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»

Методические указания для проведения лабораторныхработ и практических занятий по дисциплине Сетевые технологии (интернет-технологии)

(направление подготовки 10.03.01 Информационная безопасность)

Ростов-на-Дону
2022

Методические указания для проведения
лабораторныхработ и практических занятий
по дисциплине
Сетевые технологии (интернет-технологии)

(направление подготовки 10.03.01 Информационная безопасность)

Составитель: И.А. Сосновский, доцент кафедры ИТСС

Рассмотрено и одобренона заседании кафедры
Протокол от «29» августа 2022 г. № 1

Лабораторная работа №1. Расчет телефонной нагрузки при проектировании АТС и распределение ее по направлениям межстанционных связей.

Цель работы: исследование вопросов распределения трафика в сетях общего пользования и привитие первичных навыков расчета объемов коммутационного оборудования при проектировании сетей связи.

Задание.

Существующая сеть связи общего пользования (ССОП) содержит две АТС – координатную (АТСК) и электронную (АТСЭ). Кроме того, имеются узел спецслужб (УСС) и выход на зоновый узел связи (ЗУС). Необходимо произвести расчеты, позволяющие спроектировать на сети третью цифровую АТС в соответствии с исходными данными для одного варианта.

Произвести расчет интенсивности нагрузки для цифровой системы коммутации с учетом заданных характеристик и приведенной на рисунке 1 схемы сети связи.

Номер варианта определяется двумя последними цифрами студенческого билета и одной последней цифрой текущего года.

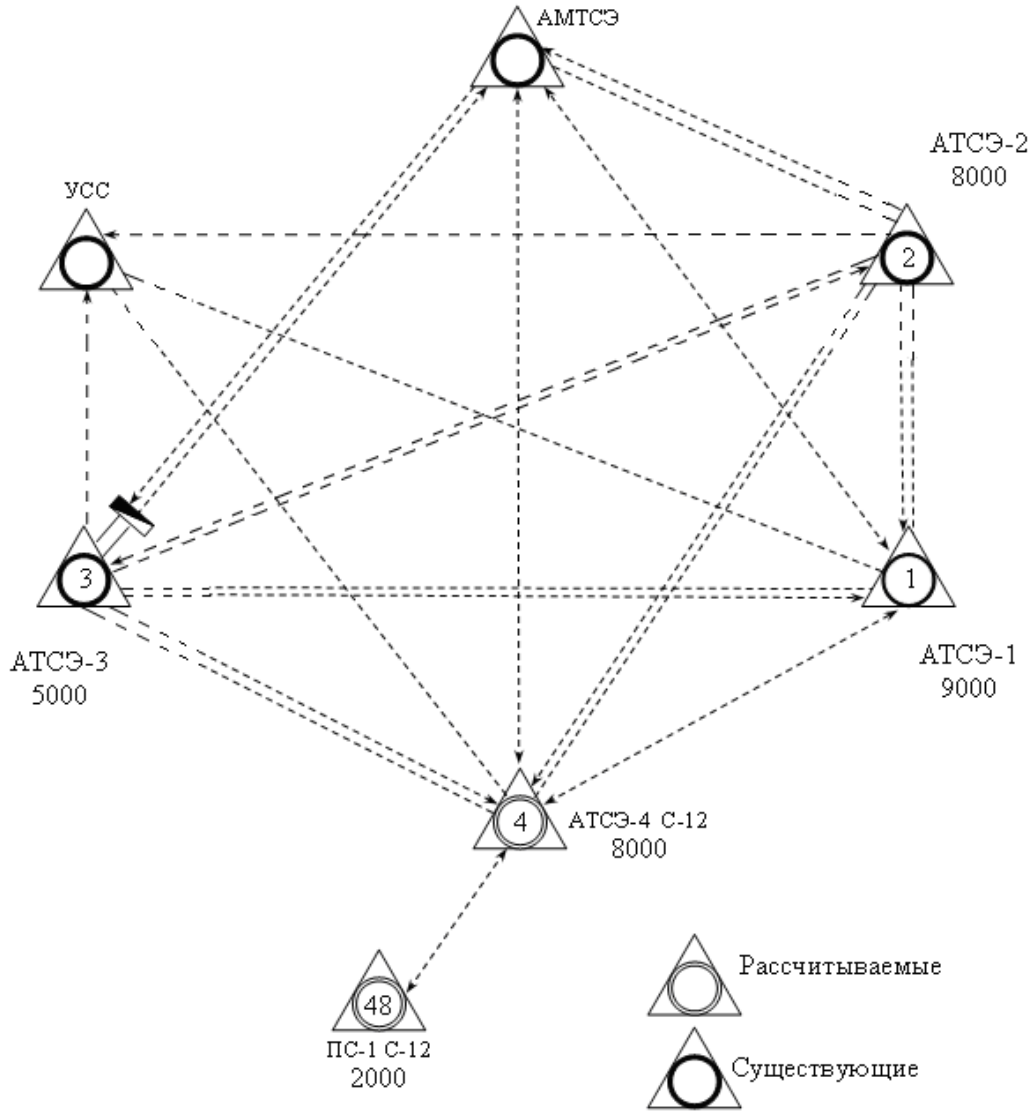


Рисунок 1 – Схема сети связи

Сведения о телефонной сети и рассчитываемой станции представлены в таблице 3.

В верхней строке таблицы 3 указана емкость рассчитываемой станции электронного типа. Во второй строке приведено число подстанций (цифра слева) и емкость каждой подстанции в тысячах номеров (цифра справа). В последующих строках указаны емкости существующих АТС 1, 2 и 3 соответственно

Таблица 3 – Сведения о телефонной сети и рассчитываемой станции

АТСЭ, тыс. номеров		7	8	6	5	9	
ПС		2x1	1x2	2x2	2x2	1x1	
Цифры единиц	1	6\7\8	5\8\9	7\7\9	-\5\8	-\8\6	0,5
	2	-\6\7	6\5\7	6\8\9	-\6\8	8\7\5	0,52
	3	7\9\5	-\5\9	-\7\8	6\6\9	7\8\9	0,55
	4	9\5\6	-\5\7	6\7\8	6\7\8	-\9\8	0,6
	5	9\5\6	6\7\-	-\7\9	7\8\9	9\8\7	0,58
	6	9\5\6	-\5\7	5\8\5	8\7\6	-\9\8	0,5
	7	-\5\8	5\6\9	7\6\9	5\8\7	7\6\5	0,67
	8	6\5\9	-\7\9	8\6\5	-\9\6	5\7\8	0,6
	9	-\7\5	5\6\7	4\9\9	6\5\7	7\5\9	0,58
	0	5\6\8	7\8\5	6\5\8	-\7\9	7\8\9	0,56
		1,6	2,7	3,8	4,9	5,0	P
		Цифры десятков					

Сведения о поступающей нагрузке представлены в таблице 4.

Таблица 4 – Сведения о поступающей нагрузке

% физ. лица		45-42	48-30	50-35	35-55	37-25	Категория терминала
% юр. лица		53-10	50,2-15	48,5-16	62,5-30	60,2-10	
% таксофоны		2,0-15	1,8-10	1,5-6	2,5-10	2,8-9	
Цифры единиц	1	2,8/1,2/9	2,7/1,1/8	2,6/1,1/8	3/1,2/10	2,9/0,9/9	85/100/110
	2	2,6/1,1/8	3/1,1/10	3,2/0,9/9	3/1,1/8	2,4/1,2/8	90/100/110
	3	2,9/1,0/8	2,5/1,2/9	3,0/1,1/8	2,6/1,1/9	3,2/0,9/9	85/110/110
	4	2,4/1,2/9	3/1,1/10	3,1/0,9/9	3/1,1/10	3,1/1,1/9	90/115/110
	5	2,5/1,2/8	2,8/0,9/9	2,8/1,2/9	3/1,0/10	3/1,1/9	88/125/110
	6	2,7/1,1/9	2,4/1,2/9	2,5/1,1/9	3/1,1/8	2,6/1,1/8	86/110/110
	7	3/1,1/10	2,6/1,1/8	2,7/1,0/8	2,5/1,2/9	2,8/0,9/9	92/115/110
	8	3,2/0,9/8	2,5/1,2/8	3/1,0/9	2,8/1,2/9	3,1/0,9/8	91/125/110
	9	2,8/1,1/9	2,9/1,0/9	3,1/1,1/8	3,2/0,9/8	2,5/1,2/9	89/120/110
	0	2,6/1,2/8	2,8/1,1/9	3/1,1/10	2,4/1,2/9	2,6/1,1/9	87/125/110
		1,0	2,9	3,8	4,7	5,6	Ткв, Тн\х, Тт
		Цифры десятков					Средняя продолжительность разговора

Методические указания к задаче

Возникающую нагрузку создают вызовы (заявки на обслуживание), поступающие от абонентов (источников нагрузки) и занимающие на некоторое время различные соединительные устройства станции. Интенсивность местной возникающей нагрузки может быть определена, если известны ее основные параметры, к которым относятся:

— число источников нагрузки N;

— среднее число вызовов, поступающих от одного источника нагрузки в ЧНН (или в единицу времени) C;

— средняя длительность занятия коммутационной системы при обслуживании одного вызова t.

Согласно ведомственным нормам технологического проектирования (РД 45.120-2000 НТП 112-2000 «Городские и сельские телефонные сети») следует различать три категории (сектора) источников: телефонные аппараты народно-хозяйственного сектора $N_{нх}$; квартирные телефонные аппараты $N_к$; таксофоны $N_т$. Таким образом,

$$N_п = N_{нх} + N_к + N_т, \qquad (1)$$

где $N_п$ - есть номерная емкость проектируемой станции.

В соответствии с имеющимися категориями источников нагрузки среднее число вызовов в единицу времени от одного ТА народно-хозяйственного сектора обозначим $C_{нх}$, от квартирного сектора – $C_к$, от таксофонов – $C_т$.

Таким образом, средняя продолжительность одного занятия для источников i – ой категории определяется по формуле:

$$t_i = \alpha_i P_p \left(t_{со} + nt_п + t_с + t_{пв} + T_i + t_о\right), \qquad (2)$$

где α_i - коэффициент, учитывающий влияние вызовов, не закончившихся разговором, $\alpha_i = f\left(T_i, P_p\right)$, определяется графически;

P_p - доля вызовов, закончившихся разговором;

$t_{со}$ - среднее время прослушивания сигнала «ответ станции»;

n - количество цифр абонентского номера;

t_c - время установления соединения (от момента окончания набора номера до подключения вызываемого абонента);

nt_n - среднее время набора n цифр абонентского номера;

$t_{пв}$ - среднее время прослушивания сигнала «контроль посылки вызова»;

T_i - средняя продолжительность разговора;

t_0 - время отбоя.

В современных АТС время установления соединения и время отбоя ничтожно малы (десятки миллисекунд), вследствие чего без большой погрешности считаем их равным нулю.

Величина α_i зависит, в основном, от T_i и P_p, и определяется графически. Графики приведены в многочисленных источниках, например, в [7].

Остальные значения можно принять следующие:

$t_n = 0{,}8$ с для частотного набора номера;

$t_n = 1{,}5$ с для декадного набора номера;

$t_{пв} = 7$ с;

$t_{со} = 3$ с;

$n = 5.$

С учетом этих данных, а также формулы (2.2) находятся средние длительности занятия для источников всех категорий. Необходимо при расчете учесть долю телефонных аппаратов с декадным и частотным набором номера. Доля абонентов, использующих декадный набор, приведена в таблице 5. Остальные абоненты используют частотный набор.

Таблица 5 – Доля абонентов, использующих декадный набор номера

Цифра единиц	1	2	3	4	5	6	7	8	9	0
КВ	10	12	16	14	18	15	20	24	21	13
НХ	5	10	8	9	7	12	6	11	13	15

Таксофоны, включаемые в рассчитываемую АТС, имеют частотный набор. Интенсивность возникающей нагрузки для каждой из категорий абонентов определяется по формуле:

$$Y_i = \frac{N_i C_i t_i}{3600}, \text{ Эрл.} \quad (3)$$

Результаты расчетов сводятся в таблицу 6.

Таблица 6 – Результаты расчета возникающей нагрузки

Категория и тип ТА	N_i, ТА	T_i, с	t_i, с	C_i выз/ЧНН	Y_i, Эрл
НХ, частотный набор					
НХ, декадный набор					
КВ, частотный набор					
КВ, декадный набор					
Таксофоны					

Общая интенсивность нагрузки рассчитываемой АТС будет равна сумме интенсивностей нагрузок, создаваемых источниками различных категорий. Она рассчитывается путем суммирования значений, находящихся в последнем столбце таблицы 6.

Контрольные вопросы:

1. Пояснить что такое нагрузка в 1 Эрланг?
2. Что такое час наивысшей нагрузки?
3. Привести пример пятизначной нумерации и пояснить порядок формирования номера.
4. Что такое внутристанционная нагрузка?
5. Почему линия связи между АТС и УСС имеет однонаправленный вид?
6. Что представляет собой АТС?
7. Что представляет собой УСС?
8. Пояснить алгоритм произведённых вычислений.
9. Что понимается под интенсивностью нагрузки?
10. Почему произведено разделение всех абонентов на три категории?

Список использованных источников:

1. Лабунько О.С., Михалин И.С., Манин А.А., Шарыпова Т.Н. Системы коммутации. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2009. – 117 с.: ил.

2. Михалин И.С., Шарыпова Т.Н. Цифровая система коммутации АТСЭ-200. Методическое пособие для курсового проектирования. – Ростов-на-Дону: СКФ МТУСИ, 2002. – 45 с.: ил.

Лабораторная работа №2. Исследование вопроса распределения потоков нагрузки на ГТС при проектировании новой станции.

Цель работы: исследование вопросов распределения нагрузки в сетях общего пользования и привитие первичных навыков расчета параметров трафика при проектировании сетей связи.

Задание.

Уяснить исходные данные для проведения расчёта. Построить матрицу распределения нагрузок. Произвести интеграцию в матрицу распределения нагрузок параметров новой станции в соответствии с методом Раппа. Произвести анализ новой матрицы нагрузок и сделать выводы о произошедшем влиянии на величину трафика в сети.

В соответствии с методом Раппа предполагается, что включение на сети новой АТС не окажет влияния на общий исходящий поток нагрузки в существующих АТС. Т.е. для существующих АТС произойдёт только перераспределение исходящей нагрузки без изменения её величины, а нагрузка на новую станцию будет создаваться за счет пропорционального снижения нагрузки с существующих направлений и передачи ее на направление к новой АТС. Пусть матрица потоков нагрузки до включения новой АТС размерности n*n имеет вид:

$$y_{ij} = \begin{array}{c|c|c|c|c} & 1 & 2 & \dots & n \\ \hline 1 & y_{11} & y_{12} & \dots & y_{1n} \\ 2 & y_{21} & y_{22} & \dots & y_{2n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ n & y_{n1} & y_{n2} & \dots & y_{nn} \\ \hline y_{вхj} & \sum_{i=1}^{n} y_{i1} = y'_1 & \dots & \sum_{i=1}^{n} y_{in} = y'_n & M \end{array} \qquad y_{исх\,i} \quad \begin{array}{l} \sum_{j=1}^{n} y_{1j} = y_1 \\ \\ \sum_{j=1}^{n} y_{nj} = y_n \\ \\ M \end{array}$$

Исходящие и входящие потоки нагрузки на АТС определяются суммированием соответствующих строк и столбцов матрицы. Общая нагрузка на сети равна сумме элементов матрицы:

$$M = \sum_{i=1}^{n} \sum_{j=1}^{n} y_{ij} .$$

Допустим, что новая (n + 1)-я АТС имеет исходящую нагрузку Y_{n+1} равную входящей, и внутристанционную - $Y_{n+1,n+1}$.

Для организации в матрице Y_{ij} столбца (n +1) входящей нагрузки на $АТС_{n+1}$, необходимо снять с исходящей нагрузки существующих АТС нагрузку, равную входящей нагрузке новой АТС, т.е.

$$Y_{n+1,вх} = Y_{n+1} - Y_{n+1,n+1}$$

Доля снятой нагрузки зависит от веса вводимой станции в телефонной сети, т.е. от отношения её исходящей нагрузки к суммарной нагрузке в существующей ГТС.

Рассчитаем коэффициент снятия нагрузки

$$x = \frac{y_{n+1} - y_{n+1,n+1}}{M} ,$$

который показывает, какую часть нагрузки необходимо снять с каждого из существующих направлений и передать на новую АТС. Тогда столбец (n+1) для новой АТС запишется следующим образом:

$$y_{i,n+1} = \begin{bmatrix} y_1 & x \\ y_2 & x \\ \vdots & \\ y_n & x \\ y_{n+1,n+1} & \end{bmatrix}$$

а строка (n+1) для этой АТС представится как:

$$y_{n+1,j} = \left[y_1' x,\ y_2' x,\ \ldots,\ y_n' x,\ y_{n+1,n+1} \right]. \quad (27)$$

Новая матрица распределения нагрузки будет иметь вид :

$$y_{ij} = \left[\begin{array}{cccc|c} y_{11}(1-x) & y_{12}(1-x) & \ldots & y_{1n}(1-x) \; y_1 x & y_1 \\ y_{21}(1-x) & y_{22}(1-x) & \ldots & y_{2n}(1-x) \; y_2 x & y_2 \\ \vdots & & & \vdots & \vdots \\ y_{n1}(1-x) & y_{n2}(1-x) & \ldots & y_{nn}(1-x) \; y_n x & y_n \\ y_1' x & y_2' x & \ldots & y_n' x \quad y_{n+1,n+1} & y_{n+1} \\ \hline y' & y_2' & & y_n' \quad y_{n+1} & M + y_{n+1} \end{array}\right] \quad (28)$$

Общий поток нагрузки на сети увеличился на величину Y_{n+1} , а общие исходящие и входящие потоки нагрузки существующих АТС остались неизменными.

Контрольное задание

На ГТС полносвязной структуры с шестью АТС проектируется АТС №7. Задана матрица потоков нагрузки между существующими АТС/ размерностью 6х6 Эрл:

	1	2	3	4	5	6
1	15	7	10	5	6	11
2	4	20	12	8	5	7
3	6	11	25	8	6	9
4	5	7	12	19	3	8
5	9	11	8	13	21	7
6	9	8	11	12	10	15

Исходящая и внутристанииионная нагрузки проектируемой АТС представлены в таблице. Входящую на АТС нагрузку примем равной исходящей.

Таблица. Исходящая и внутристанииионная нагрузки по вариантам контрольного задания.

Типы нагрузок в проектируемой АТС	Нагрузки в Эрл. по вариантам									
	0	1	2	3	4	5	6	7	8	9
$Y_{исх}$, по последней цифре шифра	60	70	95	84	72	59	63	48	71	68
$Y_{вн.ст.}$, по предпосл. цифре шифра	10	15	25	20	18	17	22	19	16	14

Необходимо:

а) включить в существующую матрицу потоков нагрузки сороку и столбец для исходящей и входящей нагрузки проектируемой АТС;

б) дать перераспределение потоков нагрузки между существующими станциями, вызванное включением новой АТС;

в) определить исходящие и входящие потоки нагрузки на каждой АТС и по сети в целом.

Контрольные вопросы:

1. Что подразумевает метод Раппа?

2. Поясните состав матрицы нагрузки для рассматриваемого вами примера.

3. Что такое нагрузка на сеть в 1Эрланг.

4. Что такое внутристанционная нагрузка?

5. Что понимается под коэффициентом снятия нагрузки?

6. Каков физический смысл данных расположенных по диагонали матрицы?

7. Что понимается под определителем матрицы?

8. Как изменится определитель матрицы новой матрицы относительно старой?

9. Основываясь на построенной матрице нагрузки покажите, между какими АСТ присутствует связь.

Список использованных источников:

1. Нестерова А.В. Методические указания по расчёту распределения нагрузки на городских телефонных сетях с помощью ЭВМ / ВЗЭИС. – М., 1977.

Лабораторная работа №3. Исследование работы концентраторов и коммутаторов с использованием программного продукта Cisco Packet Tracer.

Цель работы: рассмотрение работы концентраторов и коммутаторов. Получение первичных навыков конфигурирования коммутационных устройств.

Задание.

Построить схему сети с использованием одного концентратора. В режиме моделирования работы сети просмотреть выполнение команды ping между произвольно выбранными устройствами. Рассмотреть возможность объединения трёх концентраторов в кольцо. Аналогичные действия произвести с сетью, построенной на базе коммутаторов. Сконфигурировать Vlan по указанным исходным данным. Сделать выводы.

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы меж собой соединяются кроссоверным кабелем (рис. 1).

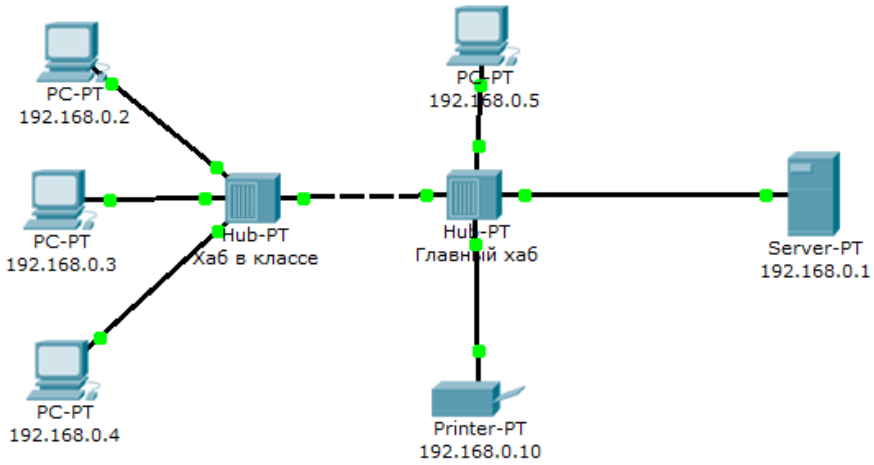


Рисунок 1 - Схема сети.

Нужно перейти в режим симуляции (Shift+S), либо кликнув на иконку симуляции в правом нижнем углу рабочего пространства. Здесь мы видим окно событий, кнопка сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Предложено много протоколов, но отфильтруем пока только ICMP, это исключит случайный трафик между узлами.

Необходимо каждому оконечному сетевому устройству задать адресацию. Это делается во вкладке Desktop. В общем случае, вид открывшегося окна с введённой адресацией показан на рисунке 2.

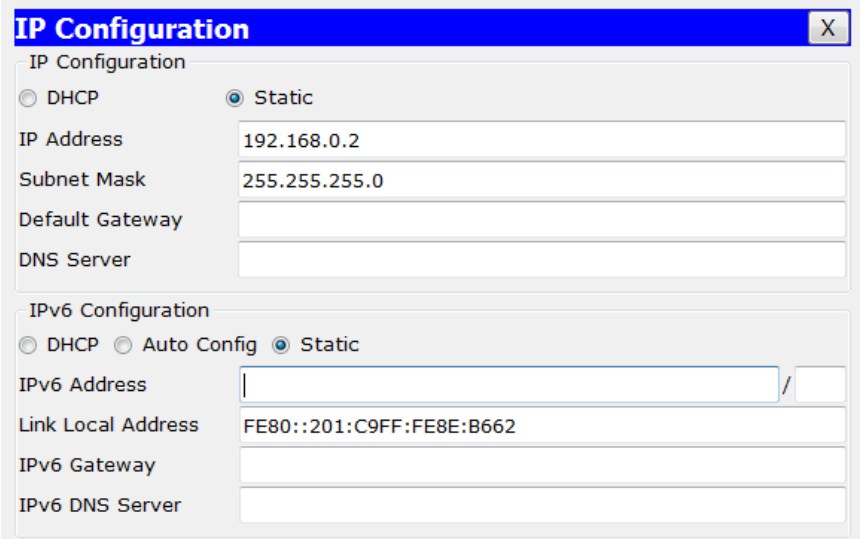


Рисунок 2 – Окно вкладки Desktop

Для перехода к следующему событию используем кнопку "Вперёд", либо автоматика (рис.3).

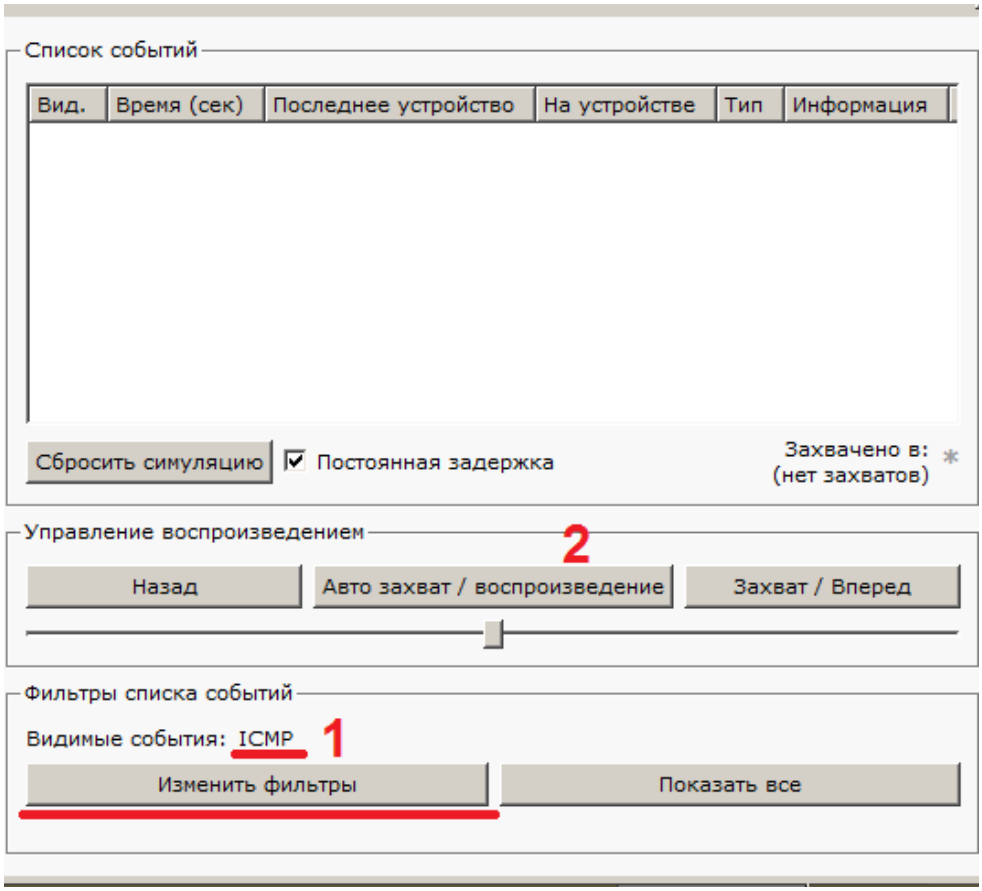


Рисунок 3 - Интерфейс симулятора.

Посылаем PING-запрос.

С одного из узлов попробуем пропинговать другой узел. Выбираем далеко расположенные узлы, чтобы наглядней увидеть как будут проходить пакеты по сети в режиме симуляции. Итак, входим на узел .4 и пошлём пинг-запрос на узел .5.

С розового узла пингуем зелёный. На розовом узле образовался пакет (конвертик), который ждёт (иконка паузы на нём). Запустить пакет в сеть можно нажав кнопку "Вперёд" в окне симуляции (рис.4).

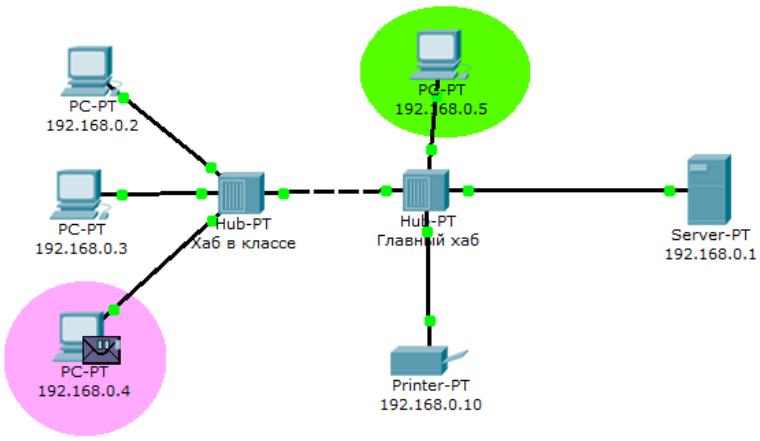


Рисунок 4 - Демонстрация работы симулятора.

Так же в окне симуляции мы увидим этот пакет, отметив его тип (ICMP) и источник (192.168.0.4) – рис.5.

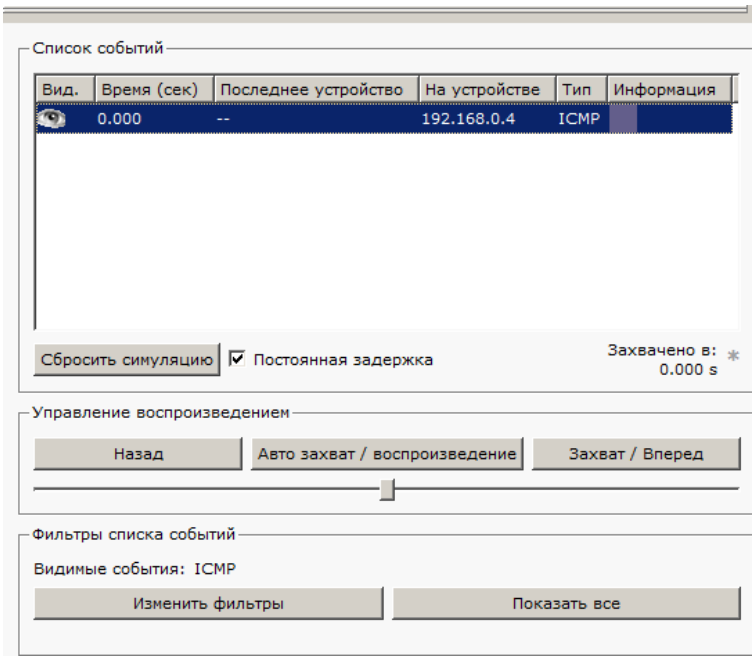


Рисунок 5 - Мониторинг работы протоколов.

Клик на пакете покажет нам подробную информацию. При этом мы увидим модель OSI. Сразу видно, что на 3-ем уровне (сетевой) возник пакет на исходящем направлении, который пойдёт до второго уровня, затем до первого, на физическую среду и передастся на следующий узел (рис. 6).

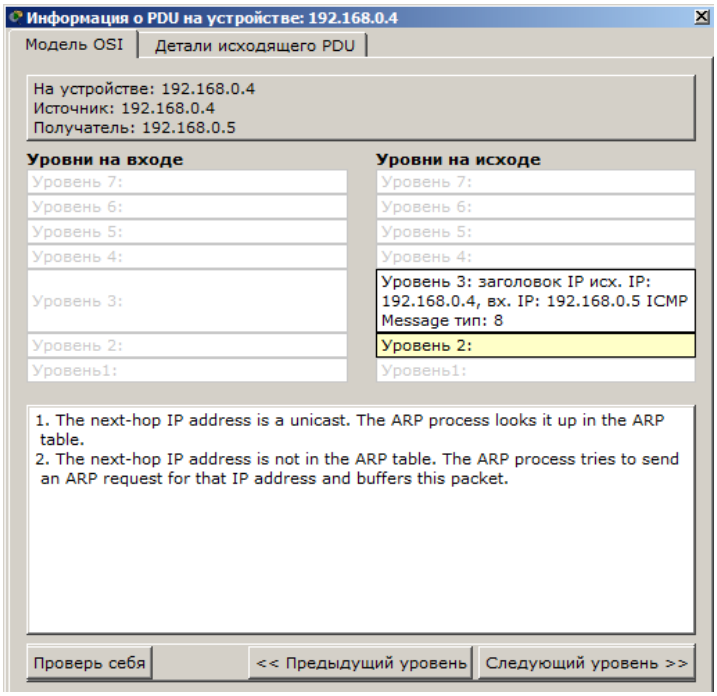


Рисунок 6 - Мониторинг работы на модели OSI

А на другой вкладке можно посмотреть структуру пакета (рис. 7).

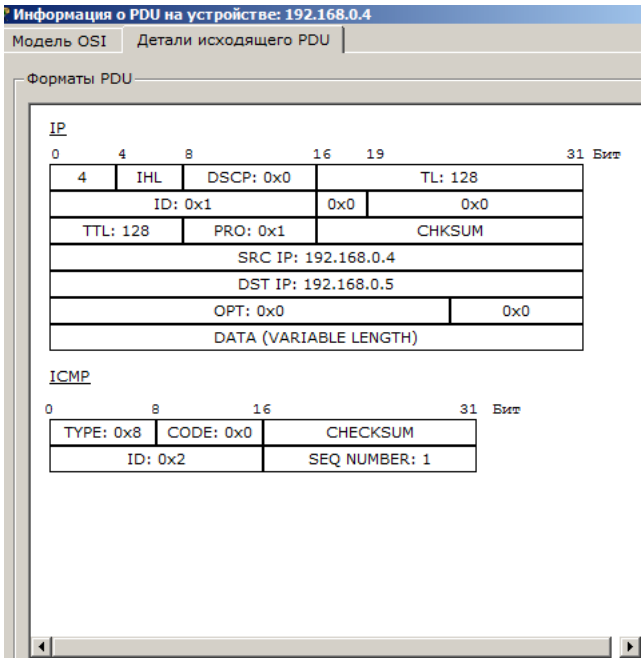


Рисунок 7 - Структура пакета

Нажмём кнопку "Вперёд". И пакет тут же двинется к концентратору. Это единственное сетевое подключение с этой стороны (8).

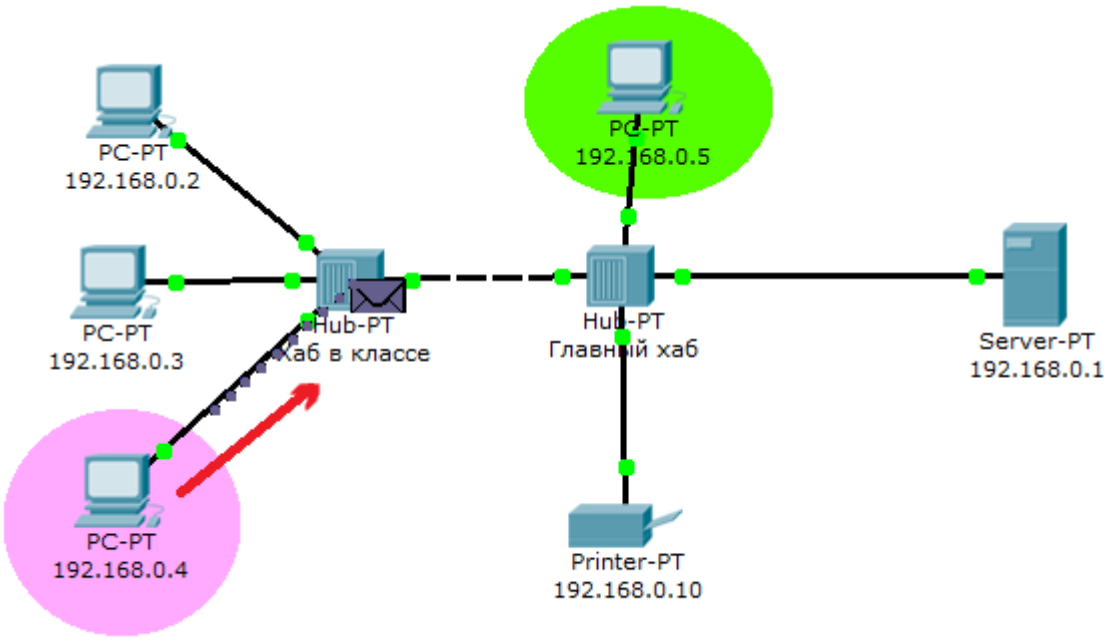


Рисунок 8 - Прохождение пакета. Первый этап

Концентратор повторяет пакет на всех остальных портах в надежде, что на одном из них есть адресат (рис.9)

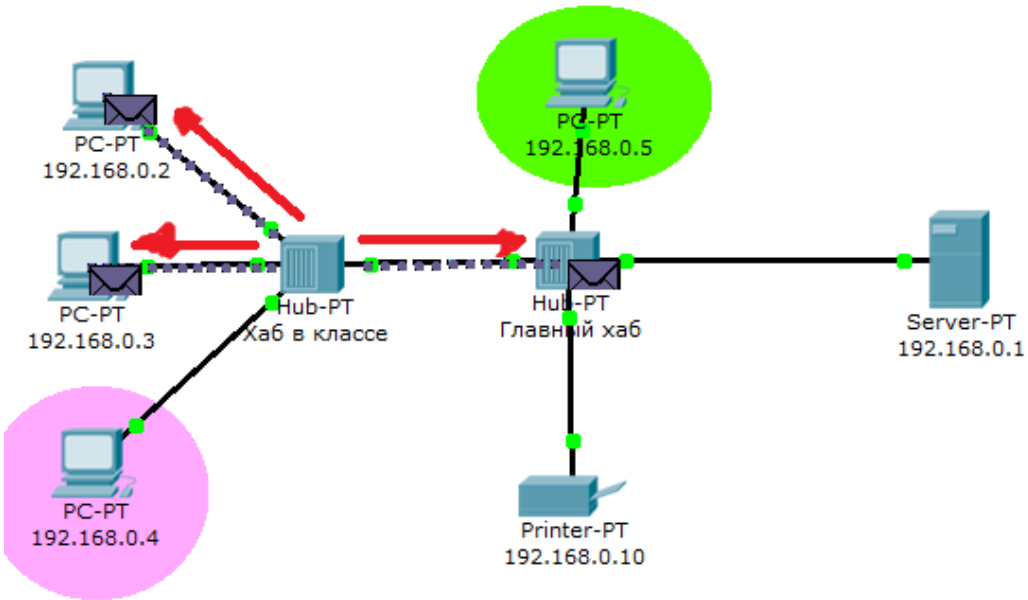


Рисунок 9 - Прохождение пакета. Второй этап

Если пакеты, каким то узлам не предназначенные, они просто игнорируют их (рис.10).

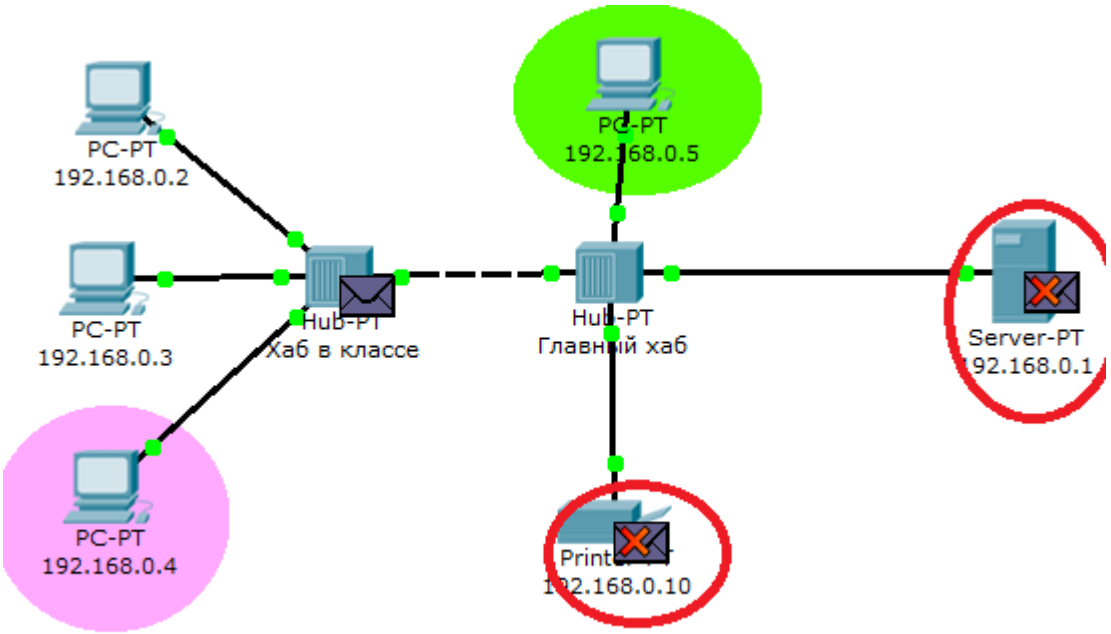


Рисунок 10 - Прохождение пакета. Третий этап

Когда пакет вернётся обратно, то увидим подтверждение соединения:

По окончании рассмотрения работы построенной сети выполните следующие действия:

Охарактеризуйте работу сети на базе концентраторов.

Составьте алгоритм работы концентратора.

Сделайте вывод о возможности построения больших сетей на базе данных устройств, а также могут ли создаваться петлевые структуры в сетях, построенных на базе концентраторов.

Далее необходимо произвести аналогичные действия с сетью, построенной на безе коммутаторов.

Общий вид такой сети представлен на рисунке 11.

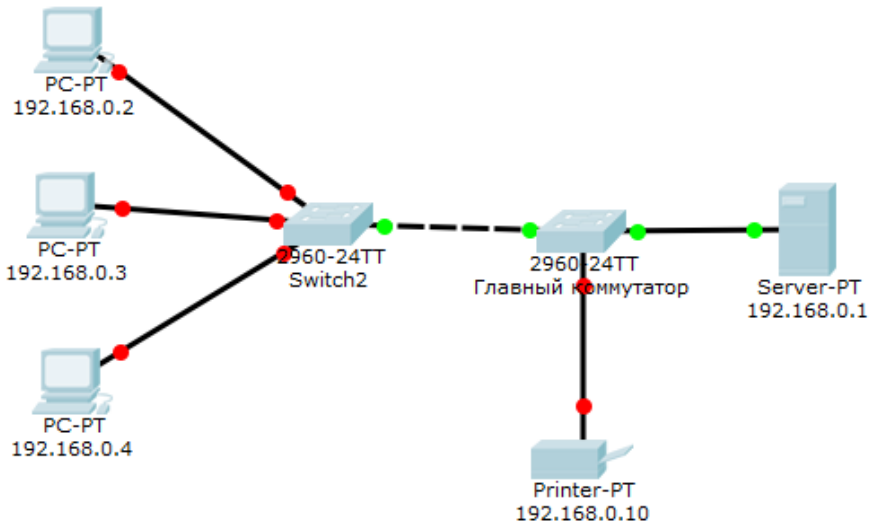


Рисунок 11 – Сеть на базе коммутатора

Обратите внимание, что коммутатор обладает более сложным алгоритмом работы. Поэтому подробным образом опишите изменения, происходящие в таблице коммутации. Данную таблицу можно просмотреть с помощью команды show vlan brief (рис. 12).

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000b.be9a.6e02    DYNAMIC     Fa0/4
Switch#
```

Copy Paste

Рисунок 12 – Таблица коммутации

Контрольные вопросы:

1. Пояснить алгоритм работы концентратора.
2. Что такое широковещательный пакетный шторм?
3. Ограничения на посторенние сети при использовании концентраторов?
4. Основные достоинства и недостатки концентраторов?
5. Поясните алгоритм работы коммутатора.
6. Поясните работу коммутатора в режиме самообучения.

7. Классификация коммутаторов.

8. Как решается вопрос борьбы с петлями на канальном уроне?

9. Что такое Vlan и для чего он может быть применён в сети?

10. Правила конфигурирования коммутатора при настройке Vlan.

11. Что такое магистральный порт и для чего он нужен?

Список использованных источников:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: «Питер», 2010. –943с.

Лабораторная работа №4. Расчёт и исследование характеристик локальной вычислительной сети Ethernet .

Цель работы: исследование вопросов распределения трафика в сетях с коммутацией пакетов. Получение навыков расчета сети и выбора коммутационного оборудования.

Задание.

Для индивидуальных исходных данных построить схему сети связи и произвести индексацию ветвей сети. Произвести определение пиковых потоков при обменах пар абонентов всех имеющихся направлениях обмена данных. На основании полученных данных произвести расчёт параметров трафика в ветвях сети. Сформулировать требования для выбора коммутационного оборудования и произвести его выбор. Сделать выводы.

В процессе работы необходимо произвести:

- построение структурной схемы сети в соответствии с исходными данными для своего индивидуального варианта;

- определение среднесуточных и пиковых потоков между всеми элементами локальной вычислительной сети (ЛВС);

- расчёт объёма информационного потока в каждой соединительной линии (ветви сети);

- расчёт канальных скоростей и выбор соответствующего стандарта технологии Ethernet;

- выбор коммутационного оборудования;

- расчёт времени реакции в системе клиент-сервер для спроектированной ЛВС;

- рассчитать стоимость выбранного оборудования.

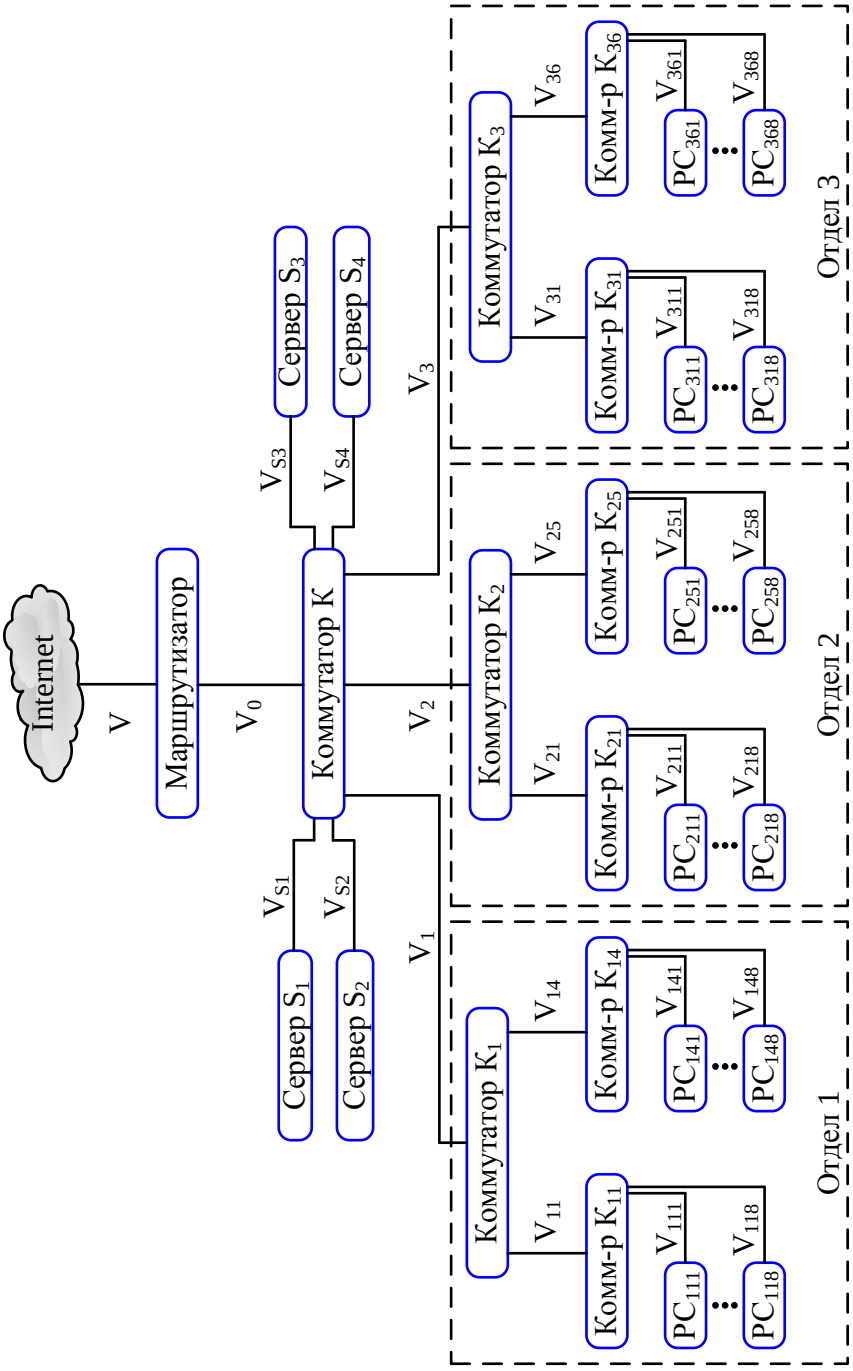


Рисунок 1 - Общая структурная схема сети компании

Исходные данные для расчета.

Рассчитываемая ЛВС представляет собой клиент – серверную систему, объединяющую серверы и рабочие станции сотрудников всей компании.

Иерархическая структура сети повторяет структуру подразделения.

Исходные данные:

1. Число серверов от 3-х до 6-и в соответствии с таблицей 1. Номера серверов - m = 1÷6.

2. Число отделов – 3. Номера отделов – i = 1÷3.

3. Число рабочих групп в каждом отделе от 3-х до 6-и в соответствии с таблицей 1. Номера рабочих групп – j = 1÷6.

4. Число ПЭВМ (рабочих станций, персональных компьютеров - PC) в каждой рабочей группе равно 8. Номера PC – k = 1÷8.

5. Интенсивность среднесуточных обменов для любой пары клиент – сервер одинакова и равна:

- в направлении ПЭВМ – сервер – 0,35 Кбайта/с;

- в направлении сервер – ПЭВМ – 3 Кбайт/с;

- коэффициент пульсаций трафика (отношение пиковых потоков к среднесуточным) определяется по таблице 2.

Таблица 1 - Число серверов и рабочих групп в отделах

Предпоследняя цифра шифра	Число серверов	Число рабочих групп		
		1 отдел	2 отдел	3 отдел
0	3	3	4	5
1	4	4	5	4
2	4	3	4	6
3	3	4	4	5
4	4	4	5	6
5	5	3	5	5
6	5	4	4	6
7	3	5	4	5
8	6	4	4	6
9	5	4	5	3

6. Интенсивность среднесуточного внешнего обмена для любой ПЭВМ одинакова и равна:

- в направлении ПЭВМ -Internet - 0,09 Кбайт/с;

- в направлении Internet – ПЭВМ – 0,8 Кбайт/с;

- коэффициент пульсации трафика определяется по таблице 3;

7. Интенсивность среднесуточного обмена между ПЭВМ одной рабочей группы – 0,4 Кбайта/с. Коэффициент пульсации – 60:1.

8.Интенсивность среднесуточного обмена между любыми ПЭВМ подразделения не входящими в одну рабочую группу – 0,15 Кбайт/с. Коэффициент пульсации – 40:1.

Таблица 2 - Коэффициент пульсаций трафика “клиент – сервер” и “сервер – клиент”

Последняя цифра шифра	0	1	2	3	4	5	6	7	8	9
Коэффициент пульсаций	40	45	50	55	60	65	70	75	80	85

Таблица 3 - Коэффициент пульсаций внешнего трафика

Последняя цифра текущего года	0	1	2	3	4	5	6	7	8	9
Коэффициент пульсаций	85	90	95	100	110	120	130	140	150	160

Порядок выполнения контрольной работы.

1. Составить структурную схему ЛВС, уточнив для схемы (рисунок 1) числа серверов и рабочих групп в отделах для своего варианта.

2. Для удобства дальнейших расчетов провести индексацию всех узлов схемы своего варианта подобно тому, как это сделано на схеме рисунке1.

В рассматриваемой сети под узлом N (Node) понимается любое устройство типа маршрутизатор (Router), коммутатор (Switch).

Линии связи (ветви) между узлами удобно индексировать так же, как узел, расположенный ниже по иерархии. Например, линию, соединяющую узел

N_1 (в данном случае коммутатор $К_1$) с узлом N_{11} (коммутатор $К_{11}$), будем обозначать как V_{11}, а линию, соединяющую N_{36} (коммутатор $К_{36}$) с узлом N_{368} (PC-368), обозначим как V_{368}. Эти обозначения будут необходимы при расчете потоков в линиях.

Самые нижние ветви (между ПЭВМ и концентратором) имеют трёхиндексное обозначение V_{ijk} , где: i – номер отдела, j – номер рабочей группы и k – номер ПЭВМ в рабочей группе.

При выполнении работы можно вводить свою нумерацию, формируемую по другому принципу, однако необходимо обеспечить не повторяемость введённых обозначений.

3. Произвести расчет пиковых потоков для направлений обменов, указанных в исходных данных. Например, если трафик ПЭВМ – Сервер составляет 0,35 Кбайта/с при пульсациях 100:1, то пиковый поток составит 35 кбайт/с. Для направления Сервер – ПЭВМ составляет 3 Кбайта/с при указанном коэффициенте пульсации пиковый поток составит 350 кбайт/с.

Необходимо понимать, что переходя на расчёт сети по пиковым потокам нами будет создаваться идеальный случай, характеризующий максимально возможные в сети уровни нагрузки во всех её ветвях. В реальных условиях эксплуатации сети такой режим работы, скорее всего, невозможен. Но опираясь при выборе оборудования на такой расчёт мы обеспечим гарантированную работу сети без перегрузок её отдельных ветвей.

4. Определить суммарные пиковые потоки для каждой ветви. Это основная расчетная часть работы, требующая точности и внимательности. Ориентируясь на суммарные пиковые потоки, необходимо будет определять пропускные способности соответствующих ветвей. Фактически это сведется к выбору одного из существующих стандартов; Ethernet (10 Мбит/с), Fast Ethernet (100 Мбит/с), Gigabit Ethernet (1000 Мбит/с) или 10 GBit Ethernet (10Гбит/с). При выполнении этого задания необходимо составить таблицу со столбцами – ветвями и строками – потоками следующего вида (таблица 4).

Таблица 4 - Объёмы потоков в ветвях ЛВС

Вид трафика	**Объёмы потоков в ветвях (Мбайт/с)**										
	V_{1jk}	**V_{2jk}**	**V_{3jk}**	**V_{1j}**	**V_{2j}**	**V_{3j}**	**V_1**	**V_2**	**V_3**	**V_0**	**V_{sm}**
ПЭВМ → Сервер											
Сервер → ПЭВМ											
ПЭВМ → Internet											
Internet → ПЭВМ											
ПЭВМ → ПЭВМ одной рабоч. групы											
ПЭВМ → ПЭВМ разных рабоч. групп											
Суммарный трафик в ветви											
Суммарная скорость в ветви, Мбит/с											

Структура таблицы отражает следующие особенности исходных данных:

- в каждом отделе потоки между ПЭВМ и концентратором одинаковы. Поэтому в таблице для ветвей нижнего уровня выделено только три столбца – V_{1jk} (ветви 1-го отдела), V_{2jk} и V_{3jk};

- в каждом отделе потоки между концентратором и коммутатором для каждой рабочей группы одинаковы. Поэтому в таблице для ветвей среднего уровня тоже выделено только три столбца – V_{1j} (ветви 1-го отдела), V_{2j} и V_{3j} .

Например, пиковый поток от сервера S_1 до PC_{118}, пройдет по ветвям $V_{S1,}$ $V_{1,}$ V_{11} и V_{118} и должен быть отмечен в столбцах V_{sm} , V_1 , V_{1j} и V_{1jk} . Поток между двумя ПЭВМ 1-го и 2-го отделов, пройдет по ветвям, например, $V_{111,}$ $V_{11,}$ $V_{1,}$ $V_{2,}V_{21}$ и V_{218} и должен быть отмечен в соответствующих столбцах.

Необходимо обязательно просчитывать количество одинаковых потоков, проходящих по той или иной ветви, и указывать их суммарный объём. Например, в 5-й строке столбца V_{1jk} указывается пиковый поток от одной из ПЭВМ 1-го отдела к семи другим ПЭВМ своей рабочей группы, умноженный на 2. Удвоение потока необходимо для учёта исходящего и входящего потоков,

так как по одной и той же ветви V_{131} проходит, например, поток $РС_{131} \rightarrow РС_{138}$ и поток $РС_{138} \rightarrow РС_{131}$.

После включения в табл. 4 всех потоков можно будет подсчитать суммарный информационный поток в каждой ветви.

Стоит отметить, что такой подсчет суммарной нагрузки является очень упрощенным, так как пики потоков носят стохастический характер и необязательно совпадают во времени. Для точных расчетов применяются методы теории телетрафика, но для сложных сетей, подобных рассматриваемой, они не разработаны. В случае необходимости получения точных значений объёмов потоков применяют методы имитационного моделирования, которые выходят за рамки данной контрольной работы. Однако, использование такой явно завышенной оценки суммарного потока в какой-то степени оправдано, так как создает определенный запас пропускной способности каналов. Обычная практика проектирования сетей - загружать каналы изначально не более, чем на 20-30%, поскольку интенсивность информационного обмена в современных сетях непрерывно возрастает.

5. Определяются требуемые канальные скорости для каждой ветви (заполняется последняя строка таблица 4). Общепринято информационные потоки измерять в байт/с, а канальные скорости в бит/с. Поэтому переход от предпоследней строки таблице 4 к последней состоит в простом умножении ее значений на 8 (на число бит в байте).

6. На заключительных этапах работы студенты должны выбрать оборудование для узлов ЛВС, определить стоимость выбранного оборудования и рассчитать время реакции в тракте “ПЭВМ – Сервер – ПЭВМ”.

Выбор оборудования для узлов ЛВС.

Рассмотрим ряд устройств (концентратор, коммутатор, маршрутизатор), которые использовались при построении данной ЛВС.

Концентратор – это многопортовый повторитель, который любой бит, появляющийся на любом из его портов, передает на все другие порты, независимо от адреса принятого кадра (адрес даже не анализируется).

Появление сигналов одновременно на двух или более входах рассматривается как столкновение и обнаруживается источниками этих сигналов. Передача временно прекращается и возобновляется через некоторый случайный промежуток времени. Концентратор – устройство физического уровня. Он проще и дешевле коммутатора, но безадресная передача кадров на все выходы сильно перегружает соответствующий сегмент сети. Это привело к тому, что данное устройство в создании четей уже не применяется. Хотя и можно его иногда встретить.

Коммутатор - любой поступающий на его порт кадр записывает в память (целиком или только заголовок), анализирует адрес получателя и передает этот кадр только в направлении к адресату. Это даёт возможность коммутатору осуществлять одновременно несколько обменов. Например, передавать кадр с порта 1 на порт 7 и одновременно с 11-го порта - на 9-й. Коммутатор – устройство второго уровня. Он производит передачу кадров в соответствии с физическими адресами портов.

Маршрутизатор – устройство 3-го уровня. В сетях, входящих в Internet, маршрутизаторы анализируют адреса IP-пакетов, поступающих на любой из его портов, и в соответствии с этими адресами направляют пакеты к другим маршрутизаторам или ПЭВМ (напрямую или через сети 2-го уровня). Другая существенная функция маршрутизатора – согласование протоколов логического уровня. Как правило, порты маршрутизатора многофункциональны (или модульны). К одному маршрутизатору могут подключаться, например, каналы ЛВС Ethernet и каналы сети ATM, Frame Relay или ISDN.

Выбор оборудования производится по следующим критериям:

- число портов. Очевидно, что приобретаемое устройство должно иметь число портов, не меньшее, чем число подходящих к нему каналов;

- наличие соответствующих физических интерфейсов: коаксиальные кабели, витая пара, оптоволоконный кабель. Для нашей схемы примем, что все каналы организованы на витых парах категории 5;

- наличие соответствующих логических интерфейсов. Для внутренних линий нашей схемы примем интерфейсы разновидностей Ethernet (Ethernet, Fast Ethernet , Gigabit Ethernet или 10GBit Ethernet);

- пропускные способности портов должны быть не ниже канальных скоростей, рассчитанных для соответствующих линий (последняя строка таблицы 4). При этом необходимо обратить внимание на следующее обстоятельство: представленные в таблице 4 потоки получены путём суммирования двухсторонних потоков в каждой ветви. Поэтому выбранные канальные скорости будут достаточны даже для полудуплексных режимов работы портов Ethernet, а в случае выбора аппаратуры с дуплексным режимом будет обеспечен определённый запас по пропускной способности ветви. В лучшем случае, при симметричном трафике, запас будет двукратным. Например, при дуплексной связи порты Ethernet 10 Мбит/с могут передавать данные со скоростью 20 Мбит/с – по 10 Мбит/с в каждом направлении. Отметим также, что современные стандарты Ethernet, кроме коаксиальных версий, используют, как правило, дуплексные режимы;

- суммарная пропускная способность устройства должна быть не ниже суммы рассчитанных канальных скоростей для всех линий, подключаемых к этому устройству.

Рекомендации по выбору оборудования.

При выборе оборудования из номенклатуры: маршрутизатор, коммутатор необходимо пользоваться следующими правилами:

- маршрутизатор по сравнению с коммутатором обладает большим интеллектом (работа с IP-адресами, борьба с широковещательными штормами), а коммутатор дешевле и обладает, как правило, большим быстродействием;

- коммутатор по сравнению с концентратором более интеллектуален (работа с MAC-адресами, что позволяет существенно ограничить зону коллизий, специфичную для технологии Ethernet). Концентратор дешевле. Однако, в последние годы в связи с массовым выпуском микрочипов для

коммутаторов их стоимость значительно снизилась и они считаются более предпочтительными.

В данной работе выбор конкретных образцов оборудования необходимо сделать самому. При этом необходимо рассмотреть оборудование как минимум трёх производителей и из него сделать выбор, при этом необходимо обязательное обоснование совершённого выбора.

Для поиск коммутационного оборудования необходимо пользоваться информацией с официальных сайтов производителей.:

http://www.tp-linkru.com – сайт компании TP-Link;

http://www.qtehc.ru – сайт компании Qtehc;

http://www.dell.ru – сайт компании Dell;

http://www.cisco.com – сайт компании Cisco;

http://www.dlink.ru – сайт компании Dlink;

http://www.huawei.com – сайт компании Huawei;

http://www8.hp.com – сайт компании Hp.

Расчет времени реакции системы.

В системе клиент - сервер под временем реакции понимается интервал времени между вводом запроса в ПЭВМ клиента и получением ответа на экране монитора. С большими упрощениями этот расчет можно произвести следующим образом.

В общем виде

$$T_p = t_{пз} + t_s + t_{по};$$

- T_p - время реакции;

- $t_{пз}$ - время передачи запроса от ПЭВМ до сервера. Так как запросы, как правило, очень короткие, то можно в $t_{пз}$ учесть только задержки в узлах. Примерно по 25мкс. на каждом узле (концентраторе или коммутаторе);

- t_s - время подготовки ответа сервером. Если не учитывать возможное стояние запроса в очереди на обслуживание сервером, то можно принять t_s равным 0,5мс;

- $t_{по}$ - время передачи ответа от сервера до ПЭВМ. Здесь, кроме задержки в узлах (25 мкс.), следует учесть и время прохождения длинного ответа через самый низкоскоростной канал.

Рассмотрим цепь каналов между сервером S_1 и PC_{111} (Рисунок 2).

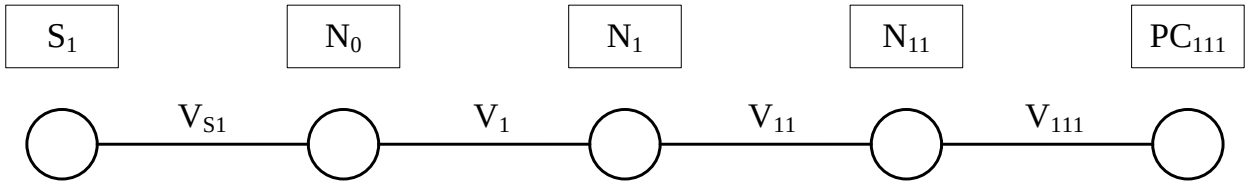


Рисунок 2 - Схема тракта сервер – рабочая станция (ПЭВМ).

Пусть в результате расчетов по пункту 5 определены следующие канальные скорости: C_{111}=10Мбит/с, C_{11}=10Мбит/с, C_1=100 Мбит/с:

Тогда, для передачи ответного файла, например, длиной в L Мбайт, по самому низкоскоростному каналу V_{111} (скорость C_{111}=10Мбит/с) потребуется время

$$t_{111} = \frac{L \cdot 8}{C} = \frac{0{,}01 \cdot 10^6 \cdot 8}{10 \cdot 10^6} = 8мс;$$

(для L=0,01 Мбайт).

Цифра 8 в числителе соответствует числу бит в байте. Таким образом, общее время реакции составит:

$T_р$= 3·25мкс + 500мкс + 3·25мкс + 8000мкс = 8650 мкс.

Коэффициенты 3 в данной формуле соответствуют 3-м узлам, разделяющим ПЭВМ и сервер. Время - 500мкс – это продолжительность подготовки ответа сервером. Время - 8000мкс – это рассчитанная выше продолжительность передачи ответа (8мс). Длину ответного файла L студент выбирает произвольно и независимо от других студентов.

Строго говоря, расчёт времени реакции должен был учитывать и время распространения сигнала (электромагнитной волны) от компьютера до сервера и обратно. В общем случае, это время определяется как $t_p = S/v$, где: S – расстояние между двумя узлами (по кабелю);

v – скорость распространения электромагнитной волны в кабеле данного типа (можно принять v = 200000 км/с).

Тогда для S = 100 м получим t_p = 0,5 мкс. А время распространения сигнала в обе стороны определится как t_{p2} = 1мкс.

В связи с тем, что топология ЛВС (расположение серверов, компьютеров, коммутаторов) в данном практическом задании не определяется, а также в связи с незначительностью времени распространения в пределах небольшой локальной сети, это время при расчёте времени реакции не учитывалось.

Заключение.

В заключении работы необходимо привести основные параметры рассчитанной системы:

- число ПЭВМ;
- время реакции;
- скорость канала доступа в Internet;
- стоимость выбранного коммутационного оборудования.

Список источников:

1. В.Л. Бройдо Вычислительные системы, сети и телекоммуникации: учебное пособие для студентов ВУЗов/В.Л. Бройдо, О.П. Ильина. - 3-е издание, - СПб: Питер, 2008. 766 с.: ил.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для ВУЗов/В.Г. Олифер, Н.А. Олифер 3-е изд.- СПб: Питер, 2009г.- 958 с.: ил.

Практическое занятие №1. Система телефонной нумерации и структуры междугородных и местных телефонных сетей.

Цель работы: исследование изучить план нумерации действующий в ТФОП и получить практические навыки построении сетей и распределения нумерации.

Задание. Изучить систему телефонной нумерации и структуры междугородных и местных телефонных сетей. Произвести построение сети связи в соответствии с указаниями индивидуальных исходных данных. Дать нумерацию абонентам местных сетей, приняв закрытую систему нумерации. Выбрать коды местных сетей и коды зон семизначной нумерации.

Под системой нумерации (numbering system) понимается совокупность правил, позволяющих идентифицировать сети, их фрагменты, а также вызывающих и вызываемых пользователей. В телефонных сетях термин «номер» используется для обозначения той последовательности цифр и символов, которая однозначно определяет место подключения к сети терминала, УАТС, ЦОВ и других устройств.

Следующее важное понятие - «план нумерации» (numbering plan). Он определяет формат и структуру номера, который должен набрать вызывающий абонент для установления требуемого соединения. Десятичные цифры (и символы), определяемые планом нумерации, обычно сегментированы в группы, которые позволяют выделять информацию, относящуюся к стране, к сети и к терминалу абонента, оператора УАТС или ЦОВ. План нумерации не включает в себя префиксы и другую дополнительную информацию, необходимую дли установления соединения. Префиксы и дополнительная информация определяются правилами набора номера (dialling рШп). Например, абонент УАТС собирается позвонить в компанию по номеру, который известен из рекламы. Допустим, что номер вызываемого абонента состоит из семи цифр - 2345678. Эти цифры установлены в соответствии с планом нумерации той местной сети, в которую включена УАТС. План набора номера будет таким:

– сначала абонент УАТС набирает префикс выхода в местную телефонную сеть, в качестве которого рекомендуется использовать цифру «9»;

– затем необходимо набрать семь цифр (2345678), которых может оказаться вполне достаточно для установления требуемого соединения;

– в некоторых случаях вызывающий абонент получает речевую подсказку, в которой, например, содержится предложение перейти в режим многочастотного набора и набрать номер «555» для получения подробных сведений о предлагаемых товарах или услугах.

Префикс выхода с УАТС в местную телефонную сеть, символ « * » для перехода в режим многочастотного набора и цифры «555» в данном случае входят в атрибуты плана набора номера. План нумерации содержит только семь упомянутых цифр - 2345678. Префикс в общем случае состоит из одной или более цифр. Он, в значительной мере, определяет структуру набираемой далее совокупности цифр и символов. Принято выделять префиксы междугородной и международной связи.

В российской ТфОП пока в качестве этих префиксов используются цифра «8» и комбинация «8-10» соответственно.

План нумерации для международной телефонной сети изложен в рекомендациях ITU-T серии E. Основная информация для ТфОП содержится в рекомендации E.164.

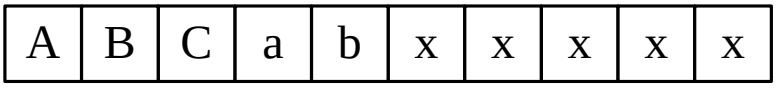
Разработка оптимального плана нумерации ТфОП - одна из самых сложных задач, возникающих перед Администрациями связи. Изменение плана нумерации связано с решением ряда организационных, экономических, технических и, в некоторых случаях, психологических задач.

План нумерации в телекоммуникационных сетях и частотный спектр в радиосвязи имеют ряд схожих черт. И то, и другое представляет собой пример применения ограниченных ресурсов. После того как эти ресурсы исчерпаны, необходимо осваивать новые диапазоны (нумерации и спектра соответственно). Этот процесс требует больших инвестиций и, как правило, сопряжен с изменениями в эксплуатируемом оборудовании.

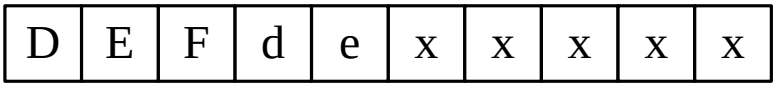
Основные особенности плана нумерации, используемого в российской ТфОП, были определены Администрацией связи СССР. Администрации связи большинства развитых стран стремились разрабатывать план нумерации, рассчитанный на несколько десятилетий. Некоторые Администрации даже декларировали период действия системы нумерации от 50 до 100 лет. Развитие электросвязи привело к тому, что за последние годы планы нумерации во многих странах претерпели заметные изменения. Аналогичные процессы характерны и для российской ТфОП.

Действующий план нумерации ЕСЭ РФ.

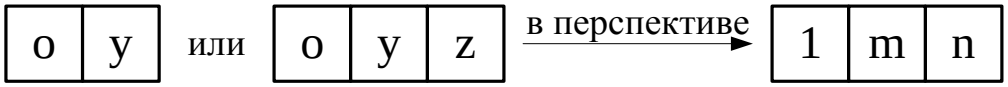
План нумерации, используемый в отечественной ТфОП, определяется рядом руководящих документов, принятых Администрацией связи России. Основным из этих документов считается «Система и план нумерации на сетях связи 7-й зоны всемирной нумерации». Этот руководящий документ утвержден в 1999 году. В названии фигурируют слова «7-я зона всемирной нумерации». Это связано с тем, что ITU-T выделил цифру «7» в качестве международного кода для связи с телефонной сетью бывшего СССР. В настоящее время цифра «7» используется для входящей международной связи с ТфОП России и республики Казахстан. Примеры номеров, используемых в ЕСЭ РФ. приведены на рис. 1.



а) Национальный номер абонента в российской ТФОП.



б) Номер абонента для негеографического плана нумерации.



в) Нумерация для выхода к экстренным и информационно-справочным службам.

Рис. 1. Примеры действующего плана нумерации в ЕСЭ РФ.

ТфОП в России делится на зоновые сети, каждой из которых выделяется код АВС (код автоматической междугородной связи). В качестве значений буквы А не могут использоваться цифры «1», «2» и «О» на значения В и С ограничения не накладываются.

Национальный номер абонента российской ТфОП состоит из десяти цифр - фрагмент (а) на рис. 1. Обычно его обозначают следующим образом: ABCabxxxxx. Код АВС «привязан» к территории субъекта Федерации. По этой причине его иногда называют географическим кодом нумерации. Большинству субъектов Федерации выделен один код АВС. В новых официальных документах Администрации связи России, которые касаются изменений плана нумерации в ТфОП, код АВС относится к географически определяемой зоне нумерации.

Номер abxxxxx называется полным местным номером абонента. Он всегда состоит из семи цифр при междугородной и международной связи. При местной телефонной связи может также использоваться пяти или шестизначный план нумерации. В этом случае при входящей междугородной и международной связи отсутствующие в номере цифры а или аЬ должны заменяться цифрами «2» или «22», соответственно.

В местных телефонных сетях используются два вида системы нумерации: закрытая и открытая. При закрытой системе нумерации в пределах местной сети (за исключением выхода к экстренным и информационно-справочным службам) всегда набирается одно и то же число цифр. В ГТС всегда используется закрытая система нумерации. Открытая система нумерации применяется в СТС. Существуют два варианта открытой нумерации - с индексом выхода и без индекса выхода. Индекс выхода позволяет отличить соединение в пределах АТС от соединения, устанавливаемого с другой станцией.

С этой точки зрения правила обслуживания вызова схожи с алгоритмом, принятым для УАТС. В системе без индекса выхода различие между вызовами определяется путем анализа набираемых цифр. В табл. 1 приведены примеры

нумерации при установлении соединений разных видов. Предполагается, что для СТС используется закрытая пятизначная система нумерации. План нумерации ГТС - семизначный. В качестве примера нумерации при использовании УСС в этой и в двух следующих таблицах приведены цифры, набираемые для связи с оператором Министерства по чрезвычайным ситуациям (МЧС).

Таблица 1. Цифры, набираемые при закрытой пятизначной системе нумерации в СТС.

Местонахождение вызывающего абонента	**Нумерация при вызове абонента или оператора**			
	ГТС своей зоновой сети	**СТС своей зоновой сети**	**ГТС или СТС другой зоновой сети**	**УСС (МЧС)**
РАТС в ГТС	abxxxxx	8 - 2 - abxxxxx	8 - ABCabxxxxx	01
ОС в СТС	8 - 2 - abxxxxx	xxxxx[а)]	8 - ABCabxxxxx	01
УАТС в ГТС	9 - abxxxxx	9 - 8 - 2 - abxxxxx [б)]	9 - 8 - ABCabxxxxx [б)]	9-01 [б)]

Примечания:

а) предполагается, что вызываемый абонент включен в одну из коммутационных станций этой же СТС;

б) префикс «9» может не набираться, если такое решение реализуемо в используемой УАТС.

Электромеханические АТС некоторых типов, имеющиеся в сельских телефонных сетях, поддерживают только открытые системы нумерации - с индексом выхода и без него. В таких случаях используются специфические планы нумерации. Примеры открытой системы нумерации без индекса (префикса) выхода приведены в табл.2.

Входящая связь от абонентов других зоновых сетей не имеет специфики всегда набирается комбинация 8 - ABCabxxxxx, Поэтому нумерация для входящей связи в табл. 2 не приводится.

Для внутристанционной связи вызывающий абонент набирает три цифры, а для межстанционной - пять. Абоненты ЦС для местной связи всегда набирают

пять цифр, то есть используют закрытую систему нумерации. В качестве «х» может использоваться любая цифра.

Таблица 2. Цифры, набираемые при открытой системе нумерации без индекса выхода.

Станция вызывающего абонента	**Нумерация при вызове абонента или оператора**		
	своей станции	**ЦС или других станций СТС**	**УСС (МЧС)**
ЦС всех типов	cxxxx [а)]	cxxxx	01
УС всех типов	dxx [б)]	cxxxx	01
ОС всех типов	dxx	cxxxx	01

Примечания:

а) в качестве значения ***c*** не должны использоваться цифры, с которых начинаются сокращенные номера (то есть $c \neq d$);

б) значения ***c*** и ***d*** не должны совпадать с цифрами «8» и «0».

Примеры открытой системы нумерации с индексом (префиксом) выхода приведены в табл. 3. Префикс выхода обозначен символом $П_м$. Для внутристанционной связи вызывающий абонент набирает две или три цифры, а для межстанционной - пять (после индекса выхода).

Абоненты ЦС для местной связи всегда набирают пять цифр, то есть используют закрытую систему нумерации. В качестве ***x*** может использоваться любая цифра.

Таблица 3. Цифры, набираемые при открытой системе нумерации с индексом выхода.

Станция вызывающего абонента	**Нумерация при вызове абонента или оператора-телефониста**		
	своей станции	**ЦС или других станций СТС [в)]**	**УСС (МЧС)**
ЦС всех типов	xxxxx	xxxxx	01
УС всех типов	xx, xxx или dxx	$П_м$ - xxxxx	$П_м$ - 01
ОС первого типа [а)]	xx, или xxx	$П_м$ - xxxxx	$П_м$ - 01
ОС второго типа [б)]	dxx	$П_м$ - xxxxx	$П_м$ - 01

Примечания:

а) к ОС первого типа относятся сельские станции всех типов, за исключением АТСК-50/200М, АТСК-100/2000, и все АТС с программным управлением;

б) к ОС второго типа относятся АТСК-50/200М, АТСК-100/2000 и все АТС с программным управлением;

в) в качестве первого знака сокращенного номера не должна использоваться цифра, выделенная для индекса Пм.

В конце XX века началось интенсивное развитие сотовых сетей и формирование платежеспособного спроса на некоторые услуги, поддерживаемые Интеллектуальной сетью (IN - Intelligent Network). Это стимулировало введение негеографических кодов, которые принято обозначать латинскими буквами **DEF**. Этим подчеркивается их отличие от кодов ABC, определяемых с учетом географического положения субъекта Федерации. В остальном структуры десятизначных номеров схожи - фрагменты (а) и (б) на рис. 5.1. Коды **DEF** присваиваются географически не определяемым зонам нумерации.

Каждый код **DEF**, выделенный Оператору сотовой сети, позволяет - теоретически - пронумеровать восемь миллионов пользователей. Существенно то, что эта емкость может распределяться по всей территории, границы которой определены лицензией, выданной Оператору. В настоящее время в качестве значения символа **D** для сетей сотовой связи обычно используется цифра «9».

Семь цифр, следующих за кодом DEF, интерпретируются как логический номер, который обычно никак не связан с местом включения в ТфОП какого-либо терминала. Все УАТС, подключаемые к коммутационным станциям ГТС или СТС, должны использовать план нумерации, принятый для соответствующей местной сети. В пределах УАТС может использоваться сокращенная нумерация. Для выхода абонентов УАТС в местную сеть рекомендуется использовать префикс «9».

Для выхода абонентов ГТС и СТС к экстренным службам пока используются двухзначные номера (01 - при пожаре, 02 - милиция, 03 - скорая медицинская помощь, 04 - аварийная служба газовой сети). На фрагменте (в) рис. 1 эти номера обозначены символами Оу. Доступ к информационно-справочным службам обычно организуется за счет набора трехзначных номеров вида Oyz.

В европейских странах для выхода к экстренным и к информационно-справочным службам принят план нумерации вида Лтп - правая часть фрагмента (в) на рис. 1. «Службе спасения» во всей Европе присвоен единый номер - «112». В конце 2003 года было принято решение о создании российской «Службы спасения». Ей тоже присвоен общеевропейский номер «112».

Особенности нумерации в российской телефонной сети.

В первой лекции была упомянута практика нарушения общепринятых норм при построении ТфОП. Эти нормы не определяются никакими международными стандартами. Они сформировались в результате анализа эволюционных процессов, характерных для ТфОП. При разработке системы и плана нумерации российской ТфОП был допущен ряд ошибок. Некоторые ошибки рассматриваются в этом разделе. В первую очередь, целесообразно рассмотреть различие планов нумерации в России и в других странах Европы. Они перечислены в табл. 4. Следует подчеркнуть, что в ближайшие годы предполагается привести план нумерации российской ТфОП в полное соответствие с европейскими нормами.

Таблица 4. Различия планов нумерации российской и европейской ТфОП.

Набираемые комбинации цифр	**в России**	**в Европе**
Префикс выхода в междугородную сеть	8	0
Префикс выхода в международную сеть	8-10	0-0
Первая цифра доступа к экстренным службам	0	1

Очевидно, что по трем перечисленным позициям принципы нумерации различны. На самом деле различия более существенны, так как аспекты

нумерации тесно связаны с принципами установления соединений в ТфОП. Общепринятый подход предусматривает накопление всех набираемых цифр в РАТС - рис. 2. После анализа этих цифр РАТС выбирает оптимальный маршрут для установления соединения. РАТС в российской ТфОП - после набора префикса выхода в междугородную телефонную сеть - не участвует в выборе маршрута для установления соединения.

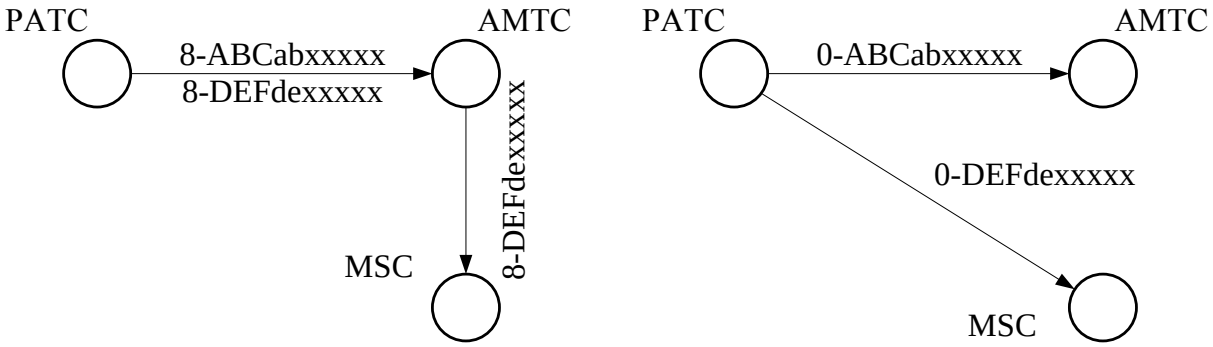


Рис. 2. План нумерации и маршрутизация вызовов.

При установлении соединения через центр коммутации мобильной связи (MSC - Mobile Switching Center) с использованием номера вида 8 - DEFdexxxxx маршрутизация вызовов в российской и в гипотетической европейской ТфОП осуществляется по-разному.

В отечественной ТфОП после набора префикса «8» подключается тракт до АМТС. Далее именно междугородная станция выполняет функции маршрутизации. В гипотетической европейской ТфОП номер DEFdexxxxx анализируется в РАТС. Далее соединение может быть установлено по прямому пучку СЛ между РАТС и MSC.

С рассматриваемым примером связана еще одна особенность российской ТфОП, обусловленная отступлением от международных норм. Речь идет о выборе Оператора дальней (междугородной и/или международной) связи.

При анализе всех цифр набранного номера в РАТС реализация функций выбора Оператора упрощается. Обычно с этой целью используются категории оконечных устройств.

В российской ТфОП, в силу принятых ранее решений об обслуживании вызовов, начинающихся с цифры «8», такой подход реализовать очень сложно. На начальном этапе введения функций, касающихся выбора Оператора дальней связи, используется дополнительный префикс, который набирается после цифры «8».

Как правило, отступления от международных норм ведут к росту затрат Оператора, которые связаны с реконструкцией ТфОП, необходимой для поддержки новых видов обслуживания.

Идентификация абонентов в ТфОП РФ

Для идентификации оконечных элементов телефонных сетей связи используются комбинации цифровых обозначений:

- код страны (Кс) – от 1 до 3 десятичных знаков (Российская Федерация, Кс=7);

- код зоны нумерации (ABC – для географически определяемой зоны нумерации, DEF – для географически не определяемой зоны нумерации) – 3 десятичных знака для РФ;

- зоновый телефонный номер ($x_1\,x_2\,x_3\,x_4\,x_5\,x_6\,x_7$) – 7 десятичных знаков.

Местный телефонный номер может включать от 3 до 7 десятичных знаков и совпадать по значности с зоновым телефонным номером или быть более коротким.

Последовательное обозначение кода страны, кода зоны нумерации и зонового телефонного номера образует международный телефонный номер (Nмн). Максимальное число десятичных знаков в международном номере равно 15 без учёта международного префикса Пмн.

Последовательное обозначение кода зоны нумерации, зонового номера образует национальный (значащий) телефонный номер Nнац. Максимальное число десятичных знаков в национальном (значащем) номере РФ равно 10.

Международный телефонный номер однозначно определяет оконечный элемент сети связи в пределах мировых сетей связи.

Национальный телефонный номер однозначно определяет оконечный элемент сети местной телефонной связи или сети подвижной связи в пределах территории РФ.

Зоновый телефонный номер однозначно определяет оконечный элемент сети местной телефонной связи в пределах территории субъекта РФ.

Местный телефонный номер однозначно определяет оконечный элемент сети местной телефонной связи в пределах муниципального образования субъекта РФ и города федерального значения.

Для установления международного телефонного соединения используется международный префикс Пмн = 00.

Для установления междугородного и внутризонового телефонного соединения используется национальный префикс Пн = 0.

В сетях фиксированной телефонной связи в РФ используются два плана нумерации – открытый и закрытый.

При закрытом плане нумерации телефонное соединение любого вида (местное, внутризоновое, междугородное) устанавливается набором национального номера. В РФ при установлении внутризонового соединения используется закрытый план нумерации, при котором количество десятичных знаков в национальном номере равно 10.

При открытом плане нумерации местное телефонное соединение устанавливается набором местного номера, а внутризоновое и междугородное телефонные соединения – набором национального номера с префиксом Пн.

При установлении телефонного соединения в сети подвижной связи используется закрытый план нумерации с префиксом Пн.

Зоновый телефонный номер, однозначно определяющий оконечный элемент местной сети, в которой используются 6-и, 5-и, 4-х и 3-х значные местные номера, дополняются до 7-и значного номера путём добавления знаков, равных значению x_1, x_1x_2, $x_1x_2x_3$, $x_1x_2x_3x_4$ зонового номера соответственно. При этом x_1 не должен быть равен 0 или 1.

Пример структурной схемы двух зон семизначной нумерации, в которых расположено по две местных сети (СТС и ГТС), показан на рис. 1.1. Там же указаны типы и емкости местных сетей и станций. Для ГТС с шестизначной нумерацией в каждом узловом районе следует показать не больше двух-трёх станций. На рисунке приведены примеры образования национальных (10-и значных) телефонных номеров.

Обозначения, которые использованы в чертеже:

ГТС - городская телефонная сеть;

СТС - сельская телефонная сеть;

ТМгУС - транзитный междугородный узел связи;

УАК – узел автоматической коммутации;

ТЗУС – транзитный зоновый узел связи;

АМТС - автоматическая междугородная телефонная станция;

УВС - узел входящей связи ГТС;

ЦС, УС, ОС - центральная, узловая и оконечная станции СТС;

ОПТС – опорно-транзитная телефонная станция.

АТС - автоматические телефонные станции ГТС. Показаны треугольниками с цифрами внутри. При этом одной цифрой обозначены АТС в районированных ГТС без узлообразования, а двумя цифрами – АТС в узловых районах. В первом случае в ГТС используется 5-и значная нумерация, а во-втором – 6-и значная.

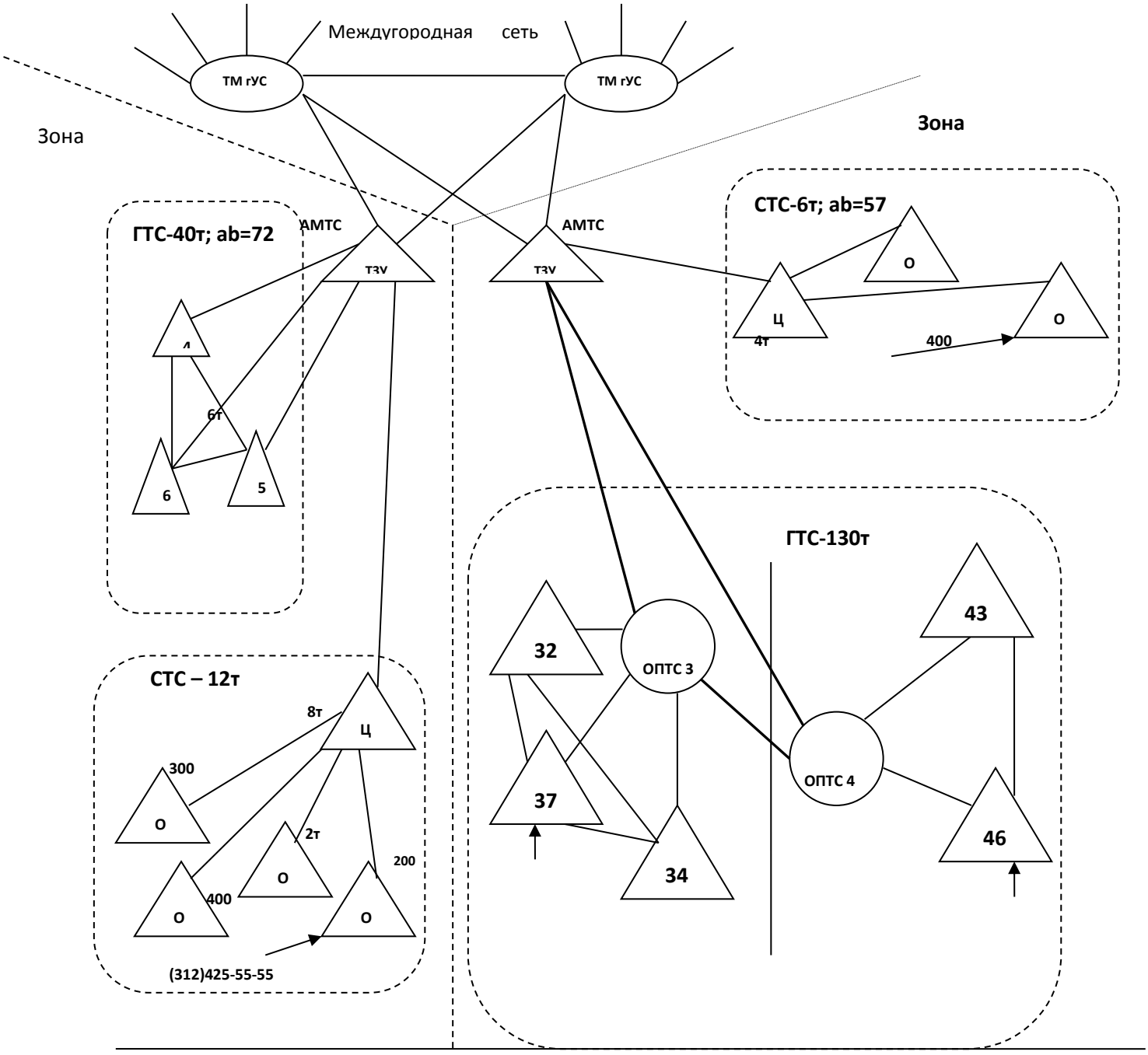


Рис. 1.1. Пример структурной схемы двух зон семизначной нумерации.

Контрольное задание

1. Привести структуру сети в двух зонах семизначной нумерации, в каждой из которых располагается по две местных сети. Емкости и типы местных сетей приведены в табл. 1.1. Номер варианта для зоны 1 определяется по предпоследней цифре шифра, а для зоны 2 – по последней.

2. Количество и емкость станций местных сетей выбираются так, чтобы показать структуру сети и нумерацию абонентов. При этом показывается такое количество станций, которое дало бы представление об особенностях построения сети.

3. Дать нумерацию абонентам местных сетей, приняв закрытую систему нумерации. Выбрать коды местных сетей и коды зон семизначной нумерации.

4. В соответствии с выбранной в п.2 нумерацией написать последовательность цифр, которые набирает абонент при осуществлении:

а) местной связи,

б) внутризоновой связи,

в) междугородной связи.

Таблица 1. Емкости и типы местных сетей

№ вар	Типы и емкости местных сетей в зоне семизначной нумерации 1	Типы и емкости местных сетей в зоне семизначной нумерации 2
1	СТС 8 тыс. ГТС 20 тыс.	ГТС 120 тыс. ГТС 45 тыс
2	ГТС 100 тыс. СТС 9 тыс.	СТС 7 тыс. ГТС 25 тыс.
3	ГТС 30 тыс. ГТС 45 тыс.	СТС 11 тыс. ГТС 85 тыс.
4	СТС 14 тыс. ГТС 35 тыс.	ГТС 8 тыс; СТС 16,5 тыс.
5	СТС 17,5 тыс. ГТС 110 тыс.	ГТС 50 тыс.СТС 10,5 тыс.
6	СТС 12,5 тыс. ГТС 100 тыс.	ГТС 25 тыс. СТС 17,5 тыс.
7	СТС 8.5 тыс. СТС 10 тыс	ГТС 95 тыс. ГТС 35 тыс.
8	СТС 7 тыс. ГТС 80 тыс	СТС 20 тыс. ГТС 45 тыс
9	ГТС 25 тыс. СТС 17 тыс	ГТС 90 тыс. СТС 9,5 тыс.
10	ГТС 75 тыс. ГТС 30 тыс.	СТС 10 тыс. СТС 16,5 тыс.

Контрольные вопросы:

1. Каким документом определяется нумерация в ТФОП.

2. Может ли на ГТС первая цифра номера начинаться с цифр 0 или 1?

3. Что понимается под кодом нумерации ab?

4. Поясните, что понимается под кодом страны, чем он устанавливается и он для Российской Федерации?

5. Что понимается под кодом АВС?

6. Поясните составные части любого телефонного номера указанного на схеме в выполненной работе.

7. Поясните сформированную вами структуру сети?

8. Покажите пример радиального и радиально-узлового подключения абонентов.

Литература.

1. Требования к порядку пропуска трафика в телефонной сети общего пользования (Приказ Министерства ИТ и Связи РФ от 08.08.2005г. № 98)

Практическое занятие №2. Изучение интерфейса и основных возможностей программного продукта Cisco Packet Tracer.

Цель занятия: Изучить интерфейс и основные возможности моделирующей среды Cisco Packet Tracer.

Задание. Изучить положение элементов на главном интерфейсе Cisco Packet Tracer. Рассмотреть возможные виды коммутационного оборудования и линий связи, на базе которых может быть построена сеть. Физическая комплектация оборудования.

Cisco Packet Tracer - это эмулятор сети, созданный компанией Cisco. Данное приложение позволяет строить сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов.

Программное решение Cisco Packet Tracer позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т.д. Работа с интерактивным симулятором дает ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств.

Настройки, в свою очередь, зависят от характера устройств: одни можно настроить с помощью команд операционной системы Cisco IOS, другие – за счет графического веб-интерфейса, третьи – через командную строку операционной системы или графические меню.

Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, пользователь может отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности. Cisco Packet Tracer может быть использован не только как симулятор, но и как сетевое приложение для симулирования виртуальной сети через реальную сеть, в том числе Интернет. Пользователи разных компьютеров, независимо от их местоположения, могут работать над одной сетевой топологией, производя ее настройку или устраняя проблемы. Эта функция многопользовательского режима Cisco Packet Tracer может применяется для организации командной работы.

В Cisco Packet Tracer пользователь может симулировать построение не только логической, но и физической модели сети и, следовательно, получать навыки проектирования. Схему сети можно наложить на чертеж реально существующего здания или даже города и спроектировать всю его кабельную проводку, разместить устройства в тех или иных зданиях и помещениях с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

Симуляция, визуализация, многопользовательский режим и возможность проектирования делают Cisco Packet Tracer уникальным инструментом для обучения сетевым технологиям.

Главное окно Cisco Packet Tracer

На рис. 1. представлен интерфейс программы, разделенный на области.

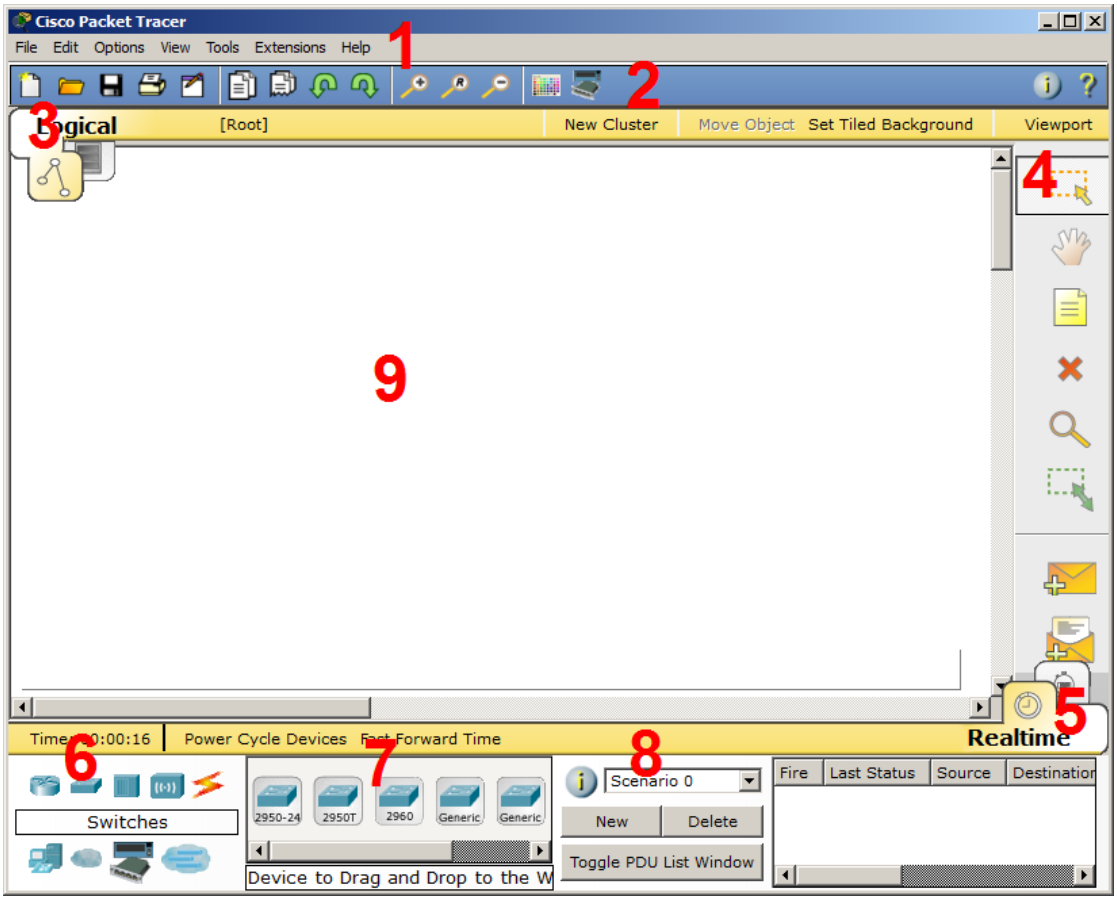


Рисунок 1 - Интерфейс программы Cisco Packet Tracer

1. Главное меню программы со следующим содержимым:

- Файл - содержит операции открытия/сохранения документов;
- Правка - стандартные операции "копировать/вырезать, отменить/повторить";
- Настройки - говорит само за себя;
- Вид - масштаб рабочей области и панели инструментов;
- Инструменты - цветовая палитра и кастомизация конечных устройств;

– Расширения - мастер проектов, многопользовательский режим и несколько приблуд, которые из CPT (так я иногда буду ласково называть Cisco Packet Tracer) могут сделать целую лабораторию;

– Помощь - ни за что не угадаете, что там содержится;

2. Панель инструментов, часть которых просто дублирует пункты меню;

3. Переключаетль между логической и физической организацией;

4. Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а так же формирование произвольных пакетов;

5. Переключатель между реальным режимом (Real-Time) и режимом симуляции;

6. Панель с группами конечных устройств и линий связи;

7. Сами конечные устройства, здесь содержатся всевозможные коммутаторы, узлы, точки доступа, проводники.

8. Панель создания пользовательских сценариев;

9. Рабочее пространство.

Пример размещения цветовых областей (рис.1.2), позволяющий например отделять визуально одну подсеть от другой.

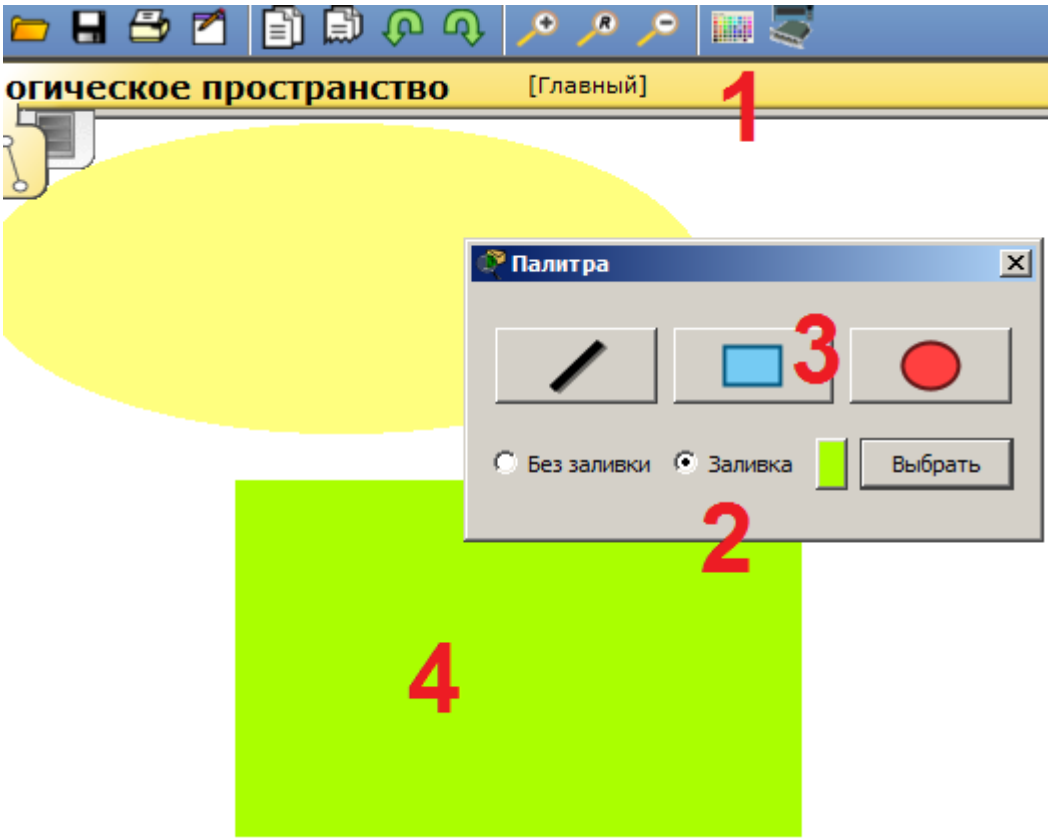


Рисунок 2 - Пример размещения цветовых областей.

Для установки цветных областей выполните следующие действия:

1 - На панели инструментов выбираем соответствующий значок;

2 - Выбираем режим области "Заливка", например;

3 - Выбираем цвет и форму;

4 - Рисуем область на рабочем пространстве.

Можно также добавить подпись и перемещать/масштабировать эту область.

Оборудование и линии связи в Cisco Packet Tracer

Маршрутизаторы

Маршрутизаторы используется для поиска оптимального маршрута передачи данных на основании специальных алгоритмов маршрутизации, например выбор маршрута (пути) с наименьшим числом транзитных узлов.

Работают на сетевом уровне модели OSI.

Коммутаторы

Коммутаторы - это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Передаёт пакеты коммутатор на основании внутренней таблицы - таблицы коммутации, следовательно трафик идёт только на тот MAC-адрес, которому он предназначается, а не повторяется на всех портах (как на концентраторе).

Концентраторы

Концентратор повторяет пакет, принятый на одном порту на всех остальных портах.

Беспроводные устройства

Беспроводные технологии Wi-Fi и сети на их основе. Включает в себя точки доступа.

Линии связи

С помощью этих компонентов создаются соединения узлов в единую схему.

Packet Tracer поддерживает широкий диапазон сетевых соединений (см. табл. 1.1).

Каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов.

Таблица 1 - Типы кабелей.

Тип кабеля	Описание
Консоль 	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Должны быть выполнены некоторые требования для работы консольного сеанса с ПК: скорость соединения с обеих сторон должна быть одинаковая, должно быть 7 бит данных (или 8 бит) для обеих сторон, контроль четности должен быть одинаковый, должно быть 1 или 2 стоповых бита (но они не обязательно должны быть

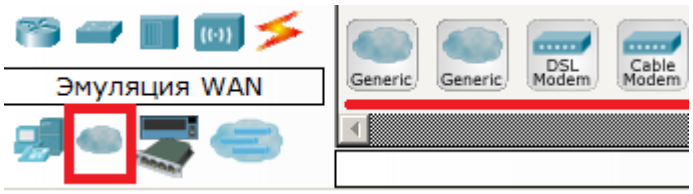
	одинаковыми), а поток данных может быть чем угодно для обеих сторон.
Медный прямой 	Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, который функционирует на разных уровнях OSI. Он должен быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).
Медный кроссовер 	Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Он может быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet)
Оптика 	Оптоволоконная среда используется для соединения между оптическими портами (100 Мбит/с или 1000 Мбит/с).
Телефонный 	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты. Стандартное представление модемного соединения - это конечное устройство (например, ПК), дозванивающееся в сетевое облако.
Коаксильный 	Коаксиальная среда используется для соединения между коаксиальными портами, такие как кабельный модем, соединенный с облаком Packet Tracer.
Серийный DCE 	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить

Серийный DTE 	синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становиться DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

Конечные устройства

Здесь представлены конечные узлы, хосты, сервера, принтеры, телефоны и т.д.

Эмуляция Интернета



Пример эмуляция глобальной сети. Модем DSL, "облако" и т.д.

Пользовательские устройства и облако для многопользовательской работы

Устройства можно комплектовать самостоятельно. Можно создавать произвольные подключения.

Физическая комплектация оборудования

Установите в рабочем поле роутер Cisco 1841 В настройках на роутере открываем его **физическую конфигурацию (рис.1.3).**

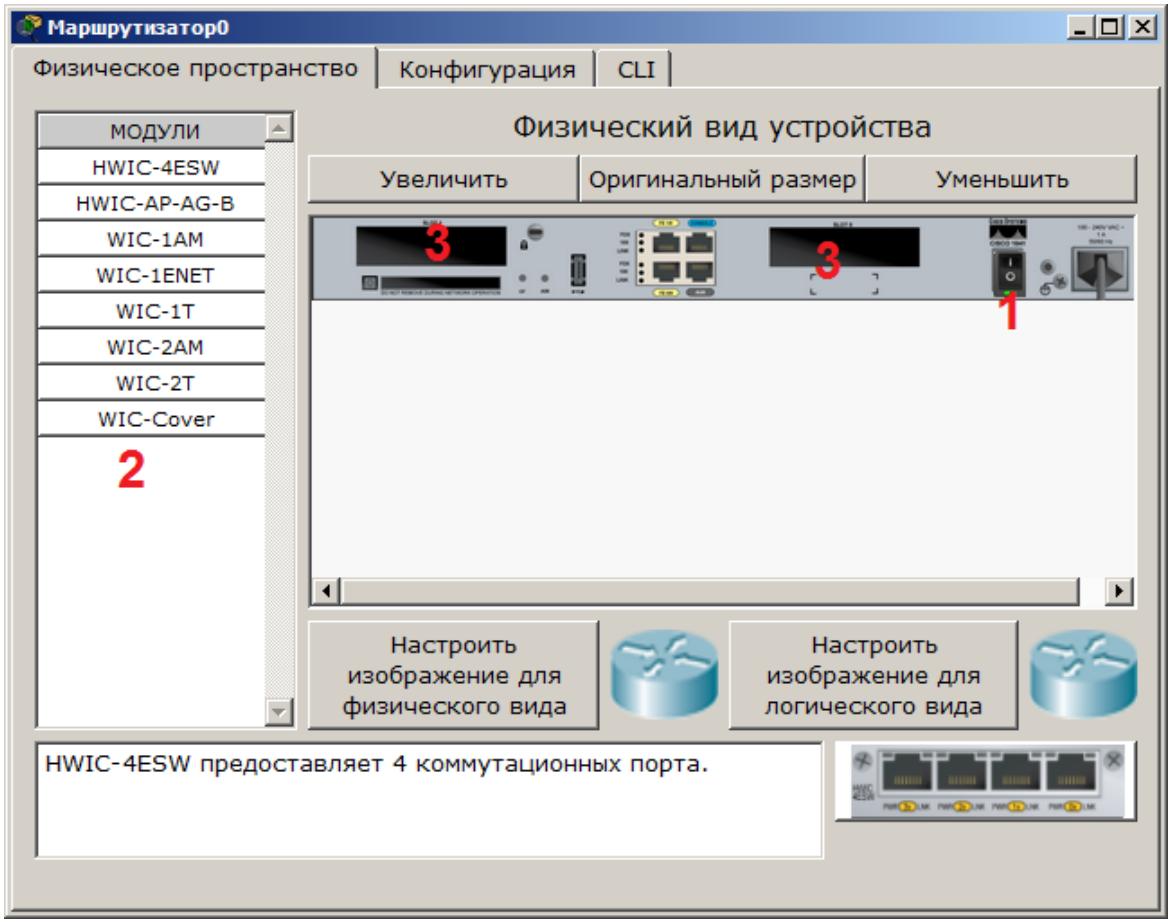


Рисунок -. Физическая конфигурация устройства

Слева, как мы видим, список модулей (цифра 2), которыми можно укомплектовать данный роутер. Сейчас в нем 2 пустоты (цифра 3). В них можно вложить эти модули. Разумеется, эту операцию нужно производить при выключенном питании (цифра 1).

Модули WIC (HWIC, VWIC) это платы расширения, увеличивающие функционал устройства:

WIC - WAN interface card. the first original models.

HWIC- high-speed wan interface card- the evolution of wic that is now in use on the ISR routers.

VIC - voice interface card, support voice only.

VIC2 - evolution of the above

VWIC - voice and wan interface card. An E1/T1 card that can be user for voice or data.

VWIC2 - evolution of the above

Например для компьютера есть платы, подключаемые к PCI-шине (TV-тюнеры, звуковые карты, USB-разветвители, сетевые карты), так и здесь. Вообще, устройство Cisco - это тот же системный блок со своей операционкой и многими сетевыми картами, который может делать что-то только с сетью.

Ниже представлена информация о каждом модуле:

– **HWIC - 4ESW** - высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45. Позволяет сочетать в маршрутизаторе возможности коммутатора.

– **HWIC-AP-AG-B** - это высокоскоростная WAN-карта, обеспечивающая функционал встроенной точки доступа для роутеров линейки Cisco 1800 (модульных), Cisco 2800 и Cisco 3800. Данный модуль поддерживает радиоканалы Single Band 802.11b/g или Dual Band 802.11a/b/g.

– **WIC-1AM** включает в себя два разъема RJ-11 (телефоннка), используемых для подключения к базовой телефонной службе. Карта использует один порт для соединения с телефонной линией, другой может быть подключен к аналоговому телефону для звонков во время простоя модема.

– **WIC-1ENET** - это однопортовая 10 Мб/с Ethernet карта для 10BASE-T Ethernet LAN.

– **WIC-1T** предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам, например SDLC концентраторам, системам сигнализации и устройствам packet over SONET (POS).

– **WIC-2AM** содержит два разъема RJ-11, используемых для подключения к базовой телефонной службе. В WIC-2AM два модемных порта, что позволяет использовать оба канала для соединения одновременно.

– **WIC-2T** - 2-портовый синхронный/асинхронный серийный сетевой модуль предоставляет гибкую поддержку многих протоколов с индивидуальной настройкой каждого порта в синхронный или асинхронный режим. Применения для синхронной/асинхронной поддержки представляют:

– низкоскоростную агрегацию (до 128 Кб/с);

– поддержку dial-up модемов;

– синхронные или асинхронные соединения с портами управления другого оборудования и передачу устаревших протоколов типа Bi-sync и SDLC.

– **WIC-Cover** - стенка для WIC слота, необходима для защиты электронных компонентов и для улучшения циркуляции охлаждающего воздушного потока.

Для изменения комплектации оборудования необходимо:

отключить питание, кликнув мышью на кнопке питания, перетащить мышью модуль **4ESW** в свободный слот и включить питание. Подождать окончания загрузки роутера. В конфигурации GUI можем увидеть появившиеся 4 новых интерфейса (рис.4).

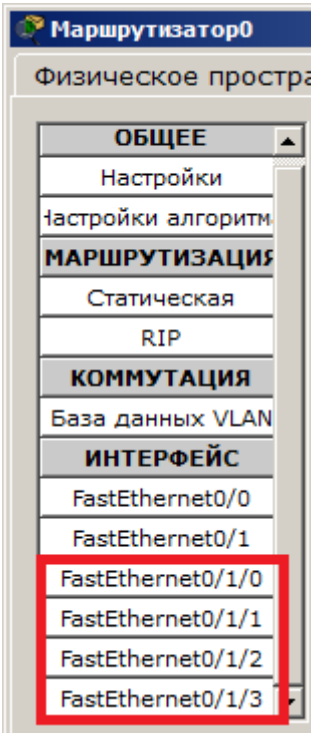


Рисунок 4 - Конфигурация интерфейсов устройства.

Остальные устройства комплектуются аналогично. Добавляются новые модули Ethernet (10/100/1000), оптоволоконные разъемы нескольких типов, адаптеры беспроводной сети. На рабочий компьютер есть возможность добавить например микрофон с наушниками, жесткий диск для хранения данных.

Контрольные вопросы:

1. Какая плата расширения обеспечивает функционал встроенной точки доступа?
2. Какая плата расширения предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам?
3. Как называется высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45?
4. Перечислите сетевые карты, позволяющие подключаться к WAN сетям?

5. Какой тип интерфейса следует выбрать при создании кластера?
6. Назовите модели коммутаторов третьего уровня?
7. Какой тип кабеля следует использовать при соединении роутеров между собой?
8. Укажите серии магистральных маршрутизаторов.
9. В каких случаях используется интерфейс SERIAL?
10. Как организовать связь двух магистральных маршрутизаторов?
11. Перечислите все возможные режимы работы программы Cisco Paket Tracer?
12. Назовите модели коммутаторов второго уровня?
13. Перечислите все типы связей, используемых в Cisco Paket Tracer и укажите их назначение.

Практическое занятие №3. Построение городской мультисервисной сети.

Цель занятия: получить навыки расчёта городской мультисервисной сети.

Задание. На основе индивидуальных исходных данных построить структуру проектируемой сети. Определить состав абонентов по информационным микрорайонам. Рассчитать объёмы мультимедийных потоков. Произвести выбор типа абонентского и корневого оборудования. Проектирование вторичной сети. Определение требуемой полосы по участкам первичной сети.

Мультисервисная сеть – это сеть способная предоставлять своим заказчикам – юридическим и физическим лицам – такие современные услуги связи, как высокоскоростной широкополосный доступ к сети Internet, передача данных по протоколу IP, передача аудио- и видеопотоков по протоколу IP с возможностью организации приоритетных потоков (Quality of Service – QoS).

Мультисервисная сеть – сеть, в которой на структурно-логическом и (или) аппаратурном уровнях объединены различные сетевые технологии, обеспечивающие весь спектр или набор услуг, предоставляемых на основе отдельных сетевых технологий.

Исторически термин мультисервисные сети возник после того, как провалились попытки безболезненного объединения в одной сети таких разнородных по характеру и требованиям к обслуживанию трафиков, как речь и видео с одной стороны и данные с другой.

Отличительной чертой трафиков речи и видео является их предсказуемость. Это так называемые потоковые трафики, для которых характерны:

- примерно постоянные требования к скорости передачи оцифрованной речи или изображения;

- крайне жесткие требования к времени задержки информации в сети и к вариации этой задержки (джиттеру);

- некритичность к потерям отдельных пакетов из общего потока.

Совершенно противоположный характер носит трафик данных. Здесь:

- всплесковый характер потоков межмашинного обмена. Коэффициент пульсаций, определяемый как отношение потока в пиковые моменты к среднесуточному, составляет для разных систем 50:1, 100:1 и даже 200:1;

- отсутствие жестких требований к времени задержки пакетов;

- критичность к потерям или искажениям пакетов.

Задержка пакетов с замерами оцифрованной речи на величину более 0,15 – 0,25с делает затруднительным ведение переговоров в режиме реального времени, т.к. собеседники могут воспринимать такую задержку как молчание, инициировать ответную фразу и их речи начнут накладываться друг на друга.

Напротив, для оператора ЭВМ задержка в получении ответа на 1 – 2 сек, обычно проходит незамеченной. Для системы распределенных вычислений, когда инициаторами большей части обменов выступают машины, задержки, как

правило, тоже не страшны, так как машины в ожидании ответа могут выполнять другие вычисления.

Потери отдельных или даже группы пакетов речевого сигнала могут быть скомпенсированы экстраполяцией предыдущих отсчетов в силу достаточно плавного характера кривой аналогового речевого сигнала. Пользователи к такого рода искажениям речи относятся терпимо.

В части видео-трафика имеется очень большой диапазон возможных скоростей (от 28,8 кбит/с до 34 Мбит/с) и допустимых задержек в зависимости от вида передачи. Например, частое сдёргивание кадра при просмотре видео по запросу может испортить художественное восприятие фильма. В то же время при проведении видеоконференцсвязи более важным является услышать все сказанное, чем увидеть непрерывное изображение.

Что касается потери пакетов из трафика данных, то очевидно, что они недопустимы. Никому не нужен файл с отсутствующими байтами.

Однако, здесь не все так страшно, поскольку помимо сетевого уровня, занимающегося непосредственно передачей пакетов, существуют надсетевые уровни. Например, транспортный (если реализован режим виртуальных соединений) или пользовательский (если пользователь дорожит целостностью своей информации), которые могут и должны обнаруживать потерю одного или части пакетов и инициировать адресный запрос потерянных пакетов или безадресный целого сообщения (файла). И в том и другом случае такие потери, в конечном счете, проявляются в задержке передачи и в дополнительной нагрузке на сеть.

Указанные особенности трафиков привели к тому, что процесс конвергенции речи и данных в единую сеть затянулся на долгие годы. В основу сети Internet лег прекрасный стек протоколов TCP/IP, который изначально был ориентирован на передачу пакетов в режиме UDP, т.е. без организации виртуальных каналов.

Поэтому провайдеры услуг Internet могут гарантировать своим речевым абонентам только более дешевые, по сравнению с ТфОП (примерно в 2 – 4

раза), тарифы на ведение междугородных и международных переговоров. Но никак не то прекрасное качество и надежность, которое гарантирует традиционная телефония.

Но традиционная телефония – это коммутация каналов, а она не может служить базой для мультисервисных сетей, т.е. для передачи трафика “данные + аудио + видео” (Triple Play), поскольку коммутировать канал с полосой под пики всплескового трафика данных – дело расточительное.

После того, как схема IP/ВОЛС или IP/SDH/ВОЛС оказалась неспособной решить задачи конвергенции триады (D+A+V) стали появляться технологии, способные дифференцировано подходить к обслуживанию разных типов мультимедийного трафика.

Так технология Frame Relay предлагала пользователям оплачивать по большей стоимости так называемый гарантированный трафик (CIR) и таким образом могла, например, обеспечить приоритетность потоковых трафиков перед трафиком данных. Следующим этапом стало появление технологии ATM, способной обслуживать потоки по 5 классам услуг и в двух высших классах (CBR и VBR) реализовать режим гарантированной доставки за счет резервирования ресурсов запрашиваемого виртуального канала. Сторонники ATM предрекали ей великое будущее как единой технологии, способной реализоваться во всех сетях – от локальных до глобальных (т.е. в LAN, MAN и WAN). Однако, в ЛВС простая и дешевая технология Ethernet не только не сдавала своих позиций, но более того, с появлением GigaBit Ethernet и 10GE стала вторгаться в городские сети (MAN).

К основным, давно известным недостаткам ATM – сложность и дороговизна – в последнее время стали прибавляться и некоторые из ее достоинств. А именно, слишком тщательный учет требуемых ресурсов для каждого запрашиваемого виртуального канала и слишком малая длина ячейки (53 байта). Переход каналов на гигабитные скорости (STM-16 и STM-64, т.е. 2,5 Гбит/с и 10 Гбит/с) делает эти достоинства не столь очевидными.

Основной конкурирующей с ATM технологией в настоящее время стала мультипротокольная коммутация меток (MPLS), которая как и ATM обеспечивает обслуживание мультимедийного трафика, но делает это немного грубее (и быстрее).

Так в MPLS определены только 3 категории трафика:

- трафик, для которого ресурсы выделяются всегда;
- трафик, для которого ресурсы выделяются по возможности;
- трафик, обслуживаемый без выделения ресурсов.

И хотя вопрос о том, что лучше – ATM или MPLS, еще не решен, вполне возможно, что какое-то время они будут сосуществовать, например, в схеме IP/ATM/MPLS, в которой сеть MPLS является ядром магистральной сети, а ATM – сетью доступа к ядру. Существуют и обратные варианты – IP/MPLS/ATM.

В рамках настоящего курсового проекта на роль технологии, обслуживающей мультимедийные потоки с заказываемым качеством в режиме статистического уплотнения с реализацией режимов виртуальных каналов можно выбрать одну из двух технологий – ATM или MPLS.

Если принять для первичной сети наиболее популярную в настоящее время технологию SDH, тогда на выбор студента-проектировщика предлагаются две схемы организации сетевой иерархии: IP/ATM/SDH или IP/MPLS/SDH. При этом IP в этой схеме означает, что первоначально в ЭВМ пользователя формируется IP-пакет с данными, аудио- или видеоинформацией. Далее, во вторичной сети реализуется технология обслуживания мультимедийных потоков (ATM или MPLS). И наконец, в первичной сети реализуется технология SDH.

В более полной схеме необходимо учесть, что между ЛВС (или индивидуальной ЭВМ) и магистральной сетью, как правило, существуют каналы (или сети) абонентского доступа. Например: ISDN, xDSL, Frame Relay и др. Тогда для общей схемы курсового проекта можно применять следующие варианты: IP/xDSL/ATM/SDH, IP/FR/MPLS/SDH, IP/FR/ATM/SDH и т.д.

Основной проблемой для расчета мультисервисных сетей является трудность расчета необходимой полосы пропускания (или канальной скорости) для пропуска мультимедийного трафика с заданными потоками по каждому типу трафика (D+A+V) и с заданными вероятностями явных или неявных потерь. Вековая история развития теории телетрафика была почти исключительно направлена на анализ телефонных систем и оказалась бессильной для расчета сетей передачи данных, а тем более мультисервисных (т.е. смешанных) сетей.

Структура проектируемой сети

Проектируемая сеть построена по классической структуре сетей с коммутацией пакетов (рис. 1), в которых имеются четко выраженные составляющие сети абонентского доступа (САД), первичной сети (ПС) и вторичной сети (ВС). В свою очередь вторичная сеть, как правило, подразделяется на ядро ВС и сеть распределения. Иногда функции первичной и вторичной сетей объединяются в одну сеть.

Рисунок 1- Иерархическая структура мультисервисной

Основой любой реальной сети связи является уровень неспециализированной (универсальной) первичной сети, представляющей собой совокупность узлов и соединяющих их типовых физических цепей,

типовых каналов передачи и сетевых трактов. Цифровая первичная сеть (ЦСП) – это базовая сеть типовых универсальных цифровых каналов передачи (ЦКП) и сетевых трактов, или транспортная сеть, образованная на базе сетевых узлов, сетевых станций коммутации или оконечных устройств первичной сети и соединяющих их линий передачи.

Современная городская опорная сеть (backbone) строится почти исключительно на базе оконечных мультиплексоров (ОМ) и мультиплексоров ввода/вывода (МВВ) и соединяющих их волоконно-оптических линий связи (ВОЛС). В основном применяются кольцевые структуры в различных модификациях (рис.2).

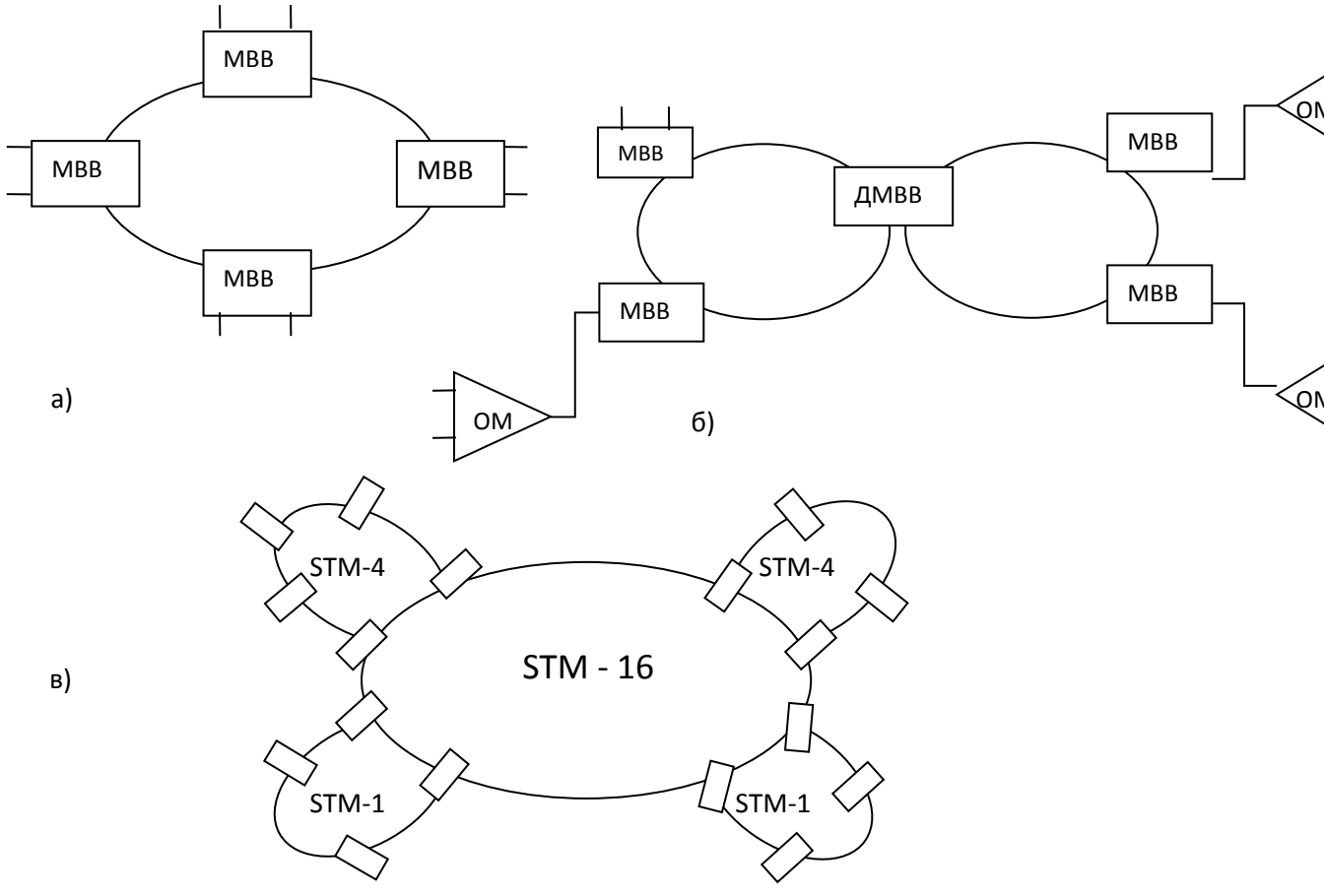


Рисунок 2- Варианты конфигураций городских опорных сетей

Для передачи применяется технология SDH с использованием стандартных транспортных модулей STM–1, STM–4, STM–16 и STM-64 (скорости соответственно (155 Мбит/с, 622 Мбит/с, 2,5 Гбит/с и 10 Гбит/с).

Упомянутая выше универсальность ПС состоит в том, что для нее безразличен тип передаваемого трафика. ПС выполняет заказ (как правило, в виде аренды) на предоставление определенной полосы пропускания для пропуска цифрового потока. При этом основными договорными параметрами являются канальные скорости передачи данных (от 2 Мбит/с и выше) и допустимая вероятность ошибок в битах – Bit Error Rate – BER=$10^{-9} \div 10^{-12}$.

В данном проекте создается однокольцевая волоконно-оптическая сеть SDH, содержащая 5 МВВ по числу узлов коммутации во вторичной мультисервисной сети и по числу информационных микрорайонов (ИМР). На самом деле, многопользовательская ПС может иметь большее число узлов и более сложную конфигурацию для нужд других вторичных сетей, но для данного проекта эти сети прозрачны.

На базе первичных сетей создаются разнообразные вторичные сети, которым ПС предоставляет сетевые тракты для пропуска трафика вторичной сети. Сетевой тракт – это групповой тракт или несколько последовательно соединенных групповых трактов с включенной на входе и выходе аппаратурой образования тракта. Сетевой тракт обеспечивает целостность передачи информации по соединениям трактов от точки формирования тракта в одном из сетевых узлов, до точки его расформирования в другом сетевом узле (в нашем случае от одного мультиплексора (ОМ или МВВ) до другого).

Вторичные сети являются специализированными для предоставления определенных услуг пользователям (телефон, данные, факс, потоковое видео и др.) путем пропуска через свои узлы коммутации (УК) и через первичную сеть потоков, специфичных для данной вторичной сети. Например:

- потоки оцифрованной речи для ТфОП;
- потоки IP–пакетов для межмашинного обмена;
- видеотрафик кабельного телевидения;

- интегральный трафик сетей ISDN;

- мультимедийный трафик мультисервисных сетей для пропуска любых потоков между любыми типами абонентов (именно такая вторичная сеть создаётся в настоящем курсовом проекте).

Наконец, третья составляющая обобщенной сетевой структуры – *сеть абонентского доступа (САД)* – предназначена для подключения пользователей (абонентов) ко всем разделяемым ресурсам как транспортной, так и любой другой (например, корпоративной) сети.

В зависимости от требуемой полосы пропускания и конкретных физических возможностей различают следующие виды абонентского доступа:

- аналоговая телефонная линия (медная пара);

- модемная связь для телефонных каналов;

- модемная связь для физических линий;

- доступ по каналам ISDN;

- доступ по каналам xDSL;

- доступ по радиолиниям,

- доступ по спутниковым линиям связи,

- доступ по волоконно-оптическим линиям связи.

Таким образом, весь тракт от абонента до абонента, в общем случае, представляется в следующем виде:

Абонент1 - канал САД – УК вторичной сети – узел первичной сети (МВВ) – тракт первичной сети - узел ПС – УК ВС – канал САД – Абонент2 (рис.3, рис.4).

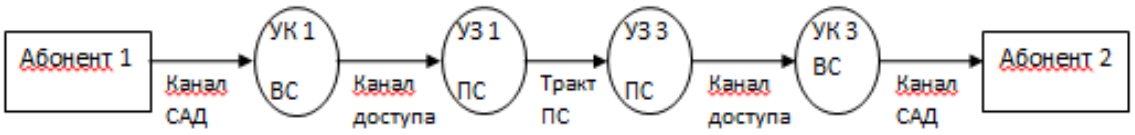


Рисунок 2

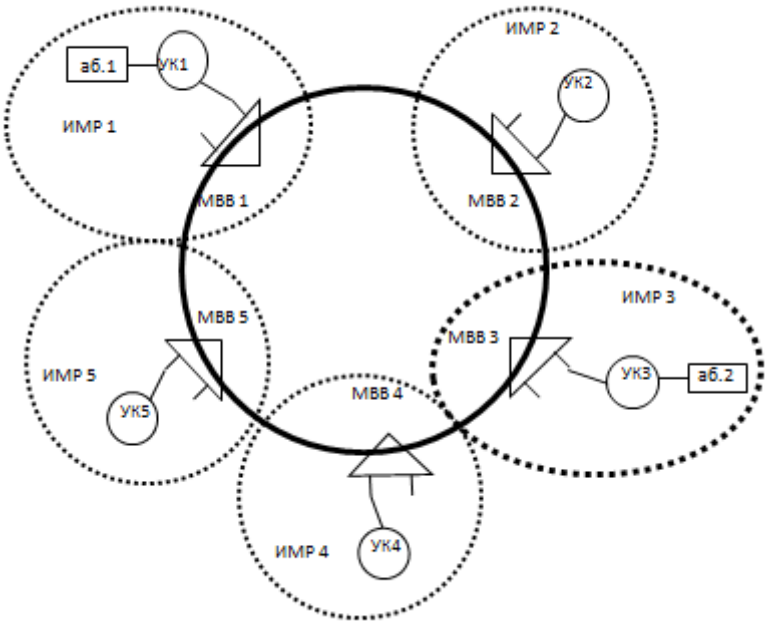


Рисунок 3

Определение состава абонентов по информационным микрорайонам (ИМР)

МСС проектируется для города, территория которого условно разделена на 5 информационных микрорайонов. В каждом ИМР организуется узел вторичной сети, являющийся центром привязки для абонентов данной ИМР.

Все абоненты (организации, офисы) для упрощения проектирования разделены на 4 категории по числу сотрудников (S_i) в них:

- АГ 1 – абонентские группы *первой категории* с числом сотрудников свыше 100, т.е. $S_1>100$. Это крупные производственные, медицинские или образовательные учреждения, крупные офисы;

- АГ 2 – абонентские группы *второй категории* с числом сотрудников от 30-ти до 100, т.е. $30<S_2\leq100$. Средние предприятия и офисы;

- АГ 3 – абонентские группы *третьей категории* с числом сотрудников от 5-ти до 30, т.е. $10<S_3\leq30$. это группа малых и домашних офисов (Small Office/Home Office – SOHO);

- АГ 4 – индивидуальные пользователи с небольшим телетрафиком. Отдельные (не организованные в ЛВС) компьютеры, в том числе и телекомьютеры.

Распределение абонентских групп (АГj) по микрорайонам (ИМРm) одинаковое для всех вариантов проекта, представлено в табл. 1.

Таблица 1 - Распределение абонентских групп по микрорайонам.

ИМРm \ АГj	ИМР1	ИМР2	ИМР3	ИРМ4	ИРМ5
АГ1	20	20	15	15	10
АГ2	30	28	25	25	20
АГ3	40	40	30	30	25
АГ4	160	150	120	110	100

Число сотрудников в первых трех группах (S_1, S_2, S_3) определяется каждым студентом индивидуально в зависимости от двух последних цифр шифра (N_1N_2) и от последней цифры текущего года (N_3) по табл. 2.

Таблица 2 - Число сотрудников в группах по вариантам курсового проекта

Группы / Варианты	0	1	2	3	4	5	6	7	8	9
S_1(по предпоследней цифре шифра)	101	105	108	112	116	120	125	130	135	140
S_2(по последней цифре шифра)	31	40	50	60	70	75	80	85	90	100
S_3 (по последней цифре текущего года)	6	8	10	12	15	18	21	24	27	30

Например, в 2003 году для студента с шифром xxx27 численность сотрудников по абонентским группам в любом ИМР составит: S_1=108, S_2=85, S_3=12 и S_4=1.

Определение объемов мультимедийных потоков

Теоретическое обоснование расчета мультимедийного трафика.

Последнее десятилетие развитие телекоммуникационных сетей идет в направлении интеграции услуг. Происходит переход к мультисервисным сетям, в которых передаются и коммутируются различные виды информации: голос, данные и видео.

Это – цифровые сети с коммутацией каналов (У–ЦСИС), а так же пакетные сети на базе технологий ATM, IP/MPLS и др. При этом традиционная проблема связистов – эффективное использование полосы пропускания – приобретает особую актуальность. Существующие методы оценки требуемой полосы для пропуска мультимедийного трафика (голос + данные + видео), используемые при проектировании сетей, либо весьма громоздки, либо носят приближенный характер. На практике широко распространено простое суммирование полос единичных каналов с ориентировочной корректировкой полосы единичного канала по степени сжатия трафика.

Ниже приведен вывод аналитического выражения для требуемой полосы мультимедийной магистрали, основанный на нетрадиционном в теории телетрафика подходе – динамики моментов [1].

Обоснование расчетной формулы. Магистральную мультисервисную сеть можно представить в виде совокупности участков (ребер) j=1, 2, …J, каждый из которых соединяет два узла (вершины) и служит для пропуска различных типов i=1, 2, …I трафика, включая транзитный (для оконечных узлов данного участка). В случае, когда по конкретному участку передается трафик только одного типа (например, голосовая телефонная связь), требуемое число n единичных каналов (каждый из которых предназначен для обслуживания одного вызова) может быть оценено в виде:

$$n = \frac{(N\rho + K\sqrt{N\rho})}{(1+\rho)}, \qquad (1)$$

где ρ - удельная интенсивность в ЧНН, Эрл;

N - число абонентов;

Nρ - суммарная интенсивность нагрузки в час наибольшей нагрузки (ЧНН), Эрл.

Коэффициент К при допустимости потерь равной 0,01 (т. е. потеря одного из 100 вызовов) равен К=2,31.

Формула (1) получена на базе тех же исходных дифференциальных уравнений теории непрерывных марковских цепей, что и классическая формула ***B*** Эрланга для вероятности потери вызова в полнодоступной системе. Отличие состоит в том, что рассматриваются только два состояния каждого из однородных абонентов: абонент пассивен и абонент занимает канал.

Для каждого типа i мультимедийного трафика, на каждом из участков j мультисервисной сети средние значения E_{ij} и дисперсии D_{ij} случайного числа занятых каналов выражаются через N_{ij} и $\rho_{ij,}$, где ρ_{ij} означает удельную интенсивность трафика типа i в ЧНН на участке j, а N_{ij} – количество абонентов i-й услуги, для которых маршрут вызова проходит через j-й участок. При этом принимается, что речевой трафик – это трафик типа 1 (i=1), video-трафик – это трафик типа 2 (i=2) и трафик данных – это трафик типа 3 (i=3).

Если предположить, что вызовы различных типов i независимы, и учесть близость распределения случайного числа каналов, занятых вызовами каждого типа, к нормальному закону, то можно определить среднее значение и дисперсию суммарного числа каналов. Сумма любого числа независимых нормально распределенных величин распределена нормально, причем среднее значение этой суммы равно сумме средних, а дисперсия суммы – сумме дисперсий.

Необходимо ввести нормировку требуемой полосы для единичного трафика каждого типа, в частности, через коэффициенты $k_i \geq 1$, характеризующие приведение к минимальной полосе η телефонного трафика, для которого $k_i=1$. Другими словами, например, коэффициент $k_2=6$ показывает, что для video-трафика требуется в 6 раз большая полоса, чем для audio-трафика,

т. е. 384 Кбит/с, если за единичный трафик принята скорость основного цифрового канала – 64 Кбит/с. При введении коэффициентов k_i сохраняется правило суммирования средних и дисперсий, поскольку линейная функция нормальной величины также имеет нормальный закон распределения.

Окончательно требуемое число единичных каналов n с полосой η на каждом участке равно (индекс j опущен):

$$n \approx \sum_i \frac{k_i N_i \rho_i}{(1+\rho_i)} + K \sum_i \frac{\sqrt{k_i N_i \rho_i}}{(1+\rho_i)}. \qquad (2)$$

При N>10 000 и k_i<4 погрешность (2) мала и составляет 1%.

Как и в (1), при допустимости вероятности отказа, равной 0,01, коэффициент К=2,31.

Расчет параметров для каждого типа трафика.

При реальном построении сетей этапу проектирования в обязательном порядке предшествует этап обследования обслуживаемой территории, в процессе которого производится анализ предполагаемых информационных потоков, включая местоположение источников нагрузки, типы трафика, его объем и статистические свойства, тяготение между абонентами и пр.

В связи с отсутствием такого этапа в данном курсовом проекте параметры информационных потоков носят огрублённый, в основном, иллюстративный характер.

Как показано в разделе 4.1 для определения общего потока, складывающегося из трафиков данных, аудио- и видео-информации, необходимо для каждого типа нагрузки i (i=1, 2, 3) определить значения параметров:

- N_i – число сотрудников, которые могут быть источником данного вида трафика;

- ρ_i – удельная интенсивность нагрузки в ЧНН от одного сотрудника по виду трафика, Эрл;

- k_i – коэффициенты, характеризующие приведение полосы каждого типа к минимальной полосе.

За минимальную полосу естественно принять полосу аудио-трафика, как наименьшую из трех рассматриваемых полос (аудио, видео, данные).

Исходная скорость цифровизированной речи составляет 64 кбит/с (Это скорость ОЦК или DS0).

Требуемая полоса для передачи такого трафика, с одной стороны, может быть снижена за счет сжатия речи (например, применение кодеков G.729 снижает скорость до 20 – 28 кбит/с). С другой стороны, специфика пакетной передачи речи требует расширения полосы за счет «накладных расходов» (доли служебной информации протоколов канального, сетевого и транспортного уровней, иногда достигающей 70% для IP–пакета).

Поэтому, не вдаваясь в детали этих процессов, для целей настоящего проекта за единицу полосы мультисервисного потока примем ΔC=64 кбит/с.

Параметры аудиотрафика (телефонные разговоры).

Таким образом, требуемая полоса аудиотрафика $C_A=\Delta C$ и $k_A = k_1 = C_A / \Delta C = 1$. Примем, что пользоваться услугами IP–телефонии могут все сотрудники организации, т.е. $N_A=N_1=S_1$, а интенсивность аудио-нагрузки от одного сотрудника составляет $\rho_A=\rho_1$=0,02 Эрл. для абонентов 1-й, 2-й и 3-й групп и ρ_A=0,01 Эрл. для абонентов 4-й группы.

Параметры видеотрафика (видеоконференцсвязь).

В зависимости от требуемого качества изображения, алгоритмов сжатия видеоданных, числа пикселов и др. требуемая скорость передачи видеотрафика меняется в очень широких пределах (от десятков кбит/с до десятков Мбит/с)

В настоящем проекте в качестве приемлемой полосы для IP-видеоконференцсвязи выберем наиболее употребимую в настоящее время скорость - C_V=384 кбит/с.

Тогда: $k_V = k_2 = C_V / \Delta C = 6.$

Примем также, что число сотрудников, участвующих в различных телевидеоконференциях, составляет 5% от общего числа сотрудников, т.е. $N_V=N_2=0{,}05S$. Удельную интенсивность видео-нагрузки примем равной $\rho_V=\rho_2=0{,}015$ Эрл. При этом абоненты 3-й и 4-й групп видеоконференцсвязью не пользуются.

Параметры трафика данных..

Представление трафиков тремя параметрами N_i, ρ_i, k_i необходимо для того, чтобы можно было определить необходимую полосу для пропуска мультимедийного трафика по формуле (1). Однако, специфика трафика данных не позволяет определить эти параметры также легко, как это было сделано для мультимедийных трафиков (речь и видео).

В связи с этим ниже дается несколько иная, в большой степени искусственная, схема определения параметров N_i, ρ_i, k_i применительно к трафику данных.

Принять, что число сотрудников, обладающих необходимостью обмениваться трафиком данных, составляет $N_D=N_3=0{,}5S$, кроме абонентов 4-й группы (индивидуальные абоненты), для которых это число $N_D=1$. Удельную интенсивность нагрузки примем равной $\rho_D=\rho_3=0{,}1$ Эрл. для абонентов 1-й, 2-й и 3-й групп и $\rho_D=0{,}01$ Эрл. - для абонентов 4-й группы.

Среднесуточную скорость исходящего трафика данных от одного сотрудника из числа N_D примем равной $C_{Dср.сут.}=1$ кбит/с. Тогда, скорость исходящего потока данных в пиковые моменты, с учетом коэффициента пульсаций 100:1, составит $C_D=100\cdot C_{Dср.сут}=100$ кбит/с. Отсюда находим:

$$k_D = k_3 = C_D \big/ \Delta C = 1{,}6.$$

На основании этих параметров можно найти суммарную полосу пропускания (ПП) для пропуска совокупного исходящего трафика A, V, D.

Входящий трафик для аудио и видео информации можно принять равным исходящему, хотя для пакетной телефонии это не обязательно. Так, если один

из собеседников говорит больше другого, то поток пакетов будет асимметричен.

Трафик данных тоже для упрощения можно принять симметричным, кроме той его части, которая связана с обменом через Internet.

Приняв, что трафик данных, входящий к абоненту из Internet, превышает исходящий трафик втрое, а сам исходящий в Internet трафик данных составляет 20% от общего исходящего трафика данных и, учитывая ранее определенное $C_{Dисх}=C_D$, мы получим следующее значение для скорости входящего потока данных:

$$C_{Dвх}=C_{Dисх}\cdot(0,8+3\cdot0,2)=1,4\cdot C_{Dисх}=1,4\cdot C_D=140 \text{ кбит/с}.$$

Проще всего реализовать асимметрию трафика в данном проекте можно, введя различные значения для коэффициента k_D, т.е.

если $$k_{D_{ИСХ}} = k_3 = C_D \big/ \Delta C = 1,6,$$

то $$k_{D_{ВХ}} = 1,4 \cdot k_{D_{ИСХ}} = 2,24.$$

Приведем пример расчета параметров N_i, ρ_i, k_i для офиса с числом сотрудников S=110.

Таблица 3 - Пример расчета параметров исходящего абонентского трафика

i	N_i	ρ_i	k_i	$N_i\cdot\rho_i\cdot k_i$
1	110	0,02	1	2,2
2	6	0,015	6	0,54
3	55	0,01	$1,6 \big/ 2,24$	$8,8 \big/ 12,32$

* Для k_3 – в числителе – данные по исходящему трафику, а в знаменателе – по входящему.

По аналогии с табл. 3 составляется табл. 4 для заданного каждому студенту варианта распределения числа служащих по группам (S_j), где j – номер группы. Содержание табл. 4 не зависит от номера ИМР, т.к. распределение S_j по микрорайонам в данном проекте не меняется, а зависит только от варианта проекта.

Таблица 4. Пример расчета исходящей/входящей нагрузки от одного абонента по группам.

Номер группы	Число служащих S_j	i	N_{ij}	ρ_{ij}	k_{ij}	$N_{ij}\cdot\rho_{ij}\cdot k_{ij}$	$V_{j\text{исх}}/V_{j\text{вх}}$
АГ1	110	1	110	0,02	1	2,2	21,94/26,29
		2	6	0,015	6	0,54	
		3	55	0,01	1,6/2,24	8,8/12,32	
АГ2	85	1					
		2					
		3					
АГ3	22	1					
		2					
		3					
АГ4	1	1					
		2					
		3					

*Здесь: i - тип трафика, а j – номер абонентской группы.

Расчет полосы пропускания для абонентских групп.

На основании приведенных выше рассуждений можно рассчитать ПП для входящих и исходящих мультимедийных потоков для каждой из четырех абонентских групп, указанных в задании на проектирование.

Расчет по формуле (1) производится для абонентов каждой j–той группы $(j=\overline{1,4})$. Например, расчет исходящей полосы для одного абонента по данным таблицы 3 (S_1=110) дает следующие результаты в условных единицах потока:

$$V_{1_{исх}} = \sum_{i=1}^{3} \frac{k_i \cdot N_i \cdot \rho_i}{1+\rho_i} + K \cdot \sum_{i=1}^{3} \frac{\sqrt{k_i \cdot N_i \cdot \rho_i}}{1+\rho_i} = 21{,}94 y.e.n.$$

В данном случае $V_{j\text{исх}}$ – число условных единиц ПП, в качестве которой мы определили скорость стандартного (основного) цифрового канала DSO или в обозначениях, сделанных выше - ΔC=64 кбит/с.

Тогда требуемая скорость исходящего канала для подключения к магистральной сети абонента группы АГ1 с числом сотрудников S_1=110 будет равна $C_{1исх}$=1,4 Мбит/с.

Аналогично рассчитывается и требуемая скорость входящего потока: $V_{1вх}$=26,3 *у.е.п.* или $C_{1вх}$=1,68 Мбит/с.

Значения полосы в условных единицах для одного абонента каждой j–той группы - $V_{jисх} / V_{jвх}$ включить в табл. 4. Как и раньше коэффициент К=2,31 в выражении (1) рассчитывался для вероятности потерь, равной 0,01. хотя в данном случае этот показатель (потери) носит несколько условный характер, т.к. система с коммутацией пакетов работает как система с очередями и современные ТК – системы стараются избегать явных потерь пакетов.

Расчеты ПП в данном разделе проекта выполняются для одного абонента каждой из 4-х абонентских групп. Они послужат основой для выбора средств абонентского доступа к узлам коммутации вторичной сети и для расчёта суммарного трафика во вторичной сети. Результаты расчета свести в табл. 5.

Таблица 5. Пример расчета входящего и исходящего трафиков по абонентским группам.

Номер абонентской группы (j)	Число сотрудников (S_j)	Скорость исходящего потока ($C_{jисх}$), Мбит/с	Скорость входящего потока ($C_{jвх}$), Мбит/с
АГ1	110	1,4	1,68
АГ2			
АГ3			
АГ4			

Выбор типа абонентского доступа и конкретного устройства доступа

Подключение абонентских устройств к МСС по различным физическим средам производится с помощью модемов. Модем в широком смысле слова (не только телефонный) - это устройство, которое в зависимости от решаемых

задач, может выполнять разные функции: модуляцию и демодуляцию сигналов, преобразование аналоговых сигналов в цифровые и их обратное восстановление, преобразование одного вида модуляции в другой. Модем может быть автономным или встроенным в устройство, с которым функционально связан.

Современные модемы по области применения можно разделить на несколько групп:

- для коммутируемых телефонных каналов;

- для выделенных (арендуемых) телефонных каналов;

- для физических соединительных линий: модемы низкого уровня (линейные драйверы) или модемы на короткие расстояния (short range modems), модемы основной полосы (baseband modems);

- для сотовых систем связи;

- для пакетных радиосетей;

- для локальных радиосетей;

- кабельные модемы для подключения к цифровым сетям по системе кабельного телевидения (КТВ);

- для цифровых систем передачи. Обеспечивают подключение к стандартным цифровым каналам, таким как E1 или ISDN, и поддерживают функции соответствующих канальных интерфейсов;

- модемы технологии xDSL, обеспечивающие передачу речи и данных по медным телефонным линиям со скоростью в несколько мегабит.

Для оптической связи аналогичные функции выполняют светодиоды (LED) или лазерные диоды (LD), преобразующие напряжение электрических сигналов в оптическую мощность. Обратное преобразование светового сигнала в электрический ток осуществляется с помощью фотодетектора, PIN – диода или лавинного диода.

В данном проекте студент самостоятельно определяет необходимые виды абонентского доступа к МСС в соответствии с данными табл. 5 и производит выбор аппаратуры для обоих концов «последней мили».

При этом необходимо учесть следующее важное обстоятельство – общемировая тенденция в отношении трафика данных: почти удвоение ежегодно. Поэтому выбор аппаратуры нужно производить для скорости потоков (табл. 5) с некоторым запасом.

Рекомендуемые варианты аппаратуры для абонентского доступа приведены в Приложении 1.

Проектирование вторичной сети

Для реализации вторичной сети (ВС) студент самостоятельно выбирает одну из двух технологий (ATM или MPLS).

По согласованию с руководителем курсового проектирования можно выбрать и другие варианты, например, 10 Gigabit Ethernet, ориентируясь на тему дипломного проекта.

Определение параметров мультимедийного трафика в узлах коммутации вторичной сети.

В соответствии с принятой схемой (см. раздел 2) узлы коммутации (УК) располагаются в каждом ИМР (желательно в центре) и обеспечивают пропуск мультимедийного трафика, исходящего от всех абонентов данного ИМР и входящего к ним.

Расчет этого трафика нужно вести по данным таблиц 1 и 4, по формуле (1), модифицировав ее следующим образом:

$$W_{mj_{ИСХ}} = n_{mj} \cdot \sum_{i=1}^{3} \frac{k_{ij} \cdot N_{ij} \cdot \rho_{ij}}{1+\rho_{ij}} + K \cdot \sqrt{n_{mj}} \sum_{i=1}^{3} \frac{\sqrt{k_{ij} \cdot N_{ij} \cdot \rho_{ij}}}{1+\rho_{ij}} \qquad (3)$$

где m – номер ИМР, $m = \overline{1,5}$;

j – номер группы, $j = \overline{1,4}$;

i – тип трафика, $i = \overline{1,3}$ (A,V,D);

n_{mj} – число абонентов в группе j в ИМРm по данным табл. 1;

$N_{ij} \cdot \rho_{ij} \cdot k_{ij}$ – параметры потока типа i в группе j, по данным табл. 4;

$W_{mjисх}$ – число условных единиц потока (*у.е.п.*), исходящего от АГj в ИМРm и входящего в УКm.

Справедливость данной модификации объясняется следующим образом. В формуле (1) в каждом слагаемом присутствует параметр N_{ij} – число источников вызовов каждого типа i, в каждой группе j. В формуле (3) число таких источников увеличивается в n_{mj} раз (т.е. становится равным n_{mj} N_{ij}) и т.к. n_{mj} (а соответственно и $\sqrt{n_{mj}}$) не зависит от типа трафика i, то эти коэффициенты вынесены за знак суммирования.

Последнее допущение, которое нам придется сделать, сославшись теперь уже на большое число источников нагрузки, это произвести простое суммирование четырех потоков (от каждой АГ) в один общий поток, т.е. определить объёмы потоков в *у.е.п.*, исходящих от всех абонентов ИМРm и входящих в УКm, а также трафик для входящего в ИМР потока как:

$$W_{m_{ИСХ}} = \sum_{mj=1}^{4} W_{mj_{ИСХ}} \quad \text{и} \quad W_{mj_{ВХ}} = \sum_{j=1}^{4} W_{mj_{ВХ}} .$$

Результаты расчетов W *у.е.п.* и канальной скорости $C_{m\ исх}$ и $C_{m\ вх}$ (напомним, что C=W·64 кбит/с) для каждого ИМР (т.е. для каждого УК) свести в табл. 6.

Таблица 6. Пример расчета входящего и исходящего трафиков в узлах коммутации.

Направления трафика	Номер УК (ИМР)				
	УК1	УК2	УК3	УК4	УК5
От АГ к УК $W_{ИСХ}(у.е.п.) / C_{ИСХ}(Мбит/с)$	800/51,2				
От УК к АГ $W_{ВХ}(у.е.п.) / C_{ВХ}(Мбит/с)$	1000/64				
Суммар. поток через УК $W(у.е.п.) / C(Мбит/с)$	1800/115,2				

По результатам расчетов, приведенных в таблице 6, определяются требуемые суммарные пропускные способности УК с учетом определенного (в пределах 50-100%) запаса на расширение объема услуг. Рекомендуемые варианты аппаратуры для узлов коммутации приведены в Приложении 2.

Определение матрицы тяготений в магистральной сети.

Обмен во ВС производится в соответствии с теми параметрами потоков, которые каждый УКm передает каждому другому УК и себе.

Такие параметры представляются в виде матрицы тяготений C размерности M, элемент C_{ms} которой определяет скорость потока от УКm к УКs.

В реальных сетях эти потоки определяются конкретными данными по интенсивностям взаимообменов между всеми абонентами сети. В общем виде матрица C размерности M, где M число УК, должна формироваться из матрицы A гораздо большей размерности (например, по общему числу абонентов N), элементы A_{pq} которой определяют поток от одного абонента (p) к другому абоненту (q).

Для данного проекта такие скрупулезные подсчеты не имеют смысла, поэтому ниже определен не безупречный, но зато упрощенный алгоритм распределения потоков между узлами коммутации ВС. Прежде всего необходимо временно расширить матрицу C на один элемент, путем добавления к квадратной матрице размерности 5 (т.к. в сети имеется 5 УК) шестой строки и шестого столбца, соответствующих такому мощному источнику и потребителю информационных потоков, как узел доступа к Internet (УД I). В дальнейшем, после того как элементы матрицы $C^{(6)}$ полностью определятся, необходимо будет вернуться к матрице $C^{(5)}$ путем объединения шестого столбца со столбцом r и шестой строки со строкой r, где r – номер УК, с которым совмещен УД I .

Сформируем для примера первую строку матрицы $C^{(6)}$ по данным табл. 6 (без запаса на расширение услуг). Асимметричность трафика УК1 ($^{51,2}\!/_{64}$)

связана как раз с тем, что поток в направлении от УК1 к УД I меньше обратного потока от УД I к УК1.

Примем следующее распределение исходящего из любого УК потока: 20% к УД I (т.е. к Internet), 20% направить абонентам своей ИМР (т.е. внутриузловой поток). Остальной поток распределить между оставшимися четырьмя УК поровну. Произведя необходимые расчеты, распределим поток $C_{1исх}$=51,2 Мбит/с и получим первую строку матрицы $C^{(6)}$ в следующем виде (Мбит/с):

$$C_{11}=10{,}24;\ C_{12}=7{,}7;\ C_{13}=7{,}7;\ C_{14}=7{,}7;\ C_{15}=7{,}7;\ C_{16}=10{,}24$$

Рассчитав аналогично еще 4 строки, соответствующие узлам УК2, УК3, УК4 и УК5, завершим формирование матрицы $C^{(6)}$ добавлением шестой строки. Элемент C_{61} формируется как разница между суммарным входящим в ИМР1 потоком (по

табл. 6 это 64 Мбит/с) и суммой уже определенных элементов первого столбца матрицы $C^{(6)}$, т.е. $C_{61} = C_{1BX} - \sum_{i=1}^{5} C_{i1}$

(Наиболее способные студенты, конечно, догадаются, что такое упрощение содержит определённую некорректность, но мы не будем отвлекаться от основной цели настоящего проекта).

Элемент C_{66} логично принять равным нулю, т.к. его ненулевое значение означало бы, что Глобальная сеть Internet использует узел доступа нашей МСС в качестве транзитного для своих потоков.

Таким образом, нами получена матрица тяготений $C^{(6)}$, элементы которой C_{ms} определяют суммарный мультимедийный поток (Мбит/с) от абонентов ИМРm (или, что то же самое – от УКm, от МВВm) к абонентам ИМРs (к УКs, к МВВs). При этом элемент C_{m6} определяет исходящий поток от ИМРm (УКm, МВВm) к узлу доступа в Internet (УД I), а элемент C_{6l} – входящий поток из УД I в ИМРs (УКs, МВВs).

Результаты расчета матрицы тяготений используются при определении требуемой канальной скорости в первичной сети.

Определение требуемой полосы по участкам первичной сети

Первичная сеть (ПС) в данном проекте представляет собой оптоволоконную сеть кольцевой структуры на базе технологии SDH. Это городская опорная сеть, предоставляющая услуги в виде определенной полосы пропускания (ПП) любым пользователям на основе долговременной аренды (принцип выделенного канала). Реализованная в настоящий момент (в данном проекте) скорость по одному волокну составляет 622 Мбит/с (стандартный транспортный модуль – STM-4).

Всего задействовано 4 волокна по 2 в каждом направлении, из которых один основной и один резервный (система резервирования 1:1, время переключения на резерв до 50 мс). Остальные волокна кабеля (так называемые «темные волокна») находятся в резерве на случай расширения пропускной способности сети или повреждения рабочих волокон.

На оптоволоконном кольце расположены 5 мультиплексоров ввода/вывода (МВВ или Add/Drop Multiplexer – ADM), с которыми совмещены 5 узлов коммутации вторичной сети, т.е. по одной паре УК – МВВ в каждом ИМР. На самом деле

SDH-кольцо может содержать больше МВВ, но для проектируемой мультисервисной сети эти МВВ прозрачны и могут не рассматриваться.

В процессе проектирования ПС в настоящем проекте необходимо решить 2 вопроса:

а). Рассчитать требуемую ПП для каждого из арендованных участков SDH-кольца.

б). Выбрать по данным Приложения 3 подходящий МВВ и описать его магистральные и пользовательские интерфейсы.

Основой для такого расчета может служить полученная в разделе 6 матрица тяготений $C^{(6)}$, 30 элементов которой (по формуле $n \cdot (n-1)$, где $n=6$) определяют все межузловые потоки. Однако, в данном случае эта матрица избыточна, т.к. при условии совмещения УД I с одним из УК, число реальных

узлов как в первичной, так и во вторичной сетях сокращается до 5 и следовательно, преобразовав матрицу $C^{(6)}$ в $C^{(5)}$, мы сократим число потоков до 20 (все по той же формуле n·(n-1), где теперь уже n=5).

Порядок преобразования $C^{(6)}$ в $C^{(5)}$ следующий:

- обнулить главную диагональ, т.е. принять $C_{mm}=0$ для всех $m=\overline{1,6}$. Значения C_{mm} определяют потоки между абонентами одного ИМР, а наша задача на данном этапе состоит в определении только межузловых потоков;

- выбрать один из УК (например $УК_2$) в качестве узла, совмещенного с УД I;

- прибавить к элементам второй строки элементы шестой строки и ликвидировать шестую строку. Теперь, например, элемент $C_{21}^{(5)}=C_{21}^{(6)}+C_{61}^{(6)}$ будет содержать сумму потоков от $УК_1$ к $УК_2$ и от $УК_1$ к УД I;

- прибавить к элементам второго столбца элементы шестого столбца и ликвидировать шестой столбец. Теперь элемент $C_{12}^{(5)}=C_{12}^{(6)}+C_{16}^{(6)}$ будет содержать сумму потоков от $УК_2$ к $УК_1$ и от УД I к $УК_1$;

- обнулить элемент C_{22}, т.к. теперь он содержит сумму входящего и исходящего потоков между совмещёнными УД I и $УК_2$ и никак не влияет на межузловые потоки.

Полученная таким образом матрица тяготений $C^{(5)}$ определяет рассчитанные значения мультимедийных потоков между всеми парами УК (и сопряженных с ними

МВВ). Однако, непосредственно использовать эти значения для аренды каналов первичной сети нельзя по следующей причине. Все входы в МВВ стандартизированы и ориентированы на две группы канальных скоростей:

- трибные порты плезиохронной цифровой иерархии (PDH): E1 (2,048 Мбит/с), E2 (8,45 Мбит/с), E3(34,368 Мбит/с) и E4 (139 Мбит/с);

- трибные порты синхронной цифровой иерархии (SDH): STM–1 (155,52 Мбит/с), STM–4 (622,08 Мбит/с), STM–16 (2488,3 Мбит/с) и т.д. в строгом учетверении канальных скоростей.

Поэтому, полученную выше матрицу $C^{(5)}$ необходимо преобразовать в некоторую матрицу стандартных скоростей Q, увеличив все значения $C_{ms}^{(5)}$ до ближайшей стандартной скорости $q_{ms}^{(5)}$ из ряда скоростей PDH или SDH.

При выборе стандартных скоростей не следует делать существенные запасы на перспективное увеличение трафика, т.к. речь идет не о покупке оборудования, а только об аренде канала, а договор об аренде, как правило, легко пересматривается.

Обратите внимание и на тот факт, что скорость E2 в настоящее время не пользуется популярностью у производителей оборудования и могут возникнуть затруднения при выборе конкретного МВВ. Матрица стандартных скоростей межузловых потоков Q, в которой элемент q_{ms} определяет требуемую канальную скорость от MBBm к MBBs, уже может служить основой для заключения договора об аренде ПП между провайдером вторичной сети и оператором первичной сети.

Однако необходимо проверить реализуемость данного проекта с точки зрения достаточности пропускной способности сети SDH с STM–4.

Решить эту задачу в полной мере может только оператор первичной сети, которому известны все арендаторы полос, но произвести предварительную оценку и убедиться, что потребности нашей МСС не выходят за рамки возможностей STM-4 мы можем.

Для определения суммарной ПП для 10 участков кольца (в каждом участке рассматриваются волокна по и против часовой стрелки) достаточно занести значения матрицы Q в табл. 7 в процессе просмотра всех 20 межузловых потоков. В пятиузловой сети все потоки будут содержать один или два участка первичной сети. В табл. 7 показан пример построения для первых 5-ти потоков.

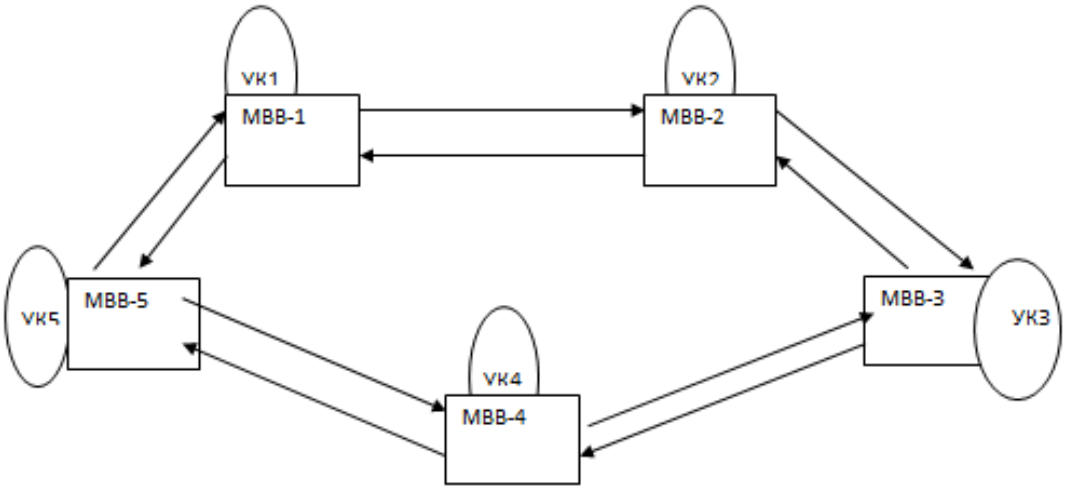


Рисунок 5 - Схема потоков первичной сети

Таблица 7 - Распределение стандартизированных потоков вторичной сети по участкам первичной сети

Прямые каналы ВС	Участки первичной сети									
	1 – 2	2 – 1	2 – 3	3 – 2	3 – 4	4 – 3	4 – 5	5 - 4	5 – 1	1 – 5
$УК_1 \rightarrow УК_2$	q_{12}									
$УК_1 \rightarrow УК_3$	q_{13}		q_{13}							
$УК_1 \rightarrow УК_4$								q_{14}		q_{14}
$УК_1 \rightarrow УК_5$										q_{15}
$УК_2 \rightarrow УК_1$		q_{21}								
и т.д.										
Общая ПП										

Правильность построения табл. 7 можно проверить по числу значений q_{ij} в каждом столбце. Их должно быть три. Например: $ПП_{1\text{-}2}=q_{12}+q_{13}+q_{52}$. А в каждой строке табл. 7 должно быть либо одно значение q_{ij} (для смежных УК), либо два. Расчеты ПП в разделах 4 и 6 для каналов доступа и каналов вторичной сети (между двумя УК), из-за статистического уплотнения пакетного трафика в них оказались достаточно сложными. В отличие от этого в трактах первичной сети отдельные канальные полосы являются независимыми и общую ПП можно определить простым суммированием составляющих полос.

Результаты такого суммирования составляют последнюю строку табл. 7.

Если на каком-нибудь участке SDH-кольца суммарный трафик превышает 70% от номинальной скорости (в нашем случае от 622 Мбит/с), то с учетом устойчивой тенденции к экспоненциальному росту трафика, оператор первичной сети должен принимать срочные меры к повышению пропускной способности SDH-кольца либо путем замены МВВ с STM–4 на МВВ с STM–16 (т.е. переход на скорость 2,5 Гбит/с), либо добавлением новых ОВ колец за счет использования «темных волокон», либо, наконец, использованием технологий грубого спектрального мультиплексирования (CWDM) или плотного спектрального мультиплексирования (DWDM).

Контрольные вопросы:

1. Какие виды трафика учитываются при расчёте сети и в чём их особенность?
2. Что понимается под первичной сетью?
3. Что понимается по вторичной сетью?
4. Поясните состав обобщённой структуры мультисервисной сети.
5. Что понимается под удельной интенсивностью нагрузки в ЧНН.
6. Как вы понимает понятие час наивысшей нагрузки ЧНН и почему производится расчёт в расчёте именно на такие значения?
7. Что понимается под коэффициентом приведения к полосе пропускания?
8. Поясните параметры аудио потока.
9. Поясните параметры видео трафика.
10. Поясните параметры трафика данных.
11. Поясните алгоритм построения расчётной таблицы.
12. Что понимается под условной единицей потока и зачем она нужна?
13. В чём заключается суть расчёта вторичной сети?
14. Поясните особенности выбора оборудования.
15. Какие параметры сети необходимо знать, для выбора оборудования?

Список источников:

1. Савостинский Ю.А. Метод определения требуемой полосы магистрали для пропуска мультимедийного трафика. Электросвязь. 2003 - №3.

2. Лагутин В.С., Костров В.О. Оценка характеристик пропускной способности мультисервисных пакетных сетей при реализации технологии разделения типов нагрузки. Электросвязь. 2003 - №3.

3. Олифер В.Г., Олифер Н.А. Компьютерные сети. СПб.: Питер. 2001.

4. Шмалько А.В. Цифровые сети связи. М.: Эко-Трендз. 2001.

5. Олифер В.Г. и др. ATM и MPLS – враги или союзники? Журнал сетевых решений. LAN. Декабрь 2002.

Практическое занятие №4. Изучение работы маршрутизатора с использованием Cisco Packet Tracer .

Цель занятия. Изучить правила составления статического маршрута и принципы динамической маршрутизации. Получить наыки конфигурирования оборудования при настройке маршрутизаторов и коммутаторов третьего уровня.

Задание. Построить сет на базе маршрутизаторов. Определить адресацию в сети. Рассмотреть процесс формирования таблиц маршрутизации. Произвести настройку статического конфигурирования. Произвести настройку протокола RIP. Произвести настройку протокола OSPF.

1 Статическая маршрутизация

Протоколы маршрутизации - это правила, по которым осуществляется обмен информации о путях передачи пакетов между маршрутизаторами. Протоколы характеризуются временем сходимости, потерями и масштабируемостью. В настоящее время используется несколько протоколов маршрутизации.

Одна из главных задач маршрутизатора состоит в определении наилучшего пути к заданному адресату. Маршрутизатор определяет пути (маршруты) к адресатам или из статической конфигурации, введённой администратором, или динамически на основании маршрутной информации,

полученной от других маршрутизаторов. Маршрутизаторы обмениваются маршрутной информацией с помощью протоколов маршрутизации.

Маршрутизатор хранит таблицы маршрутов в оперативной памяти. Таблица маршрутов это список наилучших известных доступных маршрутов. Маршрутизатор использует эту таблицу для принятия решения куда направлять пакет.

В случае статической маршрутизации администратор вручную определяет маршруты к сетям назначения.

В случае динамической маршрутизации – маршрутизаторы следуют правилам, определяемым протоколами маршрутизации для обмена информацией о маршрутах и выбора лучшего пути.

Статические маршруты не меняются самим маршрутизатором. Динамические маршруты изменяются самим маршрутизатором автоматически при получении информации о смене маршрутов от соседних маршрутизаторов. Статическая маршрутизация потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Создайте схему сети, представленную на рисунке 1.

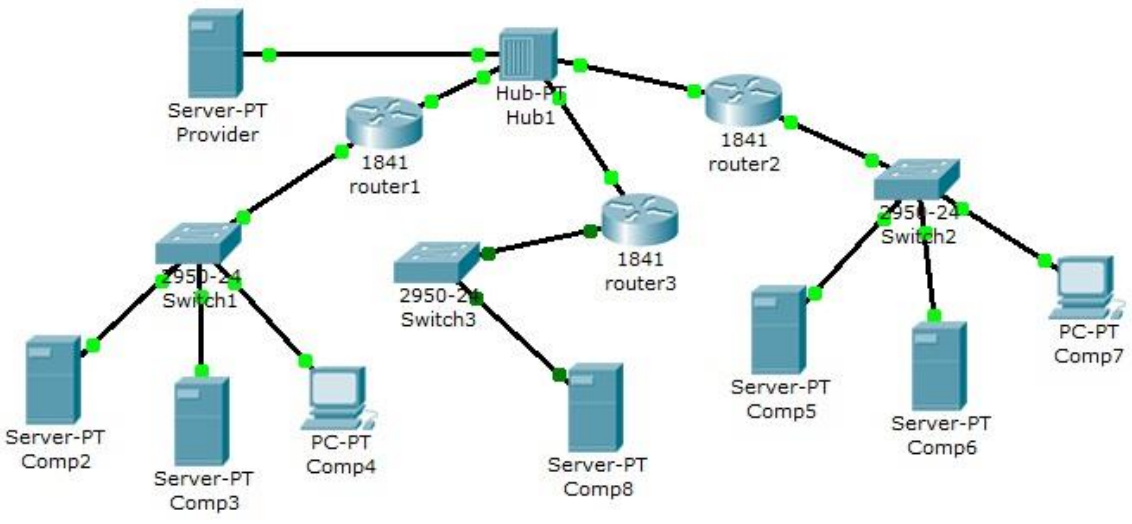


Рисунок 1 - Схема сети

Проведем настройку статической маршрутизации с помощью графических мастеров интерфейса Cisco Packet Tracer.

На данной схеме представлена корпоративная сеть, состоящая из следующих компонентов:

Сеть 1 – на Switch1 замыкается сеть первой организации (таблица 1):

Таблица 1 - Сеть первой организации

Компьютер	IP адрес	Функции
Comp2	192.168.1.2/24	DNS и HTTP сервер
Comp3	192.168.1.3/24	DHCP сервер
Comp4	Получен с DHCP сервера	Клиент сети

В данной сети на Comp2 установлен DNS и Web сервер с сайтом организации.

На Comp3 установлен DHCP сервер. Компьютер Comp4 получает с DHCP сервера IP адрес, адрес DNS сервера провайдера (сервер Provider) и шлюз. Шлюз в сети – 192.168.1.1/24.

Сеть 2 – на Switch2 замыкается сеть второй организации (таблица 2):

Таблица 2 - Сеть второй организации

компьютер	IP адрес	Функции
Comp5	10.0.0.5/8	DNS и HTTP сервер
Comp6	10.0.0.6/8	DHCP сервер
Comp7	Получен с DHCP сервера	Клиент сети

В данной сети на Comp5 установлен DNS и Web сервер с сайтом организации. На Comp4 установлен DHCP сервер. Компьютер Comp7 получает с DHCP сервера IP адрес, адрес DNS сервера провайдера (сервер Provider) и шлюз. Шлюз в сети – 10.0.0.1/8.

Сеть 3 – на Hub1 замыкается городская сеть 200.200.200.0/24. В сети установлен DNS сервер провайдера (комьютер Provaider с IP адресом - 200.200.200.10/24), содержащий данные по всем сайтам сети (Comp2, Comp5, Comp8). Сеть 4 – маршрутизатор Router3 выводит городскую сеть в интернет через коммутатор Switch3 (сеть 210.210.210.0/24). На Comp8 (IP адрес

210.210.210.8/24, шлюз 210.210.210.3/24.) установлен DNS и Web сервер с сайтом.

Маршрутизаторы имеют по два интерфейса:

Router1 – 192.168.1.1/24 и 200.200.200.1/24.

Router2 – 10.0.0.1/8 и 200.200.200.2/24.

Router3 – 210.210.210.3/24 и 200.200.200.3/24.

Задача:

1 – настроить сети организаций;

2 – настроить DNS сервер провайдера;

3 – настроить статические таблицы маршрутизации на роутерах;

4 – проверить работу сети – на каждом из компьютеров - Comp4, Comp7 и Comp8. С каждого из них должны открываться все три сайта корпоративной сети.

В предыдущих лабораторных работах рассматривалась настройка сетевых служб и DNS сервера. Приступим к настройке статической маршрутизации на роутерах. Поскольку на представленной схеме четыре сети, то таблицы маршрутизации как минимум должны содержать записи к каждой из этих сетей – т.е. четыре записи. На роутерах Cisco в таблицах маршрутизации как правило не прописываются пути к сетям, к которым подсоединены интерфейсы роутера. Поэтому на каждом роутере необходимо внести по две записи.

Настройте первый роутер.

Для этого войдите в конфигурацию маршрутизатора и в интерфейсах установите IP адрес и маску подсети. Затем в разделе МАРШРУТИЗАЦИЯ откройте вкладку СТАТИЧЕСКАЯ, внесите данные (рис.2) и нажмите кнопку ДОБАВИТЬ:

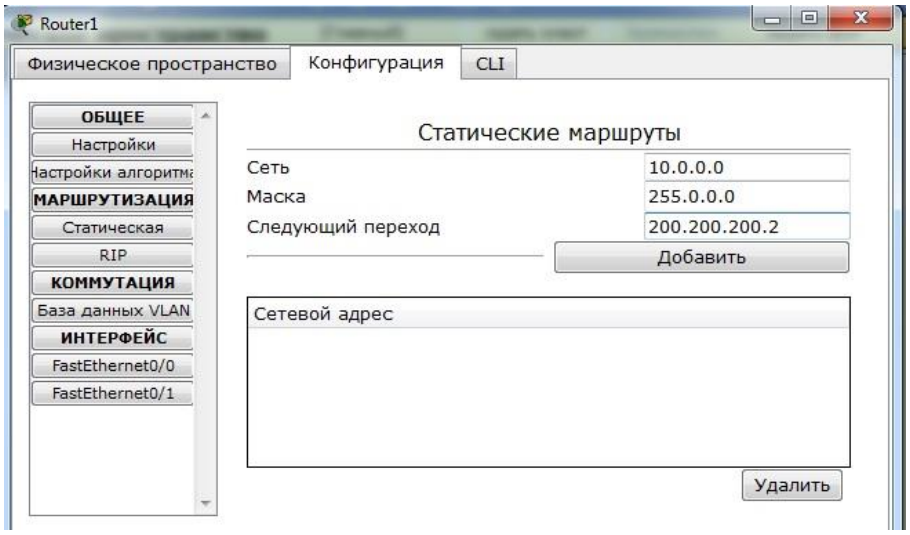


Рисунок 2 - Данные для сети 10.0.0.0/8

В результате у вас должны появиться две записи в таблице маршрутизации (рис.3):

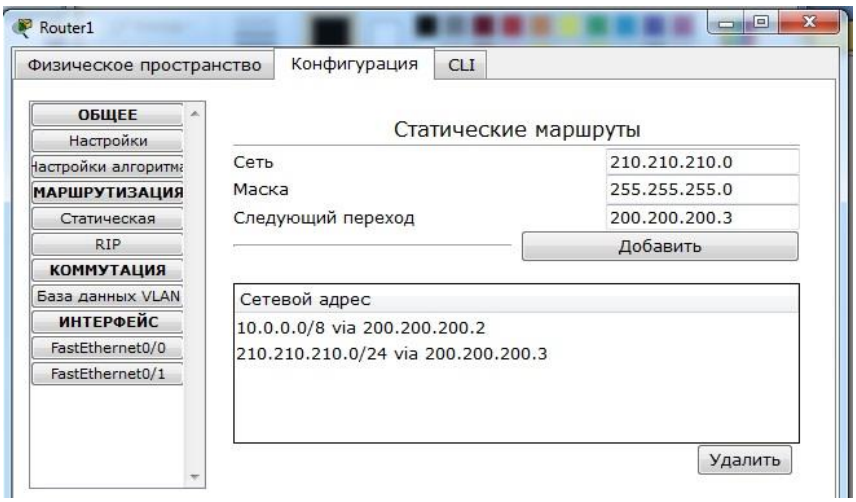


Рисунок 3 - Формирование статической таблицы маршрутизации

Чтобы посмотреть полную настройку таблицы маршрутизации, выберите в боковом графическом меню инструмент ПРОВЕРКА (пиктограмма лупы), щелкните в схеме на роутере и выберите в раскрывающемся меню пункт ТАБЛИЦА МАРШРУТИЗАЦИИ.

После настройки всех роутеров в вашей сети станут доступны IP адреса любого компьютера и вы сможете открыть любой сайт с компьютеров Comp4, Comp7 и Comp8.

Построение таблиц маршрутизации.

Выполните самостоятельно следующую работу, схема сети для которой представлена на рис.4.

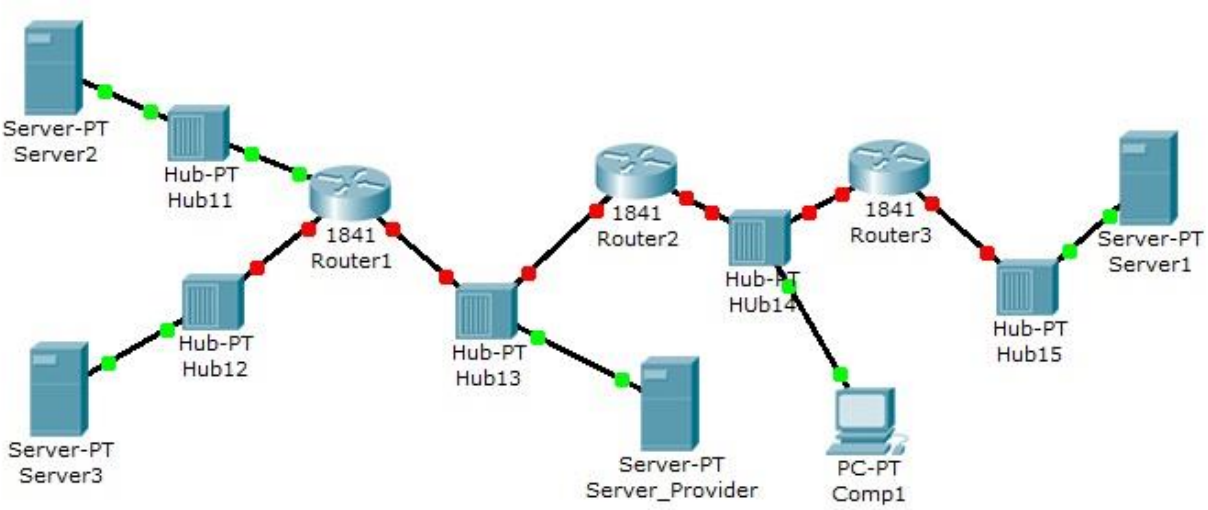


Рисунок 4 - Схема сети

Пять концентраторов представляют следующие пять сетей:

Hub11 – сеть 11.0.0.0

Hub12 – сеть 12.0.0.0

Hub13 – сеть 13.0.0.0

Hub14 – сеть 14.0.0.0

Hub15 – сеть 15.0.0.0

Router 1 имеет дополнительный сетевой интерфейс, который добавляется из модуля WIC-1ENET при выключенном роутере.

В сети три Web узла на Server1, Server2 и Server3.

Сервера и компьютер имеют произвольные IP адреса со шлюзами своих роутеров.

Интерфейсы роутеров определяются сетью на концентраторе и номером роутера.

Например для Router3: 15.0.0.3 и 14.0.0.3

Задание:

компьютер Comp1 должен открыть все три сайта на серверах корпоративной сети. В настройках Comp1 в качестве DNS сервера указан DNS сервер провайдера на Server_Provider.

2. Динамическая маршрутизация

Статическая маршрутизация не подходит для больших, сложных сетей потому, что обычно сети включают избыточные связи, многие протоколы и смешанные топологии.

Маршрутизаторы в сложных сетях должны быстро адаптироваться к изменениям топологии и выбирать лучший маршрут из многих кандидатов.

IP сети имеют иерархическую структуру. С точки зрения маршрутизации сеть

рассматривается как совокупность автономных систем. В автономных подсистемах больших сетей для маршрутизации на остальные автономные системы широко используются маршруты по умолчанию.

Динамическая маршрутизация может быть осуществлена с использованием одного и более протоколов. Эти протоколы часто группируются согласно того, где они используются. Протоколы для работы внутри автономных систем называют внутренними протоколами шлюзов (interior gateway protocols (IGP)), а протоколы для работы между автономными системами называют внешними протоколами шлюзов (exterior gateway protocols (EGP)). К протоколам IGP относятся RIP, RIP v2, IGRP, EIGRP, OSPF и IS-IS. Протоколы EGP3 и BGP4 относятся к EGP. Все эти протоколы могут быть разделены на два класса: дистанционно-векторные протоколы и протоколы состояния связи.

Дистанционно-векторная маршрутизация.

Маршрутизаторы используют метрики для оценки или измерения маршрутов. Когда от маршрутизатора к сети назначения существует много маршрутов, и все они используют один протокол маршрутизации, то маршрут с наименьшей метрикой рассматривается как лучший. Если используются разные протоколы маршрутизации, то для выбора маршрута используется административные расстояния, которые назначаются маршрутам операционной системой маршрутизатора. RIP использует в качестве метрики количество переходов (хопов).

Дистанционно-векторная маршрутизация базируется на алгоритме Белмана-Форда. Через определённые моменты времени маршрутизатор передаёт соседним маршрутизаторам всю свою таблицу маршрутизации. Такие простые протоколы как RIP и IGRP просто распространяют информацию о таблицах маршрутов через все интерфейсы маршрутизатора в широковещательном режиме без уточнения точного адреса конкретного соседнего маршрутизатора.

Соседний маршрутизатор, получая широковещание, сравнивает информацию со своей текущей таблицей маршрутов. В неё добавляются маршруты к новым сетям или маршруты к известным сетям с лучшей метрикой. Происходит удаление несуществующих маршрутов. Маршрутизатор добавляет свои собственные значения к метрикам полученных маршрутов. Новая таблица маршрутизации снова распространяется по соседним маршрутизаторам

Настройка протокола RIP.

Создайте схему, представленную на рис.6.1.

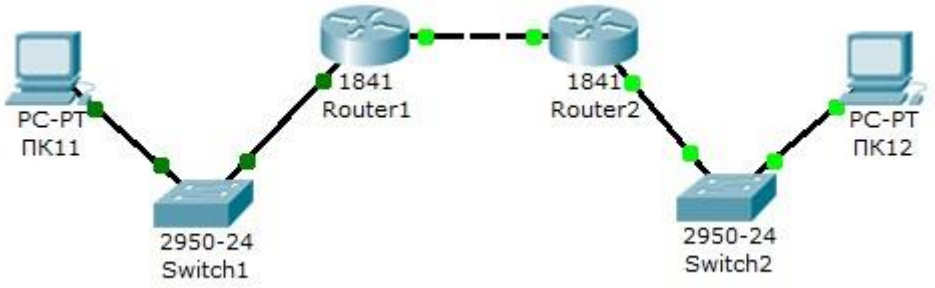


Рисунок 5 - Схема сети

На схеме представлены следующие три сети:

Switch1 – сеть 10.11.0.0/16.

Switch2 – сеть 10.12.0.0/16.

Сеть для роутеров - 10.10.0.0/16.

Введите на устройствах следующую адресацию:

Маршрутизаторы имеют по два интерфейса:

Router1 – 10.11.0.1/16 и 10.10.0.1/16.

Router2 – 10.10.0.2/16 и 10.12.0.1/16.

ПК11 - 10.11.0.11/16 .

ПК12 - 10.12.0.12/16 .

Проведем настройку протокола RIP на маршрутизаторе Router1.

Войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса роутера):

Войдите в привилегированный режим:

Router1>**en**

Войдите в режим конфигурации:

Router1>#**conf t**

Войдите в режим конфигурирования протокола RIP:

Router1(config)#**router rip**

Подключите клиентскую сеть к роутеру:

Router1(config-router)#**network 10.11.0.0**

Подключите вторую сеть к роутеру:

Router1(config-router)#**network 10.10.0.0**

Задайте использование второй версии протокол RIP:

Router1(config-router)#**version 2**

Выйдите из режима конфигурирования протокола RIP:

Router1(config-router)#**exit**

Выйдите из консоли настроек:

Router1(config)#**exit**

Сохраните настройки в память маршрутизатора:

Router1>#**write memory**

Аналогично проведите настройку протокола RIP на маршрутизаторе Router2.

Проверьте связь между компьютерами ПК11 и ПК12 командой **ping**.

Если связь есть – все настройки сделаны верно.

Настройка протокола RIP в корпоративной сети.

Создайте схему, представленную на рис.6.

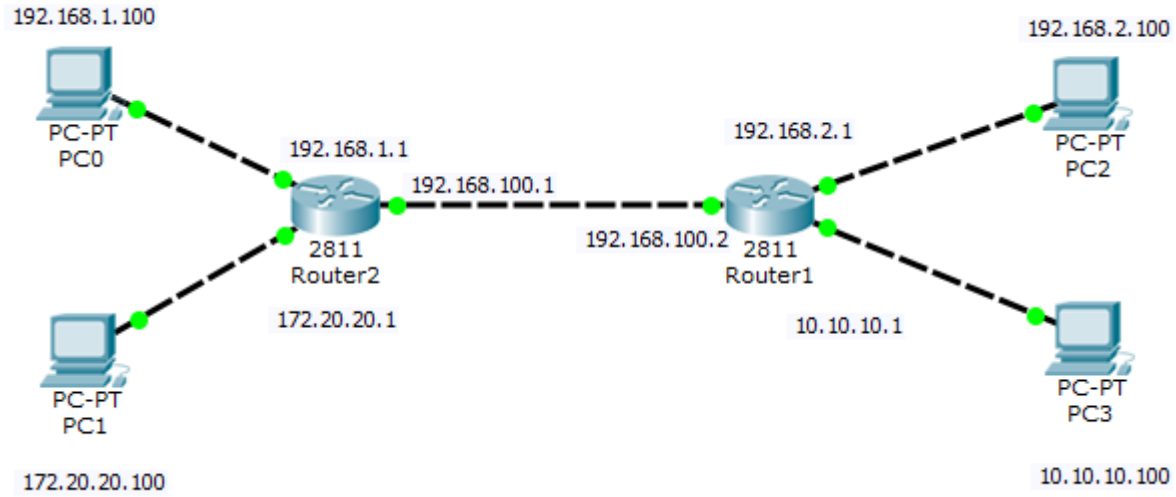


Рисунок 6

Настройте маршрутизацию по протоколу RIP на каждом из роутеров.

Для этого:

1 - настройте все маршрутизаторы, как это было показано в лабораторной работе №6;

2 – проверьте настройку маршрутизаторов по таблице маршрутизации.

Чтобы убедиться в том, что маршрутизатор действительно правильно скон-

фигурирован и работает корректно, просмотрите таблицу RIP роутера, используя команду show следующим образом:

Router#**show ip route rip**

Данная таблица показывает, что к сети 21.0.0.0 есть два пути: через Router4 (сеть 81.0.0.0) и через Router3 (сеть 61.0.0.0).

Проведите диагностику сети:

1 – проверьте правильность настройки с помощью команд **ping** и **tracert** в консоли кождого компьютера;

2 – проведите ту же диагностику сети при выключенном маршрутизаторе Router6.

3 - проверьте связь между компьютерами с адресами 12.0.0.12 и 13.0.0.13.

Количество промежуточных роутеров при прохождении пакета по сети при включенном и выключенном роутере 6 должно быть разным. При включенном Router6 должно быть на единицу меньше, чем при выключенном.

Протоколы состояния связи.

Эти протоколы предлагают лучшую масштабируемость и сходимость по сравнению с дистанционно-векторными протоколами. Работа протоколов базируется на алгоритме Дейкстры, который часто называют алгоритмом «кратчайший путь – первым» (shortest path first SPF)). Наиболее типичным представителем является протокол OSPF (Open Shortest Path First).

Маршрутизатор берёт в рассмотрение состояние связи интерфейсов других маршрутизаторов в сети. Маршрутизатор строит полную базу данных всех состояний связи в своей области, то есть имеет достаточно информации для создания своего отображения сети. Каждый маршрутизатор затем самостоятельно выполняет SPF-алгоритм на своём собственном отображении сети или базе данных состояний связи для определения лучшего пути, который заносится в таблицу маршрутов. Эти пути к другим сетям формируют дерево с вершиной в виде локального маршрутизатора.

Маршрутизаторы извещают о состоянии своих связей всем маршрутизаторам в области. Такое извещение называют LSA (link-state advertisements).

В отличие от дистанционно-векторных маршрутизаторов, маршрутизаторы состояния связи могут формировать специальные отношения со своими соседями.

Имеет место начальный наплыв LSA пакетов для построения базы данных состояний связи. Далее обновление маршрутов производится только при смене состояний связи или, если состояние не изменилось в течение определённого интервала времени. Если состояние связи изменилось, то частичное обновление пересылается немедленно. Оно содержит только состояния связей, которые изменились, а не всю таблицу маршрутов.

Администратор, заботящийся об использовании линий связи, находит эти частичные и редкие обновления эффективной альтернативой дистанционно-векторной маршрутизации, которая передаёт всю таблицу маршрутов через регулярные промежутки времени. Протоколы состояния связи имеют более быструю сходимость и лучшее использование полосы пропускания по сравнению с дистанционно-векторными протоколами. Они превосходят дистанционно-векторные протоколы для сетей любых размеров, однако имеют два главных недостатка: повышенные требования к вычислительной мощности маршрутизаторов и сложное администрирование.

Настройка протокола OSPF.

Возьмите схему сети, представленную на рис 6.

Проведем настройку протокола OSPF на маршрутизаторе Router1.

Войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса роутера):

Войдите в привилегированный режим:

Switch>**en**

Войдите в режим конфигурации:

Switch1#**conf t**

Войдите в режим конфигурирования протокола OSPF:

Router1(config)#**router ospf 1**

В команде router ospf <идентификатор_процесса> под идентификатором процесса понимается уникальное числовое значение для каждого процесса роутинга на маршрутизаторе. Данное значение должно быть больше в интервале от 1 до 65535. В OSPF процессам на роутерах одной зоны принято присваивать один и тот же идентификатор.

Подключите клиентскую сеть к роутеру:

Router1(config-router)#**network 10.11.0.0**

Подключите вторую сеть к роутеру:

Router1(config-router)#**network 10.10.0.0**

Задайте использование второй версии протокол OSPF:

Router1(config-router)#**version 2**

Выйдите из режима конфигурирования протокола OSPF:

Router1(config-router)#**exit**

Выйдите из консоли настроек:

Router1(config)#**exit**

Сохраните настройки в память маршрутизатора:

Switch1#**write memory**

Аналогично проведите настройку протокола OSPF на маршрутизаторе Router2.

Контрольные вопросы:

1. Пояснить принцип работы маршрутизатора.

2. В чем преимущества статической маршрутизации?

3. Дайте характеристику параметрам статической таблицы маршрутизации?

4. Какую из указанных ниже команд можно встретить в интерфейсе командной строки маршрутизатора, но не коммутатора?

- команда cloc rate;

- команда ip address маска адрес;

- команда ip address dhcp;

- команда interface vlan 1

5. Чем отличаются интерфейсы командной строки маршрутизатора и коммутатора компании Cisco?

6. Какая из указанных ниже команд не покажет настройки IP-адресов и масок в устройстве?

- show running-config;

- show protocol тип номер;

- show ip interface brief;

- Show version.

7. Перечислите основные функции маршрутизатора в соответствии с уровнями модели OSI.

8. Приведите классификацию маршрутизаторов по областям применения.

9. Перечислите основные технические характеристики маршрутизаторов.

10. Приведите перечень протоколов маршрутизации и дайте им краткие характеристики.

11. Приведите перечень поддерживаемых маршрутизаторами интерфейсов для локальных и глобальных сетей и определите их назначение.

12. В чем различие между топологической и дистанционно-векторной маршрутизацией?

13. Опишите схему работы протокола RIP.

14. Опишите схему работы протокола OSPF.

15. Перечислите основные этапы установки маршрутизатора.

16. Опишите четыре этапа загрузки маршрутизатора.

17. Какие из указанных ниже протоколов работают по дистанционно-векторному алгоритму и каковы их основные различия?

- RIP;
- IGRP;
- EIGRP;
- OSPF.

18. Дайте характеристику классам протоколов маршрутизации.

19. Приведите классификацию протоколов маршрутизации на основе алгоритмов их работы.

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 №5. Исследование возможностей работы протокола NAT на маршрутизаторе Cisco.

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 – Network Address Translation (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).

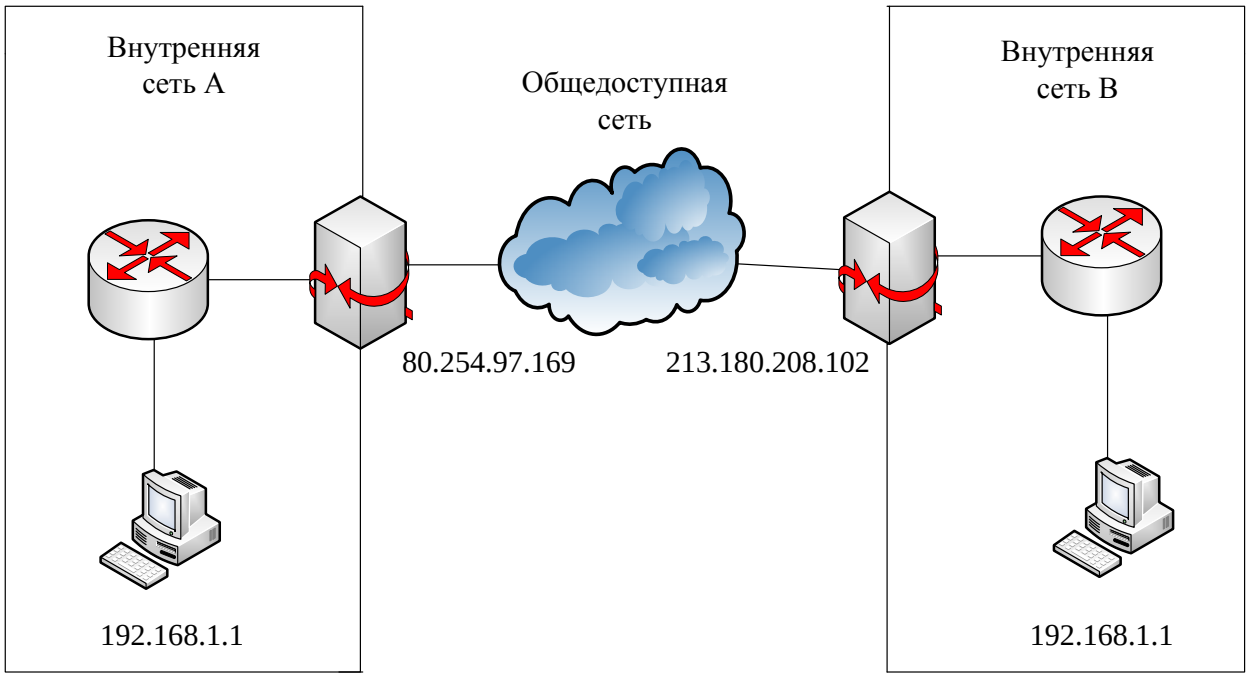


Рисунок 1 – Простейший случай использования NAT

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 В, 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.

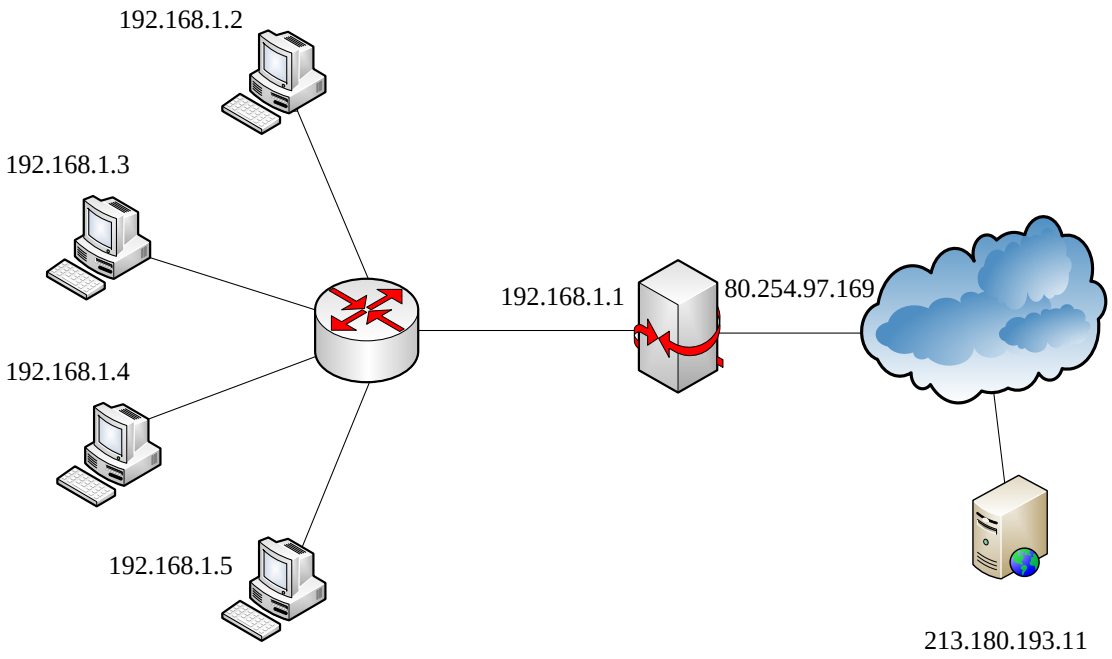


Рисунок 2 – Иллюстрация работы динамического NAT

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 статическом NAT. 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 (Network Address Port Translation) [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 Cisco Systems fa означает Fast Ethernet). 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 Source NAT (SNAT), то есть подмене подлежит IP-адрес источника (Source IP). Пакеты, прибывающие на внешний порт, подлежат трансляции в соответствии с Destination NAT (DNAT), то есть подмене подлежит IP-адрес получателя (Destination IP).

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 permit ip <адрес> <инвертированная маска> 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)# ip nat pool <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)# ip nat inside (outside).

Включается NAT командой

ip nat inside source list 100 pool <имя>.

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

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up

Router(config-if)#int fa 0/1
Router(config-if)#ip addr 80.254.97.169 255.0.0.0
Router(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o up

Router(config-if)#access-list 100 permit ip 192.168.1.1 0.255.255.255 any
Router(config)#ip nat pool primer 80.254.97.169 80.254.97.169 netmask 255.0.0.0
Router(config)#interface fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#interface fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source list 100 pool primer
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3 – Конфигурирование динамического NAT

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

```
o up

Router(config-if)#access-list 100 permit ip 192.168.1.1 0.255.255.255 any
Router(config)#ip nat pool primer 80.254.97.169 80.254.97.169 netmask 255.0.0.0
Router(config)#interface fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#interface fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source list 100 pool primer
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 80.254.97.169:25  192.168.1.5:25     80.254.97.168:25   80.254.97.168:25
icmp 80.254.97.169:26  192.168.1.5:26     80.254.97.168:26   80.254.97.168:26
icmp 80.254.97.169:27  192.168.1.5:27     80.254.97.168:27   80.254.97.168:27
icmp 80.254.97.169:28  192.168.1.5:28     80.254.97.168:28   80.254.97.168:28

Router#
```

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).

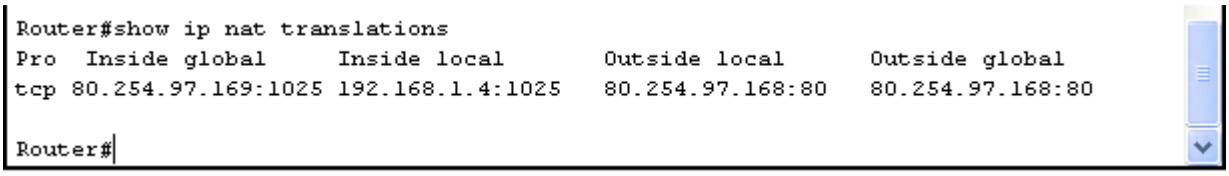


Рисунок 5 – Список трансляций после обращения к web-серверу

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 (Inside global) указывает на сокет (IP-адрес и номер порта), на который подменяется сокет отправителя.

Третья колонка (Inside local) указывает на внутренний IP-адрес отправителя с назначенным номером порта.

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

Пятая колонка (Outside global) 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 внешний www-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 №7. 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 (Access Control List) 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-list номер_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:

Стандартный список:

Switch3(config)#ip access-list standart 10

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

Расширенный список:

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 deny host 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 таблице 2:

Таблица 12.

Номер порта	Протокол	Приложение	Ключевое слово в команде access_list
20	TCP	FTP	data ftp_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 any eq 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

interface ethernetO

! Применить список доступа 111 к исходящему трафику

ip access-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

ip access-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# Sh access-list

Просмотр текущей конфигурации устройства и привязки списков к интерфейсам:

Router# Show running-config

Просмотр сохраненной конфигурации:

Router# Show configuration

Сохранение текущей конфигурации:

Router# write memory

Или

Router# copy run start

Команда удаления списка доступа:

interface ethernet0/0/0 - выбор нужного интерфейса

no access-list номер_списка – удаление списка в выбранном интерфейсе

Задание для работы

Создайте схему сети, как показано на рис.1.

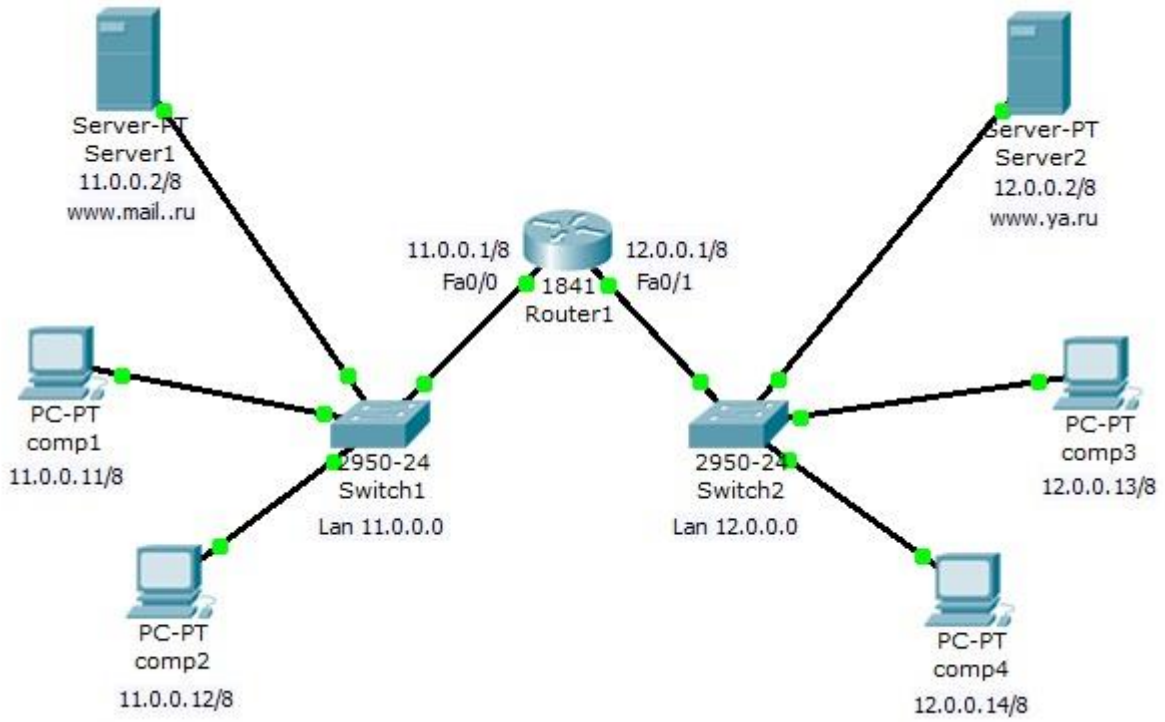


Рисунок 1 - Схема корпоративной сети

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#conf t

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 sh access-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#sh running-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
 duplex auto
 speed auto
!
```

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: Ip access-list 111 deny tcp any any eq 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: Permit any host 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 №8. Конфигурирование виртуальной локальной сети VLAN – максимум 6 баллов.

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.

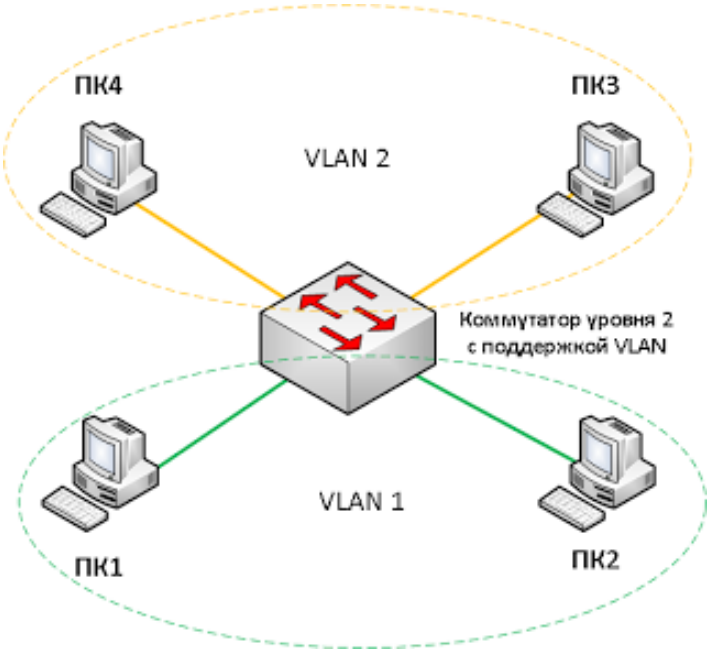


Рисунок 1 – Организация двух VLAN на одном коммутаторе

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 (Access Mode) и настройка порта в режиме магистрали (Trunk Mode).

Порты доступа применяются обычно для подключения оконечных устройств. В простейшем случае, порту доступа задается определенная VLAN, 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.

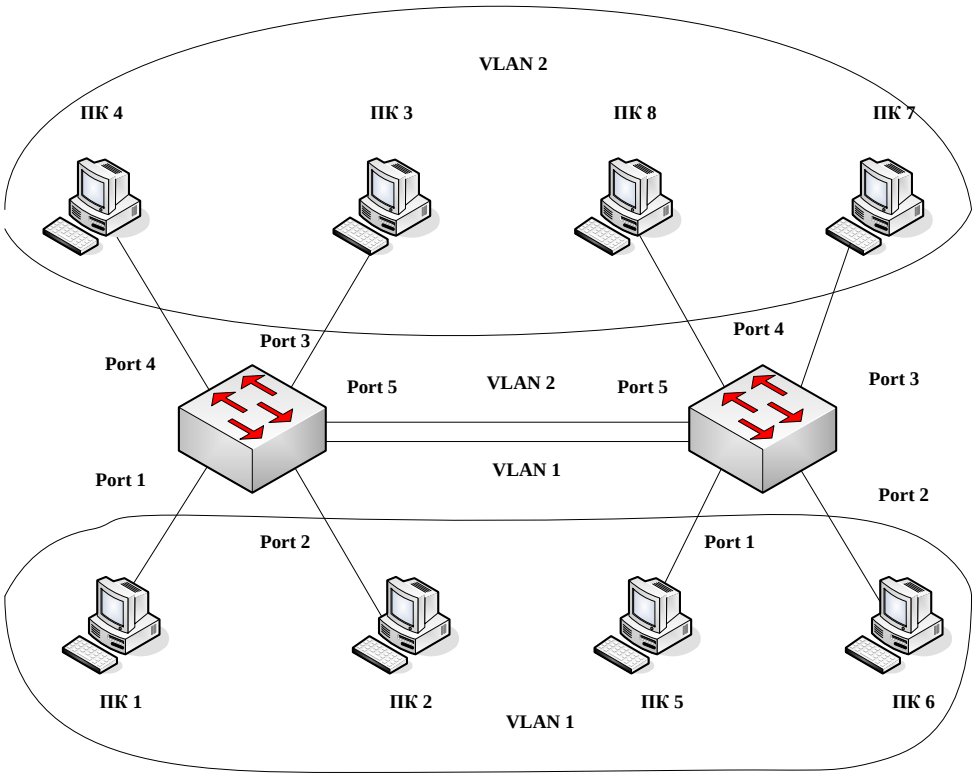


Рисунок 2 – Использование магистральных портов и портов доступа

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 show vlan brief (можно просто sh vl br).

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.

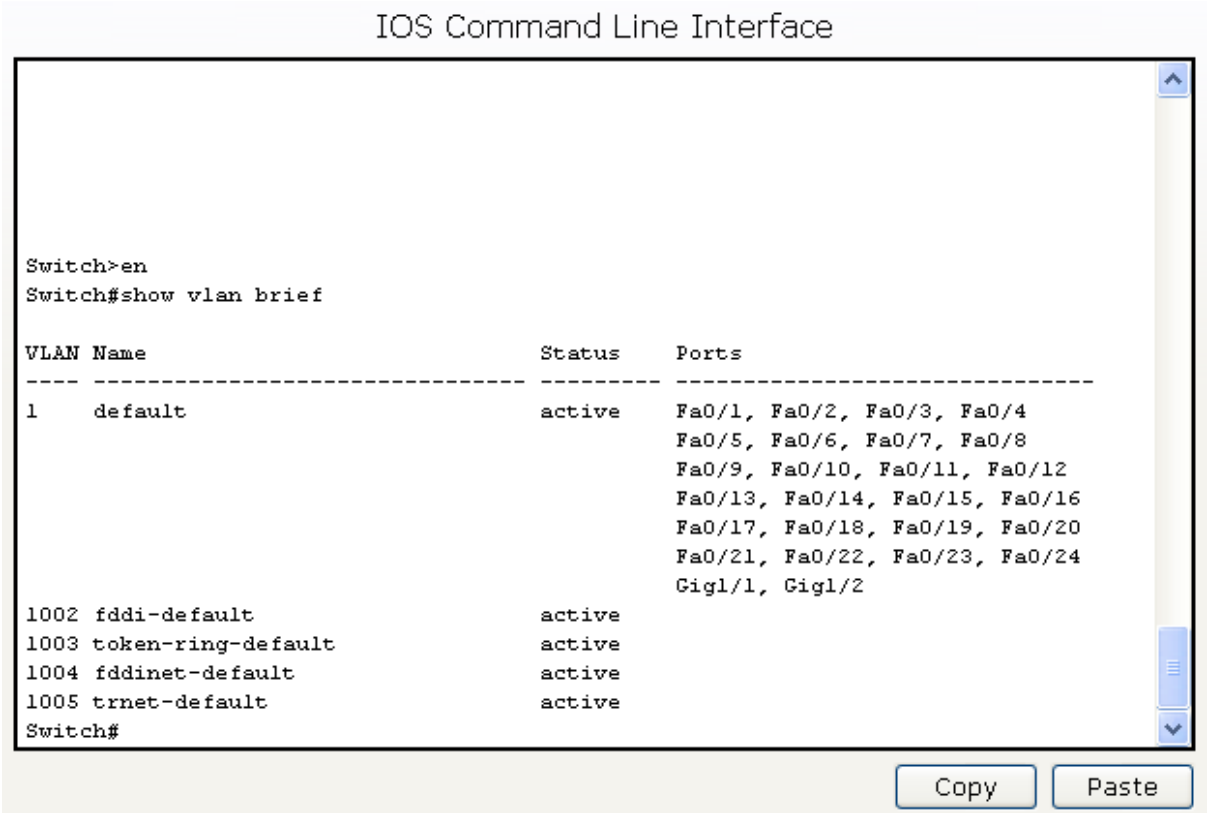


Рисунок 3 – Просмотр конфигурации VLAN

Для реализации сети, которую мы запланировали сделать, создадим на коммутаторе еще две VLAN. Для этого в привилегированном режиме необходимо выполнить команду conf t для перехода в режим глобального конфигурования. 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 отдельная VLAN, в данном случае номер 2. Если использовать команду «vlan x», где x номер VLAN, когда VLAN x 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 новую VLAN с номером 2. Команда name subnet_192 присваивает имя subnet_192 виртуальной сети номер 2. Выполняя команду interface range fastEthernet 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 switchport mode access конфигурирует выбранный порт коммутатора, как порт доступа. Команда switchport access VLAN 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 show vlan br 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.

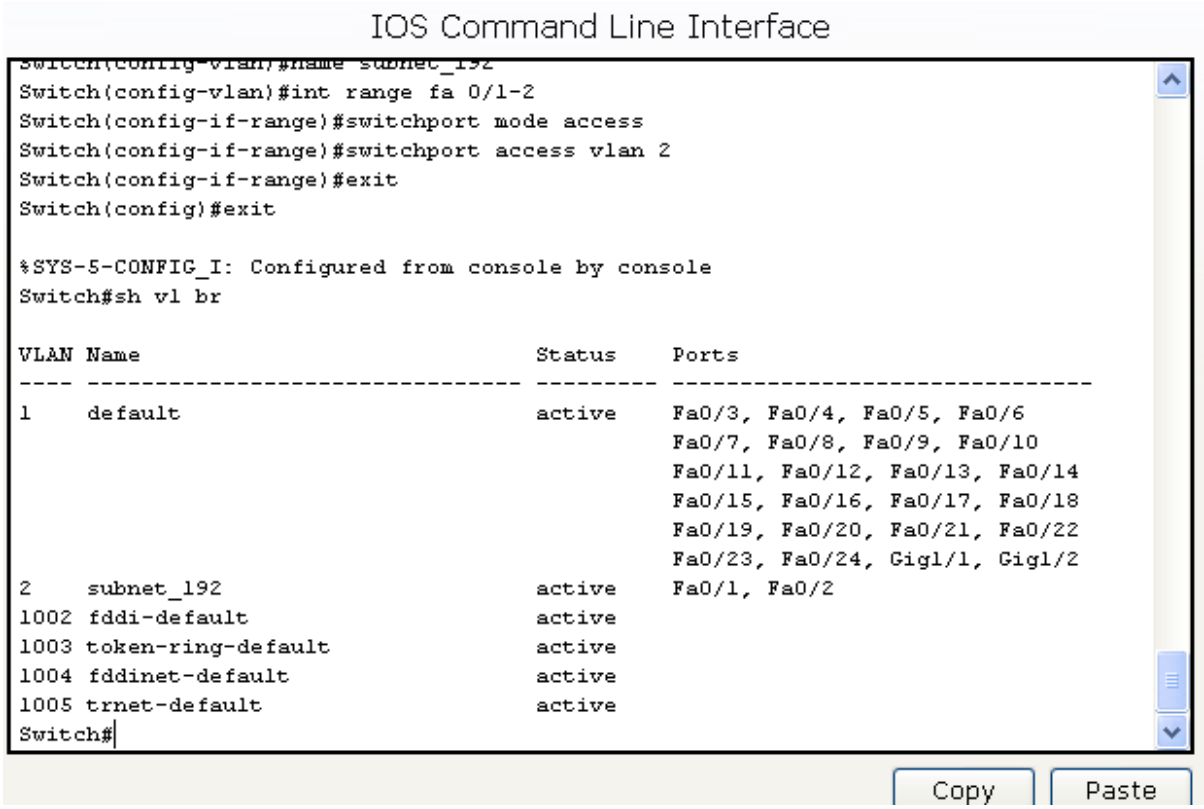


Рисунок 4 – Просмотр конфигурации VLAN

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.

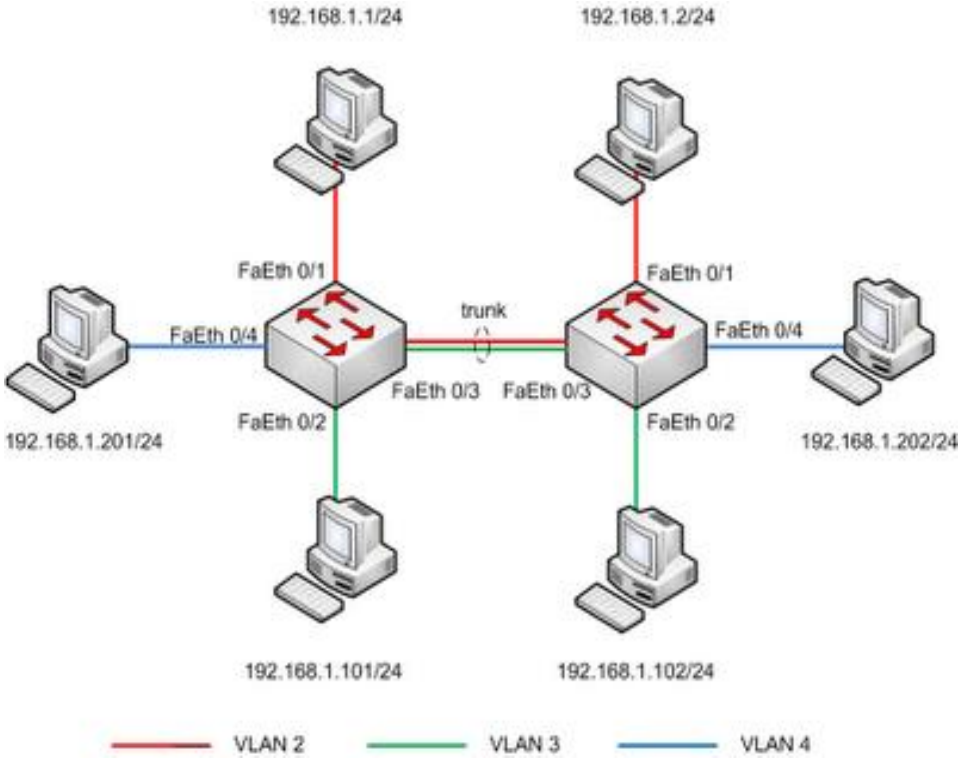


Рисунок 5 – Конфигурирование коммутаторов

По аналогии с предыдущим примером произведем конфигурирование обоих коммутаторов:

Switch(config)#vlan 2

Switch(config-vlan)#name subnet_2

Switch(config-vlan)#int fa 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)#int fa 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)#int fa 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)#int fa 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 switchport mode trunk, 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)#interface fastEthernet 0/3

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

Команда "switchport trunk allowed vlan 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 "switchport trunk allowed vlan" при своем использовании каждый раз задает разрешенные порты заново, то есть если выполнить команду switchport trunk allowed vlan 5, а потом выполнить команду switchport trunk allowed vlan 6, то разрешенным окажется только трафик VLAN номер 6. Для добавления VLAN к списку разрешенных служит команда switchport trunk allowed vlan x, где x номер добавляемого VLAN. Для удаления VLAN из списка разрешенных используется команда switchport trunk allowed vlan remove x, где x номер удаляемого VLAN. Для просмотра информации о

настроенных на коммутаторе магистральных портах служит команда show int trunk.

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 Cisco Systems. 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 – Внешний IP-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 С, 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 создаются виртуальные 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 нескольких коммутаторах 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?