Министерство образования и науки Республики Казахстан
Карагандинский государственный университет
имени академика Е.А. Букетова

Амочаева Г.П., Алпысова Г.К., Роговая К.С.

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Учебное пособие

Караганда
2018

УДК 004.056
ББК 32.973.202я73
А62

Рекомендовано Ученым советом Карагандинского государственного университета им. Е.А. Букетова

А 62 Защита информации в телекоммуникационных системах. Учебное пособие / **Амочаева Г.П., Алпысова Г.К., Роговая К.С.** - Караганда: Изд-во «Полиграфист», 2018. –79 с.

ISBN 978-9965-39-737-0

В пособии рассмотрены функции обеспечения информационной безопасности сетей, контроль управлением доступом к сетям; описаны способы организации сетей, архитектуры проводных и беспроводных сетей с функциональными элементами информационной безопасности. Кроме теоретических сведений даны описания шести лабораторных работ.

Учебное пособие предназначено для студентов высших учебных заведений, обучающихся по направлениям подготовки бакалавров специальности «Радиотехника, электроника и телекоммуникации». Так же данное пособие может быть использовано для подготовки к проведению лабораторных работ по курсам «IP-телефония» для специальности «Радиотехника, электроника и телекоммуникации» и «Телекоммуникационные системы и оборудование» для специальности «Техническая физика».

УДК 004.056
ББК 32.973.202я73

Рецензенты: **Чиркова Л.В. –** к.т.н., профессор КарГУ им. Е.А.Букетова
Кусенова А.С., - к. х. н., доцент Карагандинского государственного технического университета
Хмельницкий М.И. - начальник производственно-технологической связи АО «АрселорМиттал Темиртау»

ISBN 978-9965-39-737-0

Введение

В телекоммуникационных системах предприятий и организаций хранится и обрабатывается критически важная информация, нарушение конфиденциальности, целостности или доступности которой может привести к нежелательным последствиям. Поэтому вопросам обеспечения информационной безопасности должно уделяться внимание на всех этапах разработки и эксплуатации телекоммуникационных систем, следовательно, современный специалист в области телекоммуникаций должен обладать знаниями и навыками обеспечения информационной безопасности.

В данном пособии изложен материал учебной дисциплины «Защита информации в телекоммуникационных системах», в ходе изучения которой студенты получают базовые знания о теории защиты информации, методах и средствах обеспечения информационной безопасности, а также практические навыки организации защиты информационных систем. Пособие включает в себя три раздела.

В разделе 1 «Информационная безопасность в коммутируемых сетях» рассматриваются способы организации проводных сетей Ethernet, топология проводных сетей Ethernet. Также делается обзор петлевых элементов сети, вспомогательных функций защиты от петель, агрегирования каналов связи для повышения их пропускной способности. Также приводится методика создания VLAN и способы защиты в таких сетях. Особое внимание уделено качеству обслуживания передачи данных.

Раздел 2 «Обеспечение безопасности и управление доступом к сети» включает описание основных принципов обеспечения сетевой безопасности. Также изучаются списки управления доступом (ACL), функции контроля над подключением узлов к портам коммутатора, аутентификация пользователей 802.1X. Подробно рассматривается безопасность архитектуры беспроводных сетей стандартов типа 802.11.

В разделе 3 «Лабораторный практикум» приведены описания 6 лабораторных работ на базе оборудования D-Link.

Перед выполнением лабораторных работ необходимо:

- при наличии, повторить конспект лекции по теме, соответствующей лабораторной работе;
- понять сущность способов защиты информации, изучаемых в лабораторных работах;
- ясно представлять себе ожидаемые результаты опытов и уметь их объяснять;
- изучить инструкцию по технике безопасности при выполнении работ в лаборатории.

Каждый студент, выполняя работу, должен вести необходимые записи и по окончании работы оформить отчет. Отчеты о лабораторных работах оформляются в соответствии с требованиями, указанными в описаниях работ.

ГЛАВА 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОММУТИРУЕМЫХ СЕТЯХ

1.1. Способы организации проводных сетей Ethernet

В настоящее время коммутаторы являются основным строительным блоком для создания локальных сетей (ЛС). Современные коммутаторы Ethernet сменили концентраторы и 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 (QoS), обеспечение безопасности и многих других. Также усовершенствовались функции управления коммутаторов, благодаря чему системные администраторы получили удобные средства настройки сетевых параметров, мониторинга и анализа трафика. Эволюция локальных сетей представлена на рис. 1.1.

Рис. 1.1. Эволюция сетей

В коммутаторах ЛС могут быть реализованы различные методы передачи кадров:

1) коммутации с функцией промежуточного хранения;

2) коммутация без функции буферизации;

3) коммутация с функцией быстрой передачи;

4) коммутация с функцией исключения фрагментов.

С появлением стандарта IEEE 802.3aa-2003 PoE, описывающего технологию передачи питания по 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.

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.

1.2. Топология проводных сетей Ethernet

В топологии организации проводных сетей Ethernet выделяют три основные топологии:

- топология «шина»;
- топология «звезда»;
- топология «кольцо», которая образуется, когда шинная топология замыкается в кольцо, тем самым образуя кольцевую структуру. При этом каждый коммутатор связан с двумя крайними точками сети.

– древовидная структура - наиболее популярная, часто используемая на данный момент структура, представляет собой комбинацию вышеперечисленных структур.

Топология «шина» - топология, при которой проводная сеть Ethernet организуется между элементами сети, выстроенными в линию, при этом каждый коммутатор может связываться только с двумя другими коммутаторами, образуя цепочку (рис. 1.2).

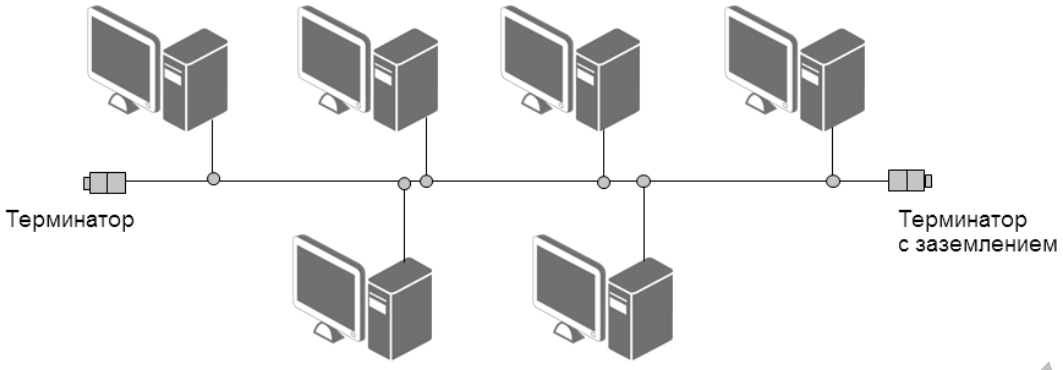


Рис. 1.2. Топология «шина»

Изменять топологию «шина» в случае модернизации сетей довольно просто - необходимо указать характеристики нового коммутатора в настройках последнего. Основной недостаток данной топологии - в случае выхода из строя одной из точек доступа, сеть разбивается на отдельные, не связанные между собой, сегменты [1].

В топологии «звезда», используется более четырех коммутаторов, один из них является центральным, который связан со всеми коммутаторами (рис. 1.3). Весь поток информации непосредственно идет через центральный коммутатор.

В случае отказа работы любого коммутатора в данной топологии, основная сеть остается работоспособна за исключением той подсети, где вышел из строя коммутатор. Но, если же выйдет из строя центральный коммутатор, то вся сеть будет не работоспособна [2].

Важным недостатком топологии «звезда» является то, что центральный коммутатор может связываться с ограниченным числом коммутаторов, так как число портов в коммутаторе ограничено.

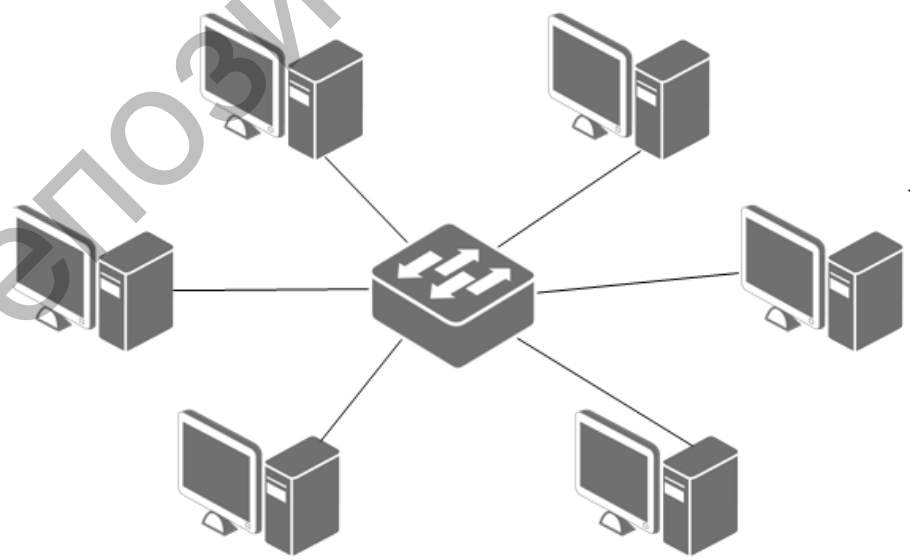


Рис. 1.3. Топология «звезда»

Топология «кольцо» образуется, когда шинная топология замыкается в кольцо, тем самым образуя кольцевую структуру, при этом каждый коммутатор

связан с двумя крайними коммутаторами (рис. 1.4). В данной топологии все коммутаторы равноправны, не выделяется центральный коммутатор как в топологии «звезда».

Основным преимуществом топологии «кольцо», по сравнению с вышеизложенными топологиями, заключается в том, что ретрансляция сигналов сети позволяет значительно расширить проводную сеть в целом.

Важно так же отметить, что при построении кольцевой проводной структуры используется протокол STP (Spanning tree Protokol – протокол связующего дерева). Этот протокол позволяет строить линии связи, свободные от петель.

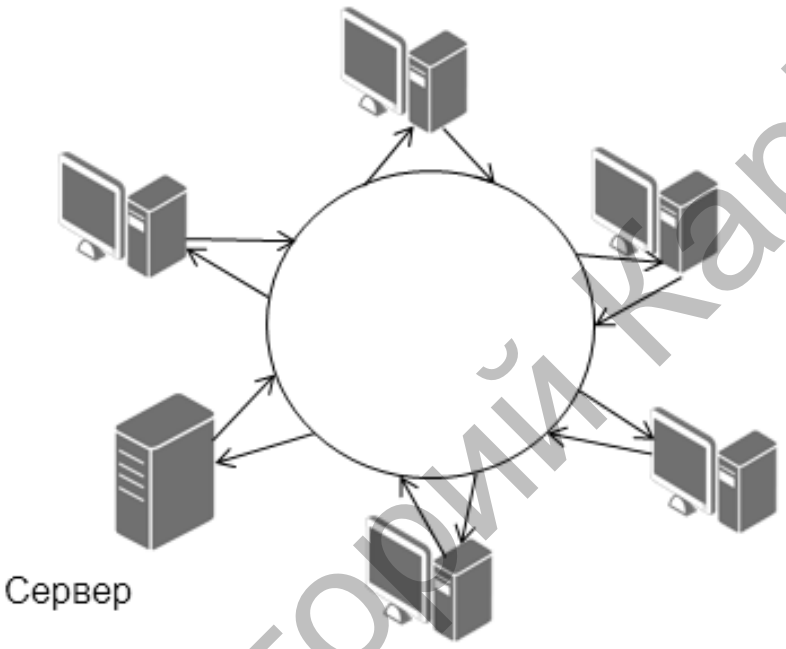
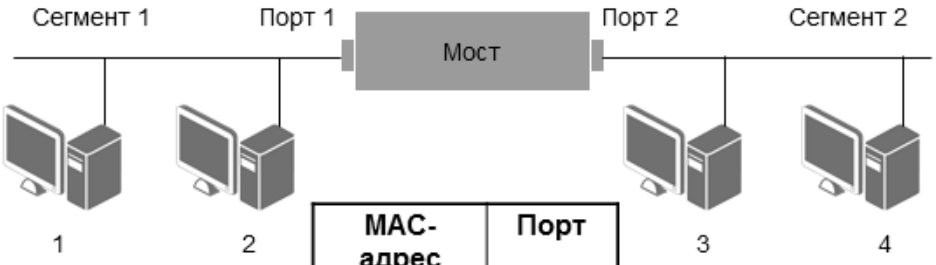


Рис. 1.4. Топология «кольцо»

При активизации данного протокола одна из связей между двумя коммутаторами виртуально отключается, для того чтобы не образовалось петля, при этом работает одна часть дуги топологии «кольцо». В случае выхода из строя коммутатора в рабочей дуге восстанавливается виртуально отключенный канал, и связь возникает по другой дуге. Таким образом, сохраняется работоспособность сети в целом [3].

Кроме этого, на канальном уровне модели OSI можно выстроить мостовую сегментацию сетей, которая позволит разделить пользователей по MAC-адресам и упорядочить передачу данных (рис.1.5).



MAC-адрес	Порт
1	1
2	1
3	2
4	2

Рис. 1.5. Мостовая сегментация сети

С развитием телекоммуникационных технологий и оборудования на сегодняшний день получила популярность древовидная структура, где элементы сети образуют сложную структуру, образуя тем самым интеллектуальные сети. Способ организации древовидной структуры приведен на рис. 1.6.

Как видно из рис. 1.6, древовидная структура представляет собой комбинацию из различных топологий, образуя тем самым сложную структуру.

Название данной структуры произошло от того, что трафик передается по оптимальным линиям связи, образуя древовидные линии передачи.

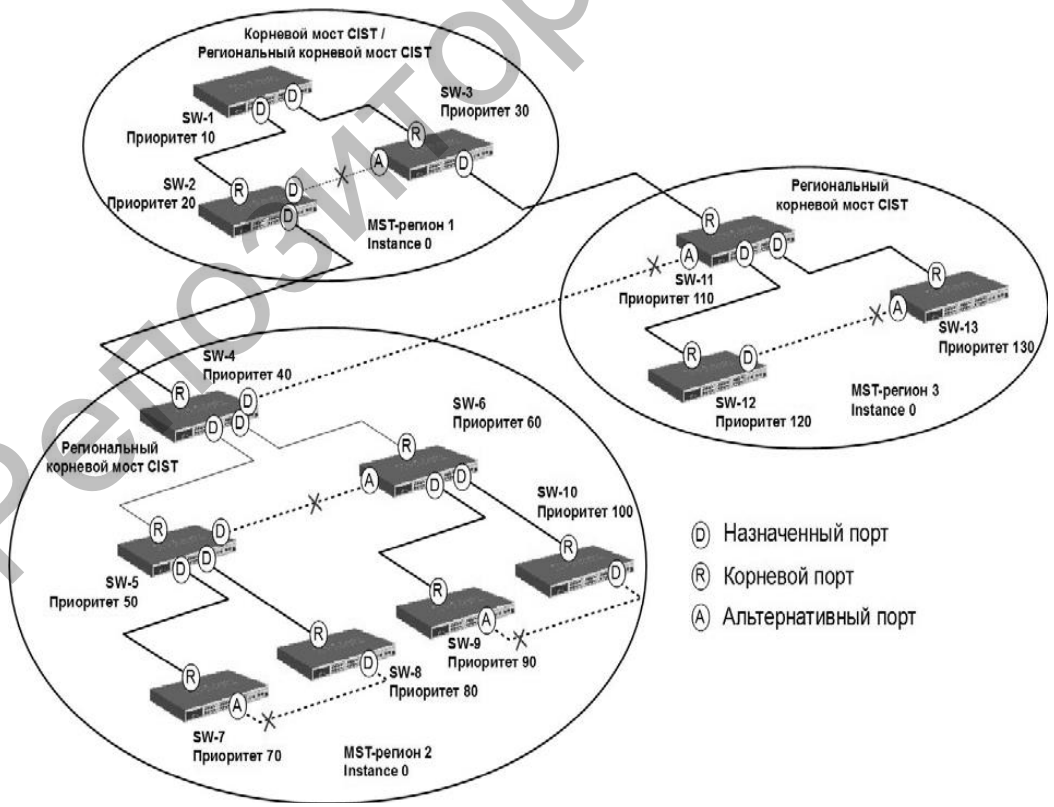


Рис. 1.6. Древовидная структура телекоммуникационной сети

В основном известные нам коммутаторы работают на канальном уровне мо-

дели OSI (рис.1.7), но существуют также коммутаторы, работающие на сетевом уровне данной модели. Эти коммутаторы имеют дополнительные функциональные возможности.

Разница между такими коммутаторами состоит в их возможности фильтровать кадры, передавать их от одного рабочего узла к другому и коммутировать. Они носят названия *L2 Switch* и *L3 Switch*. Основные особенности данных коммутаторов показаны на рис. 1.8.

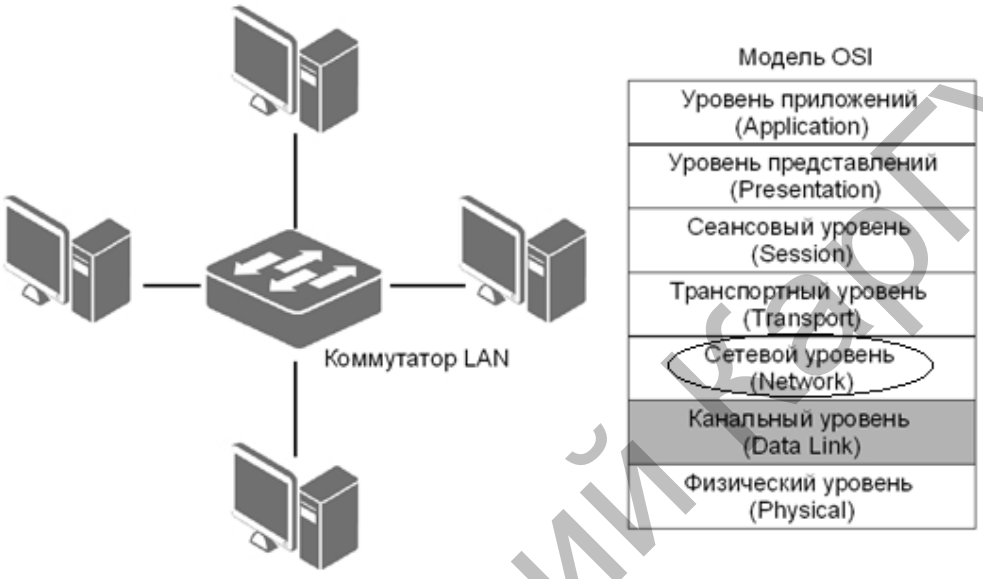


Рис. 1.7. Уровни модели OSI

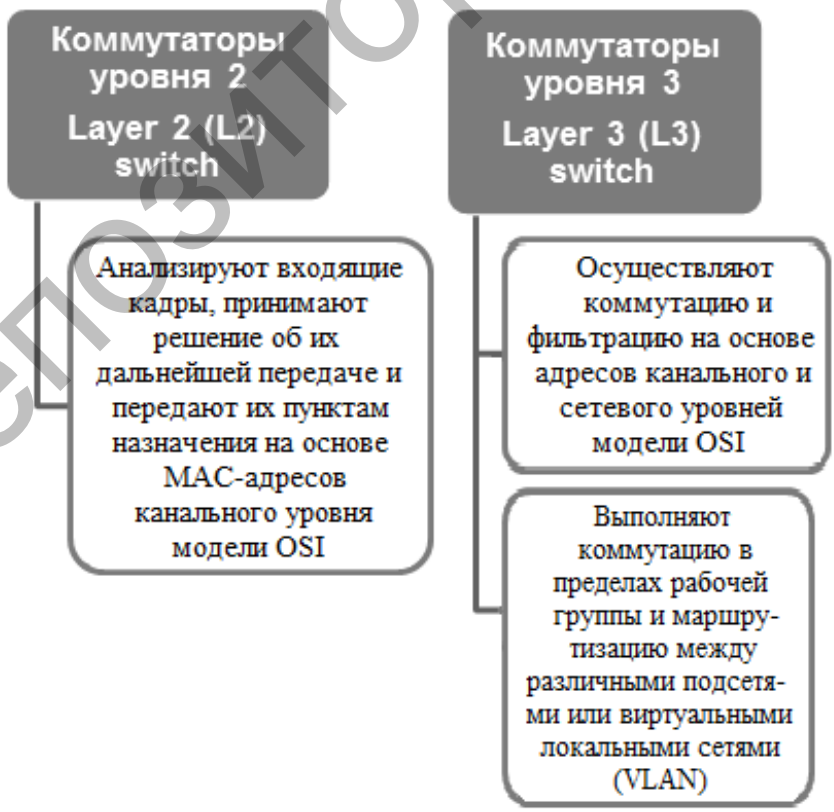


Рис. 1.8. Функциональные возможности коммутаторов

Рассмотрим типы существующих коммутаторов.

1) ***Управляемые коммутаторы*** получили такое название потому, что они работают на двух уровнях модели OSI: канальном и сетевом. Данные коммутаторы предоставляют пользователю большой выбор пользовательских интерфейсов, обладают возможностью установки дополнительных модулей и высокоскоростной внутренней магистралью, имеют возможность стекирования (рис.1.9).

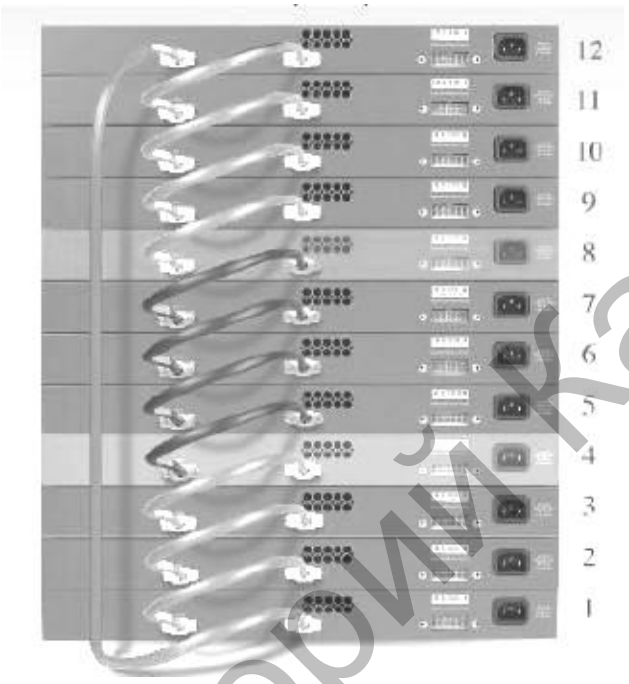


Рис.1.9. Стекирование коммутаторов

Управление коммутаторами может быть осуществлено с помощью командной строки (CLI), SNMP протокола Web-интерфейса. Такие коммутаторы применяются в корпоративных сетях крупных и средних предприятий, сети провайдеров услуг и др. (рис.1.10).

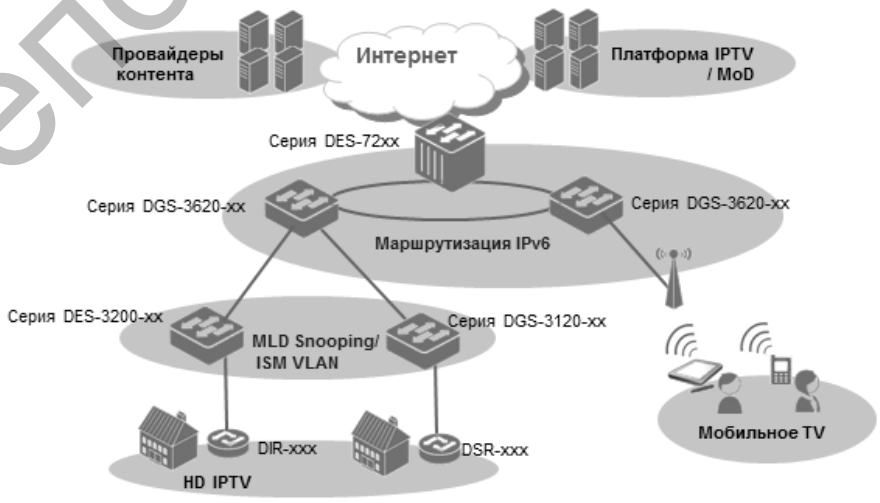


Рис. 1.10. Пример использования управляемых коммутаторов в корпоративном бизнесе

2) ***Настраиваемые коммутаторы*** получили такое название благодаря тому, что они позволяют настраивать выборочные определенные сетевые параметры с помощью Web-интерфейса или командной строки (CLI). Такие коммутаторы применяются в малых сетях провайдера услуг, в корпоративных малых и средних предприятиях и др. Пример использования таких коммутаторов в структуре предприятия показан на рисунке 1.11.

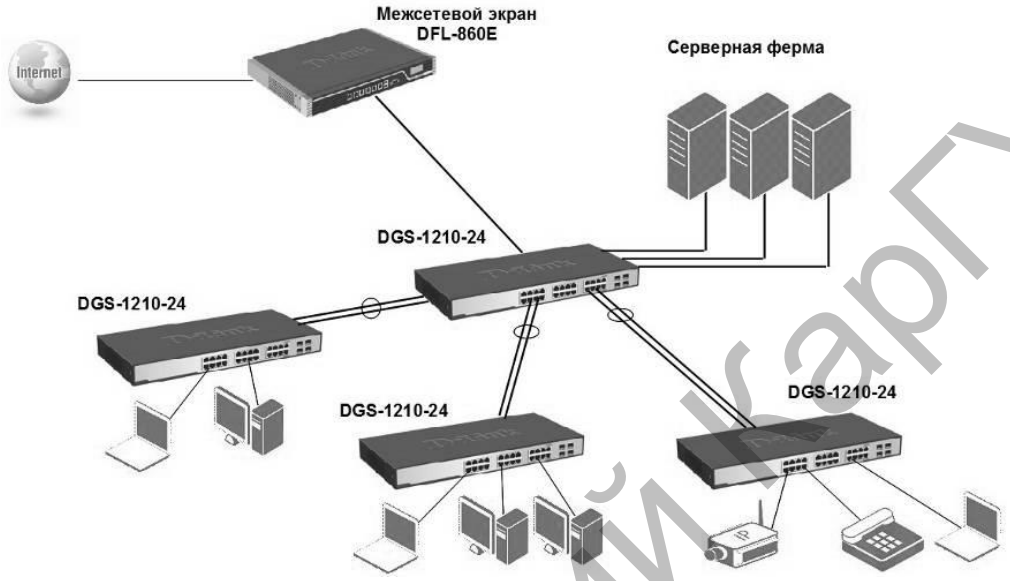


Рис. 1.11. Пример использования настраиваемых коммутаторов в корпоративном бизнесе

3) ***Неуправляемые коммутаторы*** получили такое название потому, что они не поддерживают функции управления и настройки. Такие коммутаторы имеют предустановленные функциональности, которые нельзя изменить или подкорректировать. Неуправляемые коммутаторы применяются в сетях малого бизнеса, в таких структурах, где сети не требуют внедрения дополнительных настроек. Пример использования неуправляемого коммутатора представлен на рисунке 1.12.

Рис. 1.12. Пример использования неуправляемого коммутатора в сети

Пример применения разноуровневых коммутаторов D-Link показан на рисунке 1.13.

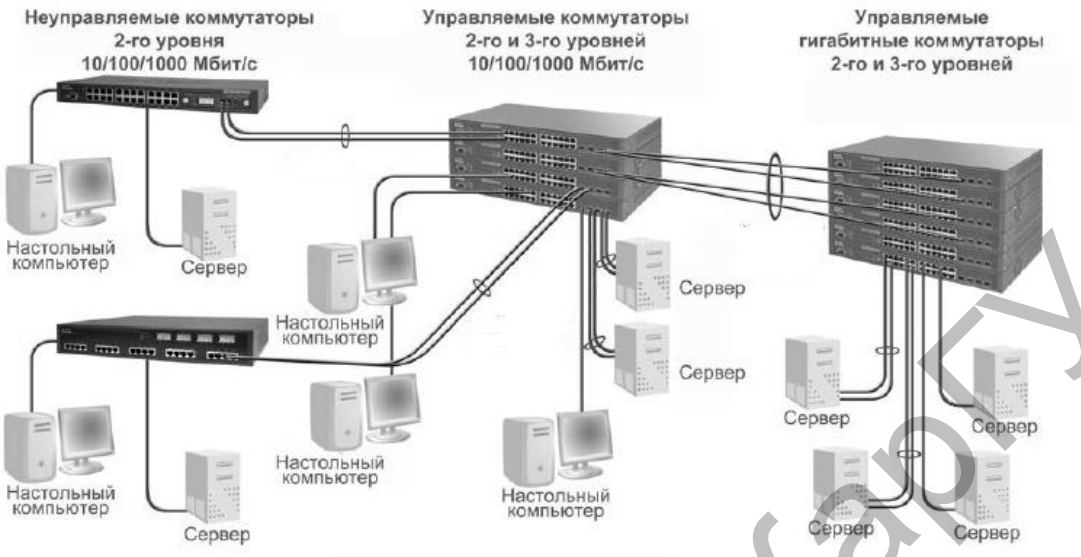


Рис. 1.13. Схема, построенная на коммутаторах

1.3. Петлевые элементы сети

Если между коммутаторами (элементами сети) создается более одной связи, то возникает петля (рис. 1.14).

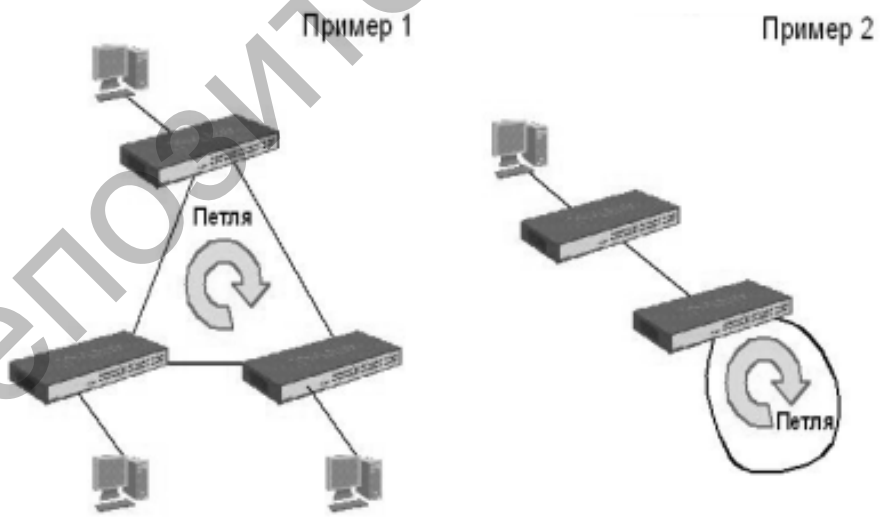


Рис. 1.14. Примеры петель между элементами сети

Сами непосредственно резервные линии актуальны, так как создают альтернативные линии связи. Но несколько линий связи, как мы уже сказали, создают петлю, которая создает следующие проблемы:

- широковещательный шторм пакетов;
- возникновение множественных копий кадров;

- зацикливание кадров.

Широковещательный шторм пакетов.

Широковещательный пакет несет в себе информацию о каждом элементе сети (компьютера, ноутбука и т.п.). В нем содержатся адреса данных элементов. Эти пакеты выпускаются элементами сети. Если в сети нет петель, то данные кадры благополучно доходят до других элементов сети, но если есть петля, как показано на рисунке 1.14, данные кадры зацикливаются и размножаются, тем самым занимая всю пропускную способность линий связи.

Возникновение множественных копий кадров.

При возникновении петель коммутатор может получить одновременно несколько одинаковых кадров, приходящих с различных линий связи.

Из-за этого таблица коммутации коммутатора не сможет определить расположение элементов в сети, будет постоянно обновляться, что приведет к значительным сбоям и загрузке центрального процессора коммутатора [4].

Для решения этих проблем и оптимизации телекоммуникационных сетей был разработан протокол связующего дерева STP, который прописан в стандарте IEEE 802.1D-1998.

Данный протокол позволяет создавать древовидную структуру сетей, свободных от петель, используя резервные линии связи. Так как данный протокол строит древовидную структуру, он получил название Spanning Tree Protocol (сокращенно STP). В дальнейшем протокол STP был модернизирован до скоростного протокола RSTP. Для крупных сетей был создан протокол MSTP с дополнительными функциями защиты от петель LoopBack Detection.

1.4. Вспомогательные функции защиты от петель

Функция LoopBack Detection (LBD) обеспечивает дополнительную защиту от петель. Она работает на втором уровне модели OSI. Существует два вида данной функции:

- STP LoopBack Detection;
- LoopBack Detection Independent STP.

Дополнительная функция LBD полезна тем, что управляемые коммутаторы могут образовать сеть с неуправляемыми коммутаторами, а последние в свою очередь не поддерживают протокол STP. В них может возникнуть петля, которая вызовет широковещательный шторм, как показано на рис. 1.15.

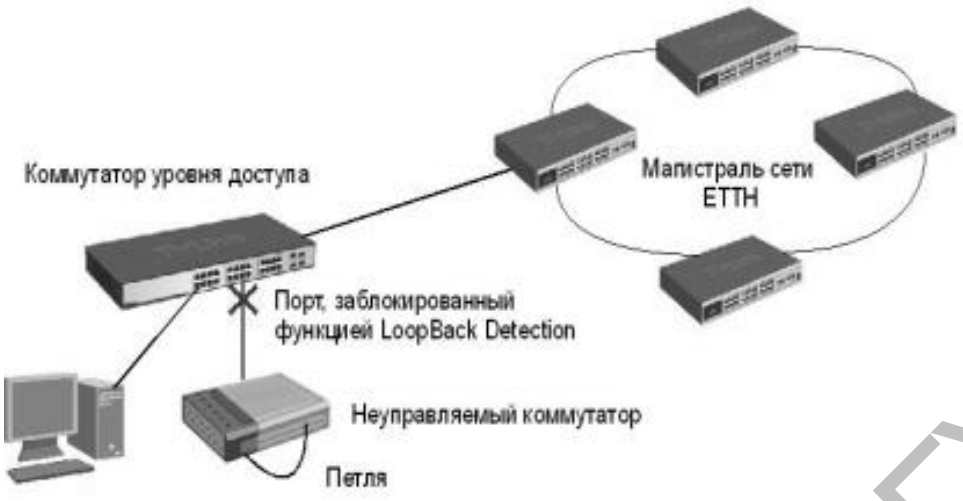


Рис. 1.15. Функция работы LoopBack Detection Independent STP

По умолчанию в коммутаторах функция LoopBack Detection отключена. После того как она активируется, управляемый коммутатор высылает BPDU кадры. Коммутатор определяет наличие петель, когда высланный им кадр BPDU возвращается на другой порт, затем он блокирует порт источника и порт приемника данного кадра. Порты будут заблокированы в течение установленного времени Recover Time. В дальнейшем снова происходит прослушивание сети до тех пор, пока петля не будет удалена.

В отличие от LoopBack Detection функция LoopBack Detection Independent STP не нуждается в активизации протокола STP на управляемом коммутаторе. В данной функции наличие петли определяется специальным служебным кадром ECTP (Ethernet Configuration Testing Protocol). При получении кадра ECTP этим же портом, порт коммутатора блокируется на неопределенное время Recover Time [5].

Функция LoopBack Detection Independent STP состоит из двух основных видов в зависимости от настройки сети и ее параметров:

- Port – Based;
- VLAN – Based.

1.5. Агрегирование каналов связи для повышения их пропускной способности

Суть агрегирования заключается в объединении нескольких линий связи для повышения пропускной способности сети. Агрегирование каналов показано на рис. 1.16.

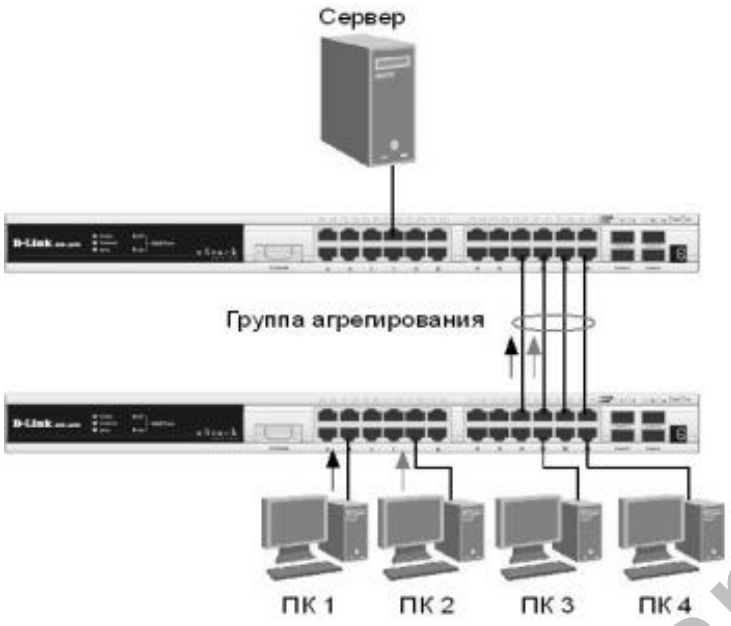


Рис. 1.16. Агрегирование каналов между коммутаторами

В отличие от протокола STP при агрегировании каналов все линии связи находятся в рабочем состоянии. Трафик распределяется равномерно по этим линиям связи, образуя высокоскоростную линию передачи. Если одна из линии выйдет из строя, трафик распределяется равномерно по оставшимся каналами связи.

Порты коммутатора, участвующие в агрегировании каналов связи, образуют группу портов, один из которых назначается главным портом (мастер-порт). Конфигурация данного мастера – порта распространяется на всю группу.

В большинстве случаев, чтобы не возникла неправильная передача кадров, используется статический метод распределения кадров. В этом случае за определенным портом закрепляется поток кадров определенного сеанса и кадры будут передаваться в строгой последовательности.

На данный момент коммутаторы D-Link поддерживают 9 видов алгоритма агрегирования портов, которые представлены на рис. 1.17.

Рис. 1.17. Виды алгоритмов агрегирования порта

По умолчанию в коммутаторах D–Link используется алгоритм MAC - адреса источника - mac_source –MAC.

Пример агрегирования с использованием алгоритма mac_source –MAC приведен на рис. 1.18.

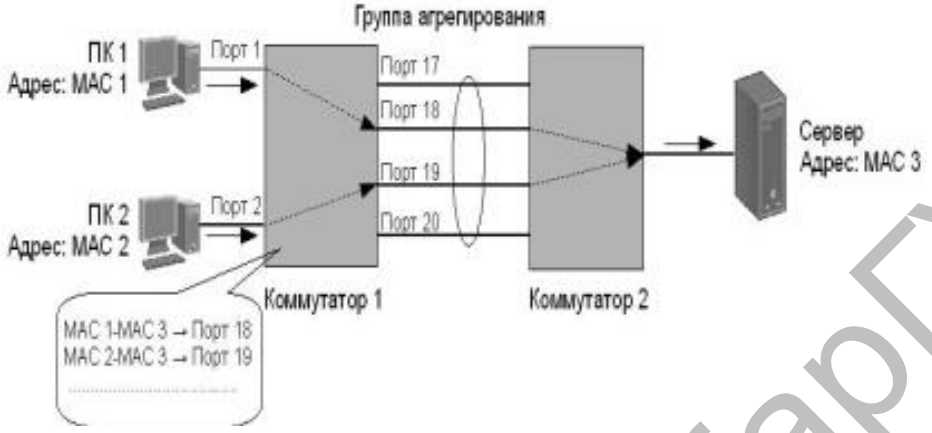


Рис. 1.18. Агрегирование каналов связи с использованием алгоритма mac_source

В основном агрегирование каналов применяется для связи коммутатор – коммутатор, коммутатор – файл сервер, так как между ними проходит основной поток трафика, соответственно необходима большая скорость передачи, чем у одиночной линии.

Важно отметить, что коммутаторы D-Link поддерживают два типа агрегирования каналов:

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

При статическом агрегировании все настройки портов делаются вручную, не допускается никаких изменений в группе портов.

Обработка пакетов данного механизма начинается с наибольшей очереди. Через установленное время, обслужив пользователей, он переключается на другой вид трафика и так по кругу.

Преимущества: не вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек.

Недостатки: нет согласования настроек с удаленной стороной. Ошибки в настройке могут привести к образованию петель.

При динамическом агрегировании используется специальный протокол управления агрегированным каналом – Link Aggregation Control Protocol (LACP).

Данный протокол согласует линии связи путем отправки управляющего кадра LACP. Порты, в которых настроен LACP, могут работать в пассивном и активном режимах. При активном режиме порты выполняют обработку и рассылку кадров, при пассивном выполняется только обработка управляющих кадров LACP. Рекомендуется на одном коммутаторе настроить все порты в активном режиме, а на другом в пассивном, чтобы было правильное автосогласование.

Преимущества: согласование настроек с удаленной стороной позволяет избежать ошибок и петель в сети. Поддержка standby-интерфейсов позволяет агрегировать до 16-ти портов, 8 из которых будут активными, а остальные в режиме standby.

Недостатки: вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек.

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 (Alow Control).

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

1.6. Виртуальные локальные сети (VLAN)

Виртуальные локальные сети очень важны, особенно для крупных локальных корпоративных сетей, так как они отделяют одну группу сетей от других. Так, например, административную часть можно отделить от другой, тем самым соблюсти конфиденциальность и защиту информации, произвести сегментирование трафика. Также создание VLAN экономически выгодно, так как используется меньшее количество оборудования и кабелей. Физическая сегментация сети на технологии VLAN приведена на рис. 1.19.

При использовании VLAN нет необходимости использовать несколько коммутаторов. Чтобы разделить отделы между собой, достаточно использовать всего один программируемый коммутатор, который разделит сеть на отдельные независимые между собой сегменты сети.

Особенно это удобно для построения как больших, так и небольших корпоративных сетей, при этом затраты будут минимальны. Так, например, при создании VLAN на малых предприятиях нет необходимости, как указывалось выше, использовать несколько коммутаторов, берется один управляемый коммутатор с достаточным числом портов. Затем все его порты делятся на определенные VLAN. После этого порты подключаются к неуправляемым коммутаторам, либо к компьютерам, в результате образуется сеть, поделенная на определенные сегменты.

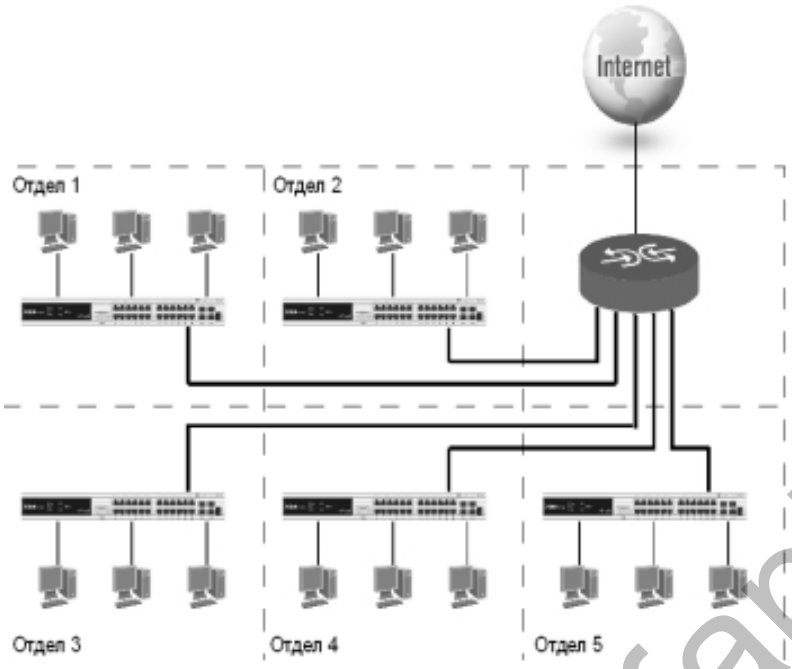


Рис. 1.19. Физическая сегментация сети по технологии VLAN

Использование технологии VLAN для одной логической сети с независимыми сегментами показано на рис. 1.20.

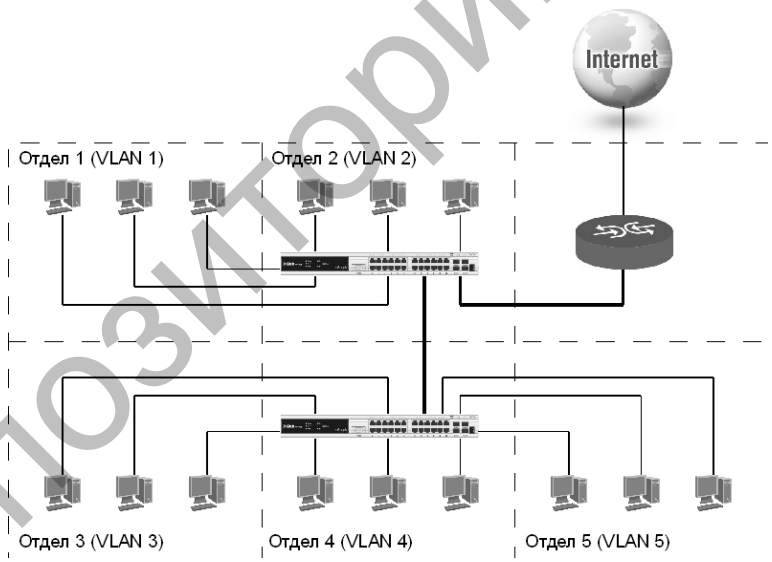


Рис. 1.20. Логическая группировка сетевых пользователей VLAN

Выделяют следующие типы VLAN, которые могут быть реализованы:

- с помощью портов;
- с использованием стандарта IEEE 802.1Q;
- с использованием стандарта IEEE 802.1ad (Q-in-Q VLAN);
- с использованием портов и протоколов IEEE 802.1v;
- с использованием MAC – адресов;

Кроме указанных типов, существуют и ассиметричные VLAN. Рассмотрим подробнее все представленные виды реализаций.

Реализация VLAN на основе портов.

При построении VLAN на основе портов (Port-Based VLAN) определённые порты в коммутаторе принадлежат заданному сегменту сети и не зависят от того, какой компьютер подключен к данному сегменту. К какому сегменту компьютеры подключены, к тому VLAN они и будут относиться (рис. 1.21).

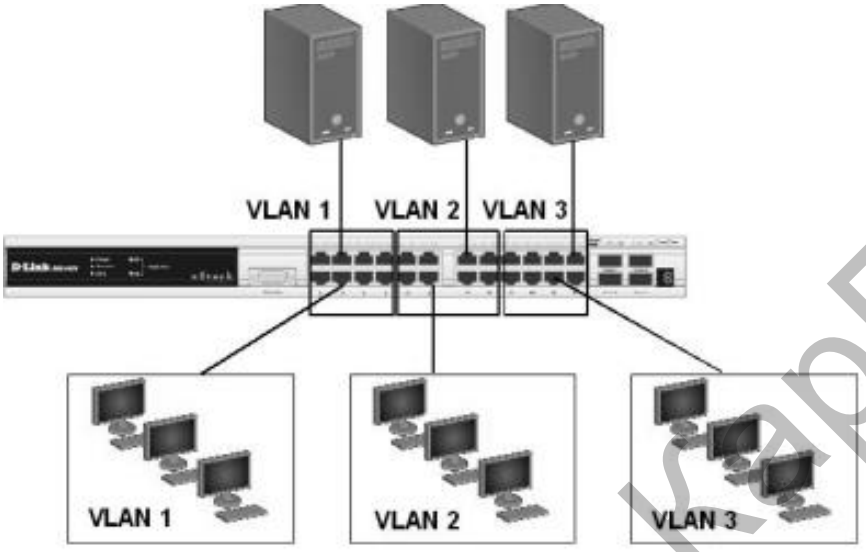


Рис. 1.21. Организация VLAN на основе портов

Выделим основные свойства VLAN на основе портов:

- способ организации портов на основе технологии VLAN строится на базе одного коммутатора, это очень удобно для маленьких отделов, так можно отделить, например, технический отдел от отдела продаж;
- простота реализации данной технологии;
- простота изменения логической топологи, которая не требует физических перестановок, необходимо просто изменить настройки портов.

Как уже указывалось выше, каждый порт входит в определенный VLAN. Для объединения VLAN 1 и VLAN 2 в пределах одного коммутатора, либо между двумя коммутаторами, необходимо использовать маршрутизаторы, работающие на сетевом уровне модели OSI. Каждый порт, представляющий определенный VLAN, должен быть подключен к маршрутизатору (рис. 1.22). Маршрутизатор создает таблицу маршрутизации и пересылает данные между VLAN.

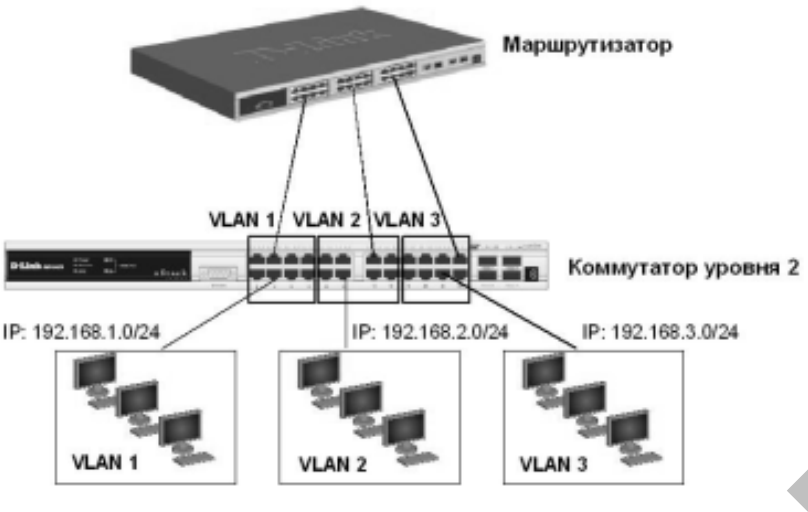


Рис. 1.22. Объединение VLAN на основе маршрутизатора

Недостаток такой технологии объединения VLAN заключается в том, что каждый VLAN необходимо соединять с маршрутизатором, а это приводит к дополнительным затратам на покупку кабеля.

VLAN на основе стандарта IEEE 802.1Q.

В отличие от построения VLAN на основе портов в стандарте IEEE 802.1 Q к кадру добавляется информация о принадлежности его к VLAN, что значительно упрощает организацию и объединение VLAN.

Приведем основные преимущества построение VLAN на основе стандарта IEEE 802.1 Q:

- удобные настройки, гибкость различных вариантов комбинаций VLAN, как на базе одного коммутатора, так и при реализации сети в целом;
- технология позволяет использовать протокол защиты от петель Spanning Tree Protocol, что весьма удобно для крупных корпоративных сетей при построении древовидной структуры;
- возможность извлекать и добавлять теги с заголовка кадра позволяет использовать коммутатор в сетях, которые не поддерживают стандарт IEEE 802.1 Q [6].

Способ организации VLAN на основе стандарта IEEE 802.1 Q приведен на рис. 1.23.

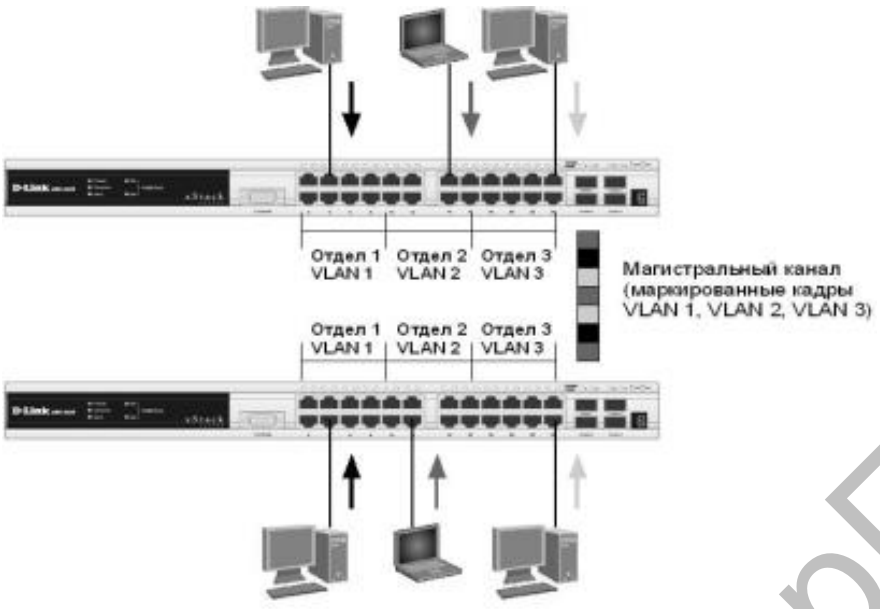


Рис. 1.23. Способ организации VLAN на основе стандарта 802.11Q с применением магистральной линии связи

Приведем основные характеристики стандарта 802.11Q, касающиеся работы с кадром:

- маркировка кадра (tagging) - добавление заголовка к кадру. Заголовок несет информацию о принадлежности кадра к определенному VLAN;
- извлечение тега из кадра (untagging) - извлечение заголовка из кадра;
- VID (VLANID) – идентификатор VLAN;
- PVID – идентификатор порта;
- входной порт (Ingress Port) – порт, на который приходят кадры и где принимается решение о принадлежности их к определенному VLAN;
- выходной порт (Egress Port) – порт с которого кадры передаются на другие сетевые устройства.

На коммутаторе, поддерживающем технологию 802.11Q, можно настроить любой порт, как маркированный (tagged), так и немаркированный (untagged). Такая технология позволяет настроить VLAN между несколькими коммутаторами, поддерживающими стандарт 802.1Q, как показано на рис. 1.24.

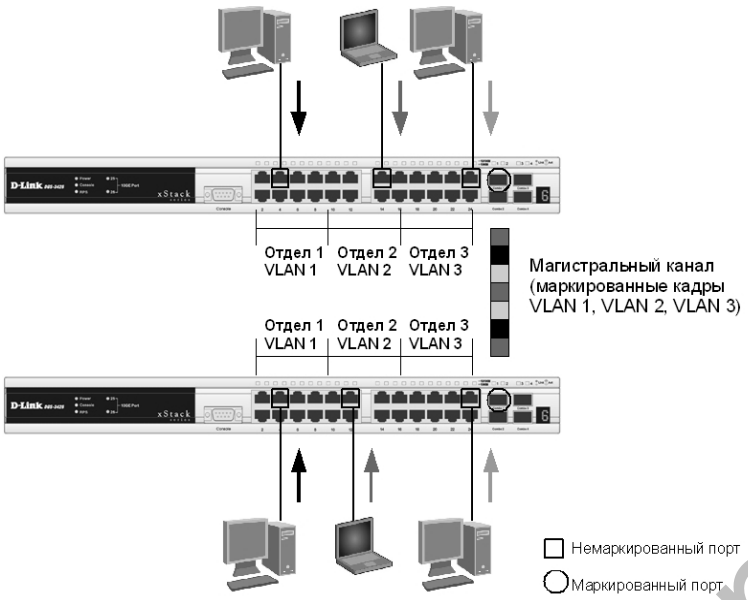


Рис. 1.24. VLAN между двумя коммутаторами с использованием маркировки кадров

Так же на коммутаторах с помощью технологии 802.1Q и большого количества точек доступа можно построить корпоративную сеть и разбить ее на подсети VLAN. Рассмотрим проектирование телекоммуникационной сети на предприятии.

Функция ***802.1X Guest VLAN*** используется для создания гостевой виртуальной частной сети, которая ограничивает неаутентифицированным пользователям права доступа. Алгоритм такого процесса представлен на рис. 1.25.

Рис. 1.25. Алгоритм процесса аутентификации с использованием Guest VLAN

При неуспешном процессе аутентификации клиент останется в Guest VLAN с ограниченными правами и доступом (рис. 1.26). При этом процессе клиент получает только доступ в Интернет, а сервер конфиденциальной информации для него не доступен.

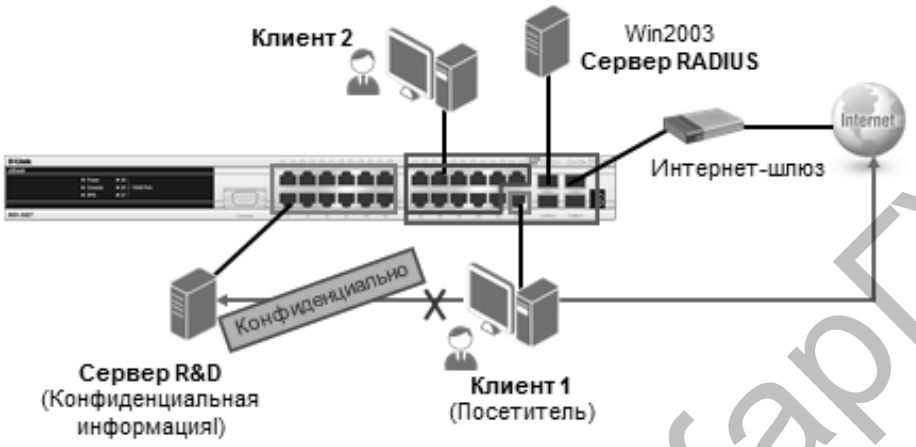


Рис. 1.26. Функция 802.1X Guest VLAN, при которой аутентификация не пройдена

При успешном процессе аутентификации, клиент динамически помещается в доверенную область и получает доступ к конфиденциальной информации на сервере (рис. 1.27).

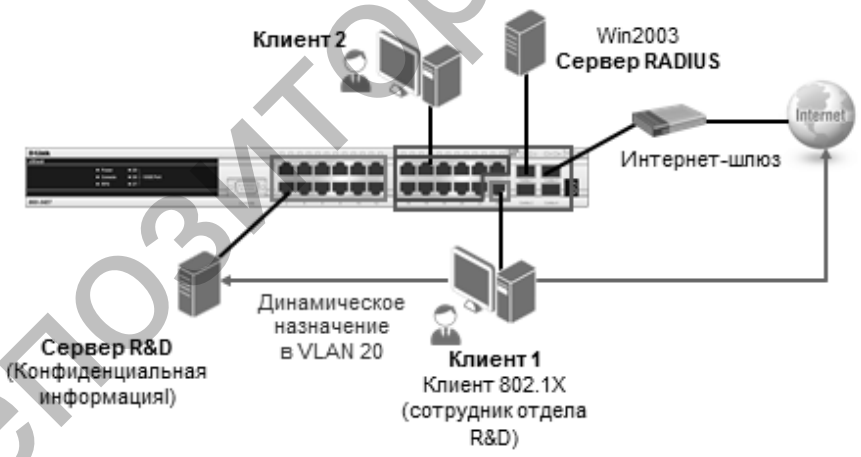


Рис. 1.27. Функция 802.1X Guest VLAN, при которой аутентификация успешно пройдена

Проектирование беспроводных сетей на предприятии связано с использованием больших количеств точек доступа. Все точки доступа образуют связь через проводную линию Ethernet, через которую администратор управляет данными точками доступа.

Сама по себе беспроводная связь в таких масштабах, как в предприятиях не организовывается, а является сегментом интегрированной телекоммуникационной инфраструктурой.

Непосредственно на предприятии используются виртуальные сети VLAN. Применение VLAN связано с тем, чтобы отделить различные подразделения предприятия, например, отделить бухгалтерию от отдела рабочего коллектива. Организация сети в режиме VLAN основана на применении стандарта 802.1 Q, соответственно точки доступа должны поддерживать данную функцию.

Современные точки доступа фирмы D-Link поддерживают до 17 VLAN и 9 SSD на одном канале. Способ организации беспроводных точек в режиме VLAN показан на рис.1.28.

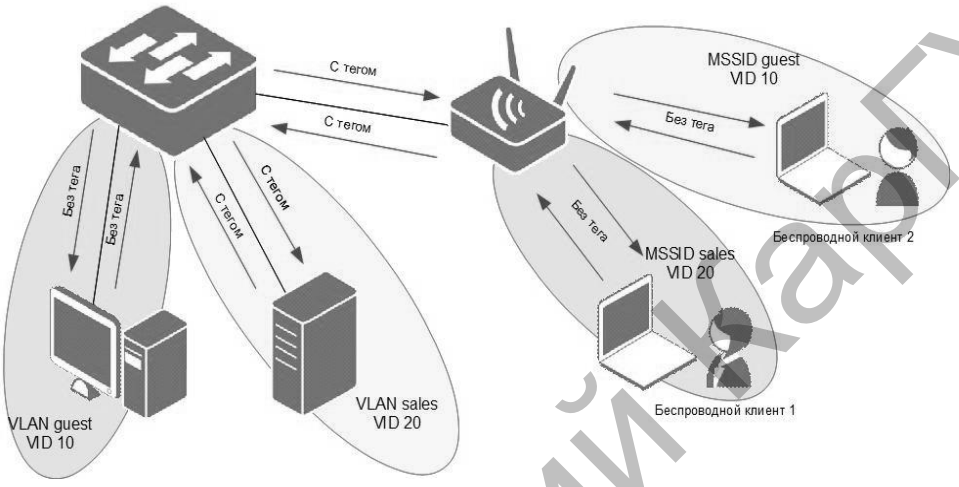


Рис. 1.28. Работа точек доступа в режиме VLAN

Точка доступа выступает в роли коммутатора с несколькими MSSD. При этом любой интерфейс точки доступа может быть выставлен как маркированный и немаркированный. Благодаря операции удаления tag в кадре возможно взаимодействие с теми элементами сети, которые не понимают маркированные кадры.

Пример организации интегрированной телекоммуникационной сети с использованием стандарта VLAN для точек доступа и коммутаторов показан на рис. 1.29.

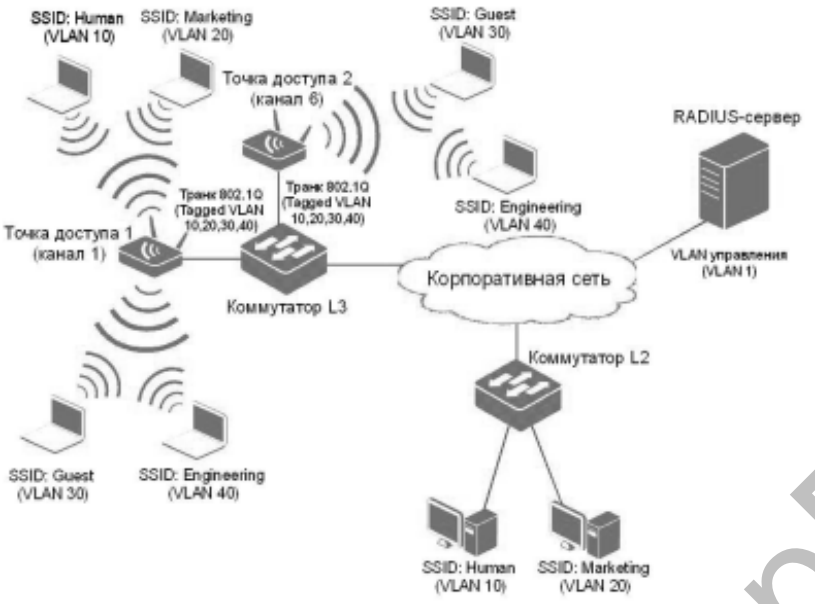


Рис. 1.29. Телекоммуникационная сеть в масштабах предприятия

Наличие в корпоративной сети VLAN позволяет внедрять различные виды услуг. Это касается организации всех уровней защиты и безопасности сети для определенных типов пользователей. С применением технологии VLAN возможно деление трафика между различными отделами предприятия. Так, с помощью технологии VLAN, можно выставить голосовой трафик приоритетным перед документальным.

1.7. Функция QoS. Качество обслуживание передачи данных

При передаче мультимедийного трафика (онлайн – игр, видеоконференций и др.), для которого требуется различная пропускная способность по одной линии передачи, необходимо внедрение специальных механизмов управления и дифференцирования трафика.

Эти механизмы предоставляет специально разработанный алгоритм, обозначенный как функция качества обслуживания (Quality of Service, QoS). Технология QoS позволяет выполнять различные виды работы над трафиком, в частности, его дифференцирование по приоритетам, а так же различные механизмы по обработке очередей.

Выделяют три основные модели реализации QoS в сети:

- **Integrated Services, IntServ** – интегрированные услуги. Данная модель основана на резервировании определенных сетевых ресурсов на заданную полосу пропускания, описанную в RAC 1633. Так, например, для IP – телефонии выделяется необходимая резервная полоса пропускания 64 Кбит/с, заданная кодеком G.711. Данную модель называют жесткой QoS, так как в ней предъявляются строгие требования к ресурсам сети.

- **Best Effort Service** – негарантированная доставка данных. Данная модель обеспечивает связь между узлами, но не гарантирует целостность доставки,

время доставки, пропускную способность и назначение приоритетов для трафика.

- **Differentiated Service, DiffServ** – дифференцированное обслуживание. В этой модели траффик подразделяется на определенные классы, у каждого из которых особые требования. Описана данная модель в RAC 2474, RAC 2475.

Для работы QoS на канальном уровне используется стандарт IEEE 802.1p, с помощью которого можно задать 8 уровней приоритета траффика (от 0 до 7, где 7 - наивысший приоритет).

В кадре выделяют три бита поля, отвечающие за приоритет (рис. 1.30). 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.

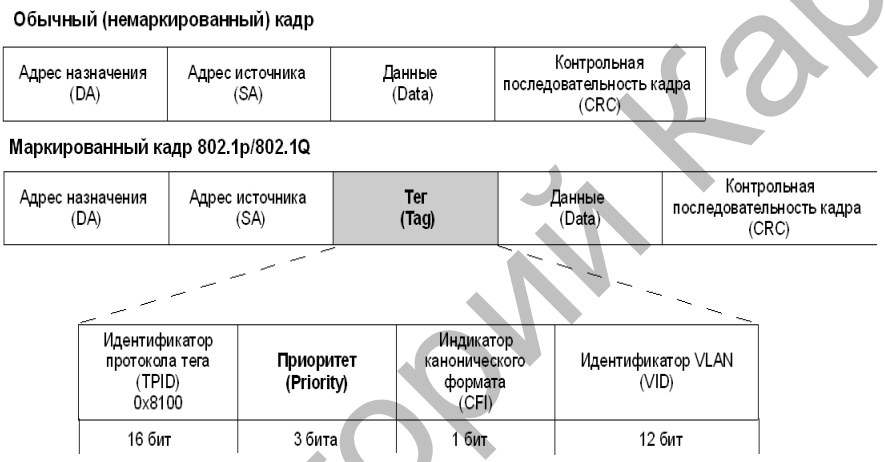


Рис. 1.30. Форма кадра IEEE 802.1Q с битами приоритета 802.1p

Поле DSCP было стандартизировано IETA с появлением модели DiffServ. Оно занимает 6 старших бит байта ToS и позволяет 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. 1.31).

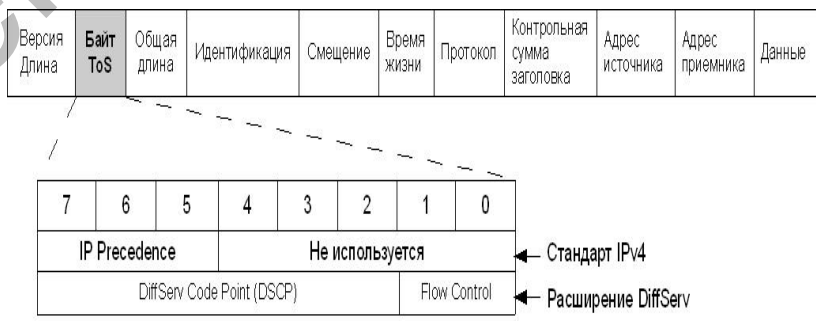


Рис. 1.31. Байт ToS заголовка IPv4

Для того, чтобы дифференцировать трафик, коммутаторы должны поддерживать от четырех до восьми очередей приоритета. Для выполнения заданной

операции необходимо настроить общий принцип обслуживания очередей и построить карту привязки очередей 802.1p, ToS, DSCP.

В начальных настройках коммутатора используется карта привязки очередей, которая показана на рис. 1.32. На рисунке указаны четыре и восемь очередей приоритета.

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

Рис. 1.32. Очереди приоритета в коммутаторах

После того, как были классифицированы приоритеты, коммутатор осуществляет маркировку пакетов (packet marking). Маркировка представляет собой запись/перезапись битов приоритетов, входящих в коммутатор пакетов.

В основном маркировка выполняется на граничных устройствах. Процесс маркировки кадров устройствами показан на рис. 1.33.

Наиболее часто возникают перегрузки на коммутаторе в местах, где участки сети подключены к коммутатору через порты, поддерживающие разные скорости. Если возникает перегрузка, пакеты попадают в буфер, затем выстраиваются в очередь в порядке их приоритетов. В дальнейшем передача происходит в соответствии с их приоритетами. Такой подход дает возможность управлять пропускной способностью линии связи. Перегрузка на коммутаторе показана на рис. 1.34.

Рис. 1.33. Маркировка кадров

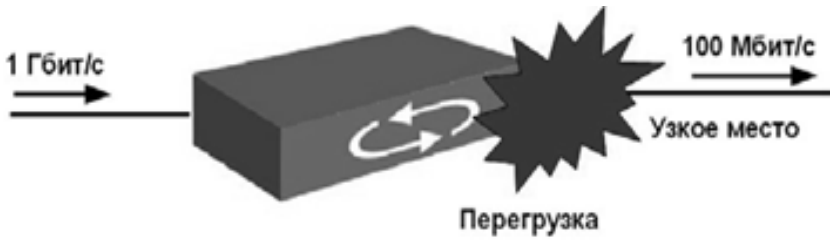


Рис. 1.34. Перегрузки на коммутаторе

Выделяют следующие механизмы обработки очередей при возникновении перегрузок в сети:

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

В механизме First-In, First-Out пакеты не классифицируются, а передаются по технологии «первый пришел, первый ушел». Все происходит в порядке следования очереди. Данный механизм передачи пакетов приведен на рис. 1.35.

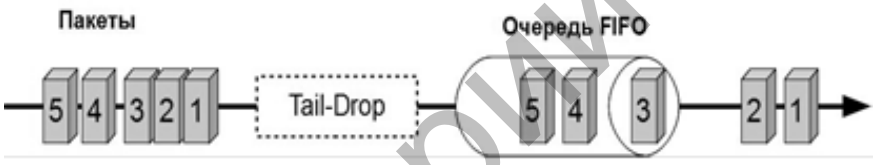


Рис. 1.35. Механизм передачи пакетов FIFO

В механизме передачи пакетов Priority Queuing выделяют четыре очереди приоритетов: высокий; средний; обычный; низкий.

Пакеты, которые относятся к высокому приоритету, обрабатываются первыми. И, таким образом, очереди будут обслуживаться в соответствии с их принадлежностью к определенному классу приоритетов. После того, как коммутатор обработал пакеты с высоким приоритетом, он переходит к средним и.т.д. по классификации. В данном механизме может произойти зависание низкого приоритетного трафика, так как до него очередь доходит последняя. Данный механизм передачи пакетов показан на рис. 1.36.

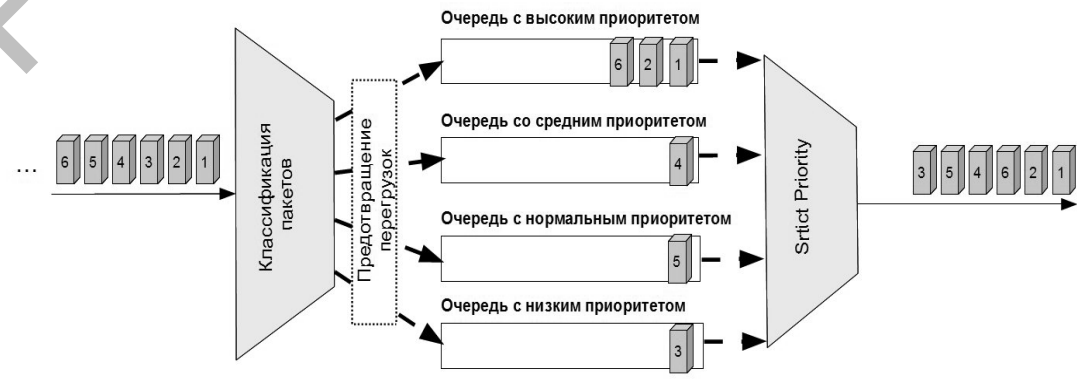


Рис. 1.36. Механизм передачи пакетов Priority Queuing

Механизм кругового обслуживания Weighted Round Robin делит всю полосу пропускания в процентном соотношении для каждой классификации пакетов. Если в какой-либо из классификаций наибольшее количество пакетов, то ей выделяется набольшая полоса пропускания (рис. 1.37).

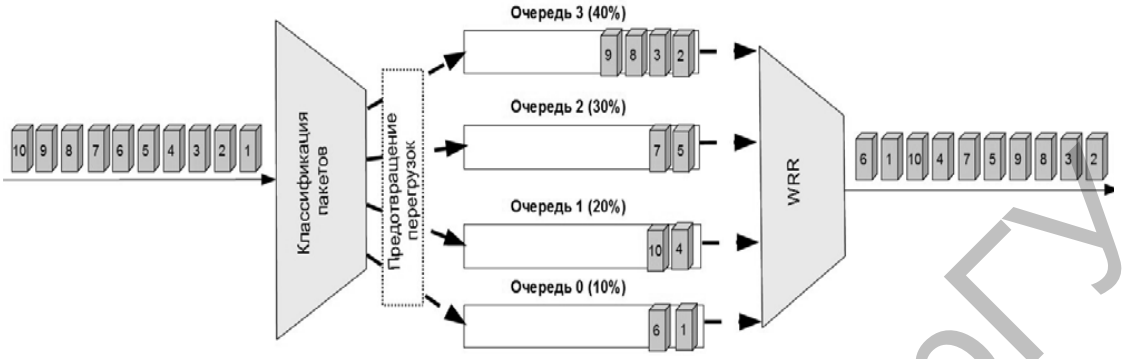


Рис. 1.37. Обслуживание очередей пакетов с использованием механизма WRR

Глава 2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И УПРАВЛЕНИЕ ДОСТУПОМ К СЕТИ

2.1. Принципы обеспечения сетевой безопасности

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 обычно 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 основным принципам обеспечения сетевой безопасности на базе оборудования D-Link.

D-Link предлагает комплексное решение вопроса обеспечения безопасности E2ES (*End-to-End Security*), включающий в себя следующие решения:

1) защита средствами межсетевых экранов (*Gateway Security*) – обеспечивает защиту внутренней сети от внешних атак;

2) защита конечного пользователя (*Endpoint Security*) –обеспечивает защиту внутренней сети от внутренних атак;

3) объединенная безопасность (*Joint Security*) – связующее звено между *Gateway Security* и *Endpoint*, которое объединяет использование коммутаторов и межсетевых экранов для защиты сети.

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

1) функции авторизации: Guest VLAN;

2) функции контроля над трафиком: ACL - Access Control List, TS - Traffic Segmentation;

3) функции аутентификации пользователей: IEEE 802.1X аутентификация, WAC - WEB-Based Access Control, MAC - MAC-Based Access Control;

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

5) функции контроля над подключением/адресацией узлов в сети: Port Security; IMPB - IP-MAC- Port Binding.

Решение Joint Security включает в себя функции:

- NAP;
- Zone Defense.

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:

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

2.2. Списки управления доступом (ACL)

ACL - Access Control List - списки управления доступом – это мощное средство фильтрации потоков данных с нулевыми потерями производительности. При этом проверка составляющих данных 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.

Списки управления доступом представляют собой последовательность условий проверки параметров пакетов данных (рис. 2.1). Когда сообщения поступают на входной порт, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определенными в ACL, и выполняет над пакетами данных одно из действий: Permit «Разрешить» или Deny «Запретить».

Критерии фильтрации могут быть определены на основе следующей информации, содержащейся в пакете данных:

1) порт коммутатора;
2) MAC/IP-адрес;
3) тип Ethernet/тип протокола;
4) VLAN;
5) 802.1p/DSCP;
6) порт TCP/UDP (тип приложения);
7) первые 80 байт пакета, включая поле данных.

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

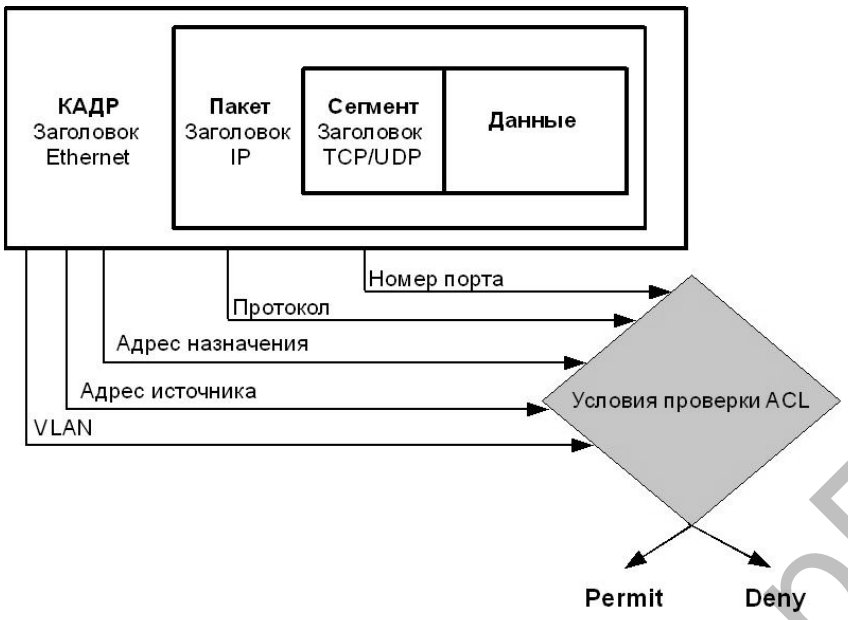


Рис. 2.1. Списки управления доступом (ACL)

Правила ACL и профили доступа.

Списки управления доступом состоят из правил и профилей доступа (Access Profile and Rule). Профили доступа, как правило, определяют такие типы критериев фильтрации, которые должны быть проверены непосредственно в пакетах данных. К ним относятся IP-адрес, MAC-адрес, VLAN, номер порта, и т.д.), а уже в правилах указываются значения их параметров. Любой 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 первого 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 пакету данных будет применено одно из действий, определенных в правиле: «Запретить», «Разрешить» или «Изменить содержимое поля пакета» (приоритет 802.1p/DSCP). Дальше пакет данных проверяться не будет. Если ни одно из правил не подходит, применяется политика по умолчанию, разрешающая прохождение всего трафика. Принцип работы ACL приведен на рис. 2.2.

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 исполь-

зуемое 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) позволят 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.

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

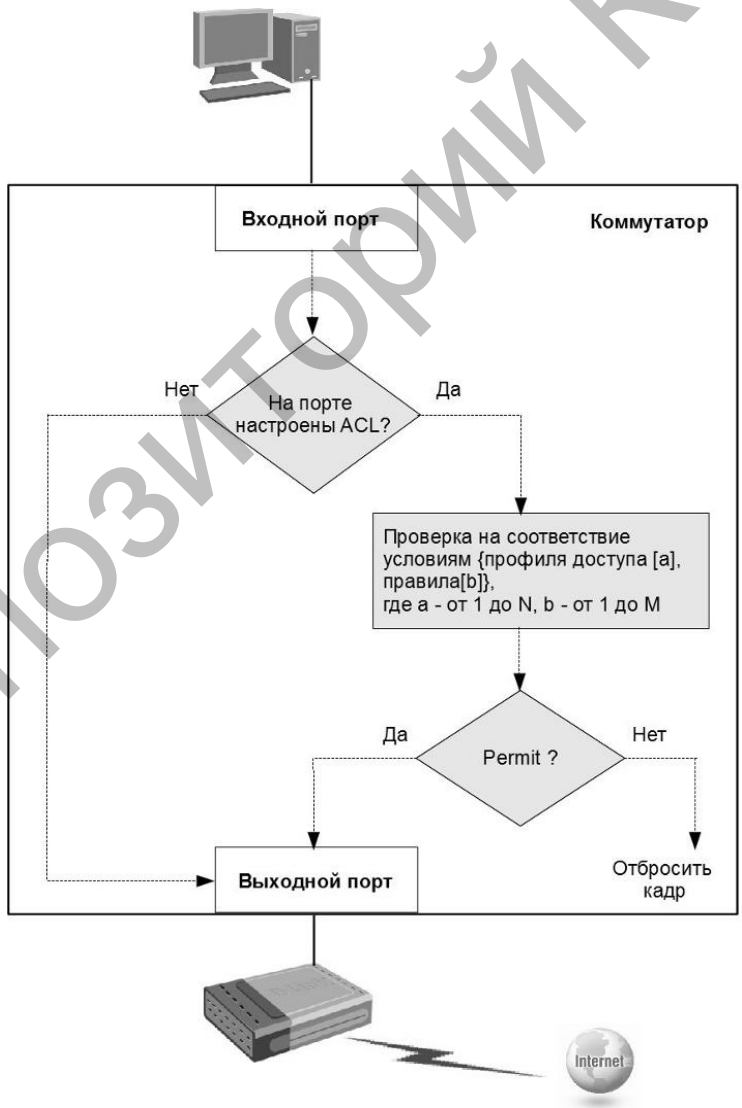


Рис. 2.2. Принцип работы (ACL)

Создание профиля доступа.

Создание профиля доступа - это процесс, который условно можно разделить на следующие основные шаги:

1) анализ задач фильтрации и определение типов профиля доступа – IP, Ethernet или Packet Content Filtering;

2) определение стратегии фильтрации.

Приведем примеры процессов создания профилей доступа:

- отбросить пакеты данных некоторых узлов и принять пакеты данных от всех остальных узлов. Данная стратегия может быть применима для такой сетевой среды, в которой имеется несколько узлов/протоколов портов/подсетей, для которых необходимо выполнять фильтрацию;

- принять пакеты данных от определенных узлов и отбросить пакеты данных остальных узлов. Данная стратегия может быть применима для такой сетевой среды, в которой имеется несколько узлов/протоколов портов/подсетей, пакеты данных от которых разрешены в сети. Трафик всех остальных узлов будет отбрасываться.

Далее, выбрав стратегию, необходимо определить какая маска профиля доступа (Access Profile Mask) необходима, и затем создать ее, используя команду create access_profile. Маска профиля доступа используется для указания битов значений полей IP-адрес, MAC-адрес, порт TCP/UDP и т.д., которые должны либо проверяться в пакете данных, либо игнорироваться.

Затем необходимо добавить правило профиля доступа (Access Profile Rule), связанное с данной маской профиля, используя команду config access_profile.

Правила профиля доступа должны проверяться в соответствии с присвоенным номером access_id. Причем чем меньше этот номер, тем раньше будет проверяться правило. Если же ни одно правило не сработало, то пакет данных пропускается.

В среде Quality of Service, после того как срабатывает правило, перед отправкой пакета данных биты 802.1p/DSCP могут быть заменены на новые высоко/низкоприоритетные значения.

Расчет значения маски профиля доступа.

Маска профиля доступа определяет, какие биты в значениях полей MAC-адрес, IP-адрес, порт UDP/TCP приходящих на коммутатор кадров должны проверяться, а какие игнорироваться. Биты маски профиля доступа могут иметь следующие значения:

1) цифра 1 означает проверку значения соответствующего бита поля пакета данных;

2) цифра 0 означает абсолютное игнорирование 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 такого адреса будет равна AA-AA-AA-AA-AA-AA. Если необходимо разрешить или запретить прохождение трафика любого узла из подсетей в диапазоне от 192.168.16.0/24 до 192.168.31.0/24 через коммутатор, то маска профиля

доступа будет рассчитываться, как показано на рис. 2.3.

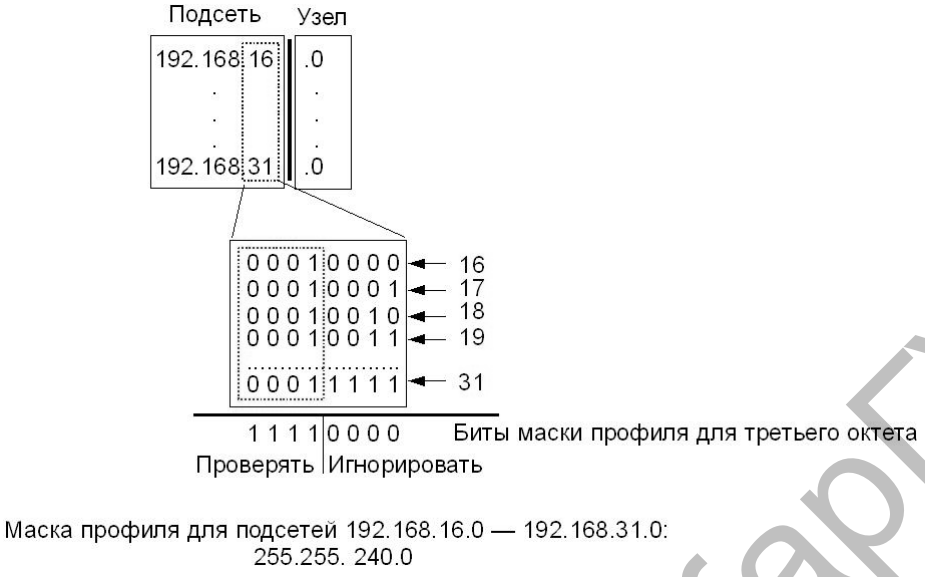


Рис. 2.3. Вычисление маски профиля

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 (0001111), имеющие одинаковые значения (0001) первых четырех битов. Последние четыре бита третьего октета IP-адреса маска профиля будет игнорировать, как малозначащие.

2.3. 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, коммутаторы 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.

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, опреде-

ляются по MAC-адресам. MAC-адреса могут быть назначены 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:

- постоянный (*Permanent*) режим, при котором занесенные в таблицу коммутации MAC-адреса никогда не устаревают, даже если коммутатор был перезагружен или при условии истечения времени, установленного таймером ADB Aging Time;
- удалить при сбросе настроек (*Delete on Reset*) – режим, используемый по умолчанию, при котором MAC-адреса, занесенные в таблицу коммутации, будут удалены после перезагрузки коммутатора;
- удалить при истечении времени (*Delete on TimeOut*) – режим, при котором MAC-адреса, занесенные в таблицу коммутации, устареют после истечения времени, установленного таймером ADB Aging Time и будут удалены.

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.

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 ADB Aging Time. Функция Port Security приведена на рис. 2.4.

Рис. 2.4. Функция Port Security

Функция IP-MAC-Port Binding.

Реализованная в коммутаторах D-Link функция IMPB (IP-MAC-Port Binding) позволяет осуществлять контроль доступа компьютеров в сеть, взяв за основу их MAC- и IP-адреса и порты подключения. Сетевой администратор может создать определенные записи, называемые «белым листом», которые связывают IP- и MAC-адреса компьютеров с портами коммутатора, к которым они подключены. Основываясь на этих записях, клиенты смогут получать доступ к сети со своих компьютеров только при совпадении всех необходимых составляющих. В противном случае, если при запросе на подключение у клиента связка IP-MAC порт будет отличаться от данных, которые были заранее сконфигурированы, коммутатор заблокирует MAC-адрес соответствующего узла и занесет его в зону, называемую «черный лист» (рис. 2.5).

Функция IP-MAC-Port Binding в основном была разработана для управления подключением связующих узлов в офисных сетях и сетях Ethernet-To-The-Home (*ETTH*). Помимо этого функция IMPB 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 содержит три режима работы: ACL Mode, DHCP Snooping Mode, а также установленный по умолчанию ARP Mode.

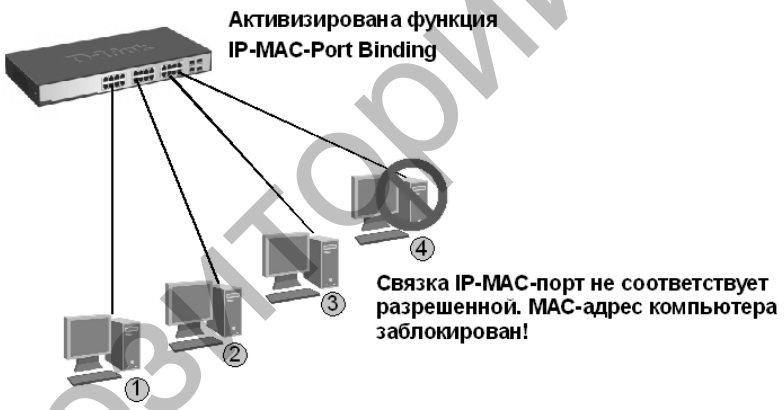


Рис. 2.5. Функция IP-MAC-Port Binding

В режиме работы *ACL Mode* коммутатор, основываясь на предустановленных администратором данных «белого листа» IMPB, создает правила ACL. Пакет с данными, связка MAC-IP которого отсутствует в данных «белого листа», будет заблокирован ACL. Если режим ACL отключен, правила для записей IMPB 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).

Коммутатор, работающий в режиме *DHCP Snooping*, динамически создает MAC-IP записи, основываясь на анализе пакетов DHCP и их привязке к портам коммутатора с функцией IMPB. При этом администратору не требуется создавать записи вручную. Коммутатор сам автоматически создает в таблице коммутации или аппаратной таблице ACL «белый лист» (при условии активизации

режима ACL).

ARP Mode - это режим, который используется по умолчанию, при настройке IP-MAC-Port Binding на портах коммутатора. При работе в таком режиме коммутатор проводит анализ ARP-пакетов и сопоставляет необходимые ему MAC-IP параметры пакета с предустановленной администратором MAC-IP связкой. При несовпадении минимум одного параметра, MAC-адрес узла будет размещен в таблице коммутации с пометкой «Drop» или «Отброшен». Если же все параметры совпадают, то MAC-адрес узла будет размещен в таблице коммутации с пометкой «Allow» или «Разрешен».

Внимание: режим DHCP Snooping отдельно от режимов ARP или ACL не используется.

Для того, чтобы активизировать функцию IMPB на порте, администратору необходимо указать режим его работы:

1) ***Strict Mode*** – режим, при котором порт заблокирован по умолчанию. Прежде чем передавать пакеты он будет отправлять их на ЦПУ для проверки совпадения их параметров IP-MAC 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.

2) ***Loose Mode*** – режим, при котором порт открыт по умолчанию. Порт будет заблокирован, как только через него пройдет первый недостоверный пакет. Порт проверяет только пакеты ARP и IP Broadcast.

2.4. Аутентификация пользователей 802.1X

Технология стандарта IEEE 802.1X описывает использование Extensible Authentication Protocol (EAP протокола) для поддержки аутентификации. Кроме того данная технология инкапсулирует передаваемые от клиента к серверам аутентификации данные. IEEE 802.1X стандарт позволяет осуществлять контроль доступа и не допускает подключения устройств без авторизации к локальной сети через порты коммутатора.

Аутентификационный сервер *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.

Протокол 802.1X не поддерживает работу на агрегированных каналах связи. Сеть с аутентификацией 802.1X приведена на рис. 2.6.

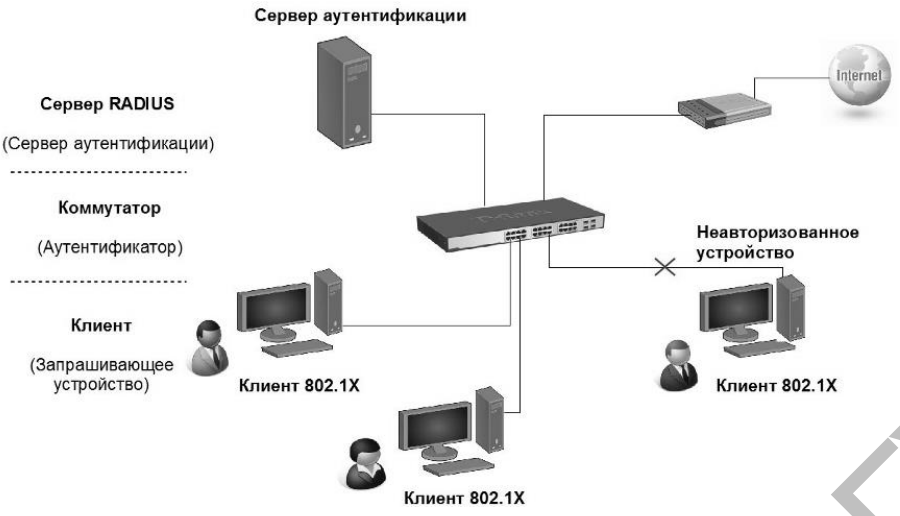


Рис. 2.6. Сеть с аутентификацией 802.1X

Роли устройств в стандарте 802.1X.

В стандарте IEEE 802.1X определяются три роли устройств:

- *Authenticator* (Аутентификатор);
- *Authentication Server* (Сервер аутентификации);
- *Client/Supplicant* (Клиент).

Client/Supplicant (Клиент) представляет собой рабочую станцию, запрашивающую доступ к локальной сети и сервисам коммутатора и отвечающую на запросы от коммутатора (рис. 2.7). На рабочей станции должно быть установлено программное обеспечение для 802.1X, например, то, которое встроено в операционную систему Microsoft Windows.

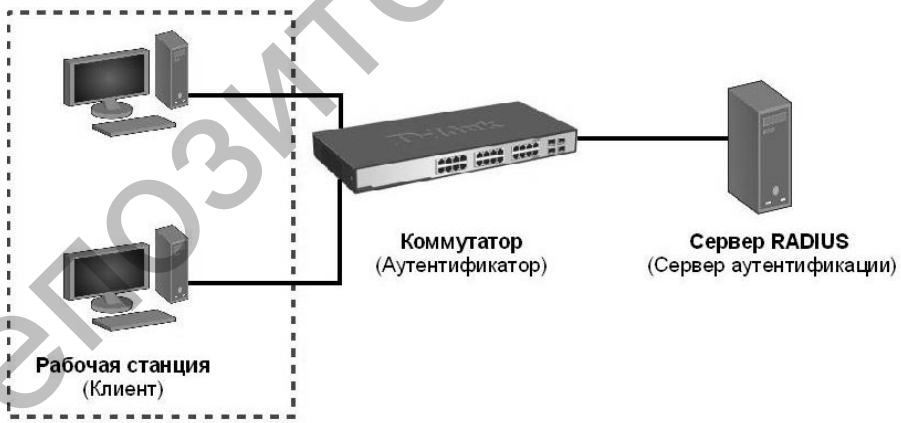


Рис. 2.7. Клиент 802.1X

Authentication Server (Сервер аутентификации) проверяет подлинность клиента и предоставляет коммутатору данные о разрешении или запрете предоставления доступа клиенту к локальной сети. Сервер Remote Authentication Dial-In User Service (RADIUS) работает в модели клиент/сервер, то есть передает всю информацию между ними (рис. 2.8).

Authenticator (Аутентификатор) выполняет функции управления физическим доступом к сети, взяв за основу статус аутентификации клиента (рис. 2.9). Роль аутентификатора выполняет коммутатор. Он является фактическим «по-

средником» между сервером аутентификации и клиентом: получает запрос на проверку подлинности данных от клиента, проверяет полученную информацию при помощи сервера аутентификации и отправляет обратный ответ клиенту.

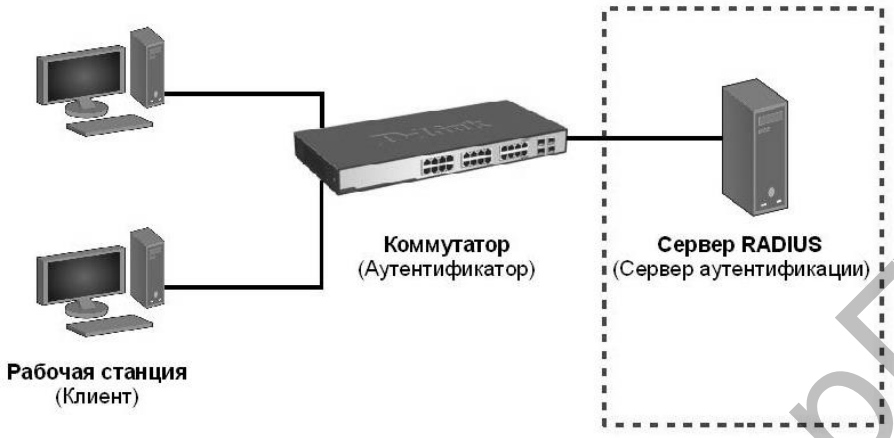


Рис. 2.8. Сервер аутентификации

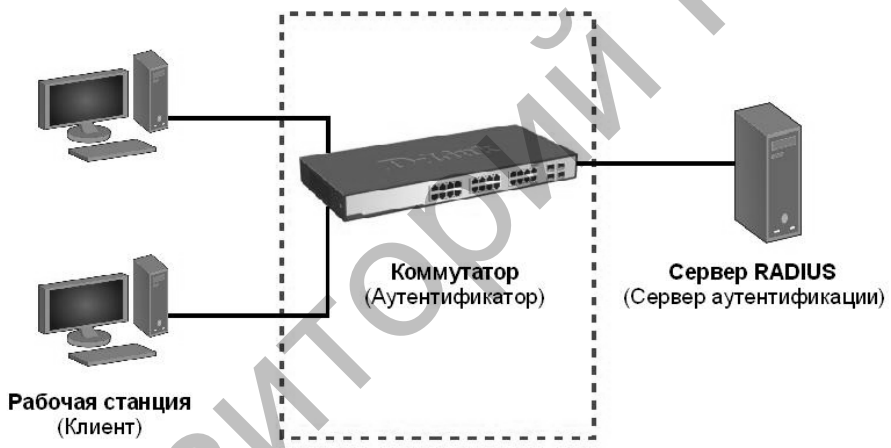


Рис. 2.9. Аутентификатор

Инициировать процесс аутентификации может 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 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. 2.10. показана схема обмена, инициируемого клиентом, где сервером RADIUS используется метод аутентификации One-Time-Password (OTP).

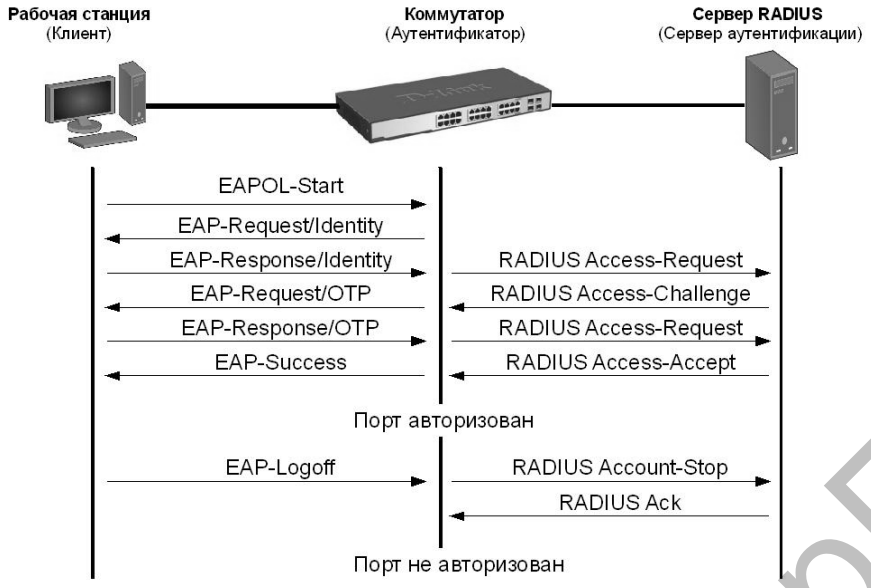


Рис. 2.10. Процесс аутентификации 802.1X

Коммутаторы D-Link поддерживают два типа реализации аутентификации 802.1X:

• Port-Based 802.1X: после того как порт был авторизован, любой пользователь, подключенный к нему, может получить доступ к сети (рис.2.11);

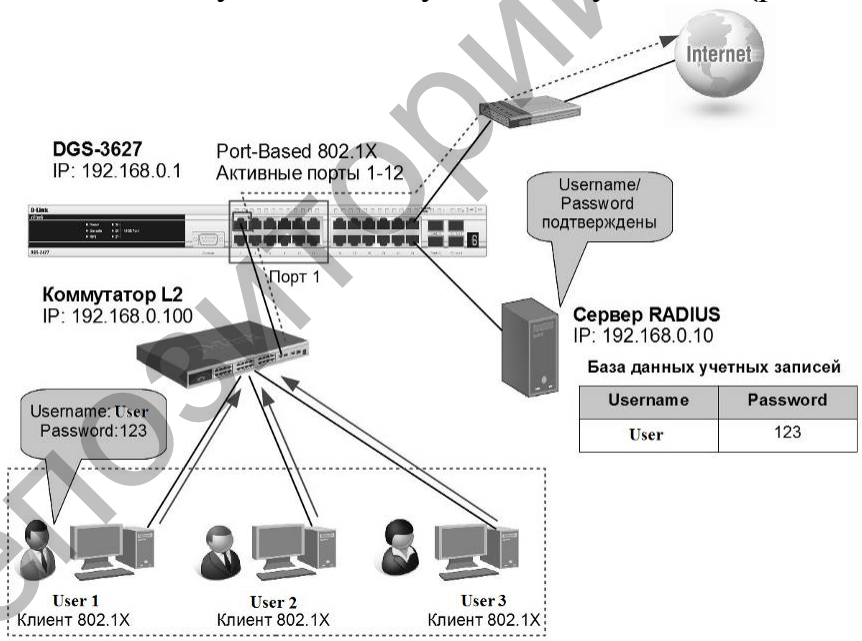


Рис. 2.11. Аутентификация 802.1X на основе портов

• MAC-Based 802.1X: при таком типе аутентификации проверяются не только имя пользователя/пароль подключенных к порту коммутатора клиентов, но и их количество. Количество подключаемых клиентов ограничено максимальным количеством MAC-адресов, которые 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.

В отличие от аутентификации 802.1X на основе портов, где один порт, авторизированный клиентом, остается открытым для всех клиентов, аутентификация 802.1X на основе MAC-адресов – это аутентификация множества клиентов на одном физическом порте коммутатора (рис. 2.12).

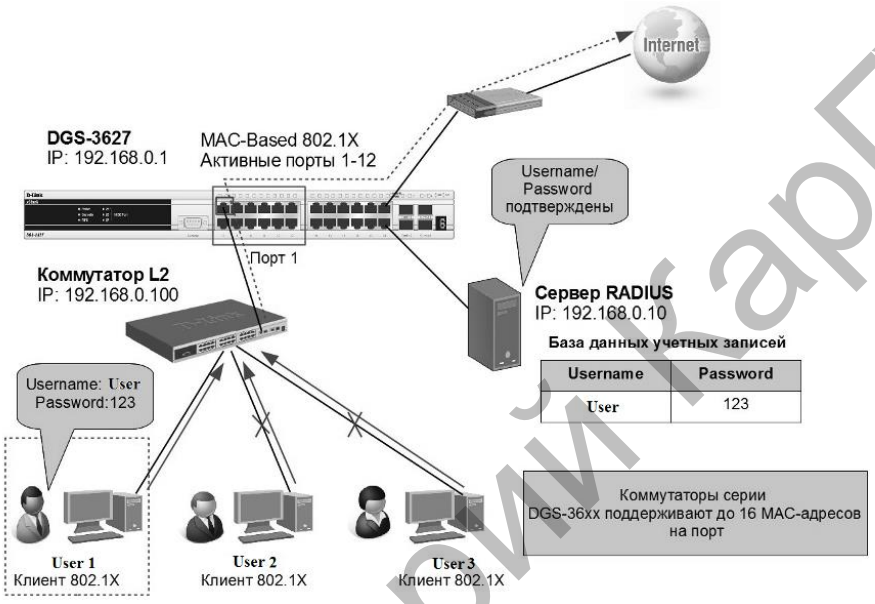


Рис. 2.12. Аутентификация 802.1X на основе MAC-адресов

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. 2.13 показана локальная аутентификация 802.1X на основе MAC-адресов.

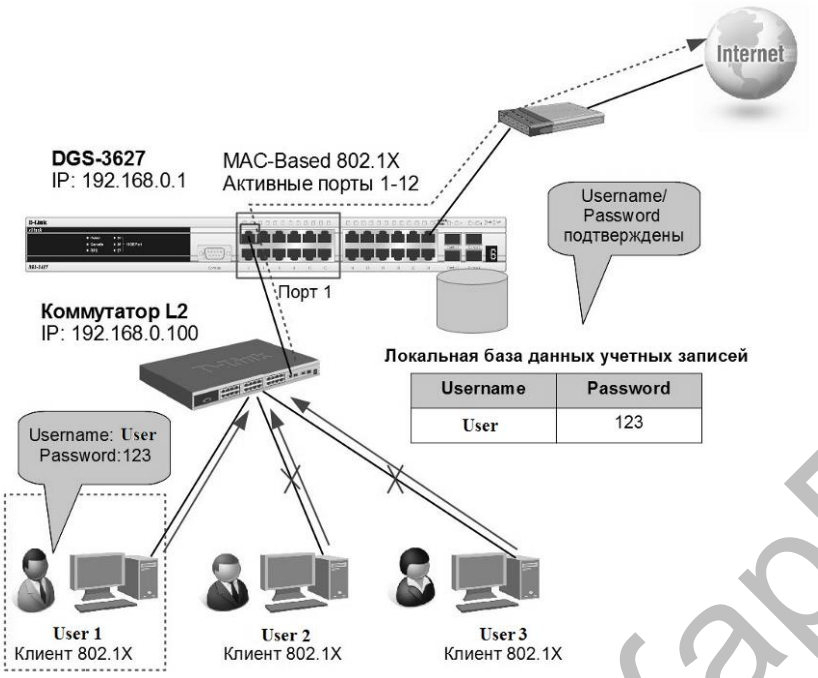


Рис. 2.13. Аутентификация 802.1X на основе MAC-адресов с использованием локальной базы данных учетных записей пользователей

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:

1) состояние порта по умолчанию без поддержки 802.1X (рис.2.14);

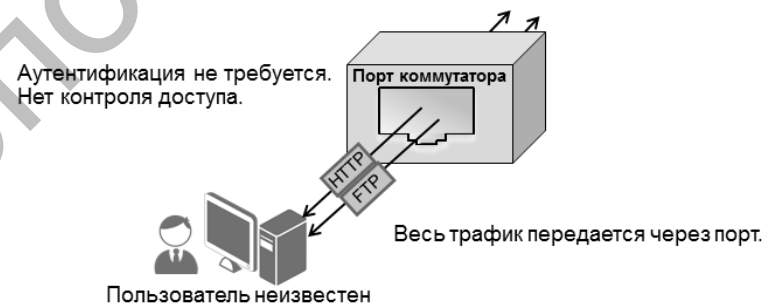


Рис. 2.14. Состояние порта по умолчанию без 802.1X

2) состояние порта по умолчанию с поддержкой 802.1X (рис. 2.15);

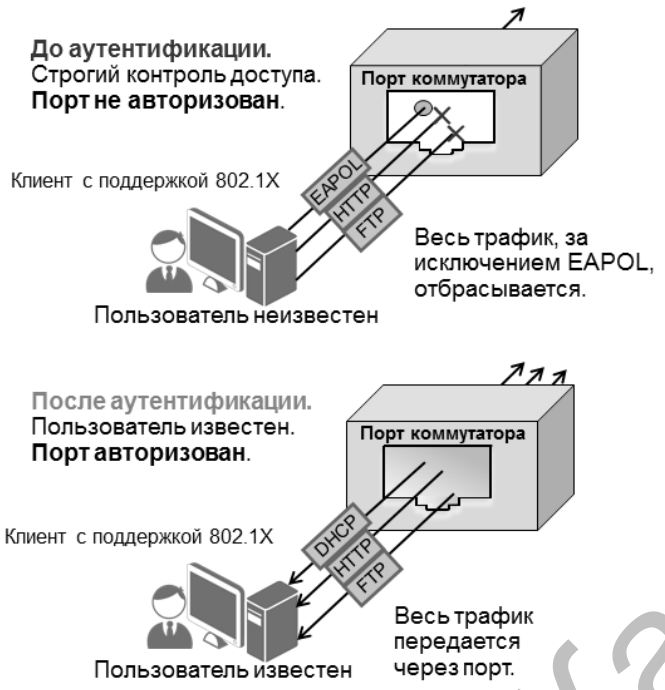


Рис. 2.15. Состояние порта по умолчанию с 802.1X

3) состояние порта с поддержкой 802.1X при подключении клиента без поддержки 802.1X (рис. 2.16). Коммутатор посылает EAPOL-запрос. Устройство не может отправить EAPOL-ответ;

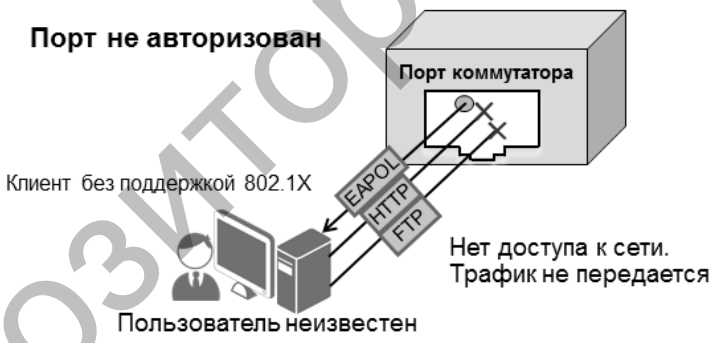


Рис. 2.16. Состояние порта с поддержкой 802.1X при подключении клиента без поддержки 802.1X

4) состояние порта без поддержки 802.1X при подключении клиента с поддержкой 802.1X (рис. 2.17).

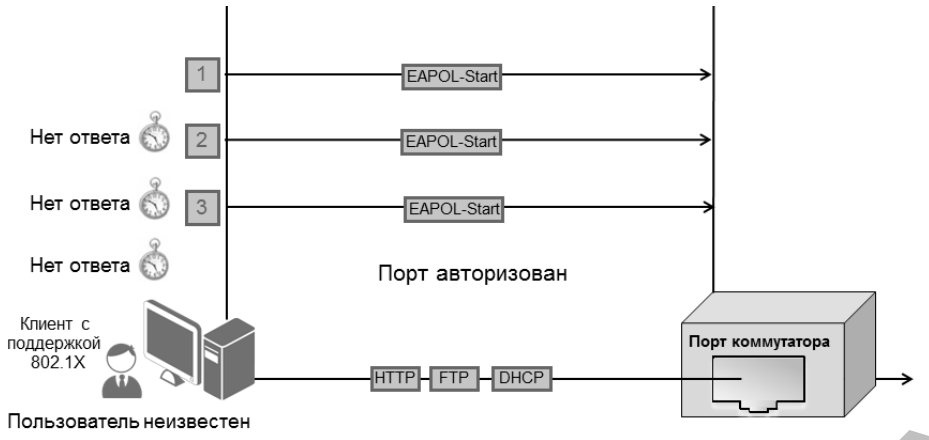


Рис. 2.17. Состояние порта без поддержки 802.1X при подключении клиента с поддержкой 802.1X

2.5. Безопасность архитектуры беспроводных сетей стандартов типа 802.11

Безопасность беспроводных сетей всегда играла важную роль, по сравнению с Ethernet-сетями, так как здесь вместо проводной линии связи используется радиоканал.

Основные проблемы безопасности сетей архитектуры типа 802.11 подразделяются на:

1) *Authentication* или «Механизмы аутентификации»;

2) *Privacy* или «Конфиденциальность»;

3) *Integrity* или «Целостность».

Открытая аутентификация используется для быстрого подключения беспроводных сетей, в процессе аутентификации происходит обмен сообщениями, характеристики и условия которых представлены на рис. 2.18:

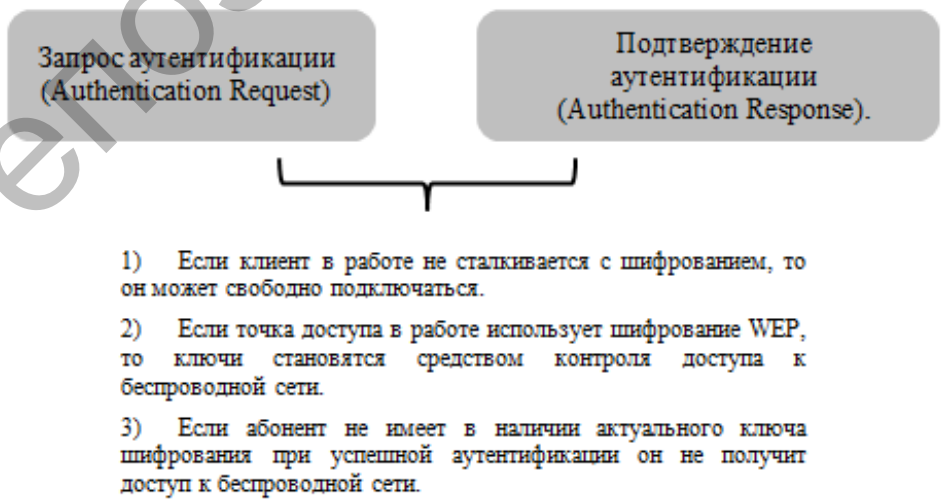


Рис. 2.18. Состояние порта без поддержки 802.1X при подключении клиента с поддержкой 802.1X

Процедура аутентификации указана на рис. 2.19.

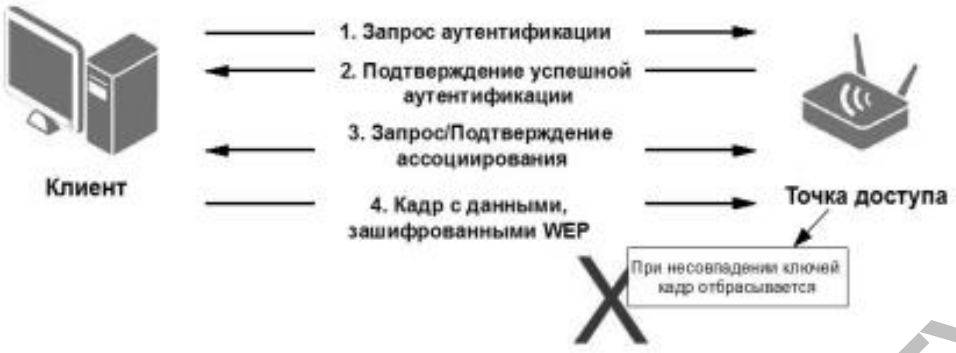


Рис. 2.19. Состояние порта без поддержки 802.1X при подключении клиента с поддержкой 802.1X

Процедуру аутентификации с использованием общего ключа можно отнести ко второму методу аутентификации стандартов архитектуры типа 802.11. Во время использования такого метода абоненту, который подключается к беспроводной точке доступа, нужен статический ключ шифрования WEP.

Процедура аутентификации статическим ключом шифрования WEP приведена на рис. 2.20.

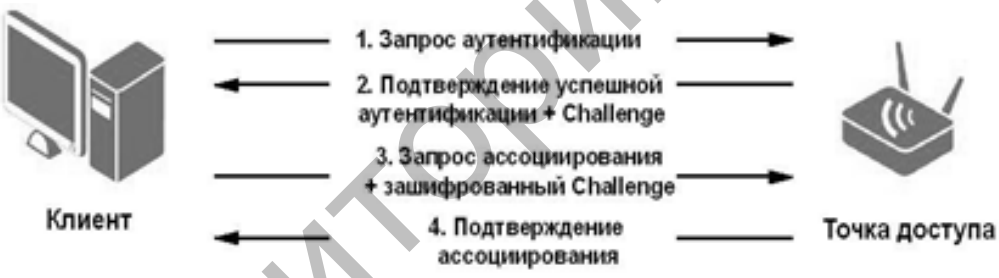


Рис. 2.20. Процедура аутентификации статическим ключом шифрования WEP

Важно отметить, что существует два механизма ограничения доступа, которые выходят за рамки использования архитектур стандартов 802.11. К ним относятся:

- MAC Filtering фильтрация MAC адресов;
- Service Set Identifier (SID) скрытие идентификатора.

Функция MAC Filtering основана на составлении ARP таблицы MAC адресов, т.е. в опциональных возможностях можно ввести статические MAC адреса, которым разрежается подключение к беспроводной сети, при этом иные MAC адреса, не входящие в список ARP таблицы, не смогут подключиться (рис. 2.21). Возможно совместное использование функции MAC фильтрации и протоколов безопасности беспроводной сети WEP и WPA [7].

Однако в функции MAC фильтрации существует уязвимость, которая заключается в том, что кадр MAC адреса передается от клиента к точке доступа в открытом виде. Вследствие чего злоумышленник может перехватить разрешен-

ный MAC адрес и подменить его.

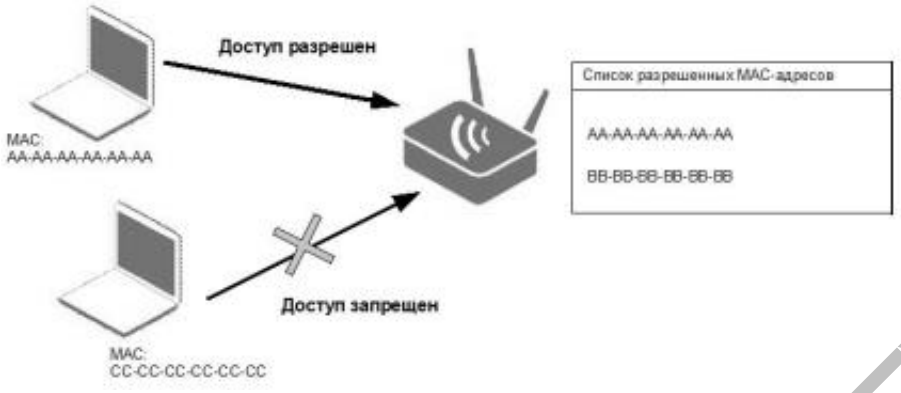


Рис. 2.21. Фильтрация по MAC-адресам

Большая часть точек доступа поддерживает функцию скрытия идентификатора. Для того, чтобы клиенты могли обнаружить точку доступа, она периодически рассылает сигнальные кадры (signal frames). Данные кадры несут в себе информацию о подключении к беспроводной сети SSID, в случае скрытия SSID беспроводную сеть практически невозможно определить. Но в функции SSID также есть недостаток. Он содержится в других типах кадров и может быть перехвачен.

Для WEP шифрования разработан код на алгоритме RC4 (Rivest's CIPher v.4, код Ривеста), при котором генерируется последовательность битов, которая суммируется с текстом. При обратном процессе данная последовательность регенерируется.

При данном виде симметричного шифрования используется один и тот же ключ для шифрования и дешифрования (рис. 2.22).

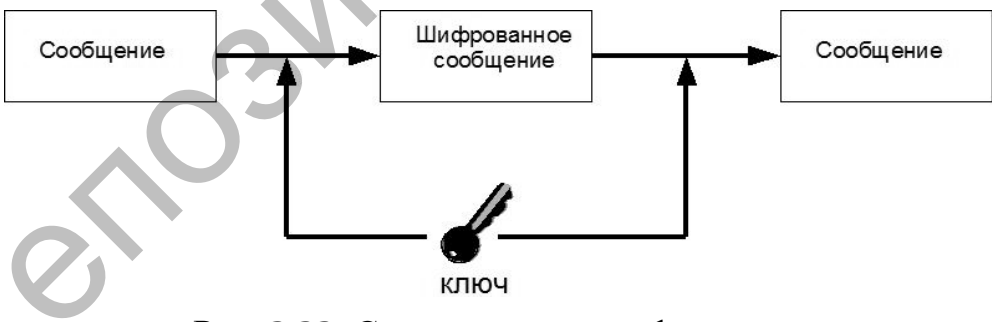


Рис. 2.22. Симметричное шифрование

Наличие в кадре 802.11 флага WEP означает, что информация зашифрована. При этом используется контрольная сумма, которая гарантирует целостность данных (рис. 2.23).

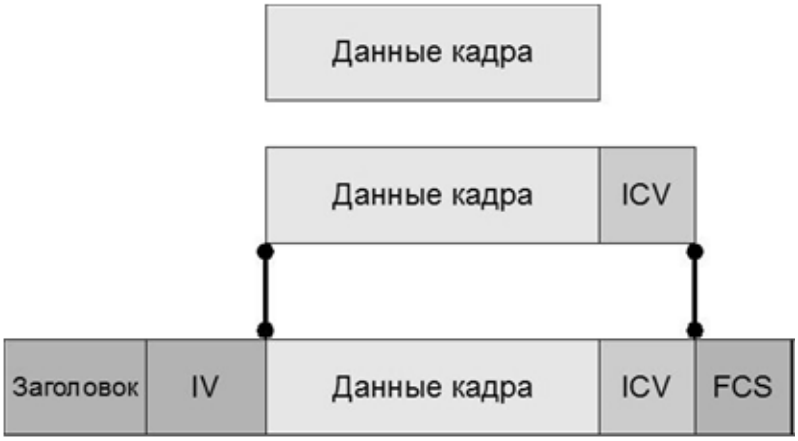


Рис. 2.23. Зашифрованный WEP кадр

Для изменения ключевой последовательности применяется процедура *Initialization Vector*. При использовании данной процедуры возникает алгоритм шифрования, при котором подается секретный ключ. Если в *Initialization Vector* происходят изменения, ключевая последовательность также меняется.

Каждый канал использует обновленный *Initialization Vector*. При этом не-шифрованный кадр при передаче будет изменять свой шифр [8].

Принцип работы *Initialization Vector* приведен на рис. 2.24.

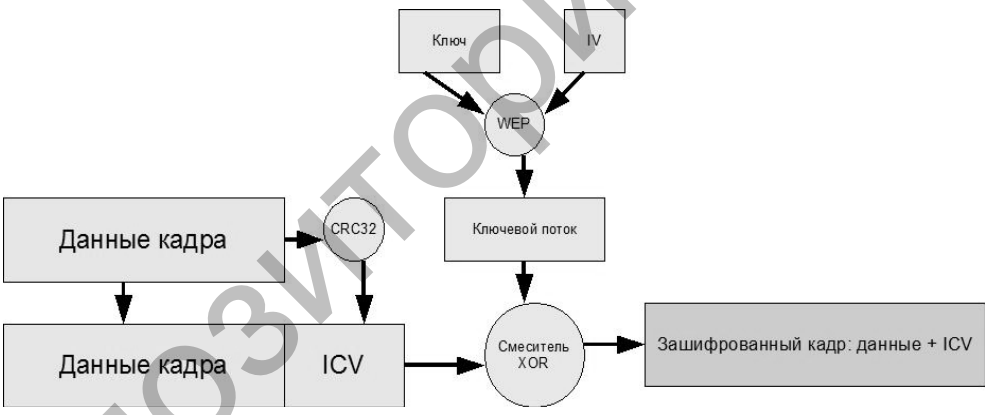


Рис. 2.24. Шифрование с использованием вектора инициализации

Основные этапы шифрования кадра приведены на рис.2.25.

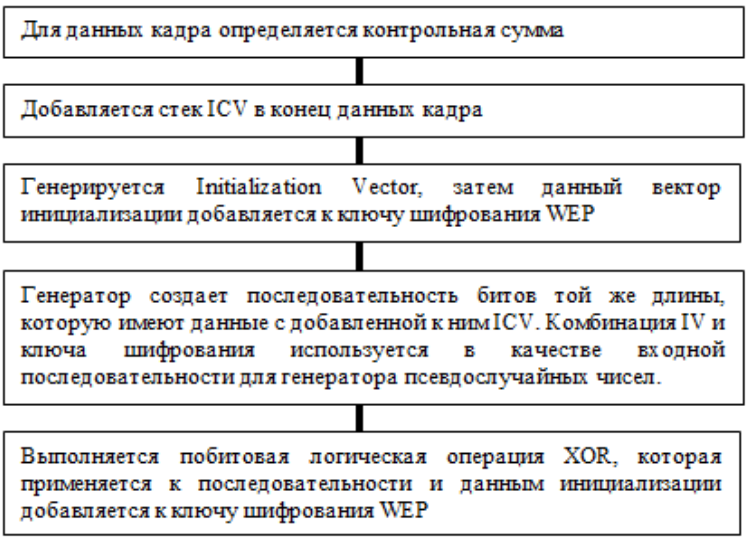


Рис. 2.25. Алгоритм шифрования кадра

Алгоритм обратного процесса дешифрования кадра приведен на рис. 2.26:

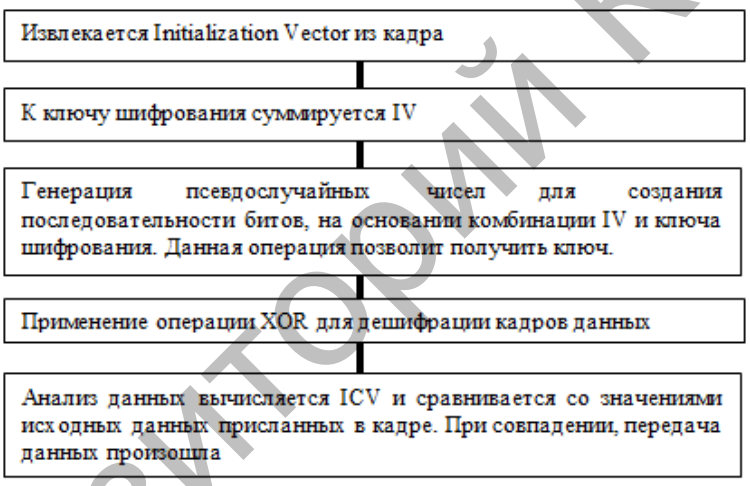


Рис. 2.26. Алгоритм дешифрования кадров

Описанные выше технологии защиты беспроводных сетей применяются для развертывания современных WLAN сетей.

ГЛАВА 3. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

3.1. Экспериментальное оборудование и правила работы с ним

Правила техники безопасности.

В учебной лаборатории используется напряжение в пределах до 250 В. Данная величина может представлять особо серьезную опасность в случае ненадлежащего соблюдения правил по технике безопасности.

Основные правила по технике безопасности следующие:

1) рабочее место обучающегося не должно загромождаться посторонними предметами, мешающими проведению лабораторных работ;

2) перед началом сборки сетевой схемы необходимо убедиться в том, что автомат на фильтре сетевого шкафа находится в выключенном состоянии;

3) не допускается использование оборудования с неисправленными зажимами, проводов с поврежденной изоляцией и другого оборудования. О не исправности сообщить инженеру или преподавателю;

4) исследуемое оборудование необходимо размещать таким образом, чтобы в процессе выполнения работы была исключена возможность случайного прикосновения к оголенным токоведущим частям;

5) сборку сети необходимо выполнять по возможности без пересечения проводов, нельзя натягивать и сворачивать провода. Не использованные соединительные провода необходимо убрать с рабочего места;

6) категорически запрещается проводить какие-либо операции на основных распределительных щитах, а также за пределами рабочего места;

7) в случае прекращения лабораторной работы или перерыва в работе источник питания сети необходимо отключить;

8) во время лабораторной работы запрещается производить переподключение в сети, находящейся под напряжением;

9) во время лабораторной работы запрещается прикасаться к оголенным токоведущим частям оборудования;

10) во время лабораторной работы запрещается включать сетевую структуру после каких-либо изменений соединений в ней до проверки преподавателем;

11) во время лабораторной работы запрещается оставлять без наблюдения включенную сеть;

12) во всех случаях обнаружения неисправного оборудования, проводов, при появлении специфического запаха, дыма нужно выключить напряжение и немедленно поставить в известность преподавателя;

13)после окончания работы необходимо выключить напряжение, разобрать сетевую структуру, а также привести в порядок рабочее место [9].

Студенты допускаются к лабораторным работам после ознакомления с настоящими правилами, что должно быть зафиксировано в специальном журнале по технике безопасности.

Описание лабораторного оборудования.

Комплект лабораторного оборудования «D-Link» предназначен для проведения лабораторного практикума по разделам курсов «Защита информации в телекоммуникационных системах», «IP-телефония», «Технология беспроводной связи» и др. в высших и средних образовательных учреждениях.

Основными компонентами комплекта «D-Link» являются:

– десять сетевых коммутаторов DES-3200-10 с 8 коммутационными LAN портами, один из которых представлен на рис. 3.1:

Рис. 3.1. Сетевой коммутатор DES-3200-10 с 8 коммутационными LAN портами

– два управляемых сетевых коммутатора DES-3810-28 с 24 коммутационными LAN портами, один из которых представлен на рис. 3.2:

Рис. 3.2. Управляемый сетевой коммутатор DES-3810-28 с 24 коммутационными LAN портами

– пять управляемых стекируемых коммутаторов DES-3528 с 24 коммутационными LAN портами, один из которых представлен на рис. 3.3:

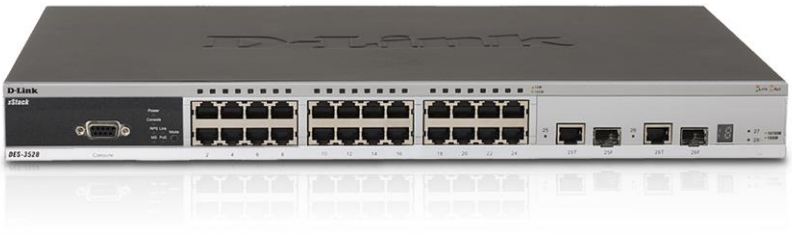


Рис. 3.3. Управляемый стекируемый коммутатор DES-3528 с 24 коммутационными LAN портами

– пять одиннадцати-портовых межсетевых экранов NetDe-fend DAL-860e, один из которых представлен на рис. 3.4:

Рис. 3.4. Одиннадцати-портовый межсетевой экран NetDefend DAL-860e

– пять гигабитных сервисных маршрутизатора DSR-250, один из которых представлен на рис. 3.5:

Рис. 3.5. Гигабитный сервисный маршрутизатор DSR-250

– беспроводная точка доступа DAP-2310, представленная на рис.3.6:

Рис. 3.6. Беспроводная точка доступа DAP-2310

– десять беспроводных USB-адаптеров DWA-160, один из которых представлен на рис. 3.7:

Рис. 3.7. Беспроводной USB-адаптер DWA-160

– программное обеспечение на рабочие станции для возможности программирования сети;

– соединительные сетевые медные и оптические кабели, стекируемые кабели, питающие кабели.

Общая компоновка типового комплекта оборудования в стендовом исполнении показана на рис. 3.8. В сетевом шкафу на стойках закреплены элементы лабораторного оборудования D-Link, в числе которых коммутаторы, марщрутизаторы и межсетевые экраны. Расположение оборудования в стойках жёстко не фиксировано. Оно может изменяться для удобства проведения того или иного конкретного эксперимента. В зависимости от выполняемой лабораторной работы, оборудование соединяется между собой сетевыми и стекируемыми кабелями. В основании шкафа находится сетевой фильтр, к которому подключается все лабораторное оборудование [10].

На все рабочие станции лаборатории устанавливается программное обеспечение. При необходимости рабочие станции подсоединяются сетевыми кабелями к лабораторному оборудованию D-Link. Во время выполнения некоторых лабораторных работ к каждой рабочей станции подключают беспроводной USB-адаптер, который принимает сигнал от маршрутизатора и обеспечивает

беспроводную связь между всеми рабочими станциями, а также доступ в сеть Интернет.

Рис. 3.8. Типовой комплект лабораторного оборудования

3.2. Лабораторная работа 1 «Агрегирование каналов»

Цель работы: изучить настройку динамического агрегирования каналов на D-Link коммутаторах.

Оборудование (на 2 рабочих места): коммутатор DES-3200-10 или DGS-3200-10 2 шт, рабочая станция 3 шт, Ethernet кабель 7 шт, кабель консольный 2 шт.

Задание. Провести настройку коммутаторов методом агрегирования каналов. Для создания искусственной нагрузки на канал связи между коммутаторами при выполнении лабораторной работы будет использоваться программа *IPera*. Схема соединения указана на рис.3.9.

Порядок выполнения эксперимента.

Примечание: не соединяйте физически соответствующие порты коммутато-

ров до тех пор, пока не настроено агрегирование каналов, т.к. в коммутируемой сети может возникнуть петля.

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

reset config

2. Настройка коммутатора 1. Создайте группу агрегирования каналов:

create link_aggregation group_id 1 type LACP

3. 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 enabled

4. Настройте порты на работу в пассивном режиме:

config LACP_Port 2,4,6,8 Mode passive

5. Проверьте выполненные настройки:

show link_aggregation

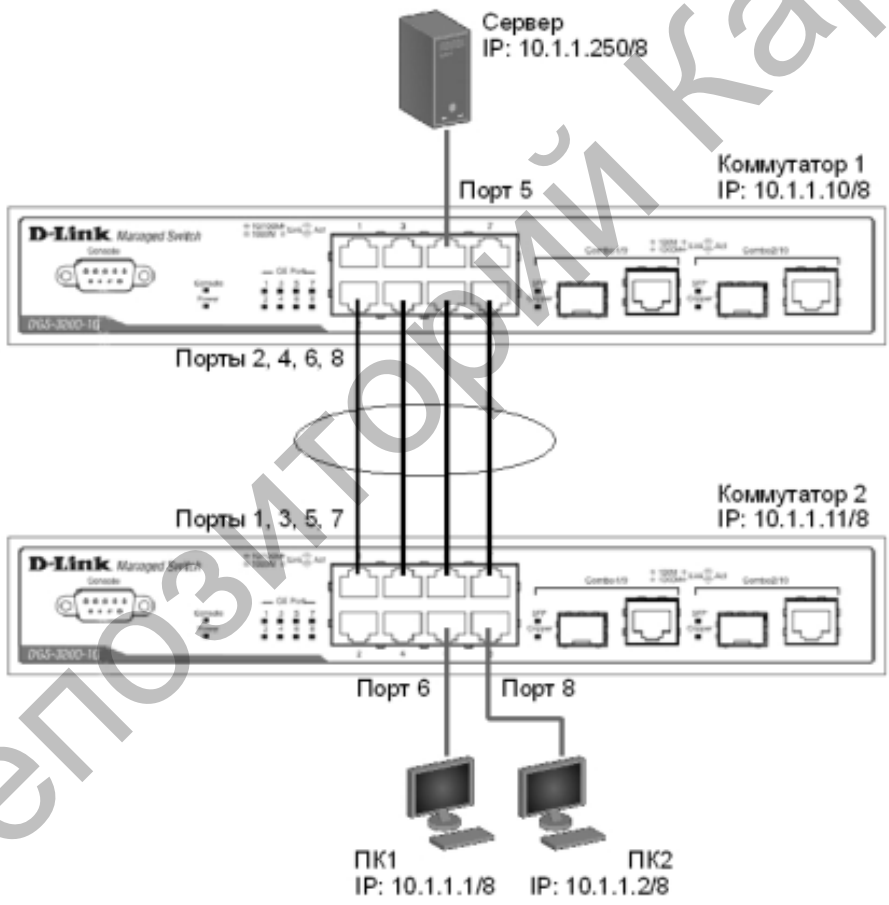


Рис. 3.9. Схема сетевого соединения оборудований рабочих станций, коммутаторов и выделенного сервера

6. Проверьте режим работы LACP на портах коммутаторов:

show LACP_Port

7. Посмотрите текущий алгоритм агрегирования каналов:

show link_aggregation algorithm

8. Настройка коммутатора 2. Создайте группу агрегирования каналов:

create link_aggregation group_id 1 type LACP

9. 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 enabled

10. Настройте порты на работу в активном режиме:

config LACP_Port 1,3,5,7 Mode active

11. Проверьте выполненные настройки:

show link_aggregation

12. Проверьте режим работы LACP на портах коммутаторов:

show LACP_Port

13. Запустите на ПК1 и ПК2 программу IPera:

IPera –c 10.1.1.250 –i 1 –t 1000 –r –u –b10M –P5

14. Запустите на сервере: *IPera –s –u*. Ключ «-c» устанавливает режим клиента и задает адрес сервера, «-i» задает интервал вывода отчета о скорости; «-t» – время длительности теста в секундах; «-r» – режим двустороннего тестирования; «-u» – режим тестирования UDP трафиком; «-b10M» задает полосу генерации трафика в 10 Мбит/с; «-P5» запускает одновременно 5 тестовых потоков.

15. Во время теста проверьте загрузку портов на обоих коммутаторах [11]:

show utilization Ports

Содержание отчета.

1. Цель работы.
2. Структурная схема.
3. Текст программы.
4. Выводы.

Контрольные вопросы.

1. Что такое агрегирование каналов связи?
2. На каком уровне модели OSI происходит агрегирование каналов связи?
3. Каково значение определения Link Aggregation Group?
4. Как распределяется роль портов при агрегировании канала связи?
5. Назовите типы агрегирования каналов связи.
6. Каковы принципы динамического агрегирования канала связи?
7. Каковы принципы статического агрегирования канала связи?

3.3. Лабораторная работа 2 «Списки управления доступом (Access Control List)»

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

Оборудование (на 1 рабочее место): коммутатор DES-3200-10 или DGS-3200-10 1 шт, рабочая станция 3 шт, кабель консольный 1 шт, Ethernet кабель 3 шт, интернет-шлюз 1 шт.

Задание. Произвести настройку ограничения доступа пользователей в сети Интернет по MAC-адресу и IP-адресу.

Порядок выполнения эксперимента.

1. Разрешите пользователям ПК1 и ПК2 доступ в Интернет, остальным пользователям – запретите. Пользователи идентифицируются по MAC-адресам их компьютеров. Необходимо придерживаться нескольких правил:

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.

2. Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам командой:

reset config

Замените указанные в командах MAC-адреса на реальные MAC-адреса рабочих станций и Интернет-шлюза.

3. По правилу 1 создайте профиль доступа 10:

create access_profile Ethernet source_mac AA-AA-AA-AA-AA-AA destination_mac AA-AA-AA-AA-AA-AA profile_id 10

4. 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

5. Создайте правило для профиля 10, разрешающее доступ ПК2, подключенного к порту 8, 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 8 permit

6. По правилу 2 создайте профиль доступа 20:

create access_profile Ethernet destination_mac AA-AA-AA-AA-AA-AA profile_id 20

7. 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 1-10 deny

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.

8. По правилу 3 разрешите все остальное:

Выполняется по умолчанию

9. Проверьте созданные профили ACL:

show access_profile

10. Подключите станции ПК1 и ПК2, как показано на рисунке 3.10. Протестируйте соединение до Интернет-шлюза командой *ping*.

11. Подведите итог. Завершите работу с системой. Удалите правило из профиля (например, для отключения ПК2 от Интернет):

config access_profile profile_id 10 delete access_id 12

Удалите профиль ACL (например, разрешающий доступ в Интернет станциям ПК1 и ПК2):

delete access_profile profile_id 10

12. Разрешите доступ в сеть Интернет пользователям с IP-адресами с 10.1.1.1/24 по 10.1.1.63/24. Остальным пользователям сети 10.1.1.0/24, с адресами не входящими в разрешенный диапазон, запретите доступ в сеть Интернет. Необходимо придерживаться нескольких правил:

Правило 1: если IP-адрес источника = IP-адресам из диапазона с 10.1.1.1 по 10.1.1.63 (подсеть 10.1.1.1/26), разрешить;

Правило 2: если MAC-адрес назначения = MAC-адресу Интернет-шлюза, запретить;

Правило 3: иначе, по умолчанию разрешить доступ всем узлам.

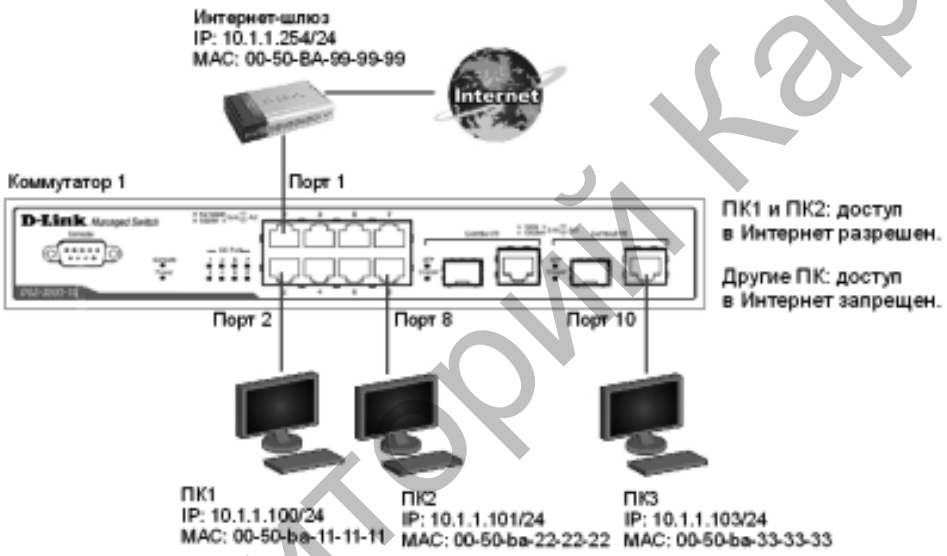


Рис. 3.10. Схема подключения рабочих станций к коммутатору

13. Перед выполнением задания удалите последний профиль из предыдущего задания:

delete access_profile profile_id 20

14. Убедитесь, что больше не осталось профилей:

show access_profile

15. По правилу 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

16. Создайте правило для профиля доступа 10:

config access_profile profile_id 10 add access_id 11 IP source_IP 10.1.1.0 Port 1-10 permit

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.

17. По правилу 2 создайте профиль доступа 40:

create access_profile Ethernet destination_mac AA-AA-AA-AA-AA-AA profile_id 40

Замените указанный в команде MAC-адрес на реальный MAC-адрес Интернет-шлюза [12].

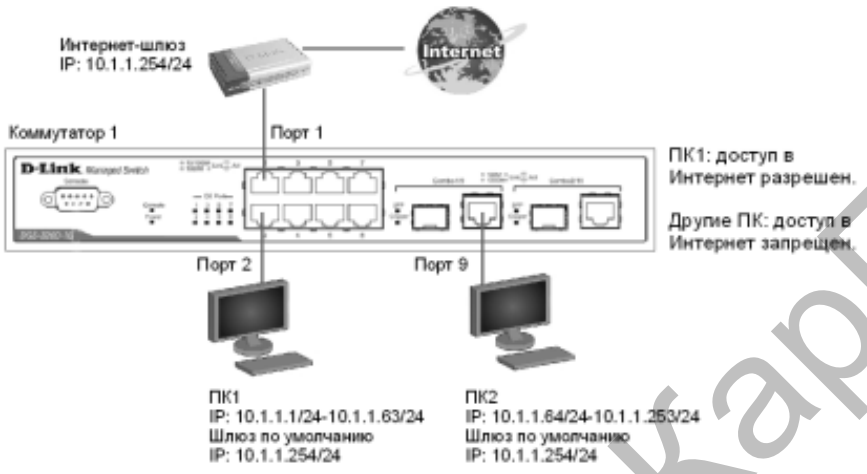


Рис. 3.11. Схема соединения рабочих станций к коммутатору

18. Создайте правило для профиля доступа 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 1-10 deny

19. По правилу 3 разрешите все остальное:

Выполняется по умолчанию

20. Проверьте созданные профили:

show access_profile

21. Подключите рабочие станции ПК1 (адрес из диапазона 10.1.1.1-63/24) и ПК2 (адрес из диапазона 10.1.1.64-253/24) к коммутатору как показано на рисунке 3.11.

22. Протестируйте командой *ping* соединение до Интернет-шлюза 10.1.1.254/24.

23. Подведите итог. Завершите работу с системой. Удалите профиль ACL (например, профиль 10).

delete access_profile profile_id 10

Проверьте соединение до Интернет-шлюза командой:

ping 10.1.1.254

Содержание отчета.

1. Цель работы.
2. Структурная схема.
3. Текст программы.
4. Выводы.

Контрольные вопросы.

1. Что такое списки управления доступом (Access Control List, ACL)?
2. Какие действия позволяет совершить список управления доступом?
3. Из чего состоят списки управления доступом?
4. Что такое профили доступа? Приведите пример.
5. Что такое правила доступа? Приведите пример.
6. Сколько типов профилей существует в коммутаторах D-Link? Назовите их.

3.4. Лабораторная работа 3 «Управление подключением рабочих узлов к портам коммутатора. Изучение функции Port Security»

Цель работы: научиться управлять подключением рабочих узлов к коммутационным портам и изучить настройку функции Port Security на D-Link коммутаторах.

Оборудование (на 1 рабочее место): коммутатор DES-3200-10 или DGS-3200-10 - 1 шт, рабочая станция - 2 шт, кабель консольный - 1 шт, Ethernet кабель - 2 шт.

Задание.

Произвести управление количеством подключаемых к портам коммутатора пользователей, путем ограничения максимального количества изучаемых MAC-адресов. Произвести настройку защиты от подключения к портам, основанной на статической таблице MAC-адресов.

Порядок выполнения работы.

1. Произведите управление количеством подключаемых к портам коммутатора пользователей, путем ограничения максимального количества изучаемых MAC-адресов. Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:

reset config

Проверьте информацию о настройках Port Security:

show Port_security

2. Установите максимальное количество изучаемых всеми портами MAC-адресов равным 1, и включите функцию на всех портах:

config Port_security Ports all admin_state enable max_learning_addr 1

3. Подключите ПК1 и ПК2 как показано на рисунке 3.12 к портам 2 и 8 коммутатора соответственно. Посмотрите MAC-адреса, которые стали известны портам 2 и 8:

show adb Port 2

show adb Port 8

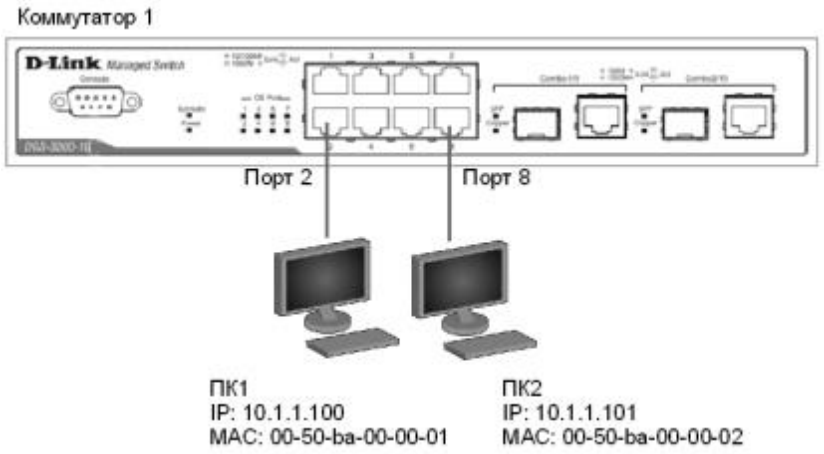


Рис.3.12. Схема подключения рабочих станций к коммутатору

4. Проверьте информацию о настройках Port Security на портах коммутатора:

show Port_security Ports 1-10

5. Настройте запись в log-файл MAC-адресов, подключающихся к порту станций и отправку сообщений SNMP Trap:

enable Port_security trap_Log

6. Выполните тестирование доступности узлов командой *ping* от ПК1 к ПК2 и наоборот.

7. Подключите ПК1 к порту 8, а ПК2 к порту 2. Повторите тестирование соединения между рабочими станциями командой *ping.*

8. Проверьте информацию в log-файле коммутатора:

show log

Сохраните конфигурацию и перезагрузите коммутатор:

save

reboot

Выполните тестирование соединения между рабочими станциями командой *ping.*

9. Настройте на порте 2 работу функции Port Security в режиме Permanent и максимальное количество изучаемых адресов равное 1:

config Port_security Ports 2 admin_state enable max_ learning_addr 1 lock_address_Mode Permanent

Сохраните конфигурацию и перезагрузите коммутатор:

save

reboot

Проверьте информацию о настройках Port Security на портах коммутатора:

show Port_security Ports 1-10

10. Очистите информацию о привязке MAC-порт на порте 2:

clear Port_security_entry Port 2

Отключите работу функции Port Security на порте 2 и приведите настройки в исходное (по умолчанию) состояние:

config Port_security Ports 2 admin_state disable max_ learning_addr 1

lock_address_Mode DeleteOnReset

Посмотрите время таймера блокирования (он соответствует времени жизни MAC-адреса в таблице коммутации):

show adb aging_Time

11. Изменить время действия таймера можно с помощью настройки времени жизни MAC-адреса в таблице коммутации (время указано в секундах):

config adb aging_Time 20

Измените режим работы функции Port Security на Delete on TimeOut:

config Port_security Ports 2 admin_state disable max_learning_addr 1 lock_address_Mode DeleteOnTimeOut

12. Проверьте MAC-адреса, которые стали известны порту 2:

show adb Port 2

Проверьте информацию о настройках Port Security на портах коммутатора:

show Port_security Ports 1-10

Выполните тестирование соединения между ПК1 и ПК2 командой *ping.*

13. Подведите итог. Завершите работу с системой. Отключите работу функции Port Security на портах:

config Port_security Ports 1-10 admin_state disable

Отключите функцию записи в log-файл и отправки SNMP Trap:

disable Port_security trap_Log

После выполнения предыдущих этапов имеется возможность отключить функцию динамического изучения MAC-адресов, тогда в таблице коммутации сохранятся изученные адреса. Таким образом, текущая конфигурация сети будет сохранена, и дальнейшее подключение новых устройств без ведома администратора будет невозможно. Новые устройства можно добавить путем создания статических записей в таблице коммутации [13].

14. Настройте защиту от подключения к портам, основанную на статической таблице MAC-адресов. Для этого сначала отключите рабочие станции от коммутатора. Сбросьте настройки коммутатора к заводским настройкам командой:

reset system

15. Активизируйте функцию Port Security на всех портах и запретите изучение MAC-адресов (параметр *max_learning_addr* установить равным 0):

config Port_security Ports 1-10 admin_state enable max_lear-ning_addr 0

Проверьте состояние портов:

show Ports

Проверьте соединение между ПК1 и ПК2 командой *ping.* Проверьте состояние таблицы коммутации:

show adb

16. В таблице коммутации вручную создайте статические записи для MAC-адресов рабочих станций, подключенных к портам 2 и 8. Замените указанные в командах MAC-адреса на реальные адреса рабочих станций, подключаемых к коммутатору.

create adb default 00-50-ba-00-00-01 Port 2

create adb default 00-50-ba-00-00-02 Port 8

17. Проверьте созданные статические записи в таблице коммутации:

show adb

Проверьте информацию о настройках Port Security на портах коммутатора:

show Port_security Ports 1-10

18. Проверьте соединение между ПК1 и ПК2 командой *ping*. Подключите ПК1 к порту 8, а ПК2 к порту 2.Повторите тестирование командой *ping*.

19. Подведите итог. Завершите работу с системой. Удалите ранее созданную статическую запись из таблицы MAC-адресов на порте 2:

delete adb default 00-50-ba-00-00-02 Port 2

Содержание отчета.

1. Цель работы.
2. Структурная схема.
3. Текст программы.
4. Выводы.

Контрольные вопросы.

1. Каковы основные свойства функции Port Security?
2. Что позволяет ограничивать функция Port Security?
3. Сколько существует режимов работы функции Port Security? Назовите их.
4. Каковы основные характеристики режима Permanent?
5. Каковы основные характеристики режима Delete on TimeOut?
6. Каковы основные характеристики режима Delete on Reset?
7. Для построения каких сетей лучше всего использовать функцию Port Security?
8. Что позволяет полностью запретить функция Port Security?

3.5. Лабораторная работа 4 «Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding»

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

Оборудование (на 1 рабочее место): коммутатор DES-3200-10 или DGS-3200-10 1 шт, рабочая станция 2 шт, кабель консольный 1 шт, Ethernet кабель 2 шт.

Задание. Произвести настройку работы функции IP-MAC-Port Binding в режимах ARP и ACL.

Порядок выполнения эксперимента.

1. Произведите настройку работы функции IP-MAC-Port Binding в режиме ARP. Для начала сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:

reset config

Замените указанные в командах MAC-адреса на реальные MAC-адреса рабочих станций, подключаемых к коммутатору.

2. Создайте запись IP-MAC-Port Binding, связывающую IP-MAC-адрес рабо-

чей станции ПК1 с портом 2 (по умолчанию режим работы функции ARP):

create address_binding IP_mac IPaddress 10.1.1.100 mac_ address 00-50-ba-00-00-01 Ports 2

3. Создайте запись IP-MAC-Port Binding, связывающую IP-MAC-адрес рабочей станции ПК2 с портом 8:

Create address_binding IP_mac IPaddress 10.1.1.101 mac_address 00-50-ba-00-00-02 Ports 8

4. Активизируйте функцию на портах 2 и 8 (по умолчанию режим работы портов Strict):

config address_binding IP_mac Ports 2,8 state enable

5. Проверьте созданные записи IP-MAC-Port Binding:

show address_binding IP_mac all

Проверьте порты, на которых настроена функция и их режим работы:

show address_binding Ports

6. Подключите рабочие станции ПК1 и ПК2 к коммутатору как показано на рисунке 3.13. Проверьте доступность соединения между рабочими станциями командой ping:

ping <IP-address>

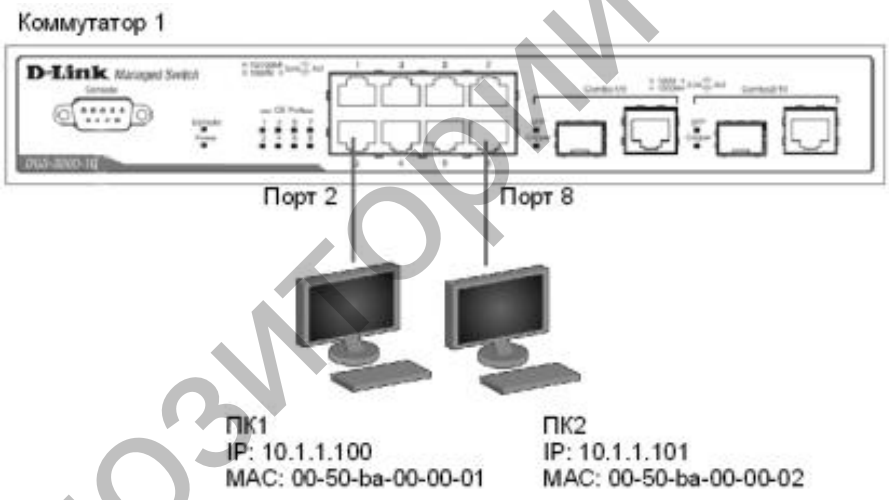


Рис. 3.13. Схема соединения рабочих станций с коммутатором

7. Настройте запись в log-файл и отправку сообщений SNMP Trap в случае несоответствия ARP-пакета связке IP-MAC:

enable address_binding trap_log

8. Подключите ПК1 к порту 8, а ПК2 к порту 2. Повторите тестирование соединения между рабочими станциями командой *ping*. Проверьте заблокированные рабочие станции:

show address_binding blocked all

Проверьте наличие заблокированных станций в log-файле:

show log

9. Подведите итог. Завершите работу с системой. 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 IPaddress 10.1.1.100 mac_address 00-50-ba-00-00-01

Отключите функцию IP-MAC-Port Binding на портах 2 и 8:

config address_binding IP_mac Ports 2,8 state disable

10. Произведите настройку работы функции IP-MAC-Port Binding в режиме ACL. Для начала создайте запись IP-MAC-Port Binding, связывающую IP-MAC-адрес станции ПК1 с портом 2:

create address_binding IP_mac IPaddress 10.1.1.100 mac_address 00-50-ba-00-00-01 Ports 2

11. Создайте запись IP-MAC-Port Binding, связывающую IP-MAC-адрес станции ПК2 с портом 8:

create address_binding IP_mac IPaddress 10.1.1.101 mac_address 00-50-ba-00-00-02 Ports 8

12. Активизируйте функцию на портах 2 и 8 (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 IMPB в режиме ACL:

config address_binding IP_mac Ports 2,8 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

13. Подключите рабочие станции ПК1 и ПК2 к коммутатору как показано на исходной схеме 12. Проверьте доступность соединения между рабочими станциями командой *ping:*

ping <IP-address>

14. Подключите ПК1 к порту 8, а ПК2 к порту 2. Повторите тестирование соединения между рабочими станциями командой *ping*. Проверьте заблокированные рабочие станции:

show address_binding blocked all

15. Подведите итог. Завершите работу с системой. 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 2 и 8:

config address_binding IP_mac Ports 2,8 state disable

Содержание отчета.

1. Цель работы.
2. Структурная схема.
3. Текст программы.
4. Выводы.

Контрольные вопросы.

1. Каковы основные свойства функции IP-MAC-Port Binding?
2. Сколько существует режимов работы функции IP-MAC-Port Binding? Назовите их.
3. Каковы основные характеристики режима ARP Mode?
4. Каковы основные характеристики режима ACL Mode?
5. Каковы основные характеристики режима DHCP Snooping?
6. Что должен указать администратор при активизации функции IP-MAC-Port Binding на порте?
7. Каковы основные характеристики режима Strict Mode?
8. Каковы основные характеристики режима Loose Mode?

3.6. Лабораторная работа 5 «Настройка QoS. Приоритизация трафика. Управление полосой пропускания»

Цель работы: изучить настройку приоритизации трафика, управление полосой пропускания на коммутаторах D-Link. Исследовать эффективность работы приоритизации.

Оборудование (на 2 рабочих места): коммутатор DES-3200-10 или DGS-3200-10 2 шт, рабочая станция 4 шт, кабель консольный 2 шт, Ethernet кабель 5 шт.

Задание. Назначить на всех ПК IP-адреса из одной подсети. Произвести тестирование сети между компьютерами сети. Провести приоритизацию трафика.

Порядок выполнения эксперимента.

1. Произведите настройку коммутаторов. Для начала необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

reset config

Для создания «узкого» места, настройте на порте 10 обоих коммутаторов функцию bandwidth_control, ограничивающую прием и передачу данных скоростью 64 Кбит/с:

config bandwidth_control 10 rx_rate 64 tx_rate 64

2. Назначьте на всех ПК IP-адреса из одной подсети. Запустите продолжительный тест *ping* между ПК1 и ПК3, а так же между ПК2 и ПК4, как показано на рисунке 3.14.

3. Собрав в течение 20-30 секунд статистику, запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они существуют.

4. Запустите продолжительный тест *ping* между ПК1 и ПК3, а так же между ПК2 и ПК4. Для создания нагрузки на линию связи между коммутаторами, запустите программу *IPera*:

- на ПК2 с ключом «-s» (в роли сервера):

IPera –s -u

- на ПК4 с ключами «-c IP-сервера -i 1 -t 1000 -r -u -b10M -P5» (в роли клиента):

IPera -c 10.1.1.2 -i 1 -t 1000 -r -u -b10M -P5

Ключ «-c» устанавливает режим клиента и задает адрес сервера, «-i» задает интервал вывода отчета о скорости; «-t» – время длительности теста в секундах; «-r» – режим двустороннего тестирования; «-u» – режим тестирования UDP трафиком; «-b10M» задает полосу генерации трафика в 10 Мбит/с; «-P5» запускает одновременно 5 тестовых потоков.

Не останавливайте запущенные программы *ping* и *IPera*. Собранная с помощью них статистика понадобится для выполнения следующего задания.

5. Собрав в течение 20-30 секунд статистику, посмотрите на ПК1 и ПК3, ПК2 и ПК4 информацию и запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они есть. Запишите примерную среднюю скорость, выводимую программой *IPera* на ПК4. Сравните данные результаты с результатами пункта 3.

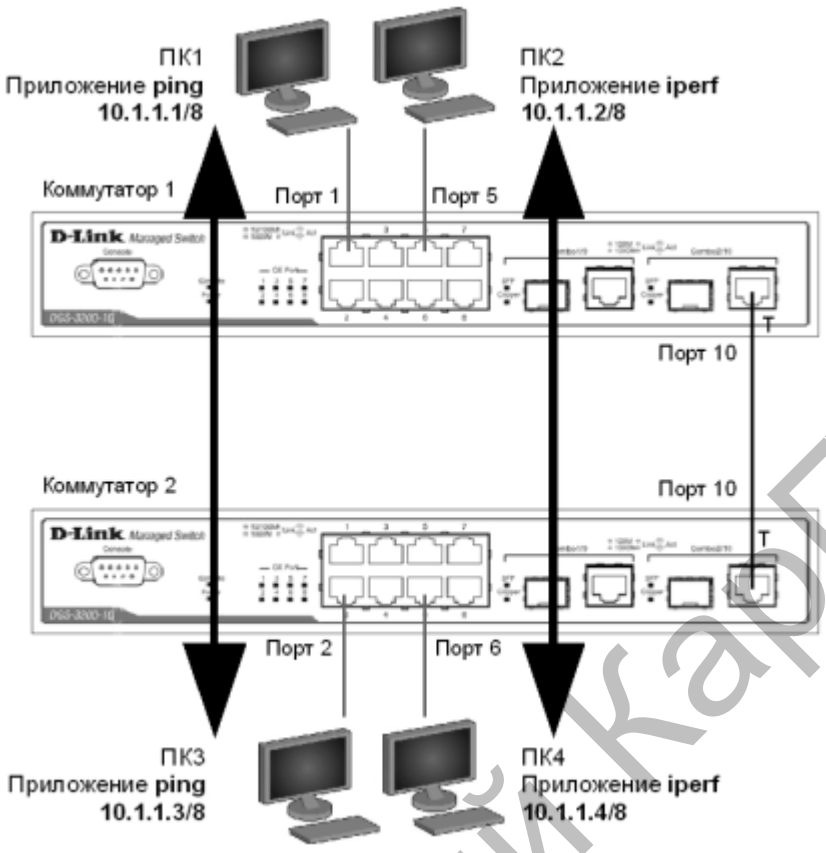


Рис. 3.14. Схема подключения рабочих станций к коммутаторам

6. Включите приоритизацию. Для этого поменяйте на порте 1, к которому подключена рабочая станция ПК1, значение приоритета по умолчанию на 7:

config 802.1p default_Priority 1 7

Пользовательский приоритет и метод обработки остаются по умолчанию.

7. Поменяйте на порте 2, к которому подключена рабочая станция ПК3, значение приоритета по умолчанию на 7:

config 802.1p default_Priority 2 7

Благодаря изменению значения приоритета портов, к которым подключены компьютеры с приоритетным трафиком на 7, все кадры, передаваемые ими, получат наивысший приоритет по сравнению с кадрами, поступающими от других компьютеров на остальные неприоритизированные порты обоих коммутаторов.

8. Посмотрите текущие настройки приоритета по умолчанию на всех портах коммутаторов 1 и 2:

show 802.1p default_Priority

Посмотрите карту привязки пользовательских приоритетов 802.1p к очередям класса обслуживания:

show 802.1p user_Priority

9. Сравните данные результаты с результатами пунктов 3 и 5. Сделайте выводы.

Содержание отчета.

1. Цель работы.

2. Структурная схема.
3. Текст программы.
4. Выводы.

Контрольные вопросы.

1. Что такое функция QoS?
2. В чем заключается функция QoS?
3. Какой стандарт поддерживают коммутаторы для обеспечания QoS?
4. Что такое «узкое» место сети?
5. Какие типы стандартов используются при передачи данных по сети?
6. Опишите стандарт IEEE 802.1p.
7. Какие критерии передачи данных гарантированно обеспечивает функция качества обслуживания?

3.7. Лабораторная работа 6 «Фильтрация ассоциаций с точкой доступа на основе MAC-адресов. Настройка шифрования WEP. Настройка WPA-PSK»

Цель работы: научиться настраивать MAC-фильтры. Научиться производить операции фильтрации с использованием точки доступа. Научиться настраивать беспроводную сеть инфраструктурной топологии с использованием статических WEP-ключей и технологии WPA-PSK.

Оборудование (на 1 рабочее место): точка доступа - 1 шт, рабочая станция - 3 шт, коммутатор – 1 шт, беспроводной адаптер - 2 шт.

Задание. Произвести настройку фильтрации ассоциаций с помощью точки доступа на основе MAC-адресов. Произвести настройку беспроводной сети инфраструктурной топологии с использованием статических WEP-ключей. Произвести настройку беспроводной сети инфраструктурной топологии с использованием технологии WPA-PSK.

Порядок выполнения эксперимента.

1. Для выполнения работы используйте следующие настройки IP-адресов проводного интерфейса компьютера 1 и беспроводных интерфейсов компьютеров 2 и 3:

Компьютер 1: 192.168.0.1/24;
Компьютер 2: 192.168.0.2/24;
Компьютер 3: 192.168.0.3/24.

Настройка точки доступа выполняется с компьютера 1 согласно рис. 3.15.

2. Сбросьте настройки точки доступа к заводским. Подключите беспроводные адаптеры к рабочим станциям 2 и 3. Проведите настройку точки доступа. С компьютера 1 получите доступ к Web-интерфейсу точки доступа, открыв браузер и введя IP-адрес точки доступа. IP-адрес DAP-2310, установленный по умолчанию, 192.168.0.50, маска – 255.255.255.0. При необходимости, смените

IP-адрес рабочей станции, чтобы он принадлежал сети 192.168.0.0/24. Имя администратора точки доступа, используемое по умолчанию – *admin*, пароля нет.

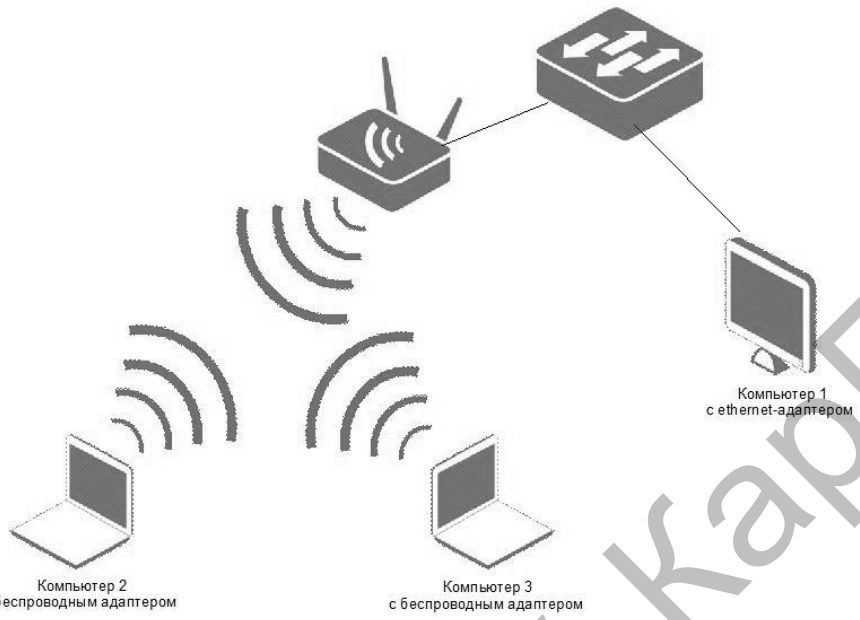


Рис. 3.15. Схема подключения рабочих станций к токам доступа и маршрутизатору

3. На рис. 3.16 показан Web-интерфейс точки доступа. В зоне 1 расположено меню настроек, в зоне 3 отображаются текущие настройки устройства и поля для их изменения (не для всех пунктов меню). В зоне 2 осуществляется доступ к настройкам Administration Settings, Airmware and SSL Certification Upload, Configuration File (пункт меню Maintenance), Save and Activate, Discard Changes (пункт меню Configuration), System Settings (пункт меню System). Для изменения IP-адреса точки доступа выберите в меню пункт Basic Settings-LAN (рис. 3.17).

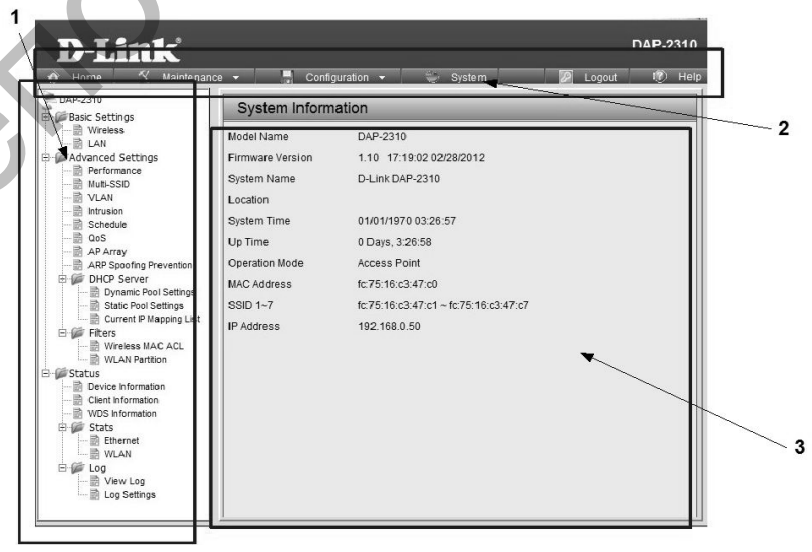


Рис. 3.16. Web-интерфейс точки доступа

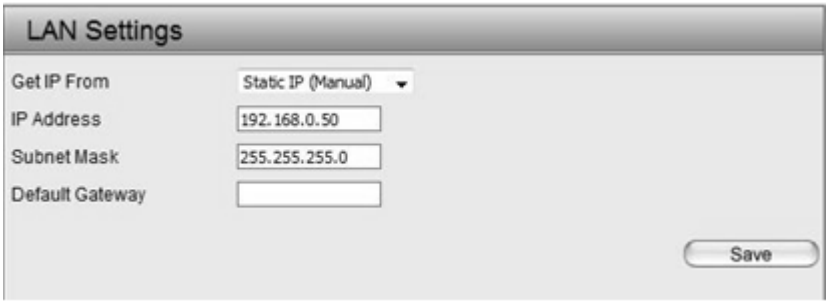


Рис. 3.17. Изменение IP-адреса точки доступа

При необходимости измените IP-адрес точки доступа. Помните, что IP-адреса в локальной сети должны быть уникальными. Основные беспроводные настройки находятся в меню Basic Settings-Wireless (рис. 3.18).

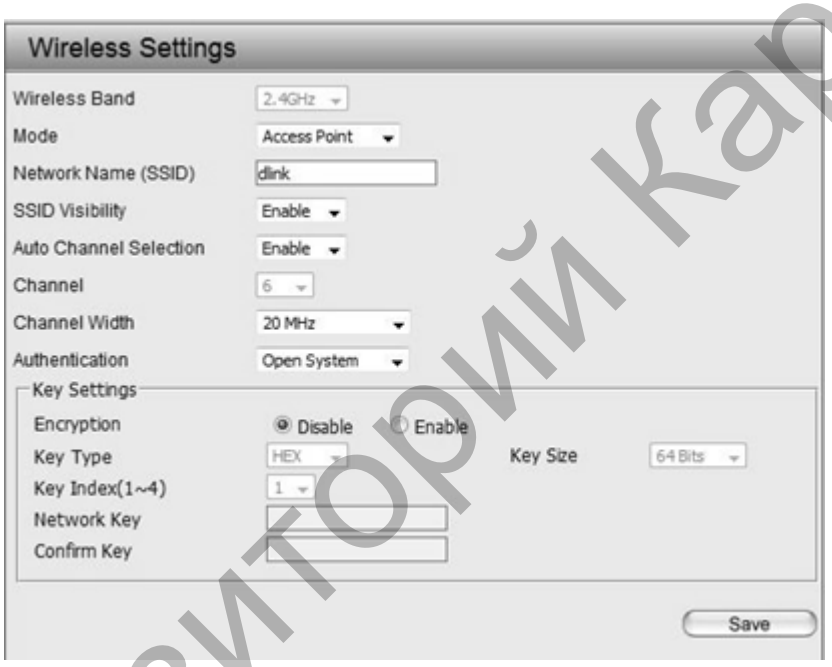


Рис. 3.18. Настройки беспроводной точки доступа

По умолчанию на точке доступа DAP-2310 настроен SSID *dlink*, частотный канал выбирается автоматически (наименее занятый). Измените SSID с *dlink* на *test*. Отключите автоматический выбор канала (Auto Channel Selection), смените *Enable* на *Disable* и выберите 10 канал (Channel). После чего нажмите на странице кнопку Save для сохранения сделанных настроек.

В меню Configuration выберите пункт *Save & Activate* для активации настроек. Дождитесь перезагрузки точки доступа.

4. После перезагрузки откройте Web-интерфейс точки доступа, вкладку Basic Settings-Wireless, укажите режим работы - Access Point , SSID и частотный канал, как было описано в пункте 3. В меню Filters-Wireless MAC ACL включите фильтрацию подключений к точке доступа по MAC-адресам: Access Control List – Accept. В этом случае фильтр будет действовать по типу «белого списка»: ассоциироваться с точкой доступа будет разрешено только устройствам, MAC-адреса которых будут содержаться в списке (рис. 3.19).

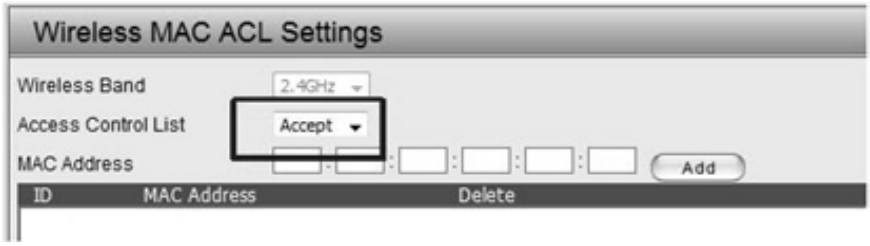


Рис. 3.19. Настройки беспроводной точки доступа

В поле MAC Address укажите MAC-адрес беспроводного сетевого адаптера рабочей станции 1. Протестируйте возможность ассоциирования с точкой доступа рабочей станции 1. Протестируйте возможность ассоциирования с точкой доступа рабочей станции 2.

5. На точке доступа измените фильтр на запрещающий: Access Control List – Reject (рис. 3.20). В этом случае фильтр будет действовать по типу «черного списка»: ассоциироваться с точкой доступа будет разрешено всем устройствам, кроме тех, чьи MAC-адреса будут содержаться в списке. Сохраните и активируйте настройки.

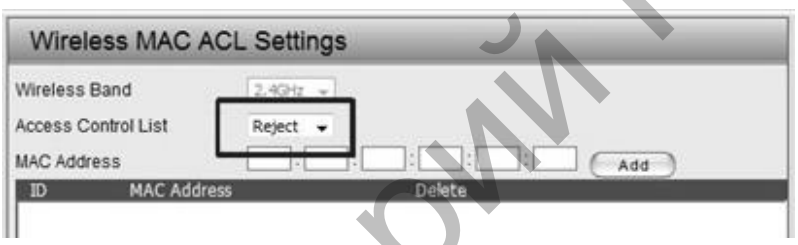


Рис. 3.20. Настройки беспроводной точки доступа

Протестируйте возможность ассоциирования с точкой доступа рабочей станции 1. Протестируйте возможность ассоциирования с точкой доступа рабочей станции 2. Отключите на точке доступа фильтрацию подключений к точке доступа по MAC-адресам. Протестируйте возможность ассоциирования с точкой доступа рабочих станций 1 и 2. Сделайте выводы.

6. Произведите настройку шифрования WEP. Для этого откройте Web-интерфейс точки доступа, вкладку Basic Settings-Wireless, укажите режим работы - Access Point , SSID и частотный канал, как было описано в пункте 3. Далее в поле Authentication ставим Shared Key (рис. 3.21). Так как аутентификация с общим ключом предполагает ещё и шифрование данных WEP, то в поле Encryption (Шифрование) активно только будет Enable (Включить). Выберите тип ключа (ASCII или Hex) и размер ключа. Вводите несколько ключей, последовательно выбирая в поле Key Index (Индекс ключа). При 64-битном ключе с типом ключа ASCII нужно ввести 5-значную последовательность, например *pass1*.

Рис. 3.21. Настройки беспроводной точки доступа

7. Сохраните и активируйте настройки. На рабочих станциях 2 и 3 при помощи D-Link Wireless Connection Manager настройте аналогичные параметры и ассоциируйте с точкой доступа (рис. 3.22). При помощи команды *ping* протестируйте возможность взаимодействия рабочих станций 2 и 3 между собой и с рабочей станцией 1.

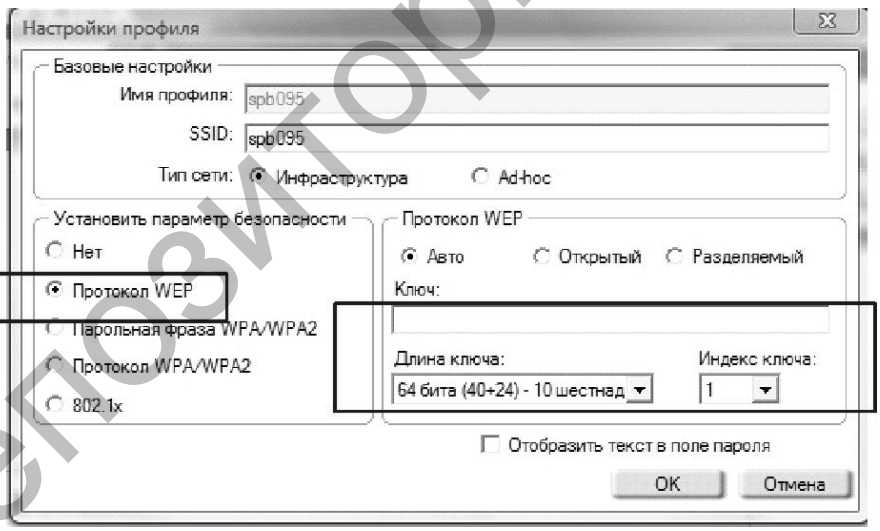


Рис. 3.22. Настройки беспроводной точки доступа

8. Проведите настройку WPA-PSK. Для этого откройте Web-интерфейс точки доступа, вкладку Basic Settings-Wireless, укажите режим работы - Access Point , SSID и частотный канал, как было описано в пункте 3. Далее в поле Authentication ставим WPA-Personal (рис. 3.23).

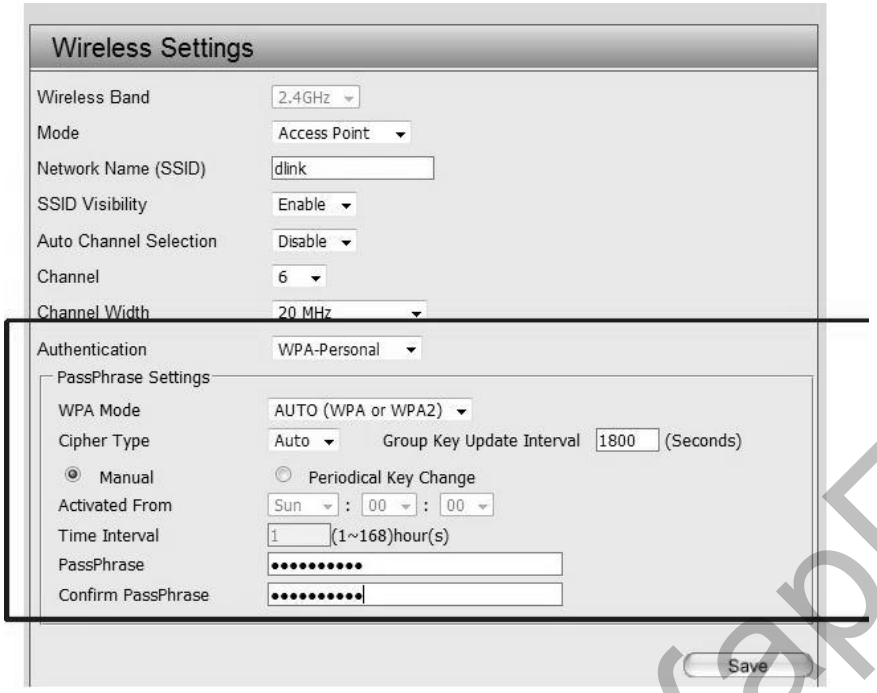


Рис. 3.23. Настройки беспроводной точки доступа

9. Выберите WPA Mode: Auto, WPA Only или WPA2 Only. При использовании параметра Auto можно использовать обе версии WPA. Укажите парольную фразу (PassPhrase). Сохраните и активируйте настройки. В настройках беспроводных подключений рабочих станций 2 и 3 укажите аналогичные параметры. Помните, что парольная фраза (ключ) должна быть той же самой, что и указанная на точке доступа (рис. 3.24).

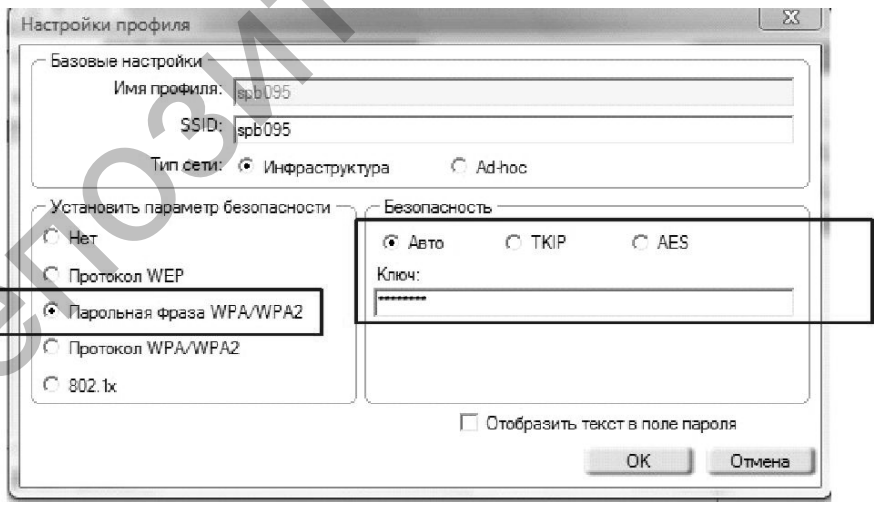


Рис. 3.24. Настройки беспроводной точки доступа

10. Ассоциируйте рабочие станции 2 и 3 с точкой доступа. При помощи команды *ping* протестируйте возможность взаимодействия рабочих станций 2 и 3 между собой и с рабочей станцией 1.

Содержание отчета.

1. Цель работы.

2. Структурная схема.

3. Пошаговые скриншоты выполняемых операций с описанием выполняемых действий и задаваемых команд.

4. Выводы.

Контрольные вопросы.

1. Что такое точка доступа?

2. Укажите основные характеристики и преимущества использования точки доступа?

3. Что такое MAC-адрес?

4. Что такое фильтрация ассоциаций?

5. Какие типы стандартов используются в работе точки доступа?

6. Какое количество пользователей может быть у точки доступа? От чего это зависит?

7. Как проводится настройка шифрования WEP?

8. Как проводится настройка WPA-PSK?

Заключение

При написании данного ученого пособия авторы ставили перед собой задачу: создать руководство, включающее в себя комплексную методику по организации защиты информации телекоммуникационных систем.

Пособие включает в себя материалы по информационной безопасности в коммутируемых сетях. Также в пособии рассмотрены вопросы по обеспечению безопасности и управлению доступом к сети.

Особое внимание уделено лабораторному практикуму, где описываются лабораторные работы на базе сетевого оборудования D-Link.

Изучение курса «Защита информации в телекоммуникационных системах» студентами всех форм обучения призвано способствовать приобретению ими необходимых знаний для применения их в своей профессиональной деятельности. Учебное пособие призвано:

– способствовать углублению и закреплению знаний, полученных студентами на лекциях и в ходе самоподготовки;

– развивать у студентов способность к творческому, самостоятельному анализу учебной и нормативной литературы;

– вырабатывать умение систематизировать и обобщать усвоенный материал, критически оценивать его;

– формировать и укреплять навыки практического применения своих знаний, аргументированного, логического и грамотного изложения своих мыслей;

– прививать студентам навыки комплексного системного подхода к изучению и применению на практике основ защиты информации в телекоммуникационных системах;

– служить материалом для самопроверки при изучении и закреплении отдельных тем и отраслей защиты информации в телекоммуникационных системах.

Список использованных источников

1. Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий // Матер. круг. стола «Внешнеполитические перспективы и новые концепты международной стратегии Казахстана». Инст. мир. эконом. и полит. при Фонде Первого Президента Республики Казахстан - Лидера Нации. – 2012. – С. 22-26. – 12 марта. // iwep.kz/index
2. Дмитриенко Т.А. Обеспечение информационной безопасности и развитие информационной инфраструктуры Республики Казахстан // Информационно-аналитический журнал «ANALYTIC». – 2009. – № 5. – С. 12-14.
3. Стрельцов А.А. Актуальные проблемы обеспечения информационной безопасности // Технологии безопасности. – 2010. – № 11. – С. 54.
4. Постановление Правительства Республики Казахстан от 30 сентября 2011г. № 1128 «О проекте Указа Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан до 2016 года» // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz
5. Информационная безопасность. Официальный сайт Комитета национальной безопасности Республики Казахстан. knb.kz
6. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2008. № ПР-1895 // Официальный сайт Совета безопасности Российской Федерации. scra.gov.ru
7. Указ № 174 Президента Республики Казахстан от 14 ноября 2011 г. «О Концепции информационной безопасности Республики Казахстан до 2016 года» // Электронная база нормативно-правовых актов «Законодательство».
8. Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2009. - С. 136.
9. Панасенко С., Грязнов Е., Безопасность локальных сетей – Электрон. журнал «Мир и безопасность» № 2, 2013. – С. 12-15 – Режим доступа к журналу: www.daily.sec.ru.
10. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2014. – С. 214.
11. Олифер Н. А., Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2010. – С. 143.
12. Карпов Е. А., Котухов М. М., Котенко И. В., Марков А. С., Рунеев А. Ю., Парр Г. А. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией Котенко И. В. – СПб: ВУС, 2010. – С. 42-48.
13. Спартак Марк, Паппас Френк. Компьютерные сети и сетевые технологии. – М.: ТИД «ДС», 2012. – С. 139.

Содержание

Амочаева Галина Павловна
Алпысова Гульнур Кенжебековна
Роговая Ксения Сергеевна

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Отпечатано с оригинала авторов

Подписано в печать __.__.2019 г. Формат 60х84 1/16. Бумага книжно-журнальная. Объем ___п.л. уч.изд. л. Тираж __ экз. Заказ № ____.

Издательство «Полиграфист»
100026, г. Караганда, ул. Язева, 2