Компьютерные системы и сети

Выпуск 1

Компьютерные системы и сети

Серия основана в 2013 году

Москва
Издательство МГТУ им. Н.Э. Баумана
2013

Компьютерные системы и сети

Выпуск 1

Технологии коммутации и маршрутизации в локальных компьютерных сетях

Под общей редакцией А.В. Пролетарского

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

Издательство МГТУ им. Н.Э. Баумана
Москва 2013

УДК 004.7
ББК 32.973.202
Т38

А в т о р ы:
Е.В. Смирнова, А.В. Пролетарский, Е.А. Ромашкина,
А.М. Суровов, Р.А. Федотов

Научный редактор С.В. Козлов (MCSE, MCITP, CCNP, MCT)

Р е ц е н з е н т ы:
зам. директора по образованию и исследованиям Mail.Ru Group *Д.А. Волошин*;
зав. кафедрой «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана
д-р техн. наук, проф. *В.В. Сюзев*

Т38 **Технологии коммутации и маршрутизации в локальных компьютерных сетях** : учеб. пособие / [Е. В. Смирнова, А. В. Пролетарский и др.] ; под общей ред. А.В. Пролетарского. – М. : Изд-во МГТУ им. Н.Э. Баумана, 2013. – 389, [3] с. : ил. – (Компьютерные системы и сети).

ISBN 978-5-7038-3733-7

В учебном пособии изложены основные сведения по фундаментальным технологиям коммутации второго и третьего уровней в локальных компьютерных сетях. Рассмотрены методы начальной настройки и управления коммутаторов D-Link. На практических примерах показаны методы построения виртуальных локальных сетей (VLAN) с применением протоколов семейства STP, технологии агрегирования каналов связи, безопасности (ACL) и обеспечения качества обслуживания (QoS), а также принципы статической и динамической IPv4- и IPv6-маршрутизации. Изложены сведения по многоадресным схемам передачи данных и управлению сетевым оборудованием с помощью протоколов SNMP и RMON. Приведена справочная информация об актуальной линейке моделей коммутаторов D-Link.

Представленные в учебном пособии теоретические положения изложены в терминах учебных материалов компании D-Link и дополнены 24 практическими занятиями (лабораторными работами), охватывающими все рассмотренные в книге темы.

Содержание учебника соответствует программе и курсу лекций, который авторы читают в МГТУ им. Н.Э. Баумана.

Для студентов высших учебных заведений, обучающихся по направлению подготовки «Информатика и вычислительная техника».

УДК 004.7
ББК 32.973.202

ISBN 978-5-7038-3733-7

Оглавление

Предисловие 11
Обозначения, используемые в книге, и синтаксис команд 12

1. Основы коммутации 13
1.1. Эволюция локальных сетей 13
1.2. Функционирование коммутаторов локальной сети 16
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 26
1.7.1. Архитектура с разделяемой шиной 27
1.7.2. Архитектура с разделяемой памятью 28
1.7.3. Архитектура на основе коммутационной матрицы 30
1.8. Характеристики, влияющие на производительность коммутаторов 35
1.8.1. Скорость фильтрации и скорость продвижения кадров 35
1.8.2. Размер таблицы коммутации 37
1.8.3. Объем буфера кадров 37
1.9. Управление потоком в полудуплексном и дуплексном режимах 38
1.10. Технологии коммутации и модель OSI 39
1.11. Программное обеспечение коммутаторов 40
1.12. Общие принципы сетевого дизайна 40
1.13. Трехуровневая иерархическая модель сети 41
1.14. Обзор функциональных возможностей коммутаторов 43

2. Начальная настройка коммутатора 44
2.1. Классификация коммутаторов по возможности управления 44
2.2. Средства управления коммутаторами 44
2.3. Подключение к коммутатору 45
2.4. Начальная конфигурация коммутатора 48
2.4.1. Вызов помощи по командам 48
2.4.2. Базовая конфигурация коммутатора 49
2.5. Подключение к Web-интерфейсу управления коммутатора 54
2.6. Загрузка нового программного обеспечения в коммутатор 56
2.7. Загрузка и резервное копирование конфигурации коммутатора 57

3. Виртуальные локальные сети (VLAN) 58
3.1. Понятие VLAN и их типы 58
3.2. VLAN на основе портов 60
3.3. VLAN на основе стандарта IEEE 802.1Q 62
3.3.1. Некоторые определения IEEE 802.1Q 64
3.3.2. Тег VLAN IEEE 802.1Q 65
3.3.3. Port VLAN ID 66
3.3.4. Продвижение кадров VLAN IEEE 802.1Q 66
3.3.5. Пример настройки VLAN IEEE 802.1Q 70
3.4. Статические и динамические VLAN 72

3.5. Протокол GVRP 73
3.5.1. Таймеры GVRP 74
3.5.2. Пример настройки протокола GVRP 76
3.6. Q-in-Q VLAN 77
3.6.1. Формат кадра Q-in-Q 77
3.6.2. Реализации Q-in-Q 78
3.6.3. Значения TPID в кадрах Q-in-Q 78
3.6.4. Роли портов в Port-based Q-in-Q и Selective Q-in-Q 79
3.6.5. Политики назначения внешнего тега и приоритета в Q-in-Q . . 79
3.6.6. Базовая архитектура сети с функцией Port-based Q-in-Q 79
3.6.7. Пример настройки функции Port-based Q-in-Q 81
3.6.8. Пример настройки функции Selective Q-in-Q 83
3.7. VLAN на основе портов и протоколов — стандарт IEEE 802.1v 83
3.8. Асимметричные VLAN 87
3.9. Функция Traffic Segmentation 89

4. Функции повышения надежности и производительности 92
4.1. Протоколы семейства Spanning Tree Protocol (STP) 92
4.1.1. Понятие петель 92
4.1.2. Построение активной топологии связующего дерева 94
4.1.3. Bridge Protocol Data Unit (BPDU) 96
4.1.4. Состояния портов 98
4.1.5. Таймеры STP 99
4.1.6. Изменение топологии 100
4.1.7. Настройка STP 101
4.2. Rapid Spanning Tree Protocol 102
4.2.1. Роли портов 103
4.2.2. Формат BPDU 104
4.2.3. Быстрый переход в состояние Forwarding 105
4.2.4. Механизм предложений и соглашений 106
4.2.5. Новый механизм изменения топологии 107
4.2.6. Стоимость пути RSTP 109
4.2.7. Совместимость с STP 109
4.2.8. Настройка RSTP 110
4.3. Multiple Spanning Tree Protocol 111
4.3.1. Логическая структура MSTP 111
4.3.2. Multiple Spanning Tree Instance (MSTI) 114
4.3.3. Формат MSTP BPDU 114
4.3.4. Вычисления топологий MSTP 114
4.3.5. Роли портов MSTP 116
4.3.6. Пример топологии MSTP 118
4.3.7. Состояние портов MSTP 120
4.3.8. Счетчик переходов MSTP 120
4.3.9. Настройка протокола MSTP на коммутаторах 120
4.4. Функция LoopBack Detection 124
4.5. Обеспечение безопасности STP 126
4.6. Агрегирование каналов связи 126

5. Адресация сетевого уровня и маршрутизация 133
5.1. Сетевой уровень 133
5.2. Обзор адресации сетевого уровня 134
5.2.1. Формат пакета IPv4 135
5.2.2. Представление и структура адреса IPv4 136
5.2.3. Классовая адресация IPv4 138
5.2.4. Частные и публичные адреса IPv4 139
5.3. Формирование подсетей 140
5.4. Бесклассовая адресация IPv4 144
5.5. Способы настройки IPv4-адреса 146
5.6. Протокол IPv6 146
5.6.1. Формат заголовка IPv6 147
5.6.2. Представление и структура адреса IPv6 150
5.7. Типы IPv6-адресов 151
5.7.1. Индивидуальные адреса 152
5.7.2. Групповые адреса 154
5.7.3. Альтернативные адреса 156
5.8. Формирование идентификатора интерфейса 158
5.9. Способы настройки IPv6-адреса 159
5.10. Планирование подсетей IPv6 161
5.11. Протокол NDP 162
5.11.1. Разрешение IPv6-адресов с помощью протокола NDP и определение недоступности соседа 163
5.11.2. Проверка дублирования адресов 166
5.11.3. Обнаружение маршрутизатора 166
5.12. Маршрутизация 167
5.12.1. Процесс обработки пакета маршрутизирующим устройством 169
5.12.2. Коммутация третьего уровня 170
5.12.3. Статическая и динамическая маршрутизация 171
5.12.4. Протоколы динамической маршрутизации 173
5.13. Дистанционно-векторные протоколы маршрутизации 176
5.13.1. Принцип работы дистанционно-векторного алгоритма маршрутизации 177
5.13.2. Проблемы функционирования дистанционно-векторного алгоритма маршрутизации 178
5.14. Протокол RIP 182
5.14.1. Протокол RIPv1 183
5.14.2. Протокол RIPv2 186
5.14.3. Протокол RIPng 189
6. Качество обслуживания (QoS) 191
6.1. Модели QoS 191
6.2. Приоритизация пакетов 192
6.3. Классификация пакетов 193
6.4. Маркировка пакетов 194
6.5. Управление перегрузкой сети и механизмы обслуживания очередей 195
6.6. Механизм предотвращения перегрузок 197
6.7. Контроль полосы пропускания 199

7. Функции обеспечения безопасности и ограничения доступа к сети . . . 204
7.1. Общие сведения о методах обеспечения безопасности в компьютерных сетях . . . 204
7.2. Списки контроля доступа (ACL) . . . 205
7.2.1. Профили доступа и правила ACL . . . 206
7.2.2. Примеры настройки ACL . . . 210
7.3. Функции контроля подключения узлов к портам коммутатора . . . 212
7.3.1. Функция Port Security . . . 212
7.3.2. Функция IP-MAC-Port Binding . . . 215
7.4. 802.1X-аутентификация . . . 218
7.4.1. Роли устройств в стандарте 802.1X . . . 219
7.4.2. Port-Based 802.1X . . . 221
7.4.3. MAC-Based 802.1X . . . 222
7.4.4. Состояние портов коммутатора . . . 224
7.5. 802.1X Guest VLAN . . . 225
7.6. Функции защиты ЦПУ коммутатора . . . 232
8. Групповая рассылка . . . 236
8.1. Общие сведения . . . 236
8.2. IP-адресация групповой рассылки . . . 236
8.3. MAC-адреса групповой рассылки . . . 238
8.4. Создание и обслуживание групп . . . 239
8.5. Управление групповой рассылкой на втором уровне модели OSI (IGMP Snooping) . . . 239
8.6. Функция IGMP Snooping Fast Leave . . . 242
9. Функции управления коммутаторами . . . 244
9.1. Управление множеством коммутаторов . . . 244
9.1.1. Объединение коммутаторов в физический стек . . . 244
9.1.2. Виртуальный стек. Технология Single IP Management (SIM) . . . 249
9.2. Протокол SNMP . . . 254
9.2.1. Компоненты SNMP . . . 254
9.2.2. База управляющей информации SNMP . . . 255
9.2.3. Типы сообщений протокола SNMP . . . 256
9.2.4. Безопасность SNMP . . . 257
9.2.5. Пример настройки протокола SNMP . . . 258
9.3. RMON (Remote Monitoring) . . . 259
9.4. Функция Port Mirroring . . . 261
10. Обзор коммутаторов D-Link . . . 262
10.1. Неуправляемые коммутаторы . . . 262
10.2. Коммутаторы серии Smart . . . 264
10.3. Управляемые коммутаторы . . . 267
Лабораторные работы по курсу «Технологии коммутации современных сетей Ethernet. Базовый курс D-Link» (с применением коммутаторов DES-3810-28 и DES-3528) . . . 275
Рекомендации по организации лабораторных работ . . . 275
Лабораторная работа № 1. Основные команды коммутатора . . . 275
1.1. Вызов помощи по командам . . . 277
1.2. Изменение IP-адреса коммутатора . . . 279

1.3. Настройка даты и времени на коммутаторе 280
1.4. Управление учетными записями пользователей 280
1.5. Управление возможностью доступа к коммутатору через Web-интерфейс и Telnet 281
1.6. Настройка баннера приветствия 282
1.7. Настройка основных параметров портов коммутатора 283
1.8. Сохранение конфигурации в энергонезависимой памяти 284
1.9. Команды мониторинга сети 285
1.10. Функция Factory Reset (сброс к заводским установкам) 286
Лабораторная работа № 2. Обновление программного обеспечения коммутатора и сохранение/восстановление конфигурационных файлов 286
2.1. Подготовка к режиму обновления и сохранения программного обеспечения коммутатора 287
2.2. Загрузка файла программного обеспечения в память коммутатора 288
2.3. Настройка порядка загрузки программного обеспечения коммутатора 288
2.4. Выгрузка и загрузка конфигурации 289
2.5. Выгрузка log-файлов 290
Лабораторная работа № 3. Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы 290
3.1. Команды управления таблицей коммутации 291
3.2. Команды управления ARP-таблицей 291
3.3. Команды просмотра таблицы коммутации 3-го уровня 292
Лабораторная работа № 4. Настройка VLAN на основе стандарта IEEE 802.1Q 292
4.1. Настройка VLAN на основе стандарта IEEE 802.1Q 294
4.2. Настройка сегментации трафика внутри VLAN 295
4.3. Оптимизация настройки коммутаторов с большим количеством VLAN 296
Лабораторная работа № 5. Настройка протокола GVRP 297
Лабораторная работа № 6. Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q 300
Лабораторная работа № 7. Настройка протоколов связующего дерева STP, RSTP, MSTP 304
7.1. Мониторинг и диагностика сети во время широковещательного шторма, вызванного наличием петли 306
7.2. Настройка протокола RSTP 308
7.3. Настройка защиты от несанкционированного подключения корневых коммутаторов 310
7.4. Настройка защиты от получения ложных кадров об изменении топологии 311
7.5. Настройка протокола MSTP 312
Лабораторная работа № 8. Настройка функции защиты от образования петель LoopBack Detection 315
8.1. Настройка функции LoopBack Detection Independent STP в режиме Port-Based 316
8.2. Настройка функции LoopBack Detection Independent STP в режиме VLAN-Based 317

Лабораторная работа № 9. Агрегирование каналов. 319
Лабораторная работа № 10. Списки контроля доступа (Access Control List) 323
10.1. Настройка ограничения доступа пользователей к серверу по IP-адресам 324
10.2. Настройка фильтрации кадров по MAC-адресам 326
Лабораторная работа № 11. Контроль подключения узлов к портам коммутатора. Функция Port Security 328
11.1. Управление количеством подключаемых к портам коммутатора узлов путем ограничения максимального количества изучаемых MAC-адресов 329
11.2. Настройка защиты от подключения к портам, основанной на статической таблице MAC-адресов 331
Лабораторная работа № 12. Контроль над подключением узлов к портам коммутатора. Функция IP–MAC–Port Binding 332
12.1. Настройка работы функции IP–MAC–Port Binding в режиме ARP 334
12.2. Настройка работы функции IP–MAC–Port Binding в режиме ACL 335
Лабораторная работа № 13. Настройка QoS. Приоритизация трафика. Управление полосой пропускания. 336
Лабораторная работа № 14. Функции анализа сетевого трафика 340
Лабораторная работа № 15. Настройка протокола LLDP 342
Лабораторная работа № 16. Настройка статической и динамической маршрутизации 345
Лабораторная работа № 17. Итоговая самостоятельная работа 353
17.1. Подготовительная работа 354
17.2. Выполнение работы 355
17.3. Ожидаемый результат 355
Лабораторная работа № 18. Настройка асимметричных VLAN. 357
Лабораторная работа № 19. Настройка сегментации трафика без использования VLAN 358
Лабораторная работа № 20. Настройка функции Q-in-Q (Double VLAN) 360
Лабораторная работа № 21. Установка и настройка протокола IPv6 на рабочей станции и коммутаторе D-Link. 363
21.1. Установка и настройка протокола IPv6 на рабочей станции. . . . 365
21.2. Настройка автоматической конфигурации (Stateless autoconfiguration) IPv6-адреса 366
21.3. Подключение к коммутатору через Web-интерфейс с помощью IPv6-адреса 367
Лабораторная работа № 22. Разрешение IPv6-адресов с помощью протокола Neighbor Discovery Protocol (NDP) 368
Лабораторная работа № 23. Списки контроля доступа (Access Control List) для IPv6 370
Лабораторная работа № 24. Настройка статической IPv6-маршрутизации 372
Глоссарий 374
Список литературы 391

Предисловие

Учебное пособие разработано для подготовки специалистов по конфигурированию, администрированию и мониторингу компьютерных сетей. В нем рассматриваются фундаментальные основы наиболее распространенных сетевых технологий, изучение которых является частью учебного плана студентов, обучающихся по направлению «Информатика и вычислительная техника». Пособие содержит 20 практических занятий на основе оборудования (коммутаторов) компании D-Link. Оно является результатом многолетнего сотрудничества Московского государственного технического университета им. Н.Э. Баумана и компании D-Link. В его основу легли материалы занятий, проводимых в учебном центре «МГТУ — D-Link», а также ранее изданных учебных пособий и методических указаний к лабораторным работам по коммутируемым сетям.

В главе 1 представлена эволюция компьютерных сетей, основные методы коммутации и архитектура коммутаторов, главные принципы сетевого дизайна, а также функциональные возможности коммутаторов.

Глава 2 посвящена первоначальной настройке коммутаторов и работе с Web-интерфейсом управления коммутатором.

В главе 3 рассматриваются виртуальные локальные сети (VLAN), их типы, протокол GVRP, Q-in-Q VLAN, VLAN на основе портов и протоколов — стандарт IEEE 802.1v, асимметричные VLAN, функция Traffic Segmentation.

Глава 4 посвящена рассмотрению функции повышения надежности и производительности коммутируемых соединений.

В главе 5 описана адресация сетевого уровня и маршрутизация, в том числе протоколы IPv4 и IPv6.

Глава 6 посвящена вопросам качества обслуживания (Quality of Service, QoS), в частности, управлению перегрузками и механизмам обслуживания очередей, контролю полосы пропускания. Приведен пример настройки QoS.

В главе 7 рассмотрены методы и функции обеспечения безопасности и ограничения доступа к сети.

В главе 8 представлена организация и управление многоадресной рассылкой.

Глава 9 посвящена изучению функции управления коммутаторами, а глава 10 — обзору коммутаторов D-Link.

Издание содержит обширный глоссарий и 24 практических занятий, позволяющих закрепить изученный материал. Каждое практическое занятие предваряется кратким теоретическим материалом. Выполнение всех занятий учебного пособия позволит получить представление о работе коммутаторов, самостоятельно конфигурировать и администрировать коммутируемые сети.

Издание подготовлено преподавателями МГТУ им. Н.Э. Баумана и Центра развития сетевых компьютерных технологий «МГТУ — D-Link» совместно со специалистами компании D-Link.

Обозначения, используемые в книге, и синтаксис команд

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

Для описания ввода команд, ожидаемых значений и аргументов при настройке коммутатора через интерфейс командной строки (CLI) используются следующие символы:

<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} содержат необязательное значение или набор необязательных аргументов.

1. Основы коммутации

1.1. Эволюция локальных сетей

Эволюция локальных сетей неразрывно связана с развитием технологии Ethernet, которая по сей день остается самой распространенной технологией локальных сетей. Первоначально она рассматривалась как экономичная технология, обеспечивающая совместное использование данных, дискового пространства и дорогостоящих периферийных устройств. Снижение стоимости персональных компьютеров и периферии привело к увеличению числа сетевых пользователей. 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 клиент-серверные архитектуры, и, как следствие, сети стали обязательным инструментом в бизнесе, обеспечив наиболее эффективную обработку информации.

В первых сетях Ethernet (10Base-2 и 10Base-5) использовалась физическая шинная топология, когда каждый компьютер соединялся с другими устройствами с помощью единого коаксиального кабеля, используемого в качестве среды передачи данных. Сетевая среда была разделяемой (все устройства находились в одном домене коллизий (Collision Domain)), 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: ограничены по размеру, функциональности и расширяемости, недостаточно надежны, а также неспособны справляться со значительным увеличением сетевого трафика. Для повышения эффективности работы локальных сетей требовались новые решения.

Следующим шагом стала разработка стандарта 10Base-T с физической топологией типа «звезда», в которой каждый узел подключался отдельным кабелем к центральному устройству — *концентратору* (*hub*), работающему на физическом (первом) уровне модели OSI и повторяющему сигналы, поступившие с одного из его портов на все остальные активные порты. Использование концентраторов позволило повысить надежность сети, так как обрыв одного из кабелей не приводил к сбою в работе сети. Несмотря на то что использование концентраторов в сети упростило задачи ее управления и сопровождения, среда передачи оставалась разделяемой. Помимо этого общее количество концентраторов и соединяемых ими сегментов сети было ограничено из-за временных задержек и других причин.

Задача *сегментации* сети, т. е. разделения устройств на группы (сегменты) в соответствии с их физическим размещением с целью уменьше-

2. Начальная настройка коммутатора

2.1. Классификация коммутаторов по возможности управления

По возможности управления существует три категории коммутаторов:

• *неуправляемые коммутаторы* — не поддерживают возможности управления и обновления программного обеспечения;

• *управляемые коммутаторы* — являются сложными устройствами, позволяющими выполнять набор функций уровней 2 и 3 модели OSI. Управление ими может осуществляться посредством Web-интерфейса, командной строки через консольный порт или удаленно по протоколу SSH, а также с помощью протокола SNMP и т. д.;

• *настраиваемые коммутаторы* — предоставляют пользователям возможность настраивать определенные параметры с помощью простых утилит управления, Web-интерфейса, упрощенного интерфейса командной строки, протокола SNMP.

2.2. Средства управления коммутаторами

Большинство современных коммутаторов поддерживает различные функции управления и мониторинга. К ним относятся Web-интерфейс управления (WUI), интерфейс командной строки (Command Line Interface, CLI), протоколы Telnet, SSH, SNMP. В коммутаторах D-Link серии Smart также реализована поддержка начальной настройки и обновления программного обеспечения с помощью утилиты D-Link SmartConsole Utility.

Web-интерфейс управления позволяет осуществлять настройку и мониторинг параметров коммутатора, используя любой компьютер, оснащенный Web-браузером. Главная страница Web-интерфейса обеспечивает доступ к различным настройкам коммутатора и отображает всю необходимую информацию об устройстве. Администратор может просмотреть статус устройства, статистику производительности и т. д. и произвести необходимые настройки.

Доступ к интерфейсу командной строки коммутатора осуществляется подключением к его консольному порту персонального компьютера с установленной программой эмуляции терминала. Этот метод наиболее удобен при первоначальном подключении к коммутатору, когда IP-адрес не известен или не настроен, в случае необходимости восстановления пароля и при выполнении расширенных настроек коммутатора. Безопасный доступ к интерфейсу командной строки может быть получен по сети с помощью протокола SSH.

Администратор может выбрать для настройки коммутатора любой удобный ему интерфейс управления, так как набор доступных через раз-

3. Виртуальные локальные сети (VLAN)

3.1. Понятие VLAN и их типы

Коммутатор Ethernet является устройством канального уровня. В соответствии с логикой работы рассылка широковещательных кадров будет осуществляться через все порты (за исключением порта-приемника такого кадра). Хотя трафик с конкретными адресами (соединения «точка — точка») изолирован парой портов, широковещательные кадры передаются во всю сеть (на каждый порт).

Широковещательные кадры используются при работе многих сетевых протоколов, таких как ARP, BOOTP или DHCP. Большой объем широковещательных кадров в сети приводит к нерациональному использованию полосы пропускания, особенно в крупных сетях. Для снижения этого эффекта ограничивают область распространения широковещательного трафика (эта область называется *широковещательным доменом*); организуют 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, полностью изолирован от других узлов сети на канальном уровне. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса (индивидуального, группового или широковещательного). В то же время внутри виртуальной сети кадры передаются по технологии коммутации, т. е. 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 приводить к широковещательным штормам и существенно снижать производительность сети.

VLAN обладают следующими преимуществами:

- гибкость внедрения — VLAN являются эффективным способом группировки сетевых узлов в виртуальные рабочие группы независимо от их физического размещения в сети;
- ограничивают распространение широковещательного трафика, что увеличивает полосу пропускания, доступную для пользователя;
- 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 решении типовой задачи организации доступа в интернет сотрудникам офиса при условии изоляции трафика разных отделов.

4. Функции повышения надежности и производительности

4.1. Протоколы семейства Spanning Tree Protocol (STP)

В настоящее время для повышения надежности и производительности каналов связи существует ряд протоколов и функций. Наиболее распространены методы создания резервных связей между коммутаторами на основе двух технологий:

- резервирование соединений с помощью протоколов семейства Spanning Tree;
- балансировка нагрузки, обеспечивающая параллельную передачу данных по всем альтернативным соединениям с помощью механизма агрегирования портов (см. раздел 4.6).

Перейдем к рассмотрению протокола связующего дерева. Spanning Tree Protocol (STP) является протоколом 2-го уровня модели OSI и позволяет строить древовидные свободные от петель конфигурации связей между коммутаторами локальной сети. Помимо этого STP обеспечивает возможность автоматического резервирования альтернативных каналов связи между коммутаторами на случай выхода из строя активных каналов.

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).

4.1.1. Понятие петель

Для обеспечения избыточности между коммутаторами можно создать несколько соединений. При этом могут возникать коммутационные петли, предполагающие существование нескольких маршрутов по промежуточным сетям. Следует отметить, что сеть с несколькими маршрутами между источником и приемником отличается повышенной отказоустойчивостью. Хотя наличие избыточных каналов связи полезно, петли тем не менее создают проблемы, наиболее актуальными из которых являются:

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

Широковещательный шторм. Предположим, что кадр, поступивший от одного из узлов, является широковещательным. В этом случае коммутаторы будут пересылать кадры бесконечно, как показано на рис. 4.1, используя всю доступную полосу пропускания сети и блокируя передачу других кадров во всех сегментах.

5. Адресация сетевого уровня и маршрутизация

5.1. Сетевой уровень

При построении сетей передачи данных возникает задача организации связи между различными сетями или подсетями, образующими *составную сеть* (*internetwork*) (рис. 5.1). Так например, в локальных сетях, логически сегментированных с использованием VLAN, администраторам зачастую требуется организовать передачу данных между ними. Эта задача решается с помощью функций *сетевого уровня* (*network layer*) модели OSI.

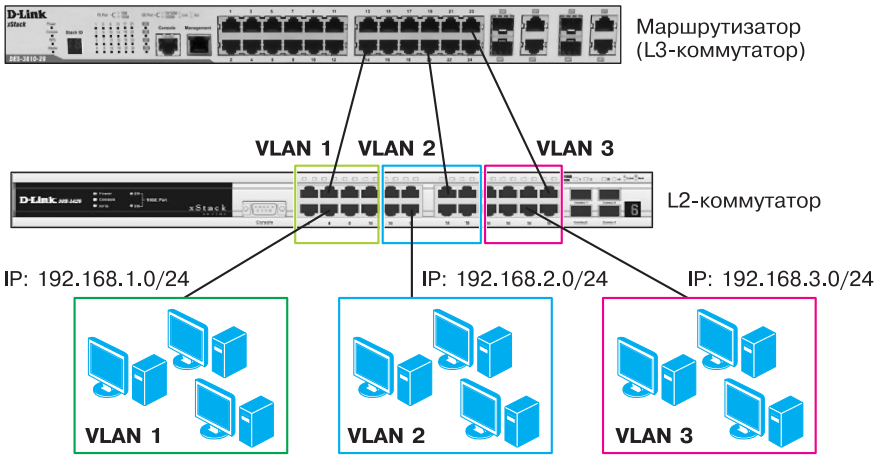

Рис. 5.1. Составная сеть

В наиболее распространенном в настоящее время стеке протоколов TCP/IP за обработку данных на сетевом уровне отвечает протокол IP, который позволяет доставлять данные в сетях TCP/IP между любыми узлами составной сети и выполняет две основные функции:

- маршрутизация;
- адресация узлов (IP-адресация).

Маршрутизация — это выбор наилучшего маршрута передачи пакета сетевого уровня от источника к получателю.

Протокол IP не гарантирует надежной доставки пакета до адресата, эта функция выполняется протоколами более высокого уровня. Такой тип доставки данных называют *best-effort*. В настоящее время существует две версии протокола IP:

- IP версии 4 (IPv4), который использует 32-битные адреса;
- IP версии 6 (IPv6), который использует 128-битные адреса.

6. Качество обслуживания (QoS)

6.1. Модели QoS

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

Функции QoS 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.

1. *Негарантированная доставка данных* (*Best Effort Service*) — обеспечивает связь между узлами, но не гарантирует надежную доставку данных, время доставки, пропускную способность и определенный приоритет.

2. *Интегрированные услуги* (*Integrated Services, IntServ*) — эта модель описана в RFC 1633 и предполагает предварительное резервирование сетевых ресурсов, гарантируя предсказуемое поведение сети для приложений, требующих для нормального функционирования 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) 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*) из-за предъявления строгих требований к ресурсам сети.

3. *Дифференцированное обслуживание* (*Differentiated Service, DiffServ*) — эта модель описана в RFC 2474, RFC 2475 и предполагает разделение трафика на классы на основе требований к качеству обслуживания.

7. Функции обеспечения безопасности и ограничения доступа к сети

7.1. Общие сведения о методах обеспечения безопасности в компьютерных сетях

Для любого системного администратора одной из наиболее важных задач остается обеспечение безопасности компьютерной сети. Эту задачу призваны решать межсетевые экраны, однако зачастую «первый удар» принимают на себя именно коммутаторы, поэтому в настоящее время они обладают широкими функциональными возможностями для обеспечения безопасности. Речь идет не о защите сетей от атак извне, а в большей степени о всевозможных атаках изнутри сети, таких как подмена DHCP-серверов, атаки типа DoS, ARP Spoofing, неавторизованный доступ и т. д. В некоторых случаях коммутаторы не способны полностью защитить сеть от подобного рода атак, но могут значительно ослабить угрозы их возникновения. Данная глава посвящена основным принципам обеспечения сетевой безопасности на базе оборудования D-Link.

Прежде чем приступить к рассмотрению темы, уточним некоторые понятия.

Аутентификация — процедура проверки подлинности субъекта на основе предоставленных им о себе данных в какой-либо форме (логин—пароль, цифровой сертификат, сведения с биометрического датчика и т. д.).

Авторизация — предоставление субъекту определенных прав (полномочий) на выполнение некоторых действий.

Как правило, за авторизацией следует аутентификация.

D-Link предлагает комплексный подход для 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 содержит 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).

8. Групповая рассылка

8.1. Общие сведения

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

- индивидуальная (Unicast) передача;
- широковещательная (Broadcast) передача;
- групповая, или многоадресная (Multicast), рассылка.

При *индивидуальной 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.

Групповая рассылка обеспечивает доставку потока данных группе узлов на IP-адрес группы рассылки. У этой группы нет физических или географических ограничений: узлы могут находиться в любой точке глобальной сети. 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 групповой рассылки, содержащие в поле назначения заголовка групповой адрес, будут поступать на этот узел и обрабатываться.

Групповая рассылка имеет ряд преимуществ при работе таких приложений, как видеоконференции, корпоративная связь, дистанционное обучение, видео и аудио-трансляции и т. д., так как позволяет значительно повысить эффективность использования полосы пропускания и распределения информации среди больших групп получателей: отправитель передает единственную копию пакета данных всем членам группы, а не рассылает множество копий, благодаря чему снижается нагрузка на канал связи.

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

8.2. IP-адресация групповой рассылки

Источник многоадресного трафика направляет пакеты не на индивидуальные IP-адреса узлов-получателей, а на групповой IP-адрес. Групповые адреса определяют произвольную группу 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 групповой рассылки IPv4-адреса класса D в диапазоне от 224.0.0.0 до 239.255.255.255. Адреса, назначенные IANA, приведены в табл. 8.1. Более подробную ин-

9. Функции управления коммутаторами

9.1. Управление множеством коммутаторов

Для независимого управления группой коммутаторов требуется выделить каждому устройству отдельный IP-адрес, что ведет к неэкономному использованию адресного пространства и необходимости фиксации администратором IP-адреса каждого коммутатора. D-Link предлагает два подхода к управлению группой коммутаторов: физическое и виртуальное стекирование коммутаторов.

Оба эти подхода предполагают объединение коммутаторов в физическую или логическую группу, управление которой будет осуществляться 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, SSH, протокол SNMP, и только одному коммутатору (мастер-коммутатору) потребуется присвоение управляющего IP-адреса.

Передача данных между коммутаторами стека ведется в полнодуплексном режиме. Коммутаторы могут быть объединены в стек кольцевой или линейной топологии. Одним из преимуществ стека кольцевой 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 только для передачи пакетов с индивидуальными адресами.

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 передает-

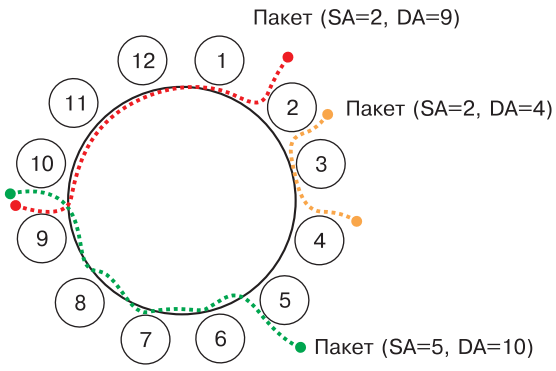

Рис. 9.1. Пример выбора оптимального пути передачи пакета в кольцевом стеке

10. Обзор коммутаторов D-Link

10.1. Неуправляемые коммутаторы

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

Неуправляемые коммутаторы (*Unmanaged Switches*) D-Link являются решением для развертывания 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 Green Ethernet, диагностика кабеля, управление потоком (IEEE 802.3x), автоматическое определение полярности кабелей (MDI/MDIX), возможность передачи Jumbo-фреймов и приоритизацию трафика (рис. 10.1). Неуправляемые коммутаторы не поддерживают функции управления и обновления ПО.

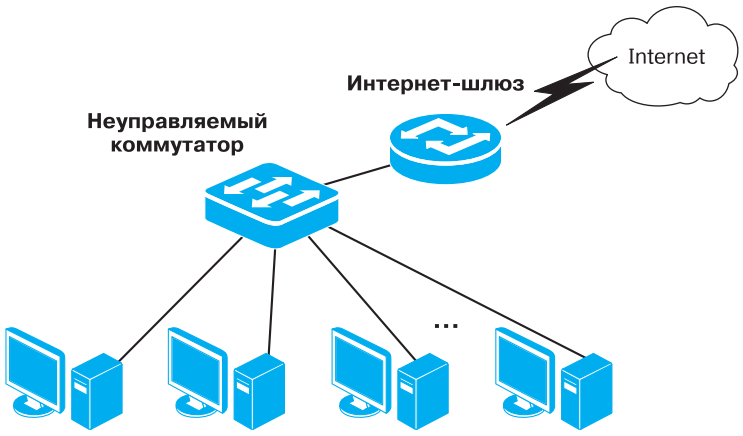

Рис. 10.1. Неуправляемый коммутатор D-Link в сети небольшой рабочей группы

Неуправляемые коммутаторы D-Link представлены сериями DES-10xx, DES-10xxA, DES-10xxD/RU, DGS-10xxD/RU, DGS-10xxD и DGS-10xxA.

Серия DES-10xx включает в себя модели коммутаторов Fast Ethernet с различным количеством портов 10/100 Мбит/с (от 5 до 48) в настольном (рис. 10.2) и стоечном исполнении. Модели DES-1026G и DES-1050G этой серии также оснащены двумя портами Gigabit Ethernet.

Лабораторные работы по курсу «Технологии коммутации современных сетей Ethernet. Базовый курс D-Link»
(с применением коммутаторов DES-3810-28 и DES-3528)

Рекомендации по организации лабораторных работ

Для выполнения настоящих лабораторных работ рекомендуется следующий комплект оборудования на учебную группу, состоящую из 10 человек:

Коммутатор DES-3810-28	6 шт.
Коммутатор DES-3528	8 шт.
Коммутатор DES-1005A	5 шт.
Рабочая станция	20 шт.
Кабель Ethernet	35 шт.
Консольный кабель	11 шт.

Каждая лабораторная работа содержит схему установки с указанием количества рабочих мест, на которое она рассчитана.

Настройка коммутаторов осуществляется через интерфейс командной строки путем подключения управляющей рабочей станции к его консольному порту.

Команды в лабораторных работах приведены для коммутаторов со следующими версиями программного обеспечения:

коммутатор DES-3810-28 — ПО версии 2.10.b024 или выше;

коммутатор DES-3528 — ПО версии 2.80.b042 или выше.

Для проведения лабораторных работ потребуется следующее ПО:

1. Генератор трафика iperf (http://sourceforge.net/projects/iperf/).
2. TFTP-сервер Tftpd32 (http://tftpd32.jounin.net).
3. Анализатор трафика Wireshark (http://www.wireshark.org).
4. Программа эмуляции терминала Putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).

Лабораторные работы № 18—24 выполняются факультативно по решению преподавателя.

Лабораторная работа № 1. Основные команды коммутатора

Для настройки различных функций коммутаторов при выполнении практических работ будет использоваться интерфейс командной строки (CLI), так как он обеспечивает возможность тонкой настройки устройства.

Все команды CLI являются чувствительными к регистру, поэтому прежде чем вводить команду, необходимо убедиться, что отключены все функции, которые могут привести к изменению регистра текста.

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 субъекту на выполнение некоторых действий.

• **Логирование (Accounting)**. Слежение за использованием пользователем сетевых ресурсов.

Access layer. Уровень доступа. Является нижним уровнем иерархической модели сети и управляет доступом узлов к ресурсам объединенной сети. Основной задачей уровня доступа является создание точек входа в сеть.

ACL (*англ*. Access Control List**)**. Список управления доступом. Список управления доступом является средством фильтрации потоков данных на аппаратном уровне. Используя ACL, можно ограничить типы приложений, разрешенных для использования в сети, контролировать доступ пользователей к устройствам сети. 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 частями. Применительно к SNMP термин *агент* означает программный модуль, который находится на управляемом сетевом устройстве (маршрутизаторе, коммутаторе, точке доступа, принтере и т. д.). Агент обслуживает базу управляющей информации и отвечает на запросы менеджера SNMP.

Auto-negotiation. Автосогласование. Функция, обеспечивающая механизм автоматической настройки портов 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. Используется для динамического преобразования IPv4-адресов в физические (аппаратные) MAC-адреса устройств локальной сети. В общем случае ARP требует передачи широковещательного сообщения всем узлам, на которое отвечает узел с соответствующим запросу IPv4-адресом.

ASIC (*англ*. Application Specific Integrated Circuit**)**. Специализированная интегральная схема (ИС). Современные контроллеры ACIS зачастую содержат на одном кристалле 32-битовые 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 объем трафика и которая является 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, доступная или занимаемая для передачи потока данных, измеряется в Кбит/с, Мбит/с, Гбит/с.

BGP (*англ*. Border Gateway Protocol). Протокол пограничного шлюза. Обеспечивает динамическую маршрутизацию в сети интернет. Регламентируется RFC 4271.

BOOTP (*англ*. Bootstrap Protocol**).** Протокол загрузки. Сетевой протокол, используемый для удаленной загрузки бездисковых рабочих станций, позволяющий 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.

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 две физические сети и передающее кадры из одной сети в другую. Мосты работают на канальном (втором) 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 и могут вызвать отказ работы 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. См. также *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 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. См. также *CBS* и *EBS*.

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

Client. Клиент. Узел или программное обеспечение, которое запрашивает у сервера доступ к некоторым сервисам.

Collision. Коллизия. Возникает в сети Ethernet, когда два узла одновременно начинают передачу. Передаваемые ими по физическому носителю кадры пересекаются, что приводит к потере данных.

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 управляемом устройстве (коммутаторе, маршрутизаторе и т.п.), к которому подключается терминальный клиент. Этот порт используется для выделенного локального управления.

Core layer. Уровень ядра. Является верхним в иерархической модели сети и отвечает за надежную и быструю передачу больших объемов данных. Трафик, передаваемый через ядро, является общим для большинства узлов.

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 кадров 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 получателя (первые 6 байт после префикса) и сразу начинает передавать кадр, не дожидаясь его полного приема. Коммутация без буферизации уменьшает задержку, но не выполняет проверку на ошибки.

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. Такие коммутаторы обычно обладают относительно небольшим количеством фиксированных портов, внешним или внутренним блоком питания и ножками 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.

Diffserv (*англ*. Differentiated Services). 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. Распределенная иерархическая система получения информации об именах и IP-адресах компьютеров в локальных и глобальных сетях. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации для маршрутизации почты, а также об узлах, обслуживающих отдельные протоколы 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.

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. См. также *CBS* и *CIR*.

EAP (*англ*. Extensible Authentication Protocol**)**. Расширяемый протокол 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 (LAN), описанный в спецификации IEEE 802.3. Ethernet использует метод доступа к среде CSMA/CD. Развитием технологии Ethernet 10Base-T 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). Решение ETTH заключается в передаче данных, речи и видео по относительно простым и недорогим сетям Ethernet.

F

FDB (*англ*. Forwarding DataBase). 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). Решение FTTH заключается в передаче данных, речи и видео по сети Ethernet с оптическим волокном в качестве среды передачи данных, что позволяет обеспечить доступ к сети непосредственно из помещений клиентов услуг на высоких скоростях.

Filtering. Фильтрация. Процесс проверки пакетов в сети и определения адресатов для принятия решения о дальнейшей пересылке (данная локаль-

ная сеть, удаленная локальная сеть) или отбрасывании пакета. Фильтрация пакетов выполняется мостами, коммутаторами и маршрутизаторами.

Flooding. Лавинная передача. Способ передачи трафика, используемый в коммутаторах, 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 передачи пакета к месту его назначения с помощью 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 байт кадра, что позволяет ему отфильтровывать коллизионные кадры перед их передачей.

Frame. Кадр. Единица передаваемой информации на канальном уровне сетевой модели. В LAN 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. Является протоколом 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 автоматически 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, выбирая в интерфейсе графические элементы 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. 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, адресов и уникальных параметров протоколов Интернет.

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, если запрашиваемая услуга недоступна или узел не отвечает. Также на ICMP возлагаются некоторые сервисные функции. Регламентируется RFC 792.

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 многоадресных группах локальной сети. Узлы сети определяют принадлежность к группе, посылая IGMP-сообщения на свой локальный маршрутизатор. Регламентируется RFC 1112, 2236, 3376.

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.

IP (*англ*. Internet Protocol). Протокол интернета. Часть стека протоколов TCP/IP. Описывает программную маршрутизацию пакетов и адресацию устройств. Обеспечивает передачу пакетов без организации соединений и гарантии доставки. Регламентируется RFC 791.

IP address. IP-адрес. Адрес для протокола IP версии 4 (IPv4) — 32-битовое (4 байт) значение, определенное в STD 5 (RFC 791) и используемое для представления точек подключения в сети TCP/IP. IP-адрес состоит из номера сети и номера хоста — такое разделение позволяет сделать маршрутизацию более эффективной. Обычно для записи IP-адресов используют десятичную нотацию с разделением точками. Новая версия протокола IP версии 6 (IPv6) использует 128-битовые 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 интернета.

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 (L2-коммутатор). Анализирует входящие кадры и принимает решение об их дальнейшей передаче на основе MAC-адресов канального уровня модели OSI.

L3 switch. Коммутатор 3-го уровня (L3-коммутатор). Выполняет L2-коммутацию в пределах рабочей группы аналогично L2-коммутаторам и маршрутизацию между различными подсетями или виртуальными локальными сетями.

LAN (*англ*. Local Area Network). Локальная сеть. Высокоскоростная компьютерная сеть, покрывающая относительно небольшую площадь. Локаль-

ные сети объединяют рабочие станции, периферийные и другие устройства, находящиеся в одном здании или на единой сравнительно небольшой территории.

Latency. Задержка. Временна̀я задержка между моментом получения устройством пакета и моментом отправки пакета на порт назначения.

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

Load Balancing. Балансировка нагрузки. Процесс распределения выполняющихся заданий между несколькими устройствами сети с целью оптимизации использования ресурсов и сокращения времени вычисления.

M

MAC address. MAC-адрес. Адрес канального уровня, задаваемый для каждого порта или устройства, подключенного к сети Ethernet. Длина MAC-адреса составляет 6 байт, а их 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 по протоколу IEEE 802.1X, используя в качестве источника аутентификации MAC-адрес сетевой платы компьютера пользователя.

Managed switch. Управляемый коммутатор. Управляемые коммутаторы являются сложными сетевыми устройствами, позволяющими выполнять расширенный набор функций 2 и 3 уровня модели OSI. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протоколов 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 прочитаны или изменены с помощью команд SNMP и сетевой системы управления (например, D-Link D-View).

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 осуществляя 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, который можно передать через данный интерфейс или канал связи.

Multicast. Групповая рассылка. Доставка потока данных группе узлов на специальный групповой IP-адрес.

Multicast address. Многоадресный (групповой) адрес. Адрес некоторой группы из нескольких сетевых устройств.

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

Multicast router. Маршрутизатор с поддержкой групповых рассылок. Используется для получения IGMP-ответов и периодической отправки IGMP-запросов о принадлежности узлов к многоадресной группе, чтобы определить, какие группы 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 проверки соответствия компьютеров корпоративным политикам (например, политикам безопасности).

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

Non-blocking switch fabric. «Неблокирующая» матрица коммутации. Ее производительность не зависит от типа коммутируемого трафика и равна сумме скоростей всех портов.

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

NVRAM (*англ*. NonVolatile RAM). Энергонезависимое 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.

P

Packet. Пакет. Группа бит, 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, все его поля обрабатываются одновременно.

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

Ping (*англ*. Packet INternet Groper). Проверка доступности адресата. Инструмент, используемый для проверки доступности адресата в IP-сетях с помощью эхо-сообщения протокола ICMP и ответа на него.

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

PoE Plus (*англ*. Power over Ethernet Plus, также PoE+). Технология передачи питания по кабелю типа «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 сетевого оборудования.

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

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

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. Набор моделей, обеспечивающих показатели эффективности системы передачи данных, которые отражают качество передачи различного трафика.

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 аутентификации, авторизации и сбора сведений об использованных ресурсах. Регламентируется RFC 2865.

Rack mounted switch. Коммутаторы, монтируемые в 19” телекоммуникационную стойку.

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

Redundancy. Избыточность. Дублирование устройств, сервисов и соединений. В случае неисправности позволяет дублирующим устройствам, службам и соединениям продолжать выполнение функции вышедших из строя устройств.

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

RIP (*англ*. Routing Information Protocol). Дистанционно-векторный протокол динамической маршрутизации для IP-сетей. Регламентируется RFC 1058, 2453.

RIPng. Протокол RIP для протокола IPv6. Регламентируется RFC 2080.

RJ-45 (RJ45). Унифицированный 8-контактный разъем, используемый в телекоммуникациях. Название RJ-45 не совсем точное, правильнее этот разъем было бы называть 8P8C.

RMON (*англ*. Remote MONitoring). Удаленный мониторинг. Спецификация RMON MIB, разработанная сообществом IETF для поддержки мониторинга и анализа протоколов в локальных сетях. Первая версия спецификации RMONv1 основывается на мониторинге сетей Ethernet и Token Ring. Ее расширением является RMONv2, в которую добавлена поддержка мониторинга протоколов сетевого уровня и приложений модели OSI. Регламентируется RFC 2819, 2819.

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

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 протоколов 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, затем был 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, зачастую 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 компактных модульных приемопередатчиков (трансиверов), используемых для передачи данных.

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

SMB (*англ*. Small-to-Medium Business). Малые и средние предприятия. Название сегмента рынка электроники. Характеризизует устройства, пред-

назначенные для использования в сетях малых и средних предприятий с численностью сотрудников от 100 до 1000 человек.

SNMP (*англ*. Simple Network Management Protocol). Простой протокол управления сетью. Протокол 7 уровня модели OSI, специально разработанный для управления и мониторинга сетевых устройств. Протокол SNMP позволяет получать информацию о состоянии устройств сети, обнаруживать и исправлять неисправности сети. Регламентируется RFC 1157, 1901—1908, 3411—3418.

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 технологиях 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 осуществлять удаленное управление каким-либо устройством и туннелирование TCP-соединений. Регламентируется RFC 4253.

SSL (*англ*. Secure Sockets Layer). Уровень защищенных сокетов. Криптографический протокол, обеспечивающий безопасную передачу данных по сети интернет. Регламентируется RFC 2246, 4346. В настоящее время не рекомендуется к применению и замещается протоколом TLS.

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

STA (*англ*. Spanning Tree Algorithm). Алгоритм построения связующего дерева.

Stack. Стек. Группа сетевых устройств объединенных 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, использует алгоритм связующего дерева и позволяет самообучающемуся мосту динамически обрабатывать коммутационные петли в сетевой топологии путем создания связующего дерева. Мосты обнаруживают петли путем обмена сообщениями BPDU и ликвидируют петли посредством блокирования выбранных интерфейсов.

Store-and-forward. Коммутация с промежуточным хранением. Метод коммутации пакетов, согласно которому кадры полностью обрабатываются перед их отправкой через соответствующий порт. Обработка включает расчет контрольных сумм и проверку адреса получателя. Кроме того, кадры временно хранятся 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 (втором) уровне модели OSI.

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

Switch fabric. Коммутирующая матрица. Представляет собой чипсет (набор микросхем), соединяющий множество входов с множеством выходов на основе технологий и принципов коммутации.

T

Tag. Тег. Идентификационная информация.

TCP (*англ*. Transmission Control Protocol). Протокол управления передачей. Протокол транспортного уровня, ориентированный на соединения и обеспечивающий надежную передачу данных. TCP входит в набор протоколов TCP/IP. Регламентируется RFC 675, 793, 2581.

Telnet. Стандартный протокол виртуального терминала из набора протоколов TCP/IP. Протокол Telnet используется для терминального подключения к удаленным системам и использования их ресурсов. Регламентируется RFC 15, 854.

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

Throughput. Пропускная способность. Объем информации, проходящей через определенный участок сети за определенный промежуток 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 IEEE 802.1Q и IEEE 802.1ad.

Traffic Policing. Ограничение трафика. Механизм Traffic Policing служит для ограничения входящего и исходящего трафика в соответствии с уста-

новленными пороговыми значениями скорости. Допускается всплеск трафика. См. также *Traffic Shaping*.

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

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

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

Trunk. Магистраль. Физическое или логическое соединение между сетевыми устройствами, по которому передается трафик нескольких физических или логических каналов.

U

UDP (*англ*. User Datagram Protocol). Протокол дейтаграмм пользователя. Протокол транспортного уровня, не требующий подтверждения доставки и не ориентированный на 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, их функциональность фиксированная. Данные коммутаторы применяются там, где характеристики, необходимые в сети, стандартны и не требуют дополнительных настроек.

V

VID (VLAN ID)**.** Идентификатор VLAN.

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

VLAN (*англ*. Virtual LAN). Виртуальная локальная сеть. Группа устройств, принадлежащих одной или нескольким локальным сетям и сконфигурированных при помощи программного обеспечения таким образом, 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 устройств.

VT100. Тип текстового терминала, который использует символы в кодировке ASCII.

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. 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.

Список литературы

1. *Олифер В.Г.*, *Олифер Н.А*. Компьютерные сети. Принципы, технологии, протоколы: 4-е изд. СПб.: Питер, 2010.

2. *Смирнова Е.В.*, *Пролетарский А.В.*, *Баскаков И.В.*, *Федотов Р.А.* Управление коммутируемой средой. М.: РУСАКИ, 2011. 335 с.

3. Библиотека RFC. RFC/STD/FYI/BCP Archives. http://www.faqs.org/rfcs.

4. Руководство по технологиям объединенных сетей: 3-е изд.; пер. с англ. М.: Издательский дом «Вильямс», 2002.

5. Учебные материалы компании D-Link. ftp://ftp.dlink.ru/pub/Trainings/.

6. *Шринивас Вегешна*. Качество обслуживания в сетях IP: пер. с англ. М.: Издательский дом «Вильямс», 2003.

7. *Panoc C. Lekkas*. Network Processors. The Mc-Graw-Hill Companies, 2003.

8. *Yossi Azar*, *Yossi Richter*. An improved algorithm for CIOQ switches. http://portal.acm.org.

9. http://www.ieee.org — сайт института инженеров по электротехнике и электронике (IEEE, Institute of Electrical and Electronics Engineers).

Учебное издание

Компьютерные системы и сети

Смирнова Елена Викторовна
Пролетарский Андрей Викторович
Ромашкина Екатерина Александровна
Суровов Александр Михайлович
Федотов Роман Анатольевич

ТЕХНОЛОГИИ КОММУТАЦИИ И МАРШРУТИЗАЦИИ В ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Редактор *К.А. Осипова*
Технический редактор *Э.А. Кулакова*
Художник *О.В. Левашова*
Корректор *О.Ю. Соколова*
Компьютерная графика *О.В. Левашовой*
Компьютерная верстка *Н.Ф. Бердавцевой*

Оригинал-макет подготовлен в Издательстве МГТУ им. Н.Э. Баумана.
Сертификат соответствия № РОСС RU. АЕ51. Н 16228 от 18.06.2012.

Подписано в печать 25.05.2013. Формат 70×100 1/16.
Усл. печ. л. 31,85. Тираж 2000 экз. (1-й з-д 1–1000).
Заказ

Издательство МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., 5, стр.1.
press@bmstu.ru http//www.baumanpress.ru

Отпечатано в типографии МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., 5, стр.1.
baumanprint@gmail.com