Основы информационных технологий

ПОСТРОЕНИЕ КОММУТИРУЕМЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие
2-е издание, дополненное и исправленное

Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника»

Национальный Открытый Университет «ИНТУИТ»
www.intuit.ru

Москва
2015

УДК 004.7(075.8)
ББК 32.973.202я73-1
П63

Авторский коллектив:
Е.В. Смирнова, А.В. Пролетарский, И.В. Баскаков, Р.А. Федотов, Е.А. Ромашкина

П63 Построение коммутируемых компьютерных сетей: учебное пособие / Е.В. Смирнова и др. — М.: Национальный Открытый Университет «ИНТУИТ», 2015. — 392 с.: ил., табл. — (Основы информационных технологий).

ISBN 978-5-9556-0175-5

В книге описаны принципы построения и обслуживания коммутируемых компьютерных сетей, приведено полное описание фундаментальных технологий коммутации, таких как коммутация 2-го уровня, коммутация 3-го уровня, IEEE 802.1Q, IEEE 802.1p, RSTP, MSTP, IGMP и многих других. Большой объем практических занятий посвящен самостоятельному конфигурированию, администрированию и мониторингу сетей на примере коммутаторов компании D-Link. В конце книги приведен обширный глоссарий.

Адресовано студентам, обучающимся по направлению «Информатика и вычислительная техника», аспирантам, сетевым администраторам, специалистам предприятий, внедряющим новые информационные технологии.

УДК 004.7(075.8)
ББК 32.973.202я73-1

D-Link®
Building Networks for People

Данная книга написана совместно сотрудниками компании D-Link, преподавателями МГТУ им. Н.Э. Баумана и Центра Сетевых Технологий МГТУ им. Н.Э.Баумана – D-Link и кафедры «Компьютерные системы и сети».

ISBN 978-5-9556-0175-5

О проекте

Национальный Открытый Университет «ИНТУИТ» – это первое в России высшее учебное заведение, которое предоставляет возможность получить дополнительное образование во Всемирной сети. Web-сайт университета находится по адресу www.intuit.ru.

Мы рады, что вы решили расширить свои знания в области компьютерных технологий. Современный мир – это мир компьютеров и информации. Компьютерная индустрия – самый быстрорастущий сектор экономики, и ее рост будет продолжаться еще долгое время. Во времена жесткой конкуренции от уровня развития информационных технологий, достижений научной мысли и перспективных инженерных решений зависит успех не только отдельных людей и компаний, но и целых стран. Вы выбрали самое подходящее время для изучения компьютерных дисциплин. Профессионалы в области информационных технологий сейчас востребованы везде: в науке, экономике, образовании, медицине и других областях, в государственных и частных компаниях, в России и за рубежом. Анализ данных, прогнозы, организация связи, создание программного обеспечения, построение моделей процессов – вот далеко не полный список областей применения знаний для компьютерных специалистов.

Обучение в университете ведется по собственным учебным планам, разработанным ведущими российскими специалистами на основе международных образовательных стандартов Computer Curricula 2001 Computer Science. Изучать учебные курсы можно самостоятельно по учебникам или на сайте НОУ «ИНТУИТ», задания выполняются только на сайте. Для обучения необходимо зарегистрироваться на сайте университета. Удостоверение об окончании учебного курса или специальности выдается при условии выполнения всех заданий к лекциям и успешной сдачи итогового экзамена.

Книга, которую вы держите в руках, – очередная в многотомной серии «Основы информационных технологий», выпускаемой НОУ «ИНТУИТ». В этой серии будут выпущены учебники по всем базовым областям знаний, связанным с компьютерными дисциплинами.

Добро пожаловать в
Национальный Открытый Университет «ИНТУИТ»!

Об авторах

Смирнова Елена Викторовна, кандидат технических наук, менеджер по образовательным проектам российского представительства компании D-Link. Окончила Московский государственный университет путей сообщения (МИИТ) в 1997 году. Занимается разработкой учебных материалов, отвечает за сотрудничество с учебными заведениями. Является автором ряда учебных пособий по технологиям коммутируемых сетей. Имеет сертификаты компании D-Link.

Баскаков Игорь Владимирович, кандидат технических наук, старший научный сотрудник, доцент кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана. Окончил МВТУ им. Н.Э. Баумана в 1962 году. Стаж научно-педагогической работы более 50 лет. Основные направления образовательной деятельности – организация беспроводных и коммутируемых сетей, администрирование операционных систем, периферийные устройства, защита информации.

Пролетарский Андрей Викторович, доктор технических наук, декан факультета «Информатика и системы управления» МГТУ им. Н.Э. Баумана, профессор кафедры «Системы автоматического управления». Окончил МВТУ им. Н.Э. Баумана в 1987 году. Стаж научно-педагогической работы более 20 лет. Автор более 100 научных и учебных работ по интеллектуальным системам управления, системам управления движением и навигации, информационным технологиям.

Федотов Роман Анатольевич, преподаватель МГТУ им. Н.Э. Баумана, технический директор ЗАО «2В Сервис». Окончил МГТУ им. Н.Э. Баумана в 1994 году. Стаж научно-педагогической работы более 15 лет. Автор ряда учебных пособий по организации беспроводных и коммутируемых сетей, администрированию операционных систем, мультимедийным технологиям.

Ромашкина Екатерина Александровна, аспирант кафедры «Вычислительные системы и сети» МИИТ, консультант по образовательным проектам российского представительства компании D-Link. Окончила Московский государственный университет путей сообщения (МИИТ) в 2012 году. Занимается разработкой учебных материалов. Имеет сертификаты компании D-Link.

Лекции

Оглавление

Введение

По мере развития сетевых технологий современные коммутаторы становятся все более сложными устройствами. Для успешного построения и обслуживания сетей ключевым моментом является понимание фундаментальных основ наиболее распространенных сетевых технологий, таких как коммутация 2-го уровня, коммутация 3-го уровня, IEEE 802.1Q, IEEE 802.1p, RSTP, MSTP, IGMP и многих других, а также знание того, как данные технологии можно применить на практике наиболее эффективно.

Книга «Построение коммутируемых компьютерных сетей» появилась благодаря многолетнему сотрудничеству компании D-Link и ведущего технического университета страны — МГТУ им. Н. Э. Баумана. Книга направлена на глубокое изложение теории и формирование практических знаний. В ее основу легли учебные материалы компании D-Link, а также практические занятия, проводимые в Центре Сетевых Технологий МГТУ им. Н.Э.Баумана – D-Link и кафедры «Компьютерные системы и сети».

Книга содержит полное описание фундаментальных технологий коммутации локальных сетей, примеры их использования, а также настройки на коммутаторах D-Link. Она будет полезна студентам, обучающимся по направлению «Информатика и вычислительная техника», аспирантам, сетевым администраторам, специалистам предприятий, внедряющим новые информационные технологии, а также всем, кто интересуется современными сетевыми технологиями и принципами построения коммутируемых сетей.

Авторы хотят поблагодарить всех людей, вовлеченных в процесс консультирования, редактирования и подготовки рисунков для книги. Авторы выражают благодарность руководителям Представительства компании «Д-Линк Интернешнл ПТЕ Лтд» и МГТУ им. Н. Э. Баумана, специалистам компании D-Link Павлу Козику, Руслану Бигарову, Александру Зайцеву, Евгению Рыжову и Денису Евграфову, Александру Щадневу за технические консультации; Ольге Кузьминой за редактирование книги; Алесе Дунаевой за помощь в подготовке иллюстраций. Большую помощь в подготовке рукописи и тестировании практических занятий оказали преподаватели МГТУ им. Н. Э. Баумана Михаил Калинов, Дмитрий Чирков.

Обозначения, используемые в книге

В тексте книги используются следующие пиктограммы для обозначения сетевых устройств различных типов:


Маршрутизатор


Коммутатор уровня 3


Коммутатор уровня 2


Коммутатор на основе шасси


Сервер


Рабочая станция


Портативный компьютер


Персональный компьютер


Пользователь


Сетевая среда


Линия последовательной передачи

Синтаксис команд

Следующие символы используются для описания ввода команд, ожидаемых значений и аргументов при настройке коммутатора через интерфейс командной строки (CLI).

Таблица 1.

Символ	Назначение
<угловые скобки >	Содержат ожидаемую переменную или значение, которое должно быть указано
[квадратные скобки]	Содержат требуемое значение или набор требуемых аргументов. Может быть указано одно значение или аргумент
| вертикальная черта	Отделяет два или более взаимно исключающих пунктов из списка, один из которых должен быть введен/указан
{фигурные скобки}	Содержит необязательное значение или набор необязательных аргументов

Лекция 1. Основы коммутации

1.1. Эволюция локальных сетей

Эволюция локальных сетей неразрывно связана с историей развития технологии Ethernet, которая по сей день остается самой распространенной технологией локальных сетей.

Первоначально технология локальных сетей рассматривалась как времясберегающая и экономичная технология, обеспечивающая совместное использование данных, дискового пространства и дорогостоящих периферийных устройств. Снижение стоимости персональных компьютеров и периферии привело к их широкому распространению в бизнесе, и количество сетевых пользователей резко возросло. Одновременно изменились архитектура приложений («клиент-сервер») и их требования к вычислительным ресурсам, а также архитектура вычислений (распределенные вычисления). Стал популярным *downsizing* (разукрупнение) — перенос информационных систем и приложений с мэйнфреймов на сетевые платформы. Все это привело к смещению акцентов в использовании сетей: они стали обязательным инструментом в бизнесе, обеспечив наиболее эффективную обработку информации.

В первых сетях Ethernet (10Base2 и 10Base5) использовалась шинная топология, когда каждый компьютер соединялся с другими устройствами с помощью единого коаксиального кабеля, используемого в качестве среды передачи данных. Сетевая среда была разделяемой и устройства, прежде чем начать передавать пакеты данных, должны были убедиться, что она свободна. Несмотря на то, что такие сети были простыми в установке, они обладали существенными недостатками, заключающимися в ограничениях по размеру, функциональности и расширяемости, недостаточной надежности, а также неспособностью справляться с экспоненциальным увеличением сетевого трафика. Для повышения эффективности работы локальных сетей требовались новые решения.

Следующим шагом стала разработка стандарта 10Base-T с топологией типа «звезда», в которой каждый узел подключался отдельным кабелем к центральному устройству — *концентратору* (*hub*). Концентратор работал на физическом уровне модели OSI и повторял сигналы, поступавшие с одного из его портов на все остальные активные порты, предварительно восстанавливая их. Использование концентраторов позволило повысить надежность сети, т.к. обрыв какого-нибудь кабеля не влек за собой сбой в работе всей сети. Однако, несмотря на то, что использование концентраторов в сети упростило задачи ее управления и сопровождения, среда передачи оставалась разделяемой (все устройства находились в одном домене коллизий). Поми-

мо этого, общее количество концентраторов и соединяемых ими сегментов сети было ограничено из-за временных задержек и других причин.

Задача *сегментации сети*, т.е. разделения пользователей на группы (сегменты) в соответствии с их физическим размещением с целью уменьшения количества клиентов, соперничающих за полосу пропускания, была решена с помощью устройства, называемого *мостом* (*bridge*). Мост был разработан компанией Digital Equipment Corporation (DEC) в начале 1980-х годов и представлял собой устройство канального уровня модели OSI (обычно двухпортовое), предназначенное для объединения сегментов сети. В отличие от концентратора, мост не просто пересылал пакеты данных из одного сегмента в другой, а анализировал и передавал их только в том случае, если такая передача действительно была необходима, то есть адрес рабочей станции назначения принадлежал другому сегменту. Таким образом, мост изолировал трафик одного сегмента от трафика другого, уменьшая домен коллизий и повышая общую производительность сети.

Однако мосты были эффективны лишь до тех пор, пока количество рабочих станций в сегменте оставалось относительно невелико. Как только оно увеличивалось, в сетях возникала перегрузка (переполнение приемных буферов сетевых устройств), которая приводила к потере пакетов.

Увеличение количества устройств, объединяемых в сети, повышение мощности процессоров рабочих станций, появление мультимедийных приложений и приложений «клиент-сервер» требовали большей полосы пропускания. В ответ на эти растущие требования фирмой Kalpana в 1990 г. на рынок был выпущен первый *коммутатор* (*switch*), получивший название EtherSwitch.

Коммутатор представлял собой многопортовый мост и также функционировал на канальном уровне модели OSI. Основное отличие коммутато-

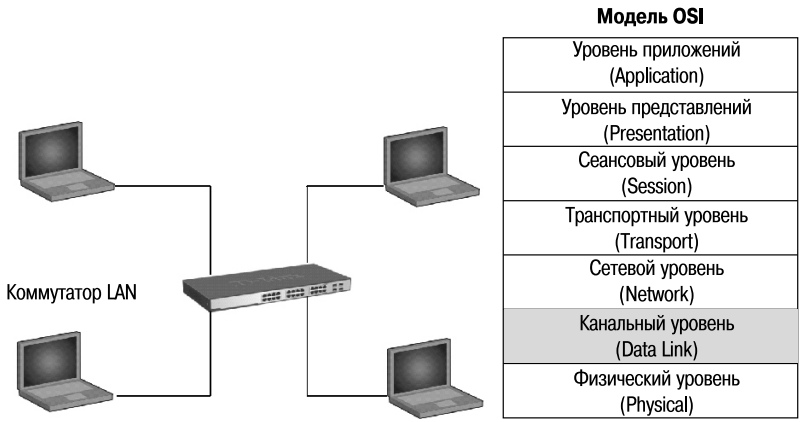


Рис. 1.1. Коммутатор локальной сети

Лекция 2. Начальная настройка коммутатора

2.1. Классификация коммутаторов по возможности управления

Коммутаторы локальной сети можно классифицировать по возможности управления. Существует три категории коммутаторов:

- неуправляемые коммутаторы;
- управляемые коммутаторы;
- настраиваемые коммутаторы.

Неуправляемые коммутаторы не поддерживают возможности управления и обновления программного обеспечения.

Управляемые коммутаторы являются сложными устройствами, позволяющими выполнять расширенный набор функций 2-го и 3-го уровня модели OSI. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протокола SNMP, Telnet и т.д.

Настраиваемые коммутаторы занимают промежуточную позицию между ними. Они предоставляют пользователям возможность настраивать определенные параметры сети с помощью интуитивно понятных утилит управления, Web-интерфейса, упрощенного интерфейса командной строки, протокола SNMP.

2.2. Средства управления коммутаторами

Большинство современных коммутаторов поддерживают различные функции управления и мониторинга. К ним относятся дружественный пользователю Web-интерфейс управления, интерфейс командной строки (Command Line Interface, CLI), Telnet, SNMP-управление. В коммутаторах D-Link серии Smart также реализована поддержка начальной настройки и обновления программного обеспечения через утилиту D-Link SmartConsole Utility.

Web-интерфейс управления позволяет осуществлять настройку и мониторинг параметров коммутатора, используя любой компьютер, оснащенный стандартным Web-браузером. Браузер представляет собой универсальное средство доступа и может непосредственно подключаться к коммутатору по протоколу HTTP.

Главная страница Web-интерфейса обеспечивает доступ к различным настройкам коммутатора и отображает всю необходимую информацию об устройстве. Администратор может быстро посмотреть статус устройства, статистику по производительности и т.д., а также произвести необходимые настройки.

Доступ к интерфейсу командной строки коммутатора осуществляется путем подключения к его консольному порту терминала или персонального компьютера с установленной программой эмуляции терминала. Это метод доступа наиболее удобен при первоначальном подключении к коммутатору, когда значение IP-адреса неизвестно или не установлено, в случае необходимости восстановления пароля и при выполнении расширенных настроек коммутатора. Также доступ к интерфейсу командной строки может быть получен по сети с помощью протокола Telnet.

Пользователь может использовать для настройки коммутатора любой удобный ему интерфейс управления, т.к. набор доступных через разные интерфейсы управления функций одинаков для каждой конкретной модели.

Еще один способ управления коммутатором – использование протокола SNMP (Simple Network Management Protocol). Протокол SNMP является протоколом 7-го уровня модели OSI и разработан специально для управления и мониторинга сетевыми устройствами и приложениями связи. Это выполняется путем обмена управляющей информацией между агентами, располагающимися на сетевых устройствах, и менеджерами, расположенными на станциях управления. Коммутаторами D-Link поддерживается протокол SNMP версий 1, 2c и 3.

Также стоит отметить возможность обновления программного обеспечения коммутаторов (за исключением неуправляемых). Это обеспечивает более долгий срок эксплуатации устройств, т.к. позволяет добавлять новые функции либо устранять имеющиеся ошибки по мере выхода новых версий ПО, что существенно облегчает и удешевляет использование устройств. Компания D-Link распространяет новые версии ПО бесплатно. Сюда же можно включить возможность сохранения настроек коммутатора на случай сбоев с последующим восстановлением или тиражированием, что избавляет администратора от выполнения рутинной работы.

2.3. Подключение к коммутатору

Перед тем, как начать настройку коммутатора, необходимо установить физическое соединение между ним и рабочей станцией. Существуют два типа кабельного соединения, используемых для управления коммутатором. Первый тип – через консольный порт (если он имеется у устройства), второй – через порт Ethernet (по протоколу Telnet или через Web-интерфейс). Консольный порт используется для первоначальной конфигурации коммутатора и обычно не требует настройки. Для того чтобы получить доступ к коммутатору через порт Ethernet, в браузере необходимо ввести IP-адрес по умолчанию его интерфейса управления (обычно он указан в руководстве пользователя).

Лекция 3. Виртуальные локальные сети (VLAN)

Поскольку коммутатор Ethernet является устройством канального уровня, то в соответствии с логикой работы он будет рассылать широковещательные кадры через все порты. Хотя трафик с конкретными адресами (соединения «точка – точка») изолирован парой портов, широковещательные кадры передаются во всю сеть (на каждый порт). *Широковещательные кадры* – это кадры, передаваемые на все узлы сети. Они необходимы для работы многих сетевых протоколов, таких как ARP, BOOTP или DHCP. С их помощью рабочая станция оповещает другие компьютеры о своем появлении в сети. Так же рассылка широковещательных кадров может возникать из-за некорректно работающего сетевого адаптера. Широковещательные кадры могут привести к нерациональному использованию полосы пропускания, особенно в крупных сетях. Для того чтобы этого не происходило, важно ограничить область распространения широковещательного трафика (эта область называется *широковещательным доменом*) – организовать небольшие **широковещательные домены,** или **виртуальные локальные сети (Virtual LAN, VLAN)**.

Виртуальной локальной сетью называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса – уникального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра. Таким образом с помощью виртуальных сетей решается проблема распространения широковещательных кадров и вызываемых ими следствий, которые могут развиться в широковещательные штормы и существенно снизить производительность сети.

VLAN обладают следующими преимуществами:

- гибкость внедрения. VLAN являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети;
- VLAN обеспечивают возможность контроля широковещательных сообщений, что увеличивает полосу пропускания, доступную для пользователя;
- VLAN позволяют повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

Рассмотрим пример, показывающий эффективность использования логической сегментации сетей с помощью технологии VLAN при реше-

нии типовой задачи организации доступа в Интернет сотрудникам офиса. При этом трафик каждого отдела должен быть изолирован.

Предположим, что в офисе имеется несколько комнат, в каждой из которых располагается небольшое количество сотрудников. Каждая комната представляет собой отдельную рабочую группу.

При стандартном подходе к решению задачи с помощью физической сегментации трафика каждого отдела потребовалось бы в каждую комнату устанавливать отдельный коммутатор, который бы подключался к маршрутизатору, предоставляющему доступ в Интернет. При этом маршрутизатор должен обладать достаточным количеством портов, обеспечивающим возможность подключения всех физических сегментов (комнат) сети. Данное решение плохо масштабируемо и является дорогостоящим, т.к. при увеличении количества отделов увеличивается количество необходимых коммутаторов, интерфейсов маршрутизатора и магистральных кабелей.

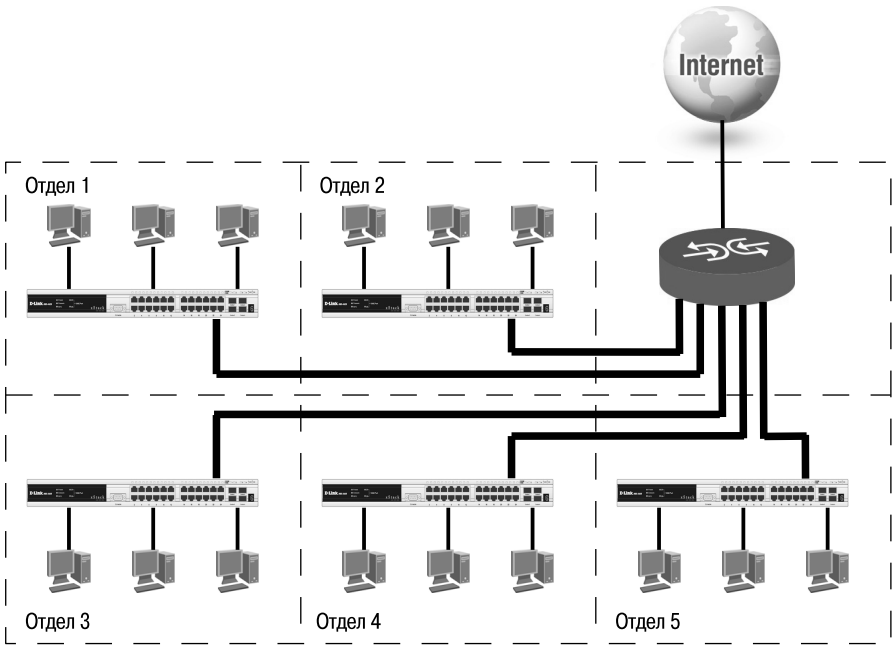


Рис. 3.1. Физическая сегментация сети

При использовании виртуальных локальных сетей уже не требуется подключать пользователей одного отдела к отдельному коммутатору, что позволяет сократить количество используемых устройств и магистраль-

Лекция 4. Функции повышения надежности и производительности

В настоящее время для повышения надежности и производительности каналов связи в распоряжении интеграторов и сетевых администраторов имеется целый набор протоколов и функций. Наиболее распространенным является создание резервных связей между коммутаторами на основе двух технологий:

1) резервирование соединений с помощью протоколов семейства Spanning Tree;
2) балансировка нагрузки, обеспечивающая параллельную передачу данных по всем альтернативным соединениям с помощью механизма агрегирования портов.

4.1. Протоколы Spanning Tree

Протокол связующего дерева **Spanning Tree Protocol (STP)** является протоколом 2 уровня модели OSI, который позволяет строить древовидные, свободные от петель, конфигурации связей между коммутаторами локальной сети. Помимо этого, алгоритм обеспечивает возможность автоматического резервирования альтернативных каналов связи между коммутаторами на случай выхода активных каналов из строя.

В настоящее время существуют следующие версии протоколов связующего дерева:

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

4.2. Spanning Tree Protocol (STP)

4.2.1. Понятие петель

Если для обеспечения избыточности между коммутаторами создается несколько соединений, то могут возникать коммутационные петли. Петля предполагает существование нескольких маршрутов по промежуточным сетям, а сеть с несколькими маршрутами между источником и приемником отличается повышенной отказоустойчивостью. Хотя наличие избыточных каналов связи очень полезно, петли, тем не менее, создают проблемы, самые актуальные из которых:

- широковещательные штормы;
- множественные копии кадров;
- множественные петли.

Широковещательный шторм.

Распространение широковещательных сообщений в сетях с петлями представляет серьезную проблему. Предположим, что первый кадр, поступивший от одного из узлов, является широковещательным. Тогда все коммутаторы будут пересылать кадры бесконечно, как показано на рис. 4.1 (пример 1), используя всю доступную полосу пропускания сети и блокируя передачу других кадров во всех сегментах.

Множественные копии кадров.

Еще одна проблема заключается в том, что коммутатор нередко получает несколько копий одного кадра, одновременно приходящих из нескольких участков сети. В этом случае таблица коммутации не сможет определить расположение устройства, потому что коммутатор будет получать кадр из нескольких каналов. Может случиться так, что коммутатор вообще не сможет переслать кадр, т.к. будет постоянно обновлять таблицу коммутации.

Множественные петли.

Одна из самых сложных проблем – это множественные петли, образующиеся в объединенной сети. Возможно появление петли внутри других петель. Если за этим последует широковещательный шторм, то сеть не сможет выполнять коммутацию кадров.

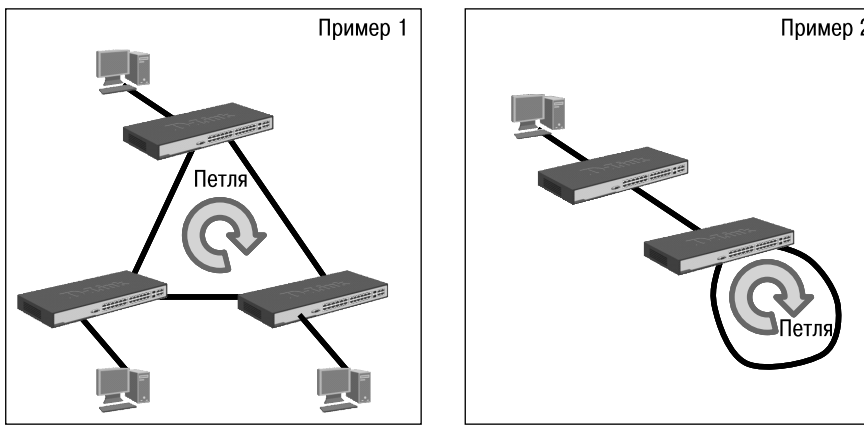


Рис. 4.1. Примеры петель между коммутаторами

Для решения этих проблем и был разработан протокол связующего дерева, который был определен в стандарте IEEE 802.1D-1998.

Коммутаторы, поддерживающие протокол STP, автоматически создают древовидную конфигурацию связей без петель в компьютерной се-

Лекция 5. Качество обслуживания (QoS)

5.1. Модели QoS

Для поддержки передачи по одной сети трафика потоковых мультимедийных приложений (Voice over IP (VoIP), IPTV, видеоконференции, онлайн игры и др.) и трафика данных с различными требованиями к пропускной способности необходимы механизмы, обеспечивающие возможность дифференцирования и обработки различных типов сетевого трафика в зависимости от предъявляемых ими требований. Негарантированная доставка данных (*best effort service*), традиционно используемая в сетях, построенных на основе коммутаторов, не предполагала проведения какой-либо классификации трафика и не обеспечивала надежную доставку трафика приложений, гарантированную пропускную способность канала и определенный уровень потери пакетов. Для решения этой проблемы было введено такое понятие, как **качество обслуживания** (*Quality of Service, QoS*).

Функции качества обслуживания в современных сетях заключаются в обеспечении гарантированного и дифференцированного уровня обслуживания сетевого трафика, запрашиваемого теми или иными приложениями на основе различных механизмов распределения ресурсов, ограничения интенсивности трафика, обработки очередей и приоритизации.

Можно выделить три модели реализации QoS в сети.

- **Негарантированная доставка данных (Best Effort Service)** – обеспечивает связь между узлами, но не гарантирует надежную доставку данных, время доставки, пропускную способность и определенный приоритет.
- **Интегрированные услуги (Integrated Services, IntServ)** – эта модель описана в RFC 1633 и предполагает предварительное резервирование сетевых ресурсов с целью обеспечения предсказуемого поведения сети для приложений, требующих для нормального функционирования гарантированной выделенной полосы пропускания на всем пути следования трафика. В качестве примера можно привести приложения IP-телефонии, которым для обеспечения приемлемого качества передачи голоса требуется канал с минимальной пропускной способностью 64 Кбит/с (для кодека G.711).

Модель IntServ использует сигнальный протокол RSVP (Resource Reservation Protocol, протокол резервирования ресурсов) для резервирования ресурсов для каждого потока данных, который должен поддерживаться каждым узлом на пути следования трафика. Эту модель также часто называют *жестким QoS* (*hard QoS*) в связи с предъявлением строгих требований к ресурсам сети.

- **Дифференцированное обслуживание (Differentiated Service, DiffServ)** – эта модель описана в RFC 2474, RFC 2475 и предполагает разделе-

ние трафика на классы на основе требований к качеству обслуживания. В архитектуре DiffServ каждый передаваемый пакет снабжается информацией, на основании которой принимается решение о его продвижении на каждом промежуточном узле сети, в соответствии с политикой обслуживания трафика данного класса (Per-Hop Behavior, PHB).

Модель дифференцированного обслуживания занимает промежуточное положение между негарантированной доставкой данных и моделью IntServ и сама по себе не предполагает обеспечение гарантий предоставляемых услуг, поэтому дифференцированное обслуживание часто называют *мягким QoS* (*soft QoS*).

5.2. Приоритизация пакетов

Для обеспечения QoS на канальном уровне модели OSI коммутаторы поддерживают стандарт IEEE 802.1p. Стандарт IEEE 802.1p позволяет задать до 8 уровней приоритетов (от 0 до 7, где 7 – наивысший), определяющих способ обработки кадра, используя 3 бита поля приоритета тега IEEE 802.1Q.

Для обеспечения QoS на сетевом уровне модели OSI в заголовке протокола IPv4 предусмотрено 8-битное поле ToS (Type of Service). Этот байт может быть заполнен либо значением приоритета IP Precedence, либо значением DSCP (Differentiated Services Code Point) в зависимости от решаемой задачи.

Поле IP Precedence имеет размерность 3 бита и может принимать значения от 0 до 7. Оно используется для указания относительного приоритета обработки пакета на сетевом уровне.

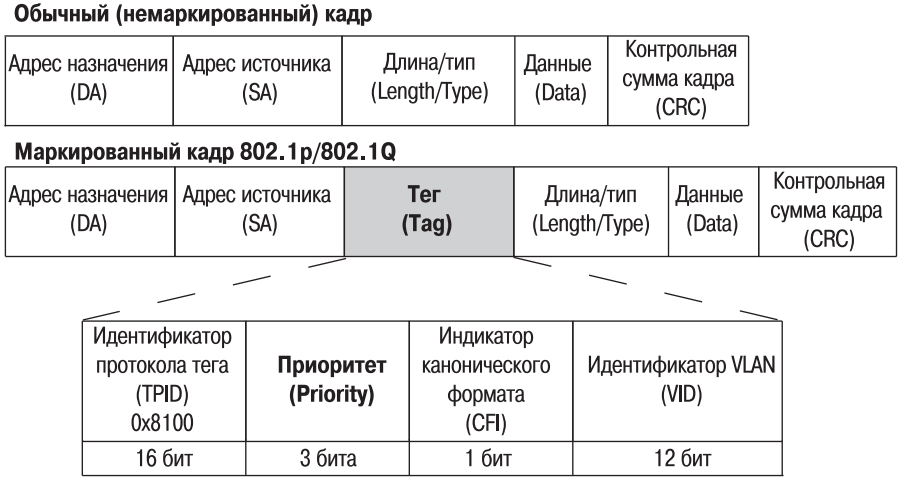


Рис. 5.1. Формат кадра 802.1Q с битами приоритета 802.1p

Лекция 6. Многоадресная рассылка

В современных IP-сетях существует три способа отправки пакетов от источника к приемнику:

- одноадресная передача *(Unicast)*;
- широковещательная передача *(Broadcast)*;
- многоадресная рассылка *(Multicast)*.

При *одноадресной передаче* поток данных передается от узла-отправителя на индивидуальный IP-адрес конкретного узла-получателя. *Широковещательная передача* предусматривает доставку потока данных от узла-отправителя – множеству узлов-получателей, подключенных к сети, используя широковещательный IP-адрес.

Многоадресная рассылка обеспечивает доставку потока данных группе узлов на IP-адрес *группы многоадресной рассылки*. У этой группы нет физических или географических ограничений: узлы могут находиться в любой точке мира. Узлы, которые заинтересованы в получении данных для определенной группы, должны присоединиться к этой группе (подписаться на рассылку) при помощи протокола IGMP (Internet Group Management Protocol, межсетевой протокол управления группами). После этого пакеты многоадресной рассылки, содержащие в поле назначения заголовка групповой адрес, будут поступать на этот узел и обрабатываться.

Многоадресная рассылка имеет ряд преимуществ при работе таких приложений как видеоконференции, корпоративная связь, дистанционное обучение, видео и аудио-трансляции и т.д., т.к. позволяет значительно повысить эффективность использования полосы пропускания и распределения информации среди больших групп получателей. Во-первых, отправитель может один раз передать единственную копию пакета данных всем членам группы, а не рассылать множество его копий. Во-вторых, благодаря передаче только одной копии пакета снижается нагрузка на канал связи.

Особенностью многоадресной рассылки является то, что она использует в качестве протокола транспортного уровня протокол UDP, который не гарантирует успешную доставку пакетов в отличие от протокола TCP.

6.1. IP-адресация многоадресной рассылки

Источник многоадресного трафика направляет пакеты многоадресной рассылки не на индивидуальные IP-адреса каждого из узлов-получателей, а на групповой IP-адрес. Групповые адреса определяют произвольную группу IP-узлов, желающих получать адресованный ей трафик.

Агентство IANA (Internet Assigned Numbers Authority, Агентство по выделению имен и уникальных параметров протоколов Интернет), которое управляет назначением групповых адресов, определило для многоадресной рассылки адреса IPv4 класса D в диапазоне от 224.0.0.0 до 239.255.255.255. Адреса, назначенные IANA, приведены в таблице ниже. Более подробную информацию о зарегистрированных адресах можно получить на Web-сайте: http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml#multicast-addresses-12

Таблица 6.1. Назначенные IANA диапазоны адресов многоадресной рассылки

Диапазон	**Описание**
224.0.0.0 – 224.0.0.255	Блок управления локальной сети (Local Network Control Block). Адреса этого диапазона зарезервированы для использования сетевыми протоколами в сегментах локальных сетей
224.0.1.0 – 224.0.1.255	Межсетевой блок управления (Internetwork Control Block). Адреса из этого диапазона используются для трафика управления протоколов, который может быть передан через Интернет
224.0.2.0 – 224.0.255.255	Блок AD-HOC I (AD-HOC Block I). Используется для приложений, которые не попадают в блок управления локальной сетью и межсетевой блок управления
224.1.0.0 – 224.1.255.255	Зарезервировано
224.2.0.0 – 224.2.255.255	Блок SDP/SAP (SDP/SAP Block). Этот диапазон адресов используется для приложений, которые получают адреса через протокол SAP для использования через приложения подобные SDR
224.3.0.0 – 224.4.255.255	Блок AD-HOC II (AD-HOC Block II). Используется для приложений, которые не попадают в блок управления локальной сетью и межсетевой блок управления
224.5.0.0 – 224.255.255.255	Зарезервировано
225.0.0.0 – 231.255.255.255	Зарезервировано
232.0.0.0 – 232.255.255.255	Блок специфичной для источника многоадресной рассылки (Source-Specific Multicast Block). Этот диапазон адресов зарезервирован для протокола SSM, который представляет собой расширение протокола PIM

Лекция 7. Функции обеспечения безопасности и ограничения доступа к сети

На сегодняшний день для любого системного администратора одной из самых острых проблем остается обеспечение безопасности компьютерной сети. Казалось бы, такие задачи призваны решать межсетевые экраны, однако подчас первый удар принимают на себя именно коммутаторы. Хотя это и не основная их задача, тем не менее, на данный момент коммутаторы обладают широким функционалом для успешного решения подобного рода задач. Речь идет не только о защите сетей от атак извне, но и о всевозможных атаках внутри сети, таких как подмена DHCP-сервера, атаки типа DoS, ARP Spoofing, неавторизованный доступ и т.д. В некоторых случаях коммутаторы не способны полностью защитить сеть от подобного рода атак, но способны значительно ослабить угрозы их возникновения. Данная глава будет посвящена принципам обеспечения сетевой безопасности на базе оборудования D-Link.

D-Link предлагает комплексный подход к решению вопросов обеспечения безопасности *End-to-End Security* (E2ES), который включает в себя следующие решения:

- *Endpoint Security* («Защита конечного пользователя») – обеспечивает защиту внутренней сети от внутренних атак;
- *Gateway Security* («Защита средствами межсетевых экранов») – обеспечивает защиту внутренней сети от внешних атак;
- *Joint Security* («Объединенная безопасность») – связующее звено между Endpoint и Gateway Security, объединяющее использование межсетевых экранов и коммутаторов для защиты сети.

Решение Endpoint Security включает следующие функции, обеспечивающие аутентификацию и авторизацию пользователей, контроль над трафиком, узлами и их адресацией в сети:

- функции аутентификации пользователей:
  - аутентификация IEEE 802.1X;
  - MAC-based Access Control (MAC);
  - WEB-based Access Control (WAC);
- функция авторизации:
  - Guest VLAN;
- функции контроля над трафиком:
  - Traffic Segmentation;
  - Access Control List (ACL);
- функции контроля над подключением/адресацией узлов в сети:
  - Port Security;
  - IP-MAC-Port Binding (IMPB);

- функции ослабления атак в сети:
  - Access Control List (ACL);
  - IP-MAC-Port Binding (IMPB);
  - Broadcast Storm Control;
  - ARP Spoofing Prevention;
  - LoopBack Detection (LBD).

Решение Joint Security включает в себя функции:
- Zone Defense;
- NAP.

Помимо основных функций безопасности, в коммутаторах D-Link реализованы дополнительные решения, позволяющие обнаруживать аномальные потоки кадров в сети Ethernet и уменьшать загрузку ЦПУ в результате множественных широковещательных запросов, вызванных атаками типа ARP Flood:
- D-Link Safeguard Engine;
- Traffic Storm Control.

Прежде чем приступить к рассмотрению темы, уточним некоторые понятия.

Аутентификация – процедура проверки подлинности субъекта на основе предоставленных им данных.

Авторизация – предоставление определенных прав лицу на выполнение некоторых действий.

Как правило, за аутентификацией следует авторизация.

7.1. Списки управления доступом (ACL)

Списки управления доступом (*Access Control List, ACL*) являются мощным средством фильтрации потоков данных без потери производительности, т.к. проверка содержимого пакетов выполняется на аппаратном уровне. Фильтруя потоки данных, администратор может ограничить типы приложений, разрешенных для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS путем классификации трафика и переопределения его приоритета.

ACL представляют собой последовательность условий проверки параметров пакетов данных. Когда сообщения поступают на входной порт, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определенными в ACL, и выполняет над пакетами одно из действий: Permit («Разрешить») или Deny («Запретить»). Критерии фильтрации могут быть определены на основе следующей информации, содержащейся в пакете данных:

Лекция 8. Технология Power over Ethernet

Устанавливая точку доступа Wi-Fi, IP-камеру или IP-телефон, часто приходиться учитывать, где находится ближайшая электрическая розетка, чтобы подключить к ней блок питания устройства. Иногда наилучшее положение устройства может вступать в противоречие с его физическим расположением. Например, для достижения лучшего уровня беспроводного сигнала требуется поместить точку доступа на потолке или крыше, а камеру на заборе или высокой стене. Установка оборудования в труднодоступных местах, где поблизости нет источника питания, а электропроводка отсутствует, представляет собой серьезную проблему. Прокладка силовых кабелей в подобных случаях может оказаться дорогостоящей и непростой задачей.

Установка оборудования сопряжена не только с подводкой кабеля питания к месту его монтажа, но и с подключением сетевых кабелей, по которым передаются данные.

Для решения проблемы электропитания устройств, находящихся в труднодоступных местах была разработана технология Power over Ethernet (PoE). Эта технология позволяет передавать удаленному (оконечному) устройству вместе с данными электрическую энергию через кабель на основе стандартной витой пары в сети Ethernet. Благодаря технологии PoE точку доступа, например, можно устанавливать в месте наилучшего приема сигнала, IP-камеру поместить в любом удобном для обзора месте, а для подключения IP-телефона не монтировать дополнительную розетку.

В качестве основных преимуществ технологии PoE можно выделить следующие:

- электропитание удаленного сетевого устройства и обмен данными с ним осуществляется по одному сетевому кабелю;
- низкие затраты на инсталляцию систем, их модернизацию и сервисное обслуживание;
- повышенная эксплуатационная безопасность: обеспечивается защита от короткого замыкания, падения напряжения, превышения потребляемого тока и т.п.;
- простота развертывания сети, особенно в сложных пространственных условиях (крыши, заборы, внутренние помещения в аэропортах и вокзалах, кафе, кинотеатры и т.п.) и простота перемещения PoE-совместимых оконечных устройств;
- возможность управления параметрами питания удаленных устройств, т.к. оборудование с поддержкой PoE часто является управляемым, что упрощает администрирование сети.

Технология PoE является расширением стандарта IEEE 802.3. Первая версия технологии была описана в стандарте IEEE 802.3af-2003, которая в 2005 году вошла в 33 раздел стандарта IEEE 802.3-2005. В 2009 году появилась новая расширенная версия технологии PoE, описанная в стандарте IEEE 802.3at-2009, также известном как PoE+ или PoE plus. В настоящее время требования к PoE-системам определяются разделом 33 стандарта IEEE 802.3-2012 (в него полностью включен стандарт IEEE 802.3at-2009). Технология PoE предназначена для использования в устройствах с интерфейсами 10Base-T, 100Base-TX и 1000Base-T.

Спецификация PoE описывает работу двух типов устройств: питающих устройств **(Power Sourcing Equipment, PSE)** и питаемых устройств **(Powered Device, PD)**.

Питающие устройства (PSE) выполняют функции источников питания и предназначены для подачи электропитания в сеть Ethernet, к которой подключены питаемые устройства (PD). *Питаемые устройства (PD)* получают электропитание через кабель от питающих устройств.

Питающее устройство (PSE) может входить в состав активного оборудования или быть выполнено в виде отдельного устройства, которое включается в сетевой сегмент (в разрыв Ethernet-канала). В первом случае питающее устройство в терминологии PoE обозначается как «Endpoint» и обычно представляет собой коммутатор с поддержкой PoE (коммутаторы D-Link с поддержкой PoE содержат букву «P» в конце названия модели, например, DGS-1210-28P). Во втором случае питающее устройство в терминологии PoE обозначается как «Midspan» и представляет собой инжектор PoE.

Инжекторы являются пассивными устройствами. Они не влияют на передачу данных и используются только для передачи электропитания через кабель. На вход инжектор получает данные и электропитание через соответствующие разъемы, а на выходе объединяет их и передает через стандартный разъем RJ-45, к которому подключен кабель. Инжекторы удобно использовать в том случае, когда в существующую сеть Ethernet требуется добавить функционал PoE, например, чтобы подключить камеру или точку доступа. В том случае, если требуется подключить большое количество устройств с поддержкой PoE, например, несколько камер видеонаблюдения, то наилучшим решением будет установка коммутатора PoE. При этом для питания коммутатора PoE рекомендуется использовать источник бесперебойного питания (UPS).

Коммутаторы PoE бывают как управляемые так и неуправляемые. Управляемые коммутаторы предпочтительнее, так как позволяют устанавливать максимальные и минимальные значения потребляемого тока, приоритеты по портам, получать информацию об ошибках, а также автоматически проверять подключенные устройства с помощью прерываний и перегружать их путем кратковременного отключения питания в случае необходимости.

Лекция 9. Функции управления коммутаторами

9.1. Управление множеством коммутаторов

Независимое управление множеством коммутаторов требует выделения каждому устройству отдельного IP-адреса, что ведет к неэкономному использованию адресного пространства и необходимости запоминания администратором сети IP-адреса каждого коммутатора. D-Link предлагает два подхода к управлению множеством коммутаторов:

- физическое стекирование коммутаторов;
- виртуальное стекирование коммутаторов.

Оба эти подхода предполагают объединение коммутаторов в физическую или логическую группу, которая будет управляться через единый IP-адрес.

9.1.1. Объединение коммутаторов в физический стек

При физическом стекировании коммутаторы представляют собой одно логическое устройство, что обеспечивает удобство управления и мониторинга их параметров. Для управления коммутаторами можно использовать интерфейс командной строки (CLI), Web-интерфейс, Telnet, протокол SNMP, и только одному коммутатору (мастеру-коммутатору) потребуется присвоение управляющего IP-адреса.

Передача данных между коммутаторами стека ведется в полнодуплексном режиме. Коммутаторы могут быть объединены в стек либо кольцевой топологии, либо линейной топологии. Одним из преимуществ стека кольцевой топологии над стеком линейной топологии является поддержка технологии определения оптимального пути передачи пакетов. Эта технология позволяет достичь полного использования полосы пропускания и повысить отказоустойчивость стека.

Внимание: технология определения оптимального пути используется для передачи только одноадресных пакетов.

В примере, приведенном на рис. 9.1, показано, что данные от коммутатора 2 передаются не по кругу (через коммутаторы 3, 4, 5 и т.д.), а непосредственно в направлении коммутатора 9 (через коммутаторы 1,12,11,10). При этом следует отметить, что весь трафик в стеке передается одновременно, и локальный трафик не оказывает влияния на трафик, циркулирующий внутри стека (рис. 9.2).

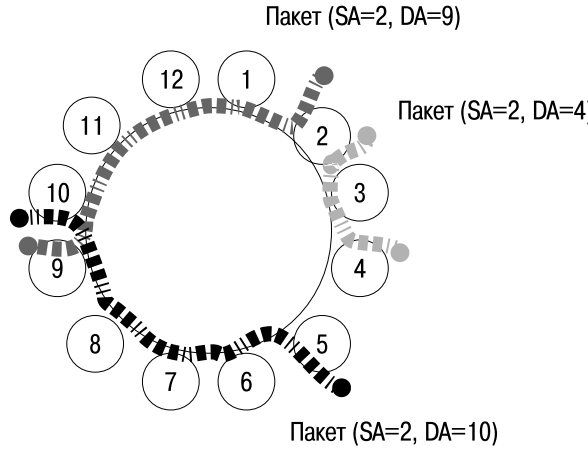


Рис. 9.1. Пример выбора оптимального пути передачи пакета в стеке типа «кольцо»

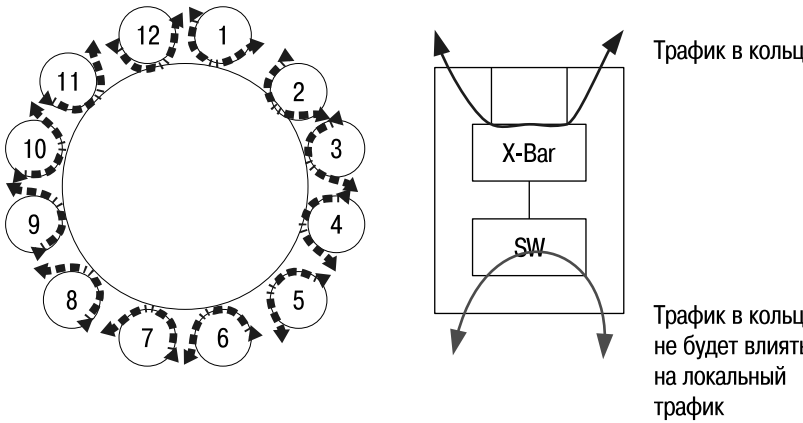


Рис. 9.2. Потоки трафика в стеке

В стеке линейной топологии данные передаются только в одном направлении, и выход из строя какого-либо коммутатора стека повлияет на его работу.

В стекируемых коммутаторах D-Link для повышения отказоустойчивости и производительности стека, реализованы следующие механизмы:

- механизм *Resilient Master Technology (RMT)* обеспечивает непрерывную работу стека при выходе какого-либо устройства из строя,

Лекция 10. Обзор коммутаторов D-Link

Исходя из решаемой задачи, учитывая размер сети, объем трафика и требуемый функционал, можно подобрать наиболее подходящие коммутаторы D-Link. Производимые D-Link устройства можно классифицировать по принадлежности к трем уровням иерархической модели сети, что помогает пользователям определить, какое оборудование оптимально использовать для решения поставленной задачи в конкретном случае.

10.1. Неуправляемые коммутаторы

Неуправляемые коммутаторы *(Unmanaged Switches)* D-Link предназначены для развертывания сетей небольших рабочих групп или домашних сетей (SOHO, Small-Office-Home-Office). Также их можно использовать на уровне доступа сетей малых предприятий. Эти коммутаторы просты в установке и поддерживают (в зависимости от модели) такие функции, как Plug and Play, диагностика кабеля, управление потоком (IEEE 802.3x), автоматическое определение полярности кабелей (MDI/MDIX), возможность передачи Jumbo-фреймов и приоритизацию трафика. Технологии Green Ethernet и энергоэффективный Ethernet (IEEE 802.3az Energy-Efficient Ethernet, EEE) позволяют снизить электропотребление коммутаторов. Поддержка передачи питания через Ethernet позволяет использовать коммутаторы для питания устройств, расположенных в труднодоступных местах или при отсутствии требуемого количества электрических розеток.

Неуправляемые коммутаторы не поддерживают функции управления и обновления программного обеспечения.

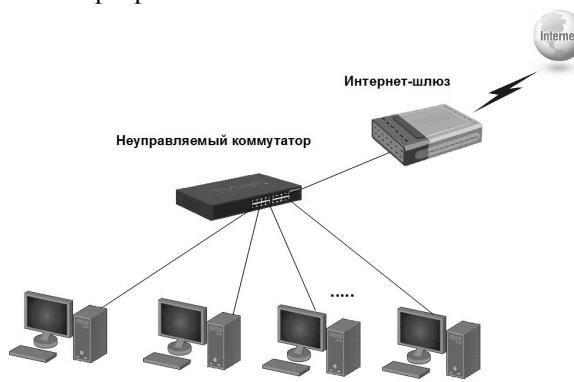


Рис. 10.1. Неуправляемые коммутаторы D-Link в сети небольшой рабочей группы

Неуправляемые коммутаторы D-Link представлены сериями DES-10xxA, DES-10xxC, DES-10xxD, DES-10xxP, DES-10xxG, DGS-10xxA, DGS-10xxC, DGS-10xxD и DGS-10xxP.

Серии **DES-10xxA**, **DES-10xxC** и **DES-10xxD** состоят из экономичных неуправляемых коммутаторов с различным количеством портов 10/100 Мбит/с (от 5 до 24) в настольном и стоечном исполнении.

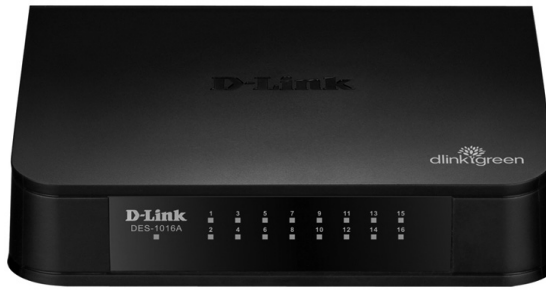


Рис. 10.2. Коммутатор DES-1016A

Серии **DGS-10xxA**, **DGS-10xxC** и **DGS-10xxD** включают в себя модели неуправляемых коммутаторов Gigabit Ethernet с различным количеством портов 10/100/1000 Мбит/с (от 5 до 24), выполненные в настольном и стоечном исполнении.

Коммутаторы DES-1005D/1008D, DES-1016A, DES-1005P, DGS-1005D/1008D, DGS-1005A/1008A, DGS-1008P поддерживают стандарт IEEE 802.1p и четыре аппаратных очереди приоритетов на каждом физическом порте.

Коммутаторы DES-1026G/1050G, DES-1018P/1018MP оборудованы двумя комбо-портами 1000BASE-T/SFP, что обеспечивает гибкость при подключении к магистрали сети.

В неуправляемых коммутаторах DES-1005P, DES-1018P, DES-1018MP и DGS-1008P поддерживается передача питания через медные порты Ethernet по стандарту IEEE 802.3af, в коммутаторе DES-1008P+ – по стандарту IEEE 802.3at-2009. Коммутатор DES-1018MP обладает повышенным энергетическим потенциалом, позволяющим осуществлять питание IP-камер с функциями поворота, ИК-подсветкой, со встроенными нагревателями и вентиляторами.

Практически все серии неуправляемых коммутаторов поддерживают энергосберегающие технологии Green Ethernet и энергоэффективный Ethernet (EEE).

Обе технологии позволяют сократить расходы на электроэнергию, при этом, не оказывая влияния на производительность и функциональность устройств. Технология EEE автоматически уменьшает потребление энергии в

Приложение

Практические занятия

Комплекс практических работ разработан для подготовки специалистов по базовому конфигурированию, администрированию и поиску неисправностей в сетях на примере оборудования (коммутаторов) компании D-Link. В состав комплекса входит 19 практических занятий. Рассматриваются следующие вопросы: первоначальная настройка коммутаторов; команды обновления конфигурации и программного обеспечения коммутаторов; организация виртуальных локальных сетей; борьба с петлеобразованием; повышение отказоустойчивости локальных сетей; агрегирование каналов передачи данных; качество предоставления сервиса; безопасность сетей, ограничение доступа к сети на основе списков управления доступом и команд безопасности портов; управление сетью; поиск неисправностей в коммутируемых сетях. Каждое практическое занятие предваряется кратким теоретическим материалом. Все занятия представлены в оригинальной табличной форме, отражающей цель действия и способ ее достижения.

Список практических занятий

Занятие №1. Основные команды коммутаторов. Управление коммутаторами.

Занятие №2. Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов.

Занятие №3. Команды управления таблицами MAC, IP, ARP.

Занятие №4. Команды VLAN на основе портов и стандарта IEEE 802.1Q.

Занятие №5. Команды протокола GVRP (продвижение информации о VLAN в сети).

Занятие №6. Команды настройки асимметричных VLAN и сегментации трафика.

Занятие №7. Команды настройки функции Q-in-Q (Double VLAN).

Занятие №8. Команды настройки протоколов связующего дерева STP, RSTP, MSTP.

Занятие №9. Настройка функции предотвращения петлеобразования (LoopBack Detection).

Занятие №10. Команды агрегирования каналов.

Занятие №11. Списки управления доступом (Access Control List).

Занятие №12. Контроль над подключением узлов к портам коммутатора. Функция Port Security.

Занятие №13. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding.

Занятие №14. Ограничение административного доступа к управлению коммутатором.

Занятие №15. Команды протокола IEEE 802.1X.

Занятие №16. Управление полосой пропускания.

Занятие №17. Настройка QoS. Приоритизация трафика.

Занятие №18. Команды зеркалирования портов (Port Mirroring).

Занятие №19. Команды мониторинга состояния коммутатора.

Занятие №1. Основные команды коммутаторов. Управление коммутаторами

Коммутаторы D-Link классифицируются по возможностям управления. Существует три основных типа:

1) **неуправляемые коммутаторы** не поддерживают функции настройки и управления, имеют уже предустановленную функциональность. Данные коммутаторы применяются там, где характеристики, необходимые в сети, стандартные и не требуют дополнительных настроек. Обычно это сети класса SOHO (Small Office Home Office);
2) **настраиваемые коммутаторы** позволяют настраивать определенные параметры сети, используя Web-интерфейс или компактный интерфейс командной строки (Compact Command Line Interface, CLI), доступный через Telnet. Применяются на уровне доступа сетей малых и средних предприятий (Small-to-Medium Business, SMB), в бюджетных решениях сетей провайдеров услуг. Отличаются невысокой стоимостью, простотой настроек и интуитивно понятным интерфейсом;
3) **управляемые коммутаторы** являются сложными устройствами, поддерживающими расширенный набор функций 2 и 3 уровня модели OSI. Такие устройства предоставляют большой выбор интерфейсов, обладают высокоскоростной внутренней магистралью, возможностью установки дополнительных модулей и физического стекирования. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протокола SNMP, сетевых консолей Telnet, SSH и т.д. Область применения данных коммутаторов – сети провайдеров услуг, корпоративные сети средних и крупных предприятий и др.

Для настройки различных функций коммутаторов при выполнении практических заданий будет использоваться интерфейс командной строки, так как он наиболее удобен для использования подготовленными администраторами и обеспечивает более тонкую настройку устройства.

Цель: Ознакомиться с основными командами настройки, контроля и устранения неполадок коммутаторов D-Link.

Оборудование:

DES-3200-28	1 шт.
Рабочая станция	1 шт.
Консольный кабель	1 шт.

Схема 1:

1. Настройка DES-3200-28

1.1. Вызов помощи по командам

Внимание! При написании команд в CLI важно учитывать регистр. Для получения информации о правильности написания команд и последовательности выполнения операций можно обращаться к встроенной помощи по командам!

Напишите в консоли (просмотр списка всех команд коммутатора)	*?*
Напишите в консоли (просмотр списка команд конфигурирования)	*config ?*
Напишите в консоли (вывод команд просмотра настроек коммутатора)	*show ?*

1.2. Изменение IP-адреса интерфейса управления коммутатора

IP-адрес интерфейса управления коммутатора по умолчанию: 10.90.90.90/8.

Измените IP-адрес интерфейса управления коммутатора	*config ipif System ipaddress 10.1.1.10/8*
Настройте IP-адрес шлюза по умолчанию	*create iproute default 10.1.1.254*

Занятие №2. Команды обновления программного обеспечения коммутатора и сохранения/ восстановления конфигурационных файлов

Обновление программного обеспечения (его иногда называют «прошивкой» коммутатора) может быть необходимо, когда доступна новая функциональность или требуется коррекция ошибок. Сохранять конфигурацию коммутатора необходимо при изменении его настроек, а также для упрощения восстановления функционирования коммутатора в результате сбоя его работы или поломки. Основным протоколом, применяемым для этих целей, служит протокол TFTP (Trivial File Transfer Protocol, простейший протокол передачи данных). Для передачи/загрузки программного обеспечения/конфигурации необходимо наличие в сети TFTP-сервера. Коммутаторы D-Link поддерживают возможность хранения на коммутаторе двух версий программного обеспечения и конфигурации, причем любая из них может быть настроена в качестве основной, т.е. используемой при загрузке коммутатора. Это позволяет обеспечить отказоустойчивость оборудования при переходе на новое программное обеспечение или изменении конфигурации. Для анализа работы коммутатора имеется возможность выгрузки через протокол TFTP Log-файла.

Цель: Изучить процесс обновления программного обеспечения и сохранения/восстановления конфигурации.

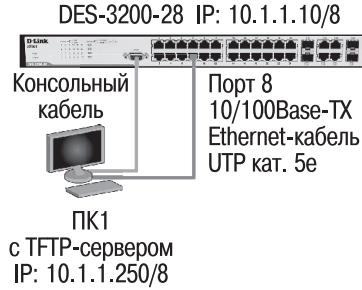
Оборудование:

DES-3200-28	1 шт.
Рабочая станция (с TFTP-сервером)	1 шт.
Консольный кабель	1 шт.
Кабель Ethernet	1 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

Схема 1:



1. Настройка DES-3200-28

1.1. Подготовка к режиму обновления и сохранения программного обеспечения коммутатора

Настройте TFTP-сервер (на примере Tftpd32 by Ph.Jounin)	*1. В настройках необходимо установить директорию приема файлов.* *2. Отключить все другие сервисы, кроме TFTP server.*
Подготовьте файл программного обеспечения	*1. Найдите необходимый файл «прошивки» на сайте* ftp://ftp.dlink.ru. *2. Скачайте файл и перенесите его в указанную директорию TFTP-сервера.* *3. Прочитайте файл сопровождения к «прошивке».*

1.2. Загрузка файла программного обеспечения в память коммутатора

Настройте IP-адрес интерфейса управления коммутатора	*config ipif System ipaddress 10.1.1.10/8*
Настройте TFTP-сервер	*Задать IP-адрес рабочей станции с установленным TFTP-сервером: 10.1.1.250/8*
Проверьте доступность соединения с TFTP-сервером	*ping 10.1.1.250*

Занятие №3. Команды управления таблицами MAC, IP, ARP

При эксплуатации активного сетевого оборудования сетевые администраторы вынуждены тратить до 70% своего времени (особенно в больших корпоративных сетях и сетях провайдеров) на изменение конфигурации активного оборудования вследствие изменения месторасположения рабочих мест пользователей, миграции пользователей между отделами и т.п. Для этого администратору необходимо максимально быстро определить порт подключения клиентского оборудования на основе MAC- и IP-адресов и перевести его в нужную VLAN и IP-подсеть. Таким образом, администратору необходимо уметь управлять таблицами продвижения пакетов и ARP-таблицами.

Цель: Изучить процесс управления таблицами MAC, IP и ARP.

Оборудование:

DES-3200-28	1 шт.
DGS-3612G	1 шт.
Рабочая станция	1 шт.
Кабель Ethernet	1 шт.
Консольный кабель	2 шт.

Схема 1:

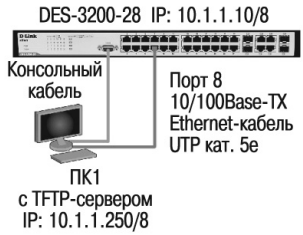
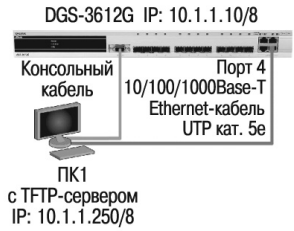


Схема 2:



1. Настройка DES-3200-28

1.1. Изучение команд просмотра таблиц MAC-адресов

Посмотрите таблицу MAC-адресов	*show fdb*
Найдите порт коммутатора, к которому подключено устройство с определенным MAC-адресом (например, 00-14-85-F2-D7-BE)	*show fdb mac_address 00-14-85-F2-D7-BE*

Внимание! Замените указанные в командах MAC-адреса на реальные.

Посмотрите список MAC-адресов устройств, принадлежащих VLAN по умолчанию	*show fdb vlan default*
Посмотрите MAC-адреса устройств, изученные портом 8	*show fdb port 8*
Посмотрите время нахождения записи в таблице MAC-адресов	*show fdb aging_time*

1.2. Изучение команд управления таблицей MAC-адресов

Создайте статическую запись в таблице MAC-адресов	*create fdb default 00-00-00-00-01-02 port 5*
Удалите статическую запись из таблицы MAC-адресов	*delete fdb default 00-00-00-00-01-02*
Измените время нахождения MAC-адреса в таблице до 350 секунд	*config fdb aging_time 350*
Удалите все динамически созданные записи из таблицы MAC-адресов	*clear fdb all*

2. Настройка DGS-3612G (работа с таблицей коммутации уровня 3 (IP FDB))

Примечание. Данные команды выполняются только на коммутаторах уровня 3.

Занятие №4. Команды VLAN на основе портов и стандарта IEEE 802.1Q

Виртуальная локальная сеть (Virtual Local Area Netwrok, VLAN) представляет собой коммутируемый сегмент сети, который логически выделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического расположения пользователей. Виртуальные локальные сети имеют все свойства физических локальных сетей, но рабочие станции можно группировать, даже если они физически расположены не в одном сегменте, т.к. любой порт коммутатора можно настроить на принадлежность определенной VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть, т.е. кадры, предназначенные станциям, которые не принадлежат данной VLAN, должны передаваться через маршрутизирующее устройство (маршрутизатор или коммутатор 3-го уровня). Таким образом, с помощью виртуальных локальных сетей решается проблема ограничения области передачи широковещательных кадров и вызываемых ими следствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Типы VLAN:

- *VLAN на основе портов (Port-based VLAN)* – 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 VLAN)* – членство в VLAN основывается на MAC-адресе рабочей станции. В этом случае на коммутаторе необходимо создать привязку MAC-адресов всех устройств к VLAN;
- *VLAN на основе портов и протоколов IEEE 802.1v* – тип протокола используется для определения членства в VLAN;
- *VLAN на основе стандарта IEEE 802.1Q* – поле принадлежности VLAN, интегрируется в структуру кадра Ethernet, 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 использования оборудования разных производителей при организации сети. Данный тип VLAN используется чаще остальных.

Существуют два метода назначения порта в определенную VLAN:

- статическое назначение – когда принадлежность порта VLAN задается 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 IEEE 802.1X. При использовании IEEE 802.1X для получения доступа к порту коммутатора пользователь проходит аутентификацию на сервере RADIUS. По результатам аутентификации порт коммутатора помещается в ту или иную VLAN.

Основные определения IEEE 802.1Q:

- *Tag* («Тег») – дополнительное поле данных длиной 4 байта, содержащее информацию о VLAN и добавляемое в кадр Ethernet. Первые 2 байта содержат фиксированное значение 0x8100, остальные 2 байта содержат идентификатор VLAN (12 бит), поле приоритета (3 бита), поле индикатора канонического формата (1 бит);
- *Tagging* («Маркировка кадра») – процесс добавления информации (тега) о принадлежности к 802.1Q VLAN в заголовок кадра;
- *Untagging* («Удаление тега из кадра») – процесс извлечения информации 802.1Q VLAN из заголовка кадра;
- *Ingress port* («Входной порт») – порт коммутатора, на который поступают кадры, и принимается решение о принадлежности 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* (маркированный) или как *untagged* (немаркированный). Функция *untagging* позволяет работать с теми сетевыми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать VLAN между несколькими коммутаторами, поддерживающими стандарт IEEE 802.1Q, подключать сетевые устройства, понимающие IEEE 802.1Q (например, серверы с сетевыми интерфейсами с поддержкой 802.1Q), обеспечивать возможность создания сложных сетевых инфраструктур.

В данной лабораторной работе рассматриваются примеры использования и настройки VLAN.

Цель: Понять технологию VLAN и ее настройку на коммутаторах D-Link.

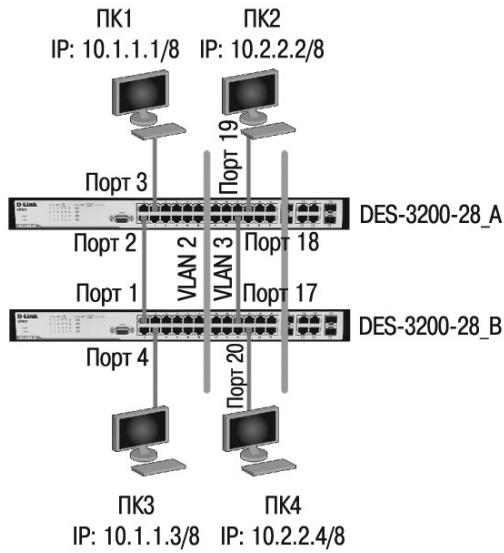
Оборудование:

DES-3200-28	2 шт.
Рабочая станция	8 шт.
Кабель Ethernet	10 шт.
Консольный кабель	2 шт.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой
reset config

1. Настройка VLAN на основе портов

Схема 1:



1.1. Настройка DES-3200-28_A

Удалите порты из VLAN по умолчанию *config vlan default delete 1-24*
для использования в других VLAN

Занятие №5. Команды протокола GVRP (продвижение информации о VLAN в сети)

Существуют два основных способа, позволяющих устанавливать членство в VLAN:

- статические VLAN;
- динамические VLAN.

В статических VLAN установление членства осуществляется вручную администратором сети. При изменении топологии сети или перемещении пользователя на другое рабочее место администратору требуется вручную выполнять привязку порт-VLAN для каждого нового соединения.

Членство в динамических VLAN может устанавливаться динамически на основе протокола GVRP (GARP VLAN Registration Protocol).

Порт с поддержкой протокола GVRP подключается к сети VLAN только в том случае, если он непосредственно получает оповещение о ней. Если порт с поддержкой протокола GVPR передает оповещение, полученное от другого порта коммутатора, он не подключается к этой сети VLAN.

Главная цель протокола GVRP – позволить коммутаторам автоматически обнаруживать информацию о VLAN, которая иначе должна была бы быть вручную сконфигурирована на каждом коммутаторе. Наиболее рационально использовать протокол GVRP на магистральных коммутаторах для динамической передачи информации о статических VLAN на уровень доступа.

Цель: Изучить процесс динамического продвижения информации о VLAN в сети.

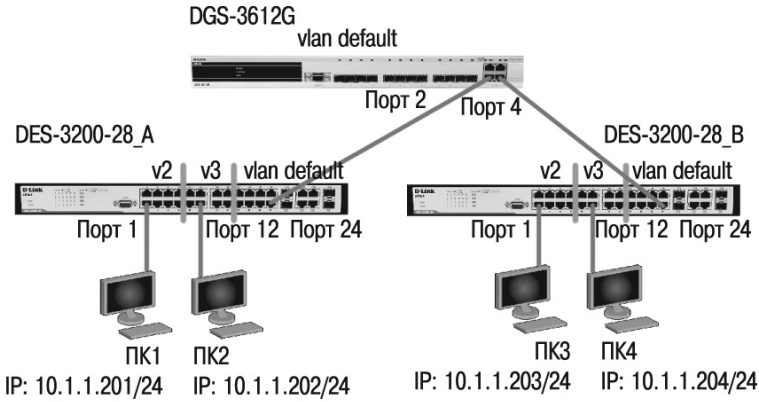
Оборудование:

DGS-3612G	1 шт.
DES-3200-28	3 шт.
Рабочая станция	4 шт.
Кабель Ethernet	6 шт.
Консольный кабель	4 шт.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой

reset config

Схема 1:



1. Настройка VLAN

1.1. Настройка DES-3200-28_A и DES- 3200-28_B

Удалите порты из VLAN по умолчанию для использования в других VLAN	*config vlan default delete 1-16*
Создайте VLAN v2, добавьте в нее порты, которые необходимо настроить немаркированными. Настройте порт 24 маркированным	*create vlan v2 tag 2* *config vlan v2 add untagged 1-8* *config vlan v2 add tag 24*
Создайте VLAN v3, добавьте в нее порты, которые необходимо настроить немаркированными. Настройте порт 24 маркированным	*create vlan v3 tag 3* *config vlan v3 add untagged 9-16* *config vlan v3 add tag 24*
Настройте оповещение о VLAN v2 и v3	*config vlan v2 advertisement enable* *config vlan v3 advertisement enable*
Включите работу протокола GVRP	*enable gvrp*
Установите возможность приема и отправки информации о VLAN через порт 24 коммутатора	*config port_vlan 24 gvrp_state enable*

Занятие №6. Команды настройки асимметричных VLAN и сегментации трафика

Применение асимметричных VLAN (Asymmetric VLAN)

Для обеспечения возможности использования разделяемых ресурсов (серверов, Интернет-шлюзов и т.д.) пользователями из разных сетей VLAN в программном обеспечении коммутаторов **2-го уровня** D-Link реализована поддержка функции *Asymmetric VLAN* (ассиметричные VLAN). Эта функция позволяет клиентам из разных VLAN взаимодействовать с разделяемыми устройствами (например, серверами), *не поддерживающим* тегирование *802.1Q,* через один физический канал связи с коммутатором, не требуя использования внешнего маршрутизатора. Активизация функции Asymmetric VLAN на коммутаторе 2-го уровня позволяет сделать его *немаркированные* порты *членами нескольких виртуальных локальных сетей*. При этом рабочие станции остаются полностью изолированными друг от друга.

При активизации асимметричных VLAN каждому порту коммутатора назначается уникальный PVID в соответствии с идентификатором VLAN, членом которой он является. При этом каждый порт может получать кадры от VLAN по умолчанию.

Применение сегментации трафика (Traffic Segmentation)

Функция Traffic Segmentation служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов или магистрали сети. Функция сегментации трафика может использоваться с целью сокращения трафика внутри сетей VLAN 802.1Q, позволяя разбивать их на более мелкие группы. При этом правила VLAN имеют более высокий приоритет при передаче трафика. Правила Traffic Segmentation применяются после них.

Цель: Изучить настройку асимметричных VLAN и сегментации трафика.

Оборудование:

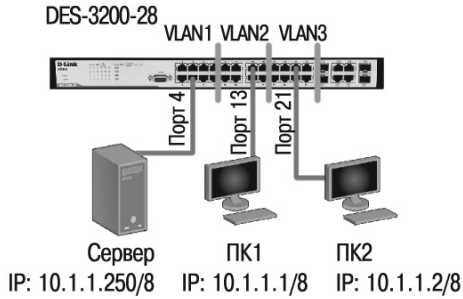
DES-3200-28	2 шт.
Рабочая станция	4 шт.
Кабель Ethernet	5 шт.
Консольный кабель	2 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

1. Настройка асимметричных VLAN (пример 1)

Схема 1:



1.1. Настройка DES-3200-28

Внимание! Коммутаторы уровня 3 (например, DGS-3612G) не поддерживают функцию асимметричных VLAN! Аналогичные функции выполняются с помощью маршрутизации и ACL (списков управления доступом).

Включите функцию асимметричных VLAN	*enable asymmetric_vlan*
Проверьте, все ли порты назначены в VLAN по умолчанию?	*show vlan*
Создайте VLAN v2 и v3	*create vlan v2 tag 2* *create vlan v3 tag 3*
Добавьте в созданные VLAN немаркированные порты	*config vlan v2 add untagged 1-16* *config vlan v3 add untagged 1-8, 17-24*
Назначьте PVID немаркированным портам, созданных VLAN	*config gvrp 1-8 pvid 1* *config gvrp 9-16 pvid 2* *config gvrp 17-24 pvid 3*

Занятие №7. Команды настройки функции Q-in-Q (Double VLAN)

Функция Q-in-Q, также известная как Double VLAN, соответствует стандарту IEEE 802.1ad, который является расширением стандарта IEEE 802.1Q. Она позволяет добавлять в маркированные кадры Ethernet второй тег IEEE 802.1Q.

Благодаря функции Q-in-Q провайдеры могут использовать их собственные уникальные идентификаторы VLAN (называемые Service Provider VLAN ID, или *SP-VLAN ID*) при оказании услуг пользователям, в сетях которых настроено несколько VLAN. Это позволяет сохранить используемые пользователями идентификаторы VLAN (Customer VLAN ID, или *CVLAN ID*), избежать их совпадения и изолировать трафик разных клиентов во внутренней сети провайдера.

Инкапсуляция кадра Ethernet вторым тегом происходит следующим образом: тег, содержащий идентификатор VLAN сети провайдера SP-VLAN ID (*внешний тег*), вставляется перед *внутренним тегом*, содержащим клиентский идентификатор VLAN – CVLAN ID. Передача кадров в сети провайдера осуществляется только на основе внешнего тега SP-VLAN ID, внутренний тег пользовательской сети CVLAN ID при этом скрыт.

Существует две реализации функции Q-in-Q: *Port-based Q-in-Q* и *Selective Q-in-Q*. Функция *Port-based Q-in-Q* по умолчанию присваивает любому кадру, поступившему на порт доступа граничного коммутатора провайдера, идентификатор *SP-VLAN* равный идентификатору PVID порта. Порт маркирует кадр независимо от того, является он маркированным или немаркированным. При поступлении маркированного кадра в него добавляется второй тег с идентификатором, равным *SP-VLAN*. Если на порт пришел немаркированный кадр, в него добавляется только тег с *SP-VLAN* порта.

Роли портов в Port-based Q-in-Q

Все порты граничного коммутатора, на котором используется функция Port-based Q-in-Q, должны быть настроены как *порты доступа* (*UNI*) или *Uplink-порты* (*NNI*).

UNI-порт предназначен для подключения к граничному коммутатору клиентских сетей VLAN. NNI-порт используется для подключения граничного коммутатора к сети провайдера услуг.

Цель: Изучить настройку функции Port-based Q-in-Q.

Оборудование:

DGS-3612G	2 шт.
Трансивер SFP DEM-311GT	2 шт.
DES-3200-28	4 шт.
Рабочая станция	4 шт.
Кабель Ethernet	8 шт.
Многомодовый оптический кабель	1 шт.
Консольный кабель	6 шт.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой

reset config

Настройка функции Port-based Q-in-Q

1. Настройка DES-3200-28_1 (остальные коммутаторы данной серии настраиваются аналогично)

Удалите порты из VLAN по умолчанию для использования в других VLAN	*config vlan default delete 1-24*
Создайте VLAN v2, v3, v4	*create vlan v2 tag 2* *create vlan v3 tag 3* *create vlan v4 tag 4*
Добавьте в VLAN v2 порты 1-8 как немаркированные	*config vlan v2 add untagged 1-8*
Добавьте в VLAN v3 порты 9-16 как немаркированные	*config vlan v3 add untagged 9-16*
Добавьте в VLAN v4 порты 17-24 как немаркированные	*config vlan v4 add untagged 17-24*
Добавьте магистральные порты 25 и 26 как маркированные в VLAN v2, v3, v4	*config vlan v2 add tagged 25-26* *config vlan v3 add tagged 25-26* *config vlan v4 add tagged 25-26*

Занятие №8. Команды настройки протоколов связующего дерева STP, RSTP, MSTP

Протокол Spanning Tree Protocol (STP).

Протокол связующего дерева Spanning Tree Protocol (STP) является протоколом 2 уровня модели OSI, который позволяет строить древовидные, свободные от петель конфигурации связей между коммутаторами локальной сети.

Конфигурация связующего дерева строится коммутаторами автоматически с использованием обмена служебными кадрами, называемыми Bridge Protocol Data Units (BPDU). Существует три типа кадров BPDU:

- Configuration BPDU (CBPDU) – конфигурационный кадр BPDU, который используется для вычисления связующего дерева (тип сообщения: 0x00);
- Topology Change Notification (TCN) BPDU – уведомление об изменении топологии сети (тип сообщения: 0x80);
- Topology Change Notification Acknowledgement (TCA) – подтверждение о получении уведомления об изменении топологии сети.

Для построения устойчивой активной топологии с помощью протокола STP необходимо с каждым коммутатором сети ассоциировать уникальный идентификатор моста (Bridge ID), с каждым портом коммутатора ассоциировать стоимость пути (Path Cost) и идентификатор порта (Port ID).

Процесс вычисления связующего дерева начинается с выбора корневого моста (Root Bridge), от которого будет строиться дерево. Второй этап работы STP – выбор корневых портов (Root Port). Третий шаг работы STP – определение назначенных портов (Designated Port).

В процессе построения топологии сети каждый порт коммутатора проходит несколько стадий: Blocking («Блокировка»), Listening («Прослушивание»), Learning («Обучение»), Forwarding («Продвижение»), Disable («Отключен»).

Протокол Rapid Spanning Tree Protocol (RSTP).

Протокол Rapid Spanning Tree Protocol (RSTP) является развитием протокола STP. Основные понятия и терминология протоколов STP и RSTP одинаковы. Существенным их отличием является способ перехода портов в состояние продвижения и то, каким образом этот переход влияет на роль порта в топологии. RSTP объединяет состояния Disabled, Blocking и Listening, используемые в STP, и создает единственное состояние Discarding («Отбрасывание»), при котором порт не активен. Выбор активной топологии завершается присвоением протоколом RSTP опреде-

ленной роли каждому порту: корневой порт (Root Port), назначенный порт (Designated Port), альтернативный порт (Alternate Port), резервный порт (Backup Port).

Протокол RSTP предоставляет механизм предложений и соглашений, который обеспечивает быстрый переход корневых и назначенных портов в состояние Forwarding, а альтернативных и резервных портов в состояние Discarding. Для этого протокол RSTP вводит два новых понятия: граничный порт и тип соединения. Граничным портом (Edge Port) объявляется порт, непосредственно подключенный к сегменту сети, в котором не могут быть созданы петли. Граничный порт мгновенно переходит в состояние продвижения, минуя состояния прослушивания и обучения. Назначенный порт может выполнять быстрый переход в состояние продвижения в соединениях типа «точка – точка» (*Point-to-Point, P2P*), т.е. если он подключен только к одному коммутатору.

Администратор сети может вручную включать или выключать статусы Edge и P2P либо устанавливать их работу в автоматическом режиме, выполнив соответствующие настройки порта коммутатора.

Протокол Multiple Spanning Tree Protocol (MSTP).

Протокол Multiple Spanning Tree Protocol (MSTP) является расширением протокола RSTP, который позволяет настраивать отдельное связующее дерево для любой VLAN или группы VLAN, создавая множество маршрутов передачи трафика и позволяя осуществлять балансировку нагрузки.

Протокол MSTP делит коммутируемую сеть на **регионы MST** (*Multiple Spanning Tree (MST) Region*), каждый из которых может содержать множество **копий связующих деревьев** (*Multiple Spanning Tree Instance, MSTI*) с независимой друг от друга топологией.

Для того чтобы два и более коммутатора принадлежали одному региону MST, они должны обладать одинаковой конфигурацией MST, которая включает: номер ревизии MSTP (*MSTP revision level number*), имя региона (*Region name*), карту привязки VLAN к копии связующего дерева (*VLAN-to-instance mapping*).

Внутри коммутируемой сети может быть создано множество MST-регионов.

Протокол MSTP определяет следующие типы связующих деревьев:

- **Internal Spanning Tree (IST)** – специальная копия связующего дерева, которая по умолчанию существует в каждом MST-регионе. IST присвоен номер 0 (Instance 0). Она может отправлять и получать кадры BPDU и служит для управления топологией внутри региона. Все VLAN, настроенные на коммутаторах данного MST-региона, по умолчанию привязаны к IST;

- **Common Spanning Tree (CST)** – единое связующее дерево, вычисленное с использованием протоколов STP, RSTP, MSTP и объединяющее все регионы MST и мосты SST;
- **Common and Internal Spanning Tree (CIST)** – единое связующее дерево, объединяющее CST и IST каждого MST-региона;
- **Single Spanning Tree (SST) Bridge** – это мост, поддерживающий только единственное связующее дерево, CST. Это единственное связующее дерево может поддерживать протокол STP или протокол RSTP.

Вычисления в MSTP

Процесс вычисления MSTP начинается с выбора **корневого моста CIST** (*CIST Root*) сети. В качестве CIST Root будет выбран коммутатор, обладающий наименьшим значением идентификатора моста среди всех коммутаторов сети.

Далее в каждом регионе выбирается **региональный корневой мост CIST** (*CIST Region Root*). Им становится коммутатор, обладающий наименьшей внешней стоимостью пути к корню CIST среди всех коммутаторов, принадлежащих данному региону.

При наличии в регионе отдельных связующих деревьев MSTI для каждой MSTI, независимо от остальных, выбирается **региональный корневой мост MSTI** (*MSTI Regional Root*). Им становится коммутатор, обладающий наименьшим значением идентификатора моста среди всех коммутаторов данной MSTI этого MST-региона.

При вычислении активной топологии CIST и MSTI используется тот же фундаментальный алгоритм, который описан в стандарте IEEE 802.1D-2004.

Роли портов

Протокол MSTP определяет роли портов, которые участвуют в процессе вычисления активной топологии CIST и MSTI аналогичные протоколам STP и RSTP. Дополнительно в MSTI используется еще роль – мастер-порт (*Master Port*).

Счетчик переходов MSTP

При вычислении активной топологии связующего дерева IST и MSTI не используют значения полей Max Age и Message Age конфигурационного BPDU для отбрасывания устаревших сообщений. Вместо этого используется механизм счетчика переходов (Hop count).

С помощью команды **config stp maxhops** на коммутаторах D-Link можно настроить максимальное число переходов между устройствами внутри региона, прежде чем кадр BPDU будет отброшен. Значение счет-

чика переходов устанавливается региональным корневым мостом MSTI или CIST и уменьшается на 1 каждым портом коммутатора, получившим кадр BPDU. После того как значение счетчика станет равным 0, кадр BPDU будет отброшен и информация, хранимая портом, будет помечена как устаревшая.

Пользователь может установить значение счетчика переходов от 1 до 20. Значение по умолчанию – 20.

В данной лабораторной работе рассматривается работа протоколов связующего дерева и их настройка на коммутаторах.

Цель: Понять функционирование протоколов связующего дерева и изучить их настройку на коммутаторах D-Link.

Оборудование:

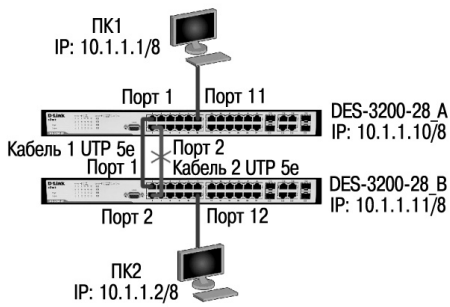
DES-3200-28	2 шт.
Рабочая станция	4 шт.
Кабель Ethernet	8 шт.
Консольный кабель	2 шт.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой

reset config

1. Настройка протокола RSTP (IEEE 802.1w)

Схема 1:



Примечание. Не соединяйте кабелем Ethernet порты коммутатора с образованием петли во время настройки.

Занятие №9. Функция предотвращения петлеобразования (LoopBack Detection)

Функция LoopBack Detection (LBD) обеспечивает дополнительную защиту от образования петель на уровне 2 модели OSI. Существует две реализации этой функции:

- STP LoopBack Detection;
- LoopBack Detection Independent STP.

Коммутатор, на котором настроена функция STP LoopBack Detection, определяет наличие петли, когда отправленный им кадр BPDU вернулся назад на другой его порт. В этом случае порт-источник кадра BPDU и порт-приемник будут автоматически заблокированы и администратору сети будет отправлен служебный пакет-уведомление. Порты будут находиться в заблокированном состоянии до истечения времени, установленного таймером LBD Recover Timer.

Функция LoopBack Detection Independent STP не требует настройки протокола STP на портах, на которых необходимо определять наличие петли. В этом случае наличие петли обнаруживается путем отправки портом специального служебного кадра ECTP (Ethernet Configuration Testing Protocol). При получении кадра ECTP этим же портом он блокируется на указанное в таймере время. Начиная с LBD версии 4.03, функция LoopBack Detection Independent STP также может определять петли, возникающие между портами одного коммутатора. Существуют два режима работы этой функции: Port-Based и VLAN-Based (начиная с LBD версии v.4.00).

В режиме Port-Based при обнаружении петли происходит автоматическая блокировка порта и никакой трафик через него не передается.

В режиме VLAN-Based порт будет заблокирован для передачи трафика только той VLAN, в которой обнаружена петля. Остальной трафик через этот порт будет передаваться.

На данном занятии изучается работа функции LoopBack Detection Independent STP в режимах Port-Based и VLAN-Based.

Цель: Понять способы работы LBD-алгоритма в различных режимах функционирования.

Оборудование:

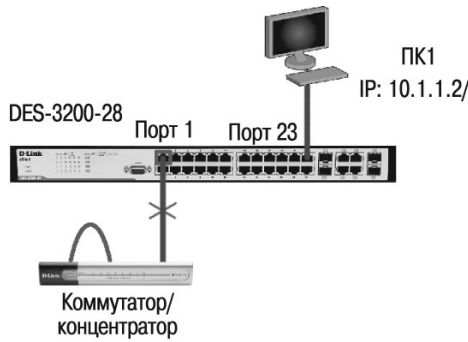
DES-3200-28	2 шт.
DES-1005A	1 шт.
Рабочая станция	4 шт.
Кабель Ethernet	7 шт.
Консольный кабель	2 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

1. Настройка LoopBack Detection Independent STP в режиме Port-Based

Схема 1:



1.1. Настройка DES-3200-28

В данном задании рассматривается блокирование порта управляемого коммутатора при обнаружении петли в подключенном сегменте.

Включите функцию LBD глобально на коммутаторе	*enable loopdetect*
Активизируйте функцию LBD на всех портах коммутатора	*config loopdetect ports 1-28 state enabled*
Сконфигурируйте режим Port-Based, чтобы при обнаружении петли отключался порт	*config loopdetect mode port-based*

Внимание! При блокировании порта трафик не будет передаваться ни из одной VLAN.

Занятие №10. Команды агрегирования каналов

Агрегирование каналов связи (Link Aggregation) – это объединение нескольких физических портов в одну логическую магистраль на канальном уровне модели OSI с целью образования высокоскоростного канала передачи данных и повышения отказоустойчивости.

Все избыточные связи в одном агрегированном канале остаются в рабочем состоянии, а имеющийся трафик распределяется между ними для достижения балансировки нагрузки. При отказе одной из линий, входящих в такой логический канал, трафик распределяется между оставшимися линиями.

Включенные в агрегированный канал порты называются членами группы агрегирования (Link Aggregation Group). Один из портов в группе выступает в качестве мастера-порта (master port). Так как все порты агрегированной группы должны работать в одном режиме, конфигурация мастера-порта распространяется на все порты в группе.

Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Выбор порта для конкретного сеанса выполняется на основе выбранного алгоритма агрегирования портов, т.е. на основании некоторых признаков поступающих пакетов. В коммутаторах D-Link поддерживается 9 алгоритмов агрегирования портов:

1) mac_source – MAC-адрес источника;
2) mac_destination – MAC-адрес назначения;
3) mac_source_dest – MAC-адрес источника и назначения;
4) ip_source – IP-адрес источника;
5) ip_destination – IP-адрес назначения;
6) ip_source_dest – IP-адрес источника и назначения;
7) l4_src_port – TCP/UDP-порт источника;
8) l4_dest_port – TCP/UDP-порт назначения;
9) l4_src_dest_port – TCP/UDP-порт источника и назначения.

В коммутаторах D-Link по умолчанию используется алгоритм mac_source (MAC-адрес источника).

Программное обеспечение коммутаторов D-Link поддерживает два типа агрегирования каналов связи: статическое и динамическое, на основе стандарта IEEE 802.3ad (LACP).

При статическом агрегировании каналов (установлено по умолчанию) все настройки на коммутаторах выполняются вручную, и они не допускают динамических изменений в агрегированной группе.

Для организации динамического агрегирования используется протокол управления агрегированным каналом – Link Aggregation Control Protocol (LACP). Протокол LACP определяет метод управления объеди-

нением нескольких физических портов в одну логическую группу и предоставляет сетевым устройствам возможность автосогласования каналов путем отправки управляющих кадров протокола LACP непосредственно подключенным устройствам с поддержкой LACP. Порты, на которых активизирован протокол LACP, могут быть настроены для работы в одном из двух режимов: активном (active) или пассивном (passive). При работе в активном режиме порты выполняют обработку и рассылку управляющих кадров протокола LACP. При работе в пассивном режиме порты выполняют только обработку управляющих кадров LACP.

Для того чтобы динамический канал обладал функцией автосогласования, рекомендуется порты, входящие в агрегированную группу, с одной стороны канала настраивать как активные, а с другой – как пассивные.

Цель: Изучить настройку статического и динамического агрегирования каналов на коммутаторах D-Link.

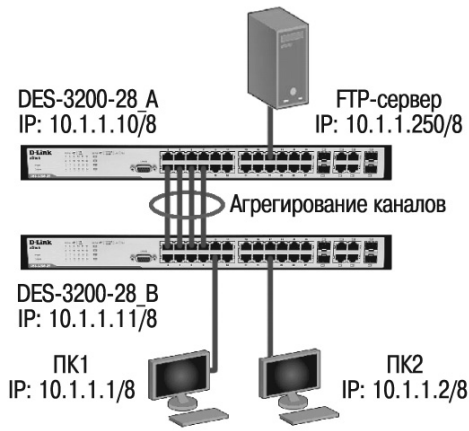
Оборудование:

DES-3200-28	3 шт.
Рабочая станция	5 шт.
Кабель Ethernet	9 шт.
Консольный кабель	3 шт.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой

reset config

Схема 1:



Занятие №11. Списки управления доступом (Access Control List)

Списки управления доступом (Access Control List, ACL) являются средством фильтрации потоков данных. Фильтруя потоки данных, администратор может ограничить типы приложений, разрешенных для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS путем классификации трафика и переопределения его приоритета.

ACL представляют собой последовательность условий проверки параметров пакетов данных. Когда сообщения поступают на входной интерфейс, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определенными в ACL, и выполняет над пакетами одно из действий: Permit («Разрешить») или Deny («Запретить»).

Списки управления доступом состоят из профилей доступа (Access Profile) и правил (Rule). Профили доступа определяют типы критериев фильтрации, которые должны проверяться в пакете данных (MAC-адрес, IP-адрес, номер порта, VLAN и т.д.), а в правилах указываются непосредственные значения их параметров. Каждый профиль может состоять из множества правил.

В коммутаторах D-Link существует три типа профилей доступа: Ethernet, IP и Packet Content Filtering (фильтрация по содержимому пакета).

Защита коммутатора от атак на блок управления (функция CPU Interface Filtering)

Некоторые кадры, полученные коммутатором, направляются на обработку в ЦПУ (CPU), при этом такие кадры не могут быть отфильтрованы аппаратными ACL. Например, кадр, в котором MAC-адрес назначения, – это MAC-адрес коммутатора (в случае тестирования соединения командой ping с указанием IP-адреса интерфейса управления коммутатора).

Для решения задач блокировки трафика, отправляемого для обработки на CPU, используется функция CPU Interface Filtering (программные ACL). В задании 3 рассматривается пример блокировки трафика, отправляемого для обработки на центральный процессор.

Цель: На коммутаторе D-Link настроить списки управления доступом, в качестве критериев фильтрации используются MAC- и IP-адреса.

Оборудование:

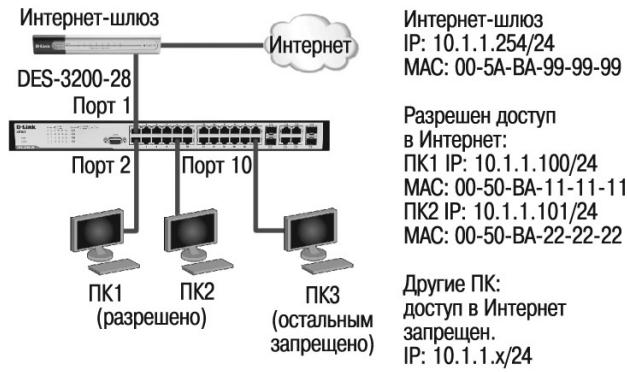
DES-3200-28	1 шт.
Рабочая станция	3 шт.
Кабель Ethernet	5 шт.
Консольный кабель	1 шт.
Интернет-шлюз	1 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

1. Настройка ограничения доступа пользователей в Интернет по MAC-адресу

Схема 1:



Задача: пользователям ПК1 и ПК2 разрешен доступ в Интернет, остальным пользователям – запрещен. Пользователи идентифицируются по MAC-адресам их компьютеров.

Правила:

Правило 1:

Если MAC-адрес назначения = MAC-адресу Интернет-шлюза и MAC-адрес источника = ПК1 – разрешить;

Если MAC-адрес назначения = MAC-адресу Интернет-шлюза и MAC-адрес источника = ПК2 – разрешить;

Правило 2:

Если MAC-адрес назначения = MAC-адресу Интернет-шлюза – запретить;

Занятие №12. Контроль над подключением узлов к портам коммутатора. Функция Port Security

Функция Port Security позволяет настроить какой-либо порт коммутатора так, чтобы доступ к сети через него мог осуществляться только определенными устройствами. Устройства, которым разрешено подключаться к порту, определяются по MAC-адресам. MAC-адреса могут быть изучены динамически или вручную настроены администратором сети. Помимо этого, функция Port Security позволяет ограничивать количество изучаемых портом MAC-адресов, тем самым ограничивая количество подключаемых к нему узлов.

Существует три режима работы функции Port Security:

- *Permanent* («Постоянный») – занесенные в таблицу коммутации MAC-адреса никогда не устаревают, даже если истекло время, установленное таймером Aging Time, или коммутатор был перезагружен;
- *Delete on Timeout* («Удалить по истечении времени») – занесенные в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером Aging Time, и будут удалены. Если состояние канала связи на подключенном порте изменяется, MAC-адреса, изученные на нем, удаляются из таблицы коммутации, что аналогично выполнению действий по истечении времени, установленного таймером Aging Time;
- *Delete on Reset* («Удалить при сбросе настроек») – занесенные в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

Функция Port Security оказывается весьма полезной при построении домовых сетей, сетей провайдеров Интернета и локальных сетей с повышенным требованием по безопасности, где требуется исключить доступ незарегистрированных рабочих станций к услугам сети.

Используя функцию Port Security, можно полностью запретить динамическое изучение MAC-адресов указанными или всеми портами коммутатора. В этом случае доступ к сети получат только те пользователи, MAC-адреса которых указаны в статической таблице коммутации.

Цель: Научиться управлять подключением узлов к портам коммутатора и изучить настройку функции Port Security на коммутаторах D-Link.

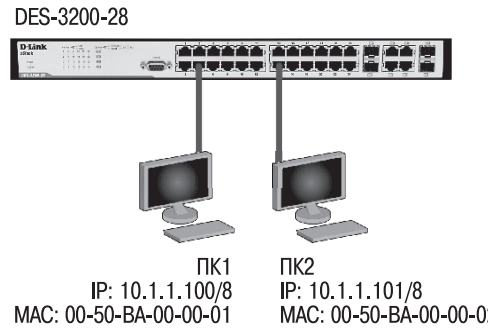
Оборудование:

DES-3200-28	1 шт.
Рабочая станция	2 шт.
Кабель Ethernet	2 шт.
Консольный кабель	1 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

Схема 1:



1. Настройка управления количеством подключаемых к портам коммутатора пользователей путем ограничения максимального количества изучаемых MAC-адресов

1.1. Настройка DES-3200-28

Установите максимальное количество изучаемых всеми портами MAC-адресов равным 1	*config port_security ports 1-28 admin_state enable max_learning_addr 1*
Подключите ПК1 и ПК2 к портам коммутатора	*В этом примере используются порты 4 и 14*
Проверьте MAC-адреса, которые стали известны портам	*show fdb port 4 show fdb port 14*

Занятие №13. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding

Функция IP-MAC-Port Binding (IMPB), реализованная в коммутаторах D-Link, позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения. Администратор сети может создать записи («белый лист»), связывающие MAC- и IP-адреса компьютеров с портами подключения коммутатора. На основе этих записей, в случае совпадения всех составляющих, клиенты будут получать доступ к сети со своих компьютеров. В том случае, если при подключении клиента, связка MAC-IP-порт будет отличаться от параметров заранее сконфигурированной записи, то коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «черный лист».

Функция IP-MAC-Port Binding включает три режима работы: ARP mode (по умолчанию), ACL mode и DHCP Snooping mode.

ARP mode является режимом, используемым по умолчанию при настройке функции IP-MAC-Port Binding на портах. При работе в режиме ARP коммутатор анализирует ARP-пакеты и сопоставляет параметры IP-MAC ARP-пакета с предустановленной администратором связкой IP-MAC. Если хотя бы один параметр не совпадает, то MAC-адрес узла будет занесен в таблицу коммутации с отметкой «Drop» («Отбрасывать»). Если все параметры совпадают, MAC-адрес узла будет занесен в таблицу коммутации с отметкой «Allow» («Разрешен»).

При функционировании в *ACL mode* коммутатор на основе предустановленного администратором «белого листа» IMPB создает правила ACL. Любой пакет, связка IP-MAC которого отсутствует в «белом листе», будет блокироваться ACL.

Режим *DHCP Snooping* используется коммутатором для динамического создания записей IP-MAC на основе анализа DHCP-пакетов и привязки их к портам с включенной функцией IMPB (администратору не требуется создавать записи вручную). Таким образом, коммутатор автоматически создает «белый лист» IMPB в таблице коммутации или аппаратной таблице ACL (если режим ACL включен). При этом для обеспечения корректной работы сервер DHCP должен быть подключен к доверенному порту с выключенной функцией IMPB. Администратор может ограничить максимальное количество создаваемых в процессе автоизучения записей IP-MAC на порт, т.е. ограничить для каждого порта с активизированной функцией IMPB количество узлов, которые могут получить IP-адрес с DHCP-сервера. При работе в режиме DHCP Snooping коммутатор не будет создавать записи IP-MAC для узлов с IP-адресом, установленным вручную.

При активизации функции IMPB на порте администратор должен указать режим его работы:

- **Strict Mode** – в этом режиме порт по умолчанию заблокирован;
- **Loose Mode** – в этом режиме порт по умолчанию открыт.

Цель: Научиться управлять подключением узлов к портам коммутатора и изучить настройку функции IP-MAC-Port Binding на коммутаторах D-Link.

Оборудование:

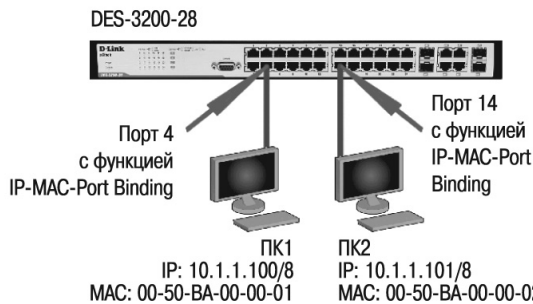
DES-3200-28	1 шт.
DES-1005A	1 шт.
Рабочая станция	3 шт.
Кабель Ethernet	4 шт.
Консольный кабель	1 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

1. Настройка работы функции IP-MAC-Port Binding в режиме ARP

Схема 1:



1.1. Настройка DES-3200-28

Внимание! Замените указанные в командах MAC-адреса на реальные.

Занятие №14. Ограничение административного доступа к управлению коммутатором

В современных сетях, особенно в сетях провайдеров услуг, необходимо осуществлять не только защиту периметра сети и ограничения передачи трафика, но и контроль над консолями управления активным оборудованием, минимизировать доступ к средствам управления, учетным административным записям коммутатора. В данной лабораторной работе рассматриваются наиболее распространенные способы защиты доступа к коммутатору и его консолей управления.

Понятия, которые используются в данной лабораторной работе:

- SSL (Secure Sockets Layer, уровень защищенных сокетов) – криптографический протокол, обеспечивающий безопасную передачу данных по сети Интернет. При его использовании создается защищенное соединение между клиентом и сервером. Использует шифрование с открытым ключом для подтверждения подлинности отправителя и получателя. Поддерживает надежность передачи данных за счет использования корректирующих кодов и безопасных хэш-функций. SSL состоит из двух уровней. На нижнем уровне многоуровневого транспортного протокола он является протоколом записи и используется для инкапсуляции различных протоколов.

Для доступа к Web-страницам, защищенным протоколом SSL, в адресной строке браузера вместо обычного префикса http, применяется префикс https, указывающий на то, что будет использоваться SSL-соединение. Стандартный TCP-порт для соединения по протоколу https – 443. Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат;

- SSH (Secure SHell, «безопасная оболочка») – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений. Сходен по функциональности с протоколом Telnet, но, в отличие от него, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы имеются для большинства сетевых операционных систем. SSH позволяет безопасно передавать в незащищенной среде практически любой другой сетевой протокол.

Цель: Изучить механизмы ограничения административного доступа к управлению коммутатором.

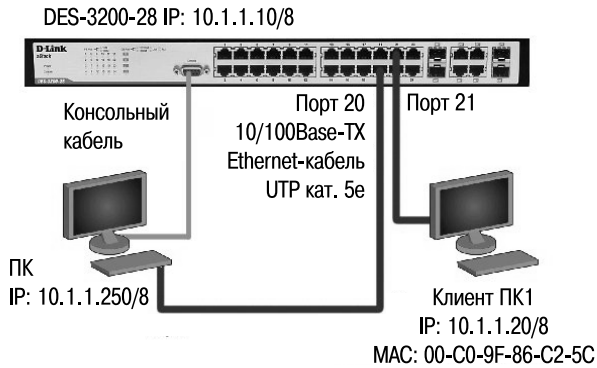
Оборудование:

DES-3200-28	1 шт.
Рабочая станция	2 шт.
Кабель Ethernet	2 шт.
Консольный кабель	1 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

Схема 1:



1. Настройка «доверенного узла» (Trusted Host) на DES-3200-28

Настройте IP-адрес интерфейса управления коммутатора	*config ipif System ipaddress 10.1.1.10/8*
Создайте доверенную рабочую станцию, с которой разрешено управление коммутатором	*create trusted_host 10.1.1.250*
Посмотрите список доверенных узлов сети	*show trusted_host*

Занятие №15. Команды протокола IEEE 802.1X

Стандарт IEEE 802.1X (IEEE Std 802.1X-2010) описывает использование протокола EAP (Extensible Authentication Protocol) для поддержки аутентификации с помощью сервера аутентификации и определяет процесс инкапсуляции данных EAP, передаваемых между клиентами (запрашивающими устройствами) и серверами аутентификации. Стандарт IEEE 802.1X осуществляет контроль доступа и не позволяет неавторизованным устройствам подключаться к локальной сети через порты коммутатора.

Сервер аутентификации проверяет права доступа каждого клиента, подключаемого к порту коммутатора, прежде чем разрешить доступ к любому из сервисов, предоставляемых коммутатором или локальной сетью.

До тех пор, пока клиент не будет аутентифицирован, через порт коммутатора, к которому он подключен, будет передаваться только трафик протокола Extensible Authentication Protocol over LAN (EAPOL). Обычный трафик начнет передаваться через порт коммутатора сразу после успешной аутентификации клиента.

Архитектура IEEE 802.1X включат в себя следующие обязательные логические элементы:

- *клиент (Supplicant)* находится в операционной системе абонента, обычно это рабочая станция, которая запрашивает доступ к локальной сети и сервисам коммутатора и отвечает на запросы от коммутатора. На рабочей станции должно быть установлено клиентское ПО для 802.1X, например то, которое встроено в ОС Microsoft Windows;
- *сервер аутентификации (Authentication Server)* выполняет фактическую аутентификацию клиента. Он проверяет подлинность клиента и информирует коммутатор, предоставлять или нет клиенту доступ к локальной сети. В качестве сервера аутентификации обычно используется сервер RADIUS;
- *аутентификатор (Authenticator)* управляет физическим доступом к сети, основываясь на статусе аутентификации клиента. Эту роль выполняет коммутатор. Он работает как посредник (Proxy) между клиентом и сервером аутентификации: получает запрос на проверку подлинности от клиента, проверяет данную информацию при помощи сервера аутентификации и пересылает ответ клиенту. Коммутатор поддерживает клиент RADIUS, который отвечает за инкапсуляцию и деинкапсуляцию кадров EAP, и взаимодействие с сервером аутентификации.

В коммутаторах D-Link поддерживаются две реализации аутентификации 802.1X:

- Port-Based 802.1X (802.1X на основе портов);
- MAC-Based 802.1X (802.1X на основе MAC-адресов).

При аутентификации 802.1X на основе портов (Port-Based 802.1X), после того как порт был авторизован, любой пользователь, подключенный к нему, может получить доступ к сети.

Аутентификация 802.1X на основе MAC-адресов – это аутентификация множества клиентов на одном физическом порте коммутатора. При аутентификации 802.1X на основе MAC-адресов (MAC-Based 802.1X) проверяются не только имя пользователя/пароль подключенных к порту коммутатора клиентов, но и их количество. Количество подключаемых клиентов ограничено максимальным количеством MAC-адресов, которое может изучить каждый порт коммутатора. Для функции MAC-Based 802.1X количество изучаемых MAC-адресов указывается в спецификации на устройство.

Для выполнения данной лабораторной работы необходимо, чтобы в лабораторной среде была создана инфраструктура PKI (Public Key Infrastructure) на основе Microsoft Windows, Unix и т.п., установлен сервер RADIUS (например, IAS MS Windows 2003). Стандартные порты работы протокола RADIUS:

Application protocol	**Protocol**	**Ports**
Legacy RADIUS	UDP	1645
Legacy RADIUS	UDP	1646
RADIUS Accounting	UDP	1813
RADIUS Authentication	UDP	1812

На рабочей станции необходимо установить клиентское ПО (Supplicant) для 802.1X, если оно отсутствует (клиент 802.1X встроен в ОС Window XP).

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

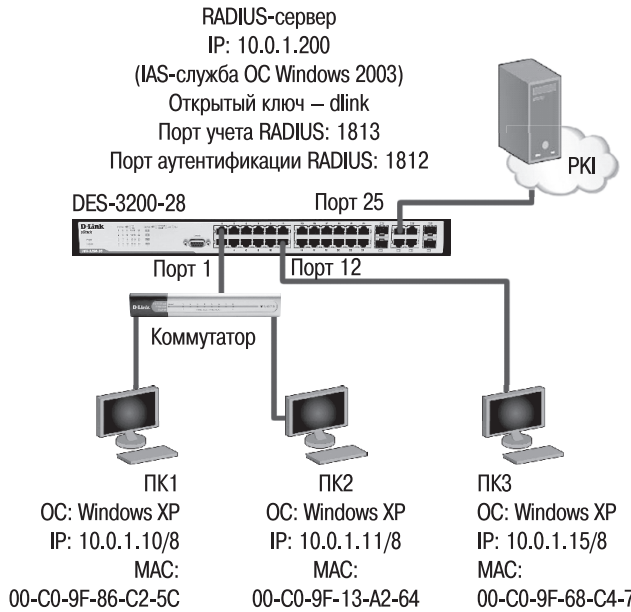
Цель: Изучить процесс настройки протокола 802.1X.

Оборудование:

DES-3200-28	1 шт.
DES-1005A	1 шт.
Рабочая станция	3 шт.
Кабель Ethernet	5 шт.

Radius-сервер	1 шт.
Консольный кабель	1 шт.

Схема 1:



1. Настройка DES-3200-28

1.1. Изучение команд протокола 802.1X

Включите функцию 802.1X	*enable 802.1x*
Настройте параметры первичного RADIUS-сервера	*config radius add 1 10.0.1.200 key dlink auth_port 1812 acct_port 1813*
Проверьте настройки данных RADIUS-сервера	*show radius*

Внимание! Для обеспечения отказоустойчивости коммутатор может поддерживать информацию о трех серверах аутентификации (RADIUS-серверах).

Занятие №16. Управление полосой пропускания

Современные коммутаторы позволяют регулировать интенсивность трафика на своих портах с целью обеспечения функций качества обслуживания.

Для управления полосой пропускания входящего и исходящего трафика на портах Ethernet коммутаторы D-Link поддерживают функцию Bandwidth Control, которая использует для ограничения скорости механизм Traffic Policing. Администратор может вручную устанавливать требуемую скорость соединения на порте в диапазоне от 64 Кбит/с до максимально поддерживаемой скорости интерфейса с шагом 64 Кбит/с.

Цель: Настроить ограничение полосы пропускания на коммутаторе D-Link.

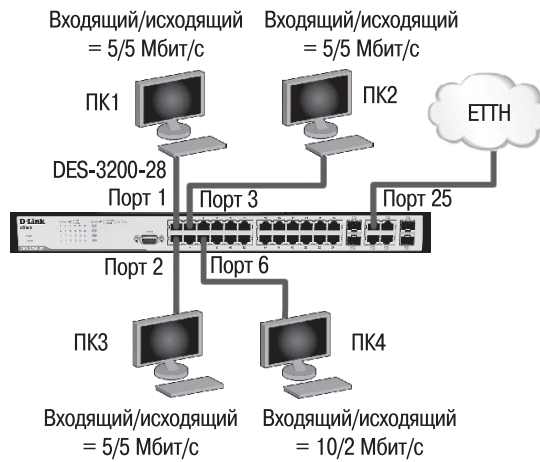
Оборудование:

DES-3200-28	1 шт.
Рабочая станция	4 шт.
Кабель Ethernet	5 шт.
Консольный кабель	1 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

Схема 1:



Занятие №17. Настройка QoS. Приоритизация трафика

Сети с коммутацией пакетов на основе протокола IP не обеспечивают гарантированной пропускной способности, поскольку не обеспечивают гарантированной доставки.

Для приложений, где не важен порядок и интервал прихода пакетов, время задержек между отдельными пакетами не имеет решающего значения. Для приложений, чувствительных к задержкам, в сети должны быть реализованы механизмы, обеспечивающие функции качества обслуживания (Quality of Service, QoS).

Функции качества обслуживания в современных сетях заключаются в обеспечении гарантированного и дифференцированного уровня обслуживания сетевого трафика, запрашиваемого теми или иными приложениями на основе различных механизмов распределения ресурсов, ограничения интенсивности трафика, обработки очередей и приоритизации.

Для обеспечения QoS на канальном уровне модели OSI коммутаторы поддерживают стандарт IEEE 802.1p. Стандарт IEEE 802.1p позволяет задать до 8 уровней приоритетов (от 0 до 7, где 7 – наивысший), определяющих способ обработки кадра, используя 3 бита поля приоритета тега IEEE 802.1Q.

В лабораторной работе рассматривается следующий пример: на компьютерах B и D запущены приложения VoIP, и им необходимо обеспечивать высокий приоритет обработки по сравнению с приложениями других станций.

Цель: Изучить настройку приоритизации трафика на коммутаторах D-Link.

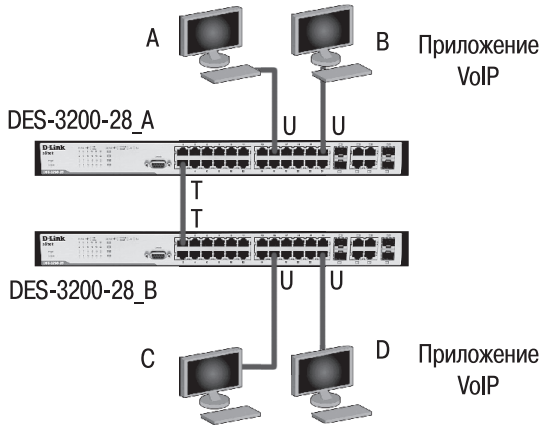
Оборудование:

DES-3200-28	2 шт.
Рабочая станция	4 шт.
Кабель Ethernet	5 шт.
Консольный кабель	2 шт.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой

reset config

Схема 1:



1. Настройка DES-3200-28_A

Переведите порт 1 на коммутаторе в состояние передачи маркированных кадров (для обеспечения возможности передачи информации о приоритете 802.1 p)	*config vlan default delete 1* *config vlan default add tagged 1*
Поменяйте приоритет по умолчанию порта 23, к которому подключена станция B	*config 802.1p default_priority 23 7*

Примечание. Пользовательский приоритет и метод обработки остаются по умолчанию.

2. Настройка DES-3200-28_B

Переведите порт 1 на коммутаторе в состояние передачи маркированных кадров (для обеспечения возможности передачи информации о приоритете 802.1 p)	*config vlan default delete 1* *config vlan default add tagged 1*
Поменяйте приоритет по умолчанию порта 23, к которому подключена станция D	*config 802.1p default_priority 24 7*

Занятие №18. Команды зеркалирования портов (Port Mirroring)

Коммутаторы улучшают производительность и надежность сети, передавая трафик только на те порты, которым он предназначен. При этом анализ критичных данных – сложная задача, поскольку инструментальные средства сетевого анализа физически изолированы от анализируемого трафика.

На коммутаторах D-Link реализована поддержка функции Port Mirroring («Зеркалирование портов»), которая полезна администраторам для мониторинга и поиска неисправностей в сети.

Функция Port Mirroring позволяет отображать (копировать) кадры, принимаемые и отправляемые портом-источником (Source port) на целевой порт (Target port) коммутатора, к которому подключено устройство мониторинга (например, с установленным анализатором сетевых протоколов) с целью анализа проходящих через интересующий порт пакетов.

В настоящее время анализаторы сетевых протоколов эффективно используются IT-отделами и отделами информационной безопасности для решения широкого круга задач. С их помощью можно быстро определить причину медленной работы IT-сервиса или бизнес-приложения. Они позволяют документировать сетевую активность пользователей и использовать полученные данные, например, для определения источника утечки информации.

Цель: Настроить отображение портов и понять способы его настройки.

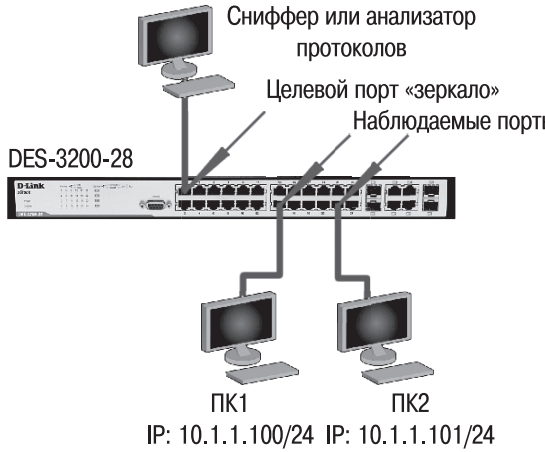
Оборудование:

DES-3200-28	1 шт.
Рабочая станция	3 шт.
Кабель Ethernet	3 шт.
Консольный кабель	1 шт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой

reset config

Схема 1:



1. Настройка DES-3200-28

Настройте список портов (с 13 по 24), трафик которых будет пересылаться на целевой порт 1	*config mirror port 1 add source ports 13-24 both*
Включите зеркалирование портов	*enable mirror*
Проверьте настройки функции	*show mirror*

Внимание!
Целевой порт и порт-источник должны принадлежать одной VLAN и иметь одинаковую скорость работы. В том случае, если скорость порта-источника будет выше скорости целевого порта, коммутатор снизит скорость порта-источника до скорости работы целевого порта. Также целевой порт не может быть членом группы агрегированных каналов.

Упражнения

Задание	**Наблюдение**

Установите на рабочей станции, подключенной к порту 1, анализатор протоколов (например,Wireshark).

www.wireshark.org – официальный сайт Wireshark.

Занятие №19. Команды мониторинга

Мониторинг работоспособности компьютерной сети является очень важным элементом управления сетью. Он позволяет быстро локализовать проблему, найти источник сбоя, посмотреть загрузку сети, оценить возможность масштабирования сети и т.п.

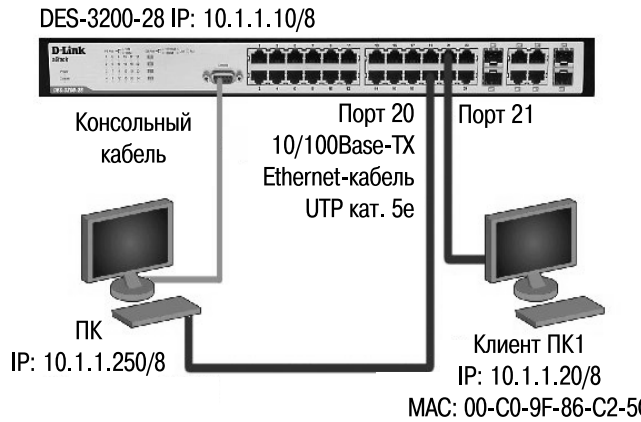
В данной лабораторной работе изучаются основные команды мониторинга работы коммутатора.

Цель: Изучить процесс мониторинга состояния коммутатора.

Оборудование:

DES-3200-28	1 шт.
Рабочая станция	2 шт.
Кабель Ethernet	2 шт.
Консольный кабель	1 шт.

Схема 1:



1. Настройка DES-3200-28

1.1. Изучение команд просмотра утилизации (загрузки) портов и CPU коммутатора

Просмотрите загрузку CPU коммутатора	*show utilization cpu*

Внимание! В случае длительной загрузки CPU более 90-100% необходимо проверить следующие характеристики:

1. возможные атаки на коммутатор, неправильная настройка сети. Данная проблема может быть решена путем включения функции SafeGuard Engine;
2. неправильная настройка ACL или других функций коммутатора, влияющих на производительность и работу CPU;
3. некорректная работа ПО коммутатора при выполнении некоторых функций. Данная проблема может быть решена путем замены ПО коммутатора.

Просмотрите загрузку портов коммутатора *show utilization ports 1-24*

Примечание. С помощью данной команды можно посмотреть как загрузку (утилизацию) портов коммутатора, так и объем передаваемого трафика.

1.2. Изучение команд просмотра статистики/ошибок передаваемых пакетов на порте коммутатора

Просмотрите пакеты, передаваемые станцией ПК1, подключенной к порту 21 *show packet ports 21*

Примечание. Данная команда позволяет определять количественные характеристики передаваемых пакетов. В случае большого количества широковещательного трафика (более 15% от общего числа передаваемого трафика) необходимо провести анализ на наличие в сети DOS-атак или ее неисправности (широковещательный шторм).

Просмотрите статистику об ошибках пакетов, принимаемых и передаваемых через порт 21 *show error ports 21*

Примечание. Данная команда позволяет определять ошибки передаваемых данных и локализовать проблемы в коммутируемой сети.

Очистите счетчики статистики на порте 21 *clear counters ports 21*

Глоссарий

A

AAA (англ. Authentication, Authorization, Accounting**).** Функция, которая представляет собой комплексную структуру организации доступа пользователя в сеть. Она включает следующие базовые процессы:

- **Аутентификация (Authentication)**. Процедура проверки подлинности субъекта на основе предоставленных им данных;
- **Авторизация (Authorization)**. Предоставление определенных прав лицу на выполнение некоторых действий;
- **Учет (Accounting)**. Слежение за использованием пользователем сетевых ресурсов.

Access layer Уровень доступа. Уровень доступа является нижним уровнем иерархической модели сети и управляет доступом пользователей и рабочих групп к ресурсам объединенной сети. Основной задачей уровня доступа является создание точек входа/выхода пользователей в сеть.

ACL (англ. Access Control List**).** Списки управления доступом. Списки управления доступом являются средством фильтрации потоков данных на аппаратном уровне. Используя ACL, можно ограничить типы приложений, разрешенных для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS путем классификации трафика и переопределения его приоритета.

Agent Агент. В модели «клиент-сервер» – часть системы, выполняющая подготовку информации и обмен ею между клиентской и серверной частью. Применительно к SNMP термин «агент» означает программный модуль для управления сетью, который находится на управляемом сетевом устройстве (маршрутизаторе, коммутаторе, точке доступа, Интернет-шлюзе, принтере и т.д.). Агент обслуживает базу управляющей информации и отвечает на запросы менеджера SNMP.

Auto-negotiation Автосогласование. Функция, обеспечивающая механизм автоматической настройки портов мультискоростных устройств. Устройства, поддерживающие функцию автосогласования, могут определять режимы работы партнеров по соединению, оповещать их о своих режимах работы и выбирать наилучший режим для совместного функционирования.

ARP (англ. Address Resolution Protocol**).** Протокол разрешения адресов. Протокол, используемый для динамического преобразования IP-адресов в физические (аппаратные) MAC-адреса устройств локальной сети TCP/IP. В общем случае ARP требует передачи широковещательного сообщения всем узлам, на которое отвечает узел с соответствующим запросу IP-адресом.

ASIC (англ. Application Specific Integrated Circuit). Специализированная для решения конкретной задачи интегральная схема (ИС). Современные контроллеры ACIS часто содержат на одном кристалле 32-битные процессоры, блоки памяти, включая ROM, RAM, EEPROM, Flash, и встроенное программное обеспечение. Такие ASIC получили название System-on-a-Chip (SoC).

B

Backbone Магистраль, часть сети, по которой передается основной трафик и которая является чаще всего источником и приемником трафика других сетей.

Backplane Объединительная плата. Физическое соединение между интерфейсным процессором или платой, шинами данных и шинами распределения питания системного блока устройства.

Bandwidth Полоса пропускания определяет частотный диапазон сигналов, пропускаемых линией связи без значительных искажений.

BGP (англ. Border Gateway Protocol). Протокол пограничных шлюзов. Обеспечивает основную динамическую маршрутизацию в сети Интернет. Регламентируется RFC 4271 и другими.

BOOTP (англ. Bootstrap Protocol**).** Протокол загрузки. Сетевой протокол, используемый для удаленной загрузки бездисковых рабочих станций. Позволяет им автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Регламентируется RFC 951 и другими.

BPDU (англ. Bridge Protocol Data Unit). Блоки данных протокола моста. Служебные кадры протокола связующего дерева (Spanning Tree Protocol), которые посылаются через заданные интервалы времени для обмена информацией между мостами.

Bridge Мост. Устройство, соединяющее между собой два физических сегмента локальной сети и передающее кадры из одного сегмента в другой. Мосты работают на канальном уровне модели OSI.

Broadcast Широковещание. Система доставки пакетов, при которой копия каждого пакета передается всем узлам, подключенным к сети.

Broadcast storm Широковещательный шторм. Множество одновременных широковещательных рассылок в сети, которые, как правило, поглощают доступную полосу пропускания сети и могут вызвать отказ сети.

Bus topology Шинная топология. Топология сети, при которой в качестве среды передачи используется единый кабель (он может состоять из последовательно соединенных отрезков), к которому подключаются все сетевые устройства.

C

CBS (англ. Committed Burst Size). Согласованный размер всплеска. В алгоритме «корзина маркеров» – объем трафика, на который может быть превышен размер корзины маркеров в отдельно взятый момент всплеска. Также см. *CIR* и *EBS*.

CDT (англ. Cross Device Trunking). Функция объединения нескольких физических портов разных коммутаторов физического стека в один агрегированный канал с повышенной полосой пропускания. См. также Link Aggregation.

Channel Канал. Путь передачи [электрических] сигналов между двумя или несколькими точками. Используются также термины: link, line, circuit и facility.

Chassis Шасси. Специальная конструкция для установки модулей и других компонент, образующих вместе единое устройство. Шасси обеспечивает питание и соединяющую модули магистраль.

CIOQ (англ. Combined Input and Output Queued). Тип буферизации в коммутаторах с комбинированными входными и выходными очередями. Буферы памяти подключаются как к входным, так и выходным портам.

CIR (англ. Committed Information Rate). Согласованная скорость передачи. В алгоритме «корзина маркеров» – средняя скорость передачи трафика через интерфейс коммутатора/маршрутизатора. Также см. CBS и EBS.

CLI (англ. Command Line Interface**)**. Интерфейс командной строки. Позволяет пользователю взаимодействовать с операционной системой настраиваемого устройства путем ввода команд и параметров.

Client Клиент. Узел или программное обеспечение (внешнее устройство), которое запрашивает у сервера некоторые сервисы.

Collision Коллизия. Возникает в сети Ethernet, когда два узла одновременно ведут передачу. Передаваемые ими по физическому носителю кадры сталкиваются и разрушаются.

Collision domain Домен коллизий. Часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части сети эта коллизия возникла.

Console port Консольный порт. Порт на коммутаторе, к которому подключается терминальное или модемное соединение. Он преобразует параллельное представление данных в последовательное, которое используется при передаче данных. Этот порт используется для выделенного локального управления через консоль.

Core layer Уровень ядра. Уровень ядра находится на самом верху иерархической модели сети и отвечает за надежную и быструю передачу больших объемов данных. Трафик, передаваемый через ядро, является общим для большинства пользователей. Сами пользовательские

данные обрабатываются на уровне распределения, который, при необходимости, пересылает запросы к ядру.

CoS (англ. Class of Service). Класс обслуживания. Способ классификации и приоритизации пакетов на основе типа приложения или других методов классификации (802.1p, ToS, DiffServ) для обеспечения качества обслуживания в сети.

Cut-through Коммутация без буферизации. Способ коммутации, при котором коммутатор копирует в буфер только MAC-адрес приемника (первые 6 байт после префикса) и сразу начинает передавать кадр, не дожидаясь его полного приема. Коммутация без буферизации уменьшает задержку, но проверку на ошибки не выполняет.

CVLAN (англ. Customer VLAN ID). В Q-in-Q – идентификатор VLAN, используемый в сетях пользователей. См. также SP-VLAN.

D

D-View Программное обеспечение SNMP компании D-Link, используемое для управления и мониторинга сетевого оборудования.

Desktop switch. Настольный коммутатор. Настольные коммутаторы предназначены для размещения на столах. Иногда они могут оснащаться входящими в комплект поставки скобами для крепления на стену. Обычно такие коммутаторы обладают корпусом обтекаемой формы с относительно небольшим количеством фиксированных портов, внешним или внутренним блоком питания и небольшими ножками (обычно резиновыми) для обеспечения вентиляции нижней поверхности устройства.

DHCP (англ. Dynamic Host Configuration Protocol). Протокол динамической конфигурации узла. Сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Является расширением протокола BOOTP. Регламентируется RFC 2131 и другими.

Diffserv (англ. Differentiated Services). Простой метод классификации, управления и предоставления качества обслуживания в современных IP-сетях. Использует для своей работы поле DSCP. Регламентируется RFC 2475, 3260.

Distribution layer Уровень распределения/агрегации. Средний уровень иерархической модели сети, который иногда называют уровнем рабочих групп, является связующим звеном между уровнями доступа и ядра.

DNS (англ. Domain Name System). Система доменных имен. Компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене.

DoS (англ. Denial-of-service). Атака типа «отказ в обслуживании».

Double VLAN См. Q-in-Q.

DSCP (англ. Differentiated Services Code Point). Поле в заголовке IP-пакета, используемое для классификации (приоритизации) передаваемой информации. Регламентируется RFC 2774 и другими.

E

E2ES (англ. End-to-End Security). Дословно «Безопасность от края до края». Концепция комплексной защиты сети предприятия.

EBS (англ. Extended Burst Size). Расширенный размер всплеска. В алгоритме «корзина маркеров» – объем трафика, на который может быть превышен размер корзины маркеров в экстренном случае. Также см. CBS и CIR.

EAP (англ. Extensible Authentication Protocol**)**. Расширяемый протокол аутентификации. Протокол, поддерживающий множество механизмов аутентификации.

ECTP (англ. Ethernet Configuration Testing Protocol). Служебный протокол, используемый для работы функции LoopBack detection.

Enterprise Крупные предприятия. Название сегмента рынка электроники. Обычно характеризует устройства, предназначенные для использования в сетях крупных предприятий с численностью сотрудников более 1000 человек.

Ethernet Стандарт организации локальных сетей (ЛВС), описанный в спецификациях IEEE и других организаций. IEEE 802.3. Ethernet использует полосу 10 Мбит/с и метод доступа к среде CSMA/CD. Наиболее популярной реализацией Ethernet является 10Base-T. Развитием технологии Ethernet является Fast Ethernet (100 Мбит/с), Gigabit Ethernet (1 Гбит/с), 10 Gigabit Ethernet (10 Гбит/с).

ETTH (англ. Ethernet to the Home). Ethernet до дома (квартиры). Цель решения ETTH заключается в передаче данных, речи и видео по простой и недорогой сети Ethernet.

F

FDB (англ. Forwarding DataBase). Таблицы коммутации. Таблица коммутации создается коммутатором в процессе работы и содержит данные о соответствии MAC-адреса узла порту коммутатора.

FIFO (англ. First Input First Output). Тип очереди «первым пришел, первым ушел».

FTTH (англ. Fiber to the Home). Оптический кабель до дома (квартиры). Цель решения FTTH заключается в передаче данных, речи и видео по простой и недорогой сети, чаще всего Ethernet. Уникальным преимуществом данного решения является то, что использование Ethernet с оптическим волокном в качестве среды передачи данных

позволяет обеспечить доступ к сети непосредственно из помещений клиентов услуг на высоких скоростях.

Filtering Фильтрация. Процесс проверки пакетов данных в сети и определения адресатов для принятия решения о дальнейшей пересылке (данная локальная сеть, удаленная локальная сеть) или отбрасывании пакета. Фильтрация пакетов выполняется мостами, коммутаторами и маршрутизаторами.

Flooding Лавинная передача. Способ передачи трафика, используемый в коммутаторах и мостах, при котором полученный интерфейсом трафик пересылается всем другим интерфейсам этого устройства.

Flow control Управление потоком. Методы, используемые для контроля над передачей данных между двумя точками сети и позволяющие избегать потери данных в результате переполнения приемных буферов.

Forwarding Продвижение. Процесс продвижения пакета к месту его назначения посредством сетевого устройства.

Fragment-free Коммутация с исключением фрагментов. Этот метод коммутации является компромиссным решением между методами store-and-forward и cut-through switching. Коммутатор принимает в буфер первые 64 байта кадра, что позволяет ему отфильтровывать коллизионные кадры перед их передачей.

Frame Кадр. Единица информации на канальном уровне сетевой модели. В ЛВС кадр представляет собой единицу данных подуровня MAC, содержащую управляющие данные и пакет сетевого уровня. Иногда для обозначения кадров используется термин «пакет», но термины «кадр» или «фрейм» никогда не используются для обозначения пакетов сетевого уровня. Кадр обычно содержит ограничители, управляющие поля, адреса, контрольную сумму и собственно информацию.

FTP (англ. File Transfer Protocol). Протокол передачи файлов. Протокол FTP относится к протоколам прикладного уровня стека TCP/IP и предназначен для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер.

Full duplex Дуплексная передача. Одновременная передача данных между станцией-отправителем и станцией- получателем.

G

GBIC (англ. Gigabit Interface Converter). Спецификация SFF-8053 комитета SFF на компактные сменные интерфейсные модули, описывающая конвертеры гигабитного интерфейса.

GVRP (англ. GARP VLAN Registration Protocol). В стандарте IEEE 802.1Q протокол GVRP определяет способ, посредством которого коммутаторы обмениваются информацией о сети VLAN, чтобы автоматиче-

ски зарегистрировать членов VLAN на портах во всей сети. Позволяет динамически создавать и удалять VLAN на магистральных портах коммутаторов, автоматически регистрировать и исключать атрибуты VLAN.

GUI (англ. Graphical User Interface). Графический интерфейс пользователя. Метод взаимодействия между пользователем и компьютером, при котором пользователь может вызывать различные функции, указывая на графические элементы (кнопки) вместо ввода команд с клавиатуры.

H

Half duplex Полудуплексная передача. Способность канала в каждый момент времени только передавать или принимать информацию. Прием и передача, таким образом, должны выполняться поочередно.

HDMI (англ. High-Definition Multimedia Interface). Цифровой интерфейс, использующийся в некоторых коммутаторах D-Link для физического стекирования.

HOL (англ. Head-Of-Line blocking). Блокировка первым в очереди. Блокировка возникает в том случае, когда коммутатор пытается одновременно передать пакеты из нескольких входных очередей на один выходной порт. При этом пакеты, находящиеся в начале этих очередей, блокируют все остальные пакеты, находящиеся за ними.

I

IANA (англ. Internet Assigned Numbers Authority). Агентство по выделению имен и уникальных параметров протоколов Интернета.

ICMP (англ. Internet Control Message Protocol). Межсетевой протокол управляющих сообщений. Сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или узел или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции. Регламентируется RFC 792 и другими.

IEEE (англ. Institute of Electrical and Electronic Engineers). Институт инженеров по электротехнике и радиоэлектронике. Профессиональная организация, основанная в 1963 году для координации разработки компьютерных и коммуникационных стандартов. Институт подготовил группу стандартов 802 для локальных сетей. Членами IEEE являются ANSI и ISO.

IGMP (англ. Internet Group Management Protocol). Межсетевой протокол управления группами. Протокол IGMP используется для динамической регистрации отдельных узлов в многоадресной группе локальной сети. Узлы сети определяют принадлежность к группе, посылая

IGMP-сообщения на свой локальный многоадресный маршрутизатор. Регламентируется RFC 1112, 2236, 3376 и другими.

IMPB (англ. IP-MAC-Port Binding). Функция коммутаторов D-Link, позволяющая контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения.

IntServ (англ. Integrated Services). Интегрированные услуги. Модель приоритизации, предполагающая предварительное резервирование сетевых ресурсов с целью обеспечения предсказуемого поведения сети для приложений, требующих гарантированной выделенной полосы пропускания на всем пути следования трафика. Регламентируется RFC 1633 и другими.

IP (англ. Internet Protocol). IP-протокол. Часть стека протоколов TCP/IP. Описывает программную маршрутизацию пакетов и адресацию устройств. Стандарт используется для передачи через сеть базовых блоков данных и дейтаграмм IP. Обеспечивает передачу пакетов без организации соединений и гарантии доставки. Регламентируется RFC 791 и другими.

IP address. IP-адрес. Адрес для протокола IP – 32 битовое (4 байта) значение, определенное в STD 5 (RFC 791) и используемое для представления точек подключения в сети TCP/IP. IP-адрес состоит из номера сети (network portion) и номера хоста (host portion) – такое разделение позволяет сделать маршрутизацию более эффективной. Обычно для записи IP-адресов используют десятичную нотацию с разделением точками. Новая версия протокола IPv6 использует 128-разрядные адреса, позволяющие решить проблему нехватки адресного пространства.

ISO (англ. International Organization for Standardization). Международная организация по стандартизации.

ISO/OSI (англ. Open Systems Interconnection Reference Model). Эталонная модель взаимодействия открытых систем (OSI), разработанная организацией ISO.

ISP (англ. Internet Service Provider). Поставщик услуг сети Интернет.

L

LACP (англ. Link Aggregation Control Protocol). Протокол управления агрегированным каналом, регламентируемый в стандарте IEEE 802.3ad. См. также Link Aggregation.

LBD (англ. LoopBack Detection). Функция коммутаторов D-Link, блокирующая коммутационные петли на пользовательских портах.

L2 switch Коммутатор 2-го уровня. Анализирует входящие кадры, принимает решение об их дальнейшей передаче и передает их получателю на основе MAC-адресов канального уровня модели OSI.

L3 switch Коммутатор 3-го уровня. Выполняет L2 коммутацию в пределах рабочей группы (точно так же, как коммутатор 2-го уровня) и марш-

рутизацию между различными подсетями или виртуальными локальными сетями.

LAN (англ. Local Area Network). Локальная сеть. Высокоскоростная компьютерная сеть, покрывающая относительно небольшую площадь. Локальные сети объединяют рабочие станции, периферийные устройства, терминалы и другие устройства, находящиеся в одном здании или на другой небольшой территории.

Latency Задержка. Временная задержка между моментом, когда устройство получило пакет, и моментом, когда пакет был отправлен на порт назначения.

Link Aggregation Агрегирование каналов связи. Объединение нескольких физических портов в одну логическую магистраль на канальном уровне модели OSI с целью образования высокоскоростного канала передачи данных и повышения отказоустойчивости.

Load Balancing Балансировка нагрузки. Распределение процесса выполнения заданий между несколькими устройствами сети с целью оптимизации использования ресурсов и сокращения времени вычисления.

M

MAC address MAC-адрес. Стандартный адрес канального уровня, который требуется задавать для каждого порта или устройства, подключенного к локальной сети. Другие устройства используют эти адреса для обнаружения специальных сетевых портов, а также для создания и обновления таблиц маршрутизации и структур данных. Длина MAC-адреса составляет 6 байтов, а его содержимое регламентируется IEEE. MAC-адреса также называют аппаратными или физическими адресами.

MAC (англ. MAC-based Access Control). Функция коммутаторов D-Link, позволяющая проводить аутентификацию пользователей через протокол IEEE 802.1X, используя в качестве источника аутентификации MAC-адрес сетевой платы пользователя.

Managed switch Управляемый коммутатор. Управляемые коммутаторы являются сложными устройствами, позволяющими выполнять расширенный набор функций 2 и 3 уровня модели OSI. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протокола SNMP, Telnet и т.д.

MIB (англ. Management Information Base). База управляющей информации. Совокупность иерархически организованной информации, доступ к которой осуществляется посредством протокола управления сетью SNMP. База управляющей информации состоит из управляемых объектов (MIB-объектов), значения которых могут быть изменены или извлечены с помощью команд SNMP и сете-

вой системы управления (например, D-Link D-View) с GUI-интерфейсом.

MDI (англ. Medium Dependent Interface). Ethernet-порт абонентского устройства, например, сетевой карты ПК.

MDIX (англ. Medium Dependent Interface with Crossover). Ethernet-интерфейс с перекрёстным подключением цепей приема и передачи. Используется в Ethernet-коммутаторах.

MSTP (англ. Multiple Spanning Tree Protocol). Является расширением протокола RSTP и позволяет настраивать отдельное связующее дерево для любой VLAN или группы VLAN, создавая множество маршрутов передачи трафика, и позволяя осуществлять балансировку нагрузки. Первоначально протокол MSTP был определен в стандарте IEEE 802.1s, но позднее был добавлен в стандарт IEEE 802.1Q-2003. Протокол MSTP обратно совместим с протоколами STP и RSTP.

MTU (англ. Maximum Transmission Unit). Модуль передачи максимального размера. Максимальный размер (в байтах) пакета данных, который можно передать через данный интерфейс.

Multicast Многоадресная рассылка. Доставка потока данных группе узлов на IP-адрес группы многоадресной рассылки.

Multicast address Групповой адрес. Общий адрес, который относится к некоторой группе нескольких сетевых устройств.

Multicast group Группа многоадресной рассылки. Динамически определенная группа IP-узлов, идентифицируемая одним групповым IP-адресом.

Multicast router. Многоадресный маршрутизатор. Маршрутизатор, используемый для получения IGMP-ответов и периодической отправки IGMP-запросов о принадлежности узлов к многоадресной группе, чтобы определить, какие группы многоадресной рассылки активны или неактивны в данной сети.

N

NAP (англ. Network Access Protection). Защита доступа к сети. Технология компании Microsoft для управления доступом клиентских компьютеров к сетевым ресурсам на основе удостоверения компьютера и соответствия корпоративным политикам.

Network Address Сетевой адрес. Адрес сетевого уровня, который относится к логическому, а не к физическому сетевому устройству. Он также называется протокольным адресом (protocol address).

Node Узел. Точка присоединения к сети, устройство, подключенное к сети.

Non-blocking switch fabric «Неблокирующая» коммутирующая матрица. Матрица, у которой производительность и QoS не зависят от типа

трафика, коммутируемого через матрицу, и производительность равна сумме скоростей всех портов.

NNI (англ. Network-to-Network Interface). Интерфейс «сеть-сеть». В Q-in-Q – роль порта, который подключается к внутренней сети провайдера или другим граничным коммутаторам.

NVRAM (англ. NonVolatile RAM). Энергонезависимое ОЗУ. Оперативное запоминающее устройство, содержимое которого сохраняется при отключении питания.

O

OID (англ. Object Identifier). В протоколе SNMP – идентификатор объекта в базе MIB.

OSI См. ISO/OSI.

OSPF (англ. Open Shortest Path First). Протокол динамической маршрутизации для IP-сетей. Регламентируется RFC 2328, 5340 и другими.

P

Packet Пакет. Группа битов, включающая данные и служебные поля, представленные в соответствующих форматах, и передаваемая целиком. Структура пакета зависит от протокола. В общем случае пакет включает 3 основных элемента: управляющую информацию (адрес получателя и отправителя, длина пакета и т.п.), передаваемые данные, биты контроля и исправления ошибок.

PCF (англ. Packet Content Filtering, также ACL PCF). Фильтрация по содержимому пакета. Тип ACL, побайтно обрабатывающий заголовок кадра. Тип заголовка (Ethernet, IP, или любой другой) при этом не имеет значения, обрабатываются все его поля одновременно.

PDU (англ. Protocol Data Unit). Модуль данных протокола. Термин OSI для пакетов данных.

Ping (англ. Packet INternet Groper). Проверка доступности адресата. Эхосообщение протокола ICMP и ответ на него. Инструмент, используемый для проверки доступности адресата в IP-сетях.

PoE (англ. Power over Ethernet). Технология передачи питания по кабелю «витая пара» в сетях Ethernet. Регламентируется стандартом IEEE 802.3af.

PoE Plus (англ. Power over Ethernet Plus, также PoE+). Технология передачи питания по кабелю «витая пара» в сетях Ethernet. Является расширением технологии PoE и обеспечивает подачу большей мощности. Регламентируется стандартом IEEE 802.3at.

Port density Плотность портов. Количество портов на шасси.

Port Security Безопасность портов. Функция, применяемая в коммутаторах для обеспечения контроля над подключением узлов к их портам.

PPPoE (англ. PPP over Ethernet). Реализация протокола PPP для сетей Ethernet. Регламентируется RFC 2516 и другими.

Proxy ARP (англ. Proxy Address Resolution Protocol). Агент протокола разрешения адресов. Вариант протокола ARP, в котором промежуточное устройство (например, маршрутизатор) посылает ответ ARP от имени конечного узла запрашивающему устройству.

PVID (англ. Port VLAN ID). Идентификатор порта VLAN.

Q

QoS (англ. Quality of Service). Качество обслуживания. Показатель эффективности системы передачи данных, который отражает качество передачи.

Q-in-Q (или QinQ)**.** Расширение стандарта IEEE 802.1Q. Позволяет добавлять в маркированные кадры Ethernet второй тег IEEE 802.1Q. Регламентируется стандартом IEEE 802.1ad.

R

RADIUS (англ. Remote Authentication Dial-In User Service). Служба аутентификации удаленных пользователей. Протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием. Регламентируется RFC 2865 и другими.

Rack mounted switch Коммутаторы, монтируемые в телекоммуникационную стойку. Коммутаторы в стоечном исполнении высотой 1U обладают корпусом для монтажа в 19" стойку, встроенным блоком питания и фиксированным количеством портов.

RED (англ. Random Early Detection). В приоритизации – алгоритм произвольного раннего обнаружения, позволяющий избегать перегрузок в сети.

Redundancy Избыточность. Дублирование устройств, сервисов и соединений. В случае неисправности позволяет избыточным устройствам, службам и соединениям выполнять функции исправных.

Redundant system. Избыточная система. Компьютер, маршрутизатор, коммутатор или другая система, которая содержит два или более экземпляра наиболее важных подсистем, таких как дисководы, центральные процессоры или источники питания.

Reliability Надежность. В общем случае свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования.

RIP (англ. Routing Information Protocol). Протокол динамической маршрутизации для IP-сетей. Регламентируется RFC 1058, 2453 и другими.

RIPNg Протокол RIP для протокола IPv6. Регламентируется RFC 2080.

RJ-45 (8P8C) Унифицированный разъем, используемый в телекоммуникациях, имеет 8 контактов и защелку.

RMON (англ. Remote MONitoring). Удаленный мониторинг. Спецификация RMON MIB, разработанная сообществом IETF для поддержки мониторинга и анализа протоколов в локальных сетях. Первая версия RMON v.1 основывается на мониторинге информации сетей Ethernet и Token Ring. Ее расширением является RMON v.2, которая добавила к уже имеющимся средствам мониторинга поддержку мониторинга на сетевом уровне и уровне приложений модели OSI. Регламентируется RFC 2819, 2819 и другими.

RMT (англ. Resilient Master Technology). Технология, обеспечивающая непрерывную работу физического стека при выходе какого-либо устройства из строя, замене, добавлении и удалении коммутаторов.

Router Маршрутизатор. Устройство сетевого уровня, отвечающее за принятие решений о выборе одного из нескольких путей передачи сетевого трафика. Маршрутизаторы отправляют пакеты из одной сети в другую на основе информации сетевого уровня.

Routing Маршрутизация. Процесс выбора оптимального пути для передачи сообщения.

RSTP (англ. Rapid Spanning Tree Protocol). Протокол RSTP является развитием протокола STP. Первоначально был определен в стандарте IEEE 802.1w-2001, сейчас определен в стандарте IEEE 802.1D-2004.

S

Segment Сегмент. 1. Секция сети, ограниченная мостами, маршрутизаторами или коммутаторами. 2. В LAN с шинной топологией – непрерывная электрическая цепь, часто соединенная с другими сегментами при помощи повторителей. 3. Термин, используемый в спецификации TCP для описания одиночного модуля транспортного уровня.

SIM (англ. Single IP Management). Технология виртуального стекирования, применяемая в управляемых коммутаторах D-Link.

SFP (англ. Small Form Factor Pluggable). Промышленный стандарт модульных компактных приемопередатчиков (трансиверов), используемых для передачи данных.

Smart switch Настраиваемый коммутатор. Настраиваемые коммутаторы позволяют настраивать определенные параметры сети, используя Web-интерфейс или компактный интерфейс командной строки (Compact Command Line Interface, CLI), доступный через Telnet.

SMB (англ. Small-to-Medium Business). Малые и средние предприятия. Название сегмента рынка электроники. Характеризует устройства, предназначенные для использования в сетях малых и средних предприятий с численностью сотрудников от 100 до 999 человек.

SNMP (англ. Simple Network Management Protocol). Простой протокол управления сетью. Протокол 7 уровня модели OSI, который специально разработан для управления и мониторинга сетевых устройств. Протокол SNMP входит в стек протоколов TCP/IP и позволяет получать информацию о состоянии устройств сети, обнаруживать и исправлять неисправности и планировать развитие сети. Регламентируется RFC 1157, 1901-1908, 3411-3418 и другими.

SOHO (англ. Small Office, Home Office). Малый/домашний офис. Название сегмента рынка электроники. Как правило, характеризует устройства, предназначенные для домашнего использования или использования в небольших офисах и не рассчитанные на производственные нагрузки.

SP-VLAN (англ. Service Provider VLAN ID). В Q-in-Q – идентификатор VLAN, используемый в сети ISP. См. также CVLAN.

SRED (англ. Simple Random Early Detection). В приоритизации – алгоритм произвольного раннего обнаружения, позволяющий избегать перегрузок в сети. Является расширением алгоритма RED.

SSH (англ. Secure Shell). Безопасная оболочка. Сетевой протокол сеансового уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений. Регламентируется RFC 4253 и другими.

SSL (англ. Secure Sockets Layer). Уровень защищенных сокетов. Криптографический протокол, обеспечивающий безопасную передачу данных по сети Интернет. Регламентируется RFC 2246, 4346 и другими.

SST (англ. Single Spanning Tree Bridge). Мост, поддерживающий только единственное связующее дерево. Это единственное связующее дерево может поддерживать протоколы STP или RSTP.

STA (англ. Spanning Tree Algorithm). Алгоритм построения связующего дерева. Алгоритм, используемый протоколом связующего дерева для построения связующего дерева.

Stack Стек. Группа сетевых устройств, которые объединены в одно логическое устройство с целью увеличения количества портов, удобства управления и мониторинга.

STP (англ. Spanning Tree Protocol). Протокол связующего дерева. Стандарт IEEE 802.1D-1998, использующий алгоритм связующего дерева и позволяющий самообучающемуся мосту динамически обрабатывать коммутационные петли в сетевой топологии путем создания связующего дерева. Мосты обнаруживают петли путем обмена сообщениями BPDU с другими мостами и ликвидируют петли посредством блокирования выбранных мостовых интерфейсов.

Store-and-forward Коммутация с промежуточным хранением. Методика коммутации пакетов, согласно которой кадры полностью обрабаты-

ваются перед их отправкой через соответствующий порт. Обработка включает расчет CRC и проверку адреса приемника. Кроме того, кадры необходимо временно хранить до тех пор, пока не станут доступными сетевые ресурсы (например, свободный канал) для передачи сообщения. Эта технология противоположна коммутации без буферизации (cut-through).

Switch Коммутатор. Сетевое устройство, которое фильтрует, пересылает и направляет кадры в зависимости от их адреса приемника. Коммутатор работает на канальном уровне модели OSI.

Switch capacity Производительность коммутирующей матрицы. Производительность определяется как общая полоса пропускания (bandwidth), обеспечивающая коммутацию без отбрасывания пакетов трафика любого типа (одноадресного, многоадресного, широковещательного).

Switch fabric Коммутирующая матрица. Коммутирующая матрица представляет собой чипсет, соединяющий множество входов с множеством выходов на основе фундаментальных технологий и принципов коммутации.

T

Tag Тег. Идентификационная информация, в том числе и номер.

TCP (англ. Transmission Control Protocol). Протокол управления передачей. Ориентированный на соединение протокол транспортного уровня, обеспечивающий надежную дуплексную передачу данных. TCP входит в набор протоколов TCP/IP. Регламентируется RFC 675, 793, 2581 и другими.

Telnet Стандартный протокол виртуального терминала из набора протоколов TCP/IP. Протокол Telnet используется для удаленного терминального соединения, что дает возможность пользователям подключаться к удаленным системам и использовать их ресурсы, как если бы они работали через обычный терминал. Регламентируется RFC 15, 854 и другими.

TFTP (англ. Trivial File Transfer Protocol). Простейший протокол передачи файлов. Упрощенная версия протокола FTP, который позволяет компьютерам обмениваться файлами по сети. Регламентируется RFC 1350 и другими.

Throughput Пропускная способность. Объем информации, поступающей и, возможно, проходящей через определенный участок сети в определенный момент времени.

ToS (англ. Type of Service). Тип сервиса. Поле в заголовке протокола IP, используемое для обеспечения QoS.

TPID (англ. Tag Protocol Identifier). Идентификатор протокола тегирования в кадрах протоколов IEEE 802.1Q и IEEE 802.1ad.

Traffic Policing Ограничение трафика. Механизм Traffic Policing служит для ограничения входящего и исходящего трафика в соответствии с установленными пороговыми значениями скорости. Допускается всплеск трафика. См. также Traffic Shaping.

Traffic Segmentation Сегментация трафика. Функция, используемая в коммутаторах для разграничения доменов на уровне 2.

Traffic Shaping Выравнивание трафика. Механизм Traffic Shaping служит для выравнивания исходящего трафика с целью предотвращения перегрузки канала и удовлетворения требования поставщика услуг. См. также Traffic Policing.

Trap Ловушка. Тревожное сообщение (alarm message), которое устройство, находящееся под мониторингом, посылает управляющей станции при возникновении тревожных условий. Условия тревоги могут включать ошибки устройств, сетевые ошибки, изменения состояний и переход заданных пороговых значений.

Trunk Магистраль. Физическое и логическое соединение между двумя коммутаторами, по которому передается сетевой трафик.

U

UDP (англ. User Datagram Protocol). Протокол дейтаграмм пользователя. Протокол транспортного уровня, не требующий подтверждения соединения. Входит в набор протоколов TCP/IP. UDP обеспечивает обмен дейтаграммами без подтверждения и гарантий доставки.

UNI (англ. User-to-Network Interface). В Q-in-Q – роль порта, через который будет осуществляться взаимодействие граничного коммутатора провайдера с клиентскими сетями.

Unmanaged switch Неуправляемый коммутатор. Неуправляемые коммутаторы не поддерживают функции настройки и управления, имеют уже предустановленную функциональность. Данные коммутаторы применяются там, где характеристики, необходимые в сети, стандартные и не требуют дополнительных настроек.

V

VID (VLAN ID) Идентификатор VLAN.

VoIP (англ. Voice over IP). IP-телефония. Система связи, обеспечивающая передачу речевого сигнала по любым IP-сетям.

VLAN (англ. Virtual LAN). Виртуальная локальная сеть. Группа устройств, принадлежащих одной или нескольким локальным сетям и сконфигурированных таким образом (при помощи программного обеспечения), что обмен данными между ними происходит так, как будто они подключены к одному кабелю, хотя на самом деле находятся в разных сегментах локальной сети. VLAN основаны на логическом соединении.

VT100 Тип терминала, который использует символы ASCII. Терминалы VT100 представляют информацию в текстовом виде.

X

XFP (англ. 10 Gigabit Small Form Factor Pluggable). Протоколо-независимый оптический трансивер горячей замены, обычно работающий на длинах волны 850 нм, 1310 нм или 1550 нм на скорости 10 Гбит/с в стандартах SONET/SDH, Fibre Channel, Gigabit Ethernet, 10 Gigabit Ethernet, включая каналы WDM.

W

WAC (англ. Web-based Access Control). Функция коммутаторов D-Link, используемая для аутентификации пользователей при их попытке подключиться к сети Интернет через коммутатор. Процесс аутентификации использует протокол HTTP. Коммутатор может выступать в качестве сервера аутентификации и выполнять аутентификацию на основе локальной базы данных или быть клиентом RADIUS и использовать для аутентификации протокол IEEE 802.1X.

WDM (англ. Wavelength Division Multiplexing). Спектральное уплотнение каналов. Технология, позволяющая одновременно передавать несколько информационных каналов по одному оптическому волокну на разных несущих частотах.

Литература

1. *Смирнова Е.В., Пролетарский А.В., Ромашкина Е.А., Суровов А.М., Федотов Р.А.* Технологии коммутации и маршрутизации в локальных компьютерных сетях. М.: Издательство МГТУ им. Н.Э. Баумана, 2013. 389 с.
2. *Смирнова Е.В., Пролетарский А.В., Баскаков И.В., Федотов Р.А.* Управление коммутируемой средой. М.: РУСАКИ, 2011. 335 с.
3. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2000.
4. *Федотов Р.А., Пролетарский А.В., Баскаков И.В.* Методические указания к лабораторным работам по курсу «Коммутируемые сети». М.: Издательство МГОУ, 2008. 70 с.
5. Руководство по технологиям объединенных сетей. 3-е издание. Пер. с англ. М.: Издательский дом «Вильямс», 2002.
6. *Вегешна Шринивас.* Качество обслуживания в сетях IP. Пер. с англ. М.: Издательский дом «Вильямс», 2003.
7. *Scott Mueller.* Upgrading and Repairing Networks, Third Edition. Que, 2002.
8. *Panos C. Lekkas.* Network Processors. The McGraw-Hill Companies, 2003.
9. Руководства пользователя коммутаторов D-Link и учебные материалы компании D-Link [электронный ресурс] ftp://ftp.dlink.ru/
10. *Бараш Л.* Коммутаторы в локальных сетях. [электронный ресурс] http://desna.kiev.ua
11. History of LAN Switching. [электронный ресурс] http://www.myipaddressinfo.com
12. *Жилкина Н.* Сменные интерфейсы // Журнал сетевых решений/ LAN. 2004. № 05.
13. Evolution: 20 years of switching fabric. Ori Aruj, Dune Networks [электронный ресурс] http://www.commsdesign.com
14. On-chip Global Interconnects for Networking ASICs [электронный ресурс] http://www.lsi.com
15. *Andreas D. Bovopoulos and Micha Zeiger.* Shared-Memory Fabrics Meet 10-Gbit Backplane Demands. TeraChip, Inc. [электронный ресурс] http://www.commsdesign.com
16. *Shang-Tse Chuang, Ashish Goel, Nick McKeown, Balaji Prabhakar.* Matching Output Queueing with a Combined Input Output Queued Switch [электронный ресурс] http://www-rcf.usc.edu
17. An improved algorithm for CIOQ switches. Yossi Azar, Yossi Richter. [электронный ресурс] http://portal.acm.org
18. Сайт научной базы данных «SciVerse ScienceDirect» [электронный ресурс] http://www.sciencedirect.com
19. Сайт Института инженеров по электротехнике и электронике (IEEE, Institute of Electrical and Electronics Engineers) [электронный ресурс] http://www.ieee.org

20. Телекоммуникационные технологии. Сайт Натальи и Виктора Олифер [электронный ресурс] http://www.olifer.co.uk/
21. Internet RFC/STD/FYI/BCP Archives [электронный ресурс] http://www.faqs.org/rfcs

Лабораторные работы,
описанные в данном курсе, проводятся в Центре Сетевых Технологий МГТУ им. Н.Э.Баумана – D-Link и кафедры «Компьютерные системы и сети» (http://dop.bmstu.ru/iu-addon-study/429).

После прохождения курса в учебном центре слушатель получает выпускной документ о повышении квалификации, а после сдачи сертификационного экзамена - сертификат компании D-Link.

Все, кто интересуется современными сетевыми технологиями, также может пройти обучение по авторизованным курсам D-Link на портале дистанционного обучения и сертификации D-Link (http://learn.dlink.ru/login/index.php).

Программы авторизованных курсов, информация о технологиях и настройке оборудования, перечень авторизованных учебных центров доступны на сайте D-Link по адресу: http://www.dlink.ru/ru/education/

D-Link®
Building Networks for People

Учебное издание

Смирнова Елена Викторовна
Пролетарский Андрей Викторович
Баскаков Игорь Владимирович
Федотов Роман Анатольевич
Ромашкина Екатерина Александровна

ПОСТРОЕНИЕ КОММУТИРУЕМЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие

Компьютерная верстка *И.Ю.Галкин, Н.И.Галкин*

Подписано в печать 23.05.2015. Формат 60x90 $^{1}/_{16}$.
Гарнитура Ньютон. Бумага офсетная. Печать офсетная.
Усл. печ. л. 24,5. Тираж 2000 экз.

Национальный Открытый Университет «ИНТУИТ»
123056, Москва, Электрический пер., 8, стр. 3.
E-mail: admin@intuit.ru, http://www.intuit.ru