Приложение 2.29.1 к ОПОП по специальности
09.02.11 Разработка и управление программным обеспечением

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

Многопрофильный колледж

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ЛАБОРАТОРНЫХ И ПРАКТИЧЕСКИХ ЗАНЯТИЙ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.07 КОМПЬЮТЕРНЫЕ СЕТИ

для обучающихся специальности
09.02.11 Разработка и управление программным обеспечением

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Важную часть теоретической и профессиональной практической подготовки обучающихся составляют практические и лабораторные занятия.

Состав и содержание практических и лабораторных занятий направлены на реализацию Федерального государственного образовательного стандарта среднего профессионального образования.

Ведущей дидактической целью практических занятий является формирование профессиональных практических умений (умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности) или учебных практических умений (организовывать и конфигурировать КС, устанавливать и настраивать параметры протоколов.), необходимых в последующей учебной деятельности.

Ведущей дидактической целью лабораторных занятий является экспериментальное подтверждение и проверка существенных теоретических положений (законов, зависимостей).

В соответствии с рабочей программой учебной дисциплины «Компьютерные сети» предусмотрено проведение практических и лабораторных занятий.

В результате их выполнения, обучающийся должен уметь:

Уд 1_ОП.07 организовывать и конфигурировать компьютерные сети

Уд 2_ОП.07 строить и анализировать модели компьютерных сетей

Уд 3_ОП.07 работать с протоколами разных уровней

Уд 4_ОП.07 устанавливать и настраивать параметры протоколов

Уд 5_ОП.07 проводить сбор и анализ исходных данных по сетевой инфраструктуре

Содержание практических и лабораторных занятий ориентировано на подготовку обучающихся к освоению профессиональных модулей программы подготовки специалистов среднего звена по специальности и овладению ***профессиональными компетенциями:***

ПК 1.5. Защищать информацию в базе данных с использованием технологий защиты информации.

А также формированию *общих компетенций*:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.

Практические и лабораторные занятия проводятся в рамках соответствующей темы, после освоения дидактических единиц, которые обеспечивают наличие знаний, необходимых для ее выполнения.

2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Тема 1.2 Сетевые модели и протоколы

Лабораторное занятие №1

Расчёт IP-адресов и масок подсетей

Цель: _Сформировать умения рассчитывать параметры подсетей: адрес сети, адрес широковещательной рассылки, диапазон допустимых адресов хостов, количество хостов — методом CIDR

Выполнив работу, вы будете уметь:

Уд 3_ОП.07 работать с протоколами разных уровней; Уд 4_ОП.07 устанавливать и настраивать параметры протоколов; Уо 01.03 определять этапы решения задачи; Уо 02.06 оформлять результаты поиска.

Материальное обеспечение:

ПК с ОС Windows/Linux; браузер; онлайн-калькулятор подсетей (subnet-calculator.org); электронные таблицы (LibreOffice Calc / MS Excel).

Задание:

1. Для каждого из 5 вариантов (см. таблицу 1) рассчитайте: маску подсети в формате /N и в записи x.x.x.x; адрес сети; широковещательный адрес; диапазон допустимых IP-адресов хостов; максимальное количество хостов.

2. Разбейте сеть 10.0.0.0/8 на 16 равных подсетей; для каждой укажите адрес сети, маску и диапазон хостов.

3. Определите, принадлежат ли адреса 172.16.5.10 и 172.16.5.200 одной подсети при маске /25. Обоснуйте ответ.

Порядок выполнения работы:

1. Откройте электронную таблицу. Создайте столбцы: IP-адрес, Префикс, Маска (x.x.x.x), Адрес сети, Широковещательный, Первый хост, Последний хост, Кол-во хостов.

2. Задание 1: введите IP-адреса из варианта. Для каждого вычислите количество хостовых битов: h = 32 − N.

3. Вычислите количество адресов: 2^h. Максимально хостов: 2^h − 2.

4. Найдите маску подсети в формате x.x.x.x: сетевые биты = 1, хостовые биты = 0. Переведите каждый октет из двоичной в десятичную.

5. Вычислите адрес сети: выполните побитовое AND IP-адреса с маской (в каждом октете умножьте числа побитно). Запишите результат.

6. Широковещательный адрес: возьмите адрес сети, замените все хостовые биты на 1 (в последних (32−N) битах поставьте 1). Или: широковещательный = адрес сети + (2^h − 1).

7. Первый хост = адрес сети + 1. Последний хост = широковещательный − 1.

8. Задание 2: сеть 10.0.0.0/8, нужно 16 подсетей. Новый префикс: /N = /8 + $\log_2(16)$ = /12. Перечислите 16 подсетей с шагом 2^20 адресов.

9. Задание 3: преобразуйте оба адреса в двоичную, наложите маску /25, сравните сетевые части.

10. Занесите результаты в таблицу, сделайте вывод о методе CIDR.

11. Пример выполнения: Расчёт подсети 192.168.1.64/26

Дано: 192.168.1.64/26

Шаг 1. Хостовые биты: h = 32 − 26 = 6

Шаг 2. Кол-во адресов: 2^6 = 64. Хостов: 64 − 2 = 62

Шаг 3. Маска: 11111111.11111111.11111111.11000000 = 255.255.255.192

Шаг 4. Адрес сети:

192 AND 255 = 192

168 AND 255 = 168

1 AND 255 = 1

64 AND 192 = 64 (01000000 AND 11000000 = 01000000)

Адрес сети: 192.168.1.64

Шаг 5. Широковещательный: 64 + 64 − 1 = 127 → 192.168.1.127

Шаг 6. Диапазон: 192.168.1.65 — 192.168.1.126

Итого хостов: 62

Форма представления результата: Отчёт содержит таблицу расчётов для всех вариантов задания, ответы на задания 2–3 и ответы на контрольные вопросы.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Лабораторное занятие №2

Тестирование сетевого подключения с помощью команд ping, traceroute, netstat

Цель: Сформировать умения диагностировать сетевые соединения с помощью стандартных утилит, интерпретировать результаты и составлять протокол диагностики.

Выполнив работу, вы будете уметь:
Уд 3_ОП.07 работать с протоколами разных уровней;
Уд 4_ОП.07 устанавливать и настраивать параметры протоколов;
Уо 01.06 реализовывать составленный план;
Уо 02.07 использовать современное ПО.

Материальное обеспечение:
ПК с ОС Windows 10/11 и/или Linux (Ubuntu); доступ к сети Интернет; командная строка (CMD / PowerShell / Bash).

Задание:
1. Выполните ping до трёх различных узлов: локального шлюза (default gateway), google.com и одноклассника. Зафиксируйте RTT и процент потерь.

2. Выполните traceroute/tracert до google.com и до 8.8.8.8. Определите количество хопов и IP-адреса промежуточных маршрутизаторов.

3. Используя netstat -an, определите, какие порты открыты на вашем ПК. Найдите порты 80, 443, 22 (если открыты) и объясните, какие сервисы на них работают.

4. Используя nslookup, определите IP-адрес домена magtu.ru и узнайте адрес DNS-сервера, который используется.

Порядок выполнения работы: (1. Откройте командную строку (Windows: Win+R → cmd; Linux: Ctrl+Alt+T).

2. Определите IP-адрес шлюза: Windows — ipconfig, найдите «Основной шлюз»; Linux — ip route | grep default.

3. Выполните ping до шлюза: ping <IP шлюза> -n 10 (Windows) или ping -c 10 <IP шлюза> (Linux). Скопируйте вывод в отчёт.

4. Выполните ping google.com -n 10. Зафиксируйте min/avg/max RTT и процент потерь.

5. Выполните tracert google.com (Windows) или traceroute google.com (Linux). Дождитесь завершения (или нажмите Ctrl+C через 30 с). Скопируйте вывод.

6. Подсчитайте количество хопов до google.com. Найдите хоп, на котором время резко возрастает (выход в Интернет).

7. Выполните netstat -an. Из вывода выберите не менее 5 соединений в состоянии ESTABLISHED и занесите их в таблицу (локальный адрес:порт, удалённый адрес:порт, состояние).

8. Выполните nslookup magtu.ru. Запишите полученный IP-адрес и адрес DNS-сервера.

9. Оформите вывод каждой команды в отчёт, добавьте интерпретацию результатов.

10. Пример выполнения: Анализ вывода ping

C:\> ping google.com -n 5

Обмен пакетами с google.com [142.250.74.46]:

Ответ от 142.250.74.46: число байт=32 время=20мс TTL=118

Ответ от 142.250.74.46: число байт=32 время=19мс TTL=118

Ответ от 142.250.74.46: число байт=32 время=21мс TTL=118

Ответ от 142.250.74.46: число байт=32 время=20мс TTL=118

Ответ от 142.250.74.46: число байт=32 время=22мс TTL=118

Статистика Ping для 142.250.74.46:

Пакетов: отправлено = 5, получено = 5, потеряно = 0 (0% потерь)

Приблизительное время приёма-передачи в мс:

Минимальное = 19мс, Максимальное = 22мс, Среднее = 20мс

Вывод: узел доступен, потерь нет, RTT ~20 мс (норма для международного сервера).

Форма представления результата: Отчёт со скриншотами или копиями вывода каждой команды, таблицей открытых портов и ответами на контрольные вопросы.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Лабораторное занятие №3

Настройка адресации и маршрутизации

Цель: Сформировать умения настраивать статические IP-адреса на хостах, добавлять статические маршруты, проверять связность сетей в среде симулятора Cisco Packet Tracer.

Выполнив работу, вы будете уметь:

Уд 1_ОП.07 организовывать и конфигурировать КС; Уд 4_ОП.07 устанавливать и настраивать параметры протоколов; Уо 01.06 реализовывать составленный план; Уо 02.07 использовать современное ПО.

Материальное обеспечение:

ПК с ОС Windows/Linux; Cisco Packet Tracer 8.x (или GNS3); методическое пособие с топологией.

Задание:

1. Создайте топологию в Cisco Packet Tracer: 2 маршрутизатора (R1, R2), соединённые последовательным (Serial) или Ethernet-каналом; к R1 подключена подсеть 192.168.1.0/24 с двумя ПК; к R2 — подсеть 192.168.2.0/24 с двумя ПК.

2. Настройте IP-адреса на всех интерфейсах маршрутизаторов и на всех хостах.

3. Добавьте статические маршруты на R1 и R2 так, чтобы хосты разных подсетей могли обмениваться данными.

4. Проверьте связность командой ping: с PC0 до PC2 (из разных подсетей). Зафиксируйте результат.

Порядок выполнения работы:

1. Запустите Cisco Packet Tracer. Откройте новую пустую топологию.

2. Добавьте 2 маршрутизатора (Router 2911). Соедините их через интерфейс GigabitEthernet0/1 (или Serial) кабелем типа Copper Cross-over или Serial DCE.

3. Добавьте 2 коммутатора (Switch 2960) и 4 ПК. Подключите: PC0, PC1 → Switch0 → R1 (GE0/0); PC2, PC3 → Switch1 → R2 (GE0/0). Используйте кабель Copper Straight-Through.

4. Настройте R1: щёлкните по R1 → CLI. Введите команды:

5. enable
6. configure terminal
7. interface GigabitEthernet0/0
8. ip address 192.168.1.1 255.255.255.0
9. no shutdown
10. interface GigabitEthernet0/1
11. ip address 10.0.0.1 255.255.255.252
12. no shutdown
13. exit

14. Настройте R2 аналогично: GE0/0 — 192.168.2.1/24; GE0/1 — 10.0.0.2/24.

15. Добавьте статические маршруты на R1:

16. ip route 192.168.2.0 255.255.255.0 10.0.0.2

17. На R2:

18. ip route 192.168.1.0 255.255.255.0 10.0.0.1

19. Настройте хосты: PC0 — 192.168.1.10/24, gateway 192.168.1.1; PC2 — 192.168.2.10/24, gateway 192.168.2.1.

20. Выполните ping с PC0 до PC2 в Packet Tracer (Desktop → Command Prompt). Зафиксируйте вывод.

21. Пример выполнения: Настройка интерфейса R1 (GE0/0)

Router> enable

Router# configure terminal

Router(config)# hostname R1

R1(config)# interface GigabitEthernet0/0

R1(config-if)# ip address 192.168.1.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# description LAN_SUBNET_1

R1(config-if)# exit

R1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2

R1(config)# end

R1# show ip route

S 192.168.2.0/24 [1/0] via 10.0.0.2

Форма представления результата: Файл топологии (.pkt) с настроенными маршрутами, скриншоты успешного ping, вывод команды show ip route на обоих маршрутизаторах.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Лабораторное занятие №4

Настройка DHCP и DNS-сервера

Цель: Сформировать умения устанавливать и конфигурировать DHCP-сервер для автоматической выдачи IP-адресов, настраивать DNS-сервер для разрешения имён, проверять работу сервисов.

Выполнив работу, вы будете уметь:
Уд 1_ОП.07 организовывать и конфигурировать КС;
Уд 4_ОП.07 устанавливать и настраивать параметры протоколов;
Уо 02.07 использовать современное ПО;
Уо 02.08 использовать цифровые средства.

Материальное обеспечение:
ПК с ОС Windows Server или Linux (Ubuntu Server); Cisco Packet Tracer; браузер для проверки DNS.

Задание:
1. В Cisco Packet Tracer: создайте топологию с роутером, коммутатором и 3 ПК. Настройте DHCP на роутере для подсети 192.168.10.0/24, исключив адреса .1–.10 из пула. Убедитесь, что ПК получают адреса автоматически.

2. Настройте DHCP-сервер (Server в Packet Tracer или Linux: isc-dhcp-server). Добавьте резервирование (static binding) для одного ПК по MAC-адресу.

3. Настройте DNS-сервер (Server в Packet Tracer). Создайте запись типа A: mysite.local → 192.168.10.20. Проверьте разрешение имени командой nslookup mysite.local с ПК.

Порядок выполнения работы:
1. Создайте топологию в Cisco Packet Tracer: Router2911 — Switch2960 — 3×PC. Укажите ПК режим DHCP (Desktop → IP Configuration → DHCP).

2. Откройте CLI роутера. Настройте интерфейс:

3. enable
4. configure terminal
5. interface GigabitEthernet0/0
6. ip address 192.168.10.1 255.255.255.0
7. no shutdown

8. Исключите служебные адреса из пула:

9. ip dhcp excluded-address 192.168.10.1 192.168.10.10

10. Создайте пул DHCP:

11. ip dhcp pool LAN_POOL
12. network 192.168.10.0 255.255.255.0
13. default-router 192.168.10.1
14. dns-server 8.8.8.8
15. lease 7
16. exit

17. Проверьте: на каждом ПК нажмите «DHCP» в настройках. Должен появиться адрес из диапазона .11–.254.

18. Для DNS: добавьте сервер (Server) с IP 192.168.10.20. В разделе Services → DNS активируйте DNS, добавьте запись: Name = mysite.local, Address = 192.168.10.20.

19. На ПК в командной строке: nslookup mysite.local 192.168.10.20. Убедитесь, что ответ содержит IP 192.168.10.20.

20. Выполните show ip dhcp binding на роутере, скопируйте результат в отчёт.

21. Пример выполнения: Вывод show ip dhcp binding

R1# show ip dhcp binding

Bindings from all pools not associated with VRF:

IP address Client-ID/ Lease expiration Type

Hardware address/

User name

192.168.10.11 0050.0F12.3456 Dec 01 2025 12:00 Automatic

192.168.10.12 0050.0F78.9ABC Dec 01 2025 12:05 Automatic

Комментарий: каждый ПК получил уникальный адрес из пула .11–.254.

Форма представления результата: Файл топологии .pkt, скриншоты IP-конфигурации ПК (показывающие DHCP-адреса), вывод команд show ip dhcp binding и результат nslookup.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Тема 1.3 Среды передачи данных

Лабораторное занятие №5

Монтаж и обжим сетевого кабеля. Создание патч-кордов по стандартам T568A и T568B

Цель: Сформировать практические умения выполнять обжим коннектора RJ-45 на кабель витой пары по стандартам прямого (T568B–T568B) и кроссового (T568A–T568B) обжима, тестировать готовый кабель**.**

Выполнив работу, вы будете уметь:

Уд 1_ОП.07 организовывать и конфигурировать КС; Уд 4_ОП.07 устанавливать и настраивать параметры протоколов; Уо 01.06 реализовывать составленный план; Уо 01.07 оценивать результат.

Материальное обеспечение:

Кабель UTP Cat.5e/Cat.6 (~0,5 м на пару студентов); коннекторы RJ-45 (4 шт.); кримпер (обжимные клещи); стриппер или нож для снятия изоляции; кабелетестер.

Задание:

1. Изготовьте прямой патч-корд (T568B–T568B) длиной ~40 см. Проверьте кабелетестером.
2. Изготовьте кроссовый патч-корд (T568A–T568B) длиной ~40 см. Проверьте кабелетестером.
3. Запишите в таблицу результаты тестирования: для каждого из 8 контактов укажите соответствие «пин А ↔ пин Б».
4. Подключите прямой патч-корд к ПК и коммутатору, убедитесь, что порт коммутатора показывает индикатор связи.

Порядок выполнения работы:

1. Возьмите кабель ~50 см. Снимите внешнюю оболочку на 3 см с помощью стриппера или ножа (не повредив изоляцию жил!).
2. Расправьте пары и разложите жилы в порядке T568B: 1-оранжево-белый, 2-оранжевый, 3-зелено-белый, 4-синий, 5-сине-белый, 6-зелёный, 7-коричнево-белый, 8-коричневый.
3. Сожмите жилы пальцами, выровняйте торцы ножницами или кримпером — торцы должны быть ровными.
4. Держите разъём RJ-45 защёлкой вниз, контактами к себе. Вставьте жилы так, чтобы каждая попала в свою канавку, а торцы жил дошли до края разъёма.
5. Вставьте разъём в соответствующий паз кримпера и сожмите ручки до щелчка. Проверьте: контакты должны «прокусить» изоляцию жил.
6. Повторите шаги 2–5 для второго конца того же кабеля (T568B для прямого, T568A для кроссового).
7. Вставьте оба конца готового кабеля в кабелетестер. Включите тест. Для прямого кабеля показания: 1→1, 2→2, …, 8→8. Для кроссового: 1→3, 2→6, 3→1, 6→2, 4→4, 5→5, 7→7, 8→8.
8. Запишите результаты теста в таблицу отчёта.
9. . Пример выполнения: Порядок проводников T568A и T568B

Контакт	T568B (прямой)	T568A (кросс)
1	Бело-оранжевый	Бело-зелёный

2	Оранжевый	Зелёный
3	Бело-зелёный	Бело-оранжевый
4	Синий	Синий
5	Бело-синий	Бело-синий
6	Зелёный	Оранжевый
7	Бело-коричневый	Бело-коричневый
8	Коричневый	Коричневый

Кроссовый кабель: один конец T568B, другой — T568A.

Прямой кабель: оба конца T568B (или оба T568A).

Форма представления результата: Два готовых патч-корда (прямой и кроссовый), проверенных тестером; таблица с результатами тестирования в отчёте.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Лабораторное занятие №6

Исследование методов доступа CSMA/CD и CSMA/CA в среде сетевого симулятора

Цель: Сформировать умения анализировать принципы работы методов доступа к среде передачи CSMA/CD (Ethernet) и CSMA/CA (Wi-Fi), исследовать поведение сети при коллизиях в симуляторе.

Выполнив работу, вы будете уметь:
Уд 2 строить и анализировать модели КС;
Уд 3_ОП.07 работать с протоколами разных уровней;
Уо 01.02 анализировать задачу;
Уо 02.06 оформлять результаты поиска.

Материальное обеспечение:
ПК; Cisco Packet Tracer 8.x (режим симуляции); методические материалы.

Задание:

1. В Cisco Packet Tracer создайте топологию Hub + 3 ПК. В режиме симуляции (Simulation Mode) отправьте одновременно пакеты от двух ПК. Наблюдайте и зафиксируйте коллизию.

2. Замените Hub на Switch. Повторите эксперимент. Сравните результаты: есть ли коллизии?

3. Создайте топологию с точкой доступа Wi-Fi (Wireless Router) и 2 беспроводными ПК. В режиме симуляции исследуйте процесс передачи: наблюдайте ACK-пакеты.

4. Сформулируйте вывод: в каком случае CSMA/CD, а в каком CSMA/CA эффективнее и почему?

Порядок выполнения работы:

1. Запустите Cisco Packet Tracer. Создайте топологию: Hub (концентратор) → PC0, PC1, PC2 (соедините Straight-Through).

2. Переключитесь в режим Simulation (Ctrl+Alt+S). Установите фильтр Event List: оставьте ICMP и Ethernet.

3. С PC0 выполните ping 10.0.0.2 (адрес PC1), одновременно нажмите Simple PDU с PC2 до PC0. Нажмите Play. Наблюдайте коллизию в Event List (пакеты с одинаковой меткой времени).

4. Зафиксируйте количество попыток до успешной доставки (счётчик ретрансмиссий в Properties пакета).

5. Замените Hub на Switch 2960. Повторите те же отправки. Убедитесь, что коллизий нет: каждый порт — отдельный домен коллизий.

6. Добавьте Wireless Router (Generic) и 2 PC с Wi-Fi-адаптером (замените адаптер в PC: Linksys WMP300N). Настройте SSID и пароль точки доступа.

7. В режиме симуляции отправьте ICMP с одного беспроводного ПК до другого. Найдите в Event List пакеты ACK — они подтверждают механизм CSMA/CA.

8. Заполните сравнительную таблицу в отчёте: CSMA/CD vs CSMA/CA — среда, стандарт, обнаружение/предотвращение коллизий, ACK, RTS/CTS.

9.Пример выполнения: Сравнительная таблица CSMA/CD и CSMA/CA

Параметр	CSMA/CD	CSMA/CA
Стандарт	IEEE 802.3 (Ethernet)	IEEE 802.11 (Wi-Fi)
Среда	Проводная (витая пара)	Беспроводная (радио)

Метод | Обнаружение коллизии | Предотвращение коллизии
Действие при кол. | Jam + backoff + повтор | Random backoff + повтор
ACK | Нет (для unicast) | Да (каждый кадр)
RTS/CTS | Нет | Опционально (для скр.)
Коллизии сегодня | Устранены коммутаторами | Сведены к минимуму

Форма представления результата: Файл топологии .pkt с двумя экспериментами (Hub и Switch), сравнительная таблица CSMA/CD vs CSMA/CA, скриншоты из режима симуляции.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Тема 1.4 Аппаратное обеспечение компьютерных сетей

Лабораторное занятие №7

Базовая настройка маршрутизатора

Цель: Сформировать умения подключаться к маршрутизатору через консоль, настраивать имя устройства, пароли, интерфейсы, базовые параметры безопасности и сохранять конфигурацию.

Выполнив работу, вы будете уметь:

Уд 1_ОП.07 организовывать и конфигурировать КС; Уд 4_ОП.07 устанавливать и настраивать параметры протоколов; Уо 01.06 реализовывать составленный план; Уо 02.07 использовать современное ПО.

Материальное обеспечение:

ПК с ОС Windows/Linux; Cisco Packet Tracer 8.x или реальный маршрутизатор + PuTTY; консольный кабель (RJ-45 → DB9/USB).

Задание:

1. Выполните базовую конфигурацию маршрутизатора R1: задайте имя, зашифрованный пароль привилегированного режима, пароль консоли и VTY-линий, сообщение дня (MOTD banner).
2. Настройте два интерфейса: LAN (GE0/0, адрес 192.168.1.1/24) и WAN (GE0/1, адрес 10.0.0.1/30). Проверьте командой show interfaces.
3. Сохраните конфигурацию. Выполните reload и убедитесь, что настройки сохранились.
4. Настройте SSH v2 для удалённого управления: создайте пользователя admin, настройте домен, сгенерируйте ключи RSA.

Порядок выполнения работы:

1. Откройте Cisco Packet Tracer. Добавьте Router 2911. Щёлкните по нему → CLI.
2. Войдите в привилегированный режим и в режим конфигурации:
3. Router> enable
4. Router# configure terminal
5. Задайте имя устройства:
6. Router(config)# hostname R1
7. Установите зашифрованный пароль привилегированного режима:
8. R1(config)# enable secret Cisco123
9. Настройте пароль консоли:
10. R1(config)# line console 0
11. R1(config-line)# password Console123
12. R1(config-line)# login
13. R1(config-line)# exit
14. Настройте VTY (Telnet/SSH):
15. R1(config)# line vty 0 4

16. R1(config-line)# password Vty123
17. R1(config-line)# login
18. R1(config-line)# transport input ssh
19. R1(config-line)# exit
20. Задайте баннер MOTD:
21. R1(config)# banner motd # Unauthorized access prohibited! #
22. Настройте интерфейс LAN:
23. R1(config)# interface GigabitEthernet0/0
24. R1(config-if)# ip address 192.168.1.1 255.255.255.0
25. R1(config-if)# description LAN
26. R1(config-if)# no shutdown
27. R1(config-if)# exit
28. Сохраните конфигурацию:
29. R1# copy running-config startup-config
30. Проверьте: R1# show running-config | R1# show ip interface brief
31. Пример выполнения: Вывод show ip interface brief

R1# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.1	YES	manual	up	up
GigabitEthernet0/1	10.0.0.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	down	down

Пояснение: Status = up означает физическое подключение,

Protocol = up означает, что канальный уровень работает.

Если Protocol = down — проблема с настройкой или нет no shutdown.

Форма представления результата: Файл топологии .pkt с сохранённой конфигурацией R1; вывод команд show running-config и show ip interface brief в отчёте.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Лабораторное занятие №8

Настройка сетевых адаптеров. Создание и управление сетевыми соединениями в ОС Windows/Linux

Цель: Сформировать умения настраивать параметры сетевого адаптера в ОС Windows и Linux, создавать сетевые мосты и VLAN-интерфейсы, применять утилиты диагностики ipconfig/ifconfig/ip.

Выполнив работу, вы будете уметь:

Уд 1_ОП.07 организовывать и конфигурировать КС; Уд 4_ОП.07 устанавливать и настраивать параметры протоколов; Уо 01.06 реализовывать составленный план; Уо 02.07 использовать современное ПО.

Материальное обеспечение:

ПК с ОС Windows 10/11; ВМ Linux (Ubuntu 22.04) в VirtualBox/VMware; PuTTY.

Задание:

1. В Windows: настройте статический IP-адрес (192.168.1.50/24, шлюз 192.168.1.1, DNS 8.8.8.8) через графический интерфейс и через командную строку (netsh). Выведите результат ipconfig /all.

2. В Linux (Ubuntu): настройте статический IP через Netplan. Проверьте с помощью ip addr show и ip route show.

3. В Linux: создайте VLAN-интерфейс eth0.100 с адресом 192.168.100.1/24. Убедитесь, что он виден в ip addr.

4. Сравните вывод команд ipconfig (Windows) и ip addr (Linux) в таблице

Порядок выполнения работы:

1. Windows — GUI: Панель управления → Сеть → Ethernet → Свойства → IPv4 → Свойства. Введите IP: 192.168.1.50, маску: 255.255.255.0, шлюз: 192.168.1.1, DNS: 8.8.8.8. ОК. Откройте CMD, выполните ipconfig /all. Скопируйте вывод.

2. Windows — CLI: откройте CMD от имени администратора:

3. netsh interface ip set address name="Ethernet" static 192.168.1.51 255.255.255.0 192.168.1.1

4. netsh interface ip set dns name="Ethernet" static 8.8.8.8

5. ipconfig /all

6. Верните DHCP: netsh interface ip set address name="Ethernet" dhcp

7. Linux — статический IP через Netplan:

8. sudo nano /etc/netplan/01-netcfg.yaml

9. Введите содержимое (пример в разделе 4). Сохраните. Примените:

10. sudo netplan apply

11. ip addr show

12. ip route show

13. Linux — создание VLAN:

14. sudo ip link add link eth0 name eth0.100 type vlan id 100

15. sudo ip addr add 192.168.100.1/24 dev eth0.100

16. sudo ip link set eth0.100 up

17. ip addr show eth0.100

18. Оформите сравнительную таблицу команд Windows vs Linux в отчёте.

19. Пример выполнения: Конфиг Netplan (Ubuntu 22.04)

```
    # /etc/netplan/01-netcfg.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
        eth0:
          addresses:
            - 192.168.1.50/24
          routes:
            - to: default
              via: 192.168.1.1
          nameservers:
            addresses:
              - 8.8.8.8
              - 1.1.1.1
```

Форма представления результата: Скриншоты вывода ipconfig /all (Windows) и ip addr show, ip route show (Linux); конфиг Netplan; сравнительная таблица команд.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Лабораторное занятие №9

Организация межсетевого взаимодействия. Настройка веб-сервера (Apache/Nginx)

Цель: Сформировать умения настраивать маршрутизацию между подсетями, устанавливать и конфигурировать веб-сервер Apache или Nginx, проверять доступность веб-ресурса из другой подсети.

Выполнив работу, вы будете уметь:

Уд 1_ОП.07 организовывать и конфигурировать КС; Уд 4_ОП.07 устанавливать и настраивать параметры протоколов; Уо 02.07 использовать современное ПО; Уо 02.08 использовать цифровые средства.

Материальное обеспечение:

ПК с ОС Linux (Ubuntu 22.04); VirtualBox (2 ВМ); браузер; Cisco Packet Tracer.

Задание:

1. Создайте в VirtualBox две ВМ Ubuntu: «Сервер» (IP 192.168.10.1/24) и «Клиент» (IP 192.168.20.1/24). Соедините их через третью ВМ-маршрутизатор с двумя сетевыми интерфейсами, обеспечив маршрутизацию между подсетями.

2. На ВМ «Сервер» установите Apache2. Создайте страницу index.html с содержимым «Добро пожаловать на сервер КС ОП.07!». Убедитесь, что сервер отвечает на запросы.

3. С ВМ «Клиент» откройте браузер и перейдите по адресу http://192.168.10.1. Убедитесь в успешном отображении страницы.

4. Настройте виртуальный хост для домена mylab.local. Добавьте запись в /etc/hosts на клиенте и проверьте доступность по имени.

Порядок выполнения работы:

1. На ВМ «Сервер» установите Apache:
2. sudo apt update && sudo apt install apache2 -y
3. sudo systemctl start apache2
4. sudo systemctl enable apache2
5. Проверьте: curl http://localhost — должна отображаться дефолтная страница Apache.
6. Создайте кастомную страницу:
7. sudo nano /var/www/html/index.html
8. Введите: <h1>Добро пожаловать на сервер КС ОП.07!</h1>. Сохраните.
9. На маршрутизаторе (третья ВМ) включите IP forwarding:
10. sudo sysctl -w net.ipv4.ip_forward=1
11. Добавьте маршруты на «Сервер» и «Клиент»:
12. # На Сервере (в сторону подсети 192.168.20.0/24):
13. sudo ip route add 192.168.20.0/24 via <IP маршрутизатора>
14. С ВМ «Клиент» выполните: curl http://192.168.10.1 или откройте браузер.
15. Создайте виртуальный хост для mylab.local:
16. sudo nano /etc/apache2/sites-available/mylab.local.conf
17. Введите конфигурацию (пример в разделе 4). Активируйте: sudo a2ensite mylab.local; sudo systemctl reload apache2.

18. На клиенте добавьте в /etc/hosts: 192.168.10.1 mylab.local. Откройте http://mylab.local в браузере.

19. Пример выполнения: Конфиг виртуального хоста Apache

```
# /etc/apache2/sites-available/mylab.local.conf
<VirtualHost *:80>
   ServerName mylab.local
   ServerAlias www.mylab.local
   DocumentRoot /var/www/mylab
   ErrorLog ${APACHE_LOG_DIR}/mylab_error.log
   CustomLog ${APACHE_LOG_DIR}/mylab_access.log combined
   <Directory /var/www/mylab>
      Options Indexes FollowSymLinks
      AllowOverride All
      Require all granted
   </Directory>
</VirtualHost>


# Создать директорию и страницу:
$ sudo mkdir -p /var/www/mylab
$ echo '<h1>mylab.local OK</h1>' | sudo tee /var/www/mylab/index.html
```

Форма представления результата: Скриншот браузера на клиенте с открытой страницей сервера; вывод curl с сервера и клиента; конфиг виртуального хоста в отчёте.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Тема 1.5 Безопасность компьютерных сетей

Лабораторное занятие №10

Сбор и анализ сетевого трафика с помощью Wireshark. Настройка защищённых соединений HTTPS

Цель: Сформировать умения перехватывать и анализировать сетевые пакеты с помощью Wireshark, выявлять незащищённые передачи данных, настраивать самоподписанный TLS-сертификат для HTTPS.

Выполнив работу, вы будете уметь:

Уд 3_ОП.07 работать с протоколами разных уровней; Уд 5 проводить сбор и анализ исходных данных по сетевой инфраструктуре; Уо 02.06 оформлять результаты; Уо 02.08 использовать цифровые средства.

Материальное обеспечение:

ПК с ОС Windows/Linux; Wireshark (бесплатная лицензия); Apache/Nginx с OpenSSL; браузер.

Задание:

1. Запустите Wireshark. Откройте браузер, перейдите на http://httpbin.org/get. В Wireshark применените фильтр http и найдите GET-запрос. Убедитесь, что заголовки видны в открытом виде.

2. Создайте самоподписанный TLS-сертификат OpenSSL. Настройте Apache/Nginx на работу по HTTPS (порт 443). Перезапустите сервер.

3. В Wireshark захватите HTTPS-трафик при обращении к своему серверу. Убедитесь, что данные не читаемы (TLS Application Data). Сравните HTTP и HTTPS пакеты.

4. Составьте таблицу сравнения: HTTP vs HTTPS — порт, шифрование, видимость данных в Wireshark.

Порядок выполнения работы:

1. Запустите Wireshark. Выберите интерфейс (Ethernet или Wi-Fi). Нажмите значок акулы (Start).

2. В браузере откройте: http://neverssl.com (или http://httpbin.org/get). В Wireshark введите фильтр: http. Найдите пакет с методом GET. Щёлкните на пакет → Packet Details → Hypertext Transfer Protocol. Скриншот.

3. Создайте сертификат OpenSSL (Linux):

4. $ sudo openssl req -x509 -newkey rsa:2048 -keyout /etc/ssl/private/mylab.key \

5. -out /etc/ssl/certs/mylab.crt -sha256 -days 365 -nodes \

6. -subj '/CN=mylab.local/O=MGTU/C=RU'

7. Включите модуль SSL и настройте Apache:

8. $ sudo a2enmod ssl

9. $ sudo nano /etc/apache2/sites-available/default-ssl.conf

10. Укажите пути к сертификату: SSLCertificateFile /etc/ssl/certs/mylab.crt; SSLCertificateKeyFile /etc/ssl/private/mylab.key

11. $ sudo a2ensite default-ssl

12. $ sudo systemctl restart apache2

13. В Wireshark установите фильтр: tcp.port == 443. Обратитесь к https://localhost в браузере (примите предупреждение о сертификате). Убедитесь, что в Wireshark пакеты помечены TLSv1.3 и тело запроса нечитаемо.

14. Сравните захваченные пакеты HTTP и HTTPS в таблице отчёта.

15. Пример выполнения: Фильтры Wireshark и примеры

Популярные фильтры Wireshark:

http — только HTTP-трафик

dns — только DNS-запросы/ответы

tcp.port == 443 — HTTPS-трафик

ip.addr == 192.168.1.1 — трафик с/на данный IP

http.request.method == "POST" — только POST-запросы

tcp.flags.syn == 1 — TCP SYN-пакеты (начало соединения)

Пример: HTTP-запрос GET виден в деталях пакета:

```
GET /get HTTP/1.1
Host: httpbin.org
User-Agent: Mozilla/5.0 ...
```

HTTPS-пакет: Application Data (зашифровано, нечитаемо).

Форма представления результата: Скриншоты Wireshark с HTTP-пакетом (видимые данные) и HTTPS-пакетом (зашифровано); конфиг HTTPS Apache/Nginx; сравнительная таблица HTTP vs HTTPS.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Тема 1.6 Сетевые технологии в разработке программного обеспечения (вариативная)

Лабораторное занятие №11

Настройка удалённого доступа к серверу. Работа с протоколами SSH и RDP

Цель: Сформировать умения настраивать и использовать SSH для защищённого управления Linux-сервером, применять аутентификацию по ключам, настраивать туннелирование портов; подключаться к Windows по RDP.

Выполнив работу, вы будете уметь:

Уд 1_ОП.07 организовывать и конфигурировать КС; Уд 4_ОП.07 устанавливать и настраивать параметры протоколов; Уо 02.07 использовать современное ПО; Уо 02.08 использовать цифровые средства.

Материальное обеспечение:

ПК с ОС Windows (клиент); ВМ Linux Ubuntu (сервер); PuTTY или OpenSSH; WinSCP или FileZilla; Windows с включённым RDP (или ВМ Windows Server).

Задание:

1. Установите SSH-сервер на ВМ Linux. Подключитесь по паролю с ПК Windows через PuTTY или командную строку (ssh). Выполните команду uptime и ls /var/log.

2. Создайте пару SSH-ключей на Windows. Скопируйте публичный ключ на сервер. Подключитесь без пароля.

3. Настройте SSH-туннель для доступа к веб-серверу сервера: ssh -L 8080:localhost:80 user@<IP_сервера>. Откройте http://localhost:8080 в браузере.

4. Подключитесь к Windows-хосту по RDP. Выполните скриншот рабочего стола удалённой машины.

5. Передайте файл на сервер через SCP или SFTP (WinSCP/FileZilla). Скриншот успешной передачи.

Порядок выполнения работы:

1. На ВМ Linux установите OpenSSH-Server:

2. $ sudo apt update && sudo apt install openssh-server -y

3. $ sudo systemctl enable ssh && sudo systemctl start ssh

4. $ sudo systemctl status ssh # убедитесь: active (running)

5. С Windows (PowerShell или CMD) подключитесь:

6. ssh student@192.168.1.100

7. Введите пароль. Выполните: uptime и ls /var/log. Скриншот.

8. Генерация ключей на Windows (PowerShell):

9. ssh-keygen -t ed25519 -C "student@college"

10. # ключи сохранятся в C:\Users\<user>\.ssh\

11. Копирование публичного ключа на сервер:

12. ssh-copy-id student@192.168.1.100

13. # или вручную: скопируйте содержимое id_ed25519.pub в ~/.ssh/authorized_keys на сервере

14. Проверьте вход без пароля:

15. ssh student@192.168.1.100 # пароль спрашиваться не должен

16. SSH-туннель:

17. ssh -L 8080:localhost:80 student@192.168.1.100

18. Откройте браузер, http://localhost:8080 — должна открыться страница с сервера.

19. RDP (Windows): Пуск → mstsc.exe → введите IP Windows-хоста → Подключить → Введите имя/пароль. Скриншот.

20. SCP (Linux/Windows PowerShell):

21. scp C:\test.txt student@192.168.1.100:/home/student/

22. Пример выполнения: Подключение SSH с ключом (вывод терминала)

PS C:\Users\student> ssh student@192.168.1.100

Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0 x86_64)

Last login: Mon Dec 1 10:00:00 2025 from 192.168.1.50

student@ubuntu-server:~$ uptime

 10:05:12 up 2 days, 3:22, 1 user, load average: 0.08, 0.05, 0.01

student@ubuntu-server:~$ hostname -I

192.168.1.100

Комментарий: подключение без пароля (аутентификация по ключу Ed25519).

Сессия зашифрована протоколом TLS/SSH, данные недоступны перехватчику.

Форма представления результата: Скриншоты: подключение SSH (с ключом), браузер через SSH-туннель, RDP-сессия, передача файла по SCP/SFTP; конфиг sshd_config (фрагмент).

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Лабораторное занятие №12

Разработка и тестирование клиент-серверного приложения с использованием REST API

Цель: Сформировать умения реализовывать HTTP-клиент и HTTP-сервер с REST API на Python, выполнять GET/POST запросы, обрабатывать JSON-ответы, тестировать API через Postman.

Выполнив работу, вы будете уметь:

Уд 3_ОП.07 работать с протоколами разных уровней; Уд 4_ОП.07 устанавливать и настраивать параметры протоколов; Уо 02.07 использовать современное ПО; Уо 02.08 использовать цифровые средства.

Материальное обеспечение:

ПК с ОС Windows/Linux; Python 3.10+; библиотеки Flask, requests (pip install); Postman; VSCode.

Задание:

1. Напишите REST API сервер на Flask: реализуйте endpoints GET /api/students (вернуть список студентов), POST /api/students (добавить студента), GET /api/students/<id> (вернуть студента по ID).
2. Напишите клиент на Python (библиотека requests): получите список студентов, добавьте нового студента через POST, получите его по ID.
3. Протестируйте API через Postman: отправьте все три запроса, скриншоты вкладки Response.
4. Добавьте обработку ошибок: 404 (студент не найден), 400 (некорректные данные).

Порядок выполнения работы:

1. Установите Flask: pip install flask requests. Создайте файл server.py.
2. Реализуйте сервер (см. пример в разделе 4). Запустите: python server.py.
3. В браузере или Postman откройте: GET http://localhost:5000/api/students — убедитесь в ответе JSON.
4. Создайте файл client.py. Реализуйте три запроса:

```
# GET список
import requests
r = requests.get('http://localhost:5000/api/students')
print(r.status_code, r.json())
# POST новый студент
data = {'name': 'Иванов Иван', 'group': '22-ПО-1'}
r = requests.post('http://localhost:5000/api/students', json=data)
print(r.status_code, r.json())
# GET по ID
r = requests.get('http://localhost:5000/api/students/1')
print(r.status_code, r.json())
```

16. Запустите python client.py. Проверьте статус-коды и тела ответов.
17. Откройте Postman. Создайте коллекцию «КС ОП.07». Добавьте 3 запроса (GET list, POST, GET by id). Выполните каждый. Скриншоты.

18. Добавьте обработку 404: если студент с id не найден — вернуть {'error': 'Not found'}, статус 404.

19. Пример выполнения: Код REST API сервера на Flask (server.py)

```
from flask import Flask, jsonify, request

app = Flask(__name__)

students = [
    {'id': 1, 'name': 'Петров Пётр', 'group': '22-ПО-1'},
    {'id': 2, 'name': 'Сидорова Анна', 'group': '22-ПО-2'},
]
next_id = 3

@app.route('/api/students', methods=['GET'])
def get_students():
    return jsonify(students), 200

@app.route('/api/students/<int:sid>', methods=['GET'])
def get_student(sid):
    s = next((s for s in students if s['id'] == sid), None)
    if s is None:
        return jsonify({'error': 'Not found'}), 404
    return jsonify(s), 200

@app.route('/api/students', methods=['POST'])
def add_student():
    global next_id
    data = request.json
    if not data or 'name' not in data:
        return jsonify({'error': 'Bad request'}), 400
    data['id'] = next_id
    next_id += 1
    students.append(data)
    return jsonify(data), 201

if __name__ == '__main__':
    app.run(debug=True, port=5000)
```

Форма представления результата: Файлы server.py и client.py; скриншоты Postman (3 запроса с ответами); вывод терминала при запуске клиента.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Лабораторное занятие №13

Построение и моделирование компьютерной сети в среде Cisco Packet Tracer / GNS3

Цель: Сформировать умения разрабатывать схему ЛВС предприятия, реализовывать её в симуляторе, настраивать адресацию, VLAN, маршрутизацию между VLAN, тестировать связность всех сегментов.

Выполнив работу, вы будете уметь:

Уд 1_ОП.07 организовывать и конфигурировать КС; Уд 2 строить и анализировать модели КС; Уо 01.06 реализовывать составленный план; Уо 02.07 использовать современное ПО.

Материальное обеспечение:

ПК; Cisco Packet Tracer 8.x; методические материалы с описанием задания.

Задание:

1. Спроектируйте и создайте в Cisco Packet Tracer топологию сети малого предприятия: 1 маршрутизатор, 2 коммутатора (ядро и доступ), 4 ПК в VLAN 10 и VLAN 20, 1 сервер в VLAN 100.
2. Настройте VLAN, access-порты для хостов и trunk-порты между устройствами.
3. Реализуйте межвлановую маршрутизацию по схеме «router-on-a-stick».
4. Проверьте связность: ping между ПК из VLAN 10 и VLAN 20, ping от ПК до сервера.
5. Выполните документирование: заполните таблицу адресации, нарисуйте логическую схему.

Порядок выполнения работы:

1. Запустите Cisco Packet Tracer. Разместите: Router 2911 (R1), Switch 3560 (SW_CORE), Switch 2960 (SW_ACCESS), PC0–PC3, Server0.
2. Соедините: R1 GE0/0 ↔ SW_CORE GE1/0/1 (Trunk); SW_CORE ↔ SW_ACCESS (Trunk); PC0,PC1 → SW_ACCESS; PC2,PC3 → SW_CORE; Server0 → SW_CORE.
3. Настройте VLAN на SW_CORE (CLI):
4. enable → configure terminal
5. vlan 10 → name DEV → exit
6. vlan 20 → name TEST → exit
7. vlan 100 → name SERVERS → exit
8. Назначьте порты SW_ACCESS (access):
9. interface FastEthernet0/1 → switchport mode access → switchport access vlan 10
10. interface FastEthernet0/2 → switchport mode access → switchport access vlan 20
11. Настройте Trunk SW_CORE → R1:
12. interface GigabitEthernet1/0/1 → switchport mode trunk
13. switchport trunk allowed vlan 10,20,100
14. Настройте подинтерфейсы R1 (router-on-a-stick):
15. interface GigabitEthernet0/0.10
16. encapsulation dot1Q 10
17. ip address 192.168.10.1 255.255.255.0
18. interface GigabitEthernet0/0.20

19. encapsulation dot1Q 20
20. ip address 192.168.20.1 255.255.255.0
21. interface GigabitEthernet0/0.100
22. encapsulation dot1Q 100
23. ip address 192.168.100.1 255.255.255.0

24. Настройте IP хостов: PC0 — 192.168.10.10/24 gw 192.168.10.1; PC2 — 192.168.20.10/24 gw 192.168.20.1; Server — 192.168.100.10/24 gw 192.168.100.1.

25. Проверьте ping с PC0 до PC2 и до Server. Зафиксируйте вывод.

26. Пример выполнения: Таблица адресации сети предприятия

Устройство	Интерфейс	IP-адрес	Маска	Шлюз
R1	GE0/0.10	192.168.10.1	255.255.255.0	—
R1	GE0/0.20	192.168.20.1	255.255.255.0	—
R1	GE0/0.100	192.168.100.1	255.255.255.0	—
PC0	Fa0	192.168.10.10	255.255.255.0	192.168.10.1
PC1	Fa0	192.168.10.11	255.255.255.0	192.168.10.1
PC2	Fa0	192.168.20.10	255.255.255.0	192.168.20.1
PC3	Fa0	192.168.20.11	255.255.255.0	192.168.20.1
Server0	Fa0	192.168.100.10	255.255.255.0	192.168.100.1

Форма представления результата: Файл .pkt с настроенной топологией; таблица адресации; скриншоты ping между VLAN; вывод show vlan brief и show ip route.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Тема 1.4 Аппаратное обеспечение компьютерных сетей

Практическое занятие №1

Анализ и выбор оборудования для проектирования локальной компьютерной сети

Цель: Сформировать умения составлять техническое задание на оборудование ЛВС, обосновывать выбор коммутаторов, маршрутизаторов и кабельной инфраструктуры по заданным требованиям, оформлять спецификацию оборудования.

Выполнив работу, вы будете уметь:

Уд 2 строить и анализировать модели КС; Уд 5 проводить сбор и анализ исходных данных по сетевой инфраструктуре; Уо 02.05 оценивать практическую значимость результатов поиска.

Материальное обеспечение:

ПК; интернет-браузер; каталоги оборудования (cisco.com, mikrotik.com, dns-shop.ru); LibreOffice Calc / MS Excel.

Задание:

1. По варианту задания (см. таблицу вариантов) изучите исходные данные предприятия (количество пользователей, отделы, расположение, требования к безопасности). Составьте техническое задание на ЛВС.

2. Подберите конкретные модели оборудования (минимум 3 позиции): коммутатор, маршрутизатор, точка доступа (если требуется). Обоснуйте выбор каждой позиции.

3. Составьте спецификацию оборудования с указанием количества и стоимости (по актуальным прайс-листам).

4. Нарисуйте упрощённую логическую схему сети (от руки или в draw.io / Cisco Packet Tracer).

Порядок выполнения работы:

1. Ознакомьтесь с вариантом задания. Запишите требования: число пользователей, число отделов, тип трафика (данные/голос/видео), требования к защите.

2. Составьте ТЗ в текстовом редакторе по структуре: Цель создания сети; Требования к пропускной способности; Требования к безопасности; Перечень сетевых сервисов; Требования к надёжности.

3. Откройте браузер. На сайте производителя (MikroTik, Cisco, TP-Link) или в интернет-магазине (DNS) подберите: управляемый коммутатор 24/48 порта Gigabit; маршрутизатор с поддержкой VLAN и VPN; беспроводную точку доступа (если есть Wi-Fi пользователи).

4. Для каждой позиции заполните таблицу: Наименование | Производитель | Модель | Ключевые характеристики | Обоснование выбора | Цена за ед. | Кол-во | Сумма.

5. Рассчитайте требуемое количество кабеля: определите расстояния от коммутаторов до рабочих мест, добавьте 10% запаса, укажите тип (Cat.5e/6).

6. Постройте логическую схему: обозначьте роутер, коммутаторы, VLAN, серверы, рабочие станции.

7. Оформите документ: ТЗ + Спецификация + Схема + Обоснование. Итоговая стоимость проекта.

8. Пример выполнения: Фрагмент спецификации оборудования

№	Наименование	Модель	Кол.	Цена	Сумма

1 | Коммутатор 24G | MikroTik CRS326-24G-2S+RM | 2 | 18000 | 36000

2 | Маршрутизатор | MikroTik hEX S (RB760iGS) | 1 | 6500 | 6500

3 | Точка доступа Wi-Fi| TP-Link EAP670 | 3 | 8000 | 24000

4 | Кабель UTP Cat.6 | Ripo UTP Cat.6, 305 м | 1 | 4500 | 4500

5 | Коннектор RJ-45 | Упаковка 100 шт. | 2 | 350 | 700

6 | Патч-панель 24 пр. | 19", 1U | 2 | 2200 | 4400

| | ИТОГО: | | | 76100

Обоснование: MikroTik CRS326 — управляемый L3-коммутатор с поддержкой VLAN 802.1Q, STP, PoE, в пределах бюджета. Гибкая настройка через RouterOS.

Форма представления результата: Документ ТЗ (1–2 страницы), спецификация оборудования (таблица), логическая схема сети, итоговая смета.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.

Тема 1.5. Безопасность компьютерных сетей

Практическое занятие №2

Разработка политики информационной безопасности компьютерной сети. Настройка VPN-туннеля

Цель: Сформировать умения составлять документ «Политика информационной безопасности сети», определять правила управления доступом, настраивать VPN-туннель с использованием OpenVPN или WireGuard для защищённого подключения удалённых пользователей.

Выполнив работу, вы будете уметь:

Уд 5 проводить сбор и анализ исходных данных по сетевой инфраструктуре; Уо 02.05 оценивать практическую значимость результатов поиска; Уо 02.06 оформлять результаты поиска.

Материальное обеспечение:

ПК с ОС Windows/Linux; ВМ Ubuntu для VPN-сервера; WireGuard или OpenVPN; текстовый редактор.

Задание:

1. Разработайте документ «Политика информационной безопасности компьютерной сети» по заданному образцу: введение, цели, область применения, управление доступом, правила для сети, ответственность. Объём — не менее 1,5 страницы.

2. Разработайте таблицу правил межсетевого экрана (ACL / Firewall Rules): укажите не менее 8 правил (разрешено/запрещено) с обоснованием.

3. Настройте VPN-туннель WireGuard: сервер на ВМ Linux, клиент на ПК Windows. Подключитесь, проверьте, что трафик идёт через VPN (curl ifconfig.me до и после подключения).

Порядок выполнения работы:

1. Откройте шаблон ПИБ (выдаётся преподавателем или скачивается с портала). Изучите структуру.

2. Заполните разделы ПИБ для учебного предприятия (вариант задания): Введение (назначение документа, область применения), Управление доступом (кто имеет доступ к каким ресурсам, роли: admin/user/guest), Правила безопасности (сложность паролей, блокировка экрана, VLAN для гостей), Сетевые правила (перечень разрешённых и запрещённых соединений), Ответственность (за нарушение политики).

3. Составьте таблицу правил МЭ:

4. № | Источник | Назначение | Протокол | Порт | Действие | Обоснование

5. Настройка WireGuard-сервера (Ubuntu):

6. sudo apt install wireguard -y

7. wg genkey | sudo tee /etc/wireguard/server_private.key | wg pubkey | sudo tee /etc/wireguard/server_public.key

8. Создайте конфиг сервера:

9. sudo nano /etc/wireguard/wg0.conf

10. Содержимое (пример в разделе 4). Запустите:

11. sudo wg-quick up wg0
12. sudo systemctl enable wg-quick@wg0

13. Настройка клиента (Windows): скачайте WireGuard для Windows с wireguard.com. Создайте конфиг клиента (пример в разделе 4). Импортируйте в приложение. Нажмите Activate.

14. Проверьте: выполните в CMD до VPN — curl ifconfig.me (покажет реальный IP). После подключения — curl ifconfig.me — должен показать IP сервера.

15. Сделайте скриншоты: статус wg0 (sudo wg show), результат curl ifconfig.me до и после VPN.

16. Пример выполнения: Конфиг WireGuard (сервер и клиент)

```
# /etc/wireguard/wg0.conf  (СЕРВЕР)
[Interface]
Address = 10.8.0.1/24
ListenPort = 51820
PrivateKey = <приватный_ключ_сервера>
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

[Peer]
PublicKey = <публичный_ключ_клиента>
AllowedIPs = 10.8.0.2/32

# ==============================
# Конфиг КЛИЕНТА (Windows)
[Interface]
Address = 10.8.0.2/24
PrivateKey = <приватный_ключ_клиента>
DNS = 8.8.8.8

[Peer]
PublicKey = <публичный_ключ_сервера>
Endpoint = <IP_сервера>:51820
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 25

# После активации всё исходящее шифруется и идёт через сервер.
```

Форма представления результата: Документ ПИБ (1,5–2 стр.); таблица правил МЭ; конфиги WireGuard (сервер и клиент); скриншоты sudo wg show и curl ifconfig.me до/после VPN.

Критерии оценки:

– «5» (отлично) — все задания выполнены в полном объёме, студент ответил на контрольные вопросы без ошибок, отчёт оформлен правильно.

– «4» (хорошо) — задания выполнены, отчёт оформлен, при ответе на контрольные вопросы допущены незначительные неточности.

– «3» (удовлетворительно) — задания выполнены с замечаниями, контрольные вопросы раскрыты частично.

– «2» (неудовлетворительно) — задания не выполнены или выполнены с грубыми ошибками, ответы на контрольные вопросы отсутствуют.