Государственное областное бюджетное
Профессиональное образовательное учреждение
«Усманский многопрофильный колледж»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по учебной дисциплине ОП.03. Компьютерные сети

Программы подготовки специалистов среднего звена (ППССЗ)

по специальности 09.02.04 Информационные системы (по отраслям)

по программе базовой подготовки

Усмань 2018

по учебной дисциплинеОП.03. Компьютерные сети по специальности 09.02.04 Информационные системы (по отраслям).

Разработчики:
Мотин И.А. преподаватель информатики

Рассмотрены и утверждены на заседании предметно-цикловой комиссии естественнонаучных дисциплин

Протокол № 6 от 29.06.2018 г.

Председатель предметно-цикловой комиссии естественнонаучных дисциплин _____ Коровина Т.В.

УТВЕРЖДАЮ

Заместитель директора Думма Т.А.

по учебно-методической работе

Введение

Практические занятия, как вид учебных занятий, направлены на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений и составляют важную часть теоретической и профессиональной практической подготовки.

В процессе практического занятия обучающиеся выполняют одно или несколько практических заданий в соответствии с изучаемым содержанием учебного материала.

Содержание практических занятий по учебной дисциплинеОП.03. Компьютерные сети должно охватывать весь круг профессиональных умений, на подготовку к которым ориентирована данная дисциплина, а в совокупности охватывать всю профессиональную деятельность, к которой готовится специалист.

При разработке содержания практических занятий следует учитывать, что наряду с формированием умений и навыков в процессе практических занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать теоретические знания на практике, развиваются интеллектуальные умения.

Выполнение обучающимися практических занятий проводится с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными ФГОС и рабочей программой учебной дисциплиныОП.03. Компьютерные сети по конкретным разделам и темам дисциплины;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- совершенствования умений применять полученные знания на практике, реализации единства интеллектуальной и практической деятельности;
- развития интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработки таких профессионально значимых качеств, как

самостоятельность, ответственность, точность, творческая инициатива при решении поставленных задач при освоении общих и профессиональных компетенций.

Соответственно в процессе освоения учебной дисциплиныОП.03. Компьютерные сетиобучающиеся должны овладеть:

умениями:

- организовывать и конфигурировать компьютерные сети;
- строить и анализировать модели компьютерных сетей;
- эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач;
- выполнять схемы и чертежи по специальности с использованием прикладных программных средств;
- работать с протоколами разных уровней (на примере конкретного стека протоколов:
- TCP/IP, IPX/SPX);
- устанавливать и настраивать параметры протоколов;
- проверять правильность передачи данных;
- обнаруживать и устранять ошибки при передаче данных.

знаниями:

- основные понятия компьютерных сетей:
- типы, топологии, методы доступа к среде передачи;
- аппаратные компоненты компьютерных сетей;
- принципы пакетной передачи данных;
- понятие сетевой модели;
- сетевую модель OSI и другие сетевые модели;
- протоколы:
- основные понятия, принципы взаимодействия, различия и особенности распространенных протоколов, установка протоколов в операционных системах;
- адресацию в сетях, организацию межсетевого воздействия.

Вышеперечисленные умения и знания направлены на формирование следующих профессиональных и общих компетенций студентов:

Профессиональные компетенции:

ПК 1.2. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной

деятельности.

ПК 1.7. Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.

ПК 1.9. Выполнять регламенты по обновлению, техническому сопровождению и восстановлению данных информационной системы, работать с технической документацией.

ПК 1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

Общие компетенции:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в

профессиональной деятельности.

Данные методические рекомендации по организации и проведению практических работ составлены в соответствии с содержанием рабочей программы учебной дисциплины Компьютерные сетиспециальности09.02.04 Информационные системы (по отраслям)по программе базовой подготовки.

Учебная дисциплина Компьютерные сети изучается в течение учебного года. Общий объем времени, отведенный на выполнение практической работы по учебной дисциплине Компьютерные сети, составляет в соответствии с учебным планом и рабочей программой– 61 часов.

Методические рекомендации призваны помочь студентам правильно организовать работу и рационально использовать свое время при овладении содержанием учебной дисциплины Компьютерные сети, закреплении теоретических знаний и практических умений.

Распределение часов на выполнение практической работы студентов по разделам и темам учебной дисциплины Компьютерные сети

Наименование раздела, темы	Количество часов на ПР
Раздел1. Основы компьютерных сетей	**14**
Тема1.1 Классификация информационных сетей. Основные понятия	6
Тема1.2Общие вопросы построения и функционирования информационных сетей	8
Раздел 2. Сетевая модель, коммутация, протоколы	**37**
Тема2.1 Структуры и архитектура телекоммуникационных сетей.	15
Тема2.2 Коммутация пакетов и каналов.	18
Тема2.3 Протоколы локальных сетей	4
Раздел 3. Сетевое оборудование, безопасность	**10**
Тема3.1 Оборудование локальных сетей	2
Тема3.2 Создание и настройка беспроводной сети	5
Тема3.3 Безопасность сети	3

Перечень рекомендуемой литературы

Основные источники:

1. Н.В. Максимов, И.И. Попов. Компьютерные сети: учебное пособие для студентов учреждений среднего профессионального образования 4 изд. Испр. –Москва: изд. Форум, 2014 – 464 с.
2. Б.Д. Виснадул, П.Ю. Чумаченко, С.А. Лупин, С.В. Сидоров. Основы компьютерных сетей: Учебное пособие для среднего профессионального образования (под ред. Л.Г. Гагариной) Москва: Инфра-М, Форум 2014. – 272 с.
3. А.В. Кузин, В.М. Демин Компьютерные сети – М:Форум, 2014 -192с.

Дополнительные источники:

1. С.В. Киселев, И.Л. Киселев. Основы сетевых технологий – Москва: Академия, 2014 – 64 с.
2. В.Л. Бройдо Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2014 - 703 с.

3. С.А. Пескова, А.В. Кузин, А.Н. Волков. Сети и телекоммуникации – Москва: изд. «Академия», 2014 – 352с.

Раздел1. Основы компьютерных сетей
Тема1.1 Классификация информационных сетей. Основные понятия

Практическая работа №1
«Оценка пропускной способности каналов связи».

Задачи обучающегося:

1. Научиться определять пропускную способность канала в зависимости от полосы частот и отношения сигнал-шум
2. Научиться определять пропускную способность канала в зависимости от полосы частот и отношения сигнал-шум

Опорные понятия: канал связи
Планируемый результат:
Студент должен
Знать методы расчета пропускной способности
Уметь рассчитывать пропускную способность сети исходя из варианта ее использования
Необходимое оборудование: учебная литература, ПК, интернет

Критерии оценки пропускной способности

Со времени возникновения теории телетрафика было разработано множество методов расчета пропускных способностей каналов. Однако в отличие от методов расчета, применяемых к сетям с коммутацией каналов, расчет требуемой пропускной способности в пакетных сетях довольно сложен и вряд ли позволит получить точные результаты. В первую очередь это связано с огромным количеством факторов (в особенности присущих современным мультисервисным сетям), которые довольно сложно предугадать. В IP-сетях общая инфраструктура, как правило, используется множеством приложений, каждое из которых может использовать собственную, отличную от других модель трафика. Причем в рамках одного сеанса трафик, передаваемый в прямом направлении, может отличаться от трафика, проходящего в обратном направлении. Вдобавок к этому расчеты осложняются тем, что скорость трафика между отдельно взятыми узлами сети может изменяться. Поэтому в большинстве случаев при построении сетей оценка пропускной способности фактически обусловлена общими рекомендациями производителей, статистическими исследованиями и опытом других организаций.

Чтобы более или менее точно определить, какая пропускная способность требуется для проектируемой сети, необходимо в первую очередь знать, какие приложения будут использоваться. Далее для каждого приложения следует проанализировать, каким образом будет происходить передача данных в течение выбранных промежутков времени, какие протоколы для этого применяются.

Для простого примера рассмотрим приложения небольшой корпоративной сети.

Пример расчета пропускной способности

Предположим, в сети расположены 300 рабочих компьютеров и столько же IP-телефонов. Планируется использовать такие сервисы: электронная почта, IP-телефония, видеонаблюдение (рис. 1). Для видеонаблюдения применяются 20 камер, с которых видеопотоки передаются на сервер. Попытаемся оценить, какая максимальная пропускная способность потребуется для всех сервисов на каналах между коммутаторами ядра сети и на стыках с каждым из серверов.

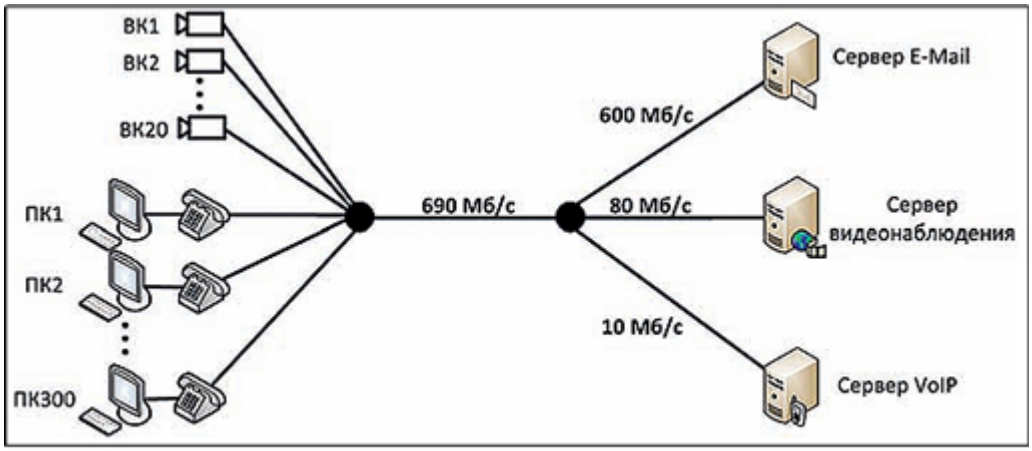


Рис. 1. Пример расчета пропускной способности для простейшей топологии сети

Следует сразу отметить, что все расчеты нужно проводить для времени наибольшей сетевой активности пользователей (в теории телетрафика – ЧНН, часы наибольшей нагрузки), поскольку обычно в такие периоды работоспособность сети наиболее важна и возникающие задержки и отказы в работе приложений, связанные с нехваткой пропускной способности, неприемлемы. В организациях наибольшая нагрузка на сеть может возникать, например, в конце отчетного периода или в сезонный наплыв клиентов, когда совершается наибольшее количество телефонных вызовов и отправляется большая часть почтовых сообщений.

Электронная почта

Возвращаясь к нашему примеру, рассмотрим сервис электронной почты. В нем используются протоколы, работающие поверх TCP, то есть скорость передачи данных постоянно корректируется, стремясь занять всю доступную пропускную способность. Таким образом, будем отталкиваться от максимального значения задержки отправки сообщения – предположим, 1 секунды будет достаточно, чтобы пользователю было комфортно. Далее нужно оценить средний объем отправляемого сообщения. Предположим, что в пиках активности почтовые сообщения часто будут содержать различные вложения (копии счетов, отчеты и т.д.), поэтому для нашего примера средний размер сообщения возьмем 500 кбайт. И наконец, последний параметр, который нам необходимо выбрать, – максимальное число сотрудников, которые одновременно отправляют сообщения. Предположим, во время авралов половина сотрудников одновременно нажмут кнопку "Отправить" в почтовом клиенте. Тогда требуемая максимальная пропускная способность для трафика электронной почты составит (500 кбайт x 150 хостов)/1 с = 75 000 кбайт/с или 600 Мбит/с. Отсюда сразу можно сделать вывод, что для соединения почтового сервера с сетью необходимо использовать канал Gigabit Ethernet. В ядре сети это значение будет одним из слагаемых, составляющих общую требуемую пропускную способность.

Телефония и видеонаблюдение

Другие приложения – телефония и видеонаблюдение – в своей структуре передачи потоков схожи: оба вида трафика передаются с использованием протокола UDP и имеют более или менее фиксированную скорость передачи. Главные отличия в том, что у телефонии потоки являются двунаправленными и ограничены временем вызова, у видеонаблюдения потоки передаются в одном направлении и, как правило, являются непрерывными.

Чтобы оценить требуемую пропускную способность для трафика телефонии, предположим, что в пики активности количество одновременных соединений, проходящих через шлюз, может достигать 100. При использовании кодека G.711 в сетях Ethernet скорость одного потока с учетом заголовков и служебных пакетов составляет примерно 100 кбит/с. Таким образом, в периоды наибольшей активности пользователей требуемая пропускная способность в ядре сети составит 10 Мбит/с.

Трафик видеонаблюдения рассчитывается довольно просто и точно. Допустим, в нашем случае видеокамеры передают потоки по 4 Мбит/с каждая. Требуемая пропускная способность будет равна сумме скоростей всех видеопотоков: 4 Мбит/с х 20 камер = 80 Мбит/с.

Витоге осталось сложить полученные пиковые значения для каждого из сетевых сервисов: 600 + 10 + 80 = 690 Мбит/с. Это и будет требуемая пропускная способность в ядре сети. При проектировании следует также предусмотреть и возможность масштабирования, чтобы каналы связи могли как можно дольше обслуживать трафик разрастающейся сети. В нашем примере будет достаточно использования Gigabit Ethernet, чтобы удовлетворить требованиям сервисов и одновременно иметь возможность беспрепятственно развивать сеть, подключая большее количество узлов

Конечно же, приведенный пример является далеко не эталонным – каждый случай нужно рассматривать отдельно. В реальности топология сети может быть гораздо сложнее (рис. 2), и оценку пропускной способности необходимо производить для каждого из участков сети.

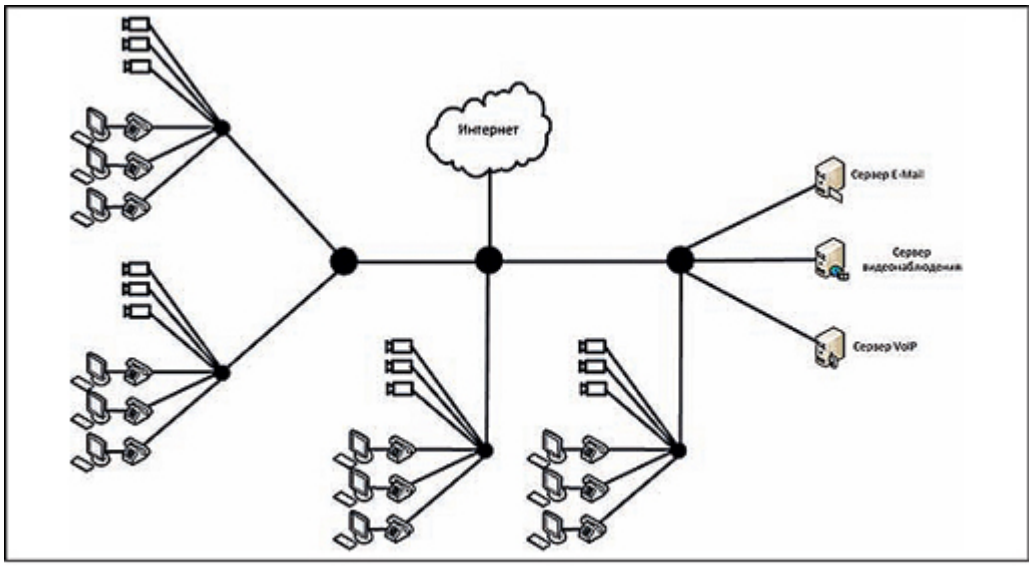


Рис. 2. Пример распределенной топологии сети предприятия

Нужно учитывать, что VoIP-трафик (IP-телефония) распространяется не только от телефонов к серверу, но и между телефонами напрямую. Кроме того, в разных отделах организации сетевая активность может различаться: служба техподдержки совершает больше телефонных вызовов, отдел проектов активнее других пользуется электронной почтой, инженерный отдел больше других потребляет интернет-трафик и т.д. В результате некоторые участки сети могут требовать большей пропускной способности по сравнению с остальными.

Полезная и полная пропускная способность

В нашем примере при расчете скорости потока IP-телефонии мы учитывали используемый кодек и размеры заголовка пакета. Это немаловажная деталь, которую нужно иметь в виду. В зависимости от способа кодирования (используемые кодеки), объема данных, передаваемых в каждом пакете, и применяемых протоколов канального уровня формируется полная пропускная способность потока. Именно полная пропускная способность должна учитываться при оценке требуемой пропускной способности сети. Это наиболее актуально для IP-телефонии и других приложений, использующих передачу низкоскоростных потоков в реальном времени, в которых размер заголовков пакета составляет существенную часть от размера пакета целиком. Для наглядности сравним два потока VoIP (см. таблицу). Эти потоки используют одинаковое сжатие, но разные размеры полезной нагрузки (собственно, цифровой аудиопоток) и разные протоколы канального уровня.

Сравнение двух потоков VoIP

Параметр	Поток 1	Поток 2
Используемый кодек	G.729 (8 кбит/с)	G.729 (8 кбит/с)
Размер полезной нагрузки	20 байт	60 байт
Протокол канального уровня	Ethernet	PPP
Суммарный размер пакета с учетом заголовка канального уровня	78 байт	106 байт
Полная пропускная способность потока	31,2 кбит/с	14,3 кбит/с

Скорость передачи данных в чистом виде, без учета заголовков сетевых протоколов (в нашем случае – цифрового аудиопотока), есть полезная пропускная способность. Как видно из таблицы, при одинаковой полезной пропускной способности потоков их полная пропускная способность может сильно различаться. Таким образом, при расчете требуемой пропускной способности сети для телефонных вызовов в пиковые нагрузки, особенно у операторов связи, выбор канальных протоколов и параметров потоков играет значительную роль.

Выбор оборудования

Выбор протоколов канального уровня обычно не составляет проблемы (сегодня чаще стоит вопрос, какая пропускная способность должна быть у канала Ethernet), но вот выбор подходящего оборудования даже у опытного инженера может вызвать затруднения.

Развитие сетевых технологий одновременно с растущими потребностями приложений в пропускной способности сетей вынуждает производителей сетевого оборудования разрабатывать все новые программно-аппаратные архитектуры. Часто у отдельно взятого производителя встречаются на первый взгляд схожие модели оборудования, но предназначенные для решения разных сетевых задач. Взять, к примеру, коммутаторы Ethernet: у большинства производителей наряду с обычными коммутаторами, используемыми на предприятиях, есть коммутаторы для построения сетей хранения данных, для организации операторских сервисов и т.д. Модели одной ценовой категории различаются своей архитектурой, "заточенной" под определенные задачи.

Кроме общей производительности, выбор оборудования также должен быть обусловлен поддерживаемыми технологиями. В зависимости от типа оборудования определенный набор функций и виды трафика могут обрабатываться на аппаратном уровне, не используя ресурсы центрального процессора и памяти. При этом трафик других приложений будет обрабатываться на программном уровне, что сильно снижает общую производительность и, как следствие, максимальную пропускную способность. Например, многоуровневые коммутаторы, благодаря сложной аппаратной архитектуре, способны осуществлять передачу IP-пакетов без снижения производительности при максимальной загрузке всех портов. При этом если мы захотим использовать более сложную инкапсуляцию (GRE, MPLS), то такие коммутаторы (по крайней мере недорогие модели) вряд ли нам подойдут, поскольку их архитектура не поддерживает соответствующие протоколы, и в лучшем случае такая инкапсуляция будет происходить за счет центрального процессора малой производительности. Поэтому для решения подобных задач можно рассматривать, например, маршрутизаторы, у которых архитектура основана на высокопроизводительном центральном процессоре и в большей степени зависит от программной, нежели аппаратной реализации. В этом случае в ущерб максимальной пропускной способности мы получаем огромный набор поддерживаемых протоколов и технологий, которые не поддерживаются коммутаторами той же ценовой категории.

Общая производительность оборудования

В документации к своему оборудованию производители часто указывают два значения максимальной пропускной способности: одно выражается в пакетах в секунду, другое – в битах в секунду. Это связано с тем, что большая часть производительности сетевого оборудования расходуется, как правило, на обработку заголовков пакетов. Грубо говоря, оборудование должно принять пакет, найти для него подходящий путь коммутации,

сформировать новый заголовок (если нужно) и передать дальше. Очевидно, что в этом случае играет роль не объем данных, передаваемых в единицу времени, а количество пакетов.

Если сравнить два потока, передаваемых с одинаковой скоростью, но с разным размером пакетов, то на передачу потока с меньшим размером пакетов потребуется больше производительности. Данный факт следует учитывать, если в сети предполагается использовать, например, большое количество потоков IP-телефонии – максимальная пропускная способность в битах в секунду здесь будет гораздо меньше заявленной.

Понятно, что при смешанном трафике, да еще и с учетом дополнительных сервисов (NAT, VPN), как это бывает в подавляющем большинстве случаев, очень сложно рассчитать нагрузку на ресурсы оборудования. Часто производители оборудования или их партнеры проводят нагрузочное тестирование разных моделей при разных условиях и результаты публикуют в Интернете в виде сравнительных таблиц. Ознакомление с этими результатами сильно упрощает задачу выбора подходящей модели.

Подводные камни модульного оборудования

Если выбранное сетевое оборудование является модульным, то, кроме гибкой конфигурации и масштабируемости, обещанной производителем, можно получить и множество "подводных камней".

При выборе модулей следует тщательно ознакомиться с их описанием или проконсультироваться у производителя. Недостаточно руководствоваться только типом интерфейсов и их количеством – нужно также ознакомиться и с архитектурой самого модуля. Для похожих модулей нередка ситуация, когда при передаче трафика одни способны обрабатывать пакеты автономно, а другие просто пересылают пакеты центральному процессорному модулю для дальнейшей обработки (соответственно для одинаковых внешне модулей цена на них может различаться в несколько раз). В первом случае общая производительность оборудования и, как следствие, его максимальная пропускная способность оказываются выше, чем во втором, поскольку часть своей работы центральный процессор перекладывает на процессоры модулей.

Кроме этого, модульное оборудование часто обладает блокируемой архитектурой (когда максимальная пропускная способность ниже суммарной скорости всех портов). Это связано с ограниченной пропускной способностью внутренней шины, через которую модули осуществляют обмен трафиком между собой. Например, если модульный коммутатор имеет внутреннюю шину с пропускной способностью 20 Гбит/с, то для его линейной платы с 48 портами Gigabit Ethernet при полной загрузке можно использовать только 20 портов. Подобные детали нужно также иметь в виду и при выборе оборудования внимательно читать документацию.

Общие рекомендации

При проектировании IP-сетей пропускная способность является ключевым параметром, от которого будет зависеть архитектура сети в целом. Для более точной оценки пропускной способности, можно руководствоваться следующим рекомендациям:

Задание для выполнения

В рамках практической работы необходимо:

1.Рассчитать пропускную способность сети небольшого предприятия (на выбор).

2.Обосновать выбор оборудования и линий связи

Раздел1. Основы компьютерных сетей
Тема1.1 Классификация информационных сетей. Основные понятия

Практическая работа №2
«Преобразование форматов IP-адресов».

Задачи обучающегося:

1. Перевести числа из одной системы счисления в другую
2. Разбираться в понятиях IP адрес, маска подсети
3. Определять классы IP адресов

Опорные понятия:адресация узлов в сети
Планируемый результат:
Студент должен
Уметь преобразовывать форматы различных IPадресов.
Необходимое оборудование: учебная литература, ПК, браузер

Алгоритм деятельности обучающегося:

Задание 1. Переведите следующие двоичные числа в десятичные.

Двоичное значение

а) 1111011
б) 1001001101
в) 101101111
г) 1011110001
д) 10101100.00101000.00000000.00000000
е) 01011110.01110111.10011111.00000000
ж) 10010001 0110000 10000000 00011001
з) 0111111100000000 00000000 00000001

Задание 2. Переведите следующие десятичные числа в двоичные.

Десятичное значение

а) 250
б) 19
в) 348
г) 93
д) 874
е) 109.128.255.254
ж) 131.107.2.89
з) 129.46.78.0

Задание 3. Укажите классы следующих IP-адресов.

Адрес

а) 126.102.128.0
б) 1.191.248.0
в) 185.74.41.184
г) 96.247.128.0
д) 168.224.0.1
е) 201.76.98.5
ж) 186.112.0.10
з) 28.0.0.0

Задание 4. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

а) 131.107.256.80
б) 222.222.255.222
в) 31.200.1.1
г) 126.1.0.0
д) 190.7.2.0
е) 127.1.1.1
ж) 198.121.254.255
з) 255.255.255.255

Контрольные вопросы:

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?

2. Какие значения не могут быть использованы в качестве идентификаторов сетей и почему?

Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?

3. Когда необходим уникальный идентификатор сети?

4. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

Раздел1. Основы компьютерных сетей
Тема1.2Общие вопросы построения и функционирования информационных сетей

Практическая работа №3
«Расчет циклических контрольных сумм».

Задачи обучающегося:

1. Познакомиться с методами расчета контрольных сумм.
2. Изучить 1-битный и 8-битный метод
3. Составить отчет о проделанной работе

Опорные понятия: контрольная сумма
Планируемый результат:
Студент должен
Знать понятия «бит-четности» и «контрольная сумма», их дифференциацию.
Производить расчет контрольных сумм исходя из условий.
Необходимое оборудование: учебная литература, калькулятор контрольных сумм, ПК, интернет

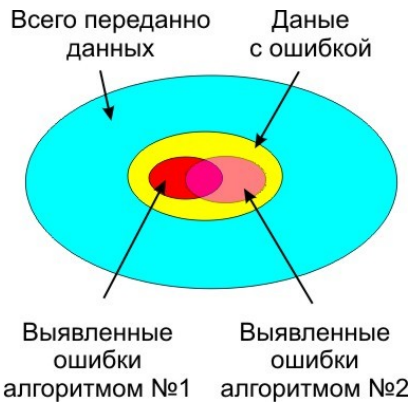
Алгоритм деятельности обучающегося:

Изучите теоретический материал

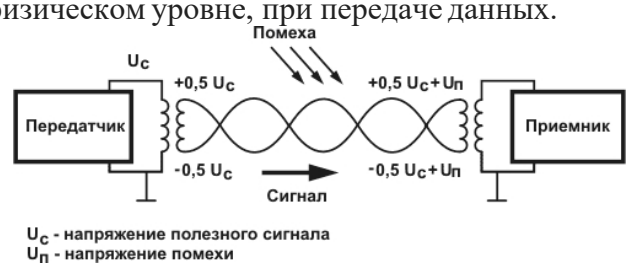
При передачи данных по линиям связи, используетсяконтрольная сумма, рассчитанная по некоторому алгоритму. Алгоритм часто сложный, конечно, он обоснован математически, но очень уж неудобен при дефиците ресурсов, например при программировании микроконтроллеров.

Чтобы упростить алгоритм, без потери качества, нужно немного «битовой магии», что интересная тема сама по себе.

Без контрольной суммы, передавать данные опасно, так как помехи присутствуют везде и всегда, весь вопрос только в их вероятности возникновения и вызываемых ими побочных эффектах. В зависимости от условий и выбирается алгоритм выявления ошибок и количество данных в контрольной сумме. Сложнее алгоритм, и больше контрольная сумма, меньше не распознанных ошибок.



Причина помех на физическом уровне, при передаче данных.



Вот пример самого типичного алгоритма для микроконтроллера, ставшего, фактически, промышленным стандартом с 1979 года.

Бит четности (1-битная контрольная сумма)

На первом месте простой бит четности. При необходимости формируется аппаратно, принцип простейший, иподробно расписан в википедии. Недостаток только один, пропускает двойные ошибки (и вообще четное число ошибок), когда четность всех бит не меняется. Можно использовать для сбора статистики о наличии ошибок в потоке передаваемых данных, но целостность данных не гарантирует, хотя и снижает вероятность пропущенной ошибки на 50% (зависит, конечно, от типа помех на линии, в данном случае подразумевается что число четных и нечетных сбоев равновероятно).

Для включения бита четности, часто и код никакой не нужен, просто указываем что UART должен задействовать бит четности.

8-битная контрольная сумма

Если контроля четности мало (а этого обычно мало), добавляется дополнительная контрольная сумма. Рассчитать контрольную сумму, можно как сумму ранее переданных байт, просто и логично.

$$CRC = byte(1) + byte(2) + byte(3) + ... + byte(N)$$

Естественно биты переполнения не учитываем, результат укладываем в выделенные под контрольную сумму 8 бит. Можно пропустить ошибку, если при случайном сбое один байт увеличится на некоторое значение, а другой байт уменьшится на то же значение. Контрольная сумма не изменится. Проведем эксперимент по передаче данных. Исходные данные такие:

1. Блок данных 8 байт.
2. Заполненность псевдослучайными данными Random($FF+1)
3. Случайным образом меняем 1 бит в блоке данных операцией XOR со специально подготовленным байтом, у которого один единичный бит на случайной позиции.
4. Повторяем предыдущий пункт 10 раз, при этом может получится от 0 до 10 сбойных бит (2 ошибки могут накладываться друг на друга восстанавливая данные), вариант с 0 сбойных бит игнорируем в дальнейшем как бесполезный для нас.

Передаем виртуальную телеграмму N раз. Идеальная контрольная сумма выявит ошибку по количеству доступной ей информации о сообщении, больше информации, выше вероятность выявления сбойной телеграммы. Вероятность пропустить ошибку, для 1 бита контрольной суммы:

$$P = 1/(2^1) = 0.5.$$

Для 8 бит:

$$P = 1/(2^8) = 1 : 256.$$

Задания для выполнения:

1.Выполните расчет контрольных сумм с помощью онлайн-калькулятора:

https://hash.online-convert.com/ru/crc32-generator

2.Оформите отчет по проделанной работе

Раздел1. Основы компьютерных сетей
Тема1.2Общие вопросы построения и функционирования информационных сетей

Практическая работа №4
«Установка и настройка DHCP-сервера».

Задачи обучающегося:

1. Научиться добавлять и настраивать роль DHCP-сервера на дополнительном контроллере домена
2. Познакомиться с понятием DHCP-сервер и его функцией в сети.

Опорные понятия:DHCP-сервер
Планируемый результат:
Студент должен
Знать понятия «распределение IP-адресов»
Знать и выполнять работы по развертыванию и настройке DHCP сервера
Необходимое оборудование: учебная литература, ПК, программное обеспечение: VirtualBox

Алгоритм деятельности обучающегося:

Теоретические сведения:

DHCP (англ. 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.

Протокол DHCP используется в большинстве сетей TCP/IP. DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

Распределение IP-адресов

Протокол DHCP предоставляет три способа распределения IP-адресов:

Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

Автоматическое распределение.

При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона. Динамическое распределение.

Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса.

По истечении срока аренды IP-адрес вновь 22.01.2021 2.1.10 считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса. Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов. Это производится при помощи протокола обновления DNS, описанного в RFC 2136

Практическая часть. Установка DHCPна сервер

Перед началом установки роли DHCP Server необходимо присвоить серверу корректное имя, а затем указать статический IP-адрес в настройках сетевого подключения. Кроме того сервер необходимо добавить в домен.

Заходим в систему под учетной записью с правами администратора домена
Открываем «Server Manager», нажимаем на кнопку «Manage» в правом верхнем углу экрана и выбираем «Add Roles and Features».

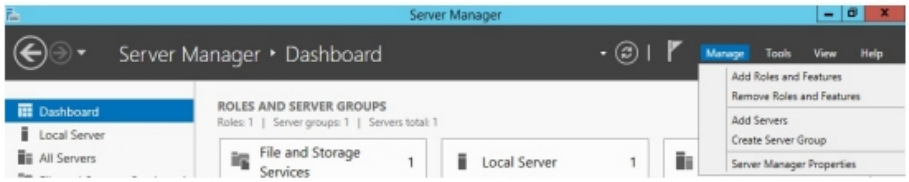


Рис. 1 – Управление сервером

Нажимаем на кнопку «Next».

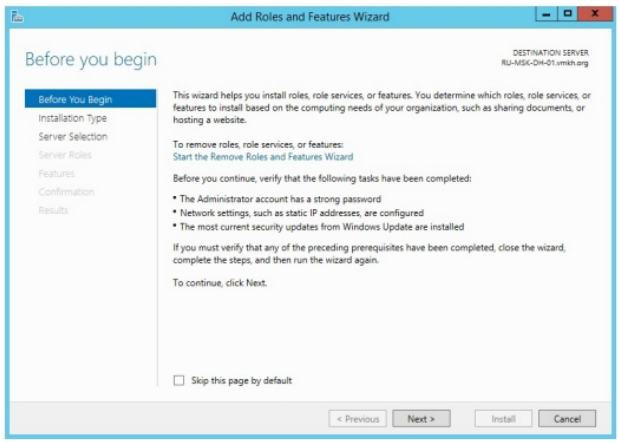


Рис.2 Окно установки ролей

Выбираемтипустановки «Role-basedorfeature-basedinstallation» инажимаемнакнопку «Next».

Нажимаем на кнопку «Next».

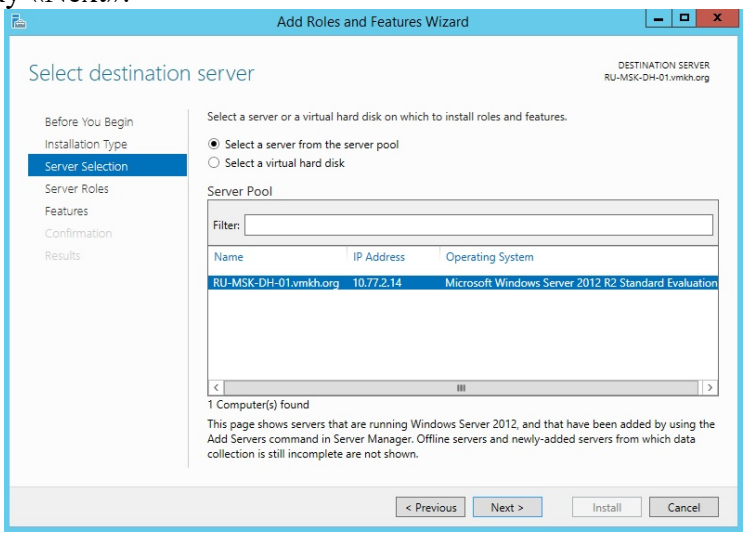


Рис. 5 Окно выбора в сервера, на который будет производиться установка роли

Выбираем роль «DHCP Server».

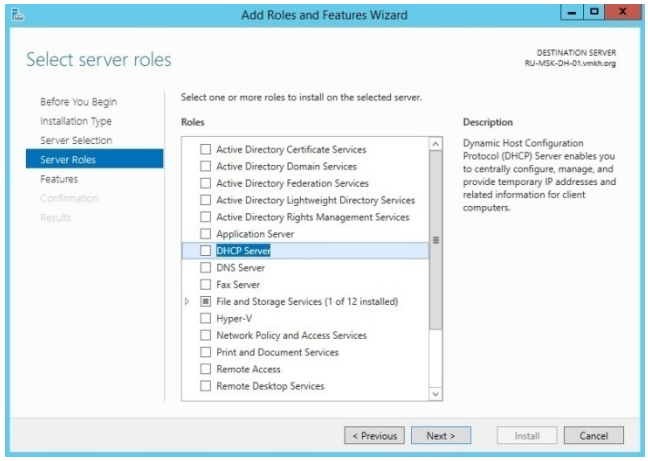


Рис. 5 Выбор роли «DHCP Server»

На следующем этапе «Мастер установки ролей» предупредит, что для установки роли «DHCP Server» нужно установить несколько компонентов.
Нажимаем на кнопку «Add Features».

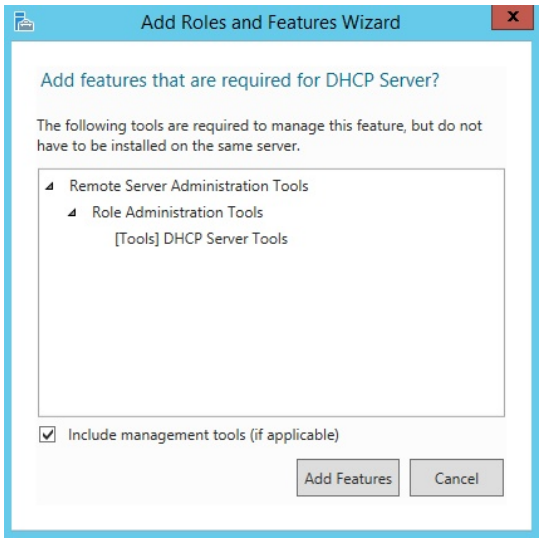


Рис. 6 Установка дополнительных компонентов

Нажимаем на кнопку «Next».

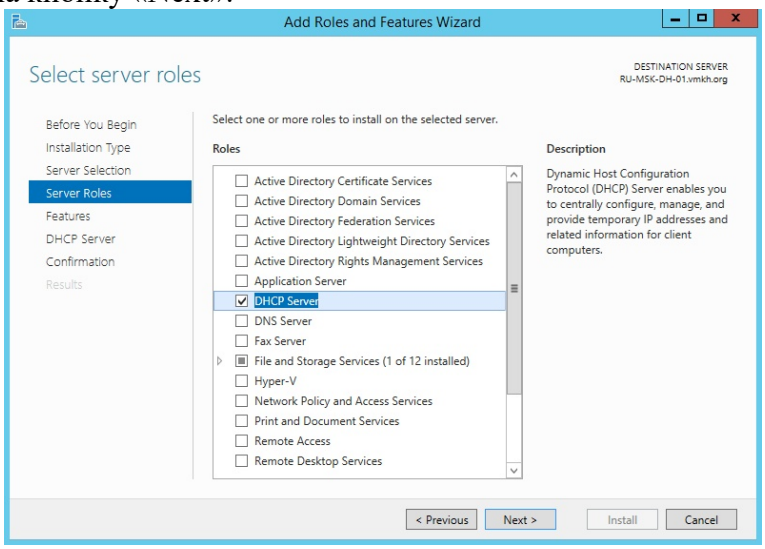


Рис. 7 Нажимаем кнопку Next

На этапе добавления компонентов оставляем все значения по умолчанию.
Нажимаем на кнопку «Next».

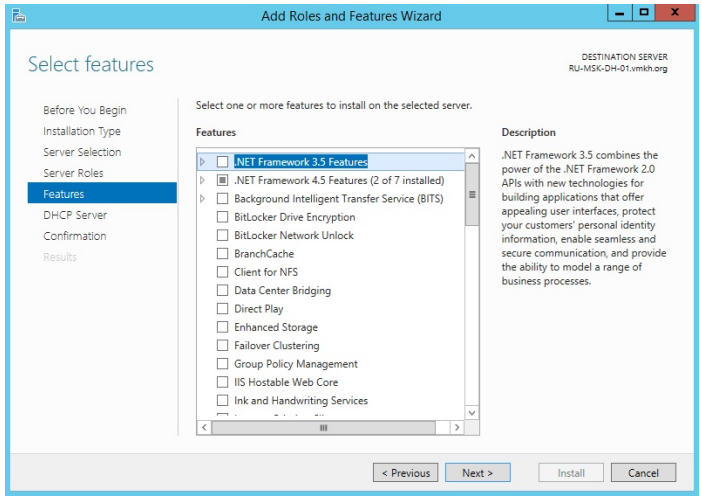


Рис. 8 Этап добавления компонентов

Далее «Мастер установки ролей» предлагает ознакомиться с дополнительной информацией касательно роли «DHCP Server».
Нажимаем на кнопку «Next».

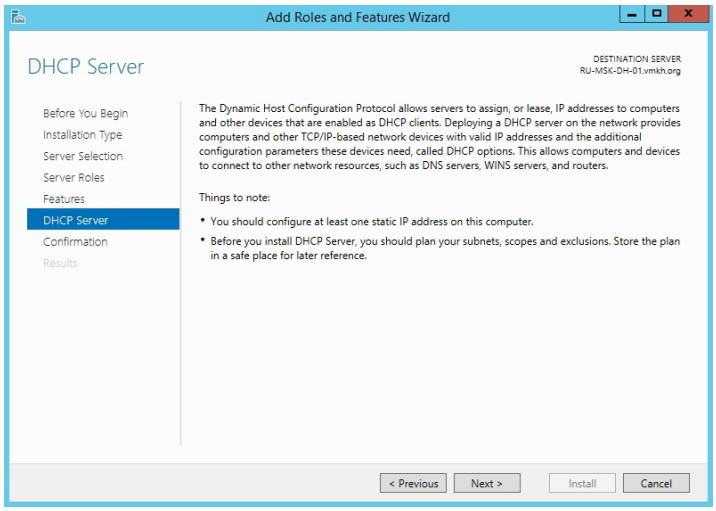


Рис.9 дополнительная информация относительно роли «DHCP Server»
Для установки роли, нажимаем на кнопку «Install».

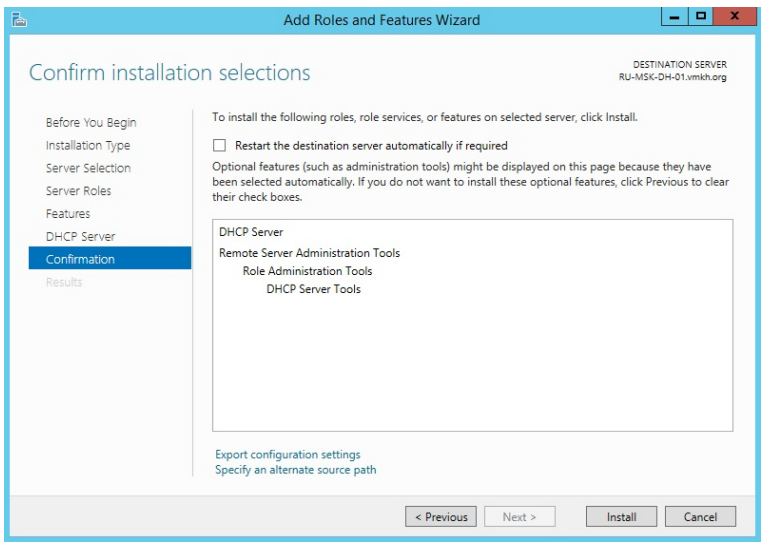


Рис. 10 Процесс установки начинается с нажатия кнопки Install

Началась установка выбранной роли и необходимых для нее компонентов.

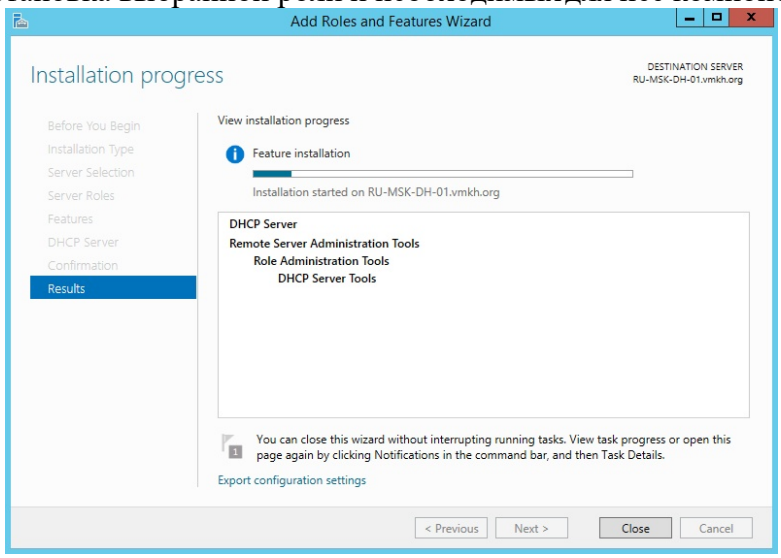


Рис. 11 Процесс установки роли

Установка роли «DHCP Server» завершена.
Теперь нажимаем на кнопку «Complete DHCP configuration», для того чтобы настроить сервер DHCP.

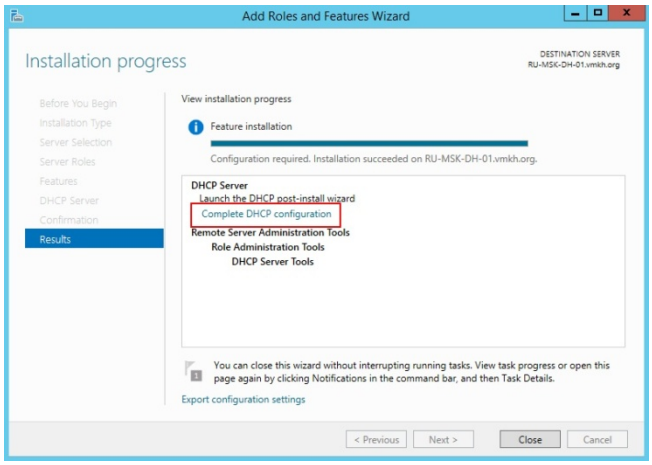


Рис. 12 Завершение уствновки роли. Выбор кнопки настройки DHCP сервера

Вам сообщат, что далее будут созданы две локальные группы безопасности для управления доступом к серверу DHCP, а затем будет произведена авторизация сервера DHCP в Active Directory.
Нажимаем на кнопку «Next».

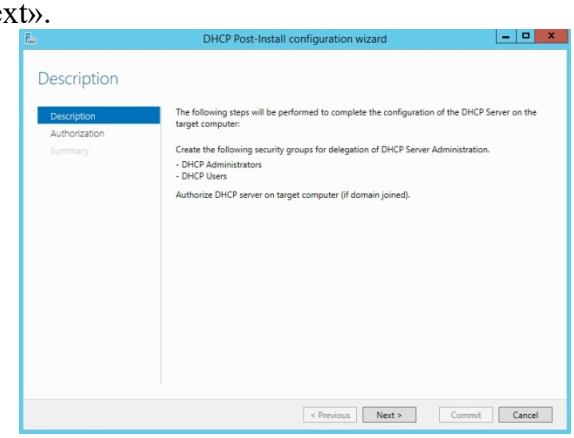


Рис. 13 Окно с сообщением о создании двух локальных групп безопасности

В разделе «Use the following user’s credentials» указываем учетную запись с правами

администратора домена.
Нажимаем на кнопку «Commit».

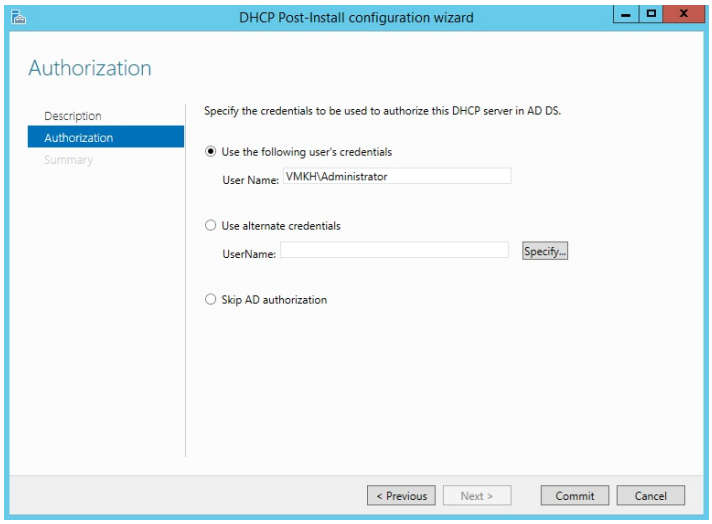


рис. 14 Указание учетной записи с правами администратора

Сервер DHCP авторизован в Active Directory, а также созданы необходимые группы безопасности для управления доступом к DHCP.
Нажимаем на кнопку «Close».

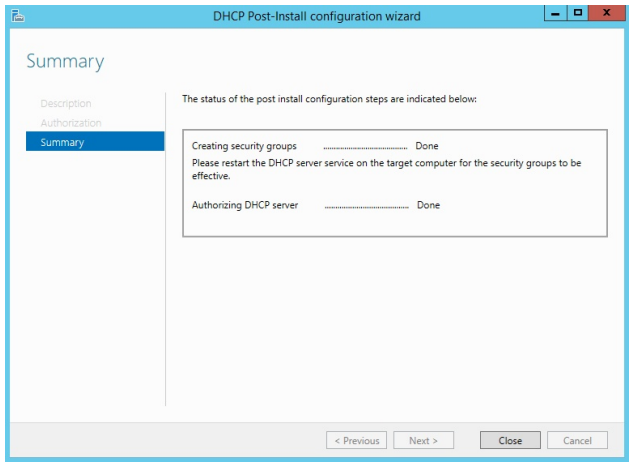


Рис. 15 Сервер DHCP авторизован в Active Directory

Возвращаемся в «Мастер установки ролей» и нажимаем на кнопку «Close».

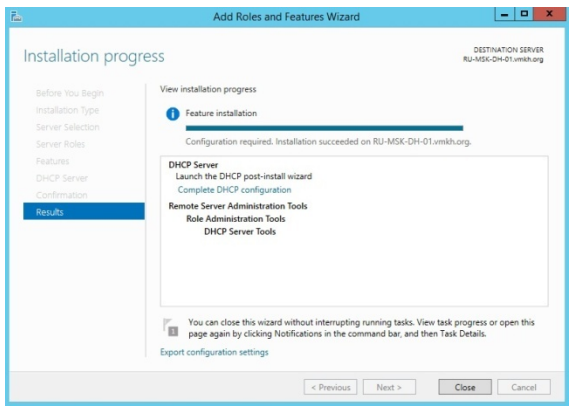


Рис. 16 Закрываем окно “Мастера установки ролей”

Проверяем, что две группы безопасности создались успешно.
На клавиатуре нажимаем сочетание клавиш «Win» и «X», затем в открывшемся меню выбираем «Computer Management».

Рис. 17 Проверяем установку локальных групп безопасности

Далеевразделе «Local Users and Groups» находим «Groups».

В правой части экрана отображаются все локальные группы безопасности. Среди них должна быть группа «DHCP Administrators», участники которой имеют полный доступ к управлению DHCP, а также группа «DHCP Users», участники которой имеют доступ только на просмотр настроек DHCP.

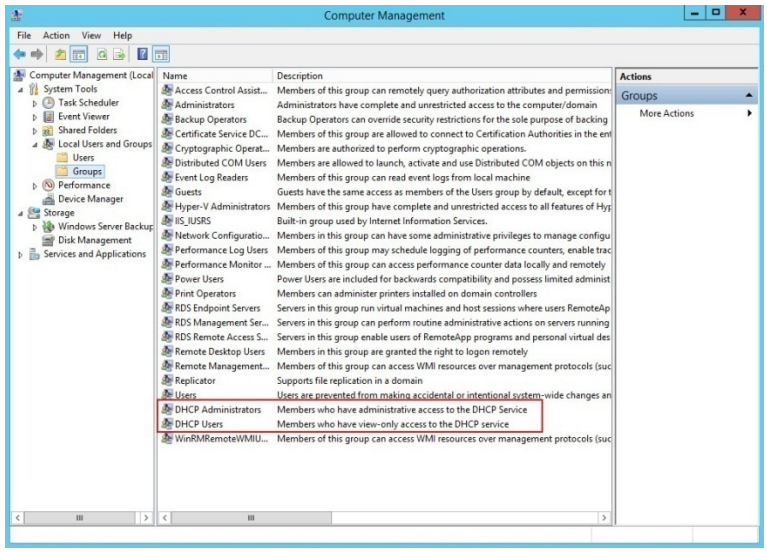


Рис. 18 Созданные группы безопасности

Произведем настройки сервера DHCP так, чтобы он раздавал сетевые настройки (IP-адрес, маска подсети, шлюз, DNS) для всех устройств, которые будут подключаться к локальной сети.

В Server Manager, нажимаем на кнопку «Tools» в правом верхнем углу экрана и выбираем «DHCP».

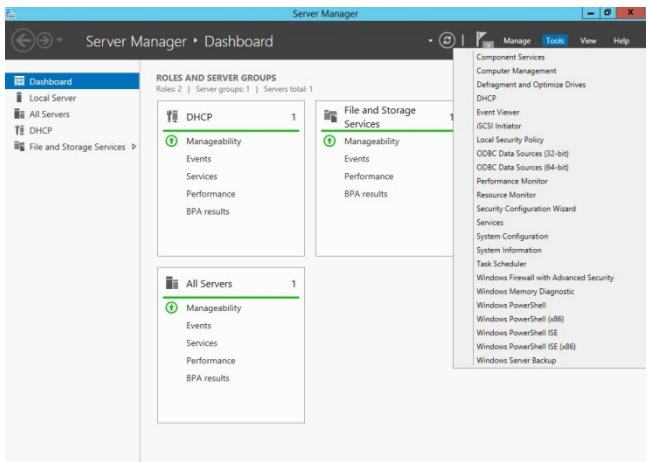


Рис. 19 Настройка DHCP на автоматическую раздачу IP – адресов

Укажем диапазон адресов, из которого сервер DHCP будет раздавать IP-адреса для устройств в локальной сети.

Нажимаем правой кнопкой мыши на «IPv4» и в открывшемся меню выбираем «New Scope».

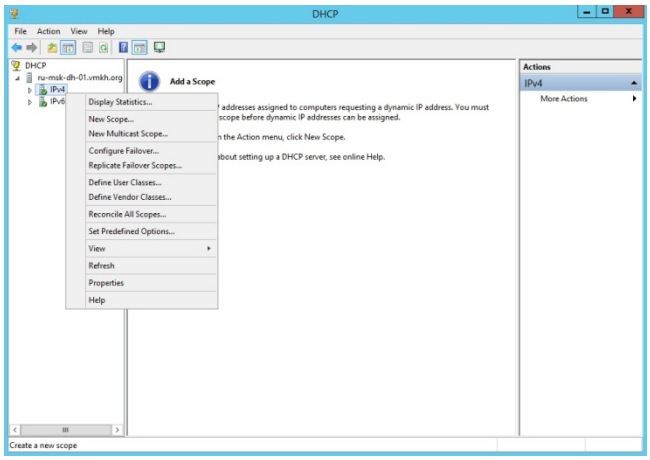


Рис. 20 Создание диапазона IP-адресов

Нажимаем на кнопку «Next».

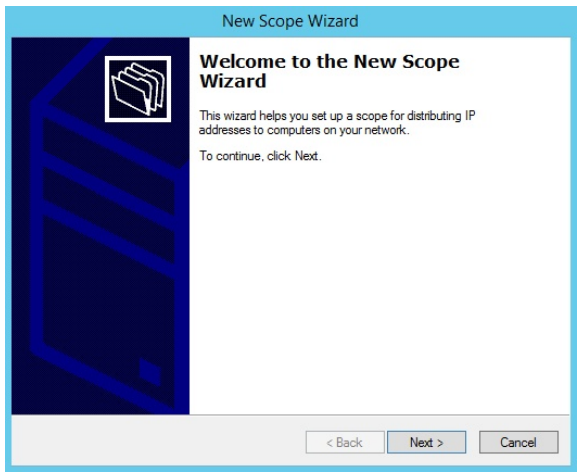


Рис. 21 Нажимаес кнопку Next

В поле «Name» указываем имя для нового диапазона адресов.
Нажимаем на кнопку «Next».

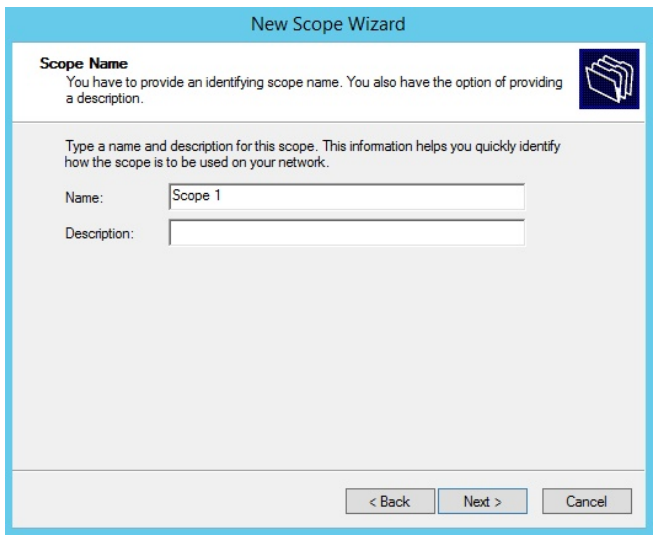


Рис. 22 Ввод имени для диапазона адресов

Указываем маску подсети и диапазон адресов, из которого сервер DHCP будет раздавать IP-адреса для устройств в локальной сети.
Нажимаем на кнопку «Next».

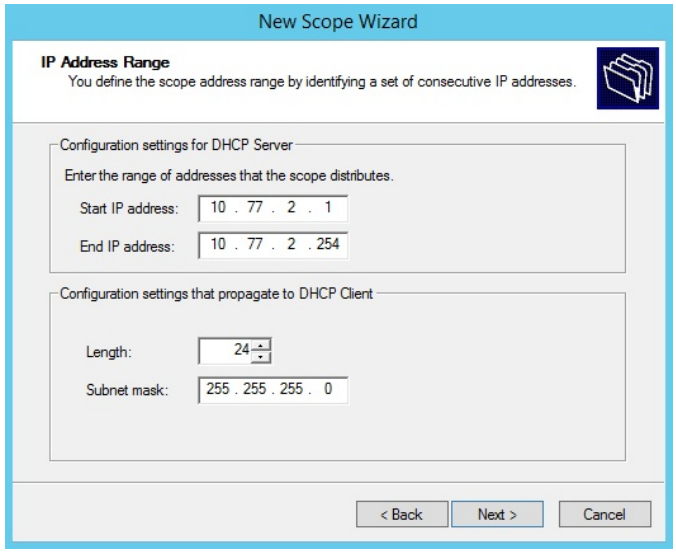


Рис. 23 Указание диапазона адресов и маски подсети

Теперь можно указать диапазон, для которого сервер DHCP не будет раздавать настройки.

Это может пригодиться, если вы знаете, что в определенном диапазоне адресов находятся сервера, принтеры или другие устройства, которым уже присвоен статический IP-адрес. В таком случае нужно исключить эту часть диапазона, так как IP-адреса из него уже используются. Также нужно исключить IP-адрес, который присвоен шлюзу.

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.1Структуры и архитектура телекоммуникационных сетей
Практическая работа №5
«Адресация в IP-сетях. Подсети и маски».

Задачи обучающегося:

1. Изучить понятия адресации в IP сетях
2. Определение количества подсетей

Опорные понятия:подсети и маски
Планируемый результат:
Студент должен
Знать понятия «IP-адрес» и «маска подсети»
Необходимое оборудование: учебная литература,ПК

Алгоритм деятельности обучающегося:

Задание 1.

Выполните логическую операцию «И» с перечисленными ниже IP-адресами и маской подсети и определите, принадлежит ли IP-адрес получателя к локальной или удаленной сети.

IP-адрес отправителя	10011001 1010101000100101 10100011
Маска подсети	11111111111111110000000000000000
Результат	
IP-адрес получателя	11011001 10101010 10101100 11101001
Маска подсети	11111111111111110000000000000000
Результат	

1. Получен ли одинаковый результат?
2. Принадлежит IP-адрес получателя к локальной или удаленной сети?

Задание 2. Для заданных IP-адресов классов A, B и C и предложенных масок определить:

- класс адреса;
- максимально возможное количество подсетей;
- диапазон изменения адресов подсетей;

- максимальное число узлов в подсетях.

№	Адрес	Маска
1.	135.209.23.246	11111111.11111111.11111111.11000000
2.	200.131.197.27	11111111.11111111.11111111.11111000
3.	214.147.120.38	11111111.11111111.11111111.11110000
4.	176.72.82.62	11111111.11111111.11111111.10000000
5.	82.67.174.114	11111111.11000000.00000000.00000000

Задание 3.

По заданным классу (A, B или C), количеству подсетей N и максимальному количеству компьютеров M1…MN в каждой подсети определить маску для разбиения на подсети. Сделать вывод о возможности такого разбиения. Если разбиение невозможно, то сформулируйте рекомендации по изменению каких-либо исходных данных для обеспечения возможности разбиения.

1.	Класс	A						
	N	3						
	M1…MN	1568		55996		1555847		
2.	Класс	B						
	N	4						
	M1…MN	1024		2048		4069		1024
3.	Класс	C						
	N	8						
	M1…MN	12	10	5	8	15	16	13	12

Контрольные вопросы:

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?
2. Какие значения не могут быть использованы в качестве идентификаторов сетей и почему?
3. Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?
4. Когда необходим уникальный идентификатор сети?
5. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.1Структуры и архитектура телекоммуникационных сетей

Практическая работа №6

«Установка и настройка сетевой операционной системы».

Задачи обучающегося:

1. Провести установку и настройку операционной системы.
2. Обобщениеи систематизация знаний по теме «Адресация в сетях»

Опорные понятия:операционная система

Планируемый результат:

Студент должен

Знать понятие сетевой операционной системы

Уметь правильно устанавливать и конфигурировать операционную систему

Необходимое оборудование: учебная литература: Психология/Под ред. И.В.Дубровиной

Алгоритм деятельности обучающегося:

Задания к работе

После установки диска и начала инсталляции вы увидите первую страницу мастера установки, на которой нужно будет определить языковые параметры, формат времени и валюты и способ ввода через клавиатуру или другое устройство. Нажимаем Далее после выбора всех опций.

Рис.1. Страница мастера установки

Нажимаем кнопку установить сейчас (Install now).

Рис.2. Install now

В инсталяционном диске содержатся все версии Windows Server 2008 R2, и мы можем выбрать версию, которую хотим установить. Обратите внимание, что можно даже установить версии Server Core. Но мы не будем устанавливать версию ядра сервера. Давайте выберем опцию Windows Server 2008 R2 Enterprise (полная установка (Full Installation)) и нажмем Далее.

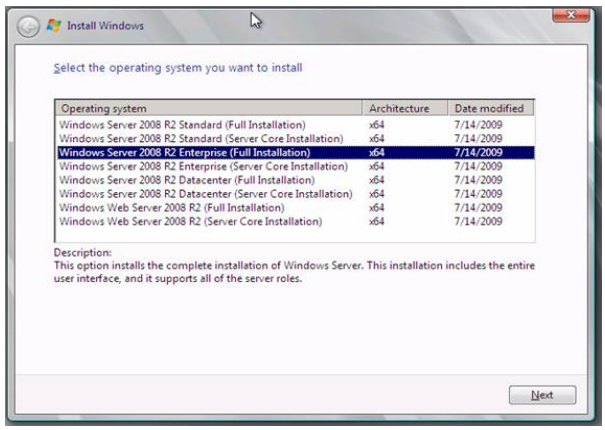


Рис.3. Full Installation

В следующем окне принимаем условия лицензионного соглашения, поставив галочку и нажимаем Далее.

Рис.4. Условия лицензионного соглашения

Нажимаем на опцию Выборочная (расширенная) - Custom (Advanced). Обратите внимание, что на этой странице нет кнопки Далее.

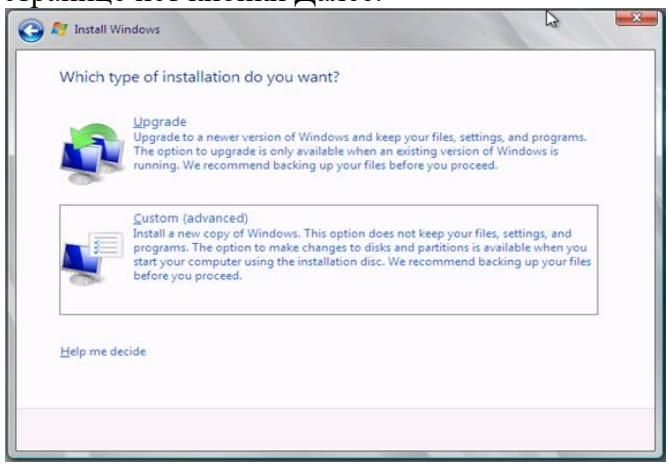


Рис. 5. Опция Выборочная (расширенная)

В следующем окне определяем, куда установить системные файлы. Выбираем имеющийся жесткий диск размером 24 ГБ для ОС, этого места будет более чем достаточно. Нажимаем Далее.

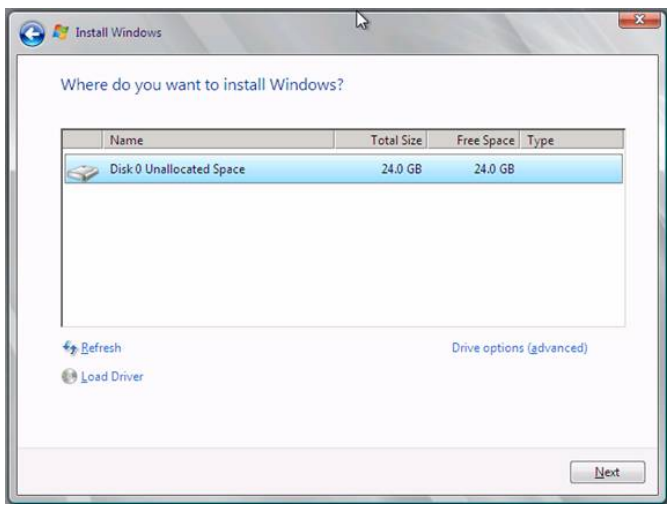


Рис. 6. Установка системных файлов

После этого - начинается непосредственно сама установка.

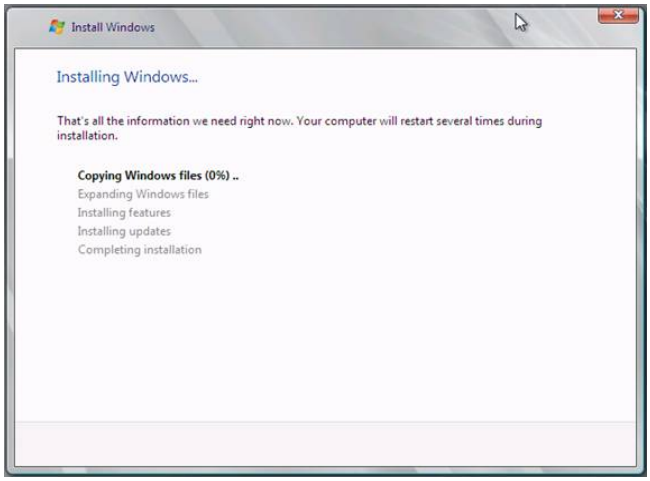


Рис. 7. Установка системных файлов

Во время первого входа в систему установщик попросит вас создать пароль. Нажмите OK, когда видите изображение, как показано ниже.

Рис. 8. Создание пароля

Введите пароль и подтверждение, но не нажимайте OK (поскольку здесь нет кнопки OK). Вместо этого нажмите на синий значок стрелки, который не имеет названия, и который расположен справа от текстового поля с подтверждением пароля.

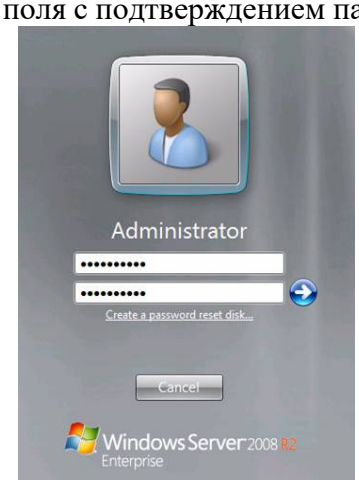


Рис 9. Подтверждение пароля

Пароль был изменен. Нажимаем OK.

Рис.10. Подтверждение пароля

Целью было обеспечить минимум вводимых данных во время установки ОС, и оставить все настройки на самый конец.

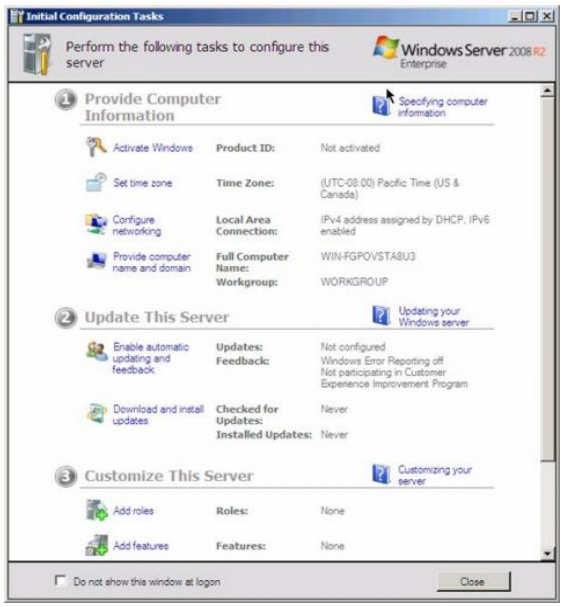


Рис 11. Настройки

На странице Initial Configuration Tasks устанавливаем следующее: часовой пояс, настройки сети, имя компьютера и домен.
Остальные настройки выполним после того, как определим IP адрес в сети для этой машины. Назовем этот сервер FFWIN2008R2DC, поскольку это будет контроллер домена в домене FFLAB. FF. Информация IP адресации будет следующей:

- IP адрес: 10.0.0.2
- Основной шлюз:‘ 10.0.0.1
- DNS: 10.0.0.2
- WINS: 10.0.0.2

Контрольные вопросы:

1.Организация функционирования ЛВС на базе операционной системы Windows Server.
2.Установка ОС и построение контроллера домена.

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.1Структуры и архитектура телекоммуникационных сетей

Практическая работа №7
«Кодирование информации».

Задачи обучающегося:

1. Провести актуализацию знаний по теме кодирование информации.
2. Определить максимально возможную разрешающую способность экрана.
3. Составить таблицу цветов при 24-битной глубине цвета в шестнадцатеричном представлении

Опорные понятия: кодирование информации
Планируемый результат:
Студент должен
Знать и выполнять кодирование информации различных видов
Необходимое оборудование: учебная литература, ПК

Алгоритм деятельности обучающегося:

1. Определить максимально возможную разрешающую способность экрана для монитора с диагональю 15” и размером точки экрана 0,28 мм.
Выразим размер диагонали в сантиметрах:
2,54 см× 15 = 38,1 см
Определим соотношение между высотой и шириной экрана для режима 1024×768 точек:
768 : 1024 = 0,75
Определим ширину экрана. Пусть ширина экрана равна L, тогда высота равна 0,75L. По теореме Пифагора имеем:
$L^2 + (0,75L)^2 = 38,1^2$
$1,5625L^2 = 1451,61$
$L^2 \approx 929$
L≈30,5 см
Количество точек по ширине экрана равно:
305 мм : 0,28 мм = 1089
Максимально возможным разрешением экрана монитора является 1024×768.
2. Запишите код красного цвета в двоичном, шестнадцатеричном и десятичном представлении.
Красный цвет соответствует максимальному значению интенсивности красного и минимальным значениям интенсивностей зеленого и синего базовых цветов. Таким образом, числовой код красного цвета следующий:

Коды/Цвета	Красный	Зеленый	Синий
двоичный	11111111	00000000	00000000
шестнадцатеричный	FF	00	00
десятичный	256	0	0

3. Сканируется цветное изображение размером 10×10 см. Разрешающая способность сканера 600 dpi и глубина цвета 32 бита. Какой информационный объем будет иметь полученный графический файл.
Переведем разрешающую способность сканера из точек на дюйм в точки на сантиметр:
600 dpi : 2,54 ≈ 236 точек/см
Следовательно, размер изображения в точках составит 2360×2360 точек.
Общее количество точек изображения равно:

2360×2360 = 5 569 600
Информационный объем файла равен:
32 бит × 5569600 = 178 227 200 бит ≈ 21 Мбайт
4.Определить соотношение между высотой и шириной экрана монитора для различных режимов. Различается ли это соотношение для различных режимов?
а) 640×480; б) 800×600; в) 1024×768; а) 1152×864; а) 1280×1024.
5 Определить максимально возможную разрешающую способность экрана для монитора с диагональю 17” и размером точки экрана 0,25 мм

6.Сканируется цветное изображение стандартного размера А4 (21×29,7 см). Разрешающая способность сканера 1200 dpi и глубина цвета 24 бита. Какой информационный объем будет иметь полученный графический файл.

7. Заполните таблицу цветов при 24-битной глубине цвета в шестнадцатеричном представлении.

Название цвета	Интенсивность		
	Красный	Зеленый	Синий
Черный			
Красный			
Зеленый			
Синий			
Белый			

Дополнительное задание:

1. Какова мощность алфавита, с помощью которого записано сообщение, содержащее 2048 символов, если его объем составляет 1/512 часть одного мегабайта.
2. Пользователь компьютера, хорошо владеющий навыками ввода информации с клавиатуры, может вводить в минуту 100 знаков. Мощность алфавита, используемого в компьютере равна 256. Какое количество информации в байтах может ввести пользователь в компьютер за 1 минуту.
3. Скорость чтения ученика 10 класса составляет приблизительно 250 символов в минуту. Приняв мощность используемого алфавита за 64, определите, какой объем информации в килобайтах получит ученик, если он будет непрерывно читать в течение 40 минут.

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.1Структуры и архитектура телекоммуникационных сетей

Практическая работа №8
«Определение IP-адресов.».

Задачи обучающегося:

1. Назначить адреса интерфейсам.
2. Изучить способы расчета общего числа подсетей

Опорные понятия:адресация хостов в сети.
Планируемый результат:
Студент должен
Знать понятия «Сеть Internet» и «адрес интерфейса», их дифференциацию.

Уметь правильно делить адресное пространство сети
Необходимое оборудование: учебная литература

Алгоритм деятельности обучающегося:

Задача 1. Сеть Internet 199.40.123.0 разбита на одинаковые подсети максимальной емкости маской 255.255.255.224. Назначить адреса интерфейсам подсетей и, по крайней мере, одной рабочей станции каждой подсети.

Задача 2. Разбить адресное пространство сети 199.40.123.0 на 4 одинаковые подсети с максимальным числом узлов в каждой и назначить IP – адрес этим подсетям. Как изменится результат, если сеть должна быть разбита на N=10 подсетей?

Задача 3. Сеть Internet 199.40.123.0 разбита на одинаковые подсети маской 255.255.255.240. Какое максимальное число узлов и рабочих станций может иметь каждая подсеть и почему?

Контрольные вопросы

1. Как рассчитать общее число подсетей?
2. Как осуществляется разбиение адресного пространства сети на подсети?
3. Каким условиям должно удовлетворять число?

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.2Коммутация пакетов и каналов

Алгоритм деятельности обучающегося:

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.2 Коммутация пакетов и каналов

Практическая работа №9
«Настройка сервера имен».

Задачи обучающегося:

1. Изучение понятий DNS-сервер, работа запросов
2. Создание пользовательских запросов

Опорные понятия: DNS сервер
Планируемый результат:
Студент должен
Знать понятия «DNS» и «Сервер имен», возможности и сферы применения
Выполнять работы по установке, настройке и обслуживании DNS-сервера,
Необходимое оборудование: учебная литература, ПК, VirtualBox, Ubuntu, VestaCP

Алгоритм деятельности обучающегося:

Система доменных имен (DNS) была исходно определена в документах RFC (*Request for Comments*) 1034 и 1035. Эти документы определяют следующие элементы, общие для всех реализаций программного обеспечения *DNS.*

- Пространство доменных имен *DNS*, которое задает структурированную иерархию доменов, используемую для организации имен.
- Записи ресурсов, сопоставляющие доменные имена *DNS* определенным типам информации о ресурсах, которые используются при регистрации и разрешении имен в пространстве имен.

- *DNS*-серверы, которые сохраняют записи ресурсов и отвечают на запросы клиентов.
- *DNS*-клиенты, которые также называют системами разрешения имен, запрашивающие серверы для поиска и разрешения имен по типам записей ресурсов, указанным в запросе.

Пространство доменных имен *DNS*, как показано на следующем рисунке, базируется на концепции дерева именованных доменов. Каждый уровень дерева может представлять ветвь или лист дерева. Ветвь представляет уровень, на котором используется несколько имен, определяющих семейство именованных ресурсов. Лист представляет единственное имя, которое используется на этом уровне для указания конкретного ресурса.

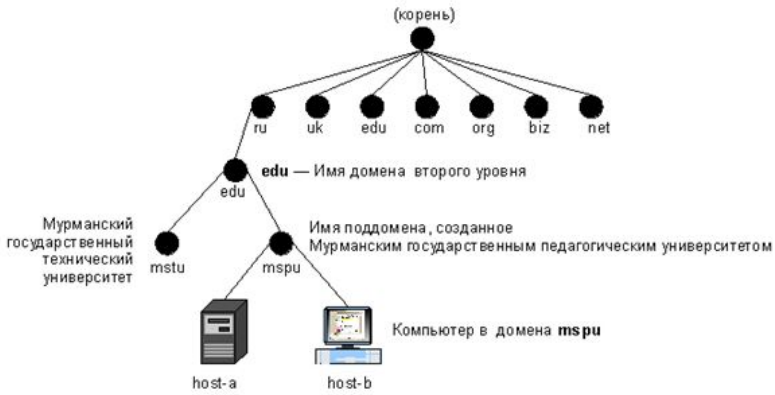


Рис.1 Пространство доменных имен

DNS представляет способ интерпретации полного пути к доменному имени ***DNS*** аналогично способу интерпретации полного пути к файлу или каталогу в окне командной строки. Например, путь в дереве каталогов помогает указать на точное расположение файла, сохраненного на компьютере. Для компьютеров с операционной системой **Windows** обратная косая черта (\) указывает каждый новый каталог, ведущий к точному расположению файла. Эквивалентным символом в ***DNS*** является точка (**.**), указывающая каждый новый уровень домена в имени. Для ***DNS*** примером имени с несколькими уровнями может служить следующее полное доменное имя узла: **host-a.mspu.edu.ru.** В отличие от имен файлов, при чтении полного доменного имени узла ***DNS*** слева направо осуществляется переход от наиболее конкретной информации (имя ***DNS***компьютера **«host-a»**) к наиболее общей (завершающая точка (**.**), которая указывает корень в дереве имен ***DNS***). Этот пример демонстрирует четыре уровня доменов ***DNS***, которые ведут от конкретного расположения**«host-a»**.

1. Домен **«mspu»**, в котором зарегистрировано для использования имя компьютера **«host-a»**.
2. Домен **«edu»**, который соответствует родительскому домену, являющемуся корнем поддомена **«mspu»**.
3. Домен **«ru»**, который соответствует домену верхнего уровня, предназначенному для использования организациями из России, который является корнем для домена **«edu»**.
4. Завершающая точка (**.**), представляющая стандартный символ разделителя, которая используется, чтобы сделать полным доменное имя ***DNS*** в дереве пространства имен ***DNS***.

Работа запросов DNS

Когда ***DNS***-клиенту требуется найти имя, используемое в программе, он запрашивает ***DNS***-серверы для сопоставления имени. Каждое сообщение с запросом, отправляемое клиентом, содержит информацию трех типов, определяющую вопрос, на который отвечает сервер:

Для ***DNS***-серверов **Windows** этот класс всегда должен быть указан как класс Интернета (**IN**).

Например, указанное имя может представлять полное доменное имя узла для компьютера, такое как **«host-a.mspu.edu.ru.»**, и тип запроса на поиск записей ресурсов адреса (A) для этого имени. Запрос ***DNS***можно представить как вопрос клиента, состоящий из двух частей, например *«Имеются ли записи ресурсов A для компьютера с именем 'hostname.mspu.edu.ru.'?»* Когда клиент получает ответ от сервера, он читает и интерпретирует содержащуюся в ответе запись ресурса A, узнавая IP-адрес компьютера, запрошенного по имени.

Запросы ***DNS*** используют несколько способов сопоставления имен. Клиент может иногда ответить на запрос с помощью локальной кэшированной информации, полученной в предыдущем запросе. ***DNS***-сервер может использовать собственный кэш информации о записях ресурсов для ответа на запрос. ***DNS*** -сервер может также запросить или обратиться к другим ***DNS***-серверам в интересах запрашивающего клиента для полного сопоставления имени, а затем отправить ответ клиенту. Этот процесс называют *рекурсией.*

В дополнение к этому, клиент может самостоятельно пытаться установить контакт с дополнительными ***DNS***-серверами для сопоставления имени. При этом клиент использует отдельные дополнительные запросы, базирующиеся на ссылочных ответах от серверов. Этот процесс называют *итерацией.* В общем случае процесс запроса ***DNS*** выполняется в две стадии.

1. Запрос к имени начинается на клиентском компьютере и передается в систему сопоставления имен службы ***DNS***-клиент.
2. Когда не удается ответить на запрос на локальном уровне, можно для сопоставления имени запрашивать ***DNS***-серверы по мере необходимости.

Обе стадии процесса подробнее рассматриваются в следующих разделах.

Локальная система разрешения имен

На начальных этапах процесса в программе на локальном компьютере используется доменное имя ***DNS***. Затем запрос передается в службу «***DNS***- клиент» для сопоставления с помощью локальной кэшированной информации. Если удается разрешить запрошенное имя, поступает ответ на запрос и процесс завершается. Кэш локального сопоставления имен может включать информацию об именах из двух возможных источников.

1. Если имеется локальный файл **Hosts**, все сопоставления имен и адресов из этого файла предварительно загружаются в кэш при запуске службы «***DNS***-клиент».
2. Записи ресурсов, полученные в ответах на запросы из предыдущих запросов ***DNS***, добавляются в кэш и сохраняются в нем в течение определенного периода времени.

Если клиент не находит сопоставления в кэше, процесс продолжается с помощью запроса на разрешение имени от клиента к ***DNS***-серверу.

Запрос к DNS-серверу

Клиент запрашивает основной ***DNS***-сервер. Из глобального списка выбирается сервер, используемый на начальной стадии запроса от клиента к серверу. Когда ***DNS***-сервер принимает запрос, он сначала проверяет, можно ли дать удостоверяющий ответ на базе записей ресурсов, содержащихся в локальной зоне в конфигурации сервера. Если запрошенное имя соответствует информации в записи ресурса в локальной зоне, сервер дает удостоверяющий ответ, используя эту информацию для разрешения имени. Если в зоне нет информации для запрошенного имени, сервер проверяет, можно ли разрешить имя, используя информацию предыдущих запросов в локальном кэше. Если здесь обнаруживается совпадение, сервер отвечает с использованием этой информации. И в этом случае, если основной сервер может дать запрашивающему клиенту утвердительный ответ на сопоставление из собственного кэша, запрос завершается. Если на основном сервере не удается найти запрошенное имя — ни в кэше, ни в зонах — процесс выполнения запроса может продолжаться с использованием рекурсии для полного разрешения имени. При этом другие ***DNS***-серверы помогают разрешить имя. Служба «***DNS***-клиент» по умолчанию указывает серверу использовать процесс рекурсии для полного разрешения имен в интересах

клиентов перед возвращением ответа. В большинстве случаев ***DNS***-серверы по умолчанию настраиваются на поддержку процесса рекурсии, как показано на следующем рисунке.

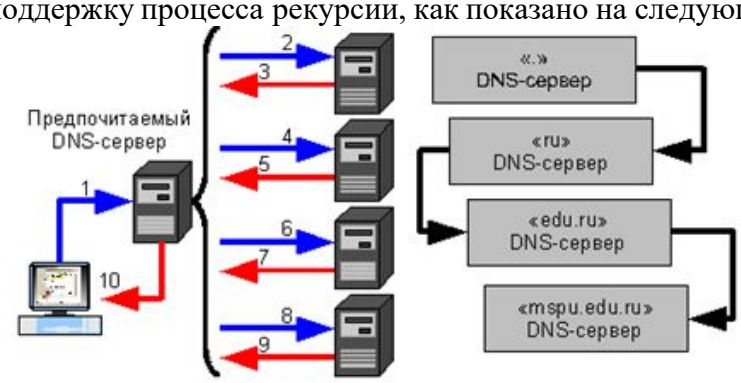


Рис.2 Процесс рекурсии при разрешении имен

Для правильного выполнения рекурсии ***DNS***-сервером ему необходимы сведения о контактах с другими ***DNS***-серверами в пространстве доменных имен ***DNS***. Такая информация обеспечивается в виде корневых ссылок, списка предварительных записей ресурсов, которые могут использоваться службой ***DNS*** для обнаружения других ***DNS***-серверов, которые являются удостоверяющими для корня дерева пространства доменных имен ***DNS*** . Корневые серверы являются удостоверяющими для корня доменов и доменов верхнего уровня в дереве пространства доменных имен ***DNS***.

Ранее отмечалось, что процесс заканчивается возвращением клиенту утвердительного ответа. Однако запросы могут возвращать и другие ответы. Приведем наиболее общие типы таких ответов:

1. удостоверяющий ответ;
2. утвердительный ответ;
3. ссылочный ответ;
4. отрицательный ответ.

Задание:

1.Откройте виртуальную машину VirtualBoxс установленной операционной системой Ubuntuserver 16/04

2.Настройте DNS-сервер в VestaCP

3.Напишите отчет о проделанной работе

Раздел 2. Сетевая модель, коммутация, протоколы

Тема2.2Коммутация пакетов и каналов

Практическая работа №10

«Решение проблем с TCP/IP»

Задачи обучающегося:

1. Актуализировать теоретические знания по стеку протоколов TCP/IP
2. Проводить диагностику неисправности сети, с последующим устранением

Опорные понятия: TCP/IP

Планируемый результат:

Студент должен

Знать теоретические сведения о стеке протоколов TCP/IP

Уметь диагностировать типовые неисправности сети

Необходимое оборудование: учебная литература, ПК

Алгоритм деятельности обучающегося:

1. Открыть окно командной строки, ввести команду ping с IP адресом машины, при

взаимодействии с которой возникают проблемы. Определить, использует ли проблемная машина конфигурацию статичного или динамичного IP адреса. Для этого откройте панель управления и выберите опцию Сетевые подключения. Теперь правой клавишей нажмите на подключении, которое собираетесь диагностировать, затем выберите опцию Свойства в появившемся меню быстрого доступа.

2. Перейдите по спискам элементов, используемых подключением, пока не дойдете до TCP/IP протокола (выбран на рисунке 3). Выберите этот протокол, нажмите на кнопке Свойства, чтобы открыть страницу свойств для Internet Protocol (TCP/IP).
3. Запишите IP конфигурацию машины. Особенно важно сделать заметки следующих элементов:

– Использует ли машина статичную или динамичную конфигурацию?
– Если используется статичная конфигурация, запишите значение IP адреса, маски подсети и основного шлюза?
– Получает ли машина адрес DNS сервера автоматически?

Если адрес DNS сервера вводится вручную, то какой адрес используется?

Если на компьютере установлено несколько сетевых адаптеров, то в панели управления будут перечислены несколько сетевых подключений.

Проверьте тип адаптера.

Определите, принимает ли Windows такую конфигурацию. Для этого откройте окно командной строки и введите следующую команду: `IPCONFIG /ALL.`

Определите правильный сетевой адаптер. В этом случае определение нужного адаптера довольно простое, поскольку в списке есть всего лишь один адаптер.

Отправьте ping запрос на адрес локального узла. Существует два различных способа того, как это сделать. Одним способом является ввод команды: *PING LOCALHOST.*

Введите команду Nslookup, за которой должно идти полное доменное имя удаленного узла. Команда Nslookup должна суметь разрешить полное доменное имя в IP адрес.

Необходимо просканировать клиентскую машину на предмет вредоносного ПО. Если на машине не обнаружено вредоносного ПО, сбросьте DNS кэш путем ввода следующей команды: *IPCONFIG /FLUSHDNS.*

Контрольные вопросы

1. Поясните, что может означать, если время TTL закончилось до получения ответа.
2. Как подтвердить наличие сетевого соединения?
3. Что показывает команда IPCONFIG /ALL?
4. Что означает наличие IP адрес со значением 0.0.0.0.?
5. С помощью какой команды можно проверить то, что конфигурация IP адреса работает корректно, и что отсутствуют проблемы с стеком локального протокола TCP/IP?
6. Как производится опрос основного шлюза?
7. Как производится опрос DNS сервера?

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.2Коммутация пакетов и каналов

Практическая работа №11
«Настройка удаленного доступа к компьютеру с помощью модема»
Задачи обучающегося:

1. Провести актуализациюпротоколов обмена данных

2. Составить блок-схему алгоритмов

Опорные понятия: удаленный доступ
Планируемый результат:
Студент должен
Знать понятия протоколы удаленного доступа
Уметь описывать сигналы RS-232
Необходимое оборудование: учебная литература

Алгоритм деятельности обучающегося:

Задания к работе

1.Описать цепи и назначение сигналов интерфейса RS-232.

2.Составить краткую сравнительную характеристику протоколов обмена данными X-modem и Z-modem.

3.Составить блок-схемы следующих алгоритмов:

-алгоритм организации соединения и ведения диалога с удаленным абонентом;
-алгоритм организации соединения и передачи файлов;
-алгоритм организации соединения и приема файлов.

Контрольные вопросы:

1.Протоколы X-modem и Z-modem.
2.Цепи и назначение сигналов интерфейса RS-232.
3.Методы управления потоком в модеме и режимы обмена данными между модемом и компьютером.

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.2Коммутация пакетов и каналов

Практическая работа №12
«Установка и настройка сетевой операционной системы: IP –адресация»
Задачи обучающегося:

1. Провести дифференциацию понятий «сетевые службы» и «протоколы».
2. Познакомиться с методами диагностики сети при помощи встроенных утилит

Опорные понятия: IP-адресация
Планируемый результат:
Студент должен
Знать сетевые утилиты встроенные в операционную систему, и уметь их применять
Необходимое оборудование: учебная литература: Психология/Под ред. И.В.Дубровиной

Алгоритм деятельности обучающегося:

Теоретические сведения
В состав TCP/IPвходят диагностические утилиты, предназначенные для проверки конфигурации тестирования сетевого соединения.

arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (AddressResolutionProtocol- определяет локальный адрес по IP-адресу)
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес,

	маску подсети, адрес шлюза по умолчанию, адреса WINS (WindowsInternetNamingService) и DNS (DomainNameSystem)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (InternetControlMessageProtocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

Проверка правильности конфигурации TCP/IP.

При устранении неисправностей и проблем в сети TCP/IPследует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig. Эта команда полезна на компьютерах, работающих с DHCP (DynamicHostConfigurationProtocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IPи какие величины были установлены с помощью DHCP.

Тестирование связи с использованием утилиты ping.

Утилита ping (PacketInternetGrouper) используется для проверки конфигурирования TCP/IPи диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование pingлучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда pingпроверяет соединение с удаленным хостом путем посылки к этому хосту эхо-пакетов ICMPи прослушивания эхо-ответов. Pingожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений pingстанет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Pingпозволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле timeуказывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение "Requesttimeout"(Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа -w.

Pingможно использовать для тестирования как имени хоста (DNSили NetBIOS), так и его IP-адреса. Если pingс IP-адресом выполнилась успешно, а с именем - неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Изучение маршрута между сетевыми соединениями с помощью утилиты tracert.

Tracert- это утилита трассировки маршрута. Она использует поле TTL (time- to-live, время жизни) пакета IPи сообщения об ошибках ICMPдля определения маршрута от одного хоста до другого.

Утилита tracertможет быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Intemet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа "Destinationnetunreachable", "Destinationhostunreachable", "Requesttimeout", "TimeExeeded".

Утилита tracertработает следующим образом: посылается по 3 пробных эхо- пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTLна единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP "TimeExeeded"(Время истекло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTLувеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL(по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTLи не будут видны утилите tracert.

Утилита ARP.

Основная задача протокола ARP- трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP- таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARPотправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Утилита netstat.

Утилита netstatпозволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Выполнение работы

1. Получение справочной информации по командам

   Выведите на экран справочную информацию по утилитам arp, ipconfig, nbstat, netstat, nslookup,route, ping, tracert, hostname. Для этого в командной строке введите имя утилиты без параметров или с /?.

   Изучите и запишите ключи, используемые при запуске утилит.

2. Получение имени хоста

   Выведите на экран имя локального хоста с помощью команды hostname.

3. Изучение утилиты ipconfig

Проверьте конфигурацию TCP/IPс помощью утилиты ipconfig.
Заполните таблицу:

Физический адрес сетевого адаптера	
IP-адрес	
Маска подсети	
Доменное имя	
Используется ли DHCP(адрес DHCP-сервера	
Описание адаптера	
Адрес DNS- сервера	
Адрес WINS- сервера	
Основной шлюз	

4. Тестирование связи с помощью утилиты ping

4.1. Проверьте правильность установки и конфигурирования TCP/IPна локальном компьютере.
ping 127.0.0.1

4.2. Проверьте правильность работы сетевого адаптера и его драйвера.
ping <адрес данного ПК>

4.3. Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.

4.4. С помощью команды pingпроверьте перечисленные ниже адреса и для каждого из них отметьте время отклика.

a) 192.168.10.5
b) 172.16.1.4
c) server
d) 172.16.1.2
e) С соседним ПК

4.5. Задайте различное количество посылаемых пакетов. Попробуйте увеличить длину посылаемых пакетов.

5. Определение пути IP-пакета
С помощью команды tracertпроверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Отметьте их: a) 72.16.1.2 b) ya.ru
Справка! Отмена работы команды <ctrl>+ <C>

6. Просмотр ARP-кэша
С помощью утилиты arpпросмотрите ARP-таблицу локального компьютера.

7. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.
С помощью утилиты netstatвыведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

8. Netview. Выводит список доменов, компьютеров или общих ресурсов на данном компьютере. Вызванная без параметров, команда netviewвыводит список компьютеров в текущем домене.
Исследовать ресурсы домена Sibcolc помощью команды **netview**.
Получить списки общих ресурсов компьютеров вашей аудитории.

9. Ответьте на контрольные вопросы

Какие утилиты можно использовать для проверки правильности

конфигурирования TCP/IP?

Каким образом каманда pingпроверяет соединение с удаленным хостом?

Что такое хост?

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.2Коммутация пакетов и каналов

Практическая работа №13
«Работа с серверами http и ftp»

Задачи обучающегося:

1. Научиться устанавливать и просматривать Active Directory, научится подключать компьютеры к домену.
2. Изучить http и ftp серверы, особенности подключения и настройки соединения

Опорные понятия:FTP,http
Планируемый результат:
Студент должен
Уметь настраивать соединение по FTP протоколу
Необходимое оборудование:компьютер, виртуальная машина; Filezilla

Алгоритм деятельности обучающегося:

Сервер - в локальных вычислительных сетях - специализированная ЭВМ, управляющая использованием разделяемых между терминалами сети дорогостоящих ресурсов системы.

Сервер (англ. server от англ. to serve — служить) — в информационных технологиях — программный компонент вычислительной системы, выполняющий сервисные функции по запросу клиента, предоставляя ему доступ к определённым ресурсам.

Сервер сети (Server) - это компьютер, подключенный к сети и предоставляющий пользователям сети определенные услуги, например, хранение данных общего пользования, печать заданий, обработка запроса к СУБД, удаленная обработка заданий и т.д. Сервер работает по заданиям клиентов. После выполнения задания сервер посылает полученные результаты клиенту, инициировавшему это задание.

Обычно связь между клиентом и сервером поддерживается посредством передачи сообщений, и при этом используется определенный протокол для кодирования запросов клиента и ответов сервера. Виды серверов: FTP; Файловый; Web; Телефонный; Терминальный; Факс; Суперсервер и т.д.

Файл-серверы представляют собой серверы для обеспечения доступа к файлам на диске сервера. Прежде всего это серверы передачи файлов по заказу, по протоколам FTP и HTTP. Протокол HTTP ориентирован на передачу текстовых файлов, но серверы могут отдавать в качестве запрошенных файлов и произвольные данные, например динамически созданные веб-страницы, картинки, музыку и т. п. Другие серверы позволяют монтировать дисковые разделы сервера в дисковое пространство клиента и полноценно работать с файлами на них. Это позволяют серверы протоколов NFS и SMB. Серверы NFS и SMB работают через интерфейс RPC.

Недостатки файл-серверной системы:

Очень большая нагрузка на сеть, повышенные требования к пропускной способности. На практике это делает практически невозможной одновременную работу большого числа пользователей с большими объемами данных.

Обработка данных осуществляется на компьютере пользователей. Это влечет

повышенные требования к аппаратному обеспечению каждого пользователя. Чем больше пользователей, тем больше денег придется потратить на оснащение их компьютеров.

Блокировка данных при редактировании одним пользователем делает невозможной работу с этими данными других пользователей.

Безопасность. Для обеспечения возможности работы с такой системой Вам будет необходимо дать каждому пользователю полный доступ к целому файлу, в котором его может интересовать только одно поле

Файловый сервер выполняет следующие функции:

хранение данных,

архивирование данных,

согласование изменений данных, выполняемых разными пользователями,

передача данных.

FTP-сервер - это понятие, за которым скрывается обычный компьютер. Но так как он содержит общедоступные файлы и настроен на поддержку протокола FTP, то его называют сервером - поставщиком информации. FTP-клиент - это сервисная программа, с помощью которой можно произвести соединение с FTP сервером. Обычно эта программа имеет командную строку, но некоторые имеют оконный интерфейс и не требуют запоминания команд. WEB-сервер необходим для обслуживания WEB-страниц вашего сайта

Доступ к WEB-серверу имеет пять уровней:

Общедоступный с возможностью только чтения всех URL за исключением тех, что помещены в каталогах /private.

Доступ сотрудников организации, которой принадлежит сервер. Здесь также допустимо только чтение, но доступны и секции каталога /private.

Разработчики WEB-сервера. Имеют возможность модифицировать содержимое сервера, инсталлировать CGI-скрипты, прерывать работу сервера.

Администраторы узла (сервера). Имеют те же привилегии, что и разработчики, но могут также реконфигурировать сервер и определять категорию доступа.

Системные администраторы. Имеют идентичные привилегии с администраторами сервера.

Оснастка Internet Information Service (IIS) обеспечивает средства управления сервером для контроля над доступом и содержимым веб-узлов и узлов FTP. Например, разработчикам это средство позволит выполнить доскональную проверку работы узла перед окончательной загрузкой на сервер интрасети организации или Интернета. Оснастка IIS имеет следующие особенности:

дополнительные параметры настройки сервера, в частности, для управления узлом FTP, независимого выполнения приложений, настройки типов MIME и назначения дополнительных средств обработки сценариев.

мастер создания виртуальных каталогов.

возможность управления установками Internet Information Services в сети.

На сегодняшний день существует огромное множество программного обеспечения для работы с протоколом FTP под все операционные системы. Все это множество программного обеспечения можно разделить на две части: серверное ПО и клиентское ПО. Серверное ПО служит для создания и управления ftp-сервером. Клиентское ПО используется для просмотра ресурсов на ftp-сервере. Этот класс программ призван обеспечить комфортную работу с удаленными ресурсами. Сюда относятся такие программы как:

ftp.exe – стандартное приложение Windows;

FileZilla – мощный ftp-клиент с открытым исходным кодом (т.е. при желание вы можете что-нибудь новое добавить в эту программу самостоятельно);

RigthFTP, CuteFTP – графические ftp-клиенты;

Total commander (или любой другой с интерфейсом Norton Commander)– имеет встроенный ftp клиент;

Explorer.exe – стандартное приложение Windows;

Любой браузер.

Выполнение работы

Задание 1. Подготовьте файловый сервер.

Подключите к виртуальной машине VM-2 образ установочного диска.

Запустите виртуальную машину VM-2.

Добавьте новую роль серверу – Файл-сервер:*откройте диалоговое окно Управление данным сервером (Пуск/дминистрирование/Управление Данным Сервером);*

активизируйте добавление ролей кнопкой Добавить или удалить роль;

выберите Файловый сервер и щелкните Далее;

установите параметры файлового сервера:

Предоставить доступ UNIX-системам к файлам;

Предоставить доступ Apple--системам к файлам;

подтвердите введенные параметры кнопкой Далее;

запустите установку роли сервера кнопкой Далее.

Перезагрузите виртуальный компьютер кнопкой Перезагрузить.

Откройте диалоговое окно Настройки файлового сервера (Пуск/администрирование/Управление Данным Сервером/Управление этим файловым сервером).

Установите стандартные квоты использования места на диске:

установите флажок Установить дисковые квоты по умолчанию для новых пользователей данного сервера;

укажите размер квот - 50Мб;

установите предупреждение о квоте - 40Мб;

установите флажок Не выделять место на диске при превышении дискового пространства;

завершите ввод стандартных квот кнопкой Далее.

Откажитесь от включения службы индексирования.

Укажите папку на сервере, для хранения файлов, например C:\Documents and settings\Администратор\Рабочий стол\PUB.

Далее мастер установки завершит свою работу. Попробуйте теперь зайти на созданную вами сетевую папку с другого компьютера сети. Обратите внимание на способ подключения. Попробуйте заполнить папку для превышения квоты.

Задание 2. Настройте Web-сервер.

Установите Internet Information Service (IIS) (Пуск/администрирование/Управление Данным Сервером/Сервер приложений IIS):

Подготовьте тестовую страницу:

создайте временную страницу, вызываемую по умолчанию: наберите в Блокноте и сохраните в файле с именем Default.html в каталоге \Inetpub\wwwroot.

Настройте Web-сервер:

откройте консоль управления сервером IIS (Пуск/администрирование/Управление Данным Сервером/Управление этим сервером приложений);

перейдите к web-узлу, заданному по умолчанию (Диспетчер служб IIS/Веб-узлы/Веб-узел по умолчанию);

откройте диалоговое окно Свойства узла по умолчанию (контекстное меню/Свойства);

добавьте страницу по умолчанию:
перейдите на вкладку Документы;
установите флажок Задать страницу содержания по умолчанию;
откройте окно добавления кнопкой Добавить;введите в поле Default.html;
подтвердите добавление кнопкой ОК.
закройте окно свойств кнопкой ОК.
Проверьте настройку Web-сервера:
на вашем компьютере откройте Internet Explorer (Пуск/Программы/Internet Explorer);
наберите в адресной строке http://127.0.01/;
сделайте скриншот происходящего на экране и сохраните его в своей папке.

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.2Коммутация пакетов и каналов

Практическая работа №14
«Кэшированние данных DNS на DNS-сервере»

Задачи обучающегося:

1. Провести установку службы DNS
2. Настроить службу на сервере и рабочей станции

Опорные понятия:служба DNS
Планируемый результат:
Студент должен
Научиться устанавливать и настраивать службу DNSна WindowsServer
Выполнять обновление ПО
Необходимое оборудование:ПК, VirtualBox

Алгоритм деятельности обучающегося:

Установка службы DNS

1. Зарегистрируйтесь на сервере serverкак Администратор.
2. Выполните команду Пуск ->Панель управления -» Установка и удаление программ. Выберите действие Установка компонентов Windows.
3. В появившемся окне Мастер компонентов Windowsвыберите Сетевые службы и нажмите на кнопку Состав.
4. В появившемся окне Сетевые службы установите флажок DomainNameServer (DNS) и нажмите ОК
5. Нажатием на кнопку Далее запустите установку службы DNS. Она не требует перезагрузки системы.

Настройка DNS

1. Выполните команду Пуск -» Панель управления -» Администрирование и выберите DNS. Откроется окно консоли с именем сервера server.
2. В левой части окна разверните объект сервера, щелкните правой кнопкой мыши по пункту Зоны прямого просмотра и выберите из контекстного меню Новая зона. Запустится Мастер создания зоны. На первом шаге нажмите кнопку Далее.
3. В диалоговом окне Тип зоны установите флажок Основная зона и нажмите Далее.
4. В поле Имя зоны введите study.local. Нажмите Далее.
5. В диалоговом окне Файл зоны установите флажок Создать новый файл и

введите имя файла: study.local. dns. Нажмите Далее.

6. В окне Динамическое обновление установите флажок Разрешить любые динамические обновления и нажмите Далее.

7. Завершите установку нажатием кнопки Готово.

Настройка DNSна сервере “server”

1. В главном меню выберите Панель управления —» Сетевые подключения, а затем правой кнопкой мыши щелкните по пункту Подключение по локальной сети.

2. Из контекстного меню выберите Свойства.

3. В окне свойств подключения к локальной сети выберите пункт Протокол сети Интернет TCP/IPи нажмите на кнопку Свойства. Откроется окно свойств протокола TCP/IP.В поле Предпочитаемый сервер DNSвведите IP-адрес сервера server— 192.168.10.2.

4. Последовательным нажатием на кнопку ОК закройте все окна.

5. В меню Пуск нажмите правой кнопкой мыши на меню Мой компьютер и выберите пункт Свойства.

6. В диалоговом окне Свойства системы откройте вкладку Имя компьютера и нажмите кнопку Изменить.

7. В диалоговом окне смены имени компьютера нажмите кнопку Дополнительно.

8. В диалоговом окне DNS-суффикс и NetBIOS-имя компьютера введите в поле Предпочитаемый DNS-суффикс имя зоны study.local. Нажатием ОКзакройте окно.

9. Вы увидите в диалоговом окне Смена имени компьютера в поле Полное имя компьютера server.study, local—имя, состоящее из имени узла и суффикса DNS. Это имя должно быть уникальным в пределах сети. Диалоговое окно закройте нажатием ОК. После этого необходимо перезагрузить компьютер.

10. После перезагрузки компьютера снова откройте консоль DNSи в левой части окна выберите зону study.local. В правой части окна обратите внимание на созданный объект А (хост) сервера server

Настройка DNS на рабочей станции

1. Зарегистрируйтесь на компьютере pc1 как Администратор.

2. В главном меню выберите Панель управления -» Сетевые подключения, а затем правой кнопкой мыши щелкните по пункту Подключение по локальной сети.

3. Из контекстного меню выберите Свойства.

4. В окне Подключение по локальной сети — свойства выберите Протокол сети Интернет TCP/IP, нажмите на кнопку Свойства.

5. В поле Предпочитаемый DNS-сервер введите адрес сервера server— 192.168.10.2. Затем нажмите ОК. Диалоговое окно свойств подключения закройте нажатием кнопки Закрыть.

6. 6. В меню Пуск нажмите правой кнопкой мыши на меню Мой компьютер и выберите пункт Свойства.

7. В диалоговом окне Свойства системы откройте вкладку Имя компьютера и нажмите кнопку Изменить.

8. В диалоговом окне смены имени компьютера нажмите кнопку Дополнительно.

9. В диалоговом окне DNS-суффикс и NetBIOS-имя компьютера введите в поле Предпочитаемый DNS-суффикс имя зоны study.local. Нажатием ОКзакройте окно.

Раздел 2. Сетевая модель, коммутация, протоколы

Тема2.3Протоколы локальных сетей

Практическая работа №15

«Применение сетевых утилит для определения работоспособности сети»

Задачи обучающегося:

1. Провести анализ средств диагностики сети
2. Научиться пользоваться встроенными утилитами для обеспечения отказоустойчивости сети

Опорные понятия:сетевые утилиты

Планируемый результат:

Студент должен

Освоить приемы и техники работы с утилитами для настройки и диагностики неисправностей сетей

Необходимое оборудование:ПК, ОС Windows10

Алгоритм деятельности обучающегося:

Теоретические сведения

В состав TCP/IPвходят диагностические утилиты, предназначенные для проверки конфигурации тестирования сетевого соединения.

arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (AddressResolutionProtocol- определяет локальный адрес по IP-адресу)
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (WindowsInternetNamingService) и DNS (DomainNameSystem)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (InternetControlMessageProtocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

Проверка правильности конфигурации TCP/IP.

При устранении неисправностей и проблем в сети TCP/IPследует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig. Эта команда полезна на компьютерах, работающих с DHCP (DynamicHostConfigurationProtocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IPи какие величины были установлены с помощью DHCP.

Тестирование связи с использованием утилиты ping.

Утилита ping (PacketInternetGrouper) используется для проверки конфигурирования

TCP/IPи диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование pingлучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда pingпроверяет соединение с удаленным хостом путем посылки к этому хосту эхо-пакетов ICMPи прослушивания эхо-ответов. Pingожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений pingстанет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Pingпозволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле timeуказывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение "Requesttimeout"(Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа -w.

Pingможно использовать для тестирования как имени хоста (DNSили NetBIOS), так и его IP-адреса. Если pingс IP-адресом выполнилась успешно, а с именем - неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Изучение маршрута между сетевыми соединениями с помощью утилиты tracert.

Tracert- это утилита трассировки маршрута. Она использует поле TTL (time- to-live, время жизни) пакета IPи сообщения об ошибках ICMPдля определения маршрута от одного хоста до другого.

Утилита tracertможет быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Intemet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа "Destinationnetunreachable", "Destinationhostunreachable", "Requesttimeout", "TimeExeeded".

Утилита tracertработает следующим образом: посылается по 3 пробных эхо- пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTLна единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP "TimeExeeded"(Время истекло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTLувеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL(по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTLи не будут видны утилите tracert.

Утилита ARP.

Основная задача протокола ARP- трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP- таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARPотправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Утилита netstat.

Утилита netstatпозволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Выполнение работы

10. Получение справочной информации по командам

Выведите на экран справочную информацию по утилитам arp, ipconfig, nbstat, netstat, nslookup,route, ping, tracert, hostname. Для этого в командной строке введите имя утилиты без параметров или с /?.

Изучите и запишите ключи, используемые при запуске утилит.

11. Получение имени хоста

Выведите на экран имя локального хоста с помощью команды hostname.

12. Изучение утилиты ipconfig

Проверьте конфигурацию TCP/IPс помощью утилиты ipconfig.

Заполните таблицу:

Физический адрес сетевого адаптера	
IP-адрес	
Маска подсети	
Доменное имя	
Используется ли DHCP(адрес DHCP-сервера	
Описание адаптера	
Адрес DNS- сервера	
Адрес WINS- сервера	
Основной шлюз	

13. Тестирование связи с помощью утилиты ping

13.1. Проверьте правильность установки и конфигурирования TCP/IPна локальном компьютере.

ping 127.0.0.1

13.2. Проверьте правильность работы сетевого адаптера и его драйвера.

ping <адрес данного ПК>

13.3. Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.

13.4. С помощью команды pingпроверьте перечисленные ниже адреса и для каждого из них отметьте время отклика.

f) 192.168.10.5
g) 172.16.1.4
h) server
i) 172.16.1.2
j) С соседним ПК

13.5. Задайте различное количество посылаемых пакетов. Попробуйте увеличить длину посылаемых пакетов.

14. Определение пути IP-пакета
С помощью команды tracertпроверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Отметьте их: a) 72.16.1.2 b) ya.ru
Справка! Отмена работы команды <ctrl>+ <C>

15. Просмотр ARP-кэша
С помощью утилиты arpпросмотрите ARP-таблицу локального компьютера.

16. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.
С помощью утилиты netstatвыведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

17. Netview. Выводит список доменов, компьютеров или общих ресурсов на данном компьютере. Вызванная без параметров, команда netviewвыводит список компьютеров в текущем домене.
Исследовать ресурсы домена Sibcolc помощью команды **netview**.
Получить списки общих ресурсов компьютеров вашей аудитории.

18. Ответьте на контрольные вопросы
Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
Каким образом каманда pingпроверяет соединение с удаленным хостом?
Что такое хост?

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.3Протоколы локальных сетей

Практическая работа №16
«Настройка протокола TCP/IP в операционных системах»

Задачи обучающегося:

1. Провести настройку протокола TCP/IP на сервере
2. Провести настройку протокола TCP/IP на клиенте

Опорные понятия:настройка сети
Планируемый результат:
Студент должен
Уметь конфигурировать систему и производить базовую настройку сети
Необходимое оборудование:ПК, VirtualBox

Алгоритм деятельности обучающегося:

Настройка протокола TCP/IPна сервере

1. В меню ***Пуск*** выберите ***Панель управления ->Сетевые подключения*** - » ***Подключение по локальной сети***.
2. В появившемся диалоговом окне состояния на вкладке ***Общие*** нажмите кнопку ***Свойства.*** Отобразится диалоговое окно ***Подключение по локальной сети — свойства***.
3. В списке компонентов, используемых этим подключением, выберите пункт ***Протокол***

Интернета (TCP/IP)и нажмите кнопку ***Свойства***.

4. В диалоговом окне ***Свойства: протокол Интернета (TCP/IP)*** установите переключатель в положение ***Использовать следующий IP- адрес*** и в поле ***IP-адрес*** введите значение 192.168.10.2.

5. В поле ***Маска подсети*** введите значение 255.255.255.0.

6. В нижней части окна свойств установите переключатель в положение ***Использовать следующие адреса серверов DNS***и в поле ***Предпочитаемый DNS-сервер*** введите значение 192.168.10.2

7. Нажатием на кнопку ОК закройте диалоговое окно свойств протокола TCP/IP.

8. Включите флажок ***При подключении вывести значок в области уведомлений*** и нажмите кнопку ***Закрыть***.

9. В углу панели задач появится значок только что настроенного вами подключения.

10. Выполните Перезагрузку.

Проверка настройки

Пуск->выполнить->cmd->ipconfig /allip-адрес, маска подсети и DNSсервер, должны соответствовать тем адресам которые вы только что прописали.

Настройка протокола TCP/IPна компьютере-клиенте

1. В меню Пуск выберите Панель управления —» Сетевые подключения - » Подключение по локальной сети.

2. В появившемся диалоговом окне состояния на вкладке Общие нажмите кнопку Свойства. Отобразится диалоговое окно Подключение по локальной сети — свойства.

3. В списке компонентов, используемых этим подключением, выберите пункт Протокол Интернета (ТСРДР) и нажмите кнопку Свойства.

4. В диалоговом окне Свойства: протокол Интернета (TCP/IP) установите переключатель в положение Использовать следующий IP-адрес и в поле IP-адрес введите адрес— 192.168.10.17.

5. В поле Маска подсети введите значение 255.255.255.0.

6. В нижней части окна свойств установите переключатель в положение Использовать следующие адреса серверов DNSи в поле Предпочитаемый DNS-сервер введите значение 192.168.10.2

7. Нажатием на кнопку ОК закройте диалоговое окно свойств протокола TCP/IP.

8. Включите флажок При подключении вывести значок в области уведомлений и нажмите кнопку Закрыть.

9. В углу панели задач появится значок только что настроенного вами подключения.

10. Выполните Перезагрузку.

Проверка настройки

Пуск->выполнить->cmd->ipconfig /allip-адрес, маска подсети и DNSсервер, должны соответствовать тем адресам которые вы только что прописали.

Проверка связи между сервером и клиентской машиной

1. Зарегистрируйтесь на serverкак Администратор.

2. Пуск->Выполнить->cmd->ping 192.168.10.17 если пинг прошел успешно, значит сеть настроена правильно.

3. Зарегистрируйтесь на pc1 как администратор.

4. Пуск->Выполнить->cmd->ping 192.168.10.2 если пинг прошел успешно, значит сеть настроена правильно.

Раздел 2. Сетевая модель, коммутация, протоколы
Тема2.3Протоколы локальных сетей

Практическая работа №17

«Работа с диагностическими утилитами протокола TCP/IP»

Задачи обучающегося:

1. Изучить возможности работы с программами для диагностики
2. Применить полученые знания на практике

Опорные понятия:диагностические утилиты
Планируемый результат:
Студент должен
Освоить средства диагностики используя штатные средства операционных систем
Необходимое оборудование:ПК

Алгоритм деятельности обучающегося:

Задание 1. Получение справочной информации по командам.

Выведите на экран справочную информацию по всем рассмотренным утилитам (см. таблицу п.1). Для этого в командной строке введите имя утилиты без параметров и дополните **/?**.

Сохраните справочную информацию в отдельном файле.

Изучите ключи, используемые при запуске утилит.

Задание 2. Получение имени хоста.

Выведите на экран имя локального хоста с помощью команды hostname. Сохраните результат в отдельном файле.

Задание 3. Изучение утилиты ipconfig.

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

Задание 4. Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.
3. Проверьте возможность установления соединения с удаленным хостом.
4. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте aspu.ru) и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

Задание 5. Определение пути IP-пакета.

С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Изучите ключи команды.

a) aspu.ru

b) mathmod.aspu.ru

c) yarus.aspu.ru

Задание 6: Просмотр ARP-кэша.

С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

Внести в кэш локального компьютера любую статическую запись.

Задание 7: Просмотр локальной таблицы маршрутизации.

С помощью утилиты route просмотреть локальную таблицу маршрутизации.

Задание 8. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы:

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети, авторитетный/неавторитетный (компетентный) DNS-сервер, порт TCP, петля обратной связи, время отклика.
2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
3. Каким образом команда ping проверяет соединение с удаленным хостом?
4. Каково назначение протокола ARP?
5. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
6. Какие могут быть причины неудачного завершения ping и tracert? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).
7. Всегда ли можно узнать символьное имя узла по его ip-адресу?
8. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

Раздел 3. Сетевое оборудование, безопасность

Тема3.1Оборудованиелокальных сетей

Практическая работа №18

«Получить навыки установки и просмотра ActiveDirectory; научится подключать компьютеры к домену»

Задачи обучающегося:

1. Научиться добавлять и настраивать роль Active Directory на сервере.
2. Познакомиться с методами и методиками исследования личности.

Опорные понятия:контроллер домена

Планируемый результат:

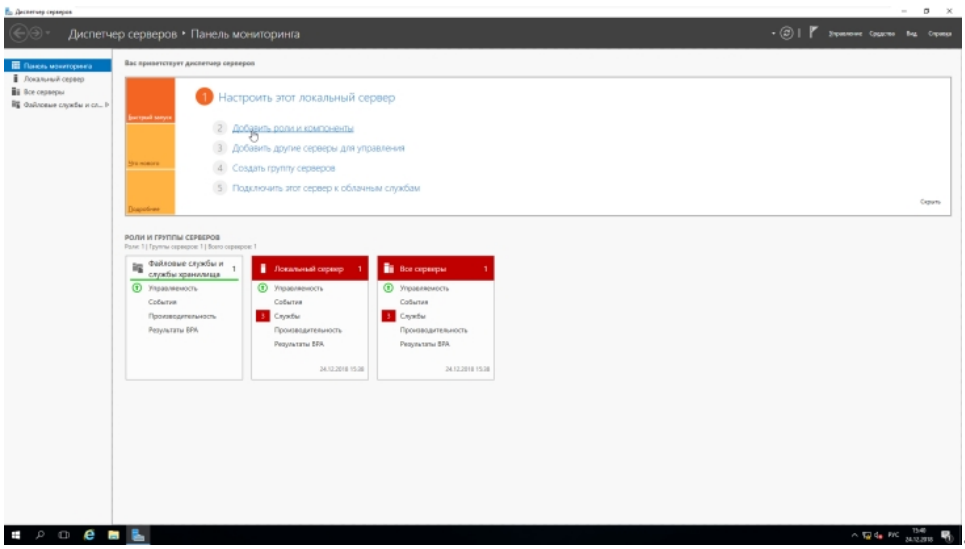
Студент должен

Знать и уметь настраивать контроллер домена на сервере и подключать к нему рабочие станции клиентов

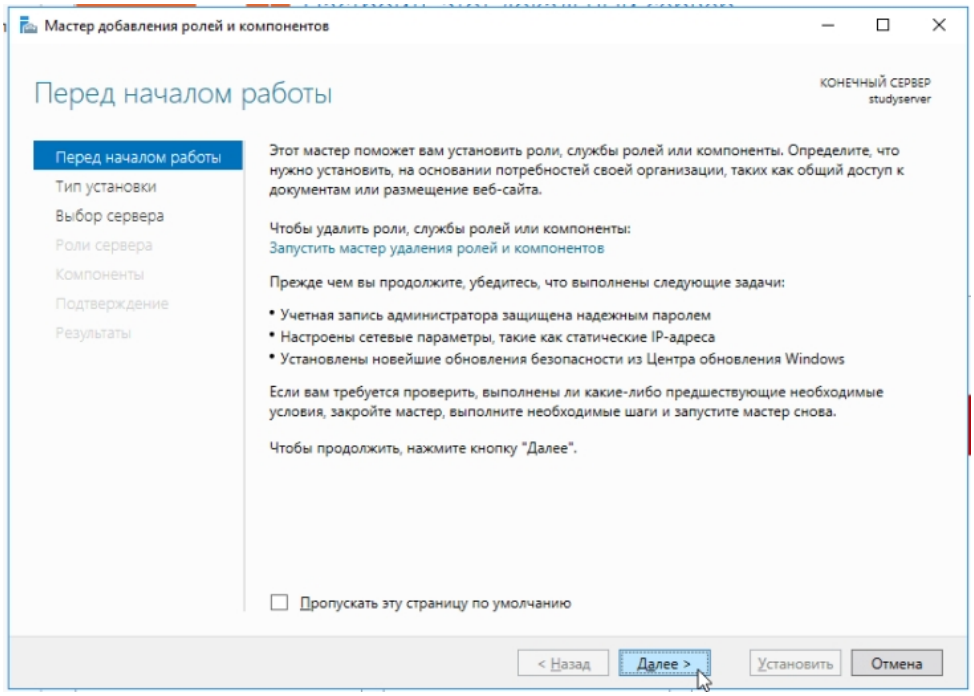
Необходимое оборудование:ПК, VirtualBox

Алгоритм деятельности обучающегося:

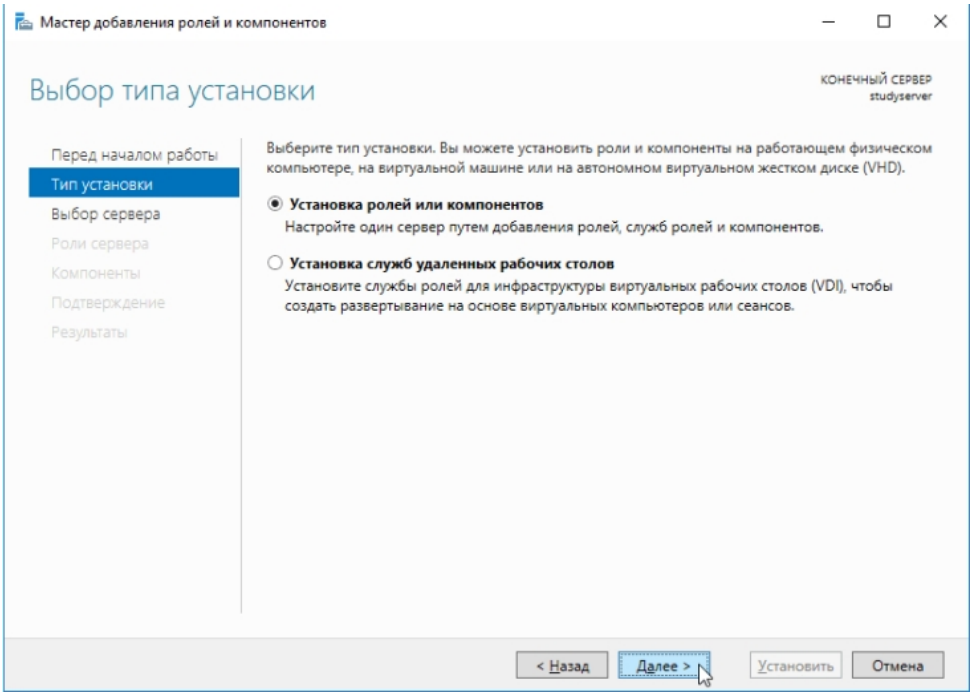
В диспетчере серверов выбрать пункт «Добавить роли и компоненты». В дальнейшем этот пункт будет часто использоваться



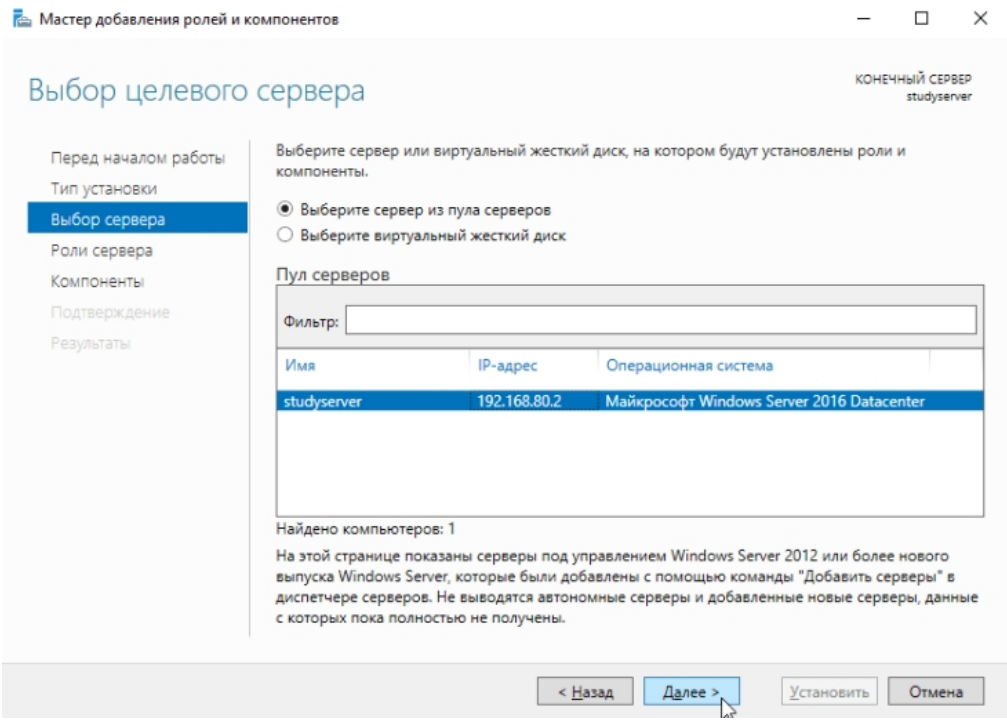
В открывшемся окне мастера нажать далее.



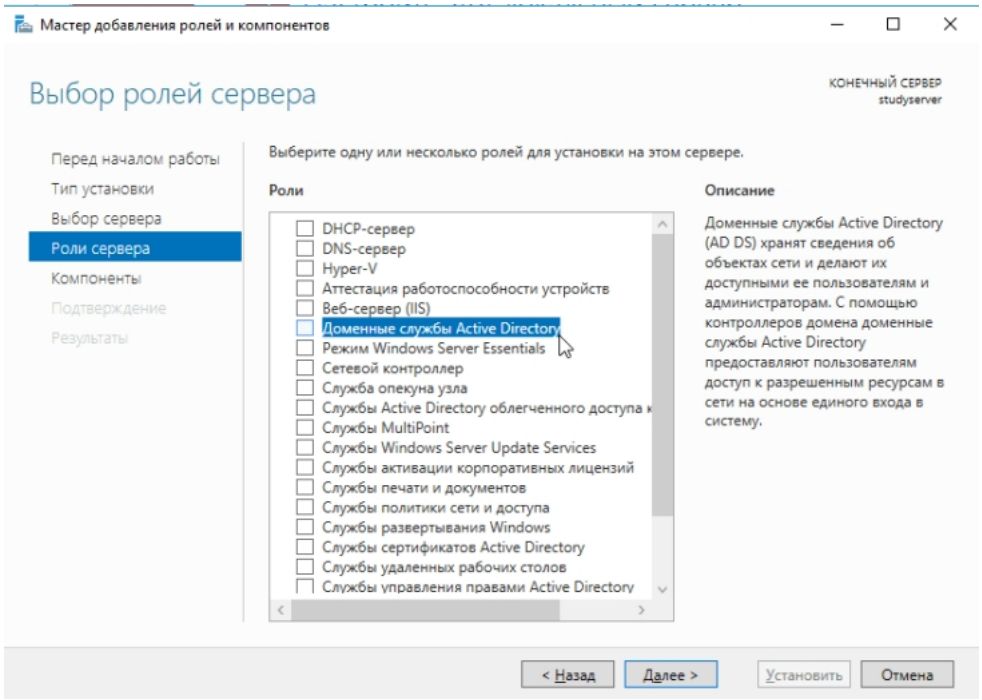
Выбрать пункт: «Установка ролей и компонентов».



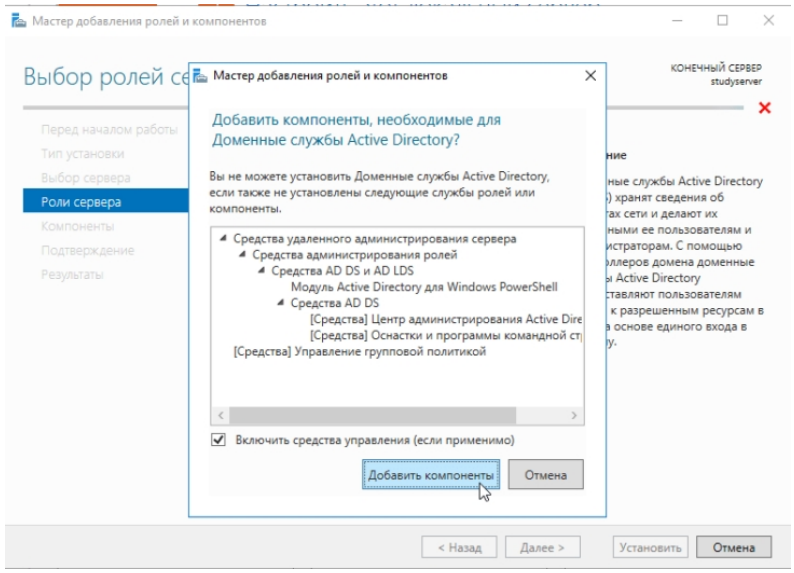
Выбрать сервер из списка.



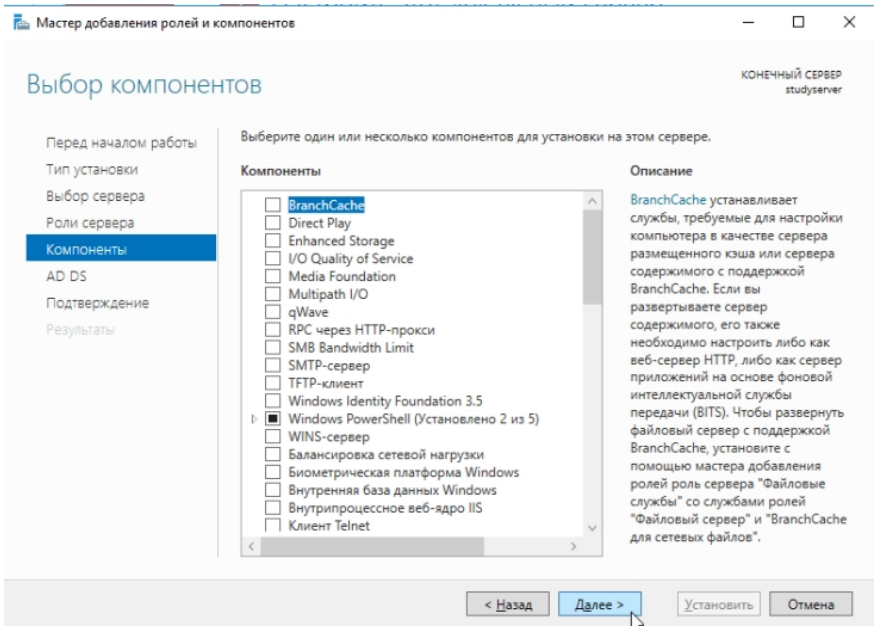
Выбрать необходимую роль. В данном случае это «Доменные службы Active Directory»



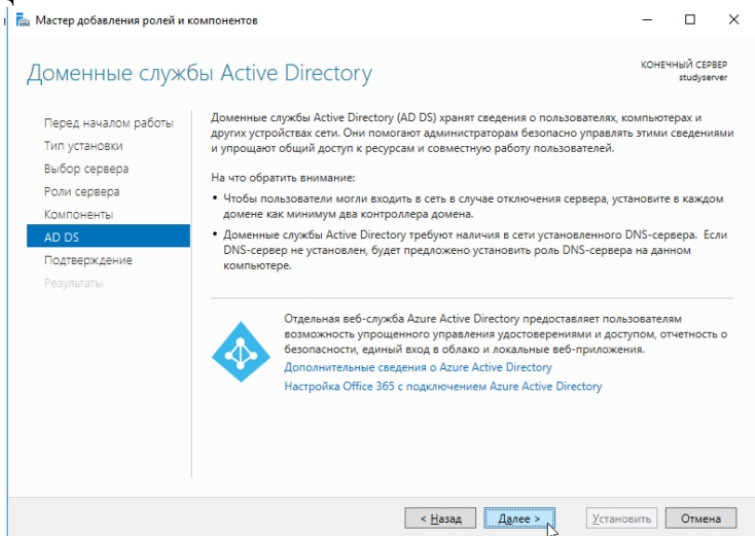
В появившемся окне предлагают установить необходимые для продолжения компоненты. Нажать «Добавить компоненты».



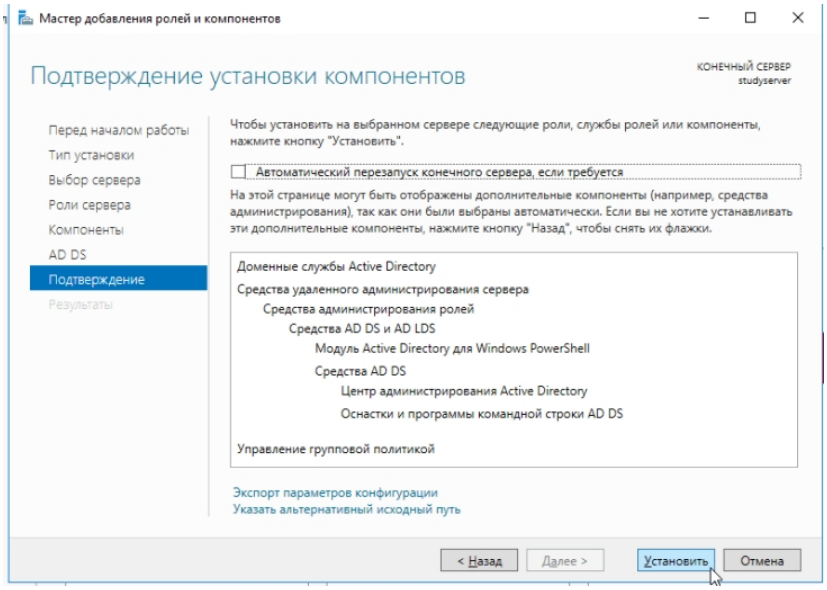
1. В окне выбора компонентов нажать «Далее», поскольку необходимые компоненты были выбраны в предыдущем пункте.



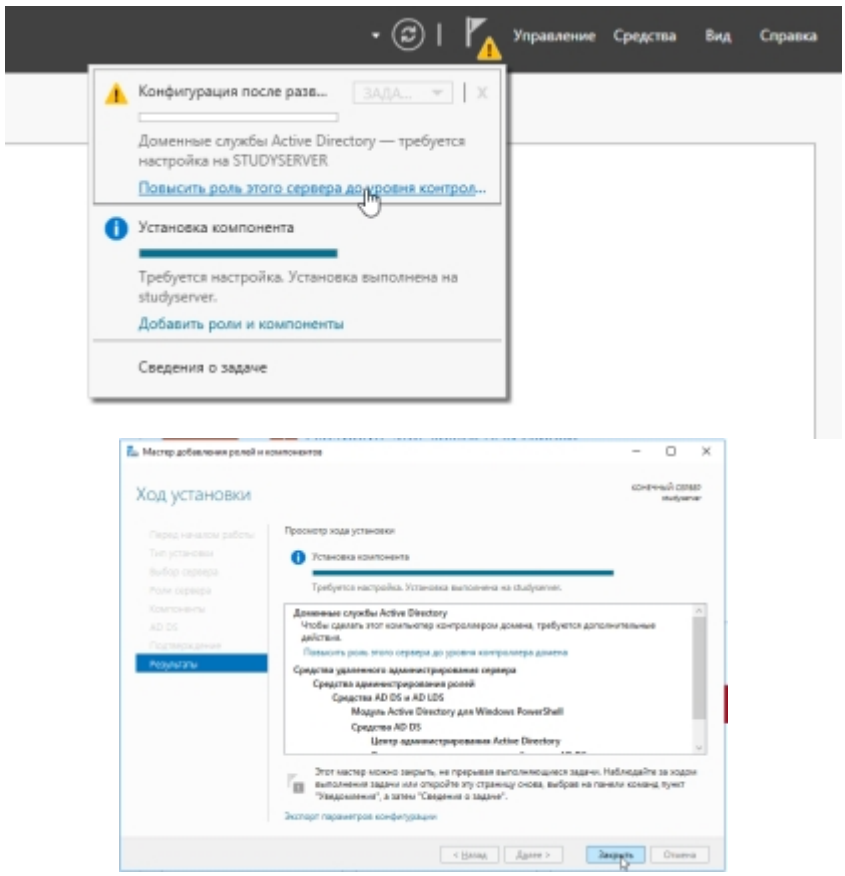
2. В следующем окне приведена краткая информация о службе Active Directory. Ознакомиться с ней и нажать «Далее».



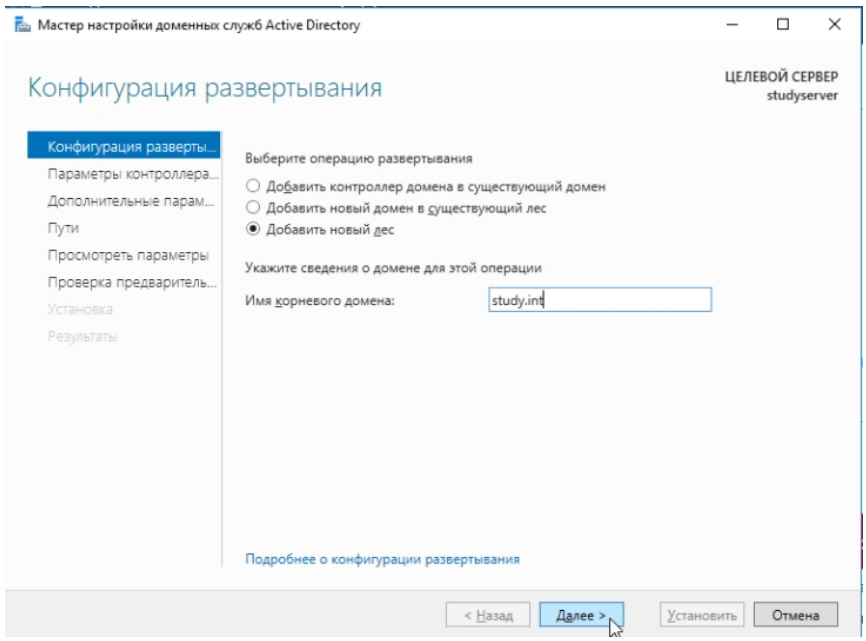
3. Ознакомиться со списком устанавливаемых компонентов и нажать «Установить».



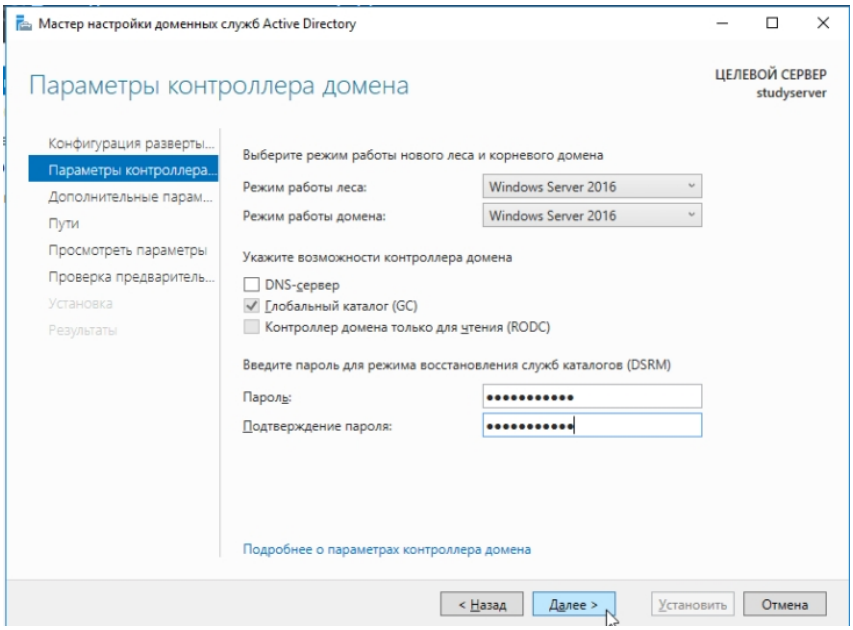
4. Дождаться окончания установки и нажать пункт «Повысить роль этого сервера до уровня контроллера домена». Либо, если мастер был случайно закрыт этот пункт можно выбрать в диспетчере серверов.



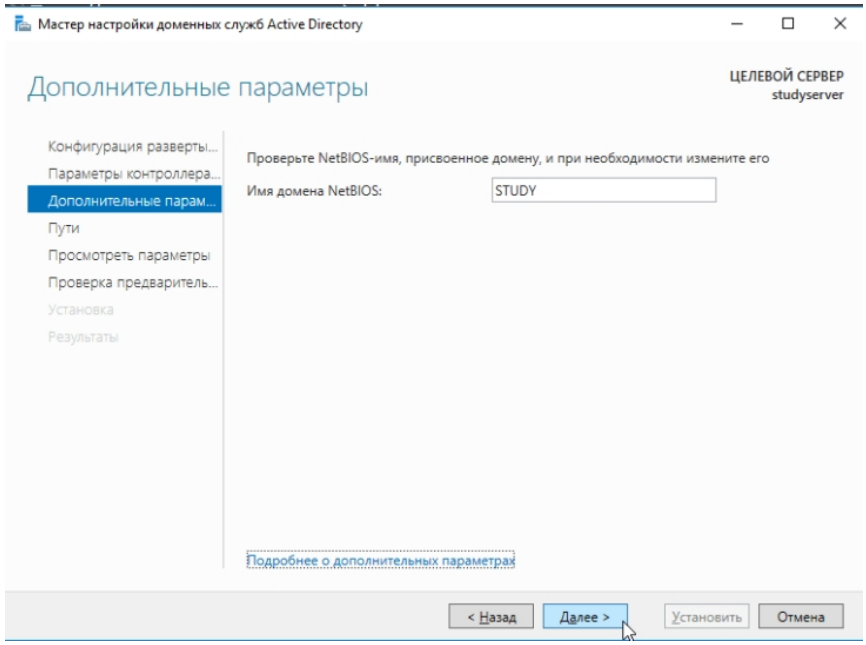
11. В мастере настройки доменных служб добавить новый лес и ввести имя домена.



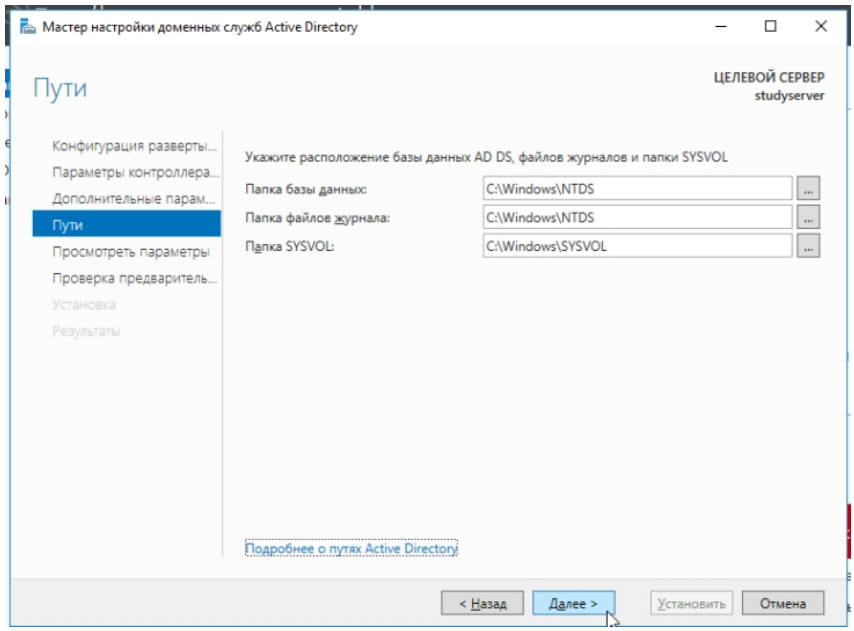
12. В параметрах контроллера домена выбрать режим работы леса и домена — Windows Server 2016 и создать пароль администратора домена.



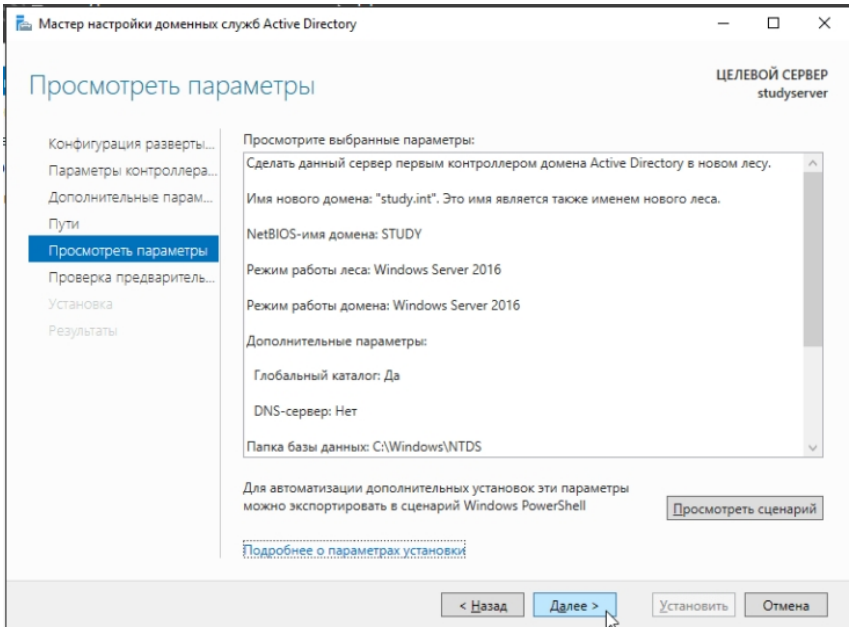
13. Проверить имя NetBIOS.



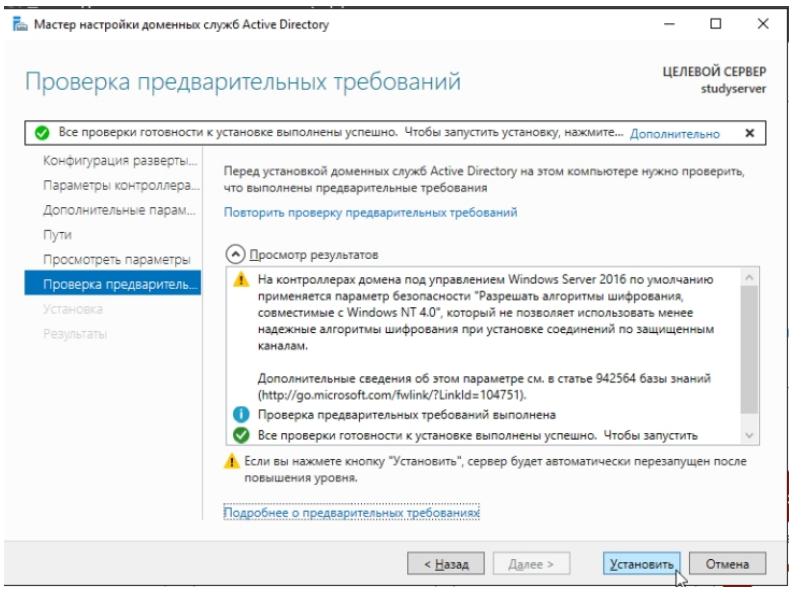
14. В пункте «Пути» оставить все по умолчанию.



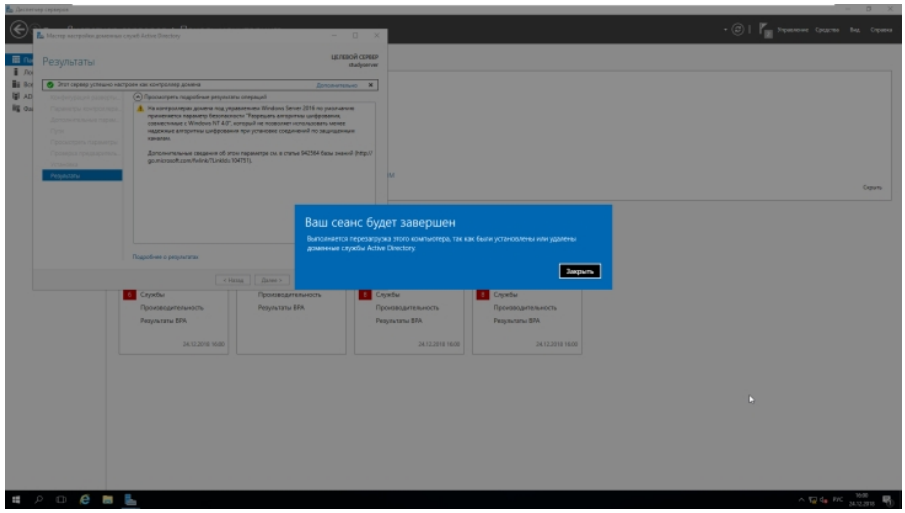
15. Проверить введенные параметры и нажать «Далее».



16. Начать установку.



17. После окончания установки сервер перезагрузится.



После перезагрузки для входа в систему нужно использовать пароль домена, поскольку машина будет автоматически введена в домен.

Проверить корректность установки можно, введя в Windows PowerShell команды:

Get-ADDomain | fl name, DomainMode

Get-ADForest | fl name, ForestMode

Ответ должен совпадать с введенными в ходе работы параметрами.

Раздел 3. Сетевое оборудование, безопасность
Тема3.2Создание и настройка беспроводной сети

Практическая работа №19

«Управление сервером WindowsServer с помощью MicrosoftManagementConsole»

Задачи обучающегося:

1. Освоить основные принципы и техники управления сервером с помощью оснастки
2. Закрепить знания по безопасности сети

Опорные понятия:консоль управления
Планируемый результат:
Студент должен
Научиться использовать возможности консоли MMC
Необходимое оборудование:ПК, VirtualBox

Алгоритм деятельности обучающегося:

Общие концепции консоли управления Microsoft

Консоль управления Microsoftпредназначена для запуска всех программных модулей администрирования, конфигурирования или мониторинга локальных компьютеров и сети в целом. Такие законченные модули называются оснастками (snap-ins). Консоль управления сама по себе не выполняет никаких функций администрирования, но служит в качестве рабочей среды для запуска оснасток, создаваемых как компанией Microsoft, так и независимыми поставщиками программного обеспечения.

Появление MMC обусловлено желанием создать единую среду управления для администрирования операционных систем Windows. Консоль MMC включает в себя интерфейсы прикладного программирования (API), оболочку пользовательского интерфейса (консоли) и набор инструкций.

Создавая специальную консоль, можно присвоить ей один из двух основных режимов доступа: авторский режим или режим пользователя. В свою очередь, существуют три уровня режима пользователя, так что всего имеется четыре варианта предустановленного режима доступа для консоли:

авторский режим;

режим пользователя - полный доступ;

режим пользователя - ограниченный доступ, многооконный;

режим пользователя - ограниченный доступ, однооконный.

Эти параметры могут быть настроены в диалоговом окне Параметры в консоли MMC.

Назначение консоли авторского режима предоставляет полный доступ ко всем возможностям MMC, включая добавление и удаление оснасток, создание новых окон и видов панели задач, добавление элементов в список "Избранное" и просмотр любых частей дерева консоли. При выборе одного из режимов пользователя исключаются авторские возможности, которые пользователь не может использовать. Например, если для консоли установлен параметр пользовательский режим - полный доступ, предоставляются все команды управления окном и полный доступ к дереву консоли, но пользователю запрещено добавление и удаление оснасток и изменение свойств консоли.

Изменения, внесенные в консоль в авторском и пользовательском режимах, сохраняются по разному. Если работа ведется в авторском режиме, при закрытии консоли будет выведено предложение сохранить изменения. Однако при работе в пользовательском режиме и снятом флажке Не сохранять изменения для этой консоли (доступном по команде Свойства в меню Консоль) изменения будут сохранены автоматически, когда консоль

закрывается.

4.1.2. Преимущества MMC

Возможность индивидуальной настройки и передача полномочий Помимо обеспечения интеграции и общей среды для административных инструментов, консоль MMC предоставляет возможность полностью индивидуальной настройки, так что администраторы могут создавать такие консоли управления, которые будут включать только необходимые им компоненты. Настройка консоли также позволяет администраторам передавать определенную часть полномочий менее опытным сотрудникам. С помощью MMC можно создать консоль, которая будет содержать объекты, необходимые для выполнения только определенных функций.

Интеграция и унификация

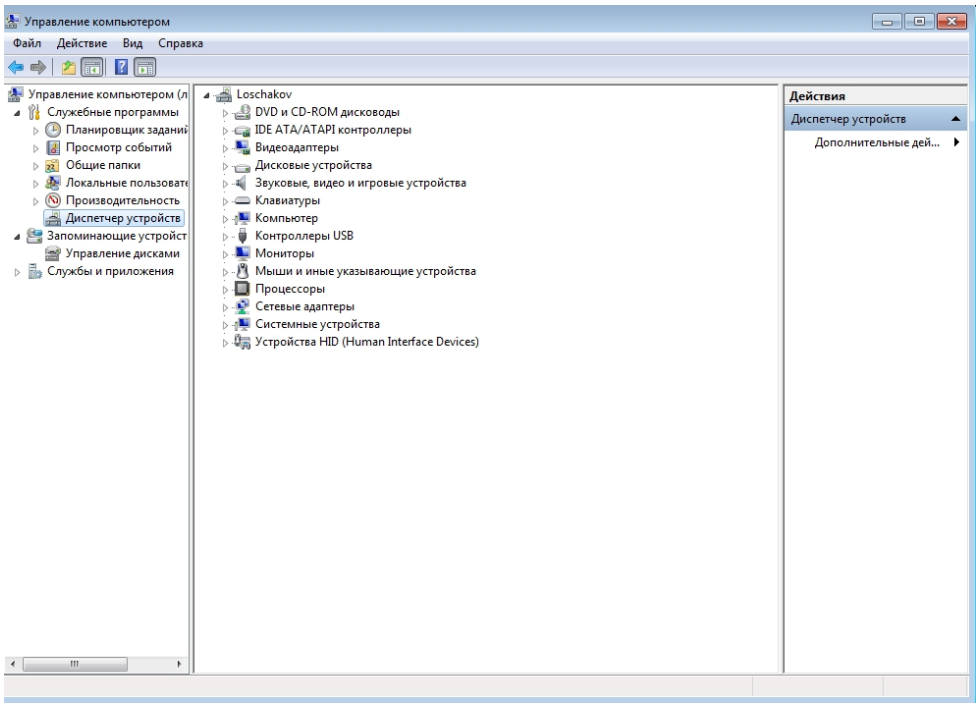
MMC обеспечивает общую среду, в которой могут запускаться оснастки. Администраторы могут управлять различными сетевыми продуктами, используя единый интерфейс, что упрощает изучение работы с различными инструментами.

Гибкость в выборе инструментов и продуктов

В среде MMC можно использовать различные инструменты и оснастки. Для использования в среде MMC оснастка должна поддерживать компонентную объектную модель (ComponentObjectModel, COM) или распределенную COM(DistributedComponentObjectModel, DCOM). Это позволяет выбирать наиболее оптимальный продукт среди оснасток, причем гарантируется его полная совместимость со средой MMC.

4.1.3. Пользовательский интерфейс MMC

Консоль управления MMC имеет пользовательский интерфейс, позволяющий открывать множество документов (MultipleDocumentInterface, MDI). Интерфейс консоли MMC на примере оснастки "Управление компьютером"



Родительское окно MMC имеет главное меню и панель инструментов. Главное меню обеспечивает функции управления файлами и окнами, а также доступ к справочной системе.

Дочерние окна MMC представляют собой различные средства просмотра автономного документа консоли. Каждое из этих дочерних окон содержит панель управления, панель структуры и панель результатов, или сведений. Панель управления содержит меню и набор инструментов. Панель структуры отображает пространство имен инструментов в виде

дерева, которое содержит все видимые узлы, являющиеся управляемым объектом, задачей или средством просмотра. Панель результатов в дочернем окне отображает список элементов выбранного узла. Данный список может содержать папки, оснастки, элементы управления, веб-страницы, панели задач и другие элементы.

4.1.4. Оснастки и работа с ними

Все инструменты MMC состоят из совокупности оснасток. Каждая оснастка представляет собой минимальную единицу управления. С технической стороны оснастка представляет собой "OLE-сервер внутри процесса" (DLL), который выполняется в контексте процесса MMC. Ряд оснасток могут быть объединены администратором в инструмент, который сохраняется в файле с расширением msc (ManagementSavedConsole).

В MMC поддерживаются два типа оснасток:

изолированная оснастка обеспечивает выполнение своих функций даже при отсутствии других оснасток, например "Управление компьютером";

оснастка расширения может работать только после активизации родительской оснастки. Функция оснастки расширения заключается в увеличении числа типов узлов, поддерживаемых родительской оснасткой. Примером оснастки расширения служит оснастка "Диспетчер устройств". Оснастки расширения могут предоставлять различные функциональные возможности. Например, такие оснастки могут расширять пространство имен консоли, увеличивать число пунктов в меню или добавлять определенные мастера.

Основные оснастки, доступные в системе Windows приведены в табл. 1.

Оснастка	Назначение
Анализинастройкабезопасности (Security Configuration and Analysis)	Служит для управления безопасностью системы с помощью шаблонов безопасности
Групповая политика (Group Policy)	Служит для назначения сценариев регистрации, групповых политик для компьютера и пользователей некоторого компьютера сети; позволяет просматривать и изменять политику безопасности, политику аудита и права пользователей
Дефрагментация диска (Disk Defragmenter)	Служит для анализа и дефрагментации дисковых томов
Диспетчер устройств (Device Manager)	Содержит список всех устройств, подключенных к компьютеру,и позволяет их конфигурировать
Локальные пользователи и группы (Local Users and Groups)	Служит для управления локальными учетными записями пользователей и групп
Общие папки (Shared Folders)	Отображает совместно используемые папки, текущие сеансы и открытые файлы
Оповещения и журналы производительности (Performance logs and Alerts)	Конфигурирует журналы данных о работе систем и службу оповещений
Папка (Folder)	Служит для добавления новой папки в дерево
Просмотр событий (Event Viewer)	Служит для просмотра и управления системным журналом, журналами безопасности и приложений

Сведения о системе (System Information)	Отображает информацию о системе
Сертификаты (Certificates)	Служит для управления сертификатами
Системный монитор (Performance)	Используется для сбора и просмотра в реальном времени данных, характеризующих работу памяти, дисков, процессора и других компонентов системы
Служба индексирования (Indexing Service)	Служит для индексирования документов различных типов с целью ускорения их поиска
Служба компонентов (Component Services)	Конфигурирует и управляет службами компонентов COM+
Службы (Services)	Запускает, останавливает и конфигурирует службы (сервисы) Windows
Ссылканаресурсвеб (Link to Web Address)	Служит для подключения веб-сраниц (html, asp, stml)
Управление дисками (Disk Management)	Служит для управления дисками и защитой данных, для разбиения дисков на логические тома, форматирования, управления совместным доступом, квотами и т. д.
Управление компьютером (Computer Management)	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток расширения
Управление политикой безопасности IP (IP Security Policy Management)	Служит для управления политиками IPSec для безопасного соединения с другими компьютерами
Управление службой факсов (Fax Service Management)	Служит для управления службой и устройствами факсимильной связи
Управление съемными носителями (Removable Storage Management)	Служит для управления сменными носителями информации
Управляющий элемент (WMI Control)	Служит для конфигурирования средств WindowsManagementInstrumentation и управления ими
Шаблоны безопасности (Security Templates)	Обеспечивает возможность редактирования файлов - шаблонов безопасности
Элемент ActiveX (ActiveX Control)	Подключение к дереву консоли различных элементов управления ActiveX

Работа в консоли управления Microsoft

Запустить консоль управления MMC. Для этого выполнить следующие операции: В меню **Пуск** выбрать пункт **Выполнить,** ввести mmc и нажать кн. OK. Откроется окно **Консоль1** с пустой консолью.

По умолчанию консоль MMC открывается в авторском режиме, в котором можно создавать новые консоли и изменять созданные ранее административные инструменты. Пустая консоль не имеет никаких функциональных возможностей до тех пор пока в нее не добавлены оснастки. Команды меню MMC на панели меню в верхней части окна применимы ко всей консоли.

Добавить в консоль необходимые оснастки:

В меню Консоль выбрать пункт Добавить/удалить оснастку. Откроется окно Добавить/удалить оснастку. В этом окне перечисляются изолированные оснастки и оснастки расширения, которые будут добавлены в консоль (или уже включены в нее).

Нажать кн. Добавить. На экране появится окно Добавить изолированную оснастку (рис. 2) со списком изолированных оснасток, имеющихся в системе.

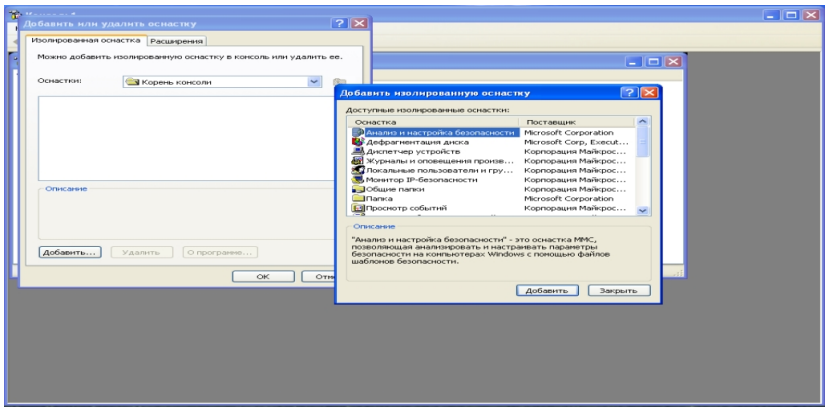


Рис. 2. Окно со списком имеющихся оснасток

Дважды щелкнуть на пункте **Управление компьютером.** Появится окно с конфигурационными опциями для данной оснастки. Оставить переключатель в положении **локальным компьютером** и щелкнуть на кн. **Готово,** далее на кн. **Закрыть.**

Закрыть окно добавления оснасток, нажав кн. OK. Теперь окно консоли содержит оснастку **"Управление компьютером",** аналогичную представленной на Сохранить созданный инструмент в личной папке, в качествеимени файла использовать свою фамилию. Для этогов меню **Консоль**выбрать пункт **Сохранить как** и указать имя файла и папку, в которойбудетсохранен файл консоли.

Развернуть окно консоли MMC на весь экран и настроитьразмеры окон и столбцов таким образом, чтобы обеспечить наиболееудобную работу.Просмотреть все узлы оснастки "Управление компьютером.Предварительно в меню **Вид** выбрать режим **Дополнительно.**

Раздел 3. Сетевое оборудование, безопасность
Тема3.3Безопасность сети

Практическая работа №20
«Установка, настройка, администрирование сетевых сервисов: создание резервных копий.»

Задачиобучающегося:

1. Познакомиться с методами и резервного копирования.
2. Изучить работу встроенных утилит

Опорные понятия:резервное копирование
Планируемый результат:

Студент должен
Уметь выполнять резервное копирование по расписанию и заданным условиям
Необходимое оборудование:ПК

Краткие теоретические и справочно-информационные материалы по теме занятия.

Ни один носитель информации не является абсолютно надежным, из строя может выйти любое устройство хранения данных, и данные могут быть потеряны. Кроме аппаратных сбоев возможна также потеря данных по причине действия вредоносных программ (вирусы и т.п.). А самая распространенная причина порчи или удаления данных — ошибки пользователей (как обычных, так и администраторов), которые могут по ошибке удалить или перезаписать не тот файл.

По этой причине возникает необходимость регулярного создания резервных копий информации — файлов с документами, баз данных и состояния операционной системы.

Системы семейства Windows Server имеют встроенный инструмент создания резервных копий — утилиту ntbackup. Данная утилита позволяет сохранять резервные копии на самых различных носителях — ленточных накопителях, магнитооптических дисках, жестких дисках (как на локальных дисках данного сервера, так и на сетевых ресурсах, размещенных на других компьютерах сети). В версии системы Windows 2003 реализован механизм т.н. теневых копий Shadow Copy, который заключается в том, что в начале процедуры архивации система делает моментальный «снимок» архивируемых файлов и уже после этого создает резервную копию из этого снимка. Данная технология позволяет архивировать файлы, которые в момент запуска утилиты ntbackup были открыты пользователями. Сетевой администратор должен совместно с пользователями определить те данные, которые нужно регулярно архивировать, спланировать ресурсы, необходимые для создания резервных копий, составить расписание резервного копирования, настроить программу резервного копирования и планировщик заданий для автоматического создания резервных копий. Кроме этого, в задачу сетевого администратора входит также регулярное тестирование резервных копий и пробное восстановление данных из резервных копий (чтобы вовремя обнаружить возникающие проблемы в создании резервных копий).

Архивирование и восстановление файловых ресурсов. Базовые понятия службы резервного копирования

Все операции по созданию резервных копий и восстановлению данных в ОС семейства Windows осуществляются утилитой ntbackup.

Рассмотрим основы резервного копирования файловых ресурсов. Каждый файл, хранящийся на диске компьютера, независимо от типа файловой системы, имеет атрибут archive, который в Свойствах файла отображается как «Файл готов для архивирования» (откройте Свойства файла и нажмите кнопку «Другие»). Если в Свойствах файла вручную убрать галочку у этого атрибута, то при любом изменении в файле операционная система автоматически снова установит этот атрибут. На использовании изменений данного атрибута основаны все используемые в системе Windows методики резервного копирования. Типы резервного копирования

Утилитой ntbackup можно создавать резервные копии различных типов. Рассмотрим их отличительные особенности и различные варианты их применения.

Обычный (Normal)

При выполнении данного типа архивирования утилита ntbackup архивирует все файлы, отмеченные для архивации, при этом у всех заархивированных файлов очищается атрибут «Файл готов для архивирования». Данный вид архивирования необходим для создания еженедельных полных резервных копий каких-либо больших файловых ресурсов. Если в компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.

Разностный (Differential)

При выполнении Разностного архивирования утилита ntbackup из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут не очищается. Использование Обычного и Разностного архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Например, если раз в неделю (как правило, в выходные дни) создавать Обычные копии, а в течение недели ежедневно (как правило, в ночное время) — Разностные, то получается выигрыш в объеме носителей для резервного копирования. При такой комбинации архивирования «Обычный + Разностный» процесс восстановления данных в случае утери информации потребует выполнения двух операций восстановления — сначала из последней Полной копии, а затем из последней Разностной резервной копии. Добавочный (Incremental) При выполнении Добавочного архивирования утилита ntbackup из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут очищается. Использование Обычного (раз в неделю по выходным) и Добавочного (ежедневно в рабочие дни) архивирования также позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Но процесс восстановления данных при использовании комбинации «Обычный + Добавочный» уже будет выполняться иначе: в случае утери информации для восстановления данных потребуется сначала восстановить данные из последней Полной копии, а затем последовательно из всех Добавочных копий, созданных после Полной копии.

Копирующий (Copy)

При таком типе архивирования утилита ntbackup заархивирует все отмеченные файлы, при этом атрибут «Файл готов для архивирования» остается без изменений.

Ежедневный (Daily)

Ежедневный тип архивирования создает резервные копии только тех файлов, которые были модифицированы в день создания резервной копии.

Два последних типа не используются для создания регулярных резервных копий. Их удобно применять в тех случаях, когда с какой-либо целью нужно сделать копию файловых ресурсов, но при этом нельзя нарушать настроенные регулярные процедуры архивирования.

Разработка и реализация стратегии резервного копирования. Понятие плана архивации

Создание и реализация плана архивации и восстановления информации — непростая задача. Сетевому администратору надо определить, какие данные требуют архивации, как часто проводить архивацию и т. д.

При создании плана ответьте на следующие вопросы:

Насколько важны данные? Этот критерий поможет решить, как, когда и какую информацию архивировать. Для критичной информации, например, баз данных, следует создавать избыточные архивные наборы, охватывающие несколько периодов архивации. Для менее важной информации, например, для текущих пользовательских файлов, сложный план архивации не нужен, достаточно регулярно сохранять их и уметь легко восстанавливать.

К какому типу относится архивируемая информация? Тип информации поможет определить необходимость архивации данных: как и когда данные должны быть сохранены.

Как часто изменяются данные? Частота изменения влияет на выбор частоты архивирования. Например, ежедневно меняющиеся данные необходимо сохранять каждый день.

Нужно ли дополнить архивацию созданием теневых копий? При этом следует помнить, что теневая копия — это дополнение к архивации, но ни в коем случае не ее замена.

Как быстро нужно восстанавливать данные? Время — важный фактор при создании плана архивации. В критичных к скорости системах нужно проводить восстановление очень

быстро. Какое оборудование оптимально для архивации и есть ли оно у вас? Для своевременной архивации вам понадобится несколько архивирующих устройств и несколько наборов носителей. Аппаратные средства архивации включают ленточные накопители (это наименее дорогой, но и самый медленный тип носителя), оптические диски и съемные дисковые накопители.

Кто отвечает за выполнение плана архивации и восстановления данных? В идеале и за разработку плана, и собственно за архивацию и восстановление должен отвечать один человек.

Какое время оптимально для архивации? Архивация в период наименьшей загрузки системы пройдет быстрее, но не всегда возможно провести ее в удобные часы. Поэтому с особой тщательностью архивируйте ключевые данные. Нужно ли сохранять архивы вне офиса? Хранение архивов вне офиса — важный фактор на случай стихийного бедствия. Вместе с архивами сохраните и копии ПО для установки или переустановки ОС.

Для построения правильной и эффективной системы резервного копирования необходимо детально изучить и задокументировать все файловые ресурсы, используемые в компании, а затем тщательно спланировать стратегию резервного копирования и реализовать ее в системе. Для планирования стратегии необходимо ответить на следующие вопросы:

какие именно ресурсы будут архивироваться;

минимальный промежуток времени для восстановления данного ресурса при возникновении аварии;

какой объем данных будет архивироваться;

какова емкость носителей для хранения резервных копий и скорость записи на эти носители;

сколько времени будет занимать архивирование каждого ресурса;

как часто будет производиться архивация каждого ресурса;

если резервные копии записываются на ленты, то как часто будет производиться перезапись лент;

по какому графику будет производиться тестовое восстановление данных.

При ответе на эти вопросы будет спланирована потребность в количестве и емкости накопителей и устройств для выполнения резервных копий, требования к пропускной способности сети для создания резервных копий, график выполнения резервного копирования, план восстановления на случай аварии.

Выбор архивных устройств и носителей

Определив, какие данные и как часто архивировать, можно выбрать аппаратные средства архивации и необходимые носители. Инструментов для архивации данных множество. Одни быстрые и дорогие, другие — медленные и надежные. Выбор подходящего оборудования для организации зависит от многих факторов.

Емкость — количество регулярно архивируемых данных. Справится ли оборудование с нагрузкой в отведенное время?

Надежность аппаратных средств и носителей. Можете ли вы пожертвовать надежностью ради экономии или скорости?

Расширяемость решения. Удовлетворяет ли ваше решение потребностям роста организации?

Скорость архивации и восстановления. Можете ли вы пожертвовать скоростью ради снижения стоимости?

Цена архивации. Приемлема ли она для вашего бюджета?

Типовые решения архивации

Итак, на план архивации влияют емкость, надежность, расширяемость, скорость и цена. Определив, какие из этих факторов наиболее важны для вашей организации, вы примете подходящее решение. Вот некоторые общие рекомендации:

Ленточные накопители — самые распространенные устройства архивации. Данные

хранятся на кассетах с магнитной лентой. Лента относительно недорога, но не особенно надежна: она может помяться или растянуться, с течением времени — размагнититься и перестать считываться. Средняя емкость кассет с лентой варьируется от единиц до десятков Гбайт. По сравнению с другими решениями ленточные накопители довольно медленны. Их достоинство — невысокая цена.

Накопители на цифровой ленте (digital audio tape, DAT) — пришли на смену традиционным ленточным накопителям. Существует несколько форматов DAT, их емкости составляют 35 и 260 Гбайт.

Ленточная библиотека с автозагрузкой — устройство для создания расширенных архивных томов на нескольких лентах, которых хватает для нужд всего предприятия. Ленты набора в процессе архивации или восстановления данных автоматически меняются. В большинстве таких библиотек применяются DAT-ленты. Их главный «минус» — высокая цена.

Магнитооптические накопители с автозагрузкой подобны ленточным библиотекам, только вместо лент в них используются магнитооптические диски. Цена также очень высока.

Съемные диски, например Iomega Jazz емкостью 1-2 Гбайт, все чаще используются в качестве устройств архивации. Они обладают хорошей скоростью и удобны в работе, но стоят дороже ленточных или DAT-накопителей.

Дисковые накопители обеспечивают наивысшую скорость при архивации и восстановлении файлов. Если при архивации на ленту вам потребуются часы, то диско- вый накопитель позволяет завершить процесс за несколько минут. К недостаткам дисковых накопителей следует отнести относительно высокую цену.

Задание:

1. Создать на диске **«С»** Вашего сервера каталог **backup** и **restore**;

2. В папке **library**, созданной в одной из предыдущих работ создать 3 текстовых файла с наименованиями **book1.txt, book2.txt и book3.txt**. Файлы должны содержать свое наименование.

3. Запустить утилиту резервного копирования **ntbackup**. Эту утилиту можно запустить из Главного меню системы (кнопка «Пуск» — «Все программы» — «Стандартные» — «Служебные» — «Архивация данных»), а можно запустить более быстро из командной строки (кнопка «Пуск» — «Выполнить» — «ntbackup» — кнопка «ОК»). При первом запуске утилиты рекомендуем убрать галочку у поля «Всегда запускать в режиме мастера».

4. Запустить «Мастер архивации» (на закладке «Добро пожаловать» нажать кнопку «Мастер архивации».

5. После запуска мастера нажмем кнопку «Далее» и выберем, что нам нужно архивировать, в данном примере — «Архивировать выбранные файлы, диски или сетевые данные»

6. Выберем для архивирования папку **library.**

7. Выберем место для создания резервной копии, создадим файл с именем **library**, этому файлу автоматически будет назначено расширение **«.bkf»**

8. На данном этапе нажмем кнопку «Готово».

9. Проверяем полученный результат.

10. Вносим изменение в файл **book1.txt и book2.txt**, у файла **book1.txt** убираем атрибут «Файл готов для архивирования», а **book3.txt - удаляем**.

11. Запускаем снова процесс архивации, но на 8 этапе нажмем кнопку «Дополнительно», чтобы задать дополнительные параметры и выбираем тип архивации **«Добавочный».** Далее все пункты по умолчанию, но при этом не забывайте запоминать, что Вы делаете. Проверяем полученный результат. Почему он такой?

12. Восстановите файл **book3.txt**. Для этого выполните следующие действия:

Запустим утилиту резервного копирования **ntbackup**.

Перейдем на закладку "Восстановление и управление носителем".

После появления в списке архивных файлов нужного архива раскроем этот архив и выберем файлы для восстановления из резервной копии. При этом мы можем восстановить файлы в то место, где они были ранее ("Исходное размещение") или выбрать иной путь для их сохранения ("Альтернативное размещение"). Выберите папку restore.

После определения всех параметров восстановления нажмем кнопку "Восстановить", утерянные данные будут восстановлены.

13. Создайте задания на выполнения архивации данных для папки **profiles,** используя выбор дополнительных возможностей:

Выбираем тип архивирования (выберем «Обычный»).

Ничего не меняем на странице «Способы архивации».

На странице «Параметры архивации» можно выбрать замену существующих архивов или добавление архива (если файл с архивной копией уже существует).

14. На странице «Когда архивировать» задайте расписание для автоматического создания резервной копии — выберите вариант «Позднее» и задайте расписание архивирования, чтобы архивирование происходило по всем рабочим дням недели. Время начала установите, исходя из текущего времени системы + пять минут.

15. Нажмите далее. Система запросит имя и пароль пользователя, с чьими полномочиями будет выполняться задание архивирования. Рекомендуем для выполнения заданий резервного копирования создать специальные учетные записи, обладающие достаточными правами (как минимум члены группы «Операторы архива»).

16. Нажмем кнопку «Готово», задание будет создано, и оно появится в списке «Назначенных заданий». Теперь оно будет выполняться регулярно в соответствии с расписанием.

17. Завершите сеанс администратора, ожидайте до завершения задания. После проверьте результат.

Контрольные вопросы

1. Какие причины резервирования данных?
2. Какие существуют типы резервного копирования?
3. Какие преимущества дает механизм теневых копий?
4. Какие типы резервного копирования Вы знаете? В чем их особенности?
5. Кто планирует какие данные нужно резервировать?