МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Казанский национальный исследовательский технический университет
им. А.Н. Туполева-КАИ»
(КНИТУ-КАИ)
Чистопольский филиал «Восток»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

по дисциплине

СЕТЕВЫЕ ТЕХНОЛОГИИ

Индекс по учебному плану: **Б1.В.ДВ.06.03**
Направление подготовки: **09.03.01 Информатика и вычислительная техника**
Квалификация: **Бакалавр**
Профиль подготовки: **Автоматизированные системы обработки информации и управления**
Типы задач профессиональной деятельности: **проектный, производственно-технологический**

Рекомендовано УМК ЧФ КНИТУ-КАИ

Чистополь
2023 г.

Введение

Методические рекомендации по выполнению лабораторных работ предназначены для закрепления и углубления знаний, полученных в процессе обучения по дисциплине «Сетевые технологии».

Издание включает в себя описания лабораторных работ, основной целью которых является получение знаний по основам построения, функционирования и использования компьютерных сетей различного масштаба, возможностей их реализации на основе базовых сетевых технологий и стандартов.

Каждая работа сопровождается кратким теоретическим материалом и заданиями на выполнение.

Перед выполнением лабораторных работ следует повторить материал соответствующей лекции и изучить теоретическую часть методических рекомендаций, приведенных ниже.

Для защиты лабораторных работ необходимо выполнить все задания по каждой работе, составить отчет с выводами, характеризующими полученные результаты, и объяснить технологию выполнения.

Лабораторная работа №1

Команды диагностики сетевых подключений

Цель работы: апробация команд на персональном компьютере.

Перечень изучаемых команд:

1. Pathping – одна из самых полезных новых команд диагностики TCP/IP. Она объединяет функциональность Ping и Tracert. Команда Pathping опрашивает каждый маршрутизатор на пути между источником и приемником сигнала, после чего фиксирует задержки при каждой ретрансляции сигнала и потери пакетов.

Пример:

C:\>pathping ya.ru

2. Ping. Команда Ping лежит в основе диагностики сетей TCP/IP. Если до системы не удается «достучаться» с помощью этой команды, вероятнее всего, с такой системой связаться не удастся. Чтобы опросить станцию с IP-адресом 192.168.100.1, следует набрать: C:\>ping 192.168.100.1

3. Tracert. Эта команда используется для верификации пути через маршрутизатор между данной станцией и удаленной. Tracert фиксирует число переходов или «прыжков» (hop), которые потребовалось совершить на пути к станции назначения.

Пример:

C:\>tracert yahoo.com

4. Nslookup – основная команда для диагностики проблем, связанных с работой DNS. Эта команда интерактивная, после ее вызова появляется специальная командная строка. Чтобы вывести список команд Nslookup, нужно вызвать справку об этой утилите. Подкоманда ls, например, выводит информацию о домене DNS:

C:\>nslookup

5. Route. Эта команда нужна для редактирования или просмотра таблицы маршрутов IP из командной строки. Windows 2000 использует таблицу маршрутов в том случае, когда нужно отыскать путь к удаленному компьютеру по TCP/IP.

Ключ ? выводит все доступные ключи при работе с Route. Для просмотра таблицы маршрутов системы используется Route Print:

Попробовать команды route print, route add, route del

6. Netstat. Команда Netstat показывает текущий статус и статистику подключений по TCP/IP или UDP. При этом выводятся данные, как о локальных, так и об удаленных именах и портах активных сетевых соединений. Ключ ? показывает все доступные ключи при работе с Netstat. Чтобы вывести все активные подключения, отсортированные по возрастанию номера порта, необходимо набрать: C:\>netstat –n

7. Ipconfig. Эта команда отображает текущие настройки TCP/IP. Кроме того, Ipconfig может вывести отчет об адресах серверов DNS:

Пример:

C:\>ipconfig /all

8. Arp. Команда Arp используется для просмотра, добавления или удаления записей в таблицах трансляции адресов IP в физические адреса. Эти записи используются при работе протокола Address Resolution Protocol (ARP). Чтобы просмотреть содержимое занесенных в кэш адресов IP и MAC-адресов конкретной системы, нужно набрать:

ПРИМЕР

C:\>arp -a

9. Lpq – показывает статус очереди удаленного принтера Line Print Daemon (LPD). Например, чтобы показать статус принтера HPLJ4 (имя указывается вслед за ключом -P) на системе с именем teca4 (указывается за ключом -S), следует набрать:

C:\>lpq

Отображение состояния удаленной очереди печати lpd.

Использование: lpq -Scepвер -Pпринтер [-l]

Параметры:

-S сервер Имя или адрес IP узла, предоставляющего службу lpd

-P принтер Имя очереди печати

-l Режим подробного вывода

ПРИМЕР

C:\>lpq -Steca4 -PHPLJ4

10. Hostname – одна из основных утилит TCP/IP. Она выводит имя системы, на которой запущена команда:

ПРИМЕР:

C:\>hostname

Задания

1. Определите сетевые настройки компьютера.
2. Определите MAC-адреса вашего компьютера и взаимодействующих с вами сетевых устройств.
3. Опишите, какие DNS-сервера у вас прописаны.
4. Проведите диагностику дееспособности DNS-серверов.
5. Определите, какие порты и соединения активны на вашем компьютере.
6. Осуществите добавления IP-адреса в таблицу маршрутизации.
7. Определите имя вашего компьютера.

Лабораторная работа №2

Основы проектирования локально-вычислительной сети

Цель работы: овладение навыками работы в Microsoft Office Visio, планирование и проектирование компьютерной сети.

Процесс построения (проектирования) сети представляет собой упрощенное моделирование не наступившей действительности и включает в себя следующие основные этапы [1]:

1. *Анализ задач*, для решения которых создается сеть, а также определение объема финансирования проекта.

2. *Проектирование физической структуры* – этап, на котором анализируются начальные условия и создается детальный проект физической организации сети.

3. *Проектирование инфраструктуры* – этап, на котором определяются протоколы взаимодействия, используемые службы, политика безопасности и т.п. - т.е. логическая организация сети.

4. *Развертывание* – этап, связанный с прокладкой линий связи, установкой и настройкой оборудования.

Этап анализа является одним из важнейших, поскольку определяет все остальные решаемые задачи: как физическую структуру сети, так и логическую. Именно на данном этапе выступает основное различие компьютерных сетей.

На *этапе проектирования* решаются следующие задачи:

1. На основе определенных целевых требований к сети определяется необходимый состав оборудования и, прежде всего, компьютеров: количество, характеристики и т.д.

2. Определяется физическое расположение рабочих мест и определяются этажи и аудитории, которые будут охватываться сетью. При решении этой задачи должна учитываться принципиальная возможность прокладки линий связи к рабочим местам/помещениям.

3. Исходя из решаемых задач, стоимости и расположения, определяется тип физических линий связи, соединяющих рабочие места, состав и расположение коммуникационного оборудования (например, концентраторов).

4. Определяется способ подключения к Интернету: выбирается провайдер – организация, обеспечивающая подключение организации к сети Интернет. При выборе провайдера учитываются факторы: характеристики возможных физических соединений с провайдером, требования к оборудованию и необходимое дополнительное оборудование, начальная стоимость подключения, стоимость эксплуатации подключения, технологические ограничения подключения (невозможность использования некоторых служб).

5. Исходя из технических требований, определяется узел проектируемой сети, который будет являться шлюзом для подключения к Интернету и определяется место его расположения. При этом учитывается удобство физического соединения шлюза с проектируемой сетью и удобство подведения физических линий для подключения к Интернету.

Общий алгоритм, описывающий процесс построения сети:

1. Определение исходных данных.

– определение целей использования сети;

– определение требований к сети;

– характеристики используемого оборудования (компьютеры, сетевое оборудование, принтеры, модемы и др.);

– характеристика сетевого ПО (операционные системы, серверное ПО, антивирусное ПО);

– примерная схема здания в котором планируется строить сеть.

2. Проектирование сети.

– способ сегментирования и объединения сегментов (определение необходимых сегментов оборудования для их формирования);

– выбор типа кабеля (как правило выбирается неэкранированная витая пара);

– определение активных устройств (модемы, маршрутизаторы и т.п.);

– выбор программного обеспечения (серверные и клиентские ОС, серверное программное обеспечение и т.п.);

– разработка схемы сети (указываются узлы сети и длины соединительных кабелей).

3. Определение стоимости.

– анализ основных направлений затрат;

– составление примерной сметы затрат.

4. Примерный план проведения работ.

5. Развертывание сети.

При создании новой сети желательно учитывать следующие факторы:

– требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу);

– структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия); основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальней перспективе); характер передаваемой по сети информации;

– технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов);

– возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля;

– обслуживание сети и контроль ее безотказности и безопасности;

– требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям контроля обмена информацией и т.д. (например, если предполагается использование одного ресурса многими пользователями, то следует использовать серверную ОС);

– необходимость подключения к другим сетям (например, глобальным);

– имеющиеся компьютеры и их программное обеспечение, а также периферийные устройства (принтеры, сканеры и т.д.).

При выборе размера (под размером сети в данном случае понимается как количество объединяемых в сеть компьютеров, так и расстояния между ними) и структуры сети необходимо учитывать:

– количество компьютеров (следует оставлять возможность для дальнейшего роста количества компьютеров в сети);

– требуемую длину линий связи сети (например, если расстояния очень большие, может понадобиться использование дорогого оборудования).

– способы объединения частей сети (для объединения частей сети могут использоваться репитеры, репитерные концентраторы, коммутаторы, мосты и маршрутизаторы, причем в ряде случаев стоимость этого объединительного оборудования может даже превысить стоимость компьютеров, сетевых адаптеров и кабеля;

Возможность масштабирования (например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим, чем требуется в настоящий момент).

Пример. Пусть небольшое предприятие занимает три этажа, на каждом по пять комнат, и включает в себя три подразделения, по три группы. В этом случае можно построить сеть таким образом (рис. 1):

Рабочие группы занимают по 1–3 комнаты, их компьютеры объединены между собой репитерными концентраторами. Концентратор может использоваться один на комнату, один на группу или один на весь этаж. Концентратор целесообразно расположить в помещении, в которое имеет доступ минимальное количество сотрудников.

Подразделения занимают отдельный этаж. Все три сети рабочих групп каждого подразделения объединяются коммутатором, а для связи с сетями других подразделений используется маршрутизатор. Коммутатор вместе с одним из концентраторов лучше поместить в отдельной комнате.

Общая сеть предприятия включает три сегмента сетей подразделений, объединенных маршрутизатором. Этот же маршрутизатор может использоваться для подключения к глобальной сети.

Серверы рабочих групп располагаются в комнатах рабочих групп, серверы подразделений – на этажах подразделений.

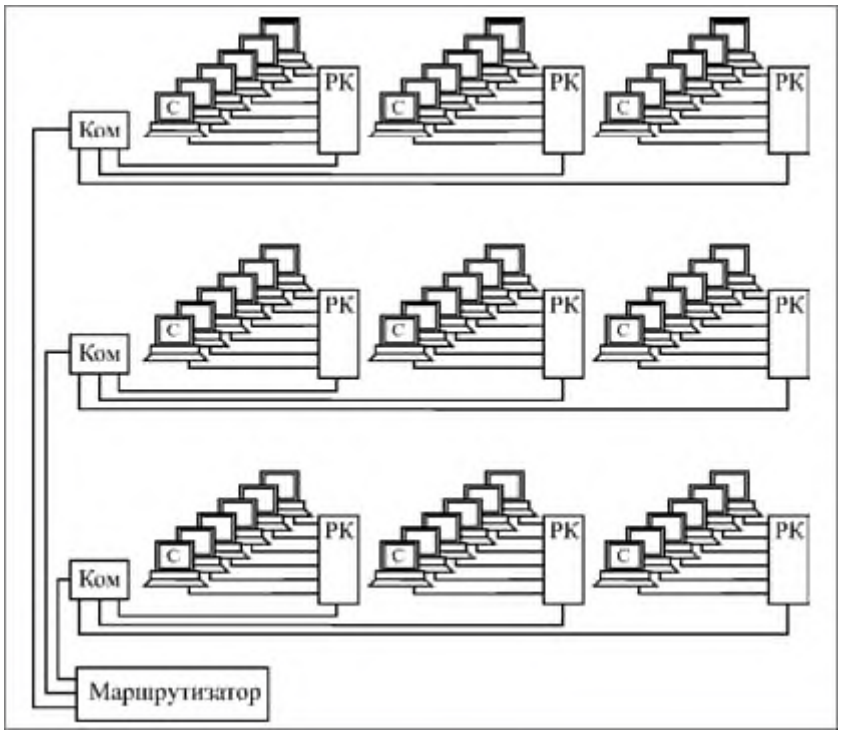

Рис. 1. Структура сети предприятия (С – серверы рабочих групп, РК – репитерные концентраторы, Ком – коммутаторы)

При выборе сетевого оборудования надо учитывать множество факторов, в частности:

– уровень стандартизации оборудования и его совместимость с наиболее распространенными программными средствами;

– скорость передачи информации и возможность ее дальнейшего увеличения;

– возможные топологии сети и их комбинации (шина, пассивная звезда, пассивное дерево);

– метод управления обменом в сети (CSMA/CD, полный дуплекс или маркерный метод);

– разрешенные типы кабеля сети, максимальную его длину, защищенность от помех;

– стоимость и технические характеристики конкретных аппаратных средств (сетевых адаптеров, трансиверов, репитеров, концентраторов, коммутаторов).

В настоящее время для организации локальных сетей в подавляющем большинстве случаев используется неэкранированная витая пара UTP. Более дорогие варианты на основе экранированной витой пары, оптоволоконного кабеля или беспроводных соединений применяются на предприятиях, где в этом существует действительно острая необходимость. Например, оптоволокно может использоваться для связи между удаленными сегментами сети без потери скорости.

При выборе сетевого программного обеспечения (ПО) надо, в первую очередь, учитывать следующие факторы:

– какую сеть поддерживает сетевое ПО: одноранговую, сеть на основе сервера или оба этих типа;

– максимальное количество пользователей (лучше брать с запасом не менее 20%);

– количество серверов и возможные их типы;

– совместимость с разными операционными системами и компьютерами, а также с другими сетевыми средствами;

– уровень производительности программных средств в различных режимах работы;

– степень надежности работы, разрешенные режимы доступа и степень защиты данных;

– какие сетевые службы поддерживаются;

– стоимость программного обеспечения, его эксплуатации и модернизации.

Еще до установки сети необходимо решить вопрос об управлении сетью. Даже в случае одноранговой сети лучше выделить для этого отдельного специалиста (администратора), который будет иметь всю информацию о конфигурации сети и распределении ресурсов и следить за корректным использованием сети всеми

пользователями. Если сеть большая, то одним сетевым администратором уже не обойтись, нужна группа, возглавляемая системным администратором.

После установки и запуска сети решать эти вопросы, как правило, слишком поздно.

При проектировании следует определить возможные направления финансовых затрат (к данному этапу проектирования необходимые предпосылки для решения этой задачи уже имеются):

– дополнительные компьютеры и обновление существующих компьютеров. Необязательное направление затрат: при достаточном количестве и качестве существующих компьютеров их обновление не требуется (или требуется в минимальном объеме – например, для установки более современных сетевых карт); в одноранговой сети не нужен (хотя и желателен) также специальный файл-сервер.

– сетевые аппаратные средства (кабели и все, что необходимо для организации кабельной системы, сетевые принтеры, активные сетевые устройства – повторители, концентраторы, маршрутизаторы и т.д.).

– сетевые программные средства, прежде всего, сетевая ОС на необходимое число рабочих станций (с запасом).

– оплата работы приглашенных специалистов при организации кабельной системы, установке и настройке сетевой ОС, при проведении периодической профилактики и срочного ремонта. Необязательное направление затрат: для небольших сетей со многими из этих работ может и должен справляться штатный сетевой администратор (возможно, с помощью других сотрудников данного предприятия).

Задание

Спроектировать компьютерную сеть (собрать исходные данные; выбрать: размер и структуру сети, оборудование, сетевые программные средства; спроектировать кабельную систему; рассчитать примерную стоимость оборудования) в соответствии с ***№ варианта.***

№ варианта	**Компьютерная сеть:**

1	Санаторий
2	Городская больница
3	Детский сад
4	Супермаркет
5	Банк
6	Городская электросеть
7	Теплоэнерго
8	Пенсионный фонд
9	Налоговая служба
10	Таможня

Лабораторная работа №3
Моделирования работы STP

Цель работы: изучение построения сетей на основе STP.

Spanning Tree Protocol – сетевой протокол, работающий на втором уровне модели OSI.

Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов. Происходит это путем автоматического блокирования ненужных в данный момент для полной связности портов.

Основное назначение протокола Spanning Tree - построение топологии ЛВС без избыточного дублирования соединений или закольцовывания, недопустимых в силу логики построения ЛВС. STP позволяет организовать в сети, построенной при помощи мостов (bridges), отказоустойчивую архитектуру [2].

Используя STP, вы можете построить сеть, в которой существует несколько параллельных путей, и гарантировать при этом, что:

– резервные пути прохождения трафика при нормальном функционировании основного пути заблокированы;

– один из резервных путей активизируется при нарушении основного пути.

Алгоритм работы STP

Spanning Tree Protocol переводится как "протокол покрывающего дерева". Кратко опишем алгоритм его действия:

1. Выбираем корневой коммутатор Root Bridge таким образом, чтобы его приоритет был наименьшим. Если существует несколько коммутаторов с одинаковыми приоритетами, то выбираем тот коммутатор, у которого наименьший MAC-адрес (младший наименьший байт).

2. Находим кратчайшие пути от корневого коммутатора ко всем остальным, опираясь на скорости соединений и стоимости портов.

3. Убираем со схемы все незадействованные соединения.

Дополнительные функции

Кроме основной задачи построения беспетлевой топологии STP решает еще одну дополнительную – изменение времени хранения MAC адресов в таблицах коммутаторов в случае изменения состояния портов. Происходит это следующим образом: коммутатор, на котором произошло изменение (например, отключился и снова включился порт), посылает в сторону корневого специальный BPDU Topology Change Notification (TCN). Корневой после его получения рассылает TCN для всех коммутаторов и они изменяют время хранения MAC адресов в своих таблицах с целью обеспечения коммутации пакетов с учетом возможных изменений (например, на порту изменился MAC адрес клиента, а коммутатор по умолчанию продержит соответствующую запись в таблице слишком долго).

Задания

1. Опишите работу протокола STP на сети из 5 коммутаторов A,B,C,D,E. Скорости соединений:A-B=100 Mbps, A-E=100 Mbps, A-D=10 Mbps, B-C=100 Mbps, B-D=100 Mbps, B-E=10 Mbps, C-D=100 Mbps, D-E=100 Mbps. Приоритеты: A-32000 B-17323 C-1523 D-1456 E-1456. MAC-адреса: A=00:16:d4:df:b6:7b, B=00:1c:f0:ce:00:c1, C=00:1a:92:34:53:41, D=00:17:9a:07:11:1d, E= 00:1a:92:34:53:be. Cost (стоимость портов): для 10 Mbps – 100 (условных единиц); для 100 Mbps – 10 (условных единиц); для 1 Gbps – 1 (условных единиц); для 10 Gbps – 1 (условных единиц).

Привести первоначальную схему включения коммутаторов, указать приоритеты, определить корень дерева, разорвать ненужные связи по STP. Смоделировать ситуацию выхода из строя коммутатор E и пересчитать STP.

2. Опишите работу протокола STP на сети из 8 коммутаторов A,B,C,D,E,F,G,H. Скорости соединений коммутаторов: A-B=100mbps, B-C=1gbps, C-D=100mbps, D-E=100mbps, E-F=10mbps, F-G=10mbps, G-H=100mbps, H-

A=100mbps, A-C=10mbps, A-E=100mbps, A-G=10mbps, B-E=100mbps, B-G=100mbps, C-F=10mbps, C-H=10mbps, D-G=100mbps, E-H=100mbps. Приоритеты у всех коммутаторов по умолчанию (*Priority=32768*) за исключением C=1200. Cost (стоимость портов): для 10 Mbps – 100 (условных единиц); для 100 Mbps – 19 (условных единиц); для 1 Gbps – 4 (условных единиц); для 10 Gbps – 2 (условных единиц).

Привести первоначальную схему включения коммутаторов, указать приоритеты, определить корень дерева, разорвать ненужные связи по STP. Смоделировать ситуацию выхода из строя коммутатор B и пересчитать STP.

3. Опишите работу протокола STP на сети из 5 коммутаторов A,B,C,D,E. Скорости соединений:A-B=100 Mbps, A-E=100 Mbps, A-D=10 Mbps, B-C=100 Mbps, B-D=100 Mbps, B-E=10 Mbps, C-D=100 Mbps, D-E=100 Mbps. Приоритеты: A-32000 B-17323 C-1523 D-1456 E-1456. MAC-адреса A=00:16:d4:df:b6:7b, B=00:1c:f0:ce:00:c1, C=00:1a:92:34:53:41, D=00:17:9a:07:11:1d, E= 00:1a:92:34:53:be. Cost (стоимость портов): для 10 Mbps – 100 (условных единиц); для 100 Mbps – 10 (условных единиц); для 1 Gbps – 1 (условных единиц); для 10 Gbps – 1 (условных единиц).

Привести первоначальную схему включения коммутаторов, указать приоритеты, определить корень дерева, разорвать ненужные связи по STP. Смоделировать ситуацию выхода из строя коммутатор D и пересчитать STP.

4. Опишите работу протокола STP на сети из 8 коммутаторов A,B,C,D,E,F,G,H. Скорости соединений коммутаторов: A-B=100mbps, B-C=1gbps, C-D=1gbps, D-E=100mbps, E-F=10mbps, F-G=10mbps, G-H=100mbps, H-A=100mbps, A-C=10mbps, A-E=100mbps, A-G=10mbps, B-E=100mbps, B-G=100mbps, C-F=10mbps, C-H=10mbps, D-G=100mbps, E-H=100mbps. Приоритеты у всех коммутаторов по умолчанию(*Priority=32768*). MAC адреса коммутаторов: A=1A:2C:33:F6:FF:A5, B = 5F:22:B3:06:00:A5, C = AA:21:DD:FE:01:35, D = 0B:21:F3:56:01:C5, E = F:89:01:E7:EF:D5, F = 11:2E:36:FC:7F:AA, G = 50:01:02:03:04:A5, H = 7A:77:35:4F:AF:BB. Cost (стоимость портов): для 10 Mbps –

100 (условных единиц); для 100 Mbps – 19 (условных единиц); для 1 Gbps – 4 (условных единиц); для 10 Gbps – 2 (условных единиц).

Привести первоначальную схему включения коммутаторов, указать приоритеты, определить корень дерева, разорвать ненужные связи по STP. Смоделировать ситуацию, когда выходит из строя коммутатор C и перестроить STP.

5. Опишите работу протокола STP на сети из 8 коммутаторов A,B,C,D,E,F,G,H. Скорости соединений коммутаторов: A-B=100mbps, B-C=1gbps, C-D=10gbps, D-E=100mbps, E-F=10mbps, F-G=10mbps, G-H=100mbps, H-A=100mbps, A-C=10mbps, A-E=100mbps, A-G=10mbps, B-E=100mbps, B-G=100mbps, C-F=10mbps, C-H=10mbps, D-G=100mbps, E-H=100mbps. Приоритеты у всех коммутаторов по умолчанию (*Priority=32768*) за исключением C=1200, D=1000. Cost (стоимость портов): для 10 Mbps – 100 (условных единиц); для 100 Mbps – 19 (условных единиц); для 1 Gbps – 4 (условных единиц); для 10 Gbps – 2 (условных единиц).

Привести первоначальную схему включения коммутаторов, указать приоритеты, определить корень дерева, разорвать ненужные связи по STP. Смоделировать ситуацию, когда выходит из строя коммутатор C и пересчитать STP.

Лабораторная работа №4
Создание общих ресурсов и управление ими

Цель работы: получение навыков предоставления доступа к ресурсам компьютера и использование сетевых ресурсов в ОС Windows.

Операционная система (ОС) – это совокупность программных средств, осуществляющая управление ресурсами компьютера, запуск прикладных программ и их взаимодействие с внешними устройствами и другими программами, а также обеспечивающая диалог пользователя с ЭВМ. Ресурсом является любой компонент ЭВМ и предоставляемые им возможности: центральный процессор, оперативная и внешняя память, внешнее устройство, программа и т.д. ОС загружается в оперативную память при включении компьютера и предоставляет пользователю удобный способ общения (интерфейс) с вычислительной системой.

В локальную сеть на базе ОС **Windows** входят следующие элементы: общие ресурсы, серверы, рабочие станции, группы.

Общий ресурс – это объект (папка, диск, принтер и др.) который могут использовать несколько пользователей одновременно, причем им не обязательно находиться за тем компьютером, на котором физически расположен данный ресурс.

Рабочая станция – это компьютер, подключенный к сети и предназначенный для выполнения задач пользователя.

Сервер – это специализированный компьютер, предоставляющий свои ресурсы в использование клиентам сети (как правило, это рабочие станции) и управляющий сетью.

Рабочая группа – логическое объединение компьютеров. Как правило, объединение в группы используется для упрощения администрирования сети. При этом несколько компьютеров выступают как единое целое – группа.

На компьютере с ОС **Windows 2000** или **Windows XP** в общее пользование можно предоставить как любую папку на диске, так и диск целиком. После создания общего ресурса пользователи с соответствующими полномочиями могут получить доступ к нему с любой рабочей станции сети.

Открывая общий доступ к папке, можно ограничить число пользователей, которые могут работать с ней одновременно. Для управления доступом к папке и ее содержимому используются разрешения, назначаемые пользователям и группам. Эти разрешения, а также сетевое имя папки в любой момент можно изменить. При необходимости можно прекратить общий доступ к папке. Если к ней в это время подключены пользователи, на экране появится диалоговое окно с информацией об этом и предложением подтвердить принятое решение.

В **Windows 2000** и **Windows XP** предоставлять папки в общее пользование разрешается членам групп *Администраторы*, *Операторы сервера* и *Опытные пользователи*, причем с некоторыми ограничениями.

Общие ресурсы.

ОС Windows автоматически открывает общий доступ к некоторым ресурсам, необходимым для администрирования компьютера. К их сетевым именам добавляется значок доллара (**$**), благодаря которому административный общий ресурс скрыт от пользователей, просматривающих содержимое компьютера через сеть.

К числу административных ресурсов относятся: корневые папки каждого тома, корневая системная папка и папки, в которых находятся драйверы принтеров.

Открывая общий доступ к папке, обязательно нужно присвоить ей сетевое имя. Кроме того, при желании можно сопроводить папку описанием, ограничить число пользователей, которые могут пользоваться ею одновременно, и назначить для нее разрешения. Одну и ту же папку можно сделать общей под несколькими сетевыми именами.

Чтобы общий ресурс был доступен клиенту и в автономном режиме, то есть при отсутствии подключения к сети, **Windows 2000** или **Windows XP** может сохранить копии файлов ресурса в специальной области на локальном диске клиентского компьютера – кэше. По умолчанию размер кэша составляет 10 % от доступного дискового пространства, но его можно изменить с помощью вкладки **Автономные файлы** диалогового окна **Свойства папки**.

В **Windows XP** и **Windows 2000** входит оснастка **Общие папки**, позволяющая контролировать доступ к сетевым ресурсам и уведомлять пользователей посредством административных сообщений. Это возможность контролировать доступ к сетевым ресурсам для оценки и управления загруженностью сетевых серверов, а также доступ к общим папкам, чтобы определить, как много пользователей в данный момент подключены к каждой папке [3].

Возможности раздела **Общие ресурсы** в оснастке **Общие папки** позволяют просматривать список всех общих папок на компьютере и определять, сколько пользователей могут обращаться к каждой папке.

Кроме того, можно отслеживать, какие файлы открыты, а также отключать пользователей от одного открытого файла или от всех открытых файлов.

Если изменить разрешения файловой системы **NTFS** для файла, который в данный момент открыт пользователем, новые разрешения не будут действовать для этого пользователя, пока он не закроет файл и затем не откроет его.

Чтобы изменения вступили в силу немедленно, нужно выполнить одно из указанных далее действий:

– отключить всех пользователей от всех открытых файлов. Для этого в дереве консоли оснастки **Общие папки** открыть раздел **Открытые файлы** и в меню Действие активизировать пункт *Отключить все открытые файлы;*

– отключить всех пользователей от одного открытого файла. Для этого в дереве консоли оснастки **Общие папки** открыть раздел **Открытые**. В правой части окна указать открытый файл, а затем в меню Действие указать пункт *Закрыть открытый файл*.

Задания

Задание 1. Изучение структуры локальной сети.

1. Откройте папку Мое сетевое окружение.

2. Отобразите компьютеры рабочей группы.

3. Получите сведения о компьютере с именем Имя_Компьютера. Для этого воспользуйтесь командой контекстное_меню_компьютера/ Свойства.

В окне свойств будут перечислены параметры конкретного компьютера.

Задание 2. Получение доступа к папке из сети.

1. Включите запрос имени пользователя и пароля при доступе из сети:

- откройте диалоговое окно Свойства папки (Пуск/Панель управления/Свойства Папки);
- перейдите на вкладку Вид;
- сбросьте флажок Использовать простой общий доступ к файлам;
- подтвердите изменения кнопкой ОК.

2. Создайте на рабочем столе папку, дав ей имя со своей фамилией.

3. Откройте диалоговое окно свойств созданной вами папки (Контекстное меню папки/Свойства) и перейдите на вкладку Доступ.

4. Выберите Открыть общий доступ к этой папке.

5. Установите сетевое имя вашего ресурса. Для этого в поле Общий ресурс введите MyFolder.

В это поле вводится имя вашего ресурса, которое увидят пользователи сети. Это имя может отличаться от настоящего имени папки.

6. В поле Примечание введите текст, который описывает этот ресурс. Например, вы можете ввести Моя папка.

7. Установите Предельное число пользователей – 3.

Т.е. теперь к опубликованному ресурсу смогут подключаться одновременно только 3 пользователя.

8. Разрешите всем полный доступ к ресурсу:

- щелкните по кнопке Разрешения;
- выделите в верхнем поле группа Все;
- в нижнем поле установите флажок Полный доступ – разрешить;
- примените параметры кнопкой ОК.

9. Установите автоматическое кэширование документов:

- щелкните по кнопке Кэширование;
- выберите в списке Автоматическое кэширование программ и документов;
- примените параметры кнопкой ОК.

10. Завершите публикацию ресурса кнопкой ОК.

11. Просмотрите созданный сетевой ресурс с другого компьютера.

Задание 3. Создание скрытого административного ресурса.

1. Выполняйте действия из Задания 2 до установки сетевого имени.

2. Установите сетевое имя вашего ресурса. Для этого в поле Общий ресурс введите MyFolder2$.

Скрытый административный ресурс создается, как и обычный, путем добавления к сетевому имени ресурса знака - $. Например, если ваш ресурс будет называться MyFolder2, то для превращения его в скрытый необходимо ввести MyFolder2$.

3. Убедитесь в невидимости ресурса. Для этого на другом компьютере воспользуйтесь Сетевым окружением.

4. Перейдите к скрытому ресурсу. Для этого в адресной строке окна Сетевое окружение введите полный путь к опубликованному ресурсу в формате \\имя_компьютера\имя_ресурса$.

Например, \\l57c28pc1\MyFolder2$.

Задание 4. Открытие общего доступа к папке на удаленном компьютере.

1. Создайте на рабочем столе папку с именем RemoteFolder.

2. На основном компьютере запустите консоль с оснасткой Общие папки:

запустите Microsoft Management Console (Пуск/Выполнить/mmc);

– добавьте оснастку Общие папки: выполните команду меню Файл/Добавить удалить оснастку и щелкните по кнопке Добавить; выберите оснастку Общие папки и подтвердите выбор кнопкой Добавить;

– активизируйте другим компьютером и введите в поле имя удаленного компьютера;

– подтвердите кнопкой Готово;

– закройте окно Добавить изолированную оснастку кнопкой Закрыть;

– завершите добавление оснастки кнопкой ОК.

3. Разверните в левой части окна элемент Общие папки.

4. Для элемента Общие ресурсы выполните команду контекстное меню/ Новый общий ресурс.

5. Ознакомьтесь с описанием мастера создания общей папки и перейдите к следующему окну кнопкой Далее.

6. С помощью кнопки Обзор найдите на удаленном компьютере папку RemoteFolder.

7. Введите Имя общего ресурса в соответствующее поле - Удаленная папка и закройте окно кнопкой Далее.

8. Установите тип доступа к ресурсу – У всех пользователей доступ только для чтения и закройте окно кнопкой Далее.

9. Завершите создание общей папки кнопкой Готово.

Задание 5. Подключение удаленного ресурса в качестве локального диска.

Способ 1:

1. Используя Сетевое окружение, откройте папку виртуального компьютера.

2. Подключите в виде диска каталог RemoteFolder:

– выполните команду контекстного меню Подключить сетевой диск;

– выберите в списке букву диска, например Z;

– сбросьте флажок Восстанавливать при входе в систему;

– примените параметры кнопкой ОК.

3. Проверьте подключенный диск (Мой компьютер).

Способ 2:

1. Откройте окно Сетевые подключения.

2. Выполните команду Сервис/Подключить сетевой диск.

3. Щелкните по кнопке Обзор и перейдите в папку виртуального компьютера.

4. Примените параметры кнопкой ОК.

5. Выберите в списке Диск букву диска - Y.

6. Завершите подключение диска кнопкой Готово.

Способ 3:

1. Откройте командную строку.

2. Просмотрите параметры команды subst, для этого введите subst /?.

3. Подключите удаленный ресурс в качестве диска X: для этого введите команду в формате: subst X: \\имя_компьютера\имя_ресурса.

Лабораторная работа №5
Настройка стека протоколов TCP/IP

Цель работы: изучение способов диагностики настроек стека протоколов TCP/ IP; получение сведений о настройке TCP/IP для работы с DHCP сервером.

На концептуальной модели взаимодействия открытых систем OSI основан стек протоколов TCP/IP (Transmission Control Protocol – протокол управления передачей / Internet Protocol – Интернет-протокол), который предоставляет ряд стандартов для связи компьютеров и сетей.

Стек протоколов TCP/IP – промышленный стандарт, который позволяет организовать сеть масштаба предприятия и связывать компьютеры, работающие под управлением различных операционных систем [2].

Применение стека протоколов TCP/IP дает следующие преимущества:

– поддерживается почти всеми операционными системами; почти все большие сети основаны на TCP/IP;

– технология позволяет соединить разнородные системы;

– надежная, расширяемая интегрированная среда на основе модели «клиент-сервер»;

– получение доступа к ресурсам сети Интернет.

Каждый узел ***TCP/IP*** идентифицирован своим логическим IP-адресом, который идентифицирует положение компьютера в сети почти таким же способом, как номер дома идентифицирует дом на улице.

Реализация ***TCP/IP*** позволяет узлу ***TCP/IP*** использовать статический IP-адрес или получить IP-адрес автоматически с помощью ***DHCP-сервера*** (Dynamic Host Configuration Protocol – протокол динамической конфигурации хоста).

Для простых сетевых конфигураций, основанных на локальных сетях (LAN, Local Area Network), он поддерживает автоматическое назначение IP-адресов.

По умолчанию компьютеры клиентов, работающие под управлением ОС ***Windows*** или ***Linux***, получают информацию о настройке протокола ***TCP/IP*** автоматически от службы ***DHCP***.

Однако даже в том случае, если в сети доступен ***DHCP-сервер***, необходимо назначить статический IP-адрес для отдельных компьютеров в сети. Например, компьютеры с запущенной службой ***DHCP*** не могут быть клиентами ***DHCP***, поэтому они должны иметь статический IP-адрес.

Если служба ***DHCP*** недоступна, можно настроить ***TCP/IP*** для использования статического IP-адреса.

Для каждой платы сетевого адаптера в компьютере, которая использует ***TCP/IP***, можно установить IP-адрес, маску подсети и шлюз по умолчанию.

Ниже описаны параметры, которые используются при настройке статического адреса ***TCP/IP***.

Параметр	Описание
IP-адрес	Логический 32-битный адрес, который идентифицирует TCP/IP узел. Каждой плате сетевого адаптера в компьютере с запущенным протоколом TCP/IP необходим уникальный IP-адрес, такой, как 192.168.0.108. Каждый адрес имеет две части: ID сети, который идентифицирует все узлы в одной физической сети и ID узла, который идентифицирует узел в сети. В этом примере ID сети – 192.168.0, и ID узла – 108.
Маска подсети	Подсети делят большую сеть на множество физических сетей, соединенных маршрутизаторами. Маска подсети закрывает часть IP-адреса так, чтобы TCP/IP мог отличать ID сети от ID узла. При соединении узлов TCP/IP, маска подсети определяет, где находится узел получателя: в локальной или удаленной сети. Для связи в локальной сети компьютеры должны иметь одинаковую маску подсети.

Шлюз по умолчанию	Промежуточное устройство в локальной сети, на котором хранятся сетевые идентификаторы других сетей предприятия или Интернета. TCP/IP посылает пакеты в удаленную сеть через шлюз по умолчанию (если никакой другой маршрут не настроен), который затем пересылает пакеты другим шлюзам, пока пакет не достигнет шлюза, связанного с указанным адресатом.

Если сервер с запущенной службой DHCP доступен в сети, он автоматически предоставляет информацию о параметрах TCP/IP клиентам DHCP.

Задания

Задание 1. Проверка работоспособности стека протоколов TCP/IP.

1. Запустите консоль (Пуск/Программы/Стандартные/Командная строка).

2. В командной строке введите ipconfig /all | more.

3. Используя приведенную ниже информацию, создайте в своей папке текстовый документ со следующими данными:

– Имя компьютера;

– Основной DNS-суффикс;

– Описание DNS-суффикса для подключения;

– Физический адрес;

– DHCP включен;

– Автоконфигурация включена;

– IP-адрес автоконфигурации;

– Маска подсети;

– Шлюз по умолчанию.

4. Убедитесь в работоспособности стека TCP/IP, отправив эхо-запросы на IP-адреса. Для этого воспользуйтесь командой ping:

– отправьте эхо-запросы на локальный адрес компьютера (loopback) ping 127.0.0.1 (на экране должны появиться сообщения о полученном ответе от узла 127.0.0.1);

– отправьте эхо-запрос по другому IP-адресу, например 172.16.2.107.

Задание 2. Настройка стека протоколов TCP/IP для использования статического IP-адреса.

1. Откройте окно Сетевые подключения (Пуск/Панель управления/Сетевые подключения).

2. Вызовите свойства подключения по локальной сети. Для этого можно воспользоваться контекстным меню.

3. В появившемся диалоговом окне на вкладке Общие откройте свойства Протокол Интернета TCP/IP.

4. Щелкните переключатель Использовать следующий IP-адрес и введите в соответствующие поля данные: IP_адрес; Маску подсети; Основной шлюз; Предпочитаемый DNS.

5. Примените параметры кнопкой ОК.

6. Закройте окно свойств подключения кнопкой ОК (если потребуется, то согласитесь на перезагрузку компьютера).

7. Проверьте работоспособность стека протоколов TCP/IP.

Задание 3. Настройка TCP/IP для автоматического получения IP-адреса.

1. Откройте окно Сетевые подключения.

2. Вызовите свойства Подключения по локальной сети.

3. Откройте свойства Протокол Интернета TCP/IP.

4. Установите переключатель Получить IP-адрес автоматически.

5. Закройте диалоговое окно Свойства: Протокол Интернета TCP/IP кнопкой ОК.

6. Примените параметры кнопкой ОК.

7. Проверьте настройку стека протоколов TCP/IP.

8. Получите другой адрес для своего компьютера. Для этого:

– запустите консоль (командную строку);

– введите команду для сброса назначенных адресов - ipconfig /release;

– введите команду для получения нового адреса ipconfig / renew;

9. Проверьте работоспособность стека протоколов TCP/IP.

Задание 4. Создание IP-калькулятора в табличном процессоре для облегчения формирования маски подсети.

1. Откройте табличный процессор и сформируйте таблицу по следующему шаблону:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
1		1-й октет								2-й октет								3-й октет								4-й октет							
2	биты	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
3		ID-сети																													ID-узла		
4	IP- адрес	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
5	Десятичная запись	192								0								1								255							
6	Маска подсети	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
7	Десятичная запись	255								255								255								248							

Далее необходимо ввести в ячейки B5, J5, R5, Z5 формулы для перевода двоичного представления IP-адреса в точечную десятичную нотацию по октетам.

1. Введите в ячейку B5 формулу для преобразования 1-го октета IP-адреса в десятичную систему счисления:

=I4*2^I2+H4*2^H2+G4*2^G2+F4*2^F2+E4*2^E2+D4*2^D2+C4*2^C2+B4*2^B2

2. Скопируйте введенную формулу в остальные ячейки (J5, R5, Z5).

3. Самостоятельно введите в ячейки B7, J7, R7, Z7 формулы для преобразования маски подсети из двоичного представления в точечную десятичную нотацию.

Лабораторная работа №6

Настройка клиента службы DNS

Цель работы: получение навыков настройки клиентов службы DNS.

Система доменных имен (**Domain Name System, DNS**) строится на основе распределенной базы данных, используемой в сетях ***TCP/IP*** для преобразования имен компьютеров в IP-адреса. ***Служба DNS*** облегчает идентификацию компьютеров и других ресурсов в сетях. Она обычно ассоциируется с Интернетом. Однако частные сети активно используют ее для определения имен компьютеров и идентификации компьютеров в локальной сети и Интернете [3].

Пространство имен домена (***domain namespace***) – система имен, которая обеспечивает иерархическую структуру для базы данных ***DNS***. Каждый узел называется доменом (domain) и представляет раздел базы данных ***DNS***.

База данных DNS индексирована по имени, поэтому каждый домен должен иметь имя. Имя домена идентифицирует его положение в иерархии. Поскольку домены добавляются в иерархию, имя родительского домена добавляется к дочернему домену, называемому *субдоменом (subdomain)*.

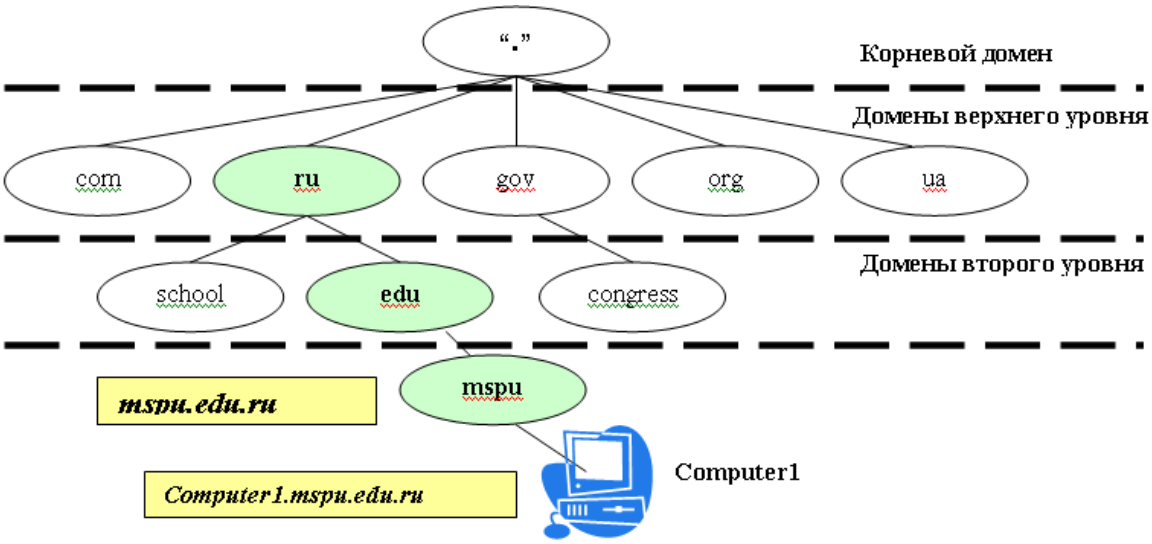

Рис. 2. Пример образования иерархии пространства имен домена

Например, на рисунке 2 имя домена **mspu.edu.ru** идентифицирует этот домен **mspu** как субдомен домена **edu.ru**, а **edu** – как субдомен домена **ru**.

Иерархическая структура пространства имен домена состоит из *корневого домена*, *доменов верхнего уровня*, *доменов второго уровня* и *имен узлов*. *Корневой домен* располагается на самом верху иерархии и обозначается точкой. Корневой

домен Интернета управляется несколькими организациями, включая **Network Solutions, Inc**. Домены верхнего уровня – коды имени длиной два или три символа. Домены верхнего уровня сгруппированы по типу организации или географическому положению. Например:

Домен верхнего уровня	**Описание принадлежности**
gov	Правительственные организации
com	Коммерческие организации
edu	Образовательные учреждения
org	Некоммерческие организации
ru	Код России

Домены верхнего уровня содержат домены второго уровня и имена узлов (компьютеров). Организации типа **Network Solutions, Inc.** назначают и регистрируют домены Интернета второго уровня для частных лиц и организаций. *Имя второго уровня* имеет две части: имя верхнего уровня и уникальное имя второго уровня. *Имена узлов* относятся к определенным компьютерам в Интернете или частной сети.

На рисунке 2 **Computer1** – это имя узла – левая часть полного доменного имени, которое определяет точное местонахождение узла в иерархии домена. Тогда полное доменное имя (включая последнюю точку) запишется как **Computer1.mspu.edu.ru**.

Чтобы преобразовать имя узла в IP-адрес, служба ***DNS*** использует полное доменное имя узла. *Разрешение имен* – процесс преобразования имен узлов в IP-адреса. Он напоминает поиск имени в телефонном справочнике, где каждому имени соответствует номер телефона. Например, имя **www.mspu.edu.ru** используется при соединении с Web-узлом Мурманского государственного педагогического университета. ***DNS*** находит соответствующий этому

(**www.mspu.edu.ru**) имени IP-адрес. Проекции имен на адреса IP хранятся в распределенной базе данных службы ***DNS***.

Серверы ***DNS*** осуществляют поиск соответствия в обе стороны. Прямой запрос преобразовывает имя в IP-адрес, а обратный запрос находит имя для IP-адреса. Сервер ***DNS*** имеет право делать запрос только для зоны, для которой он имеет полномочия. Если сервер ***DNS*** не может сделать запрос, он передает запрос на другие серверы имен, имеющие соответствующие полномочия.

Для разрешения имен служба ***DNS*** использует *модель «клиент-сервер»*. Чтобы осуществить прямой запрос соответствия, клиент передает запрос на локальный сервер имен. Локальный сервер ***DNS*** или обрабатывает и находит IP-адрес или делает запрос на разрешение имени на другой сервер имен.

На рисунке 3 показан клиент, запрашивающий IP-адрес для символьного адреса **www.mspu.edu.ru** с сервера имен.

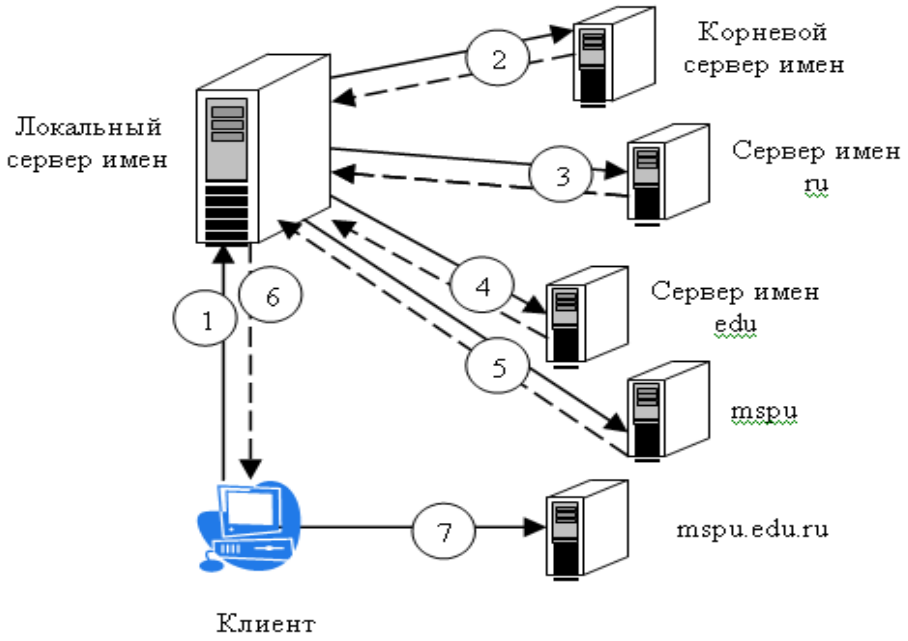

Рис. 3. Процесс разрешения адреса

Процесс строится следующим образом:

– клиент передает прямой запрос для **www.mspu.edu.ru** на свой локальный сервер имен;

– локальный сервер имен проверяет свои файлы данных зоны, чтобы определить, содержит ли тот проекцию имени на IP-адрес для запроса клиента и т.к. локальный сервер доменных имен не имеет полномочий для домена **mspu.edu.ru**, поэтому передает запрос на один из корневых серверов **DNS**, требуя разрешения имени узла, а корневой сервер доменных имен отправляет назад ссылку на серверы имен **ru**;

– локальный сервер имен посылает запрос на сервер имен **ru**, который отвечает ссылкой на серверы имен **edu**;

– локальный сервер имен посылает запрос на сервер имен **edu**, который отсылает клиенту ссылку на сервер имен **mspu**;

– локальный сервер имен посылает запрос на сервер имен **mspu** и, поскольку сервер имен **mspu** имеет полномочия для той части пространства имен домена, то при получении запроса отсылает адрес для **www.mspu.edu.ru** на локальный сервер имен;

– сервер имен отправляет IP-адрес для символьного адреса **www.mspu.edu.ru** клиенту и поскольку разрешение имени выполнено, то клиент может обратиться к адресу **www.mspu.edu.ru**;

– клиент обращается к символьному адресу **www.mspu.edu.ru**.

Задания

1. Откройте файл hosts (c:\WINDOWS\system32\drivers\etc\hosts).
2. Внесите в этот файл информацию, например: 127.0.0.1 FIO
3. Отправьте эхо-запрос на какой-нибудь компьютер по его символьному адресу (если будет получен ответ, то настройки верны), например: ping FIO

Содержание