстроить изучаемый материал, систематизировать его, сформировать коммуникативные компетенции. Материал презентации представляется в виде текста, схем, диаграмм, таблиц, которые призваны дополнить текстовую

информацию или передать ее в более наглядном виде. Желательно избегать в презентации изображений, не несущих смысловой нагрузки, если они не являются частью стилевого оформления. Цвет графических изображений не должен резко контрастировать с общим стилевым оформлением слайдов, иллюстрации рекомендуется сопровождать пояснительным текстом.

Анимационные эффекты используются для привлечения внимания слушателей или для демонстрации динамики развития какого - либо процесса. В этих случаях использование анимации оправдано, но не стоит чрезмерно насыщать презентацию такими эффектами, иначе это вызовет негативную реакцию аудитории.

Звуковое сопровождение должно отражать суть или подчеркивать особенность темы слайда, презентации. Фоновая музыка не должна отвлекать внимание слушателей и заглушать слова докладчика.

Оптимальное количество слайдов, как правило, десять - пятнадцать. Для оформления слайдов презентации рекомендуется использовать несложные шаблоны, соблюдать единый стиль. Не рекомендуется на одном слайде использовать более трех цветов. Смену слайдов для управления презентацией докладчиком желательно устанавливать по щелчку без времени. Шрифт, выбираемый для презентации, должен обеспечивать читаемость информации на экране и соответствовать выбранному шаблону оформления. Не желательно использовать разные шрифты в одной презентации.

Алгоритм выстраивания презентации должен соответствовать логической структуре работы и отражать последовательность ее этапов. Независимо от алгоритма выстраивания презентации на первом слайде рекомендуется выносить следующие данные: полное наименование образовательной организации; тема презентации; фамилия, имя, отчество студента; специальность обучения; фамилия, имя, отчество руководителя. Последний слайд должен содержать фразу «Спасибо за внимание».

Работа с электронными ресурсами в сети Интернет

Для повышения эффективности самостоятельной работы студент должен учиться работать в поисковой системе сети Интернет, в электронно-библиотечной системе и использовать найденную информацию при подготовке к занятиям.

Интернет сегодня - правомерный источник научных статей, статистической и аналитической информации, и использование его наряду с книгами давно уже стало нормой. Однако, несмотря на то, что ресурсы Интернета позволяют достаточно быстро и эффективно осуществлять поиск необходимой информации, следует помнить о том, что эта информация может быть неточной или вовсе не соответствовать действительности. В связи с этим при поиске материала по заданной тематике следует обращать внимание на научные труды признанных авторов, которые посоветовали вам преподаватели.

Поиск информации можно вести по автору, заглавию, виду издания, году издания или издательству. Также в сети Интернет доступна услуга по скачиванию методических указаний и учебных пособий, подбору необходимой учебной и научно - технической литературы.

Подготовка к семинару

Семинар — это особая форма учебно-теоретических занятий, которая, как правило, служит дополнением к лекционному курсу. Семинар обычно посвящен детальному изучению отдельной темы.

Этапы подготовки к семинару:

- проанализировать тему семинара, подумать о цели и основных проблемах, вынесенных на обсуждение;
- внимательно прочитать материал, данный преподавателем по этой теме на лекции;
- изучить рекомендованную литературу, делая при этом конспекты прочитанного или выписки, которые понадобятся при обсуждении на семинаре;
- постараться сформулировать свое мнение по каждому вопросу и аргументированно его обосновать;
- записать возникшие во время самостоятельной работы с учебниками и научной литературой вопросы, чтобы затем на семинаре получить на них ответы.

При подготовке к семинарским занятиям следует руководствоваться указаниями и рекомендациями преподавателя, использовать основную и дополнительную литературу из представленного им списка.

При подготовке доклада на семинарское занятие желательно заранее обсудить с преподавателем перечень используемой литературы, за день до семинарского занятия предупредить его о необходимых для представления материала технических средствах. Напечатанный текст доклада представить преподавателю на рецензию.

Подготовка к зачетам, экзаменам

Изучение выше перечисленных тем дисциплины завершается зачетами или экзаменами.

Подготовка к зачету или экзамену способствует закреплению, углублению и обобщению знаний, получаемых в процессе обучения, а также применению их к решению практических задач. Готовясь к зачету или экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На зачете или экзамене студент демонстрирует то, что он приобрел в процессе обучения конкретным темам междисциплинарных курсов или модулям в целом.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами, согласно графику их проведения, дается интервал времени в несколько дней. Не следует думать, что их достаточно для успешной подготовки к экзаменам. В эти дни нужно

систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки студента к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня: сон не менее 8 часов в сутки, занятия должны заканчиваться не позднее, чем за 2-3 часа до сна.

Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая- либо лекция, необходимо во время ее восстановить, обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к зачету или экзамену у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных конспектов. Вначале следует просмотреть весь материал по сдаваемой теме, отметить для себя трудные вопросы, обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения. Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Правила подготовки к экзамену:

- сориентироваться во всем материале и обязательно расположить его согласно экзаменационным вопросам или вопросам, обсуждаемым на семинарах, учебных занятиях. Эта работа может занять много времени, но все остальное - уже технические детали, главное - это ориентировка в материале;
- постараться максимально запомнить материал, переосмыслить его, рассмотреть альтернативные идеи;
- подготовить «шпаргалки», главный смысл которых систематизация и оптимизация знаний, однако пользоваться таким подспорьем не рекомендуется. Это очень сложная и важная для студента работа, более сложная и важная, чем простое поглощение массы учебной информации. Если студент самостоятельно подготовил такие «шпаргалки», то, скорее всего, он и экзамены сдавать будет более уверенно, так как у него уже сформирована общая ориентировка в сложном материале. Как это ни парадоксально, но использование «шпаргалок» часто позволяет отвечающему студенту лучше демонстрировать свои познания, точнее - ориентировку в знаниях, что намного важнее знания «запомненного» и «тут же забытого» после сдачи экзамена.

При ответе на экзамене студент сначала должен продемонстрировать преподавателю усвоенный по программе обучения материал, и лишь после этого высказать иную, желательно аргументированную точку зрения.

4 МЕТОДИКА ВЫПОЛНЕНИЯ ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Получить у преподавателя задание и необходимую литературу.
2. Найти предложенную литературу на образовательном портале или в библиотеке.
3. Изучить имеющуюся литературу в электронном или печатном виде, прочитать материалы лекций, практических и (или) семинарских занятий по теме.
4. Изучить методические рекомендации.
5. Оформить работу в тетради или на компьютере в соответствии с требованиями преподавателя.
6. Сдать самостоятельную работу преподавателю, предварительно ответив на вопросы для самоконтроля.

5 МЕТОДЫ КОНТРОЛЯ И ОЦЕНКА ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Контроль результатов самостоятельной работы проводится преподавателем одновременно с текущим и промежуточным контролем знаний обучающихся. Для контроля самостоятельной работы обучающегося используются разнообразные формы и методы: фронтальный, индивидуальный, выборочный, самоконтроль, защита презентации, участие в семинарском занятии, ответы на контрольные вопросы и т. д. При контроле результатов самостоятельной работы используются следующие критерии:

- уровень освоения обучающимся учебного материала;
- умение обучающегося использовать теоретические знания при выполнении заданий;
- обоснованность и чёткость изложения ответа;
- оформления материала в соответствии с требованиями.

Критерии оценки выполненной обучающимися работы:

– оценка «5» - работа выполнена без ошибок; чисто, без исправлений; тема раскрыта полностью;

– оценка «4» - работа выполнена с незначительными ошибками; тема раскрыта не полностью;

– оценка «3» - работа выполнена со значительными ошибками; тема практически не раскрыта;

– оценка «2» - работа не выполнена.

СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

Перечень учебной литературы для освоения дисциплины

№ п/п	Библиографическое описание	Ресурс
1	Компьютерные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2026. — 515 с. — (Профессиональное образование). — ISBN 978-5-534-21453-6. — Текст : электронный // Образовательная платформа Юрайт [сайт].	ЭБС Юрайт
2	Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях : учебник и практикум для среднего профессионального образования / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 423 с. — (Профессиональное образование). — ISBN 978-5-534-16551-7. — Текст : электронный // Образовательная платформа Юрайт [сайт].	ЭБС Юрайт
3	Компьютерные и телекоммуникационные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2026. — 96 с. — (Профессиональное образование). — ISBN 978-5-534-21456-7. — Текст : электронный // Образовательная платформа Юрайт [сайт].	ЭБС Юрайт
4	Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 464 с. — (Профессиональное образование). — ISBN 978-5-534-17310-9. — Текст : электронный // Образовательная платформа Юрайт [сайт].	ЭБС Юрайт
5	Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебник для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2025. — 167 с. — (Профессиональное образование). — ISBN 978-5-534-17558-5. — Текст : электронный // Образовательная	ЭБС Юрайт

№ п/п	Библиографическое описание	Ресурс
	платформа Юрайт [сайт].	
6	Компьютерные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2026. — 515 с. — (Профессиональное образование). — ISBN 978-5-534-21453-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590199 (дата обращения: 19.01.2026).	ЭБС Юрайт
7	Рабчевский, А. Н. Компьютерные сети и системы связи. Вводный курс : учебное пособие для среднего профессионального образования / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2026. — 207 с. — (Профессиональное образование). — ISBN 978-5-534-21488-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589740 (дата обращения: 19.01.2026).	ЭБС Юрайт

3.2.3. Дополнительные источники

1. http://digital-edu.ru – справочник образовательных ресурсов «Портал цифрового образования».
2. http://fcior.edu.ru – Федеральный центр информационно-образовательных ресурсов (ФЦИОР).
3. http://school-collection.edu.ru – Единая коллекция цифровых образовательных ресурсов.
4. http://window.edu.ru – Единое окно доступа к образовательным ресурсам Российской Федерации.
5. http://www.intuit.ru – открытые Интернет-курсы «Интуит».
6. https://stepik.org/catalog - бесплатные онлайн-курсы.

Перечень учебно-методического обеспечения

№ п/п	Библиографическое описание	Ресурс
1	Соколова, О.И. Вычислительные и инфокоммуникационные системы и сети: учеб.-метод. пособие для выполнения практических работ / О. И. Соколова; ФГБОУ ВО РГУПС. - Ростов н/Д: [б. и.], 2017. - 29 с. - Библиогр.- Текст : электронный	ЭБС РГУПС

2	Соколова, О.И. Вычислительные и инфокоммуникационные системы и сети: учеб.-метод. пособие для выполнения лабораторных работ / О. И. Соколова; ФГБОУ ВО РГУПС. - Ростов н/Д: [б. и.], 2017. - 67 с. - Библиогр.- Текст : электронный	ЭБС РГУПС
3	Соколова, О.И. Теоретические основы: сети, телекоммуникации и инфокоммуникационные системы: Учебно-методическое пособие для выполнения лабораторных работ / О. И. Соколова; ФГБОУ ВО РГУПС. - Ростов н/Д: [б. и.], 2017. - 88 с. - Библиогр.- Текст : электронный	ЭБС РГУПС
4	Соколова, О. И. Теория информационных процессов: кодирование и шифрование : учеб.-метод. пособие для выполнения лабораторных работ / О. И. Соколова ; ФГБОУ ВО РГУПС. - Ростов н/Д : [б. и.], 2017. - 44 с. - Библиогр. - Текст : электронный.	ЭБС РГУПС