Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

Рассмотрено
предметно-цикловой комиссией
Протокол заседания №1
от « 31 » августа 2020 г.
Председатель цикловой комиссии
_____Чобану Л.А..

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ЛАБОРАТОРНЫМ РАБОТАМ

ПМ 02. «Техническая эксплуатация информационно - коммуникационных сетей связи и вещания»
МДК.02.02 «Технология монтажа и обслуживания оборудования транспортных сетей систем радиосвязи и вещания»
Тема 2.1Коммутаторы и маршрутизаторы.
Тема 2.2Оборудование абонентского доступа.

по специальности
11.02.10 Радиосвязь, радиовещание и телевидение
(углубленной подготовки)

Составитель: преподаватель ОГАПОУ
«Белгородский индустриальный колледж»
Литвишков Н.А.

Белгород 2020 г.

Содержание

Тема 2.1 Коммутаторы и маршрутизаторы		
Лр№ 1	Настройка коммутатора. Подключение к коммутатору.	2 часа
Лр№ 2	Подключение к локальной консоли коммутатора.	2 часа
Лр№ 3	Подключение к Web-интерфейсу управления коммутатором.	2 часа
Лр№ 4	Настройка полосы пропускания с помощью команд CLI	2 часа
Лр№ 5	Настройка Access Control Lists (ACL) спомощьюCLI.	2 часа
Лр№ 6	Последовательность начальной загрузки и запуска маршрутизатора.	2 часа
Лр№ 7	Режимы конфигурирования маршрутизатора.	2 часа
Лр№ 8	Подключение к консоли и настройка маршрутизатора	2 часа
Лр№ 9	9 Введение в списки контроля доступа.	2 часа
Лр№ 10	Конфигурирование и проверка работы NAT	2 часа
Тема 2.2 Оборудование абонентского доступа		
Лр№ 1	Алгоритм линейного кодирования.	2 часа
Лр№ 2	Построение различных топологий беспроводных сетей.	2 часа
Лр№ 3	Распределение зон обслуживания беспроводных сетей.	2 часа
Лр№4	Подключение точек доступа беспроводных сетей.	2 часа
Лр№ 5	Кодирование по стандарту 802.11 и его аутентификация.	2 часа
Лр№ 6	Протокол шифрования WEP.	2 часа
Лр№ 7	Использование технологии WPAс сервером аутентификации.	2 часа
Лр№ 8	Аутентификация и авторизация абонента.	2 часа
Лр№ 9	Создание виртуального интерфейса в сторону абонента.	2 часа
Лр№ 10	Протоколы маршрутизации мультисервисных сетей.	2 часа
	Итого	**40 часов**

Тема 2.1Коммутаторы и маршрутизаторы.

Лабораторная работа № 1

Тема: «Настройка коммутатора. Подключение к коммутатору.»

Цель работы :изучить процедуру настройки коммутатора и подключения к коммутатору.

Порядок выполнения работы

Настройкакоммутатора

Понятие неуправляемых, управляемых и настраиваемых коммутаторов

Коммутаторы локальной сети можно классифицировать поуправлению.

Управляемые коммутаторы поддерживают широкий набор функций управления и настройки, включающие Web-интерфейс управления, интерфейс командной строки (CLI), Telnet, SNMP, TFTP и др. В качестве примера можно привести коммутаторы D-LinkDES-3226S, DES-3326SR, DES- 3526, DES-3324SR, идр.

Неуправляемые коммутаторы функции управления инастройкинеподдерживают. Примером могут служить коммутаторы D-LinkсерииDxS-10xx.

Настраиваемыекоммутаторызанимают промежуточнуюпозицию междуними. Этикоммутаторыпозволяютвыполнятьнастройку определенных параметров, но не поддерживают удаленноеуправлениепоSNMPиTelnet.ПримеромтакихкоммутаторовявляютсяDES1226GиDGS-1216T/1224T.

Большинство современных управляемых коммутаторов обеспечивают возможность конфигурирования на основе Web, что позволяет использовать в качестве станции управления любой компьютер, оснащенный Web- браузером, независимо от операционнойсистемы.

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

Подключение ккоммутатору

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

При подключении к Ethernet порту коммутатора Ethernet совместимых серверов, маршрутизаторов или рабочих станций, используется четырехпарный кабель UTP категории 5, 5e или 6 для GigabitEthernet. Поскольку коммутаторы D-Link поддерживают функцию автоматическогоопределения полярности (MDI/MDI-X), можно использовать любой типкабеля (прямой иликроссовый).

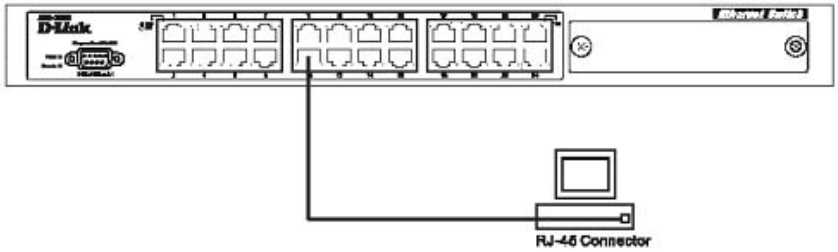


Рисунок 31 Подключение компьютера ккоммутатору

Для подключения к другому коммутатору так же можно использовать любой четырехпарный кабель UTP категории 5, 5e, 6 при условии, что порты коммутатора поддерживают автоматическое определение полярности. В противном случае надо использовать кроссовыйкабель.

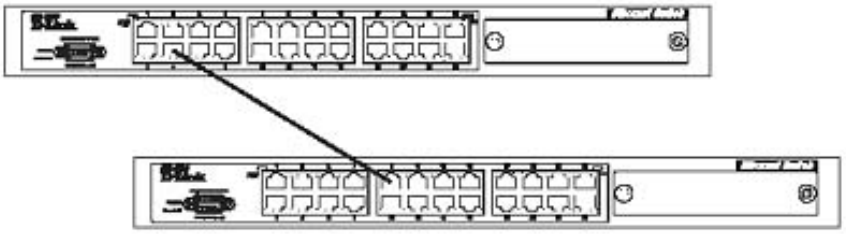


Рисунок 32 Подключение коммутатора к обычному (не -Uplink) порту коммутатора спомощью прямого или кроссовогокабеля

Правильность подключения поможет определить светодиодная индикация порта. Если соответствующий индикатор горит, то связь между коммутатором и подключенным устройством установлена. Если индикатор не горит, возможно, что не включено питание одного из устройств или возникли проблемы с сетевым адаптером подключенного устройства, или имеются неполадки с кабелем. Если индикатор загорается и гаснет, возможно, есть проблемы с автоматическим определением скорости и режимом работы (дуплекс / полудуплекс). (За подробным описание сигналов индикаторов необходимо обратиться к руководству пользователя коммутатора конкретной модели).

Функционирование коммутаторов локальной сети

Коммутаторы – это устройства канального уровня, которые позволяют соединить несколько физических сегментов локальной сети в одну большую сеть. Коммутация локальных сетей обеспечивает взаимодействие сетевых устройств по выделенной линии без возникновения коллизий, с параллельной передачей нескольких потоков данных.

Коммутаторы локальных сетей обрабатывают кадры на основе алгоритма прозрачного моста (transparent bridge) IEEE 802.1, который применяется в основном в сетях Ethernet. При включении питания коммутатор начинает изучать расположение рабочих станций всех присоединенных к нему сетей путем анализа MAC-адресов источников входящих кадров. Например, если на порт 1 коммутатора поступает кадр от узла 1, то он запоминает номер порта, на который этот кадр пришел и добавляет эту информацию в таблицу коммутации (forwarding database). Адреса изучаются динамически. Это означает, что, как только будет прочитан новый адрес, то он сразу будет занесен в контентно-адресуемую память (content-addressable memory, CAM). Каждый раз, при занесении адреса в таблицу коммутации, ему присваивается временной штамп. Это позволяет хранить адреса в таблице в течение определенного времени. Каждый раз, когда идет обращение по этому адресу, он получает новый временной штамп. Адреса, по которым не обращались долгое время, из таблицы удаляются.

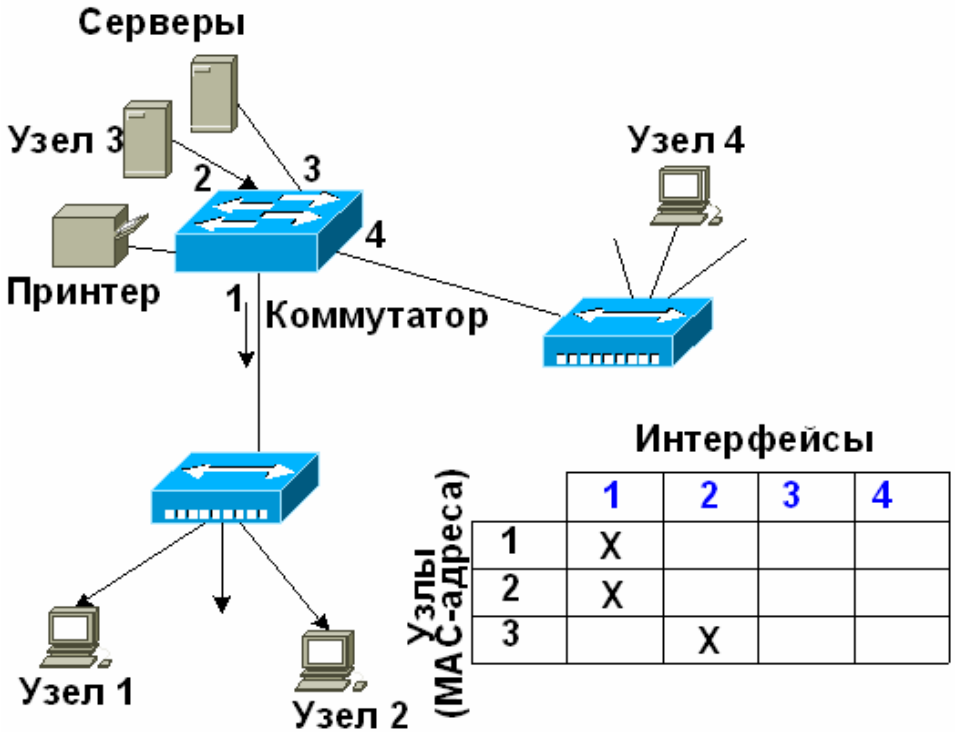


Рисунок 1 Построение таблицы коммутации

Коммутатор использует таблицу коммутации для пересылки трафика. Когда на один из его портов поступает пакет данных, он извлекает из него информацию о MAC-адресе приемника и ищет этот MAC-адрес в своей таблице коммутации. Если в таблице есть запись, ассоциирующая MAC-адрес приемника с одним из портов коммутатора, за исключением того, на который поступил кадр, то кадр пересылается через этот порт. Если такой ассоциации нет, кадр передается через все порты, за исключением того, на который он поступил. Это называется лавинным распространением (flooding). Широковещательная и многоадресная рассылка выполняется также путем лавинного распространения. С этим связана одна из проблем, ограничивающая применение коммутаторов. Наличие коммутаторов в сети не препятствует распространению широковещательных кадров (broadcast) по всем сегментам сети, сохраняя ее прозрачность. В случае если в результате каких-либо программных или аппаратных сбоев протокол верхнего уровня или сам сетевой адаптер начнет работать не правильно, и будет постоянно генерировать широковещательные кадры, коммутатор в этом случае будет передавать кадры во все сегменты, затапливая сеть ошибочным трафиком. Такая ситуация называется широковещательным штормом (broadcast storm).

Коммутаторы надежно изолируют межсегментный трафик, уменьшая таким образом трафик отдельных сегментов. Этот процесс называется фильтрацией (filtering) и выполняется в случаях, когда MAC-адреса источника и приемника принадлежат одному сегменту. Обычно фильтрация повышает скорость отклика сети, ощущаемую пользователем.

Дуплексный и полудуплексный режим работы коммутатора

Коммутаторы локальных сетей поддерживают два режима работы: *полудуплексный* режим и *дуплексный* режим.

Полудуплексный режим - это режим, при котором, только одно устройство может передавать данные в любой момент времени в одном домене коллизий1.

Дуплексный режим – это режим работы, который обеспечивает одновременную двухстороннюю передачу данных между станцией- отправителем и станцией-получателем на MAC - подуровне. При работе в дуплексном режиме, между сетевыми устройствами повышается количество передаваемой информации. Это связано с тем, что дуплексная передача не вызывает в среде передачи коллизий, не требует составления расписания повторных передач и добавления битов расширения в конец коротких кадров. В результате не только увеличивается время, доступное для передачи данных, но и *удваивается* полезная полоса пропускания канала, поскольку каждый канал обеспечивает полноскоростную одновременную двустороннюю передачу2.

Управление потоком IEEE 802.3x в дуплексном режиме

Дуплексный режим работы требует наличия такой дополнительной функции, как управление потоком. Она позволяет принимающему узлу (например, порту сетевого коммутатора) в случае переполнения дать узлу- источнику команду (например, файловому серверу) приостановить передачу кадров на некоторый короткий промежуток времени. Управление осуществляется между MAC-уровнями с помощью кадра-паузы, который автоматически формируется принимающим MAC уровнем. Если переполнение будет ликвидировано до истечения периода ожидания, то для того, чтобы восстановить передачу, отправляется второй кадр-пауза с нулевым значением времени ожидания (см. Рисунок 3).

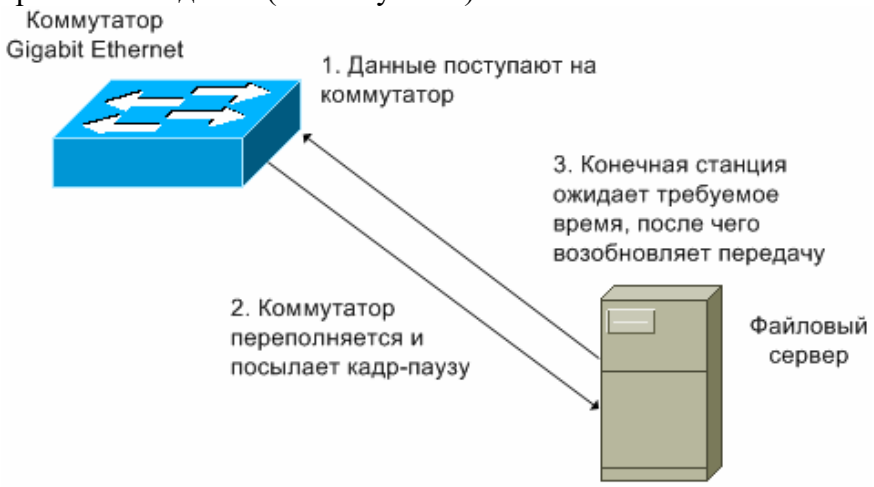


Рисунок 2 Последовательность управления потоком IEEE 802.3x

Дуплексный режим работы и сопутствующее ему управление потоком являются дополнительными режимами для всех MAC-уровней Ethernet независимо от скорости передачи. Кадры-паузы идентифицируются как управляющие MAC-кадры по индивидуальным (зарезервированным) значениям поля длины/типа. Им также присваивается зарезервированное значение адреса приемника, чтобы исключить возможность передачи входящего кадра-паузы протоколам верхних уровней или на другие порты коммутатора

Методы коммутации

В коммутаторах локальных сетей могут быть реализованы различные методы передачи кадров. При *коммутации с промежуточным хранением (store-and-forward)* – коммутатор копирует весь принимаемый кадр в буфер и производит его проверку на наличие ошибок. Если кадр содержит ошибки (не совпадает контрольная сумма, или кадр меньше 64 байт или больше 1518 байт), то он отбрасывается. Если кадр не содержит ошибок, то коммутатор находит адрес приемника в своей таблице коммутации и определяет исходящий интерфейс. Затем, если не определены никакие фильтры, он передает этот кадр приемнику.

Этот способ передачи связан с задержками - чем больше размер кадра, тем больше времени требуется на его прием и проверку на наличие ошибок.

Коммутация без буферизации (cut-through) – коммутатор локальной сети копирует во внутренние буферы только адрес приемника (первые 6 байт после префикса) и сразу начинает передавать кадр, не дожидаясь его полного приема. Это режим уменьшает задержку, но проверка на ошибки в нем не выполняется. Существует две формы коммутации без буферизации:

Коммутация с быстрой передачей (fast-forwardswitching) – эта форма коммутации предлагает низкую задержку за счет того, что кадр начинает передаваться немедленно, как только будет прочитан адрес назначения. Передаваемый кадр может содержать ошибки. В этом случае сетевой адаптер, которому предназначен этот кадр, отбросит его, что вызовет необходимость повторной передачи этого кадра.

Коммутация с исключением фрагментов (fragment-freeswitching) – коммутатор фильтрует коллизионные кадры, перед их передачей. В правильно работающей сети, коллизия может произойти во время передачи первых 64 байт. Поэтому, все кадры, с длиной больше 64 байт считаются правильными. Этот метод коммутации ждет, пока полученный кадр не будет проверен на предмет коллизии, и только после этого, начнет его передачу. Такой метод коммутации уменьшает количество пакетов передаваемых с ошибками.

распространению широковещательных кадров (broadcast) по всем сегментам сети, сохраняя ее прозрачность.

Таким образом, очевидно, что для повышения производительности сети необходима функциональность 3-го уровня OSI модели.

Коммутатор локальной сети уровня 2 с функциями уровня 3 (или *коммутатор 3-го уровня*) принимает решение о коммутации на основании бóльшего количества информации, чем просто MAC-адрес. Коммутаторы 3-го уровня осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней OSI модели. Такие коммутаторы динамически решают, коммутировать (уровень 2) или маршрутизировать (уровень 3) входящий трафик. Коммутаторы 3 уровня выполняет коммутацию в пределах рабочей группы и маршрутизацию между рабочими группами.

Коммутаторы 3-го уровня функционально практически ничем не отличаются от традиционных маршрутизаторов и выполняют те же функции:

- определение оптимальных путей передачи данных на основе логических адресов (адресов сетевого уровня, традиционно IP- адресов)
- управление широковещательным и многоадресным трафиком
- фильтрация трафика на основе информации 3-го уровня
- IP- фрагментация.

Основное отличие между маршрутизаторами и коммутаторами 3-го уровня заключается в том, что в маршрутизаторах общего назначения принятие решения о пересылке пакетов обычно выполняется программным образом, а в коммутаторах обрабатывается специализированными контроллерами ASIC. Это позволяет коммутаторам выполнять маршрутизацию пакетов на скорости канала связи.

D-Link предлагает проектировщикам сетей широкий модельный ряд высокопроизводительных коммутаторов 3-го уровня FastEthernet и GigabitEthernet. Это семейство коммутаторов серии xStack™ DGS-3324SR, DGS- 3324SRi, DXS-3326GSR, DXS-3350SR и DES-3352SR, модульный коммутатор DGS-3312SR, шасси DES-6500 и др.

Коммутация 4-го уровня считается технологией аппаратной коммутации уровня 3, которая может учитывать используемое приложение (например, Telnet или FTP). Коммутаторы D-Link используют информацию 4-го уровня (номера портов, находящиеся в заголовке транспортного уровня) при создании списков доступа для фильтрации данных протоколов верхнего уровня, программ и приложений.

Многоуровневые коммутаторы сочетают в себе технологии коммутации уровней 2, 3 и 4. Принятие решения о передаче данных осуществляется в таких коммутаторах на основе следующей информации:

- MAC - адресе источника/приемника кадра данных
- IP-адресе источника/приемника из заголовка сетевого (3-го) уровня
- типа протокола в заголовке сетевого уровня

номера порта источника/приемника в заголовке транспортного уровня.

Лабораторная работа № 2

Тема: «Подключение к локальной консоли коммутатора»

Цель работы: изучить процедуру подключения к локальной консоли коммутатора.

Порядок выполнения работы

Подключение к локальной консоликоммутатора

Управляемые коммутаторы D-Link имеют консольный порт, который с помощью кабеля стандарта RS-232, входящему в комплект поставки, подключается к последовательному порту компьютера. Подключение по консоли иногда называют ‘Out-of-Band’ подключением. Это означает, что консоль использует отличную от обычного сетевого подключения схему (не использует полосу пропускания портов Ethernet). Она может использоваться для установки и управления коммутатором, даже если нет подключения к сети.

После подключения к консольному порту необходимо следует запустить эмулятор терминала (например, программу HyperTerminal в Windows). В программе следует установить следующие параметры подключения, которые указаны в документации к устройству, какправило:

- Baud rate: 9,600
- Data width: 8bits
- Parity: none
- Stopbits: 1
- Flow Control: none

При соединении коммутатора с консолью появится следующее окно (только для коммутаторов, имеющих поддержку интерфейса командной строкиCLI):

```
            DES-3828 Fast Ethernet Switch Command Line Interface

                              Firmware: Build 3.00.B22
         Copyright(C) 2004-2005 D-Link Corporation. All rights reserved.
UserName:
```

Рисунок 33 Первоначальное окноконсоли

Более старые модели коммутаторов, например, DHS-3226 имеют систему меню (см. Рисунок 34). Настройка коммутатора с помощью системы меню рассматриваться не будет, поскольку все современные модели коммутаторов поддерживают настройку с помощью интерфейса командной строки.

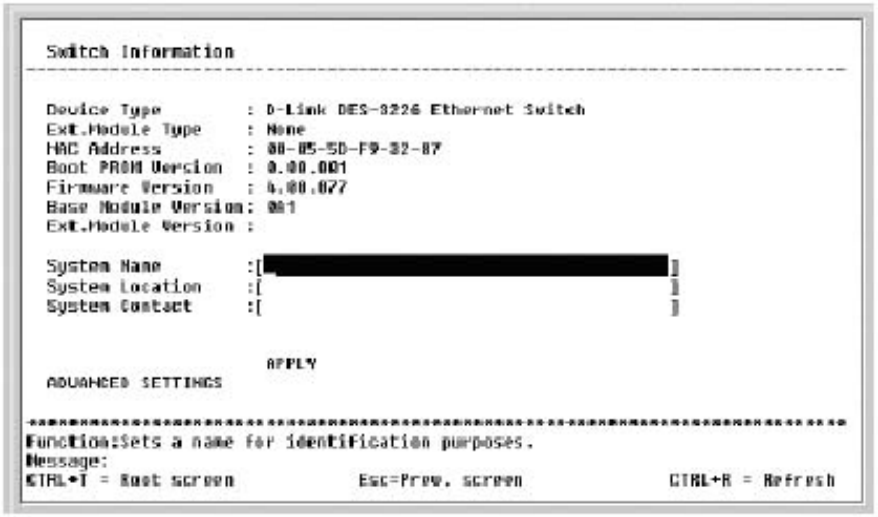


Рисунок 34 Система менюкоммутатора

Если окно не появилось, нажмите Ctrl+R , чтобы егообновить.

Все управляемые коммутаторы могут иметь защиту от доступа неавторизованных пользователей, поэтому после загрузки устройства может появиться приглашение ввести имя пользователя и пароль. По умолчанию имя пользователя и пароль в коммутуторах D-Link не определены, поэтому нажмите дважды клавишу Enter. После этого в командной строке появится приглашение, например**DES-3800:admin#**.

Теперь можно вводитькоманды.

```
                DES-3828 Fast Ethernet Switch Command Line Interface

                                Firmware: Build 3.00.B22
          Copyright(C) 2004-2005 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DES-3800:admin#
```

Рисунок 35 Строка приглашения CLIкоммутатора

В конструктивном отношении коммутаторы делятся на следующиетипы:

- автономные коммутаторы с фиксированным количествомпортов;
- модульные коммутаторы на основешасси;
- коммутаторы с фиксированным количеством портов, объединяемые встек.

Первый тип коммутаторов обычно предназначен для организации небольших рабочих групп. Они могут иметь от 8 до 50 портов со скоростями 10,100,1000Мбит/с, заключенных в корпус для настольной установки или монтажа в стойку. К этому типу можно отнести семейство неуправляемых коммутаторов FastEthernet в настольном управлении D-LinkDES-1005D, DES- 1008D, DES-1018DG, DES-1024DG, DES-1010G, DES-1016D, DES-1024D идр.

Рисунок 7 Настольный неуправляемый коммутаторDES-1018DG

Рисунок 8 Монтируемый в стойку настраиваемый коммутаторDES-1226G

Модульные коммутаторы на основе шасси чаще всего предназначены для применения на магистрали сети. Поэтому они выполняются на основе какой-либо комбинированной схемы, в которой взаимодействие модулей организуется по быстродействующей шине или же на основе быстрой разделяемой памяти большого объема. Модули такого коммутатора выполняются на основе технологии «hotswap», то есть допускают замену на ходу, без выключения коммутатора, так как центральное коммуникационное устройство сети не должно иметь перерывов в работе. Шасси обычно снабжается резервными источниками питания и резервными вентиляторами в тех жецелях.

Модульные коммутаторы уровня 2 и 3 D-Link представлены следующими моделями:

- шасси 2 уровня – DES-1200M, DES-6000,DES-7000
- шасси 3 уровня – DES-6300,DES-6500.

Рисунок 9 Модульный коммутатор 3-го уровняDES-6500

С технической точки зрения определенный интерес вызывают стековые коммутаторы. Эти устройства представляют собой коммутаторы, которые могут работать автономно, так как выполнены в отдельном корпусе, но имеют специальные интерфейсы, которые позволяют их объединять в общую систему, работающую как единый виртуальный коммутатор. Говорится, что в этом случае отдельные коммутаторы образуютстек.

Стекируемые управляемые коммутаторы D-Link представлены следующимисемействами:

- управляемые стекируемые коммутаторы Fast Ethernet 2/3-го уровня семействаDES-3x26S;
- управляемые коммутаторы Fast Ethernet 2/3-го уровня семейства DES-35xx и 38xx с поддержкой виртуального стека и технологии Single IP Management(SIM);
- семейство высокопроизводительных управляемых стекируемых коммутаторов Fast/Gigabit Ethernet 3-го уровня с поддержкой технологий SIM и xStack™ DES-3352SR, DGS-3324SR, DGS- 3324SRi, DXS-3326GSR, DXS-3350SR, DGS-34xx иDGS-36xx.

Объединение коммутаторов в стек осуществляется с помощью специализированных модулей и кабелей для стекирования по топологии
«кольцо» или«звезда».

Стек типа «кольцо» строится по следующей схеме: один специализированный интерфейс для стекирования с помощью специализированых кабелей подключается к вышележащему коммутатору, а второй - к нижележащему, при этом самый нижний и самый верхний коммутатор в стеке такжеобъединяются.

Рисунок 10 Стек на коммутатораxDGS-3324SR

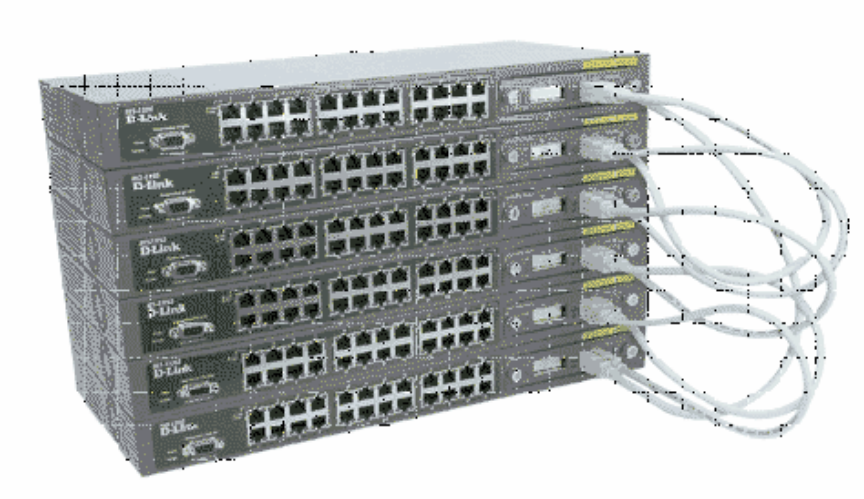


Рисунок 11 Стек на коммутатораxDES-3226S

Передача данных в таком стеке выполняется по кругу в направлении коммутаторов с большими номерами (каждый коммутатор стека имеет свой порядковый номер), как показано на рисунке10.

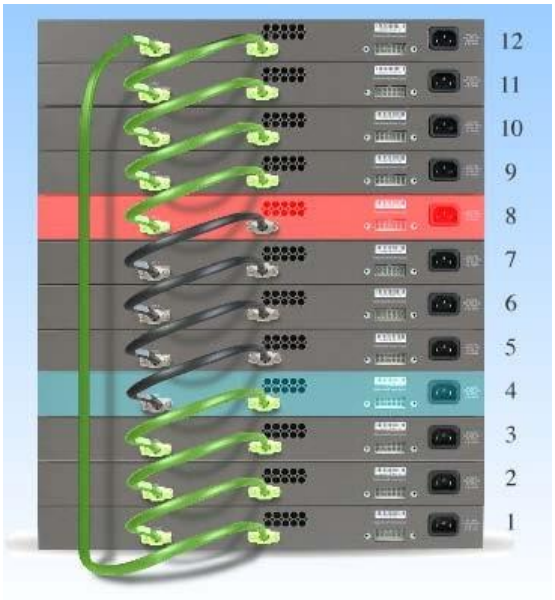


Рисунок12Передачаданныхоткоммутатора8коммутатору4встеке**«кольцо»**Максимальное количество устройств, которое может быть объединено в стек зависит от модели коммутатора и его программного обеспечения. В настоящее время в стек топологии «кольцо» можно объединить до 13 коммутаторов DES-3226S или DES-3326S и до 12 коммутаторов серии xStack DGS-3324SR.

Стек типа «звезда» строится по следующей схеме: коммутаторы объединяются не друг с другом, а с отдельным устройством, обеспечивающим более высокопроизводительный обмен данными между любыми парами коммутаторов. Роль агрегирующего устройства такого стека исполняет мастер-коммутатору.

По сравнению с топологией «кольцо», основными преимуществами данной архитектурыявляются:

- бóльшая устойчивость к ошибкам, т.к. разрыв связи между коммутатором и мастером- коммутатором не повлияет на остальные каналы связи стека. (В случае использования топологии «кольцо» у коммутаторов DES-3326S/3226S, разрыв связи между 2-мя любыми коммутаторами, приведет к прекращению работы всегостека);
- повышенная производительность, так как каждое соединение точка-точка является полнодуплекснымсоединением.

Компания D-Link производит высокопроизводительные коммутаторы GigabitEthernet 3-го уровня D-LinkDGS-3312SR и DGS-3324SRi, которые могут выступать в качестве мастер-коммутатора стека типа«звезда».

Используя стекирующие модули DEM-540, коммутатор DGS-3312SR позволяет объединить в стек до 12 стековых коммутаторов 2-го уровня DES- 3226S, получив до 288 портов 10/100 Мбит/с FastEthernet и 12 портов GigabitEthernet, и управлять ими как единым сетевым узлом. Следует отметить, что, используя DGS-3312SR в качестве агрегирующего устройства стека крупной рабочей группы предприятия или здания, можно создать гибкую, легко управляемую структуру на основе коммутаторов 2-го уровня и расширить функциональность сети, построенной на этих коммутаторах до предоставления услуг 3-гоуровня.

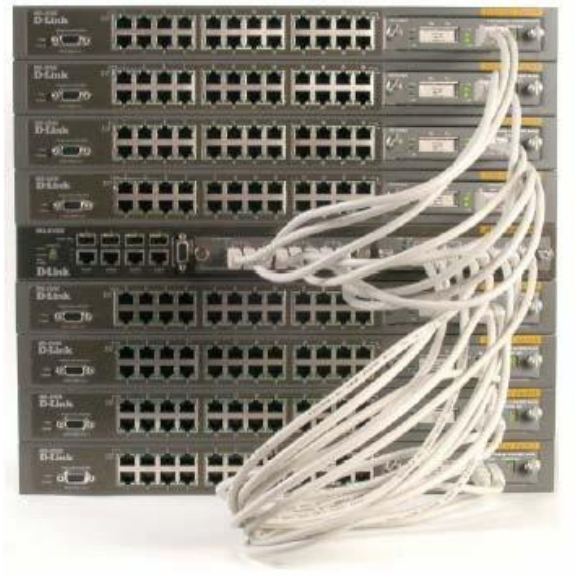


Рисунок 13 Стек типа «звезда» на коммутаторах DGS-3312SR (в середине) иDES-3226S

Лабораторная работа № 3

Тема: «Подключение к Web-интерфейсу управления коммутатором»

Цель работы:изучить процедуру настройки коммутатора и подключения к коммутатору.

Порядок выполнения работы

Подключение к Web-интерфейсу управлениякоммутатора

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

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

Связь между клиентом и сервером обычно осуществляется черезTCP/IP соединение с номером порта HTTP равным80.

Для того чтобы подключиться к HTTP серверу на коммутаторе, используя интерфейс командной строки, необходимо выполнить следующие шаги:

Назначить коммутатору IP-адрес из диапазона адресов Вашей сети, используякоманду:

*DES-3800:admin #***config ipif System ipaddress xxx.xxx.xxx.xxx/yy,**

где xxx.xxx.xxx.xxx – IP-адрес, yyy.yyy.yyy.yyy – маскаподсети

Проверить правильность настройки IP-адреса коммутатора с помощью команды:

*DES-3800:admin#***showipif**

На рабочей станции запустить Web-браузер, в командной строке которого ввести IP-адрес коммутатора, появится соответствующая страничка (см. Рисунок49)

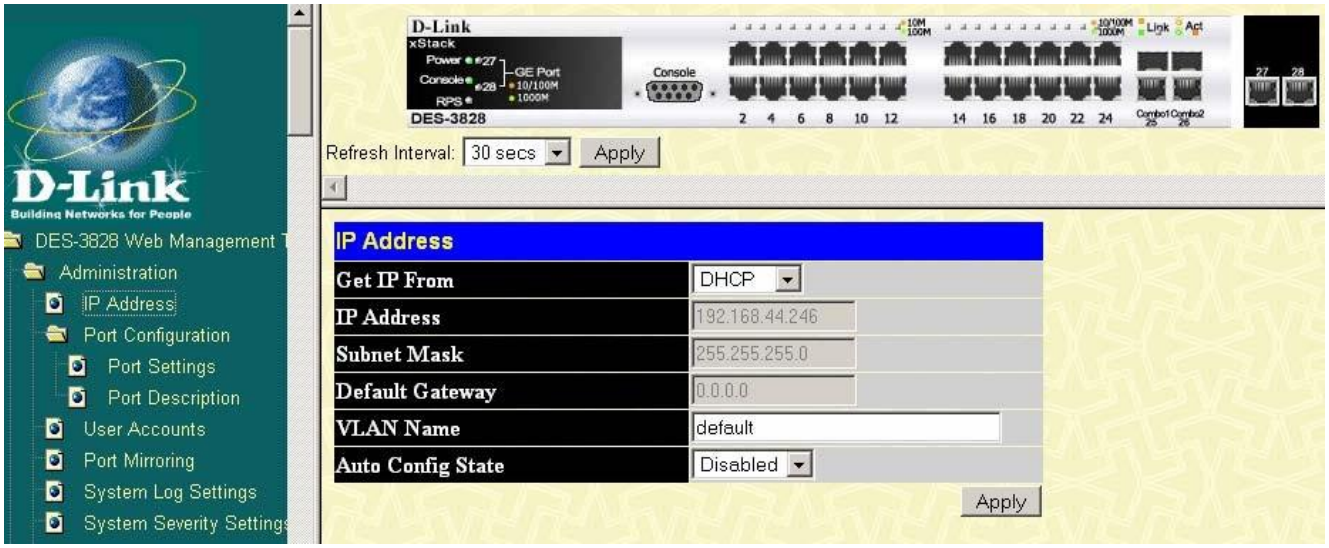


Рисунок 49 Web-интерфейскоммутатора

Дополнительные функциикоммутаторов

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

- VLAN;
- Семейство протоколов Spanning Tree IEEE 802.1d, 802.1w,802.1s;
- Статическое и динамическое по протоколу IEEE 802.3ad LACP агрегирование каналовEthernet;
- агрегирование каналов по протоколу IEEE 802.3adLACP;
- Сегментация трафика и обеспечение качества обслуживанияQoS;
- Функции обеспечения безопасности, включая аутентификацию IEEE 802.1x и функцию PortSecurity;
- Протоколы групповоговещания;
- SNMP – управление идр.

Лабораторная работа № 4

Тема: «Настройка полосы пропускания с помощью команд CLI»

Цель работы:изучить процедурунастройки полосы пропускания с помощью команд CLI.

Порядок выполнения работы

Контроль полосыпропускания

Контроль полосы пропускания обычно используется для ограничения скорости передачи и приема битов данных для порта, не зависимо от реальной скоростиподключения.

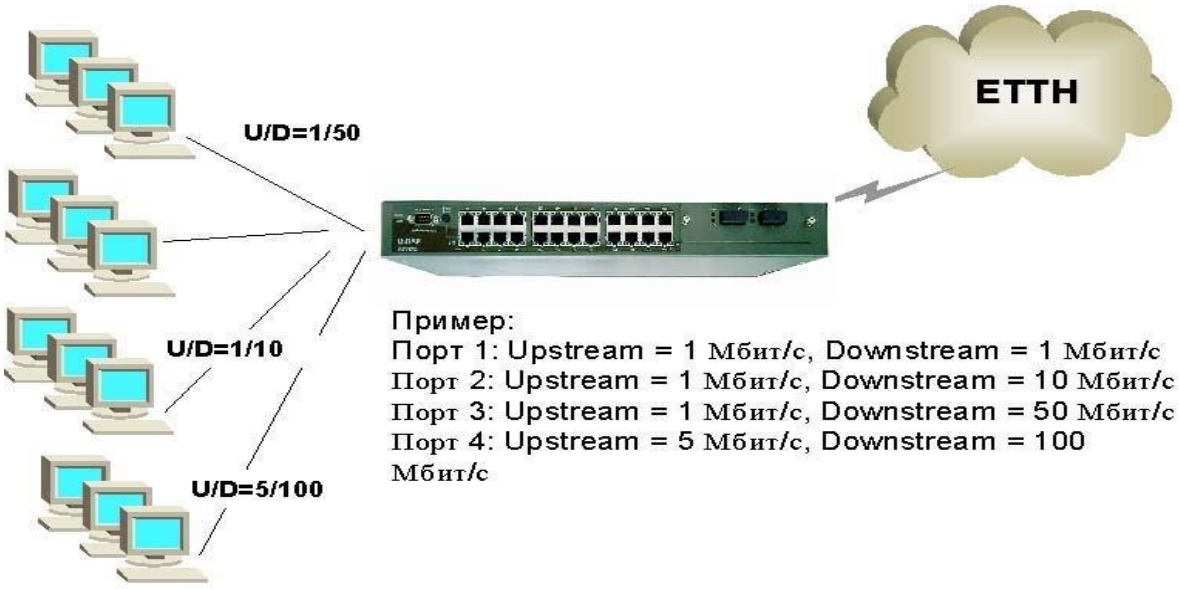


Рисунок 125 Ограничение полосы пропускания дляПК

Конфигурирование полосы пропускания с помощью командCLI

Ниже приведены команды для конфигурирования полосы пропускания портов с помощью CLI (см. Таблица9).

Таблица 9 Команды для настройки Trafficcontrol

Команда	Параметры	Описание
config bandwidth_control	<portlist> rx_rate no_limit <value64-1024000> tx_rate no_limit	Настройка полосы пропускания на указанномпорте
show bandwidth_control	<portlist>	Просмотр настроек полосы пропускания для каждогопорта

Шаг 1. Настроить на портах с 1 по 8 скорость передачи пакетов, равную 1 Мбит/с командой “configbandwidth_control 1-8 tx_rate1000”:

```
DES-3010F:4#config bandwidth_control 1-8 tx_rate 1000
Command: config bandwidth_control 1-8 tx_rate 1000

Note: To perform precise bandwidth control, it is required to enable the flow
control to mitigate the retransmission of TCP traffic.

Success.
```

Рисунок 126 Конфигурирование полосыпропускания

Шаг 2. Проверить настройки полосы пропускания на каждом порте командой

“showbandwidth_control”:

```
DES-3010F:4#show bandwidth_control
Command: show bandwidth_control

Bandwidth Control Table

Port   RX Rate (kbit/sec)          TX_RATE (kbit/sec)
----   -------------------------   ----------------------
1      no_limit                    no_limit
2      no_limit                    no_limit
3      no_limit                    no_limit
4      no_limit                    no_limit
5      no_limit                    no_limit
6      no_limit                    no_limit
7      no_limit                    no_limit
8      no_limit                    no_limit
9      no_limit                    no_limit
10     no_limit                    no_limit
```

Рисунок 127 Просмотр настроек полосы пропускания

Вызов помощи покомандам

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

Используйте знак вопроса «?» так же в том случае, если Вы не знаете параметров команды. Например, если надо узнать возможные варианты синтаксиса команды config, введите в командойстроке:

DES-3800:admin#config

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

```
DES-3800:admin#config ?
Command: config

Next possible completions:
802.1p              802.1x              access_profile      account
accounting          address_binding     admin               arp_aging
arpentry            authen              authen_enable       authen_login
bandwidth_control   command_history     command_prompt      configuration
cpu                 dhcp_relay          dnsr                double_vlan
dst                 dvmrp               fdb                 firmware
greeting_message    gvrp                igmp                igmp_snooping
ipif                lacp_port           limited             link_aggregation
mac_based_access_control                mac_based_access_control_local
mac_notification    md5                 mirror              multicast_fdb
ospf                pim                 port_security       ports
radius              rip                 route               router_ports
safeguard_engine    scheduling          scheduling_mechanism
serial_port         sim                 sim_group           snmp
sntp                ssh                 ssl                 stp
syslog              system_severity     time                time_zone
traffic             traffic_segmentation                    vlan
vrrp                wac                 wred

DES-3800:admin#
```

Рисунок 37 Результат вызова помощи о возможных параметрах командыconfig

Базовая конфигурациякоммутатора

Шаг 1. Обеспечениезащитыкоммутатораотдоступанеавторизованных пользователей.

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

Создать учетную запись пользователя можно с помощью следующих команды “createaccountadmin/user<username>”

(знак «/» означает ввод или одного параметра, илидругого)

Далее появится приглашение для ввода пароля и подтвержденияввода:

Enter a case-sensitive newpassword:

Enter the new password again forconfirmation*:*

Максимальная длина имени пользователя и пароля от 0 до 15 символов. После успешного создания учетной записи на экране появитсяслово *Success*.

Ниже приведен пример создания учетной записи с уровнем привилегий «Admin» и именем пользователя (Username)«dlink»:

```
DES-3800:admin#create account admin dlink
Command: create account admin dlink

Enter a case-sensitive new password:*
Enter the new password again for confirmation:*
Success.

DES-3800:admin#
```

Рисунок 38 Создание учетнойзаписи

Изменить пароль для пользователя с существующей учетной записью, можно с

помощьюкоманды:

DES-3800:admin# **config account**<*username*>

```
DES-3800:admin#config account dlink
Command: config account dlink

Enter a old password:*
Enter a case-sensitive new password:*
Enter the new password again for confirmation:*
Success.

DES-3800:admin#
```

Рисунок 39 Изменение учетной записиdlink

Проверить созданную учетную запись можно с помощьюкоманды:
DES-3800:admin# **showaccount**

```
DES-3800:admin#show account
Command: show account

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

Total Entries : 1

DES-3800:admin#
```

Рисунок 40 Просмотр созданных учетныхзаписей

Удалить учетную запись можно, выполнив команду **delete account**<*username*>.

```
DES-3800:admin#delete account dlink
Command: delete account dlink

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

DES-3800:admin#
```

Рисунок 41 Удаление учетной записиdlink

При создании учетной записи администратора следует запоминать заданные имя и пароль. Утеря администраторского пароля потребует обращения в сервисный центр компанииD-Link!

Шаг 2. НастройкаIP-адреса.

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

DES-3800:admin# **config ipif Systemdhcp**

DES-3800:admin# **config ipif System ipaddress**xxx.xxx.xxx.xxx/yy

гдеxxx.xxx.xxx.xxx–IP-адрес,yy–маскавCIDRформате,например /24 или /30), System- имя управляющего интерфейсакоммутатора.

```
DES-3800:admin#config ipif System ipaddress 192.168.44.42/24
Command: config ipif System ipaddress 192.168.44.42/24

Note: All configuration on this interface will return to default setting.
Success.

DES-3800:admin#
```

Рисунок 42 ИзменениеIP-адреса

Лабораторная работа № 5

Тема: «НастройкаAccessControlLists (ACL) спомощьюCLI»

Цель работы:изучить процедуру настройкиAccessControlLists (ACL) спомощьюCLI.

Порядок выполнения работы

AccessControlLists(ACL)

Списки управления доступом (AccessControlLists) обеспечивают ограничение прохождения трафика через коммутатор. Профили доступа указывают коммутатору, какие виды пакетов принимать, а какие – отвергать. Прием пакетов или отказ в приеме основывается на определенных признаках, таких как адрес источника, адрес приемника, адрес порта, и других.

Профиль управления доступом дает возможность управлять трафиком и просматривать определенные пакеты, применяя списки доступа (ACL) на всех интерфейсахкоммутатора.

В коммутаторах D-Link существует два основных типа профилей управления доступом: Ethernet и IP. Фильтрация в этих типах профилей может выполняться на основе MAC -адресов источника и приемника, VLAN, IP-адресов, номеровпортов.

Профили доступа работают последовательно, в порядке возрастания их номеров (ProfileID). Пакет проверяется на соответствие условиям, указанным в профилях доступа, начиная с первого профиля. Если профиль подходит, пакет или принимается, или отбрасывается и дальше не проверяется. Если не один профиль не подходит, применяется политика по умолчанию, разрешающая прохождение всеготрафика.

Алгоритм создания профилядоступа

Проанализируйте задачи фильтрации иопределите:

- какой профиль доступа использовать: Ethernet илиIP;
- определитесь со стратегией и запишитеее;
- основываясь на стратегии, определите, какие маски профилядоступа Access Profile Mask нужны и создайтеих;
- добавьте правила Access Profile Rule связанные смаской.

В коммутаторах существуют ограничения на максимальное количество профилей доступа и правил, определенных для них. Так, например, коммутатор DES-3226S может поддерживать максимально 10 профилей доступа, содержащих максимум 50 правил (50 правил – суммарное количество правил для всех 10 определенных профилей), коммутатор DES- 3526 – 9 профилей и до 800правил.

Создание профилей доступа (с использованиемWeb-интерфейса)

Процесс создание профиля доступа делится на 2 основныечасти:

Создание маски профиля доступа - указывается какую часть или части кадра будет проверять коммутатор, например MAC адрес источника или IP адресназначения.

Создание правил профиля доступа: вводится условие, которое коммутатор будет использовать для определения действий над кадром (принять илиотбросить).

Access Profile Table

Profile ID	Type	Owner	Access Rule	Delete
1	IP	ACL	Modify	✕
2	Ethernet	ACL	Modify	✕

Рисунок 146 Таблица настроек масокпрофилей

Шаг 1: Создание маски профиля (AccessProfileMask)

1. Зайдите на Web-интерфейс управления коммутатором.

ВыберитепунктConfiguration/ Access ProfileTable.

2. Щелкните на кнопке Add на странице таблицы настройки масок профилей Access Profile Table. Появится новое меню. Используйте его для создания профиля доступа и укажите, какие условия использовать для проверки кадра. Как только профиль будет создан, к профилю можно будет применитьправила.
3. Задайте следующие параметры маски профилядоступа:

   а) **Идентификатор профиля (ProfileID)**: Наберите уникальный идентификационный номер для профиля или разрешите установить этот номер автоматически, выбрав опцию AutoAssign. Это значение может быть в диапазоне от 1 до255;

   б) **Тип профиля доступа (Type)**: Выберите профиль Ethernet, IP, или PacketContentMask. Вид меню изменится в соответствии с требованиями для выбранного типа профиля (см.Рисунок 147, Рисунок 148 и Рисунок 149). Используйте Ethernet, для того, чтобы коммутатор исследовал часть заголовка 2-го уровня каждого пакета. Используйте IP, для того, чтобы коммутатор исследовал IP адрес в заголовке каждого кадра. Используйте PacketContentMask для обработки пакетов по первым 80-ти байтам заголовкапакетов.

   в) **VLAN**: Выберите эту опцию, для того, чтобы коммутатор исследовал поле VLAN заголовка каждого пакета и использовал его в качестве критерия или части критерия для принятия решения о передачепакетов.

Для профиляEthernet:

4. **Маска адреса источника MAC (Source MAC Mask)**: Маска адреса источника MAC – введите маску MAC адреса для MAC адресаисточника.
5. **Маска адреса назначения MAC (Destination MAC Mask)**: Маска адреса назначения MAC – введите маску MAC адреса для MAC адресаназначения.
6. **802.1p**: Выберите эту опцию, для того, чтобы коммутатор исследовал значение приоритета IEEE 802.1p заголовка каждого пакета и использовал его в качестве критерия или части критерия для принятия решения о передачепакетов.
7. **Ethernet Type**: Выберите эту опцию для того, чтобы коммутатор исследовал значение типа Ethernet в заголовке каждогокадра.

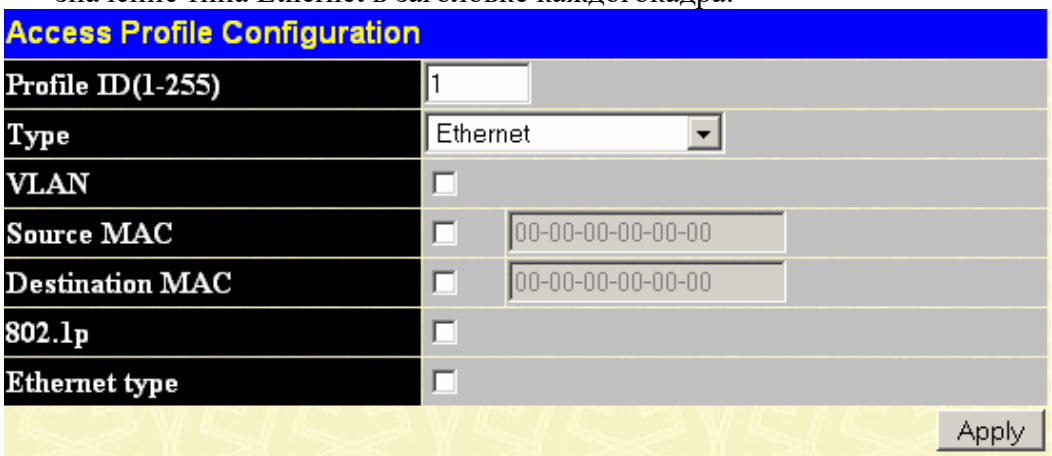


Рисунок 147 Профили доступа на уровнеMAC

Для профиляIP:

4. **Маска адреса источника IP (Source IP Mask):** Маска адреса источника IP - введите маску IP адреса для IP адресаисточника.
5. **Маска адреса назначения IP (Destination IP Mask):** Маска адреса назначения IP - введите маску IP адреса для IP адреса назначения.
6. **DSCP**: Выберите эту опцию, для того, чтобы коммутатор исследовал DiffServ Code Point (DSCP) поле каждого пакета и использовал его в качестве критерия или части критерия для принятия решения о передачепакетов.
7. **Protocol**: Выберите эту опцию для того, чтобы коммутатор исследовал

определенные поля соответствующих протоколов (ICMP, IGMP, TCP, UDP) в заголовке каждого кадра. Для протоколов TCP и UDP в качестве критерия указываются номера портов приложений. Можно использовать либо номер порта источника, либо номер порта приемника, либо оба критерия вместе. В поле *Source Port Mask Ox* укажите маску порта TCP/UDP для порта источника в шестнадцатеричном виде (hex 0x0-0xffff).В поле *Destination Port Mask Ox* укажите маску порта TCP/UDP для порта приемника в шестнадцатеричном виде (hex0x0-0xffff).

8.

Для профиляPacketContentMask:

9. **Offset**: по какому смещению располагаются обрабатываемые поля. 80 байт разбиты на 5 блоков по 16байт.

Шаг 2: Создание правила для маски профилядоступа.

4. Выберите нужный профиль доступа в таблице настроек масок профилей и нажмите кнопкуModify;
5. Создайте новое правило для профиля доступа, щелкнув на кнопке Add. Удалить, ранее созданное правило, можно, нажав напротив него кнопкуDelete;
6. Введите значения в соответствие с ранее заданной маской профиля;
7. Укажите к каким физическим портам будет привязанаправило;
8. Укажите каким будет правило Permit (разрешающее) или Deny (запрещающее).

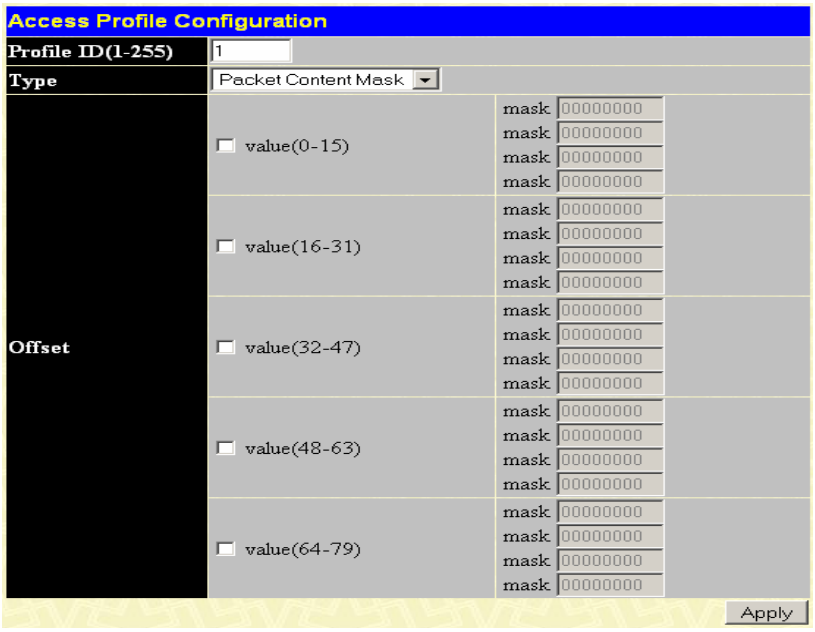


Рисунок 149 Профиль на базеPacketContentMask

Рисунок 150 Установка правил профилядоступа

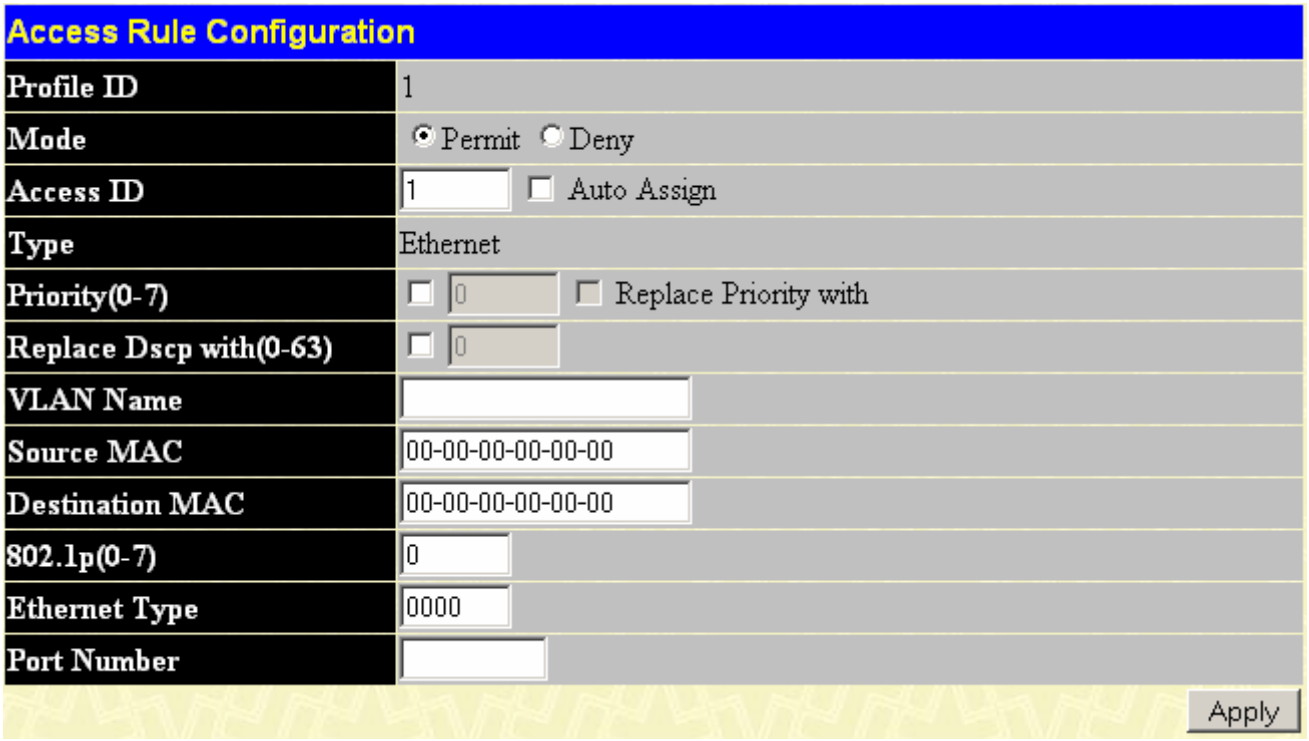


Рисунок 151 Создание правила для профилядоступа

В случае необходимости, при совпадении профиля, значения тега для IEEE 802.1p может быть заменено новым, меняющим приоритет пакета. Для этого надо выбрать опцию priority и ввести нужное значение в соседнем поле. Самый низший приоритет имеет значение 0, наивысший–7.

Лабораторная работа № 6

Тема: «Последовательность начальной загрузки и запуска маршрутизатора»
Цель работы:изучитьпоследовательность начальной загрузки и запуска маршрутизатора.

Порядок выполнения работы

Последовательность начальной загрузки маршрутизатора

При инициализации маршрутизатора последовательно загружается программа начальной загрузки (bootstrap), операционная система и файл конфигурации. Если при инициализации маршрутизатор не обнаруживает конфигурационный файл, то он автоматически входит в режим начальной настройки (setupmode). Резервная копия нового файла конфигурации, создаваемого в режиме настройки, сохраняется в энергонезависимой памяти с произвольным доступом (NVRAM - NonvolatileRandomAccessMemory).

После включения питания маршрутизатор Cisco выполняет самотестирование (POST - Power-OnSelf-Test). Программа самотестирования записана в постоянном запоминающем устройстве (ROM - ReadOnlyMemory). При самотестировании происходит проверка работоспособности всех аппаратных компонентов маршрутизатора: центрального процессора, памяти и сетевых интерфейсов. После проверки аппаратных средств маршрутизатор запускает процесс инициализации программного обеспечения, который состоит из двух этапов:

- Системные стартовые подпрограммы инициализируют программное обеспечение маршрутизатора;
- Резервные подпрограммы, предназначенные для восстановления программного обеспечения, по мере необходимости выполняют альтернативный запуск программного обеспечения.

Стартовые подпрограммы предназначены для запуска операционной системы маршрутизатора CiscoIOS. Маршрутизатор должен обеспечить надежное взаимодействие объединенных сетей согласно заданной конфигурации. Для достижения требуемой цели стартовые подпрограммы должны выполнить следующие действия:

- Удостовериться в том, что аппаратные средства маршрутизатора проверены и нормально функционируют;
- Найти и загрузить основную операционную систему CiscoIOS;
- Найти и применить стартовый конфигурационный файл или, в случае его отсутствия, войти в режим начальной настройки.
-

Последовательность запуска маршрутизатора

Последовательность запуска маршрутизатора Cisco представлена на рисунке 1.2.

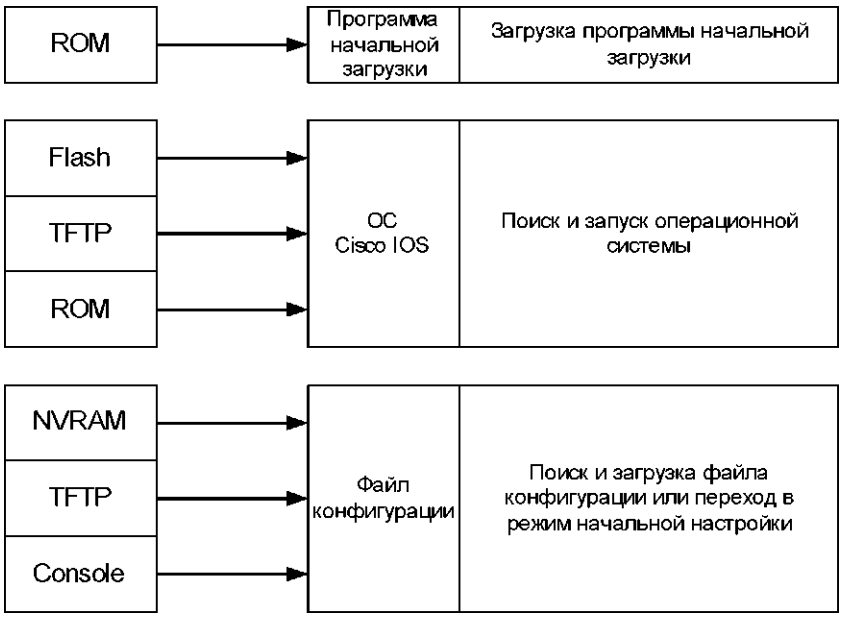


Рисунок 1.2 - Последовательность запуска маршрутизатора Cisco

После выполнения процедур самотестирования при инициализации маршрутизатора происходят перечисленные ниже события.

1. Выполняется программа начальной загрузки, которая находится в ROM. Она представляет собой простую, предустановленную программу, которая способна выполнять элементарные инструкции. Кроме всего прочего, эта программа может загружать в память альтернативные инструкции или переводить маршрутизатор в другие режимы конфигурирования.

2. Образ операционной системы может находиться в нескольких местах. Для определения местоположения операционной системы используется загрузочное поле конфигурационного регистра. Если загрузочное поле указывает на Flash память или на загрузку из сети, то команда bootsystem в конфигурационном файле указывает имя и местоположения файла-образа операционной системы. Конфигурационный файл, называемый стартовым, хранится в памяти NVRAM и содержит команды, которые администратор заранее внес в конфигурацию и сохранил в маршрутизаторе. Если в стартовом конфигурационном файле явно не указано, откуда маршрутизатор должен загружать образ операционной системы CiscoIOS, стандартно устройство ищет его во Flash памяти.

3. Далее загружается образ операционной системы CiscoIOS. После загрузки операционная система создает список программных и аппаратных компонентов, который выводится в терминальное приложение консоли.

4. В основную память загружается и построчно выполняется файл стартовой конфигурации, который сохранен в NVRAM. Команды этого файла запускают процессы маршрутизации, задают адреса интерфейсов, устанавливают характеристики носителей и т.д.

5. Если в памяти NVRAM хранится неправильный файл конфигурации или эта память очищена, то после перезагрузки операционная система вызывает программу начальной конфигурации, также называемую диалогом начальной настройки.

Определение местонахождения и загрузка программного обеспечения

Стандартно при загрузке источник программного обеспечения CiscoIOS определяется платформой аппаратного обеспечения. Однако обычно маршрутизатор сначала ищет сохраненные в памяти NVRAM команды**bootsystem.** Вместе с тем программное обеспечение CiscoIOS предоставляет пользователю несколько возможных альтернатив. В частности, пользователь может задать маршрутизатору другие источники для загрузки программного обеспечения. При необходимости для загрузки программного обеспечения маршрутизатор может также

использовать свою собственную резервную загрузочную последовательность (fallback). На рисунке 1.3 показан процесс поиска маршрутизатором образа программного обеспечения CiscoIOS.

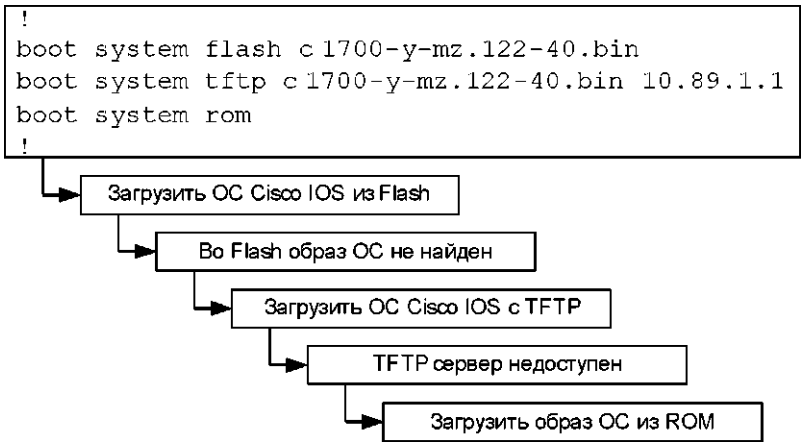


Рисунок 1.3 - Процесс поиска файла операционной системы

- В режиме глобального конфигурирования пользователь может ввести несколько команд bootsystem, определяющих резервные источники (fallback), которые будет последовательно использовать маршрутизатор. В таком случае при повторном запуске маршрутизатор будет использовать эти команды.

- Если в памяти NVRAM отсутствуют команды**bootsystem,** которые мог бы использовать маршрутизатор, то стандартно он использует программное обеспечение CiscoIOS, которое записано во Flash память устройства.

- Если во Flash памяти образ CiscoIOS отсутствует, то для загрузки образа программного обеспечения из сети маршрутизатор пытается использовать простейший протокол передачи файлов (TrivialFileTransferProtocol - TFTP). Для указания имени файла, из которого будет загружаться стандартный образ системы, хранимый на сетевом сервере, маршрутизатор использует конфигурационный регистр.

- Если сервер TFTP недоступен, то маршрутизатор загружает сокращенную версию Cisco IOS, которая хранится в памяти ROM устройства.

Для задания резервной последовательности (fallback) при загрузке программного обеспечения CiscoIOS используется последовательность нескольких команд bootsystem.

1.8 Светодиодные индикаторы маршрутизатора

Для отображения текущего состояния маршрутизатора используются светодиодные индикаторы (LED-индикаторы). Назначение и количество индикаторов зависит от модели маршрутизатора Cisco (Рисунок 1.4).

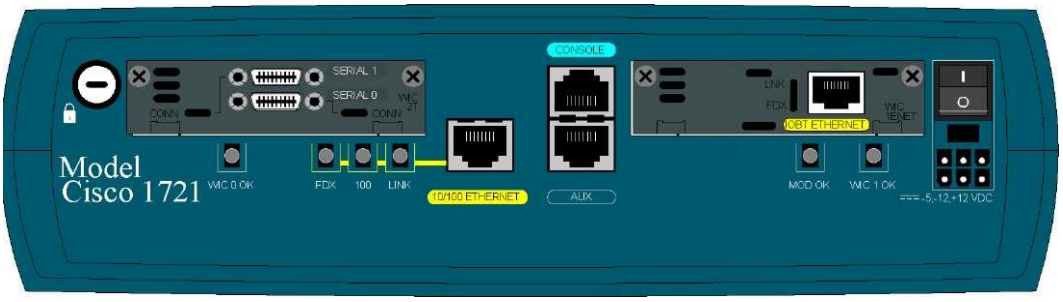


Рисунок 1.4 - Пример LED-индикаторы для маршрутизатора Cisco 1721

Индикаторы на маршрутизаторах показывают активность соответствующих

интерфейсов. Если индикатор не светится, но интерфейс корректно подсоединен к сети, то это свидетельствует о проблемах в работе оборудования. Если же интерфейс маршрутизатора загружен в полной мере, то индикатор будет светиться постоянно. На платах интерфейсов в случае успешной их инициализации должен светиться зеленый индикатор.

1.9 Информация, выводимая при запуске маршрутизатора

Загрузка маршрутизатора происходит по описанному ниже сценарию.

1. Для проверки работоспособности основных компонентов - центрального процессора, памяти и интерфейсов - маршрутизатор выполняет процедуру самодиагностики POST.
2. Для проверки корректной работы программы начальной загрузки отрабатывается образ загрузочного программного обеспечения, а также ищется подходящий образ ОС CiscoIOS. Источником, содержащим образ ОС CiscoIOS, может быть Flash память устройства или TFTP сервер, что определяется конфигурацией регистров маршрутизатора. Стандартное значение регистров устанавливается на заводе изготовителе и равно 0x2102. Оно указывает маршрутизатору, что следует загружать операционную систему из Flash памяти вне зависимости оттого, что указано в качестве параметра команды bootsystem. Если команда bootsystem с какими-либо параметрами в конфигурационном файле отсутствует, маршрутизатор использует стандартную последовательность резервной загрузки операционной системы, т.е. устройство сначала ищет образ системы IOS во Flash памяти.
3. Если после пяти попыток во Flash памяти не обнаруживается подходящий образ операционной системы, то маршрутизатор загружается, используя программное обеспечение, хранимое в ROM. Такое урезанное программное обеспечение используется для установки или обновления образов операционной системы CiscoIOS.
4. Если подходящий образ операционной системы все же был найден, то далее маршрутизатор пытается найти подходящий файл конфигурации.
5. Если файл конфигурации не обнаружен в NVRAM памяти, то маршрутизатор ищет его на TFTP сервере, последовательно перебирая все интерфейсы. Если файл конфигурации не найден, маршрутизатор запускает диалог для ручной настройки устройства.

Из информации, которая показана в примере 1.9, можно определить версию начальной загрузочной программы и версию операционной системы CiscoIOS, которая используется в маршрутизаторе. Также пользователь может уточнить модель маршрутизатора, серию используемого процессора и количество системной памяти.

Лабораторная работа № 7

Тема: «Режимы конфигурирования маршрутизатора»

Цель работы:изучитьрежимы конфигурирования маршрутизатора.

Порядок выполнения работы

Базовая настройка маршрутизатора должна включать:

- назначение IP-адресов (статических или динамических) интерфейсам, участвующим в маршрутизации данных;
- создание зон безопасности и распределение интерфейсов по зонам;
- создание политик, регулирующих прохождение данных между зон;
- настройка сервисов, сопутствующих маршрутизации данных (NAT, Firewall и прочие).

Расширенные настройки зависят от требований конкретной схемы применения устройства и легко могут быть добавлены или изменены с помощью имеющихся интерфейсов управления.

Подключение к маршрутизатору

Предусмотрены следующие способы подключения кустройству:

- подключение по локальной сети Ethernet.

Для первоначального сетевого подключения к устройству рекомендуется использовать интерфейс GigabitEthernet 1/0/2, на котором в заводской конфигурации задан статический IP-адрес.

Подключите сетевой кабель к порту GigabitEthernet 1/0/2 (порт 2 на передней панели устройства) и к компьютеру, предназначенному для управления.

В заводской конфигурации маршрутизатора активированDHCP-сервер с пулом IP-адресов в подсети 192.168.1.0/24. При подключении сетевого интерфейса управляющегокомпьютера он должен получить сетевой адрес от сервера.

Если IP-адрес не получен по какой-либо причине, то следует назначить адресинтерфейса вручную, используя любой адрес, кроме 192.168.1.1, в подсети192.168.1.0/24.

- подключение через консольный порт RS232.

Подключите кабель RJ-45/DB-9, который входит в комплект поставки устройства, к разъёму RJ-45 «Console», расположенному на передней панели устройства. Второй конец кабеля подключите к разъёму порта RS232 компьютера.

Для связи с маршрутизатором следует использовать программу эмуляции терминала, например, HyperTerminal или Minicom. Должен быть использован режим эмуляции терминала VT100.

Параметры интерфейса RS232 на компьютере должны быть следующими: 115200, 8 ,n, 1, без управления потоком данных.

Базовая настройка маршрутизатора

Процедура настройки маршрутизатора при первом включении содержит следующие этапы:

- изменение пароля пользователя «admin».
- создание новых пользователей.
- назначение имени устройства (hostname).
- установка параметров подключения к публичной сети в соответствии с требованиями провайдера.
- настройка удаленного доступа к маршрутизатору.
- применение базовых настроек.

Изменение пароля пользователя «admin»

Для обеспечения защищенного входа в систему необходимо сменить пароль привилегированному пользователю «admin». По умолчанию задан пароль

«password».

Имя пользователя и пароль вводится при входе в систему во время сеансов администрирования устройства. Для изменения пароля пользователя «admin» используются следующие команды:

esr-1000# configureesr-1000(config)#
usernameadminesr-1000(config-user)# password<new-
password>esr-1000(config-user)# exit

Создание новых пользователей

Для создания нового пользователя системы или настройки любого из параметров - имени пользователя, пароля, уровня привилегий, используются команды:

esr-1000(config)# username<name>esr-1000(config-user)# password<password>esr-1000(config-user)# privilege<privilege>esr-1000(config-user)# exit esr-1000(config)#

Уровень привилегий 1 разрешает доступ к устройству, но запрещает настройку.

Уровень привилегий 15 разрешает как доступ, так и настройку устройства.

Пример команд для создания пользователя«fedor»с паролем «12345678» и уровнем привилегий и создания пользователя«ivan» с паролем«password» и уровнем привилегий 1:

esr-1000# configure esr-1000(config)# username fedor esr-1000(config-user)# password 12345678 esr-1000(config-user)# privilege 15 esr-1000(config-user)# exit esr-1000(config)# username ivan esr-1000(config-user)# password password esr-1000(config-user)# privilege 1 esr-1000(config-user)# exit esr-1000(config)#

Назначение имени устройства

Для назначения имени устройства используются следующие команды:

esr-1000# configure

esr-1000(config)# hostname <new-name>

После применения конфигурации приглашение командной строки изменится на <new-name>.

Настройка параметров публичной сети

Для настройки сетевого интерфейса маршрутизатора в публичной сети необходимо назначить устройству параметры, назначенные провайдером сети. В перечень параметров входят IP-адрес, маска подсети и адрес шлюза по умолчанию.

Пример команд настройки статического IP-адреса для субинтерфейса GigabitEthernet 1/0/2.150 для доступа к маршрутизатору через VLAN 150.

Параметры интерфейса:

- IP-адрес, назначаемый для интерфейса GigabitEthernet- 1/0/2.150- 192.168.16.144;
- Маска подсети - 255.255.255.0;
- IP-адрес шлюза по умолчанию - 192.168.16.1.

esr-1000# configure

esr-1000(config)# interface gigabitethernet 1/0/2.150 esr1000(config-subif)# ip address 192.168.16.144/24 esr-1000(config-subif)# exit

esr-1000(config)# iproute0.0.0.0/0 192.168.16.1

Для того чтобы убедиться, что адрес был назначен интерфейсу, введите следующую команду после применения конфигурации:

esr-1000# show ip interfaces Configured IP interfaces:	
IP address I/F name	Type
192.168.16.144/24 gigabitethernet 1/0/2.150	static

Для получения IP-адреса может использоваться протокол DHCP, в случае если в сети присутствует сервер DHCP. IP-адрес от сервера DHCP можно получать через любой интерфейс - физический порт, субинтерфейс.

Пример настройки, предназначенной для получения динамического IP-адреса от DHCP-сервера на интерфейсе GigabitEthernet 1/0/10:

esr-1000# configure

esr-1000(config)# interface gigabitethernet 1/0/10

esr-1000(config-if)# ip address dhcp enable esr-1000(config-if)# exit

Для того чтобы убедиться, что адрес был назначен интерфейсу, введите следующую команду после применения конфигурации:

esr-1000# show ip interfaces Configured IP interfaces:

IP address	I/F name	Type
192.168.11.5/25	gigabitethernet 1/0/10	DHCP

Настройка удаленного доступа к маршрутизатору

Для того чтобы разрешить удаленный доступ к маршрутизатору по протоколам Telnet или SSH, необходимо создать соответствующие правила в firewall. Правила создаются для пары зон:

- source-zone - зона, из которой будет осуществляться удаленный доступ;
- destination-zone - зона self, так как данный трафик предназначен для маршрутизатора.

Для создания разрешающего правила используются следующие команды:

esr-1000# configure

esr-1000(config)# security zone-pair <source-zone> self esr-1000(config-zone-pair)# rule <number> esr-1000(config-zone-rule)# action permit esr-1000(config-zone-rule)# match protocol tcp

esr-1000(config-zone-rule)# match source-address <network object-group> esr-1000(config-zone-rule)# match destination-address <network object-group> esr-1000(config-zone-rule)# match source-port any

esr-1000(config-zone-rule)# match destination-port <service object-group>

esr-1000(config-zone-rule)# enable

esr-1000(config-zone-rule)# exit

esr-1000(config-zone-pair)# exit

esr-1000(config)#

Пример команд для разрешения пользователям из зоны LAN с IP-адресами 192.168.10.10192.168.10.20 подключаться к маршрутизатору с IP-адресом 192.168.10.1 по протоколу SSH:

esr-1000# configure

esr-1000(config)# object-group network clients

esr-1000(config-addr-set)# ip address-range 192.168.10.10-192.168.10.20

esr-1000(config-addr-set)# exit

esr-1000(config)# object-group network gateway

esr-1000(config-addr-set)# ip address-range 192.168.10.1

esr-1000(config-addr-set)# exit

esr-1000(config)# object-group service ssh

esr-1000(config-port-set)# port-range 22

esr-1000(config-port-set)# exit

esr-1000(config)# security zone-pair LAN self

esr-1000(config-zone-pair)# rule 10

esr-1000(config-zone-rule)# action permit

esr-1000(config-zone-rule)# match protocol tcp

esr-1000(config-zone-rule)# match source-address clients

esr-1000(config-zone-rule)# match destination-address gateway

esr-1000(config-zone-rule)# match source-port any

esr-1000(config-zone-rule)# match destination-port ssh

esr-1000(config-zone-rule)# enable

esr-1000(config-zone-rule)# exit

esr-1000(config-zone-pair)# exit

esr-1000(config)#

5.2.2.6 Применение базовых настроек

Для применения выполненных изменений конфигурации маршрутизатора требуется ввести следующие команды из корневого раздела командного интерфейса.

esr-1000# commitesr-1000# confirm

Лабораторная работа № 8

Тема: «Подключение к консоли и настройка маршрутизатора»

Цель работы:изучить процедуруподключения к консоли и настройки маршрутизатора».

Порядок выполнения работы

Крепление кронштейнов

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства. Для установки кронштейнов:

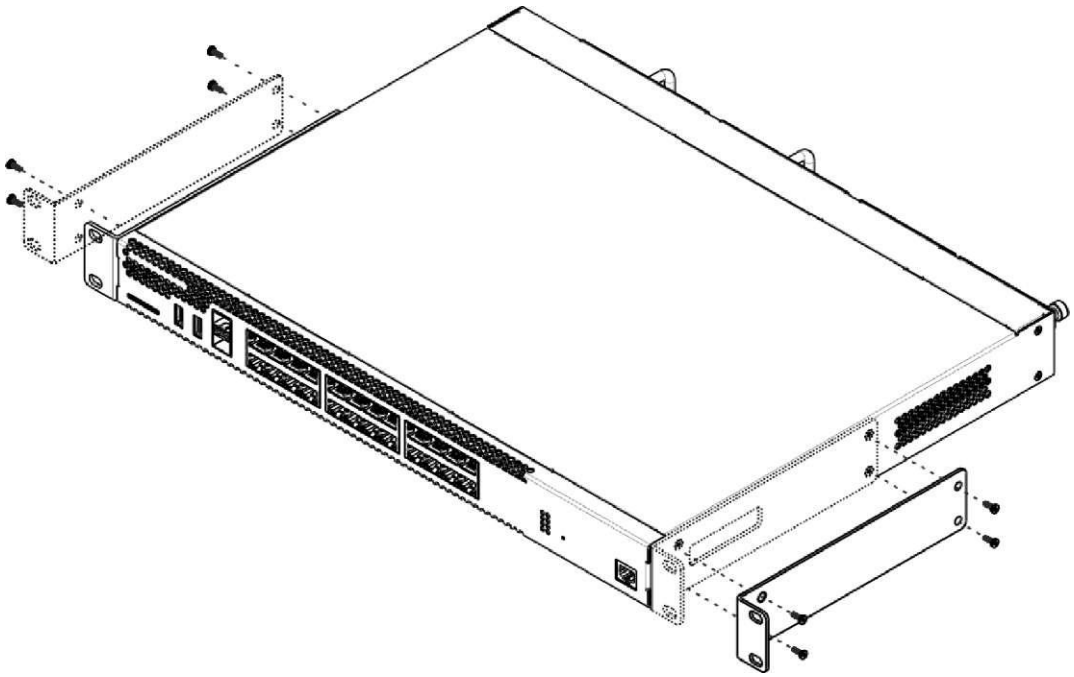


Рисунок 7- Крепление кронштейнов

3.2 Установка устройства в стойку

Для установки устройства в стойку:

1. Приложите устройство к вертикальным направляющим стойки.
2. Совместите отверстия кронштейнов с отверстиями на направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки, для того чтобы устройство располагалось горизонтально.
3. С помощью отвертки прикрепите маршрутизатор к стойке винтами.

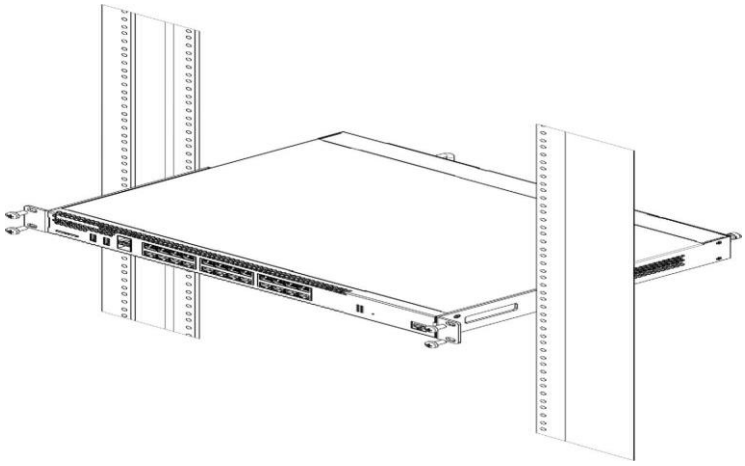


Рисунок 8 - Установка устройства в стойку

3.3 Установка модулей питания

Маршрутизаторможет работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

Места для установки модулей питания с электрической точки зрения равноценны. С точки зрения использования устройства, модуль питания, находящийся ближе к краю, считается основным, ближе к центру - резервным. Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания коммутатор продолжает работу без перезапуска.

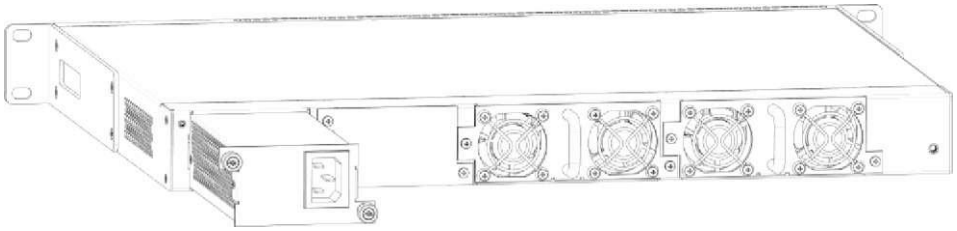


Рисунок 9 - Установка модулей питания

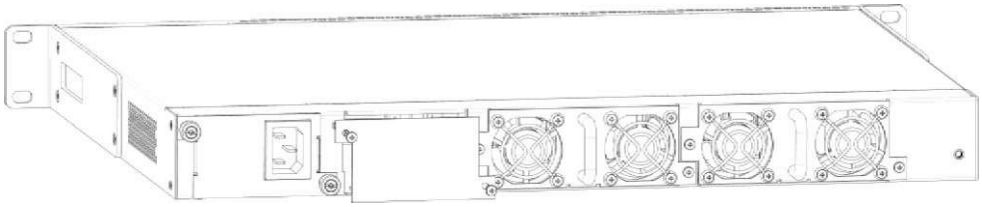


Рисунок 10 - Установка заглушки

Индикация аварии модуля питания может быть вызвана не только отказом модуля, но и отсутствием первичного питания.

Состояние модулей питания может быть проверено по индикации на передней панели коммутатора (см. раздел 2.4.4) или по диагностике, доступной через интерфейсы управления коммутатором.

Подключение питающей сети

Прежде, чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства. Заземление необходимо выполнять изолированным многожильным

проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиями Правил устройства электроустановок (ПУЭ).

Если предполагается подключение компьютера или иного оборудования к консольному порту коммутатора, это оборудование также должно быть надежно заземлено.

Подключите к устройству кабель питания. В зависимости от комплектации устройства, питание может осуществляться от сети переменного тока либо от сети постоянного тока. При подключении сети переменного тока следует использовать кабель, входящий в комплект устройства. Для подключения к сети постоянного тока используйте провод сечением не менее 1 мм^2.

Включите питание устройства и убедитесь в отсутствии аварий по состоянию индикаторов на передней панели.

Маршрутизаторы ESR предназначены для выполнения функцийпограничного шлюза и обеспечения безопасности сети пользователя при подключении ее к публичным сетям передачи данных.

Базовая настройка маршрутизатора должна включать:

назначение IP-адресов (статических или динамических) интерфейсам, участвующим в маршрутизации данных;

создание зон безопасности и распределение интерфейсов по зонам;

создание политик, регулирующих прохождение данных между зон;

настройка сервисов, сопутствующих маршрутизации данных (NAT, Firewall и прочие).

Расширенные настройки зависят от требований конкретной схемы применения устройства и легко могут быть добавлены или изменены с помощью имеющихся интерфейсов управления.

Подключение к маршрутизатору

Предусмотрены следующие способы подключения к устройству:

1. Подключение по локальной сети Ethernet.

При первоначальном старте маршрутизатор загружается с заводской конфигурацией.

Для первоначального сетевого подключения к устройству рекомендуется использовать интерфейс GigabitEthernet 1/0/2, на котором в заводской конфигурации задан статический IP-адрес.

Подключите сетевой кабель к порту GigabitEthernet 1/0/2 (порт 2 на передней панели устройства) и к компьютеру, предназначенному для управления.

В заводской конфигурации маршрутизатора активированDHCP-сервер с пулом IP-адресов в подсети 192.168.1.0/24. При подключении сетевого интерфейса управляющего
компьютера он должен получить сетевой адрес от сервера.

Если IP-адрес не получен по какой-либо причине, то следует назначить адрес интерфейса вручную, используя любой адрес, кроме 192.168.1.1, в подсети 192.168.1.0/24.

2. Подключение через консольный порт RS232.

Подключите кабель RJ-45/DB-9, который входит в комплект поставки устройства, к разъёму RJ-45 «Console», расположенному на передней панели устройства. Второй конец кабеля подключите к разъёму порта RS232 компьютера.

Для связи с маршрутизатором следует использовать программу эмуляции терминала, например, HyperTerminal или Minicom. Должен быть использован режим эмуляции терминала VT100.

Параметры интерфейса RS232 на компьютере должны быть следующими:
115200, 8 ,n, 1, без управления потоком данных.

Базовая настройка маршрутизатора

Процедура настройки маршрутизатора при первом включении содержит следующие этапы:

Изменение пароля пользователя «admin».

Создание новых пользователей.

Назначение имени устройства (Hostname).

Установка параметров подключения к публичной сети в соответствии с требованиями провайдера.

Настройка удаленного доступа к маршрутизатору.

Применение базовых настроек.

Изменение пароля пользователя «admin»

Для обеспечения защищенного входа в систему необходимо сменить пароль привилегированному пользователю «admin». По умолчанию задан пароль «password».

Имя пользователя и пароль вводится при входе в систему во время сеансов администрирования устройства. Для изменения пароля пользователя «admin» используются следующие команды:

esr-1000# configureesr-1000(config)# usernameadminesr-1000(config-user)# password<*new-password*>esr-1000(config-user)# exit

Лабораторная работа № 9

Тема: «Введение в списки контроля доступа»
Цель работы:изучить процедурувведения в списки контроля доступа
Порядок выполнения работы

Введение в списки контроля доступа

Сетевой администратор должен уметь запрещать несанкционированный доступ к сети и в то же время обязан обеспечить доступ к сети авторизированных пользователей. Несмотря на то, что средства безопасности, такие, как пароли, средства установления обратного вызова и физические устройства безопасности, достаточно полезны, им часто не хватает гибкости при фильтрации потока данных и специализированных управляющих средств, которые чаще всего предпочитают администраторы. Например, бывают ситуации, когда сетевой администратор готов предоставить пользователям локальной сети выход в сеть Internet, но при этом не хочет разрешать пользователям сети Internet, находящимся вне такой локальной сети, входить в сеть предприятия средствами протокола telnet.

Следует помнить, что списки контроля доступа интенсивно используют ресурсы центрального процессора маршрутизатора. При использовании списков доступа каждый поступающий на устройство пакет должен быть обработан центральным процессором.

Маршрутизаторы предоставляют администраторам основные возможности фильтрации, такие, как блокирование потока данных из сети Internetс использованием списков контроля доступа (AccessControlList- ACL). Список контроля доступа представляет собой последовательный набор разрешающих или запрещающих директив, которые относятся к адресам или протоколам верхнего уровня.

Правила списка ACL, которые принадлежат одному и тому же списку контроля доступа, всегда содержат один и тот же номер списка:

- список контроля доступа 1
- правило списка ACL 1,
- правило списка ACL 1,
- правило списка ACL 1,
- правило списка ACL 1;
- список контроля доступа 2
- правило списка ACL 2,
- правило списка ACL 2,
- правило списка ACL 2,
- правило списка ACL 2,
- правило списка ACL 2;
- список контроля доступа 3
- правило списка ACL3,
- правило списка ACL 3,
- правило списка ACL 3.

В приведенной структуре списков ACLправило, номер которого совпадает с номером списка, относится к определенному нумерованному списку. Сами правила выполняются в процессе отработки списка последовательно.

Администратору и техническому специалисту необходимо уметь правильно конфигурировать списки контроля доступа и знать, где их следует разместить в сети.

Основные функции списков контроля доступа включают в себя:

- фильтрацию внутренних пакетов;
- защиту внутренней сети от несанкционированного доступа;
- ограничение доступа к портам виртуального терминала.

Списки ACLпредставляют собой набор инструкций применяемых к интерфейсу маршрутизатора. Они указывают маршрутизатору, какие пакеты следует принять, а какие - отбросить. Решение о том, как поступить пакетом, может быть основано на определенных критериях, таких, как адреса отправителя и получателя или номер TCP/UDPпорта.

Списки контроля доступа позволяют администратору управлять потоками данных и сканировать определенные пакеты. Любые потоки данных, которые проходят через интерфейс маршрутизатора, проверяются на соответствие условиям списка.

Списки контроля доступа могут быть созданы для всех маршрутизируемых сетевых протоколов, например, IPили IPXс целью фильтрации пакетов по мере их поступления на маршрутизатор. Для списков ACLможет быть установлена конфигурация, позволяющая управлять доступом к сети или подсети.

Алгоритм списков контроля доступа при фильтрации потока данных принимает решение о том, направить пакет далее или заблокировать его на интерфейсе. Каждый пакет исследуется на соответствие условиям, которые указаны в списке; в качестве условий могут выступать адреса отправителя и получателя, идентификатор протокола верхнего уровня или другая информация.

Список ACLдолжен составляться для каждого отдельного протокола. Иными словами, для каждого используемого на интерфейсе маршрутизатора протокола должен быть составлен список, который будет регулировать трафик именно на этом интерфейсе. Например, если интерфейс маршрутизатора используется для передачи IP, AppleTalkи IPXтрафика, то необходимо будет сконфигурировать, по меньшей мере, три списка контроля доступа.

Списки могут быть использованы в качестве гибкого средства фильтрации пакетов, поступающих на интерфейс маршрутизатора или отправляемых с него (Рисунок 3.1).

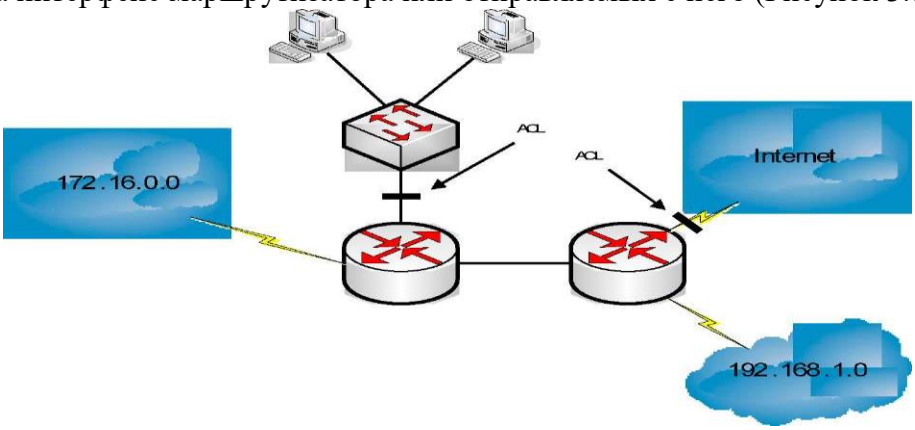


Рисунок 3.1 - Применение списков ACL

Для создания списков доступа существует множество причин:

- Списки ACLможно использовать для ограничения потока данных в сети и повышения ее производительности. В частности, списки могут быть использованы для того, чтобы некоторые пакеты какого-либо протокола обрабатывались маршрутизатором ранее других. Такая функция называется установкой очередности и используется для того, чтобы маршрутизатор не обрабатывал пакеты, которые в данный момент не являются жизненно необходимыми. Установка пакетов в очередь ограничивает поток данных в сети и уменьшает вероятность перегрузки.

- Списки ACLможно использовать для управления потоком данных. Например, с помощью списков можно ограничить или уменьшить количество сообщений об изменениях в сети. Такие ограничения используются для предотвращения распространения информации об отдельных сетях на всю сеть.

- Списки ACLможно использовать для обеспечения базового уровня защиты от несанкционированного доступа. Например, списки доступа позволяют разрешить одному узлу доступ к некоторому сегменту сети, а другому закрыть доступ к этой же области. Если на маршрутизатор не установлен список контроля доступа, то все пакеты, проходящие через него, поступают во все сегменты сети.

- Списки ACLможно использовать для указания данных, которые будут направляться далее или блокироваться на интерфейсе маршрутизатора. Например, можно разрешить маршрутизацию трафика электронной почты и в то же время заблокировать весь поток данных протокола telnet.

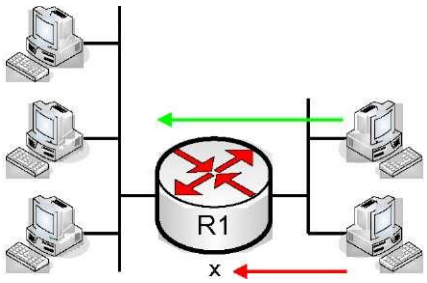


Рисунок 3.2 - Обработка пакетов списком ACL

Принимая решение о дальнейшей отправке пакета или его блокировке, ОС CiscoIOSпроверяет его соответствие всем директивам в том порядке, в каком они записаны. Как показано на рисунке 3.2 пакеты последовательно проверяются на соответствие записям до тех пор, пока не будет найдено соответствие одному из правил. Если такое соответствие обнаружено, то остальные директивы списка не рассматриваются, и к пакету применяется указанное в списке действие. Например, если было указано правило, которое разрешает передачу всех данных, то все последующие директивы не проверяются. Если требуется внести дополнительные директивы, то нужно удалить весь список и заново создать его с новыми записями. Поэтому при изменении списков доступа целесообразнее всего отредактировать конфигурацию маршрутизатора с помощью текстового редактора, а затем переслать ее на устройство посредством TFTPили встроенной возможностью терминальной программы.

Каждая добавленная запись заносится в конец списка. Таким образом, невозможно удалить в нумерованном списке отдельные директивы после того, как они были созданы, а можно удалить только весь список полностью. ОС CiscoIOSпроверяет пакет и заголовки верхних уровней для списков доступа как показано на рисунке 3.3.

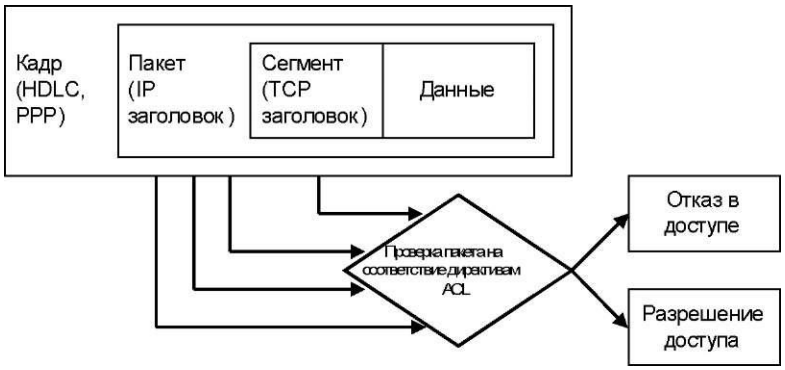


Рисунок 3.3 - Последовательная проверка заголовка пакета списком ACL

Принцип работы списков ACL

Список контроля доступа представляет собой набор директив, которые определяют то, как пакеты:

- поступают на входной интерфейс маршрутизатора,
- доставляются внутри маршрутизатора,
- пересылаются далее через выходной интерфейс маршрутизатора.

Начальная стадия процесса установления связи не зависит от того, используются ли списки контроля доступа или нет.

Когда пакет поступает на интерфейс, маршрутизатор определяет, куда его направить. Если пакет по какой-либо причине не может быть обработан маршрутизатором или мостом, он отбрасывается. Далее операционная система проверяет, связан ли со входным интерфейсом какой-либо список доступа. Если список есть, то операционная система сверяет параметры пакета с записями такого списка ACL. Если пакет соответствует разрешающему правилу и подвергается маршрутизации, то в таблице маршрутизации выполняется поиск сети получателя, определяется метрика маршрут или состояние и интерфейс, через который следует отправить пакет. Список контроля доступа не фильтрует пакеты, которые возникают внутри маршрутизатора, но фильтрует пакеты из иных источников.

Далее маршрутизатор проверяет, находится ли интерфейс получателя в группе списка контроля доступа. Если его там нет, то пакет может быть направлен на интерфейс получателя.

Директивы списка исполняются в последовательном порядке. Если заголовок пакета соответствует директиве списка, то остальные директивы пропускаются. Если условие директивы выполнено, пакет передается далее или отбрасывается в соответствии с конфигурацией. Если заголовок пакета не соответствует ни одной директиве списка, то к нему применяется стандартное правило, размещенное конце списка, которое запрещает передачу любых пакетов. Такая директива не отображается в последней строке списка контроля доступа, она стандартно там присутствует. Если пакет не соответствует условию первой директивы, он проверяется на соответствие второй директиве из списка контроля доступа, и т.д. Алгоритм обработки пакетов списком ACLпредставлен на рисунке 3.4.

Списки ACLпозволяют контролировать, каким пользователям разрешен доступ к конкретной сети. Условия в списке контроля доступа позволяют:

- просмотреть адреса определенных узлов для того, чтобы разрешить или заблокировать им доступ к некоторой части сети;

разрешить или запретить доступ пользователям только к определенным видам приложений, таким, как службы FTPи HTTP

Лабораторная работа № 10

Тема: «Конфигурирование и проверка работы NAT»

Цель работы:изучить процедуру настройки коммутатора и подключения к коммутатору.

Порядок выполнения работы

Конфигурирование NAT

Конфигурирование статического преобразования адресов

Для конфигурирования службы статического NAT необходимо выполнить следующие шаги:

Шаг 1. В качестве подготовительного этапа на маршрутизаторе сконфигурировать IP маршрутизацию и указать соответствующие IP адреса.

Шаг 2. Если используется механизм статического преобразования для внутренних локальных адресов, то следует указать необходимые адреса, используя команду ipnatinsidesourcestatic в режиме глобального конфигурирования. Для удаления записи статического преобразования используется форма данной команды с ключевым словом no перед ней.

Шаг 3. Войти в режим конфигурирования интерфейса и включить преобразование с помощью службы NAT, по крайней мере, на одном внутреннем и на одном внешнем интерфейсах посредством ввода команды ipnat {inside | outside}.

Параметры команды ipnatinsidesourcestatic приведены в таблице 4.2.

Таблица 4.2 - Параметрыкоманды ip nat inside source static

Параметр	Описание
local-ip	Задает отдельную запись статического преобразования. Задает локальный IP адрес, назначенный узлу во внутренней сети. Такой адрес должен соответствовать стандарту RFC 1918
global-ip	Задает отдельную запись статического преобразования. Задает глобальный уникальный IP адрес внутреннего узла в том виде, как он выглядит для внешней сети

В примере приводится пример настройки статическогоNAT. Соответствующая ей топология сети представлена на рисунке 4.8

Настройка статического преобразования адресов

!
ip nat inside source static 10.1.1.1 192.168.2.2 !
interface Ethernet 0
ip address 10.1.1.10 255.255.255.0
ip nat inside !
interface Serial O
ip address 172.16.2.1 255.255.255.0 ip nat outside !
Внешняя сеть

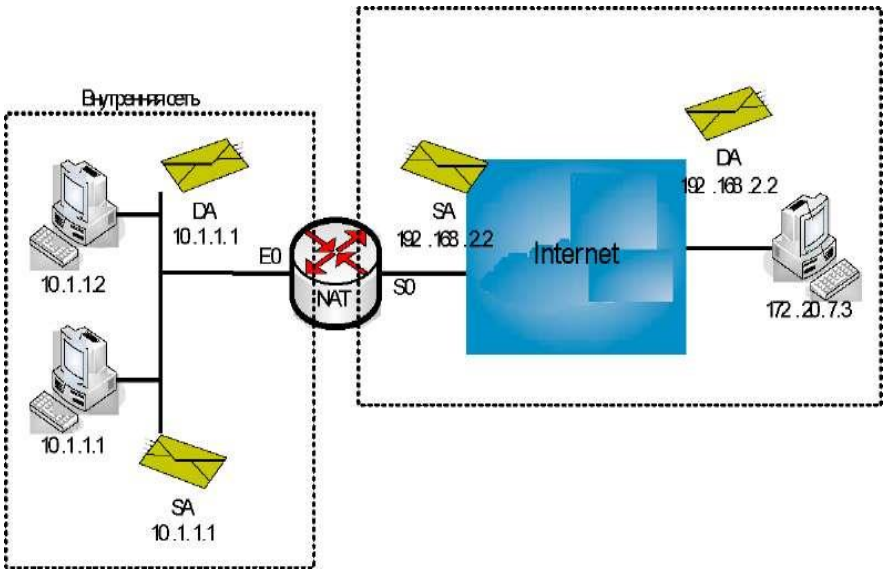


Рисунок 4.8 - Статическое преобразование адресов

Конфигурирование динамического преобразования адресов

Для включения службы динамического преобразования IP-адресов необходимо выполнить следующее шаги.

Шаг 1. В качестве подготовительного этапа сконфигурировать на маршрутизаторе IP маршрутизацию и указать соответствующие IP адреса.

Шаг 2. Далее необходимо задать стандартный IP список доступа с помощью команды access-list.

Шаг 3. Указать пул адресов для службы NAT протокола IP с помощью команды ipnatpool*pool-name*start-ipend-ip {netmask*netmask* | prefix-length*prefix-length*] [typerotary].Параметры которой описаны в таблице 4.3.

Шаг 4. Выполнить привязку списка доступа к пулу службы NAT с помощью команды ipnatinsidesourcelist*access-listnumberpool-name.*

Шаг 5. Включить службу NAT, по крайней мере, на одном внутреннем и на одном внешнем интерфейсе с помощью команды ipnat {inside | outside}.

Таблица 4.3 - Параметры команды ipnatpool

Параметр	Описание
pool-name	Имя пула.
start-ip	Начальный IP адрес выделенного диапазона адресов пула.
end-ip	Заключительный IP адрес выделенного диапазона адресов пула.
netmask	Маска сети для адресов пула.
prefix-length	Префикс сети.
type rotary	Диапазон адресов в пуле описывает реальные внутренние узлы, между которыми будет происходить распределение нагрузки по протоколу TCP.

Транслироваться будут только пакеты, перемещающиеся между внутренними и внешними интерфейсами. Например, если пакет получен на внутреннем интерфейсе и не направляется во внешний интерфейс, то его адрес не будет преобразован.

В примере 4.2 приводится пример настройки динамическогоNAT.

-Настройка динамического преобразования адресов

ipnatpooldyn-nat 192.168.2.1 192.168.2.254 netmask 255.255.255.0 ipnatinsidesourcelist 1 pooldyn-nat !
interface Ethernet 0
ip address 10.1.1.10 255.255.255.0

```
ip nat inside !
interface Serial 0
ip address 172.16.2.1 255.255.255.0
ip nat outside !
access-list 1 permit 10.1.1.0 0.0.0.255 !
```

Конфигурирование перегрузки внутренних глобальных адресов

Для того чтобы сконфигурировать перегрузку внутренних глобальных адресов, необходимо выполнить следующее:

Шаг 1. В качестве подготовительного этапа сконфигурировать на маршрутизаторе IP-маршрутизацию и указать соответствующиеIP-адреса.

Шаг 2. Сконфигурировать службу динамического преобразования адресов.

Шаг 3. После того, как сконфигурирован список доступа для пула адресов службы NAT необходимо ввести команду ipnatinsidesourcelist*access- listnumberpoolname*overload.

Шаг 4. Далее необходимо включить службу NAT на соответствующих интерфейсах с помощью команды ipnat {inside | outside}.

В примере приведена конфигурация механизма перегрузки адресов. Соответствующая ей топология сети представлена на рисунке 4.9.

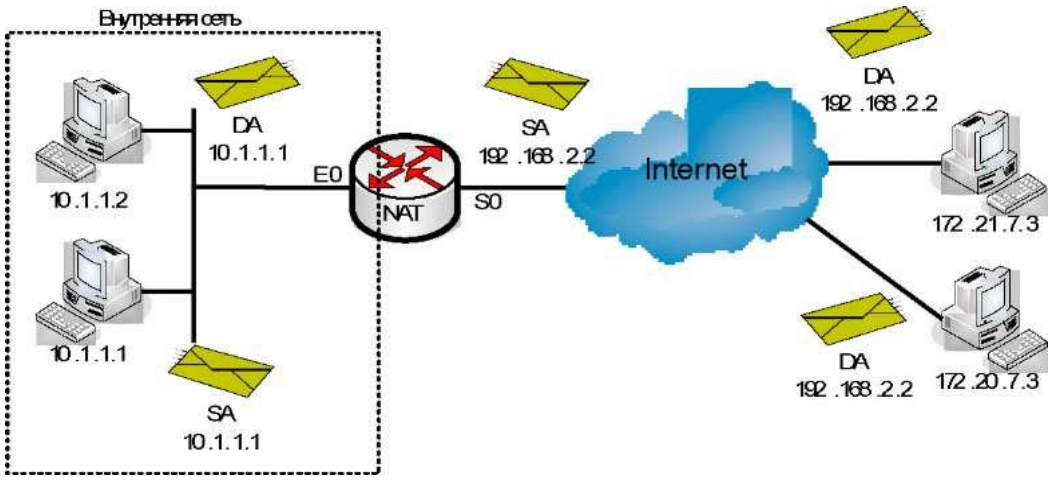


Рисунок 4.9 - Перегрузка нагрузки

Тема 2.2Оборудование абонентского доступа.

Лабораторная работа № 1

Тема: «Алгоритм линейного кодирования»
Цель работы:изучитьалгоритм линейного кодирования.
Порядок выполнения работы

Алгоритм линейного кодирования в системах ADSL

Специфическая особенность ADSL - это использование модуляции 256DMT, о чем необходимо сказать подробнее. Метод передачи информации, разработанный для ADSL, состоит в том, что для передачи сигналов используются 256 несущих. Это означает, что в канале передачи работают 256 мини-модемов, каждый из которых передает информацию на своей несущей. Применение такой методики позволяет повысить эффективность использования ресурса за счет компенсации любых селективных шумовых влияний на параметры передачи. Между несущими устанавливается защитный интервал 4312,5 Гц. Часть несущих отдается под передачу данных по линии вверх, часть - для передачи по линии вниз). Передача данных на несущей осуществляется посредством амплитудно-фазовой модуляции (Quadrature Amplitude Modulation, QAM).

Объем передаваемой информации на отдельной несущей зависит от соотношения сигнал/шум на данной частоте. Если на несущей соотношение сигнал/шум оказывается небольшим, то количество бит/с на ней устанавливается меньшим. В результате распределение скорости передачи по частоте в абонентской паре повторяет зависимость отношения сигнал/шум от частоты. В качестве примера функционирования единого алгоритма передачи256DMT/QAM представлен вариант абонентской линии, в которой присутствует неравномерность амплитудно-частотной характеристики (АЧХ) и селективная помеха. В результате профиль уровней передачи сигнала ADSL повторяет профиль АЧХ, селективная помеха воздействует не на весь сигнал ADSL, а только на одну или несколько несущих. Двухшаговый алгоритм 256DMT/QAM адаптирует передачу цифрового потока к любым параметрам абонентской пары.

Факторы, влияющие на параметры качества ADSL

Можно выделить две группы факторов влияющих на параметры качества ADSL:

- влияние параметров абонентской кабельной пары,
- влияние со стороны пары модем-DSLAM.

Выше мы уже говорили об адаптации технологии ADSL к любым параметрам распределения шумов в диапазоне передачи. Использование модуляции 256DMT позволяет устанавливать на каждой несущей определенный уровень передачи в зависимости от отношения сигнал/шум (SNR) на несущей. Технология ADSL в этом смысле является адаптивной и подстраивается под любые параметры существующей абонентской линии.

Следует отметить, что алгоритм 256DMT сочетается с алгоритмом QAM. Происходит это в следующем порядке:

- В процессе настройки параметров передачи/приема наотдельной несущей устанавливается уровень передачи сигнала в 256 DMT.
- После определения уровня передачи сигнала на каждой несущей определяется допустимый для данного уровня SNR алгоритм модуляции QAM. За счет этого регулируется уровень помехозащищенности передачи и допустимой скорости передачи на несущей.

В качестве примера функционирования единого алгоритма передачи 256DMT/QAM на рис.1 представлен вариант абонентской линии, в которой присутствует неравномерность амплитудно-частотной характеристики (АЧХ) и селективная помеха.

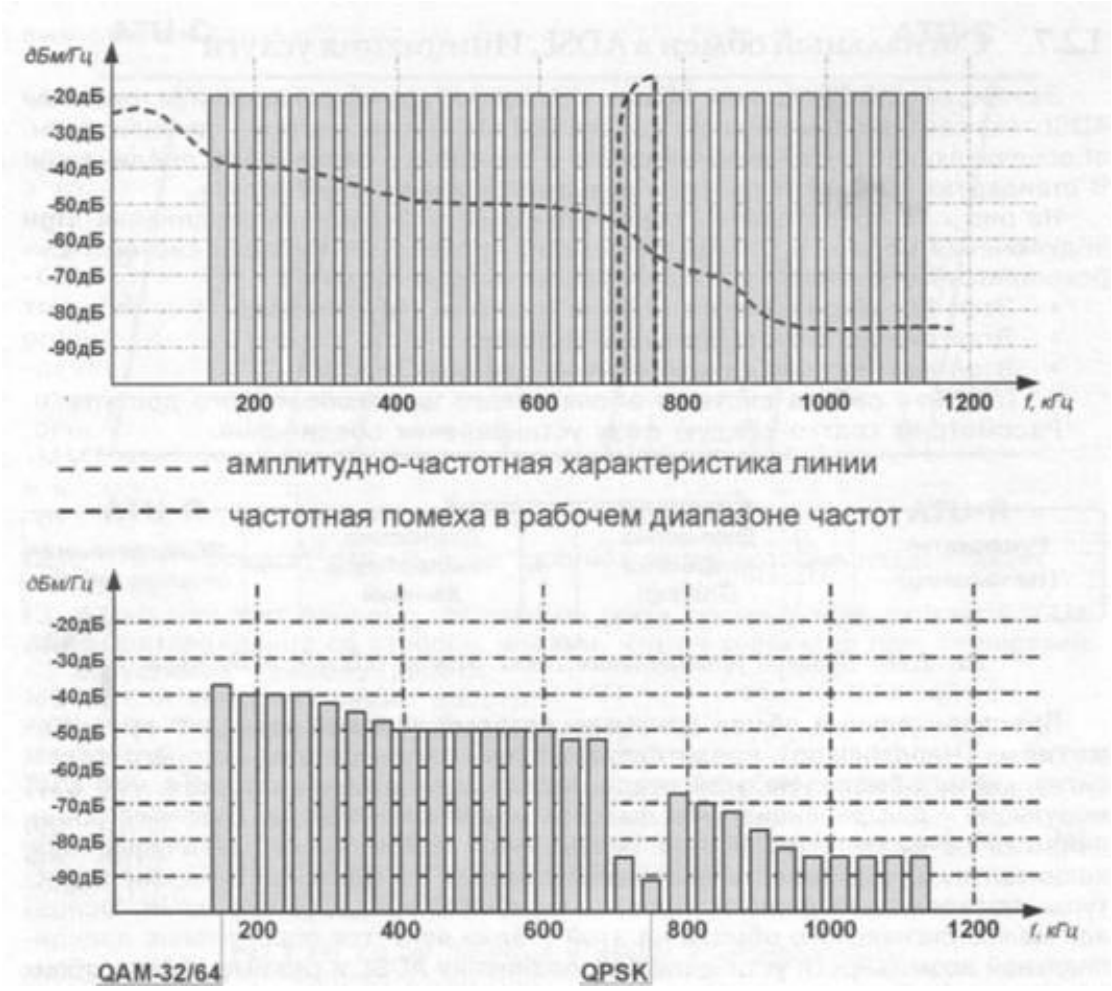


Рис.1. Влияние шумов на распределение уровней передачи по отдельным тонам

Внизу на рис. 1 показано поведение пары модем-DSLAM для указанной линии. Неравномерность АЧХ приводит к тому, что уровни передачи сигнала в ADSL подстраиваются в соответствии с допустимыми уровнями передачи в кабеле. В результате профиль уровней передачи сигнала ADSL повторяет профиль АЧХ.

Наличие селективной помехи в определенном диапазоне частот делает передачу на нескольких несущих весьма затруднительной. В процессе адаптации алгоритма 256DMT для данных несущих устанавливается небольшой уровень сигнала. Одновременно для этих несущих выбирается более помехозащищенная модуляция QPSK. В результате скорость передачи информации на «поврежденных» несущих будет минимальной, но все равно успешной.

Таким образом, в ADSL нельзя говорить о двух технологиях модуляции сигнала. Существует единый двухшаговый алгоритм 256DMT/QAM, адаптирующий передачу цифрового потока к любым параметрам абонентской пары.

Сигнальный обмен в ADSL. Инициация услуги

Завершая рассмотрение общих принципов функционирования системы ADSL, укажем на применение в канале DSLAM-модем системы сигнализации, обеспечивающей установление связи и настройку параметров соединения. В стандартах ADSL этот процесс называется инициацией услуги.

На рис.2 представлены основные фазы установления соединения. При подключении модема к DSLAM происходит процесс активизации системы широкополосного доступа через следующие четыре стадии.

- Этап предварительного обмена данными («рукопожатие»).
- Этап диагностики соединения (training).
- Этап диагностики канала обмена данными.
- Штатная работа системы абонентского широкополосного доступа.

Рассмотрим кратко каждую фазу установления соединения.

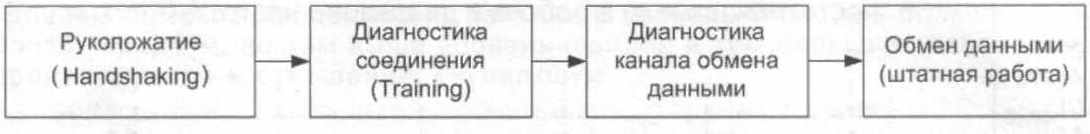


Рис. 2.. Процесс установления связи между DSLAM и модемом

Предварительный обмен данными, который условно называют «рукопожатием» (Handshaking), представляет собой начальную стадию подготовки к сигнальному обмену.

На этой стадии используется более простая, чем DMT модуляция - дифференциальная фазовая модуляция DPSK, за счет чего обмен данными на физическом уровне оказывается максимально устойчивым. Дополнительную устойчивость дает использование специальной цикловой структуры, позволяющей диагностировать ошибки в процессе передачи. Основной целью сигнального обмена на этой стадии является определение принципиальной возможности установления соединения ADSL и режима работы обоих устройств.

Лабораторная работа № 2

Тема: «Построение различных топологий беспроводных сетей»
Цель работы:изучить построение различных топологий беспроводных сетей.
Порядок выполнения работы

Беспроводная технология WIMAX

WiMAX - семейство стандартов IEEE 802.16 - это радиотехнология, которая обеспечивает двусторонний доступ к Интернету на дальнем расстоянии со скоростями до75 Мбит/с, а также QoS [6].

WiMAX - Worldwide Interoperability for Microwave Access, стандартизированная институтом IEEE технология широкополосной беспроводной связи, дополняющая линии DSL и кабельные технологии в качестве альтернативного решения проблемы "последней мили" на больших расстояниях. Технологию WiMAX можно использовать для реализации широкополосных соединений "последней мили", развертывания точек беспроводного доступа, организации высокоскоростной связи между филиалами компаний и решения других подобных задач.

Базовая станция (БС, BS — Base Station) размещается в здании или на вышке и осуществляет связь с абонентскими станциями (АС, SS —Subscriber Station) по схеме —точка – мультиточка (Point to Multipoint —PMP). Возможен сеточный режим связи (Mesh — сетка связей —точка – точка — PTP), когда любые клиенты (АС) могут осуществлять связь между собой непосредственно, а антенные системы, как правило, являются ненаправленными. БС предоставляет соединение с основной сетью и радиоканалы к другим станциям. Радиус действия БС может достигать 30 км (в случае прямой видимости) при типовом радиусе сети 6–8 км. АС может быть радиотерминалом или повторителем, который используется для организации локального трафика. Трафик может проходить через несколько повторителей, прежде чем достигнет клиента. Антенны в этом случае являются направленными.

Канал связи предполагает наличие двух направлений передачи: восходящий канал (АС – БС, uplink) и нисходящий (БС – АС, downlink). Эти два канала используют разные неперекрывающиеся частотные диапазоны при частотном дуплексе и различные интервалы времени при временном дуплексе.

Простейший способ представления архитектуры сетей WiMAX заключается в их описании как совокупности БС, которые располагаются на крышах высотных зданий или вышках, и клиентских приемо-передатчиков (см. рисунок 5.1).

Радиосеть обмена данными между БС и АС работает в СВЧ-диапазоне от 2 до 11 ГГц. Такая сеть в идеальных условиях может обеспечить техническую скорость передачи информации до 75 Мбит/с и не требует того, чтобы БС находилась на расстоянии прямой видимости от пользователя.

Рисунок 5.1 – Схематичное изображение сети WiMAX

Диапазон частот от 10 до 66 ГГц используется для установления соединения между соседними базовыми станциями при условии, что они располагаются в зоне прямой видимости друг от друга. Так как в городской среде это условие может оказаться невыполнимым, связь между базовыми станциями иногда организуют посредством прокладки кабелей.

При более детальном рассмотрении сеть WiMAX можно описать как совокупность беспроводного и базового (опорного) сегментов. Первый описывается в стандарте IEEE 802.16, второй определяется спецификациями WiMAX Forum. Базовый сегмент объединяет все аспекты, не относящиеся к абонентской радиосети, т. е. связь базовых станций друг с другом, связь с локальными сетями (в том числе, интернетом) и т. п. Базовый сегмент основывается на IP-протоколе и стандарте IEEE 802.3-2005 (Ethernet). Однако само описание архитектуры в части, не относящейся к беспроводной клиентской сети, содержится в документах WiMAX Forum, объединенных под общим названием – "Network Architecture".

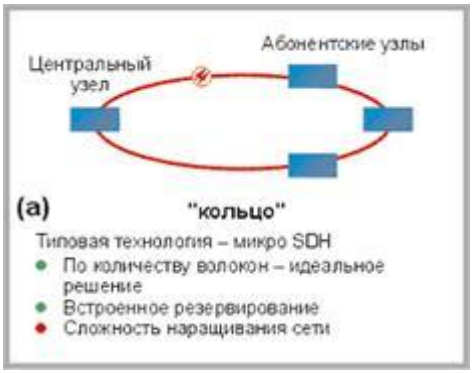
В этих спецификациях к сетям WiMAX предъявляются такие требования, как независимость архитектуры от функций и структуры транспортной IP-сети. В то же время, должны обеспечиваться услуги, основанные на применении IP-протокола (SMS over IP, MMS, WAP и др.), а также мобильная телефония на основе VoIP и мультимедийные услуги. Обязательным является условие поддержки архитектурой протоколов IPv4 и IPv6. Сети WiMAX должны быть легко масштабируемыми и гибко изменяемыми и основываться на принципе декомпозиции (строиться на основе стандартных логических модулей, объединяемых через стандартные интерфейсы). Свойства масштабируемости и гибкости необходимо обеспечивать по таким эксплуатационным характеристикам, как плотность абонентов, географическая протяженность зоны покрытия, частотные диапазоны, топология сети, мобильность абонентов. Сети WiMAX должны поддерживать взаимодействие с другими беспроводными (3GPP, 3GPP2) или проводными (DSL) сетями. Большое значение имеет способность обеспечивать различные уровни качества обслуживания QoS.

Режимы WiMAX

–FixedWiMAX–фиксированный доступ. –NomadicWiMAX– сеансовый доступ. –PortableWiMAX– доступ в режиме перемещения.

Топологии сетей оптического доступа:

1) "Кольцо" - кольцевая топология на основе SDH применяется в сетях доступа, но в сетях доступа нельзя заранее знать где, когда и сколько абонентских узлов будет установлено (см. рисунок 7.2) [2, 9]. При случайном территориальном и временном подключении пользователей кольцевая топология может превратится в сильно изломанное кольцо со множеством ответвлений, подключение новых абонентов осуществляется путем разрыва кольца и вставки дополнительных сегментов. На практике часто такие петли совмещаются в одном кабеле, что приводит к появлению колец, похожих больше на ломаную – “сжатых” колец (collapsedrings), что значительно снижает надежность сети.



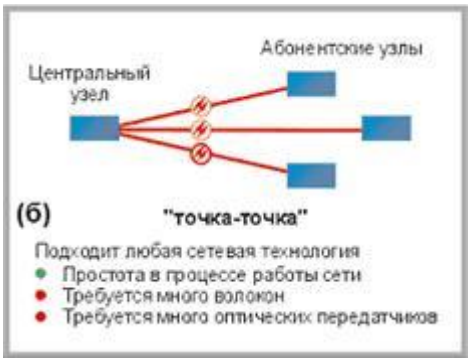
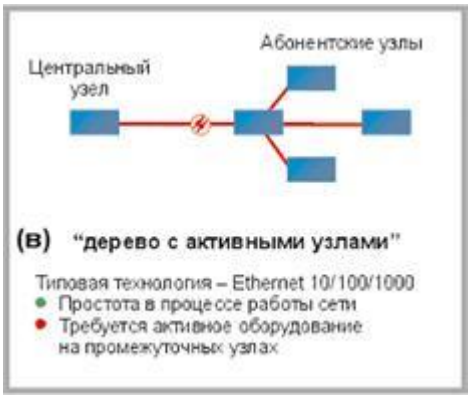


Рисунок 7.2 – Топология "Кольцо" Рисунок 7.3 – Топология "Точка-точка"

2)"Точка-точка" (P2P) - топология P2P не накладывает ограничения на используемую сетевую технологию (см. рисунок 7.3). P2P может быть реализована как для любого сетевого стандарта, так и для нестандартных (proprietary) решений, например, использующих оптические модемы. С точки зрения безопасности и защиты передаваемой информации, при соединении P2P обеспечивается максимальная защищенность абонентских узлов. Поскольку оптический кабель нужно прокладывать индивидуально до абонента, этот подход является наиболее дорогим и привлекателен в основном для крупных абонентов.

3) "Дерево с активными узлами" – это экономичное с точки зрения

использования волокна решение (см. рисунок 7.4). Это решение хорошо вписывается в рамки стандарта Ethernet с иерархией по скоростям от центрального узла к абонентам 1000/100/10 Мбит/с (1000Base-LX, 100Base-FX, 10Base-FL). Однако в каждом узле дерева обязательно должно находиться активное устройство (применительно к IP-сетям, коммутатор или маршрутизатор). Оптические сети доступа Ethernet, преимущественно использующие данную топологию, относительно недороги. К основному недостатку следует отнести наличие на промежуточных узлах активных устройств, требующих индивидуального питания.



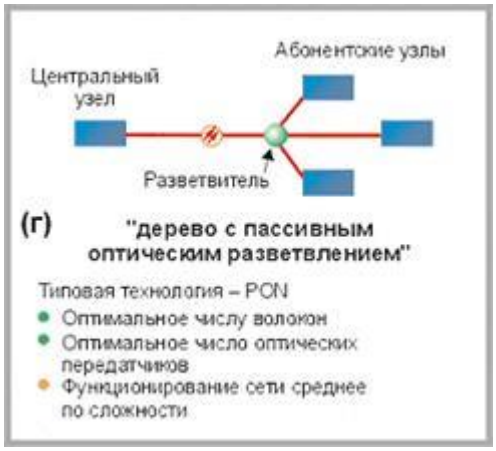


Рисунок 7.4 – Топология "Дерево с активными узлами"

Рисунок 7.5 – Топология "Дерево с пассивными узлами"

4) "Дерево с пассивным оптическим разветвлением PON (P2MP)" - решения на основе архитектуры PON используют логическую топологии "точка-многоточка" P2MP (point-to-multipoint) , которая положена в основу технологии PON, к одному порту центрального узла можно подключать целый волоконно-оптический сегмент древовидной архитектуры, охватывающий десятки абонентов (см. рисунок 7.5). При этом в промежуточных узлах дерева устанавливаются компактные, полностью пассивные оптические разветвители (сплиттеры), не требующие питания и обслуживания.

PON позволяет экономить на кабельной инфраструктуре, за счет сокращения суммарной протяженности оптических волокон, т.к. на участке от центрального узла до разветвителя используется всего одно волокно. В меньшей степени обращают внимание на другой источник экономии – сокращение числа оптических передатчиков и приемников в центральном узле. Между тем экономия о второго фактора в некоторых случаях оказывается даже более существенной.

Лабораторная работа № 3

Тема: «Распределение зон обслуживания беспроводных сетей»
Цель работы:изучить процедуру распределения зон обслуживания беспроводных сетей.
Порядок выполнения работы

Топология

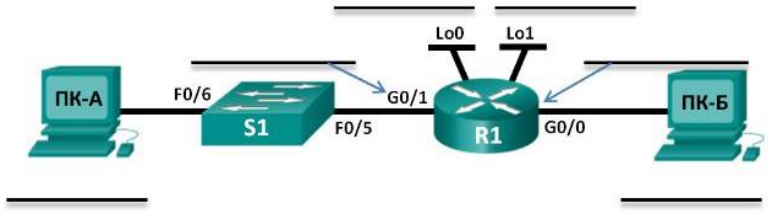


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.224	Недоступно
	G0/1	192.168.0.33	255.255.255.224	Недоступно
	Lo0	192.168.0.65	255.255.255.224	Недоступно
S1	Lo1 VLAN 1	192.168.0.97 Недоступно	255.255.255.224 255.255.255.224 Недоступно	Недоступно 192.168.0.33 Недоступно
ПК-А	Сетевой адаптер	. . .34 192.168.0.2	255.255.255.224	192.168.0.1
ПК-Б	Сетевой адаптер			

Задачи
Часть 1. Разработка схемы распределения зон обслуживания
•Создайте схему разделения на подсети, которая соответствует количеству подсетей и адресов узлов.
•Заполните диаграмму, указав, где будут применяться IP-адреса узлов.
Часть 2. Настройка устройств
•Назначьте компьютерам IP-адреса, маски подсети и шлюзы по умолчанию.

•Настройте IP-адреса и маски подсети для интерфейсов Gigabit Ethernet маршрутизатора.
•На маршрутизаторе создайте два логических интерфейса loopback и настройте для каждого из них IP-адрес и маску подсети.

Часть 3. Проверка сети и устранение неполадок

•Проверьте подключение и устраните неполадки, используя команду ping.

Исходные данные/сценарий

В этой лабораторной работе вам нужно будет разделить сеть, начиная с адреса и маски одной сети, на несколько подсетей. При создании схемы подсети необходимо учитывать количество компьютеров каждой подсети и другие аспекты, например дальнейшее расширение узлов в сети. После того как вы составите схему разделения на подсети и диаграмму сети и укажете IP-адреса узлов и интерфейсов, вам нужно будет настроить компьютеры и интерфейсы маршрутизаторов, включая логические интерфейсы loopback. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей, подключённых к маршрутизатору R1.

После того как сетевые устройства и компьютеры будут настроены, вы проверите сетевые подключения с помощью команды **ping**.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии ПО CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейсов см. в сводной таблице интерфейсов маршрутизатора в конце лабораторной работы.

Необходимые ресурсы

•1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичным)
•1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
•2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например Tera Term)
•Консольные кабели для настройки устройств Cisco IOS через консольные порты
•Кабели Ethernet в соответствии с топологией

Примечание. Интерфейсы Gigabit Ethernet на маршрутизаторах Cisco 1941 определяют скорость автоматически, поэтому для подключения маршрутизатора кПК-Бможно использовать прямой кабель Ethernet. При использовании маршрутизатора Cisco другой модели может потребоваться кроссовый кабель Ethernet.

Часть 1: Разработка схемы разделения сети на подсети

Шаг 1: Создайте схему разделения на подсети, которая соответствует необходимому количеству подсетей и адресов узлов.

В этом сценарии вы выступаете в роли сетевого администратора, работающего в небольшом филиале крупной компании. Вам необходимо создать несколько подсетей в пространстве сетевого адреса 192.168.0.0/24, выполнив следующие требования:

•Первая подсеть — это сеть для сотрудников. Необходимо не меньше 25 IP-адресов узлов.
•Вторая подсеть — сеть администрирования. Необходимо не меньше 10 IP-адресов узлов.
•Третья и четвёртая подсети зарезервированы как виртуальные сети на интерфейсах виртуальных маршрутизаторов, loopback 0 и loopback 1. Интерфейсы виртуальных маршрутизаторов используются для моделирования локальных сетей, подключённых к маршрутизатору R1.
•Вам также необходимы две дополнительные неиспользуемые подсети для дальнейшего расширения сети.

Примечание. Маски подсети переменной длины использоваться не будут. Все маски подсети для устройств будут иметь одинаковую длину.
Составить схему разделения на подсети, отвечающую указанным условиям, помогут приведённые ниже вопросы.
1) Сколько адресов узлов необходимо для самой крупной подсети? 25
2)Каково минимальное количество необходимых подсетей? 6
3)Сеть, которую необходимо разделить на подсети, имеет адрес 192.168.0.0/24. Как маска подсети /24 будет выглядеть в двоичном формате?
11111111.11111111.11111111.00000000
4)Маска подсети состоит из двух частей — сетевой и узловой. В двоичном формате они представлены в маске подсети единицами и нулями.
Что в маске сети представляют единицы? сетевая часть Что в маске сети представляют нули? узловая часть
5)Чтобы разделить сеть на подсети, биты из узловой части исходной маски сети заменяются битами подсети. Количество битов подсетей определяет количество подсетей. Если каждая из возможных масок подсети представлена в указанном двоичном формате, сколько подсетей и сколько узлов будет создано в каждом примере?
Совет: помните, что количество битов узлов (во второй степени) определяет количество узлов для каждой подсети (минус 2), а количество битов подсетей (во второй степени) определяет количество подсетей. Биты подсетей (выделены полужирным шрифтом) — это биты, заимствованные за пределами исходной маски подсети /24. /24 — префиксная запись с косой чертой, которая соответствует десятичному представлению маски 255.255.255.0.
(/25) 11111111.11111111.11111111.**1**0000000
Эквивалент десятичного представления маски подсети с разделением точками:
255.255.255.128
Количество подсетей? 2 126
Количество узлов?
(/26) 11111111.11111111.11111111.**11**000000
Эквивалент десятичного представления маски подсети с разделением точками:
255.255.255.192
Количество подсетей?4, Количество узлов? 62
(/27) 11111111.11111111.11111111.**111**00000
Эквивалент десятичного представления маски подсети с разделением точками:
255.255.255.224
Количество подсетей?8, Количество узлов? 30
(/28) 11111111.11111111.11111111.**1111**0000
Эквивалент десятичного представления маски подсети с разделением точками:
255.255.255.240
Количество подсетей?16, Количество узлов? 14
(/29) 11111111.11111111.11111111.**11111**000
Эквивалент десятичного представления маски подсети с разделением точками:
255.255.255.248
Количество узлов? 6
Количество подсетей?32
(/30) 11111111.11111111.11111111.**111111**00
Эквивалент десятичного представления маски подсети с разделением точками:
255.255.255.252
Количество узлов?2

Количество подсетей?64
6)Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количеству адресов узлов?
/27, /26, /25
7)Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количеству подсетей?
/27 - /30
8)Учитывая ваши ответы, какая маска подсети соответствует минимальному необходимому количеству как узлов, так и подсетей?
/27
9)Выяснив, какая маска подсети соответствует всем указанным требованиям к сети, вы определите каждую подсеть, начиная с исходного сетевого адреса. Ниже перечислите все подсети от первой до последней. Помните, что первая подсеть – 192.168.0.0 с новой полученной маской подсети.

Маска подсети	**Префикс**	**Адрес подсети (десятичное представление с точками)**
192.168.0.0	27	255.255.255.224
192.168.0.32	27	255.255.255.224
192.168.0.64	27	255.255.255.224
192.168.0.96	27	255.255.255.224
192.168.0.128	27	255.255.255.224
192.168.0.160	27	255.255.255.224
192.168.0.192	27	255.255.255.224
192.168.0.224	27	255.255.255.224

Шаг 2: Заполните диаграмму, указав, где будут применяться IP-адреса узлов.
В приведённых ниже строках укажите IP-адреса и маски подсетей в виде префиксной записи с косой чертой. На маршрутизаторе укажите первый допустимый адрес в каждой подсети для каждого интерфейса – Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0 и loopback 1. Впишите IP-адрес для каждого компьютера (ПК-АиПК-Б). Внесите эти данные в таблицу адресации на стр. 1.

Часть 2: Настройка устройств
В части 2 вам нужно настроить топологию сети и основные параметры на компьютерах и маршрутизаторе, такие как IP-адреса интерфейса Gigabit Ethernet и компьютеров, маски подсети и шлюзы по умолчанию. Имена устройств и IP-адреса указаны в таблице адресации.
Примечание. В приложении А приведены сведения о конфигурации для выполнения шагов в части 2. Постарайтесь выполнить задания в части 2, не пользуясь приложением А.
Шаг 1: Настройте маршрутизатор.
a. Войдите в привилегированный режим, а затем в режим глобальной конфигурации.
b. Укажите **R1** в качестве имени узла для маршрутизатора.
c. Укажите и активируйте IP-адреса и маски подсети для интерфейсов **G0/0** и **G0/1**.
d. Интерфейсы loopback создаются для моделирования дополнительных локальных сетей, подключённых к маршрутизатору R1. Укажите IP-адреса и маски подсети для интерфейсов loopback. Созданные интерфейсы loopback по умолчанию будут активны. (Чтобы создать адреса loopback, введите команду **interface loopback 0** в режиме глобальной конфигурации.)
Примечание. При необходимости можно создать дополнительные адреса loopback для проверки в различных схемах адресации.
e. Сохраните текущую конфигурацию в файл загрузочной конфигурации.
Шаг 2: Настройте интерфейсы ПК.

a. Настройте на ПК-AIP-адрес, маску подсети и параметры шлюза по умолчанию.
b. Настройте на ПК-БIP-адрес, маску подсети и параметры шлюза по умолчанию.

Часть 3: Проверка сети и устранение неполадок

В части 3 вы проверите подключение сети с помощью команды **ping**.

a. Проверьте, может ли ПК-А установить связь со своим шлюзом по умолчанию. На ПК-А откройте окно командной строки и отправьте эхо-запрос с помощью команды ping на IP-адрес интерфейса Gigabit Ethernet 0/1 маршрутизатора. Получен ли ответ? да

b. Проверьте, может ли ПК-Б установить связь со своим шлюзом по умолчанию. На ПК-Б откройте окно командной строки и отправьте эхо-запрос с помощью команды ping на IP-адрес интерфейса Gigabit Ethernet 0/0 маршрутизатора. Получен ли ответ? да

c. Проверьте, может ли ПК-А установить связь с ПК-Б. На ПК-А откройте окно командной строки и отправьте эхо-запрос с помощью команды ping на IP-адрес компьютера ПК-Б. Получен ли ответ? да

d. Если вы ответили отрицательно на любой из заданных выше вопросов, вернитесь назад и проверьте введённые IP-адреса и маски подсети, а также убедитесь в том, что шлюзы по умолчанию ПК-А и ПК-Б правильно настроены.

e. Если все параметры указаны верно, но эхо-запросы с помощью команды pingпо по-прежнему не проходят, проверьте дополнительные факторы, которые могут блокировать сообщения по протоколу ICMP. На ПК-А и ПК-Б под управлением ОС Windows убедитесь в том, что межсетевой экран Windows для сетей типа «Домашняя», «Сеть предприятия» и «Общественная» отключён.

f. Попробуйте ввести заведомо неправильный адрес шлюза на ПК-А, указав значение 10.0.0.1. Что происходит при попытке отправить эхо-запрос с помощью команды ping с ПК-Б на ПК-А ?Получен ли ответ? нет

Лабораторная работа № 4

Тема: «Подключение точек доступа беспроводных сетей»

Цель работы:изучить процедуруподключения точек доступа беспроводных сетей.

Порядок выполнения работы

Беспроводные сети – это технология, позволяющая создавать сети, полностью соответствующие стандартам для обычных проводных сетей (например, Ethernet) без использования кабельной проводки. В качестве носителя информации в таких сетях выступают радиоволны СВЧ-диапазона.

Беспроводные сети используются там, где кабельная проводка затруднена или невозможна. Сеть, развернутая в соответствии со стандартом “RadioEthernet”, представляет собой аналог обычной кабельной сети Ethernet с коллизионным механизмом доступа к среде передачи данных. Разница состоит только в характере этой среды. RadioEthernet полностью обеспечивает все потребности беспроводной передачи данных внутри помещений.

При наружном применении RadioEthernet очень удобно использовать сети на “последней миле” взамен кабельной, то есть для соединения между абонентом и ближайшим узлом опорной сети. При этом реальная протяженность “последней мили” может быть от нескольких сотен метров до 20-30 км и ограничена лишь наличием прямой видимости.

Все компьютеры сети оснащаются беспроводными сетевыми адаптерами (внешними с интерфейсом USB, или внутренними с интерфейсом PCI или PCMCI), работающими в диапазоне 2,4 ГГц в соответствии со стандартом IEEE 802.11.

Стандарт IEEE 802.11 входит в серию стандартов IEEE 802.x, относящихся к сетям и коммуникациям. Сюда также входят такие стандарты, как 802.3 Ethernet, 802.5 TokenRing и т.д. Таким образом, стандарт IEEE 802.11 определяет компоненты и характеристики сети на физическом уровне передачи данных и на уровне доступа к среде с учетом беспроводного способа передачи данных и возможности взаимодействия с существующими сетями.

Преимущества RadioEthernet.

- Скорость, простота развертывания и настройки беспроводной сети.
- Сохранение инвестиций в локальную сеть при смене офиса.
- Гибкость: быстрая реструктуризация, изменение конфигурации и размеров сети.
- Мобильность пользователей в зоне охвата сети.
- Беспроводная сеть работает там, где не работает кабельная.

Возможны два режима работы беспроводной сети:

"каждый с каждым" (peer-to-peer, ad-hoc) – компьютеры обмениваются данными непосредственно друг с другом. Можно провести аналогию с проводной сетью Ethernet на коаксиальном кабеле;

"инфраструктура" – компьютеры обмениваются данными через центральное устройство – точку доступа (AccessPoint). Можно провести аналогию с проводной сетью Ethernet на витой паре с использованием коммутатора.

В нашей лабораторной работе точка доступа – это устройство компании D-LinkDWL-7000AP, которое является центральным элементом беспроводной сети. DWL-7000AP объединяет пользователей, оснащёнными беспроводными адаптерами DWL-AG520 и DWL-AG650 (беспроводной адаптер для мобильных ПК), друг с другом и с внешним миром. Точка доступа (DWL-7000AP) получает, буферизует и передает данные, поддерживая группу беспроводных пользователей. Оборудование работает на частоте 5 ГГц, используется метод мультиплексирования с ортогональным делением частот (OFDM), поддерживает скорость

передачи до 54 Мбит/с (48, 36, 24, 18, 12, 9 и 6 Мбит/с), реальная скорость передачи данных от 22 до 26 Мбит/с. 12 одновременно доступных для работы каналов.

Параметры устройств

DWL-7000AP:

- Поддержка стандартов 802.11a / 802.11b.
- Диапазон частот:

802.11b: 2.4-2.462 ГГц;

802.11a: 5,150-5,350 ГГц.

- Стандарт IEEE 802.1X, Wi-Fi сертификат.
- Порт ЛВС: RJ-45 10/100Base-TX.
- Защита данных:

802.11a: 64-, 128-, 152-бит WEP;

802.11b: 64-, 128-, 256-бит WEP.

- Скорость передачи:

802.11a: до 54 Мбит/с (до 72 Мбит/с в режиме turbo);

802.11b+: до 22 Мбит/с.

- Режим работы: точка доступа, мост между сегментами

802.11a и 802.11b.

- Web-управление.
- Две дипольные всенаправленные антенны 5 dB.

DWL-AG520:

- Шина PCI.
- Поддержка стандартов 802.11a / 802.11b.
- Диапазон частот:

802.11b: 2.4-2.4835 ГГц;

802.11a: 5,150-5,350 ГГц.

- Скорость передачи:

802.11a: до 54 Мбит/с;

802.11b: до 11 Мбит/с.

- Съемная антенна, возможность подключения внешней антенны.

DWL-AG650:

- Спецификация PCMCIA типа II, шина CardBus.
- Поддержка стандартов 802.11a / 802.11b.
- Диапазон частот:

802.11b: 2.4-2.4835 ГГц;

802.11a: 5,150-5,350 ГГц.

- Стандарт IEEE 802.1X, Wi-Fi сертификат.
- Поддерживаемые ОС: Windows 98, NT, 2000, ME, XP.
- Защита данных:

802.11a: 64-, 128-, 152-бит WEP;

802.11b: 64-, 128-, 256-бит WEP. Advanced Encryption Security (AES)

- Скорость передачи:

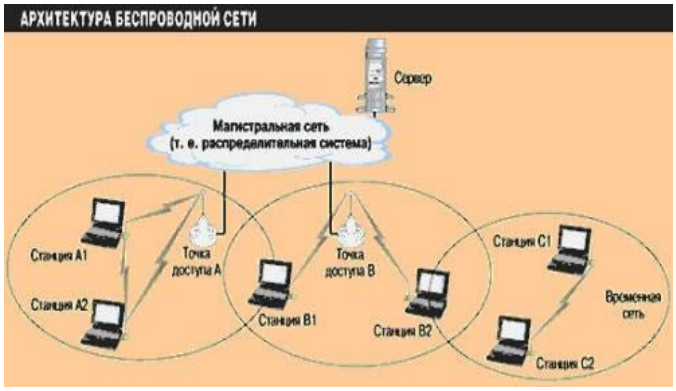
802.11a: до 54 Мбит/с;

802.11b: до 11 Мбит/с.

Применение точки доступа позволяет:

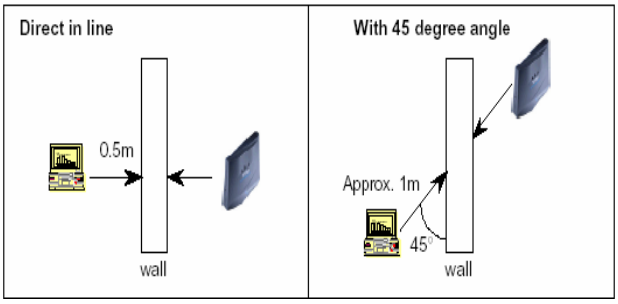
- устранить коллизии (когда два компьютера пытаются занять один канал);
- организовать соединение с локальной сетью или Интернет;
- увеличить дальность действия в 2 раза;

• усилить безопасность беспроводной сети путем фильтрации физических и сетевых адресов, портов и протоколов;
• построить беспроводную сеть на большой площади путем установки дополнительных точек доступа.



Планирование беспроводной сети

При планировании беспроводной сети необходимо учитывать следующие моменты:
• Расположение точек доступа зависит от необходимой площади охвата и конструкции здания.
• Толстые стены, или стены с металлоконструкциями, будут блокировать сигнал сильнее, чем светопропускающие конструкции.
• Количество стен и перегородок желательно свести к минимуму – каждая стена может сокращать максимальную дистанцию для передачи данных на 1-30 м.
• Располагайте беспроводные устройства по прямой линии к препятствию, так как стена толщиной в 0,5 м при расположении устройств под углом в 45 градусов превращается в преграду толщиной почти 1м.



• Офисная мебель, кабинеты могут образовывать “тени” в зоне охвата.
• Для получения широкой зоны охвата необходима прямая видимость.
• Удостоверьтесь, что антенна настроена для лучшего приема.
• Используя поставляемые с устройствами утилиты для оценки качества связи, необходимо построить карту зоны охвата в заданном помещении.

Например: утилита к беспроводному адаптеру имеет функцию диагностики, позволяет определить уровень сигнала по каждому каналу. Также можно проверить качество связи между клиентом и точкой доступа.

Некоторые типичные проблемы при проектировании беспроводной сети

Отношение сигнал-шум (SNR) хорошее, но производительность данных относительно низкая:
• Перегруженная сеть – слишком много клиентов пытаются получить доступ к среде передачи.
• Электрическое устройство, генерирующее радиосигнал, расположено рядом с беспроводным клиентом.

• Качество связи другого клиента недостаточно хорошее и поэтому возникает много повторной передачи пакетов.
• Коллизии, возникающие из-за проблемы «скрытый узел».

Концентрация пользователей на точку доступа слишком высокая:
• Разместите ближе точки доступа, чтобы распределить нагрузку.
• Добавьте дополнительные точки доступа к беспроводной сети.

Уровень сигнала низкий:
• Устройства могут быть слишком далеко друг от друга.
• Имеется преграда между устройствами.

Цель работы:

Наладить беспроводную сеть между рабочими станциями.

Для этого необходимо:
– подключить оборудование;
– настроить конфигурацию сети;
– установить соединение между двумя ПК без точки доступа;
– установить соединение между тремя ПК с точкой доступа;
– осуществить передачу данных по беспроводной сети.

Шаг 1. Подключить оборудование.

1. Сначала подключите адаптер питания к гнезду на задней панели устройства и включите другой его конец в розетку питания. Индикатор POWER загорится, что говорит о правильной работе.
2. Вставьте кабель Ethernet в порт LAN на задней панели DWL-7000AP и в доступный порт Ethernet на сетевом адаптере компьютера, который будет использоваться для настройки устройства. Индикатор Link порта LAN загорится, показывая наличие соединения.
3. Включить точку доступа, проверить питание и подключение.

Шаг 2. Сконфигурировать оборудование с помощью мастера установки.

1. Откройте Web-браузер и наберите http://192.168.0.50 в адресной строке, затем нажмите клавиши Enter или Return.
2. Наберите “admin” в строке username и оставьте поле password. Нажмите OK.
3. Нажмите RunWizard и затем Next.
4. Установите новый пароль, затем нажмите Next.
5. Измените настройки беспроводной сети 802.11a так, чтобы они удовлетворяли требованиям существующей беспроводной сети. Нажмите Next.
6. Выберите размер ключа, который вы хотите использовать и введите ключ в соответствующем поле. Нажмите Next.
7. Если есть необходимость, измените настройки беспроводной сети 802.11g. Нажмите Next.
8. То же, что и шаг 6, но для 802.11g. Нажмите Next.
9. Нажмите Restart.

Шаг 3. Установить соединение между двумя ПК без точки доступа.

Шаг 4. Установить соединение между тремя ПК с точкой доступа.

Лабораторная работа № 5

Тема: «Кодирование по стандарту 802.11 и его аутентификация»
Цель работы:изучить процедуру кодирования по стандарту 802.11 и его аутентификацию
Порядок выполнения работы

Стандарт IEEE 802.11b.
Спецификация IEEE 802.11b по инициативе в основном Lucent Technologies и Intersil Corp была разработана для диапазона 2,4 ГГц ISM. Назначение спецификации – организация беспроводных LAN Ethernet.
Основное добавление 802.11b к стандарту беспроводной локальной сети должно было стандартизировать поддержку физического уровня двух новых скоростей – 5,5 и 11 Мбит/с. Чтобы достичь этого, в качестве физического уровня для стандарта была выбрана прямая последовательность частот (Direct Sequence Spread Spectrum – DSSS), так как переключающиеся частоты не могли поддерживать более высокие скорости, не нарушая текущие инструкции Федеральной Комиссии по связи. Более эффективная схема кодирования – Complimentary code keying (CCK) – была включена в стандарт, чтобы достигнуть конечной скорости передачи данных 11 Мбит/с.
Однако, 802.11b несовершенен. Один из наиболее существенных недостатков – полоса частот. Многочисленные устройства могут вторгнуться в полосу 2,4 ГГц и поэтому представляют потенциальный источник помех. Сюда входят микроволновые печи, переносные телефоны, радиосистемы и домашние контрольные устройства, использующие протокол X-10. Самая большая опасность, однако, – от все более широко распространяющихся устройств Bluetooth. Проблема усугубляется тем фак- том, что 802.11b рассчитан не просто на связь на расстоянии от 15 до 45 м (через стены и потолки), но и до 300 м прямой видимости на открытой местности. Ограниченная полоса пропускания, возможно, – еще большая проблема. Номинально 802.11b обеспечивает скорость, эквивалентную 10 Мбит/с Ethernet. Однако, перегрузка, конфигурация и требования безопасности могут уменьшить фактическую производительность до типичного значения в 5 Мбит/с. Хотя этого и достаточно для Web-браузеров, но неадекватно для большого количества приложений типа потокового видео. Проблемы на физическом уровне — одна из причин для деградации работы. Например, префикс (преамбула), включаемый в каждый пакет используемого здесь протокола Physical Layer Convergence Protocol (PLCP), который содержит значение скорости передачи и данные для проверки синхронизации, состоит из 24 байтов.
Безопасность – другая важная проблема. Система защиты Wired Equivalent Privacy (WEP), встроенная в протокол 802.11, показала уязвимость и относительную несложность расшифровки кода с 40-битовым ключом. Хакеры могут подъехать к дому на автомобиле, имея ноутбук, снабженный радиосистемой, и войти в сеть. Разработчики предлагают несколько решений, включая в алгоритм шифровки со 128-битовым ключом, известный как Advanced Encryption Standard (AES), который, однако, требует обновления технических и программных средств или Temporal Key Integrity Protocol (TKIP), который будет совместимым с WEP.
IEEE 802.11a. Если 802.11b размещается в полосе 2,4 ГГц, то стандарт 802.11a был разработан для диапазона 5 ГГц «Нелицензируемая национальная информационная инфраструктура» (Unlicensed National Information Infrastructure — UNI1). Кроме того, в отличие от 802.11b, 802.11a использует совершенно другую схему кодирования — ортогональное мультиплексирование с разделением частот (Coded orthogonal frequency division multi-plexing — COFDM) для беспроводного использования внутри помещения.

COFDM расщепляет одну высокоскоростную несущую час- тоту на несколько поднесущих более малого быстродействия, которые передаются параллельно (рис. 2.18). Высоко скоростная несущая шириной 20 МГц разделена на 52 подканала, каждый приблизительно по 300 кГц. COFDM использует 48 из этих подканалов для данных, а остающиеся четыре — для исправления ошибок. COFDM поставляет более высокие скорости передачи данных и высокую степень восстановления благодаря схеме кодирования и исправлению ошибки. Метод обеспечивает скорости передачи в 5, 12 и 24 Мбит/с.

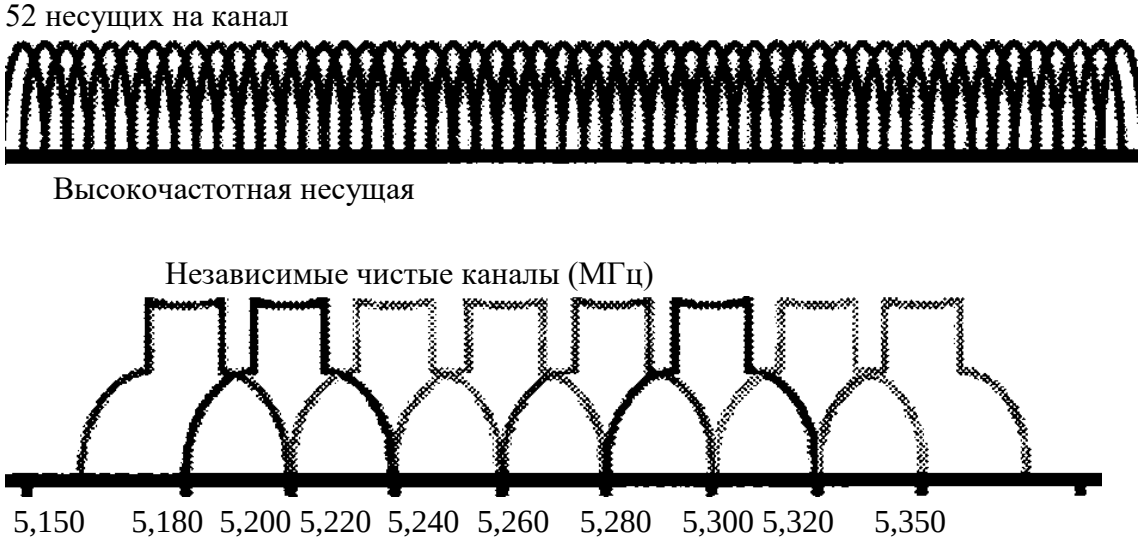


Рис. 18. Структура диапазонов в протоколе 802.11a

IEEE 802.1In. Потребность в беспроводных LAN весьма возросла после ратификации IEEEa 802.11a летом 1999 г. Появилось множество пользователей, подключающих ноутбуки к сетям на работе и к Internet дома так же, как и в магазинах, кафе, аэропортах, гостиницах и других местах, обеспеченных доступом к Wi-Fi. Тем временем, однако, выпуск единиц Wi-Fi-оборудования существенно вырос – до 100 млн модулей в 2005 г. сравнительно с менее чем 10 млн в 2001 г. Технология использовалась не только в П К и ноутбуках, но и в мобильных телефонах и других бытовых устройствах для реализации Internet телефонии, интерактивных игр, передачи музыки, фотографий и домашнего видео. Поэтому существующие сетевые инфраструктуры Wi-Fi начали испытывать перегрузку.

Эта ситуация предвиделась, и IEEE (2003 г.) принял предложения рабочей группы 802.11 TGn о поправках к стандартам предполагающих приблизительно 4-кратное повышение производительности WLAN по сравнению с потоком 802.1 la/g.

Спецификация проекта 802.1 In отличается от предшественников тем, что предусматривает разнообразие дополнительных режимов и конфигураций для различных скоростей передачи данных. Это дает возможность стандарту обеспечить базовые параметры для всех 802.1 ln-устройств, разрешая изготовителям охватывать широкий спектр различных приложений и цен на оборудование. Максимальная скорость, допускаемая 802.1 In – до 600 Мбит/с, однако, если аппаратные средства WLAN не поддерживают каждую опцию, они могут быть совместимыми со стандартом.

Один из наиболее широко известных компонентов спецификации известен как многократный вход-выход (Multiple Input Multiple Output — MIMO). MIMO использует такое явление, как многопутевая передача, когда радиоволны, будучи отраженными от стен, дверей и других объектов, достигают антенны приемника

многократно, различными маршрутами и в различные времена. Неконтролируемая многопутевая передача искажает первоначальный сигнал, делая более трудной расшифровку и ухудшая функционирование Wi-Fi. MIMO
использует методику, известную как пространственное мультиплексирование (space-division multiplexing). Передающее устройство WLAN фактически разбивает поток данных на части, названные пространственными потоками, и передает каждый из них через отдельные антенны к соответствующим антеннам приемникам. Стандарт 802.1 In предусматривает до четырех пространственных потоков, даже при том, что совместимые аппаратные средства не обязаны это поддерживать.
Удвоение числа пространственных потоков фактически удваивает скорость данных. Другой дополнительный режим в 802.1 In также увеличивает скорость, удваивая ширину WLAN канала связи от 20 до 40 М Гц.
Вообще говоря, 802.1 In предусматривает 576 возможных конфигураций потока данных. Для сравнения, 802.1 lg обеспечивает 12 возможных потоков данных, а 802.11a и 802.11b определяют восемь и четыре, соответственно.
Таблица 10 демонстрирует характеристики различных версий спецификации 802.11.
Таблица 10. **Характеристики стандартов семейства 802.11**

Характеристики	Стандарты			
	802.11a	802.11b	802.11 g	802.11л
Когда принят	Июль 1999 г.	Июль 1999 г.	Июнь 2003 г.	Обсуждается
Максимальная скорость, Мбит/с	54	11	54	600
Метод модуляции	0FDM	DSSSwih CCK	DSSS илиCCK; или 0FDM	DSSS или CCK, или 0FDM
Диапазон радиочастот, ГГц	5,0	2,4	2,4	2,4-5,0
Число пространственных потоков	1	1	1	1,2,3 или 4
Ширина канала, МГц	20	20	20	20-40

Лабораторная работа № 6

Тема: «Протокол шифрования WEP»

Цель работы:изучитьпротокол шифрования WEP

Порядок выполнения работы

Протокол WEP позволяет шифровать поток передаваемых данных на основе алгоритма RC4 с ключом размером 64 или 128 бит — эти ключи имеют так называемую статическую составляющую длиной от 40 до 104 бит и дополнительную динамическую составляющую размером 24 бита, называемую вектором инициализации (Initialization Vector, IV).

Процедура WEP-шифрования выглядит следующим образом. Первоначально передаваемые в пакете данные проверяются на целостность (алгоритм CRC-32), после чего контрольная сумма (integrity check value, ICV) добавляется в служебное поле заголовка пакета. Далее генерируется 24-битный вектор инициализации (IV), а к нему добавляется статический (40- или 104-битный) секретный ключ. Полученный таким образом 64- или 128-битный ключ и является исходным ключом для генерации псевдослучайного числа, которое используется для шифрования данных. Далее данные смешиваются (шифруются) с помощью логической операции XOR с псевдослучайной ключевой последовательностью, а вектор инициализации добавляется в служебное поле кадра. Вот, собственно, и всё.

Протокол безопасности WEP предусматривает два способа аутентификации пользователей: Open System (открытая) и Shared Key (общая). При использовании открытой аутентификации, по сути, никакой аутентификации не выполняется, то есть любой пользователь может получить доступ в беспроводную сеть. Однако даже при открытой системе допускается применение WEP-шифрования данных

Взлом беспроводной сети с протоколом WEP

Но перечисленных средств защиты не достаточно. И, чтобы это доказать, начну с инструкции по взлому беспроводных сетей стандарта 802.11b/g на базе протокола безопасности WEP.

Для взлома сети, кроме ноутбука с беспроводным адаптером, потребуется специальная утилита, например aircrack 2.4, которую можно найти в свободном доступе в Интернете.

Данная утилита поставляется сразу в двух вариантах: под Linux и под Windows. Нас интересуют только те файлы, которые размещены в директории aircrack-2.4win32.

В этой директории имеются три небольшие утилиты (исполняемых файла): airodump.exe, aircrack.exe и airdecap.exe. Первая утилита предназначена для перехвата сетевых пакетов, вторая — для их анализа и получения пароля доступа, а третья — для расшифровки перехваченных сетевых файлов.

Конечно же, не всё так просто, как может показаться. Дело в том, что все подобные программы разработаны под конкретные модели чипов, на базе которых построены сетевые адаптеры. Таким образом, нет гарантии, что выбранный произвольно беспроводной адаптер окажется совместим с программой aircrack-2.4. Более того, даже при использовании совместимого адаптера (список совместимых адаптеров (точнее, чипов беспроводных адаптеров) можно найти в документации к программе) придется повозиться с драйверами, заменив стандартный драйвер от производителя сетевого адаптера на специализированный под конкретный чип.

Процедура взлома беспроводной сети довольно проста. Начинаем с запуска утилиты airodump.exe, которая представляет собой сетевой сниффер для перехвата пакетов. При запуске программы откроется диалоговое окно, где потребуется указать беспроводной сетевой адаптер, тип чипа сетевого адаптера (Network interface type (o/a)), номер канала беспроводной связи (Channel(s): 1 to 14, 0=all) (если номер канала неизвестен, то можно сканировать все каналы). Также задается имя выходного файла, в котором хранятся перехваченные пакеты (Output filename prefix), и указывается, требуется ли захватывать все пакеты целиком (cap-файлы) или только часть пакетов с векторами инициализации (ivs-файлы) (Only write WEP IVs (y/n)). При использовании WEP-шифрования для подбора секретного ключа вполне достаточно сформировать ivs-файл. По умолчанию ivs- или cap-файлы создаются в той же директории, что и сама программа airodump.

После настройки всех опций утилиты airodump откроется информационное окно, в котором отображаются информация об обнаруженных точках беспроводного доступа, сведения о клиентах

сети и статистика перехваченных пакетов. Если точек доступа несколько, то статистика будет выдаваться по каждой из них.
Первым делом запишите MAC-адрес точки доступа, SSID беспроводной сети и MAC-адрес одного из подключенных к ней клиентов (если их несколько). Ну а затем нужно подождать, пока не будет перехвачено достаточное количество пакетов.
Количество пакетов, которые нужно перехватить для успешного взлома сети, зависит от длины WEP-ключа (64 или 128 бит) и, конечно же, от удачи. Если в сети используется 64-битный WEP-ключ, то для успешного взлома вполне достаточно захватить полмиллиона пакетов, а во многих случаях и того меньше. Время, которое для этого потребуется, зависит от интенсивности трафика между клиентом и точкой доступа, но, как правило, оно не превышает нескольких минут. В случае же применения 128-битного ключа для гарантированного взлома потребуется перехватить порядка двух миллионов пакетов. Для остановки процесса захвата пакетов (работы утилиты) используется комбинация клавиш Ctrl+C.
После того как выходной ivs-файл сформирован, можно приступать к его анализу. В принципе, это можно делать и одновременно с перехватом пакетов, но для простоты мы рассмотрим последовательное выполнение этих двух процедур. Для анализа сформированного ivs-файла потребуется утилита aircrack.exe, которая запускается из командной строки. В нашем примере применялись следующие параметры запуска:
aircrack.exe –b 00:13:46:1C:A4:5F –n 64 –i 1 out.ivs.
В данном случае –b 00:13:46:1C:A4:5F — это указание MAC-адреса точки доступа, –n 64 — указание длины используемого ключа шифрования, –i 1 — индекс ключа, а out.ivs — файл, который подвергается анализу. Полный перечень параметров запуска утилиты можно посмотреть, просто набрав в командной строке команду aircrack.exe без параметров.
В принципе, поскольку такая информация, как индекс ключа и длина ключа шифрования, обычно заранее неизвестна, традиционно применяется следующий упрощенный вариант запуска команды: aircrack.exe out.ivs.
Вот так легко и быстро проводится вскрытие беспроводных сетей с WEP-шифрованием, так что говорить о безопасности сетей в данном случае вообще неуместно. Действительно, можно ли говорить о том, чего на самом деле нет!
В самом начале статьи мы упомянули, что во всех точках доступа имеются и такие возможности, как применение режима скрытого идентификатора сети и фильтрации по MAC-адресам, которые призваны повысить безопасность беспроводной сети. Но это не спасает.
На самом деле не столь уж и невидим идентификатор сети — даже при активации этого режима на точке доступа. К примеру, уже упомянутая нами утилита airodump все равно покажет вам SSID сети, который впоследствии можно будет использовать для создания профиля подключения к сети (причем несанкционированного подключения).
А если уж говорить о такой несерьезной мере безопасности, как фильтрация по MAC-адресам, то здесь вообще все очень просто. Существует довольно много разнообразных утилит и под Linux, и под Windows, которые позволяют подменять MAC-адрес сетевого интерфейса. К примеру, для несанкционированного доступа в сеть мы подменяли MAC-адрес беспроводного адаптера с помощью утилиты SMAC 1.2. Естественно, в качестве нового MAC-адреса применяется MAC-адрес авторизованного в сети клиента, который определяется все той же утилитой airodump.
Хочется отметить, что после появления WPA, проблема WEP не потеряла актуальности. Дело в том, что в некоторых случаях для увеличения радиуса действия беспроводной сети разворачиваются так называемые распределенные беспроводные сети (WDS) на базе нескольких точек доступа. Но самое интересное заключается в том, что эти самые распределенные сети не поддерживают WPA-протокола и единственной допустимой мерой безопасности в данном случае является применение WEP-шифрования. Ну а взламываются эти WDS-сети абсолютно так же, как и сети на базе одной точки доступа.
Итак, преодолеть систему безопасности беспроводной сети на базе WEP-шифрования никакого труда не представляет. WEP никогда не предполагал полную защиту сети. Он попросту должен был обеспечить беспроводную сеть уровнем безопасности, сопоставимым с проводной сетью. Это ясно даже из названия стандарта "Wired Equivalent Privacy" - безопасность, эквивалентная проводной сети. Получение ключа WEP, если можно так сказать, напоминает получение

физического доступа к проводной сети. Что будет дальше - зависит от настроек безопасности ресурсов сети.

Большинство корпоративных сетей требуют аутентификацию, то есть для получения доступа к ресурсам пользователю придётся указать имя и пароль. Серверы таких сетей физически защищены - закрыты в специальной комнате, патч-панели и коммутаторы кабельной сети заперты в шкафах. Кроме того, сети часто бывают сегментированы таким образом, что пользователи не могут добраться туда, куда не нужно.

Лабораторная работа № 7

Тема: «Использование технологии WPAс сервером аутентификации»

Цель работы:изучить процедуру использования технологии WPAс сервером аутентификации.

Порядок выполнения работы

Стандарт безопасности WPA

WPA — это временный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.11i. По сути, WPA = 802.1X + EAP + TKIP + MIC, где:

WPA — технология защищенного доступа к беспроводным сетям (Wi-Fi Protected Access),

EAP — протокол расширяемый протокол аутентификации (Extensible Authentication Protocol),

TKIP — протокол временной целостности ключей, другой вариант перевода - протокол целостности ключей во времени (Temporal Key Integrity Protocol),

MIC — технология криптографическая проверка целостности пакетов (Message Integrity Code).

Протокол RADIUS. RADIUS- предназначен для работы в связке с сервером аутентификации, в качестве которого обычно выступает RADIUS-сервер. В этом случае беспроводные точки доступа работают в enterprise-режиме.

Если в сети отсутствует RADIUS-сервер, то роль сервера аутентификации выполняет сама точка доступа - так называемый режим WPA-PSK (pre-shared key, общий ключ). В этом режиме в настройках всех точек доступа заранее прописывается общий ключ. Он же прописывается и на клиентских беспроводных устройствах. Такой метод защиты тоже довольно секьюрен (относительно WEP), очень не удобен с точки зрения управления. PSK-ключ требуется прописывать на всех беспроводных устройствах, пользователи беспроводных устройств его могут видеть. Если потребуется заблокировать доступ какому-то клиенту в сеть, придется заново прописывать новый PSK на всех устройствах сети и так далее. Другими словами, режим WPA-PSK подходит для домашней сети и, возможно, небольшого офиса, но не более того.

Ключевыми здесь являются новые модули TKIP и MIC.

За шифрование данных в WPA отвечает протокол TKIP, который, хотя и использует тот же алгоритм шифрования - RC4 - что и в WEP, но в отличие от последнего, использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом и общее число вариаций которых достигает 500 миллиардов. Он применяет более длинный вектор инициализации и использует криптографическую контрольную сумму (MIC) для подтверждения целостности пакетов (последняя является функцией от адреса источника и назначения, а также поля данных). Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через каждые 10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищенной.

Правда, TKIP сейчас не является лучшим в реализации шифрования, поскольку в силу вступают новые алгоритмы, основанные на технологии Advanced Encryption Standard (AES), которая, кстати говоря, уже давно используется в VPN.

Технология проверки целостности сообщений MIC(Message Integrity Check) обороняет от внешнего проникновения и изменения информации. Достаточно сложный математический алгоритм позволяет сверять отправленные в одной точке и полученные в другой данные. Если замечены изменения и результат сравнения не сходится, такие данные считаются ложными и выбрасываются.

Фильтрация MAC-адресов, которая поддерживается всеми современными точками доступа и беспроводными маршрутизаторами, хотя и не является составной частью стандарта 802.11, однако, как считается, позволяет повысить уровень безопасности беспроводной сети. Для реализации данной функции в настройках точки доступа создается таблица MAC-адресов беспроводных адаптеров клиентов, авторизованных для работы в данной сети.

Еще одна мера предосторожности, которую часто используют в беспроводных сетях, — режим скрытого идентификатора сети. Каждой беспроводной сети назначается свой уникальный идентификатор (SSID), который представляет собой название сети. Когда пользователь пытается войти в сеть, драйвер беспроводного адаптера прежде всего сканирует эфир на предмет наличия в

ней беспроводных сетей. При применении режима скрытого идентификатора (как правило, этот режим называется Hide SSID) сеть не отображается в списке доступных и подключиться к ней можно только в том случае, если, во-первых, точно известен ее SSID, а во-вторых, заранее создан профиль подключения к этой сети.

Механизмы работы WPA

Технология WPA являлась временной мерой до ввода в эксплуатацию стандарта 802.11i. Часть производителей до официального принятия этого стандарта ввели в обращение технологию WPA2, в которой в той или иной степени используются технологии из 802.11i. Такие как использование протокола CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), взамен TKIP, в качестве алгоритма шифрования там применяется усовершенствованный стандарт шифрования AES (Advanced Encryption Standard). А для управления и распределения ключей по-прежнему применяется протокол 802.1x.

Аутентификация пользователя

Как уже было сказано выше, протокол 802.1x может выполнять несколько функций. В данном случае нас интересуют функции аутентификации пользователя и распределение ключей шифрования. Необходимо отметить, что аутентификация происходит «на уровне порта» - то есть пока пользователь не будет аутентифицирован, ему разрешено посылать/принимать пакеты, касающиеся только процесса его аутентификации (учетных данных) и не более того. И только после успешной аутентификации порт устройства (будь то точка доступа или умный коммутатор) будет открыт и пользователь получит доступ к ресурсам сети.

Стандарт WPA использует 802.1x и расширенный протокол аутификации (Extensible Authentication Protocol, EAP) в качестве основы для механизма аутентификации.

Аутентификация требует, чтобы пользователь предъявил свидетельства/ мандат (credentials) того, что ему позволено получать доступ в сеть. Для этого права пользователя проверяются по базе данных зарегистрированных пользователей. Для работы в сети пользователь должен обязательно пройти через механизм аутентификации.

База данных и система проверки в больших сетях обычно принадлежат специальному серверу - чаще всего RADIUS(централизованный сервер аутентификации).

Однако, поскольку применение WPA подразумевается всеми категориями пользователей беспроводных сетей, стандарт имеет упрощ¨нный режим, который не требует использования сложных механизмов.

Этот режим называется Pre-Shared Key (WPA-PSK) - при его использовании необходимо ввести один пароль на каждый узел беспроводной сети (точки доступа, беспроводные маршрутизаторы, клиентские адаптеры, мосты). До тех пор, пока пароли совпадают, клиенту будет разрешен доступ в сеть.

Функции аутентификации возлагаются на протокол EAP, который сам по себе является лишь каркасом для методов аутентификации. Вся прелесть протокола в том, что его очень просто реализовать на аутентификаторе (точке доступа), так как ей не требуется знать никаких специфичных особенностей различных методов аутентификации. Аутентификатор служит лишь передаточным звеном между клиентом и сервером аутентификации.

Если можно применить WPA, то необходимо выбрать между WPA, WPA2 и WPA-PSK. Главным фактором при выборе WPA или WPA2, с одной стороны, и WPA-PSK — с другой, является возможность развернуть инфраструктуру, необходимую WPA и WPA2 для аутентификации пользователей. Для WPA и WPA2 требуется развернуть серверы RADIUS и, возможно, Public Key Infrastructure (PKI). WPA-PSK, как и WEP, работает с общим ключом, известным беспроводному клиенту и AP. WPA-PSK можно смело использовать общий ключ WPA-PSK для аутентификации и шифрования, так как ему не присущ недостаток WEP.

Лабораторная работа № 8

Тема: «Аутентификация и авторизация абонента»
Цель работы:изучить процедуру настройки коммутатора и подключения к коммутатору.

Порядок выполнения работы

Transport Layer Security (TLS) -- процедура аутентификации, которая предполагает использование цифровых сертификатов X.509 в рамках инфраструктуры открытых ключей (Public Key Infrastructure -- PKI). EAP-TLS поддерживает динамическое создание ключей и взаимную аутентификацию между саппликантом и сервером аутентификации. Недостатком данного метода является необходимость поддержки инфраструктуры открытых ключей.
Tunneled TLS (TTLS) -- EAP расширяющий возможности EAP-TLS. EAP-TTLS использует безопасное соединение, установленное в результате TLS-квитирования для обмена дополнительной информацией между саппликантом и сервером аутентификации.
Так же существуют и другие методы:
EAP-SIM, EAP-AKA - используются в сетях GSM мобильной связи
LEAP - пропреоретарный метод от Cisco systems
EAP-MD5 - простейший метод, аналогичный CHAP (не стойкий)
EAP-MSCHAP V2 - метод аутентификации на основе логина/пароля пользователя в MS-сетях
EAP-TLS - аутентификация на основе цифровых сертификатов
EAP-SecureID - метод на основе однократных паролей
Кромевышеперечисленных, следует отметить следующие два метода, EAP-TTLS и EAP-PEAP. В отличие отпредыдущих, эти два метода перед непосредственной аутентификацией пользователя сначала образуют TLS-туннель между клиентом и сервером аутентификации. А уже внутри этого туннеля осуществляется сама аутентификация, с использованием как стандартного EAP (MD5, TLS), или старых не-EAP методов (PAP, CHAP, MS-CHAP, MS-CHAP v2), последние работают только с EAP-TTLS (PEAP используется только совместно с EAP методами). Предварительное туннелирование повышает безопасность аутентификации, защищая от атак типа «man-in-middle», «session hihacking» или атаки по словарю.
Протокол PPP засветился там потому, что изначально EAP планировался к использованию поверх PPP туннелей. Но так как использование этого протокола только для аутентификации по локальной сети - излишняя избыточность, EAP-сообщения упаковываются в «EAP over LAN» (EAPOL) пакеты, которые и используются для обмена информацией между клиентом и аутентификатором (точкой доступа).

Схема аутентификации
Она состоит из трех компонентов:
Supplicant - софт, запущенный на клиентской машине, пытающейся подключиться к сети
Authenticator - узел доступа, аутентификатор (беспроводная точка доступа или проводной коммутатор с поддержкой протокола 802.1x)
Authentication Server - сервер аутентификации (обычно это RADIUS-сервер)
Теперь рассмотрим сам процесс аутентификации. Он состоит из следующих стадий:
Клиент может послать запрос на аутентификацию (EAP-start message) в сторону точки доступа.
Точка доступа (Аутентификатор) в ответ посылает клиенту запрос на идентификацию клиента (EAP-request/identity message). Аутентификатор может послать EAP-request самостоятельно, если увидит, что какой-либо из его портов перешел в активное состояние.

Клиент в ответ высылает EAP-response packet с нужными данными, который точка доступа (аутентификатор) перенаправляет в сторону Radius-сервера (сервера аутентификации).
Сервер аутентификации посылает аутентификатору (точке доступа) challenge-пакет (запрос информации о подлинности клиента). Аутентификатор пересылает его клиенту.
Далее происходит процесс взаимной идентификации сервера и клиента. Количество стадий пересылки пакетов туда-сюда варьируется в зависимости от метода EAP, но для беспроводных сетей приемлема лишь «strong» аутентификация с взаимной аутентификацией клиента и сервера (EAP-TLS, EAP-TTLS, EAP-PEAP) и предварительным шифрованием канала связи.
На следующий стадии, сервер аутентификации, получив от клиента необходимую информацию, разрешает (accept) или запрещает (reject) тому доступ, с пересылкой данного сообщения аутентификатору. Аутентификатор (точка доступа) открывает порт для Supplicant-a, если со стороны RADIUS-сервера пришел положительный ответ (Accept).
Порт открывается, аутентификатор пересылает клиенту сообщение об успешном завершении процесса, и клиент получает доступ в сеть.
После отключения клиента, порт на точке доступа опять переходит в состояние «закрыт».
Для коммуникации между клиентом (supplicant) и точкой доступа (authenticator) используются пакеты EAPOL. Протокол RADIUS используется для обмена информацией между аутентификатором (точкой доступа) и RADIUS-сервером (сервером аутентификации). При транзитной пересылке информации между клиентом и сервером аутентификации пакеты EAP переупаковываются из одного формата в другой на аутентификаторе.

Типы аутентификации

TLS

Тип метода аутентификации, использующий протокол EAP и протокол безопасности, именуемый протоколом защиты транспортного уровня (Transport Layer Security - TLS). EAP-TLS использует сертификаты на основе паролей. Аутентификация EAP-TLS поддерживает динамическое управление WEP-ключом. Протокол TLS необходим для защиты и аутентификации коммуникаций в сетях общего пользования путем шифрования данных. Протокол квитирования TLS позволяет клиенту и серверу до посылки данных провести взаимную аутентификацию и выработать алгоритм и ключи шифрования.

TTLS

Эти настройки определяют протокол и идентификационную информацию, используемую для аутентификации пользователя. В аутентификации TTLS (Tunneled Transport Layer Security) клиент использует EAP-TLS для проверки подлинности сервера и создания канала между сервером и клиентом, шифрованного с помощью TLS. Клиент может использовать другой аутентификационный протокол. Обычно протоколы на основе паролей используются через необъявляемый, защищенный TLS-шифрованный канал. В настоящее время TTLS поддерживает все методы, применяемые в EAP, а также некоторые более старые методы (PAP, CHAP, MS-CHAP и MS-CHAP-V2). TTLS легко расширяется для работы с новыми протоколами посредством установки новых атрибутов для описания новых протоколов.

PEAP

PEAP - это новый аутентификационный протокол EAP (Extensible Authentication Protocol - EAP) стандарта IEEE 802.1X, разработанный для улучшения системы защиты EAP-Transport Layer Security (EAP-TLS) и поддержки различных методов аутентификации, включающих пароли пользователей, одноразовые пароли и карты доступа (Generic Token Cards).

LEAP

Версияпротоколааутентификации Extensible Authentication Protocol (EAP). LEAP (Light Extensible Authentication Protocol) представляет собой специальный расширяемый протокол аутентификации,

разработанный Cisco, который отвечает за обеспечение процедуры аутентификации "запрос/ответ" и назначение динамического ключа.

EAP-SIM

Протокол EAP-SIM (Extensible Authentication Protocol Method for GSM Subscriber Identity) - это механизм аутентификации и распространения ключей сеанса. Он использует модуль идентификации подписчика SIM (Subscriber Identity Module) системы глобального позиционирования для мобильных коммуникаций GSM (Global System for Mobile Communications). Аутентификация EAP-SIM использует динамический WEP-ключ, созданный специально для сеанса, полученный для шифрования данных от адаптера клиента или сервера RADIUS. Для EAP-SIM необходим специальный код проверки пользователя или PIN для обеспечения взаимодействия с SIM-картой (Subscriber Identity Module). SIM-карта - это специальная смарт-карта, которая используется в беспроводных цифровых сетях стандарта GSM (Global System for Mobile Communications). Описание протокола EAP-SIM представлено в документации RFC 4186.

EAP-AKA

Метод аутентификации EAP-AKA (Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement) - это механизм EAP, используемый для аутентификации и сеанса распространения ключей, используемый подписчиком модуля идентификации USIM (Subscriber Identity Module) универсальной мобильной телекоммуникационной системы UMTS (Universal Mobile Telecommunications System). Карта USIM - это специальная смарт-карта, предназначенная для проверки подлинности пользователей в сотовых сетях.

Протоколы аутентификации

PAP

Протокол PAP (Password Authentication Protocol) - двусторонний протокол обмена подтверждениями, предназначенный для использования с протоколом PPP. PAP является обычным текстовым паролем, используемым в более ранних системах SLIP. Он не защищен. Этот протокол доступен только для типа аутентификации TTLS.

CHAP

CHAP (Challenge Handshake Authentication Protocol) - это трехсторонний протокол обмена подтверждениями, предполагающий лучшую защиту, чем протокол аутентификации PAP (Password Authentication Protocol). Этот протокол доступен только для типа аутентификации **TTLS.**

MS-CHAP (MD4)

Использует версию Microsoft протокола RSA Message Digest 4. Работает только в системах Microsoft и позволяет осуществлять шифрование данных. Выбор этого метода аутентификации вызовет шифрование всех передаваемых данных. Этот протокол доступен только для типа аутентификации TTLS.

MS-CHAP-V2

Предоставляет дополнительную возможность для изменения пароля, недоступную с MS-CHAP-V1 или стандартной аутентификацией CHAP. Данная функция позволяет клиенту менять пароль учетной записи, если сервер RADIUS извещает о том, что срок действия пароля истек. Этот протокол доступен только для типов аутентификации TTLS и PEAP.

GTC (Generic Token Card)

Предлагает использование специальных пользовательских карт для аутентификации. Главная функция основана на аутентификации с помощью цифрового сертификата/специальной платы в GTC. Кроме того, в GTC имеется возможность скрытия идентификационной информации

пользователя во время использования шифрованного туннеля TLS, обеспечивающего дополнительную конфиденциальность, основанную на запрещении широкой рассылки имен пользователей на стадии аутентификации. Этот протокол доступен только для типа аутентификации PEAP.

TLS

Протокол TLS необходим для защиты и аутентификации коммуникаций в сетях общего пользования путем шифрования данных. Протокол квитирования TLS позволяет клиенту и серверу до посылки данных провести взаимную аутентификацию и выработать алгоритм и ключи шифрования. Этот протокол доступен только для типа аутентификации PEAP.

Функции Cisco.

Cisco LEAP.

Cisco LEAP (Cisco Light EAP) - это аутентификация сервера и клиента 802.1X с помощью пароля, предоставляемого пользователем. Когда точка доступа беспроводной сети взаимодействует с LEAP-совместимым сервером Cisco RADIUS (сервер Cisco Secure Access Control Server [ACS]), Cisco LEAP осуществляет управление доступом через взаимную аутентификацию между адаптерами WiFi клиентов и сетью, и предоставляет динамические, индивидуальные ключи шифрования пользователей для защиты конфиденциальности передаваемых данных.

Функция защиты точки доступа Cisco Rogue.

Функция "Cisco Rogue AP" обеспечивает защиту от попытки доступа фальшивой или недопустимой точки доступа, которая может имитировать реальную точку доступа в сети для получения идентификационной информации пользователей и протоколов аутентификации, нарушая тем самым целостность защиты сети. Эта функция работает только в среде аутентификации Cisco LEAP. Технология стандарта 802.11 не защищает сеть от несанкционированного доступа фальшивых точек доступа. Более подробную информацию см. в разделе Аутентификация LEAP.

Протокол безопасности в смешанных средах 802.11b и 802.11g.

Режим работы, когда некоторые точки доступа, например, Cisco 350 или Cisco 1200 поддерживают среды, в которых не все клиентские станции поддерживают WEP-шифрование, называется смешанным режимом (Mixed-Cell). Когда некоторые беспроводные сети работают в режиме "выборочного шифрования", клиентские станции, подключившиеся к сети в режиме WEP-шифрования, отправляют все сообщения в шифрованном виде, а станции, подключившиеся к сети в стандартном режиме, передают все сообщения нешифрованными. Эти точки доступа передают широковещательные сообщения нешифрованными, но позволяют клиентам использовать режим WEP-шифрования. Когда "смешанный режим" разрешен в профиле, вы можете подключиться к точке доступа, которая сконфигурирована для "дополнительного шифрования".

CKIP

Cisco Key Integrity Protocol (CKIP) - это собственный протокол защиты Cisco для шифрования в среде 802.11. Протокол CKIP использует следующие особенности для усовершенствования защиты 802.11 в режиме "infrastructure":

Быстрый роуминг (CCKM)

Когда беспроводная ЛС сконфигурирована для выполнения быстрого повторного подключения, клиент с активной поддержкой протокола LEAP может перемещаться от одной точки доступа к другой без вмешательства главного сервера. Используя централизованное управление Cisco (Cisco Centralized Key Management - CCKM), точка доступа, сконфигурированная для обеспечения работы беспроводной службы доменов (Wireless Domain Services - WDS), заменяет сервер RADIUS и аутентифицирует клиента без существенных задержек, которые возможны для голосовых или других, зависимых от времени приложений.

Управление радиообменом

Если эта функция включена, адаптер WiFi обеспечивает информацию управления радиообменом для режима Cisco infrastructure. Если программа Cisco Radio Management используется в сети "infrastructure", она конфигурирует параметры радиообмена, определяет уровень помех и фиктивные точки доступа.

EAP-FAST

EAP-FAST, подобно EAP-TTLS и PEAP, использует туннелирование для защиты сетевого трафика. Главным отличием является то, что EAP-FAST не использует сертификаты для аутентификации. Аутентификация в среде EAP-FAST представляет собой единственный коммуникационный обмен, инициируемый клиентом, когда идентификация EAP-FAST запрошена сервером. Если клиент не имеет предварительно опубликованного ключа PAC (Protected Access Credential), он может запросить аутентификационный обмен EAP-FAST для динамического получения ключа от сервера.

EAP-FAST имеет два метода доставки ключа PAC: доставка вручную с помощью внеполосного механизма и автоматического входа.

Механизмы доставки вручную представляются любым способом передачи, которые наиболее защищены и выбраны администратором.

Автоматический вход представляет собой туннелированный шифрованный канал, необходимый для обеспечения безопасной аутентификации клиента и доставки клиенту ключа PAC. Этот механизм не такой защищенный, как метод аутентификации вручную, но более надежен, чем аутентификация LEAP.

Метод EAP-FAST можно разделить на две части: вход и аутентификация. Фаза входа представляет собой начальную доставку клиенту ключа PAC. Эта часть нужна клиенту и пользователю только один раз.

Лабораторная работа № 9

Тема: «Создание виртуального интерфейса в сторону абонента»

Цель работы:изучить процедуру создания виртуального интерфейса в сторону абонента.

Порядок выполнения работы

Можно присвоить более чем один IP-адрес физическому сетевому интерфейсу. Эта техника очень полезна, например при работе с Apache и виртуальными хостами, так как позволяет получить доступ к одному и тому же серверу Apache с двух разных IP-адресов.

1. Временный виртуальный сетевой интерфейс

Процесс создания виртуального сетевого интерфейса в Linux не занимает много времени. Он включает один запуск команды ifconfig.

$ ifconfig eth0:0 123.123.22.22

Приведенная выше команда создает виртуальный сетевой интерфейс, базирующийся на оригинальном физическом сетевом интерфейсе eth0. Самое важное условие для создания виртуального сетевого интерфейса - должен существовать физический сетевой интерфейс, в нашем случае eth0. Ниже приведен полный пример:

 # ifconfig eth0
eth0 Link encap:Ethernet HWaddr 3c:97:0e:02:98:c8
inet addr:192.168.100.23 Bcast:192.168.100.255 Mask:255.255.255.0
 # ping 192.168.100.23
PING 192.168.100.23 (192.168.100.23) 56(84) bytes of data.
64 bytes from 192.168.100.23: icmp_req=1 ttl=64 time=0.023 ms
64 bytes from 192.168.100.23: icmp_req=2 ttl=64 time=0.059 m

Теперь мы можем настроить новый виртуальный интерфейс на базе eth0. После выполнения команды ifconfig новый виртуальный интерфейс готов к немедленному использованию.

 # ifconfig eth0:0
eth0:0 Link encap:Ethernet HWaddr 3c:97:0e:02:98:c8
UP BROADCAST MULTICAST MTU:1500 Metric:1
Interrupt:20 Memory:f1600000-f1620000

 # ifconfig eth0:0 123.123.22.22
 # ifconfig eth0:0
eth0:0 Link encap:Ethernet HWaddr 3c:97:0e:02:98:c8
inet addr:123.123.22.22 Bcast:123.255.255.255 Mask:255.0.0.0
 # ping 123.123.22.22
PING 123.123.22.22 (123.123.22.22) 56(84) bytes of data.
64 bytes from 123.123.22.22: icmp_req=1 ttl=64 time=0.060 ms
64 bytes from 123.123.22.22: icmp_req=2 ttl=64 time=0.057 ms

1.1. Отключение виртуального сетевого интерфейса

Для отключения нашего, созданного ранее, временного сетевого интерфейса мы можем также использовать команду ifconfig с флагом down.

 # ifconfig eth0:0 down

2. Присвоение виртуальному интерфейсу постоянного адреса

Описанные выше настройки не сохраняются после перезагрузки. Если вы хотите, чтобы виртуальный сетевой интерфейс работал постоянно, необходимо модифицировать конфигурационные файлы в соответствии с требованиями вашего дистрибутива Linux. Ниже описан этот процесс для самых распространенных дистрибутивов:

2.1. Debian / Ubuntu

2.1.1. Статический адрес

В Debian или Ubuntu вам необходимо отредактировать файл /etc/network/interfaces, добавив в него следующие строки:

iface eth0:0 inet static
address 123.123.22.22
netmask 255.0.0.0
broadcast 123.255.255.255

2.1.2. Dhcp

Возможно также использовать витруальный сетевой интерфейс с DHCP. В этом случае вам необходимо добавить в /etc/network/interfaces следующую строку:

iface eth0:0 inet dhcp

Для того, чтобы изменения вступили в силу, необходимо перезапустить сеть:

 # /etc/init.d/networking restart

2.2. Redhat / Fedora / CentOS

2.2.1. Статический адрес

В Redhat, Fedora или CentOS Linux директория, отвечающая за присвоение постоянных IP-адресов - это /etc/sysconfig/network-scripts. В этой директории необходимо создать файл, соответствующий вашему новому виртуальному интерфейсу. В нашем случае этот файл будет называться ifcfg-eth0:0. Создайте этот новый файл и вставьте в него приведенные ниже строки. После перезагрузки адрес будет присвоен виртуальному интерфейсу на постоянной основе.

DEVICE=eth0:0
IPADDR=123.123.22.22
NETMASK=255.0.0.0
NETWORK=123.0.0.0
BROADCAST=123.255.255.255
ONBOOT=yes

2.2.2. Dhcp

DEVICE=eth0:0
BOOTPROTO=dhcp
ONBOOT=yes

Когда закончите, перезапустите ваши интерфейсы:

 # service network restart

3. Заключение

Раньше один физический сервер обслуживал один веб-сайт. Сегодня такой способ хостинга уже не является жизнеспособным, поэтому способность операционной системы создавать виртуальные сетевые интерфейсы действительно необходима.

Лабораторная работа № 10

Тема: «Протоколы маршрутизации мультисервисных сетей.»
Цель работы:изучитьпротоколы маршрутизации мультисервисных сетей.».
Порядок выполнения работы

Протоколы маршрутизации в мультисервисных сетях

Поскольку протоколы маршрутизации определяют пути следования IP-пакетов, от них напрямую зависит, будет ли пакет доставлен вовремя и будет ли доставлен вообще. Они определяют и эффективность работы протоколов более высокого уровня, например TCP или SMTP, - будут ли те "страдать" от задержек или потери пакетов, дублирования дейтаграмм и прочих казусов, ответственность за возникновение которых несут службы маршрутизации. Проще говоря, успешная работа IP и элементов более высокого уровня зависит от эффективности IP-маршрутизации: если ее базовые службы не справляются со своими задачами, то нарушается работа всей системы. А если нарушается работа всей системы, то онлайновые покупатели не захотят возвращаться на ваш сайт, а ваши бизнес - подразделения не смогут вовремя получить нужную информацию.

1 Протокол OSPF

OSPF (англ. Open Shortest Path First) - протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути Алгоритм Дейкстры (Dijkstras algorithm).

Протокол OSPF был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 2328. Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol - IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.имеет следующие преимущества:
Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
Поддержка сетевых масок переменной длины (VLSM);
Оптимальное использование пропускной способности (т. к. строится минимальный остовный граф по алгоритму Дейкстры);

Описание работы протокола

1.Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых активирован OSPF. Маршрутизаторы, разделяющие общий канал передачи данных, становятся соседями, когда они приходят к договоренности об определённых параметрах, указанных вих hello-пакетах.

2.На следующем этапе работы протокола маршрутизаторы будут пытаться перейти в состояние смежности со своими соседями. Переход в состояние смежности определяется типом маршрутизаторов, обменивающихся hello-пакетами, и типом сети, по которой передаются hello-пакеты. OSPF определяет несколько типов сетей и несколько типов маршрутизаторов. Пара маршрутизаторов, находящихся в состоянии смежности, синхронизирует между собой базу данных состояния каналов.

.Каждый маршрутизатор посылает объявления о состоянии канала маршрутизаторам, с которыми он находится в состоянии смежности.

.Каждый маршрутизатор, получивший объявление от смежного маршрутизатора, записывает передаваемую в нём информацию в базу данных состояния каналов маршрутизатора и рассылает копию объявления всем другим смежным с ним маршрутизаторам.

.Рассылая объявления внутри одной OSPF-зоны, все маршрутизаторы строят идентичную базу данных состояния каналов маршрутизатора.

.Когда база данных построена, каждый маршрутизатор использует алгоритм "кратчайший путь первым" для вычисления графа без петель, который будет описывать кратчайший путь к каждому известному пункту назначения с собой в качестве корня. Этот граф - дерево кратчайших путей.

.Каждый маршрутизатор строит таблицу маршрутизации из своего дерева кратчайших путей

2 Протокол BGP

BGP (англ. Border Gateway Protocol, протокол граничного шлюза) - основной протокол динамической маршрутизации в Интернете.

Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС), то есть группами маршрутизаторов под единым техническим управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляет исходя из правил, принятых в сети.поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации. С 1994 года действует четвёртая версия протокола, все предыдущие версии являются устаревшими., наряду с DNS, является одним из главных механизмов, обеспечивающих функционирование Интернета.является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт 179). После установки соединения передаётся информация обо всех маршрутах, предназначенных для экспорта. В дальнейшем передаётся только информация об изменениях в таблицах маршрутизации. При закрытии соединения удаляются все маршруты, информация о которых передана противоположной стороной.

3 Протокол RIP

Протокол маршрутной информации (англ. Routing Information Protocol) - один из самых простых протоколов маршрутизации. Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

Алгоритм маршрутизации RIP (алгоритм Беллмана - Форда) был впервые разработан в 1969 году, как основной для сети ARPANET.

Прототиппротокола RIP - Gateway Information Protocol, частьпакета PARC Universal Packet.

Версия RIP, которая поддерживает протокол интернета была включена в пакет BSD операционной системы Unix под названием *routed* (route daemon), а также многими производителями, реализовавшими свою версию этого протокола. В итоге протокол был унифицирован в документе RFC 1058.

В 1994 году был разработан протокол *RIP2* (RFC 2453), который является расширением протокола RIP, обеспечивающим передачу дополнительной маршрутной информации в сообщениях RIP и повышающим уровень безопасности.

Для работы в среде IPv6 была разработана версия *RIPng*.- так называемый протокол дистанционно-векторной маршрутизации, который, оперирует *хопами* (ретрансляционными "скачками") в качестве метрики маршрутизации. Максимальное количество хопов, разрешенное в RIP - 15 (метрика 16 означает "бесконечно большую метрику"). Каждый RIP - маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи. RIP работает на прикладном уровне стека TCP/IP, используя UDP порт 520. В современных сетевых средах RIP - не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 хопов не дает применять его в больших сетях. Преимущество этого протокола - простота конфигурирования.

Методика проведения лабораторных работ.

При выполнении лабораторной работы каждого студента нужно обеспечить программным и теоретическим материалом, инструкцией к работе, где надо отразить, порядок и шаблон выполнения лабораторных работ, описанием работ. Текст задания лабораторных работ записывается в печатных документах, специализированным плакатах и методичках или в документе формата .pdf или .doc, открыв который студент найдёт для себя описание работы, вариант, инструкцию и другие необходимые материалы к данной работ.

В соответствии с учебно-методическими указаниями методика выполнения каждой лабораторной работы включает в себя следующие этапы:

1. Вводное слово преподавателя, в котором описывается порядок выполнения работы и обращается особое внимание на некоторые детали;

2. Самостоятельная подготовка к работе, в процессе которой студенты обязаны:

- уяснить цель и порядок выполнения лабораторной работы;

- изучить или повторить основные теоретические положения по изучаемой теме, для чего использовать конспект лекций, теоретические данные в тексте лабораторной, а также рекомендованные преподавателем учебные пособия. Качество своей подготовки можно оценить с помощью контрольных вопросов, приведённых в методическом указании к лабораторной работе;

- подготовить отчёт, форма которого дана в методическом указании.

3. Получение допуска на выполнение лабораторной работы. Допуск к лабораторной работе проводится преподавателем индивидуально с персональным опросом каждого студента. Для допуска:

-каждый студент предварительно оформляет свой персональный конспект данной лабораторной работы в рабочей тетради, учитывая соответствующие требования;

-преподаватель индивидуально проверяет оформление конспекта и задает вопросы по теории и методике выполнения заданий;

- студент устно отвечает на заданные вопросы;

- в случае готовности студента к работе преподаватель допускает его к работе и ставит свою подпись в конспекте у студента (графа Допуск в таблице на обложке). Студент, не подготовленный теоретически или не имеющий подготовленного шаблона отчета, к выполнению работы не допускается

4. Конспект для допуска к лабораторной работе готовится заранее в рабочей тетради.

5. Выполнение задания, номер варианта которого определяется преподавателем, в лаборатории с использованием автоматизированных рабочих мест.

6. Оформление лабораторной работы к зачету. Полностью оформленная и подготовленная к зачету работа должна соответствовать следующим требованиям:

- выполнение всех пунктов раздела «Задания» лабораторной работы;

- записаны ответы по установленной форме;

7. Получение зачета у преподавателя. После завершения работы отчет и выполненные практические задания предъявляются для проверки преподавателю, который своей подписью удостоверяет правильность результатов.

При подготовке к работе учащийся должен:

1. Ознакомиться с содержанием работы и изучить теоретические положения, на которых данная работа базируется.

2. Продумать методику снятия зависимостей, указанных в описании. Следует внимательно проследить по схеме, каким образом будет изменяться исходная величина, как она регулируется, и каким образом будет отсчитываться исследуемая величина.

3. Ознакомиться с исследуемым полупроводниковым прибором.

При выполнении работы учащийся обязан:

1. Познакомиться с рабочим местом, установить наличие необходимой аппаратуры, соединительных проводов, источников питания и вспомогательных приборов.

2. Выбрать соответствующую измерительную аппаратуру, определить пределы измерения, используя справочные материалы, издания на исследование.

3. Самостоятельно определить число отсчетов, необходимых для правильного воспроизведения исследуемой зависимости. На тех участках, где исследуемая величина резко изменяется или ее изменение соответствует особой точке (максимум, минимум, перегиб и т.д.),

надо брать от точки отсчета чаще, чем на тех участках, где исследуемая величина изменяется мало.

4. Собрать электрическую схему исследования. В процессе выполнения лабораторной работы учащийся должен произвести записи, проанализировать их и предоставить на проверку преподавателю.

5. К следующей лабораторной работе каждому учащемуся необходимо предоставить отчет по предыдущей работе, выполненный на специальном бланке. Отчет по работе аккуратно оформляется. Схемы вычерчиваются в соответствии с ЕСКД, графики выполняются на миллиметровой бумаге, на графике наносятся экспериментальные точки, по ним проводится плавная кривая.

6. Полученные зависимости необходимо сравнить со справочными и сделать необходимые выводы и расчеты по проделанной работе.

Содержание отчета по лабораторной работе

1.Фамилия и инициалы учащегося, номер группы и дата выполнения работы.

2.Наименование работы.

3.Содержание работы.

4.Электрические схемы исследования.

5.Описание конструкции исследуемого полупроводникового прибора.

6.Основные паспортные данные прибора.

7.Результаты измерений (в виде таблиц).

8.Графические зависимости и осциллограммы на миллиметровой бумаге.

9.Сопутствующие измерениям расчеты.

10.Перечень измерительной аппаратуры с указанием типа прибора, его заводского номера, предела измерения, цены деления.

11. Краткие выводы по проделанной работе.