РОСЖЕЛДОР

**Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Ростовский государственный университет путей сообщения»
(ФГБОУ ВПО РГУПС)
Тихорецкий техникум железнодорожного транспорта
(ТТЖТ – филиал РГУПС)**

Методическое пособие по проведению практических занятий по МДК 05.01 Компьютерные и телекоммуникационные сети

для обучающихся очной формы обучения

для специальности

09.02.01 Компьютерные системы и комплексы

2022

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
Н.Ю.Шитикова
01 . 09.2022 г.

Методическое пособие по проведению практических занятий по

МДК 05.01 Компьютерные и телекоммуникационные сети разработаны для студентов очной формы обучения специальности **09.02.01 Компьютерные системы и комплексы**.

Организация-разработчик: Тихорецкий техникум железнодорожного транспорта – филиал Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Ростовский государственный университет путей сообщения» (ТТЖТ – филиал РГУПС)

Составитель:

Чуркина О.Н., преподаватель ТТЖТ- филиала РГУПС

Рекомендована цикловой комиссией № 7 Специальностей 09.02.01, 11.02.06, 38.02.01.

Протокол заседания № 1 от 01.09.2022 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Данные методические указания предназначены для студентов по выполнению практических занятий согласно программе МДК 05.01 "Компьютерные и телекоммуникационные сети" (1 семестр) по специальности 09.02.01 **Компьютерные системы и комплексы** с целью закрепления теоретических знаний.

Цели и задачи методических указаний:

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

–проектирования, монтажа и эксплуатации компьютерных сетей;
–проектирования компьютерных сетей с наложением на них IP-телефонии;
–выполнение мероприятий по защите информации в компьютерных системах, комплексах и сетях;

уметь:

–участвовать в проектировании, монтаже и эксплуатации и диагностике компьютерных сетей;
–правильно выявлять и оценивать угрозы безопасности информации;
–категорировать информацию в соответствии с действующим законодательством;
–определять сферу действия и использовать законодательство в области информационной безопасности;
–реализовывать технологии VPN и VLAN;
–правильно выбирать программные и/или аппаратные средства защиты информации от всех видов угроз по различным критериям;
–использовать оснастки политик безопасности различных операционных систем.

знать:

–типы сетей, серверов, сетевую топологию;
–типы передачи данных, стандартные стеки коммуникационных протоколов;
–установку и конфигурирование сетевого оборудования;
–основы проектирования и монтажа локальных вычислительных сетей;
–принципы построения телекоммуникационных вычислительных сетей (ТВС);
–принципы построения беспроводного соединения;
–основы технологии IP – телефонии;
– технологию виртуальных частных сетей VPN;
– технологию виртуальных сетей VLAN;
–методы и средства обеспечения информационной безопасности;
–защиту от несанкционированного доступа, основные принципы защиты информации;

–технические методы и средства защиты информации;
–правила применения, эксплуатации и обслуживания технических средств защиты информации.

Правила выполнения практических работ

1. Студент должен прийти на занятие подготовленным к выполнению практической или лабораторной работы (проведения лабораторного или практического занятия).
2. Практические занятия должны быть оформлены в виде отчета, с указанием фамилии, инициалов и шифра студента.
3. Отчет о проделанной работе следует выполнять на листах формата А4 с одной стороны листа. В отчете представить результат работы (выполненного задания): решение, графики, схемы, диаграммы, скриншоты (если необходимо).
4. Каждый отчет должен заканчиваться самостоятельными выводами, поскольку студент должен творчески подходить к полученным экспериментальным данным, используя свои теоретические и практические знания.
5. Вспомогательные расчеты можно выполнять на отдельных листах, а при необходимости на листах отчета.
6. Оценку по практической или лабораторной работе студент получает, если:

- расчеты выполнены правильно и в полном объеме;

- сделаны выводы по результатам работы;

- может пояснить выполнение любого этапа работы;

- отчет выполнен в соответствии с требованиями к выполнению работы,

- отвечает на контрольные вопросы на удовлетворительную оценку и выше.

Практическое занятие №1

Одноранговая сеть

Цель работы: изучить характеристики одноранговой сети.

Ход работы:

Краткие теоретические сведения

В одноранговой сети все компьютеры равноправны: нет иерархии среди компьютеров и нет выделенного (dedicated) сервера. Как правило, каждый компьютер функционирует и как клиент, и как сервер; иначе говоря, нет отдельного компьютера, ответственного за администрирование всей сети. Все пользователи самостоятельно решают, какие данные на своем компьютере сделать общедоступными по сети.

Размеры

Одноранговые сети называют также рабочими группами. Рабочая группа — это небольшой коллектив, поэтому в одноранговых сетях чаще всего не более 30 компьютеров.

Стоимость

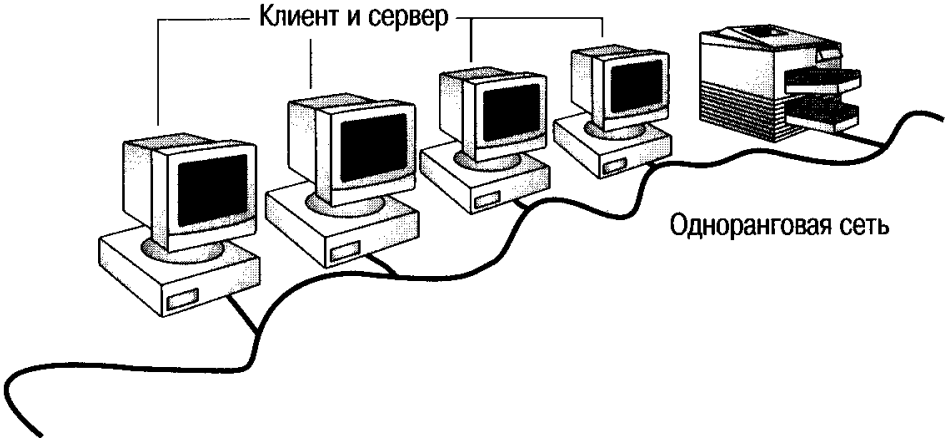
Одноранговые сети относительно просты. Поскольку каждый компьютер является одновременно и клиентом, и сервером, нет необходимости в мощном центральном сервере или в других компонентах, обязательных для более сложных сетей. Одноранговые сети обычно дешевле сетей на основе сервера, но требуют более мощных (и более дорогих) компьютеров.

Операционные системы

Водноранговой сети требования к производительности и к уровню защиты для сетевого программного обеспечения, как правило, ниже, чем в сетях с выделенным сервером. Выделенные серверы функционируют исключительно в качестве серверов, но не клиентов или рабочих станций (workstation). О них мы еще поговорим подробнее на этом занятии, но чуть позже.

Реализация

Одноранговая сеть характеризуется рядом стандартных решений:



- компьютеры расположены на рабочих столах пользователей;

- пользователи сами выступают в роли и обеспечивают защиту информации;

- для объединения компьютеров в сеть применяется простая кабельная система.

Целесообразность применения

Одноранговая сеть вполне подходит там, где:

- количество пользователей не превышает 30 человек;

- пользователи расположены компактно;

- вопросы зашиты данных не критичны;

- в обозримом будущем не ожидается значительного расширения фирмы и следовательно, сети.

Если эти условия выполняются, то скорее всего, выбор одноранговой сети будет правильным (чем сети на основе сервера).

Некоторые соображения

Несмотря на то что одноранговые сети вполне удовлетворяют потребностям небольших фирм, иногда возникают ситуации, когда их использование может оказаться неуместным. Выскажем некоторые замечания относительно одпоранювых сетей, которые Вы должны иметь в виду, выбирая тип сети.

Администрирование

Сетевое администрирование (administration) решает ряд задач, в том числе:

- управление работой пользователей и защитой данных;

- обеспечение доступа к ресурсам;

- поддержка приложений и данных;

- установка и модернизация прикладного программного обеспечения.

В типичной одноранговой сети системный администратор, контролирующий всюсеть, не выделяется. Каждый пользователь сам администрирует свой компьютер.

Разделяемые ресурсы

Все пользователи могут «поделиться» своими ресурсами с другими. К совместно используемым ресурсам относятся каталоги, принтеры, факс-модемы и т.н.

Требования к компьютерам

В одноранговой сети каждый компьютер должен:

- большую часть своих вычислительных ресурсов предоставлять локальному пользователю (сидящему за этим компьютером);

- для поддержки доступа к ресурсам удаленного пользователя (обращающегося к серверу по сети) подключать дополнительные вычислительные ресурсы.

Сеть на основе сервера требует более мощных серверов, поскольку они должны обрабатывать запросы всех клиентов сети.

Защита

Зашита подразумевает установку пароля на разделяемый ресурс, например на каталог. Централизованно управлять защитой в одноранговой сети очень сложно, так как каждый пользователь устанавливает ее самостоятельно, да и «общие» ресурсы могут находиться на всех компьютерах, а не только на центральном сервере. Такая ситуация представляет серьезную угрозу для всей сети, кроме того, некоторые пользователи могут вообще не установить защиту. Если для Вас вопросы конфиденциальности являются принципиальными, рекомендуем выбрать сеть на основе сервера.

Подготовка пользователя

Поскольку в одноранговой сети каждый компьютер функционирует и как клиент, и как сервер, пользователи должны обладать достаточным уровнем знаний, чтобы работать и как пользователи, и как администраторы своего компьютера.

Сети на основе сервера

Если к сети подключено более 30 пользователей, то одноранговая сеть, где компьютеры выступают в роли и клиентов, и серверов, может оказаться недостаточно производительной. Поэтому большинство сетей использует выделенные серверы. Выделенным называется такой сервер, который функционирует только как сервер (исключая функции клиента или рабочей станции). Они специально оптимизированы для быстрой обработки запросов от сетевых клиентов и для управления защитой файлов и каталогов. Сети на основе сервера стали промышленным стандартом, и именно они будут приводиться обычно в качестве примера в этом пособии.

С увеличением размеров сети и объема сетевого трафика необходимо увеличивать количество серверов. Распределение задач среди нескольких серверов гарантирует, что каждая задача будет выполняться самым эффективным способом из всех возможных.

Значение программного обеспечения

Сетевой сервер и операционная система работают как единое целое. Без операционной системы даже самый мощный сервер представляет собой лишь груду железа. А операционная система позволяет реализовать потенциал аппаратных ресурсов сервера. Некоторые системы, например MicrosoftWindows 2003 Server, были созданы специально для того, чтобы использовать преимущества наиболее передовых серверных технологий.

Преимущества

Разделение ресурсов

Сервер спроектирован так, чтобы предоставлять доступ к множеству файлов и принтеров, обеспечивая при этом высокую производительность и защиту.

Администрирование и управление доступом к данным осуществляется централизованно. Ресурсы, как правило, расположены также централизованно, что облегчает их поиск и поддержку. Например, в системе Windows NT Server разделение каталогов осуществляется через FileManager.

Резервное копирование данных

Поскольку жизненно важная информация расположена централизованно, т.е. сосредоточена на одном или нескольких серверах, нетрудно обеспечить ее регулярное резервное копирование (backup).

Избыточность

Благодаря избыточным системам данные на любом сервере могут дублироваться в реальном времени, поэтому в случае повреждения основной области хранения данных информация не будет потеряна — легко воспользоваться резервной копией.

Количество пользователей

Сети на основе сервера способны поддерживать тысячи пользователей. Сетями такого размера, будь они одноранговыми, было бы невозможно управлять.

Аппаратное обеспечение

Так как компьютер пользователя не выполняет функций сервера, требования к его характеристикам зависят от потребностей самого пользователя. Типичный компьютер-клиент имеет, по крайней мере, 486-й процессор и от 8 до 16 Мб оперативной памяти.

Комбинированные сети

Существуют и комбинированные типы сетей, совмещающие лучшие качества одноранговых сетей и сетей на основе сервера. Многие администраторы считают, что такая сеть наиболее полно удовлетворяет их запросы, так как в ней могут функционировать оба типа операционных систем.

Операционные системы для сетей на основе сервера, например MicrosoftWindows NT Server или Novell® NetWare®, в этом случае отвечают за совместное использование основных приложений и данных. На компьютерах-клиентах могут выполняться операционные системы MicrosoftWindows NT Workstation или Windows 95, которые будут управлять доступом к ресурсам выделенного сервера и в то же время предоставлять в совместное использование свои жесткие диски, а по мере необходимости разрешать доступ и к своим данным.

Комбинированные сети — наиболее распространенный тип сетей, но для их правильной реализации и надежной защиты необходимы определенные знания и навыки планирования.

Аппаратное обеспечение сервера

Одноранговые сети и сети на основе сервера объединяет общая цель — разделение ресурсов. А вот различия между одноранговыми серверами и выделенными серверами определяют:

- требования к аппаратному обеспечению;
- способ поддержки пользователей.

Контрольные вопросы:

1. Какие типы сетей распространены? Поясните ответ.
2. Характеристики одноранговой сети и сети с выделенным сервером.

Практическое занятие №2

Изучение типов серверов и их специфика обслуживания

Цель работы: изучить типы серверов.
Оборудование: справочная литература.

Ход занятия:

1. Изучить теоретические сведения:

Специфика обслуживания сервера

Техническое обслуживание серверов и сопутствующего оборудования – важное условие качественной и стабильной работы информационных систем. Именно от него зависит сохранность информации и ее защищенность от несанкционированного доступа.

Полное комплексное обслуживание серверов включает в себя множество операций. В первую очередь оно предполагает собственно монтаж, настройку и обслуживание серверов и серверного оборудования.

Перед тем как осуществить монтаж серверного оборудования, подвергаются серьезному анализу все требования, которые имеются к технике. И на их основе выбирается именно тот вид оснащения и конфигурация системы, которые уместны в данном конкретном случае.

Потом осуществляется установка серверного оборудования, его конфигурирование. Затем его подключают и производят запуск. Устанавливается, тестируется, настраивается и начинает использоваться необходимое программное обеспечение.

Когда все необходимые операции будут произведены, в постоянном режиме обслуживания сервера производится:

–непрерывный мониторинг состояния системы и отдельных ее сервисов

–осуществляется поддержка ее работоспособности

–осуществляется проверка основного и резервного электропитания

–необходимо достаточно часто проверять и заменять аккумуляторы

–работу устройств ввода/вывода, к которым относятся клавиатура, мышь, монитор, свитчи для их подключения к системным блокам, провода и разъемы

–регулярно следует осматривать кабели на предмет внешних повреждений

–проверке также подвергается уровень нагрева тепловыделяющих компонентов аппаратуры

–и работа систем вентиляции и кондиционирования – в данном случае крайне важно, чтобы не было никаких помех для охлаждения оснащения

В операции по обслуживанию сервера также входит ремонт оснащения и замена комплектующих в том случае, если нагрузка на сервер будет повышаться.

Также осуществляется проверка правильности настройки сервера, обеспечение хорошей их работы с помощью частой проверки программных и аппаратных составляющих. Особое внимание уделяется управлению правом доступа к секретной информации и периодическое резервное копирование. В связи с этим происходит постоянная проверка работоспособности и износа оборудования резервного копирования.

Одной из целей выполняемых работ по обслуживанию серверов являются защита данных как от внешних опасностей, к примеру, от несанкционированного доступа и вредоносных программ, именуемых вирусами, так и от внутренних, к которым относятся сбои в работе программного обеспечения.

Помимо прочих вышеуказанных процедур при осуществлении обслуживания серверов, обязательных для совершения, также важно проводить периодическую чистку серверов.

В течение определенного времени в серверном корпусе и блоках питания собирается грязь и пыль, от которой крайне важно своевременно избавляться. В противном случае вы можете столкнуться с крайне неприятной ситуацией - перегревом системы. Также крайне важной процедурой является осмотр рабочей способности вентиляторов. Если не совершать

вышеуказанные процедуры своевременно, в результате может существенно замедлиться работа серверного оснащения или оно даже придет в негодность. Для того чтобы подобная проблема не возникала, вам следует периодически осуществлять проводить проверку и чистку сервера.

Помимо прочих процедур, в перечень услуг, предоставляемых компаниями, занимающимися обслуживанием серверов, также включены работы:

по диагностике и аудиту оснащения

Вряд ли для кого-то будет секретом тот факт, что по истечении определенного промежутка времени системы начинают работать медленнее, что становится заметно без определенных замеров времени. В задачи аудита входит повышение производительности систем и произведение перенастройки и модернизации серверного оснащения. Постоянный контроль помогает осуществить диагностику на ранних этапах возникновения неполадок. Благодаря этому не возникают различные критические ситуации при работе системы.

К операциям по обслуживанию сервера причисляют обновление ОС (операционных систем), программ и контрольной панели.

В связи с этим специалист, занимающийся обслуживанием серверов, периодически осуществляет проверку наличия последних обновлений ПО. Важным направлением работы специалиста, занимающегося обслуживанием серверов, является:

поддержка и администрирование корпоративной почты

К примеру, он будет заниматься образованием и изменением учетных записей почты, обеспечением ее приватности.

Благодаря обслуживанию серверов становится возможной проверка сроков окончания лицензий. Чтобы определить, насколько хорошо будет работать сервер, специалист проверяет его скорость работы, целостность, приходящуюся на него среднюю и пиковую нагрузку, систему дублирования, резервирования и т. д.

В обслуживание серверов входит:

оптимизация интернет-трафика, которая предполагает ее фильтрацию

Осуществляется проверка суммарного внешнего трафика, выясняется, какие порты являются открытыми, заполняются устройства массовой памяти

Существует и такой вид обслуживания серверов, как удаленное администрирование.

Он включает в себя управление учетными записями и соответствующими сетевыми ресурсами. Данный вид работ предполагает обслуживание специализированных серверных ролей, к которым относятся Active Directory, Exchange Server, ISA, SQL и другие.

Организация файл-сервера предприятия на базе Free BSD или Linux

Для централизованного хранения данных, необходимых для работы предприятия, используется файловый сервер. Как правило, это выделенный компьютер, работающий под серверной операционной системой и имеющий быструю и надежную дисковую подсистему. Помимо хранения и организации доступа к документам, файловый сервер решает такую важную задачу, как разграничение прав доступа пользователей к информации. Каждый сотрудник может просматривать или вносить изменения только в те документы, на которые он имеет соответствующие права.

Хранение всех данных в одном месте сильно упрощает управление правами доступа пользователей.

Если в локальной сети присутствуют рабочие станции под управлением операционных систем семейства Windows, что характерно для большинства предприятий, то для общего доступа к файлам и принтерам используется протокол SMB.

Использование серверных продуктов от Microsoft не всегда может оказаться оправданным по экономическим соображениям. Тем более, когда есть альтернатива.

Экономичным и в то же время производительным и надежным решением может выступить операционная система Free BSD или Linux.
Для организации доступа к данным используется свободная реализация SMB протокола – Samba. Установка Samba позволяет использовать компьютер на базе Free BSD или Linux в качестве члена домена либо контроллера домена (PDC) в Windows сети. Так же Samba может стать частью домена Active Directory. Для того чтобы обеспечить общую систему безопасности Active Directory, используется протокол Kerberos. Поддержка данного протокола в FreeBSD может быть реализована при помощи программы heimdal.
Таким образом возможна организация сети предприятия, в которой клиентские машины работают под управлением Windows, в то время как для серверов используют Free BSD или Linux системы.
Несмотря на то, что у некоторых специалистов подобная идея может вызвать сомнение, совместную работу Windows и UNIX систем в одной сети настроить можно. Причем сложность подобного решения вовсе не так высока, как это может показаться на первый взгляд. Вместе с тем, настроить и в дальнейшем обслуживать сервер Linux / Free BSD будет более выгодно силами компаний профессионально занимающихся обслуживанием серверов.
Доступность веб-интерфейсов настройки печати и доступа к файлам, а также возможность настройки при помощи ACL управления правами доступа при помощи стандартного инструментария Windows делают администрирование подобной системы достаточно несложным. С текущим обслуживанием сервера может справиться любой сотрудник, имеющий минимальные навыки работы в операционных системах, схожих с UNIX. Опытный администратор или специализированная компания, предоставляющая услуги по обслуживанию серверов Linux / Free BSD понадобится только на этапе проектирования и внедрения системы, а также при внесении достаточно сложных изменений.

К преимуществам серверов, работающих под управлением Free BSD или Linux систем, можно отнести:

–высокую производительность

–возможность гибкой настройки практически под любые задачи

–и высокую стабильность.

Системы Free BSD и Linux отличаются большой гибкостью настройки. Их можно адаптировать практические под любые задачи. На работающем сервере будут исполняться только те процессы, которые необходимы, что экономит системные ресурсы и снижает вероятность возникновения программного сбоя.
Обслуживание файлового сервера на основе Free BSD с установленной Samba может осуществляться путем внесения изменений в файл конфигурации smb.conf, который после инсталляции Samba должен находиться по адресу /usr/local/etc/smb.conf. Его можно создать либо воспользоваться образцом smb.conf.sample, куда вносятся все необходимые изменения. Для облегчения процесса настройки Samba можно использовать веб-интерфейс SWAT. К преимуществам его использования, помимо графического интерфейса, можно отнести хорошую систему справки по всем параметрам настройки.
Порой возникает ситуация, когда руководителю или ответственному сотруднику необходимо изменить права доступа к отдельным файлам и папкам. Если администратор отсутствует, это может оказаться затруднительным. Ведь далеко не все пользователи имеют навыки работы в Free BSD или Linux системах. Для того чтобы организовать возможность настройки прав доступа к файлам и каталогам при помощи проводника Windows, можно использовать списки доступа ACL (Access Control Lists). Поддержка ACL реализована в большинстве актуальных версий Free BSD или Linux на уровне ядра – все, что необходимо, - это включить ее для выбранных файловых систем.
Нередко, помимо хранения и предоставления доступа к документам, файл-сервер выполняет и некоторые другие функции. Достаточно часто файловый сервер является и сервером

печати, то есть организует возможность работать с принтерами для всех рабочих станций сети предприятия. В случае при обслуживании сервера с установленной операционной системы Free BSD используется система печати CUPS. Для упрощения процедуры настройки доступен веб-интерфейс.
Кроме того, именно на файл-сервер обычно ложится организация резервного копирования. Собранные в одном месте данные, без которых работа предприятия в нормальном режиме попросту невозможна, очень уязвимы.
Причин повреждения данных может быть множество – это аппаратная неисправность, проблемы с электропитанием, воздействия вредоносного ПО или пожар, но все они могут принести предприятию значительные убытки. Для того чтобы предотвратить потерю данных, необходимо при выполнении регулярного обслуживания сервера делать резервные копии всех важных документов и хранить их в надежном, желательно удаленном от сервера месте.
Существует три основных типа серверов удалённого доступа:
серверы удаленного управления
серверы удаленных узлов
и терминальные серверы

Серверы удаленных узлов выступают в роли маршрутизаторов, или шлюзов, выполняя лишь транспортный сервис, тем самым соединяя клиентов с центральной сетью. Обслуживание серверов происходит при использовании протоколов IP, IPX или NetBIOS.
Серверы удаленного управления помогают обеспечить транспортный сервис, а также способны запускать от имени клиента различные приложения на компьютерах, подсоединённых к центральной сети, на экране удаленного компьютера создают образ графической среды этого приложения. Как правило, серверы удалённого управления работают с системой Windows.
Терминальные серверы работают аналогично, но при использовании многотерминальных операционных систем, таких как Unix, VAX VMS, IBM VM.
Терминальный сервер обеспечивает клиентов вычислительными ресурсами: память, процессорное время и пр. С технической стороны вопроса терминальный сервер – это мощный компьютер высокой производительности, который способен обслужить одновременно несколько пользователей. Расположение терминального сервера для работы не имеет значения – он может находиться как в соседней комнате, так и в другой стране.
Доступ к серверу и обслуживание сервера обеспечивают специальные терминальные клиенты – программы, которые в течение работы воспроизводят данные по работе сервера.
Обслуживание сервера контроллера доменов
Для того чтобы повысить эффективность любой ИТ-инфраструктуры, очень важно правильно выполнить все необходимые настройки на базе вашей операционной системы.

Качественная настройка и обслуживание сервера включает в себя:
–настройку всех основных служб для работы сети
–таких как контроллер домена
–сервер баз данных
–файл-сервер
–почтовый и прокси-серверы и т. д.

Сервер терминалов достаточно часто используется при совместной работе в программе 1С. Это позволяет не только значительно повысить производительность программного обеспечения 1С, но и обеспечить высокую надежность программы и возможный удаленный доступ к 1С через Интернет.

При необходимости в некоторой степени экономить интернет-траффик при полном контроле доступа в глобальную сеть в офисе хорошим решением становится установка интернет-шлюза и прокси-сервера и дальнейшее обслуживание северов этих типов. При настройке ограничения доступа в глобальную сеть Интернет появляется возможность намного эффективнее использовать рабочее время ваших сотрудников.
При установке важно убедиться в том, что сервер, на который устанавливается Active Directory, имеет специальный раздел с файловой системой NTFS. Также перед установкой важно убедиться в том, что служба DNS правильно настроена. Обратите внимание на то, что сервер может вести себя по-разному, что следует учитывать при обслуживании сервера, в зависимости от версии и выпуска установленной операционной системы, а также прав и разрешений учетной записи и настроек меню.

Какое же оборудование может понадобиться для установки сервера на предприятии? К нему относятся:

- коммутаторы
- маршрутизаторы
- принт-серверы и прочее

А для того чтобы оборудование не выходило из строя, требуется своевременное обслуживание сервера.
Благодаря своевременному обслуживанию сервера появляется возможность значительно увеличить срок его службы, а также избежать его внезапного выхода из строя. Оперативно устранять ошибки в программной части сервера возможно даже при удаленном обслуживании сервера. Если вы являетесь владельцем малого или среднего бизнеса и используете на фирме небольшое количество серверов, то чаще всего содержать в штате высококвалифицированного, а, следовательно, и высокооплачиваемого специалиста для настроек и обслуживания сервера довольно часто экономически нецелесообразно. Поэтому обслуживание серверов логичнее и более экономически выгодно поручить компании, которая специализируется по данному профилю.

Обслуживание серверов windows 2003 и windows 2008

Сегодня практически каждая компания старается оборудовать свой офис различными видами оргтехники, первое место среди которой занимает компьютер. Компьютеризировать офис – это всего лишь пол дела, надо научиться грамотно обслуживать дорогостоящую технику. Корректная настройка позволяет повысить эффективность деятельности хозяйствующего субъекта. Столь популярные на сегодняшний день автоматизированные системы и программные продукты, позволяющие облегчить ведение учета и контроля за теми или иными процессами. Но для их полноценного функционирования необходимо создание определенных условий, в частности это касается операционной системы и набора дополнительных программных модулей. На сегодняшний день многие компании для повышения эффективности ИТ-инфраструктуры устанавливают и настраивают сервера именно на базе операционной системы Windows Server.
Обслуживание компьютеров, обслуживание сервера windows 2003 или обслуживание сервера windows 2008 считается одной из важных расходных статей для любой компании. Обслуживание техники заключается не только в поддержке оборудования в рабочем состоянии, но и в эффективных методах борьбы с вредоносными программами, обновлении базы данных, переустановке операционной системы и пр.
Сегодня сервера – это надёжное обеспечение как на аппаратном, так и на программном уровне. Однако не стоит забывать, что своевременное обслуживание сервера windows 2003 и обслуживание сервера windows 2008 позволит увеличить его работоспособность и значительно продлить срок службы. Обслуживание сервера windows 2003 и обслуживание сервера windows 2008 возможное в виде удаленного обслуживания указанных серверов

позволит оперативно исправлять большое количество ошибок в программной части серверов.
Качественная настройка и обслуживание сервера windows 2008, windows 2003 подразумевает комплексную настройку основных служб для работы внутренней сети предприятия, т.е. подключение интернет-шлюза, файл-сервера, сервера баз данных, почтового сервера, DNS, DHCP, VPN и пр.
Данная система предназначена для серверного использования, в домашних условиях её применяют крайне редко. Конечно, при большом желании и грамотном обслуживании сервера windows 2003, вполне возможно использовать и на домашнем ПК эту операционную систему, но лучше для таких целей предназначены другие операционные системы.
Ещё одна операционная система от компании Microsoft, которая отлично подходит для использования на предприятии - Windows Server 2008.
Гибкая и надёжная операционная система Windows Server 2008 включает в свой состав новые технологии, к примеру, режим Server Core, командная оболочка Windows PowerShell и др. Модернизированные сетевые технологии Windows Server 2008 повышают управляемость и доступность серверной инфраструктуры. Качественное и выгодное обслуживание сервера windows 2008 разрешает сэкономить время и значительно сократить затраты.
Если обслуживание сервера windows 2008 проводится качественно, то данная ОС позволяет реализовать заложенный в ней потенциал, существенно улучшая и расширяя возможности по администрированию, диагностике, управлению службами и сервисами.
Значительно повысить эффективность использования оборудования и улучшить доступность серверов помогает встроенная технология виртуализации Windows Server 2008. Кроме того, Windows Server 2008 считается самым защищённым из всех аналогичных продуктов. Повышенную безопасность операционной системе гарантируют защита сетевого доступа, контроллер домена только для чтения и федеративные службы управления правами. Обслуживание сервера windows 2008 на предприятии позволяет полностью обезопасить бизнес в целом.
Стоит отметить, что серверы Windows Server 2008 могут быть использованы в качестве терминального сервера в том случае, если это редакции Standard, Enterprise и Datacenter, содержащие службы Terminal Services. Обслуживание сервера windows 2008 подразумевает обеспечение каждого пользователя лицензией Windows CAL, а также отдельной клиентской лицензией на доступ к серверу терминалов.

Контрольные вопросы:

1. Понятие сервера. Типы серверов.
2. ОС для серверов

Практическое занятие №3

Изучение уровней управления модели OSI

Цель занятия: изучить назначение и уровни сетевой модели.

Оборудование: справочный материал.

Ход занятия:

Изучить теоретические сведения:

Сетевая система конструируется по слоям или уровням. Каждый уровень выполняет определенный набор присущих ему функций. В результате объединения уровней образуется сетевая архитектура. Сетевая архитектура выделяет функции связи по определенным логическим группам — уровням, что в значительной степени упрощает стандартизацию. Главной чертой открытой сетевой архитектуры является то, что правила взаимодействия уровней не представляют закрытую информацию или собственность какой-либо организации, а открыты для всеобщего изучения и использования.

Каждый уровень имеет свои определенные правила и процедуры, которые называются протоколами. Протоколы регулируют активность в пределах уровня и характер взаимодействия между уровнями. Допускается взаимодействие как между соседними уровнями по вертикали в пределах одного сетевого устройства, так и между однотипными уровнями разных сетевых устройств. В результате этого происходит передача и преобразование данных между уровнями в пределах одного сетевого устройства и между различными сетевыми устройствами. Уровни независимы друг от друга в том смысле, что изменение одного уровня или его внутренних протоколов не влечет изменения протоколов в соседних уровнях.

Разделение на уровни очень удобно и позволяет следующее:
- упростить конструирование сети и структурировать ее функции;
- расширить набор приложений, ориентированных на пользователей сети;
- обеспечить наращивание сети в процессе ее развития.

Наибольшую популярность в мире получила открытая сетевая архитектура, использующая в своей основе эталонную модель взаимодействия открытых систем или ЭМВОС (Open Systems Interconnection/Reference Model), или кратко модель OSI (ВОС).

Эта семиуровневая модель была разработана в 1977 г. совместно ISO и CCITT (современное название ITU-T) и на сегодняшний день составляет основу для развития международных стандартов в области компьютерных коммуникаций, табл. 5.4 [12].

Таблица 5.4. Уровни модели OSI и их основные функции

Уровень (layer)	Назначение
1 Физический (Physical)	Ответственен за физические, электрические характеристики линии связи, между узлами (коаксиальные кабели; витые пары; волоконно-оптические кабели; разъемы, например RJ-45, AUI, DB-9, MIC, ST, SC; повторители; транн сиверы и т.д.).
2 Канальный (Data Unk)	Обеспечивает надежную передачу данных по физическим линиям связи. На этом уровне (эвена данных) происходит исправление ошибок передачи, ко^ дирование и декодирование отправляемых или принимаемых битовых последовательностей. Канальный уровень подразделяется на подуровень Medium Access Control (MAC) — Управление доступом к среде и на подуровень Logical Link Control (LLC) —

	Управление логическим каналом. Уровень MAC -определяет характер доступа к среде — детерминированный доступ с передачей маркера (Arcnet, Token Ring, FDDI, 100VG AnyLAN) или множественный доступ с распознаванием коллизий (Ethernet — IEEE 802.3). Уровень LLC -верхний подуровень -. посылает и получает сообщения с полезными данными.
3 Сетевой , (Network)	Обеспечивает для верхних уровней независимость от стандарта передачи данных (прозрачность), оперирует с такими протоколами, как IPX, TCP/IP и др., а также отвечает за адресацию и доставку сообщений.
4 Транспортный (Transport)	Управляет упорядочиванием компонентов сообщений и регулирует входящий поток, если на обработку приходит два или более пакетов одновременно. Дублированные пакеты распознаются этим уровнем и лишние дубликаты фильтруются.
5 Сессионный (Session)	Открывает соединение (сессию или сеанс), поддерживает диалог, т.е. управляет отправкой сообщений туда и обратно, и закрывает сессии. Этот уровень позволяет прикладным программам, работающим на разных сетевых устройствах, координировать свое взаимодействие в рамках отдельных сессий (сеансов).
6 Представительный (Presentation)	Осуществляет преобразования данных из внутреннего числового формата, присущего данному сетевому устройству, в стандартный коммуникационный формат. Примеры: кодирование, сжатие, переформатирование текста.
7 Прикладной (Application)	Предоставляет программисту интерфейс к модели OSi. Примеры: сервер транзакций, протокол FTP, сетевое администрирование.

Уровни с меньшим номером принято называть низкими уровнями, а уровни с большим Номером — высокими.

Стандарты IEEE 802

Сетевые протоколы и стандарты, охватывающие два нижних уровня модели OSI (физический и канальный) были разработаны комитетом IEEE 8802 (сокращенно IEEE 802). Получила распространение несколько различных вариантов построения этих уровней. Причем у канального уровня только его нижний подуровень — MAC (управление доступом к среде) — был выделен и объединен с физическим уровнем для организации сетевого стандарта. Таким образом, протоколы подуровня LLC (канального уровня) и более высоких уровней 3, 4 и т.д. остались независимыми от сетевых стандартов, Следует отметить, что стандарт FDDI, несмотря на то, что был разработан другой организацией, также включен в эту группу сетевых стандартов, так как он выполнен в полном соответствии с эталонной моделью OSI/IEEE 802.

Контрольные вопросы:

1. Уровни модели OSI.
2. Понятие протокола.

Практическое занятие № 4

Стек протоколов TCP/IP. Диагностические утилиты протокола.

Цель работы: практически освоить работу с утилитами TCP/IP, необходимыми в следующих работах.

Оборудование: инструкционные карты, ПК

Методические указания

Так как стек TCP/IP был разработан до появления модели взаимодействия открытых систем ISO/OSI, то, хотя он также имеет многоуровневую структуру, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Структура протоколов TCP/IP приведена на рисунке . Протоколы TCP/IP делятся на 4 уровня.

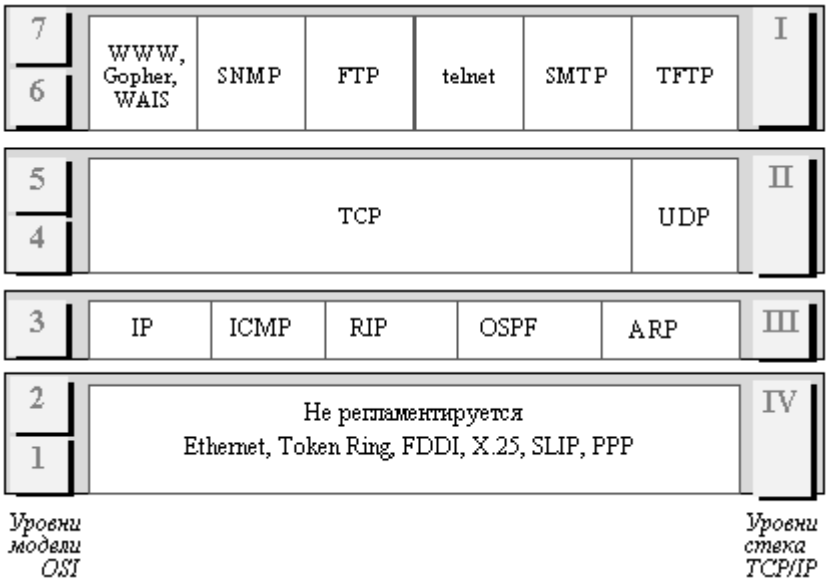


Рис. Стек TCP/IP

Диагностические утилиты TCP/IP.
В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения.

Утилита	**Применение**
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control

	Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
telnet	Осуществляет соединение с другим хостом по протоколу эмуляции терминала TELNET. Используется для проверки работоспособности сетевых служб, использующих tcp-порты (например, возможности соединения с почтовым сервером по протоколам POP3 и SMTP).

1. Проверка правильности конфигурации TCP/IP с помощью ipconfig.

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

Параметры:

all выдает весь список параметров. Без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

renew[adapter] обновляет параметры конфигурации DHCP для указанного сетевого адаптера;

release[adapter] освобождает выделенный DHCP IP-адрес;

adapter – имя сетевого адаптера;

displaydns выводит информацию о содержимом локального кэша клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

- если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;

- если IP-адреса дублируются, то маска сети будет 0.0.0.0;
- если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0 .

2. Тестирование связи с использованием утилиты *ping*.

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

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

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

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

Утилита ping используется следующими способами:

1) Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address):
ping 127.0.0.1

Если тест успешно пройден, то вы получите следующий ответ:

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

2) Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера:

ping IP-адрес_локального_хоста

3) Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping IP-адрес_шлюза

4) Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

ping IP-адрес_удаленного хоста

Синтаксис:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] |

[-k host-list]] [-w timeout] destination-list

Параметры:

-t выполняет команду ping до прерывания. Control-Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

-a позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count посылает количество пакетов ECHO, указанное параметром count;

-l length посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos устанавливает тип поля «сервис» в величину tos;

-r count записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;

-s count позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;

-w timeout указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);

destination-list указывает удаленный хост, к которому надо направить пакеты ping.

<u>Пример использования утилиты ping:</u>

C:\WINDOWS>ping –n 10 www.netscape.com

Обмен пакетами с www.netscape.com [205.188.247.65] по 32 байт:

Ответ от 205.188.247.65: число байт=32 время=194мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=240мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=173мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=250мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=187мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=239мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=263мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=230мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=185мс TTL=48

Ответ от 205.188.247.65: число байт=32 время=406мс TTL=48

Статистика Ping для 205.188.247.65:

Пакетов: послано = 10, получено = 10, потеряно = 0 (0% потерь)

Приблизительное время передачи и приема:

Наименьшее = 173мс, наибольшее = 406мс, среднее =236мс

В случае невозможности проверить доступность хоста утилита выводит информацию об ошибке. Ниже приведен пример ответа утилиты ping при попытке послать запрос на несуществующий хост.

Обмен пакетами с 172.16.6.21 по 32 байт:

Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 172.16.6.21:
Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потерь),

Приблизительное время передачи и приема:

наименьшее = 0мс, наибольшее = 0мс, среднее = 0мс

Утилита сообщает не об отсутствии хоста, а о том, что за отведенное время не был получен ответ на посланный запрос. Причиной этого не обязательно является отсутствие хоста в сети. Проблема может крыться в сбоях связи, перегрузке или неправильной настройке маршрутизаторов и т. п. Ошибка «сеть недоступна» (network unreachable) прямо указывает на проблемы маршрутизации.

3. Изучение маршрута между сетевыми соединениями с помощью утилиты *tracert*.

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

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

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

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

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

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста

Параметры:

-d указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops указывает максимальное число хопов для того, чтобы искать цель;

-j host-list указывает нежесткую статическую маршрутизацию в соответствии с host-list;

-w timeout указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

4. Утилита *arp*.

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

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметры:

-s занесение в кэш статических записей;

-d удаление из кэша записи для определенного IP-адреса;

-a просмотр содержимого кэша для всех сетевых адаптеров локального компьютера;

inet_addr - IP-адрес;

eth_addr - MAC-адрес.

5. Утилита route.

Утилита **route** предназначена для работы с локальной таблицей маршрутизации. Она имеет следующий

Синтаксис:
route [-f] [-p] [команда [узел] [MASK маска] [шлюз] [METRIC метрика] [IF интерфейс]]

Параметры:

-f Очистка таблицы маршрутизации.

-p При указании совместно с командой ADD создает постоянную запись, которая сохраняется после перезагрузки компьютера. По умолчанию записи таблицы маршрутов не сохраняются при перезагрузке.

команда одна из четырех команд:

PRINT - вывод информации о маршруте;

ADD - добавление маршрута;

DELETE - удаление маршрута;

CHANGE - изменение маршрута.

узел адресуемый узел

маска маска подсети; по умолчанию используется маска 255.255.255.255

шлюз адрес шлюза

метрика метрика маршрута;

интерфейс идентификатор интерфейса, который будет использован для пересылки пакета

Для команд PRINT и DELETE возможно использование символов подстановки при указании адресуемого узла или шлюза. Параметр шлюза для этих команд может быть опущен.

При добавлении и изменении маршрутов утилита route осуществляет проверку введенной информации на соответствие условию (УЗЕЛ & МАСКА) == УЗЕЛ. Если это условие не выполняется, то утилита выдает сообщение об ошибке и не добавляет или не изменяет маршрут.

Утилита осуществляет поиск имен сетей в файле networks. Поиск имен шлюзов осуществляется в файле hosts. Оба файла расположены в папке %systemroot%\system32\drivers\etc. Наличие и заполнение этих файлов не обязательно для нормального функционирования утилиты route и работы маршрутизации.

Хотя в большинстве случаев на рабочей станции это не требуется, можно вручную редактировать таблицы маршрутизации.

Пример использования утилиты route:

Добавление статического маршрута:
route add 172.16.6.0 MASK 255.255.255.0 172.16.11.1 METRIC 1 IF 0x1000003

6. Утилита *netstat*.

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

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

Параметры:

-a выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n выводит информацию по всем текущим соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;

-s выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет просмотреть информацию постранично;

-r выводит содержимое таблицы маршрутизации.

7. Утилита *nslookup*.

Утилита **nslookup** предназначена для диагностики службы DNS, в простейшем случае - для выполнения запросов к DNS-серверам на разрешение имен в IP-адреса. В общем случае утилита позволяет просмотреть любые записи DNS-сервера:

A – каноническое имя узла, устанавливает соответствие доменного имени ip-адресу.

SOA – начало полномочий, начальная запись, единственная для зоны;

MX – почтовые серверы (хосты, принимающие почту для заданного домена);

NS – серверы имен (содержит авторитетные DNS-серверы для зоны);

PTR – указатель (служит для обратного преобразования ip-адреса в символьное имя хоста)

и т. д.

Утилита nslookup достаточно сложна и содержит свой собственный командный интерпретатор.

В простейшем случае (без входа в командный режим) утилита **nslookup** имеет следующий

Синтаксис:
nslookup хост [сервер]

Параметры:

Хост DNS-имя хоста, которое должно быть преобразовано в IP-адрес.

Сервер Адрес DNS-сервера, который будет использоваться для разрешения имени. Если этот параметр опущен, то будут последовательно использованы адреса DNS-серверов из параметров настройки протокола TCP/IP.

8. Утилита *telnet*.

Утилита telnet (_en. **TEL**ecommunication **NET**work) реализует клиентскую часть сетевого протокола telnet, организующего текстовый интерфейс по сети (при помощи транспортного протокола TCP).

Исторически Telnet служил для удалённого доступа к интерфейсу командной строки операционных систем. Впоследствии его стали использовать для прочих текстовых интерфейсов, вплоть до игр MUD и анимированного ASCII-art. Теоретически, даже обе стороны протокола могут являться программами, а не человеком.

Иногда клиенты telnet используются для доступа к другим протоколам на основе транспорта TCP.

Протокол telnet используется в управляющем соединении FTP, т.е. заходить на сервер командой telnet ftp.example.net ftp для выполнения отладки и экспериментов не только возможно, но и **правильно** (в отличие от применения клиентов telnet для доступа к HTTP, IRC и большинству других протоколов).

В протоколе не предусмотрело ни шифрования, ни проверки подлинности данных. Поэтому он уязвим для любого вида атак на TCP. Для функциональности удалённого доступа к системе в настоящее время применяется сетевой протокол SSH (особенно его версия 2), при создании которого упор делался именно на вопросы безопасности. Следует иметь в виду, что сессия telnet обладает крайне низкой защищенностью, если только не осуществляется в полностью контролируемой сети или с применением защиты на сетевом уровне (различные реализации виртуальных частных сетей). По причине ненадёжности от telnet как средства управления операционными системами давно отказались.

Тем не менее, клиент telnet пригоден для осуществления ручного доступа (например, в целях отладки) к таким протоколам прикладного уровня как HTTP, IRC, SMTP, POP3 и прочим текст-ориентированным протоколам на основе транспорта TCP.

По умолчанию (если порт не задан), telnet использует порт 23.

Синтаксис:

telnet имя_узла номер_порта

Примеры использования утилиты telnet:

1) Доступ к почтовому серверу по протоколу POP3 (проверка работоспособности почтового ящика).

Введите:
telnet имя_почтового_сервера 110

Ответ сервера:
+OK Hello there.

В качестве имени пользователя введите свой адрес электронной почты:
user test@domain.ru

Ответ сервера:
+OK Password required.

Введите пароль для этого почтового ящика:
pass *пароль*

Ответ сервера:
+OK logged in.

Для выхода введите:
quit

+OK Bye-bye

2) Проверка доступа к smtp-серверу.
Введите:
telnet имя_почтового_сервера 25

Если в результате Вы получите сообщение, начинающееся с цифры 2, то у Вас есть доступ к smtp-серверу, в противном случае можно судить об ошибке.

Задание

1. Изучите методические указания к лабораторной работе.
2. Выполните упражнения.
3. Оформите отчет по лабораторной работе, описав выполнение упражнений и дав краткие ответы на контрольные вопросы.

Упражнение 1. Получение справочной информации по командам.
Выведите на экран справочную информацию по всем рассмотренным утилитам (см. таблицу п.1). Для этого в командной строке введите имя утилиты без параметров или с /?. Для получения справочной информации по nslookup необходимо войти в командный режим, набрав nslookup без параметров, и ввести команду help.

Изучите ключи, используемые при запуске утилит.

Упражнение 2. Получение имени хоста.
Выведите на экран имя локального хоста с помощью команды hostname.

Упражнение 3. Изучение утилиты ipconfig.
Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

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

Упражнение 4. Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.
3. Проверьте функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта.
4. Проверьте возможность установления соединения с удаленным хостом.
5. С помощью команды ping проверьте перечисленные ниже адреса и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

a) stg-m.ru
b) router.auditory.ru
c) любой узел из локальной сети

Упражнение 5. Определение пути IP-пакета.
С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Время жизни установить равным 10. Отметьте их:

a) 195.82.146.114

b) yandex.ru

c) 213.247.189.211

Упражнение 6: Просмотр ARP-кэша.

С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

Внести в кэш локального компьютера любую статическую запись.

Упражнение 7: Просмотр локальной таблицы маршрутизации.
С помощью утилиты route просмотреть локальную таблицу маршрутизации.

Упражнение 8. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.
С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Упражнение 9. Получение DNS-информации с помощью nslookup.
1) Узнайте ip-адреса узлов:

auditory.ru

photo.auditory.ru

sova.auditory.ru

wiki.auditory.ru

share.auditory.ru

2) Узнайте авторитетные (компетентные) сервера для этих узлов.

3) Получите запись SOA с одного из этих серверов для домена auditory.ru.

Упражнение 10. Диагностика tcp-соединений с помощью утилиты telnet.

1) Проверить, принимает ли хост share.auditory.ru подключения по SMB (445 порт).

2) Присоединиться к 4899 порту хоста 213.247.189.211.

3) Узнать, какой почтовый сервер использует Майкрософт (использовать nslookup + telnet)

Контрольные вопросы:

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети, авторитетный/неавторитетный (компетентный) DNS-сервер, порт TCP, петля обратной связи, время отклика.
2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
3. Каким образом каманда ping проверяет соединение с удаленным хостом?
4. Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?
5. Как работает утилита tracert?
6. Каково назначение протокола ARP?
7. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
8. Какие могут быть причины неудачного завершения ping и tracert? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).
9. Объяснить, каким образом при неудачной проверке маршрута до хоста 213.247.189.211, к нему возможно подключиться telnet'ом.
10. Всегда ли можно узнать символьное имя узла по его ip-адресу?
11. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

Практическое занятие №5

Изучение сетевого адаптера

Цель: изучить принцип действия сетевого адаптера**.**

Оборудование: адаптер, ПК, справочный материал.

Теоретические сведения:

Сетевой адаптер (сетевая карта) — периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети. Сетевые адаптеры работают на втором уровне модели OSI. Адаптеры различаются по типу интеграции с компьютером (PCI, USB, PCMCIA, встроенные), по виду используемой среды передачи данных (витая пара, оптоволокно), а также по поддерживаемым технологиям (Ethernet 10Mbit/100Mbit/1Gbit).
Совместно со своим драйвером, сетевая карта реализует на конечном узле (компьютере) физический и канальный уровень модели OSI, причем подуровень LLC (Logical Link Control. *Каковы его функции?*) реализуется как правило средствами операционной системы. В задачи сетевого адаптера в совокупности с драйвером входит прием и отправка кадров в сеть. Операция передачи данных обычно состоит из следующих этапов:
1. Прием LLC кадра
2. Оформление MAC-кадра
3. Кодирование с избыточностью и скремблирование
4. Выдача сигналов в кабель с помощью линейных кодов (Манчестер, NRZI и.т.п.)

Прием кадра из сети фактически повторяет данную последовательность, но в обратном порядке.
1. Прием сигналов
2. Выделение сигналов на фоне шума и дескремблирование
3. Подсчет контрольной суммы кадра. Если контрольная сумма неверна, то кадр отбрасывается и происходит отправка LLC сообщения с кодом ошибки.

В соответствие с периодами функционального развития сетевых адаптеров, производят их разделение на 4 поколения. Сейчас используются адаптеры четвертого поколения, которые характеризуются высокой скоростью передачи данных (Gigabit Ethernet), собственным процессором для обработки кадров, а так же реализацией большого числа высокоуровневых функций (например, удаленного мониторинга).

Настройка параметров сетевого адаптера

Настройка параметров сетевого адаптера в операционной системе Linux производится с помощью консольных утилит **ifconfig**, **ethtool** и **mii-tool**.
Вывод общей информации о настройках сетевого адаптера производится с помощью команды
ethtool eth0
Где eth0 — символьное имя сетевого интерфейса в операционной системе (полный список интерфейсов доступен с помощью команды **ifconfig -a**).
Получить информацию об используемом драйвере можно с помощью команды
ethtool -i <имя_интерфейса>
Перед изменением какого-либо из параметров адаптера рекомендуется отключать его командой
ifconfig <имя_интерфейса> down.
После изменения нового параметра адаптер следует включить командой

ifconfig <имя_интерфейса> up
7
Settings for eth0:
Supported ports: [TP]
Supported link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Supports auto-negotiation: Yes
Advertised link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Advertised pause frame use: No
Advertised auto-negotiation: Yes
Speed: 100Mb/s
Duplex: Full
Port: Twisted Pair
PHYAD: 2
Transceiver: internal
Auto-negotiation: on
MDI-X: off
Supports Wake-on: pumbag
Wake-on: d
Current message level: 0x00000001 (1)
drv
Link detected: yes
Листинг 1: Вывод информации о сетевом адаптере командой ethtool
8
Значения некоторых полей вывода представлено в следующей таблице.
Параметр Значение
Supported link modes Поддерживаемые режимы связи
Supported auto-negotiation Поддержка режима авто-согласования
Speed Текущая скорость приема/передачи
Duplex Режим двухстороннего обмена
Transceiver Тип передатчика
Auto-negotiation Состояние режима авто-согласования
Link detected Состояние соединения
Таблица 3: Значения параметров вывода ethtool
Режим авто-согласования
Режим авто-согласования предполагает, что сетевое устройство само определяет присутствует ли двусторонний обмен и сколько мегабит он
составляет, поэтому при установке собственных параметров сетевого адаптера, отличных от стандартных (определенных в ходе авто-согласования) следует отключать данный режим.
Существует два режима двухстороннего обмена:
- Дуплекс (полный) — устройства принимают и передают данные по двум разделенным физически каналам. Из этого следует отсутствие коллизий.
- Половинный (полу-дуплекс) — устройства в каждый момент времени могут либо передавать либо только принимать данные. Принимающее данные устройство не может при этом ничего передавать вынуждено дожидаться окончания приема.
Изменить режим двухстороннего обмена можно командой
ethtool -s <имя_интерфейса> duplex <half|full> autoneg off

Чтобы получить подробную статистику по интерфейсу воспользуйтесь Командой **ethtool -S <имя_интерфейса>**
Информацию о прочих параметрах команды ethtool можно получить с помощью утилиты man.

Задания

1. Получить информацию о драйвере сетевого адаптера, скорости соединения и режиме двухстороннего обмена.
2. Переключить сетевой адаптер в режим half-duplex, загрузить предложенный тестовый файл и вывести статистику. Далее, переключить адаптер в режим full-duplex, загрузить тот же файл, вывести статистику. Сравнить полученные значения, а так же скорость загрузки файла.
3. Используя справку по утилите ethtool для получения соответствующих параметров команд проведите:

a) Online тестирование сетевого адаптера.
b) Получите информацию о параметрах управления высокой нагрузкой (offload) сетевого адаптера. Попробуйте самостоятельно описать каждый из параметров.
c) Выведите дамп состояния регистров сетевого устройства. Насколько полезной может быть полученная информация?

Примечание: *Для загрузки файла предлагается использовать консольную утилиту wget.*

Практическое занятие №6
Расчет Ethernet –сетей, состоящих из сегментов различных технологий

Цель работы: изучение принципов построения сетей по стандарту Ethernet и приобретение практических навыков оценки корректности их конфигурации.

Оборудование: справочный материал.

Ход занятия:

Принципы расчета конфигурации сети

Соблюдение многочисленных ограничений, установленных для различных стандартов физического уровня сетей Ethernet, гарантирует корректную работу сети (естественно, при исправном состоянии всех элементов физического уровня). Основные характеристики и ограничения технологии Ethernet приведены в таблицах 6.1 и 6.2.

Таблица 6.1 - Общие ограничения для всех стандартов Ethernet

Характеристика	Значение
Номинальная пропускная способность	10 Мбит/с
Максимальное число станций в сети	1024
Максимальное расстояние между узлами в сети	2500 м (в 10Base-FB - 2750 м)
Максимальное число коаксиальных сегментов в сети	5

Таблица 6.2 - Параметры спецификаций физического уровня для стандарта Ethernet

Параметр	10Base-5	10Base-2	10Базе-Т	10Base- F
Кабель	Толстый коаксиальный кабель RG-8 или RG-11	Тонкий коаксиальный кабель RG-58	Неэкранированная витая пара категорий 3,4,5	Многомодовый волоконно-оптический кабель
Максимальная длина сегмента, м	500	185	100	2000
Максимальное расстояние между узлами сети (при использовании повторителей), м	2500	925	500	2500(2740 для 10Base-FB)
Максимальное число станций в сегменте	100	30	1024	1024
Максимальное число повторителей между любыми станциями сети	4	4	4	4 (5 для 10Base-FB)

Наиболее часто приходится проверять ограничения, связанные с длиной отдельного сегмента кабеля, а также количеством повторителей и общей длиной сети.

Правила «5-4-3» *(допускается соединение в линию до 5 сегментов не более чем через 4 повторителя, из этих сегментов только 3 могут использоваться для подключения узлов (Trunk segments), остальные (Link segments)* используются как удлинители) для коаксиальных сетей и «4 хабов» *(число повторителей (концентраторов) между любыми двумя компьютерами в сети Ethernet не может быть больше четырех)* для сетей на основе витой пары и оптоволокна не только дают гарантии работоспособности сети, но и оставляют большой «запас прочности» сети. Например, если посчитать время двойного оборота в сети,

состоящей из 4 повторителей 10Base-5 и 5 сегментов максимальный длины 500 м, то окажется, что оно составляет 537 битовых интервала. А так как время передачи кадра минимальной длины (вместе с преамбулой), составляющей 72 байт, равно 575 битовым интервалам, то видно, что разработчики стандарта Ethernet оставили 38 битовых интервала в качестве запаса для обеспечения надежности. Тем не менее в документах комитета IEEE 802.3 утверждается, что и 4 дополнительных битовых интервала создают достаточный запас надежности.

Комитет IEEE 802.3 приводит исходные данные о задержках (таблицы 6.3 и 6.4), вносимых повторителями и различными средами передачи данных, для тех специалистов, которые хотят самостоятельно рассчитывать максимальное количество повторителей и максимальную общую длину сети, не довольствуясь теми значениями, которые приведены в правилах «5-4-3» и «4 хабов».

Таблица 6.3 - Данные для расчета значения PDV*(Path Delay Value - время двойного оборота)*

Тип сегмента	База левого сегмента, bt	База промежуточного сегмента, bt	База правого сегмента, bt	Задержка среды на 1 м, bt	Максимальная длина сегмента, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	-	24,0	-	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000
FOIRL	7,8	29,0	152,0	0,1	1000
AUI (>2 м)	0	0	0	0,1026	2+48

Таблица 6.4 - Уменьшение межкадрового интервала повторителями

	Передающий сегмент, bt	Промежуточный сегмент, bt
10Base-5 или 10Base-2	16	11
10Base-FB	-	2
10Base-FL	10,5	8
10Base-T	10,5	8

Особенно такие расчеты полезны для сетей, состоящих из смешанных кабельных систем, например, коаксиала и оптоволокна, на которые правила о количестве повторителей не рассчитаны. При этом максимальная длина каждого отдельного физического сегмента должна строго соответствовать стандарту, то есть 500 м для «толстого» коаксиала, 100 м для витой пары и т. д.

Чтобы сеть Ethernet, состоящая из сегментов различной физической природы, работала корректно, необходимо выполнение четырех основных условий:

- количество станций в сети - не более 1024;
- максимальная длина каждого физического сегмента - не более величины, определенной в соответствующем стандарте физического уровня;
- время двойного оборота сигнала (Path Delay Value, PDV) между двумя самыми удаленными друг от друга станциями сети - не более 575 битовых интервала;
- сокращение межкадрового интервала (Path Variability Value, PVV) при прохождении последовательности кадров через все повторители - не больше, чем 49 битовых интервала (так как при отправке кадров конечные узлы обеспечивают начальное межкадровое

расстояние в 96 битовых интервала, то после прохождения повторителя оно должно быть не меньше, чем 96 - 49 = 47 битовых интервала).
Соблюдение этих требований обеспечивает корректность работы сети даже в случаях, когда нарушаются простые правила конфигурирования, определяющие максимальное количество повторителей и общую длину сети в 2500 м.

Методика расчета времени двойного оборота и уменьшения межкадрового интервала
Для упрощения расчетов обычно используются справочные данные IEEE, содержащие значения задержек распространения сигналов в повторителях, приемопередатчиках и различных физических средах (таблица 6.3). Битовый интервал обозначен как bt.

Комитет 802.3 старался максимально упростить выполнение расчетов, поэтому данные, приведенные в таблице, включают сразу несколько этапов прохождения сигнала. Например, задержки, вносимые повторителем, состоят из задержки входного трансивера, задержки блока повторения и задержки выходного трансивера. Тем не менее в таблице все эти задержки представлены одной величиной, названной базой сегмента.
Чтобы не нужно было два раза складывать задержки, вносимые кабелем, в таблице даются удвоенные величины задержек для каждого типа кабеля.
В таблице используются также такие понятия, как левый сегмент, правый сегмент и промежуточный сегмент. Поясним эти термины на примере сети, приведенной на рисунке 6.1.
Левым сегментом называется сегмент, в котором начинается путь сигнала от выхода передатчика конечного узла. На рисунке 6.1 это сегмент 1. Затем сигнал проходит через промежуточные сегменты 2-5 и доходит до приемника наиболее удаленного узла наиболее удаленного сегмента 6, который называется правым. Именно здесь в худшем случае происходит столкновение кадров и возникает коллизия.

С каждым сегментом связана постоянная задержка, названная базой, которая зависит только от типа сегмента и от положения сегмента на пути сигнала (левый, промежуточный или правый). База правого сегмента, в котором возникает коллизия, намного превышает базу левого и промежуточных сегментов.
Кроме этого, с каждым сегментом связана задержка распространения сигнала вдоль кабеля сегмента, которая зависит от длины сегмента и вычисляется путем умножения времени

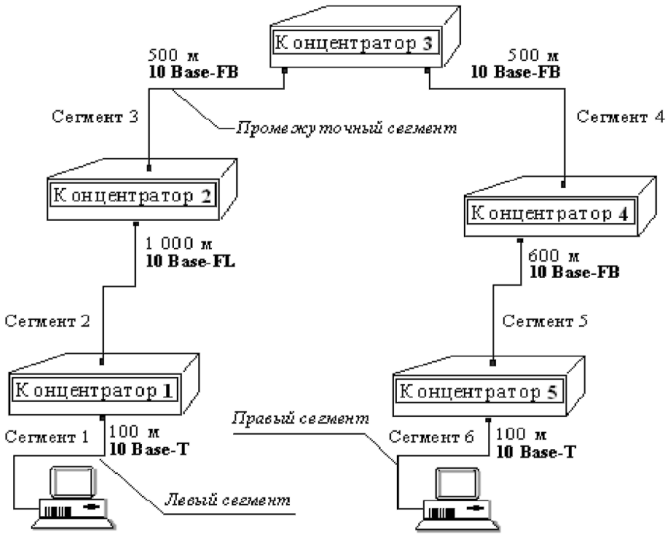


Рисунок 6.1 - Пример сети Ethernet, состоящей из сегментов различных физических стандартов

распространения сигнала по одному метру кабеля (в битовых интервалах) на длину кабеля в метрах.
Расчет PDV заключается в вычислении задержек, вносимых каждым отрезком кабеля (приведенная в таблице задержка сигнала на 1 м кабеля умножается на длину сегмента), а затем суммировании этих задержек с базами левого, промежуточных и правого сегментов. Общее значение PDV не должно превышать 575.
Так как левый и правый сегменты имеют разные величины базовой задержки, то в случае различных типов сегментов на удаленных краях сети необходимо выполнить расчеты дважды: один раз принять в качестве левого сегмента сегмент одного типа, а во второй - сегмент другого типа. Результатом можно считать максимальное значение PDV.
Чтобы признать конфигурацию сети корректной, нужно рассчитать также уменьшение межкадрового интервала повторителями, то есть величину PVV.
Для расчета PVV также можно воспользоваться значениями максимальных величин уменьшения межкадрового интервала при прохождении повторителей различных физических сред, рекомендованными IEEE и приведенными в таблице 1.4.

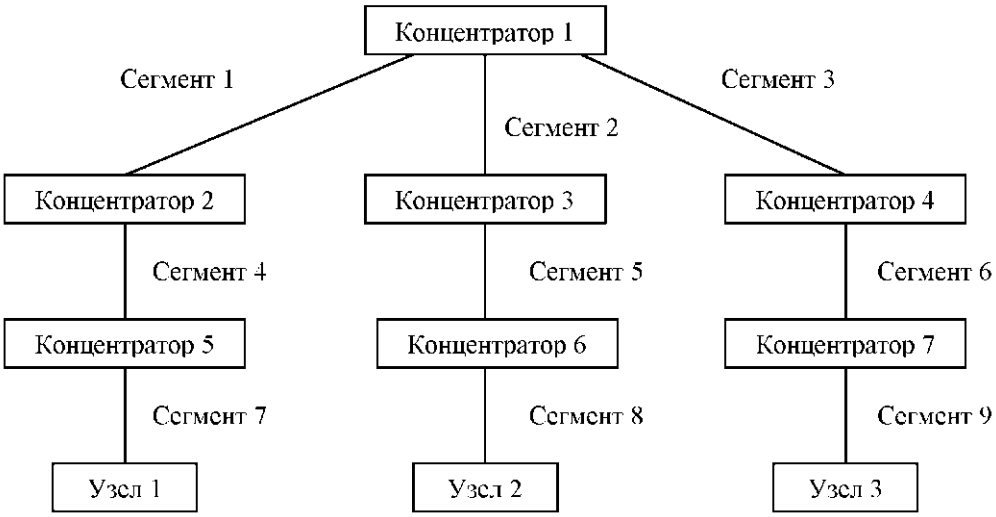
Пример расчета конфигурации сети
В примере крайние сегменты сети принадлежат к одному типу - стандарту 10Base-T, поэтому двойной расчет не требуется.
Приведенная на рисунке 6.1 сеть в соответствии с правилом «4 хабов» не является корректной - в сети между узлами сегментов 1 и 6 имеются 5 хабов, хотя не все сегменты являются сегментами 10Base-FB. Кроме того, общая длина сети равна 2800 м, что нарушает правило 2500 м. Рассчитаем значение PDV.
Левый сегмент 1:
15,3 (база) + 100-0,113 = 26,6
Промежуточный сегмент 2:
33,5 + 1000-0,1 = 133,5
Промежуточный сегмент 3:
24 + 500-0,1 = 74,0
Промежуточный сегмент 4:
24 + 500-0,1 = 74,0.
Промежуточный сегмент 5:
24 + 600-0,1 = 84,0
Правый сегмент 6:
165 + 100-0,113 = 176,3.
Сумма всех составляющих дает значение PDV, равное 568,4.
Так как значение PDV меньше максимально допустимой величины 575, то эта сеть проходит по критерию времени двойного оборота сигнала несмотря на то, что ее общая длина превышает 2500 м, а количество повторителей больше 4.
Рассчитаем значение PVV.
Левый сегмент 1 10Base-T: сокращение в 10,5 bt.
Промежуточный сегмент 2 10Base-FL: 8.
Промежуточный сегмент 3 10Base-FB: 2.
Промежуточный сегмент 4 10Base-FB: 2.
Промежуточный сегмент 5 10Base-FB: 2.
Сумма этих величин дает значение PVV, равное 24,5, что меньше предельного значения в 49 битовых интервала.
В результате сеть соответствует стандартам Ethernet по всем параметрам.

Задание
1. Ознакомиться с теоретическим материалом.
2. Произвести оценку конфигурации сети в соответствии с вариантом:

- по физическим ограничениям: на длину сегмента, на длину сети, правило «4 хаба» («5 хабов» для 10Base-FB);
- по времени двойного оборота сигнала в сети;
- по уменьшению межкадрового интервала.

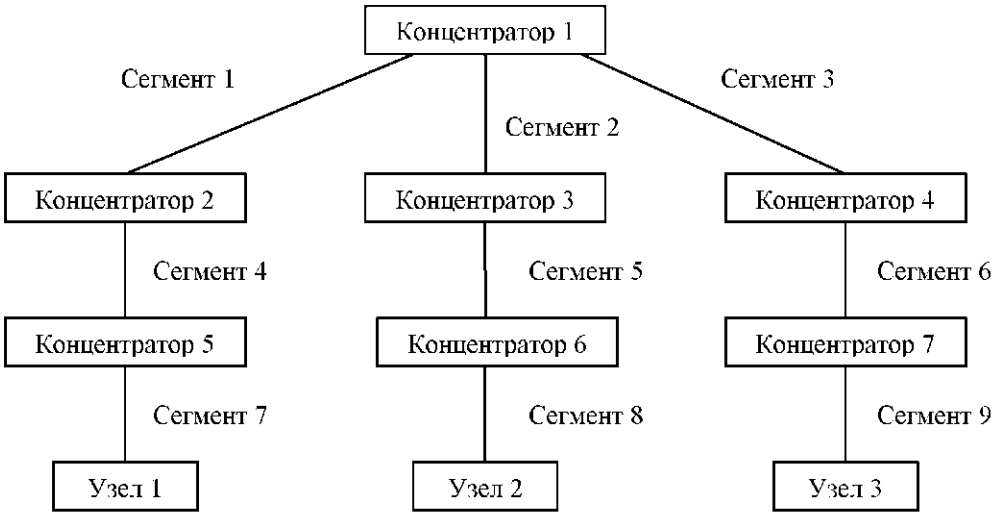
3. По результатам расчетов сделать вывод о корректности конфигурации сети Ethernet.
4. По результатам работы оформить отчет. Содержание отчета: исходные данные, расчеты указанных параметров, выводы.

Вариант 1



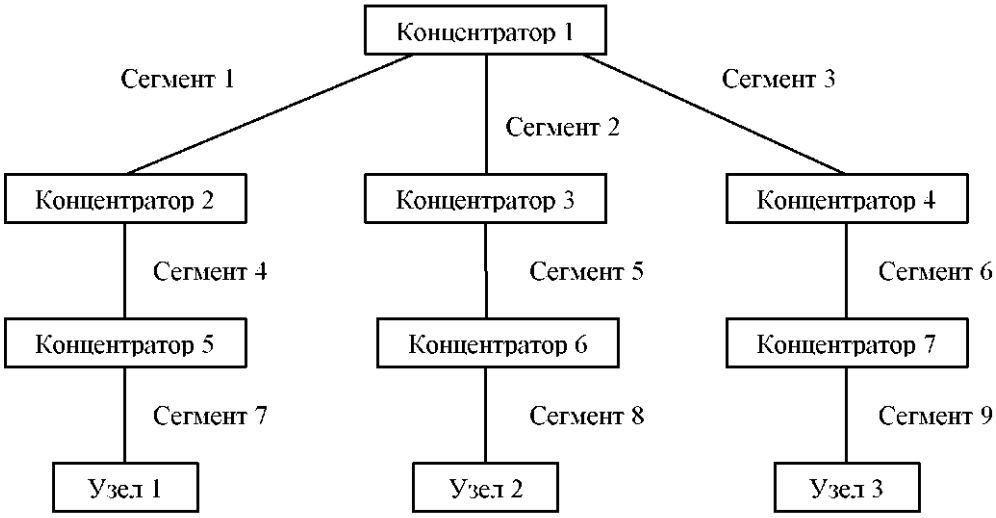
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			500
Сегмент 2	+			300
Сегмент 3	+			400
Сегмент 4		+		1000
Сегмент 5		+		300
Сегмент 6		+		400
Сегмент 7			+	100
Сегмент 8			+	50
Сегмент 9			+	100

Вариант 2



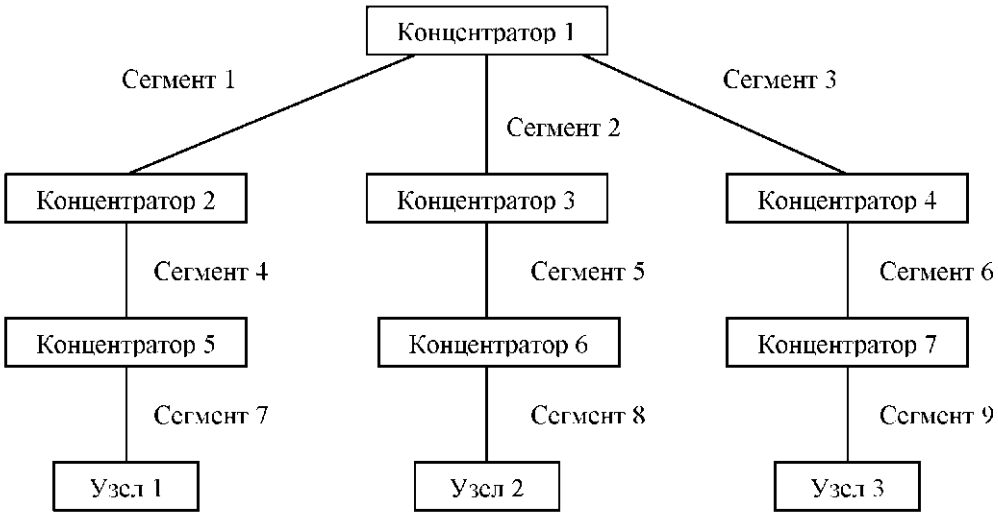
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		700
Сегмент 2	+			400
Сегмент 3	+			400
Сегмент 4		+		700
Сегмент 5		+		200
Сегмент 6	+			500
Сегмент 7			+	80
Сегмент 8			+	100
Сегмент 9			+	80

Вариант 3



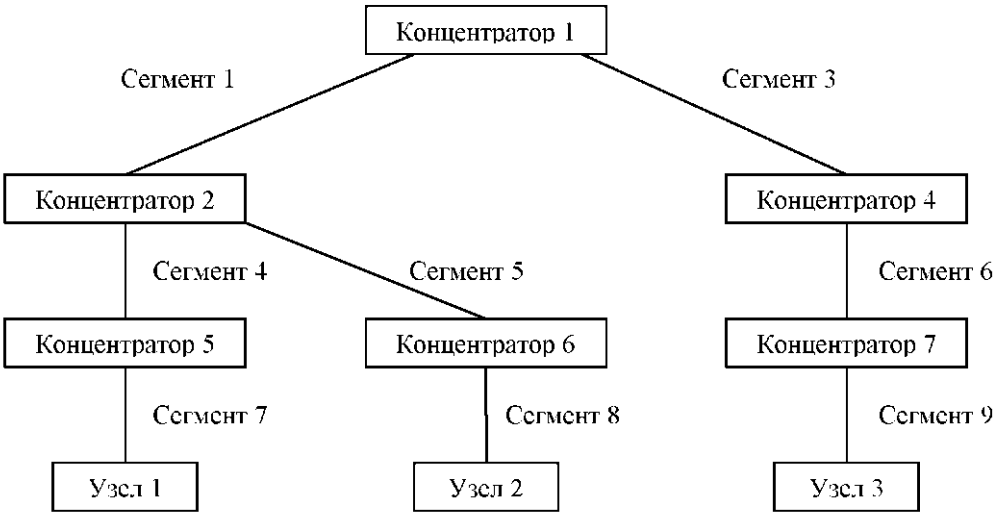
	10 Basc-FB	10 Basc-FL	10 Basc-T	Длина, м
Сегмент 1	+			1000
Сегмент 2		+		200
Сегмент 3		+		200
Сегмент 4		+		400
Сегмент 5	+			300
Сегмент 6		+		200
Сегмент 7			+	100
Сегмент 8			+	100
Сегмент 9			+	40

Вариант 4



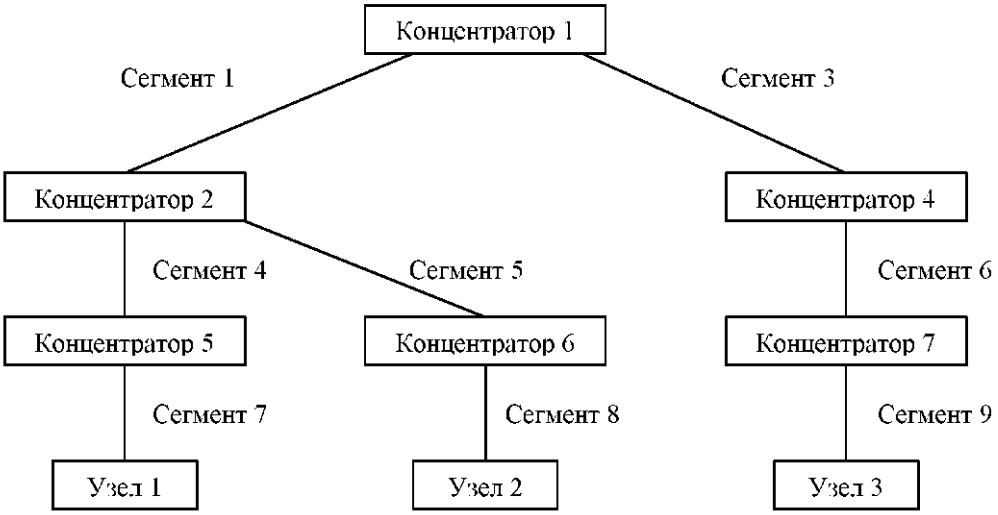
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		600
Сегмент 2		+		400
Сегмент 3		+		200
Сегмент 4	+			800
Сегмент 5	+			500
Сегмент 6	+			800
Сегмент 7			+	50
Сегмент 8			+	100
Сегмент 9			+	50

Вариант 5



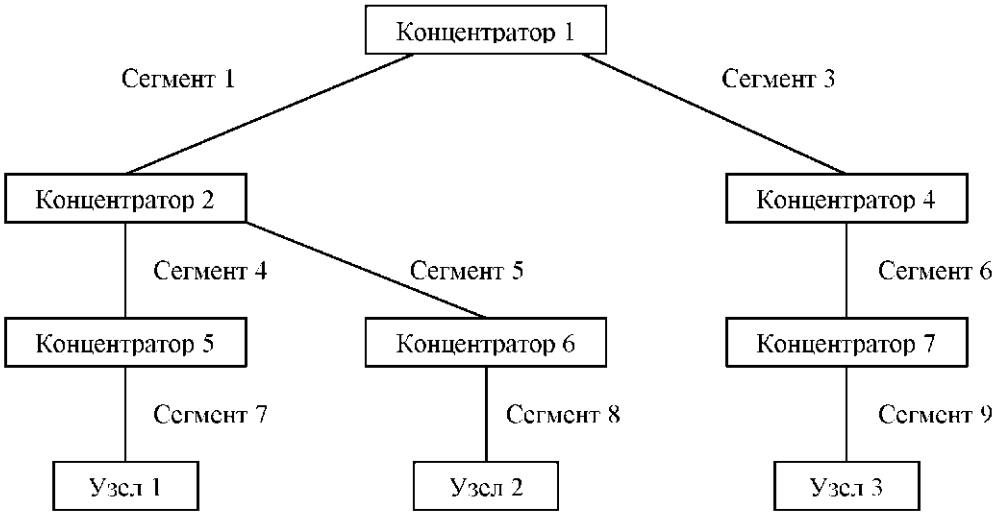
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			400
Сегмент 3	+			500
Сегмент 4		+		1100
Сегмент 5		+		1100
Сегмент 6		+		600
Сегмент 7			+	100
Сегмент 8			+	100
Сегмент 9			+	100

Вариант 6



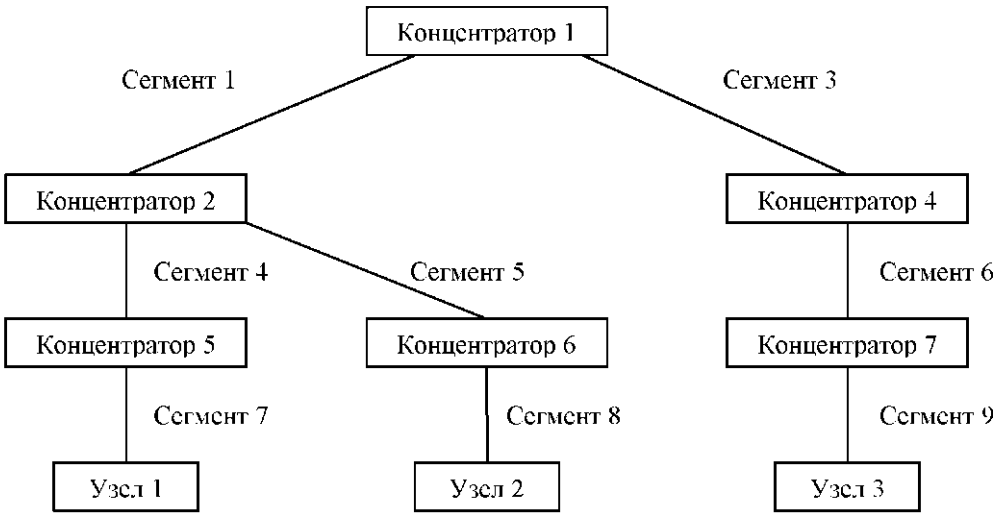
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			500
Сегмент 3		+		500
Сегмент 4	+			1000
Сегмент 5	+			1000
Сегмент 6		+		500
Сегмент 7			+	80
Сегмент 8			+	80
Сегмент 9			+	100

Вариант 7



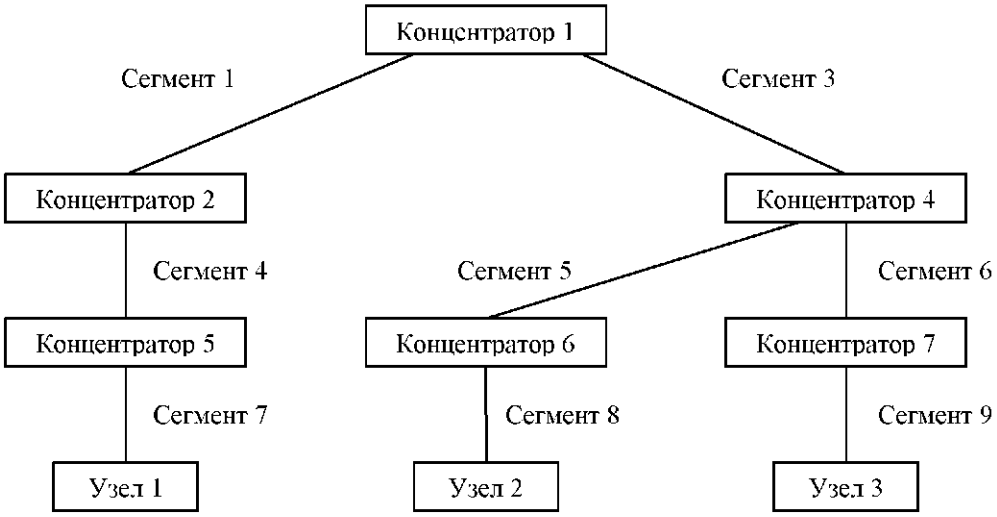
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		1000
Сегмент 3	+			1000
Сегмент 4		+		600
Сегмент 5		+		600
Сегмент 6	+			400
Сегмент 7			+	60
Сегмент 8			+	60
Сегмент 9			+	90

Вариант 8



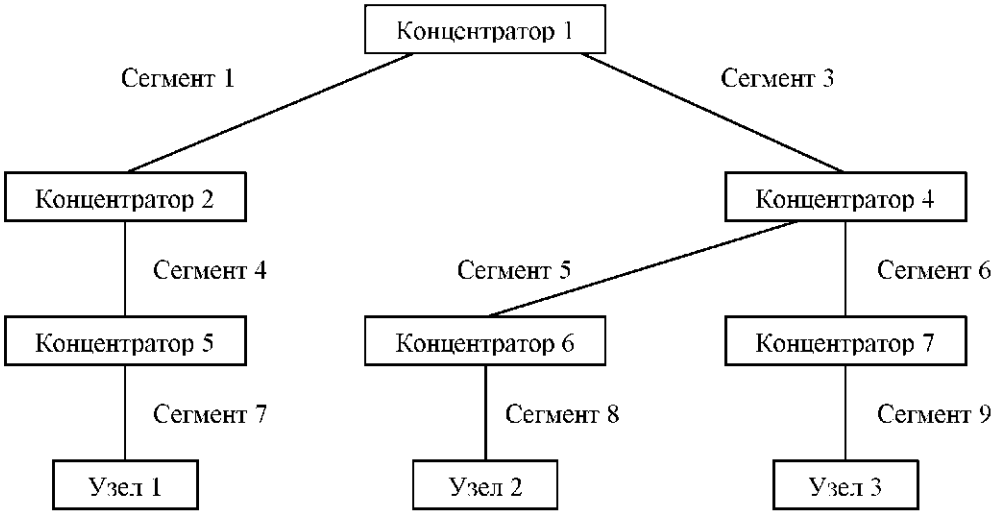
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		900
Сегмент 3		+		900
Сегмент 4	+			700
Сегмент 5	+			700
Сегмент 6	+			500
Сегмент 7			+	70
Сегмент 8			+	70
Сегмент 9			+	100

Вариант 9



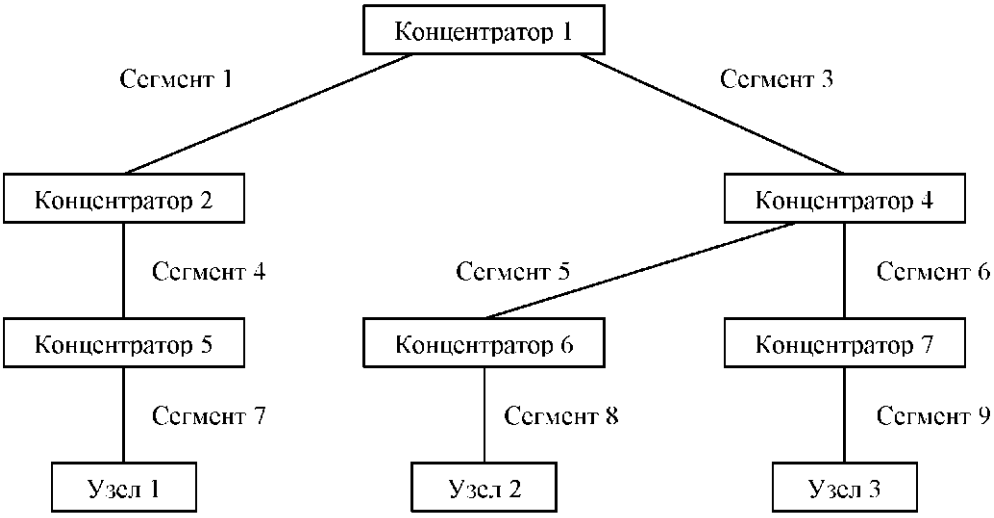
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			400
Сегмент 3	+			500
Сегмент 4		+		1100
Сегмент 5		+		1100
Сегмент 6		+		600
Сегмент 7			+	100
Сегмент 8			+	100
Сегмент 9			+	100

Вариант 10



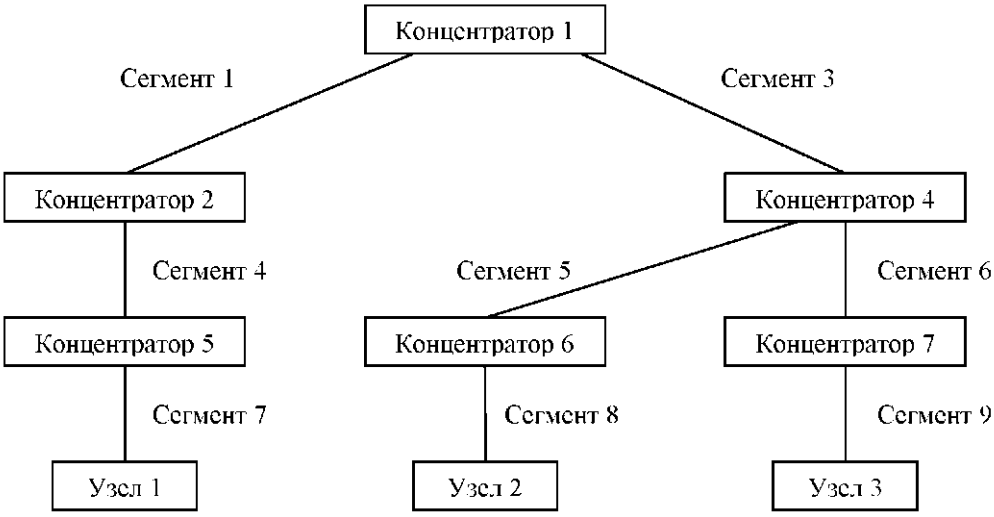
	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			500
Сегмент 3		+		500
Сегмент 4	+			1000
Сегмент 5	+			1000
Сегмент 6		+		500
Сегмент 7			+	80
Сегмент 8			+	80
Сегмент 9			+	100

Вариант 11



	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		1000
Сегмент 3	+			1000
Сегмент 4		+		600
Сегмент 5		+		600
Сегмент 6	+			400
Сегмент 7			+	60
Сегмент 8			+	60
Сегмент 9			+	90

Вариант 12



	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1		+		600
Сегмент 3		+		600
Сегмент 4	+			900
Сегмент 5	+			1000
Сегмент 6	+			500
Сегмент 7			+	70
Сегмент 8			+	80
Сегмент 9			+	90

Контрольные вопросы

1. Механизм доступа к разделяемой среде в технологии Ethernet.
2. Принципы оценки корректности конфигурации по физическим ограничениям.
3. Условия надежного распознавания коллизий.
4. Цели ограничения на уменьшение межкадрового интервала.
5. Правила расчета для самого длинного пути конфигурации сети.

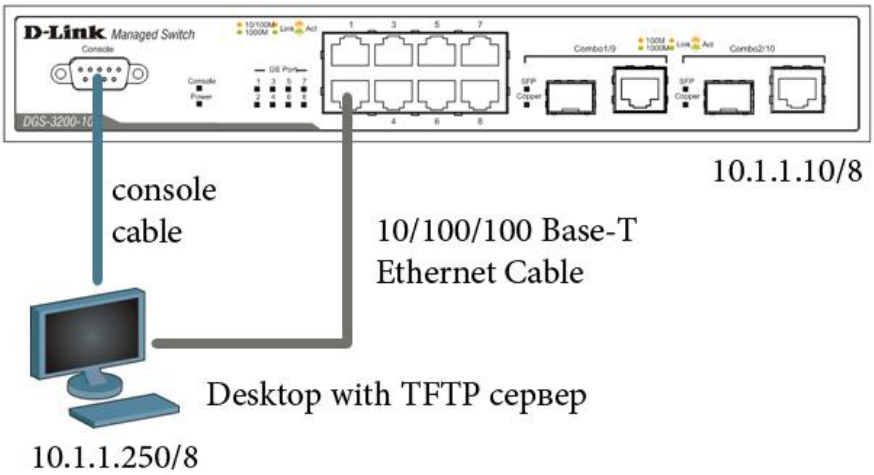
Практическое занятие №7.

Команды обновления микропрограммного

обеспечения коммутатора и сохранения/восстановления конфигурационных файлов.

Обновление микропрограммного обеспечения (или иногда называют «прошивки» коммутатора) и загрузчика может быть необходимо, когда доступна новая функциональность или требуется коррекция ошибок. Сохранять конфигурацию коммутатора необходимо при выполнении работ по изменению работы коммутатора, а также для упрощения восстановления работы коммутаторов в результате сбоя работы оборудования или поломки. Основным протоколом, применяемым для этих целей, служит TFTP (TrivialFileTransferProtocol, простейший протокол передачи данных). Для передачи/загрузки в сети необходимо наличие в сети TFTP-сервера. Коммутаторы D-Link, поддерживают технологию MultipleImageServices – возможность хранения на коммутаторе нескольких версий микропрограммного обеспечения и конфигурации, причем любая из них может быть настроена в качестве основной, т.е. используемой при загрузке коммутатора, что позволяет обеспечить отказоустойчивость оборудования при переходе на новое микропрограммное обеспечение или изменении конфигурации. Для изучения работы коммутатора, имеется возможность выгрузки через протокол TFTP log-файла оборудования.

Исходная схема:



Цель:

Изучить процесс обновления микропрограммного обеспечения и загрузчика.

Оборудование:

Коммутатор DGS-3200-10	1 шт.
Рабочая станция с TFTP сервером	1 шт.

Консольный кабель 1 шт.

Ethernet кабель 1 шт.

Подготовка к режиму обновления и сохранения микропрограммного обеспечения коммутатора.

Настройте TFTP-сервер (на примере Tftpd32 byPh.Jounin)

1. В настройках необходимо установить директорию приема файлов

2. Отключить все другие сервисы кроме TFTPserver

Подготовьте файл обновления

1. Поиск необходимого файла обновления «прошивки» на сайте http://www.dlink.ru (или http://www.dlink.com)

2. Выкачивание файла и перенос в директорию указанную в TFTP-сервере.

3. Прочитайте файл сопровождения к «прошивке».

Загрузка файла микропрограммного обеспечения в память коммутатора.

Все официальные версии прошивки включают примечания, которые описывают новые функции и последние коррекции ошибок.

Внимание: НЕ перезагружайте коммутатор во время загрузки записи микропрограммногообеспечения.

Выполнение команды без ключа image_id приводит к перезаписи текущей firmware!

НастройтеIP-адрес *configipifSystemipaddress 10.1.1.10/8*

Настройте TFTP-сервер

Выставить IP адрес рабочей станции 10.1.1.250/8

Запустить TFTP сервер; указать директорию с прошивкой CurrentDirectory.

Проверьте доступность TFTP-сервера *ping 10.1.1.250*

Проверьте текущее микропрограммное обеспечение *showfirmwareinformation*

Загрузите микропрограммное обеспечение на коммутатор

downloadfirmware_fromTFTP 10.1.1.250 DGS3200_Run_1_50_B038.had image_id 2

Убедитесь что программное обеспечение загружено *showfirmwareinformation*

Конфигурирование загрузки firmware коммутатора

Смените микропрограммное обеспечение, с которого будет загружаться коммутатор

config firmware image_id 2 boot_up

Сохраните изменения *save*

Перезагрузите коммутатор *reboot*

Обновленная прошивка вступит в силу

только после перезагрузки

Проверьте информацию прошивки *showfirmwareinformation*

Что вы наблюдаете

1.4. Управление изменениями конфигураций

Посмотрите текущую версию коммутатора (в RAM) *showconfigcurrent_config*

Посмотрите конфигурацию загрузки (из NVRAM) *showconfigconfig_in_nvram 1*

Выгрузите конфигурацию на TFTP-сервер *uploadcfg_toTFTP 10.1.1.250 config.txt*

Открыть выгруженный конфигурационный файл любым текстовым редактором, например блокнотом и просмотреть его структуру.

*Замените IP адрес 10.1.1.**10**/8 на 10.1.1.**8**/8*

 # IP

*configipif System ipaddress 10.1.1.**10**/8 vlan default state enable*

disableautoconfig

 # IP

*configipif System ipaddress 10.1.1.**8**/8 vlan default state enable*

disableautoconfig

сохраните файл.

Загрузите измененную конфигурацию *downloadcfg_fromTFTP 10.1.1.250 config.txt*

Проверьте, изменился ли IP-адрес коммутатора *showswitch*

Что вы наблюдаете

_____

_____

Чему будет равен IP адрес после перезагрузки коммутатора? _____

1.5. Выгрузка log-файлов

Просмотрите log коммутатора *showlog*

Выгрузите log-файл на TFTP-сервер *uploadlog_toTFTP 10.1.1.250 logfiles.txt*

Открыть выгруженный лог файл любым текстовым редактором, например блокнотом и просмотреть его структуру.

Практическое занятие №8:

Анализ трафика компьютерной сети с помощью снифферов

Цель занятия: приобретение практических знаний и навыков в перехвате и анализе трафика сегмента компьютерной сети.

Теоретические сведения:

Снифферы (дословный перевод - ‘вынюхиватели’) являются специализированным ПО, предназначенным для анализа потока сообщений (трафика) компьютерной сети передачи информации [4]. Известными системами подобного рода (но глобального уровня) являются ЭШЕЛОН (североамериканский проект, назначением которого является анализ содержимого линий связи Европы) и СОРМ (тотальное протоколирование трафика русскоязычной Сети). Большинство программ и сервисов (ICQ, TelNet, FTP, HTTP, POP3 и т.д.) пересылают пароль и логин пользователя открытым текстом (без всякой кодировки и шифровки), и работающий сниффер без труда позволит перехватывать такие сессии.

К простым ПО подобного класса относится, например комплект SpyNet (simik.lgg.ru/spynet312.exe); в штатную поставку Windows’NT Server и др. входит утилита Network Monitor (устанавливается добавлением сервиса Network Monitor Tools & Agent).

Обычно сетевая карта, работающая в сегменте некоммутируемой Ethernet в принципе ‘прослушивает’ весь трафик своего сегмента; однако в нормальном (без PROMISCUOUS MODE) режиме анализируются лишь первые 48 бит заголовка пакета и, если не найден собственный MAC-адрес, карта перестает читать ‘чужой’ пакет. Функциональность сниффера достигается переводом сетевой карты в режим PROMISCUOUS MODE, обеспечивающий перехват всех сообщений, циркулирующих в данном сегменте сети безотносительно MAC-адресов (достигается программной установкой соответствующего бита управляющего регистра карты). В случае коммутируемого Ethernet перевод карты в PROMISCUOUS MODE не позволяет прослушивать ‘чужие’ сообщения, в этом случае используется технология ‘ARP-спуфинга’ (путем соответствующей подделки ARP-сообщений данная сетевая карта ‘притворяется’ маршрутизатором с MAC-адресом, однако, данной карты), при этом трафик всех составляющих сегмента сети насильственно направится в сторону карты-обманщика.

Контрольные вопросы:

1. Что представляет из себя ПО класса снифферов и с какой целью применяется?
2. Каковы ограничения методов перехвата информации снифферами?
3. Каким образом сетевая плата конкретной ПЭВМ в локальной сети распознает назначение пакетов по принципу ‘свой-чужой’?
4. Какие методы применяют с целью исключения возможности перехвата сообщений снифферами?

Практическое занятие №9 Основные команды коммутаторов. Управление коммутаторами

Коммутаторы D-Link можно квалифицировать по возможностям управления.

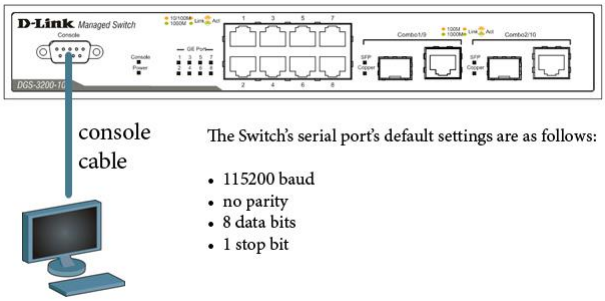
Существует три основных типа:

1. Неуправляемые коммутаторы – функции настройки и управления не поддерживают, имеют уже предустановленную функциональность. Данные коммутаторы применяются там, где характеристики необходимые в сети стандартные и не требуют дополнительных настроек. Обычно, это сети класса SOHO (SmallOfficeHomeOffice) малые предприятия и домашние сети.

2. Настраиваемые коммутаторы (Smart) – данные коммутаторы имеют ограниченные возможности управления, чаще всего через Web-консоль иногда через telnet. Применяются в сетях SOHO, бюджетных решениях ISP-сетей (InternetServiceProvider), в небольших корпоративных сетях. Отличаются небольшой стоимостью и легкостью настроек и интуитивно понятным интерфейсом.

3. Управляемые коммутаторы – коммутаторы, имеющие широкий набор функций управления и возможность получить максимально точные и необходимые настройки сети. Включающие в себя возможности управления через Web-интерфейс, через последовательный порт, с помощью сетевых консолей TELNET, SSH, протокола SNMP, имеют возможности удаленного мониторинга RMON. Область применения данных коммутаторов – ISP-сети, корпоративные сети средних и крупных предприятий и др. Интерфейс командной строки (Command-LineInterface, CLI) может быть использован для настройки и управления коммутаторами через последовательный порт и telnet.

<u>Исходная схема:</u>



<u>Цель:</u>

Ознакомится с основными командами настройки, контроля и устранения неполадок коммутаторов D-Link.

<u>Оборудование:</u>

Коммутатор DGS-3200-10 1 шт.

Рабочая станция	1 шт.
Консольный кабель	1 шт.

1.1. Вызов помощи по командам

Внимание! При написании команд в CLI важно учитывать регистр. Для того чтобы ознакомиться с правильностью написания команд, последовательностью выполнения операции можно обращаться к встроенной помощи по командам!

Напишите в консоли	*?*
Напишите в консоли	*dir*
Напишите в консоли	*config*
Напишите в консоли	*show*

1.2. Изменение IP-адреса коммутатора

Проверить параметры настройки IP-интерфейса *showipif*

Чему равен IP адрес по умолчанию (вписать) _____

Измените IP-адрес *configipifSystemipaddress10.1.1.10/8*

Настройте IP-адрес шлюза по умолчанию *createiproutedefault 10.1.1.254*

Замечание. IP-адрес шлюз по умолчанию назначается, если управление коммутатором осуществляется из других IP-подсетей.

Проверьте настройки *showswitch*

(IP адрес, Маска, Шлюз)

1.3. Управление учетными записями пользователей

Внимание! *Существует три основных уровня привелегий пользователей: Admin-максимальныеправа управления коммутатором, Operator – средние права управления (мониторинг сети,чтение системных параметров и конфигураций), User - минимальные права, в основном начтение.*

Заведите учетную запись администратора *createaccountadmindlink*

Укажите пароль и подтверждение пароля администратора: dlink

Enter a case-sensitive new password: dlink

Enter the new password again for confirmation: dlink

Для выхода из режима с текущими правами введите команду *logout*

Осуществить вход по новой созданной учетной записи администратора

Username: dlin

Password: dlink

DES-3526:4#

Заведите учетную запись пользователя *createaccountuserswuser*

Укажите пароль и подтверждение пароляпользователя: dlink1

Enter a case-sensitive new password: dlink1

Enter the new password again for confirmation: dlink1

Проверьте настройки учетных записей пользователей *showaccount*

Измените пароль пользователя *configaccountswuser*

После ввода команды укажите старый

пароль пользователя и 2 раза новый пароль.

*Enter a old password:****

*Enter a case-sensitive new password:****

*Enter the new password again for confirmation:****

Удалите учетную запись *deleteaccountswuser*

Проверьте удаление учетной записи пользователя *showaccount*

1.4. Настройка параметров идентификации коммутатора

Настройте имя коммутатора *configsnmpsystem_nameTEST*

Настройте месторасположение (локализацию) *configsnmpsystem_locationTEST_PRACTICE*

Настройте ответственный контакт *configsnmpsystem_contactLABORANT*

Проверьте внесенные параметры *showswitch*

Внимание: Длина параметров идентификации коммутаторов от 0 до 255 символов.

0 символов подразумевает, что информация отсутствует

1.5. Настройкапараметровбаннеровприветствия (Login banner (greeting message) and Command Prompt)

Для лучшей идентификации активного оборудования пользователями или создания уникальных логотипов оборудования возможно изменения баннера загрузки, который появляется в момент загрузки оборудования. Также возможно изменения указателя CommandPrompt в командной строке CLI.

Изменитеуказатель Command Prompt *configcommand_prompt TEST_SWITCH*

Установите указатель по умолчанию *configcommand_promptdefault*

Посмотрите текущий баннер приветствия *showgreeting_message*

Войдите в режим конфигурирования баннера *configgreeting_message*

Команды конфигурирования в остнастке

<FunctionKey> *<ControlKey>*

Ctrl+C *Quit without save* *left/right/*

Ctrl+W *Save and quit* *up/down* *Move cursor*

Ctrl+D *Delete line*

Ctrl+X *Erase all setting*

Ctrl+L *Reload original setting*

Добавьтестрочкувприветствие SWITCH_TEST tel +7(499) 000-00-00

Сохранитьивыйти*Ctrl+W*

Проверьтебаннер *show greeting_message*

==========

SWITCH_TEST tel +7(499)000-00-00

Command Line Interface

Copyright(C) 2008 D-Link Corporation. Allrightsreserved.

Восстановите настройки баннера по умолчанию *configgreeting_message default*

Проверьте баннер *show greeting_message*

1.6. Настройка времени на коммутаторе

Проверьте время *showtime*

Введите команду *configtime 16dec2010 15:45:30*

Дату и время выставить текущую

УстановитечасовойпоясМосква (GMT +3:00) *configtime_zone operator + hour 3 min 0*

Проверьте время *showtime*

Внимание! При перезагрузке коммутатора возможен сброс настроек текущего времени на коммутаторе, это обусловлено тем, что время храниться на некоторых моделях в RAM памяти коммутатора, т.о. в случае если в сети существуют серверы службы времени (NTP сервера) или открыт доступ к серверам времени расположенным в интернете, желательно настроить синхронизацию с этими серверами.

Включите работу протокола SNTP на коммутаторе *enablesntp*

Занесите список серверов SNTP и интервал обращений к серверам в сек.

configsntp primary 10.1.1.200 secondary 10.1.1.201 poll-interval 3600

Проверьте текущее время *showtime*

Проверьте descriptions портов *show ports description*

1.8. Функция FactoryReset (сброс к заводским установкам)

Сбросьте настройки по умолчанию командой:

resetconfig

Все заводские настройки по умолчанию восстановятся на коммутаторе, включая IP-адрес, учетные записи пользователей и журнал историй. Коммутатор не сохранит настройки и

не перегрузится.

resetsystem

Все заводские настройки по умолчанию восстановятся на коммутаторе в полном объеме. Коммутатор сохранит эти настройки в энергонезависимой памяти и перегрузится.

reset

Все заводские настройки по умолчанию восстановятся на коммутаторе исключая IP-адрес, учетные записи пользователей и журнал историй. Коммутатор не сохранит настройки и не перегрузится.

Сохраните изменения в энергонезависимую память	*save*
Перезагрузите коммутатор	*reboot*

Практическое занятие №10

Построение ЛВС. Структурированная кабельная система.

Цель: изучить назначение и способы организации СКС.

Оборудование: образцы кабелей, обжимной инструмент, инструкционные карты.

Теоретические сведения:

СКС – основа компьютерной локальной сети (ЛВС)

Для работы организации требуется локальная сеть, объединяющая компьютеры, телефоны, периферийное оборудование. Без компьютерной сети можно обойтись. Только неудобно обмениваться файлами при помощи дискет, выстраиваться в очередь возле принтера, а доступ в интернет реализовывать через один компьютер. Решением служит технология, обозначаемая сокращенно СКС.

Структурированная кабельная система это универсальная телекоммуникационная инфраструктура здания или комплекса зданий, обеспечивающая передачу сигналов всех типов, включая речевые, информационные, видео. СКС может быть установлена прежде, чем станут известны требования пользователей, скорость передачи данных, тип сетевых протоколов.

Рекомендуемые стандартами рамки СКС составляют 50 – 50 000 пользователей на площади до 1 000 000 м^2.

СКС создает основу компьютерной сети, интегрированной с телефонной сетью. Совокупность телекоммуникационного оборудования здания / комплекса зданий, соединенного с помощью структурированной кабельной системы, называют локальной сетью.

СКС или компьютерная плюс телефонная сеть

Структурированные кабельные системы обеспечивают длительный срок службы, сочетая удобство эксплуатации, качество передачи данных, надежность. Внедрение СКС создает основу повышения эффективности организации, снижения эксплуатационных расходов, улучшения взаимодействия внутри компании, обеспечения качества обслуживания клиентов.

Структурированная кабельная система строится таким образом, чтобы каждый интерфейс (точка подключения) обеспечивал доступ ко всем ресурсам сети. При этом на рабочем месте достаточно двух линий. Одна линия является компьютерной, вторая – телефонной. Линии взаимозаменяемы. Кабели соединяют телекоммуникационные разъемы рабочих мест с портами распределительных пунктов. Распределительные пункты объединяют магистральными линиями по топологии «иерархическая звезда».

СКС является интегрированной системой. Сравним СКС с устаревшей моделью "компьютерная плюс телефонная сеть". Ряд преимуществ является очевидным.

- интегрированная локальная сеть позволяет передавать разнотипные сигналы;

- СКС обеспечивает работу нескольких поколений компьютерных сетей;

- интерфейсы СКС позволяют подключать любое оборудование локальных сетей и речевых приложений;

- СКС реализует большой диапазон скорости передачи данных от 100 Кбит/сек речевых приложений до 10 Гбит/сек информационных приложений;

- администрирование СКС сокращает трудозатраты обслуживания локальной сети благодаря простоте эксплуатации;

- компьютерная сеть допускает одновременное использование разнотипных сетевых протоколов;

- стандартизация плюс конкуренция рынка СКС обеспечивают снижение цен комплектующих;

- локальная сеть позволяет реализовать свободу перемещения пользователей без изменения персональных данных (адресов, телефонных номеров, паролей, прав доступа, классов обслуживания);

- администрирование СКС обеспечивает прозрачность компьютерной и телефонной сети – все интерфейсы СКС промаркированы и документированы. Работа организация не зависит от сотрудника-монополиста соединений телефонной сети.

Надежная и долговечная структурированная кабельная система является фундаментом локальной сети. Однако всякое достоинство имеет обратную сторону. Стандарты СКС рекомендуют избыточность количественных параметров системы, что влечет существенные единовременные затраты. Зато можно забыть о кошмаре перманентного ремонта действующего офиса для наращивания компьютерной сети под текущие потребности.

Стандарты СКС

Стандарты определяют структуру СКС, рабочие параметры конструктивных элементов, принципы проектирования, правила монтажа, методику измерения, правила администрирования, требования телекоммуникационного заземления.

Администрирование СКС включает маркировку портов, кабелей, панелей, шкафов, других элементов, а также систему записей, дополняемую ссылками. Вместе с продуманной организацией кабелей, заложенной на этапе создания кабельной системы, система администрирования позволяет поддерживать хорошую организацию локальной сети. Стандарты СКС 2007 года считают наличие администрирования одним из условий соответствия смонтированной системы требованиям стандартов.

СКС определяются международными, европейскими и национальными стандартами. Стандарты СКС адресованы строителям-профессионалам. В России СКС чаще создают специализированные фирмы.

Россия является членом Международной организации стандартизации (ISO), поэтому руководствуется международными стандартами. Данная информация отражает требования международного стандарта ISO/IEC 11801.

Подсистемы СКС

Стандарт ISO/IEC 11801 подразделяет структурированную кабельную систему на три подсистемы:

- магистральную подсистему комплекса зданий;
- магистральную подсистему здания;
- горизонтальную подсистему.

Магистральная подсистема СКС и телефонная сеть

Магистральная подсистема комплекса зданий соединяет кабельные системы зданий.Магистральная подсистема здания соединяет распределительные пункты этажей.

Магистральная подсистема включает информационную и речевую подсистемы СКС. Основная среда передачи информационной подсистемы – оптоволокно (одномодовое или многомодовое), дополняемое симметричными четырехпарными кабелями. Если длина магистральной линии не превышает 90 метров, применяют симметричные кабели категории 5 и выше. При большей длине для информационных приложений, то есть компьютерной сети, требуется прокладывать оптоволоконный кабель.

Речевые приложения магистрали здания работают по многопарным кабелям. Речевые приложения, создающие телефонную сеть, относятся к низшим классам СКС. Это позволяет увеличивать длину линий магистральной подсистемы, создаваемых многопарными кабелями, до двух-трех километров.

Горизонтальная подсистема СКС и компьютерная сеть

Горизонтальная подсистема СКС включает распределительные панели, коммутационные кабели распределительных пунктов этажа, горизонтальные кабели, точки консолидации, телекоммуникационные разъемы. Горизонтальная подсистема обеспечивает локальную сеть для абонентов, предоставляет доступ к магистральным ресурсам. Среда передачи горизонтальной подсистемы – симметричные кабели не ниже категории 5. Стандарты СКС 2007 года предусматривают для центров обработки данных выбор СКС не ниже категории 6. Для информационных технологий (компьютерная плюс телефонная сеть) частных домов новые стандарты рекомендуют использовать категорию 6 / 7. Среда передачи вещательных коммуникационных технологий (сокращенно ВКТ: телевидение, радио) частных домов / квартир – симметричные защищенные кабели с полосой частот 1 ГГц, плюс коаксиальные кабели до 3 ГГц. Допускается также применение оптоволокна.

В горизонтальной подсистеме СКС преобладает компьютерная сеть. Отсюда вытекает ограничение максимальной длины канала – 100 метров независимо от типа среды. Чтобы продлить срок службы без модификаций, горизонтальная подсистема СКС должна обеспечить избыточность, резерв параметров.

Рабочая область в структуре горизонтальной подсистемы СКС

Рабочая область СКС – помещения (часть помещений), где пользователи работают с терминальным (телекоммуникационным, информационным, речевым) оборудованием.

Рабочая область не относится к горизонтальной подсистеме СКС. Функциональным элементом горизонтальной подсистемы является телекоммуникационный разъем – ТР.

Рабочие места оснащаются розетками, включающими два или более телекоммуникационных разъема. Подключение оборудования рабочей области выполняют абонентскими кабелями. Абонентские / сетевые кабели находятся за рамками СКС, однако они позволяют создавать каналы, параметры которых определяются стандартами СКС. К СКС относят коммутационные кабели / перемычки, используемые для соединений между портами панелей / контактами кроссов.

Более 90% кабелей СКС приходится на горизонтальную подсистему. Кабели горизонтальной подсистемы максимально интегрированы в инфраструктуру здания. Любые изменения в горизонтальной подсистеме влияют на работу организации. Поэтому так важна избыточность горизонтальной подсистемы, обеспечивающая беспроблемную длительную эксплуатацию локальной сети.

Существует два метода прокладки кабелей — скрытый и открытый. Для скрытой прокладки используют конструкцию стен, полов, потолков. Однако, это не всегда возможно. Наиболее распространенный вариант кабель каналов – пластиковые короба.

Варианты открытой прокладки кабельных жгутов включают лотки, короба, миниколонны. Скрытая прокладка кабелей предусматривает установку встроенных розеток, монтаж напольных лючков.

Распределительные пункты СКС – узлы локальной сети

Распределительные пункты СКС представляют собой окончания горизонтальных и магистральных линий, которые для удобства использования фиксируют на панелях или кроссах. Для установки панелей, кроссов, сетевого оборудования служат напольные / настенные шкафы, телекоммуникационные стойки. Распределительный пункт может занимать часть шкафа, несколько шкафов. Помещения распределительных пунктов называют телекоммуникационными помещениями, дословно – телекоммуникационными чуланами (Telecommunicationclosets). На каждом этаже здания рекомендуется устанавливать один РП этажа. Если офисная площадь этажа превышает 1000 квадратных метров, предусматривают дополнительный РП, соединяемый магистральными каналами.

Распределительные пункты СКС создают узлы локальной сети где компактно размещается сетевое и серверное оборудование.

Напольные шкафы позволяют размещать окончания сотен линий, оборудование, блоки УАТС. Телекоммуникационные стойки обеспечивают вместимость шкафов, но имеют меньшую стоимость. Их используют когда не требуется дополнительной защиты оборудования локальной сети или особых условий эксплуатации. Настенные шкафы рекомендуется выбирать при небольшом числе линий, отсутствии телекоммуникационного помещения. Оборудование шкафов охлаждают вентиляторами.

Удобство эксплуатации локальной сети зависит от качества организации, наличия маркировки СКС. Стандартная цветовая маркировка позволяет различать назначение портов панелей. Цвет говорит о принадлежности порта к магистральной подсистеме комплекса, магистральной подсистеме здания, горизонтальной подсистеме, подсистемам, не относящимся к СКС.

Цветом выделяют интерфейсы внешних подсистем, обозначают порты компьютерных и телефонных сетей. На фото линии магистральной информационной, горизонтальной, а также сигнальной подсистем маркированы согласно требованиям стандарта TIA/EIA-606-A. Первая

цифра маркировки обозначает номер панели, вторая — номер порта панели. При этом соответствие номера портов розеток и панелей такое же, как номера соединяющих их кабелей.

Система телекоммуникационного заземления

Телекоммуникационное заземление должно быть установлено во всех СКС независимо от наличия экранированных линий. Такое требование определено стандартом J-STD-607-A 2002 года «Совместный стандарт. Требования по заземлению телекоммуникационных систем коммерческих зданий».

Основное назначение заземления – безопасность персонала, защита магистралей, а также оборудования от воздействия грозовых разрядов, обеспечение балансировки приемо-передатчиков локальной сети. Внутренние шины заземления телекоммуникационного оборудования (мультиплексоры, оптоэлектронные устройства), УАТС должны подключаться к системетелекоммуникационного заземления.

Телекоммуникационные шины заземления (ТШЗ) устанавливают в каждом распределительном пункте возле шкафов / стоек. Шины распределительных пунктов соединяют магистралями заземления с главной телекоммуникационной шиной заземления (ГТШЗ), устанавливаемой рядом с электрическим терминалом заземления. Современные стандарты рекомендуют увеличивать площадь сечения проводника магистрали заземления при увеличении длины магистрали. Максимальное рекомендуемое сечение может составлять 3/0 AWG или 90 кв.мм. Ответвления магистрали выполняются изотермической сваркой или неразъемным соединением.

Часто приходится сталкиваться с отсутствием или ненадлежащим исполнением систем заземления в старых постройках. Проектирование системы телекоммуникационного заземления не требует устранения недостатков электрического заземления. Когда эквипотенциальность заземления не обеспечена, реализуется принцип «эффективного экранирования».

Система электропитания

В большинстве случаев для работы компьютерной сети требуется обеспечить электропитание устройств, подключаемых к телекоммуникационным разъемам. На каждом рабочем месте устанавливают силовые розетки. Одни розетки служат для подключения компьютеров и оргтехники, другие – бытовых электроприборов. Такое разделение систем позволяет организовать централизованное гарантированное электропитание.

Известно, что прокладка силовых кабелей параллельно информационным ухудшает качество передачи данных по слаботочным линиям, что может вызвать сбои локальных сетей. Для уменьшения этого влияния требуется выдержать минимально допустимые расстояния параллельной прокладки, зависящие от напряжения, мощности нагрузки. Монтаж силовых и слаботочных сетей одним подрядчиком позволяет решить проблему электромагнитной совместимости, уменьшить инвестиционные затраты.

Варианты установки розеток

Силовые и телекоммуникационные розетки могут быть установлены в коробах, накладных розетках, стенах, телекоммуникационных колоннах, напольных лючках.

На фотографиях изображены варианты размещения телекоммуникационных разъемов (TP) с блоками силовых розеток. Самый распространенный вариант создания кабель каналов – пластиковые короба. Для фиксации коробов используют стены, офисную мебель, даже потолки. Короба высотой более 80 мм удобны для размещения розеток. Узкие короба дополняют настеннымиподрозетниками.

Группы розеток могут быть отмечены маркировкой или цветом вставок. Например, красные вставки для питания компьютерной сети, белые – подключение бытовых электроприборов.

Телекоммуникационные колонны, напольные стойки, напольные лючки применяются реже. Причина — более высокая стоимость таких решений.

Самый дешевый вариант — встроенные розетки. Он также является наиболее эстетичным. Реализация такого способа монтажа розеток оптимальна при строительстве или ремонте офиса. Альтернативный недорогой вариант — установка настенных подрозетников, прокладка мини-коробов.

Тестирование и гарантии

Мнение о том, что тестирование СКС — это формальная процедура, весьма распространено. Многие заказчики считают, что измерение параметров линий это гарантийная процедура. Это верно, но только наполовину. Во-первых, тестирование позволяет обнаружить скрытые дефекты, которые могут быть незамеченными. Во-вторых, это единственная возможность избежать проблем работы приложений компьютерной сети.

Вопреки распространенному мнению о полном соответствии стандартов СКС требованиям сетевых протоколов это заблуждение. Параметры среды передачи ниже требований приложений. Стандарты СКС классов D (100 МГц), E (250 МГц) и F (600 МГц) предусматривают нулевое – отрицательно отношение затухания / суммарных наводок на верхней границе частотного диапазона. Для рабочих пар приложений класса D, реализуемых в компьютерных сетях, отношение сигнал / шум во всем диапазоне частот должно быть не менее 10-19 дБ, то есть на один – два порядка лучше, чем предусматривают стандарты СКС. Более того, некоторые приложения класса D работают в полосе частот более 100 МГц, определяемых категорией 5е. Диапазон частот 1000BASE-T GigabitEthernet составляет 125 МГц, ATM 155 – 155 МГц.

Таким образом, СКС может соответствовать стандартам, но не обеспечивать работу ряда приложений локальной сети по параметру коэффициента битовых ошибок (BER – BitErrorRate). При этом уменьшается скорость передачи данных вплоть до "зависаний" компьютерной сети.Качество передачи сигналов по каналам СКС обеспечивается благодаря резерву параметров. Чтобы проверить, достаточен ли резерв, проводится тестирование соответствия сетевым протоколам. Например, при использовании кабельного анализатора Fluke (пример отчета), подтверждается соответствие базовой линии / канала одиннадцати сетевым протоколам. Это означает возможность использования также любых приложений низших классов.

Контрольные вопросы:

1.Оборудование СКС.

2. Подсистемы СКС.

3. стандарты СКС.

Практическое занятие №12

Алгоритм покрывающего дерева: сущность алгоритма, его применение.

Команды управления протоколами связующего дерева STP, RSTP, MSTP

Протокол STP (Spanning Tree Protocol). Методы обеспечения отказоустойчивости сети

Метод STP разработан в 1983 году, но до сих пор остается актуальным. В основе действия протокола лежат алгоритмы, применяемые в дискретной математике (теория графов, и поиск связного графа без циклов, называемого деревом). Это позволяет иметь в сетях коммутаторов второго уровня древовидные структуры, не содержащие петель. Петля предполагает наличие нескольких маршрутов передачи данных в инфраструктуре коммутируемых сетей. Наличие дополнительных маршрутов может быть вызвано обеспечением отказоустойчивости в сети, либо неправильно построенной сетью, ошибкой администратора сети, и являться так называемой неконтролируемой петлей. Данные петли могут создавать трудности в работе сети: широковещательный шторм, множественные копии кадров, невозможность передачи полезной нагрузки через коммутатор и как следствие недоступность коммутатора. Широковещательный шторм (broadcast storm) – лавина (всплеск) широковещательных (служебных) пакетов. Размножение некорректно сформированных широковещательных сообщений в каждом узле приводит к экспоненциальному росту их числа и парализует работу сети. Обычно такие пакеты используются сетевыми сервисами стации для оповещения других станций о своем присутствии. Считается нормальным, если широковещательные пакеты составляют около 10% от общего числа пакетов в сети. При наличии широковещательных пакетов больше 20%, приводит практически к полной остановке работы сети, т.к. полезный трафик не может продвигаться по сети. Возникновение и рост широковещательных пакетов при петлях в сети обусловлен тем, что в технологии Ethernet не предусмотрено методов уничтожения зацикленных кадров средствами самого протокола (как например, в протоколах сетевого уровня, и наличия поля TTL). Это приводит к тому, что кадр в петле будет передаваться до тех пор, пока не произойдет широковещательный шторм (рис. 1.1).

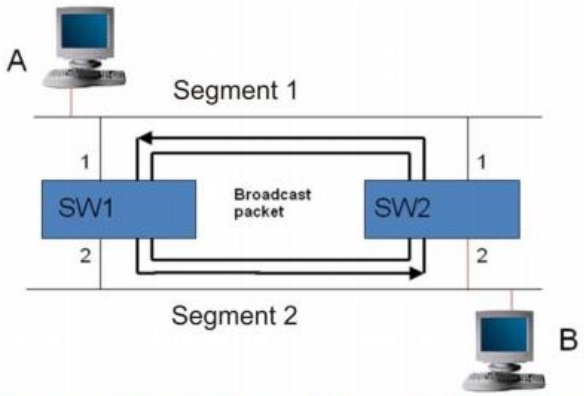


Рис. 1.1. Возникновение широковещательного шторма

Для решения данных проблем был разработан протокол Spanning Tree Protocol использующий Spanning Tree Algorithm (STA). Коммутаторы, поддерживающие протокол STP автоматически создают древовидную конфигурацию связей без петель в компьютерной сети. Данная конфигурация строится автоматически с помощью обмена служебными пакетами. В результате работы протокола происходит устранение петель с сохранением избыточных связей.

Коммутаторы D-Link поддерживают следующие версии протокола STP:

- IEEE 802.1d, Spanning Tree Protocol (STP);
- IEEE 802.1w, Rapid Spanning Tree Protocol (RSTP);
- IEEE 802.1s, Multiple Spanning Tree Protocol (MSTP).

IEEE 802.1d. Spanning Tree Protocol (STP)

Обмен информацией между коммутаторами

Для работы протокола STP при обмене информацией между коммутаторами используются служебные пакеты BPDU (Bridge Protocol Data Units)

Существует 2 типа пакетов BPDU:

1. Configuration BPDU – используется для конфигурирования и установки односвязной коммутируемой инфраструктуры;

2. Topology Change Notification (TCN) BPDU – позволяет отслеживать и анонсировать изменения сетевой топологии.

Преимущества RSTP

RSTP по стандарту содержит большинство разработанных усовершенствований для связующего дерева STP. В правильно настроенной сети RSTP может достигать гораздо более быстрого схождения, иногда на это требуется не более 2-3 секунд. По умолчанию коммутаторы D-Link работают по протоколу RSTP.

В данной практической части рассмотрим работу протоколов STP и настройку конфигурации коммутаторов для обеспечения связующего дерева.

<u>Цель:</u>

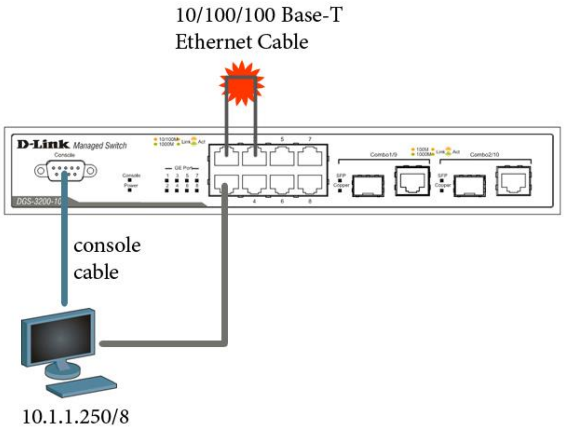
Понять функциональность протокола связующего дерева, а также узнать, как протокол STP настраивается на коммутаторах D-Link.

<u>Оборудование:</u>

Коммутатор DGS-3200-10	2 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Ethernet кабель	2 шт.

ЗАДАНИЕ 1

Исходная схема:



Примечание: Не соединяйте петлю Ethernet проводом во время конфигурирования коммутатора.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским командой *reset config*

Просмотр пакетов передаваемых через порт *show packet ports 1*

Соедините кабелем Ethernet порты 1 и 3 коммутатора

Что вы наблюдаете? Почему нет широковещательного шторма?

_____

_____

_____

Выполните на рабочей станции команду *ping yandex.ru*

Что вы наблюдаете? Объясните почему

_____

_____

_____

Посмотреть загрузку CPU *show utilization cpu*

Просмотреть загрузку порта *show utilization ports*

Отсоедините кабель, удалите петлю.

Оставить порты 1,3,5,9 в управляющем VLANe default, а порты 2,4,6,8 поместить в новый VLAN

config vlan default delete 2,4,6,8

create vlan v2 tag 2

config vlan v2 add untagged 2,4,6,8

Проверьте настройки VLAN

show vlan

Просмотр пакетов передаваемых через порт *show packet ports 1*

Соедините кабелем порты 1 и 3, рабочую станцию подключить к порту 2

Что вы наблюдаете? Почему нет широковещательного шторма?

_____

Практическое занятие №13 Организация обмена данными с использованием протокола TCP/UDP.

Практическое занятие №14 Адресация в IP- сетях. Подсети и маски.

Цель занятия: Научится определять IP-адрес рабочей станции, маску сети и определить к какому классу сети принадлежит адрес.

Оборудование: справочный материал.

Ход занятия:

• Каждый компьютер в сети (или на сетевом жаргоне **хост** (host) - узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую) имеет уникальный двоичный 4-х байтовый адрес, идентифицирующий его в Интернет.

Например, **10111110101001110010001000000010**. Для наглядности каждый байт (или октет) адреса выделен особым цветом. Во избежание ошибок принято после каждого октета адреса, кроме последнего, ставить точку. Тогда адрес запишется как

10111110.10100111.00100010.00000010 или 190.167.34.2, если перевести каждый октет в десятичную систему счисления.

Таким образом, адрес компьютера записывается в формате A.B.C.D, где 0<=A<=255, 0<=B<=255, 0<=C<=255, 0<=D<=255. Этот адрес называют **IP-адресом**.

Протокол TCP/IP является открытым, с его официальным описанием (RFC-791, RFC-793) может познакомится в Интернет любой желающий. Неудивительно, что существуют программные реализации этого протокола практически для любой операционной системы. Например, Microsoft TCP/IP для Windows, Berkly TCP/IP для Unix линии BSD и т.д. И, хотя этот протокол не стандартизован ни одним государством мира, он стал фактически международным стандартом Интернет.

Как происходит передача данных

1. IP-адрес в двоичном представлении разбивается на 2 части - адрес сети (левая часть адреса) и адрес хоста (правая часть адреса).
Например, в адресе 190.167.34.2 первые 24 бита могут быть адресом сети, а последние 8 - адресом хоста. Тогда наш адрес будет выглядеть как **10111110101001110010001000000010**, где зеленым цветом выделена сетевая часть адреса (она одинакова для всех хостов локальной сети), а красным - часть адреса, адресующая хост внутри локальной сети. Для того, чтобы быстро вычислять по IP-адресу адрес сети или хоста, используется понятие **маски подсети** (subnet mask). Это двоичное число, в котором все биты адреса сетевой части адреса равны 1, а все остальные биты равны нулю.

В нашем случае для адреса

10111110101001110010001000000010
получим маску подсети

11111111111111111111111100000000.
Маску подсети принято записывать в том же десятичном формате, что и IP-адрес. Для этого нужно каждый байт маски перевести в десятичное число и записать полученные десятичные числа через точки.

В нашем случае

$\mathbf{11111111}_2$=255
$\mathbf{11111111}_2$=255
$\mathbf{11111111}_2$=255
$\mathbf{00000000}_2$=0
Ответ:
255.255.255.0 - маска подсети.

Маску подсети в настоящее время все чаще называют ***маской сети***, что точней отображает ее смысл.

2. Информационные пакеты пересылаются напрямую от компьютера-отправителя к компьютеру-получателю только в пределах одной сети. Если компьютер-получатель находится в другой сети, то информация пересылается специальному компьютеру сети, который называется **шлюзом** (gateway). Его адрес всегда известен. Об этом заботится системный администратор. Компьютер-шлюз имеет связь с как минимум с одной другой сетью и ретранслирует информацию в нужном направлении. Этот процесс называется **маршрутизацией** (routing).

Если ваш компьютер, имеющий IP адрес 192.169.204.12 и маску подсети 255.255.192.0 должен отправить информацию компьютеру с адресом 192.169.198.15, то прежде всего ваш компьютер проверит, находится ли получатель информации в той же сети.
Для этого двоичное представление адреса получателя он побитово умножит на двоичное представление маски подсети, то в результате получится адрес сети:

11000000101010001100011000001100 (адрес компьютера - получателя)

*
11111111111111111100000000000000 (текущая маска подсети)

11000000101010001100000000000000 (адрес сети получателя)

Аналогичную процедуру компьютер проделает со своим адресом для того, чтобы узнать адрес своей собственной сети:

11000000101010011100110000001100 (адрес компьютера - отправителя)

*
11111111111111111100000000000000 (текущая маска подсети)

11000000101010011100000000000000 (адрес своей собственной сети)

Адрес сети получателя совпадает с адресом собственной сети. Следовательно, получатель находится в локальной сети, и информация может быть послана напрямую. Если бы совпадения не произошло, то информация была бы отправлена шлюзу (с адресом, например,192.168.192.2) с указанием адреса получателя 192.169.204.15, а он переслал бы ее в другую сеть. Этот процесс продолжался бы до тех пор, пока информация не дошла бы до получателя.

Задание:

1. Выясните, каков будет порядок отправки информации по адресам 192.168.193.31 и 192.167.192.3 для хоста с адресом 192.167.12.3 и маской подсети 255.255.0.0. Решение задачи запишите в отчет.
2. При помощи любой известной вам поисковой системы определите число документов Интернет, в которых цитируется описание протокола IP. Попробуйте найти собственно описание протокола.
Указание. Этот документ называется RFC-791 (Request For Comments-791).
3. Запишите двоичный IP-адрес **11111110101111110110001000000111** в стандартном формате.

Практическое занятие №15

Команды VLAN на основе портов и меток 802.1q

Виртуальная локальная сеть (Virtual Local Area Netwrok, VLAN) представляет собой коммутируемый сегмент сети, который логически отделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического

расположения пользователей. Виртуальные локальные сети имеют все свойства физических локальных сетей, но вы можете группировать рабочие станции, даже если они физически расположены не в одном сегменте. Любой порт коммутатора может принадлежать к VLAN, и одноадресный, широковещательный и групповой трафик передается только рабочим станциям принадлежащим данной VLAN. Каждый VLAN рассматривается как логическая сеть, т.е. пакеты, предназначенные станциям, которые не принадлежат данной VLAN должны передаваться через маршрутизатор или мост. Таким образом, с помощью виртуальных сетей решается проблема ограничений при передаче широковещательных пакетов и вызываемых ими следствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Сети, построенные с применением VLAN, обладают следующими преимуществами:

- Гибкость внедрения. VLAN является эффективным способом группировки сетевых устройств (рабочие станции, сервера, сетевые принтеры, МФУ) в виртуальные рабочие группы, несмотря на их размещение в сети;

- VLAN обеспечивает возможность контроля широковещательных сообщений, что увеличивает полосу пропускания доступную для пользователя;

- VLAN позволяет усилить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе политику взаимодействия пользователей из разных виртуальных сетей (в простейшем случае сетевые устройства из одного VLAN в другой VLAN не имеют доступа на канальном уровне, что позволяет бороться с различными типами сетевых атак, например ARP-spoofing).

Существует несколько способов (типов) организации VLAN:

- VLAN на базе портов (Port-based) – каждый порт коммутатора назначается в определенную VLAN и любое сетевое устройство подключенное в данный порт, будет находиться в назначенной виртуальной сети;
- VLAN на основе MAC-адресов (MAC-based) – членство в VLAN’е основывается на MAC-адресе рабочей станции. В этом случае на коммутаторе необходимо создать привязку MAC-адресов всех устройств к VLAN;
- VLAN на основе протокола (Protocol-based) – данные 3-4 уровня в заголовке пакета используются чтобы определить членство в VLAN’е;
- VLAN на основе меток (IEEE 802.1q) – поле о принадлежности к VLAN, интегрируется в структуру кадра, что позволяет передавать данную информацию по сети. Преимуществом является гибкость настройки, использование не только на одном коммутаторе, но и в пределах всей коммутируемой сети, возможность использовать оборудование разных

производителей при организации сети. Данный тип организации VLAN используется чаще остальных методов.

Существуют два подхода назначения порта в определѐнный VLAN:

- Статическое назначение – когда принадлежность порта VLAN задаѐтся администратором в процессе настройки;
- Динамическое назначение – когда принадлежность порта VLAN определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как 802.1x. При использовании 802.1x для того чтобы получить доступ к порту коммутатора, пользователь проходит аутентификацию на RADIUS-сервере. По результатам аутентификации порт коммутатора размещается в тот или иной VLAN.

Введем основные определения IEEE 802.1q:

- Tag (Тег) – дополнительное поле данных 4 байта, содержащее информацию о VLAN (vlan id/12bit, поле приоритета/3bit, поле обозначения типа сети/1bit), добавляется в кадр;
- Tagging (Вставка тега в кадр) – процесс добавления информации (тега) о принадлежности к VLAN в заголовок кадра;
- Untagging (Удаление тега из кадра) – процесс извлечения информации IEEE 802.1q из заголовка кадра;
- Ingress port (Входной порт) – порт коммутатора, на который поступают кадры, и принимается решение о принадлежности к VLAN;
- Egress port (Выходной порт) – порт коммутатора, с которого кадры передаются на другие сетевые устройства (коммутаторы, рабочие станции) и на нем соответственно принимается решение о маркировке кадра.

Любой порт коммутатора может быть настроен как «tagged» или «untagged». Функция «untagged» позволяет работать с такими сетевыми устройствами VLAN, которые не понимают меток в заголовках кадров Ethernet. Функция «tagged» позволяет настраивать VLAN между несколькими коммутаторами, передавать информацию о нескольких VLAN через данные порты коммутаторов, подключать сетевые устройства, понимающие IEEE 802.1q (например, сервера с сетевыми интерфейсами с поддержкой 802.1q), обеспечивать возможность создания сложных сетевых инфраструктур.

В данной работе мы рассмотрим примеры использования VLAN и

конфигурирование коммутаторов с применением VLAN.

<u>Цель:</u>

Понять технологию VLAN и способы настройки коммутаторов D-Link.

<u>Оборудование:</u>

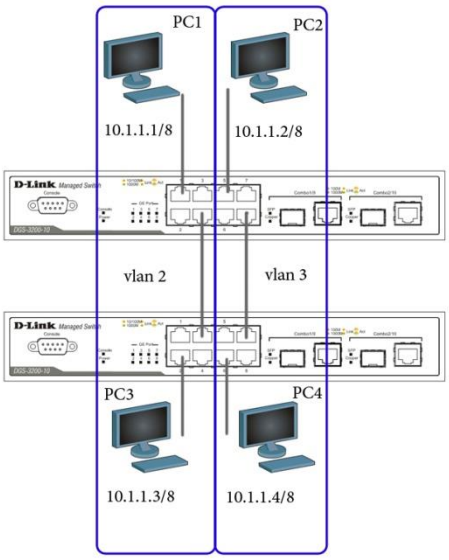
Коммутатор DGS-3200-10	2 шт.
Рабочая станция	4 шт.

Консольный кабель 1 шт.

Ethernet кабель 6 шт.

Настройка VLAN, основанной на портах.

<u>Исходная схема:</u>



Удалите порты из VLAN по умолчанию для использования в других VLAN

config vlan default delete 1-10

Создайте VLAN v2 и v3, назначьте нетэгированные порты соответствующим VLAN

create vlan v2 tag 2

config vlan v2 add untagged 1-4

create vlan v3 tag 3

config vlan v3 add untagged 5-8

Проверьте настройки VLAN

show vlan

Повторите процедуру настройки для второго коммутатора

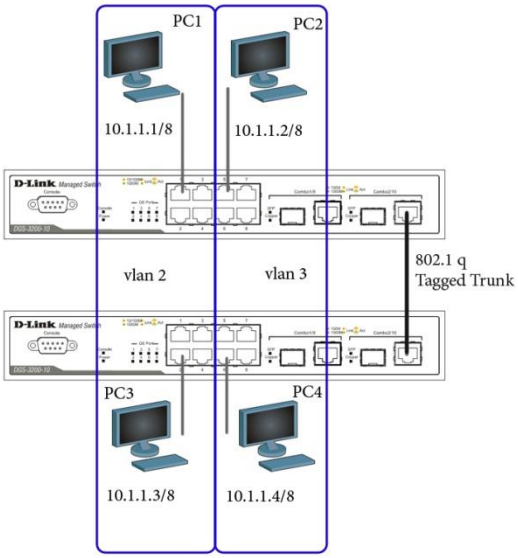
Проверьте доступность узлов командой ping

- от PC1 к PC3 _____
- от PC2 к PC4 _____

- от PC1 к PC2 & PC4 _____
- от PC2 к PC1 & PC3 _____

Настройка VLAN на основе меток 802.1q

<u>Исходная схема:</u>



Перед выполнением данной процедуры необходимо сбросить настройки коммутатора к заводским командой *reset config*

Удалите порты из VLAN по умолчанию для использования в других VLAN

config vlan default delete 1-10

Создайте VLAN v2 и v3, назначьте нетэгированные порты соответствующим VLAN

create vlan v2 tag 2

config vlan v2 add untagged 1-4

config vlan v2 add tagged 10

create vlan v3 tag 3

config vlan v3 add untagged 5-8

config vlan v3 add tagged 10

Проверьте настройки VLAN

show vlan

Повторите процедуру настройки для второго коммутатора

Проверьте доступность узлов командой ping

- от PC1 к PC3 _____
- от PC2 к PC4 _____
- от PC1 к PC2 & PC4 _____
- от PC2 к PC1 & PC3 _____

Оптимизация конфигурирования коммутаторов с большим количеством VLAN

Перед выполнением данной процедуры необходимо сбросить настройки коммутатора к заводским командой *reset config*

Удалите порты из VLAN по умолчанию для использования в других VLAN

config vlan default delete 1-10

Создайте двадцать VLAN с тегами с 2 по 21 *create vlan vlanid 2-21*

Примечание: При создании VLAN имена присваиваются по шаблону (VLAN x , где x – тег создаваемого VLAN)

Добавьте теггированные порты в несколько VLAN, включите функции объявления

config vlan vlanid 2-21 add tagged 1-10 advertisement enable

Проверьте настройки VLAN *show vlan*

Измените имя VLAN и добавьте untagged порты:

config vlan vlanid 11 name SALE add untagged 1-8

Удалите порты из нескольких VLAN

config vlan vlanid 2-21 delete 1-7

Проверьте настройки VLAN *show vlan*

Удалите несколько VLAN *delete vlan vlanid 2-21*

Проверьте корректность выполнения команды *show vlan*

Практическое занятие №16

Команды VLAN на основе портов и меток 802.1q

Виртуальная локальная сеть (Virtual Local Area Netwrok, VLAN) представляет собой коммутируемый сегмент сети, который логически отделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического

расположения пользователей. Виртуальные локальные сети имеют все свойства физических локальных сетей, но вы можете группировать рабочие станции, даже если они физически расположены не в одном сегменте. Любой порт коммутатора может принадлежать к VLAN, и одноадресный, широковещательный и групповой трафик передается только рабочим станциям принадлежащим данной VLAN. Каждый VLAN рассматривается как логическая сеть, т.е. пакеты, предназначенные станциям, которые не принадлежат данной VLAN должны передаваться через маршрутизатор или мост. Таким образом, с помощью виртуальных сетей решается проблема ограничений при передаче широковещательных пакетов и вызываемых ими следствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Сети, построенные с применением VLAN, обладают следующими преимуществами:

- Гибкость внедрения. VLAN является эффективным способом группировки сетевых устройств (рабочие станции, сервера, сетевые принтеры, МФУ) в виртуальные рабочие группы, несмотря на их размещение в сети;

- VLAN обеспечивает возможность контроля широковещательных сообщений, что увеличивает полосу пропускания доступную для пользователя;

- VLAN позволяет усилить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе политику взаимодействия пользователей из разных виртуальных сетей (в простейшем случае сетевые устройства из одного VLAN в другой VLAN не имеют доступа на канальном уровне, что позволяет бороться с различными типами сетевых атак, например ARP-spoofing).

Существует несколько способов (типов) организации VLAN:

- VLAN на базе портов (Port-based) – каждый порт коммутатора назначается в определенную VLAN и любое сетевое устройство подключенное в данный порт, будет находиться в назначенной виртуальной сети;
- VLAN на основе MAC-адресов (MAC-based) – членство в VLAN'е основывается на MAC-адресе рабочей станции. В этом случае на коммутаторе необходимо создать привязку MAC-адресов всех устройств к VLAN;
- VLAN на основе протокола (Protocol-based) – данные 3-4 уровня в заголовке пакета используются чтобы определить членство в VLAN'е;
- VLAN на основе меток (IEEE 802.1q) – поле о принадлежности к VLAN, интегрируется в структуру кадра, что позволяет передавать данную информацию по сети. Преимуществом является гибкость настройки, использование не только на одном коммутаторе, но и в пределах всей коммутируемой сети, возможность использовать оборудование разных производителей при организации сети. Данный тип организации VLAN используется чаще остальных методов.

Существуют два подхода назначения порта в определѐнный VLAN:

- Статическое назначение – когда принадлежность порта VLAN задаѐтся администратором в процессе настройки;
- Динамическое назначение – когда принадлежность порта VLAN определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как 802.1x. При использовании 802.1x для того чтобы получить доступ к порту коммутатора, пользователь проходит аутентификацию на RADIUS-сервере. По результатам аутентификации порт коммутатора размещается в тот или иной VLAN.

Введем основные определения IEEE 802.1q:

- Tag (Тег) – дополнительное поле данных 4 байта, содержащее информацию о VLAN (vlan id/12bit, поле приоритета/3bit, поле обозначения типа сети/1bit), добавляется в кадр;
- Tagging (Вставка тега в кадр) – процесс добавления информации (тега) о принадлежности к VLAN в заголовок кадра;
- Untagging (Удаление тега из кадра) – процесс извлечения информации IEEE 802.1q из заголовка кадра;
- Ingress port (Входной порт) – порт коммутатора, на который поступают кадры, и принимается решение о принадлежности к VLAN;
- Egress port (Выходной порт) – порт коммутатора, с которого кадры передаются на другие сетевые устройства (коммутаторы, рабочие станции) и на нем соответственно принимается решение о маркировке кадра.

Любой порт коммутатора может быть настроен как «tagged» или «untagged». Функция «untagged» позволяет работать с такими сетевыми устройствами VLAN, которые не понимают меток в заголовках кадров Ethernet. Функция «tagged» позволяет настраивать VLAN между несколькими коммутаторами, передавать информацию о нескольких VLAN через данные порты коммутаторов, подключать сетевые устройства, понимающие IEEE 802.1q (например, сервера с сетевыми интерфейсами с поддержкой 802.1q), обеспечивать возможность создания сложных сетевых инфраструктур.

В данной лабораторной работе мы рассмотрим примеры использования VLAN и конфигурирование коммутаторов с применением VLAN.

<u>Цель:</u>

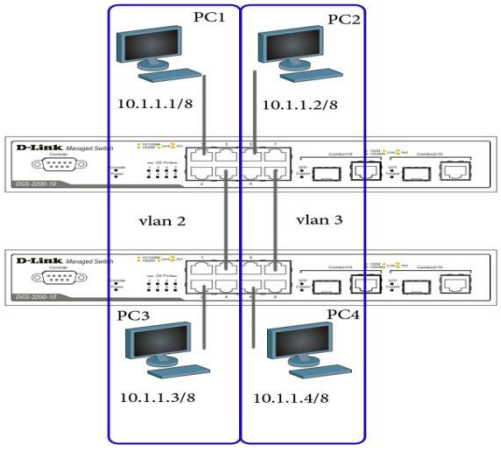
Понять технологию VLAN и способы настройки коммутаторов D-Link.

<u>Оборудование:</u>

Коммутатор DGS-3200-10	2 шт.
Рабочая станция	4 шт.
Консольный кабель	1 шт.
Ethernet кабель	6 шт.

Настройка VLAN, основанной на портах.

Исходная схема:



Удалите порты из VLAN по умолчанию для использования в других VLAN

config vlan default delete 1-10

Создайте VLAN v2 и v3, назначьте нетэгированные порты соответствующим VLAN

create vlan v2 tag 2

config vlan v2 add untagged 1-4

create vlan v3 tag 3

config vlan v3 add untagged 5-8

Проверьте настройки VLAN

show vlan

Повторите процедуру настройки для второго коммутатора

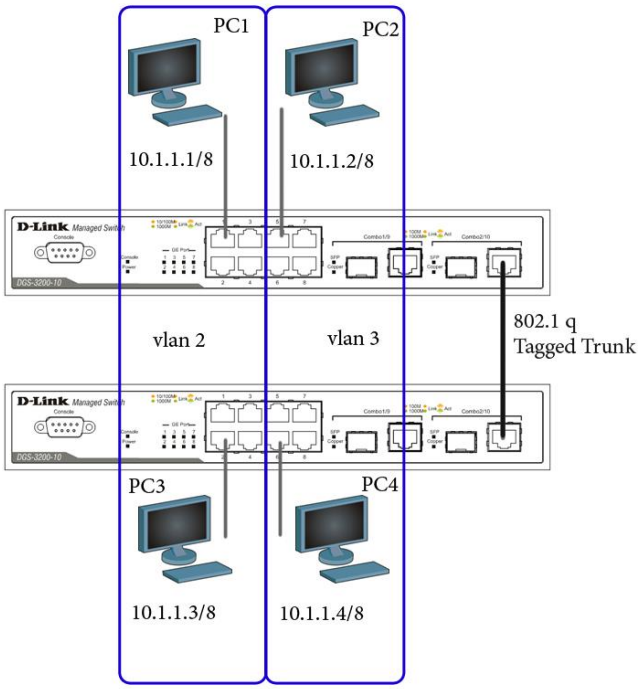
Проверьте доступность узлов командой ping

- от PC1 к PC3 _____
- от PC2 к PC4 _____

- от PC1 к PC2 & PC4 _____
- от PC2 к PC1 & PC3 _____

Настройка VLAN на основе меток 802.1q

<u>Исходная схема:</u>



Перед выполнением данной процедуры необходимо сбросить настройки коммутатора к заводским командой *reset config*

Удалите порты из VLAN по умолчанию для использования в других VLAN

config vlan default delete 1-10

Создайте VLAN v2 и v3, назначьте нетэгированные порты соответствующим VLAN

create vlan v2 tag 2

config vlan v2 add untagged 1-4

config vlan v2 add tagged 10

create vlan v3 tag 3

config vlan v3 add untagged 5-8

config vlan v3 add tagged 10

Проверьте настройки VLAN

show vlan

Повторите процедуру настройки для второго коммутатора

Проверьте доступность узлов командой ping

- от PC1 к PC3 _____
- от PC2 к PC4 _____
- от PC1 к PC2 & PC4 _____
- от PC2 к PC1 & PC3 _____

Оптимизация конфигурирования коммутаторов с большим количеством VLAN

Перед выполнением данной процедуры необходимо сбросить настройки коммутатора к заводским командой *reset config*

Удалите порты из VLAN по умолчанию для использования в других VLAN

config vlan default delete 1-10

Создайте двадцать VLAN с тегами с 2 по 21 *create vlan vlanid 2-21*

Примечание: При создании VLAN имена присваиваются по шаблону (VLAN x , где x – тег создаваемого VLAN)

Добавьте теггированные порты в несколько VLAN, включите функции объявления

config vlan vlanid 2-21 add tagged 1-10 advertisement enable

Проверьте настройки VLAN *show vlan*

Запишите ваши наблюдения:

_____

Измените имя VLAN и добавьте untagged порты:

config vlan vlanid 11 name SALE add untagged 1-8

Удалите порты из нескольких VLAN

config vlan vlanid 2-21 delete 1-7

Проверьте настройки VLAN *show vlan*

Запишите ваши наблюдения:

Удалите несколько VLAN *delete vlan vlanid 2-21*

Проверьте корректность выполнения команды *show vlan*

Практическое занятие №18

Изучение принципа работы маршрутизаторов.

Цель занятия: изучить виды маршрутизаторов, их классификацию.

Оборудование: инструкционные карты, справочный материал.

Ход выполнения работы:

1. Изучить виды маршрутизаторов:

1.1 Многопротокольные маршрутизаторы концептуально напоминают мосты с той существенной разницей, что они работают на сетевом уровне. Как и любой маршрутизатор, они берут пакет с одной линии и передают его на другую, но при этом линии принадлежат к разным сетям и используют разные протоколы (например, IP и IPX). Кроме того, сетевые устройства типа моста/маршрутизатора (brouter или bridge/router) работают в нормальном режиме как многопротокольные маршрутизаторы, а при получении пакета с неизвестным сетевым протоколом обрабатывают его как мост. Другие устройства со сходным названием "маршрутизирующий мост" (routing bridge) принадлежат к устройствам второго уровня и упоминаются здесь лишь из-за причастия routing. Они работают как мосты, но при этом поддерживают некоторые функции третьего уровня для оптимизации передачи данных.

1.2 Маршрутизаторы с интеграцией услуг гарантируют приоритетному трафику, в частности трафику реального времени, своевременную доставку. Они поддерживают протокол RSVP для резервирования таких ресурсов, как пропускная способность и буферы в очереди.

1.3 Коммутаторы третьего уровня, по сути, также являются маршрутизаторами, причем пакетные коммутаторы (Packet-by-Packet Switch) - на самом деле обычные, только быстрые маршрутизаторы.

2. Изучить типы маршрутизаторов:

2.1 Внутренний маршрутизатор (internal router) — маршрутизатор все интерфейсы, которого принадлежат одной зоне. У таких маршрутизаторов только одна база данных состояния каналов.

2.2 Пограничный маршрутизатор (area border router, ABR) — соединяет одну или больше зон с магистральной зоной и выполняет функции шлюза для межзонального трафика. У пограничного маршрутизатора всегда хотя бы один интерфейс принадлежит магистральной зоне. Для каждой присоединенной зоны маршрутизатор поддерживает отдельную базу данных состояния каналов.

2.3 Магистральный маршрутизатор (backbone router) — маршрутизатор, у которого всегда хотя бы один интерфейс принадлежит магистральной зоне. Внутренний маршрутизатор интерфейсы, которого принадлежат нулевой зоне, также является магистральным.

2.4 Пограничный маршрутизатор автономной системы (AS boundary router, ASBR) — обменивается информацией с маршрутизаторами принадлежащими другим автономным системам. Пограничный маршрутизатор автономной системы может находиться в любом месте автономной системы и быть внутренним, пограничным или магистральным маршрутизатором.

3. Классификация маршрутизаторов по областям применения

По областям применения маршрутизаторы делятся на несколько классов.

3.1 *Магистральные маршрутизаторы (backbone routers)* предназначены для построения центральной сети корпорации. Центральная сеть может состоять из большого количества локальных сетей, разбросанных по разным зданиям и использующих самые разнообразные сетевые технологии, типы компьютеров и операционных систем. Магистральные маршрутизаторы - это наиболее мощные устройства, способные обрабатывать несколько

сотен тысяч или даже несколько миллионов пакетов в секунду, имеющие большое количество интерфейсов локальных и глобальных сетей. Поддерживаются не только среднескоростные интерфейсы глобальных сетей, такие как T1/E1, но и высокоскоростные, например, ATM или SDH со скоростями 155 Мбит/с или 622 Мбит/с. Чаще всего магистральный маршрутизатор конструктивно выполнен по модульной схеме на основе шасси с большим количеством слотов - до 12-14. Большое внимание уделяется в магистральных моделях надежности и отказоустойчивости маршрутизатора, которая достигается за счет системы терморегуляции, избыточных источников питания, заменяемых «на ходу» (hot swap) модулей, а также симметричного муль-типроцессирования. Примерами магистральных маршрутизаторов могут служить маршрутизаторы Backbone Concentrator Node (BCN) компании Nortel Networks (ранее Bay Networks), Cisco 7500, Cisco 12000.

3.2 *Маршрутизаторы региональных отделений* соединяют региональные отделения между собой и с центральной сетью. Сеть регионального отделения, так же как и центральная сеть, может состоять из нескольких локальных сетей. Такой маршрутизатор обычно представляет собой некоторую упрощенную версию магистрального маршрутизатора. Если он выполнен на основе шасси, то количество слотов его шасси меньше: 4-5. Возможен также конструктив с фиксированным количеством портов. Поддерживаемые интерфейсы локальных и глобальных сетей менее скоростные. Примерами маршрутизаторов региональных отделений могут служить маршрутизаторы BLN, ASN компании Nortel Networks, Cisco 3600, Cisco 2500, NetBuilder II компании 3Com. Это наиболее обширный класс выпускаемых маршрутизаторов, характеристики которых могут приближаться к характеристикам магистральных маршрутизаторов, а могут и опускаться до характеристик маршрутизаторов удаленных офисов.

3.3 *Маршрутизаторы удаленных офисов* соединяют, как правило, единственную локальную сеть удаленного офиса с центральной сетью или сетью регионального отделения по глобальной связи. В максимальном варианте такие маршрутизаторы могут поддерживать и два интерфейса локальных сетей. Как правило, интерфейс локальной сети - это Ethernet 10 Мбит/с, а интерфейс глобальной сети - выделенная линия со скоростью 64 Кбит/с, 1,544 или 2 Мбит/с. Маршрутизатор удаленного офиса может поддерживать работу по коммутируемой телефонной линии в качестве резервной связи для выделенного канала. Существует очень большое количество типов маршрутизаторов удаленных офисов. Это объясняется как массовостью потенциальных потребителей, так и специализацией такого типа устройств, проявляющейся в поддержке одного конкретного типа глобальной связи. Например, существуют маршрутизаторы, работающие только по сети ISDN, существуют модели только для аналоговых выделенных линий и т. п. Типичными представителями этого класса являются маршрутизаторы Nautika компании Nortel Networks, Cisco 1600, Office Connect компании 3Com, семейство Pipeline компании Ascend.

3.4 *Маршрутизаторы локальных сетей (коммутаторы 3-го уровня)* предназначены для разделения крупных локальных сетей на подсети. Основное требование, предъявляемое к ним, - высокая скорость маршрутизации, так как в такой конфигурации отсутствуют низкоскоростные порты, такие как модемные порты 33,6 Кбит/с или цифровые порты 64 Кбит/с. Все порты имеют скорость по крайней мере 10 Мбит/с, а многие работают на скорости 100 Мбит/с. Примерами коммутаторов 3-го уровня служат коммутаторы CoreBuilder 3500 компании 3Com, Accelar 1200 компании Nortel Networks, Waveswitch 9000 компании Plaintree, Turboiron Switching Router компании Foudry Networks.

Контрольные вопросы:

1. Маршрутизатор – понятие, классы.
2. Назначение магистрального маршрутизатора.
3. Перечислить виды маршрутизаторов и дать характеристику каждому.

Практическое занятие №19

Объединение локальных сетей с помощью маршрутизаторов

Цель занятия: изучить принцип работы маршрутизатора на сетевом уровне

Маршрутизаторы объединяют сегменты LAN на сетевом уровне. *Маршрутизация* включает в себя два этапа: определение оптимальных маршрутов и передача пакетов по этим маршрутам. Оптимальность маршрута определяется на основе некоторого критерия в качестве которого могут выступать показатели скорости передачи, задержки, стоимости маршрутов. Исходя из численных значений критериев для каждого из известных маршрутов формируется таблица маршрутов. На основе этой таблицы и информации об адресе сетевого уровня, содержащихся в пересылаемом пакете, маршрутизатор осуществляет пересылку пакета по определенному маршруту. Алгоритмы определения оптимальных маршрутов придают маршрутизаторам более высокий “интеллект” по сравнению с мостами.

Это позволяет:

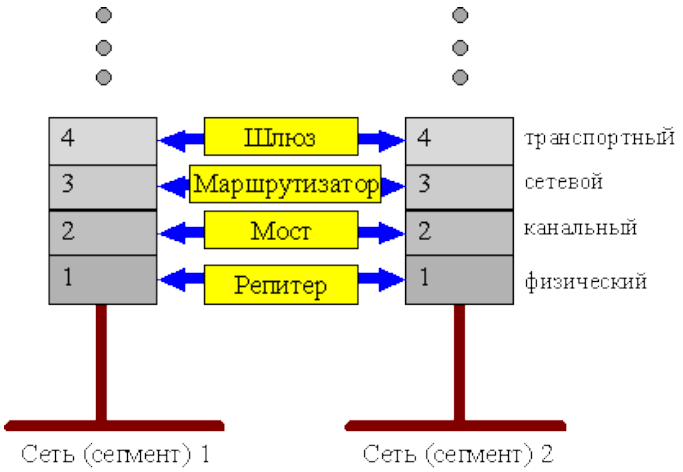
избегать больших задержек при передаче пакетов, выбирая альтернативные пути;

динамически изменять маршруты при отказе каналов или больших нагрузках в сети;

уменьшать стоимость передачи за счет выбора альтернативных путей.

Объединение через межсетевые интерфейсы, называемые также **шлюзами** (gateway) осуществляется на уровнях 4-7. Применение шлюзов связано с необходимостью осуществлять сетевые взаимодействия в неоднородной среде. Неоднородность заключается в существовании различных стеков протоколов, установленных на станциях между которыми необходимо осуществлять взаимодействие. Наиболее известными стеками протоколов являются SPX/IPX, TCP/IP, ISO. Работа шлюза заключается в преобразовании пакетов одного стека протоколов в другой.

Каждое из перечисленных устройств обеспечивает функциональные возможности, соответствующие своему уровню, а также использует функциональные возможности всех более низких уровней. “Интеллектуальность”, а вместе с ней сложность и стоимость межсетевых устройств повышаются с уровнем OSI на котором в них происходит объединение в LAN.



Задание: Опишите процесс объединения LAN.

Практическое занятие №20

Изучение системы управления сетевым оборудованием. Протокол SNMP

Цель занятия: изучить задачи протокола SNMP.
Оборудование: раздаточный материал.
Основные теоретические сведения
Основная задача при управлении компьютерными сетями – автоматизировать процесс конфигурации и мониторинга параметров сети. На сегодня существует множество моделей и систем сетевого управления. Эта статья должна помочь читателю разобраться во всем этом разнообразии. Обычно, система сетевого управления представляет собой прикладную программу высокого уровня, которая использует один из стандартных протоколов сетевого управления. (SimpleNetworkManagementProtocol (SNMP) или CommonManagementInformationProtocol (CMIP)).
CMIP применяется в телекоммуникационных сетях, где необходимы все доступные возможности управления сетями, в то время как SNMP используется в локальных и корпоративных сетях, где достаточно минимума данных.
Информационная структура большинства компаний представляет собой сложную разнородную сеть, которая состоит из разнообразного программного и аппаратного обеспечения многих производителей, а интеллектуальная система управления сетевым оборудованием способна значительно упростить процесс управления телекоммуникационным оборудованием.
Основными задачами системы управления являются:
1. обеспечение высокой производительности сети;
2. обеспечение удобной среды для управления сетевыми ресурсами;
3. сбор информации о состоянии всех сетевых устройств;
4. анализ и хранение информации о состоянии всех сетевых устройств;
5. прогнозирование возможных сбоев в работе сети.

ПРОТОКОЛЫ УПРАВЛЕНИЯ СЕТЯМИ

Системы управления сетями используют один из стандартных протоколов (SNMPили CMIP).

Система, основанная на протоколе SNMP, включает в себя:

1.протокол взаимодействия агента и менеджера;
2.язык описания моделей MIB и сообщений SNMP — язык абстрактной синтаксической нотации ASN.1
3.ограниченное количество моделей MIB (MIB-I, MIB-II, RMON, …)

Изначально, протокол SNMP и база SNMPMIB разрабатывались как временное решение для управления маршрутизаторами Интернет. Но решение оказалось настолько простым, эффективным и гибким, что и по сей день, оно находит повсеместное применение при управлении сетевым оборудованием.
С помощью протокола SNMP можно оценить производительность сетевых устройств, количество свободных ресурсов, загруженность и получить множество других полезных характеристик, необходимых для управления сетевыми устройствами. SNMP – протокол типа “запрос-ответ” т.е на каждый запрос от менеджера должен быть передан ответ от агента.

Протокол SNMP обладает достаточно небольшим набором команд:

1.Команда ‘Get-request’ применяется менеджером для получения от агента значения объекта по имени;
2.Команда ‘GetNext-request’ применяется менеджером для получения значения следующего объекта при последовательном обходе MIB;
3.При помощи команды ‘Get-response’ агент SNMP передает менеджеру результаты вышеперечисленных команд;
4.Команда ‘Set’ устанавливает значения объекта;
5.Команда ‘Trap’ сообщает менеджеру о возникновении какой-либо нестандартной ситуации;
6.В SNMPv.2 добавлена команда ‘GetBulk’, при помощи которой менеджер может получить несколько значений переменных за один запрос.

Сама структура MIB имеет стандартизированную структуру, которой придерживаются все фирмы-производители сетевого оборудования. Для специфических параметров сетевого оборудования используются специальные частные (private) поддеревья.

В протоколе SNMP присутствует агент, который обрабатывает данные, полученные из MIB, и передает их менеджеру, на управляющей станции сети. В результате управляющие станции обладают всей информацией, которая им необходима из MIB. главное достоинство протокола SNMP заключается в его простоте и в том, что он поддерживается почти всеми производителями сетевого оборудования.

Из-за своей простоты, протокол SNMP обладает еще и некоторыми недостатками:
1.при опросе происходит загрузка сети сервисной информацией, что ухудшает пропускную способность сети в целом;
2.данные практически не шифруются при передаче;
3.Так как вкачестве транспортного протокола используется протокол низкого уровня (UDP), нет возможности подтвердить доставку информации.
В следующей таблице представлены наиболее важные характеристики самых распространенных платформ управления:

	HP OpenView Network Node Manager	**IBM Tivoli NetView**	**Sun Solstice Domain Manager**
Определение имени хоста по его адресу через сервер DNS	+	+	+
Возможность модификации присвоенного имени хоста	+	+	+
Распознавание сетевых топологий	Любые сети, работающие по TCP/IP	Распознавание по интерфейсам устройств	Ethernet, Token Ring, FDDI, распределенные сети
Поддержка баз данных	MicrosoftSQLServer, Oracle, интегрированные	DB2, Informix, Oracle, SQL, Sybase	Informix, Oracle, Sybase
Формат отчетов	Формат HTML,электронная почта	Формат HTML	Консоль
Поддерживаемые веб серверы	MicrosoftIIS,Apache	WebSphere® Application Server, BEA WebLogic Application Server, Apache, Microsoft IIS, Planet Web Server	
Поддерживаемые протоколы	SNMPv1; SNMPv2, TCP/IP,	SNMP, SOAP, SSH,	CMIP, SNMP,

	IPX/DMI, UDP, ICMP, ARP/RARP	TCP/IP	NC/NFS, IPX, TCP/IP, SunNet OSI, X.25 Start, DCE, Netware
Взаимодействие с мэйнфреймами	При помощи приложений третьих фирм	Может обращаться к NetView на мэйнфрейме	+
Поддержка ОС	HP-UX, Solaris, Windows, Linux	AIX, OSF/1, Windows NT	Solaris 2.4илиболеепоздняяверсия Solaris 1.1.1 (SunOS™ 4.1.3) Или более поздняя версия

Контрольные вопросы:

1. Достоинства и недостатки SNMP.
2. Основные задачи системы управления.
3. Набор команд протокола SNMP.

Практическое занятие №21

Протокол маршрутизации RIP.

Цель занятия: изучить назначение протоколов маршрутизации.

Оборудование: справочный материал.

Краткие теоретические сведения:

Интернет – это комбинация сетей, соединяемых с помощью маршрутизаторов. Когда *дейтаграмма* идет от источника к пункту назначения, она, вероятнее всего, проходит много маршрутизаторов, пока достигает маршрутизатора, закрепленного за сетью пункта назначения. *Маршрутизатор* получает пакет от сети и передает его другой сети. *Маршрутизатор* обычно закрепляется за несколькими сетями. Когда он получает пакет, он должен решить две задачи:

1. к какой сети он должен его передать;
2. по какому пути.

Последнее решение основано на выборе оптимального пути. Какой доступный *путь* является оптимальным путем? Это обычно определяется метрикой. **Метрика** – это условная *стоимость* передачи *по* сети. Полное измерение конкретного маршрута равно сумме метрик сетей, которые включают в себя *маршрут*. *Маршрутизатор* выбирает *маршрут* с наименьшей метрикой. *Метрика* назначается для интерфейса сети в зависимости от типа протокола. Некоторые простые протоколы, подобно протоколу маршрутной информации (*RIP – Routing Information Protocol*), рассматривают все сети как одинаковые. Тогда *стоимость* прохождения через каждую *сеть* — одна и та же, и для определения метрики подсчитываются участки. Так, если пакет, чтобы достигнуть конечного пункта, проходит через 10 сетей, полная *стоимость* составляет 10 участков.

Другие протоколы, такие как "первоочередное открытие наикратчайших путей" (*OSPF — Open* Shortest *Path First*), позволяют администратору назначить *стоимость* для передачи через *сеть*, основанную на типе требуемого обслуживания. *Маршрут* через *сеть* может иметь различную *стоимость* (метрику). Например, если для типа сервиса желательна максимальная *производительность*, спутниковый канал имеет меньшую метрику, чем оптическая линия. С другой стороны, если типу сервера желательна минимальная задержка, оптическая линия имеет меньшую метрику, чем спутниковый канал. *OSPF* позволяет каждому маршрутизатору иметь таблицу последовательностей маршрутов, основанную на требуемом типе сервиса.

Другие протоколы определяют метрику различно. В протоколе пограничной маршрутизации (*BGP — Border Gateway Protocol*) критерий — это политика, которую может устанавливать *администратор*. Политика — это принцип, *по* которому определяется *путь*.

В любой метрике *маршрутизатор* должен иметь таблицы маршрутизации, чтобы консультироваться при дальнейшей передаче пакета. *Таблица* маршрутизации задает оптимальный *путь* для пакета. *Таблица* может быть либо статическая, либо *динамическая*. **Статическая таблица** — одна из тех, которые часто не меняются. **Динамическая таблица** — одна из тех, которая обновляется автоматически, когда имеются изменения где-либо в Интернете. Сегодня *Интернет* нуждается в динамических таблицах. Таблицы нужно

обновлять *по* мере появления изменений в Интернете. Например, их нужно обновить, когда *маршрут* вышел из строя, или они должны быть обновлены всякий раз, когда создается лучший *маршрут*.

Протоколы маршрутизации созданы для отображения требований таблиц *динамической маршрутизации*. *Протокол маршрутизации*— комбинация правил и процедур, которые позволяют в Интернете маршрутизаторам информировать друг друга об изменениях. Протоколы маршрутизации также включают процедуры для комбинирования информации, полученной от других маршрутизаторов.

В этой лекции мы поговорим об однонаправленных протоколах маршрутизации. Многонаправленные протоколы маршрутизации мы обсудим в следующей лекции.

Внутренняя и внешняя маршрутизация

Сегодня *Интернет* — громадная *сеть*, так что один *протокол маршрутизации* не может обрабатывать задачу обновления таблиц всех маршрутизаторов. *По* этой причине *Интернет* разделяется на автономные системы. **Автономная система (Autonomous System – AS)** — *группа* сетей и маршрутизаторов под управлением одного администратора. *Маршрутизация* внутри автономной системы отнесена к **внутренней маршрутизации**. *Маршрутизация* между автономными системами отнесена к **внешней маршрутизации**. Каждая автономная система может выбрать протокол внутренней маршрутизации для того, чтобы обрабатывать маршрутизацию внутри автономной системы. Однако для обработки маршрутизации между автономными системами выбирается только один*протокол маршрутизации*.

Разработано несколько внутренних и внешних протоколов. В этой лекции мы коснемся только наиболее популярных из них — внутренних протоколов *RIP* и *OSPF* и одного внешнего протокола *BGP*. *RIP* и *OSPF* используются для обновления таблиц маршрутизации внутри автономной системы. Протокол *BGP* применяется в обновлении таблиц маршрутизации для маршрутизаторов, которые объединяют вместе автономные системы.

Протокол маршрутной информации (RIP)

Протокол маршрутной информации (*RIP – Routing Information Protocol*) — внутренний *протокол маршрутизации*, используется внутри автономной системы. Это очень простой протокол, основанный на применении дистанционного вектора маршрутизации. В этом разделе сначала рассмотрим принцип дистанционного вектора маршрутизации, так как он применяется в *RIP*, а затем обсудим сам протокол *RIP*.

Вектор расстояния маршрутизации

Используя **вектор расстояния маршрутизации**, каждый маршрутизатор периодически делится своей информацией о входах в Интернет со своими соседями. Ниже приводятся три основных принципа этого процесса, для того чтобы понять, как работает алгоритм.

1. **Распределение информации о входе в автономную систему**. Каждый маршрутизатор распределяет информацию о входе соседним автономным системам. Вначале эта информация может быть не подробной. Однако объем и качество информации не играют роли. Маршрутизатор посылает, во всяком случае, все что имеет.

2. **Распределение только соседям**. Каждый маршрутизатор посылает свою информацию только к соседям. Он посылает информацию, которую получает через все интерфейсы.
3. **Распределение через регулярные интервалы**. Каждый маршрутизатор посылает свою информацию соседней автономной системе через фиксированные интервалы, например, каждые 30 с.

Таблицы маршрутизации

Каждый *маршрутизатор* хранит таблицы маршрутизации, имеющие один вход для каждой сети назначения, которую *маршрутизатор* зарегистрировал. Вход содержит:

- адрес сети пункта назначения,
- кратчайший путь для того, чтобы достичь пункта назначения, отсчитываемый в участках,
- следующий участок (следующий маршрутизатор), к которому должен быть доставлен пакет по пути к своему конечному пункту назначения,
- счетчик участков – это число сетей, которые пакет пересечет для достижения своего конечного пункта назначения.

Таблица может содержать другую информацию, такую как маску подсети (или *префикс*) или время, когда этот вход был обновлен.

Табл. 8.1. показывает пример таблицы маршрутизации.

Номер входа в таблицу участков	Пункт назначения	Счет участков	Следующий участок	Другая информация
0	163.5.0.0	7	172.6.23.4	
1	197.5.13.0	5	176.3.6.17	
2	189.45.0.0	4	200.5.1.6	
3	115.0.0.0	6	131.4.7.19	

Контрольные вопросы:

1. Назначение протокола RIP
2. Как составляется таблица маршрутизации

Практическое занятие №22

Протокол маршрутизации OSPF. Построение маршрутных таблиц

Цель занятия: изучить назначение и принцип работы протокола OSPF.

Оборудование: справочный материал.

Теоретические сведения:

Протокол OSPF (Open Shortest Pass First, RFC-1245-48, RFC-1583-1587, алгоритмы предложены Дикстрой) является альтернативой RIP в качестве внутреннего протокола маршрутизации. OSPF представляет собой протокол состояния маршрута (в качестве метрики используется - коэффициент качества обслуживания). Каждый маршрутизатор обладает полной информацией о состоянии всех интерфейсов всех маршрутизаторов (переключателей) автономной системы. Протокол OSPF реализован в демоне маршрутизации gated, который поддерживает также RIP и внешний протокол маршрутизации BGP.

Автономная система может быть разделена на несколько областей, куда могут входить как отдельные ЭВМ, так и целые сети. В этом случае внутренние маршрутизаторы области могут и не иметь информации о топологии остальной части AS. Сеть обычно имеет выделенный (designated) маршрутизатор, который является источником маршрутной информации для остальных маршрутизаторов AS. Каждый маршрутизатор самостоятельно решает задачу оптимизации маршрутов. Если к месту назначения ведут два или более эквивалентных маршрута, информационный поток будет поделен между ними поровну. Переходные процессы в OSPF завершаются быстрее, чем в RIP. В процессе выбора оптимального маршрута анализируется ориентированный граф сети. Приведена схема узлов (A-J) со значениями метрики для каждого из отрезков пути. Анализ графа начинается с узла A (Старт). Пути с наименьшим суммарным значением метрики считаются наилучшими. Именно они оказываются выбранными в результате рассмотрения графа ("кратчайшие пути").

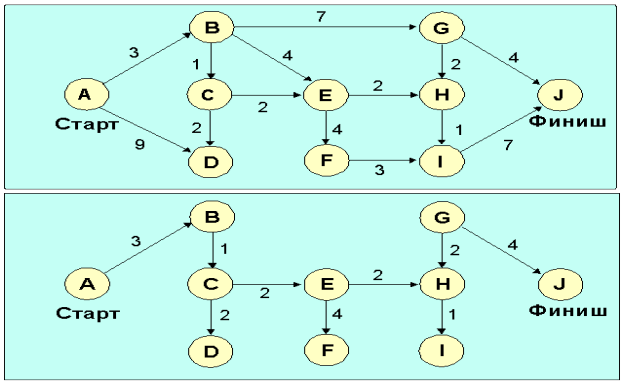


Рис. 4.2.11.2.1 Иллюстрация работы алгоритма Дикстры

Ниже дается формальное описание алгоритма. Сначала вводим некоторые определения.

Пусть D(v) равно сумме весов связей для данного пути.
Пусть c(i,j) равно весу связи между узлами с номерами i и j.

Далее следует последовательность шагов, реализующих алгоритм.

Устанавливаем множество узлов N = {1}.

Для каждого узла v не из множества n устанавливаем D(v)= c(1,v).

Для каждого шага находим узел w не из множества N, для которого D(w) минимально, и добавляем узел w в множество N.

Актуализируем D(v) для всех узлов не из множества N D(v)=min{D(v), D(v)+c(w,v)}.

Повторяем шаги 2-4, пока все узлы не окажутся в множестве N.

Топология маршрутов для узла a приведена на нижней части рис. 4.2.11.2.1. В скобках записаны числа, характеризующие метрику отобранного маршрута согласно критерию пункта 3.

Таблица 4.2.11.2.1. Реализация алгоритма

	Множество	Метрика связи узла a с узлами								
Шаг	N	B	C	D	E	F	G	H	I	J
0	{A}	3	-	9	-	-	-	-	-	-
1	{A,B}	(3)	4	9	7	-	10	-	-	-
2	{A,B,C}	3	(4)	6	6	10	10	8	-	14
3	{A,BC,D}	3	4	(6)	6	10	10	8	9	14
4	{A,B,C,D,E}	3	4	6	(6)	10	10	8	9	14
5	{A,B,C,D,E,H}	3	4	6	6	10	10	(8)	9	14
6	{A,B,C,D,E,H,I}	3	4	6	6	10	10	8	(9)	14
7	{A,B,C,D,E,H,I,F}	3	4	6	6	(10)	10	8	9	14
8	{A,B,C,D,E,H,I,F,G}	3	4	6	6	10	(10)	8	9	14
9	{A,B,C,D,E,H,I,F,G,J}	3	4	6	6	10	10	8	9	(14)

Таблица 4.2.11.2.1 может иметь совершенно иное содержимое для какого-то другого вида сервиса, выбранные пути при этом могут иметь другую топологию. Качество сервиса (QoS) может характеризоваться следующими параметрами:

пропускной способностью канала;

задержкой (время распространения пакета);

числом дейтограмм, стоящих в очереди для передачи;

загрузкой канала;

требованиями безопасности;

типом трафика;

числом шагов до цели;

возможностями промежуточных связей (например, многовариантность достижения адресата).

Определяющими являются три характеристики: задержка, пропускная способность и надежность. Для транспортных целей OSPF использует IP непосредственно, т.е. не привлекает протоколы UDP или TCP. OSPF имеет свой код (89) в протокольном поле IP-заголовка. Код TOS (type of service) в IP-пакетах, содержащих OSPF-сообщения, равен нулю, значение TOS здесь задается в самих пакетах OSPF. Маршрутизация в этом протоколе определяется IP-адресом и типом сервиса. Так как протокол не требует инкапсуляции пакетов, сильно облегчается управление сетями с большим количеством бриджей и сложной топологией (исключается циркуляция пакетов, сокращается транзитный трафик).

Автономная система может быть поделена на отдельные области, каждая из которых становится объектом маршрутизации, а внутренняя структура снаружи не видна (узлы на рис. 4.2.11.2.1 могут представлять собой как отдельные ЭВМ или маршрутизаторы, так и целые сети). Этот прием позволяет значительно сократить необходимый объем маршрутной базы данных. В OSPF используется термин опорной сети (backbone) для коммуникаций между выделенными областями. Протокол работает лишь в пределах автономной системы. В пределах выделенной области может работать свой протокол маршрутизации.

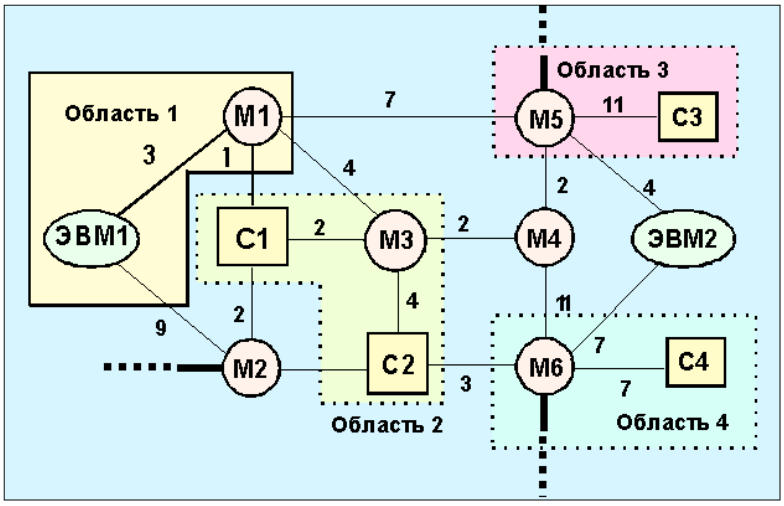


Рис. 4.2.11.2.2 Пример выделения областей при ospf маршрутизации в автономной системе (М - маршрутизаторы; с - сети).

На рис 4.2.11.2.2 (см. также рис. 4.2.11.2.1) приведен пример выделения областей маршрутизации при ospf-маршрутизации в пределах автономной системы. На рис. 4.2.11.2.2 маршрутизаторы М4 и М2 выполняют функция опорной сети для других областей. В выделенных областях может быть любое число маршрутизаторов. Более толстыми линиями выделены связи с другими автономными системами.

При передаче OSPF-пакетов фрагментация не желательна, но не запрещается. Для передачи статусной информации OSPF использует широковещательные сообщения Hello. Для повышения безопасности предусмотрена авторизация процедур. OSPF-протокол требует резервирования двух мультикастинг-адресов:

224.0.0.5	предназначен для обращения ко всем маршрутизаторам, поддерживающим этот протокол.
224.0.0.6	служит для обращения к специально выделенному маршрутизатору.

Любое сообщение ospf начинается с 24-октетного заголовка:

Версия	Тип	Длина сообщения
IP-адрес маршрутизатора-отправителя		
Идентификатор области		
Контрольная сумма		Тип идентификации
Идентификация (октеты 0-3)		
Идентификация (октеты 4-7)		

Рис. 4.2.11.2.3 Формат заголовка сообщений для протокола маршрутизации ospf

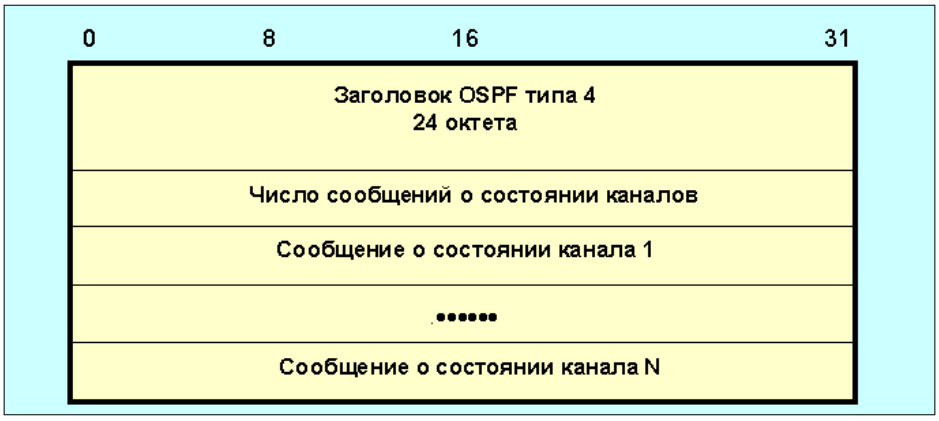


Рис. 4.2.11.2.7 Сообщение об изменении маршрутов

Сообщения об изменениях маршрутов могут быть вызваны следующими причинами:

1. Возраст маршрута достиг предельного значения (lsrefreshtime).
2. Изменилось состояние интерфейса.
3. Произошли изменения в маршрутизаторе сети.
4. Произошло изменение состояния одного из соседних маршрутизаторов.
5. Изменилось состояние одного из внутренних маршрутов (появление нового, исчезновение старого и т.д.)
6. Изменение состояния межзонного маршрута.
7. Появление нового маршрутизатора, подключенного к сети.
8. Вариация виртуального маршрута одним из маршрутизаторов.
9. Возникли изменения одного из внешних маршрутов.
10. Маршрутизатор перестал быть пограничным для данной as (например, перезагрузился).

Каждое сообщение о состоянии канала начинается с заголовка - "объявление состояния канала" (LS- link state).

Маршрутная таблица OSPF содержит в себе:

IP-адрес места назначения и маску;

тип места назначения (сеть, граничный маршрутизатор и т.д.);

тип функции (возможен набор маршрутизаторов для каждой из функций TOS);

область (описывает область, связь с которой ведет к цели, возможно несколько записей данного типа, если области действия граничных маршрутизаторов перекрываются);

тип пути (характеризует путь как внутренний, межобластной или внешний, ведущий к AS);

цена маршрута до цели;

очередной маршрутизатор, куда следует послать дейтограмму;

объявляющий маршрутизатор (используется для межобластных обменов и для связей автономных систем друг с другом).

Преимущества OSPF:

Для каждого адреса может быть несколько маршрутных таблиц, по одной на каждый вид IP-операции (TOS).

Каждому интерфейсу присваивается безразмерная цена, учитывающая пропускную способность, время транспортировки сообщения. Для каждой IP-операции может быть присвоена своя цена (коэффициент качества).

При существовании эквивалентных маршрутов OSFP распределяет поток равномерно по этим маршрутам.

Поддерживается адресация субсетей (разные маски для разных маршрутов).

При связи точка-точка не требуется IP-адрес для каждого из концов. (Экономия адресов!)

Применение мультикастинга вместо широковещательных сообщений снижает загрузку не вовлеченных сегментов.

Недостатки:

Трудно получить информацию о предпочтительности каналов для узлов, поддерживающих другие протоколы, или со статической маршрутизацией.

OSPF является лишь внутренним протоколом.

Контрольные вопросы:

1. Алгоритм Дейкстры.
2. Причины сообщений об изменениях маршрутов.