

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ  
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ

«ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт математики и информационных систем  
Факультет автоматики и вычислительной техники  
Кафедра систем автоматизации управления

А. И. СТАРИКОВ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К КУРСОВОЙ РАБОТЕ ПО  
ДИСЦИПЛИНЕ

## **ГЛОБАЛЬНЫЕ СЕТИ**

Методические указания к курсовой работе

Киров

2018

УДК 004.738.1 (07)

С254

Допущено к изданию методическим советом факультета автоматики и вычислительной техники ВятГУ в методических указаний к курсовой работы по дисциплине «Глобальные сети» для студентов направления 27.03.04 «Управление в технических системах» всех форм обучения

Рецензент:

кандидат технических наук, доцент кафедры экономики Петров И.Е.

**Стариков, А. И.**

С254 Глобальные сети: Методические указания / А. И. Стариков. – Киров: ВятГУ, 2018. – 60 с.

УДК 004.738.1 (07)

Методические указания предназначены для выполнения курсовой работы по дисциплине «Глобальные сети».

Авторская редакция

Тех. редактор Е. О. Гладких

## Оглавление

|   |    |
|---|----|
| ВВЕДЕНИЕ .....  | 3  |
| КУРСОВОЙ РАБОТЕ .....                                   | 12 |
| 2.1 Педагогический адрес .....                          | 12 |
| 2.2 Анализ учебной документации .....                   | 12 |
| 2.3 Программно-технические средства .....               | 13 |
| 2.4 Структура и содержание курсовой работы .....        | 22 |
| 2.4.1 Введение к курсовой работе .....                  | 22 |
| 2.4.2 Анализ инфраструктуры предприятия .....           | 25 |
| 2.4.3 Проектирование логической схемы предприятия ..... | 28 |
| 2.4.4 Виртуализация серверной части .....               | 41 |
| СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....                  | 48 |

## ВВЕДЕНИЕ

Технологии компьютерных коммуникаций изучаются студентами направления подготовки 27.03.04 Управление в технических системах. Будущие бакалавры должны уметь проектировать корпоративные компьютерные сети, выполнять анализ их стоимости и владеть технологиями виртуализации. Курсовая работа по дисциплине «Глобальные сети» обобщает все знания и умения в области сетевого и системного администрирования,

полученные студентами после изучения дисциплин «Операционные системы», «Локальные сети».

Актуальность работы обусловлена тем, что, выполняя курсовую работу, студенты должны применить все полученные ранее знания в едином, сложном и практико-ориентированном проекте. Такой проект возможен, во-первых, за счет применения современных программных средств виртуализации операционных систем и симуляции работы сетевого оборудования и, во-вторых, благодаря применению современных педагогических технологий, таких как метод проектов, в котором симулируется работа отдела информационных технологий.

Выполнение данной курсовой работы, в отличие от проанализированных аналогов, формирует не только умения, которые используются при построении больших сетей, но и умения презентовать, обосновать и убедить заказчика в целесообразности проекта.

# 1. ОПИСАНИЕ СЕТЕВЫХ ТЕХНОЛОГИЙ В КОРПОРАТИВНОЙ СРЕДЕ

**VLAN** (Virtual Local Area Network) — виртуальная локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к ширококвещательному домену, независимо от их физического местонахождения.

Виртуальные локальные сети имеют те же свойства, что и физические, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств [30].

Виртуальные локальные сети применяются для уменьшения ширококвещательного трафика в сети.

**VTP** — разработанный компанией «Cisco» протокол. Данный протокол сокращает необходимость администрирования VLAN в коммутируемых сетях [14]. Протокол работает по модели «клиент-сервер». При создании новой виртуальной локальной сети на сервере VTP, информация о созданных

VLAN распространяется на все коммутаторы в домене.

**STP** (Spanning Tree Protocol) — семейство сетевых протоколов, предназначенных для автоматического удаления петель коммутации из топологии сети на канальном уровне. Первоначальный протокол STP описан в стандарте 802.1D. Позже появилось несколько новых протоколов RSTP, MSTP, PVST, PVST+, отличающихся некоторыми особенностями в алгоритме работы, в скорости, в отношении к виртуальным локальным сетям и ряде других вопросов. Все их принято обобщённо называть STP-протоколами [25].

Функция **EtherChannel** позволяет объединить несколько физических каналов в один логический канал. Это дает возможность распределения

трафика в логическом канале по физическим каналам и возможность резервирования в случае сбоя одного или нескольких физических каналов в логическом канале. EtherChannel может использоваться для соединения друг с другом коммутаторов локальных сетей, маршрутизаторов, серверов, клиентов через кабель из неэкранированной витой пары или оптоволоконными кабелями [1].

**Маршрутизация** — процесс определения лучшего пути, по которому пакет может быть доставлен получателю. Возможные пути передачи пакетов называются маршрутами. Лучшие маршруты к известным получателям хранятся в таблице маршрутизации. В зависимости от способа заполнения таблицы маршрутизации, различают два вида маршрутизации [7].

**Статическая маршрутизация** — вид маршрутизации, при котором маршруты вручную указываются администратором при настройке маршрутизатора [20].

**Динамическая маршрутизация.** При динамической маршрутизации происходит обмен маршрутной информацией между соседними маршрутизаторами, в ходе которого они сообщают друг другу, какие сети в данный момент доступны через них. К наиболее распространенным внутренним протоколам маршрутизации относятся:

- **RIP (Routing Information Protocol)** — протокол маршрутной информации;
- **OSPF (Open Shortest Path First)** — протокол выбора кратчайшего маршрута;
- **EIGRP (Enhanced Interior Gateway Routing Protocol)** — усовершенствованный протокол маршрутизации внутреннего шлюза [3].

**DHCP (Dynamic Host Configuration Protocol)** — протокол динамической настройки узла. Сетевой протокол, позволяющий компьютерам автоматически

получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. [25].

**NAT** (Network Address Translation) — преобразование сетевых адресов. Это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов [27].

NAT позволяет «серым» сетям подключаться к Интернету. Преобразование сетевых адресов преобразует серые адреса во внутренней сети в белые адреса перед отправкой пакетов в Интернет. Это обеспечивает дополнительную безопасность и позволяет скрыть внутреннюю сеть от доступа извне.

Маршрутизаторы компании «Cisco» поддерживает несколько разновидностей NAT.

**Статический NAT** — Отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному. Применяется, когда устройство должно быть доступным снаружи сети.

**Динамический NAT** — Отображает незарегистрированный IP-адрес на зарегистрированный адрес из группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

**Перегруженный NAT** — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

**VPN** — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений) [6].

О моделировании VPN-технологий существует достаточное количество учебных пособий, однако большинство из них нацелены либо на демонстрацию применения виртуальных частных сетей в упрощенных ситуациях [16], либо на студентов-«новичков» [2].

Можно выделить три фундаментальных свойства, превращающих наложенную корпоративную сеть, построенную на базе мультисервисной сети, в виртуальную частную сеть:

- шифрование;
- аутентификация (защита от несанкционированного доступа);
- контроль доступа.

Только реализация всех этих трех свойств позволяет защитить пользовательские машины, серверы предприятия и данные, передаваемые по



физически незащищенным каналам связи, от внешних нежелательных вторжений, утечки информации и несанкционированных действий.

**Site-to-Site VPN** идеально подходит для связи центрального офиса компании с ее филиалами. Виртуальный канал позволяет связать локальные компьютерные сети офисов и организовать несколько каналов связи, в том числе для доступа в Интернет.

**Remote Access VPN** — Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или с компьютера общественного пользования.

**DNS** (Domain Name System) — система доменных имён. Компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста, получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене.

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

Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу, что позволяет возложить ответственность за актуальность информации на серверы различных организаций, отвечающих только за «свою» часть доменного имени

**SSH** — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCPсоединений (например, для передачи файлов). Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов

шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем [21].

SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через командную оболочку, но и передавать по зашифрованному каналу звуковой поток или видео.

**VLSM** (variable length subnet masks) — сетевые маски переменной длины. Используются в бесклассовой маршрутизации для задания масок сетей. Например, 4 сети класса C (4 \* 255 адресов, маска 255.255.255.0 или /24) могут быть объединены в одну сеть /22. Кроме того сети можно разбивать на более мелкие подсети [24].

По сравнению с обычной (классовой) системой адресации, VLSM разрешает использование подсетей, с номерами, состоящими из всех нулей или единиц (в двоичной форме). Возможно применение различных масок подсетей к различным подсетям. Появляется возможность использования подподсетей (подсетей в подсетях).

**CIDR** (Classless Inter-Domain Routing) — Бесклассовая междоменная маршрутизация. Появление этой технологии было вызвано резким увеличением объема трафика в Internet и, как следствие, увеличением количества маршрутов на магистральных маршрутизаторах. Так, если в 1994 году, до развертывания CIDR, таблицы маршрутизаторов содержали до 70 000 маршрутов, то после внедрения их количество сократилось до 30 000. На сентябрь 2002, количество маршрутов перевалило за отметку 110 000, технология CIDR предназначена для их оптимизации.

Она позволяет уйти от классовой схемы адресации, эффективней использовать адресное пространство протокола IP. Кроме того, CIDR позволяет агрегировать маршрутные записи. Одной записью в таблице маршрутизатора описываются пути ко многим сетям.

Суть технологии CIDR состоит в том, что каждому поставщику услуг Internet (или, для корпоративных сетей, какому-либо структурнотерриториальному подразделению) должен быть назначен неразрывный диапазон IP-адресов. При этом вводится понятие обобщенного сетевого префикса, определяющего общую часть всех назначенных адресов. Соответственно, маршрутизация на магистральных каналах может реализовываться на основе обобщенного сетевого префикса. Результатом является агрегирование маршрутных записей, уменьшение размера таблиц маршрутных записей и увеличение скорости обработки пакетов.

**Wi-Fi** (Wireless Fidelity) — торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

## **2 ОПИСАНИЕ МЕТОДИЧЕСКИХ УКАЗАНИЙ К КУРСОВОЙ РАБОТЕ**

### **2.1 Педагогический адрес**

Курсовая работа «Компьютерные коммуникации и сети» предназначена для студентов четвертого курса направления подготовки 27.03.04 «Управление в технических системах».

### **2.2 Анализ учебной документации**

Учебная дисциплина «Глобальные сети» включена в учебный план по подготовке бакалавров по направлению 27.03.04 «Управление в технических системах». Дисциплина «Глобальные сети» входит в вариативную часть дисциплин профессионального цикла ФГОС по направлению подготовки 27.03.04 «Управление в технических системах».

Целью освоения дисциплины является знакомство с различными сетевыми технологиями, а также спецификой их использования в различных видах профессиональной деятельности.

Предлагаемый курс обучения предназначен для формирования у студентов представления о назначении и возможностях компьютерных коммуникациях и сетях различных типов и умений их эффективного применения в профессиональной деятельности.

На практических занятиях работа студентов предусматривает формирование умения использования основных свойств сетей и серверов, навыков практического использования данных знаний для решения различных прикладных задач.

На выполнение курсовой работы по дисциплине «Глобальные сети» студенту отводится 70 часов (таблица 2).

Таблица 2 — Объем дисциплины и виды учебной работы

|   | Очная   | Заочная |
|---|---------|---------|
| Общая трудоемкость дисциплины                   | 8(288)  | 8(288)  |
| Самостоятельная работа                          | 162     | 256     |
| Написание и подготовка к защите курсовой работы | 70      | 90      |
| Вид итогового контроля                          | экзамен | экзамен |

## 2.3 Программно-технические средства

**Cisco Packet Tracer** — симулятор сети передачи данных, выпускаемый фирмой Cisco Systems. Позволяет делать работоспособные модели сети, настраивать (командами Cisco IOS) маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями (через облако). В симуляторе реализованы серии маршрутизаторов Cisco 800, 1800, 1900, 2600, 2800, 2900 и коммутаторов Cisco Catalyst 2950, 2960, 3560, а также межсетевой экран ASA 5505. Беспроводные устройства представлены маршрутизатором Linksys WRT300N, точками доступа и сотовыми вышками. Кроме того, есть серверы DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP и EMAIL, рабочие станции, различные модули к компьютерам и маршрутизаторам, IPфоны, смартфоны, хабы, а также облако, эмулирующее WAN. Объединять сетевые устройства можно с помощью различных типов кабелей, таких как прямые и обратные патч-корды, оптические и коаксиальные кабели, последовательные кабели и телефонные пары [22].

Успешно позволяет создавать даже сложные макеты сетей, проверять на работоспособность топологии. Однако, стоит заметить, что реализованная

функциональность устройств ограничена и не предоставляет всех возможностей реального оборудования. Cisco Packet Tracer доступен бесплатно для участников Программы Сетевой Академии Cisco.

Cisco Packet Tracer — это симулятор сети, созданный компанией Cisco, оборудование которой используется на крупных предприятиях в построении корпоративных сетей. Данное приложение позволяет строить сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов. В Cisco Packet Tracer можно симулировать построение не только логической, но и физической модели сети и, следовательно, получать навыки проектирования. Схему сети можно наложить на чертеж реально существующего здания или даже города и спроектировать всю его кабельную проводку, разместить устройства в тех или иных зданиях и помещениях с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети. Благодаря такому свойству, как режим визуализации, обучаемые могут отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов, проанализировать события, происходящие в сети, что позволит понять механизм ее работы и обнаружить неисправности. Симуляция, визуализация, и возможность проектирования делают Cisco Packet Tracer уникальным инструментом для обучения сетевым технологиям. Данную программу целесообразно изучать в рамках дисциплины «Компьютерные коммуникации и сети».

**Hyper-V.** Технология виртуализации Hyper-V включена во многие версии Windows 10. Hyper-V позволяет запускать виртуализированные компьютерные системы поверх физического узла. Эти виртуализированные системы можно использовать и контролировать как физические компьютерные системы, но они находятся в виртуализированной и изолированной среде. Специальное программное обеспечение, называемое

низкоуровневой оболочкой, управляет доступом между виртуальными системами и физическими аппаратными ресурсами. Виртуализация обеспечивает быстрое развертывание компьютерных систем, быстрое восстановление системы до предыдущего рабочего состояния и возможность миграции систем между физическими узлами.

Виртуализация позволяет запускать несколько операционных систем, программных и аппаратных конфигураций на одном физическом компьютере. Hyper-V предоставляет как виртуализацию, так и инструменты для управления виртуальными машинами.

Hyper-V можно использовать несколькими способами.

Запуск программного обеспечения, для которого требуются более старые версии Windows или операционные системы, отличные от Windows.

Эксперименты с другими операционными системами. Hyper-V существенно упрощает создание и удаление различных операционных систем.

Тестирование программного обеспечения в нескольких операционных системах с помощью нескольких виртуальных машин. Благодаря Hyper-V их можно запускать на настольном компьютере или ноутбуке. Эти виртуальные машины можно экспортировать, а затем импортировать в любую другую систему Hyper-V, включая Azure.

Устранение неполадок с виртуальными машинами из любого развертывания Hyper-V. Вы можете экспортировать виртуальную машину из рабочей среды, открыть ее на настольном компьютере с Hyper-V, устранить неполадки виртуальной машины и экспортировать ее обратно в рабочую среду.

С помощью виртуальных сетей можно создать среду из нескольких машин для тестирования, разработки или демонстрации и не беспокоиться о воздействии на рабочую сеть.

Требования к системе. Hyper-V доступен только в Windows 8 Профессиональная, Windows 8 Корпоративная, Windows 8 для образовательных учреждений и более поздних версиях ОС. Для Hyper-V требуется 64разрядная система с функцией преобразования адресов второго уровня (SLAT). Она есть в текущем поколении 64-разрядных процессоров Intel и AMD. Необходимо использовать 64-разрядную версию ОС Windows. При этом в виртуальных машинах Hyper-V поддерживает 32-разрядные и 64разрядные операционные системы. На узле, имеющем 4 ГБ оперативной памяти, можно запустить три-четыре базовые виртуальные машины, однако для большего числа виртуальных машин потребуется больше ресурсов. Кроме того, можно создать мощные виртуальные машины с 32 процессорами и 512 ГБ ОЗУ в зависимости от оборудования.

Hyper-V в Windows поддерживает много гостевых операционных систем, в том числе различные выпуски Linux, FreeBSD и Windows. Напоминаем, что необходимо иметь действующую лицензию на все операционные системы, используемые на виртуальной машине.

**VMware Workstation Player** (прежнее название — Player Pro) — это приложение для виртуализации настольных компьютеров, которое предоставляется бесплатно для личного использования. При использовании коммерческой лицензии в VMware Workstation Player можно выполнять виртуальные машины с ограниченным доступом, созданные с помощью VMware Workstation Pro и Fusion Pro.

VMware Workstation Player можно использовать бесплатно в личных некоммерческих целях. Если вы просто хотите больше узнать о виртуальных машинах или использовать их в домашних условиях, вы можете получить VMware Workstation Player бесплатно. Студенты и преподаватели аккредитованных учебных заведений могут использовать VMware Workstation



Player бесплатно, если они являются участниками программы VMware Academic.

VMware Workstation Player устанавливается подобно стандартному приложению для настольного компьютера. После установки VMware Workstation Player пользователи могут устанавливать новые операционные системы и запускать их как виртуальные машины в отдельном окне. VMware Workstation Player включает в себя возможности, с помощью которых пользователи могут создавать и настраивать собственные виртуальные машины, а также обеспечивать оптимальную производительность и доступ к любым подключенным к компьютеру устройствам.

VMware Workstation Player можно использовать для создания, запуска и оценки ПО, работающего в виртуальных машинах, а также обеспечения общего доступа к нему.

С помощью VMware Workstation Player можно создавать виртуальные машины с новейшими 32- и 64-разрядными ОС Windows и Linux. Благодаря возможности Easy Install это легче, чем установка операционной системы на ПК.

VMware Workstation Player можно использовать для запуска виртуальных машин на ПК с Windows или Linux. VMware Workstation Player обеспечивает быстрый и удобный доступ к возможностям безопасности, гибкости и переносимости виртуальных машин.

VMware Workstation Player идеально подходит для безопасной оценки программного обеспечения, распространяемого как виртуальное устройство. Виртуальные устройства — это предварительно настроенные и готовые к работе корпоративные приложения, «упакованные» вместе с операционной системой в виртуальную машину. С помощью VMware Workstation Player любой пользователь может быстро и без сложностей, сопровождающих установку и настройку ПО, воспользоваться преимуществами готовых к

работе продуктов. В VMware Solution Exchange доступно более 900 виртуальных устройств, предоставляемых ведущими поставщиками ПО.

В чем разница между бесплатной и платными редакциями VMware Workstation Player?

VMware Workstation Player — это бесплатное ПО, но приобретение и ввод лицензионного ключа дают пользователям следующие дополнительные преимущества.

Лицензируемая редакция VMware Workstation Player разработана для использования в коммерческих целях. Продукт лицензируется для использования сотрудниками, учебными организациями, подрядчиками и может быть передан партнерам или потенциальным заказчикам.

В лицензируемой редакции VMware Workstation Player можно запускать виртуальные машины с ограниченным доступом, созданные с помощью VMware Fusion Pro или VMware Workstation.

Лицензируемая редакция VMware Workstation Player обеспечивает улучшенную поддержку массового развертывания для тысяч пользователей. В это решение включены разные варианты установки и конфигурации, благодаря которым можно запускать автоматическую установку с использованием ПО для настройки систем и скрывать ненужные параметры [31].

**VirtualBox** является самым простым решением является Innotek

VirtualBox, потому что в нем сочетаются прекрасные качества настоящей и простой в использовании ВМ. Предпосылкой создания VirtualBox послужило создание ВМ на базе VMware, доступной каждому. Также он переведен на несколько языков, в.т.ч Русский, но пока не идеально. Но сообщество пользователей ВМ растет и создает удобства для пользователей. VirtualBox доступен для различных ОС, включая Linux, Windows, Mac OS X в виде бинарных файлов, что облегчает установку и основан на QT GUI, который

использует SDL библиотеки для доступа к мультимедийным устройствам. Существует две версии его воспроизведения: это открытая(OSE) с ограничениями и полная, свободная от обязательств. Она поддерживает большое количество ОС в роли гостевых, таких как Linux (2,4 и 2,6), Windows (NT 4.0, 2000, XP, Server 2003, Vista), DOS/Windows 3.x и OpenBSD, FreeBSD, но это не предел. Также VirtualBox отличается высокой производительностью и поддержка интеграции «на лету». Параметры гостевой системы можно выбрать и настроить. В роли могут выступать x86 от производителей Intel и AMD, 64-битная архитектура процессора, пока в разработке.

Некоторые характеристики VirtualBox. Модульность: VirtualBox имеет оптимально модульную конструкцию с хорошо продуманным внутренним интерфейсом и клиент/сервер дизайном. Это делает легким контроль над несколькими интерфейсами одновременно: к примеру, вы можете запустить виртуальную машину в обычном VM GUI (Графический интерфейс пользователя) и затем контролировать эту машину из командной строки, или возможно удаленно. VirtualBox также приходит с полным SDK («Инструментом для разработки»): даже если это Открытое программное обеспечение, вы не должны быть специалистом чтоб написать новый интерфейс для VirtualBox.

Виртуальная машина описывается в XML формате. Конфигурация параметров виртуальной машины сохраняется в XML и независимо от локальных машин. Определения Виртуальной машины поэтому могут легко перенесены на другие компьютеры.

Добавления гостя для Linux и Windows. VirtualBox имеет специальное программное обеспечение, что может быть установлено внутри VM Windows или Linux для улучшения производительности и создания внедрения более сильного. Среди характеристик, обеспечивающих Добавление гостя — это

внедрение указателя мыши и изменение разрешения экрана (так как изменение размера окна).

Ниже приведено несколько оптимальных характеристик доступных с полной версией VirtualBox.

**Виртуальные USB контроллеры.** VirtualBox имеет инструменты для USB контроллеров, которые позволяют Вам присоединить произвольно USB устройства на вашу виртуальную машину без установки специальных драйверов на машину.

**Протокол удаленного доступа к рабочему столу.** В отличие от других виртуального программного обеспечения, VirtualBox имеет полную поддержку стандартного Удаленного Рабочего Протокола(RDP). Виртуальная машина может действовать, как RDP сервер, позволяющий вам «запустить» дистанционно на некотором тонком клиенте, который просто показывает данные по RDP.

**USB над RDP.** Этим уникальным качеством, виртуальная машина может действовать как RDP сервер, который может получить доступ к произвольным USB устройствам, что соединены на RDP клиенте. Это дорого, мощной серверной машины, которая может виртуализировать много тонких клиентов, что просто покажут нужные RDP данные и подключенные USB устройства.

**Общие папки.** Еще много других виртуальных разрешений, для легкого обмена данными между хостами и гостями, VirtualBox позволяет объявлять каталоги как «общие папки», которые могут затем использоваться в пределах виртуальных машин [29].

**Microsoft Visio** — это мощное решение для создания диаграмм, которое позволяет упростить и связать информацию, а также поделиться ей. Microsoft Visio обладает мощным интерфейсом со множеством опций для создания собственных методов организации информации.

Оно идеально подходит для ИТ-специалистов, разработчиков и аналитиков (например, связанных с бизнес-процессами, кадрами и управлением), которым требуется интерпретировать, обновлять и передавать сложную информацию о процессах, инфраструктуре и приложениях.

Visio предоставляет мощные средства для создания графических диаграмм и работы с данными без художественных или технических навыков. Создаете ли вы организационную диаграмму, сетевую диаграмму или диаграмму процессов, вы можете получить нужное изображение с помощью готовых фигур.

Visio также содержит десятки наборов элементов и шаблонов, например, для разработки центра обработки данных, инженерных задач, управления, системного проектирования, планирования системы безопасности, разработки приложений, дизайна веб-сайтов и многого другого.

Утилита поставляется в трех вариантах.

Standard — включает инструменты построения диаграмм для представления в визуальной форме информации о людях, процессах и проектах;

Professional — рассчитан на использование специалистами профессионалами в области интернет технологий, разработчиками и инженерами, поскольку, помимо функций первого пакета, позволяет визуализировать существующие и новые идеи, системы и информацию;

Enterprise NetworkTools — включает дополнительные средства документирования сети и построения сетевых диаграмм.

**Acrobat Reader DC** средство для просмотра и печати документов PDF.

Бесплатная программа Adobe Acrobat Reader DC предлагает больше возможностей, чем другие программы для чтения, печати и рецензирования файлов PDF. Интеграция с облачными сервисами Adobe Document Cloud дает

дополнительное преимущество — теперь работать с документами PDF на компьютерах и мобильных устройствах стало еще проще.

Acrobat Reader DC связан с облаком Adobe Document Cloud, поэтому с документами PDF можно работать из любого места. Хранить файлы можно также в Box, Dropbox и Microsoft OneDrive.

Преобразование файлов PDF в документы Word. Всего один клик, и вы сможете пользоваться дополнительными сервисами PDF. Приложение Reader позволяет активировать дополнительные возможности для создания файлов PDF и экспорта этих файлов в Word или Excel.

Заполнение, подписание и отправка PDF-форм. Попрощайтесь с бумажными формами. Вводите текст непосредственно в формы PDF. Добавляйте электронные подписи. Отправляйте формы по электронной почте. Сохраняйте копии для себя.

Управление развертыванием программного обеспечения и обеспечение соответствия стандартам. Управляйте обновлениями и осуществляйте их развертывание с помощью инструментов Adobe и Microsoft. Получите поддержку широкого спектра стандартов безопасности документов. Расширяйте функциональность приложения Reader с помощью бесплатного комплекта средств разработки Acrobat SDK.

## **2.4 Структура и содержание курсовой работы**

### **2.4.1 Введение к курсовой работе**

Курсовая работа по дисциплине «Глобальные сети» является важным элементом учебного процесса, способствующим закреплению, углублению, обобщению и прикладному применению знаний и умений, сформированных у

студентов при изучении дисциплин «Операционные системы» и «Локальные сети».

Цель курсовой работы: сформировать у студентов умения практической работы, связанной с применением технологий компьютерных сетей для решения задач организации сетевого взаимодействия.

Данная цель может быть достигнута при успешном решении студентами следующего круга задач:

- анализ инфраструктуры предприятия;
- проектирование логической схемы предприятия в симуляторе;
- виртуализация серверной части.

Публичная защита курсовой работы является неотъемлемой частью учебного процесса и существенно влияет на оценку курсовой работы.

Данные методические указания предназначены для студентов, изучающих дисциплину «Глобальные сети» и направлены на оказание им практической помощи в подготовке курсовой работы. В качестве результатов выполненной курсовой работы студенты должны предоставить:

1. Презентация в MS Power Point, отражающая основные результаты курсового проектирования.

Обязательный титульный лист с указанием списка авторов, номером варианта, а также слайд с заданием и схемой офисов.

На следующих слайдах для сетевого оборудования указать: марку и модель, поддерживаемые технологии, количество портов, поддерживаемую скорость передачи данных, какие возможности оборудование предоставляет.

Для линий связи: указать технологию, поддерживаемую скорость передачи данных, тип разъёмов. Необходимо рассчитать длину линий связи и количество разъёмов.

Размещение линий связи и сетевого оборудования должно соответствовать трехуровневой модели сетевого дизайна.

Для компьютеров-клиентов указать программное обеспечение (операционную систему, прочее установленное программное обеспечение), настройки для подключения к сети.

Для серверов указать: программное обеспечение (операционную систему, сетевые сервисы, прочее установленное программное обеспечение), настройки для подключения к сети.

Критерии оценки презентации: в презентации должны быть отражены результаты трех заданий курсовой работы; презентация должна сопровождаться защитным словом.

## 2. Выполненная схема в программном симуляторе Cisco Packet Tracer.

Критерии оценки логической схемы: в схеме должны быть настроены все технологии, указанные в методических указаниях, согласно заданию по варианту (за исключением серверной части); студенты должны быть готовы к внесению в схему изменений по заданию преподавателя.

## 3. Настроенные виртуальные машины в любой среде виртуализации.

Критерии оценки виртуальных машин: количество виртуальных машин должно быть обосновано сетевой инфраструктурой; на серверах должны быть настроены все технологии, указанные в методических указаниях, студенты должны быть готовы к внесению в конфигурацию виртуальных машин изменений по заданию преподавателя.

Выбор варианта. Выбор варианта определяется по последней цифре номера зачетной книжки. На данном этапе мы выбираем вариант задания по последнему номеру зачетной книжки. Допустим, номер зачетной книжки 1302612, следовательно, мы выбираем 2 Вариант (Основная сеть – заштрихованная, сеть арендаторов — незаштрихованная) (рисунок 1).





Рисунок 1 — План помещения

## 2.4.2 Анализ инфраструктуры предприятия

Пример выполнения анализа инфраструктуры предприятия на основе схемы, по номеру варианта.

Планируем трех уровневую модель сети. В результате должен получиться список оборудования для каждого уровня модели сети. Список серверного, сетевого оборудования и программного обеспечения. Также необходимо учитывать, что при составлении списка берется предварительный анализ, в процессе выполнения работы оборудование может добавляться (таблица 3).

Таблица 3 — Список оборудования

| Наименование  | Описание  | Кол<br>во | Стоимость<br>руб. | Сумма  |
|---|---|-----------|-------------------|--------|
| Напольный серверный шкаф Metal Box 25U 600x1000                                 | Напольный серверный шкаф Metal Box 25U 1236*600*1000 мм (В.*Ш.*Г.), RAL9005. Для размещения 19 дюймового серверного оборудования  | 2 шт.     | 87768             | 175536 |
| Источник бесперебойного питания APC Smart-UPS C 3000VA Rackmount LCD 230V       | интерактивный ИБП, 1-фазное входное напряжение, выходная мощность 3000 ВА / 2700 Вт, 3 мин работы при полной нагрузке, 11.3 мин. работы при половинной нагрузке, выходных разъемов: 3, возможность установки в стойку, высота 2 U, интерфейсы: RS-232, USB. время зарядки 3 ч | 2         | 201380            | 402760 |
| Сервер IBM System x3550 M3 б/у  | 2 процессора Intel Xeon Quad-Core L5520 2.26GHz, 24GB DRAM, 4x146 SAS<br>1 сервер (Виртуализация Hyper-V) Active Directory + Файловый сервер (FS).<br>2 сервер (Виртуализация Hyper-V) Active Directory + Файловый сервер (FS).   | 2         | 163398            | 326796 |
| Рельсы для IBM System x3550 x3650   | Набор для крепления серверов IBM System x3550M2, x3550M3, x3650M2, x3650M3 в стойку 19"   | 2         | 18830             | 37660  |
| Маршрутизатор Cisco 2911 2 штуки б/у  | Маршрутизатор, 3 порта 10/100/1000BaseT Ethernet, 4 слота EHWIC, 2 слота PVDM3, 1 слот SM, 1 слот ISM, блок питания AC.   | 2         | 93444             | 186888 |
| Коммутатор Cisco Catalyst WSC3750G-24T-S для маршрутизации VLAN (ядро сети) б/у | Коммутатор, Layer3, 24 порта 10/100/1000BaseTX  | 1         | 62578             | 62578  |
| Коммутатор Cisco Catalyst WS-C2960-24TT-L 7 шт. б/у.                            | Управляемый коммутатор Layer2, 24 порта 10/100Base-TX, 2 порта 10/100/1000Base-T  | 7         | 48083             | 336581 |
| Точка доступа Ubiquiti UniFi AP   | Wi-Fi-роутер, стандарт Wi-Fi: 802.11n, макс. скорость: 300 Мбит/с.  | 2         | 9746              | 19492  |

Продолжение таблицы 3

|  |   |  |       |       |
|--|---|--|-------|-------|
| Линии связи  | Кабель UTP CAT6, максимальная   |  | 27,41 | 27,41 |
|  | скорость передачи данных на конечных устройствах 1000 Мбит/с., на серверном оборудовании 1000 Мбит/с. |  |       |       |
| Операционная система: Windows 10<br>Профессиональная |   |  | 13900 | 13900 |
| Операционная система: Windows Server 2016 Standard   |   |  | \$882 | 60417 |

Составление IP-плана.

Пример определение количества логических сетей, с минимизацией избыточности IP-адресов для каждой из сетей. Выбор адресации из local unicast диапазонов вносится в документ Visio в виде таблицы (таблица 4).

Таблица 4 — «IP план»

| № vlan | Имя vlan | Кол-во IP адресов в сети | IP сети   | Bitmask | Netmask         |
|--------|----------|--------------------------|-----------|---------|-----------------|
| 10     | Printers | 17                       | 10.0.0.0  | 27      | 255.255.255.224 |
| 20     | 101_kab  | 2                        | 10.0.0.32 | 30      | 255.255.255.252 |

На данном этапе анализируется схема расположения рабочих мест.

*Примечание:* Стоит обратить внимание, что при различных вариантах выполнения курсовой работы, количество оборудования может возрасти.

При составлении IP плана рекомендуется использовать технологии VLSM и CIDR.

Суть технологии CIDR состоит в том, что каждому поставщику услуг Internet (или, для корпоративных сетей, какому-либо структурнотерриториальному подразделению) должен быть назначен неразрывный диапазон IP-адресов. Из этого следует что для каждого офиса мы будем создавать отдельный неразрывный диапазон IP адресов.

IP-план возможного офиса представлен ниже (таблица 5).

Таблица 5 — «IP план» офиса

| № vlan | Имя vlan  | Кол-во IP<br>адресов в сети | IP сети    | Bitmask | Netmask         |
|--------|-----------|-----------------------------|------------|---------|-----------------|
| *      | nat       | 2                           | 10.0.0.8   | 29      | 255.255.255.248 |
| 5      | Arenda    |                             | 10.0.0.240 | 28      | 255.255.255.240 |
| 6      | Wi-Fi     |                             | 10.0.0.208 | 28      | 255.255.255.240 |
| 8      | Manage    |                             | 10.0.0.224 | 28      | 255.255.255.240 |
| 9      | Printer   | 10/14                       | 10.0.0.192 | 28      | 255.255.255.240 |
| 10     | Reception | 2/2                         | 10.0.0.0   | 30      | 255.255.255.252 |
| 11     | Server    | */14                        | 10.0.0.16  | 28      | 255.255.255.240 |
| 12     | Kab12     | 6/6                         | 10.0.0.32  | 29      | 255.255.255.248 |
| 13     | Kab13     | 9/14                        | 10.0.0.48  | 28      | 255.255.255.240 |
| 14     | Kab14-old | 4/6                         | 10.0.0.64  | 29      | 255.255.255.248 |
| 15     | Kab15-old | 5/6                         | 10.0.0.72  | 29      | 255.255.255.248 |
| 16     | Kab16-old | 2/2                         | 10.0.0.80  | 30      | 255.255.255.252 |
| 17     | Kab17     | 2/2                         | 10.0.0.84  | 30      | 255.255.255.252 |
| 18     | Kab18-old | 10/14                       | 10.0.0.96  | 28      | 255.255.255.240 |

Все сети для первого офиса легко влезут в диапазон 10.0.0.0/24.

Общая сеть 10.0.0.0/23 (маска 255.255.254.0). Все подсети сделаны «с запасом» для возможности увеличения инфраструктуры.

### 2.4.3 Проектирование логической схемы предприятия

Технологии для логического проектирования:

- стандартные IP протоколы (таблица 6);

Таблица 6 — Интернет протоколы

| Название технологии | Краткое описание  | Дисциплина           |
|---------------------|---|----------------------|
| IPv4                | IPv4 — четвёртая версия интернет протокола (IP). IPv4 использует 32-битные (четырёхбайтные) адреса, ограничивающие адресное пространство 4 294 967 296 (232) возможными уникальными адресами. Традиционной формой записи IPv4 адреса является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками. Через дробь указывается длина маски подсети. | Операционные системы |
| IPv6                | IPv6 — новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в Интернете, за счёт использования длины адреса 128 бит вместо 32.   | Локальные сети       |

- протоколы физического уровня модели OSI (таблица 7);

7 — Протоколы физического уровня

| Название технологии | Краткое описание  | Дисциплина           |
|---------------------|---|----------------------|
| Ethernet            | Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3.   | Операционные системы |
| WI-FI               | Wi-Fi — торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. | Локальные сети       |

- протоколы для работы с VLAN (таблица 8);

Таблица 8 — Протоколы для работы с виртуальными локальными сетями

| Название технологии | Краткое описание  | Дисциплина     |
|---------------------|---|----------------|
| VLAN                | VLAN — виртуальная локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к ширококвещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств. | Локальные сети |
| VTP                 | Протокол VTP — протокол локальной вычислительной сети, служащий для обмена информацией о VLAN, имеющихся на выбранном транковом порту. Разработан и используется компанией Cisco.   | Локальные сети |

|      |  |                |
|------|--|----------------|
| VLSM | Бесклассовая адресация — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям. | Локальные сети |
|------|--|----------------|

• протоколы для используемые для обеспечения отказоустойчивой корпоративной локальной сети (таблица 9);

9 — Протоколы для отказоустойчивости сети

| Название технологии | Краткое описание   | Дисциплина     |
|---------------------|--|----------------|
| Port-Channel        | Агрегирование каналов — технология, которая позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала. Агрегирование каналов может быть настроено между двумя коммутаторами, коммутатором и маршрутизатором, между коммутатором и хостом.  | Локальные сети |
| RPVST               | Spanning Tree Protocol — канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.   | Локальные сети |
| HSRP                | Основная задача и предназначение данного протокола состоит в том, чтобы добиться практически 100% доступности и отказоустойчивости первого хоста от отправителя (также иногда называемый «маршрут по умолчанию» или "шлюз последней надежды"). Это достигается путём использования у двух или более маршрутизаторов или маршрутизирующих коммутаторов третьего уровня одного IP-адреса и MAC-адреса так называемого виртуального маршрутизатора. Такая группа называется HSRP-группой. | Локальные сети |

• протоколы динамической маршрутизации (таблица 10);

Таблица 10 — Протоколы динамической маршрутизации

| Название технологии | Краткое описание  | Дисциплина     |
|---------------------|---|----------------|
| OSPF                | OSPF — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры.  | Локальные сети |
| EIGRP               | EIGRP — протокол маршрутизации, разработанный фирмой Cisco на основе протокола IGRP той же фирмы. Релиз протокола состоялся в 1994 году. EIGRP использует механизм DUAL для выбора наиболее короткого маршрута. | Локальные сети |

- протоколы для настройки сети Интернет (таблица 11);
- 11 — Протоколы для работы с сетью «Интернет»

| Название технологии | Краткое описание   | Дисциплина      |
|---------------------|--|-----------------|
| NAT                 | NAT — преобразование адреса методом NAT может производиться почти любым маршрутизирующим устройством — маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является SNAT, суть механизма которого состоит в замене адреса источника при прохождении пакета в одну сторону и обратной замене адреса назначения в ответном пакете. Наряду с адресами источник/назначение могут также заменяться номера портов источника и назначения. | Глобальные сети |
| PAT                 | Трансляция порт-адрес — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP -адрес, используя различные порты  | Глобальные сети |

- протоколы, обеспечивающие безопасность, как корпоративной сети на сеансовом уровне модели OSI, так и при взаимодействии пользователей публичных сетей с корпоративной сетью. В курсовой работе они будут настроены на сетевом оборудовании компании «Cisco Inc.» (таблица 12);



Таблица 12 — Протоколы с шифрованием

| Название технологии | Краткое описание   | Дисциплина      |
|---------------------|--|-----------------|
| StVPN               | Идеально подходит для связи центрального офиса компании с ее филиалами. Виртуальный канал позволяет связать локальные компьютерные сети офисов и организовать несколько каналов связи, в том числе для доступа в Интернет.   | Локальные сети  |
| RaVPN               | Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или с компьютера общественного пользования. | Глобальные сети |
| SSH                 | SSH — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. Схож по функциональности с протоколами Telnet, но, в отличие от него, шифрует весь трафик, включая и передаваемые пароли.                                       | Глобальные сети |
| ACL                 | Access Control List — список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту.  | Глобальные сети |

Пример размещения оборудования в программном симуляторе. При размещении конечных устройств, не рекомендуется представлять все физические устройства в программном симуляторе, достаточно представить по одному экземпляру конечного устройства из категории принтеры, компьютеры. Например, если на физической схеме кабинета размещено 5 ПК и 2 принтера, то в Cisco Packet Tracer достаточно 1 ПК и 1 принтера (рисунок 2).

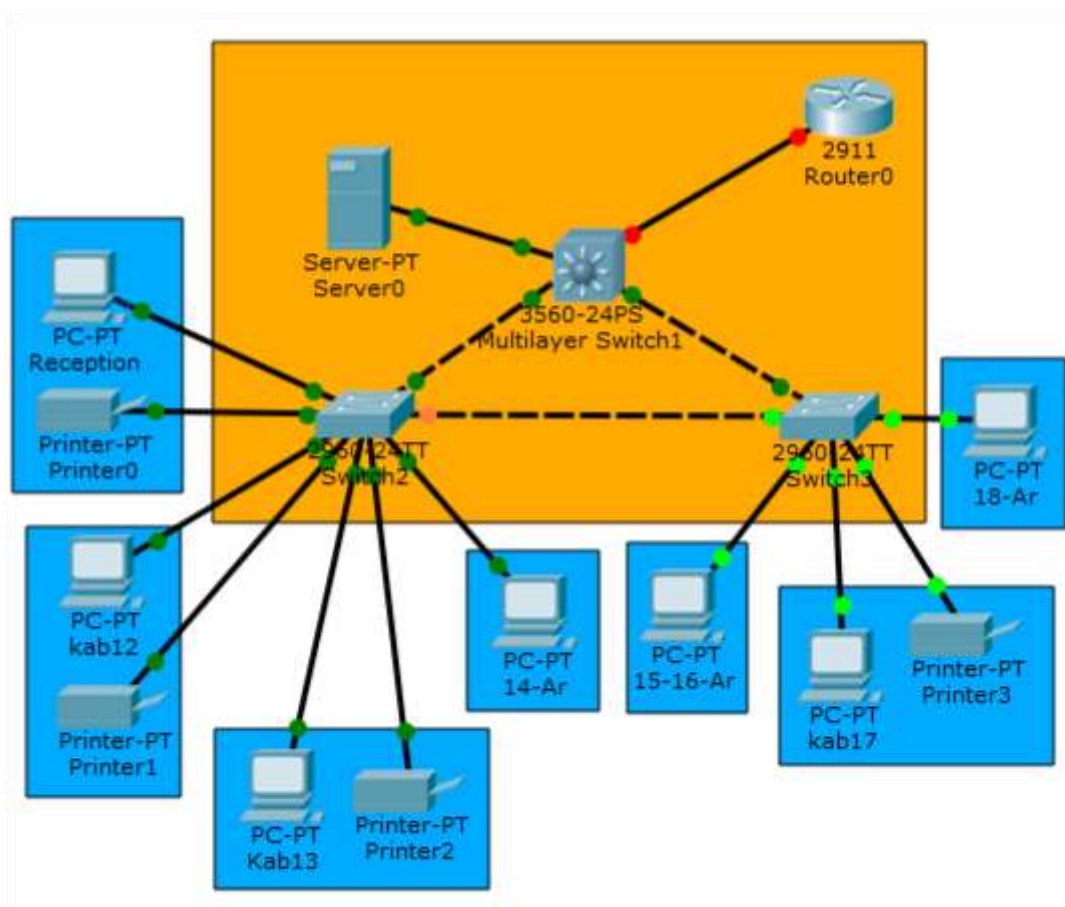


Рисунок 2 — Расположение оборудования по кабинетам в офисе

При соединении устройств необходимо обеспечивать отказоустойчивость локальной сети, а критически важными участками сети являются соединения между коммутаторами. Для их соединения необходимо использовать технологии «**etherchannel**» и протокол **остовного дерева**. Именно эти технологии помогут получить повышенную пропускную способность и высокую отказоустойчивость нашей сети.

Технология агрегации каналов в Cisco Packet Tracer, представлена двумя протоколами LACP и PAgP.

*Примечание.* В Cisco Packet Tracer не рекомендуется использовать технологию etherchannel, это может привести в неправильной работе и зависанию программного продукта (рисунок 3).

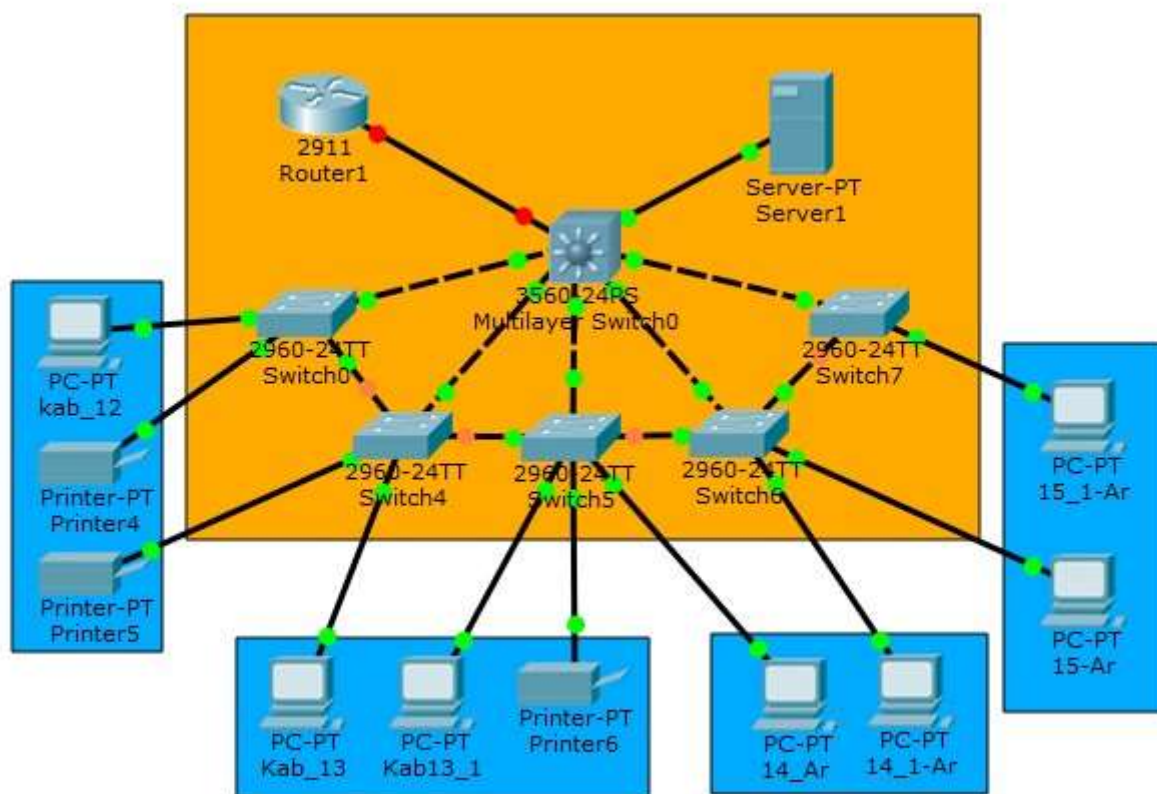


Рисунок 3 — Расположение оборудования по кабинетам в офисе

Пример конфигурирования виртуальных локальных сетей согласно IP плану. В офисах, в которых более 2-ух коммутаторов, настраиваем получение информации о виртуальных сетях с главного коммутатора.

На данном этапе необходимо настраивается протокол **VTP** и создается на главных коммутаторах VLAN-ы согласно IP плану. Далее настраиваем на портах режимы **trunk** и **access** (рисунок 4).

| Port  | Link | VLAN | IP Address | MAC Address    |
|---|------|------|------------|----------------|
| FastEthernet0/1   | Up   | --   | --         | 00D0.BC43.E701 |
| FastEthernet0/2   | Up   | --   | --         | 00D0.BC43.E702 |
| FastEthernet0/3   | Up   | 10   | --         | 00D0.BC43.E703 |
| FastEthernet0/4   | Up   | 9    | --         | 00D0.BC43.E704 |
| FastEthernet0/5   | Up   | 12   | --         | 00D0.BC43.E705 |
| FastEthernet0/6   | Down | 12   | --         | 00D0.BC43.E706 |
| FastEthernet0/7   | Down | 12   | --         | 00D0.BC43.E707 |
| FastEthernet0/8   | Down | 12   | --         | 00D0.BC43.E708 |
| FastEthernet0/9   | Down | 1    | --         | 00D0.BC43.E709 |
| FastEthernet0/10  | Up   | 9    | --         | 00D0.BC43.E70A |
| FastEthernet0/11  | Up   | 13   | --         | 00D0.BC43.E70B |
| FastEthernet0/12  | Down | 13   | --         | 00D0.BC43.E70C |
| FastEthernet0/13  | Down | 13   | --         | 00D0.BC43.E70D |
| FastEthernet0/14  | Down | 13   | --         | 00D0.BC43.E70E |
| FastEthernet0/15  | Down | 13   | --         | 00D0.BC43.E70F |
| FastEthernet0/16  | Down | 13   | --         | 00D0.BC43.E710 |
| FastEthernet0/17  | Down | 13   | --         | 00D0.BC43.E711 |
| FastEthernet0/18  | Down | 13   | --         | 00D0.BC43.E712 |
| FastEthernet0/19  | Down | 13   | --         | 00D0.BC43.E713 |
| FastEthernet0/20  | Up   | 9    | --         | 00D0.BC43.E714 |
| FastEthernet0/21  | Up   | 5    | --         | 00D0.BC43.E715 |
| FastEthernet0/22  | Down | 5    | --         | 00D0.BC43.E716 |
| FastEthernet0/23  | Down | 5    | --         | 00D0.BC43.E717 |
| FastEthernet0/24  | Down | 5    | --         | 00D0.BC43.E718 |
| GigabitEthernet0/1  | Down | 1    | --         | 00D0.BC43.E719 |
| GigabitEthernet0/2  | Down | 1    | --         | 00D0.BC43.E71A |
| Vlan1   | Down | 1    | <not set>  | 0060.47DB.C5A3 |
| Hostname: Switch  |      |      |            |                |
| Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet |      |      |            |                |

Рисунок 4 - Конфигурация портов коммутатора второго уровня

Пример настройки динамического конфигурирование протокола IPv4 на конечных устройствах.

На данном этапе настраивается технологию DHCP. Прежде чем настраивать DHCP, необходимо задать ip адреса VLAN (рисунок 5).

|                  |      |    |               |
|------------------|------|----|---------------|
| Vlan1            | Down | 1  | <not set>     |
| Vlan9            | Up   | 9  | 10.0.0.193/28 |
| Vlan10           | Up   | 10 | 10.0.0.1/30   |
| Vlan11           | Up   | 11 | 10.0.0.17/28  |
| Vlan12           | Up   | 12 | 10.0.0.33/29  |
| Vlan13           | Up   | 13 | 10.0.0.49/28  |
| Vlan14           | Up   | 14 | 10.0.0.65/29  |
| Vlan15           | Up   | 15 | 10.0.0.73/29  |
| Vlan16           | Up   | 16 | 10.0.0.81/30  |
| Vlan17           | Up   | 17 | 10.0.0.85/30  |
| Vlan18           | Up   | 18 | 10.0.0.97/28  |
| Hostname: Switch |      |    |               |

Рисунок 5 - IP адреса VLAN-интерфейсов в первом офисе

Данные IP адреса необходимо исключить из DHCP диапазона. После настройки автоматической раздачи IP адресов, необходимо посмотреть какие IP адреса выдал DHCP сервер (рисунок 6).

```
Switch#show ip dhcp binding
```

| IP address | Client-ID/<br>Hardware address | Lease expiration | Type      |
|------------|--------------------------------|------------------|-----------|
| 10.0.0.195 | 00E0.F781.3C9A                 | --               | Automatic |
| 10.0.0.196 | 0090.2192.6C94                 | --               | Automatic |
| 10.0.0.198 | 00D0.BC40.AE27                 | --               | Automatic |
| 10.0.0.199 | 0001.C9BA.1ED5                 | --               | Automatic |
| 10.0.0.2   | 00D0.97AA.539A                 | --               | Automatic |
| 10.0.0.34  | 0060.47E3.9A6C                 | --               | Automatic |
| 10.0.0.50  | 000C.8522.2179                 | --               | Automatic |
| 10.0.0.86  | 000B.BE24.1140                 | --               | Automatic |

Рисунок 6 – Выданные IP- адреса

Пример настройки выхода в интернет всем сотрудникам, кроме секретарей. На данном этапе будет настроена технология NAT. Выход секретарей в интернет будет ограничивать access-list. Правила в access-list необходимо прописывать в следующем порядке: сначала запрещаем потом разрешаем. На рисунке 7 приведен пример, первым правилом мы запрещаем выход секретарей в интернет, а вторым правилом разрешаем всем (рисунок 7).

```
deny ip 10.0.0.0 0.0.0.3 any
permit ip 10.0.0.0 0.0.0.255 any
```

Рисунок 7 — Пример access list

После настройки NAT, компьютеры организации могут выходить в глобальную сеть, кроме компьютеров секретарей (рисунок 8)

```
Router#show ip nat translations
```

| Pro  | Inside global | Inside local | Outside local | Outside global |
|------|---------------|--------------|---------------|----------------|
| icmp | 8.8.8.2:1     | 10.0.0.34:1  | 8.8.8.8:1     | 8.8.8.8:1      |
| icmp | 8.8.8.2:2     | 10.0.0.34:2  | 8.8.8.8:2     | 8.8.8.8:2      |
| icmp | 8.8.8.2:3     | 10.0.0.34:3  | 8.8.8.8:3     | 8.8.8.8:3      |
| icmp | 8.8.8.2:4     | 10.0.0.34:4  | 8.8.8.8:4     | 8.8.8.8:4      |

Рисунок 8 - Статистика сетевых трансляций

*Примечание:* Назначение технологии NAT в том, чтобы выводить «серые» адреса в глобальную сеть, поэтому самым первым правилом необходимо прописать запрет на трансляцию сетевых адресов из «серой» сети в «серую» (рисунок 9).

```
Extended IP access list FOR-NAT
10 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
20 deny ip 10.0.0.0 0.0.0.3 any
30 permit ip 10.0.0.0 0.0.0.255 any
```

Рисунок 9 — Запрет трансляции «серых» сетей

Настройка веб-сервер и сконфигурировать таким образом, чтобы клиенты нашей компании могли заходить на наш сайт.

На данном этапе необходимо настроить трансляцию из глобальной сети в «серую». Проверка осуществляется следующим образом: — с компьютера в глобальной сети, в адресной строке, необходимо ввести «белый» IP адрес нашей организации и в результате будет доступен веб-сайт нашей компании (рисунок 10).



Рисунок 10 - Проверка работоспособности PAT



Пример настройки защищенного соединения между офисами на основе применения технологии Site-to-Site VPN, с использованием IPSec, представлен на рисунке 11.

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status

IPv6 Crypto ISAKMP SA

Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
8.8.8.3      8.8.8.2      QM_IDLE       1086     0 ACTIVE

IPv6 Crypto ISAKMP SA
```

Рисунок 11 - Проверка работы защищенного соединения

Предоставление возможности сотрудникам компании получать доступ к любым ее ресурсам из публичной сети организуется с помощью технологии трансляции номеров портов в IP-адреса (рисунок 12).



Рисунок 12 — Результат успешного подключения

Пример предоставления арендаторам, из нашего офиса, отдельного выхода в интернет через наше оборудование, с ограничением уровня доступа представлен на рисунке 13 и рисунке 14.

```
Extended IP access list IN_AREDA
 10 deny ip any 10.0.0.0 0.0.0.255 (3 match(es))
 20 permit ip any any (16 match(es))
Extended IP access list OUT_AREDA
 10 deny ip 10.0.0.0 0.0.0.255 any
 20 permit ip any any (3 match(es))
```

Рисунок 13 — Access-list-ы для арендаторов

```
interface Vlan5
 ip address 10.0.0.241 255.255.255.240
 ip access-group IN_AREDA in
 ip access-group OUT_AREDA out
```

Рисунок 14 — Конфигурация интерфейса для арендаторов

Пример предоставления гостям офиса доступ в интернет (не к ресурсам компании) через сети Wi-fi.

Сети Wi-fi необходимо строить на точках доступа, связанных с основной сетью проводными линиями связи. В зависимости от нагрузки, создаваемой трафиком пользователей, рекомендуется применять технологию агрегации проводных каналов. Размещая точки доступа следует учитывать физические особенности здания (например, наличие стен). Задание для студентов устроено так, чтобы группы устройств, соединенных беспроводной сетью, были выделены цветом (рисунок 15).

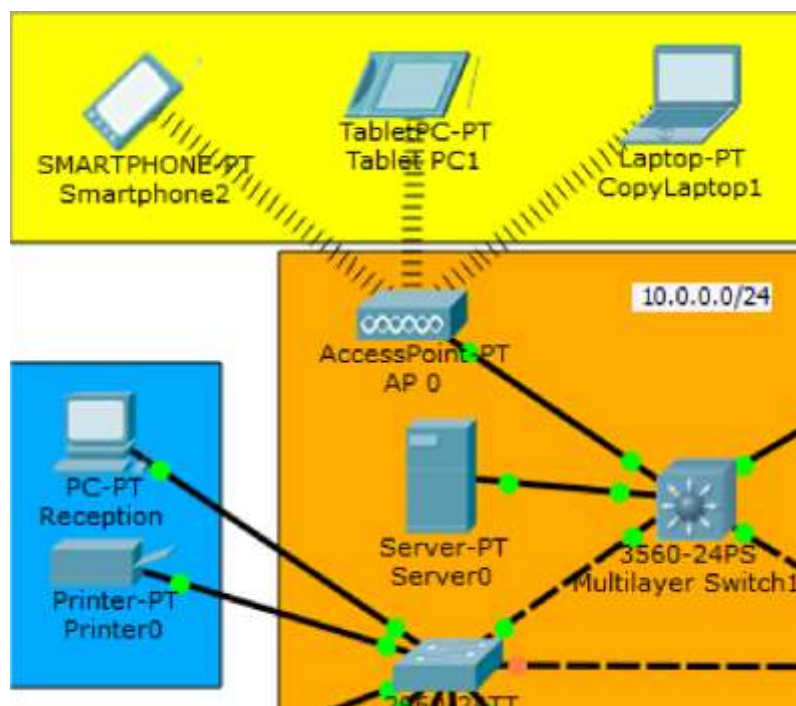


Рисунок 15 — Построение беспроводной сети



Для ограничения доступа к ресурсам компании необходимо использовать списки контроля доступа (рисунок 16).

```
MS1#show ip access-lists
Extended IP access list OUT_WIFI
 10 deny ip 10.0.0.0 0.0.0.255 any
 20 permit ip any any
Extended IP access list IN_WIFI
 10 deny ip any 10.0.0.0 0.0.0.255
 20 permit ip any any (9 match(es))
```

Рисунок 16 – Access-list-ы для беспроводной сети

Пример обеспечения возможности удаленного управления всеми коммутаторами и маршрутизаторами по защищенному каналу (рисунок 17).

```
MS1#ssh -l admin 10.0.0.10
Open
Password:
r0>ena
Password:
r0#
```

Рисунок 17 — Пример подключения по защищенному соединению

Пример настройки динамической маршрутизации (рисунок 18).

```
router eigrp 100
 network 10.0.0.0
 no auto-summary
```

Рисунок 18 — Результат настройки «EIGRP»

#### 2.4.4 Виртуализация серверной части

Технологии для виртуализации (таблица 13).

Таблица 13 — Роли и службы Windows Server

| Название технологии | Краткое описание  | Дисциплина           |
|---------------------|---|----------------------|
| AD DS               | Active Directory («Активный каталог», AD) — службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Первоначально создавалась, как LDAP-совместимая реализация службы каталогов, однако, начиная с Windows Server 2008, включает возможности интеграции с другими службами авторизации, выполняя для них интегрирующую и объединяющую роль. | Операционные системы |

Продолжение таблицы 13

|            |  |                      |
|------------|--|----------------------|
| DHCP       | DHCP — протокол динамической настройки узла — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели клиент-сервер.  | Операционные системы |
| DNS        | DNS — система доменных имён — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста, компьютера или устройства, получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).   | Глобальные сети      |
| SNMP       | SNMP — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора. | Операционные системы |
| Веб сервер | Веб-сервер — сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-поток или другими данными. Веб -сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер, на котором это программное обеспечение работает.  | Глобальные сети      |

|                 |   |                      |
|-----------------|---|----------------------|
| Файловый сервер | Файл-сервер — это выделенный сервер, предназначенный для выполнения файловых операций ввода-вывода и хранящий файлы любого типа. Как правило, обладает большим объемом дискового пространства, реализованном в форме RAID -массива для обеспечения бесперебойной работы и повышенной скорости записи и чтения данных. | Операционные системы |
|-----------------|---|----------------------|

Виртуализация серверной части выполняется в одной из трех систем управления виртуальными машинами на выбор:

- VMware Workstation Player;
- Hyper-V;
- VirtualBox.

Этапы работы с системой виртуализации:

1. Первым этапом происходит загрузка операционной системы с официального сайта производителя.
2. Создаётся виртуальная машина из любой из выше представленных сред с учетом минимальных системных требований и учетом возможности оборудования.
3. Устанавливается операционная система на созданную виртуальную машину и процесс снимается на видео (рисунок 19).

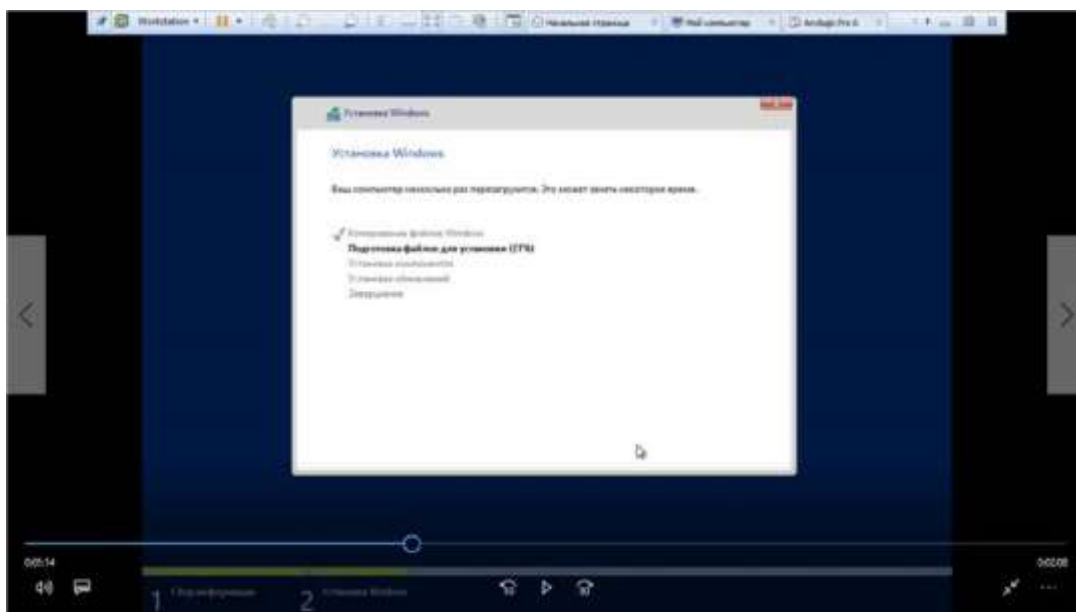


Рисунок 19 — Установка операционной системы

4. Настраиваются службы Active Directory Domain Services.

Пример добавления роли «Доменные службы Active Directory» показан на рисунке 20.

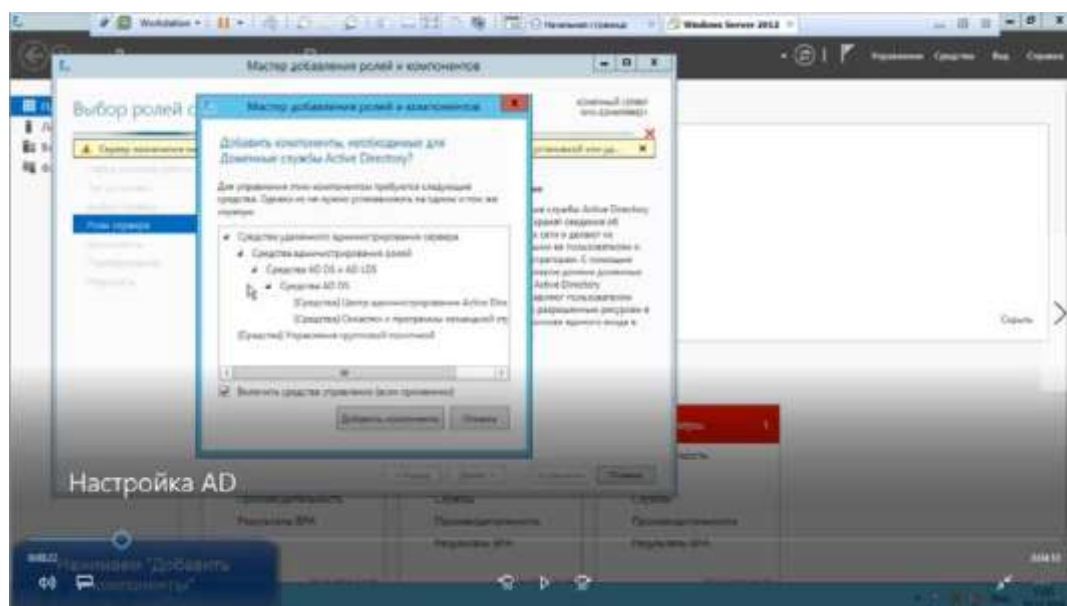


Рисунок 20 — Настройка Active Directory

Пример повышения роли сервера в службах Active Directory Domain Services показан на рисунке 21.

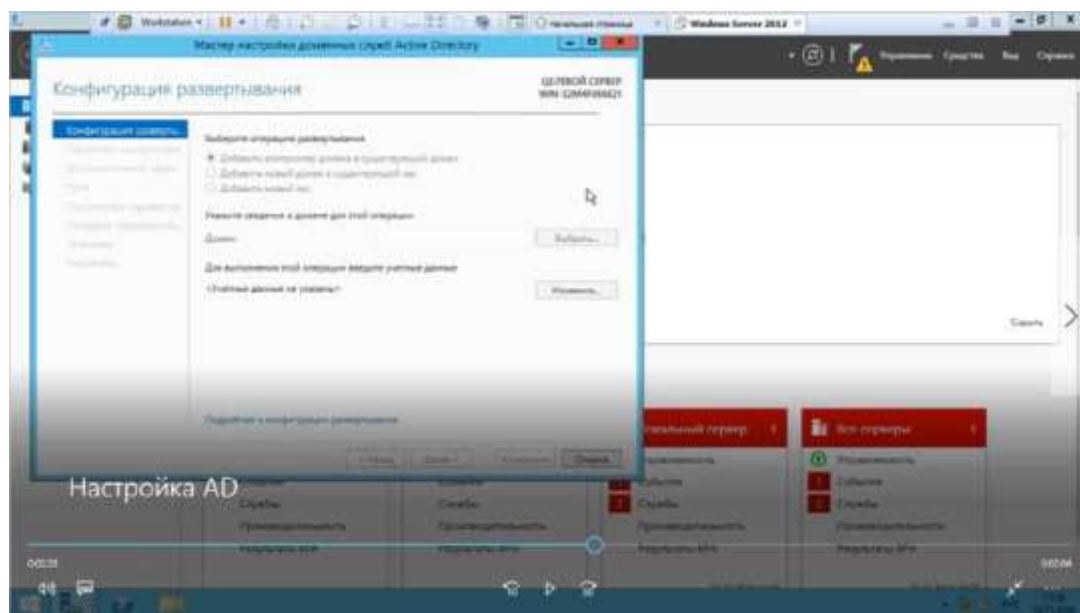


Рисунок 21 — Повышение роли до уровня «Контроллер»

5. Создание десяти пользователей и пяти отделов представлено на рисунке 22 и рисунке 23.

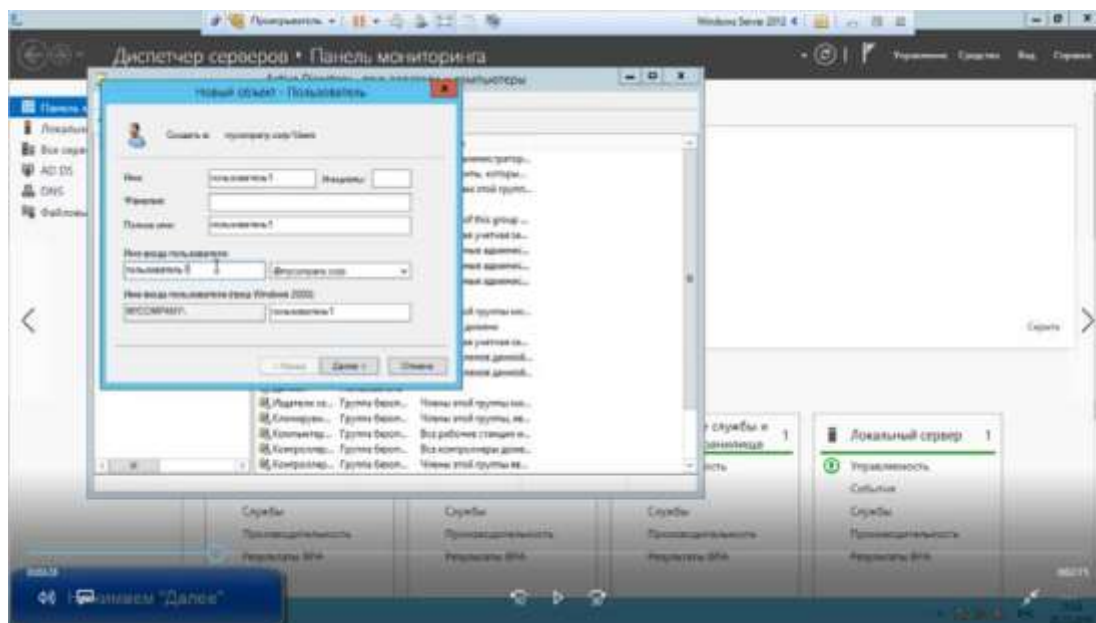


Рисунок 22 — Создание пользователей

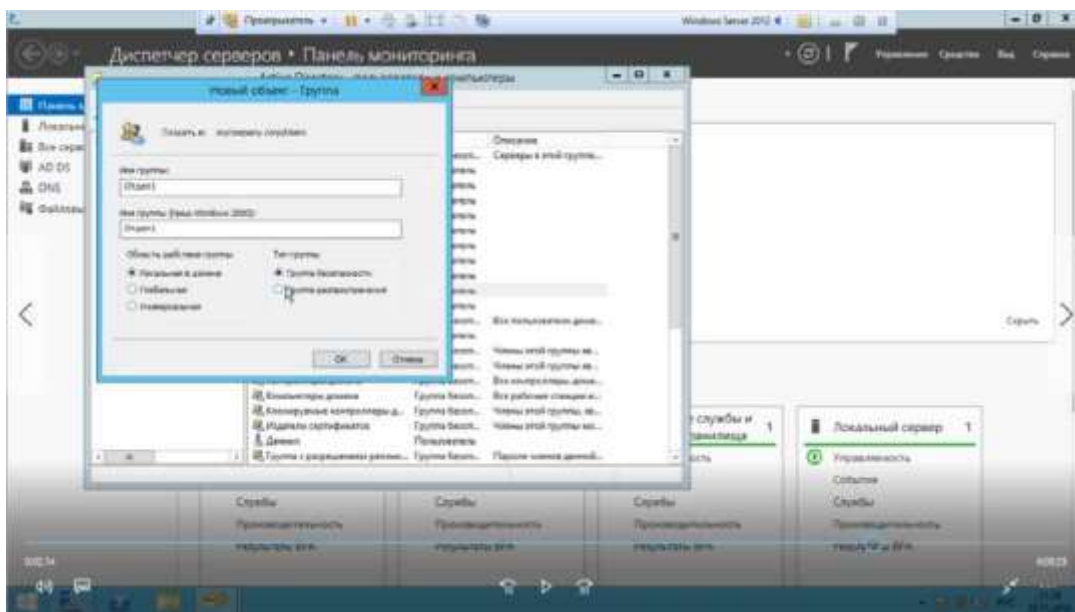


Рисунок 23 — Создание групп

6. Создание для каждого отдела по одной папке на общем ресурсе. Папкам необходимо настроить доступ таким образом, что каждый пользователь из отдела имеет разный уровень доступа (чтение/запись) (рисунок 24).

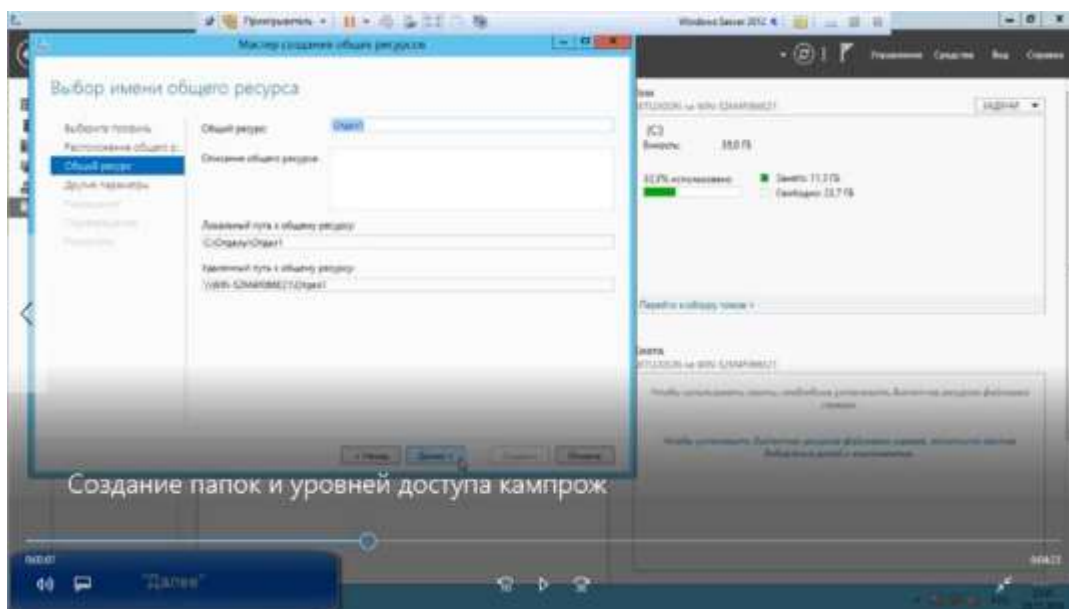


Рисунок 24 — Создание общего ресурса

7. Процесс настройки Web-сервера представлен на рисунке 25.

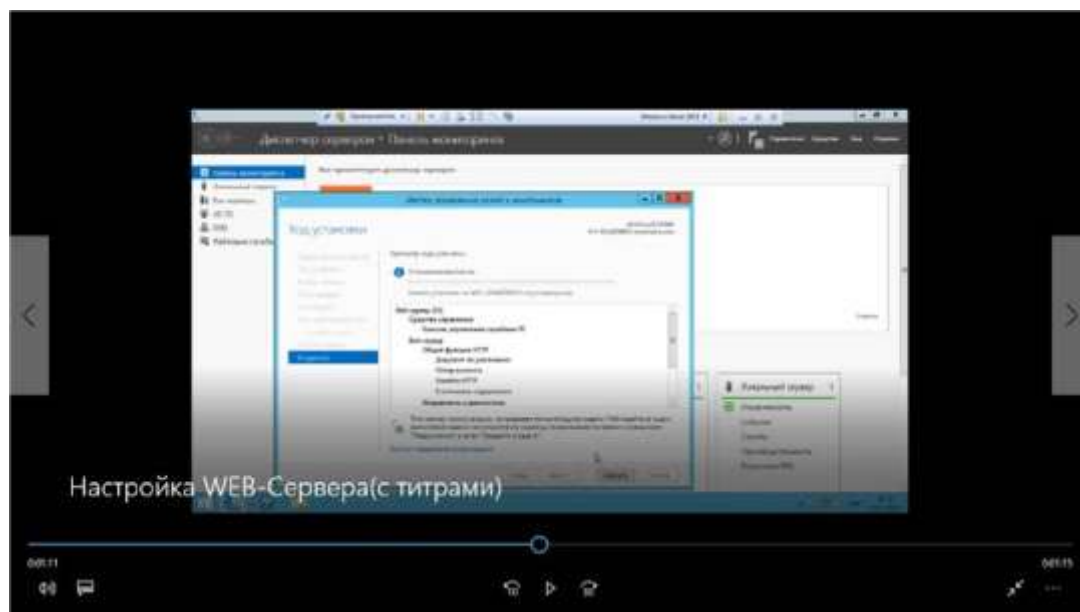


Рисунок 25 — Добавление роли «WEB-сервер»

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Балансировка загрузки канала EtherChannel и избыточность на коммутаторах Catalyst» [Электронный ресурс]. — Режим доступа: [http://www.cisco.com/cisco/web/support/RU/9/92/92066\\_4.html](http://www.cisco.com/cisco/web/support/RU/9/92/92066_4.html) (дата обращения: 16.11.2016).
2. Городилов Н.В. Лабораторный практикум «Технологии удаленного доступа» [Текст]: выпускная квалификационная работа бакалавра — Екатеринбург: РГППУ, 2016. — 49 с.
3. Динамическая маршрутизация [Электронный ресурс]. — Режим доступа: <http://it-donnet.ru/route-rip-ospf/> (дата обращения: 18.11.2016).
4. Динамическая настройка параметров сервера DHCP [Электронный ресурс]. — Режим доступа: [http://www.cisco.com/cisco/web/support/RU/9/92/92144\\_dhcp\\_ser.html](http://www.cisco.com/cisco/web/support/RU/9/92/92144_dhcp_ser.html) (дата обращения: 19.11.2016).
5. Корневская О. С. Электронное учебное пособие «Динамическая маршрутизация в корпоративных компьютерных сетях» [Текст]. выпускная квалификационная работа бакалавра — Екатеринбург: РГППУ, 2016. — 48 с.
6. Максимов Н.В. Компьютерные сети [Текст]: учебник для вузов / Н.В. Максимов, И.И. Попов — под общ. ред. Н.В. Максимова. — 3-е изд. — Москва: Форум, 2013. — 448 с.
7. Маршрутизация [Электронный ресурс]. — Режим доступа: <http://xgu.ru/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F> (дата обращения: 22.11.2016).



8. Методические рекомендации по выполнению и оформлению курсовой работы по дисциплине «Компьютерные сети и коммуникации» [Текст]. / Сыктывкар, Сыктывкарский целлюлозно-бумажный техникум, 2014. — 24 с.

9. Методические указания по выполнению курсового проекта по дисциплине «Компьютерные сети и телекоммуникации» для студентов специальности 230106 – Техническое обслуживание средств вычислительной техники и компьютерных сетей [Электронный ресурс]. / сост. Н. В. Максименко. – Новокузнецк: Кузнецкий индустриальный техникум, 2012.

10. Методические указания по выполнению курсовой работы по дисциплине «Информационные технологии управления» для студентов специальности 080507.65 – «Менеджмент организации» [Текст]. / сост. Прокофьева М.А. – Пятигорск, КМВИС ФГБОУ ВПО «ЮРГУЭС», 2013 – 24с.

11. Методические указания по выполнению курсовой работы по дисциплине «Сети и телекоммуникации» для студентов направления 230100 – Информатика и вычислительная техника [Текст] / Челябинск, ФГБОУ ВПО «ЧелГУ», 2015. – 28 с.

12. Методические указания для выполнения курсовых работ по дисциплине «Компьютерные коммуникации и сети» для студентов всех форм обучения специальности 230201 – Информационные системы и технологии [Текст]. / сост. А.А. Карасик, Н.В. Ломовцева. – Екатеринбург, ФГАОУ ВПО «Рос. гос. проф.-пед. ун-т», 2012. – 28 с.

13. Настройка трансляции сетевых адресов: Начало работы [Электронный ресурс]. — Режим доступа: [http://www.cisco.com/cisco/web/support/RU/9/92/92026\\_12.html](http://www.cisco.com/cisco/web/support/RU/9/92/92026_12.html) (дата обращения: 28.11.2016).

14. Общие сведения и настройка магистрального протокола VLAN (VTP) [Электронный ресурс]. — Режим доступа: [http://www.cisco.com/cisco/web/support/RU/9/92/92030\\_21.html](http://www.cisco.com/cisco/web/support/RU/9/92/92030_21.html) (дата обращения: 29.11.2016).

15. Общие сведения о протоколе быстрого связующего дерева (802.1w) [Электронный ресурс]. — Режим доступа: [http://www.cisco.com/cisco/web/support/RU/9/92/92067\\_146.html](http://www.cisco.com/cisco/web/support/RU/9/92/92067_146.html) (дата обращения: 30.11.2016).

16. Протокол EIGRP (усовершенствованный внутренний протокол маршрутизации шлюзов)» [Электронный ресурс]. — Режим доступа:

[http://www.cisco.com/cisco/web/support/RU/9/92/92088\\_eigrp-toc.html](http://www.cisco.com/cisco/web/support/RU/9/92/92088_eigrp-toc.html) (дата обращения: 01.12.2016).

17. Руководство по проектированию OSPF [Электронный ресурс]. — Режим доступа: [http://www.cisco.com/cisco/web/support/RU/9/92/92027\\_1.html](http://www.cisco.com/cisco/web/support/RU/9/92/92027_1.html) (дата обращения: 02.12.2016).

18. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс [Текст]. учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков; под общ. ред. Н. И. Синадского. — Екатеринбург: Изд-во Урал. ун-та, 2014. — 180 с.

19. Создание сетей VLAN на коммутаторах Catalyst [Электронный ресурс]. — Режим доступа: [http://www.cisco.com/cisco/web/support/RU/9/92/92047\\_3.html](http://www.cisco.com/cisco/web/support/RU/9/92/92047_3.html) (дата обращения: 04.12.2016).

20. Статическая маршрутизация [Электронный ресурс]. — Режим доступа: [http://xgu.ru/wiki/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F\\_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F](http://xgu.ru/wiki/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) (дата обращения: 05.12.2016).

21. Техническое примечание по настройке Secure Shell на маршрутизаторах и коммутаторах с программным обеспечением Cisco IOS [Электронный ресурс]. — Режим доступа:

[http://www.cisco.com/c/ru\\_ru/support/docs/securityvpn/secure-shell-ssh/4145-ssh.html](http://www.cisco.com/c/ru_ru/support/docs/securityvpn/secure-shell-ssh/4145-ssh.html) (дата обращения: 06.12.2016).

22. Cisco Packet Tracer [Электронный ресурс]. — Режим доступа: [https://ru.wikipedia.org/wiki/Cisco\\_Packet\\_Tracer](https://ru.wikipedia.org/wiki/Cisco_Packet_Tracer) (дата обращения: 04.10.2016).

23. Cisco Systems, Inc Основы организации сетей Cisco Том 1 Исправленное издание [Текст]: учебное пособие / Издательский дом "Вильямс", 2004. — 512 с.

24. Cisco Systems, Inc Основы организации сетей Cisco Том 2 Исправленное издание [Текст]. учебное пособие / Издательский дом "Вильямс", 2004. — 464 с.

25. DHCP [Электронный ресурс]. — Режим доступа: <https://ru.wikipedia.-org/wiki/DHCP> (дата обращения: 09.12.2016).

26. Hyper-V в Windows 10 [Электронный ресурс]. — Режим доступа: [https://msdn.microsoft.com/ru-ru/virtualization/hyperv\\_on\\_windows/welcome](https://msdn.microsoft.com/ru-ru/virtualization/hyperv_on_windows/welcome) (дата обращения: 10.12.2016).

27. NAT [Электронный ресурс]. — Режим доступа: <https://ru.wikipedia.org/wiki/NAT> (дата обращения: 11.12.2016).

28. STP [Электронный ресурс]. — Режим доступа: <http://xgu.ru/wiki/STP> (дата обращения: 12.12.2016).

29. VIRTUALBOX [Электронный ресурс]. — Режим доступа: <https://www.virtualbox.org/wiki/VirtualBox> (дата обращения: 13.12.2016).

30. VLAN [Электронный ресурс]. — Режим доступа: <https://ru.wikipedia.-org/wiki/VLAN> (дата обращения: 14.12.2016).

31. VMWARE [Электронный ресурс]. — Режим доступа:  
<http://www.vmware.com/ru/products/player/faqs.html> (дата обращения:  
15.12.2016).