

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



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».

Полное или частичное воспроизведение или размножение каким-либо способом, в том числе и публикация в Сети, настоящего издания допускается только с письменного разрешения Национального Открытого Университета «ИНТУИТ».

ISBN 978-5-9556-0175-5

© Национальный Открытый
Университет «ИНТУИТ», 2015

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

Лекция 1. Основы коммутации	12
Лекция 2. Начальная настройка коммутатора	49
Лекция 3. Виртуальные локальные сети (VLAN)	66
Лекция 4. Функции повышения надежности и производительности	101
Лекция 5. Качество обслуживания (QoS)	146
Лекция 6. Многоадресная рассылка	161
Лекция 7. Функции обеспечения безопасности и ограничения доступа к сети	171
Лекция 8. Технология Power over Ethernet	207
Лекция 9. Функции управления коммутаторами	217
Лекция 10. Обзор коммутаторов D-Link	238

Оглавление

Введение	10
Лекция 1. Основы коммутации	12
1.1. Эволюция локальных сетей	12
1.2. Функционирование коммутаторов локальной сети	15
1.3. Методы коммутации	18
1.4. Конструктивное исполнение коммутаторов	20
1.5. Физическое стекирование коммутаторов	21
1.6. Типы интерфейсов коммутаторов	22
1.7. Архитектура коммутаторов	30
1.8. Характеристики, влияющие на производительность коммутаторов	39
1.9. Управление потоком в полудуплексном и дуплексном режимах	42
1.10. Технологии коммутации и модель OSI	44
1.11. Программное обеспечение коммутаторов	45
1.12. Общие принципы сетевого дизайна	45
1.13. Трехуровневая иерархическая модель сети	46
1.14. Обзор функциональных возможностей коммутаторов	48
Лекция 2. Начальная настройка коммутатора	49
2.1. Классификация коммутаторов по возможности управления	49
2.2. Средства управления коммутаторами	49
2.3. Подключение к коммутатору	50
2.4. Начальная конфигурация коммутатора	53
2.5. Подключение к Web-интерфейсу управления коммутатора	61
2.6. Загрузка нового программного обеспечения на коммутатор	63
2.7. Загрузка и резервное копирование конфигурации коммутатора	64
Лекция 3. Виртуальные локальные сети (VLAN)	66
3.1. Типы VLAN	68
3.2. VLAN на основе портов	69

3.3. VLAN на основе стандарта IEEE 802.1Q	70
3.4. Статические и динамические VLAN	81
3.5. Протокол GVRP	81
3.6. Q-in-Q VLAN	86
3.7. VLAN на основе портов и протоколов – стандарт IEEE 802.1v	93
3.8. Асимметричные VLAN	96
3.9. Функция Traffic Segmentation	98
Лекция 4. Функции повышения надежности и производительности ...	101
4.1. Протоколы Spanning Tree	101
4.2. Spanning Tree Protocol (STP)	101
4.3. Rapid Spanning Tree Protocol	112
4.4. Multiple Spanning Tree Protocol	123
4.5. Дополнительные функции защиты от петель	136
4.6. Функции безопасности STP	138
4.7. Агрегирование каналов связи	139
Лекция 5. Качество обслуживания (QoS)	146
5.1. Модели QoS	146
5.2. Приоритизация пакетов	147
5.3. Классификация пакетов	148
5.4. Маркировка пакетов	150
5.5. Управление перегрузками и механизмы обслуживания очередей	150
5.6. Механизм предотвращения перегрузок	152
5.7. Контроль полосы пропускания	154
5.8. Пример настройки QoS	158
Лекция 6. Многоадресная рассылка	161
6.1. IP-адресация многоадресной рассылки	161
6.2. MAC-адреса групповой рассылки	163
6.3. Подписка и обслуживание групп	165
6.4. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping)	165
6.2. Функция IGMP Snooping Fast Leave	169

Лекция 7. Функции обеспечения безопасности	
и ограничения доступа к сети	171
7.1. Списки управления доступом (ACL)	172
7.2. Функции контроля над подключением узлов	
к портам коммутатора	180
7.3. Аутентификация пользователей 802.1X	187
7.4. 802.1X Guest VLAN	195
7.5. Функции защиты ЦПУ коммутатора	203
Лекция 8. Технология Power over Ethernet	207
8.1. Как выбрать коммутатор PoE для сети	216
Лекция 9. Функции управления коммутаторами	217
9.1. Управление множеством коммутаторов	217
9.2. Протокол SNMP	228
9.3. RMON (Remote Monitoring)	233
9.4. Функция Port Mirroring	236
Лекция 10. Обзор коммутаторов D-Link	238
10.1. Неуправляемые коммутаторы	238
10.2. Коммутаторы серии Smart	241
10.3. Управляемые коммутаторы	248
Приложение	259
Занятие №1. Основные команды коммутаторов.	
Управление коммутаторами	261
Занятие №2. Команды обновления программного	
обеспечения коммутатора и сохранения/восстановления	
конфигурационных файлов	269
Занятие №3. Команды управления таблицами MAC, IP, ARP ...	273
Занятие №4. Команды VLAN на основе портов	
и стандарта IEEE 802.1Q	277
Занятие №5. Команды протокола GVRP	
(продвижение информации о VLAN в сети)	286
Занятие №6. Команды настройки асимметричных VLAN	
и сегментации трафика	292
Занятие №7. Команды настройки функции Q-in-Q	
(Double VLAN)	298

Занятие №8. Команды настройки протоколов связующего дерева STP, RSTP, MSTP	302
Занятие №9. Функция предотвращения петлеобразования (LoopBack Detection)	315
Занятие №10. Команды агрегирования каналов	320
Занятие №11. Списки управления доступом (Access Control List)	328
Занятие №12. Контроль над подключением узлов к портам коммутатора. Функция Port Security	337
Занятие №13. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	343
Занятие №14. Ограничение административного доступа к управлению коммутатором	350
Занятие №15. Команды протокола IEEE 802.1X	356
Занятие №16. Управление полосой пропускания	360
Занятие №17. Настройка QoS. Приоритизация трафика	362
Занятие №18. Команды зеркалирования портов (Port Mirroring)	366
Занятие №19. Команды мониторинга	369
Глоссарий	372
Литература	389

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 Шадневу 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:



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, поступающие 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-

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.

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 развиваться 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-

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.

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-

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.

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);

Лекция 8. Технология Power over Ethernet

Устанавливая точку доступа Wi-Fi, IP-камеру или IP-телефон, часто приходится 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 установку 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.

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).

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.

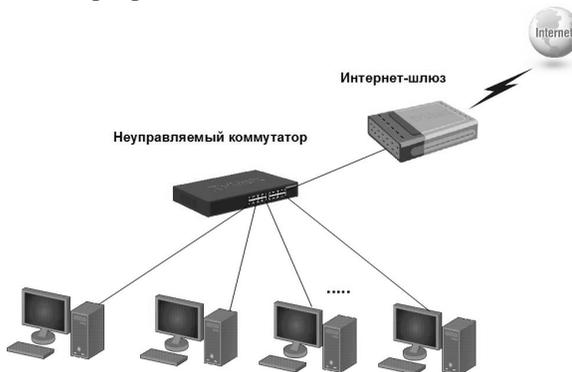


Рис. 10.1. Неуправляемые коммутаторы D-Link в сети небольшой рабочей группы

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.

Глоссарий

А

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).

В

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.

С

- 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 к 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 вершине 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.

Е

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).

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

Ф

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 коллизийные 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.

Н

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.

И

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.

М

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.

О

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.

Р

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. Эхо-сообщение 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 избежать 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.

Т

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 сконфигурованных 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., Суоровов 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. *Вегишна Шпринивас.* 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. *Барааш 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/>



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 60х90 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>