

Основы информационных технологий

ПОСТРОЕНИЕ КОММУТИРУЕМЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие

**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**



**БИНОМ.
Лаборатория знаний
www.lbz.ru**

**Москва
2011**

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

П63 Построение коммутируемых компьютерных сетей: учебное пособие / Е.В. Смирнова и др. — М.: Национальный Открытый Университет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. — 367 с.: ил., табл. — (Основы информационных технологий).

ISBN 978-5-9963-0685-5

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 и преподавателями МГТУ им. Н.Э. Баумана и Центра сетевых технологий «МГТУ – D-Link»

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».

По вопросам приобретения обращаться:
«БИНОМ. Лаборатория знаний»
Телефон (499) 157-1902, (499) 157-5272,
e-mail: binom@Lbz.ru, <http://www.Lbz.ru>

ISBN 978-5-9963-0685-5

© Национальный Открытый
Университет «ИНТУИТ», 2011
© БИНОМ. Лаборатория
знаний, 2011

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 Интернет-Университета, 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 Интернет-Университетом Информационных Технологий. В этой серии будут выпущены учебники по всем базовым областям знаний, связанным с компьютерными дисциплинами.

**Добро пожаловать в
Интернет-Университет Информационных Технологий!**

**Анатолий Шкред
anatoli@shkred.ru**

Об авторах

Смирнова Елена Викторовна – кандидат технических наук, менеджер по образовательным проектам компании D-Link.

Пролетарский Андрей Викторович – доктор технических наук, профессор МГТУ имени Н. Э. Баумана.

Баскаков Игорь Владимирович – кандидат технических наук, доцент МГТУ имени Н. Э. Баумана.

Федотов Роман Анатольевич – технический директор ЗАО «2В Сервис», преподаватель МГТУ имени Н. Э. Баумана.

Лекции

Лекция 1.	Основы коммутации	11
Лекция 2.	Начальная настройка коммутатора	44
Лекция 3.	Обзор функциональных возможностей коммутаторов	61
Лекция 4.	Виртуальные локальные сети (VLAN)	62
Лекция 5.	Функции повышения надежности и производительности	97
Лекция 6.	Качество обслуживания (QoS)	142
Лекция 7.	Функции обеспечения безопасности и ограничения доступа к сети	157
Лекция 8.	Многоадресная рассылка	193
Лекция 9.	Функции управления коммутаторами	203
Лекция 10.	Обзор коммутаторов D-Link	224

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	19
1.5. Физическое стекирование коммутаторов	20
1.6. Типы интерфейсов коммутаторов	21
1.7. Архитектура коммутаторов	26
1.8. Характеристики, влияющие на производительность коммутаторов	35
1.9. Управление потоком в полудуплексном и дуплексном режимах	38
1.10. Технологии коммутации и модель OSI	40
1.11. Программное обеспечение коммутаторов	41
1.12. Общие принципы сетевого дизайна	41
1.13. Трехуровневая иерархическая модель сети	42
Лекция 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
2.5. Подключение к Web-интерфейсу управления коммутатора	56
2.6. Загрузка нового программного обеспечения на коммутатор	58
2.7. Загрузка и резервное копирование конфигурации коммутатора	59
Лекция 3. Обзор функциональных возможностей коммутаторов	61
Лекция 4. Виртуальные локальные сети (VLAN)	62
4.1. Типы VLAN	64
4.2. VLAN на основе портов	65

4.3. VLAN на основе стандарта IEEE 802.1Q	66
4.4. Статические и динамические VLAN	77
4.5. Протокол GVRP	77
4.6. Q-in-Q VLAN	82
4.7. VLAN на основе портов и протоколов – стандарт IEEE 802.1v	89
4.8. Асимметричные VLAN	92
4.9. Функция Traffic Segmentation	94
Лекция 5. Функции повышения надежности и производительности ...	97
5.1. Протоколы Spanning Tree	97
5.2. Spanning Tree Protocol (STP)	97
5.3. Rapid Spanning Tree Protocol	108
5.4. Multiple Spanning Tree Protocol	119
5.5. Дополнительные функции защиты от петель	132
5.6. Функции безопасности STP	134
5.7. Агрегирование каналов связи	135
Лекция 6. Качество обслуживания (QoS)	142
6.1. Модели QoS	142
6.2. Приоритизация пакетов	143
6.3. Классификация пакетов	144
6.4. Маркировка пакетов	146
6.5. Управление перегрузками и механизмы обслуживания очередей	146
6.6. Механизм предотвращения перегрузок	149
6.7. Контроль полосы пропускания	150
6.8. Пример настройки QoS	154
Лекция 7. Функции обеспечения безопасности и ограничения доступа к сети	157
7.1. Списки управления доступом (ACL)	158
7.2. Функции контроля над подключением узлов к портам коммутатора	166
7.3. Аутентификация пользователей 802.1X	173
7.4. 802.1X Guest VLAN	181
7.5. Функции защиты ЦПУ коммутатора	189

Лекция 8. Многоадресная рассылка	193
8.1. Адресация многоадресной IP-рассылки	193
8.2. MAC-адреса групповой рассылки	195
8.3. Подписка и обслуживание групп	196
8.4. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping)	197
8.5. Функция IGMP Snooping Fast Leave	201
Лекция 9. Функции управления коммутаторами	203
9.1. Управление множеством коммутаторов	203
9.2. Протокол SNMP	214
9.3. RMON (Remote Monitoring)	219
9.4. Функция Port Mirroring	222
Лекция 10. Обзор коммутаторов D-Link	224
10.1. Неуправляемые коммутаторы	224
10.2. Коммутаторы серии Smart	227
10.3. Управляемые коммутаторы	228
Приложение	237
Занятие №1. Основные команды коммутаторов. Управление коммутаторами	239
Занятие №2. Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	247
Занятие №3. Команды управления таблицами MAC, IP, ARP ...	251
Занятие №4. Команды VLAN на основе портов и стандарта IEEE 802.1Q	255
Занятие №5. Команды протокола GVRP (продвижение информации о VLAN в сети)	264
Занятие №6. Команды настройки асимметричных VLAN и сегментации трафика	270
Занятие №7. Команды настройки функции Q-in-Q (Double VLAN)	276
Занятие №8. Команды настройки протоколов связующего дерева STP, RSTP, MSTP	280
Занятие №9. Функция предотвращения петлеобразования (LoopBack Detection)	293

Занятие №10. Команды агрегирования каналов	298
Занятие №11. Списки управления доступом (Access Control List)	306
Занятие №12. Контроль над подключением узлов к портам коммутатора. Функция Port Security	315
Занятие №13. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	321
Занятие №14. Ограничение административного доступа к управлению коммутатором	328
Занятие №15. Команды протокола IEEE 802.1X	334
Занятие №16. Управление полосой пропускания	338
Занятие №17. Настройка QoS. Приоритизация трафика	340
Занятие №18. Команды зеркалирования портов (Port Mirroring)	344
Занятие №19. Команды мониторинга	347
Глоссарий	350
Литература	367

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 учебном центре D-Link — МГТУ им. Н. Э. Баумана.

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

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

Обозначения, используемые в книге

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



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 (10Base-2 и 10Base-5) 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-

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

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

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

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

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

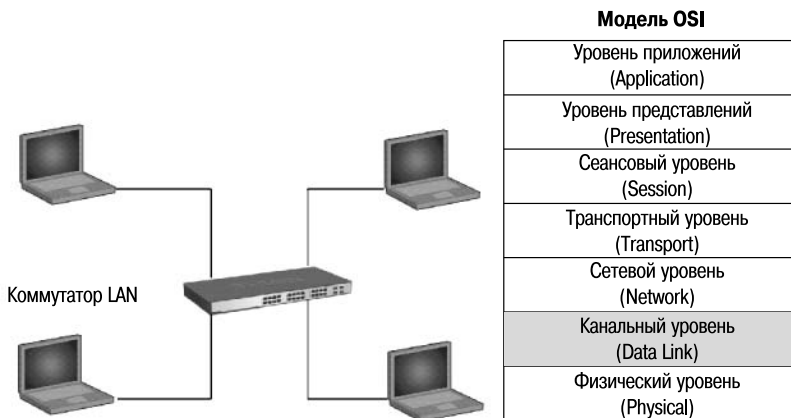


Рис. 1.1. Коммутатор локальной сети

ра от моста заключалось в том, что он мог устанавливать *одновременно несколько соединений* между разными парами портов. При передаче пакета через коммутатор в нем создавался отдельный виртуальный (либо реальный, в зависимости от архитектуры) канал, по которому данные пересылались напрямую от порта-источника к порту-получателю с максимально возможной для используемой технологии скоростью. Такой принцип работы получил название «*микросегментация*». Благодаря микросегментации коммутаторы получили возможность функционировать в *режиме полного дуплекса (full duplex)*, что позволяло каждой рабочей станции одновременно передавать и принимать данные, используя всю полосу пропускания в обоих направлениях. Рабочей станции не приходилось конкурировать за полосу пропускания с другими устройствами, в результате чего не происходили коллизии и повышалась производительность сети.

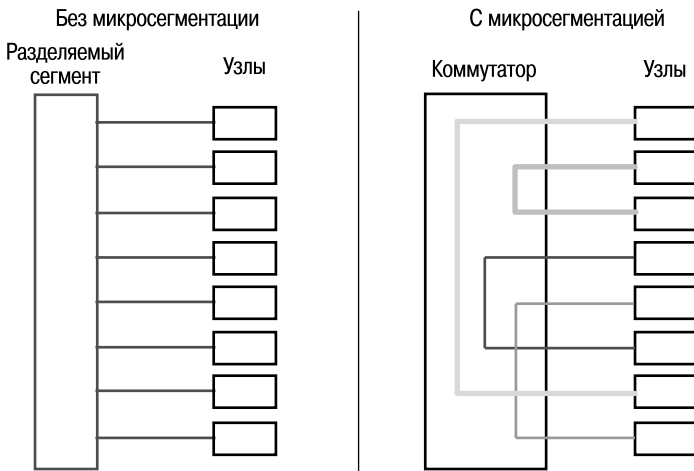


Рис. 1.2. Микросегментация

В настоящее время коммутаторы являются основным строительным блоком для создания локальных сетей. Современные коммутаторы Ethernet превратились в интеллектуальные устройства со специализированными процессорами для обработки и перенаправления пакетов на высоких скоростях и реализации таких функций, как организация резервирования и повышения отказоустойчивости сети, агрегирование каналов, создание виртуальных локальных сетей (VLAN), маршрутизация, управление качеством обслуживания (Quality of Service, QoS), обеспечение безопасности и многих других. Также усовершенствовались функции управления коммутаторов, благодаря чему системные администраторы получи-

ли удобные средства настройки сетевых параметров, мониторинга и анализа трафика.

С появлением стандарта IEEE 802.3af-2003 PoE, описывающего технологию передачи питания по Ethernet (Power over Ethernet, PoE), разработчики начали выпускать коммутаторы с поддержкой данной технологии, что позволило использовать их в качестве питающих устройств для IP-телефонов, Интернет-камер, беспроводных точек доступа и другого оборудования.

С ростом популярности технологий беспроводного доступа в корпоративных сетях производители оборудования выпустили на рынок унифицированные коммутаторы с поддержкой технологии PoE для питания подключаемых к их портам точек беспроводного доступа и централизованного управления как проводной, так и беспроводной сетью.

Повышение потребностей заказчиков и тенденции рынка стимулируют разработчиков коммутаторов более или менее регулярно расширять аппаратные и функциональные возможности производимых устройств, позволяющие предоставлять в локальных сетях новые услуги, повышать их надежность, управляемость и защищенность.

1.2. Функционирование коммутаторов локальной сети

Коммутаторы локальных сетей обрабатывают кадры на основе алгоритма *прозрачного моста (transparent bridge)*, который определен стандартом IEEE 802.1D. Процесс работы алгоритма прозрачного моста начинается с построения *таблицы коммутации (Forwarding DataBase, FDB)*.

Изначально таблица коммутации пуста. При включении питания, одновременно с передачей данных, коммутатор начинает изучать расположение подключенных к нему сетевых устройств путем анализа MAC-адресов источников получаемых кадров. Например, если на порт 1 коммутатора, показанного на рис. 1.3, поступает кадр от узла А, то он создает в таблице коммутации запись, ассоциирующую MAC-адрес узла А с номером входного порта. Записи в таблице коммутации создаются *динамически*. Это означает, что, как только коммутатором будет прочитан новый MAC-адрес, то он сразу будет занесен в таблицу коммутации. Дополнительно к MAC-адресу и ассоциированному с ним порту в таблицу коммутации для каждой записи заносится *время старения (aging time)*. Время старения позволяет коммутатору автоматически реагировать на перемещение, добавление или удаление сетевых устройств. Каждый раз, когда идет обращение по какому-либо MAC-адресу, соответствующая запись получает новое время старения. Записи, к которым не обращались долгое время, из таблицы удаляются. Это позволяет хранить в таблице коммутации только актуальные MAC-адреса, что уменьшает время поиска соот-

ветствующей записи в ней и гарантирует, что она не будет использовать слишком много системной памяти.

6 байт	6 байт	2 байта	4 байта	
Адрес назначения FF-FF-FF-FF-FF-FF	Адрес источника 00-0C-29-9B-E6-B5	Тип Ethernet	Данные	
			FCS	

Таблица коммутации
Порт 1 00-0C-29-9B-E6-B5

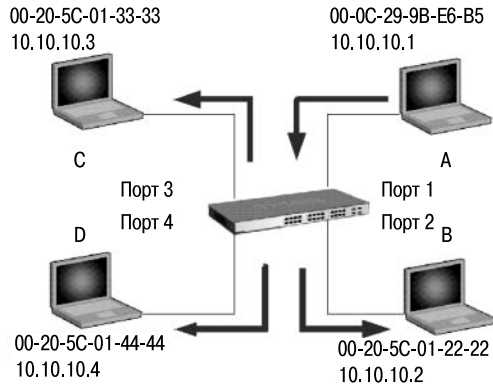


Рис. 1.3. Построение таблицы коммутации

Помимо динамического создания записей в таблице коммутации в процессе самообучения коммутатора, существует возможность создания статических записей таблицы коммутации вручную. Статическим записям, в отличие от динамических, не присваивается время старения, поэтому время их жизни не ограничено.

Статическую таблицу коммутации удобно использовать с целью повышения сетевой безопасности, когда необходимо гарантировать, что только устройства с определенными MAC-адресами могут подключаться к сети. В этом случае необходимо отключить автоизучение MAC-адресов на портах коммутатора.

Внимание: как правило, размер статической таблицы коммутации меньше размера динамической таблицы коммутации. Размеры обеих таблиц также зависят от модели коммутатора. Обычно производители указывают размеры таблиц коммутации в спецификациях на устройства.

Как только в таблице коммутации появляется хотя бы одна запись, коммутатор начинает использовать ее для пересылки кадров. Рассмотрим пример, показанный на рис. 1.4, описывающий процесс пересылки кадров между портами коммутатора.

Таблица коммутации	
Порт 1	00-0C-29-9B-E6-B5
Порт 2	00-20-5C-01-22-22

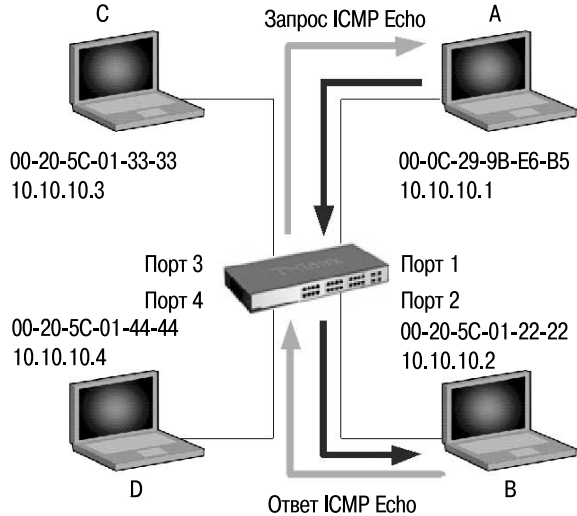


Рис. 1.4. Передача кадра с порта на порт коммутатора

Когда коммутатор получает кадр, отправленный компьютером А компьютеру В, он извлекает из него MAC-адрес приемника и ищет этот MAC-адрес в своей таблице коммутации. Как только в таблице коммутации будет найдена запись, ассоциирующая MAC-адрес приемника (компьютера В) с одним из портов коммутатора, за исключением порта-источника, кадр будет передан через соответствующий выходной порт (в приведенном примере — порт 2). Этот процесс называется *продвижением (forwarding)* кадра.

Если бы оказалось, что выходной порт и порт-источник совпадают, то передаваемый кадр был бы отброшен коммутатором. Этот процесс называется *фильтрацией (filtering)*.

В том случае, если MAC-адрес приемника в поступившем кадре неизвестен (в таблице коммутации отсутствует соответствующая запись), коммутатор создает множество копий этого кадра и передает их через все свои порты, за исключением того, на который он поступил. Этот процесс называется *лавинной передачей (flooding)*. Несмотря на то, что процесс лавинной передачи занимает полосу пропускания, он позволяет коммутатору избежать потери кадров, когда MAC-адрес приемника неизвестен, и осуществлять процесс самообучения.

Помимо лавинной передачи одноадресных кадров, коммутаторы также выполняют лавинную передачу многоадресных и широковещательных кадров, которые генерируются сетевыми мультимедийными приложениями.

1.3. Методы коммутации

Первым шагом, который выполняет коммутатор прежде чем принять решение о передаче кадра, является его получение и анализ содержимого. В коммутаторе может быть реализован один из трех режимов работы, определяющих его поведение при получении кадра:

- коммутация с промежуточным хранением (*store-and-forward*);
- коммутация без буферизации (*cut-through*);
- коммутация с исключением фрагментов (*fragment-free*).

При *коммутации с промежуточным хранением (store-and-forward)* коммутатор, прежде чем передать кадр, полностью копирует его в буфер и производит проверку на наличие ошибок. Если кадр содержит ошибки (не совпадает контрольная сумма или кадр меньше 64 байт или больше 1518 байт), то он отбрасывается. Если кадр не содержит ошибок, то коммутатор находит MAC-адрес приемника в своей таблице коммутации и определяет выходной порт. Затем, если не определены никакие фильтры, коммутатор передает кадр через соответствующий порт устройству назначения.

Несмотря на то, что этот способ передачи связан с задержками (чем больше размер кадра, тем больше времени требуется на его прием и проверку на наличие ошибок), он обладает двумя существенными преимуществами:

- коммутатор может быть оснащен портами, поддерживающими разные технологии и скорости передачи, например, 10/100 Мбит/с, 1000 Мбит/с и 10 Гбит/с;
- коммутатор может проверять целостность кадра, благодаря чему поврежденные кадры не будут передаваться в соответствующие сегменты.

В коммутаторах D-Link реализован этот метод коммутации. Благодаря использованию в устройствах высокопроизводительных процессоров и контроллеров ASIC (Application-Specific Integrated Circuit) задержка, вносимая коммутацией *store-and-forward* при передаче пакетов, оказывается незначительной.

Коммутация без буферизации (cut-through) была реализована в первом коммутаторе Ethernet, разработанном фирмой Kalpana в 1990 г. При работе в этом режиме коммутатор копирует в буфер только MAC-адрес назначения (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. Данный метод коммутации может использоваться только в том случае, когда порты коммутатора поддерживают одинаковую скорость.

Коммутация с исключением фрагментов (fragment-free) является компромиссным решением между методами *store-and-forward* и *cut-through*. При этом методе коммутации коммутатор принимает в буфер первые

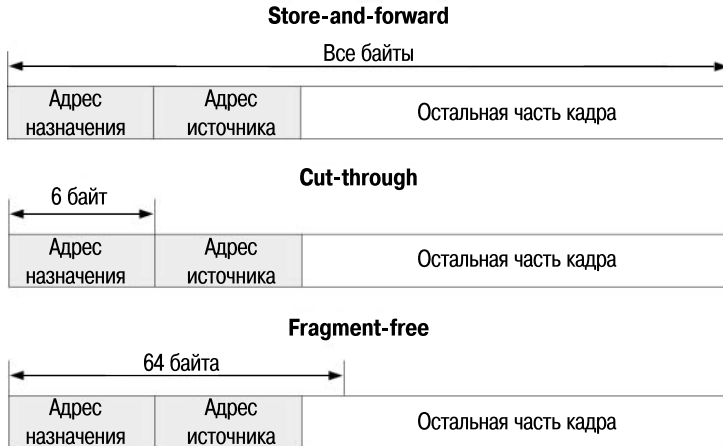


Рис. 1.5. Методы коммутации

64 байта кадра, что позволяет ему отфильтровывать коллизийные кадры перед их передачей. В соответствии со спецификацией Ethernet коллизия может произойти во время передачи первых 64 байт. Поэтому все кадры с длиной больше 64 байт считаются правильными. Этот метод коммутации ожидает, пока полученный кадр не будет проверен на предмет коллизии, и только после этого начинает его передачу.

1.4. Конструктивное исполнение коммутаторов

В зависимости от конструктивного исполнения (габаритных размеров) можно выделить три группы коммутаторов:

- настольные коммутаторы (Desktop switch);
- автономные коммутаторы, монтируемые в телекоммуникационную стойку (Rack mounted switch);
- коммутаторы на основе шасси (Chassis switch).

Как следует из названия, *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 (у коммутаторов D-Link количество портов варьируется от 5 до 16), внешним или внутренним блоком питания и небольшими ножками (обычно резиновыми) для обеспечения вентиляции нижней поверхности устройства. Чаще всего коммутаторы настольного форм-фактора используются в сетях класса *SOHO* (*Small Office, Home Office*), где не требуется высокая производительность и рас-

ширенные сетевые функции. В качестве примера коммутатора в настольном исполнении можно привести коммутатор D-Link модели DES-1008A.

Автономные коммутаторы в стоечном исполнении высотой 1U обладают корпусом для монтажа в 19” стойку, встроенным блоком питания и фиксированным количеством портов (у коммутаторов D-Link количество портов может достигать 52-х штук). По сравнению с настольными коммутаторами коммутаторы, монтируемые в стойку, обеспечивают более высокую производительность и надежность, а также предлагают широкий набор сетевых функций и интерфейсов. Как правило, такие коммутаторы используются на уровнях доступа и распределения сетей малых и средних предприятий (*Small to Medium Business, SMB*), корпоративных сетей и сетей провайдеров услуг (*Internet Service Provider, ISP*).

Среди коммутаторов в стоечном исполнении с фиксированным количеством портов можно выделить отдельную группу устройств — *стековые коммутаторы*. Эти устройства представляют собой коммутаторы, которые могут работать как автономно, так как выполнены в отдельном корпусе, так и совместно, благодаря наличию специальных интерфейсов, позволяющих объединять коммутаторы в одно логическое устройство с целью увеличения количества портов, удобства управления и мониторинга. Говорится, что в этом случае отдельные коммутаторы образуют *стек*.

Коммутаторы на основе шасси содержат слоты, которые могут быть использованы для установки интерфейсных модулей расширения, резервных источников питания и процессорных модулей. Модульное решение обеспечивает гибкость применения, высокую плотность портов и возможность резервирования критичных для функционирования коммутатора компонентов. Модули такого коммутатора поддерживают технологию *hot swap* («горячая замена»), то есть допускают замену на ходу, без выключения питания коммутатора. Коммутаторы на основе шасси предназначены для применения на магистрали сети крупных корпоративных сетей, городских сетей или сетей операторов связи.

1.5. Физическое стекирование коммутаторов

Под **физическим стекированием** понимается объединение нескольких коммутаторов в одно логическое устройство с целью увеличения количества портов, удобства управления и мониторинга. Объединенные в стек коммутаторы имеют общие таблицы коммутации и маршрутизации (для коммутаторов 3 уровня).

В коммутаторах D-Link используются 2 топологии стекирования: «кольцо» (ring) и «цепочка» (chain).

Стек типа «кольцо» (кольцевая топология) строится по следующей схеме: каждое устройство в стеке подключается к вышележащему и ниже-

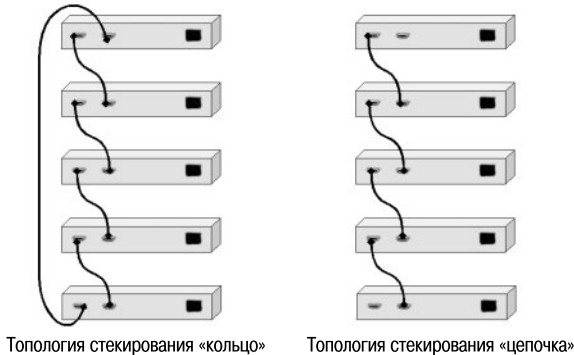


Рис. 1.6. Топологии стекирования «кольцо» и «цепочка»

лежащему, при этом самый нижний и самый верхний коммутатор в стеке также соединяются. При передаче данных пакет последовательно передается от одного устройства стека к другому до тех пор, пока не достигнет порта назначения. Система автоматически определяет оптимальный путь передачи трафика, что позволяет достичь полного использования полосы пропускания. Преимуществом топологии «кольцо» является то, что при выходе одного устройства из строя или обрыве связи остальные устройства стека будут продолжать функционировать в обычном режиме.

В стеке типа «цепочка» (линейная топология) каждое устройство соединено с вышележащим и нижележащим. Самый верхний и самый нижний коммутаторы не соединяются.

Физическое стекирование по линейной и кольцевой топологии реализовано в семи сериях коммутаторов D-Link. Коммутаторы серии DGS-3120-xx позволяют объединить в стек до 6 устройств, коммутаторы серии DGS-3610-xx – до 8 устройств, а коммутаторы серий DGS-3420-xx и DGS-36xx, DGS-3620-xx – до 12 устройств, используя интерфейсы 10 Gigabit Ethernet (10GE). Коммутаторы серии DGS-31xx объединяются в стек через интерфейсы HDMI. Максимальное количество коммутаторов в стеке равно 6. Коммутаторы серии DES-3528/3552 поддерживают физическое стекирование через интерфейсы Gigabit Ethernet и позволяют объединить в стек до 8 устройств.

Все устройства стека управляются через один IP-адрес. Передача данных между ними ведется в полнодуплексном режиме.

1.6. Типы интерфейсов коммутаторов

В зависимости от выполняемых задач коммутаторы могут быть оборудованы различным количеством и типом портов. В таблице 1.1 приведены

типы наиболее часто используемых интерфейсов и их основные характеристики в соответствии со стандартом IEEE 802.3-2008.

Наиболее распространенными интерфейсами, реализуемыми в коммутаторах, являются фиксированные интерфейсы с разъемом RJ-45 на основе витой пары, поддерживающие технологию Fast или Gigabit Ethernet, автосогласование скоростей, полудуплексного или дуплексного режима работы и автоматического определения полярности витой пары MDI/MDIX. Для обеспечения большей гибкости в выборе типа подключения многие коммутаторы оборудованы специальными слотами для установки компактных сменных интерфейсных модулей *GBIC* (Gigabit Interface Converter), *SFP* (Small Form Factor Pluggable), *XFP* (10 Gigabit Small Form Factor Pluggable) и *SFP+* (Enhanced Small Form Factor Pluggable), поддерживающих режим горячей замены.

Таблица 1.1.

Стандарт	Тип кабеля	Максимальное расстояние передачи, м
10BASE-T	Кабель на основе витой пары категории 3 или 5	100
100BASE-TX	Кабель на основе витой пары категории 5	100
100BASE-FX	Многомодовый оптический кабель	412 (полудуплекс) 2000 (дуплекс)
100BASE-BX10	Одномодовый одномодовый оптический кабель (длина волны: 1310 нм – восходящий поток, 1550 нм – нисходящий)	10 000
100BASE-LX10	Одномодовый оптический кабель (длина волны 1310 нм)	10 000
1000BASE-T	Кабель на основе витой пары категории 5, 5e, 6 или 7	100
1000BASE-SX	Многомодовый оптический кабель 62.5/125 микрон/50/125 микрон	220/550
1000BASE-LX	Одномодовый оптический кабель	5 000
	Многомодовый оптический кабель	550
1000BASE-LX10	Одномодовый оптический кабель (длина волны 1310 нм)	10 000
	Многомодовый оптический кабель (длина волны 1310 нм)	550

1000BASE-BX10	Одномодовый оптический кабель (длина волны: 1310 нм – восходящий поток, 1550 нм – нисходящий)	10 000
1000BASE-ZX	Одномодовый оптический кабель (длина волны 1550 нм)	80 000
1000BASE-LH (Long Haul)	Одномодовый оптический кабель	50 000
10GBASE-CX4	Экранированный сбалансированный медный кабель	15
10GBASE-SR	Многомодовый оптический кабель	300
10GBASE-LR	Одномодовый оптический кабель	10 000
10GBASE-ER	Одномодовый оптический кабель	40 000

Самой первой спецификацией на компактные сменные интерфейсные модули была спецификация SFF-8053 комитета SFF, описывающая конвертеры гигабитного интерфейса (Gigabit Interface Converter, GBIC). Модули GBIC поддерживают стандарты Gigabit Ethernet или Fibre Channel для передачи данных, голоса и видео по медным или оптическим кабелям, но преимущественно представляют собой оптические трансиверы для приема или передачи сигнала по многомодовому или одномодовому волокну. Компания D-Link выпускает большой перечень модулей GBIC с поддержкой технологии Gigabit Ethernet с оптическими и медными интерфейсами.



Рис. 1.7. Модуль GBIC DGS-703 с одним портом 1000Base-LX для одномодового оптического кабеля

Спустя несколько лет после появления спецификации GBIC разработчики предложили усовершенствованную, компактную модификацию сменного интерфейса (Small Form Factor Pluggable, SFP). Модули SFP в два раза меньше своих предшественников по габаритным размерам. Посадочный размер SFP (форм-фактор) определяется величиной медного разъема RJ-45. Интерфейсы SFP поддерживают практически любые существующие протоколы: Ethernet (на 10, 100, 1000 Мбит/с), SONET/SDH (OC3/ 12/48 и STM 1/4/16), Fibre Channel (1 и 2 Гбит/с). Компания

D-Link выпускает модули SFP, поддерживающие стандарты Fast и Gigabit Ethernet и предназначенные для работы с разнообразным оптическим кабелем — одномодовым, одноволоконным одномодовым для систем с технологией *WDM* (Wavelength Division Multiplexing) и многомодовым.



Рис. 1.8. Модуль SFP DEM-310GT с одним портом 1000Base-LX для одномодового оптического кабеля

Технология сменных модулей оказалась очень эффективной в системах оптического уплотнения (Wavelength Division Multiplexing, WDM), широко применяемых в сетях передачи данных и в телекоммуникационной отрасли. Основной принцип, на котором базируется работа этих устройств — модуляция сигнала для смещения спектра несущего сигнала в другой диапазон. Сигналы каждого канала переносятся в собственном диапазоне частот. Далее они собираются в мультиплексоре и передаются уже по одному волокну, образуя широкополосный канал. Таким образом, по одному волокну параллельно передается несколько независимых каналов (каждый на своей длине волны), что позволяет повысить пропускную способность системы передачи в целом. Задача объединения или разделения частот решается на уровне приемника или передатчика.

Компания D-Link производит модули SFP с использованием технологии WDM, поддерживающие скорости передачи 100 и 1000 Мбит/с. Эти



Рис. 1.9. Модули SFP DEM-331R и DEM-331T с одним портом 1000BASE-BX10 с поддержкой технологии WDM

модули позволяют одновременно передавать и получать сигналы на длинах волн 1310 нм и 1550 нм по одному оптическому волокну на расстояние до 40 км. Это достигается путем установки SFP-модуля передатчика и SFP-модуля приемника на разных концах линии связи.

Модули SFP могут поддерживать важные функции цифровой диагностики (описанные в спецификации SFF-8472), позволяющие в реальном времени осуществлять мониторинг таких параметров, как мощность передатчика, чувствительность приемника, напряжение питания и температура каждого оптического компонента. Информация о поддержке этой функции обычно указывается в спецификации на устройство.

Каждый модуль SFP выпускается с собственной электронной меткой, где содержатся сведения об идентификационном номере устройства и спецификации внешнего порта. Информация о внешнем порте может включать данные о длине волны, характеристиках волокна, скорости передачи данных, поддерживаемых протоколах, а также о длине канала. Идентификация SFP полезна при инвентаризации: с ее помощью отслеживается установка и замена компонентов и определяется местонахождение того или иного модуля.

Следующей ступенью эволюции сменных интерфейсов стала разработка оптических трансиверов XFP (10 Gigabit Small Form Factor Pluggable) для волн 850, 1310 и 1550 нм. Они поддерживают 10GE, 10 Gigabit SONET/SDH, Fibre Channel и еще некоторые высокоскоростные протоколы. XFP имеют несколько большие размеры, чем трансиверы SFP. Модули могут поддерживать систему цифровой диагностики для мониторинга состояния оптических линий.

В настоящее время компания D-Link выпускает трансиверы XFP 10 GE, предназначенные для работы с одномодовым и многомодовым оптическим кабелем разной дальности передачи.

Новым поколением оптических сменных интерфейсных модулей с поддержкой скоростей 10 Гбит/с стали трансиверы SFP+. Требования к модулям SFP+, которые являются расширенной версией SFP, определены в спецификации SFF-8431. Несмотря на то, что модули SFP+ имеют



Рис. 1.10. Модуль XFP DEM-423ХТ с одним портом 10GE (10GBASE-ER) для одномодового оптического кабеля

ряд усовершенствований по сравнению с классическими модулями SFP, в коммутаторах D-Link слоты SFP+ поддерживают установку модулей SFP.

По сравнению с трансиверами XFP, модули SFP+ обладают меньшими габаритными размерами и тепловыделением, что позволяет повысить плотность размещения портов 10 Гбит/с на корпусе телекоммуникационных устройств.

Модули SFP+, так же как и модули SFP, могут поддерживать систему цифровой диагностики в соответствии со спецификацией SFF-8472.

Компания D-Link производит широкий спектр трансиверов SFP+ с поддержкой и без поддержки функции цифровой диагностики. Различают модули, предназначенные для работы как с одномодовым или многомодовым оптическим кабелем на длинах волн 850, 1310 и 1550 нм, так и с одноволоконным с поддержкой технологии WDM, использующие длины волн 1330 и 1270 нм для приема/передачи сигналов.



Рис. 1.11. Модуль SFP+ DEM-432XT-DD с одним портом 10GE (10GBASE-LR) для одномодового оптического кабеля и поддержкой функции цифровой диагностики

1.7. Архитектура коммутаторов

Одним из основных компонентов всего коммутационного оборудования является *коммутирующая матрица (switch fabric)*. Коммутирующая матрица представляет собой чипсет, соединяющий множество входов с множеством выходов на основе фундаментальных технологий и принципов коммутации. Коммутирующая матрица выполняет три функции:

- переключает трафик с одного порта матрицы на другой, обеспечивая их равнозначность;
- предоставляет качество обслуживания (Quality of Service, QoS);
- обеспечивает отказоустойчивость.

Поскольку коммутирующая матрица является ядром аппаратной платформы, к ней предъявляются требования по масштабированию производительности и возможности быстрого развития системы QoS.

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

«Неблокирующей» коммутирующей матрицей (*non-blocking switch fabric*) является такая матрица, у которой производительность и QoS не зависят от типа трафика, коммутируемого через матрицу, и производительность равна сумме скоростей всех портов:

$$\sum_1^N C p_i \times 2 \text{ Мбит/с}^*,$$

где N — количество портов, $C p_i$ — максимальная производительность протокола, поддерживаемого i -м портом коммутатора.

Например, производительность коммутатора с 24 портами 10/100 Мбит/с и 2 портами 1 Гбит/с вычисляется следующим образом:

$$((24 \times 100 \text{ Мбит/с}) + (2 \times 1 \text{ Гбит/с})) \times 2 = 8.8 \text{ Гбит/с}$$

Коммутатор обеспечивает портам равноправный доступ к матрице, если в системе не установлено преимущество одних портов над другими.

Поскольку коммутирующая матрица располагается в ядре платформы коммутатора, то одним из наиболее важных вопросов остается ее отказоустойчивость. Этот вопрос решается за счет реализации отказоустойчивой архитектуры, предусматривающей резервирование критичных для работы коммутатора блоков.

Одним из ключевых компонентов архитектуры современных коммутаторов является контроллер ASIC (*Application Specific Integrated Circuit*). Контроллеры ASIC представляют собой быстродействующие и относительно недорогие кремниевые кристаллы, которые предназначены для выполнения определенных операций. Использование в архитектуре коммутаторов контроллеров ASIC повышает производительность системы, т.к. ASIC выполняет операции аппаратно, благодаря чему не возникают накладные расходы, связанные с выборкой и интерпретацией хранимых команд. Современные контроллеры ASIC 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 настоящее время существует много типов архитектур коммутирующих матриц. Выбор архитектуры матрицы во многом определяется ролью коммутатора в сети и количеством трафика, которое ему придется обрабатывать. В действительности, матрица обычно реализуется на основе комбинации двух или более базовых архитектур. Рассмотрим самые распространенные типы архитектур коммутирующих матриц.

* Умножение на 2 для дуплексного режима работы.

1.7.1. Архитектура с разделяемой шиной

Архитектура с разделяемой шиной (Shared Bus), как следует из ее названия, использует в качестве разделяемой среды шину, которая обеспечивает связь подключенных к ней устройств ввода-вывода (портов). Шина используется в режиме разделения времени, т.е. в каждый момент времени только одному источнику разрешено передавать по ней данные. Управление доступом к шине осуществляется через централизованный арбитр, который предоставляет источнику право передавать данные.

Применительно к системам с разделяемой шиной под термином «неблокирующая» понимается то, что сумма скоростей портов матрицы меньше, чем скорость шины. Т.е. производительность системы ограничена производительностью шины. Даже если общая полоса пропускания ниже производительности шины, количество и производительность устройств ввода-вывода ограничены производительностью централизованного арбитра.

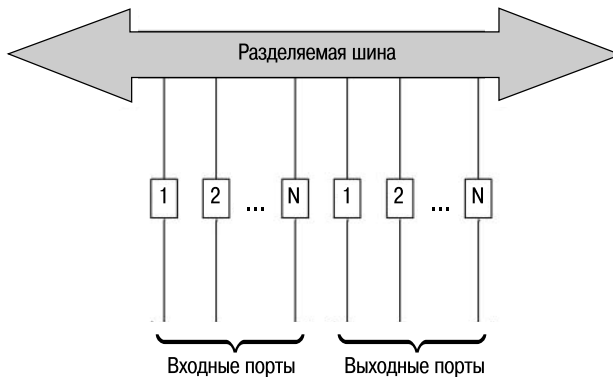


Рис. 1.12. Архитектура с разделяемой шиной

1.7.2. Архитектура с разделяемой памятью

Улучшения архитектуры с разделяемой шиной привели к появлению высокопроизводительной *архитектуры с разделяемой памятью (Shared Memory)*. Архитектура с разделяемой памятью обычно основана на использовании быстрой памяти RAM большой емкости в качестве общего буфера коммутационной системы, предназначенного для хранения входящих пакетов перед их передачей. Память обычно организуется в виде множества выходных очередей, ассоциирующихся с одним из устройств ввода-вывода или портом. Для обеспечения неблокирующей работы полоса пропускания памяти для операции «запись» и операции «чтение» должна быть равна максимальной суммарной полосе пропускания всех входных портов.

Типовая архитектура коммутаторов с разделяемой памятью показана на рис. 1.12. Входящие пакеты преобразуются из последовательного формата в параллельный и затем записываются в двухпортовую память. Запись в память осуществляется по принципу мультиплексирования с разделением по времени (Time Division Multiplexing, TDM), поэтому в каждый момент времени только один входной порт может поместить кадр в ячейку разделяемой памяти. Заголовки каждого кадра передаются в контроллер памяти. На основе этой информации он определяет выходной порт назначения и выходную очередь, в которую необходимо поместить кадр. Порядок, в котором выходные кадры будут считываться из памяти, определяется контроллером памяти с помощью механизма арбитража. Считанные кадры отправляются на соответствующие выходные порты (выходные кадры демультиплексируются с разделением по времени таким образом, что только один выходной порт может получить доступ к разделяемой памяти), где они вновь преобразуются из параллельного формата в последовательный.

Одним из преимуществ использования общего буфера для хранения пакетов является то, что он позволяет минимизировать количество выходных буферов, требуемых для поддержания скорости потери пакетов на низ-

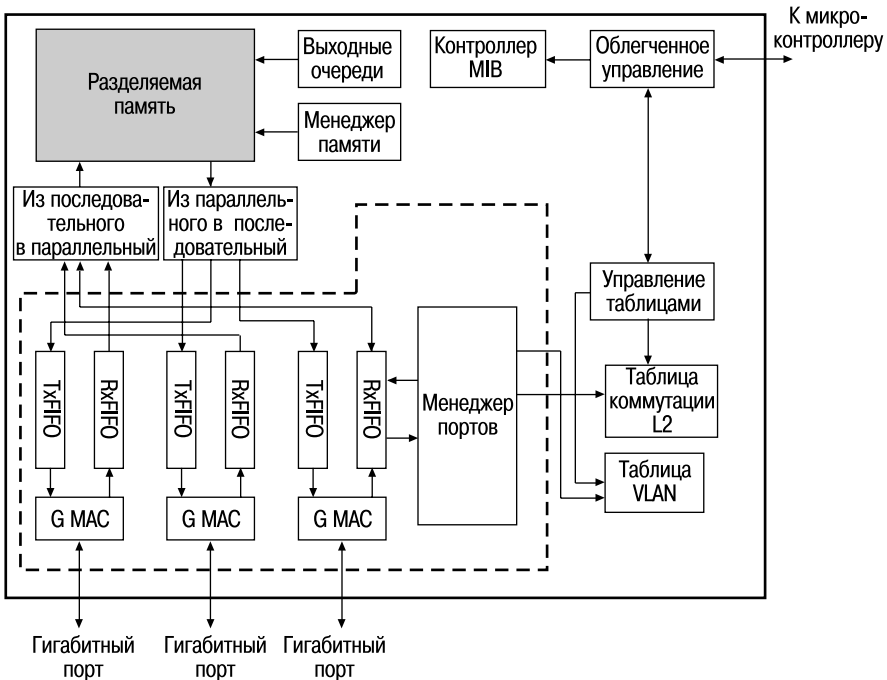


Рис. 1.13. Архитектура с разделяемой памятью

ком уровне. С помощью централизованного буфера можно воспользоваться преимуществами статического разделения буферной памяти. При высокой скорости трафика на одном из портов он может захватить большее буферное пространство, если общий буферный пул не занят полностью.

Архитектура с разделяемой памятью обладает рядом недостатков. Так как пакеты записываются и считываются из памяти одновременно, она должна обладать суммарной пропускной способностью портов, т.е. операции записи и чтения из памяти должны выполняться в N (количество портов) раз выше скорости работы портов. Т.к. доступ к памяти физически ограничен, необходимость ускорения работы в N раз ограничивает масштабируемость архитектуры. Более того, контроллер памяти должен обрабатывать пакеты с той же скоростью, что и память. Такая задача может быть трудно выполнимой в случае управления множеством классов приоритетов и сложными операциями планирования. Коммутаторы с разделяемой памятью обладают единой точкой отказа, поскольку добавление еще одного общего буфера является сложным и дорогим. В результате этого в чистом виде архитектура с разделяемой памятью используется для построения коммутаторов с небольшим количеством портов.

1.7.3. Архитектура на основе коммутационной матрицы

Параллельно с появлением архитектуры с разделяемой памятью (в середине 1990-х годов) была разработана *архитектура на основе коммутационной матрицы (Crossbar architecture)*. Эта архитектура используется для построения коммутаторов различных типов.

Существует множество вариаций архитектуры этого типа. Базовая архитектура на основе коммутационной матрицы $N \times N$ непосредственно соединяет N входных портов с N выходными портами в виде матрицы. В местах пересечения проводников, соединяющих входы и выходы, находятся коммутирующие устройства, которыми управляет специальный контроллер. В каждый момент времени, анализируя адресную информацию, контроллер сообщает коммутирующим устройствам, какой выход должен быть подключен к какому входу. В том случае, если два входящих пакета от разных портов-источников будут переданы на один и тот же выходной порт, он будет заблокирован. Существуют различные подходы к решению этой проблемы: повышение производительности матрицы по сравнению с производительностью входных портов или использование буферов памяти и арбитров.

Несмотря на простой дизайн, одной из фундаментальных проблем архитектуры на основе коммутационной матрицы остается ее масштабируемость. При увеличении количества входов и выходов усложняется схемотехника матрицы и в особенности контроллера. Поэтому для построения многопортовых коммутационных матриц используется другой подход, ко-

торый заключается в том, что простые коммутационные матрицы связываются между собой, образуя одну большую коммутационную матрицу.

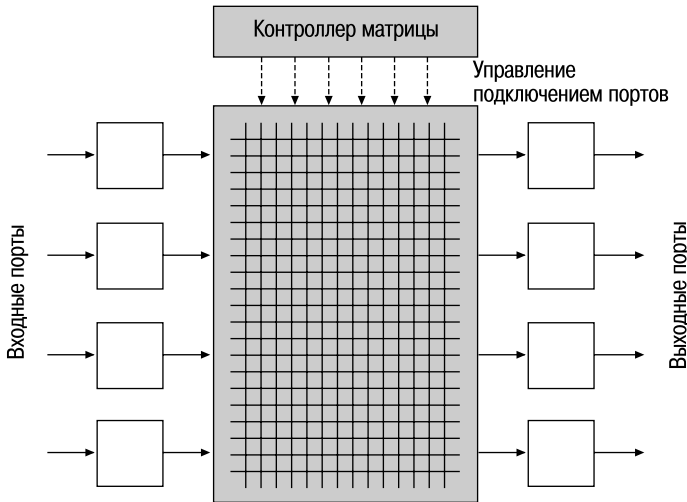


Рис. 1.14. Архитектура на основе коммутационной матрицы

Можно выделить два типа коммутаторов на основе коммутационной матрицы:

- коммутаторы на основе коммутационной матрицы с буферизацией (buffered crossbar);
- коммутаторы на основе коммутационной матрицы с арбитражем (arbitrated crossbar).

1.7.3.1. Коммутаторы на основе коммутационной матрицы с буферизацией

В коммутаторах на основе коммутационной матрицы с буферизацией буферы расположены на трех основных стадиях: на входе и выходе и непосредственно на коммутационной матрице. Благодаря наличию очередей на трех стадиях эта архитектура позволяет избежать сложностей, связанных с реализацией механизма централизованного арбитража. На выходе каждой из стадий осуществляется управление очередями с помощью одного из алгоритмов диспетчеризации.

Несмотря на то, что эта архитектура является простейшей архитектурой коммутаторов, из-за независимости стадий для нее существуют сложности с реализацией качества обслуживания (QoS) в пределах коммутатора.

1.7.3.2. Коммутаторы на основе коммутационной матрицы с арбитражем

Эта архитектура характеризуется наличием безбуферных коммутирующих элементов и арбитра, который управляет передачей трафика между входами и выходами матрицы. Отсутствие буферов у коммутирующих элементов компенсируется наличием буферов входных и выходных портов. Обычно разработчики используют один из трех методов буферизации: выходные буферы, входные буферы, комбинированные входные и выходные буферы.

В коммутаторах с входными очередями (*Input-Queued Switch*) память каждого входного порта организована в виде очереди типа FIFO (First Input First Output — «первым пришел, первым ушел»), которая используется для буферизации пакетов перед началом процесса коммутации. Одной из проблем этого типа коммутационной матрицы является *блокировка первым в очереди (Head-Of-Line blocking, HOL)*. Она 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. Для принятия решения о том, какой пакет и из какой очереди может получить доступ к матрице, используется арбитр. Перед передачей пакета входные порты направляют арбитру запросы на подключение к разделяемому ресурсу (в данном случае — пути матрицы) и получают от него право на подключение.

Арбитр принимает решение о последовательности передачи пакетов из входных очередей на основе алгоритма диспетчеризации (*scheduling algorithm*).

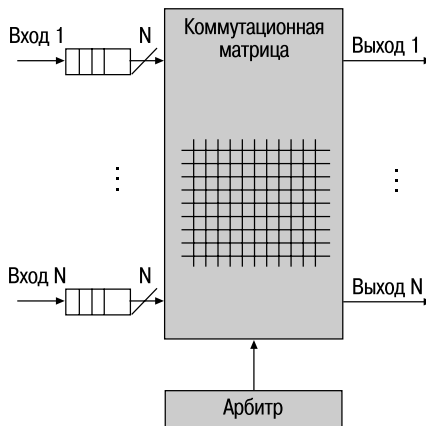


Рис. 1.15. Архитектура на основе коммутационной матрицы с входными очередями

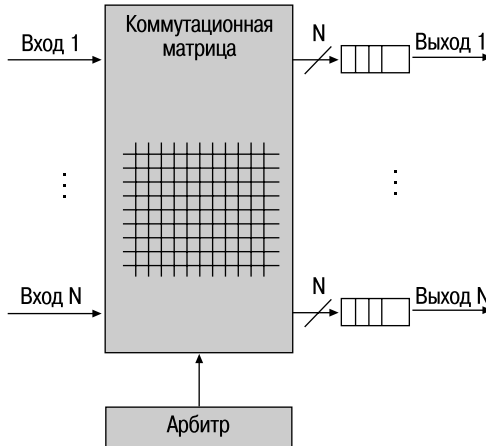


Рис. 1.16. Архитектура на основе коммутационной матрицы с выходными очередями

В коммутаторах с выходными очередями (*output-queued switch*) пакеты буферизируются только на выходных портах после завершения процесса коммутации. В этом случае удастся избежать проблемы, связанной с блокированием очередей HOL. Коммутаторы этой архитектуры используют арбитр для управления временем, за которое пакеты коммутируются через матрицу. При правильно разработанном арбитре коммутаторы с выходными очередями могут обеспечивать качество обслуживания (QoS).

Следует отметить, что выходной буфер каждого порта требует большего объема памяти по сравнению с входным буфером. Это позволяет избежать блокирования на выходе, когда все входные порты пытаются подключиться к одному выходу. Еще одним важным фактором является скорость выполнения операции «запись» коммутируемых пакетов в выходную очередь. По этим двум причинам архитектура с выходными очередями должна быть реализована на высокоскоростных элементах, что делает ее очень дорогостоящей.

Коммутаторы с *виртуальными очередями (Virtual Output Queues, VOQ)* позволяют преодолеть проблему блокировки очередей HOL, не внося издержек по сравнению с коммутаторами с выходными очередями. В этой архитектуре память каждого входного порта организована в виде N (где N — количество выходных портов) логических очередей типа FIFO, по одной для каждого выходного порта. Эти очереди используются для буферизации пакетов, поступающих на входной порт и предназначенных для выходного порта j ($j = 1, \dots, N$).

В том случае, если существует несколько виртуальных очередей, может возникнуть проблема, связанная с одновременным доступом к ком-

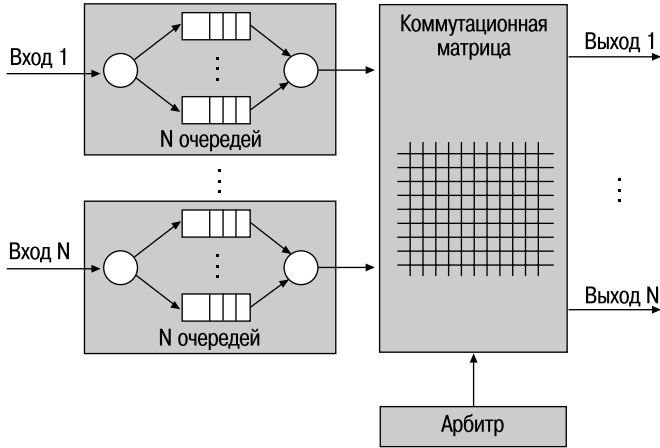


Рис. 1.17. Архитектура на основе коммутационной матрицы с виртуальными очередями

мутационной матрицы и блокировкой очередей. Для решения этой проблемы используется арбитр, который на основе алгоритма диспетчеризации выбирает пакеты из разных очередей.

В коммутаторах с комбинированными входными и выходными очередями (*Combined Input and Output Queued, CIOQ*) буферы памяти подключены как к входным, так и к выходным портам. Память каждого из входных портов организована в виде N виртуальных выходных очередей типа FIFO, по одной для каждого выходного порта. Каждый из N выходных портов также содержит очередь типа FIFO, которая используется для буферизации пакетов, ожидающих передачи через него. Система коммутации работает по принципу конвейера, каждая стадия которого называется временным слотом (*time slot*). В течение временного слота 1, который называется стадией прибытия, пакеты поступают на входные порты. Для передачи внутри коммутатора все пакеты сегментируются на ячейки фиксированного размера. Размер такой ячейки данных определяется производителем коммутатора. Каждая ячейка снабжается меткой с указанием размера, номера входного порта и порта назначения и помещается в виртуальную выходную очередь соответствующего выходного порта. Входные порты отправляют «запросы на подключение к выходам» централизованному арбитру, а все выходные порты отправляют ему «информацию о перегрузке» (переполнении выходных буферов).

Во временной слот 2, который называется стадией диспетчеризации, ячейки передаются из входных очередей в выходные. Последовательность передачи ячеек определяется централизованным арбитром с помощью алго-

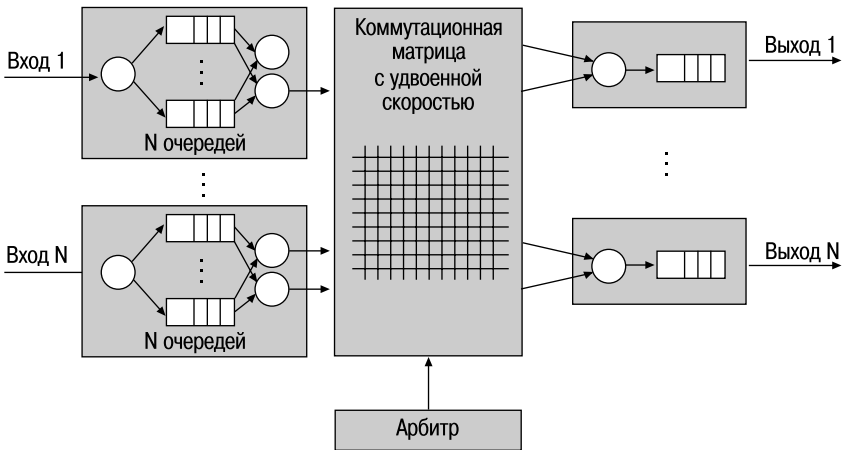


Рис. 1.18. Архитектура на основе коммутационной матрицы с CIOQ

ритма диспетчеризации. Для того чтобы выходные очереди быстро заполнялись пакетами из входных очередей (с целью уменьшения задержки передачи пакетов и обеспечения QoS), алгоритм диспетчеризации должен обеспечивать циклическое высокоскоростное сопоставление входных и выходных очередей. Это сопоставление используется для настройки управляемых переключателей матрицы перед передачей пакетов с входов на выходы.

Во временной слот 3, который называется стадией передачи, осуществляется сборка пакетов и их передача с выходных портов.

1.8. Характеристики, влияющие на производительность коммутаторов

Производительность коммутатора — характеристика, на которую сетевые интеграторы и опытные администраторы обращают внимание в первую очередь при выборе устройства.

Основными показателями коммутатора, характеризующими его производительность, являются:

- скорость фильтрации кадров;
- скорость продвижения кадров;
- пропускная способность;
- задержка передачи кадра.

Кроме того, существует несколько характеристик коммутатора, которые в наибольшей степени влияют на указанные характеристики производительности. К ним относятся:

- тип коммутации;
- размер буфера (буферов) кадров;
- производительность коммутирующей матрицы;
- производительность процессора или процессоров;
- размер таблицы коммутации.

1.8.1. Скорость фильтрации и скорость продвижения кадров

Скорость фильтрации и продвижения кадров — это две основные характеристики производительности коммутатора. Эти характеристики являются интегральными показателями и не зависят от того, каким образом технически реализован коммутатор.

Скорость фильтрации (filtering) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:

- прием кадра в свой буфер;
- отбрасывание кадра, в случае обнаружения в нем ошибки (не совпадает контрольная сумма, или кадр меньше 64 байт или больше 1518 байт);
- отбрасывание кадра для исключения петель в сети;
- отбрасывание кадра в соответствии с настроенными на порте фильтрами;
- просмотр таблицы коммутации с целью поиска порта назначения на основе MAC-адреса приемника кадра и отбрасывание кадра, если узел-отправитель и получатель кадра подключены к одному порту.

Скорость фильтрации практически у всех коммутаторов является неблокирующей — коммутатор успевает отбрасывать кадры в темпе их поступления.

Скорость продвижения (forwarding) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:

- прием кадра в свой буфер;
- просмотр таблицы коммутации с целью нахождения порта назначения на основе MAC-адреса получателя кадра;
- передача кадра в сеть через найденный по таблице коммутации порт назначения.

Как скорость фильтрации, так и скорость продвижения измеряется обычно в кадрах в секунду. Если в характеристиках коммутатора не уточняется, для какого протокола и для какого размера кадра приведены значения скоростей фильтрации и продвижения, то по умолчанию считается, что эти показатели даются для протокола Ethernet и кадров минимального размера, то есть кадров длиной 64 байт (без преамбулы) с полем данных в 46 байт. Применение в качестве основного показателя скорости обработки коммутатором кадров минимальной длины объясняется тем, что такие кадры всегда

создают для коммутатора наиболее тяжелый режим работы по сравнению с кадрами другого формата при равной пропускной способности передаваемых пользовательских данных. Поэтому при проведении тестирования коммутатора режим передачи кадров минимальной длины используется как наиболее сложный тест, который должен проверить способность коммутатора работать при наихудшем сочетании параметров трафика.

Пропускная способность коммутатора (throughput) измеряется количеством пользовательских данных (в мегабитах или гигабитах в секунду), переданных в единицу времени через его порты. Так как коммутатор работает на канальном уровне, для него пользовательскими данными являются те данные, которые переносятся в поле данных кадров протоколов канального уровня — Ethernet, Fast Ethernet и т. д. Максимальное значение пропускной способности коммутатора всегда достигается на кадрах максимальной длины, так как при этом доля накладных расходов на служебную информацию кадра гораздо ниже, чем для кадров минимальной длины, а время выполнения коммутатором операций по обработке кадра, приходящееся на один байт пользовательской информации, существенно меньше. Поэтому коммутатор может быть блокирующим для кадров минимальной длины, но при этом иметь очень хорошие показатели пропускной способности.

Задержка передачи кадра (forward delay) измеряется как время, прошедшее с момента прихода первого байта кадра на входной порт коммутатора до момента появления этого байта на его выходном порту. Задержка складывается из времени, затрачиваемого на буферизацию байт кадра, а также времени, затрачиваемого на обработку кадра коммутатором, а именно на просмотр таблицы коммутации, принятие решения о продвижении и получение доступа к среде выходного порта.

Величина вносимой коммутатором задержки зависит от используемого в нем метода коммутации. Если коммутация осуществляется без буферизации, то задержки обычно невелики и составляют от 5 до 40 мкс, а при полной буферизации кадров — от 50 до 200 мкс (для кадров минимальной длины).

1.8.2. Размер таблицы коммутации

Максимальная емкость таблицы коммутации определяет предельное количество MAC-адресов, которыми может одновременно оперировать коммутатор. В таблице коммутации для каждого порта могут храниться как динамически изученные MAC-адреса, так и статические MAC-адреса, которые были созданы администратором сети.

Значение максимального числа MAC-адресов, которое может храниться в таблице коммутации, зависит от области применения коммутатора. Коммутаторы D-Link для рабочих групп и малых офисов обычно

поддерживают таблицу MAC-адресов емкостью от 1К до 8К. Коммутаторы крупных рабочих групп поддерживают таблицу MAC-адресов емкостью от 8К до 16К, а коммутаторы магистралей сетей — как правило, от 16К до 64К адресов и более.

Недостаточная емкость таблицы коммутации может служить причиной замедления работы коммутатора и засорения сети избыточным трафиком. Если таблица коммутации полностью заполнена, и порт встречает новый MAC-адрес источника в поступившем кадре, коммутатор не сможет занести его в таблицу. В этом случае ответный кадр на этот MAC-адрес будет разослан через все порты (за исключением порта-источника), т.е. вызовет лавинную передачу.

1.8.3. Объем буфера кадров

Для обеспечения временного хранения кадров в тех случаях, когда их невозможно немедленно передать на выходной порт, коммутаторы, в зависимости от реализованной архитектуры, оснащаются буферами на входных, выходных портах или общим буфером для всех портов. Размер буфера влияет как на задержку передачи кадра, так и на скорость потери пакетов. Поэтому чем больше объем буферной памяти, тем менее вероятны потери кадров.

Обычно коммутаторы, предназначенные для работы в ответственных частях сети, обладают буферной памятью в несколько десятков или сотен килобайт на порт. Общий для всех портов буфер обычно имеет объем в несколько мегабайт.

1.9. Управление потоком в полудуплексном и дуплексном режимах

Механизм *управления потоком (Flow Control)* позволяет предотвратить потерю данных в случае переполнения буфера принимающего устройства.

Для управления потоком в *полудуплексном режиме* обычно используется *метод обратного давления (Backpressure)*. Принимающее устройство (порт коммутатора) в случае переполнения его буфера отправляет искусственно созданный сигнал обнаружения коллизии или отправляет обратно устройству-отправителю его кадры.

Для управления потоком в *дуплексном режиме* используется стандарт IEEE 802.3х. Согласно этому стандарту управление потоком осуществляется между MAC-уровнями с помощью специального кадра-паузы, который автоматически формируется MAC-уровнем принимающего устройства. В случае переполнения буфера принимающее устройство отправляет кадр-паузу с указанием периода времени, на который требуется остановить передачу данных, либо на уникальный MAC-адрес соответст-

вующей станции, либо на специальный групповой адрес 01-80-C2-00-00-01. Если переполнение буфера будет ликвидировано до истечения периода ожидания, то для восстановления передачи принимающая станция отправляет второй кадр-паузу с нулевым значением времени ожидания.

Общая схема управления потоком показана на рис. 1.19.

Дуплексный режим работы и сопутствующее ему управление потоком являются дополнительными режимами для всех MAC-уровней Ethernet независимо от скорости передачи. Кадры-паузы идентифицируются как управляющие MAC-кадры по уникальным значениям полей «Длина/тип» (88-08) и «Код операции управления MAC» (00-01).

Правильно сконфигурированная функция управления потоком на устройствах позволяет повысить общую производительность сети за счет уменьшения потери данных и повторных передач. Управление потоком

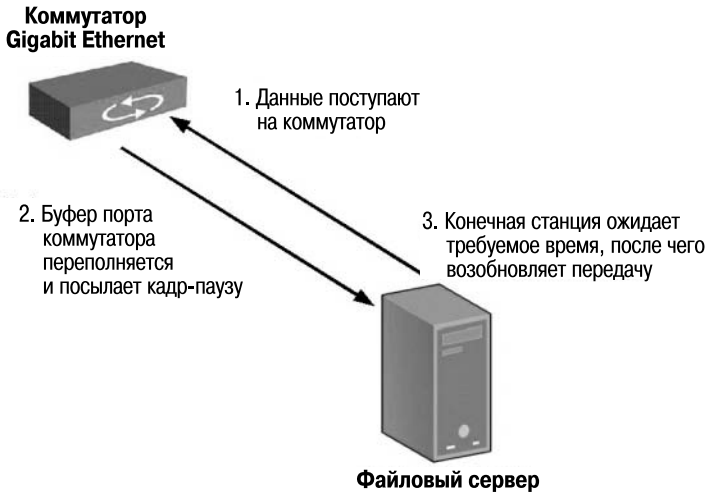


Рис. 1.19. Последовательность управления потоком IEEE 802.3x

Заголовок	Признак начала кадра	Адрес назначения	Длина/тип	Адрес источника	Код операции управления MAC (00-01)	Параметры управления MAC (от 00-00 до FF-FF)	Зарезервировано	Контрольная последовательность кадров
7 байт	1 байт	6 байт	6 байт	2 байта	2 байта	2 байта	42 байта	4 байта

Рис. 1.20. Формат кадра-паузы

данных IEEE 802.3х большинства интерфейсных сетевых карт и встроенных сетевых карт включено по умолчанию. Коммутаторы D-Link имеют разные настройки функции IEEE 802.3х по умолчанию:

- неуправляемые коммутаторы — управление потоком IEEE 802.3х включено;
- коммутаторы серии Smart — управление потоком IEEE 802.3х отключено;
- управляемые коммутаторы — управление потоком IEEE 802.3х отключено.

Поэтому для корректной работы функции IEEE 802.3х на порте коммутатора должна быть активизирована функция управления потоком.

1.10. Технологии коммутации и модель OSI

Коммутаторы локальных сетей можно классифицировать в соответствии с уровнями модели OSI, на которых они передают, фильтруют и коммутируют кадры. Различают коммутаторы уровня 2 (Layer 2 (L2) Switch) и коммутаторы уровня 3 (Layer 3 (L3) Switch).

Коммутаторы уровня 2 анализируют входящие кадры, принимают решение об их дальнейшей передаче и передают их пунктам назначения на основе MAC-адресов канального уровня модели OSI. Основное преимущество коммутаторов уровня 2 — прозрачность для протоколов верхнего уровня. Т.к. коммутатор функционирует на 2-м уровне, ему нет необходимости анализировать информацию верхних уровней модели OSI.

Коммутация 2-го уровня — аппаратная. Она обладает высокой производительностью. Передача кадра в коммутаторе может осуществляться специализированным контроллером ASIC. В основном коммутаторы 2-го уровня используются для сегментации сети и объединения рабочих групп.

Несмотря на преимущества коммутации 2-го уровня, она все же имеет некоторые ограничения. Наличие коммутаторов в сети не препятствует распространению широковещательных кадров по всем сегментам сети.

Коммутаторы уровня 3 осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней модели OSI. Коммутаторы 3-го уровня выполняют коммутацию в пределах рабочей группы и маршрутизацию между различными подсетями или виртуальными локальными сетями (VLAN).

Коммутаторы уровня 3 осуществляют маршрутизацию пакетов аналогично традиционным маршрутизаторам. Они поддерживают протоколы маршрутизации RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol) для обеспечения связи с другими коммутаторами уровня 3 или маршрутизаторами и построения

таблиц маршрутизации, осуществляют маршрутизацию на основе политик, управление многоадресным трафиком.

Существует две разновидности маршрутизации: аппаратная (коммутация 3 уровня) и программная. При аппаратной реализации пересылка пакетов осуществляется посредством специализированных контроллеров ASIC. При программной реализации для пересылки пакетов устройство использует центральный процессор. Обычно в коммутаторах 3-го уровня и старших моделях маршрутизаторов маршрутизация пакетов аппаратная, что позволяет выполнять ее на скорости канала связи, а в маршрутизаторах общего назначения функция маршрутизации выполняется программно.

1.11. Программное обеспечение коммутаторов

Программное обеспечение коммутаторов D-Link предоставляет набор программных сервисов, предназначенных для выполнения различных функций, обеспечивающих безопасность, отказоустойчивость сети, управление многоадресной рассылкой, качество обслуживания (QoS), а также развитые средства настройки и управления. Помимо этого, программное обеспечение коммутаторов взаимодействует с приложениями D-Link D-View v.6, представляющими собой прикладные программы сетевого управления. Эти управляющие программы поддерживаются всей линейкой управляемых коммутаторов D-Link.

Системное программное обеспечение располагается во Flash-памяти коммутатора, размер которой, в зависимости от модели, может быть до 32 Мбайт. Компания D-Link предоставляет возможность бесплатного обновления программного обеспечения коммутаторов по мере появления новых версий с обновленным функционалом.

1.12. Общие принципы сетевого дизайна

Грамотный сетевой проект основывается на многих принципах, базовыми из которых являются:

- *изучение возможных точек отказа сети.* Для того чтобы единичный отказ не мог изолировать какой-либо из сегментов сети, в ней может быть предусмотрена избыточность. Под избыточностью понимается резервирование жизненно важных компонентов сети и распределение нагрузки. Так, в случае отказа в сети может существовать альтернативный или резервный путь к любому ее сегменту. Распределение нагрузки используется в том случае, если к пункту назначения имеется два или более пути, которые могут использоваться в зависимости от загруженности сети. Требуемый уровень избыточности сети меняется в зависимости от ее конкретной реализации;

- *определение типа трафика сети.* Например, если в сети используются клиент-серверные приложения, то поток вырабатываемого ими трафика является критичным для эффективного распределения ресурсов, таких как количество клиентов, использующих определенный сервер, или количество клиентских рабочих станций в сегменте;
- *анализ доступной полосы пропускания.* Например, в сети не должно быть большого различия в доступной полосе пропускания между различными уровнями иерархической модели (описание иерархической модели сети находится в следующем разделе). Важно помнить, что иерархическая модель ссылается на концептуальные уровни, которые обеспечивают функциональность;
- *создание сети на базе иерархической или модульной модели.* Иерархия позволяет объединить через межсетевые устройства отдельные сегменты, которые будут функционировать как единая сеть. Фактическая граница между уровнями не обязательно должна проходить по физическому каналу связи — ею может быть и внутренняя магистраль определенного устройства.

1.13. Трехуровневая иерархическая модель сети

Иерархическая модель определяет подход к проектированию сетей и включает в себя три логических уровня (рис. 1.21):

- уровень доступа (*access layer*);
- уровень распределения/агрегации (*distribution layer*);
- уровень ядра (*core layer*).

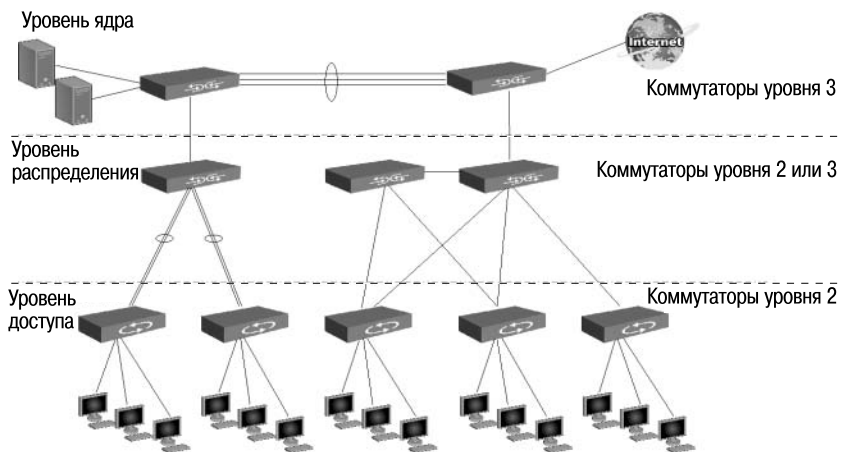


Рис. 1.21. Трехуровневая модель сети

Для каждого уровня определены свои функции. Три уровня не обязательно предполагают наличие трех различных устройств. Если провести аналогию с иерархической моделью OSI, то в ней отдельный протокол не всегда соответствует одному из семи уровней. Иногда протокол соответствует более чем одному уровню модели OSI, а иногда несколько протоколов реализованы в рамках одного уровня. Так и при построении иерархических сетей, на одном уровне может быть как несколько устройств, так и одно устройство, выполняющее все функции, определенные на двух соседних уровнях.

Уровень ядра находится на самом вершине иерархии 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.

Для уровня ядра большое значение имеет его отказоустойчивость, поскольку сбой на этом уровне может привести к потере связности между уровнями распределения сети.

Уровень распределения, который иногда называют уровнем рабочих групп, является связующим звеном между уровнями доступа и ядра. В зависимости от способа реализации уровень распределения может выполнять следующие функции:

- обеспечение маршрутизации, качества обслуживания и безопасности сети;
- агрегирование каналов;
- переход от одной технологии к другой (например, от 100Base-TX к 1000Base-T).

Уровень доступа управляет доступом пользователей и рабочих групп к ресурсам объединенной сети. Основной задачей уровня доступа является создание точек входа/выхода пользователей в сеть. Уровень выполняет следующие функции:

- управление доступом пользователей и политиками сети;
- создание отдельных доменов коллизий (сегментация);
- подключение рабочих групп к уровню распределения;
- использование технологии коммутируемых локальных сетей.

Лекция 2. Начальная настройка коммутатора

2.1. Классификация коммутаторов по возможности управления

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

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

Неуправляемые коммутаторы не поддерживают возможности управления и обновления программного обеспечения.

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

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

2.2. Средства управления коммутаторами

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

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

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

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

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

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

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

2.3. Подключение к коммутатору

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

При подключении к медному (разъем RJ-45) порту Ethernet коммутатора Ethernet-совместимых серверов, маршрутизаторов или рабочих станций используется четырехпарный кабель UTP категории 5, 5е или 6 для Gigabit Ethernet. Поскольку коммутаторы D-Link поддерживают функцию автоматического определения полярности (MDI/MDIX), можно использовать любой тип кабеля (прямой или кроссовый).

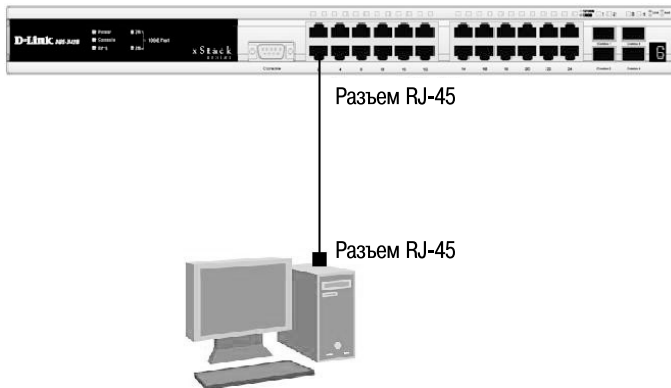


Рис. 2.1. Подключение компьютера к коммутатору

Для подключения к медному (разъем RJ-45) порту Ethernet другого коммутатора также можно использовать любой четырехпарный кабель UTP категории 5, 5е, 6, при условии, что порты коммутатора поддерживают автоматическое определение полярности. В противном случае надо использовать кроссовый кабель.

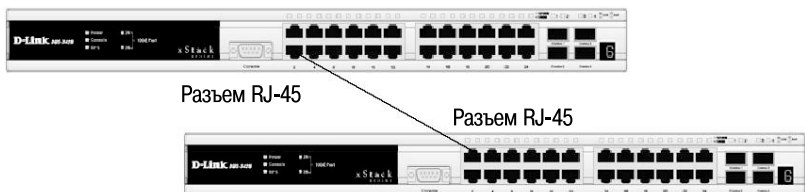


Рис. 2.2. Подключение коммутатора к обычному (не Uplink) порту коммутатора с помощью прямого или кроссового кабеля

Правильность подключения поможет определить светодиодная индикация порта. Если соответствующий индикатор горит, то связь между коммутатором и подключенным устройством установлена. Если индикатор не горит, возможно, что не включено питание одного из устройств,

или возникли проблемы с сетевым адаптером подключенного устройства, или имеются неполадки с кабелем. Если индикатор загорается и гаснет, возможно, есть проблемы с автоматическим определением скорости и режимом работы (дуплекс/полудуплекс) (за подробным описанием сигналов индикаторов необходимо обратиться к руководству пользователя коммутатора конкретной модели).

2.3.1. Подключение к консоли интерфейса командной строки коммутатора

Управляемые коммутаторы D-Link оснащены консольным портом. В зависимости от модели коммутатора консольный порт может обладать разъемом DB-9 или RJ-45. С помощью консольного кабеля, входящего в комплект поставки, коммутатор подключается к последовательному порту компьютера. Подключение по консоли иногда называют «Out-of-Band»-подключением. Это означает, что консоль использует отличную от обычного сетевого подключения схему (не использует полосу пропускающих портов Ethernet).

После подключения к консольному порту коммутатора на персональном компьютере необходимо запустить программу эмуляции терминала VT100 (например, программу HyperTerminal в Windows). В программе следует установить следующие параметры подключения, которые, как правило, указаны в документации к устройству:

Скорость (бит/с):	9600 или 115200*
Биты данных:	8
Четность:	нет
Стоповые биты:	1
Управление потоком:	нет

При соединении коммутатора с консолью появится следующее окно (только для коммутаторов, имеющих поддержку интерфейса командной строки CLI) (рис. 2.3).

Если окно не появилось, необходимо нажать Ctrl+r, чтобы его обновить.

Все управляемые коммутаторы обладают защитой от доступа неавторизованных пользователей, поэтому после загрузки устройства появится приглашение ввести имя пользователя и пароль. По умолчанию имя пользователя и пароль не определены, поэтому необходимо дважды на-

* Этот параметр зависит от модели коммутатора и указывается в руководстве пользователя.

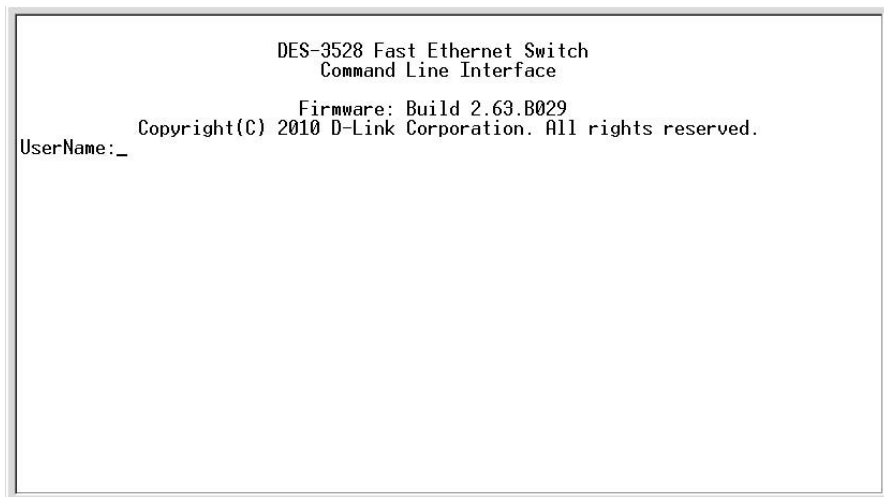


Рис. 2.3. Первоначальное окно консоли

жать клавишу Enter. После этого в командной строке появится следующее приглашение, например **DES-3528#**. Теперь можно вводить команды.

2.4. Начальная конфигурация коммутатора

2.4.1. Вызов помощи по командам

Существует большое количество команд CLI. Команды бывают сложные, многоуровневые, требующие ввода большого количества параметров, и простые, состоящие из одного параметра. Наберите в командной строке «?» и нажмите клавишу «Enter», для того чтобы вывести на экран список всех команд данного уровня.

Используйте знак вопроса «?» также в том случае, если вы не знаете параметров команды. Например, если надо узнать возможные варианты синтаксиса команды show, введите в командной строке:

```
DES-3528#show + пробел
```

Далее можно ввести «?» или нажать кнопку Enter. На экране появятся все возможные завершения команды. Также можно воспользоваться кнопкой TAB, которая будет последовательно выводить на экран все возможные завершения команды.


```

?
cable_diag ports
cfm linktrace
cfm lock md
cfm loopback
clear
clear address_binding dhcp_snoop binding_entry ports
clear address_binding nd_snoop binding_entry ports
clear arptable
clear attack_log
clear cfm pkt_cnt
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear ethernet_oam ports
clear fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear jwac auth_state
clear log
clear mac_based_access_control auth_state
CTRL+C ESC Quit SPACE h Next Page ENTER Next Entry a All

```

Рис. 2.4. Результат выполнения команды «?»

Внимание: при работе в CLI можно вводить сокращенный вариант команды. Например, если ввести команду «sh sw», то коммутатор интерпретирует эту команду как «show switch».

```

DES-3528:admin#show
Command: show
Next possible completions:
802.1p          802.1x          access_profile  account
accounting      acct_client     address_binding asymmetric_vlan
arp_spoofing_prevention
attack_log      auth_client     auth_diagnostics auth_statistics  authen
auth_session_statistics
authen_enable  authen_login    authen_policy   authentication
authorization  autoconfig      bandwidth_control bpdu_protection
cfm            command         command_history config
cpu           cpu_filter      current_config  device_status
dhcp          dhcp_local_relay dhcp_relay      dhcp_server
dhcpv6_relay   dnsr            dot1v_protocol_group
dscp          duld           erps            error

```

Время подключения: 0:09:23 Автовыбор 115200 8-N-1 SCROLL CAPS NUM Запись протокола Эхо

Рис. 2.5. Результат вызова помощи о возможных параметрах команды show

Внимание: далее в книге примеры настроек приведены для коммутаторов серии DES-3528, если не указано иное.

2.4.2. Базовая конфигурация коммутатора

Шаг 1. Обеспечение защиты коммутатора от доступа неавторизованных пользователей.

Самым первым шагом при создании конфигурации коммутатора является обеспечение его защиты от доступа неавторизованных пользователей. Самая простая форма безопасности — создание учетных записей для пользователей с соответствующими правами. Создавая учетную запись для пользователя, можно задать один из следующих уровней привилегий: *Admin*, *Operator* или *User*. Учетная запись *Admin* имеет наивысший уровень привилегий.

Создать учетную запись пользователя можно с помощью следующих команд CLI:

```
create account [admin | operator | user] <username 15>
```

Далее появится приглашение для ввода пароля и подтверждения ввода:

```
Enter a case-sensitive new password:  
Enter the new password again for confirmation:
```

Максимальная длина имени пользователя и пароля — от 0 до 15 символов. На коммутаторе можно создать до 10 учетных записей пользователей. После успешного создания учетной записи на экране появится слово *Success*.

Внимание: все команды чувствительны к регистру. Перед вводом команды удостоверьтесь, что отключен Caps Lock или другие нежелательные функции, которые изменяют регистр текста.

Ниже приведен пример создания учетной записи с уровнем привилегий «admin» и именем пользователя (Username) «dlink» на коммутаторе DES-3528:

```
DES-3528#create account admin dlink  
Command: create account admin dlink  
Enter a case-sensitive new password:****  
Enter the new password again for confirmation:****  
Success.
```

Изменить пароль для пользователя с существующей учетной записью, можно с помощью команды

```
config account <username> {encrypt [plain_text | sha_1]
<password>}
```

Ниже приведен пример создания на коммутаторе DES-3528 нового пароля для учетной записи dlink:

```
DES-3528#config account dlink
Command: config account dlink
Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success
```

Проверить созданную учетную запись можно с помощью команды

```
show account
```

Ниже приведен пример выполнения этой команды на коммутаторе DES-3528.

```
DES-3528#show account
Command: show account

Current Accounts:
Username           Access Level
-----           -
dlink              Admin

Total Entries: 1
```

Удалить учетную запись можно, выполнив команду

```
delete account <username>
```

Ниже приведен пример удаления учетной записи dlink на коммутаторе DES-3528.

```
DES-3528#delete account dlink
Command: delete account dlink
```

```
Are you sure to delete the last administrator account?(y/n)
Success.
```

Шаг 2. Настройка IP-адреса.

Для того чтобы коммутатором можно было удаленно управлять через Web-интерфейс или Telnet, ему необходимо назначить IP-адрес из адресного пространства сети, в которой планируется его использовать. IP-адрес может быть задан автоматически, с помощью протоколов DHCP или BOOTP, или статически, с помощью следующих команд CLI:

```
config ipif System dhcp
config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy
```

где xxx.xxx.xxx.xxx – IP-адрес, yyy.yyy.yyy.yyy – маска подсети, System – имя управляющего интерфейса коммутатора.

Ниже приведен пример использования команды присвоения IP-адреса управляющему интерфейсу на коммутаторе DES-3528:

```
DES-3528#config ipif System ipaddress 192.168.100.240/255.255.255.0
Command: config ipif System ipaddress 192.168.100.240/24
Success.
```

Шаг 3. Настройка параметров портов коммутатора.

По умолчанию порты всех коммутаторов D-Link поддерживают автоматическое определение скорости и режима работы (дуплекса). Но может возникнуть ситуация, в которой автоопределение будет действовать некорректно и потребуются ручная установка скорости и режима. В этом случае ручную настройку параметров необходимо выполнить на обоих концах канала связи.

Для установки параметров портов, таких как скорость передачи, дуплексный/полудуплексный режим работы, активизация/отключение управления потоком, изучение MAC-адресов, автоматическое определение полярности и т.д., на коммутаторах D-Link можно воспользоваться командой **config ports**.

Ниже приведен пример настройки параметров портов на коммутаторе DES-3528. Для портов 1, 2, 3 производятся следующие настройки: скорость передачи устанавливается равной 10 Мбит/с, активизируются дуплексный режим работы, изучение MAC-адресов, управление потоком, порты переводятся в состояние «включен».

```
DES-3528#config ports 1-3 speed 10_full learning enable state
enable flow_control enable
Command: config ports 1-3 speed 10_full learning enable state
enable flow_control enable
Success
```

Команда **show ports** <список портов> выведет на экран информацию о настройках портов коммутатора. Ниже показан результат выполнения команды **show ports** на коммутаторе DES-3528.

```
DES-3528#show ports 1-3
Command: show ports 1-3
```

Port	State/ MDIX	Settings Speed/Duplex/ FlowCtrl	Connection Speed/Duplex/ FlowCtrl	Address Learning
1	Enabled Auto	10M/Full/Enabled	Link Down	Enabled
2	Enabled Auto	10M/Full/Enabled	Link Down	Enabled
3	Enabled Auto	10M/Full/Enabled	Link Down	Enabled

Шаг 4. Сохранение текущей конфигурации коммутатора в энергонезависимую память NVRAM. Для этого необходимо выполнить команду **save**.

```
DES-3528#save
Command: save
Saving all settings to NV-RAM.....Done
```

Внимание: активная конфигурация хранится в оперативной памяти SDRAM. При отключении питания конфигурация, хранящаяся в этой памяти, будет потеряна. Для того чтобы сохранить конфигурацию в энергонезависимой памяти NVRAM, необходимо выполнить команду «save».

Шаг 5. Перезагрузка коммутатора с помощью команды **reboot**.

```
DES-3528#reboot
Command: reboot
Are you sure you want to proceed with the system reboot? (y/n)
Please wait, the switch is rebooting...
```

Сброс настроек коммутатора к заводским установкам выполняется с помощью команды

```
reset {[config | system]} {force_agree}
```

Если в команде не будет указано никаких ключевых слов, то все параметры, за исключением IP-адреса, учетных записей пользователей и Log-файла, будут возвращены к заводским параметрам по умолчанию. Коммутатор не сохранит настройки в энергонезависимой памяти NVRAM и не перезагрузится.

Если указано ключевое слово **config**, на коммутаторе восстановятся все заводские настройки по умолчанию, включая IP-адрес интерфейса управления, учетные записи пользователей и журнал регистрации. Коммутатор не сохранит настройки в энергонезависимой памяти NVRAM и не перезагрузится.

Если указано ключевое слово **system**, на коммутаторе восстановятся все заводские настройки по умолчанию в полном объеме. Коммутатор сохранит эти настройки в энергонезависимой памяти NVRAM и перезагрузится.

Параметр **force_agree** позволяет произвести безусловное выполнение команды **reset**. Не нужно вводить «Y/N». На коммутаторе восстановятся все заводские настройки по умолчанию, исключая IP-адрес, учетные записи пользователей и журнал регистрации.

```
DES-3528#reset
Command: reset
Success
```

Шаг 6. Просмотр конфигурации коммутатора.

Получить информацию о коммутаторе (посмотреть его общую конфигурацию) можно с помощью команды **show switch**.

```
DES-3528#show switch
Command: show switch
Device Type           : DES-3528 Fast Ethernet Switch
MAC Address           : 00-1E-58-50-15-10
IP Address             : 192.168.100.241 (Manual)
VLAN Name              : default
Subnet Mask            : 255.255.255.0
Default Gateway       : 0.0.0.0
Boot PROM Version     : Build 1.00.B007
Firmware Version      : Build 2.20.B028
```

```

Hardware Version      : A1
Serial Number        : P1UM186000004
System Name          :
System Location      :
System Contact       :
Spanning Tree        : Disabled
GVRP                 : Disabled
IGMP Snooping        : Disabled
MLD Snooping         : Disabled
VLAN Trunk           : Disabled
TELNET               : Enabled (TCP 23)
WEB                  : Enabled (TCP 80)
SNMP                 : Disabled
SSL Status           : Disabled

```

Команды «**Show**» являются удобным средством проверки состояния и параметров коммутатора, предоставляя информацию, требуемую для мониторинга и поиска неисправностей в работе коммутаторов. Ниже приведен список наиболее общих команд «**Show**».

show config	эта команда используется для отображения конфигурации, сохраненной в NV RAM или созданной в текущий момент
show fdb	эта команда используется для отображения текущей таблицы коммутации
show switch	эта команда используется для отображения общей информации о коммутаторе
show device_status	эта команда используется для отображения состояния внутреннего и внешнего питания коммутатора
show error ports	эта команда используется для отображения статистики об ошибках для заданного диапазона портов
show packet ports	эта команда используется для отображения статистики о переданных и полученных портом пакетах
show firmware information	эта команда используется для отображения информации о программном обеспечении коммутатора (прошивке)
show ipif	эта команда используется для отображения информации о настройках IP-интерфейса на коммутаторе
show log	эта команда используется для просмотра Log-файла коммутатора

2.5. Подключение к Web-интерфейсу управления коммутатора

Коммутаторы D-Link позволяют выполнять настройки через Web-интерфейс управления, который состоит из дружественного пользовательского графического интерфейса (GUI), запускающегося на клиенте, и HTTP-сервера, запускающегося на коммутаторе.

Web-интерфейс является альтернативой командной строки, обеспечивает графическое представление интерфейса управления коммутатора в режиме реального времени и предоставляет подробную информацию о состоянии портов, модулей, их типе и т.д.

Связь между клиентом и сервером обычно осуществляется через TCP/IP соединение с номером порта HTTP равным 80.

При первом подключении к HTTP-серверу на коммутаторе, необходимо выполнить следующие шаги:

- 1) проверить, что IP-адрес компьютера, с которого осуществляется управление, принадлежит той же подсети, что и IP-адрес коммутатора, если в сети не настроена маршрутизация. На компьютере запустить Web-браузер, в адресной строке которого ввести IP-адрес интерфейса управления коммутатора по умолчанию (обычно он указывается в руководстве пользователя);
- 2) в появившемся окне аутентификации поля User name и Password необходимо оставить пустыми и нажать кнопку ОК. После этого появится окно Web-интерфейса управления коммутатора.

Если требуется изменить IP-адрес интерфейса управления на новый, то в случае использования управляемого коммутатора необходимо подключиться к его консольному порту и, используя интерфейс командной строки, выполнить следующую команду:

```
config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy ,
```

где xxx.xxx.xxx.xxx – IP-адрес, yyy.yyy.yyy.yyy – маска подсети

Проверить правильность настройки IP-адреса коммутатора можно с помощью команды: **show ipif**

```
DES-3528#show ipif  
Command: show ipif
```

```
IP Interface           : System  
VLAN Name              : default  
Interface Admin State : Enabled
```



```

DHCPv6 Client State      : Disabled
Link Status              : LinkUp
IPv4 Address             : 192.168.100.241/24 (Manual)
Primary
Proxy ARP                : Disabled (Local : Disabled)
IPv4 State               : Enabled
IPv6 State                : Enabled

```

Total Entries: 1

При использовании настраиваемых коммутаторов изменить IP-адрес можно с помощью программы SmartConsole Utility, установленной на рабочую станцию управления.

Условно пользовательский интерфейс можно разделить на 3 области, как показано на рис. 2.6. Область 1 содержит список папок, объединяющих семейство функций, предназначенных для выполнения той или иной задачи. Например, в папке Configuration находятся функции, предназначенные для выполнения базовой конфигурации коммутатора, включая настройку IP-адреса, учетных записей пользователей, конфигурации портов и т.д. В папке L2 Features находятся функции 2-го уровня, включая Jumbo Frame, 802.1Q VLAN, QinQ, 802.1v Protocol VLAN и т.д.

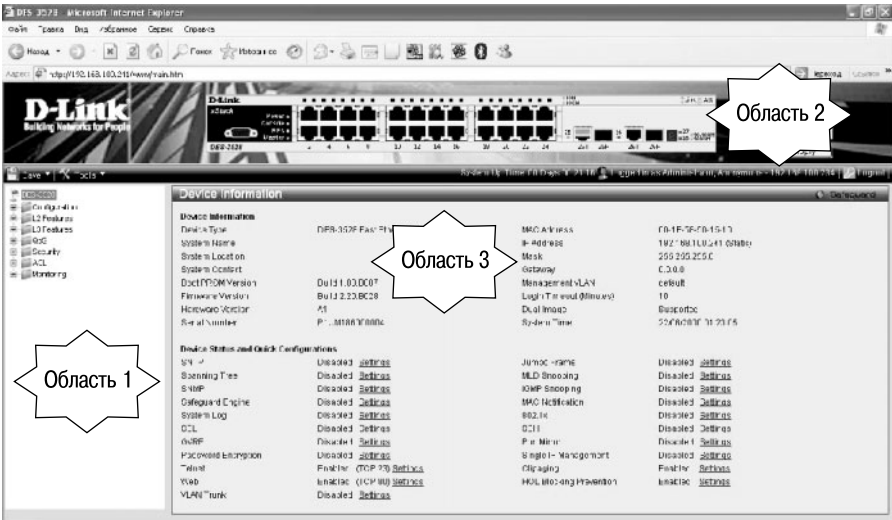


Рис. 2.6. Web-интерфейс управления

Если щелкнуть кнопкой мыши по одной из папок и выбрать необходимую функцию, то в области 3 Web-интерфейса появится окно, предназначенное для ввода и/или выбора данных.

Область 2 представляет собой графическое изображение передней панели коммутатора в режиме реального времени. Эта область отражает порты и модули расширения коммутатора и их состояние.

2.6. Загрузка нового программного обеспечения на коммутатор

В результате добавления нового функционала или исправления ошибок появляются новые версии программного обеспечения для коммутаторов D-Link, которые можно бесплатно загрузить с FTP-сервера компании ftp.dlink.ru.

Новое программное обеспечение загружается на коммутатор с помощью протокола TFTP (Trivial File Transfer Protocol). В рабочую папку установленного на рабочую станцию сервера TFTP необходимо поместить новое программное обеспечение. Сервер TFTP должен быть включен и находиться в той же IP-подсети, что и коммутатор, если в сети не настроена маршрутизация. В процессе обновления ПО нельзя выключать питание коммутатора.

Некоторые модели управляемых коммутаторов D-Link могут хранить в памяти две версии прошивки, что позволяет обеспечить работоспособность устройства в случае проблем с одной из них. Пользователи могут указать, какая из прошивок будет загружаться при старте коммутатора.

Для загрузки прошивки на коммутатор используется следующая команда (здесь приводится синтаксис коммутатора модели DES-3528; синтаксис команды в других моделях коммутаторов может отличаться):

```
download firmware_fromTFTP <ipaddr> <path_filename 64> {image_id  
<int 1-2>}
```

В качестве параметров команды надо указать IP-адрес сервера TFTP, путь к загружаемому файлу и его имя, например, C:\3528.had (можно не указывать полный путь к файлу, если он находится в рабочей директории TFTP-сервера), а также идентификатор загружаемой при старте прошивки. Например:

```
DES-3528#download firmware_fromTFTP 10.48.74.121 3528.had  
image_id 1
```

Посмотреть информацию о хранимых в памяти коммутатора прошивках можно с помощью команды

```
show firmware information
```

```
DES-3528#show firmware information
```

```
Command: show firmware information
```

ID	Version	Size(B)	Update Time	From	User
1	1.00-T003	2103164	2000/01/02 01:21:21	10.90.90.11(R)	Anonymous
*2	1.03.B008	2317149	days 00:00:00	Serial Port (Prom)	Unknown

'*' means boot up firmware

(R) means firmware update through Serial Port(RS232)

(T) means firmware update through TELNET

(S) means firmware update through SNMP

(W) means firmware update through WEB

(SSH) means firmware update through SSH

(SIM) means firmware update through Single IP Management

Для того чтобы изменить номер, загружаемой при старте коммутатора прошивки, необходимо выполнить команду:

```
config firmware image_id <int 1-2> boot_up
```

Удалить файл ПО коммутатора можно с помощью команды:

```
config firmware image_id <int 1-2> delete
```

2.7. Загрузка и резервное копирование конфигурации коммутатора

Управляемые коммутаторы позволяют осуществлять загрузку и резервное копирование конфигурации на TFTP-сервер.

Так же, как и в случае загрузки ПО, сервер TFTP должен быть включен и находиться в той же IP-подсети, что и коммутатор, если в сети не настроена маршрутизация.

Для загрузки конфигурации на коммутатор используется следующая команда:

```
download cfg_fromTFTP <ipaddr> <path_filename 64>
```

В качестве параметров команды надо указать IP-адрес сервера TFTP, путь к загружаемому файлу конфигурации, его имя.

Например:

```
DES-3528#download cfg_fromTFTP 10.48.74.121 /cfg/setting.txt
```

Для сохранения текущей конфигурации на сервере TFTP, необходимо выполнить команду:

```
upload cfg_toTFTP <ipaddr> <path_filename 64>
```

Например:

```
DES-3528#upload cfg_toTFTP 10.48.74.121 /cfg/setting.txt
```

Лекция 3. Обзор функциональных возможностей коммутаторов

Так как коммутатор представляет собой довольно сложное вычислительное устройство, имеющее несколько процессорных модулей, то, помимо выполнения основной функции передачи кадров с порта на порт по алгоритму моста, в нем реализованы дополнительные функции, полезные при построении современных, расширяемых, надежных и гибких сетей. Большинство современных коммутаторов, независимо от производителя, поддерживают множество дополнительных возможностей, отвечающих общепринятым стандартам. Среди них самые распространенные и наиболее используемые сегодня:

- виртуальные локальные сети (VLAN);
- семейство протоколов Spanning Tree – IEEE 802.1D, 802.1w, 802.1s;
- статическое и динамическое по протоколу IEEE 802.3ad агрегирование каналов Ethernet;
- сегментация трафика;
- обеспечение качества обслуживания QoS;
- функции обеспечения безопасности, включая аутентификацию 802.1X, функции Port Security, IP-MAC-Port Binding и т.д.;
- протоколы поддержки Multicast-вещания;
- SNMP-управление и др.

Лекция 4. 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-

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

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

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

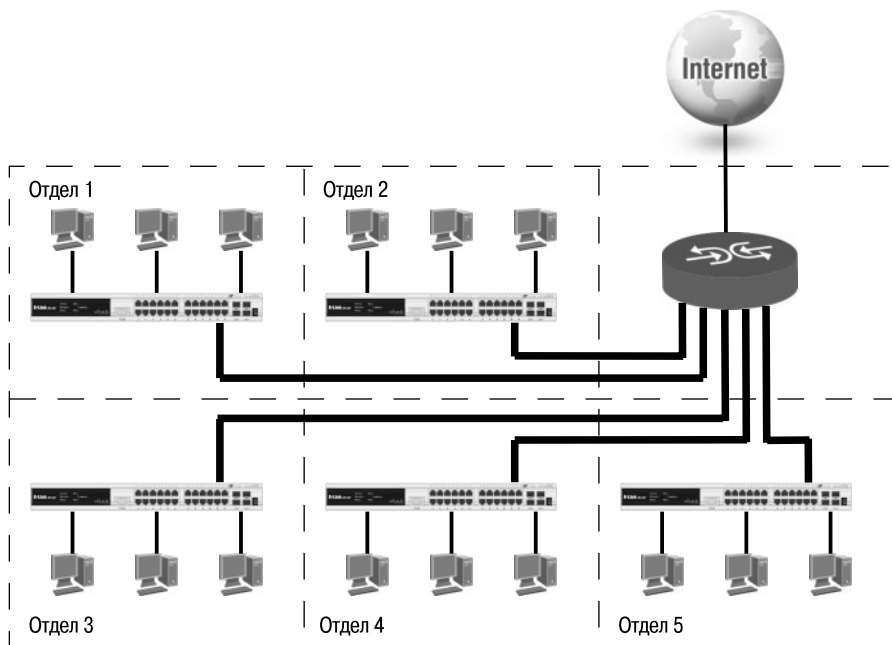


Рис. 4.1. Физическая сегментация сети

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

ных кабелей. Коммутатор, программное обеспечение которого поддерживает функцию виртуальных локальных сетей, позволяет выполнять логическую сегментацию сети путем соответствующей программной настройки. Это дает возможность подключать пользователей, находящихся в разных сегментах, к одному коммутатору, а также сокращает количество необходимых физических интерфейсов на маршрутизаторе.

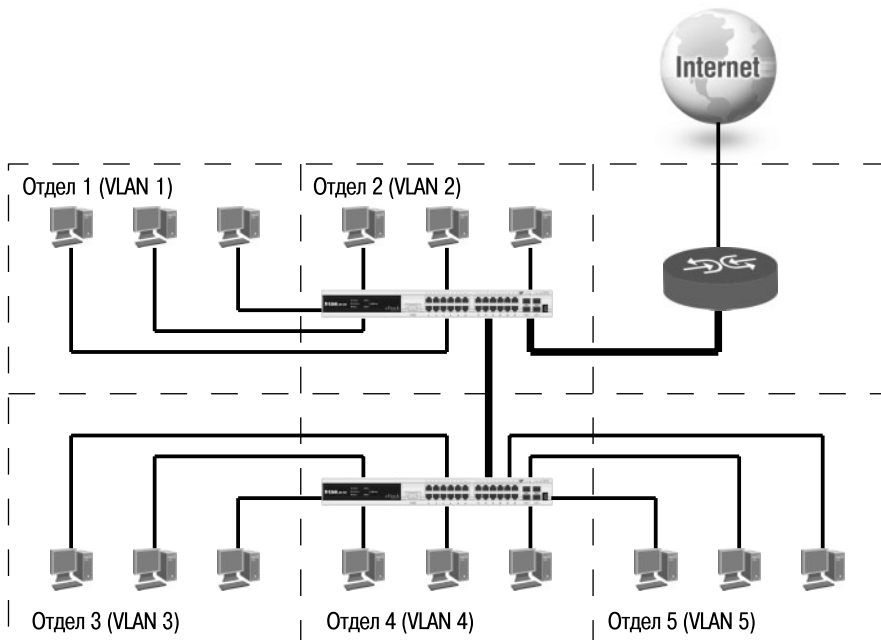


Рис. 4.2. Логическая группировка сетевых пользователей в VLAN

4.1. Типы VLAN

В коммутаторах могут быть реализованы следующие типы VLAN:

- на основе портов;
- на основе стандарта IEEE 802.1Q;
- на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
- на основе портов и протоколов IEEE 802.1v;
- на основе MAC-адресов;
- асимметричные.

Также для сегментирования сети на канальном уровне модели OSI в коммутаторах могут использоваться другие функции, например функция *Traffic Segmentation*.

4.2. VLAN на основе портов

При использовании VLAN на основе портов (Port-based VLAN) каждый порт назначается в определенную VLAN, независимо от того, какой пользователь или компьютер подключен к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной VLAN. Конфигурация портов статическая и может быть изменена только вручную.

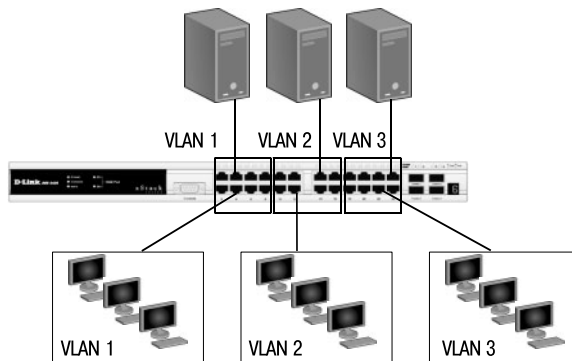


Рис. 4.3. VLAN на основе портов

Основные характеристики VLAN на основе портов:

- 1) применяются в пределах одного коммутатора. Если необходимо организовать несколько рабочих групп в пределах небольшой сети на основе одного коммутатора, например, необходимо разнести технический отдел и отдел продаж, то решение VLAN на базе портов оптимально подходит для данной задачи;
- 2) простота настройки. Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы – достаточно всем портам, помещаемым в одну VLAN, присвоить одинаковый идентификатор VLAN (VLAN ID);
- 3) возможность изменения логической топологии сети без физического перемещения станций. Достаточно всего лишь изменить настройки порта с одной VLAN (например, VLAN технического отдела) на другую (VLAN отдела продаж), и рабочая станция сразу же получает возможность совместно использовать ресурсы с членами новой VLAN. Таким образом, VLAN обеспечивают гибкость при перемещениях, изменениях и наращивании сети;
- 4) каждый порт может входить только в одну VLAN. Для объединения виртуальных подсетей как внутри одного коммутатора, так и

между двумя коммутаторами, нужно использовать сетевой уровень OSI-модели. Один из портов каждой VLAN подключается к интерфейсу маршрутизатора, который создает таблицу маршрутизации для пересылки кадров из одной подсети (VLAN) в другую (IP-адреса подсетей должны быть разными).

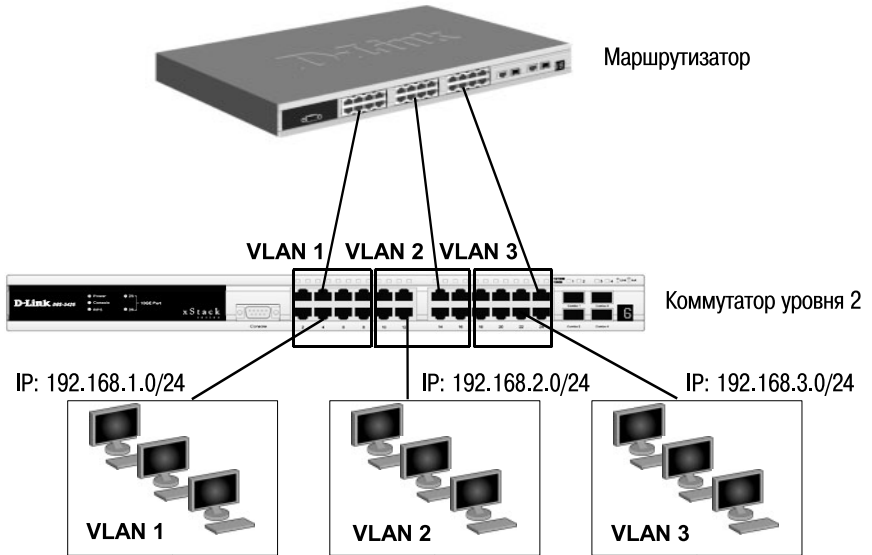


Рис. 4.4. Объединение VLAN с помощью маршрутизирующего устройства

Недостатком такого решения является то, что один порт каждой VLAN необходимо подключать к маршрутизатору. Это приводит к дополнительным расходам на покупку кабелей и маршрутизаторов, а также порты коммутатора используются очень расточительно. Решить данную проблему можно двумя способами: использовать коммутаторы, которые на основе фирменного решения позволяют включать порт в несколько VLAN, или использовать коммутаторы уровня 3.

4.3. VLAN на основе стандарта IEEE 802.1Q

Построение VLAN на основе портов основано только на добавлении дополнительной информации к адресным таблицам коммутатора и не использует возможности встраивания информации о принадлежности к виртуальной сети в передаваемый кадр. Виртуальные локальные

сети, построенные на основе стандарта IEEE 802.1Q, используют дополнительные поля кадра для хранения информации о принадлежности к VLAN при его перемещении по сети. С точки зрения удобства и гибкости настроек, VLAN стандарта IEEE 802.1Q является лучшим решением по сравнению с VLAN на основе портов. Его основные преимущества:

- 1) гибкость и удобство в настройке и изменении – можно создавать необходимые комбинации VLAN как в пределах одного коммутатора, так и во всей сети, построенной на коммутаторах с поддержкой стандарта IEEE 802.1Q. Способность добавления тегов позволяет информации о VLAN распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению (*магистральному каналу, Trunk Link*);
- 2) позволяет активизировать алгоритм связующего дерева (Spanning Tree) на всех портах и работать в обычном режиме. Протокол Spanning Tree оказывается весьма полезным для применения в крупных сетях, построенных на нескольких коммутаторах, и позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой. Для нормальной работы коммутатора требуется отсутствие замкнутых маршрутов в сети. Эти маршруты могут создаваться администратором специально для образования резервных связей или же возникать случайным образом, что вполне возможно, если сеть имеет многочисленные связи, а кабельная система плохо структурирована или документирована. С помощью протокола Spanning Tree коммутаторы после построения схемы сети блокируют избыточные маршруты. Таким образом, автоматически предотвращается возникновение петель в сети;
- 3) способность VLAN IEEE 802.1Q добавлять и извлекать теги из заголовков кадров позволяет использовать в сети коммутаторы и сетевые устройства, которые не поддерживают стандарт IEEE 802.1Q;
- 4) устройства разных производителей, поддерживающие стандарт, могут работать вместе, независимо от какого-либо фирменного решения;
- 5) чтобы связать подсети на сетевом уровне, необходим маршрутизатор или коммутатор L3. Однако для более простых случаев, например, для организации доступа к серверу из различных VLAN, маршрутизатор не потребуется. Нужно включить порт коммутатора, к которому подключен сервер, во все подсети, а сетевой адаптер сервера должен поддерживать стандарт IEEE 802.1Q.

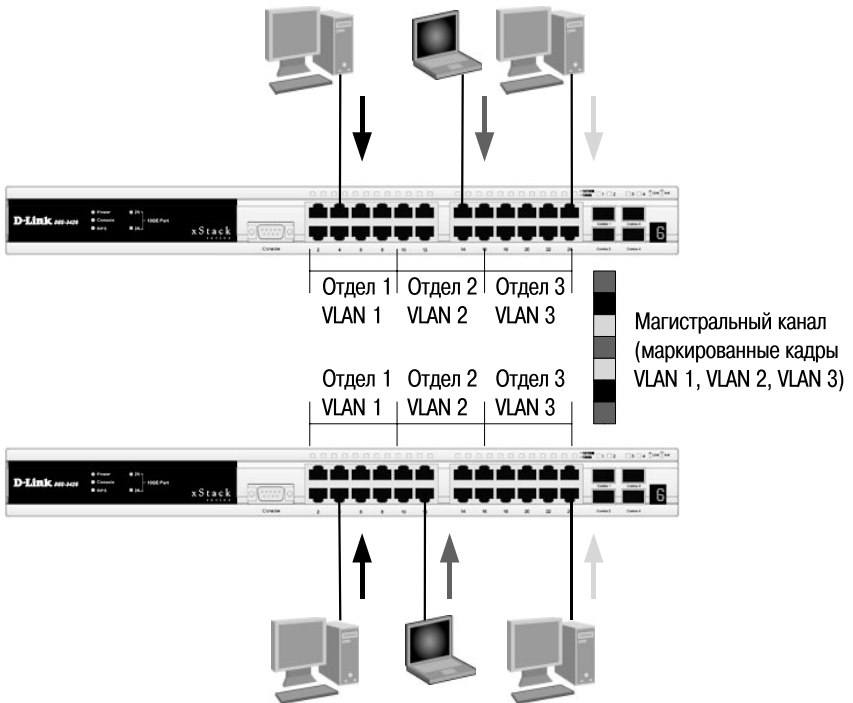


Рис. 4.5. Передача кадров разных VLAN по магистральному каналу связи

4.3.1. Некоторые определения IEEE 802.1Q

- **Tagging** («Маркировка кадра») – процесс добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра.
- **Untagging** («Извлечение тега из кадра») – процесс извлечения информации о принадлежности к 802.1Q VLAN из заголовка кадра.
- **VLAN ID (VID)** – идентификатор VLAN.
- **Port VLAN ID (PVID)** – идентификатор порта VLAN.
- **Ingress port** («Входной порт») – порт коммутатора, на который поступают кадры, и при этом принимается решение о принадлежности к VLAN.
- **Egress port** («Выходной порт») – порт коммутатора, с которого кадры передаются на другие сетевые устройства, коммутаторы или рабочие станции, и, соответственно, на нем должно приниматься решение о маркировке.

Любой порт коммутатора может быть настроен как *tagged* (маркированный) или как *untagged* (немаркированный). Функция *untagging* позволяет работать с теми сетевыми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать VLAN между несколькими коммутаторами, поддерживающими стандарт IEEE 802.1Q.

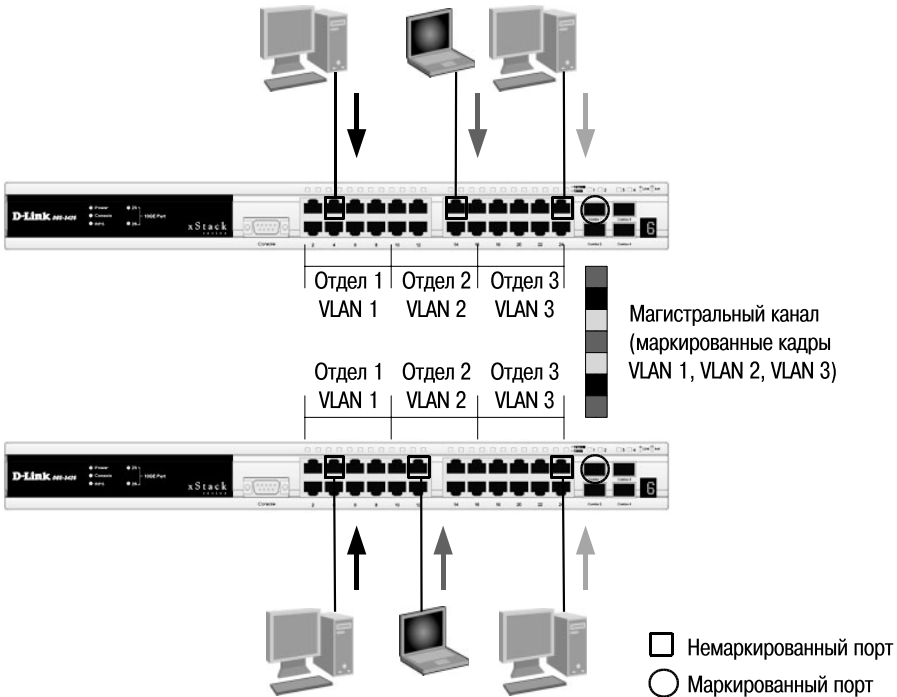


Рис. 4.6. Маркированные и немаркированные порты VLAN

4.3.2. Тер VLAN IEEE 802.1Q

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети. На рис. 4.7 изображен формат тега 802.1Q VLAN. К кадру Ethernet добавлены 32 бита (4 байта), которые увеличивают его размер до 1522 байт. Первые 2 байта (поле Tag Protocol Identifier, TPID) с фиксированным значением 0x8100 определяют, что кадр содержит тег протокола 802.1Q. Остальные 2 байта содержат следующую информацию:

- Priority («Приоритет») – 3 бита поля приоритета передачи кодируют до восьми уровней приоритета (от 0 до 7, где 7 – наивысший приоритет), которые используются в стандарте 802.1p;
- Canonical Format Indicator (CFI) – 1 бит индикатора канонического формата зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet;
- VID (VLAN ID) – 12-битный идентификатор VLAN определяет, какой VLAN принадлежит трафик. Поскольку под поле VID отведено 12 бит, то можно задать 4094 уникальных VLAN (VID 0 и VID 4095 зарезервированы).

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Данные (Data)	Контрольная последовательность кадра (CRC)
--------------------------	-------------------------	------------------	--

Маркированный кадр 802.1p/802.1Q

Адрес назначения (DA)	Адрес источника (SA)	Тег (Tag)	Данные (Data)	Контрольная последовательность кадра (CRC)
--------------------------	-------------------------	--------------	------------------	--

Идентификатор протокола тега (TPID) 0x8100	Приоритет (Priority)	Индикатор канонического формата (CFI)	Идентификатор VLAN (VID)
16 бит	3 бита	1 бит	12 бит

Рис. 4.7. Маркированный кадр Ethernet

4.3.3. Port VLAN ID

Каждый физический порт коммутатора имеет параметр, называемый *идентификатор порта VLAN (PVID)*. Этот параметр используется для того, чтобы определить, в какую VLAN коммутатор направит входящий немаркированный кадр с подключенного к порту сегмента, когда кадр нужно передать на другой порт (внутри коммутатора в заголовки всех *немаркированных кадров* добавляется идентификатор VID, равный PVID порта, на который они были приняты). Этот механизм позволяет одновременно существовать в одной сети устройствам с поддержкой и без поддержки стандарта IEEE 802.1Q.

Коммутаторы, поддерживающие протокол IEEE 802.1Q, должны хранить таблицу, связывающую идентификаторы портов PVID с идентификаторами VID сети. При этом каждый порт такого коммутатора может иметь только один PVID и столько идентификаторов VID, сколько поддерживает данная модель коммутатора.

Если на коммутаторе не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID = 1.

4.3.4. Продвижение кадров VLAN IEEE 802.1Q

Решение о продвижении кадра внутри виртуальной локальной сети принимается на основе трех следующих видов правил.

- Правила входящего трафика (*ingress rules*) – классификация получаемых кадров относительно принадлежности к VLAN.
- Правила продвижения между портами (*forwarding rules*) – принятие решения о продвижении или отбрасывании кадра.
- Правила исходящего трафика (*egress rules*) – принятие решения о сохранении или удалении в заголовке кадра тега 802.1Q перед его передачей.

Правила входящего трафика выполняют классификацию каждого получаемого кадра относительно принадлежности к определенной VLAN, а также могут служить для принятия решения о приеме кадра для дальнейшей обработки или его отбрасывании на основе формата принятого кадра.

Классификация кадра по принадлежности VLAN осуществляется следующим образом:

- а) если кадр не содержит информацию о VLAN (*немаркированный кадр*), то в его заголовок коммутатор добавляет тег с идентификатором VID, равным идентификатору PVID порта, через который этот кадр был принят;
- б) если кадр содержит информацию о VLAN (*маркированный кадр*), то его принадлежность к конкретной VLAN определяется по идентификатору VID в заголовке кадра. Значение тега в нем не изменяется.

Активизировав функцию проверки формата кадра на входе, администратор сети может указать, кадры каких форматов будут приниматься коммутатором для дальнейшей обработки. Управляемые коммутаторы D-Link позволяют настраивать прием портами либо только маркированных кадров (*tagged_only*), либо обоих типов кадров – маркированных и немаркированных (*admit_all*).

Внимание: внутри коммутатора все кадры являются маркированными.

Правила продвижения между портами осуществляют принятие решения об отбрасывании или передаче кадра на порт назначения на основе его информации о принадлежности конкретной VLAN и MAC-адреса узла-приемника.

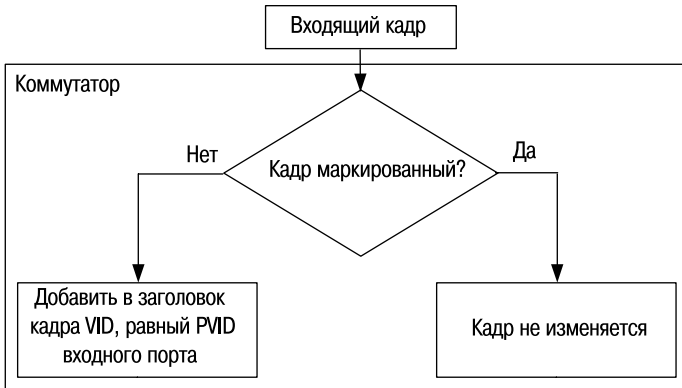


Рис. 4.8. Правила входящего трафика

Если входящий кадр маркированный, то коммутатор определяет, является ли входной порт членом той же VLAN, путем сравнения идентификатора VID в заголовке кадра и набора идентификаторов VID, ассоциированных с портом, включая его PVID. Если нет, то кадр отбрасывается. Этот процесс называется *ingress filtering* (входной фильтрацией) и используется для сохранения пропускной способности внутри коммутатора путем отбрасывания кадров, не принадлежащих той же VLAN, что и входной порт, на стадии их приема.

Если кадр немаркированный, входная фильтрация не выполняется.

Далее определяется, является ли порт назначения членом той же VLAN. Если нет, то кадр отбрасывается. Если же выходной порт входит в данную VLAN, то коммутатор передает кадр в подключенный к нему сегмент сети.

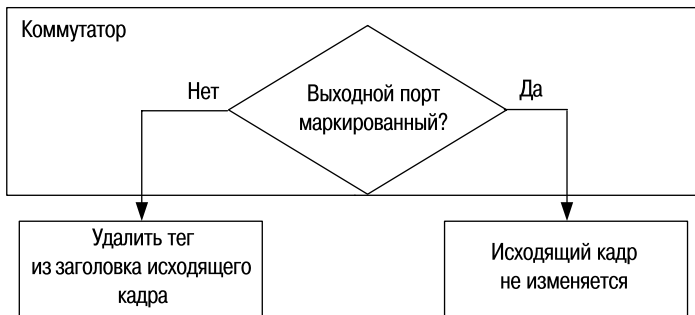


Рис. 4.9. Правила исходящего трафика

Правила исходящего трафика определяют формат исходящего кадра — маркированный или немаркированный. Если выходной порт является немаркированным (*untagged*), то он будет извлекать тег 802.1Q из заголовков всех выходящих через него маркированных кадров. Если выходной порт настроен как маркированный (*tagged*), то он будет сохранять тег 802.1Q в заголовках всех выходящих через него маркированных кадров.

На рис. 4.10–4.13 приведен пример передачи немаркированного и маркированного кадра через маркированный и немаркированный порты коммутатора.

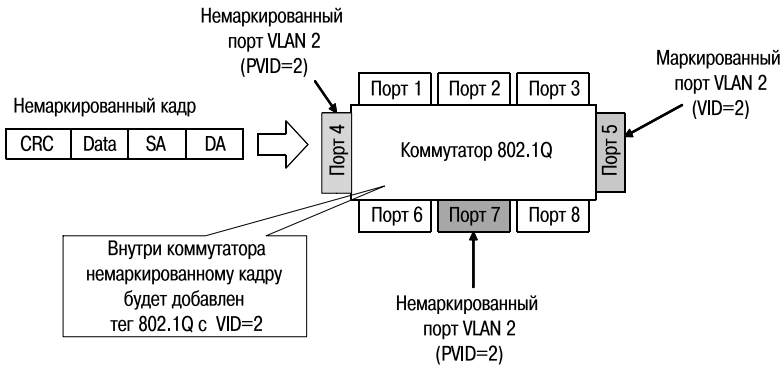
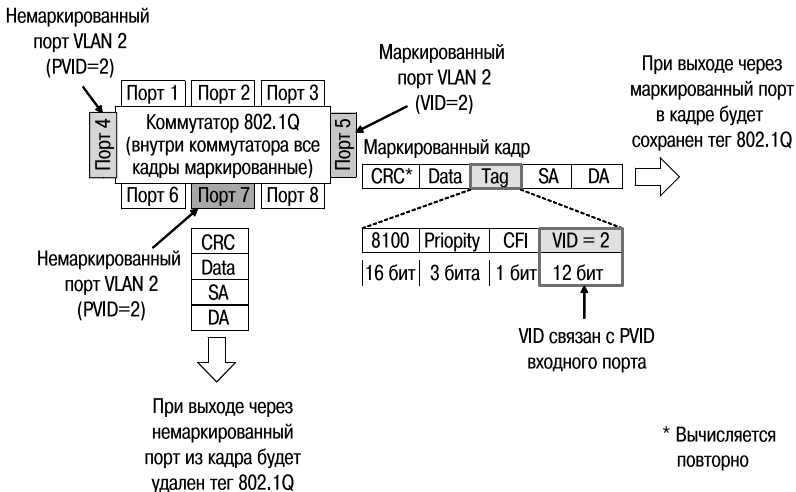


Рис. 4.10. Входящий немаркированный кадр



* Вычисляется повторно

Рис. 4.11. Немаркированный кадр, передаваемый через маркированный и немаркированный порты

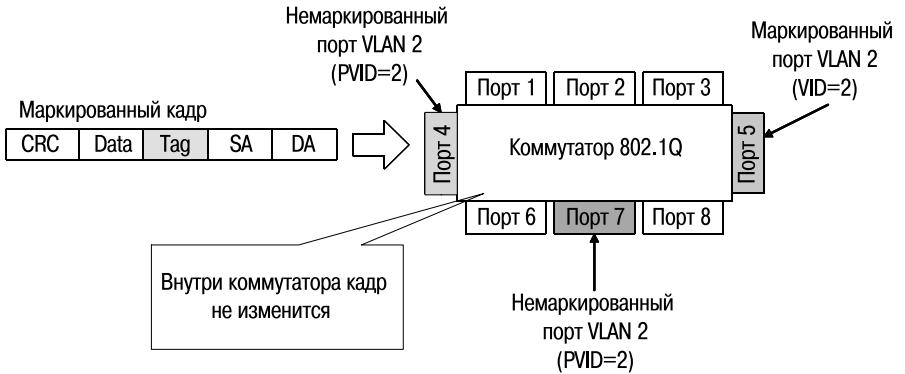


Рис. 4.12. Входящий маркированный кадр

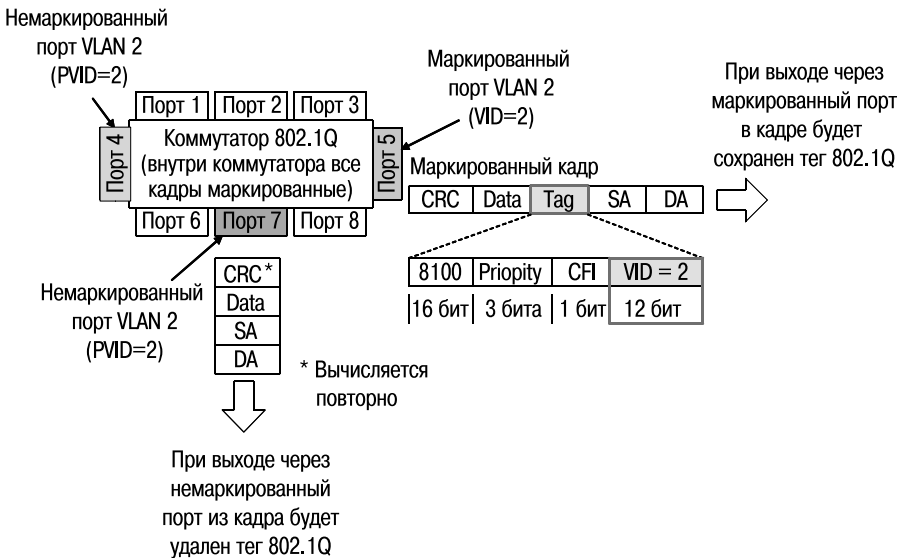


Рис. 4.13. Маркированный кадр, передаваемый через маркированный и немаркированный порты

4.3.5. Пример настройки VLAN IEEE 802.1Q

На рис. 4.14 показана схема сети, состоящая из двух групп VLAN. В качестве примера передачи данных между устройствами одной VLAN,

построенной на нескольких коммутаторах, рассмотрим пересылку кадра с порта 5 коммутатора 1 на порт 6 коммутатора 3.

- Порт 5 коммутатора 1 является немаркированным портом VLAN v2 (PVID=2). Поэтому, когда любой немаркированный кадр поступает на порт 5, коммутатор снабжает его тегом 802.1Q со значением VID, равным 2.
- Далее коммутатор 1 проверяет в своей таблице коммутации, через какой порт необходимо передать кадр и принадлежит ли этот порт VLAN v2. Кадр может быть передан через порт 1, т.к. он является маркированным членом VLAN v2. После передачи кадра через порт 1 тег 802.1Q в нем будет сохранен.
- После этого маркированный кадр поступит на порт 1 коммутатора 2. Прежде чем передать кадр дальше, порт 1 проверит, является ли он сам членом VLAN v2. Поскольку порт 1 коммутатора 2 является маркированным членом VLAN v2, он примет кадр и передаст его на порт 2, согласно таблице коммутации. После передачи кадра через порт 2 коммутатора 2 тег 802.1Q в нем будет сохранен, т.к. порт 2 является маркированным портом VLAN v2.
- Порт 1 коммутатора 3 примет поступивший кадр. После проверки на принадлежность к VLAN порт 1 передаст кадр на порт 6, найденный обычным образом в таблице коммутации коммутатора 3. Порт 6 является немаркированным портом VLAN v2, поэтому при выходе кадра через этот порт тег 802.1Q из него будет удален.

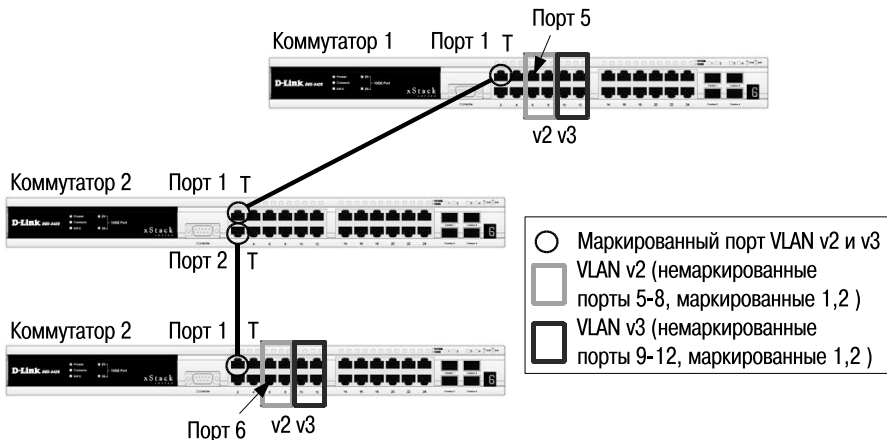


Рис. 4.14. Схема сети VLAN

Ниже приведен пример настройки коммутаторов, позволяющий реализовать заданную схему сети VLAN.

Настройка коммутатора 1

- Удалить соответствующие порты из VLAN по умолчанию (default VLAN) и создать новые VLAN.

```
config vlan default delete 1-12
create vlan v2 tag 2
create vlan v3 tag 3
```

- В созданные VLAN добавить порты, для которых необходимо указать, какие из них являются маркированными и немаркированными.

```
config vlan v2 add untagged 5-8
config vlan v2 add tagged 1-2
config vlan v3 add untagged 9-12
config vlan v3 add tagged 1-2
```

Настройка коммутатора 2

```
config vlan default delete 1-2
create vlan v2 tag 2
create vlan v3 tag 3
config vlan v2 add tagged 1-2
config vlan v3 add tagged 1-2
```

Настройка коммутаторов 3

```
config vlan default delete 1-12
create vlan v2 tag 2
create vlan v3 tag 3
config vlan v2 add untagged 5-8
config vlan v2 add tagged 1
config vlan v3 add untagged 9-12
config vlan v3 add tagged 1
```

Внимание: заводские установки по умолчанию назначают все порты коммутатора в default VLAN с VID = 1. **Перед созданием новой VLAN необходимо удалить из default VLAN все порты, которые требуется сделать немаркированными членами новой VLAN.**

4.4. Статические и динамические VLAN

Для корректной работы виртуальной локальной сети требуется, чтобы в базе данных фильтрации (*Filtering Database*) содержалась информация о членстве в VLAN. Эта информация необходима для принятия правильного решения (переслать или отбросить) при передаче кадров между портами коммутатора.

Существуют два основных способа, позволяющие устанавливать членство в VLAN:

- статические VLAN;
- динамические VLAN.

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

Членство в динамических VLAN может устанавливаться динамически на магистральных интерфейсах коммутаторов на основе протокола GVRP (GARP VLAN Registration Protocol). Протокол GARP (Generic Attribute Registration Protocol) используется для регистрации и отмены регистрации атрибутов, таких как VID.

Статические записи о регистрации в VLAN (*Static VLAN Registration Entries*) используются для представления информации о статических VLAN в базе данных фильтрации. Эти записи позволяют задавать точные настройки для каждого порта VLAN: идентификатор VLAN, тип порта (маркированный или немаркированный), один из управляющих элементов протокола GVRP:

- Fixed (порт всегда является членом данной VLAN);
- Forbidden (порту запрещено регистрироваться как члену данной VLAN);
- Normal (обычная регистрация с помощью протокола GVRP).

Управляющие элементы GVRP используются для активизации работы протокола на портах коммутатора, а также для указания того, может ли данная VLAN быть зарегистрирована на порте.

Динамические записи о регистрации в VLAN (*Dynamic VLAN Registration Entries*) используются для представления в базе данных фильтрации информации о портах, членство в VLAN которых установлено динамически. Эти записи создаются, обновляются и удаляются в процессе работы протокола GVRP.

4.5. Протокол GVRP

Протокол GVRP определяет способ, посредством которого коммутаторы обмениваются информацией о сети VLAN, чтобы автоматически за-

регистрировать членов VLAN на портах во всей сети. Он позволяет динамически создавать и удалять VLAN стандарта IEEE 802.1Q на магистральных портах, автоматически регистрировать и исключать атрибуты VLAN (под регистрацией VLAN подразумевается включение порта в VLAN, под исключением – удаление порта из VLAN).

Протокол GVRP использует сообщения GVRP BPDU (GVRP Bridge Protocol Data Units), рассылаемые на многоадресный MAC-адрес 01-80-C2-00-00-21 для оповещения устройств-подписчиков о различных событиях. Оповещения (*advertisement*) могут содержать информацию о выполнении следующих действий:

- **Join message** – регистрация порта в VLAN.

JoinEmpty: VLAN на локальном подписчике не настроена;

JoinIn: VLAN на локальном подписчике зарегистрирована;

- **Leave message** – удаление VLAN с конкретного порта.

LeaveEmpty: VLAN на локальном подписчике не настроена;

LeaveIn: VLAN на локальном подписчике удалена;

- **Leave message** – удаление всех, зарегистрированных на порте VLAN. Это сообщение отправляется после того, как истечет время, заданное таймером *LeaveAll Timer*;
- **Empty message** – требование повторного динамического оповещения и статической настройки VLAN.

4.5.1. Таймеры GVRP

- **Join Timer** – время в миллисекундах (100-100000), через которое отправляются сообщения *JoinIn* или *JoinEmpty*. Определяет промежуток времени между моментом получения коммутатором информации о вступлении в VLAN и фактическим моментом вступления в VLAN. По умолчанию установлено значение 200 миллисекунд.
- **Leave Timer** – когда коммутатор получает сообщение об исключении порта из VLAN (*Leave message*) от другого подписчика GVRP, он ожидает заданный период времени (от 100 до 100000 миллисекунд), определяемый таймером *Leave Timer*, чтобы убедиться, что информация о данной VLAN больше не существует в сети. Например, когда коммутатор получает сообщение *Leave*, он не удаляет мгновенно информацию о соответствующей VLAN, а запускает *Leave Timer* и ждет, когда его время истечет. Если за это время не

будет получено сообщение JoinIn с информацией об удаляемой VLAN, то она будет коммутатором удалена. Обычно значение таймера Leave Timer устанавливают в два раза больше значения таймера Join Timer. По умолчанию значение таймера равно 600 миллисекунд.

- **LeaveAll Timer** – интервал времени в миллисекундах (100-100000), через который отправляется сообщение LeaveAll. Когда коммутатор – подписчик GVRP получает это сообщение, он перезапускает все таймеры, включая LeaveAll Timer. Обычно значение таймера LeaveAll устанавливают в два раза больше значения таймера Leave Timer. По умолчанию значение таймера равно 10000 миллисекунд.

На рис. 4.15 показан процесс распространения информации о VLAN по сети с использованием протокола GVRP. На коммутаторе 1 созданы статические виртуальные сети VLAN v10, v20 и v30. Порт 25 является маркированным членом всех VLAN. Коммутатор 1 отправляет оповещение о VLAN v30 через порт 25 коммутатору 2 (сообщение JoinEmpty). Коммутатор 2 получает это оповещение, динамически создает VLAN v30 и включает в нее порт 25. Порт 26 коммутатора 2 отправляет оповещение о VLAN v30 коммутатору 3 (сообщение JoinEmpty), но сам не становится членом этой VLAN.

Коммутатор 3 получает оповещение, динамически создает VLAN v30 и включает в нее порт 26. Далее коммутатор 3 изменяет состояние VLAN v30 с динамического на статическое и отправляет через порт 26 сообщение JoinIn о регистрации виртуальной сети. Коммутатор 2 получает это

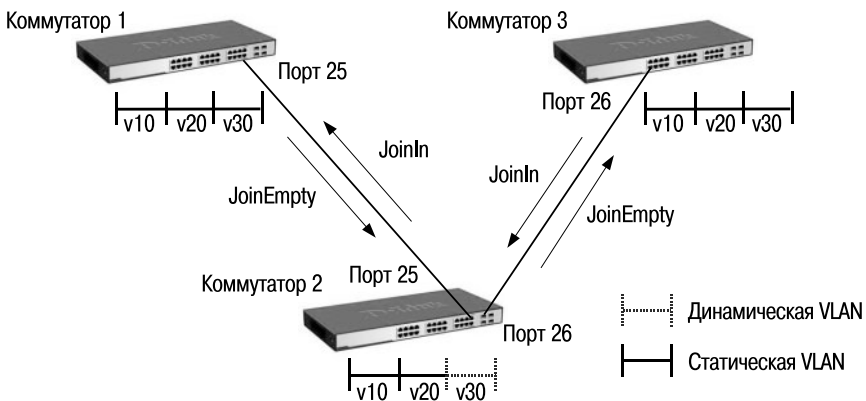


Рис. 4.15. Процесс распространения информации о регистрации VLAN по сети

оповещение и регистрирует порт 26 в VLAN v30, которая уже была создана ранее. Сообщение о регистрации VLAN v30 отправляется через порт 25 коммутатору 1. Получив это сообщение, коммутатор 1 перестает рассылать оповещения о VLAN v30.

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

Рис. 4.16 показывает процесс распространения информации об удалении VLAN по сети. На коммутаторе 1 удалена статическая VLAN v30, и он отправляет сообщение *LeaveIn* через порт 25 коммутатору 2. Когда коммутатор 2 получит оповещение об удалении VLAN v30, он исключит порт 25 из этой VLAN и отправит сообщение *LeaveIn* коммутатору 3 через порт 26. Коммутатор 3 получит оповещение об удалении VLAN v30, но удалит ее не сразу, а по истечении периода, установленного таймером *Leave Timer*. После удаления VLAN v30 коммутатор 3 отправит через порт 26 сообщение *LeaveEmpty*. После получения этого сообщения коммутатор 2 исключит порт 26 из VLAN v30 и удалит ее по истечении периода, установленного таймером *Leave Timer*. Через порт 25 будет передано сообщение *LeaveEmpty* коммутатору 1. Коммутатор 1 исключит свой порт 25 из динамической VLAN v30.

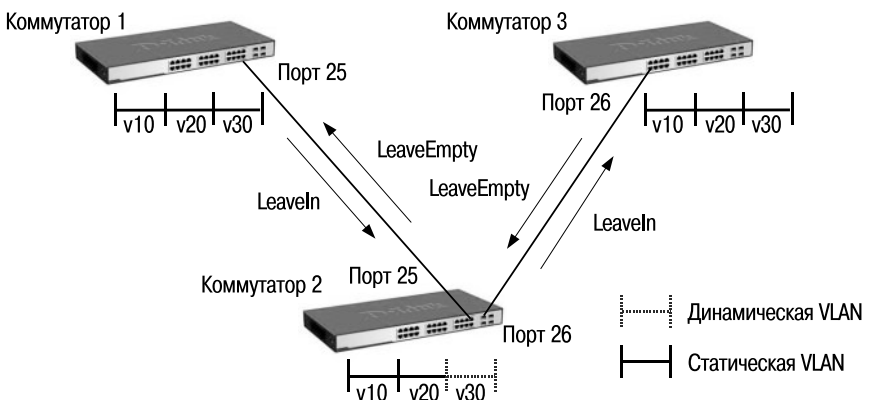
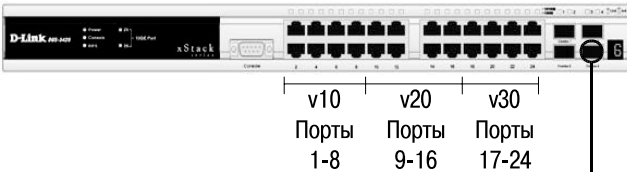


Рис. 4.16. Процесс распространения информации об удалении VLAN по сети

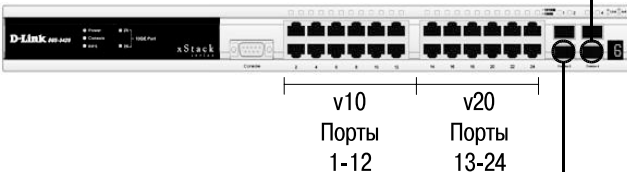
4.5.2. Пример настройки протокола GVRP

В примере, показанном на рис. 4.17, требуется настроить возможность динамического распространения по сети информации о VLAN v30 с использованием протокола GVRP. Ниже приведены настройки коммутаторов.

Коммутатор 1



Коммутатор 2



○ Маркированные порты

Коммутатор 3

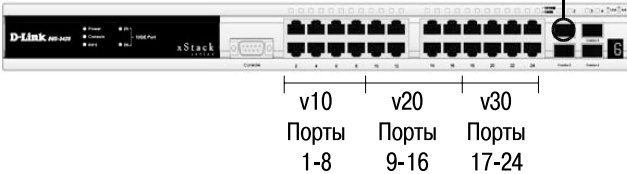


Рис. 4.17. Схема сети VLAN

Настройка коммутаторов 1, 3

- Удалить соответствующие порты из VLAN по умолчанию (default VLAN) и создать новые VLAN.

```
config vlan default delete 1-24
create vlan v10 tag 10
create vlan v20 tag 20
create vlan v30 tag 30
```

- В созданные VLAN добавить порты, для которых необходимо указать, какие из них являются маркированными и немаркированными.

```
config vlan v10 add untagged 1-8
config vlan v20 add untagged 9-16
config vlan v30 add untagged 17-24
config vlan v10 add tag 25-26
config vlan v20 add tag 25-26
```

- Активизировать протокол GVRP и функцию оповещения о соответствующей VLAN (в данном примере VLAN v30) по сети.

```
config vlan v30 advertisement enable
enable gvrp
config port_vlan 25-26 gvrp_state enable
```

Настройка коммутатора 2

```
config vlan default delete 1-24
create vlan v10 tag 10
create vlan v20 tag 20
config vlan v10 add untagged 1-12
config vlan v20 add untagged 13-24
config vlan v10 add tagged 25-26
config vlan v20 add tagged 25-26
enable gvrp
config port_vlan 25-26 gvrp_state enable
```

4.6. Q-in-Q VLAN

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

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

4.6.1. Формат кадра Q-in-Q

На рис. 4.18 изображены форматы обычного кадра Ethernet, кадра Ethernet с тегом 802.1Q, кадра Ethernet с двумя тегами 802.1Q.

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Данные (Data)	Контрольная последовательность кадра (CRC)
-----------------------	----------------------	---------------	--

Кадр с одним тегом 802.1Q

Адрес назначения (DA)	Адрес источника (SA)	Тег (Tag)	Данные (Data)	Контрольная последовательность кадра (CRC)
-----------------------	----------------------	-----------	---------------	--

Кадр с двумя тегами 802.1Q

Адрес назначения (DA)	Адрес источника (SA)	Тег (Tag)	Тег (Tag)	Данные (Data)	Контрольная последовательность кадра (CRC)
-----------------------	----------------------	-----------	-----------	---------------	--

Рис. 4.18. Формата кадра Ethernet с двумя тегами 802.1Q

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

Функция Q-in-Q позволяет расширить доступное пространство идентификаторов и использовать до $4094 \times 4094 = 16\,760\,836$ уникальных виртуальных локальных сетей.

4.6.2. Реализации Q-in-Q

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

Функция *Selective Q-in-Q* является более гибкой по сравнению с *Port-based Q-in-Q*. Она позволяет:

- маркировать кадры внешними тегами с различными идентификаторами SP-VLAN в зависимости от значений внутренних идентификаторов CVLAN;

- задавать приоритеты обработки кадров внешних SP-VLAN на основе значений приоритетов внутренних пользовательских CVLAN;
- добавлять к немаркированным пользовательским кадрам помимо внешнего тега SP-VLAN внутренний тег CVLAN.

4.6.3. Значения TPID в кадрах Q-in-Q

В теге VLAN имеется поле идентификатора протокола тега (TPID, Tag Protocol Identifier), который определяет тип протокола тега. По умолчанию значение этого поля для стандарта IEEE 802.1Q равно 0x8100.

На устройствах разных производителей TPID внешнего тега VLAN кадров Q-in-Q может иметь разные значения по умолчанию. Для того чтобы кадры Q-in-Q могли передаваться по общедоступным сетям через устройства разных производителей, рекомендуется использовать значение TPID внешнего тега равное 0x88A8, согласно стандарту IEEE 802.1ad.

4.6.4. Роли портов в Port-based Q-in-Q и Selective Q-in-Q

Все порты граничного коммутатора, на котором используются функции Port-based Q-in-Q или Selective Q-in-Q, должны быть настроены как **порты доступа (UNI)** или **Uplink-порты (NNI)**:

- **UNI (User-to-Network Interface)** – эта роль назначается портам, через которые будет осуществляться взаимодействие граничного коммутатора провайдера с клиентскими сетями;
- **NNI (Network-to-Network Interface)** – эта роль назначается портам, которые подключаются к внутренней сети провайдера или другим граничным коммутаторам.

4.6.5. Политики назначения внешнего тега и приоритета в Q-in-Q

Функция Selective Q-in-Q позволяет добавлять в кадры различные внешние теги VLAN, основываясь на значениях внутренних тегов. Для этого на портах UNI граничного коммутатора необходимо задать правила соответствия идентификаторов CVLAN идентификаторам SP-VLAN (*vlan translation*).

Помимо этого, на коммутаторах D-Link с поддержкой функции Q-in-Q, можно активизировать режим Missdrop. При настройке Selective Q-in-Q, включение этого режима позволит отбрасывать кад-

ры, не подходящие ни под одно из правил соответствия идентификаторов. При настройке Port-based Q-in-Q, режим Missdrop надо отключать, чтобы порт коммутатора мог принимать кадры не подходящие ни под одно из правил vlan translation. В этом случае входящим кадрам будет присваиваться внешний тег равный PVID соответствующего порта UNI.

Значение приоритета внешнего тега по умолчанию равно значению приоритета внутреннего тега, если кадр является маркированным. Если приоритет в полученном кадре отсутствует, то в качестве приоритета внешнего тега будет использоваться приоритет соответствующего входного порта UNI.

4.6.6. Базовая архитектура сети с функцией Port-based Q-in-Q

На рис. 4.19 показана базовая архитектура сети провайдера услуг с функцией Port-based Q-in-Q. Граничные коммутаторы сети провайдера услуг PE-1 и PE-2 позволяют обрабатывать трафик виртуальных локальных сетей двух подключенных к ним клиентских сетей. Каждому клиенту провайдером присвоен уникальный идентификатор VLAN: SP-VLAN 50 для клиента А и SP-VLAN 100 для клиента В. При передаче кадра из клиентской сети в сеть провайдера, в его заголовок будет добавляться второй тег 802.1Q: для сети А – SP-VLAN 50, для сети В – SP-VLAN 100. При передаче кадра из сети провайдера в клиентскую сеть второй тег будет удаляться граничным коммутатором.

4.6.7. Пример настройки функции Port-based Q-in-Q

Рассмотрим пример настройки функции Port-based Q-in-Q на коммутаторах D-Link. На рис. 4.20 приведена схема подключения двух клиентских VLAN к сети провайдера услуг. Граничными коммутаторами являются коммутаторы Gigabit Ethernet 3-го уровня. В сети клиента используются коммутаторы Fast Ethernet 2-го уровня.

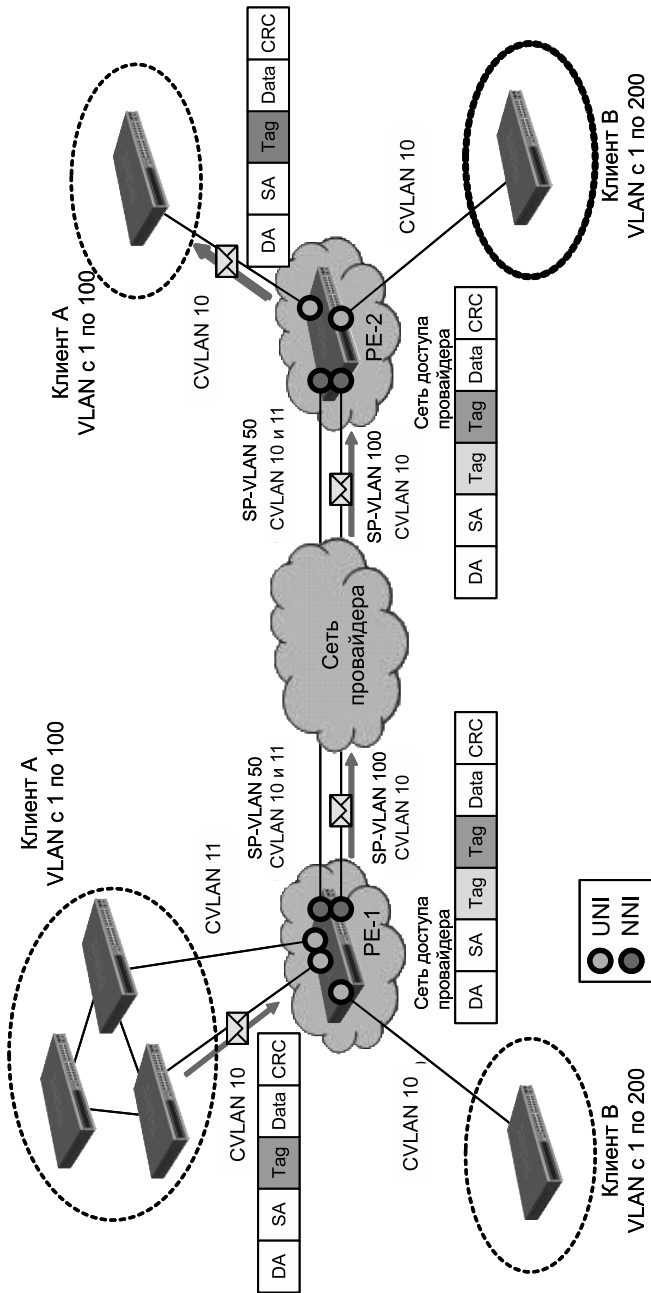
Внимание: функцию Q-in-Q VLAN необходимо настраивать только на устройствах сети провайдера услуг.

Настройка коммутатора DGS-3627

- Активизировать функцию Q-in-Q VLAN на коммутаторе.

```
enable qinq
```

Рис. 4.19. Базовая архитектура сети провайдера с применением функции Port-based Q-in-Q



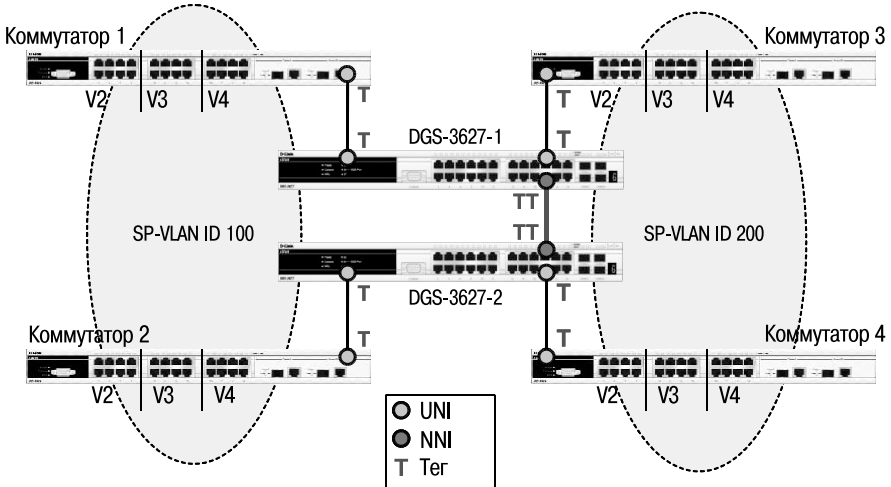


Рис. 4.20. Схема подключения клиентских VLAN к сети провайдера услуг

- Удалить соответствующие порты из Q-in-Q VLAN по умолчанию и создать новые VLAN.

```
config vlan default delete 1-24
create vlan d100 tag 100
create vlan d200 tag 200
```

- Назначить порты доступа в созданных Q-in-Q VLAN.

```
config vlan d100 add untagged 1-12
config vlan d200 add untagged 13-24
```

- Назначить Uplink-порты в созданных Q-in-Q VLAN.

```
config vlan d100 add tagged 25-27
config vlan d200 add tagged 25-27
```

- Настроить роли портов доступа в Q-in-Q и отключить режим Missdrop на них.

```
config qinq ports 1-24 role uni missdrop disable
```

Настройка коммутаторов 1, 2, 3, 4

- Удалить соответствующие порты из VLAN по умолчанию (default VLAN) и создать новые VLAN.

```
config vlan default delete 1-26
create vlan v2 tag 2
create vlan v3 tag 3
create vlan v4 tag 4
```

- В созданные VLAN добавить порты, для которых необходимо указать, какие из них являются маркированными и немаркированными.

```
config vlan v2 add untagged 1-8
config vlan v2 add tagged 25-26
config vlan v3 add untagged 9-16
config vlan v3 add tagged 25-26
config vlan v4 add untagged 17-24
config vlan v4 add tagged 25-26
```

4.6.8. Пример настройки функции Selective Q-in-Q

На рис. 4.21 показана схема подключения двух клиентских VLAN к граничным коммутаторам провайдера. Каждому клиенту провайдером назначен уникальный идентификатор: SP-VLAN 1000 для клиента CVLAN 200 и SP-VLAN 1001 для клиента CVLAN 300. В качестве граничных коммутаторов используются коммутаторы Fast Ethernet 2-го уровня. Порты 9 обоих граничных коммутаторов служат для подключения к пользовательским сетям (UNI-порты), передача данных в сеть провайдера осуществляется через порты 11 (NNI-порты).

Для того чтобы граничные коммутаторы могли осуществлять передачу пользовательских кадров с использованием функции Selective Q-in-Q, на них необходимо выполнить следующие настройки.

Настройка коммутаторов 1, 2

- Создать требуемые VLAN и добавить порты, для которых необходимо указать, какие из них являются маркированными и немаркированными.

```
create vlan v1000 tag 1000
create vlan v1001 tag 1001
```

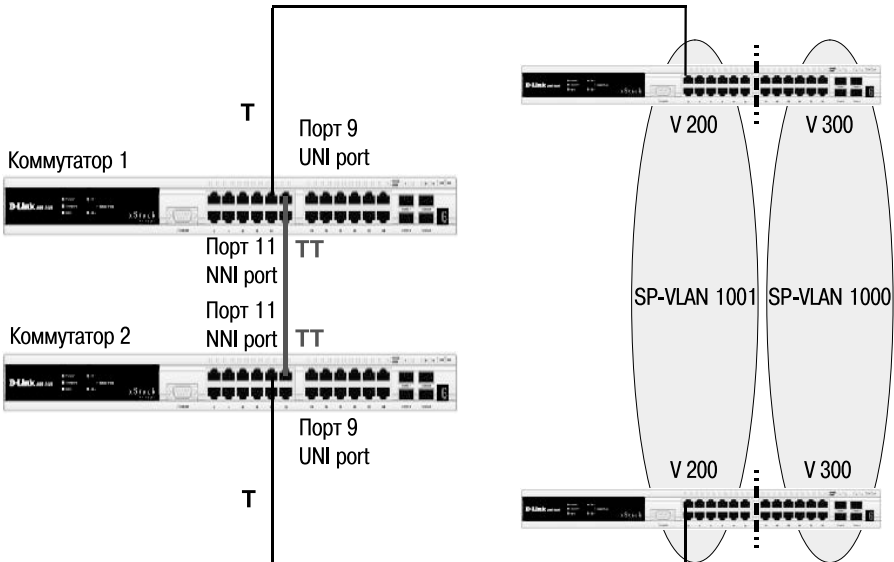



Рис. 4.21. Схема подключения клиентских VLAN к пограничным коммутаторам сети провайдера услуг

```
config vlan v1000 add tag 9,11
config vlan v1001 add tag 9,11
```

- Активизировать функцию Q-in-Q VLAN, указать значения TPID внутреннего и внешнего тега, роли портов и задать правила соответствия идентификаторов CVLAN идентификаторам SP-VLAN.

```
enable qinq
config qinq ports all 0x8100
config qinq ports 9 role uni
create vlan_translation ports 9 cvid 200 add svid 1000
create vlan_translation ports 9 cvid 300 add svid 1001
```

4.7. VLAN на основе портов и протоколов – стандарт IEEE 802.1v

Стандарт IEEE 802.1v является расширением стандарта IEEE 802.1Q. Он позволяет объединять узлы сети в виртуальные локальные сети на ос-

нове поддерживаемых ими протоколов. При определении членства в VLAN стандарт классифицирует *немаркированные* кадры по типу протокола и порту. Формат тега 802.1v аналогичен формату тега 802.1Q.

В стандарте IEEE 802.1v определены следующие правила классификации входящих кадров:

- при поступлении на порт *немаркированного* кадра, коммутатором осуществляется проверка заголовка канального уровня и типа протокола вышележащего уровня. Если тип протокола соответствует типу VLAN 802.1v на этом порте, то в заголовок кадра добавляется тег с идентификатором VID, равным идентификатору соответствующей VLAN 802.1v. Если совпадения не найдены, то в заголовок кадра добавляется тег с идентификатором VID, равным идентификатору входного порта *PVID*;
- при поступлении на порт *маркированного* кадра значение тега VLAN в нем не изменяется.

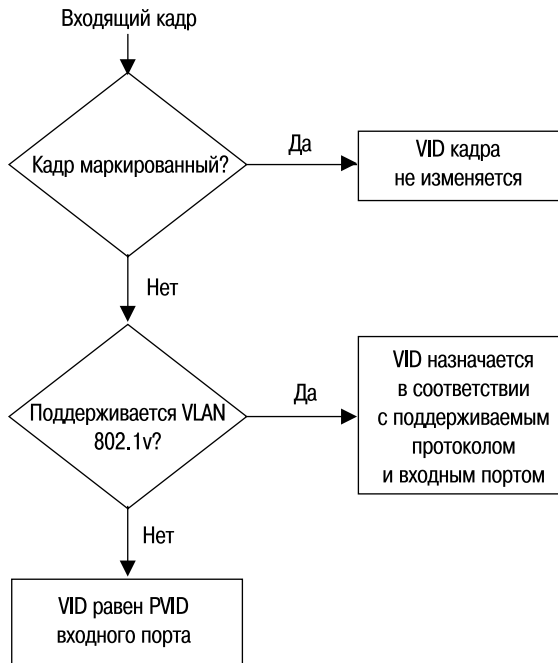


Рис. 4.22. Правила классификации входящих кадров

Внутри коммутатора все кадры являются маркированными. Передача кадров осуществляется на основе таблицы VLAN путем сравнения зна-

чений идентификаторов VID. Если порт назначения является членом той же VLAN, что и входной порт, то он передает кадр в подключенный к нему сегмент сети. В противном случае кадр отбрасывается.

Для выходных портов действуют такие же правила, как для стандарта IEEE 802.1Q.

Механизм классификации 802.1v требует, чтобы на коммутаторе были настроены группы протоколов. Каждый протокол в группе определяется типом кадра (Ethernet II, IEEE 802.3 SNAP или IEEE 802.3 LLC) и значением поля идентификации протокола в нем. Порт может быть ассоциирован с несколькими группами протоколов, что позволяет классифицировать поступающие немаркированные кадры по принадлежности к разным VLAN в зависимости от их содержимого. Одна и та же группа протоколов может быть ассоциирована с разными портами коммутатора, при этом на каждом входном порте ей должны быть присвоены уникальные идентификаторы VLAN.

4.7.1. Пример настройки IEEE 802.1v VLAN

На рис. 4.23 показано типовое подключение клиентов к сети провайдера услуг. Пользователи локальной сети находятся в выделенной VLAN

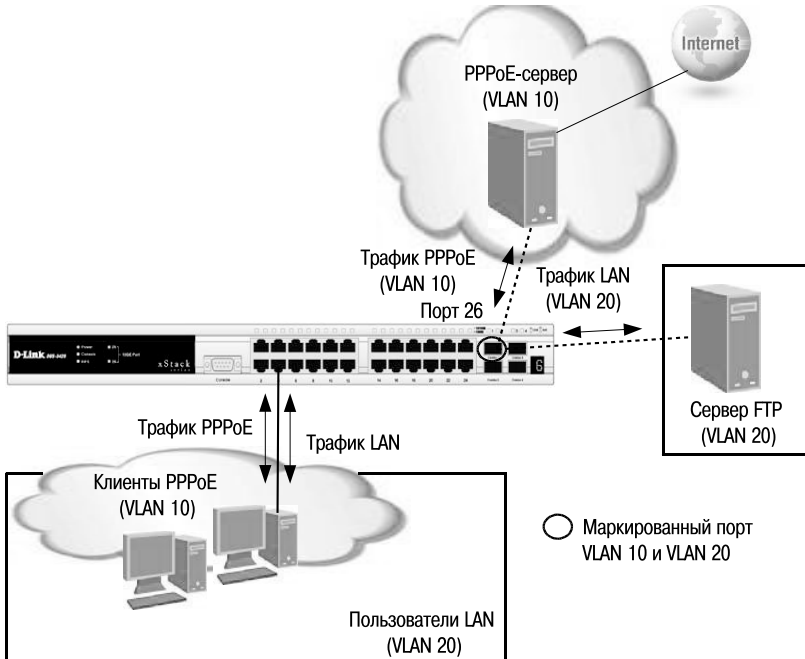


Рис. 4.23. Схема сети VLAN

(VLAN 20). Их подключение в Интернет осуществляется через PPPoE-сервер (VLAN 10). Для того чтобы трафик локальной сети был отделен от трафика PPPoE, на коммутаторе для протокола PPPoE создана VLAN 802.1v с идентификатором VID=10.

Настройка коммутатора

- Создание новых VLAN 802.1Q.

```
config vlan default delete 1-28
create vlan pppoe tag 10
config vlan pppoe add untagged 1-24
config vlan pppoe add tagged 26
create vlan base tag 20
config vlan base add tagged 26
config vlan base add untagged 1-24
```

- Настройка PVID портов, к которым подключены пользователи.

```
config port_vlan 1-24 pvid 20
```

- Создание VLAN 802.1v для протокола PPPoE (первая группа протоколов настроена для кадров PPPoE, передаваемых на стадии исследования, вторая — для кадров PPPoE установленной сессии).

```
create dot1v_protocol_group group_id 1 group_name pppoe_disc
config dot1v_protocol_group group_id 1 add protocol ethernet_2 8863
create dot1v_protocol_group group_id 2 group_name pppoe_session
config dot1v_protocol_group group_id 2 add protocol ethernet_2 8864
config port dot1v ports 1-24 add protocol_group group_id 1 vlan pppoe
config port dot1v ports 1-24 add protocol_group group_id 2 vlan pppoe
```

4.8. Асимметричные VLAN

Для обеспечения возможности использования разделяемых ресурсов (серверов, Интернет-шлюзов и т.д.) пользователями из разных сетей VLAN в программном обеспечении коммутаторов **2-го уровня D-Link** реализована поддержка функции *Asymmetric VLAN* (асимметричные VLAN). Эта функция позволяет клиентам из разных VLAN взаимодействовать с разделяемыми устройствами (например, серверами), *не поддерживающими* тегирование *802.1Q*, через один физический канал связи с коммутатором, не требуя использования внешнего маршрутизатора.

ра. Активизация функции Asymmetric VLAN на коммутаторе 2-го уровня позволяет сделать его *немаркированные* порты членами *нескольких виртуальных локальных сетей*. При этом рабочие станции остаются полностью изолированными друг от друга. Например, асимметричные VLAN могут быть настроены так, чтобы обеспечить доступ к почтовому серверу всем почтовым клиентам. Клиенты смогут отправлять и получать данные через порт коммутатора, подключенный к почтовому серверу, но прием и передача данных через остальные порты будет для них запрещена.

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

Внимание: функция Asymmetric VLAN не поддерживается коммутаторами 3-го уровня. Организация обмена данными между устройствами различных VLAN, не поддерживающих тегирование, реализуется в таких коммутаторах с помощью маршрутизации и списков управления доступом (ACL), ограничивающих доступ устройств к сети.

Основное различие между базовым стандартом 802.1Q VLAN (или симметричными VLAN) и асимметричными VLAN заключается в том, как выполняется отображение MAC-адресов. Симметричные VLAN используют отдельные адресные таблицы, и, таким образом, не происходит пересечения MAC-адресов между виртуальными локальными сетями. Асимметричные VLAN используют одну общую таблицу MAC-адресов.

При использовании асимметричных VLAN существует следующее ограничение: не функционирует механизм IGMP Snooping.

По умолчанию асимметричные VLAN на коммутаторах D-Link отключены.

4.8.1. Примеры настройки асимметричных VLAN

На рис. 4.24 показана схема реализации асимметричных VLAN в пределах одного коммутатора. Пользователи VLAN v2 и v3 могут получать доступ к разделяемым серверам и Интернет-шлюзу, находящимся в VLAN v1. Виртуальные локальные сети VLAN v2 и v3 изолированы друг от друга.

Для реализации этой схемы на коммутаторе D-Link необходимо выполнить следующие настройки:

Настройка коммутатора

```
enable asymmetric_vlan
create vlan v2 tag 2
create vlan v3 tag 3
config vlan v2 add untagged 9-24
config vlan v3 add untagged 1-8, 17-24
config gvrp 1-8 pvid 3
config gvrp 9-16 pvid 2
config gvrp 17-24 pvid 1
```

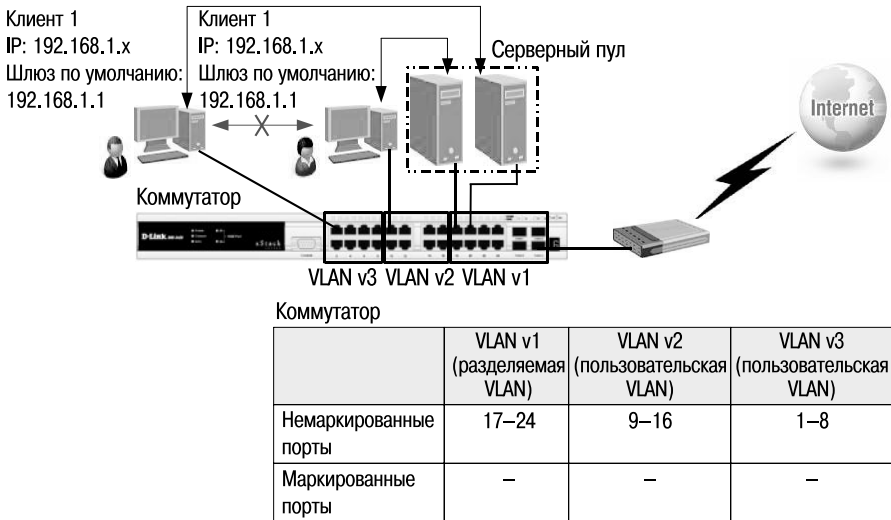


Рис. 4.24. Асимметричные VLAN в пределах одного коммутатора

4.9. Функция Traffic Segmentation

Функция *Traffic Segmentation* (сегментация трафика) служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов или магистральной сети. Этот метод изоляции трафика аналогичен функции Asymmetric VLAN, но его применение ограничено пределами одного коммутатора или нескольких коммутаторов в стеке, т.к. членство в группе портов не может распространяться по сети.

Можно выделить следующие преимущества функции Traffic Segmentation по сравнению с Asymmetric VLAN:

- простота настройки;
- поддерживается работа IGMP Snooping;
- функция Traffic Segmentation может быть представлена в виде иерархического дерева (при иерархическом подходе разделяемые ресурсы должны быть на «вершине» дерева);
- нет ограничений на создание количества групп портов.

Функция сегментации трафика может использоваться с целью сокращения трафика внутри сетей VLAN 802.1Q, позволяя разбивать их на более маленькие группы. При этом правила VLAN имеют более высокий приоритет при передаче трафика. Правила Traffic Segmentation применяются после них.

4.9.1. Примеры использования и настройки функции Traffic Segmentation

В качестве примера рассмотрим решение задачи совместного использования ресурсов сети разными группами пользователей с использованием функции Traffic Segmentation (рис. 4.25).

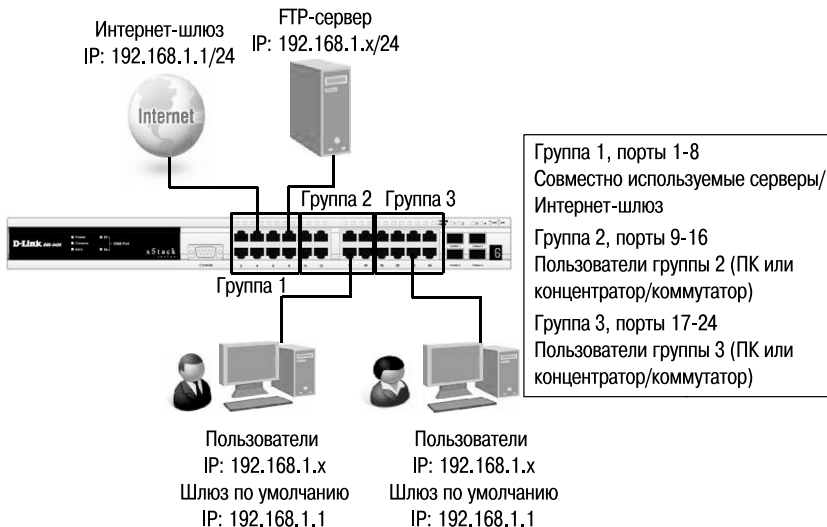


Рис. 4.25. Пример использования функции Traffic Segmentation

Пользователи групп 2 и 3 имеют доступ к совместно используемому FTP-серверу и Интернет-шлюзу, но обмен данными между группами 2 и 3 запрещен.

Настройка коммутатора

```
config traffic_segmentation 1-8 forward_list 1-24
config traffic_segmentation 9-16 forward_list 1-16
config traffic_segmentation 17-24 forward_list 1-8,17-24
```

Используя возможности построения иерархического дерева функции Traffic Segmentation, можно решать типовые задачи изоляции портов в сетях с многоуровневой структурой.

В примере, показанном на рис. 4.26, все компьютеры от А до Q, находящиеся в одной IP-подсети, не могут принимать/отправлять пакеты данных друг другу, но при этом имеют доступ к серверам и Интернету. Все коммутаторы сети поддерживают иерархию Traffic Segmentation.

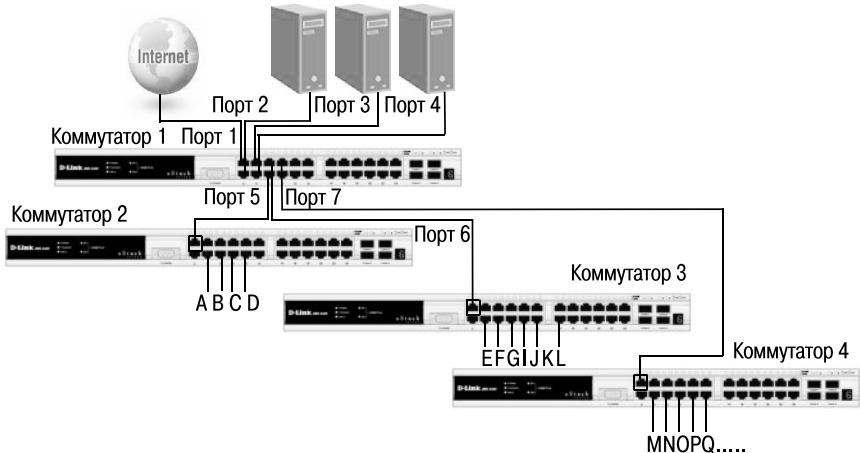


Рис. 4.26. Иерархическая структура Traffic Segmentation

Настройка коммутатора 1

```
config traffic_segmentation 1-4 forward_list 1-26
config traffic_segmentation 5 forward_list 1-5
config traffic_segmentation 6 forward_list 1-4, 6
config traffic_segmentation 7 forward_list 1-4, 7
```

Настройка коммутаторов 2, 3, 4

```
config traffic_segmentation 1 forward_list 1-26
config traffic_segmentation 2-26 forward_list 1
```


Лекция 5. 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.

5.1. 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).

5.2. Spanning Tree Protocol (STP)

5.2.1. Понятие петель

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

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

Широковещательный шторм.

Распространение широковещательных сообщений в сетях с петлями представляет серьезную проблему. Предположим, что первый кадр, поступивший от одного из узлов, является широковещательным. Тогда все коммутаторы будут пересылать кадры бесконечно, как показано на рис. 5.1 (пример 1), используя всю доступную полосу пропускания сети и блокируя передачу других кадров во всех сегментах.

Множественные копии кадров.

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

Множественные петли.

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

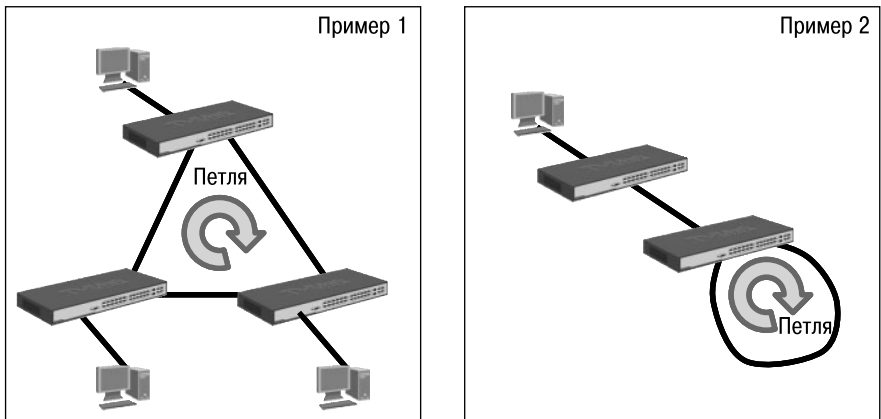


Рис. 5.1. Примеры петель между коммутаторами

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

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

ти. Такая конфигурация называется связующим деревом – Spanning Tree (иногда ее называют остовым или покрывающим деревом). Конфигурация связующего дерева строится коммутаторами автоматически с использованием обмена служебными кадрами, называемыми *Bridge Protocol Data Units (BPDU)*.

5.2.2. Построение активной топологии связующего дерева

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

Процесс вычисления связующего дерева начинается с выбора **корневого моста (Root Bridge)**, от которого будет строиться дерево. В качестве корня дерева выбирается коммутатор с наименьшим значением идентификатора моста. Идентификатор моста – это 8-байтное поле, которое состоит из 2-х частей: приоритета моста (2 байта), назначаемого администратором сети, и MAC-адреса блока управления коммутатора (6 байт). При сравнении идентификаторов двух коммутаторов сначала сравниваются значения приоритетов. Корневым мостом становится коммутатор с наименьшим значением приоритета. Если они одинаковы (по умолчанию приоритет равен 32768), то корневой мост определяется по наименьшему MAC-адресу.

Для того чтобы в качестве корневого моста было выбрано определенное устройство (исходя из структуры сети), администратор может вручную назначить соответствующему коммутатору наименьший приоритет.

Второй этап работы STP – выбор **корневых портов (Root Port)**.

Когда процесс выбора корневого моста завершен, оставшиеся коммутаторы сети определяют стоимость каждого возможного пути от себя до корня дерева. Стоимость пути рассчитывается как *суммарное условное время* на передачу данных от порта данного коммутатора до порта корневого моста. Условное время сегмента рассчитывается как время передачи одного бита информации через канал с определенной полосой пропускания. Стоимости пути по умолчанию для каждого канала определены в стандарте IEEE 802.1D-1998.

Сравнив стоимости всех возможных маршрутов до корня, каждый коммутатор выбирает среди них один с наименьшим значением стоимости. Порт, соединяющий коммутатор с этим маршрутом, становится корневым портом. В случае если минимальные стоимости пути нескольких маршрутов окажутся одинаковыми, корневым портом станет порт, имеющий наименьшее значение идентификатора порта.

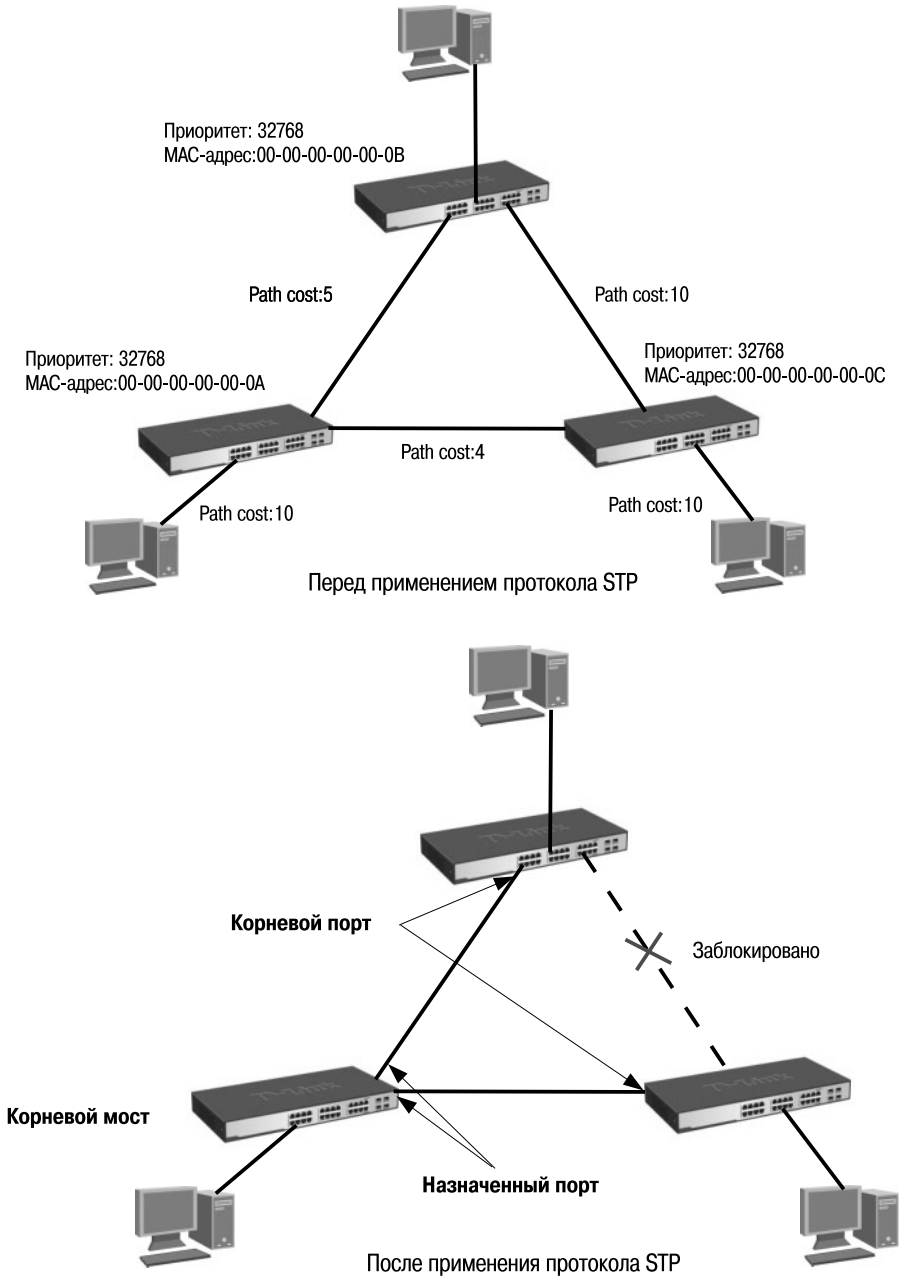


Рис. 5.2. Пример функционирования протокола STP

Третий шаг работы STP – определение **назначенных портов** (*Designated Port*).

Каждый сегмент в коммутируемой сети имеет один назначенный порт. Этот порт функционирует как единственный порт моста, т.е. принимает кадры от сегмента и передает их в направлении корневого моста через корневой порт данного коммутатора. Коммутатор, содержащий назначенный порт для данного сегмента, называется **назначенным мостом** (*Designated Bridge*) этого сегмента. Назначенный порт сегмента определяется путем сравнения значений стоимости пути всех маршрутов от данного сегмента до корневого моста. Им становится порт, имеющий наименьшее значение стоимости, среди всех портов, подключенных к данному сегменту. Если минимальные значения стоимости пути окажутся одинаковыми у двух или нескольких портов, то для выбора назначенного порта сегмента STP принимает решение на основе последовательного сравнения идентификаторов мостов и идентификаторов портов.

У корневого моста все порты являются назначенными, а их расстояние до корня полагается равным нулю. Корневого порта у корневого моста нет.

После выбора корневых и назначенных портов все остальные порты коммутаторов сети переводятся в состояние Blocking («Блокировка»), то есть такое, при котором они принимают и передают только кадры BPDU. При таком выборе активных портов в сети исключаются петли, и оставшиеся связи образуют связующее дерево.

5.2.3. Bridge Protocol Data Unit (BPDU)

Вычисление связующего дерева происходит при включении коммутатора и при изменении топологии. Эти вычисления требуют периодического обмена информацией между коммутаторами связующего дерева, что достигается при помощи специальных кадров, называемых блоками данных протокола моста – BPDU (Bridge Protocol Data Unit).

Коммутатор отправляет BPDU, используя уникальный MAC-адрес порта в качестве адреса-источника и многоадресный MAC-адрес протокола STP 01-80-C2-00-00-00 в качестве адреса-приемника. Кадры BPDU помещаются в поле данных кадров канального уровня, например, кадров Ethernet.

Внимание: иногда, с целью повышения безопасности, сетевым администраторам необходимо отключать возможность передачи кадров BPDU на граничные коммутаторы сети, чтобы избежать получения случайных кадров BPDU клиентскими портами, которые могут распространить вычисления STP по клиентским сетям. Управляемые коммутаторы D-Link поддерживают возможность включения и отключения передачи кадров BPDU для каждого порта.

Существует три типа кадров BPDU:

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

Коммутаторы обмениваются BPDU через равные интервалы времени (по умолчанию 2 сек.), что позволяет им отслеживать состояние топологии сети.

	Байты
Идентификатор протокола (Protocol Identifier)	2
Версия протокола (Protocol Version Identifier)	1
Тип BPDU (BPDU Type)	1
Флаги (Flags)	1
Идентификатор корневого моста (Root Identifier)	8
Расстояние до корневого моста (Root Path Cost)	2
Идентификатор моста (Bridge Identifier)	8
Идентификатор порта (Port Identifier)	2
Время жизни сообщения (Message Age)	2
Максимальное время жизни сообщения (Max Age)	2
Время приветствия (Hello Time)	2
Задержка смены состояний (Forward Delay)	2

Рис. 5.3. Формат кадра BPDU

Кадр BPDU состоит из следующих полей:

- идентификатор протокола (Protocol Identifier) – 2 байта. Значение всегда равно 0;
- версия протокола STP (Protocol Version Identifier) – 1 байт. Значение всегда равно 0;
- тип BPDU (BPDU Type) – 1 байт. Значение «00» – конфигурационный BPDU, «01» – изменение топологии;

- флаги (Flags) – 1 байт. Бит 1 – флаг изменения топологии, бит 8 – флаг подтверждения изменения топологии;
- идентификатор корневого моста (Root Identifier) – 8 байтов. Идентификатор текущего корневого моста;
- расстояние до корневого моста (Root Path Cost) – 2 байта. Суммарная стоимость пути до корневого моста;
- идентификатор моста (Bridge Identifier) – 8 байтов. Идентификатор текущего моста;
- идентификатор порта (Port Identifier) – 2 байта. Уникальный идентификатор порта, который отправил этот BPDU;
- время жизни сообщения (Message Age) – 2 байта. Нефиксированный временной интервал в секундах, прошедший с момента отправки BPDU корневым мостом. Служит для выявления устаревших сообщений BPDU. Первоначальное значение равно нулю. По мере передачи кадра BPDU по сети каждый коммутатор добавляет ко времени жизни сообщения время его задержки данным коммутатором. По умолчанию оно равно 1 сек. Значение параметра Message Age должно быть меньше значения таймера Max Age;
- максимальное время жизни сообщения (Max Age) – 2 байта. Временной интервал в секундах, определяющий максимальное время хранения конфигурации STP, прежде чем коммутатор ее отбросит;
- время приветствия (Hello Time) – 2 байта. Временной интервал в секундах, через который посылаются кадры BPDU;
- задержка смены состояний (Forward Delay) – 2 байта. Временной интервал в секундах, в течение которого порт коммутатора находится в состояниях «Прослушивание» и «Обучение».

5.2.4. Состояния портов

В процессе построения топологии сети каждый порт коммутатора проходит несколько стадий:

- **Blocking** («Блокировка») – при инициализации коммутатора все порты (за исключением отключенных) автоматически переводятся в состояние «Заблокирован». В этом случае порт принимает и обрабатывает только кадры BPDU. Все остальные кадры отбрасываются;
- **Listening** («Прослушивание») – в этом состоянии порт продолжает принимать, обрабатывать и ретранслировать только кадры BPDU. Из этого состояния порт может перейти в состояние «Заблокирован», если получит BPDU с лучшими параметрами, чем его собственные (стоимость пути, идентификатор моста или порта). В противном случае, при истечении периода, установленного

таймером задержки смены состояний (Forward Delay), порт перейдет в следующее состояние «Обучение»;

- **Learning** («Обучение») – порт начинает принимать все кадры и на основе MAC-адресов источника строить таблицу коммутации. Порт в этом состоянии все еще не продвигает кадры. Порт продолжает участвовать в работе алгоритма STP и при поступлении BPDU с лучшими параметрами переходит в состояние «Заблокирован». В противном случае, при истечении периода, установленного таймером задержки смены состояний, порт перейдет в следующее состояние «Продвижение»;
- **Forwarding** («Продвижение») – в этом состоянии порт может обрабатывать кадры данных в соответствии с построенной таблицей коммутации. Также продолжают приниматься, передаваться и обрабатываться кадры BPDU;
- **Disable** («Отключен») – в это состояние порт переводит администратор. Отключенный порт не участвует ни в работе протокола STP, ни в продвижении кадров данных. Порт можно также вручную включить, и первоначально он перейдет в состояние «Заблокирован».

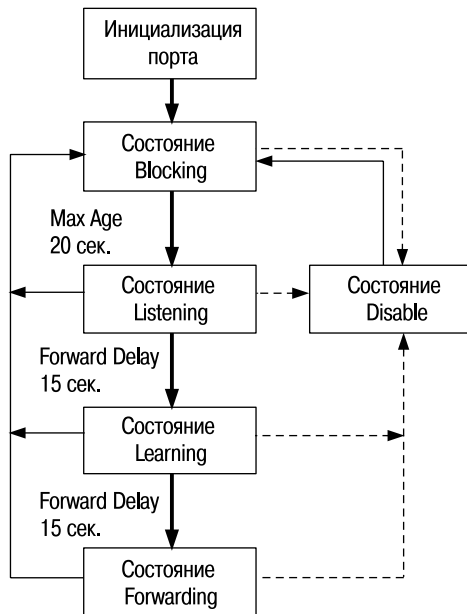


Рис. 5.4. Состояния портов

В процессе нормальной работы корневой мост продолжает генерировать служебные кадры BPDU, а остальные коммутаторы продолжают их принимать своими корневыми портами и ретранслировать назначенными. Если по истечении максимального времени жизни сообщения (по умолчанию – 20 секунд) корневой порт любого коммутатора сети не получит служебный кадр BPDU, то он инициализирует новую процедуру построения связующего дерева.

5.2.5. Таймеры STP

Для того чтобы все коммутаторы сети имели возможность получить точную информацию о конфигурации связующего дерева, в протоколе STP используются следующие таймеры.

- **Hello Time** – это интервал времени, через который корневой мост отправляет конфигурационные BPDU. Значение таймера Hello Time, настроенное на корневом мосте, будет определять значения таймеров Hello Time на всех некорневых коммутаторах, т.к. они просто пересылают конфигурационные BPDU, когда получают их от корня. Значение таймера Hello Time по умолчанию 2 секунды: диапазон возможных значений от 1 до 10 секунд.
- **Forward Delay** – это интервал времени, в течение которого порт коммутатора находится в состояниях «Прослушивание» и «Обучение». Такая задержка смены состояний необходима, чтобы исключить возможность временного возникновения альтернативных маршрутов при одновременной смене состояний портов во время реконфигурации. Значение таймера Forward Delay по умолчанию 15 секунд. диапазон возможных значений от 4 до 30 секунд.
- **Max Age** – это интервал времени, в течение которого коммутатор хранит параметры текущей конфигурации связующего дерева. Значение таймера Max Age устанавливается корневым мостом и позволяет гарантировать, что все коммутаторы сети обладают одинаковой информацией о времени хранения конфигурации STP. Если период времени, определенный таймером, истек, а коммутатор за это время не получил кадр BPDU от корневого моста, то он начинает считать себя корневым мостом и рассылает свои собственные BPDU всем коммутаторам сети, иницируя новую процедуру построения связующего дерева. Значение таймера Max Age по умолчанию 20 секунд, диапазон возможных значений от 6 до 40 секунд.

Значения таймеров Hello Time, Forward Delay и Max Age могут быть вручную настроены администратором сети на коммутаторе. Обычно эти настройки выполняются только на коммутаторе, являющемся корневым

для данной топологии связующего дерева. При настройке важно помнить, что неправильно подобранные значения таймеров могут значительно увеличить время сходимости топологии STP и снизить производительность сети, поэтому рекомендуется использовать значения таймеров по умолчанию.

5.2.6. Изменение топологии

Коммутатор отправляет BPDU с уведомлением об изменении топологии (Topology Change Notification BPDU, TCN BPDU) в случае возникновения одного из следующих событий:

- некорневой мост получает сообщение TCN BPDU на свой назначенный порт;
- после истечения времени, определенного таймером Forward Delay, порт переходит в состояние Forwarding, но коммутатор уже имеет назначенный порт для данного сегмента;
- порт, находившийся в состоянии Forwarding или Listening, переходит в состояние Blocking (в случае проблем с каналом связи);
- когда коммутатор становится корневым мостом.

TCN BPDU отправляется коммутатором в тот сегмент сети, к которому подключен его корневой порт. Эти BPDU будут передаваться через интервал Hello до тех пор, пока коммутатор не получит подтверждение Topology Change Notification Acknowledgement (TCN-ACK) от вышестоящего коммутатора. Соседний коммутатор продолжит трансляцию TCN BPDU через свой корневой порт в направлении корневого моста сети, используя такую же процедуру. Этот процесс будет продолжаться до тех пор, пока TCN BPDU не достигнет корневого моста.

Когда корневой мост получает TCN BPDU или сам изменяет топологию, он устанавливает во всех передаваемых конфигурационных BPDU

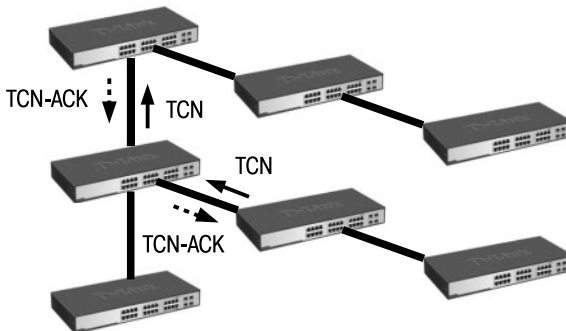


Рис. 5.5. Процесс уведомления об изменении топологии

флаг изменения топологии (Topology Change, TC) на период времени, равный сумме значений таймеров Forward Delay и Max Age. Когда нижележащие коммутаторы получают конфигурационные BPDU с флагом Topology Change, они установят значения таймеров старения записей адресных таблиц (Aging Timer) равными длительности таймера задержки передачи Forward Delay.

Управляемые коммутаторы D-Link при настройке функции STP позволяют включать и отключать на каждом порте возможность приема TCN BPDU с помощью параметра *restricted_tcn*. По умолчанию параметр *restricted_tcn* отключен. Использование данного параметра позволяет избежать сетевых атак, связанных с отправкой ложных кадров TCN BPDU.

5.2.7. Настройка STP

Рассмотрим пример настройки STP на коммутаторах D-Link в сети, показанной на рис. 5.6.

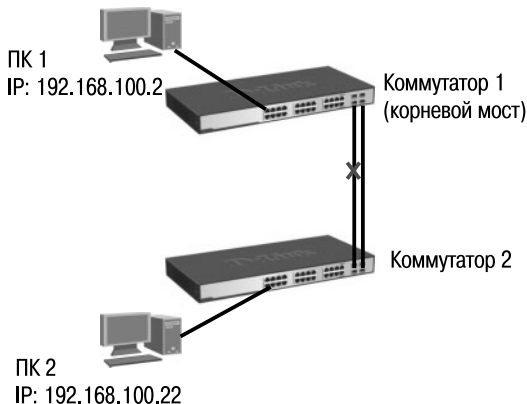


Рис. 5.6. Схема сети

Внимание: по умолчанию протокол STP на коммутаторах D-Link отключен.

Настройка коммутатора 1

- Активизировать STP

```
enable stp
config stp version stp
```

- Установить коммутатору 1 наименьшее значение приоритета, чтобы он был выбран корневым мостом (приоритет по умолчанию равен 32768)

```
config stp priority 4096 instance_id 0
```

- Настроить порты STP

```
config stp ports 1-24 edge true
```

Настройка коммутатора 2

```
enable stp  
config stp version stp  
config stp ports 1-24 edge true
```

5.3. Rapid Spanning Tree Protocol

Протокол Rapid Spanning Tree Protocol (RSTP) является развитием протокола STP и в настоящее время определен в стандарте IEEE 802.1D-2004 (ранее был определен в стандарте IEEE 802.1w-2001). Он был разработан для преодоления отдельных ограничений протокола STP, связанных с его производительностью. Протокол RSTP значительно ускоряет время сходимости коммутируемой сети за счет мгновенного перехода корневых и назначенных портов в состояние продвижения.

RSTP может работать с оборудованием, поддерживающим STP, однако все преимущества от его использования будут потеряны.

Основные понятия и терминология протоколов STP и RSTP одинаковы. Существенным их отличием является способ перехода портов в состояние продвижения и то, каким образом этот переход влияет на роль порта в топологии. RSTP объединяет состояния Disabled, Blocking и Listening, используемые в STP, и создает единственное состояние *Discarding* («Отбрасывание»), при котором порт не активен.

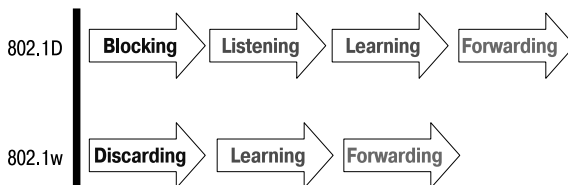


Рис. 5.7. Состояния портов протоколов STP и RSTP

Таблица 5.1. Различия между состояниями портов в STP и RSTP

Состояние порта STP	Административное состояние порта коммутатора	Порт изучает MAC-адреса?	Состояние порта RSTP	Роль порта в активной топологии
Disable	Disabled	Нет	Discarding	Исключен (Disabled)
Disable	Enabled	Нет	Discarding	Исключен (Disabled)
Blocking	Enabled	Да	Discarding	Исключен (Alternate, Backup)
Listening	Enabled	Да	Discarding	Включен (Root, Designated)
Learning	Enabled	Да	Learning	Включен (Root, Designated)
Forwarding	Enabled	Да	Forwarding	Включен (Root, Designated)

5.3.1. Роли портов

Выбор активной топологии завершается присвоением протоколом RSTP определенной роли каждому порту. Эти роли следующие:

- корневой порт (Root Port);
- назначенный порт (Designated Port);
- альтернативный порт (Alternate Port);
- резервный порт (Backup Port).

Корневой порт — это порт коммутатора, который имеет по сети кратчайшее расстояние (в терминах стоимости пути) до корневого коммутатора.

Порт является **назначенным**, если он посылает BPDU с наилучшими параметрами в тот сегмент, к которому подключен.

Роли «корневой порт» и «назначенный порт» включают порт в активную топологию.

В RSTP существуют две дополнительные роли — альтернативный порт (*Alternate*) и резервный порт (*Backup*), соответствующие состоянию «Заблокирован» в STP и исключающие порт из активной топологии.

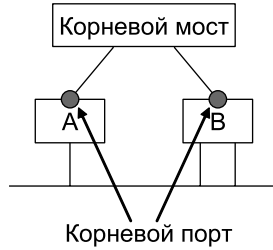


Рис. 5.8. Корневой порт

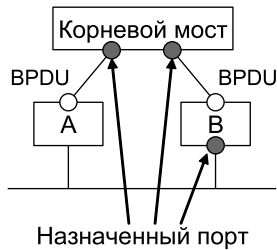


Рис. 5.9. Назначенный порт

Альтернативный порт предлагает альтернативный основному маршруту путь в направлении корневого моста и может заменить корневой порт в случае выхода его из строя.

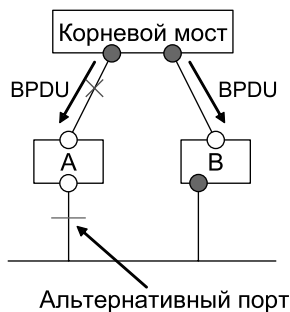


Рис. 5.10. Альтернативный порт

Резервный порт предназначен для резервирования пути, предоставляемого назначенным портом в направлении сегментов сети, и не может гарантировать альтернативное подключение к корневому мосту. Резерв-

ные порты существуют только в конфигурациях, где есть два или более соединения данного моста с данной сетью (сегментом сети).

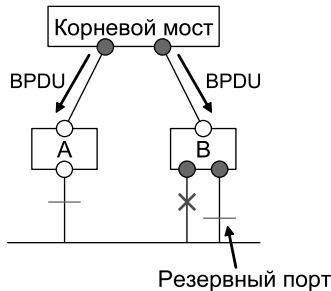


Рис. 5.11. Резервный порт

5.3.2. Формат BPDU

Формат кадра BPDU протокола RSTP аналогичен формату BPDU протокола STP за исключением следующего:

- поля версии протокола и типа BPDU RSTP содержат значение 2;
- в поле Flag BPDU протокола STP используются только два бита, которые определяют флаги изменения топологии TC и подтверждения TC (TCA). В поле Flag протокола RSTP используются все 8 бит. Бит 1 – флаг изменения топологии (*Topology Change*), бит 2 – флаг предложения (*Proposal*), биты 3 и 4 предназначены для кодирования роли порта (*Port Role*), бит 5 – флаг изучения (*Learning*), бит 6 – флаг продвижения (*Forwarding*), бит 7 – флаг соглашения (*Agreement*), бит 8 – флаг подтверждения TC (*Topology Change Acknowledgment*).
- кадр BPDU протокола RSTP имеет дополнительное поле *Version 1 Length* длиной 1 байт. Это поле содержит значение 0000 0000 и показывает, что BPDU не содержит никакой информации протокола STP версии 1.

5.3.3. Быстрый переход в состояние продвижения

Процесс построения связующего дерева у протоколов STP и RSTP одинаков. Однако при работе RSTP порт может перейти в состояние продвижения значительно быстрее, т.к. он больше не зависит от настроек таймеров. Протокол RSTP предоставляет механизм предложений и соглашений, который обеспечивает быстрый переход корневых и назначенных портов в состояние Forwarding, а альтернативных и резервных портов –

	Байты
Идентификатор протокола (Protocol Identifier)	2
Версия протокола (Protocol Version Identifier)	1
Тип BPDU (BPDU Type)	1
Флаги (Flags)	1
Идентификатор корневого моста (Root Identifier)	8
Расстояние до корневого моста (Root Path Cost)	2
Идентификатор моста (Bridge Identifier)	8
Идентификатор порта (Port Identifier)	2
Время жизни сообщения (Message Age)	2
Максимальное время жизни сообщения (Max Age)	2
Время приветствия (Hello Time)	2
Задержка смены состояний (Forward Delay)	2
Длина версии 1 (Version 1 Length)	1

Рис. 5.12. Формат кадра BPDU протокола RSTP

в состояние Discarding. Для этого протокол RSTP вводит два новых понятия: **граничный порт** и **тип соединения**.

Граничным портом (*Edge Port*) объявляется порт, непосредственно подключенный к сегменту сети, в котором не могут быть созданы петли. Например, порт подключен к рабочей станции, которая может периодически включаться или выключаться и активизировать механизм уведомления об изменении топологии или чтобы избежать распространения вычислений STP по клиентским сетям, с целью повышения безопасности. Граничный порт мгновенно переходит в состояние продвижения, минуя состояния прослушивания и обучения. Граничный порт теряет свой статус и становится обычным портом связующего дерева в том случае, если получит кадр BPDU.

При работе протокола RSTP назначенный порт может выполнять быстрый переход в состояние продвижения в соединениях типа «точка – точка» (*Point-to-Point, P2P*), т.е. если он подключен только к одному коммутатору.

Порты, удовлетворяющие, по крайней мере, одному из следующих условий, автоматически рассматриваются протоколом RSTP как порты P2P:

- порт принадлежит агрегированному каналу связи;
- на порте включена функция автосогласования и она определила работу в полнодуплексном режиме;
- работа в полнодуплексном режиме на порте была настроена вручную администратором сети.

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

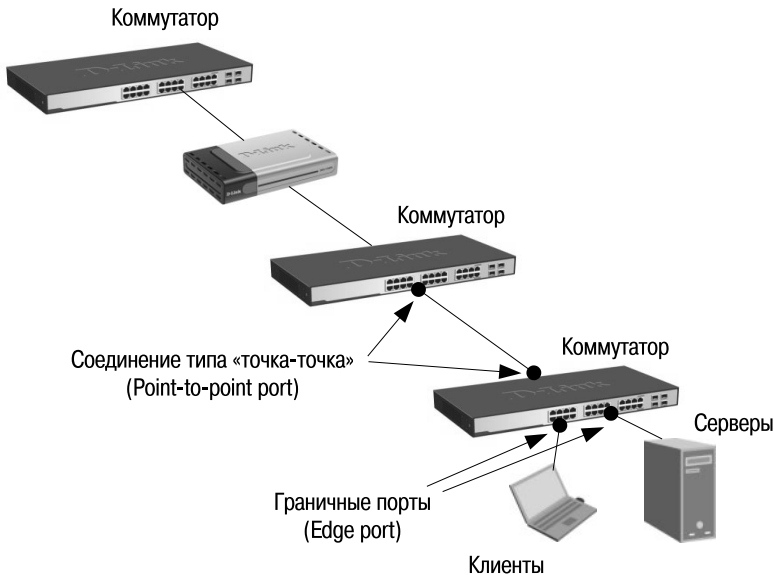


Рис. 5.13. Граничные порты и порты «точка – точка»

5.3.4. Механизм предложений и соглашений

На рис. 5.14 показан процесс работы механизма предложений и соглашений. Коммутаторы А и В соединены между собой каналом типа «точка – точка». Предположим, что коммутатор А является корневым мостом сети. Коммутатор А посылает коммутатору В кадр BPDU с установленным флагом Proposal (шаг 1 на рис. 5.14), предлагая себя в качестве назначенного моста этого сегмента (BPDU-предложение будет передаваться только в том случае, если порт находится в состоянии Discarding или Learning). После получения предложения коммутатор В выберет в качестве нового корневого порта тот порт, через который этот BPDU был получен (порт p2), и переведет все неграничные порты в заблокированное со-

стояние. Все остальные порты будут синхронизированы с новой информацией, чтобы иметь непротиворечивую информацию о топологии сети.

Порт является синхронизированным *«in-sync»*, если он удовлетворяет следующим критериям:

- он находится в заблокированном состоянии (это состояние Discarding в стабильной топологии);
- он является граничным портом.

Чтобы продемонстрировать действие метода синхронизации на различные типы портов, предположим, что в коммутаторе В имеются граничные порты р3 и р5 и назначенный порт р4. Порты р3 и р5 уже удовлетворяют одному из условий синхронизации. Чтобы находиться в режиме синхронизации (шаг 2 на рис. 5.14), коммутатору В необходимо заблокировать порт р4, переведя его в состояние Discarding.

После того, как коммутатор В убедится, что все порты синхронизированы, он разблокирует свой новый корневой порт (шаг 3 на рис. 5.14) и отправит через него коммутатору А согласие на предложение. Это сообщение является копией BPDU-предложения, в котором вместо бита Proposal установлен бит Agreement. Благодаря этому порт р1 коммутатора А точно знает, какому предложению соответствует полученное согласие.

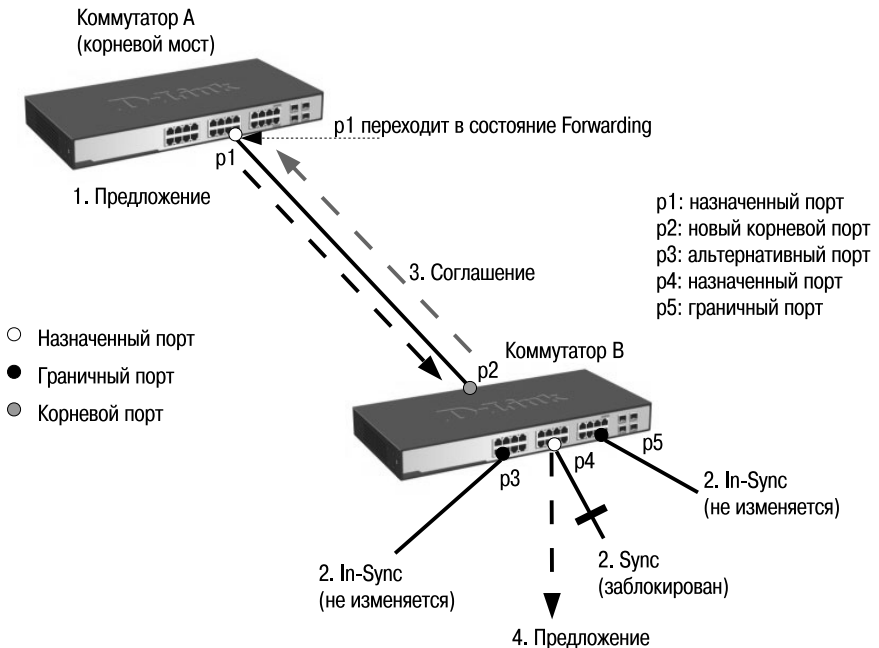


Рис. 5.14. Механизм предложений и соглашений

После этого коммутатор А мгновенно переведет свой назначенный порт р1 в состояние продвижения.

Находясь в заблокированном состоянии порт р4 коммутатора В начнет отсылать предложения нижележащему коммутатору и попытается быстро перейти в состояние продвижения (шаг 4 на рис. 5.14).

5.3.5. Новый механизм изменения топологии

1. Определение изменений топологии.

В протоколе RSTP только неграничные порты, переходя в состояние продвижения, могут вызвать процесс изменения топологии. Это означает, что разрыв соединения больше не рассматривается как изменение в топологии, в отличие от протокола STP, т.е. при переходе порта в заблокированное состояние соответствующий коммутатор не генерирует TCN BPDU. Когда мост RSTP обнаруживает изменение топологии, происходит следующее:

- коммутатор устанавливает начальное значение таймера TC While равным удвоенному интервалу Hello для всех неграничных назначенных портов и корневого порта. While Timer – это интервал времени, в течение которого мост RSTP активно информирует остальные мосты в сети об изменении топологии;
- удаляет MAC-адреса, ассоциированные со всеми неграничными назначенными портами и корневым портом;
- до тех пор, пока не истечет время, установленное таймером TC While, запущенным на порте, в BPDU, отправляемых через него, будет установлен бит TC.

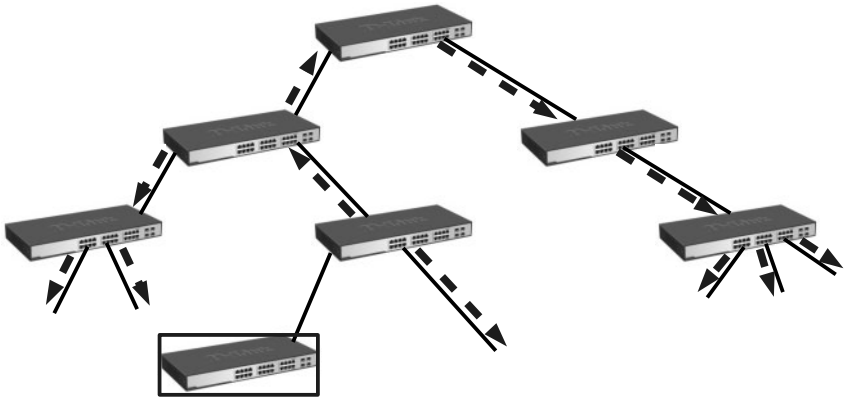
2. Распространение информации об изменении топологии.

Когда коммутатор получает от соседа BPDU с установленным битом TC, происходит следующее:

- коммутатор удаляет все MAC-адреса, изученные его неграничными назначенными портами и корневым портом, за исключением того порта, который получил информацию об изменении топологии;
- коммутатор запускает таймер TC While и отправляет BPDU с установленным битом TC через все неграничные порты (RSTP не использует специальные TCN BPDU, за исключением случаев, когда требуется уведомить коммутатор, поддерживающий только протокол STP).

Коммутатор-отправитель BPDU с битом TC непосредственно распространяет информацию об изменении топологии через всю сеть (в отличие от STP, где это может выполнить только корневой мост). Этот механизм распространения информации об изменении топологии быстрее, чем его аналог в протоколе STP, т.к. нет необходимости ждать, когда будет уведомлен корневой мост, и потом поддерживать состояние

изменения топологии для всей сети в течение периода времени, равного сумме значений таймеров Forward Delay и Max Age.



Коммутатор определил изменение топологии

1. Запускается таймер TC While и удаляются MAC-адреса, ассоциированные со всеми неграничными портами.
2. Коммутатор отправляет BPDU с установленным битом TC через все свои неграничные порты.

Рис. 5.15. Новый механизм изменения топологии

5.3.6. Стоимость пути RSTP

Протокол RSTP определяет следующие рекомендованные значения стоимости пути по умолчанию для портов коммутаторов. Эти значения вычисляются в соответствии со скоростью канала связи, к которому подключен порт.

Таблица 5.2. Стоимость пути RSTP

Параметр	Скорость канала	Рекомендованное значение	Рекомендованный диапазон	Диапазон значений
Стоимость пути	10 Мбит/с	2 000 000	200 000– 20 000 000	1– 200 000 000
Стоимость пути	100 Мбит/с	200 000	20 000– 2 000 000	1– 200 000 000
Стоимость пути	1 Гбит/с	20 000	2 000–200 000	1– 200 000 000
Стоимость пути	10 Гбит/с	2 000	200–20 000	1– 200 000 000

5.3.7. Совместимость с STP

Протокол RSTP может взаимодействовать с оборудованием, поддерживающим STP, и, если необходимо, автоматически преобразовывать кадры BPDU в формат 802.1D. Однако преимущество быстрой сходимости RSTP (когда все коммутаторы быстро переходят в состояние пересылки или блокировки и обладают тождественной информацией) теряется.

Каждый порт хранит переменную, определяющую тип протокола, используемого в соответствующем сегменте. При включении порта активируется таймер задержки миграции (*Migration delay timer*) длительностью 3 секунды. При запуске этого таймера текущий режим (STP или RSTP) ассоциированный с портом, блокируется. Как только истечет время задержки миграции, порт начнет работать в режиме, соответствующем типу следующего полученного им BPDU. Если в результате получения BPDU порт изменил свой режим работы, таймер задержки миграции запускается вновь, что позволяет ограничить частоту возможной смены режимов.

Предположим, что коммутаторы А и В (рис. 5.16) работают в режиме RSTP. Коммутатор А является выделенным мостом этого сегмента. К существующему каналу связи подключается коммутатор С, который является коммутатором с поддержкой протокола STP. Так как коммутаторы STP игнорируют BPDU протокола RSTP и отбрасывают их, то коммутатор С считает, что в этом сегменте сети больше коммутаторов нет и начинает отправлять BPDU формата 802.1D.

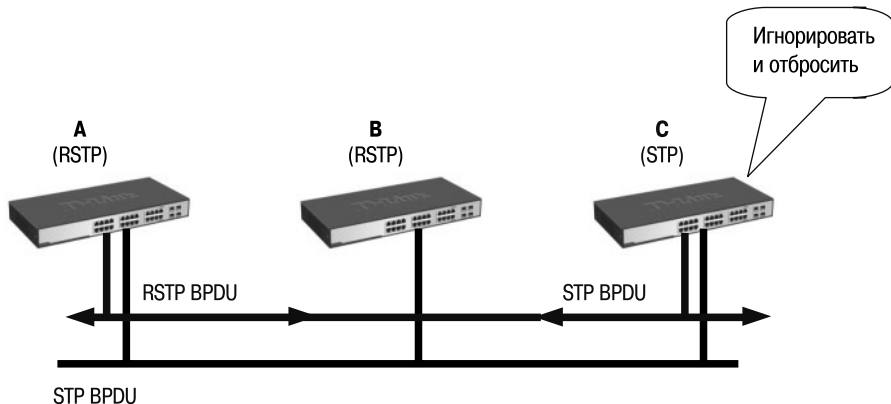


Рис. 5.16. Пример совместной работы коммутаторов STP и RSTP

Коммутатор А получает эти BPDU и после истечения периода времени, установленного таймером задержки миграции, переходит на этом порте

в режим работы STP. В результате коммутатор С начинает понимать BPDU коммутатора А и признает его назначенным коммутатором этого сегмента.

Следует отметить, что если бы в этом частном случае коммутатор С был удален из сегмента, то коммутатор А остался бы работать в режиме STP на этом порте, хотя он мог бы эффективно работать в режиме RSTP со своим единственным соседом коммутатором В. Т.е. у коммутатора А нет возможности узнать, что коммутатор С удален из этого сегмента. В этом частном случае для перезагрузки протокола, используемого на порте коммутатора, требуется вмешательство администратора сети. Когда порт находится в режиме, совместимом с 802.1D, он также может обрабатывать уведомления об изменении топологии TCN BPDU с установленными битами TC и TCA.

5.3.8. Настройка RSTP

Настройка протокола RSTP на коммутаторах D-Link аналогична настройке протокола STP. Рассмотрим пример настройки RSTP в сети, показанной на рис. 5.17.

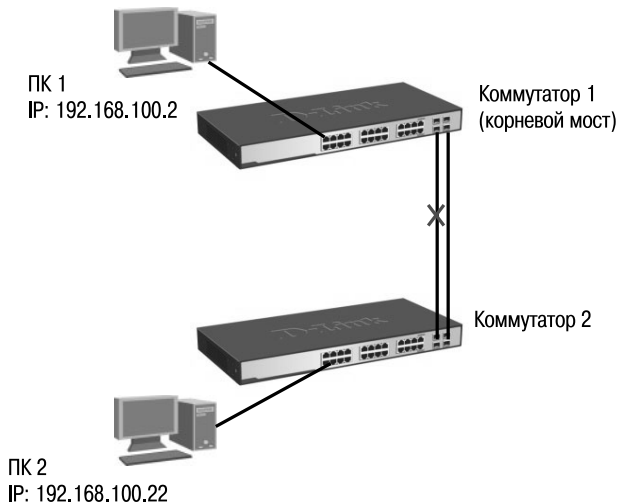


Рис. 5.17. Схема сети

Настройка коммутатора 1

- Активизировать RSTP

```
enable stp
config stp version rstp
```

- Установить коммутатору 1 наименьшее значение приоритета, чтобы он был выбран корневым мостом (приоритет по умолчанию равен 32768)

```
config stp priority 4096 instance_id 0
```

- Настроить граничные порты RSTP

```
config stp ports 1-24 edge true
```

Настройка коммутатора 2

```
enable stp  
config stp version rstp  
config stp ports 1-24 edge true
```

5.4. Multiple Spanning Tree Protocol

Несмотря на то, что протокол RSTP обеспечивает быструю сходимость сети, он так же, как и протокол STP, обладает следующим недостатком – не поддерживает возможность создания отдельного связующего дерева для каждой VLAN, настроенной в сети. Это означает, что резервные каналы связи не могут блокироваться на основе VLAN и все VLAN образуют одну логическую топологию, не обладающую достаточной гибкостью.

Протокол Multiple Spanning Tree Protocol (MSTP), являющийся расширением протокола RSTP, преодолевает это ограничение. В дополнение к обеспечению быстрой сходимости сети он 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.

5.4.1. Логическая структура MSTP

Протокол MSTP делит коммутируемую сеть на **регионы MST** (*Multiple Spanning Tree (MST) Region*), каждый из которых может содержать множество **копий связующих деревьев** (*Multiple Spanning Tree Instance, MSTI*) с независимой друг от друга топологией. Другими словами, регион MST, представляющий собой набор физически подключенных друг к другу коммутаторов, делит данную физическую топологию на множество логических.

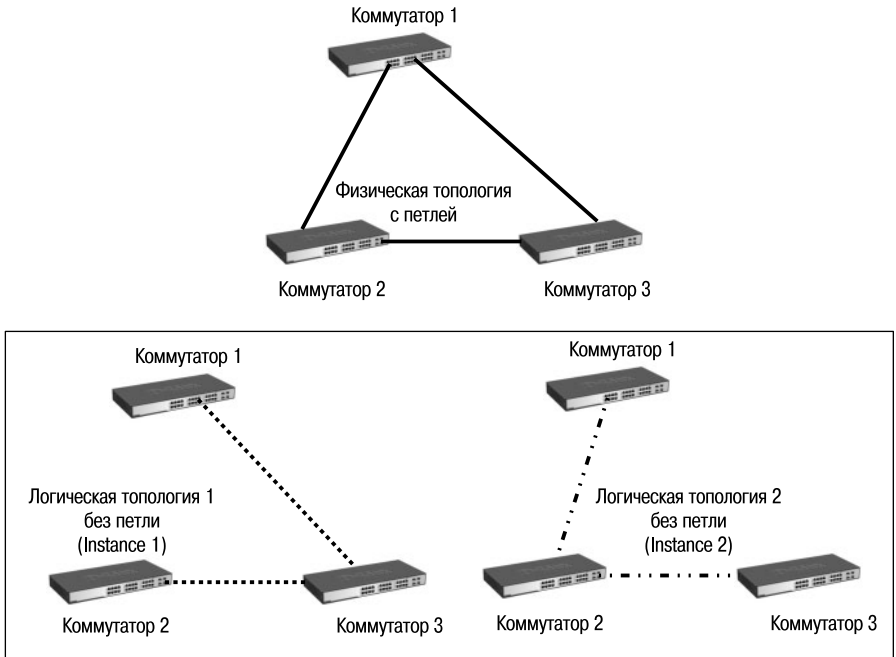


Рис. 5.18. Физическая и логическая топология региона MST

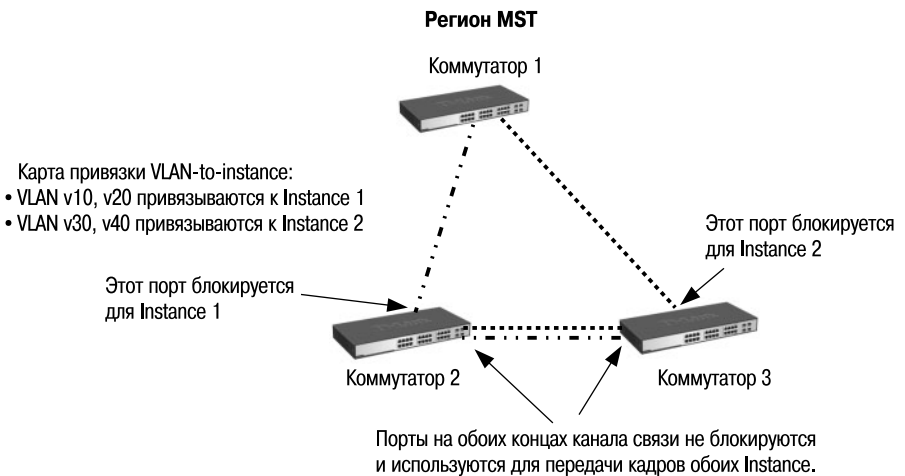


Рис. 5.19. Регион MST

Для того чтобы два и более коммутатора принадлежали одному региону MST, они должны обладать одинаковой конфигурацией MST.

Конфигурация MST включает такие параметры, как номер ревизии MSTP (*MSTP revision level number*), имя региона (*Region name*), карту привязки VLAN к копии связующего дерева (*VLAN-to-instance mapping*).

Внутри коммутируемой сети может быть создано множество MST-регионов.

Протокол MSTP определяет следующие типы связующих деревьев:

- **Internal Spanning Tree (IST)** – специальная копия связующего дерева, которая по умолчанию существует в каждом MST-регионе. IST присвоен номер 0 (Instance 0). Она может отправлять и получать кадры BPDU и служит для управления топологией внутри региона. По умолчанию все VLAN одного региона привязаны к IST. Если в регионе создано несколько MSTI, то VLAN, не ассоциированные с ними, остаются привязанными к IST. Динамические VLAN, созданные с помощью протокола GVRP, также ассоциируются с IST;
- **Common Spanning Tree (CST)** – единое связующее дерево, вычисленное с использованием протоколов STP, RSTP, MSTP и объединяющее все регионы MST и мосты SST (Single Spanning Tree (SST) Bridge);
- **Common and Internal Spanning Tree (CIST)** – единое связующее дерево, объединяющее CST и IST каждого MST-региона;

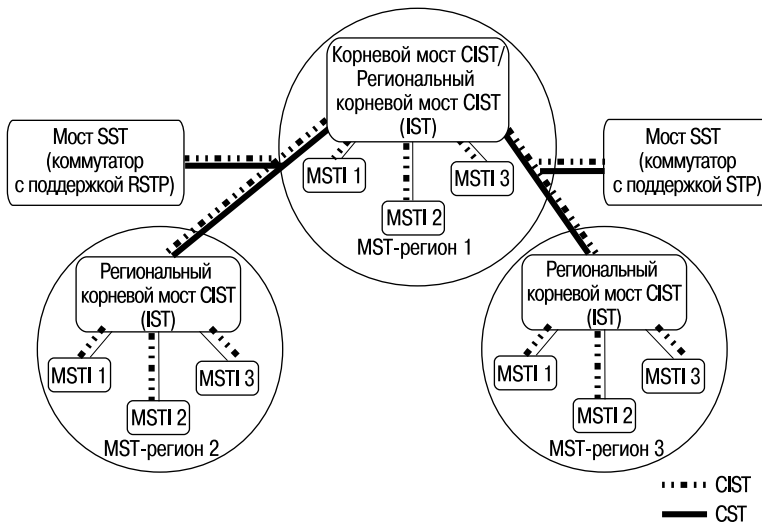


Рис. 5.20. Логическая структура MSTP

- **Single Spanning Tree (SST) Bridge** – мост, поддерживающий только единственное связующее дерево, CST. Это единственное связующее дерево может поддерживать протокол STP или протокол RSTP.

5.4.2. Multiple Spanning Tree Instance (MSTI)

По умолчанию все VLAN данного MST-региона назначены в IST. Помимо IST, в каждом MST-регионе может быть дополнительно создано множество связующих деревьев с независимой друг от друга архитектурой – MSTI. К каждой MSTI администратор сети может вручную привязать соответствующие сети VLAN.

MSTI обладают следующими характеристиками:

- MSTI является копией связующего дерева, существующей только внутри региона;
- MSTI не может отправлять BPDU за пределы своего региона (отправлять и получать BPDU может только IST);
- все MSTI внутри региона могут нумероваться 1, 2, 3, 4 и т.д. (максимальное количество MSTI зависит от модели коммутатора и версии программного обеспечения);
- MSTI не отправляет индивидуальные BPDU. Вся информация о данной MSTI помещается в конфигурационное сообщение MSTI (MSTI Configuration Message, M-record), которое инкапсулируется в кадры MSTP BPDU, рассылаемые IST.

Для того чтобы каждая MSTI представляла собой отдельную от IST логическую топологию, администратор сети может присвоить коммутаторам и портам внутри MSTI собственные значения приоритетов и стоимости пути.

5.4.3. Формат MSTP BPDU

Формат MSTP BPDU аналогичен формату RSTP BPDU, за исключением полей, предназначенных для передачи информации об IST, каждой MSTI (если они созданы в регионе) и конфигурации MST.

5.4.4. Вычисления в MSTP

Прежде чем начать рассматривать вопрос вычисления активной топологии MSTP, следует отметить, что спецификация MSTP рассматривает MST-регион как один виртуальный мост RSTP, и вычисление активной топологии внутри региона отделено от вычисления топологии всей коммутируемой сети. Другими словами, соединения между мостами внутри региона не зависят от внешних соединений между MST-регионами.

		Байты
Идентификатор протокола (Protocol ID)		2
Версия (Version)		1
Тип BPDU (BPDU Type)		1
Флаги CIST (CIST Flags)		1
Идентификатор корневого моста CIST (CIST Root Bridge ID)		8
Внешняя стоимость пути до корня CIST (CIST External Root Path Cost)		4
Идентификатор регионального моста CIST (CIST Regional Root ID)		8
Идентификатор порта CIST (CIST Port ID)		2
Время жизни сообщения (Message Age)		2
Максимальное время жизни сообщения (Maximum Age)		2
Время приветствия (Hello Time)		2
Задержка смены состояний (Forward Delay)		2
Длина версии 1 (Version 1 Length = 0)		1
Длина версии 3 (Version 3 Length)		2
Идентификатор конфигурации MST (MST Configuration ID)		51
Внутренняя стоимость пути до корня CIST (CIST Internal Root Path Cost)		4
Идентификатор моста CIST (CIST Bridge ID)		8
Оставшееся число переходов CIST (CIST Remaining Hops)		1
Конфигурационное сообщение MSTI (MSTI Configuration Messages)		2

Идентификатор конфигурации MST (MST Configuration ID)	Байты
Имя региона (Region Name)	32
Номер ревизии (Revision Number)	2
Карта привязки VLAN к копии связующего дерева (VLAN-to-instance assignment map)	17

Конфигурационное сообщение MSTI (MSTI Configuration Messages, M-record)	Биты
Флаги MSTI (MSTI Flags)	1
Идентификатор регионального корня MSTI (MSTI Regional Root ID)	8
Внутренняя стоимость пути до корня MSTI (MSTI Internal Root Path Cost)	4
Приоритет моста MSTI (MSTI Bridge Priority)	1
Приоритет порта MSTI (MSTI Port Priority)	1
Оставшееся число переходов MSTI (MSTI remaining Hops)	1

Рис. 5.21. Формат MSTP BPDU

Процесс вычисления в MSTP начинается с выбора **корневого моста CIST (CIST Root)** сети. При выборе CIST Root используется тот же фундаментальный алгоритм, который описан в стандарте IEEE 802.1D-2004.

Первоначально каждый коммутатор сети считает себя корневым мостом CIST и рассылает BPDU, в поле CIST Root Bridge ID которых указано значение его идентификатора, а **внешняя стоимость пути до корня (CIST External Root Path Cost)** равна нулю. Эти два параметра являются основными для определения активной топологии всей коммутируемой сети.

Коммутатор перестанет заявлять себя в качестве корневого моста CIST, как только получит BPDU с меньшим значением идентификатора моста. В качестве CIST Root будет выбран коммутатор, обладающий наименьшим значением идентификатора моста среди всех коммутаторов сети.

Одновременно с выбором корневого моста CIST в каждом регионе выбирается **региональный корневой мост CIST (CIST Regional Root)**.

Им становится коммутатор, обладающий наименьшей внешней стоимостью пути к корню CIST среди всех коммутаторов принадлежащих данному региону. Внешняя стоимость пути до корня CIST представляет собой суммарное условное время пути от граничного коммутатора MST-региона или моста SST до порта корневого моста CIST. Следует отметить, что значение CIST External Root Path Cost не изменяется при передаче конфигурационного BPDU между коммутаторами внутри региона. Это значение увеличивается на условное время передачи только портами граничных коммутаторов, подключающих данный регион к другим регионам. В протоколе MSTP рекомендованные значения стоимости пути аналогичны значениям, определенным в RSTP.

В случае наличия в регионе коммутаторов с одинаковой стоимостью пути в качестве CIST Regional Root будет выбран коммутатор с наименьшим значением идентификатора моста. При этом маршрут от этого коммутатора до CIST Root не должен проходить через другие коммутаторы этого региона. Т.е. в качестве CIST Regional Root выбирается коммутатор, находящийся на границе региона. Следует отметить, что регион, содержащий CIST Root, использует его также в качестве CIST Regional Root.

Протокол MSTP, используя механизм предложений и соглашений RSTP, блокирует все избыточные каналы связи от всех CIST Regional Root к CIST Root, делая их резервными или альтернативными.

При наличии в регионе отдельных связующих деревьев MSTI, для каждой MSTI, независимо от остальных, выбирается **региональный корневой мост MSTI** (*MSTI Regional Root*). Им становится коммутатор, обладающий наименьшим значением идентификатора моста среди всех коммутаторов данной MSTI этого MST-региона. Определение роли портов и блокирование избыточных связей происходит аналогично процедурам, описанным в RSTP.

5.4.5. Роли портов MSTP

Протокол MSTP определяет роли портов, которые участвуют в процессе вычисления активной топологии CIST и MSTI, аналогичные протоколам STP и RSTP:

- корневой порт (Root Port);
- назначенный порт (Designated Port);
- альтернативный/резервный порт (Alternate/Backup Port).

Дополнительно в MSTI используется еще одна роль, которая может быть присвоена порту, — **мастер-порт** (*Master Port*).

Роли портов CIST определяют роли каждого порта коммутатора, участвующего в построении активной топологии CIST.

Корневой порт (Root Port) (*Root Port*) – это порт, который обладает минимальной стоимостью пути от коммутатора до корневого моста CIST (в случае если мост не является CIST Root) через региональный мост (в том случае, если коммутатор не является региональным корнем CIST).

Назначенный порт (Designated Port) (*Designated Port*) – это порт, обладающий наименьшей стоимостью пути от подключенного сегмента сети до корневого моста CIST.

Альтернативный/резервный порт (Alternate/Backup Port) (*Alternate/Backup Port*) – это порт, который обеспечивает подключение, если происходит потеря соединения с какими-либо коммутаторами или сегментами сети.

Роли портов MSTI определяют роли каждого порта коммутатора, участвующего в построении активной топологии MSTI внутри границы региона.

Корневой порт (Root Port) – это порт, который обладает минимальной стоимостью пути от коммутатора до регионального корневого моста MSTI (в случае если мост не является региональным корнем для этой MSTI).

Назначенный порт (Designated Port) – это порт, обладающий наименьшей стоимостью пути от подключенного сегмента сети до регионального корневого моста MSTI.

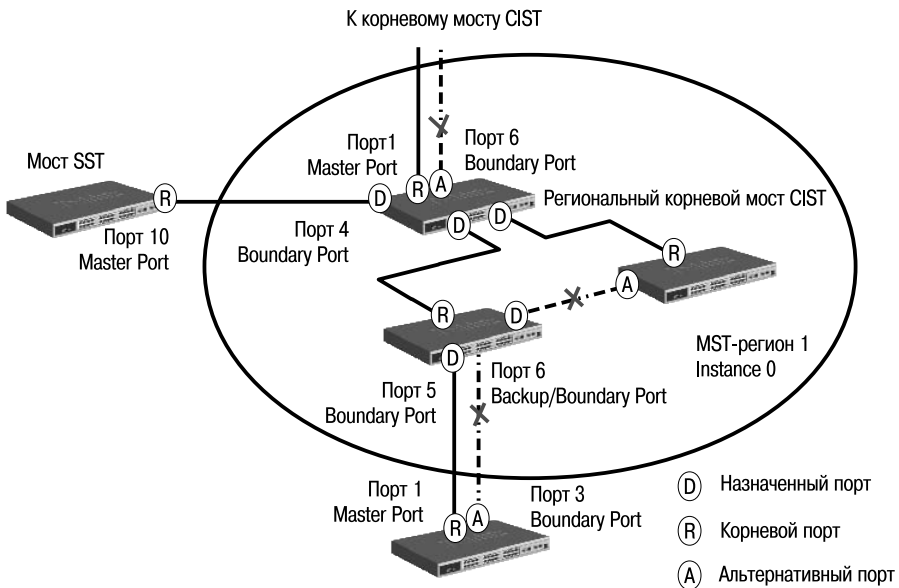
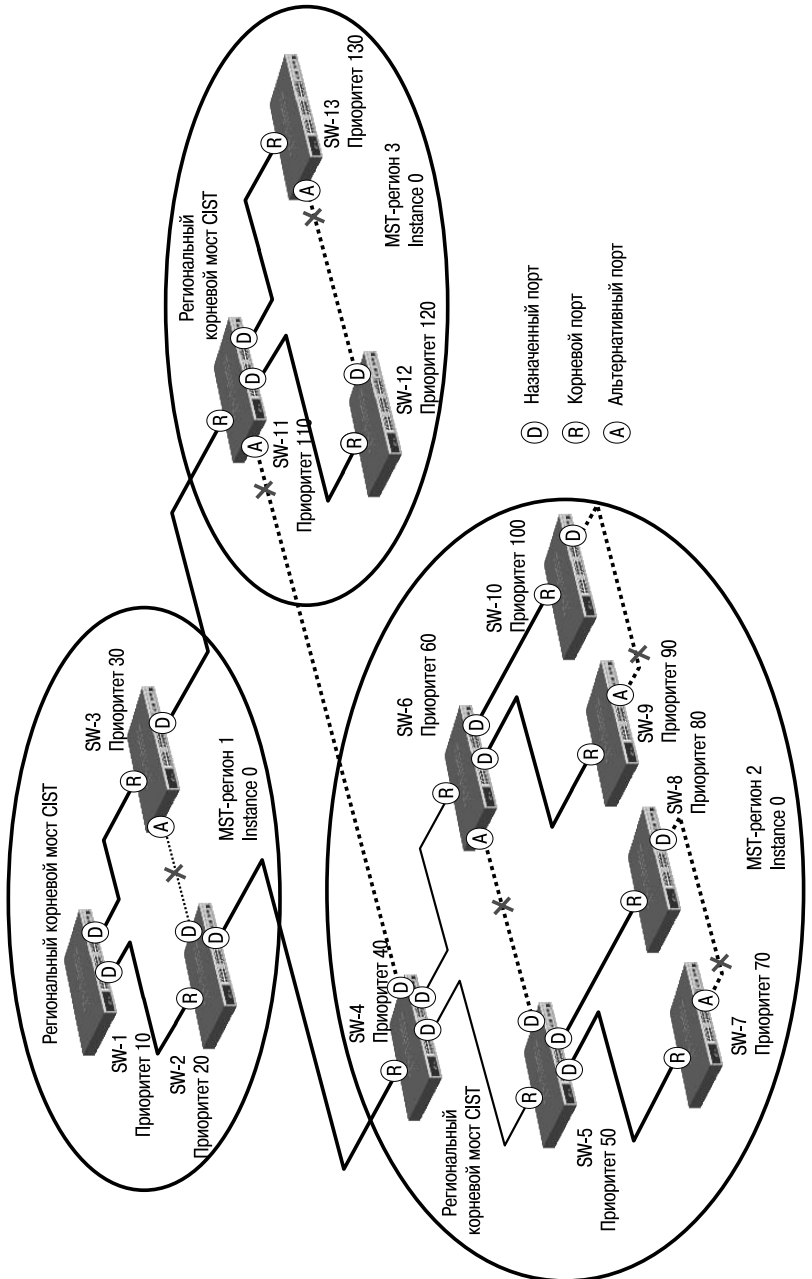


Рис. 5.22. Роли портов

Рис. 5.23. Пример топологии MSTP



Альтернативный/резервный порт (*Alternate/Backup Port*) – это порт, который обеспечивает подключение, если происходит потеря соединения с какими-либо коммутаторами или сегментами сети.

Мастер-порт (*Master Port*) – это порт, который обеспечивает подключение региона к корневому мосту CIST, находящемуся за пределами данного региона. Корневой порт CIST регионального корневого моста CIST является мастером-портом для всех MSTI.

Протокол MSTP вводит еще одну роль, которая может быть присвоена порту, – **пограничный порт** (*Boundary Port*). Пограничным портом является порт, который подключает MST-регион к другому региону или SST-мосту.

5.4.6. Пример топологии MSTP

Рассмотрим пример топологии MSTP, приведенный на рис. 5.23. Сеть разбита на 3 MST-региона, в каждом регионе все коммутаторы ассоциированы с Instance 0.

1. Коммутатор 1 (SW-1) выбран в качестве корневого моста CIST, т.к. он обладает наименьшим среди всех коммутаторов сети значением идентификатора моста.
2. Коммутаторы 1, 2 и 3 (SW-1, SW-2, SW-3) находятся в одном MST-регионе с номером 1, т.к. обладают одинаковым идентификатором MST-конфигурации. Коммутаторы 2 и 3 находятся в одном регионе с корневым мостом CIST (коммутатор 1), поэтому их внешняя стоимость пути равна 0 и их региональный мост CIST совпадает с корневым мостом CIST.
3. Коммутаторы 4-10 (SW-4-SW-10) принадлежат одному региону, т.к. имеют одинаковые идентификаторы MST-конфигурации. Коммутатор 4 (SW-4) является региональным корневым мостом CIST для MST-региона 2, т.к. обладает наименьшей внешней стоимостью пути к CIST Root.
4. Коммутаторы 11, 12 и 13 (SW-11-SW-13) принадлежат к MST-региону 3, т.к. обладают одинаковыми идентификаторами MST-конфигурации. Коммутатор 11 (SW-11) выбран в качестве регионального корневого моста CIST для MST-региона 3, т.к. обладает наименьшей внешней стоимостью пути к CIST Root.

5.4.7. Состояние портов MSTP

В протоколе MSTP определены состояния, в которых могут находиться порты, аналогичные протоколу RSTP:

- **Learning** («Обучение») – порт может принимать/отправлять кадры BPDU, изучать MAC-адреса и строить таблицу коммутации. Порт в этом состоянии не передает пользовательские кадры;
- **Forwarding** («Продвижение») – в этом состоянии порт может передавать пользовательские кадры, изучать новые MAC-адреса и принимать/отправлять кадры BPDU;
- **Discarding** («Отбрасывание») – в этом состоянии порт может только принимать кадры BPDU, передача пользовательского трафика и изучение MAC-адресов не выполняется.

5.4.8. Счетчик переходов MSTP

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

С помощью команды **config stp maxhops** на коммутаторах D-Link можно настроить максимальное число переходов между устройствами внутри региона, прежде чем кадр BPDU будет отброшен. Значение счетчика переходов устанавливается региональным корневым мостом MSTI или CIST и уменьшается на 1 каждым портом коммутатора, получившим кадр BPDU.

Внимание: значение счетчика переходов зависит от модели коммутатора. По умолчанию используется значение счетчика переходов, равное 20.

После того как значение счетчика станет равным 0, кадр BPDU будет отброшен и информация, хранимая портом, будет помечена как устаревшая.

Следует отметить, что коммутаторы не изменяют данные, хранимые в полях Max Age и Message Age конфигурационных BPDU, при их передаче через коммутаторы MST-региона. Значение Message Age изменяется только коммутаторами, расположенными на границе региона, чтобы обеспечить совместимость с мостами STP и RSTP, которые могут использоваться в сети.

5.4.9. Настройка протокола MSTP на коммутаторах

Ниже приведены основные шаги, которые позволяют настроить протокол MSTP на коммутаторах D-Link.

1. Активизировать STP на всех устройствах.
2. Изменить версию STP на MSTP (по умолчанию используется RSTP).
3. Настроить имя MST-региона и ревизию.
4. Создать MSTI и карту привязки VLAN к MSTI.
5. Задать приоритет STP для выбора корневого моста. По умолчанию используется приоритет 32768.
6. Настроить приоритеты портов.
7. Настроить граничные порты.

Рассмотрим пример, показанный на рис. 5.24. В сети созданы две виртуальные локальные сети – VLAN v2 и VLAN v3. Каждая VLAN привязывается к одной копии связующего дерева.

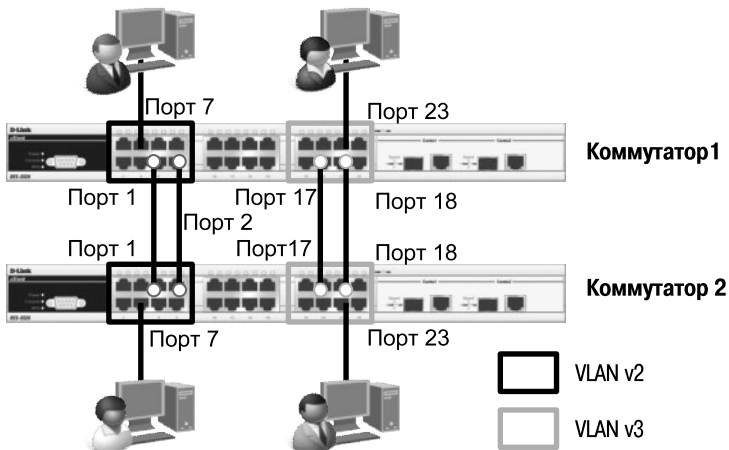


Рис. 5.24. Схема сети

Настройка коммутатора 1

- Создание VLAN

```
config vlan default delete 1-8,17-24
create vlan v2 tag 2
config vlan v2 add untagged 1-8
create vlan v3 tag 3
config vlan v3 add untagged 17-24
```

- Настройка MSTP

```
enable stp
config stp version mstp
```

```
config stp mst_config_id name dlink revision_level 1
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
config stp priority 4096 instance_id 0
config stp priority 4096 instance_id 2
config stp priority 4096 instance_id 3
config stp ports 7,23 edge true
```

Настройка коммутатора 2

- Создание VLAN

```
config vlan default delete 1-8,17-24
create vlan v2 tag 2
config vlan v2 add untagged 1-8
create vlan v3 tag 3
config vlan v3 add untagged 17-24
```

- Настройка MSTP

```
enable stp
config stp version mstp
config stp mst_config_id name dlink revision_level 1
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
config stp ports 7,23 edge true
```

Рассмотрим второй пример настройки протокола MSTP, позволяющий осуществлять балансировку нагрузки между каналами связи.

В примере, показанном на рис. 5.25, каждая VLAN привязывается к одной копии связующего дерева. Порты 25 и 26 являются маркированными портами обеих VLAN. Порт 25 используется в качестве активного канала связи для VLAN v2, порт 26 используется в качестве активного канала связи для VLAN v3. Т.к. для каждой VLAN будет построена своя собственная активная топология связующего дерева, то кадры VLAN v2 и VLAN v3 будут передаваться по разным маршрутам (через порты 25 и 26 соответственно), благодаря чему будет обеспечена балансировка нагрузки. В случае если один из каналов связи выйдет из строя, трафик VLAN v2 и VLAN v3 будет передаваться по одному оставшемуся каналу.

Настройка коммутатора 1

- Создание VLAN

```
config vlan default delete 1-8,17-24
create vlan v2 tag 2
config vlan v2 add tagged 25-26
config vlan v2 add untagged 1-8
create vlan v3 tag 3
config vlan v3 add tagged 25-26
config vlan v3 add untagged 17-24
```

- Настройка MSTP

```
enable stp
config stp version mstp
config stp mst_config_id name dlink revision_level 1
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
config stp ports 7,23 edge true
```

Настройка коммутатора 2

- Создание VLAN

```
config vlan default delete 1-8,17-24
create vlan v2 tag 2
config vlan v2 add tagged 25-26
config vlan v2 add untagged 1-8
create vlan v3 tag 3
config vlan v3 add tagged 25-26
config vlan v3 add untagged 17-24
```

- Настройка MSTP

```
enable stp
config stp version mstp
config stp mst_config_id name dlink revision_level 1
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
```

```

config stp mst_ports 25 instance_id 2 priority 96
config stp mst_ports 26 instance_id 2 priority 128
config stp mst_ports 25 instance_id 3 priority 128
config stp mst_ports 26 instance_id 3 priority 96
config stp ports 7,23 edge true

```

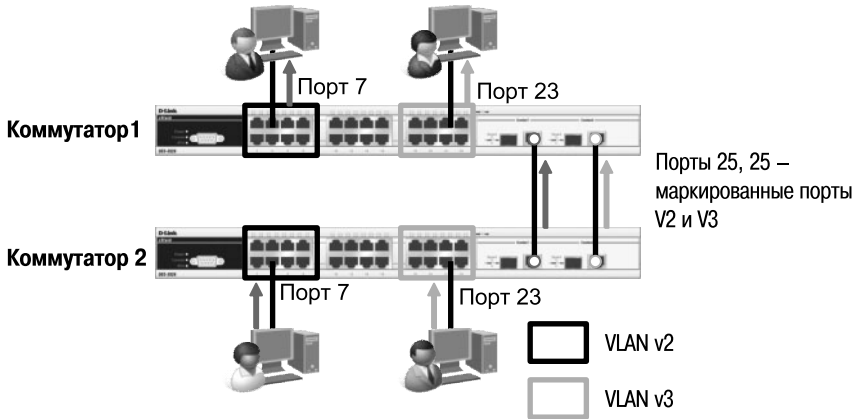


Рис. 5.25. Балансировка нагрузки с помощью MSTP

5.5. Дополнительные функции защиты от петель

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

- STP LoopBack Detection;
- LoopBack Detection Independent STP.

На рис. 5.26 показана ситуация, когда к порту управляемого коммутатора подключен неуправляемый коммутатор, порты которого соединены с образованием петли. В этом случае в сети может возникнуть широковещательный шторм и ее работоспособность будет нарушена.

Функция STP LoopBack Detection предназначена для отслеживания таких ситуаций и временного блокирования тех портов коммутатора, на которых обнаружены петли, тем самым предотвращая проблемы в сети. Коммутатор определяет наличие петли, когда отправленный им кадр BPDU вернулся назад на другой его порт. В этом случае порт-источник кадра BPDU и порт-приемник будут автоматически заблокированы и администратору сети будет отправлен служебный пакет-уведомление. Порты будут находиться в заблокированном состоянии до истечения периода

времени, установленного таймером LBD Recover Timer. По умолчанию на коммутаторах D-Link эта функция отключена. Следует отметить, что функция STP LoopBack Detection не определяет петлю, когда отправленный кадр BPDU вернулся назад на этот же порт.

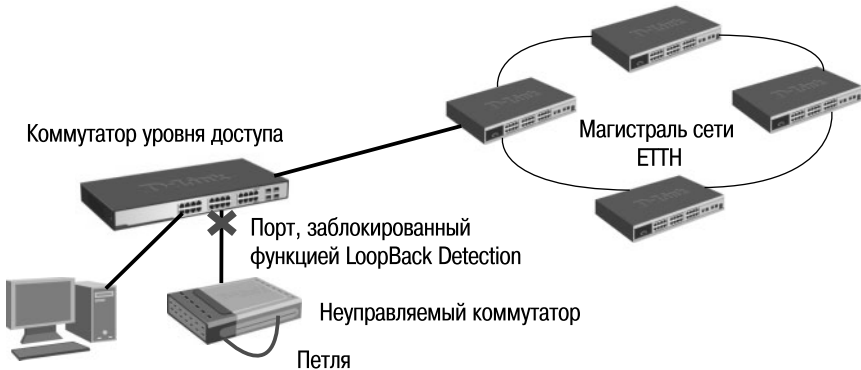


Рис. 5.26. Пример работы функции LoopBack Detection Independent STP

В отличие от STP LoopBack Detection функция LoopBack Detection Independent STP не требует настройки протокола STP на портах, на которых необходимо определять наличие петли. В этом случае наличие петли обнаруживается путем отправки портом специального служебного кадра ECTP (Ethernet Configuration Testing Protocol). При получении кадра ECTP этим же портом он блокируется на указанное в таймере время.

Следует отметить, что функция LoopBack Detection Independent STP версии 4.03 также может определять петли, возникающие между портами одного коммутатора.

Внимание: чтобы получить информацию о поддержке коммутатором функции LBD v.4.03, необходимо обратиться в службу технической поддержки D-Link.

Существуют два режима работы этой функции: Port-Based и VLAN-Based (начиная с LBD версии v.4.00).

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

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

5.5.1. Настройка функции LoopBack Detection

В качестве примера приведем настройку функций STP LoopBack Detection и LoopBack Detection Independent STP в режимах Port-Based и VLAN-Based для ситуации, показанной на рис. 5.26.

Настройка функции STP LoopBack Detection

```
enable stp
config stp ports 1-24 state enable edge true lbd enable
config stp lbd_recover_timer 60
```

Настройка функции LoopBack Detection Independent STP (Port-Based)

```
enable looopdetect
config looopdetect recover_timer 60
config looopdetect interval 10
config looopdetect mode port-based
config looopdetect ports 1-24 state enabled
```

Настройка функции LoopBack Detection Independent STP (VLAN-Based)

```
enable looopdetect
config looopdetect recover_timer 60
config looopdetect interval 10
config looopdetect mode vlan-based
config looopdetect ports 1-24 state enabled
```

Внимание: таймер `recover_timer` – интервал времени в секундах, через который будет проверяться статус заблокированного функцией LBD порта. Если установить значение таймера равным 0, заблокированный порт не сможет быть автоматически разблокирован и для его восстановления потребуется вмешательство администратора. Значение таймера задается глобально на коммутаторе.

`loopdetect interval` – временной интервал в секундах между отсылаемыми кадрами ECTP (Ethernet Configuration Testing Protocol).

5.6. Функции безопасности STP

Из-за ошибок в конфигурации или вредоносных атак в сети может возникнуть ситуация, когда корневой мост получит кадр BPDU, содержа-

щий лучший приоритет, и потеряет свою позицию. При настройке протоколов RSTP или MSTP на управляемых коммутаторах, расположенных на границе сети, с помощью параметра *restricted_role* можно ограничить роли выполняемые портом в активной топологии. При активизации этого параметра порт не будет выбран в качестве корневого порта даже в том случае, если получит BPDU с наилучшим приоритетом. После выбора корневого порта этот порт будет выбран в качестве альтернативного. По умолчанию функция *restricted_role* отключена.

Настройка коммутатора

```
enable stp
config stp version rstp
config stp priority 32768 instance_id 0
config stp ports 1-24 edge true restricted_role true
restricted_tcn true state enable
config stp ports 25-28 edge false state enable fbpdu enable
```

5.7. Агрегирование каналов связи

Агрегирование каналов связи (Link Aggregation) – это объединение нескольких физических портов в одну логическую магистраль на каналь-

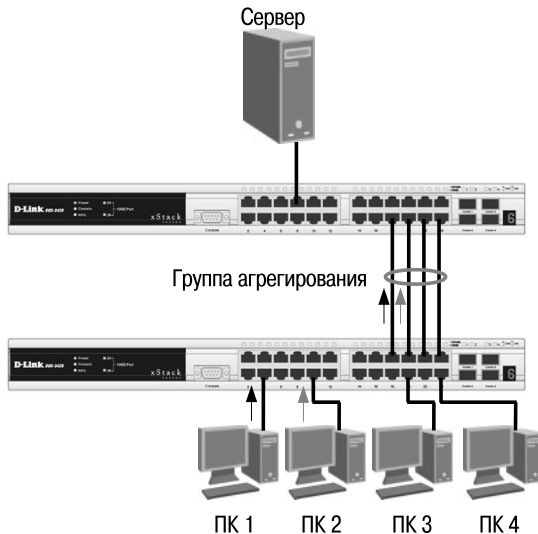


Рис. 5.27. Пример агрегированного канала связи между коммутаторами

ном уровне модели OSI с целью образования высокоскоростного канала передачи данных и повышения отказоустойчивости.

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

Включенные в агрегированный канал порты называются членами **группы агрегирования** (*Link Aggregation Group*).

Внимание: количество портов в группе зависит от модели коммутатора. В управляемых коммутаторах в группу можно объединить до 8 портов.

Один из портов в группе выступает в качестве **мастера-порта** (*master port*). Так как все порты агрегированной группы должны работать в одном режиме, конфигурация мастера-порта распространяется на все порты в группе. Таким образом, при конфигурировании портов в группе агрегирования достаточно настроить мастер-порт.

Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Если пакеты одного сеанса будут передаваться по разным портам агрегированного канала, то может возникнуть проблема на более высоком уровне модели OSI. Например, если два или более смежных кадров одного сеанса станут передаваться через разные порты агрегированного канала, то из-за неодинаковой длины очередей в их буферах может возникнуть ситуация, когда из-за неравномерной задержки передачи кадра более поздний кадр обгонит своего предшественника. Поэтому в большинстве реализаций механизмов агрегирования используются методы статического, а не динамического распределения кадров по портам, т.е. закрепление за определенным портом агрегированного канала потока кадров определенного сеанса между двумя узлами. В этом случае все кадры будут проходить через одну и ту же очередь и их последовательность не изменится. Обычно при статическом распределении выбор порта для конкретного сеанса выполняется на основе выбранного алгоритма агрегирования портов, т.е. на основании некоторых признаков поступающих пакетов. В коммутаторах D-Link поддерживается 9 алгоритмов агрегирования портов:

- 1) `mac_source` – MAC-адрес источника;
- 2) `mac_destination` – MAC-адрес назначения;
- 3) `mac_source_dest` – MAC-адрес источника и назначения;
- 4) `ip_source` – IP-адрес источника;
- 5) `ip_destination` – IP-адрес назначения;

- 6) ip_source_dest – IP-адрес источника и назначения;
- 7) l4_src_port – TCP/UDP-порт источника;
- 8) l4_dest_port – TCP/UDP-порт назначения;
- 9) l4_src_dest_port – TCP/UDP-порт источника и назначения.

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

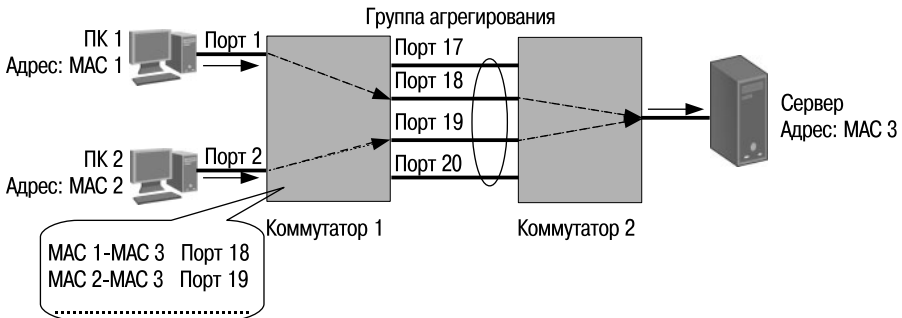


Рис. 5.28. Распределение потоков данных по каналам агрегированной линии связи для алгоритма **mac_source_dest**

Объединение каналов следует рассматривать как вариант настройки сети, используемый преимущественно для соединений «коммутатор – коммутатор» или «коммутатор – файл-сервер», требующих более высокой скорости передачи, чем может обеспечить одиночная линия связи. Также эту функцию можно применять для повышения надежности важных каналов связи. В случае повреждения линии связи объединенный канал быстро перенастраивается (не более чем за 1 сек.), а риск дублирования и изменения порядка кадров незначителен.

Программное обеспечение коммутаторов D-Link поддерживает два типа агрегирования каналов связи:

- статическое;
- динамическое, на основе стандарта IEEE 802.3ad (LACP).

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

Для организации динамического агрегирования каналов между коммутаторами и другими сетевыми устройствами используется протокол управления агрегированным каналом – Link Aggregation Control Protocol (LACP). Протокол LACP определяет метод управления объединением нескольких физических портов в одну логическую группу и

предоставляет сетевым устройствам возможность автосогласования каналов (их добавления или удаления) путем отправки управляющих кадров протокола LACP непосредственно подключенным устройствам с поддержкой LACP. Пакеты LACP отправляются устройством через все порты, на которых активизирован протокол. Порты, на которых активизирован протокол LACP, могут быть настроены для работы в одном из двух режимов: **активном** (*active*) или **пассивном** (*passive*). При работе в активном режиме порты выполняют обработку и рассылку управляющих кадров протокола LACP. При работе в пассивном режиме порты выполняют только обработку управляющих кадров LACP.

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

Следует отметить, что у портов, объединяемых в агрегированный канал, нижеперечисленные характеристики должны обладать одинаковыми настройками:

- тип среды передачи;
- скорость;
- режим работы — полный дуплекс;
- метод управления потоком (Flow Control) .

При объединении портов в агрегированный канал на них не должны быть настроены функции аутентификации 802.1X, зеркалирования трафика и блокировки портов.

5.7.1. Настройка статических и динамических агрегированных каналов

Рассмотрим пример, показанный на рис. 5.29. Для повышения пропускной способности канала связи между коммутатором 1, к которому подключен сервер, и коммутатором 2, к которому подключены пользователи, требуется объединить порты коммутаторов в статический агрегированный канал.

На коммутаторах необходимо выполнить следующую настройку:

Настройка коммутатора 1

- Создать группу агрегирования (тип канала Static) и задать алгоритм агрегирования.

```
create link_aggregation group_id 1 type static
config link_aggregation algorithm mac_destination
```

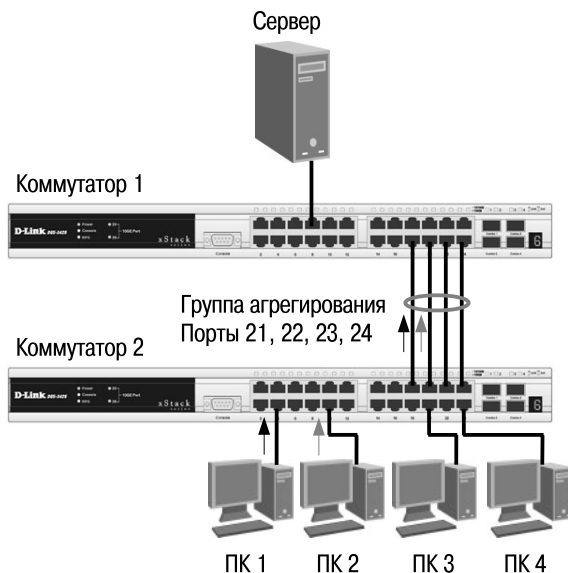


Рис. 5.29. Схема сети

- Включить порты 21, 22, 23, 24 в группу и выбрать порт 21 в качестве мастера-порта.

```
config link_aggregation group_id 1 master_port 21 ports
21,22,23,24 state enabled
```

Настройка коммутатора 2

- Создать группу агрегирования и задать алгоритм агрегирования.

```
create link_aggregation group_id 1 type static
config link_aggregation algorithm mac_source
```

- Включить порты 21, 22, 23, 24 в группу и выбрать порт 21 в качестве мастера-порта.

```
config link_aggregation group_id 1 master_port 21 ports
21,22,23,24 state enabled
```

Рассмотрим пример настройки коммутаторов при создании динамического агрегированного канала связи.

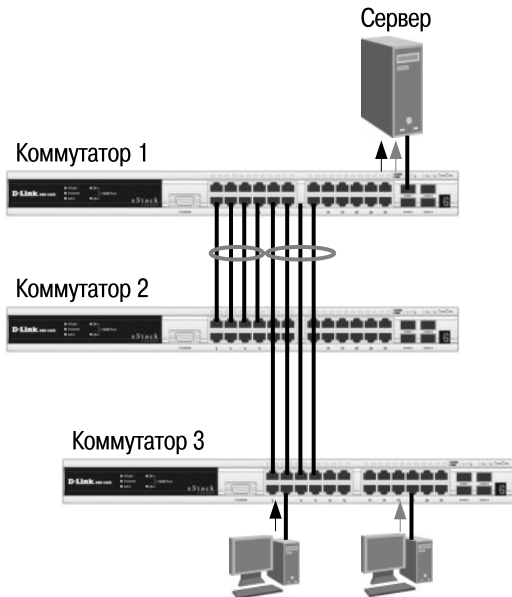


Рис. 5.30. Схема сети

Настройка коммутатора 1

- Создать группы агрегирования (тип канала LACP) и задать алгоритм агрегирования.

```
create link_aggregation group_id 1 type lacp
create link_aggregation group_id 2 type lacp
config link_aggregation algorithm mac_destination
```

- Включить порты 1, 2, 3, 4 в группу 1 и выбрать порт 1 в качестве мастера-порта.

```
config link_aggregation group_id 1 master_port 1 ports 1-4 state
enabled
```

- Включить порты 5, 6, 7, 8 в группу 2 и выбрать порт 5 в качестве мастера-порта.

```
config link_aggregation group_id 2 master_port 5 port 5-8 state
enabled
```

- Настроить для портов 1-8 активный режим работы.
`config lacp_port 1-8 mode active`

Настройка коммутаторов 2 и 3 (на портах 1-4 этих коммутаторов включено автосогласование)

```
create link_aggregation group_id 1 type lacp
config link_aggregation algorithm mac_source
config link_aggregation group_id master_port 1 ports 1-4 state
enabled
```

Внимание:

1. Если один конец агрегированного канала настроен как LACP, другой конец должен также иметь тип LACP. Если один конец имеет тип LACP, а другой Static, то соединение установлено не будет.
2. Если коммутатор с поддержкой LACP требуется подключить к коммутатору, поддерживающему только статическое агрегирование, то тип агрегированного канала на коммутаторе LACP необходимо установить в Static.
3. Не соединяйте физически соответствующие порты устройств до тех пор, пока не настроено агрегирование каналов, т.к. в коммутируемой сети может возникнуть петля.

Лекция 6. Качество обслуживания (QoS)

6.1. Модели QoS

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

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

Можно выделить три модели реализации QoS в сети.

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

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

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

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

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

6.2. Приоритизация пакетов

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

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

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

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Данные (Data)	Контрольная последовательность кадра (CRC)
-----------------------	----------------------	---------------	--

Маркированный кадр 802.1p/802.1Q

Адрес назначения (DA)	Адрес источника (SA)	Тег (Tag)	Данные (Data)	Контрольная последовательность кадра (CRC)
-----------------------	----------------------	------------------	---------------	--

Идентификатор протокола тега (TPID) 0x8100	Приоритет (Priority)	Индикатор канонического формата (CFI)	Идентификатор VLAN (VID)
16 бит	3 бита	1 бит	12 бит

Рис. 6.1. Формат кадра 802.1Q с битами приоритета 802.1p

Поле DSCP было стандартизировано IETF с появлением модели DiffServ. Оно занимает 6 старших бит байта ToS и позволяют задать до 64 уровней приоритетов (от 0 до 63). По сути код DSCP является расширением 3-битового поля IP Precedence и обладает обратной совместимостью с IP-приоритетом.

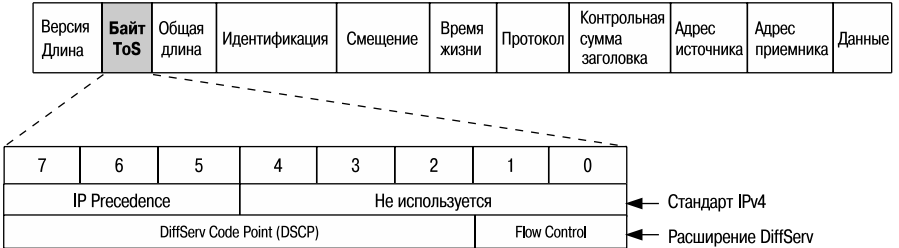


Рис. 6.2. Байт ToS заголовка IPv4

6.3. Классификация пакетов

Для обеспечения дифференцированного обслуживания трафика коммутаторы поддерживают в зависимости от модели от 4 до 8 аппаратных очередей приоритетов на каждом из своих портов. Для обеспечения требуемой очередности передачи пакетов данных в коммутаторе необходимо настроить алгоритм обслуживания очередей и карту привязки приоритетов 802.1p, ToS, DSCP к очередям.

По умолчанию в коммутаторах D-Link используются следующие карты привязки пользовательских приоритетов 802.1p к аппаратным очередям:

- **4 очереди приоритетов**

Приоритет	Номер очереди
0	Q1
1	Q0
2	Q0
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

- 8 очередей приоритетов

Приоритет	Номер очереди
0	Q2
1	Q0
2	Q1
3	Q3
4	Q4
5	Q5
6	Q6
7	Q6

Внимание: класс 7 в коммутаторах D-Link с поддержкой 8 очередей приоритетов зарезервирован для внутреннего использования и поэтому не настраивается.

В коммутаторах с поддержкой 4-х очередей приоритетов очереди нумеруются от 0 до 3, где очередь 3 обладает наивысшим приоритетом, очередь 0 – низшим. В коммутаторах с поддержкой 8-ми очередей приоритетов очереди нумеруются от 0 (низший приоритет) до 7 (наивысший приоритет).

Программное обеспечение коммутаторов позволяет настраивать карты привязки приоритетов 802.1p, ToS, DSCP к очередям в соответствии с требованиями пользователей.

Для того чтобы поместить пакет в одну из очередей приоритетов в соответствии с заданной политикой QoS, коммутатор анализирует содержимое одного или нескольких полей его заголовка – приоритет 802.1p, IP-приоритет или поле DSCP в байте ToS. Этот процесс называется *классификацией пакетов (packet classification)*.

Следует отметить, что при этом коммутатор не изменяет значения приоритетов внутри пакетов данных, а только определяет очередность и способ их обработки выходным портом, основываясь на реализованной в нем политике QoS.

В том случае, если на входной порт коммутатора поступает немаркированный кадр (заголовок кадра не содержит битов приоритета), то его классификация осуществляется на основе значения приоритета 802.1p, по умолчанию назначенного данному порту.

Также для классификации пакетов данных на основании различных параметров их заголовков, например MAC-адреса, IP-адреса, номера порта TCP/UDP, тега VLAN и т.д., могут использоваться списки управления доступом (Access Control List, ACL).

6.4. Маркировка пакетов

После процесса классификации коммутатор может осуществить *маркировку пакетов (packet marking)*. Маркировка пакетов определяет способ записи/перезаписи значений битов приоритета (DSCP, 802.1p или IP Precedence) входящих пакетов данных. Обычно процесс маркировки выполняется на граничных устройствах и позволяет последующим коммутаторам/маршрутизаторам использовать новое значение приоритета пакета для отнесения его к одному из поддерживаемых в сети классов обслуживания. Изменить значения битов приоритета в заголовках входящих пакетов данных можно с помощью списков управления доступом.

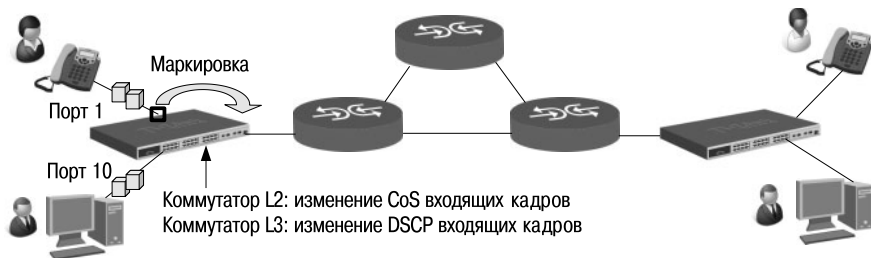


Рис. 6.3. Маркировка пакетов

6.5. Управление перегрузками и механизмы обслуживания очередей

Наиболее часто перегрузка сети возникает в местах соединения коммутаторами сетей с разной полосой пропускания. В случае возникновения перегрузки сети пакеты данных начинают буферизироваться и распределяться по очередям. Порядок передачи через выходной интерфейс поставленных в очередь пакетов на основе их приоритетов опреде-

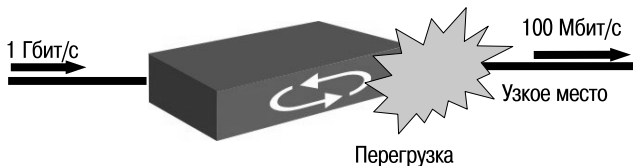


Рис. 6.4. Возникновение перегрузки в сети

ляется *механизмом обслуживания очередей (Queuing mechanism)*, который позволяет управлять пропускной способностью сети при возникновении перегрузок.

Механизм управления перегрузками (*Congestion management*) включает следующие механизмы обслуживания очередей:

- механизм FIFO (First-In, First-Out);
- очереди приоритетов (Priority Queuing);
- взвешенный алгоритм кругового обслуживания (Weighted Round Robin, WRR);
- настраиваемые очереди (Custom Queuing).

В коммутаторах D-Link для обслуживания очередей используются взвешенный алгоритм кругового обслуживания, очереди приоритетов и комбинации этих методов.

Механизм обслуживания очередей FIFO («первым пришел, первым ушел») передает пакеты, поставленные в очередь в том порядке, в котором они поступили в нее. Этот механизм не обеспечивает классификации пакетов и рассматривает их как принадлежащие одному классу.

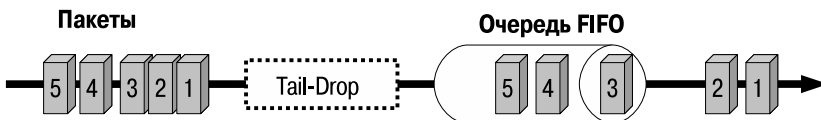


Рис. 6.5. Очередь FIFO

Очереди приоритетов со строгим режимом (Strict Priority Queue) предполагают передачу трафика строго в соответствии с приоритетом выходных очередей. В этом механизме предусмотрено наличие 4-х очередей — с высоким, средним, обычным и низким приоритетами обслуживания. Пакеты, находящиеся в очереди с высоким приоритетом, обрабатываются первыми. Пакеты из следующей по приоритету очереди начнут передаваться только после того, как опустеет высокоприоритетная очередь. Например, пакеты из средней по приоритету очереди не будут передаваться до тех пор, пока не будут обслужены пакеты из высокоприоритетной очереди. Пакеты из очереди с нормальным приоритетом не начнут передаваться до тех пор, пока не опустеет очередь со средним приоритетом и т.д.

Следует отметить, что пакеты очереди с высоким приоритетом всегда получают предпочтение при обслуживании независимо от количества пакетов в других очередях и времени, прошедшего с момента передачи последнего пакета из очереди с низким приоритетом. В некоторых случа-

ях это может привести к «зависанию» обслуживания низкоприоритетного трафика, т.е. пакеты из очередей с низким приоритетом долго не будут обрабатываться.

По умолчанию на коммутаторах D-Link настроены очереди приоритетов со строгим режимом.

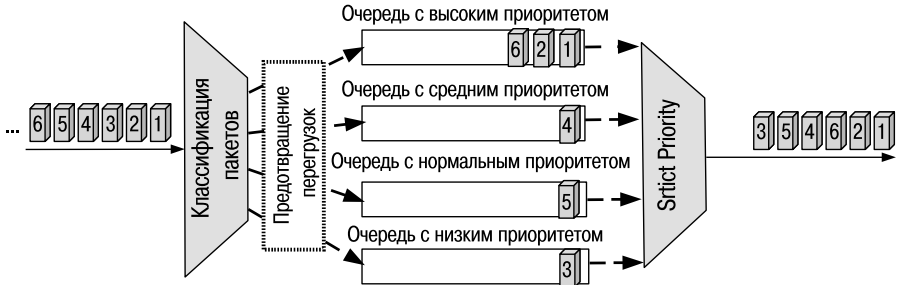


Рис. 6.6. Очереди приоритетов со строгим режимом

Еще одним механизмом обслуживания очередей является *взвешенный алгоритм кругового обслуживания* (Weighted Round Robin, WRR). Этот механизм исключает главный недостаток очередей приоритетов, обеспечивая обработку очередей в соответствии с назначенным им весом и предоставляя полосу пропускания для пакетов из низкоприоритетных очередей.

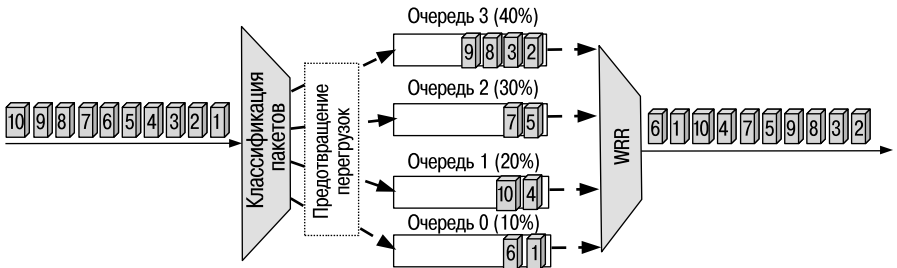


Рис. 6.7. Обслуживание очередей с использованием алгоритма WRR

Процесс обработки очередей осуществляется по круговому принципу, начиная с самой приоритетной очереди. Из каждой непустой очереди передается некоторый объем трафика, пропорциональный назначенному ей весу, после чего выполняется переход к следующей по убыванию приоритета очереди и т.д. по кругу.

6.6. Механизм предотвращения перегрузок

Механизм предотвращения перегрузок (Congestion avoidance) – это процесс выборочного отбрасывания пакетов во избежание перегрузок в сети в случае достижения выходными очередями своей максимальной длины (в пакетах).

Традиционной политикой обработки пакетов коммутаторами в случае переполнения всех выходных очередей является их отбрасывание, которое продолжается до тех пор, пока длина очередей не уменьшится за счет передачи находящихся в них пакетов. Такой алгоритм управления длиной выходных очередей получил название *«отбрасывание хвоста» (Tail-Drop)*. Отбрасывание пакета будет служить сигналом о перегрузке сети источнику ТСП-соединения, т.к. он не получит подтверждения о доставке пакета от приемника ТСП-соединения. В этом случае он уменьшит скорость передачи путем уменьшения размера окна перегрузки до одного сегмента и перезапустит алгоритм *медленного старта (slow start)*.

Поскольку коммутатор обрабатывает множество ТСП-потоков в один момент времени, отбрасывание пакетов послужит сигналом о перегрузке тысячам источникам ТСП-соединений, которые снизят скорость передачи. При этом почти все источники ТСП-соединений будут использовать одинаковое время таймеров задержки перед началом увеличения скорости передачи. Значения этих таймеров достигнут своего лимита практически одновременно, что вызовет увеличение интенсивности трафика и переполнение очередей, которое приведет к отбрасыванию пакетов, и весь процесс повторится вновь.

Процесс, когда каждый источник ТСП-соединения уменьшает и увеличивает скорость передачи одновременно с другими источниками ТСП-соединений, получил название *эффекта глобальной синхронизации (global synchronization)*. Эффект глобальной синхронизации приводит к неэффективному использованию полосы пропускания, а также к возрастанию задержки передачи пакетов.

Для решения проблемы поведения источников ТСП-соединения в момент отбрасывания пакетов был разработан *алгоритм произвольного раннего обнаружения (Random Early Detection, RED)*.

В отличие от алгоритма «отбрасывания хвоста», алгоритм RED отбрасывает поступающие пакеты вероятностно, на основе оценки среднего размера очередей. Он не дожидается полного заполнения очередей, а начинает отбрасывать пакеты с некоторой вероятностью, когда средний размер очереди превысит определенное минимальное пороговое значение. Это позволяет избежать эффекта глобальной синхронизации, т.к. будут отбрасываться не все пакеты, а только пакеты произвольным образом выбранных потоков.

В коммутаторах D-Link поддерживается *простой алгоритм произвольного раннего обнаружения (Simple Random Early Detection, SRED)*, который является расширенной версией алгоритма RED, реализованной на основе ASIC, и выполняет вероятностное отбрасывание входящих «окрашенных» пакетов. «Окрашивание» пакетов позволяет реализовать разные политики обслуживания пакетов (различную вероятность отбрасывания) на основе их приоритетов. Так пакеты, «окрашенные» в зеленый цвет обладают наивысшим приоритетом. Пакеты «окрашенные» в желтый цвет – средним, в красный цвет – низшим приоритетом.

Алгоритм SRED позволяет задавать два пороговых значения размера для каждой очереди – минимальное и максимальное. Если длина очереди меньше минимального порогового значения, то пакеты будут помещаться в очередь. Если размер очереди будет находиться в интервале между минимальным и максимальным пороговыми значениями, т.е. будет наблюдаться умеренная перегрузка, то пакеты, «окрашенные» в красные и желтые цвета, будут отбрасываться с заданной вероятностью. Если длина очереди превысит максимальное пороговое значение, то пакеты любых цветов будут отбрасываться с заданной вероятностью. Т.е. алгоритм SRED обеспечивает возможность настройки более интенсивного отбрасывания пакетов низкоприоритетного трафика и менее интенсивного отбрасывания пакетов высокоприоритетного трафика.

В коммутаторах D-Link при настройке SRED существует возможность выбора из восьми значений скоростей (вероятностей) отбрасывания пакетов:

	Скорость отбрасывания
1	100%
2	6.25%
3	3.125%
4	1.5625%
5	0.78125%
6	0.390625%
7	0.1953125%
8	0.09765625%

6.7. Контроль полосы пропускания

Современные коммутаторы позволяют регулировать интенсивность трафика на своих портах с целью обеспечения функций качества обслуживания. Для этого они используют механизмы, называемые *Traffic Policing* (ограничение трафика) и *Traffic Shaping* (выравнивание трафика).

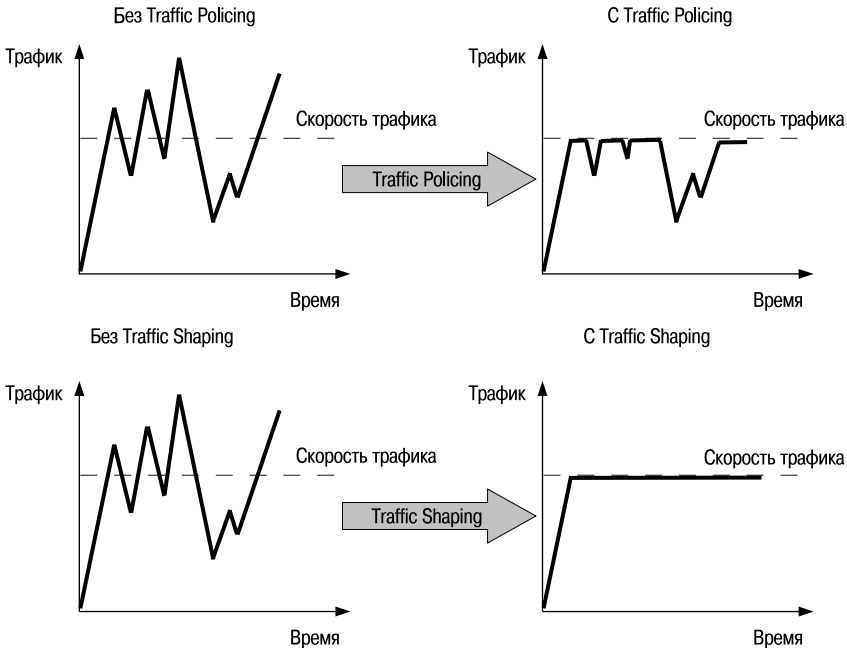


Рис. 6.8. Механизмы Traffic Policing и Traffic Shaping

Механизм Traffic Policing служит для ограничения скорости трафика, получаемого или отправляемого с интерфейса коммутатора. Когда эта функция активна, администратор может устанавливать различные пороговые значения скорости передачи на каждом из выходных портов коммутатора. Трафик, скорость которого меньше или равна пороговому значению, будет передаваться; трафик, скорость которого превышает пороговое значение, будет обрабатываться в соответствии с настроенной политикой, например, отбрасываться или маркироваться новым значением приоритета.

Основным средством, используемым для ограничения трафика, является хорошо известный алгоритм «корзина маркеров» (*token bucket*). Этот алгоритм предполагает наличие следующих параметров:

- **согласованная скорость передачи (Committed Information Rate, CIR)** — средняя скорость передачи трафика через интерфейс коммутатора/маршрутизатора. Этот параметр также определяет скорость помещения маркеров в корзину;
- **согласованный размер всплеска (Committed Burst Size, CBS)** — это объем трафика (в битах), на который может быть превышен размер корзины маркеров в отдельно взятый момент всплеска;

- **расширенный размер всплеска (Extended Burst Size, EBS)** – это объем трафика (в битах), на который может быть превышен размер корзины маркеров в экстренном случае.

На рис. 6.9 показана схема реализации алгоритма «корзина маркеров» в рамках механизма Traffic Policing.

Размер стандартной корзины маркеров (максимальное число маркеров, которое она может вместить) равен согласованному размеру всплеска (CBS). Маркеры генерируются и помещаются в корзину с определенной скоростью (CIR). Если корзина полна, то поступающие избыточные маркеры отбрасываются. Для того чтобы передать пакет из корзины вынимается число маркеров, равное размеру пакета в битах. Если маркеров в корзине достаточно, то пакет передается. Если размер пакета оказался больше, чем маркеров в корзине, то маркеры из корзины не извлекаются, а пакет рассматривается как не удовлетворяющий (non-conform) заданному профилю или избыточный. Для избыточных пакетов могут применяться различные способы обработки: они могут отбрасываться или перемаркироваться.



Рис. 6.9. Алгоритм «корзина маркеров» в рамках механизма Traffic Policing

Стандартная корзина маркеров не поддерживает экстренное увеличение размера всплеска, поэтому в такой реализации расширенный размер всплеска (EBS) равен согласованному размеру всплеска (CBS).

В корзине маркеров с возможностью экстренного увеличения размера всплеска расширенный размер всплеска (EBS) больше согласованного размера всплеска (CBS). Объем трафика (в битах), на который может быть превышен размер корзины, рассчитывается по формуле:

$$\begin{aligned} \text{CBS} &= 1,5 \times \text{CIR}/8 \\ \text{EBS} &= 2 \times \text{CBS} \end{aligned}$$

При такой реализации корзины маркеров, в случае нехватки маркеров, необходимых для передачи пакета, учитывается расширенный размер всплеска.

Механизм Traffic Shaping служит для сглаживания исходящего с интерфейсов коммутатора трафика. В отличие от механизма Traffic Policing, который в случае превышения скорости трафика заданного порогового значения может отбрасывать пакеты, механизм Traffic Shaping помещает избыточные пакеты в буфер.

В качестве средства выравнивания трафика механизм Traffic Shaping также использует алгоритм «корзина маркеров». В соответствии с меха-

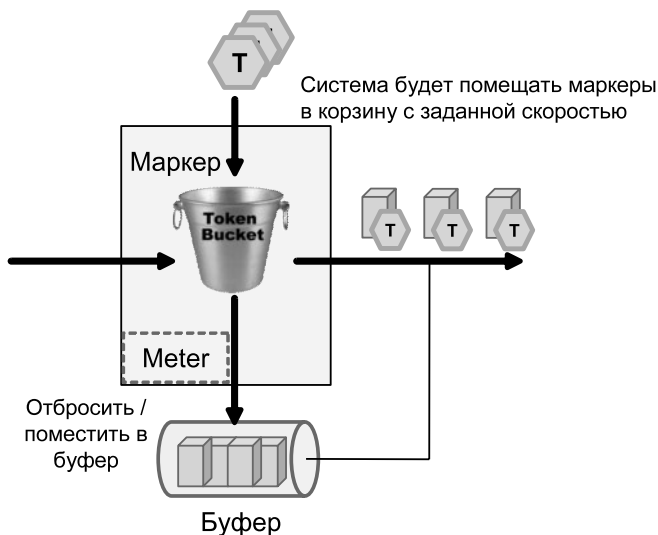


Рис. 6.10. Алгоритм «корзина маркеров» в рамках механизма Traffic Shaping

низмом Traffic Shaping из корзины вынимается число маркеров, равное размеру пакета в битах. Если в корзине имелось достаточное количество маркеров, то пакет передается. В противном случае пакет маркируется как неудовлетворяющий заданному профилю и ставится в очередь (буферизируется) для последующей передачи. Как только в корзине накопится количество маркеров, достаточное для передачи пакета, он будет передан.

Следует отметить, что механизм Traffic Shaping вносит задержку в передачу трафика, что критично для приложений, чувствительных к задержкам, таким как IP-телефония, потоковое видео и т.д. Однако этот механизм более дружелюбен к TCP-потокам, т.к. благодаря буферизации уменьшается количество отбрасываемых пакетов и число их повторных передач.

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

В качестве примера приведем настройку ограничения скорости до 128 Кбит/с для трафика, передаваемого с интерфейса 5 коммутатора.

```
config bandwidth_control 5 tx_rate 128
```

Более гибким решением ограничения полосы пропускания является функция *per-flow Bandwidth control*, реализованная на старших моделях управляемых коммутаторов D-Link. Эта функция позволяет ограничивать полосу пропускания не всему трафику, получаемому или передаваемому с интерфейса коммутатора, а конкретным потокам данных, определенным администратором сети.

Функция *per-flow Bandwidth control* использует механизм списков управления доступом для просмотра определенного типа трафика и ограничения для него полосы пропускания. Весь этот процесс происходит на микросхемах портов ASIC. Таким образом, это не влияет на загрузку ЦПУ, соответственно, не снижает производительности коммутатора.

6.8. Пример настройки QoS

На рис. 6.11 приведена схема локальной сети, в которой пользователи 1 и 3 используют приложения IP-телефонии. Голосовому трафику пользователей 1 и 3 требуется обеспечить наивысшее качество обслужи-

вания по сравнению с трафиком других приложений, выполняемых на компьютерах остальных пользователей сети.

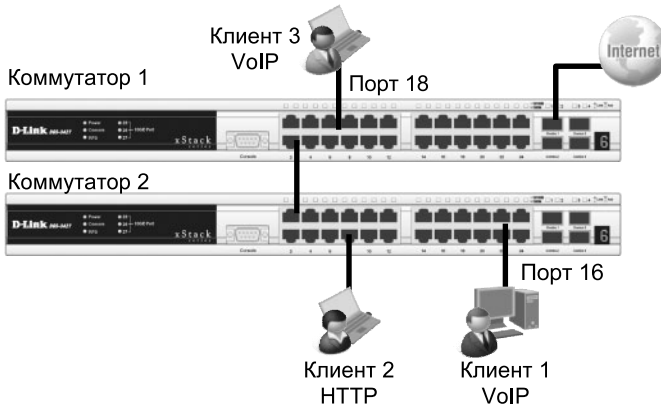


Рис. 6.11. Пример настройки QoS

Настройка коммутатора 1

- Для того чтобы внутри коммутатора могла обрабатываться информация о приоритетах 802.1p, состояние портов коммутатора, к которым подключены пользователи, необходимо перевести из «немаркированные» в «маркированные».

```
config vlan default add tagged 1-6
```

- Изменить приоритет порта 18, к которому подключен пользователь 3, использующий приложения IP-телефонии, с 0 (установлено по умолчанию) на 7. Пакеты с приоритетом 7 будут помещаться в очередь Q6, которая имеет наивысший приоритет обработки.

```
config 802.1p default_priority 18 7
```

Настройка коммутатора 2

- Изменить состояния портов с «немаркированные» на «маркированные»

```
config vlan default add tagged 1-6
```

- Изменить приоритет порта 16, к которому подключен пользователь 1, использующий приложения IP-телефонии, с 0 (установле-

но по умолчанию) на 7. Пакеты с приоритетом 7 будут помещаться в очередь Q6, которая имеет наивысший приоритет обработки.

```
config 802.1p default_priority 16 7
```

Карта привязки приоритетов 802.1p к очередям и механизм обслуживания очередей не изменяются и используют параметры, настроенные по умолчанию.

Лекция 7. Функции обеспечения безопасности и ограничения доступа к сети

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

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

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

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

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

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

Решение Joint Security включает в себя функции:

- Zone Defense;
- NAP.

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

- D-Link Safeguard Engine;
- Traffic Storm Control.

Прежде чем приступить к рассмотрению темы, уточним некоторые понятия.

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

Авторизация – предоставление определенных прав лицу на выполнение некоторых действий.

Как правило, за аутентификацией следует авторизация.

7.1. Списки управления доступом (ACL)

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

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

- порт коммутатора;
- MAC/ IP-адрес;
- тип Ethernet/ тип протокола;
- VLAN;
- 802.1p/ DSCP;
- порт TCP/ UDP (тип приложения);
- первые 80 байт пакета, включая поле данных.

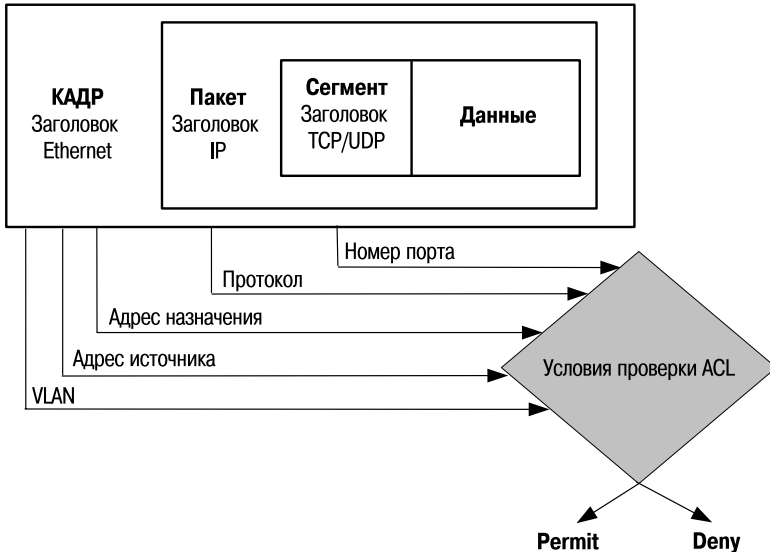


Рис. 7.1. Списки управления доступом (ACL)

Внимание: наборы критериев фильтрации ACL могут отличаться у разных моделей коммутаторов, поэтому прежде чем приступать к конфигурированию функции, необходимо ознакомиться с документацией на используемое устройство.

7.1.1. Профили доступа и правила ACL

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

Когда коммутатор получает кадр, он проверяет его поля на совпадение с типами критериев фильтрации и их параметрами, заданными в профилях и правилах. Последовательность, в которой коммутатор проверяет кадр на совпадение с параметрами фильтрации, определяется порядковым номером профиля (Profile ID) и порядковым номером правила (Rule ID). Профили доступа и правила внутри них работают последовательно, в порядке возрастания их номеров. Т.е. кадр проверяется на соответствие условиям фильтрации, начиная с первого профиля и пер-

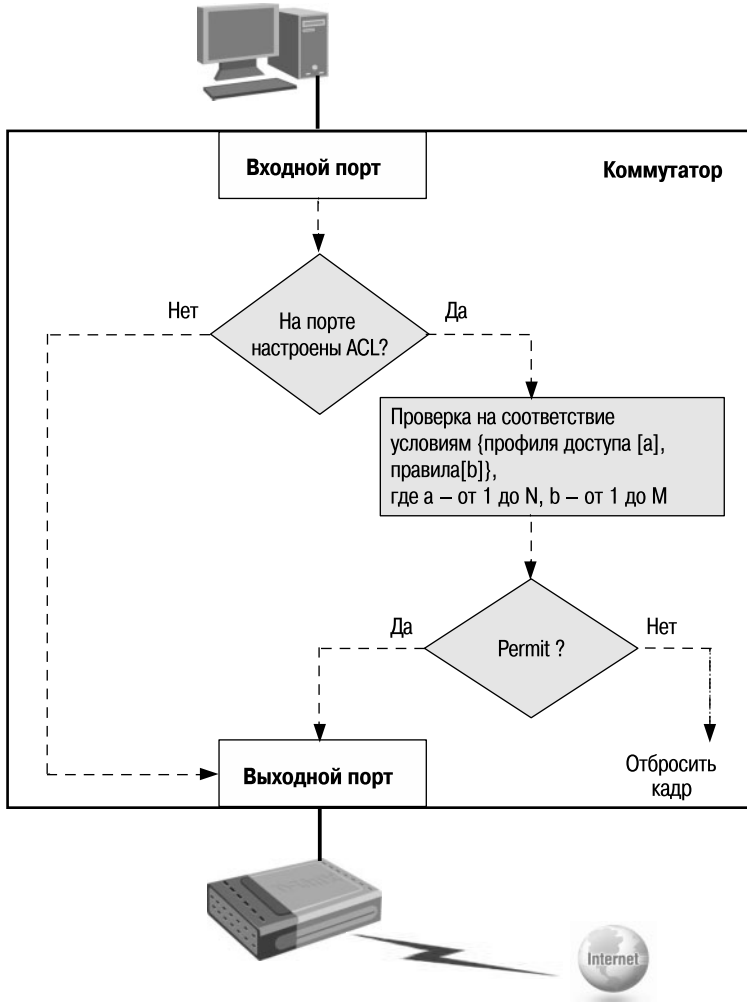


Рис. 7.2. Принцип работы ACL

вого правила в нем. Так, кадр сначала будет проверяться на соответствие условиям, определенным в правиле 1 профиля 1. Если параметры кадра не подходят под условия проверки, то далее кадр будет проверяться на совпадение с условиями, определенными в правиле 2 профиля 1 и т.д. Если ни одно из правил текущего профиля не совпало с параметрами кадра, то коммутатор продолжит проверку на совпадение параметров кадра с условиями правила 1 следующего профиля. При первом совпадении параметров кадра с правилом к кадру будет применено одно из действий, определенных в правиле: «Запретить», «Разрешить» или «Изменить содержимое поля пакета» (приоритет 802.1p/ DSCP). Дальше кадр проверяться не будет. Если ни одно из правил не подходит, применяется политика по умолчанию, разрешающая прохождение всего трафика.

Следует отметить, что коммутаторы имеют ограничения по количеству обрабатываемых профилей и правил. Информацию о максимальном количестве поддерживаемых профилей и правил можно найти в документации на используемое устройство.

Типы профилей доступа

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

Профиль Ethernet (Ethernet Profile) позволяют фильтровать кадры по следующим типам критериев:

- VLAN;
- MAC-адрес источника;
- MAC-адрес назначения;
- 802.1p;
- тип Ethernet.

Профиль IP (IP Profile) поддерживает следующие типы критериев фильтрации:

- VLAN;
- маска IP-источника;
- маска IP-назначения;
- DSCP;
- протокол (ICMP, IGMP, TCP, UDP);
- номер порта TCP/UDP.

Профиль фильтрации по содержимому пакета (Packet Content Filtering Profile) используется для идентификации пакетов, путем побайтного исследования их заголовков Ethernet.

Внимание: не все модели коммутаторов поддерживают Packet Content Filtering Profile. За информацией о поддержке функции необходимо обратиться к документации на используемый коммутатор.

Процесс создания профиля доступа

Процесс создание профиля доступа можно разделить на следующие основные шаги:

- проанализируйте задачи фильтрации и определитесь с типом профиля доступа – Ethernet, IP или Packet Content Filtering;
- определите стратегию фильтрации.

Например:

- ♦ отбрасывать кадры некоторых узлов и принимать кадры от всех остальных узлов – эта стратегия применима для сетевой среды с несколькими узлами/протоколами портов/подсетями, для которых необходимо выполнять фильтрацию;
- ♦ принимать кадры от некоторых узлов и отбрасывать кадры всех остальных узлов – эта стратегия применима для сетевой среды с несколькими узлами/протоколами портов/подсетями, кадры от которых разрешены в сети. Трафик остальных узлов будет отбрасываться.

Основываясь на выбранной стратегии, определите, какая маска профиля доступа (Access Profile Mask) необходима, и создайте ее (команда *create access_profile*). Маска профиля доступа используется для указания, какие биты значений полей IP-адрес, MAC-адрес, порт TCP/UDP и т.д. должны проверяться в пакете данных, а какие игнорироваться;

- добавьте правило профиля доступа (Access Profile Rule), связанное с этой маской (команда *config access_profile*).

Правила профиля доступа проверяются в соответствии с номером *access_id*. Чем меньше номер, тем раньше проверяется правило. Если ни одно правило не сработало, кадр пропускается.

В среде QoS, после того как срабатывает правило, перед отправкой пакета данные биты 802.1p/DSCP могут быть заменены на новые низко/высокоприоритетные значения.

Вычисление маски профиля доступа

Маска профиля доступа определяет, какие биты в значениях полей «IP-адрес», «MAC-адрес», «порт TCP/UDP» и т.д. входящих на коммутатор кадров должны проверяться, а какие игнорироваться. Биты маски имеют следующие значения:

«0» – означает игнорирование значения соответствующего бита поля пакета данных;

«1» – означает проверку значения соответствующего бита поля пакета данных.

Предположим, администратору сети необходимо запретить прохождение трафика от узла с MAC-адресом 01-00-00-00-AC-11. Маска профиля доступа для этого адреса будет равна FF-FF-FF-FF-FF-FF. Если необходимо запретить или разрешить прохождение через коммутатор трафика любого узла из подсетей 192.168.16.0/24 – 192.168.31.0/24, то маска профиля доступа будет вычисляться, как показано на рисунке ниже.

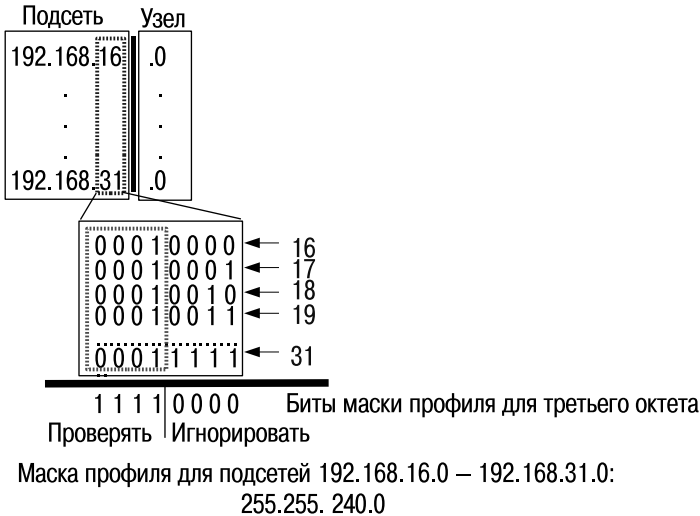


Рис. 7.3. Вычисление маски профиля

Первые два октета IP-адресов из проверяемого диапазона имеют одинаковое значение – «192.168». Они будут использоваться при проверке пакета, поэтому соответствующие биты маски содержат все 1. Последний октет IP-адреса будет игнорироваться, т.к. нет заинтересованности в проверке индивидуальных адресов узлов подсетей. Поэтому последний октет маски профиля содержит все 0. В третьем октете значение маски будет равно 240 (11110000), т.к. оно охватывает все номера с 16 (00010000) до 31 (00011111), имеющие одинаковые значения (0001) первых четырех битов. Последние четыре бита третьего октета IP-адреса маска профиля будет игнорировать, как малозначащие.

7.1.2. Примеры настройки ACL

Предположим, что администратору сети необходимо разрешить доступ в Интернет только некоторым пользователям, а остальным пользо-

вателям запретить. Пользователи идентифицируются по MAC-адресам их компьютеров.

В примере, показанном на рис. 7.4, пользователи ПК 1 и ПК 2 получают доступ в Интернет, т.к. их MAC-адреса указаны в разрешающем правиле 1. Как только пользователи других компьютеров попытаются выйти в Интернет, сработает правило 2, которое запрещает прохождение через коммутатор кадров с MAC-адресом назначения, равным MAC-адресу Интернет-шлюза.



Рис. 7.4. Пример ACL для профиля Ethernet

Настройка коммутатора для профиля Ethernet

- Правило 1: если MAC-адрес источника SourceMAC равен MAC-адресам ПК 1 или ПК 2 – разрешить (Permit).

```
create access_profile ethernet source_mac FF-FF-FF-FF-FF-FF
profile_id 1 profile_name Permit_Internet
config access_profile profile_id 1 add access_id 1 ethernet
source_mac 00-50-ba-11-11-11 port 1 permit
config access_profile profile_id 1 add access_id 2 ethernet
source_mac 00-50-ba-22-22-22 port 10 permit
```

- Правило 2: если MAC-адрес назначения DestMAC равен MAC-адресу Интернет-шлюза – запретить (Deny).

```
create access_profile ethernet destination_mac FF-FF-FF-FF-FF-FF
profile_id 2 profile_name Deny_Internet
config access_profile profile_id 2 add access_id 1 ethernet destination_mac 00-50-ba-99-99-99 port 11 deny
```

- Иначе — по умолчанию разрешить доступ всем узлам.

В качестве второго примера приведем настройку ACL с профилем IP. Предположим, что администратору необходимо разрешить доступ в Интернет только пользователям с IP-адресами с 192.168.0.1/24 по 192.168.0.63/24. Остальным пользователям сети 192.168.0.0/24 с адресами, не входящими в разрешенный диапазон, доступ в Интернет запрещен.

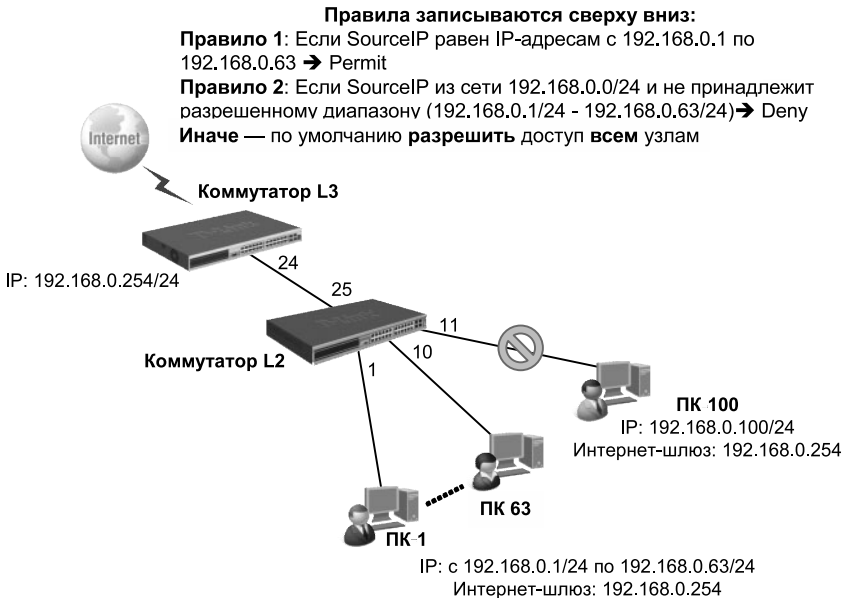


Рис. 7.5. Пример ACL для профиля IP

Настройка в коммутаторе L3 профиля IP

- Правило 1: если IP-адрес источника Source IP равен IP-адресам из диапазона с 192.168.0.1 по 192.168.0.63 — разрешить (Permit).

```
create access_profile ip source_ip_mask 255.255.255.192 profile_id 1
config access_profile profile_id 1 add access_id 1 ip source_ip
192.168.0.0 port 24 permit
```

- Правило 2: если IP-адрес источника Source IP принадлежит сети 192.168.0.0/24, но не входит в разрешенный диапазон адресов – запретить (Deny).

```
create access_profile ip source_ip_mask 255.255.255.0 profile_id 2
config access_profile profile_id 2 add access_id 1 ip source_ip
192.168.0.0 port 24 deny
```

- Иначе – по умолчанию разрешить доступ всем узлам.

7.2. Функции контроля над подключением узлов к портам коммутатора

В том случае, если какой-либо порт на коммутаторе активен, к нему может подключиться любой пользователь и получить несанкционированный доступ к сети. Этот пользователь может начать генерировать вредоносный трафик, который попадет в сеть и создаст проблемы внутри нее. Для защиты от подобных ситуаций, а также для контроля подключения узлов к портам коммутатора D-Link предоставляют функции безопасности, которые позволяют указывать MAC- и/или IP-адреса устройств, которым разрешено подключаться к данному порту, и блокировать доступ к сети узлам с неизвестными коммутатору адресами.

7.2.1. Функция Port Security

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

Внимание: для функции Port Security существуют ограничения по количеству MAC-адресов, которые может обслуживать каждый порт. Эти ограничения различны для разных моделей коммутаторов. Для получения информации о максимальном количестве обслуживаемых портом MAC-адресов необходимо обратиться к спецификации на используемое устройство.

Существует три режима работы функции Port Security:

- *Permanent* («Постоянный») – занесенные в таблицу коммутации MAC-адреса никогда не устаревают, даже если истекло время, установленное таймером FDB Aging Time, или коммутатор был перезагружен;
- *Delete on Timeout* («Удалить по истечении времени») – занесенные в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером FDB Aging Time, и будут удалены.

Если состояние канала связи на подключенном порте изменяется, MAC-адреса, изученные на нем, удаляются из таблицы коммутации, что аналогично выполнению действий при истечении времени, установленного таймером FDB Aging Time;

- *Delete on Reset* («Удалить при сбросе настроек») – занесенные в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

При подключении неавторизованного пользователя к порту коммутатора он будет заблокирован, а коммутатор отправит сообщение SNMP Trap или создаст запись в Log-файле, если администратор настроил выполнение этих действий. Порт коммутатора будет отбрасывать трафик, поступающий с неизвестного MAC-адреса.



Рис. 7.6. Функция Port Security

7.2.1.1. Пример настройки функции Port Security

В качестве примера рассмотрим ситуацию, показанную на рис. 7.6. На портах 1-3 управляемого коммутатора настроено ограничение по количеству подключаемых пользователей (к каждому порту может подключиться не более двух пользователей). MAC-адреса подключаемых пользователей изучаются портами 1-3 динамически.

Настройка коммутатора

```
config port_security ports 1-3 admin_state enabled
max_learning_addr 2 lock_address_mode DeleteOnTimeout
```

В приведенном примере конфигурации используется режим Delete on Timeout. Это означает, что изученные на порте MAC-адреса будут удалены из таблицы коммутации по истечении времени, установленного таймером Aging Time, если по ним не было обращений (например, рабочая станция отключилась от сети). В этом случае к сети смогут подключиться новые пользователи, MAC-адреса, которых будут динамически изучены портом (рис. 7.7).



Рис. 7.7. Функция Port Security в режиме Delete on Timeout

При использовании режима работы Permanent адреса, изученные портом, будут добавлены в статическую таблицу MAC-адресов и будут храниться в ней даже после включения/выключения питания и перезагрузки коммутатора.

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

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

Настройка коммутатора

- Активизировать функцию Port Security на соответствующих портах и запретить изучение MAC-адресов (параметр *max_learning_addr* установить равным 0).

```
config port_security ports 1-24 admin_state enabled
max_learning_addr 0
```

- Создать записи в статической таблице MAC-адресов (имя VLAN в примере “default”).

```
create fdb default 00-50-ba-00-00-01 port 2
create fdb default 00-50-ba-00-00-02 port 2
create fdb default 00-50-ba-00-00-03 port 2
create fdb default 00-50-ba-00-00-04 port 2
create fdb default 00-50-ba-00-00-05 port 8
(аналогично для всех требуемых портов)
```

7.2.2 Функция IP-MAC-Port Binding

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

ет MAC-адрес соответствующего узла с занесением его в «черный лист».

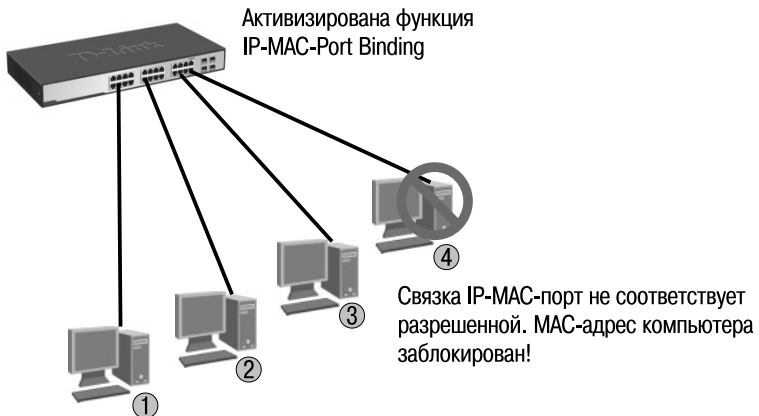


Рис. 7.8. Функция IP-MAC-Port Binding

Функция IP-MAC-Port Binding специально разработана для управления подключением узлов в сетях ЕТТН (Ethernet-To-The-Home) и офисных сетях. Помимо этого функция IMPV позволяет бороться с атаками типа ARP Spoofing, во время которых злонамеренные пользователи перехватывают трафик или прерывают соединение, манипулируя пакетами ARP.

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

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

При функционировании в *ACL mode* коммутатор на основе предустановленного администратором «белого листа» IMPV создает правила ACL. Любой пакет, связка IP-MAC которого отсутствует в «белом листе», будет блокироваться ACL. Если режим ACL отключен, правила для записей IMPV будут удалены из таблицы ACL. Следует отметить, что этот режим не поддерживается коммутаторами, в которых отсутствуют аппаратные

таблицы ACL (информацию о поддержке или отсутствии режима ACL можно найти в спецификации на соответствующую модель коммутатора).

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

Внимание: режим DHCP Snooping отдельно от режимов ARP или ACL не используется.

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

- **Strict Mode** – в этом режиме порт по умолчанию заблокирован. Прежде чем передавать пакеты, он будет отправлять их на ЦПУ для проверки совпадения их параметров IP-МАС с записями в «белом листе». Таким образом, порт не будет передавать пакеты до тех пор, пока не убедится в их достоверности. Порт проверяет все IP и ARP-пакеты;
- **Loose Mode** – в этом режиме порт по умолчанию открыт. Порт будет заблокирован, как только через него пройдет первый недостоверный пакет. Порт проверяет только пакеты ARP и IP Broadcast.

7.2.2.1. Пример настройки функции IP-МАС-Port Binding

На рис. 7.9 показан пример работы функции IP-МАС-Port Binding в режиме ARP. Хакер инициировал атаку типа ARP Spoofing. Коммутатор обнаруживает, что на порт 10 приходят пакеты ARP, связка IP-МАС для которых отсутствует в «белом листе» IMPB, и блокирует МАС-адрес узла.

Настройка коммутатора

- Создать запись IP-МАС-Port Binding, связывающую IP-МАС-адрес узла с портами подключения, и указать режим работы функции.

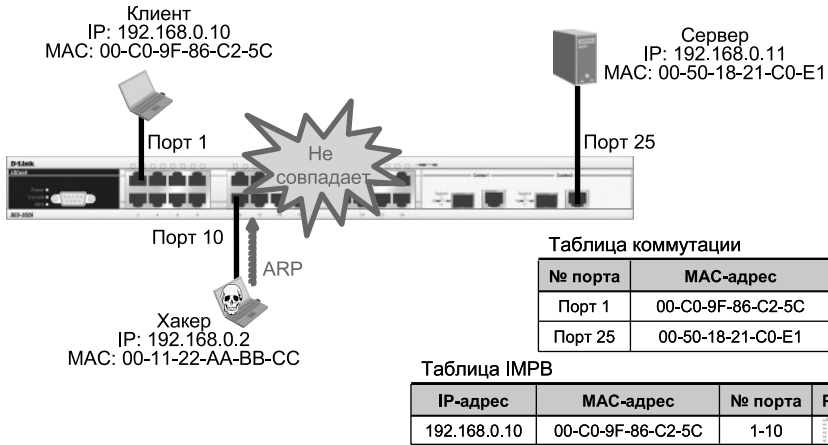
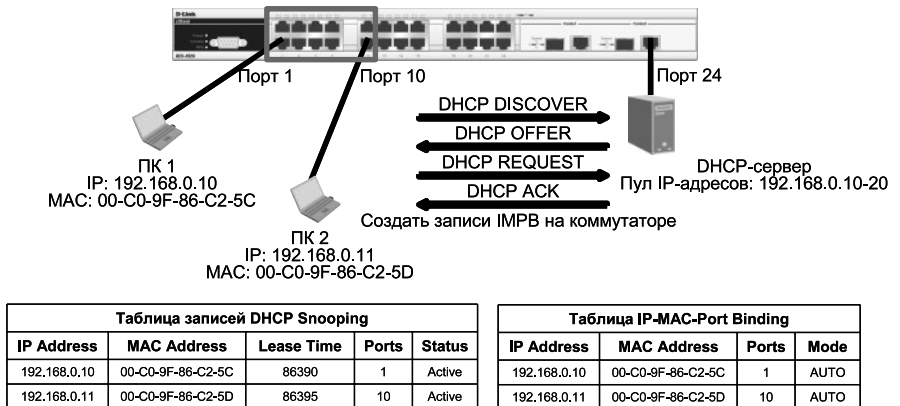


Рис. 7.9. Пример работы функции IP-MAC-Port Binding в режиме ARP

```
create address_binding ip_mac ipaddress 192.168.0.10 mac_address 00-C0-9F-86-C2-5C ports 1-10 mode arp
```

- Активизировать функцию на требуемых портах и указать режим работы портов.

```
config address_binding ip_mac ports 1-10 state enable loose
```



Коммутатор автоматически создает записи IP-MAC-Port Binding, когда получает пакет DHCP.

Рис. 7.10. Пример работы функции IP-MAC-Port Binding в режиме DHCP Snooping

На рис. 7.10 приведен пример работы функции IP-MAC-Port Binding в режиме DHCP Snooping. Коммутатор динамически создает запись IMPV после того, как клиент получит IP-адрес от DHCP-сервера.

Настройка коммутатора

- Активизировать функцию IP-MAC-Port Binding в режиме DHCP Snooping глобально на коммутаторе.

```
enable address_binding dhcp_snoop
```

- Указать максимальное количество создаваемых в процессе автоматизации записей IP-MAC на порт.

```
config address_binding dhcp_snoop max_entry ports 1-10 limit 10
```

- Активизировать функцию IP-MAC-Port Binding в режиме DHCP Snooping на соответствующих портах.

```
config address_binding ip_mac ports 1-10 state enable
```

7.3. Аутентификация пользователей 802.1X

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

Сервер аутентификации Remote Authentication in Dial-In User Service (RADIUS) проверяет права доступа каждого клиента, подключаемого к порту коммутатора, прежде чем разрешить доступ к любому из сервисов, предоставляемых коммутатором или локальной сетью.

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

Внимание: протокол 802.1X не поддерживает работу на агрегированных каналах связи.

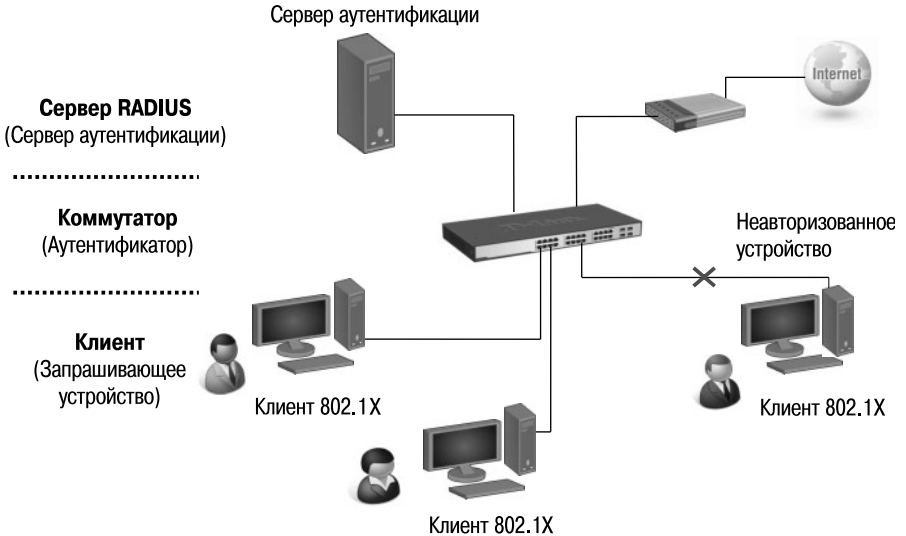


Рис. 7.11. Сеть с аутентификацией 802.1X

7.3.1. Роли устройств в стандарте 802.1X

В стандарте IEEE 802.1X определены следующие три роли, которые могут выполнять устройства:

- клиент (Client/Supplicant);
- аутентификатор (Authenticator);
- сервер аутентификации (Authentication Server).

Клиент (Client/Supplicant) – это рабочая станция, которая запрашивает доступ к локальной сети и сервисам коммутатора и отвечает на запросы от коммутатора. На рабочей станции должно быть установлено клиентское ПО для 802.1X, например, то, которое встроено в ОС Microsoft Windows XP.

Сервер аутентификации (Authentication Server) выполняет фактическую аутентификацию клиента. Он проверяет подлинность клиента и информирует коммутатор, предоставлять или нет клиенту доступ к локальной сети. RADIUS (Remote Authentication Dial-In User Service) работает в модели «клиент-сервер», в которой информация об аутентификации передается между сервером RADIUS и клиентами RADIUS.

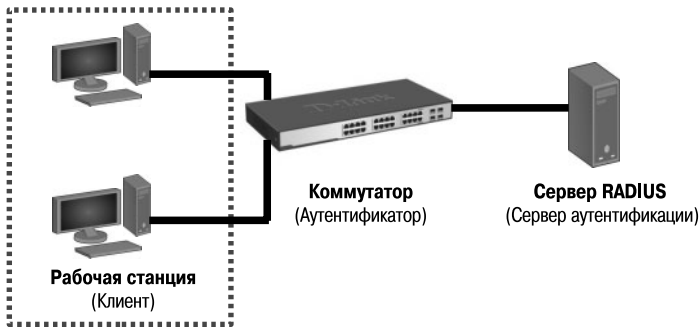


Рис. 7.12. Клиент 802.1X

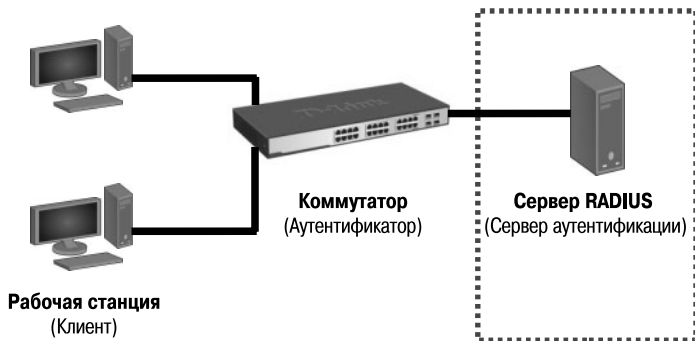


Рис. 7.13. Сервер аутентификации

Аутентификатор (Authenticator) управляет физическим доступом к сети, основываясь на статусе аутентификации клиента. Эту роль выполняет коммутатор. Он работает как посредник (Proxy) между клиентом и сервером аутентификации: получает запрос на проверку подлинности от клиента, проверяет данную информацию при помощи сервера аутентификации и пересылает ответ клиенту. Коммутатор поддерживает клиент RADIUS, который отвечает за инкапсуляцию и деинкапсуляцию кадров EAP и взаимодействие с сервером аутентификации.

Инициировать процесс аутентификации могут или коммутатор, или клиент.

Клиент инициирует аутентификацию, посылая кадр EAPOL-start, который вынуждает коммутатор отправить ему запрос на идентификацию. Когда клиент отправляет EAP-ответ со своей идентификацией, коммутатор начинает играть роль посредника, предающего кадры EAP между

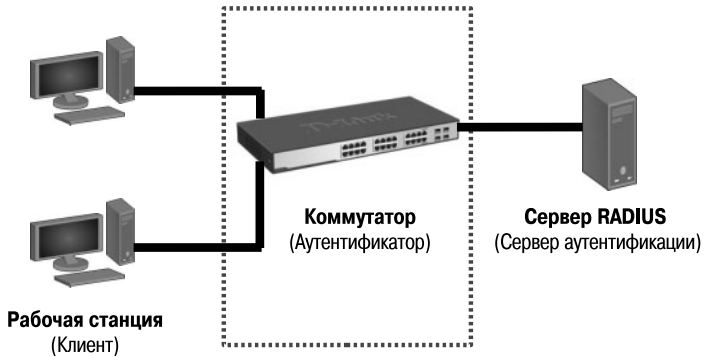


Рис. 7.14. Аутентификатор

клиентом и сервером аутентификации до успешной или неуспешной аутентификации. Если аутентификация завершилась успешно, порт коммутатора становится авторизованным.

Схема обмена EAP-кадрами зависит от используемого метода аутентификации. На рис. 7.15 показана схема обмена, инициируемого клиентом, где сервером RADIUS используется метод аутентификации One-Time-Password (OTP).

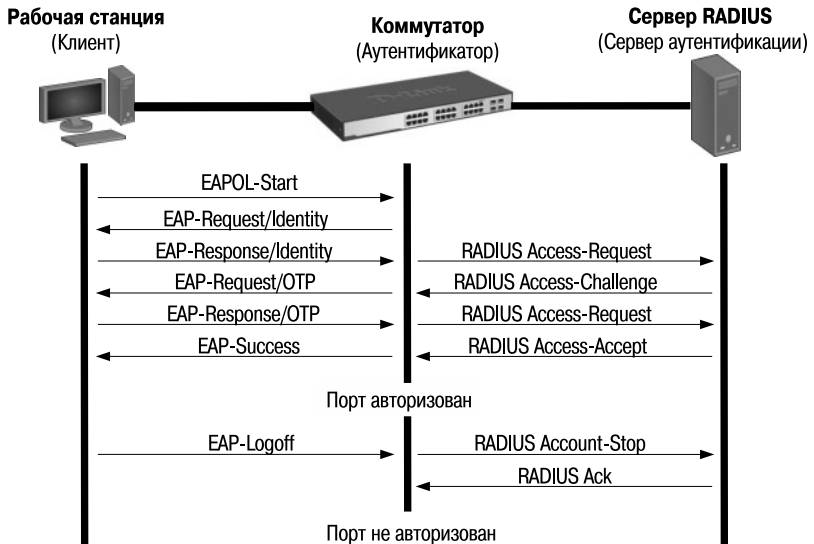


Рис. 7.15. Процесс аутентификации 802.1X

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

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

7.3.2. Port-Based 802.1X

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

Рассмотрим пример настройки функции Port-Based 802.1X для схемы, показанной на рис. 7.16.

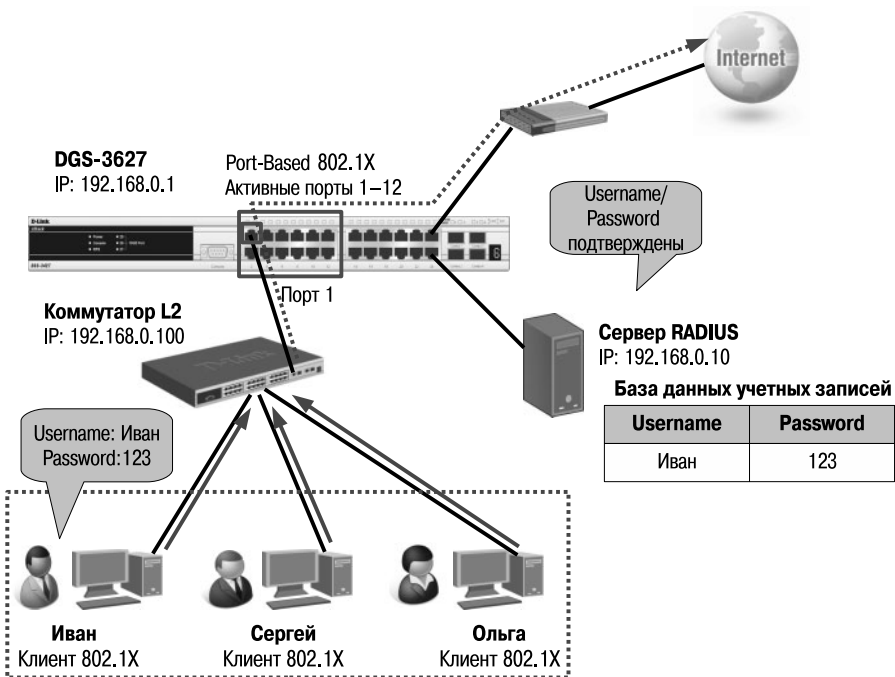


Рис. 7.16. Аутентификация 802.1X на основе портов

Настройка коммутатора DGS-3627

- Настроить проверку подлинности пользователей на сервере RADIUS.

```
config 802.1x auth_protocol radius_eap
```

- Настроить тип аутентификации 802.1X: port-based.

```
config 802.1x auth_mode port_based
```

- Настроить порты, к которым подключаются клиенты в качестве аутентификатора (на uplink-портах к вышестоящим коммутаторам не следует настраивать режим «authenticator»).

```
config 802.1x capability ports 1-12 authenticator
```

- Активизировать функцию 802.1X.

```
enable 802.1x
```

- Настроить параметры сервера RADIUS.

```
config radius add 1 192.168.0.10 key 123456 default
```

7.3.3. MAC-Based 802.1X

В отличие от аутентификации 802.1X на основе портов, где один порт, авторизованный клиентом, остается открытым для всех клиентов, аутентификация 802.1X на основе MAC-адресов – это аутентификация множества клиентов на одном физическом порте коммутатора. При аутентификации 802.1X на основе MAC-адресов (MAC-Based 802.1X) проверяются не только имя пользователя/пароль подключенных к порту коммутатора клиентов, но и их количество. Количество подключаемых клиентов ограничено максимальным количеством MAC-адресов, которое может изучить каждый порт коммутатора. Для функции MAC-Based 802.1X количество изучаемых MAC-адресов указывается в спецификации на устройство. Сервер аутентификации проверяет имя пользователя/пароль, и если информация достоверна, аутентификатор (коммутатор) открывает логическое соединение на основе MAC-адреса клиента. При этом если достигнут предел изученных портом коммутатора MAC-адресов, новый клиент будет заблокирован. Рассмотрим пример настройки функции MAC-Based 802.1X для схемы, показанной на рис. 7.17.

Настройка коммутатора DGS-3627

- Настроить проверку подлинности пользователей на сервере RADIUS.

```
config 802.1x auth_protocol radius_eap
```

- Настроить тип аутентификации 802.1X: MAC-based.

```
config 802.1x auth_mode mac_based
```

- Настроить порты, к которым подключаются клиенты в качестве аутентификатора.

```
config 802.1x capability ports 1-12 authenticator
```

- Активизировать функцию 802.1X.

```
enable 802.1x
```

- Настроить параметры сервера RADIUS.

```
config radius add 1 192.168.0.10 key 123456 default
```

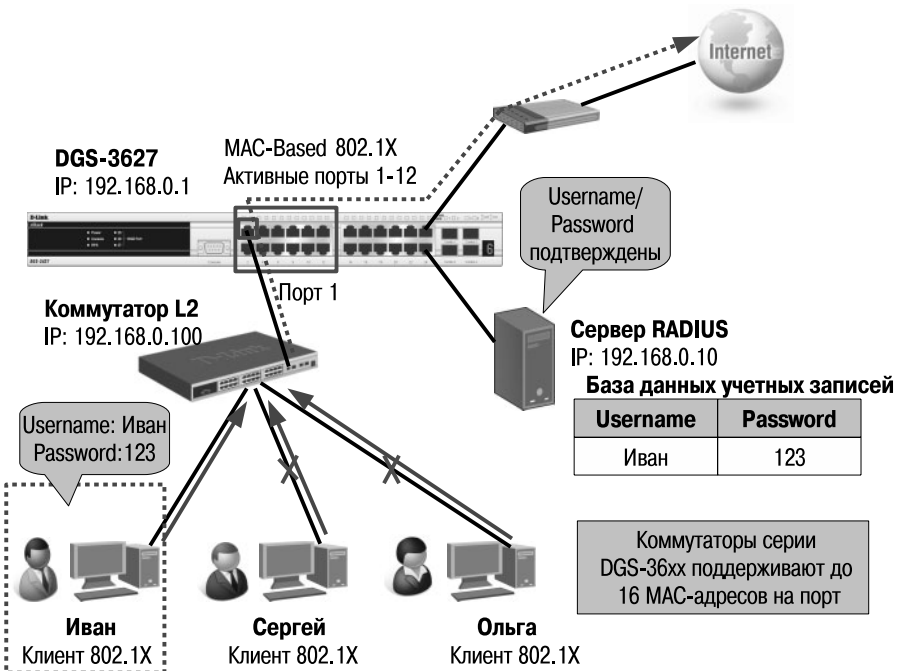


Рис. 7.17. Аутентификация 802.1X на основе MAC-адресов

Следует отметить, что коммутатор может выполнять роль сервера аутентификации. В этом случае база данных учетных записей пользователей будет храниться локально на самом коммутаторе. На рис. 7.18 показана локальная аутентификация 802.1X на основе MAC-адресов.

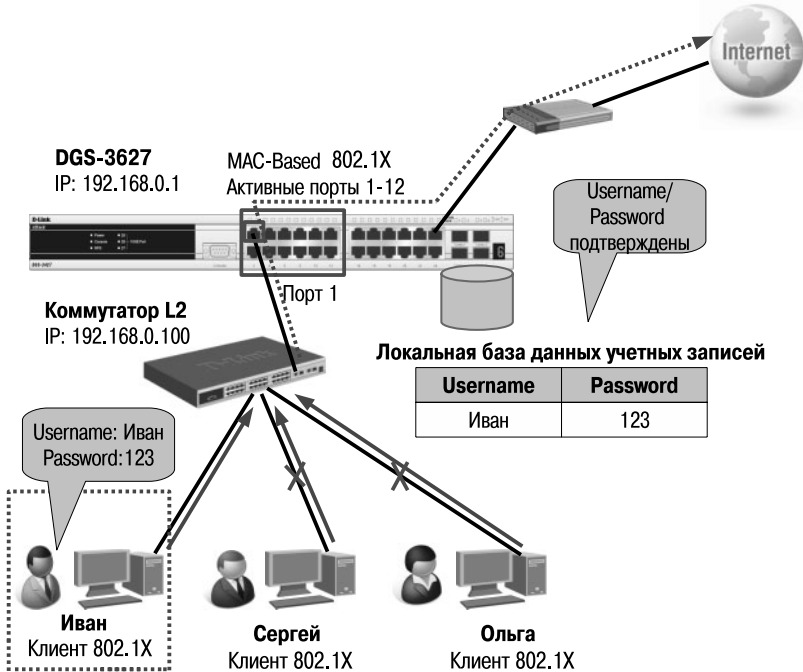


Рис. 7.18. Аутентификация 802.1X на основе MAC-адресов с использованием локальной базы данных учетных записей пользователей

7.3.4. Состояние портов коммутатора

Состояние порта коммутатора определяется тем, получил или не получил клиент право доступа к сети. Первоначально порт находится в *неавторизованном* состоянии. В этом состоянии он запрещает прохождение всего входящего и исходящего трафика за исключением пакетов EAPOL. Когда клиент аутентифицирован, порт переходит в *авторизованное* состояние, позволяя передачу через него любого трафика.

Возможны следующие варианты, когда клиент или коммутатор не поддерживают 802.1X.

Если клиент, который не поддерживает 802.1X, подключается к неавторизованному порту 802.1X, коммутатор посылает клиенту запрос на авторизацию. Поскольку в этом случае клиент не ответит на запрос, порт останется в неавторизованном состоянии и клиент не получит доступ к сети.

Когда клиент с поддержкой 802.1X подключается к порту, на котором не поддерживается протокол 802.1X, он начинает процесс аутентификации, посылая кадр EAPOL-start. Не получив ответа, клиент посылает запрос определенное количество раз. Если после этого ответ не получен, клиент, считая, что порт находится в авторизованном состоянии, начинает передавать данные.

В случае, когда и клиент, и коммутатор поддерживают 802.1X, при успешной аутентификации клиента порт переходит в авторизованное состояние и начинает передавать все кадры клиента. Если в процессе аутентификации возникли ошибки, порт остается в неавторизованном состоянии, но аутентификация может быть восстановлена. Если сервер аутентификации не может быть достигнут, коммутатор может повторно передать запрос. Если от сервера не получен ответ после определенного количества попыток, клиенту будет отказано в доступе к сети из-за ошибок аутентификации. Чтобы вероятность такой ситуации была минимальной, на коммутаторе можно настроить параметры нескольких серверов RADIUS.

Когда клиент завершает сеанс работы, он посылает сообщение EAPOL-logoff, переводящее порт коммутатора в неавторизованное состояние.

Если состояние канала связи порта переходит из активного (up) в неактивное (down) или получен кадр EAPOL-logoff, порт возвращается в неавторизованное состояние.

7.4. 802.1X Guest VLAN

Функция 802.1X Guest VLAN используется для создания гостевой VLAN с ограниченными правами для пользователей, не прошедших аутентификацию. Когда клиент подключается к порту коммутатора с активизированной аутентификацией 802.1X и функцией Guest VLAN, происходит процесс аутентификации (локально или удаленно с использованием сервера RADIUS). В случае успешной аутентификации клиент будет помещен в VLAN назначения (Target VLAN) в соответствии с предустановленным на сервере RADIUS параметром VLAN. Если этот параметр не определен, то клиент будет возвращен в первоначальную VLAN (в соответствии с настройками порта подключения).

В том случае, если клиент не прошел аутентификацию, он помещается в Guest VLAN с ограниченными правами и доступом.

Более наглядно данный процесс приведен на блок-схеме (рис. 7.19).

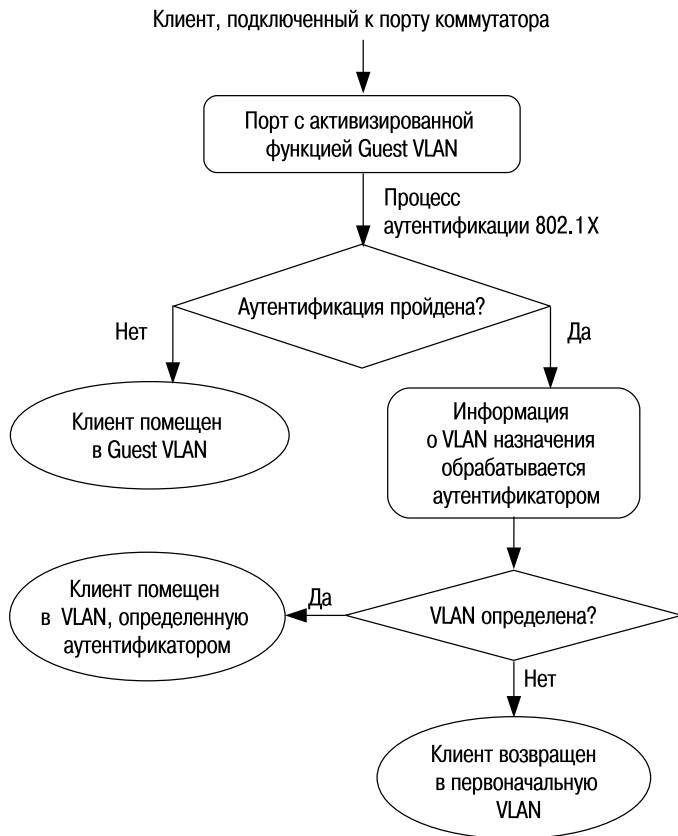


Рис. 7.19. Процесс аутентификации с использованием Guest VLAN

Члены Guest VLAN могут взаимодействовать друг с другом в пределах этой VLAN, даже если они не прошли аутентификацию 802.1X. После успешного прохождения аутентификации член Guest VLAN может быть перемещен в VLAN назначения (Target VLAN) в соответствии с атрибутом VLAN, указанном на сервере RADIUS.

Внимание: функция Guest VLAN поддерживается только для аутентификации 802.1X на базе портов.

Следует отметить, что, используя функцию 802.1X Guest VLAN, клиентам можно предоставлять ряд ограниченных сервисов *до прохождения*

процесса аутентификации 802.1X. Например, клиент может загрузить с сервера и установить необходимое программное обеспечение 802.1X.

Рассмотрим пример, показанный на рис. 7.20. До аутентификации клиент 1 находится в Guest VLAN и имеет доступ к рабочим станциям, расположенным в ней, и общедоступному Web/FTP-серверу. После успешной аутентификации клиента 1 порт коммутатора, к которому он подключен, будет добавлен в VLAN 10 и клиент 1 сможет получить доступ к конфиденциальной информации, хранящейся на FTP-сервере VLAN 10.

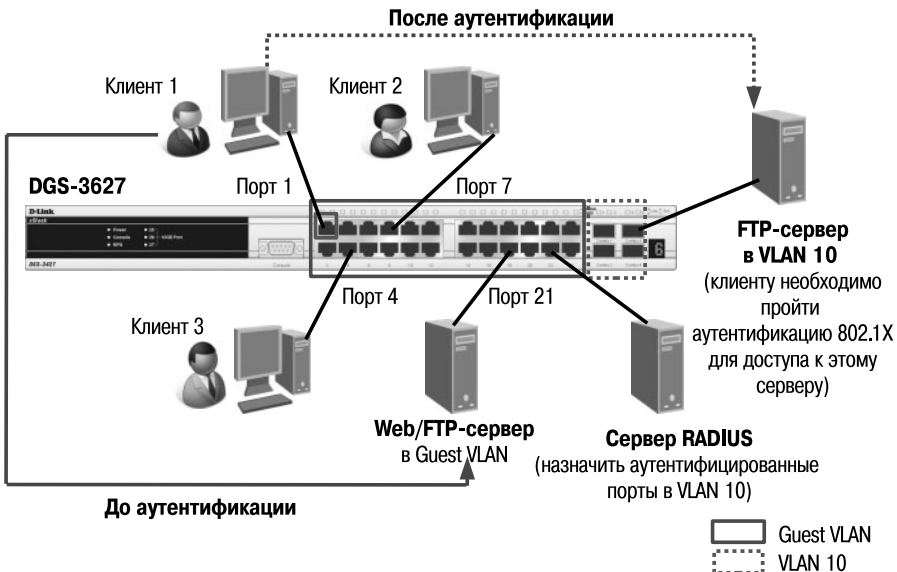


Рис. 7.20. Ресурсы, доступные клиенту до и после аутентификации 802.1X при использовании Guest VLAN

Если клиент не прошел аутентификацию 802.1X, он останется в Guest VLAN с ограниченными правами.

7.4.1. Пример настройки 802.1X Guest VLAN

В качестве примера использования и настройки функции 802.1X Guest VLAN рассмотрим схему сети компании (рис. 7.21), в которой неаутентифицированным пользователям, находящимся в VLAN 10, разрешен доступ в Интернет. После успешной аутентификации пользователей порты, к которым они подключены, будут добавлены в VLAN 20.

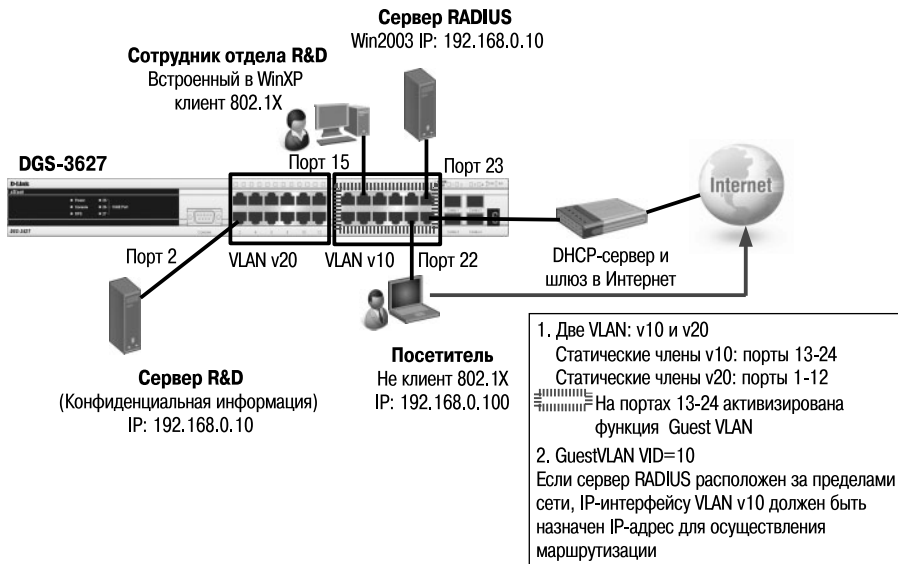


Рис. 7.21. Пример использования 802.1X Guest VLAN

Настройка коммутатора DGS-3627

- Создать на коммутаторе VLAN v10 и v20.

```
config vlan default delete 1-24
create vlan v10 tag 10
config vlan v10 add untagged 13-24
create vlan v20 tag 20
config vlan v20 add untagged 1-12
config ipif System ipaddress 192.168.0.1/24 vlan v10
```

- Активизировать функции 802.1X и Guest VLAN.

```
enable 802.1x
create 802.1x guest_vlan v10
config 802.1x guest_vlan ports 13-24 state enable
```

- Настроить коммутатор в качестве аутентификатора и задать параметры сервера RADIUS.

```
config 802.1x capability ports 13-24 authenticator
config radius add 1 192.168.0.10 key 123456 default
```


Настройка параметров на сервере RADIUS включает установку следующих пользовательских атрибутов:

Tunnel-Medium-Type (65) = 802

Tunnel-Pvt-Group-ID (81) = 20 ← VID

Tunnel-Type (64) = VLAN

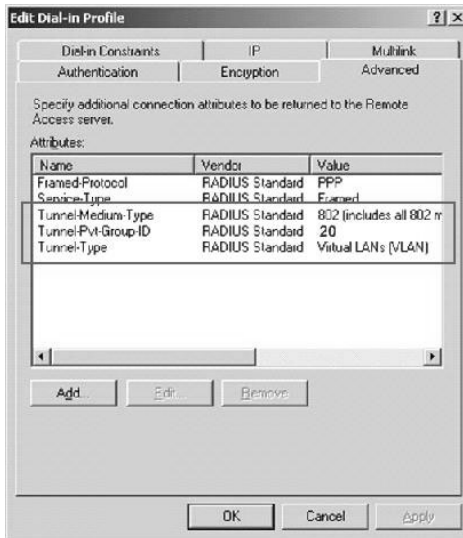


Рис. 7.22. Пользовательские атрибуты на сервере RADIUS

Проверить конфигурацию коммутатора можно с помощью следующих команд:

```
DGS-3627#show 802.1x auth_configuration
```

```
Command: show 802.1x auth_configuration
```

```
802.1X : Enabled
Authentication Mode : Port_based
Authentication Protocol : RADIUS_EAP
```

```
Port number : 1
Capability : None
AdminCr1Dir : Both
OpenCr1Dir : Both
Port Control : Auto
```

```

QuietPeriod      : 60 sec
TxPeriod         : 30 sec
Supp Timeout     : 30 sec
Server Timeout   : 30 sec
MaxReq           : 2 times
ReAuthPeriod     : 3600 sec
ReAuthenticate   : Disabled

```

DGS-3627#**show 802.1x guest_vlan**

Command: show 802.1x guest_vlan

Guest VLAN Setting

```

Guest VLAN : v10
Enable Guest VLAN Ports : 13-24

```

DGS-3627#**show radius**

Command: show radius

Idx	IP Address	Auth-Port	Acct-Port	Status	Key
1	192.168.0.10	1812	1813	Active	123456

Total Entries: 1

Пока клиент, подключенный к порту 22, не прошел аутентификацию, текущая конфигурация VLAN и состояние аутентификации 802.1X на коммутаторе будут следующими:

DGS-3627#**show vlan**

```

VID: 1  VLAN Name   : default
VLAN Type: Static Advertisement : Enabled
Member Ports      : 25-27
Static Ports      : 25-27
Current Tagged Ports :
Current Untagged Ports : 25-27
Static Tagged Ports :
Static Untagged Ports: 25-27
Forbidden Ports   :

```

```

VID: 10 VLAN Name   : v10
VLAN Type: Static Advertisement : Disabled

```

```

Member Ports      : 13-24
Static Ports      : 13-24
Current Tagged Ports :
Current Untagged Ports : 13-24
Static Tagged Ports :
Static Untagged Ports : 13-24
Forbidden Ports   :

```

```

VID: 20 VLAN Name      : v20
VLAN Type: Static Advertisement : Disabled
Member Ports          : 1-12
Static Ports          : 1-12
Current Tagged Ports  :
Current Untagged Ports : 1-12
Static Tagged Ports   :
Static Untagged Ports : 1-12
Forbidden Ports       :

```

```
Total Entries      : 3
```

```
DGS-3627#show 802.1x auth_state
```

```
Command: show 802.1x auth_state
```

Port	Auth PAE State	Backend State	Port State
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	Disconnected	Idle	Unauthorized
14	Disconnected	Idle	Unauthorized

```
.....
```

22	Connecting	Idle	Unauthorized
----	------------	------	--------------

После аутентификации клиента текущие настройки VLAN и состояние аутентификации 802.1X изменятся следующим образом:

```
DGS-3627#show vlan
VID: 1  VLAN Name      : default
VLAN Type: Static Advertisement : Enabled
Member Ports      : 25-27
Static Ports      : 25-27
Current Tagged Ports :
Current Untagged Ports : 25-27
Static Tagged Ports :
Static Untagged Ports : 25-27
Forbidden Ports    :

VID: 10 VLAN Name      : v10
VLAN Type: Static Advertisement : Disabled
Member Ports      : 13-21,23-24
Static Ports      : 13-21,23-24
Current Tagged Ports :
Current Untagged Ports : 13-21,23-24
Static Tagged Ports :
Static Untagged Ports : 13-21,23-24
Forbidden Ports    :

VID: 20 VLAN Name      : v20
VLAN Type: Static Advertisement : Disabled
Member Ports      : 1-12,22
Static Ports      : 1-12,22
Current Tagged Ports :
Current Untagged Ports : 1-12,22
Static Tagged Ports :
Static Untagged Ports : 1-12,22
Forbidden Ports    :

Total Entries : 3
```

```
DGS-3627#show 802.1x auth_state
Command: show 802.1x auth_state
```

Port	Auth PAE State	Backend State	Port State
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized

3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	Disconnected	Idle	Unauthorized
14	Disconnected	Idle	Unauthorized

.....

22	Authenticated	Idle	Authorized
----	---------------	------	------------

7.5. Функции защиты ЦПУ коммутатора

При возникновении в сети многоадресных или ширококвещательных штормов, вызванных неправильной настройкой оборудования или сетевыми атаками, может возникнуть проблема, связанная с перегрузкой ЦПУ коммутатора и его недоступностью для выполнения важных сетевых задач. В коммутаторах D-Link реализованы функции **Safeguard Engine** и **CPU Interface Filtering**, обеспечивающие защиту ЦПУ от обработки нежелательных кадров и повышающие общую отказоустойчивость и доступность сети.

7.5.1. Функция Safeguard Engine

Функция **Safeguard Engine** специально разработана для обеспечения доступности коммутатора в ситуациях, когда в результате наводнения сети вредоносным трафиком его ЦПУ испытывает сильную нагрузку. В результате этого ЦПУ коммутатора не может надлежащим образом обрабатывать пакеты протоколов STP/RSTP/MSTP, IGMP, предоставлять административный доступ через Web-интерфейс, CLI, SNMP и выполнять другие задачи, требующие обработки на ЦПУ. Функция Safeguard Engine позволяет идентифицировать и приоритизировать направляемый для обработки на ЦПУ трафик (например, ARP-широковещание, пакеты с неизвестным IP-адресом назначения и т.д.) с целью отбрасывания нежелательных пакетов для сохранения функциональности коммутатора.

Когда коммутатор с включенной функцией Safeguard Engine получает большое количество пакетов, предназначенных для обработки на ЦПУ и превышающее установленное верхнее пороговое значение *Rising Threshold*, он переходит в режим высокой загрузки (**Exhausted mode**). Находясь в этом режиме, коммутатор может выполнять одно из следующих действий для уменьшения загрузки ЦПУ:

- прекращение получения всех ARP-пакетов и широковещательных IP-пакетов (при работе функции в строгом режиме (*strict mode*));
- ограничение полосы пропускания для получаемых ARP-пакетов и широковещательных IP-пакетов путем ее динамического изменения (при работе функции в нестрогом режиме (*fuzzy mode*)).

При нормализации работы сети и снижении количества нежелательных пакетов до установленного нижнего порогового значения *Falling Threshold* коммутатор выйдет из режима высокой загрузки и механизм Safeguard Engine перестанет функционировать.

Следует отметить, что при переключении коммутатора в режим Exhausted могут возникать следующие побочные эффекты:

- при работе функции Safeguard Engine в строгом режиме будет невозможно осуществлять административный доступ к коммутатору уровня 2, так как этот режим предусматривает отбрасывание всех ARP-запросов, поступающих на интерфейс ЦПУ.

Для решения этой проблемы в статической ARP-таблице управляющей рабочей станции можно создать запись, связывающую MAC-адрес коммутатора с IP-адресом его интерфейса управления. В этом случае рабочей станции не потребуется отправлять ARP-запрос коммутатору;

- при работе функции Safeguard Engine в строгом режиме на коммутаторе уровня 3, помимо невозможности административного доступа, также может быть нарушена маршрутизация между подключенными к нему подсетями, т.к. будут отбрасываться ARP-запросы, поступающие не только на интерфейс ЦПУ, но и на IP-интерфейсы коммутатора.

Преимуществом нестрогого режима работы функции Safeguard Engine является то, что в нем не просто отбрасываются все ARP-пакеты или широковещательные IP-пакеты, а динамически изменяется полоса пропускания для них. Таким образом, даже при серьезной вирусной эпидемии, коммутатор уровня 2/3 будет доступен по управлению, а коммутатор уровня 3, в том числе, сможет обеспечивать маршрутизацию между подсетями.

7.5.1.1. Пример настройки функции Safeguard Engine

В качестве примера использования функции Safeguard Engine рассмотрим ситуацию, когда одна из рабочих станций, подключенных к ком-

мутатору, постоянно рассылает ARP-пакеты с очень высокой скоростью. Загрузка ЦПУ коммутатора при этом меняется от нормальной до 90%. При устранении причины, вызвавшей лавинную генерацию ARP-пакетов на рабочей станции, загрузка ЦПУ снизится до нормы.

Для защиты ЦПУ от подобных ситуаций и снижения его загрузки на коммутаторе можно настроить функцию Safeguard Engine.

Настройка коммутатора

- Активируйте функцию Safeguard Engine.

```
config safeguard_engine state enable
```

- Задайте нижнее и верхнее пороговые значения (указываются значения в процентах от загрузки ЦПУ), при которых будет происходить переключение между нормальным режимом работы и режимом Exhausted. Укажите режим работы функции.

```
config safeguard_engine utilization rising 40 falling 25 mode strict
```

- Активируйте функцию Safeguard Engine.

```
config safeguard_engine state enable
```

- Задайте нижнее и верхнее пороговые значения (указываются значения в процентах от загрузки ЦПУ), при которых будет происходить переключение между нормальным режимом работы и режимом Exhausted. Укажите режим работы функции.

```
config safeguard_engine utilization rising 40 falling 25 mode strict
```

7.5.2. Функция CPU Interface Filtering

Стандартные списки управления доступом выполняют фильтрацию трафика на аппаратном уровне и не могут фильтровать потоки данных, предназначенные для обработки на ЦПУ, например, сообщения ICMP, отправляемые на IP-адрес управления коммутатором. В случае возникновения большого количества таких пакетов производительность коммутатора может сильно снизиться из-за высокой загрузки ЦПУ.

Функция **CPU Interface Filtering**, поддерживаемая на старших моделях коммутаторов D-Link, является еще одним решением, позволяющим

ограничивать пакеты, поступающие для обработки на ЦПУ, путем фильтрации нежелательного трафика на аппаратном уровне. По своей сути функция CPU Interface Filtering представляет собой списки управления доступом к интерфейсу ЦПУ и обладает аналогичными стандартным ACL принципами работы и конфигурации.

7.5.2.1 Пример настройки функции CPU Interface Filtering

В качестве примера рассмотрим задачу, в которой необходимо настроить коммутатор таким образом, чтобы пакеты ICMP, передаваемые компьютером ПК 2, не отправлялись на обработку на ЦПУ, но при этом ПК 2 мог передавать данные другим устройствам, например ПК 1.

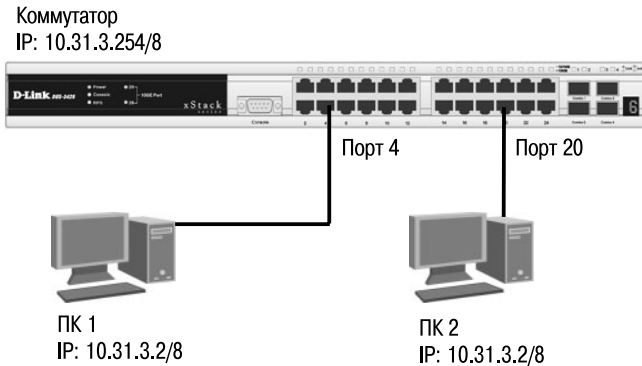


Рис. 7.23. Схема сети

Настройка коммутатора

- Активизируйте функцию CPU Interface Filtering глобально на коммутаторе.

```
enable cpu_interface_filtering
```

- Создайте профиль доступа для интерфейса ЦПУ.

```
create cpu access_profile ip source_ip_mask 255.255.255.128 icmp  
profile_id 1
```

- Создайте правило для профиля доступа.

```
config cpu access_profile profile_id 1 add access_id 1 ip  
source_ip 10.31.3.2 icmp deny
```


Лекция 8. 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 *однадресной 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, с использованием широковещательного IP-адреса.

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 IP, 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 аудиотрансляции 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 перегрузка канала связи.

Одним из недостатков 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.

8.1. Адресация многоадресной IP-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, присоединившихся к этой группе и желающих получать адресованный ей трафик.

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

Таблица 8.1. Назначенные IANA диапазоны адресов многоадресной рассылки

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

233.0.0.0 – 233.251.255.255	Блок GLOP (GLOP Block). Этот диапазон адресов зарезервирован для использования в качестве адресов, статически определяемых организациями с зарезервированным номером автономной системы
233.252.0.0 – 233.255.255.255	Блок AD-НОС III (AD-НОС Block III). Этот диапазон известен как расширенный GLOP (EGLOP, Extended GLOP)
234.0.0.0 – 238.255.255.255	Зарезервировано
239.0.0.0 – 239.255.255.255	Блок административно ограниченных адресов (Administratively Scoped Block). Эти адреса могут локально использоваться внутри домена

Использование групповых IP-адресов из блока с административным ограничением наиболее удобно при организации многоадресной рассылки в локальной сети предприятия или организации. В соответствии с RFC 2365 «Administratively Scoped IP Multicast» подсеть 239.192.0.0/14 выделена для частного использования и определена как локальная область организации IPv4.

Формат IP-адреса класса D показан на рис. 8.1. Первые 4 бита адреса всегда равны 1110, остальные 28 бит используются для идентификации конкретной группы получателей многоадресного трафика.

Класс D	1	1	1	0	Multicast ID
	Первые 4 бита				

Рис. 8.1. Формат IP-адреса класса D

8.2. MAC-адреса групповой рассылки

Как правило, рабочие станции локальной сети получают и обрабатывают кадры только в случае совпадения MAC-адреса назначения кадра с их собственным MAC-адресом или если MAC-адрес – широковещательный. При использовании многоадресной рассылки необходимо, чтобы несколько узлов могли получать поток данных с общим MAC-адресом. Одним из способов, позволяющих достичь этого, является преобразование группового IP-адреса в MAC-адрес.

В спецификации IEEE 802.3 определена возможность указания типа MAC-адреса назначения: индивидуальный или групповой (широковещательный или многоадресный). Для этого используется первый бит поля

посылают запросы, чтобы определить, какие группы активны или не активны в данной сети.

В общем случае протокол IGMP определяет следующие типы сообщений:

- запрос о принадлежности к группе (Membership Query);
- ответ о принадлежности к группе (Membership Report);
- сообщение о выходе из группы (Leave Group Message).

В настоящее время существуют три версии протокола IGMP:

- IGMP версии 1 (IGMP v1, описан в RFC 1112);
- IGMP версии 2 (IGMP v2, описан в RFC 2236);
- IGMP версии 3 (IGMP v3, описан в RFC 3376).

Протокол IGMP используется только в сетях с адресацией IPv4, так как в сетях с адресацией IPv6 групповая передача пакетов реализована по-другому.

8.4. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping)

Когда коммутатор 2-го уровня получает многоадресный трафик, он начинает передавать кадры через все порты, т.к. не находит записи о MAC-адресе в своей таблице коммутации. Это противоречит основному назначению коммутатора, которое заключается в ограничении трафика и передаче его только тем портам, к которым подключены пользователи.

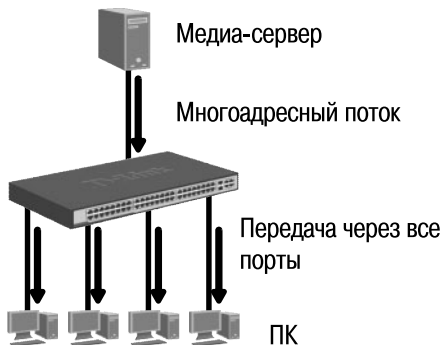


Рис. 8.3. Передача многоадресного трафика без поддержки управления им на коммутаторе

Управление многоадресной рассылкой на коммутаторе 2-го уровня может быть выполнено двумя способами.

Первый способ заключается в создании статических таблиц коммутации для портов, к которым не подключены подписчики многоадресных групп. Это позволяет ограничить многоадресный трафик и передавать его только через те порты, к которым подключены узлы-подписчики. Однако этот способ не позволяет динамически отслеживать добавление или исключение членов из многоадресной группы.

Вторым способом, позволяющим решить проблему лавинной передачи (flooding) многоадресных пакетов и динамически отслеживать состояние подписки узлов, является функция **IGMP Snooping** (IGMP-прослушивание).

IGMP Snooping — это функция второго уровня модели OSI, которая позволяет коммутаторам изучать членов многоадресных групп, подключенных к его портам, прослушивая IGMP-сообщения (запросы и ответы), передаваемые между узлами-подписчиками и маршрутизаторами (коммутаторами уровня 3) сети.

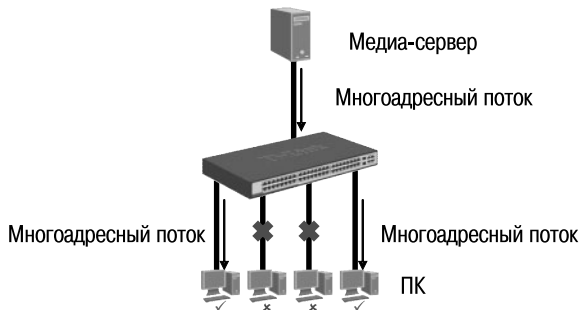


Рис. 8.4. Передача многоадресного трафика с поддержкой IGMP Snooping

Когда узел, подключенный к коммутатору, хочет вступить в многоадресную группу или отвечает на IGMP-запрос, полученный от маршрутизатора (коммутатора уровня 3) многоадресной рассылки, он отправляет IGMP-ответ, в котором указан адрес многоадресной группы. Коммутатор просматривает информацию в IGMP-ответе и создает в своей ассоциативной таблице коммутации IGMP Snooping запись для этой группы (если она не существует). Эта запись связывает порт, к которому подключен узел-подписчик, порт, к которому подключен маршрутизатор (коммутатор уровня 3) многоадресной рассылки, и MAC-адрес многоадресной группы.

Если коммутатор получает IGMP-ответ для этой же группы от другого узла данной VLAN, то он добавляет номер порта в уже существующую запись ассоциативной таблицы коммутации IGMP Snooping.

Формируя таблицу коммутации многоадресной рассылки, коммутатор осуществляет передачу многоадресного трафика только тем узлам, которые в нем заинтересованы.

Рассмотрим пример работы функции IGMP Snooping для сети, показанной на рис. 8.5.

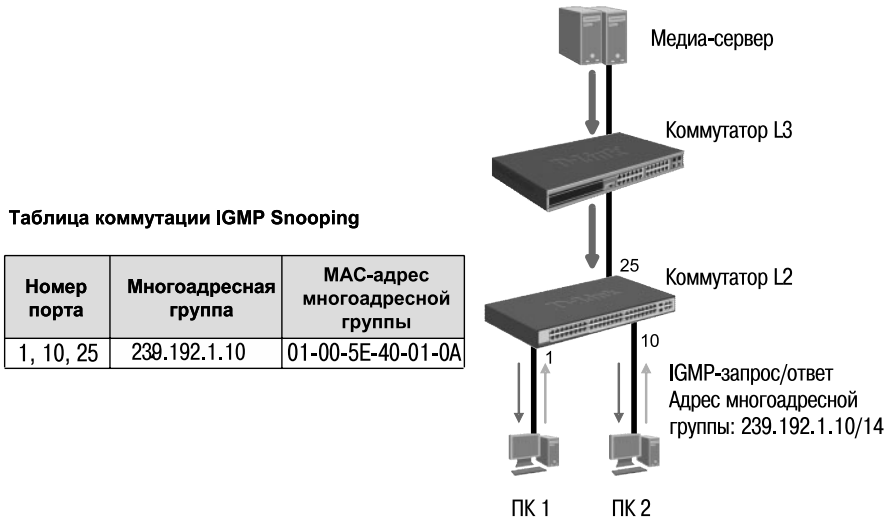


Рис. 8.5. Процесс создания таблицы коммутации IGMP Snooping

Коммутатор L3 отправляет IGMP-запрос о принадлежности к группе коммутатору L2, который рассылает его через все порты, за исключением порта-получателя. ПК 1 хочет вступить в многоадресную группу 239.192.1.10 и отправляет IGMP-ответ на адрес группы, указывая в качестве многоадресного MAC-адреса назначения 0x01-00-5E-40-01-0A. Процессор коммутатора L2 анализирует IGMP-ответ и создает в ассоциативной таблице коммутации IGMP Snooping (в первоначальный момент времени она пуста) запись для MAC-адреса 0x01-00-5E-40-01-0A, эквивалентного групповому адресу 239.192.1.10. Также в эту запись заносится информация о портах, к которым подключены ПК 1 и коммутатор L3.

ПК 2 хочет вступить в многоадресную группу 239.192.1.10 и отправляет IGMP-ответ на адрес группы, не дожидаясь получения очередного IGMP-запроса. Коммутатор L2 анализирует IGMP-ответ и добавляет порт 10, к которому подключен ПК 2, в уже существующую запись для MAC-адреса 0x01-00-5E-40-01-0A.

В результате порты 1, 10 и 25 ассоциированы с многоадресным MAC-адресом 0x01-00-5E-40-01-0A.

Когда коммутатор получает IGMP-сообщение о выходе узла из группы, он удаляет номер порта, к которому подключен этот узел, из соответствующей записи таблицы коммутации IGMP Snooping.

Функция IGMP Snooping сильно загружает центральный процессор и может снизить производительность коммутатора. Поэтому в коммутаторах обычно используются специализированные микросхемы ASIC, которые проверяют IGMP-сообщения на аппаратном уровне.

8.4.1. Пример настройки IGMP Snooping

Рассмотрим пример настройки функции IGMP Snooping на коммутаторах D-Link. На рис. 8.6 показана схема сети, в которой реализован сервис многоадресной рассылки. Клиенты, среди которых имеются подписчики многоадресной рассылки, подключены к коммутаторам второго уровня.

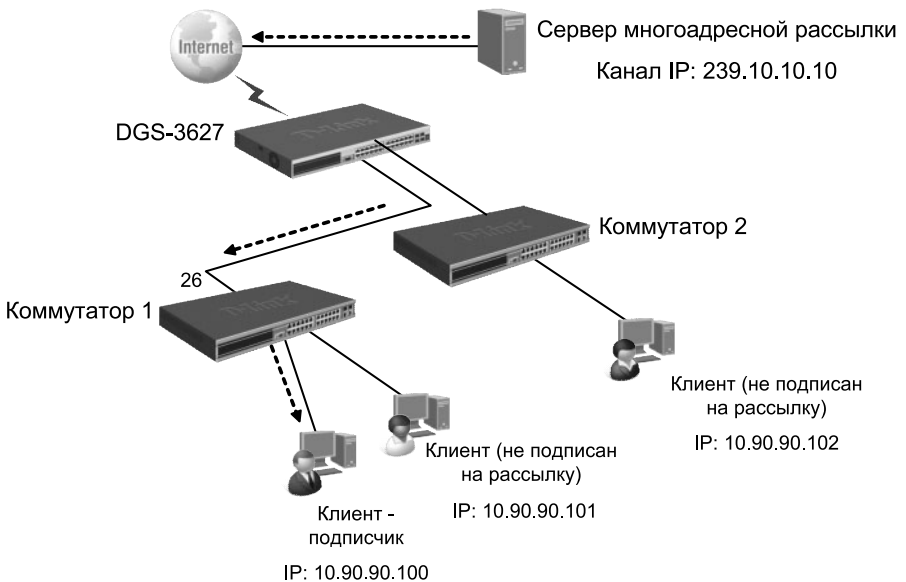


Рис. 8.6. Схема сети

Настройка коммутатора 1

- Активизировать функцию IGMP Snooping глобально на коммутаторе.

```
enable igmp_snooping
```


- Активизировать функцию IGMP Snooping в указанной VLAN (в данном примере VLAN по умолчанию).

```
config igmp_snooping vlan default state enable
```

- Включить фильтрацию многоадресного трафика, чтобы избежать его передачи узлам, не являющимся подписчиками многоадресной рассылки.

```
config multicast vlan_filtering_mode vlan default filter_unregistered_groups
```

8.5. Функция IGMP Snooping Fast Leave

Функция IGMP Snooping Fast Leave, активизированная на коммутаторе, позволяет мгновенно исключить порт из таблицы коммутации IGMP Snooping при получении им сообщения о выходе из группы. Это позволяет прекратить передачу по сети ненужных потоков данных и более эффективно использовать полосу пропускания. Функция IGMP Snooping Fast Leave полезна в приложениях IPTV, т.к. благодаря ей можно уменьшить время отклика, когда пользователи переключаются между телевизионными каналами.

Следует отметить, что порт будет удален из таблицы коммутации IGMP Snooping только в том случае, если к нему больше не подключено ни одного узла-подписчика.

8.5.1. Пример настройки IGMP Snooping Fast Leave

Рассмотрим пример настройки функции IGMP Snooping Fast Leave. На рис. 8.7 приведена схема сети, в которой на коммутаторе 2 активизирована функция IGMP Snooping Fast Leave. Все порты коммутатора 2 находятся в VLAN по умолчанию (Default VLAN). К одному из портов коммутатора подключен узел-подписчик многоадресной рассылки.

Настройка коммутатора 2

- Активизировать функцию IGMP Snooping глобально на коммутаторе и в указанной VLAN (в данном примере VLAN по умолчанию). Включить фильтрацию многоадресного трафика.

```
enable igmp_snooping  
config igmp_snooping vlan default state enable
```



Рис. 8.7. Схема сети

```
config multicast vlan_filtering_mode vlan default  
filter_unregistered_groups
```

- Активизировать функцию IGMP Snooping Fast Leave в указанной VLAN.

```
config igmp_snooping vlan default fast_leave enable
```

Лекция 9. Функции управления коммутаторами

9.1. Управление множеством коммутаторов

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

- физическое стекирование коммутаторов;
- виртуальное стекирование коммутаторов.

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

9.1.1. Объединение коммутаторов в физический стек

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

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

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

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

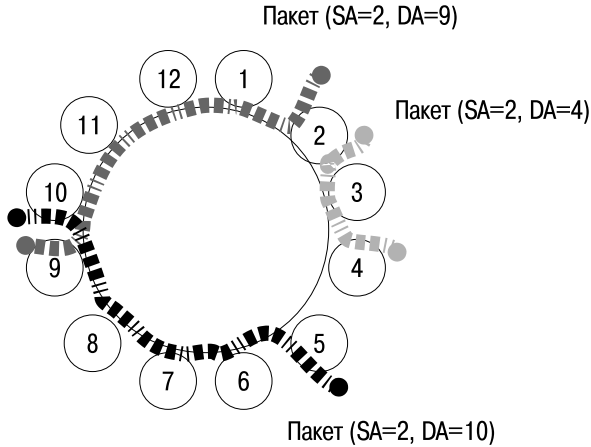


Рис. 9.1. Пример выбора оптимального пути передачи пакета в стеке типа «кольцо»

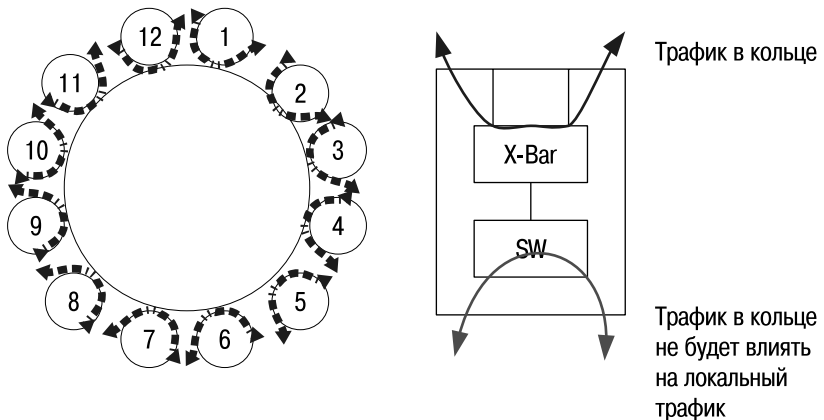


Рис. 9.2. Потоки трафика в стеке

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

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

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

замене, добавлении и удалении коммутаторов, а также позволяет автоматически назначать нового мастера-коммутатора в случае неработоспособности текущего и автоматически восстанавливать работу стека;

- механизм *Cross Device Trunking (CDT)* позволяет объединять несколько физических портов разных коммутаторов стека в один агрегированный канал с повышенной полосой пропускания. При этом такая логическая магистраль будет продолжать функционирование, даже если какой-либо порт или коммутатор выйдут из строя;
- технология *SmartRoute* позволяет копировать таблицы коммутации 3-го уровня, хранимые на мастере-коммутаторе, на все другие устройства стека (в том случае, если стек построен на коммутаторах L3). Благодаря этому каждый коммутатор стека может маршрутизировать трафик локально, не пересылая его на мастер-коммутатор, что уменьшает потребление полосы пропускания между коммутаторами и повышает отказоустойчивость стека.

Роли коммутаторов стека

Каждому коммутатору стека присваивается определенная роль. Эти роли могут быть вручную настроены администратором сети на каждом коммутаторе или определены стеком автоматически. Существуют 3 роли, которые могут быть назначены коммутаторам стека.

Основной мастер (*Primary Master*) – основной мастер-коммутатор является ведущим устройством стека и единой точкой управления. Он следит за нормальной работой стека, топологией, назначает идентификаторы устройствам стека (Vox ID), синхронизирует конфигурации и передает команды другим коммутаторам. Роль основного мастера может быть присвоена коммутатору вручную, путем назначения наивысшего приоритета администратором сети, или определена автоматически в процессе выборов.

Резервный мастер (*Backup Master*) – резервный мастер дублирует основной мастер-коммутатор и в случае его выхода из строя берет на себя функции основного мастера. Резервный мастер-коммутатор следит за состоянием соседних коммутаторов стека, основного мастера-коммутатора и выполняет его команды. Роль резервного мастера может быть назначена коммутатору вручную, путем присвоения ему второго по значению наивысшего приоритета до физического объединения устройств в стек или автоматически во время выборов.

Ведомый (*Slave*) – ведомыми являются все остальные коммутаторы стека. Ведомые коммутаторы выполняют операции, требуемые основным мастером, следят за состоянием соседних коммутаторов стека и топологи-

ей, следуют командам резервного мастера, когда он становится основным. Ведомые коммутаторы принимают участие в процессе выбора нового резервного мастера, в случае если:

- резервный мастер стал основным мастером;
- резервный мастер вышел из строя или удален из стека;
- оба, и основной, и резервный мастер, вышли из строя или удалены из стека.

Выборы основного мастера-коммутатора стека

После того как коммутаторы будут объединены в стек, каждое устройство начнет собирать информацию (такую как приоритет, MAC-адрес) о соседних коммутаторах и сохранять ее во временной базе данных топологии стека (self temp stacking topology database). Далее коммутаторы приступят к выбору основного мастера-коммутатора стека. Основным мастером выбирается путем сравнения приоритетов (по умолчанию приоритет 32) и MAC-адресов коммутаторов стека.

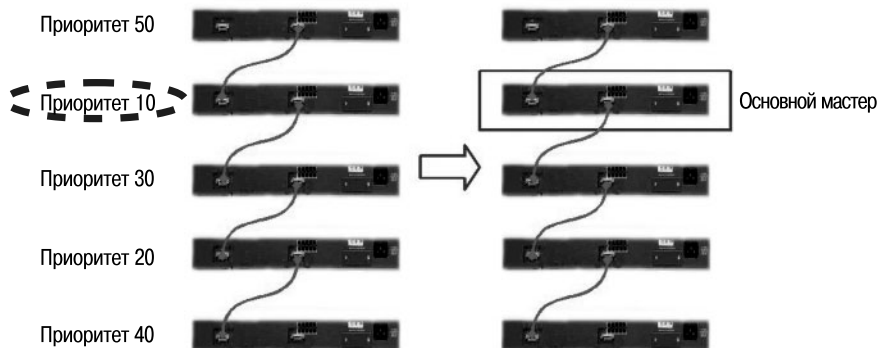


Рис. 9.3. Процесс выбора основного мастера на основании приоритетов

Основным мастером становится коммутатор с наименьшим значением приоритета. Если приоритеты коммутаторов равны, то будет выбран коммутатор с наименьшим значением MAC-адреса.

После выбора основного мастера, начинается процесс выбора резервного мастера из оставшихся устройств стека по аналогичному сценарию.

Как только выбраны основной и резервный мастер, всем коммутаторам стека будут присвоены порядковые номера Vox ID. Если в настройках коммутатора параметр Vox ID установлен в Auto, основной мастер назначит

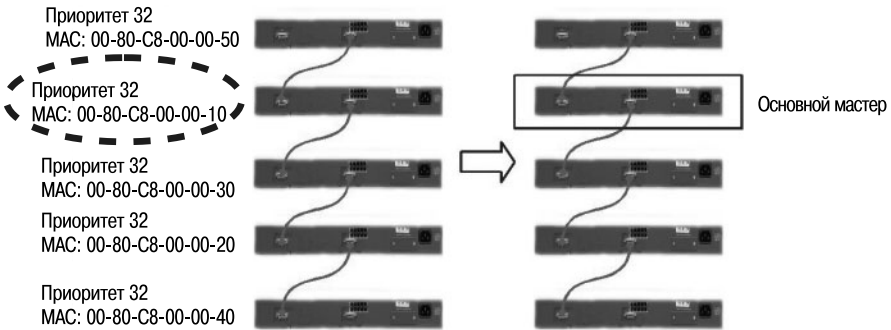


Рис. 9.4. Процесс выбора основного мастера на основании MAC-адресов при равном значении приоритетов

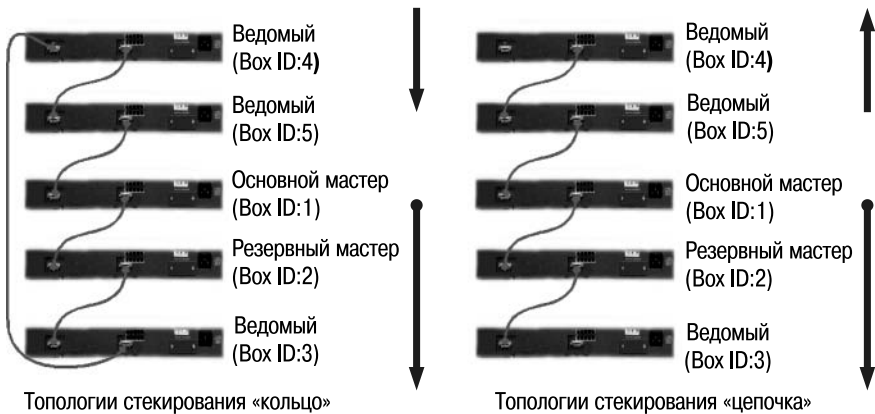


Рис. 9.5. Назначение порядковых номеров в автоматическом режиме

каждому устройству стека порядковый номер в соответствии с правилами автоматического назначения номеров (основному мастеру в автоматическом режиме присваивается номер 1). Эта информация о топологии будет разослана всем устройствам стека.

Когда значение параметра Vox ID установлено в статический режим (STATIC), присвоение порядковых номеров коммутаторам будет осуществляться вручную администратором сети. При этом настройки любого коммутатора с новым, отличным от предыдущего, значением Vox ID будут возвращены к заводским настройкам по умолчанию. Если в процессе

изучения топологии стека возник конфликт идентификационных номеров коммутаторов, устройства с одинаковыми Vох ID переводятся в автономный режим работы. Все порты для стекирования отключаются, и система выдает сообщение о конфликте Vох ID.

Следует отметить, что основной мастер-коммутатор и резервный мастер-коммутатор не имеют фиксированных номеров, т.е. основному мастеру может быть присвоен Vох ID, отличный от 1.

При работе в смешанном режиме, когда на коммутаторах используется автоматическое и статическое назначение номеров, действует следующее правило:

- 1) сначала основной мастер собирает информацию о Vох ID всех коммутаторов стека;
- 2) выполняется проверка на наличие конфликтов Vох ID;
- 3) если конфликт не обнаружен, то основной мастер сначала присвоит идентификационные номера устройствам, работающим в статическом режиме, а затем устройствам, работающим в автоматическом режиме.

Изменение топологии стека

В случае добавления или удаления коммутатора(-ов) из стека или изменения топологии протокол стекирования, реализованный в устройствах, быстро обнаружит изменения и синхронизирует информацию о новой топологии стека.

Когда новый коммутатор добавляется в работающий стек, ему присваивается роль ведомого или резервного мастера, в зависимости от значений приоритета и MAC-адреса.

Если в стек добавляется только одно устройство, то процесс выбора основного мастера не запускается.

При удалении одного или нескольких коммутаторов из работающего стека оставшиеся коммутаторы удаляют информацию о выбывших устройствах из своих баз данных топологии стека.

При удалении резервного мастера запускается процесс выборов нового резервного мастера. Этот процесс также запускается при удалении или выходе из строя основного мастера, т.к. резервный мастер становится в этом случае основным. При этом для минимизации нарушения работы сети новому основному мастеру присваивается тот же IP-адрес, который был у предыдущего (Vох ID не меняется).

При удалении обоих мастеров (основного и резервного) мгновенно инициируется процесс выбора нового основного и резервного мастеров из оставшихся коммутаторов стека.

Когда происходит изменение топологии стека – с линейной на кольцевую или наоборот, состояние устройств не изменяется.

Пример настройки стекирования

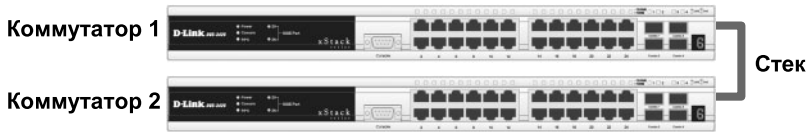


Рис. 9.6. Коммутаторы, объединенные в стек

В качестве примера приведем настройку двух коммутаторов, объединенных в физический стек.

Настройка коммутатора 1

```
config stacking mode enable
config box_priority current_box_id 1 priority 1
```

Настройка коммутатора 2

```
config stacking mode enable
config box_priority current_box_id 1 new_box_id 2
config box_priority current_box_id 2 priority 2
```

9.1.2. Виртуальный стек.

Технология Single IP Management (SIM)

Технология **Single IP Management (SIM)** является простым и удобным способом сетевого управления. Она разработана для управления группой коммутаторов, называемых *SIM-группой*, как единым устройством. При этом для управления SIM-группой требуется только один IP-адрес, который назначается выделенному коммутатору группы (Commander switch).

Технология SIM позволяет:

- устранить ограничения на модели коммутаторов, объединяемых в стек;
- уменьшить количество управляющих IP-адресов в сети;
- устранить необходимость использования специализированных модулей и кабелей, предназначенных для стекирования; преодолеть ограничения, связанные с длиной кабелей в стеке.

В отличие от стеков, построенных с использованием традиционных методов стекирования, виртуальный стек на основе технологии

SIM не ограничивается 6-ю или 12-ю коммутаторами. В SIM-группу может входить до 32-х коммутаторов любых моделей, поддерживающих функции Single IP Management. Это означает, что виртуальный стек может включать коммутаторы разного типа, от недорогих коммутаторов 2-го уровня до высокопроизводительных коммутаторов на основе шасси (для ядра сети).

Объединение коммутаторов в SIM-группу не требует использования специальных соединительных кабелей. Трафик, передаваемый между устройствами стека, проходит через интерфейсы Fast Ethernet, Gigabit Ethernet или 10 Gigabit Ethernet по обычным медным или оптическим кабелям. Отказ от использования специализированных стекирующих кабелей позволяет преодолеть ограничения, связанные с их длиной. Устройства SIM-группы могут быть подключены друг к другу через промежуточные устройства, не поддерживающие технологию SIM. Объединение коммутаторов в SIM-группу не влияет на их нормальное функционирование.

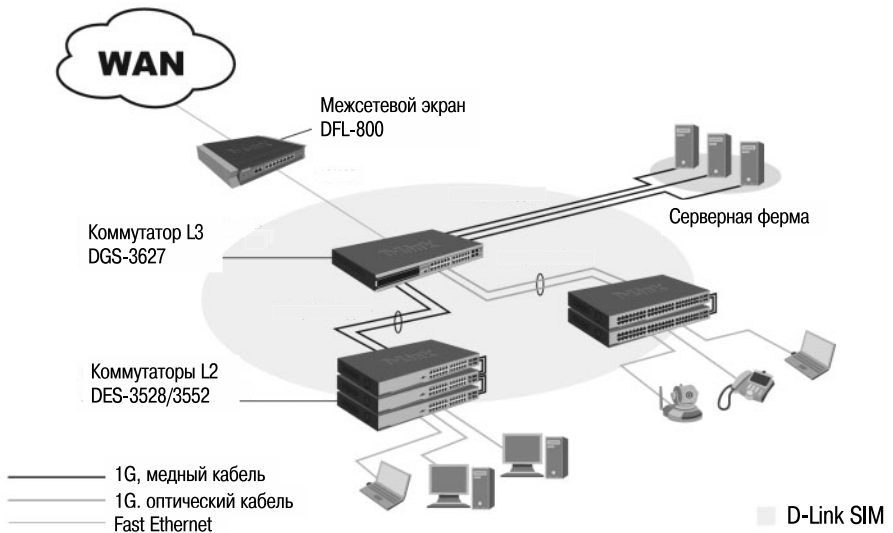


Рис. 9.7. Технология SIM

Внимание: SIM является дополнительной функцией коммутаторов и может быть активизирована или отключена через Web-интерфейс или CLI. По умолчанию эта функция на коммутаторе отключена.

Технология SIM предусматривает три роли, которые могут быть назначены коммутаторам группы:

- **Commander Switch (CS)** – это коммутатор, который вручную настраивается администратором сети как управляющее устройство SIM-группы. В SIM-группе может быть только один Commander Switch. CS обладает следующими характеристиками:
 - ♦ ему присвоен IP-адрес;
 - ♦ он не является Commander Switch или Member Switch другой SIM-группы;
 - ♦ он подключен к коммутаторам Member Switch через управляющую VLAN (VLAN, к которой привязан управляющий интерфейс коммутатора System. По умолчанию управляющей VLAN является default VLAN);
- **Member Switch (MS)** – коммутатор, который вступил в SIM-группу и доступен через Commander Switch. Member Switch обладает следующими характеристиками:
 - ♦ он не является Commander Switch или Member Switch другой SIM-группы;
 - ♦ он подключен к Commander Switch через управляющую VLAN;
- **Candidate Switch (CaS)** – это коммутатор, который готов вступить в SIM-группу (стать Member Switch), используя либо автоматический метод, либо ручную настройку. Коммутатор, настроенный как Candidate Switch, не является членом SIM-группы. Он обладает следующими характеристиками:
 - ♦ он не является Commander Switch или Member Switch другой SIM-группы;
 - ♦ он подключен к Commander Switch через управляющую VLAN.

Все коммутаторы, объединенные в одну SIM-группу, должны принадлежать одной IP-подсети (широковещательному домену). В пределах одной подсети может быть создано несколько SIM-групп, но при этом каждый коммутатор должен принадлежать только одной SIM-группе. Каждая группа может содержать до 32 коммутаторов (от 0 до 31), включая Commander Switch (его номер 0). Если в сети настроено несколько VLAN, SIM-группа будет использовать только управляющую VLAN любого коммутатора.

По умолчанию после активизации функции SIM всем коммутаторам присваивается роль «Candidate Switch». Это означает, что они смогут стать членами SIM-группы (Member Switch), как только получат запрос от Commander Switch.

После того, как одному из коммутаторов группы была присвоена роль «Commander Switch», он начинает формировать SIM-группу, добавляя в нее новых членов. Для этого Commander Switch просматривает список канди-

датов (Candidate Switch) и отправляет им периодические запросы. Кандидат отправляет Commander Switch ответ, содержащий информацию о нем, что позволяет ему стать членом SIM-группы. Если коммутатор-кандидат имел ранее сконфигурированный пароль, он не сможет стать членом группы до тех пор, пока не будут введены его аутентификационные данные.

Можно добавлять членов группы, используя Web-интерфейс. Функционал SIM встроен в Web-интерфейс управления коммутаторов и не требует установки дополнительного ПО.

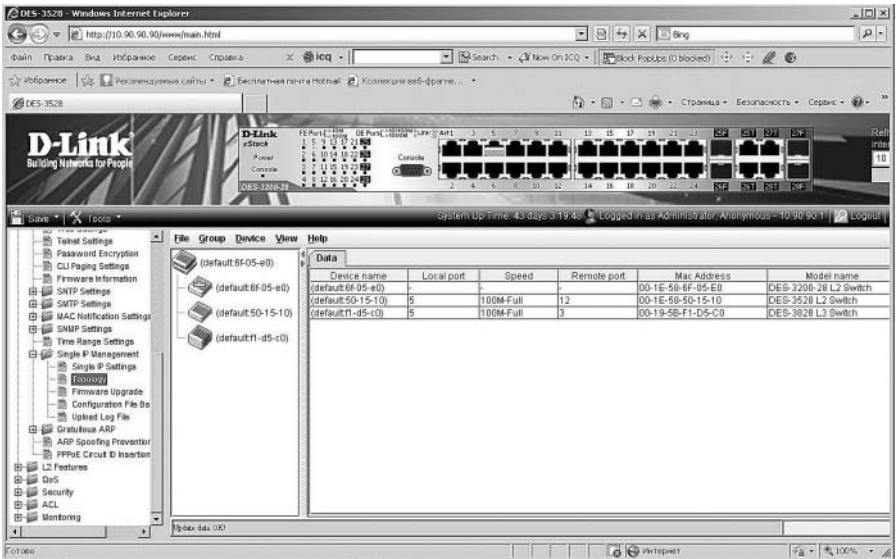


Рис. 9.8. Функция SIM в Web-интерфейсе

После настройки Commander Switch в папке Single IP Management Web-интерфейса станет доступна опция Topology. Эта опция позволяет настраивать коммутаторы и управлять ими внутри SIM-группы. При выборе пункта View окна Topology появится топологическая карта, показывающая, как подключены устройства внутри SIM-группы. Топологическая карта автоматически обновляется каждые 20 секунд.

Используя топологическую карту, администратор может получать детальную информацию о группе, просматривать краткую информацию о каждом коммутаторе SIM-группы, настраивать его, добавлять и удалять устройства из SIM-группы.

В топологической карте используются следующие иконки для обозначения Commander Switch, Member Switch и Candidate Switch.

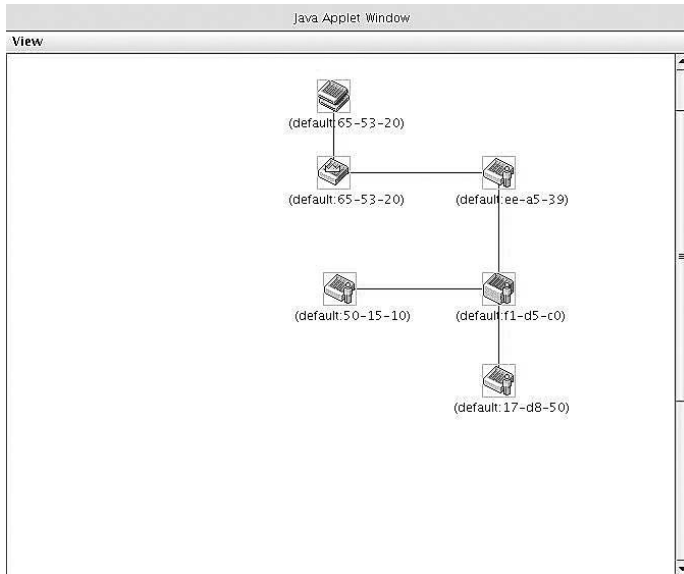


Рис. 9.9. Топологическая карта


Иконки Commander Switch

 Commander Switch уровня 2

 Commander Switch уровня 3


 Commander Switch уровня 3

Иконки Member Switch

 Member Switch уровня 2

 Member Switch уровня 3

Иконки Candidate Switch

 Candidate Switch уровня 2

 Candidate Switch уровня 3

Рис. 9.10. Иконки, используемые для представления устройств в топологической карте

9.2. Протокол SNMP

Протокол SNMP (Simple Network Management Protocol) является протоколом 7 уровня модели OSI, который специально разработан для управления и мониторинга сетевых устройств. Протокол SNMP входит в стек протоколов TCP/IP и позволяет администраторам сетей получать информацию о состоянии устройств сети, обнаруживать и исправлять неисправности и планировать развитие сети.

В настоящее время существует три версии протокола SNMP: SNMP v1 (RFC 1157), SNMP v2c (RFC 1901-1908) и SNMP v3 (RFC 3411-3418). Эти версии отличаются предоставляемым уровнем безопасности при обмене данными между менеджером и агентом SNMP. Коммутаторы D-Link поддерживают все три версии протокола.

9.2.1. Компоненты SNMP

Сеть, управляемая по протоколу SNMP, основывается на архитектуре «клиент/сервер» и состоит из трех основных компонентов: менеджера SNMP, агента SNMP, базы управляющей информации.

Менеджер SNMP (SNMP Manager) – это программное обеспечение, установленное на рабочей станции управления, наблюдающее за сетевыми устройствами и управляющее ими.

Агент SNMP (SNMP Agent) – это 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.

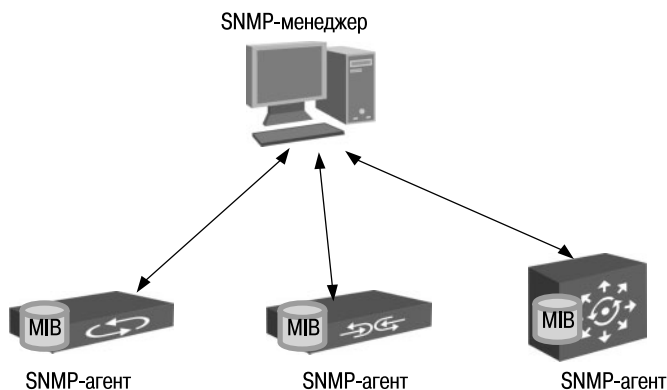


Рис. 9.11. Компоненты SNMP

База управляющей информации (Management Information Base, MIB) – это совокупность иерархически организованной информации, доступ к которой осуществляется посредством протокола управления сетью.

Менеджер взаимодействует с агентами при помощи протокола SNMP с целью обмена управляющей информацией. В основном это взаимодействие реализуется в виде периодического опроса менеджером множества агентов, которые предоставляют доступ к информации.

9.2.2. База управляющей информации SNMP

Базы управляющей информации описывают структуру управляющей информации устройств и состоят из управляемых объектов (переменных). *Управляемый объект* (или MIB-объект) – это одна из нескольких

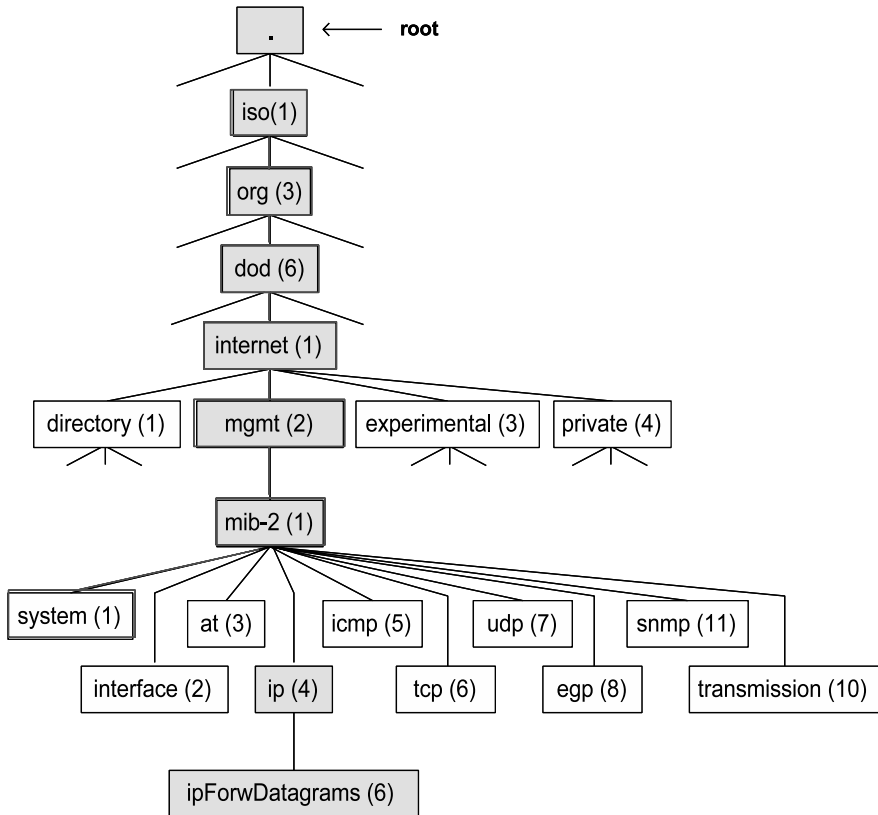


Рис. 9.12. Пространство имен OID

характеристик управляемого сетевого устройства (например, имя системы, время, прошедшее с ее перезапуска, количество интерфейсов устройства, IP-адрес и т.д.).

Обращение к управляемым объектам MIB происходит посредством идентификаторов объекта (Object Identifier, OID). Каждый управляемый объект имеет уникальный идентификатор в пространстве имен OID и контролируется агентством IANA. Пространство имен OID можно представить в виде иерархической структуры с корнем без названия, идентификаторы верхних уровней которой отданы организациям, контролирующим стандартизацию, а идентификаторы нижних уровней определяются самими этими организациями. Каждая ветвь дерева OID нумеруется целыми числами слева направо, начиная с единицы. Идентификатор представляет собой последовательность целых десятичных цифр, разделенных точкой, записанных слева направо и включает полный путь от корня до управляемого объекта. Числам могут быть поставлены в соответствие текстовые строки для удобства восприятия. В целом структура имени похожа на систему доменных имен Интернета (Domain Name System, DNS).

Каждая MIB (в настоящее время основными стандартами на базы управляющей информации для протокола SNMP являются MIB-I и MIB-II) определяет набор переменных, т. е. определенную ветку дерева OID, описывающую управляющую информацию в определенной области. Например, ветка 1.3.6.1.2.1.1 (символьное эквивалентное имя: iso.org.dod.internet.mgmt.mib-2.system) описывает общую информацию о системе.

Производители сетевого оборудования определяют частные ветви пространства имен OID (группа объектов private (4)), куда помещают управляемые объекты для своей продукции. Так, D-Link в качестве вершины иерархии для своей продукции использует OID, равный 1.3.6.1.4.1.171.

Помимо непосредственного описания данных необходимо вести операции над ними. Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Спецификация MIB-II дополнительно определяет операции изменения или установки значений управляемых объектов.

9.2.3. Типы сообщений протокола SNMP

Протокол SNMP является простым протоколом типа «запрос – ответ», т.е. на каждый запрос менеджера, агент должен дать ответ. В протоколе определено несколько типов сообщений, которыми обмениваются менеджер и агент:

- **Get-Request** – запрос значений одного или нескольких объектов;
- **Get-Next-Request** – запрос значения следующего объекта в соответствии с алфавитным порядком идентификаторов OID;

- **Set-Request** – запрос на изменение значения одного или нескольких объектов;
- **Get(Set)-Reply** – получение ответа от агента на сообщение Get-Request, Get-Next-Request или Set-Request.

Сообщение **Trap** (ловушка) используется агентом SNMP для асинхронного сообщения менеджеру SNMP о событии, происходящем на управляемом сетевом устройстве. События могут быть серьезные, например перезагрузка устройства, или менее серьезные, например изменение состояния порта.

Версия SNMP v.2 добавляет к этому набору команду GetBulk, которая позволяет менеджеру получить несколько переменных за один запрос.

При передаче управляющих сообщений в качестве протокола транспортного уровня используется протокол UDP.

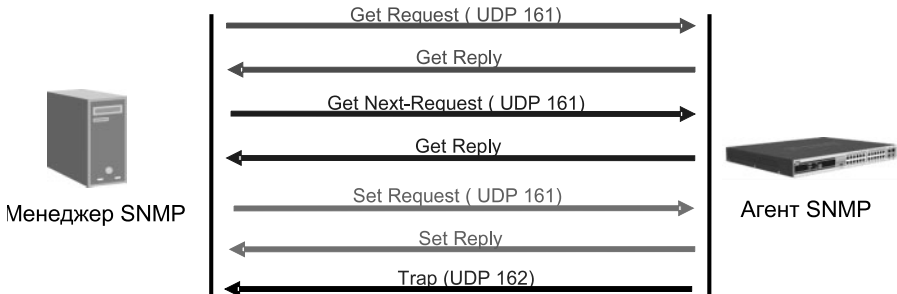


Рис. 9.13. Типы сообщения протокола SNMP

9.2.4. Безопасность SNMP

В протоколе SNMP v.1 и v.2c предусмотрена аутентификация пользователей, которая выполняется с помощью строки сообщества (Community string). Строки Community string функционирует подобно паролю, который разрешает удаленному менеджеру SNMP доступ к агенту. Менеджер и агент SNMP должны использовать одинаковые строки Community string, т.к. все пакеты от менеджера SNMP, не прошедшего аутентификацию, будут отбрасываться. В коммутаторах с поддержкой SNMP v.1 и v.2c используются следующие Community string по умолчанию:

- **public** – позволить авторизованной рабочей станции читать (право «read only») MIB-объекты;
- **private** – позволить авторизованной рабочей станции читать и изменять (право «read/write») MIB-объекты.

Внимание: Community string передаются по сети в открытом виде.

Протокол SNMP v.3 использует более сложный процесс аутентификации, который разделен на две части. Первая часть – обработка списка и атрибутов пользователей, которым позволено функционировать в качестве менеджера SNMP. Вторая часть описывает действия, которые каждый пользователь из списка может выполнять в качестве менеджера SNMP.

На коммутаторе SNMP можно создавать группы со списками пользователей (менеджеров SNMP) и настраивать для них общий набор привилегий. Помимо этого, для каждой группы может быть установлена версия используемого ею протокола SNMP. Таким образом, можно создать группу менеджеров SNMP, которым позволено просматривать информацию с правом «read only» или получать ловушки (trap), используя SNMP v.1, в то время как другой группе можно настроить наивысший уровень привилегий с правами «read/write» и возможность использования протокола SNMP v.3.

При использовании протокола SNMP v.3 отдельным пользователям или группам менеджеров SNMP может быть разрешено или запрещено выполнять определенные функции SNMP-управления. Помимо этого, в SNMP v.3 доступен дополнительный уровень безопасности, при котором SNMP-сообщения могут шифроваться при передаче по сети.

9.2.5. Пример настройки протокола SNMP

На рис. 9.14 показана схема сети, в которой управление коммутатором может выполняться через управляющую консоль SNMP по протоко-

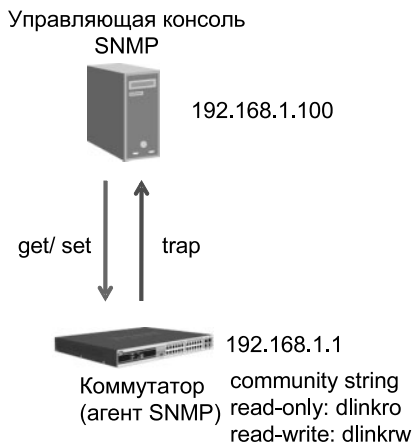


Рис. 9.14. Схема сети

лу SNMP v.2. В случае обнаружения SNMP-агентом коммутатора каких-либо неполадок он будет отправлять сообщения Trap менеджеру SNMP. В целях повышения безопасности строки Community string по умолчанию удалены.

Настройка коммутатора

- Активизировать функцию SNMP глобально на коммутаторе.

```
enable snmp
```

- Удалить строки Community string по умолчанию и создать новые строки Community string.

```
delete snmp community public  
delete snmp community private  
create snmp community dlinkro view CommunityView read_only  
create snmp community dlinkrw view CommunityView read_write
```

- Задать параметры получателя сообщений Trap от агента и активизировать функцию отправки сообщений Trap.

```
create snmp host 192.168.1.100 v2c dlinkrw  
enable snmp traps  
enable snmp authenticate_traps
```

9.3. RMON (Remote Monitoring)

Спецификация *RMON* MIB (Remote MONitoring, удаленный мониторинг) была разработана сообществом IETF для поддержки мониторинга и анализа протоколов в локальных сетях. Первая версия RMON v.1 (RFC 2819) основывается на мониторинге информации сетей Ethernet и Token Ring. Ее расширением является RMON v.2 (RFC 2021), которая добавила к уже имеющимся средствам мониторинга поддержку мониторинга на сетевом уровне и уровне приложений модели OSI.

Реализация RMON основывается на модели «клиент/сервер». На устройствах мониторинга, называемых в терминологии RMON «зондами» (probe), установлено специальное программное обеспечение – агент RMON, которое собирает информацию и анализирует пакеты. Зонды действуют как серверы, а приложения сетевого управления, установленные на станциях управления сетью, исполняют роль клиентов. Агенты RMON могут как размещаться на автономных устройствах, так и встраи-

ваться в коммутаторы, маршрутизаторы и другие сетевые устройства. Станция управления сетью и распределенные зонды RMON взаимодействуют по сети по протоколу SNMP.



Рис. 9.15. Консоль и зонд RMON

Несмотря на то, что RMON является расширением протокола SNMP, он отличается от него тем, что зонды RMON могут самостоятельно выполнять сбор и обработку данных. Это позволяет сократить трафик SNMP в сети и нагрузку на станцию управления, причем информация будет передаваться на станцию только когда это необходимо. Расположенные в различных частях сети приложения RMON могут одновременно взаимодействовать и получать информацию от одного и того же зонда.

RMON поставляет информацию в группы RMON MIB, каждая из которых поддерживает определенный набор данных, удовлетворяющих общим требованиям мониторинга сети. RMON v.1 содержит десять групп RMON MIB, а RMON v.2 добавляет к ним еще девять групп RMON MIB. Вместе RMON v.1 и RMON v.2 позволяют собирать статистику о трафике на всех уровнях модели OSI. Из-за того, что при выполнении обработки данных на ресурсы устройств мониторинга ложится большая нагрузка, то производители реализуют на оборудовании ограниченный набор групп RMON MIB. Обычно агент RMON поддерживает только группы statistics, history, alarm и event.

Для настройки RMON на коммутаторах D-Link второго уровня требуется активизировать эту функцию глобально на коммутаторе с помощью команды *enable rmon*.

Таблица 9.1. Группы мониторинга RMON v.1

№	Группа RMON	Функция
1	Statistics	Содержит статистические данные, измеренные датчиком на каждом интерфейсе устройства, для которого проводится мониторинг
2	History	Периодическая запись статистических выборок из сети и их хранение для дальнейшего использования
3	Alarm	Периодическое извлечение статистических выборок из переменных в датчике и их сравнение с заранее выбранными пороговыми значениями. Если наблюдаемые значения выходят за границы пороговых, генерируется событие
4	Host	Содержит статистические данные, связанные с каждым узлом, обнаруженным в сети
5	Hosts top N	Содержит отсортированные данные по указанному числу узлов в порядке убывания их статистики
6	Matrix	Содержит статистику по диалогам между парами узлов, в том числе о величине трафика и количестве ошибок в обоих направлениях
7	Filter	Содержит условия фильтрации пакетов
8	Capture	Содержит пакеты, захваченные интерфейсом в соответствии с условиями фильтрации
9	Event	Протоколирование событий и определение действий при их наступлении
10	Token Ring	Расширенная статистика для сетей Token Ring

Таблица 9.2. Группы мониторинга RMON v.2

№	Группа RMON	Функция
1	Protocol Directory	Список протоколов, для которых зонд может осуществлять мониторинг пакетов
2	Protocol Distribution	Статистика трафика для каждого протокола с информацией о распределении и тенденциях в использовании протоколов
3	Address Map	Соответствия между адресами сетевого уровня и MAC-адресами, обнаруженные зондом на интерфейсе
4	Network-Layer Host	Статистика трафика передаваемого от и к каждому обнаруженному зондом узлу
5	Network-Layer Matrix	Содержит статистику по диалогам между парами узлов на сетевом уровне

6	Application-Layer Host	Статистика трафика передаваемого от и к каждому обнаруженному зондом узлу по протоколам
7	Application-Layer Matrix	Статистика трафика по диалогам между парами узлов на сетевом уровне по протоколам
8	User History	Периодические выборки для определенных пользователем переменных
9	Probe Configuration	Удаленная конфигурация параметров зонда

При настройке функции на коммутаторе третьего уровня необходимо дополнительно активизировать протокол SNMP и определить Community string.

9.4. Функция Port Mirroring

Функция *Port Mirroring* («Зеркалирование портов») позволяет отображать (копировать) кадры, принимаемые и отправляемые портом-источником (Source port) на целевой порт (Target port) коммутатора, к которому подключено устройство мониторинга с целью анализа проходящих через интересующий порт пакетов. Эта функция полезна администраторам для мониторинга и поиска неисправностей в сети.

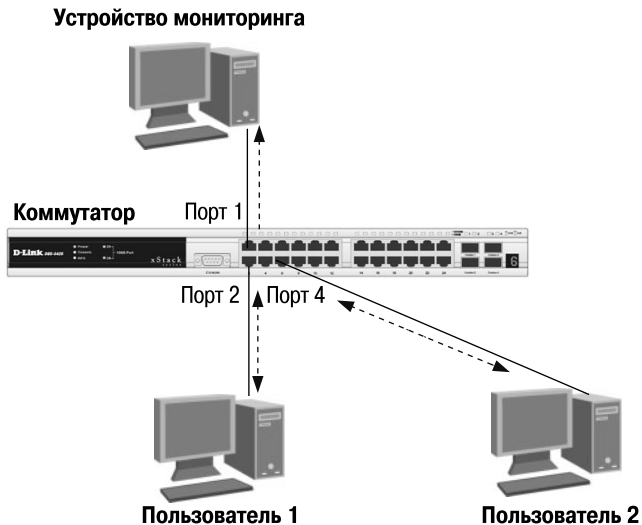


Рис. 9.16. Функция Port Mirroring

Следует отметить, что целевой порт и порт-источник должны принадлежать одной VLAN и иметь одинаковую скорость работы. В том случае, если скорость порта-источника будет выше скорости целевого порта, коммутатор снизит скорость порта-источника до скорости работы целевого порта.

На рис. 9.16 показан пример, в котором трафик, передаваемый и получаемый портами 2 и 4, будет зеркалироваться на порт 1, к которому подключено устройство мониторинга.

Настройка коммутатора

```
config mirror port 1 add source ports 2, 4 both  
enable mirror
```

Лекция 10. Обзор коммутаторов D-Link

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

10.1. Неуправляемые коммутаторы

Неуправляемые коммутаторы (*Unmanaged Switches*) D-Link являются идеальным решением 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 Green Ethernet, диагностика кабеля, управление потоком (IEEE 802.3x), автоматическое определение полярности кабелей (MDI/MDIX), возможность передачи Jumbo-фреймов и приоритизацию трафика.

Неуправляемые коммутаторы не поддерживают функции управления и обновления программного обеспечения.

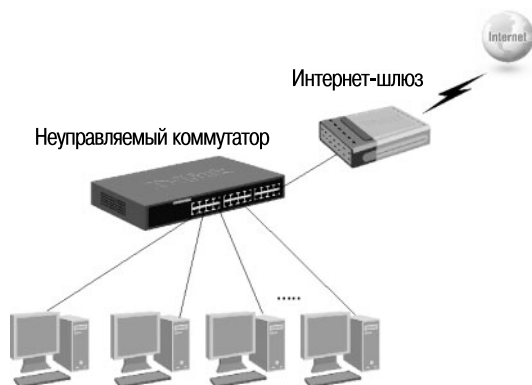


Рис. 10.1. Неуправляемые коммутаторы D-Link в сети небольшой рабочей группы

Неуправляемые коммутаторы D-Link представлены сериями DES-10xx, DES-10xxA, DES-10xxD/RU, DGS-10xxD/RU и DGS-10xxD/GE. Серия DES-10xx включает в себя модели неуправляемых коммутаторов Fast

Ethernet с различным количеством портов 10/100 Мбит/с (от 5 до 48) в настольном и стоечном исполнении. Модели DES-1026G и DES-1050G этой серии также оснащены двумя портами Gigabit Ethernet.

Серия DES-10xxA состоит из экономичных неуправляемых коммутаторов с различным количеством портов 10/100 Мбит/с (от 5 до 24).

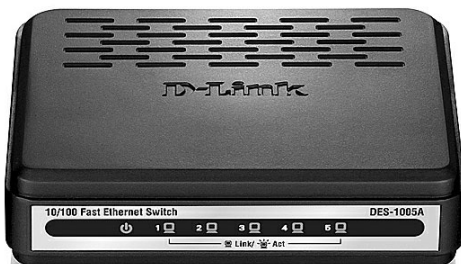


Рис. 10.2. Коммутатор DES-1005A

Серии коммутаторов улучшенного дизайна DES-10xxD/RU и DGS-10xxD/RU включают коммутаторы с 5 и 8 портами Fast и Gigabit Ethernet соответственно.

Серия DGS-10xxD/GE включает в себя модели неуправляемых коммутаторов Gigabit Ethernet с различным количеством портов 10/100/1000 Мбит/с (от 5 до 24). Эти коммутаторы поддерживают стандарт IEEE 802.1p и четыре аппаратных очереди приоритетов на каждом физическом порте.



Коммутаторы серий DGS-10xxD/RU и DGS-10xxD/GE поддерживают технологию Green Ethernet. Эта энергосберегающая технология позволяет сократить расходы на электроэнергию, при этом не оказывая влияния на производительность и функциональность устройств. Технология Green Ethernet может регулировать потребление электроэнергии, основываясь на определении состояния канала связи и длины кабеля. Когда коммутатор с поддержкой этой технологии определяет, что питание подключенного к нему компьютера отключено, то переводит соответствующий порт в режим сохранения энергии (power standby mode). Также коммутатор может регулировать энергопотребление путем анализа длины кабеля Ethernet. Т.к. в большинстве случаев для подключения пользователей домашних/офисных сетей используются кабели длиной менее 20 м, энергопотребление может быть снижено.

Благодаря уменьшению энергопотребления (до 80%), выделяется меньше тепла, что увеличивает срок эксплуатации устройства и снижает эксплуатационные расходы.

Также данная технология подразумевает использование материалов, не наносящих вред окружающей среде.

Помимо технологии Green Ethernet, в коммутаторах серий DGS-10xxD/RU и DGS-10xxD/GE реализована поддержка функции диагностики кабеля (Cable Diagnostic). Эта функция позволяет пользователям определять состояние кабеля по индикаторам, расположенным на передней панели коммутатора. С помощью нее можно определить следующие повреждения кабеля:

- разомкнутая цепь (Open Circuit) – оборвана жила кабеля Ethernet или кабель не подключен;
- короткое замыкание (Short Circuit) – короткое замыкание пары кабеля (два проводника касаются друг друга);
- неправильная терминация кабеля (Improper Termination) – сопротивление между кабелем и его разъемом не совпадает или сопротивление больше чем 100 Ом.

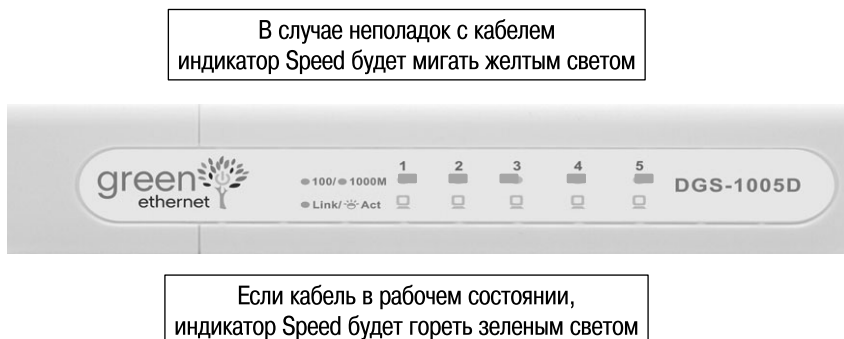


Рис. 10.3. Функция диагностики кабеля

Функция диагностики кабеля сканирует все порты Ethernet и определяет состояние каждого подключенного кабеля. Во время этого процесса индикатор каждого порта последовательно мигает зеленым светом. Первоначальное сканирование порта требует около 10 секунд. Если обнаруживается повреждение кабеля, индикатор соответствующего порта будет мигать желтым светом около 5 секунд. Далее коммутатор автоматически перезагрузится и продолжит работу в обычном режиме. Этот процесс займет около 2-х секунд.

Внимание: для неуправляемых коммутаторов повреждение кабеля не определяется в режиме обычной работы. Диагностика кабеля осуществляется только во время загрузки или цикла выключения/включения коммутатора.

10.2. Коммутаторы серии Smart

Традиционно существуют только 2 категории коммутаторов: неуправляемые и управляемые. Однако D-Link предлагает еще одну, промежуточную категорию – **настраиваемые коммутаторы** (*Smart Switches*). Эти коммутаторы предназначены для использования на уровне доступа сетей малых и средних предприятий (*Small-to-Medium Business, SMB*).

Настраиваемые коммутаторы D-Link представлены двумя сериями: Easy Smart и Smart.

Коммутаторы Easy Smart в настоящее время включают две модели: DES-1100-16 и DES-1100-24. Эти коммутаторы помещены в металлический корпус компактного размера (11”) и оснащены 16 и 24 портами 10/100Base-TX соответственно. Они предоставляют пользователям возможность настраивать определенные параметры сети с помощью интуитивно понятных средств управления, например Web-интерфейса или утилиты SmartConsole. По сравнению с коммутаторами серии Smart, устройства Easy Smart обладают ограниченным функционалом.

Третье поколение коммутаторов серии Smart представлено продуктовыми линейками DES-1210-xx и DGS-1210-xx. Серия DES-1210-xx в настоящее время включает модели DES-1210-28 и DES-1210-52, оснащенные 24 и 48 портами 10/100 Мбит/с соответственно, 2 портами Gigabit Ethernet и 2 комбинированными Uplink-портами 1000Base-T/SFP. Серия DGS-1210-xx включает четыре модели: DGS-1210-10P, DGS-1210-16, DGS-1210-24 и DGS-1210-48. Модели DGS-1210-16, DGS-1210-24 и DGS-1210-48 оснащены 12, 20 и 44 портами 1000Base-T соответственно и 4 комбинированными Uplink-портами 1000Base-T/SFP. В модели DGS-1210-10P реализована поддержка технологии Power over Ethernet (PoE) (стандарты IEEE 802.3af и IEEE 802.3at (PoE+)), которая позволяет передавать питание по неиспользуемым парам кабеля Ethernet одновременно с передачей данных. Все устройства, за исключением DGS-1210-10P, помещены в металлический корпус размером для установки в стойку (19”). Размер корпуса DGS-1210-10P составляет 13”.



Рис. 10.4. Коммутатор DES-1210-28

Коммутаторы серии Smart поддерживают функции обеспечения отказоустойчивости, безопасности, сегментации сети, качества обслуживания, мониторинга трафика и диагностики кабеля. Управление коммутаторами может осуществляться через Web-интерфейс, утилиту SmartConsole, упрощенный интерфейс командной строки и протокол SNMP.

Помимо этого, коммутаторы серии DGS-1210-xx поддерживают технологию Green Ethernet и Jumbo-фреймы.

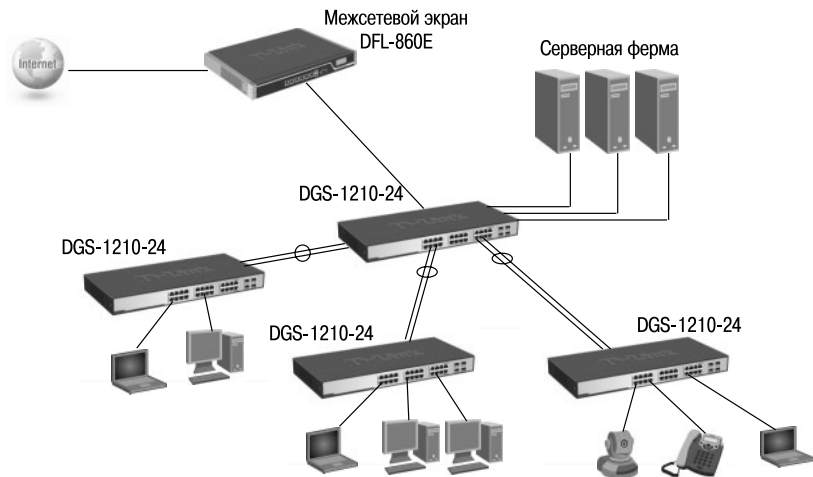


Рис. 10.5. Пример использования коммутаторов серии Smart в сетях SMB

10.3. Управляемые коммутаторы

Управляемые коммутаторы (*Managed Switches*) по сравнению с неуправляемыми коммутаторами и коммутаторами серии Smart являются сложными устройствами, поддерживающими расширенный набор функций 2 и 3 уровня модели OSI. Такие устройства предоставляют большой выбор интерфейсов, обладают высокоскоростной внутренней магистралью, возможностью установки дополнительных модулей и физического стекирования. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протокола SNMP, Telnet и т.д.

Серия бюджетных управляемых коммутаторов Fast Ethernet 2 уровня DES-1228/ME, DES-3028/52 может использоваться на уровне доступа сетей малых, средних и крупных предприятий, а также в сетях провайдеров для предоставления услуг Triple Play. Коммутаторы поддерживают базовый и расширенный функционал 2 уровня, обеспечивающий возможность управления доступом пользователей, контроля полосы пропуски

ния, сегментации сети, управления широковещательными пакетами, многоадресной рассылкой. Коммутаторы DES-1228/ME также поддерживают функцию диагностики кабеля.

DES-1228/ME	24 порта 10/100Base-TX, 2 порта SFP, 2 комбо-порта 1000Base-T/SFP
DES-3028	24 порта 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3028P	24 порта PoE 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3052	48 портов 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3052P	48 портов PoE 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP

Коммутаторы Fast Ethernet 2 уровня серии DES-3200-xx предназначены для использования на уровне доступа сетей провайдеров, предоставляющих услуги по подключению к сети Интернет посредством технологий Metro Ethernet (Ethernet-To-The-Home, EТТН и Fiber-To-The-Home, FTTH) и реализующих сервисы Triple Play.

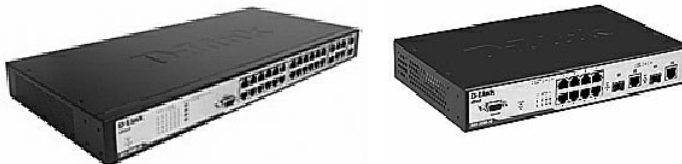


Рис. 10.6. Коммутаторы серии DES-3200-xx

DES-3200-10	8 портов 10/100Base-TX, 2 комбо-порта 1000Base-T/SFP
DES-3200-18	16 портов 10/100Base-TX, 2 комбо-порта 1000Base-T/SFP
DES-3200-26	24 порта 10/100Base-TX, 2 комбо-порта 1000Base-T/SFP
DES-3200-28	24 порта 10/100Base-TX, 4 комбо-порта 1000Base-T/SFP
DES-3200-28F	24 порта SFP, 4 комбо-порта 1000Base-T/SFP

Серия коммутаторов Fast Ethernet 2 уровня DES-3528/3552 предназначена для использования на уровне доступа сетей крупных предприятий и Metro Ethernet с сервисами Triple Play. Коммутаторы поддерживают физическое сте-

кирование по Ethernet, статическую маршрутизацию, функции управления многоадресной рассылкой, расширенные функции безопасности и виртуальных локальных сетей VLAN. Устройства легко интегрируются с коммутаторами L3 уровня ядра для формирования многоуровневой сетевой структуры с высокоскоростной магистралью и централизованными серверами.

DES-3528	24 порта 10/100Base-TX, 2 порта 1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3528DC	24 порта 10/100Base-TX, 2 порта 1000Base-T, 2 комбо-порта 1000Base-T/SFP (питание 48В DC)
DES-3528P	24 порта PoE 10/100Base-TX, 2 порта 1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3552	48 портов 10/100Base-TX, 2 порта 1000Base-T, 2 комбо-порта 1000Base-T/SFP

Коммутаторы Fast Ethernet 3 уровня серии DES-3810-xx являются новым поколением мультисервисных коммутаторов D-Link, предназначенным для использования на уровне доступа сетей крупных предприятий и Metro Ethernet, в которых реализованы сервисы Triple Play и VPN. В настоящее время серия представлена моделью DES-3810-28. Одной из особенностей коммутаторов серии DES-3810-xx является то, что в них встроены два разных образа программного обеспечения: Standard Image (SI) и Enhanced Image (EI). В стандартной прошивке реализованы такие функции, как качество обслуживания (QoS), включая механизм Traffic Shaping, Q-in-Q VLAN, маршрутизация пакетов IPv4, многоадресная рассылка, Ethernet OAM и множество функций безопасности. Расширенная прошивка включает поддержку маршрутизации IPv6, протоколов BGP и MPLS. Также коммутаторы серии DES-3810-xx поддерживают функцию Switch Resource Management (SRM), позволяющую администратору оптимизировать ресурсы коммутатора при его использовании в различных сетевых средах.



Рис. 10.7. Коммутатор DES-3810-28

DES-3810-28	24 порта 10/100Base-TX, 4 комбо-порта 1000Base-T/SFP
-------------	---

Коммутаторы Gigabit Ethernet 2 уровня серии DGS-3120-xx могут использоваться как на уровне доступа, так и на уровне субагрегации сетей SOHO/SMB и Metro Ethernet. В коммутаторах реализован базовый и расширенный функционал 2 уровня; поддерживаются физическое стекирование через порты 10GE, подключение резервных источников питания, функция диагностики кабеля. Благодаря высокой плотности портов SFP коммутаторы DGS-3120-24SC и DGS-3120-24SC-DC обеспечивают возможность гибкого подключения по оптике к магистрали сети и серверам в сетях провайдеров услуг. Коммутаторы DGS-3120-24PC и DGS-3120-48PC поддерживают спецификацию передачи питания по Ethernet (стандарты IEEE 802.3af и IEEE 802.3at (PoE+)).



Рис. 10.8. Коммутаторы серии DGS-3120-xx

DGS-3120-24TC	20 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP
DGS-3120-48TC	44 порта 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP
DGS-3120-24PC	20 портов PoE 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP
DGS-3120-48PC	44 порта PoE 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP
DGS-3120-24SC	8 комбо-портов 1000Base-T/ SFP, 16 портов SFP
DGS-3120-24SC-DC	8 комбо-портов 1000Base-T/ SFP, 16 портов SFP (питание 48В DC)

Малопортовые коммутаторы Gigabit Ethernet 2 уровня серии DGS-3200-xx обладают полным набором функций, позволяющих обеспечить безопасность, контроль доступа, отказоустойчивость и управляемость сети, и предназначены для использования на уровне доступа сетей средних и крупных предприятий. Коммутаторы DGS-3200-10 и DGS-3200-16 помещены в компактный корпус размером 11". В коммутаторе DGS-3200-10

применяется безвентиляторная технология, благодаря чему он бесшумно работает. В коммутаторе DGS-3200-16 используется технология автоматической вентиляции.

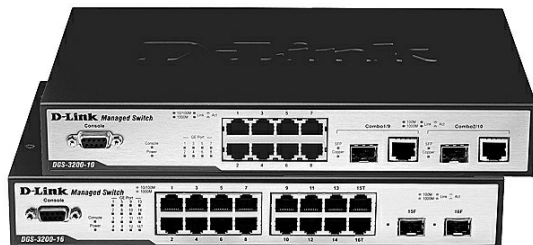


Рис. 10.9. Коммутаторы серии DGS-3200-xx

DGS-3200-10 8 портов 10/100/1000Base-T, 2 комбо-порта 1000Base-T/ SFP

DGS-3200-16 14 портов 10/100/1000Base-T, 2 комбо-порта 1000Base-T/ SFP

Коммутаторы Gigabit Ethernet 2 уровня серии DGS-3420-xx предназначены для использования на уровне распределения сетей крупных предприятий и Metro Ethernet.

DGS-3420-26SC 20 портов SFP, 4 комбо-порта 1000Base-T/ SFP, 2 порта 10GE SFP+

DGS-3420-28SC 20 портов SFP, 4 комбо-порта 1000Base-T/ SFP, 4 порта 10GE SFP+

DGS-3420-28TC 20 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP, 4 порта 10GE SFP+

DGS-3420-28PC 20 портов PoE 10/100/1000Base-T, 4 комбо-порта 1000Base-T(PoE)/ SFP, 4 порта 10GE SFP+

DGS-3420-52T 48 портов 10/100/1000Base-T, 4 порта 10GE SFP+

DGS-3420-52P 48 портов 10/100/1000Base-T PoE, 4 порта 10GE SFP+

Коммутаторы обеспечивают высокую плотность портов для подключения рабочих мест, оснащены слотами SFP и SFP+ для гибкого подключения по оптике на скоростях Gigabit и 10 Gigabit Ethernet соответственно, обладают высокопроизводительной внутренней магистралью, поддерживают возможность физического стекирования (до 12 устройств в стеке) через порты 10 GE и подключение резервных источников питания.

Среди функциональных возможностей можно выделить поддержку статической маршрутизации IPv4/IPv6 и протокола RIP, расширенные функции безопасности, качества обслуживания виртуальных локальных сетей и управления. Также в коммутаторах реализована поддержка функции ERPS (Ethernet Ring Protection Switching), которая обеспечивает защиту от колец Ethernet в коммутируемой сети.

Коммутаторы Gigabit Ethernet 2 уровня серии DGS-3700-хх спроектированы с учетом требований операторов телекоммуникационных услуг при построении сетей Metro Ethernet. Коммутаторы поддерживают широкий набор функций безопасности, качества обслуживания, управления многоадресными пакетами и обеспечивают расширенную поддержку VLAN. Коммутаторы обладают модульной архитектурой ядра, поддерживают возможность выбора источника питания (постоянного или переменного тока) и расширенный диапазон рабочих температур.

DGS-3700-12	8 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/SFP
DGS-3700-12G	8 портов SFP, 4 комбо-порта 1000Base-T/SFP

Семейство маршрутизирующих управляемых коммутаторов Gigabit Ethernet 3 уровня с поддержкой портов 10 GE DGS-36хх обладает высокой производительностью и предназначено для использования на уровнях распределения и ядра крупных корпоративных сетей, сетей предприятий малого и среднего бизнеса (SMB) и городских сетей Metro Ethernet. Благодаря расширенной поддержке функций многоадресной передачи данных, среди которых IGMP v.3, PIM SM и PIM DM, коммутаторы позволяют значительно повысить эффективность предоставляемых операторами связи таких услуг, как видео по требованию (VoD), IP-телевидение (IPTV) и телевидение высокой четкости (HDTV). Коммутаторы поддерживают протоколы маршрутизации BGP, OSPF, RIP v.1/2, возможность создания статических и плавающих статических маршрутов IP v4/v6.

DGS-3612	8 портов 10/100/1000Base-T, 4 комбо-порта SFP / 1000Base-T
DGS-3612G	8 портов SFP, 4 комбо-порта SFP /1000Base-T
DGS-3627	20 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/SFP, 3 слота расширения
DGS-3627G	20 портов SFP, 4 комбо-порта SFP /1000Base-T, 3 слота расширения
DGS-3650	44 порта 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP, 2 слота расширения

Высокопроизводительные коммутаторы Gigabit Ethernet 3 уровня с поддержкой портов 10 GE серии DGS-3610-xx обладают расширенным функционалом, включая поддержку BGP, и могут применяться на магистрали сетей Metro Ethernet и крупных предприятий.



Рис. 10.10. Коммутатор DGS-3610-26

DGS-3610-26	12 портов 10/100/1000Base-T, 12 комбо-портов 1000Base-T/ SFP, 2 слота расширения
DGS-3610-26G	12 портов SFP, 12 комбо-портов 1000Base-T/ SFP, 2 слота расширения

Семейство высокопроизводительных коммутаторов Gigabit Ethernet 3 уровня с поддержкой портов 10 GE серии DGS-3620-xx предназначено для использования на уровне ядра сетей крупных предприятий и Metro Ethernet. Коммутаторы поддерживают физическое стекирование через порты 10GE SFE+ и позволяют объединить в стек до 12 устройств. Коммутатор поддерживает расширенные функции 2 уровня, включая ERPS, Q-in-Q VLAN, 802.3ah Ethernet Link OAM, Optical Transceiver Digital Diagnostic Monitoring (DDM). Функции 3 уровня включают поддержку протоколов маршрутизации OSPF v.2/3, RIP v.1/2/ng для IP v4/v6, протоколов многоадресной рассылки IGMP v.1/2/3, PIM SM и PIM DM. Расширенные функции безопасности обеспечивают возможность контроля доступа к ресурсам сети и предотвращения распространенных атак типа ARP Spoofing. Расширенный набор средств и функций управления позволяет администратору сети производить гибкую настройку сети и следить за ее состоянием.



Рис. 10.11. Коммутатор DGS-3620-28TC

DGS-3620-28SC	20 портов SFP, 4 комбо-порта 1000Base-T/ SFP, 4 порта 10GE SFP+
DGS-3620-28TC	20 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP, 4 порта 10GE SFP+
DGS-3620-28PC	20 портов PoE 10/100/1000Base-T, 4 комбо-порта 1000Base-T(PoE)/ SFP, 4 порта 10GE SFP+
DGS-3620-52T	48 портов 10/100/1000Base-T, 4 порта 10GE SFP+
DGS-3620-52P	48 портов 10/100/1000Base-T PoE, 4 порта 10GE SFP+

Модульные коммутаторы 3 уровня серии DGS-66xx представляют собой высокопроизводительные устройства с высокой плотностью портов, предназначенные для использования на уровне субядра сетей крупных предприятий, сетей небольших операторов связи, а также для организации широкополосного доступа в Интернет в крупных торговых комплексах и бизнес-центрах. В настоящее время серия представлена 4-слотовым шасси. Широкий выбор модулей позволяет обеспечить гибкость при подключении пользователей. В максимальной конфигурации шасси поддерживает до 192 гигабитных портов или до 24 портов 10GE. Шасси поддерживает расширенный набор функций 2 уровня. Функции 3 уровня включают поддержку маршрутизации OSPF v.2/3, RIP v.1/2/ng для IP v4/v6, BGP. Расширенные функции управления, мониторинга и сбора статистики, включая sFlow, LLDP, IPv6 Neighbor Discover (ND), DHCP relay option 82/60/61, предоставляют администратору сети возможность следить за состоянием сети и анализировать причины возникновения в ней ошибок и узких мест.

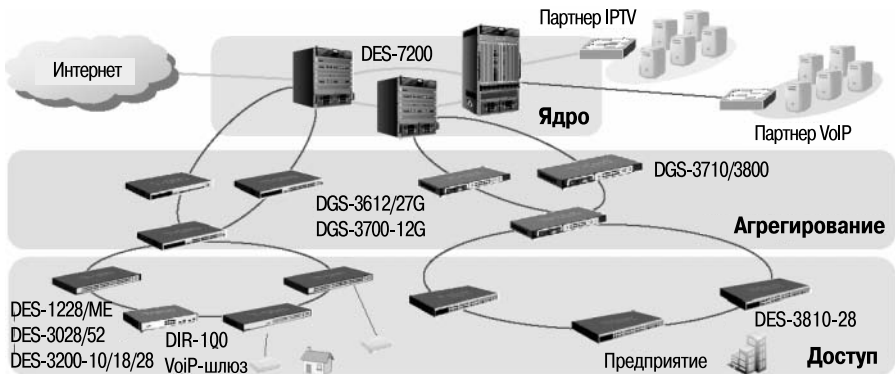


Рис. 10.12. Типовая схема применения коммутаторов D-Link

Коммутаторы 3 уровня на основе шасси серии DES-72xx являются высокопроизводительными устройствами с высокой плотностью портов, предназначенными для уровня ядра сетей крупных предприятий и Metro Ethernet. Устанавливая в шасси модули расширения, пользователи могут получить до 384 гигабитных портов, до 64 портов 10GE, до 192 портов SFP или их комбинаций. Коммутаторы поддерживают богатый набор функций 2 и 3 уровня, включая поддержку протоколов BGP, MPLS (Multi-protocol Label Switching), функции IPFIX, позволяющей получать статистику о сетевом трафике.

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 операционной системы коммутаторов; организация виртуальных локальных сетей; борьба с петлеобразованием; повышение отказоустойчивости локальных сетей; агрегирование каналов передачи данных; качество предоставления сервиса; безопасность сетей, ограничение доступа к сети на основе списков управления доступом и команд безопасности портов; управление сетью; поиск неисправностей в коммутируемых сетях. Каждое практическое занятие предваряется кратким теоретическим материалом. Все занятия представлены в оригинальной табличной форме, отражающей цель действия и способ ее достижения.

Список практических занятий

- Занятие №1.** Основные команды коммутаторов. Управление коммутаторами.
- Занятие №2.** Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов.
- Занятие №3.** Команды управления таблицами MAC, IP, ARP.
- Занятие №4.** Команды VLAN на основе портов и стандарта IEEE 802.1Q.
- Занятие №5.** Команды протокола GVRP (продвижение информации о VLAN в сети).
- Занятие №6.** Команды настройки асимметричных VLAN и сегментации трафика.
- Занятие №7.** Команды настройки функции Q-in-Q (Double VLAN).
- Занятие №8.** Команды настройки протоколов связующего дерева STP, RSTP, MSTP.
- Занятие №9.** Настройка функции предотвращения петлеобразования (LoopBack Detection).
- Занятие №10.** Команды агрегирования каналов.
- Занятие №11.** Списки управления доступом (Access Control List).
- Занятие №12.** Контроль над подключением узлов к портам коммутатора. Функция Port Security.

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

Занятие №14. Ограничение административного доступа к управлению коммутатором.

Занятие №15. Команды протокола IEEE 802.1X.

Занятие №16. Управление полосой пропускания.

Занятие №17. Настройка QoS. Приоритизация трафика.

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

Занятие №19. Команды мониторинга состояния коммутатора.

Занятие №1. Основные команды коммутаторов. Управление коммутаторами

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

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

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

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

Оборудование:

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

Схема 1:**1. Настройка DES-3200-28****1.1. Вызов помощи по командам**

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

Напишите в консоли *dir*
 (данной командой выводится список всех команд коммутатора)

Напишите в консоли *?*
 (аналогично команде dir)

Напишите в консоли *config ?*
 (просмотр списка команд конфигурирования)

Напишите в консоли *show ?*
 (вывод команд просмотра настроек коммутатора)

1.2. Изменение IP-адреса интерфейса управления коммутатора

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

Измените IP-адрес интерфейса управления коммутатора *config ipif System vlan default ipaddress 10.1.1.10/8*

Настройте IP-адрес шлюза по умолчанию *create iproute default 10.1.1.254*

Примечание. IP-адрес шлюза по умолчанию назначается, если управление коммутатором осуществляется из других IP-подсетей.

Проверьте настройки *show switch*

Внимание! При написании команды `show switch` выводится основная информация о коммутаторе. Например, MAC-адрес коммутатора, IP-адрес интерфейса управления, IP-адрес шлюза по умолчанию, серийный номер, версия программного обеспечения, доступные консоли управления, имя коммутатора и т.п.

1.3. Управление учетными записями пользователей

Внимание! Существует три уровня привилегий пользователей: Admin — максимальные права управления коммутатором, Operator — средние права управления (мониторинг сети, чтение системных параметров и конфигураций), User — минимальные права, в основном на чтение.

Создайте учетную запись администратора *create account admin dlink*

Введите пароль и подтверждение пароля пользователя: dlink *Enter a case-sensitive new password: dlink*
Enter the new password again for confirmation: dlink

Создайте учетную запись пользователя *create account user swuser*

Введите пароль и подтверждение пароля пользователя: dlink1 *Enter a case-sensitive new password: dlink1*
Enter the new password again for confirmation: dlink1

Проверьте настройки учетных записей пользователей *show account*

Отключите режим администрирования *logout*

Войдите в режим администрирования *login*

Введите данные для учетной записи администратора	<i>UserName: dlink PassWord: dlink</i>
Измените пароль пользователя.	<i>config account swuser</i>
После ввода команды укажите старый пароль пользователя и 2 раза новый пароль	<i>Enter a old password:**** Enter a case-sensitive new password:**** Enter the new password again for confirmation:****</i>
Удалите учетную запись пользователя	<i>delete account swuser</i>
Проверьте удаление учетной записи пользователя	<i>show account</i>

Внимание! Длина имени пользователя должна быть от 1 до 15 символов, длина пароля от 0 до 15 символов, максимальное количество пользователей 8.

Никогда не сохраняйте настройки конфигурации после создания пользователей, не проверив, можете ли вы зайти в систему! В случае утраты сведений о логине и пароле разблокировать коммутатор можно только в сервисном центре компании D-Link (для старых версий firmware)!

1.4. Настройка параметров идентификации коммутатора

Настройте имя коммутатора	<i>config snmp system_name HQ-SW01</i>
Укажите месторасположение (локализацию) коммутатора	<i>config snmp system_location HQ 5F</i>
Настройте ответственный контакт	<i>config snmp system_contact HQ IT Department</i>
Проверьте внесенные параметры	<i>show switch</i>

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

0 символов подразумевает, что информация отсутствует.

1.5. Настройка параметров баннеров приветствия (Login banner (greeting message) and Command Prompt)

Примечание. Для упрощения идентификации активного оборудования пользователями или создания уникальных логотипов оборудования возможно изменение баннера приветствия, который появляется в момент загрузки оборудования. Также возможно изменение приглашения Command Prompt в командной строке CLI.

Измените приглашение Command Prompt `config command_prompt switch-mipk`

Установите приглашение по умолчанию `config command_prompt default`

Посмотрите текущий баннер приветствия `show greeting_message`

Войдите в режим конфигурирования баннера `config greeting_message`

Для редактирования приветствия используйте следующие команды:

<Function Key>		<Control Key>
Ctrl+C	Quit without save	left/right/ up/down
Ctrl+W	Save and quit	Move cursor
		Ctrl+D Delete line
		Ctrl+X Erase all setting
		Ctrl+L Reload original setting

Добавьте строчку в приветствие `SWITCH MIPK tel +7(499) 263-62-92`

Сохраните изменения в приветствии и выйдите из режима редактирования: Ctrl+W

Проверьте баннер `show greeting_message`

```
=====
DES-3200-28 Fast Ethernet Switch
  Command Line Interface
SWITCH MIPK tel +7(499) 263-26-92
  Firmware: Build 1.10.B014
```

Copyright(C) 2009 D-Link Corporation. All rights reserved.

```
=====
```

Восстановите настройки баннера по умолчанию *config greeting_message default*

1.6. Настройка времени на коммутаторе

Введите команду *config time 01092010 15:45:30*

Установите часовой пояс Москва (GMT +3:00) *config time_zone operator + hour 3 min 0*

Проверьте время *show time*

Внимание! При перезагрузке коммутатора возможен сброс настроек текущего времени. Это обусловлено тем, что на некоторых моделях коммутаторов время хранится в памяти RAM. Таким образом, если в сети существуют серверы службы времени (NTP-серверы) или открыт доступ к серверам времени, расположенным в Интернете, желательно настроить синхронизацию с этими серверами.

Со списком серверов службы времени, расположенных в Интернете, можно ознакомиться здесь: <http://support.microsoft.com/kb/262680>

Включите работу протокола SNTP на коммутаторе *enable sntp*

Создайте список серверов SNTP и интервал обращений к серверам в секундах *config sntp primary 10.1.1.200 secondary 10.1.1.201 poll-interval 3600*

Проверьте текущее время *show time*

Примечание. Установка времени необходима для правильного отображения информации в журналах регистрации коммутаторов (Log files), проведения аудита работы сети, мониторинга сети и т.п.

1.7. Настройка основных параметров портов Ethernet коммутатора

Настройте скорость и режим работы порта *config ports 1-5 speed 10_half*

Посмотрите режим работы портов *show ports*

Подключите компьютер к порту 2 коммутатора. Что вы наблюдаете?

Отключите работу портов *config ports 1-5 state disable*

Включите работу порта *config ports 5 state enable*

Задайте имя порта (описание порта) *config ports 5 description
Magistral_port_Mipk*

Проверьте описания портов *show ports description*

Внимание! Описание имени порта, имени коммутатора, места размещения значительно облегчит дальнейшую эксплуатацию устройства и поиск неисправностей в случае сбоя оборудования.

Задайте тип работы COMBO-порта (комбинированного): оптика *config ports 25 medium_type fiber
state enable*

Задайте тип работы COMBO-порта (комбинированного): медь *config ports 25 medium_type copper
state disable*

Внимание! Все параметры работы порта можно настроить одновременно в одной команде.

1.8. Функция Factory Reset (сброс к заводским установкам)

Сбросьте настройки коммутатора к настройкам по умолчанию *reset config*

На коммутаторе восстановятся все заводские настройки по умолчанию, включая IP-адрес, учетные записи пользователей и журнал регистрации. Коммутатор не сохранит настройки и не перезагрузится.

reset system

На коммутаторе восстановятся все заводские настройки по умолчанию в полном объеме. Коммутатор сохранит эти настройки в энергонезависимой памяти и перезагрузится.

или

reset

На коммутаторе восстановятся все заводские настройки по умолчанию, исключая IP-адрес, учетные записи пользователей и журнал регистрации. Коммутатор не сохранит настройки и не перезагрузится.

reset force_agree

Параметр *force_agree* позволяет произвести безусловное выполнение команды *reset*. Не нужно вводить Y/N. На коммутаторе восстановятся все заводские настройки по умолчанию, исключая IP-адрес, учетные записи пользователей и журнал регистрации.

Сохраните изменения в энергонезависимую память

save

Перезагрузите коммутатор

reboot

Перезагрузите коммутатор с безусловным выполнением

reboot force_agree

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

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

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

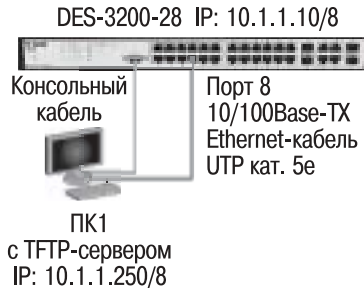
Оборудование:

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

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

reset config

Схема 1:

**1. Настройка DES-3200-28****1.1. Подготовка к режиму обновления и сохранения программного обеспечения коммутатора**

Настройте TFTP-сервер (на примере Tftpd32 by Ph.Jounin)

1. В настройках необходимо установить директорию приема файлов.
2. Отключить все другие сервисы, кроме TFTP server.

Подготовьте файл программного обеспечения

1. Найдите необходимый файл «прошивки» на сайте <ftp://ftp.dlink.ru>.
2. Скачайте файл и перенесите его в указанную директорию TFTP-сервера.
3. Прочитайте файл сопроводения к «прошивке».

1.2. Загрузка файла программного обеспечения в память коммутатора

Настройте IP-адрес интерфейса управления коммутатора

```
config ipif System vlan default  
ipaddress 10.1.1.10/8
```

Настройте TFTP-сервер

Задать IP-адрес рабочей станции с установленным TFTP-сервером:
10.1.1.250/8

Проверьте доступность соединения с TFTP-сервером

```
ping 10.1.1.250
```


Проверьте информацию о текущем программном обеспечении	<i>show firmware information</i>
Загрузите программное обеспечение на коммутатор	<i>download firmware_fromTFTP 10.1.1.250 des3200_runtime_v1.10.b021.had image_id 2</i>
Убедитесь, что программное обеспечение загружено	<i>show firmware information</i>

Внимание! НЕ перезагружайте коммутатор во время записи программного обеспечения.

Выполнение команды без ключа `image_id` приводит к перезаписи текущей версии программного обеспечения!

1.3. Настройка порядка загрузки программного обеспечения коммутатора

Измените программное обеспечение, которое будет загружаться при старте коммутатора	<i>config firmware image_id 2 boot_up</i>
Сохраните изменения	<i>Save</i>
Перезагрузите коммутатор. Обновленная прошивка вступит в силу только после перезагрузки	<i>Reboot</i>

Упражнения

Задание	Наблюдение
Проверьте информацию о программном обеспечении	<i>show firmware information</i>

Что вы наблюдаете?

1.4. Управление изменением конфигурации

Посмотрите текущую версию конфигурации коммутатора, хранящуюся в RAM	<i>show config current_config</i>
--	-----------------------------------

Посмотрите конфигурацию коммутатора, сохраненную в NVRAM	<i>show config config_in_nvram</i>
Выгрузите конфигурацию на TFTP-сервер	<i>upload cfg_toTFTP 10.1.1.250 config.txt</i>
Измените в разделе Management выгруженной конфигурации имя коммутатора с HQ-SW01 на HQ-SW02	<i># MANAGEMENT enable snmp traps enable snmp authenticate traps config snmp system_name HQ-SW02</i>
Загрузите измененную конфигурацию на коммутатор	<i>download cfg_fromTFTP 10.1.1.250 config.txt</i>
Проверьте, изменилось ли имя коммутатора	<i>show switch</i>

Что вы наблюдаете?

1.5. Выгрузка Log-файлов

Выгрузите Log-файл на TFTP-сервер	<i>upload log_toTFTP 10.1.1.250 logfiles.txt</i>
-----------------------------------	--

1.5.1. Выгрузка информации для технической поддержки (Tech_support)

Выгрузите файл tech_support на TFTP-сервер	<i>upload tech_support_toTFTP 10.1.1.250 support.txt</i>
--	--

Внимание! В файле support.txt содержится информация, позволяющая технической поддержке получить сведения о коммутаторе и выявить причину отказа или неправильной работы коммутатора.

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

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

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

Оборудование:

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

Схема 1:

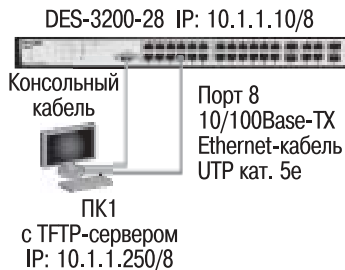
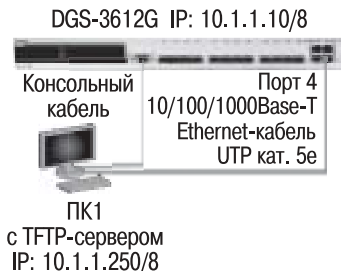


Схема 2:



1. Настройка DES-3200-28

1.1. Изучение команд просмотра таблиц MAC-адресов

Посмотрите таблицу MAC-адресов `show fdb`

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

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

Посмотрите список MAC-адресов устройств, принадлежащих VLAN по умолчанию `show fdb vlan default`

Посмотрите MAC-адреса устройств, изученные портом 16 `show fdb port 16`

Посмотрите время нахождения записи в таблице MAC-адресов `show fdb aging_time`

1.2. Изучение команд управления таблицей MAC-адресов

Создайте статическую запись в таблице MAC-адресов `create fdb default 00-00-00-00-01-02 port 5`

Удалите статическую запись из таблицы MAC-адресов `delete fdb default 00-00-00-00-01-02`

Измените время нахождения MAC-адреса в таблице до 350 секунд `config fdb aging_time 350`

Удалите все динамически созданные записи из таблицы MAC-адресов `clear fdb all`

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

Примечание. Данные команды выполняются только на коммутаторах уровня 3.

2.1. Изучение команд просмотра таблиц коммутации IP-адресов

Посмотрите таблицу коммутации IP-адресов *show ipfdb*

Найдите порт коммутатора, к которому подключено устройство с определенным IP-адресом *show ipfdb ip_address 10.1.1.250*

Упражнения

Задание	Наблюдение
---------	------------

Подключите станцию к любому порту коммутатора, как показано на схеме 1, и попробуйте найти по MAC-адресу порт подключения станции и наоборот.

Что вы наблюдаете?

3. Настройка DES-3200-28 /DGS-3612G (управление ARP-таблицами)

3.1. Изучение команд просмотра ARP-таблиц

Посмотрите ARP-таблицу *show arpentry*

Найдите в ARP-таблице сопоставления IP-MAC по указанному IP-адресу *show arpentry ipaddress 10.1.1.250*

Посмотрите в ARP-таблице все сопоставления IP-MAC на интерфейсе System *show arpentry ipif System*

3.2. Изучение команд управления ARP-таблицей

Создайте статическую запись в ARP-таблице *create arpentry 10.1.1.250 00-50-BA-00-07-36*

Удалите запись из ARP-таблицы *delete arpentry 10.1.1.250*

Измените время нахождения записи в ARP-таблице до 30 минут (по умолчанию – 20 минут) *config arp_aging time 30*

Удалите все динамически созданные записи из ARP-таблицы *clear arptable*

Упражнения

Задание

Наблюдение

Подключите станцию к любому порту коммутатора, как показано на схеме 1.

Попробуйте найти соответствие IP-МАС-адресов подключенной станции в ARP-таблице.

Что вы наблюдаете?

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

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

Типы VLAN:

- *VLAN на основе портов (Port-based VLAN)* – каждый порт коммутатора назначается в определенную VLAN и любое сетевое устройство, подключенное в данный порт, будет находиться в назначенной виртуальной сети;
- *VLAN на основе MAC-адресов (MAC-based VLAN)* – членство в VLAN основывается на MAC-адресе рабочей станции. В этом случае на коммутаторе необходимо создать привязку MAC-адресов всех устройств к VLAN;
- *VLAN на основе портов и протоколов IEEE 802.1p* – тип протокола используется для определения членства в VLAN;
- *VLAN на основе стандарта IEEE 802.1Q* – поле принадлежности VLAN, интегрируется в структуру кадра Ethernet, что позволяет передавать данную информацию по сети. Преимуществом является гибкость настройки, использование не только на одном коммутаторе, но и в пределах всей коммутируемой сети; возможность использования оборудования разных производителей при организации сети. Данный тип VLAN используется чаще остальных.

Существуют два метода назначения порта в определенную VLAN:

- статическое назначение — когда принадлежность порта VLAN задается администратором в процессе настройки;
- динамическое назначение — когда принадлежность порта VLAN определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как IEEE 802.1X. При использовании IEEE 802.1X для получения доступа к порту коммутатора пользователь проходит аутентификацию на сервере RADIUS. По результатам аутентификации порт коммутатора помещается в ту или иную VLAN.

Основные определения IEEE 802.1Q:

- *Tag* («Тег») — дополнительное поле данных длиной 4 байта, содержащее информацию о VLAN и добавляемое в кадр Ethernet. Первые 2 байта содержат фиксированное значение 0x8100, остальные 2 байта содержат идентификатор VLAN (12 бит), поле приоритета (3 бита), поле индикатора канонического формата (1 бит);
- *Tagging* («Маркировка кадра») — процесс добавления информации (тега) о принадлежности к 802.1Q VLAN в заголовок кадра;
- *Untagging* («Удаление тега из кадра») — процесс извлечения информации 802.1Q VLAN из заголовка кадра;
- *Ingress port* («Входной порт») — порт коммутатора, на который поступают кадры, и принимается решение о принадлежности VLAN;
- *Egress port* («Выходной порт») — порт коммутатора, с которого кадры передаются на другие сетевые устройства (коммутаторы, рабочие станции), и на нем, соответственно, принимается решение о маркировке кадра.

Любой порт коммутатора может быть настроен как *tagged* (маркированный) или как *untagged* (немаркированный). Функция *untagging* позволяет работать с теми сетевыми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать VLAN между несколькими коммутаторами, поддерживающими стандарт IEEE 802.1Q, подключать сетевые устройства, понимающие IEEE 802.1Q (например, серверы с сетевыми интерфейсами с поддержкой 802.1Q), обеспечивать возможность создания сложных сетевых инфраструктур.

В данной лабораторной работе рассматриваются примеры использования и настройки VLAN.

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

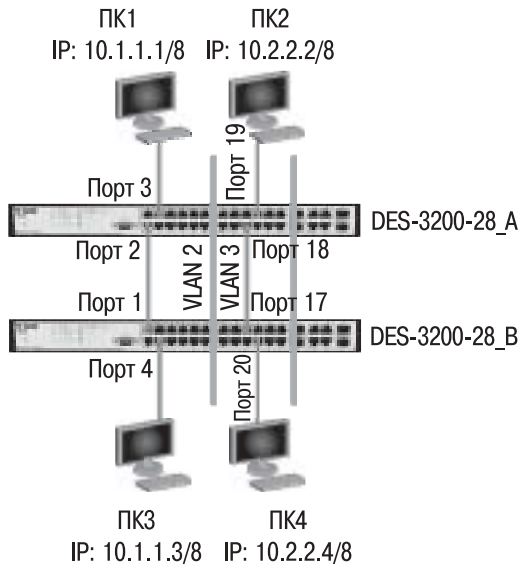
Оборудование:

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

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

1. Настройка VLAN на основе портов

Схема 1:



1.1. Настройка DES-3200-28_A

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

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными

```
create vlan v2 tag 2
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-24
```

1.2. Настройка DES-3200-28_B

Удалите порты из VLAN по умолчанию для использования в других VLAN

```
config vlan default delete 1-24
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными

```
create vlan v2 tag 2
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-24
```

Упражнения

Задание

Наблюдение

Проверьте настройки VLAN на обоих коммутаторах

```
show vlan
```

Проверьте доступность соединения командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК3
- от ПК2 к ПК4
- от ПК1 к ПК2 и ПК4
- от ПК2 к ПК1 и ПК3

2. Настройка VLAN на основе стандарта IEEE 802.1Q

2.1. Настройка DES-3200-28_A

Сбросьте настройки коммутатора к заводским настройкам по умолчанию

```
reset config
```

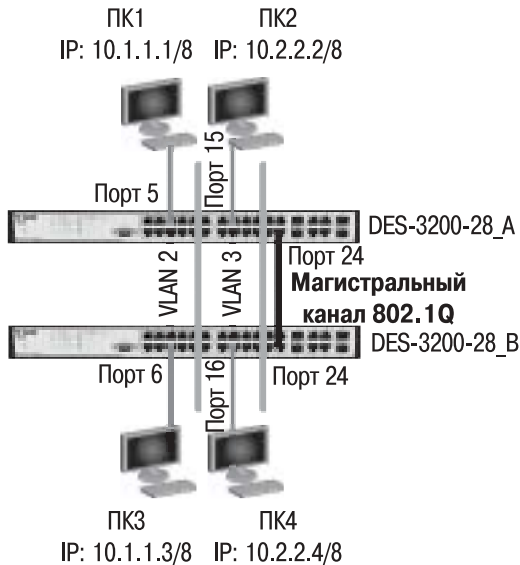
Удалите порты из VLAN по умолчанию для использования в других VLAN

```
config vlan default delete 1-24
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными

```
create vlan v2 tag 2
config vlan v2 add untagged 1-10
config vlan v2 add tagged 24
```

Схема 2:



Настройте порт 24 маркированным

```
create vlan v3 tag 3
config vlan v3 add untagged 11-20
config vlan v3 add tagged 24
```

2.2. Настройка DES-3200-28_B

Сбросьте настройки коммутатора к заводским настройкам по умолчанию

```
reset config
```

Удалите порты из VLAN по умолчанию для использования в других VLAN

```
config vlan default delete 1-24
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными.

```
create vlan v2 tag 2
config vlan v2 add untagged 1-10
config vlan v2 add tagged 24
```

Настройте порт 24 маркированным

```
create vlan v3 tag 3
config vlan v3 add untagged 11-20
config vlan v3 add tagged 24
```

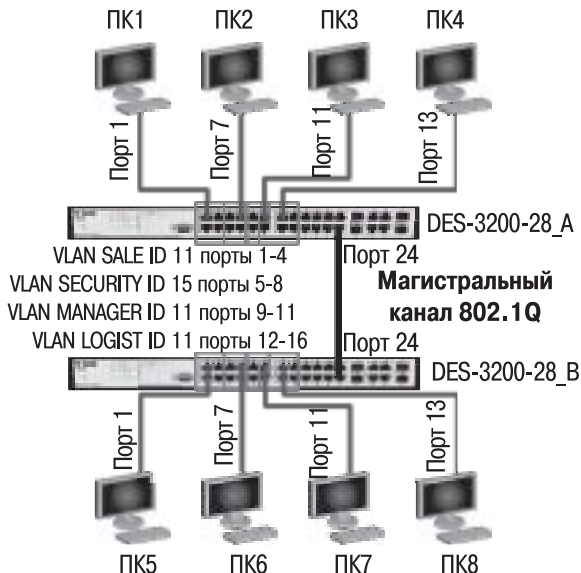
Упражнения

Задание Проверьте настройку VLAN на обоих коммутаторах	Наблюдение <i>show vlan</i>
Проверьте доступность соединения командой ping: – от ПК1 к ПК3 – от ПК2 к ПК4 – от ПК1 к ПК2 и ПК4 – от ПК2 к ПК1 и ПК3	<i>ping <IP-address></i>

3. Оптимизация настройки коммутаторов с большим количеством VLAN

Целью данного задания является изучение команд оптимизации работы при создании, удалении, конфигурировании множества VLAN.

Схема 3:



3.1. Настройка DES-3200-28_A

Сбросьте настройки коммутатора к заводским настройкам по умолчанию	<i>reset config</i>
Удалите порты из VLAN по умолчанию для использования в других VLAN	<i>config vlan vlanid 1 delete 1-24</i>
Создайте двадцать VLAN с тегами с 2 по 21	<i>create vlan vlanid 2-21</i>
<p>Примечание. При создании VLAN имена присваиваются по шаблону: VLAN x (где x – тег создаваемой VLAN).</p>	
Добавьте маркированные порты в несколько VLAN, включите функцию оповещения (advertisement) о созданных VLAN	<i>config vlan vlanid 2-21 add tagged 1-24 advertisement enable</i>
Проверьте выполненные действия	<i>show vlan</i>
<p>Что вы наблюдаете? Запишите:</p>	
Удалите порты из нескольких VLAN	<i>config vlan vlanid 2-21 delete 1-24</i>
Измените имя VLAN и добавьте немаркированные порты	<i>config vlan vlanid 11 name SALE add untagged 1-4</i> <i>config vlan vlanid 15 name SECURITY add untagged 5-8</i> <i>config vlan vlanid 18 name MANAGER add untagged 9-11</i> <i>config vlan vlanid 19 name LOGIST add untagged 12-16</i>
Проверьте выполненные действия	<i>show vlan</i>
<p>Что вы наблюдаете? Запишите:</p>	
Назначьте магистральный порт передачи VLAN	<i>config vlan_trunk ports 24 state enable</i>

Проверьте выполненные действия *show vlan_trunk*

Включите возможность работы магистрального порта *enable vlan_trunk*

Внимание! При настройке порта в качестве магистрального (*vlan_trunk*) через него можно передавать кадры с VID с 1-4094; порт динамически добавляется во все доступные VLAN как маркированный!

3.2. Настройка DES-3200-28_V

Сбросьте настройки коммутатора к заводским настройкам по умолчанию *reset config*

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

Создайте десять VLAN с тегами с 10 по 19 *create vlan vlanid 10-19*

Измените имя VLAN и добавьте немаркированные порты *config vlan vlanid 11 name SALE add untagged 1-4*
config vlan vlanid 15 name SECURITY add untagged 5-8
config vlan vlanid 18 name MANAGER add untagged 9-11
config vlan vlanid 19 name LOGIST add untagged 12-16

Проверьте выполненные действия *show vlan*

Что вы наблюдаете? Запишите:

Назначьте магистральный порт передачи VLAN *config vlan_trunk ports 24 state enable*

Включите возможность работы магистрального порта *enable vlan_trunk*

Проверьте выполненные действия *show vlan_trunk*

Проверьте доступность соединения командой ping: *ping <IP-address>*

- от ПК1 к ПК2 (Vlan SALE)
- от ПК3 к ПК4 (Vlan SECURITY)
- от ПК5 к ПК6 (Vlan MANAGER)
- от ПК7 к ПК8 (Vlan LOGIST)
- между станциями соседних VLAN

Что вы наблюдаете? Запишите:

Отключите магистральные порты на коммутаторах А и В *disable vlan_trunk*

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

Существуют два основных способа, позволяющих устанавливать членство в VLAN:

- статические VLAN;
- динамические VLAN.

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

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

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

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

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

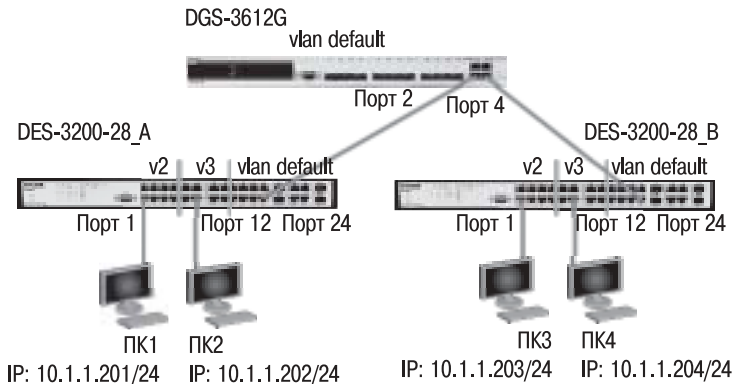
Оборудование:

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

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

reset config

Схема 1:



1. Настройка VLAN

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

Удалите порты из VLAN по умолчанию для использования в других VLAN

```
config vlan default delete 1-16
```

Создайте VLAN v2, добавьте в нее порты, которые необходимо настроить немаркированными. Настройте порт 24 маркированным

```
create vlan v2 tag 2
config vlan v2 add untagged 1-8
config vlan v2 add tag 24
```

Создайте VLAN v3, добавьте в нее порты, которые необходимо настроить немаркированными. Настройте порт 24 маркированным

```
create vlan v3 tag 3
config vlan v3 add untagged 9-16
config vlan v3 add tag 24
```

Настройте оповещение о VLAN v2 и v3

```
config vlan v2 advertisement enable
config vlan v3 advertisement enable
```

Включите работу протокола GVRP

```
enable gvrp
```

Установите возможность приема и отправки информации о VLAN через порт 24 коммутатора

```
config gvrp 24 state enable
```

1.2. Настройка DGS-3612G

Включите работу протокола GVRP *enable gvrp*

Установите возможность приема *config gvrp all state enable*
и отправки информации о VLAN

- типовую **через все порты коммутатора**
- ♦

Внимание! При динамической передаче информации о VLAN через магистральные коммутаторы рекомендуется передавать информацию только о пользовательских VLAN, а служебные VLAN и управляющие VLAN настраивать на магистральных коммутаторах статически.

Упражнения

Задание	Наблюдение
---------	------------

Проверьте состояние GVRP на портах всех коммутаторов	<i>show gvrp</i>
--	------------------

Проверьте настройки VLAN на коммутаторе DGS-3612G	<i>show vlan</i>
---	------------------

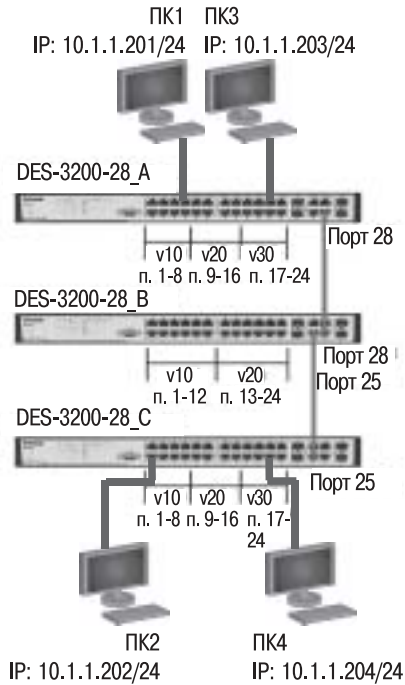
Что вы наблюдаете? Запишите:

Проверьте доступность соединения командой <i>ping</i> :	<i>ping <IP-address></i>
---	--------------------------------

- от ПК1 к ПК2
- от ПК1 к ПК3
- от ПК2 к ПК4

Могут ли рабочие станции взаимодействовать друг с другом?

Схема 2:



2. Настройка VLAN

2.1. Настройка DES- 3200-28_A и DES-3200-28_C

Сбросьте настройки коммутатора к заводским настройкам по умолчанию *reset config*

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

Создайте VLAN v10, добавьте в нее порты, которые необходимо настроить немаркированными *create vlan v10 tag 10*
config vlan v10 add untagged 1-8

Создайте VLAN v20, добавьте в нее порты, которые необходимо настроить немаркированными *create vlan v20 tag 20*
config vlan v20 add untagged 9-16

Создайте VLAN v30, добавьте в нее порты, которые необходимо настроить немаркированными	<i>create vlan v30 tag 30 config vlan v30 add untagged 17-24</i>
Добавьте магистральные порты как маркированные в созданные VLAN	<i>config vlan v10 add tag 25-26 config vlan v20 add tag 25-26 config vlan v30 add tag 25-26</i>
Настройте оповещение о VLAN v10, v20 и v30	<i>config vlan v10 advertisement enable config vlan v20 advertisement enable config vlan v30 advertisement enable</i>
Включите работу протокола GVRP	<i>enable gvrp</i>
Установите возможность приема и отправки информации о VLAN через порты 25 и 26	<i>config gvrp 25-26 state enable</i>

2.2. Настройка DES-3200-28_B

Сбросьте настройки коммутатора к заводским настройкам по умолчанию	<i>reset config</i>
Удалите порты из VLAN по умолчанию для использования в других VLAN	<i>config vlan default delete 1-24</i>
Создайте VLAN v10, добавьте в нее порты, которые необходимо настроить немаркированными	<i>create vlan v10 tag 10 config vlan v10 add untagged 1-12</i>
Создайте VLAN v20, добавьте в нее порты, которые необходимо настроить немаркированными	<i>create vlan v20 tag 20 config vlan v20 add untagged 13-24</i>
Добавьте магистральные порты как маркированные в созданные VLAN	<i>config vlan v10 add tag 25-26 config vlan v20 add tag 25-26</i>
Настройте оповещение о VLAN v10 и v20	<i>config vlan v10 advertisement enable config vlan v20 advertisement enable</i>
Включите работу протокола GVRP	<i>enable gvrp</i>

Установите возможность приема и отправки информации о VLAN через порты 25 и 26

config gvrp 25-26 state enable

Внимание! При динамической передаче информации о VLAN через магистральные коммутаторы рекомендуется передавать информацию только о пользовательских VLAN, а служебные VLAN и управляющие VLAN настраивать на магистральных коммутаторах статически.

Упражнения

Задание	Наблюдение
----------------	-------------------

Проверьте состояние GVRP на портах всех коммутаторов	<i>show gvrp</i>
--	------------------

Проверьте настройки VLAN на всех коммутаторах	<i>show vlan</i>
---	------------------

Что вы наблюдаете? Запишите:

Проверьте доступность соединения командой ping:	<i>ping <IP-address></i>
---	--------------------------------

- от ПК1 к ПК2
- от ПК1 к ПК 3
- от ПК2 к ПК 4
- от ПК3 к ПК 4

Могут ли рабочие станции взаимодействовать друг с другом?

Занятие №6. Команды настройки асимметричных VLAN и сегментации трафика

Применение асимметричных VLAN (Asymmetric VLAN)

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

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

Применение сегментации трафика (Traffic Segmentation)

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

Цель: Изучить настройку асимметричных VLAN и сегментации трафика.

Оборудование:

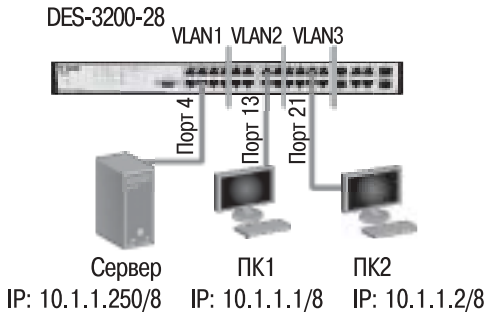
DES-3200-28	2 шт.
Рабочая станция	4 шт.
Кабель Ethernet	5 шт.
Консольный кабель	2 шт.

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

reset config

1. Настройка асимметричных VLAN (Пример 1)

Схема 1:



1.1. Настройка DES- 3200-28

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

Включите функцию асимметричных VLAN *enable asymmetric_vlan*

Проверьте, все ли порты назначены в VLAN по умолчанию? *show vlan*

Создайте VLAN v2 и v3 *create vlan v2 tag 2*
create vlan v3 tag 3

Добавьте в созданные VLAN немаркированные порты *config vlan v2 add untagged 1-16*
config vlan v3 add untagged 1-8, 17-24

Назначьте PVID немаркированным портам, созданных VLAN *config gvrp 1-8 pvid 1*
config gvrp 9-16 pvid 2
config gvrp 17-24 pvid 3

Упражнения

Задание

Наблюдение

Проверьте доступность соединения командой `ping`:

`ping <IP-address>`

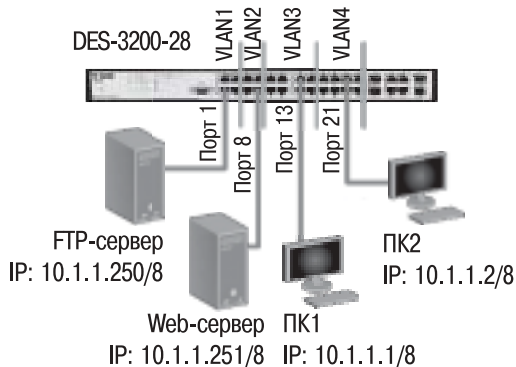
- от ПК1 к серверу
- от ПК2 к серверу
- от ПК1 к ПК2
- от ПК2 к ПК1

Проверьте состояние PVID на всех портах коммутатора

`show vgrp`

2. Настройка асимметричных VLAN (Пример 2)

Схема 2:



2.1. Настройка DES-3200-28

Сбросьте настройки коммутатора к заводским настройкам по умолчанию

`reset config`

Включите функцию асимметричных VLAN

`enable asymmetric_vlan`

Проверьте, все ли порты назначены в VLAN по умолчанию?

`show vlan`

Создайте VLAN v2, v3, v4

```
create vlan v2 tag 2
create vlan v3 tag 3
create vlan v4 tag 4
```

Добавьте в созданные VLAN немаркированные порты

```
config vlan v2 add untagged 5-8,17-24
config vlan v3 add untagged 1-4,9-16
config vlan v4 add untagged 1-8,17-24
```

Назначьте PVID немаркированным портам созданных VLAN

```
config gvrp 1-4 pvid 1
config gvrp 5-8 pvid 2
config gvrp 9-16 pvid 3
config gvrp 17-24 pvid 4
```

Упражнения

Задание

Наблюдение

Проверьте доступность соединения командой ping:

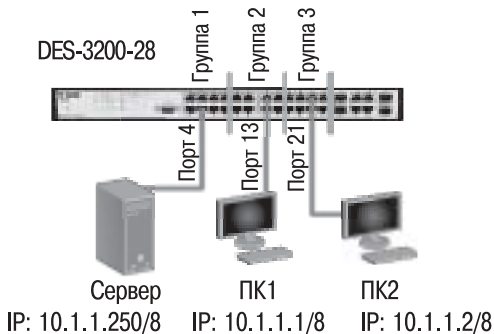
```
ping <IP-address>
```

- от ПК1 (VLAN3) к FTP (VLAN1)
- от ПК2 (VLAN4) к FTP (VLAN1)
- от ПК1 (VLAN3) к Web (VLAN2)
- от ПК2 (VLAN4) к Web (VLAN2)
- от FTP (VLAN1) к Web (VLAN2)
- от ПК1 (VLAN3) к ПК2 (VLAN4)

3. Настройка сегментации трафика (пример 1)

В данном задании выполняется настройка сегментации трафика, которая позволит рабочим станциям из групп 2 и 3 получить доступ к серверу из группы 1. При этом обмен данными между устройствами групп 2 и 3 запрещен.

Схема 3:



3.1. Настройка DES-3200-28

Сбросьте настройки коммутатора к заводским настройкам по умолчанию *reset config*

Настройте сегментацию трафика *config traffic_segmentation 1-8*
forward_list 1-24
config traffic_segmentation 9-16
forward_list 1-16
config traffic_segmentation 17-24
forward_list 1-8,17-24

Упражнение

Задание **Наблюдение**

Проверьте настройки *show traffic_segmentation*

Проверьте доступность соединения командой *ping*: *ping <IP-address>*

- от ПК1 (группа 2) к серверу (группа 1)
- от ПК2 (группа 3) к серверу (группа 1)
- от ПК1 (группа 2) к ПК2 (группа 3)

4. Настройка сегментации трафика (пример 2)

В данном задании выполняется настройка сегментации трафика на двух коммутаторах, позволяющая разным группам получать доступ к совместно используемому серверу, но запрещающая доступ друг к другу.

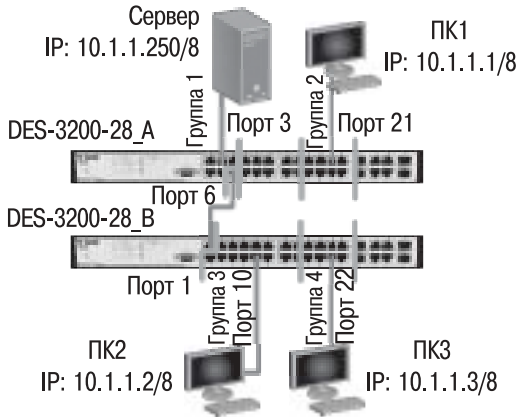
4.1. Настройка DES-3200-28_A

Сбросьте настройки коммутатора к заводским настройкам по умолчанию

reset config

Настройте сегментацию трафика *config traffic_segmentation 1-5*
forward_list 1-24
config traffic_segmentation 6
forward_list 1-6
config traffic_segmentation 7-16
forward_list 1-5,7-16
config traffic_segmentation 17-24
forward_list 1-5,17-24

Схема 4:



4.2. Настройка DES-3200-28_B

Сбросьте настройки коммутатора к заводским настройкам по умолчанию `reset config`

Настройте сегментацию трафика

```
config traffic_segmentation 1 forward_list 1-24
config traffic_segmentation 2-16 forward_list 1-16
config traffic_segmentation 17-24 forward_list 1,17-24
```

Упражнения

Задание

Наблюдение

Проверьте настройки
Проверьте доступность соединения командой `ping`:

```
show traffic_segmentation
ping <IP-address>
```

- от ПК1 (группа 2) к серверу (группа 1)
- от ПК2 (группа 3) к серверу (группа 1)
- от ПК3 (группа 4) к серверу (группа 1)
- от ПК1 (группа 2) к ПК2 (группа 3)
- от ПК2 (группа 3) к ПК3 (группа 4)
- от ПК3 (группа 4) к ПК1 (группа 2)

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

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

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

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

Функция Q-in-Q позволяет расширить доступное пространство идентификаторов и использовать до $4094 \times 4094 = 16\,760\,836$ уникальных виртуальных локальных сетей.

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

Роли портов в Port-based Q-in-Q

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

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

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

Оборудование:

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

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

reset config

Настройка функции Port-based Q-in-Q

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

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

Создайте VLAN v2, v3, v4 *create vlan v2 tag 2*
create vlan v3 tag 3
create vlan v4 tag 4

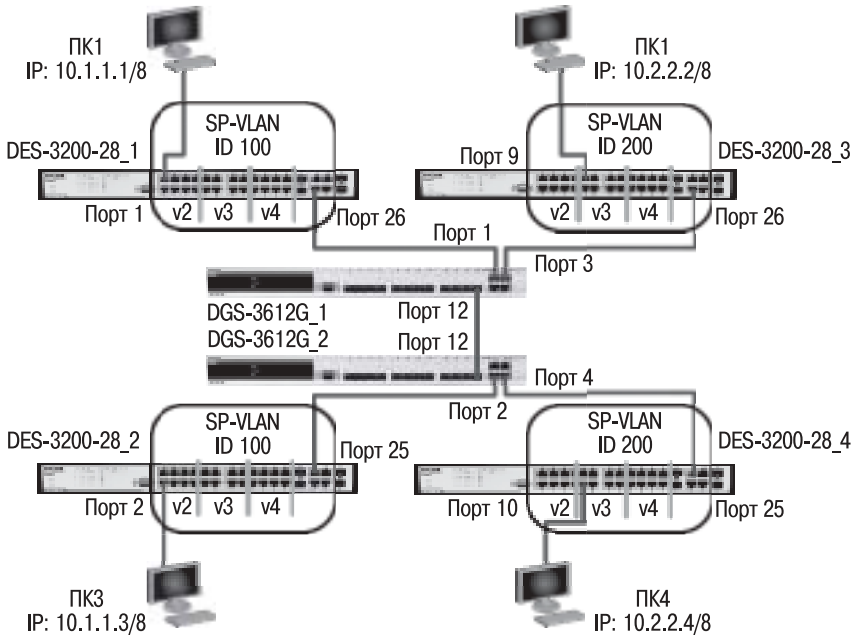
Добавьте в VLAN v2 порты 1-8 как немаркированные *config vlan v2 add untagged 1-8*

Добавьте в VLAN v3 порты 9-16 как немаркированные *config vlan v3 add untagged 9-16*

Добавьте в VLAN v4 порты 17-24 как немаркированные *config vlan v4 add untagged 17-24*

Добавьте магистральные порты 25 и 26 как маркированные в VLAN v2, v3, v4 *config vlan v2 add tagged 25-26*
config vlan v3 add tagged 25-26
config vlan v4 add tagged 25-26

Схема 1:



2. Настройка DGS-3612G_1 (остальные коммутаторы данной серии настраиваются аналогично)

Включите функцию Q-in-Q

```
enable qinq
```

Удалите порты из Q-in-Q VLAN по умолчанию

```
config vlan default delete 1-12
```

Создайте Q-in-Q VLAN с SP-VLAN ID, равным d100, для первого клиента

```
create vlan d100 tag 100
```

Создайте Q-in-Q VLAN с SP-VLAN ID, равным d200, для второго клиента

```
create vlan d200 tag 200
```

Настройте порты доступа в Q-in-Q VLAN d100

```
config vlan d100 add untagged 1-2
```

Настройте порты доступа в Q-in-Q VLAN d200	<i>config vlan d200 add untagged 3-4</i>
Настройте порт 12 как Uplink-порт в Q-in-Q VLAN d100 и d200	<i>config vlan d100 add tagged 12 config vlan d200 add tagged 12</i>
Настройте роли портов доступа и отключите режим Missdrop на них	<i>config qinq ports 1-4 role uni missdrop disable</i>

Упражнения

Задание	Наблюдение
Проверьте доступность соединения командой ping: – от ПК1 к ПК2 – от ПК3 к ПК4 – от ПК1 к ПК3 – от ПК2 к ПК4	<i>ping <IP-address></i>
Проверьте настройку функции Q-in-Q	<i>qinq ports all</i>

Что вы наблюдаете? Запишите:

Внимание! В теге VLAN имеется поле идентификатора протокола тега (Tag Protocol Identifier, TPID), которое определяет тип протокола тега. По умолчанию значение этого поля для стандарта IEEE 802.1Q равно 0x8100.

На устройствах разных производителей TPID внешнего тега VLAN кадров Q-in-Q может иметь разные значения по умолчанию. Для того чтобы кадры Q-in-Q могли передаваться по общедоступным сетям через устройства разных производителей, рекомендуется использовать значение TPID внешнего тега, равное 0x88A8, согласно стандарту IEEE 802.1ad.

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

Протокол Spanning Tree Protocol (STP).

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

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

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

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

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

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

Протокол Rapid Spanning Tree Protocol (RSTP).

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

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

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

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

Протокол Multiple Spanning Tree Protocol (MSTP).

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

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

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

Внутри коммутируемой сети может быть создано множество MST-регионов.

Протокол MSTP определяет следующие типы связующих деревьев:

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

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

Вычисления в MSTP

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

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

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

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

Роли портов

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

Счетчик переходов MSTP

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

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

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

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

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

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

Оборудование:

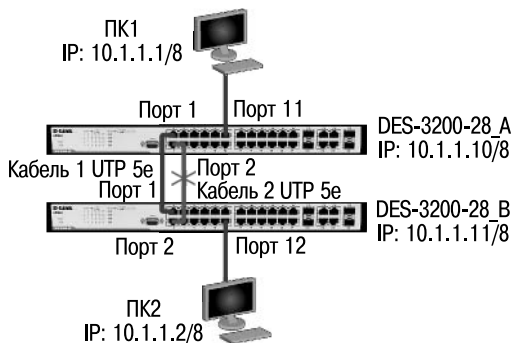
DES-3200-28	2 шт.
Рабочая станция	4 шт.
Кабель Ethernet	8 шт.
Консольный кабель	2 шт.

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

reset config

1. Настройка протокола RSTP (IEEE 802.1w)

Схема 1:



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

1.1. Настройка DES-3200-28_A

Настройте IP-адрес интерфейса управления коммутатора *config ipif System ipaddress 10.1.1.10/8*

Включите протокол связующего дерева на коммутаторе *enable stp*

Проверьте текущую конфигурацию протокола связующего дерева *show stp*

Протокол RSTP используется по умолчанию после активизации протокола связующего дерева. Если нет, включите его *config stp version rstp*

Установите на коммутаторе наименьшее значение приоритета, чтобы он мог быть выбран корневым мостом (приоритет по умолчанию = 32768) *config stp priority 4096 instance_id 0*

Назначьте порты 5-24 граничными портами *config stp ports 5-24 edge true*

Активизируйте протокол связующего дерева на портах *config stp ports 1-24 state enable*

1.2. Настройка DES-3200-28_B

Настройте IP-адрес управляющего интерфейса коммутатора *config ipif System ipaddress 10.1.1.11/8*

Включите протокол связующего дерева на коммутаторе *enable stp*

Проверьте текущую конфигурацию протокола связующего дерева *show stp*

Протокол RSTP используется по умолчанию после активизации протокола связующего дерева. Если нет, включите его *config stp version rstp*

Назначьте порты 5-24 граничными портами `config stp ports 5-24 edge true`

Активизируйте протокол связующего дерева на портах `config stp ports 1-24 state enable`

Соедините между собой порты 1 и порты 2 коммутаторов А и В с помощью кабелей, как показано на схеме 1.

Упражнения

Задание	Наблюдение
----------------	-------------------

Проверьте настройки RSTP, состояние портов и их роли у обоих коммутаторов	<code>show stp ports</code>
---	-----------------------------

Вопросы:

Какой коммутатор является корневым?

Какие порты являются заблокированными?

Какая роль у заблокированных портов?

Выполните продолжительный ping от компьютера ПК1 до ПК2 и наоборот	На ПК1, <code>ping 10.1.1.2 -t</code> На ПК2, <code>ping 10.1.1.1 -t</code>
--	--

Отсоедините кабель от корневого порта.

Что происходит с тестом ping?

Превышен ли интервал ожидания для запроса?

Как долго пришлось ждать появления ответа?

Проверьте состояние заблокированных портов.

Поменяйте RSTP на STP	<code>config stp version stp</code>
------------------------------	-------------------------------------

Выполните повторно продолжительный ping от компьютера ПК1 до ПК2 и наоборот	На ПК1, <code>ping 10.1.1.2 -t</code> На ПК2, <code>ping 10.1.1.1 -t</code>
---	--

Отсоедините кабель от корневого порта.

Что происходит с тестом ping?

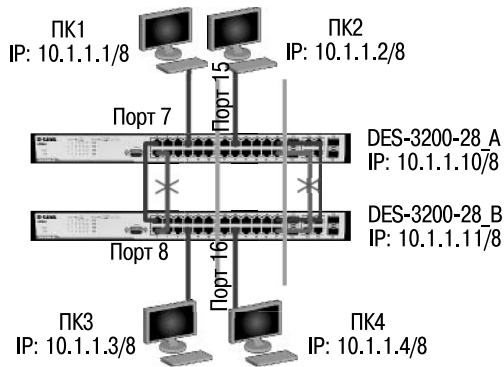
Превышен ли интервал ожидания для запроса?

Как долго пришлось ждать появления ответа?

Проверьте состояние заблокированного порта.

2. Настройка протокола MSTP (IEEE 802.1s) для каждой VLAN

Схема 2:



2.1. Настройка DES-3200-28_A

Сбросьте настройки коммутатора к заводским настройкам по умолчанию *reset config*

Настройте IP-адрес интерфейса управления коммутатора *config ipif System ipaddress 10.1.1.10/8*

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

Создайте VLAN v2 и v3 и добавьте в каждую из них немаркированные порты *create vlan v2 tag 2*
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-24

Включите протокол связующего дерева на коммутаторе	<i>enable stp</i>
Проверьте текущую конфигурацию STP на портах коммутатора	<i>show stp ports</i>
Измените версию STP на MSTP (по умолчанию используется RSTP).	<i>config stp version mstp</i>
Настройте имя MST-региона и ревизию	<i>config stp mst_config_id name abc config stp mst_config_id revision_level 1</i>
Создайте две MSTI и карту привязки VLAN к MSTI	<i>create stp instance_id 2 config stp instance_id 2 add_vlan 2 create stp instance_id 3 config stp instance_id 3 add_vlan 3</i>
Настройте приоритет STP так, чтобы коммутатор был выбран корневым мостом (приоритет по умолчанию 32768) в каждой MSTI	<i>config stp priority 4096 instance_id 0 config stp priority 4096 instance_id 2 config stp priority 4096 instance_id 3</i>
Настройте порты 1-10 и 13-22 как граничные порты	<i>config stp ports 1-10 edge true config stp ports 13-22 edge true</i>
Активизируйте протокол связующего дерева на портах	<i>config stp ports 1-24 state enable</i>

2.2. Настройка DES-3200-28_B

Сбросьте настройки коммутатора к заводским настройкам по умолчанию	<i>reset config</i>
Настройте IP-адрес интерфейса управления коммутатора	<i>config ipif System ipaddress 10.1.1.11/8</i>
Удалите порты из VLAN по умолчанию для использования в других VLAN	<i>config vlan default delete 1-24</i>
Создайте VLAN v2 и v3 и добавьте в каждую из них немаркированные порты	<i>create vlan v2 tag 2 config vlan v2 add untagged 1-12 create vlan v3 tag 3 config vlan v3 add untagged 13-24</i>

Включите протокол связующего дерева *enable stp*
на коммутаторе

Проверьте доступность соединения *ping <IP-address>*
между рабочими станциями
командой *ping*

Может ли ПК1 получить доступ к ПК3 из той же VLAN?

Может ли ПК2 получить доступ к ПК4 из той же VLAN?

Проверьте текущую конфигурацию *show stp ports*
STP на портах коммутатора

Измените версию STP на MSTP *config stp version mstp*
(по умолчанию используется RSTP)

Настройте имя MST-региона *config stp mst_config_id name abc*
и ревизию *config stp mst_config_id revision_level 1*

Создайте две MSTI и карту привязки *create stp instance_id 2*
VLAN к MSTI *config stp instance_id 2 add_vlan 2*
create stp instance_id 3
config stp instance_id 3 add_vlan 3

Настройте порты 1-10 и 13-22 как *config stp ports 1-10 edge true*
граничные порты *config stp ports 13-22 edge true*

Активизируйте протокол связующего *config stp ports 1-24 state enable*
дерева на портах

Подключите кабели как показано на схеме 2. Используйте порты 11 и 12 для VLAN 2, порты 23 и 24 для VLAN 3.

Упражнения

Задание

Наблюдение

Проверьте доступность соединения *ping <IP-address>*
командой *ping*:
– от ПК1 к ПК3
– от ПК2 к ПК4

- от ПК1 к ПК2
- от ПК3 к ПК4
- от ПК1 к ПК4
- от ПК3 к ПК2

Проверьте текущую конфигурацию `show stp ports`
 STP на портах коммутатора

Какие порты являются корневым и альтернативным для VLAN v2?

Какие порты являются корневым и альтернативным для VLAN v3?

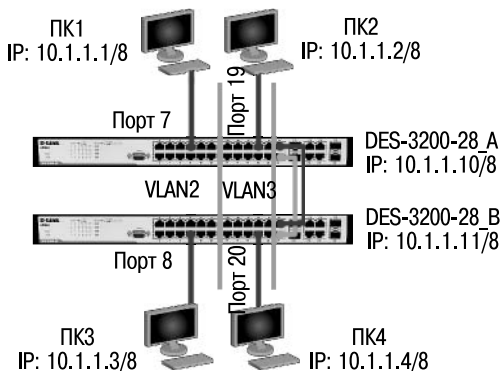
Какие порты являются назначенными для VLAN v2?

Какие порты являются назначенными для VLAN v3?

Какой вы сделаете вывод по поводу связи между корневым мостом и корневыми портами?

3. Настройка протокола MSTP (IEEE 802.1s) для балансировки нагрузки

Схема 3:



3.1. Настройка DES-3200-28_A

Сбросьте настройки коммутатора `reset config`
 к заводским настройкам по умолчанию

Настройте IP-адрес интерфейса управления коммутатора	<i>config ipif System ipaddress 10.1.1.10/8</i>
Удалите порты из VLAN по умолчанию для использования в других VLAN	<i>config vlan default delete 1-22</i>
Создайте VLAN v2 и v3 и добавьте в каждую из них немаркированные и маркированные порты	<i>create vlan v2 tag 2 config vlan v2 add untagged 1-10 config vlan v2 add tagged 23-24 create vlan v3 tag 3 config vlan v3 add untagged 11-22 config vlan v3 add tagged 23-24</i>
Включите протокол связующего дерева на коммутаторе	<i>enable stp</i>
Измените версию STP на MSTP (по умолчанию используется RSTP)	<i>config stp version mstp</i>
Настройте имя MST-региона и ревизию	<i>config stp mst_config_id name abc config stp mst_config_id revision_level 1</i>
Создайте две MSTI и карту привязки VLAN к копии MSTI	<i>create stp instance_id 2 config stp instance_id 2 add_vlan 2 create stp instance_id 3 config stp instance_id 3 add_vlan 3</i>
Настройте приоритет STP так, чтобы коммутатор был выбран корневым мостом (приоритет по умолчанию 32768) в каждой MSTI	<i>config stp priority 4096 instance_id 0 config stp priority4096 instance_id 2 config stp priority4096 instance_id 3</i>
Задайте приоритет порта, так чтобы порт 23 был активным портом для VLAN v2, а порт 24 – активным портом для VLAN v3	<i>config stp mst_ports 23 instance_id 2 priority 96 config stp mst_ports 24 instance_id 3 priority 96</i>
Настройте порты 1-22 как граничные порты	<i>config stp ports 1-22 edge true</i>
Активизируйте протокол связующего дерева на портах	<i>config stp ports 1-24 state enable</i>

3.2. Настройка DES-3200-28_B

Сбросьте настройки коммутатора к заводским настройкам по умолчанию	<i>reset config</i>
Настройте IP-адрес интерфейса управления коммутатора	<i>config ipif System ipaddress 10.1.1.11/8</i>
Удалите порты из VLAN по умолчанию для использования в других VLAN	<i>config vlan default delete 1-22</i>
Создайте VLAN v2 и v3 и добавьте в каждую из них немаркированные и маркированные порты	<i>create vlan v2 tag 2 config vlan v2 add untagged 1-10 config vlan v2 add tagged 23-24 create vlan v3 tag 3 config vlan v3 add untagged 11-22 config vlan v3 add tagged 23-24</i>
Включите протокол связующего дерева на коммутаторе	<i>enable stp</i>
Измените версию STP на MSTP (по умолчанию используется RSTP)	<i>config stp version mstp</i>
Настройте имя MST-региона и ревизию	<i>config stp mst_config_id name abc config stp mst_config_id revision_level 1</i>
Создайте две MSTI и карту привязки VLAN к MSTI	<i>create stp instance_id 2 config stp instance_id 2 add_vlan 2 create stp instance_id 3 config stp instance_id 3 add_vlan 3</i>
Настройте порты 1-22 как граничные порты	<i>config stp ports 1-22 edge true</i>
Активируйте протокол связующего дерева на портах	<i>config stp ports 1-24 state enable</i>

Упражнения

Задание

Наблюдение

Проверьте доступность соединения командой `ping`:

- от ПК1 к ПК3
- от ПК2 к ПК4
- от ПК1 к ПК2
- от ПК3 к ПК4
- от ПК1 к ПК4
- от ПК3 к ПК2

`ping <IP-address>`

Проверьте текущую конфигурацию STP на портах коммутатора

`show stp ports`

Какие порты являются корневым и альтернативным для VLAN v2?

Какие порты являются корневым и альтернативным для VLAN v3?

Какие порты являются назначенными для VLAN v2?

Какие порты являются назначенными для VLAN v3?

Отсоедините кабель от корневого порта для VLAN v2.

Проверьте доступность соединения командой `ping`:

- от ПК1 к ПК3
- от ПК2 к ПК4

`ping <IP-address>`

Какие выводы вы сделаете из выполненных ping-тестов?

Занятие №9. Функция предотвращения петлеобразования (LoopBack Detection)

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

- STP LoopBack Detection;
- LoopBack Detection Independent STP.

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

Функция LoopBack Detection Independent STP не требует настройки протокола STP на портах, на которых необходимо определять наличие петли. В этом случае наличие петли обнаруживается путем отправки портом специального служебного кадра ECTP (Ethernet Configuration Testing Protocol). При получении кадра ECTP этим же портом он блокируется на указанное в таймере время. Начиная с LBD версии 4.03, функция LoopBack Detection Independent STP также может определять петли, возникающие между портами одного коммутатора. Существуют два режима работы этой функции: Port-Based и VLAN-Based (начиная с LBD версии v4.00).

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

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

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

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

Оборудование:

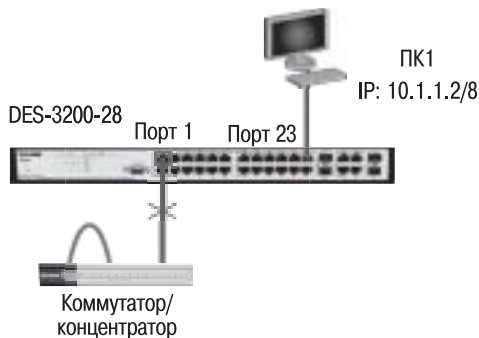
DES-3200-28	2 шт.
DES-1005D	1 шт.
Рабочая станция	4 шт.
Кабель Ethernet	7 шт.
Консольный кабель	2 шт.

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

reset config

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

Схема 1:



1.1. Настройка DES-3200-28

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

Включите функцию LBD глобально на коммутаторе *enable loopdetect*

Активизируйте функцию LBD на всех портах коммутатора *config loopdetect ports 1-28 state enabled*

Сконфигурируйте режим Port-Based, чтобы при обнаружении петли отключался порт *config loopdetect mode port-based*

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

Упражнения

Задание	Наблюдение
Подключите неуправляемый коммутатор с петлей к DES-3200-28, как показано на схеме 1.	
Проверьте текущую конфигурацию функции LBD	<i>show loopdetect</i>
Что вы наблюдаете, запишите:	
Посмотрите, обнаружена ли петля на коммутаторе	<i>show loopdetect ports all</i>
Что вы наблюдаете, запишите:	
Проверьте, выполнил ли коммутатор блокировку порта	<i>show ports</i>
Отключите неуправляемый коммутатор с петлей от коммутатора DES-3200-28.	

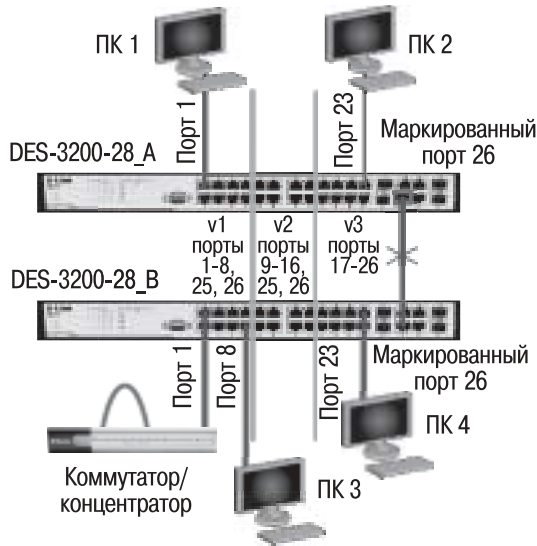
2. Настройка функции LoopBack Detection Independent STP в режиме VLAN-Based (для версии LBD 4.0)

В данном задании рассматривается блокирование порта для передачи трафика только той VLAN, в которой обнаружена петля. Остальной трафик через этот порт будет передаваться.

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

Сбросьте настройки коммутатора к заводским настройкам по умолчанию	<i>reset config</i>
Удалите порты из VLAN по умолчанию для использования в других VLAN	<i>config vlan default delete 8-26</i>
Создайте VLAN v2 и v3	<i>create vlan v2 tag 2</i> <i>create vlan v3 tag 3</i>

Схема 2:



Добавьте в созданные VLAN немаркированные порты.
Добавьте порты 25-26 как маркированные в созданные VLAN и VLAN по умолчанию

```
config vlan default add tagged 25-26
config vlan v2 add untagged 9-16
config vlan v2 add tagged 25-26
config vlan v3 add untagged 17-24
config vlan v3 add tagged 25-26
```

Включите функцию LBD глобально на коммутаторе

```
enable loopdetect
```

Активизируйте функцию LBD на всех портах коммутатора

```
config loopdetect ports 1-28 state enabled
```

Сконфигурируйте режим VLAN-Based LBD

```
config loopdetect mode vlan-based
```

Внимание! При обнаружении петли порт не будет передавать трафик только той VLAN, в которой обнаружена петля.

Упражнения

Задание

Подключите неуправляемый коммутатор с петлей к DES-3200-28_B, как показано на схеме 2.

Наблюдение

Что вы наблюдаете, запишите:

Проверьте текущую конфигурацию функции LBD

show loopdetect

Что вы наблюдаете, запишите:

Посмотрите, обнаружена ли петля на коммутаторе

show loopdetect ports all

Что вы наблюдаете, запишите:

Проверьте, выполнил ли коммутатор блокировку порта

show ports

Проверьте состояние подключения и причину блокировки портов

show ports err_disabled

Занятие №10. Команды агрегирования каналов

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

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

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

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

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

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

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

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

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

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

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

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

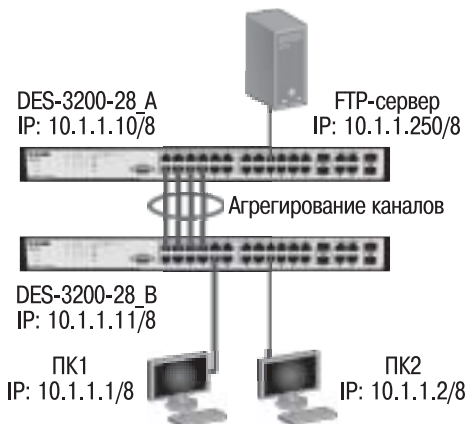
Оборудование:

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

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

reset config

Схема 1:



1. Настройка статического агрегирования каналов

Не соединяйте физически соответствующие порты устройств до тех пор, пока не настроено агрегирование каналов, т.к. в коммутируемой сети может возникнуть петля.

1.1. Настройка DES-3200-28_A

Создайте группу агрегирования каналов *create link_aggregation group_id 1 type static*

Настройте алгоритм агрегирования каналов. Эти установки применяются к коммутатору глобально *config link_aggregation algorithm mac_source_dest*

Включите порты 2, 4, 6, 8 в группу агрегирования каналов и выберите порт 2 в качестве мастера-порта *config link_aggregation group_id 1 master_port 2 ports 2,4,6,8 state enable*

1.2. Настройка DES-3200-28_B

Создайте группу агрегирования каналов *create link_aggregation group_id 1 type static*

Настройте алгоритм агрегирования каналов. Эти установки применяются к коммутатору глобально *config link_aggregation algorithm mac_source_dest*

Включите порты 1, 3, 5, 7 в группу агрегирования каналов и выберите порт 1 в качестве мастера-порта *config link_aggregation group_id 1 master_port 1 ports 1,3,5,7 state enable*

Подключите устройства, как показано на схеме 1.

Упражнения

Задание

Наблюдение

Проверьте выполненные настройки

show link_aggregation

Скачайте файлы с FTP-сервера (IP-адрес 10.1.1.250/8), используя

Наберите в командной строке (cmd) Windows:

рабочие станции ПК1 и ПК2, при помощи FTP-клиента или приведенной команды

```
ftp 10.1.1.250 hash mget *
```

Во время скачивания файлов на две рабочие станции проверьте загрузку портов на обоих коммутаторах

```
show utilization ports
```

Что вы наблюдаете?

Распределяется нагрузка между каналами?

2. Настройка динамического агрегирования каналов (LACP)

Перед выполнением задания отсоедините коммутаторы друг от друга.

2.1. Настройка DES-3200-28_A

Перед созданием группы агрегирования каналов, основанной на LACP, удалите существующую группу

```
delete link_aggregation group_id 1
```

Создайте группу агрегирования каналов

```
create link_aggregation group_id 1
type lacp
```

Включите порты 2, 4, 6, 8 в группу агрегирования каналов и выберите порт 2 в качестве мастера-порта

```
config link_aggregation group_id 1
master_port 2 port 2,4,6,8 state
enabled
```

Настройте порты на работу в пассивном режиме

```
config lacp_port 2,4,6,8 mode passive
```

2.2. Настройка DES-3200-28_B

Перед созданием группы агрегирования каналов, основанной на LACP, удалите существующую группу

```
delete link_aggregation group_id 1
```

Создайте группу агрегирования каналов

```
create link_aggregation group_id 1
type lacp
```

Включите порты 1, 3, 5, 7 в группу агрегирования каналов и выберите порт 1 в качестве мастера-порта

```
config link_aggregation group_id 1
master_port 1 port 1,3,5,7 state
enable
```

Подключите устройства, как показано на схеме 1.

Упражнения

Задание

Наблюдение

Скачайте файлы с FTP-сервера (IP-адрес 10.1.1.250/8), используя рабочие станции ПК1 и ПК2, при помощи FTP-клиента или приведенной команды

Наберите в командной строке (cmd) Windows:
ftp 10.1.1.250 hash mget *

Во время скачивания файлов проверьте загрузку портов на обоих коммутаторах

```
show utilization ports
```

Что вы наблюдаете?

Распределяется ли нагрузка между каналами?

Проверьте выполненные настройки

```
show link_aggregation
```

Проверьте режим работы LACP на портах коммутаторов

```
show lacp_port 1-8
```

Измените режим работы LACP на портах коммутатора DES-3200-28_A на активный и выполните задание повторно

```
config lacp_ports 2,4,6,8 mode active
```

Что вы наблюдаете?

Распределяется ли нагрузка между каналами?

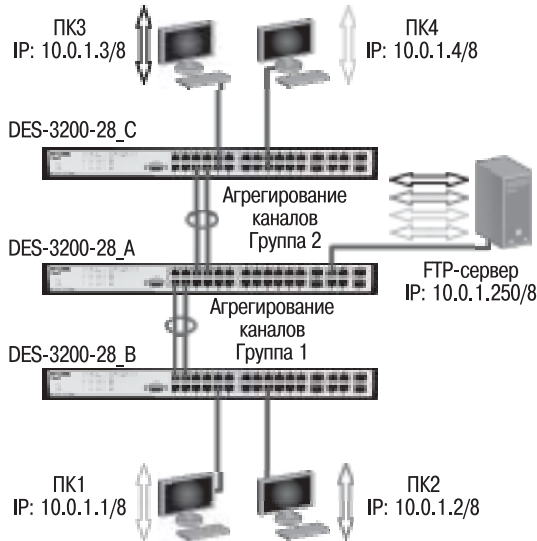
Отсоедините коммутаторы друг от друга.

3. Настройка динамического агрегирования каналов (LACP) при распределении каналов между тремя коммутаторами

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

```
reset config
```

Схема 2:



3.1. Настройка DES-3200-28_A

Создайте две группы агрегирования каналов

```
create link_aggregation group_id 1
type lacp
create link_aggregation group_id 2
type lacp
```

Настройте алгоритм агрегирования

```
config link_aggregation algorithm
mac_destination
```

Включите порты 1-4 в группу агрегирования каналов id1 и выберите порт 2 в качестве мастера-порта

```
config link_aggregation group_id 1
master_port 2 ports 1-4 state enabled
```

Настройте порты на работу в пассивном режиме *config lacp ports 1-4 mode active*

Включите порты 5-8 в группу агрегирования каналов id2 и выберите порт 6 в качестве мастера-порта *config link_aggregation group_id 2 master_port 6 ports 5-8 state enabled*

Настройте порты на работу в активном режиме *config lacp ports 5-8 mode active*

3.2. Настройка DES-3200-28_B

Создайте группу агрегирования каналов *create link_aggregation group_id 1 type lacp*

Настройте алгоритм агрегирования *config link_aggregation algorithm mac_destination*

Включите порты 1-4 в группу агрегирования каналов id1 и выберите порт 1 в качестве мастера-порта *config link_aggregation group_id 1 master_port 1 ports 1-4 state enabled*

3.3. Настройка DES-3200-28_C

Создайте группу агрегирования каналов *create link_aggregation group_id 2 type lacp*

Настройте алгоритм агрегирования *config link_aggregation algorithm mac_destination*

Включите порты 5-8 в группу агрегирования каналов id2 и выберите порт 6 в качестве мастера-порта *config link_aggregation group_id 2 master_port 6 ports 5-8 state enabled*

Внимание!

1. Если один конец агрегированного канала настроен как LACP, другой конец должен также иметь тип LACP. Если один конец имеет тип LACP, а другой Static, то соединение установлено не будет.
2. Если коммутатор с поддержкой LACP требуется подключить к коммутатору, поддерживающему только статическое агрегирование, то тип агрегированного канала на коммутаторе LACP необходимо установить в Static.

Подключите устройства, как показано на схеме 2, и попробуйте передать данные между рабочими станциями.

Упражнения

Задание	Наблюдение
Проверьте выполненные настройки	<i>show link_aggregation</i>
Проверьте режим работы LACP на портах коммутаторов	<i>show lacp_port 1-8</i>
Во время скачивания файлов проверьте загрузку портов на всех коммутаторах	<i>show utilization ports</i>
Что вы наблюдаете?	
Нагрузка распределяется между каналами?	

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

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

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

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

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

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

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

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

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

Оборудование:

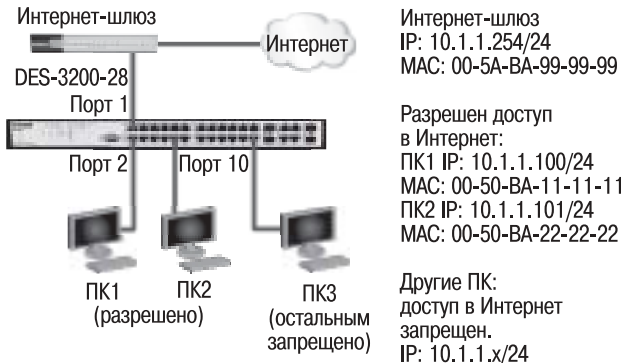
DES-3200-28	1 шт.
Рабочая станция	3 шт.
Кабель Ethernet	5 шт.
Консольный кабель	1 шт.
Интернет-шлюз	1 шт.

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

reset config

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

Схема 1:



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

Правила:

Правило 1:

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

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

Правило 2:

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

Правило 3:

Иначе — по умолчанию разрешить доступ всем узлам.

Внимание! Замените указанные в командах MAC-адреса на реальные MAC-адреса рабочих станций и Интернет-шлюза.

Правило 1.

Создайте профиль доступа с номером 10

```
create access_profile ethernet
source_mac FF-FF-FF-FF-FF-FF
destination_mac FF-FF-FF-FF-FF-FF
profile_id 10
```

Создайте правило для профиля 10, разрешающее доступ ПК1, подключенного к порту 2, в Интернет

```
config access_profile profile_id 10 add
access_id 11 ethernet source_mac
00-50-ba-11-11-11 destination_mac
00-50-ba-99-99-99 port 2 permit
```

Создайте правило для профиля 10, разрешающее доступ ПК2, подключенного к порту 10, в Интернет

```
config access_profile profile_id 10 add
access_id 12 ethernet source_mac
00-50-ba-22-22-22 destination_mac
00-50-ba-99-99-99 port 10 permit
```

Правило 2.

Создайте профиль доступа номером 20

```
create access_profile ethernet
destination_mac FF-FF-FF-FF-FF-FF
profile_id 20
```

Создайте правило для профиля 20, запрещающее доступ остальным пользователям в Интернет

```
config access_profile profile_id 20 add
access_id 21 ethernet
destination_mac 00-50-ba-99-99-99
port 1-28 deny
```

Внимание!

Созданное правило запретит прохождение кадров, содержащих MAC-адрес назначения, равный MAC-адресу Интернет-шлюза, на всех портах коммутатора. Если данное правило необходимо применить на одном из портов, в конфигурации указывается определенный порт, к которому подключена станция, трафик которой необходимо блокировать.

Правило 3.

Разрешите все остальное

Выполняется по умолчанию

Упражнения

Задание

Наблюдение

Проверьте созданные профили

show access_profile

Что вы наблюдаете?

Сколько профилей создано, сколько в них правил?

Подключите станции ПК1 и ПК2 к коммутатору и протестируйте соединение до Интернет-шлюза командой *ping*

ping <IP-address>

Подключите к коммутатору другую станцию и попробуйте получить доступ к Интернет-шлюзу (подключите станции ПК1 и ПК2 к другим портам).

Протестируйте соединение командой *ping* до Интернет-шлюза

ping <IP-address>

Что вы наблюдаете? Запишите:

Удалите правило из профиля 10 (например, правило с номером 12, что приведет к отключению ПК2 от Интернета)

*config access_profile profile_id 10
delete access_id 12*

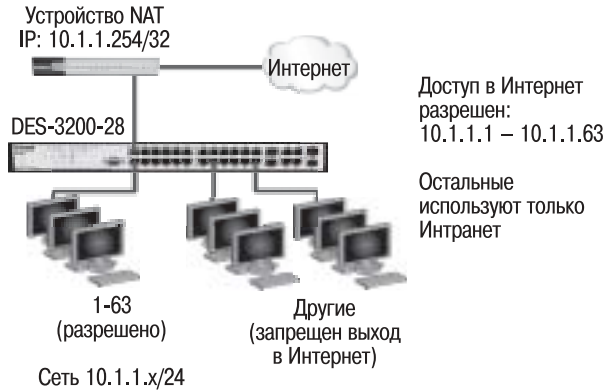
Удалите профиль доступа (например, профиль 10, что приведет к отключению ПК1 от Интернета)

delete access_profile profile_id 10

2. Настройка ограничения доступа пользователей в Интернет по IP-адресам

Задача: пользователям с IP-адресами с 10.1.1.1/24 по 10.1.1.63/24 разрешен доступ в Интернет. Остальным пользователям сети 10.1.1.0/24 с адресами, не входящими в разрешенный диапазон, доступ в Интернет запрещен.

Схема 2:

**Правила:***Правило 1:*

Если IP-адрес источника = IP-адресам из диапазона с 10.1.1.1 по 10.1.1.63 – разрешить.

Правило 2:

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

Правило 3:

Иначе – по умолчанию разрешить доступ всем узлам.

Перед выполнением настройки удалите последний профиль из предыдущего задания

```
delete access_profile profile_id 20
```

Убедитесь, что больше не осталось профилей

```
show access_profile
```

Правило 1.

Создайте профиль доступа с номером 10, разрешающий доступ для подсети 10.1.1.0/26 (узлам с 1 по 63)

```
create access_profile ip
source_ip_mask 255.255.255.192
profile_id 10
```

Сконфигурируйте правило для профиля доступа 10

```
config access_profile profile_id 10 add
ccess_id 11 ip source_ip 10.1.1.0 port
1-28 permit
```

Внимание! Созданное правило разрешает прохождение трафика IP-подсети 10.1.1.0/26 на всех портах коммутатора. Если данное правило необходимо применить на одном из портов, в конфигурации указывается определенный порт, к которому подключена станция, чей трафик необходимо разрешить.

Правило 2.
Создайте профиль доступа с номером 40

```
create access_profile ethernet
destination_mac FF-FF-FF-FF-FF-FF
profile_id 40
```

Сконфигурируйте правило для профиля 40, запрещающее остальным станциям подключаться к Интернет-шлюзу

```
config access_profile profile_id 40 add
access_id 41 ethernet destination_mac
00-50-ba-99-99-99 port 1-28 deny
```

Правило 3.
Разрешите все остальное

Выполняется по умолчанию

Проверьте созданные профили

```
show access_profile
```

Упражнения

Задание **Наблюдение**

Подключите станции ПК1 (IP-адрес из диапазона 10.1.1.1-63/24) и ПК2 (10.1.1.64-253/24) к коммутатору и протестируйте соединение до Интернет-шлюза (IP-адрес 10.1.1.254/24) командой ping

```
ping 10.1.1.254
```

Что вы наблюдаете? Запишите:

Удалите правило из профиля 10

```
config access_profile profile_id 10
delete access_id 11
```

Проверьте профили доступа

```
show access_profile
```

Что вы наблюдаете? Запишите:

Протестируйте соединение до Интернет-шлюза от PC1 и PC2 командой ping

ping 10.1.1.254

Что вы наблюдаете? Запишите:

Удалите профиль доступа (например, профиль 10)

delete access_profile profile_id 10

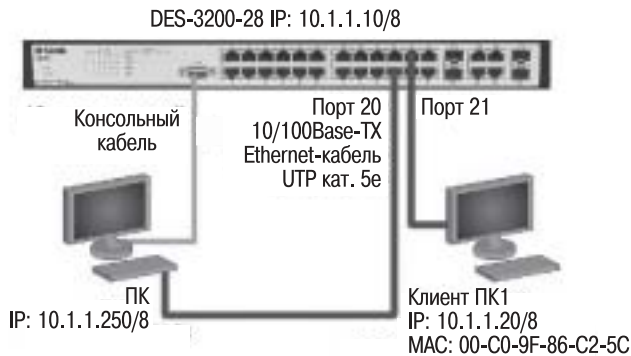
Протестируйте соединение до Интернет-шлюза командой ping

ping 10.1.1.254

Что вы наблюдаете? Запишите:

3. Настройка функции CPU Interface Filtering

Схема 3:



Правила:

Правило 1:

Если IP-адрес источника = 10.1.1.250 – разрешить доступ к CPU коммутатора по протоколу ICMP.

Правило 2:

Другим станциям запретить доступ по протоколу ICMP к коммутатору.

Правило 3:

Иначе – по умолчанию разрешить доступ всем узлам.

Перед выполнением настройки удалите последний профиль из предыдущего задания *delete access_profile profile_id 40*

Настройте IP-адрес интерфейса управления коммутатора	<i>config ipif System ipaddress 10.1.1.10/8</i>
Включите функцию CPU Interface Filtering	<i>enable cpu_interface_filtering</i>
Правило 1. Создайте профиль доступа 1	<i>create cpu_access_profile ip source_ip_mask 255.255.255.255 icmp profile_id 1</i>
Сконфигурируйте правила для профиля доступа 1	<i>config cpu_access_profile profile_id 1 add access_id 1 ip source_ip 10.1.1.250 icmp permit</i>
Правило 2. Создайте профиль доступа 2	<i>create cpu_access_profile ip source_ip_mask 255.0.0.0 icmp profile_id 2</i>
Сконфигурируйте правила для профиля доступа 2	<i>config cpu_access_profile profile_id 2 add access_id 1 ip source_ip 10.0.0.0 icmp deny</i>
Правило 3. Разрешите все остальное	<i>Выполняется по умолчанию</i>

Упражнения

Задание	Наблюдение
Подключите станции ПК1 и ПК2 и протестируйте соединение до CPU коммутатора (IP-адрес 10.1.1.10) командой ping	<i>ping 10.1.1.10</i>
Что вы наблюдаете? Запишите:	
Проверьте список стандартных профилей ACL	<i>show access_profile</i>
Проверьте правила в списке фильтров CPU	<i>show cpu_access_profile</i>

Удалите правило 1 из профиля 1

*config cpu access_profile profile_id 1
delete access_id 1*

Что вы наблюдаете? Запишите:

Удалите профиль CPU ACL

delete cpu access_profile profile_id 1

Протестируйте соединение до CPU коммутатора командой ping.

Что вы наблюдаете? Запишите:

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

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

Существует три режима работы функции Port Security:

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

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

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

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

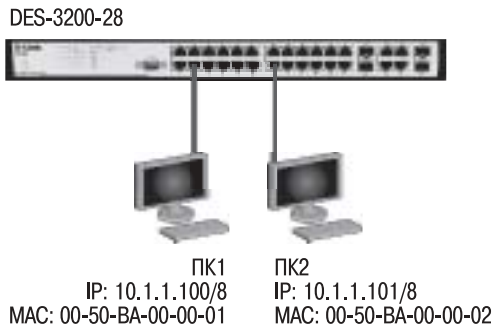
Оборудование:

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

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

reset config

Схема 1:



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

1.1. Настройка DES-3200-28

Установите максимальное количество изучаемых всеми портами MAC-адресов равным 1

*config port_security ports 1-28
admin_state enable
max_learning_addr 1*

Подключите ПК1 и ПК2 к портам коммутатора

В этом примере используются порты 4 и 14

Проверьте MAC-адреса, которые стали известны портам

*show fdb port 4
show fdb port 14*

Проверьте, соответствуют ли зарегистрированные адреса адресам рабочих станций:

Проверьте информацию о настройках Port Security на портах коммутатора *show port_security ports 1-28*

Настройте запись в Log-файл MAC-адресов, подключающихся к порту станций и отправку сообщений SNMP Trap *enable port_security trap_log*

Упражнения

Задание

Наблюдение

Выполните тестирование соединения командой *ping* от ПК1 к ПК2 и наоборот *ping <IP-address>*

Поменяйте местами порты подключения рабочих станций.

Повторите тестирование соединения командой *ping* *ping <IP-address>*

Проверьте информацию в Log-файле коммутатора *show log*

Какой вы сделаете вывод?

Сохраните конфигурацию и перезагрузите коммутатор *save*
reboot

Повторите тестирование соединения командой *ping* *ping <IP-address>*

Какой вы сделаете вывод?

Сохраняется ли информация о привязке MAC-port?

Настройте на порте 4 работу функции Port Security в режиме Permanent *config port_security ports 4*
admin_state enable

и максимальное количество изучаемых адресов, равное 1	<i>max_learning_addr 1 lock_address_mode Permanent</i>
Сохраните конфигурацию и перезагрузите коммутатор	<i>save reboot</i>
Проверьте информацию о настройках Port Security на портах коммутатора	<i>show port_security ports 1-28</i>
Какой вы сделаете вывод?	
Сохраняется информации о привязке MAC-port?	
Очистите информацию о привязке MAC-port на порте 4	<i>clear port_security_entry port 4</i>
Отключите работу функции Port Security на порте 4 и приведите настройки в исходное (по умолчанию) состояние	<i>config port_security ports 4 admin_state disable max_learning_addr 1 lock_address_mode DeleteOnReset</i>
Посмотрите время таймера блокирования (оно соответствует времени жизни MAC-адреса в таблице коммутации)	<i>show fdb aging_time</i>
Изменить время действия таймера можно с помощью настройки времени жизни MAC-адреса в таблице коммутации (время указано в секундах)	<i>config fdb aging_time 300</i>
Переведите режим работы функции Port Security на порте 4 в Delete on Timeout	<i>config port_security ports 4 admin_state enable max_learning_addr 1 lock_address_mode DeleteOnTimeout</i>
Проверьте MAC-адреса, которые стали известны порту 4	<i>show fdb port 4</i>
Проверьте информацию о настройках Port Security на портах коммутатора	<i>show port_security ports 1-28</i>

Выполните тестирование соединения командой `ping` от ПК1 к ПК2 и наоборот `ping <IP-address>`

Какой вы сделаете вывод?

Сохраняется ли информация о привязке MAC-port?

Отключите работу функции Port Security на портах `config port_security ports 1-28 admin_state disable`

Отключите функцию записи в Log-файл и отправки SNMP Trap `disable port_security trap_log`

2. Настройка защиты от подключения к портам, основанной на статической таблице MAC-адресов

2.1. Настройка DES-3200-28

Сбросьте настройки коммутатора к заводским настройкам по умолчанию `reset config`

Активизируйте функцию Port Security на всех портах и запретите изучение MAC-адресов (параметр `max_learning_addr` установить равным 0) `config port_security ports 1-28 admin_state enable max_learning_addr 0`

Выполните тестирование соединения командой `ping` от ПК1 к ПК2 и наоборот `ping <IP-address>`

Вручную создайте статические записи в таблице MAC-адресов `create fdb default 00-50-ba-00-00-01 port 4`
`create fdb default 00-50-ba-00-00-02 port 4`

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

Проверьте созданные статические записи в таблице коммутации `show fdb port 4`
`show fdb port 14`

Проверьте информацию о настройках Port Security на портах коммутатора `show port_security ports 1-28`

Упражнения

Задание

Наблюдение

Выполните тестирование соединения командой ping от ПК1 к ПК2 и наоборот

ping <IP-address>

Поменяйте местами порты подключения рабочих станций.

Повторите тестирование соединения командой ping

ping <IP-address>

Какой вы сделаете вывод?

Удалите запись из таблицы MAC-адресов на порте 4

*delete fdb default 00-50-ba-00-00-02
port 4*

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

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

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

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

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

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

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

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

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

Оборудование:

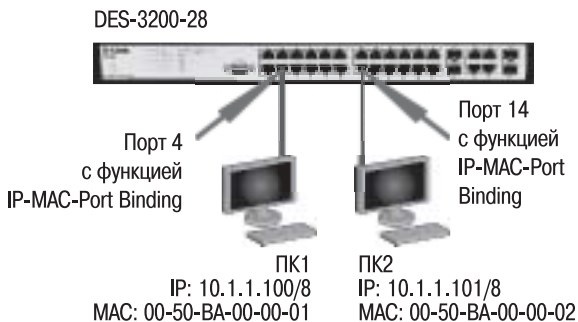
DES-3200-28	1 шт.
DES-1005D	1 шт.
Рабочая станция	3 шт.
Кабель Ethernet	4 шт.
Консольный кабель	1 шт.

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

reset config

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

Схема 1:



1.1. Настройка DES-3200-28

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

Создайте запись IP-MAC-Port Binding, связывающую IP-MAC-адрес станции ПК1 с портом 4 (по умолчанию режим работы функции ARP)	<i>create address_binding ip_mac ipaddress 10.1.1.100 mac_address 00-50-ba-00-00-01 ports 4</i>
Создайте запись IP-MAC-Port Binding, связывающую IP-MAC-адрес станции ПК2 с портом 14	<i>create address_binding ip_mac ipaddress 10.1.1.101 mac_address 00-50-ba- 00-00-02 ports 14</i>
Активизируйте функцию на портах 4, 14 (по умолчанию режим работы портов Strict)	<i>config address_binding ip_mac ports 4,14 state enable</i>
Проверьте созданные записи IP-MAC-Port Binding	<i>show address_binding ip_mac all</i>
Проверьте порты, на которых настроена функция и их режим работы	<i>show address_binding ports</i>

Подключите рабочие станции к коммутатору, как показано на схеме 1.

Упражнения

Задание	Наблюдение
Выполните тестирование соединения между ПК1 и ПК2 командой ping	<i>ping <IP-address></i>
Измените подключение рабочих станций. PC1 подключите к порту 14, PC2 к порту 4. Повторите тестирование соединения командой ping.	
Настройте запись в Log-файл и отправку сообщений SNMP Trap в случае несоответствия ARP-пакета связке IP-MAC	<i>enable address_binding trap_log</i>
Проверьте заблокированные рабочие станции	<i>show address_binding blocked all</i>
Проверьте наличие заблокированных станций в Log-файле	<i>show log</i>

Какой вы сделаете вывод?

Удалите адрес из списка заблокированных адресов

```
delete address_binding blocked  
vlan_name System mac_address  
00-50-ba-00-00-01
```

Удалите запись IP-MAC-Port Binding

```
delete address_binding ip_mac ipad-  
dress 10.1.1.100 mac_address 00-50-  
ba-00-00-01
```

Отключите функцию IP-MAC-Port Binding на портах 4 и 14

```
config address_binding ip_mac ports  
4,14 state disable
```

2. Настройка работы функции IP-MAC-Port Binding в режиме ACL

2.1. Настройка DES-3200-28

Создайте запись IP-MAC-Port Binding, связывающую IP-MAC-адрес станции ПК1 с портом 4

```
create address_binding ip_mac  
ipaddress  
10.1.1.100 mac_address 00-50-  
ba-00-00-01 ports 4
```

Создайте запись IP-MAC-Port Binding, связывающую IP-MAC-адрес станции ПК2 с портом 14

```
create address_binding ip_mac  
ipaddress  
10.1.1.101 mac_address 00-50-ba-  
00-00-02 ports 14
```

Активизируйте функцию на портах 4, 14 (по умолчанию режим работы портов Strict), включите режим allow_zeroip, благодаря которому коммутатор не будет блокировать узлы, отправляющие ARP-пакеты с IP-адресом источника 0.0.0.0, и установите работу функции IMPV в режиме ACL

```
config address_binding ip_mac ports  
4,14 state enable allow_zeroip enable  
mode acl
```

Проверьте созданные записи IP-MAC-Port Binding

```
show address_binding ip_mac
```

Проверьте порты, на которых настроена функция и их режим работы

```
show address_binding ports
```

Проверьте созданные профили доступа ACL *show access_profile*

Упражнения

Задание **Наблюдение**

Выполните тестирование соединения между ПК1 и ПК2 командой ping *ping <IP-address>*

Измените подключение рабочих станций. PC1 подключите к порту 14, PC2 к порту 4.
Повторите тестирование соединения командой ping.

Проверьте заблокированные рабочие станции *show address_binding blocked all*

Какой вы сделаете вывод?

Удалите адрес из списка заблокированных адресов *delete address_binding blocked
vlan_name System mac_address
00-50-ba-00-00-01*

Удалите все заблокированные адреса *delete address_binding blocked all*

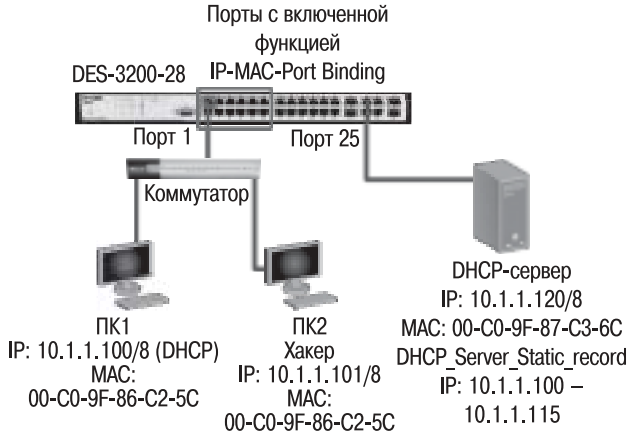
Удалите все записи IP-MAC-Port Binding *delete address_binding ip_mac
ipaddress 10.1.1.100 mac_address
00-50-ba-00-00-01
delete address_binding ip_mac
ipaddress 10.1.1.101 mac_address
00-50-ba-00-00-02*

Отключите функцию IP-MAC-Port Binding на портах 4 и 14 *config address_binding ip_mac ports
4,14 state disable*

Какой можно сделать вывод о работе функции IP-MAC-Port Binding в режиме ACL?

3. Настройка работы функции IP-MAC-Port Binding в режиме DHCP Snooping

Схема 2:



3.1. Настройка DES-3200-28

Активизируйте функцию IP-MAC-Port Binding в режиме DHCP Snooping глобально на коммутаторе

```
enable address_binding dhcp_snoop
```

Укажите максимальное количество создаваемых в процессе автоизучения записей IP-MAC на портах 1-10, равное 1

```
config address_binding  
allow_dhcp_snoop 1-10 total_entries 1
```

Активизируйте функцию IP-MAC-Port Binding в режиме DHCP Snooping на портах 1-10

```
config address_binding ip_mac ports  
1-10 state enable
```

Настройте возможность передачи нулевого IP-адреса (0.0.0.0) для корректной работы протокола DHCP

```
config address_binding ip_mac ports  
1-10 allow_zeroip enable
```

Настройте возможность передачи пакетов от DHCP-сервера

```
config address_binding ip_mac ports  
1-10 forward_dhcppkt enable
```

Упражнения

Задание	Наблюдение
Проверьте состояние функции IP-MAC-Port Binding в режиме DHCP Snooping	<i>show address_binding dhcp_snoop</i>
Выполните на рабочей станции динамическое получение IP-адреса.	
Посмотрите созданные записи IP-MAC-Port Binding	<i>show address_binding dhcp_snoop binding_entry</i>
Подключите вторую станцию и попробуйте получить еще один динамический IP-адрес.	
Настройте запись в Log-файл и отправку сообщений SNMP Trap в случае несоответствия ARP-пакета связке IP-MAC	<i>enable address_binding trap_log</i>
Проверьте наличие заблокированных станций на коммутаторе	<i>show address_binding blocked all</i>
Проверьте наличие заблокированных станций в Log-файле	<i>show log</i>
Какой вы сделаете вывод?	
Отключите функцию IP-MAC-Port Binding на портах 1-10	<i>config address_binding ip_mac ports 1-10 state disable</i>
Отключите функцию IP-MAC-Port Binding в режиме DHCP Snooping глобально на коммутаторе	<i>disable address_binding dhcp_snoop</i>

Занятие №14. Ограничение административного доступа к управлению коммутатором

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

Понятия, которые используются в данной лабораторной работе:

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

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

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

Цель: Изучить механизмы ограничения административного доступа к управлению коммутатором.

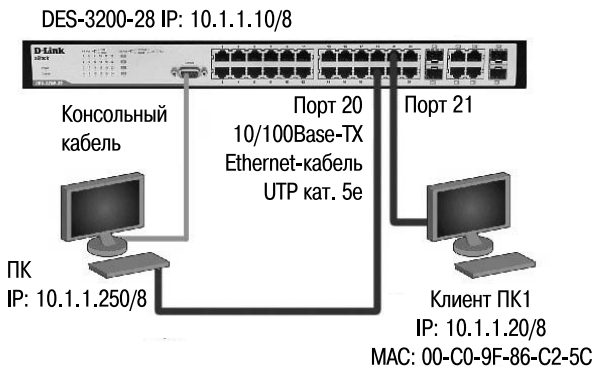
Оборудование:

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

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

reset config

Схема 1:



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

Настройте IP-адрес интерфейса управления коммутатора *config ipif System ipaddress 10.1.1.10/8*

Создайте доверенную рабочую станцию, с которой разрешено управление коммутатором *create trusted_host 10.1.1.250*

Посмотрите список доверенных узлов сети *show trusted_host*

Упражнения

Задание

Наблюдение

Проверьте возможность управления коммутатором со станций ПК1 и ПК2

telnet 10.1.1.10

Что вы наблюдаете?

Повторите упражнение после установки подсети управления.

Удалите доверенную станцию управления

delete trusted_host ipaddr 10.1.1.250

Создайте сеть, из которой разрешено управление коммутатором

create trusted_host network 10.1.1.0/8

Проверьте возможность управления коммутатором со станций ПК1 и ПК2

telnet 10.1.1.10

Что вы наблюдаете?

Удалите сеть, из которой разрешено управление коммутатором

delete trusted_host network 10.1.1.0/8

Внимание! После создания IP-адресов доверенных станций или сетей управления управление коммутатором через Web-интерфейс или через Telnet будет доступно только с этих станций или сетей. Максимальное количество объектов управления – 10.

2. Включение режима шифрования паролей учетных записей в конфигурационных формах

Внимание! По умолчанию информация о паролях пользователей хранится в незашифрованном виде в конфигурационном файле коммутатора. Так как данные файлы могут пересылаться по сети с помощью протокола TFTP (без шифрования), они могут быть скомпрометированы. Таким образом, рекомендуется обязательное включение функции шифрования паролей или создание учетных записей с механизмом шифрования.

Создайте учетную запись пользователя *DES-3200-28#create account admin swadmin*
Command: create account admin swadmin
*Enter a case-sensitive new password:******
*Enter the new password again for confirmation:******
Success.

Посмотрите созданную учетную запись *show account*

Посмотрите информацию и способ хранения паролей в конфигурационном файле *show config current_config*

Включите хранение паролей в зашифрованном виде *enable password encryption*

Посмотрите информацию и способ хранения паролей в конфигурационном файле *show config current_config*

Отключите режим шифрования паролей *disable password encryption*

Дешифруйте пароль учетной записи swadmin в конфигурационном файле *config account swadmin encrypt plain_text dlink*

Посмотрите выполнение дешифрования *show config current_config*

Что вы наблюдаете?

3. Отключите доступ к коммутатору по Telnet или через Web-интерфейс

Примечание. В случае если для управления коммутатором не используются Telnet или Web-интерфейс, для повышения безопасности сети желательно отключить неиспользуемые консоли.

Отключите подключение к Web-интерфейсу *disable web*

Проверьте возможность подключения к Web-интерфейсу *http://10.1.1.10*

Что вы наблюдаете?

Включите управление через Web-интерфейс и установите номер TCP-порта 8080 *enable web 8080*

Проверьте возможность управления коммутатором через Web-интерфейс и TCP-порт 8080 *http://10.1.1.10:8080*

Что вы наблюдаете?

Отключите работу протокола Telnet на коммутаторе *disable telnet*

Что вы наблюдаете?

Включите работу протокола Telnet, используя программу HyperTerminal в Windows или Web-интерфейс *enable telnet*

4. Настройка Web-консоли (по протоколу SSL)

Примечание. Для работы коммутатора по протоколу SSL необходимо наличие сертификатов. В случае наличия в организации развернутой инфраструктуры открытых ключей (PKI) необходимо сгенерировать данные ключи. При отсутствии PKI можно использовать сертификат по умолчанию, поддерживаемый программным обеспечением коммутаторов D-Link.

Включите режим SSL (при этом автоматически будет отключен режим Web) *enable ssl*

Попробуйте зайти на сайт через консоль SSL *https://10.1.1.10*

Какой вы сделаете вывод?

5. Настройка Secure Console (SSH)

Примечание. Для управления коммутатором через SSH необходима специализированная консоль. В отличие от UNIX-систем, в ОС Windows отсутствует встроенная консоль SSH. Для примера будем применять консоль Putty (ее можно скачать с сайта <http://www.putty.org>).

Включите функцию SSH	<i>enable ssh</i>
Проверьте включение встроенного сервера SSH	<i>show ssh server</i>
Измените период времени смены ключей SSH (по умолчанию ключи никогда не изменяются)	<i>config ssh server rekey 10min</i>
Сконфигурируйте настройки пользователя SSH (учетная запись пользователя уже должна быть создана)	<i>config ssh user dlink authmode password</i>

Проверьте возможность управления коммутатором через SSH-консоль.

Занятие №15. Команды протокола IEEE 802.1X

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

Сервер аутентификации Remote Authentication in Dial-In User Service (RADIUS) проверяет права доступа каждого клиента, подключаемого к порту коммутатора, прежде чем разрешить доступ к любому из сервисов, предоставляемых коммутатором или локальной сетью.

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

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

- *клиент (Supplicant)* находится в операционной системе абонента, обычно это рабочая станция, которая запрашивает доступ к локальной сети и сервисам коммутатора и отвечает на запросы от коммутатора. На рабочей станции должно быть установлено клиентское ПО для 802.1X, например то, которое встроено в ОС Microsoft Windows;
- *сервер аутентификации (Authentication Server)* выполняет фактическую аутентификацию клиента. Он проверяет подлинность клиента и информирует коммутатор, предоставлять или нет клиенту доступ к локальной сети. RADIUS (Remote Authentication Dial-In User Service) работает в модели «клиент/сервер», в которой информация об аутентификации передается между сервером RADIUS и клиентами RADIUS;
- *аутентификатор (Authenticator)* управляет физическим доступом к сети, основываясь на статусе аутентификации клиента. Эту роль выполняет коммутатор. Он работает как посредник (Проху) между клиентом и сервером аутентификации: получает запрос на проверку подлинности от клиента, проверяет данную информацию при помощи сервера аутентификации и пересылает ответ клиенту. Коммутатор поддерживает клиент RADIUS, который отвечает

за инкапсуляцию и деинкапсуляцию кадров EAP, и взаимодействие с сервером аутентификации.

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

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

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

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

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

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

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

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

reset config

Цель: Изучить процесс настройки протокола 802.1X.

Оборудование:

DES-3200-28

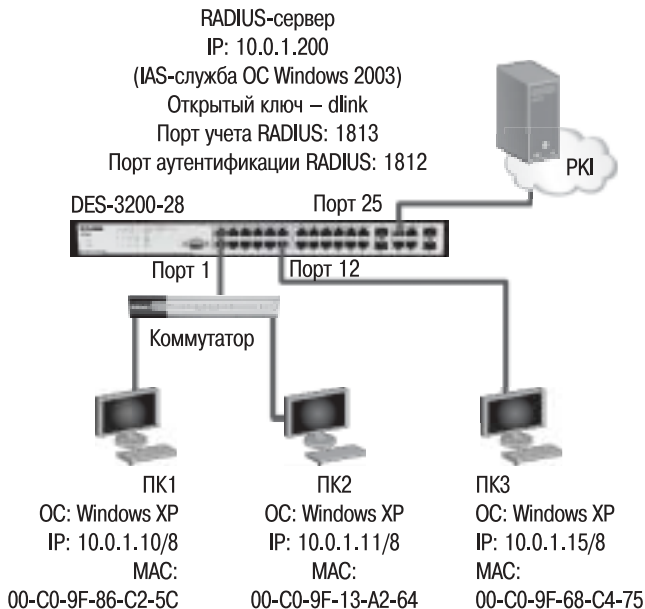
1 шт.

DES-1005D

1 шт.

Рабочая станция	3 шт.
Кабель Ethernet	5 шт.
Radius-сервер	1 шт.
Консольный кабель	1 шт.

Схема 1:



1. Настройка DES-3200-28

1.1. Изучение команд протокола 802.1X

Включите функцию 802.1X

```
enable 802.1x
```

Настройте параметры первичного RADIUS-сервера

```
config radius add 1 10.0.1.200 key  
dlink auth_port 1812 acct_port 1813
```

Проверьте настройки данных RADIUS-сервера

```
show radius
```

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

1.2. Настройка аутентификации 802.1X на основе портов

Включите аутентификацию 802.1X на портах 9-24 *config 802.1x capability ports 9-24 authenticator*

Включите принудительную повторную аутентификацию 802.1X на портах 9-24 *config 802.1x reauth port_based ports 9-24*

Настройте тип аутентификации 802.1X: Port-Based *config 802.1x auth_mode port_based*

Внимание! При аутентификации 802.1X на основе портов, после того как порт был авторизован, любой пользователь, подключенный к порту, может получить доступ к локальной сети.

Проверьте текущее состояние аутентификации 802.1X на портах 1-24 *show 802.1x auth_state ports 1-24*

Проверьте текущую конфигурацию 802.1X *show 802.1x auth_configuration*

1.3. Настройка аутентификации 802.1X на основе MAC-адресов

Включите аутентификацию на портах 1-8 по протоколу 802.1X *config 802.1x capability ports 1-8 authenticator*

Включите принудительную повторную аутентификацию портов 1-8 *config 802.1x reauth mac_based ports 1-8*

Настройте тип аутентификации 802.1X: MAC-Based *config 802.1x auth_mode mac_based*

Внимание! Максимальное количество изучаемых каждым портом MAC-адресов для коммутатора DES-3200-28 равно 16.

Проверьте текущее состояние аутентификации 802.1X на портах 1-24 *show 802.1x auth_state ports 1-24*

Проверьте текущую конфигурацию 802.1X *show 802.1x auth_configuration*

Занятие №16. Управление полосой пропускания

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

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

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

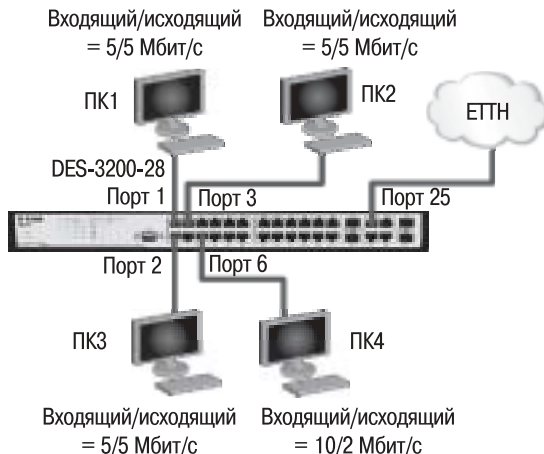
Оборудование:

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

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

reset config

Схема 1:



1. Настройка DES-3200-28

Примечание. Значение скорости в командах указывается в килобитах.

Настройте полосу пропускания на портах 1-4 равной 5 Мбит/с для входящего и исходящего трафика

```
config bandwidth_control 1-4 rx_rate 5270 tx_rate 5270
```

Настройте полосу пропускания на порте 6 равной 10 Мбит/с для входящего и 2 Мбит/с для исходящего трафика

```
config bandwidth_control 6 rx_rate 10240 tx_rate 2048
```

Проверьте выполненные настройки

```
show bandwidth_control 1-10
```

Упражнения

Задание

Наблюдение

Подключите станции ПК1 и ПК2 к портам 8 и 10 и попробуйте скачать файл размером 50 Мб со станции ПК1 на станцию ПК2 и обратно.

Запишите время передачи файла (в секундах):

Подключите станцию ПК1 к порту 1, повторите скачивание.

Запишите время передачи файла (в секундах):

Подключите станцию ПК1 к порту 6, повторите скачивание.

Запишите время передачи файла (в секундах):

Что вы наблюдаете?

Занятие №17. Настройка QoS. Приоритизация трафика

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

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

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

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

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

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

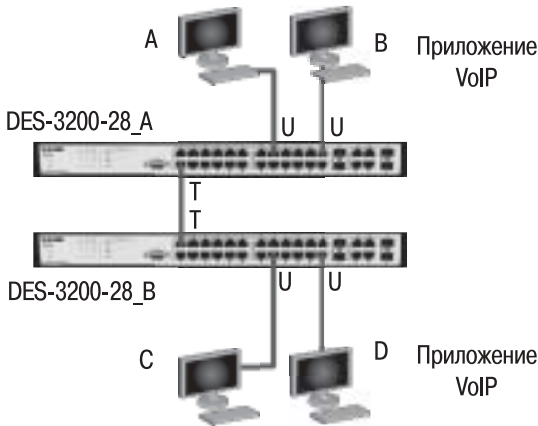
Оборудование:

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

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

reset config

Схема 1:



1. Настройка DES-3200-28_A

Переведите порт 1 на коммутаторе в состояние передачи маркированных кадров (для обеспечения возможности передачи информации о приоритете 802.1 p)

```
config vlan default delete 1
config vlan default add tagged 1
```

Поменяйте приоритет по умолчанию порта 23, к которому подключена станция B

```
config 802.Ip default_priority 23 7
```

Примечание. Пользовательский приоритет и метод обработки остаются по умолчанию.

2. Настройка DES-3200-28_B

Переведите порт 1 на коммутаторе в состояние передачи маркированных кадров (для обеспечения возможности передачи информации о приоритете 802.1 p)

```
config vlan default delete 1
config vlan default add tagged 1
```

Поменяйте приоритет по умолчанию порта 23, к которому подключена станция D

```
config 802.Ip default_priority 24 7
```

Примечание. Благодаря изменению значения приоритета портов, к которым подключены компьютеры с VoIP-приложениями на 7, все кадры, передаваемые ими, получают наивысший приоритет по сравнению с кадрами, поступающими от других компьютеров на остальные порты обоих коммутаторов.

Упражнение 1

Задание

Посмотрите текущие настройки приоритета по умолчанию на всех портах коммутаторов А и В
Посмотрите карту привязки пользовательских приоритетов 802.1р к очередям класса обслуживания

Наблюдение

show 802.Ip default_priority

show 802.Ip user_priority

Запишите, что вы наблюдаете:

Упражнение 2 (дополнительно)

Изучите механизм обслуживания очередей приоритетов Weighted Round Robin (WRR, взвешенный алгоритм кругового обслуживания).

Примечание. Для обработки очередей приоритетов могут использоваться различные механизмы обслуживания. В коммутаторах D-Link используются две схемы обслуживания очередей: очереди приоритетов со строгим режимом (Strict Priority Queue) и взвешенный алгоритм кругового обслуживания (Weighted Round Robin). В первом случае пакеты, находящиеся в очереди с высшим приоритетом, начинают передаваться первыми. При этом пока очередь с более высоким приоритетом не опустеет, пакеты из очередей с низким приоритетом передаваться не будут. Второй алгоритм WRR устраняет это ограничение, а также исключает нехватку полосы пропускания для очередей с низким приоритетом. Этот механизм обеспечивает обработку очередей в соответствии с назначенным им весом и предоставляет полосу пропускания для пакетов из низкоприоритетных очередей.

Поменяйте механизм обработки очередей на WRR (Strict используется по умолчанию)

config scheduling_mechanism weight_fair

**Проверьте механизм обработки
очереди**

show scheduling_mechanism

Назначьте вес обработки

*config scheduling 0 weight 10
config scheduling 1 weight 15
config scheduling 2 weight 25
config scheduling 3 weight 55*

**Выполните команду просмотра
очередности обслуживания**

show scheduling

Запишите, что вы наблюдаете:

Занятие №18. Команды зеркалирования портов (Port Mirroring)

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

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

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

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

Цель: Настроить отображение портов и понять способы его настройки.

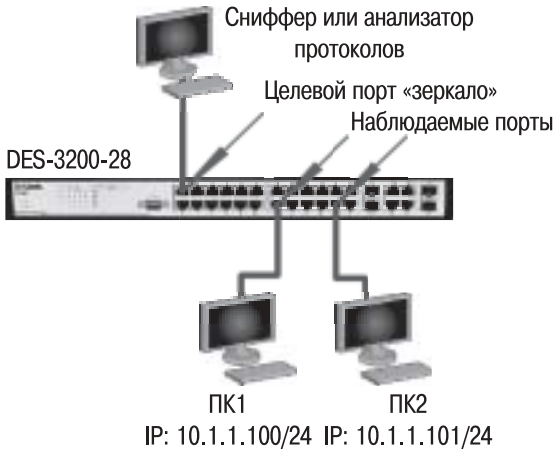
Оборудование:

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

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

reset config

Схема 1:



1. Настройка DES-3200-28

Настройте список портов (с 13 по 24), трафик которых будет пересылаться на целевой порт 1

```
config mirror port 1 add source ports 13-24 both
```

Включите зеркалирование портов

```
enable mirror
```

Проверьте настройки функции

```
show mirror
```

Внимание!

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

Упражнения

Задание

Наблюдение

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

www.wireshark.org – официальный сайт Wireshark.

Выполните тестирование соединения *ping <IP-address>*
командой ping от ПК1 к ПК2 и наоборот

Захватите и проанализируйте трафик с помощью анализатора протоколов.

Вы видите пакеты, передаваемые от и к рабочим станциям?

Отключите зеркалирование портов *disable mirror*

Проверьте настройки функции *show mirror*

Выполните тестирование соединения *ping <IP-address>*
командой ping от ПК1 к ПК2 и наоборот

Запустите анализатор протоколов.

Что вы наблюдаете теперь?

Занятие №19. Команды мониторинга

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

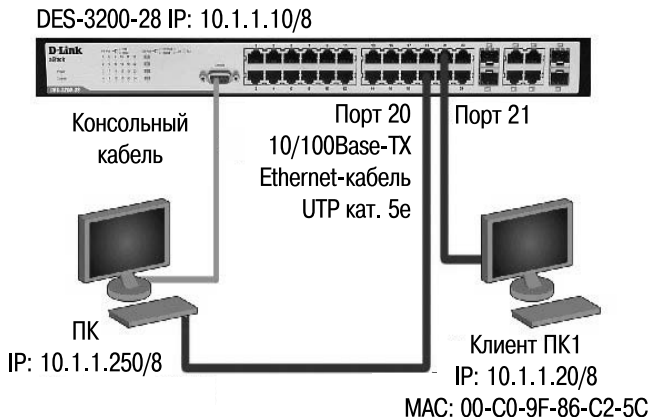
В данной лабораторной работе изучаются основные команды мониторинга работы коммутатора.

Цель: Изучить процесс мониторинга состояния коммутатора.

Оборудование:

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

Схема 1:



1. Настройка DES-3200-28

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

Просмотрите загрузку CPU коммутатора

show utilization cpu

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

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

Посмотрите загрузку портов коммутатора

show utilization ports 1-24

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

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

Посмотрите пакеты, передаваемые станцией ПК1, подключенной к порту 21

show packet ports 21

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

Посмотрите статистику об ошибках пакетов, принимаемых и передаваемых через порт 21

show error ports 21

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

Очистите счетчики статистики на порте 21

clear counters ports 21

Примечание. В случае устранения выявленных ошибок или проверки отчета загрузки портов можно обнулить устаревшие данные.

1.3. Изучение команд просмотра сессий подключенных к коммутатору пользователей и Log-файла коммутатора.

Проверьте сессии пользователей,
подключенных к коммутатору *show session*

Просмотрите Log-файл коммутатора *show log*

Просмотрите Log-файл коммутатора,
начиная с определенного индекса *show log index 25*

Очистите Log-файл *clear log*

1.4. Команда диагностики кабелей

Протестируйте состояние медных
кабелей, подключенных к портам
коммутатора *cable_diag ports all*

Примечание. Данная функция позволяет определить состояние пар подключенного к порту коммутатора медного кабеля, а также его длину. Функция определяет следующие повреждения кабеля: разомкнутая цепь (Open Circuit) и короткое замыкание (Short Circuit).

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, доступная или занимаемая для передачи потока данных, измеряется в Кбит/с, Мбит/с, Гбит/с.

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 две или несколько физических сетей и передающее кадры из одной сети в другую. 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 избежать 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 ответственности 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. Соотношение ожидаемых и полученных по каналу вспомогательных элементов сетевых служб. Чем выше это соотношение, тем надежнее линия.

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 (RJ45) 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 специ-

ально 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 обрабатываются перед их отправкой через соответствующий порт. Обработка включает расчет CRC и проверку адреса приемника. Кроме того, ка-

дры 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.

Switch LAN Коммутируемая сеть. Локальная сеть с коммутаторами.

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 сконфигурированных таким образом (при помощи программного обеспечения), что обмен данными между ними происходит так, как будто они подключены к одному кабелю, хотя на самом деле находятся в разных сегментах локальной сети. VLAN основаны на логическом соединении.

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

X

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

W

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

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

Литература

1. *Смирнова Е.В., Пролетарский А.В., Баскаков И.В., Федотов Р.А.* Управление коммутируемой средой. М.: РУСАКИ, 2011. 335 с.
2. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2000.
3. *Федотов Р.А., Пролетарский А.В., Баскаков И.В.* Методические указания к лабораторным работам по курсу «Коммутируемые сети». М.: Издательство МГОУ, 2008. 70 с.
4. Руководство по технологиям объединенных сетей. 3-е издание. Пер. с англ. М.: Издательский дом «Вильямс», 2002.
5. *Вегишна Шринивас.* Качество обслуживания в сетях IP. Пер. с англ. М.: Издательский дом «Вильямс», 2003.
6. *Scott Mueller.* Upgrading and Repairing Networks, Third Edition. Que, 2002.
7. *Panos C. Lekkas.* Network Processors. The McGraw-Hill Companies, 2003.
8. Руководства пользователя коммутаторов D-Link и учебные материалы компании D-Link [электронный ресурс] <ftp://ftp.dlink.ru/>
9. *Бараиш Л.* Коммутаторы в локальных сетях. [электронный ресурс] <http://desna.kiev.ua>
10. History of LAN Switching. [электронный ресурс] <http://www.myipaddressinfo.com>
11. *Жилкина Н.* Сменные интерфейсы // Журнал сетевых решений/ LAN. 2004. № 05.
12. Evolution: 20 years of switching fabric. Ori Aruj, Dune Networks [электронный ресурс] <http://www.commsdesign.com>
13. On-chip Global Interconnects for Networking ASICs [электронный ресурс] <http://www.lsi.com>
14. *Andreas D. Bovopoulos and Micha Zeiger.* Shared-Memory Fabrics Meet 10-Gbit Backplane Demands. TeraChip, Inc. [электронный ресурс] <http://www.commsdesign.com>
15. *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>
16. An improved algorithm for CIOQ switches. Yossi Azar, Yossi Richter. [электронный ресурс] <http://portal.acm.org>
17. Сайт научной базы данных «SciVerse ScienceDirect» [электронный ресурс] <http://www.sciencedirect.com>
18. Сайт Института инженеров по электротехнике и электронике (IEEE, Institute of Electrical and Electronics Engineers) [электронный ресурс] <http://www.ieee.org>
19. Телекоммуникационные технологии. Сайт Натальи и Виктора Олифер [электронный ресурс] <http://www.olifer.co.uk/>
20. Internet RFC/STD/FYI/BCP Archives [электронный ресурс] <http://www.faqs.org/rfcs>

Учебное издание

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

ПОСТРОЕНИЕ КОММУТИРУЕМЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие

Литературный редактор *С. Перепелкина*
Корректор *О. Ривоненко*
Компьютерная верстка *Н. Овчинникова*

Подписано в печать 25.09.2011. Формат 60x90 ¹/₁₆.
Гарнитура Таймс. Бумага офсетная. Печать офсетная.
Усл. печ. л. 23. Тираж 2000 экз. Заказ №

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

ООО «БИНОМ. Лаборатория знаний»
125167, Москва, проезд Аэропорта, д. 3
Телефон: (499) 157-1902, (499) 157-5272
E-mail: binom@Lbz.ru, <http://www.Lbz.ru>