МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

КАФЕДРА
ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ

ЗАЩИТА ИНФОРМАЦИИ В БЕСПРОВОДНЫХ ВЫСОКОСКОРОСТНЫХ СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ

МЕТОДИЧЕСКИЕУКАЗАНИЯ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

для студентов направления подготовки
11.03.02 Инфокоммуникационные технологии и системы связи
Профиль **Защищенные инфокоммуникационные системы**
квалификация «бакалавр» всех форм обучения

Ростов-на-Дону
2022

Составитель: доцент кафедры «ИТСС», к.т.н., доцент Решетникова И.В.

Данное методическое пособие предназначено для обеспечения проведения практических занятий со студентами направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи, профиль **Защищенные инфокоммуникационные системы,** квалификации «бакалавр».

Пособие обеспечивает получение практических навыков по основополагающим вопросам изучаемой дисциплины.

Рецензент: Зав. кафедрой ИТСС, к.т.н., доцент Юхнов В.И.

Методическое пособие рассмотрено и утверждено на заседании кафедры ИТСС 26.08. 2022 г. Протокол № 1

I ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

1.1 Цели и задачи

Данный практикум является основополагающим звеном в изучении принципов построения цифровых систем коммутации.

Основная цель практикума – научить:

1. производить все виды инженерных расчетов, связанных с проектированием и эксплуатацией современных цифровых систем передачи;
2. работать с основными характеристиками и параметрами цифровых сигналов связи и передачи данных.

1.2 Общие правила работы в лаборатории

Поскольку все практические занятия рассчитаны на применение компьютеров, то при работе в лаборатории студенты должны:

1. Строго соблюдать установленные правила внутреннего распорядка и техники безопасности.
2. Неукоснительно выполнять требования инженерно-технического состава лаборатории.
3. Начало любых видов работ начинать с приема исходного состояния комплекса технических средств на рабочем месте и заканчивать приведением комплекса технических средств в исходное состояние.

1.3 Подготовка к практическим занятиям

1. повторить теоретический материал, относящийся к работе, пользуясь конспектом лекций и указанной литературой;

2. хорошо уяснить цели работы, программу работы, порядок выполнения работы.

1.4. Порядок проведения практических занятий

1. Уяснение цели и темы практического занятия.

2. Краткое ознакомление с теоретическим материалом по теме занятия с помощью компьютера.

3. Получение от преподавателя индивидуальных исходных данных для расчета.

4.Выполнение расчетов и составление отчета.

5. Верификация результатов расчетов.

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
1	2	3	4	5	6
Курс 4 , Семестр 7					
Модуль 1 Основные сведения о беспроводных системах – 112 (14+6+12+80 часов)					
1.3	Практическое занятие 1 Расчет рабочих частот для радиосвязи в диапазоне коротких волн	ПЗ1	4	ПК-10	Л3.1
1.4	Практическое занятие 2 Расчет зоны уверенного приёма	ПЗ2.	4	ПК-10	Л3.1
1.10	Практическое занятие № 3. Исследование формирования сигнала в стандарте GSM	ПЗ 3	4	ПК-10	Л3.1
Модуль 2 - Защита информации в беспроводных высокоскоростных системах 106 (12+4+14+74 часов)					
2.2	Практическое занятие 4. Принципы построения и типы транкинговых систем	ПЗ4	4	ПК-10	Л3.1
2.4	Практическое занятие 5. Исследование возможностей работы протокола NAT.	ПЗ5	4	ПК-10	Л2.1 Л3.1
2.6	Практическое занятие 6. Конфигурирование списков управления доступом ACL.	ПЗ6	4	ПК-10	Л2.1 Л3.1
2.8	Практическое занятие №7. Конфигурирование виртуальной локальной сети VLAN	ПЗ7	2	ПК-10	Л1.4 Л3.1

Практическая работа № 1
Расчет рабочих частот для рад иосвязи в диапазоне коротких волн

1 Цель работы

1.1 Научиться определять оптимальные рабочие частоты для радиосвязи в диапазоне коротких волн (КВ).

1.2 Научиться определять ширину зоны молчания в диапазоне КВ.

2 Литература

2.1 Ерохин, Г.А. Антенно-фидерные устройства и распространение радиоволн. – Москва: «Академия», 2007, с. 461 – 463.

2.2 Нефедов, Е.И. Антенно-фидерные устройства и распространение радиоволн. – Москва: Издательский центр «Академия», 2008, с.97 – 99.

3 Подготовка к работе

3.1 Повторить пройденный материал по теме «Распространение коротких волн».

3.2 Подготовить бланк отчета.

3.3 Ответить на контрольные вопросы:

3.3.1 Что такое максимально применимая частот (МПЧ), оптимальная рабочая частота (ОРЧ) и наименьшая применимая частота (НПЧ)?

3.3.2 Что такое зона молчания?

3.3.3 Что такое критическая частота?

3.3.4 Что такое критический угол падения?

4 Задание

4.1 Рассчитать оптимальную рабочую частоту на радиолинии заданной длины днем и ночью при заданной концентрации электронов и высоте отражающего слоя ионосферы. В ночное время концентрация N уменьшается в 10 раз.

4.2 Вычислить ширину зоны молчания для найденных частот $f_{ОРЧ}$.

5 Порядок выполнения работы

В диапазоне коротких волн и частично в диапазоне средних волн (СВ) широкое применение находят пространственные радиоволны, которые отражаются от слоев ионосферы F_2 , F_1, E и обеспечивают дальнее распространение радиосигналов в системах передачи радиосвязи и радиовещания.

5.1 Выбор оптимальных рабочих частот на радиолиниях зависит от расстояния длинны радиолинии ℓ, а также от концентрации электронов в отражающем слое N. Значения $h_э$, ℓ, N *и* $r_{ВНУТР}$ взять из приложения 8, по варианту, заданному преподавателем.

Для определения $f_{ОРЧ}$ вначале находят $f_{МПЧ}$, пользуясь законом косинуса, формула 1.

$$f_{МПЧ} = \frac{f_{кр}}{\cos\theta_{кр}}, \qquad (1)$$

где $f_{КР}$ – критическая частота слоя, МГц;

$\theta_{КР}$ - критический угол падения, град.

Критическая частота слоя ионосферы определяется по формуле:

$$f_{КР} = \sqrt{80{,}8N}, \qquad (2)$$

где N – концентрация электронов в слое ионосферы, 1/м^3.

Критический угол падения, рисунок 1, определяют, исходя из высоты отражающего слоя $h_э$ и расстояния ℓ от точки излучения (А) до точки падения отраженного луча (В).

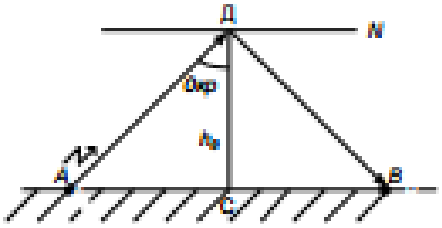

Рисунок 1 – Определение МПЧ

Определив $f_{МПЧ}$, находят $f_{ОРЧ}$, которая меньше $f_{МПЧ}$ на 15%.

5.2 При работе радиосистем передачи пространственными лучами возможно образование вокруг точки излучения радиоволн кольцевой зоны, в которой не возможен прием радиосигнала. Её называют зоной молчания.

Внешний радиус R зависит от критического угла падения луча на отражающий слой ионосферы, рисунок 2.

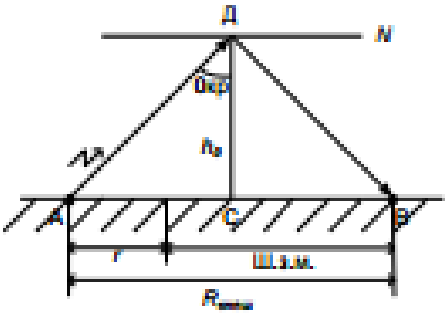

Рисунок 2 – Определение ширины зоны молчания

Ширина зоны молчания определяется по формуле:

$$Ш.з.м. = R - r\,, \qquad (3)$$

где R – внешний радиус зоны, км;
r – внутренний радиус, км.

Внешний радиус R можно определить пользуясь формулой 1 и определив из треугольника АДС катет АС. $f_{МПЧ}$ взять равной $f_{ОРЧ}$ для дневного и ночного времени.

Результаты расчетов записать в таблицу 1.

Таблица 1

	Концентрация электронов N, 1/м^3	Оптимальная рабочая частота, МГц	Ширина зоны молчания, км
День			
Ночь			

6 Содержание отчета

6.1 Наименование работы.
6.2 Цель работы.
6.3 Задание по варианту.
6.4 Формулы для расчета.
6.5 Результаты расчетов.
6.6 Выводы по проделанной работе.
6.7 Ответы на вопросы из п.7.

7 Контрольные вопросы

7.1 Как получается дальнее распространение коротких волн?
7.2 От чего зависит радиус действия поверхностных волн КВ диапазона и чему он может быть равен?
7.3 Почему образуется зона молчания на КВ?
7.4 Как определяют практически критические частоты слоев?
7.5 Как получаются замирания на КВ и как с ними борются в системах радиосвязи?
7.6 Как устраняют прямое кругосветное эхо на КВ?

8 Приложение

Таблица 2

№ варианта	Длинна радиолинии ℓ, км	Действующая высота $hд$, км	Концентрация электронов (днем) N, 1/см^3	Внутренний радиус r, км	Слои ионосферы
1	4000	380	$1{,}5\cdot10^6$	30	F2
2	3800	350	10^6	35	
3	3500	300	$1{,}5\cdot10^5$	40	
4	3200	250	$4\cdot10^5$	43	
5	3100	220	$8\cdot10^5$	45	
6	4100	400	$2\cdot10^6$	25	
7	3600	340	$1{,}8\cdot10^6$	37	
8	3300	270	$5\cdot10^5$	42	
9	3000	230	$4\cdot10^5$	48	F1
10	2500	210	$3\cdot10^5$	50	
11	2000	180	$2\cdot10^5$	53	
12	1500	170	$1{,}8\cdot10^5$	55	
13	1000	160	10^5	60	
14	2800	220	$3{,}5\cdot10^5$	48	
15	2200	190	$2{,}5\cdot10^5$	49	
16	1200	165	$1{,}5\cdot10^5$	57	
17	2000	125	$25\cdot10^3$	70	E
18	1700	120	$23\cdot10^3$	73	
19	1500	115	$20\cdot10^3$	75	
20	1300	110	$19\cdot10^3$	80	
21	1100	105	$15\cdot10^3$	85	
22	1000	100	$12\cdot10^3$	90	
23	800	95	$10\cdot10^3$	95	
24	600	90	$8\cdot10^3$	100	

Практическая работа № 2

Расчет зоны уверенного приёма

1 Цель работы

1.1 Научиться определять зону уверенного приёма в диапазоне метровых волн (МВ) и дециметровых волн (ДМВ).

1.2 Научиться рассчитывать напряжённость поля в зоне уверенного приёма.

2 Литература

2.1 Ерохин, Г.А. Антенно-фидерные устройства и распространение радиоволн. – Москва: «Академия», 2007, с. 431 – 442.

2.2 Нефедов, Е.И. Антенно-фидерные устройства и распространение радиоволн. – Москва: Издательский центр «Академия», 2008, с.92 – 94.

3 Подготовка к работе

3.1 Повторить пройденный материал по теме «Распространение метровых волн и дециметровых волн».

3.2 Подготовить бланк отчета.

3.3 Ответить на контрольные вопросы:

3.3.1 Какие радиосистемы передачи работают в диапазонах МВ и ДМВ?

3.3.2 Чем объясняется распространение МВ и ДМВ на близкое расстояние?

3.3.3 Как влияет ионосфера на распространение радиоволн МВ и ДМВ?

3.3.4 На каком расстоянии располагают промежуточные радиорелейные станции прямой видимости?

4 Задание

4.1 Определить расстояние прямой видимости для заданной радиосистемы передачи.

4.2 Рассчитать напряженность поля электромагнитной волны в зоне уверенного приёма.

5 Порядок выполнения работы

Предельное расстояние действия МВ и ДМВ определяется расстоянием прямой видимости, которое зависит от высоты подвеса антенн. Поэтому антенны в радиосистемах передачи подвешивают на высоких мачтах или башнях. МВ и ДМВ диапазоны являются основными для радиосистем телевещания, радиовещания и мобильных систем радиосвязи. Значения h_1 и h_2, r, $Д$, P_{Σ}, и № ТВ канала, взять из приложения 8, по варианту, заданному преподавателем.

5.1 Расстояние прямой видимости, без учета рефракции радиолучей, рассчитывают по формуле:

$$r_{01} = 3{,}57 \cdot \left(\sqrt{h_1} + \sqrt{h_2}\right), \qquad (1)$$

где h_1 и h_2 – высоты подвеса передающей и приемной антенн, м.

Расстояние прямой видимости с учетом рефракции радиолучей в слоях тропосферы, это расстояние увеличивается и определяется по формуле:

$$r_{02} = 4{,}52 \cdot \left(\sqrt{h_1} + \sqrt{h_2}\right) \qquad (2)$$

5.2 Напряжённость поля электрической волны в зоне уверенного приёма без учета сферичности Земли, создаваемую передающей антенной радиосистемы передачи, рассчитывают по формуле:

$$E_{\partial} = \frac{2{,}18 \cdot \sqrt{P_{\Sigma} Д} \cdot h_1 \cdot h_2}{r^2 \cdot \lambda} \text{, (мВ/м)} \qquad (3)$$

где P_{Σ} – мощность излучаемая антенной, кВт;

$Д$ – коэффициент направленного действия передающей антенны;

h_1 и h_2 – высоты подвеса передающей и приёмной антенн, м;

r – расстояние от антенны до точки, в которой определяется напряженность поля, км;

λ – длинна волны, м.

Для определения длинны волны, на которой определяют напряженность поля, необходимо найти среднюю частоту телевизионного канала.

Результаты всех расчетов записать в таблицу 1.

Таблица 1

№ ТВ канала	№ ТВ диапазона	Полоса частот канала, МГц	Средняя частота канала МГц	λ м	r_{02} км	E_{∂} В/м

6 Содержание отчета

6.1 Наименование работы.

6.2 Цель работы.

6.3 Задание по варианту.

6.4 Формулы для расчета.

6.5 Результаты расчетов.

6.6 Выводы по проделанной работе.

6.7 Ответы на вопросы из п.7.

7 Контрольные вопросы

7.1 Какие стандартные диапазоны радиочастот используются для телевещания?

7.2 Какие стандартные диапазоны радиочастот используются в радиовещании на метровых радиоволнах?

7.3 От чего зависит расстояние прямой видимости?

7.4 Как влияет нормальная рефракция в тропосфере на дальность распространения радиоволн МВ и ДМВ?

7.5 Чем можно объяснить дальнее распространение УКВ и ДМВ над морской поверхностью?

7.6 Возможно ли отражение радиоволн МВ диапазона от ионосферы?

8 Приложение

Таблица 2

Номер канала		Полоса частот, МГц	Номер канала		Полоса частот, МГц
I ТВ	1	48,5…56,5	IV ТВ	27	518…526
	2	58,0…66,0		28	526…534
II ТВ ОВЧ ЧМ УКВ 1 РВ 66,0…74 МГц УКВ 2 87,5…108 МГц	ОВЧ ЧМ	66,0…74,0		29	534…542
	3	76,0…84,0		30	542…550
	4	84,0…92,0		31	550…558
	5	92,0…100,0		32	558…566
III ТВ	6	174,0…182,0		33	566…574
	7	182,0…190,0		34	574…582
	8	190,0…198,0	V ТВ	35	582…590
	9	198,0…206,0		36	590…598
	10	206,0…214,0		37	598…606
	11	214,0…222,0		38	606…614
	12	222,0…230,0		39	614…622
IV ТВ	21	470…478		40	622…630
	22	478…486		41	630…638
	23	486…494		42	638…646
	24	494…502		43	646…654
	25	502…510		44	654…662
	26	510…518		45	662…670

Практическое занятие № 3.
Исследование формирования сигнала в стандарте GSM

Цель работы: Исследовать процессы формирования сигнала в квадратурном модуляторе и демодулирования сигнала в стандарте GSM. Исследовать влияние многолучевого характера распространения радиоволн на величину ошибок в канале связи.

В стандарте GSM применяется спектрально-эффективная гауссовская частотная манипуляция с минимальным частотным сдвигом (GMSK). Манипуляция называется "гауссовской" потому, что последовательность информационных бит до модулятора проходит через фильтр нижних частот (ФНЧ) с характеристикой Гаусса, что дает значительное уменьшение полосы частот излучаемого радиосигнала.

Метод GMSK представляет собой частотную манипуляцию, при которой несущая частота дискретно (через интервалы времени, кратные периоду T битовой модулирующей последовательности) принимает значения

$$f_н=f_0-F/4 \text{ или } f_в=f_0+F/4,$$

где f_0 – центральная частота используемого частотного диапазона;

$F=1/T$ – частота битовой последовательности.

Разнос частот $\Delta f=f_в-f_н$ – минимально возможный, при котором обеспечивается ортогональность колебаний с частотами $f_в$ и $f_н$ на интервале T длительности одного бита. При этом за время T между колебаниями с частотами $f_в$ и $f_н$ набегает разность фаз, равная π.

В методе частотной манипуляции с минимальным сдвигом (MSK – Minimum Shift Keying) входная последовательность битовых импульсов модулятора разбивается на две последовательности, состоящие из четных и нечетных импульсов. Модулированный сигнал на выходе на протяжении одного бита определяется выражением, зависящим от состояния текущего n-го и предшествующего $(n-1)$-го бита:

$$S(t)=\pm\cos(\pi t/2T)\cos\omega_0 t\pm\sin(\pi t/2T)\sin\omega_0 t=\pm\cos(\omega_0 t\pm\pi t/2T), \qquad (1)$$

$$(n-1)T \le t \le nT$$

Здесь $\omega_0=2\pi f_0$ – центральная частота канала. Выбор знака в (1) определяется табл. 1.

Таблица 1

Биты входной последовательности модулятора		Выбор знака в (6.2)		Выбор знака в (6.2)		f
Нечетный	Четный	$\pm\cos(\pi t/2T)$	$\pm\sin(\pi t/2T)$	$\pm\cos$	$\pm\pi t/2T$	
1	1	+	+	+	-	$f_н$
0	1	+	-	+	+	$f_в$
0	0	-	-	-	-	$f_н$
1	0	-	+	-	+	$f_в$

Мгновенная частота принимает одно из двух значений – $f_в$ или $f_н$, постоянное на протяжении одного бита. Изменение знака в начальной фазе ($\pm\pi t/2T$ в выражении (1) означает переход от $f_н$ к $f_в$ или обратно. Изменение общего знака в выражении (1) эквивалентно изменению начальной фазы на π, что позволяет сохранить непрерывность фазы при изменении частоты.

Метод формирования сигнала MSK иллюстрируется на рис. 1.

Формирование GMSK радиосигнала осуществляется таким образом, что на интервале одного информационного бита фаза несущей изменяется на 90°. Это наименьшее возможное изменение фазы, распознаваемое при данном типе модуляции.

Применение фильтра Гаусса позволяет при дискретном изменении частоты получить "гладкие переходы". В стандарте GSM применяется GMSK-модуляция с величиной полосы фильтра по уровню минус 3 дБ выбирается равной $B = 0{,}3F$, где F – частота битовой модулирующей последовательно. В стандарте GSM F =279,833 кГц, полоса гауссовского фильтра B =81,3 кГц. Использование гауссовского фильтра приводит к сужению главного лепестка и снижениию боковых лепестков спектра сигнала на выходе модулятора. Этим снижается уровень помех по соседним частотным каналам. Структурная схема модулятора показана на рис. 2.

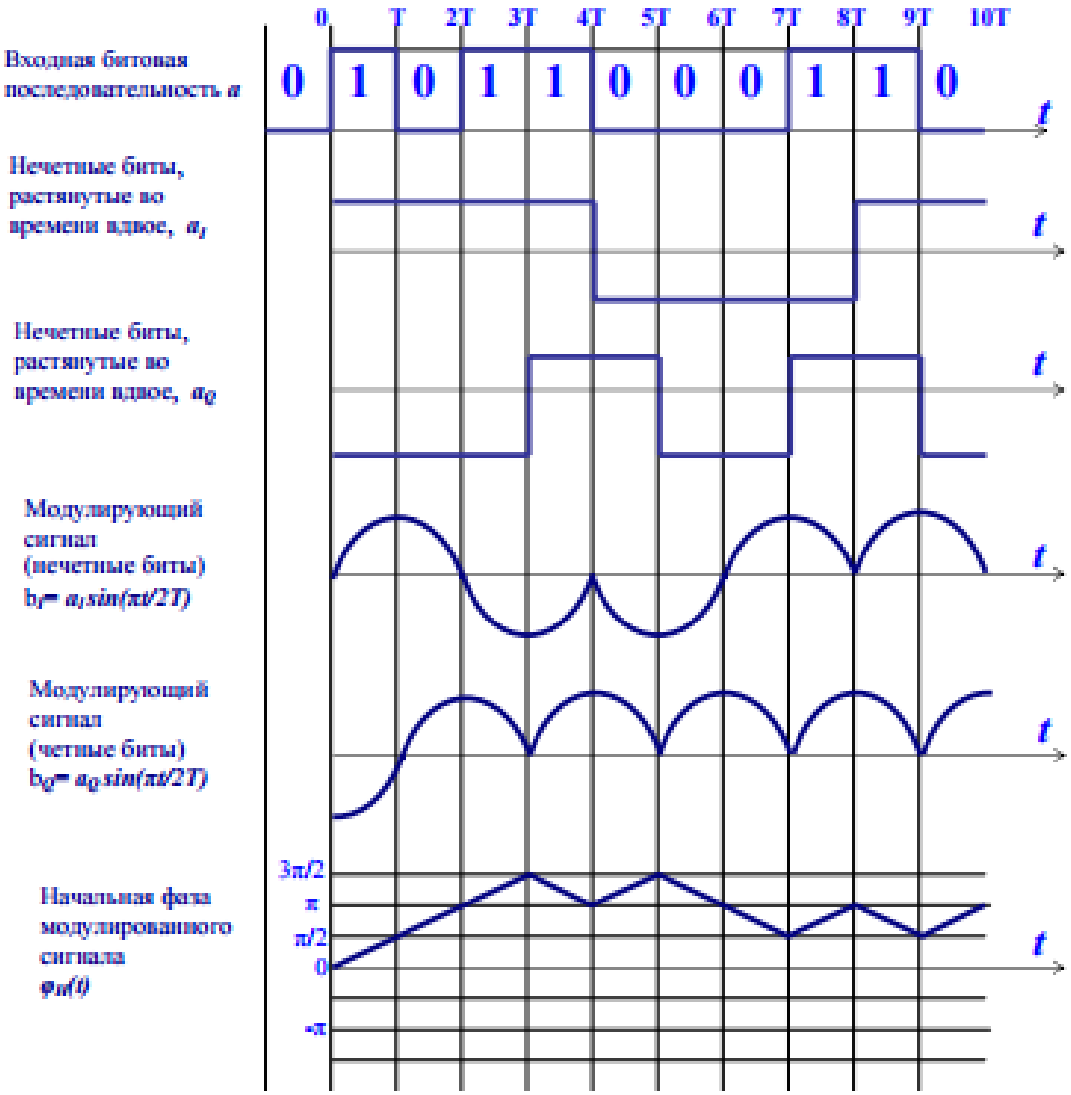

Рис. 1. Временные диаграммы сигналов в методе MSK

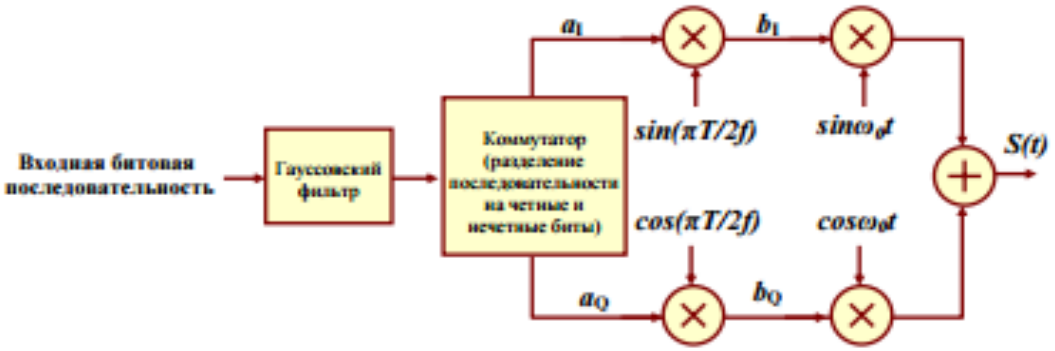

Рис. 2. Структурная схема модулятора GMSK

На рис.3 показан спектр реального сигнала.

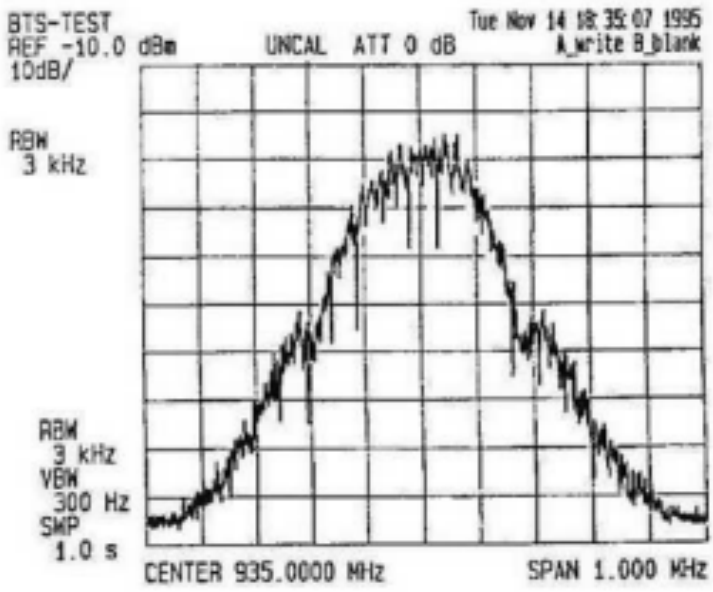

Рис. 3. Спектр реального сигнала в стандарте GSM

Для упрощения схемы при выполнении лабораторной работы фильтр Гаусса исключен.

В лабораторной работе формирование сигнала в передатчике стандарта GSM моделируется схемой, показанной на рис.4.

Отчет должен содержать:

1. Схему модулятора с пояснением назначения его узлов.
2. Схему демодулятора с пояснением назначения его узлов.
3. Схему моделирования канала связи и оценки его качества
4. Спектр сигнала при передаче трафика и передаче временного интервала коррекции частоты

5. Вид сигналов при передаче трафика и передаче временного интервала коррекции частоты во временной области
6. График зависимости вероятности ошибок от скорости движения объекта
7. График зависимости вероятности ошибок от задержки отраженного луча
8. График зависимости вероятности ошибок от относительного уровня отраженного луча
9. Выводы о степени влияния рассмотренных факторов на работу радиоканала и способы уменьшения этого влияния.

Таблица 2

Частота несущей радиоканала

Номер бригады	Частота, МГц
1	880
2	890
3	900
4	910
5	920
6	930
7	940
8	950

Контрольные вопросы

1. Принцип работы квадратурного модулятора
2. Временные интервалы в стандарте GSM.
3. Требования к спектру излучаемого сигнала
4. Принцип работы квадратурного демодулятора
5. Частотная манипуляция с минимальным частотным сдвигом
6. Эффект многолучевого распространения радиоволн
7. Способы борьбы с влиянием отраженных сигналов
8. Влияние скорости движения мобильной станции на работу канала связи

Практическое занятие 4
Принципы построения и типы транкинговых систем

Цель работы

1. Изучить принципы построения, функционирования и типы транкинговых систем.

Задание

1. Изучить принципы построения и функционирования тарнкинговых систем. Изучить режимы работы транкинговых систем.
2. Ознакомиться с комплексом документов регламентирующих работу транкинговых сетей связи Российской Федерации.
3. Изучить основные типы транкинговых систем:
4. Система стандарта TETRA.

Литература

1. Бабков В.Ю., Вознюк М.А., Дмитриев В.И. Системы мобильной связи. / СПб ГУТ, - СПб, 1999.
2. Бабков В.Ю., Воробьев О.В., Певцов Н.В., Петров Д.А., Сиверс М.А. Транкинговые системы связи. СПб.: Судостроение, 2000.

Краткая теория

Можно утверждать, что важнейшей стратегией развития подвижной радиосвязи является разработка и внедрение единых международных стандартов, создание на их основе международных глобальных сетей подвижной радиосвязи общего пользования. Однако продолжают успешно развиваться сравнительно простые системы радиосвязи, имеющие специальное ограниченное применение. Профессиональные системы подвижной радиосвязи создавались и развертывались в России в интересах обеспечения служебной деятельности различных государственных структур (министерства обороны, правоохранительных органов, промышленных групп и других организаций). Основными требованиями к этим системам являются: обеспечение связи в данной зоне обслуживания, возможность взаимодействия различных абонентских групп и циркулярной

(диспетчерской) связи, оперативность управления связью и возможность приоритетного установления связи. Общие тенденции развития профессиональных отечественных систем подвижной радиосвязи в целом отвечают современному мировому уровню, но не обеспечивают совместимость оборудования при работе в составе систем связи, построенных на основе единых стандартов. В то же время на Западе на практике реализуется международная унификация и стандартизация оборудования. Общий рынок систем и оборудования позволил разработать унифицированную элементную базу, массовый выпуск которой обеспечил высокую элементную надежность и значительное снижение цен на эту продукцию. В результате ежегодный рост количества абонентов профессиональных систем в западных странах составляет около 25 %. В профессиональных системах подвижной радиосвязи наиболее эффективное использование частотного ресурса обеспечивается в транкинговых системах - системах со свободным доступом радиоабонентов к общему частотному ресурсу. Одной из первых транкинговых систем, использующих принцип выбора соответствующего канала для обеспечения гарантированного доступа к связи и ориентированной на телефонию, была отечественная радиотелефонная система АЛТАЙ. Ее появление и повсеместное распространение в нашей стране вызвано жестким государственным регулированием всех сфер деятельности. На Западе системы, нацеленные на экономию частотного ресурса, появились и стали широко использоваться в первую очередь в США, лишь немногим более 10 лет назад, когда сотовые сети уже существовали и стала ощущаться острая нехватка свободных каналов для обычной радиосвязи. Что касается Европы, то ее потребность в радиосвязи по сравнению с США значительно меньше. Затрудненность достижения консенсуса многочисленными странами и разобщенность научного потенциала серьезно препятствовали глубине и единообразию технических решений. Все это привело к созданию целого ряда систем, как правило, дорогих и не всегда оригинальных. Тем не менее, появление и

развитие транкинговых радиосистем на Западе стало следствием нескольких основных причин: потребности гарантированного доступа к связи для оперативного руководства; нехваткой частотного ресурса; наличие достаточно разветвленной телефонной сети, в том числе сотовых систем; уровнем спроса на новые технические решения. Под термином транкинг понимается метод равного доступа абонентов к общему выделенному пучку (термин trunk (англ.) - пучок) каналов, при котором конкретный канал закрепляется для каждого сеанса связи индивидуально в зависимости от распределения нагрузки в системе. Термин транкинг впервые стал употребляться для обозначения систем радиотелефонной связи, ориентированных на организацию ведомственной, внутрипроизводственной и технологической связи. Первоначально такие системы использовались при организации систем подвижной радиосвязи, не имеющих присоединения к телефонным сетям общего пользования. В основу этих систем подвижной радиосвязи закладывался принцип общности интересов (корпоративности) пользователей, поэтому в сетях, построенных на их основе, трафик должен замыкаться внутри этих сетей. В последние годы появилась тенденция создания на базе транкинговых систем — систем радиосвязи общего пользования, которые являются продолжением телефонных сетей общего пользования (ТфОП). Общие требования Транкинговые системы связи, как специализированные системы связи (ведомственные, выделенные, технологические и внутрипроизводственные сети), находят широкое применение во всем мире. В соответствии с концепцией использования в России транкинговая сеть может считаться сетью связи общего пользования, если она отвечает следующим требованиям: обеспечивает круглосуточное предоставление абонентам входящей и исходящей местной, междугородной и международной связи и возможность тарификации услуг; обеспечивает закрепление за каждым абонентом системы номера телефонной сети общего пользования; имеет дуплексный способ организации канала; обладает вероятностью отказа не более 5% при расчетной нагрузке на одного абонента

- 0,025 Эрл1; имеет защиту от несанкционированного доступа в систему; обеспечивает выполнение условий для организации оперативно-розыскных мероприятий. Эти требования соответствуют рекомендациям Международного союза электросвязи (МСЭ), в которых указано, что сети радиотелефонной связи общего пользования и абоненты таких сетей должны являться продолжением (или иметь нумерацию) ТфОП. В транкинговых сетях общего пользования допускается использование только сертифицированного оборудования, отвечающего техническим требованиям к оборудованию с многостанционным доступом. Выдача лицензий на организацию сетей связи общего пользования на основе транкинговых систем предусматривает обязательное наличие сертификата на оборудование, допускающее включение в ТфОП и выполнение оператором ряда технических требований. В соответствии с федеральным законом «О связи» допускается предоставление коммерческих услуг ведомственными транкинговыми сетями при условии, что это не повлияет на выполнение ими основных задач

Контрольные вопросы

1. Дайте характеристику общих требований к транкинговым системам.
2. Каковы принципы построения и функционирования транкинговых систем?
3. Дайте характеристику режимов работы транкинговых систем.
4. Какова классификация транкинговых систем?
5. Поясните принцип передачи речи в стандарте TETRA.
6. Поясните принцип передачи данных в стандарте TETRA.
7. Какова структура сети стандарта TETRA?

Практическое занятие № 5
Исследование возможностей работы протокола NAT

Цель работы: Исследование свойств и особенностей работы сети при настройке протокола NAT. Получить навыки конфигурирования протокола NAT на маршрутизаторе Cisco.

Задание. Произвести построение сети. Настроить DHSP сервер с указанными параметрами. Настроить работу службы NAT. Произвести удалённое подключение к веб серверу.

Содержание работы

Технология трансляции сетевых адресов – NetworkAddressTranslation (NAT). NAT широко используется в современных сетях по следующим причинам. Во-первых, уже сейчас наблюдается дефицит IP-адресов четвертой версии. Кардинальным решением здесь может служить переход к шестой версии IP-протокола, но пока повсеместно используется IPv4. При использовании NAT в пределах внутренней сети могут использоваться частные адреса, о которых уже шла речь в третьей главе настоящего пособия. Преобразование частных адресов в общедоступные и обратно осуществляется с использованием протокола NAT. Одни и те же частные адреса могут использоваться в различных корпоративных сетях, что и приводит к экономии адресного пространства.

Во-вторых, NAT существенно повышает безопасность корпоративной сети, так как в этом случае извне сеть представляется единственным или несколькими общедоступными адресами. Поэтому определить структуру корпоративной сети, проанализировать данные, циркулирующие в ней, становится проблематично.

Основная идея технологии NAT состоит в следующем. Внутренняя корпоративная сеть использует адресное пространство частных адресов. В маршрутизаторе или другом устройстве, связывающем внутреннюю сеть с внешней IP-сетью, настраивается протокол NAT, осуществляющий при

передаче во внешнюю сеть преобразование частного адреса в общедоступный и обратное преобразование при приеме. Так как внутренняя сеть также может содержать маршрутизаторы для разделения ее на подсети, они должны получать объявления о маршрутной информации от маршрутизаторов внешней сети. В свою очередь, внешние маршрутизаторы не должны ничего знать о маршрутизаторах внутренней сети. Поэтому NAT-устройство должно пропускать из внешней сети во внутреннюю сообщения протоколов маршрутизации (RIP, OSPF и т.д.), но не пропускать эти сообщения в обратном направлении. Число общедоступных адресов чаще всего меньше числа частных адресов, за счет чего и достигается экономия адресного пространства. В частном, но далеко не самом редком случае, может использоваться всего один общедоступный адрес, настраиваемый на внешнем порту NAT-маршрутизатора.

Рассмотрим сначала наиболее простой случай, когда количество конечных узлов внутренней сети равно количеству общедоступных адресов, полученных данной сетью от провайдера сетевых услуг (рисунок 1).

На рисунке представлены две внутренние сети, обозначенные A и B, связанные между собой через общедоступную сеть. Выход из внутренней сети в общедоступную осуществляется с использованием NAT-устройства, в качестве которого может использоваться маршрутизатор или межсетевой экран с установленным программным обеспечением NAT. В данном примере полагаем, что внутренняя адресация каждой из сетей одинакова, то есть и в сети A, и в сети B могут быть узлы с одинаковыми частными IP-адресами (192.168.1.1 в данном примере).

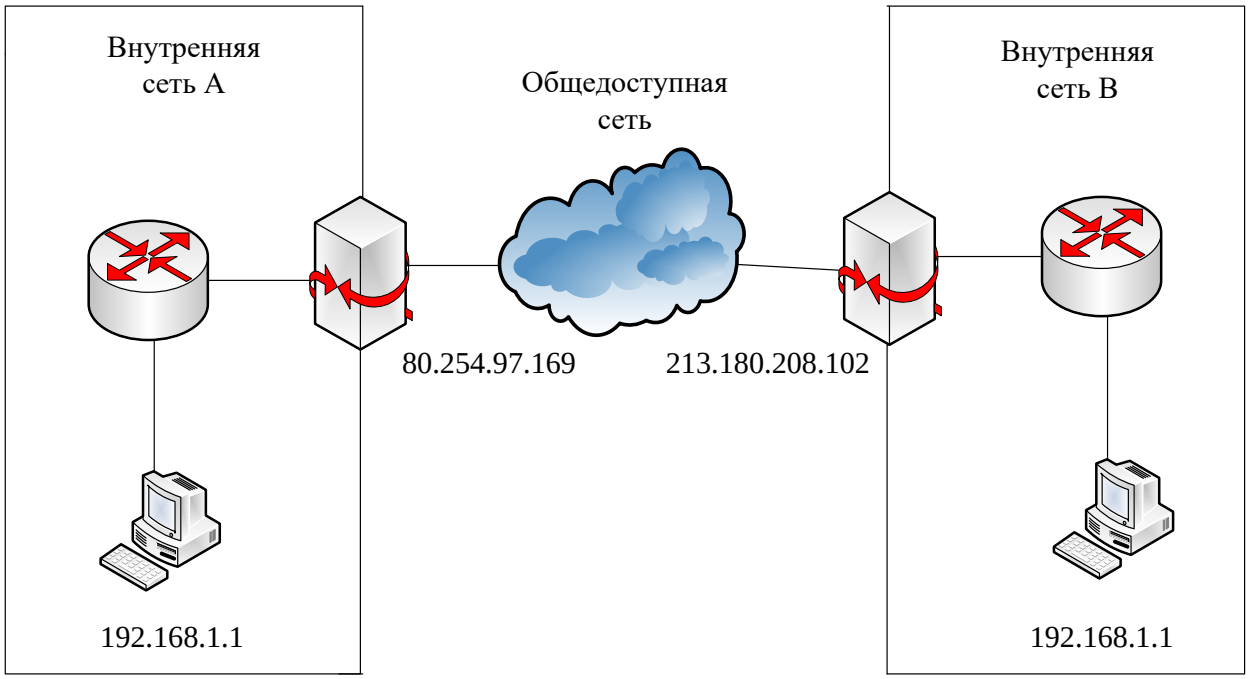

Рисунок 1 – Простейший случай использования NAT

Внешние адреса NAT-устройств являются общедоступными и, соответственно, уникальными.

Предположим, что конечный узел внутренней сети А собирается послать пакет данных конечному узлу внутренней сети В. В качестве IP-адреса получателя в пакете указывается адрес 213.180.208.102, и пакет передается на маршрутизатор внутренней сети А. Как указывалось выше, внутренние маршрутизаторы получают уведомления о маршрутной информации из внешней сети, поэтому внутренний маршрутизатор сети А «знает» о маршруте к адресу 213.180.208.102, в нашем примере этот маршрут пролегает через NAT-устройство. Соответственно, пакет попадает на NAT-устройство, соединяющее внутреннюю сеть А с общедоступной сетью.

Однако в пакет должен быть помещен также и IP-адрес отправителя. Конечный узел сети А помещает в пакет свой адрес – 192.168.1.1, и этот пакет без каких-либо изменений достигает NAT-устройства сети А. В свою очередь, NAT-устройство должно подменить адрес источника 192.168.1.1 на свой общедоступный адрес 80.254.97.169 (точнее, на адрес своего внешнего интерфейса). Эта подмена осуществляется с использованием таблицы,

хранящейся в памяти NAT-устройства, упрощенный вид которой представлен в таблице 1.

Таблица 1 – Соответствие частных и общедоступных адресов

Частный адрес	Общедоступный адрес
192.168.1.1	80.254.97.169

Очевидно, что количество общедоступных адресов у NAT-устройства должно соответствовать количеству узлов внутренней сети, имеющих права доступа во внешнюю сеть.

Пакет с измененным адресом источника достигает NAT-устройства сети B, которое хранит в своей памяти аналогичную таблицу 2.

Таблица 2 – Соответствие частных и общедоступных адресов

Частный адрес	Общедоступный адрес
192.168.1.1	213.180.208.102

Приняв данный пакет, NAT-устройство сети B изменяет адрес получателя в пакете в соответствии с таблицей 2, то есть адрес 213.180.208.102 изменяется на адрес 192.168.1.1. Видоизмененный таким образом пакет передается на внутренний маршрутизатор сети B и в конечном итоге достигает нужного узла.

В частном случае, когда сеть B не использует технологию NAT, пакет передается в узел сети B без изменений.

Рассмотренный пример использования NAT имеет ряд существенных недостатков.

Во-первых, экономии адресов в данном случае не происходит – внутренние адреса жестко закреплены за общедоступными адресами в таблицах NAT-устройств. Поэтому в этом виде NAT может использоваться только для повышения безопасности сети.

Во-вторых, записи в таблицу в данном случае являются статическими, то есть их необходимо вносить вручную, что при значительном количестве внутренних узлов является трудоемкой процедурой, подверженной ошибкам. Однако следует заметить, что иногда статические записи в таблице NAT необходимы, например, если во внутренней сети имеется сервер, к которому нужно обеспечить доступ из внешней сети.

Соответственно, рассмотренный выше NAT получил название статического NAT.

Для преодоления указанных недостатков был разработан динамический NAT, суть которого рассмотрим с использованием рисунка 2.

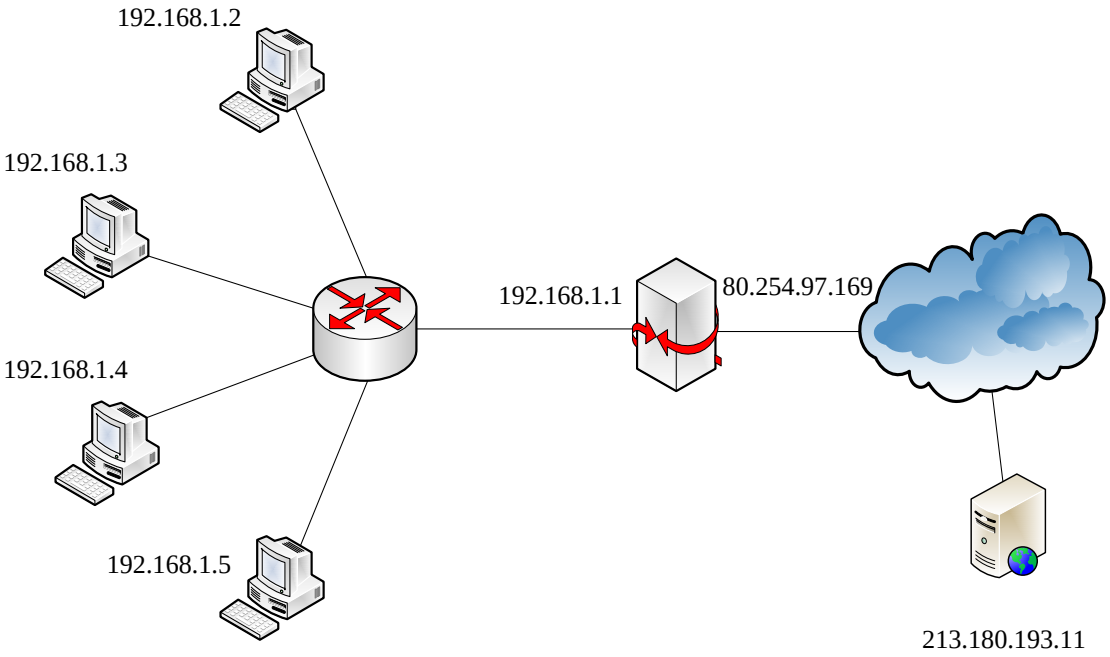

Рисунок 2 – Иллюстрация работы динамическогоNAT

На рисунке представлена внутренняя сеть, использующая частный адрес 192.168.1.0/24. Выход во внешнюю сеть организуется с использованием NAT-устройства, внешнему интерфейсу которого присвоен общедоступный адрес 80.254.97.169. Необходимо обеспечить всем четырем конечным узлам внутренней сети доступ к внешней сети, в частности, к web-серверу с адресом 213.180.193.11.

Очевидно, что статический NAT для решения такой задачи непригоден, так как доступ узлов к внешней сети осуществляется с использованием единственного внешнего адреса (на практике внешних адресов также может быть несколько, но в любом случае количество внутренних узлов превышает количество внешних адресов).

При передаче пакета во внешнюю сеть NAT-устройство может подменить частный адрес отправителя на свой общедоступный адрес, как и в статическомNAT. Однако при приеме пакета-ответа из внешней сети необходимо определить, какому из внутренних конечных узлов этот пакет нужно передать. Или, другими словами, при приеме необходимо определить, на какой частный адрес нужно изменить общедоступный адрес назначения, содержащийся в ответном IP-пакете.

Таким образом, для надежного различения принимаемых пакетов NAT-устройством необходима, помимо IP-адресов, дополнительная информация. В качестве такой информации можно использовать номера портов TCP- или UDP-сегментов, переносимых IP-пакетами. Однако в нашем примере все четыре узла могут обратиться с запросом к web-серверу с адресом 213.180.193.11, ответы которого будут иметь один и тот же номер порта 80 или 8080. Поэтому в данном случае используются так называемые назначенные номера портов. В качестве назначенных портов используются порты источника, которым в процессе передачи присваиваются значения, не стандартизированные в протоколах TCP и UDP. Назначенный порт может быть выбран произвольно, но с учетом того, что он должен быть уникален в пределах внутренней сети.

В соответствии с этим таблица NAT-устройства усложняется, в нее теперь должны входить не только IP-адреса, но и номера портов (таблица 3.3).

Поскольку описанная выше технология использует не только сетевые адреса, но и номера портов, она получила название NAPT (NetworkAddressPortTranslation) [5].

Таблица 3 – Соответствие адресов и номеров портов

Частный адрес	Порт	Общедоступный адрес	Назначенный порт
192.168.1.2	8080	80.254.97.169	61001
192.168.1.3	8080	80.254.97.169	61002
192.168.1.4	8080	80.254.97.169	61003
192.168.1.5	8080	80.254.97.169	61004

При передаче пакета, например, от узла 192.168.1.2 к серверу глобальной сети с адресом 213.180.193.11 в заголовок пакета в качестве адреса получателя будет указан 213.180.193.11, в качестве номера порта получателя – 8080. В качестве адреса отправителя будет указан 192.168.1.2, а в качестве номера порта отправителя – 8080. После приема этого пакета NAT-устройством будет произведена подмена адреса отправителя на 80.254.97.169, а номера порта отправителя на 61001. Эта информация динамически заносится в таблицу 5.3.

При приеме ответа от сервера глобальной сети будет выполнено обратное преобразование – адрес получателя будет заменен на 192.168.1.2. При этом в качестве номера порта получателя будет указан назначенный порт, который сервер укажет исходя из номера порта источника принятого сегмента. При этом NAT-устройство «поймет», какому из внутренних узлов передать пакет, используя номер назначенного порта.

Если NAT-устройство имеет несколько общедоступных адресов (пул адресов), то таблица 5.3 ведется динамически, то есть при передаче пакета запоминается, на какой именно адрес из пула была осуществлена подмена, и данная информация заносится таблицу. Эти действия, естественно, являются абсолютно прозрачными для конечных узлов.

Рассмотрим настройку протокола NAT для примера, представленного на рисунке 3.2, полагая, что в качестве NAT-устройства используется маршрутизатор Cisco.

Предположим, что в маршрутизаторе, используемом в качестве NAT-устройства, порт с адресом 192.168.1.1 является портом fa 0/0, а порт с адресом 80.254.97.169 – портом fa 0/1 (напомним, что в устройствах и программном обеспечении CiscoSystemsfa означает FastEthernet). В терминологии NAT порт fa 0/0 является внутренним портом (inside), а порт fa 0/1 – внешним портом (outside).

Пакеты, прибывающие на внутренний порт и подлежащие передаче на внешний порт, подлежат трансляции в соответствии с SourceNAT (SNAT), то есть подмене подлежит IP-адрес источника (SourceIP). Пакеты, прибывающие на внешний порт, подлежат трансляции в соответствии с DestinationNAT (DNAT), то есть подмене подлежит IP-адрес получателя (DestinationIP).

Сначала необходимо создать список доступа (подробнее списки доступа будут рассмотрены в следующем параграфе). Для этого в режиме глобального конфигурирования необходимо выполнить следующую команду:

(config)# access-list 100 permitip<адрес><инвертированнаямаска> any

Забегая вперед, отметим, что данной командой создан список доступа с номером 100, разрешающий передавать пакеты с адресом источника, указанного в команде, на любые адреса.

Пул адресов создается на маршрутизаторе в режиме глобального конфигурирования командой

(config)# ipnatpool<имя><начальный адрес><конечный адрес>netmask<маска>.

Если, как в нашем примере, используется единственный общедоступный адрес, начальный и конечный адреса в команде совпадают.

Затем назначаются внутренние и внешние интерфейсы:

- (config)# interface fa 0/0;
- (config-if)#ipnat inside (outside).

Включается NAT командой

ipnat inside source list 100 pool <имя>.

Конфигурирование маршрутизатора Cisco с использованием указанных команд для нашего примера (рисунок 2) представлен на рисунке 3.

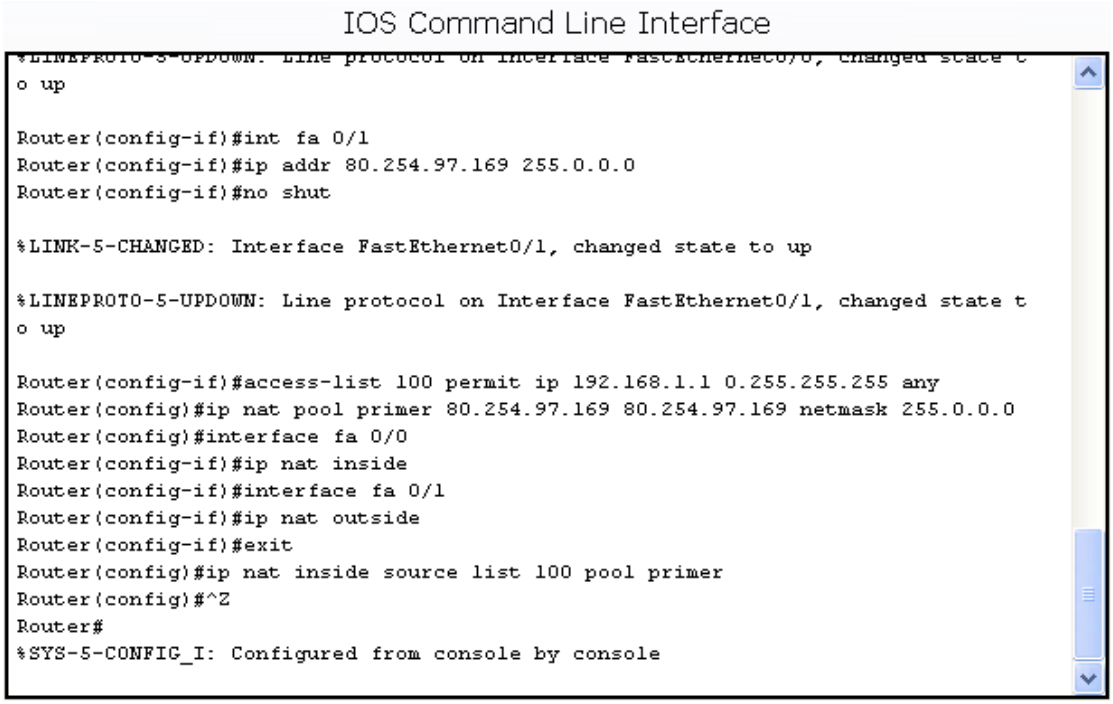

Рисунок 3 – Конфигурирование динамическогоNAT

После того, как какой-либо из внутренних узлов обменяется пакетами с внешней сетью, можно будет просмотреть трансляции адресов, произведенные NAT (рисунок 4).

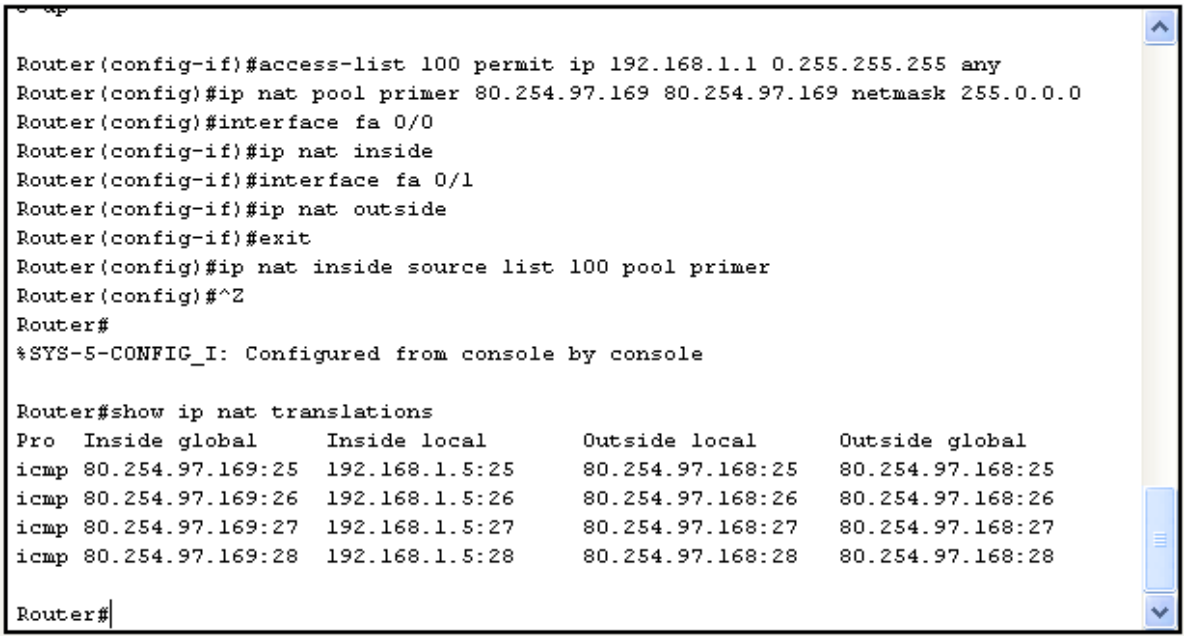

Рисунок 4 – Список трансляций

Для большей наглядности произведем обращение с внутреннего компьютера к web-серверу, расположенному во внешней сети по адресу 80.254.97.168, и опять выведем список трансляций (рисунок 5).

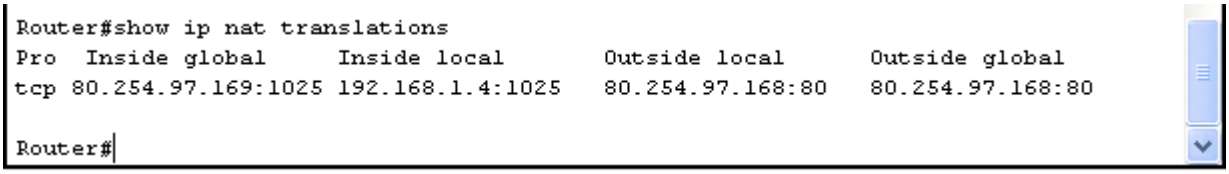

Рисунок 5 – Список трансляций после обращения к web-серверу

Из рисунка 5 следует, что была произведена одна трансляция, информация о которой представлена в четырех колонках.

Первая колонка указывает на транспортный протокол, в нашем случае это TCP.

Вторая колонка (Insideglobal) указывает на сокет (IP-адрес и номер порта), на который подменяется сокет отправителя.

Третья колонка (Insidelocal) указывает на внутреннийIP-адрес отправителя с назначенным номером порта.

Четвертая колонка (Outsidelocal) указывает на сокет узла назначения во внешней сети, который сформирован внутренним узлом-отправителем.

Пятая колонка (Outsideglobal) указывает на IP-адрес и номер порта, используемые во внешней сети.

Таким образом, из рисунка 3.5 следует, что внутренний узел с адресом 192.168.1.4 направляет пакет web-серверу с адресом 80.254.97.168. Соответственно, IP-адрес и номер порта получателя, указанные в пакете:

80.254.97.168:80 (напомним, что для протокола HTTP используются порты 80 и 8080).

IP-адрес и порт источника в этом же пакете:

192.168.1.4:80 .

При передаче пакета во внешнюю сеть маршрутизатор подменяет IP-адрес и порт источника:

80.254.97.169:1025.

Соответственно, при приеме ответного пакета от сервера сокет 80.254.97.169:1025 будет изменен на 192.168.1.4:80, и пакет получит нужный узел внутренней сети.

Задание:

1. Построить сеть, структура которой определяется преподавателем.
2. Установить внешнийwww-сервер.
3. Настроить на маршрутизаторе статическую маршрутизацию.
4. Настроить на маршрутизаторе динамический NAT.
5. Осуществить обращение к внешнему серверу, просмотреть и проанализировать списки трансляций сетевых адресов.

Контрольные вопросы:

1. Опишите все возможные схемы работы службы NAT.
2. Какие частные IP адреса используются службой NAT в каждом классе адресов?
3. Перечислите преимущества и недостатки службы NAT.
4. Перечислите этапы настройки службы NAT.
5. Опишите схему проверки работы службы NAT.
6. Опишите основные проблемы в работе сервера NAT.Что обеспечивает служба NAT?

Список литературы:

1. Манин А.А. Системы коммутации. Принципы и технологии пакетной коммутации. Учебное пособие.– Ростов-на-Дону: СКФ МТУСИ, 2014. – 108 с.

Практическое занятие № 6
Конфигурирование списков управления доступом ACL

Цели занятия: Получить первичные навыки фильтрации трафика в пакетных сетях.

Задание. Рассмотреть общую теорию управления доступом ACL. Уяснить синтаксис команд для работы. Для указанных исходных данных произвести построения схемы сети. Настроить необходимую адресацию. Настроить списки доступа.

Списки доступа ACL (AccessControlList) позволяют создавать правила управления трафиком, по которым будет происходить межсетевое взаимодействие как в локальных, так и в корпоративных сетях.

Существует шестнадцать типов списков доступа, но наиболее часто используются два типа: standart – стандартные (номера с 1 по 99) и extended – расширенные (номера с 100 по 199 или с 2000 по 2699). Различия между этими двумя списками заключаются в возможности фильтровать пакеты не только по IP – адресу, но и по другим различным параметрам.

Стандартные списки обрабатывают только входящие IP адреса источников, т.е. ищут соответствие только по IP адресу отправителя. Расширенные списки работают со всеми адресами корпоративной сети и дополнительно могут фильтровать трафик по портам и протоколам.

Работа списка доступа напрямую зависит от порядка следования строк в этом списке, где в каждой строке записано правило обработки трафика. Просматриваются все правила списка с первого до последнего по порядку, но просмотр завершается, как только было найдено первое соответствие, т.е. для пришедшего пакета было найдено правило, под которое он подпадает. После этого остальные правила списка игнорируются. Если пакет не подпал ни под одно из правил, то включается правило по умолчанию:

access-listномер_списка deny any

которое запрещает весь трафик по тому интерфейсу сетевого устройства, к которому данный список был применен.

Для того, чтобы начать использовать список доступа, необходимо выполнить следующие три этапа:

1 – создать список;

2 – наполнить список правилами обработки трафика;

3 – применить список доступа к интерфейсу устройства на вход или на выход этого интерфейса.

Этап первый – создание списка доступа:

Стандартныйсписок:

Switch3(config)#ip access-list standart 10

(создается стандартный список доступа под номером 10, в данном случае создается на коммутаторе).

Расширенныйсписок:

Router1(config)#ip access-list extended 100

(создается расширенный список доступа под номером 100, в данном случае создается на маршрутизаторе).

Этап второй – ввод правил в список доступа:

Каждое, правило в списке доступа сдержит три важных элемента:

1 - число, идентифицирующее список при обращении к нему в других частях конфигурации маршрутизатора или коммутатора третьего уровня;

2 - инструкцию deny (запретить) или permit (разрешить);

3 - идентификатор пакета, который задается по одному из трех вариантов:

- адрес сети (например 192.168.2.0 0.0.0.255) – где вместо маски подсети указывается шаблон маски подсети;

- адрес хоста (host 192.168.2.1);

- любой IP адрес (any).

Пример стандартного списка доступа №10:

access-list 10 denyhost 11.0.0.5

access-list 10 deny 12.0.0.0 0.255.255.255

access-list 10 permit any

В этом списке:

- запрещен весь трафик хосту с IP адресом 11.0.0.5;

- запрещен весь трафик в сети 12.0.0.0/8 (в правиле указывается не реальная маска подсети, а ее шаблон);

- весь остальной трафик разрешен.

В расширенных списках доступа вслед за указанием действия ключами permit или deny должен находиться параметр с обозначением протокола (возможны протоколы IP, TCP, UDP, ICMP), который указывает, должна ли выполняться проверка всех пакетов IP или только пакетов с заголовками ICMP, TCP или UDP. Если проверке подлежат номера портов TCP или UDP, то должен быть указан протокол TCP или UDP (службы FTP и WEB используют протокол TCP).

При создании расширенных списков в правилах доступа можно включать фильтрацию трафика по протоколам и портам. Для указания портов в правиле доступа указываются следующие обозначения (таблица 1):

Таблица 1

обозначение	действие
lt n	Все номера портов, меньшие n.
gt n	Все номера портов, большие n.
eq n	Порт n
neq n	Все порты, за исключением n.
range n m	Все порты от n до m включительно.

Распространенные приложения и соответствующие им стандартные номера портов приведены в следующей таблице2:

Таблица 12.

Номер порта	Протокол	Приложение	Ключевое слово в команде access_list
20	TCP	FTP	dataftp_data
21	TCP	Управление сервером FTP	ftp
22	TCP	SSH	
23	TCP	Telnet	telnet
25	TCP	SMTP	Smtp
53	UDP, TCP	DNS	Domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	Tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	Snmp

Пример расширенного списка доступа №111:

! Запретить трафик на порту 80 (www-трафик)

ip access-list 111 deny tcp any anyeq 80

ip access-list 111 deny ip host 10.0.0.15 host 12.0.0.5

ip access-list 111 permit ip any any

interfaceethernetO

! Применить список доступа 111 к исходящему трафику

ipaccess-group 111 out

В этом списке внешние узлы не смогут обращаться на сайты внутренней сети, т.к. список доступа был применен на выход (для внешних узлов) интерфейса, а так же узлу 10.0.0.15 запрещен доступ к узлу 12.0.0.5

Остальной трафик разрешен.

Этап третий – применение списка доступа.

Списки доступа могут быть использованы для двух типов устройств:

1 – на маршрутизаторе;

2 - на коммутаторе третьего уровня.

На каждом интерфейсе может быть включено два списка доступа: только один список доступа для входящих пакетов и только один список для исходящих пакетов.

Каждый список работает только с тем интерфейсом, на который он был применен и не действует на остальные интерфейсы устройства, если он там не применялся.

Однако один список доступа может быть применен к разным интерфейсам.

Применение списка доступа к устройству осуществляется следующими командами:

interface ethernet0/0/0

ip access-group 1 in

ipaccess-group 2 out

В данном случае к интерфейсу ethernet0/0/0 применили два списка доступа:

список доступа №1 – на вход интерфейса (т.е. для внутренних адресов);

список доступа №2 – на выход интерфейса (применение к внешней сети).

Чтобы просмотреть все созданные списки доступа и применение их к интерфейсам устройства используйте следующие команды:

Команда просмотра списков доступа:

Router# Shaccess-list

Просмотр текущей конфигурации устройства и привязки списков к интерфейсам:

Router# Showrunning-config

Просмотр сохраненной конфигурации:

Router# Show configuration

Сохранениетекущейконфигурации:

Router# write memory

Или

Router# copyrunstart

Команда удаления списка доступа:

interfaceethernet0/0/0 - выбор нужного интерфейса

noaccess-listномер_списка – удаление списка в выбранном интерфейсе

Задание для работы

Создайте схему сети, как показано на рис.1.

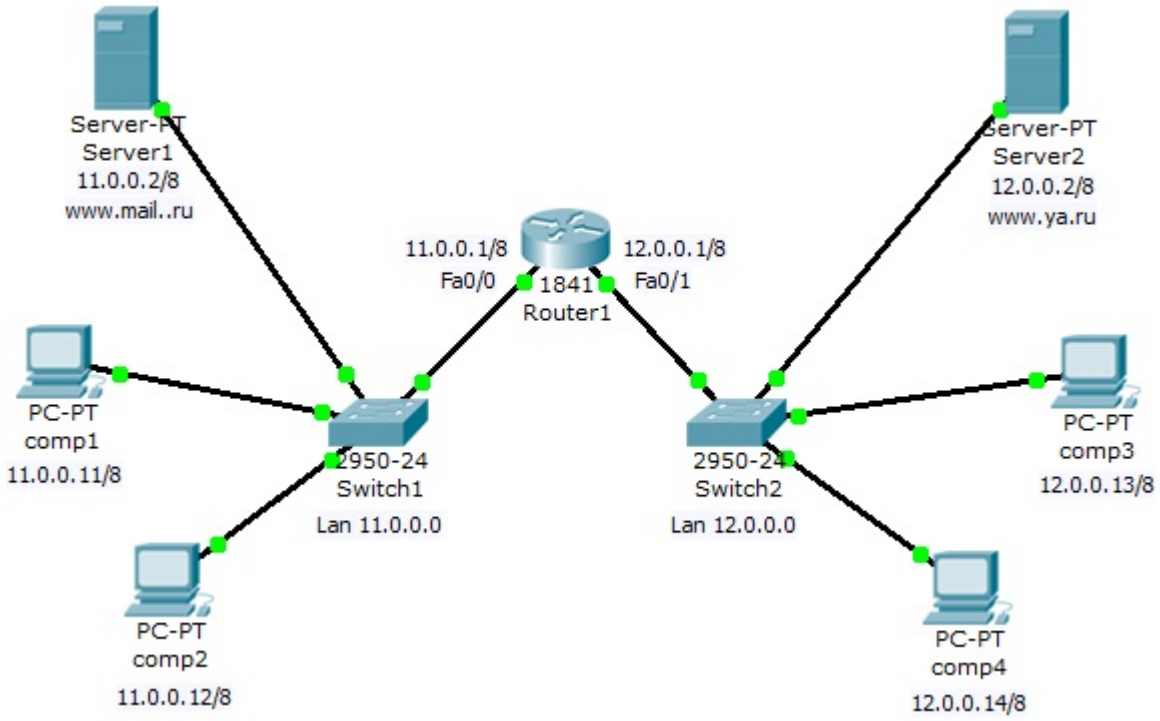

Рисунок 1 - Схема корпоративной сети

Задача (номера подсетей устанавливаются преподавателем):

1 - Компьютеры comp1 и comp2 должны открывать все сайты, но им запрещено входить на компьютеры comp3 и comp4.

2 - Компьютеры comp3 и comp4 доступны друг для друга и должны открывать только сайт своей сети, сеть 11.0.0.0 для них недоступна.

Создадим стандартный список доступа, где укажем правила блокировки на хосты comp3 и comp4 и применим этот список на выход интерфейса Fa0/0.

Включите привилегированный режим и войдите в конфигурацию роутера:

Router1>en

Router1#conft

Создадим стандартный список доступа и введем правила доступа:

Router1(config)#ip access-list standard 10

Router1(config-std-nacl)#deny host 12.0.0.13

Router1(config-std-nacl)#deny host 12.0.0.14

Router1(config-std-nacl)#permit any

Здесь мы разрешили весь трафик, за исключением двух адресов: 12.0.0.13 и 12.0.0.14.

Просмотрим созданный список доступа в настройках роутера. Для этого надо выйти из режима конфигурации роутера и ввести команду просмотра списков на устройстве shaccess-list:

Router1#sh access-list

Standard IP access list 10

deny host 12.0.0.13

deny host 12.0.0.14

permit any

Router1#

Применим созданный список на выход интерфейса Fa0/0:

Router1#

Router1#conf t

Router1(config)#interface fa0/0

Router1(config-if)#ip access-group 10 out

В результете того, что список доступа был применен к выходу интерфейса сети 11.0.0.0 мы получили следующую политику доступа:

1 – пакеты, входящие на роутер из сети 11.0.0.0 получают блокировку на два внешних адреса – 12.0.0.13 и 12.0.0.14;

2 – всем внешним пакетам, входящим из роутера в сеть 11.0.0.0 разрешается все, кроме двух адресов - 12.0.0.13 и 12.0.0.14 (этим адресам запрещен вход в сеть 11.0.0.0)

Просмотрим привязку списка доступа к интерфейсу Fa0/0 в конфигурации роутера:

Router1(config-if)#exit

Router1(config)#exit

Router1#

Router1#shrunning-config

Используя данную команду, вы увидите полную конфигурацию роутера, в том числе и привязку списка доступа к конкретному интерфейсу (в данном случае на выход интрфейса):

interface FastEthernet0/0

ip address 11.0.0.1 255.0.0.0

ip access-group 10 out

duplexauto

speedauto

!

Проверьте созданную политику доступа к ресурсам сети. Должны выполняться следующие правила:

1 - компьютеры comp3 и comp4 доступны друг для друга и должны открывать только сайт своей сети, вход в сеть 11.0.0.0 им заблокирован;

2 – сервера Server2 доступен всем ресурсам сети;

3 - компьютерам comp1 и comp2 доступны все ресурсы, кроме адресов 12.0.0.13 и 12.0.0.14.

Контрольные вопросы:

1. Какие параметры контролирует расширенные списки доступа?

2. Приведите пример команды, разрешающей передачу пакетов от хоста на все веб-сервера.

3. Перечислите основные типы списков доступа.

4. Что такое шаблон маски подсети и приведите примеры его использования в списках доступа.

5. Какое правило обработки сетевого трафика задает следующий список доступа: Ipaccess-list 111 denytcpanyanyeq 80.

6. Локальная сеть соединена с роутером по интерфейсу Fa0/0, а внешняя сеть соединена по интерфейсу Fa0/1. Из локальной сети запрещен вход во внешнюю сеть, а из внешней сети запрещено входить на FTP сервер, расположенный во внутренней сети. Для реализации этих правил был создан список доступа. Назовите интерфейс и в каком направлении (на вход или на выход), к которому следует применить созданный список доступа.

7. Для какого варианта не может быть проведено сравнение на основе расширенного списка доступа IP?

- протокол;
- IP адрес отправителя;
- IP адрес получателя;
- имя файла для передачи по протоколу FTP.

8. Назовите, какой шаблон маски соответствует сети 10.16.0.0./12?

9. В списке доступа содержится следующее правило: Permitanyhost 192/168/1/1/it 25. Какие номера портов оно обрабатывает?

10. Напишите правило доступа для входа в любую сеть вашей схемы.

Список источников:

1. Д. Бони. Руководство по Cisco IOS. Изд. Питер, Русская Редакция, 2008, 786 с.

2. К. Кеннеди, К. Гамильтон. Принципы коммутации в локальных сетях Cisco. Изд. Вильямс, 2003,976 с.

Практическое занятие № 7
Конфигурирование виртуальной локальной сети VLAN

Задание. Рассмотреть общую теорию создания виртуальных сетей. Уяснить синтаксис команд для работы. Для указанных исходных данных произвести построения схемы сети. Настроить необходимую адресацию. Настроить виртуальные локальные сети в соответствии с заданием.

Конфигурирование виртуальных сетей

Виртуальные локальные сети VLAN – это технология, позволяющая организовывать несколько независимых виртуальных сетей внутри одной физической сети. С помощью VLAN можно выполнять гибкое разнесение пользователей по различным сегментам сети с разной адресацией, даже если они подключены к единому устройству, а также дробить широковещательные домены.

Принцип организации двух VLAN на одном коммутаторе иллюстрируется рисунком 1.

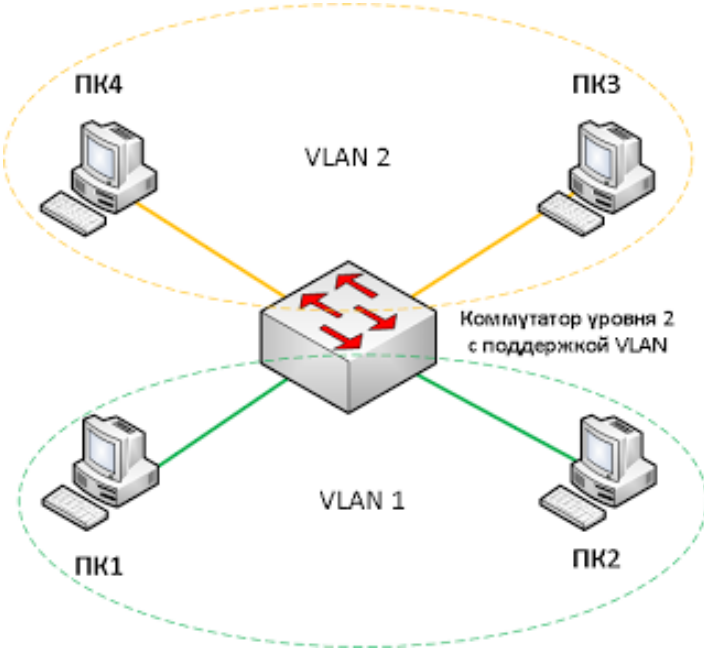

Рисунок 1 – Организация двух VLAN на одном коммутаторе

Компьютеры 1 и 2 объединены в одну VLAN, компьютеры 3 и 4 объединены в другую VLAN. Хотя все компьютеры подключены к одному и тому же коммутатору, все они не смогут общаться между собой. Компьютер

номер 1 сможет общаться только с компьютером 2, компьютер 3 будет видеть только компьютер 4. То есть данная ситуация будет аналогична тому, как если бы мы подключили компьютеры 1 и 2 к одному коммутатору, а компьютеры 3 и 4 к другому коммутатору, и не соединили бы эти коммутаторы между собой. Как легко заметить, в данном случае, технология VLAN помогла нам разделить единую физическую сеть на несколько виртуальных не связанных между собой сетей, при этом компьютеры, находящиеся в этих виртуальных сетях, работают точно так же, как это было бы в обычной сети.

Для взаимодействия устройств в VLAN сетях их порты настраиваются специальным образом. Существует два типа настройки портов: настройка порта в режиме доступа (AccessMode) и настройка порта в режиме магистрали (TrunkMode).

Порты доступа применяются обычно для подключения оконечных устройств. В простейшем случае, порту доступа задается определеннаяVLAN, и он передает весь поступающий на него трафик именно в нее. Порты, к которым подключены компьютеры 1,2,3 и 4 на рисунке 2, являются портами доступа. Магистральные порты предназначены для передачи трафика сразу нескольких VLAN и обычно используются для соединения сетевых устройств между собой. Порты 5 обоих коммутаторов на рисунке 2, являются магистральными портами.

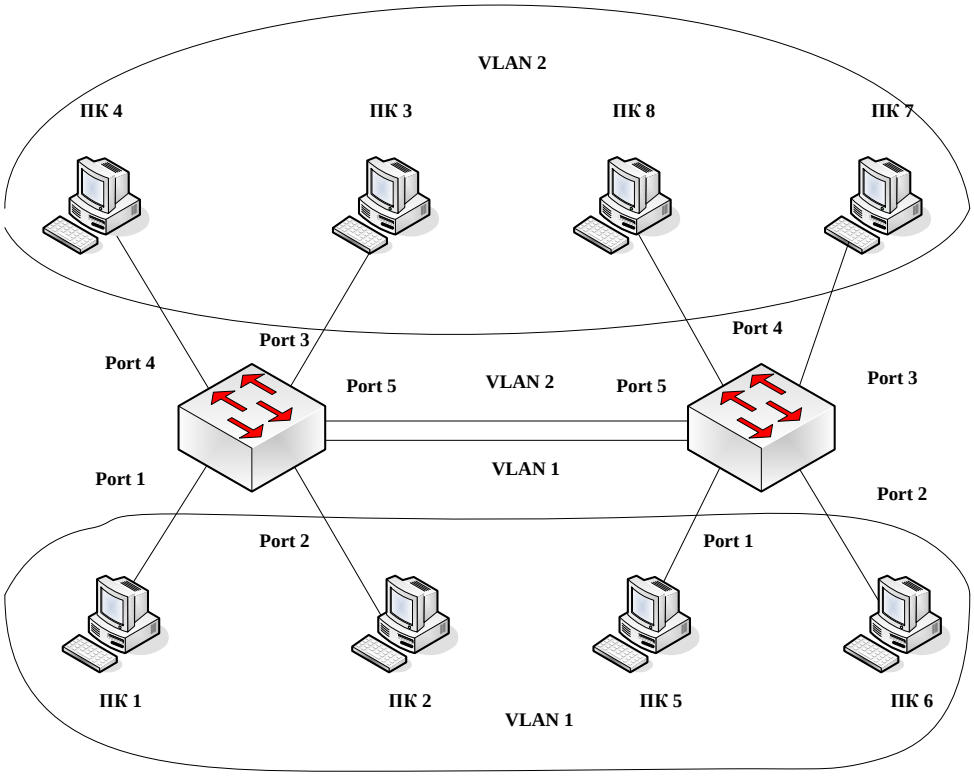

Рисунок 2 – Использование магистральных портов и портов доступа

На данном рисунке порты 1 – 4 работают в режиме доступа, порт 5 – в режиме магистрали и передает через себя трафик сразу двух виртуальных локальных сетей VLAN 1 и VLAN 2 (поэтому условно на рисунке порты 5 обоих коммутаторов связаны между собой двумя линиями, хотя физически это – одна линия).

Передавать трафик VLAN между коммутаторами можно не только с помощью магистральных портов, но и с помощью портов доступа, но так как порты доступа могут пропускать трафик только одной VLAN, для соединения устройств между собой потребуется выделение портов, количество которых будет равно количеству передаваемых между устройствами VLAN. Данный способ обычно находит применение только в том случае, если между устройствами необходимо передать трафик небольшого числа VLAN.

Для настройки VLAN необходимо перейти в привилегированный режим, выполнив команду enable. Информацию о существующих на

коммутаторе VLAN можно, выполнив команду showvlanbrief (можно просто shvlbr).

Рассмотрим пример создания двух VLAN на одном коммутаторе. Для этого по-прежнему будем использовать сеть, представленную на рисунке 3.10. Перейдем в привилегированный режим, выполнив команду enable, и просмотрим информацию о существующих на коммутаторе VLAN(рисунок 3).

В результате выполнения команды на экране появится: номера VLAN – первый столбец; название VLAN - второй столбец; состояние VLAN (работает она в данный момент или нет) – третий столбец; порты, принадлежащие к данной VLAN – четвертый столбец. Как мы видим, по умолчанию на коммутаторе существует пять VLAN . Все порты коммутатора по умолчанию принадлежат VLAN 1. Остальные четыре VLAN являются служебными и используются не очень часто.

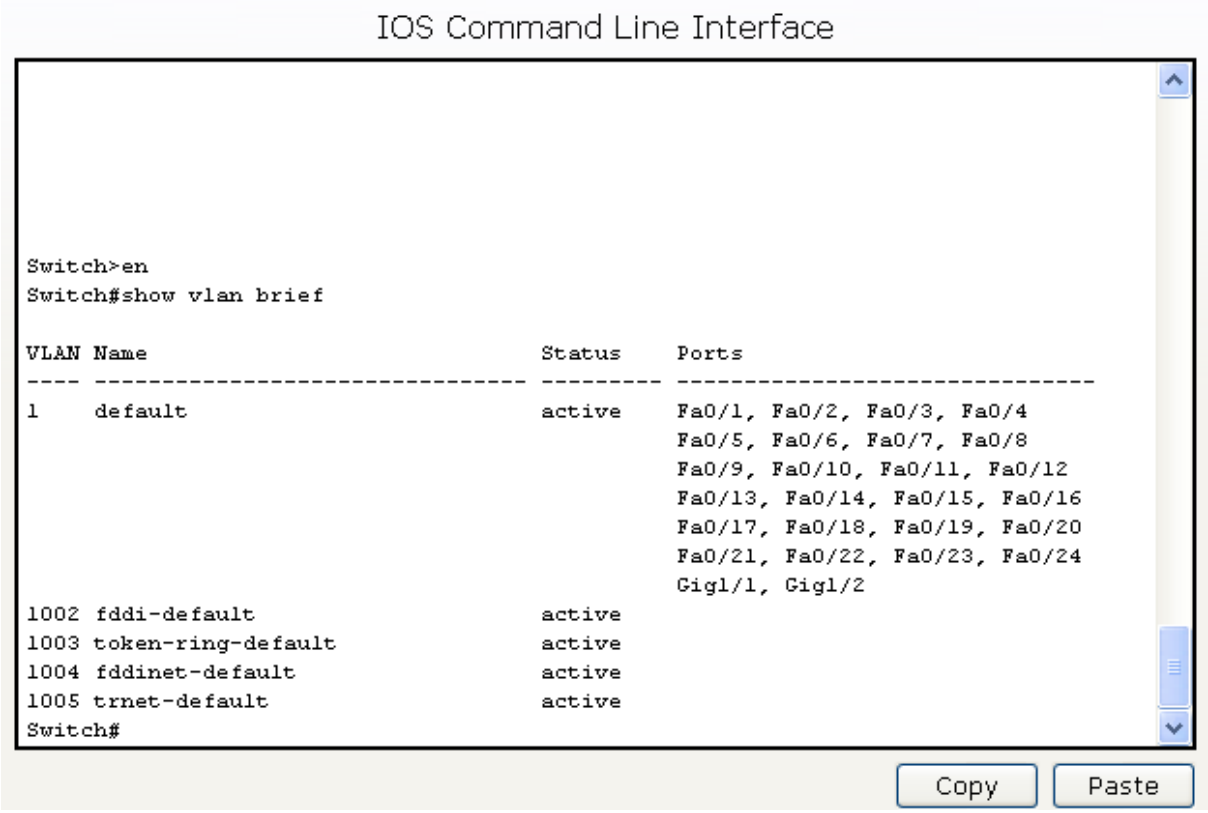

Рисунок 3 – Просмотр конфигурации VLAN

Для реализации сети, которую мы запланировали сделать, создадим на коммутаторе еще две VLAN. Для этого в привилегированном режиме необходимо выполнить команду conft для перехода в режим глобального конфигурирования. Вводим команду vlan 2. Данной командой создается на коммутаторе VLAN с номером 2. Указатель ввода Switch(config)# изменится на Switch(config-vlan)#, это свидетельствует о том, что конфигурируется уже не весь коммутатор в целом, а только отдельнаяVLAN, в данном случае номер 2. Если использовать команду «vlanx», где x номер VLAN, когда VLANx еще не создана на коммутаторе, то она будет автоматически создана и будет осуществлен переход к ее конфигурированию.

Для решения поставленной задачи коммутатор необходимо сконфигурировать следующим образом.

```
Switch(config)#vlan 2
Switch(config-vlan)#name subnet_192
Switch(config)#interface range fastEthernet 0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
```

Разберем данную конфигурацию. Как уже говорилось ранее, командой vlan 2 мы создаем на коммутаторе новуюVLAN с номером 2. Команда namesubnet_192 присваивает имя subnet_192 виртуальной сети номер 2. Выполняя команду interfacerangefastEthernet 0/1-2, мы переходим к конфигурированию интерфейсов fastEthernet 0/1 и fastEthernet 0/2 коммутатора. Ключевое слово range в данной команде указывает на то, что мы будем конфигурировать не один единственный порт, а целый диапазон портов, в принципе ее можно не использовать, но тогда последние три строки придется заменить на:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/2
```

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 2

Команда switchportmodeaccess конфигурирует выбранный порт коммутатора, как порт доступа. Команда switchportaccessVLAN 2 указывает, что данный порт является портом доступа для VLAN номер 2.

Как и в предыдущих примерах, команды можно набирать сокращенно, кроме того, вместо fastEthernet можно использовать обозначение fa.

Просмотрим результат конфигурирования, выполнив команду showvlanbr еще раз, рисунок 4.

Из рисунка видно, что в коммутаторе появилась вторая VLAN с именем subnet_192, к которой относятся порты 0/1 и 0/2.

Далее аналогичным образом создадим vlan 3 с именем subnet_172, и сделаем его портами доступа интерфейсы fastEthernet 0/3 и fastEthernet 0/4.

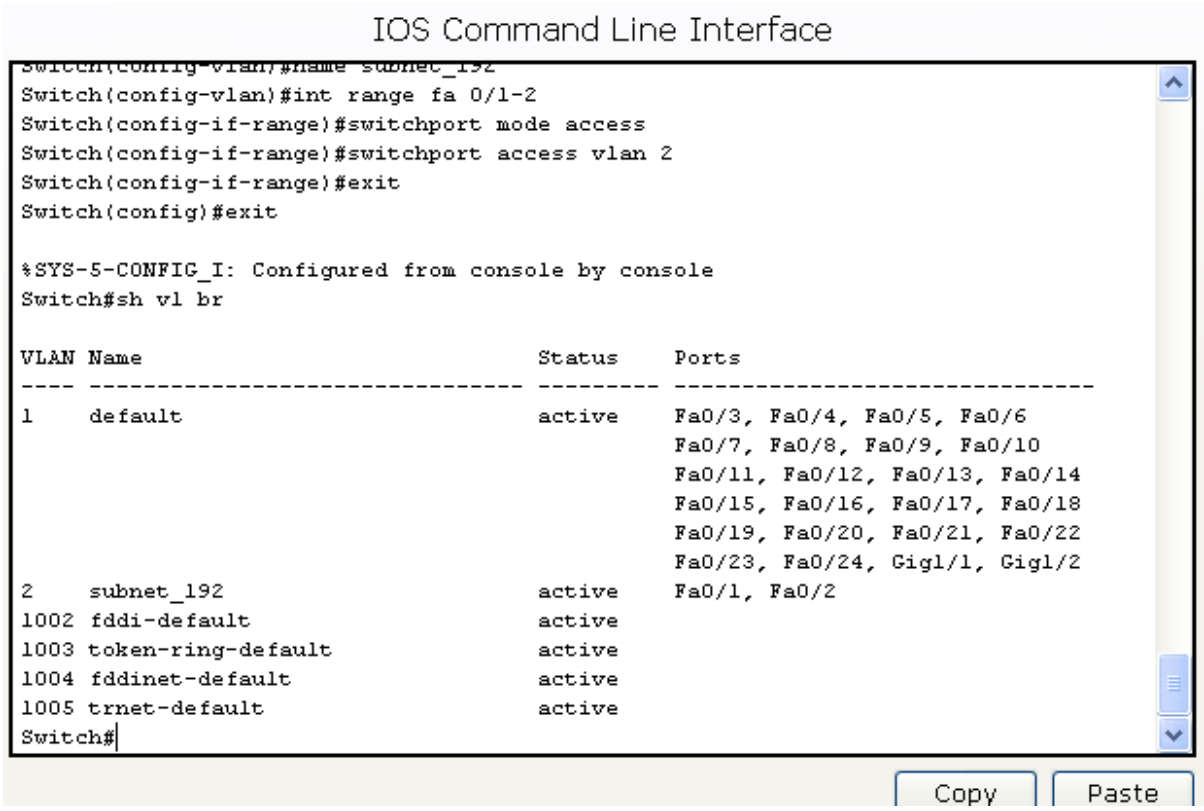

Рисунок 4 – Просмотр конфигурации VLAN

Соответственно, компьютеры, находящиеся в разных виртуальных сетях, будут недоступны друг другу, что легко проверить с использованием утилиты **ping**.

Наибольшую практическую ценность представляет конфигурирование VLAN на нескольких коммутаторах с использованием магистральных портов, как это иллюстрируется рисунком 2. Рассмотрим конфигурирование коммутаторов в этом случае.

Рассмотрим сеть, показанную на рисунке 5.

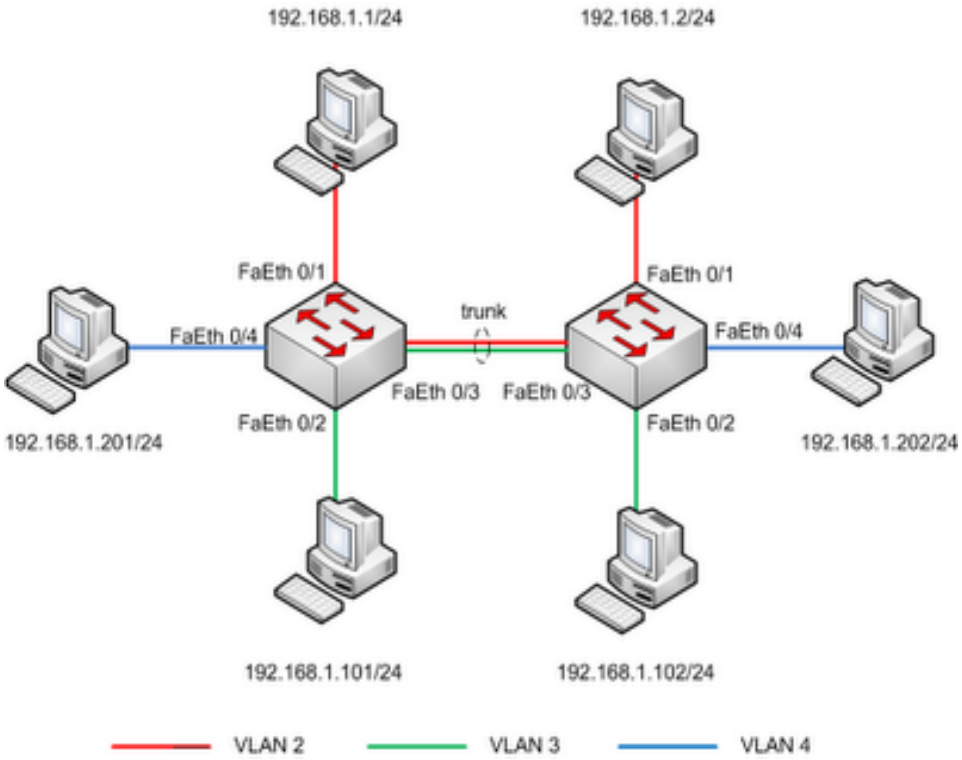

Рисунок 5 – Конфигурирование коммутаторов

По аналогии с предыдущим примером произведем конфигурирование обоих коммутаторов:

```
Switch(config)#vlan 2
Switch(config-vlan)#name subnet_2
Switch(config-vlan)#intfa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
```

Switch(config)#vlan 3

Switch(config-vlan)#name subnet_3

Switch(config-vlan)#intfa 0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 3

Switch(config-if)#exit

Switch(config)#vlan 4

Switch(config-vlan)#name subnet_4

Switch(config-vlan)#intfa 0/4

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 4

Switch(config-if)#exit

Как следует из перечня команд, на обоих коммутаторах созданы три VLAN. Теперь необходимо сконфигурировать на третьем порту каждого из коммутаторов магистральный режим:

Switch(config)#intfa 0/3

Switch(config-if)# switchport mode trunk

В результате трафик всех трех созданных ранее VLAN будет проходить через порт 3.

Используя на интерфейсе команду switchportmodetrunk, мы перевели его в магистральный режим, в котором интерфейс пропускает через себя трафик всех существующх на коммутаторе VLAN, но иногда необходимо передавать через данный интерфейс трафик не всех VLAN, а лишь некоторых. Для этого на обоих коммутаторов выполним команды:

Switch(config)#interfacefastEthernet 0/3

Switch(config-if)#switchport trunk allowed vlan 2-3

Команда "switchporttrunkallowedvlan 2-3" указывает магистральному порту коммутатора, трафик каких VLAN ему пропускать через себя. После того, как будет выполнена эта команда, компьютер PC4 должен перестать видеть компьютер PC5. Команда "switchporttrunkallowedvlan" при своем

использовании каждый раз задает разрешенные порты заново, то есть если выполнить команду switchporttrunkallowedvlan 5, а потом выполнить команду switchporttrunkallowedvlan 6, то разрешенным окажется только трафик VLAN номер 6. Для добавления VLAN к списку разрешенных служит команда switchporttrunkallowedvlanx, где x номер добавляемого VLAN. Для удаления VLAN из списка разрешенных используется команда switchporttrunkallowedvlanremovex, где x номер удаляемого VLAN. Для просмотра информации о настроенных на коммутаторе магистральных портах служит команда showinttrunk.

Таким образом, с использованием коммутаторов второго уровня единую сеть можно разделить на виртуальные сети с изолированным друг от друга трафиком. Однако на практике часто возникают задачи гибкого объединения нескольких VLAN между собой. Эту задачу решают маршрутизаторы и коммутаторы третьего уровня, которые будут рассмотрены ниже.

Необходимо отметить, что рассмотренная выше терминология (Access-порт, Trunk-порт) характерна только для устройств CiscoSystems. В ряде случаев порты, способные пропускать через себя трафик нескольких VLAN, называются тэгированными (tagging). Объясняется это тем, что такой порт перед передачей кадра помещает в него дополнительную информацию (тэг), анализируя которую, принимающий порт имеет возможность определить номер VLAN, к которой этот кадр относится. Соответственно, принимающий порт этот тэг удаляет.

Порты, не вносящие изменений в передаваемые кадры (Access-порты в терминологии Cisco), называются нетэгированными (untagging).

Задание для работы.

Каждый студент выполняет проект в одном варианте, номер варианта определяется последней цифрой студенческого билета (СБ) и одной последней цифрой текущего года (Г).

Внешний IP-адрес класса B проектируемой сети выбирается исходя из таблицы 1.

Таблица 1 – ВнешнийIP-адрес проектируемой сети

СБ	IP-адрес	СБ	IP-адрес
1	135.12.00	6	214.125.0.0
2	128.34.0.0	7	138.234.0.0
3	65.20.0.0	8	85.76.0.0
4	112.38.0.0	9	75.89.0.0
5	94.56.0.0	0	76.94.0.0

Количество виртуальных локальных сетей представлено в таблице 2.

Таблица 2 – Количество виртуальных локальных сетей

СБ	Кол-во VLAN	СБ	Кол-во VLAN
1	5	6	7
2	6	7	8
3	4	8	12
4	9	9	11
5	10	0	3

Внутренняя адресация сети должна использовать частные адреса класса C, до разделения проектируемой сети на подсети адрес сети определяется исходя из значения Г в соответствии с таблицей 3.

Таблица 3 – Внутренняя адресация проектируемой сети

Г				
1,0	2,9	3,6	4,7	8,5
192.168.10.0	192.168.15.0	192.168.20.0	192.168.25.0	192.168.30.0

Количество пользователей каждой VLAN определяется как сумма СБ+5. Например, студент с СБ 12 проектирует сеть, у которой количество пользователей в каждой VLAN должно быть не меньше

1+2+5=7.

VLAN организуются на базе коммутаторов, поддерживающих данную технологию. Разделение адресного пространства между VLAN осуществляется с использованием маски переменной длины (VLSM) с учетом таблицы 2 и количества пользователей.

Контрольные вопросы:

1. Для чего создаютсявиртуальные локальные сети и каковы их достоинства?
2. Как связываются между собой VLAN и порты коммутатора?
3. Как обеспечивается общение между узлами разных виртуальных сетей?
4. Как обеспечивается управление виртуальными локальными сетями?
5. Можно ли построить VLAN на несколькихкоммутаторах и как это сделать?
6. Для чего служит идентификатор кадра (tag) и где он размещается?
7. Что такое транковый порт и зачем он создаётся?
8. Как он создается транковый порт на коммутаторе и маршрутизаторе?
9. Какие команды используются для назначения VLAN на интерфейсы?
10. Какие команды используются для создания транковых соединений?
11. Какие команды используются для верификации VLAN?