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 лабораторных
работ и практических занятий
по дисциплине

# Сети и телекоммуникации

(направление подготовки 09.03.01 - Информатика и вычислительная техника)

Ростов-на-Дону
2022

Методические указания для проведения лабораторных
работ и практических занятий
по дисциплине

# Сети и телекоммуникации

Составил: И.А. Сосновский, доцент кафедры ИТСС

Рассмотрено и одобрено
на заседании кафедры
Протокол от «19» декабря 2022 г. № 5

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

***Цель работы:*** рассмотрение 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.

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

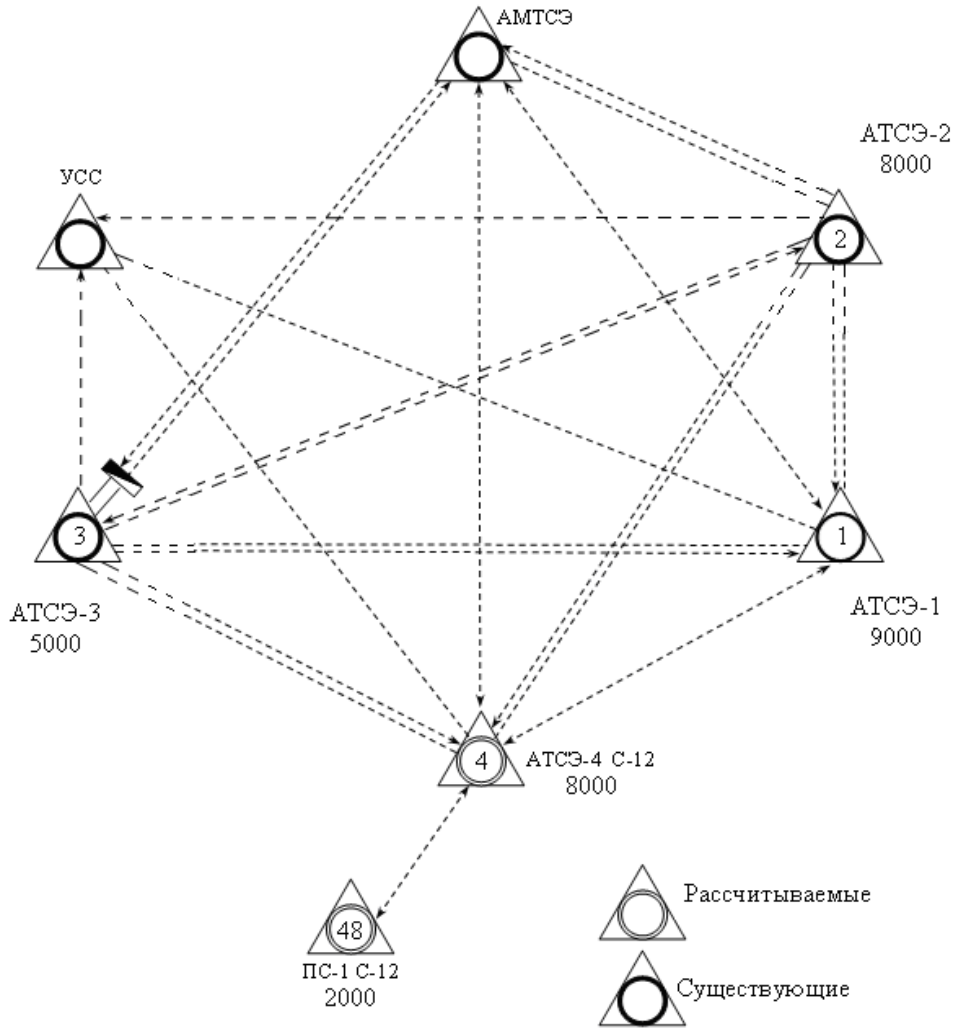



Рисунок 1 – Схема сети связи

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,

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

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:

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

где $\alpha_i$ - 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;

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

$nt_п$ - 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 $\alpha_i$ 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:

$t_п = 0{,}8$ 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:

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

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.

***Практическое занятие №2.*** 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.

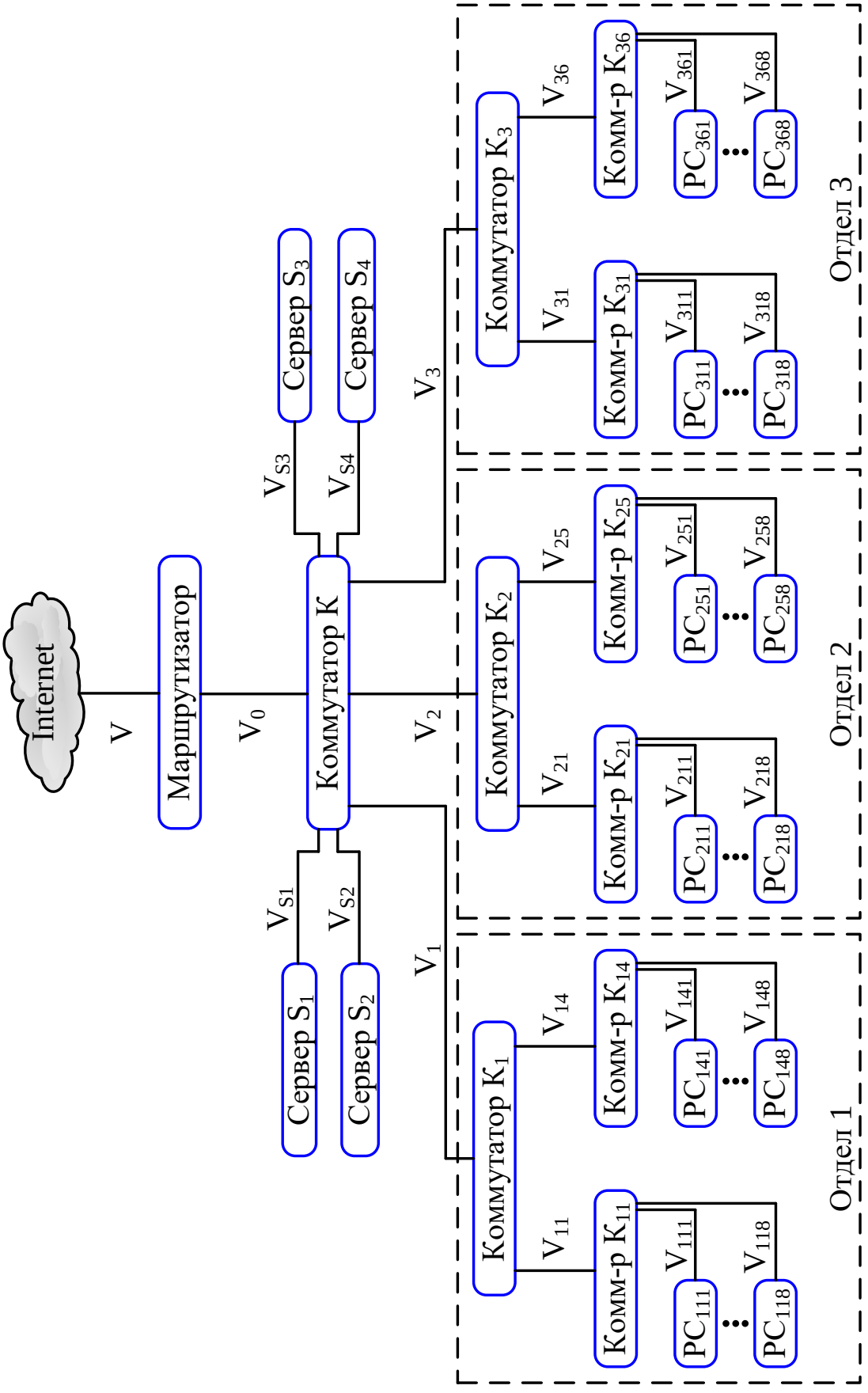



Рисунок 1 - Общая структурная схема сети компании

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 $PC_{131} \rightarrow PC_{138}$ и поток $PC_{138} \rightarrow PC_{131}$ .

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).

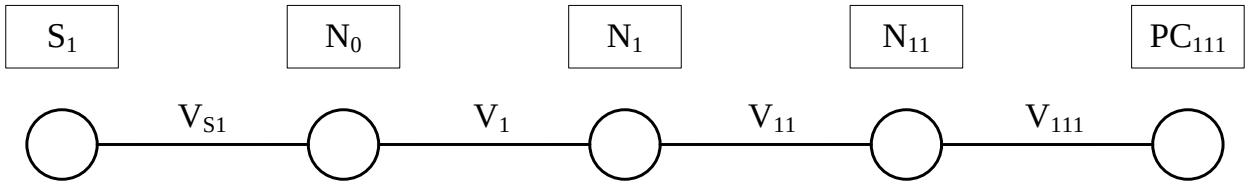



Рисунок 2 - Схема тракта сервер – рабочая станция (ПЭВМ).

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 $t_р$ = 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.

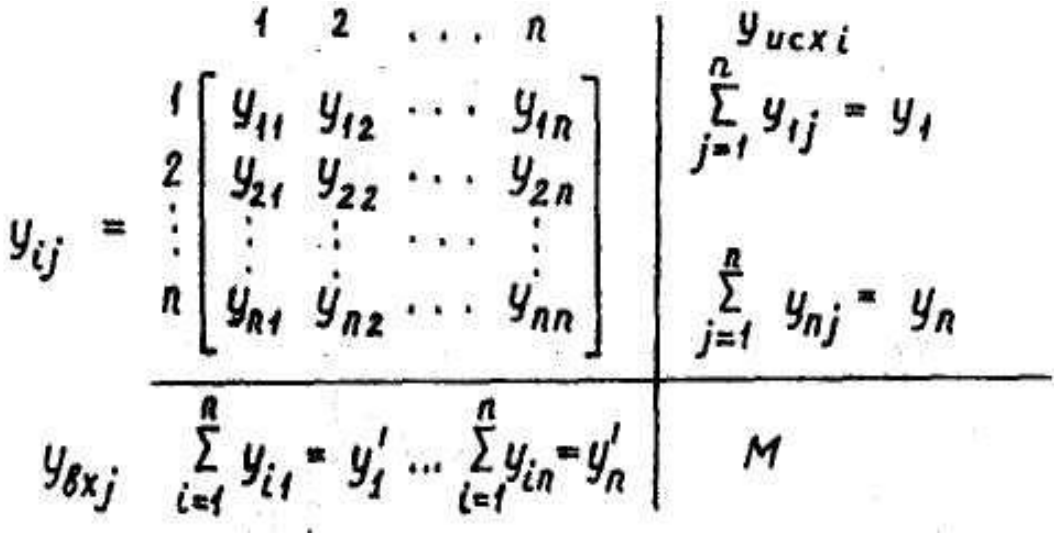
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для ВУЗов/В.Г. Олифер, Н.А. Олифер 3-е изд.- СПб: Питер, 2009г.- 958 с.: ил.

***Практическая работа №3.*** Исследование вопроса распределения потоков нагрузки на ГТС при проектировании новой станции.

**Цель работы:** рассмотрение 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:



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 :

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

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 внутристаниионная 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 №1.*** 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.

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.

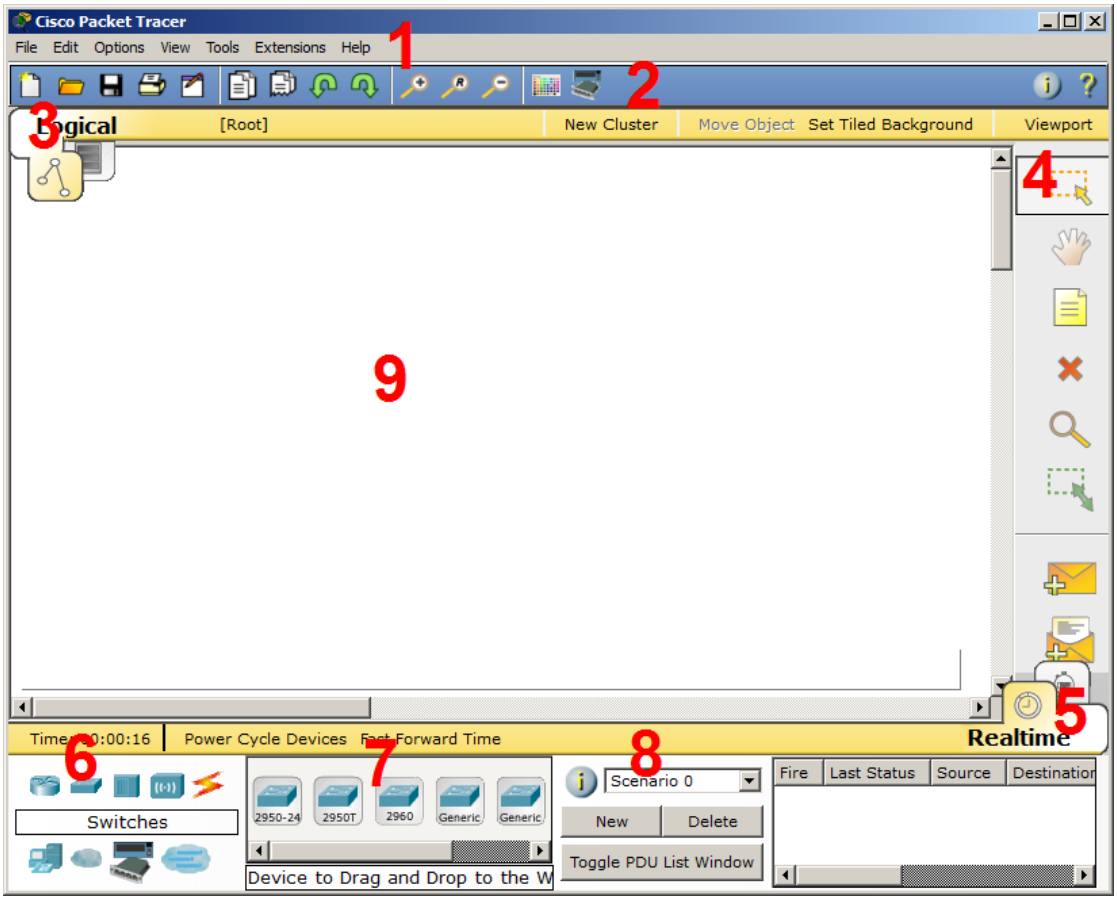
Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, пользователь может отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов. Анализ событий, происходящих в сети, позволяет 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.



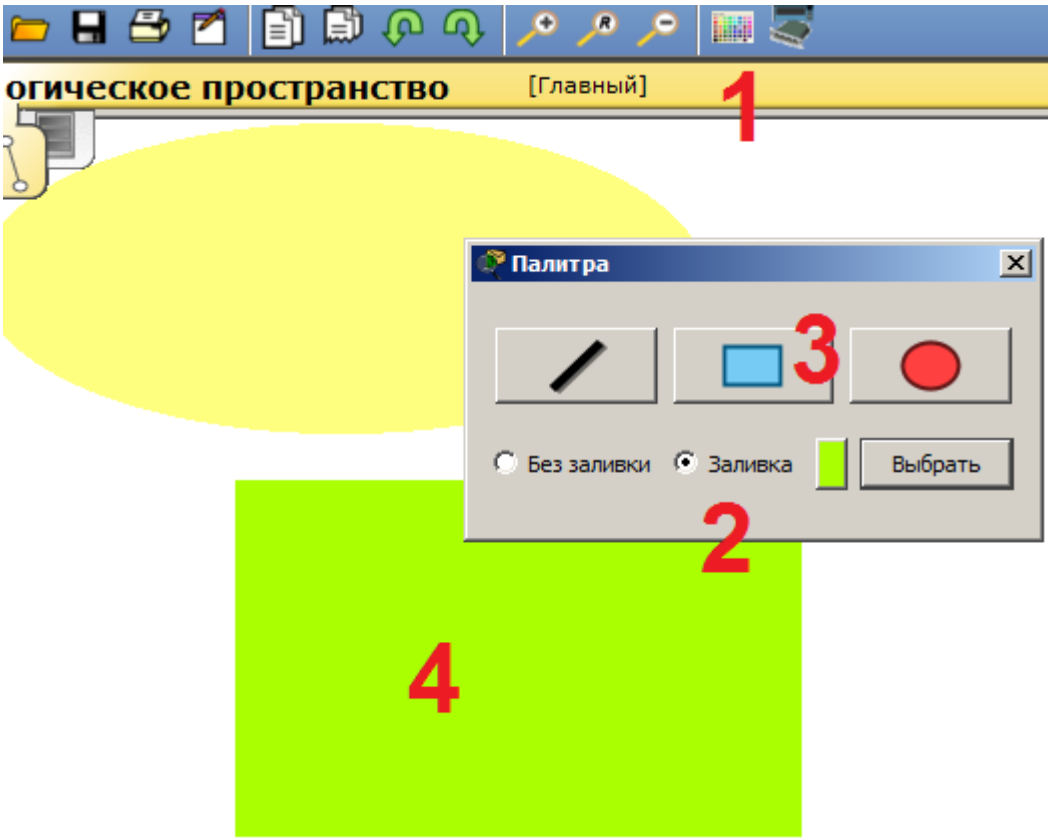

Интерфейс программы Cisco Packet Tracer

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.




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 |

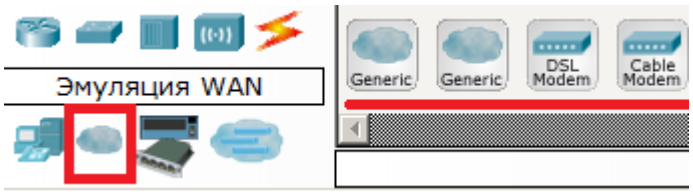
| | |
|---|---|
| | одинаковыми), а поток данных может быть чем угодно для обеих сторон. |
| Медный прямой  | Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, который функционирует на разных уровнях OSI. Он должен быть соединен со следующими типами портов: медный 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**

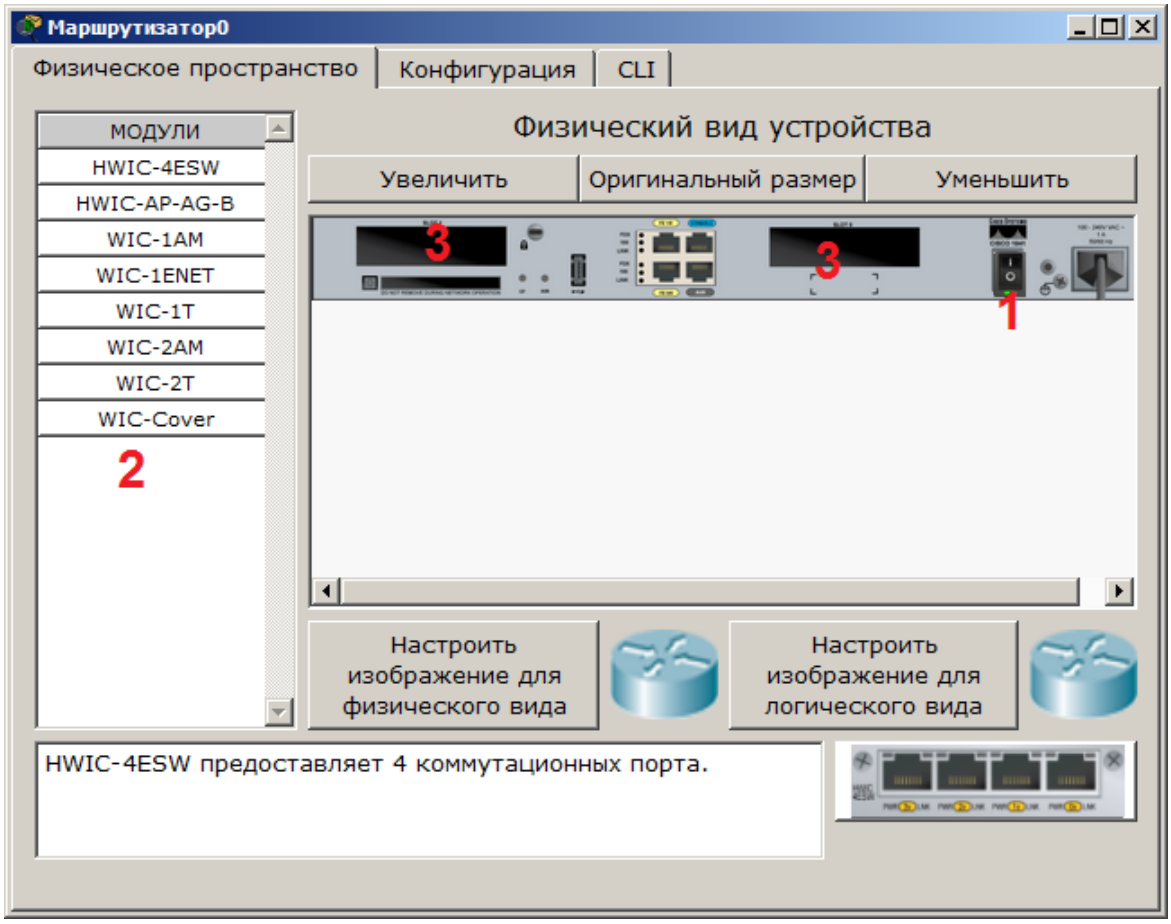



Рисунок -. Физическая конфигурация устройства

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.

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.


Конфигурация интерфейсов устройства.

***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).

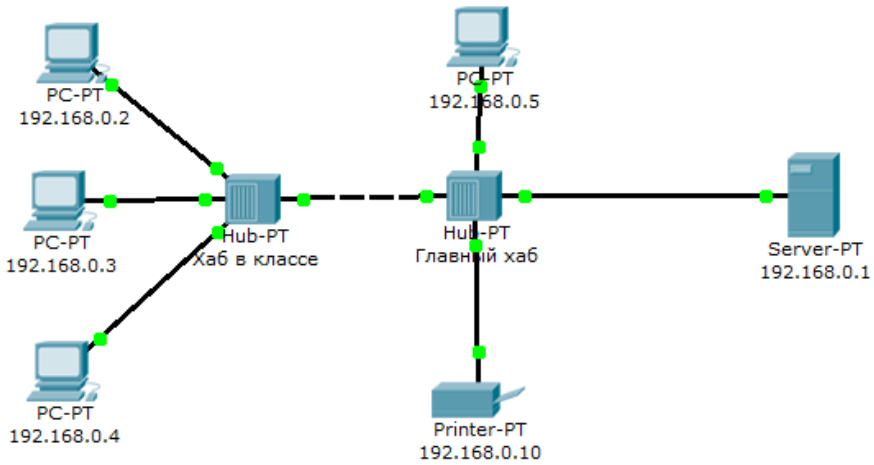



Рисунок 1 - Схема сети.

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.

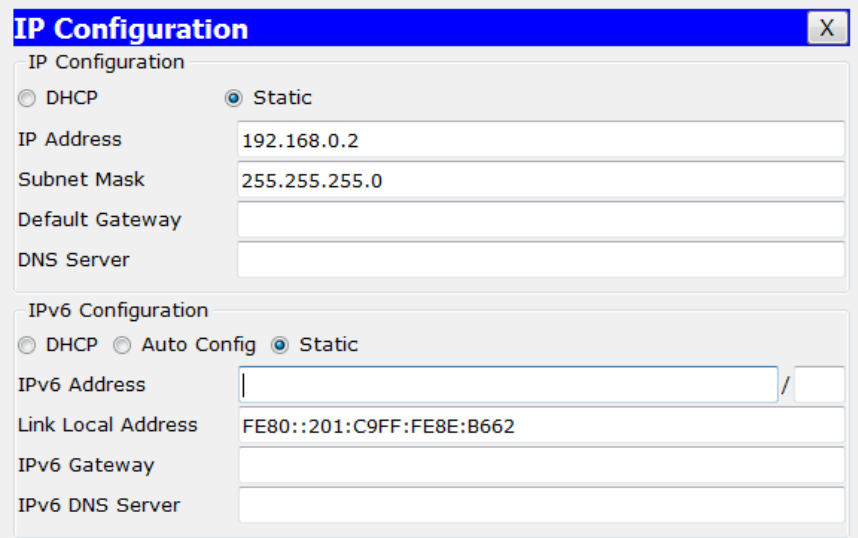



Рисунок 2 – Окно вкладки Desktop

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

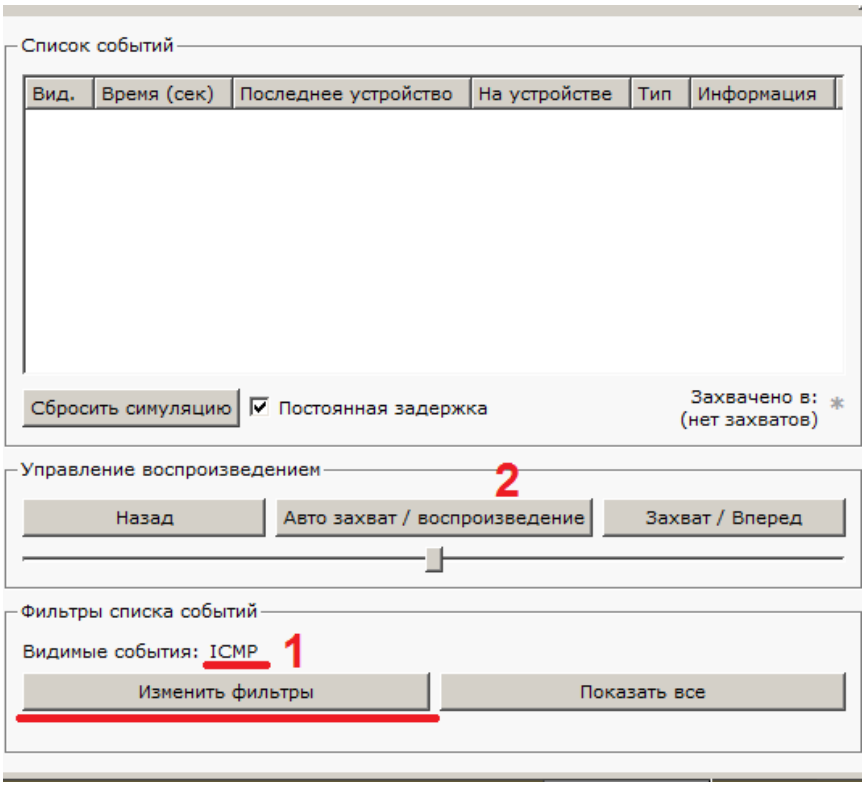



Рисунок 3 - Интерфейс симулятора.

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).

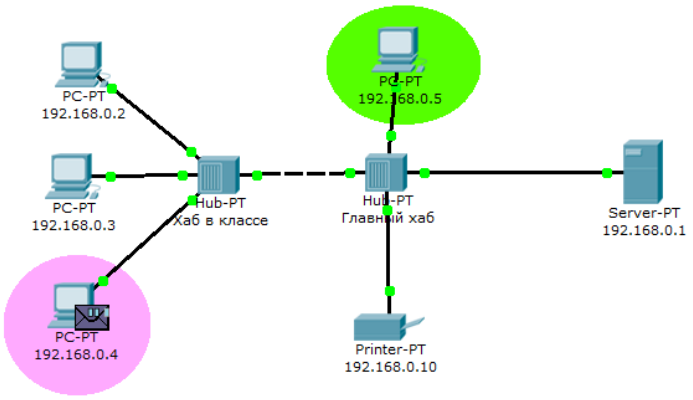



Рисунок 4 - Демонстрация работы симулятора.

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

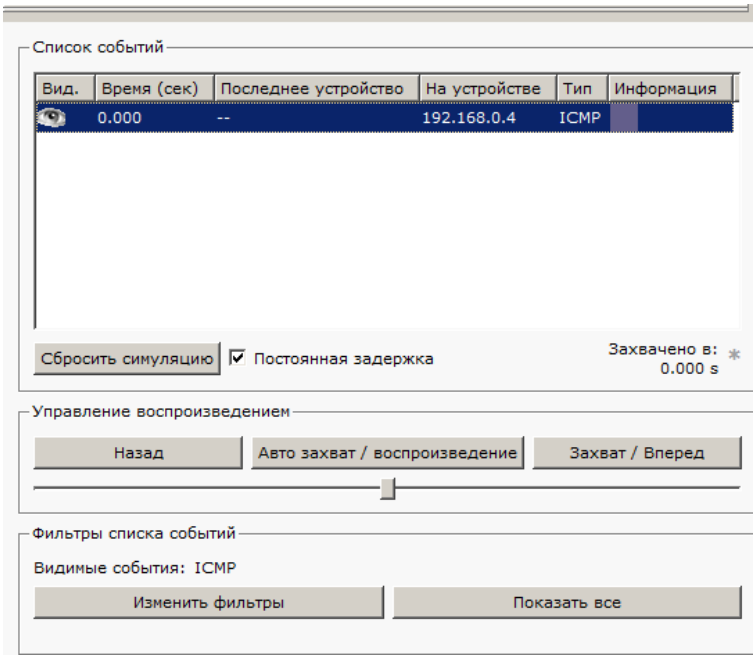



Рисунок 5 - Мониторинг работы протоколов.

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).

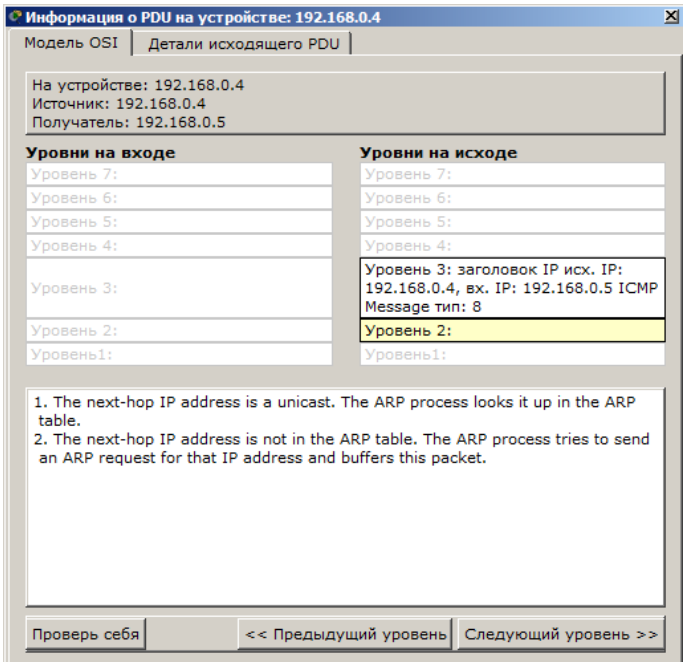



Рисунок 6 - Мониторинг работы на модели OSI

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

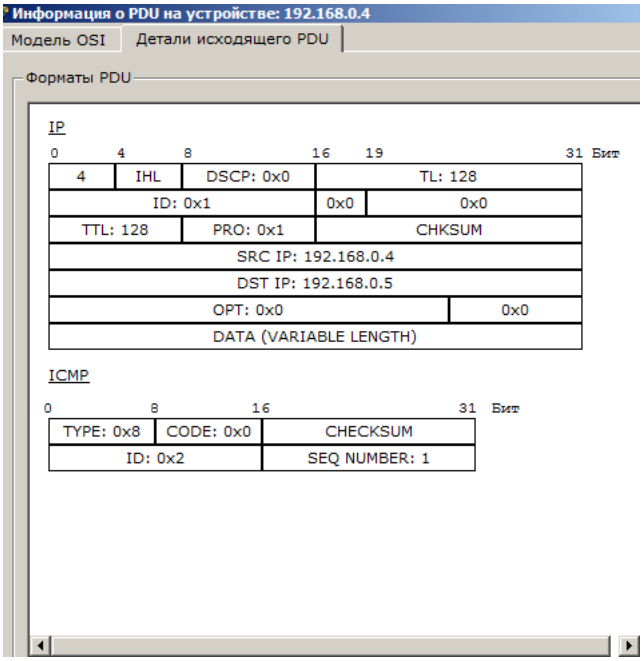



Рисунок 7 - Структура пакета

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

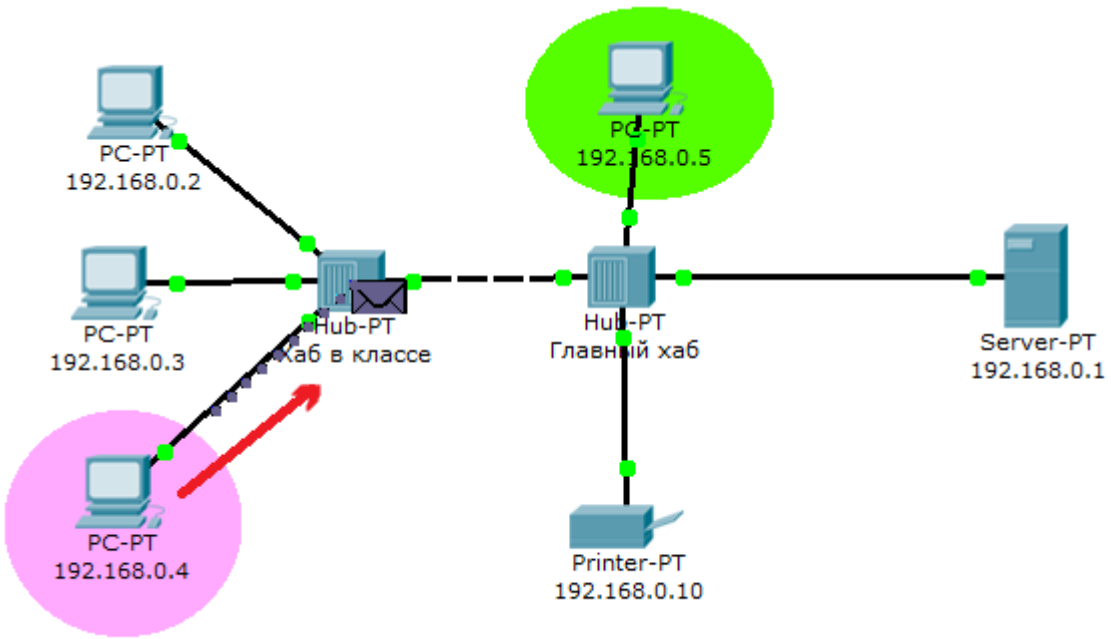



Рисунок 8 - Прохождение пакета. Первый этап

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

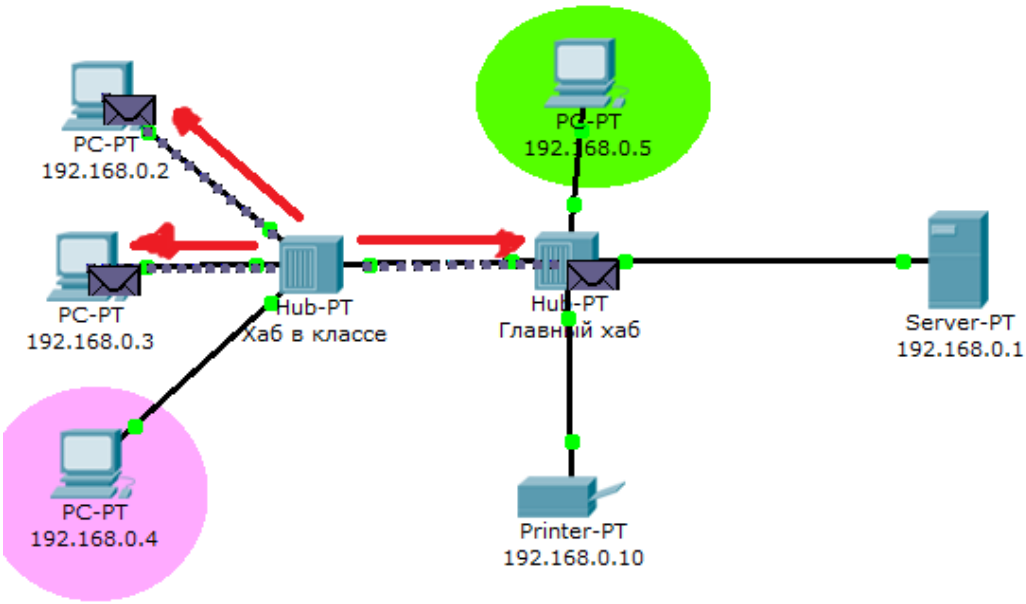



Рисунок 9 - Прохождение пакета. Второй этап

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

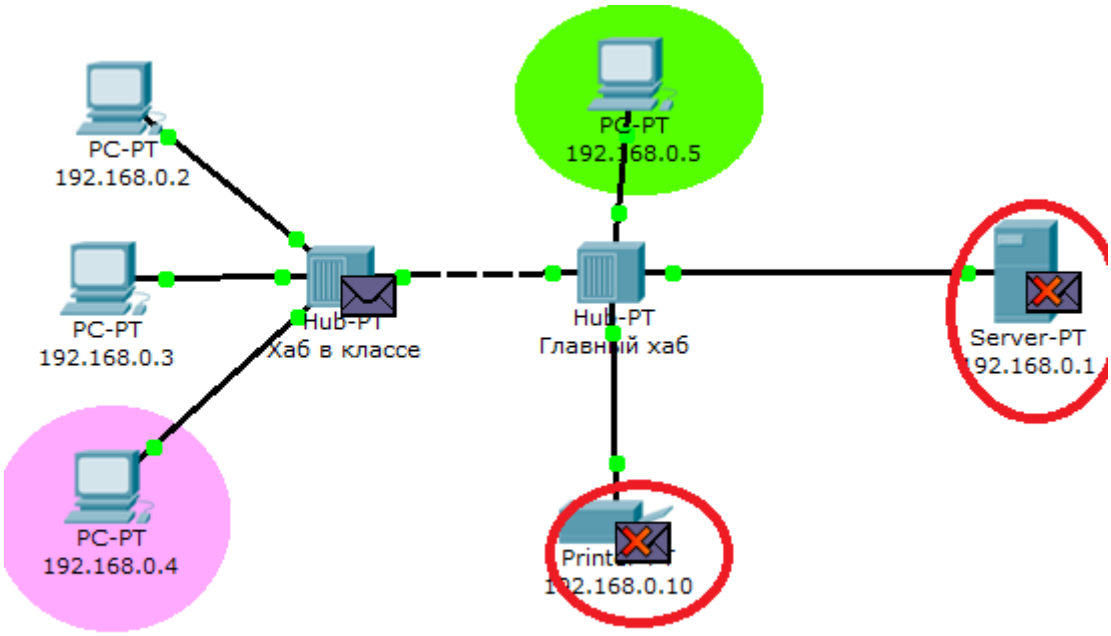



Рисунок 10 - Прохождение пакета. Третий этап

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.

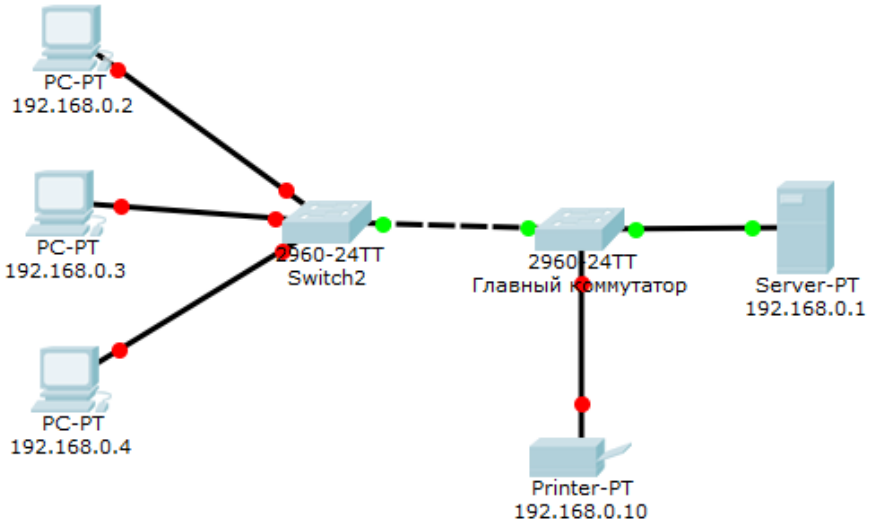



Рисунок 11 – Сеть на базе коммутатора

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).

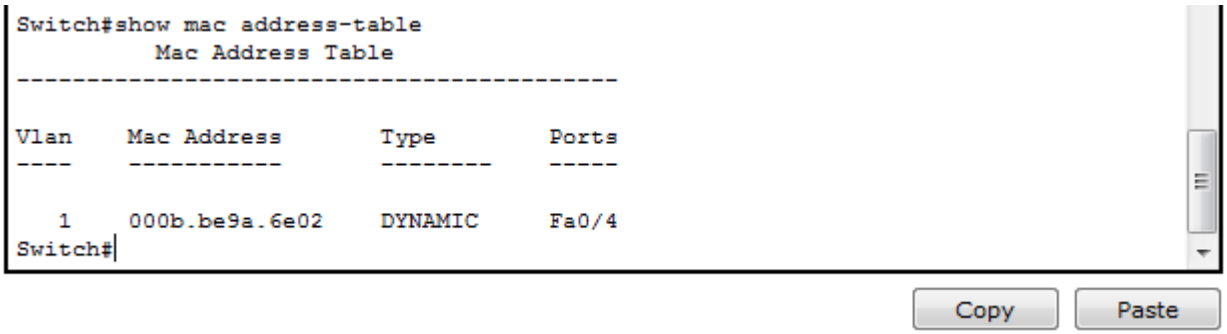



Рисунок 12 – Таблица коммутации

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 №2.** Исследование работы маршрутизатора с использованием Cisco Packet Tracer.

***Цель занятия.*** Рассмотреть правила составления статического маршрута и принципы динамической маршрутизации. Получить навыки 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.

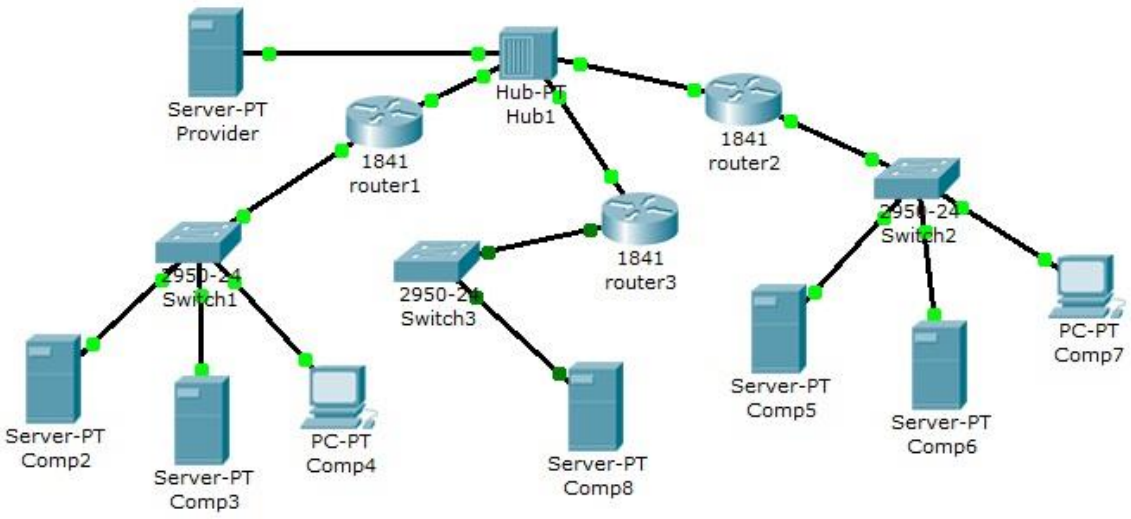



Рисунок 1 - Схема сети

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:

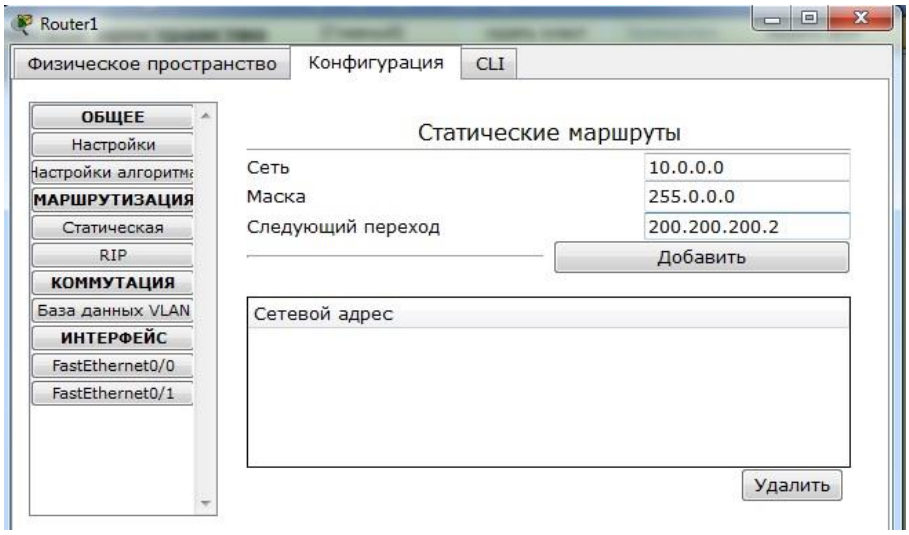



Рисунок 2 - Данные для сети 10.0.0.0/8

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

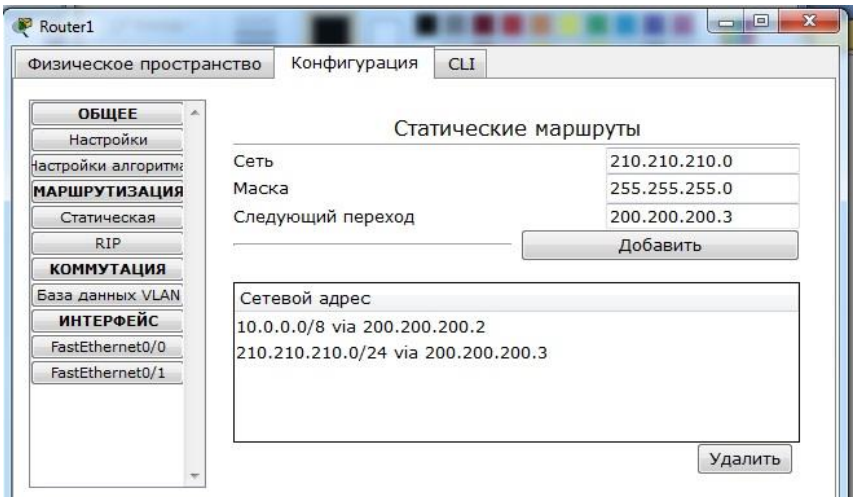



Рисунок 3 - Формирование статической таблицы маршрутизации

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.

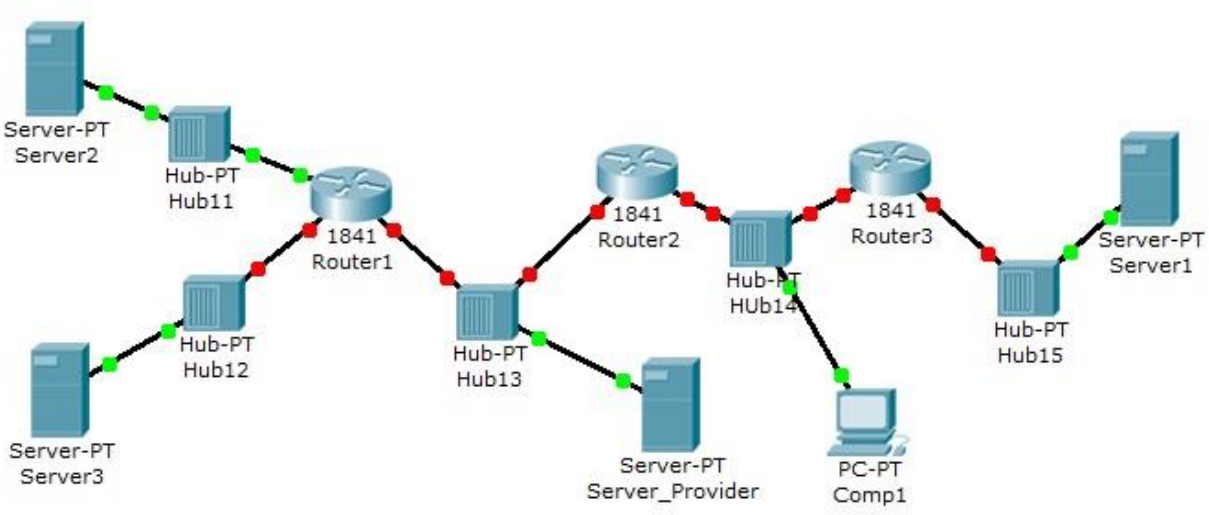



Рисунок 4 - Схема сети

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.

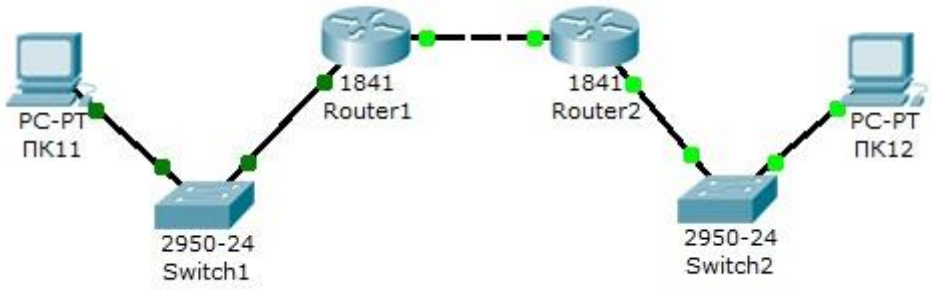



Рисунок 5 - Схема сети

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.

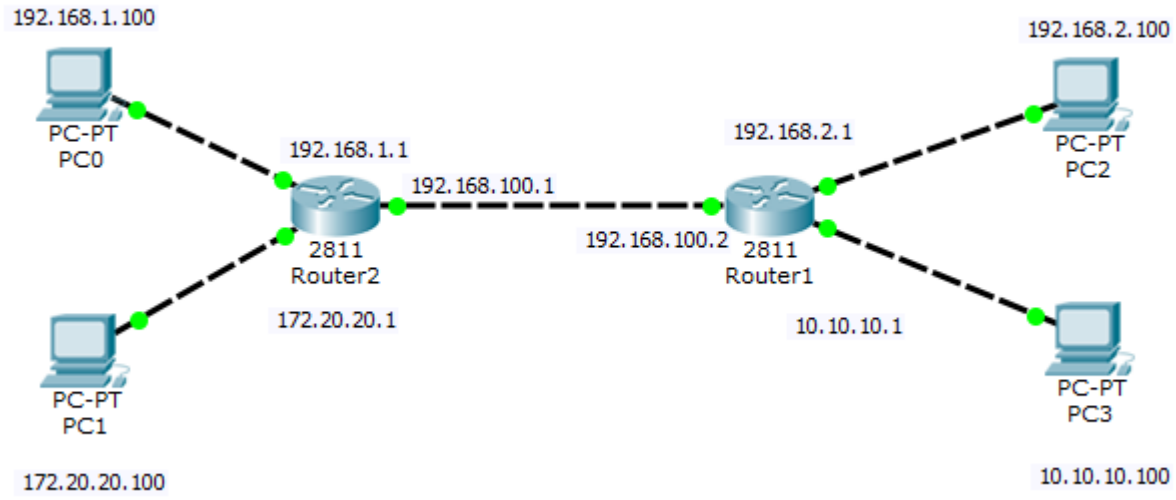



Рисунок 6

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.

**Лабораторная работа №3.** Исследование возможностей работы протокола DHSP и 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.

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).

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

Предположим, что конечный узел внутренней сети A собирается послать пакет данных конечному узлу внутренней сети B. В качестве IP-адреса получателя в пакете указывается адрес 213.180.208.102, и пакет передается на маршрутизатор внутренней сети A. 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.

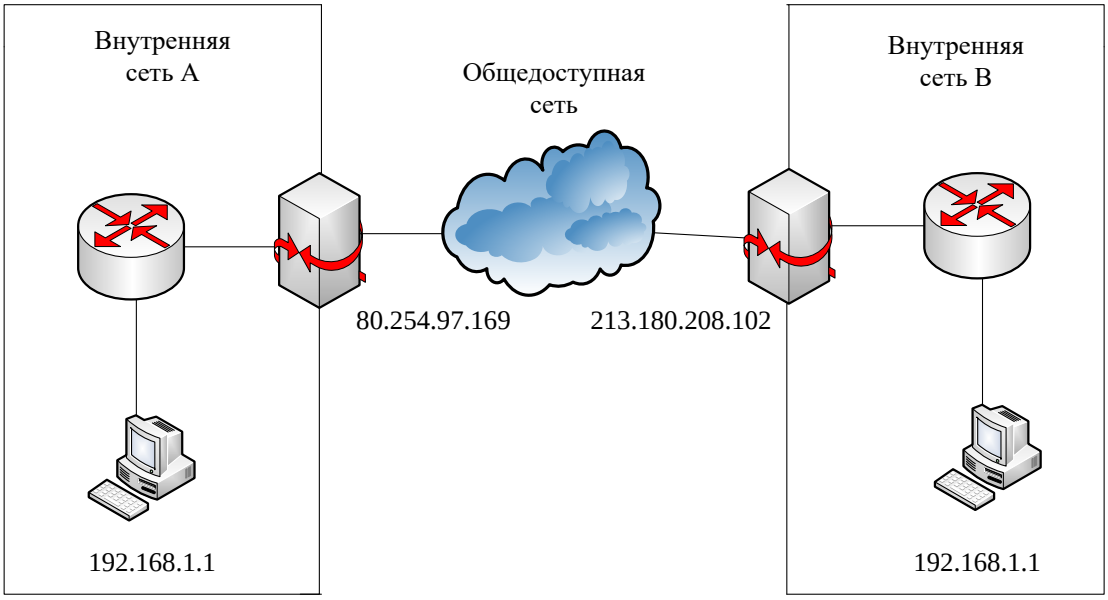



Рисунок 1 – Простейший случай использования NAT

Однако в пакет должен быть помещен также и IP-адрес отправителя. Конечный узел сети А помещает в пакет свой адрес – 192.168.1.1, и этот пакет без каких-либо изменений достигает NAT-устройства сети А. В свою очередь, NAT-устройство должно подменить адрес источника 192.168.1.1 на свой общедоступный адрес 80.254.97.169 (точнее, на адрес своего внешнего интерфейса). Эта подмена осуществляется с использованием таблицы, хранящейся в памяти NAT-устройства, упрощенный вид которой представлен в таблице 1.

Таблица 1 – Соответствие частных и общедоступных адресов

| Частный адрес | Общедоступный адрес |
|---|---|
| 192.168.1.1 | 80.254.97.169 |

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

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

Таблица 2 – Соответствие частных и общедоступных адресов

| Частный адрес | Общедоступный адрес |
|---|---|
| 192.168.1.1 | 213.180.208.102 |

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

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

Рассмотренный пример использования NAT имеет ряд существенных недостатков.

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

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

Соответственно, рассмотренный выше NAT получил название статического NAT.

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

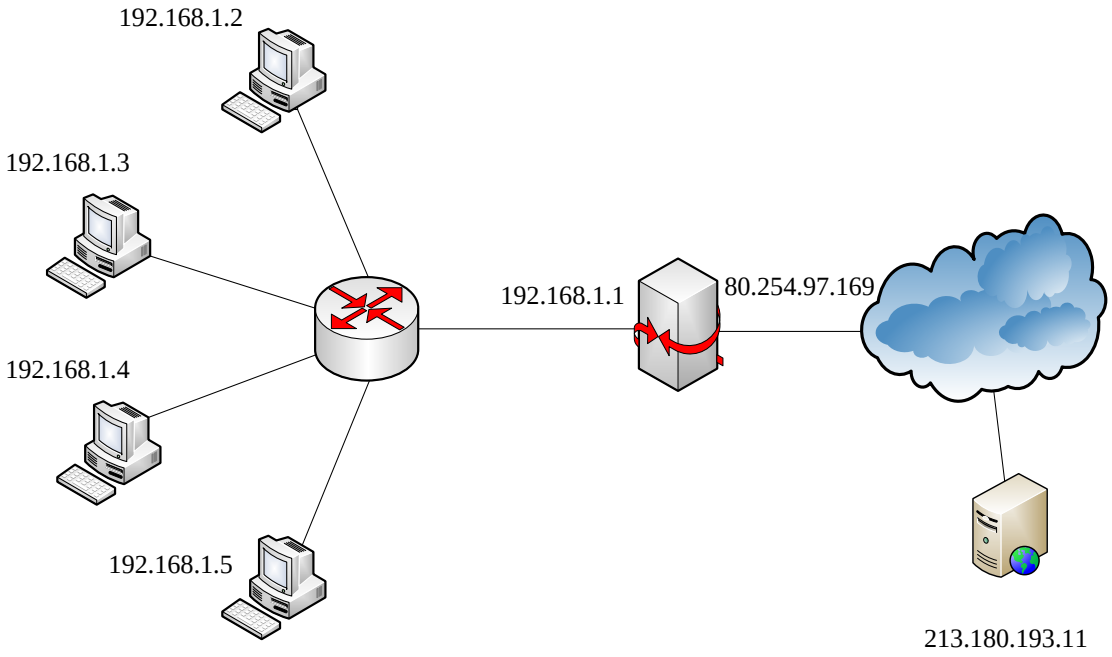



Рисунок 2 – Иллюстрация работы динамического NAT

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.

```
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).

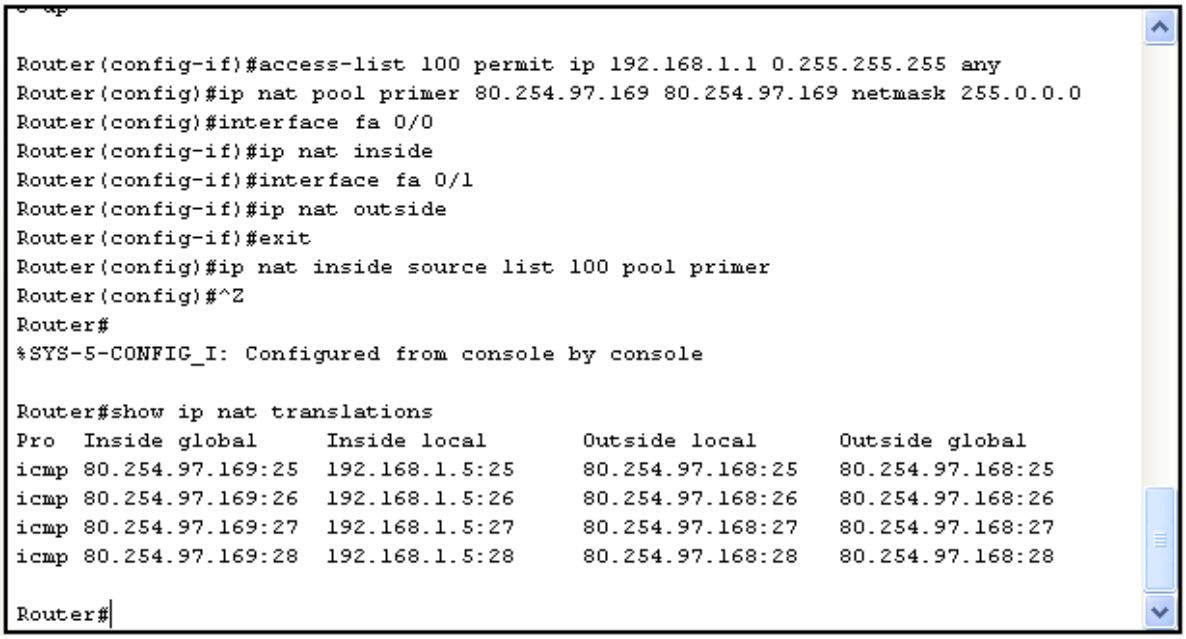



Рисунок 4 – Список трансляций

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).

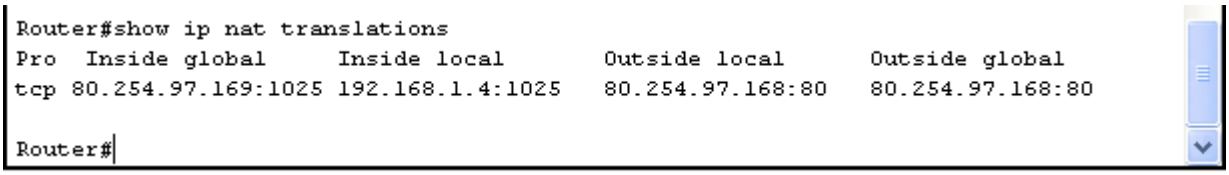



Рисунок 5 – Список трансляций после обращения к web-серверу

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.