

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Шебалин Тимур Александрович

Должность: Директор Пятигорского института (филиал) Северо-Кавказского

федерального университета

Дата подписания: 05.09.2023 14:13:37

Уникальный программный ключ:

d74ce93cd40e39275c3ba2f58486412a1c8ef96

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Пятигорский институт (филиал) СКФУ

Колледж Пятигорского института (филиала) СКФУ

«Компьютерные сети» МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

**Специальности СПО 09.02.07 Информационные системы и
программирование**

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Пятигорск 2021 г.

Методические указания для практических занятий по дисциплине «Компьютерные сети» составлены в соответствии с требованиями ФГОС СПО к подготовке выпуска для получения квалификации. Предназначены для студентов, обучающихся по специальности 09.02.07 Информационные системы и программирование.

Рассмотрено на заседании ПЦК Колледжа Пятигорского института (филиала) СКФУ

Протокол № 8 от «22» марта 2021г.

Практическая работа №1

Тема: Основные принципы построения компьютерных сетей.

Цель: Изучение понятий абсолютный, измерительный и относительный уровни передачи

1.1 Краткие теоретические сведения

Электрические сигналы количественно описываются мощностью, напряжением, током. В технике электросвязи принято пользоваться логарифмическими характеристиками (уровнями передачи). Уровни передачи, вычисленные посредством десятичных логарифмов, называются децибелами (дБ).

Уровни передачи по мощности, напряжению и току:

$$\begin{aligned} P_m = 10 \cdot \lg \frac{P_x}{P_0}, \quad P_n = 20 \cdot \lg \frac{U_x}{U_0}, \quad P_t = 20 \cdot \lg \frac{I_x}{I_0}, \\ P = \frac{U^2}{|Z|}, \quad P = I^2 \cdot |Z|, \end{aligned} \quad (1.1)$$

где P_x , U_x , I_x – величины мощности, напряжения и тока в рассматриваемой точке x ; P_0 , U_0 , I_0 – величины, принятые за исходные. За исходную величину принята мощность $P_0 = 1 \text{ мВт}$ (за эталонный уровень шума принята мощность в 1 пВт). Тогда при номинальном сопротивлении $|Z| = 600 \text{ Ом}$ действующие значения напряжения и тока соответственно равны $U_0 = 0,7746 \text{ В}$ и $I_0 = 1,291 \text{ мА}$.

Средняя мощность сигнала в общем случае равна

$$P_c = \frac{1}{T} \int_0^T I(t) U(t) dt. \quad (1.2)$$

При подаче на вход тракта гармонического сигнала с абсолютным уровнем, регламентированным для данного вида измерений, в точках тракта устанавливаются абсолютные уровни, которые называются *измерительными*. Значения измерительных уровней приводятся в технической документации. Они обозначаются дБм, дБн, дБт.

Иногда за исходные величины принимают значения P_n , U_n , I_n в начале тракта. Тогда вычисленные уровни

$$P_{m0} = 10 \cdot \lg \frac{P_x}{P_n} \quad (1.3)$$

называют относительными и обозначают как дБ_{0м}, дБ_{0н}, дБ_{0т}. Приведенные уровни совпадают с коэффициентом усиления по мощности, напряжению и тока. Если величины положительные, то имеет место усиление, если уровни отрицательные – то затухание.

При нормировании величин сигналов используют понятие точки нулевого относительного уровня по мощности (ТНОУ). Абсолютный уровень P_{M0} , определенный в ТНОУ, обозначается дБм0, и он равен $P_{M0} = P_H - P_H = 0$ дБм0.

Тогда нормированный уровень в измерительной точке равен: $P_{M0} = P_{изм} - P_H$.

Остаточное затухание – это рабочее затухание канала, определяемое как разность между суммой всех затуханий и суммой всех усилений в канале на заданной частоте. Имея ввиду равенство входного и выходного сопротивлений канала, остаточное затухание можно определить как разность уровней передачи

$$a_{ост} = P_{вх} - P_{вых} \quad (1.4)$$

1.2. Задание к лабораторной работе

1.2.1. Рассчитать аттенюатор, приведенный на рис. 1.1. Исходные данные взять из табл. 1.1 согласно варианту задания.

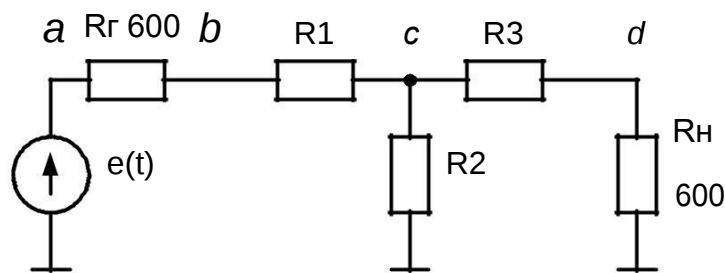


Рис. 1.1. Схема исследуемого аттенюатора

Табл. 1.1

Варианты заданий

№ варианта	Ослабление, дБ	$\frac{R1}{R2} = \frac{R3}{R2}$, Ом	$\frac{R2}{R2}$, Ом
1	1	0,0575	8,668
2	2	0,1147	4,305
3	3	0,1708	2,838
4	4	0,2263	2,097
5	5	0,2800	1,645
6	6	0,3323	1,339
7	7	0,3823	1,117
8	8	0,4305	0,9458
9	9	0,4762	0,8118
10	10	0,5195	0,7032

1.2.2. Открыть файл АТТ.ewb.

1.2.3. Измерить мощность сигнала в точках $a - d$. Результаты измерений занести в табл. 1.2. За ТНОУ принять вход аттенюатора (точка b).

Табл. 1.2

Результаты измерений

Уровень сигнала	P_a	P_b	P_c	P_d
Мощность сигнала, Вт				
Измерительный уровень, дБ				
Относительный уровень, дБ				
Нормированный относительный уровень, дБ				

1.2.4. Определить остаточное затухание исследуемого аттенюатора.

1.2.5. Установить на входе аттенюатора эталонный уровень 1 мВт. Повторить п. 1.2.3.

1.2.6. Открыть файл АТТ1.ewb. Измерить среднюю мощность шума на нагрузке 1 Ом. Найти измерительный уровень шума.

Замечание. В процессе измерения использовать режим расчета переходных процессов (Analysis/ Transient). Время анализа установить 1 с.

1.2.7. Оформить отчет, сделать выводы по работе.

1.3. Контрольные вопросы

1. Дайте понятие уровню передачи.
2. Что такое остаточное затухание?
3. Назовите причины использования логарифмических единиц измерения.
4. Для чего используется психометрическое взвешивание при измерении мощности шума.
5. Перечислите источники шума в телефонных линиях связи.

Практическая работа №2

Тема: Сетевые архитектуры: типы, топологии, методы доступа к среде передачи.

Цель работы: Приобретение навыков классификации и анализа IP-адресов.

Ход выполнения работы:

В IP-сетях все сетевые устройства (хосты, серверы, шлюзы, маршрутизаторы и т.д.) получают [уникальные IP-адреса](#).

IP-адрес состоит из **4-х байтов (32 битов)**. Этот адрес используется на сетевом уровне эталонной модели OSI. Он [делится на две части](#).

Первая часть IP-адреса задаёт сеть, в которой располагается сетевое устройство.

Вторая часть IP-адреса однозначно задаёт само сетевое устройство. Для обозначения сетевых устройств используют различные термины:

хост;

сетевой интерфейс.

0 1 2 ...		... 29 30 31
Ключ	Номер сети	Номер устройства в сети

Адресное пространство IP-протокола делится на три класса - **A**, **B**, **C**.

Адрес класса **A**:

0	1 2 3 ... 7	8 ...	... 29 30 31
0			
Номер сети		Номер устройства	

Адрес класса **B**:

0 1	2 3 4 ...	...15	16...	31	... 29 30
10					
Номер сети			Номер устройства		

Адрес класса **C**:

0 1 2	3 4 5 ...	...23	24...	... 29 30
110				31
Номер сети			Номер устр-ва	

IP-АДРЕСА КЛАССА **A**.

Сети класса A имеют 8-битный сетевой префикс «/8».

Структура адреса класса **A**:

0	1 2 3 ... 7	8 ...	... 29 30 31
0			
Номер сети		Номер устройства	

Максимальное число сетей класса **A** составляет $2^7 - 2 = 126$.

Каждая сеть класса **A** поддерживает до $2^{24} - 2 = 16\,777\,214$ сетевых устройств.

Адресное пространство, выделенное классу **A**, занимает 50% общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса **A** приведён ниже.

Класс адреса	Диапазон значений
A	1.0.0.0—126.255.255.255

Примеры адресов сетей класса **A**:

1.100.120.148

98.180.220.250

121.196.244.198

IP-АДРЕСА КЛАССА В.

Сети класса В имеют 16-битный сетевой префикс «/16».

Структура адреса класса В:

0 1	2 3 4 ...	...15	16...	... 29 30 31
10				
Номер сети			Номер устройства	

Максимальное число сетей класса В составляет $2^{14} = 16384$.

Каждая сеть класса В поддерживает до $2^{16} - 2 = 65\,534$ сетевых устройств.

Адресное пространство, выделенное классу В, занимает 25% общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса В приведён ниже.

Класс адреса	Диапазон значений
В	128.0.0.0—191.255.255.255

Примеры адресов сетей класса В:

128.100.120.148

164.180.220.250

190.196.244.198

IP-АДРЕСА КЛАССА С.

Сети класса С имеют 24-битный сетевой префикс «/24».

Структура адреса класса С:

0 1 2	3 4 5 ...	...23	24...	... 29 30 31
110				
Номер сети			Номер устр-ва	

Максимальное число сетей класса С составляет

$2^{21} = 2\,097\,152$.

Каждая сеть класса С поддерживает до $2^8 - 2 = 254$ сетевых устройств.

Адресное пространство, выделенное классу С, занимает 12.5% общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса С приведён ниже.

Класс адреса	Диапазон значений
--------------	-------------------

C	192.0.0.0—223.255.255.255
----------	----------------------------------

Примеры адресов сетей класса **C**:

192.100.120.148

212.180.220.250

223.196.244.198

ОСТАЛЬНЫЕ IP-АДРЕСА.

Оставшийся резерв IP-адресов отводится следующим классам сетей:

Класс адреса	Диапазон значений
D	224.0.0.0—239.255.255.255
E	240.0.0.0—247.255.255.255
Резерв	248.0.0.0—254.255.255.255

В сетях класса **D** первые (0..3) биты адреса имеют значение **1110**. Адреса этого класса используются для поддержки групповой передачи данных.

В сетях класса **E** первые (0..4) биты адреса имеют значение **11110**. Адреса этого класса зарезервированы для экспериментального использования.

ЗАПИСЬ IP-АДРЕСА В РАЗЛИЧНЫХ НОТАЦИЯХ.

Запись IP-адресов.

Примеры записи IP-адресов

в 2-ой,

16-ой,

точно-десятичной нотациях:

0111 1001	1100 0100	1111 0100	1100 0110
79	C4	F4	C6

121.196.244.198

1001 1001	1110 0110	1101 1010	1011 0111
99	E6	DA	B7

153.230.218.183

1101 1110	0110 0101	0111 0101	1100 0110
DE	65	75	78

222.101.117.120

МАСКА СЕТИ.

Маска сети представляет собою 32-разрядный адрес, 8, 16, 24 старших разрядов которого заполнены "1".

Маски сетей классов **A**, **B**, **C** представлены ниже:

Маска IP-адресов класса **A**:

0 1 2 3 ... 7	8 ... 31	... 29 30
11111111	00000000 00000000 00000000	
FF	00 00 00	
255.0.0.0		
Маска сети	Номер устройства	

Маска IP-адресов класса **B**:

0 1 2 3 4... ...15	16... ... 29 30 31
11111111 11111111	00000000 00000000
FF FF	00 00
255.255.0 . 0	
Маска сети	Номер устройства

Маска IP-адресов класса **C**:

0 1 2 3 4 5... ...23	24... ... 29 30 31
11111111 11111111 11111111	00000000
FF FF FF	00
255.255.255. 0	
Маска сети	Номер устр-ва

ПРИМЕРЫ МАСОК СЕТЕЙ:

IP-адрес	Маска
192.100.120.148	255.255.255.0
10.190.178.177	255.0.0.0
144.100.137.125	255.255.0.0
123.119.137.223	255.0.0.0
222.110.170.190	255.255.255.0

СПЕЦИАЛЬНЫЕ IP-АДРЕСА.

Некоторые IP-адреса используются для специальных целей.

IP-адрес	Пояснение
0.0.0.0	Данный хост (любой сети)
0.200.150.100	Хост данной сети (класс А)
0.0.150.100	Хост данной сети (класс В)
0.0.0.100	Хост данной сети (класс С)
100.0.0.0	IP-адрес сети (класс А)
150.200.0.0	IP-адрес сети (класс В)
200.220.240.0	IP-адрес сети (класс С)
255.255.255.255	Широковещание в данной сети (любого класса)
100.255.255.255	Широковещание в удаленной сети класса А
150.200.255.255	Широковещание в удаленной сети класса В
200.220.240.255	Широковещание в удаленной сети класса С
127.X.X.X	Тестирование сетевого программного обеспечения

IP-АДРЕСАЦИЯ В ПОДСЕТЯХ

По мере роста сети Интернет всё острее стала ощущаться нехватка сетевых адресов. В 1985 году данная проблема была разрешена посредством [введения подсетей](#).

Подсети формировались посредством деления IP-адреса на части, именно: **номер сетевого устройства** сети делится на 2 части:

- **номер подсети**;
- **номер сетевого интерфейса** в этой подсети.

2-х уровневая сетевая иерархия (без подсетей):

№ сети	№ хоста в сети
--------	----------------

3-х уровневая сетевая иерархия (с подсетями):

№ сети	№ подсети	№ хоста в подсети
--------	-----------	-------------------

Внешние маршрутизаторы (внешние по отношению к сети с заданным №) используют деление IP-адреса на **2 части**: № сети и № хоста в сети ([как будто никаких подсетей нет](#)).

Внутренние маршрутизаторы (функционирующие внутри сети с заданным №) используют деление IP-адреса на **3 части**: № сети, № конкретной подсети и № конкретного хоста в конкретной подсети.

Внешние маршрутизаторы используют в качестве [сетевого префикса](#) только адрес сети:

Сетевой префикс	
№ сети	№ хоста в сети

Внутренние маршрутизаторы используют так называемый [расширенный сетевой префикс](#), включающий как адрес сети, так и подсети:

Расширенный сетевой префикс		
№ сети	№ подсети	№ хоста в подсети

[Пример.](#)

Предположим, в сети класса **В**, сетевой префикс которой имеет значение **150.160.0.0**, сетевой администратор **3-ий байт** сетевого адреса отвлёл под адреса подсетей:

1-ый и 2-ой байты	3-ий байт	4-ый байт0
-------------------	-----------	------------

№ сети	№ подсети	№ хоста
В этом случае мы получаем следующие параметры сетевой архитектуры: - класс сети: B; - размер сетевого префикса: 16 разрядов; - маска сети: 255.255.0.0; - адрес сети: 150.160.0.0/16; - размер расширенного сетевого префикса: 24 разряда; - маска подсетей: 255.255.255.0; - адреса подсетей: 150.160.0.0/24; 150.160.1.0/24; 150.160.2.0/24; ... ; 150.160.254.0/24; 150.160.255.0/24.		

ТИПОВОЕ ЗАДАНИЕ

<u>Условие:</u> По заданному IP-адресу: 120.140.160.170/14 определить следующие параметры сетевой архитектуры: - Класс сети. - Маску сети. - Адрес сети. - Размер расширенного сетевого префикса. - Маску подсети. - Адрес подсети. - Адрес хоста. <u>Решение:</u> - Класс A (так как 0 < 120 < 127). - Маска сети: 255.0.0.0. - Адрес сети: 120.0.0.0. - Размер расширенного сетевого префикса: 14 разрядов. - Так как размер расширенного сетевого префикса составляет 14 разрядов, маска подсети, представленная в 2-ой системе счисления, состоит из 14 "1" и (32 - 14 = 18) 18 "0": <table> <tr> <td colspan="2">14 разрядов маски подсети</td><td colspan="2">18 разрядов сетевого адреса хоста</td></tr> <tr> <td>1111 1111</td><td>1111 1100</td><td>0000 0000</td><td>0000 0000</td></tr> <tr> <td>F F</td><td>F C</td><td>0 0</td><td>0 0</td></tr> <tr> <td>255.</td><td>252.</td><td>0.</td><td>0</td></tr> </table> 6. Адрес подсети определяется первыми 14 разрядами заданного IP-адреса. Остальные 18 разрядов заполняются "0": <table> <tr> <td colspan="2">14 сетевых разрядов</td><td colspan="2">18 разрядов хоста</td></tr> <tr> <td>0111 1000</td><td>1000 1100</td><td>0000 0000</td><td>0000 0000</td></tr> <tr> <td>7 8</td><td>8 C</td><td>0 0</td><td>0 0</td></tr> <tr> <td>120.</td><td>140.</td><td>0.</td><td>0</td></tr> </table> 7. Адрес хоста определяется первыми 14 "0" и 18 остальными разрядами заданного				14 разрядов маски подсети		18 разрядов сетевого адреса хоста		1111 1111	1111 1100	0000 0000	0000 0000	F F	F C	0 0	0 0	255.	252.	0.	0	14 сетевых разрядов		18 разрядов хоста		0111 1000	1000 1100	0000 0000	0000 0000	7 8	8 C	0 0	0 0	120.	140.	0.	0
14 разрядов маски подсети		18 разрядов сетевого адреса хоста																																	
1111 1111	1111 1100	0000 0000	0000 0000																																
F F	F C	0 0	0 0																																
255.	252.	0.	0																																
14 сетевых разрядов		18 разрядов хоста																																	
0111 1000	1000 1100	0000 0000	0000 0000																																
7 8	8 C	0 0	0 0																																
120.	140.	0.	0																																

IP-адреса:

14 сетевых разрядов		18 разрядов хоста	
0000 0000	0000 0000	1010 0000	0000 0000
0 0	0 0	A 0	A A
0.	0.	160.	170

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Определить параметры сетевой архитектуры:

1. Класс сети.
2. Маску сети.
3. Адрес сети.
4. Размер расширенного сетевого префикса.
5. Маску подсети.
6. Адрес подсети.
7. Адрес хоста.

по заданному IP-адресу:

1. 100.110.120.130/10
2. 140.160.180.200/18
3. 160.180.200.220/22
4. 180.200.220.240/26
5. 200.210.220.230/27

Практическая работа №3

Тема: Технологии локальных сетей.

Цель работы: Построить локальную сеть с использованием коммутатора.

ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

Теоретические основы

Сетевой коммутатор или **свитч** (жарг. от англ. switch — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю,

исключение составляет широковещательный трафик (на MAC-адрес FF:FF:FF:FF:FF:FF) всем узлам сети. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались [1].

Коммутатор работает на канальном уровне модели OSI, и потому в общем случае может только объединять узлы одной сети по их MAC-адресам. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы [1].

Принцип работы коммутатора

Коммутатор хранит в памяти таблицу коммутации (хранящуюся в ассоциативной памяти), в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует кадры и, определив MAC-адрес хоста-отправителя, заносит его в таблицу. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя ещё не известен, то кадр будет продублирован на все интерфейсы. Со временем коммутатор строит полную таблицу для всех своих портов, и в результате трафик локализуется. Стоит отметить малую латентность и высокую скорость пересылки на каждом порту интерфейса [1].

Режимы коммутации

Существует три способа коммутации. Каждый из них — это комбинация таких параметров, как время ожидания и надёжность передачи.

С промежуточным хранением (Store and Forward). Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.

Сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.

Бесфрагментный (fragment-free) или гибридный. Этот режим является модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (кадр размером 64 байта обрабатывается по технологии store-and-forward, остальные по технологии cut-through).

Латентность, связанная с «принятием коммутатором решения», добавляется к времени, которое требуется кадру для входа на порт коммутатора и выхода с него и вместе с ним определяет общую задержку коммутатора.

Концентратор, который выполняет только пересылку кадра (не выполняет фильтрации и не принимает никаких решений) имеет лишь задержку, связанную с передачей кадра с одного порта на другой [1].

Симметричная и асимметричная коммутация

Свойство симметрии при коммутации позволяет дать характеристику коммутатора с точки зрения ширины полосы пропускания для каждого его порта. Симметричный коммутатор обеспечивает коммутируемые соединения между портами с одинаковой шириной полосы пропускания, например, когда все порты имеют ширину пропускания 10 Мб/с или 100 Мб/с.

Асимметричный коммутатор обеспечивает коммутируемые соединения между портами с различной шириной полосы пропускания, например, в случаях комбинации портов с шириной полосы пропускания 10 Мб/с и 100 Мб/с или 100 Мб/с и 1000 Мб/с.

Асимметричная коммутация используется в случае наличия больших сетевых потоков типа клиент-сервер, когда многочисленные пользователи обмениваются информацией с сервером одновременно, что требует большей ширины пропускания для того порта коммутатора, к которому подсоединен сервер, с целью предотвращения переполнения на этом порте. Для того, чтобы направить поток данных с порта 100 Мб/с на порт 10 Мб/с без опасности переполнения на последнем, асимметричный коммутатор должен иметь буфер памяти.

Асимметричный коммутатор также необходим для обеспечения большей ширины полосы пропускания каналов между коммутаторами, осуществляемых через вертикальные кросс-соединения или каналов между сегментами магистрали [1].

Буфер памяти

Для временного хранения пакетов и последующей их отправки по нужному адресу коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. Буфером называется область памяти, в которой коммутатор хранит передаваемые данные.

Буфер памяти может использовать два метода хранения и отправки пакетов — буферизация по портам и буферизация с общей памятью. При буферизации по портам, пакеты хранятся в очередях (queue), которые связаны с отдельными входными портами. Пакет передается на выходной порт только тогда, когда все пакеты, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один пакет задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные пакеты могут быть переданы на открытые порты их пунктов назначения.

При буферизации в общей памяти, все пакеты хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. Такой метод называется динамическим распределением буферной памяти. После этого пакеты, находившиеся в буфере динамически распределяются по выходным портам. Это позволяет получить пакет на одном порте и отправить его с другого порта, не устанавливая его в очередь.

Коммутатор поддерживает карту портов, в которые требуется отправить

пакеты. Очистка этой карты происходит только после того, как пакет успешно отправлен.

Поскольку память буфера является общей, размер пакета ограничивается всем размером буфера, а не долей предназначенной для конкретного порта. Это означает, что крупные пакеты, могут быть переданы с меньшими потерями, что особенно важно при асимметричной коммутации, т. е. когда порт с шириной полосы пропускания 100 Мб/с должен отправлять пакеты на порт 10 Мб/с [1].

Проведение работы

1. Установить IP адрес для «Рабочее место №1».

- 1.1 На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».
- 1.2 «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сети» и выбрать «Свойства».
- 1.3 Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».
- 1.4 Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.1. В поле «Маска подсети» ввести 255.255.255.0.
- 1.5 Нажать «ОК».
- 1.6 Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.
- 1.7 После того как последнее окно закроется настройка IP – адреса завершена.

2. Установить IP адрес для «Рабочее место №2».

- 2.1 На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».
- 2.2 «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сети» и выбрать «Свойства».
- 2.3 Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».
- 2.4 Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.2. В поле «Маска подсети» ввести 255.255.255.0.
- 2.5 Нажать «ОК».
- 2.6 Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.
- 2.7 После того как последнее окно закроется настройка IP – адреса завершена.

3. Установить IP адрес для «Рабочее место №3».

- 3.1 На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».
- 3.2 «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сет»

и выбрать «Свойства».

3.3 Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».

3.4 Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.10. В поле «Маска подсети» ввести 255.255.255.0.

3.5 Нажать «ОК».

3.6 Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.

3.7 После того как последнее окно закроется настройка IP – адреса завершена.

4. Перевести «Рабочее место №1» в новую группу CLASS.

4.1 Щелкнуть правой кнопкой мыши на ярлыке «Мой компьютер», выбрать «Свойства».

4.2 Перейти на вкладку «Имя компьютера», нажать кнопку «Изменить».

4.3 В поле «Рабочая группа», ввести имя рабочей группы CLASS.

4.4 Нажать кнопку «ОК».

4.5 Нажать кнопку «ОК».

5. Перевести «Рабочее место №2» в новую группу CLASS.

4.1 Щелкнуть правой кнопкой мыши на ярлыке «Мой компьютер», выбрать «Свойства».

4.2 Перейти на вкладку «Имя компьютера», нажать кнопку «Изменить».

4.3 В поле «Рабочая группа», ввести имя рабочей группы CLASS.

4.4 Нажать кнопку «ОК».

4.5 Нажать кнопку «ОК».

6. Перевести «Рабочее место №3» в новую группу CLASS.

4.1 Щелкнуть правой кнопкой мыши на ярлыке «Мой компьютер», выбрать «Свойства».

4.2 Перейти на вкладку «Имя компьютера», нажать кнопку «Изменить».

4.3 В поле «Рабочая группа», ввести имя рабочей группы CLASS.

4.4 Нажать кнопку «ОК».

4.5 Нажать кнопку «ОК».

7. Подключить рабочие места в единую сеть.

7.1 Используя патчкорд, соединить *двенадцатый* порт патч-панели, расположенной горизонтально на рабочем месте №1 и *третий* порт патч-панели №2, расположенной на рабочем месте №2.

7.2 Используя патчкорд, соединить *двенадцатый* порт патч-панели, расположенной горизонтально на рабочем месте №2 и *четвертый* порт патч-панели №2.

7.3 Используя патчкорд, соединить *двенадцатый* порт патч-панели, расположенной горизонтально на рабочем месте №3 и *пятый* порт патч-панели №2, расположенной на рабочем месте №2.

8. Проверяем соединение на рабочем месте №1.
 - 8.1 На рабочем столе нажать кнопку «Пуск» → «Выполнить».
 - 8.2 В появившемся окне, в поле «Открыть», ввести «cmd». Нажать «Enter».
 - 8.3 В командной строке ввести «ping 192.168.0.2». Нажать «Enter».
 - 8.4 Проверить наличие соединения.
 - 8.3 В командной строке ввести «ping 192.168.0.10». Нажать «Enter».
 - 8.4 Проверить наличие соединения.
9. Проверяем соединение на рабочем месте №2.
 - 9.1 На рабочем столе нажать кнопку «Пуск» → «Выполнить».
 - 9.2 В появившемся окне, в поле «Открыть», ввести «cmd». Нажать «Enter».
 - 9.3 В командной строке ввести «ping 192.168.0.1». Нажать «Enter».
 - 9.4 Проверить наличие соединения.
 - 9.3 В командной строке ввести «ping 192.168.0.10». Нажать «Enter».
 - 9.4 Проверить наличие соединения.
10. Проверяем соединение на рабочем месте №3.
 - 10.1 На рабочем столе нажать кнопку «Пуск» → «Выполнить».
 - 10.2 В появившемся окне, в поле «Открыть», ввести «cmd». Нажать «Enter».
 - 10.3 В командной строке ввести «ping 192.168.0.1». Нажать «Enter».
 - 10.4 Проверить наличие соединения.
 - 10.3 В командной строке ввести «ping 192.168.0.2». Нажать «Enter».
 - 10.4 Проверить наличие соединения.
11. Вывод: Из пунктов 8,9,10 видно, что нам удалось соединить три рабочих места в единую сеть, используя коммутатор.

Контрольные вопросы

1. Что такое сетевой коммутатор или свитч
2. Принцип работы коммутатора.
3. Опишите, как строится таблица коммутации
4. Опишите режим коммутации с промежуточным хранением
5. Опишите сквозной режим коммутации
6. Опишите бесфрагментный режим коммутации
7. Различие между симметричной и асимметричной коммутацией.
8. Когда используется асимметричная коммутация
9. Опишите, как используется буфер памяти при коммутации
10. Охарактеризуйте буферизацию по портам
11. Охарактеризуйте буферизацию в общей памяти

Практическая работа №4

Тема: Понятие сетевой модели. Сетевая модель OSI.

Цель : Построить беспроводную локальную сеть, используя две точки доступа.

Теоретические основы

Беспроводная точка доступа (англ. Wireless Access Point, WAP) — устройство для объединения компьютеров в единую беспроводную сеть [1].

Использование

Чаще всего беспроводные точки доступа используются для предоставления доступа мобильным устройствам (ноутбуки, принтеры и др.) к стационарной локальной сети.

Также беспроводные точки доступа часто используются для создания так называемых «горячих точек» — областей, в пределах которых клиенту предоставляется, как правило, бесплатный доступ к сети Интернет. Обычно такие точки находятся в библиотеках, аэропортах, уличных кафе крупных городов.

В последнее время наблюдается повышение интереса к беспроводным точкам доступа при создании домашних сетей. Для создания такой сети в пределах одной квартиры достаточно одной точки доступа. Возможно, этого будет достаточно для включения в сеть и соседей прилегающих квартир. Для включения в сеть квартиры через одну, определенно, потребуется ещё одна точка доступа, которая будет служить ретранслятором сигнала, ослабевшего вследствие прохождения через несущую стену [1].

Конструкция

Это устройство во многом аналогично клиентскому адаптеру. Как и последний, оно состоит из приёмопередатчика и интегрированного интерфейсного чипа, но наделено большим количеством интеллектуальных функций и более сложной электроникой.

Конструктивно точки доступа могут быть выполнены как для наружного использования (защищённый от воздействий внешней среды вариант), так и для использования внутри деловых и жилых помещений. Также существуют устройства, предназначенные для промышленного использования, учитывающие специфику производства.

Что касается функциональности, у различных точек доступа она может существенно различаться, иногда предоставляя средства диагностики и контроля сети, удалённой настройки и устранения неисправностей. Кроме того, в последнее время появились точки доступа, позволяющие производить многопользовательский обмен файлами (их трансляцию), минуя сервер.

На конец 2009 можно говорить о растущей популярности комбинированных устройств, интегрирующих в себе функции собственно беспроводного сетевого адаптера (платы, карты, контроллера), маршрутизатора и, например, кабельного модема [1].

Применение

Точки доступа призваны выполнять самые разнообразные функции, как для подключения группы компьютеров (каждый с беспроводным сетевым адаптером) в самостоятельные сети (режим Ad-hoc), так и для выполнения

функции моста между беспроводными и кабельными участками сети (режим Infrastructure).

Для режима Ad-hoc максимально возможное количество станций — 256. В Infrastructure-режиме допустимо до 2048 беспроводных узлов. На практике, одна точка доступа может обслуживать не более 15 клиентов одновременно.

Следует учитывать, что точка доступа — это обычный концентратор. При нескольких подключениях к одной точке полоса пропускания делится на количество подключённых пользователей. Теоретически ограничений на количество подключений нет, но на практике стоит ограничиться, исходя из минимально необходимой скорости передачи данных для каждого пользователя.

С помощью точки доступа можно легко организовать роуминг при перемещении мобильного компьютера пользователя в зоне охвата большей, чем зона охвата одной точки доступа, организовав «соты» из нескольких точек доступа и обеспечив перекрытие их зон действия. В этом случае необходимо обеспечить, чтобы в предполагаемой зоне перемещения мобильного пользователя все точки доступа и мобильные компьютеры имели одинаковые настройки (номера каналов, идентификаторы и др.) [1].

Пример применения

Если вам требуется не только объединить компьютеры в беспроводную сеть, но и соединить этот сегмент сети с проводным, то самый простой способ — установка так называемой «точки доступа». При использовании точки доступа, вы фактически имеете выделенное сетевое устройство, работа которого не зависит ни от загруженности других ПК, ни от их конфигурации, что является несомненным плюсом. Вам не придётся выполнять настройки сложного программного обеспечения, или опасаться, что компьютер окажется в очередной раз выключенным, а необходимая служба не будет запущена [1].

Стандарты

Самыми популярными стандартами для точек доступа являются Wi-Fi (802.11a/b/g/n) и Bluetooth. В технологии Bluetooth существует специальный профиль PAN (Personal Area Network) для этих целей [1].

Проведение работы

1. Настроить беспроводную точку доступа на рабочем месте №1.

1.1 Используя патчкорд, соединить *двенадцатый* порт патч-панели, расположенной горизонтально на рабочем месте №1 и *второй* порт патч-панели №1.

1.2 Установить IP -адрес ПК 192.168.0.1.

2.7.1. На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».

2.7.2. «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сет» и выбрать «Свойства».

2.7.3. Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».

2.7.4. Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.1. В поле «Маска подсети» ввести 255.255.255.0.

2.7.5. Нажать «ОК».

2.7.6. Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.

После того как последнее окно закроется настройка IP – адреса завершена.

1.3 На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».

1.4 В строке «Адрес» ввести: «192.168.0.50» и нажать «Enter».

1.5 В окне «Подключение к 192.168.0.50», ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».

1.6 На загрузившейся странице выбрать кнопку «Wireless».

1.7 Выставить настройки согласно таблице 1:

Таблица 1.

Название	Значение
Mode	Access Point
Wireless Network Name	DWL-2100AP
Authentication	WPA-PSK
Pass Phrase	123456789

1.8 Нажать «Apply». Подождать 30 секунд.

1.9 В окне «Подключение к 192.168.0.50», ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».

1. На загрузившейся странице выбрать кнопку «LAN».

1.11 Выставить настройки согласно таблице 2:

Таблица 2.

Название	Значение
Get IP From	Static
IP Address	192.168.0.55
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1

1.12 Нажать «Apply». Подождать 30 секунд.

1.13 Точка настроена.

2. Настроить беспроводную точку доступа на рабочем месте №2.

2.1 Используя патчкорд, соединить двенадцатый порт патч-панели, расположенной горизонтально на рабочем месте №2 и второй порт патч-панели №2.

2.2 Установить IP -адрес ПК 192.168.0.2.

- 1.2.1 На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».
 - 1.2.2 «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сет» и выбрать «Свойства».
 - 1.2.3 Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».
 - 1.2.4 Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.2. В поле «Маска подсети» ввести 255.255.255.0.
 - 1.2.5 Нажать «ОК».
 - 1.2.6 Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.
- После того как последнее окно закроется настройка IP – адреса завершена.

- 2.3 На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».
- 2.4 В строке «Адрес» ввести: «192.168.0.50» и нажать «Enter».
- 2.5 В окне «Подключение к 192.168.0.50», ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».
- 2.6 На загрузившейся странице выбрать кнопку «Wireless».
- 2.7 Выставить настройки согласно таблице 3:

Таблица 3.

Название	Значение
Mode	Wireless Client
Authentication	WPA-PSK
Pass Phrase	123456789

- 2.8 Нажать «Apply». Подождать 30 секунд.
 - 2.9 В окне «Подключение к 192.168.0.50», ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».
 - 2.10 На загрузившейся странице выбрать кнопку «Wireless».
 - 2.11 Нажать кнопку «Scan». Дождаться появления доступных сетей.
 - 2.12 Из появившегося списка, выбрать точку доступа с именем DWL-2100AP.
 - 2.13 Нажать «Apply». Подождать 30 секунд.
3. Проверяем соединение на рабочем месте №1.
 - 3.1 На рабочем столе нажать кнопку «Пуск» → «Выполнить».
 - 3.2 В появившемся окне, в поле «Открыть», ввести «cmd». Нажать «Enter».
 - 3.3 В командной строке ввести «ping 192.168.0.2». Нажать «Enter».
 - 3.4 Проверить наличие соединения.
 4. Проверяем соединение на рабочем месте №2.
 - 4.1 На рабочем столе нажать кнопку «Пуск» → «Выполнить».
 - 4.2 В появившемся окне, в поле «Открыть», ввести «cmd». Нажать «Enter».

4.3В командной строке ввести «ping 192.168.0.1». Нажать «Enter».

4.4Проверить наличие соединения.

5. Вывод: Из пунктов 3 и 4 следует, что нам удалось построить беспроводную локальную сеть, используя две точки доступа.

Контрольные вопросы

1. Для чего используют беспроводные точки доступа?
2. Конструктивное исполнение беспроводных точек доступа
3. Основные функции беспроводных точек доступа
4. Два режима использования беспроводных точек доступа
5. Как обеспечить роуминг с использованием беспроводных точек доступа
6. Опишите стандарты беспроводной связи.

Практическая работа №5

Тема: Адресация в сетях.

Цель: Получить представление и навыки кроссплатформенным программным обеспечением

Теоретические основы

Принт-сервер - это устройство, позволяющее группе пользователей проводных и беспроводных сетей совместно использовать принтер дома или в офисе. Имеет высокоскоростной порт USB 2.0, LPT или COM порты для подключения принтера. Как правило, оснащено интерфейсом 10/100BASE Ethernet и часто - высокоскоростным интерфейсом беспроводных сетей 802.11g. Поддерживая множество сетевых операционных систем, придает высокий уровень гибкости и производительности процессу печати [1].

Как правило, подключение к локальной сети осуществляется через порт 10/100Мбит/с Fast Ethernet, который автоматически определяет скорость сети и используя автосогласование, устанавливает наибольшую возможную скорость передачи. Этот порт поддерживает автонастройку на полярность подключаемого кабеля MDI/MDIX, что позволяет использовать один тип кабеля для подключения к устройствам сети. Принт-сервер можно легко подключить к концентратору или коммутатору с помощью патч-корда на витой паре.

Проведение работы

1. Установить IP адрес для «Рабочее место №2».
 - 1.8 На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».
 - 1.9 «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сет» и выбрать «Свойства».

- 1.10 Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».
- 1.11 Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.2. В поле «Маска подсети» ввести 255.255.255.0.
- 1.12 Нажать «ОК».
- 1.13 Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.
- 1.14 После того как последнее окно закроется настройка IP – адреса завершена.

2. Настроить принт-сервер.

- 2.1 На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».
- 2.2 В строке «Адрес» ввести: «192.168.0.10» и нажать «Enter».
- 2.3 Нажать кнопку «System», перейти на вкладку «Configuration». Ознакомиться с доступными параметрами. В поле «Port Name» ввести «DP-301U».
- 2.4 Нажать «Apply». Подождать 30 секунд.
- 2.5 Нажать кнопку «Network», перейти на вкладку «Configuration». Ознакомиться с доступными параметрами. В поле «Workgroup» ввести «CLASS».
- 2.6 Нажать «Apply». Подождать 30 секунд.

3. Настройка Windows XP.

2. На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Принтеры и факсы» → «Установка принтера».
3. Откроется окно «Мастер установки принтеров», нажать «Далее».
4. Выбрать пункт «Локальный принтер, подключенный к этому компьютеру». Убедиться, что отключена функция «Автоматическое определение и установка принтера Plug and Play». Нажать «Далее».
5. Выбрать «Создать новый порт». В выпадающем меню выбрать «Standart TCP/IP Port». Нажать «Далее».
6. Нажать «Далее».
7. В поле «Имя принтера или IP – адрес» указать «192.168.0.10». Имя порта заполнится автоматически. Нажать «Далее». Дождаться появления следующего окна, это может занять несколько минут.
8. Выбрать «Особое», нажать кнопку «Параметры»
9. В качестве используемого протокола выбрать «протокол LPR», в поле «Имя очереди» ввести «DP-301U». Нажать «ОК». Нажать «Далее».
10. Нажать кнопку «Готово».
11. В текущем окне, из доступного списка, выбрать ваш принтер. Если в списке его нет, вставить диск с программным обеспечением принтера, нажать кнопку «Установить с диска». Нажать «Далее».
12. Задать имя принтера, нажать «Далее».
13. Выбрать, печатать или нет пробную страницу, нажать «Далее».
14. Теперь принтер и компьютер готовы для сетевой печати. Нажать

кнопку «Готово».

Контрольные вопросы

1. Назначение принт-сервера.
2. Как подключается принт-сервер к сети

Практическая работа №6

Тема: Межсетевое взаимодействие.

Цель: Настроить маршрутизатор для доступа в «Internet» из локальной сети.

Маршрутизатор или **роутер, рутер** — сетевое устройство, на основании информации о топологии сети и определённых правил, принимающее решения о пересылке пакетов сетевого уровня (уровень 3 модели OSI) между различными сегментами сети.

Работает на более высоком уровне, нежели коммутатор и сетевой мост.

Принцип работы

Обычно маршрутизатор использует адрес получателя, указанный в пакетах данных, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Существуют и другие способы определения маршрута пересылки пакетов, когда, например, используется адрес отправителя, используемые протоколы верхних уровней и другая информация, содержащаяся в заголовках пакетов сетевого уровня. Нередко маршрутизаторы могут осуществлять трансляцию адресов отправителя и получателя, фильтрацию транзитного потока данных на основе определённых правил с целью ограничения доступа, шифрование/дешифрование передаваемых данных и т.д [1].

Таблица маршрутизации

Таблица маршрутизации содержит информацию, на основе которой маршрутизатор принимает решение о дальнейшей пересылке пакетов. Таблица состоит из некоторого числа записей — маршрутов, в каждой из которых содержится адрес сети получателя, адрес следующего узла, которому следует передавать пакеты и некоторый вес записи — метрика. Метрики записей в таблице играют роль в вычислении кратчайших маршрутов к различным получателям. В зависимости от модели маршрутизатора и используемых протоколов маршрутизации, в таблице может содержаться некоторая дополнительная служебная информация [1].

Таблица маршрутизации может составляться двумя способами:

2. статическая маршрутизация — когда записи в таблице вводятся и изменяются вручную. Такой способ требует вмешательства администратора каждый раз, когда происходят изменения в топологии сети. С другой стороны, он является наиболее стабильным и требующим минимума аппаратных

ресурсов маршрутизатора для обслуживания таблицы.

3. динамическая маршрутизация — когда записи в таблице обновляются автоматически при помощи одного или нескольких протоколов маршрутизации — RIP, OSPF, IGRP, EIGRP, IS-IS, BGP, и др. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям назначения на основе различных критериев — количества промежуточных узлов, пропускной способности каналов, задержки передачи данных и т. п. Критерии вычисления оптимальных маршрутов чаще всего зависят от протокола маршрутизации, а также задаются конфигурацией маршрутизатора. Такой способ построения таблицы позволяет автоматически держать таблицу маршрутизации в актуальном состоянии и вычислять оптимальные маршруты на основе текущей топологии сети. Однако динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных [1].

Применение

Маршрутизаторы помогают уменьшить загрузку сети, благодаря её разделению на домены коллизий или широковебательные домены, а также благодаря фильтрации пакетов. В основном их применяют для объединения сетей разных типов, зачастую несовместимых по архитектуре и протоколам, например для объединения локальных сетей Ethernet и WAN-соединений, использующих протоколы xDSL, PPP, ATM, Frame relay и т. д. Нередко маршрутизатор используется для обеспечения доступа из локальной сети в глобальную сеть Интернет, осуществляя функции трансляции адресов и межсетевого экрана.

В качестве маршрутизатора может выступать как специализированное (аппаратное) устройство (характерные представители Cisco, Juniper), так и обычный компьютер, выполняющий функции маршрутизатора. Существует несколько пакетов программного обеспечения (в большинстве случаев на основе ядра Linux) с помощью которого можно превратить ПК в высокопроизводительный и многофункциональный маршрутизатор, например Quagga [1].

Проведение работы

1. Установить IP адрес для «Рабочее место №3».
- 2.8 На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».
- 2.9 «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сет» и выбрать «Свойства».
- 2.10 Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».
- 2.11 Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.10. В поле «Маска подсети» ввести 255.255.255.0.

2.12 Нажать «ОК».

2.13 Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.

2.14 После того как последнее окно закроется настройка IP – адреса завершена.

2. Настроить маршрутизатор.

2.1 Используя патчкорд, соединить *двенадцатый* порт патч-панели, расположенной горизонтально на рабочем месте №3 и *второй* порт патч-панели №3.

2.2 На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».

2.3 В строке «Адрес» ввести: «192.168.0.1» и нажать «Enter».

2.4 В поле «User Name» ввести «admin», поле «Password» - оставить пустым, в поле «Bebow» ввести символы изображенные на картинке. Нажать «Enter».

2.3 Выбрать первую строку слева «Internet Setup». Это меню для настройки интернет соединения. Доступны два способа: через мастер, используя кнопку «Internet Connection Setup Wizard» или вручную - «Manual Internet Connection Setup».

2.4 Настроить подключение к сети «Internet» в зависимости от вашего провайдера.

2.5 В столбце слева выбрать строку «Wireless Setup». Для настройки беспроводной сети доступны два способа: автоматически, через кнопку «Wireless Connection Setup Wizard» или вручную - «Manual Wireless Connection Setup».

2.6 Нажать кнопку «Wireless Connection Setup Wizard».

2.7 Нажать «Next».

2.8 В строке «Wireless Network Name (SSID)» ввести «DIR-300». Выбрать «Manually assign a network key». Нажать «Next».

2.9 В поле «Network key» ввести «123456789». Нажать «Next».

2.10 Нажать «Save». Дождаться пока пока применятся настройки и перезагрузится устройство.

2.11 В окне приветствия вновь ввести логин и запрашиваемый код. Нажать «Enter».

15. Слева в столбце выбрать «LAN Setup». Загрузится страница, на которой можно установить настройки для проводной сети. При необходимости сменить IP – адрес устройства. По окончании настроек нажать «Save Setting» для того чтобы применить новые настройки, или «Don't Save Setting» - для отмены изменений.

3. Настроить беспроводную точку доступа для соединения с маршрутизатором..

3.1 Используя патчкорд, соединить *двенадцатый* порт патч-панели, расположенной горизонтально на рабочем месте №2 и *второй* порт патч-панели №2.

3.2 Установить IP -адрес ПК 192.168.0.2.

3.2.1 На рабочем столе нажать кнопку «Пуск» → «Панель

управления» → «Сетевые подключения».

3.2.2 «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сети» и выбрать «Свойства».

3.2.3 Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».

3.2.4 Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.2. В поле «Маска подсети» ввести 255.255.255.0.

3.2.5 Нажать «ОК».

3.2.6 Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.

После того как последнее окно закроется настройка IP – адреса завершена.

3.3 На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».

3.4 В строке «Адрес» ввести: «192.168.0.50» и нажать «Enter».

3.5 В окне «Подключение к 192.168.0.50», ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».

3.6 На загрузившейся странице выбрать кнопку «Wireless».

3.7 Выставить настройки согласно таблице 3:

Таблица 3.

Название	Значение
Mode	Wireless Client
Authentication	WPA-PSK
Pass Phrase	123456789

3.8 Нажать «Apply». Подождать 30 секунд.

3.9 В окне «Подключение к 192.168.0.50», ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».

3.10 На загрузившейся странице выбрать кнопку «Wireless».

3.11 Нажать кнопку «Scan». Дождаться появления доступных сетей.

3.12 Из появившегося списка, выбрать точку доступа с именем «DIR-300».

3.13 Нажать «Apply». Подождать 30 секунд.

4. Проверяем соединение на рабочем месте №2.

4.1 На рабочем столе нажать кнопку «Пуск» → «Выполнить».

4.2 В появившемся окне, в поле «Открыть», ввести «cmd». Нажать «Enter».

4.3 В командной строке ввести «ping 192.168.0.10». Нажать «Enter».

4.4 Проверить наличие соединения.

5. Проверяем соединение на рабочем месте №3.

5.1 На рабочем столе нажать кнопку «Пуск» → «Выполнить».

5.2 В появившемся окне, в поле «Открыть», ввести «cmd». Нажать «Enter».

5.3 В командной строке ввести «ping 192.168.0.2». Нажать «Enter».

5.4 Проверить наличие соединения.

6. Вывод: Из пунктов 4 и 5 следует, что нам удалось соединить компьютеры через маршрутизатор. При наличии активного соединения с сетью «Internet» на маршрутизаторе, доступ в сеть «Internet» будет возможен из локальной и беспроводной сети.

Контрольные вопросы

1. Для чего предназначен маршрутизатор?
2. Принцип работы маршрутизатора.
3. Для чего применяется «Таблица маршрутизации»?
4. Опишите статическую маршрутизацию
5. Опишите динамическую маршрутизацию
6. Перечислите основные протоколы маршрутизации
7. Опишите применение маршрутизаторов
8. Достоинства и недостатки динамической маршрутизации

Теоретические основы

В настоящее время сфера применения многопроцессорных вычислительных систем (МВС) непрерывно расширяется, охватывая все новые области в самых различных отраслях науки, бизнеса и производства. Стремительное развитие кластерных систем создает условия для использования многопроцессорной вычислительной техники в реальном секторе экономики. Если традиционно МВС применялись в основном в научной сфере для решения вычислительных задач, требующих мощных вычислительных ресурсов, то сейчас, из-за бурного развития бизнеса резко возросло количество компаний, отводящих использованию компьютерных технологий и электронного документооборота главную роль. В связи с этим непрерывно растет потребность в построении централизованных вычислительных систем для критически важных приложений, связанных с обработкой транзакций, управлением базами данных и обслуживанием телекоммуникаций. Можно выделить две основные сферы применения описываемых систем: обработка транзакций в режиме реального времени (OLTP, on-line transaction processing) и создание хранилищ данных для организации систем поддержки принятия решений (Data Mining, Data Warehousing, Decision Support System). Система для глобальных корпоративных вычислений — это, прежде всего, централизованная система, с которой работают практически все пользователи в корпорации, и, соответственно, она должна все время находиться в рабочем состоянии. Как

правило, решения подобного уровня устанавливают в компаниях и корпорациях, где любые, даже самые кратковременные, простои сети могут привести к громадным убыткам. Поэтому для организации такой системы не

подойдет обыкновенный сервер со стандартной архитектурой, вполне пригодный там, где не стоит жестких требований к производительности и времени простоя. Высокопроизводительные системы для глобальных корпоративных вычислений должны отличаться такими характеристиками, как повышенная производительность, масштабируемость, минимально допустимое время простоя. Наряду с расширением области применения, по мере совершенствования МВС происходит усложнение и увеличение количества задач в областях, традиционно использующих высокопроизводительную вычислительную технику. В настоящее время выделен круг фундаментальных и прикладных проблем, объединенный понятием "Grand challenges", эффективное решение которых возможно только с использованием сверхмощной вычислительных ресурсов. Этот круг включает следующие задачи: - Предсказания погоды, климата и глобальных изменений в атмосфере - Науки о материалах - Построение полупроводниковых приборов - Сверхпроводимость - Структурная биология - Разработка фармацевтических препаратов - Генетика - Квантовая хромодинамика - Астрономия - Транспортные задачи - Гидро- и газодинамика - Управляемый термоядерный синтез - Эффективность систем сгорания топлива - Геоинформационные системы - Разведка недр - Наука о мировом океане - Распознавание и синтез речи - Распознавание изображений Для того, чтобы оценить эффективность работы вычислительной системы на реальных задачах, был разработан фиксированный набор тестов. Наиболее известным из них является LINPACK – программа, предназначенная для решения системы линейных алгебраических уравнений с плотной матрицей с выбором главного элемента по строке. LINPACK используется для формирования списка Top500 – пятисот самых мощных компьютеров мира. В настоящее время большое распространение получили тестовые программы, взятые из разных предметных областей и представляющие собой либо модельные, либо реальные промышленные приложения. Такие тесты позволяют оценить производительность компьютера действительно на реальных задачах и получить наиболее полное представление об эффективности работы компьютера с конкретным приложением.

1. Составить презентацию на тему многопроцессорных вычислительных систем

2. Проанализировать работу процессора по примеру на данной компьютерной системе.

Контрольные вопросы

1. В чем смысл архитектурного решения многопроцессорных вычислительных систем Флинна?

2. Как работает мультипроцессорная система с общей памятью?

3. Дайте определение кластерной системе?

4. Какие существуют проблемы связи процессоров в кластерной системе?

Практическая работа №7

Тема: Глобальные вычислительные сети (ГВС).

Цель: Построить виртуальную частную сеть.

Теоретическая часть

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, сеть «Internet»). Несмотря на то, что коммуникации осуществляются по сетям с меньшим (неизвестным) уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрованию, аутентификация, инфраструктуры публичных ключей, средствам для защиты от повторов и изменения передаваемых по логической сети сообщений) [1].

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Уровни реализации

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети — PPTP, причём используемую зачастую не для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол — IP (такой способ использует реализация PPTP — Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» для предоставления выхода в сеть «Internet».

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в Сети [1].

Структура VPN

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит

инкапсулированное соединение (обычно используется сеть «Internet»). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов, удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации [1].

Классификация VPN

Классифицировать VPN решения можно по нескольким основным параметрам:

По степени защищенности используемой среды

Защищённые

Наиболее распространённый вариант виртуальных частных сетей. С его помощью возможно создать надёжную и защищенную подсеть на основе ненадёжной сети, как правило, сеть «Internet». Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

Доверительные

Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решений являются: Multi-protocol label switching (MPLS) и L2TP (Layer 2 Tunnelling Protocol). (точнее сказать, что эти протоколы переключают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec).

По способу реализации

В виде специального программно-аппаратного обеспечения

Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

В виде программного решения

Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

Интегрированное решение

Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания [1].

По назначению

Intranet VPN

Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по

открытым каналам связи.

Remote Access VPN

Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет-киоска.

Extranet VPN

Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубёжей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

Internet VPN

Используется для предоставления доступа к интернету провайдерами, обычно в случае если по одному физическому каналу подключаются несколько пользователей.

Client/Server VPN

Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика, используется его шифрование [1].

По типу протокола

Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство VPN решений поддерживает именно его. Адресация в нём чаще всего выбирается в соответствии со стандартом RFC5735, из диапазона Приватных сетей TCP/IP

По уровню сетевого протокола

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

Примеры VPN

1. IPSec (IP security) — часто используется поверх IPv4.
2. PPTP (point-to-point tunneling protocol) — разрабатывался совместными усилиями нескольких компаний, включая Microsoft.
3. PPPoE (PPP (Point-to-Point Protocol over Ethernet))
4. L2TP (Layer 2 Tunnelling Protocol) — используется в продуктах компаний Microsoft и Cisco.

5. L2TPv3 (Layer 2 Tunnelling Protocol version 3).
6. OpenVPN SSL - VPN с открытым исходным кодом, поддерживает режимы PPP, bridge, point-to-point, multi-client server [1].

Проведение работы

Для проведения этой работы, предположим, что рабочее место №2 и рабочее место №3 удалены друг от друга на значительное расстояние (находятся в разных частях города или страны). Каждое рабочее место имеет подключение к сети «Internet» с выделенным статическим IP адресом, для рабочего места №2 это 192.168.100.195, для рабочего места №3 — 192.168.100.201.

1. Настроить VPN маршрутизатор на рабочем месте №3.

1.1 Используя патчкорд, соединить *двенадцатый* порт патч-панели, расположенной горизонтально на рабочем месте №3 и *девятый* порт патч-панели №3.

1.2 Установить IP -адрес ПК 192.168.0.10.

1.13.1. На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».

1.13.2. «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сет» и выбрать «Свойства».

1.13.3. Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».

1.13.4. Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.10. В поле «Маска подсети» ввести 255.255.255.0.

1.13.5. Нажать «ОК».

1.13.6. Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.

После того как последнее окно закроется настройка IP – адреса завершена.

1.3 На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».

1.4 В строке «Адрес» ввести: «192.168.0.1» и нажать «Enter».

1.5 Ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».

1.6 На загрузившейся странице выбрать кнопку «LAN».

1.7 В поле «LAN IP Address» ввести «192.168.3.1», в поле «Subnet Mask» - «255.255.255.0». Нажать «Apply». Дождаться пока устройство перезагрузится.

1.8 Установить IP -адрес ПК 192.168.3.10.

4.8.1. На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».

4.8.2. «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сет» и выбрать «Свойства».

4.8.3. Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».

4.8.4. Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.3.10. В поле «Маска подсети» ввести 255.255.255.0.

4.8.5. Нажать «ОК».

4.8.6. Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время. После того как последнее окно закроется настройка IP – адреса завершена.

1.8 На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».

1.9 В строке «Адрес» ввести: «192.168.3.1» и нажать «Enter».

1.10 Ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».

1.11 На загрузившейся странице выбрать кнопку «WAN».

1.12 Выбрать «Static IP Address». Установить настройки согласно таблице 1

Таблица 1.

Параметр	Значение
WAN IP Address	192.168.100.201
WAN Subnet Mask	255.255.255.0
WAN Gateway	192.168.100.195

Нажать «Apply». Дождаться пока устройство перезагрузится.

1.13 На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».

1.14 В строке «Адрес» ввести: «192.168.3.1» и нажать «Enter».

1.15 Ввести имя пользователя «admin», поле «Пароль» - оставить пустым. Нажать «Enter».

1.16 На загрузившейся странице выбрать кнопку «VPN».

1.17 Включить «Enable» напротив «VPN». В поле «Max. number of tunnels» ввести количество туннелей равное 4. Напротив ID1 в поле «Tunnel Name» вписать название туннеля, например «New VPN». В выпадающем меню «Method» выбираем IKE, жмём кнопку «More». Установить настройки согласно таблице 2.

Таблица 2.

Параметр	Значение
Tunnel Name	New VPN
Local Subnet	192.168.3.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.0.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.100.201

1. Нажать на кнопку «Select IKE Proposal ...», попадаем в меню Set IKE Proposal. Заполнить соответствующие поля, как показано на рисунке 2.

D-Link
Building Networks for People

DI-804HV
Broadband Hardware VPN Router

Home Advanced Tools Status Help

VPN Settings - Tunnel 1 - Set IKE Proposal

Item	Setting
IKE Proposal index	IKE Proposal Remove

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	IKE Proposal	Group 1	3DES	SHA1	28800	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

Proposal ID -- select one --

Рис 2.

Выбирать в выпадающем меню «Proposal ID» — «1» и нажать кнопку «Add to». Далее «Apply», «Restart».

- 1.19 После перезагрузки, зайти в меню «Set IPSEC Proposal». Заполнить соответствующие поля, как показано на рисунке 3.

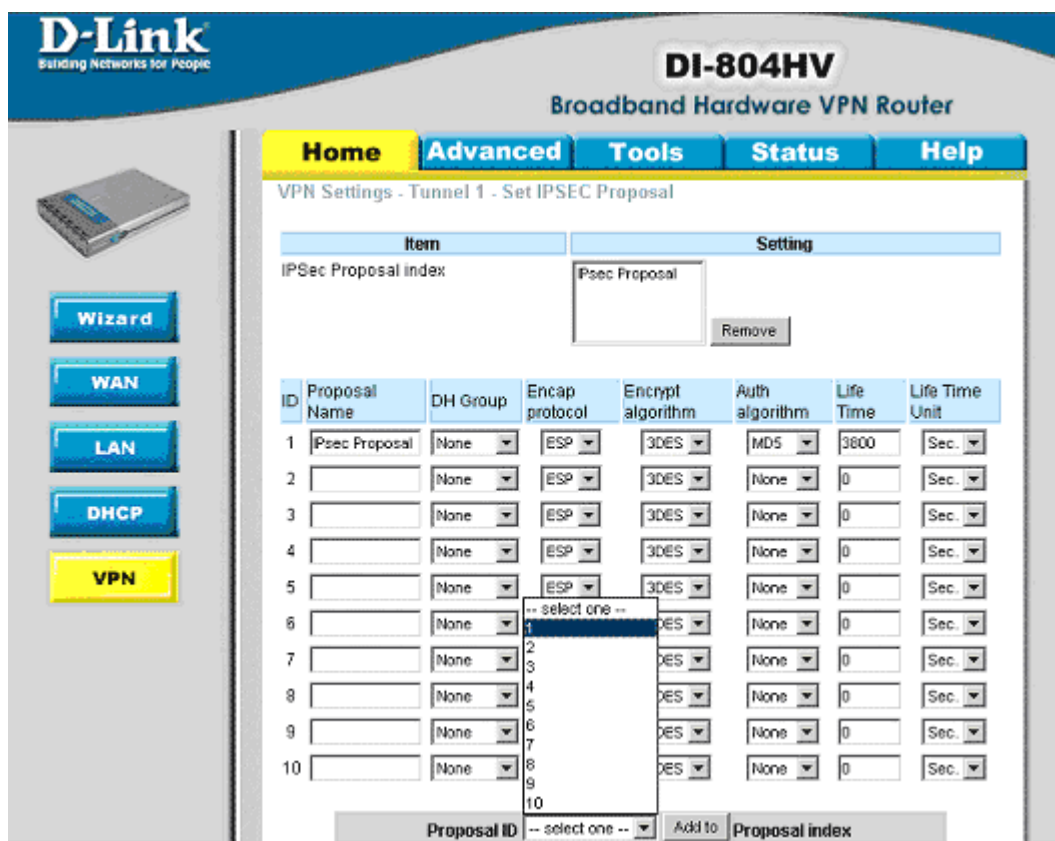


Рис. 3

Выбирать в выпадающем меню «Proposal ID» — «1» и нажать кнопку «Add to». Далее «Apply», «Restart».

1.20 На этом настройка рабочего места №3 и VPN маршрутизатора закончена.

2. Настроить VPN маршрутизатор на рабочем месте №2.

2.1 Используя патчкорд, соединить *двенадцатый* порт патч-панели, расположенной горизонтально на рабочем месте №2 и *седьмой* порт патч-панели №2.

2.2 Установить IP -адрес ПК 192.168.0.2.

2.2.1 На рабочем столе нажать кнопку «Пуск» → «Панель управления» → «Сетевые подключения».

2.2.2 «Щелкнуть» правой кнопкой мыши на «Подключение по локальной сет» и выбрать «Свойства».

2.2.3 Выделить «Протокол интернета (TCP/IP)», затем нажать кнопку «Свойства».

2.2.4 Выбрать «Использовать следующий IP - адрес». Ввести адрес 192.168.0.2. В поле «Маска подсети» ввести 255.255.255.0.

2.2.5 Нажать «ОК».

2.2.6 Нажать «ОК». Для установки адреса компьютеру может потребоваться несколько минут. При этом последнее окно может «повиснуть» на это время.

После того как последнее окно закроется настройка IP – адреса завершена.

2.3На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».

2.4В строке «Адрес» ввести: «192.168.0.1» и нажать «Enter».

а загрузившейся странице выбрать кнопку «WAN».

2.5Выбрать «Static IP Address». Установить настройки согласно таблице 3.

Таблица 3.

Параметр	Значение
WAN IP Address	192.168.100.195
WAN Subnet Mask	255.255.255.0
WAN Gateway	192.168.100.201

Нажать «Apply». Дождаться пока устройство перезагрузится.

2.6На рабочем столе нажать кнопку «Пуск» → «Internet Explorer».

2.7В строке «Адрес» ввести: «192.168.0.1» и нажать «Enter».

2.8Ввести имя пользователя «admin», поле «Пароль» - оставить пустым.

Нажать «Enter».

2.9На загрузившейся странице выбрать кнопку «VPN».

2.10 Включить «Enable» напротив «VPN». В поле «Max. number of tunnels» ввести количество туннелей равное 4. Напротив ID1 в поле «Tunnel Name» вписать название туннеля, например «New VPN». В выпадающем меню «Method» выбираем IKE, жмём кнопку «More». Установить настройки согласно таблице 4.

Таблица 4.

Параметр	Значение
Tunnel Name	New VPN
Local Subnet	192.168.0.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.3.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.100.195
Preshare Key	123456789

2.11 Нажать на кнопку «Select IKE Proposal ...», попадаем в меню Set IKE Proposal. Заполнить соответствующие поля, как показано на рисунке 4.

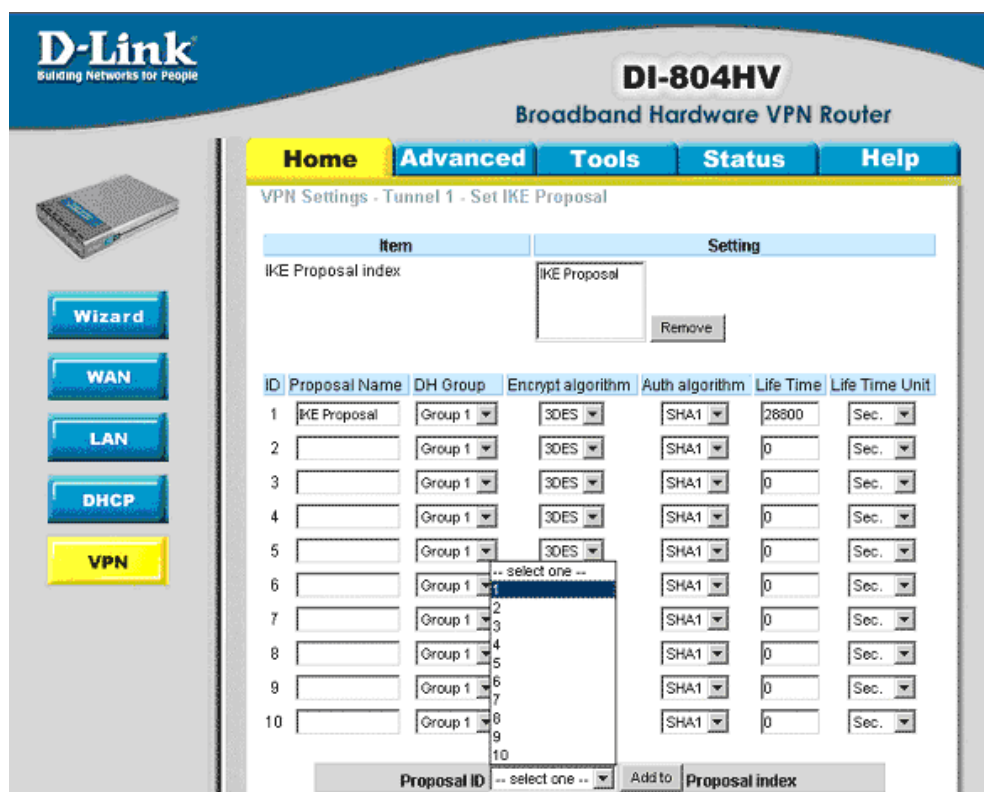


Рис 4.

Выбирать в выпадающем меню «Proposal ID» — «1» и нажать кнопку «Add to». Далее «Apply», «Restart».

2.12 После перезагрузки, зайти в меню «Set IPSEC Proposal». Заполнить соответствующие поля, как показано на рисунке 5.

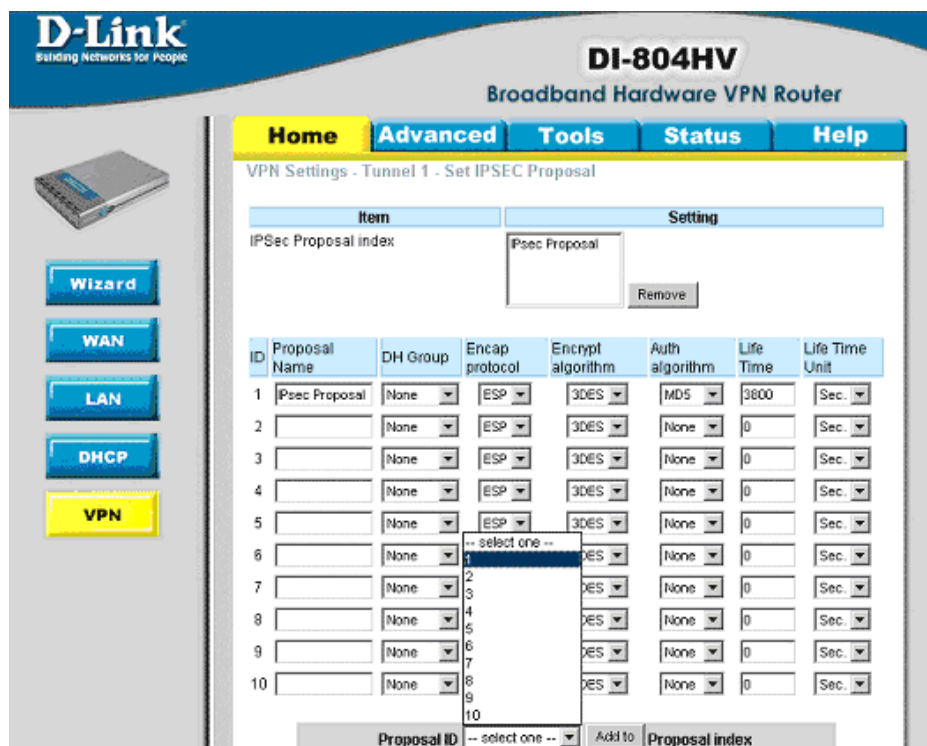


Рис. 5

Выбирать в выпадающем меню «Proposal ID» — «1» и нажать кнопку «Add to». Далее «Apply», «Restart».

2.13 На этом настройка рабочего места №3 и VPN маршрутизатора закончена.

3. Вывод. В проделанной работе нам удалось настроить VPN туннель. При наличии активного подключения к сеть «Internet», рабочее место №2 и рабочее место №3 будут объединены в единую локальную сеть.

Контрольные вопросы

1. Что такое виртуальная частная сеть (VPN)
2. Перечислите 3 вида соединения VPN
3. Опишите уровни реализации VPN
4. Опишите структуру VPN
5. Перечислите типы классификаций VPN решений
6. Опишите защищенные VPN-решения
7. Опишите доверительные VPN-решения
8. Опишите VPN-решения в виде специального программно-аппаратного обеспечения
9. Опишите VPN-решения в виде программного решения
10. Опишите интегрированные VPN-решения
11. Опишите Intranet VPN-решения
12. Опишите Remote Access VPN-решения
13. Опишите Extranet VPN-решения
14. Опишите Internet VPN-решения
15. Опишите Client/Server VPN-решения
16. Опишите VPN-решения по уровню протокола
17. Для чего используют VPN?
18. Приведите примеры VPN.

Практическая работа №8

Тема: Информационные ресурсы Интернет и протоколы прикладного уровня.

Цель: Изучить понятие и назначение сетевых протоколов.

I. Передача файлов по протоколу FTP: клиент ftp.

1. Выполните команду "ftp ftp.rsu.ru". В качестве имени пользователя введите "anonymous", а в качестве пароля свой адрес электронной почты.
2. Определите текущий каталог ftp-сервера (pwd).
3. Просмотрите содержимое этого каталога (ls).
4. Перемещаясь по каталогам, найдите каталог с именем "games" (cd, ls).
5. Завершите соединение с сервером ftp (quit).

6. Находясь на сервере losfs, создайте в своем каталоге файл abc.dat, содержащий семь любых латинских букв.
7. Подключитесь по ftp к серверу sun.mmf.rsu.ru и создайте в своем домашнем каталоге на этом сервере подкаталог Letters.
8. Скопируйте файл abc.dat в созданный каталог.
9. Скопируйте какой-нибудь файл с сервера на клиент.
10. Завершите сеанс ftp.

II. Служба электронной почты: клиент mail, кодирование сообщений.

1. Запустите клиент mail и просмотрите все сообщения.
2. Удалите сообщение с номером 2.
3. Сохраните первое сообщение в файле с именем letter1.
4. Завершите работу клиента mail.
5. Отправьте письмо пользователю bravit с темой "Lab2: sending mail" и телом, содержащим Ваши фамилию и имя.
6. Подготовьте файл с сообщением для Вашего знакомого и отправьте его.
7. Выполните кодирование любого двоичного файла и посмотрите результат этого кодирования, сравните размеры исходного и закодированного файлов.
8. Осуществите декодирование файла и сравните результат с исходным файлом.

III. Протокол SMTP для передачи сообщений электронной почты.

1. Подключитесь по SSH к серверу losfs.
2. Выполните команду "telnet sun.mmf.rsu.ru 25" и дождитесь сообщения "220 sun.mmf.rsu.ru".
3. поприветствуйте сервер командой "HELO losfs.math.rsu.ru" ("HELO" - это не опечатка!).
4. Введите команду "MAIL FROM: " (адрес может быть любым).
5. Введите команду "RCPT TO: user" (user - это адрес получателя на сервере sun.mmf.rsu.ru, здесь нужно ввести свой личный логин).
6. Введите команду "DATA".
7. Теперь можно вводить текст сообщения (не забудьте о пустой строке, разделяющей заголовок и тело сообщения).

8. После последней строки сообщения введите строку, содержащую точку:
".".
9. Выполните команду "QUIT". На этом соединение закончится.
10. Подключитесь к серверу sun по протоколу SSH, запустите клиент mail и убедитесь, что сообщение доставлено.

IV. Протокол доставки почты POP3.

1. Попробуйте подключиться к своему pop3-серверу и посмотреть список хранящихся там сообщений (по желанию).

V. Схема работы службы WWW, клиенты HTTP.

1. Загрузите в свой домашний каталог файл с этой лабораторной работой (`wget www.hightart.ru/students/cnet/lab2.html`) и просмотрите его содержимое.
2. Откройте ту же страницу в браузере lynx, попробуйте перемещаться по ссылкам, перейдите на сайт `uic.rsu.ru`
3. С помощью протокола FTP скачайте файл `lab2.html` из домашнего каталога на сервере sun на локальную машину и просмотрите его в каком-нибудь графическом браузере, сделайте выводы.
4. Найдите какой-нибудь голосовой браузер (домашнее задание).

VI. Запросы и ответы в протоколе HTTP.

1. Подключитесь к веб-серверу `www.rsu.ru` по протоколу HTTP (`"telnet www.rsu.ru 80"`).
2. Введите текст запроса для главной страницы. Не забудьте дважды нажать клавишу Enter в конце запроса.
3. Исследуйте заголовки ответа сервера, попытайтесь определить их значение.
4. Попробуйте послать серверу запрос на несуществующую страницу и проанализируйте результат такого запроса.
5. Попробуйте послать серверу неправильный запрос (например, HELLO) и проанализируйте результат такого запроса.

VII. Введение в язык разметки гипертекста HTML.

1. Напишите на локальном компьютере HTML-документ, содержащий следующую информацию о Вас: фамилия, имя, факультет, курс, группа, хобби и что-нибудь еще. Поставьте ссылки на Ваших одногруппников.
2. Создайте в домашнем каталоге на сервере sun подкаталог "public_html".
3. Скопируйте созданную страницу по протоколу FTP в каталог public_html на сервере.

С помощью браузера lynx обратитесь к Вашей странице по адресу: `sun.mmf.rsu.ru/~login/имя_файла` (login - это Ваше имя на сервере sun).

Список рекомендуемой литературы

Основная литература:

1. Гущин, А.П. Анализ ошибок передачи данных в компьютерной сети и разработка методов их устранения : выпускная квалификационная работа / А.П. Гущин ; Министерство образования и науки Российской Федерации, Крымский федеральный университет имени В. И. Вернадского, Гуманитарно-педагогическая академия (филиал) в г. Ялте, Институт экономики и управления и др. - Ялта : , 2017. - 88 с. : ил., табл. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=463257>
2. Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс]: учебное пособие/ Оливер Ибе— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 333 с.— Режим доступа: <http://www.iprbookshop.ru/63577.html>.— ЭБС «IPRbooks»

Дополнительная литература:

1. Технологии защиты информации в компьютерных сетях/Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=428820>
2. Е.В. Смирнова, И.В.Баскаков, А.В. Пролетарский,Р.А. Федотов "Построение коммутируемых компьютерных сетей "Издательств: Национальный Открытый Университет «ИНТУИТ», 2016 То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429834>
3. Новожилов Е.О. Компьютерные сети. –М.: ОИЦ «Академия» 2013.