МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.01.01 Компьютерные сети

программы подготовки специалистов среднего звена
09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2026

Рабочая программа учебной дисциплины МДК.01.01 Компьютерные сети профессионального модуля ПМ,01 Настройка сетевой инфраструктуры разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование, утверждённого приказом Минобр-науки РФ от 10.07.2023 г. № 519, примерной образовательной программой.

Разработчики:

Головин Д.И, преподаватель Колледжа сервиса и дизайна ВВГУ

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № _9__ от «_18» 05 2026_ г.

Председатель ЦМК ___ _____Е.А. Стефанович
подпись

Согласована:

Начальник отдела информационных технологий, Филиал Российской телевизионной и радиовещательной сети «Приморский краевой радиотелевизионный передающий центр»

Д.М. Шумов

(подпись, печать)

СОДЕРЖАНИЕ

1	Общая характеристика рабочей программы учебной дисциплины	4
2	Структура и содержание учебной дисциплины	6
3	Условия реализации программы учебной дисциплины	23
4	Контроль и оценка результатов освоения учебной дисциплины	24
5	Фонд оценочных средств	

1. Общая характеристика рабочей программы учебной дисциплины

1.1 Место дисциплины в структуре основной образовательной программы

Рабочая программа МДК.01.01 Компьютерные сети является частью профессионального цикла основной образовательной программы (далее ООП) в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

1.2 Цель и планируемые результаты освоения дисциплины

По итогам освоения дисциплины, обучающиеся должны продемонстрировать результаты обучения, соотнесённые с результатами освоения ООП СПО, приведенные в таблице:

Код ОК, ПК	Код результата обучения	Наименование результата обучения
ПК1.1- ПК.1.7 ОК1- ОК9	У1	Проектировать локальную сеть, выбирать сетевые топологии
	У2	Использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети
	З1	Общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям
	З2	Архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры
	З3	Базовые протоколы и технологии локальных сетей
	З4	Принципы построения высокоскоростных локальных сетей
	З5	Стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	161
В том числе	
- теоретическое обучение	54
- практические занятия	78
- самостоятельная работа	23
- промежуточная аттестация (экзамен)	4

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовой проект		Объём в часах
1	**2**		**3**
Раздел 1. Компьютерные сети			
МДК.01.01. Компьютерные сети			**161**
Тема 1.1. Введение в сетевые технологии	**Содержание**		**16**
	1	**Компьютерные сети** Совместная работа, Интернет и современные сетевые технологии – область применения и назначение. Виды компьютерных сетей. Глобальные и локальные сети. Одноранговые и клиент-серверные архитектуры. Основные компоненты сетей, сетевая среда и сетевые устройства. Технологии подключения к Интернет. Конвергентные сети. Качество и надежность сетей. Основные понятия сетевой безопасности. Тенденции развития сетей.	
	2	**Сетевые протоколы и коммуникации** Кодирование и параметры сообщения. Сетевые протоколы. Взаимодействие протоколов. Набор протоколов TCP/IP и процесс обмена данными. Организации по стандартизации: ISOC, IAB, IETF, IEEE, ISO. Многоуровневые модели OSI и TCP/IP. Инкапсуляция данных. Протокольные блоки данных (PDU). Доступ к локальным ресурсам. Сетевая адресация. MAC- и IP-адреса. Доступ к удалённым ресурсам. Шлюз по умолчанию.	
	3	**Сетевой доступ** Протоколы и стандарты физического уровня. Способы подключения к сети. Сетевые интерфейсные платы (NIC). Среды передачи данных и их характеристики: пропускная способность, производительность. Виды медных сетевых кабелей: UTP, STP, коаксиальный. Разновидности, особенности прокладки и тестирования кабелей. Структура и особенности прокладки оптоволоконных кабелей. Беспроводные средства передачи данных. Стандарт Wi-Fi IEEE 802.11. Канальный уровень и его подуровни: Управление логическим каналом (LLC) и Управление доступом к среде передачи данных MAC. Структура кадра канального уровня и принципы его формирования. Стандарты канального уровня. Физическая и логическая топология сети. Топологии «точка-точка», «звезда», «полносвязанная», «кольцевая». Полудуплексная и полнодуплексная передача данных. Особенности кадров LAN, WAN, Ethernet, PPP, 802.11.	
	4	**Сетевые технологии Ethernet** Семейство сетевых технологий Ethernet. Принцип работы Ethernet. Взаимодействие на подуровнях LLC и MAC. Управление доступом к среде передачи данных (CSMA). MAC-адрес: идентификация Ethernet. Атрибуты кадра Ethernet. Представления MAC-адресов. Одно- и мно-	

		гоадресной, широковещательной рассылок. Сквозное подключение, MAC- и IP-адреса. Протокол разрешения адресов (ARP): принципы работы, роль в процессе удаленного обмена данными. Таблицы ARP на сетевых устройствах. Основные недостатки протокола ARP - Нагрузка на среду передачи данных и безопасность. Основная информация о портах коммутатора. Таблица MAC-адресов коммутатора. Функция Auto-MDIX. Способы пересылки кадра на коммутаторах Cisco. Буферизация памяти на коммутаторах. Фиксированная и модульная конфигурации коммутаторов. Сравнение коммутации уровня 2 и уровня. Технология Cisco Express Forwarding. Виртуальный интерфейс коммутатора (SVI), Маршрутизируемый порт, EtherChannel уровня 3. Конфигурация маршрутизируемого порта.	
	5	**Сетевой уровень** Сетевой уровень в процессе передачи данных. Протоколы сетевого уровня. Основные характеристики IP-протокола. Структура пакетов IPv4 и IPv6. Особенности и преимущества протокола Pv6. Методы маршрутизации узлов. Таблица маршрутизации узлов и маршрутизатора для протоколов IPv4 и IPv6. Устройство маршрутизатора – Процессор, память, операционная система. Подключение к маршрутизатору через различные порты. Настройка исходных параметров, интерфейсов, шлюза по умолчанию и других характеристик маршрутизатора.	
	6	**IP-адресация** Структура IPv4-адресов. Сетевая и узловая часть IP-адреса. Преобразование адресов между двоичным и десятеричным представлением. Маска подсети IPv4. Сетевой адрес, адрес узла и широковещательный адрес сети IPv4. Присвоение узлу статического и динамического IPv4-адреса. Многоадресная передача. Публичные и частные IPv4-адреса. IPv4-адреса специального назначения. Присвоение IP-адресов. Совместное использование протоколов IPv4 и IPv6: двойной стек, туннелирование, преобразование. Представление IPv6-адресов. Правила сокращения записи IPv6-адресов. Индивидуальный, групповой, произвольный типы IPv6-адресов. Структуры локального и глобального индивидуальных IPv6-адресов. Статическая и динамическая конфигурации глобального индивидуального адреса. Процесс EUI-64 и случайно сгенерированный идентификатор интерфейса. ICMP-сервисы. Отличия для протоколов IPv4 и IPv6. Сообщения ICMPvI6 «Запрос к маршрутизатору», «Объявление от маршрутизатора», «Запрос соседнего узла» и «Объявление соседнего узла». Тестирование сети с помощью эхо-запросов. Трассировка маршрута. Время прохождения сигнала в прямом и обратном направлениях (RTT). Время жизни (TTL) IPv4 и предел переходов IPv6.	
	7	**Разделение IP-сетей на подсети** Сегментация IP-сетей. Обмен данными между подсетями. Планирование адресации в подсетях. Расчетные формулы для сегментации сети. Разбиение на подсети на основе требований узлов и сетей, в соответствии с требованиями сетей. Определение маски подсети. Разбиение на подсети с использованием маски переменной длины (VLSM).	

		Базовая модель и назначение блоков адресов VLSM. Планирование адресации сети. Особенности проектирования IPv6-сети. Разбиение на подсети с использованием идентификатора интерфейса.	
	8	**Транспортный уровень** Назначение и задачи транспортного уровня. Мультиплексирование сеансов связи. Описание и сравнение протоколов TCP и UDP – надежность и производительность, область применения. Адресация портов и сегментация TCP и UDP. Обмен данными по TCP. Процессы TCP сервера. Установление TCP-соединения и его завершение. Принципы «трёхстороннего рукопожатия» TCP. Надёжность и управление потоком TCP - Подтверждение получения сегментов, потеря данных и повторная передача, управление потоком. Обмен данными с использованием UDP. Процессы и запросы UDP-сервера, UDP-датаграммы, процессы UDP-клиента. Приложения, использующие UDP и TCP.	
	9	**Уровень приложений** Уровень приложений, уровень представления и сеансовый уровень. Примеры распространенных приложений. Протоколы уровня приложений. Одноранговые сети (P2P). Модель типа «клиент-сервер». Обзор протоколов HTTP, HTTPS, SMTP, POP и IMAP. Служба доменных имён (DNS). Формат сообщений и иерархия DNS. Утилита «nslookup». Служба DHCP. Протокол передачи файлов (FTP). Протокол обмена блоками серверных сообщений (SMB). Концепции «Всеобъемлющий Интернет» BYOD. Доставка данных по конвергентным сетям.	
	Практические занятия		**2**
	1.1.1	Разделение сети на подсети	
Тема 1.2. Принципы маршрутизации и коммутации	**Содержание**		**28**
	1	**Введение в коммутируемые сети** Объединённые сети. Иерархия в коммутируемой сети. Роль коммутируемых сетей. Коммутируемая среда. Динамическое заполнение таблицы MAC-адресов коммутатора. Методы пересылки на коммутаторе. Коммутация с промежуточным хранением. Сквозная коммутация. Коммутационные домены. Снижение перегрузок сети.	
	2	**Основные концепции и настройка коммутации** Основные концепции и настройка коммутации. Первоначальная настройка коммутатора и восстановление после системного сбоя. Настройка доступа для базового управления коммутатором с IPv4. Дуплексная связь. Настройка портов коммутатора на физическом уровне. Функция автоматического определения типа кабеля (Auto-MDIX). Проверка настроек порта коммутатора. Поиск и устранение проблем на уровне доступа к сети. Безопасность коммутатора. Защищённый удалённый доступ. Настройка SSH. Распространённые угрозы безопасности: переполнение таблицы MAC-адресов, DHCP-спуфинг, использование уязвимостей протокола CDP, Атаки Telnet и др. Аудит и практические рекомендации по	

		обеспечению безопасности сети. Безопасность порта коммутатора. Отслеживание DHCP сообщений. Функция безопасности порта. Виды защиты MAC-адресов. Режимы реагирования на нарушение безопасности. Проверка и настройка портов. Протокол сетевого времени (NTP).	
	3	**Виртуальные локальные сети (VLAN)** Виртуальные локальные сети (VLAN) – классификация и основные характеристики. Транки виртуальных сетей. Контроль широковещательных доменов в сетях VLAN. Тегирование кадров Ethernet для идентификации сети VLAN. Сети native VLAN и тегирование стандарта 802.1Q. Тегирование голосовой VLAN. Реализации виртуальной локальной сети. Назначение портов сетям VLAN. Настройка транковых каналов. Протокол динамического создания транкового канала (DTP). Поиск и устранение неполадок в виртуальных локальных сетях и транковых каналах. Проблемы с IP-адресацией сети VLAN. Несовпадения режимов транковой связи. Проектирование и обеспечение безопасности VLAN: hopping, спуфинг коммутатора, атака с двойным тегированием, Сеть PVLAN периметра. Практические рекомендации по проектированию виртуальной локальной сети.	
	4	**Концепция маршрутизации** Настройка маршрутизатора. Механизмы пересылки пакетов. Подключение и настройка устройств. Светодиодные индикаторы на маршрутизаторе. Активация и настройка IP-адресации. Проверка связности сетей с прямым подключением. Проверка настроек интерфейса. Фильтрация выходных данных команд «show». Коммутация пакетов между сетями. Функция коммутации маршрутизатора. Маршрутизация пакетов. Определение пути. Процесс принятия решения о пересылке пакетов. Выбор оптимального пути. Протоколы RIP, OSPF, EIGRP. Распределение нагрузки. Администрирование расстояние (AD) и надежность маршрута. Анализ таблиц маршрутизации – источник данных, принципы формирование возможности настройки. Записи таблицы маршрутизации для сетей с прямым подключением. Задание статических маршрутов. Протоколы динамической маршрутизации сетей IPv4 и IPv6.	
	5	**Маршрутизация между VLAN** Принципы работы маршрутизации между VLAN. Настройка маршрутизации на базе маршрутизаторов с несколькими физическими интерфейсами, с использованием конфигурации router-on-a-stick, через многоуровневый коммутатор. Проблемы маршрутизации между VLAN. Проверка конфигурации коммутатора и настроек маршрутизатора. Неполадки в работе интерфейса. Ошибки в IP-адресах и масках подсети. Настройка и работа коммутации на 3-м уровне. Маршрутизация между VLAN через виртуальные интерфейсы коммутатора, маршрутизируемые порты. Неполадки в настройках коммутатора 3-го уровня.	
	6	**Статическая маршрутизация** Преимущества и задачи статической маршрутизации. Типы статических маршрутов: стандартный, по умолчанию, суммарный, плавающий. Настройка статических маршрутов IPv4 и IPv6. Команда «ip route». Маршрут следующего перехода. Напрямую подключённый статиче-	

		ский маршрут. Полностью заданный статический маршрут. Настройка статического маршрута по умолчанию. Классовая адресация. Классовые маски подсети. Бесклассовая междоменная маршрутизация CIDR. Объединение маршрутов. Организация суперсетей. Использование масок подсети фиксированной длины (FLSM). Маска подсети переменной длины (VLSM). Настройка суммарных и плавающих статических маршрутов. Расчёт суммарного маршрута. Объединение сетевых адресов IPv4 и IPv6. Поиск и устранение неполадок в настройках статического маршрута и маршрута по умолчанию.	
	7	**Динамическая маршрутизация** Протоколы динамической маршрутизации – назначение, принципы работы и история развития. Сравнение динамической и статической маршрутизации. Принципы работы протоколов маршрутизации: пуск после включения питания, Сетевое обнаружение, Обмен данными маршрутизации, Обеспечение сходимости. Классификация протоколов маршрутизации. Протоколы IGP и EGP. Дистанционно-векторные протоколы RIP, IGRP. Протоколы маршрутизации по состоянию канала OSPF и IS-IS. Классовые и бесклассовые протоколы маршрутизации. Характеристики и метрики протоколов. Динамическая дистанционно-векторная маршрутизация. Дистанционно-векторный алгоритм. Механизмы отправки и получения данных маршрутизации, расчёта оптимальных путей и добавления маршрутов в таблицу маршрутизации, обнаружения и реагирования на изменения в топологии. Настройка протокола RIP: включение RIPv2, отключение автоматического объединения, настройка пассивных интерфейсов, передача маршрута по умолчанию по сети. Настройка протокола RIPng. Процесс маршрутизации по состоянию канала. Hello протокол. пакет состояния канала (LSP). Лавинная рассылка пакетов состояния канала. Лавинная рассылка пакетов состояния канала. Создание дерева кратчайших путей SPF. Добавление маршрутов OSPF в таблицу маршрутизации. Недостатки протоколов маршрутизации по состоянию канала. Таблица маршрутизации. Записи с прямым подключением и удалённой сети. Динамически получаемые маршруты IPv4/6. Процесс поиска маршрута.	
	8	**Протокол DHCP** Протокол DHCP. DHCPv4: базовая операция, формат сообщений, сообщения обнаружения и предложения. Настройка, проверка и ретрансляция простого DHCPv4-сервера. Настройка маршрутизатора в качестве DHCPv4-клиента. Настройка маршрутизатора класса SOHO. Поиск и устранение неполадок в работе маршрутизатора DHCPv4. Протокол DHCPv6. Автоматическая настройка адреса без отслеживания состояния (SLAAC). Принцип работы SLAAC с DHCPv6. DHCPv6 с и без отслеживания состояния. Процессы DHCPv6. Настройка маршрутизатора в качестве DHCPv6-сервера и DHCPv6-клиента. Поиск и устранение неполадок в работе DHCPv6.	
	9	**Преобразование сетевых адресов IPv4** Преобразование сетевых адресов IPv4. Концептуальное преобразование сетевых адресов	

		(NAT). Терминология и принципы работы NAT. Пространство частных IPv4-адресов. Статическое и динамическое преобразование сетевых адресов (NAT). Преобразование адресов портов (PAT). Сравнение NAT и PAT. Преимущества и недостатки NAT. Анализ статического преобразования NAT. Принцип работы динамического NAT Настройка и проверка NAT, PAT. Переадресация портов. Настройка NAT и протокола IPv6. Поиск и устранение неполадок в работе NAT.	
	10	**Создание и настройка небольшой компьютерной сети** Планирование и создание небольшой компьютерной сети: определение ключевых факторов, выбор топологии и сетевых устройств, выбор и настройка протоколов, системы адресации. Меры по обеспечению безопасности сети. Уязвимости и сетевые атаки. Разведывательные атаки, Атаки доступа, Отказ в обслуживании (DoS-атаки). Резервное копирование, обновление и установка исправлений. Межсетевые экраны. Аутентификация, авторизация и учёт. Включение протокола SSH. Файловые системы маршрутизаторов и коммутаторов. Резервное копирование и восстановление с помощью текстовых файлов, протокола TFTP, USB-накопителя. Встроенные службы маршрутизации. Поддержка беспроводных подключений. Настройка встроенного маршрутизатора.	
	Лабораторные работы и практические занятия		**76**
	1.2.1	Настройка коммутатора: • Базовая настройка коммутатора; • Настройка параметров безопасности коммутатора.	
	1.2.2	Конфигурация сетей VLAN: • Конфигурация сетей VLAN и транковых каналов; • Поиск и устранение неполадок в конфигурации VLAN; • Реализация системы безопасности сети VLAN; • Реализация сетей VLAN для сегментации сетей предприятий малого и среднего бизнеса.	
	1.2.3	Настройка маршрутизатора: • Использование команды traceroute для обнаружения сети; • Документирование сети; • Настройка интерфейсов IPv4 и IPv6; • Настройка и проверка небольшой сети; • Исследование маршрутов с прямым подключением.	
	1.2.4	Маршрутизация между VLAN: • Настройка маршрутизации между VLAN для каждого интерфейса; • Настройка маршрутизации между VLAN на основе стандарта 802.1Q и транкового ка-	

		нала; • Поиск и устранение неполадок в маршрутизации между сетями VLAN.	
	1.2.5	Настройка статической маршрутизации: • Настройка статических маршрутов IPv4/IPv6 по умолчанию; • Разработка и реализация схемы адресации IPv4 с использованием VLSM; • Расчёт суммарных маршрутов IPv4 и IPv6; • Поиск и устранение неполадок статических маршрутов IPv4 и IPv6.	
	1.2.6	Преобразование сетевых адресов: • Изучение принципа работы NAT; • Настройка статического и динамического NAT; • Реализация статического и динамического NAT; • Настройка переадресации портов на маршрутизаторе Linksys; • Проверка, поиск и устранение неполадок конфигураций NAT; • Отработка комплексных практических навыков.	
	1.2.7	Отработка комплексных практических навыков	
Тема 1.3. Всероссийское чемпионатное движение по профессиональному мастерству «Профессионалы»	**Содержание** 1. Движение «Профессионалы» — это Стратегическая цель Движения «Профессионалы». Основные задачи Движения «Профессионалы». Этапы Всероссийского чемпионатного движения по профессиональному мастерству «Профессионалы». 2. Общие документы Всероссийского чемпионатного движения по профессиональному мастерству «Профессионалы». Положение о ВЧД. Положение об этике. Приказ 01-09-55 об итогах рассмотрения заявок для проведения конкурсного отбора для организации соревнований ИМЭЧ. Календарный план мероприятий Всероссийского чемпионатного движения по профессиональному мастерству на чемпионатный цикл 2025-2026 года. Перечень компетенций Чемпионата высоких технологий в 2026 году основной категории. Порядок проведения конкурсного отбора субъектов РФ и организаций для проведения соревнований ИМЭЧ в 2026-2027 гг. Положение о Всероссийском чемпионатном движении по профессиональному мастерству «Профессионалы». Порядок организации и проведения Регионального этапа чемпионата по профессиональному мастерству «Профессионалы» и чемпионата высоких технологий. 3. Конкурсное задание компетенции «Сетевое и системное администрирование». Разделы конкурсного задания. Используемые сокращения. Основные требования компетенции. Специальные правила компетенции. Приложения. 4. Критерии оценивания. Перечень профессиональных задач компетенции «Сетевое и системное администрирование». 5. Инфраструктурные листы. Общая зона конкурсной площадки (оборудование, инструмент, мебель). Рабочее место Конкурсанта (основное сетевое и серверное оборудование, вспомогательное оборудование, монтажный инструмент). Рабочее место Конкурсанта (расходные материалы: витая пара, патч-корды, коннекторы RJ-45). Личный инструмент (тулбокс) конкурсанта. Программа		**10**

Самостоятельная работа при изучении раздела 1 ПМ.01 • Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). • Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа при самом широком использовании Интернета и других IT технологий. • Проектные формы работы, подготовка сообщений к выступлению на семинарах и конференциях; подготовка • рефератов, докладов. • Выполнение чертежей, схем; выполнение расчётно-графических работ; модельный экономический анализ, • Опытно-экспериментальная работа. • Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** 1. Изучить характеристики, принципы работы, компоненты и конфигурирование протокола RIP. 2. Изучить характеристики, принципы работы, компоненты и конфигурирование протокола EIGRP. 3. Изучить характеристики, принципы работы, компоненты и конфигурирование протокола OSPF для одной области. 4. Изучить характеристики, принципы работы, компоненты и конфигурирование протокола DHCP. 5. Изучить характеристики, принципы работы, компоненты и конфигурирование протокола DNS. 6. Изучить технологии VLSM и CIDR.	**23**
Консультации по разделу 1 ПМ.01	**2**
Промежуточная аттестация	**4**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Кабинет информационных технологий:

количество посадочных мест – 25, стол для преподавателя 1 шт., стул для преподавателя 1 шт., компьютерный стол 20 шт., персональный компьютер ПК i3 2120/500Gb/4Gb 20 шт., мультимедийный комплект: проектор, интерактивная доска Elite Panaboard UBT-T880W 1 шт., звуковые колонки 1 шт., доска маркерная меловая комбинированная 1 шт., информационный стенд 2 шт., дидактические пособия.

ПО: 1. Windows 7(профессиональная лицензия, ООО "Битроникс Владивосток" Контракт№ 0320100030814000018-45081 от 09.09.14 № 48609744, №62096196, № 48958910, № 45829305, бессрочно);

2. MS Office 2010 pro (лицензия № 48958910, № 47774898, бессрочно);
3. Autodesk AutoCAD 2019 Edu (свободное);
4. visual c++ 2008 express edition (свободное),
5. oracle vm virtualbox (свободное),
6. cisco packet tracer (свободное),
7. microsoft SQL server 2008 (свободное),
8. k-lite codec pack (свободное),
9. visual studio 2008 (свободное).

Лаборатория организации и принципов построения компьютерных систем:

количество посадочных мест – 15, стол для преподавателя 1 шт., стул для преподавателя 1 шт.,

мультимедийный проектор с экраном 1 шт., персональный компьютер "B-tronix professional 3872\2015" 13 шт, стартовый набор Arduino UNO R3 Starter Kit V2 6 компонентов,

myRIO 6 шт контроллер ILC 131 STARTEKIT 10 шт., коммутатор 6 шт., маршрутизатор 6 шт.,

доска маркерная 1 шт.

Программное обеспеспечение:

1. "Microsoft Windows 7 Professional Russian, ООО ""Битроникс Владивосток" "Контракт№ 0320100030814000018-45081 от 09.09.14, лицензия №64099496, бесрочно"
2. Microsoft Office профессиональный плюс 2013
3. "AUTOMATIONWORX Software Suite 2016 v1.83, ООО ""Лидер Электро Поставки"", Договор ЛАП059177 от 12.08.14, лицензия №77190396 от 24.10.14"
4. Android Studio (свободное),
5. Microsoft Visual Studio (свободное)
6. Visual Studio Community 2019 (свободное)

Студия проектирования и дизайна сетевых архитектур и инженерной графики

автоматизированные рабочие места на 20 обучающихся (персональный компьютер Lenovo ThinkStation P330 Tiny (процессор I7 9700T, оперативная память 32gb, жесткий диск 1tb)

монитор Lenovo ThinkCentre TIO27 2560x1440 (веб камера, микрофон, динамики встроены в

монитор), мышь, клавиатура;

автоматизированное рабочее место преподавателя (ноутбук Lenovo IdealPad L340, процессор i7 9750H, оперативная память 8gb, жесткий диск 1tb), мышь, клавиатура;

специальная эргономическая мебель для работы за компьютером: компьютерный стол 20шт., компьютерное кресло 20 шт., стол преподавателя 1 шт., компьютерное кресло для преподавателя 1шт., 1 роектор CASIO XJ-F210WN 1 шт., экран 1 шт., принтер МФУ Xerox VersaLink C7020, цветной 1 шт., графический планшет WACOM Cintiq 16-10 шт.

25

Программное обеспечение:

1. Windows 10 Pro, ИП Струлев О.Ю. Д№32008976244 от 06.04.2020, OEM
2. OfficeProfessional Plus 2019 AcademicEdition, ООО "Акцент", Договор №292 от 24.04.2020 лицензия №V6635206 от 07.05.2020, бессрочно;
3. Adobe Creative Cloud, ООО"ИНФОРМИКА", Договор №32008982727 от 16.04.2020, лицензия от 19.04.2020;
4. Corona Render for 3ds Max-Educational-1WS+NODE, ООО"ИНФОРМИКА", Договор №32008982727 от 16.04.2020, лицензия от 08.04.2020;
5. Autodesk 3ds Max (свободное);
6. Autodesk Maya (свободное);
7. Autodesk AutoCad 2020 (свободное);
8. Autodesk Fusion 360 (свободное)

Мастерская по компетенции «Сетевое и системное администрирование»

Ноутбук -9шт; монитор 9; маршрутизатор 15; модуль Serial 9; коммутатор L2 - 9; межсетевой экран 5; напольная рэковая стойка 5; сервер 9; источник бесперебойного питания 9; коммутатор 1; телекоммуникационный шкаф 1; коммутатор L3- 9in/

Программное обеспечение:

1. Microsoft Office 2019
2. Microsoft Windows 10
3. Desktop & Application Virtualization VMware Horizon Standard Price

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 464 с.

Сергеев А.Н. Основы локальных компьютерных сетей: учебное пособие. СПО. – Москва: Лань, 2020. – 184 с.

3.2.2. Электронные издания (электронные ресурсы)

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2019. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437357 (дата обращения: 26.07.2021).
2. Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189333 (дата обращения: 26.07.2021). – Режим доступа: по подписке.

3.2.3. Дополнительные источники *(при необходимости)*

Новожилов Е.О. Компьютерные сети. – М.: ОИЦ «Академия, 2013.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации. ПК 1.2. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем. ПК 1.3. Устранять неисправности в работе инфокоммуникационных систем ПК 1.4. Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности. ПК 1.5. Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем ПК 1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта. ПК 1.7 Осуществлять регламентное обслуживание и замену расход-	Определение профессиональной задачи и этапов ее выполнения. Эффективный поиск информации для решения профессиональной задачи. Определение ресурсов для решения профессиональной задачи. Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием. Экспертное наблюдение и оценка на лабораторно-практических занятиях, при выполнении работ по учебной и производственной практикам. Защита отчетов по практическим и лабораторным работам. Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экзамен квалификационный.

ных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.		

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Подбор вариантов решения конкретной профессиональной задачи или проблемы.	Оценка полноты перечня подобранных вариантов
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.	Демонстрация навыков использования информационных порталов в сети Интернет, включая официальные информационно-правовые порталы.	Оценка полноты перечня подобранных вариантов
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	Демонстрация интереса к выбранной специальности, к инновационным технологиям в области профессиональной деятельности.	Участие в мероприятиях (олимпиады, конкурсы профессионального мастерства, стажировки и др.), проводимых как образовательным заведением, так и ведущими предприятиями отрасли
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.	Демонстрация навыков межличностного общения с соблюдением общепринятых правил со сверстниками в образовательной группе, с преподавателями во время обучения, с руководителями производственной практики.	Экспертное наблюдение поведенческих навыков в ходе обучения
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	Демонстрация навыков грамотной устной и письменной речи	Экспертное наблюдение навыков устного и письменного общения в ходе обучения
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе тради-	Формирование чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению; взаимного уважения, бе-	Участие в мероприятиях патриотической направленности, в проведении военно-спортивных игр; участие в программах антикоррупционной

ционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	режного отношения к культурному наследию и традициям многонационального народа Российской Федерации; нетерпимости к коррупционным Проявлениям.	направленности
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.	Формирование бережного отношения к природе и окружающей среде.	Экспертное наблюдение демонстрации навыков соблюдения правил экологической безопасности в ведении профессиональной деятельности; формирование навыков эффективных действий в чрезвычайных ситуациях
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Формирование бережного отношения к здоровью.	Участие в спортивных мероприятиях, проводимых образовательным учреждением; ведение здорового образа жизни.
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	Демонстрация умения составлять тексты документов, относящихся к профессиональной деятельности, на государственном и иностранном языках	Экспертная оценка соблюдения правил составления документов

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине

МДК.01.01 Компьютерные сети

программы подготовки специалистов среднего звена
09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2026

Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации по МДК.01.01 Компьютерные сети разработан в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование, утверждённого приказом Минобрнауки РФ от 10.07.2023 г. № 619, примерной образовательной программой.

Разработчик: Д.И. Головин, преподаватель КСД ВВГУ

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 9 от « 18 » 05 2026 г.

Председатель ЦМК _____ *Е.А. Стефанович*

1 Общие положения

Фонд оценочных средств (далее – ФОС) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины 09.02.01 Основы проектирования цифровой техники.

ФОС включают в себя контрольные материалы для проведения текущего контроля успеваемости в виде устного собеседования или теста и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачета (с использованием оценочного средства - опрос в форме ответов на тест).

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК	Код результата обучения	Наименование результата обучения
ПК1.1- ПК.1.7 ОК1- ОК9	У1	Проектировать локальную сеть, выбирать сетевые топологии
	У2	Использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети
	З1	Общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям
	З2	Архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры
	З3	Базовые протоколы и технологии локальных сетей
	З4	Принципы построения высокоскоростных локальных сетей
	З5	Стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы.

3 Соответствие оценочных средств контролируемым результатам обучения
3.1 Средства, применяемые для оценки уровня теоретической подготовки

Краткое наименование раздела (МДК), темы, параграфа дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
Тема 1.1 Введение в сетевые технологии: - компьютерные сети; - сетевые протоколы и коммуникации; - сетевой доступ; - сетевые технологии Ethernet; - сетевой уровень; - IP-адресация; - разделение IP-сетей на подсети; - транспортный уровень; - уровень приложений.	**З1**	Способность использовать знания общих принципов построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям при создании и эксплуатации компьютерных сетей	*Устный опрос (п. 5.1, вопросы 1.1 – 1.200)* *Реферат (п. 5.2)*	*Тесты 1* *Билеты на экзамен*
	З2	Способность использовать знания архитектуры протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры при создании и эксплуатации компьютерных сетей		
	З3	Способность использовать знания базовых протоколов и технологий локальных сетей при создании и эксплуатации компьютерных сетей		
	З4	Способность использовать знания принципов построения высокоскоростных локальных сетей при создании и эксплуатации компьютерных сетей		
	З5	Способность использовать знания стандартов кабелей, основных видов коммуникационных устройств, терминов, понятий, стандартов и типовых		

	У1	элементов структурированной кабельной системы при создании и эксплуатации компьютерных сетей Способность использовать умения проектирования локальной сети, выбора сетевой топологии		
	У2	Способность использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети при эксплуатации компьютерных сетей.		
Тема 2 Принципы маршрутизации и коммутации: - введение в коммутируемые сети; - основные концепции и настройки коммутации; - виртуальные локальные сети (VLAN); - концепции маршрутизации; - маршрутизация между VLAN; - статическая маршрутизация; - динамическая маршрутизация; - протокол DHCP; - преобразование сетевых адресов IPv4; - создание и настройка небольшой компьютерной сети.	**З1**	Способность использовать знания общих принципов построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям при создании и эксплуатации компьютерных сетей	*Устный опрос (п. 5.1, вопросы 2.1-2.210)* *Реферат (п. 5.2)*	*Тест 2* *Билеты на экзамен*
	З2	Способность использовать знания архитектуры протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры при создании и эксплуатации компьютерных сетей		
	З3	Способность использовать знания базовых протоколов и технологий локальных сетей при создании и эксплуатации компьютерных сетей		
	З4	Способность использовать знания принципов построения высокоскоростных локальных сетей при создании и эксплуатации компьютерных сетей		

	З5	Способность использовать знания стандартов кабелей, основных видов коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы при создании и эксплуатации компьютерных сетей		
	У1	Способность использовать умения проектирования локальной сети, выбора сетевой топологии		
	У2	Способность использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети при эксплуатации компьютерных сетей.		

3.2 Средства, применяемые для оценки уровня практической подготовки

Краткое наименование раздела (МДК), темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	
Тема 1 Введение в сетевые технологии *Практическая работа 1.1.1* Разделение сети на подсети	**З1**	Способность использовать знания общих принципов построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям при создании и эксплуатации компьютерных сетей	*Защита практической работы 1.1.1;*	*Тест 1* *Билеты на экзамен*

	З2	Способность использовать знания архитектуры протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры при создании и эксплуатации компьютерных сетей		
Тема 2 Принципы маршрутизации и коммутации *Практическая работа 1.2.1* Настройка коммутатора: - базовая настройка коммутатора; - Настройка параметров безопасности коммутатора. *Практическая работа 1.2.2* Конфигурация сетей VLAN: - конфигурация сетей VLAN и транковых каналов; - поиск и устранение неполадок в конфигурации VLAN; - реализация системы безопасности сети VLAN; - реализация сетей и VLAN для сегментации сетей предприятий малого и среднего бизнеса. *Практическая работа 1.2.3* Настройка маршрутизатора: - использование команды traceroute для обнаружения сети; - документирование сети; - настройка интерфейсов IPV4 и IPv6; - настройка и проверка небольшой сети; - исследование маршрутов с прямым	**З1**	Способность использовать знания общих принципов построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям при создании и эксплуатации компьютерных сетей	*Защита практических работ 1.2.1;* *Защита практических работ 1.2.2;* *Защита практических работ 1.2.3;* *Защита практических работ 1.2.4;* *Защита практических работ 1.2.5;* *Защита практических работ 1.2.6;* *Защита практических работ 1.2.7;*	*Тест 2 (п. 6.2)* *Билеты на экзамен*
	З2	Способность использовать знания архитектуры протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры при создании и эксплуатации компьютерных сетей		
	З3	Способность использовать знания базовых протоколов и технологий локальных сетей при создании и эксплуатации компьютерных сетей		
	З4	Способность использовать знания принципов построения высокоскоростных локальных сетей при создании и эксплуатации компьютерных сетей		
	З5	Способность использовать знания стандартов кабелей, основных видов коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы		

подключением. *Практическая работа 1.2.4* Маршрутизация между VLAN: - настройка маршрутизации между VLAN для каждого интерфейса; - настройка маршрутизации между VLAN на основе стандарта 802.1Q и транкового канала; - поиск и устранение неполадок в маршрутизации между сетями VLAN. *Практическая работа 1.2.5* Статическая маршрутизация: - настройка статических маршрутов IPv4/IPv6 по умолчанию; - разработка и реализация схемы адресации IPv4 с использованием VLSM; - расчет суммарных маршрутов IPv4 и IPv6; - поиск и устранение неполадок статических маршрутов IPv4 и IPv6. *Практическая работа 1.2.6* Преобразование сетевых адресов: - изучение принципа работы NAT; - настройка статического и динамического NAT; - реализация статического и динамического NAT; - настройка переадресации портов на маршрутизаторе; - проверка, поиск и устранение неполадок конфигурация NAT. *Практическая работа 1.3.7* Отработка комплексных практических навыков.		при создании и эксплуатации компьютерных сетей		
	У1	Способность использовать умения проектирования локальной сети, выбора сетевой топологии		
	У2	Способность использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети при эксплуатации компьютерных сетей.		

4 Описание процедуры оценивания

Результаты обучения по учебной дисциплине, уровень сформированности компетенций оцениваются по четырёх бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по профессиональному модулю проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками при проведении практических работ, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой профессиональному модулю).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по учебной дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом. Оценка на зачете выставляется с учетом оценок, полученных при прохождении текущей аттестации.

Критерии оценивания устного ответа

Оценочные средства: собеседование, устное сообщение, семинар.

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

Оценочные средства: реферат, конспект, контрольная работа, письменный отчет по лабораторной работе, доклад (сообщение), в том числе выполненный в форме презентации.

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полно-

стью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

Оценка	*Отлично*	*Хорошо*	*Удовлетворительно*	*Неудовлетворительно*
Количество правильных ответов	91 % и ≥	от 81% до 90,9 %	не менее 60%	менее 60%

Критерии выставления оценки студенту на зачете

Оценочные средства: устный опрос в форме ответов на контрольные вопросы, устный опрос в форме собеседования, выполнение реферата.

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и

	умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для собеседования (устного опроса):

Раздел 1 Введение в сетевые технологии

Тема 1.1 Компьютерные сети

1.1 Что такое Интернет с точки зрения устройства с использованием основных аппаратных и программных компонентов, из которых он состоит?
1.2 Что такое Интернет на языке сетевой инфраструктуры, предоставляющей службы для распределенных приложений?
1.3 Что такое служба?
1.4 Дайте развернутое объяснение понятию «протокол».
1.5 Приведите любой вариант классификации компьютерной сетей.
1.6 Объясните различие LAN и WAN с точки зрения собственника каналов связи.
1.7 Какие модели сетевого взаимодействия Вы знаете?
1.8 Что относится к промежуточным сетевым устройствам?
1.9 Перечислите технологии интернет-подключения для дома и небольшого офиса.
1.10 Перечислите технологии интернет-подключения для предприятий.
1.11 Объясните понятие «конвергентные сети».
1.12 Перечислите показатели качества компьютерной сети.
1.13 В чем заключается отличие между понятиями «расширение» и «масштабирование»?
1.14 В чем смысл понятия «качество обслуживания»?
1.15 Охарактеризуйте три основных требования для достижения безопасности сети.
1.16 Назовите и охарактеризуйте этапы развития компьютерных сетей и Интернета.

Тема 1.2 Сетевые протоколы и коммуникации

1.17 Что такое протокол?
1.18 Объясните требования к сетевым компьютерным протоколам.
1.19 Объясните понятия «форматирование и инкапсуляция сообщений».
1.20 Перечислите набор основных протоколов стека TCP/IP.
1.21 Будьте готовы кратко охарактеризовать любой протокол из стека TCP/IP.

1.22 На примере протокола HTTP объясните процесс межсетевого взаимодействия между веб-браузером и веб-сервером.
1.23 Объясните понятие «открытые стандарты».
1.24 Какие стандарты Интернета Вы можете назвать?
1.25 За какие стандарты компьютерных сетей отвечает IEEE?
1.26 Что такое модель OSI?
1.27 Охарактеризуйте уровни модели OSI.
1.28 Что такое модель TCP/IP?
1.29 Охарактеризуйте уровни модели TCP/IP.
1.30 Сравните между собой модели TCP/IP и OSI.
1.31 Что такое сегментация сообщений?
1.32 Объясните понятие PDU.
1.33 Раскройте процессы инкапсуляции и деинкапсуляции при передаче сообщения.
1.34 Что такое адреса канального и сетевого уровней?
1.35 Объясните, как выполняется сетевой обмен между устройствами в одной сети.
1.36 Объясните, как выполняется сетевой обмен между устройствами в разных сетях.

Тема 1.3 Сетевой доступ
1.37 Какие типы подключений к сети существуют?
1.38 Расскажите про сетевые интерфейсные платы.
1.39 За что отвечает физический уровень?
1.40 Назовите и кратко охарактеризуйте средства подключения физического уровня.
1.41 Перечислите стандарты физического уровня.
1.42. Чем пропускная способность средства подключения отличается от производительности?
1.43 Дайте определение производительности сети.
1.44 Дайте определение пропускной способности сети.
1.45 Перечислите типы физических средств подключения.
1.46 Какие типы медных кабелей Вы знаете?
1.47 Охарактеризуйте коаксиальный кабель.
1.48 Охарактеризуйте кабель UTP.
1.49 Охарактеризуйте кабель STP.
1.50 Конструкция оптоволоконного кабеля.
1.51 Типы оптоволоконных кабелей.
1.52 Что такое многомодовый оптоволоконный кабель?
1.53 Что такое одномодовый оптоволоконный кабель?
1.54 Перечислите свойства беспроводной среды передачи данных.
1.55 Охарактеризуйте типы средств беспроводного подключения.
1.56 Назовите функции канального уровня.
1.57 Какие подуровни канального уровня Вы можете назвать, их назначение?
1.58 Как осуществляется управление доступом к среде передачи?
1.59 Назовите стандарты канального уровня.
1.60 Как Вы понимаете понятия «физическая и логическая топология»?
1.61 Охарактеризуйте распространенные физические топологии WAN.
1.62 Охарактеризуйте физические топологии LAN.
1.63 Какие режимы передачи с точки зрения направлений передачи Вы знаете?
1.64 Охарактеризуйте методы управления доступом к среде?
1.65 Как функционирует маркерный метод доступа к среде?
1.66 Как функционирует метод доступа CSMA/CD?
1.67 Как функционирует метод доступа CSMA/CA?
1.69 Какой формат кадра Ethernet?

1.70 Расскажите про кадры канального уровня сетей LAN и WAN.
1.71 Какие адреса используются на канальном уровне?

Тема 1.4. Сетевые технологии Ethernet
1.72 Что такое инкапсуляция Ethernet?
1.73 Охарактеризуйте подуровень LLC технологии Ethernet.
1.74 Какие задачи выполняет подуровень MAC технологии Ethernet?
1.75 Назовите функции инкапсуляции данных подуровня MAC технологии Ethernet.
1.76 Как выполняется управление доступом к среде в технологии Ethernet?
1.77 Перечислите этапы развития технологии Ethernet.
1.78 Охарактеризуйте поля кадра Ethernet.
1.79 Что представляет структура MAC-адреса?
1.80 Как выполняется обработка кадра Ethernet?
1.81 Охарактеризуйте индивидуальный MAC-адрес Ethernet.
1.82 Охарактеризуйте MAC-адрес широковещательной рассылки.
1.83 Охарактеризуйте MAC-адрес многоадресной рассылки.
1.84 Что такое таблица адресов (коммутации) коммутатора?
1.85 Какие задачи решает коммутатор 2-го уровня в технологии Ethernet?
1.86 Как самообучается коммутатор 2-го уровня?
1.87 Как коммутатор 2-го уровня продвигает кадры?
1.88 Как коммутатор 2-го уровня осуществляет фильтрацию трафика?
1.89 Охарактеризуйте три способа пересылки кадров коммутаторами 2-го уровня.
1.90 Как реализуется в коммутаторах подключение независимо от типа кабеля UTP?
1.91 Какой выполняется преобразование IP-адресов пакета в MAC-адреса кадра?
1.92 Объясните алгоритм работы протокола ARP.
1.93 Опишите процесс продвижения пакета между узлами в одной сети.
1.94 Опишите процесс продвижения пакета между узлами в разных сетях.
1.95 Что такое спуфинг с помощью протокола разрешения ARP?

Тема 1.5. Сетевой уровень
1.96 Перечислите и охарактеризуйте функции сетевого уровня при передаче данных.
1.97 Какие протоколы сетевого уровня существуют?
1.98 Как выполняет инкапсуляцию протокол IP?
1.99 Назовите и охарактеризуйте три основные характеристики протокола IP.
1.100 Какие поля есть в заголовке IPv4-пакета, их назначение?
1.101 Назовите три основных ограничения IPv4.
1.102 Какие улучшения предлагает IPv6?
1.103 Охарактеризуйте инкапсуляцию IPv6.
1.104 Какие поля есть в заголовке IPv6-пакета, их назначение?
1.105 Как хостом принимается решение о переадресации пакетов?
1.106 Зачем нужна маска сети?
1.107 Что такое шлюз по умолчанию?
1.109 Что такое таблица маршрутизации?
1.110 Какие маршруты хранятся в таблице маршрутизации маршрутизатора?
1.111 Охарактеризуйте записи таблицы маршрутизации удаленной сети.
1.112 Что понимается под адресом следующего перехода?
1.113 Какие базовые компоненты необходимы маршрутизатору?
1.114 Какие типы памяти и для чего используются в маршрутизаторе?
1.114 Какие разъемы используются для подключения к маршрутизатору?
1.115 Какие способы доступа к командной строке (CLI) существуют?
1.116 Перечислите интерфейсы подключения к маршрутизатору.

1.117 Опишите процесс загрузки маршрутизатора.
1.118 Перечислите этапы базовой настройки коммутатора.
1.119 Перечислите этапы базовой настройки маршрутизатора.
1.120 Опишите процесс настройки интерфейса маршрутизатора.
1.121 Какие команды можно использовать для проверки конфигурации интерфейса?
1.122 Как настроить шлюз по умолчанию маршрутизатора?
1.123 Зачем нужен шлюз по умолчанию для коммутатора и как его настроить?

Тема 1.6. IP-адресация
1.124 Что из себя представляет десятично-точечная запись IPv4–адреса?
1.125 Как быстро преобразовать двоичную форму октета в десятичную и наоборот?
1.126 Из каких двух частей состоит IPv4-адрес?
1.127 Объясните назначение маски подсети.
1.128 Что такое префикс в IP-адресе и как изображается его длина?
1.129 Что такое классовая IPv4 адресация?
1.130 Что такое бесклассовая IPv4 адресация?
1.131 Расскажите про технологию VLSM.
1.132 Расскажите про технологию CIDR.
1.133 Какие диапазоны относятся к приватным IP-адресам?
1.134 Перечислите и охарактеризуйте IPv4-адреса специального назначения.
1.135 Какие организации назначают IP-адреса?
1.136 Зачем понадобилась IPv6-адресация?
1.137 Перечислите и охарактеризуйте методы перехода на протокол IPv6.
1.138 Изобразите предпочтительный формат IPv6-ажресов.
1.138 Изобразите пропуск начальных нулей в IPv6 адресах.
1.139 Как пропустить все нулевые сегменты IPv6-адреса.
1.140 Перечислите три типа IPv6-адресов.
1.141 Чему равна длина префикса IPv6-адреса.
1.142 Расскажите про индивидуальные IPv6-адреса
1.143 Объясните, как используются локальные индивидуальные IPv6-адреса канала?
1.144 Объясните структуру глобального индивидуального IPv6-адреса.
1.145 Чему равен префикс глобальной маршрутизации IPv6?
1.146 Что такое идентификатор подсети и идентификатор интерфейса в IPv6-адресах?
1.147 Как статически сконфигурировать глобальный индивидуальный IPv6?
1.148 Что такое динамическая конфигурация SLAAC?
1.149 Как работает динамическая конфигурация DHCPv6?
1.150 Объясните, как работает процесс EUI-64.
1.151 Как создаются динамические локальные адреса канала?
1.152 Как создаются статические локальные адреса канала?
1.153 Как проверить конфигурацию IPv6-адреса?
1.154 Перечислите групповые IPv6-адреса.
1.155 Сравните сообщения ICMPv4 и ICMPv6.
1.156 Как выполнить команду Ping?

Тема 1.7. Разделение IP-сетей на подсети
1.157 Что такое домен широковещательной рассылки?
1.158 Какие существуют проблемы с крупными широковещательными доменами?
1.159 Назовите причины для разделения сети на подсети.
1.160 Как разделить сеть на подсети на границе октетов?
1.161 Как разделить на подсети с бесклассовой адресацией?

1.162 Объясните использование маски подсети.
1.163 Выполните разделение на подсети с бесклассовой адресацией предложенной сети.
1.164 Объяснить работу VLSM.
1.165 Объяснить работу CIDR.
1.166 Объясните разделение IPv6-сети на подсети.

Тема 1.8. Транспортный уровень
1.167 Объясните роль транспортного уровня.
1.168 Назовите пять функций транспортного уровня.
1.169 Сравните протоколы TCP и UDP.
1.170 Как выполняется функция мультиплексирования с помощью номера порта?
1.171 Как обеспечивается надежность сеанса связи?
1.172 Как осуществляется упорядоченная доставка пакетов?
1.173 Как выполняется управление потоком передачи данных с помощью окна?
1.174 Как выполняется установка и разрыв соединения в протоколе TCP?
1.175 Перечислите поля заголовка TCP.
1.176 Перечислите поля заголовка UDP.
1.177 Что такое номера портов?
1.178 Назовите группы номеров портов.
1.179 Как функционирует пара сокетов?
1.180 Как работает команда netstat?
1.181 Как выполняется сборка датаграмм UDP?
1.182 Приведите примеры приложений, использующих TCP.
1.183 Приведите примеры приложений, использующих UDP.

Тема 1.9. Уровень приложений
1.184 Какие уровни модели OSI включены в уровень приложений стека TCP/IP?
1.185 Приведите примеры протоколов уровня приложения.
1.186 Объясните работу уровня представлений и сеансового уровня.
1.187 Объясните работу модели «клиент-сервер»
1.188 Объясните работу одноранговой сети.
1.189 Объясните работу P2P приложений.
1.190 Перечислите наиболее распространенные P2P приложения.
1.191 Объявите работу протокола HTTP и языка HTML.
1.192 Сравните протоколы HTTP и HTTPS.
1.193 Как работают протоколы электронной почты?
1.194 Объясните принцип работы протокола POP.
1.195 Объясните принцип функционирования DNS.
1.196 Объясните иерархию DNS.
1.197 Как работает команда nslookup?
1.198 Зачем нужен протокол DHCP?
1.199 Объясните работу протоколов FTP и TFTP.
1.200 Объясните работу протокола SMB.

Раздел 2. Принципы маршрутизации и коммутации

Тема 2.1 Введение в коммутируемые сети
2.1 Объясните понятие «конвергентные сети».
2.2 Перечислите функции объединенной сети.
2.3 Назовите принципы построения больших конвергентных сетей.
2.4 Нарисуйте структуру трехуровневой иерархии коммутируемой сети

2.5 Нарисуйте структуру коммутируемой сети с вырожденным ядром.
2.6 Перечислите функции уровня доступа коммутируемой сети.
2.7 Перечислите функции уровня распределения коммутируемой сети.
2.8 Перечислите функции уровня ядра коммутируемой сети.
2.9 Какие функции и параметры предоставляют коммутаторы с фиксированной коммутацией?
2.10 Какие функции и параметры предоставляют модульные коммутаторы?
2.11 Какие функции и параметры предоставляют стекируемые коммутаторы?
2.12 Опишите, как выполняется обучение коммутатора?
2.13 Опишите, как выполняется пересылка кадров на коммутаторе.
2.13 Опишите, как выполняется фильтрация кадров коммутатором?
2.14 Как выполняется коммутация Store-and-forward?
2.14 Как выполняется коммутация Cut-Through?
2.16 Как выполняется коммутация Fragment-free?
2.17 Объясните, что такое домен коллизий
2.18 Объясните, что такое широковещательный домен.
2.19 Как снизить перегрузку сети?

Тема 2.2 Основные концепции и настройки коммутации
2.20 Перечислите стадии загрузки коммутатора.
2.21 Как работает начальный загрузчик коммутатора?
2.22 Объясните процесс настройки переменной среды BOOT.
2.23 Перечислите шаги восстановления коммутатора после системного сбоя.
2.24 Перечислите и объясните работу светодиодных индикаторов коммутатора.
2.25 Как выполнить подготовку к удаленному управлению коммутатором?
2.26 Объясните процесс настройки интерфейса управления коммутатором.
2.27 Объясните процесс настройки портов коммутатора.
2.28 Как настроить дуплексный режим и скорость портов коммутатора?
2.29 Объясните смысл и процесс настройки функции Auto-MDIX.
2.30 Как проверить настройки порта коммутатора?
2.31 Назовите неполадки коммутатора на уровне сетевого доступа.
2.32 Перечислите шаги устранения неполадок коммутатора на уровне сетевого доступа.
2.33 Как настроить защищенный удаленный доступ к коммутатору?
2.34 Перечислите шаги настройки протокола SSH.
2.35 Как проверить работу SSH?
2.36 Назовите способы защиты неиспользуемых портов коммутатора.
2.37 Охарактеризуйте три вида защиты MAC-адресов.
2.38 Охарактеризуйте три функции безопасности портов коммутатора.

Тема 2.3 Виртуальные локальные сети (VLAN)
2.39 Что такое VLAN?
2.40 Перечислите основные преимущества VLAN.
2.41 Назовите и охарактеризуйте типы VLAN.
2.42 Назовите характеристики голосовых сетей VLAN.
2.43 Что такое транки виртуальных сетей?
2.44 Сравните широковещательные домены сетей с VLAN и сетей без VLAN.
2.45 Объясните тегирование кадров Ethernet для идентификации сети VLAN.
2.46 Что из себя представляет поле тега VLAN?
2.47 Что такое тегированные кадры в сети native VLAN?
2.48 Что такое нетегированные кадры в сети native VLAN?
2.49 Расскажите про тегирование голосовой VLAN.

2.50 Опишите пример конфигурации с голосовой VLAN.
2.51 Что такое VLAN стандартного диапазона?
2.52 Что такое сети VLAN расширенного диапазона?
2.53 Опишите процесс создания сети VLAN.
2.54 Как назначить порты сетям VLAN?
2.55 Как выполнить изменение принадлежности портов сети VLAN?
2.56 Как удалить VLAN?
2.57 Выполните проверку информации о сети VLAN.
2.58 Как настроить транковые каналы IEEE 802.1Q?
2.59 Как проверит конфигурацию магистрального канала?
2.60 Назовите возможные проблемы с IP-адресацией сетей VLAN.
2.61 Назовите возможные неполадки и проблемы в транковых каналах.
2.62 Как влияет неверный режим порта?

Тема 2.4 Концепции маршрутизации
2.63 Перечислите ключевые структуры и свойства, связанные с производительностью сети
2.64 Обоснуйте необходимость маршрутизации.
2.65 Сравните архитектуру компьютера и маршрутизатора.
2.66 Назовите функции маршрутизатора.
2.67 Перечислите и охарактеризуйте механизмы пересылки пакетов.
2.68 Как маршрутизаторы и коммутаторы подключаются к сети?
2.69 Как настраивается шлюз по умолчанию?
2.70 Приведите пример документирования сетевой адресации.
2.71 Как выполняется активация IP-адресации на узле?
2.72 Объясните работу светодиодных индикаторов на маршрутизаторе.
2.73 Расскажите, как настроить консольный доступ
2.74 Как выполняется активация IP-адресации на коммутаторе?
2.75 Перечислите этапы настройки основных параметров маршрутизатора.
2.76 Как настроить консольный доступ маршрутизатора?
2.77 Приведите пример настройки основных параметров маршрутизатора.
2.78 Объясните, как настроить параметры IPv4 на интерфейсе маршрутизатора.
2.79 Объясните, как настроить параметры IPv6 на интерфейсе маршрутизатора.
2.80 Объясните, как настроить интерфейс loopback для IPv4.
2.81 Объясните, как проверить настройки интерфейса маршрутизатора.
2.82 Объясните, как проверить настройки IPv6 на интерфейсе маршрутизатора.
2.83 Объясните, как организовать фильтрацию выходных данных команды show.
2.84 Расскажите про функции истории команд.
2.85 Перечислите этапы коммутации в маршрутизаторе.
2.86 Перечислите и охарактеризуйте этапы отправки пакетов маршрутизатором.
2.87 Перечислите и охарактеризуйте этапы определения пути маршрутизатором.
2.88 Объясните, как выполняется балансировка нагрузки.
2.89 Что такое административное расстояние.
2.90 Объясните, как выполняется анализ таблицы маршрутизации.
2.91 Какие источники таблицы маршрутизации Вы можете назвать?
2.92 Охарактеризуйте записи маршрутизации удаленной сети.
2.93 Объясните определения интерфейсов с прямым подключением.
2.94 Объясните записи таблицы маршрутизации с прямым подключением.
2.95 Объясните, как настроить статический маршрут IPv4.
2.96 Объясните, как настроить статический маршрут IPv6.
2.97 Что такое динамическая маршрутизация?
2.98 Назовите известные Вам протоколы IPv4.

2.99 Назовите известные Вам протоколы IPv6.

Тема 2.5 Маршрутизация между VLAN
2.100 Объясните, что такое маршрутизация между VLAN.
2.101 Опишите устаревшие методы маршрутизации между VLAN.
2.102 Опишите маршрутизацию между сетями VLAN методом router-on-a-stick.
2.103 Опишите настройку маршрутизации между VLAN устаревшим методом.
2.104 Опишите настройку коммутатора устаревшим методом маршрутизации между VLAN.
2.105 Опишите настройку маршрутизатора устаревшим методом маршрутизации между VLAN.
2.106 Опишите настройку конфигурации router-on-a-stick.
2.107 Опишите настройку коммутатора при маршрутизации методом router-on-a-stick.
2.108 Опишите настройку подынтерфейса при маршрутизации методом router-on-a-stick.
2.109 Опишите проверку подынтерфейса при маршрутизации методом router-on-a-stick.
2.110 Опишите настройку и маршрутизации методом router-on-a-stick.

Тема 2.6 Статическая маршрутизация
2.111 Объясните, что такое статическая маршрутизация.
2.112 Объясните, что такое динамическая маршрутизация.
2.113 Сравните статическую и динамическую маршрутизацию.
2.114 Опишите и охарактеризуйте задачи статической маршрутизации.
1.115 Перечислите типы статических маршрутов IPv4 и IPv6.
1.116 Опишите стандартный статический маршрут.
1.117 Опишите статический маршрут по умолчанию.
1.118 Опишите объединенный статический маршрут.
1.119 Опишите плавающий статический маршрут.
1.120 Опишите порядок настройки статического маршрута IPv4.
1.121 Опишите порядок настройки полностью заданного статического маршрута.
1.122 Перечислите команды проверки статического маршрута.
1.123 Опишите порядок настройки статического маршрута по умолчанию.
1.124 Опишите порядок настройки статического маршрута IPv6.
1.125 Назовите параметры следующего перехода статического маршрута IPv6.
1.126 Опишите настройку статического маршрута IPv6 следующего перехода.
1.127 Опишите настройку напрямую подключенного статического маршрута IPv6.
1.128 Опишите настройку полностью заданного статического маршрута IPv6.
1.129 Перечислите команды проверки статических маршрутов IPv6.
1.130 Опишите порядок настройки статического маршрута IPv6 по умолчанию.
1.131 Опишите порядок настройки плавающих статических маршрутов.
1.132 Опишите порядок настройки статических маршрутов хостов.

Тема 2.7 Динамическая маршрутизация
1.132 Приведите хронологию внедрения различных динамических протоколов.
1.133 Назовите компоненты протоколов динамической маршрутизации
1.134 Сравните динамическую маршрутизацию со статической.
1.135 Опишите настройку протокола RIP на маршрутизаторе.
1.136 Опишите проверку протокола RIP на маршрутизаторе.
1.137 Как включить и отключить автоматическое суммирование в протоколе RIP?
1.138 Как настроить пассивные интерфейсы?
1.139 Опишите распространение маршрута по умолчанию в протоколе RIP.
1.140 Объясните записи таблицы маршрутизации.

1.141 Опишите критерии обсуждения маршрутов.
1.142 Что такое окончательный маршрут?
1.143 Что такое маршрут 1-го уровня?
1.144 Что такое родительский маршрут 1-го уровня?
1.145 Что такое дочерний маршрут 2-го уровня?
1.146 Опишите процесс поиска маршрута IPv4.
1.147 Объясните фразу «Оптимальный маршрут = самое длинное совпадение».
1.148 Опишите анализ записей таблицы маршрутизации IPv6.
1.149 Опишите записи с прямым подключением IPv6.
1.150 Опишите записи удаленной сети IPv6.

Тема 2.8 Протокол DHCP
1.151 Опишите назначение протокола DHCP.
1.152 Перечислите операции DHCP.
1.153 Опишите шаги первоначальной аренды адреса.
1.154 Опишите шаги продления аренды адреса
1.155 Опишите формат сообщений DHCPv4.
1.156 Опишите сообщения обнаружения и предложения DHCPv4.
1.157 Опишите шаги настройки базового DHCPv4-сервера.
1.158 Опишите процесс проверки DHCPv4.
1.159 Как осуществляется DHCPv4-ретрансляция?
1.160 Опишите настройку маршрутизатора в качестве DHCPv4-клиента.
1.161 Как проверить настройки DHCPv4 на маршрутизаторе?
1.162 Опишите процесс настройки SLAAC.
1.163 Опишите процесс настройки DHCPv6.
1.164 Что такое EUI-64?

Тема 2.9 Преобразование сетевых адресов
1.165 Назовите максимально возможное число публичных IPv4-адресов.
1.166 Где должны быть зарегистрированы публичные IPv4 адреса?
1.167 Назовите пространства частных IPv4 адресов.
1.168 Что такое NAT?
1.169 Перечислите и охарактеризуйте 4 типа адресов по терминологии NAT.
1.170 Опишите принцип работы NAT
1.171 Перечислите все типы механизмов преобразования сетевых адресов.
1.172 Что такое статическое преобразование NAT?
1.173 Что такое динамическое преобразование NAT?
.174 Что такое преобразование адресов портов?
175 Сравните NAT и PAT.
176 Перечислите преимущества преобразования NAT.
177 Перечислите недостатки преобразования NAT.
178 Опишите шаги настройки статического NAT.
179 Как проверить статический NAT?
180 Опишите шаги настройки динамического NAT.
181 Опишите анализ динамического NAT.
182 Как проверить динамический NAT?
183 Опишите шаги настройки PAT для пула общедоступных адресов.
184 Опишите шаги настройки PAT для одного публичного IPv4-адреса.
185 Опишите анализ PAT.
186. Как проверить PAT?

187 Что такое перенаправление портов?
188 Расскажите про NAT в IPv6.

Тема 2.10 Создание и настройка небольшой компьютерной сети
189 Какие факторы необходимо учитывать при выборе сетевых устройств?
190 Какие функции должно поддерживать сетевое устройство?
191 Какие типы устройств должны учитываться при проектировании схемы IP-адресации?
192 Как спланировать резервирование в компьютерной сети?
193 Какие приложения и протоколы должны быть в небольшой сети?
194 Какие элементы требуются для масштабирования сети?
195 Как обеспечить сетевую безопасность?
196 Как использовать команду Ping?
197 Как протестировать виртуальный интерфейс loopback?
198 Как использовать команды traceroute и tracert?
199 Как использовать команды show?
200 Как использовать команду ipconfig?
201 Зачем нужна команда arp?
202 Как использовать команду show cdp neighbors?
203 Как использовать команду show ip interface brief?
204 Как использовать команду debug?
205 Как использовать команду terminal monitor?
206 Перечислите шесть шагов поиска и устранения неполадок.
207 Что будет при несовпадении дуплексных режимов?
208 Какие могут быть проблемы с IP-адресами на устройствах?
209 Назовите неполадки, связанные со шлюзом по умолчанию.
210 Какие проблемы могут быть связаны с DNS?

5.2 Темы рефератов

1. Методы коммутации информации (данных) в сетях ЭВМ. Сравнительный анализ.

2. Межсетевые экраны - перспективное направление обеспечения безопасности информации в сетях ЭВМ.

3. Пути и способы реализации компьютерной IP-телефонии в сетях ЭВМ.

4. Направления развития аппаратно-программных методов и средств сетевого контроля и диагностики сетей ЭВМ.

5. Направления развития аппаратно-программных методов и средств сетевого контроля и диагностики локальных вычислительных сетей (ЛВС).

6. Коммутаторы в сетях ЭВМ. Сравнительный анализ и пути развития.

7. Маршрутизаторы в сетях ЭВМ. Сравнительный анализ и пути развития.

8. АТМ - технология. Сравнительный анализ. Способы и средства реализации. Области рационального применения.

9. Глобальные и локальные сети ЭВМ. Сравнительный анализ. Способы интеграции и взаимодействия. Области использования.

10. Аппаратно-программные средства доступа в сети ЭВМ. Сравнительный анализ. Варианты построения и реализации, области применения.

11. Серверы в сетях ЭВМ. Типы, характеристики, области применения.

12. Сетевые протоколы в сетях ЭВМ. Сравнительный анализ. Тенденции развития. Средства реализации.

13. Средства и протоколы управления в сетях ЭВМ, Сравнительный анализ. Тенденции развития. Способы реализации.

14. Защита ЛВС и информации в ЛВС. Способы и средства защиты. Направления развития средств защиты.

15. Сетевые архитектуры ЛВС. Виды. Сравнительный анализ. Области применения.

16. Сетевые архитектуры систем передачи данных. Виды, сравнительный анализ. Тенденции развития.

17. Терминальные (абонентские) комплексы сетей ЭВМ. Сравнительный анализ. Способы построения. Тенденции развития.

18. Перспективные способы и средства приема и обработки сигналов в каналах передачи данных сетей ЭВМ. Сравнительный анализ. Тенденции развития.

19. Сети передачи данных интегрального обслуживания. Способы построения. Направления развития.

20. Каналы связи в сетях ЭВМ. Классификация. Сравнительный анализ. Типы, характеристики. Области применения. Направления развития.

21. Способы и средства защиты программных средств сетей ЭВМ. Сравнительный анализ. Направления развития.

22. Способы и средства защиты аппаратно-программных средств и информации управления сетями ЭВМ. Сравнительный анализ. Направления развития.

23. Способы и средства защиты аппаратно-программных средств обеспечения безопасности в сетях ЭВМ. Сравнительный анализ. Направления развития.

24. Способы и средства защиты баз данных в сетях ЭВМ. Сравнительный анализ. Направления развития.
25. Комплексные методы и средства защиты информации (крипто-имитозащита, защита от помех (ошибок)) в сетях ЭВМ. Сравнительный анализ. Рациональные решения.

26. Сети ЭВМ на основе оптоволоконной элементной базы. Способы и средства построения. Перспективы создания и развития.

27. Среды передачи данных в сети.

28. Витая пара и ее разновидности. Основные параметры.

29. Коаксиальный кабель как среда передачи данных в сети

30. Волоконно-оптический кабель (ВОК) как среда передачи данных в сети. Режимы работы ВОК.

31. Типы организации локальных сетей: одноранговые и клиент-серверные сети.

32. Кодирование информации в компьютерных сетях. Виды кодов.

33. Кластеризация компьютерных сетей.

34. Использование пакетов при обмене данными в сети. Структура пакета. Адресация пакетов.

35. Методы управления обменом информацией в сети: централизованный и децентрализованный.

36. Протоколы обмена данными в сети и их виды;

37. Уровни сетевой архитектуры (OSI).

38. Основные методы доступа в сети (Ethernet, Token Ring, ARCnet, FDDI) и их особенности

39. Технологии PON, APON, EPON, GPON в сетях на оптоволокне и их особенности.

40. Сеть Ethernet на толстом и тонком коаксиале. Основные характеристики.

41. Сеть FDDI. Основные характеристики.

42. Оптоволоконные мультисервисные сети FTTH, FTTB, FTTC и их особенности.

43. Технологии TDMA, FDMA, CDMA в беспроводных сетях.

44. Поколения беспроводных сетей 2G, 3G, 4G, 5G, 6G и их сравнение.

45. Технологии беспроводной связи GPRS, EDGE, EV-DO и их особенности.

46. Сети X.25 и их особенности.

47 Сети Frame Relay и их особенности

48. Применение ЛВС в системах видеонаблюдения и охраны.

49. Служба HelpDesk как средство повышения эффективности работы ЛВС.

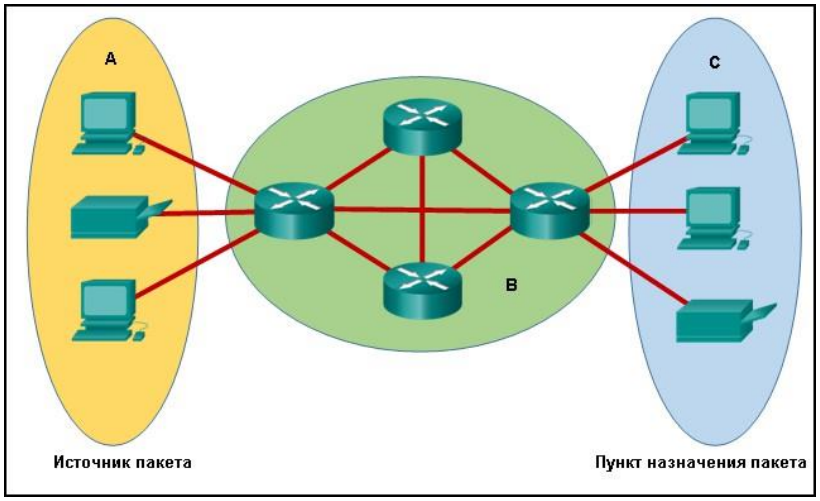
50. Применение компьютерных ГРИД-систем.

5.3 Примеры тестовых заданий

Тест 1 Введение в сетевые технологии

Количество вопросов – 115. Преподаватель формирует нужное количество вариантов теста с любым количеством вопросов.

№ п/п	Вопрос с вариантами ответов	Правильный ответ
1.	Назовите две характеристики масштабируемой сети (выберите два варианта). 1. быстрая перегрузка при увеличении трафика 2. наращивание размера без ущерба для имеющихся пользователей 3. не так надежна, как небольшая сеть 4. для нее подходят модульные устройства, допускающие расширение 5. предлагает ограниченное число приложений	2, 4
2.	Какие три устройства считаются оконечными устройствами в сети? (Выберите три варианта.) 1. Маршрутизатор 2. Коммутатор 3. телефон VoIP 4. камера видеонаблюдения 5. точка доступа 6. оконечное устройство системы TelePresence	3, 4, 6
3.	Какое из утверждений описывает одну из особенностей объединенной сети? 1. Единая сеть, которая обеспечивает передачу голоса, видео и данных на различные устройства. 2. Сетевые сервисы предоставляются с использованием разнообразных сетевых платформ. 3. Для каждого сетевого сервиса используются отдельные каналы связи. 4. В сети используются различные технологии для передачи голоса, видео и данных.	1
4.	Колледж строит новое общежитие на территории кампуса. Рабочие копают землю, чтобы проложить новый водопровод для общежития. Работник случайно повреждает оптоволоконный кабель, соединяющий два действующих общежития с центром обработки данных кампуса. Несмотря на то что кабель был перерезан, студенты не имели доступа к сетевым сервисам лишь очень короткий отрывок времени. О какой характеристики сети здесь идет речь? 1. качество обслуживания (QoS) 2. масштабируемость 3. безопасность	4

	4. отказоустойчивость 5. целостность	
5.	 Заполните пустое поле. Посмотрите на изображение. Это изображение представляет собой пример _____угрозы безопасности организации. (Одно прилагательное на русском языке).	внутренней
6.	 Посмотрите на рисунок. Какой термин правильно определяет тип устройства, приведенного в области B? 1. устройство-источник 2. конечное устройство 3. передающее устройство 4. промежуточное устройство	4
7.	Что такое ISP? 1. организация, занимающаяся разработкой стандартов в отношении кабелей и проводов при организации сетей 2. протокол, определяющий метод взаимодействия компьютеров в локальной сети 3. организация, предоставляющая возможность физическим лицам и предприятиям подключаться к сети Интернет 4. сетевое устройство, которое объединяет функциональность нескольких различных сетевых устройств в единую	3

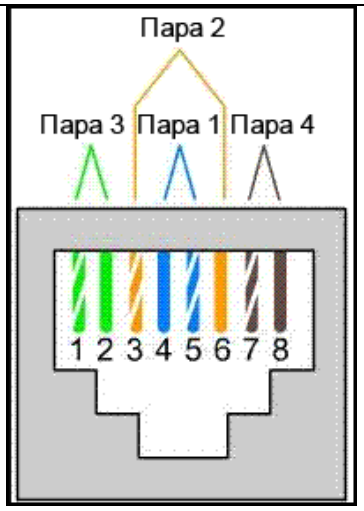
8.	Во время плановой проверки технический специалист обнаружил, что установленное на ПК программное обеспечение осуществляло тайный сбор данных об интернет-сайтах, посещаемых пользователями с данного компьютера. Какому типу угрозы подвергается данный компьютер? 1. DoS -атака 2. кража личной информации 3. шпионское ПО 4. атака нулевого дня	3
9.	Что такое глобальная сеть (WAN)? 1. сетевая инфраструктура, предназначенная для хранения, получения и репликации данных 2. сетевая инфраструктура, которая предоставляет доступ к другим сетям в обширной географической области 3. сетевая инфраструктура, охватывающая ограниченное физическое пространство, например, город 4. сетевая инфраструктура, которая предоставляет доступ к сети в небольшой географической области	2
10.	Заполните пустое поле. _____- это компонент операционного программного обеспечения, предоставляющий пользовательский интерфейс. (термин на русском языке)	Оболочка
11.	Для экономии времени команды операционной системы IOS можно вводить частично. Какая клавиша или комбинация клавиш завершит ввод? 1. Tab 2. Ctrl-P 3. Ctrl-N 4. Стрелка вверх 5. Стрелка вправо 6. Стрелка вниз	1
12.	Какая команда не позволит просмотреть все незашифрованные пароли, содержащиеся в конфигурационном файле в виде обычного текста? 1. (config)# **enable password secret** 2. (config)# **enable secret Secret_Password** 3. (config-line)# **password secret** 4. (config)# **service password-encryption** 5. (config)# **enable secret Encrypted_Password**	4
13.	Каких трех правил следует придерживаться при настройке имени узла через командную строку на устройствах Cisco? (Выберите три варианта.) 1. имя узла должно состоять меньше, чем из 64 символов 2. имя узла должно состоять только из строчных символов 3. имя узла не должно содержать пробелов 4. имя узла должно завершаться специальным символом 5. имя узла должно начинаться с буквы	1, 3, 5

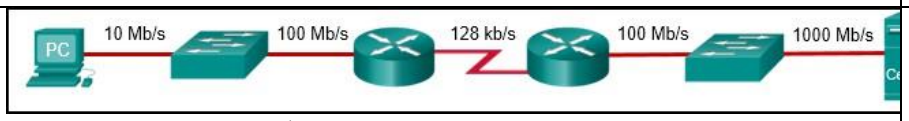
14.	Верно или неверно? Мобильным устройствам не нужны IP-адреса для обмена данными в Интернете. 1. Верно 2. Неверно	2
15.	Пароли можно использовать для ограничения доступа ко всей системе Cisco IOS или только к её частям. Выберите режимы и интерфейсы, для защиты которых можно использовать пароли. (Выберите три варианта ответа.) 1. интерфейс VTY 2. консольный интерфейс 3. интерфейс Ethernet 4. режим загрузки IOS 5. привилегированный режим EXEC 6. режим конфигурации маршрутизатора	1, 2, 5
16.	Чем протокол SSH отличается от протокола Telnet? 1. Протокол SSH позволяет осуществить подключение в пределах сети, тогда как протокол Telnet предназначен для создания доступа за ее пределами. 2. Протокол SSH обеспечивает безопасность удаленных сеансов посредством шифрования сообщений и аутентификации пользователей. Протокол Telnet отправляет сообщения в незашифрованном виде и считается небезопасным. 3. Для работы протокола SSH необходима программа эмуляции терминала PuTTY. Для подключения к устройствам посредством использования протокола Telnet необходима программа Tera Term. 4. Протокол SSH должен быть настроен на активное сетевое подключение, тогда как протокол Telnet используется для подключения к устройству с помощью консольного подключения.	2
17.	Какие два утверждения о пользовательском режиме EXEC верны? (Выберите два варианта.) 1. доступны все команды маршрутизатора 2. доступ к режиму глобального конфигурирования можно получить с помощью команды **enable** 3. командная строка устройства в этом режиме заканчивается символом «>» 4. в этом режиме можно настраивать интерфейсы и протоколы маршрутизатора 5. только некоторые аспекты конфигурации маршрутизатора доступны для просмотра в этом режиме	3, 5
18	Администратор только что изменил IP-адрес интерфейса на устройстве с операционной системой IOS. Что еще необходимо сделать, чтобы изменения вступили в силу на этом устройстве?	4

	1. Скопировать текущую копию файла конфигурации в файл загрузочной конфигурации. 2. Скопировать сведения из файла загрузочной конфигурации в текущую копию файла конфигурации. 3. Перезагрузить данное устройство и ввести yes, когда система предложит сохранить конфигурацию. 4. Никаких дополнительных действий не требуется. Изменения конфигурации на устройстве с операционной системой IOS вступят в силу сразу после корректного ввода данной команды и нажатия клавиши Enter.	
19.	Какое устройство выполняет роль шлюза, позволяя узлам отправлять трафик к удаленным IP-сетям? 1. сервер DNS 2. сервер DHCP 3. локальный маршрутизатор 4. локальный коммутатор	3
20.	Какие две функции предоставляются пользователям с помощью контекстной справки интерфейса командной строки (CLI) системы CISCO IOS? (Выберите два варианта ответа.) 1. выдача сообщения об ошибке при отправке неверной команды 2. отображение списка всех доступных команд в текущем режиме 3. предоставление пользователю возможности завершить частично введённую сокращённую команду с помощью клавиши TAB 4. определение варианта, ключевого слова или аргумента, доступного для введённой команды 5. выбор наиболее подходящей команды для выполнения задачи	2, 4
21.	Почему в отрасли связи так важны открытые стандарты? 1. Они необходимы устройствам для получения доступа к Интернету. 2. Они устраняют угрозу нарушения безопасности. 3. Они допускают взаимодействие между программным и аппаратным обеспечением от разных поставщиков. 4. Они стимулируют сетевые организации разрабатывать собственное программное обеспечение, чтобы сохранить конкурентоспособность.	4
22.	Какой вариант доставки сообщений используется в том случае, когда все устройства должны получить одно и то же сообщение одновременно? 1. дуплексная передача 2. одноадресная рассылка 3. многоадресная рассылка 4. широковещательная рассылка	4
23.	Если шлюз по умолчанию был неправильно сконфигурирован на узле, каким образом это влияет на передачу данных?	2

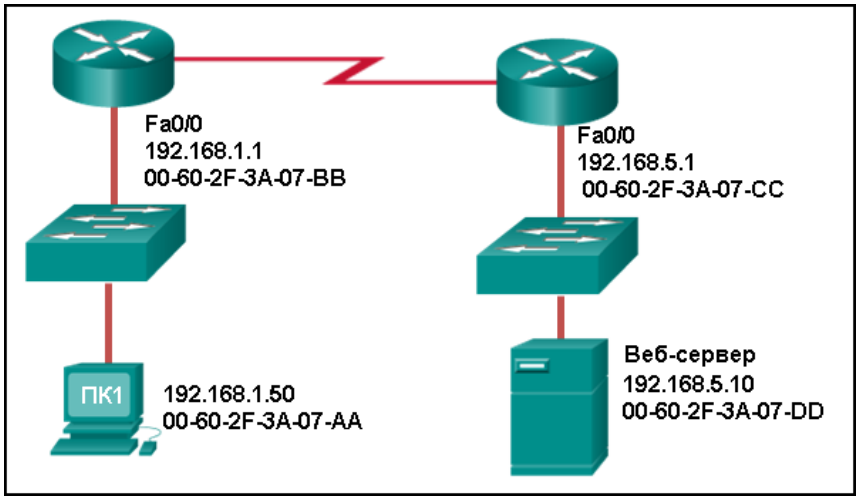
	1. Узел не может обмениваться данными в своей локальной сети. 2. Узел может обмениваться данными с другими узлами в своей локальной сети, но не может обмениваться данными с узлами в других сетях. 3. Узел может обмениваться данными с узлами в других сетях, но не может обмениваться данными с узлами в своей локальной сети. 4. Это никак не влияет на передачу данных.	
24	Какой из приведённых ниже адресов используется для доставки данных к удалённой сети? 1. MAC-адрес назначения 2. IP-адрес назначения 3. номер порта назначения 4. MAC-адрес источника 5. IP-адрес источника	2
25	Какие три требования определены протоколами, используемыми при сетевой передаче данных, для обеспечения передачи сообщений по сети? (Выберите три варианта.) 1. технические характеристики разъемов 2. кодирование сообщений 3. выбор среды передачи данных 4. размер сообщения 5. варианты доставки 6. установка оконечного устройства.	1, 4, 5
26	Заполните пустое поле. Если переместить ПК в другую сеть, его MAC-адрес не изменится, поскольку MAC-адрес зашит в (Два слова на русском языке) _____этого ПК.	сетевую плату, сетевую карту
27	Какой тип доставки используют адреса канального уровня? 1. удалённая доставка 2. локальная и удалённая доставка 3. локальная доставка 4. удалённая доставка с помощью маршрутизаторов	3
28	Какой уровень модели протокола TCP/IP определяет наилучший путь через сеть? 1. уровень приложений 2. транспортный 3. межсетевой 4. уровень доступа к сети	3
29	Каким общим термином описывают данные на любом уровне модели сети? 1. Кадр 2. Пакет 3. Блок данных протокола (protocol data unit) 4. Сегмент	3
30	Каково назначение протоколов в процессе передачи данных?	3

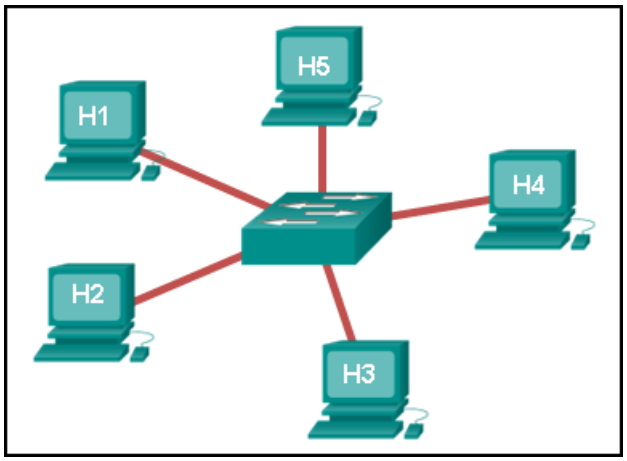
	1. определение пропускной способности конкретного канала или среды передачи данных для каждого отдельного типа связи 2. определение типа установленных на устройство операционных систем, которые будут поддерживать процесс обмена данными 3. обеспечение правил, необходимых для осуществления определенного типа обмена данными 4. определение содержимого сообщения, отправляемого во время передачи данных	
31	Какие три аббревиатуры означают организации по стандартизации? (Выберите три варианта.) 1. IANA 2. TCP/IP 3. IEEE 4. IETF 5. OSI 6. MAC	1, 3, 4
32	На каком из уровней модели OSI будет инкапсулирован физический адрес? 1. физический уровень 2. канальный уровень 3. сетевой уровень 4. транспортный уровень	2
33	Какой уровень модели OSI определяет сервисы сегментации и повторной сборки данных для отдельных сеансов передачи данных между оконечными устройствами? 1. уровень приложений 2. представления 3. сеансовый 4. транспортный 5. сетевой	4
34	Как называется рассылка сообщения определенной группе узлов? 1. статическая 2. одноадресная 3. динамическая 4. групповая 5. широковещательная	4
35	В чем состоит роль физического уровня OSI? 1. управление доступом к среде передачи данных 2. передача битов через локальную среду передачи данных 3. обнаружение ошибок в принятых кадрах 4. обмен кадрами между узлами по физической сетевой среде передачи данных	2
36	Какой метод передачи данных позволяет передавать и принимать информацию одновременно?	1

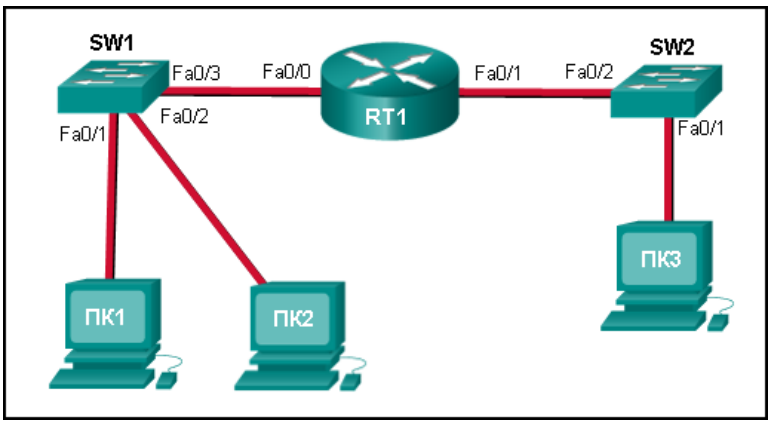
	1. полный дуплекс 2. полудуплекс 3. мультиплексирование 4. симплекс	
37	 Посмотрите на изображение. Один конец кабеля оконцован, как показано на рисунке, а другой оконцован в соответствии со стандартом T568A. Какой тип кабеля будет создан таким образом? 1. кроссовый 2. консольный 3. прямой 4. оптоволоконный	3
38	Какова характеристика топологии «звезда» глобальной вычислительной среды? 1. Она требует, чтобы некоторые узлы разветвления были взаимоподключены посредством соединения «точка-точка». 2. Она требует, чтобы все узлы были взаимоподключены посредством соединения «точка-точка». 3. Для всех узлов требуется наличие устройства-концентратора, подключённого к маршрутизатору. 4. Узлы разветвления подключены к центральному узлу посредством соединения «точка-точка».	4
39	Заполните пустое поле. В оптоволоконной среде сигналы представлены в качестве шаблонов_____сигналов.	световых, оптических
40	Сопоставьте каждый тип поля кадра с его функцией. (Не все варианты используются.) Это поле помогает направить кадр к месту назначения – адресация. Это поле проверяет кадр на наличие повреждений во время передачи - обнаружение ошибок. Это поле используется LLC для определения протокола уровня	

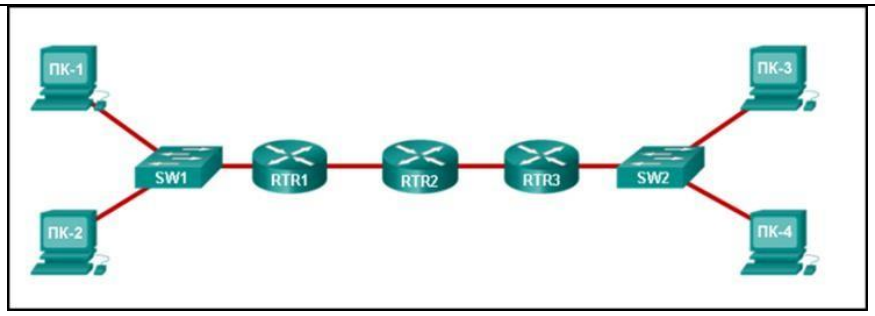
	3 – тип. Это поле определяет начало кадра – начало кадра. Это поле определяет специальные сервисы управления потоком.	
41	Сетевой администратор разрабатывает новую сетевую инфраструктуру, которая включает как проводные, так и беспроводные соединения. При каких условиях рекомендуется беспроводное соединение? 1. У пользовательского устройства есть только сетевая интерфейсная плата Ethernet. 2. Из-за требований к производительности пользовательскому устройству требуется отдельное подключение. 3. При подключении к сети пользовательскому устройству необходим мобильный доступ. 4. Область пользовательских устройств характерна большим количеством запросов на получение информации (RFI).	3
42	Какой тип кабеля используется для подключения последовательного порта рабочей станции к консольному порту маршрутизатора или коммутатора? 1. кроссовый 2. консольный 3. прямой 4. коаксиальный	2
43	 Посмотрите на изображение. Назовите максимально возможную пропускную способность между ПК и сервером. 1. 128 Кбит/с 2. 10 Мбит/с 3. 100 Мбит/с 4. 1000 Мбит/с	1
44	Сетевые специалисты сравнивают топологии для подключения в общей среде передачи данных. Какая физическая топология является примером гибридной топологии для локальной сети? 1. шина 2. расширенная звезда 3. кольцо 4. частично-ячеистая	2
45	Благодаря чему оптоволоконный кабель, в отличие от медного, лучше всего подходит для соединений между зданиями? (Выберите три варианта ответа.) 1. возможность прокладки кабеля на большие расстояния 2. более низкая стоимость установки 3. ограниченная восприимчивость к электромагнитным помехам или к радиопомехам 4. прочность соединений	1, 3, 5

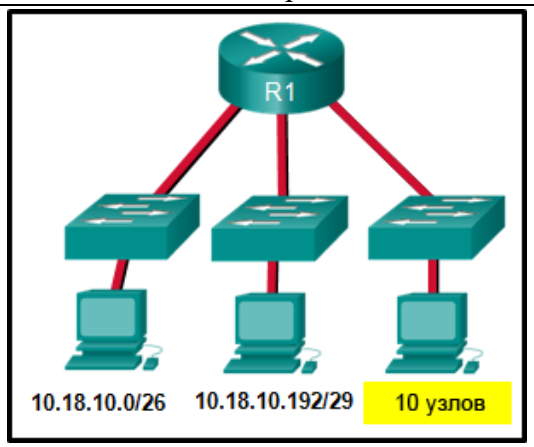
	5. больший потенциал пропускной способности 6. простота оконцевания	
46	Какой метод используется для управления ассоциативным доступом в беспроводной сети? 1. CSMA/CD 2. приоритетное упорядочение 3. CSMA/CA 4. Передача маркера	3
47	В чём заключается функция подуровня управления логическим соединением (LLC)? 1. определять процессы доступа к среде передачи, выполняемые аппаратным обеспечением 2. обеспечить функцию адресации канального уровня 3. определить тип используемого протокола сетевого уровня 4. принять сегменты и упаковать их в блоки данных, называемые пакетами	3
48	Какие два фактора оказывают влияние на способ, который используется для управления доступом к среде передачи данных? (Выберите два варианта ответа.) 1. то, как данные генерируются приложениями оконечных устройств 2. то, как канальный уровень воспринимает соединение между узлами 3. то, как сигналы кодируются сетевым адаптером на оконечных устройствах 4. то, как узлы совместно используют среду передачи данных 5. то, как IP-протокол пересылает пакет по адресу назначения	2, 4
49	Какое утверждение верно описывает кодирование кадров? 1. При кодировании кадров используется характеристика одной волны для изменения характеристики другой волны. 2. При кодировании кадров сигналы данных передаются вместе с тактовым сигналом, который издается через равные промежутки времени. 3. При кодировании кадров генерируются электрические, оптические и беспроводные сигналы, которые представляют двоичные числа кадра. 4. При кодировании кадров последовательности битов преобразуются в определённые коды, чтобы обеспечить их предсказуемость и отличить биты данных от битов управления.	4
50	Какое утверждение описывает свойство полей заголовка кадров канального уровня? 1. Все из них включают в себя поля управления потоками данных и поля логического соединения.	3

	2. Поля заголовка кадра Ethernet содержат адреса источника и назначения уровня 3. 3. Они могут различаться в зависимости от протоколов. 4. Они содержат сведения о пользовательских приложениях.	
51	Коммутатор уровня 2 используется для коммутации входящих кадров от порта 1000BASE-T к порту, подключённого к сети 100Base-T. Какой метод буферизации памяти наилучшим образом подходит для этой задачи? 1. буферизация на основе портов 2. буферизация кэша уровня 1 3. буферизация совместного доступа к памяти 4. буферизация фиксированной конфигурации	3
52	 Посмотрите на рисунок. Укажите MAC-адрес назначения кадра Ethernet, когда тот покидает веб-сервер, если конечное устройство назначения — ПК1. 1. 00-60-2F-3A-07-AA 2. 00-60-2F-3A-07-BB 3. 00-60-2F-3A-07-CC 4. 00-60-2F-3A-07-DD	3
53	Какому десятичному числу соответствует шестнадцатеричное значение 3F? 1. 18 2. 34 3. 45 4. 46 5. 63	5
54	В чем состоит основное назначение протокола разрешения адресов (ARP)? 1. преобразование URL-адресов в IP-адреса 2. преобразование IPv4-адресов в MAC-адреса 3. обеспечение динамической IP-конфигурации для сетевых устройств 4. преобразование внутренних частных адресов во внешние публичные адреса	2

55	Какое действие предпринимает коммутатор второго уровня при получении широковещательного кадра такого же уровня? 1. Сбрасывает кадр. 2. Отправляет данный кадр на все порты, кроме порта, получившего этот кадр. 3. Отправляет этот кадр на все порты, зарегистрированные для пересылки широковещательных пакетов. 4. Отправляет кадр на все порты.	2
56	Заполните пустое поле, вставив число. Минимальный размер кадра Ethernet составляет _____ байт. Кадры с меньшим размером считаются «карликовыми».	64
57	Заполните пустое поле. Двоичное число 0000 1010 можно выразить как _____в шестнадцатеричной системе счисления.	0A
58	Заполните пустое поле. Подуровень Ethernet _____ отвечает за обмен данными напрямую с физическим уровнем.	MAC
59	 Посмотрите на рисунок. Узел H2 отправил широковещательное сообщение всем узлам. Какое из приведенных утверждений верно в случае, когда узел H1 хочет отправить ответ на широковещательное сообщение? 1. Узел H1 отправляет одноадресное сообщение на узел H2, но коммутатор пересылает его на все устройства. 2. Узел H1 отправляет одноадресное сообщение на узел H2, и коммутатор пересылает его непосредственно на узел H2. 3. Узел H1 отправляет широковещательное сообщение на узел H2, но коммутатор пересылает его на все устройства. 4. Узел H1 отправляет многоадресное сообщение на узел H2, и коммутатор пересылает его непосредственно на узел H2.	2
60	Каким типом адреса является 01-00-5E-0A-00-02? адрес, который позволяет связаться с каждым узлом в пределах локальной подсети 1. адрес, который позволяет связаться с конкретным узлом	3

	2. адрес, который позволяет связаться с каждым узлом данной сети 3. адрес, который позволяет связаться с конкретной группой узлов	
61	Какие две функции или действия выполняет подуровень MAC? (Выберите два варианта ответа.) 1. Отвечает за управление доступом к среде. 2. Выполняет функцию программного обеспечения драйвера NIC. 3. Добавляет заголовок к концевику для образования блока данных уровня 2 модели OSI. 4. Устанавливает связь между верхними и нижними уровнями. 5. Добавляет сведения об управлении к данным уровня сетевого протокола.	1, 3
62	Заполните пустое поле. В сетях Ethernet шестнадцатеричный адрес формата FF-FF-FF-FF-FF-FF представляет собой MAC-адрес. (Одно прилагательное на русском языке) _____MAC-адрес.	широковещательный
63	К какому способу коммутации вернется коммутатор при достижении определенного числа ошибок на порту, в случае если на этом порту пользователь настроил пороговые значения? 1. коммутация с исключением фрагментов 2. быстрая пересылка 3. сквозная коммутация 4. коммутация с промежуточным хранением	4
64	 Посмотрите на рисунок. ПК1 выдает запрос ARP, поскольку ему необходимо отправить пакет на ПК3. Что произойдёт далее при таком развитии событий? 1. RT1 перешлёт запрос ARP на ПК3. 2. RT1 отправит ответ ARP с собственным MAC-адресом Fa0/0. 3. RT1 отправит ответ ARP с собственным MAC-адресом PC3. 4. SW1 отправит ответ ARP с собственным MAC-адресом Fa0/1.	5

	5. RT1 отправит ответ ARP с собственным MAC-адресом Fa0/1.	
65	Какая часть кадра Ethernet используется для проверки ошибок при коммутации с промежуточным хранением? 1. циклический избыточный код (CRC) в концевике 2. MAC-адрес источника в заголовке 3. MAC-адрес назначения в заголовке 4. тип протокола в заголовке	1
66	Какая часть адреса сетевого уровня используется маршрутизатором для пересылки пакетов? 1. узловая часть 2. широковещательный адрес 3. сетевая часть 4. адрес шлюза	3
67	Маршрутизатору может потребоваться фрагментировать пакет при его пересылке из одной среды передачи данных в другую среду с меньшим максимальным размером пакета. При пересылке пакета из одной среды передачи данных в другую среду с меньшим значением (аббревиатура на английском) маршрутизатору может потребоваться фрагментировать пакет _____	MTU
68	 Посмотрите на рисунок. Заполните пустое поле. Пакет, покидающий ПК-1, должен совершить _____ переход (-а)(-ов) для достижения ПК-4.	3
69	Какие две из перечисленных ниже функций предоставляют сетевой уровень? 1. перенос данных между процессами, исполняемыми на узлах-источниках и узлах-адресатах 2. присвоение оконечным устройствам уникального сетевого идентификатора 3. размещение данных в сетевой среде 4. направление пакетов данных к узлам-адресатам, расположенным в пределах других сетей 5. обеспечение выделенных сквозных подключений	2, 4
70	Где программа загрузки маршрутизатора ищет образ IOS по умолчанию во время процесса загрузки? 1. флеш-память 2. NVRAM 3. ОЗУ 4. ПЗУ	1

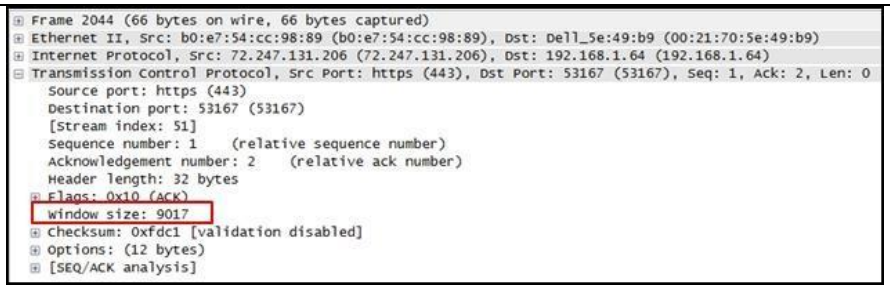
71	Какая комбинация клавиш позволяет пользователю прервать режим первоначальной настройки (setup mode)? 1. Ctrl-C 2. Ctrl-R 3. Ctrl-Z 4. Ctrl-Shift-6	4
72	В колледже пять кампусов. В каждом кампусе установлены IP-телефоны. Каждому кампусу назначен свой диапазон IP-адресов. Например, IP-адреса одного кампуса начинаются с 10.1.x.x. Диапазон адресов другого кампуса — 10.2.x.x. В соответствии со стандартом колледжа IP-телефонам назначаются IP-адреса, третий октет которых имеет вид 4X. Например, диапазоны адресов телефонов в одном кампусе включают адреса 10.1.40.x, 10.1.41.x, 10.1.42.x и т.д. Какие два принципа группировки узлов были использованы для создания этой схемы IP-адресации? (Выберите два варианта.) 1. географическое местоположение 2. тип устройства 3. отдел 4. тип персонала 5. модель поддержки	2, 3
73	 Посмотрите на изображение. Какие два сетевых адреса могут быть использованы для сети, содержащей 10 узлов? Выберите ответы, которые экономят наибольшее количество адресов, не пересекаются с уже назначенными адресами и не выходят за рамки диапазона адресов 10.18.10.0/24. (Выберите два варианта.) 1. 10.18.10.200/28 2. 10.18.10.208/28 3. 10.18.10.224/28 4. 10.18.10.200/27 5. 10.18.10.224/27 6. 10.18.10.240/27	1, 3
74	Администратор хочет создать четыре подсети из сетевого адреса 192.168.1.0/24. Какими будут адрес сети и маска подсети второй используемой подсети? 1. подсеть 192.168.1.64	4

	маска подсети 255.255.255.192 2. подсеть 192.168.1.32 маска подсети 255.255.255.240 3. подсеть 192.168.1.64 маска подсети 255.255.255.240 4. подсеть 192.168.1.128 маска подсети 255.255.255.192 5. подсеть 192.168.1.8 маска подсети 255.255.255.224	
75	Сколько адресов узлов доступно в сети с адресом 192.168.10.128/26? 1. 30 2. 32 3. 60 4. 62 5. 64	4
76	Три устройства находятся в трех различных подсетях. Сопоставьте сетевой адрес и широковещательный адрес с каждой подсетью, в которой расположены эти устройства. (Не все варианты используются.) Устройство 1: IP-адрес 192.168.10.77/28 в подсети 1 Устройство 2: IP-адрес 192.168.10.17/30 в подсети 2 Устройство 3: IP-адрес 192.168.10.35/29 в подсети 3 • Номер сети для подсети 1 - **192.168.10.64** • Широковещательный адрес подсети 1 – **192.168.10.79** • Номер сети для подсети 2 – **192.168.10.16** • Широковещательный адрес подсети 2 – **192.168.10.19** • Номер сети для подсети 3 – **192.168.10.32** • Широковещательный адрес подсети 3 – **192.168.10.39** • **192.168.10.47**	
77	Сетевой администратор получил следующий префикс IPv6 для выделения подсети — 2001:DB8::/48. Сколько подсетей может создать сетевой администратор с префикса /48, если учесть, что администратор не будет выделять подсеть в область идентификатора интерфейса адресного пространства? 1. 16 2. 256 3. 4096 4. 65536	3
78	Назовите два преимущества разделения сетей на подсети. (Выберите два варианта.)	2, 4

	1. объединение нескольких небольших сетей в крупные сети 2. уменьшение размера доменов широковещательной рассылки 3. снижение количества доменов широковещательной рассылки 4. группировка устройств для улучшения возможностей по управлению и обеспечению безопасности 5. увеличение размера коллизионных доменов	
79	Сетевой администратор разделил сеть 192.168.10.0/24 на подсети с масками /26. Сколько подсетей одинакового размера он создал? 1. 1 2. 2 3. 4 4. 8 5. 16 6. 64	3
80	Каков адрес подсети для IPv6-адреса 2001:D12:AA04:B5::1/64? 1. 2001::/64 2. 2001:D12::/64 3. 2001:D12:AA04::/64 4. 2001:D12:AA04:B5::/64	4
81	Сетевой инженер выполняет разделение сети с адресом 10.0.240.0/20 на более мелкие подсети. Каждая новая подсеть будет содержать 20-30 узлов, где 20 является минимальным количеством, а 30 — максимальным. Какая маска подсети будет соответствовать таким требованиям? 1. 255.255.224.0 2. 255.255.240.0 3. 255.255.255.224 4. 255.255.255.240	3
82	Протоколы IPv4 и IPv6 могут существовать одновременно благодаря использованию трех способов. Сопоставьте каждый способ с их описанием. (Не все варианты используются.) • Пакеты IPv4 и пакеты IPv6 одновременно сосуществуют в одной и той же сети – **двойной стек** • Пакет IPv6 транспортируется внутри пакета IPv4 - **тунелирование** • Пакеты IPv6 преобразованы в пакеты IPv4, и наоборот - **преобразование** • **DHCP**	
83	Что представляет собой IP-адрес 192.168.1.15/29? 1. адрес подсети	4

	2. адрес многоадресной рассылки 3. адрес одноадресной рассылки 4. широковещательный адрес	
84	Заполните пустое поле. Последний адрес узла в сети с адресом 10.15.25.0/24 имеет следующий вид: _____	10.10.25.254/24
85	Префикс адреса 172.16.30.5/16 имеет следующий вид: _____	172.16
86	Сопоставьте описание с компонентом IPv6-адресации. (Не все варианты используются.) • Эта часть адреса используется компанией для определения подсетей – **идентификатор подсети** • Эта сетевая часть адреса присваивается поставщиком – **глобальный префикс маршрутизации** • Эта часть адреса аналогична узловой части IPv4-адреса – **идентификатор интер**фейса • **маска подсети**	
87	Каково представление длины префикса для маски подсети 255.255.255.224? 1. /25 2. /26 3. /27 4. /28	3
88	Каким двум типам устройств обычно присваиваются статические IP-адреса? (Выберите два варианта.) рабочие станции 1. веб-серверы 2. принтеры 3. концентраторы 4. ноутбуки	1, 2
89	Заполните пустое поле. 8-значное двоичное значение последнего октета IPv4-адреса 172.17.10.7 _____	00000111
90	Сетевой адрес 172.16.30.5/16 имеет следующий вид:	172.16.0.0
91	Какой альтернативный метод можно использовать вместо DHCPv6 для того, чтобы маршрутизатор динамически предоставлял на узлы информацию о конфигурации IPv6? 1. ARP 2. EUI-64 3. ICMPv6 4. SLAAC	4

92	Сопоставьте каждое описание с соответствующими IP-адресами. (Не все варианты используются.) • локальный адрес канала - **198.133.219.2** • публичный адрес – **169.254.1.5** • экспериментальный адрес – **240.2.6.255** • адрес loopback – **127.0.0.1** • **240.2.6.255**	
93	Заполните пустое поле. Последний адрес узла в сети с адресом 10.15.25.0/24 имеет следующий вид: _____	10.15.25.254/24
94	Пользователь, который не может подключиться к файловому серверу, обращается в службу поддержки. Технический специалист службы поддержки просит пользователя отправить эхо-запрос на IP-адрес шлюза по умолчанию, который настроен на рабочей станции. С какой целью отправляется этот эхо-запрос ping? 1. получить от сервера динамический IP-адрес 2. запросить шлюз переслать запрос на соединение к файловому серверу 3. проверить, может ли узел достичь узлов, находящихся в других сетях 4. преобразовать имя домена файлового сервера в его IP-адрес	3
95	Какой уровень OSI отвечает за установление временного сеанса обмена данными между двумя приложениями и повторное восстановление переданных данных в правильной последовательности? 1. транспортный 2. сетевой 3. канальный 4. сеансовый	1
96	Какая функция транспортного уровня используется для гарантированного установления сеанса? 1. флаг UDP ACK 2. трёхстороннее рукопожатие TCP 3. номер последовательности UDP 4. номер TCP-порта	2

97	 Посмотрите на рисунок. На что указывает значение размера окна? 1. на объём данных, который можно отправить за один раз 2. на общее количество бит, полученных во время этого сеанса TCP 3. на объём данных, которые можно отправить, прежде чем потребуется подтверждение 4. на случайное число, которое используется для установления соединения с помощью процедуры трёхстороннего рукопожатия	1
98	В чём заключается преимущество протокола UDP над протоколом TCP? 1. При обмене данными с использованием протокола UDP требуется меньше затрат вычислительных ресурсов. 2. Обмен данными с использованием протокола UDP более надёжен. 3. С помощью протокола UDP происходит переупорядочивание сегментов, которые поступают в неправильном порядке. 4. С помощью протокола UDP происходит подтверждение полученных данных.	1
99	Какой тип приложений лучше всего подходит для использования протокола UDP? приложения, чувствительные к задержке 1. приложения, которым необходимо обеспечить надежную доставку 2. приложения, требующие повторной передачи потерянных сегментов 3. приложения, чувствительные к потере пакетов	1
100	Какое действие выполняется клиентом при установлении соединения с сервером с помощью протокола UDP на транспортном уровне? 1. Клиент устанавливает размер окна сеанса. 2. Клиент отправляет ISN к серверу, чтобы начать процедуру трёхстороннего рукопожатия. 3. Клиент случайным образом выбирает номер порта источника. 4. Клиент отправляет синхронизирующий сегмент, чтобы начать сеанс.	3
101	Какие три поля используются в заголовке сегмента блока данных UDP? (Выберите три варианта ответа.)	2, 3, 5

	1. Размер окна 2. Длина 3. Порт-источник 4. Номер подтверждения 5. Контрольная сумма 6. Последовательный номер	
102	Перегрузка сети привела к тому, что узел источника узнал о потере сегментов TCP, которые были отправлены узлу назначения. Каким одним из указанных ниже способов протокол TCP решает эту проблему? 1. Узел источника снижает объем данных, которые он передает, прежде чем получает подтверждение об их приемке узлом назначения. 2. Узел источника уменьшает размер окна, чтобы снизить скорость передачи данных из узла назначения. 3. Узел назначения уменьшает размер окна. 4. Узел назначения отправляет меньшее количество подтверждающих сообщений, чтобы сохранить необходимую пропускную способность.	2
103	Какая команда используется для отправки запроса серверу DNS вручную, чтобы преобразовать конкретное имя узла? **4. nslookup** **5. ipconfig /displaydns** **6. tracert** 7. **ping**	1
104	Проводной лазерный принтер подключен к домашнему компьютеру. Это принтер сделан общим, чтобы другие компьютеры в домашней сети также могли его использовать. Какая модель сети используется в этом случае? 1. одноранговая (P2P) 2. клиентская 3. ведущий-ведомый 4. точка-точка	1
105	Верно или неверно? При передаче данных по FTP клиент FTP устанавливает соединение со своей стороны, чтобы скачать файлы с сервера FTP. 1. верно 2. неверно	1
106	Какое устройство в домашней сети чаще всего обеспечивает динамическую выдачу IP-адресов клиентам этой сети? 1. выделенный файловый сервер 2. домашний маршрутизатор 3. DHCP-сервер интернет-провайдера 4. DNS-сервер	2
107	Какие три уровня модели OSI обеспечивают аналогичные сетевые сервисы тем сервисам, которые обеспечены уровнем приложений модели TCP/IP? (Выберите три варианта ответа.)	2, 4, 5

	1. физический уровень 2. сеансовый уровень 3. транспортный уровень 4. уровень приложений 5. уровень представления 6. канальный уровень	
107	Какой протокол может быть использован для передачи сообщений с сервера электронной почты на клиент электронной почты? 1. SMTP 2. POP3 3. SNMP 4. HTTP	2
108	Какие из приведенных ниже утверждений о сети типа клиент/сервер являются верными? 1. В сети присутствует выделенный сервер. 2. Каждое устройство может функционировать в качестве сервера и клиента. 3. Рабочие станции обращаются к сетевым ресурсам с помощью SAMBA или Gnutella. 4. Каждый узел обращается к серверу индексации, чтобы получить местоположение ресурса в гибридной сетевой системе.	1
109	Почему в крупных сетях предпочтительно использование DHCP? 1. Крупные сети отправляют больше запросов к домену для разрешения IP-адреса, чем это делают более мелкие сети. 2. DHCP использует надежный протокол транспортного уровня. 3. Он препятствует обмену файлами, защищенными авторским правом. 4. Это более эффективный способ управления IP-адресами, чем статическое назначение адресов. 5. Узлам больших сетей требуется больше параметров конфигурации IP-адресации, чем узлам малых сетей.	4
110	В чём заключается преимущество протокола SMB над протоколом FTP? 1. Обмен данными происходит только с помощью протокола SMB. 2. Только протокол SMB устанавливает два одновременных подключения с клиентом, что позволяет быстрее передавать данные. 3. Протокол SMB более надёжен, чем FTP, поскольку SMB использует протокол TCP, а FTP — UDP. 4. Клиенты SMB могут устанавливать длительное подключение к серверу.	4
111	Какие три протокола или стандарта используются на уровне	2, 3, 4

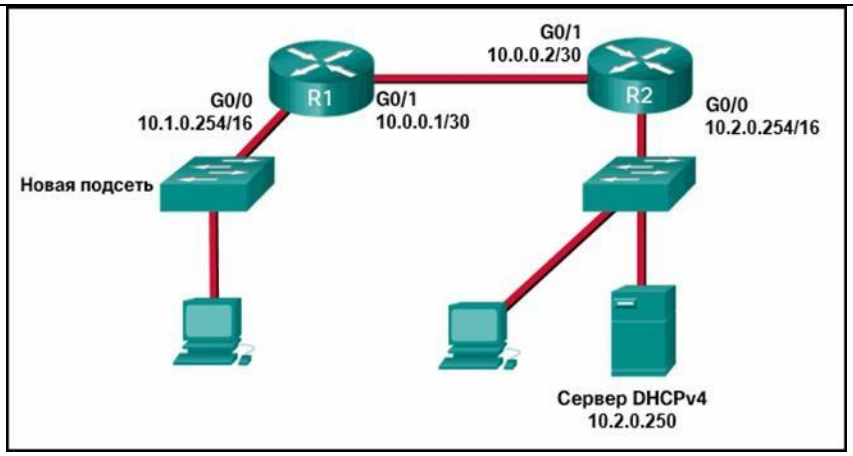
	приложений модели TCP/IP? (Выберите три варианта.) 1. TCP 2. HTTP 3. MPEG 4. GIF 5. IP 6. UDP	
112	Пользователь безуспешно пытается открыть веб-сайт http://www.cisco.com/. Какие две настройки должны быть сделаны на узле, чтобы подключение было возможно? (Выберите два варианта.) 1. DNS-сервер 2. номер порта источника 3. HTTP-сервер 4. шлюз по умолчанию 5. MAC-адрес источника	1, 4
113	Какой самый распространенный протокол используется в таких одноранговых приложениях, как WireShare, Bearshare и Shareaza? 1. Ethernet 2. Gnutella 3. POP 4. SMTP	2
114	Какой уровень модели TCP/IP находится ближе всего к конечному пользователю? 1. уровень приложений 2. межсетевой 3. сетевой доступ 4. транспортный	1
115	Какой тип информации содержится в записи DNS MX? 1. полное доменное имя (FQDN) алиаса, используемого для идентификации сервиса 2. IP-адрес для записи FQDN 3. доменное имя, сопоставленное почтовым серверам 4. IP-адрес утвержденного сервера доменных имен	3

Тест 2 Принципы маршрутизации и коммутации

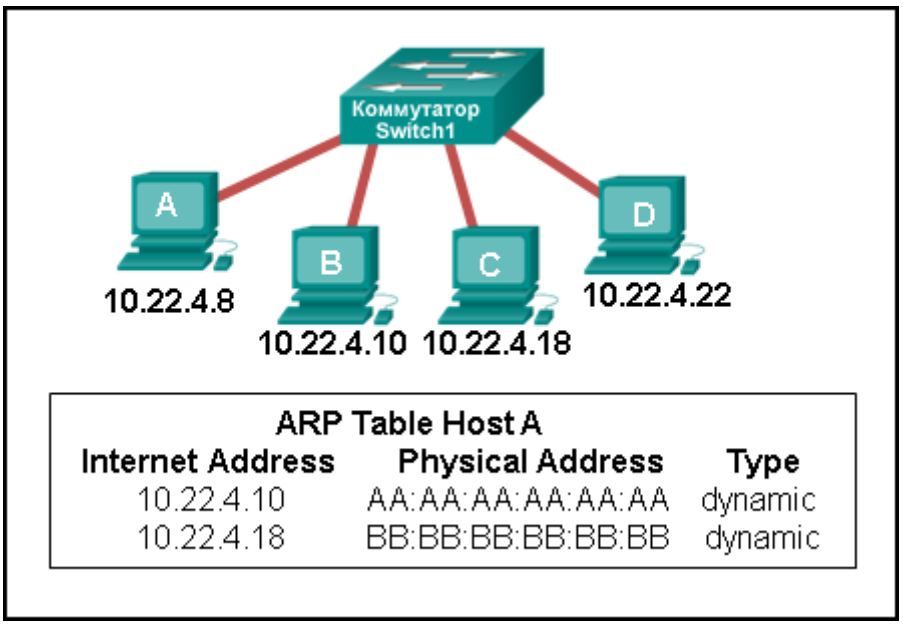
Количество вопросов – 150. Преподаватель формирует нужное количество вариантов теста с любым количеством вопросов.

№ п/п	Вопрос с вариантами ответов	Правильный ответ

1.	A# **show ip route** **<данные опущены>** Gateway of last resort is not set S 10.0.0.0/8 [1/0] via 172.16.40.2 64.0.0.0/16 is subnetted, 1 subnets C 64.100.0.0 is directly connected, Serial0/1 C 128.107.0.0/16 is directly connected, Loopback2 172.16.0.0/24 is subnetted, 1 subnets C 172.16.40.0 is directly connected, Serial0/0 C 192.168.1.0/24 is directly connected, FastEthernet0/0 S 192.168.2.0/24 [1/0] via 172.16.40.2 C 198.133.219.0/24 is directly connected, Loopback0 A# Посмотрите на изображение. Для какой из двух сетей предназначены пакеты, рекурсивный поиск которых необходимо выполнить маршрутизатору? (Выберите два варианта.) 1. 192.168.1.0/24 2. 10.0.0.0/8 3. 192.168.2.0/24 4. 64.100.0.0/16 5. 128.107.0.0/16 6. 172.16.40.0/24	2, 3
2.	Данные передаются с исходного ПК на сервер назначения. Какие три утверждения правильно описывают функцию TCP или UDP в этой ситуации? (Выберите три варианта.) 1. Поле порта источника определяет работающее приложение или службу, которое будет обрабатывать данные, возвращенные на ПК. 2. TCP является предпочтительным протоколом, если функция требует минимального объема служебных данных. 3. Номер порта источника TCP определяет передающий узел в сети. 4. Процесс TCP, работающий на ПК, случайным образом выбирает порт назначения при установке сеанса с сервером. 5. Номер порта назначения UDP определяет приложение или службу на сервере, которые будут обрабатывать данные. 6. Сегменты UDP инкапсулируются в IP-пакете для передачи по сети.	1, 5, 6
3.	Посмотрите на изображение. Сетевой администратор добавил в сеть новую подсеть, и теперь хосты в этой подсети должны получить IPv4 адреса с сервера DHCPv4. Какие две команды позволят хостам в новой подсети получить IPv4 адреса с сервера DHCPv4. (Выберите два варианта).	3, 6

	 1. R2(config-if)# **ip helper-address 10.2.0.250** 2. R2(config)# **interface G0/0** 3. R1(config-if)# **ip helper-address 10.2.0.250** 4. R1(config-if)# **ip helper-address 10.1.0.254** 5. R1(config)# **interface G0/1** 6. R1(config)# **interface G0/0**	
4.	Как иначе происходит обработка маршрутизатором статической маршрутизации при отключенной технологии Cisco Express Forwarding? 1. Последовательные интерфейсы с подключением «точка-точка» требуют полностью определенных статических маршрутов во избежание противоречивой маршрутизации 2. Не выполняется рекурсивный поиск 3. Статические маршруты, использующие выходной интерфейс, не понадобятся. 4. Ethernet-интерфейсы с множественным доступом требуют полностью статических маршрутов во избежание противоречивой маршрутизации.	4
5.	Сколько подсетей /30 можно создать из одной подсети /27? 1. 4 2. 6 3. 8 4. 2	3

6.	SW3(config)# **vlan 35** SW3(config-vlan)# **name marketing** SW3(config-vlan)# **vlan 150** SW3(config-vlan)# **name voice** SW3(config-vlan)# **int fa0/20** SW3(config-if)# **switchport mode access** SW3(config-if)# **switchport access vlan 35** SW3(config-if)# **mls qos trust cos** SW3(config-if)# **switchport access vlan 150** SW3(config-if)# **end** Посмотрите на изображение. Технический специалист программирует коммутатор SW3 для управления трафиком обычных и голосовых данных через порт Fa0/20. В чем ошибка данной настройки (если есть)? 1. Использована неверная команда для назначения голосовой VLAN коммутационному порту. 2. Команда mls qos trust cos должна указывать на сеть VLAN 35. 3. В данной настройке нет ошибок. 4. Интерфейсу Fa0/20 можно назначить только одну сеть VLAN.	1
7.	Какие устройства позволяют узлам в разных VLAN взаимодействовать друг с другом? (Выберите два варианта ответа.) 1. Коммутатор уровня 2. 2. Коммутатор уровня 3. 3. Концентратор. 4. Повторитель. 5. Маршрутизатор.	2, 5
8.	Сетевой администратор разрабатывает схему IPv4-адресации. Ему требуются следующие подсети. 1 подсеть из 100 узлов 2 подсети из 80 узлов 2 подсети из 30 узлов 4 подсети из 20 узлов Какое сочетание подсетей и масок обеспечит наилучший план адресации при этих требованиях? 1. 1 подсеть из 126 узлов с маской 255.255.255.192 2 подсети из 80 узлов с маской 255.255.255.224 6 подсетей из 30 узлов с маской 255.255.255.240. 2. 9 подсетей из 126 узлов с маской 255.255.255.128. 3. 3 подсети из 126 узлов с маской 255.255.255.192 6 подсетей из 30 узлов с маской 255.255.255.240. 4. 3 подсети из 126 узлов с маской 255.255.255.128 6 подсетей из 30 узлов с маской 255.255.255.224.	4
9.	На каком интерфейсе коммутатора администратор должен настроить IP-адрес для возможности удалённого управления этим коммутатором?	1

	1. VLAN 1 2. console 0 3. FastEthernet0/1 4. vty 0	
10.	Взгляните на рисунок. Коммутатор с конфигурацией по умолчанию соединяет четыре узла. Показана таблица ARP для узла A. Что происходит, когда узел A попытается отправить IP-пакет узлу D?  ARP Table Host A Internet Address Physical Address Type 10.22.4.10 AA:AA:AA:AA:AA:AA dynamic 10.22.4.18 BB:BB:BB:BB:BB:BB dynamic 1. Узел A отправляет ARP-запрос по MAC-адресу узла D. Узел D отвечает, используя свой IP-адрес. 2. Узел A отправляет пакет коммутатору. Коммутатор добавляет MAC-адрес для узла D в кадр и пересылает его в сеть. 3. Узел D отправляет ARP-запрос узлу A. Узел A отвечает, используя свой MAC-адрес. 4. Узел A инициирует широковещательное сообщение FF:FF:FF:FF:FF:FF. Все остальные узлы, подключённые к коммутатору, получают это широковещательное сообщение, и узел D отправляет ответ со своим MAC-адресом.	4
11.	Что определяет команда **ip nat pool** при настройке динамического преобразования NAT? 1. пул глобальных адресов 2. пул доступных серверов NAT 3. диапазон внешних IP-адресов, к которым внутренние хосты имеют доступ 4. диапазон внутренних IP-адресов для преобразования	1
12.	Каковы три характеристики процесса CSMA/CD? (Выберите три варианта.) 1. После коллизии данные может передавать только устройство с электронным маркером. 2. Устройства можно настроить с более высоким приоритетом передачи. 3. Устройство отслеживает среду и передает данные, только ко-	3, 5, 6

	гда она свободна. 4. Сигнал "Jam" обозначает, что коллизия разрешена и среда передачи свободна. 5. После обнаружения коллизии узлы могут попытаться возобновить передачу по истечении случайного периода задержки. 6. Все устройства в сегменте принимают данные, которые передаются в среде.	

13.	Посмотрите на изображение. Какой статический маршрут следует ввести ИТ-специалисту для создания резервного маршрута к сети 172.16.1.0, который будет использоваться при отказе основного маршрута, полученного с помощью RIP?
	`R1(config)# do show ip route`
	<анные опущены>
	`Gateway of last resort is 0.0.0.0 to network 0.0.0.0`
	`10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks`
	`C 10.0.0.0/30 is directly connected, Serial0/0/0`
	`L 10.0.0.1/32 is directly connected, Serial0/0/0`
	`172.16.0.0/24 is subnetted, 1 subnets`
	`R 172.16.1.0/24 [120/1] via 10.0.0.2, 00:00:04, Serial0/0/0`
	`192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks`
	`C 192.168.10.0/24 is directly connected, GigabitEthernet0/1`
	`L 192.168.10.1/32 is directly connected, GigabitEthernet0/1`
	`192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks`
	`C 192.168.11.0/24 is directly connected, GigabitEthernet0/0`
	`L 192.168.11.1/32 is directly connected, GigabitEthernet0/0`
	`S* 0.0.0.0/0 is directly connected, Serial0/0/0`
	1. ip route 172.16.1.0 255.255.255.0 s0/0/0 111
	2. ip route 172.16.1.0 255.255.255.0 s0/0/0
	3. ip route 172.16.1.0 255.255.255.0 s0/0/0 91
	4. **ip route 172.16.1.0 255.255.255.0 s0/0/0 121**
		4

14.	Какой тип адреса не поддерживается протоколом IPv6? 1. Индивидуальный адрес (unicast). 2. Групповой адрес. 3. Частный адрес. 4. Широковещательный адрес.	4
15.	Системный администратор устраняет неполадки с подключением между маршрутизаторами и коммутаторами Cisco, соединенными между собой. Какую команду следует использовать администратору для получения информации об IP-адресе, имени хоста и версии IOS соседних сетевых устройств? **1. show cdp neighbors detail** **2. show ip route** **3. show version** 4. **show interfaces**	1
16.	Какие три утверждения характеризуют протокол UDP? (Выберите три варианта.) 1. UDP предоставляет сложные механизмы управления потоком. 2. UDP обеспечивает основные функции транспортного уровня без установления соединения	2, 4, 5

	3. UDP обеспечивает быструю передачу данных уровня 3 с установлением соединения 4. UDP использует протоколы уровня приложений для выявления ошибок 5. UDP — это протокол с низкими накладными расходами, который не поддерживает механизмы упорядочения или управления потоком. 6. UDP использует протокол IP для выявления и устранения ошибок.	

17.	Посмотрите на изображение. Что произойдет, если ИТ-администратор введет новый статический маршрут?
	`R1(config)# do show ip route`
	`<анные опущены>`
	`Gateway of last resort is 0.0.0.0 to network 0.0.0.0`
	`10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks`
	`C 10.0.0.0/30 is directly connected, Serial0/0/0`
	`L 10.0.0.1/32 is directly connected, Serial0/0/0`
	`172.16.0.0/24 is subnetted, 1 subnets`
	`R 172.16.1.0/24 [120/1] via 10.0.0.2, 00:00:04, Serial0/0/0`
	`192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks`
	`C 192.168.10.0/24 is directly connected, GigabitEthernet0/1`
	`L 192.168.10.1/32 is directly connected, GigabitEthernet0/1`
	`192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks`
	`C 192.168.11.0/24 is directly connected, GigabitEthernet0/0`
	`L 192.168.11.1/32 is directly connected, GigabitEthernet0/0`
	`S* 0.0.0.0/0 is directly connected, Serial0/0/0`
	`R1(config)# ip route 172.16.1.0 255.255.255.0 s0/0/0`
	1. Маршрут 172.16.1.0, полученный от RIP, будет заменен на статический маршрут 172.16.1.0.
	2. Статический маршрут 172.16.1.0 будет добавлен к существующим маршрутам в таблице маршрутизации.
	3. Статический маршрут 172.16.1.0 будет добавлен в running-config, но не будет указан в таблице маршрутизации.
	4. Маршрут по умолчанию 0.0.0.0 будет заменен на статический маршрут 172.16.1.0.
		1

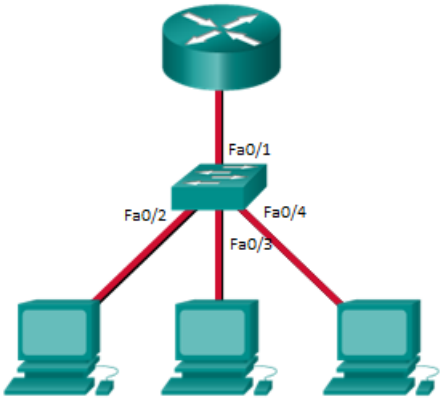
18	Посмотрите на изображение. Технический специалист по сетям вводит команду show vlan для проверки конфигурации VLAN. Исходя из выходных данных, какой порт должен быть назначен сети VLAN с нетегированным трафиком?
	`SW1# show vlan`
	`VLAN Name Status Ports`
	`---- --------------- ------- -------------------`
	`1 default active Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/21`
	`Fa0/22, Fa0/23, Gig0/1, Gig0/2`
	`10 Office1 active Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5`
	`Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10`
	`20 Management active Fa0/24`
	`30 Administration active Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15`
	`<анные опущены>`
	1. Fa0/12
	2. Fa0/24
	3. Fa0/20
	4. Gig0/1
		3

19.	По каким двум причинам администратор мог бы применить статическую маршрутизацию вместо динамической? (Выберите два варианта.)	1, 5

	1. Статическая маршрутизация безопаснее. 2. Статическая маршрутизация не требует полного представления о топологии сети. 3. Статическая маршрутизация упрощает управление маршрутами в больших сетях. 4. Статическая маршрутизация упрощает масштабирование. 5. Статическая маршрутизация не создает дополнительной нагрузки на вычислительные ресурсы маршрутизатора и подразумевает меньший объем служебного трафика.	
20.	При поиске и устранении неполадок на коммутаторе администратор заметил, что коммутационный порт, на котором настроена безопасность портов, находится в состоянии err-disabled. Как следует повторно включать порт после проверки причин нарушения, не нарушая работы сети? 1. Использовать команду **no switchport port-security**, а затем повторно включить безопасность портов. 2. Использовать для интерфейса команду **shutdown**, а затем команду **no shutdown**. 3. Использовать команду **no switchport port-security violation shutdown** для этого интерфейса. 4. Перезагрузить коммутатор.	2, 4
21.	Администратору нужно заменить файл настройки на маршрутизаторе Cisco путем загрузки нового файла настройки с сервера TFTP. Какие два элемента должен знать администратор перед выполнением этой задачи? (Выберите два варианта ответа.) 1. IP-адрес сервера TFTP 2. имя файла настройки, который в настоящее время хранится на сервере TFTP 3. значение реестра настройки 4. имя файла настройки, который в настоящее время хранится на маршрутизаторе 5. IP-адрес маршрутизатора	1, 2
22.	Сетевой специалист настраивает защиту порта для интерфейса коммутатора локальной сети. Согласно политике безопасности MAC-адреса узлов должны быть получены динамически, храниться в таблице адресов и сохраняться в текущей конфигурации коммутатора. Какую команду должен добавить технический специалист в следующую конфигурацию, чтобы реализовать эту политику? Switch(config)# **interface fa0/1** Switch(config-if)# **switchport mode access** Switch(config-if)# **switchport port-security** 1. Switch(config-if)# **switchport port-security mac-address 000B.FCFF.E880** 2. Switch(config-if)# **switchport port-security mac-address sticky** 3. Switch(config-if)# **switchport port-security mac-address** 4. Switch(config-if)# **switchport port-security maximum 40**	2
23.	Посмотрите на рисунок. Сопоставьте пакеты и их IP-адрес назначения с существующими интерфейсами на маршрутизаторе. (Не все варианты используются.)	

	<выходные данные опущены> Gateway of last resort is 0.0.0.0 to network 0.0.0.0 10.0.0.0/24 is subnetted, 1 subnets C 10.1.0.0 is directly connected, Serial0/0/0 172.17.0.0/24 is subnetted, 4 subnets O 172.17.6.0 [110/2] via 192.168.3.4, 00:10:41, FastEthernet0/0 O 172.17.10.0 [110/2] via 192.168.5.2, 00:09:52, FastEthernet1/1 O 172.17.12.0 [110/2] via 192.168.4.2, 00:12:23, FastEthernet1/0 C 172.17.14.0 is directly connected, FastEthernet0/1 C 192.168.3.0/24 is directly connected, FastEthernet0/0 C 192.168.4.0/24 is directly connected, FastEthernet1/0 C 192.168.5.0/24 is directly connected, FastEthernet1/1 S* 0.0.0.0/0 is directly connected, Serial0/0/0 пакеты с адресом назначения 172.17.10.5 пакеты с адресом назначения 172.17.12.10 пакеты с адресом назначения 172.17.14.8 пакеты с адресом назначения 172.17.8.20 пакеты с адресом назначения 172.17.6.15 • **FastEthernet0/0** – пакеты с адресом назначения 172.17.6.15 • **FastEthernet0/1** – пакеты с адресом назначения 172.17.14.8 • **FastEthernet1/0** – пакеты с адресом назначения 172.17.12.10 • **FastEthernet1/1** – пакеты с адресом назначения 172.17.10.5 • **Serial0/0/0** - пакеты с адресом назначения 172.17.8.20 • **Пакет потерян**	
24	Посмотрите на изображение. Что маршрутизатор R1 сделает с пакетом, который имеет IPv6-адрес назначения: 2001:db8:cafe:5::1? R1# show ipv6 route <анные опущены> 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 1. перешлет пакет через GigabitEthernet0/0 2. перешлет пакет через GigabitEthernet0/1 3. отправит пакет через интерфейс Serial0/0/0 4. отбросит пакет	3
25	Сетевому администратору был выделен блок IPv4-адресов 10.10.240.0/20 для локальной сети. Двум устройствам в двух разных, но смежных подсетях локальной сети были назначены адреса	1

	10.10.247.1/21 и 10.10.248.10/24, соответственно. Администратор должен создать третью подсеть из оставшегося диапазона адресов. Для оптимизации использования этого адресного пространства новая подсеть должна следовать сразу же после уже существующих подсетей. Каким будет первый доступный адрес узла в следующей доступной подсети? 1. 10.10.249.1 2. 10.10.255.17 3. 10.10.250.1 4. 10.10.248.17	
26	Когда при создании статического маршрута IPv6 должны быть одновременно указаны IPv6-адрес следующего перехода и выходной интерфейс? 1. Когда включена технология CEF. 2. Когда выходной интерфейс является интерфейсом «точка-точка». 3. Когда статический маршрут является маршрутом по умолчанию. 4. Когда следующий переход является локальным канальным адресом.	4
27	Пользователь отправляет HTTP-запрос на веб-сервер в удалённой сети. Какая информация добавляется в поле адреса кадра во время инкапсуляции для определения назначения? 1. MAC-адрес шлюза по умолчанию\ 2. Сетевой домен узла назначения 3. MAC-адрес узла назначения 4. IP-адрес шлюза по умолчанию	1

28	Взгляните на рисунок. Взаимодействие между сетями VLAN 10, VLAN 20 и VLAN 30 оказалось неудачным. В чём проблема?
	 
	
	`<output omitted>`
	`interface FastEthernet0/1`
	`switchport trunk allowed vlan 10,20,30`
	`switchport mode access`
	`switchport nonegotiate`
	`!`
	`interface FastEthernet0/2`
	`switchport access vlan 10`
	`switchport mode access`
	`switchport nonegotiate`
	`!`
	`interface FastEthernet0/3`
	`switchport access vlan 20`
	`switchport mode access`
	`switchport nonegotiate`
	`!`
	`interface FastEthernet0/4`
	`switchport access vlan 30`
	`switchport mode access`
	`switchport nonegotiate`
	1. Интерфейс коммутатора FastEthernet0/1 настроен как интерфейс доступа, а должен быть настроен как магистральный интерфейс.
	2. Для интерфейсов коммутатора FastEthernet0/2, FastEthernet0/3 и FastEthernet0/4 установлено отсутствие согласования, следует включить согласование для этих интерфейсов.
		1

	3. Для интерфейса коммутатора FastEthernet0/1 установлено отсутствие согласования, следует включить согласование для этого интерфейса. 4. Интерфейсам доступа не назначены IP-адреса, для каждого из них должен быть настроен IP-адрес.	
29	Какой диапазон префиксов адресов зарезервирован для многоадресной рассылки IPv4? 1. 224.0.0.0 - 239.255.255.255 2. 240.0.0.0 - 254.255.255.255 3. 169.254.0.0 - 169.254.255.255 4. 127.0.0.0 - 127.255.255.255	1

30	Посмотрите на изображение. Какой адрес источника используется маршрутизатором R1 для пакетов, перенаправляемых в Интернет?
	`R1# show ip nat translations`
	`Pro Inside global Inside local Outside local Outside global`
	`tcp 209.165.200.225:1405 10.6.15.2:1405 209.165.202.141:80 209.165.202.141:80`
	`tcp 209.165.200.225:1406 10.6.15.1:1406 198.51.100.3:80 198.51.100.3:80`
	1. 10.6.15.2
	2. 198.51.100.3
	3. 209.165.202.141
	4. 209.165.200.225
		4

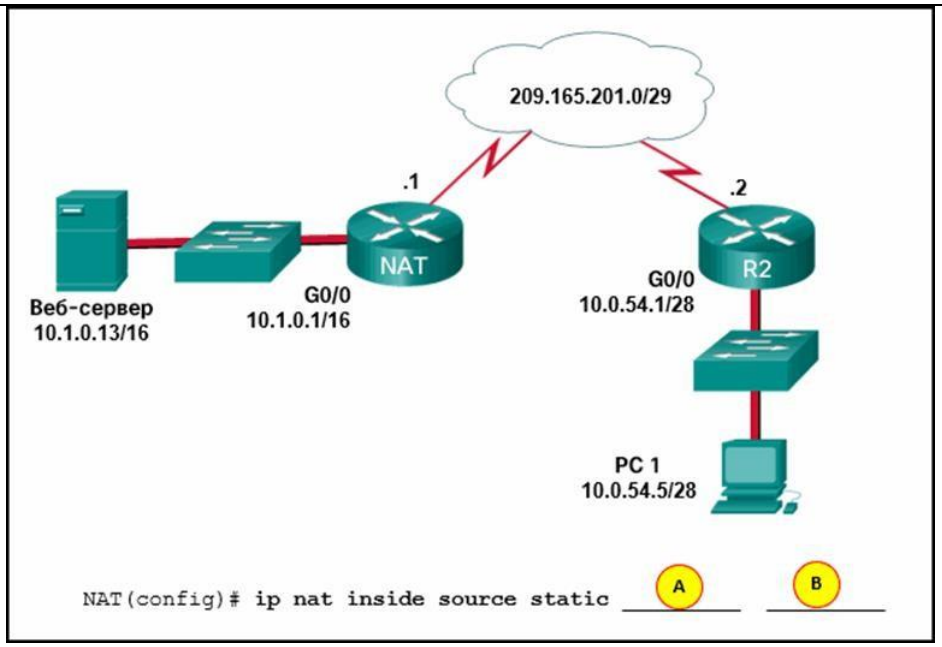
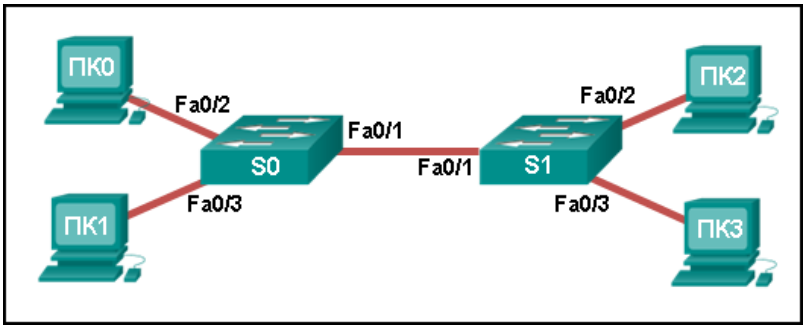
31	Какой префикс IPv6 зарезервирован для обмена данными между устройствами на одном и том же канале? 1. FDFF::/7 2. FE80::/10 3. FC00::/7 4. 2001::/32	2

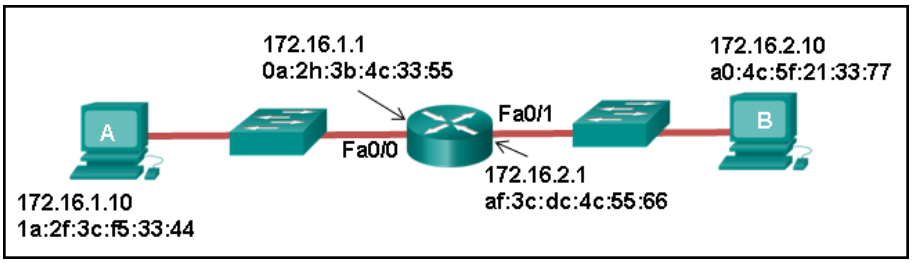
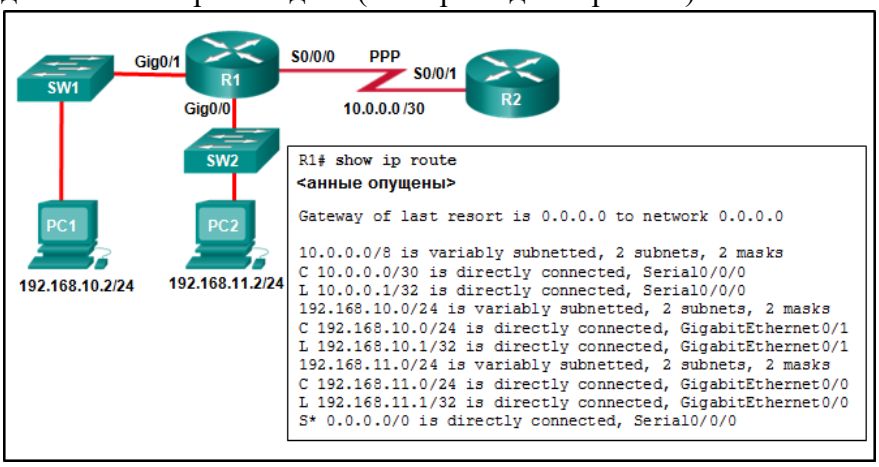
32	Взгляните на рисунок. Сетевой администратор проверяет назначение портов и VLAN на коммутаторе S2 и замечает, что интерфейсы Gi0/1 и Gi0/2 отсутствуют в результатах. Почему этих интерфейсов нет в результатах?
	 
	`S2# show vlan brief`
	`VLAN Name Status Ports`
	`---- ---------- --------- ----------`
	`1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4`
	`Fa0/5, Fa0/6, Fa0/7, Fa0/8`
	`Fa0/9, Fa0/10, Fa0/11, Fa0/12`
	`Fa0/13, Fa0/14, Fa0/15, Fa0/16`
	`Fa0/17, Fa0/18, Fa0/19, Fa0/20`
	`20 Student active Fa0/21, Fa0/22, Fa0/23, Fa0/24`
	`1002 fddi-default act/unsup`
	`1003 token-ring-default act/unsup`
	`1004 fddinet-default act/unsup`
	`1005 trnet-default act/unsup`
	1. Между коммутаторами имеется несоответствие собственной VLAN сети (native VLAN).
	2. Отсутствует среда, подключённая к интерфейсам.
		4

	3. Интерфейсы отключены администратором. 4. Интерфейсы сконфигурированы как магистральные.	

33	Посмотрите на изображение. Как маршрут хоста 2001:DB8:CAFE:4::1/128 был занесен в таблицу маршрутизации?
	`R1# show ipv6 route`
	
	`<анные опущены>`
	
	`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`
	
	1. Этот маршрут был создан динамически маршрутизатором R1.
	2. Этот маршрут был занесен автоматически при настройке IP-адреса на активном интерфейсе.
	3. Этот маршрут был получен динамически от другого маршрутизатора.
	4. Этот маршрут был введен вручную администратором.
		4

34	Сетевой администратор использует маршрутизатор модели router-on-a-stick для конфигурации коммутатора и маршрутизатора при настройке маршрутизации между сетями VLAN. Как необходимо настроить порт коммутатора, подключённый к маршрутизатору? 1. Настроить порт как магистральный порт и разрешить к нему доступ только трафику без меток. 2. Настроить порт как магистральный порт и назначить его в VLAN1. 3. Настроить порт как магистральный порт 802.1q. 4. Настроить порт как порт доступа и включить его в состав VLAN1.	3
35	Посмотрите на изображение. Настроено статическое преобразование NAT для предоставления PC 1 доступа к веб-серверу во внутренней сети. Какие два адреса необходимо указать вместо A и B для настройки статического преобразования NAT? (Выберите два варианта.)	3, 5

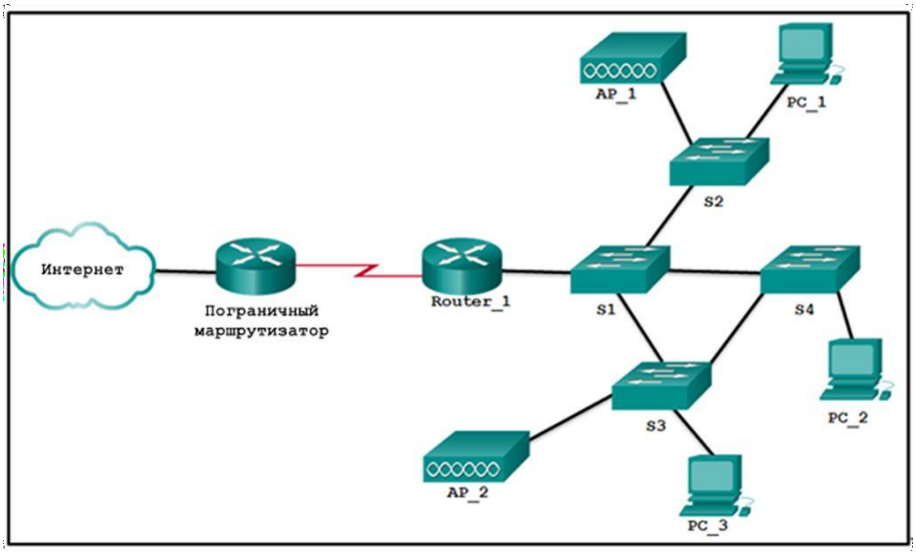
	 1. A = 209.165.201.2 2. B = 209.165.201.7 3. A = 10.1.0.13 4. B = 10.0.254.5 5. B = 209.165.201.1	
36	Какая функция на маршрутизаторе позволяет перенаправлять трафик без определенного маршрута? 1. исходящий интерфейс 2. маршрут по умолчанию (шлюз последней надежды) 3. следующий транзитный участок 4. источник маршрута	2
37	Какие два элемента должен изменить сетевой администратор на маршрутизаторе для выполнения восстановления пароля? (Выберите два варианта.) 1. системное ПЗУ 2. загрузочный конфигурационный файл 3. файл системного образа 4. файловая система NVRAM 5. значение конфигурационного реестра	2, 5
38	Посмотрите на рисунок. Эхо-запрос на ПК3 выполняется от ПК0, ПК1 и ПК2 именно в таком порядке. Какие MAC-адреса будут содержаться в таблице MAC-адресов S1, связанной с портом Fa0/1? 	4

	1. только MAC-адрес ПК0 2. только MAC-адрес ПК2 3. MAC-адреса ПК0, ПК1 и ПК2 4. только MAC-адреса ПК0 и ПК1 5. только MAC-адрес ПК1	
39	Взгляните на рисунок. Узел A отправляет узлу B пакет данных. Как будет выглядеть адресная информация пакета данных, когда он достигнет узла B?  1. Источник af:3c:dc:4c:55:66 | Назначение a0:4c:5f:21:33:77 | Источник 172.16.2.1 | Назначение 172.16.2.10 | Данные 2. Источник 0a:2h:3b:4c:33:55 | Назначение a0:4c:5f:21:33:77 | Источник 172.16.2.1 | Назначение 172.16.2.10 | Данные 3. Источник 1a:2f:3c:f5:33:44 | Назначение a0:4c:5f:21:33:77 | Источник 172.16.1.10 | Назначение 172.16.2.10 | Данные 4. Источник af:3c:dc:4c:55:66 | Назначение a0:4c:5f:21:33:77 | Источник 172.16.1.10 | Назначение 172.16.2.10 | Данные	4
40	Посмотрите на изображение. Когда на интерфейс Serial0/0/0 маршрутизатора R1 поступает пакет с IP-адресом назначения PC1, какие два события происходят? (Выберите два варианта)  1. Маршрутизатор R1 перешлет пакет из интерфейса Gig0/0. 2. Маршрутизатор R1 перешлет пакет из интерфейса Gig0/1.	2, 5

	3. Маршрутизатор R1 перешлет пакет из интерфейса S0/0/0. 4. Маршрутизатор R1 перешлет пакет из интерфейса Gig0/0. 5. Маршрутизатор R1 деинкапсулирует пакет и инкапсулирует его в кадре Ethernet. 6. Маршрутизатор R1 деинкапсулирует пакет и инкапсулирует его в кадре PPP.	
41	Посмотрите на изображение. Сетевой администратор выполняет команду show lldp neighbors для отображения информации о соседних устройствах. Что можно узнать из этой информации? A1# show lldp neighbors <анные опущены> Device ID Local Intf Hold-time Capability Port ID B1 Fa0/5 99 R Fa0/1 C1 Fa0/4 120 B Fa0/3 1. Устройство A1 подключено к порту Fa0/5 на устройстве B1. 2. Устройство C1 — это коммутатор. 3. Устройство B1 — это точка доступа к беспроводной локальной сети. 4. Устройство C1 подключено к устройству B1 через порт Fa0/3.	2
42	Какой тип адреса IPv6 относится к индивидуальному адресу для одноадресной рассылки, назначенному сразу нескольким хостам? 1. адресация любому устройству группы 2. глобальный индивидуальный адрес 3. локальный адрес канала 4. уникальный локальный адрес	1
43	Каково назначение ключевого слова "overload" в команде **ip nat inside source list 1 pool NAT_POOL overload**? 1. Позволяет перечисленным внутренним хостам взаимодействовать с конкретной группой внешних хостов. 2. Позволяет множеству внутренних хостов совместно использовать один или несколько внутренних глобальных адресов. 3. Позволяет внешним хостам инициировать сеансы с внутренними узлами. 4. Позволяет внутренним хостам использовать пул внутренних глобальных адресов.	2
44	Каким будет результат выполнения команды **default-information originate** на маршрутизаторе, который настроен для RIP? 1. Любой статический маршрут по умолчанию, полученный от соседнего маршрутизатора, передается на другие смежные маршрутизаторы. 2. Любой статический маршрут, полученный от соседнего маршрутизатора, передается на другие смежные маршрутизаторы. 3. Любой динамический маршрут, полученный от соседнего маршрутизатора, передается на другие смежные маршрутизаторы. 4. Все маршруты, полученные от соседнего маршрутизатора,	2

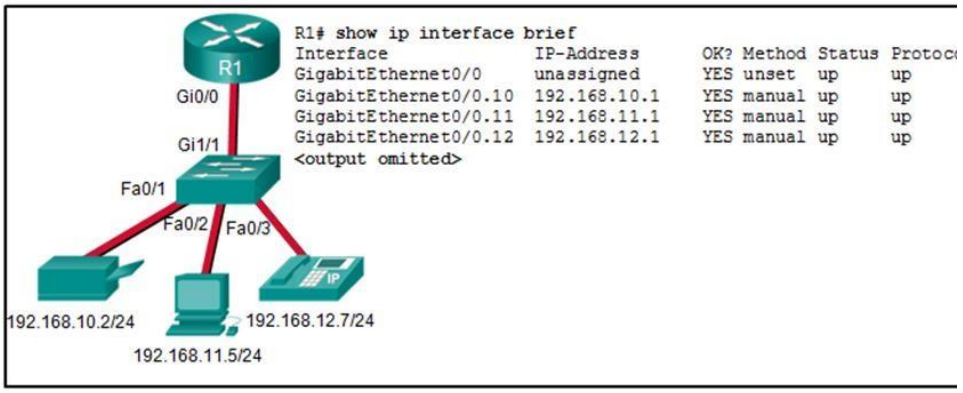
	передаются на другие смежные маршрутизаторы.	
45	Какую информацию можно проверить с помощью команды **show ip dhcp binding**? 1. IPv4-адреса, которые были исключены из пула DHCPv4 2. сообщения обнаружения DHCPv4, которые все еще принимаются сервером DHCP 3. количество IP-адресов, оставшихся в пуле DHCP 4. IPv4-адреса, назначенные хостам сервером DHCP	4
46	Сетевой администратор настраивает маршрутизатор с помощью последовательности команд: R1(config)# **boot system tftp://c1900-universalk9-mz.SPA.152-4.M3.bin** R1(config)# **boot system rom** Каков результат этой последовательности? 1. Маршрутизатор загрузит образ IOS с TFTP-сервера. Если произошел сбой загрузки образа, маршрутизатор загрузит образ IOS из ПЗУ. 2. Маршрутизатор скопирует образ IOS с TFTP-сервера и затем перезагрузит систему. 3. Маршрутизатор будет искать действующий образ IOS последовательно во флеш-памяти, на TFTP-сервере и в ПЗУ, а затем загрузит его. 4. При следующей перезагрузке маршрутизатор загрузит образ IOS из ПЗУ.	1
47	Какие условия должен проверить администратор перед попыткой обновления образа Cisco IOS с помощью сервера TFTP? (Выберите два варианта ответа.) **1.** Убедиться, что сервер TFTP запущен, с помощью команды **tftpdnld.** 2. Проверить правильность контрольной суммы для образа с помощью команды **show version**. 3. Убедиться в наличии достаточного объёма флеш-памяти для нового образа Cisco IOS с помощью команды **show flash**. **4.** Проверить соединение между маршрутизатором и сервером TFTP с помощью команды **ping** 5. Проверить имя сервера TFTP с помощью команды **show hosts.**	3, 4
48	Отправка эхо-запроса с маршрутизатора R1 к напрямую подключённому маршрутизатору R2 не удается. Затем сетевой администратор вводит команду **show cdp neighbors**. Зачем администратору вводить эту команду, если эхо-запрос между двумя маршрутизаторами оказался неудачным? 1. Сетевой администратор хочет проверить IP-адрес, настроенный на маршрутизаторе R2. 2. Сетевой администратор подозревает наличие вируса, поскольку команда ping не сработала. 3. Сетевой администратор хочет проверить наличие связи на 2	3

	уровне. 4. Сетевой администратор хочет определить, можно ли установить соединение из сети, подключённой не напрямую.	
49	Зачем сетевой администратор ввёл на маршрутизаторе команду **show cdp neighbors**? 1. для отображения состояния строки и другой информации об устройствах Cisco с прямым подключением 2. для отображения идентификатора устройства и другой информации об устройствах Cisco с прямым подключением 3. для отображения таблицы маршрутизации и другой информации об устройствах Cisco с прямым подключением 4. для отображения идентификатора маршрутизатора и другой информации о соседних устройствах OSPF	2
50	Какое утверждение о CDP на устройстве Cisco является верным? 1. Поскольку он функционирует на канальном уровне, протокол CDP можно использовать только в коммутаторах. 2. Чтобы отключить протокол CDP, в режиме конфигурации интерфейса нужно использовать команду **no cdp enable**. 3. CDP может быть отключён во всей сети или в определённом интерфейсе. 4. Команда **show cdp neighbour** отображает соседний IP-адрес, но лишь при соединении на уровне 3.	3
51	Системный администратор обновляет образ ОС Cisco IOS на маршрутизаторе 2900 серии ISR. С помощью какой команды он может проверить общий и доступный на текущий момент объём флеш-памяти? **1. show flash0:** **2. show interfaces** **3. show startup-config** 4. **show version**	1
52	Системный администратор рассматривает модель сети, в которой используется маршрутизатор корпоративного класса с фиксированной конфигурацией, поддерживающий как LAN-, так WAN-подключения. Однако администратор понимает, что в маршрутизаторе недостаточно интерфейсов для расширения и увеличения сети. Какой тип устройства следует использовать в качестве замены? 1. дополнительный маршрутизатор с фиксированной конфигурацией 2. коммутатор 3-го уровня 3. устройство PoE 4. модульный маршрутизатор	4
53	В каком из утверждений отражены особенности коммутаторов Cisco Meraki? 1. Это коммутаторы для поставщиков услуг с возможностью агрегирования трафика на границах сети. 2. Это коммутаторы доступа с управлением в облачной среде, обеспечивающие возможность виртуального стекирования коммутаторов.	2

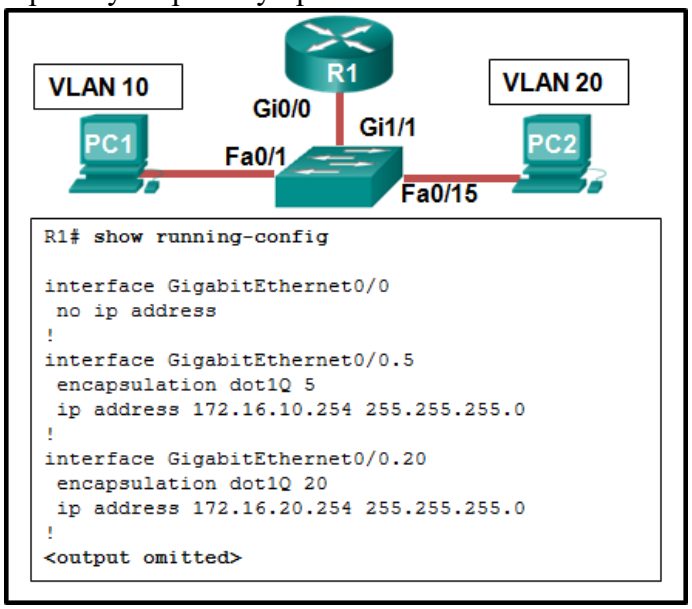
	3. Они обеспечивают масштабируемость инфраструктуры, бесперебойную работу и гибкость транспортных решений. 4. Это коммутаторы для локальных сетей с теми же функциями, что и у коммутаторов Cisco 2960.	
54	Назовите свойство оборудования корпоративного класса, поддерживающее корпоративную сеть в исправном состоянии на протяжении 99,999% рабочего времени? (Выберите два варианта.) 1. домены возникновения сбоя 2. уровень вырожденного ядра 3. аварийное переключение 4. резервные источники питания 5. модуль служб	3, 4
55	Какие функции обеспечивают специализированные встроенные микросхемы в многоуровневых коммутаторах? 1. агрегация физических портов в один логический интерфейс 2. защита трафика в случае отказа канала 3. пересылка IP-пакетов без обращения к ЦП 4. аутентификация и авторизация пользователей	3
56	Назовите отличительную характеристику внутриполосного управления устройствами. 1. Используется для начальной конфигурации или в случаях, когда сетевое подключение недоступно. 2. Использует прямое подключение к консоли или вспомогательному порту. 3. Используется для мониторинга и внесения изменений в конфигурацию сетевых устройств при помощи сетевых подключений. 4. Использует клиент эмуляции терминала.	3
57	Посмотрите на изображение. Какие устройства имеются в домене возникновения ошибки после отключения коммутатора S3 от источника питания?  1. S1 и S4 2. PC_3 и AP_2 3. S4 и PC_2	0A

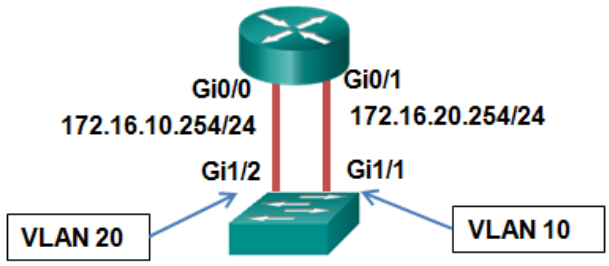
	4. AP_2 и AP_1 5. PC_3 и PC_2	
58	Посмотрите на изображение. Какая команда, выполненная на коммутаторе Cisco, привела к выводу этих данных? <выходные данные опущены> Vlan MAC Address Type Ports Remaining Age (mins) 1 0025.83a6.4b01 SecureDynamic Fa0/18 - 1 0025.83a6.4b02 SecureSticky Fa0/19 - 1. **show vlan summary** 2. **show port-security address** 3. **show mac-address-table** 4. **show vlan brief**	2
59	Какие требования обязательно необходимо учитывать при использовании управления in-band (через общий канал) устройствами для настройки сетевого устройства? (Выберите два варианта.) 1. прямое подключение к консольному порту 2. использование протоколов Telnet, SSH и HTTP для доступа к устройству 3. прямое подключение к вспомогательному порту 4. клиент эмуляции терминала 5. по крайней мере один сетевой интерфейс должен быть подключён и функционален	2, 5
60	Назовите свойства коммутатора уровня доступа, принимаемые во внимание при разработке сети? (Выберите три варианта.) 1. аварийное переключение 2. плотность портов 3. питание через Ethernet 4. скорость конвергенции 5. ограничение широковещательного трафика 6. скорость передачи трафика	2, 3, 6
61	Сопоставьте цели соответствующему элементу конфигурации. (Не все варианты используются.) идентификация безопасность сквозное доступ к удалённым сетям • **присвоение IP-адреса интерфейсу** - доступ к удалённым сетям • **инкапсуляция** - сквозное • **имя узла** – идентификация • **пароли** - безопасность • **протоколы маршрутизации**	
62	В каком случае сетевой администратор установит коммутатор Cisco Nexus или Cisco Catalyst 6500 для стимулирования масштабируемо-	4

	сти инфраструктуры? 1. в сети поставщика услуг для повышения уровня встроенной системы безопасности и упрощения управления 2. в локальной сети комплекса зданий в качестве коммутаторов уровня доступа 3. чтобы обеспечить виртуальное стекирование коммутаторов для получения доступа к управлению в облачной среде 4. в сети центра обработки данных для обеспечения расширения и гибкости транспортных решений	
63	Какое свойство модели ограничит размер домена возникновения ошибки в корпоративной сети? 1. использование развертывания сети с объединением уровней ядра и распределения 2. использование метода создания блока коммутаторов 3. установка резервных источников питания 4. приобретение оборудования корпоративного класса, разработанного для больших объёмов трафика	2
64	Сразу после загрузки маршрутизатора сетевой администратор планирует проверить настройки маршрутизаторов. Какую из следующих команд, вызываемых из привилегированного режима, может применить администратор для этой цели? (Выберите два варианта.) **1. show startup-config** **2. show NVRAM** **3. show running-config** **4. show flash** 5. **show version**	1
65	Техническому специалисту по сетям необходимо подключить компьютер к сетевому устройству для исходной конфигурации. Что необходимо для настройки конфигурации этого устройства? 1. доступ по протоколу Telnet 2. доступ HTTP 3. клиент с поддержкой эмуляции терминала. 4. как минимум один рабочий сетевой интерфейс устройства	3
66	Назовите функции маршрутизатора. (Выберите два варианта.) 1. Связь нескольких IP-сетей. 2. Определение лучшего пути для отправки пакетов. 3. Управление потоком данных с помощью адресов 2-го уровня. 4. Увеличение размера широковещательного домена. 5. Управление базой данных VLAN.	1, 2
67	Назовите преимущества расширения уровня доступа подключения пользователей через беспроводную среду? (Выберите два варианта.) 1. снижение расходов 2. повышенная гибкость 3. снижение количества критических точек отказа 4. улучшенные варианты управления сетями 5. улучшенная пропускная способность	1, 2
68	Какой тип информации отображается командой **show ip protocols**, которая выдается из приглашения ко вводу команды маршрутизато-	3

	ра? 1. включенный маршрутизируемый протокол и состояние протокола интерфейсов 2. информация об интерфейсе, в том числе о том, включена ли ACL на этом интерфейсе 3. настроенные протоколы маршрутизации и сети, которые объявляет маршрутизатор 4. интерфейсы с данными со строкой о состоянии (протокола) и статистике ввода-вывода	
69	Наличие каких функций предполагается у современных корпоративных сетей? (Выберите два варианта.) 1. поддержка трафика объединённой сети 2. поддержка важнейших приложений 3. поддержка распределённого административного управления 4. поддержка ограниченного роста 5. поддержка 90% надёжности	1, 2
70	Какой элемент проектирования сети может уменьшить последствия отдельных неполадок для всей сети? 1. установка в сети только оборудования корпоративного класса 2. настройка всех устройств одного уровня доступа на использование одного шлюза 3. развертывание коммутаторов уровня распределения парами и разделение переключаемых соединений данного уровня доступа между ними 4. сокращение количества резервных устройств и соединений в ядре сети	3
71	Какое утверждение описывает отличительную черту коммутаторов Cisco Catalyst 2960? 1. Они не поддерживают активный коммутируемый виртуальный интерфейс (SVI) с операционной системой IOS версий до 15.x. 2. Это модульные коммутаторы. 3. Новые коммутаторы Cisco Catalyst 2960-C поддерживают сквозной доступ PoE. 4. Они более всего подходят для применения в качестве коммутаторов уровня распределения.	3
72	Взгляните на рисунок. Между сетями VLAN нет связи. В чём может быть причина? 	4

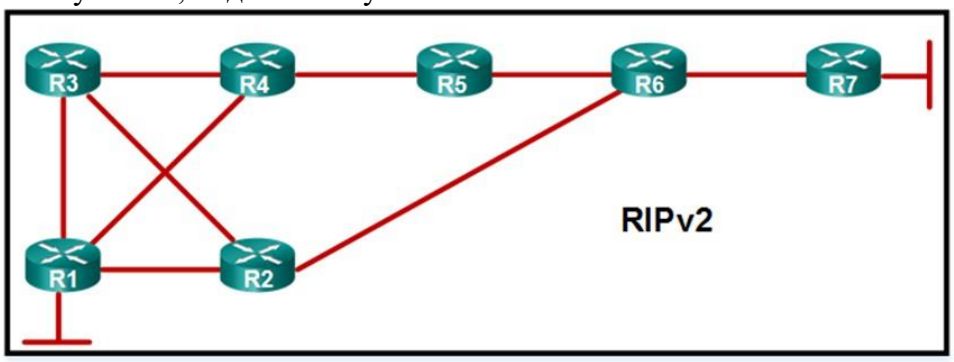
	1. Для каждой сети VLAN не были настроены шлюзы по умолчанию. 2. На маршрутизаторе использован неверный порт. 3. Между коммутатором и маршрутизатором возникла проблема выбора дуплексного режима. 4. Порт коммутатора Gi1/1 работает не в режиме магистрального канала.	
73	Посмотрите на изображение. Конфигурация router-on-a-stick реализована для сетей VLAN 15, 30 и 45, что видно из результатов выполнения команды show running-config. У компьютеров в сети VLAN 45, использующих сеть 172.16.45.0 /24, возникают проблемы при подключении к компьютерам в сети VLAN 30 в рамках сети 172.16.30.0 /24. Какая ошибка вероятнее всего вызвала эту проблему? **<анные опущены>** ! interface GigabitEthernet0/0 no ip address duplex auto speed auto ! interface GigabitEthernet0/0.15 encapsulation dot1Q 15 ip address 172.16.15.254 255.255.255.0 ! interface GigabitEthernet0/0.30 encapsulation dot1Q 30 ip address 172.16.3.254 255.255.255.0 ! interface GigabitEthernet0/0.45 encapsulation dot1Q 45 ip address 172.16.45.254 255.255.255.0 ! **<анные опущены>** 1. Интерфейсу GigabitEthernet 0/0 не назначен IP-адрес. 2. Для субинтерфейса GigabitEthernet 0/0.30 настроен неправильный IP-адрес. 3. На интерфейсе GigabitEthernet 0/0.30 не использована команда **no shutdown**. 4. На интерфейсе GigabitEthernet 0/0.45 настроена неправильная сеть VLAN.	2
74	Где файл vlan.dat сохраняется на коммутаторе? 1. в NVRAM 2. в ОЗУ 3. во флеш-памяти 4. на внешнем носителе или внутреннем жестком диске	3
75	Какая команда отображает для интерфейса Fa0/1 тип инкапсуляции, идентификатор голосовой VLAN и сеть VLAN режима доступа? **1. show vlan brief** **2. show interfaces trunk**	3

	3. **show interfaces Fa0/1 switchport** 4. **show mac address-table interface Fa0/1**	
76	В чём заключается недостаток использования многоуровневых коммутаторов для маршрутизации между сетями VLAN? 1. Многоуровневые коммутаторы дороже, чем реализация модели router-on-a-stick. 2. На многоуровневом коммутаторе для маршрутизации необходимо отключить протокол spanning tree. 3. Для многоуровневых коммутаторов характерна более высокая задержка при маршрутизации уровня 3. 4. Многоуровневые коммутаторы могут использовать для маршрутизации уровня 3 только магистральные каналы.	1
77	Взгляните на рисунок. Сетевой администратор проверяет конфигурацию маршрутизации между VLAN. Пользователи недовольны тем, что компьютер PC2 не может обмениваться данными с компьютером PC1. Исходя из показанных результатов, укажите наиболее вероятную причину проблемы.  1. Для субинтерфейсов не введена команда no shutdown. 2. Команда interface GigabitEthernet0/0.5 была введена неправильно. 3. Команда encapsulation dot1Q 5 содержит неверную VLAN. 4. Gi0/0 не настроен как магистральный порт. 5. Для интерфейса Gi0/0 не настроен IP-адрес.	3
78	Посмотрите на изображение. Администратор сети настраивает маршрутизацию между VLAN. Однако связь между VLAN 10 и VLAN 20 не устанавливается. На какую причину проблемы указывают результаты работы команды **show vlan**?	3

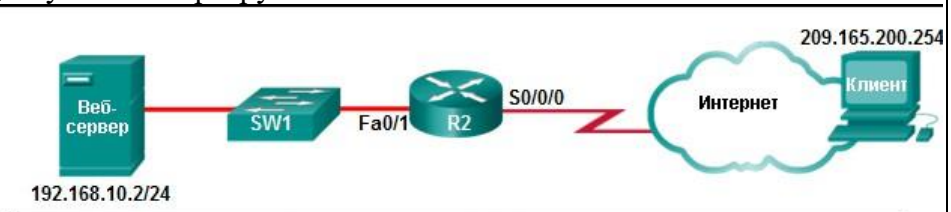
	
	`Switch# show vlan`
	
	`VLAN Name Status Ports`
	`---- ---------- --------- ----------`
	`1 default active Gig1/1, Gig1/2`
	`10 VLAN0010 active Fa0/1, Fa0/2, Fa0/3, Fa0/4`
	`Fa0/5, Fa0/6, Fa0/7, Fa0/8`
	`Fa0/9, Fa0/10, Fa0/11, Fa0/12`
	`20 VLAN0020 active Fa0/13, Fa0/14, Fa0/15, Fa0/16`
	`Fa0/17, Fa0/18, Fa0/19, Fa0/20`
	`Fa0/21, Fa0/22, Fa0/23, Fa0/24`
	
	`<выходные данные опущены>`
	
	1. На Gi1/1 и Gi1/2 не настроен магистральный режим.
	2. IP-адреса на Gi0/0 и Gi0/1 отключены по ошибке.
	3. Gi1/1 и Gi1/2 не назначены соответствующим VLAN.
	4. IP-адреса на Gi0/0 и Gi0/1 находятся в разных сетях.	

79	Как влияет архитектура IP-адресации на реализацию VLAN? 1. Сети VLAN не используют адреса трансляции. 2. Каждой сети VLAN необходима другая маска подсети. 3. Каждой сети VLAN необходим другой номер сети. 4. Сети VLAN не поддерживают VLSM.	3
80	Где на коммутаторе Cisco хранятся данные VLAN расширенного диапазона? 1. файл текущей конфигурации 2. Энергонезависимая память (NVRAM) 3. флеш-память 4. файл загрузочной конфигурации	1

81	Взгляните на рисунок. После попытки входа в конфигурацию, показанную в RTA маршрутизатора, администратор получает сообщение об ошибке, а пользователи сети VLAN 20 сообщают, что не могут связаться с пользователями VLAN 30. В чём причина проблемы?
	`RTA# configure terminal`
	`RTA(config)# interface Fa0/0`
	`RTA(config-if)# no shutdown`
	`RTA(config-if)# interface Fa0/0.10`
	`RTA(config-subif)# encapsulation dot1q 10`
	`RTA(config-subif)# ip address 192.168.3.30 255.255.255.224`
	`RTA(config-subif)# interface Fa0/0.20`
	`RTA(config-subif)# encapsulation dot1q 20`
	`RTA(config-subif)# ip address 192.168.3.49 255.255.255.224`
	`RTA(config-subif)# interface Fa0/0.30`
	`RTA(config-subif)# encapsulation dot1q 30`
	`RTA(config-subif)# ip address 192.168.3.62 255.255.255.224`
	
	1. Для Fa0/0.20 и Fa0/0.30 нужно было выполнить команду no
		3

	shutdown. 2. Dot1q не поддерживает субинтерфейсы. 3. RTA использует одну и ту же подсеть для сетей VLAN 20 и VLAN 30. 4. Ни один адрес из Fa0/0 нельзя использовать в качестве шлюза по умолчанию.	
82	Что является результатом «широковещательного шторма» 2-го уровня? 1. Широковещательные запросы ARP будут возвращаться на передающий узел. 2. Новый трафик будет отброшен коммутатором из-за отсутствия возможности его обработки. 3. Маршрутизаторы начнут пересылать кадры из-за перегрузки коммутаторов. **4.** CSMA/CD заставит каждый узел продолжать передачу кадров.	2
83	Выберите 2 протокола маршрутизации, которые относятся к дистанционно-векторным протоколам. (Выберите два варианта.) 1. OSPF 2. EIGRP 3. BGP 4. RIP 5. IS-IS	2, 4
84	Какой протокол маршрутизации отправляет обновление маршрутизации соседним маршрутизаторам каждые 30 секунд? 1. RIP 2. EIGRP 3. OSPF 4. BGP	1
85	Посмотрите на изображение. Сетевой администратор настроил в данной топологии протокол RIPv2. Какой путь должен выбрать пакет, чтобы попасть из локальной сети, подключенной к R1, в локальную сеть, подключенную к R7?  1. R1--R2--R6--R7 2. R1--R3--R4--R5--R6--R7 3. R1--R3--R2--R6--R7 4. R1--R4--R5--R6--R7	1
86	Как определяется время сходимости в контексте протоколов маршрутизации?	2

	1. Возможность передачи данных, видео и голоса по одной среде. 2. Время, необходимое для согласования таблиц маршрутизации после изменения топологии. 3. Мера сложности конфигурации протоколов. 4. Время, необходимое сетевому администратору для настройки протокола маршрутизации в сетях малого и среднего размера.	
87	В чём состоит отличие протоколов внутренней и внешней маршрутизации? 1. Протоколы внутренней маршрутизации используются для обмена данными в пределах одной автономной системы. Протоколы внешней маршрутизации используются для обмена данными между несколькими автономными системами. 2. Протоколы внутренней маршрутизации используются для маршрутизации в сети Интернет. Протоколы внешней маршрутизации используются в пределах организаций. 3. Протоколы внешней маршрутизации используются только крупными интернет-провайдерами. Протоколы внутренней маршрутизации используются небольшими интернет-провайдерами. 4. Протоколы внешней маршрутизации используются для администрирования одной автономной системы. Внутренние протоколы маршрутизации используются для администрирования нескольких доменов.	1
88	Сопоставьте характеристики протоколов на основе состояния каналов с их преимуществами и недостатками. (**Не все варианты используются.)** Использование пропускной способности. Управляемые событиями обновления. **Использование числа переходов в качестве метрики.** Создание топологической схемы. Использование памяти. Быстрая сходимость. **Отправка обновлений с широковещательной адресацией.** Время обработки на ЦП. <u>Преимущества</u> Создание топологической схемы. Быстрая сходимость. Управляемые событиями обновления. <u>Недостатки</u> Время обработки на ЦП. Использование памяти. Использование пропускной способности	1, 2
89	Укажите 2 цели протоколов динамической маршрутизации. (Выберите два варианта.) 1. уменьшение сетевого трафика	3, 4

	2. обеспечение безопасности сети 3. выбор оптимального пути к сетям назначения 4. обнаружение удаленных сетей 5. создание маршрута по умолчанию для сетевых хостов	
90	Какая функция обеспечивает безопасные обновления маршрутизации между соседними устройствами RIPv2? 1. keepalive-сообщения 2. одноадресные обновления 3. таблица смежности 4. проверка подлинности протокола маршрутизации	4
91	Какой протокол динамической маршрутизации был разработан как протокол внешнего шлюза для соединения различных интернет-провайдеров? 1. OSPF 2. EIGRP 3. RIP 4. BGP	4
92	Каково основное преимущество использования NAT с преобразованием адресов портов? 1. Предоставление пула публичных адресов, которые могут быть назначены внутренним хостам. 2. Совместное использование одного общедоступного IPv4-адреса множеством внутренних хостов. 3. Повышение производительности сети для протоколов реального времени. 4. Предоставление внешним хостам доступ к внутренним серверам.	2
93	Взгляните на рисунок. Сетевой специалист настраивает маршрутизатор R2 для использования статического преобразования NAT, чтобы предоставить клиенту доступ к веб-серверу. Назовите возможную причину того, что клиентский компьютер не может получить доступ к веб-серверу.  R2(config)# ip nat inside source static 192.168.10.2 209.165.201.5 R2(config)# interface Fa0/1 R2(config-if)# ip address 192.168.10.254 255.255.255.0 R2(config-if)# ip nat inside R2(config-if)# exit R2(config)# interface Serial0/0/0 R2(config-if)# ip address 209.165.200.225 255.255.255.224 1. Неправильная инструкция IP NAT. 2. В конфигурации отсутствует правильный список управления доступом. 3. В качестве внешнего интерфейса NAT должен быть указан интерфейс Fa0/1. 4. В качестве внешнего интерфейса NAT должен быть указан	4

	интерфейс S0/0/0.	
94	В чем заключается преимущество развертывания технологии IPv4 NAT для внутренних хостов в организации? 1. обеспечивает гибкость при проектировании схемы адресации IPv4 2. позволяет упростить развертывание приложений, требующих сквозной трассировки 3. повышает производительность передачи данных в Интернет 4. упрощает доступ к внутренней сети для внешних хостов с использованием UDP	1
95	Посмотрите на изображение. Какой адрес или адреса являются внутренними глобальными адресами? Router1 (config)# **ip nat inside source static 192.168.0.100 209.165.20.2** Router1 (config)# **interface serial0/0/0** Router1 (config-if)# **ip nat inside** Router1 (config-if)# **ip address 10.1.1.2 255.255.255.0** Router1 (config)# **interface serial 0/0/2** Router1 (config-if)# **ip address 209.165.20.25 255.255.255.0** Router1 (config-if)# **ip nat outside** 1. 10.1.1.2 2. 192.168.0.100 3. 209.165.20.25 4. любой адрес в пределах сети 10.1.1.0	3
96	Какие два действия необходимо предпринять для настройки PAT? (Выберите два варианта ответа.) 1. Определить диапазон портов источника, который необходимо использовать. 2. Создать стандартный список доступа для определения приложений, которые необходимо преобразовывать. 3. Определить пул глобальных адресов, которые будет использоваться для преобразования с перегрузкой. 4. Определить таймеры для сообщений-приветствий и интервалов для сопоставления с соседним маршрутизатором. 5. Определить внутренний интерфейс.	3 5
97	Если используется динамическое преобразование NAT без перегрузки, что произойдет, если семь пользователей попытаются получить доступ к публичному серверу в Интернете, когда в пуле NAT доступно только шесть адресов? 1. Ни один из пользователей не сможет получить доступ к серверу. 2. Все пользователи смогут получить доступ к серверу. 3. Седьмой пользователь не сможет отправить запрос к серверу. 4. Когда седьмой пользователь отправит запрос, первый пользователь будет отсоединён.	3
98	Сопоставьте шаги и действия, необходимые, когда внутренний узел с IP-адресом 192.168.10.10 пытается отправить пакет внешнему серверу с IP-адресом 209.165.200.254 через маршрутизатор R1, на кото-	

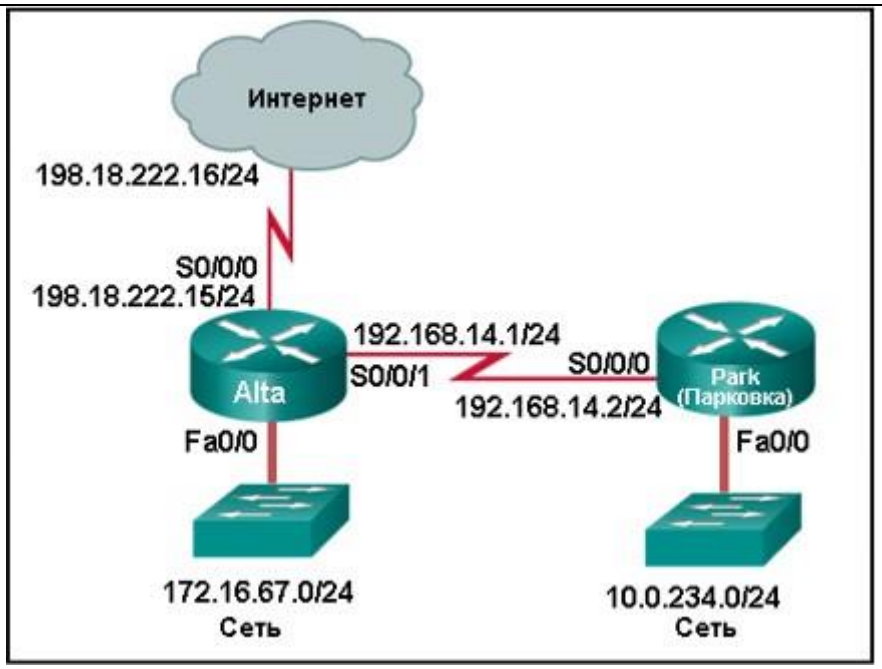
	ром работает динамическое преобразование NAT. (Не все варианты используются.) Шаг 1 Шаг 2 Шаг 3 Шаг 4 Шаг 5 • **Маршрутизатор R1 преобразует IP-адрес в пакетах с 209.65.200.254 на 192.168.10.10.** • **Маршрутизатор R1 заменяет адрес 192.168.10.10 на преобразованный внутренний глобальный адрес** - Шаг 5 • **Маршрутизатор R1 проверяет конфигурацию NAT, чтобы определить, нужно ли преобразовывать этот пакет** - Шаг 2 • **Маршрутизатор R1 выбирает доступный глобальный адрес из пула динамических адресов** - Шаг 4 • **Узел отправляет пакеты, которые запрашивают соединение с сервером, по адресу 209.165.200.254** - Шаг 1 • **Если для этого IP-адреса нет записи преобразования, маршрутизатор R1 решает, что должен быть преобразован адрес источника 192.168.10.10** - Шаг 3	
99	Какой метод используется маршрутизатором с поддержкой PAT для отправки входящих пакетов соответствующим внутренним узлам? 1. Номер TCP- или UDP-порта назначения из входящего пакета. 2. IP-адрес источника из входящего пакета. 3. Комбинация TCP- или UDP-порта источника и IP-адреса назначения из входящего пакета. 4. Номер TCP- или UDP-порта источника из входящего пакета.	1
100	В чем состоит основное назначение преобразования NAT? 1. повышение безопасности сети 2. обеспечение обмена файлами между одноранговыми устройствами 3. повышение производительности сети 4. экономия IPv4-адресов	4
101	Сетевой инженер настроил маршрутизатор с помощью команды **ip nat inside source list 4 pool corp overload**. Почему инженер использовал параметр overload? 1. Маршрутизатор компании должен ограничивать или буферизировать трафик, поскольку производительность маршрутизатора недостаточна для обработки нормальной нагрузки внешнего интернет-трафика. 2. Компании нужно больше доступных публичных IP-адресов для использования в Интернете. 3. В компании число частных IP-адресов превышает число доступных публичных IP-адресов. 4. В компании мало серверов, которые должны быть доступны для клиентов из Интернета.	3
102	Чем характерны уникальные локальные адреса?	3

	1. Их реализация зависит от интернет-провайдеров, предоставляющих услугу. 2. Они разработаны для повышения уровня безопасности IPv6-сетей. 3. Они позволяют объединять объекты, не создавая конфликтов адресов. 4. Они определены в документе RFC 3927.	
103	Сетевой администратор настраивает пограничный маршрутизатор с помощью команды R1(config)# **ip nat inside source list 4 pool corp**. Что нужно настроить для работоспособности этой конкретной команды? 1. Список доступа под номером 4, который определяет начальный и конечный публичные IP-адреса. 2. Список доступа с именем corp, определяющий частные адреса, на которые влияет NAT. 3. Включённая и активная сеть VLAN с именем corp, маршрутизируемая маршрутизатором R1. 4. Пул NAT с именем corp, который определяет начальный и конечный публичные IP-адреса. 5. Выполнить команду **ip nat outside** для интерфейса, подключённого к локальной сети, на которую влияет NAT.	4
104	Укажите два преимущества использования преобразования сетевых адресов (NAT). (Выберите два варианта ответа.) 1. NAT упрощает туннелирование с помощью IPsec. 2. NAT упрощает диагностику и устранение неполадок при маршрутизации. 3. NAT позволяет экономить публичные IP-адреса. 4. NAT обеспечивает повышенный уровень конфиденциальности и безопасности сети. 5. NAT повышает производительность маршрутизации.	3, 4
105	Для чего предназначена переадресация портов? 1. Переадресация портов обеспечивает преобразование внутренних локальных IP-адресов во внешние локальные адреса. 2. Переадресация портов позволяет внутренним пользователям получить доступ к службе с публичным IPv4-адресом, находящимся вне локальной сети. 3. Переадресация портов позволяет пользователям получить доступ к серверам в Интернете, не использующим стандартные номера портов. 4. Переадресация портов позволяет внешним пользователям получить доступ к службе с частным IPv4-адресом, находящимся в локальной сети.	4
106	Какое утверждение описывает адреса ULA в протоколе IPv6? 1. Они назначаются интернет-провайдером. 2. Они не маршрутизируются в Интернете. 3. Они экономят пространство IPv6-адресов. 4. Они начинаются с префикса fe80::/10.	2
107	Сетевой администратор настраивает статическое преобразование	3

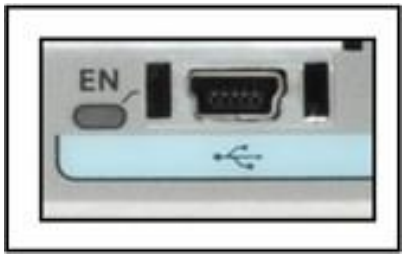
	NAT на граничном маршрутизаторе для веб-сервера в сети DMZ. Веб-сервер настроен на прослушивание TCP-порта 8080. Веб-сервер используется в паре с внутренним IP-адресом 192.168.5.25 и внешним IP-адресом 209.165.200.230. Чтобы упростить доступ к веб-серверу хостов из Интернета, внешним пользователям не требуется указывать порт. Какая команда позволяет настроить статическое преобразование NAT? **1.** R1(config)# **ip nat inside source static tcp 209.165.200.230 8080 192.168.5.25 80** **2.** R1(config)# **ip nat inside source static tcp 192.168.5.25 80 209.165.200.230 8080** 3. R1(config)# **ip nat inside source static tcp 192.168.5.25 8080 209.165.200.230 80** 4. R1(config)# **ip nat inside source static tcp 209.165.200.230 80 192.168.5.25 8080**	
107	В чём заключается недостаток NAT? 1. Внутренние узлы должны использовать один IPv4-адрес для внешнего обмена данными. 2. Стоимости переадресации узлов могут быть высокими для сети с публичной адресацией. 3. Маршрутизатору не нужно изменять контрольную сумму IPv4-пакетов. 4. Нет сквозной адресации.	4
108	Техническому специалисту необходимо настроить граничный маршрутизатор для использования разных номеров портов TCP при каждом сеансе связи с сервером в Интернете. Какой тип преобразования сетевых адресов (NAT) следует реализовать? 1. сопоставление локальных и глобальных адресов по схеме «многие к одному» 2. сопоставление локальных и глобальных адресов по схеме «многие ко многим» 3. сопоставление локальных и глобальных адресов по схеме «один к одному» 4. сопоставление локальных и глобальных адресов по схеме «один ко многим»	1
109	Что определяет команда **ip nat pool** при настройке динамического преобразования NAT? 1. пул глобальных адресов 2. пул доступных серверов NAT 3. диапазон внутренних IP-адресов для преобразования 4. диапазон внешних IP-адресов, к которым внутренние хосты имеют доступ	1

110	Взгляните на рисунок. Исходя из показанного результата, какой тип NAT реализован?
	`R1# show ip nat translations`
	`Pro Inside global Inside local Outside local Outside global`
	`tcp 209.165.200.225:1405 10.6.15.2:1405 209.165.202.141:80 209.165.202.14`
	`tcp 209.165.200.225:1406 10.6.15.1:1406 198.51.100.3:80 198.51.100.3:8`
		1

	1. PAT с использованием внешнего интерфейса. 2. Статическое NAT с пулом NAT. 3. Динамическое NAT с пулом из двух публичных IP-адресов. 4. Статическое NAT с одной записью.	
111	Какая команда позволяет создать допустимый маршрут IPv6 по умолчанию? 1. ipv6 route ::/0 fe80::1 2. ipv6 route 2001:db8:acad:1::/64::1 3. ipv6 route ::/0 2001:db8:acad:2::a 4. ipv6 route ::/128 2001:db8:acad:1:1	3
112	Системный администратор замечает, что правильно указанный статический маршрут отсутствует в таблице маршрутизации. Какие две команды маршрутизатора следует определить, был ли включен выходной интерфейс и доступен адрес следующего перехода? (Выберите два варианта). **1. ping** **2. show ip protocols** **3. show ip interface brief** **4. show ip route** 5. **tracert**	1, 3
113	С какой целью на маршрутизаторе настраивается суммарный статический маршрут? 1. чтобы сократить число публичных IP-адресов, требуемых для организации 2. чтобы обеспечить лучший маршрут, чем предоставляет конкретный протокол маршрутизации 3. чтобы предоставить шлюз по умолчанию для маршрутизатора, используемого для соединения с интернет-провайдером 4. чтобы уменьшить размер таблицы маршрутизации 5. чтобы уменьшить размер обновления протокола маршрутизации для соседнего маршрутизатора	4
114	Взгляните на рисунок. Какой набор команд используется для настройки статических маршрутов, позволяющих маршрутизаторам Park и Alta а) пересылать пакеты во все локальные сети и б) направлять весь остальной трафик в сеть Интернет?	1

	 1. Park(config)#ip route 0.0.0.0 0.0.0.0 192.168.14.1 Alta(config)#ip route 10.0.234.0 255.255.255.0 192.168.14.2 Alta(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 2. Park(config)#ip route 0.0.0.0 0.0.0.0 192.168.14.1 Alta(config)#ip route 10.0.234.0 255.255.255.0 192.168.14.2 Alta(config)#ip route 198.18.222.0 255.255.255.255 s0/0/0 3. Park(config)#ip route 17.16.67.0 255.255.255.0 192.168.14.1 Alta(config)#ip route 0.0.0.0 0.0.0.0 192.168.14.1 Alta(config)#ip route 10.0.234.0 255.255.255.0 192.168.14.2 4. Park(config)#ip route 172.16.67.0 255.255255.0 192.168.14.1 Alta(config)#ip route 10.0.234.0 255.255.255.0 192.168.14.2 Alta(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0	
115	Дана команда: **ip route 192.168.100.0 255.255.255.0 10.10.10.5** Какой маршрут должен стать недоступным, чтобы указанный статический маршрут появился в таблице маршрутизации? 1. маршрут по умолчанию 2. статический маршрут к сети 192.168.10.0/24 3. маршрут к сети 192.168.10.0/24, полученный динамически при помощи протокола OSPF 4. маршрут к сети 192.168.10.0/24, полученный динамически при помощи протокола EIGRP	3
116	Какой оператор статического маршрута отображает рекурсивный статический маршрут IPv67 **1. ipv6 route 0::0/0 s0/0/0**	4

	2. ipv6 route 0::0/0 s0/0/254 **3. ipv6 route 2001:db8:cafe:1::/56 s0/0/0** **4. ipv6 route 2001:db8:cafe:1::/56 2001:db8:1000::10:1** 5. **ipv6 route 2001:db8:cafe:1::/56 s0/0/0 2001:db8:1000::10:1**	
117	Какую комбинацию сетевого адреса и маски подсети необходимо использовать для создания статического маршрута по умолчанию, который подходит для любого адреса назначения IPv4? 1. 0.0.0.0 0.0.0.0 2. 0.0.0.0 255.255.255.255 3. 255.255.255.255 255.255.255.255 4. 255.255.255.255 0.0.0.0	
118	Статический маршрут какого типа создается при указании IP-адреса следующего перехода и выходного интерфейса? 1. Рекурсивный статический маршрут 2. Статический маршрут с прямым подключением 3. Полностью определенный статический маршрут 4. Плавающий статический маршрут	3
119	Сетевой администратор вводит на маршрутизаторе Router1 следующую команду **ip route 192.168.0.0 255.255.255.0 s0/1/0/.** Затем маршрутизатор получает пакет, отправленный на адрес 192.168.0.22/24. Каковы будут дальнейшие действия маршрутизатора по обработке пакета после обнаружения в таблице маршрутизации недавно настроенного статического маршрута? 1. Пропуск пакета, так как в таблице маршрутизации отсутствует узел назначения 2. Поиск MAC-адреса интерфейса S0/1/0 для определения MAC-адреса места назначения нового кадра 3. Рекурсивный поиск IP-адреса интерфейса S0/1/0 перед пересылкой ракета 4. Инкапсуляция пакета в кадр для канала сети WAN и отправка пакета из интерфейса S0/1/0	4
120	Заполните пустое поле Сеть _____ - это сеть, доступ к которой осуществляется по одному маршруту. (англоязычный термин).	stub
121	По каким двум причинам администратор мог бы применить статическую маршрутизацию вместо динамической? (Выберите два варианта). 1. Статическая маршрутизация упрощает управление маршрутами в больших сетях. 2. Статическая маршрутизация безопаснее 3. Статическая маршрутизация упрощает масштабирование 4. Статическая маршрутизация не создает дополнительной нагрузки на вычислительные ресурсы маршрутизатора и подразумевает меньший объем служебного трафика 5. Статическая маршрутизация не требует полного представления о топологии сети	2, 4
122	Что является характеристикой статического маршрута по умолчанию?	3

	1. Создает резервную копию маршрута, ранее обнаруженного при помощи протокола динамической маршрутизации 2. Использует один сетевой адрес для отправки нескольких статических маршрутов одному адресу назначения 3. Идентифицирует IP-адрес шлюза, куда маршрутизатор отправляет все IP-пакеты, для которых нет динамического или статического маршрута 4. Настраивается с более высоким значением административного расстояния, чем значение административного расстояния исходного протокола динамической маршрутизации	
123	Какая команда или набор команд используются для проверки правильности работы на маршрутизаторе HQ следующей конфигурации **1. ip route 0.0.0.0 0.0.0.0 serial 0/0/0 10** **ip route 0.0.0.0 0.0.0.0 serial 0/0/0** **2. HQ(config)# interface serial 0/1/0** **HQ(config)# shutdown** **HQ(config)# end** **HQ(config)# show ip route** **3. HQ# traceroute 128.107.0.99** **4. HQ# show ip interface brief** **5. HQ# ping 128.107.0.99** **HQ# ping 64.100.0.5** 6. **HQ# show ip route**	2
124	Для чего служат маршрутизаторы в сети? 1. Для подключения устройств к локальной сети 2. Для гарантированной доставки пакетов 3. Для предоставления данных о состоянии доставки пакета 4. Для перенаправления сетевого трафика в удаленные сети 5. Для маршрутизации информации и получения подтверждения о доставке данных	4
125	Взгляните на рисунок. Каково назначение показанного порта маршрутизатора?  1. Резервное копирование IOS	2

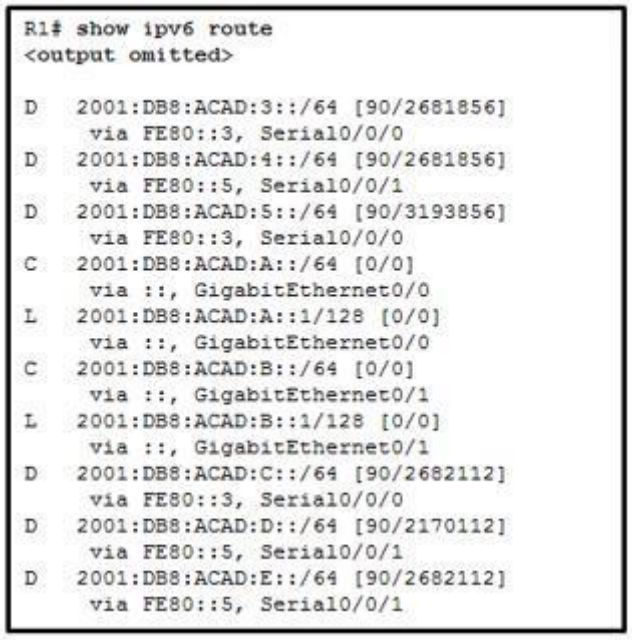
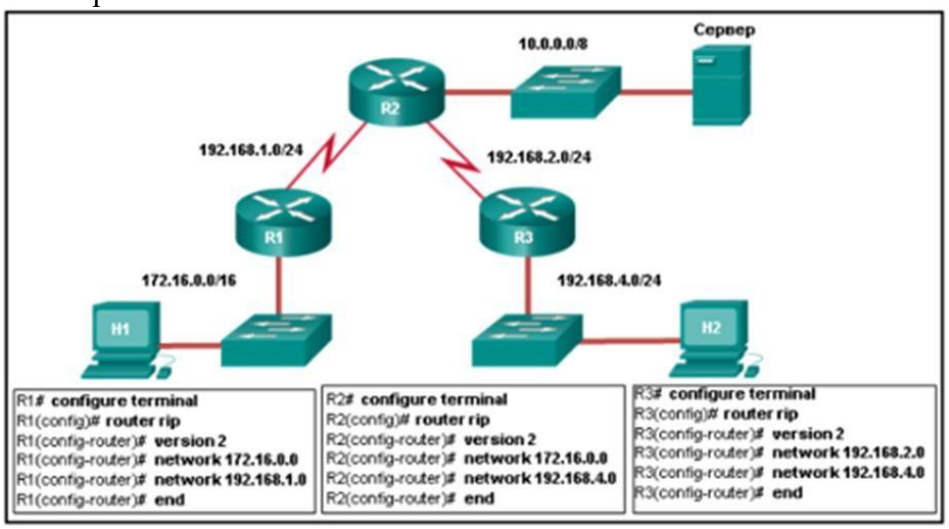
	2. Настройка маршрутизатора 3. Запуск IOS из другого расположения 4. Подключение к порту коммутатора	
126	Какой код используется в таблице маршрутизации для обозначения маршрутов, данные о которых получены с помощью EIGRP? 1. C 2. D 3. L 4. O 5. S	2
127	Какая функция на маршрутизаторе позволяет перенаправлять трафик без определенного маршрута? 1. следующий транзитный участок 2. маршрут по умолчанию (шлюз последней надежды) 3. источник маршрута 4. исходящий интерфейс	2
128	Для чего предназначен протокол маршрутизации? 1. Он используется для создания и ведения таблиц ARP 2. Он предоставляет способ сегментации и повторной сборки пакетов данных 3. Он позволяет администратору разрабатывать схему адресации для сети 4. Он позволяет маршрутизатору обмениваться информацией об известных сетях с другими маршрутизаторами 5. Он предоставляет процедуру кодирования данных в биты и их декодирования для пересылки пакетов.	4
129	Какая длина адреса и префикса используется для настройки статического маршрута IPv6 по умолчанию? 1. ::/0 2. ::1/128 3. 0.0.0.0/0 4. FF02::1/8	1
130	Новый стажер на должность младшего сетевого администратора подключает ноутбук к коммутатору уровня доступа в коммутационном шкафу. После настройки программы эмуляции терминала стажер нажимает клавишу Enter и появляется запрос S1_ATC_E2». Что больше всего подходит для защиты коммутатора? 1. Создайте баннерное сообщение 2. Создайте пароль консоли 3. Введите команду enable secret 4. Используйте команду service password-encryption	2
131	Что такое шлюз последней надежды? 1. IP-адрес другого маршрутизатора 2. IP-адрес интернет-провайдера 3. Термин, описывающий шлюз по умолчанию на физическом узле 4. Адрес отправки отбрасываемых пакетов	1
132	Результат команды show ip route содержит следующую запись:	3

	S 10/2/0/0 [1/0] via 172.16.2.2 Какое значение обозначено цифрой 1 в части [1/0] результата? 1. метрика 2. число переходов 3. административное расстояние 4. идентификатор интерфейса, используемого для доступа к сети	
133	Если маршрутизатор определил, что при использовании одного протокола маршрутизации доступно несколько сетей к пути назначения, какие факторы учитываются маршрутизатором при выборе оптимального пути для пересылки пакета? 1. Наименьшая метрика 2. Порядок путей в таблице маршрутизации 3. Наивысшая пропускная способность существующих интерфейсов 4. Уровень надежности соседних маршрутизаторов	1
134	Какие два утверждения правильно описывают компоненты маршрутизатора? (Выберите два варианта) 1. ОЗУ используется для постоянного хранения конфигурационного файла, используемого при загрузке 2. В ОЗУ хранятся данные диагностики аппаратных модулей 3. В энергонезависимой памяти (NVRAM) хранится резервная копия IOS, используемая при загрузке 4. Содержимое флеш-памяти не теряется при перезагрузке 5. ПЗУ содержит самую полную и последнюю версию IOS 6. Флеш-память содержит команды boot system, которые определяют положение IOS	4
135	Какие два утверждения правильно описывают статические маршруты? (Выберите два варианта). 1. Они создаются в режиме конфигурации интерфейса 2. Они требуют повторной настройки вручную в соответствии с изменениями сети 3. Они автоматически становятся для маршрутизатора шлюзом по умолчанию 4. В таблице маршрутизации они обозначены префиксом США 5. Они автоматически обновляются при каждой перенастройке или закрытии интерфейса	2, 4
136	Как в процессе инкапсуляции ПК определяет, предназначен ли пакет для отправки узлу в удаленной сети? 1. Проверяет наличие MAC-адреса узла назначения в кэше ARP 2. Отправляет DNS-серверу запрос сведений об узле назначения 3. Отправляет широковещательное сообщение в локальный сегмент локальной сети для проверки отклика 4. Выполняет операцию и (AND) для IP-адреса назначения и своей маски подсети	4
137	Посмотрите на изображение. Чему равно значение административного расстояния маршрута для маршрутизатора R1 достижения	4

	IPv6-адреса назначения 2001:DB8:CAFÉ:4::A?
	`R1# show ipv6 route`
	`IPv6 Routing Table - 8 entries`
	`<анные опущены>`
	`S ::/0 [1/0] via 2001:DB8:F00D::A`
	`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`
	`S 2001:DB8:CAFE:2::/64 [1/0] via 2001:DB8:F00D:3::3`
	`O 2001:DB8:CAFE:3::/64 [110/65]via GigabitEthernet0/0, directly connected`
	`R 2001:DB8:CAFE:4::/64 [120/4]via GigabitEthernet0/1, directly connected`
	`C 2001:DB8:F00D::/48 [0/0] via GigabitEthernet0/0, directly connected`
	`L 2001:DB8:F00D::1/128 [0/0] via GigabitEthernet0/0, receive`
	`L FF00::/8 [0/0] via Null0, receive`
	1. 1
	2. 4
	3. 110
	4. 120	

138	Заполните пустое поле. Протоколы _____ используются для динамического обмена данными маршрутизации между маршрутизаторами. (два слова в родительном падеже)	динамической маршрутизации
139	Какой следующий этап процесса поиска маршрутизатора после того, как маршрутизатор определит IPv6-адрес назначения и соответствующий сетевой маршрут 1-го уровня? 1. Проверяются дочерние маршруты 2-го уровня 2. Проверяются суперсетевые маршруты 1-го уровня 3. Маршрутизатор отбрасывает пакет 4. Маршрутизатор перенаправляет пакет	4
140	Заполните пустое поле. В процессе создания и обслуживания крупной сети вы обнаруживаете, что проще настроить _____ маршрутизацию, нежели статическую маршрутизацию (одно слово в винительном падеже)	динамическую
141	Сопоставьте записи таблицы маршрутизации с соответствующими функциями (Используются не все варианты). • **Обозначает способ получения маршрута** - источник маршрута • **Определяет адрес удаленной сети** – сеть назначения • **Определяет значение, заданное для достижения удаленной сети** – метрика • **Определяет достоверность источника информации о маршруте** – административное расстояние • **Определяет выходной интерфейс, который используется для направления пакета в место назначения**	
142	Для чего записи в таблице маршрутизации IP-адресов классифицируются как окончательный маршрут, маршрут уровня 1, родительский маршрут уровня 1 и дочерние маршруты уровня 2? 1. Чтобы обеспечить возможность внедрения протоколов динамической маршрутизации 2. Чтобы объяснить принципы работы таблицы маршрутизации как плоской базы данных 3. Чтобы обеспечить маршрутизаторам возможность реализации видов маршрутизации IPv4 и IPv6	4

	4. Чтобы объяснить принципы работы иерархической структуры таблицы маршрутизации	
143	Сетевой администратор проверяет таблицу маршрутизации RIPv2 и замечает, что несколько подсетей объявлены в отдельных записях. Что может сделать администратор, чтобы настроить маршрутизатор RIPv2 для автоматической группировки нескольких подсетей с прямым подключением в одном операторе network? 1. Используйте команду **passive-interface**. 2. Используйте команду **auto-summary**. 3. Используйте команду **default-information originate**. 4. используйте команду **version 2**.	2
145	Какой тип маршрута имеет сетевой адрес с маской подсети, которая меньше классового эквивалента сети? 1. сетевой маршрут 2. маршрут по умолчанию 3. маршрут суперсети 4. дочерний маршрут	3
146	Какие два кода источника маршрутизации автоматически создаются в таблице маршрутизации при каждой настройке интерфейса маршрутизатора с помощью IP-адреса и его активации? (Выберите два варианта). 1. C 2. O 3. L 4. R 5. D	1, 3
147	Сетевой администратор изучил таблицу маршрутизации маршрутизатора и обратил внимание, что запись для сети назначения 172.16.4.0/24 начинается с буквы D. Что обозначает эта буква? 1. Маршрут к сети 172.16.4.0/24 является непосредственно подключенным 2. Сведения об источнике маршрута получены динамически 3. Это прямой маршрут для пакетов к этой сети 4. Маршрут к этой сети настроен на маршрутизаторе статически.	2
148	Какие две функции выполняет протокол динамической маршрутизации? 1. Ведение таблиц маршрутизации 2. Снижение накладных расходов для маршрутизатора 3. Предотвращение раскрытия конфиденциальной информации 4. Обнаружение сетей 5. Выбор пути, указанного администратором	1, 4
149	Взгляните на рисунок. Какая метрика используется для пересылки пакета данных на IPv6-адрес назначения 2001:DB8:ACAD:E:240:BFF:FTD$:9DD2?	5

	 1. 90 2. 128 3. 2170112 4. 2681856 5. 2682112 6. 3193856	
150	Взгляните на рисунок, Все узлы и интерфейсы маршрутизатора настроены правильно. Не проходят эхо-запросы ping на сервер с узлов H1 и H2, а также эхо-запросы межу узлами H1 и H2. В чем причина проблемы?  1. RIPv2 не поддерживает VLSM 2. На маршрутизаторе R1 неправильно настроен RIPv2 3. На маршрутизаторе R2 неправильно настроен RIPv2 4. На маршрутизаторе R3 неправильно настроен RIPv2 5. RIPv2 не поддерживает несмежные сети	3

6 Примеры оценочных средств для проведения промежуточной аттестации

6.1 Примеры экзаменационных билетов – 40 билетов

<table>
<tr><td colspan="3">ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА</td></tr>
<tr><td>Рассмотрено ЦМК
Протокол №_____
«____» _____ 2026 г.
Председатель ЦМК
_____
Е.А. Стефанович</td><td>Билет № 1
по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование:
Группа СОССА-24-1, ССССА-25-1
Курс 2</td><td>Утверждаю
Зам. Директора по УР
А.Т. Бондарь
«____»_____2026 г.</td></tr>
<tr><td colspan="3">Компетенции: ПК 1-7, ОК 1-9
Инструкция
1. Внимательно прочитайте задание.
Текст задания:
ЗАДАНИЕ № 1 - теоретическое.
Опишите два аспекта внутреннего устройства Интернета: аппаратные и программные компоненты, из которых он состоит, и сетевую инфраструктуру, предоставляющую службы для распределенных приложений.

ЗАДАНИЕ № 2 - практическое.

Исследуйте HTTP-трафик и элементы семейства протоколов TCP/IP.

2. Задание выполнить:
• в виде устного ответа на теоретический вопрос;
• на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин</td></tr>
</table>

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 2** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Предложите классификацию компьютерных сетей по размеру, принадлежности, назначению и области применения.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку начальных параметров коммутатора.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 3** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Предложите модели сетевого взаимодействия.

ЗАДАНИЕ № 2 - практическое.

Выполните работу по обеспечению базовой связности коммутаторов.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 4** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Назовите и охарактеризуйте основные компоненты компьютерной сети.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку сетей VLAN.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 5** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Предложите и опишите варианты Интернет-подключения для дома, небольшого офиса и предприятий.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку магистральных каналов.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 6** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Раскройте понятие «Конвергентная сеть». Перечислите и опишите основные показатели качества сети.

ЗАДАНИЕ № 2 - практическое.

Выполните первоначальную настройку маршрутизатора.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 7** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССCА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите исторические этапы компьютерных сетей и Интернета.

ЗАДАНИЕ № 2 - практическое.

Выполните подключение маршрутизатора к локальной сети.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 8** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Перечислите и охарактеризуйте пять основных требований к компьютерным протоколам.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку IP-интерфейсов.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 9** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите понятие протокола и алгоритм их взаимодействия в стеке TCP/IP.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку статических маршрутов.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 10** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Перечислите и опишите набор протоколов в стеке TCP/IP.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку статических маршрутов.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 11** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССCА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите открытые стандарты Интернета, электроники и связи.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку протокола RIPv2.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 12** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите эталонную модель OSI.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку протокола DHCP.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 13** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите эталонную модель протоколов TCP/IP. Сравните с моделью OSI.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку беспроводной сети.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 14** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите процессы инкапсуляции и деинкапсуляции при передаче данных по сети.

ЗАДАНИЕ № 2 - практическое.

Исследуйте протокол NAT в процессе преобразования адресов.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 15** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите процессы доступа к устройствам, находящимся в локальной и удаленной сетях.

ЗАДАНИЕ № 2 - практическое.

Выполните настройку статического NAT.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 16** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите физический уровень сетевого доступа (средства подключения, стандарты, характеристики; характеристики медного и оптического кабеля).

ЗАДАНИЕ № 2 - практическое.

Выполните настройку динамического NAT.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 17** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите физический уровень сетевого доступа (средства подключения, стандарты, характеристики; типы и характеристики медного, оптоволоконного кабеля и беспроводной среды передачи).

ЗАДАНИЕ № 2 - практическое.

Исследуйте адресацию подсетей IPv6.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 18** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите канальный уровень сетевого доступа (подуровни канального уровня, управление доступом к среде, стандарты, топологии глобальных и локальных сетей, понятия полудуплексной и полнодуплексной передачи, CSMA/CD, CSMA/CA, структуру кадра локальной и глобальной сети, назначение полей кадра).

ЗАДАНИЕ № 2 - практическое.

Выполните поиск и устранение неполадок последовательных интерфейсов.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 19** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите кадр Ethernet (инкапсуляция, подуровни LLC и MAC, управление доступом к среде, развитие, поля кадра, MAC-адреса обработка кадров, типы адресов).

ЗАДАНИЕ № 2 - практическое.

Выполните конфигурацию безопасности коммутатора.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 20** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Охарактеризуйте коммутаторы локальных сетей (таблица MAC-адресов, самообучение коммутатора, продвижение фильтра, фильтрация кадра, способы пересылки кадров, настройка портов).

ЗАДАНИЕ № 2 - практическое.

Выполните поиск и устранение неполадок в сети.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 21** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите протокол разрешения адресов ARP (назначение и алгоритм работы).

ЗАДАНИЕ № 2 - практическое.

Выполните подключение проводной и беспроводной локальных сетей.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 22** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите сетевой уровень в процессе передачи данных (протоколы сетевого уровня, характеристики протокола IP, структура пакета IPv4, назначение полей).

ЗАДАНИЕ № 2 - практическое.

Выполните исследование таблицы ARP.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 23** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите процесс маршрутизации в сети (решение о переадресации, шлюз по умолчанию, таблица маршрутизации, типы маршрутов, записи таблицы маршрутизации).

ЗАДАНИЕ № 2 - практическое.

Выполните исследование межсетевых устройств.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 24** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите работу маршрутизатора (устройство, типы памяти, подключение к маршрутизатору, интерфейсы LAN и WAN, процесс загрузки, просмотр данных, шаги базовой настройки).

ЗАДАНИЕ № 2 - практическое.

Выполните анализ трафика одноадресной, широковещательной и многоадресной рассылки.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 25** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Охарактеризуйте IP-адресацию (структура IPv4-адреса, классовая адресация, бесклассовая адресация, маска и длина префикса, частные диапазоны, специальные адреса, разбиение на подсети, VLSM и CIDR, IPv6-адресация).

ЗАДАНИЕ № 2 - практическое.

Выполните поиск и устранение неполадок шлюза по умолчанию.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 26** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Охарактеризуйте транспортный уровень (назначение, протоколы транспортного уровня, пять функций протокола TCP, структура и назначение полей заголовка, использование протокола UDP, типы портов, структура сокета, использование пары сокетов).

ЗАДАНИЕ № 2 - практическое.

Выполните команды ping и трассировки.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 27** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите уровень приложений (назначение, состав, протоколы уровня TCP/IP, модель «клиент-сервер», одноранговая сеть, P2P приложения, HTTP, почтовые протоколы, DNS, DHCP, FTP, TFTP, SMB).

ЗАДАНИЕ № 2 - практическое.

Поиск и устранение проблем IPv4 и IPv6.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 28** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Охарактеризуйте коммутируемые сети (конвергентные сети, уровни иерархии коммутируемых сетей: доступа, распределения и ядра; форм-факторы коммутаторов, пересылка кадров, способы коммутации, коммутационные домены).

ЗАДАНИЕ № 2 - практическое.

Отработайте сценарий разделения на подсети.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 29** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите основные концепции и настройки коммутации (загрузка коммутатора, устройство, базовое и удаленное управление, настройка, безопасность).

ЗАДАНИЕ № 2 - практическое.

Разработайте и реализуйте схему адресации VLSM.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 30** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите процесс разделения на виртуальные локальные сети VLAN (определение VLAN, преимущества, типы VLAN, транки виртуальных сетей, тегирование кадров Ethernet).

ЗАДАНИЕ № 2 - практическое.

Выполните обмен данными с помощью TCP и UDP.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 31** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите процесс реализации виртуальной локальной сети VLAN (диапазоны VLAN на коммутаторе, создание сети VLAN, назначение и настройка портов, проверка, настройка транковых каналов IEEE 802.1Q, возможные проблемы).

ЗАДАНИЕ № 2 - практическое.

Настройте Интернет и электронную почту.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 32** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите концепции маршрутизации (семь характеристик сети, необходимость маршрутизации, функции маршрутизатора, компоненты маршрутизатора, выбор оптимального пути, механизмы пересылки пакетов, подключение устройств, шлюзы по умолчанию, активация IP-адресации на узле, базовое и дистанционное управление, настройка интерфейсов, проверка связности).

ЗАДАНИЕ № 2 - практическое.

Настройте FTP-серверы.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 33** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Охарактеризуйте решения маршрутизации (функция коммутации маршрутизатора, отправка пакета, пересылка на следующий переход, маршрутизация пакетов, достижение места назначения, определение пути, балансировка нагрузки, административное расстояние, таблица маршрутизации, записи маршрутизации, типы маршрутов, статически изученные маршруты, динамические протоколы маршрутизации).

ЗАДАНИЕ № 2 - практическое.

Исследуйте работу сети.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 34** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите маршрутизацию между сетями VLAN (устаревшие методы маршрутизации, методы router-on-a-stick, настройка подынтерфейсов маршрутизатора, проверка маршрутизации

.

ЗАДАНИЕ № 2 - практическое.

Выполните команду Traceroute.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 35** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Охарактеризуйте статическую маршрутизацию (доступ к удаленным сетям, преимущества и недостатки, тпы статических маршрутов, их описание, оманды настройки, рекурсивная и нерекурсивная настройка, проверка, маршрут по умолчанию, плавающие статические маршруты).

ЗАДАНИЕ № 2 - практическое.

Выполните команду Show.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 36** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите динамическую маршрутизацию (эволюция динамических протоколов, компоненты протоколов, преимущества и недостатки; протокол RIPv2: конфигурация, настройка).

ЗАДАНИЕ № 2 - практическое.

Выполните поиск и устранение неполадок сети.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- на компьютере в Packet Tracer.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 37** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Охарактеризуйте таблицу динамической маршрутизации (записи таблицы маршрутизации, типы подключения, динамически подключаемые маршруты, критерии маршрутов, процесс поиска маршрута, оптимальный маршрут = самое длинное совпадение)

ЗАДАНИЕ № 2 - практическое.

Разделение IP-сети на подсети на границе октетов.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- практическое задание выполнить вручную на листе бумаги.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 38** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите работу протокола DHCPv4. (операции протокола, формат сообщений, настройка базового протокола, проверка, DHCPv4-ретрансляция).

ЗАДАНИЕ № 2 - практическое.

Разделение IP-сети на подсети по технологии VLSM.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- практическое задание выполнить вручную на листе бумаги.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 39** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите процесс преобразования сетевых адресов с помощью протокола NAT для IPv4 (принцип работы, терминология NAT, типы NAT, статическое преобразование, динамическое преобразование, преобразование адресов портов).

ЗАДАНИЕ № 2 - практическое.

Суммировать IP-сети по технологии CIDR.

2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- практическое задание выполнить вручную на листе бумаги.

Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

Рассмотрено ЦМК Протокол №_____ «____» _____ 2026 г. Председатель ЦМК _____ Е.А. Стефанович	**Билет № 40** по МДК.01.01 «Компьютерные сети» специальность: 09.02.06 Сетевое и системное администрирование: Группа СОССА-24-1, ССССА-25-1 Курс 2	Утверждаю Зам. Директора по УР А.Т. Бондарь «____»_____2026 г.

Компетенции: ПК 1-7, ОК 1-9

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ЗАДАНИЕ № 1 - теоретическое.

Опишите процесс настройки NAT (настройка статического NAT, настройка динамического NAT, настройка PAT).

ЗАДАНИЕ № 2 - практическое.

Заполнить таблицу маршрутизации сети.

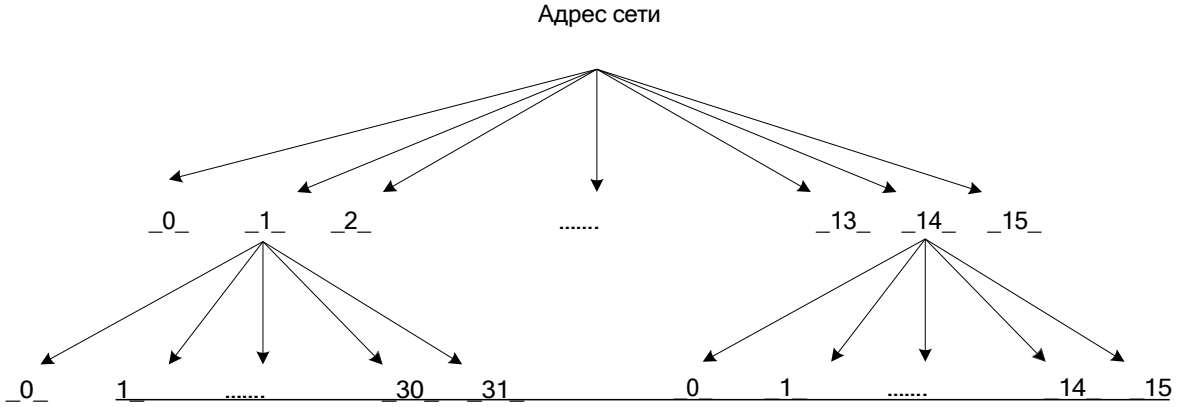
2. Задание выполнить:

- в виде устного ответа на теоретический вопрос;
- практическое задание выполнить вручную на листе бумаги.

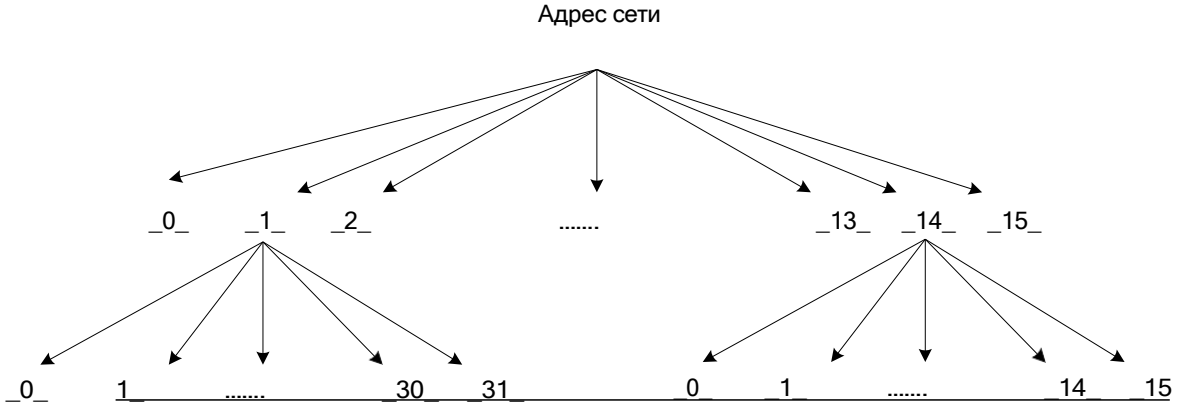
Время выполнения задания - 2 академических часа

Преподаватель Д.И. Головин

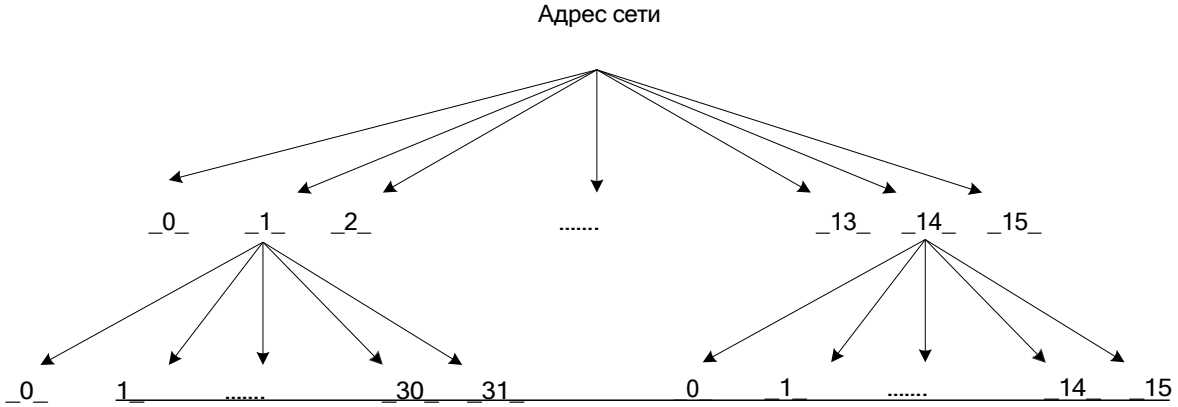
5.4 Варианты заданий на практическую работу по разделению IP-сетей на подсети с использованием VLSM



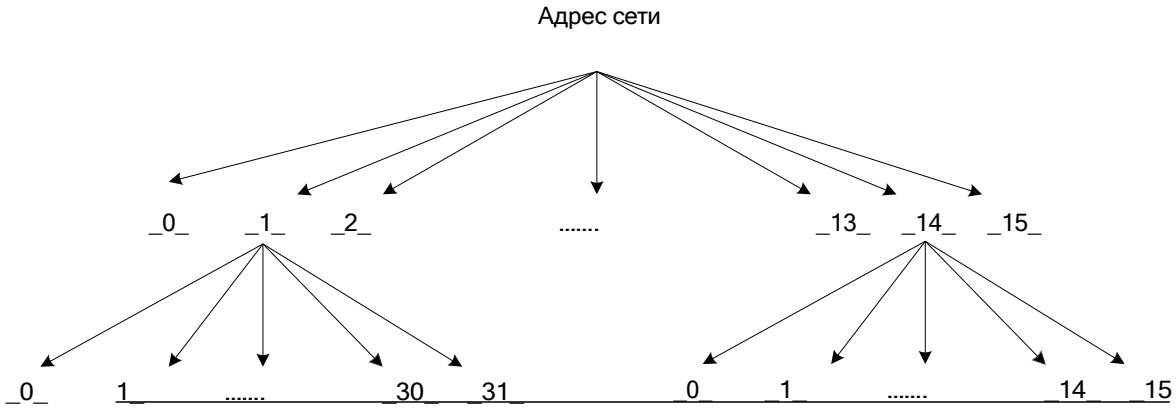
132.11.0.0/16



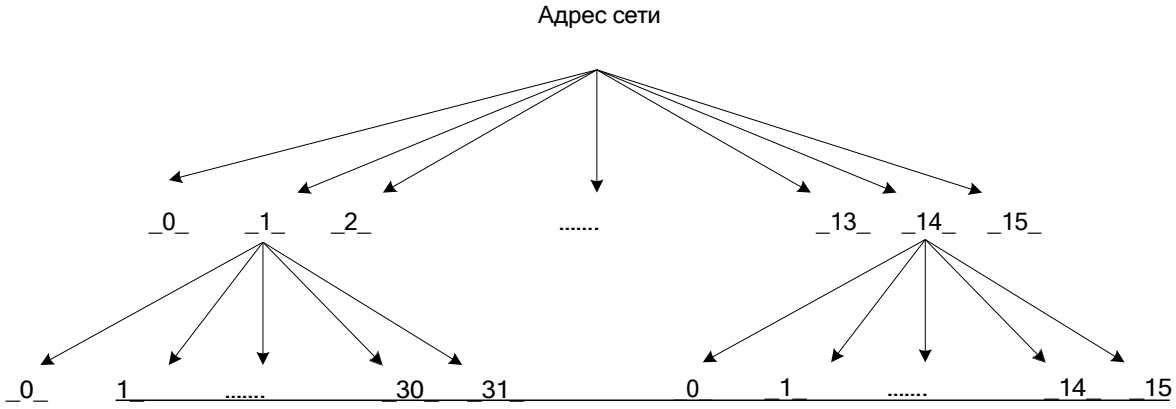
145.250.0.0/16



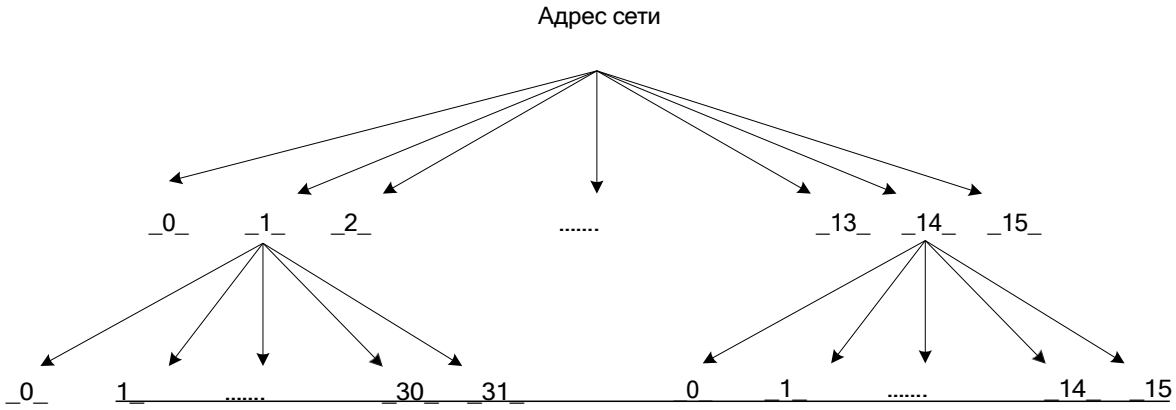
56.48.0.0/15



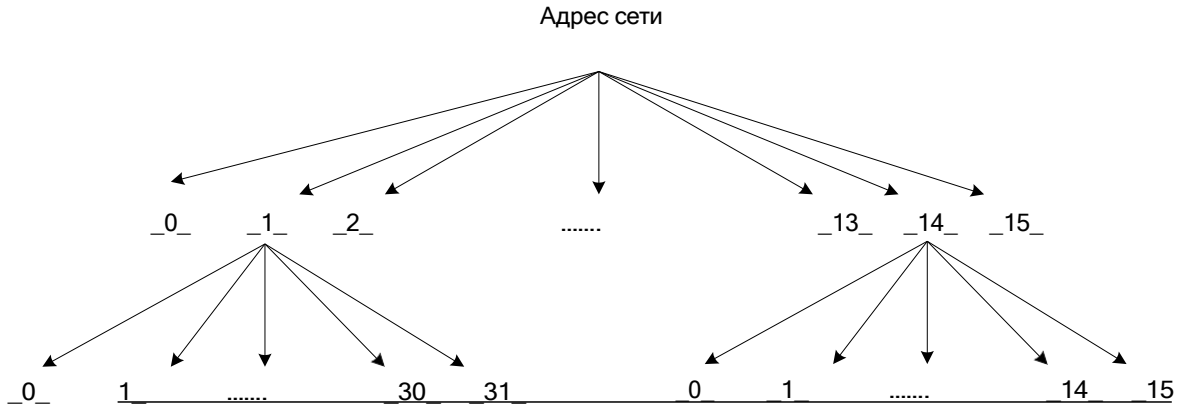
89.48.0.0/12



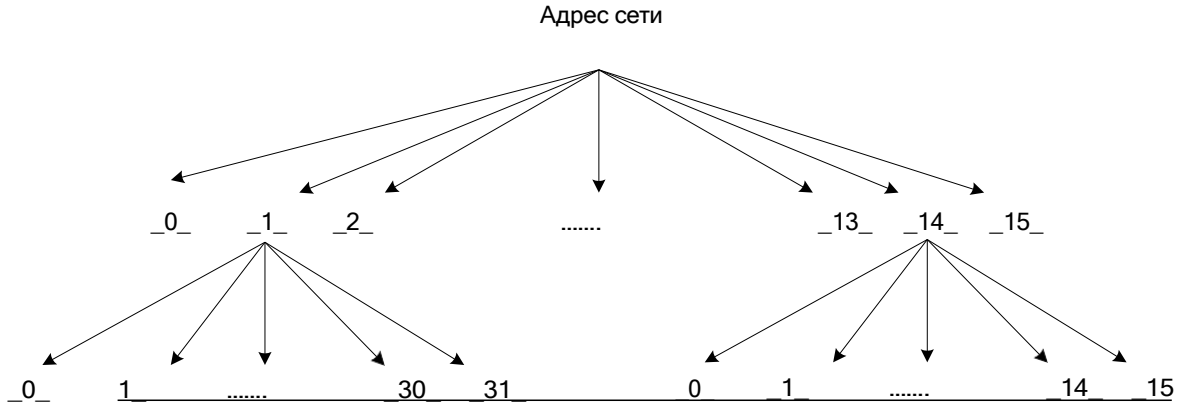
150.24.0.0/16



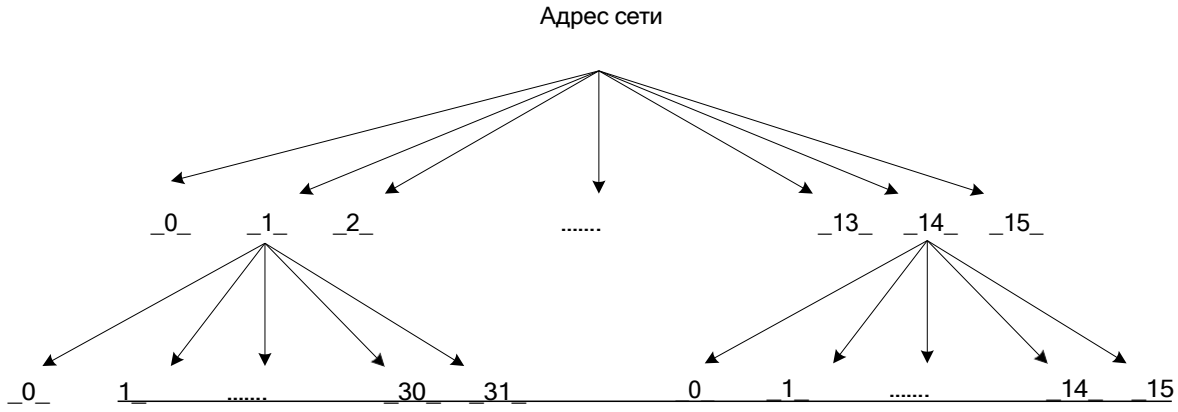
182.54.64.0/18



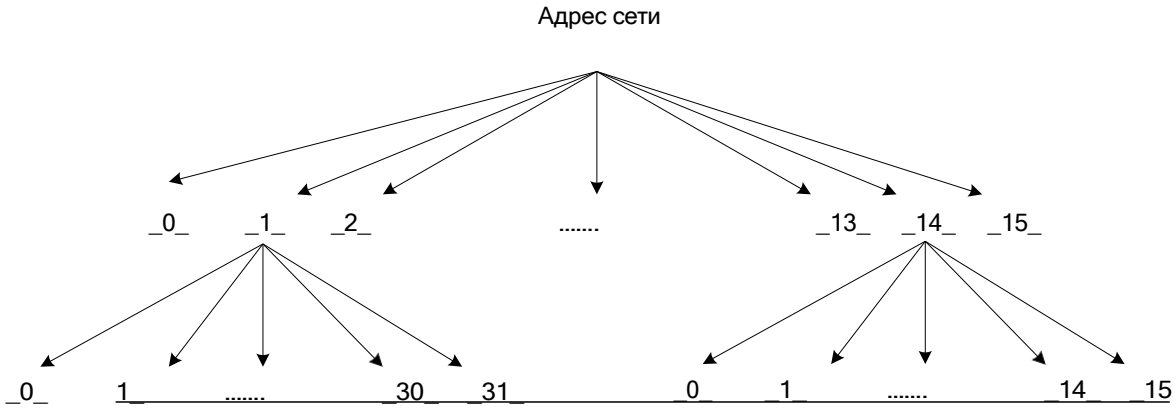
175.0.0.0/20



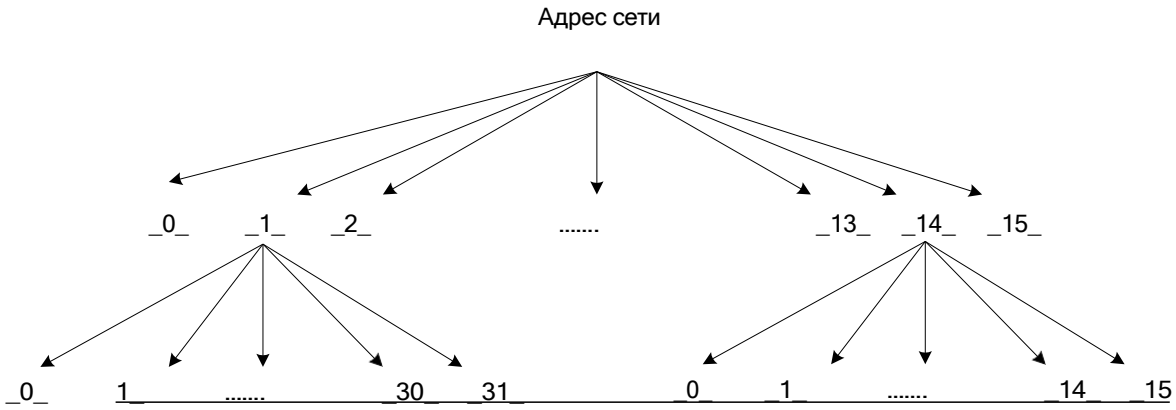
148.56.0.0/16



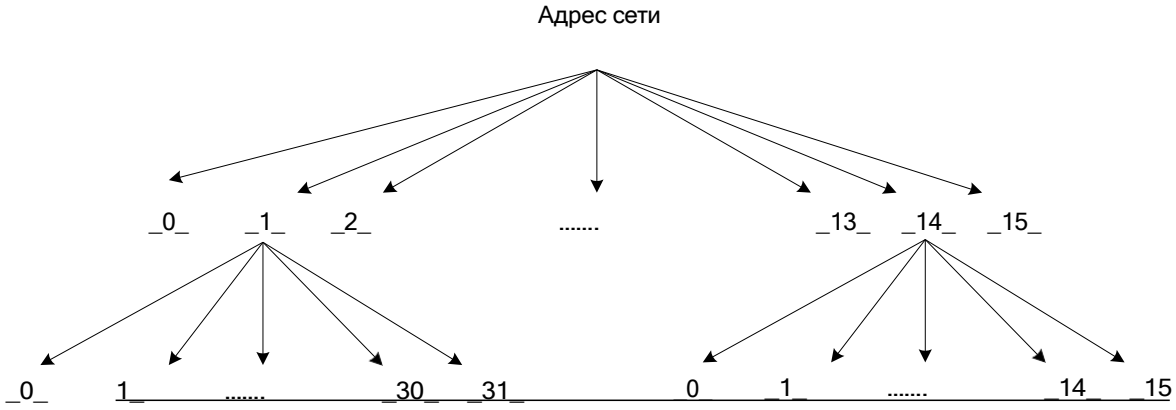
180.23.128.0/17



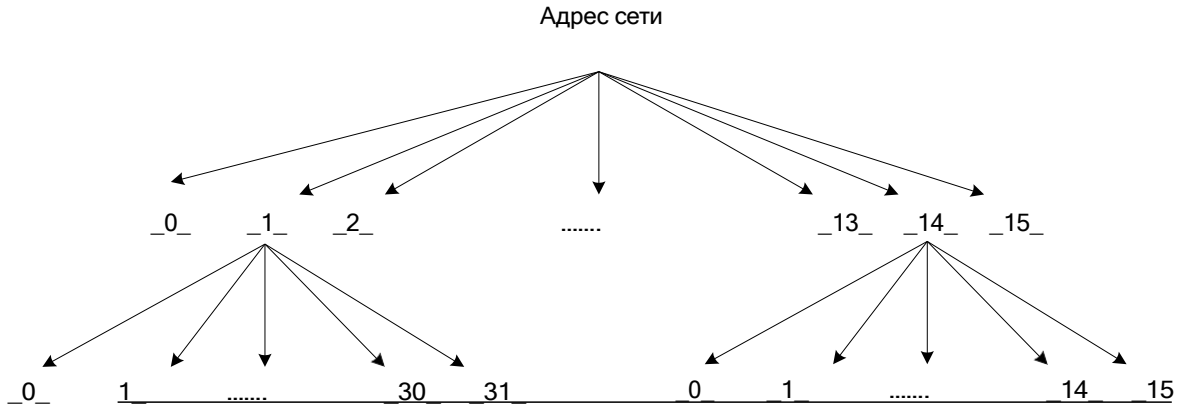
132.11.0.0/16



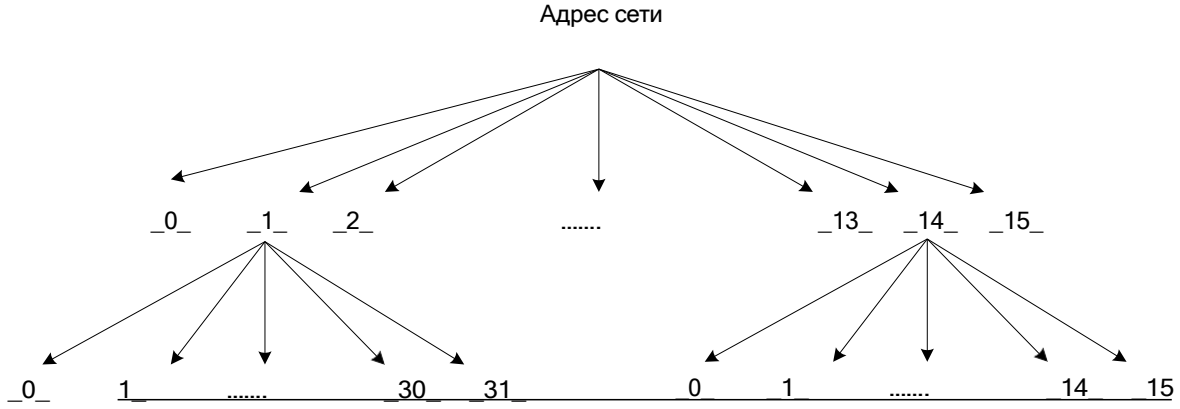
145.250.0.0/16



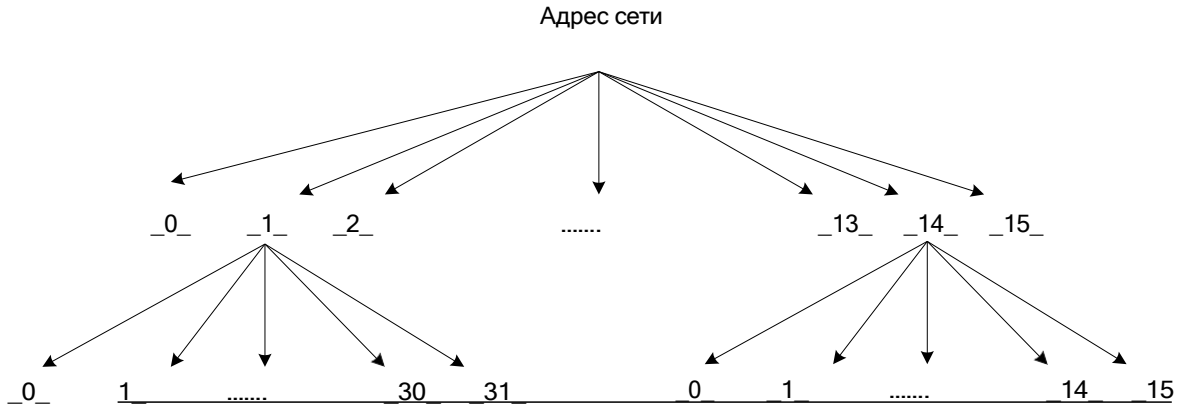
56.48.0.0/15



89.48.0.0/12

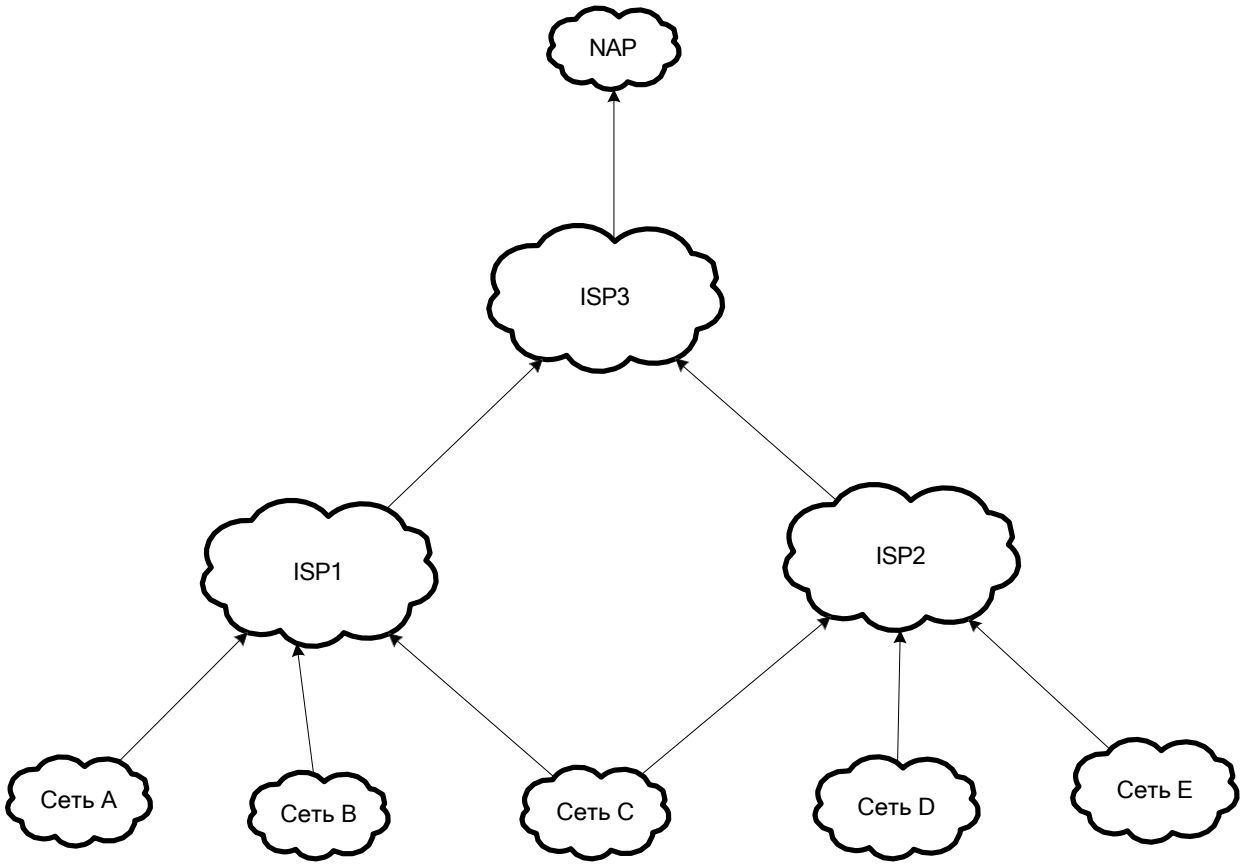


150.24.0.0/16



182.54.64.0/18

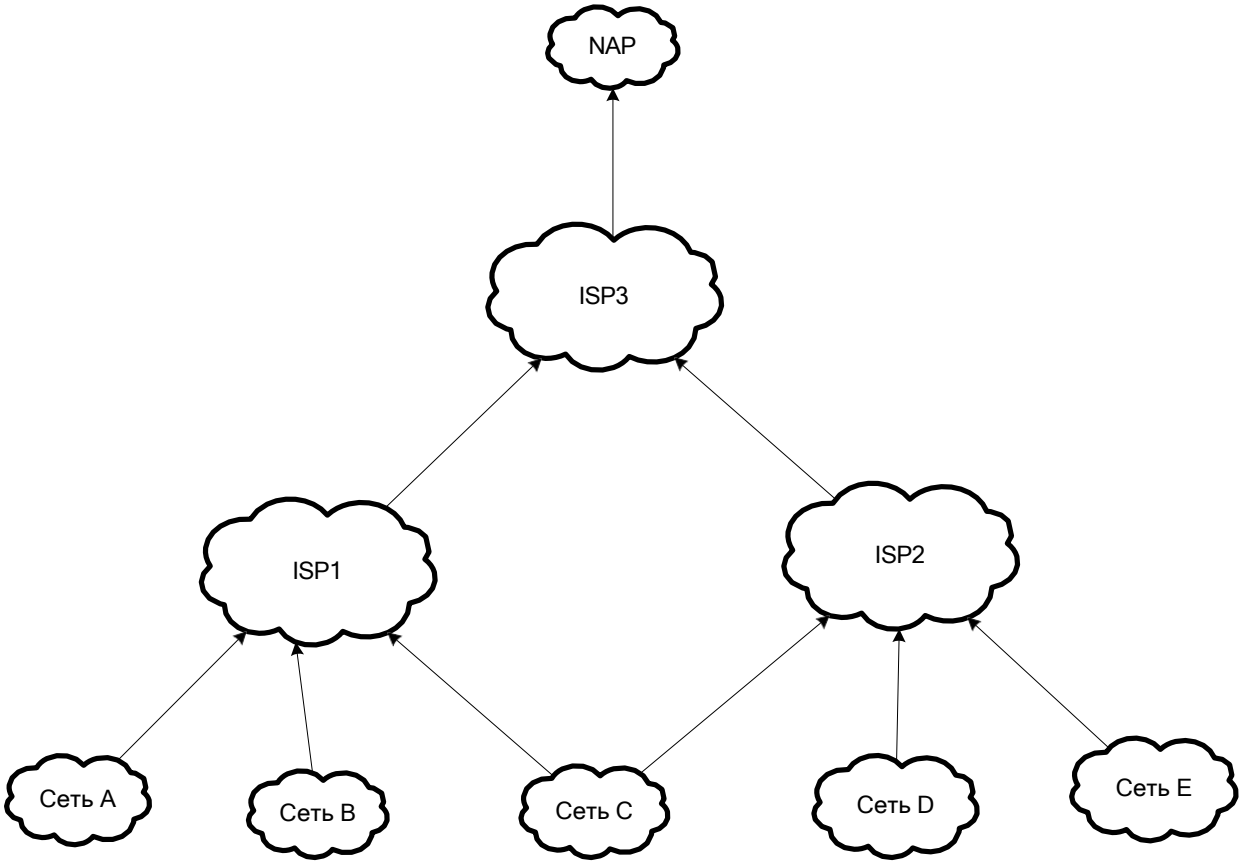
5.5 Варианты заданий на практическую работу по суммированию IP-сетей с использованием CIDR



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 1

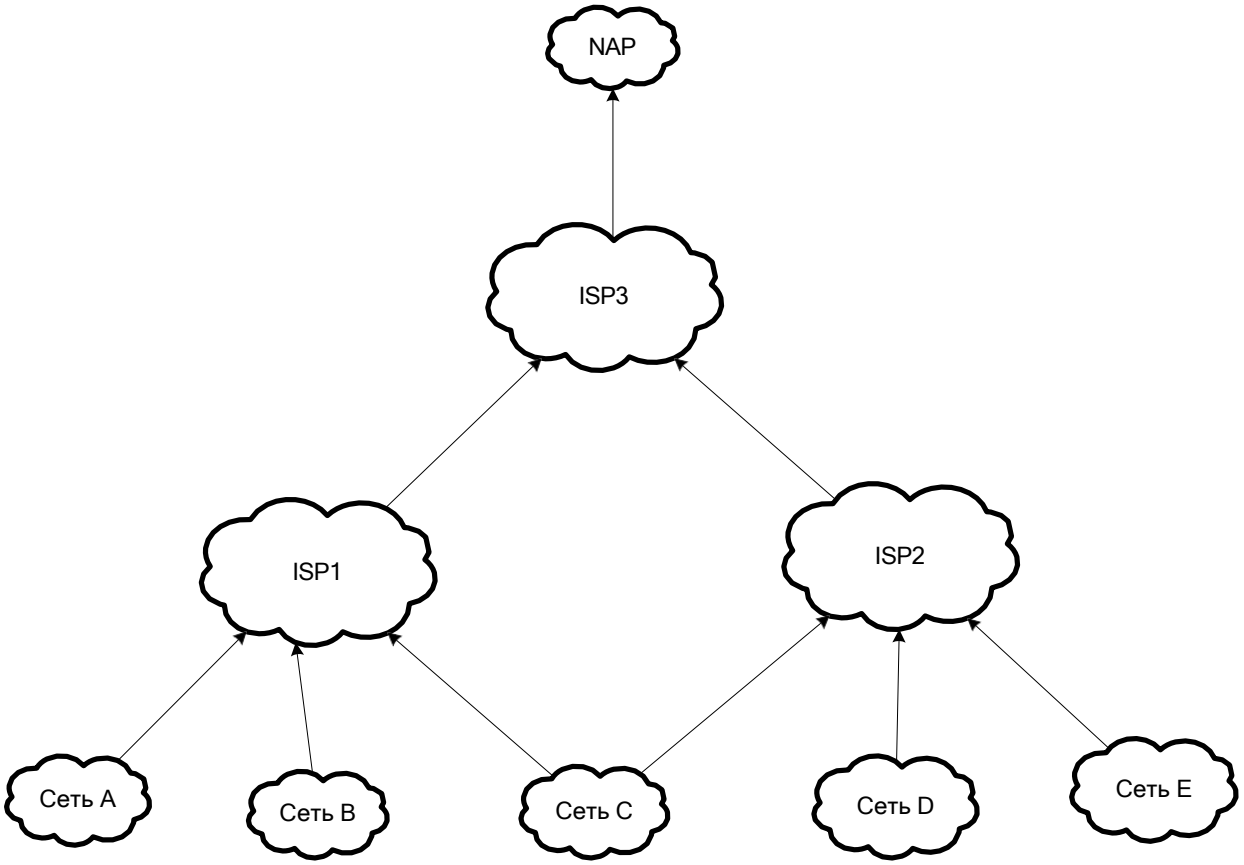
Сеть	Адрес сети	
A	201.18.35.0/26	
B	201.18.35.64/26	
C	201.13.35.128/25	
D	195.28.47.0/25	
E	195.28.47.128/25	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 2

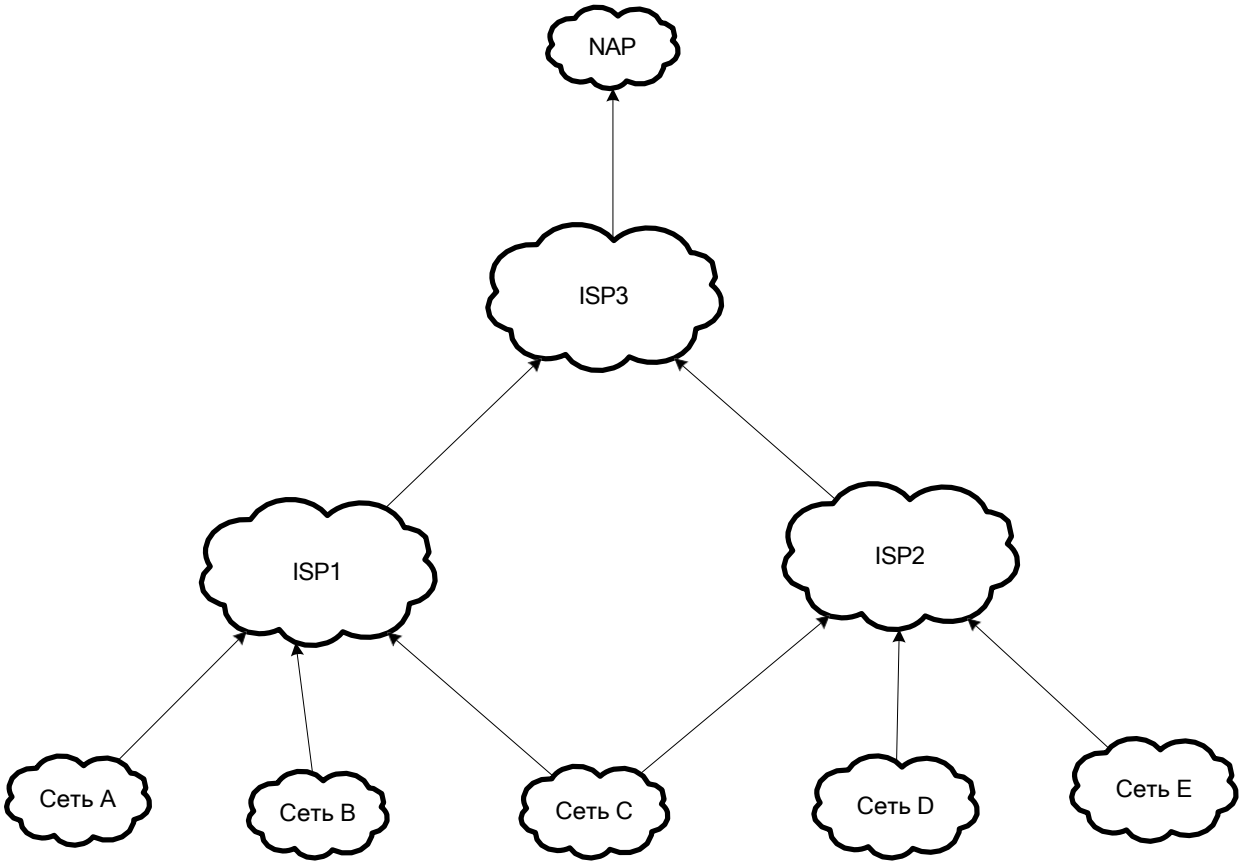
Сеть	Адрес сети
A	118.67.14.0/23
B	118.67.28.0/23
C	12.128.0.0/9
D	12.0.0.0/10
E	12.64.0.0/10



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 3

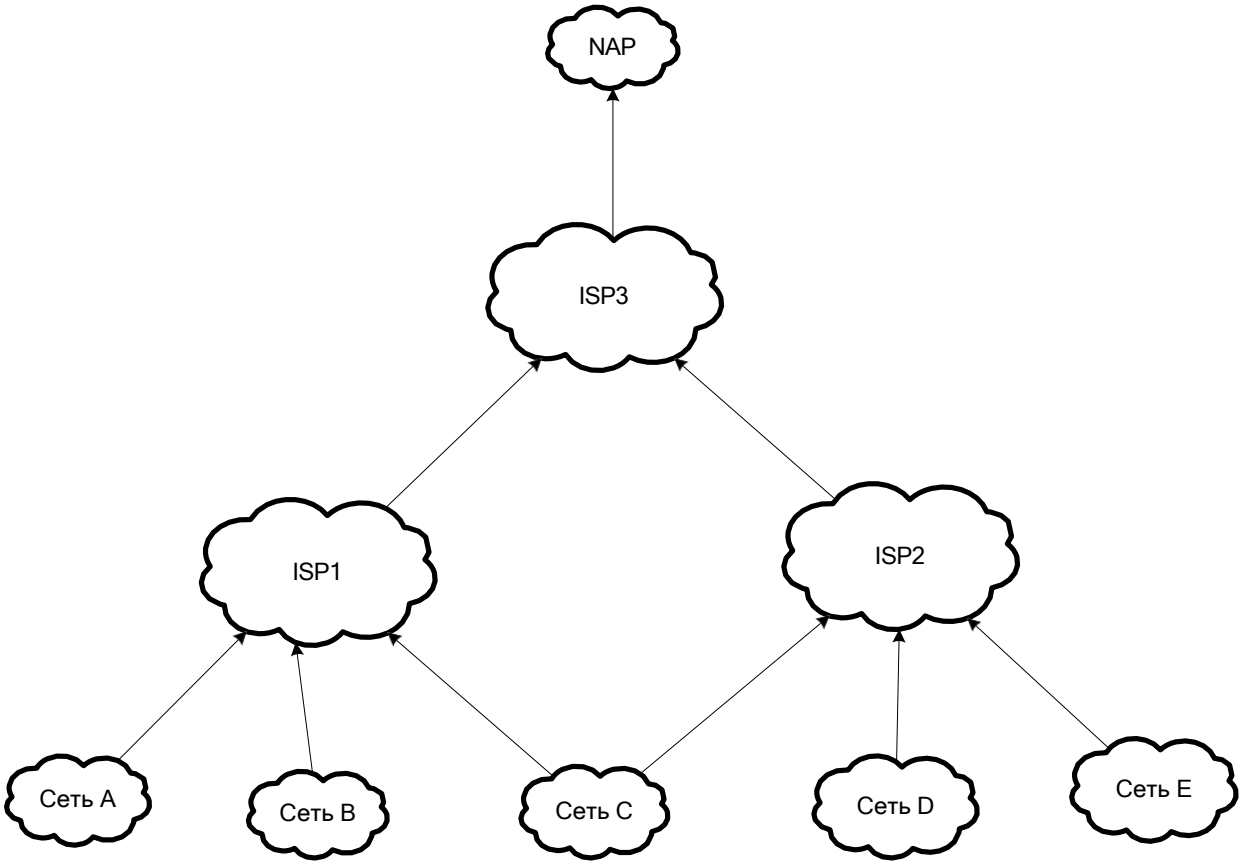
Сеть	Адрес сети
A	216.56.98.0/24
B	216.56.100.0/25
C	216.56.100.128/25
D	56.45.84.0/24
E	56.45.85.0/24



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 4

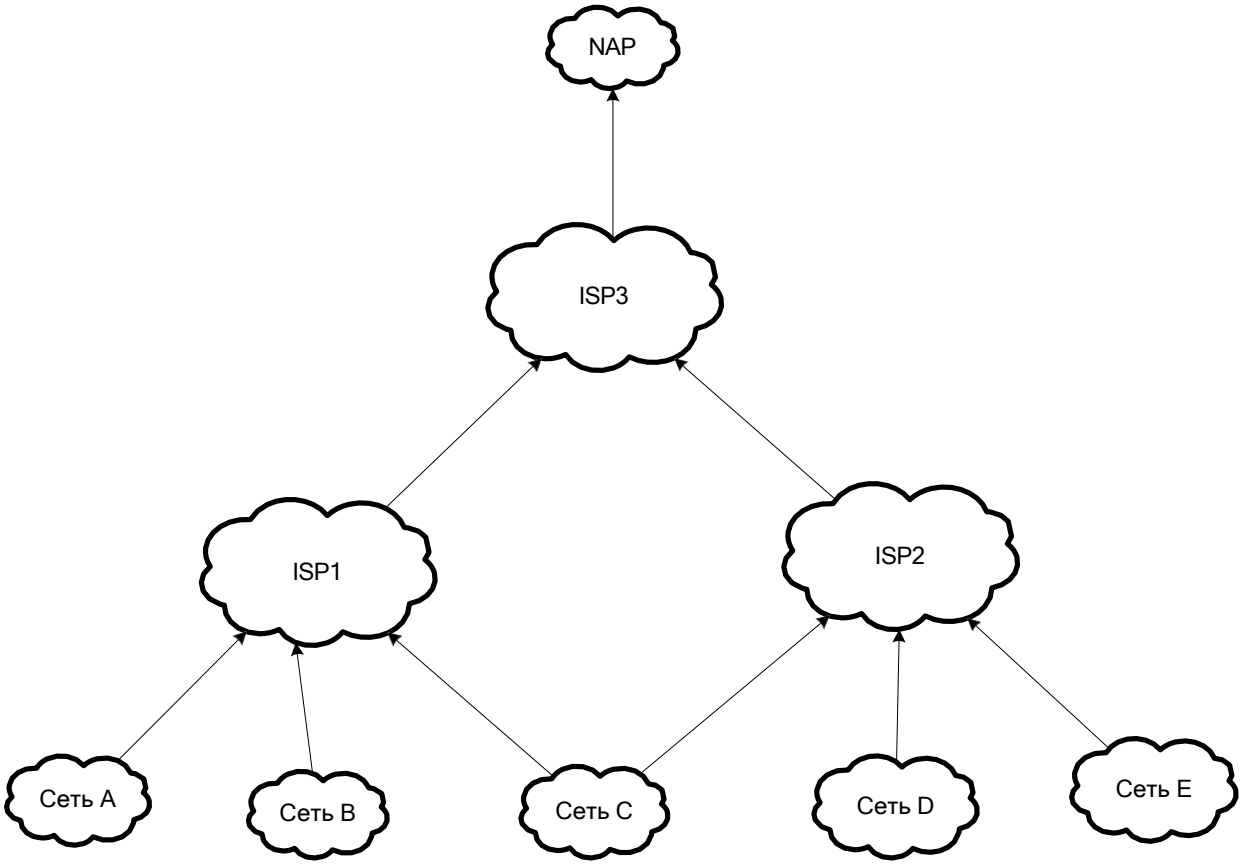
Сеть	Адрес сети
A	143.64.0.0/18
B	143.64.64.0/18
C	143.64.128.0/18
D	143.64.196.0/18
E	143.65.0.0/18



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 5

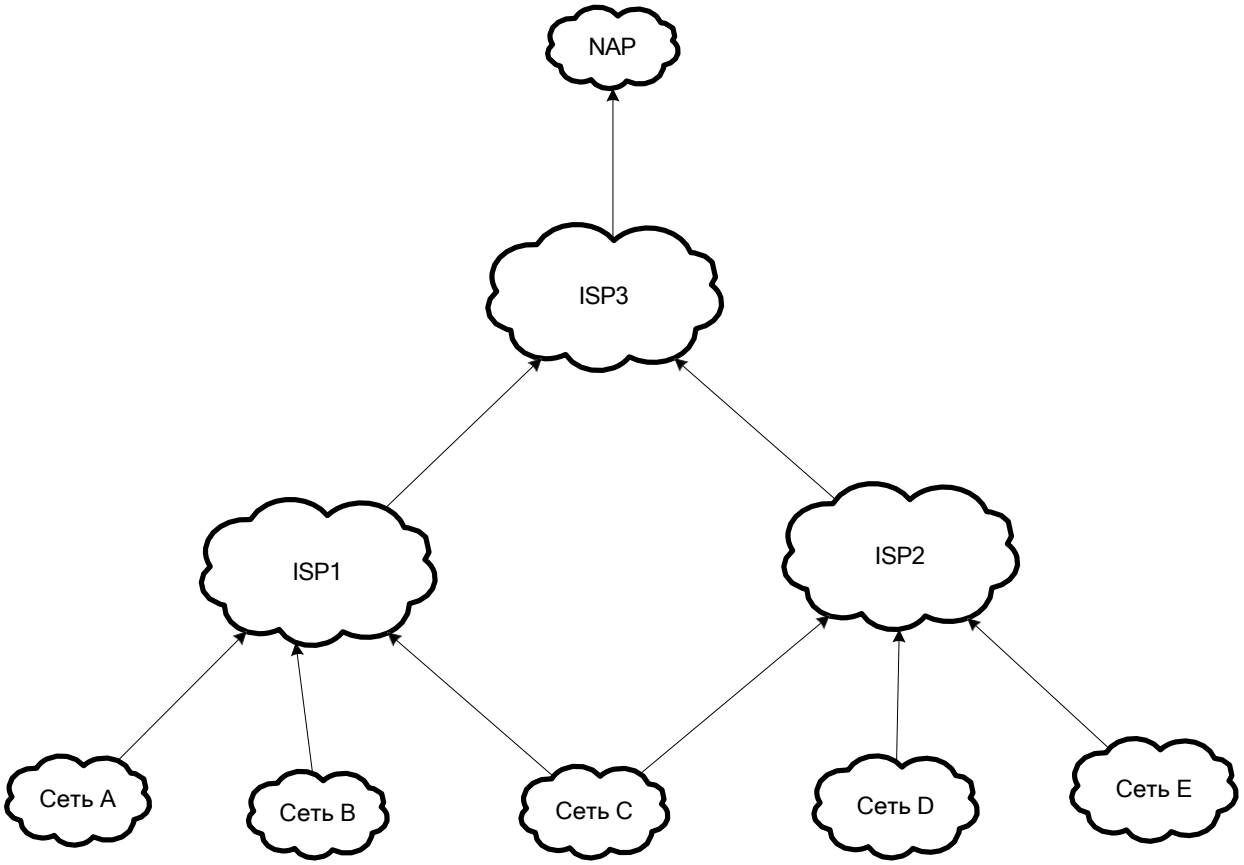
Сеть	Адрес сети	
A	182.15.16.0/20	
B	212.212.212.0/25	
C	212.212.212.128/25	
D	85.128.0.0/9	
E	85.0.0.0/9	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 6

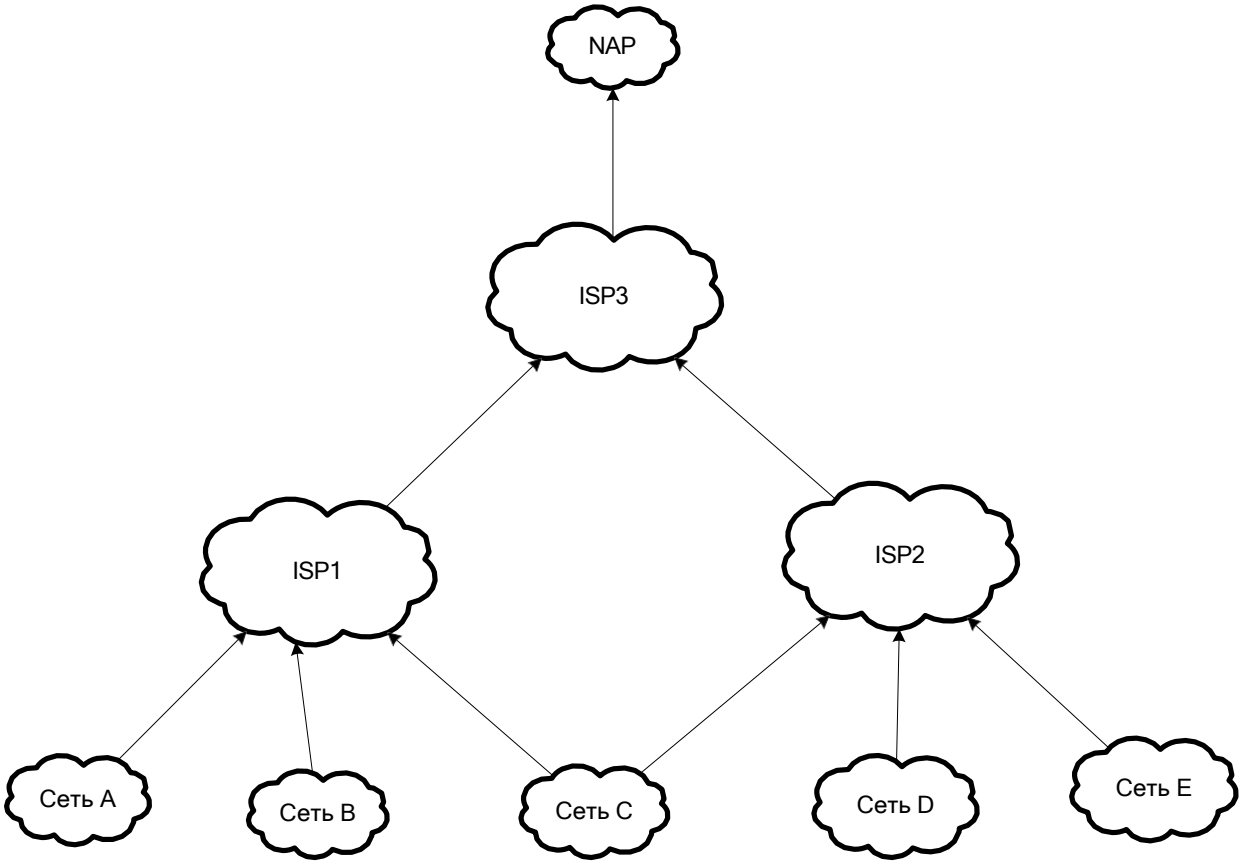
Сеть	Адрес сети	
A	202.20.35.0/26	
B	202.20.35.64/26	
C	202.20.35.128/25	
D	199.29.47.0/25	
E	199.29.47.128/25	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 7

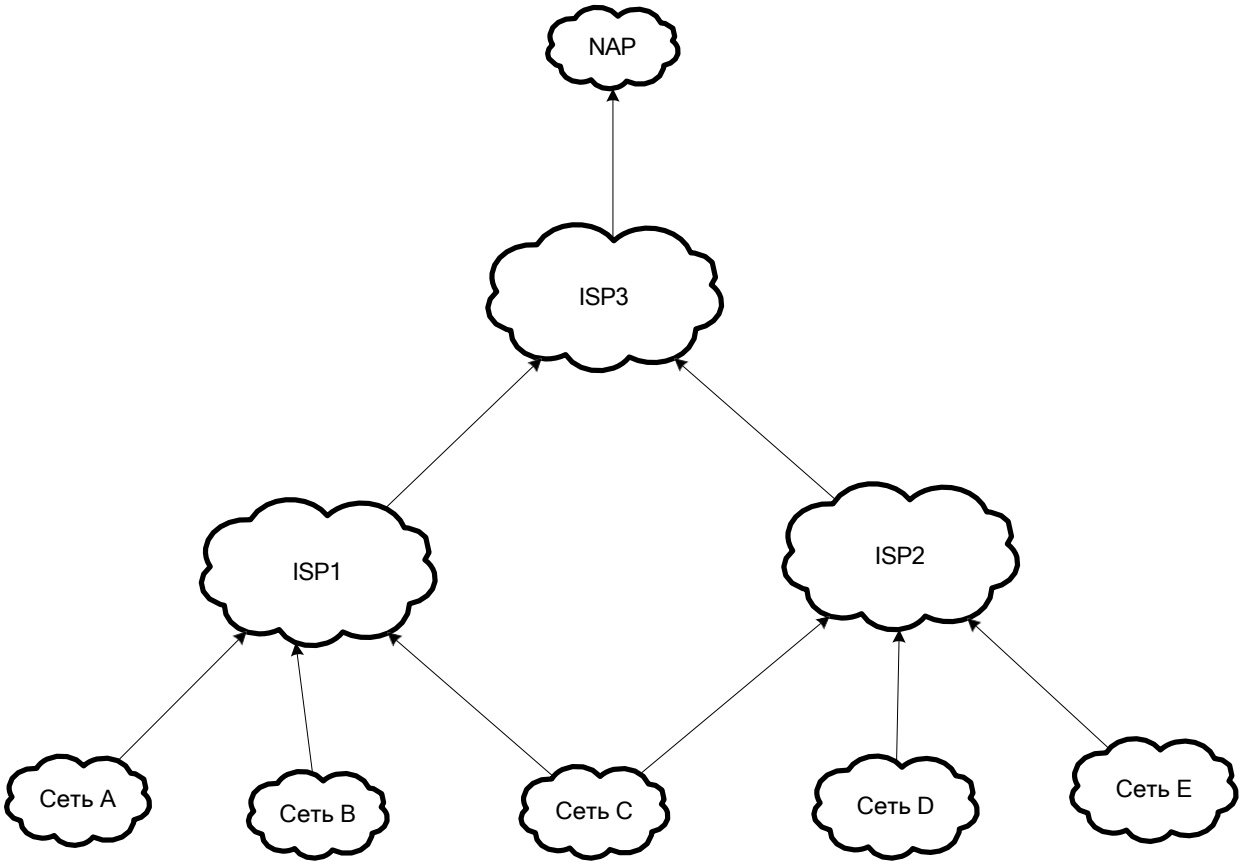
Сеть	Адрес сети	
A	120.167.14.0/23	
B	120.167.28.0/23	
C	112.128.0.0/9	
D	112.0.0.0/10	
E	112.64.0.0/10	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 8

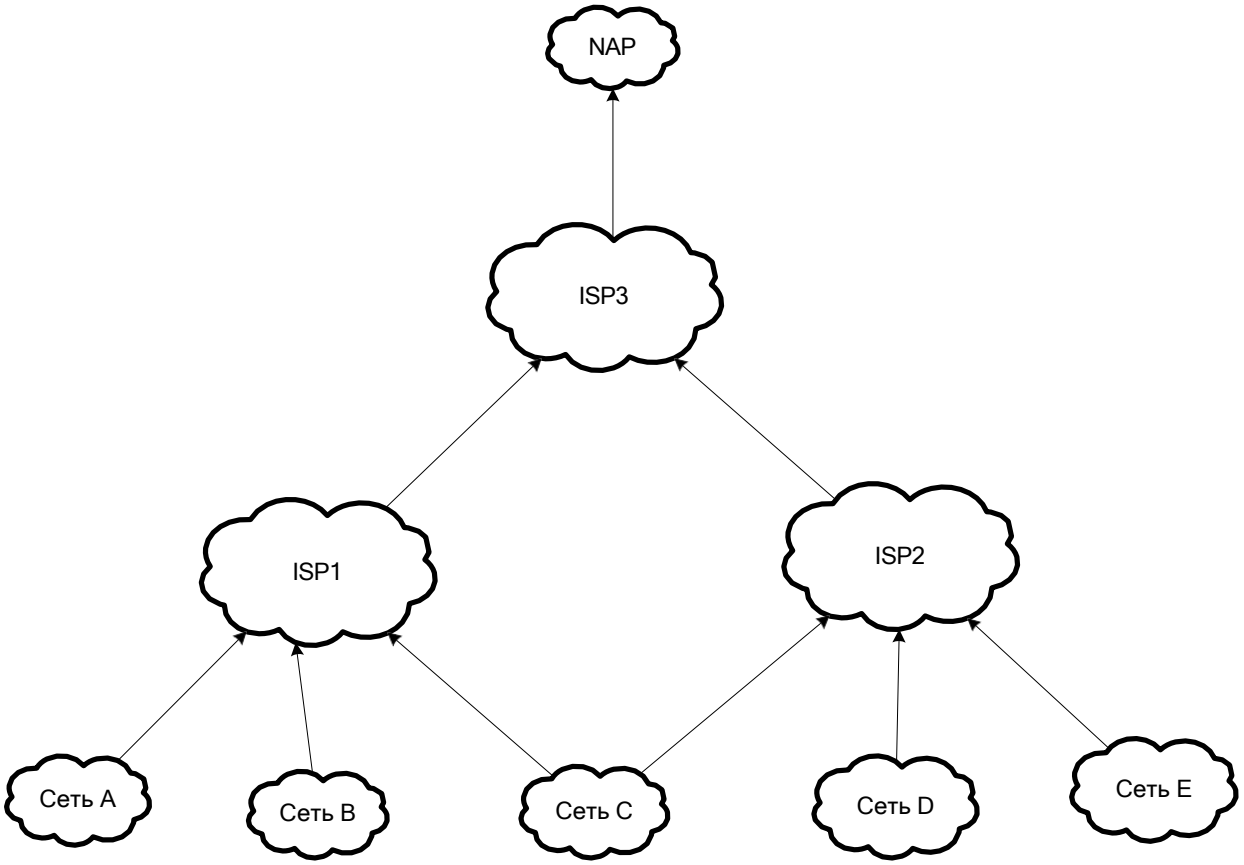
Сеть	Адрес сети	
A	206.156.98.0/24	
B	206.156.100.0/25	
C	206.156.100.128/25	
D	56.45.84.0/24	
E	56.45.85.0/24	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 9

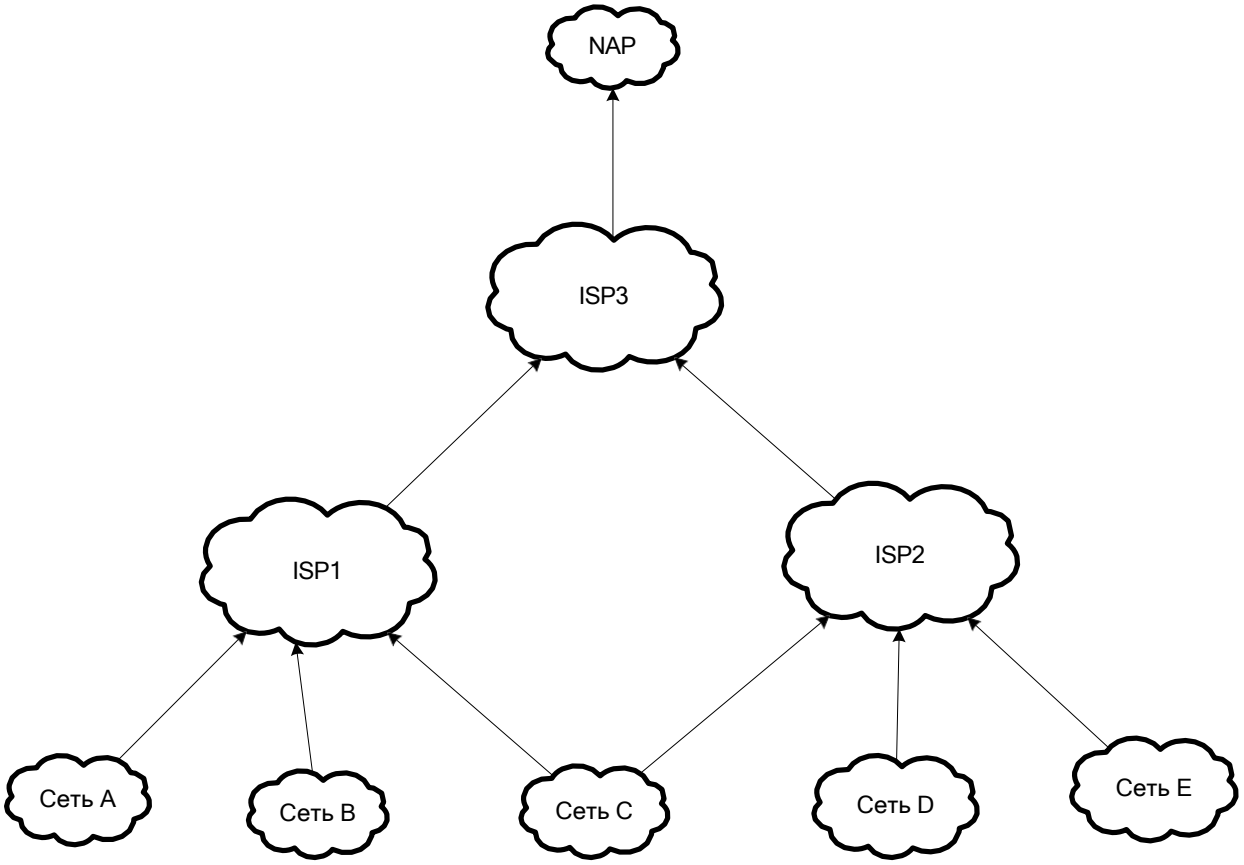
Сеть	Адрес сети	
A	166.4.0.0/18	
B	166.4.64.0/18	
C	166.4.128.0/18	
D	166.4.196.0/18	
E	166.5.0.0/18	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 10

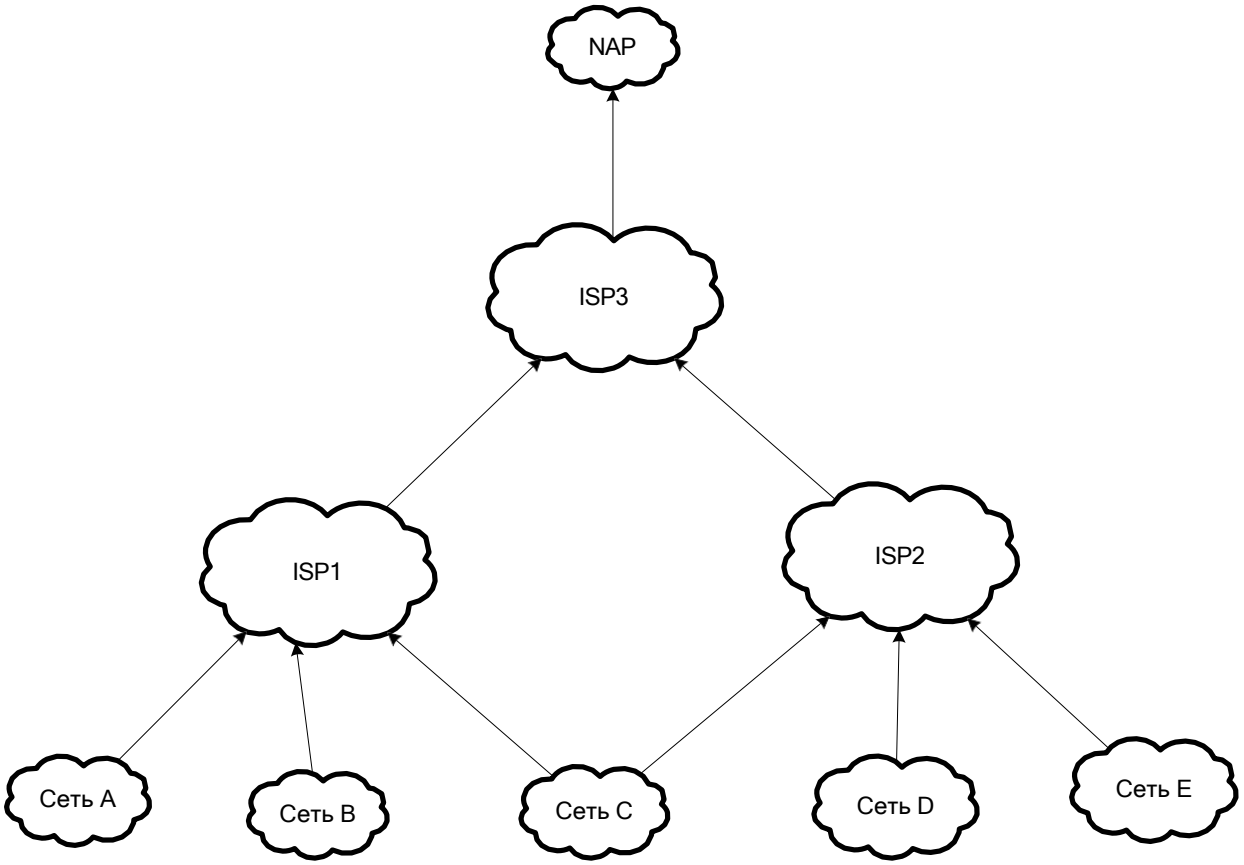
Сеть	Адрес сети	
A	172.16.16.0/20	
B	202.200.200.0/25	
C	202.200.200.128/25	
D	85.128.0.0/9	
E	85.0.0.0/9	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 11

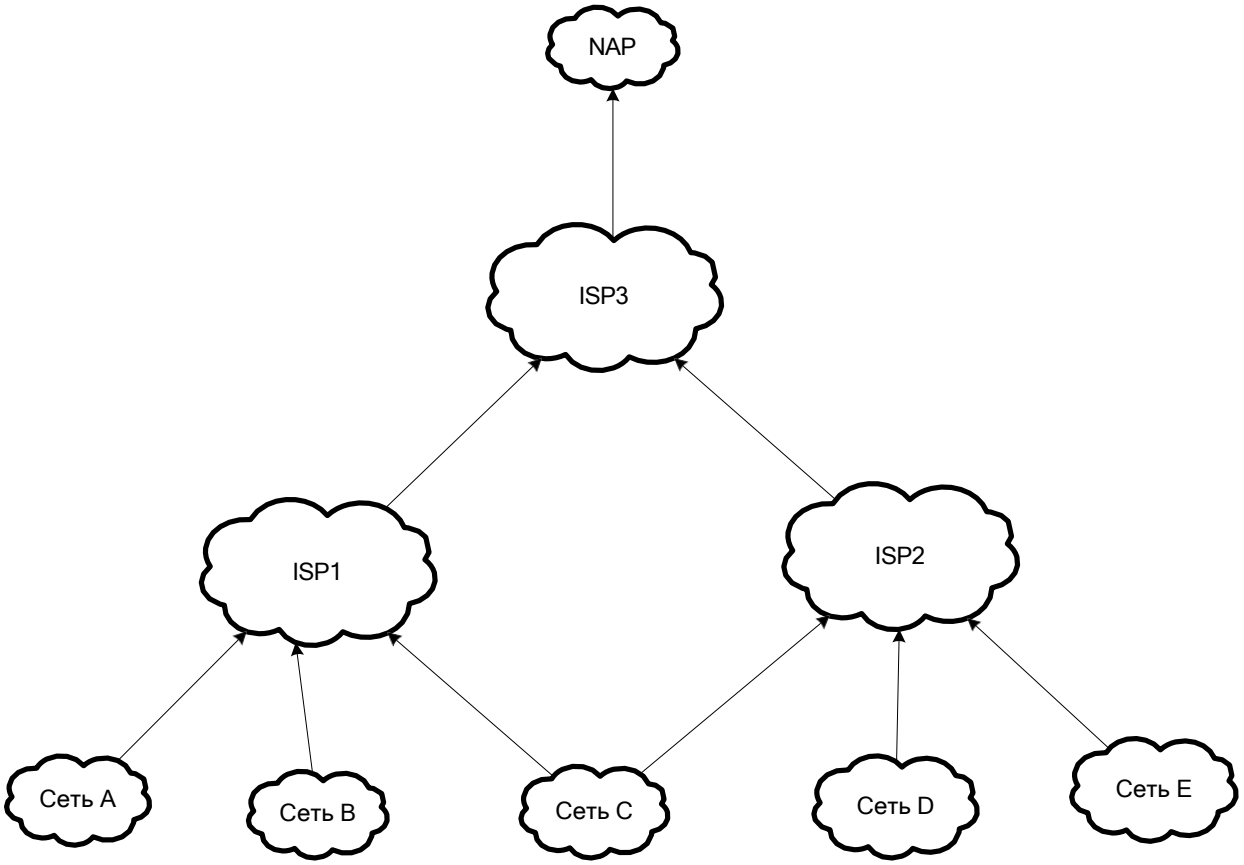
Сеть	Адрес сети
A	193.21.35.0/26
B	193.21.35.64/26
C	193.21.35.128/25
D	219.30.147.0/25
E	219.30.147.128/25



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 12

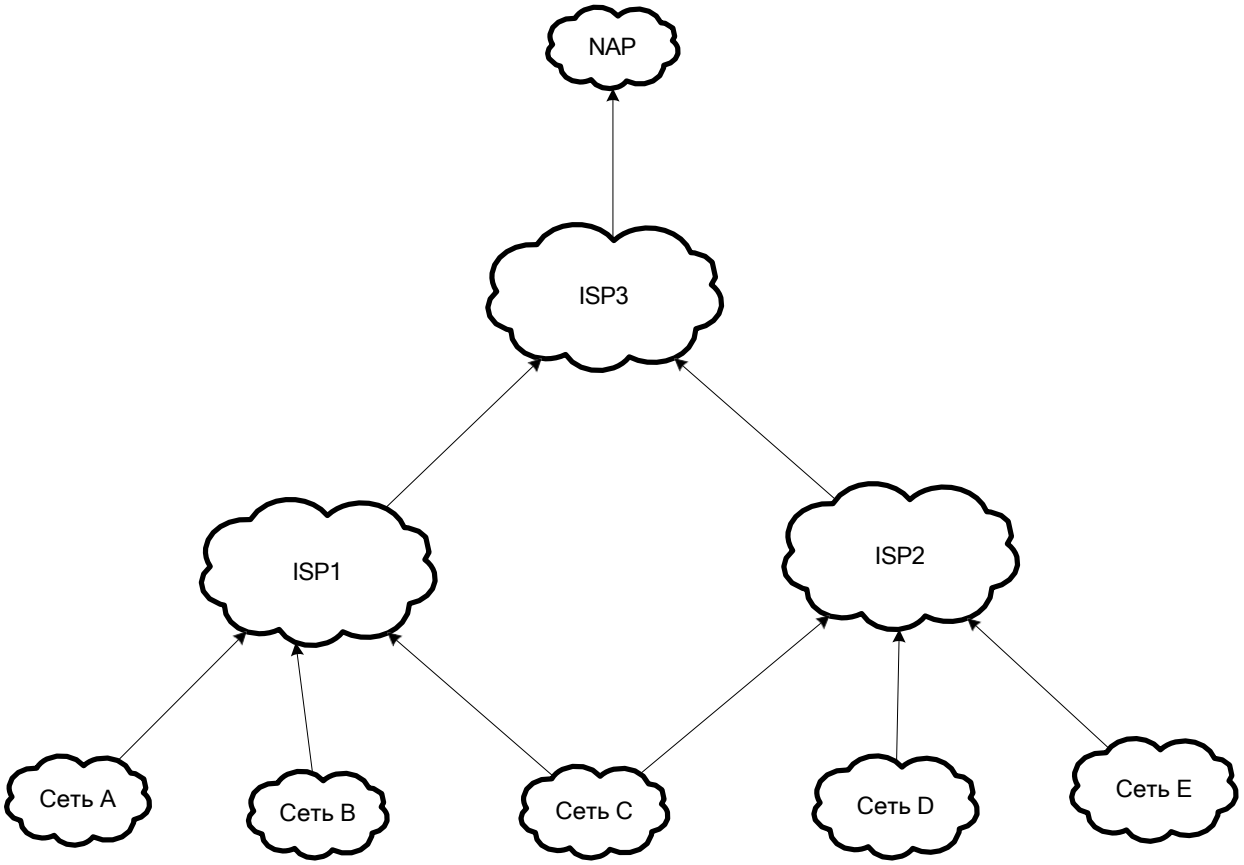
Сеть	Адрес сети	
A	100.7.14.0/23	
B	100.7.28.0/23	
C	122.128.0.0/9	
D	122.0.0.0/10	
E	122.64.0.0/10	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 13

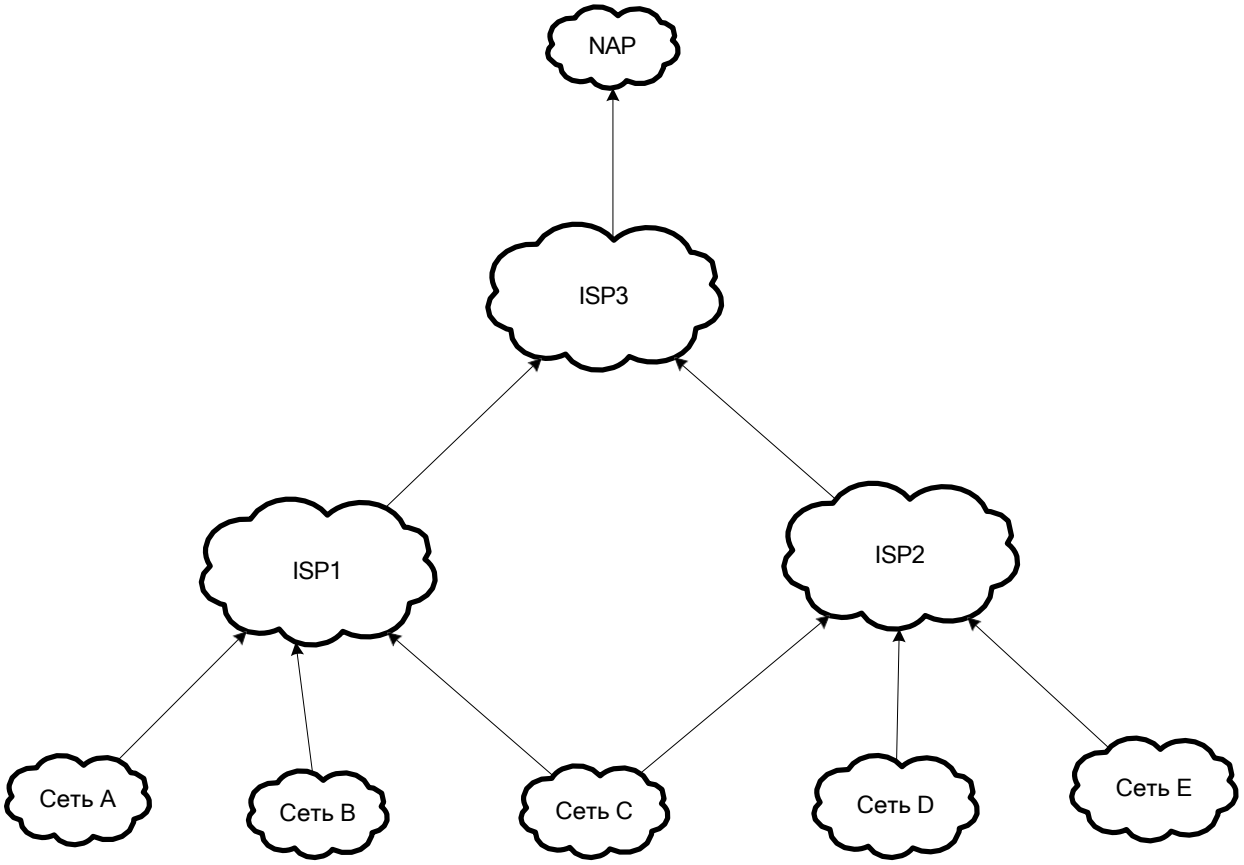
Сеть	Адрес сети	
A	197.156.98.0/24	
B	197.156.100.0/25	
C	197.156.100.128/25	
D	26.45.84.0/24	
E	26.45.85.0/24	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 14

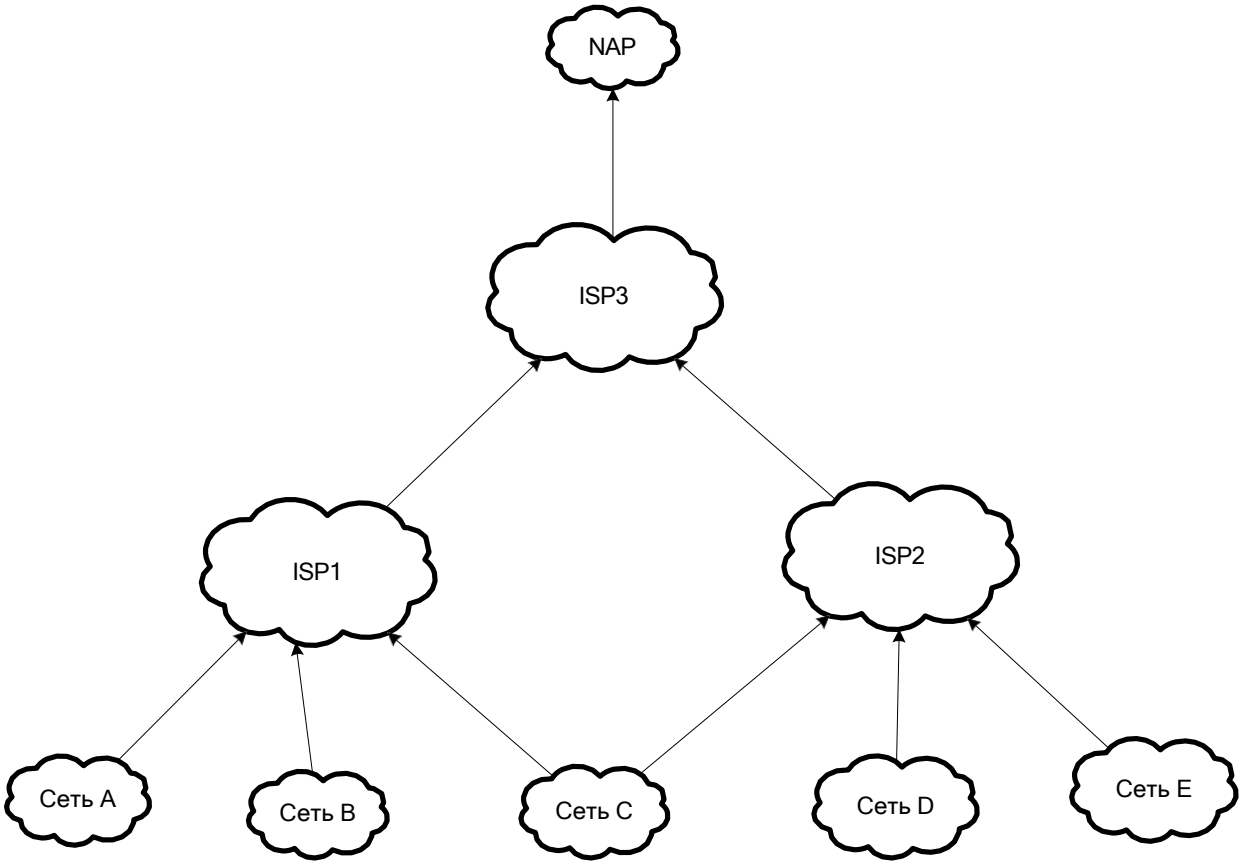
Сеть	Адрес сети
A	176.74.0.0/18
B	176.74.64.0/18
C	176.74.128.0/18
D	176.74.196.0/18
E	176.75.0.0/18



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 15

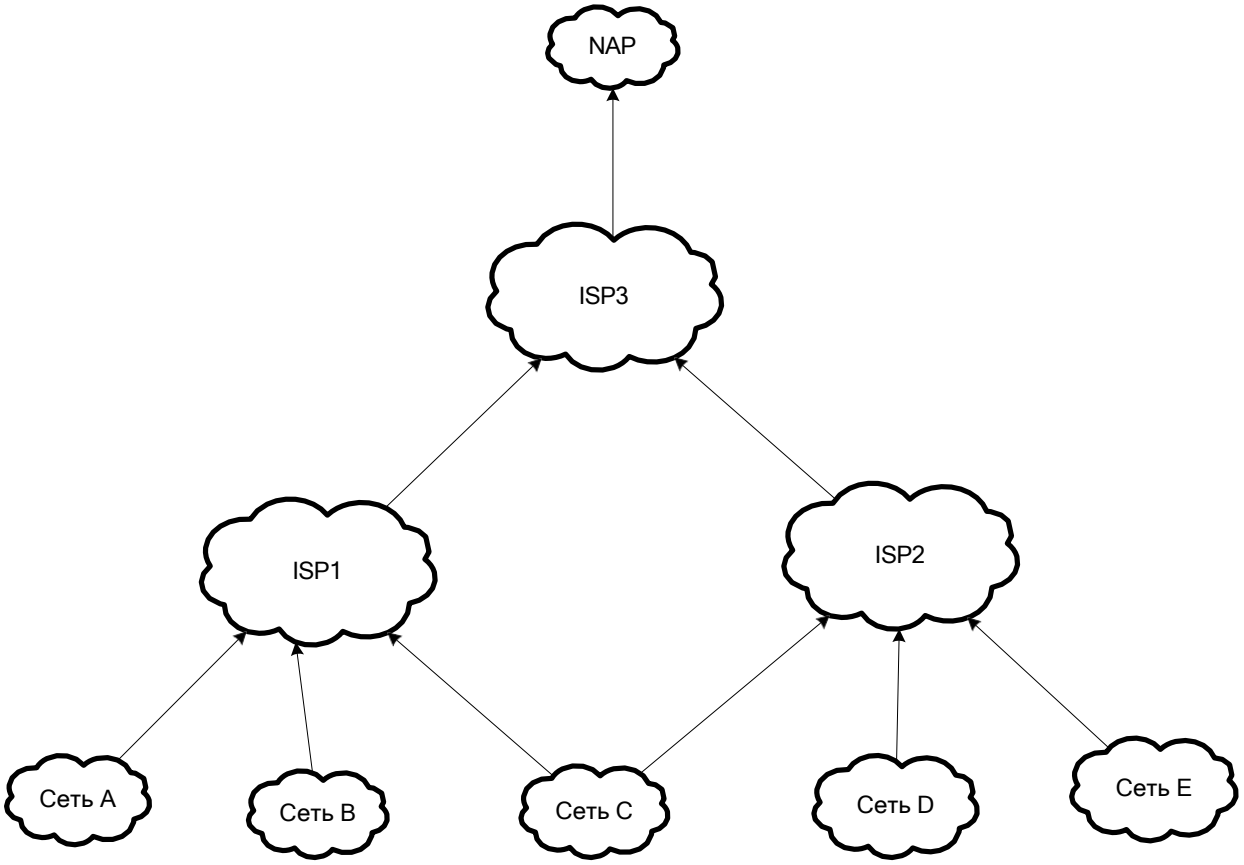
Сеть	Адрес сети	
A	12.16.16.0/20	
B	222.33.33.0/25	
C	232.33.33.128/25	
D	21.128.0.0/9	
E	21.0.0.0/9	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 16

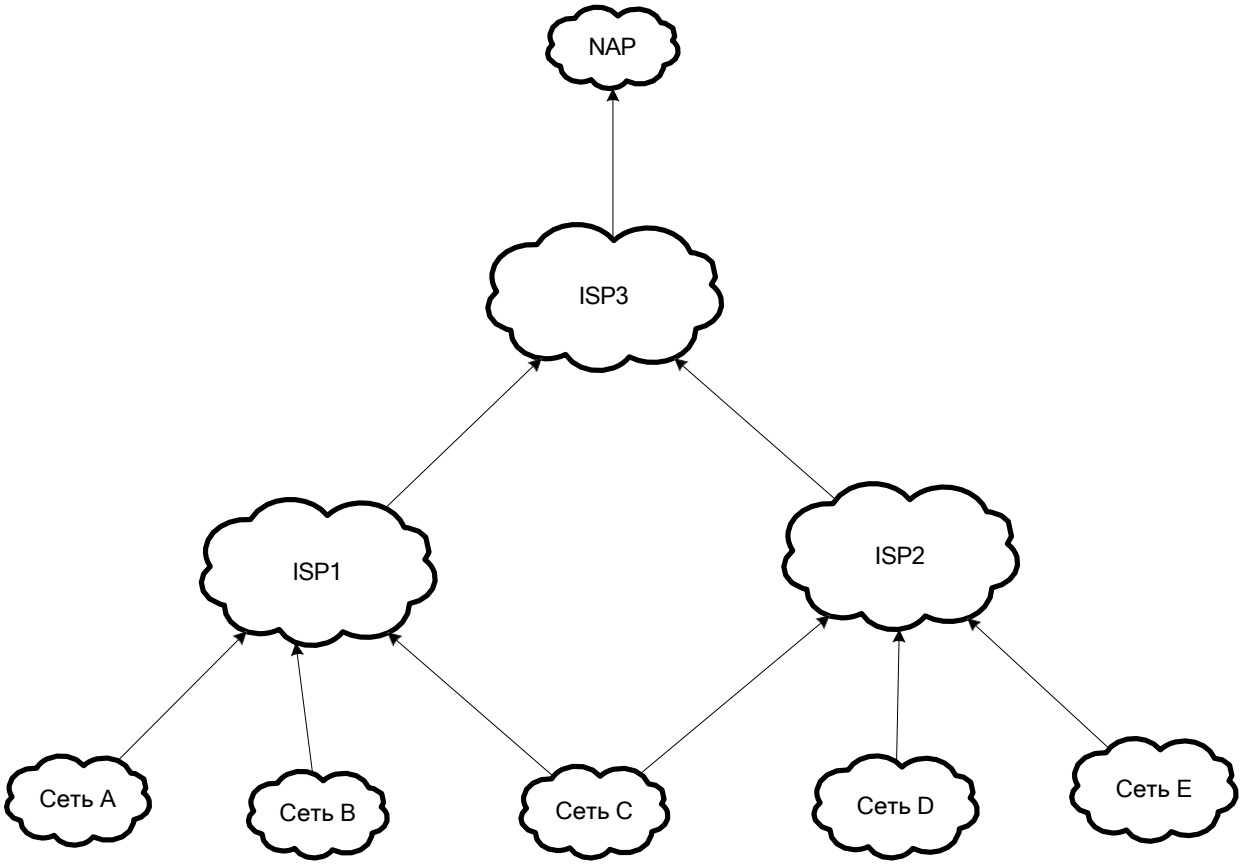
Сеть	Адрес сети	
A	223.21.35.0/26	
B	223.21.35.64/26	
C	223.21.35.128/25	
D	195.30.147.0/25	
E	195.30.147.128/25	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 17

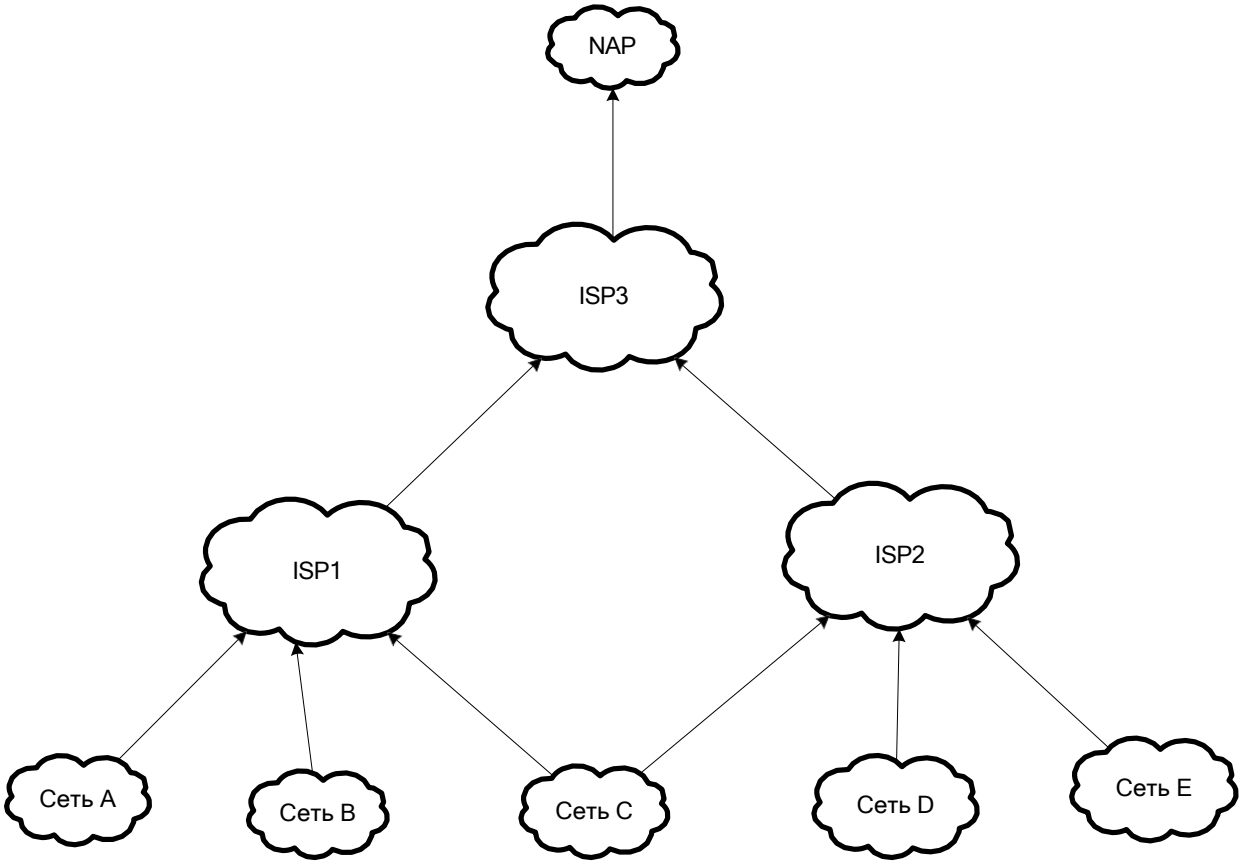
Сеть	Адрес сети	
A	111.17.14.0/23	
B	111.17.28.0/23	
C	122.128.0.0/9	
D	122.0.0.0/10	
E	122.64.0.0/10	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 18

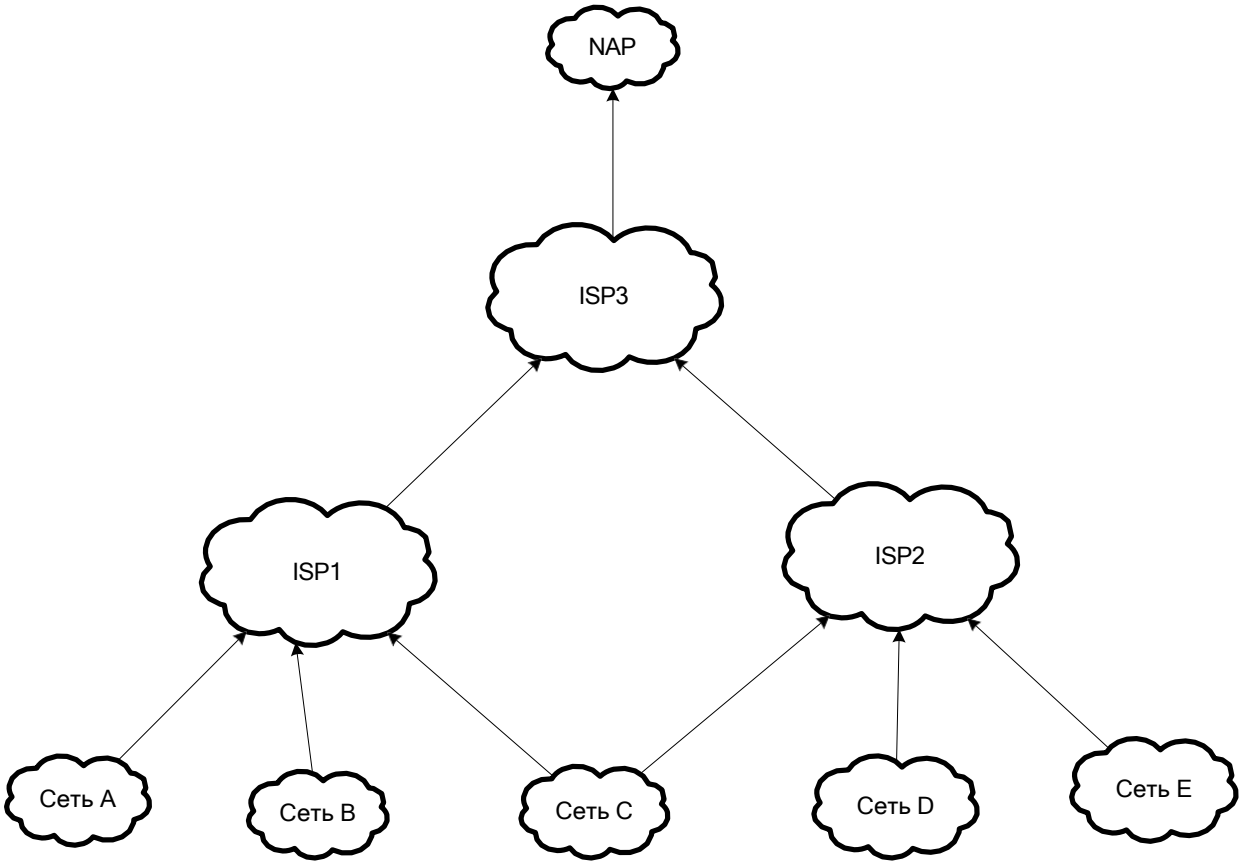
Сеть	Адрес сети	
A	214.6.98.0/24	
B	214.6.100.0/25	
C	214.6.100.128/25	
D	26.145.84.0/24	
E	26.145.85.0/24	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 19

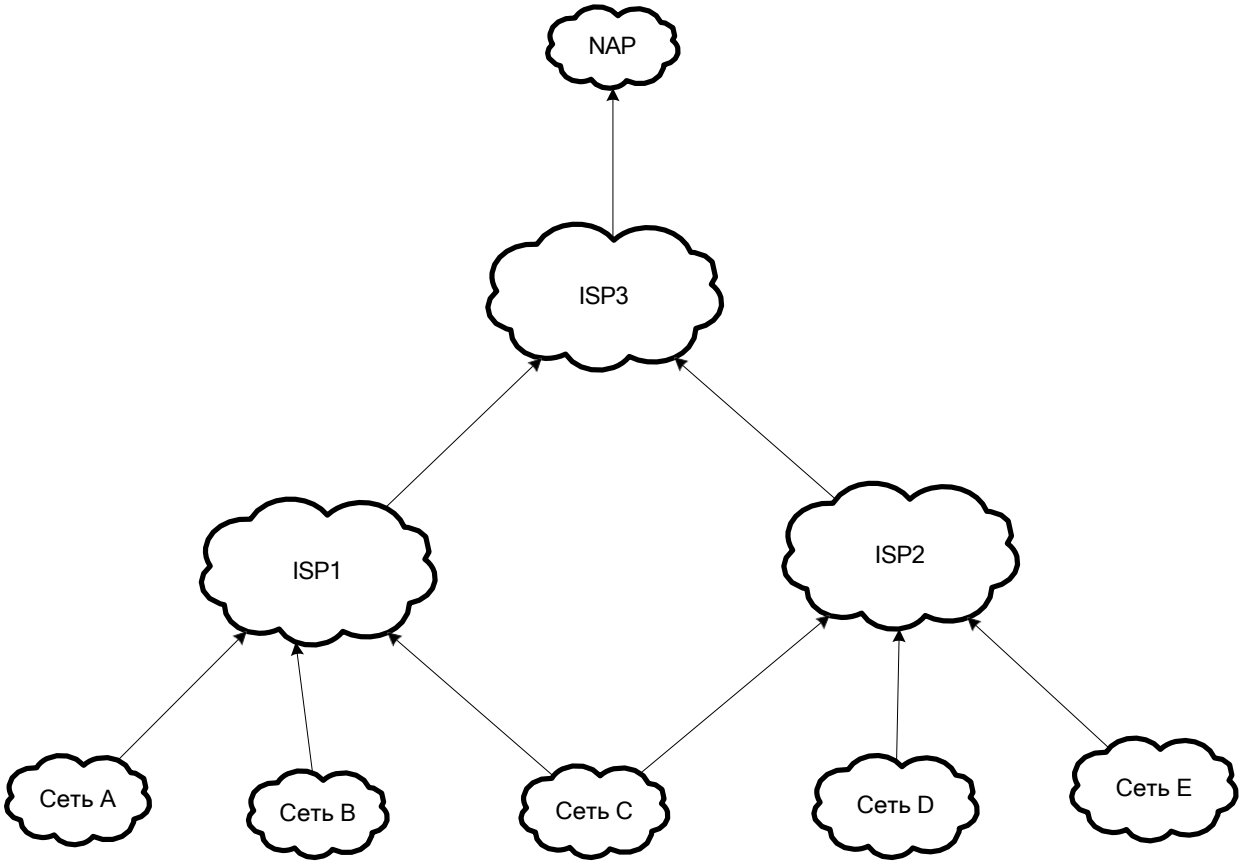
Сеть	Адрес сети
A	76.74.0.0/18
B	76.74.64.0/18
C	76.74.128.0/18
D	76.74.192.0/18
E	76.75.0.0/18



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 20

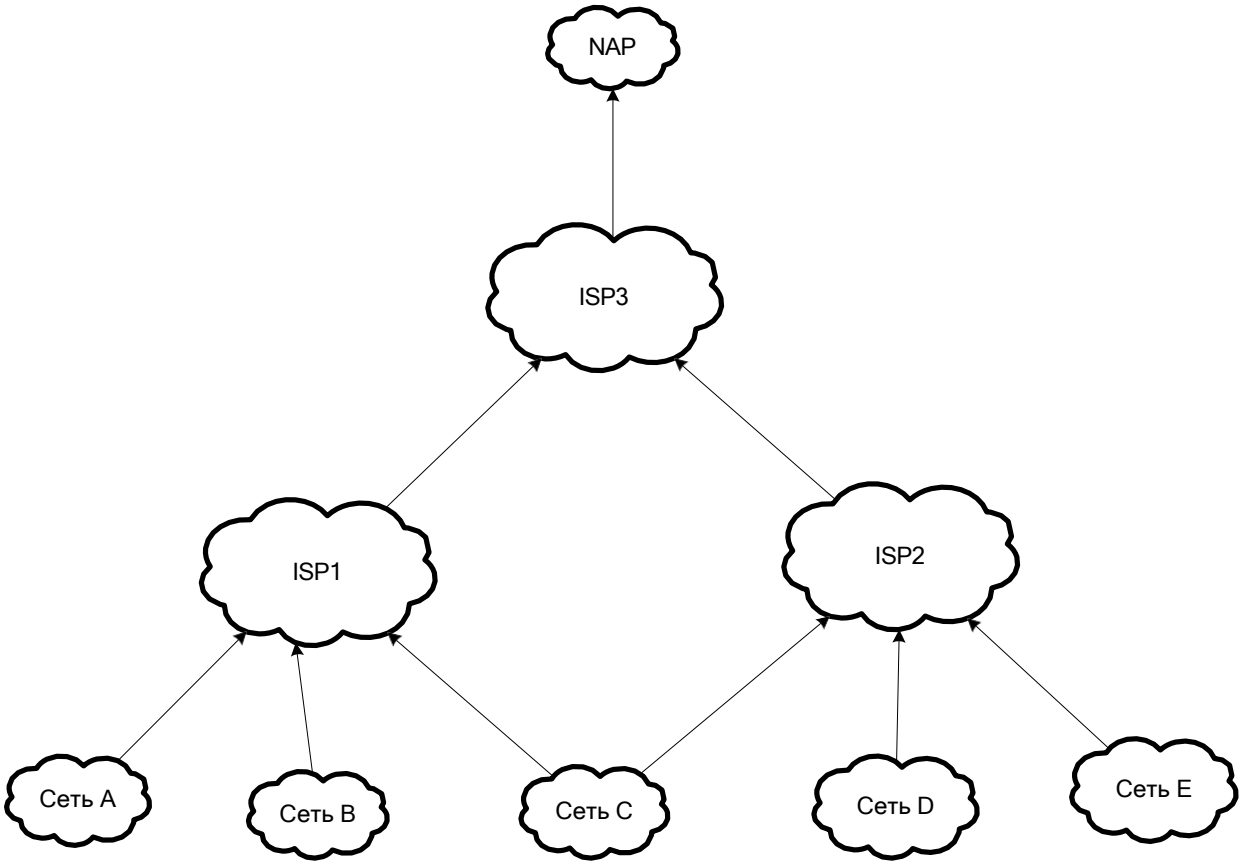
Сеть	Адрес сети	
A	162.16.16.0/20	
B	193.33.33.0/25	
C	193.33.33.128/25	
D	121.128.0.0/9	
E	121.0.0.0/9	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 21

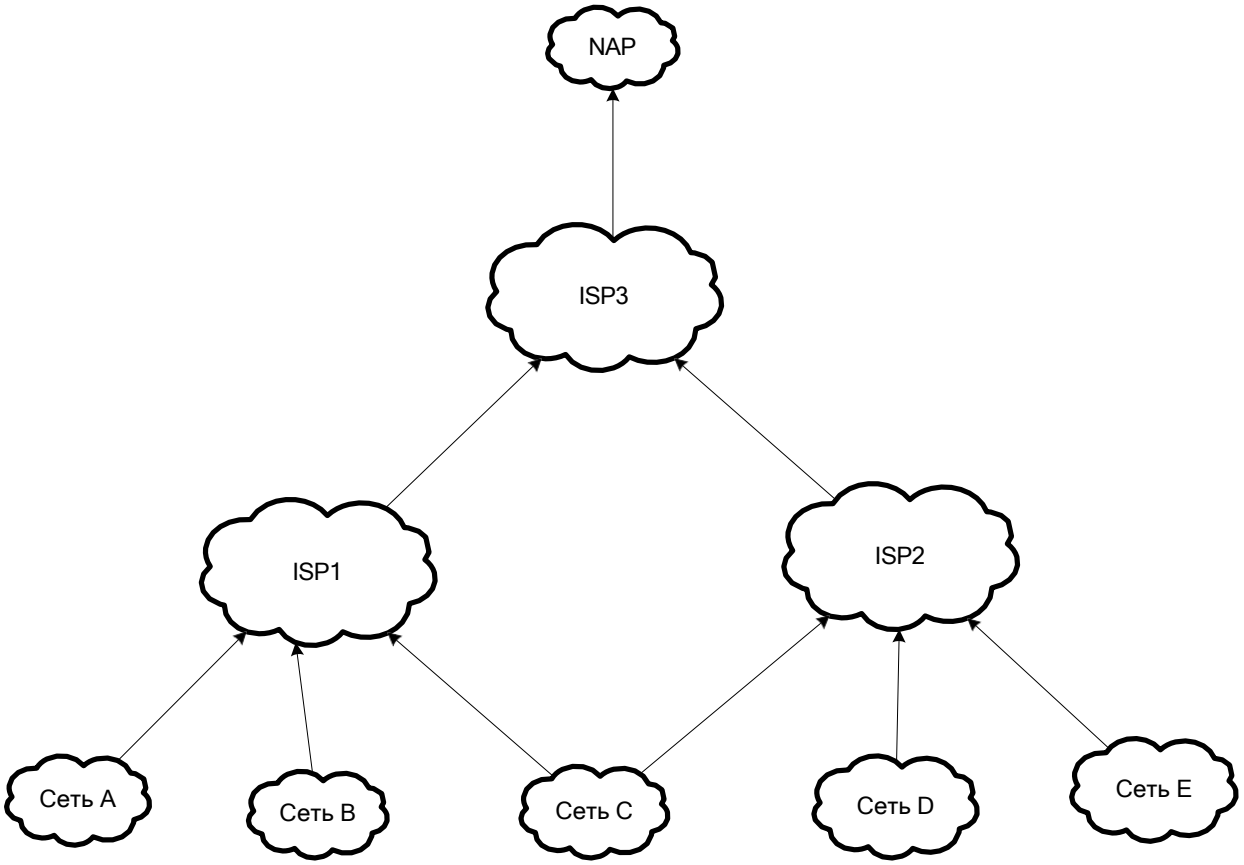
Сеть	Адрес сети	
A	201.18.35.0/26	
B	201.18.35.64/26	
C	201.13.35.128/25	
D	195.28.47.0/25	
E	195.28.47.128/25	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 22

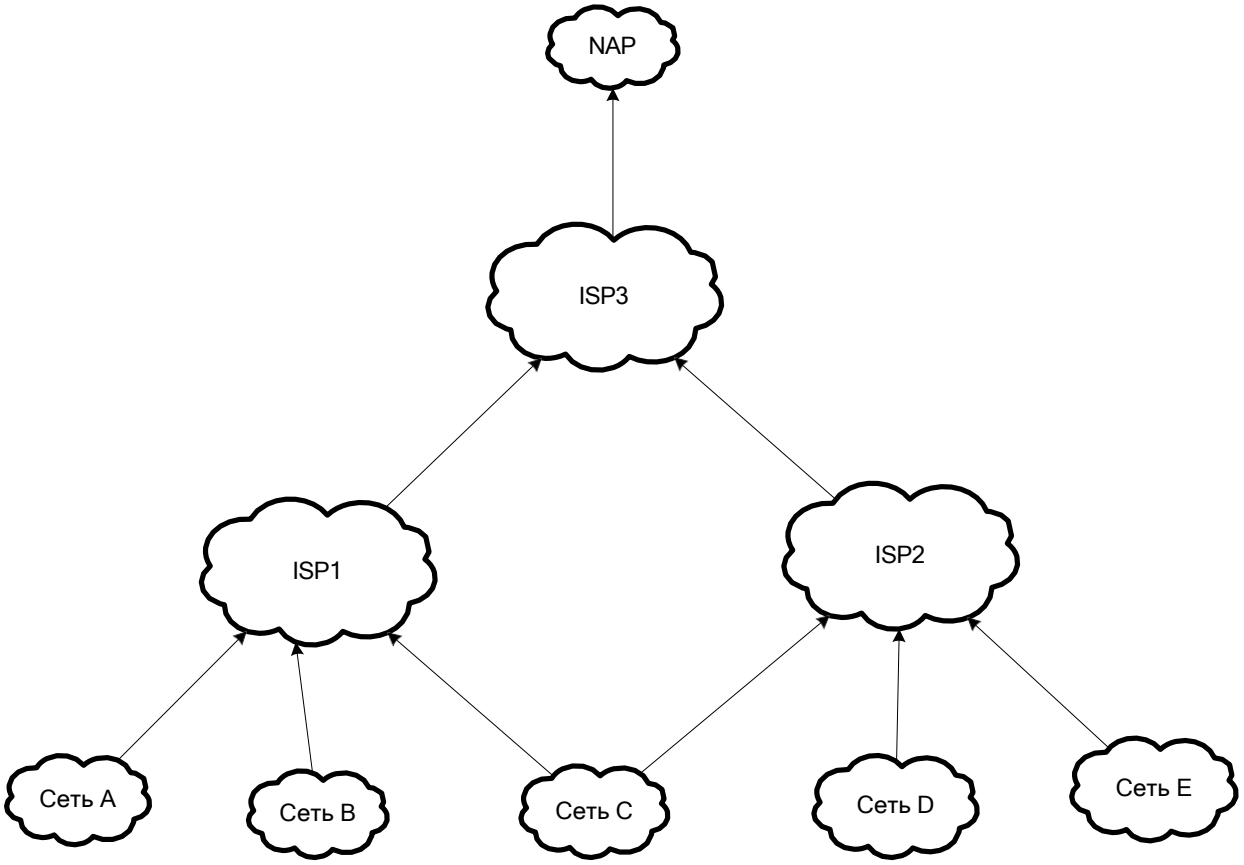
Сеть	Адрес сети	
A	118.67.14.0/23	
B	118.67.28.0/23	
C	12.128.0.0/9	
D	12.0.0.0/10	
E	12.64.0.0/10	



Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 23

Сеть	Адрес сети	
A	216.56.98.0/24	
B	216.56.100.0/25	
C	216.56.100.128/25	
D	56.45.84.0/24	
E	56.45.85.0/24	

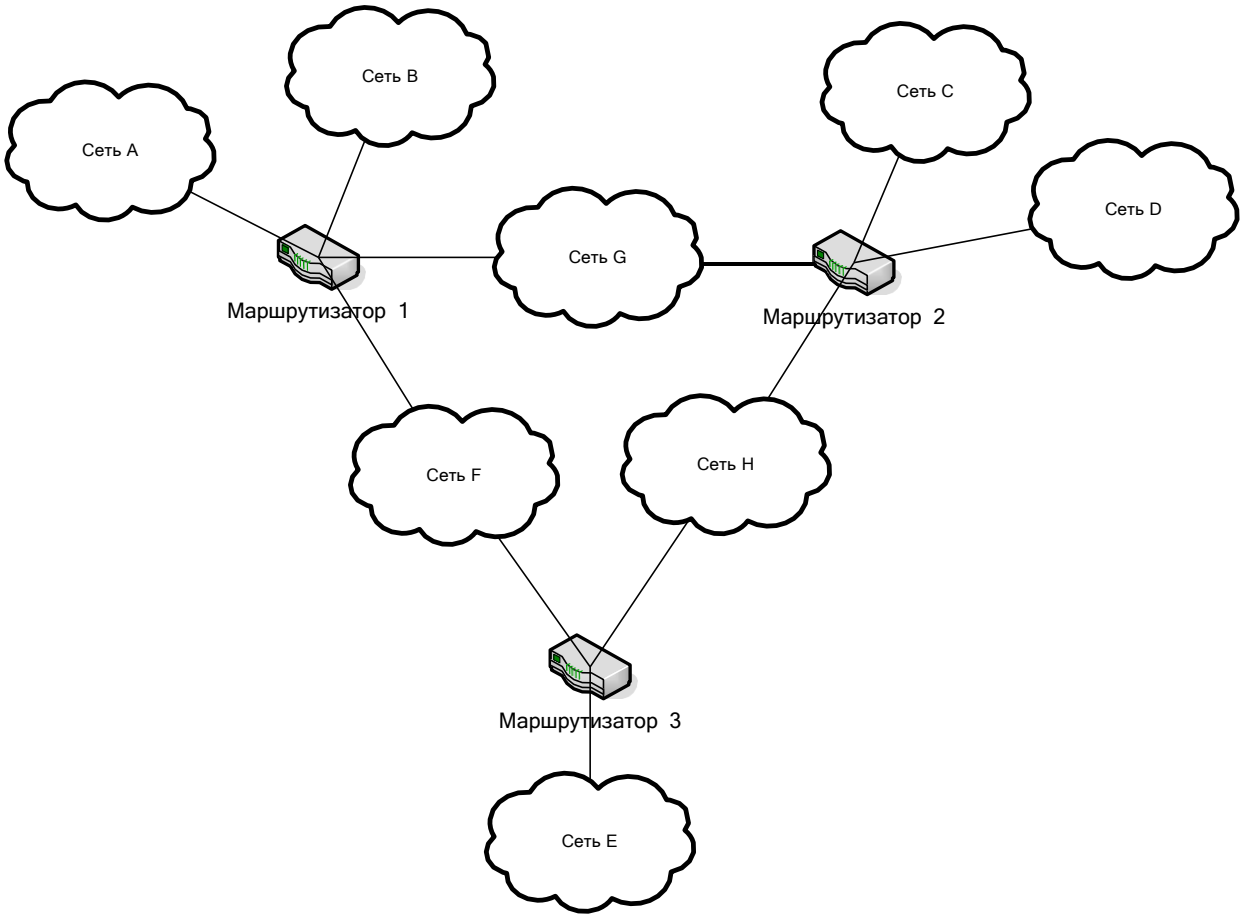


Задана схема подключения сетей. Необходимо определить какие маршруты будут передаваться провайдерами выше по иерархии при использовании технологии CIDR.

Вариант 24

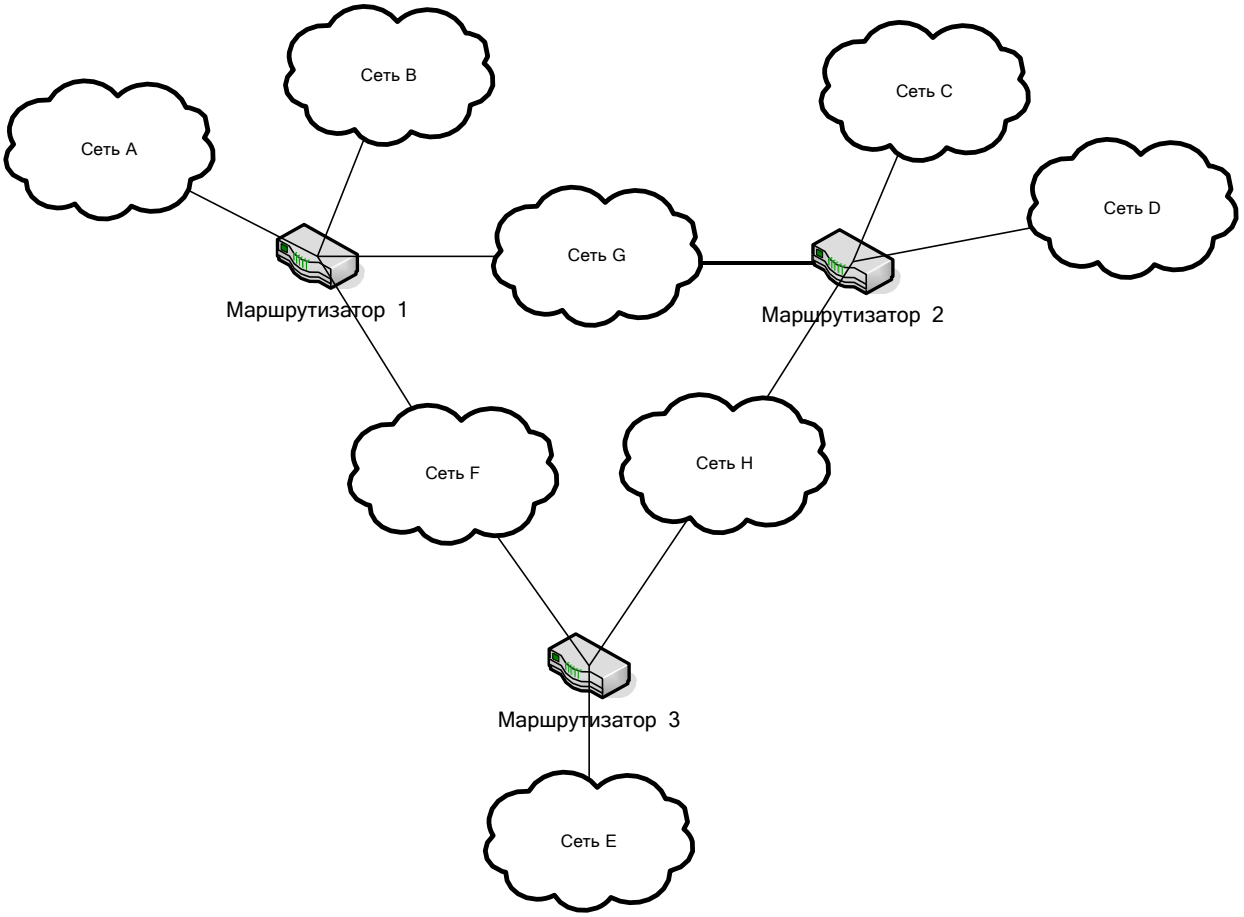
Сеть	Адрес сети
A	143.64.0.0/18
B	143.64.64.0/18
C	143.64.128.0/18
D	143.64.196.0/18
E	143.65.0.0/18

5.6 Варианты заданий на практическую работу по заполнению таблиц маршрутизации



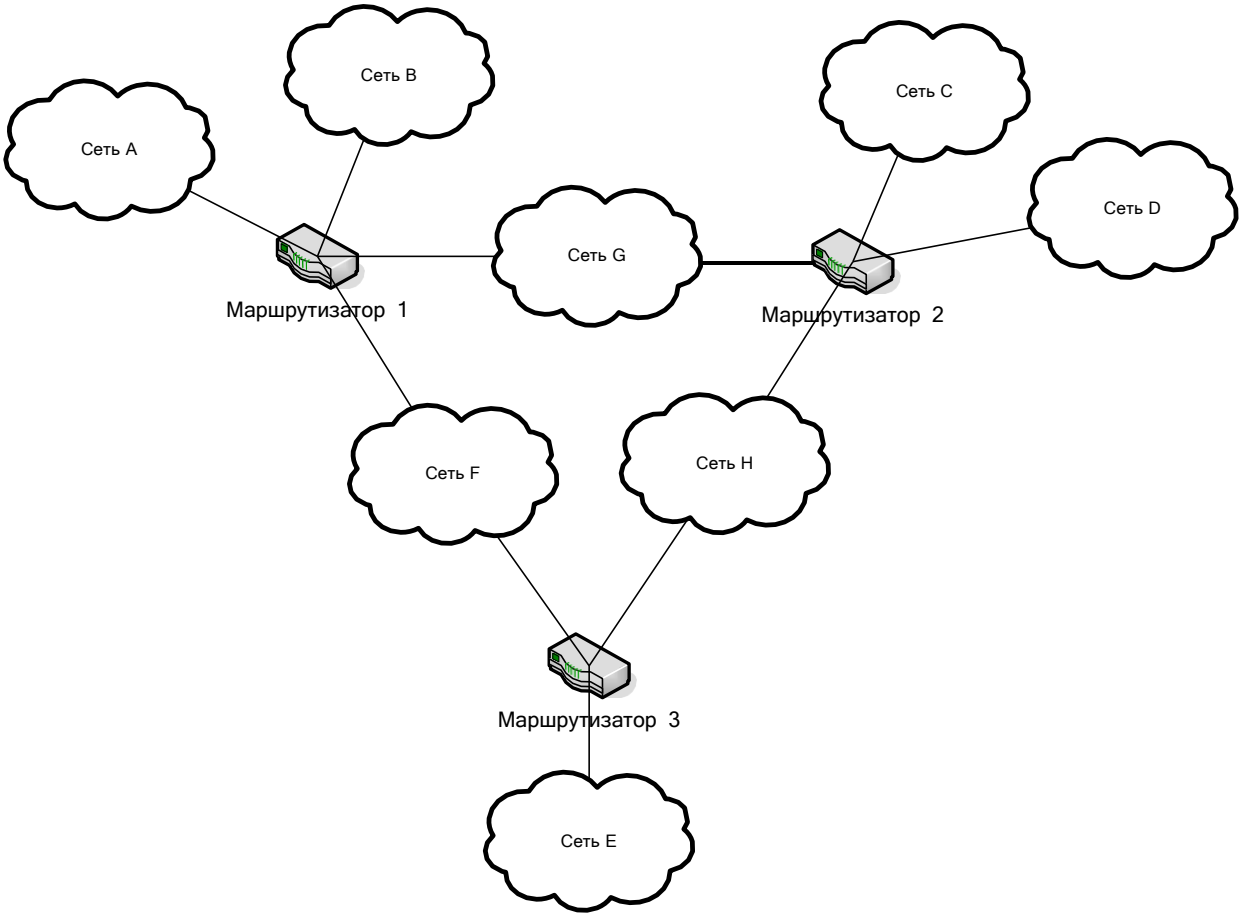
Вариант 1

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	218.75.13.0/26	218.75.13.6/26		
B	148.18.64.0/18	148.18.66.18/18		
C	137.52.0.0/16		137.52.7.215/16	
D	15.128.0.0/10		15.138.76.15/10	
E	216.218.148.32/27			216.218.148.33/27
F	211.152.13.48/28	211.152.13.49/28		211.152.13.50/28
G	211.167.208.64/28	211.167.208.65/28	211.167.208.66/28	
H	211.178.15.80/28		211.178.15.81/28	211.178.15.82/28



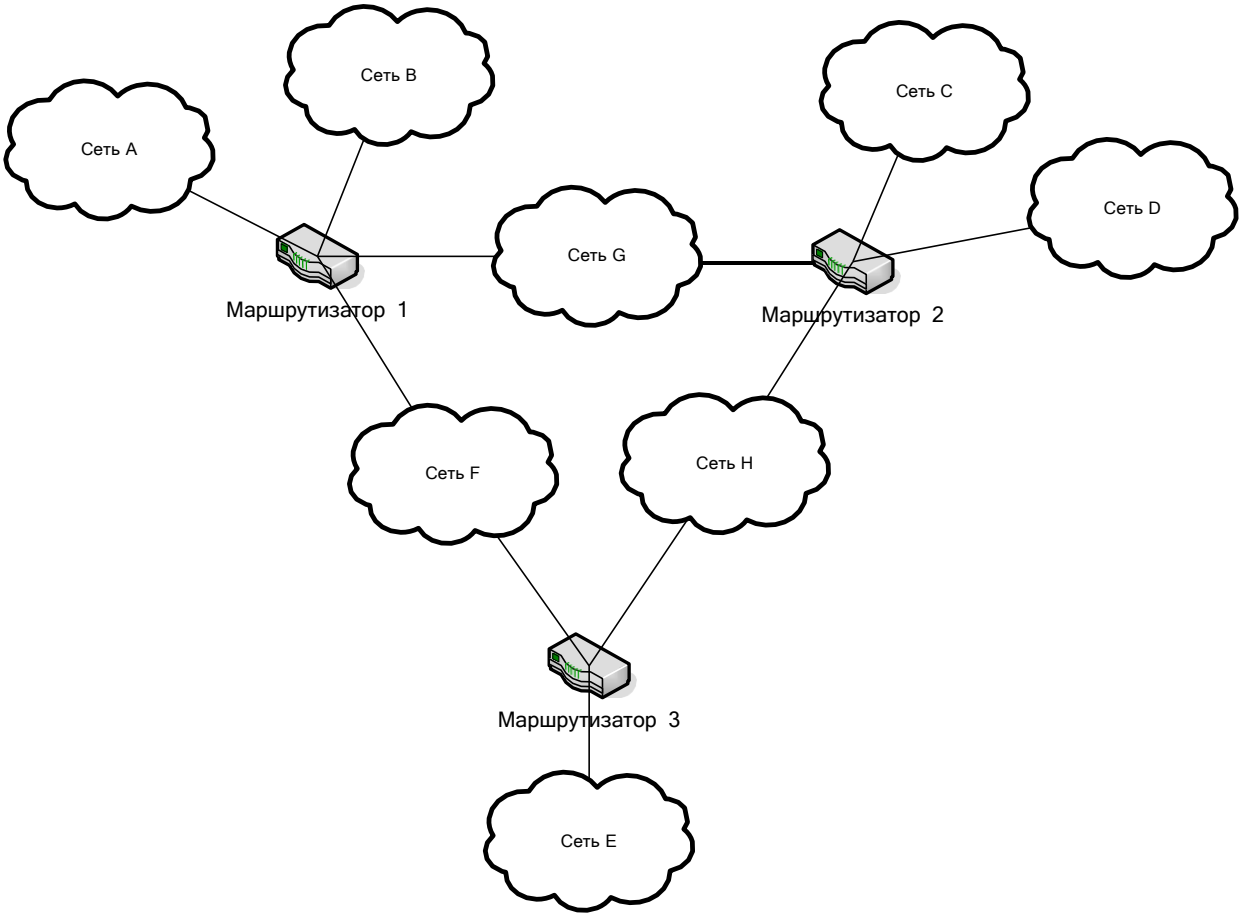
Вариант 2

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.18.64.0/18	148.18.66.123/18		
B	149.18.128.0/18	148.18.137.15/18		
C	218.75.13.64/26		218.75.13.75/26	
D	216.218.148.64/27		216.218.148.73/27	
E	13.0.0.0/8			13.1.1.1/8
F	179.18.64.0/20	179.18.65.1/20		179.18.65.2/20
G	213.157.240.96/28	213.157.240.97/28	213.157.240.98/28	
H	201.118.15.48/28		201.118.15.49/28	201.118.15.50/28



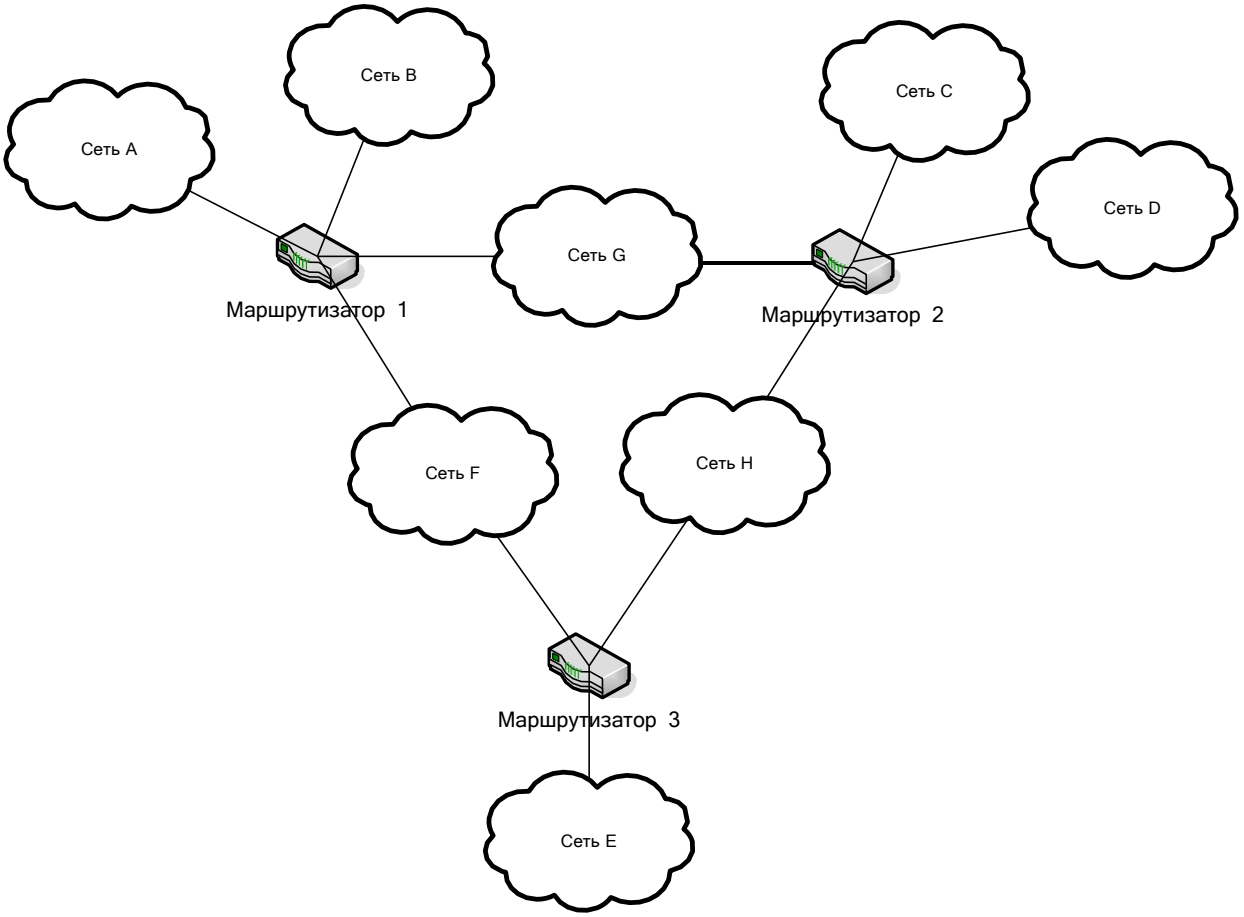
Вариант 3

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.18.0.0/16	148.18.75.18/16		
B	221.153.119.32/27	221.153.119.35/27		
C	15.128.0.0/10		15.138.76.15/10	
D	121.18.90.0/20		121.19.92.15/20	
E	216.218.131.32/27			216.218.131.33/27
F	211.182.17.48/28	211.182.17.49/28		211.182.17.50/28
G	217.157.213.64/28	217.157.213.65/28	217.157.213.66/28	
H	211.178.15.80/28		211.178.15.81/28	211.178.15.82/28



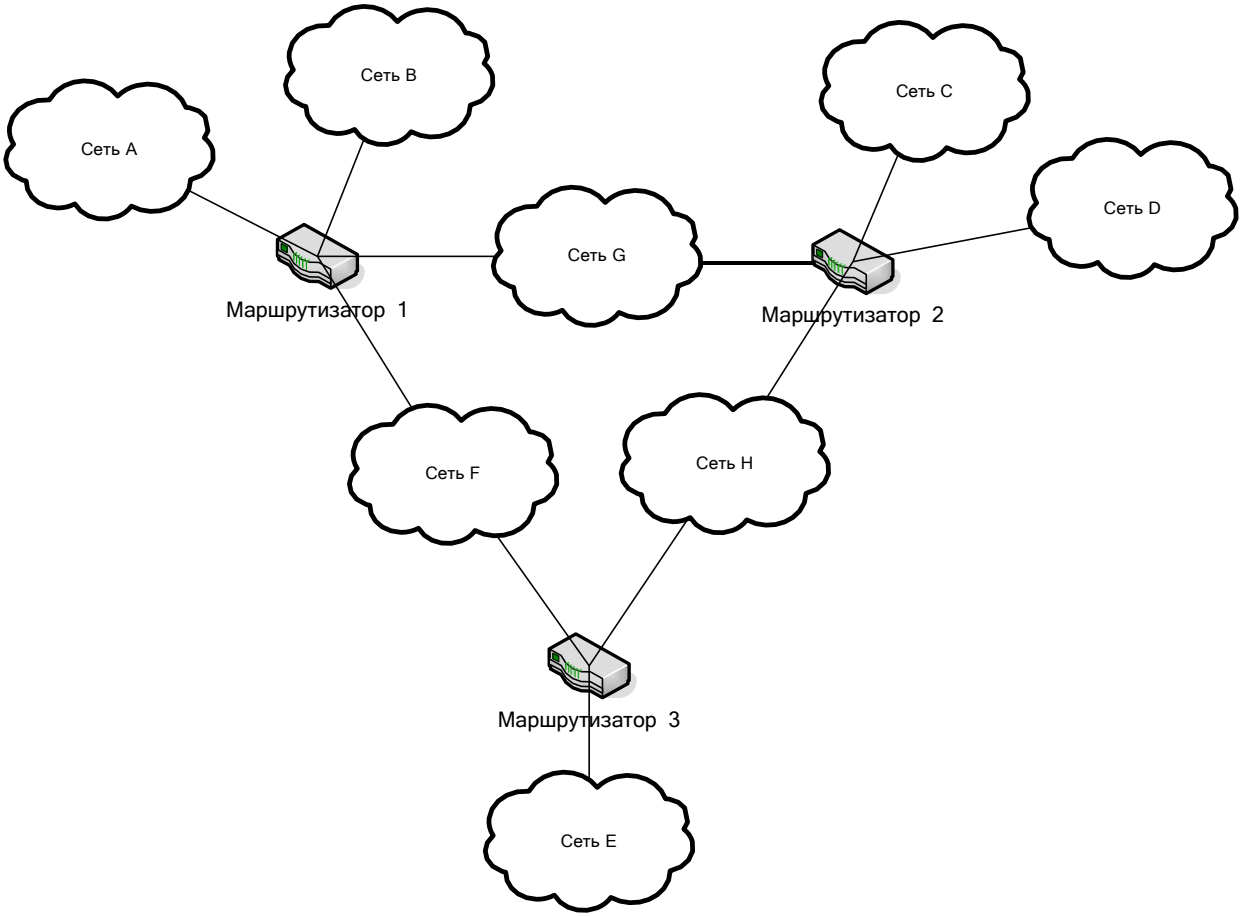
Вариант 4

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	153.15.166.0/24	153.15.166.15/24		
B	9.8.0.0/13	9.8.7.6/13		
C	137.128.64.0/18		137.128.67.99/18	
D	215.215.215.192/26		215.215.215.215/26	
E	18.0.0.0/8			18.18.18.18/8
F	200.200.111.128/28	200.200.111.131/28		200.200.111.132/28
G	222.1.0.0/28	222.1.0.13/28	222.1.0.14/28	
H	199.18.175.112/28		199.18.175.114/28	199.18.175.116/28



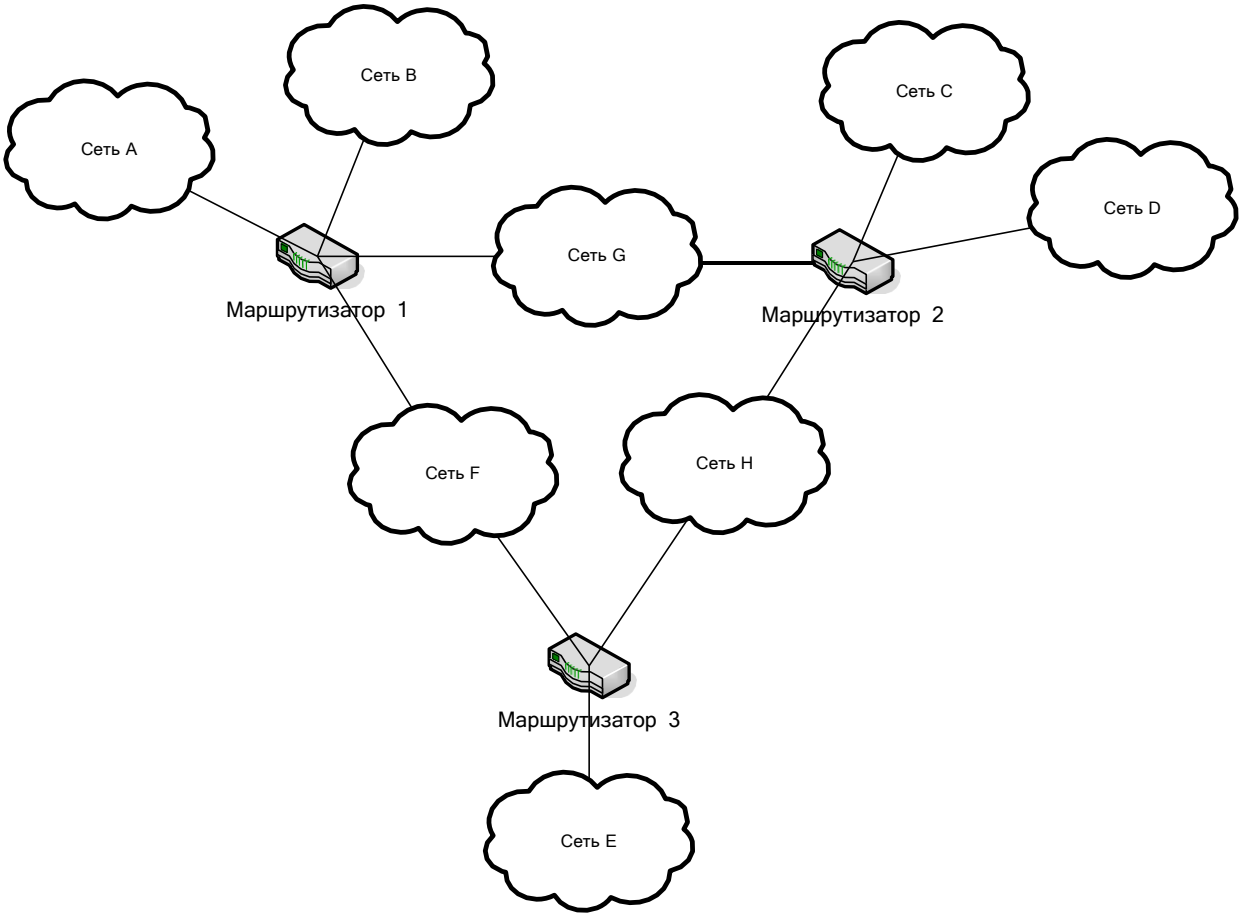
Вариант 5

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	18.80.0.0/12	18.82.35.244/12		
B	215.231.109.192/26	215.231.109.196/26		
C	9.8.0.0/13		9.8.251.250/13	
D	220.18.146.0/24		220.18.146.185/24	
E	35.118.0.0/16			35.118.100.100/16
F	213.13.113.0/26	213.13.113.15/26		213.13.113.16/26
G	218.1.148.144/28	218.1.148.145/28	218.1.148.146/28	
H	193.168.15.64/28		193.168.15.65/28	193.168.15.66/28



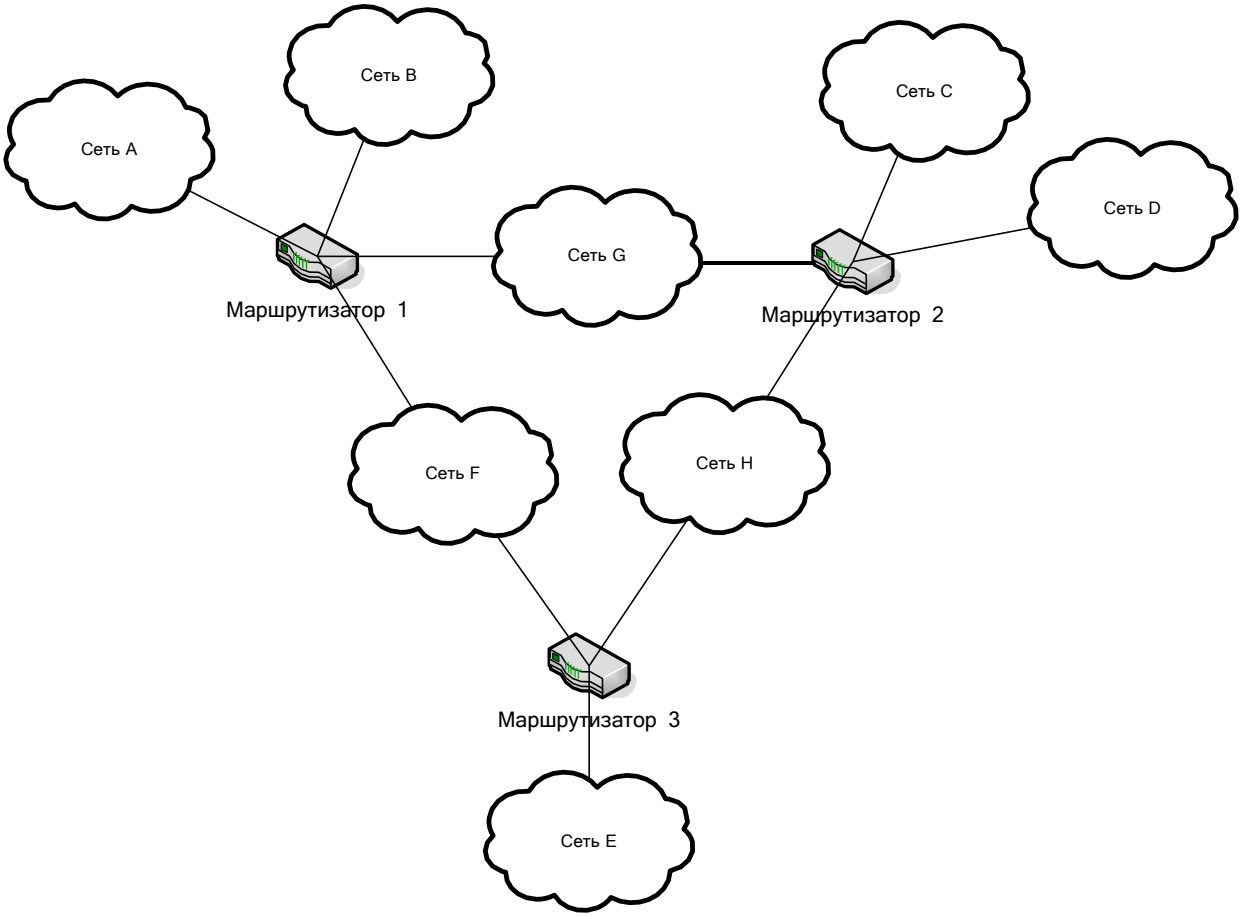
Вариант 6

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.17.128.0/17	148.17.138.115/17		
B	197.148.215.64/26	197.148.215.92/26		
C	137.128.64.0/18		137.128.67.99/18	
D	215.118.96.0/24		215.118.96.48/24	
E	187.26.56.0/23			187.26.57.211/23
F	199.18.175.112/28	199.18.175.114/28		199.18.175.116/28
G	193.168.15.64/28	193.168.15.65/28	193.168.15.66/28	
H	218.1.152.144/28		218.1.152.145/28	218.1.152.146/28



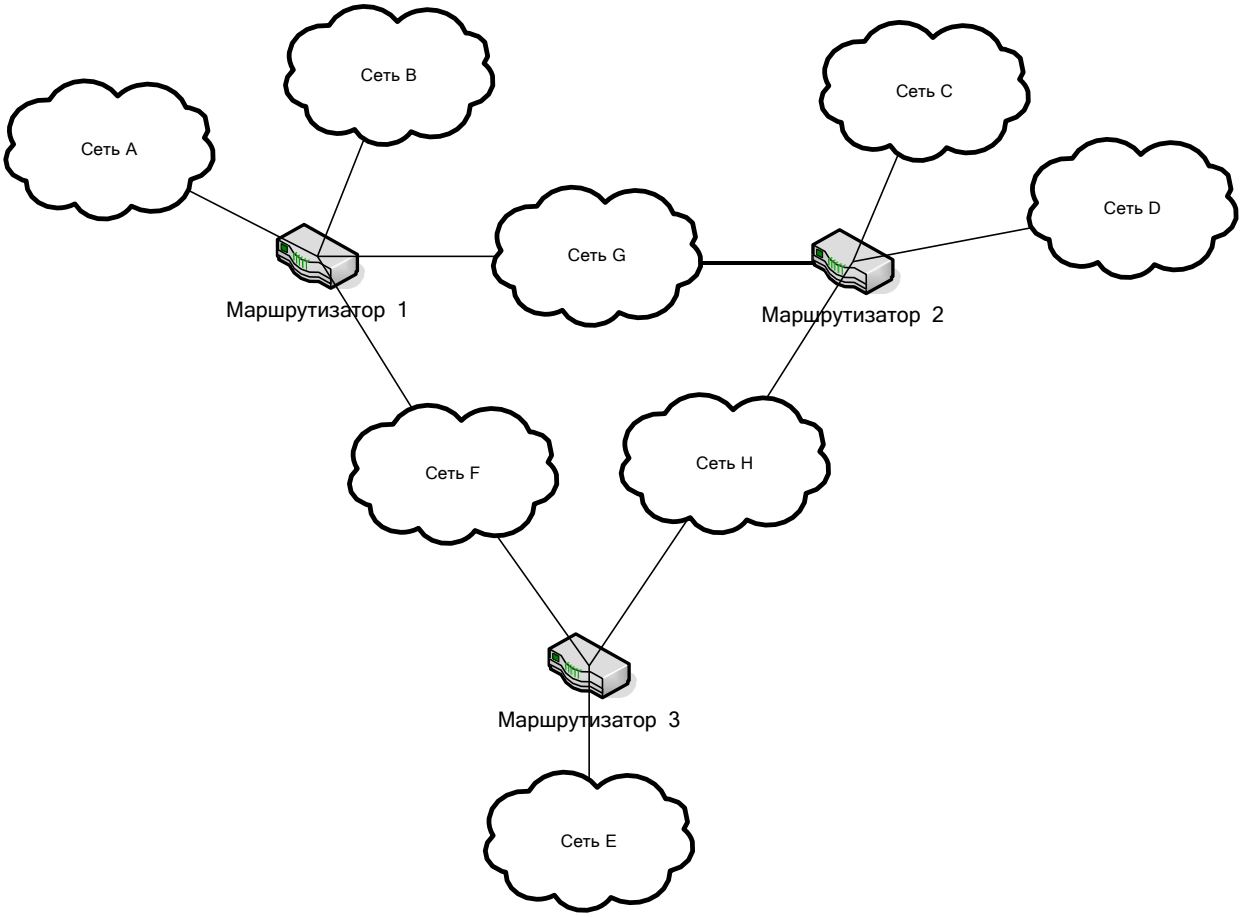
Вариант 7

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	118.115.0.0/16	118.115.21.18/16		
B	211.118.15.0/24	211.118.15.19/24		
C	97.128.0.0/9		97.128.18.235/9	
D	196.44.36.0/24		196.44.36.36/24	
E	218.56.136.128/26			218.56.136.132/26
F	201.116.18.64/28	201.116.18.65/28		201.116.18.66/28
G	203.86.35.80/28	203.86.35.81/28	203.86.35.82/28	
H	197.221.56.128/28		197.221.56.129/28	197.221.56.130/28



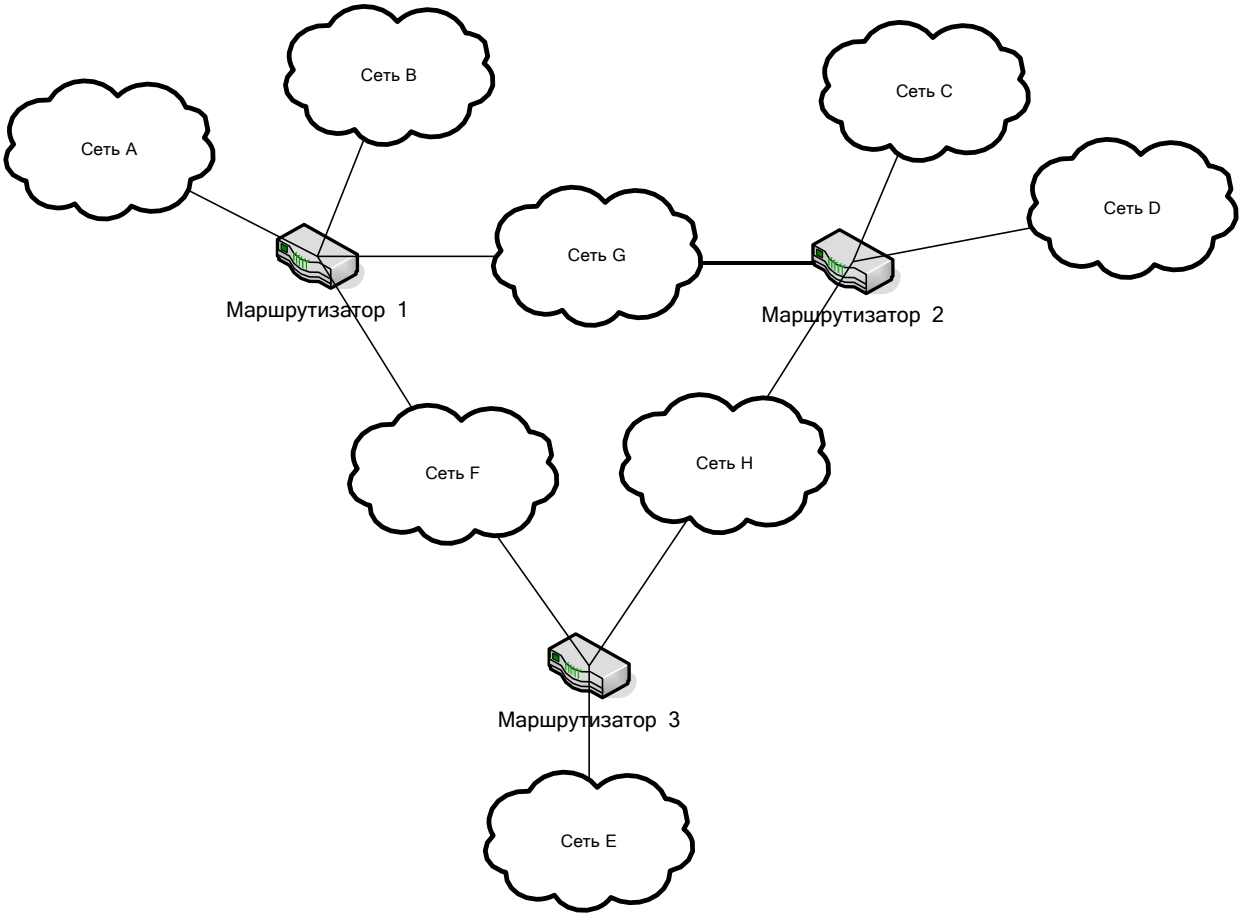
Вариант 8

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	220.18.46.0/24	220.18.46.35/24		
B	182.138.0.0/16	182.138.18.46/16		
C	204.39.183.128/25		204.39.183.196/25	
D	205.46.38.0/24		205.46.38.118/24	
E	47.128.0.0/10			47.128.35.153/10
F	222.11.12.0/29	222.11.12.1/29		222.11.12.2/29
G	222.11.13.0/29	222.11.13.1/29	222.11.13.2/29	
H	222.11.14.0/29		222.11.14.1/29	222.11.14.2/29



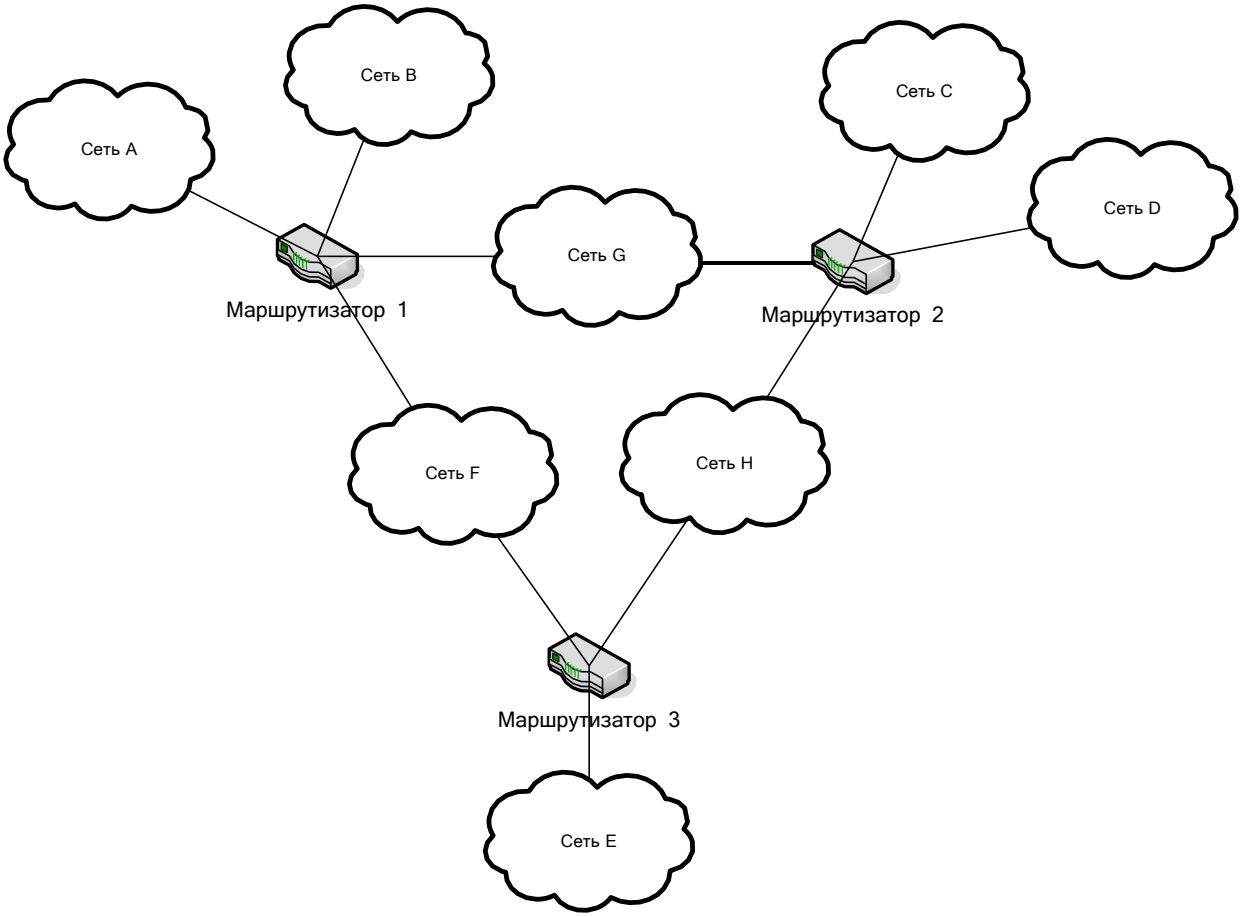
Вариант 9

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	15.0.0.0/8	15.35.46.38/8		
B	207.11.181.0/16	207.11.181.12/16		
C	212.48.56.0/24		212.48.56.38/24	
D	183.21.0.0/16		183.21.46.182/16	
E	206.35.48.64/26			206.35.48.66/26
F	221.35.48.0/28	221.35.48.1/28		221.35.48.2/28
G	223.48.121.192/28	223.48.121.193/28	223.48.121.194/28	
H	225.121.39.208/28		225.121.39.209/28	225.121.39.210/28



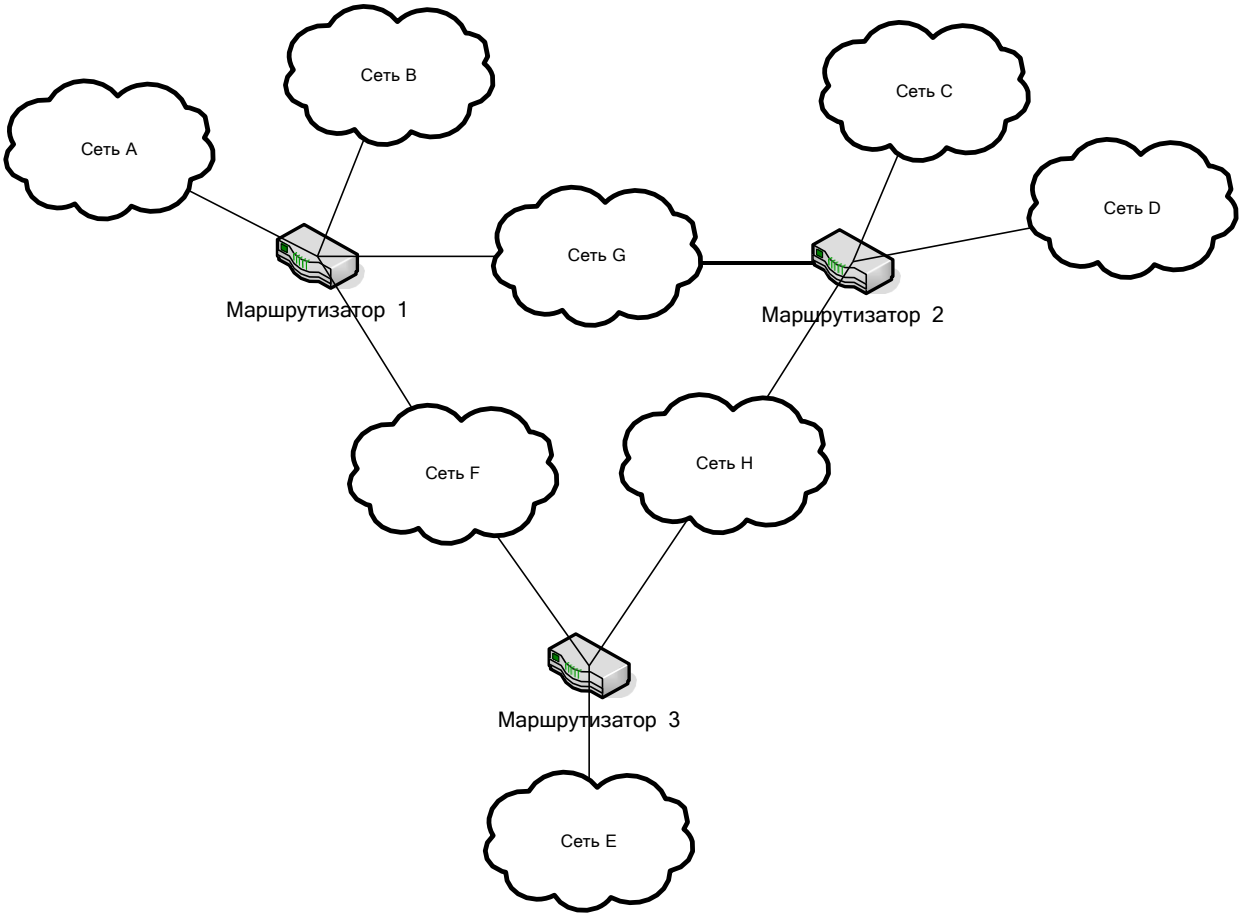
Вариант 10

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	13.0.0.0/8	13.13.13.13/8		
B	146.92.0.0/16	146.92.35.78/16		
C	193.18.48.0/24		193.18.48.35/24	
D	211.81.146.64/26		211.81.146.65/26	
E	211.149.37.0/24			211.149.37.245/24
F	197.1.1.0/28	197.1.1.1/28		197.1.1.11/28
G	197.1.2.0/28	197.1.2.3/28	197.1.2.4/28	
H	197.1.3.0/28		197.1.3.4/28	197.1.3.6/28



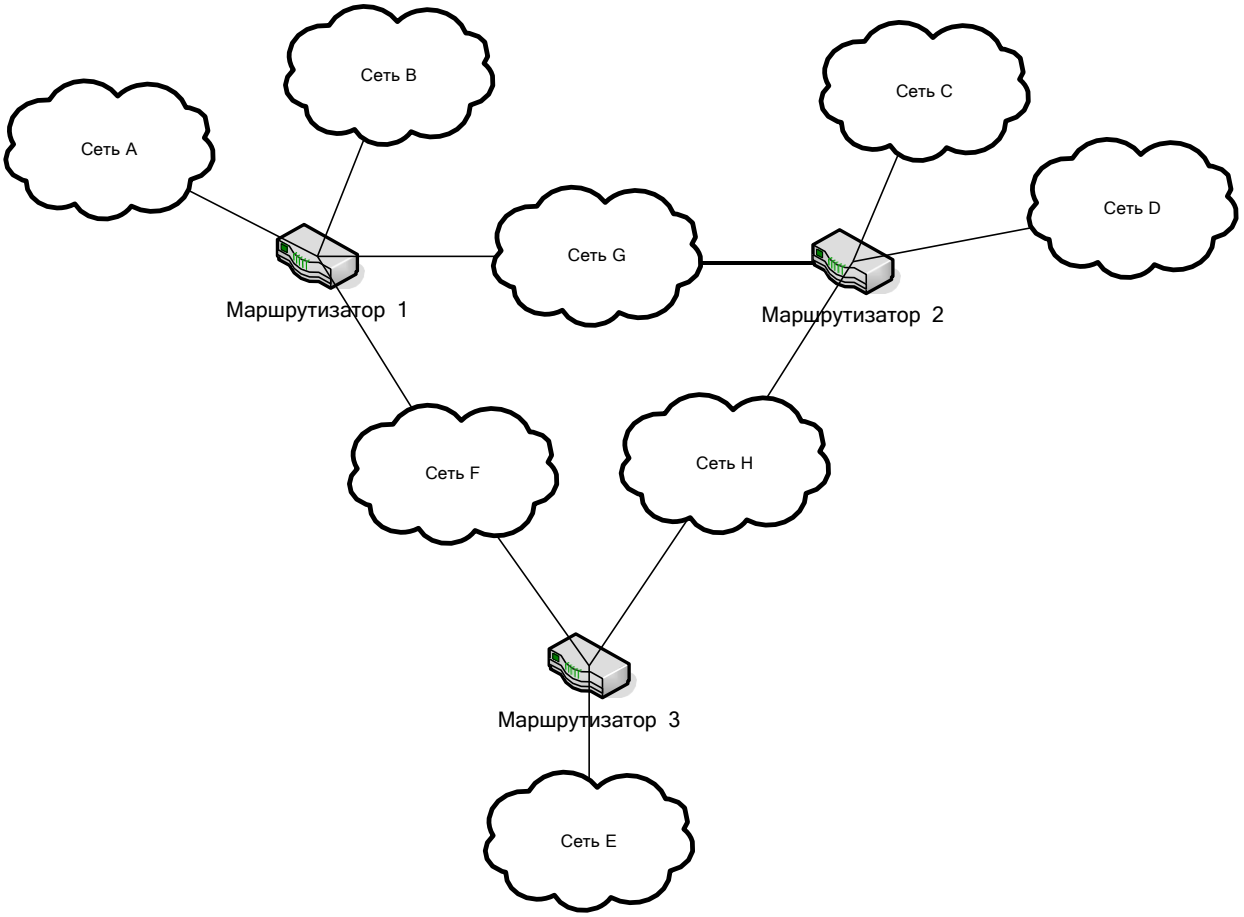
Вариант 11

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.17.128.0/17	148.17.138.115/17		
B	197.148.215.64/26	197.148.215.92/26		
C	137.128.64.0/18		137.128.67.99/18	
D	220.18.146.0/24		220.18.146.185/24	
E	35.118.0.0/16			35.118.100.100/16
F	200.200.111.128/28	200.200.111.131/28		200.200.111.132/28
G	222.1.0.0/28	222.1.0.13/28	222.1.0.14/28	
H	199.18.175.112/28		199.18.175.114/28	199.18.175.116/28



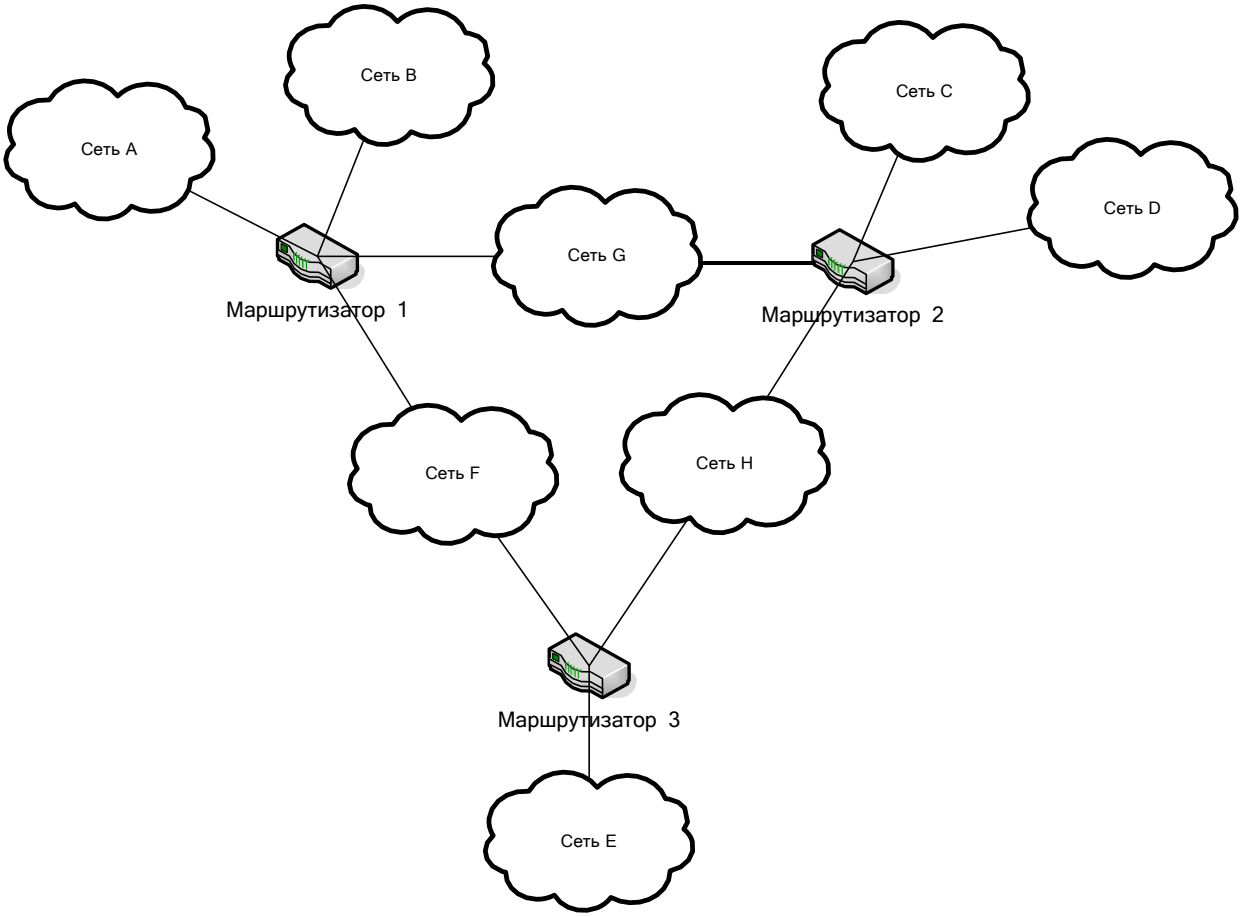
Вариант 12

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	18.80.0.0/12	18.82.35.244/12		
B	215.231.109.192/26	215.231.109.196/26		
C	9.8.0.0/13		9.8.251.250/13	
D	215.118.96.0/24		215.118.96.48/24	
E	187.26.56.0/23			187.26.57.211/23
F	199.18.175.112/28	199.18.175.114/28		199.18.175.116/28
G	217.157.213.64/28	217.157.213.65/28	217.157.213.66/28	
H	211.178.15.80/28		211.178.15.81/28	211.178.15.82/28



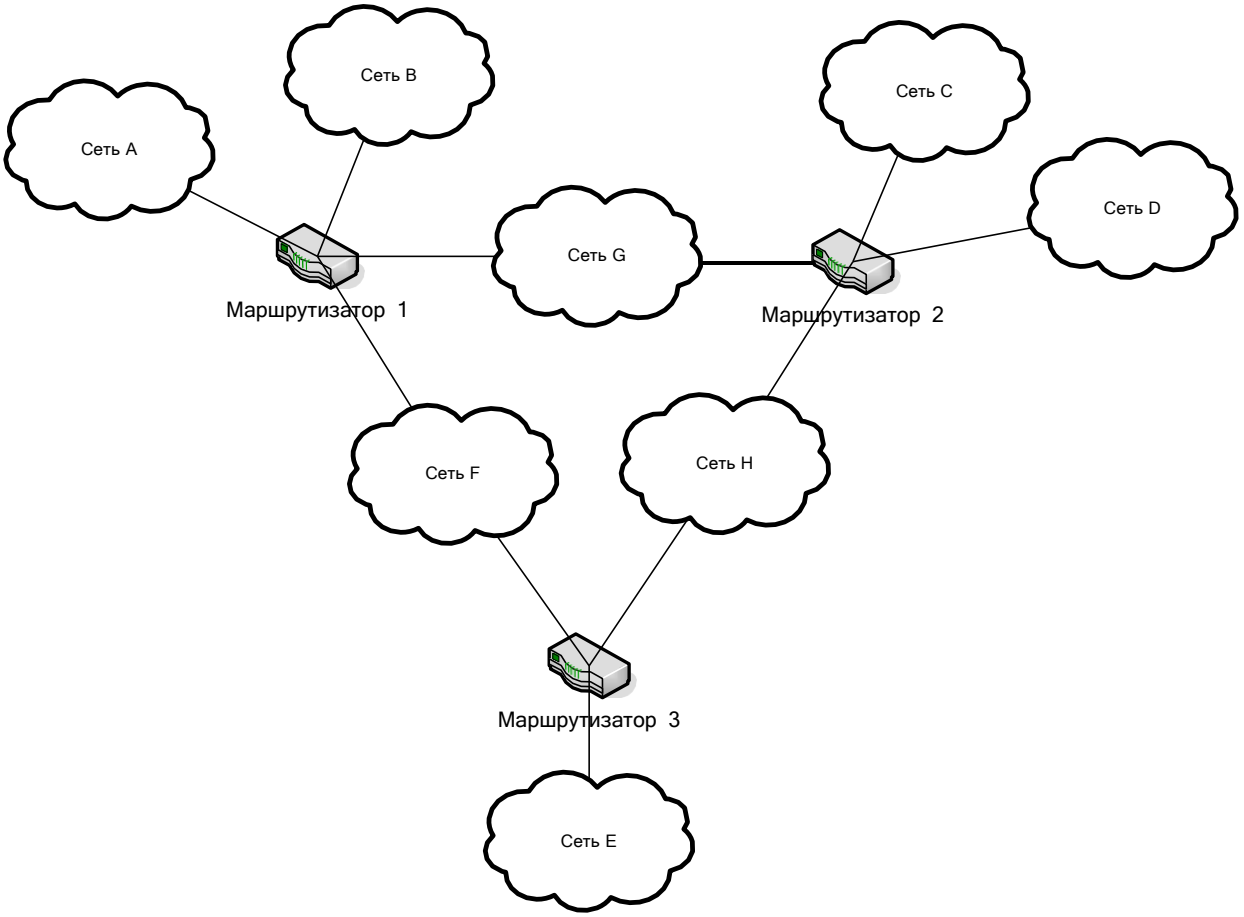
Вариант 13

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	153.15.166.0/24	153.15.166.15/24		
B	9.8.0.0/13	9.8.7.6/13		
C	137.128.64.0/18		137.128.67.99/18	
D	215.215.215.192/26		215.215.215.215/26	
E	18.0.0.0/8			18.18.18.18/8
F	213.13.113.0/26	213.13.113.15/26		213.13.113.16/26
G	193.168.15.64/28	193.168.15.65/28	193.168.15.66/28	
H	218.1.152.144/28		218.1.152.145/28	218.1.152.146/28



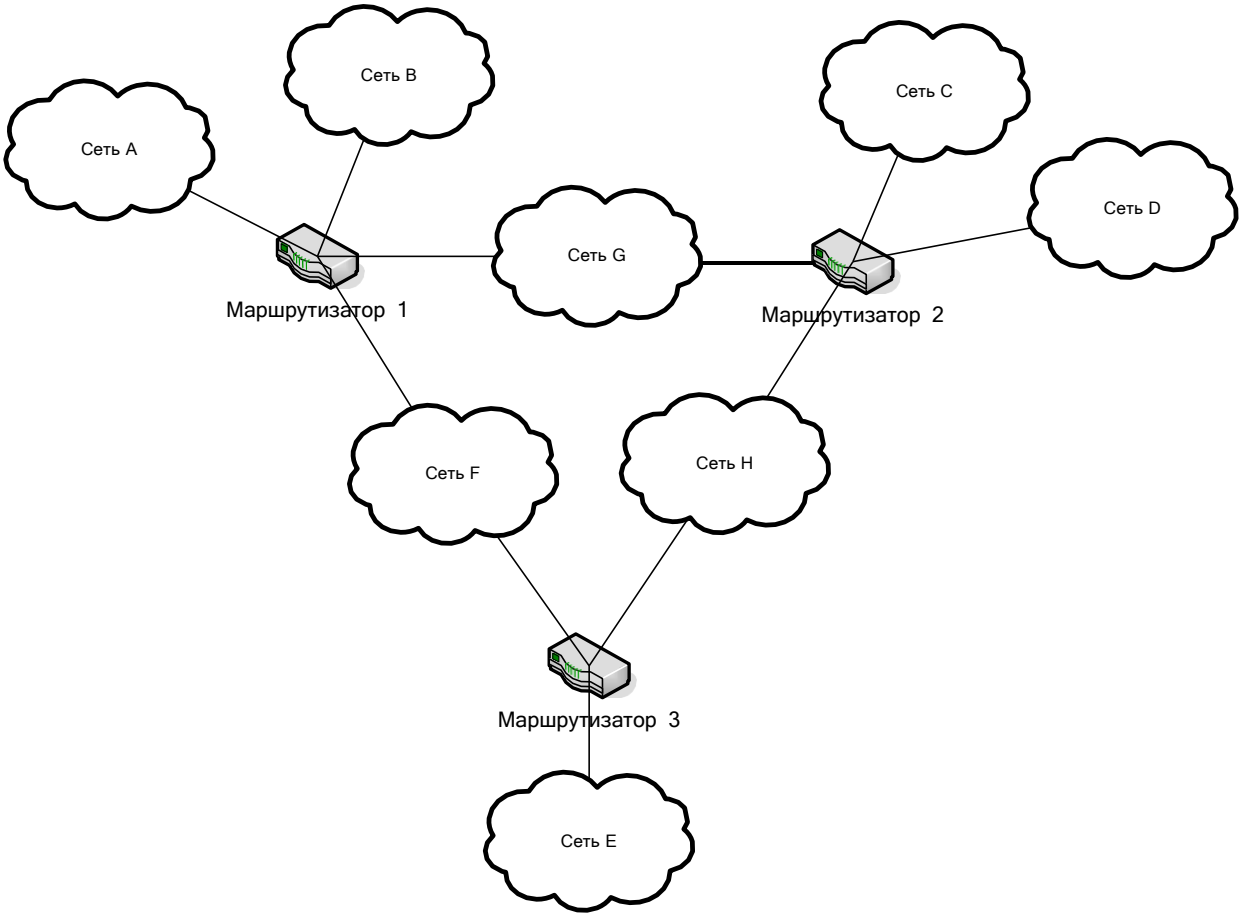
Вариант 14

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.18.0.0/16	148.18.75.18/16		
B	221.153.119.32/27	221.153.119.35/27		
C	137.52.0.0/16		137.52.7.215/16	
D	15.128.0.0/10		15.138.76.15/10	
E	216.218.148.32/27			216.218.148.33/27
F	213.13.113.0/26	213.13.113.15/26		213.13.113.16/26
G	218.1.148.144/28	218.1.148.145/28	218.1.148.146/28	
H	193.168.15.64/28		193.168.15.65/28	193.168.15.66/28



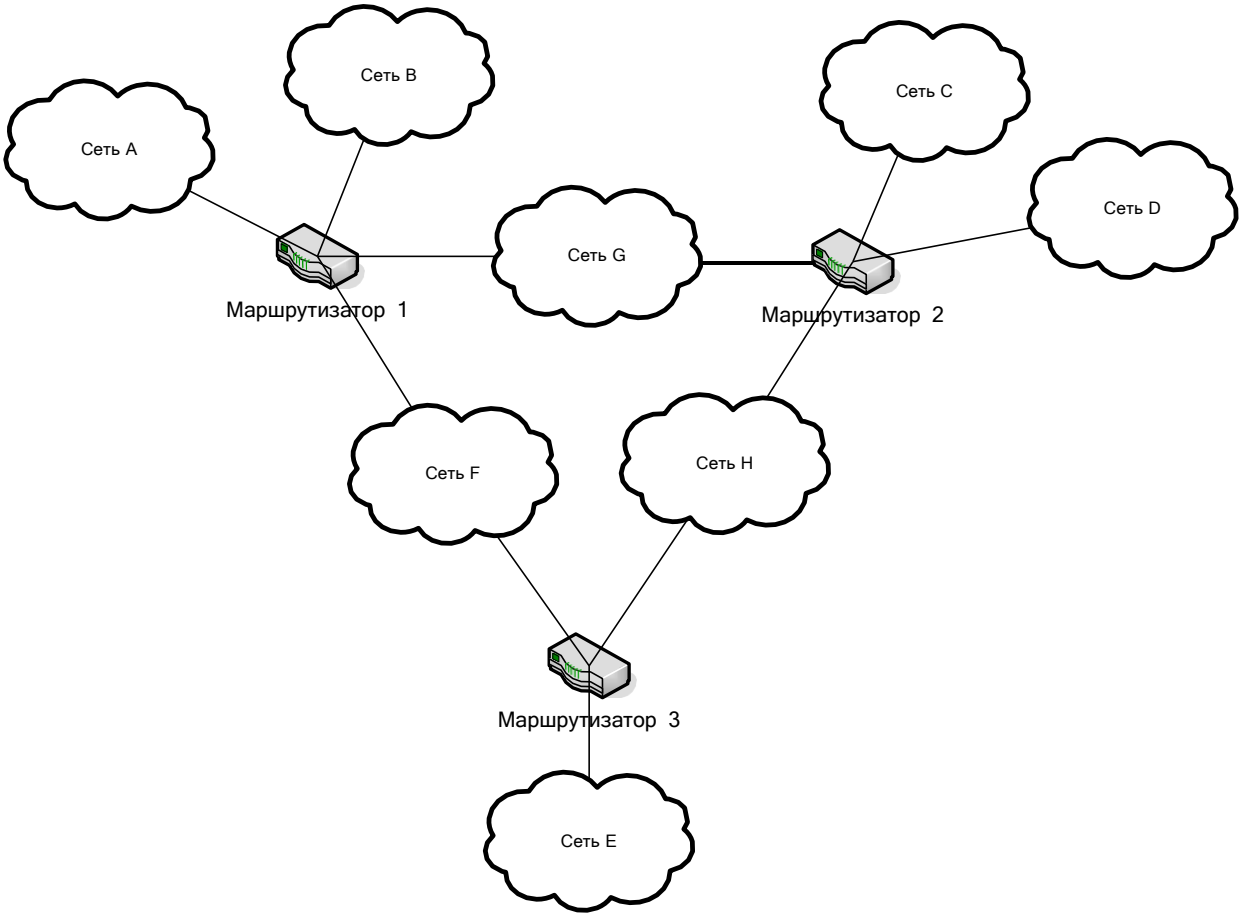
Вариант 15

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	218.75.13.0/26	218.75.13.6/26		
B	148.18.64.0/18	148.18.66.18/18		
C	15.128.0.0/10		15.138.76.15/10	
D	121.18.90.0/20		121.19.92.15/20	
E	216.218.131.32/27			216.218.131.33/27
F	200.200.111.128/28	200.200.111.131/28		200.200.111.132/28
G	211.167.208.64/28	211.167.208.65/28	211.167.208.66/28	
H	211.178.15.80/28		211.178.15.81/28	211.178.15.82/28



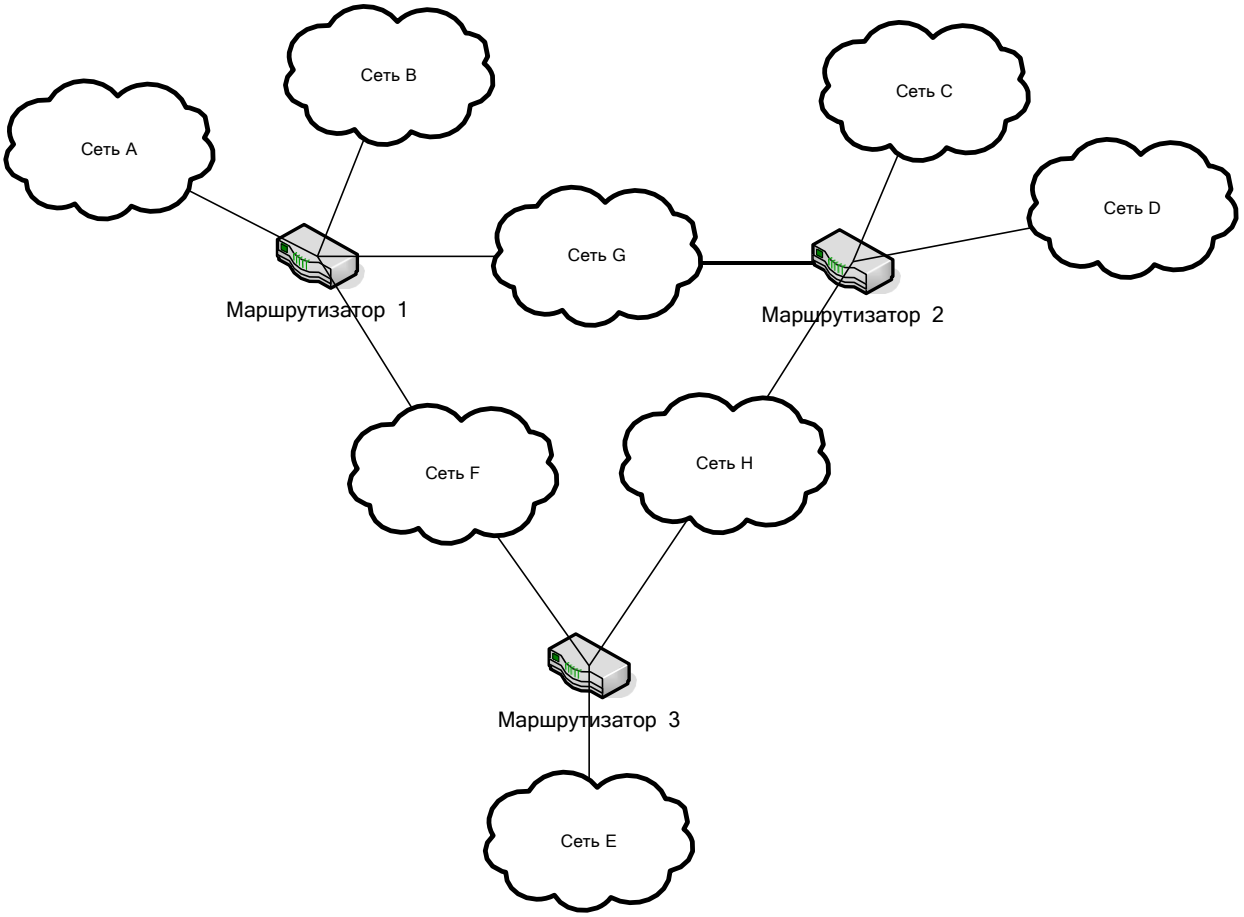
Вариант 16

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	220.18.46.0/24	220.18.46.35/24		
B	182.138.0.0/16	182.138.18.46/16		
C	212.48.56.0/24		212.48.56.38/24	
D	183.21.0.0/16		183.21.46.182/16	
E	211.149.37.0/24			211.149.37.245/24
F	197.1.1.0/28	197.1.1.1/28		197.1.1.11/28
G	197.1.2.0/28	197.1.2.3/28	197.1.2.4/28	
H	197.1.3.0/28		197.1.3.4/28	197.1.3.6/28



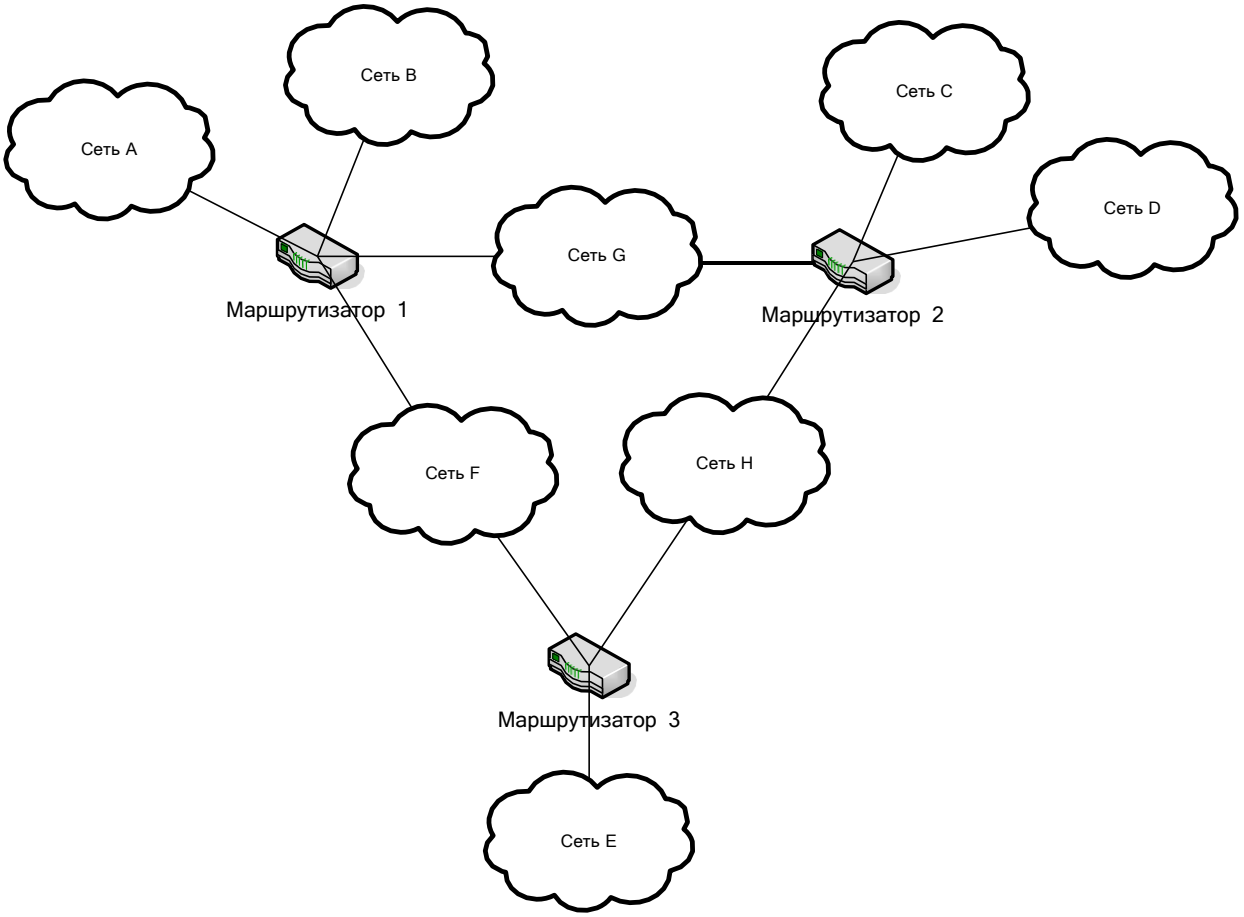
Вариант 17

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	15.0.0.0/8	15.35.46.38/8		
B	207.11.181.0/16	207.11.181.12/16		
C	204.39.183.128/25		204.39.183.196/25	
D	205.46.38.0/24		205.46.38.118/24	
E	211.149.37.0/24			211.149.37.245/24
F	197.1.1.0/28	197.1.1.1/28		197.1.1.11/28
G	197.1.2.0/28	197.1.2.3/28	197.1.2.4/28	
H	197.1.3.0/28		197.1.3.4/28	197.1.3.6/28



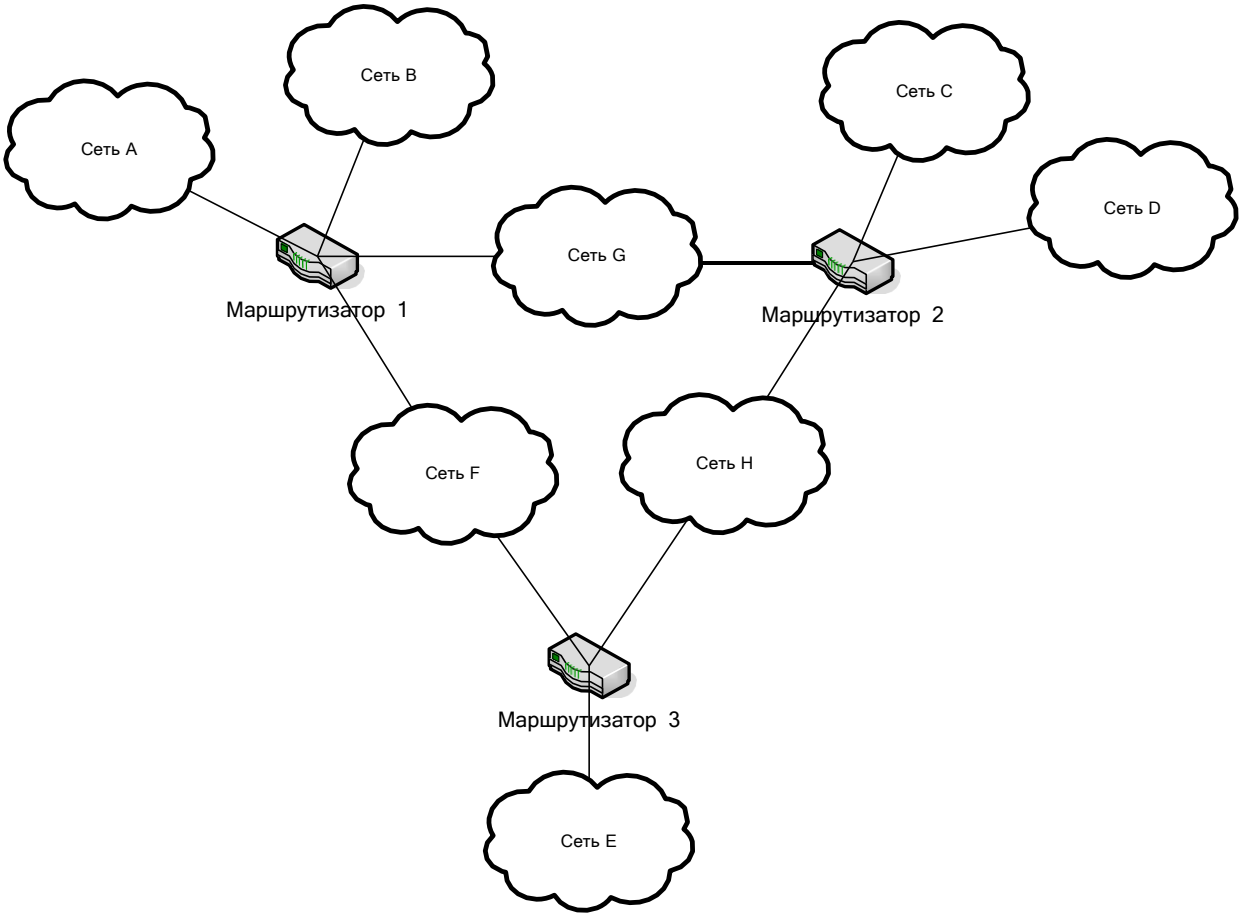
Вариант 18

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	13.0.0.0/8	13.13.13.13/8		
B	146.92.0.0/16	146.92.35.78/16		
C	193.18.48.0/24		193.18.48.35/24	
D	211.81.146.64/26		211.81.146.65/26	
E	47.128.0.0/10			47.128.35.153/10
F	222.11.12.0/29	222.11.12.1/29		222.11.12.2/29
G	222.11.13.0/29	222.11.13.1/29	222.11.13.2/29	
H	222.11.14.0/29		222.11.14.1/29	222.11.14.2/29



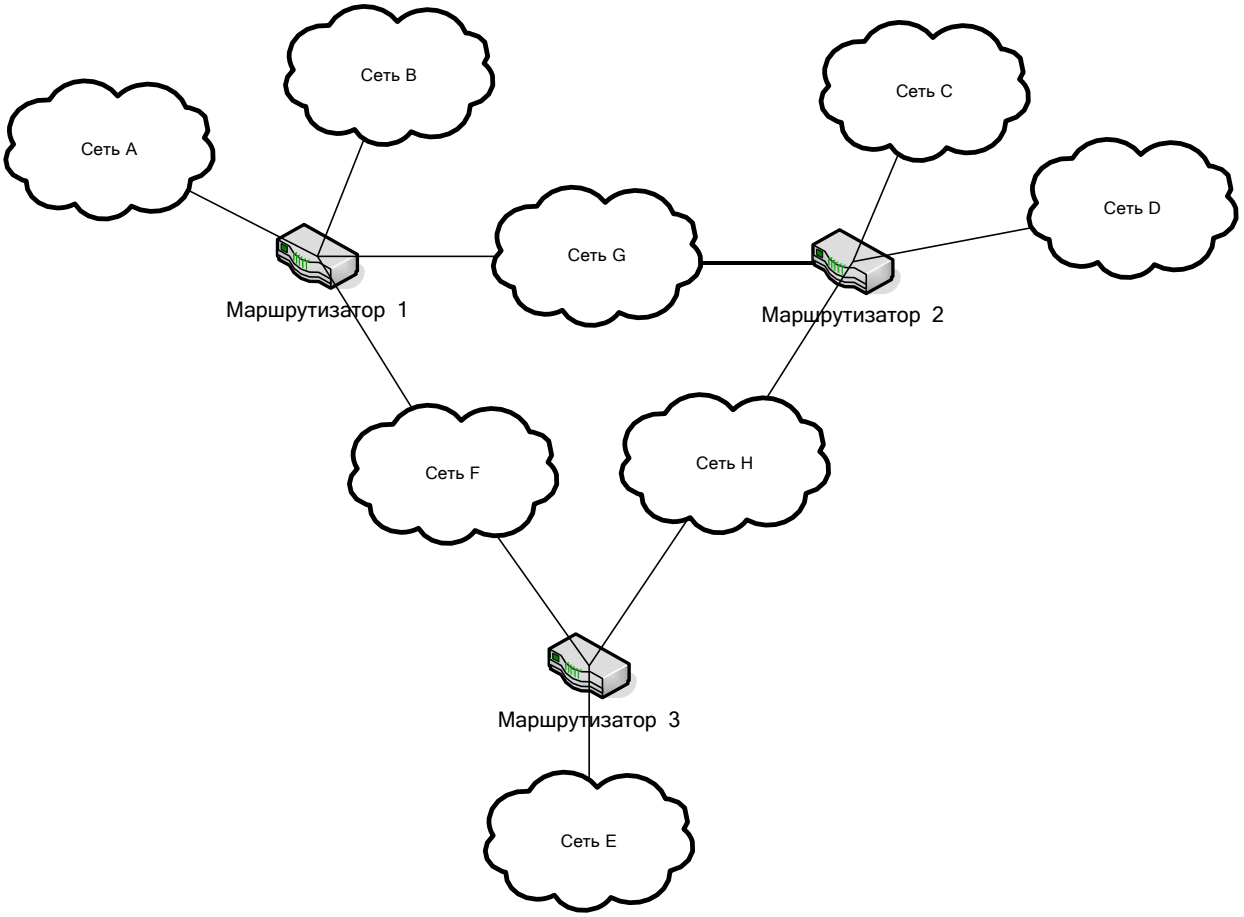
Вариант 19

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	220.18.46.0/24	220.18.46.35/24		
B	182.138.0.0/16	182.138.18.46/16		
C	193.18.48.0/24		193.18.48.35/24	
D	211.81.146.64/26		211.81.146.65/26	
E	206.35.48.64/26			206.35.48.66/26
F	221.35.48.0/28	221.35.48.1/28		221.35.48.2/28
G	223.48.121.192/28	223.48.121.193/28	223.48.121.194/28	
H	225.121.39.208/28		225.121.39.209/28	225.121.39.210/28



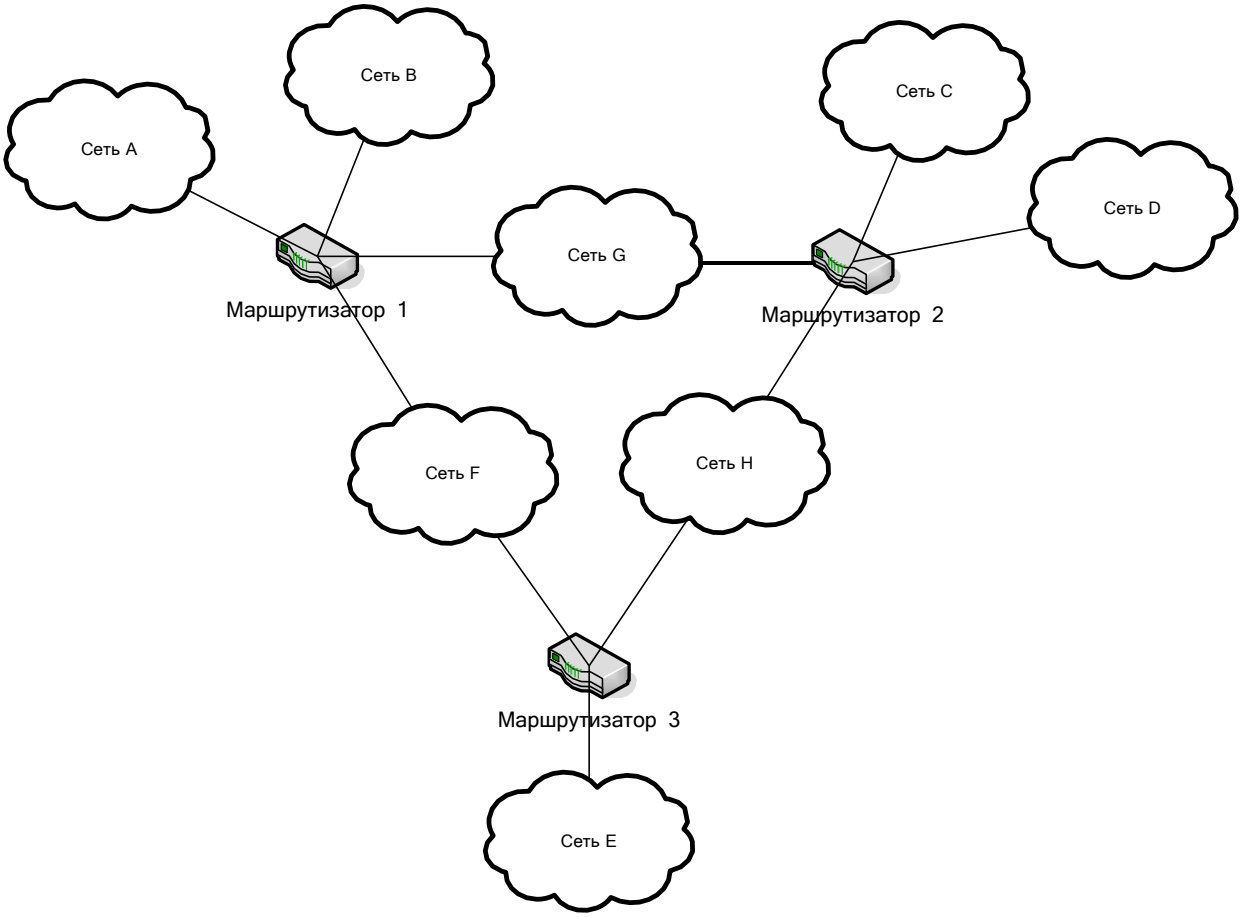
Вариант 20

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	118.115.0.0/16	118.115.21.18/16		
B	211.118.15.0/24	211.118.15.19/24		
C	193.18.48.0/24		193.18.48.35/24	
D	211.81.146.64/26		211.81.146.65/26	
E	218.56.136.128/26			218.56.136.132/26
F	201.116.18.64/28	201.116.18.65/28		201.116.18.66/28
G	222.11.13.0/29	222.11.13.1/29	222.11.13.2/29	
H	222.11.14.0/29		222.11.14.1/29	222.11.14.2/29



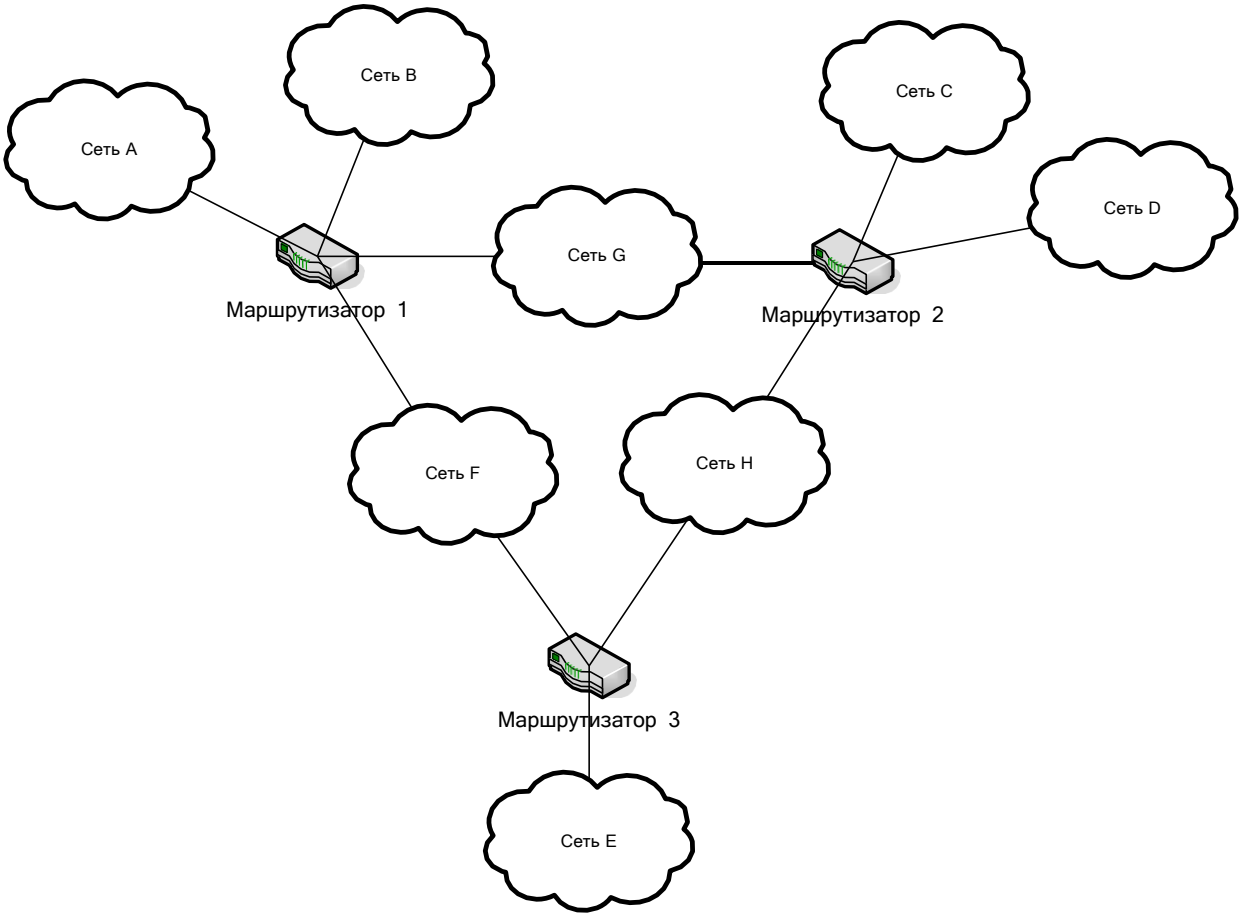
Вариант 1

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	218.75.13.0/26	218.75.13.6/26		
B	148.18.64.0/18	148.18.66.18/18		
C	137.52.0.0/16		137.52.7.215/16	
D	15.128.0.0/10		15.138.76.15/10	
E	216.218.148.32/27			216.218.148.33/27
F	211.152.13.48/28	211.152.13.49/28		211.152.13.50/28
G	211.167.208.64/28	211.167.208.65/28	211.167.208.66/28	
H	211.178.15.80/28		211.178.15.81/28	211.178.15.82/28



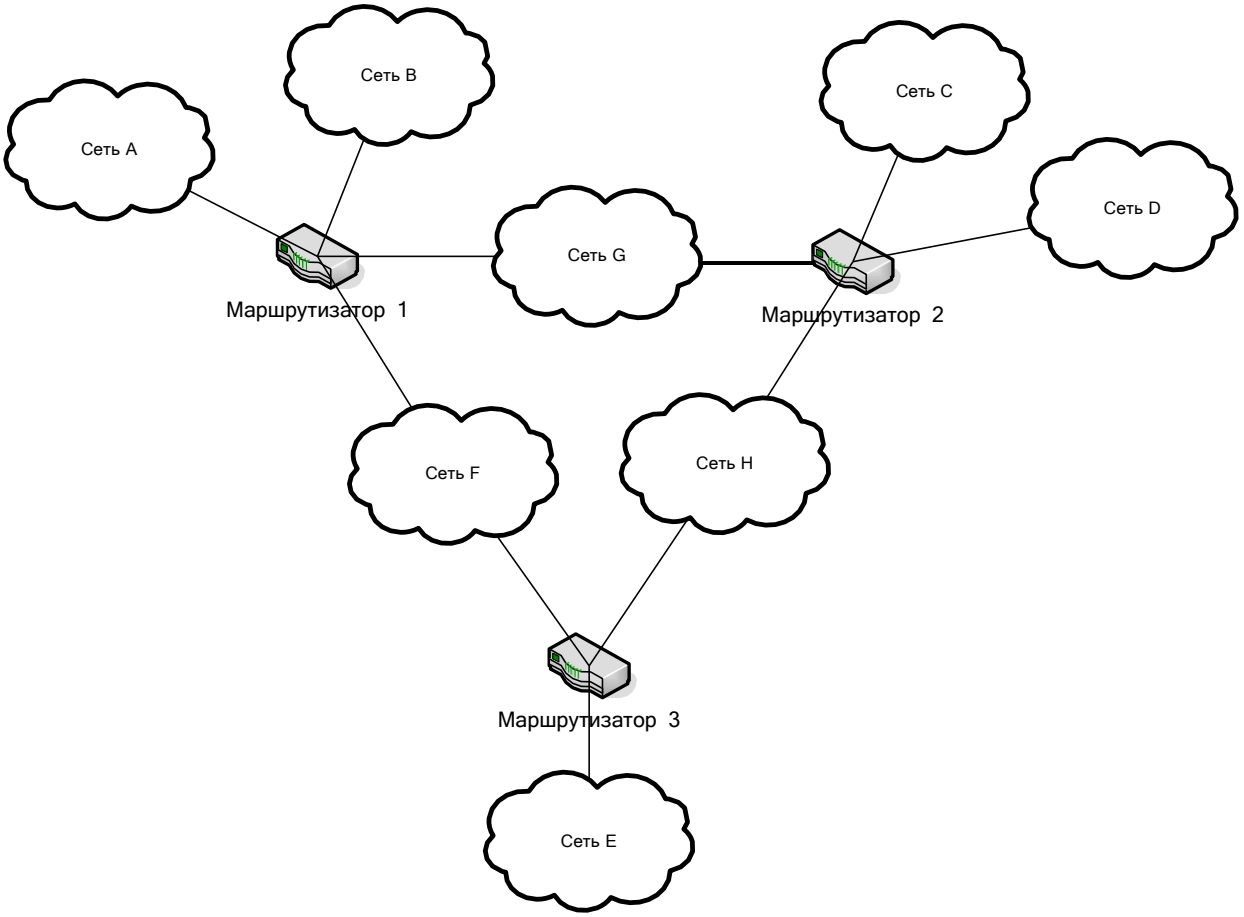
Вариант 2

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.18.64.0/18	148.18.66.123/18		
B	149.18.128.0/18	148.18.137.15/18		
C	218.75.13.64/26		218.75.13.75/26	
D	216.218.148.64/27		216.218.148.73/27	
E	13.0.0.0/8			13.1.1.1/8
F	179.18.64.0/20	179.18.65.1/20		179.18.65.2/20
G	213.157.240.96/28	213.157.240.97/28	213.157.240.98/28	
H	201.118.15.48/28		201.118.15.49/28	201.118.15.50/28



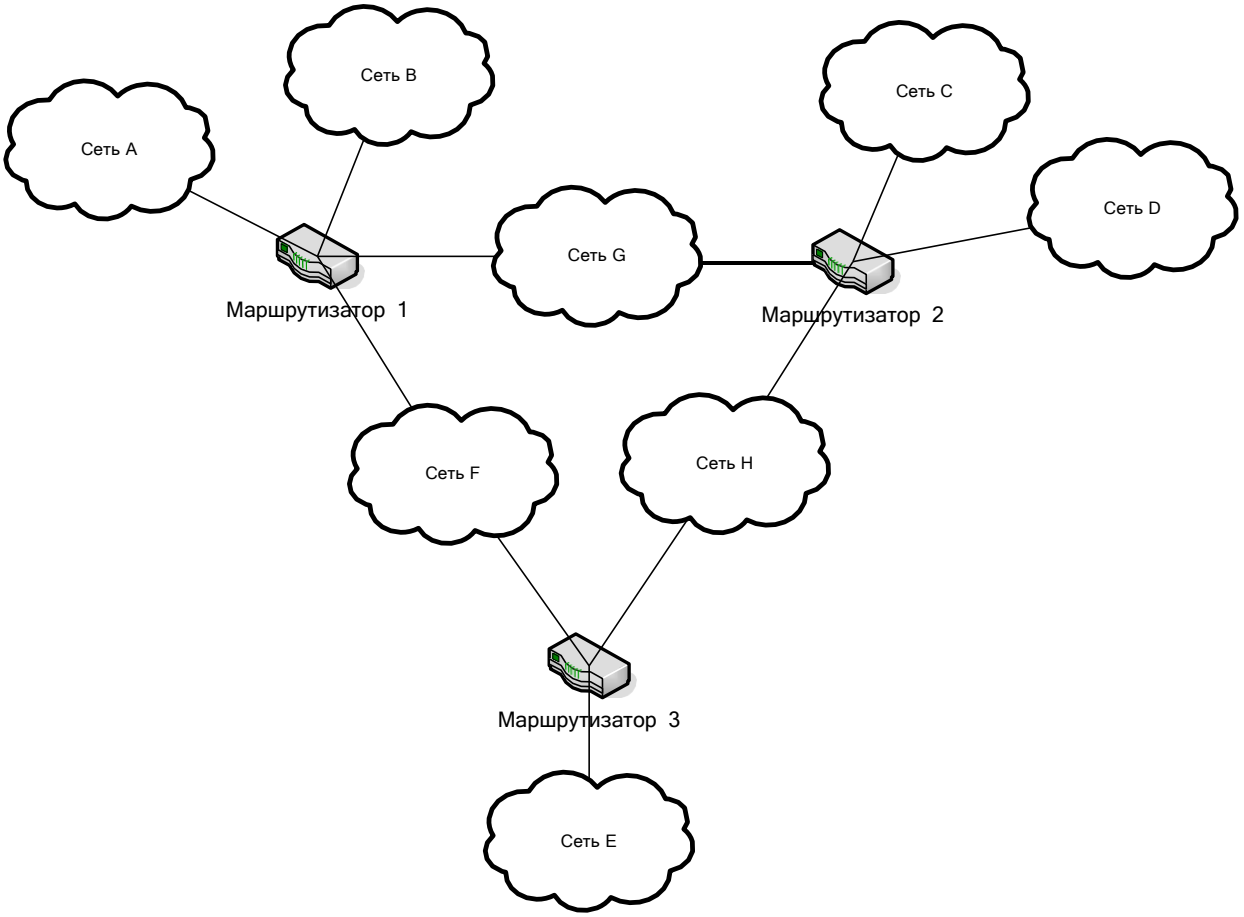
Вариант 3

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.18.0.0/16	148.18.75.18/16		
B	221.153.119.32/27	221.153.119.35/27		
C	15.128.0.0/10		15.138.76.15/10	
D	121.18.90.0/20		121.19.92.15/20	
E	216.218.131.32/27			216.218.131.33/27
F	211.182.17.48/28	211.182.17.49/28		211.182.17.50/28
G	217.157.213.64/28	217.157.213.65/28	217.157.213.66/28	
H	211.178.15.80/28		211.178.15.81/28	211.178.15.82/28



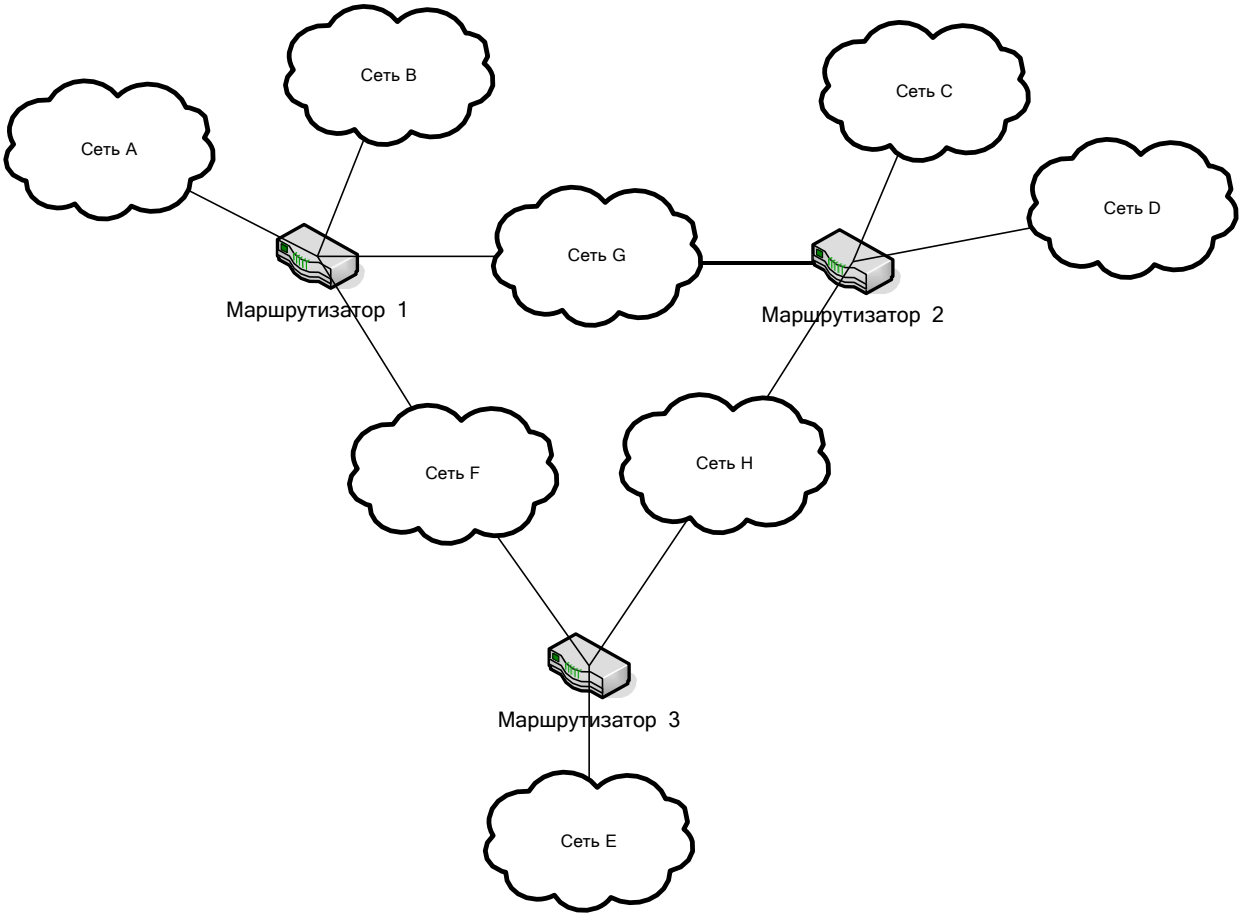
Вариант 4

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	153.15.166.0/24	153.15.166.15/24		
B	9.8.0.0/13	9.8.7.6/13		
C	137.128.64.0/18		137.128.67.99/18	
D	215.215.215.192/26		215.215.215.215/26	
E	18.0.0.0/8			18.18.18.18/8
F	200.200.111.128/28	200.200.111.131/28		200.200.111.132/28
G	222.1.0.0/28	222.1.0.13/28	222.1.0.14/28	
H	199.18.175.112/28		199.18.175.114/28	199.18.175.116/28



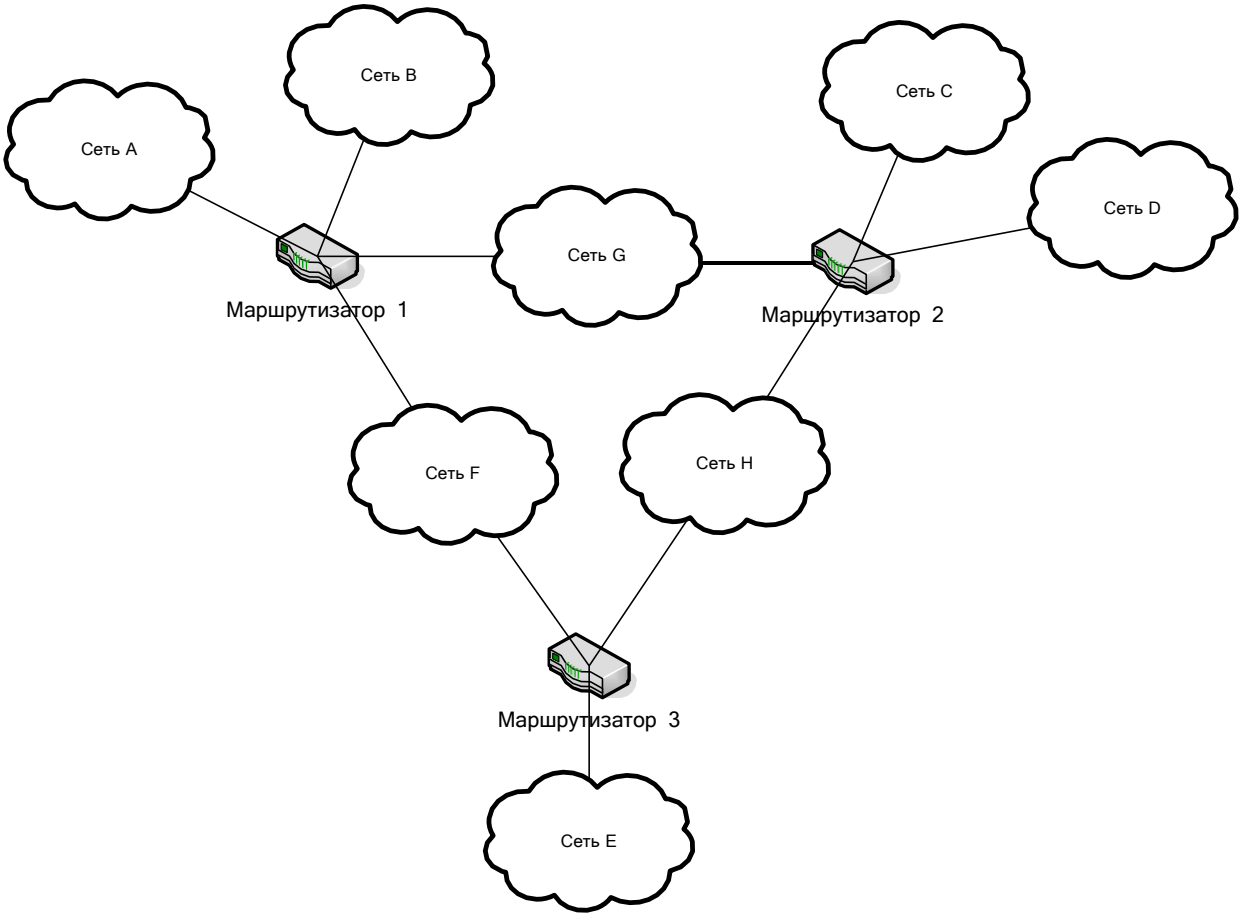
Вариант 5

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	18.80.0.0/12	18.82.35.244/12		
B	215.231.109.192/26	215.231.109.196/26		
C	9.8.0.0/13		9.8.251.250/13	
D	220.18.146.0/24		220.18.146.185/24	
E	35.118.0.0/16			35.118.100.100/16
F	213.13.113.0/26	213.13.113.15/26		213.13.113.16/26
G	218.1.148.144/28	218.1.148.145/28	218.1.148.146/28	
H	193.168.15.64/28		193.168.15.65/28	193.168.15.66/28



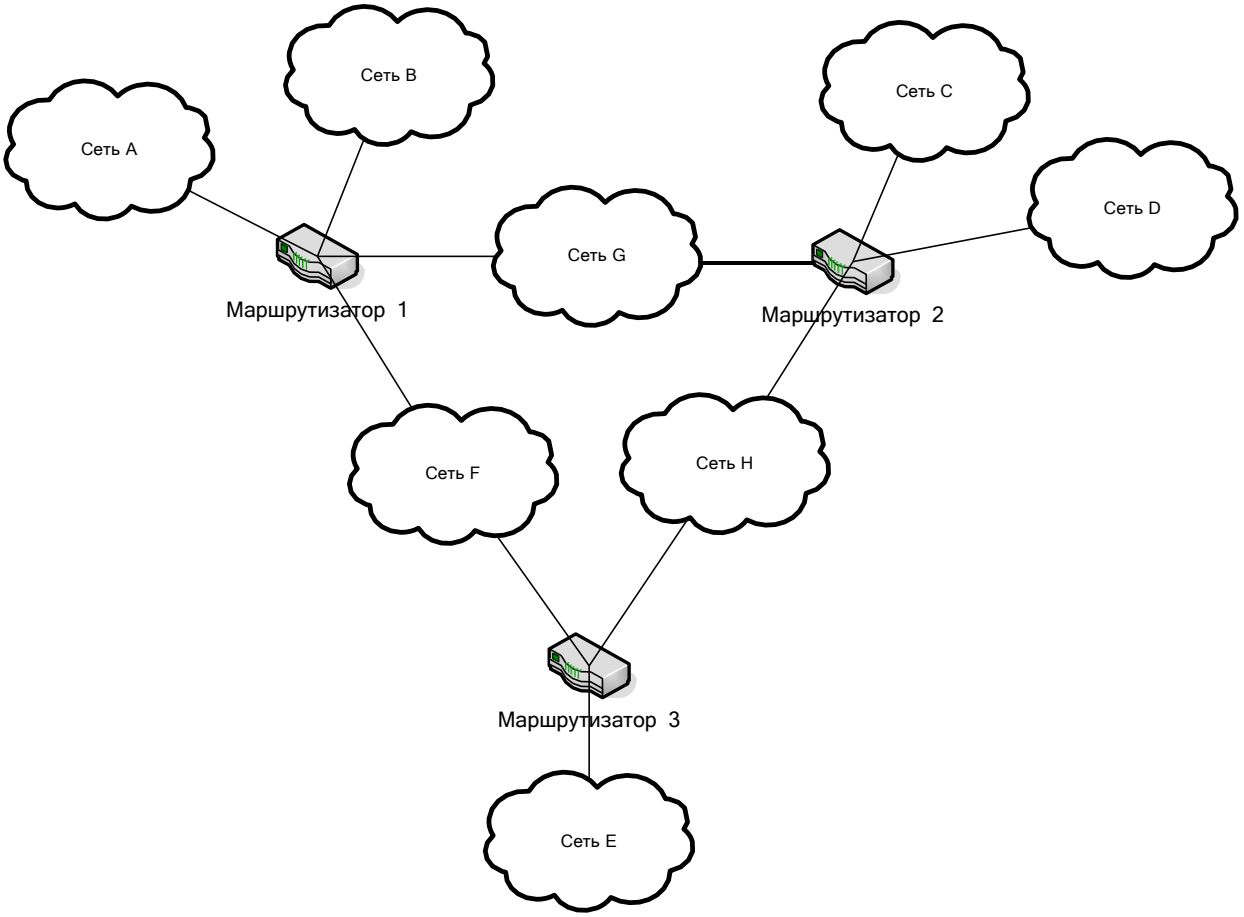
Вариант 6

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.17.128.0/17	148.17.138.115/17		
B	197.148.215.64/26	197.148.215.92/26		
C	137.128.64.0/18		137.128.67.99/18	
D	215.118.96.0/24		215.118.96.48/24	
E	187.26.56.0/23			187.26.57.211/23
F	199.18.175.112/28	199.18.175.114/28		199.18.175.116/28
G	193.168.15.64/28	193.168.15.65/28	193.168.15.66/28	
H	218.1.152.144/28		218.1.152.145/28	218.1.152.146/28



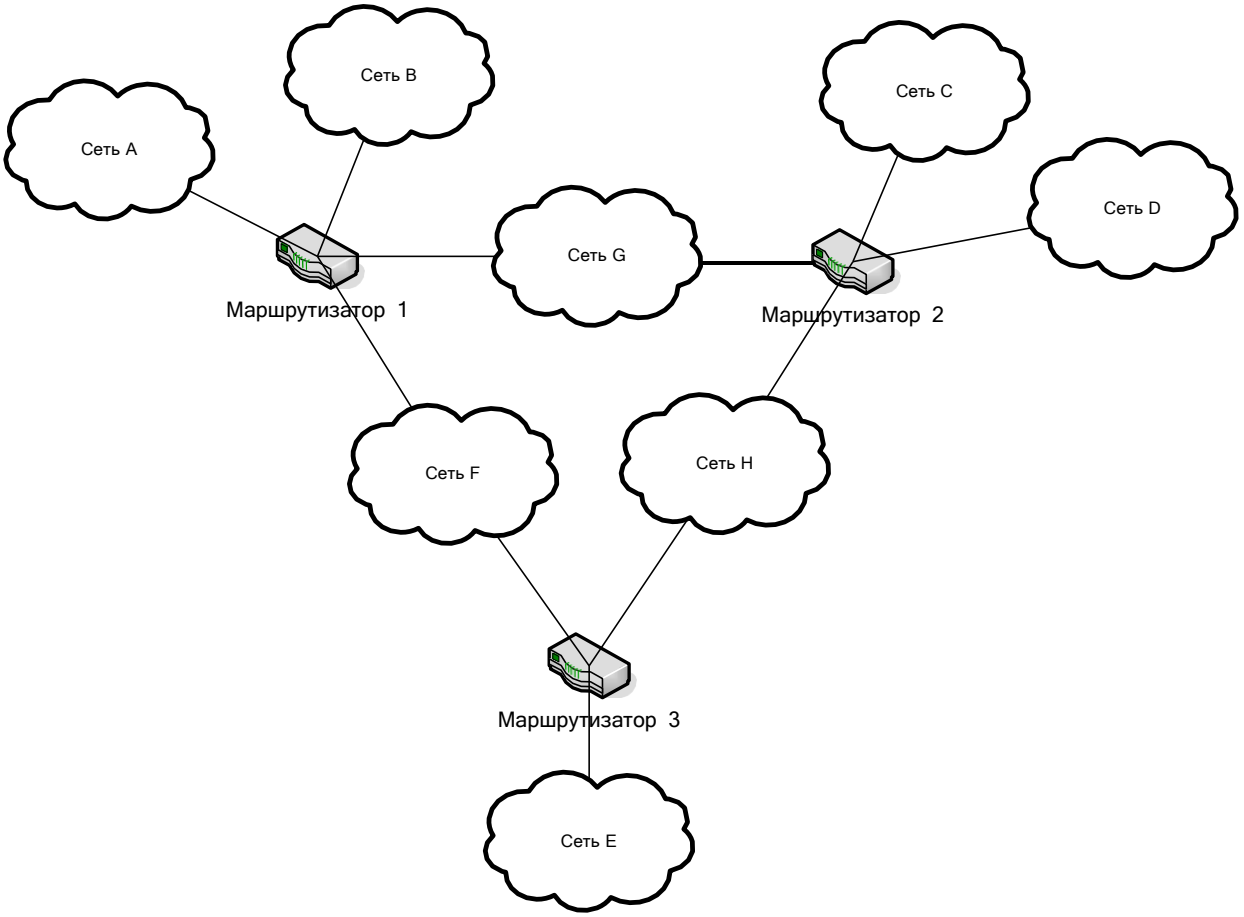
Вариант 7

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	118.115.0.0/16	118.115.21.18/16		
B	211.118.15.0/24	211.118.15.19/24		
C	97.128.0.0/9		97.128.18.235/9	
D	196.44.36.0/24		196.44.36.36/24	
E	218.56.136.128/26			218.56.136.132/26
F	201.116.18.64/28	201.116.18.65/28		201.116.18.66/28
G	203.86.35.80/28	203.86.35.81/28	203.86.35.82/28	
H	197.221.56.128/28		197.221.56.129/28	197.221.56.130/28



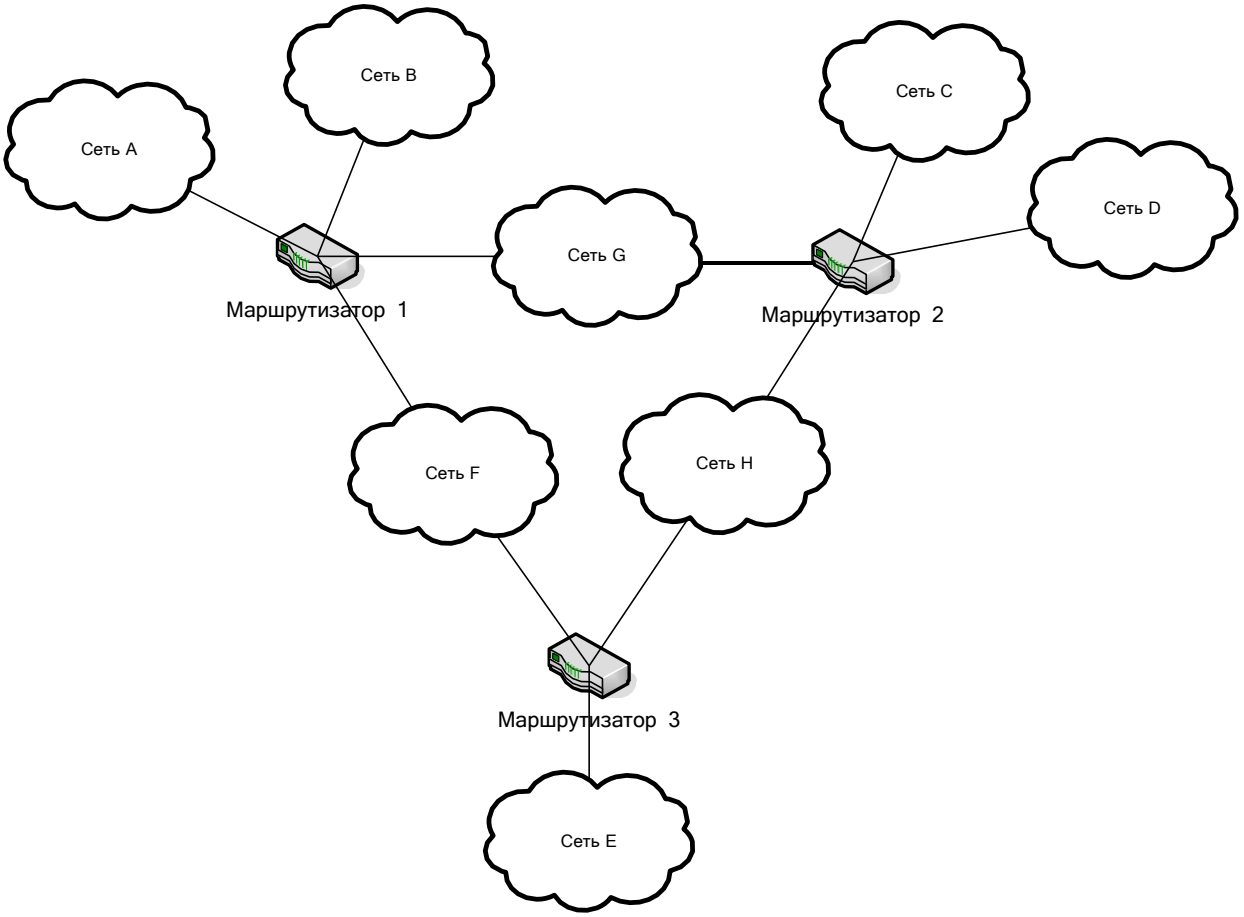
Вариант 8

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	220.18.46.0/24	220.18.46.35/24		
B	182.138.0.0/16	182.138.18.46/16		
C	204.39.183.128/25		204.39.183.196/25	
D	205.46.38.0/24		205.46.38.118/24	
E	47.128.0.0/10			47.128.35.153/10
F	222.11.12.0/29	222.11.12.1/29		222.11.12.2/29
G	222.11.13.0/29	222.11.13.1/29	222.11.13.2/29	
H	222.11.14.0/29		222.11.14.1/29	222.11.14.2/29



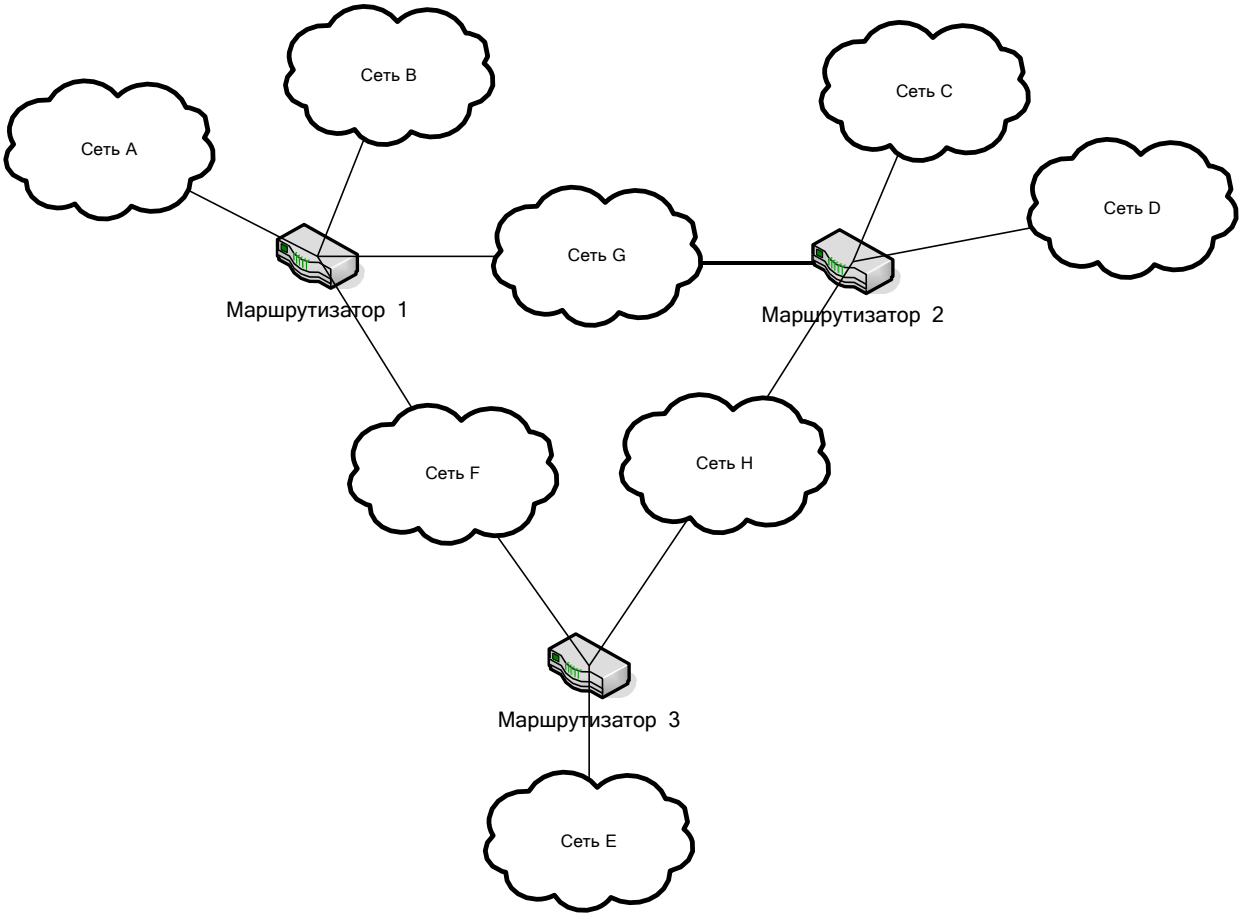
Вариант 9

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	15.0.0.0/8	15.35.46.38/8		
B	207.11.181.0/16	207.11.181.12/16		
C	212.48.56.0/24		212.48.56.38/24	
D	183.21.0.0/16		183.21.46.182/16	
E	206.35.48.64/26			206.35.48.66/26
F	221.35.48.0/28	221.35.48.1/28		221.35.48.2/28
G	223.48.121.192/28	223.48.121.193/28	223.48.121.194/28	
H	225.121.39.208/28		225.121.39.209/28	225.121.39.210/28



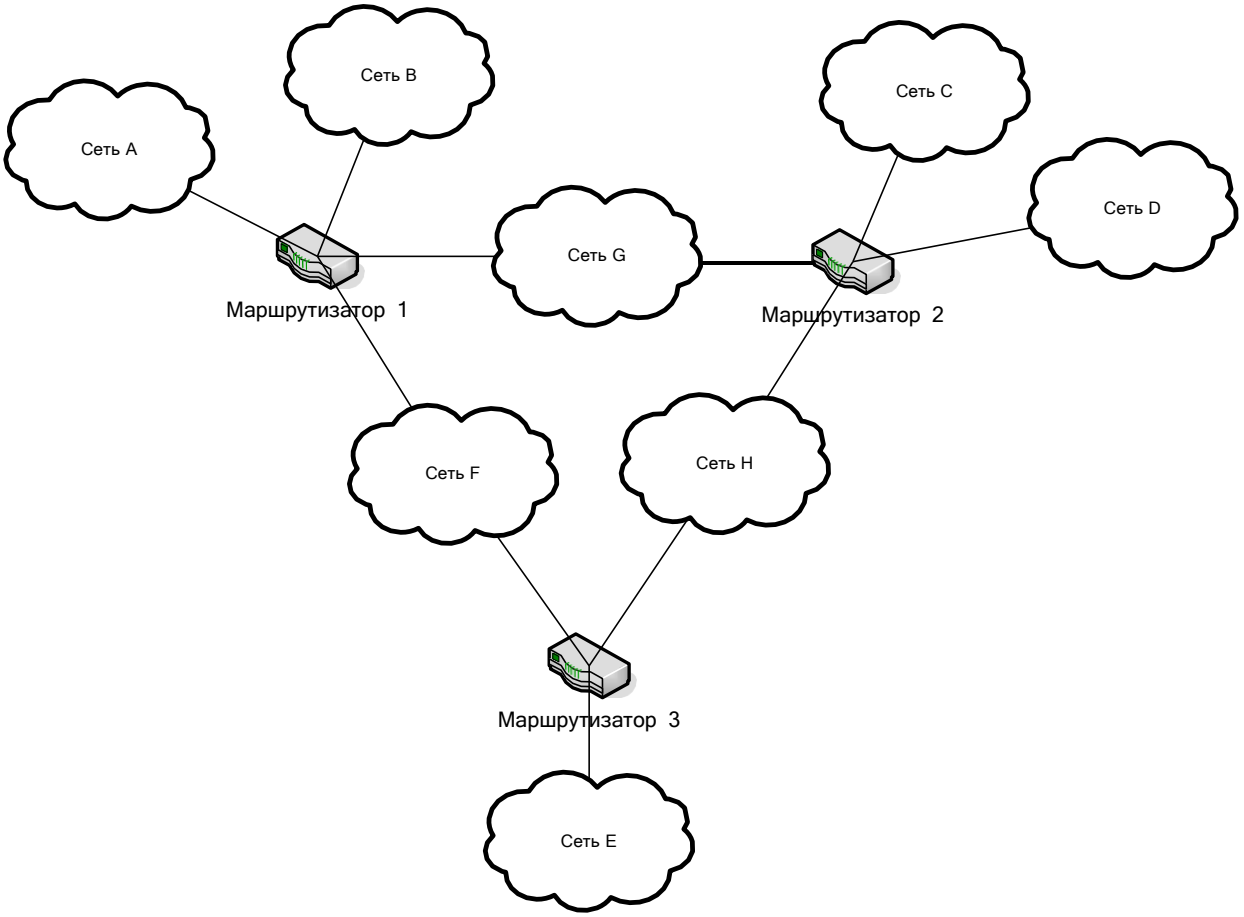
Вариант 10

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	13.0.0.0/8	13.13.13.13/8		
B	146.92.0.0/16	146.92.35.78/16		
C	193.18.48.0/24		193.18.48.35/24	
D	211.81.146.64/26		211.81.146.65/26	
E	211.149.37.0/24			211.149.37.245/24
F	197.1.1.0/28	197.1.1.1/28		197.1.1.11/28
G	197.1.2.0/28	197.1.2.3/28	197.1.2.4/28	
H	197.1.3.0/28		197.1.3.4/28	197.1.3.6/28



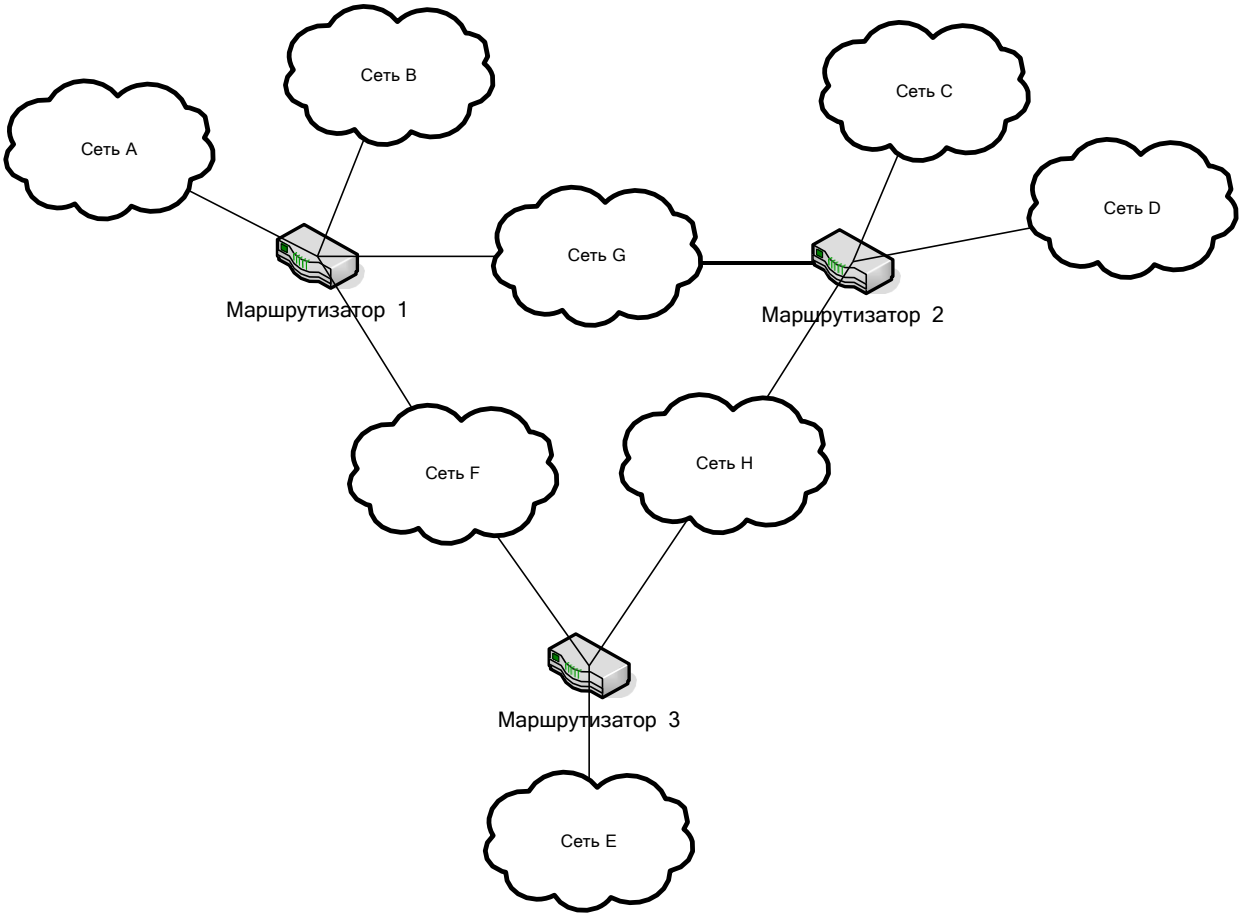
Вариант 11

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.17.128.0/17	148.17.138.115/17		
B	197.148.215.64/26	197.148.215.92/26		
C	137.128.64.0/18		137.128.67.99/18	
D	220.18.146.0/24		220.18.146.185/24	
E	35.118.0.0/16			35.118.100.100/16
F	200.200.111.128/28	200.200.111.131/28		200.200.111.132/28
G	222.1.0.0/28	222.1.0.13/28	222.1.0.14/28	
H	199.18.175.112/28		199.18.175.114/28	199.18.175.116/28



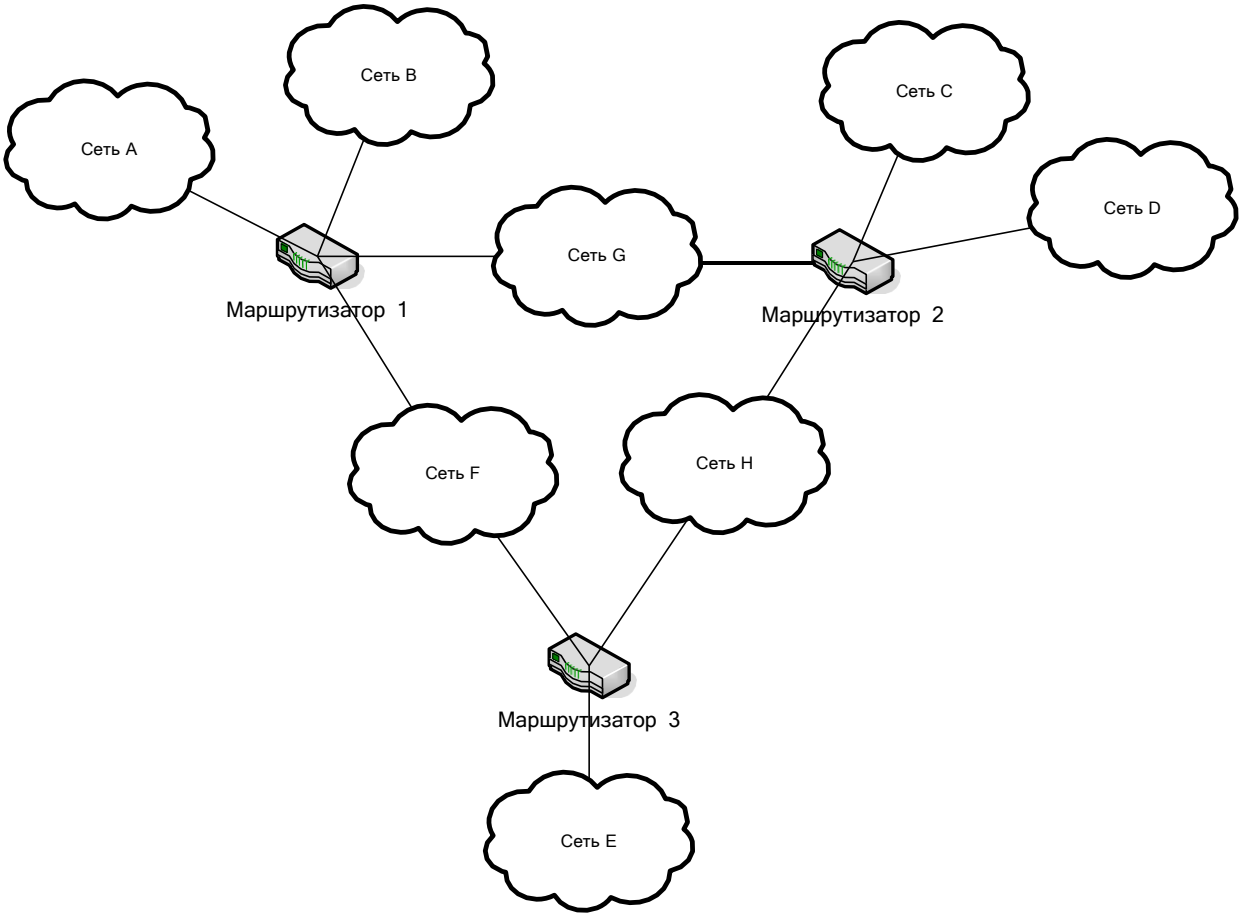
Вариант 12

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	18.80.0.0/12	18.82.35.244/12		
B	215.231.109.192/26	215.231.109.196/26		
C	9.8.0.0/13		9.8.251.250/13	
D	215.118.96.0/24		215.118.96.48/24	
E	187.26.56.0/23			187.26.57.211/23
F	199.18.175.112/28	199.18.175.114/28		199.18.175.116/28
G	217.157.213.64/28	217.157.213.65/28	217.157.213.66/28	
H	211.178.15.80/28		211.178.15.81/28	211.178.15.82/28



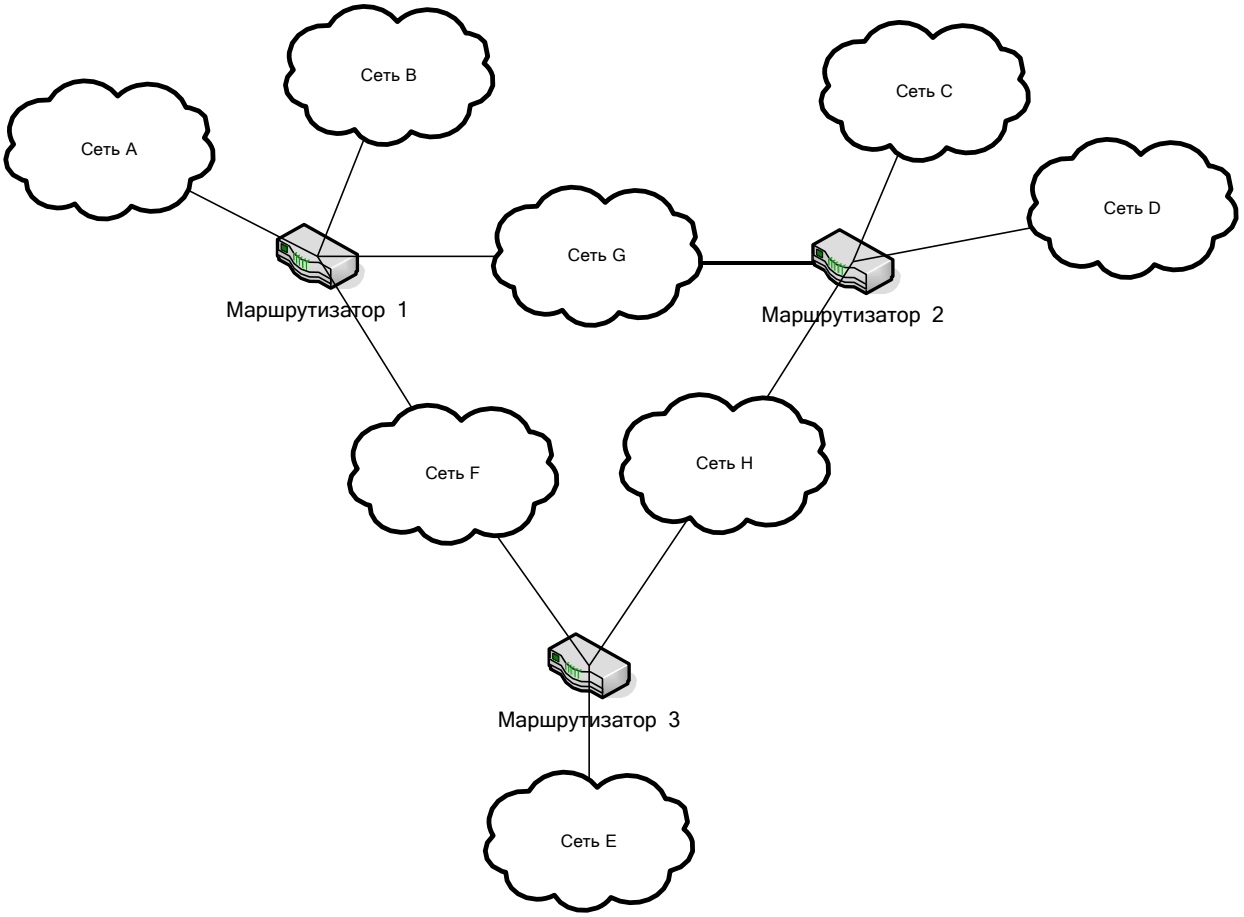
Вариант 13

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	153.15.166.0/24	153.15.166.15/24		
B	9.8.0.0/13	9.8.7.6/13		
C	137.128.64.0/18		137.128.67.99/18	
D	215.215.215.192/26		215.215.215.215/26	
E	18.0.0.0/8			18.18.18.18/8
F	213.13.113.0/26	213.13.113.15/26		213.13.113.16/26
G	193.168.15.64/28	193.168.15.65/28	193.168.15.66/28	
H	218.1.152.144/28		218.1.152.145/28	218.1.152.146/28



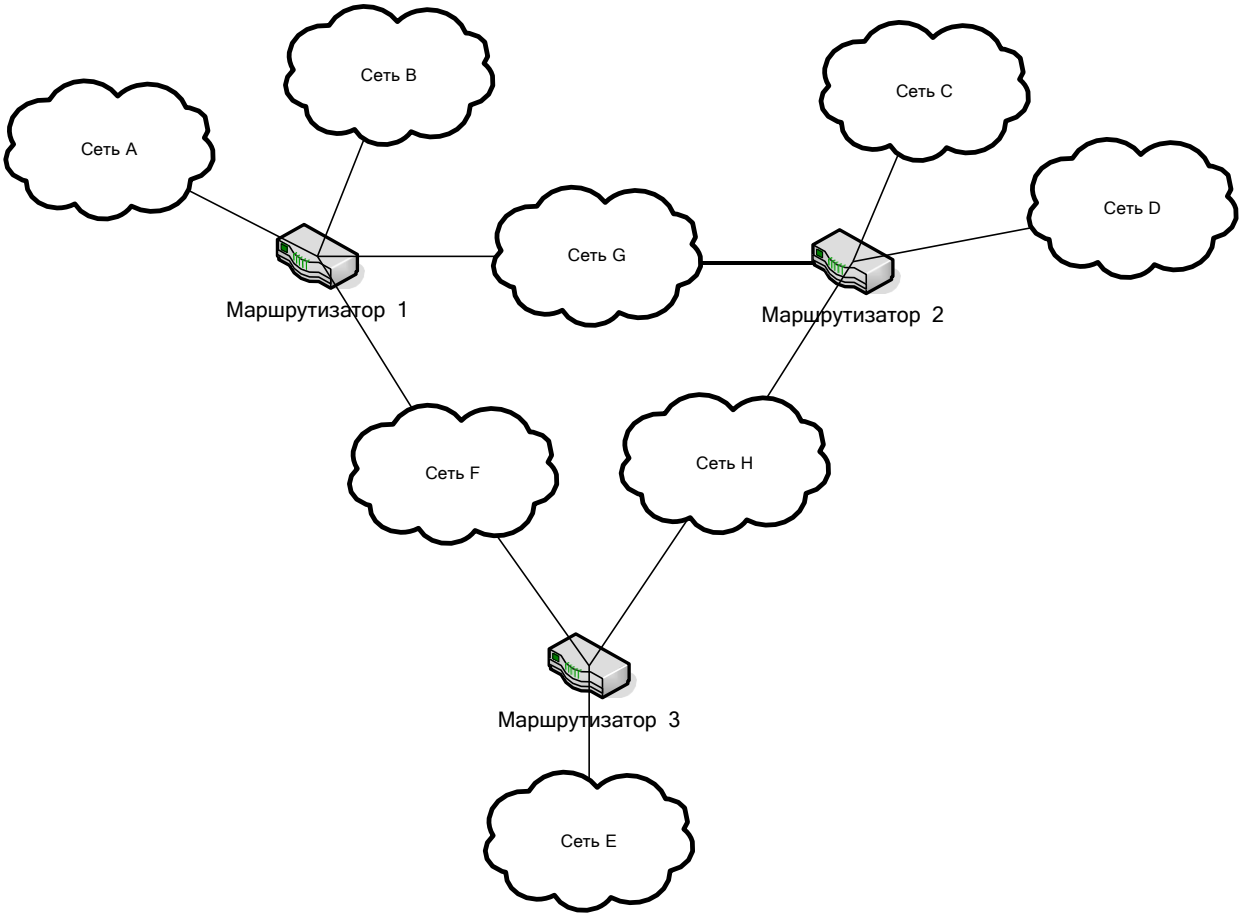
Вариант 14

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	148.18.0.0/16	148.18.75.18/16		
B	221.153.119.32/27	221.153.119.35/27		
C	137.52.0.0/16		137.52.7.215/16	
D	15.128.0.0/10		15.138.76.15/10	
E	216.218.148.32/27			216.218.148.33/27
F	213.13.113.0/26	213.13.113.15/26		213.13.113.16/26
G	218.1.148.144/28	218.1.148.145/28	218.1.148.146/28	
H	193.168.15.64/28		193.168.15.65/28	193.168.15.66/28



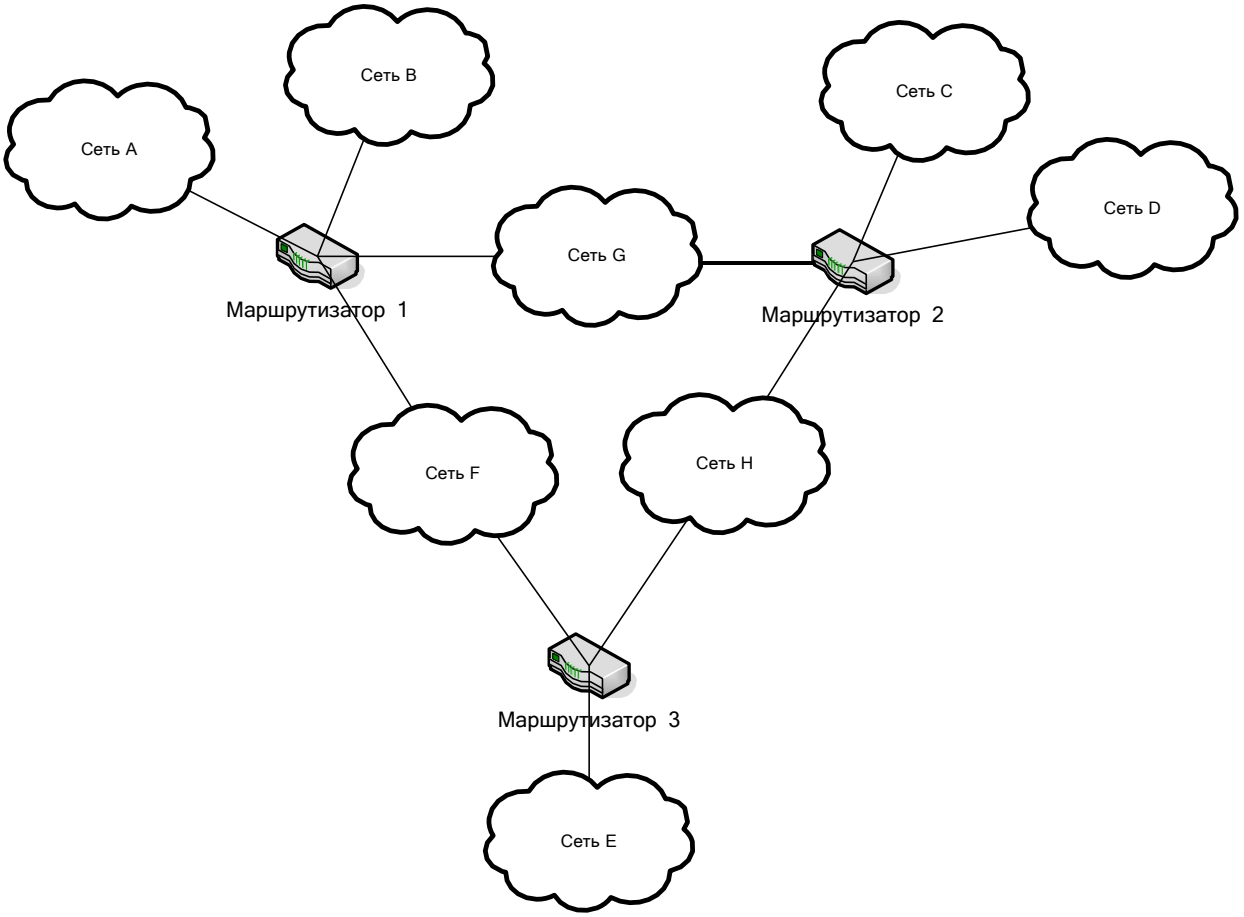
Вариант 15

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	218.75.13.0/26	218.75.13.6/26		
B	148.18.64.0/18	148.18.66.18/18		
C	15.128.0.0/10		15.138.76.15/10	
D	121.18.90.0/20		121.19.92.15/20	
E	216.218.131.32/27			216.218.131.33/27
F	200.200.111.128/28	200.200.111.131/28		200.200.111.132/28
G	211.167.208.64/28	211.167.208.65/28	211.167.208.66/28	
H	211.178.15.80/28		211.178.15.81/28	211.178.15.82/28



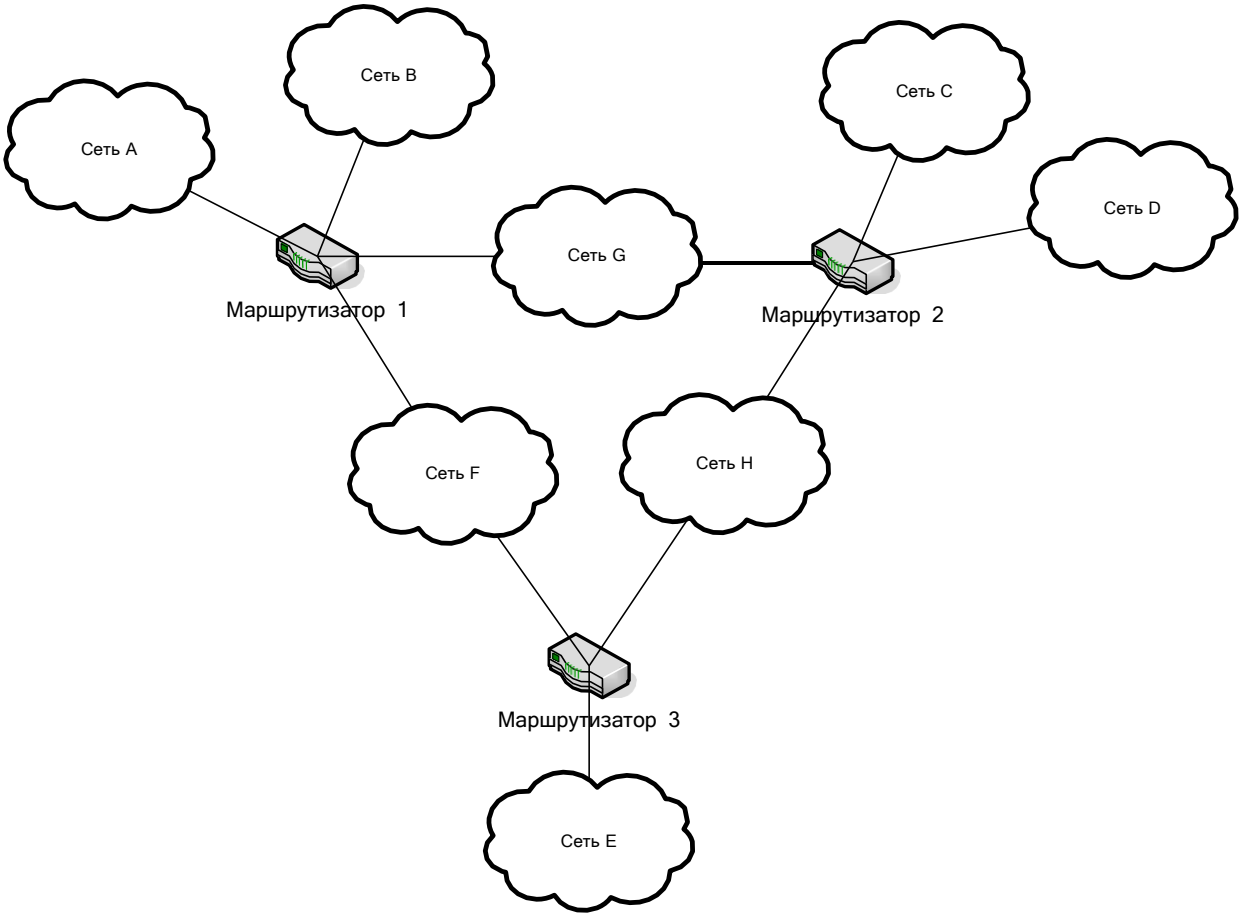
Вариант 16

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	220.18.46.0/24	220.18.46.35/24		
B	182.138.0.0/16	182.138.18.46/16		
C	212.48.56.0/24		212.48.56.38/24	
D	183.21.0.0/16		183.21.46.182/16	
E	211.149.37.0/24			211.149.37.245/24
F	197.1.1.0/28	197.1.1.1/28		197.1.1.11/28
G	197.1.2.0/28	197.1.2.3/28	197.1.2.4/28	
H	197.1.3.0/28		197.1.3.4/28	197.1.3.6/28



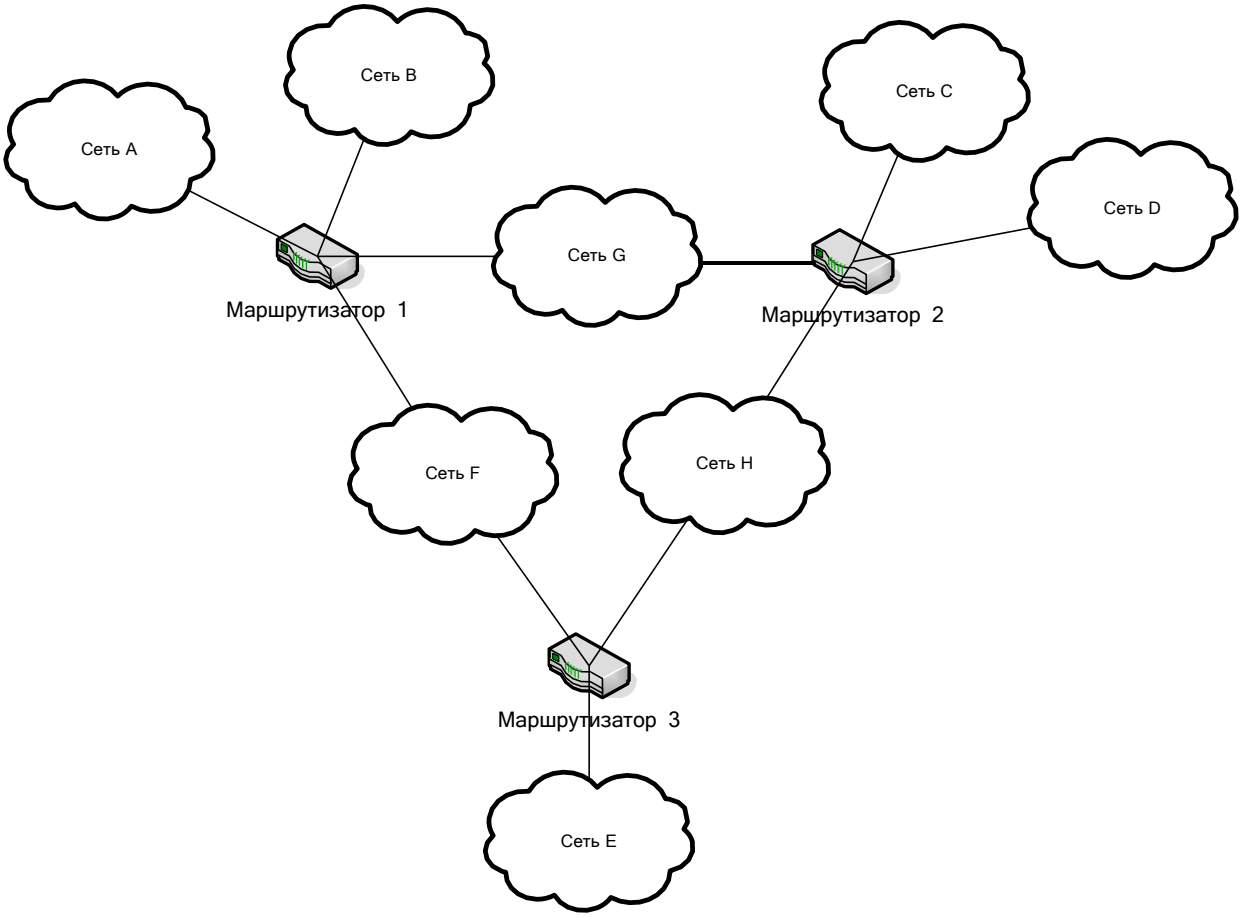
Вариант 17

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	15.0.0.0/8	15.35.46.38/8		
B	207.11.181.0/16	207.11.181.12/16		
C	204.39.183.128/25		204.39.183.196/25	
D	205.46.38.0/24		205.46.38.118/24	
E	211.149.37.0/24			211.149.37.245/24
F	197.1.1.0/28	197.1.1.1/28		197.1.1.11/28
G	197.1.2.0/28	197.1.2.3/28	197.1.2.4/28	
H	197.1.3.0/28		197.1.3.4/28	197.1.3.6/28



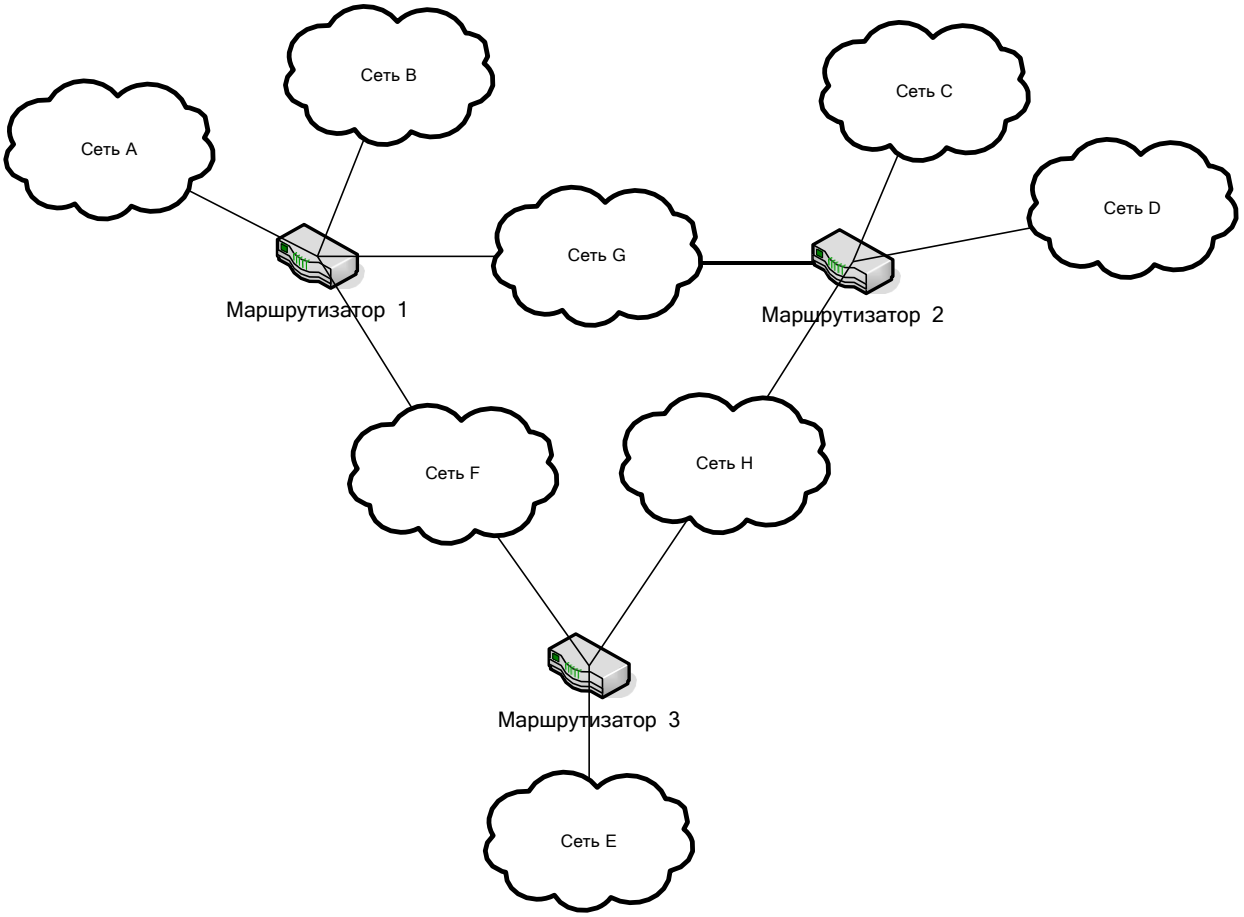
Вариант 18

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	13.0.0.0/8	13.13.13.13/8		
B	146.92.0.0/16	146.92.35.78/16		
C	193.18.48.0/24		193.18.48.35/24	
D	211.81.146.64/26		211.81.146.65/26	
E	47.128.0.0/10			47.128.35.153/10
F	222.11.12.0/29	222.11.12.1/29		222.11.12.2/29
G	222.11.13.0/29	222.11.13.1/29	222.11.13.2/29	
H	222.11.14.0/29		222.11.14.1/29	222.11.14.2/29



Вариант 19

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	220.18.46.0/24	220.18.46.35/24		
B	182.138.0.0/16	182.138.18.46/16		
C	193.18.48.0/24		193.18.48.35/24	
D	211.81.146.64/26		211.81.146.65/26	
E	206.35.48.64/26			206.35.48.66/26
F	221.35.48.0/28	221.35.48.1/28		221.35.48.2/28
G	223.48.121.192/28	223.48.121.193/28	223.48.121.194/28	
H	225.121.39.208/28		225.121.39.209/28	225.121.39.210/28



Вариант 20

Сеть	Адрес сети	Адрес маршрутизатора в сети		
		Маршрутизатор 1	Маршрутизатор 2	Маршрутизатор 3
A	118.115.0.0/16	118.115.21.18/16		
B	211.118.15.0/24	211.118.15.19/24		
C	193.18.48.0/24		193.18.48.35/24	
D	211.81.146.64/26		211.81.146.65/26	
E	218.56.136.128/26			218.56.136.132/26
F	201.116.18.64/28	201.116.18.65/28		201.116.18.66/28
G	222.11.13.0/29	222.11.13.1/29	222.11.13.2/29	
H	222.11.14.0/29		222.11.14.1/29	222.11.14.2/29

Ключи к ФОС по дисциплине «Компьютерные сети»

5.1 Ответы на вопросы для собеседования (устного опроса):

Тема 1.1 Компьютерные сети

1.1 Интернет — это компьютерная сеть, которая связывает между собой сотни миллионов вычислительных устройств по всему миру. Конечные системы соединяются вместе с помощью линий связи и коммутаторов пакетов. Коммутаторы поставляются в разных формах и разновидностях, но двумя наиболее известными типами в современном Интернете являются маршрутизаторы и коммутаторы канального уровня. Коммутаторы обоих типов направляют пакеты в их конечные пункты назначения. Коммутаторы канального уровня обычно применяются в сетях доступа, тогда как маршрутизаторы обычно используются в ядре сети. Последовательность линий связи и коммутаторов пакетов, через которые проходит пакет из отправляющей конечной системы в принимающую, называется маршрутом или путем в сети.

1.2 Интернет – это инфраструктура, которая предоставляет службы для приложений. Эти приложения включают электронную почту, веб-серфинг, социальные сети, обмен мгновенными сообщениями, передача речи по IP-протоколу(VoIP), потоковое видео, сетевые игры, одноранговый совместный доступ к файлам, телевидение через Интернет (IP TV), удаленный доступ и многое-многое другое. Все они считаются распределенными приложениями, поскольку вовлекают в работу множество конечных систем, которые обмениваются данными друг с другом. Важно, что Интернет-приложения выполняются на конечных системах, а не на коммутаторах пакетов в ядре сети. Хотя коммутаторы пакетов обеспечивают обмен данными между конечными системами, они не имеют отношения к конкретным приложениям, являющимся источниками или получателями данных.

1.3 В связи со значимостью протоколов для Интернета важно, чтобы все договорились о том, что делает каждый протокол, тогда пользователи могут создавать взаимодействующие системы и изделия. Вот где вступают в действие стандарты. Интернет-стандарты разрабатываются инженерным советом Интернета (IETF, Internet Engineering Task Force). Документы стандартов IETF называются запросами на отзывы, или рабочими предложениями (request for comments, RFC). Документы RFC появились в виде общих предложений к обсуждению (отсюда их название) для решения проблем, с которыми сталкивался при разработке сетей и протоколов предшественник Интернета. Документы RFC отличаются технической направленностью и подробностью изложения. В них определяются протоколы, такие как TCP, IP, HTTP (для Всемирной паутины) и SMTP (для электронной почты). В настоящее время существует более 9000 документов RFC.

1.4 Протокол определяет формат и порядок сообщений, которыми обмениваются два или более взаимодействующих объектов, а также действия, предпринимаемые при передаче и/или приеме сообщения либо при возникновении другого события.

1.5 Классификация компьютерных сетей, как любых больших и сложных систем, может быть выполнена на основе различных признаков, в качестве которых могут быть использованы, как показано на рисунке 1:

- размер (территориальный охват) сети;
- принадлежность;
- назначение;
- область применения.

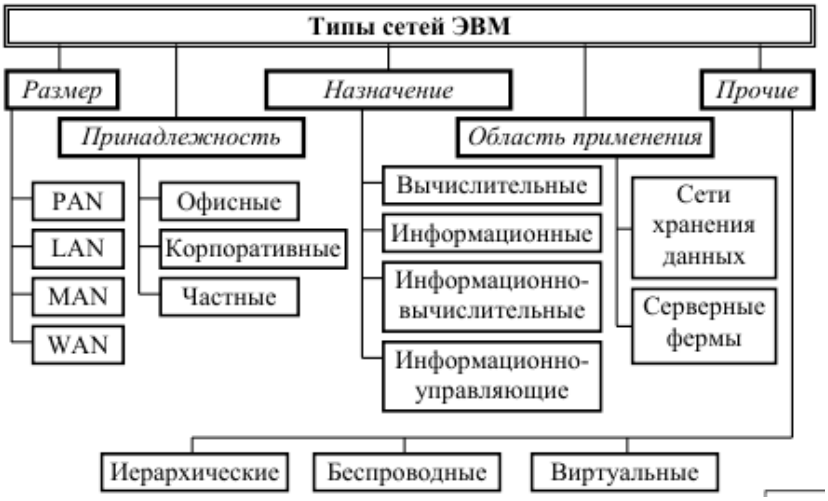


Рисунок 1– Классификация компьютерных сетей

1.6 В LAN – каналы связи принадлежат собственнику сети, в WAN – провайдеру (оператору связи).

1.7 Модели сетевого взаимодействия:

- централизованной обработки информации;
- «клиент-сервер»;
- распределенной обработки информации;
- совместной обработки информации;
- «клиент-сеть»

1.8 Промежуточные устройства соединяют отдельные оконечные устройства с сетью и могут соединять несколько отдельных сетей для создания объединенной сети. Такие устройства обеспечивают подключение и прохождение потоков данных по сети. Это повторители, концентраторы, коммутаторы, маршрутизаторы.

1.9 Технологии интернет-подключения для дома и небольшого офиса:

- Кабельное подключение
- DSL
- Сотовая связь
- Спутниковая связь
- Телефонный коммутируемый доступ

1.10 Технологии интернет-подключения для предприятий:

- Выделенная арендованная линия

- Глобальная сеть Ethernet
- DSL
- Спутниковая связь

1.11 Сегодня разрозненные сети данных, телефонные и видео сети объединяются. В отличие от выделенных сетей конвергентные сети позволяют передавать данные, голос и видео между различными типами устройств при использовании одной и той же сетевой инфраструктуры. Сетевая инфраструктура использует одни и те же правила, соглашения и стандарты реализации.

1.12 Основными показателями качества сети являются:

- полнота выполняемых функций;
- производительность (среднее количество запросов пользователей сети, исполняемых в единицу времени);
- пропускная способность (количество данных, переданных через сеть за единицу времени);
- надежность сети (способность сети выполнять заданные функции в течение заданного времени с заданными параметрами);
- достоверность информации;
- безопасность информации в сети (способность сети обеспечить защиту информации от несанкционированного доступа);
- прозрачность сети (невидимость особенностей внутренней архитектуры сети для пользователя);
- масштабируемость (возможность расширения сети без заметного снижения ее производительности);
- универсальность сети (возможность подключения к сети разнообразного технического оборудования и программного обеспечения от разных производителей).

1.13 Расширение – увеличение диаметра сети, количества подключенных устройств, пользователей и приложений за счет снижения показателей качества; - масштабирование – то же самое без ухудшения показателей качества.

1.14 Качество обслуживания (QoS) сегодня является одним из постоянно растущих требований к сети. Новые веб-приложения, например, передача голоса и видео в режиме реального времени, задают более высокие требования к качеству предоставляемых услуг. Приходилось ли вам когда-нибудь смотреть видео с постоянными разрывами и паузами? За счет объединения функций передачи данных, голоса и видео в одной сети QoS становится основным механизмом предотвращения перегрузок сети и надежной доставки контента всем пользователям.

1.15 Три основных требования для достижения безопасности сети:

- Конфиденциальность — только указанные и авторизованные получатели могут иметь доступ к данным.
- Целостность — гарантия того, что информация не была изменена в процессе передачи от исходного пункта к месту назначения.
- Доступность — своевременный и надежный доступ к данным для авторизованных пользователей.

1.16 Этапы развития компьютерных сетей и Интернета

1 Развитие коммутации пакетов: 1961 – 1972

2 Развитие частных сетей и Интернета: 1972-1980
3 Рост компьютерных сетей: 1980-1990
4 Интернет-взрыв: 1990-е
5 Новое тысячелетие
6 Развитие мобильных технологий – 2000-е

Тема 1.2 Сетевые протоколы и коммуникации

1.17 Коммуникации начинаются с сообщения (информации), которое нужно передать от источника к получателю. Отправка этого сообщения посредством индивидуального общения или по сети регулируется правилами, которые называются протоколами. Эти протоколы соответствуют способу коммуникации. Протоколы отвечают следующим требованиям:

- Известные отправитель и получатель
- Общепринятые язык и грамматика
- Скорость и время доставки
- Требования к утверждению или подтверждению

1.18 Кроме того, компьютерные протоколы должны соответствовать следующим единым требованиям:

- кодирование сообщений;
- форматирование и инкапсуляция сообщений;
- размер сообщений;
- синхронизация сообщений;
- варианты доставки сообщений.

1.19 При отправке сообщения от источника к адресату необходимо использовать определенный формат или структуру. Формат зависит от типа сообщения и канала доставки. Кроме того, большинство сообщений нужно не только составить в правильном формате, но и поместить в другое сообщение для доставки. Процесс размещения одного формата сообщения (письмо) внутри другого (конверт) называется инкапсуляцией. Деинкапсуляция происходит в тот момент, когда получатель достает письмо из конверта.

1.20 Набор основных протоколов стека TCP/IP приведен на рисунке 2.

Рисунок 2 – Набор протоколов стека TCP/IP

1.21 Будьте готовы кратко охарактеризовать любой протокол из стека TCP/IP.

Система (или служба) доменных имен (Domain Name System или Service, DNS) – преобразует имена доменов, например, Cisco.com в IP-адреса.

Протокол загрузки (Bootstrap Protocol, BOOTP):

- Позволяет бездисковым рабочим станциям узнавать свой IP-адрес, IP-адреса BOOT-сервера в сети, а также загружать файл в память для запуска компьютера.
- BOOTP был вытеснен протоколом DHCP.

Протокол динамической конфигурации сетевого узла (Dynamic Host Configuration Protocol, DHCP):

- Динамически присваивает IP-адреса клиентским станциям при запуске.
- Позволяет повторно использовать освобождающиеся адреса.

Протокол простого обмена электронной почты (Simple Mail Transfer Protocol):

- Позволяет клиентам отправлять электронные сообщения на почтовый сервер.
- Позволяет серверам отправлять электронные сообщения на другие серверы.

Протокол почтового отделения (Post Office Protocol version 3, POP3):

- Позволяет клиентам получать электронные сообщения с почтового сервера.
- Загружает электронные сообщения с почтового сервера на компьютер.

Протокол доступа к сообщениям в Интернете (Internet Message Access Protocol, IMAP):

- позволяет клиентам получать доступ к электронным сообщениям, которые хранятся на почтовом сервере.
- Синхронизирует электронные сообщения с почтовым сервером.

Протокол передачи файлов (File Transfer Protocol, FTP):

- Устанавливает правила, которые позволяют пользователю получать доступ к файлам на других узлах и обмениваться ими по сети.
- Надежный протокол доставки файлов с подтверждением и установлением соединения.

Простой протокол передачи файлов (Trivial File Transfer Protocol, TFTP):

- Простой протокол передачи файлов без установления соединения.
- Протокол передачи файлов без подтверждения в режиме негарантированной доставки (“best effort”).

- Накладные расходы ниже, чем у протокола FTP.

Протокол передачи гипертекста (Hypertext Transfer Protocol, TFTP) задает правила обмена в Интернете текстом, графическими изображениями, звуковыми, видео и другими файлами мультимедиа.

Протокол передачи датаграмм пользователя (User Datagram Protocol, UDP)

- Позволяет процессу, запущенному на одном узле, отправлять пакеты процессу, запущенному на другом узле.
- Не подтверждает успешную доставку датаграммы.

Протокол управления передачей (Transmission Control Protocol, TCP):

- Обеспечивает надежную связь между процессами, запущенными на разных узлах.
- Обеспечивает надежную передачу данных с подтверждением успешной доставки.

Протокол Интернета (Internet Protocol):

- Принимает сегменты сообщений с транспортного уровня.
- Формирует из них пакеты.
- Добавляет в пакеты адресную информацию для доставки конечному получателю сети.

Преобразование сетевых адресов (Network Address Translation, NAT) преобразует IP-адреса частной сети в глобальны уникальные IP-адреса.

Протокол управляющих сообщений в Интернете (Internet Control Message Protocol, ICMP) обеспечивает обратную связь от узла назначения к исходному узлу, чтобы сообщать об ошибках доставки пакета.

Протокол предпочтения кратчайшего пути (Open Shortest Path First, OSPF):

- Протокол маршрутизации по состоянию канала.
- Иерархическая структура на основе зон.
- Протокол внутренней маршрутизации, являющийся открытым стандартом.

Расширенный протокол внутренней маршрутизации между шлюзами (EIGRP):

- Проприетарный (принадлежащий компании) протокол маршрутизации Cisco.
- Использует составную метрику, основанную на пропускной способности, задержке, нагрузке и надежности.

Протокол разрешения адресов (Address Resolution Protocol, ARP) обеспечивает динамическое сопоставление между Ip-адресами и аппаратными адресами.

Протокол точка-точка (Point-to-Point Protocol, PPP) предоставляет средства инкапсуляции пакетов для передачи через последовательный канал.

Ethernet определяет правила для стандартов прокладки кабелей и обмена сигналами на уровне доступа к сети.

Драйвер интерфейса предоставляет компьютеру инструкции для управления конкретным интерфейсом на сетевом уровне.

1.22 На примере протокола HTTP процесс межсетевого взаимодействия между веб-браузером и веб-сервером показан на рисунках 2 - 7.

Рисунок 3 – Схема работы приложения с веб-сервером

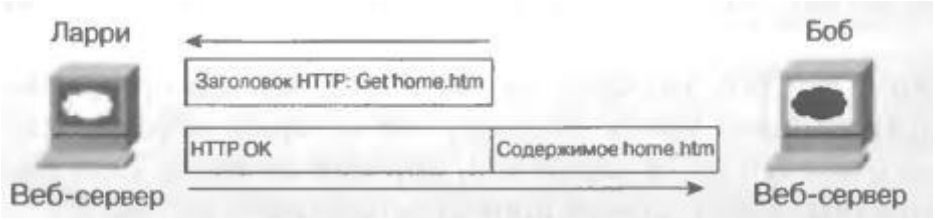


Рисунок 4 – Запрос GET протокола HTTP и HTTP – ответ

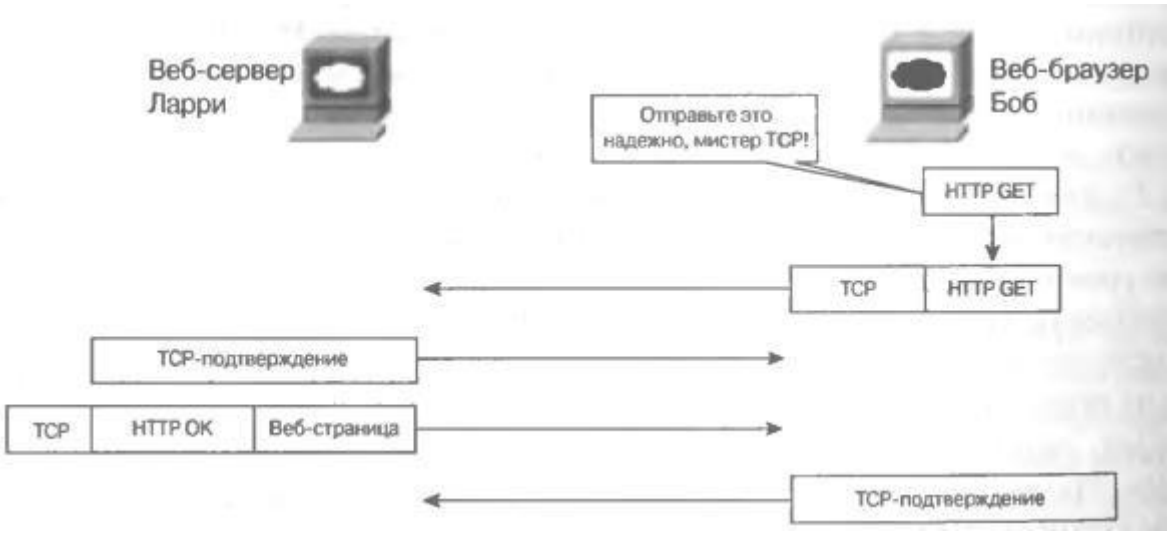


Рисунок 5 – TCP-службы, используемые протоколом HTTP

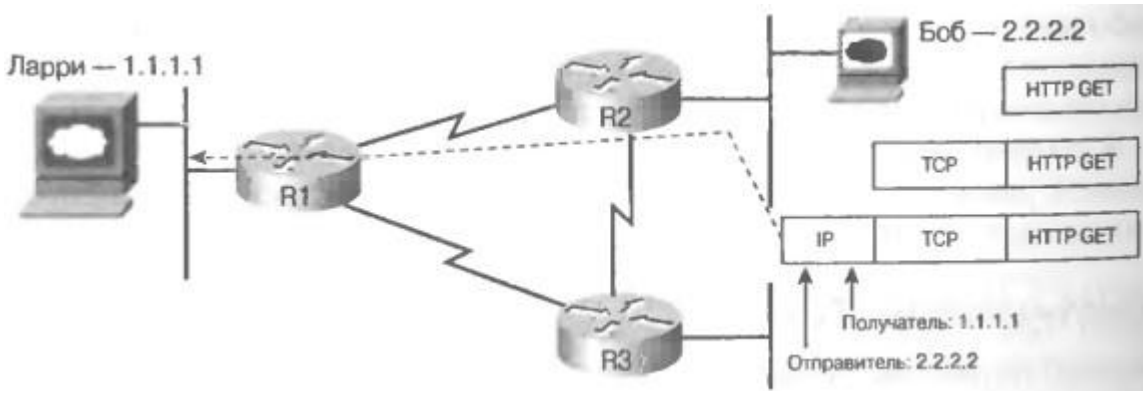


Рисунок 6 – IP-службы для протокола TCP

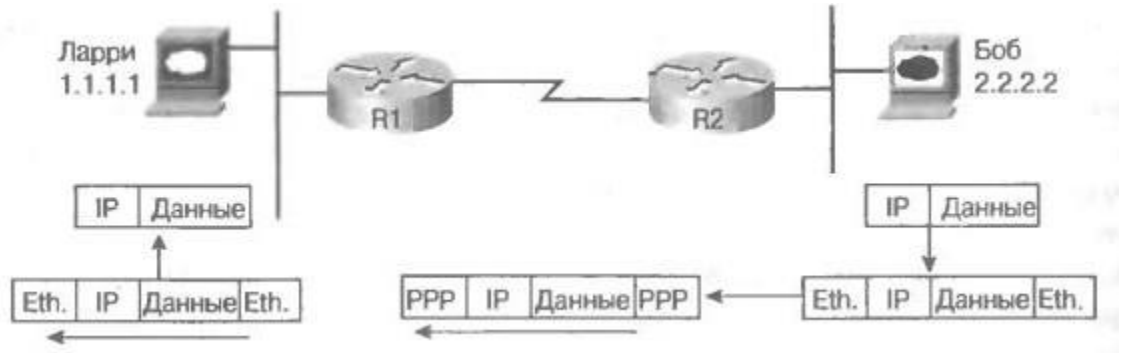


Рисунок 7 – Протокол IP использует службы Ethernet и PPP

1.23 Открытые стандарты способствуют совместимости, конкуренции и инновациям. Кроме того, они гарантируют, что продукт отдельной компании не сможет монополизировать рынок или получить несправедливое преимущество по сравнению с конкурентами.

Хороший пример — покупка беспроводного маршрутизатора для дома. Существует множество вариантов маршрутизаторов различных производителей, каждый из которых включает стандартные протоколы, такие как IPv4, DHCP, 802.3 (Ethernet) и 802.11 (беспроводная сеть LAN). Открытые стандарты также позволяют клиенту с операционной системой OS X от компании Apple загрузить веб-страницу с веб-сервера под управлением операционной системы Linux. Это связано с тем, что обе операционные системы используют протоколы открытых стандартов, например, из набора протоколов TCP/IP.

Организации по стандартизации играют важную роль в поддержании открытого Интернета со свободно доступной спецификацией и протоколами, которые могут быть реализованы любым поставщиком. Организация по стандартизации может разработать набор правил самостоятельно или в других случаях может выбрать частный протокол в качестве основы для стандарта. Если используется частный протокол, разработка стандарта, как правило, происходит с участием поставщика, который его создал.

Организации по стандартизации обычно являются независимыми от поставщиков некоммерческими организациями, созданными для разработки и продвижения концепции открытых стандартов.

1.24 Стандарты Интернета:

- **Общество Интернет (Internet Society, ISOC)** отвечает за содействие открытой разработке и расширению использования Интернета во всем мире.
- **Совет по архитектуре сети Интернет (Internet Architecture Board, IAB)** отвечает за общее руководство и разработку интернет-стандартов.
- **Инженерная группа по развитию Интернета (Internet Engineering Task Force, IETF)** разрабатывает, обновляет и поддерживает технологии Интернета и TCP/IP. Она также выпускает документы для разработки новых и обновления существующих протоколов, известные как «Рабочие предложения» (Request for Comments, RFC).
- **Исследовательская группа интернет-технологий (Internet Research Task Force, IRTF)**, проводящая долгосрочные исследования Интернета и протоколов TCP/IP, включает в себя Группу исследования защиты от спама (Anti-Spam Research Group, ASRG), Группу исследования криптографической защиты (Crypto Forum Research Group, CFRG) и Группу исследования одноранговых сетей (Peer-to-Peer Research Group, P2PRG).
- **Корпорация по управлению доменными именами и IP-адресами (Internet Corporation for Assigned Names and Numbers, ICANN)** — некоммерческая организация в США, координирующая действия по выделению IP-адресов, управлению доменными именами, а также другими данными, используемыми в протоколах TCP/IP.
- **Администрация адресного пространства Интернет (Internet Assigned Numbers Authority, IANA)** отвечает за контроль и управление распределением IP-адресов, управление доменными именами и идентификаторами протоколов для ICANN.

1.25 **Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE;** произносится по-английски «ай трипл и») —

организация, занимающаяся внедрением технологических инноваций и созданием стандартов в различных отраслях, включая энергетику, здравоохранение, телекоммуникации и сетевые технологии. Некоторые сетевые стандарты.

1.26 Модель OSI - эталонная модель обеспечивает единообразное применение всех сетевых протоколов и сервисов, описывая то, что необходимо сделать на определенном уровне, но не предписывая конкретные способы выполнения. Модель OSI является популярной эталонной моделью объединенной сети, одновременно будучи протокольной моделью для набора протоколов OSI. Модель OSI определяет широкий список функций и сервисов, реализуемых на каждом уровне. Кроме того, она описывает взаимодействие каждого уровня с вышестоящими и нижестоящими уровнями.

1.27 Уровни модели OSI

Уровень приложений содержит протоколы для обмена данными между процессами.

Уровень представлений обеспечивает общее представление данных, передаваемых между службами уровня приложений.

Сеансовый уровень передает сервисы на уровень представлений для организации его диалога и управления обмена данными.

Транспортный уровень определяет сервисы для сегментации, передачи и сборки данных для отдельных коммуникаций между оконечными устройствами.

Сетевой уровень предоставляет функции для обмена отдельными частями данных по сети между указанными оконечными устройствами.

Канальный уровень – протоколы канального уровня описывают способы обмена кадрами между устройствами по общей среде передачи данных.

Физический уровень – протоколы физического уровня описывают электрические, механические, функциональные и процедурные средства для активации, поддержки и де-

активации физического соединения, обеспечивающего передачу битов из одного сетевого устройства в другое.

1.28 Модель TCP/IP - протокольная модель соответствует структуре определенного набора протоколов. TCP/IP является протокольной моделью, поскольку в ней описываются функции, которые выполняются на каждом уровне протоколов, входящих в набор протоколов TCP/IP. TCP/IP также используется в качестве эталонной модели. Протоколы TCP/IP соотносятся как с моделью OSI, так и с моделью TCP/IP.

1.29 Уровни модели TCP/IP показаны на рисунке 8.

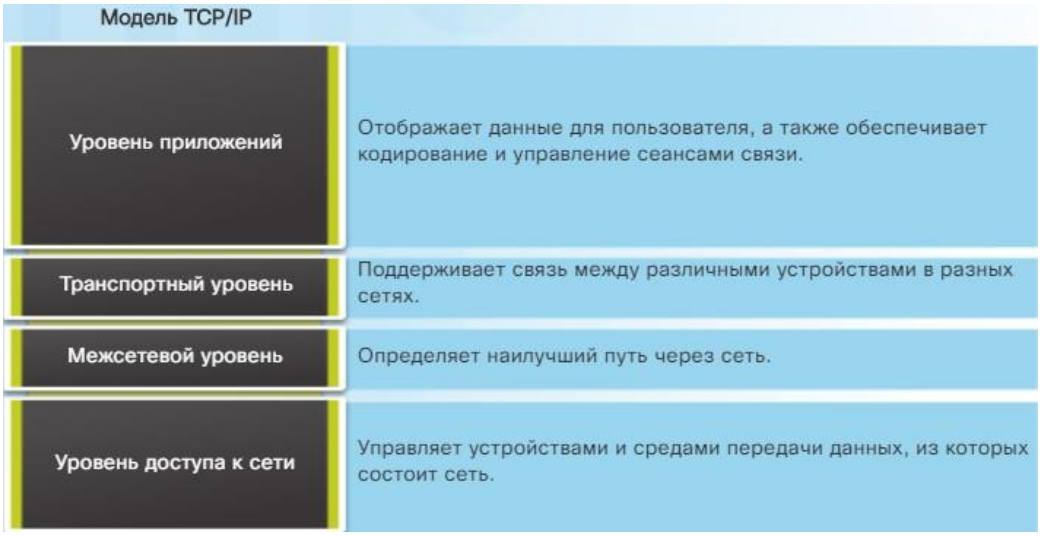


Рисунок 8 – Модель TCP/IP

1.30 Сравнение моделей TCP/IP и OSI показано на рисунке 9.

Рисунок 9 - Сравнение моделей OSI и TCP/IP

1.31 Разделение потока данных на более мелкие части называется сегментацией. Сегментация сообщения предоставляет два основных преимущества.

- Отправка небольших отдельных частей от источника к получателю в сети позволяет поддерживать множество различных чередующихся сеансов обмена сообщениями, это называется мультиплексированием.
- Сегментация позволяет повысить надежность сетевого взаимодействия. Если какую-либо часть сообщения не удается доставить к месту назначения из-за отказа сети, необходимо будет повторно передать только недостающие части сообщения.

Недостаток использования сегментации и мультиплексирования для передачи сообщений через сеть — сложность, которая свойственна всему процессу. Представьте себе, что необходимо отправить письмо из 100 страниц, но каждый конверт вмещает только одну страницу. Процесс написания адресов, наклеивание марок, получение и открытие всех 100 конвертов отнимает много времени у отправителя и получателя.

В области сетевых коммуникаций все сегменты сообщения должны пройти подобный процесс, чтобы сообщение было доставлено до нужного места назначения и было воссоздано содержимое исходного сообщения.

1.32 Форма, которую принимает массив данных на каждом из уровней, называется протокольным блоком данных (Protocol Data Unit, PDU). В ходе инкапсуляции каждый последующий уровень инкапсулирует PDU, полученную от вышестоящего уровня в соответствии с используемым протоколом. На каждом этапе процесса PDU получает другое имя, отражающее новые функции. Универсальной схемы именования для PDU нет, поэтому часто PDU называют в соответствии с терминологией набора протоколов TCP/IP.

1.33 При отправке сообщения по сети процесс инкапсуляции идет от верхнего уровня к нижнему. Данные на каждом уровне оказываются вложенными внутрь инкапсулированного протокола. Например, сегмент TCP является частью данных внутри IP-пакета. Обратный процесс на принимающем узле называется деинкапсуляцией. Деинкапсуляция — это процесс удаления одного или нескольких заголовков принимающим устройством. По мере продвижения данных по стеку к приложениям для конечных пользователей они деинкапсулируются.

1.34 Сетевой и канальный уровни отвечают за доставку данных с устройства-источника на устройство назначения. Протоколы на обоих уровнях содержат адреса источника и места назначения, но эти адреса служат разным целям.

- **Адрес источника и места назначения сетевого уровня** необходим для доставки IP-пакета от источника к месту назначения в той же или в удаленной сети.
- **Адрес источника и места назначения канального уровня** необходим для доставки кадра канала данных от одной сетевой интерфейсной платы (NIC) к другой сетевой интерфейсной плате в той же сети.

1.35 Если отправитель и получатель IP-пакета находятся в одной и той же сети, кадр канала данных отправляется напрямую принимающему устройству. В сети

Ethernet адреса канала данных называются MAC-адресом (Media Access Control) Ethernet. MAC-адреса физически присвоены сетевой интерфейсной плате Ethernet.

1.36 Если отправитель и получатель пакета находятся в разных сетях, IP-адреса источника и места назначения будут представлять узлы в разных сетях. На это будет указывать сетевая часть IP-адреса узла назначения. Для каждого узла в локальной сети важно правильно настроить IP-адрес основного шлюза. Все пакеты, предназначенные для отправки в удаленную сеть, направляются на шлюз по умолчанию.

Тема 1.3 Сетевой доступ

1.37 Независимо от того, подключаетесь ли вы к домашнему локальному принтеру или же к веб-сайту в другой стране, для передачи данных по сети необходимо сначала установить физическое подключение к локальной сети. В качестве физического подключения может использоваться проводное соединение с помощью кабеля или беспроводное соединение по радиоканалу.

1.38 Сетевые интерфейсные платы (Network Interface Card, NIC) служат для подключения устройства к сети. Сетевые платы Ethernet используются для проводного подключения, как показано на рисунке, а сетевые платы беспроводной локальной сети (Wireless Local Area Network, WLAN) — для беспроводного подключения. Устройство конечного пользователя может содержать один или оба типа сетевых плат. Например, если сетевой принтер оснащен только сетевой платой Ethernet, то он должен подключаться к сети с помощью кабеля Ethernet. Другие устройства, например, планшеты и смартфоны, могут быть оснащены только сетевой платой WLAN и поэтому для них необходимо использоваться беспроводное подключение.

1.39 Физический уровень сетевого доступа обеспечивает средства транспортировки битов, образующих кадр данных канального уровня, по средствам сетевого подключения. Этот уровень принимает от канального уровня целый кадр данных и кодирует его в виде последовательности сигналов, которые затем пересылаются по средству подключения локальной или глобальной сети. Закодированные биты, из которых состоит кадр, принимаются либо оконечным, либо промежуточным устройством.

1.40 Существует три основных типа средств сетевого подключения. Физический уровень создает представления битов и группирует их для каждого из этих типов следующим образом.

- **Медный кабель**: сигналы представляют собой последовательность электрических импульсов.
- **Оптоволоконный кабель**: сигналы представляют собой управляемые изменения светового излучения.
- **Беспроводная сеть**: сигналы представляют собой радиосигналы микроволнового диапазона.

1.41 Физический уровень состоит из электронных схем, средств подключения и разъемов, разрабатываемых инженерами. Поэтому закономерно, что стандарты, регламентирующие это оборудование, определяются соответствующими организациями по электротехнике и связи.

В создании и реализации стандартов физического уровня участвует целый ряд различных международных и национальных организаций, правительственных регулирующих организаций, а также частных компаний. Например, стандарты на оборудование, средства подключения, кодирование и сигналы физического уровня разрабатывают следующие организации.

- Международная организация по стандартизации (ISO)
- Ассоциация телекоммуникационной промышленности/Ассоциация электронной промышленности (TIA/EIA)
- Международный союз электросвязи (ITU)
- Американский национальный институт стандартизации (ANSI)
- Институт инженеров по электротехнике и электронике (IEEE)
- Региональные органы регулирования телекоммуникаций, в том числе Федеральная комиссия по связи (FCC) в США и Европейский институт телекоммуникационных стандартов (ETSI).

Кроме этого, нередко местные спецификации разрабатываются региональными группами по кабельным стандартам, например, CSA (Канадская ассоциация по стандартизации), CENELEC (Европейский комитет электротехнической стандартизации) и JSA/JIS (Японская ассоциация по стандартизации).

1.42. Производительность сети, состоящей из нескольких сетей или нескольких сегментов, не может превышать скорость самого медленного соединения между источником и получателем. Даже если все или большинство сегментов имеют высокую пропускную способность, один-единственный сегмент с низкой производительностью создаст узкое место и производительность всей сети будет снижена.

1.43 **Производительность (throughput)** — это количество битов, передаваемых по средствам подключения за определенный период времени.
Из-за множества факторов производительность (throughput) обычно не соответствует заявленной пропускной способности (bandwidth) в реализациях на физическом уровне. На производительность влияет ряд факторов, в том числе следующие.
- Объем трафика
- Тип трафика
- Суммарная задержка, зависящая от количества сетевых устройств между источником и пунктом назначения.

Задержки в сети оказывают влияние на итоговое время, необходимое для доставки данных из одной точки в другую.

1.44 **Пропускная способность (bandwidth)** — это количественная характеристика, отражающая возможности передачи данных по конкретному средству подключения. В цифровых сетях под пропускной способностью понимается объем данных, который можно передать из одной точки в другую за определенное время. Обычно пропускная способность измеряется в килобитах в секунду (Кбит/с), мегабитах в секунду (Мбит/с) или гигабитах в секунду (Гбит/с). Иногда под пропускной способностью понимают скорость доставки битов, хотя это не совсем точно. Например, и в сети Ethernet 10 Мбит/с, и в сети Ethernet 100 Мбит/с биты передаются со скоростью распространения электрического сигнала. Разница заключается в количестве битов, передаваемых в секунду.

Фактическая пропускная способность сети определяется сочетанием следующих факторов.
- Свойства физических средств подключения
- Технологии передачи и обнаружения сигналов в сети.
На реальную пропускную способность влияют свойства физических средств подключения, используемые технологии и законы физики.

Существует также третий параметр, характеризующий передачу полезных данных, который называется **полезной пропускной способностью (goodput)**. Полезная пропускная способность — это объем полезных данных, передаваемых за определенный период времени. Полезная пропускная способность (goodput) равна производительности (throughput) за вычетом служебного трафика, необходимого для создания сеансов, подтверждений и инкапсуляции.

1.45 Физический уровень обеспечивает представление потока битов в виде изменений уровней напряжения, модулированных радиочастотных сигналов или световых импульсов. Организациями по стандартизации были совместно выработаны требования к физическим, электрическим и механическим свойствам средствам подключения для разных видов коммуникаций. Эти спецификации гарантируют надлежащую работу кабелей и разъемов с различными реализациями канального уровня. Например, для средств подключения на основе медного кабеля определены следующие стандарты.
- Тип используемого медного кабеля
- Пропускная способность
- Тип используемых разъемов
- Назначение и цветовая маркировка контактов разъемов средства подключения
- Максимально допустимая длина кабеля.

1.46 Коаксиальный кабель (толстый и тонкий) и кабель на основе витой пары (экранированной и неэкранированной).

1.47 Коаксиальный кабель называется так потому, что он содержит два соосных проводника. Коаксиальный кабель состоит из следующих элементов.
- Медный проводник, используемый для передачи электрических сигналов.
- Слой гибкой пластиковой изоляции вокруг медного проводника.
- Медная оплетка или металлическая фольга, окружающая слой изолирующего материала и выступающая в качестве второго провода в цепи, а также экрана для внутреннего проводника. Этот второй слой, называемый экраном, также снижает уровень внешних электромагнитных помех.
- Снаружи кабель покрыт кабельной оболочкой для защиты от незначительных физических повреждений.

1.48 Кабели на основе неэкранированной витой пары (UTP) являются самым распространенным средством подключения. Кабели UTP с разъемами RJ-45 используются для соединения узлов с промежуточными сетевыми устройствами, такими как коммутаторы и маршрутизаторы.

Кабель UTP для локальных сетей состоит из четырех скрученных пар проводников с цветовой маркировкой, которые заключены в общую гибкую пластиковую оболочку, защищающую кабель от незначительных повреждений. Скручивание проводников снижает влияние помех от других проводников.

1.49 Кабели на основе экранированной витой пары (STP) лучше защищены от помех, чем кабели UTP. Но при этом они значительно дороже, и их сложнее монтировать. Как и для кабелей типа UTP, для кабелей STP используется разъем RJ-45.
В кабелях STP применяется как экранирование для защиты от ЭМП и РЧП, так и скручивание проводников для защиты от переходных помех. Для получения наиболее полного эффекта от экранирования кабели STP оснащаются специальными экранированными разъемами для линий передачи данных STP. Если такой кабель не заземлить должным образом, то экран может действовать как антенна и принимать нежелательные сигналы.

1.50 Оптическое волокно — это гибкая, очень тонкая и прозрачная нить из химически чистого стекла толщиной немногим более человеческого волоса. Для передачи по оптоволоконному кабелю биты кодируются с помощью световых импульсов. Оптоволоконный кабель действует как световод, или «оптический волновод», обеспечивающий передачу светового сигнала между двумя концами кабеля с минимальными потерями.
Оптоволокно состоит из двух видов стеклянных компонентов (сердечника и внутренней оболочки) и защитной внешней оболочки.
Хотя оптоволокно очень тонкое и может легко гнуться, но благодаря свойствам сердечника и оболочки оно очень прочное. Благодаря своей прочности оптическое волокно может использоваться в самых тяжелых условиях эксплуатации.

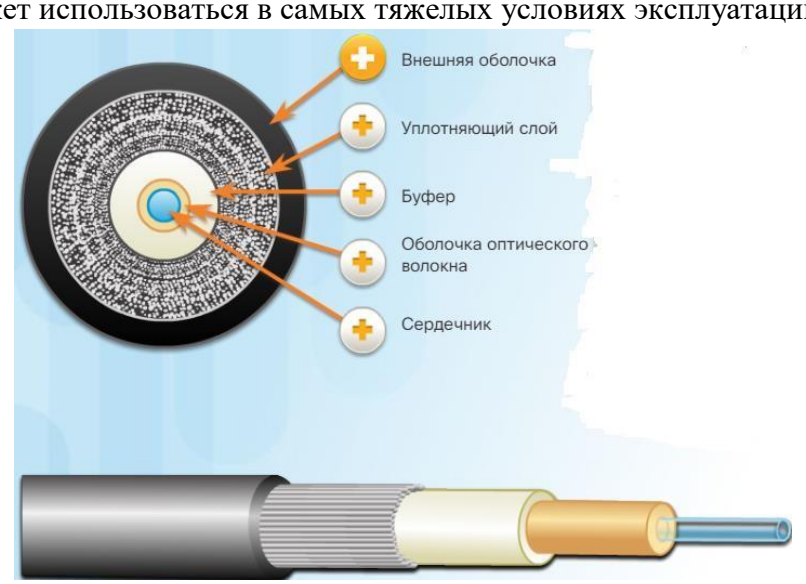


Рисунок 10 Конструкция оптоволоконного кабеля

Сердечник – это и есть светопередающая среда в центре оптоволоконного кабеля. Как правило, он выполняется из кварца или стекла. По сердечнику передаются световые импульсы.
- Оболочка оптического волокна изготавливается из материалов, слегка отличающихся от тех, из которых изготавливается сердечник. Играет роль своего рода зер-

кала, которое отражает свет в сердечник оптоволоконного кабеля. Это предотвращает рассеивание света при прохождении его по кабелю.
- Буфер используется для защиты сердечника кабеля и оболочки оптического волокна от повреждений.
- Уплотняющий слой окружает буфер и защищает оптоволоконный кабель от растяжения при вытаскивании. В качестве материала для уплотняющего слоя часто используется материал для изготовления бронежилетов.
- Внешняя оболочка – это ПВХ-оболочка для защиты волокна от истирания, влаги и загрязнений. Состав внешней оболочки зависит от области применения кабеля.

1.51 Оптоволоконные кабели подразделяются на два основных типа:
- одномодовый;
- многомодовый.
Одно из основных отличий между МОК и ООК — уровень дисперсии. Под дисперсией в данном контексте понимается расширение светового импульса по мере его движения по оптическому волокну. Чем выше дисперсия, тем больше потери сигнала.

1.52 Многомодовый оптоволоконный кабель (МОК). Имеет сердечник большего диаметра. Для передачи световых импульсов используются светодиодные излучатели. Свет, излучаемый светодиодом, входит в многомодовое волокно под разными углами. Такие кабели популярны в локальных сетях, поскольку позволяют использовать для работы недорогие светодиоды. Многомодовый кабель обеспечивает пропускную способность до 10 Гбит/с на расстоянии до 550 метров.

1.53 Одномодовый оптоволоконный кабель (ООК). Имеет сердечник очень малого диаметра. Для передачи луча света требуется дорогостоящая лазерная технология. Широко используется для организации линий связи протяженностью несколько сот километров, например, для дальней телефонии и кабельного телевидения.

1.54 Беспроводная среда имеет следующие особенности, которые необходимо учитывать.
- Зона покрытия. Беспроводные технологии передачи данных хорошо работают на открытых пространствах. Однако некоторые строительные материалы, используемые при возведении зданий и сооружений, а также условия местности могут ограничивать зону покрытия.
- Помехи. Качество беспроводных соединений восприимчиво к помехам и может ухудшаться при работе таких обычных устройств, как беспроводные телефоны, некоторые типы флуоресцентных ламп, микроволновые печи, а также под влиянием других беспроводных коммуникаций.
- Безопасность. Для доступа к среде беспроводного подключения не требуется подключаться к физическим кабелям. Поэтому доступ к этой среде могут получать несанкционированные пользователи и устройства. Следовательно, главным аспектом администрирования беспроводной сети является безопасность.
- Совместный доступ к средству подключения. Сети WLAN работают в полудуплексном режиме, что означает, что в каждый момент времени передачу или прием может осуществлять только одно устройство. Средства беспроводного подключения совместно используют все беспроводные пользователи. Чем больше пользова-

телей одновременно подключаются к WLAN, тем меньшая пропускная способность приходится на каждого из них.

1.55 Чаще всего беспроводная передача данных используется для беспроводной связи устройств через локальную сеть (LAN). Как правило, для создания беспроводной LAN требуются следующие сетевые устройства.

- Беспроводная точка доступа (AP): концентрирует беспроводные сигналы от пользователей. Подключается к сетевой инфраструктуре на основе медных кабелей, например, Ethernet. Беспроводные маршрутизаторы для дома и небольших предприятий (смотри рисунок 34) в одном устройстве сочетают функции маршрутизатора, коммутатора и точки доступа.
- Беспроводные сетевые платы: обеспечивают возможность беспроводного подключения для каждого узла в сети.

По мере развития технологии был создан целый ряд стандартов беспроводной локальной сети (WLAN) на основе Ethernet. Поэтому, приобретая беспроводные устройства, следует обращать особое внимание на их совместимость.

1.56 Канальный уровень сетевого доступа (уровень 2 модели OSI) выполняет следующие функции.

- Обеспечение доступа вышестоящих уровней к средству подключения
- Прием пакетов уровня 3 и упаковка их в кадры
- Подготовка сетевых данных для передачи по физической сети
- Управление передачей и приемом данных в средстве подключения
- Обмен кадрами между узлами по физическим средствам сетевого подключения, например, по кабелям UTP или оптоволоконным кабелям
- Прием пакетов и их перенаправление протоколам вышестоящего уровня
- Обнаружение ошибок.

1.57 Канальный уровень разделяется на следующих два подуровня.

- Управление логическим соединением (Logical Link Control, LLC). Этот верхний подуровень взаимодействует с сетевым уровнем. Он помещает в кадр информацию, указывающую, какой протокол сетевого уровня используется для данного кадра. Данная информация позволяет различным протоколам 3-го уровня, таким как IPv4 и IPv6, использовать один и тот же сетевой интерфейс, и одно и то же средство подключения.
- Управление доступом к среде (Media Access Control, MAC). Это нижний подуровень, который определяет процессы доступа к среде, выполняемые оборудованием. Он обеспечивает адресацию канального уровня и доступ к различным сетевым технологиям.

1.58 Протоколы уровня 2 определяют инкапсуляцию пакета в кадр, а также методы ввода инкапсулированных пакетов в различные средства подключения и обратного извлечения этих пакетов. Технология, используемая для ввода кадра в средство подключения и его обратного извлечения, называется методом управления доступом к среде.

При прохождении пакетов от узла источника к узлу адресата они обычно передаются по различным физическим сетям. Эти физические сети могут состоять из физических средств подключения различного типа, например, медных и оптоволо-

конных кабелей, средств беспроводного подключения на основе электромагнитных сигналов, а также радиочастотных, микроволновых и спутниковых каналов.
Если бы канального уровня не существовало, протоколы сетевого уровня, например, IP, должны были бы обеспечивать соединение для всех типов средств подключения, которые могли встретиться на пути следования пакета. Более того, протоколу IP пришлось бы каждый раз адаптироваться к новой сетевой технологии или среде. Такой процесс затруднил бы обновление и развитие протоколов и средств сетевого подключения. В этом и заключается основная причина использования многоуровневого подхода к построению сетей.
Несмотря на то, что два узла взаимодействуют друг с другом исключительно через IP, для передачи IP-пакетов по различным типам локальных и глобальных сетей могут использоваться различные протоколы канального уровня. Каждый переход на маршрутизаторе может потребовать иного протокола канального уровня для передачи в новой среде.

1.59 В отличие от протоколов верхних уровней стека TCP/IP протоколы канального уровня, как правило, не определяются документами RFC (Request for Comments, RFC). Несмотря на то, что Инженерная группа по развитию Интернета (IETF) поддерживает функциональные протоколы и службы для стека протоколов TCP/IP на верхних уровнях, IETF не определяет функции и принципы работы уровня доступа к сети для этой модели.
Определением открытых стандартов и протоколов, применимых к канальному уровню доступа, занимаются следующие организации:
- Институт инженеров по электротехнике и электронике (IEEE)
- Международный союз электросвязи (ITU)
- Международная организация по стандартизации (ISO)
- Американский национальный институт стандартизации (ANSI).

1.60 Топология сети описывает расположение или взаимосвязь сетевых устройств, а также соединения между ними. Топологии LAN и WAN можно рассматривать с двух точек зрения.
- Физическая топология. Этот термин относится к физическим соединениям и определяет, каким образом соединяются друг с другом оконечные устройства и устройства сетевой инфраструктуры, такие как маршрутизаторы, коммутаторы и беспроводные точки доступа. Физическая топология чаще всего организована по схеме «точка-точка» или «звезда».
- Логическая топология: термин, используемый для описания путей передачи кадров между узлами. Структура логической топологии состоит из виртуальных соединений между узлами сети. Эти логические пути сигналов определены протоколами канального уровня. Логическая топология каналов «точка-точка» сравнительно проста, хотя совместно используемая среда подключения позволяет применять различные методы управления доступом.

1.61 Соединения в глобальных сетях обычно организуются с помощью следующих физических топологий.
- «Точка-точка» (Point-to-Point): это простейшая топология, представляющая собой постоянное соединение между двумя оконечными точками. Именно по этой причине данная топология глобальной сети является наиболее распространенной.

- «Звездообразная» (Hub and spoke): версия звездообразной топологии для глобальной сети, в которой центральный узел соединен с периферийными с помощью соединений «точка-точка».
- Ячеистая (Mesh): эта топология обеспечивает высокую доступность, но требует, чтобы каждая оконечная система была связана со всеми остальными системами. Поэтому административные и физические расходы могут быть весьма значительными. Каждый канал в такой сети фактически является каналом, связанным с другим узлом соединением «точка-точка».

1.62 Физическая топология определяет, как именно физически соединены оконечные системы. В локальных сетях с совместно используемой средой оконечные устройства могут быть соединены с помощью следующих физических топологий.
- Звезда (Star): в топологиях типа «звезда» оконечные устройства подключаются к центральному промежуточному устройству. В ранних топологиях типа «звезда» оконечные устройства соединялись с помощью концентраторов Ethernet. Однако теперь в топологиях типа «звезда» используются коммутаторы Ethernet. Топологию типа «звезда» отличают простой монтаж, высокая масштабируемость (простое добавление и удаление оконечных устройств) и простое устранение неполадок.
- Расширенная звезда (Extended Star): в расширенной звездообразной топологии дополнительные коммутаторы Ethernet обеспечивают соединение с другими звездообразными топологиями. Расширенная звезда — это пример гибридной топологии.
- Шина (Bus): все оконечные системы связаны друг с другом общим кабелем, имеющим на концах специальные заглушки («терминаторы»). Для соединения оконечных устройств коммутаторы не требуются. Шинные топологии на основе коаксиальных кабелей использовались ранее в сетях Ethernet благодаря своей дешевизне и простому монтажу.
- Кольцо (Ring): каждая оконечная система соединяется с соседней системой, образуя сеть в форме кольца. В отличие от шинной топологии кольцевая топология не требует применения терминаторов. Кольцевые топологии использовались в устаревших сетях FDDI (Fiber Distributed Data Interface) и Token Ring. Хотя эта топология и показана в разделе физических, на самом деле это – логическая топология, так как кольцо организовано логически внутри концентратора, а сами устройства подсоединяются по физической топологии звезда.

1.63 Дуплексная связь — это связь с возможностью передачи информации между двумя устройствами в обоих направлениях. При полудуплексной связи передача данных в каждый момент времени возможна только в одном направлении (т. е. их можно либо передавать, либо принимать), тогда как при полнодуплексной связи данные можно передавать и принимать одновременно.
- Полудуплексная связь: оба устройства могут передавать и получать информацию через среду, но не одновременно. Полудуплексный режим используется в устаревших шинных топологиях и при использовании концентраторов Ethernet. Сети WLAN также работают в полудуплексном режиме. Полудуплексный режим позволяет осуществлять передачу или прием по общей среде одновременно только одному устройству и используется в случае применения методов конкурентного доступа.

- Полнодуплексная связь: оба устройства одновременно могут передавать и принимать данные по средствам подключения. Канальный уровень предполагает одновременную доступность среды обоим узлам для передачи. Коммутаторы Ethernet по умолчанию работают в полнодуплексном режиме, но могут работать и в полудуплексе при подключении к таким устройствам, как коммутаторы Ethernet.
- Симплексная связь – однонаправленная связь (радио, телевидение).

1.64 В некоторых сетевых топологиях множество узлов использует общее средство подключения. Такие сети называются сетями с множественным доступом. Примерами таких сетей являются локальные сети Ethernet и беспроводные локальные сети (WLAN). В любой момент может возникнуть ситуация, когда несколько устройств пытается отправить или получить данные, используя одно и то же средство подключения.
В некоторых сетях с множественным доступом необходимы правила регулирования доступа устройств к общей физической среде. Существует два основных метода управления доступом к общей среде.
- Конкурентный доступ: все узлы, работающие в полудуплексном режиме, соревнуются за использование среды, но осуществлять передачу в каждый момент времени может лишь одно устройство. Однако существует специальный протокол, определяющий, что должно происходить в случае одновременной передачи обоими устройствами. Примерами такого типа управления доступом являются локальные сети Ethernet с концентраторами и беспроводные локальные сети (WLAN).
- Управляемый доступ: каждому узлу отводится собственное время для использования среды. Такие детерминистические типы сетей являются неэффективными из-за того, что устройство должно дожидаться своей очереди для доступа к среде. Примерами такого типа управления доступом являются устаревшие сети Token Ring.

1.65 Маркерный метод доступа к среде используется в устаревших сетях Token Ring с логической топологией «кольцо». Право на передачу своего кадра получает компьютер, получивший маркер – кадр специального формата.

1.66 CSMA/CD (Carrier Sense Multiple Access with Collision Detection) — метод доступа к сети (стандарт IEEE 802.3), при котором узел «слушает» среду перед передачей. Если канал свободен, он начинает передачу, а при обнаружении коллизии (конфликта сигналов) прерывает ее, выжидает случайное время и пытается отправить данные снова, что критично для Ethernet. Использовался в первых сетях Ethernet с логической топологией «общая шина».

1.67 CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) — это метод доступа к сети, используемый преимущественно в беспроводных сетях (Wi-Fi, 802.11) для предотвращения коллизий, а не их обнаружения. Устройство «прослушивает» эфир, и, если он свободен, ждет случайное время, прежде чем начать передачу, чтобы избежать конфликтов с другими узлами.

1.69 Канальный уровень подготавливает пакет для перемещения по среде передачи данных локальной сети, добавляя к нему заголовок и концевик с целью создать кадр. Описание кадра является ключевым элементом каждого протокола канального уровня. Хотя кадры канального уровня описываются множеством различных

протоколов канального уровня, кадры любого типа состоят из трех основных компонентов.
- Заголовок
- Данные
- Концевик.

Все протоколы канального уровня инкапсулируют единицу данных протокола (PDU) уровня 3 в пределах поля данных кадра. Однако структура кадра и полей, содержащихся в заголовке и концевике, отличается в зависимости от протокола.

Не существует такой структуры кадра, которая соответствовала бы требованиям всех видов передачи данных во всех типах средств подключения. Количество управляющей информации, которая должна присутствовать в кадре, зависит от окружения и изменяется в соответствии с требованиями управления доступом для конкретной среды и логической топологии.

1.70 В сети на основе стека протоколов TCP/IP все протоколы уровня 2 модели OSI работают с протоколом IP на уровне 3 модели OSI. Однако фактически используемый протокол уровня 2 зависит от логической топологии сети и физической среды передачи данных.

Каждый протокол управляет доступом к среде для указанных логических топологий уровня 2. Это означает, что при реализации этих протоколов в качестве узлов, действующих на канальном уровне, может использоваться целый ряд различных сетевых устройств. К таким устройствам относятся сетевые платы на компьютерах, а также интерфейсы на маршрутизаторах и коммутаторах уровня 2.

Протокол уровня 2, используемый для конкретной топологии сети, определяется технологией, используемой для реализации этой топологии. Эта технология, в свою очередь, определяется размером сети (с точки зрения количества узлов и территории) и сервисами, предоставляемыми в этой сети.

В локальных сетях обычно используются технологии, которые обеспечивают высокую пропускную способность и поддерживают большое количество узлов. Сравнительно небольшая протяженность локальных сетей (в пределах одного здания или комплекса зданий) и высокая плотность пользователей обеспечивают рентабельность этой технологии.

Однако использование технологии с высокой пропускной способностью обычно нерентабельно для глобальных сетей, охватывающих обширные территории (например, города или целые области). Ввиду высокой стоимости физических каналов большой протяженности и технологий, используемых для передачи сигналов на большие расстояния, пропускная способность таких сетей, как правило, определяется уровнем рентабельности.

Разница в пропускной способности требует использования различных протоколов для локальных и глобальных сетей.

К протоколам канального уровня относятся:
- Ethernet
- Беспроводная сеть 802.11
- Протокол точка-точка (протокол PPP)
- HDLC
- Протокол ретрансляции кадров (протокол Frame Relay)

1.71 Канальный уровень обеспечивает адресацию, используемую при пересылке кадра по совместно используемой среде передачи данных в локальной сети. Адреса устройств на этом уровне называются физическими адресами. Адресация канального уровня содержится в заголовке кадра и указывает узел назначения кадра в локальной сети. Заголовок кадра может также содержать адрес источника кадра.
В отличие от логических адресов уровня 3, которые являются иерархическими, физические адреса не указывают, в какой сети находится устройство. Физический адрес — это адрес конкретного физического устройства. Если устройство перемещается в другую сеть или подсеть, оно продолжит функционировать с тем же физическим адресом уровня 2.
В ходе пересылки IP-пакетов от узла к маршрутизатору, между маршрутизаторами и, наконец, от маршрутизатора к узлу в каждой точке на пути своего следования IP-пакет инкапсулируется в новый кадр канала передачи данных. Каждый кадр канального уровня содержит адрес канала-источника (передавшего этот кадр сетевой платы) и адрес канала назначения (сетевой платы, принимающей этот кадр).
Адрес, соответствующий конкретному устройству и не являющийся иерархическим, нельзя использовать для поиска устройств в больших сетях или в Интернете. Это было бы так же сложно, как искать единственный конкретный дом по всему земному шару, зная лишь номер дома и название улицы. Однако физический адрес можно использовать для обнаружения устройства в ограниченной зоне. Поэтому адрес канального уровня используется только для локальной доставки пакетов. Адреса этого уровня не имеют смысла за пределами локальной сети. Сравните их с уровнем 3, где адреса в заголовке пакета передаются от узла источника на узел назначения, независимо от количества транзитных участков сети на протяжении маршрута.
Если данные должны перейти в другой сегмент сети, необходимо промежуточное устройство, например, маршрутизатор. Маршрутизатор должен принять кадр согласно физическому адресу и деинкапсулировать его для анализа иерархического адреса или IP-адреса. С помощью IP-адреса маршрутизатор может определить местоположение устройства назначения в сети, а также наилучший путь к нему. Узнав, куда необходимо переслать пакет, маршрутизатор создает для него новый кадр, который отправляется в следующий сетевой сегмент к месту назначения.

Тема 1.4. Сетевые технологии Ethernet

1.72 Процесс инкапсуляции данных включает в себя сборку кадра перед его отправкой и разборку кадра после его получения. При формировании кадра на уровне MAC к единице данных протокола (PDU) сетевого уровня добавляются заголовок и концевик.
Инкапсуляция данных обеспечивает три основных функции.
- Разделение кадра: процесс формирования кадров предоставляет важные разделители, которые используются для определения группы бит, составляющих кадр. Эти разграничивающие биты обеспечивают синхронизацию между передающими и получающими узлами.
- Адресация: процесс инкапсуляции содержит единицу данных протокола (PDU) уровня 3 и также обеспечивает адресацию канального уровня.
- Обнаружение ошибок: каждый кадр содержит концевик, позволяющий выявлять ошибки передачи.

Использование кадров облегчает отправку бит в среду передачи данных, а также позволяет группировать биты на принимающем узле.

1.73 Подуровень LLC технологии Ethernet обеспечивает связь между верхними и нижними уровнями. Как правило, это происходит между сетевым программным обеспечением и аппаратным обеспечением устройства. Подуровень LLC использует данные сетевых протоколов, которые обычно представлены в виде IPv4-пакета, и добавляет управляющую информацию для доставки пакета к узлу назначения. LLC используется для связи с верхними уровнями приложений и передачи пакета на нижние уровни.
LLC реализован в программном обеспечении, и его применение не зависит от оборудования. LLC для компьютера можно рассматривать как программное обеспечение драйвера сетевой платы (NIC). Драйвер сетевой платы — это программа, которая непосредственно взаимодействует с аппаратными средствами компьютера на сетевой плате для передачи данных между подуровнем MAC и физической средой.

1.74 MAC представляет собой более низкий подуровень канального уровня. MAC реализуется аппаратно — обычно в сетевой плате компьютера. Спецификации содержатся в стандартах IEEE 802.3.
Подуровень MAC технологии Ethernet выполняет две основные задачи.
- Инкапсуляция данных
- Управление доступом к среде.

1.75 Инкапсуляция данных обеспечивает три основных функции.
- Разделение кадра: процесс формирования кадров предоставляет важные разделители, которые используются для определения группы бит, составляющих кадр. Эти разграничивающие биты обеспечивают синхронизацию между передающими и получающими узлами.
- Адресация: процесс инкапсуляции содержит единицу данных протокола (PDU) уровня 3 и также обеспечивает адресацию канального уровня.
- Обнаружение ошибок: каждый кадр содержит концевик, позволяющий выявлять ошибки передачи.

1.76 Управление доступом к среде передачи данных отвечает за размещение кадров в этой среде и удаление из нее кадров. Как понятно из названия этой функции, она позволяет управлять доступом к среде передачи данных. Этот подуровень напрямую взаимодействует с физическим уровнем.
Основная логическая топология Ethernet — это шина с множественным доступом; следовательно, среда передачи данных используется всеми узлами (устройствами) в одном сегменте сети. Ethernet — это способ организации сети на основе конкурентного доступа. Конкурентный доступ означает, что любое устройство может постоянно пытаться передавать данные в общей среде при наличии у него таких данных для отправки. В полудуплексных локальных сетях Ethernet для обнаружения и устранения коллизий используется метод множественного доступа с контролем несущей и обнаружением коллизий (Carrier Sense Multiple Access/Collision Detection; CSMA/CD). В современных локальных сетях Ethernet используются полнодуплексные коммутаторы, которые позволяют одновременно нескольким устройствам отправлять и получать данные без коллизий.

1.77 Этапы развития технологии Ethernet приведены ниже на рисунках 11-15

Год	1973	1980	1983
Стандарт	Ethernet	Стандарт DIX Ethernet II	IEEE 802.3 10 BASE-5
Описание	Технология Ethernet была изобретена доктором Робертом Меткалфом (Robert Metcalf), сотрудником корпорации Xerox.	Корпорации Digital Equipment Corp, Intel и Xerox (DIX) разработали стандарт Ethernet 10 Мбит/с передачей по коаксиальному кабелю	Ethernet, 10 Мбит/с, по толстому коаксиальному кабелю

Рисунок 11 – Изменение стандартов с 1973 по 1983 годы

Год	1985	1990	1993
Стандарт	IEEE 802.3a 10 BASE-2	IEEE 802.3i 10 BASE-T	IEEE 802.3j 10 BASE-F
Описание	Ethernet, 10 Мбит/с, по тонкому коаксиальному кабелю	Ethernet, 10 Мбит/с, по витой паре (TP)	Ethernet, 10 Мбит/с, по оптоволоконному кабелю

Рисунок 12 – Изменение стандартов с 1983 по 1993 годы

Год	1995	1998	1999
Стандарт	IEEE 802.3u 100 BASE-xx	IEEE 802.3z 1000 BASE-X	IEEE 802.3ab 1000 BASE-T
Описание	Fast Ethernet: Ethernet, 100 Мбит/с, по витой паре (TP) и оптоволоконному кабелю (различные стандарты)	Gigabit Ethernet, по оптоволоконном кабелю	Gigabit Ethernet, по витой паре (TP)

Рисунок 13 - Изменение стандартов с 1993 по 1999 годы

Год	2002	2006	2009 г.
Стандарт	IEEE 802.3ae 10G BASE-xx	IEEE 802.3an 10G BASE-T	802.3at (PoE)
Описание	802.3at (PoE)	Усовершенствования PoE	Усовершенствования PoE

Рисунок 14 – Изменение стандартов с 1999 по 2009 годы

2015	2016
100GbE и 40GbE	2.5GBASE-T и 5GBASE-T
100G/40G для оптоволоконного кабеля	Ethernet 2,5 и 5 Гбит/с по витой паре

Рисунок 15 – Изменение стандартов с 2009 по настоящее время

1.78 Кадр Ethernet (стандарт DIX/Ethernet II) — это блок данных канального уровня, который состоит из обязательных полей: преамбулы (8 байт), MAC-адресов получателя/отправителя (по 6 байт), типа протокола (2 байта), данных (46-1500 байт) и контрольной суммы FCS (4 байта). Общая длина кадра варьируется от 64 до 1518 байт.
Основные поля кадра Ethernet:

- Преамбула (Preamble) — 7 байт: Последовательность чередующихся 0 и 1 для синхронизации часов отправителя и получателя.
- Разделитель начала кадра (SFD) — 1 байт: Обозначает начало кадра (заканчивается на 11).
- MAC-адрес получателя (Destination Address) — 6 байт: Физический адрес целевого устройства (unicast, multicast или broadcast).
- MAC-адрес источника (Source Address) — 6 байт: Физический адрес отправителя.
- Тип/EtherType — 2 байта: Определяет протокол верхнего уровня (например, 0x0800 — IPv4, 0x86DD — IPv6).
- Данные (Payload) — 46–1500 байт: Полезная нагрузка (например, IP-пакет). Если данных меньше 46 байт, добавляется поле заполнения (padding).
- Контрольная сумма (FCS/CRC) — 4 байта: Используется для обнаружения ошибок при передаче.

В некоторых случаях, например, при использовании VLAN (стандарт 802.1Q), в кадр добавляется 4-байтовый тег, увеличивая его размер.

1.79 MAC-адрес (48 бит/6 байт) — это уникальный идентификатор сетевого устройства, состоящий из двух частей: 24-битного OUI (код производителя, выданный IEEE) и 24-битного NIC (уникальный серийный номер устройства). Адрес обычно записывается в шестнадцатеричном формате, разделенном двоеточиями или дефисами (например, 00:1A:2B:3C:4D:5E).
Детальная структура MAC-адреса
OUI (Organizationally Unique Identifier) — первые 3 байта (24 бита):
- Идентификатор производителя сетевого оборудования.
- Регистрируется и выдается организацией IEEE.
NIC (Network Interface Controller) — последние 3 байта (24 бита):
Уникальный порядковый номер, назначаемый производителем для каждого конкретного устройства.
Особенности первого байта:
- В первом байте (самом левом) содержатся два важных служебных бита:
I/G (Individual/Group) — младший бит первого байта: если 0, то это обычный адрес устройства (Unicast); если 1, то это групповой адрес (Multicast/Broadcast).
- U/L (Universal/Local) — второй бит первого байта: если 0, адрес задан производителем глобально уникальным (Universal); если 1, адрес назначен локально (Local).
Форматы записи
MAC-адреса записываются в шестнадцатеричной системе счисления, где каждые 8 бит (1 байт) представлены двумя символами (0-9, A-F).
- Двоеточия: 00:1A:2B:3C:4D:5E (Linux/macOS).
- Дефисы: 00-1A-2B-3C-4D-5E (Windows).

- Точки: 001A.2B3C.4D5E (Cisco).
Всего существует
(примерно 281 триллион) возможных уникальных адресов.

1.80 MAC-адрес часто называется «встроенным» или «зашитым» адресом (burned-in address, BIA), поскольку исторически сложилось так, что он записывается в ПЗУ (постоянное запоминающее устройство) на сетевой плате. Это означает, что адрес вносится в чип ПЗУ на аппаратном уровне без возможности дальнейшего изменения.
Операционные системы и сетевые платы современных компьютеров поддерживают возможность изменения MAC-адреса с помощью программ. Это удобно при попытке получения доступа к сети, в которой используется фильтрация на основе BIA. Следовательно, фильтрация или отслеживание трафика на основе MAC-адреса более не является надежным способом.
При запуске компьютера сетевая плата сначала копирует MAC-адрес из ПЗУ в ОЗУ. Когда устройство пересылает сообщение в сеть Ethernet, оно добавляет к кадру информацию заголовка. Информация заголовка содержит MAC-адреса источника и назначения.
При поступлении кадра Ethernet на сетевую плату она проверяет MAC-адрес назначения, чтобы определить, совпадает ли он с физическим MAC-адресом устройства, сохраненным в ОЗУ. Если не удается обнаружить совпадения, устройство отклоняет кадр. При наличии совпадения сетевая плата передает кадр вверх по уровням модели OSI, где происходит процесс деинкапсуляции.
Сетевые платы устройств Ethernet принимают кадры также в том случае, если MAC-адрес назначения является широковещательной рассылкой или группой многоадресной рассылки, в которую включен узел.
Всем устройствам, которые могут быть узлами источника или назначения кадра Ethernet, необходимо присвоить MAC-адрес. К ним относятся рабочие станции, серверы, принтеры, мобильные устройства и маршрутизаторы.

1.81 Индивидуальный MAC-адрес (Media Access Control) — это уникальный 48-битный (6-байтовый) идентификатор, жестко прошитый производителем в сетевую карту Ethernet, используемый для адресации оборудования в локальной сети. Он выглядит как 12 шестнадцатеричных символов (напр., 00:1A:2B:3C:4D:5E), где первая половина — код производителя, а вторая — серийный номер.
Основные характеристики:
- Уникальность: Почти все устройства в мире имеют неповторимый MAC-адрес.
- Уровень OSI: Работает на канальном уровне (Layer 2) модели OSI.
- Назначение: Используется для доставки данных от отправителя к получателю внутри одной сети.
Как найти свой MAC-адрес в Windows:
Откройте командную строку (Win+R, введите cmd).
Введите ipconfig /all.
Найдите «Физический адрес» в разделе Ethernet-адаптера.
Примечание: MAC-адрес можно изменить программно (спуфинг), но его заводское значение остается неизменным в ПЗУ.

1.82 MAC-адрес широковещательной рассылки (broadcast) в сетях Ethernet — это специальный логический адрес FF-FF-FF-FF-FF-FF, состоящий из 48 единиц. Он используется для отправки кадров всем узлам локального сегмента сети (LAN). Получив такой кадр, все сетевые устройства обязаны его обработать, часто используется протоколами DHCP и ARP.
Основные характеристики:
- Формат: Шестнадцатеричное представление — FF:FF:FF:FF:FF:FF или FF-FF-FF-FF-FF-FF.
- Назначение: Доставка сообщений одновременно всем получателям в широковещательном домене.
- Особенность: Данный адрес не присваивается конкретному физическому устройству.
- Применение: Используется, когда отправитель не знает точный MAC-адрес получателя, например, при поиске IP-адреса через ARP-запрос.
Все устройства в одном домене широковещания, получив пакет с адресом назначения FF:FF:FF:FF:FF:FF, принимают его, в отличие от unicast-сообщений, предназначенных для одного конкретного получателя.

1.83 MAC-адрес многоадресной рассылки (multicast MAC) — это специальный адрес Ethernet (начинается с 01-00-5E для IPv4), используемый для передачи данных группе устройств, а не одному (unicast) или всем (broadcast). Он создается путем отображения нижних 23 бит IP-адреса мультикаст-группы на фиксированный префикс MAC-адреса.
Основные особенности multicast MAC:
Диапазон (IPv4): Многоадресные MAC-адреса соответствуют IPv4-адресам диапазона 224.0.0.0 – 239.255.255.255
Формат: Адрес имеет вид 01-00-5E-xx-xx-xx. Первые 25 бит фиксированы, а последние 23 бита формируются из младших 23 бит IP-адреса, который преобразуется из 4-го октета IP и части 3-го октета.
Применение: Используется для снижения нагрузки на сеть, позволяя коммутатору (через IGMP/MLD snooping) доставлять трафик только тем портам, которые запросили данные.
Пример:
Для IP-адреса 224.128.1.1:
Нижние 23 бита — 10000000.00000001.00000001 (128.1.1).
Результат — 01-00-5E-00-00-01 (старший бит в 25-м бите всегда 0).

1.84 Таблица коммутации (MAC-таблица или CAM-таблица) — это динамическая база данных в памяти коммутатора, связывающая MAC-адреса устройств с физическими портами. Она позволяет коммутатору направлять кадры только получателю, изучая адреса источников и храня их ограниченное время.
Структура таблицы коммутации (Пример)
Обычно таблица содержит следующие поля:
- VLAN ID: Виртуальная локальная сеть.
- MAC Address: Физический адрес устройства.
- Type: Тип записи (Dynamic — изучен автоматически, Static — настроен вручную).
- Ports: Номер физического порта, к которому подключено устройство.
Пример таблицы:

VLAN	MAC Address	Type	Ports
1	00:1A:2B:3C:4D:5E	Dynamic	Fa0/1
1	00:50:56:C0:00:08	Dynamic	Fa0/5
10	00:AA:BB:CC:DD:EE	Static	Gi0/1

1.85 Коммутатор 2-го уровня (L2) в Ethernet обеспечивает передачу кадров данных внутри одной локальной сети (LAN) на основе MAC-адресов. Ключевые задачи включают изучение и запоминание MAC-адресов, фильтрацию трафика, создание сегментов сети (доменов коллизий), поддержку VLAN, предотвращение петель (Spanning Tree) и повышение безопасности портов.
Основные функции и задачи коммутатора 2-го уровня:

- Коммутация по MAC-адресу: Коммутатор строит таблицу MAC-адресов, запоминая, на каком порту находится конкретное устройство, и направляет кадр только получателю, а не всем.
- Сегментация сети (домены коллизий): Устройство создает отдельные домены коллизий для каждого порта, что устраняет коллизии трафика и повышает производительность сети, в отличие от концентраторов.
- Виртуальные локальные сети (VLAN): Позволяет логически разделять физическую сеть на несколько независимых сегментов для улучшения безопасности и организации трафика.
- Обучение адресам: Автоматическое наполнение таблицы MAC-адресов при получении данных от подключенных устройств.
- Безопасность портов (Port Security): Ограничение доступа к порту на основе MAC-адреса, защита от сетевых атак (например, MAC-flooding).
- Предотвращение петель: Использование протоколов, таких как STP (Spanning Tree Protocol), для предотвращения широковещательных штормов в случае резервных связей.

L2-коммутаторы не выполняют маршрутизацию между разными IP-подсетями, работая исключительно с кадрами канального уровня.?

1.86 Коммутатор 2-го уровня (L2) самообучается, строя таблицу MAC-адресов (CAM-таблицу) на основе анализа источников входящих кадров. Когда устройство отправляет данные, коммутатор запоминает его MAC-адрес и привязывает к конкретному порту. Если адресат неизвестен, кадр рассылается на все порты (flooding), пока получатель не ответит и не внесет себя в таблицу.

1.87 Коммутатор 2-го уровня (L2) продвигает кадры, анализируя их MAC-адреса назначения и сопоставляя их с портами на основе динамически формируемой таблицы MAC-адресов (CAM-таблицы). Он работает исключительно внутри локальной сети, обеспечивая передачу данных только на нужный порт (unicast) или широковещательно (broadcast/unknown unicast), если адрес получателя неизвестен.

1.88 Коммутатор 2-го уровня (L2) фильтрует трафик, анализируя MAC-адреса источника и получателя в Ethernet-кадрах. Он строит таблицу MAC-адресов (CAM-таблицу) и пересылает данные только на соответствующий порт, блокируя их передачу на другие порты, тем самым изолируя трафик между устройствами.

1.89 Коммутаторы 2-го уровня (L2) используют три основных способа пересылки кадров: с промежуточным хранением (Store-and-Forward), обеспечивающий максимальную надежность; сквозную коммутацию (Cut-through), отличающуюся высо-

кой скоростью; и бесфрагментную коммутацию (Fragment-Free), представляющую собой гибрид, балансирующий между надежностью и скоростью.
Описание этих трех способов:
С промежуточным хранением (Store-and-Forward):

- Принцип: Коммутатор получает весь кадр целиком, сохраняет его в буфере, проверяет на отсутствие ошибок (CRC), проверяет MAC-адрес назначения и только потом отправляет в порт назначения.
- Плюсы: Высокая надежность, отбрасывание поврежденных кадров.
- Минусы: Самая высокая задержка, зависящая от длины кадра.

Сквозная коммутация (Cut-through):

- Принцип: Коммутатор считывает из кадра только первые несколько байт — адрес назначения — и сразу начинает его пересылку, не дожидаясь получения всего кадра и не проверяя его на ошибки.
- Плюсы: Минимальная задержка (скорость пересылки практически не зависит от длины кадра).
- Минусы: Пересылает поврежденные кадры.

Бесфрагментная коммутация (Fragment-Free / Hybrid):

- Принцип: Модификация сквозного метода. Коммутатор считывает первые 64 байта кадра (в которых обычно содержатся ошибки коллизий) перед пересылкой. Если кадр прошел проверку, он отправляется дальше.
- Плюсы: Быстрее метода store-and-forward и надежнее чистого cut-through.
- Минусы: Не проверяет ошибки на всем протяжении ка, в отличие от метода с промежуточным хранением.

1.90 Эта технология называется Auto-MDIX (Automatic Medium-Dependent Interface Crossover).
Она позволяет портам коммутатора автоматически определять тип подключенного кабеля (прямой или перекрестный) и подстраивать контакты для корректной передачи данных.
Как это работает:

- Детекция сигнала: Контроллер порта анализирует входящие сигналы на парах контактов.
- Переключение: Если устройство на другом конце «говорит» на тех же контактах, что и коммутатор пытается «слушать», контроллер виртуально меняет местами контакты передачи (Tx) и приема (Rx).
- Результат: Вам не нужно искать специальный кросс-кабель для соединения двух коммутаторов или прямой кабель для компьютера — всё работает «из коробки».

Для работы этой функции на обоих концах кабеля должно быть включено автосогласование (Auto-negotiation). Если на одном из портов скорость или дуплекс заданы вручную, Auto-MDIX может не сработать.

1.91 Преобразование IP-адресов пакета в MAC-адреса кадра выполняется протоколом ARP (Address Resolution Protocol). Он работает в локальных сетях (Ethernet), сопоставляя 32-битный IPv4-адрес с 48-битным физическим MAC-адресом получателя, чтобы обеспечить доставку данных на канальном уровне.

1.92 Основные принципы работы ARP:

- Таблица ARP (Кэш): Устройство сначала ищет соответствие в своей локальной таблице (ARP cache), где хранятся записи об IP и соответствующих им MAC-адресах.
- Широковещательный запрос: Если IP-адреса нет в таблице, компьютер рассылает по всей локальной сети ARP-запрос: «У кого IP-адрес X? Ответьте мне [MAC-адрес]».
- Ответ получателя: Узел с запрошенным IP-адресом отправляет прямой ответ (Unicast), содержащий его MAC-адрес, после чего эта пара добавляется в ARP-кэш отправителя.
- Маршрутизация: При отправке пакета за пределы локальной сети (в Интернет) ARP сопоставляет IP-адрес не целевого узла, а MAC-адрес шлюза по умолчанию (маршрутизатора).

Для IPv6 эту функцию выполняет протокол NDP (Neighbor Discovery Protocol).

1.93 Продвижение пакета между узлами в одной сети (локальной, LAN) основано на коммутации пакетов. Отправитель разбивает данные на пакеты, добавляет MAC-адрес получателя и передает их через коммутатор (switch), который изучает MAC-адреса и направляет кадры точно на нужный порт, обеспечивая независимую доставку данных.

1.94 Если IP-адрес назначения находится в удаленной сети, то MAC-адресом назначения является адрес шлюза узла по умолчанию, например, сетевой платы маршрутизатора. При получении маршрутизатором кадра Ethernet происходит деинкапсуляция информации уровня 2. На основе IP-адреса назначения маршрутизатор определяет следующее транзитное устройство и инкапсулирует IP-пакет в новый кадр для передачи в исходящий интерфейс. В каждом канале на своем пути IP-пакет инкапсулируется в кадре в зависимости от используемой технологии канала передачи данных, которая связана с этим каналом, например, технологии Ethernet. Если следующее транзитное устройство является назначением, то MAC-адресом назначения будет адрес сетевой платы Ethernet этого устройства.
Каким образом IPv4-адреса IPv4-пакетов в потоке данных ассоциируются с MAC-адресами в каждом канале на пути к узлу назначения? Для этого используется протокол разрешения адресов (ARP).

1.95 ARP-спуфинг (ARP-отравление) — это атака на локальную сеть (LAN), при которой злоумышленник отправляет ложные ARP-сообщения. Они связывают его физический MAC-адрес с IP-адресом легитимного узла (например, шлюза), позволяя перехватывать, модифицировать или блокировать трафик жертвы, действуя по принципу «человек посередине» (MITM).

Тема 1.5. Сетевой уровень

1.96 Сетевой уровень (L3) обеспечивает доставку данных между сетями, используя логическую адресацию (IP-адреса) и маршрутизацию. Он формирует пакеты из данных транспортного уровня, определяет оптимальный путь к получателю с помощью маршрутизаторов, управляет фрагментацией при необходимости и контролирует заторы.
Основные функции сетевого уровня при передаче данных:

- Логическая адресация: Присвоение и использование IP-адресов (IP-адрес источника и назначения) для уникальной идентификации устройств в различных сетях.
- Маршрутизация (Routing): Определение наиболее эффективного пути для доставки пакета от отправителя к получателю через цепочку маршрутизаторов.
- Формирование пакетов (Encapsulation): Прием сегментов от транспортного уровня и добавление к ним заголовков, содержащих IP-адреса, превращая их в пакеты (датаграммы).
- Перенаправление (Forwarding): Анализ IP-адреса назначения в заголовке и передача пакета на соответствующий интерфейс маршрутизатора.
- Фрагментация и сборка: Разделение больших пакетов на более мелкие фрагменты, если они не проходят через промежуточные сети, и последующая их сборка.
- Управление потоком и ошибками: Обработка сообщений об ошибках (например, с помощью протокола ICMP), если пакет не может быть доставлен.

На этом уровне работают такие протоколы, как IPv4, IPv6, ICMP, а основным устройством является маршрутизатор.

1.97 Протоколы сетевого уровня (Layer 3 по модели OSI) отвечают за логическую адресацию, маршрутизацию и доставку пакетов между сетями. Основными являются IPv4 и IPv6, поддерживаемые вспомогательными протоколами: ICMP (диагностика ошибок), IGMP (групповая передача) и IPsec (безопасность).
Протоколы маршрутизации (взаимодействуют на 3 уровне). Они обеспечивают обмен информацией между маршрутизаторами для выбора лучшего пути

1.98 Протокол IP (Internet Protocol) выполняет инкапсуляцию, упаковывая сегменты транспортного уровня (обычно TCP или UDP) в пакеты, добавляя к ним свой заголовок с IP-адресами источника и назначения. Этот процесс позволяет передавать данные через сети, формируя дейтаграммы, которые затем передаются на канальный уровень для дальнейшей упаковки в кадры.

1.99 Три основные характеристики протокола IP:

- Без установления соединения – перед отправкой пакетов данных соединение с получателем не установлено.
- Негарантированная доставка - IP-протокол считается ненадежным, так как доставка пакетов не гарантируется.
- Независимость от среды – Работа не зависит от средства подключения (медный, оптоволоконный

1.100 Заголовок IPv4-пакета (обычно 20–60 байт) содержит 14 полей, обеспечивающих маршрутизацию и доставку данных

Основные поля заголовка IPv4 и их назначение

1. Version (Версия) (4 бита): Указывает версию IP-протокола. Для IPv4 значение равно 4 (0100).
2. IHL (Internet Header Length — Длина заголовка) (4 бита): Длина заголовка в 32-битных словах. Минимальное значение 5 (20 байт).
3. Type of Service (ToS / DSCP — Тип обслуживания) (8 бит): Определяет приоритет пакета и требования к качеству обслуживания (QoS).

4. Total Length (Общая длина) (16 бит): Полная длина пакета (заголовок + данные) в байтах.
5. Identification (Идентификатор) (16 бит): Уникальный номер, используемый для переупорядочивания фрагментированных пакетов.
6. Flags (Флаги) (3 бита): Управляют фрагментацией (DF — не фрагментировать, MF — есть еще фрагменты).
7. Fragment Offset (Смещение фрагмента) (13 бит): Указывает позицию фрагмента в исходном пакете.
8. Time to Live (TTL — Время жизни) (8 бит): Ограничивает время жизни пакета, предотвращая зацикливание (уменьшается на 1 каждым маршрутизатором).
9. Protocol (Протокол) (8 бит): Определяет протокол верхнего уровня (TCP, UDP, ICMP).
10. Header Checksum (Контрольная сумма заголовка) (16 бит): Обеспечивает целостность заголовка.
11. Source Address (Адрес источника) (32 бита): IPv4-адрес отправителя.
12. Destination Address (Адрес назначения) (32 бита): IPv4-адрес получателя.
13. Options (Опции) (переменная длина): Необязательное поле для отладки, безопасности или маршрутизации.
14. Padding (Выравнивание): Заполняет заголовок нулями для достижения границы 32 бит, если используются Опции.

1.101 На протяжении многих лет протокол IPv4 периодически обновлялся для решения новых задач. Тем не менее даже в результате изменений IPv4 по-прежнему имеет три основных недостатка.

- Нехватка IP-адресов. IPv4 может предложить лишь ограниченное количество уникальных публичных IP-адресов. Несмотря на то что существует примерно 4 миллиарда IPv4-адресов, возросшее число новых устройств, в которых используется протокол IP, а также потенциальный рост менее развитых регионов привели к необходимости дополнительного увеличения количества адресов.
- Расширение таблицы интернет-маршрутизации. Таблица маршрутизации используется маршрутизаторами для определения оптимальных путей пересылки данных. По мере увеличения количества серверов (узлов), подключенных к Интернету, также растет число сетевых маршрутов. Эти маршруты IPv4 потребляют значительное количество памяти и ресурсов процессоров интернет-маршрутизаторов.
- Нехватка сквозных соединений. Преобразование сетевых адресов (NAT) представляет собой технологию, которая обычно применяется в сетях IPv4. NAT позволяет различным устройствам совместно использовать один публичный IPv4-адрес. При этом, поскольку публичный IPv4-адрес используется совместно, IPv4-адрес узла внутренней сети скрыт. Это может представлять проблему при использовании технологий, для которых необходимы сквозные соединения.

1.102 К улучшениям, которые предлагает протокол IPv6, относятся следующие.

- Расширенное адресное пространство. IPv6-адреса используют 128-битную иерархическую адресацию, в отличие от протокола IPv4, использующего 32 бита.
- Улучшенная обработка пакетов. Структура заголовка IPv6 была упрощена благодаря уменьшению количества полей.

- Отсутствие необходимости в использовании NAT. Благодаря большому количеству публичных IPv6-адресов нет необходимости в преобразовании сетевых адресов (NAT) между частными и публичными адресами IPv4. Это позволяет устранить некоторые проблемы, связанные с преобразованием сетевых адресов, которые возникают при работе приложений, требующих сквозного соединения.1.103 Охарактеризуйте инкапсуляцию IPv6.

1.104 Заголовок IPv6 имеет фиксированный размер 40 байт и включает 8 основных полей:

1. Version (Версия): 4 бита, содержащие значение 6 (0110), указывающее на использование протокола IPv6.
2. Traffic Class (Класс трафика): 8 бит, используемые для обеспечения качества обслуживания (QoS) и маркировки пакетов (аналог DSCP в IPv4).
3. Flow Label (Метка потока): 20 бит, идентифицируют последовательность пакетов, требующих одинаковой обработки маршрутизаторами (например, в реальном времени).
4. Payload Length (Длина полезной нагрузки): 16 бит, указывают размер данных (в октетах), следующих после заголовка, включая расширенные заголовки.
5. Next Header (Следующий заголовок): 8 бит, определяют тип заголовка, идущего сразу за основным (например, TCP, UDP или заголовок расширения).
6. Hop Limit (Предел перехода): 8 бит, аналог TTL в IPv4. Значение уменьшается на 1 каждым маршрутизатором; если достигает 0, пакет отбрасывается.
7. Source Address (Адрес отправителя): 128 бит, IPv6-адрес узла, отправившего пакет.
8. Destination Address (Адрес получателя): 128 бит, IPv6-адрес получателя.

В отличие от IPv4, в базовом заголовке IPv6 нет полей контрольной суммы, длины заголовка и информации о фрагментации (они перенесены в заголовки расширений).

1.105 Другим предназначением сетевого узла является пересылка пакетов между узлами. Узел может отправить пакет, на следующие адреса.

- Самому себе. Узел может отправить эхо-запрос на специальный IPv4-адрес, который представлен как 127.0.0.1 и называется интерфейсом loopback. Отправка эхо-запроса на интерфейс loopback тестирует стек протокола TCP/IP на узле.
- Локальный узел. Узел в той же локальной сети, в которой также находится отправляющий узел. Узлы используют один и тот же сетевой адрес.
- Удаленный узел. Узел в удаленной сети. Узлы не используют один и тот же сетевой адрес.

Какому узлу адресован пакет — локальному или удаленному — определяется комбинацией IPv4-адреса и маски подсети устройства источника (или отправляющего устройства), которые сравниваются с IPv4-адресом и маской подсети устройства назначения.

В домашней или корпоративной сети могут находиться несколько проводных и беспроводных устройств, соединенных друг с другом с помощью промежуточного устройства, такого как коммутатор локальной сети (LAN) и (или) точка беспроводного доступа (WAP). Это промежуточное устройство обеспечивает соединение между локальными узлами в локальной сети. Локальные узлы могут получать до-

ступ друг к другу и обмениваться информацией без использования каких-либо дополнительных устройств. Если узел отправляет пакет устройству, которое настроено в этой же IP-сети в качестве главного устройства, пакет просто пересылается из интерфейса узла через промежуточное устройство прямо на устройство назначения.
Разумеется, в большинстве случаев нам требуется, чтобы наши устройства могли устанавливать соединения за пределами сегмента локальной сети: подключаться к другим домам, офисам и Интернету. Устройства, которые не входят в сегмент локальной сети, называются удаленными узлами. Если исходное устройство отправляет пакет к удаленному устройству назначения, то в этом случае требуется помощь маршрутизаторов и выполнение маршрутизации. Маршрутизация — это процесс определения наилучшего пути к узлу назначения. Маршрутизатор, подключенный к сегменту локальной сети, называется шлюзом по умолчанию.

1.106 Маска подсети (subnet mask) — это инструмент, делящий IP-адрес на две части: адрес самой сети и адрес конкретного устройства (хоста) в ней. Она позволяет устройствам определять, находится ли получатель в локальной сети (прямая передача) или во внешней (через маршрутизатор), управляя трафиком и безопасностью. Основные функции маски сети:

- Идентификация границ сети: Маска показывает, какая часть IP-адреса фиксирована (сеть), а какая уникальна (устройство). Например, при маске 255.255.255.0 (или /24) у устройств 192.168.1.5 и 192.168.1.10 первые три числа — это общая сеть, а последнее — номер устройства.
- Маршрутизация (куда слать данные): Если компьютер видит, что IP-адрес получателя входит в его подсеть, он отправляет данные напрямую. В ином случае — передает на шлюз (роутер).
- Разделение на подсети: Позволяет эффективно использовать адресное пространство, разделяя одну крупную сеть на несколько небольших, например, для разных отделов компании.
- Определение размера сети: Маска определяет максимальное количество узлов (хостов) в сети.

1.107 Шлюз по умолчанию (default gateway) — это сетевое устройство (обычно роутер), которое перенаправляет пакеты данных из локальной сети в другие сети, включая интернет. Он служит "выходом" для трафика, когда получатель находится за пределами текущей подсети. Это ключевой узел, обеспечивающий доступ к внешним ресурсам.

- Функция: Если компьютер не знает конкретного пути к другому IP-адресу, он отправляет пакет на адрес шлюза по умолчанию.
- Где находится: Обычно это внутренний IP-адрес вашего домашнего роутера (например, 192.168.1.1 или 192.168.0.1).
- Применение: Необходим для доступа к сайтам, файлам и другим сетям, выходящим за рамки вашего локального устройства.
- Настройка: IP-адрес шлюза прописывается в настройках сети компьютера, либо получается автоматически через DHCP-сервер.

Если шлюз по умолчанию не задан или работает неверно, компьютер может работать в локальной сети, но не будет иметь доступа к интернету.

1.109 Таблица маршрутизации — это база данных (или файл), хранящаяся на маршрутизаторе или компьютере, которая содержит правила пересылки пакетов данных. Она определяет путь, по которому пакет должен идти до целевой сети, указывая IP-адрес назначения, шлюз и сетевой интерфейс, обеспечивая тем самым качественную доставку данных.

Основные составляющие таблицы маршрутизации:

- Сеть назначения (Destination): IP-адрес целевой подсети или конкретного узла.
- Маска сети (Netmask): Определяет размер подсети назначения.
- Шлюз (Gateway): IP-адрес следующего маршрутизатора («next hop»), на который нужно отправить пакет.
- Интерфейс (Interface): Локальный порт устройства (например, Ethernet0), через который будет отправлен пакет.
- Метрика (Metric): Числовой показатель, определяющий «вес» маршрута. Чем меньше метрика, тем предпочтительнее путь.
- Флаги (Flags): Показывают состояние маршрута (активен, статический, динамический и т.д.).

Как работает:

1. Когда маршрутизатор получает пакет, он смотрит на IP-адрес получателя.
2. Он сравнивает его с записями в таблице маршрутизации.
3. Маршрутизатор выбирает наиболее точный маршрут (с самой длинной маской), либо маршрут по умолчанию (default route).
4. Пакет отправляется через указанный интерфейс к следующему шлюзу.

1.110 В таблице маршрутизации маршрутизатора может храниться следующая информация.

- Маршруты с прямым подключением. Эти маршруты предоставляются активными интерфейсами маршрутизаторов. Маршрутизаторы добавляют маршрут с прямым подключением, когда интерфейс настроен с IP-адресом и активирован. Каждый из интерфейсов маршрутизатора подключен к разному сегменту сети.
- Удаленные маршруты. Эти маршруты предоставляются удаленными сетями, подключенными к другим маршрутизаторам. Маршруты к этим сетям могут быть настроены на локальном маршрутизаторе вручную сетевым администратором или назначены динамически с помощью локального маршрутизатора, который обменивается данными маршрутизации с другими маршрутизаторами, используя для этого протоколы динамической маршрутизации.
- Маршрут по умолчанию. Подобно узлу, маршрутизаторы также используют маршрут по умолчанию в качестве последнего средства, если иного маршрута до нужной сети в таблице маршрутизации нет.

1.111 Маршрутизатор обычно имеет несколько настроенных интерфейсов. В таблице маршрутизации хранится информация как о сетях с прямым подключением, так и об удаленных сетях.

На рисунке 16 показана попытка маршрутизатора R1 переслать пакет в сеть 10.1.1.0. Записи в таблице маршрутизации:

Рисунок 16 – Основные сведения об операциях удаленного маршрута

- Источник маршрута D – определяет, каким образом маршрутизатор получил сведения о сети. Общие источники маршрута включают в себя S (статический маршрут), D (улучшенный протокол маршрутизации между шлюзами – Enhanced Interior Gateway Protocol или EIGRP) и O (открытый протокол предпочтения кратчайшего пути – Open Shortest Path First). Другие источники маршрута в данной лекции не рассматриваются.
- Сеть назначения 10.1.1.0/24 – определяет сеть назначения.
- Административное расстояние 90 – определяет административное расстояние (достоверность) источника маршрута. Низкие значения означают высокую достоверность источника маршрута.
- Метрика 2170112 – указывает значение, заданное для достижения удаленной сети. Предпочтительные маршруты имеют низкое значение.
- Следующий переход 209.165.200.226 – определяет IP-адрес следующего маршрутизатора для пересылки пакета.
- Временная метка маршрута 00:00:05 –определяет последнюю активность маршрутизатора.
- Исходящий интерфейс Serial0/0/0 – определяет выходной интерфейс для его использования для передачи пакета к месту назначения.

1.112 Адрес следующего перехода (next-hop address) в компьютерных сетях — это IP-адрес ближайшего маршрутизатора или шлюза (следующего узла на пути), которому текущий маршрутизатор должен передать пакет данных, чтобы тот продвинулся ближе к получателю. Это ключевой элемент маршрутизации, определяющий эффективный путь передачи.

- Основные характеристики адреса следующего перехода:
- Определение пути: Маршрутизатор сверяет адрес назначения пакета со своей таблицей маршрутизации и находит соответствующий ему IP-адрес следующего прыжка (hop).
- Использование: Если сеть назначения не подключена напрямую, пакет отправляется на «следующий переход» (next-hop).

- Локальность: Это адрес устройства, находящегося в том же сегменте сети (канале связи), что и текущий маршрутизатор, но находящегося «дальше» на пути к цели.
- Маршрутизация по умолчанию: Если в таблице нет точного маршрута, используется адрес шлюза по умолчанию (default gateway).

При отсутствии прямого подключения к целевой сети, адрес следующего перехода позволяет пакету последовательно передаваться от одного маршрутизатора к другому.

1.113 Независимо от своих функций, размера или сложности все модели маршрутизаторов фактически представляют собой компьютеры. Как и компьютерам, планшетам и интеллектуальным устройствам, маршрутизаторам необходимы следующие компоненты:
Центральный процессор (ЦП).
Операционная система (ОС).
Память, которая включает оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ), энергонезависимое оперативное запоминающее устройство (NVRAM) и флеш-память.

1.114 В маршрутизаторе используется четыре типа памяти:

- ОЗУ. Это энергонезависимая память используется в маршрутизаторах Cisco для хранения приложений, процессов и данных, необходимых для их обработки центральным процессором. Маршрутизаторы Cisco используют быстрый тип ОЗУ, называемый синхронным динамическим ОЗУ (SDRAM). Нажмите изображение ОЗУ на рисунке, чтобы посмотреть дополнительную информацию.
- ПЗУ. Эта энергонезависимая память используется для хранения важных инструкций по эксплуатации и ограниченной версии IOS. Таким образом, ПЗУ — это встроенная в микросхему микропрограмма внутри маршрутизатора, которая может быть изменена только компанией Cisco. Нажмите изображение ПЗУ на рисунке, чтобы посмотреть дополнительную информацию.
- NVRAM. Эта энергонезависимая память используется как место постоянного хранения файла загрузочной конфигурации (startup-config).
- Флеш. Это энергонезависимая память компьютера, использующаяся в качестве места постоянного хранения IOS и других системных файлов, таких как файлы журналов, файлы голосовой конфигурации, HTML файлы, конфигурации резервного копирования и многое другое. При перезагрузке маршрутизатора IOS копируется из флеш-памяти в ОЗУ.

1.114 Как правило, маршрутизаторы и коммутаторы Cisco соединяют друг с другом множество устройств. Поэтому эти устройства имеют несколько типов портов и интерфейсов, которые используются для подключения кабелей к устройству. Например, на задней панели маршрутизатора Cisco 1941 находятся разъемы и порты, описанные на рисунке 17. Как и во многих других сетевых устройствах, в маршрутизаторах используются светодиоды, которые предоставляют информацию об их состоянии. Светодиодный индикатор обозначает активность соответствующего интерфейса. Если при активном правильно подключенном интерфейсе индикатор не горит, это может означать, что с этим интерфейсом возникла проблема.

Если интерфейс выполняет значительное количество операций, его индикатор горит постоянно.

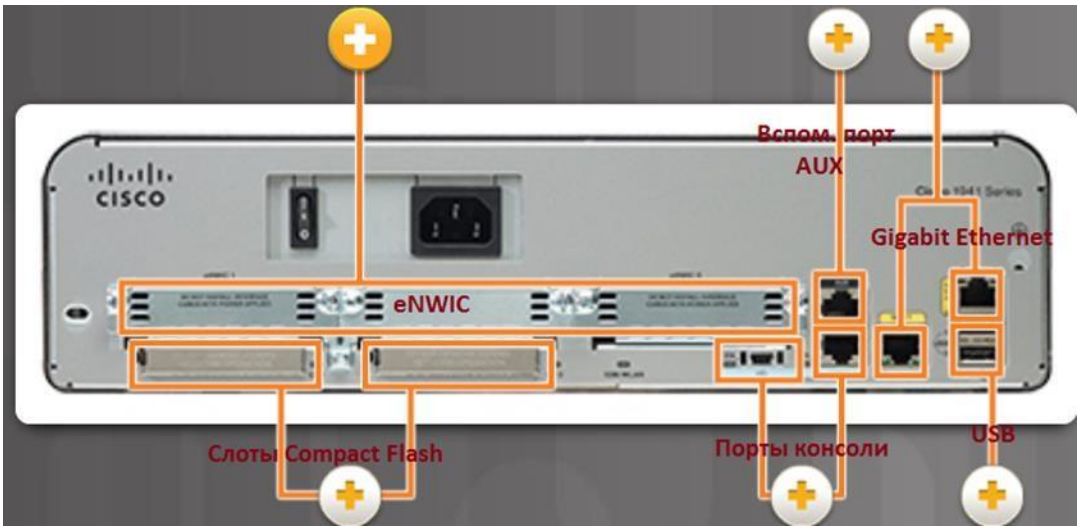


Рисунок 17 – Подключение к маршрутизатору

- Разъемы усовершенствованной интерфейсной платы для высокоскоростного WAN (eHWIC) – помечены как eHWIC 0 и eHWIC 1. Обеспечивают модульность и адаптивность маршрутизатора благодаря поддержке различных типов интерфейсных модулей, включая последовательный интерфейс, интерфейс цифровой абонентской линии DSL), коммутационный порт и беспроводное подключение.
- Слоты Compact Flash – помечены как CF0 и CF1. Могут быть использованы для установки флеш-памяти 4 Гб в каждый из них, что позволит увеличить объем запоминающего устройства. По умолчанию в разъем CF0 установлена карта Compact Flash 256 Мб, которая используется для загрузки системы.
- Порты консоли – предназначены для начальной настройки и административного доступа к интерфейсу командной строки (CLI). Как правило, используется два порта: стандартный порт RJ-45 и новый разъем USB типа B (mini-B USB). Однако доступ к консоли возможен только через один порт.
- Вспомогательный порт (AUX) – порт RJ-45 для удаленного административного доступа, аналогичен порту консоли. Сегодня он считается устаревшим портом, поскольку использовался для обеспечения поддержки коммутируемых модемов.
- Гигабитный Ethernet – интерфейсы, помеченные как GE0/0 и GE0/1. Обычно используются для обеспечения доступа к локальной сети (LAN) путем подключения к коммутаторам и пользователям, или для соединения с другим маршрутизатором.
- USB – порты, помеченные как USB 0 и USB 1, предназначены для предоставления дополнительного пространства хранения, аналогичного флеш-памяти.

1.115 Как и в случае с коммутатором, на маршрутизаторе существует несколько способов доступа к среде интерфейса командной строки (CLI) пользовательского режима EXEC. Ниже представлены наиболее распространенные из них.

- Консоль — это физический порт управления, обеспечивающий внеполосный доступ к устройству Cisco. Внеполосный доступ осуществляется через

выделенный административный канал, который используется исключительно в целях технического обслуживания устройства.

- Secure Shell (SSH) — метод, позволяющий удаленно установить защищенное подключение CLI через виртуальный интерфейс по сети. В отличие от консольного подключения для SSH-подключений на устройстве должны быть активны сетевые службы, включая активный интерфейс с настроенным адресом.
- Telnet — это незащищенный протокол, позволяющий удаленно начать сеанс CLI через виртуальный интерфейс по сети. В отличие от SSH, Telnet не обеспечивает защищенное зашифрованное соединение. Данные для аутентификации пользователя, пароли и команды передаются по сети в виде простого текста.

1.116 Подключения на маршрутизаторе можно разделить на две категории: внутриполосные интерфейсы маршрутизатора и порты управления.

Внутриполосные интерфейсы получают и пересылают IP-пакеты. Каждый настроенный и активный интерфейс на маршрутизаторе является участником или узлом в разной IP-сети. Для каждого интерфейса необходимо настроить IPv4-адрес и маску подсети другой сети. Операционная система IOS не допускает, чтобы два активных интерфейса на одном маршрутизаторе принадлежали одной и той же сети.

- Порты управления – включают консольные и AUX-порты, используемые для настройки маршрутизатора, его управления, и устранения возникающих в нем неполадок. В отличие от LAN- и WAN-интерфейсов, порты управления не используются для пересылки пакетов трафика пользователя.
- Внутриполосные интерфейсы маршрутизатора – это LAN-интерфейсы (например, Gigabit Ethernet) и WAN-интерфейсы (например, eHWIC), настроенные с помощью IP-адресации для передачи трафика пользователя. Интерфейсы Ethernet – это наиболее распространенные LAN-подключения, а наиболее распространенные WAN-подключения включают последовательный интерфейс и интерфейс цифровой абонентской линии (DSL).
- Последовательные WAN-интерфейсы – добавлены в слот eHWIC 0 и помечены строкой Serial 0 (например, S0/0/0) и Serial 1 (например, S0/0/1). Последовательные интерфейсы используются для подключения маршрутизаторов к внешним глобальным сетям (WAN). Каждый последовательный WAN-интерфейс имеет свой собственный IP-адрес и маску подсети, которые определяют его в качестве элемента определенной сети.
- Ethernet-интерфейсы локальной сети – помечены строкой GE 0/0 (например, G0/1). Интерфейсы Ethernet используются для подключения к другим устройствам с поддержкой Ethernet, включающим коммутаторы, маршрутизаторы, межсетевые экраны и т.д. Каждый LAN-интерфейс имеет свой собственный IP-адрес и маску подсети и/или IPv6-адрес и префикс, которые определяют его в качестве элемента определенной сети.

1.117 Процесс загрузки состоит из трех основных этапов.

1. Выполнение процедуры POST (самотестирование после включения питания) и загрузка программы начального запуска.

2. Поиск и загрузка программного обеспечения Cisco IOS.

3. Поиск и загрузка файла загрузочной конфигурации или переход в режим настройки.

Рассмотрим процесс загрузки маршрутизатора. Создается консольное подключение к маршрутизатору, например, с помощью программы Tera Term. Загрузка состоит из трех основных этапов.

- На первом этапе маршрутизатор проводит самотестирование при включении питания, запуская процедуру POST. Эта процедура, записанная в постоянной памяти, проверяет наличие аппаратных ошибок, в том числе в процессоре, в оперативной и энергонезависимой памяти. После завершения программы POST маршрутизатор запускает загрузчик (bootstrap). Загрузчик тоже хранится в ПЗУ. На этом первый этап завершается.
- Второй этап. Назначение загрузчика— поиск и загрузка программного обеспечения Cisco IOS. IOS — это операционная система Cisco для маршрутизатора. По умолчанию Cisco IOS хранится во флеш-памяти. Если файл образа IOS не найден во флеш-памяти и не загружен в ОЗУ, маршрутизатор попытается найти в сети TFTP-сервер и отыскать на нем другой образ IOS.
- Третий этап. После завершения загрузки IOS маршрутизатор загружает файл с настройками, который называется загрузочной конфигурацией (startup config). В нем записаны все настройки, сделанные на маршрутизаторе, включая имя хоста и IP-адреса интерфейсов. Этот файл конфигурации хранится в энергонезависимой памяти маршрутизатора. Если в энергонезависимой памяти нет файла конфигурации, маршрутизатор попытается найти в сети TFTP-сервер и отыскать на нем другой файл конфигурации. Если файл конфигурации не найден и на TFTP-сервере, маршрутизатор переходит в режим настройки (setup), то есть попросту запускает мастер первоначальной настройки.

1.118 Шаги базовой настройки коммутатора

Маршрутизаторы и коммутаторы Cisco во многом похожи. Они поддерживают похожие операционные системы, используют аналогичные командные структуры и множество идентичных команд. Кроме того, при внедрении этих устройств в сеть выполняются одинаковые настройки исходной конфигурации.

Задайте имя устройства

- hostname *имя*

Обеспечьте безопасность доступа к пользовательскому режиму EXEC

- line console 0
- password *пароль*
- login

Обеспечьте безопасность удаленного доступа по протоколу Telnet или SSH

- line vty 0 15
- password *пароль*
- login

Обеспечьте безопасность доступа к привилегированному режиму EXEC

- enable secret *пароль*

Обеспечьте безопасность всех паролей в файле config

- service password-encryption

Создайте баннер с правовым уведомлением

- banner motd *разделитель сообщение разделитель*

Настройте административный SVI

- interface vlan 1
- ip address *ip-адрес маска_подсети*
- no shutdown

Сохраните конфигурацию

- copy running-config startup-config

1.119 Шаги базовой настройки маршрутизатора
Как и для настройки коммутатора, для настройки исходных параметров маршрутизатора необходимо выполнить задания, указанные ниже.

- Задайте имя устройства
  - hostname *имя*
- Обеспечьте безопасность доступа к пользовательскому режиму EXEC
  - line console 0
  - password *пароль*
  - login
- Обеспечьте безопасность удаленного доступа по протоколу Telnet или SSH
  - line vty 0 15
  - password *пароль*
  - login
- Обеспечьте безопасность доступа к привилегированному режиму EXEC
  - enable secret *пароль*
- Обеспечьте безопасность всех паролей в файле config
  - service password-encryption
- Создайте баннер с правовым уведомлением
  - banner motd *разделитель сообщение разделитель*
- Сохраните конфигурацию
  - copy running-config startup-config

1.120 Для обеспечения доступности маршрутизаторов необходимо настроить его внутриполосные интерфейсы. На маршрутизаторах используется множество разных интерфейсов.

Настройте интерфейс
- interface *тип_и_номер*
- description *текст_описания*
- ip address *ipv4-адрес маска_подсети*
- no shutdown

1.121 Для проверки конфигурации интерфейса можно использовать несколько команд. Наиболее полезная из них — команда **show ip interface brief**. Полученная информация содержит все интерфейсы, их IPv4-адреса и текущее состояние. Активные и действующие интерфейсы представлены значением «up» в столбцах «Состояние» и «Протокол». Любые другие значения будут означать наличие проблемы либо с настройками, либо с подключением кабелей.

Подключение можно проверить с интерфейса с помощью команды **ping**. Маршрутизаторы Cisco отправляют пять последовательных эхо-запросов и определяют минимальное, среднее и максимальное время прохождения сигнала в прямом и обратном направлении. Восклицательные знаки подтверждают наличие подключения.
К дополнительным командам проверки интерфейса относятся следующие команды.

- **show ip route**— отображает содержимое таблицы маршрутизации IPv4, которая хранится в ОЗУ
- **show interfaces**— отображает статистические сведения по всем интерфейсам устройства
- **show ip interface**— отображает статистику IPv4 всех интерфейсов маршрутизатора.

1.122 Настройка шлюза по умолчанию (Default Gateway) на маршрутизаторе выполняется через веб-интерфейс в разделе сетевых настроек (WAN/Internet) или через CLI командой ip route 0.0.0.0 0.0.0.0 [IP_адрес_провайдера]. Обычно шлюз определяется автоматически от провайдера (DHCP), но при статической настройке вводится IP-адрес пограничного устройства.
Основные способы настройки шлюза:

- Веб-интерфейс (GUI):
  1. Войдите в панель управления маршрутизатором (обычно 192.168.0.1 или 192.168.1.1).
  2. Перейдите в раздел Сеть (Network) -> WAN или Интернет.
  3. Выберите тип подключения: Статический IP (Static IP).
  4. Введите IP-адрес, маску подсети и в поле Основной шлюз (Default Gateway) укажите адрес провайдера.
  5. Сохраните настройки.
- Интерфейс командной строки (CLI - например, Cisco):
- Используйте команду: ip default-gateway [IP-адрес].
- Или ip route 0.0.0.0 0.0.0.0 [IP-адрес].
- Автоматическая настройка:
- В разделе WAN выберите тип подключения Динамический IP (DHCP) — шлюз будет получен автоматически.

При наличии нескольких интерфейсов (WAN и резервный) можно настроить переключение на запасной шлюз в случае сбоя основного.

1.123 Шлюз по умолчанию (default gateway) на коммутаторе необходим для удаленного управления устройством (SSH, Telnet, SNMP) из других подсетей. Он указывает коммутатору, на какой IP-адрес маршрутизатора отправлять пакеты, предназначенные за пределы локальной сети. Без него коммутатор доступен только в
Зачем нужен шлюз по умолчанию

1. Удаленное управление: Позволяет администратору подключаться к коммутатору из другой сети.
2. Маршрутизация ответов: Если коммутатор получает запрос от удаленного узла, он использует шлюз, чтобы вернуть ответ.
3. Сетевые службы: Необходим для работы с серверами времени (NTP), системными журналами (Syslog) или серверами аутентификации (RADIUS/TACACS), находящимися за пределами локального сегмента L2.
   Настройка:
   Вход в режим конфигурации:
   configure terminal

Настройка шлюза:
ip default-gateway 192.168.1.1, где 192.168.1.1 - IP маршрутизатора
Сохранение конфигурации:
write memory

Тема 1.6. IP-адресация

1.124 Десятично-точечная запись IPv4-адреса — это удобный для чтения человеком формат представления 32-битного двоичного числа, состоящий из четырех десятичных чисел (октетов) от 0 до 255, разделенных точками (например, 192.168.0.1). Каждый октет представляет собой 8-битное значение, соответствующее 1 байту.
Ключевые характеристики:

- Структура: Четыре десятичных числа, разделенных тремя точками, формат: A.B.C.D
- Диапазон значений: Каждый октет принимает значения от 0 до 255 (2^8 = 256 возможных значений).
- Двоичное представление: в сумме составляют 32 бита (4*8 бит).
- Пример: 192.168.0.1 в двоичном виде выглядит как 11000000.10101000.00000000.00000001.

Эта система упрощает запоминание и использование IP-адресов людьми по сравнению с длинными цепочками из 32 нулей и единиц.

1.125 Быстрое преобразование октета (8 бит) основано на позиционных весах степеней двойки: 128, 64, 32, 16, 8, 4, 2, 1. Для перевода из двоичной в десятичную — сложите веса единиц. Для обратного перевода — последовательно вычитайте максимальную степень двойки из числа.
1. Двоичная -> Десятичная (Пример: 11010100)
Запишите веса над каждым битом и сложите те, где стоит 1:

- Бит: 1 1 0 1 0 1 0 0
- Вес: 128 64 32 16 8 4 2 1
- Расчет: 128 + 64 + 0 + 16 + 0 + 4 + 0 + 0 = 212

2. Десятичная -> Двоичная (Пример: 173)
Находите максимальную степень двойки, меньшую числа, и ставьте 1, затем вычитайте:
173 - 128 (2^7) = 45 (Бит: 1)
45 - 32 (2^5) = 13 (Бит: 101)
13 - 8 (2^3) = 5 (Бит: 10101)
5 - 4 (2^2) = 1 (Бит: 101011)
1 - 1 (2^0) = 0 (Бит: 10101101)
Результат: 10101101.
Совет: Выучите веса: 1, 2, 4, 8, 16, 32, 64, 128. Это ускорит вычисления в уме.

1.126 Pv4-адрес состоит из двух основных частей: номера сети (Network ID) и номера узла (Host ID). Сетевая часть определяет, к какой сети принадлежит устройство, а часть хоста идентифицирует конкретное устройство (компьютер, смартфон, принтер) внутри этой сети.

- Номер сети: Первые биты адреса, общие для всех устройств в данном сегменте сети

- Номер узла (хоста): Оставшиеся биты, уникальные для каждого устройства в этой сети
- Разделение: Граница между этими частями определяется не фиксировано, а с помощью маски подсети

Например, в адресе 192.168.0.3 с маской 255.255.255.0 часть 192.168.0 указывает на сеть, а .3 — на конкретное устройство в ней.

1.127 Маска подсети — это 32-битный шаблон (например, 255.255.255.0), который определяет, какая часть IP-адреса относится к адресу сети, а какая — к уникальному адресу устройства (хоста). Она позволяет компьютерам понимать, находится ли получатель в локальной сети или за её пределами, обеспечивая прямую связь или маршрутизацию через шлюз.

1.128 Префикс в IP-адресе — это часть адреса, определяющая конкретную сеть (подсеть), к которой принадлежит устройство, отделяя ее от адреса самого узла (хоста). Он обозначает количество общих старших бит для всех устройств в этой сети. Длина префикса изображается в нотации CIDR через косую черту («/») после IP-адреса, указывая число бит сети (например, 192.168.1.0/24).

1.129 Классовая IPv4-адресация — это устаревший метод разделения 32-битного адресного пространства на пять фиксированных классов (A, B, C, D, E) на основе первых битов адреса. Длина IPv4-адреса составляет 32 бита (4 байта), где классы
Основные характеристики классов (длина префикса):

- Класс A (0-127): Префикс сети — 8 бит (маска 255.0.0.0). Предназначен для очень больших сетей.
- Класс B (128-191): Префикс сети — 16 бит (маска 255.255.0.0). Для средних сетей.
- Класс C (192-223): Префикс сети — 24 бита (маска 255.255.255.0). Для небольших сетей.
- Класс D (224-239): Зарезервирован для многоадресной рассылки (multicast).
- Класс E (240-255): Зарезервирован для экспериментальных целей.

Этот метод оказался неэффективным из-за расточительного использования адресов и был заменен бесклассовой адресацией (CIDR).

1.130 Бесклассовая IPv4-адресация (CIDR — Classless Inter-Domain Routing) — это современный метод распределения IP-адресов, отменяющий жесткое деление на классы (A, B, C). Она использует маски подсетей переменной длины (VLSM), позволяя гибко выделять блоки адресов нужного размера, что значительно экономит ограниченный ресурс IPv4-адресов.

1.131 Технология VLSM (Variable Length Subnet Masks — маски подсети переменной длины) — это метод эффективного распределения IP-адресов, позволяющий разбивать одну сеть на подсети разных размеров в зависимости от потребностей, а не фиксированного числа хостов. Это предотвращает расточительство адресов, обеспечивая гибкость, масштабируемость и экономию IPv4-пространства.
Основные принципы VLSM:

- Гибкость маски: Для каждой подсети используется маска, соответствующая фактическому числу необходимых хостов (например, /24, /27, /30), а не одна фиксированная для всех.

- Иерархическое деление: Сеть можно разбивать на подсети, а затем эти подсети — на более мелкие подсети (подсети второго уровня).
- Экономия адресов: Применение VLSM позволяет использовать маски сетей вида /30 или /31 для линков между маршрутизаторами, сохраняя адреса для больших сетей.

Процесс применения VLSM:

1. Анализ требований: Определение необходимого количества хостов для каждой подсети.
2. Сортировка: Расположение подсетей в порядке убывания (от самой большой к самой маленькой).
3. Распределение: Назначение диапазонов, начиная с самого большого блока, чтобы избежать перекрытия.

Сравнение с FLSM:

- FLSM (Fixed Length Subnet Masks): Все подсети имеют одинаковый размер, что приводит к значительным потерям IP-адресов.
- VLSM: Каждая подсеть индивидуальна по размеру, что создает более плотную и эффективную структуру.

VLSM является критической техникой в современном проектировании сетей, обеспечивающей оптимальное использование доступного адресного пространства.

1.132 CIDR (Classless Inter-Domain Routing — бесклассовая междоменная маршрутизация) — это современный метод распределения IP-адресов и маршрутизации, заменяющий устаревшую классовую систему (A, B, C). Он позволяет гибко делить сеть на подсети любого размера, используя маски переменной длины (/0-32), что экономно расходует IPv4-адреса и сокращает таблицы маршрутизации.

Основные принципы и преимущества CIDR:

- Гибкая маска подсети: Вместо жестких 8, 16 или 24 бит, CIDR позволяет использовать любое количество бит для префикса сети.
- Запись через слэш (CIDR-нотация): Адрес записывается как IP-адрес/количество_бит_префикса. Например, 192.168.1.0/24 означает, что первые 24 бита — это адрес сети.
- Экономия адресов: Организации получают блоки адресов, соответствующие их реальным потребностям, а не фиксированные классы, что предотвращает расточительство.
- Агрегирование маршрутов (Supernetting): Позволяет объединить несколько мелких сетей в одну запись в таблице маршрутизации, что ускоряет работу маршрутизаторов.

CIDR избавляется от разделения на классы. При маршрутизации используется метод «самого длинного совпадения префикса», что позволяет точно определить путь к получателю.

1.133 Приватные (частные) IP-адреса используются для локальных сетей и не маршрутизируются в интернете. К ним относятся три основных диапазона, зарезервированных RFC 1918: 10.0.0.0—10.255.255.255 (класс A), 172.16.0.0—172.31.255.255 (класс B), 192.168.0.0—192.168.255.255 (класс C).

Основные диапазоны частных IP-адресов:

10.0.0.0 — 10.255.255.255 (маска /8, или 255.0.0.0).

172.16.0.0 — 172.31.255.255 (маска /12, или 255.240.0.0).

192.168.0.0 — 192.168.255.255 (маска /16, или 255.255.255.0).

Частные IP-адреса помогают экономить пространство IPv4-адресов, позволяя устройствам в локальной сети обмениваться данными без прямого выхода в интернет.

1.134 Дополнительные зарезервированные диапазоны:

- 100.64.0.0 — 100.127.255.255 (маска /10, или 255.0.0.0): Используется для CGN (Carrier-Grade NAT) провайдеров.
- 169.254.0.0 — 169.254.255.255 (маска /16, или 255.255.0.0): APIPA (Automatic Private IP Addressing), для автоматической настройки адресов в локальной сети.
- 127.0.0.0 — 127.255.255.255 (маска /8): Петлевой интерфейс (localhost) для обратной связи с самим устройством.

1.135 IP-адреса назначаются иерархической системой, возглавляемой корпорацией ICANN (Internet Corporation for Assigned Names and Numbers) и её подразделением IANA. IANA распределяет блоки адресов между пятью региональными интернет-регистраторами (RIR), которые затем передают их локальным провайдерам (ISP), назначающим IP-адреса конечным пользователям.
Основные уровни распределения IP-адресов:

- IANA / ICANN: Глобально управляют распределением IP-адресов (IPv4 и IPv6) и номеров автономных систем.
- Региональные интернет-регистраторы (RIRs): Пять организаций, отвечающих за свои географические зоны (например, RIPE NCC для Европы и России, ARIN для Северной Америки).
- Локальные интернет-регистраторы (LIR) / Интернет-провайдеры (ISP): Получают пулы адресов от RIR и назначают их конечным устройствам пользователей.
- Локальные маршрутизаторы (роутеры): Присваивают «серые» (внутренние) IP-адреса устройствам в локальной сети.

1.136 IPv6-адресация понадобилась, прежде всего, для преодоления критической нехватки уникальных адресов в протоколе IPv4 из-за взрывного роста интернета вещей (IoT), смартфонов и подключенных устройств. IPv6 обеспечивает практически неограниченное количество адресов (2^{128}), автоматическую настройку устройств, повышенную безопасность (IPSec) и ускоренную маршрутизацию.

1.137 Переход на IPv6 осуществляется тремя основными методами: двойной стек (Dual Stack) для одновременной работы протоколов, туннелирование (Tunneling) для передачи IPv6 через IPv4-сети и трансляция (NAT64/DNS64) для связи несовместимых сетей. Эти методы обеспечивают плавную миграцию, поддерживая работоспособность старой инфраструктуры.
Основные методы перехода на IPv6:

- Двойной стек (Dual Stack):
  - Характеристика: На сетевом оборудовании (маршрутизаторы, коммутаторы) и конечных узлах (ПК, серверы) одновременно функционируют оба протокола — IPv4 и IPv6.
  - Применение: Самый предпочтительный метод. Устройства сами выбирают, какой протокол использовать (приоритет обычно у IPv6).
- Туннелирование (Tunneling):

- Характеристика: Пакеты IPv6 упаковываются (инкапсулируются) в пакеты IPv4 для передачи через инфраструктуру, работающую только на IPv4.
- Применение: Используется для связности островков IPv6-сети через IPv4-интернет. Существуют автоматические и настроенные вручную туннели.

- Трансляция (NAT64/DNS64):
- Характеристика: Технология преобразования адресов, позволяющая устройствам, поддерживающим только IPv6, взаимодействовать с узлами, поддерживающими только IPv4, и наоборот.
- Применение: DNS64 преобразует имена в IPv6-адреса, а NAT64 осуществляет трансляцию заголовков пакетов, что критично на последних этапах отказа от IPv4.

Каждый из методов может использоваться отдельно или в комбинации в зависимости от готовности сети к полному переходу на IPv6.

1.138 Предпочтительный формат IPv6-адреса — это 8 групп по 4 шестнадцатеричные цифры, разделенные двоеточиями, где отображаются все символы, включая ведущие нули.
Пример: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

1.138 Пропуск начальных нулей в IPv6 — это правило сокращения записи, при котором ведущие нули в любой из восьми 16-битных групп (между двоеточиями) удаляются, оставляя значимые цифры. Например, 2001:0db8:0000:0000:0000:0000:1428:57ab превращается в 2001:db8:0:0:0:0:1428:57ab, сохраняя структуру, но экономя место.

1.139 Чтобы пропустить нулевые сегменты в IPv6-адресе, используйте двойное двоеточие (::), которое заменяет один или несколько последовательных блоков нулей. Это правило применяется только один раз в адресе, чтобы избежать неоднозначности. Также можно удалять ведущие нули внутри каждого 16-битного блока (гекстета).

1.140 Основные типы IPv6-адресов включают Unicast (одноадресная передача) для связи «один-к-одному», Multicast (многоадресная) для «один-ко-многим», и Anycast (выборочная) для доставки ближайшему узлу. В отличие от IPv4, IPv6 не использует широковещательные (broadcast) адреса, заменяя их групповыми рассылками.
Три основных типа IPv6-адресов:
- Unicast (Одноадресный): Идентифицирует конкретный интерфейс узла. Пакеты, отправленные на этот адрес, доставляются только этому интерфейсу. Включает глобальные (Global Unicast) и локальные (Link-local) адреса.
- Multicast (Многоадресный): Идентифицирует группу интерфейсов (обычно на разных узлах). Пакет, отправленный на такой адрес, доставляется всем членам группы. Начинаются с префикса FF00::/8.
- Anycast (Выборочный): Назначается группе интерфейсов (часто на разных устройствах), но пакет доставляется только одному, ближайшему интерфейсу в соответствии с метриками маршрутизации. Используется для балансировки нагрузки.

1.141 Длина префикса IPv6-адреса указывает количество бит, отведенных под сетевую часть, и обозначается числом после слеша (например, /64). В отличие от фиксированной структуры, длина префикса варьируется, но стандартом для подсетей

конечных узлов является 64 бита. Чаще всего используются префиксы /48 (для сайтов) и /64 (для локальных сетей).

- Общая длина IPv6-адреса: 128 бит.
- Типичный префикс подсети: /64 (первые 64 бита — сеть, последние 64 — идентификатор узла).
- Префикс маршрутизации: Может варьироваться (например, /32, /48, /56, /64).

Пример: в адресе 2001:db8:a::1/64 префикс — это 2001:db8:a::, а его длина — 64 бита.

1.142 Приватные (частные) адреса в IPv6, известные как Unique Local Addresses (ULA), предназначены для использования внутри локальных сетей (LAN) и не маршрутизируются в интернете. Они обеспечивают безопасность и автономность сети, аналогично частным диапазонам в IPv4, но используют префикс fd00::/8.

1.143 Локальные индивидуальные IPv6-адреса канала (Link-Local, диапазон FE80::/10) используются для связи между устройствами внутри одного сегмента сети (подсети) без участия маршрутизатора. Они назначаются автоматически, работают без DHCP, используются для обнаружения соседей (NDP), маршрутизации и настройки оборудования.

1.144 Глобальный индивидуальный IPv6-адрес (Global Unicast Address, GUA) состоит из 128 бит и делится на три основные части: 48-битный префикс маршрутизации (сеть), 16-битный идентификатор подсети и 64-битный идентификатор интерфейса (хост). Адреса обычно начинаются с диапазона 2000::/3.
Структура IPv6-адреса (128 бит)
Адрес делится на части следующим образом:

1. Префикс глобальной маршрутизации (Global Routing Prefix) — 48 бит:
- Назначается провайдером (ISP) или региональным регистратором.
- Используется для маршрутизации в интернете.
- Чаще всего имеет длину /48.
2. Идентификатор подсети (Subnet ID) — 16 бит:
- Используется внутри организации или дома для создания подсетей.
- Позволяет создать до 65 536 подсетей (при префиксе /48).
3. Идентификатор интерфейса (Interface ID) — 64 бита:
- Уникально идентифицирует устройство (хост) в подсети.
- Часто создается автоматически с использованием EUI-64 или случайных чисел.

Пример структуры

- Адрес: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- 2001:0db8:85a3 — Префикс маршрутизации (48 бит)
- 0000 — Идентификатор подсети (16 бит)
- 0000:8a2e:0370:7334 — Идентификатор интерфейса (64 бита)

Формат записи
IPv6 записывается как восемь групп по четыре шестнадцатеричные цифры, разделенные двоеточиями (:).

- Ведущие нули можно опускать: 2001:db8:0:0:0:0:0:1.
- Длинные последовательности нулей заменяются двойным двоеточием :: (только один раз в адресе): 2001:db8::1.

1.145 Префикс глобальной маршрутизации IPv6 (Global Unicast Address) обычно имеет длину /48 (48 бит). Он назначается интернет-регистраторами провайдерам, а затем корпоративным сетям или пользователям, обеспечивая маршрутизацию в интернете. Глобальные адреса начинаются с двоичных цифр 001 (диапазон 2000::/3).

- Структура /48: Первые 48 бит — префикс провайдера/сайта, следующие 16 бит — подсеть, последние 64 бита — идентификатор узла.
- Альтернативы: Часто конечным пользователям выделяется префикс /56 или /60, что позволяет им разбивать сеть на множество подсетей /64.

1.146 IPv6-адрес (128 бит) делится на две основные части: идентификатор подсети (обычно часть префикса, 64 бита) и идентификатор интерфейса (последние 64 бита). Подсеть определяет конкретную сеть (маршрутизацию), а идентификатор интерфейса уникально обозначает конкретное устройство (узел) внутри этой подсети.

1.147 Статическая настройка глобального уникального IPv6-адреса (GUA) включает ручное указание адреса, длины префикса (обычно /64) и шлюза по умолчанию в настройках сетевого интерфейса. На устройствах Cisco используется команда ipv6 address <адрес>/<префикс>, а в ОС (Windows/Linux) — сетевые параметры адаптера, отключая DHCPv6/SLAAC.

1.148 SLAAC (Stateless Address Autoconfiguration) — это механизм автоконфигурации IPv6-адресов, позволяющий устройствам самостоятельно генерировать уникальный глобальный адрес без участия центрального DHCPv6-сервера. Устройство получает от маршрутизатора префикс сети, добавляет к нему свой уникальный идентификатор (часто на основе MAC-адреса) и автоматически настраивает параметры сети.

1.149 Динамическая конфигурация DHCPv6 работает как централизованный механизм назначения IPv6-адресов и сетевых параметров, использующий четырехэтапный обмен сообщениями (Solicit-Advertise-Request-Reply) через мультикаст-адреса. В отличие от DHCPv4, клиент находит сервер через сообщения маршрутизатора (RA) и может работать в режиме с отслеживанием состояния (Stateful) для выдачи адресов или без него (Stateless) для получения настроек DNS.

1.150 Процесс EUI-64 (Extended Unique Identifier) автоматически создает 64-битный идентификатор интерфейса для адреса IPv6 на основе 48-битного MAC-адреса устройства. Он заключается в разделении MAC-адреса пополам, вставке между частями кода FFFE и инверсии 7-го бита (bit U/L), что позволяет устройству самостоятельно сформировать уникальный IP-адрес.

1.151 Динамические локальные адреса канала (Link-Local) создаются автоматически при включении сетевого интерфейса, начинаясь с префикса FE80::/10 (обычно FE80::/64 в IPv6). Они генерируются устройством самостоятельно (без DHCP-сервера) на основе MAC-адреса или случайного числа для связи только внутри одного канала (подсети).
Способы создания локальных адресов канала (Link-Local):

- Автоматическая генерация (IPv6): Устройство автоматически формирует адрес FE80::/64, используя метод EUI-64 (на основе MAC-адреса) или случайный идентификатор интерфейса.

- Проверка уникальности: Устройство проверяет сеть на наличие дубликатов (сообщение Neighbor Solicitation), гарантируя уникальность адреса внутри текущего канала.
- Ручная настройка (для фиксированных сред): В конфигурации интерфейса можно принудительно задать локальный адрес, например, ipv6 address fe80::1 link-local (на Cisco), что часто используется для шлюзов по умолчанию.

Локальные адреса канала, такие как FE80::1, не маршрутизируются в Интернет и действительны только в пределах одного канала связи.

1.152 Статические локальные адреса канала (link-local, IPv6: FE80::/10) создаются путем ручного назначения (конфигурирования) администратором через интерфейс устройства. В отличие от автоматического получения, статический адрес позволяет задать запоминающийся идентификатор интерфейса, например, FE80::1, который сохраняется после перезагрузки.

1.153 Проверка конфигурации IPv6 выполняется через командную строку (ip -6 addr в Linux, ipconfig в Windows) или настройки сети, где ищется адрес с двоеточиями (например, 2a00:...), отличный от локального fe80::. Для проверки работоспособности используют пинг (ping -6 google.com) или специализированные сайты.

1.154 Групповые IPv6-адреса (multicast) начинаются с префикса FF00::/8 и используются для отправки пакетов группе узлов, заменяя широковещание IPv4. Основные предопределенные адреса: FF02::1 (все узлы в канале) и FF02::2 (все маршрутизаторы в канале). Структура адреса: FF<Флаги><Scope>::<Группа>.

1.155 ICMPv4 и ICMPv6 служат для диагностики и обмена сообщениями об ошибках в сетях IP, но ICMPv6 является неотъемлемой частью IPv6, функционально превосходя ICMPv4. Главные отличия: ICMPv6 включает протокол поиска соседей (NDP) для автонастройки (SLAAC) и заменяет ARP, использует новые типы сообщений и обязателен для функционирования IPv6-сетей.
Ключевые сравнения сообщений ICMPv4 и ICMPv6:

- Функциональность: ICMPv4 используется в основном для диагностики (ping, traceroute) и уведомления об ошибках. ICMPv6 помимо этого берет на себя функции ARP (определение адресов) и управление группами (IGMP) в IPv6.
- Поиск соседей (NDP): В ICMPv6 добавлены сообщения Neighbor Solicitation/Advertisement и Router Solicitation/Advertisement, заменяющие ARP и обеспечивающие обнаружение маршрутизаторов.
- Автонастройка адресов (SLAAC): ICMPv6 позволяет устройствам автоматически получать IPv6-адреса, что отсутствует в ICMPv4.
- Типы сообщений: Основные сообщения (эхо-запрос/ответ) похожи, но в ICMPv6 добавлены новые типы для поддержки NDP и специфики IPv6.
- Интеграция: ICMPv6 обязателен для реализации IPv6, тогда как ICMPv4 формально является дополнительным, хотя и необходимым протоколом.

ICMPv6 предоставляет более эффективную и расширяемую структуру для современных сетей по сравнению с ICMPv4.

1.156 Команда ping — это инструмент командной строки для проверки сетевого соединения с конкретным узлом (сайтом или IP-адресом). Она отправляет пакеты данных (ICMP) и измеряет время ответа. Используется для диагностики доступности серверов и качества связи.
Базовая команда: ping google.com или ping 8.8.8.8.
Остановка: Нажмите Ctrl+C в окне терминала.

Тема 1.7. Разделение IP-сетей на подсети

1.157 Домен широковещательной рассылки (broadcast domain) — это логический участок компьютерной сети, в котором все устройства получают широковещательные кадры (сообщения), отправленные любым узлом, без участия маршрутизатора. Границами таких доменов являются сетевые устройства третьего уровня (маршрутизаторы) или VLAN.

1.158 Крупные широковещательные домены (broadcast domains) вызывают снижение производительности сети из-за высокой нагрузки на устройства, обрабатывающие лишний трафик (ARP, DHCP), увеличивают риск возникновения «широковещательных штормов». Это приводит к медленной работе сети, частым сбоям, а также увеличивает риски безопасности, так как вредоносный трафик распространяется шире.
Основные проблемы крупных широковещательных доменов:

- Высокая загрузка ЦП узлов: Все устройства в домене обязаны принять, обработать и подтвердить каждый широковещательный пакет, что снижает их производительность.
- Снижение пропускной способности сети: Огромный объем фонового мусорного трафика занимает полосу пропускания, оставляя меньше места для полезных данных.
- Широковещательные штормы: При сбое в работе одного узла или зацикливании коммутации, широковещательные пакеты могут бесконечно множиться, полностью парализуя сеть.
- Проблемы с Wi-Fi: Большое количество широковещательных запросов «убивает» беспроводную сеть, так как Wi-Fi по своей природе является разделяемой средой, и отправка широковещания заставляет все устройства ожидать передачи.
- Низкая безопасность: Чем больше домен, тем больше устройств получают подозрительные пакеты, что упрощает сетевые атаки.

Для решения этих проблем применяют сегментацию сети с помощью виртуальных локальных сетей (VLAN) или маршрутизаторов, которые ограничивают распространение широковещательных пакетов.

1.159 Разделение сети на подсети (subnetting) необходимо для повышения производительности, безопасности и управляемости, предотвращая перегрузку широковещательными запросами. Это позволяет изолировать трафик разных отделов, эффективно распределять IP-адреса и ограничивать доступ к конфиденциальным узлам.
Основные причины для разделения:

- Уменьшение широковещательного шторма (Broadcast Traffic): Разбиение сети на мелкие подсети ограничивает распространение широковещательного

трафика (ARP, запросы Windows), что предотвращает замедление работы всей сети.

- Повышение безопасности (Безопасность): Разделение позволяет изолировать критически важные сегменты (например, серверы или бухгалтерию) от остальных пользователей, повышая защищенность данных.
- Эффективное управление IP-адресами: Позволяет рациональнее использовать адресное пространство, выделяя подсети необходимого размера, что особенно важно при ограниченном количестве публичных IP-адресов.
- Улучшение производительности: Снижение нагрузки на сетевые устройства за счет сегментации трафика.
- Организационная структура: Позволяет логически организовать устройства по географическому признаку (например, этаж, офис) или функциональному назначению.

Разделение обычно реализуется с помощью маршрутизаторов или VLAN на коммутаторах.

1.160 Разделение сети на границе октетов (/8, /16, /24) — это самый простой способ сабнетинга, при котором меняется только один октет маски (255.0.0.0, 255.255.0.0, 255.255.255.0). Достаточно заимствовать биты из хостовой части, изменяя значения маски (например, с /24 на /25 или /26), чтобы увеличить число сетей за счет уменьшения количества узлов в них.

1.161 Разделение на подсети с бесклассовой адресацией (CIDR/VLSM) выполняется путем заимствования бит у хостовой части адреса для создания новых сетей, что позволяет гибко использовать IP-пространство. Процесс включает определение количества необходимых хостов, выбор новой маски подсети (например, /26, /27) и расчет границ сетей (адрес сети, диапазон хостов, широковещательный адрес) для каждой подсети

1.162 Маска подсети — это 32-битное число (например, 255.255.255.0), которое делит IP-адрес на две части: адрес сети и адрес узла (хоста). Она используется устройствами для определения того, находится ли другой компьютер в их локальной сети (прямая передача) или во внешней (передача через маршрутизатор). Это необходимо для маршрутизации трафика и безопасности.

1.163 Выполните разделение на подсети с бесклассовой адресацией предложенной сети.

1.164 VLSM (Variable Length Subnet Mask, маска подсети переменной длины) — это метод разделения IP-сети на подсети разного размера, оптимизирующий использование адресного пространства. В отличие от фиксированной маски (FLSM), VLSM позволяет выделять подсети точно под требуемое количество хостов, сокращая трату адресов.

1.165 CIDR (Classless Inter-Domain Routing — бесклассовая междоменная маршрутизация) — это современный метод распределения IP-адресов, пришедший на смену жесткой классовой системе (A, B, C). Он позволяет гибко назначать маски подсетей переменной длины (VLSM), выделяя сети точно под требуемое количество хостов, что значительно экономит дефицитное пространство IPv4.

1.166 Разделение IPv6-сети (субнетизация) основано на использовании префикса длиной /64 для конечных устройств, что дает 2^{64} адресов на подсеть. Организациям обычно выделяется префикс /48, позволяющий создать 65 536 подсетей (до /64), меняя 4-ю шестнадцатеричную группу (16 бит). Это упрощает маршрутизацию, управление трафиком и безопасностью в отличие от сложного деления в IPv4.

Тема 1.8. Транспортный уровень

1.167 Транспортный уровень (4-й уровень модели OSI) обеспечивает надежную или быструю передачу данных между приложениями на разных узлах сети, выполняя сегментацию данных, контроль потока, исправление ошибок и мультиплексирование портов. Он связывает сетевую инфраструктуру с прикладным уровнем, гарантируя доставку сообщений (TCP) или обеспечивая минимальные задержки (UDP). Транспортный уровень действует как посредник, отделяя прикладные процессы от технических особенностей физической передачи данных в сети.

1.168 Основные функции транспортного уровня:

- Сегментация и сборка: Разбиение больших объемов данных от верхних уровней на более мелкие сегменты перед отправкой и сборка их в исходный поток на стороне получателя
- Связь между приложениями (Порты): Использование номеров портов для идентификации конкретных программ (например, веб-браузер, почтовый клиент) на устройствах-отправителях и получателях, что позволяет мультиплексировать данные
- Надежная доставка (TCP): Протокол Transmission Control Protocol устанавливает соединение, нумерует пакеты, подтверждает их получение, гарантируя доставку без ошибок, потерь и дубликатов в нужном порядке.
- Быстрая доставка (UDP): Протокол User Datagram Protocol обеспечивает передачу данных с минимальными задержками, что критично для видеозвонков и онлайн-игр, не гарантируя доставку каждого пакета.
- Управление потоком: Регулирование скорости передачи данных между отправителем и получателем для предотвращения переполнения буфера приемника.

1.169 Основные отличия TCP и UDP:

- Надежность: TCP гарантирует доставку, переотправляя потерянные пакеты. UDP отправляет пакеты без проверки их получения.
- Установление соединения: TCP требует «рукопожатия» (handshake) перед передачей данных, UDP — нет.
- Скорость: UDP работает значительно быстрее из-за отсутствия задержек на подтверждения и проверки.
- Порядок данных: TCP упорядочивает пакеты, UDP может доставлять их в хаотичном порядке.
- Потоковая передача: TCP передает данные как непрерывный поток, UDP — отдельными дейтаграммами.

Таблица сравнения:

Характеристика	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Надежность	Высокая (гарантирует доставку)	Низкая (не гарантирует)

Скорость	Ниже (из-за подтверждений)	Высокая (быстрая передача)
Соединение	С установлением соединения	Без установления соединения
Порядок	Гарантирован	Не гарантирован
Заголовок	Тяжелый (20-60 байт)	Легкий (8 байт)
Применение	Браузеры (HTTP/HTTPS), Email (SMTP), FTP	Стриминг видео, VoIP, игры, DNS

Когда использовать:

- TCP: Когда критична целостность данных (файлы, почта).
- UDP: Когда критична скорость и допустима потеря пакетов (стриминг, игры).

1.170 Мультиплексирование с помощью номеров портов — это процесс объединения данных от нескольких приложений в один сетевой поток на транспортном уровне (TCP/UDP). Каждый пакет получает заголовок с портом источника и назначения, что позволяет сетевому стеку однозначно распределять входящий трафик между запущенными программами.

Как работает процесс:

- Мультиплексирование (отправка): Операционная система присваивает каждому исходящему запросу от приложения (браузер, почта) уникальный временный номер порта отправителя. Все эти данные собираются в один поток.
- Идентификация: в заголовке TCP/UDP-пакета указываются:
  - Порт источника: Уникальный номер приложения-отправителя.
  - Порт назначения: Порт, по которому приложение-получатель ждет данные (например, 80 для HTTP).
- Демультиплексирование (прием): На принимающем устройстве модуль TCP анализирует номер порта назначения в заголовке и направляет данные именно тому прикладному процессу, который их запросил.

Это позволяет одному IP-адресу одновременно работать с сотнями сетевых служб, эффективно разделяя трафик.

1.171 Надежность сеанса в TCP обеспечивается через гарантированную доставку: каждый байт нумеруется, получатель отправляет подтверждения (ACK), а при потере сегмента он переотправляется.

1.172 Упорядоченная доставка пакетов осуществляется преимущественно протоколом TCP (Transmission Control Protocol), который разбивает данные на части, присваивает каждой уникальный порядковый номер, а получатель переупорядочивает их на основе этих номеров. Этот механизм гарантирует сборку сообщения в исходном порядке, даже если пакеты пришли быстрее, медленнее или по разным маршрутам.

Основные этапы упорядоченной доставки:

- Сегментация и нумерация: Данные разбиваются на части, в заголовке каждого пакета прописывается порядковый номер, указывающий его место в исходном сообщении.
- Маршрутизация: Пакеты отправляются по сети, где они могут идти разными путями, из-за чего могут приходить к получателю в неверном порядке.
- Буферизация и переупорядочивание: Получатель (TCP-стек) помещает полученные пакеты в буфер и на основе номеров расставляет их в правильной последовательности.
- Подтверждение приема (ACK): Получатель отправляет отправителю подтверждение приема с номером следующего ожидаемого пакета. Если пакеты пришли не по порядку, получатель может задержать их выдачу приложению, пока не придут недостающие элементы.

Этот процесс обеспечивает надежную передачу данных, предотвращая потерю, дублирование или неправильную сборку данных.

1.173 Управление потоком с помощью окна (скользящего окна) — это механизм, при котором получатель сообщает отправителю объем данных (размер окна), который он готов принять, не дожидаясь подтверждения. Отправитель отправляет пакеты только в пределах этого окна, сдвигая его по мере получения подтверждений (ACK). Это предотвращает переполнение буфера получателя.
Основные принципы работы:

- Окно отправителя: Определяет, сколько кадров/байтов можно отправить без получения подтверждения.
- Окно получателя: Указывает на объем свободного места в буфере, готового к приему данных.
- Сдвиг окна: При получении ACK на кадр, нижняя граница окна сдвигается вправо, открывая возможность отправки новых данных.
- Закрытие окна: Если буфер получателя заполнен, он посылает размер окна 0, и отправитель останавливает передачу, пока окно снова не "откроется".
- Гибкость: Размер окна может меняться динамически в зависимости от скорости обработки данных получателем.

Этот метод используется в протоколе TCP для обеспечения надежности и адаптации скорости передачи к возможностям сети.

1.174 Установка TCP-соединения выполняется через «трехстороннее рукопожатие» (SYN, SYN-ACK, ACK) для синхронизации порядковых номеров. Разрыв соединения происходит через «четырехэтапное прощание» (FIN-ACK с обеих сторон), что обеспечивает полную двустороннюю передачу данных и надежное закрытие. Также возможно принудительное завершение сбросом (RST).
Установка соединения (Three-Way Handshake)

1. SYN (Synchronize): Клиент отправляет серверу пакет с установленным флагом SYN, сообщая свой начальный порядковый номер (Sequence Number).
2. SYN-ACK (Synchronize-Acknowledgment): Сервер получает SYN, отправляет в ответ SYN-ACK. Он подтверждает получение (ACK) порядкового номера клиента и сообщает свой.
3. ACK (Acknowledgment): Клиент получает SYN-ACK и отправляет финальный ACK, подтверждая порядковый номер сервера.

Соединение установлено.
Разрыв соединения (Four-Way Wave)
Поскольку TCP-соединение полнодуплексное (данные идут в обе стороны независимо), каждая сторона закрывает его отдельно:

1. FIN (Finish) / ACK: Инициатор отправляет флаг FIN, сообщая, что больше не будет передавать данные.
2. ACK: Получатель подтверждает FIN, закрывая поток данных в одну сторону.
3. FIN / ACK: Вторая сторона отправляет свой флаг FIN, завершая отправку данных со своей стороны.
4. ACK: Инициатор подтверждает финальный FIN, соединение закрывается окончательно.

Принудительный разрыв (RST)

Если возникают ошибки или соединение невозможно, используется флаг RST (Reset). Он немедленно прекращает соединение, не дожидаясь закрытия потоков.

1.175 Заголовок протокола TCP (Transmission Control Protocol) имеет фиксированную длину в 20 байт (без учета дополнительных опций) и содержит следующие поля:

Основные поля заголовка

- Порт источника (Source Port) — 16 бит: Номер порта отправителя.
- Порт назначения (Destination Port) — 16 бит: Номер порта получателя.
- Порядковый номер (Sequence Number) — 32 бита: Номер первого байта данных в текущем сегменте. Если установлен флаг SYN, это начальный порядковый номер (ISN).
- Номер подтверждения (Acknowledgment Number) — 32 бита: Номер следующего байта, который отправитель ожидает получить. Поле действительно, только если установлен флаг ACK.
- Смещение данных (Data Offset / Header Length) — 4 бита: Длина заголовка в 32-битных словах. Показывает, где начинаются данные.
- Зарезервировано (Reserved) — 3–6 бит (в зависимости от использования флагов): Зарезервировано для будущего использования, должно быть равно нулю.
- Управляющие флаги (Flags / Control Bits) — 9 бит: Служат для управления сессией (URG, ACK, PSH, RST, SYN, FIN, а также ECE, CWR, NS).
- Размер окна (Window Size) — 16 бит: Количество байт, которое отправитель готов принять от партнера без подтверждения.
- Контрольная сумма (Checksum) — 16 бит: Используется для проверки целостности заголовка и данных.
- Указатель важности (Urgent Pointer) — 16 бит: Показывает смещение относительно порядкового номера, где заканчиваются «срочные» данные (используется с флагом URG).

Дополнительные поля

- Опции (Options) — переменная длина: Дополнительные параметры, такие как максимальный размер сегмента (MSS), масштабирование окна или временные метки.
- Заполнитель (Padding) — переменная длина: Используется для того, чтобы размер заголовка был кратен 32 битам.

1.176 Заголовок UDP (User Datagram Protocol) состоит всего из 4 полей, общим размером 8 байт (по 2 байта или 16 бит на каждое поле), что обеспечивает низкую задержку при передаче данных.

Поля заголовка UDP:

1. Порт источника (Source Port) (16 бит) — идентифицирует порт отправителя, используется для обратной связи.
2. Порт назначения (Destination Port) (16 бит) — указывает порт получателя, на который доставляется дейтаграмма.
3. Длина (Length) (16 бит) — общая длина UDP-заголовка и данных (в байтах), минимум 8 байт.
4. Контрольная сумма (Checksum) (16 бит) — используется для проверки целостности данных; обязательна в IPv6, но необязательна в IPv4.

Каждое поле играет важную роль в обеспечении быстрой передачи пакетов без необходимости установления соединения.

1.177 Номера портов — это числовые идентификаторы (от 0 до 65535), используемые в протоколах TCP/IP (TCP, UDP) для определения конкретного приложения или службы, которой предназначен сетевой пакет на определенном хосте. Они работают как «двери» или «номера квартир» в доме, роль которого выполняет IP-адрес, позволяя различать службы (например, 80 для HTTP).

1.178 Основные сведения о номерах портов:

- Диапазон: Номер порта — целое число от 0 до 65535 ($2^{16} – 1$).
- Типы портов:
  - Системные (0–1023): Зарезервированы для известных протоколов (например, FTP-21, SSH-22, HTTP-80, HTTPS-443).
  - Зарегистрированные (1024–49151): Используются конкретными приложениями, например, базами данных или играми.
  - Динамические/Частные (49152–65535): Присваиваются системой временно для исходящих соединений.
- Назначение: Порт позволяет компьютеру понять, какому именно процессу (программе) передать полученные данные, даже если используется один IP-адрес.
- Разделение: Порты TCP не пересекаются с портами UDP, то есть порт 1234 для TCP — это не то же самое, что порт 1234 для UDP.

При передаче данных по сети используется сокет - пара: IP-адрес (адрес устройства) + номер порта (адрес службы внутри устройства).

1.179 Пара сокетов (socket pair) представляет собой двусторонний канал связи между двумя конечными точками (процессами), где данные, записанные в один сокет, мгновенно становятся доступными для чтения из другого. Обычно это пара «клиент-сервер» (IP-адрес + порт), обеспечивающая надежный обмен данными (TCP) или быструю передачу (UDP), при этом пара может работать и локально без сети.

Принцип работы пары сокетов:

- Создание и связывание: Программы создают сокеты (функция socket()), после чего сервер «привязывает» его к порту (bind()), а клиент явно подключается (connect()) или пара создается системным вызовом socketpair() (для локальных процессов).
- Установление соединения: Сервер ожидает подключений (listen(), accept()), а клиент инициирует соединение. После рукопожатия образуется устойчивый канал передачи данных между двумя точками.
- Обмен данными: После подключения приложения используют функции send()/write() для передачи и recv()/read() для получения данных.
- Завершение: По окончании работы оба сокета закрываются функцией close().
- Специфика (Self-pipe trick): Локальная пара сокетов (UNIX-сокеты) используется для межпроцессного взаимодействия или для того, чтобы разбудить блокированный цикл событий (epoll_wait), записывая байт в один сокет и считывая из другого.

Пара сокетов работает как двусторонняя труба, соединяющая конкретные процессы, где ОС гарантирует доставку данных.

1.180 Команда netstat (network statistics) — это консольная утилита для мониторинга сетевых подключений (входящих/исходящих), таблиц маршрутизации, статисти-

ки интерфейсов и открытых портов. Она работает в Windows, Linux и macOS, показывая состояние TCP/UDP сокетов в реальном времени, помогая диагностировать неполадки сети и аудит безопасности.
Основные функции и принципы работы:

- Активные соединения: Отображает, какие программы подключены к сети, их IP-адреса и порты.
- Слушаемые порты: Показывает порты, ожидающие входящих подключений (состояние LISTENING).
- Статистика протоколов: Выводит данные по протоколам TCP, UDP, ICMP, IP.
- Таблица маршрутизации: Показывает маршруты пакетов в системе (netstat -r).

Популярные примеры использования:

- netstat -a — отобразить все активные подключения и порты.
- netstat -n — отобразить IP-адреса и номера портов в числовом формате (работает быстрее).
- netstat -b (Windows) / netstat -p (Linux) — показать, какой процесс (PID) использует порт.
- netstat -an | find "LISTENING" (Windows) — найти все открытые порты.
- netstat -rn — показать таблицу маршрутизации.

Команда особенно полезна для выявления программ, которые «занимают» сетевые порты, или для анализа подозрительной сетевой активности.

1.181 Сборка датаграмм UDP выполняется на транспортном уровне: данные приложения разбиваются на пакеты, к каждому добавляется 8-байтовый заголовок (порты, длина, контрольная сумма), после чего они отправляются как отдельные сущности. UDP не гарантирует порядок доставки; если данные разбиты на уровне приложения, их сборка и упорядочивание — задача самого приложения, а не протокола.
Основные аспекты формирования и сборки UDP-датаграмм:

- Структура датаграммы: UDP-пакет состоит из заголовка (порт отправителя/получателя, длина, контрольная сумма) и данных (данные пользователя).
- Отсутствие сборки в UDP: В отличие от TCP, протокол UDP не упорядочивает пакеты и не собирает их из фрагментов. Если пакеты пришли не по порядку, приложение получает их в том же порядке.
- Роль контрольной суммы: Для проверки целостности данных вычисляется контрольная сумма, которая включает заголовок и данные, позволяя определить, были ли они изменены при передаче.
- Фрагментация IP: Если UDP-датаграмма слишком велика для сети (больше MTU), IP-уровень фрагментирует её. Сборка таких фрагментов выполняется IP-уровнем получателя, а не UDP, и при потере одного фрагмента весь пакет отбрасывается.
- Сборка на уровне приложений: Если приложение использует большой объем данных, оно должно само разбить их на пакеты, добавить порядковые номера и собрать их на приемной стороне.

Таким образом, UDP — это протокол «отправил и забыл», где сборка «сообщения» из нескольких датаграмм возлагается на приложение.

1.182 Протокол TCP — это отличный пример того, как различные уровни набора протоколов TCP/IP могут выполнять определенные роли. TCP сам выполняет все задачи, связанные с разбиением потока данных на сегменты, обеспечением надежности их передачи, управлением потоком и переупорядочением сегментов. TCP освобождает приложение от необходимости брать на себя управление любой из этих задач. Приложения, подобные тем, которые показаны на рисунке 18, могут просто отправить поток данных протоколу транспортного уровня и использовать сервисы TCP.

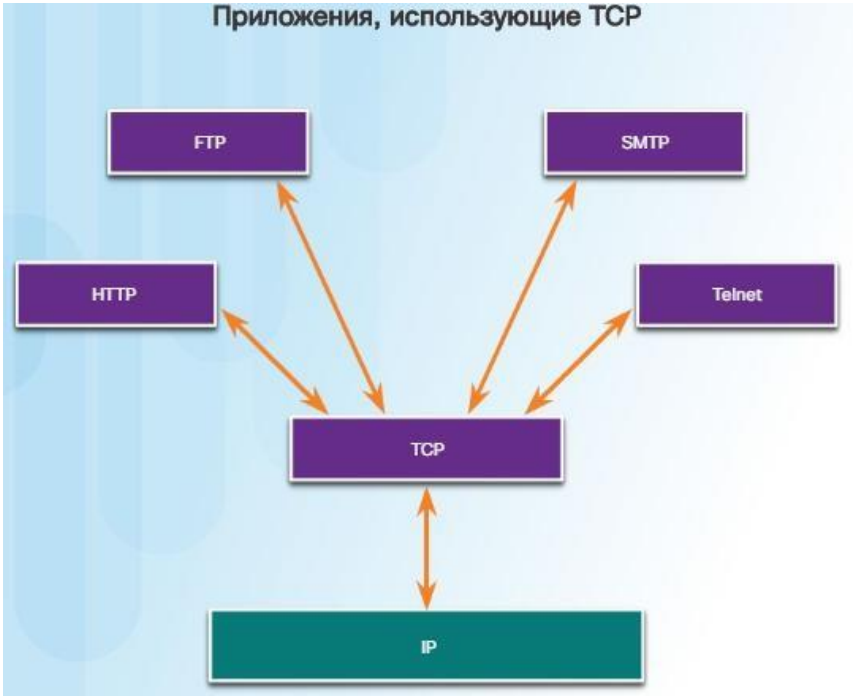


Рисунок 18 – Приложения, использующие TCP

1.183 Существуют три типа приложений, которые лучше всего подходят для работы с протоколом UDP, смотри рисунок 19:
Приложения для передачи аудио в режиме реального времени и мультимедийные приложения — такие приложения допускают потерю некоторых данных, однако для них важна низкая задержка или полное ее отсутствие Примерами могут служить VoIP и потоковое видео.
Приложения, осуществляющие лишь транзакции по отправке запросов и получению ответов, — когда узел отправляет запрос и неизвестно, поступит ответ или нет. В качестве примера можно указать DNS и DHCP.
Приложения, самостоятельно обеспечивающие надежность передачи данных, — ненаправленный обмен данными, при котором управление потоком, обнаружение ошибок, отправка подтверждений и восстановление после сбоев не требуются или выполняются самим приложением (например, SNMP и TFTP).
И хотя DNS и SNMP по умолчанию используют протокол UDP, они также могут использовать и TCP. DNS использует протокол TCP в случае, когда размер DNS-запроса или DNS-ответа превышает 512 байт (например, когда в DNS-ответе содержится большое количество разрешений имен). Аналогичным образом при определенных обстоятельствах администратор сети может настроить SNMP на использование протокола TCP.

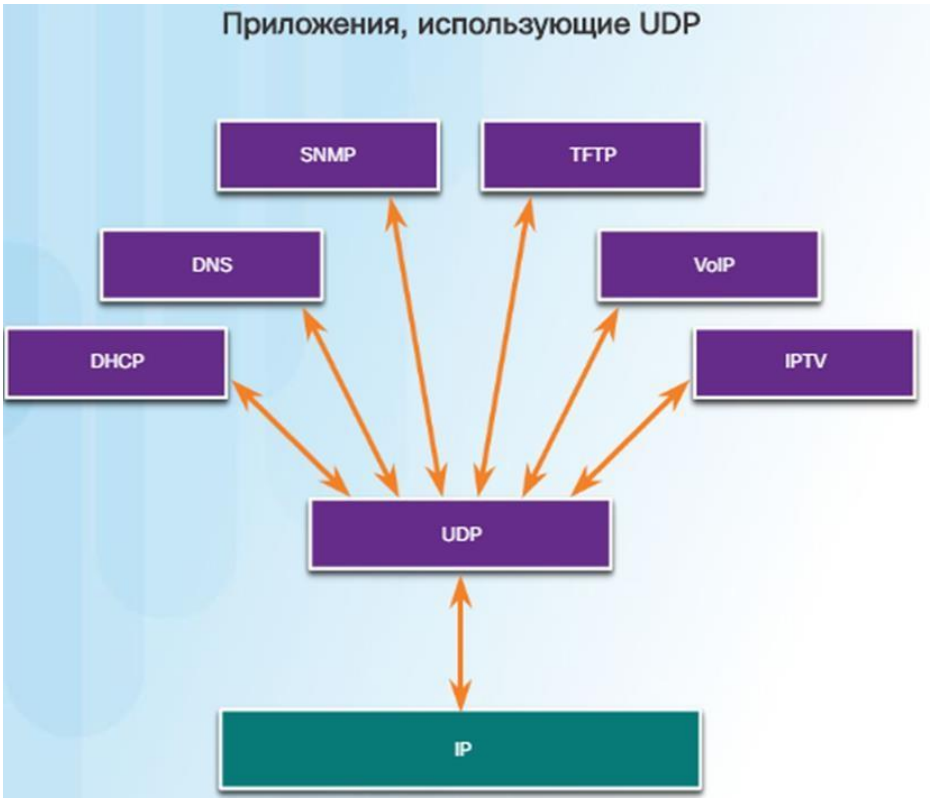


Рисунок 19 – Приложения, использующие UDP

Тема 1.9. Уровень приложений

1.184 Уровень приложений (Application Layer) стека TCP/IP объединяет три верхних уровня модели OSI: прикладной (7-й), представительский (6-й) и сеансовый (5-й). Он обеспечивает работу сетевых приложений, управление сессиями, форматирование, сжатие и шифрование данных.
7. Прикладной (Application): HTTP, FTP, SMTP, DNS.
6. Представления (Presentation): Кодирование, сжатие, шифрование (например, SSL/TLS).
5. Сеансовый (Session): Управление диалогом, создание и завершение сессий.
В отличие от 7-уровневой модели OSI, стек TCP/IP возлагает логику сеансов и представления данных непосредственно на сами приложения.

1.185 Протоколы прикладного уровня (уровня приложений) обеспечивают взаимодействие между пользовательским программным обеспечением (браузеры, почтовые клиенты) и сетью. Основные примеры включают HTTP/HTTPS (веб-страницы), FTP (файлы), SMTP/IMAP/POP3 (почта), DNS (доменные имена) и SSH (удаленное управление). Они работают поверх транспортных протоколов TCP/UDP.

1.186 Уровень представлений (6-й) и сеансовый уровень (5-й) в модели OSI обеспечивают подготовку, безопасность и управление соединением данных перед их передачей. Уровень представления кодирует, сжимает и шифрует данные (переводчик), а сеансовый уровень устанавливает, поддерживает и завершает диалог между узлами, обеспечивая синхронизацию.
Уровень представлений (Presentation Layer, 6-й уровень)

Этот уровень отвечает за то, чтобы данные, отправленные прикладным уровнем (7-й) одного устройства, были понятны прикладному уровню другого.
Основные функции:

- Преобразование данных (Кодирование): Перевод форматов данных (например, ASCII в EBCDIC), конвертация кодировок (UTF-8, Unicode) и стандартизация форматов файлов.
- Сжатие данных: Уменьшение объема данных для ускорения передачи (например, алгоритмы ZIP, JPEG, MPEG).
- Шифрование: Обеспечение конфиденциальности данных (например, шифрование SSL/TLS перед отправкой).

Примеры: Стандарты файлов GIF, TIFF, JPEG (изображения), ASCII, EBCDIC (текст), форматы видео (MPEG, QuickTime).
Сеансовый уровень (Session Layer, 5-й уровень)
Сеансовый уровень управляет процессом взаимодействия между приложениями — «диалогом», отвечая за начало, поддержание и завершение сессии.
Основные функции:

- Установление и завершение сеанса: Инициализация диалога между отправителем и получателем, а также его корректное закрытие.
- Поддержание сессии: Контроль за активностью соединения в течение длительного времени.
- Синхронизация: Вставка контрольных точек (checkpoints) в поток данных. Если происходит обрыв, передача возобновляется с последней точки, а не с начала.
- Управление диалогом: Определение того, кто отправляет данные, а кто принимает (дуплексный или полудуплексный режим).

Примеры: Протоколы SQL, RPC (Remote Procedure Call), NetBIOS, протоколы синхронизации данных.
Взаимодействие (Пример с мессенджером)

1. Приложение (7) формирует текст.
2. Уровень представления (6) шифрует текст и конвертирует его в нужный формат.
3. Сеансовый уровень (5) проверяет, открыто ли соединение с сервером Telegram, и поддерживает его.
4. Данные передаются на транспортный уровень (4).

1.187 Модель «клиент-сервер» — это сетевая архитектура, где задачи распределены между отправителями запросов (клиентами) и поставщиками услуг (серверами). Клиент (например, браузер) инициирует запрос, а сервер (удаленный компьютер) обрабатывает его, обращается к базе данных и возвращает ответ. Это основа работы интернета, веб-приложений и корпоративных сетей.
Основные компоненты:

- Клиент (активная сторона): Рабочая станция, приложение (браузер, мобильное приложение), которое запрашивает данные или действия.
- Сервер (пассивная сторона): Мощный компьютер или программа, ожидающая запросов, обрабатывающая их и предоставляющая ресурсы.
- Сеть: Среда передачи запросов и ответов между клиентом и сервером.

Принцип работы (пошагово):

1. Запрос: Пользователь (клиент) делает действие (например, нажимает «Войти» на сайте).

2. Передача: Запрос отправляется по сети на сервер.
3. Обработка: Сервер получает запрос, проверяет данные (например, пароль в БД), выполняет необходимые вычисления.
4. Ответ: Сервер отправляет обратно результат: запрошенную страницу, данные или подтверждение ошибки.

Преимущества:

- Централизованное хранение данных на сервере упрощает их обновление и защиту.
- Клиентские устройства (смартфоны, ноутбуки) не требуют высокой мощности, так как основные вычисления делает сервер.
- Возможность подключения множества клиентов к одному серверу.

Пример: Когда вы открываете сайт, ваш браузер (клиент) посылает запрос на сервер сайта, который в ответ присылает файлы страницы, и браузер их отображает.

1.188 Одноранговая сеть (P2P или peer-to-peer) — это децентрализованная сеть, в которой каждый компьютер (узел или пир) равноправен и выполняет функции как клиента, так и сервера. Участники напрямую обмениваются файлами, данными или ресурсами без использования центрального сервера. Это обеспечивает высокую отказоустойчивость, масштабируемость и отсутствие единой точки отказа, так как данные хранятся распределенно на машинах пользователей.

1.189 Ключевые принципы работы:

- Равноправие узлов: Нет главного компьютера-сервера. Каждый участник может как запрашивать данные (клиент), так и отдавать их (сервер).
- Прямой обмен: Файлы передаются напрямую от пользователя к пользователю, часто разбиваясь на фрагменты для ускорения загрузки.
- Распределенное хранение: Данные хранятся не в одном месте, а на жестких дисках участников, что делает сеть устойчивой к отключению отдельных узлов.
- Децентрализация: Если один компьютер выйдет из строя, сеть продолжит функционировать, так как другие узлы возьмут на себя его функции. 1.190 Перечислите наиболее распространенные P2P приложения.

Преимущества: Высокая скорость при большом количестве пользователей, надежность (устойчивость к кибератакам), отсутствие цензуры.

Недостатки: Сложность управления, потенциально более низкая безопасность, зависимость от активности других участников.

1.191 HTTP — это протокол прикладного уровня, обеспечивающий обмен данными (запрос-ответ) между браузером и сервером. HTML — это язык разметки, определяющий структуру и контент веб-страницы, которую браузер интерпретирует и отображает. HTTP доставляет HTML-код, а браузер превращает его в визуальную страницу.

Как работает HTTP (протокол передачи гипертекста):

- Клиент-сервер: Браузер (клиент) отправляет запрос к серверу, сервер возвращает ответ (данные или ошибку).
- Запрос (Request): Содержит метод (GET — получить, POST — отправить), адрес ресурса (URL) и заголовки.
- Ответ (Response): Содержит статус-код (например, 200 OK или 404 Not Found) и тело ответа (обычно HTML, CSS, картинки).

- Без сохранения состояния: HTTP не запоминает предыдущие запросы, поэтому используются куки (cookies) для сессий.

Как работает HTML (язык разметки гипертекста):

- Теги: HTML использует теги (например, <h1>, <p>, <a>) для структурирования контента.
- Структура: Документ делится на заголовок (<head> с метаданными) и тело (<body> с видимым контентом).
- Гиперссылки: Позволяют связывать документы между собой (атрибут href в теге <a>).
- Отображение: Браузер читает HTML-код и рисует страницу, интерпретируя теги как заголовки, абзацы, изображения и таблицы.

Вместе они составляют основу веб-серфинга: браузер запрашивает файл по HTTP, а сервер отправляет HTML-файл, который браузер отображает пользователю.

1.192 HTTP (HyperText Transfer Protocol) — открытый протокол для передачи данных, а HTTPS (HTTP Secure) — его защищенная версия, использующая шифрование SSL/TLS. Главное отличие: HTTPS гарантирует конфиденциальность и целостность данных, предотвращая перехват паролей и карт, тогда как HTTP передает информацию в открытом виде. HTTPS требует SSL-сертификата и работает через порт 443, а HTTP — через 80.

1.193 Протоколы электронной почты (SMTP, IMAP, POP3) — это набор правил, определяющих, как письма создаются, отправляются, хранятся и получаются. SMTP отвечает за отправку писем от клиента на сервер и между серверами, а IMAP и POP3 — за получение и загрузку писем пользователем.

1.194 Протокол POP (Post Office Protocol, обычно используется версия POP3) — это почтовый протокол прикладного уровня, предназначенный для получения электронной почты. Его принцип работы заключается в подключении к серверу, загрузке всех писем на локальное устройство пользователя и последующем их удалении с сервера (по умолчанию), что идеально подходит для использования на одном компьютере.

1.195 DNS (Domain Name System) — это иерархическая распределенная система, преобразующая понятные человеку доменные имена (например, google.com) в цифровые IP-адреса (142.250.179.174), необходимые для связи компьютеров в сети. Она работает как телефонная книга, где DNS-резолверы по цепочке опрашивают серверы для поиска нужного адреса и кэшируют результаты.

Основные этапы функционирования DNS:

1. Запрос: Пользователь вводит адрес. Браузер и ОС сначала проверяют локальный кэш (файл hosts, кэш браузера).
2. Рекурсивный резолвер (провайдер): Если адрес не найден, запрос отправляется к DNS-серверу провайдера. Он действует как посредник.
3. Корневой сервер (Root Server): Резолвер спрашивает корневой сервер, который знает, где находятся серверы для зон верхнего уровня (TLD, например, .com или .ru).
4. TLD-сервер: Сервер зоны (например, .com) перенаправляет на авторитетный DNS-сервер, который управляет конкретным доменом (например, example.com).

5. Авторитетный сервер (Authoritative DNS Server): Этот сервер содержит точные IP-адреса и возвращает искомый IP-адрес резолверу.
6. Кэширование и ответ: Резолвер запоминает (кэширует) ответ на время (TTL), чтобы не искать его снова, и отдает IP-адрес браузеру, который загружает сайт.

1.196 Иерархия DNS (Domain Name System) — это древовидная структура, преобразующая человекочитаемые имена сайтов (например, google.com) в IP-адреса, понятные компьютерам. Она строится от корневого домена (точка в конце) вниз к доменам верхнего уровня (TLD, например, .com), доменам второго уровня (например, google) и поддоменам.

Основные уровни иерархии DNS (сверху вниз):

- Корневой сервер DNS (Root Server): Вершина иерархии (обозначается точкой.). Существует 13 основных комплексов корневых серверов (дублированных по всему миру), которые не знают точного IP, но перенаправляют запрос к нужному TLD-серверу.
- Сервер домена верхнего уровня (TLD Server): Обслуживают зоны верхнего уровня: общего назначения (.com, .net, .org) или национальные (.ru, .ua, .uk).
- Авторитетный сервер DNS (Authoritative Name Server): Последний уровень в поиске. Содержит точные записи (A, AAAA, CNAME) для конкретного домена (example.com) и возвращает финальный IP-адрес.
- Рекурсивный резолвер (Recursive Resolver): Обычно предоставляется провайдером. Он принимает запрос от браузера и проходит всю цепочку (корень -> TLD -> авторитетный) для поиска IP-адреса, кэшируя результат для ускорения.

Как работает иерархия (на примере запроса ya.ru):

1. Браузер запрашивает IP у резолвера.
2. Резолвер идет к корневому серверу: "Где .ru?"
3. Корневой сервер: "Иди к серверу TLD .ru".
4. Резолвер идет к TLD-серверу .ru: "Где ya.ru?"
5. TLD-сервер: "Иди к авторитетному серверу ya.ru".
6. Резолвер идет к авторитетному серверу: "Какой IP у ya.ru?"
7. Авторитетный сервер отдает IP, который получает пользователь.

Такая система обеспечивает высокую надежность, скорость работы за счет кэширования и независимость управления разными уровнями доменов.

1.197 Nslookup (Name Server Lookup) — это консольная утилита для диагностики DNS, которая отправляет запросы к DNS-серверам для получения информации о доменных именах, IP-адресах и типах записей (A, MX, NS, TXT). Она позволяет проверить работоспособность DNS-сервера, выявить неверные записи и продиагностировать сетевые проблемы, работая как в интерактивном, так и в прямом режиме.

Как работает nslookup:

1. Отправка запроса: Пользователь вводит команду nslookup example.com. Утилита берет доменное имя и формирует запрос.
2. Обращение к DNS-серверу: Запрос отправляется на локальный DNS-сервер (обычно провайдера) или на указанный сервер (через @server).
3. Поиск в DNS-зоне: DNS-сервер ищет информацию в своей базе (или кэше) и возвращает IP-адрес или требуемую запись (MX, NS и т.д.).

4. Отображение результата: nslookup выводит ответ в консоль: сервер, ответивший на запрос, и найденные записи (обычно A-записи — IP-адреса).

Основные режимы использования:

- Прямой запрос (однократный): nslookup ya.ru — показывает IP-адрес домена.
- Интерактивный режим: Ввод nslookup без параметров открывает приглашение >, где можно менять параметры (например, тип записи).
- Смена сервера: nslookup ya.ru 8.8.8.8 — запрос информации у конкретного сервера (в данном случае Google).

Что можно узнать (типы запросов):

С помощью set type=... (в интерактивном режиме) можно искать конкретные данные:

- A/AAAA: IP-адрес (v4/v6) хоста.
- MX: Почтовые сервера домена.
- NS: Серверы имен, отвечающие за домен.
- TXT: Текстовые записи (часто для SPF/DKIM).
- PTR: Обратный поиск (имя хоста по IP).

Nslookup помогает убедиться, что DNS-сервер возвращает верные данные, и диагностировать проблемы, если сайт не открывается из-за кэширования старых записей.

1.198 Протокол DHCP (Dynamic Host Configuration Protocol) нужен для того, чтобы устройства в сети могли получать настройки подключения (IP-адрес и другие параметры) автоматически, без ручного вмешательства

1.199 FTP (File Transfer Protocol) — это надежный протокол TCP, использующий два порта (21 для команд, 20 для данных) для интерактивной передачи файлов, требующий аутентификации. TFTP (Trivial FTP) — упрощенный протокол UDP, работающий без паролей и структуры каталогов, используемый для быстрой передачи небольших файлов (загрузка ОС, конфигураций) в локальных сетях.

Работа протокола FTP (File Transfer Protocol):

Два соединения: FTP устанавливает постоянное управляющее соединение (порт 21) для передачи команд и временное соединение данных (порт 20 или динамический) для файлов.

- Аутентификация: Требует логин и пароль (или анонимный доступ).
- Функциональность: Позволяет просматривать каталоги, удалять, переименовывать и передавать файлы.
- Надежность: Работает поверх TCP, гарантируя доставку пакетов.

Работа протокола TFTP (Trivial File Transfer Protocol):

- UDP-протокол: Работает поверх UDP, не гарантирует доставку, что делает его быстрее, но менее надежным.
- Простота: Нет аутентификации (логинов/паролей), не поддерживает просмотр каталогов.
- Ограничения: Передает файлы поблочно (обычно 512 байт), ожидая подтверждения (ACK) на каждый блок.
- Область применения: Чаще всего используется в локальных сетях для загрузки прошивок на сетевое оборудование, загрузки бездисковых станций.

Основные отличия:

- FTP: Надежный, сложный, для интернет-обмена, с аутентификацией.

- TFTP: Быстрый, простой, для локальной сети, без аутентификации.

1.200 Протокол SMB (Server Message Block) — это сетевой протокол прикладного уровня, используемый для предоставления удаленного доступа к файлам, принтерам и последовательным портам в локальных сетях (LAN), работающий по модели «клиент-сервер». Он позволяет пользователям открывать, читать, записывать и изменять файлы на удаленном сервере так же, как если бы они находились на локальном диске.

Как работает протокол SMB

1. Установление соединения (TCP/IP): Клиент отправляет запрос на сервер по порту 445 (в современных версиях) или 139 (в устаревших) для начала диалога.
2. Согласование диалекта (Negotiation): Клиент и сервер договариваются о наиболее высокой версии протокола SMB, которую поддерживают обе стороны, чтобы обеспечить совместимость (например, SMB 2.x, SMB 3.0).
3. Аутентификация: Пользователь проходит проверку подлинности, предоставляя учетные данные (имя пользователя/пароль), чтобы получить доступ к общим ресурсам (шарам).
4. Доступ к ресурсу (Tree Connect): Клиент подключается к конкретному общему ресурсу (папке или принтеру).
5. Операции с файлами: После подключения клиент отправляет команды для открытия, чтения, записи или удаления файлов, а сервер выполняет их и отправляет ответ.

Ключевые возможности SMB

- Совместный доступ: Позволяет нескольким пользователям одновременно работать с файлами на общем сервере.
- Безопасность (SMB 3.x): Современные версии используют шифрование данных при передаче и подписывание пакетов для предотвращения атак «человек посередине» (MitM).
- Высокая производительность: Поддержка многоканальности (SMB3 Multichannel) позволяет использовать несколько сетевых подключений для увеличения скорости.

SMB является стандартом в сетях Windows, обеспечивая работу через сеть, как Samba в Linux.

Раздел 2. Принципы маршрутизации и коммутации

Тема 2.1 Введение в коммутируемые сети

2.1 Конвергентные сети — это объединение различных типов трафика (голос, видео, данные) в единую сетевую инфраструктуру, основанную на протоколе IP. Это позволяет использовать одну сеть для телефонии, интернета и мультимедиа, что снижает расходы, повышает эффективность управления, обеспечивает гибкость масштабирования и улучшает качество обслуживания (QoS).

Основные аспекты конвергентных сетей:

- Единая инфраструктура: Вместо отдельных сетей для телефонии (АТС) и передачи данных, используется одна IP-сеть.
- Мультимедийность: Одновременная передача голоса (VoIP), видеоконференций и обычных данных.
- Конвергентная инфраструктура (CI): В ЦОД это означает интеграцию серверов, систем хранения данных (СХД) и сетевого оборудования в единый комплекс, что упрощает управление.

Преимущества:

- Экономия: Снижение капитальных и операционных затрат (на оборудование, обслуживание, электроэнергию).
- Управляемость: Единая система управления и мониторинга.
- Скорость: Быстрое развертывание и масштабирование ИТ-ресурсов.

Конвергенция позволяет переходить от разрозненных узкоспециализированных систем к единой, более гибкой и экономически выгодной среде передачи информации.

2.2 Объединенная компьютерная сеть обеспечивает совместный доступ к ресурсам (файлам, принтерам, базам данных), оперативный обмен данными, удаленное управление, информационную безопасность и доступ в интернет. Она объединяет узлы (ПК, серверы) для связи между системами, передачи информации и стандартизации взаимодействия.

- Основные функции объединенной компьютерной сети включают:
- Совместное использование ресурсов (Resource Sharing): Доступ к общим файлам, принтерам, сканерам, базам данных и накопителям информации, что снижает затраты на оборудование.
- Обмен данными и связь (Data Communication): Быстрая передача сообщений, документов, электронной почты (e-mail) и использование приложений для общения, а также передача файлов через FTP.
- Информационная и вычислительная функции: Централизованное хранение и доступ к базам данных, возможность распределенных вычислений и использования удаленных серверов.
- Управление сетью и безопасность: Централизованное администрирование, мониторинг трафика, защита данных от несанкционированного доступа и управление правами пользователей.
- Доступ к глобальным сетям: Предоставление возможности выхода в интернет для всех устройств сети через одно общее соединение.

Сеть также обеспечивает совместимость различных устройств и работу популярных служб, таких как World Wide Web (WWW).

2.3 Построение больших конвергентных сетей базируется на интеграции голоса, видео и данных в единую IP-инфраструктуру, обеспечивающую высокую производительность, централизованное управление, безопасность и масштабируемость. Ключевые принципы включают использование иерархической архитектуры (уровни ядра, распределения, доступа), внедрение механизмов QoS (качества обслуживания) для приоритезации трафика и гибкую модульность для масштабирования.

2.4 Трехуровневая иерархическая модель коммутируемой сети (по модели Cisco) — это стандарт проектирования, обеспечивающий масштабируемость, надежность и управляемость. Она включает: уровень ядра (высокоскоростная передача), уровень

распределения (маршрутизация, политики, безопасность) и уровень доступа (подключение пользователей).

2.5 Структура коммутируемой сети с вырожденным ядром (collapsed core) представляет собой упрощенную двухуровневую иерархическую модель, в которой функции уровня ядра (core) и уровня агрегации (distribution) объединены в одном устройстве или группе устройств.

2.6 Уровень доступа коммутируемой сети (Access Layer) обеспечивает подключение конечных устройств (ПК, IP-телефоны, точки доступа) к сети, отвечая за аутентификацию пользователей, безопасность портов, сегментацию трафика с помощью VLAN и использование PoE (Power over Ethernet). Это пограничный уровень с высокой плотностью портов и низкой стоимостью коммутаторов.
Основные функции уровня доступа:
Подключение пользователей: Создание точек входа/выхода в сеть для конечных узлов.

- Безопасность и аутентификация: Контроль доступа к сети, включая аутентификацию по MAC-адресам и протоколу 802.1X.
- Сегментация сети (VLAN): Разделение широковещательных доменов для улучшения производительности и безопасности.
- Управление трафиком: Ограничение скорости (rate limiting) и фильтрация трафика на порту.
- Поддержка питания (PoE): Подача электропитания на устройства (IP-камеры, VoIP-телефоны) через витую пару.
- Создание доменов коллизий: Изоляция сбоев связи за счет работы на втором (канальном) уровне модели OSI.

Коммутаторы этого уровня обычно характеризуются высокой плотностью портов и поддержкой технологий, необходимых для надежного взаимодействия с конечными устройствами.

2.7 Уровень распределения (Distribution Layer) в трехуровневой модели сети служит связующим звеном между доступом и ядром. Основные функции: агрегация трафика от коммутаторов доступа, реализация политик безопасности (ACL), маршрутизация между VLAN, обеспечение резервирования (L2/L3) и фильтрация широковещательных запросов, что снижает нагрузку на ядро.
Ключевые функции уровня распределения:

- Агрегация трафика: Собирает данные с большого количества коммутаторов доступа (access switches) и передает их на высокоскоростное ядро, оптимизируя структуру сети.
- Маршрутизация (L3): Осуществляет маршрутизацию между виртуальными локальными сетями (VLAN), обеспечивая взаимодействие между различными отделами или сегментами.
- Политики безопасности и QoS: Реализует списки контроля доступа (ACL) для ограничения трафика, пакетную фильтрацию и настройку приоритетов обслуживания (QoS) для критически важных данных.
- Резервирование и отказоустойчивость: Использует технологии резервных каналов (например, STP, EtherChannel) для предотвращения петель и автоматического переключения при авариях.

- Определение доменов вещания: Фильтрация широковещательных пакетов, что предотвращает их распространение по всей сети и защищает ядро от перегрузок.
- Адресация и управление сетью: Обеспечивает разделение IP-адресов и маршрутизацию между подсетями, обеспечивая контроль над трафиком.

2.8 Уровень ядра коммутируемой сети (Core Layer) служит высокоскоростной магистралью (backbone) для передачи данных между узлами распределения, обеспечивая максимальную производительность, надежность и отказоустойчивость. Основные функции включают быструю коммутацию, агрегацию трафика, избыточность связей и минимальные задержки.
Функции уровня ядра:

- Высокоскоростная коммутация: Передача данных с минимальными задержками (низкая latency).
- Агрегация трафика: Объединение потоков данных от множества коммутаторов уровня распределения.
- Отказоустойчивость (резервирование): Обеспечение непрерывной работы сети за счет дублирования компонентов и связей.
- Маршрутизация (Layer 3): Высокопроизводительная маршрутизация между подсетями и VLAN.
- Масштабируемость: Возможность наращивания пропускной способности сети без перепроектирования.
- Оптимизация трафика (QoS): Поддержка качества обслуживания для приоритезации критически важных данных.
- Безопасность: Применение политик безопасности (списков доступа ACL) на высокой скорости.
- Быстрое восстановление: Использование протоколов (например, RSTP, MSTP) для мгновенного переключения при отказах.

2.9 Коммутаторы с фиксированной конфигурацией (фиксированной коммутацией) — это устройства с определенным, неизменяемым количеством портов и фиксированным функционалом (обычно 1U), обеспечивающие объединение сетевых устройств (ПК, IP-телефоны) в локальную сеть. Они предоставляют базовую коммутацию кадров на основе MAC-адресов, сегментацию (VLAN), качество обслуживания (QoS) и безопасность портов.
Основные параметры:
Количество портов: Обычно 8, 12, 16, 24, 48 портов, фиксированное производителем.
Скорость портов: Поддержка Fast Ethernet (100 Мбит/с), Gigabit Ethernet (1 Гбит/с), 10G и выше (10 Gigabit Ethernet).

- Тип портов: Медные (RJ-45) для пользовательских устройств, оптические (SFP/SFP+) для магистральных подключений (uplink).
- Поддержка PoE/PoE+: Наличие технологии Power over Ethernet позволяет питать IP-камеры, точки доступа и телефоны через кабель данных.
- Управляемость: Делятся на неуправляемые (plug-and-play) и управляемые (настройка VLAN, STP, QoS через консоль/web).

- Производительность: Пропускная способность (Gbps) и скорость пересылки кадров (Mpps), определяющие нагрузку, которую свитч выдержит без потери пакетов.

Основные функции:

- Коммутация по MAC-адресам: Точная передача данных целевому получателю, что снижает нагрузку на сеть.
- Поддержка VLAN (802.1Q): Логическое разделение сети на изолированные сегменты.
- QoS (Quality of Service): Приоритезация трафика, например, для голосовых данных (VoIP) или видеонаблюдения.
- Безопасность: Функции безопасности на уровне портов, защита от сетевых петель (Spanning Tree Protocol).
- Мониторинг: Функции для управления сетью.

Такие коммутаторы часто применяются на уровне доступа, обеспечивая надежное и быстрое подключение конечных пользователей.

2.10 Модульные коммутаторы — это высокопроизводительные сетевые устройства с шасси, позволяющим устанавливать сменные линейные карты (порты), модули управления, питания и охлаждения. Они обеспечивают гибкую масштабируемость, высокую плотность портов (1G/10G/40G/100G/400G), резервирование компонентов (горячая замена) и расширенные функции управления трафиком.

Основные функции и параметры модульных коммутаторов:

- Гибкая конфигурация: Возможность установки различных модулей: портов Ethernet (медных и оптических SFP/SFP+), модулей питания и вентиляторов.
- Высокая производительность: Высокая пропускная способность коммутационной фабрики и скорость маршрутизации/фильтрации пакетов (иногда >100 Гбит/с на слот).
- Резервирование и отказоустойчивость: Поддержка горячей замены (hot-swap) модулей питания, вентиляторов и линейных карт, что позволяет обслуживать устройство без остановки сети.
- Управление трафиком (L2/L3): Поддержка VLAN (виртуальные сети), QoS (качество обслуживания), маршрутизация пакетов между сетями, защита от петель.
- Масштабируемость: Поддержка стекирования (объединение нескольких физических коммутаторов в один логический) для увеличения общего количества портов.
- Безопасность: Функции безопасности на уровне портов, защита от широковещательных штормов, списки контроля доступа (ACL).
- Мониторинг: Диагностика оптических параметров (мощность сигнала), управление энергопотреблением портов.

Модульные коммутаторы обычно используются в качестве магистральных (core) устройств или в центрах обработки данных (ЦОД), где требуется высокая надежность и возможность быстрого расширения сети.

2.11 Стекируемые коммутаторы объединяют несколько физических устройств в один логический узел с общим IP-адресом и управлением, что упрощает администрирование, повышает отказоустойчивость и масштабируемость сети. Они предо-

ставляют функции централизованного управления (single management plane), быстрого стекирования через выделенные порты, поддержку резервирования питания и активное перенаправление трафика при сбое одного из коммутаторов.
Основные функции и параметры стекируемых коммутаторов:

- Единое управление (Single IP Management): Весь стек из 4–16 устройств управляется как один, с единым IP-адресом, конфигурацией и интерфейсом командной строки (CLI).
- Высокая отказоустойчивость: При выходе из строя одного коммутатора стек продолжает функционировать, а трафик перенаправляется, обеспечивая минимальный простой.
- Масштабируемость: Возможность горячего добавления новых коммутаторов для увеличения количества портов без остановки сети.
- Высокая пропускная способность стека: Коммутаторы соединяются специальными кабелями, обеспечивая высокую скорость обмена данными между устройствами (например, до 320 Гбит/с и более), что выше стандартных восходящих каналов.
- Резервирование питания: Поддержка подключения внешних источников питания, обеспечивающих бесперебойную работу всего стека.
- Расширенные функции (L2/L3): Поддержка виртуальных локальных сетей (VLAN), качества обслуживания (QoS) для приоритезации трафика и питания устройств через PoE/PoE+/PoE++.

Стекирование позволяет эффективно использовать порты и объединять их в агрегированные каналы связи (Link Aggregation) между разными физическими устройствами в стеке.

2.12 Обучение коммутатора — это автоматический процесс формирования таблицы MAC-адресов (CAM-таблицы) для определения местоположения устройств. При получении кадра коммутатор записывает MAC-адрес отправителя и соответствующий порт в таблицу, а при неизвестном получателе рассылает кадр на все порты (flood), постепенно снижая широковещательный трафик.

2.13 Коммутатор пересылает кадры, анализируя их MAC-адреса получателя (Destination MAC) и сверяя их с таблицей MAC-адресов. Он принимает кадр, «обучается» (запоминает MAC источника), ищет порт для получателя и отправляет кадр только туда, либо делает широковещательную рассылку (flooding) на все порты, если адресат неизвестен.

2.13 Фильтрация кадров коммутатором — это процесс принятия решения о пересылке, блокировке или дублировании кадров на основе их MAC-адресов получателя (Destination MAC) и таблицы коммутации (MAC-table). Коммутатор анализирует кадр, проверяет адрес получателя и передает его только в нужный порт (если он известен) или отбрасывает, если кадр предназначен для той же сети.

2.14 Коммутация Store-and-Forward (с промежуточным хранением) — это метод, при котором коммутатор принимает весь кадр целиком, сохраняет его в буфере, проверяет на ошибки (контрольная сумма CRC) и только затем пересылает получателю. Этот метод гарантирует высокую целостность данных, предотвращая передачу поврежденных кадров, но вносит задержку, пропорциональную размеру кадра.

2.15 Коммутация Cut-Through (сквозная коммутация) выполняется путем немедленной пересылки кадра сразу после считывания адреса назначения (первые 6 байт). Коммутатор не ждет получения всего пакета и не проверяет его контрольную сумму, что обеспечивает минимальную задержку.

2.16 Коммутация Fragment-free (без фрагментации) — это гибридный метод, при котором коммутатор считывает адрес назначения и первые 64 байта кадра, проверяя их на ошибки, прежде чем начать пересылку. Этот метод исключает большинство коллизий («фрагментов коллизий») в сетях Ethernet, обеспечивая баланс между низкой задержкой «сквозной» коммутации и надежностью метода «с промежуточным хранением».

2.17 Домен коллизий — это сегмент сети Ethernet, в котором сигналы от разных устройств могут наложиться друг на друга (коллизия), вызвав ошибки передачи. Все узлы в таком домене делят общую пропускную способность, и при одновременной отправке данных возникает столкновение. Концентраторы (Hubs) объединяют все порты в один домен, а коммутаторы (Switches) разбивают его, изолируя устройства.

2.18 Широковещательный домен (broadcast domain) — это логический сегмент компьютерной сети, в котором все устройства (узлы) получают широковещательные кадры, отправленные любым участником этого сегмента. Это область «слышимости» широковещательных запросов, ограниченная сетевыми устройствами уровня 3 (маршрутизаторами) или VLAN.

2.19 Снижение перегрузки компьютерной сети достигается за счет ограничения фонового трафика, использования проводного подключения (Ethernet) вместо Wi-Fi, приоритезации трафика (QoS) и обновления оборудования. Основные методы включают перезагрузку роутера, отключение автоматических обновлений и разделение сети на подсети.

Тема 2.2 Основные концепции и настройки коммутации

2.20 Загрузка коммутатора (на примере Cisco) проходит следующие основные стадии:
POST (Power-On Self-Test): Самотестирование оборудования (ЦП, память, флэш).
Загрузка Bootloader: Инициализация загрузчика из ROM.
Загрузка ОС (IOS): Поиск и загрузка операционной системы из Flash-памяти.
Применение конфигурации: Загрузка файла конфигурации (startup-config) из NVRAM в оперативную память.
Если файл конфигурации не найден, коммутатор запускает мастер начальной настройки (setup mode).

2.21 Начальный загрузчик коммутатора (bootloader, например, U-Boot) — это микропрограмма в ПЗУ (ROM), которая запускается сразу при включении питания. Она выполняет самотестирование оборудования (POST), инициализирует оперативную память (RAM) и загружает основную операционную систему (IOS/Firmware) из Flash-памяти в оперативную для начала работы устройства.
Основные этапы работы загрузчика:

1. POST (Power-On Self-Test): Проверка работоспособности ЦП, памяти и основных контроллеров.
2. Инициализация оборудования: Загрузчик инициализирует шины, порты ввода-вывода и оперативную память.
3. Поиск образа ОС: Программа ищет файл операционной системы во Flash-памяти или, если не находит, пытается загрузить его по сети (TFTP).
4. Загрузка ОС: Перенос файла ОС в RAM и передача управления ядру системы.
5. Консольный доступ: в случае сбоя, загрузчик обеспечивает доступ к меню, позволяющему переустановить прошивку.

Если загрузчик не может найти образ ОС, коммутатор часто останавливается в режиме загрузки (boot > или switch:), ожидая команд от администратора.

2.22 Настройка переменной среды (например, BOOT или PATH) заключается в указании операционной системе пути к исполняемым файлам. В Windows это делается через «Свойства системы» -> «Переменные среды», а в Unix-системах — через экспорт в файлах конфигурации оболочки (например, .bashrc или .zshrc). Это позволяет запускать программы из любого каталога.

Пошаговая настройка в Windows:

1. Нажмите правой кнопкой мыши на «Этот компьютер» (или «Мой компьютер») -> Свойства.
2. Выберите Дополнительные параметры системы -> Переменные среды.
3. В разделе Системные переменные нажмите «Создать» (или «Изменить», если она уже есть).
4. В поле «Имя переменной» введите BOOT (или нужное имя).
5. В поле «Значение переменной» укажите полный путь к папке (например, C:\Program Files\App\bin).
6. Нажмите «ОК» во всех окнах, чтобы применить изменения.

2.23 Восстановление коммутатора после системного сбоя обычно включает перезагрузку, вход в режим загрузчика (bootloader/ROMMON), проверку целостности файловой системы, переустановку прошивки через TFTP/XMODEM и восстановление конфигурации из резервной копии. Ключевые действия требуют консольного подключения для диагностики.

Основные шаги восстановления:

1. Подготовка: Подключите компьютер к консольному порту коммутатора с помощью консольного кабеля (speed 9600 или 115200).
2. Аппаратный сброс/Вход в режим загрузчика:

1) Отключите питание, зажмите кнопку Mode (или Reset) и подайте питание снова, удерживая кнопку до появления приглашения switch: или начала мигания индикаторов.

3. Диагностика и восстановление прошивки (если повреждена):

1) В режиме загрузчика используйте команды (например, copy tftp flash или xmodem), чтобы загрузить корректный файл прошивки (.bin).
2) Проверьте файловую систему на наличие ошибок, если применимо.

4. Сброс настроек (при необходимости):

1) Если сбой вызван конфигурацией, выполните команду сброса в заводские настройки (например, erase startup-config или setenv в режиме ROMMON).

5. Перезагрузка:
1) Введите команду reboot или boot, чтобы перезагрузить коммутатор в нормальный режим.
6. Восстановление конфигурации:
1) Настройте базовые параметры (IP-адрес, пароль) и восстановите ранее сохраненную рабочую конфигурацию.

Совет: Никогда не перезапускайте систему многократно, если подозревается повреждение памяти, так как это может ухудшить ситуацию.

2.24 Светодиодные индикаторы коммутатора (Switch LED indicators) отображают текущее состояние устройства, портов, питания и передачи данных, помогая диагностировать сеть. Основные индикаторы включают Power (питание), System (системная ошибка), Link/Act (подключение/активность) и Speed (скорость). Зеленый цвет обычно означает нормальную работу, оранжевый/желтый — ошибку или низкую скорость.

2.25 Подготовка коммутатора к удаленному управлению включает настройку IP-адреса на интерфейсе управления (обычно VLAN 1), задание шлюза по умолчанию, создание пользователя с паролем и активацию протоколов SSH (рекомендуется) или Telnet. Физически устройство подключается к сети, а настройка производится через консоль.

Основные этапы подготовки:

1. Подключение через консоль: Подключите компьютер к консольному порту коммутатора с помощью консольного кабеля (RJ45-DB9 или USB) для начальной настройки, используя эмулятор терминала (например, Putty).
2. Настройка IP-адреса: Присвойте интерфейсу управления (VLAN) статический IP-адрес из рабочей сети, маску подсети и шлюз по умолчанию, чтобы обеспечить доступ из других подсетей.

Пример (Cisco): interface vlan 1 -> ip address 192.168.1.10 255.255.255.0 -> no shutdown.

2.26 Настройка интерфейса управления коммутатором (Management Interface) позволяет удаленно управлять устройством через Web-интерфейс, SSH или Telnet. Процесс включает присвоение IP-адреса, маски подсети и шлюза, что чаще всего делается через консольный кабель (CLI) или по умолчанию через Web-интерфейс (192.168.1.x/10.x.x.x).

```
switch> enable
switch# configure terminal
switch(config)# interface vlan 1  // Часто management-интерфейс
switch(config-if)# ip address 192.168.1.100 255.255.255.0
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# ip default-gateway 192.168.1.1  // Шлюз для удал
```

2.27 Настройка портов коммутатора — это процесс управления параметрами физических или виртуальных интерфейсов для обеспечения связи, безопасности и сегментации сети. Основные действия включают вход через консоль или веб-интерфейс, выбор порта, настройку VLAN (Access/Trunk), скорости, дуплекса и статуса (вкл/выкл).

2.28 Настройка дуплексного режима и скорости портов коммутатора (обычно Cisco) выполняется в режиме конфигурации интерфейса командами speed {10|100|1000|auto} и duplex {half|full|auto}. По умолчанию используется автосогласование (auto), но для устранения ошибок (mismatch) или подключения к старому оборудованию параметры задают вручную.

2.29 Auto-MDIX (Automatic Medium-Dependent Interface Crossover) — это технология сетевого оборудования, автоматически определяющая тип кабеля (прямой или перекрестный/crossover) и настройки пар передачи/приема (MDI/MDIX). Она устраняет необходимость подбирать кабели при подключении устройств, позволяя использовать любой патч-корд для соединения «коммутатор-коммутатор» или «компьютер-коммутатор».

2.30 Проверка настроек порта коммутатора выполняется через CLI (командную строку) с помощью команд show (например, show running-config, show interfaces status, show vlan) при подключении по Telnet/SSH/Console. Это позволяет увидеть текущий VLAN, скорость, дуплекс и состояние порта (Up/Down). Для визуальной проверки используют веб-интерфейс управления.

2.31 Неполадки коммутатора на уровне доступа (Access Layer) чаще всего связаны с физическим уровнем, ошибками конфигурации (VLAN, порты), перегревом или сбоями электропитания. Основные признаки: отсутствие линка (индикации) на портах, низкая скорость, недоступность хостов в VLAN, зацикливание сети (шторм).

2.32 Устранение неполадок коммутатора доступа включает проверку физического уровня (кабели, питание, индикаторы портов), диагностику логической конфигурации (VLAN, STP, дуплекс), анализ загрузки портов и перезагрузку устройства. Начните с локализации проблемы, определив, касается ли она одного устройства или всего сегмента.

2.33 Настройка защищенного удаленного доступа к коммутатору осуществляется через протокол SSH (Secure Shell), который шифрует все данные, включая пароли. Ключевые шаги включают включение SSH, генерацию ключей шифрования, создание надежного пользователя, настройку виртуальных линий (VTY) и обязательное отключение небезопасного протокола Telnet.

2.34 Настройка SSH на коммутаторе (на примере Cisco) включает задание имени устройства и домена, генерацию RSA-ключей, создание локального пользователя с правами, настройку линий VTY для использования локальной базы данных и включение протокола SSH (обычно версии 2). Это обеспечивает безопасный удаленный доступ, заменяя незащищенный Telnet.

2.35 Проверка работы SSH на коммутаторе выполняется через CLI командами display ssh server status (Huawei), show ip ssh (Cisco) или через попытку подключе-

ния с ПК по 22 порту (PuTTY/terminal). Убедитесь, что сервер включен, сгенерированы RSA-ключи, настроена аутентификация и разрешен VTY-доступ.

2.36 Защита неиспользуемых портов коммутатора — это базовая мера сетевой безопасности, включающая: программное отключение (shutdown), перевод в изолированный VLAN, настройку Port Security (привязка MAC-адресов) и физическое блокирование заглушками. Это предотвращает несанкционированный доступ к сети, мак-спуфинг и VLAN-hopping.

2.37 Защита MAC-адресов обеспечивает безопасность локальной сети (L2), предотвращая несанкционированный доступ и атаки подмены адресов (MITM). Основные виды включают Port Security (статическая/динамическая привязка), Sticky MAC-адреса и DHCP Snooping, ограничивая доступ по принципу «разрешен только этот адрес».

2.38 Безопасность портов (Port Security) коммутатора ограничивает несанкционированный доступ, привязывая MAC-адреса к портам. Три основные функции включают: статическую привязку (вручную заданные MAC), динамическое обучение (автоматическое запоминание) и sticky-привязку (запоминание и сохранение MAC в конфигурации). При нарушении порт может отключаться или блокировать трафик.

Тема 2.3 Виртуальные локальные сети (VLAN)

2.39 VLAN (Virtual Local Area Network) — это технология, позволяющая логически разделить одну физическую локальную сеть на несколько изолированных виртуальных сетей. Устройства в разных VLAN не видят друг друга на канальном уровне (L2), даже если подключены к одному коммутатору, что повышает безопасность, производительность и упрощает управление сетью.

2.40 VLAN (виртуальные локальные сети) обеспечивают сегментацию сети для повышения безопасности, производительности и управляемости. Основные преимущества включают изоляцию трафика (уменьшение широковещательных штормов), усиленную защиту данных за счет логического разделения устройств, гибкость при перемещении пользователей без перекоммутации кабелей и снижение затрат на оборудование.

2.41 VLAN (Virtual Local Area Network) — это технология логической сегментации физической сети на несколько изолированных широковещательных доменов. Основные типы VLAN делятся по способу назначения портов (статические/динамические) и по функциональному назначению (Data, Voice, Management, Native), обеспечивая повышенную безопасность, производительность и удобство управления сетью.

2.42 Голосовые VLAN (Voice VLAN) — это выделенные виртуальные сети для VoIP-трафика, обеспечивающие высокое качество связи за счет приоритезации (QoS), изоляции от компьютерного трафика и автоматической настройки IP-телефонов. Они гарантируют низкую задержку, минимизируют дрожание сигнала и повышают безопасность, предотвращая перегрузки сети.

2.43 Транк виртуальных сетей (VLAN Trunk) — это физический канал связи между сетевыми устройствами (обычно коммутаторами или маршрутизаторами), который позволяет передавать трафик нескольких различных VLAN (виртуальных локальных сетей) через один интерфейс. Он используется для объединения сегментов сети, распределенных по разным коммутаторам, сохраняя их логическую изоляцию.

2.44 Сети с VLAN (виртуальными локальными сетями) разделяют один физический коммутатор на несколько логических широковещательных доменов, изолируя трафик между группами устройств. Сети без VLAN (обычные LAN) объединяют все устройства в один общий домен, где широковещательные запросы получают все порты, создавая высокую нагрузку и риски безопасности.

2.45 Тегирование кадров Ethernet (стандарт IEEE 802.1Q) — это процесс добавления специальной метки в заголовок кадра, чтобы коммутатор понимал, какой виртуальной сети (VLAN) принадлежит этот трафик.

2.46 Поле тега VLAN (согласно стандарта IEEE 802.1Q) — это 4-байтовая вставка в Ethernet-кадр, которая позволяет коммутаторам определять принадлежность трафика к конкретной виртуальной сети.
Оно вклинивается между адресом отправителя и полем типа/длины. Вот из чего оно состоит:

1. TPID (Tag Protocol Identifier): 16 бит. Всегда имеет значение 0x8100. Это «сигнал» для оборудования, что кадр содержит метку 802.1Q.
2. TCI (Tag Control Information): оставшиеся 16 бит, которые делятся на:

1) PCP (Priority Code Point): 3 бита. Используется для приоритезации трафика (QoS). Позволяет задать уровень важности кадра от 0 до 7.
2) DEI (Drop Eligible Indicator): 1 бит. Указывает на возможность удаления кадра при перегрузках сети (раньше назывался CFI).
3) VID (VLAN Identifier): 12 бит. Самая важная часть — собственно ID сети. Позволяет создать до 4094 уникальных VLAN (значения 0 и 4095 зарезервированы).

Если говорить совсем просто: это «цифровая бирка», которую вешает коммутатор, чтобы пакеты из разных отделов (например, Бухгалтерия и Гостевой Wi-Fi) не перемешивались, даже если они идут по одному проводу.

2.47 В контексте сетей 802.1Q тегированные кадры в native VLAN — это кадры, которые имеют в заголовке метку (VLAN ID), совпадающую с номером «родной» (native) сети порта.
По классическим правилам, трафик native VLAN должен передаваться по транку без тегов. Однако появление тегированных кадров в этой сети может быть вызвано специфическими настройками или угрозами безопасности

2.48 Нетегированные кадры в контексте Native VLAN — это пакеты данных, которые передаются через транковый порт без специальной метки (тега 802.1Q).
В обычной работе транковый порт ожидает, что каждый кадр будет иметь тег с номером VLAN. Однако для Native VLAN сделано исключение:

Принцип работы: Если коммутатор получает на транковый порт кадр без тега, он автоматически относит его к той VLAN, которая настроена как «родная» (Native) для этого порта.

2.49 Тегирование голосовой VLAN (Voice VLAN) — это технология, позволяющая передавать по одному физическому кабелю одновременно трафик данных (от компьютера) и голосовой трафик (от IP-телефона), разделяя их на логическом уровне. Обычно IP-телефон имеет встроенный коммутатор с двумя портами: один подключается к розетке (коммутатору доступа), а второй — к компьютеру. Тегирование позволяет коммутатору различать эти потоки:

- Трафик данных (Untagged): Компьютер обычно не умеет работать с тегами 802.1Q, поэтому его трафик идет без меток в так называемую Native или Access VLAN.
- Голосовой трафик (Tagged): Телефон помечает свои пакеты тегом определенной VLAN (например, ID 2). Это позволяет назначить голосу более высокий приоритет (QoS), чтобы избежать задержек и прерываний при разговоре.

2.50 Конфигурация Voice VLAN (голосовой VLAN) обычно подразумевает создание отдельной сети для IP-телефонов (например, VLAN 100) и настройку порта в гибридном режиме: телефон получает тегированный трафик (voice vlan), а подключенный за ним ПК — нетегированный (data vlan). Это обеспечивает приоритет (QoS) голосовому трафику.

Пример конфигурации (Cisco IOS)

1. **Создание VLAN для голоса и данных:**

cisco

```
vlan 100
 name VOICE
vlan 200
 name DATA
```

2. **Настройка порта (Access + Voice VLAN):**

cisco

```
interface GigabitEthernet0/1
 switchport mode access
 switchport access vlan 200    ! VLAN для ПК (не-тегированный)
 switchport voice vlan 100    ! VLAN для телефона (тегированный
 spanning-tree portfast       ! Ускорение перехода порта в режи
 spanning-tree bpduguard enable
```

3. **Приоритет голосового трафика (QoS):**

cisco

```
mls qos trust cos
! Или использование LLDP-MED для автоматической настройки телеф
lldp network-policy voice vlan 100 cos 5
```

2.51 VLAN стандартного диапазона — это виртуальные локальные сети с идентификаторами (VLAN ID) от 1 до 1005, используемые в малых и средних сетях. Они автоматически хранятся в файле vlan.dat на коммутаторе, поддерживаются протоколом VTP (VLAN Trunking Protocol) и включают зарезервированные номера (1002–1005) для устаревших технологий, таких как Token Ring и FDDI.

2.52 Сети VLAN расширенного диапазона — это виртуальные локальные сети с идентификаторами (VLAN ID) от 1006 до 4094, используемые для сегментации крупных корпоративных сетей и провайдерских инфраструктур. Они расширяют стандартный диапазон (1–1005), обеспечивая поддержку тысяч независимых широковещательных доменов на одном коммутаторе, при этом требуя конфигурации в прозрачном режиме VTP.

2.53 Создание сети VLAN (Virtual Local Area Network) включает логическое разделение физического коммутатора на несколько независимых сегментов. Процесс состоит из создания VLAN с уникальным ID, назначения портов (Access для ПК, Trunk для связи коммутаторов) и сохранения конфигурации. Это позволяет изолировать трафик и повысить безопасность сети.

2.54 Назначение портов VLAN (Virtual Local Area Network) осуществляется через веб-интерфейс или CLI (командную строку) коммутатора. В веб-интерфейсе нужно создать VLAN (указав ID), выбрать порты и присвоить им статус Untagged (Access) для конечных устройств (ПК, телефоны) или Tagged (Trunk) для связи между коммутаторами.

2.55 Изменение принадлежности порта VLAN выполняется через CLI (командами) или Web-интерфейс коммутатора. Основной принцип: перевести порт в режим access и указать новый ID сети командой switchport access vlan <id>. Для удаления используется no switchport access vlan.

2.56 Для удаления VLAN в Cisco IOS используется команда no vlan [ID] в глобальном режиме конфигурации. Перед удалением необходимо убрать VLAN с интерфейсов (команда no switchport access vlan или no switchport trunk allowed vlan). Удаление vlan.dat через delete flash:vlan.dat удаляет все VLAN, кроме дефолтных.

2.57 Проверка информации о VLAN осуществляется через CLI коммутатора (в основном Cisco) командами show vlan или show vlan brief, которые отображают ID, имена, статус и принадлежность портов. Для детального анализа транков используется show interfaces trunk, а для проверки активности конкретного VLAN — show vlan id <id>.

2.58 Настройка транковых каналов 802.1Q (VLAN Trunking) включает перевод портов коммутатора в режим trunk, что позволяет передавать трафик нескольких VLAN через одно физическое соединение, маркируя кадры тегами (tagging). Основная команда на устройствах типа Cisco — switchport mode trunk, при необходимости указывается инкапсуляция switchport trunk encapsulation dot1q.

2.59 Проверка конфигурации магистрального канала (Trunk/Eth-Trunk) включает анализ физического состояния портов, настроек VLAN (802.1Q), агрегирования ка-

налов (LACP) и тестирование пропускной способности. Используются команды display, show, interface, а также тесты типа J-QuickCheck или RFC 2544 для проверки целостности.

2.60 Основные проблемы с IP-адресацией VLAN возникают из-за нарушения соответствия «одна VLAN — одна подсеть». Ключевые сложности включают перекрытие подсетей (overlapping), конфликты IP-адресов, ошибки в настройке маршрутизации между VLAN (inter-VLAN routing) и некорректную настройку тегирования портов. Решение требует строгого учета уникальности подсетей для каждой VLAN.

2.61 Основные неполадки в транковых каналах (VLAN trunk) связаны с ошибками конфигурации, несоответствием настроек на концах канала, проблемами с протоколами Spanning Tree (STP) или физическими неисправностями кабелей/портов. Ключевые проблемы включают несоответствие Native VLAN, ошибки инкапсуляции (802.1Q), перегрузку канала и ограничения разрешенных VLAN.

2.62 Неверный режим порта коммутатора (Access вместо Trunk или наоборот) чаще всего приводит к блокировке трафика VLAN, неработоспособности сети между коммутаторами или потере связи с конечными устройствами. Это вызывает нарушения в передаче кадров с тегами, проблемы с производительностью, ошибочную работу Spanning Tree и может перевести порт в состояние err-disabled.

Тема 2.4 Концепции маршрутизации

2.63 Производительность сети определяется пропускной способностью, задержками (latency), вариацией задержки (джиттер) и надежностью. Ключевые структуры включают топологии (звезда, кольцо, ячеистая) и иерархические уровни (ядро, распределение, доступ). Важнейшие компоненты — коммутаторы, маршрутизаторы и высокоскоростные каналы, обеспечивающие передачу данных.

2.64 Маршрутизация необходима для эффективной передачи данных между разными сетями и узлами, обеспечивая выбор оптимального пути, надежность доставки пакетов, масштабируемость инфраструктуры и управление сетевым трафиком. Без нее невозможно функционирование интернета и объединение локальных сетей (LAN) в глобальные (WAN), так как маршрутизаторы принимают решения о наилучшем маршруте.

2.65 Компьютер (ПК) — это универсальное устройство общего назначения, оптимизированное для вычислений, хранения данных и пользовательских приложений. Маршрутизатор (роутер) — это специализированный встроенный компьютер, оптимизированный для быстрой обработки, анализа заголовков и пересылки сетевых пакетов (трафика) между сетями, используя специализированное ПО и аппаратные ускорители

2.66 Маршрутизатор (роутер) — это сетевое устройство, которое соединяет разные сети, определяет оптимальный путь для доставки пакетов данных, обеспечивает интернет-подключение для нескольких устройств, защищает сеть с помощью брандмауэра и управляет скоростью трафика.

2.67 Маршрутизатор пересылает пакеты, анализируя IP-адрес назначения и сверяясь с таблицей маршрутизации, используя три основных механизма: процессную

коммутацию (медленная, программная), быструю коммутацию (кэширование путей) и Cisco Express Forwarding (CEF) (высокоскоростная, аппаратная на базе таблиц FIB и ADJ).

2.68 Маршрутизаторы (роутеры) и коммутаторы (свитчи) подключаются к сети преимущественно через Ethernet-кабели (RJ-45) для создания локальной сети (LAN) и доступа в интернет (WAN). Маршрутизатор соединяет локальную сеть с интернетом, подключаясь к модему, а коммутатор расширяет эту сеть, объединяя устройства (ПК, принтеры) между собой и с маршрутизатором для обмена данными.

2.69 Шлюз по умолчанию настраивается в сетевых параметрах операционной системы (Windows, Linux) или устройства (роутер) путем указания IP-адреса маршрутизатора в той же подсети. В Windows это делается через «Центр управления сетями» -> «Свойства TCP/IPv4», а в Linux — через ip route add default via [IP]. Чаще всего используется автоматическое получение через DHCP.

2.70 Документирование сетевой адресации — это создание таблицы или схемы, фиксирующей распределение IP-адресов, масок подсетей и шлюзов для оборудования, что обеспечивает удобство администрирования. Пример включает сеть, подсети (VLAN), диапазоны IP для устройств, шлюзы и маски (например, 192.168.1.0/24 или 10.0.0.0/8).

Таблица обычно создается в Excel, Google Sheets или специализированных системах.

Название сети/VLAN	Имя устройства / Описание	IP-адрес	Маска подсети	Шлюз (GW)
Management	Core Switch	192.168.10.1	255.255.255.0 (/24)	-
Management	Firewall/Router	192.168.10.254	255.255.255.0 (/24)	-
Servers	DC01 (Primary)	10.0.1.10	255.255.255.0 (/24)	10.0.1.1
Servers	File Server	10.0.1.11	255.255.255.0 (/24)	10.0.1.1
Users	DHCP Range Start	192.168.20.10	255.255.255.0 (/24)	192.168.2(
Users	DHCP Range End	192.168.20.250	255.255.255.0 (/24)	192.168.2(

2.71 Активация IP-адресации на узле выполняется путем назначения уникального IP-адреса, маски подсети и шлюза, что делается через настройки ОС (Windows/Linux), веб-интерфейс (DHCP/статически) или команды CLI (например, ip address на сетевом интерфейсе). В промышленных системах это часто требует перевода узла в сервисный режим с последующим обновлением сетевых параметров.

2.72 Светодиодные индикаторы на маршрутизаторе (роутере) — это система визуальной диагностики, показывающая текущее состояние устройства и сети. Постоянное свечение обычно означает исправную работу, быстрое мигание — обмен данными, а красный или оранжевый цвет — отсутствие интернета или ошибку.

2.73 Настройка консольного доступа (физического) осуществляется подключением консольного кабеля (COM/RJ45-to-USB) от порта устройства (Cisco, роутер, сервер) к ПК. Используйте эмуляторы терминала (PuTTY, Tera Term, Minicom) с настройками порта: Скорость 9600, Бит данных 8, Четность нет, Стоп-бит 1, Управление потоком нет.

2.74 Активация IP-адресации на коммутаторе (уровня L2/L3) для удаленного управления выполняется путем настройки IP-адреса на виртуальном интерфейсе VLAN (SVI — Switch Virtual Interface), обычно VLAN 1 или отдельном Management VLAN. Это включает вход в режим настройки, назначение IP-адреса, маски, включение интерфейса командой no shutdown и указание шлюза по умолчанию.

2.75 Настройка основных параметров маршрутизатора включает физическое подключение, вход в панель управления, настройку интернет-соединения (WAN), создание защищенной сети Wi-Fi (SSID и пароль), смену пароля администратора и сохранение конфигурации.

2.76 Настройка консольного доступа к маршрутизатору (обычно Cisco или аналоги) выполняется через специальный консольный кабель (RJ45-COM или USB-COM) и программу-эмулятор терминала (PuTTY, Tera Term), подключенные к COM-порту ПК. В настройках терминала выберите Serial, укажите номер порта (например, COM3) и скорость 9600 или 115200 бод.

2.77 Базовая настройка маршрутизатора (на примере Cisco CLI) включает присвоение имени, защиту паролями консоли и привилегированного режима, шифрование паролей, настройку баннера и сохранение конфигурации. Это обеспечивает безопасность и идентификацию устройства в сети.
Пример основных команд настройки:

1. Вход в режим конфигурации:
   Router> enable
   Router# configure terminal
2. Задание имени устройства:
   Router(config)# hostname R1-Main
3. Установка пароля на привилегированный режим (enable):
   R1-Main(config)# enable secret strongpassword
4. Защита консольного подключения:
   R1-Main(config)# line console 0

R1-Main(config-line)# password consolepassword
R1-Main(config-line)# login
R1-Main(config-line)# exit

5. Защита удаленного доступа (SSH/Telnet):
   R1-Main(config)# line vty 0 4
   R1-Main(config-line)# password vtypassword
   R1-Main(config-line)# login
   R1-Main(config-line)# transport input ssh (рекомендуется SSH вместо Telnet)
6. Шифрование паролей:
   R1-Main(config)# service password-encryption
7. Настройка баннера (MOTD):
   R1-Main(config)# banner motd #Authorized Access Only!#
8. Сохранение настроек:
   R1-Main(config)# exit
   R1-Main# copy running-config startup-config

Для домашних роутеров эти параметры задаются через веб-интерфейс (обычно по адресу 192.168.1.1 или 192.168.0.1), где главными являются настройка Wi-Fi (SSID + пароль WPA2/WPA3) и типа подключения к провайдеру (IPoe, PPPoE).

2.78 Настройка IPv4-адреса на интерфейсе маршрутизатора (обычно Cisco) включает вход в режим конфигурации интерфейса (interface <type> <number>), назначение IP-адреса и маски подсети командой ip address <ip> <mask> и включение интерфейса командой no shutdown. Это обеспечивает базовую сетевую связность для устройства.

2.79 Настройка IPv6 на маршрутизаторе включает активацию протокола в разделе WAN/Internet, выбор типа подключения (DHCPv6, SLAAC или Static), настройку префикса LAN и включение SLAAC+RDNSS для автоматической адресации устройств. Рекомендуется включить «Enable SLAAC» и указать публичные DNS-серверы (например, Google 2001:4860:4860::8888).

2.80 Настройка интерфейса loopback (обычно lo или lo0) для IPv4 обеспечивает локальную связь устройства с самим собой, используя адрес 127.0.0.1 (маска 255.0.0.0 или /8). В Linux это делается через ifconfig lo 127.0.0.1 или добавлением в /etc/network/interfaces, а на Cisco/MikroTik — созданием виртуального интерфейса loopback с IP-адресом, обычно.

2.81 Для проверки настроек интерфейса маршрутизатора подключитесь к нему по Wi-Fi или кабелю, введите IP-адрес (обычно 192.168.1.1 или 192.168.0.1) в браузере, авторизуйтесь (логин/пароль admin/admin). В меню найдите разделы «WAN», «Internet» или «Status», чтобы просмотреть настройки подключения, портов, Wi-Fi и DHCP.

2.82 Проверка настроек IPv6 на маршрутизаторе осуществляется через его веб-интерфейс в разделах «Сеть», «WAN» или «IPv6». Необходимо убедиться, что включен режим работы IPv6, выбран правильный тип подключения (Native/DHCPv6) от провайдера, а в статусе отображается присвоенный IPv6-адрес, префикс и DNS-серверы.

2.83 Фильтрация вывода команд show (обычно в Cisco IOS) осуществляется с помощью символа вертикальной черты (|), за которым следует один из параметров фильтрации: include (включить), exclude (исключить), begin (начать с) или section (раздел). Это позволяет быстро найти нужные данные, такие как IP-адреса, статус интерфейсов или конкретные настройки конфигурации.

2.84 История команд (history) — это инструмент терминала (Bash, PowerShell, CMD), сохраняющий ранее введённые команды для ускорения работы, автоматизации и повторного использования. Ключевые функции включают быстрый вызов через стрелки, поиск по журналу (Ctrl+R), создание скриптов, удобное редактирование длинных строк и просмотр выполненных действий.

2.85 Коммутация в маршрутизаторе (пересылка пакетов) — это процесс передачи данных из входного порта во входной буфер, затем через коммутационную матрицу к выходному порту. Основные этапы включают: прием пакета, анализ заголовка (поиск в таблице маршрутизации), коммутацию (переключение) и буферизацию на выходе.
Основные этапы коммутации пакетов:

1. Прием пакета (Ingress): Входной интерфейс получает кадр, проверяет его целостность и извлекает IP-пакет.
2. Поиск в таблице маршрутизации (Look-up): Маршрутизатор анализирует заголовок пакета (IP-адрес назначения) и сверяет его с таблицей маршрутизации (FIB — Forwarding Information Base) для определения лучшего следующего узла (next hop) и выходного интерфейса.
3. Переключение (Switching): Пакет перемещается через внутреннюю коммутационную матрицу (фабрику) из входного порта в соответствующий выходной порт.
4. Буферизация и отправка (Egress): Пакет помещается в очередь выходного порта, обрабатывается согласно QoS и отправляется в физическую среду.

В зависимости от модели, коммутация может происходить на уровне центрального процессора (программная), с использованием кэша (быстрая) или аппаратно на ASIC (экспресс-коммутация).

2.86 Отправка пакетов маршрутизатором — это процесс, включающий прием данных, анализ IP-адреса назначения, поиск в таблице маршрутизации лучшего пути и пересылку пакета через соответствующий интерфейс (на следующий узел или в сеть назначения).
Основные этапы:

1. Прием пакета (De-encapsulation): Маршрутизатор получает кадр на входном интерфейсе, проверяет целостность (CRC) и удаляет канальный заголовок, извлекая IP-пакет.
2. Анализ заголовка и принятие решения: Маршрутизатор анализирует IP-адрес назначения в пакете и ищет совпадения в своей таблице маршрутизации.
3. Поиск маршрута: Используется алгоритм longest prefix match (совпадение с самой длинной маской). Определяется адрес следующего узла (next-hop) и выходной интерфейс.

4. Переинкапсуляция: Пакет упаковывается в новый кадр канального уровня, соответствующий выходному интерфейсу (например, Ethernet), с новыми MAC-адресами источника и назначения.
5. Отправка пакета (Switching): Пакет переключается на выходной интерфейс и передается в физическую среду.

Если путь не найден, пакет отбрасывается, а отправителю может быть выслано сообщение ICMP "Destination Unreachable" (направление недоступно).

2.87 Определение пути маршрутизатором — это процесс выбора наилучшего маршрута для пакета данных, который включает получение пакета, анализ IP-адреса назначения, поиск совпадений в таблице маршрутизации, выбор наилучшего пути (на основе метрик) и пересылку пакета через соответствующий выходной интерфейс.

Основные этапы определения пути:

1. Получение пакета (Ingress): Маршрутизатор принимает кадр данных на входящем интерфейсе, проверяет его на ошибки и извлекает IP-пакет, просматривая адрес назначения.
2. Анализ таблицы маршрутизации: Маршрутизатор сверяет IP-адрес получателя с записями в своей таблице маршрутизации (созданной статически или через протоколы динамической маршрутизации: RIP, OSPF, EIGRP).
3. Выбор наилучшего пути (Best Path Selection):
    1) Длиннейшее совпадение префикса (Longest Prefix Match): Выбирается маршрут с наиболее точным совпадением сетевой части адреса.
    2) Административное расстояние (Administrative Distance): Если есть несколько путей от разных источников, выбирается тот, которому больше доверяют.
    3) Метрика (Metric): Если источник один, выбирается путь с наименьшей стоимостью (число хопов, пропускная способность, задержка).
4. Пересылка пакета (Egress): Маршрутизатор определяет выходной интерфейс и адрес следующего перехода (next hop), инкапсулирует пакет в новый кадр и отправляет его.
5. Функционирование (Switching): Пакет перемещается с входного интерфейса на выходной (на уровне аппаратной части), если маршрут найден, иначе пакет отбрасывается (если нет маршрута по умолчанию).

2.88 Балансировка нагрузки на маршрутизаторе — это распределение входящего и исходящего сетевого трафика между несколькими каналами связи или серверами. Это повышает скорость работы, надежность и отказоустойчивость сети за счет использования алгоритмов (например, Round Robin, Least Connections). Маршрутизатор направляет запросы на доступные интерфейсы, предотвращая перегрузку отдельных линий.

2.89 Административное расстояние (Administrative Distance, AD) — это критерий надежности источника маршрутной информации (протокола маршрутизации) в сетевых устройствах, используемый для выбора лучшего пути при получении данных о сети из нескольких источников. Чем меньше значение AD (от 0 до 255), тем выше доверие к маршруту.

2.90 Анализ таблицы маршрутизации выполняется путем сравнения IP-адреса назначения пакета с записями в таблице, где приоритет отдается самой длинной маске подсети (Longest Prefix Match). Маршрутизатор или ОС выбирает наиболее специфичный маршрут, или маршрут по умолчанию (gateway), а при совпадении путей — наименьшую метрику.

2.91 Источники таблицы маршрутизации — это механизмы, с помощью которых маршрутизатор узнает о сетях и путях к ним. Основными источниками являются непосредственно присоединенные сети (Directly Connected), статические маршруты (Static Routes), настроенные вручную, и динамические протоколы маршрутизации (RIP, OSPF, EIGRP, BGP), обменивающиеся данными автоматически.

2.92 Записи маршрутизации удаленной сети в таблице маршрутизатора указывают путь к сетям, не подключенным напрямую, определяя адрес следующего прыжка (next-hop) и выходной интерфейс. Они включают целевую удаленную сеть, маску, шлюз и метрику для выбора лучшего пути. Эти записи создаются статически или динамическими протоколами (RIP, OSPF).
Основные характеристики записей для удаленных сетей:

- Целевая сеть (Destination Network): IP-адрес и маска подсети удаленной сети назначения.
- Адрес следующего перехода (Next-Hop Address): IP-адрес следующего маршрутизатора на пути к цели.
- Выходной интерфейс (Exit Interface): Физический или виртуальный порт, через который отправляются данные.
- Метрика (Metric): Значение, указывающее «стоимость» пути; используется для выбора наилучшего маршрута, если их несколько.
- Тип источника: Указывает, как маршрут был изучен: статический (введен вручную) или динамический (через протоколы маршрутизации).

2.93 Интерфейсы с прямым подключением (Direct-Attached) — это аппаратные средства связи, соединяющие устройства напрямую, без промежуточных сетевых коммутаторов или маршрутизаторов. Они характеризуются низкими задержками, высокой скоростью передачи данных и надежностью, часто используя последовательный (USB, CAN) или специализированный параллельный способ обмена данными.

2.94 Записи с прямым подключением (Directly Connected) — это маршруты к сетям, физически подключенным к интерфейсам маршрутизатора. Они создаются автоматически, когда интерфейсу присваивается IP-адрес и он переводится в активное состояние (up). В таблице они обозначаются буквой «C» (Connected) для подсети и «L» (Local) для конкретного IP-адреса интерфейса.

2.95 Настройка статического маршрута IPv4 включает указание сети назначения, маски подсети, шлюза (next hop) и, опционально, метрики. Это выполняется через командную строку (Windows: route -p add, Linux: ip route add) или веб-интерфейс роутера/файрвола в разделе «Маршрутизация/Static Routes». Основная цель — вручную задать путь для трафика.
Основные параметры
Для настройки требуются следующие данные:

- Сеть назначения (Destination Network): IP-адрес удаленной подсети или конкретного хоста.
- Маска подсети (Subnet Mask): Маска для сети назначения.
- Шлюз (Gateway/Next Hop): IP-адрес маршрутизатора, на который отправлять пакеты.
- Метрика (Metric): Приоритет маршрута (чем меньше число, тем выше приоритет).

1. Настройка в Windows
Используйте командную строку (cmd) от имени администратора:
route -p ADD <сеть> MASK <маска> <шлюз> METRIC <метрика>
Пример: route -p add 192.168.10.0 mask 255.255.255.0 10.10.10.1.
-p делает маршрут постоянным (сохраняется после перезагрузки).
2. Настройка в Linux
Используйте команду ip route (временно) или конфигурационные файлы (постоянно):
sudo ip route add <сеть>/<CIDR> via <шлюз> dev <интерфейс>
Пример: sudo ip route add 10.0.0.0/24 via 192.168.1.1 dev eth0.
3. Настройка на роутерах (MikroTik, Cisco, Keenetic)
1) Откройте веб-интерфейс -> Маршрутизация (Routing/Static Routes).
2) Нажмите «Добавить» (Add).
3) Введите сеть, маску, шлюз и выберите интерфейс.

4. Настройка в облачных сетях (VPC)
1) Перейдите в раздел VPC / Подсети.
2) Выберите подсеть и нажмите «Привязать таблицу маршрутизации».
3) Создайте маршрут, указав направление и шлюз.

Важно: Убедитесь, что IP-адрес шлюза находится в той же подсети, что и ваш текущий интерфейс.

2.96 Настройка статического маршрута IPv6 включает указание целевой сети (префикса), длины префикса и адреса следующего перехода (next-hop) или исходящего интерфейса. На устройствах Cisco используется команда ipv6 route [префикс]/[длина] [интерфейс/адрес next-hop] в режиме глобальной конфигурации, обеспечивая явное указание пути.

2.97 Динамическая маршрутизация — это автоматический процесс обмена данными между сетевыми устройствами (маршрутизаторами) с помощью специальных протоколов (OSPF, BGP, RIP) для формирования и обновления таблиц маршрутизации. Она обеспечивает гибкость, отказоустойчивость и автоматический выбор оптимального пути для трафика в реальном времени, в отличие от ручной настройки в статической маршрутизации.

2.98 Протоколы маршрутизации IPv4 делятся на внутренние (IGP) для обмена маршрутами внутри автономной системы и внешние (EGP) для взаимодействия между ними. Основные протоколы включают OSPF, EIGRP, RIP (IGP) и BGP (EGP). Они позволяют маршрутизаторам автоматически изучать пути к сетям, адаптируясь к изменениям топологии.

2.99 Основные протоколы маршрутизации IPv6 включают протоколы внутреннего шлюза (IGP), такие как RIPng (RIP next generation), OSPFv3 и EIGRP для IPv6, а также протоколы внешнего шлюза, в частности MP-BGP (Multiprotocol BGP), обеспечивающие обмен маршрутами между автономными системами. Они поддерживают иерархию адресов, встроенную безопасность и многоадресную рассылку.

Тема 2.5 Маршрутизация между VLAN

2.100 Маршрутизация между VLAN (Inter-VLAN routing) — это процесс пересылки сетевого трафика между изолированными виртуальными локальными сетями (VLAN) с использованием устройств 3-го уровня (маршрутизатор или L3-коммутатор). Поскольку VLAN изолируют домены широковещания, маршрутизация необходима для взаимодействия между пользователями из разных VLAN.

2.101 Устаревший метод маршрутизации между VLAN («Legacy Inter-VLAN Routing») основан на использовании физического маршрутизатора, где каждый VLAN подключается отдельным физическим кабелем к собственному интерфейсу маршрутизатора. Это решение плохо масштабируется, требует много портов и кабелей, поэтому используется только в малых сетях.

2.102 Маршрутизация Router-on-a-Stick (ROAS) — это метод соединения нескольких сетей VLAN через один физический интерфейс маршрутизатора и один порт коммутатора. Маршрутизатор использует субинтерфейсы (логические интерфейсы) для каждого VLAN, а коммутатор настраивается в режиме транка (802.1Q), обеспечивая обмен данными между подсетями.

2.103 Устаревший метод маршрутизации между VLAN («Legacy Inter-VLAN Routing») заключается в физическом подключении отдельного порта маршрутизатора к каждому VLAN на коммутаторе. Каждый порт маршрутизатора выступает шлюзом по умолчанию (Default Gateway) для своей подсети, что требует большого количества физических интерфейсов, ограничивая масштабируемость сети.

1. **Настройка коммутатора:** Создать VLAN и назначить порты, ведущие к маршрутизатору, в режим доступа (access) для соответствующих VLAN.

```
Switch(config)# vlan 10
Switch(config-vlan)# vlan 20
Switch(config-vlan)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# interface fastethernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

2. **Настройка маршрутизатора:** Настроить каждый физический интерфейс, назначив IP-адреса из подсетей соответствующих VLAN.

```
Router(config)# interface gigabitethernet 0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface gigabitethernet 0/1
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config-if)# no shutdown
```

3. **Настройка клиентов:** Настроить конечные устройства (ПК) использовать IP-адреса портов маршрутизатора в качестве шлюза по умолчанию (192.168.10.1 для VLAN10, 192.168.20.1 для VLAN20).

2.106 Настройка Router-on-a-Stick (ROAS) — это метод маршрутизации между VLAN, использующий один физический интерфейс маршрутизатора и один транковый (Trunk) порт коммутатора. Основная конфигурация включает создание VLAN на коммутаторе, настройку транка и разделение физического интерфейса маршрутизатора на логические подинтерфейсы (subinterfaces), каждый из которых служит шлюзом для своей VLAN.

2.107 Настройка коммутатора при методе Router-on-a-Stick (роутер на «палке») включает создание VLAN, назначение портов доступа (access) для конечных устройств и настройку транкового (trunk) порта, подключенного к маршрутизатору. Порт, ведущий к маршрутизатору, должен пропускать все VLAN (802.1Q) для маршрутизации трафика.

2.108 Настройка подынтерфейсов (subinterfaces) при методе router-on-a-stick (Cisco) обеспечивает маршрутизацию между VLAN через один физический порт, разделяя его на логические части. Для каждой VLAN создается подынтерфейс, инкапсулируется трафик через 802.1Q и назначается IP-адрес (шлюз).
Основные шаги настройки (на примере интерфейса GigabitEthernet0/0/1):

1) Активация физического порта:
   Router(config)# interface gigabitethernet 0/0/1
   Router(config-if)# no shutdown
   Физический интерфейс должен быть включен, но без IP-адреса, как описано на сайте itexamanswers.net.
2) Создание и настройка подынтерфейса (например, для VLAN 10):
   Router(config)# interface gigabitethernet 0/0/1.10
   Router(config-subif)# description Gateway for VLAN 10
   Подынтерфейсы создаются командой с точкой, например, interface, как описано на сайте termilab.ru.
3) Настройка инкапсуляции 802.1Q:
   Router(config-subif)# encapsulation dot1Q 10
   Команда `encapsulation dot1Q [vlan_id]` привязывает подынтерфейс к конкретной VLAN, как описано в лабораторной работе termilab.ru.
4) Назначение IP-адреса (шлюза для VLAN):
   Router(config-subif)# ip address 192.168.10.1 255.255.255.0
   IP-адрес подынтерфейса становится шлюзом по умолчанию для устройств в этой VLAN, как описано на сайте termilab.ru.
5) Повторение шагов 2-4 для других VLAN (напр., 0/0/1.20, encapsulation dot1Q 20 и т.д.).
6) Настройка порта коммутатора: Порт, подключенный к маршрутизатору, должен быть переведен в режим trunk
   (switchport mode trunk) по протоколу 802.1Q

2.109 Проверка подынтерфейсов при маршрутизации Router-on-a-Stick (на Cisco) включает верификацию их состояния, инкапсуляции и IP-адресов. Основные команды: show ip interface brief (статус), show interfaces <interface>.<subinterface> (параметры инкапсуляции) и show running-config (соответствие VLAN).2.110 Опишите настройку и маршрутизации методом router-on-a-stick.

Тема 2.6 Статическая маршрутизация

2.111 Статическая маршрутизация — это метод настройки сетевых маршрутов, при котором пути передачи данных задаются администратором вручную, без использования автоматических протоколов. Маршруты фиксированы, предсказуемы, не требуют высокой вычислительной мощности оборудования, но требуют ручного обновления при изменении структуры сети.

2.112 Динамическая маршрутизация — это автоматический процесс обмена данными между сетевыми устройствами (маршрутизаторами) с помощью специальных протоколов (OSPF, BGP, RIP) для формирования и обновления таблиц маршрутизации. Она обеспечивает гибкость, отказоустойчивость и автоматический выбор оптимального пути для трафика в реальном времени, в отличие от ручной настройки в статической маршрутизации.

2.113 Статическая маршрутизация подразумевает ручную настройку маршрутов администратором, обеспечивая простоту, безопасность и экономию ресурсов в малых сетях. Динамическая маршрутизация использует протоколы (OSPF, BGP) для автоматического обновления таблиц, что необходимо для больших, масштабируемых сетей с частыми изменениями топологии.

2.114 Статическая маршрутизация — это метод ручной настройки маршрутов в таблице маршрутизатора, при котором администратор явно указывает путь для пакетов, без использования протоколов динамического обмена маршрутной информацией. Основные задачи включают обеспечение связи в малых сетях, подключение тупиковых сетей (stub) и создание маршрутов по умолчанию.

1.115 Статические маршруты IPv4 и IPv6 используются для ручного управления трафиком и включают следующие основные типы: стандартные (для конкретной сети), маршруты по умолчанию (0.0.0.0/0 или ::/0), суммарные (объединяющие несколько сетей), плавающие (резервные с повышенной административной дистанцией) и маршруты к хосту (одиночный адрес /32 или /128).

1.116 Стандартный статический маршрут — это вручную настроенная администратором запись в таблице маршрутизации, указывающая путь к конкретной удаленной сети (IP-адрес назначения и маска), а также адрес следующего прыжка (next-hop) или интерфейс выхода. В отличие от динамических протоколов, он фиксирован, не меняется автоматически и обеспечивает надежную передачу трафика без нагрузки на сеть.

1.117 Статический маршрут по умолчанию — это специальный тип маршрута (0.0.0.0/0), используемый маршрутизатором, когда в таблице маршрутизации нет более специфичных (точных) записей для адреса назначения. Он направляет весь трафик с неизвестными адресами на определенный шлюз («шлюз последней надежды»), что критично для подключения к интернету.

1.118 Объединенный статический маршрут (часто называемый суммированием маршрутов или супернетизацией) — это метод настройки маршрутизатора, при котором несколько специфических статических маршрутов в разные подсети объеди-

няются в один общий маршрут с более короткой маской подсети. Это позволяет упростить таблицу маршрутизации, уменьшить нагрузку на процессор и сократить объем обмениваемых данных.

1.119 Плавающий статический маршрут — это резервный статический маршрут, который активируется только при сбое основного (основного статического или динамического) пути. Он имеет повышенное административное расстояние (AD), что делает его менее приоритетным, заставляя «плавать» в резерве.

1.120 Настройка статического маршрута IPv4 включает указание сети назначения, маски подсети, IP-адреса следующего прыжка (шлюза) или исходящего интерфейса. Маршрут добавляется в таблицу маршрутизации через CLI (команда ip route) или веб-интерфейс, обеспечивая принудительное направление трафика.

1.121 Полностью заданный статический маршрут IPv4 (Fully Specified Static Route) настраивается для сетей с множественным доступом (например, Ethernet), указывая сеть назначения, IP-адрес следующего прыжка (next-hop) и исходящий интерфейс. Это устраняет необходимость в рекурсивном поиске в таблице маршрутизации.

1.122 Для проверки статических IPv4-маршрутов на оборудовании Cisco (IOS) используются команды: show ip route static (только статические), show ip route (вся таблица) и show ip route <ip_адрес> (маршрут к конкретной сети). Эти команды отображают состояние, следующий прыжок (next-hop) и интерфейс выхода.

1.123 Настройка статического маршрута по умолчанию (шлюза по умолчанию) заключается в указании устройству перенаправлять весь неизвестный трафик на определенный IP-адрес следующего перехода (next-hop) или через выходной интерфейс. Это достигается использованием сети назначения и маски 0.0.0.0 0.0.0.0 (или 0.0.0.0/0 для IPv4), что соответствует «любой сети».

1.124 Настройка статического маршрута IPv6 включает активацию маршрутизации (ipv6 unicast-routing), указание сети назначения, длины префикса и адреса следующего прыжка (next-hop) или исходящего интерфейса. Основная команда: ipv6 route [префикс/длина] [next-hop_address | interface]. Это обеспечивает явное указание пути для пакетов.

1.125 Параметры статического маршрута следующего перехода (next-hop) в IPv6 включают целевую сеть (префикс/длину), IPv6-адрес следующего устройства (маршрутизатора) и, опционально, выходной интерфейс. Главный параметр — глобальный (unicast) IPv6-адрес соседа, определяющий путь, через который пакеты покинут сеть.

1.126 Настройка статического маршрута IPv6 с указанием следующего перехода (next-hop) выполняется командой ipv6 route в режиме глобальной конфигурации. Она указывает маршрутизатору перенаправлять трафик для определенной сети-назначения на IPv6-адрес соседнего маршрутизатора. Основной синтаксис: ipv6 route <сеть-назначения/префикс> <адрес-следующего-перехода>.

1.127 Настройка напрямую подключенного статического маршрута IPv6 (directly connected static route) заключается в указании удаленной сети и только исходящего интерфейса, без указания IP-адреса следующего перехода (next-hop). Маршрутиза-

тор считает, что получатель находится в непосредственной видимости, и использует адрес назначения пакета как следующий переход.

1.128 Полностью заданный статический маршрут IPv6 (fully specified static route) — это маршрут, в котором явно указаны и адрес следующего перехода (next-hop), и исходящий интерфейс. Он необходим, если адрес следующего перехода — это link-local адрес (fe80::/10), так как маршрутизатору нужно знать, в какой интерфейс отправить пакет.

1.129 Для проверки статических маршрутов IPv6 (преимущественно на оборудовании Cisco) используются команды: show ipv6 route (общая таблица), show ipv6 route static (только статика), show ipv6 route [адрес/префикс] (конкретный маршрут), а также ping и traceroute для проверки связности. Эти команды позволяют удостовериться в наличии маршрута, cisco.nitaet.com его типе (S — static) и корректности следующего перехода.

1.130 Настройка статического маршрута IPv6 по умолчанию (шлюза по умолчанию) заключается в указании сети ::/0 (все адреса) и адреса следующего перехода (next-hop) или выходного интерфейса. Основная команда на оборудовании Cisco: ipv6 route ::/0 {адрес_next-hop | интерфейс}. Это направляет весь неизвестный IPv6-трафик к указанному граничному маршрутизатору.

1.131 Плавающие статические маршруты настраиваются путем создания нескольких маршрутов к одной сети с разным административным расстоянием (AD). Основной маршрут имеет AD по умолчанию (1), а резервный — более высокое значение AD (например, 10–255), активируясь только при падении основного пути.

1.132 Настройка статических маршрутов хоста включает определение сети назначения, маски подсети, IP-адреса шлюза (next hop) и интерфейса выхода. В Windows маршрут добавляется командой route add, в Linux — через ip route add, а на сетевых устройствах — в меню Static Routes. Требуется указать точный IP-адрес назначения и метрику для определения приоритета.

Тема 2.7 Динамическая маршрутизация

1.132 Хронология внедрения динамических протоколов маршрутизации отражает эволюцию сетей от простых к масштабируемым (IGP/EGP). Процесс начался с RIP (1960-70-е), перешел к алгоритмам состояния канала OSPF (1989), гибридным решениям EIGRP (1990-е) и стандартизации внешнего обмена BGP (1989), обеспечивая автоматическую адаптацию к изменениям топологии.
Основные этапы внедрения:

- Конец 1960-х — 1970-е: Эра дистанционно-векторных протоколов. Появились первые протоколы, включая RIP (Routing Information Protocol), основанные на алгоритме Беллмана-Форда, которые обменивались таблицами маршрутизации целиком, что создавало высокую нагрузку.
- Конец 1980-х: Появление протоколов состояния канала. Разработан OSPF (Open Shortest Path First), использующий алгоритм Дейкстры для более быстрого и эффективного расчета путей (состояние канала), что решило проблемы медленной сходимости RIP.

- 1989 г.: Стандартизация внешних протоколов. Принят BGP (Border Gateway Protocol) для обмена маршрутной информацией между автономными системами в Интернете, ставший основой современной маршрутизации в сети.
- 1990-е: Гибридные протоколы. Cisco разрабатывает EIGRP (Enhanced Interior Gateway Routing Protocol), объединяющий преимущества дистанционно-векторных протоколов и протоколов состояния канала, обеспечивая быструю сходимость.
- Современность: Развитие протоколов для IPv6 (RIPng, OSPFv3) и расширений BGP (MP-BGP) для MPLS и VPN сетей.

1.133 Компоненты протоколов динамической маршрутизации включают механизмы обнаружения соседей, обмен информацией о топологии (объявления о состоянии каналов или таблицы маршрутизации), алгоритмы расчета кратчайшего пути (например, алгоритм Дейкстры) и базу данных маршрутов. Ключевые метрики (стоимость, пропускная способность, количество переходов) позволяют выбирать лучшие пути.

1.134 Статическая маршрутизация — это ручная настройка путей администратором, идеальная для малых, стабильных сетей (безопаснее, без нагрузки на ЦП). Динамическая маршрутизация использует протоколы (OSPF, BGP) для автоматического выбора путей и адаптации к сбоям, что необходимо в крупных, меняющихся сетях. Статика предсказуема, динамика — масштабируема.

1.135 Настройка протокола RIP на маршрутизаторе (обычно Cisco) включает активацию процесса, выбор версии 2 для поддержки масок переменной длины (VLSM), объявление напрямую подключенных сетей с помощью команды network и, при необходимости, настройку пассивных интерфейсов для защиты локальной сети от лишних обновлений, отправляемых каждые 30 секунд.
Пошаговая настройка RIPv2 (на примере Cisco)

1. Вход в режим глобальной конфигурации:
   Router> enable
   Router# configure terminal
2. Активация процесса RIP:
   Router(config)# router rip
3. Выбор версии 2 (рекомендуется):
   Использование версии 2 позволяет передавать маски подсетей (поддержка VLSM/CIDR), что эффективнее первой версии.
   Router(config-router)# version 2
4. Отключение автоматического суммирования (по желанию):
   Позволяет анонсировать подсети, а не классовые сети.
   Router(config-router)# no auto-summary
5. Объявление сетей (Network):
   Укажите сети, которые подключены непосредственно к данному маршрутизатору. RIP будет отправлять обновления через интерфейсы, попадающие в этот диапазон, и анонсировать эти сети соседям.
   Router(config-router)# network 192.168.1.0
   Router(config-router)# network 10.0.0.0
6. Настройка пассивных интерфейсов (Passive Interface):

Чтобы маршрутизатор не отправлял служебные RIP-пакеты в сеть, где нет других маршрутизаторов (например, в сторону клиентов), используйте passive-interface.
Router(config-router)# passive-interface FastEthernet0/0

1.136 Проверка протокола RIP (Routing Information Protocol) на маршрутизаторах (в основном Cisco) включает анализ таблицы маршрутизации (show ip route rip), проверку активности процессов (show ip protocols), диагностику соседей и тестирование связности. Основные метрики — количество хопов (макс. 15), административная дистанция (120).

1.137 Автоматическое суммирование в RIPv2 включается по умолчанию, а в RIPv1 — всегда активно. Для управления этой функцией в Cisco IOS используются команды в режиме настройки RIP: auto-summary (включить, по умолчанию) и no auto-summary (отключить). Отключение (no auto-summary) необходимо для передачи масок подсетей (VLSM).

1.138 Пассивные интерфейсы (passive-interface) в протоколах маршрутизации (OSPF, EIGRP, RIP) используются для предотвращения отправки приветственных сообщений (Hello) в сеть, где нет соседних маршрутизаторов, что повышает безопасность и экономит ресурсы. Настройка осуществляется в режиме конфигурации протокола командой passive-interface [интерфейс].

1.139 Распространение маршрута по умолчанию (0.0.0.0) в RIP осуществляется через объявление его соседям с использованием команды default-information originate. Маршрутизатор, имеющий статический маршрут по умолчанию, транслирует его как сеть с метрикой 1, позволяя другим узлам отправлять неизвестный трафик через него.

1.140 Таблица маршрутизации — это набор правил, определяющих путь сетевых пакетов. Каждая запись содержит сеть назначения, маску, шлюз (gateway), интерфейс и метрику. Она помогает устройству решить, куда отправить данные: напрямую в локальную сеть, через следующий роутер или по умолчанию.

1.141 Критерии обсуждения и выбора маршрутов компьютерной сети (метрики) определяют оптимальный путь для передачи данных, базируясь на таких факторах, как количество переходов (hop count), пропускная способность, задержка (latency), надежность, нагрузка на канал и стоимость передачи. Цель — обеспечить быструю и надежную доставку пакетов.

1.142 Окончательный маршрут (ultimate route) в таблице маршрутизации — это запись, содержащая всю необходимую информацию для пересылки пакета: адрес следующего перехода (next-hop) или выходной интерфейс. В отличие от родительских маршрутов, окончательные маршруты напрямую указывают, куда отправлять данные, включая прямые соединения, статические и динамические маршруты.

1.143 Маршрут 1-го уровня (Level 1 route) в таблице маршрутизации (особенно в Cisco IOS) — это «родительский» маршрут, который описывает сеть целиком, включая её классовую маску (subnet mask), но не указывает конкретный IP-адрес следующего прыжка (next-hop).?

1.144 Родительский маршрут 1-го уровня (Level 1 Parent Route) в Cisco IOS — это классовый (classful) сетевой адрес, используемый для обобщения нескольких дочерних маршрутов 2-го уровня (подсетей) с одинаковым классовым адресом. Он не содержит информации о следующем узле (next-hop) и используется только для поиска подсети

1.145 Дочерний маршрут 2-го уровня (level 2 child route) — это конечный маршрут в иерархической таблице маршрутизации (например, Cisco), указывающий на конкретную подсеть или хост, который вложен в маршрут 1-го уровня (основную сеть). Он включает маску подсети и IP-адрес следующего прыжка (next-hop) или выходной интерфейс.

1.146 Поиск маршрута IPv4 — это процесс выбора маршрутизатором наилучшего пути для доставки пакета, основанный на анализе IP-адреса назначения в таблице маршрутизации. Основной принцип — выбор маршрута с наиболее длинной маской подсети (самое точное совпадение), обеспечивающий пересылку на следующий узел (next-hop) или в прямой интерфейс.

1.147 Фраза «Оптимальный маршрут = самое длинное совпадение» (Longest Prefix Match) — это основной принцип работы сетевых маршрутизаторов, при котором из таблицы маршрутизации выбирается путь, чей сетевой префикс наиболее конкретно соответствует адресу назначения. Чем длиннее совпавшая маска подсети (больше бит), тем точнее и приоритетнее маршрут.

1.148 Анализ таблицы маршрутизации IPv6 включает проверку префиксов (сетей), следующих переходов (next-hop) и интерфейсов для обеспечения связности. Основные записи включают маршруты к локальным каналам (link-local), прямым сетям и шлюзу по умолчанию, часто с использованием префиксов длиной /64. Команды вроде netstat -r или show ipv6 route показывают адреса, метрики и интерфейсы.

1.149 Записи с прямым подключением IPv6 представляют собой 128-битные адреса, состоящие из восьми групп по четыре шестнадцатеричных цифры, разделенных двоеточиями (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Они обеспечивают уникальный публичный доступ каждому устройству без NAT, часто используя сокращения (:: для нулей) и префиксы, такие как /64 для подсетей.

1.150 Записи удаленной сети IPv6 представляют собой 128-битные адреса, разделенные на 8 групп по 4 шестнадцатеричных цифры (гекстета), например, 2001:0db8:0000:0042:0000:8a2e:0370:7334. Для удобства ведущие нули в группах опускаются, а подряд идущие нулевые группы заменяются двойным двоеточием ::, которое можно использовать в записи только один раз.

Тема 2.8 Протокол DHCP

1.151 DHCP (Dynamic Host Configuration Protocol) — это сетевой протокол, автоматизирующий выдачу IP-адресов, масок подсети, шлюзов и DNS-серверов устройствам. Он устраняет необходимость ручной настройки, снижает риск конфликтов

IP-адресов и упрощает управление крупными сетями, обеспечивая динамическое переиспользование адресов.

1.152 Операции DHCP (Dynamic Host Configuration Protocol) — это процесс автоматического назначения IP-адресов, известный как DORA (Discovery, Offer, Request, Acknowledgement). Он включает четыре основных этапа: обнаружение сервера, предложение адреса, запрос на использование и подтверждение аренды.

1.153 Первоначальная аренда IP-адреса через DHCP — это четырехэтапный процесс, известный как DORA (Discover, Offer, Request, Acknowledgement), который позволяет устройству автоматически получить сетевые настройки. Клиент отправляет широковещательный запрос, выбирает предложение сервера, подтверждает его и получает конфигурацию (IP, маска, шлюз, DNS) на определенный срок аренды.

1.154 Продление аренды DHCP-адреса происходит автоматически. По истечении 50% срока аренды (T1) клиент отправляет серверу запрос DHCPREQUEST. Если сервер доступен, он подтверждает продление сообщением DHCPACK, и таймер обновляется. Если сервер не ответил к 87,5% срока (T2), клиент ищет любой другой сервер (REBINDING). 1.155 Опишите формат сообщений DHCPv4.

1.156 Сообщения DHCPv4 Discover и Offer — это первые два шага процесса DORA для автоматического получения IP-адреса. Discover (клиент -> сервер) — это широковещательный запрос устройства на поиск DHCP-сервера, а Offer (сервер -> клиент) — ответное сообщение с предложением свободных сетевых настроек (IP, маска, шлюз).

1.157 Настройка базового DHCPv4-сервера включает установку роли (или службы), определение пула адресов (диапазона), указание маски подсети, шлюза по умолчанию и DNS-серверов. Ключевые шаги: создание области, исключение статических адресов, настройка времени аренды и активация службы.

1.158 Проверка работы DHCPv4 (процесс DORA) — это четырехэтапный обмен сообщениями: Discover (клиент ищет сервер), Offer (сервер предлагает IP), Request (клиент принимает), ACK (сервер подтверждает). Проверка настройки включает использование команд ipconfig /all на клиенте и show ip dhcp binding на сервере (Cisco).

1.159 DHCPv4-ретрансляция (DHCP Relay) позволяет клиентам получать IP-адреса от сервера в другой подсети. Маршрутизатор (агент) перехватывает широковещательный DHCP-запрос, преобразует его в одноадресный (unicast) пакет и пересылает на удаленный DHCP-сервер, указывая в поле giaddr адрес своего интерфейса для выбора пула адресов.

1.160 Настройка маршрутизатора Cisco в качестве DHCPv4-клиента (например, для получения IP от провайдера) выполняется командой ip address dhcp в режиме настройки интерфейса. Это автоматически назначает интерфейсу IP-адрес, маску подсети и шлюз по умолчанию.

1.161 Проверка настроек DHCPv4 на маршрутизаторе обычно выполняется через веб-интерфейс в разделе «LAN»/«Network» или командами CLI. На оборудовании

Cisco используйте show ip dhcp binding (список арендованных адресов), show ip dhcp pool (настройки пула) и show run | section dhcp для просмотра конфигурации.

1.162 SLAAC (Stateless Address Autoconfiguration) — это метод автоматической настройки IPv6-адреса хостом без участия DHCPv6-сервера. Процесс основан на сообщениях протокола ICMPv6: хост запрашивает параметры у маршрутизатора (RS), получает префикс сети в объявлениях (RA) и самостоятельно генерирует уникальный идентификатор интерфейса (EUI-64 или случайный) для формирования полного адреса.

1.163 Настройка DHCPv6 включает создание пула IPv6-адресов, DNS-серверов и доменных имен на сервере, а также настройку маршрутизатора для отправки сообщений RA (Router Advertisement) с флагами «Managed» (M=1 для Stateful) или «Other» (O=1 для Stateless). Это обеспечивает автоматическое назначение адресов (Stateful) или только параметров (Stateless) клиентам.

1.164 EUI-64 (Extended Unique Identifier) — это 64-битный формат идентификатора, используемый в IPv6 для автоматического создания уникального адреса устройства (interface ID) на основе его 48-битного MAC-адреса. Он позволяет устройству самостоятельно генерировать вторую половину IPv6-адреса (последние 64 бита), вставляя FFFE в середину MAC-адреса и инвертируя 7-й бит.

Тема 2.9 Преобразование сетевых адресов

1.165 Максимально возможное число уникальных IPv4-адресов составляет 2^{32}, что равно 4 294 967 296 (примерно 4,3 миллиарда) комбинаций. Этот 32-битный формат определяет весь пул публичных адресов, однако значительная их часть зарезервирована для специальных нужд (локальные, частные, мультикаст-адреса) и не используется в глобальном интернете.

1.166 Публичные IPv4-адреса регистрируются и распределяются иерархически через региональные интернет-регистраторы (RIR), такие как RIPE NCC (Европа, РФ), ARIN (Северная Америка) и другие, которые получают их от корпорации ICANN. Конечные пользователи получают адреса у интернет-провайдеров (ISP) или облачных провайдеров.

1.167 Частные (приватные) IPv4-адреса — это диапазоны, зарезервированные для локальных сетей (не маршрутизируемые в интернете), определенные в RFC 1918. Они включают три основных блока: 10.0.0.0/8 (10.0.0.0 – 10.255.255.255), 172.16.0.0/12 (172.16.0.0 – 172.31.255.255) и 192.168.0.0/16 (192.168.0.0 – 192.168.255.255). Также используется блок для CGN 100.64.0.0/10.

1.168 NAT (Network Address Translation, «преобразование сетевых адресов») — это технология на роутерах и шлюзах, которая подменяет частные IP-адреса локальной сети на один публичный внешний IP-адрес для выхода в интернет. Она решает нехватку IPv4-адресов, позволяя сотням устройств работать через один адрес, а также обеспечивает базовую безопасность, скрывая внутреннюю структуру сети.

1.169 В терминологии NAT (Network Address Translation) выделяют 4 основных типа адресов, описывающих преобразование частных IP-адресов локальной сети в публичные адреса интернета: Inside Local, Inside Global, Outside Local и Outside

Global. Они обеспечивают маскировку внутренних узлов и маршрутизацию трафика.

4 типа адресов NAT

1. Inside Local Address (Внутренний локальный)
    1) Характеристика: IP-адрес, присвоенный узлу во внутренней (частной) сети, например, из диапазона 192.168.x.x или 10.x.x.x.
    2) Особенность: Этот адрес не маршрутизируется в интернете и виден только внутри локальной сети.
2. Inside Global Address (Внутренний глобальный)
    1) Характеристика: Публичный IP-адрес, зарегистрированный у провайдера, который представляет внутренний узел во внешней сети (интернете).
    2) Особенность: Именно этот адрес видят внешние ресурсы (веб-сайты, сервера) как адрес источника запроса.
3. Outside Global Address (Внешний глобальный)
    1) Характеристика: Реальный, публичный IP-адрес узла, находящегося за пределами локальной сети (в интернете).
    2) Особенность: Это адрес назначения, с которым хочет связаться внутренний узел.
4. Outside Local Address (Внешний локальный)
    1) Характеристика: IP-адрес внешнего узла, каким он представляется локальной сети.
    2) Особенность: В большинстве случаев (если не используется специфический NAT) Outside Local совпадает с Outside Global, так как внешний узел уже имеет реальный IP.

1.170 NAT (Network Address Translation) — это технология на маршрутизаторах, подменяющая частные IP-адреса локальной сети на один публичный при выходе в интернет. Она позволяет множеству устройств работать через один внешний IP, экономя адресное пространство IPv4 и скрывая внутреннюю сеть, обеспечивая безопасность.

1.171 Основные механизмы преобразования сетевых адресов (NAT) включают статическую трансляцию (Static NAT, 1:1), динамическую трансляцию (Dynamic NAT, N:M) и маскарадинг (PAT/NAPT, N:1 с портами). Они позволяют использовать частные IP-адреса для выхода в интернет через один или несколько публичных адресов, обеспечивая экономию ресурсов.

1.172 Статический NAT (Static Network Address Translation) — это метод трансляции сетевых адресов, обеспечивающий постоянное, фиксированное сопоставление один-к-одному (1:1) между частным (внутренним) IP-адресом и публичным (внешним) IP-адресом. В отличие от динамического NAT, этот адрес не меняется, что позволяет внешним пользователям инициировать соединения с внутренним узлом напрямую.

1.173 Динамическое преобразование NAT (Dynamic Network Address Translation) — это технология, автоматически сопоставляющая внутренние частные IP-адреса с публичными адресами из заранее определенного пула (группы). В отличие от статического NAT, здесь используется принцип «многие ко многим»: устройство вре-

менно занимает свободный публичный адрес из пула для выхода в интернет на время сессии.

1.174 Преобразование адресов портов (PAT, Port Address Translation или NAT с перегрузкой) — это сетевая технология, позволяющая множеству устройств из частной локальной сети выходить в Интернет через один публичный IP-адрес. Маршрутизатор заменяет внутренние адреса и номера портов на свой внешний IP-адрес и уникальный порт, отслеживая соединения для корректной доставки ответов.

175 NAT (Network Address Translation) и PAT (Port Address Translation) — технологии преобразования адресов, где NAT часто заменяет один IP-адрес на другой (1:1), а PAT (разновидность NAT) позволяет множеству внутренних устройств использовать один внешний IP-адрес, добавляя уникальные номера портов, что критично для экономии IPv4-адресов

176 Преобразование сетевых адресов (NAT) позволяет использовать один публичный IPv4-адрес для доступа в интернет множеству устройств, экономя дефицитные адреса, скрывает внутреннюю структуру сети, повышая ее безопасность, и упрощает администрирование, устраняя необходимость перенумерации хостов при смене провайдера.

177 Преобразование сетевых адресов (NAT) обеспечивает экономию IPv4-адресов и безопасность, но имеет ряд серьезных недостатков: увеличивает задержки из-за обработки пакетов, нарушает сквозную связность (end-to-end), затрудняет работу P2P-приложений, VoIP и VPN (IPsec), а также усложняет трассировку и диагностику сети.

178 Настройка статического NAT (Static NAT) включает создание постоянного соответствия между внутренним частным IP-адресом (Inside Local) и внешним публичным адресом (Inside Global), а также определение интерфейсов маршрутизатора как внутренних и внешних. Это позволяет устройствам из интернета инициировать соединения с серверами во внутренней сети.

179 Проверка статического NAT (Static NAT) выполняется через консоль маршрутизатора с помощью команд, отображающих таблицу трансляций и статистику, а также через внешние проверки доступности. Основные методы включают использование команд show ip nat translations (на Cisco) и проверку связи (ping, telnet) с публичного IP на внутренний ресурс.

180 Настройка динамического NAT (Dynamic NAT) на устройствах Cisco включает создание пула публичных IP-адресов, определение внутренних хостов через ACL, связывание их между собой и указание внешнего/внутреннего интерфейсов. Это позволяет автоматически назначать свободный адрес из пула внутренним пользователям при выходе в интернет.

181 Динамический NAT — это технология преобразования сетевых адресов, использующая пул публичных IP-адресов для назначения внутренним узлам. Адреса выдаются автоматически по принципу «первым пришел, первым обслужен» (FIFO). Анализ включает мониторинг таблицы трансляций, пула адресов, времени жизни сессий и использование ACL для выбора трафика.

182 Проверка динамического NAT (PAT) выполняется путем анализа активных трансляций на маршрутизаторе и проверки связности изнутри сети. Основные команды на оборудовании Cisco: show ip nat translations (активные трансляции) и show ip nat statistics (статистика пула). Необходимо убедиться, что локальные IP преобразуются в публичные из заданного пула.

183 Настройка PAT (Port Address Translation) с пулом общедоступных адресов (Dynamic NAT с перегрузкой) включает создание пула внешних IP, определение разрешенной внутренней сети через ACL и привязку их на внешнем интерфейсе. Это позволяет множеству внутренних хостов выходить в интернет через ограниченный набор публичных IP-адресов.

184 Настройка PAT (Port Address Translation или PAT/NAT Overload) для одного публичного IPv4-адреса позволяет множеству локальных устройств выходить в интернет через один внешний IP. Основные шаги включают настройку интерфейсов (внешнего и внутреннего), создание списка доступа (ACL) для определения трафика и активацию перегрузки NAT.

185 Port Address Translation (PAT), или «NAT перегрузка», — это технология, позволяющая множеству локальных устройств (с частными IP) выходить в интернет через один публичный IP-адрес, преобразуя IP-адреса и номера портов TCP/UDP. Она сохраняет дефицитные IPv4-адреса, обеспечивая безопасность сети за счет скрытия внутренней структуры.
Основные аспекты анализа PAT

- Принцип работы: Когда пакет выходит из внутренней сети, маршрутизатор заменяет частный IP-адрес на публичный, а исходный порт — на уникальный порт из своего пула, фиксируя это в таблице трансляций.
- Таблица трансляций: Маршрутизатор хранит записи: [Внутренний IP : Внутренний порт] <-> [Внешний IP : Внешний порт]. Это позволяет правильно вернуть ответный пакет нужному узлу.
- Емкость: Теоретически один публичный IP-адрес может обслуживать до 65 536 одновременных сессий, так как порт описывается 2 байтами. Однако на практике из-за ограничений процессора и ОЗУ маршрутизатора это число меньше.
- Типы PAT: Может работать с одним публичным IP или пулом IP-адресов, предоставленных провайдером.
- Преимущества: Экономия адресов, безопасность (внешние хосты не знают адресов внутренней сети), прозрачность для пользователей.

Анализ работы PAT включает проверку таблицы NAT (show ip nat translations на Cisco) для отслеживания соответствия локальных портов внешним.

186. Проверка протокола трансляции адресов PAT (Port Address Translation/NAT Overload) выполняется путем анализа таблицы трансляций на сетевом оборудовании (маршрутизатор, межсетевой экран). Ключевой инструмент — команды CLI (show ip nat translations), которые позволяют увидеть, какой внутренний IP: порт отображаются во внешний IP: порт.

187 Port forwarding (проброс портов) — это механизм перенаправления входящего трафика из интернета с определенного порта роутера на конкретное устройство в

локальной сети. Технология позволяет сделать домашние сервисы (веб-серверы, IP-камеры, игры, удаленный рабочий стол) доступными из любой точки мира через интернет

188 В IPv6 технология NAT (Network Address Translation) технически не является необходимой из-за колоссального адресного пространства, устраняющего дефицит IP-адресов. В отличие от IPv4, где NAT маскирует устройства для экономии, в IPv6 каждое устройство получает уникальный публичный адрес, обеспечивая прямую связь. NAT в IPv6 используется редко, в основном для обеспечения безопасности или специфических сетевых переходов.

Тема 2.10 Создание и настройка небольшой компьютерной сети

189 При выборе сетевых устройств (маршрутизаторов, коммутаторов, точек доступа) необходимо учитывать цели сети, производительность (скорость, порты), надежность, безопасность и возможности масштабирования. Также критически важны совместимость с текущей инфраструктурой, возможность удаленного управления и бюджет на внедрение и обслуживание.

190 Сетевые устройства (маршрутизаторы, коммутаторы, адаптеры) должны обеспечивать установление соединения, передачу данных, их обработку и защиту. К основным функциям относятся коммутация и маршрутизация пакетов, усиление сигналов, управление трафиком, обеспечение информационной безопасности, а также конфигурация сети, диагностика неисправностей и поддержка работы с различными сетевыми протоколами.

191 При проектировании схемы IP-адресации необходимо учитывать критически важные устройства, требующие статических адресов (серверы, маршрутизаторы, принтеры), и динамические устройства пользователей (ноутбуки, телефоны, IoT), обслуживаемые DHCP. Схема должна обеспечивать уникальность адресов, поддерживать сегментацию сетей (VLAN) и масштабируемость.

192 Планирование резервирования компьютерной сети включает дублирование критических узлов (маршрутизаторов, коммутаторов), организацию резервных каналов связи от разных провайдеров и внедрение протоколов автоматического переключения (HSRP/VRRP). Основные этапы: анализ рисков, выбор уровня резервирования (N+1, 2N), настройка мониторинга и регулярное тестирование переключений для обеспечения непрерывности бизнес-процессов.

193 Для небольшой сети (офис, дом) необходимы базовые протоколы для связности, безопасности и управления IP-адресами: TCP/IP (основа), DHCP (автоматическая настройка IP), DNS (имена сайтов), HTTPS/TLS (безопасный веб), SMB (общие файлы) и Wi-Fi протоколы (WPA2/3). Приложения включают браузеры, файловые менеджеры, почтовые клиенты и VPN.

194 Для масштабирования сети (увеличения её пропускной способности и производительности) необходимы балансировщики нагрузки, дополнительные вычислительные мощности (CPU, RAM), скоростные сетевые интерфейсы, хранилища дан-

ных (SSD/NVMe) и гибкая архитектура, поддерживающая горизонтальное (добавление серверов) или вертикальное (увеличение мощности) расширение.

195 Обеспечение сетевой безопасности требует многоуровневого подхода: использования межсетевых экранов (firewalls), систем обнаружения вторжений (IDS/IPS), шифрования данных (VPN, SSL), регулярного обновления ПО, настройки многофакторной аутентификации (MFA) и сегментации сети. Ключевые меры включают смену паролей по умолчанию, ограничение прав доступа и постоянный мониторинг трафика.

196 Команда ping — это инструмент диагностики сети, используемый для проверки связи с удаленным узлом (сайтом, IP-адресом) путем отправки эхо-запросов (пакетов данных). Она измеряет время ответа в миллисекундах (мс) и показывает потерю пакетов. Используется в командной строке (cmd в Windows, Terminal в Linux/macOS) командой ping <адрес>.197 Как протестировать виртуальный интерфейс loopback?

198 Команды tracert (Windows) и traceroute (Linux/macOS) используются для отслеживания пути пакетов до целевого узла (сайта или IP), показывая каждый промежуточный маршрутизатор (хоп) и время отклика. В Windows введите tracert domain.com в командной строке, в Linux/macOS — traceroute domain.com в терминале.

199 Команда show — это универсальный инструмент для просмотра настроек, состояния и статистики системы. Чаще всего она встречается в сетевых технологиях (Cisco, Juniper, D-Link) и базах данных (MySQL, PostgreSQL).

200 Команда ipconfig в Windows используется для отображения и обновления текущей сетевой конфигурации (IP-адреса, маски подсети, шлюза). Введите ipconfig в командной строке для быстрого просмотра адресов или ipconfig /all для детальной информации, включая DNS и MAC-адреса. Основные ключи: /release (освободить IP) и /renew (получить новый).

201 Команда arp (Address Resolution Protocol) используется для отображения и управления кэш-таблицей, содержащей соответствия IP-адресов физическим MAC-адресам устройств в локальной сети. Она позволяет просматривать, добавлять или удалять записи, помогая диагностировать проблемы с подключением, обнаруживать конфликты IP-адресов и проверять доступность узлов.

202 Команда show cdp neighbors используется на устройствах Cisco для обнаружения и отображения информации о соседних устройствах, подключенных напрямую.

203 Команда show ip interface brief (или сокращенно sh ip int br) используется в консоли Cisco IOS для быстрого просмотра состояния всех сетевых интерфейсов, их IP-адресов, статуса (up/down) и метода настройки. Это лучший инструмент для диагностики подключений на 3-м уровне модели OSI.

204 Команда debug (debug.exe) — это отладчик MS-DOS, используемый для проверки, редактирования и исполнения бинарных файлов, а также работы с памятью и регистрами процессора. Она запускается из командной строки (Win+R -> debug),

предоставляя приглашение -, где используются однобуквенные команды (например, d — дамп, r — регистры, u — дизассемблирование).

205 Команда terminal monitor используется на сетевом оборудовании (преимущественно Cisco, Huawei) для вывода системных сообщений, журналов (logs) и результатов отладки (debug) непосредственно в текущую сессию SSH/Telnet. По умолчанию при удаленном подключении сообщения часто скрыты.

206 Шесть шагов поиска и устранения неполадок включают: 1) определение симптомов (сбор информации), 2) выявление причин (формирование гипотез), 3) составление плана действий, 4) реализацию решения, 5) проверку работоспособности системы и 6) документирование проблемы и принятых мер. Этот подход систематизирует работу, повышая эффективность диагностики.

207 Несовпадение дуплексных режимов (например, Full Duplex на одной стороне и Half Duplex на другой) приводит к резкому падению скорости сети, высокой задержке и появлению большого количества ошибок передачи, таких как коллизии и битые кадры. Связь становится нестабильной: работает, но крайне медленно.

208 Основные проблемы с IP-адресами на устройствах включают конфликты (два устройства с одинаковым адресом), сбои DHCP-сервера при автоматическом получении, неправильную настройку статических параметров и блокировку IP-адреса провайдером или веб-сайтами. Это приводит к отсутствию интернета, невозможности подключиться к локальной сети или умному дому.

209 Неполадки со шлюзом по умолчанию (обычно роутером) приводят к отсутствию интернета при работающей локальной сети. Основные причины: сбои DHCP-сервера, неправильные IP-настройки, устаревшие драйверы, зависание роутера или конфликты в реестре Windows. Ошибка проявляется как «Шлюз, установленный по умолчанию, не доступен».

210 Проблемы с DNS («DNS-сервер не отвечает», «не удается найти IP-адрес») приводят к невозможности открыть сайты при рабочем интернете. Основные причины: сбои у провайдера, некорректные настройки роутера/ОС, поврежденный локальный кэш, блокировка антивирусом или атаки (спуфинг, отравление кэша). Чаще всего лечится очисткой кэша, сменой DNS или перезагрузкой сети.