

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины
Компьютерные сети

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 26 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Дисциплина «Компьютерные сети» имеет целью формирование у студентов знаний по основным принципам проектирования локальных и глобальных сетей, администрированию сетевых служб и компонентов, и технологиям локальных и глобальных сетей.

Дисциплина посвящена технологиям коммутации и принципам работы маршрутизаторов для поддержки сетей малых и средних организаций. В ней также рассматриваются беспроводные локальные сети (WLAN) и вопросы обеспечения безопасности. В рамках второй части дисциплины, студенты научатся проводить базовую настройку средних сетей, находить и устранять неполадки, выявлять и устранять угрозы безопасности LAN, а также настраивать и защищать базовые среды WLAN.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерные сети» относится к обязательной части образовательной программы.

Дисциплина «Компьютерные сети» является предшествующей для изучения базовой дисциплины «Основы построения защищенных компьютерных сетей». Знания и практические навыки, полученные в результате освоения дисциплины «Компьютерные сети» могут непосредственно использоваться при работе по специальности.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции		
ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	И-ОПК-8.5 Способен осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам информационной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Иметь навыки: работы с научно-технической литературой по изучению перспективных систем и сетей связи с целью повышения эффективности использования защищенных телекоммуникационных систем.
ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования	И-ОПК-15.1 Знает архитектуру основных типов современных компьютерных систем; принципы построения современных операционных систем и особенности их применения; основы организации	Знать: - принципы связи и обмен данными в локальной проводной сети; - уровни доступа и распределения в сети Ethernet; - схемы IP-адресации; - базовые понятия сетевой безопасности;

	и построения компьютерных сетей; эталонную модель взаимодействия открытых систем; функции, принципы действия и алгоритмы работы сетевого оборудования.	<ul style="list-style-type: none"> - структуру и принципы обмена данными между узлами в сети Интернет; - виды, характеристики и маркировки сетевых кабелей и контактов
	И-ОПК-15.2 Умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования компьютерных сетей.	Уметь: <ul style="list-style-type: none"> - проектировать и устанавливать домашнюю сеть или сеть малого предприятия, подключать ее к сети Интернет; - выполнять настройку основных параметров маршрутизаторов и коммутаторов; - выполнять проверку и устранять неполадки сети и подключения к глобальной сети
	И-ОПК-15.3 Владеет навыками администрирования компьютерных сетей; навыками работы с сетевым оборудованием и сетевым программным обеспечением	Владеть навыками: <ul style="list-style-type: none"> - создания и настройки одноранговой сети, компьютерной сети с помощью маршрутизатора, беспроводной сети; - создания подсетей и настройки обмена данными; - установки и настройки сетевых устройств: сетевых плат, маршрутизаторов, коммутаторов и др.; - использования основных команд для проверки подключения к Интернету, отслеживания сетевых пакетов, параметров IP-адресации;
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	И-ОПК-16.1 Знает средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.	Знать: <ul style="list-style-type: none"> - принципы связи и обмен данными в локальной проводной сети; - типы сетевых атак и методы борьбы с ними; - технологии коммутации; - принципы работы маршрутизаторов для поддержки сетей малых и средних организаций; - принципы поддержки доступных и надежных сетей с помощью динамической адресации и протоколов резервирования первого перехода
	И-ОПК-16.2 Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства	Уметь: <ul style="list-style-type: none"> - выявлять и устранять угрозы безопасности локальной компьютерной сети; - проводить базовую настройку сетей; - находить и устранять неполадки, выявлять и устранять угрозы безопасности LAN; - настраивать и защищать базовые

	обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	среды WLAN
	И-ОПК-16.3 Владеет навыками настройки межсетевых экранов; владеет методиками анализа сетевого трафика.	Владеть навыками: - работы с маршрутизаторами, коммутаторами и беспроводными устройствами в рамках настройки и устранения неполадок VLAN, беспроводных локальных сетей и маршрутизации между сетями VLAN; - настройки и устранения неполадок резервирования в коммутируемой сети с помощью STP и EtherChannel; - анализа сетевого трафика и навыками решения проблем при использовании физического оборудования и Cisco Packet Tracer;

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **7** зачетных единиц, **252** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Основы сетевого подключения и связи	7	4	2				6	Задания для самостоятельной и совместной практической работы
2	Основы Ethernet	7	6	2		1		8	Задания для самостоятельной и совместной практической работы
3	Обмен данными между сетями	7	6	2		1		8	Задания для самостоятельной и совместной практической работы

4	IP-адресация	7	8	4		1		12	Задания для самостоятельной и совместной практической работы
5	Связь с сетевыми приложениями	7	4	1		1		6	Задания для самостоятельной и совместной практической работы
6	Построение и обеспечение безопасности небольшой сети	7	4	5		1		10	Задания для самостоятельной и совместной практической работы
							0,3	4,7	зачет
	Всего за 7 семестр 108 акад. часов		32	16		5	0,3	54,7	
7	Принципы коммутации, VLAN и маршрутизация между VLAN	8	8	2		1		13	Задания для самостоятельной и совместной практической работы
8	Избыточность сетей	8	4	4		1		8	Задания для самостоятельной и совместной практической работы
9	Доступные и надежные сети	8	6	4		1		10	Задания для самостоятельной и совместной практической работы
10	Безопасность на уровне 2 и безопасность WLAN	8	8	2		1		10	Задания для самостоятельной и совместной практической работы
11	Концепция маршрутизации и конфигурация	8	6	4		1		14	Задания для самостоятельной и совместной практической работы
						2	0,5	33,5	экзамен
	Всего за 8 семестр 144 акад, часа		32	16		7	0,5	88,5	
	ИТОГО		64	32		12	0,8	143,2	

Содержание разделов дисциплины:

Тема 1. Основы сетевого подключения и связи.

1.1. Современные сетевые технологии.

1.1.1. Введение. Влияние сетей на жизнь людей. Сети без границ.

1.1.2. Компоненты сети. Одноранговые сети. Оконечные устройства. Промежуточные устройства. Средства сетевого подключения

1.1.3. Представления и топологии сетей. Топологические схемы.

1.1.4. Основные типы сетей. Сети различного размера. Сети LAN и WAN. Интернет. Внутренние сети и внешние сети.

1.1.5. Подключение к Интернету. Технологии доступа в Интернет. Интернет-подключение для дома и небольшого офиса. Интернет-подключение для предприятий. Конвергентная сеть.

1.1.6. Надежные сети. Сетевая архитектура. Отказоустойчивость. Масштабируемость. Качество обслуживания. Безопасность сети.

1.1.7. Тенденции развития сетей. Последние тенденции. Концепция BYOD. Совместная работа через Интернет. Видеосвязь. Облачные вычисления. Технологические тенденции в домашних сетях. Сети по линиям электропитания. Беспроводная широкополосная сеть.

1.1.8. Обеспечение сетевой безопасности. Угрозы безопасности. Решения обеспечения безопасности.

1.2. Базовая конфигурация коммутатора и оконечного устройства.

1.2.1. Доступ к Cisco IOS. Операционные системы. Графический интерфейс пользователя. Назначение ОС. Способы доступа. Программы эмуляции терминала.

1.2.2. Навигация по IOS. Основные командные режимы. Режим конфигурации и вложенные режимы конфигурации. Переключение между режимами IOS. Компоненты справки IOS.

1.2.3. Структура команд. Базовая структура команд IOS. Проверка синтаксиса команд IOS. Горячие клавиши и клавиши быстрого вызова.

1.2.4. Базовая настройка устройств. Имена устройств. Правила выбора паролей. Настройка паролей. Шифрование паролей. Баннерные сообщения.

1.2.5. Сохранение конфигураций. Файлы конфигурации. Изменение текущей конфигурации. Запись конфигурации в текстовый файл.

1.2.6. Порты и адреса. IP-адреса. Интерфейсы и порты.

1.2.7. Настройка IP-адресации. Настройка IP-адресов оконечных устройств вручную. Автоматическая настройка IP-адресов оконечных устройств. Настройка виртуального интерфейса коммутатора (SVI).

1.2.8. Проверка подключения. Проверка назначения интерфейса. Проверка сквозного подключения.

1.3. Протоколы и модели.

1.3.1. Правила. Основы коммуникаций. Протоколы связи. Установление правил. Требования к сетевому протоколу. Кодирование сообщения. Форматирование и инкапсуляция сообщений. Размер сообщений. Синхронизация сообщений. Варианты доставки сообщений.

1.3.2. Протоколы. Обзор сетевых протоколов. Функции сетевого протокола. Взаимодействие протоколов.

1.3.3. Наборы протоколов. Стеки сетевых протоколов. Эволюция протоколов. Пример протокола TCP/IP. Набор протоколов TCP/IP. Обмен данными TCP/IP.

1.3.4. Организации по стандартизации. Открытые стандарты. Стандарты интернета. Организации по стандартизации электроники и коммуникаций.

1.3.5. Эталонные модели. Преимущества использования многоуровневой модели. Эталонная модель OSI. Модель протоколов TCP/IP. Сравнение моделей OSI и TCP/IP.

1.3.6. Инкапсуляция данных. Сегментация сообщений. Последовательность. Единица данных протокола (PDU). Примеры инкапсуляции и деинкапсуляции.

1.3.7. Доступ к данным. Адреса. IP-адрес (логический адрес 3-го уровня). Устройства в одной сети. Роль адресов канального уровня: Одна IP-сеть. Роль адресов сетевого уровня. Роль адресов канального уровня: Разные IP-сети. Адреса канального уровня.

Тема 2. Основы Ethernet.

2.1. Физический уровень.

2.1.1. Назначение физического уровня. Физическое подключение. Физический уровень.

2.1.2. Характеристики физического уровня. Стандарты физического уровня. Физические компоненты. Кодирование. Способы передачи сигналов. Пропускная способность. Терминология пропускной способности.

2.1.3. Медный кабель. Характеристики медных кабелей. Типы медных кабелей. Неэкранированная витая пара (UTP). Экранированная витая пара (STP). Коаксиальный кабель.

2.1.4. Кабели типа UTP. Свойства кабелей UTP. Стандарты прокладки кабелей UTP. Прямые и перекрестные кабели UTP.

2.1.5. Прокладка оптоволоконных кабелей. Свойства оптоволоконных кабелей. Типы оптоволоконных кабелей. Оптоволоконные разъемы. Соединительные оптоволоконные кабели. Оптоволоконные кабели и медные кабели: сравнение.

2.1.6. Средства беспроводного подключения. Свойства средств беспроводного подключения. Типы средств беспроводного подключения. Беспроводная локальная сеть.

2.2. Системы счисления.

2.2.1. Двоичные адреса и адреса IPv4. Двоичная позиционная система счисления. Адреса IPv4.

2.2.2. Шестнадцатеричная система счисления. Шестнадцатеричные адреса и адреса IPv6. Преобразование десятичных чисел в шестнадцатеричные. Преобразование шестнадцатеричного числа в десятичное.

2.3. Канальный уровень.

2.3.1. Назначение канального уровня. Канальный уровень. Подуровни канала передачи данных IEEE 802 LAN/MAN. Предоставление доступа к среде передачи данных. Стандарты канального уровня.

2.3.2. Топологии. Физическая и логическая топология. Топологии глобальных сетей (WAN). Топология «точка-точка» (point-to-point) сети WAN. Топологии локальных сетей (LAN). Полудуплексная и полнодуплексная связь. Управление доступом к среде передачи данных. Конкурентный доступ — CSMA/CD. Конкурентный доступ — CSMA/CA.

2.3.3. Кадр канала передачи данных. Кадр. Поля кадра. Адрес уровня 2. Кадры LAN и WAN.

2.4. Коммутация в сетях Ethernet.

2.4.1. Кадры Ethernet. Инкапсуляция Ethernet. Подуровни канального уровня. Подуровень MAC. Поля кадра Ethernet.

2.4.2. MAC-адрес Ethernet. MAC-адрес и шестнадцатеричная система счисления. MAC-адрес Ethernet. Обработка кадров. Индивидуальный (одноадресный) MAC-адрес. MAC-адрес широковещательной рассылки. MAC-адрес многоадресной рассылки.

2.4.3. Таблица MAC-адресов. Основная информация о коммутаторах. Коммутатор в режиме обучения. Фильтрация кадров. Таблицы MAC-адресов на подключенных друг к другу коммутаторах. Отправка кадра на шлюз по умолчанию.

2.4.4. Скорость и способы пересылки на коммутаторах. Способы переадресации кадра на коммутаторах Cisco. Сквозная коммутация (Cut-Through). Буферизация памяти на коммутаторах. Настройка дуплексного режима и скорости. Функция Auto-MDIX.

Тема 3. Обмен данными между сетями

3.1. Сетевой уровень.

3.1.1. Характеристики сетевого уровня. Протоколы сетевого уровня. Инкапсуляция IP. Характеристики протокола IP. Без установления соединения. Негарантированная доставка. Независимость от среды.

3.1.2. Пакет IPv4. Поля заголовка пакета IPv4.

3.1.3. Пакет IPv6. Ограничения IPv4. Обзор IPv6. Поля заголовка пакета IPv4 в заголовке пакета IPv6. Заголовок пакета IPv6.

3.1.4. Методы маршрутизации узлов. Решение о перенаправлении узла. Шлюз по умолчанию. Хост-маршруты к шлюзу по умолчанию. Таблицы маршрутизации узла.

3.1.5. Введение в маршрутизацию. Решение о пересылке пакетов маршрутизатора. Таблица маршрутизации IP-маршрутизатора. Статическая маршрутизация. Динамическая маршрутизация.

3.2. Разрешение адресов.

3.2.1. MAC и IP. Устройство назначения в той же сети. Устройство назначения в удаленной сети.

3.2.2. Протокол ARP. Обзор ARP. Функции ARP. Принцип работы протокола ARP — ARP-запрос и ARP-ответ. Роль ARP в обмене данными с удаленными сетями. Удаление

записей из таблицы ARP. Таблицы ARP на сетевых устройствах. Проблемы ARP широковещательная рассылка ARP и ARP-спуфинг.

3.2.3. Обнаружение соседних IPv6 устройств. Сообщения об обнаружении соседей IPv6. Обнаружение соседей IPv6 - разрешение адресов.

3.3. Базовая конфигурация маршрутизатора.

3.3.1. Первоначальная настройка маршрутизатора. Шаги базовой конфигурации маршрутизатора. Базовая конфигурация.

3.3.2. Настройка интерфейсов маршрутизатора. Пример настройки интерфейсов маршрутизатора. Проверка конфигурации интерфейса. Команды проверки конфигурации.

3.3.3. Настройка шлюза по умолчанию. Шлюз по умолчанию для хоста. Шлюз по умолчанию для коммутатора.

Тема 4. IP-адресация

4.1. IPv4-адресация.

4.1.1. Структура IPv4-адреса. Сетевая и узловая части адреса. Маска подсети. Длина префикса. Определение сети: логическое И. Сетевой адрес, адрес хоста и широковещательный адрес.

4.1.2. Одноадресная, широковещательная и многоадресная рассылка IPv4. Одноадресная рассылка. Широковещательная рассылка. Многоадресная рассылка.

4.1.3. Типы адресов IPv4. Общедоступные и частные адреса IPv4. Маршрутизация в Интернет. IPv4-адреса специального назначения. Устаревшая классовая адресация. Назначение IP-адресов.

4.1.4. Сегментация сети. Широковещательный домен и сегментация. Проблемы с крупными широковещательными доменами. Причины сегментации сетей.

4.1.5. Разделение сети IPv4 на подсети. Разделение на подсети на границе октетов. Подсеть в пределах октета.

4.1.6. Подсеть: /16 и /8. Создание подсетей с префиксом /16. Создание 100 подсетей с помощью префикса /16. Создание 1000 подсетей с помощью префикса /8. Организация подсетей по нескольким октетам. Расчет маски подсети.

4.1.7. Разделение на подсети для соответствия требованиям. Частная подсеть и общедоступное адресное пространство IPv4. Минимизация неиспользуемых адресов IPv4 узлов и максимизация подсетей. Эффективное разделение на подсети IPv4.

4.1.8. VLSM (Маска подсети переменной длины). Основы VLSM. Сохранение адресов IPv4. VLSM. Назначение адреса топологии VLSM.

4.1.9. Структурированное проектирование. Планирование адресации сети. Назначение адресов устройствам.

4.2. IPv6-адресация.

4.2.1. Проблемы с протоколом IPv4. Потребность в IPv6. Совместное использование протоколов IPv4 и IPv6.

4.2.2. Представление IPv6-адресов. Форматы адресов IPv6. Пропуск начальных нулевых разрядов. Двойной двоеточие.

4.2.3. IPv6-адреса: типы. Одноадресный, многоадресный, произвольный. Длина префикса IPv6-адреса. Другие типы IPv6-адресов одноадресной рассылки. Уникальный локальный адрес. Глобальные индивидуальные IPv6-адреса (GUA). Структура GUA IPv6. Локальный IPv6-адрес канала.

4.2.4. Статическая настройка глобальных динамических адресов для одноадресной рассылки и динамически настраиваемые локальные адреса канала. Статическая конфигурация GUA на маршрутизаторе. Статическая конфигурация глобального уникального IPv6-адреса на узле Windows. Статическая конфигурация локального адреса одноадресной рассылки.

4.2.5. Динамическая адресация для глобальных динамических адресов для одноадресной рассылки IPv6. Сообщения RS и RA ICMPv6. SLAAC. SLAAC и DHCPv6-сервер без

сохранения состояния адресов. DHCPv6 с поддержкой состояния. Процесс EUI-64. Случайно сгенерированные идентификаторы интерфейса.

4.2.6. Динамическая адресация локальных адресов канала IPv6. Динамические LLA. Динамические LLA в Windows. Динамические LLA на маршрутизаторах Cisco. Проверка конфигурации IPv6-адреса.

4.2.7. Групповые IPv6-адреса. Присвоенные групповые IPv6-адреса. Известные адреса многоадресной рассылки IPv6. Групповые IPv6-адреса запрашиваемых узлов.

4.2.8. Разделение сети IPv6 на подсети с использованием идентификатора подсети. Пример создания подсетей IPv6. Распределение IPv6-адресов подсети. Маршрутизатор, сконфигурированный с подсетями IPv6.

4.3. ICMP.

4.3.1. Сообщения ICMPv4 и ICMPv6. Достижимость узла. Узел назначения или сервис недоступен. Превышен интервал ожидания. Сообщения ICMPv6.

4.3.2. Тестирование при помощи ping и traceroute. Ping - Тест связанности. ping до интерфейса loopback. Проверка связи со шлюзом по умолчанию. Установка связи с удаленным узлом с помощью команды ping. Traceroute — тестирование пути. Проверка адресации IPv4 и IPv6.

Тема 5. Связь с сетевыми приложениями

5.1. Транспортный уровень.

5.1.1. Передача данных. Роль транспортного уровня. Функции транспортного уровня. Протоколы транспортного уровня. Протокол управления передачей (TCP). Протокол пользовательских дейтаграмм (UDP). Соответствующий протокол транспортного уровня для соответствующего приложения.

5.1.2. Обзор протокола TCP. Функции протокола TCP. Заголовок и поля заголовка TCP. Приложения, использующие протокол TCP.

5.1.3. Обзор протокола UDP. Функции протокола UDP. Заголовок и поля заголовка UDP. Приложения, использующие протокол UDP.

5.1.4. Номера портов. Несколько отдельных сеансов передачи данных. Пары сокетов. Группы номеров портов. Команда netstat.

5.1.5. Обмен данными по протоколу TCP. Процессы TCP-сервера. Установление и прекращение TCP-соединения. Анализ трехстороннего квитирования TCP.

5.1.6. Надежность и управление потоком передачи данных. Надежность TCP - гарантированная и упорядоченная доставка. Потеря данных и повторная передача. Управление потоком TCP. Размер окна и подтверждения. Максимальный размер сегмента (MSS). Предотвращение перегрузок.

5.1.7. Обмен данными по протоколу UDP. Низкие накладные расходы или надежность. Сборка дейтаграмм UDP. Процессы и запросы UDP-сервера. Процессы и запросы UDP-сервера.

5.2. Уровень приложений.

5.2.1. Уровень приложений, уровень представления, сеансовый уровень. Протоколы уровня приложений TCP/IP.

5.2.2. Модель «клиент-сервер». Одноранговые сети. Одноранговые приложения. Наиболее распространенные одноранговые приложения.

5.2.3. Протоколы веб-трафика и электронной почты. Протокол передачи гипертекста (HTTP) и язык гипертекстовой разметки (HTML). Протоколы HTTP и HTTPS. Протоколы электронной почты (SMTP, POP, и IMAP).

5.2.4. Сервисы IP-адресации. Служба доменных имен (DNS). Формат сообщений DNS. Иерархия DNS. Команда nslookup. Протокол динамической настройки сетевого узла (Dynamic Host Configuration Protocol, DHCP). Принцип работы DHCP.

5.2.5. Сервисы совместного доступа к файлам. Протокол передачи файлов (FTP). Протокол SMB.

Тема 6. Построение и обеспечение безопасности небольшой сети

6.1. Основы сетевой безопасности.

6.1.1. Типы угроз. Типы уязвимостей. Физическая защита.

6.1.2. Сетевые атаки. Типы вредоносного ПО. Разведывательные атаки. Атаки доступа. Атаки типа «отказ в обслуживании» (DoS-атаки).

6.1.3. Углубленный подход к защите. Сохранение резервных копий. Резервное копирование, обновление и установка исправлений. Аутентификация, авторизация и учет (AAA). Межсетевые экраны. Типы брандмауэров. Безопасность оконечных устройств.

6.1.4. Обеспечение безопасности устройств. Cisco AutoSecure. Пароли. Расширенная защита пароля. Активация подключения по SSH. Отключение неиспользуемых служб.

6.2. Организация небольшой сети.

6.2.1. Устройства в рамках небольшой сети. Топологии небольших сетей. Выбор устройств для сети небольшого размера. IP-адресация в рамках небольшой сети. Резервирование в небольшой сети. Управление трафиком.

6.2.2. Распространенные приложения в небольшой сети. Распространенные протоколы. Приложения для передачи голоса и видео.

6.2.3. Расширение небольшой сети. Анализ протоколов. Использование сети сотрудниками.

6.2.4. Проверка подключения с помощью Ping. Расширенная команда ping. Проверка подключения с помощью команды Traceroute. Расширенная команда traceroute. Базовый уровень сети.

6.2.5. Команды хоста и IOS. Настройка IP-конфигурации хоста под управлением Windows. Настройка IP-конфигурации хоста под управлением Linux. Настройка IP-конфигурации хоста под управлением macOS. Команда arp. Повторное рассмотрение наиболее распространенных команд show. Команда show cdp neighbors. Команда show ip interface brief. Команда show version.

6.2.6. Основные подходы к поиску и устранению неполадок. Что следует сделать с проблемой. Команда debug. Команда terminal monitor.

6.2.7. Вопросы работы и несоответствия настроек дуплекса на интерфейсе. Проблемы с IP-адресами на устройствах IOS. Проблемы с IP-адресами на оконечных устройствах. Неполадки, связанные со шлюзом по умолчанию. Поиск и устранение неполадок, связанных с DNS.

Тема 7. Принципы коммутации, VLAN и маршрутизация между VLAN.

7.1. Базовая настройка устройств

7.1.1. Введение. Первоначальная настройка коммутатора. Последовательность загрузки коммутатора. Команда "boot system". Светодиодные индикаторы коммутатора. Восстановление после системного сбоя. Доступ к управлению коммутатором. Пример конфигурации коммутатора SVI.

7.1.2. Настройка портов коммутатора. Дуплексная связь. Настройка портов коммутатора на физическом уровне. Функция Auto-MDIX. Команды проверки коммутатора. Проверка конфигурации порта коммутатора. Неполадки на уровне сетевого доступа. Ошибки ввода и вывода интерфейса. Поиск и устранение неполадок на уровне сетевого доступа.

7.1.3. Удаленный защищенный доступ. Принцип работы Telnet. Принцип работы SSH. Конфигурация SSH. Проверка работы SSH.

7.1.4. Базовая конфигурация маршрутизатора. Настройка основных параметров маршрутизатора. Топология с использованием двойного стека. Настройка интерфейсов маршрутизатора. Интерфейсы обратной петли IPv4.

7.1.5. Проверка связи между подключенными напрямую сетями. Команды проверки интерфейса. Проверка состояния интерфейса. Проверка локальных адресов канала и многоадресных адресов IPv6. Проверка конфигурации интерфейса. Проверка маршрутов маршрутизатора. Фильтрация выходных данных команды show. Функция истории команд.

7.2. Принципы коммутации.

7.2.1. Пересылка кадров. Коммутация в сети. Таблица MAC-адресов коммутатора. Получение информации и пересылка коммутатором. Способы пересылки на коммутаторе. Коммутация с промежуточным хранением (store-and-forward). Сквозная коммутация (Cut-Through).

7.2.2. Коммутационные домены. Домены коллизий. Домены широковещательной рассылки. Снижение перегрузок сети.

7.3. Сети VLAN.

7.3.1. Обзор виртуальных локальных сетей. Определения виртуальной локальной сети. Преимущества виртуальных локальных сетей (VLAN). Типы виртуальных локальных сетей.

7.3.2. Виртуальные локальные сети в среде с несколькими коммутаторами. Определение магистральных каналов VLAN. Сеть без VLAN. Сеть с VLAN. Идентификация сети VLAN с помощью меток. VLAN с нетегированным трафиком и тегирование по протоколу 802.1Q. Тегирование голосовой VLAN. Исследование методов реализации сети VLAN.

7.3.3. Настройка VLAN. Диапазоны VLAN на коммутаторах Catalyst. Команды создания VLAN. Команды назначения портов VLAN. VLAN для передачи данных и голоса. Проверка информации о сетях VLAN. Изменение принадлежности порта сети VLAN. Удаление VLAN.

7.3.4. Транки виртуальных сетей. Команды конфигурации магистрального канала (транка). Пример конфигурации магистрального канала. Проверка конфигурации транкового канала. Сброс транка в состояние по умолчанию.

7.3.5. Динамический протокол транкинга (DTP). Знакомство с DTP. Согласованные режимы интерфейса. Результаты настройки DTP. Проверка режима протокола DTP.

Тема 8. Избыточность сетей.

8.1. Маршрутизация между сетями VLAN

8.1.1. Принципы маршрутизации между виртуальными локальными сетями. Что такое маршрутизация между VLAN? Устаревшие методы маршрутизации между сетями VLAN. Маршрутизация между сетями VLAN с использованием метода Router-on-a-Stick. Маршрутизация между VLAN на коммутаторе уровня 3.

8.1.2. Маршрутизация между сетями VLAN с использованием метода Router-on-a-Stick. Конфигурация ROS (Router-on-a-stick). Сети VLAN и конфигурации магистральных каналов. Конфигурация подинтерфейса. Проверка маршрутизации между сетями VLAN с использованием метода Router-on-a-Stick.

8.1.3. Маршрутизация между виртуальными локальными сетями с помощью устройств коммутации уровня 3. Маршрутизация между сетями VLAN 3-го уровня. Сценарий переключения уровня 3. Настройка коммутатора уровня 3. Проверка маршрутизации между VLAN коммутатором уровня 3. Маршрутизация на коммутаторе уровня 3. Сценарий маршрутизации на коммутаторе уровня 3. Конфигурация маршрутизации на коммутаторе уровня 3.

8.1.4. Поиск и устранение неполадок маршрутизации между VLAN. Общие проблемы с маршрутизацией между VLAN. Отсутствующие сети VLAN. Проблемы магистрального порта коммутатора. Неполадки в работе порта коммутатора. Неполадки в настройках маршрутизатора.

8.2. Принципы STP

8.2.1. Назначение протокола STP. Резервирование в коммутируемых сетях уровня 2. Протокол STP. Перестройка STP. Проблемы с избыточными каналами коммутатора. Петли 2-го уровня. Широковещательный шторм. Алгоритм связующего дерева.

8.2.2. Принципы работы STP. Шаги к без петельной топологии. Выбор корневого моста. Влияние BID по умолчанию. Определение стоимости корневого пути. Выбор корневых портов. Выбор назначенных портов. Выбор альтернативных (заблокированных) портов. Выбор корневого порта из нескольких путей равной стоимости. Таймеры STP и состояния

портов. Эксплуатационные данные каждого состояния порта. Протокол PerVLAN Spanning Tree Protocol.

8.2.3. Эволюция STP. Различные версии STP. Принципы STP. RSTP состояния и роли портов. PortFast и BPDU Guard. Альтернативы STP.

8.3. EtherChannel

8.3.1. Принципы работы EtherChannel. Агрегирование каналов. EtherChannel. Преимущества EtherChannel. Ограничения использования. Протоколы автосогласования. Функции PAgP. Пример настроек режима PAgP. Функции LACP. Пример настроек режима LACP.

8.3.2. Настройка EtherChannel. Инструкции по настройке. Пример конфигурации LACP.

8.3.3. Поиск и устранение проблем в работе EtherChannel. Проверка EtherChannel. Общие проблемы с конфигурациями EtherChannel. Пример поиска и устранения неисправностей в работе EtherChannel.

Тема 9. Доступные и надежные сети

9.1. DHCPv4.

9.1.1. Серверы и клиенты DHCPv4. Принципы работы DHCPv4. Шаги для получения аренды. Шаги, чтобы возобновить аренду.

9.1.2. Настройка сервера DHCPv4 в Cisco IOS. Действия по настройке сервера DHCPv4 Cisco IOS. Пример конфигурации. Команды проверки DHCPv4 сервера. Как проверить, что DHCPv4 работает? Отключение сервера DHCPv4 Cisco IOS. DHCPv4-ретрансляция. Ретрансляция других сервисов.

9.1.3. Маршрутизатор Cisco как клиент DHCPv4. Пример конфигурации. Домашний маршрутизатор как клиент DHCPv4.

9.2. SLAAC и DHCPv6.

9.2.1. Конфигурация узла IPv6. IPv6 Локальный адрес канала хоста. Назначение GUA IPv6. Три флага сообщений RA.

9.2.2. Обзор SLAAC. Включение SLAAC. Только метод SLAAC. Сообщения RS ICMPv6. Хост процесс для создания идентификатора интерфейса. Обнаружение дублирующихся адресов (DAD).

9.2.3. Шаги работы DHCPv6. DHCPv6 без сохранения состояния. Включение протокола DHCPv6 без сохранения состояния на интерфейсе. Работа DHCPv6 с отслеживанием состояния. Включение DHCPv6 с поддержкой состояния на интерфейсе.

9.2.4. Роли маршрутизатора DHCPv6. Настройка маршрутизатора в качестве DHCPv6-сервера без отслеживания состояния. Настройка маршрутизатора в качестве DHCPv6-клиента без отслеживания состояния. Настройка маршрутизатора в качестве сервера DHCPv6 с отслеживанием состояния. Конфигурация клиента DHCPv6 с сохранением состояния. Команды проверки DHCPv6 сервера. Настройка маршрутизатора в качестве агента ретрансляции DHCPv6. Проверка агента ретрансляции DHCPv6.

9.3. Принципы работы FHRP.

9.3.1. Протокол резервирования первого перехода (FHRP). Ограничения шлюза по умолчанию. Резервирование маршрутизаторов. Действия при переключении в случае отказа маршрутизатора. Варианты FHRP.

9.3.2. Общие сведения о протоколе HSRP. Приоритет и приоритетное вытеснение HSRP. Состояния и таймеры HSRP.

Тема 10. Безопасность на уровне 2 и безопасность WLAN

10.1. Принципы обеспечения безопасности сети.

10.1.1. Безопасность оконечных устройств. Сетевые атаки сегодня. Устройства сетевой безопасности. Защита оконечных устройств. Устройство Cisco для защиты электронной почты. Устройство для защиты веб-трафика Cisco Web Security Appliance.

10.1.2. Контроль доступа. Аутентификация с локальным паролем. Компоненты AAA. Аутентификация. Авторизация. Учет. 802.1X.

10.1.3. Угрозы безопасности на уровне 2. Уязвимости на уровне 2. Категории атак на коммутаторы. Технологии нейтрализации атак на коммутацию.

10.1.4. Атака на таблицу MAC-адресов. Обзор работы коммутатора. Атака переполнением на таблицу MAC-адресов. Противодействие атакам на таблицы CAM.

10.1.5. Атаки на локальную сеть. VLAN и DHCP-атаки. Атака VLAN Hopping. Атака с двойным тегированием (Double-Tagging) VLAN. Сообщения DHCP. Атаки, связанные с DHCP. ARP-атаки, STP-атаки и CDP-зондирование. ARP атаки. Атака с подменой адреса. Атака STP. Разведывательная атака CDP.

10.2. Настройка параметров безопасности коммутатора.

10.2.1. Обеспечение безопасности портов. Защита неиспользуемых портов. Нейтрализация атак таблицы MAC-адресов. Включение защиты портов. Ограничение и изучение MAC-адресов. Устаревание безопасности порта. Режимы нарушения безопасности порта. Порт в состоянии error-disabled. Проверка функции безопасности портов. Реализация безопасности порта.

10.2.2. Отражение атак на виртуальные локальные сети. Обзор атак VLAN. Шаги, чтобы нейтрализовать атаки VLAN Hopping.

10.2.3. Отражение атак через DHCP. Обзор атак DHCP. Отслеживание DHCP-сообщений. Шаги по реализации DHCP Snooping. Пример настройки DHCP Snooping.

10.2.4. Отражение атак через ARP. Динамический анализ ARP. Руководство по внедрению DAI. Пример конфигурации DAI.

10.2.5. Отражение атак через STP. PortFast и BPDU Guard. Настройка PortFast. Настройка BPDU Guard.

10.3. Основные понятия WLAN.

10.3.1. Введение в технологии беспроводной связи. Преимущества беспроводной связи. Типы беспроводных сетей. Беспроводные технологии. Стандарты 802.11. Радиочастоты. Организации по стандартизации беспроводных сетей.

10.3.2. Составляющие WLAN. Беспроводные сетевые адаптеры. Домашний беспроводной маршрутизатор. Беспроводные точки доступа. Категории AP. Антенны для беспроводных устройств.

10.3.3. Принципы работы беспроводной локальной сети. Режимы топологии беспроводной сети 802.11. BSS и ESS. Структура кадра 802.11. CSMA/CA. Ассоциация беспроводных клиентов и точек доступа. Пассивный и активный режим обнаружения.

10.3.4. Введение в CAPWAP. Разделенная MAC-архитектура. Шифрование DTLS. FlexConnect AP.

10.3.5. Управление каналами. Насыщение частотного канала. Выбор канала. Планирование развертывания беспроводной сети.

10.3.6. Угрозы для беспроводных локальных сетей. Обзор безопасности беспроводной сети. Атаки типа «отказ в обслуживании» (DoS-атаки). Вредоносные точки доступа. Атака с перехватом.

10.3.7. Безопасность беспроводных локальных сетей. Соккрытие SSID и фильтрация MAC-адресов. 802.11 Оригинальные методы аутентификации. Методы аутентификации согласованного ключа. Аутентификация домашнего пользователя. Методы шифрования. Аутентификация на корпоративном уровне. WPA3.

10.4. Настройка беспроводных сетей.

10.4.1. Беспроводной маршрутизатор. Вход на беспроводной маршрутизатор. Базовая настройка сети. Базовая настройка беспроводной сети. Настройка беспроводной ячеистой сети. NAT для IPv4. Гарантированное качество обслуживания. Перенаправление портов.

10.4.2. Конфигурация Базового WLAN с контроллером беспроводной сети. Топология WLC. Просмотр всей информации о точках доступа. Расширенные настройки. Настройка WLAN.

10.4.3. Конфигурация WPA2 Enterprise WLAN с контроллером беспроводной сети. SNMP и RADIUS. Настройка информации о сервере SNMP. Настройка информации о сервере

RADIUS. Настройка VLAN для новой WLAN. Топология с адресацией VLAN. Настройка нового интерфейса. Настройка области DHCP. Конфигурация WPA2 Enterprise WLAN.

10.4.4. Способы поиска и устранения неполадок с беспроводными сетями. Невозможно подключить беспроводной клиент. Поиск и устранение неполадок в случае медленной работы сети. Обновление микропрограммного обеспечения.

Тема 11. Концепция маршрутизации и конфигурация

11.1. Принципы маршрутизации.

11.1.1. Определение пути. Две функции маршрутизатора. Пример функций маршрутизатора. Лучший путь - дающий самое длинное совпадение. Пример наиболее длинного соответствия адреса IPv4. Пример наиболее длинного соответствия адреса IPv6. Построение таблицы маршрутизации.

11.1.2. Процесс принятия решения о переадресации пакетов. Сквозная пересылка пакетов. Механизмы пересылки пакетов.

11.1.3. Таблица IP-маршрутизации. Источник маршрута. Принципы таблицы маршрутизации. Записи таблицы маршрутизации. Напрямую подключённые сети. Статические маршруты. Статические маршруты в таблице IP-маршрутизации. Динамические протоколы маршрутизации. Динамические маршруты в таблице IP-маршрутизации. Маршрут по умолчанию. Структура таблицы маршрутизации IPv4. Структура таблицы маршрутизации IPv6. Административное расстояние.

11.1.4. Статическая и динамическая маршрутизация. Эволюция протоколов динамической маршрутизации. Принципы динамических протоколов маршрутизации. Оптимальный путь. Распределение нагрузки.

11.2. Статическая IP-маршрутизация.

11.2.1. Типы статических маршрутов. Параметры следующего перехода. Команда статического маршрута IPv4. Команда статического маршрута IPv6. Топология двойного стека. IPv4 Начальные таблицы маршрутизации. IPv6 Начальные таблицы маршрутизации.

11.2.2. Статический маршрут IPv4 с использованием следующего перехода. Статический маршрут IPv6 с использованием следующего перехода. Статический маршрут IPv4 с прямым подключением. Статический маршрут IPv6 с прямым подключением. Полностью определенный IPv4 статический маршрут. Полностью определенный IPv6 статический маршрут. Проверка статического маршрута.

11.2.3. Статический маршрут по умолчанию. Настройка статического маршрута по умолчанию. Проверка статического маршрута по умолчанию.

11.2.4. Плавающие статические маршруты. Настройка плавающих статических маршрутов IPv4 и IPv6. Проверка плавающего статического маршрута.

11.2.5. Настройка статических маршрутов хостов. Автоматически устанавливаемые локальные маршруты хостов. Статический узловой маршрут. Настройка статических маршрутов хостов. Проверка статических маршрутов хостов. Настройка статического IPv6-маршрута узла с помощью локального адреса канала (LLA) следующего перехода.

11.3. Поиск и устранение неполадок, связанных со статическими маршрутами и маршрутами по умолчанию.

11.3.1. Обработка пакетов с использованием статических маршрутов.

11.3.2. Поиск и устранение проблем с конфигурацией статических маршрутов IPv4 и маршрутов IPv4 по умолчанию. Изменения в сети. Часто используемые команды для поиска и устранения неполадок. Устранение проблем соединения.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- Linux Ubuntu (GNU GPL v.3);
- OpenOffice (GNU LGPL);
- Cisco Packet Tracer 8.1.0 (доступен бесплатно для участников Программы Сетевой Академии Cisco);
- Cisco SDM (доступен бесплатно для участников Программы Сетевой Академии Cisco);
- Cisco Network Assistant (доступен бесплатно для участников Программы Сетевой Академии Cisco);
- Cisco Configuration Professional (доступен бесплатно для участников Программы Сетевой Академии Cisco);
- Google Chrome (freeware).

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
- Электронно-библиотечная система «Юрайт» <https://urait.ru>
- Электронно-библиотечная система «Консультант Студента»
<https://www.studentlibrary.ru/>
- Электронно-библиотечная система «Лань» <http://e.lanbook.com/>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Олифер В. Г. Компьютерные сети: принципы, технологии, протоколы.: учеб. пособие для вузов. / В. Г. Олифер, Н. А. Олифер; М-во образования и науки РФ - 3-е изд. - СПб.: Питер, 2009. - 957 с.
2. Учебно-методическое пособие в LMS NetAcad. Режим доступа: свободный для участников Программы Сетевой Академии Cisco (<https://www.netacad.com/>)

б) дополнительная литература

1. Олифер В. Г., Олифер Н. А. Основы сетей передачи данных. - Москва: НОУ "ИНТУИТ", 2016. https://www.studentlibrary.ru/doc/intuit_225-SCN0000/000.html
2. Проскуряков, А. В. Компьютерные сети. Основы построения компьютерных сетей и телекоммуникаций : учебное пособие / Проскуряков А. В. - Ростов н/Д : Изд-во ЮФУ, 2018. - 201 с. - ISBN 978-5-9275-2792-2. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785927527922.html>
3. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей : учебное пособие для вузов / О. М. Замятина. — Москва : Издательство Юрайт, 2023. — 167 с. — (Высшее образование). — ISBN 978-5-534-16305-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/530772>

в) ресурсы сети «Интернет»

1. <http://netacad.com>
2. <http://cisco.com>
3. <http://learningnetwork.cisco.com/>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения лабораторных работ;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- компьютерный класс, оборудованный ПЭВМ класса не ниже Intel i5-7400 , 8gb RAM, 1Tb HDD с установленным программным обеспечением: Windows 7/8/10, Linux, Packet Tracer 8.0 (и новее), Cisco SDM, Cisco Network Assistant, Cisco Configuration Professional. Из расчета одна ПЭВМ на одного человека.
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

Приложение № 1 к рабочей программе дисциплины «Компьютерные сети»

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Пример заданий для самостоятельной практической работы

(Задания размещаются в ЭУК «Компьютерные сети» в LMS Moodle и выполняются в программе эмуляции сети «Cisco Packet Tracer (доступен бесплатно для участников Программы Сетевой Академии Cisco)»)

Во время выполнения работы студент может видеть свой прогресс в процентном соотношении. Большинство работ сопровождаются методическими материалами.

Тема: Разработка и реализация схемы адресации VLSM

(проверка сформированности ОПК-15, индикатор ИД-ОПК-15.2, индикатор ИД-ОПК-15.3 в части практического применения умения проектировать и устанавливать домашнюю сеть или сеть малого предприятия, владения навыками создания подсетей и настройки обмена данными)

Цели:

- Разработка схемы IP-адресации VLSM с учетом требований.
- Настройка адресации на сетевых устройствах и узлах.
- Проверка IP-подключения.
- Поиск и устранение неполадок подключения

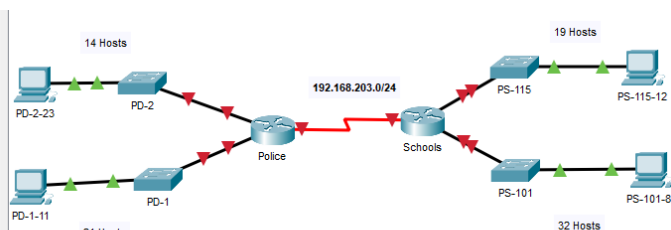
Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
	G0/0			Нет
	G0/1			Нет
	S0/0/0			Нет
	G0/0			Нет
	G0/1			Нет
	S0/0/0			Нет
	VLAN 1			
	VLAN 1			
	VLAN 1			
	VLAN 1			
	NIC			
	NIC			
	NIC			
	NIC			

Цели

В этой лаборатории вы разработаете схему адресации VLSM с учетом сетевого адреса и требований к узлу. Вы будете настраивать адресации на маршрутизаторах, коммутаторах и узлах сети.

- Разработка схемы IP-адресации VLSM с учетом требований.
- Настройка адресации на сетевых устройствах и узлах.
- Проверка IP-подключения.
- Поиск и устранение неполадок подключения



Тема: Конфигурация безопасности коммутатора (проверка сформированности ОПК-116, индикатор ИД-ОПК-16.2,

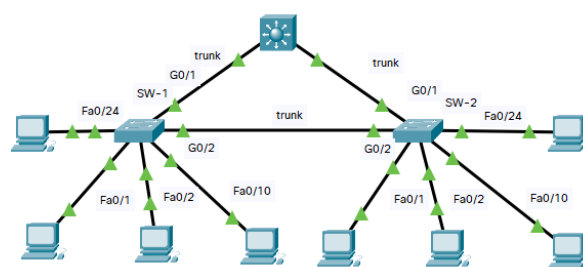
индикатор ИД-ОПК-16.3 в части практического применения выявлять и устранять угрозы безопасности локальной компьютерной сети, владения навыками в рамках настройки и устранения неполадок VLAN)

Цели:

Создать защищенное магистральное соединение
Создать Vlan'ы согласно предоставленной таблице Vlan'ов.
Настроить безопасность неиспользуемых портов коммутатора
Обеспечить безопасность портов
Включить отслеживание DHCP
Настроить Rapid PVST, PortFast и BPDU Guard.

Таблица VLAN

Коммутатор	Номер VLAN	Имя VLAN	Членство в порту	Сеть
SW-1	10	Администратор	F0/1, F0/2	192.168.10.0/24
	20	Продажи	F0/10	192.168.20.0/24
	99	Управление	F0/24	192.168.99.0/24
	100	Собственный	G0/1, G0/2	Нет
	999	BlackHole	Все неиспользуемые	Нет
SW-2	10	Администратор	F0/1, F0/22	192.168.10.0/24
	20	Продажи	F0/10	192.168.20.0/24
	99	Управление	F0/24	192.168.99.0/24
	100	Собственный	Нет	Нет
	999	BlackHole	Все неиспользуемые	None



Правила интерпретации результатов выполнения самостоятельной практической работы:

Практическая работа считается выполненной (засчитывается), если достигнуты все поставленные цели.

Пример теста для самопроверки (тест проводится в ЭУК «Компьютерные сети» в LMS NetAcad)

В тесте представлены задания на проверку знаний по теме «Базовая конфигурация коммутатора и оконечного устройства». В тесте по каждой теме в среднем 15 вопросов.
Количество попыток выполнения не ограничено.
Время на прохождение теста не ограничено.
Итоги прохождения теста не оцениваются.

Вопросы теста:

Вопрос 1. Какое утверждение верно для исполняемого файла конфигурации на устройстве Cisco IOS?

- 1) Его следует удалить с помощью команды ***erase running-config***;
- 2) Он автоматически сохраняется при перезагрузке маршрутизатора.;
- 3) Это влияет на работу устройства сразу после изменения;
- 4) Он хранится в NVRAM.

Вопрос 2. Какие два утверждения о пользовательском режиме EXEC верны? (Выберите два варианта.)

- 1) Доступ к режиму глобальной конфигурации можно получить с помощью команды ***enable***;
- 2) в этом режиме можно настраивать интерфейсы и протоколы маршрутизатора;

- 3) только некоторые аспекты конфигурации маршрутизатора доступны для просмотра в этом режиме;
- 4) доступны все команды маршрутизатора;
- 5) командная строка устройства в этом режиме заканчивается символом «>».

Вопрос 3 Какой тип доступа защищен на маршрутизаторе или коммутаторе Cisco с помощью *enable secret* команды?

- 1) Виртуальные терминалы;
- 2) Порт AUX;
- 3) Привилегированный режим EXEC;
- 4) Консольная линия.

Вопрос 4 Какой интерфейс является интерфейсом SVI по умолчанию на коммутаторе Cisco?

- 1) VLAN1;
- 2) VLAN99;
- 3) VLAN100;
- 4) VLAN999;

Вопрос 5 Каких трех правил следует придерживаться при настройке имени узла через командную строку на устройствах Cisco? (Выберите три варианта.)

- 1) имя узла должно состоять только из строчных символов;
- 2) имя узла должно завершаться специальным символом;
- 3) имя узла не должно содержать пробелов;
- 4) имя узла должно начинаться с буквы;
- 5) имя узла должно состоять меньше, чем из 64 символов.

Вопрос 6 В чем назначение оболочки операционной системы?

- 1) обеспечивает работу специализированных сервисов межсетевого экрана;
- 2) взаимодействует с аппаратными средствами устройства;
- 3) обеспечивает взаимодействие между пользователями и ядром;
- 4) обеспечивает работу сервисов защиты от вторжения.

Вопрос 7 На маршрутизаторе с рабочей операционной системой имеется файл конфигурации, сохраненный в NVRAM. В файле конфигурации есть секретный пароль привилегированного режима, но нет пароля консоли. Когда маршрутизатор загрузится, какой на нем будет режим?

- 1) режим глобальной конфигурации;
- 2) привилегированный режим EXEC;
- 3) пользовательский режим EXEC;
- 4) режим настройки.

Вопрос 8 Администратор только что изменил IP-адрес интерфейса на устройстве IOS. Что еще нужно сделать, чтобы применить эти изменения к устройству?

- 1) Скопируйте информацию в файле конфигурации запуска в рабочую конфигурацию;
- 2) Перезагрузите устройство и введите **yes** при появлении запроса на сохранение конфигурации;
- 3) Ничего не надо делать. Изменения в конфигурации на устройстве IOS вступают в силу, как только команда набрана правильно и нажата клавиша Enter;
- 4) Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Правильные ответы

Вопрос №	Вариант ответа		Вопрос №	Вариант ответа
1	3		5	3,4,5
2	3,5		6	3
3	3		7	3
4	1		8	3

Самостоятельные работы в виде тестовых заданий.

Тесты проводятся в ЭУК «Компьютерные сети» в LMS NetAcad

В каждом тесте в среднем 60 вопросов по пройденным темам (2-4).

Количество попыток выполнения - 5. Время на прохождение теста - 1,5 часа.

При завершении теста показываются ошибки (если есть) и какую тему и раздел смотреть, чтобы разобраться и исправить ошибку. Итоги прохождения теста оцениваются.

(проверка сформированности ОПК-15, индикатор ИД-ОПК-15.1 и ОПК-16, индикатор ИД-ОПК-16.1 в части знания видов, характеристик и маркировок сетевых кабелей и контактов, типов сетевых атак и методов борьбы с ними)

Примеры вопросов:

1. Во время плановой проверки техник обнаружил, что программное обеспечение, установленное на компьютере, тайно собирало данные о веб-сайтах, которые посещали пользователи компьютера. Какому типу угрозы подвергся этот компьютер?

- DoS-атака
- кража личных данных
- шпионское ПО
- атака нулевого дня

2. Какой термин относится к сети, которая обеспечивает безопасный доступ к корпоративным офисам для поставщиков, клиентов и сотрудников?

- Интернет
- интранет
- экстранет
- расширенная сеть

3. Крупная корпорация модифицировала свою сеть, чтобы пользователи могли получать доступ к сетевым ресурсам со своих личных ноутбуков и смартфонов. Какая сетевая тенденция описывает это?

- облачные вычисления
- онлайн-сотрудничество
- принеси свое устройство (BYOD)
- видеоконференции

4. Что такое интернет-провайдер?

- Это орган по стандартизации, который разрабатывает стандарты кабелей и проводки для сетей.
- Это протокол, который устанавливает, как взаимодействуют компьютеры в локальной сети.

- Это организация, которая позволяет отдельным лицам и предприятиям подключаться к Интернету.
- Это сетевое устройство, которое сочетает в себе функциональность нескольких различных сетевых устройств в одном.

5. Какие два критерия помогают выбрать сетевой носитель из различных сетевых сред? (Выберите два.)

- типы данных, которые должны быть приоритетными
- стоимость конечных устройств, используемых в сети
- расстояние, на которое выбранная среда может успешно передавать сигнал
- количество промежуточных устройств, установленных в сети
- среда, в которой будет установлен выбранный носитель

6. Сопоставьте каждую характеристику с соответствующим типом подключения к Интернету. (Не все варианты используются.)

не подходит для лесистых зон	DSL
для передачи данных использует коаксиальный кабель	
как правило, имеет низкую пропускную способность	подключение по телефонной линии
высокоскоростное соединение по телефонной линии	
обычно использует схему T1/E1 или T3/E3	спутниковая передача
	кабельное подключение

Правила выставления оценки по результатам самостоятельной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное

- задание с 1 вариантом ответа – 1 балл;
- задание с множественным выбором – 2 балла, 1 балл - если только один ответ верный, 0 баллов – если нет правильных ответов или выбрано больше вариантов, чем необходимо;
- задание с сопоставлением – 2 балла.

Полностью неправильно выполненное задание – 0 баллов.

В среднем, максимальное количество баллов по итогам самостоятельной работы – 100

Набранное количество баллов интерпретируется в процентное соотношение и оценивается. От 70-100% - работа засчитана, менее 70% – работа не засчитана (знания и умения на данном этапе освоения дисциплины не сформированы).

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

На момент проведения промежуточной аттестации должно быть выполнено и засчитано не менее 70% домашних работ.

Примерные вопросы итогового теста для получения зачёта:

1) Какой тип сервера использует такие типы записей, как A, NS, AAAA и MX, для предоставления услуг?

Сервер доменных имён
Почтовый сервер
Файловый сервер
Веб-сервер

2) Что такое проприетарные протоколы?

Протоколы, разработанные частными организациями для работы на оборудовании любого поставщика.

Протоколы, которые могут свободно использоваться любой организацией или поставщиком.

Протоколы, разработанные организациями, которые контролируют их определение и работу.

Набор протоколов, известный как стек протоколов TCP/IP.

3) Какую команду можно использовать на ПК с Windows, чтобы увидеть IP-конфигурацию этого компьютера?

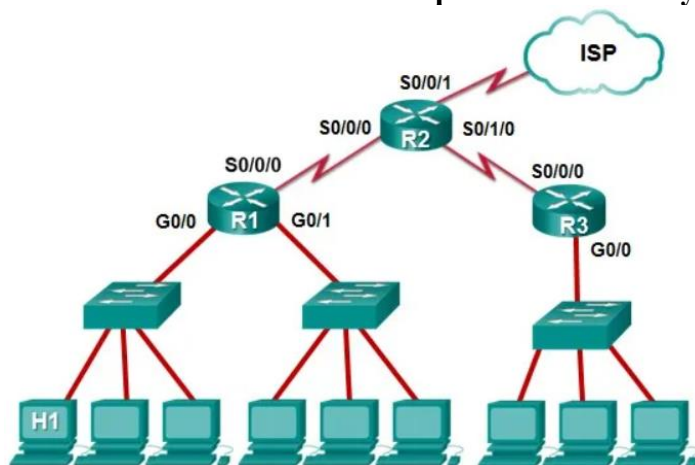
show ip interface brief

ping

show interfaces

ipconfig

4) Посмотрите на картинку. IP-адрес интерфейса какого устройства следует использовать в качестве настройки шлюза по умолчанию для хоста H1?



R1: S0/0/0

R2: S0/0/1

R1: G0/0

R2: S0/0/0

5) Сетевой администратор добавляет новую локальную сеть в филиал. Новая локальная сеть должна поддерживать 25 подключенных устройств. Какова наименьшая сетевая маска, которую сетевой администратор может использовать для новой сети?

255.255.255.128

255.255.255.192

255.255.255.224

255.255.255.240

6) Администратор пытается настроить коммутатор, но получает сообщение об ошибке, показанное на картинке. В чем проблема?

```
Switch1> config t
      ^
% Invalid input detected at '^' marker.
```

Необходимо использовать всю команду *configure terminal*.

Администратор уже находится в режиме глобальной конфигурации.

Прежде чем вводить команду, администратор должен войти в привилегированный режим EXEC.

Администратор должен подключиться через порт консоли, чтобы получить доступ к режиму глобальной конфигурации.

7) Какие два утверждения описывают, как оценивать схемы потоков трафика и типы сетевого трафика с помощью анализатора протоколов? (Выберите два.)

Выполните захват трафика в выходные дни, когда большинство сотрудников не работают.

Выполните захват трафика в часы пиковой загрузки, чтобы получить хорошее представление о различных типах трафика.

Выполните захват трафика только в тех областях сети, которые получают большую часть трафика, таких как центр обработки данных.

Выполните захват в разных сегментах сети.

Выполните захват только трафика WAN, потому что трафик в Интернете отвечает за наибольший объем трафика в сети.

8) Какой тип угрозы безопасности возникает, если надстройка для работы с электронными таблицами отключает локальный программный брандмауэр?

брутфорс

троянский конь

DoS

переполнение буфера

Зачет по итогам 7 семестра изучения дисциплины выставляется при выполнении следующих условий:

1. Должны быть сданы все домашние задания.

2. Пройден итоговый тест – с результатом не менее 70% набранных баллов от максимально возможных по тесту.

В тесте в среднем 60 вопросов по курсу (несколько вариантов финального теста).

Количество попыток выполнения - 1. Время на прохождение теста - 1,5 часа.

Оценка по результатам финального теста считается в баллах по следующему принципу: правильно выполненное

- задание с 1 вариантом ответа – 1 балл;

- задание с множественным выбором – 2 балла, 1 балл - если только один ответ верный, 0 баллов – если нет правильных ответов или выбрано больше вариантов, чем необходимо;

- задание с сопоставлением – 2 балла.

Полностью неправильно выполненное задание – 0 баллов.

В среднем, максимальное количество баллов по итогам самостоятельной работы – 100

Набранное количество баллов интерпретируется в процентное соотношение и оценивается. От 70-100% - оценка зачтено, менее 70% – оценка «неудовлетворительно» (знания и умения на данном этапе освоения дисциплины не сформированы).

3. Правила выставления оценки на экзамене.

Экзамен состоит из двух частей.

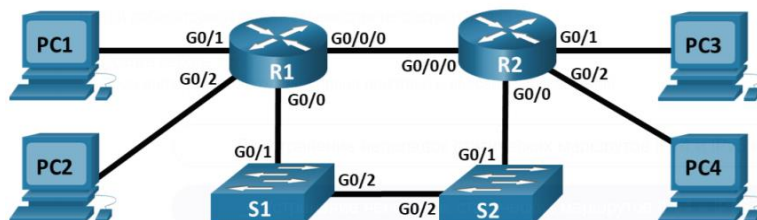
1 часть:

Выполнение практической работы на сетевом оборудовании Cisco.

Все сетевые устройства были предварительно настроены с включением преднамеренных ошибок, препятствующих маршрутизации в сети и не отвечающих требованиям безопасности. Задача студента состоит в том, чтобы оценить сеть, определить и исправить ошибки конфигурации для восстановления полной связи.

Студенту предоставляется:

1) Предварительно настроенное сетевое оборудование следующей топологии -



, где R1 и R2 – маршрутизаторы, S1 и S2 – коммутаторы.

- 2) Дополнительные сетевые кабели (UTP) и консольный кабель.
- 3) Таблица адресации.
- 4) Описание требований для оценки.

Исправить все преднамеренные ошибки и в том числе:

- а) Обеспечить доступность устройств согласно таблице адресации
- б) Настроить безопасное удаленное подключение к сетевым устройствам (к 1 коммутатору и 1 маршрутизатору на выбор студента) с использованием асимметричных ключей шифрования длиной 1024 бит. Доступ должен быть со всех ПК.
- в) Обеспечить безопасность 2-го уровня модели OSI
- г) Создать резервные маршруты для повышения надежности сети.

Работа считается выполненной если студент выполнил все требования.

Временное ограничение на выполнение практической работы – 60 минут.

Во время выполнения разрешается использовать учебно-методическое пособие в LMS NetAcad, а также собственные конспекты.

При условии успешного выполнения работы студент переходит ко второй части экзамена.

2 часть:

Итоговый тест

В тесте представлены задания на проверку знаний по курсу «Компьютерные сети».

В тесте в среднем 60 вопросов.

Количество попыток выполнения - 1.

Время на прохождение теста – 90 минут.

Примеры вопросов:

1) Что сделает маршрутизатор R1 с пакетом, имеющим IPv6-адрес назначения 2001:db8:cafe:5::1?

```
R1# show ipv6 route
```

```
<output omitted>
```

```
S ::/0 [1/0]
via Serial0/0/0, directly connected
C 2001:DB8:CAFE:1::/64 [0/0]
via GigabitEthernet0/1, directly connected
L 2001:DB8:CAFE:1::1/128 [0/0]
via GigabitEthernet0/1, receive
C 2001:DB8:CAFE:2::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:CAFE:2::1/128 [0/0]
via GigabitEthernet0/0, receive
C 2001:DB8:CAFE:3::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:CAFE:3::1/128 [0/0]
via Serial0/0/0, receive
S 2001:DB8:CAFE:4::1/128 [1/0]
via Serial0/0/0, directly connected
L FF00::/8 [0/0]
via Null0, receive
```

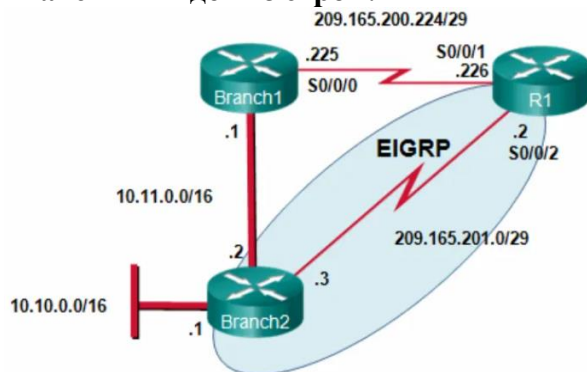
переслать пакет из GigabitEthernet0/0

отбросить пакет

переслать пакет из GigabitEthernet0/1

переслать пакет из Serial0/0/0

2) В настоящее время маршрутизатор R1 использует маршрут EIGRP, полученный от Branch2, для доступа к сети 10.10.0.0/16. Какой плавающий статический маршрут создаст резервный маршрут к сети 10.10.0.0/16 на случай, если связь между R1 и Branch2 выйдет из строя?



IP-маршрут 10.10.0.0 255.255.0.0 Serial 0/0/0 100

IP-маршрут 10.10.0.0 255.255.0.0 209.165.200.226 100

IP-маршрут 10.10.0.0 255.255.0.0 209.165.200.225 100

IP-маршрут 10.10.0.0 255.255.0.0 209.165.200.225 50

3) Что необходимо настроить для безопасного удаленного доступа к сетевому устройству?

Настроить ACL и применить его к линиям VTY.

Настроить 802.1x.

Настроить SSH.

Настроить Telnet.

4) Какой метод беспроводного шифрования самый безопасный?

WPA2 with AES

WPA2 with TKIP

WEP

WPA

5) Какой протокол или технология отключает избыточные пути для устранения петель уровня 2?

VTP

STP

EtherChannel

DTP

6) Какие сетевые атаки можно предотвратить, включив защиту BPDU?

Мошеннические коммутаторы в сети

Атаки переполнения таблицы CAM

Подмена MAC-адреса

Мошеннические DHCP-серверы в сети

7) Что может быть основной причиной, по которой злоумышленник может начать атаку с переполнением MAC-адреса?

чтобы коммутатор перестал пересылать трафик

чтобы законные хосты не могли получить MAC-адрес

чтобы злоумышленник мог видеть кадры, предназначенные для других хостов

чтобы злоумышленник мог выполнить произвольный код на коммутаторе

8) Какой метод смягчения последствий не позволит мошенническим серверам предоставлять клиентам ложные параметры конфигурации IP?

обеспечение безопасности портов

включение отслеживания DHCP

отключение CDP на граничных портах

реализация защиты портов на пограничных портах

Экзаменационная оценка выставляется по итогам теста по правилам:

В случае невыполнения практической работы (часть 1 экзамена) студенту выставляется оценка «неудовлетворительно».

Итоги прохождения теста оцениваются следующим образом:

- задание с 1 вариантом ответа – 1 балл;

- задание с множественным выбором – 2 балла, 1 балл - если только один ответ верный, 0 баллов – если нет правильных ответов или выбрано больше вариантов, чем необходимо;

- задание с сопоставлением – 2 балла.

Полностью неправильно выполненное задание – 0 баллов.

В среднем, максимальное количество баллов по итогам финального теста – 100

Набранное количество баллов интерпретируется в процентное соотношение и оценивается. От 90-100% соответствует оценке «отлично», 80-90% – оценке «хорошо», 70-80% – оценке «удовлетворительно», менее 70% – оценка «неудовлетворительно» (знания и умения на данном этапе освоения дисциплины не сформированы).

Приложение № 2 к рабочей программе дисциплины «Компьютерные сети»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Компьютерные сети» являются лекции и практические работы, причем в достаточно большом объеме. Это связано с тем, что в основе Компьютерных сетей лежат самые современные теоретические и практические знания и навыки. По всем темам предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам и отработка навыков работы с сетевым оборудованием.

Для успешного освоения дисциплины очень важно решение достаточно большого количества теоретических и практических работ, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения работ разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения теоретических и практических работ – помочь усвоить фундаментальные понятия и основы компьютерных сетей.

Задания для самостоятельного решения формулируются на лекциях и практических занятиях. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач. Полный список заданий для самостоятельной работы по темам (разделам) дисциплины приведен в ЭУК в LMS Moodle «Компьютерные сети» и ЭУК в LMS NetAcad. Вопросы, возникающие в процессе или по итогам решения этих задач, можно задать на консультациях или в форуме (чате) в ЭУК в LMS Moodle.

Для самостоятельной работы, в том числе и повтора, разобранного на лекциях и практических занятиях материала первого семестра изучения дисциплины, рекомендуется использовать учебно-методическое пособие в LMS NetAcad. Материал каждого раздела включает в себя изложение теоретического материала по заданной теме, который затем иллюстрируется подробным решением типичных задач. В заключение каждого раздела приводятся задания для самостоятельного решения, ответы к этим заданиям и указания по их решению показываются после их выполнения.

В конце первого семестра изучения дисциплины студенты сдают зачет, в конце всего курса – экзамен. Зачет по итогам первого семестра выставляется по итогам финального теста и практической работы в программе Cisco Packet Tracer. На зачете проверяются знания, умения и навыки студентов в работе с основными компонентами компьютерных сетей, являющимися основой для построения сетевой инфраструктуры.

В конце второго семестра изучения дисциплины студенты сдают экзамен. Экзамен принимается в виде теста и практической работы на сетевом оборудовании. Проверяются знания, полученные в ходе прохождения курса, навыки и умения, применяемые для построения сети, обеспечения ее бесперебойной работы и обеспечения базового уровня безопасности ее работы.