Кировское областное государственное образовательное автономное
учреждение дополнительного профессионального образования
«Институт развития образования Кировской области»
(КОГОАУ ДПО «ИРО Кировской области»)

Создание локально-вычислительной сети в образовательной организации

Учебно-методическое пособие

Киров
2018

УДК 004.72
ББК 32.973.202
С-58

Автор-составитель: Скурихина Ю.А., старший преподаватель кафедры предметных областей КОГОАУ ДПО «ИРО Кировской области».
Авторы:
Скурихина Ю.А., старший преподаватель кафедры предметных областей КОГОАУ ДПО «ИРО Кировской области»: раздел 1, раздел 2, раздел 3 (глава 1)
Ярославцев В.Л., заместитель директора по УВР, учитель информатики МКОУ СОШ № 7 г. Слободского: раздел 3 (глава 1)

Рецензенты:
Чупраков Н.И., преподаватель кафедры предметных областей КОГОАУ ДПО «ИРО Кировской области»
Смирнов П.А., заместитель директора по УВР МОАУ «Лицей информационных технологий №28» г. Кирова

С-58 Создание локально-вычислительной сети в образовательной организации. – Киров: КОГОАУ ДПО «ИРО Кировской области». – 2018. – 99 с.

Учебно-методическое пособие посвящено рассмотрению теоретических аспектов проектирования компьютерной сети, вопросам администрирования локальной сети, включает методические рекомендации по созданию и администрированию локальной сети образовательной организации. Пособие адресовано учителям информатики, техническим специалистам, заместителям руководителя образовательной организации.

Оглавление

Введение

В настоящее время компьютерные сети стали неотъемлемой частью нашей повседневной жизни. Они используются как в производственной деятельности для обеспечения доступа к единой базе данных и создания единой автоматизированной системы управления, так и для объединения домашних компьютеров в целях развлечения.

В образовательных организациях локальная сеть решает множество разных задач: обеспечение доступа к электронному журналу, управление документооборотом, предоставление общего доступа к документам, обеспечение возможности общения.

Именно поэтому вопросы создания и администрирования локальной сети образовательной организации являются такими актуальными. Локальная вычислительная сеть в настоящее время создана только в половине образовательных организаций, еще в четверти организаций в локальную сеть включены только компьютеры компьютерного класса. Данное учебно-методическое пособие посвящено рассмотрению теоретических аспектов проектирования компьютерной сети, вопросам администрирования локальной сети, а также содержит методические рекомендации по созданию и администрированию локальной сети образовательной организации.

Институтом развития образования был проведен вебинар «Создание локальной сети организации», запись которого доступна по ссылке : https://youtu.be/GoYSngnzU6M

РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОЕКТИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Глава 1. Компьютерные сети: основные понятия и классификации

Компьютерная сеть – набор компьютеров, соединенных коммуникационными средствами, при помощи которых компьютеры могут обмениваться данными и услугами.

Самая простая компьютерная сеть состоит из двух компьютеров. Объединение компьютеров позволяет им использовать данные и вычислительные мощности совместно. Именно эта идея лежит в основе любой компьютерной сети.

Идея соединения компьютеров с помощью кабеля в свое время явилась значительным достижением в области информационных технологий. Она возникла как ответ на потребность иметь возможность совместного использования и обработки данных. Компьютеры, объединенные в сеть, могут совместно использовать файлы, базы данных, другие данные, принтеры, факсимильные аппараты, модемы и другие устройства.

Развитие компьютерных сетей началось с появления модели ц**ентрализованных вычислений**. Такая модель предполагает расположение всех данных и вычислительных мощностей на центральном устройстве - мейнфреймаме (mainframe). А пользователи соединяются с мейнфреймом через индивидуальные устройства, называемые терминалами (terminals), которые состоят из устройства ввода и устройства передачи данных на мейнфрейм. Сам по себе один мейнфрейм с терминалами еще не является полноценной компьютерной сетью, т.к. нет полноценного обмена данными и услугами.

На следующем этапе формируются сети передачи данных, объединяющие между собой мейнфреймы для реализации распределенных баз данных и децентрализации процессов обработки информации.

С появлением ПК на первый план выходит проблема объединения в сеть ПК для обмена данными, совместного использования баз данных и дорогостоящего оборудования и появляется модель **распределенных вычислений**. В такой модели каждое устройство обладает своей вычислительной мощностью и выполняет свои задачи независимо от других устройств. Однако каждый ПК в такой сети выполняет задание независимо друг от друга.

Однако с развитием ВТ происходит усложнение задач, решаемых с использованием компьютеров. Поэтому возникает необходимость распределять одно задание между несколькими устройствами, которые должны координировать действия друг друга. Такая модель называется

моделью **коллективных вычислений**. В этом случае задание распределяется между устройствами более эффективным способом.

В настоящее время компьютерные сети получили широкое распространение. Они используются как в огромных корпорациях для организации единой автоматизированной системы управления, так и в небольших компаниях для обеспечения доступа к единой базе данных, а также для создания домашних , городских и глобальных развлекательных сетей.

1.1 Виды сетей в зависимости от охватываемого расстояния

Выделяют следующие виды сетей в зависимости от охватываемого расстояния:

- персональные сети (PAN – personal area network);
- локальные сети (LAN – local area network);
- городские сети (MAN – metropolian area network);
- глобальные сети (WAN – wide area network).

Персональные сети (PAN) позволяют подключить к персональному компьютеру различные устройства, такие как КПК, сотовый телефон, ноутбук. Чаще всего для подключения используется инфракрасное излучение или технология BlueTuth, хотя возможно использование кабеля.

Локальные сети (LAN) имеют относительно малый размер. Как правило, такие сети используют только одну среду для передачи данных, например один вид кабеля. Размер таких сетей не превышает 10 километров и обычно такие сети заключены в пределах одного здания. Примером локальной сети может служить сеть, организованная в компьютерном классе.

Городские сети (MAN) занимают уже пространство от нескольких десятков до ста километров и находятся обычно в пределах города. В таких сетях используется уже различное оборудование и различные среды передачи данных, что связано с большим удалением структур сети друг от друга. В настоящее время распространены как городские сети предприятий и организаций, так и сети, объединяющие домашние компьютеры (для обмена играми, музыкой и фильмами).

Глобальные сети (WAN) обычно связывают локальные сети, которые могут находиться на очень большом расстоянии, например на разных континентах или в разных местах одного государства.

Глобальные сети в свою очередь подразделяются на корпоративные (Enterprise) и истинно глобальные сети (Global). Корпоративные сети принадлежат какой-то одной организации, и связывают филиалы или удаленные подразделения, находящиеся в разных городах или странах. Истинно глобальные сети связывают множество локальных сетей разных организаций и отдельные ПК между собой. Самым ярким примером истинно глобальной сети является сеть Интернет.

1.2 Одноранговые и клиент-серверные сети

В зависимости от структуры выделяют два вида сетей:

- на основе сервера (Server based, client/server)
- одноранговые (peer-to-peer)

Члены **одноранговой** сети могут быть и потребителями и поставщиками услуг одновременно. Установленное на каждом из компьютеров одноранговой сети ПО как правило предоставляет одинаковый комплекс услуг. Ни один компьютер не имеет ни высшего приоритета на доступ, ни повышенной ответственности за предоставление ресурсов в совместное использование. Чаще всего в таких сетях находится не более 10 компьютеров. Такие сети дешевы, так как не имеют выделенного сервера. Пользователи сами выступают в роли сетевых администраторов и обеспечивают защиту информации. Каждый пользователь может дать всем остальным неограниченный доступ к локальным ресурсам, дать ограниченный доступ, а может не дать вообще никакого доступа. При большом количестве клиентов такой сетью трудно управлять. Самая основная проблема в такой сети – безопасность. Здесь нет средств обеспечения безопасности в масштабах сети. Этот тип сети будет хорошо работать в маленьких сетях. Производительность сети может упасть, когда много пользователей попытаются одновременно получить доступ к ресурсам какого-то одного компьютера. К тому же пользователь, работающий на этом компьютере, будет ощущать падение производительности, когда другие пользователи будут использовать ресурсы этого компьютера.

В сетях **на основе сервера** существует выделенный сервер, предоставляющий услуги. Он имеет специализированное аппаратное и программное оснащение и специально рассчитан на исполнение большого количества запросов клиентов. Важное отличие от одноранговых сетей состоит в повышении безопасности. Здесь существует централизованная проверка учетных записей пользователей, их прав и паролей. Прежде чем получить доступ к любому ресурсу, пользователь должен сообщить центральному серверу (его называют контроллером домена, domain controller) свое имя и пароль. Ключевым моментом безопасности такой сети является физическое ограничение доступа к серверу. Специальный человек – администратор – формирует единую политику безопасности сети. Общие файлы как правило хранятся в одном месте, что упрощает их резервирование. Такие сети также лучше масштабируются и могут обслуживать от единиц до десятка тысяч пользователей.

1.3 Топологии сети

В сети выделяют физическую структуру среды передачи данных и называют ее физической топологией. Существуют следующие виды топологий: шина, кольцо, звезда, сетка, сотовая.

1) Топология шина (bus)

Физическая топология шина как правило использует один длинный кабель, называемый магистралью. В разрыв магистрали могут быть присоединены отводки, которые подводятся к компьютерам. Второй вариант - компьютеры напрямую подсоединяются к магистрали используя Т-соединитель. Чтобы предотвратить отражения сигнала, на концах магистрали должны быть установлены терминаторы. Обычно сигналы передаются от устройства в двух направлениях.

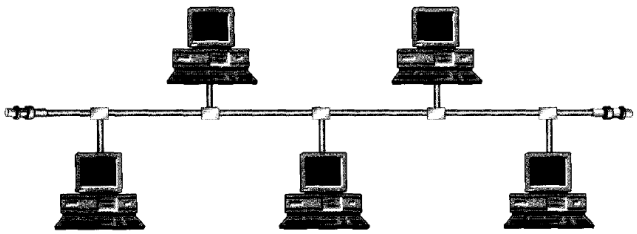

Рисунок 1.1. Топология «шина»

Шинную топологию сравнительно несложно устанавливать. Так как шинная топология опирается на минимизацию расхода кабеля и в силу существующих ограничений на минимальное расстояние между разъемами изменение конфигурации шинной топологии трудоемко.

Для нахождения неисправности необходимо обнаружить и изолировать неисправный сегмент. Поскольку шинная топология базируется на одном сегменте – магистрали, задача сильно усложняется.

Неисправность магистрали приводит к полному отказу сети по двум причинам: во-первых при разрыве кабеля сигнал отражается от места разрыва и создает помехи и во-вторых сеть разделяется на два сегмента и компьютеры уже не могут передавать информацию в другой сегмент.

2) Топология кольцо (ring)

Данная топология основывается на кольце. Каждое устройство либо напрямую входит в кольцо, либо подсоединяется к нему через отводок.

Обычно электрические сигналы передаются от одного устройства к другому в одном направлении. На устройстве происходит регенерация принятого сигнала.

Начальная установка кольца достаточно проста. Но кольцевая топология требует большего расхода кабеля в отличие от шинной. По мере роста узлов кольца, конфигурацию становится все труднее изменять, т.к. существуют ограничения как на максимальную длину кольца так и на максимальное число подключенных устройств.

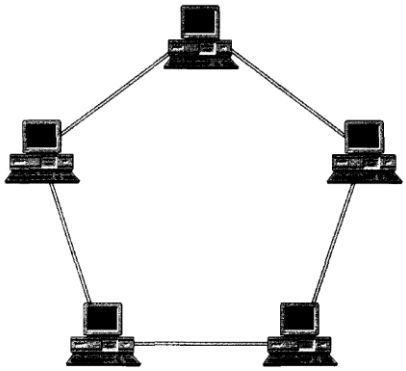

Рисунок 1.2. Топология «кольцо»

Так как в каждом подключенном устройстве находится повторитель (repeater), можно легко найти сбойный участок кабеля, так как следующее за сбойным участком устройство не будет получать сигнал и сможет сигнализировать об ошибке.

Большинство сетей используют одно кольцо. Отказ устройства в таком кольце приводит к неработоспособности всей сети. Однако в двойном кольце при повреждении кабель связь может идти по второму кольцу, что повышает отказоустойчивость сети.

3) Топология звезда (star)

В топологии звезда сетевые устройства подключаются к центральному устройству (концентратору) через отдельные сегменты кабеля.

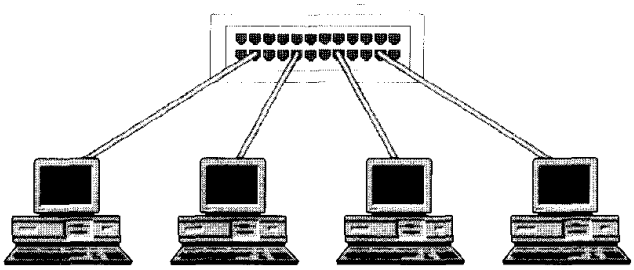

Рисунок 1.3. Топология «звезда»

В топологии звезда электрический сигнал передается по сегменту кабеля от сетевого устройства к концентратору. Далее концентратор пересылает сигнал другим сетевым устройствам. Концентратор может передавать пакет на все остальные сегменты (активный концентратор) или только на сегмент получателя (интеллектуальный концентратор).

Топология звезда отличается средней сложностью установки, зато конфигурацию сети звездообразной топологии можно легко изменять. Для добавления устройства достаточно добавить сегмент кабеля к концентратору.

Так как все данные проходят через центральное устройство, можно легко обнаружить и изолировать неисправный участок.

Топология «звезда» отличается хорошей отказоустойчивостью. При возникновении ошибки в сети можно легко найти и изолировать неисправный сегмент с помощью концентратора.

4) Топология «сетка» (полносвязная топология)

При использовании топологии «сетка» каждое устройство сети осуществляет соединение с каждым устройством.

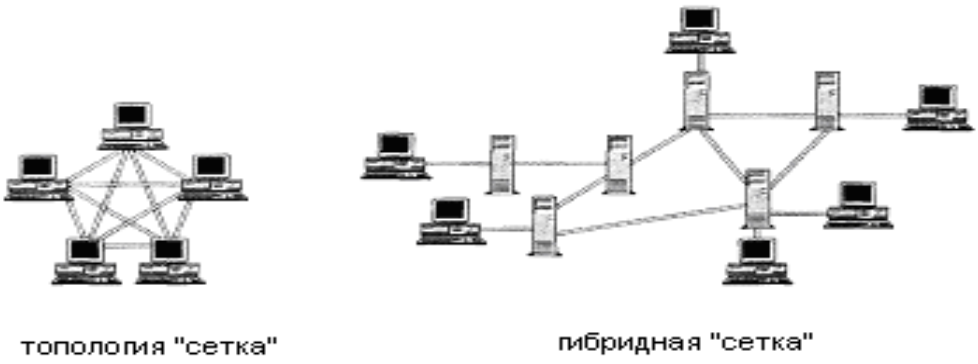

Рисунок 1.4. Топология «сетка»

Такая сеть редко используется на практике (если устройство не общается сразу со всеми остальными устройствами, большая часть пропускной способности такой сети теряется). Однако такая структура сети отличается высокой отказоустойчивостью и всегда может гарантировать определенную пропускную способность между двумя устройствами, поэтому в реальной жизни встречается топология «гибридная сетка», которая связывает между собой сервера нескольких локальных сетей, компьютеры которых образуют другую топологию (например, звезда).

Топологию сетка сложно устанавливать, так как нужно соединить каждое устройство с каждым. Изменение конфигурации сети с топологией «сетка» также является трудоемким по тем же причинам.

В такой топологии сравнительно просто найти и изолировать неисправный сегмент, так как все сегменты являются независимыми.

Сети на основе топологии сетка отличаются высокой отказоустойчивостью, так как существует несколько вариантов прохождения сигнала от устройства к устройству.

5) Сотовая топология (cellular)

При использовании сотовой топологии применяются беспроводные соединения. Пространство физически разделяется на соты (cells). Устройства, находящиеся в пределах соты, связываются с центральным устройством или концентратором. Концентраторы связаны между собой и образуют сетевую инфраструктуру.

Сложность установки сети на основе сотовой топологии зависит от сложности установки концентраторов. Беспроводные сети не требуют изменения конфигурации при добавлении или перемещении пользователя внутри области действия сети. Пользователь может работать в зоне действия любого концентратора.

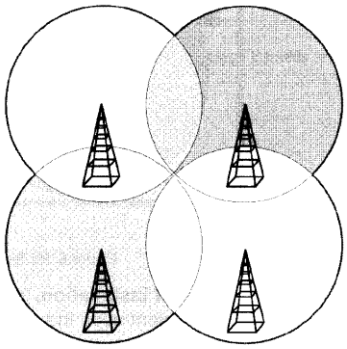

Рисунок 1.5. Топология «сотовая»

Найти неисправность в клиентском устройстве достаточно просто, так как каждый концентратор производит независимую связь с устройством пользователя. При неисправности концентратора, связь теряют все устройства в его зоне действия. Но возможно временное перемещение устройства в зону действия другого концентратора.

Глава 2. Обеспечение компьютерных сетей

Для функционирование компьютерной сети необходимо наличие следующих элементов:

- информационное обеспечение
- программное обеспечение
- техническое обеспечение

2.1 Информационное обеспечение компьютерных сетей

Информационное обеспечение компьютерной сети – это весь объем информации, доступной для совместного использования.

Эта информация может быть представлена в виде:

- отдельных файлов (текстовых, графических, аудио и видео файлов);
- фактографических баз данных
- хранилищ документальных данных
- хранилищ гипертекстовых документов

2.2 Программное обеспечение компьютерных сетей. Сетевые службы

К программному обеспечению относятся сетевые средства и службы. Специальные программы, называемые сетевыми приложениями, позволяют программам пользователя использовать услуги сети. Сетевые приложения выполняются «прозрачно» для пользователя, т.е. пользователь не видит непосредственно их работу. Сетевые приложения обычно входят в состав сетевой операционной системы (NOS – networking operating system), хотя некоторые такие приложения интегрированы и в состав обычных операционных систем. Сетевые операционные системы специально разработаны чтобы координировать и поставлять различные сетевые услуги пользовательским приложениям. Если обычная операционная система находится на одном компьютере, то сетевая операционная система может быть распределена по многим компьютерам, входящим в сеть.

Самыми распространенными являются следующие сетевые службы:

- Файловые службы
- Службы печати
- Службы передачи сообщений
- Средства приложений
- Средства баз данных.

1) Файловые службы

Файловые службы – одни из важнейших сетевых служб, так как они позволяют создать эффективное хранение информации и обеспечить доступ к информации.

Файловые службы производят следующие операции:

1. Передача файлов;

До широкого использования компьютерных сетей пользователям приходилось передавать файлы друг другу вручную, используя любой подходящий носитель. Этот путь передачи информации является очень медленным и дорогим – работник тратит свое время на перенос информации.

Служба передачи файлов использует сетевые услуги по получению, записи или переносу файлов от клиента.

Службами передачи файлов можно легко пользоваться независимо от размера файла, удаленности источника и даже от операционной системы источника. Использование файловых служб позволяет повысить эффективность работы организации, а также облегчить доступ сотрудникам к информации.

Так как файловые службы работают с информацией, они предоставляют средства ограничения прав доступа к файлам. Эти средства включают и ограничение доступа по пользователям, и шифрование данных.

2. Хранение и перемещение данных;

В последнее время объемы обрабатываемой информации существенно возросли, что привело к появлению трех типов сетевых устройств хранения данных.

1) Оперативно доступные (online storage) устройства хранения данных обеспечивают немедленный доступ к хранимой информации без вмешательства человека. Например, жесткий диск.

2) Автономные (offline storage) – это устройства хранения данных, которые требуют вмешательства человека для получения информации. Например, дискета, оптический диск.

3) Полуавтономные устройства (nearline storage), занимающие промежуточное положение не являются оперативно доступными для компьютера (требуют определенного времени на доступ к информации), но им не нужно человеческое вмешательство. Например, магазин компакт-дисков.

Данные, к которым пользователи обращаются редко, можно перенести с дорогих жестких дисков на более дешевые автономные устройства (в расчете на единицу информации). Такой процесс переноса информации называется миграцией данных

3. Синхронизация изменений файлов;

Если в организации используются мобильные компьютеры, то они на какое-то время могут терять связь с файловым сервером. Обычно пользователи хранят в таких случаях копии необходимых файлов на своем локальном диске. Однако если в на файловом сервере произойдет изменение информации, то файлы на локальном компьютере окажутся устаревшими. Для урегулирования таких ситуаций и служит служба синхронизации изменений файлов. Как правило, служба сравнивает размер и дату последнего изменения файла и автоматически замещает старые файлы более

новыми версиями. Эта служба также может отследить кто и когда вносил изменения в файл.

В случае, если и локальная копия файла, и копия на файл-сервере были изменены, то служба синхронизации может либо совместить изменения в обоих файлах, либо обратиться к администратору для разрешения конфликта

4. Архивация файлов.

Для предотвращения утери важной информации используют резервное копирование файлов. Для уменьшения объема резервной копии, выполняют ее архивирование.

Компьютерная сеть позволяет сделать операцию резервного копирования централизованной. Сейчас существует большое количество сетевых приложений, реализующих службу архивации автоматически.

2) Службы печати

Службы печати включают в себя сетевые приложения, которые управляют доступом к принтерам и факсам. В их задачу входит принятие запроса к принтеру, перевод данных в язык, понятный принтеру, управление очередью печати принтера, и печать на сетевой принтер или факс.

Сетевая служба печати производит следующие операции:

1. обеспечивает доступ к принтерам большому числу пользователей;
2. устраняет ограничения по расстоянию;
3. управляет очередью печати;
4. обеспечивает общий доступ к специализированному оборудованию;
5. также существует специальная служба сетевого факса.

Если бы не существовало очереди печати, то служба печати выполняла бы первое пришедшее задание клиента. Остальным клиентам пришлось бы ждать пока служба печати не освободится. Для решение этой проблемы существует очередь печати (print queue). Если принтер уже занят одним клиентом, то служба печати примет задание от другого клиента и поместит его в очередь. После завершения первого задания на принтер будет послано следующее задание из очереди. Служба печати также поддерживает управление очередью – можно устанавливать приоритеты на задания, можно «замораживать» и удалять задания из очереди.

При использовании очереди печати, приложение отсылает задание на сервер печати и не ждет непосредственной распечатки задания. Процесс печати сервер полностью берет на себя, а пользовательское приложение может выполнять другие задачи. Очередь печати повышает эффективность работы в сети.

Использование службы сетевого факса становится все более и более популярной. Обычная факс-машина сочетает в себе технологии модема, сканера и принтера чтобы превратить изображение в цифровой вид и отослать получателю. Сетевой факс добавляет технологии компьютерной сети, что позволяет экономить ресурсы организации.

3) Службы передачи сообщений

Службы передачи сообщений обеспечивают хранение, доставку сообщений и доступ к ним. Сообщение может содержать любые виды информации: текстовую, графическую, видео- и аудиоинформацию. Важно, что службы передачи сообщений не просто передают данные, а информируют приложение пользователя или самого пользователя о поступившем сообщении.

Сетевые приложения, входящие в службы передачи сообщений, можно разделить на пять основных групп:

1. Электронная почта (e-mail);

Электронная почта – одна из самых используемых и популярных служб в сети. Под электронной почтой понимают передачу сообщений между двумя или более компьютерами. Изначально сообщения электронной почты содержали только текст, но сейчас в сообщение можно включать практически любой вид информации. Поэтому, приложения электронной почты должны иметь не только средства доставки сообщений, но и средства воспроизведения различных видов информации. Службы электронной почты обязаны отслеживать перемещение адресатов в сети чтобы правильно доставлять сообщения

2. Голосовая почта;

Голосовая почта – это служба передачи голоса, использующая специальное программное и аппаратное обеспечение. Она может быть интегрирована в электронную почту. Например, специальный сервер принимает входящие телефонные звонки, записывает их и передает через сообщения электронной почты.

Сейчас существует множество решений для передачи голоса по компьютерной сети, и ведутся исследований в этой области. Одно из возможных применений – это IP-телефония, то есть организация одной сети как для передачи компьютерной информации, так и для телефонных переговоров.

3. Службы поддержки объектно-ориентированных приложений;

Обьектно-ориентированные приложения – это компьютерные программы, которые для выполнения сложных задач используют более мелкие приложения (объекты), выполняющие простые задачи.

Службы передачи сообщений передают информацию от одного такого объекта к другому в компьютерной сети. Объект не выполняет задачи поиска другого объекта и передачи информации, он передает эти обязанности на службу передачи сообщений.

4. Специализированное ПО документооборота;

Приложения по управлению документооборотом выполняют работу по маршрутизации документов среди клиентов сети. При введении компьютерной системы управления предприятием службы управления документооборотом играют немаловажную роль. Процессы обработки и передачи информации происходят намного быстрее и эффективнее.

5. Служба каталога.

Служба каталога не относится напрямую к службам доставки сообщений. Она поддерживает единый источник информации о пользователях, компьютерах и ресурсах в сети, называемый каталогом (directory). Служба каталога постоянно отслеживает местоположение пользователей и ресурсов в компьютерной сети. Каталог широко используется приложениями и пользователями для быстрого поиска ресурсов.

4) Средства приложений

Средства приложений могут запускать программы на компьютере по требованию клиентов сети. Эти службы отличны от файловых служб, так как идет не только обмен информацией, но и предоставление вычислительных мощностей другому компьютеру.

Средства приложений обеспечивают следующие функции:

- координируют работу аппаратного и программного обеспечения по запуску необходимых приложений на наиболее подходящем ресурсе;
- увеличивают вычислительную мощность без модернизации отдельных компьютеров.

Эти средства используются в тех случаях, когда для работы используется программное обеспечение, требующее больших вычислительных затрат (большой объем памяти, мощный процессор), а у организации нет возможности закупить дорогое оборудование для каждой рабочей станции. Тогда закупается один мощный компьютер – сервер приложений, на который устанавливается программное обеспечение, а все остальные устройства (клиенты) передают свои данные серверу, запускают программу для обработки этих данных и получают результаты. Если необходимо модернизировать такую сеть, то достаточно заменить (или усовершенствовать) сервер приложений или установить новое программное обеспечение только на центральном компьютере.

5) Средства баз данных

Средства баз данных предусматривают централизованное хранение данных, их поиск и передачу клиентам сети. Существует специальный термин – СУБД – система управления базами данных, который характеризует такие взаимодействия (client-server database). Обычно задание разделяется между СУБД и приложением пользователя. Как правило, приложение пользователя подготавливает запрос и обрабатывает ответ, а СУБД обслуживает запрос и возвращает требуемые данные.

Существует два варианта организации единой базы данных:

1. Распределенная база данных

В больших организациях существует несколько отделов. Каждый отдел работает со своей частью базы данных, хранящейся в пределах локальной сети. СУБД должна представлять такую распределенную базу как единое целое и своевременно отражать изменения, производимые в отдельных частях базы.

2. Централизованная база данных

В организации существует единая база данных, с которой работают все пользователи, используя сеть. Однако работа с небольшой локальной базой происходит обычно быстрее чем с удаленным сервером. Поэтому пользователи иногда предпочитают использовать локальные копии общей базы данных.

В такой ситуации существует опасность использования устаревших данных. Важно, чтобы данные во всех базах своевременно синхронизировались. Такой процесс называется тиражированием.

Существует два вида тиражирования:

1). В сети есть только одна (центральная) база данных, в которую можно вносить изменения и дополнения. СУБД в таком случае несет ответственность за запись изменения в основную базу данных и своевременное тиражирование главной базы на другие копии.

2). При использовании второго способа локальные базы несут ответственность за изменения и дополнения, и уже локальные части СУБД тиражируют изменения на другие копии базы данных.

При разработке сети следует не только выбрать требуемые сетевые службы, но и определить, будут они централизованными, распределенными или сочетать в себе оба этих качества. Сетевые службы могут быть на одном или на небольшой группе компьютеров или распределены между всеми компьютерами сети.

Глава 3. Техническое обеспечение компьютерной сети.

Технические средства компьютерных сетей включают в себя следующие группы оборудования:

– средства линий передачи данных (кабель)

– средства организации беспроводной связи

– соединительное оборудование

Носитель - это среда, по которой происходит передача информации. Для передачи информации компьютеры используют электромагнитные (ЭМ) волны, которые могут быть разной частоты – от низкочастотных ЭМ волн вплоть до гамма-лучей.

Носители для передачи данных можно разделить на две категории – ограниченные (кабельные) и неограниченные (беспроводные).

При выборе носителя следует учитывать следующие факторы:

- стоимость носителя
- простоту установки
- пропускную способность
- величину затухания сигнала
- величину электромагнитных помех.

Под *пропускной способностью* понимают среднее количество переданных бит в секунду, или bps (bits per second).

Затуханием (attenuation) называют свойство ЭМ волн искажаться или ослабляться при передаче. При прохождении волны через какую-либо среду, некоторая часть ее энергии поглощается или рассеивается. Затухание достаточно легко измерить, поэтому эта величина лежит в основе таких характеристик носителей, как максимальная дальность сегмента сети.

3.1 Ограниченные носители

В ограниченных носителях для передачи сигнала используют кабель. Кабель – это провод или волокно, которые проводят такие виды ЭМ волн как электрический ток или свет. Самыми распространенными кабелями являются

- витая пара (twisted pair)
- коаксиальный кабель (coaxial cable)
- волоконно-оптический кабель (fiber-optic cable).

1) Витая пара

В кабеле, который называют витой парой, использует медные проводники так как медь является очень хорошим проводником. Два изолированных медных провода перевивают вокруг друг друга, что позволяет уменьшить как перекрестные помехи, так и внешние ЭМ помехи. В одном кабеле типа «витая пара» может быть от одной до нескольких таких пар. Витую пару разделяют на два вида:

- экранированная витая пара (STP)

- неэкранированная витая пара (UTP).

Неэкранированная витая пара представляет собой несколько переплетенных медных пар, заключенных в общий пластиковый кожух. Такой вид кабеля повсеместно используется в американских телефонных сетях.

Стоимость UTP невелика по сравнению с остальными видами кабелей.

Установка UTP как правило не сложная и может производиться уже после небольшой тренировки. Кабель UTP легко перемещать и изменять его конфигурацию.

Пропускная способность. UTP имеет пропускную способность от 1 до более 1000 Мбит/с на расстояниях до 100 м. Наиболее используется 100 Мбит/с.

Как и любой медный проводник, кабель витой пары сильно подвержен **затуханию** сигнала. Поэтому эффективная длина сегмента не превышает 100 м (10BaseT,100BaseTX/T4,1000BaseT).

Медные проводники очень чувствительны к **внешним ЭМ воздействиям**. Электрический сигнал, проходящий по витой паре можно легко перехватить и прослушать с помощью специальных устройств. Витая пара не подходит для использования в помещениях с сильными электромагнитными помехами.

Экранированная витая пара используется более редко неэкранированной. Кабель STP содержит несколько пар медных проводников, которые обернуты фольгой и заключены в пластиковый кожух.

2) Коаксиальный кабель

В центре коаксиального кабеля находится либо цельный либо переплетенный медный проводник, окруженный пластиковой вспененной изоляцией. Следующим слоем является второй проводник - проволочная медная оплетка, иногда еще окруженная слоем фольги. Цель этого слоя – защищать кабель от ЭМ помех. И последний слой – жесткое пластиковое покрытие.

Коаксиальный кабель чаще всего прокладывается от одного устройства к другому.

Стоимость коаксиального кабеля зависит от его диаметра и используемых соединителей. Стоимость «тонкого» коаксиального кабеля равна стоимости UTP 5 категории. Стоимость же «толстого» кабеля выше и находится в средней ценовой категории.

Начальная **установка** коаксиального кабеля достаточно проста. Однако его достаточно сложно проверять и диагностировать. С «толстым» Ethernet работать проще, так как он связан с компьютером специальным кабелем.

Теоретически **пропускная способность** коаксиального кабеля выше, чем у витой пары. Однако существующие сейчас технологии используют скорость передачи всего 10 Мбит/с (10Base2/5).

Так как коаксиальный кабель изготавливается из медного проводника, он имеет достаточно большой **коэффициент затухания**.

Для сегмента «тонкого» Ethernet максимальная длина одного сегмента составляет 185 м. Этот вид Ethernet соответствует спецификации 10Base2.

Для сегмента «толстого» Ethernet максимальная длина одного сегмента составляет 500 м. Однако такой кабель имеет более высокую стоимость. Толстый коаксиальный кабель иногда используют в качестве основного магистрального кабеля для соединения нескольких небольших сетей, построенных на тонком коаксиальном кабеле. Этот вид Ethernet соответствует спецификации 10Base5.

Коаксиальный кабель имеет более высокую **устойчивость к электромагнитным помехам** чем витая пара. Сейчас обычно используется при прокладке линий кабельного телевидения.

3) Волоконно-оптический кабель

Этот вид кабеля состоит из светопроводящего пластикового или стеклянного волокна, окруженного светопроводящей средой с более высокой оптической плотностью, и защитным кожухом. По центральному волокну проходят световые кванты, а роль прозрачного кожуха сводится к отражению света от границы раздела центрального волокна и прозрачного кожуха, что достигается благодаря эффекту полного внутреннего отражения.

Оптическое волокно имеет меньший размер и вес, чем медный проводник, что удобно при условии ограниченности места для прокладки кабеля.

Также волоконно-оптический кабель различают по двум режимам: **одномодовый** и **многомодовый**. В одномодовом кабеле свет может идти только по одному пути в волокне. В многомодовых кабелях таких путей может быть много. Это затрудняет процесс передачи, так как оптическая плотность волокна неодинакова и световые кванты, проходя по разным путям, могут прийти раньше или позже соседних квантов или слиться в один импульс с соседними квантами. Одномодовые кабели обеспечивают более высокую скорость передачи, однако стоимость их выше.

В компьютерных сетях устройства, использующие волоконно-оптический кабель, содержат два интерфейса – входящий и исходящий. Соответственно к каждому устройству нужно подводить два волоконно-оптических кабеля через специальные соединители.

Для передачи данных по ВО кабелю конечные устройства преобразовывают электрические сигналы в световые кванты и обратно.

Оптическое волокно имеет более высокую **стоимость** по сравнению с медным проводником. В последнее время намечается тенденция удешевления ВО кабеля. Стоимость установки и настройки кабеля также очень высока.

Оптический кабель очень трудно **устанавливать**, так как по пути следования света не должно быть помех. Поэтому обжимку кабеля или склеивание нужно проводить очень осторожно. Также нужно избегать излишнего скручивания или излома кабеля.

Пропускная способность ВО кабеля очень высока. Современные технологии позволяют передавать данные со скоростями от 100 Мбит/с до 200 Гбит/с.

У ВО кабеля очень низкий **коэффициент затухания**. Его величина зависит от частоты передаваемой волны, но она намного ниже медного проводника. Допустимая длина одного сегмента обычно находится в интервале от 2 до 25 км.

Свет не покидает пределы оболочки ВО кабеля, поэтому прослушивать ВО кабель практически невозможно. ЭМ поля слабо влияют на передачу светового потока, поэтому ВО кабель почти не подвержен ЭМ помехам.

Выбор кабеля

Перед выбором типа кабеля следует проанализировать проект сети по следующим параметрам:

1. Интенсивность сетевого траффика (объем передаваемой информации)
2. Требования к защите от прослушивания
3. Максимальная длина одного сегмента
4. Требуемые характеристики кабеля
5. Наличие денежных средств

Также следует прогнозировать развитие компьютерной сети.

3.2 Неограниченные носители.

Неограниченный носитель может передавать сигналы без использования кабеля. Для передачи сигнала используются волны различной частоты. Их разделяют на три диапазона:

- Radio (радиоволны);
- Microwave (микроволновое излучение);
- Infrared (ИК излучение).

1) Радиоволны

Радиоволны находятся в диапазоне частот от 10 KHz до нескольких GHz. К радиоволнам относят следующие полосы частот:

Полоса частот – это непрерывный интервал частот, которые используются для передачи информации.

В радиоволнах полосы частот бывают регулируемыми и нерегулируемыми.

Использование регулируемой полосы частот возможно только после получения лицензии в соответствующих организациях (Госсвязьнадзор в России, Federal Communications Commission FCC - федеральная комиссия по связи в США и т.д.). Лицензирование позволяет гарантировать что данная частота не будет никем занята.

Можно также использовать нерегулируемые полосы частот, которые находятся в диапазонах 902-928 МГц, 2,4 ГГц. При использовании нерегулируемых частот нельзя гарантировать безошибочную передачу сигнала.

Характеристики электромагнитных волн сильно зависят от частоты. Чем выше частота, тем выше скорость передачи. При передаче в зоне прямой видимости использование высокочастотных волн выгоднее, так как они имеют меньший коэффициент затухания чем низкочастотные волны.

С другой стороны, низкочастотные радиоволны могут проникать сквозь преграды намного эффективнее высокочастотных волн. Волны с очень низкими частотами используются для связи с погруженными подводными лодками, хотя и скорость передачи при этом очень сильно снижается. Проникающая способность волн также очень сильно зависит от мощности передатчика. Чем выше мощность, тем лучше волны проникают сквозь препятствия, например, стены зданий.

В зависимости от количества используемых частот и мощности передатчика радиоволны классифицируют:

- одночастотная передача низкой мощности;
- одночастотная передача высокой мощности;
- передача в широком диапазоне частот.

Одночастотная передача низкой мощности (ОПНМ)

Низкая мощность передатчика используется для предотвращения взаимных помех нескольких близлежащих передатчиков. Поэтому область передачи обычно ограничена 30 или даже 20 метрами. Такой подход напоминает сотовую технологию, когда географическая область разделяется на маленькие изолированные ячейки, в результате чего все они могут использовать одну и ту же частоту без взаимных помех. Низкая частота и низкая мощность не позволяют достигать высоких скоростей передачи, достаточных для локальной сети. Обычно скорость передачи бывает ниже 1 Мбит/с.

Стоимость сильно зависит от используемого передатчика и антенны. Некоторые одночастотные системы требуют получения лицензии, но обычно продавец сам обеспечивает ее получение.

Одночастотная передача высокой мощности

Оборудование ОПВМ отличается более высокой мощностью от передатчиков ОПНМ, что позволяет покрывать большие расстояния. В зависимости от частоты ОПВМ может использоваться для передачи вне зоны прямой видимости или использовать эффект отражения сигнала от верхних слоев атмосферы.

Стоимость мощных передатчиков выше, чем обычных. К тому же в ОПВМ используются дорогие антенные башни и ретрансляторы.

Установка ОПВМ достаточно сложна. Обычно в ОПВМ используется высокое напряжение, а настройка должна производиться

квалифицированным специалистом. Оборудование должно быть грамотно настроено, чтобы точно соответствовать лицензии. При неправильной установке передатчик может мешать другим радиостанциям.

ОПВМ также сильно подвержена помехам. Так как ОПВМ охватывает значительную площадь, сигнал не сложно перехватить и прослушать.

Передача в широком диапазоне частот

Этот вид передачи изначально был разработан для военной связи. ПШДЧ увеличивает надежность передачи и уменьшает чувствительность к помехам. Передачу в широком диапазоне частот сложно прослушать.

Хотя такой вид передачи также основан на радиоволнах, одновременно используется несколько частот (более широкий диапазон частот). В ПШДЧ задействованы две схемы модуляции сигнала:

- непосредственная последовательная модуляция;
- скачкообразная перестройка частоты.

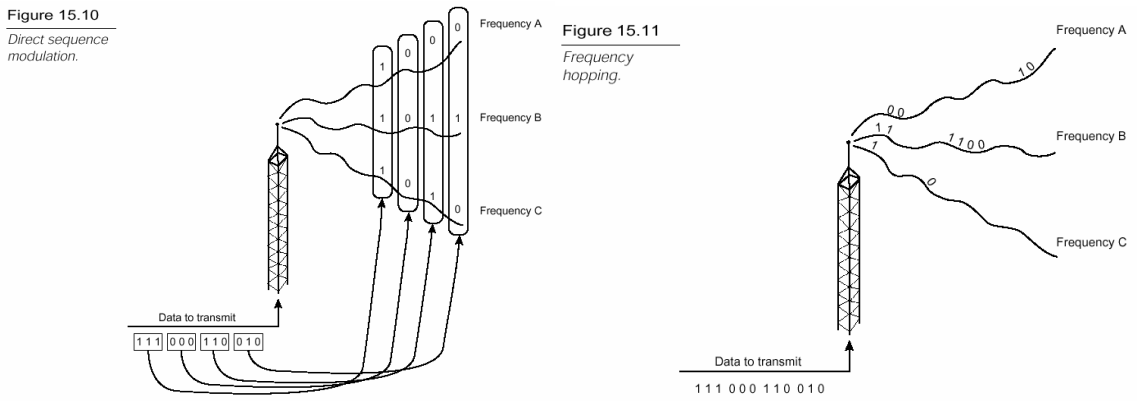

Рисунок 1.6. Передача в широком диапазоне частот

Существующие 900 МГц системы передают информацию со скоростью до 10 Мбит/с. При использовании скачкообразной перестройки частоты, данные передаются методом последовательного переключения на разные частоты. И источник и приемник должны синхронизировать график переключения. Также одновременно могут использоваться несколько частот для повышения скорости передачи информации.

Диапазон частот. Передача может идти во всем диапазоне радиочастот от 10 кГц до нескольких ГГц, но наиболее часто используются нерегулируемые частоты. По стоимости системы ПШДЧ занимают среднюю ценовую позицию. В большинстве случаев требуется установка уже готовой системы. Поэтому в зависимости от оборудования установка может быть от легкой до средней степени сложности.

Величина коэффициента затухания сигнала зависит от частоты и мощности передатчика. Чем выше частота и мощность передатчика, тем меньше затухание сигнала. Обычно используются маломощные передатчики, поэтому такие системы имеют высокий коэффициент затухания.

Как и другие радиоволны, ПШДЧ сильно подвержены ЭМ помехам. Однако, в силу передачи сигнала по нескольким частотам, потеря одной частоты не ведет к полной потере информации.

2) Микроволновое излучение

Микроволновую связь разделяют на два вида:

- наземная микроволновая связь;
- спутниковая микроволновая связь.

Наземная микроволновая связь

В наземной микроволновой связи используются направленные параболические антенны в условиях прямой видимости.

Наземная микроволновая связь использует нижние гигагерцовые диапазоны 4-6 и 21-23 ГГц, на которые как правило требуется лицензия.

Стоимость оборудования напрямую зависит от мощности передатчика и частоты волны.

При большой дальности связи оборудование стоит достаточно дорого.

Установка направленных антенн прямой видимости очень сложна, т.к. требуется крайне точная настройка, которая обычно производится методом проб и ошибок. К тому же при установке требуется соблюдать условие прямой видимости.

Максимальная **пропускная способность** зависит от частоты волны, она обычно составляет от 1 до 150 Мбит/с.

Величина затухания сигнала зависит как от частоты волны так и от типа используемой антенны. Высокочастотное микроволновое излучение сильно ослабляется дождем или туманом.

Микроволновое излучение можно заглушить или перехватить, однако шифрация информации уменьшает риск прослушивания.

Спутниковая микроволновая связь

Связь происходит между узконаправленными параболическими антеннами в условиях прямой досягаемости. Одна антенна установлена на земле, другая на геостационарном спутнике. Тарелка наземной антенны подключается к контроллеру, который имеет выход на локальную сеть. Антенна передает сигналы на геостационарный спутник, который вращается синхронно с Землей, находясь все время над одной фиксированной точкой на экваторе. Далее сигнал со спутника передается на наземную станцию.

Стоимость спутниковой микроволновой связи одинакова для любого расстояния. Для нее характерны большие задержки, которые колеблются от 0,5 с до 5 с, что связано с большим расстоянием, которое должен преодолеть сигнал.

Диапазон частот спутниковой микроволновой связи обычно находится в интервале от 11 до 14 ГГц.

Стоимость оборудования высока. Спутниковый канал можно арендовать у крупных коммуникационных компаний.

Установка наземной «тарелки» требует точной настройки на спутник. К тому же, чаще всего необходимо получение лицензии.

Пропускная способность зависит от частоты и составляет не боле 45 Мбит/с.

Коэффициент затухания сигнала зависит от его частоты и размера «тарелки». Волны могут ослабляться дождем и туманом.

Микроволны легко подвержены как глушению так и перехвату (сигнал может быть закодирован для уменьшения вероятности прослушивания).

3) Инфракрасное излучение

Для передачи ИК излучения используются светодиоды, лазерные диоды или фотодиоды (такие же, как и в волоконной оптике или бытовой технике). Прием ИК света возможен как в условиях прямой видимости, так и при отражении от различных поверхностей. При отражении теряется до половины энергии волны. Однако ИК излучение не может проникать сквозь стены или другие препятствия, и сильные источники света также могут заглушить ИК свет.

ИК изучение характеризуется высокой частотой (100 GHz – 1000 THz), поэтому теоретически оно может обеспечивать более высокую пропускную способность, однако технологии для этого продвинулись еще недостаточно далеко.

Различают две категории ИК связи:

- направленная ИК связь (point-to-point);
- ненаправленная ИК связь (broadcast).

Направленная ИК связь

Луч ИК волны узко направляется непосредственно на приемник. Соответственно, требуется точная настройка приемника и передатчика. Для связи на расстояния порядка нескольких сотен метров используются мощные инфракрасные лазеры. При этом должно соблюдаться условие прямой видимости.

Диапазон частот ИК связи – от 100 ГГц до 1000 ТГц.

Стоимость ИК оборудования зависит от типа источника ИК излучения. Мощные и высококачественные лазеры достаточно дороги, в то время как светодиоды имеют небольшую стоимость.

Направленная ИК связь требует точной настройки при **установке** и дальнейшей подстройки при эксплуатации.

Скорость передачи направленной инфракрасной связи – до 16 Мбит/с.

Коэффициент затухания ИК волны зависит от мощности источника, от качества сигнала, атмосферных условий и препятствий на пути волны. Надежная передача информации с помощью ИК волн возможна на расстояние не более нескольких километров.

ИК излучение ухудшается под влиянием сильного света. Направленное ИК излучение сложно прослушать, так как любое препятствие на пути волны будет сильно ухудшать связь.

Ненаправленная ИК связь

В случае ненаправленной связи передатчик рассеивает или расфокусирует сигнал чтобы его можно было принимать на большей площади. Такой метод также широко используется в бытовой аппаратуре. Таким образом намного легче настроить связь и принимающее устройство можно перемещать в зоне приема сигнала.

К тому же, один такой передатчик может связываться с другими такими же передатчиками.

Существует два подхода к реализации ненаправленной ИК связи. В первом случае, на некоторой высоте в помещении размещается передатчик, использующий ИК излучение с широкой площадью охвата. Другой подход заключается в использовании отражающего покрытия на потолке, таким образом сигнал от одного устройства отражается от потолка и передается на другие устройства.

Диапазон частот такой же как и у направленной ИК связи.

Стоимость ИК оборудования зависит от типа источника ИК излучения. Как правило, используются обычные светодиоды низкой стоимости.

Ненаправленную ИК связь легко **устанавливать**, учитывая условия прямой видимости источника и приемника. Также в зоне приема можно легко изменять конфигурацию сети.

Обычно **пропускная способность** таких систем не превышает 1 Мбит/с, но теоретически возможна и большая скорость.

Коэффициент затухания ненаправленной ИК связи зависит от тех же условий что и направленной – это мощность источника, качество сигнала и атмосферные условия. Однако наличие препятствий на пути сигнала уже не является значительной помехой, так как приемник можно переместить в другое место. Обычно дальность таких систем измеряется в десятках метров.

Как в любой ИК системе связь сильно ухудшается под воздействием сильного света. Ненаправленная ИК связь подвержена прослушиванию, так как сигнал можно перехватить в зоне приема.

3.3 Соединительное оборудование

Существует два типа соединительного оборудования:

- Сетевое (Network)
- Межсетевое (Internetwork)

1) Сетевое соединительное оборудование

Модемы (Modems)

Модемы (МОДулятор/ДЕМодулятор, modem) используются для преобразования цифровых сигналов компьютера в аналоговые сигналы для передачи через телефонные линии или микроволновые передатчики. Преобразование цифрового сигнала в аналоговый называется модуляцией (modulation), обратное преобразование – демодуляцией (demodulation).

Модемы могут использоваться для связи компьютеров или даже целых сетей, находящихся на значительном расстоянии. Некоторые модемы используют обычные коммутируемые линии (PSTN, public switched-telephone network), другие связываются только по специальной выделенной линии (dedicated line).

Использование модемов в локальных сетях дает следующие преимущества:

- обеспечивает пользователям удаленное подключение к LAN;
- модем с функциями факса позволяет принимать и передавать факсы с помощью факс-сервера;
- удаленные серверы могут производить синхронизацию данных с помощью модемной связи.

Повторители (Repeaters)

Как уже говорилось, при прохождении через среду передачи сигнала, ЭМ волны постепенно ослабляются (явление затухания). У каждого вида среды передачи существует максимально допустимое расстояние. Однако можно преодолеть это ограничения, используя повторители, которые усиливают сигнал.

Один вид повторителей, который называется усилителем (amplifier), просто усиливают сигнал вместе с нежелательным шумом. Другой вид повторителей, называемый повторителем с регенерацией сигнала (signal regenerating repeater), отделяет полезные данные из входящего сигнала и передает уже очищенный от шумов и усиленный сигнал.

Хотя, казалось бы, через повторители можно соединить бесконечно число сегментов, в каждой сетевой архитектуре существуют ограничения на количество повторителей, находящихся между источником и приемником информации. Каждая перепосылка сигнала увеличивает время передачи. Время, за которое сигнал передается до самой удаленной точки сети называется задержкой на распространение сигнала (propagation delay). Если эта задержка будет больше допустимой, связи с узлом не произойдет. В каждом сетевом стандарте определено максимально допустимое время задержки.Повторители могут связывать разную среду передачи (например, коаксиальный кабель и витую пару), но все подключенные кабели должны использовать одинаковый протокол доступа к среде (например, Ethernet).

Концентраторы (Hubs)

Некоторые типы компьютерных сетей требуют подсоединения отдельных сегментов к центральному устройству. Эти центральные устройства называются концентраторами, многопортовыми повторителями или хабами. Как и повторители, они позволяют преодолеть ограничения на длину сегмента. (multiport repeater, concentrator).

Например, нужно соединить несколько сегментов UTP. Параллельно их соединить нельзя, так как это приведет к проблемам передачи: отражению сигнала и повышению уровня помех. Поэтому в таких случая следует использовать концентратор.

Концентратор упорядочивает кабельное соединение и передает входящий сигнал на все подсоединенные кабели. Концентраторы разделяют на два вида: пассивные (passive), активные (active)

Пассивный концентратор только соединяет несколько сегментов кабеля вместе. Он не имеет никаких электронных компонент и не производит регенерации сигнала, поэтому каждый из сегментов не может быть длиннее половины максимальной длины.

Активный концентратор отличается от пассивного тем, что он усиливает и очищает сигнал, поэтому можно использовать кабель с его максимальной длиной сегмента.

Мосты

Мост соединяет вместе отдельные сегменты сети, причем мосты выборочно передают данные из одного сегмента в другой.

Функциональность моста будет заключаться в следующем:

1. получить все сигналы, посланные в сегменте А
2. отбросить сигналы, адресованные устройствам в сегменте А. Эта функция называется фильтрация (filtering)
3. передать все оставшиеся сигналы на другой порт – в требуемый сегмент
4. произвести все те же операции на других подключенных сегментах.

Мосты осуществляют эти операции с помощью определения **физического** местоположения источника и приемника в сети. Это местоположение определяется физическим или аппаратным адресом (MAC address).

Так как мосты могут производить фильтрацию сигналов, они часто используются для разделения перегруженной сети на несколько сегментов. Мост предотвращает утечку внутрисегментных сигналов за пределы сегмента, что снижает сетевой трафик (traffic).

Как сказано выше, мосты пропускают только те сообщения, которые предназначены другому сегменту. Для этого мост должен знать, в каком сегменте находится тот или иной адрес. Местоположение каждого узла указывается в специальной таблице адресов.

Информация, предназначенная всем устройствам сети, называется широковещательной (broadcast). Мосты пропускают широковещательный трафик. В некоторых случаях, сеть может быть переполнена широковещательными сообщениями.

Коммутаторы (switch), многопортовые мосты или интеллектуальные концентраторы сочетают функции повторителей и мостов.

Мультиплексоры

В компьютерной сети может возникнуть ситуация, когда нужно передать несколько сигналов через один носитель. Для этого следует установить мультиплексоры. Мультиплексор (multiplexor, MUX) принимает на входе несколько сигналов, а на выходе выдает один сигнал. Демультиплексор (demultiplexor) производит обратную функцию.

2) Межсетевое соединительное оборудование

Маршрутизаторы

Маршрутизаторы физически соединяют две (или больше) логически разделенные сети. Такие логически разделенные сети часто называют подсетями. Все подсети составляют одну большую интерсеть – совокупность подсетей. Каждая подсеть имеет свой адрес. Такой адрес называется сетевым адресом. Таким образом, каждый узел в интерсети характеризуется двумя параметрами – сетевым адресом и физическим адресом. Все подсети являются физически соединенными, но логически каждая подсеть отделена от другой маршрутизатором.

Маршрутизаторы намного «умнее» мостов. Они не только строят таблицы маршрутизации, где указаны все оптимальные маршруты, но и используют специальные алгоритмы для поиска и выявления маршрута до нужной подсети. Маршрутизаторы обмениваются между собой информацией о структуре сети с помощью специальных протоколов маршрутизации, которые будут рассмотрены позднее. В отличие от мостов, маршрутизаторы могут связывать сети с разной архитектурой (канального и физического уровней) – например, Token Ring и Ethernet. Маршрутизаторы могут управлять широковещательный трафиком.

Мосты-маршрутизаторы

Многие маршрутизаторы на самом деле являются мостами-маршрутизаторами (bridge-routers, brouters), то есть дополнительно выполняют функции моста. Мост-маршрутизатор всегда пытается доставить информацию используя протокол сетевого уровня (используется сетевой адрес). Если используемый протокол не поддерживается маршрутизатором, то мост-маршрутизатор работает как мост и отправляет информацию в соответствии с протоколом канального и физического уровней (используется физический адрес).

Устройства обслуживания канала и данных DSU/CSU

Эти устройства позволяют преобразовать электрический сигнал для передачи по носителю глобальных сетей. Они проверяют достаточно ли силен сигнал и соответствует ли он требуемому формату. Эти устройства защищают пользователя и сеть от нежелательных электрических шумов или скачков высокого напряжения. К тому же они преобразуют поступающие данные в соответствии с накладываемыми другой сетью правилами. Работа DSU/CSU похожа на работу модема, отличие заключается в том, что модемы работают с аналоговой средой передачи сигнала, а DSU/CSU – с цифровой.

Шлюзы

Шлюз – это аппаратно-программный комплекс, осуществляющий преобразование протоколов. В стеке TCP/IP термин «шлюз» может обозначать маршрутизатор. Шлюзом может быть и устройство, и программа, и их комбинация. Подробнее шлюзы будут рассматриваться на сетевом уровне.

Глава 4. Сетевая модель OSI

4.1. Сетевые протоколы и модели

В компьютерной сети должны быть приняты правила для обеспечения связи между поставщиками и потребителями услуг в сети. Протокол – это свод правил и стандартов по которым взаимодействуют различные устройства.

Протоколы в сети контролируют следующие вопросы:

- способ установки связи и обмена данными между сетевыми устройствами при использовании ими «разных языков»
- методы, позволяющие сетевым устройствам знать, когда нужно передавать данные, а когда нет
- методы, обеспечивающие корректное получение передаваемой по сети информации нужным адресатом
- организация и соединение физической среды передачи данных
- поддержание нужной скорости передачи данных всеми сетевыми устройствами
- методы представления битов в среде передачи данных.

Различные организации пытались создать стандарты и модели чтобы обобщить и структурировать задачи, выполняемые различными сетевыми протоколами.

Наиболее популярна модель Open Systems Interconnect (OSI) – модель открытого системного взаимодействия. Эта модель была разработана в 1977-78 гг Международной организацией стандартизации ISO. С тех пор она широко используется для пояснения сетевых коммуникаций.

Модель OSI состоит из следующих семи уровней (layers)

Application – Прикладной
Presentation – Представительный
Session – Сеансовый
Transport – Транспортный
Network – Сетевой
Data Link – Канальный
Physical – Физический

Уровни нумеруются снизу вверх. Физический уровень имеет номер 1, прикладной – номер 7. Каждый уровень отвечать за свой круг определенных задач. Такая структура уровней была определена базируясь на сложившейся структуре сетевых взаимоотношений. В каждом конкретном применении могут использоваться как все уровни сетевой модели, так и лишь несколько из них.

Каждый уровень в стеке протоколов обслуживается нижерасположенным уровнем и реализует сервис для вышерасположенного уровня. Например, уровень N использует сервис нижерасположенного уровня (N-1) и обслуживает вышерасположенный уровень (N+1).

Для обеспечения взаимодействия двух компьютеров на каждом из них должен выполняться один и тот же стек протоколов. Каждый уровень стека протоколов на компьютере взаимодействует со своим эквивалентом на другой машине (peer communication). Но при этом сообщение должно перейти на самый нижний уровень стека на одной машине и после передачи вернуться на нужный уровень вверх на другой машине.

При прохождении сообщения вниз по первому стеку, каждый уровень кроме физического добавляет свой заголовок (header) к сообщению. Заголовок содержит фрагменты управляющей информации, которая считывается и обрабатывается соответствующим уровнем принимающего стека. При перемещении сообщения вверх по стеку протокола, каждый уровень удаляет соответствующий заголовок.

4.2. Уровни сетевой модели OSI

На **физическом уровне** не описывается среда передачи данных. Однако протоколы физического уровня предусматривают определенную среду передачи данных.

На физическом уровне определяется физическая топология сети, сигналы передачи данных (цифровые, аналоговые), схема кодирования (уровнем, фронтом), мультиплексирование.

Канальный уровень OSI выполняет следующие функции:

1. Организация битов физического уровня (0 и 1) в логические единицы информации, называемые кадрами (frames).
2. Обнаружение и, по возможности, исправление ошибок
3. Контроль потока данных
4. Идентификация компьютера в сети

Канальный уровень добавляет заголовок к данным, поступающим сверху. В заголовке содержится информация о физическом адресе отправителя и получателя, длина кадра, и информация об использовании более высоких уровней.

Канальный уровень определяет:

- логическую топологию (звезда или кольцо)
- доступ к среде передачи (Media access, MAC-подуровень). При использовании каждой логической топологии существуют правила, которые определяют, может устройство передавать данные или нет. Эти правила управляют доступом к среде передачи данных.

- Конкуренция

Доступ к среде передачи получит первое запросившее устройство. То есть каждое сетевое устройство получает контроль над средой передачи и может вести передачу когда угодно. На практике такой метод часто приводит к коллизиям и потере данных. Для уменьшения числа коллизий были разработаны специальные протоколы (CSMA). При использовании такого протокола устройство перед передачей прослушивает носитель. Если

обнаруживается сигнал, то передача откладывается. Если сигнала не обнаруживается, происходит передача.

- Передача маркера

При использовании метода передачи маркера между устройствами в установленном порядке передается небольшой кадр данных, называемый маркером (token). Устройство, получившее маркер получает контроль над средой передачи и может передавать данные. Протоколы устанавливают как долго устройство может владеть маркером.

- Опрос

Этот метод предусматривает наличие центрального устройства (primary, controller), которое управляет доступом к среде передачи данных. Этот контроллер опрашивает вторичные устройства (secondaries) на предмет наличия информации для передачи. Для получения данных контроллер посылает запрос на вторичное устройство, принимает данные от него и передает их на получателя.

– Адресация (MAC-подуровень)

Каждому сетевому устройству присвоен уникальный адрес, который называется физическим адресом устройства или MAC-адресом (MAC-address). Хотя физические адреса устройств известны, в локальных сетях передача данных обычно производится на все устройства. То устройство, чей адрес совпадает с адресом получателя пакета, принимает данные. Все остальные устройства игнорируют пакет.

– Синхронизация передачи (transmission synchronization) (LLC-подуровень)

– Обслуживание соединений

Обслуживание соединений реализуется двумя способами:

- управление потоком данных
- контроль ошибок

Основное назначение **сетевого уровня** OSI заключается в передаче данных получателю. На сетевом уровне описываются методы доставки информации между независимыми и разными подсетями (subnets), которые образуют составную сеть или интерсеть. (internetworks). Подсети соединяются между собой маршрутизаторами. Компонентами интерсети могут являться как локальные, так и глобальные сети.

На сетевом уровне можно выбрать определенный маршрут следования пакета к получателю во избежание утечки данных в незадействованные сети. Для этого на сетевом уровне используется коммутация, адресация сетевого уровня и маршрутизация.

Протоколы физического и канального уровней передают пакеты между устройствами. На сетевом уровне информация передается уже между сервисами, работающими на этих устройствах. **Транспортный уровень** передает информацию между конечными сервисами.

Транспортный уровень передает пакеты данных, которые также называются сегментами. Основное предназначение транспортного уровня –

скрыть инфраструктуру сети от протоколов более высоких уровней. При передаче информации с более высоких уровней на транспортный, данные формируются в сегменты. Транспортный уровень другого устройства принимает сегменты, обрабатывает их и передает полученную информацию на более высокие уровни.

Транспортный уровень отвечает за надежную (reliable) доставку информации. Термин «надежная» не обозначает полное отсутствие ошибок. Он говорит о том, что если произойдет ошибка, произойдет повторная передача или об этом будет сообщено более высокому уровню.

Сеансовый уровень используется для управления сеансами, то есть диалогами между конечными сервисами. На этом уровне происходит установление диалога, управление диалогом (симплексный, дуплексный и полудуплексный режимы) и синхронизация.

На **уровне представления** осуществляет преобразование информации в понятный обоим приложениям вид с помощью трансляции. Для защиты от несанкционированного доступа используется шифрование данных.

На **прикладном уровне** реализуются все сетевые службы. Прикладной уровень обеспечивает интерфейс между сетевыми службами и операционной системой.

Соответственно прикладной уровень осуществляет две функции: объявление служб и обеспечение доступности служб.

РАЗДЕЛ 2. АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

Глава 1. Стек протоколов TCP/IP

Стек протоколов TCP/IP был создан в результате разработки сетей с коммутацией пакетов, которые проводились агентством ARPA DoD (Department of Defense Advanced Research Projects Agency) в конце 60-х – начале 70-х годов. Стек был разработан для глобальных сетей.

1.1. История появления стека

Одна из причин популярности состоит в том, что никто не является владельцем стека TCP/IP. Стек TCP/IP является открытым стеком, и его поддерживают подавляющее большинство производителей оборудования и операционных систем. Изначально протокол TCP/IP применялся в системах Unix, в частности, был встроен в BSD (Berkeley Standard Distribution) версию Unix. С тех пор TCP/IP получил всестороннее признание сообщества Unix и сейчас поддерживается всеми версиями этой системы.

Стек протоколов TCP/IP был разработан за 10 лет до принятия модели OSI, поэтому он не полностью ей соответствует и состоит из 4 уровней. Протоколы TCP/IP не касаются физического и канального уровня, то есть они работают поверх разных существующих стандартов, например, поверх Ethernet. В такой универсальности состоит одна из причин успеха TCP/IP.

Стек TCP/IP является наиболее совершенным и распространенным протоколом из всех доступных на сегодняшний день. Все современные ОС поддерживают стек TCP/IP, и почти все крупные сети используют его для обеспечения большей части своего трафика. TCP/IP является стандартным для сети Интернет.

Еще одно преимущество TCP/IP – возможность объединения неоднородных (гетерогенных) систем. Существуют протоколы и соответствующие утилиты, позволяющие взаимодействовать различным системам. Например, в поставку Windows NT входят утилиты FTP (File Transfer Protocol) и Telnet.

TCP/IP также является каркасом для разработки приложений, использующих архитектуру клиент/сервер. Существует стандартный сетевой интерфейс для приложений Windows (API, application program interface), называемый Windows Sockets. Он был разработан на основе Berkeley UNIX Sockets. Приложения, разработанные под Windows Sockets версии 2 (Winsock 2 API), могут работать и в других совместимых с интерфейсом протоколах. Например, в IPX, NetBEUI, DecNET, OSI и ATM.

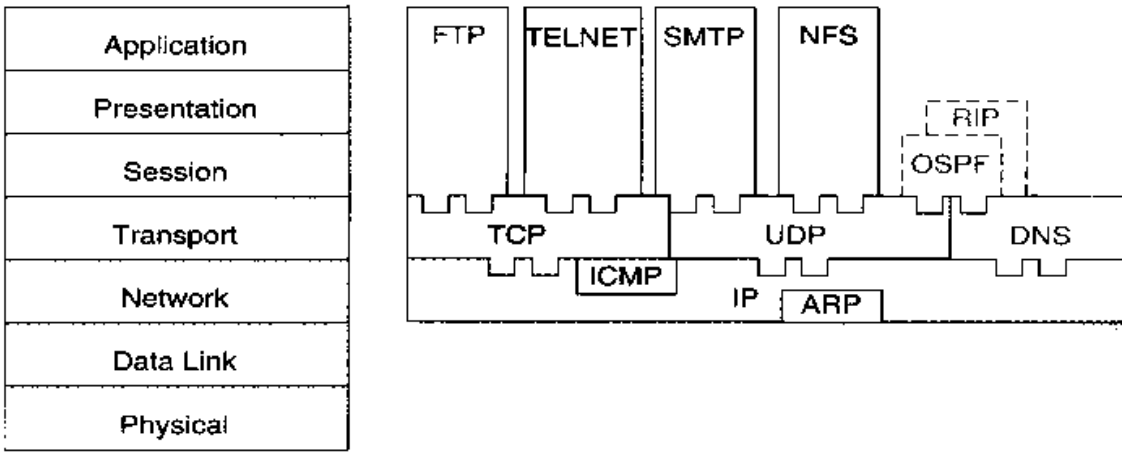

Рисунок 2.1. Стек TCP/IP

Верхний уровень стека TCP/IP называется прикладным уровнем (application layer). В него входят протоколы TELNET, FTP, SMTP, HTTP и другие. Протоколы прикладного уровня обеспечивают работу сетевых служб и программ. Прикладной уровень соответствует трем верхним уровням OSI: Прикладному, Представительному, Сеансовому. Интерфейс между программами и транспортным уровнем осуществляется с помощью портов (ports).

Третий уровень TCP/IP называется транспортным (transport). На нем реализуются два протокола: TCP and UDP. Транспортный уровень обеспечивает конечную передачу данных (между программами) и может использовать конечное обслуживание соединений. Третий уровень TCP/IP точно соответствует транспортному уровню OSI.

Второй уровень TCP/IP называется межсетевым (internet) соответствует сетевому уровню OSI. На этом уровне представлена инфраструктура интерсети, скрытая от верхних уровней. На межсетевом уровне рассматриваются протоколы IP, ICMP, RIP, OSPF, ARP.

Первый уровень называется уровнем сетевого интерфейса (network interface layer) и реализуется другими протоколами канального и физического уровней, не входящими в стек TCP/IP.

1.2. Протоколы стека

IP (Internet Protocol)

IP – протокол сетевого уровня с использованием дейтаграммной коммутации пакетов без установления соединения. Он выполняет сетевую IP адресацию и динамический выбор маршрута. Протокол IP разбивает поступающие сверху пакеты на более мелкие части при необходимости. Далее IP добавляет заголовок и передает пакет на канальный уровень в качестве кадра.

IP использует динамическую маршрутизацию: на каждом хопе происходит выбор маршрута в соответствии с таблицами маршрутизации. В качестве обслуживания соединений IP осуществляет только контроль ошибок

заголовка: в IP заголовок помещается контрольная сумма. Но контрольная сумма проверяет только заголовок а не пакет в целом. Максимальная длина IP пакета составляет 65535 байт. Заголовок обычно занимает 20 байт.

ICMP (Internet Control Message Protocol)

ICMP (протокол межсетевых управляющих сообщений) является протоколом сетевого уровня, работающим совместно с IP. ICMP обеспечивает обслуживание соединений на сетевом уровне: он определяет перегрузку, обрыв связи и другие ошибки. ICMP используется для информирования IP и протоколов более высоких уровней о таких сетевых ошибках.

RIP (Routing Information Protocol)

RIP это протокол маршрутизации основанный на алгоритме дистанционно-векторного типа (DVA). Маршрутизаторы периодически и широковещательно пересылают свои таблицы по своим подсетям. В качестве цены маршрута используется количество хопов. RIP присущи все недостатки DVA протоколов – плохая работа в больших и сложных интерсетях. IP RIP по своим функциям похож на IPX RIP, хотя они являются разными протоколами.

OSPF (Open Shortest Path First)

OSPF был разработан как замена RIP и является протоколом маршрутизации с использования алгоритма состояния связей (LSA). Соответственно маршрутизаторы владеют графом структуры сети, и могут более грамотно строить маршрут в интерсетях. OSPF выполняет распределение загрузки каналов (load balancing), то есть при наличии нескольких путей с одинаковой ценой, направляет пакеты попеременно по этим путям. Также OSPF может осуществлять маршрутизацию на основе типа службы.

TCP (Transmission Control Protocol)

TCP (протокол управления передачей) является главным транспортным протоколом Internet с установлением соединения. Он принимает сообщения любого размера с верхних уровней, обеспечивает конечное обслуживание соединений и дуплексный режим работы.

TCP принимает поток данных, разбивает его на сегменты и передает их на сетевой уровень протоколу IP. TCP присваивает каждому сегменту номер и при приеме производит упорядочивание. Также возможна агрегация сегментов, когда в один сегмент входят данные от нескольких сетевых служб.

Если задача IP заключалась в передаче данных между произвольными устройствами сети, TCP передает данные между любыми службами на любых узлах сети.

Пакетам каждого соединения присваивается идентификатор соединения CID, который также называется портом. Для некоторых служб номера портов закреплены и стандартизированы. Например, FTP: 21. Каждый порт может поддерживать несколько соединений и таким образом осуществлять их мультиплексирование.

Протокол TCP по своей функциональности похож на SPX.

UDP (User Datagram Protocol)

Протокол UDP (протокол дейтаграмм пользователя) принадлежит к транспортному уровню, но в отличие от TCP не устанавливает логического соединения и не использует подтверждений. UDP просто осуществляет обмен дейтаграммами между сетевым и высшими уровнями. UDP также использует адрес службы, называемый портом. Порт здесь является просто указателем на конкретную службу, а не идентификатором соединения. Номера портов в TCP и UDP разные, и не влияют друг на друга. 21 порт в UDP не зависит от 21 порта в TCP.

Так как UDP не выполняет процедуры установления соединения и контроля потока, он работает быстрее чем TCP.

UDP подходит для сетей, где быстродействие важнее надежной доставки. Также для приложений, передающих данные небольшого объема за один раз.

ARP (Address Resolution Protocol)

Протокол ARP преобразует физический адрес в IP адрес. Сетевой IP адрес состоит из 4 байт, каждый из них представлен в десятичной системе и отделен точкой. Например, 195.151.147.4. IP адрес состоит из номера подсети и номера компьютера в этой подсети. ARP использует широковещательные пакеты или составленную ранее таблицу адресов для определения соответствия IP адреса и физического адреса.

DNS (Domain Name System)

DNS – это распределенная база данных, производящая преобразование имени по запросу клиента в сетевой адрес и обратно. Записи в DNS связаны иерархией имен: например, в имени www.vspu.kirov.ru, ru обозначает Россию, kirov – регион, vspu – клиента в регионе, а www – компьютер или службу у клиента.

FTP (File Transfer Protocol)

Протокол FTP позволяет передавать файлы между двумя компьютерами. FTP обеспечивает защиту с помощью пароля на соединение, передачу списка файлов, выполнение операций с файлами, исполнение файлов. FTP может использоваться для передачи файлов между двумя разными операционными системами, так как язык запросов FTP не зависит от локальной ОС.

SMTP (Simple Mail Transfer Protocol)

SMTP – протокол маршрутизации электронной почты, который использует TCP и IP для передачи сообщений между компьютерами. SMTP не обеспечивает хороший интерфейс для конечного пользователя. Для чтения и написания писем, для управления почтовым ящиком требуются специальные пользовательские почтовые программы.

TELNET (Remote Terminal Emulation)

TELNET позволяет пользователям получать доступ к приложениям сервера, используя клиентские компьютеры в роли терминалов. Так же как и

FTP, TELNET обеспечивает связь между разными операционными системами, например UNIX и VMS.

NFS (Network File System)

NFS была впервые разработана фирмой Sun Microsystems в рамках концепции Sun ONC (Open Network Computing). Три самых популярных протокола – это NFS, XDR (external Data Representation, Прикладной уровень), and RPC (Remote Procedure Call, Сеансовый уровень).

Для внедрения этих протоколов, Sun сделала их открытыми. Далее они были приняты и доработаны сообществом Интернет.

NFS является протоколом прикладного уровня, реализующий файловую службу. NFS отличается от таких протоколов как FTP и TELNET своей «прозрачностью». NFS позволяет пользователям различных компьютеров работать с удаленными файлами так же легко, как и с локальными. Пользователь может не знать никаких специализированных команд.

XDR является протоколом представительного уровня, осуществляющий трансляцию данных. Протокол XDR позволяет передавать данные в специальном кодированном формате, не зависящем от операционной системы. XDR реализуется в виде серии библиотек, позволяющих программистам встраивать XDR в приложения.

RPC является протоколом сеансового уровня, осуществляющим администрирование сеанса. RPC функционирует следующим образом. Редиректор перенаправляет запрос на локальные или сетевые ресурсы в зависимости от места расположения ресурса. Существуют специальные серверы RPC, которые обрабатывают запросы. Сервер принимает запрос и отсылает клиенту результат запроса.

Глава 2. IP – адресация.

2.1. Понятие IP-адреса

IP адрес – число, однозначно определяющее TCP/IP узел в интерсети. Узлом называется любая машина, имеющая сетевой интерфейс, использующий TCP/IP. Например, это компьютер в сети под управлением Windows NT, Unix или любой из маршрутизаторов.

Каждый IP адрес состоит из двух частей – идентификатора сети (network ID) и идентификатора узла (host ID). Первый определяет физическую сеть. Он одинаков для всех узлов в данной сети и уникален для каждой из сетей, входящих в интерсеть.

Host ID соответствует каждому узлу в данной сети. Он должен быть уникален в пределах данной сети.

Можно считать, что если Интернет – это один город, то Network ID соответствует улице в этом городе, а Host ID – номеру дома на улице.

Интерсеть состоит из множества подсетей (или сетей). Границы каждой подсети определяются маршрутизаторами, которые разделяют сетевой трафик. Каждый интерфейс маршрутизатора обращен в отдельную подсеть, и имеет идентификатор этой сети. Если в подсеть обращено несколько маршрутизаторов, их интерфейсы имеют одинаковый Network ID и уникальный Host ID.

Все узлы, использующие один и тот же Network ID должны быть физически расположены в одном сегменте сети. Если узел переносится из одного сегмента в другой, его Network ID тоже должен быть изменен.

Узлы обычно имеют один сетевой интерфейс (сетевую карту), но некоторые узлы, например, маршрутизаторы, могут быть настроены на использование нескольких сетевых интерфесов. В таком случае, каждый интерфейс узла должен иметь свой уникальный IP адрес.

Форматы IP адресов

IP адреса могут быть представлены как в двоичном, так и в десятичном формате. В десятичном формате IP адрес состоит из четырех групп цифр (октетов), каждая из которых отделена от соседей точкой. Такой способ адреса называется точечно-десятичной записью. Для компьютера IP-адрес является 32-битным числом (или 4-байтным). Каждый октет может принимать в десятичной записи значения от 0 до 255, что представляется восемью битами в двоичном коде, или одним байтом (октетом).

Например, если запись числа в десятичном виде выглядит следующим образом:

192.168.0.1

то в двоичном виде число будет записано как

11000000 10101000 00000000 00000001

Получение IP адресов

Как уже говорилось, IP адрес в интерсети должен быть уникальным, независимо от количества узлов в ней. Если сеть компании использует TCP/IP и не соединена с Интернетом, то назначение уникальных IP адресов не является большой проблемой. Однако при соединении с Интернетом, необходимо убедиться, что данный IP адрес никем не используется и свободен.

За распределение и присвоение адресов в Интернете отвечает InterNIC (Internet Networking Information Center). То есть одна организация следит за адресным пространством в Интернете. Однако, это не означает, что InterNIC следит за каждым IP адресом. Он выделяет каждой организации Network ID, и организация может создать в этой сети необходимые узлы. Размеры выданной подсети определяются классом.

2.2.Классы IP адресов

Изначально система адресации Интернета базировалась на классов – ее называют классовой адресацией (RFC-791).

Когда Интернет только зарождался, было решено что 32-битное адресное пространство будет достаточно для всех узлов (32-битным значением можно адресовать примерно 4,3 млрд узлов). Однако сейчас такое количество уже нельзя считать исчерпывающим. Новая версия протокола IPv6 в будущем еще увеличит адресное пространство.

Общее адресное пространство интерсети делится на сети различного размера (различного количества узлов). Размер сети зависит от ее класса. Класс сети можно определить по значению старших битов первого октета IP адреса. Классы A,B,C используются для обычной адресации, класс D – для групповой адресации, класс E зарезервирован для будущего использования.

Таблица 2.1. Классовая адресация

Класс адреса	Старшие биты 1 октета	Диапазон десятичных значений первого октета	Доступное количество сетей в классе	Доступное количество узлов в классе
A	0	1-126	27-2 = 126	(224)-2 = 16 777 214
B	10	128-191	214=16 384	216 -2 = 65 534
C	110	192-223	221 =2 097 152	28-2= 254

В зависимости от класса, разное количество октетов относится к Network ID и Host ID.

Таблица 2.2. Структура классов

Класс адреса	IP-адрес	Host ID	Network ID
A	w.x.y.z	w	x.y.z
B	w.x.y.z	w.x	y.z
C	w.x.y.z	w.x.y	z

Класс A

Класс A использует для Network ID только первый октет, а три оставшихся – для Host ID. Поскольку старший бит первого октета всегда равен 0, то для Network ID остается 7 бит. Они позволяют идентифицировать 127 различных сетевых адресов. Но Network ID 0 использовать нельзя, а Network ID 127 зарезервировано для локального сетевого адаптера (loopback adapter), поэтому в классе A доступны 126 уникальных сетевых адресов. В такой сети можно использовать 16 777 214 (224-2) адресов узлов. Вычитание 2 связано с тем, что никакому узлу нельзя присваивать номера, состоящие из одних нулей (это значение зарезервировано для указания маршрута по умолчанию) или одних единиц (используется для групповой рассылки).

Такие адреса сетей закреплены за очень крупными организациям, как правило военными учреждениями и университетами.

Например, в адресе 124.29.88.7 Network ID будет 124, а Host ID – 29.88.7.

Класс B

Для Network ID используется первый и второй октеты, а два оставшихся – для Host ID. Два старших бита первого октета всегда равны 10. Поэтому для Network ID остается 14 бит, которые позволяют использовать 16 384 адреса сетей. Оставшиеся 16 бит обеспечивают адресацию 65 534 (216-2) узлов. Этот класс предназначен для средних и больших сетей.

Например, в адресе 130.29.88.7 Network ID будет 130.29, а Host ID – 88.7.

Класс C

Этот класс использует первые три октета для Network ID, а оставшийся – для Host ID. Три старших бита первого октета равны 110, что оставляет 21 бит для Network ID. Это позволяет адресовать 2 097 152 сети. Оставшиеся 8 бит доступны для использования в качестве адреса узла. Это позволяет использовать 254 (28-2) адреса узлов. Сеть класса C проще всего получить в InterNIC. Но организация должна продемонстрировать, что она нуждается в целом блоке из 254 адресов. Например, в адресе 192.29.88.7 Network ID будет 192.29.88, а Host ID – 7.

Если организации необходимо больше адресов, чем может предоставить подсеть класса C, но значительно меньше, чем содержится в подсети класса B, можно получить несколько подсетей класса C. Но это усложнит таблицы маршрутизации Интернета. Обычно одной организации соответствует одна подсеть, и одна строчка в таблицах маршрутизации. После того, как пакеты с данным Network ID поступают в локальную сеть

организации, локальные маршрутизаторы уже распределяют информацию внутри подсети.

Необходимость эффективного использования доступного адресного пространства и необходимость уменьшения таблиц маршрутизации на центральных маршрутизаторах Интернета стимулировала создание новой системы IP-адресации CIDR (Classless Inter-Domain Routing, межклассовая междудоменная маршрутизация). CIDR не распознает классы адресов, а использует сетевые идентификаторы переменной длины, называемые масками подсети.

Класс D

Этот класс используется для групповых рассылок, для отправки информации определенной группе узлов. Старшие биты адреса класса D всегда установлены в 1110. Оставшиеся биты используются для обозначения логической группы узлов. (Первый октет – 224-239).

Класс E

Класс E – экспериментальный класс адресов, зарезервированный для будущего использования. Четыре старших бита первого октета устанавливаются в 1111.

Советы IP адресации

Рассмотрим простейший случай подключения организации к Интернету с использованием классовой схемы адресации.

Чтобы соединить сеть организации с Интернетом, необходимо получить Network ID и соответствующий блок адресов от InterNIC. Нельзя выбирать произвольный идентификатор сети. Однако если сеть TCP/IP будет закрыта из внешней сети, то можно выбирать Network ID произвольно, и при этом следовать некоторым советам (RFC-1918).

1. Планируйте на будущее – выбирайте класс, который допускает дальнейший рост сети.

2. Убедитесь в уникальности. При присвоении Network ID необходимо помнить, что он должен быть уникальным. Каждый сегмент, подключенный к маршрутизатору, должен иметь свой уникальный Network ID.

3. Не используйте зарезервированные адреса. Например, адрес сети 127 зарезервирован как loopback adapter. Список зарезервированных адресов можно найти по адресу ds.internic.net.

4. Network ID не может состоять из всех единиц или нулей. Все нули в Network ID означают, что узел находится в локальной сети, и пакеты для него не будут маршрутизироваться наружу. Использование всех единиц означает, что пакет представляет собой широковещательное сообщение.

При выборе правильного Host ID необходимо следовать правилам:

1. Убедиться в уникальности Host ID в данной подсети.

2. Не использовать зарезервированные адреса. Идентификатор узла не может состоять из всех нулей или всех единиц. Все нули в Host ID обозначают, что пакет предназначен для сети без указания конкретного узла. Все единицы означают, что пакет представляет собой широковещательное сообщение для всех узлов определенной сети.

3. Будьте последовательны в присвоении Host ID. Создайте какие-либо правила, чтобы облегчить администрирование в дальнейшем. Например, небольшие числа можно использовать для адресации маршрутизаторов (192.168.0.1-192.168.0.5), а большие числа – для серверов (192.168.0.246-192.168.0.254). Промежуток – для рабочих станций (192.168.0.6-192.168.0.245).

Ошибки IP адресации

Если узел использует неверный Network ID, информация для этого узла будет отправлена в другую сеть. Эта проблема может возникнуть при переносе компьютера из другой сети.

Если два узла в одной сети пытаются использовать один и тот же Host ID, то могут возникнуть ошибки приема и передачи. Такой проблемы не должно быть в Windows NT, так как при инициализации система отправит широковещательное сообщение, в котором говорится о том, какой адрес система будет использовать. Если какой-нибудь узел ответит, что адрес занят, IP адрес проинициализирован не будет. Но при использовании других TCP/IP стеков подобная проблема может привести к неработоспособности обоих узлов.

2.3. Разделение сети на подсети

Перейдем к более современной схеме адресации – бесклассовой (RFC-950).

Можно видеть, что все адресное пространство Интернета разделено на три большие группы: классы A, B и C. Мы могли бы выбрать нужный класс исходя из количества узлов в сети. Класс A предоставлял мало сетей и много узлов, класс C – много сетей и мало узлов. Оптимальным выбором был бы класс B, но такое множество адресов вряд ли использовалось бы полностью – трудно создать сеть с 65-ю тысячами узлов. Огромное количество адресов класса C переполнило бы таблицы маршрутизации. Большинство сетей класса C не задействовали 254 узла.

Как известно, InterNIC обычно выдает одну подсеть определенного класса (чаще всего C) на одну организацию. То есть выдается уникальный Network ID. Он не может быть изменен никоим образом. Но идентификаторы узлов организация может использовать по своему усмотрению. Довольно часто требуется разделить подсеть на несколько логических подсетей, и часть бит Host ID используют для Network ID. Количество бит Network ID увеличивается и количество бит Host ID уменьшается.

Подсеть – в данном случае создается при помощи переноса нескольких бит из Host ID в Network ID.

Суперсеть (для упрощения таблиц маршрутизации) создается с помощью переноса бит из Network ID в Host ID.

Но тогда возникает проблема – как узнать, какое количество бит относится к Network ID, а какое – к Host ID. Для решения этой проблемы и предназначены маски подсетей.

Маска подсети – это 32-битный адрес, позволяющий определить, сколько бит в адресе используется для Network ID. Маска использует единицы в позициях, соответствующих сетевому идентификатору.

Например, для классов приняты следующие маски по умолчанию.

Таблица 2.3. Маски классов

Класс	Маска	Двоичная маска
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

При инициализации стека TCP/IP, каждый узел сравнивает свой IP адрес с заданной маской подсети при помощи процесса логического «И». Для определения, предназначен пакет для локальной или удаленной сети, узел сравнить IP адрес получателя со своей маской подсети, а затем сравнит результат со значением, полученным при инициализации. Если результаты совпадают, то пакет предназначен для локального узла и не маршрутизируется. Если результаты различны, пакет передается в другую сеть маршрутизатору.

Рассмотрим операцию подробнее

Например

IP адрес (десятичный) 192.168.2.66

IP адрес (двоичный)

11000000.10101000.00000010.01000010

Маска подсети (десятичная) 255.255.255.0

Маска подсети (двоичная)

11111111.11111111.11111111.00000000

Результат выполнения логического «И»

11000000.10101000.00000010.00000000

Например, вам нужно разбить сеть класса C (192.168.24.0) на две логические подсети. Для этого обычно Network ID увеличивается на 1 бит. Маска подсети в таком случае записывается как 255.255.255.128. Число 128 (10000000) показывает, что старший бита октета используются Network ID. В большинстве случаев добавочные биты, использующиеся для организации подсети, могут состоять из всех нулей или единиц. Кроме специальных случаев, когда используется устаревшее оборудование. Поэтому получается две подсети. Последние октеты Network ID будут записываться как (00000000 и 10000000). В каждой такой сети может существовать 27-2=126 узла.

Предположим, вы работаете в компании, имеющей три физические сети. Вы получили сеть класса C (192.168.24.0) и вам нужно ее разбить на три подсети. Для этого необходимо два бита из Host ID перенести в Network ID. Из двух битов могут быть получены четыре (22) подсети.

Например, до разбиения IP адрес был 192.168.24.65 и использовалась маска по умолчанию 255.255.255.0. В двоичном виде:

IP адрес Network ID: 11000000 10101000 00011000 Host ID: 01000001

Маска: 11111111 11111111 11111111 00000000

После разбиения:

Такой же IP адрес (192.168.24.65) с другой маской (255.255.255.192) будет иметь другой Host ID и Network ID:

IP адрес Network ID: 11000000 10101000 00011000 010 Host ID: 00001

Маска: 11111111 11111111 11111111 11000000

Получается что 65 узел превратился в первый узел новой подсети.

Четыре логические подсети будут иметь следующие два старших бита четвертого октета в Network ID: 00, 01, 10 и 11. В десятичном виде последний октет Network ID будет следующим: 0, 64, 128, 192, . IP адреса для первого узла (Host ID 00001) для каждой подсети будут выглядеть следующим образом.

Таблица 2.4. Адреса первого узла подсети

Последний октет Network ID10	IP адрес10 для Host ID 00001
0	192.168.24.1
64	192.168.24.65
128	192.168.24.129
192	192.168.24.193

В каждой из подсетей может существовать 26-2=62 узла. Всего может быть 248 узлов. То есть при разбиении часть доступных адресов узлов теряется (без разбиения доступно 254 узла).

Рассмотрим пример операции логического «И» для данных IP адресов.

Пусть IP адрес исходного узла – 192.168.2.65 с маской 255.255.255.192. Network ID: 11000000 10101000 00000010 01, Host ID: 000001. Маска: 11111111 11111111 11111111 11000000. Результат операции логического «И» в десятичной форме: 192.168.2.64, в двоичном виде: 11000000 10101000 00000010 01.

IP адрес для локального узла: 192.168.2.91 с маской 255.255.255.192. Network ID: 11000000 10101000 00000010 01, Host ID: 011011. Маска: 11111111 11111111 11111111 11000000. Результат операции логического «И» в десятичной форме: 192.168.2.65, в двоичном виде: 11000000 10101000 00000010 01.

IP адрес для удаленного узла: 192.168.2.129 с маской 255.255.255.192. Network ID: 11000000 10101000 00000010 10, Host ID: 00001. Маска: 11111111 11111111 11111111 11000000. Результат операции логического «И» в десятичной форме: 192.168.2.128, в двоичном виде: 11000000 10101000 00000010 10.

Видно, что результат логического «И» одинаков для локального узла и разный для удаленного узла. Таким образом определяется место назначения

пакета. Пакет для локального узла перенаправляется на узел назначения, а пакет для удаленного узла – на маршрутизатор.

Реализация архитектуры подсетей

При разделении сети на несколько подсетей, необходимо выполнить следующие шаги.

1. Определить требуемое количество подсетей. При этом необходимо учитывать дальнейший рост сети.
2. Определить требуемое количество узлов для каждой подсети. Здесь также необходимо учитывать дальнейший рост подсетей.
3. Определить маску подсети для данного количества Network ID и Host ID.
4. Определить значения Network ID каждой подсети.
5. Определить значений Host ID в подсетях.

Разберем каждый шаг подробнее.

Определение требуемого количества подсетей

Свой Network ID должен быть у каждого сегмента, подключенного к маршрутизатору. Необходимо сосчитать количество сегментов сети, каждый из которых может быть ограничен одним или более маршрутизаторами. На рис. изображен пример конфигурации сети. Там показаны четыре различные сети, входящие в состав организации и одна внешняя сеть, обеспечивающая доступ в Интернет. Каждая подсеть требует уникального Network ID. Подсети, которые будут иметь выход в Интернет через реальные IP адреса, должны иметь Network ID, удовлетворяющий полученному у InterNIC. Если некоторые подсети не будут иметь выход в Интернет через реальные IP адреса, или выход будет осуществляться через прокси-сервер или NAT (network address translation), Network ID этих сетей можно выбирать произвольно. За маршрутизатором, разделяющим сеть организации и Интернет, обычно находится сеть провайдера Интернета и сам провайдер отвечает за правильную адресацию в ней. Для удобства администрирования сети, рекомендуется использовать одинаковые маски, и, соответственно, одинаковые по размеру подсети для всей организации.

В показанном примере в организации существуют четыре подсети. Возможно, в будущем будет добавлено еще от четырех до восьми подсетей.

Определение требуемого количества узлов для каждой подсети

Сетевые карты, установленные внутри компьютеров, обычно используют один Host ID. Принтеры и интерфейсы маршрутизаторов, обращенные в данную сеть, также требуют одного Host ID. Каждый интерфейс маршрутизатора требует отдельного IP адреса. Компьютер, с установленной на нем Windows NT может выступать в роли маршрутизатора. Маршрутизатор обычно содержит от двух до 24 интерфейсов. Необходимо учитывать рост сети в будущем. Например, если одна подсеть содержит 35 компьютеров, в будущем там может быть порядка 60 узлов. Если требуемого количества узлов данное разбиение не предоставляет, перенастройка всей сети повлечет большие трудности.

Определение маски подсети

Необходимо выбирать маску, при которой можно будет реализовать и достаточное количество подсетей, и достаточное количество узлов в каждой подсети.

Например, компании выдана сеть класса С: 192.169.220.0. В такой сети может быть до 254 узлов. Компания уже имеет шесть сетей, в самой большой из которых девять узлов. Необходимо найти маску сети, которая поддерживала бы существующую конфигурацию сети и допускала бы ее дальнейшее развитие.В таблице приведено количество возможных масок подсетей для сети класса С.

Таблица 2.5. Возможные маски подсети

Маска подсети	Количество подсетей	Количество узлов в подсети	Общее кол-во узлов
255.255.255.192	2	62	124
255.255.255.224	6	30	180
255.255.255.240	14	14	196
255.255.255.248	30	6	180
255.255.255.252	62	2	124
255.255.255.254	126	-	-
255.255.255.255	254	-	-

В таблицу не включена маска по умолчанию (255.255.255.0), поскольку она предоставляет только один идентификатор сети. Маска .128 также отсутствует, так как она обеспечивает только один дополнительный бит для Network ID, который не может состоять из всех 0 или 1. Маски .254 и .255 не позволяют создать Host ID в таких подсетях. Следовательно, для выбора имеются только 5 масок. Примечание. В ряде случаев, дополнительные биты Network ID могут принимать значения всех 0 или всех 1, если маршрутизаторы и оборудование поддерживает этот режим. Так как компания уже имеет шесть сетей, то маска .192 выпадает. Маска .224 позволяет создать 6 подсетей с 30 узлами. Однако, она не учитывает рост сети в будущем. Поэтому лучше выбрать маску .240, которая позволит создать 14 подсетей с 14 узлами в каждой.

Определение значений Network ID

Первый шаг в определении идентификаторов сетей состоит в том, чтобы выписать все возможные комбинации дополнительных битов. Например, для маски .240 под Network ID отводятся 4 дополнительных бита. Они образуют 24=16 комбинаций (0000, 0001 … 1111). Второй шаг – исключение комбинаций, состоящих из всех нулей или единиц. Здесь две такие комбинации – 0000 и 1111. Останутся 14 комбинаций. Третий шаг – необходимо к Network ID добавить четыре бита для Host ID и преобразовать полученные числа в десятичный вид. Получается следующая таблица.

Таблица 2.6. Идентификаторы сети

Последний октет Network ID	Последний октет Network ID	Маска подсети
0001 0000	.16	255.255.255.240
0010 0000	.32	255.255.255.240
0011 0000	.48	255.255.255.240
…	…	…
1110 0000	.224	255.255.255.240

Определение значений Host ID

Также как и при определении Network ID, сначала необходимо выписать возможные комбинации Host ID. В нашем примере таких комбинаций будет 24=16. Далее, следует исключить Host ID, состоящие из комбинаций всех нулей или всех единиц. Останется 14 комбинаций. Составим таблицу для Network ID .16

Таблица 2.7. Классовая адресация

Последний октет Nework ID	Host ID	Последний октет IP адреса
0001 0000 (16)	0001 (1)	.17
0001 0000 (16)	0010 (2)	.18
…	…	
0001 0000 (16)	1110 (14)	.30

2.4. Объединение сетей

При объединении сетей часть битов Network ID переходит в Host ID. Это позволяет сокращать таблицы маршрутизаторов. Например, в организации 2000 узлов. InterNIC выделил для нее 8 сетей класса С. Каждая такая сеть может состоять из 254 узлов, что в сумме обеспечивает 2032 узла. Например, таблица маршрутизации выглядела бы следующим образом.

Таблица 2.8. Адреса подсетей

Network ID сети	Маска	IP адрес маршрутизатора
220.78.168.0	255.255.255.0	220.78.168.1
220.78.169.0	255.255.255.0	220.78.168.1
…		
220.78.174.0	255.255.255.0	220.78.168.1
220.78.175.0	255.255.255.0	220.78.168.1

При использовании CIDR таблица сократится:

Таблица 2.9. Адрес объединенной сети

Network ID сети	Маска	IP адрес маршрутизатора
220.78.168.0	255.255.248.0	220.78.168.1

Глава 3. Маршрутизация.

3.1. Понятие маршрутизации

Маршрутизация (routing) – это процесс, при помощи которого данные передаются узлу-адресату в другой сети. Роль маршрутизатора в сети сводится к просмотру поступающих пакетов и перенаправлению их в соответствующий пункт назначения. Маршрутизатор (router) – это устройство, распределяющее сетевой трафик. Маршрутизатор может быть как отдельным устройством, так и службой, запущенной на компьютере (например, NT Server или Unix). Так как маршрутизаторы позволяют взаимодействовать с другими сетями, они часто называются шлюзами (gateway). Маршрутизаторы содержат два или более сетевых интерфейса.

Маршрутизатор перенаправляет пакеты из одного своего интерфейса на другой, на основании таблицы маршрутизации. Таблица маршрутизации – это база данных, в которой хранятся соответствия между Network ID подсетей и интерфейсами маршрутизатора. Когда с какого-либо узла приходят данные, маршрутизатор проверяет таблицу. Если в ней указана сеть узла-адресата, то маршрутизатор передает пакет на соответствующий интерфейс. Если сеть не указана, данные передаются шлюзу по умолчанию.

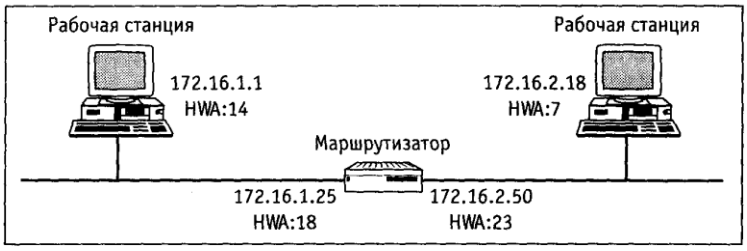

Рисунок 2.2. Стек TCP/IP

Например, пусть даны две подсети – 172.16.1.0 255.255.255.0 и 172.16.2.0 255.255.255.0 разделенные маршрутизатором. В первой подсети узел отправитель 172.16.1.1 (аппаратный адрес 14) и интерфейс 172.16.1.25 (аппаратный адрес 18). Во второй подсети узел получатель 172.16.2.18 (аппаратный адрес 7) и интерфейс 172.16.2.50 (аппаратный адрес 23).

Опишем алгоритм передачи данных от узла-отправителя к узлу-получателю.

1. Отправитель 172.16.1.1 проверяет, находится ли узел 172.16.2.18 в локальной сети.

2. Узел не находится в локальной сети, поэтому данные должны передаваться маршрутизатору (шлюзу по умолчанию).

3. При помощи ARP определяется аппаратный адрес шлюза по умолчанию. IP адрес шлюза должен быть задан при настройке TCP/IP на узле-отправителе.

4. 172.16.1.1 отправляет пакет данных на шлюз по умолчанию 172.16.1.25.

В заголовке содержатся:

MAC адрес отправителя: 14

IP адрес отправителя: 172.16.1.1

MAC адрес получателя: 18

IP адрес получателя: 172.16.2.18

5. Маршрутизатор, расположенный по адресу шлюза 172.16.1.25 и аппаратному адресу 18 определяет по заголовкам пакета подсеть назначения – 172.16.2.0.

6. Маршрутизатор при помощи ARP определяет аппаратный адрес узла-получателя 172.16.2.18. Полученный аппаратный адрес сохраняется в кэше для последующего использования.

7. Маршрутизатор отправляет в сеть 172.16.2 пакет с заголовком:

MAC адрес отправителя: 23

IP адрес отправителя: 172.16.1.1

MAC адрес получателя: 7

IP адрес получателя: 172.16.2.18.

8. Данные передаются от интерфейса маршрутизатора к узлу-получателю. Узел сравнивает MAC адрес получателя со своим, и при совпадении обрабатывает пакет.

Необходимо отметить, что IP адрес исходного узла и узла-адресата сохраняется в заголовке пакета во время передачи. Однако в качестве MAC адреса указан аппаратный адрес интерфейса последнего шлюза, через который в подсеть попал пакет. При передаче пакета по подсетям, IP адреса узлов отправителя и получателя не изменяются, а MAC адрес – изменяется.

Процесс маршрутизации усложняется, если в него вовлекаются несколько сетей. В этом случае активно используются таблицы маршрутизации.

Если пакет направляется в локальную сеть, то такой процесс называется прямой маршрутизацией (direct routing). Если пакет предназначен для удаленной сети, то он передается маршрутизатору. Такая маршрутизация называется косвенной (indirect). Благодаря существованию косвенной маршрутизации возможна иерархическая система маршрутизации. Сети с «плоской» адресацией на базе мостов и коммутаторов могут использовать только прямую маршрутизацию.

3.2. Таблицы маршрутизации

Существует два типа таблиц маршрутизации – статические и динамические. Статические таблицы изменяются вручную администраторами сети. Динамические таблицы маршрутизации создаются и поддерживаются автоматически при помощи протоколов маршрутизации.

Статическая маршрутизация

Статическая маршрутизация – встроенная функция IP. Она не требует каких-либо служб для своей работы. Статическая таблица должна

создаваться и поддерживаться на каждом маршрутизаторе вручную. Статическая таблица состоит из следующих пяти столбцов:

Адрес сети. Адрес каждой известной сети назначения.

Маска подсети. Маска подсети, используемая для каждой из сетей.

Адрес шлюза. IP адрес следующего шлюза (интерфейса маршрутизатора) для каждой сети.

Интерфейс. Адрес интерфейса маршрутизатора, на который нужно направить пакет.

Метрика. Число ретрансляций (хопов) для достижения сети.

Приведем пример простейшей статической таблицы маршрутизации.

Таблица 2.10. Пример таблицы маршрутизации

Network Address	Netmask	Gateway Address	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
0.0.0.0	0.0.0.0	198.21.17.7	198.21.17.5	1
56.0.0.0	255.0.0.0	213.34.12.4	213.34.12.3	15
116.0.0.0	255.0.0.0	213.34.12.4	213.34.12.3	13
129.13.0.0	255.255.0.0	198.21.17.6	198.21.17.5	2
198.21.17.0	255.255.255.0	198.21.17.5	198.21.17.5	1
198.21.17.5	255.255.255.255	127.0.0.1	127.0.0.1	1
198.21.17.255	255.255.255.255	198.21.17.5	198.21.17.5	1
213.34.12.0	255.255.255.0	213.34.12.3	213.34.12.3	1
213.34.12.3	255.255.255.255	127.0.0.1	127.0.0.1	1
213.34.12.255	255.255.255.255	213.34.12.3	213.34.12.3	1
224.0.0.0	224.0.0.0	198.21.17.5	198.21.17.5	1
224.0.0.0	224.0.0.0	213.34.12.3	213.34.12.3	1
255.255.255.255	255.255.255.255	198.21.17.5	198.21.17.5	1

Рассмотрим, из чего состоит минимальная таблица маршрутизации. Во-первых, это записи о сетях, непосредственно подключенных к маршрутизатору. В нашем случае это сети 213.34.12.0 и 198.21.17.0. А также запись маршрутизатора по умолчанию. В Windows NT это запись с адресом сети 0.0.0.0.

В таблицу также заносятся записи об адресах специального назначения. Например, это адрес 127.0.0.0 (loopback adapter). Пакеты, отправленные на адрес сети 127 не передаются протоколом IP на канальный уровень для последующей передачи в сеть. Записи с адресом 224.0.0.0 требуются для обработки групповых адресов (multicast address).

В таблицу могут быть добавлены адреса для обработки широковещательных рассылок. Например, адреса 198.21.17.255 255.255.255.255 и 213.34.12.255 255.255.255.255 содержат адрес отправки широковещательного сообщения в соответствующих подсетях, а последняя запись таблицы – адрес широковещательной рассылки сообщения.

Остальные записи в таблицу заносит администратор с помощью команды route.

В таблице маршрутизации может быть указано несколько шлюзов по умолчанию, но для маршрутизации будет использоваться только первый. Другие шлюзы будут использоваться, если основной шлюз отключен от сети или недостижим.

Необходимо запомнить, что для просмотра таблицы маршрутизации и ее исправления служит команда route. Для проверки маршрута и измерения времени прохождения пакетов до любого узла служит команда tracert.

Динамическая маршрутизация

Плоскими сетями на основе прямой маршрутизации невозможно управлять при дальнейшем росте сети, они плохо поддаются масштабированию. Дело в том, что в «плоской» сети все компьютеры видят друг друга. На практике же это не нужно, а иногда и вредно. Поэтому большие сети разбивают на подсети, перенаправлением пакетов между которыми и занимаются маршрутизаторы. Чтобы маршрутизаторы могли перенаправлять данные в другие сети, им нужны специальные протоколы, которые помогают строить карту окружающего пространства. Эти протоколы называются протоколами маршрутизации. Различают два вида протоколов: внутренние (Internal Gateway Protocol, IGP) и внешние (External Gateway Protocol, EGP). Внутренние протоколы работают внутри автономной системы, внешние – между автономными системами. Автономная система – это совокупность сетей и маршрутизаторов, расположенных в одном административном домене (находящихся под единым административным управлением). Например, если у вас есть несколько офисов в разных странах, то все они принадлежат к одному административному домену. Протокол EGP – это Border Gateway Protocol, BGP. Он используется только некоторыми провайдерами, большинство же провайдеров подключено по иерархической схеме с помощью статической маршрутизации.

Самые распространенные протоколы внутренней маршрутизации – это RIP (Routing Information Protocol) и OSPF (Open Shortest Path First). RIP использует алгоритм DVA («вектор-расстояние»), OSPF – алгоритм LSA («состояние связей»).

3.3. Протоколы маршрутизации

Протокол RIP

При использовании DVA сведения, посылаемые другому маршрутизатору оформляются как табличные элементы, имеющие вид «вектор, расстояние», где вектор – это номер сети, расстояние – количество маршрутизаторов, лежащих между маршрутизатором и конечной сетью. Расстояние часто называют метрикой (metric). Максимальный охват сетевого пространства для RIP – 15 маршрутизаторов. Расстояние, равное 16 означает

недостижимость сети. Протокол RIP поддерживает на маршрутизаторах таблицу, подобную статической таблице, с добавлением поля «возраст», которое показывает, сколько времени осталось до удаления элемента из таблицы. Также если маршрутизатор использует несколько протоколов маршрутизации, в таблицу добавляется поле, указывающее, по какому протоколу получена запись.

Некоторые элементы таблицы пересылаются через порты маршрутизатора для корректировки информации в других маршрутизаторах (в частности, об известных маршрутизатору сетях). Эти данные не маршрутизируются, поэтому они остаются внутри сетей, локальных рассылающему маршрутизатору. Любой маршрутизатор в этих сетях получает пакет и обновляет свою таблицу (если необходимо). То есть каждый маршрутизатор рассылает таблицу через все активные порты. По мере получения таблиц маршрутизаторы строят карту сети, после каждой рассылки в сети накапливается все больше информации, в конце концов все маршрутизаторы будут знать обо всех сетях в своем пространстве. Существуют три причины, по которым маршрутизатор будет корректировать свою таблицу:

1. Если полученная таблица содержит сеть, в которой меньше переходов. Маршрутизатор заменяет элемент своей таблицы новым элементов с меньшим количеством переходов.

2. Если в полученную таблицу входит сеть, которой нет в собственной таблице. Тогда маршрутизатор добавляет новую запись.

3. Если маршрутизатор перенаправляет пакеты для некоторой сети через конкретный маршрутизатор, и количество переходов от этого маршрутизатора до целевой сети изменяется, наш маршрутизатор изменит элемент своей таблицы.

Если в сети используется один маршрутизатор, то он указывается как «шлюз по умолчанию», и рабочие станции посылают пакеты для внешних сетей на этот шлюз. Если же маршрутизаторов в сети несколько, то рабочая станция должна также выполнять маршрутизацию. Поэтому существует два варианта работы протокола RIP: активный и пассивный. Второй предназначен для рабочей станции, при этом станция только «слушает» сеть и строит свою таблицу, но не рассылает маршрутную информацию.

Кроме широковещательной рассылки протокол RIP предусматривает и режим запроса, когда маршрутизатор может запросить часть таблицы у другого маршрутизатора. Поэтому существует два вида пакетов RIP – для запроса и для ответа.

В пакете RIP v1 присутствуют следующие поля

1. Версия протокола.

2. Семейство сетевых протоколов – для указания протоколов, работающих на сетевом уровне. RIP применяется как с IP, так и с IPX, AppleTalk, XNS.

3. IP адрес целевой сети. Заполняется запрашивающей станцией.

4. Следующая часть пакета показывает IP адреса и метрики. Всего пакет может нести запись о 25 сетях.

Для своей работы RIP использует UDP, порт 520.

Всеобщее признание первой версии протокола RIP в Интернете было следствием его применения в BSD UNIX в виде программы routed. До реализации RIP таблицы маршрутизаторов должны были строиться вручную, RIP же предоставил возможность динамического построения таблиц. Однако у первой версии существуют значительные недостатки.

1. RIP умеет работать только с кратчайшими маршрутами. Предположим, если существует два маршрута: первый – через две волоконно-оптические линии (два хопа), а второй – через модемную линию (один хоп), то RIP будет считать второй маршрут лучшим. Некоторые версии RIP преодолевают этот недостаток с помощью «утяжеления» нежелательных маршрутов. Однако искусственное увеличение числа хопов приводит к достижению предела в 15 хопов.

2. Информация RIP верна настолько, насколько точен приславший ее маршрутизатор. Если произойдет ошибка маршрутизатора, она будет всеми получена и обработана.

3. Маршрутные таблицы могут становиться очень большими. Рассмотрим сеть, состоящую из 300 подсетей. Любая таблица содержала бы 300 элементов. Максимальный же размер пакета RIP – 512 кб, что позволяет посылать данные о 25 сетях. Таким образом, маршрутизатор будет использовать 13 пакетов для рассылки информации всем остальным маршрутизаторам. Такая рассылка производилась бы всеми 300 маршрутизаторами каждые 30 секунд. Даже при условии, что конфигурация сети не изменилась.

Существуют и другие ограничения, на которых мы не будем подробно останавливаться.

В 1994 году вышла вторая версия протокола RIP v2, обратно совместимая с первой. В ней реализовано несколько новых возможностей и исправлены недостатки первой версии.

Протокол OSPF

Кроме RIP разрабатывались и другие протоколы. Сам RIP обладал существенными недостатками, что ограничивало его применение. Протокол OSPF (открой кратчайший путь первым) начал разрабатываться в 1978 году. Можно выделить следующие основные особенности OSPF.

1. Для оценки маршрутов используется истинная метрика, а не количество переходов.

2. Маршрутные таблицы рассылаются по адресам и только при необходимости.

3. Реализовано распределение нагрузки по нескольким путям.

4. Поддерживается тип службы (Type of Service)

4.1. Протокол DHCP

Протокол DHCP (Dynamic Host Configuration Protocol) был разработан для преодоления такого недостатка TCP/IP, как отсутствие возможности централизованного управления IP адресами. DHCP является надстройкой над протоколом BOOTP (Bootstrap Protocol), который ранее использовался для динамического выделения IP адресов и передачи файлов на бездисковые станции. BOOTP разрабатывался для той же цели, что и DHCP, но оказался далеко не столь удобным как ожидалось. Самое крупное преимущество DHCP перед BOOTP – возможность динамического распределения IP адресов. Это дает возможность распределения адресов между компьютерами по мере их подключения к сети, не заставляя администратора заранее резервировать IP-адреса для всех компьютеров. Кроме того, DHCP позволяет передавать клиентам больше параметров конфигурации чем BOOTP.

DHCP обеспечивает автоматическую установку IP адреса и маски подсети, шлюза по умолчанию, адреса одного или нескольких серверов DNS и другие параметры.

Сеть может работать и без сервера DHCP, но в этом случае необходимо вводить параметры настройки TCP/IP на каждом компьютере. Пользователь сам вводит адрес, что может привести к многочисленным ошибкам, которые сложно бывает локализовать. При перемещении компьютера из одной сети в другую необходимо также вручную изменять параметры настройки.

Работа протокола DHCP в сети контролируется сервером DHCP, который выполняет запросы клиентов и отвечает за то, чтобы в сети не было повторяющихся IP адресов. В сети может содержаться неограниченное число DHCP серверов, каждому серверу должен быть выделен свой диапазон (scope) IP адресов. Если эти диапазоны совпадают или перекрываются, возникает опасность появления в сети совпадающих IP адресов.

Использование DHCP сервера в сети имеет следующие преимущества.

1. Администратор задает параметры TCP/IP централизованно.
2. Не нужно настраивать параметры на клиентах вручную.
3. При перемещении компьютера между сетями его старый адрес освобождается. Клиент автоматически переконфигурирует параметры TCP/IP при загрузке компьютера.
4. Большинство маршрутизаторов могут пересылать BOOTP/DHCP запросы, так что нет необходимости устанавливать DHCP сервер в каждой подсети.

Аренда DHCP и ее продление

Когда клиент для своей настройки использует DHCP, он арендует (lease) у сервера IP адрес на определенное время. Когда срок DHCP аренды подходит к концу, клиент может продлить аренду. Процесс получения аренды IP адреса состоит из четырех шагов.

1. Запрос аренды. Клиент отправляет широковещательное сообщение на локальный сегмент сети. Так как клиент не имеет своего собственного IP адреса, в пакете указывается адрес 0.0.0.0 в качестве адреса отправителя и адрес 255.255.255.255 в качестве адрес получателя. Такой пакет называется DHCP запросом DCHPDISCOVER и, кроме аппаратного адреса отправителя, содержит еще и имя клиента, которое будет использоваться на втором шаге. Сообщение может содержать и другую информацию, например выделенный ранее IP адрес.

Процесс запроса используется в трех случаях:

а. Происходит первая инициализация TCP/IP на клиенте DHCP.

б. Клиент запросил определенный адрес и получил отказ, вероятно по причине окончания аренды на DHCP сервере.

в. Клиент уже арендовал IP адрес, но освободил его и запрашивает новый.

Запрос аренды может передаваться через маршрутизатор, если на нем разрешена ретрансляция BOOTP пакетов.

Например, клиент посылает пакет DHCPDISCOVER, содержащий.

IP адрес отправителя: 0.0.0.0

IP адрес получателя: 255.255.255.255

Данные: Адрес сетевого адаптера отправителя: 08004…

Имя: PC1

2. Второй шаг – предложение аренды. Каждый сервер DHCP ищет в своих таблицах размещение клиента. Если адрес найден, сервер отвечает сообщением DHCPOFFER, в котором записаны аппаратный адрес клиента, предлагаемый IP адрес и маска подсети, срок аренды, IP адрес сервера и другая информация о конфигурации. Пакет посылается широковещательно, поскольку клиент еще не имеет своего IP адреса. Клиент берет IP адрес из первого полученного предложения. DHCP сервер, предложивший IP адрес, временно резервирует адрес для избежания присвоения одного адреса нескольким клиентами.

Клиент ждет предложения 1 с. Если предложение не пришло, клиент посылает еще три запроса. Если после четырех запросов ответа не пришло, клиент возобновляет попытки каждые 5 минут.

Пакет DHCPOFFER может выглядеть следующим образом:

IP адрес отправителя: 131.107.3.24

IP адрес получателя: 255.255.255.255

Данные:

Предлагаемый IP адрес: 131.107.8.13

Адрес сетевого адаптера клиента: 08004…

Маска подсети: 255.255.255.0

Продолжительность аренды: 72 часа

Идентификатор сервера: 131.107.3.24

Клиенты Windows 2000 могут автоматически настроить IP адрес и маску подсети, если DHCP сервер недоступен при загрузке. Эта возможность

называется Automatic Private IP Addressing (APIPA). Она полезна для клиентов в небольших сетях и работает следующим образом.

1. DHCP-клиент пытается найти DHCP сервер и получить адрес и параметры.

2. Если DHCP сервер не найден и не отвечает, клиент автоматически настраивает свой IP адрес и маску подсети, используя диапазон 169.254.0.0 с маской 255.255.0.0, зарезервированный за Microsoft. Клиент проверяет, используется ли выбранный адрес в сети. При обнаружении конфликта клиент выбирает другой адрес.

3. Если адрес выбран успешно, то сетевой интерфейс настраивается под данный адрес. После этого клиент в фоновом режиме проверяет наличие DHCP сервера каждые 5 минут. Если сервер будет обнаружен, клиент откажется от прежней конфигурации и будет использовать полученный от DHCP сервера.

3. Выбор аренды. Клиент принимает первое полученное предложение, после чего отправляет сообщение DHCPREQEST. Это широковещательное сообщение содержит адрес сервера DHCP, предложение которого принято. Все другие серверы DHCP при этом отменяют сделанные ими предложения.

Пакет DHCPREQEST может выглядеть следующим образом:

IP адрес отправителя: 0.0.0.0

IP адрес получателя: 255.255.255.255

Данные:

Адрес сетевого адаптера: 08004…

Запрашиваемый IP адрес: 131.107.8.13

Идентификатор сервера: 131.107.3.24

4. Подтверждение аренды. Сервер выделяет клиенту данный IP адрес и отправляет DHCPACK сообщение (подтверждение), после чего клиент использует выданный IP адрес. В сообщении может быть указана какая-либо дополнительная информация. Если сервер по какой-либо причине не принимает сообщение DHCPREQUEST, он отвечает негативным подтверждением DHCPNACK, после чего процесс повторяется с самого начала.

Например, пакет DHCPACK может выглядеть следующим образом:

IP адрес отправителя: 131.107.3.24

IP адрес получателя: 255.255.255.255

Данные:

Предлагаемый IP адрес: 131.107.8.13

Адрес сетевого адаптера клиента: 08004…

Маска подсети: 255.255.255.0

Продолжительность аренды: 72 часа

Идентификатор сервера: 131.107.3.24

Дополнительная информация о настройке

Аренда может быть прекращена пользователем вручную при помощи команды ipconfig /release. Команда ipconfig /renew принуждает клиента к отправке сообщения DHCPREQUEST на сервер.

4.2. Планирование и реализация DHCP

Перед тем, как начать эксплуатацию DHCP сервера, следует ответить на несколько вопросов.

1. Все ли компьютеры будут использовать DHCP? Если нет, то следует исключить из раздаваемых DHCP сервером адресов статические адреса клиентов. Если клиенту нужен конкретный адрес, то он должен быть зарезервирован.

2. Будет ли сервер работать на несколько подсетей? В таком случае необходимо настроить ретрансляцию BOOTP/DHCP на маршрутизаторах.

3. Сколько потребуется DHCP серверов? Следует учесть, что DHCP сервер не обменивается информацией с другими DHCP серверами. Поэтому каждый сервер должен иметь свой уникальный диапазон. Microsoft рекомендует использовать не менее двух серверов DHCP. Если один из серверов выйдет из строя, работа сети не прекратится.

4. Какие параметры IP-адресации будут получать клиенты от DHCP сервера?

Настройка DHCP

Со стороны клиента следует установить переключатель «Получить IP-адрес автоматически» в окне свойств TCP/IP.

На сервере следует запустить службу DHCP-сервера. Установка и настройка будет рассмотрена на лабораторной работе.

В Windows 2000 DHCP сервер необходимо авторизовать сервер в Active Directory.

Реализация DHCP на нескольких подсетях

Рассмотрим пример реализации DHCP на нескольких подсетях.

Предположим, сеть состоит из двух подсетей, каждая из которых использует свой DHCP сервер. Подсети соединяются маршрутизатором, пропускающим BOOTP пакеты. Microsoft рекомендует чтобы каждый DHCP сервер отводил 75% IP адресов под локальную сеть и 25% под удаленную сеть. Рабочие станции в нормальных условиях будут получать IP адрес от локального DHCP сервера, так как он ответит быстрее. При поломке локального DHCP сервера, станции могут получить адрес из 25% пула удаленного DHCP сервера.

Например, для подсети А выделен диапазон адресов 120.50.7.10 – 120.50.7.110 и диапазон 120.50.8.10-120.50.8.110 для подсети В. Конфигурация пулов каждого сервера будет следующая:

Сервер подсети А:

120.50.7.10-120.50.7.84 и 120.50.8.10-120.50.8.34

Сервер подсети B:
120.50.7.85-120.50.7.110 и 120.50.8.35 – 120.50.8.110
Следует обратить внимание, что пулы адресов нигде не пересекаются.

Недостатки DHCP

Хотя DHCP сильно помогает администратору сети и позволяет централизованно менять все важные параметры, он имеет ряд недостатков.

1. Спецификации DHCP являются недостаточно жесткими. Клиент не обязан включать все параметры конфигурации, присланные сервером. Для избежания несогласованных и неизвестных параметров, надо каждый раз проверять, какие параметры могут обрабатываться используемыми в текущий момент программами клиента.

2. DHCP не интегрирован с DNS и требует наличия сервера DNS. Особенно это ощущается при переходе к Windows 2000. DHCP и DNS не обмениваются информацией и возможны ситуации, когда DHCP сервер изменит все IP адреса без ведома DNS сервера (следовательно, без обновления таблицы DNS). Обмен информацией мог бы сильно облегчить регистрационную работу.

3. Самая большая проблема связана с работоспособностью DHCP. Текущая спецификация DHCP не позволяет использовать резервные серверы для службы DHCP, так как не существует протокола взаимодействия типа сервер-сервер. Таким образом, единственный способ обеспечения надежности состоит в том, чтобы осуществить разбиение конкретного пространства IP адресов на большое количество независимых частей и распределить их по разным серверам DHCP.

Недостатком такой процедуры является нерациональное использование IP адресов и увеличение накладных расходов, связанных с регистрацией DHCP.

В группе по созданию DHCP ведется работа над протоколом сервер-сервер, который позволит создавать резервные серверы DHCP.

4. Защита DHCP несовершенна. Можно установить несанкционированные серверы, которые смогут перехватывать запросы клиентов и сообщать ложную информацию о конфигурации. Клиент будет использовать тот адрес, который получит первым. Проблемы защиты мешают широкому внедрению DHCP.

Глава 5. Доменная система имен

5.1. Понятие доменной системы имен (DNS).

Как известно, любой узел в TCI/IP сети должен иметь свой IP адрес. Для того, чтобы обратиться на этот узел, необходимо знать IP адрес. Но пользователю проще запоминать имена, а не цифры. Поэтому существует возможность присвоить имя каждому TCP/IP узлу. Хотя имена и проще запомнить, для взаимодействия двух узлов должна существовать система обратного преобразования имени в IP адрес.

Раньше соответствие имен узлов и IP адресов записывалось в файле HOSTS. Каждый узел должен был периодически получать обновленную копию файла HOSTS. С ростом числа компьютеров этот процесс стал неконтролируемым. В результате была создана распределенная база данных DNS (Domain Name System), заменившая HOSTS файл. DNS обладает иерархией имен, обеспечивает распределенное администрирование, расширяемые типы данных, поддерживает практически неограниченный объем данных и обладает высоким быстродействием.

Помимо применения в Интернете, DNS является основной службой имен в Windows 2000. Клиенты Windows 2000 используют DNS для разрешения имен и поиска служб. DNS сервер Windows 2000 обладает своими особенностями, однако он совместим с другими стандартными реализациями DNS.

Задача DNS заключается в трансляции имен компьютеров в IP адреса. Клиент DNS называется распознавателем, серверы – серверами имен. DNS включает три основные компонента: распознаватели, серверы имен и пространство имен домена. В простейшем случае распознаватель посылает запрос серверу DNS, который возвращает требуемую информацию, либо указатель на другой сервер имен, либо отказ.

Задача распознавателя – передать запрос разрешения имени от приложения к серверу DNS. Распознаватель может быть встроен в приложение или запускаться как отдельная процедура. Первоначально распознаватели посылают запросы по протоколу UDP и переходят на TCP только при потере данных.

Серверы имен содержат информацию об адресах компьютеров в сети, которая передается клиентам в ответ на запросы. Если сервер не способен разрешить запрос, он может перенаправить его другому серверу DNS. Серверы имен состоят во главе доменов – логических групп компьютеров.

Иерархия в базе имен DNS определяется доменами. Вершина иерархии называется корневым доменом, его обозначают точкой. Далее следуют домены верхнего уровня (com, edu, etc), которые могут содержать как домены второго уровня, так и узлы. Домены второго уровня могут содержать как и другие домены, называемые поддоменами, так и узлы.

Имя домена вместе с именем узла образует полное доменное имя (fully qualified domain name, FQDN). К имени узла добавляется точка, и затем – имя домена. FQDN однозначно определяет компьютер в сети.

В соответствии с RFC 1123, существуют ограничения на символы, которые могут применяться в именах TCP/IP узлов. Полное имя узла может содержать до 255 буквенных символов, включая a-z, A-Z, 0-9, дефис (-) или точку (.). Остальные символы не допускаются. Кроме того, имя узла не может состоять только из цифр.

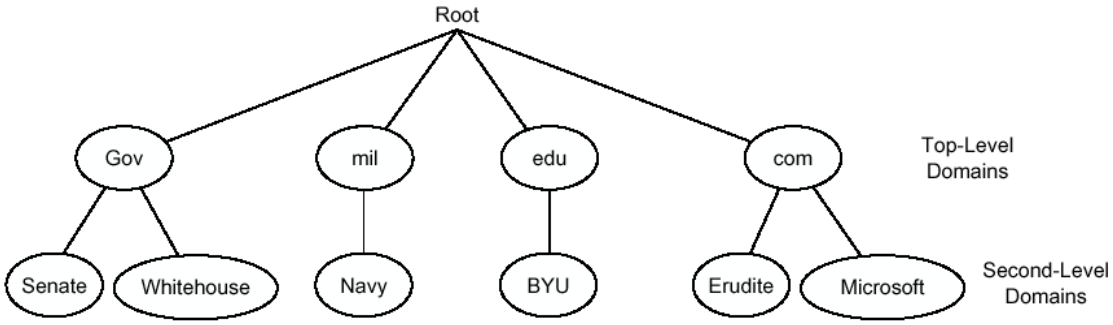

Рисунок 2.3. Узлы DNS

Для администрирования пространства имен DNS используются зоны. Зона – административная единица DNS, поддерево в базе данных DNS, которое администрируется отдельно. Зона может состоять как из простого домена, так и из домена с поддоменами. Поддомены зоны также разрешается разбивать на отдельные зоны.

Зоной полномочий сервера DNS называется часть пространства имен домена, за которую отвечает один сервер имен. Он хранит все привязки адресов для пространства имен в рамках зоны и обрабатывает клиентские запросы. В состав зоны полномочий сервера входит минимум один домен – корневой домен зоны. Может существовать дополнительный сервер DNS, на который копируется информация зоны с основного сервера. Процесс копирования называется передачей зоны.

Разбиение домена на зоны требуется для делегирования управления доменом нескольким группам пользователей и повышения эффективности репликации данных.

Серверы DNS могут выполнять несколько ролей. Сервер DNS Microsoft может быть как основным, так и дополнительным сервером DNS, в том числе и для серверов с другими ОС. Для каждой зоны рекомендуется использовать минимум два сервера – основной и дополнительный.

Основные серверы имен получают информацию о своей зоне с локальных файлов DNS. Если в базе происходят изменения, их необходимо вносить на основном сервере DNS, чтобы обновления были отражены в локальном файле зоны.

Дополнительные серверы DNS получают данные от основных серверов DNS. Процесс копирования файла зоны с основного на дополнительный сервер называется передачей зоны.

Использование дополнительных серверов дает три преимущества:

Избыточность – рекомендуется использовать минимум два сервера – основной и дополнительный, чтобы обеспечить работу зоны даже в случае отказа одного сервера.

Быстрый доступ удаленных клиентов – для обслуживания крупной группы удаленных клиентов рекомендуется использовать дополнительный сервер DNS, который ускорит разрешение имен.

Снижение нагрузки – дополнительный сервер снижает нагрузку на основной сервер.

Информация о каждой зоне хранится в отдельном файле. Поэтому сервер DNS может быть основным сервером для одних зон, и дополнительным – для других.

Серверы кэширования. Хотя все DNS серверы могут кэшировать запросы, некоторые выделяются исключительно для этой цели. В их зону полномочий не входит ни один домен (то есть они не хранят файлы зоны). Они содержат данные, накопленные при разрешении запросов.

С помощью утилиты hostname можно посмотреть имя узла, а с помощью ipconfig /all – имя FQDN. Первое имя в FQDN слева – имя локального узла.

5.2. Процесс разрешения имен и структура файлов DNS

Клиент может выполнять запросы трех типов: рекурсивные, итеративные и обратные. Серверы DNS хранят информацию в файлах четырех типов: файлах базы данных, файлах обратного просмотра, кэш-файлах и загрузочных файлах.

В ответ на рекурсивный запрос сервер имен должен возвратить требуемые данные либо сообщение об ошибке. Сервер не может переслать рекурсивный запрос другому серверу имен.

В ответ на итеративный запрос сервер имен дает наилучший возможный ответ. Либо сервер разрешает запрос, либо дает ссылку на другой сервер, который может ответить на данный вопрос.

Итеративные запросы в случае обычно осуществляются между серверами, что можно проиллюстрировать на следующем примере.

Клиент запрашивает у DNS сервера IP адрес, соответствующий узлу www.whitehouse.gov.

1. DNS клиент посылает локальному серверу DNS рекурсивный запрос, в котором просит определить IP адрес для узла www.whitehouse.gov. Локальный сервер DNS отвечает за распознавание имени и не может перенаправить клиента к другому DNS серверу.

2. Локальный DNS-сервер просматривает свои зоны и не ходит зону, содержащую указанное имя домена. Тогда он посылает к корневому серверу имен итеративный запрос об узле www.whitehouse.gov.

3. Корневой DNS сервер, ответственный за корневой домен, возвращает IP адрес сервера имен для домена верхнего уровня .gov.

4. Локальный DNS сервер посылает DNS серверу домена .gov итеративный запрос о www.whitehouse.gov.

5. DNS сервер домена .gov возвращает IP адрес сервера имен, обслуживающего домен whitehous.org.

6. Локальный DNS сервер посылает DNS серверу домена whitehouse.gov итеративный запрос о www.whitehouse.org.

7. DNS сервер домена whitehouse.gov возвращает IP адрес, соответствующий www.whitehouse.gov.

8. Локальный DNS сервер посылает клиенту IP адрес www.whitehouse.gov.

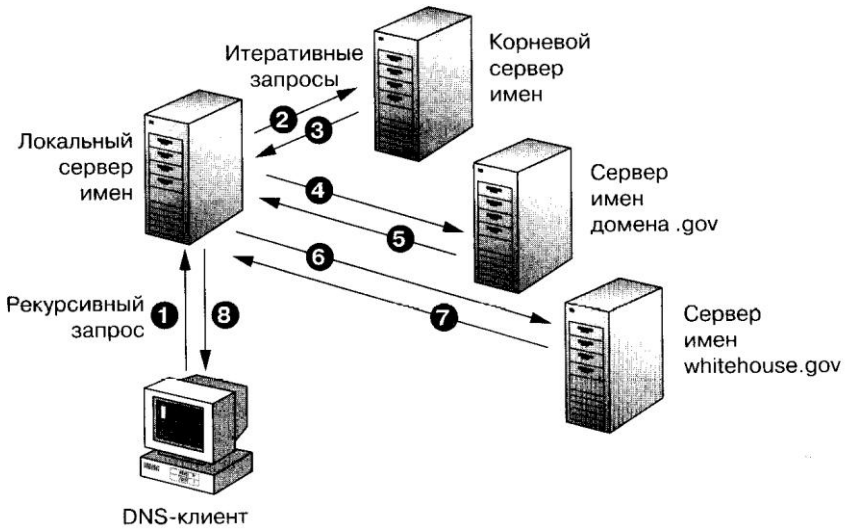

Рисунок 2.4. Пример запроса адреса

Обратные запросы происходят если требуется решить обратную задачу: узнать имя узла по его IP адресу. Поскольку между IP адресом и именем домена корреляции не существует, то ответ можно получить, лишь выполнив просмотр по всем доменам.

Для предотвращения полного просмотра всех доменов создан специальный домен in-addr.arpa. Домен in-addr.arpa поддерживает список соответствий имен IP адресам. Особенность этого списка заключается в том, что IP адреса записаны в обратном порядке. Например, IP адрес 205.240.248.93 узла product.aus-tx.saturn.com должен быть записан как 93.248.240.205.in-addr.arpa. Обратный порядок связан в тем, что иерархия в IP адресе считается слева направо, а в имени DNS – справа налево, поэтому управление ветвями домена in-addr.arpa можно делегировать организациям, которым присвоены адреса классов A, B, C.

Если клиент получает сеть класса C 192.168.1.0, то зона для обратного разрешения имен будет называться 1.168.192.in-addr.arpa.

После построения домена in-addr.arpa, в него добавляются записи указателей ресурсов (PTR), связывающие IP адреса с соответствующими именами узлов.

Кэширование и время жизни

При обработке рекурсивного запроса иногда требуется несколько попыток для его разрешения. DNS кэширует полученную в этом процессе информацию и хранит ее в течение времени, указанного в возвращенных данных. Это – время жизни (TTL, time to live). Время жизни для данных задает администратор сервера имен зоны. Малые значения TTL обеспечивают большую достоверность данных в сети, если изменения происходят часто. Однако это увеличивает нагрузку на серверы DNS.

После получения данных сервером DNS, он начинает понижать их TTL с первоначального значения, чтобы знать, когда удалить данные из кэша. Если приходит вопрос, который может быть разрешен данными кэша, то возвращаемое TTL означает время, оставшееся до удаления данных из кэша сервера DNS. Распознаватели клиента также кэшируют данные и учитывают TTL, поэтому они знают, когда данные устаревают.

5.3. Интеграция DNS с DHCP

Хотя DHCP обеспечивает мощный механизм автоматической настройки IP адреса клиента, до недавнего времени DHCP не извещал службу DNS об обновлении DNS записей клиентов, а именно привязок IP-адрес/имя и имя/IP-адрес.

В Windows 2000 DHCP серверы и клиенты могут взаимодействовать, если сервер поддерживает обновления динамической системы доменных имен (Dynamic DNS, DDNS). DHCP сервер Windows 2000 может зарегистрировать на DNS сервере и обновить записи ресурсов узла (A) и записи ресурсов указателя (PTR) для своих DHCP-клиентов с помощью протокола обновлений DDNS.

DHCP и статическая служба DNS не способны синхронизировать информацию о привязках имя-IP адрес, что вызывает проблему при использовании DHCP и DNS.

Глава 6. Служба каталогов Active Directory

6.1. Понятие службы каталогов Active Directory

Active Directory – одна из самых интересных новинок в Windows 2000. Она является службой каталогов, обеспечивающей администраторов гибким и мощным механизмом для облегчения многих ежедневных обязанностей.

Каталог является базой данный, содержащей информацию об объектах (objects) и их атрибутах (attributes). Служба каталогов организует объекты в доступную логическую структуру и обеспечивает средство поиска их в каталоге. Любой объект может быть контейнером, то есть содержать в себе другие объекты. Мир объектов определяется схемой (schema), являющейся набором правил. В AD схема – это набор экземпляров классов объектов, хранящихся в каталоге. Приложения могут изменять схему, добавляя в нее новые атрибуты и классы. Изменение схемы сопровождается созданием или модификацией объектов, хранящихся в каталоге.

Служба каталогов обеспечивает лучшую масштабируемость чем доменная система NT 4.0, позволяет создавать миллионы объектов в домене, в отличие от 40.000 в NT 4.0.

Active Directory имеет некоторые преимущества, делающие ее глобальной службой каталога: поддержка Интернета и промышленных стандартов, таких как LDAP, DNS, DHCP и TCP/IP. А также центральное управление через единый интерфейс управления, MMC (Microsoft Management Console). AD не является каталогом X.500, она лишь использует ее информационную модель без избыточности.

Служба каталогов AD имеет как физическую структуру, определяемую сайтам (sites), так и логическую структуру, определяемую доменами (domains). Домен – организационная единица безопасности в сети. Домен может охватывать несколько физических точек. В каждом домене своя политика безопасности и отношения с другими доменами. Доменная структура иерархическая, домены, объединенные общей схемой, конфигурацией и глобальным каталогом образуют дерево (tree). Объекты на концах дерева называются листьями, они не содержат других объектов. Сами деревья объединяются в леса (forests).

Данные каталога включают в себя информацию о домене (domain data), о конфигурации (configuration data) и схеме (scheme data). Все эти данные реплицируются на все контроллеры домена, каждый из них имеет копию каталога на своем жестком диске в режиме чтения/записи.

Домены Windows 2000 используют иерархическую модель с родительским доменом (parent domain) и дочерними доменами (child domain). Одно доменное дерево состоит из родительского домена и всех дочерних. Имена доменов выбираются в соответствии со схемой именования DNS в Интернете. К примеру, если родительский домен называется vspu.kirov.ru, то дочерний домен будет train.vspu.kirov.ru. Доверительные отношения между доменами реализуются автоматически с помощью двусторонних, или

транзитивных отношений. Если домен A доверяет домену B, домен B доверяет домену C, то домен A будет доверять домену C. Также можно установить односторонние доверительные отношения или вообще их убрать. По умолчанию, права дочерних объектов наследуются от родителя (inheritance). Но наследование может быть заблокировано для отдельных объектов или классов объектов. Внутри каждого домена может быть иерархия организационных единиц OUs.

6.2. Структура Active Directory

Леса и деревья

База данных AD содержит всю информацию об объектах всех доменов: от паролей пользователей до объектов каталога. Иерархическая структура, состоящая из множества доменов, связанных доверительными отношениями, называется деревом (tree). Набор классов объектов и их атрибутов называется схемой (schema). Все домены в дереве разделяют одинаковую схему, единый глобальный каталог и имеют смежное пространство имен (namespace). Смежное пространство имен - это набор доменов, имеющих одинаковое корневое имя. Например, train.vspu.kirov.ru, teacher.vspu.kirov.ru, и eugene.vspu.kirov.ru. Разъединенное пространство имен может содержать взаимосвязные домены, но корневое имя домена у них будет разное. Такое происходит, если, например, две компании объединяются в одну. Например, vspu.kirov.ru и politeh.kirov.ru. Лес (forest) это одно или больше доменных деревьев, имеющих различные пространства имен. Все деревья в лесу разделяют общую схему, единый глобальный каталог и связаны транзитивными доверительными отношениями. Если у вас есть несколько лесов, то вы должны установить доверительные отношения между ними.

Сайты

Для управления сайтами используется консоль MMC и оснастка «Active Directory Sites and Services». Чтобы создать сайт, следует добавить подсети с контроллерами доменов в объект «сайт». Объект «сайт» – это набор адресов подсетей, которые принадлежат к одному физическому местоположению. Сайты могут охватывать домены, и домены могут охватывать сайты. Если адрес подсети клиента или контроллера домена не был включен ни в какой сайт, он считается принадлежащим изначально созданному контейнеру сайта Default-First-Site. Для быстрого доступа подсети к каталогу, ее необходимо включить в сайт. В каждом сайте, должен быть установлен, по крайней мере, один сервер глобального каталога (global catalog) для быстрого доступа к каталогу, и по крайней мере, один контроллер домена.

Для поиска ближайших ресурсов или контроллеров домена, клиенты могут использовать информацию о сайте. Если пользователь перемещается со своей рабочей станцией в новое место, то при входе в сеть она обращается к прежнему контроллеру домена. В этом случае он не является ближайшим и

сообщает клиенту о ближайшем сайте. Клиент дальше может обратиться к контроллеру домена в его собственном сайте и работать с ним, как с ближайшим контроллером. Эта информация будет задействована при следующем входе в есть.

Динамический DNS (DDNS)

AD требует установки DDNS для разрешения имен объектов. Записи в базе данных DNS автоматически обновляются вместо привычных в DNS ручных способов. DNS очень тесно интегрирована в AD, и информация о зонах DNS может быть тиражирована через стандартные механизмы или через AD, используя режим интегрирования зоны с AD (directory-integrated zone storage). Это облегчает тиражирование, поскольку переносит его на механизм AD.

Организационные единицы (OUs)

OU – контейнерный объект, который может содержать пользователей, группы, принтеры и другие объекты, причем все они должны быть членами того же домена, что и OU. OUs – наименьшая административная единица в каталоге. С помощью OUs можно организовывать логические административные группы в домене. OUs позволяют передать управление объектами внутри себя другим пользователям. Например, можно создать группу пользователей и в рамках этой группы назначить администратором определенного человека. Он не будет иметь полномочий в рамках группы, но в пределах подразделения он будет обладать всей полнотой власти. Также на OU можно присваивать отличные от домена разрешения. OU – минимальная области применения политики. Для управления OU используется оснастка MMC The Active Directory Users And Computers. Для передачи управления OU используется Delegation of Control Wizard.

Глобальный каталог (Global Catalog)

Глобальный каталог содержит все объекты в AD, а также их атрибуты (в сокращенном виде). Это позволяет легко найти объект даже в большом многодоменном окружении. Глобальный каталог служит индексом для полной структуры всех доменов и деревьев в лесу. Он также используется для аутентификации пользователей, так что пользователь может входить в любом месте системы без непосредственного обращения к своему домашнему домену. Первый сервер в дереве называется сервером глобального каталога. Дополнительные серверы глобального каталога улучшают время реакции на запросы AD объектов. Для создания дополнительных серверов каталога следует использовать оснастку «Active Directory Sites and Services».

Контроллеры домена (domain controllers)

Все контроллеры домена в Windows 2000 доменах обладают полноценной копией базы AD. Все изменения, произведенные на одном

контроллере домена, тиражируются на все другие контроллеры в этом домене через много-мастерное тиражирование. Много-мастерное тиражирование осуществляется при отсутствии главного контроллера домена (master domain controller) и все контроллеры домена считаются равными. Контроллеры домена не нуждаются в тиражировании напрямую каждый с каждым. Ближайшие друг с другом контроллеры произведут тиражирование между собой, и далее один из них произведет тиражирование с удаленным контроллером домена.

Тиражирование (replication)

AD использует тиражирование с несколькими ведущими узлами (multimaster). Однако некоторые операции могут выполняться только в системе с одним ведущим узлом (single-master). Для этих целей существует пять специальных ролей, каждая из которых присваивается одному доменному контроллеру в лесу или в домене (в зависимости от роли). Такие контроллеры называются мастерами операций (operations master). Приведем их список: мастер схемы (schema master), мастер доменных имен (domain naming master), мастер инфраструктуры (infrastructure master), RID мастер и эмулятор PDC. Мастер схемы и мастер доменных имен должны существовать в единичном количестве в лесу доменов. Остальные мастеры должны существовать в единичном количестве в домене. Мастер доменных имен позволяет добавить в лес новый домен или исключить его из леса. Мастер схемы отвечает за изменение схемы. Мастер RID отвечает за уникальность номеров RID (связано с безопасностью и будет рассмотрено позднее). Для того, чтобы перенести объект из одного домена в другой, должен быть задействован мастер RID. Эмулятор PDC выполняет функции контроллера домена для поддержки старой модели доменов Windows NT. Или при native-mode он в первую очередь принимает оповещение с других контроллеров о смене пароля. Это помогает аутентифицировать пользователя в переходный период, когда изменение пароля еще не дошло до домена, на котором происходит аутентификация. Мастер инфраструктуры следит за членством пользователей в группах.

Много-мастерный механизм тиражирования позволяет передавать данные из каталога по сети. Любые изменения, внесенные в каталог на одном из контроллеров, тиражируются на остальные контроллеры в домене. Для тиражирования AD использует объект «соединение» (connection object). Объекты «соединение» устойчивы к сбоям. Когда происходит отказ в связи, AD сама произведет реконфигурацию для выявления другого маршрута для выполнения тиражирования. Процесс, который создает объекты «соединение», называется Knowledge Consistency Checker (KCC). Он запускается на всех контроллерах домена каждые 15 минут (по умолчанию). Он создает объекты «соединение», которые обеспечивают наилучший маршрут для тиражирования. KCC использует имеющуюся модель сети для выявления связей между сайтами, но связи между контроллерами домена в пределах одного сайта он находит сам. Изменения, которые должны быть

тиражированы, имеют свой последовательный 64-битный номер update sequence number (USN). Каждый контроллер домена содержит таблицу где записана последовательность как собственных USN, так и USN партнеров по тиражированию. Таблица обновляется при внесении изменений к AD объекту. Другие контроллеры используют этот USN для определения факта изменения базы на партнерах по тиражированию. Для уменьшения сетевого трафика, информация будет передана только при факте изменения, то есть если сообщаемый USN номер больше записанного. Если у контроллера домена произошел какой-либо сбой, он будет пытаться произвести тиражирование снова при ближайшем включении. По завершению тиражирования USN на контроллере домена устанавливается равным значению, полученному от партнера.

Если данные изменились сразу на нескольких контроллерах домена, то происходит процесс разрешения коллизий. Он может производиться по номеру версии или по временной отметке. Обычно принимается изменение объекта, содержащее больший номер версии. Если номер версии одинаковый, то принимается более поздняя версия по временной отметке.

AD использует сайты для контроля трафика тиражирования по глобальным сетям. Сайт – это группа доменных контроллеров, объединенных быстрым соединением. Внутрисайтовое тиражирование может потреблять существенный трафик, хотя он и сжимается примерно 10:1.

Связи между сайтами создаются при помощи вызова удаленных процедур (Remote Procedure Call, RPC) или протокола SMTP (Simple Mail Transfer Protocol) после создания сайта. Эти связи облегчают репликацию между сайтами. Если они отсутствуют, контроллеры доменов не имеют возможности посылать или принимать обновления каталога. Доступность тиражирования, цена и частота тиражирования могут быть изменены. KCC использует настройки связей между сайтами для создания объекта связи. Для прерывающихся соединений используется SMTP в качестве транспорта. Тиражирование может быть настроено по специальному расписанию, определяющему, когда оно не может происходить, или напротив, позволяет тиражирование в любое время. По умолчанию, тиражирование происходит через три часа. Значение цены используется для выбора связи между сайтами. AD всегда использует путь с наименьшей ценой. Вы можете использовать контроллер домена как мостовой сервер (bridgehead) для работы в качестве шлюза тиражирования. Он будет принимать все данные тиражирования с других сайтов через медленные связи и распределять их по другим контроллерам доменов в сайте через быстрые связи. Мостовые серверы часто используются, если сайты отделены брандмауэрами, прокси-серверами или виртуальными частными сетями (VPN).

Связи между сайтами можно задать вручную с помощью мостов связей. Мост связи сайта определяет наиболее лучший маршрут для тиражирования. Он является процессом построения соединения между двумя сайтами. Он не нужен для полностью маршрутизируемой IP сети. Если вы

установите мосты связи, то вы должны выключить опцию по умолчанию – построение связей автоматически.

6.3. Безопасность Active Directory

Каталог и объекты в нем защищены от неавторизованного вмешательства. Не только каждый объект каталога, но и отдельные их атрибуты могут быть защищены дескрипторами безопасности (security descriptors). Дескриптор безопасности определяет пользователей и группы, имеющие доступ к данному объекту, а также вид доступа.

Таким образом, к каждому объекту можно указать своего администратора. Разграничение доступа производится с помощью делегирования полномочий. Однако делегирования не эффективно при назначении одинаковых прав доступа к нескольким объектам. Для этого используется наследование прав. Любой объект в контейнере может наследовать права доступа, установленные для контейнера. Но помимо наследования можно использовать и явное определение прав. В результате получаются следующие права.

Сначала рассматриваются явные разрешения, затем – унаследованные.

Запрещения имеют приоритет над разрешениями (строки запрещений стоят первыми в списке контроля доступа к объекту).

Список контроля доступа просматривается до первой строки, содержащей нужный SID, все разрешения или запрещения после этой строки не рассматриваются.

Установка AD выполняется с помощью команды DCPROMO.EXE на Windows 2000 Server, эта команда запускает Wizard установки. Та же самая команда может использоваться для понижения контроллера домена до роли обычного сервера, или удаления AD вообще.

Групповая политика (group policy) используется для контроля за средой пользователя, установки ПО и других целей, позволяя гибкий и выборочный административный контроль. Объекты групповой политики (GPOs) это совокупность установок групповой политики, которые могут быть применены к сайту, домену, OUs или к избранным группам.

Служба удаленной установки (Remote Installation Service, RIS) используется для реализации установки Windows 2000 Professional в автоматическом режиме (unattended mode) на несколько компьютеров.

Такие ресурсы AD как разделяемые принтеры и папки, могут быть опубликованы в каталоге, и они будут легко доступны для сетевых пользователей. Пользователи могут больше не знать физическое месторасположение объектов для поиска и доступа к ним.

РАЗДЕЛ 3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОЕКТИРОВАНИЮ ЛОКАЛЬНОЙ СЕТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ (ОО)

Глава 1. Вопросы создания и администрирования локальной сети

1.1. Задачи администратора локальной сети

В настоящее время каждая компания использует в своей работе компьютерные сети. Управлением их работой занимается отдельный специалист – администратор сети.

В задачи администратора входит:

– управление конфигурацией – планирование, конфигурирование сети, ее расширение и ведение документации;

– управление пользователями – создание и поддержка учетных записей пользователей, управление доступом к ресурсам;

– управление ресурсами – установка и поддержка сетевых ресурсов;

– управление производительностью – мониторинг и контроль за сетевыми операциями для поддержания и улучшения производительности системы;

– поддержка – предупреждение, выявление и решение проблем сети.

1.2. Процесс создания локальной сети

При подготовке к созданию локальной сети необходимо ответить на следующие вопросы:

1. Нужна ли в данном случае компьютерная сеть?
2. Какой будет сеть по протяженности (локальная, глобальная, городская)?
3. Какова должна быть архитектура КС (одноранговая или клиент-серверная)?
4. Какие сетевые службы будут необходимы?
5. Какой носитель будет использоваться для передачи данных (кабель или беспроводная связь)? Какой вид носителя будет выбран?
6. Какие сетевые устройства будут применяться для построения сети?
7. Какая топология рекомендуется для сети?

Ответы на данные вопросы позволяют определить основные параметры проектируемой сети.

Основные этапы проектирования сети будут следующими:

1. Определение необходимого количества компьютеров и другой техники, определение типа (клиент-серверная, одноранговая). Моделирование компьютерной сети (расположения компьютеров и связи между ними).

Для моделирования сети могут использоваться разные программные средства. На рисунках 3.1. и 3.2. представлены модели, созданные при помощи MS Visio.

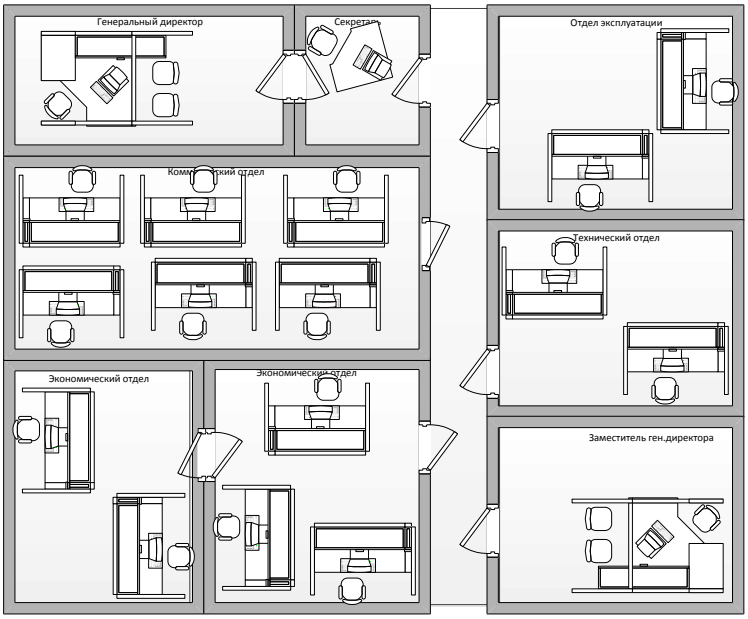

Рисунок 3.1. Модель физического расположения компьютеров

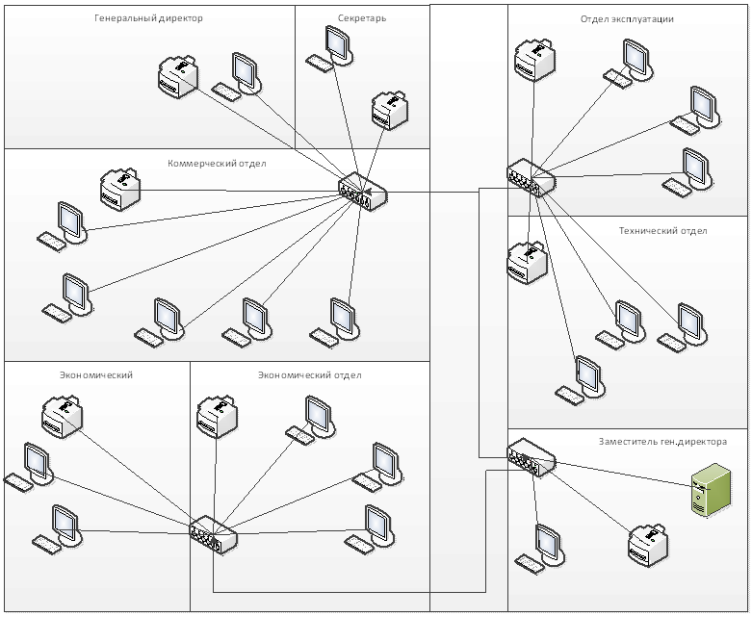

Рисунок 3.2. Структурная схема сети

2. Выбор носителей

При выборе носителя следует учитывать следующие факторы:

- стоимость носителя
- простоту установки
- пропускную способность
- величину затухания сигнала
- величину электромагнитных помех.

Перед выбором типа кабеля следует проанализировать проект сети по следующим параметрам:

1. Интенсивность сетевого трафика (объем передаваемой информации)
2. Требования к защите от прослушивания
3. Максимальная длина одного сегмента
4. Требуемые характеристики кабеля
5. Наличие денежных средств

Также следует прогнозировать развитие компьютерной сети.

Для образовательных организаций больше всего (по соотношению параметров «цена / качество») подходит кабель «витая пара».

Стоимость UTP невелика по сравнению с остальными видами кабелей.

Установка UTP как правило не сложная и может производиться уже после небольшой тренировки. Кабель UTP легко перемещать и изменять его конфигурацию.

Пропускная способность. UTP имеет пропускную способность от 1 до более 1000 Мбит/с на расстояниях до 100 м. Наиболее используется 100 Мбит/с.

Как и любой медный проводник, кабель витой пары сильно подвержен **затуханию** сигнала. Поэтому эффективная длина сегмента не превышает 100 м (10BaseT,100BaseTX,1000BaseT).

Медные проводники очень чувствительны к **внешним ЭМ воздействиям**. Электрический сигнал, проходящий по витой паре можно легко перехватить и прослушать с помощью специальных устройств. Витая пара не подходит для использования в помещениях с сильными электромагнитными помехами.

В настоящее время существуют такие категории витой пары (таблица 3.1).

Таблица 3.1. Категории кабеля «витая пара»

Категория	**Полоса частот, МГц**	**Применение**	**Примечания**
1	0,1 (0,4?)	Телефонные и старые модемные линии	1 пара, не описано в рекомендациях EIA/TIA для передачи данных. Используется только для передачи голоса или данных при помощи модема (не подходит для современных систем)
2	1 (4?)	Старые терминалы (такие как IBM 3270)	2 пары проводников, старый тип кабеля, не описано в рекомендациях EIA/TIA для передачи данных, поддерживал передачу данных на скоростях до 4 Мбит/с, использовался в сетях Token ring и Arcnet (не подходит для современных систем). Сейчас иногда встречается в телефонных сетях.

Продолжение таблицы 3.1

Категория	**Полоса частот, МГц**	**Применение**	**Примечания**
3	16	10BASE-T, 100BASE-T4 Ethernet	4-парный кабель, используется при построении телефонных и локальных сетей 10BASE-T и token ring, поддерживает скорость передачи данных до 10 Мбит/с или 100 Мбит/с по технологии 100BASE-T4 на расстоянии не дальше 100 метров[2]. В отличие от предыдущих двух, отвечает требованиям стандарта IEEE 802.3. Сейчас используется в основном для телефонных линий.
4	20	token ring, сейчас не используется	кабель состоит из 4-х скрученных пар, использовался в сетях token ring, 10BASE-T, 100BASE-T4, скорость передачи данных не превышает 16 Мбит/с по одной паре.
5	100	Fast Ethernet (100BASE-TX), Gigabit Ethernet (1000BASE-T)[4]	4-парный кабель, используется при построении локальных сетей 10BASE-T, 100BASE-TX и 1000BASE-T и для прокладки телефонных линий, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар.
5e	125	Fast Ethernet (100BASE-TX), Gigabit Ethernet (1000BASE-T)	4-парный кабель, усовершенствованная категория 5 (уточненные/улучшенные спецификации)[4]. Скорость передач данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар. Кабель категории 5e является самым распространённым и используется для построения компьютерных сетей. Иногда встречается двухпарный кабель категории 5e. Преимущества данного кабеля в более низкой себестоимости и меньшей толщине.
6	250	10 Gigabit Ethernet (10GBASE-T)	неэкранированный кабель (UTP) состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 55 м[5]. Добавлен в стандарт в июне 2002 года.
6_A	500	10 Gigabit Ethernet (10GBASE-T)	состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 100 метров. Добавлен в стандарт в феврале 2008 года, ISO/IEC 11801:2002 поправка 2. Кабель этой категории имеет либо общий экран (F/UTP), либо экраны вокруг каждой пары (U/FTP).

Продолжение таблицы 3.1

Категория	**Полоса частот, МГц**	**Применение**	**Примечания**
7	600	10 Gigabit Ethernet (10GBASE-T)	спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, но не ANSI/TIA-568-C. Скорость передачи данных до 10 Гбит/с. Кабель этой категории имеет общий экран и экраны вокруг каждой пары (F/FTP или S/FTP).
7_A	1000	10 Gigabit Ethernet (10GBASE-T)	Международный стандарт ISO 11801, скорость передачи данных до 10 Гбит/с. Общий экран и экраны вокруг каждой пары (F/FTP или S/FTP).
8/8.1	1600-2000	100 Gigabit Ethernet (40GBASE-T)	В разработке, техническая рекомендация ISO/IEC TR 11801-99-1 и международный стандарт ISO 11801 редакция 3 (для Cat. 8.1), американский стандарт ANSI/TIA-568-C.2-1 (для Cat. 8). Полностью совместим с кабелем категории 6A. Скорость передачи данных до 40 Гбит/с при использовании стандартных коннекторов 8P8C. Кабель этой категории имеет либо общий экран, либо экраны вокруг каждой пары (F/UTP или U/FTP).
8.2	1600-2000	100 Gigabit Ethernet (40GBASE-T)	В разработке, международный стандарт ISO 11801 редакция 3. Полностью совместим с кабелем категории 7A. Скорость передачи данных до 40 Гбит/с при использовании стандартных коннекторов 8P8C либо GG45/ARJ45 и TERA. Кабель этой категории имеет общий экран и экраны вокруг каждой пары (F/FTP или S/FTP).

В настоящее время наиболее распространения витая пара категории 5. Она обеспечивает достаточную скорость передачи при сравнительно невысокой стоимости и легкости установки.

Обжимка кабеля очень проста, но часто продаются уже обжатые сегменты.

3. Выбор соединительного оборудования

Чаще всего в локальной сети используется топология звезда. Дл подключения отдельных сегментов сети выбирается концентратор (хаб). Если несколько концентраторов, в свою очередь, подключаются к центральному концентратору, то сеть относится к топологии «иерархическая звезда».

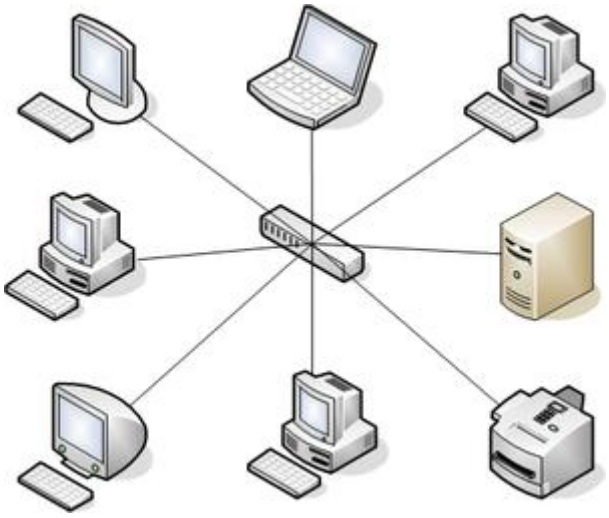

Рисунок 3.3. Сеть топологии «звезда»

Рисунок 3.4. Внешний вид концентратора

Для подключения локальной сети к глобальной сети Интернет, используется маршрутизатор.

4. Выбор программного обеспечения

Сетевая операционная система – это операционная система, ориентированная на работу с компьютерной сетью для организации доступа к общим ресурсам для нескольких компьютеров в сети, что позволяет давать общий доступ к данным для пользователей, групп, политик безопасности, приложений и других сетевых функций.

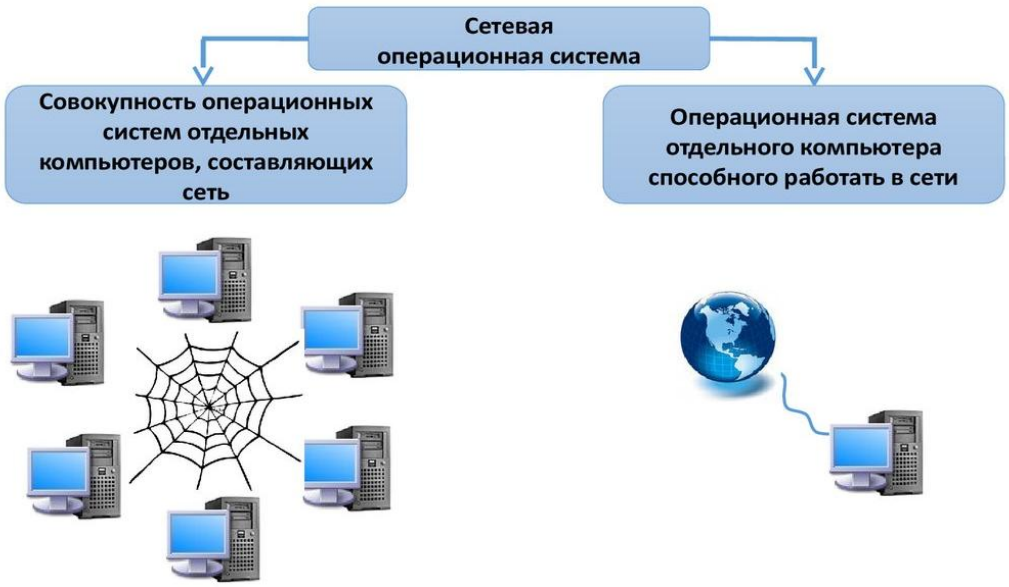

Рисунок 3.5. Разные понятия сетевой операционной системы

В настоящее время все операционные системы поддерживают возможность работы в сети. Существуют серверные операционные системы, предоставляющие специальные вопросы для настройки и администрирования сети.

5. Настройка сетевого ПО

Необходимо задать IP-адреса компьютеров. Чаще всего они определяются автоматически.

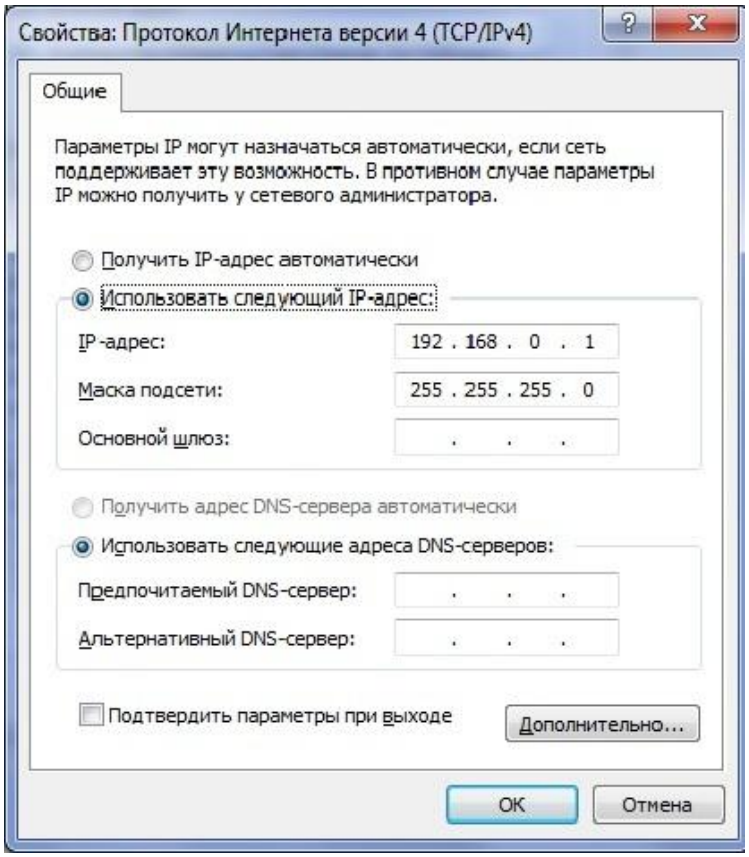

Рисунок 3.6. Параметры IP-адресов

Использование бесклассовой адресации бывает необходимо в крупных организациях с наличием большого количества подсетей. В образовательной организации чаще всего бывает достаточно сети класса С и автоматической раздачи IP-адресов.

Следующим этапом будет определение групп пользователей и уровней доступа каждой группы пользователей. Для ведения реестров таких групп пользователей может использоваться служба каталогов Active Directory.

Также важно определить и настроить общедоступные сетевые ресурсы. В локальной сети могут быть выделены общесетевые ресурсы («расшаренные» каталоги).

Также нужно продумать варианты резервного копирования важной информации, хранящейся в сети.

6. Обучение пользователей

Может понадобиться обучить пользователей локальной сети работе в ней (например, доступ к сетевым папкам).

7. Разработка локальных актов

В образовательной организации должны быть разработаны локальные акты, регулирующие работу локальной вычислительной сети.

К таким локальным актам может относиться Регламент по работе с локальной сетью и сетью Интернет. Он может содержать такие разделы:

1) Общие положения

Содержит описание того, что такое локальная сеть, что включается в данную сеть.

2) Техническое обслуживание

Определяется, кто и каким образом выполняет обслуживание локальной сети (приглашенный специалист, специалист в самой организации – администратор, техник, учитель информатики)

3) Правила использования сетей

Описывается, кто может иметь доступ к работе с сетью, для чего она используется, какова ответственность при работе в сети

4) Действия в нештатных ситуациях

Описываются возможные нештатные ситуации и действия при их возникновении.

В приложениях 1 и 2 приведен пример приказа об утверждении регламента по работе с локальной сетью и сетью Интернет, а также самого Регламента.

Также могут быть разработаны Инструкция по контролю использования обучающимися сети Интернет, Памятка по использованию сети Интернет и другие документы.

1.3. Мониторинг компьютерной сети

Под мониторингом компьютерных сетей понимают работу системы, осуществляющей непрерывное наблюдение за их функционированием с целью обнаружения медленно действующих или нерабочих систем. В задачу мониторинга входит в случае обнаружения неисправностей оповещения о них сетевого администратора заранее установленным способом – с помощью сообщения на электронную почту, мессенджер, пейджер и т.п. Выполнение данной задачи является одним из основных аспектов управления компьютерной сетью. Рассмотрим несколько программных средств мониторинга сети.

1) Cacti

Cacti — это бесплатная программа, входящее в LAMP-набор серверного программного обеспечения, которое предоставляет стандартизированную программную платформу для построения графиков на основе практически любых статистических данных. Если какое-либо устройство или сервис возвращает числовые данные, то они, скорее всего, могут быть интегрированы в Cacti. Существуют шаблоны для мониторинга широкого спектра оборудования — от Linux- и Windows-серверов до маршрутизаторов и коммутаторов Cisco, — в основном все, что общается на

SNMP (Simple Network Management Protocol, простой протокол сетевого управления). Существуют также коллекции шаблонов от сторонних разработчиков, которые еще больше расширяют и без того огромный список совместимых с Cacti аппаратных средств и программного обеспечения.

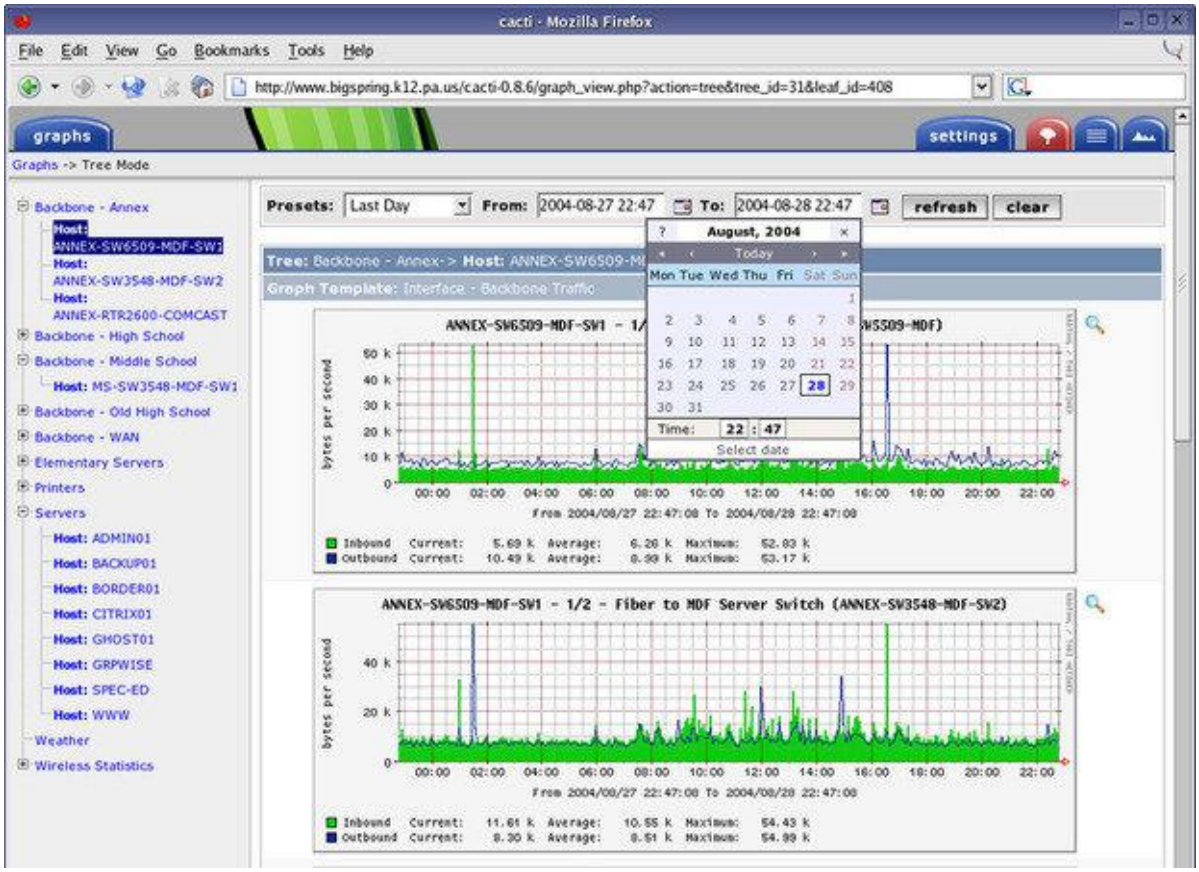

Рисунок 3.7. Внешний вид программы

Несмотря на то, что стандартным методом сбора данных Cacti является протокол SNMP, также для этого могут быть использованы сценарии на Perl или PHP. Фреймворк программной системы умело разделяет на дискретные экземпляры сбор данных и их графическое отображение, что позволяет с легкостью повторно обрабатывать и реорганизовывать существующие данные для различных визуальных представлений. Кроме того, вы можете выбрать определенные временные рамки и отдельные части графиков просто кликнув на них и перетащив.

Таким образом, Cacti — это инструментарий с обширными возможностями для графического отображения и анализа тенденций производительности сети, который можно использовать для мониторинга практически любой контролируемой метрики, представляемой в виде графика. Данное решение также поддерживает практически безграничные возможности для настройки, что может сделать его чересчур сложным при определенных применениях.

2) Nagios

Nagios — это состоявшаяся программная система для мониторинга сети, которая уже многие годы находится в активной разработке. Написанная

на языке C, она позволяет делать почти все, что может понадобится системным и сетевым администраторам от пакета прикладных программ для мониторинга. Веб-интерфейс этой программы является быстрым и интуитивно понятным, в то время его серверная часть — чрезвычайно надежной.

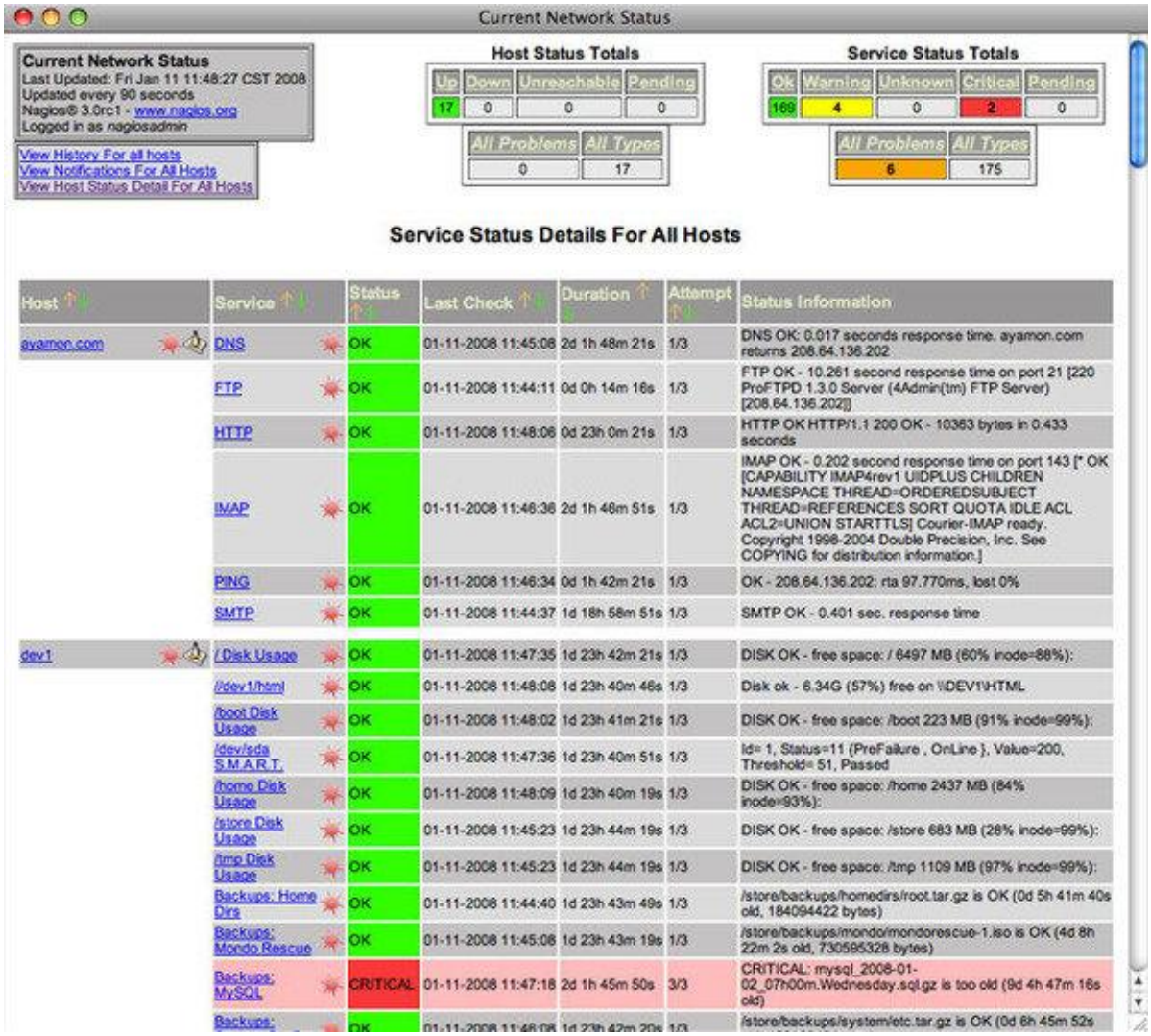

Рисунок 3.8. Внешний вид программы

Минус системы в том, что она достаточно сложна для освоения.Возможности Nagios огромны, но усилия по использованию некоторых из них не всегда могут стоить затраченных на это усилий.

3) Icinga

Icinga предлагает полноценную программную платформу для мониторинга и системы оповещения, которая разработана такой же открытой и расширяемой, как и Nagios, но с некоторыми отличиями в веб-интерфейсе.

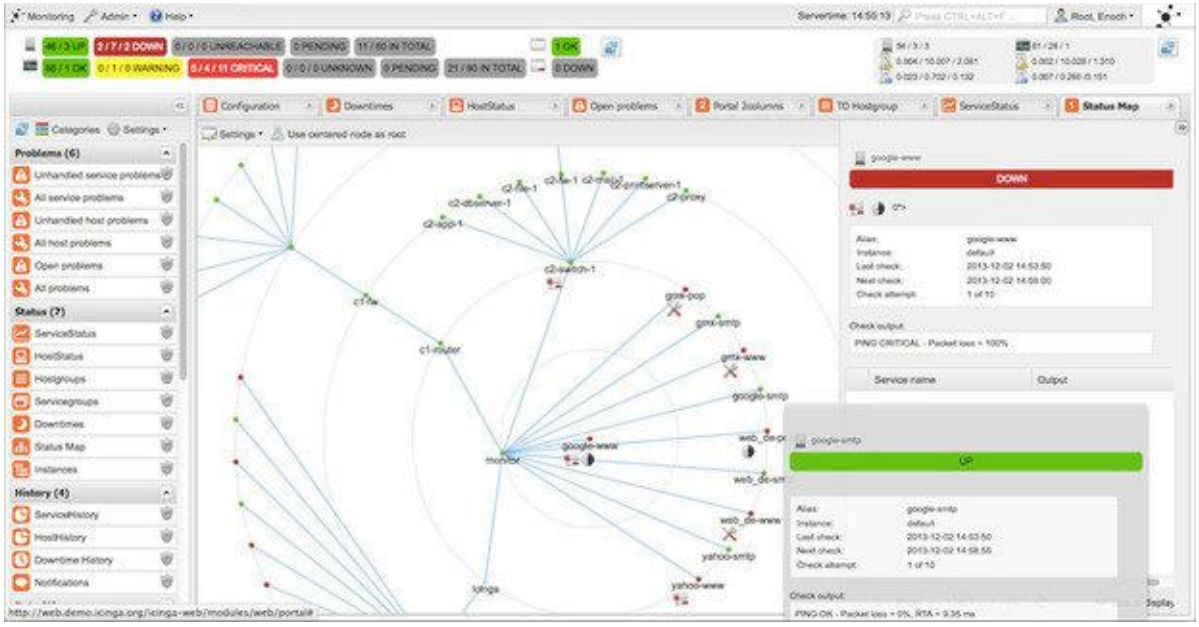

Рисунок 3.9. Внешний вид программы

Существует несколько вариаций веб-интерфейса для Icinga, но главным отличием этого программного решения для мониторинга от Nagios является конфигурация, которая может быть выполнена через веб-интерфейс, а не через файлы конфигурации. Icinga интегрируется со множеством программных пакетов для мониторинга и графического отображения, таких как PNP4Nagios, inGraph и Graphite, обеспечивая надежную визуализацию вашей сети. Кроме того, Icinga имеет расширенные возможности отчетности.

4) Ntop

Ntop — это инструмент для анализа пакетов с легким веб-интерфейсом, который показывает данные в реальном времени о сетевом трафике. Информация о потоке данных через хост и о соединении с хостом также доступны в режиме реального времени.

Ntop предоставляет легко усваиваемые графики и таблицы, показывающие текущий и прошлый сетевой трафик, включая протокол, источник, назначение и историю конкретных транзакций, а также хосты с обоих концов. Кроме того, вы найдете впечатляющий набор графиков, диаграмм и карт использования сети в реальном времени, а также модульную архитектуру для огромного количества надстроек, таких как добавление мониторов NetFlow и sFlow. Здесь вы даже сможете обнаружить Nbox — аппаратный монитор, который встраивает в Ntop.

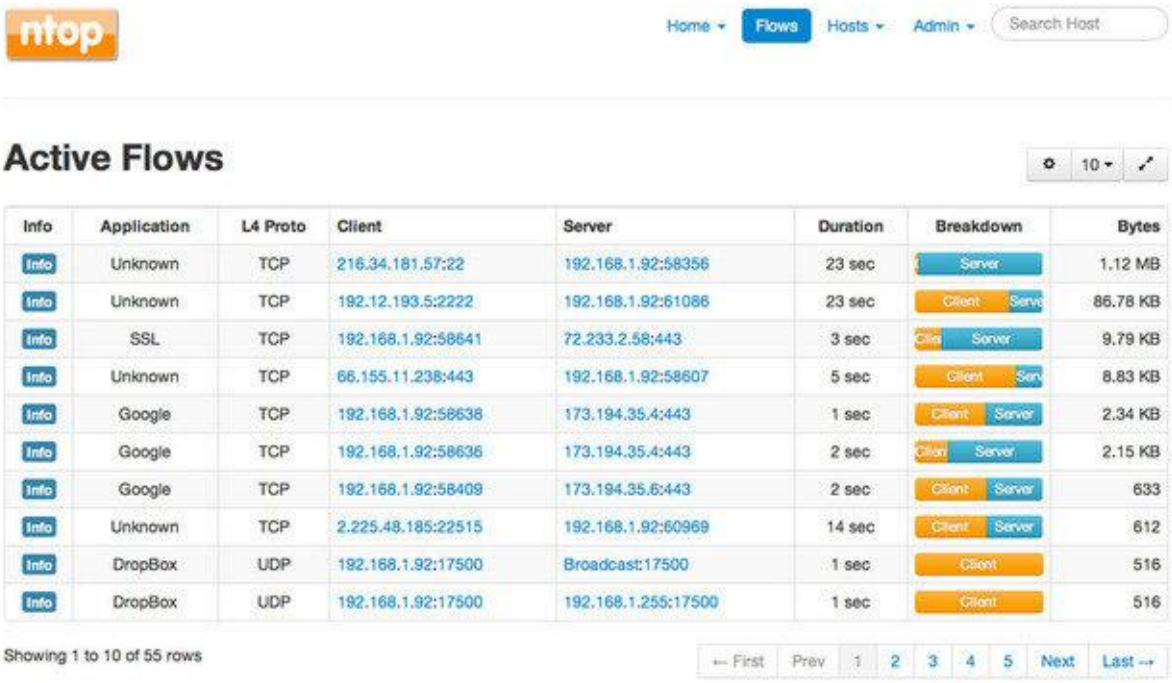

Рисунок 3.10. Внешний вид программы

Анализ трафика является процессом, важность которого известна любому ИТ-профессионалу. Сейчас на рынке представлено большое количество вариаций программного обеспечения для анализа сетевого трафика.

Представим несколько программных средств анализа трафика.

1) SolarWinds Network Bandwidth Analyzer

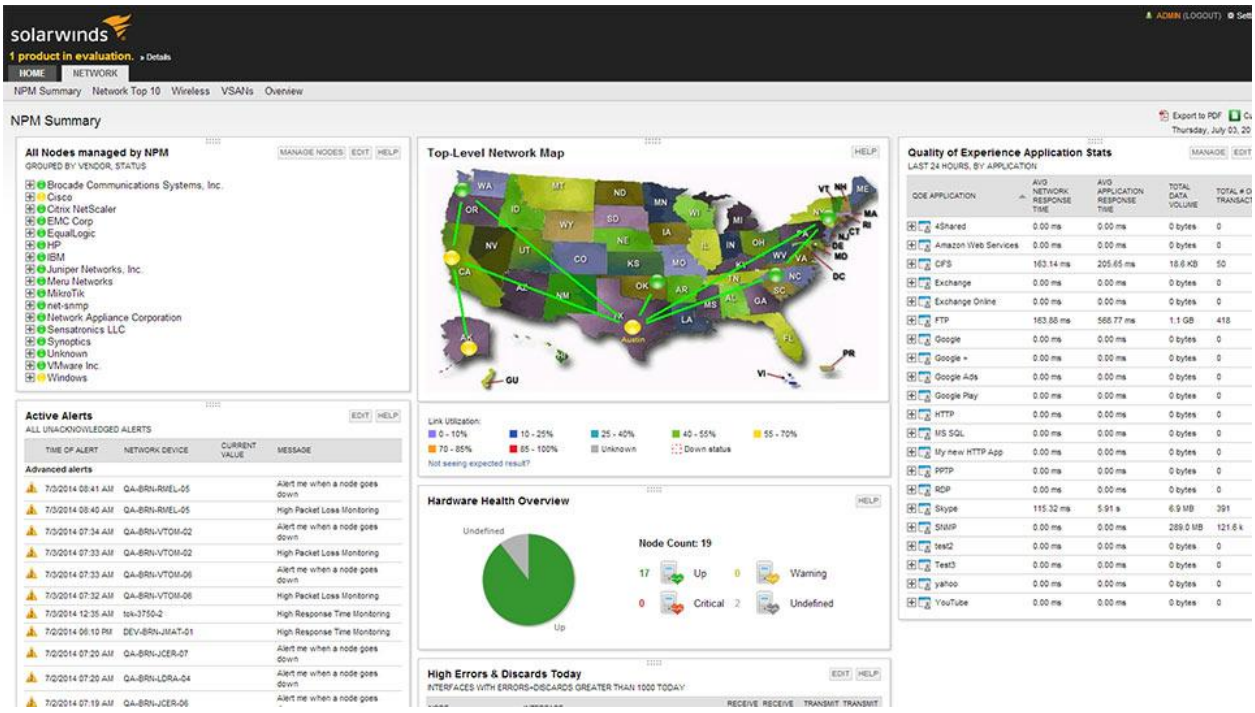

Рисунок 3.11. Внешний вид программы

Данное решение позиционируется производителем как программный пакет из двух продуктов — Network Performance Monitor (базовое решение) и NetFlow Traffic Analyzer (модульное расширение). Как заявляется, они имеют схожие, но все же отличающиеся функциональные возможности для анализа сетевого трафика, дополняющие друг друга при совместном использовании сразу двух продуктов.

Network Performance Monitor осуществляет мониторинг производительности сети. Программа предоставляет возможность контролировать общую работоспособность сети: опираясь на огромное количество статистических данных, таких как скорость и надежность передачи данных и пакетов, в большинстве случаев можно быстро идентифицировать неисправности в работе сети. А продвинутые интеллектуальные возможности программы по выявлению потенциальных проблем и широкие возможности по визуальному представлению результатов в виде таблиц и графиков с четкими предупреждениями о возможных проблемах, еще больше облегчат эту работу.

Модульное расширение NetFlow Traffic Analyzer больше сконцентрировано на анализе самого трафика. В частности, эта часть программного пакета позволит проанализировать перегрузки или аномальные скачки полосы пропускания и предоставит статистику, отсортированную по пользователям, протоколам или приложениям. Данная программа доступна только для среды Windows.

"10-Страйк: Учет Трафика" - это простая программа для контроля расхода трафика на компьютерах, коммутаторах, серверах в сети на предприятии и даже дома (3 сенсора можно мониторить бесплатно в пробной версии даже после истечения 30-дневного пробного периода). Программа постоянно осуществляет сбор статистики с хостов сети по входящему и исходящему трафику и отображает в реальном времени динамику изменения скорости передачи данных на сетевых интерфейсах в виде графиков и таблиц.

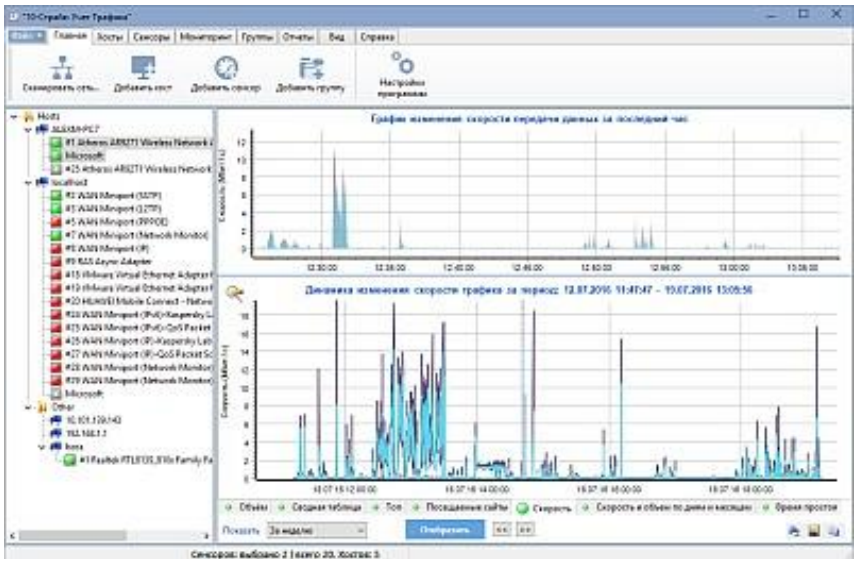

Рисунок 3.12. Внешний вид программы

С помощью программы учета можно обнаружить недобросовестных пользователей, расходующих много Интернет-трафика в организации. Нарушение трудовой дисциплины сотрудниками приводит к понижению производительности труда. Простейший анализ потребления трафика компьютерами сотрудников позволит обнаружить самых активных пользователей сети. При использовании WMI-сенсоров, на компьютеры сети даже ничего не нужно устанавливать, нужен лишь пароль администратора.

1.4. Результаты мониторинга состояния локальных сетей в ОО

В январе 2018 года ИРО Кировской области был проведен мониторинг того, насколько развиты технологии локальных сетей в образовательных организациях. По результатам мониторинга были получены следующие данные. В опросе приняло участие 68 образовательных организаций г. Кирова и Кировской области.

Опрос содержал вопросы, касающиеся наличия компьютерной сети в организации, количества компьютеров, включенных в сеть, наличия компьютерного класса, специалистов, обслуживающих сеть, а также проблем, с которыми сталкиваются эти специалисты.

В 54% образовательных организаций все компьютеры объединены в локальную сеть. В 25% образовательных организаций локальная сеть имеется только в компьютерном кабинете. В 21% организаций локальной сети нет

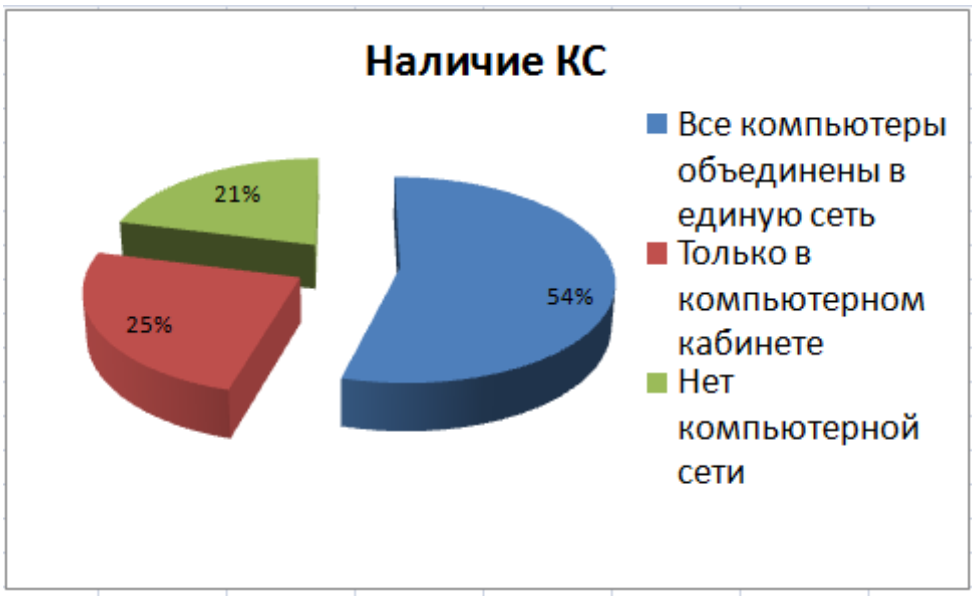

Рисунок 3.13. Анализ наличия локальной сети

В 53% образовательных организаций локальная сеть включает от 10 до 50 компьютеров. В 19% образовательных организаций – от 50 до 100 компьютеров. В 18% - до 10 устройств, а в 10% - более 100 компьютеров.

Рисунок 3.14. Количество компьютеров в локальной сети

В 54% образовательных организаций имеется один компьютерный класс. В 30% образовательных организаций – таких классов несколько. В 16% - компьютерного класса нет.

Рисунок 3.15. Наличие в ОО компьютерного класса

Информация о специалистах, обслуживающих локальную сеть, представлена в таблице

Таблица 3.2. Информация о специалистах, обслуживающих сеть

Должность	Системный администратор	Инженер-программист	Инженер	Техник	Учитель информатики
Нет такой должности (не занимается данными вопросами)	73,68%	80,70%	82,46%	78,95%	52,63%
Штатный	15,79%	8,77%	12,28%	7,02%	35,09%
Штатный совместитель	7,02%	7,02%	5,26%	7,02%	7,02%
Внешний совместитель	3,51%	3,51%	0,00%	5,26%	1,75%
Привлечение по договору для выполнения отдельных видов работ	0,00%	0,00%	0,00%	1,75%	3,51%

По таблице можно сделать вывод, что штатные специалисты (системные администраторы, инженеры, техники) имеются в очень небольшом количестве организаций (порядка 40 %). Процент совместителей (как штатных, так и нештатных) еще меньше – порядка 35%.

Во многих организациях задачи администрирования сети решает учитель информатики – порядка 50%.

Основные задачи, которые решаются в образовательных организациях при помощи локальной сети, следующие: ведение электронного журнала, обмен файлами, система обмена мгновенными сообщениями, создание и организация доступа к медиатеке, сетевые принтеры, единая система тестирования, единый сервер печати, авторизация через домен контроллер, электронная учительская, АРМ "Директор«, сетевое ПО.

Существуют и определенные проблемы:

1. Отсутствие средств на модернизацию, оптимизацию, ремонт и д.т.

2.Нежелание коллектива внедрять и использовать новые технологии.

3. Запрет на пользование иностранными сервисами

4. Незначительные сбои

5. Сложность настройки сети, обеспечение доступа с разными ОС: WIN_XP; 7; 8; 10

6. Нехватка диапазона IP-адресов при выходе в глобальную сеть

7. Отсутствие штатного дипломированного специалиста

8. Нехватка вычислительных ресурсов

9. Недостаток финансирования, устаревание компьютерного оборудования.

10 Невозможность обеспечить доступ к общим документам на некоторых компьютерах

2.1. Программное обеспечение образовательного процесса

Существует большое количество программных средств, для работы с которыми необходимо наличие локальной вычислительной сети. Рассмотрим некоторые из них.

1. Мессенджеры

Мессенджеры предназначены для передачи текстовых сообщений, а также файлов. Примером бесплатного мессенджера является LAN Messenger – мессенджер для локальной сети (рисунок 3.16).

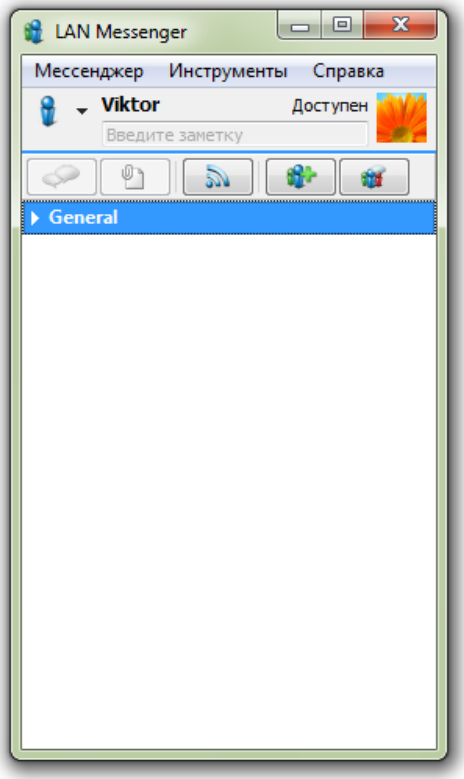

Рисунок 3.16. Внешний вид мессенджера

2. Системы электронного документооборота.

Системы электронного документооборота формируют новое поколение систем автоматизации предприятий. Основными объектами автоматизации в таких системах являются документы (в самом широком их понимании, от обычных бумажных до электронных любого формата и структуры) и бизнес-процессы, представляющие как движение документов, так и их обработку. Данный подход к автоматизации предприятий является одновременно и конструктивным и универсальным, обеспечивая автоматизацию документооборота и всех бизнес-процессов предприятия в рамках единой концепции и единого программного инструментария.

Системы электронного документооборота могут выпонять такие функции:

– регистрация корреспонденции (входящие, исходящие);

– электронный архив документов;
– согласование и утверждение ОРД;
– контроль исполнения документов и поручений;
– автоматизация договорного процесса;
– библиотека регламентов управленческих процедур;
– оформление командировок;
– организация внутреннего информационного портала предприятия и его подразделений;
– система контроля выполнения должностных инструкций.

Для регистрации документов может использоваться система – Регистрация документов организации 4.3. Программа доступна по ссылке http://www.softportal.com/getsoft-6049-registratsiya-dokumentov-organizatsii-2.html

Эта программа действует для регистрации поступивших документов и отписывании их исполнителям.

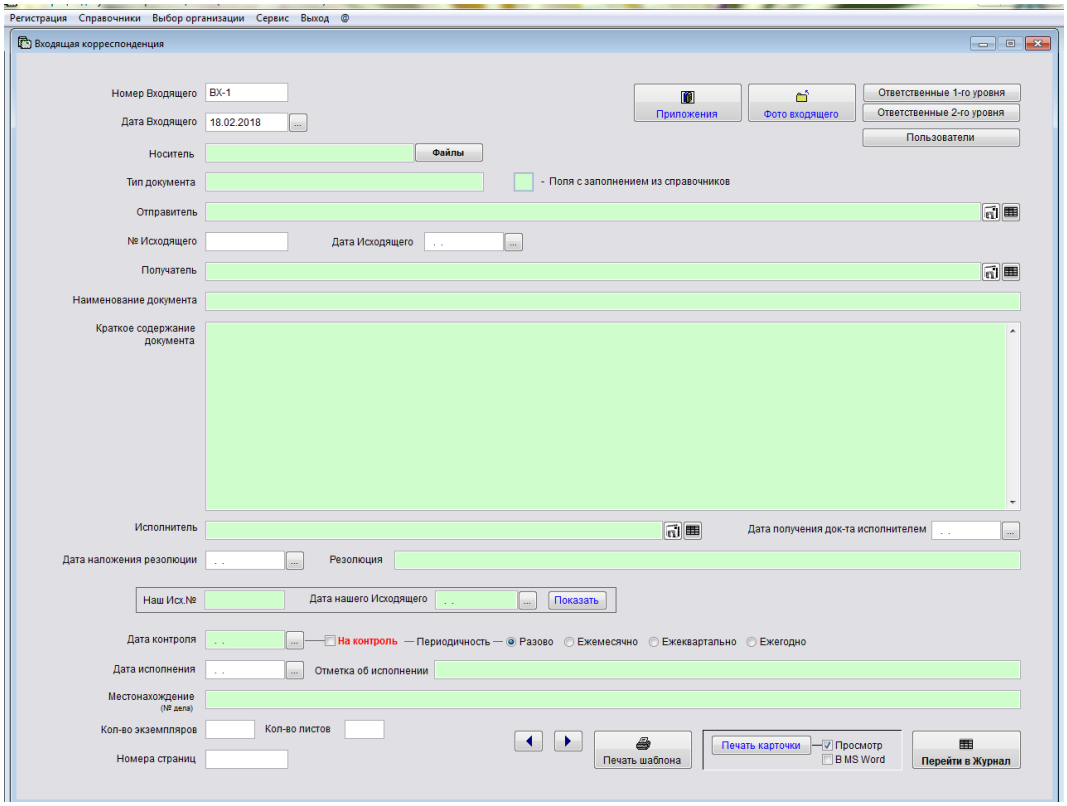

Рисунок 3.17. Внешний вид программы

Система электронного документооборота FossDoc обеспечивает полноценное управление документооборотом. Программа доступна по ссылке https://fossdoc.com/ru/downloadfree

Программа бесплатна на 5 рабочих мест, может использоваться для управления документооборотом администрации.

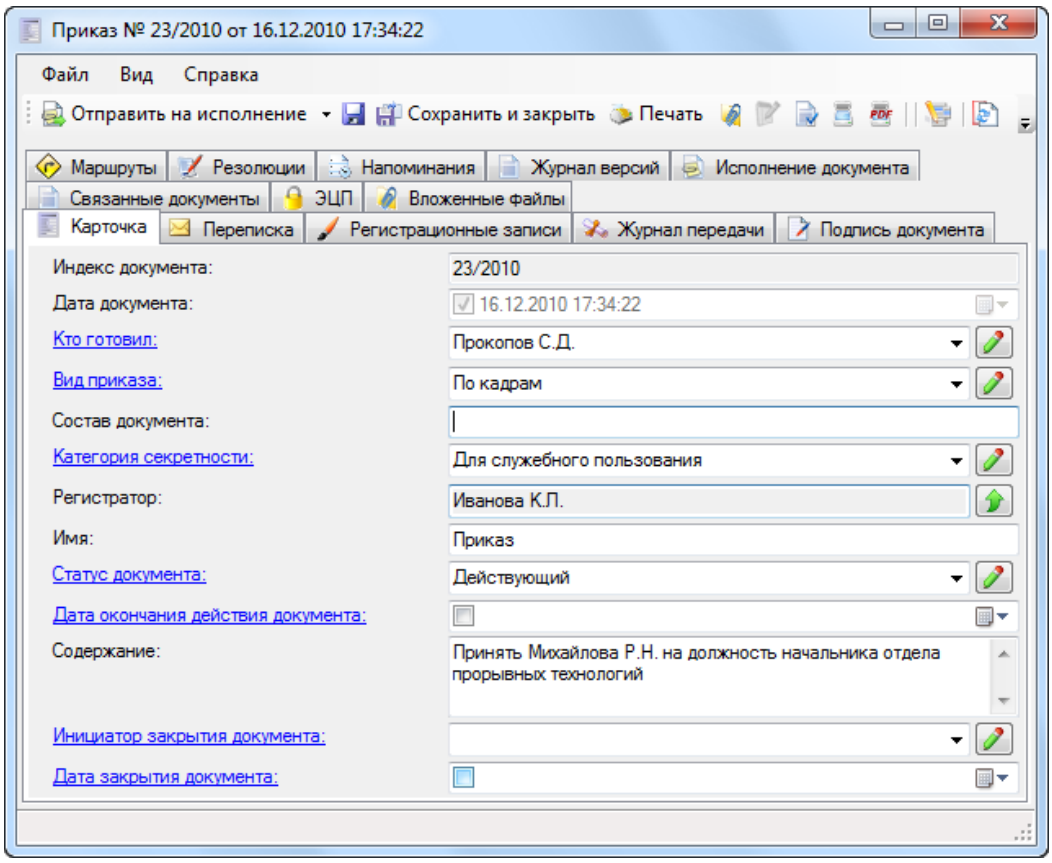

Рисунок 3.18. Внешний вид программы

3. Программный комплекс «Аверс. Директор», «Аверс. Журнал» обеспечивает ведение личных дел педагогов, детей. Имеется возможность работы в данным комплексом с различных рабочих мест, обеспечения разного уровня доступа к данной системе.

Рисунок 3.19. Внешний вид программы

4. Сетевые системы тестирования. Примером такой системы является MyTest Pro/

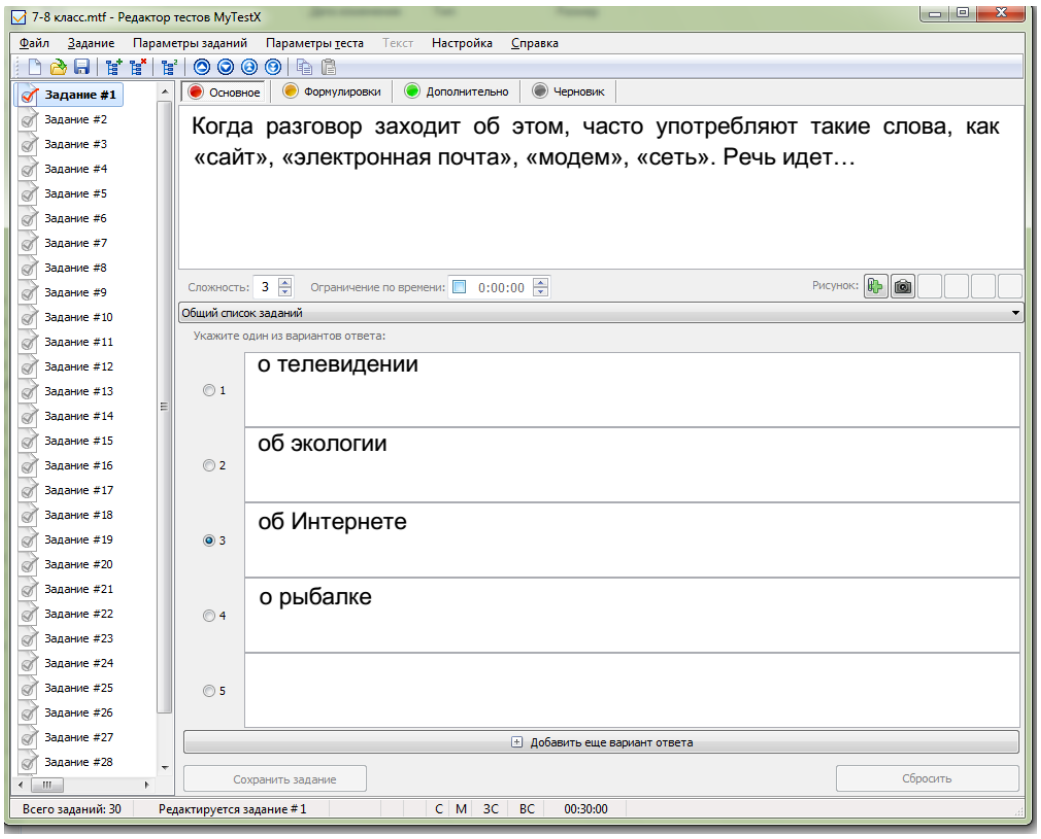

Рисунок 3.20. Внешний вид программы

Ссылка на сайт программы: http://mytest.klyaksa.net/htm/download/index.htm

Инструкции по работе с данным сервисом:

Пошаговые инструкции:

Установка программы: http://yarovik.ru/moi-razrabotki/ispolzovanie-programmy-mytestxpro-dlya-ocenki-predmetnyx-rezultatov-uchashhixsya/priobretenie-programmy/

Настройка программы: http://yarovik.ru/moi-razrabotki/ispolzovanie-programmy-mytestxpro-dlya-ocenki-predmetnyx-rezultatov-uchashhixsya/nastrojka-programmy/

Создание тестов: http://yarovik.ru/moi-razrabotki/ispolzovanie-programmy-mytestxpro-dlya-ocenki-predmetnyx-rezultatov-uchashhixsya/sozdanie-testov-v-programme/

Проведение тестирования: http://yarovik.ru/moi-razrabotki/ispolzovanie-programmy-mytestxpro-dlya-ocenki-predmetnyx-rezultatov-uchashhixsya/analiz-rezultatov-v-programme/

5. Система управления дистационными курсами Moodle. Она может использоваться в пределах локальной сети и использоваться для организации самостоятельной работы учеников.

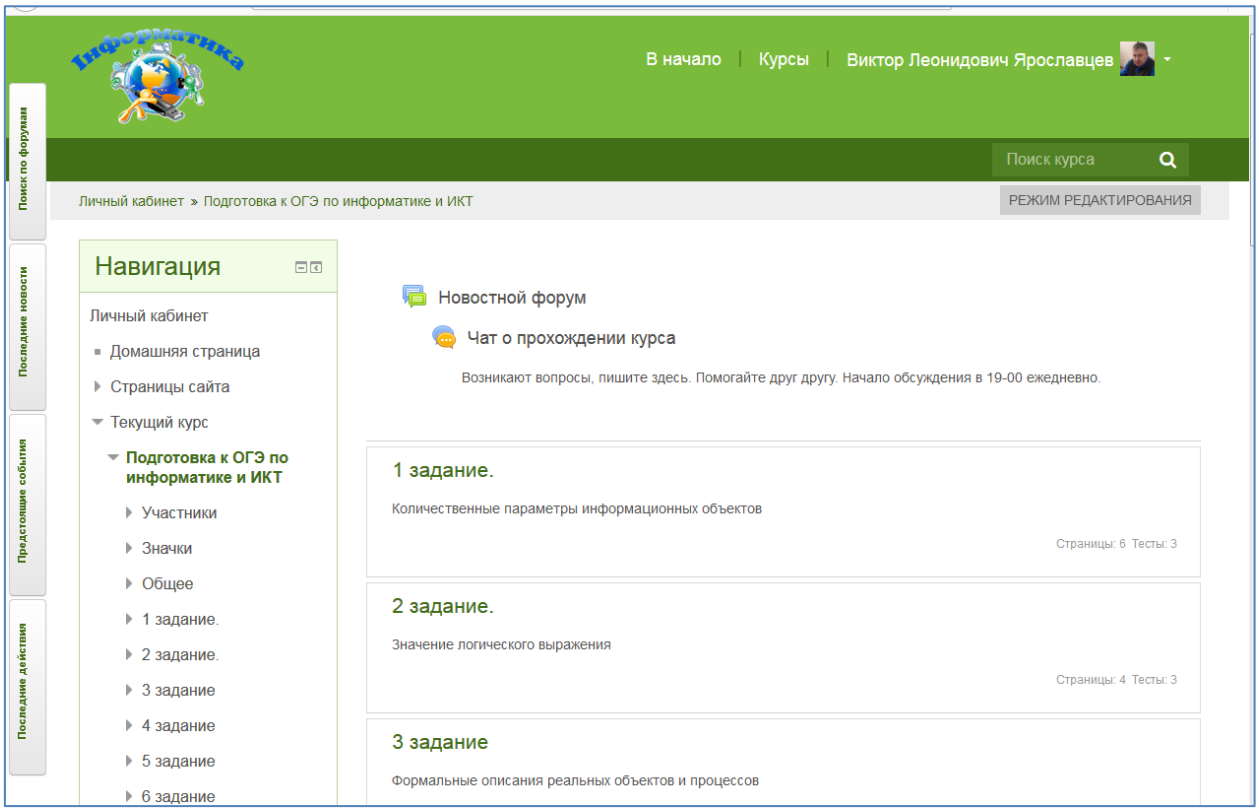

Рисунок 3.21. Внешний вид системы Moodle

В сети могут использоваться и другие программные средства, которые обеспечат возможность совместной работы пользователей.

2.2. Разворачивание ALT Linux 5.0 server (школьного)

Сервер **ALT Linux 5.0 server** обеспечивает управление локальной сетью образовательной организации. Адрес страницы программы: https://www.altlinux.org/Альт_Линукс_5.0.2_Школьный

Сервер **ALT Linux 5.0 server** выполняет следующие функции:

– Фильтрация содержимого (Netpolice).

– Создание локального репозитория для централизованного обновление серверов и рабочих станций.

– Сетевая установка рабочих станций.

– Виртуализация для установки контейнеров с дополнительным ПО.

– Создание резервных копий и восстановление из них (в том числе отдельных файлов).

– Единое файловое хранилище.

– Настройка брандмауэра сети.

– Система дистанционного обучения Moodle.

– Система коллективной подготовки текстов MediaWiki.

– "Электронный классный журнал РУЖЭЛЬ" (журнал, дневник, автоматизация работы завуча).

– Другие функции.

Для реализации сервера нужно такое аппаратное обеспечение:

– привод CD/DVD;

– процессор совместимой с Pentium III архитектуры от 500 МГц (рекомендуется тактовая частота не ниже 1 ГГц);

– объём оперативной памяти от 128 Мб (рекомендуется от 512 Мб). Если планируется использование Moodle и/или MediaWiki, то не менее 256 Мб.;

– свободное место на жёстком диске от 4 Гб (рекомендуется от 10 Гб). Необходимое место для хранения пользовательских данных, зеркал дистрибутивов и прочих потенциально объёмных данных может сильно варьироваться. Необходимо озаботиться наличием достаточного резерва вдобавок к указанным величинам;

– 2 сетевых адаптера 10/100 Мбит (рекомендуется 1 Гбит);

– видеокарта необходима только на время установки.

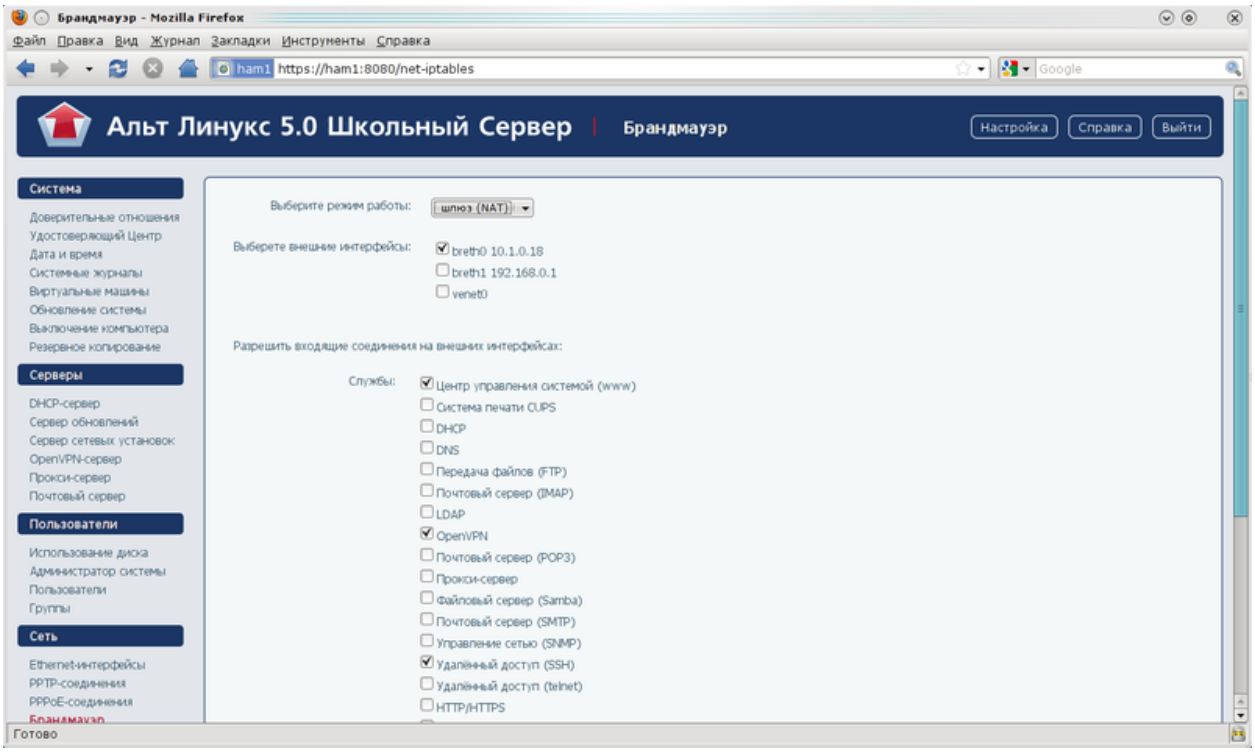

Рисунок 3.22. Внешний вид программы

Сервер **ALT Linux 5.0 server** обеспечивает удобное управление локальной сетью: установку и настройку программного обеспечение в сети, работу с единым файловым хранилищем, работу с DHCP-сервером и многое другое.

Список литературы

1. Skurikhina Yu.A. Simulation of the process for implementation of the information management system//Modern science. 2017. № 7. С. 127-132.
2. Гук М. Аппаратные средства локальных сетей. – СПб: Изд-во «Питер-пресс», 2015
3. Компьютерные сети. Учебный курс / Пер. с англ. – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd». – 1997. – 696 с. Пер. с англ. – М.: Издательский дом «Вильямс», 2016.
4. Компьютерные сети. Учебный курс / Пер. с англ. – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd». – 2017.
5. Кульгин М. Технологии корпоративных сетей. – СПб: Изд-во «Питер-пресс», 2015.
6. Олифер Н.А., Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Изд-во «Питер», 2014.
7. Скурихина Ю.А. Автоматизация процесса управления образовательной организацией//Синергия наук. 2017. № 13. -С. 638-648. -URL: http://synergy-journal.ru/archive/article0806
8. Скурихина Ю.А. Информатизация образовательной организации: проблемы и перспективы//Образование в Кировской области. 2014. № 1 (29). С. 4-5.
9. Скурихина Ю.А. Информационно-образовательная среда организации: инновационная педагогическая система//СИНЕРГИЯ НАУК. -2017. -№15. -С. 604-613.
10. Скурихина Ю.А. Использование методологии управления проектами при реализации проектов информатизации в образовательных организациях//Информационные технологии. Проблемы и решения. 2015. № 1 (2). С. 277 -281.
11. Скурихина Ю.А. Основные аспекты управления медиасредой образовательной организации//Ресурсы педагогического сообщества в глобальном информационном пространстве. Сборник материалов первой Всероссийской научно-практической конференции. 2014. -КОГОАУ ДПО «ИРО Кировской области», с. 57-61
12. Скурихина Ю.А. Подходы к развитию информационных технологий в организациях города Кирова//Современное образование: стратегии роста и эффективные образовательные практики. Материалы конференции. Омутнинск, 10-20 августа 2017 г. -2017. -с.428-434
13. Скурихина Ю.А. Современный урок математики//Современный урок математики в условиях реализации ФГОС Сборник работ участников II межрегионального заочного конкурса (ноябрь-декабрь 2016 г.)/Авт.-сост. Ю.А. Скурихина; КОГОАУ ДПО «ИРО Кировской области». -Киров, 2017. -с. 5-8
14. Скурихина Ю.А., Горадзе А.И. Опыт организации сетевого взаимодействия в рамках Подосиновского школьного округа//Образование в

Кировской области № 4(36) -Киров: ООО "Типография "Старая Вятка", 2015г. -с. 11-13

15. Титтел Э. Networking Essentials. Сертификационный экзамен – экстерном (экзамен 70-058) – СПб.: Питер Ком, 2014.

16. Фейбел В. Энциклопедия современных сетевых технологий. – Москва: Изд-во «Комиздат», 2015.

17. Храмцов П. Б. Администрирование сети и сервисов internet учебное пособие центр информационных технологий, 2016

18. Челлис Д. Основы построения сетей. – Москва: Изд-во «Лори», 2015

Приложения

Приложение 1. Приказ об утверждении регламента по работе с локальной сетью и сетью Интернет

(на бланке ОУ)

ПРИКАЗ
«____» _____ 20___ г. № _____

Об утверждении регламента по работе с локальной сетью и сетью Интернет в образовательной организации и назначении ответственных сотрудников за настройку и контроль использования сетей

В целях систематизации мероприятий по обслуживанию и использованию локальной сети и сети Интернет в образовательной организации

ПРИКАЗЫВАЮ:

1. Назначить ответственным сотрудником за настройку локальной сети [должность] [фамилия, имя, отчество].
2. Назначить ответственным сотрудником за настройку сети Интернет [должность] [фамилия, имя, отчество].
3. Назначить ответственным сотрудником за контроль над использованием сетей [должность] [фамилия, имя, отчество].
4. Утвердить прилагаемый Регламент по работе с локальной сетью и сетью Интернет в образовательной организации.
5. Сотрудникам ОУ руководствоваться утверждённым Регламентом.

Приложение: на 3 л. в 1 экз.

Директор И.О. Фамилия

Приложение 2. Регламент по работе с локальной сетью и сетью Интернет

УТВЕРЖДЁН
приказом [наименование ОУ]
№ _____
от «___» _____ 20__ г.

Регламент по работе с локальной сетью и сетью Интернет в образовательном учреждении

1. Общие положения

1.1. Настоящий Регламент разработан в целях систематизации мероприятий по обслуживанию и использованию локальной сети и сети Интернет (далее – сети) в ОО и определяет порядок работы с этими сетями учащихся, сотрудников ОО и других лиц.

1.2. Ознакомление с Регламентом и его соблюдение обязательны для всех учащихся, сотрудников ОО, а также иных лиц, допускаемых к работе с сетями в данном ОО.

1.3. Настоящий Регламент имеет статус локального нормативного акта ОО. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящим Регламентом, применяются нормы действующего законодательства.

2. Ответственные лица

2.1. Ответственные сотрудники за настройку локальной сети, за настройку сети Интернет, за контроль над использованием сетей назначаются приказами по образовательному учреждению.

3. Техническое обслуживание сетей в ОО

3.1. Подключение оборудования и настройку сетей в ОО производят ответственные сотрудники за настройку соответствующих сетей. Другим лицам запрещается осуществлять попытки подключения оборудования и настройки сети.

3.2. При необходимости участие внешних организаций в подключении оборудования и настройке сетей допускается с разрешения руководителя ОО.

4. Правила использования сетей в ОО

4.1. Использование сетей допускается только в целях, непосредственно связанных с образовательным процессом.

4.2. Доступ к ресурсам, несовместимым с целями и задачами образования и воспитания, запрещён.

4.3. Использование носящих исключительно игровой и развлекательный характер ресурсов сетей допускается: учащимися – с

отдельного разрешения и под контролем учителя только во внеурочное время; сотрудниками – только в нерабочее время.

4.4. При использовании ресурсов сетей обязательным является соблюдение законодательства об интеллектуальных правах и иного применимого законодательства.

4.5. Использование сетей учащимися допускается только с разрешения учителя. Давший учащемуся разрешение на работу учитель несёт ответственность за соблюдение учащимся Регламента наравне с ним. Данная норма распространяется на всех лиц, не являющихся сотрудниками ОО, в том числе на родителей, гостей.

4.6. Использование ресурсов сетей во время уроков допускается только в рамках выполнения задач данных уроков.

4.7. В свободное время использование учащимися и иными лицами сетей допускается по расписанию оборудованных компьютерами кабинетов в присутствии учителя, прошедшего инструктаж по технике безопасности при работе с вычислительной техникой.

4.8. Сотрудники ОО, имеющие рабочее место, оборудованное компьютером с подключением к сети (сетям), используют сети в любое время в рамках режима работы учреждения.

4.9. Всем сотрудникам ОО обеспечивается возможность использования сетей в компьютерном классе (кабинете информатики) по расписанию кабинета. Расписание предусматривает работу кабинета для указанной цели не менее чем по 2 часа 2 раза в неделю.

4.10. Ответственный сотрудник за контроль над использованием сетей обеспечивает исполнение правил использования, а при необходимости пресекает и устраняет нарушения.

4.11. Для предотвращения доступа к ресурсам используются меры дисциплинарного характера, специализированное программное обеспечение. По каждому выявленному факту доступа к таким ресурсам ответственным сотрудником за контроль над использованием сетей или выявившим данный факт учителем составляется докладная записка на имя руководителя ОО. Ответственность за последствия доступа к нежелательным ресурсам несёт лицо, осуществившее доступ к этим ресурсам.

4.12. При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учётными данными.

4.13. Все компьютеры, подключаемые к любой из сетей, обязаны иметь установленное, действующее и обновляющееся антивирусное программное обеспечение.

4.14. По решению ответственного сотрудника за контроль над использованием сетей отдельные лица могут быть лишены права пользования сетями (как временно, так и постоянно) за неоднократные нарушения настоящего Регламента. Такое решение может быть отменено только самим ответственным сотрудником за контроль над использованием сетей или руководителем ОО.

4.15. Использование школьного файлового хранилища осуществляется на основе авторизованного доступа. Ответственным за настройку локальной сети создаются по соответствующим заявкам учётные данные для доступа, устанавливаются технические ограничения на использование ресурсов файлового хранилища по согласованию с ответственным за контроль над использованием сетей. Доступ с правами добавления и удаления своих материалов предоставляется учащимся и учителям, доступ с правами редактирования всех материалов предоставляется администрации ОО, неограниченный доступ предоставляется ответственному за настройку локальной сети, являющемуся администратором школьного файлового хранилища.

4.16. Использование системы электронных дневников осуществляется на основе авторизованного доступа. Оценки, выставленные на уроках, вносятся учителями, выставляющими оценки; все другие сведения вносятся классными руководителями.

Учётные данные для доступа учителей создаются ответственным за контроль над использованием сетей по спискам классов перед началом учебного года и выдаются учителям под роспись. Учётные данные для доступа родителей и учащихся создаются классными руководителями с использованием своих учётных данных и выдаются родителям и учащимся в начале учебного года под роспись.

5. Действия в нештатных ситуациях

5.1. При утрате (в том числе частично) работоспособности локальной сети или сети Интернет лицо, обнаружившее неисправность, сообщает об этом ответственному сотруднику за настройку соответствующей сети. Ответственный сотрудник за настройку сети устраняет неисправность, а при отсутствии такой возможности ставит в известность руководителя образовательного учреждения. Руководитель организует устранение неисправности – возможно, с привлечением сил и средств окружных служб или сторонних организаций.

5.2. При прекращении работы сети Интернет во всём учреждении ответственный сотрудник за настройку сети проверяет исправность внутришкольных подключений оборудования и настроек сети. В случае их исправности ответственный за настройку сети ставит в известность руководителя ОО и связывается с поставщиком услуг сети Интернет. Если поставщиком является компания [название], то необходимо обращаться по телефону технической поддержки компании [телефон], с бязательной фиксацией номера заявки и последующим контролем исполнения.

5.3. При заражении компьютера вирусами его использование немедленно прекращается сотрудником, обнаружившим заражение. О сложившейся ситуации сообщается ответственным сотрудникам за контроль использования сетей и настройку сетей. Компьютер отключается от сетей до момента очистки от всех вирусов. Разрешение на дальнейшее использование компьютера и подключение его к сетям даёт ответственный сотрудник за контроль над использованием сетей после соответствующей проверки.