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

Кафедра математического анализа

УТВЕРЖДАЮ

Декан математического факультета

Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Компьютерные сети, курс CCNA. Часть 2

Направление подготовки (специальности)
02.03.01 Математика и компьютерные науки

Направленность (профиль)
«Программирование, алгоритмы и анализ данных»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целями освоения дисциплины “ Компьютерные сети, курс CCNA. Часть 2” являются:

1) фундаментальная подготовка в области вычислительных сетей;

2) овладение методами решения основных типов задач в этой области.

Курс “ Компьютерные сети, курс CCNA. Часть 2” обеспечивает приобретение знаний и навыков в соответствии с государственным образовательным стандартом, содействует фундаментализации образования, формированию современного представления о мире компьютерных телекоммуникаций и развитию системного мышления. Для освоения курса необходимы знания по следующим дисциплинам: информатика, аппаратные средства вычислительной техники, языки программирования, операционные системы. Знания и практические навыки, полученные в курсе “Компьютерные сети, курс CCNA. Часть 2” позволяют проектировать новые вычислительные сети и проводить анализ и оптимизацию существующих вычислительных сетей.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерные сети, курс CCNA. Часть 2» является дисциплиной по выбору и относится к вариативной части Блока 1, содействует фундаментализации образования, формированию современного представления о мире компьютерных телекоммуникаций и развитию системного мышления. Для освоения курса необходимы знания по следующим дисциплинам: информатика, аппаратные средства вычислительной техники, языки программирования, операционные системы. Знания и практические навыки, полученные в курсе “ Компьютерные сети, курс CCNA. Часть 2” позволяют проектировать новые вычислительные сети и проводить анализ и оптимизацию существующих вычислительных сетей.

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		
ПК-3 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники.	ПК-3.2 Знает основные методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов, их сопровождения, администрирования и развития (эволюции).	**Знать:** - 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;

	ПК-3.3 Умеет использовать методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта	**Уметь:** - 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 среды WLAN;
	ПК-3.3 Умеет использовать методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта	**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 4 зачетных единиц, 144 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)* *Формы ЭО и ДОТ (при наличии)*
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Принципы коммутации, VLAN и маршрутизация между VLAN.	6	2	8				13	Задания для самостоятельной и совместной практической работы
	в том числе с ЭО и ДОТ							4	Задания для самостоятельной практической работы, Тест для самопроверки Самостоятельная работа №7
2	Избыточность сетей.	6	4	4				8	Задания для самостоятельной и совместной практической работы
	в том числе с ЭО и ДОТ							3	Задания для самостоятельной практической работы, Тест для самопроверки Самостоятельная работа №8
3	Доступные и надежные сети.	6	4	6		1		10	Задания для самостоятельной и совместной практической работы
	в том числе с ЭО и ДОТ							3	Задания для самостоятельной практической работы, Тест для самопроверки Самостоятельная работа №9
4	Безопасность на уровне 2 и безопасность WLAN.	6	2	8		1		10	Задания для самостоятельной и совместной практической работы
	в том числе с ЭО и ДОТ					*1*		*3*	Задания для самостоятельной практической работы, Тест для самопроверки Самостоятельная работа №10
5	Концепция маршрутизации и конфигурация.	6	4	6		1		14	Задания для самостоятельной и совместной практической работы
	в том числе с ЭО и ДОТ							5	Задания для самостоятельной практической работы, Тест для самопроверки Самостоятельная работа №11
						2	***0,5***	***33,5***	Экзамен
	Всего за 6 семестр 144 часа		**16**	**32**		**6**	**0,5**	**54**	
	в том числе с ЭО и ДОТ					***1***		***18***	
	ИТОГО								
	в том числе с ЭО и ДОТ								

** ЭО и ДОТ выполняются в двух системах: Тестовые задания для самопроверки и проверочные тесты для оценки знаний выполняются на платформе Cisco NetAcad; Задания для самостоятельной практической работы выполняются в ЭУК «Компьютерные сети» в LMS Moodle.*

Содержание разделов дисциплины:

Принципы коммутации, VLAN и маршрутизация между VLAN.

1. Базовая настройка устройств

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.
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.
1.3. Удаленный защищенный доступ. Принцип работы Telnet. Принцип работы SSH. Конфигурация SSH. Проверка работы SSH.
1.4. Базовая конфигурация маршрутизатора. Настройка основных параметров маршрутизатора. Топология с использованием двойного стека. Настройка интерфейсов маршрутизатора. Интерфейсы обратной петли IPv4.
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.

2. Принципы коммутации.

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).
2.2. Коммутационные домены. Домены коллизий. Домены широковещательной рассылки. Снижение перегрузок сети.

3. Сети VLAN.

3.1. Обзор виртуальных локальных сетей. Определения виртуальной локальной сети. Преимущества виртуальных локальных сетей (VLAN). Типы виртуальных локальных сетей.
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.
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.
3.4. Транки виртуальных сетей. Команды конфигурации магистрального канала (транка). Пример конфигурации магистрального канала. Проверка конфигурации транкового канала. Сброс транка в состояние по умолчанию.
3.5. Динамический протокол транкинга (DTP). Знакомство с DTP. Согласованные режимы интерфейса. Результаты настройки DTP. Проверка режима протокола DTP.

Избыточность сетей.

4. Маршрутизация между сетями VLAN

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.

4. Принципы STP

5.1. 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.

5.2. 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.

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

5. EtherChannel

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

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

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

Доступные и надежные сети

6. DHCPv4.

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

7.2. 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.
7.3. Маршрутизатор Cisco как клиент DHCPv4. Пример конфигурации. Домашний маршрутизатор как клиент DHCPv4.

8. SLAAC и DHCPv6.
8.1. Конфигурация узла IPv6. IPv6 Локальный адрес канала хоста. Назначение GUA IPv6. Три флага сообщений RA.
8.2. Обзор SLAAC. Включение SLAAC. Только метод SLAAC. Сообщения RS ICMPv6. Хост процесс для создания идентификатора интерфейса. Обнаружение дублирующихся адресов (DAD).
8.3. 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.
8.4. 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. Принципы работы FHRP.
9.1. Протокол резервирования первого перехода (FHRP). Ограничения шлюза по умолчанию. Резервирование маршрутизаторов. Действия при переключении в случае отказа маршрутизатора. Варианты FHRP.
9.2. Общие сведения о протоколе HSRP. Приоритет и приоритетное вытеснение HSRP. Состояния и таймеры HSRP.

Безопасность на уровне 2 и безопасность WLAN

10. Принципы обеспечения безопасности сети.
10.1. 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.
10.2. Контроль доступа. Аутентификация с локальным паролем. Компоненты AAA. Аутентификация. Авторизация. Учет. 802.1X.
10.3. Угрозы безопасности на уровне 2. Уязвимости на уровне 2. Категории атак на коммутаторы. Технологии нейтрализации атак на коммутацию.
10.4. Атака на таблицу MAC-адресов. Обзор работы коммутатора. Атака переполнением на таблицу MAC-адресов. Противодействие атакам на таблицы CAM.
10.5. 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.

11. Настройка параметров безопасности коммутатора.
11.1. 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.

11.2. Отражение атак на виртуальные локальные сети. Обзор атак VLAN. Шаги, чтобы нейтрализовать атаки VLAN Hopping.
11.3. Отражение атак через DHCP. Обзор атак DHCP. Отслеживание DHCP-сообщений. Шаги по реализации DHCP Snooping. Пример настройки DHCP Snooping.
11.4. Отражение атак через ARP. Динамический анализ ARP. Руководство по внедрению DAI. Пример конфигурации DAI.
11.5. Отражение атак через STP. PortFast и BPDU Guard. Настройка PortFast. Настройка BPDU Guard.

12. Основные понятия WLAN.
12.1. Введение в технологии беспроводной связи. Преимущества беспроводной связи. Типы беспроводных сетей. Беспроводные технологии. Стандарты 802.11. Радиочастоты. Организации по стандартизации беспроводных сетей.
12.2. Составляющие WLAN. Беспроводные сетевые адаптеры. Домашний беспроводной маршрутизатор. Беспроводные точки доступа. Категории AP. Антенны для беспроводных устройств.
12.3. 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.
12.4. Введение в CAPWAP. Разделенная MAC-архитектура. Шифрование DTLS. FlexConnect AP.
12.5. Управление каналами. Насыщение частотного канала. Выбор канала. Планирование развертывания беспроводной сети.
12.6. Угрозы для беспроводных локальных сетей. Обзор безопасности беспроводной сети. Атаки типа «отказ в обслуживании» (DoS-атаки). Вредоносные точки доступа. Атака с перехватом.
12.7. Безопасность беспроводных локальных сетей. Сокрытие SSID и фильтрация MAC-адресов. 802.11 Оригинальные методы аутентификации. Методы аутентификации согласованного ключа. Аутентификация домашнего пользователя. Методы шифрования. Аутентификация на корпоративном уровне. WPA3.

13. Настройка беспроводных сетей.
13.1. 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.
13.2. Конфигурация Базового WLAN с контроллером беспроводной сети. Топология WLC. Просмотр всей информации о точках доступа. Расширенные настройки. Настройка WLAN.
13.3. 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.
13.4. Способы поиска и устранения неполадок с беспроводными сетями. Невозможно подключить беспроводной клиент. Поиск и устранение неполадок в случае медленной работы сети. Обновление микропрограммного обеспечения.

Концепция маршрутизации и конфигурация

14. Принципы маршрутизации.
14.1. 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.
14.2. Процесс принятия решения о переадресации пакетов. Сквозная пересылка пакетов. Механизмы пересылки пакетов.
14.3. 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.
14.4. Статическая и динамическая маршрутизация. Эволюция протоколов динамической маршрутизации. Принципы динамических протоколов маршрутизации. Оптимальный путь. Распределение нагрузки.

15. Статическая IP-маршрутизация.
15.1. 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.
15.2. 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.
15.3. Статический маршрут по умолчанию. Настройка статического маршрута по умолчанию. Проверка статического маршрута по умолчанию.
15.4. Плавающие статические маршруты. Настройка плавающих статических маршрутов IPv4 и IPv6. Проверка плавающего статического маршрута.
15.5. 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.

16. Поиск и устранение неполадок, связанных со статическими маршрутами и маршрутами по умолчанию.
16.1. Обработка пакетов с использованием статических маршрутов.
16.2. 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:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

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.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс «Компьютерные сети» в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены задания для самостоятельной практической работы обучающихся по темам дисциплины;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

Электронный учебный курс «Компьютерные сети» в LMS Cisco NetAcad, в котором:

- представлены тексты лекций по темам дисциплины;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

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

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

а) основная литература

1) Олифер, Виктор Григорьевич «Компьютерные сети: принципы, технологии, протоколы: учеб. пособие для вузов / В. Олифер, Н. Олифер;
М-во образования и науки РФ. - 5-е изд. - СПб.: Питер, 2017 - 991 с. - (Учебник для вузов). Библиогр.: с. 955-956. - ISBN 978-5-496-01967-5
http://www.lib.uniyar.ac.ru/opac/bk_cat_card.php?rec_id=2069619&cat_cd=YARSU

2)Учебно-методическое пособие в LMS NetAcad. Режим доступа: свободный для участников Программы Сетевой Академии Cisco (https://www.netacad.com/)

б) дополнительная литература

1. Компьютерные сети [Электронный ресурс] : учебник / В.Г. Карташевский [и др.]. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. — 267 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/71846.html

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 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:

Ассистент кафедры нелинейной динамики		О.Е. Бизин
должность, ученая степень	*подпись*	*И.О. Фамилия*

Приложение № 1 к рабочей программе дисциплины
«Компьютерные сети, курс CCNA, часть 2»

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

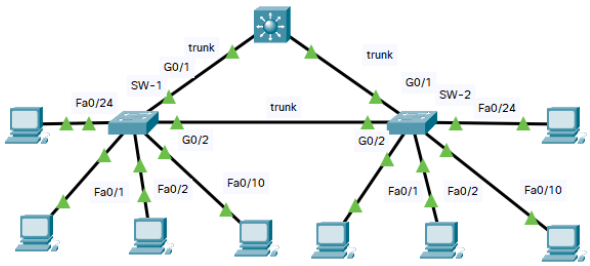
(Задания размещаются в ЭУК «Компьютерные сети» в LMS Moodle и выполняются в программе эмуляции сети «Cisco Packet Tracer (доступен бесплатно для участников Программы Сетевой Академии Cisco)»)
Во время выполнения работы студент может видеть свой прогресс в процентном соотношении. Большинство работ сопровождаются методическими материалами.

Тема: Конфигурация безопасности коммутатора

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 в отношении широковещательных и коллизионных доменов?

1) Чем больше интерфейсов маршрутизатор имеет, тем больше результирующий домен широковещательной рассылки;
2) Добавление коммутатора в сеть увеличит размер домена широковещательной рассылки;
3) Размер домена коллизии можно уменьшить путем добавления концентраторов в сеть;
4) Добавление маршрутизатора в сеть увеличит размер домена коллизии.

Вопрос 2. Что будет делать коммутатор локальной сети Cisco, если получит входящий кадр с MAC-адресом назначения, который отсутствует в таблице MAC-адресов?

1) Перешлет кадр через все порты, за исключением порта, на котором этот кадр был получен;
2) Отправит кадр на адрес шлюза по умолчанию;
3) Отбросит этот кадр;
4) Использует протокол ARP для определения порта, связанного с этим кадром.

Вопрос 3. Коммутатор Cisco в настоящее время разрешает трафик с тегами VLAN 10 и 20 через магистральный порт Fa0/5. Каков эффект ввода команды switchport trunk allowed vlan 30 на Fa0/5?

1) Он позволяет использовать только VLAN 30 на Fa0/5;
2) Он разрешает VLAN от 1 до 30 на Fa0/5;
3) Это позволяет реализовать native VLAN 30 на Fa0/5;
4) Он разрешает VLAN 10, 20 и 30 на Fa0/5.

Вопрос 4. Каково значение числа 10 в команде encapsulation dot1Q 10 native?
1) Номер подсети;
2) Номер подинтерфейса;
3) Идентификатор VLAN;
4) Номер интерфейса;

Вопрос 5. Какая дополнительная информация содержится в 12-битном расширенном идентификаторе системы BPDU?

1) IP-адрес;
2) port ID;
3) Идентификатор VLAN;
4) MAC-адрес;

Вопрос 6. Какой IPv4-адрес назначения использует клиент DHCPv4 для отправки начального пакета обнаружения DHCP Discover при поиске DHCP-сервера?

1) 127.0.0.1;
2) 224.0.0.1;
3) 255.255.255.255;
4) IP-адрес шлюза по умолчанию.

Вопрос 7. Какова цель HSRP?

1) Предотвращает превращение коммутатора в кореневой STP;
2) Позволяет порту доступа немедленно переходить в состояние пересылки;
3) Предотвращает подключение вредоносных узлов к портам магистральных каналов;
4) Обеспечивает непрерывное сетевое соединение при сбое маршрутизатора.

Вопрос 8. Верно или нет утверждение? В стандарте 802.1X клиент, пытающийся получить доступ к сети, называется запрашивающим устройством.

1) Верно
2) Неверно.

Правильные ответы

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

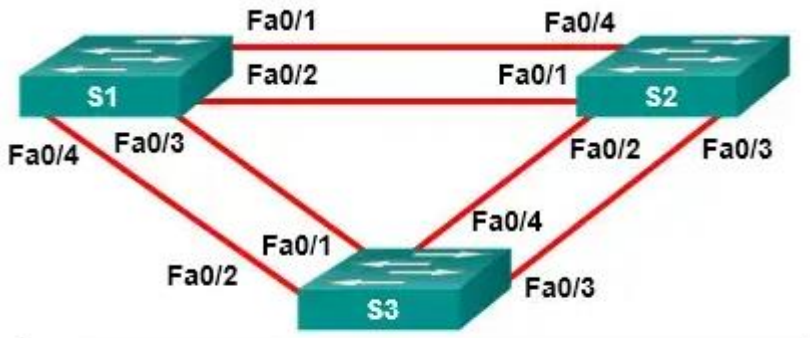
Самостоятельные работы в виде тестовых заданий.
Тесты проводятся в ЭУК «Компьютерные сети» в LMS NetAcad
В каждом тесте в среднем 60 вопросов по пройденным темам (2-4).
Количество попыток выполнения - 5. Время на прохождение теста - 1,5 часа.
При завершении теста показываются ошибки (если есть) и какую тему и раздел смотреть, чтобы разобраться и исправить ошибку. Итоги прохождения теста оцениваются.

Примеры вопросов:

1. Сеть небольшой компании имеет шесть взаимосвязанных коммутаторов уровня 2. В настоящее время все коммутаторы используют значение приоритета моста по умолчанию. Какое значение можно использовать для настройки приоритета моста одного из коммутаторов, чтобы гарантировать, что он станет корневым мостом в этой конструкции?

-1
-28672
-32768
-34816
-61440

2. Администратор попытался создать EtherChannel между S1 и двумя другими коммутаторами с помощью показанных команд, но безуспешно. В чем проблема?




```
S1(config)# interface range fa0/1 - 4
S1(config-if-range)# channel-group 1 mode on
```

-Трафик не может быть отправлен на два разных коммутатора через один и тот же канал EtherChannel.
-Трафик не может быть отправлен на два разных коммутатора, а только на два разных устройства, таких как сервер с поддержкой EtherChannel и коммутатор.
-Трафик может быть отправлен только на два разных коммутатора, если EtherChannel реализован на интерфейсах Gigabit Ethernet.
-Трафик может быть отправлен только на два разных коммутатора, если EtherChannel реализован на коммутаторах уровня 3.

3. Какая технология является стандартом открытого протокола, который позволяет коммутаторам автоматически объединять физические порты в единую логическую связь?

-PAgP
-LACP
-Многоканальный PPP
-DTP

4. Клиентский компьютер с поддержкой DHCP только что загрузился. В течение каких двух этапов клиентский КОМПЬЮТЕР будет использовать широковещательные сообщения при обмене данными с сервером DHCP? (Выберите два.)

-DHCPDISCOVER
-DHCPACK
-DHCPOFFER
-DHCPREQUEST
-DHCPNAK

5. Пул адресов DHCP-сервера настроен на 10.92.71.0/25. Администратор сети резервирует 8 IP-адресов для серверов. Сколько IP-адресов осталось в пуле для назначения другим хостам?

-122
-118
-119
-108
-116

6. При настройке коммутатора для доступа по SSH какую другую команду, связанную с локальной командой входа, необходимо ввести на коммутаторе?

-enable secret password
-password password
-username username secret secret
-login block-for seconds, number within*seconds*

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.

Правила выставления оценки на экзамене.

Экзамен состоит из двух частей.

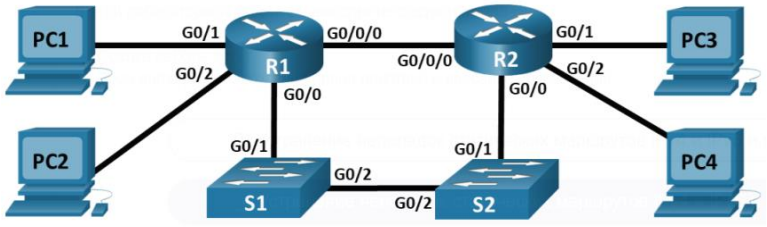
1 часть:

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 асиметричных ключей шифрования длинной 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?

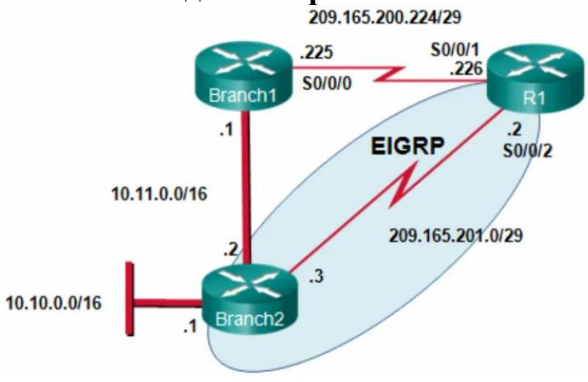
```
R1# show ipv6 route

<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, курс CCNA. Часть 2**»**

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 основной 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.