Лабораторная работа № 2
Построение сети предприятия

Цель работы

Спроектировать и построить сеть предприятия, состоящую из подсетей. Протестировать взаимодействие подсетей на сетевом уровне стека протоколов TCP/IP.

Методические указания

Требуемое программное обеспечение

Для проведения работы необходим персональный компьютер (или виртуальная машина), работающий под управлением ОС Windows (7, 8, 10), а также прикладной пакет *Cisco Packet Tracer*.

Cisco Packet Tracer

Cisco Packet Tracer – эмулятор сети передачи данных, который позволяет выполнять эмуляцию сетей передачи данных с использованием моделей реального оборудования компании Cisco, настраивать маршрутизаторы и коммутаторы. Включает в себя модели маршрутизаторов и коммутаторов, серверов DHCP, HTTP, TFTP, FTP, рабочих станций, периферийных устройств, различных типов кабелей и устройств Wi-Fi.

Главное окно программы

Главное окно программы первоначально содержит 10 областей. Общий вид окна показан на рисунке 1.

1 строка меню – File (Файл), Edit (Правка), Options (Настройки), View (Вид), Tools (Инструменты), Extensions (Расширения) и Help (Помощь);

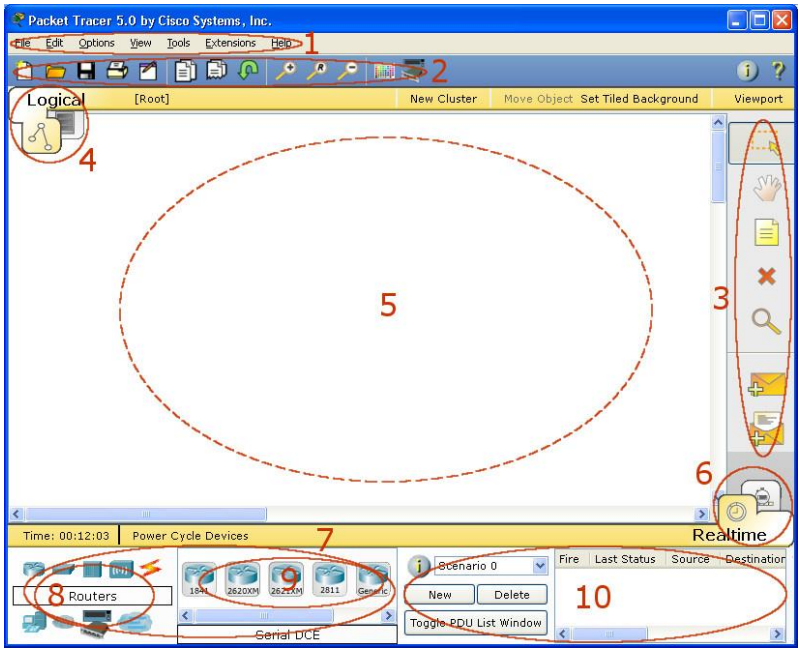


Рисунок 1 – Главное окно *Cisco Packet Tracer*

2 главная панель инструментов – ярлыки пунктов главного меню File и Edit, кнопки масштабирования рабочей области, палитры и менеджер шаблонов устройств, а также кнопки отображения информации о сети и справки (в правой части);

3 общая панель инструментов – содержит кнопки основных действий в рабочей области: Select (Выделение), Move Layout (Перемещение рабочей области), Place Note (Вставка заметки), Delete (Удаление), Inspect (Просмотр состояния объекта), Add Simple PDU (добавление сценария передачи пакета ICMP) и Add Complex PDU (добавление сценария передачи пакета);

4 переключатель «логическая/физическая» рабочая область и панель навигации –изменяет режимы представления окна программы;

5 рабочая область;

6 выбор режима эмуляции Realtime/Simulation;

7 палитра компонентов;

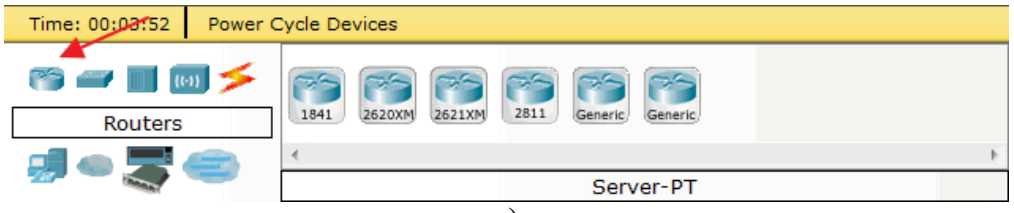
8 категории сетевых устройств;

9 сетевые устройства;

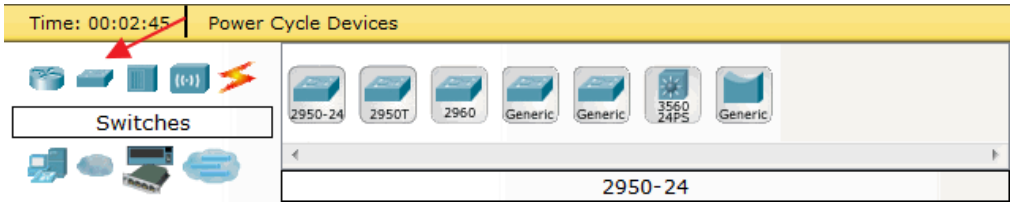
10 управление сценариями передачи пакетов пользователя.

Палитра компонентов

Палитра компонентов представляет собой набор моделей сетевых компонентов: коммутаторов, концентраторов, соединительных линий и др. (рисунок 2). В данной лабораторной работе будут использованы только коммутаторы (Switches –> 2950-24, рисунок 2, б), маршрутизаторы (Routers –> 1841, рисунок 2, а), концентраторы (Hubs –> Generic, рисунок 2, в), соединительные линии (Connections, рисунок 2, г), оконечные устройства (End Devices –> Generic Device, рисунок 2, д). Далее будут рассматриваться только используемые компоненты сети.

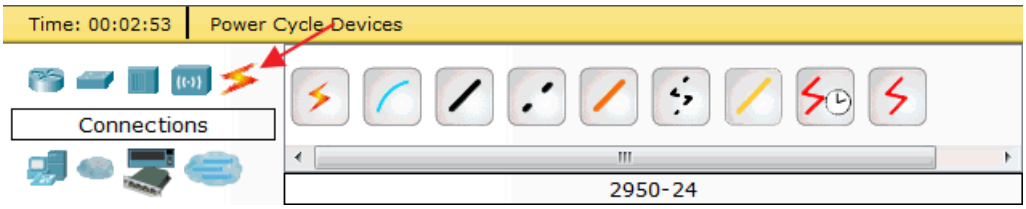


а)

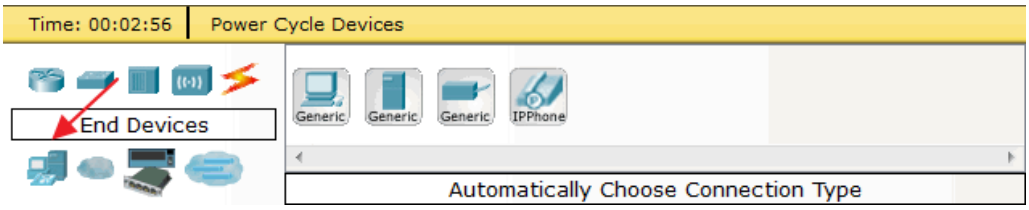


б)

в)



г)



д)

Рисунок 2 – Палитра компонентов.

Построение сети

Пример 1 – сеть с двумя ПК. Для построения сети с двумя компьютерами (рисунок 3) добавьте в рабочую область два компьютера из палитры компонентов (оконечные устройства, *End Devices*). Для объединения их в единую сеть используйте автоопределение типа соединения между сетевыми устройствами ( ).

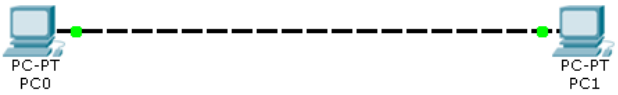
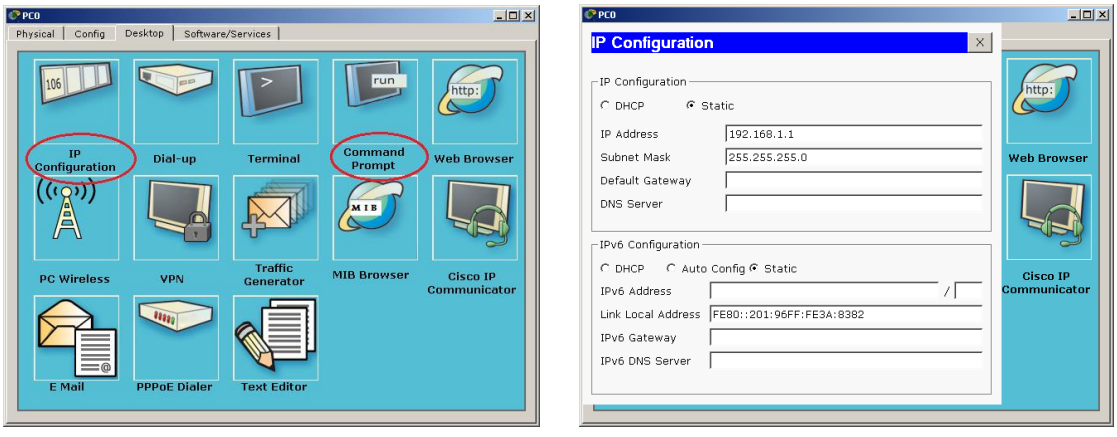


Рисунок 3 – Сеть с двумя ПК.

Каждому из компьютеров необходимо задать IP адрес. Выберите компьютер левой кнопкой мыши. В окне свойств перейдите на вкладку Desktop. Конфигурирование протокола IP удобно производить при помощи инструмента «IP Configuration», рис.4а. Необходимыми параметрами являются IP адрес (IP Address) и маска сети (Subnet Mask), рис.4б.



а) **б)**

Рисунок 4 – Настройка ПК.

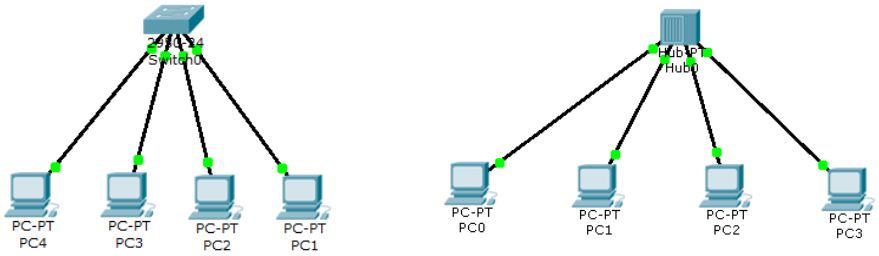
Инструмент «Command Prompt» представляет собой эмулятор командной строки. Он позволяет проверить работу моделируемой сети при помощи консольных команд arp, ipconfig, ping, tracert и др. Программа *Packet Tracer* позволяет использовать только основные функции утилит командной строки.

Программа *Packet Tracer* позволяет эмулировать передачу данных между компьютерами. Чтобы проверить работоспособность сети необходимо добавить сценарий передачи пакета ICMP, используя пиктограмму «конверт» общей панели инструментов (3, рисунок 1). После указания источника и приемника в области управления сценариями (10, рисунок 1) появится задание со статусом “In Progress”. Для запуска сценария перейдите в режим Simulation (6, рисунок 1) и в появившемся окне нажмите кнопку запуска сценария «Auto Capture / Play».

В рабочей области анимируется прохождение пакета. Пакет отображается в виде конверта. В случае успешной передачи пакета сценарий будет отмечен статусом “Successful”.

В режиме эмуляции «Real Time» можно в «Command prompt» проверить работу моделируемой сети при помощи команды ping, а также посмотреть arp таблицу и конфигурацию протокола IP.

Пример 2 – сеть с коммутатором и сеть с концентратором. Для соединения нескольких ПК в единую сеть можно использовать коммутатор (Switch) 2950-24 или концентратор (Hub). См. рисунок 5 (а, б).



а) **б)**

Рисунок 5 – Сеть с четырьмя ПК.

Разбиение сети на подсети

Документ RFC 1918 (в 1996 г.) определил диапазоны адресов для частных сетей (***address blocks for private internets***), рекомендуемые для присвоения сетям организаций, изолированным от Internet или имеющим доступ к Internet через ограниченное количество выделенных адресов Internet. Это блоки адресов:

Класс A:	10.0.0.0 – 10.255.255.255	сеть до 16 млн. узлов
Класс B:	172.16.0.0 – 172.31.255.255	сети до 65тыс. узлов
Класс C:	192.168.0.0 – 192.168.255.255	сети до 254 узлов

При построении сети предприятия, исходя из количества имеющихся компьютеров (узлов сети) с учетом возможного увеличения их в будущем, выбирается адрес сети из соответствующего класса. Приведенный адрес сети класса С можно выбрать для сети с количеством узлов порядка двух сотен с учетом возможного разбиения на подсети и увеличения числа узлов. Если не

предполагается соединение с другими сетями и (или) подключение к Internet, то достаточно присвоить адреса всем узлам сети, настроить их, и сеть готова к работе по протоколу TCP/IP. Примеры адресов узлов для сети ***192.168.7.0***:

192.168.7.1 1-й хост (узел),
192.168.7.2 2-й хост (узел),
192.168.7.3 3-й хост (узел) и т.д.

Заметим, что адресом хоста не может быть код, содержащий все нули (это адрес сети) или все единицы (это широковещательная рассылка в данной сети). Следовательно, последний возможный адрес хоста в нашем примере может быть ***192.168.7.254***.

Имеется несколько причин, ограничивающих число узлов в одной сети (сегменте):

– физические ограничения на длину кабеля и количество узлов в сегменте,
– логические ограничения на число узлов в сегменте (напр., Ethernet – 1024),
– опасность возникновения т.н. широковещательных штормов,
– увеличение трафика в сегменте и др.

Для решения этих проблем используют средства сетевого уровня. В этом случае сеть рассматривается как совокупность нескольких сетей, называемых подсетями (***subnets***).

Дефицит IP-адресов и резкий рост размеров таблиц маршрутизации побудил к поиску способов более эффективного использования IP-адресного пространства. Один из них состоит в использовании механизма подсетей (***Subnetting***).

Суть этого механизма состоит в разбиении узловой части IP-адреса на два поля: поле адреса подсети и поле адреса узла (хоста). При этом внутренняя структура сети (разбиение ее на подсети) «не видна извне», что означает независимость внешней маршрутизации (доставки пакетов **до** или **от** данной сети) от ее внутренней структуры. Другой причиной, побуждающей к разбиению большой сети на подсети, является стремление избавиться от «широковещательных штормов» и снизить суммарный трафик в сети, ограничив его внутри каждого сегмента. Для выделения подсетей в сети необходимо определить количество сегментов и количество узлов в каждом сегменте с учетом возможного развития сети предприятия в ближайшие годы.

Например, если сеть 192.168.7.0 (блок содержит 256 адресов) будет состоять из 5-ти сегментов не более чем по 20 узлов в каждом, то можно принять разбиение ее на 8 подсетей с максимальным количеством узлов 30 в каждой подсети. Принятием такого решения определяется количество бит в поле адреса подсети (3 бита т.к. 2^3=8) и в поле адреса узла (5 бит т.к. 2^5=32). Максимальное количество узлов в подсети равно 30-ти, а не 32, т.к. коды, содержащие все единицы и все нули, не могут быть адресом узла.

Определив поля адреса подсети и узла, запишем маску подсети:

11111111 11111111 11111111 11100000 – ***255.255.255.224***.

Адреса подсетей, полученные в результате применения маски подсети:

192.168.7.0 подсеть №0
192.168.7.32 подсеть №1
192.168.7.64 подсеть №2
. . .
192.168.7.192 подсеть №6
192.168.7.224 подсеть №7

Для реализации 5-ти сегментов можно выбрать любые пять адресов. Оставшиеся три адреса подсетей можно считать зарезервированными для дальнейшего расширения сети предприятия. Затем необходимо определить адреса хостов в каждой подсети. Например, для подсети №1 это адреса:

192.168.7.33 хост №1
192.168.7.34 хост №2
192.168.7.35 хост №3
…
192.168.7.62 хост №30

Маршрутизация и шлюзы

Отдельные подсети объединяются в сеть с помощью шлюзов (маршрутизаторов). Шлюзом может служить любой из компьютеров в сети, на котором установлено больше одного сетевого адаптера. Пусть есть две подсети, называемые «Подсеть А» и «Подсеть В», и их необходимо соединить через шлюз. В этом случае один из адаптеров компьтера-шлюза подключается к сегменту подсети А, а другой – к сегменту подсети В. В ОС на шлюзе необходимо активизировать службу маршрутизации (для Windows это «*Маршрутизация и удаленный доступ*» или «*Routing and Remote Access*»). Одному адаптеру необходимо присвоить адрес из множества адресов, принадлежащих подсети А, другому – из адресов подсети В. Для всех узлов в каждой подсети необходимо указать IP-адрес своего шлюза при настройке протокола TCP/IP.

Один из узлов подсети №1, напр., ***192.168.7.33***, принадлежит шлюзу, соединяющему ее, например, с подсетью №2. Другой интерфейс этого шлюза, принадлежащий подсети №2, будет иметь один из адресов этой подсети, напр., ***192.168.7.65***.

Пример 3 – маршрутизируемая сеть

Для соединения подсетей в единую сеть в программе *Cisco Packet Tracer* используется шлюз или маршрутизатор (Gateway, Router) 1841. См. рисунок 6.

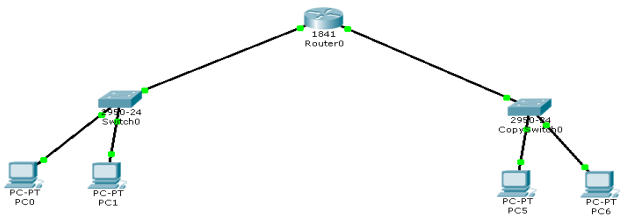
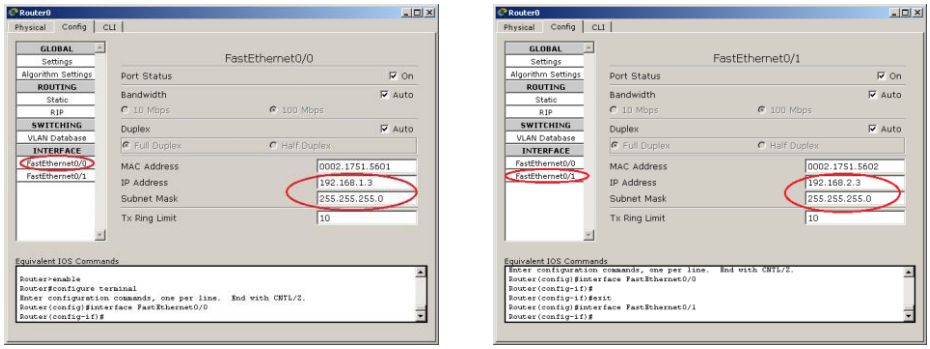


Рисунок 6 – Сеть с двумя подсетями.

При настройке шлюза двум его интерфейсам присваиваются IP-адреса из диапазона соответствующих подсетей (рисунок 7-а,7-б). Эти адреса также указываются в настройках каждого PC, подключенного к этому интерфейсу.



а) **б)**

Рисунок 7 – Настройка шлюза.

В простых сетях, где не используется сложное сетевое оборудование, не применяются, соответственно, и протоколы маршрутизации. Статическая маршрутизация – вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора. Вся маршрутизация при этом происходит без участия дополнительных протоколов маршрутизации.

Пример 4 – маршрутизируемая сеть из трех подсетей

Добавление третьей подсети требует введения второго маршрутизатора (рисунок 8).

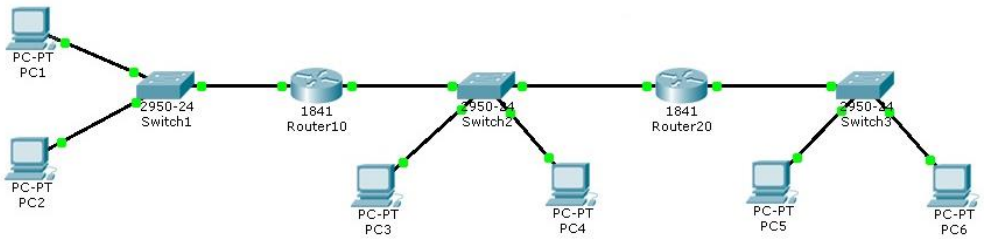


Рисунок 8 – Сеть с тремя подсетями.

Для передачи пакетов между двумя крайними подсетями противоположные маршрутизаторы должны «знать об их существовании» (Router10 – знать о подсети, расположенной по отношению к нему за Router20, и наоборот), т.е. роутеры должны иметь прописанные маршруты (здесь – статические).

При наличии нескольких подсетей и нескольких шлюзов возникает необходимость указывать несколько статических маршрутов. Эти записи представляют собой **таблицу маршрутизации**. Для сокращения списка маршрутов можно использовать указание маршрута (шлюза) по умолчанию. Обычно это путь, ведущий в сторону нескольких подсетей (при наличии выхода в сеть Интернет обычно путь по умолчанию ведет «в сторону Интернет»).

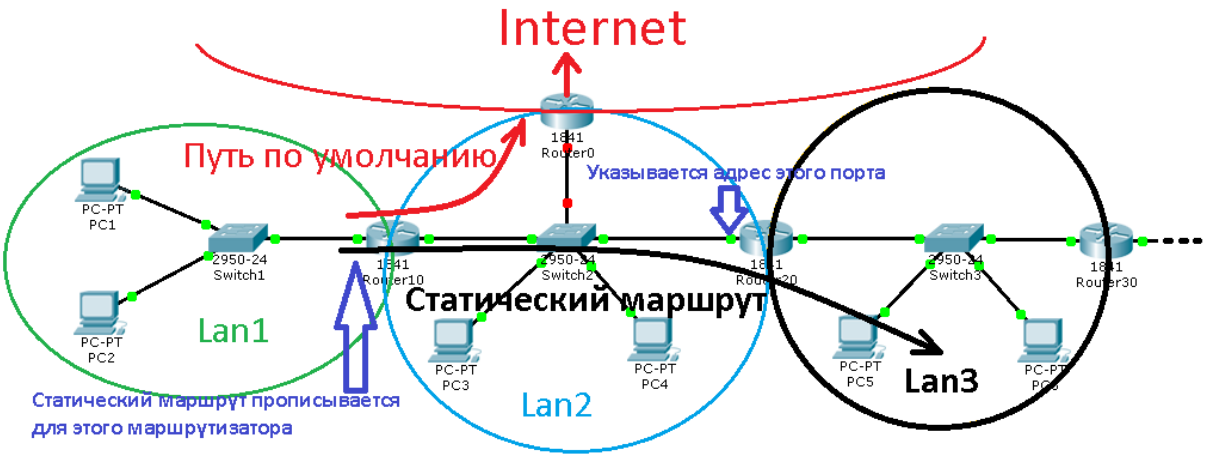


Рисунок 9 – Статический маршрут.

На рисунке 9 путь по умолчанию ведет «наверх», в сторону Интернет. В этом случае путь на подсеть 3 должен быть записан как статический маршрут с указанием маски и адреса шлюза, на который следует отправлять пакеты, предназначенные узлам подсети 3 (рисунок 10). Добавление пути по умолчанию показано на рисунке 11.

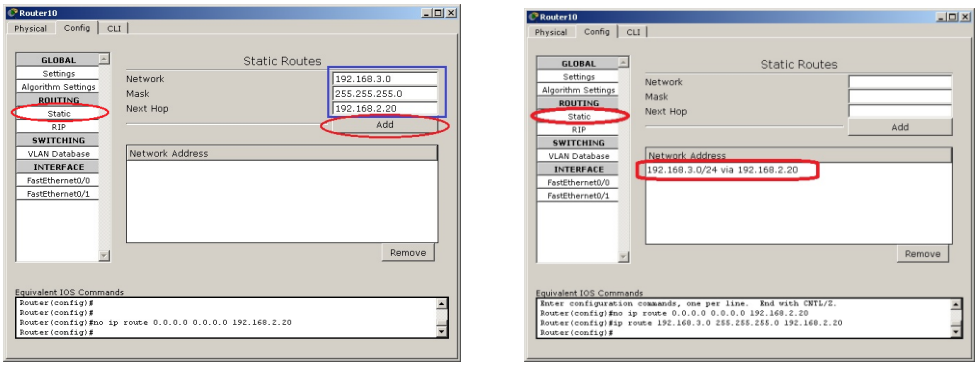


Рисунок 10 – Добавление статического маршрута.

Добавление маршрута (шлюза) по умолчанию. Прописывается IP адрес 0.0.0.0 и маска 0.0.0.0 (рисунок 11).

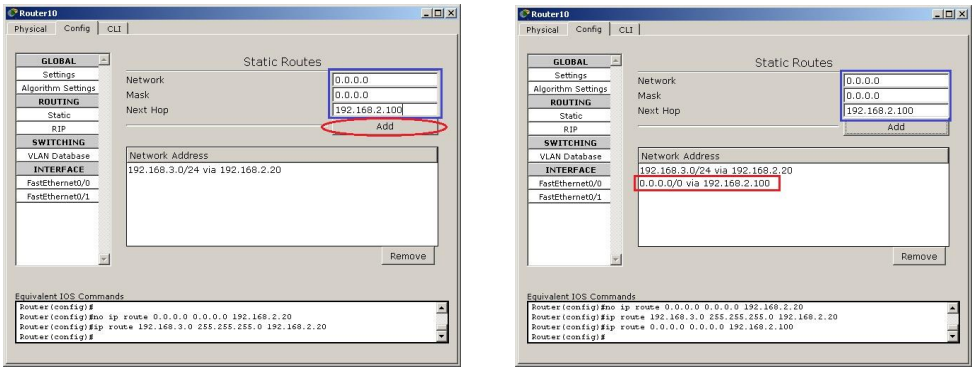


Рисунок 11 – Добавление маршрута по умолчанию.

Пример 5 – маршрутизируемая сеть из трех подсетей и внешней сети

Добавление внешней сети требует введения третьего маршрутизатора (рисунок 12).

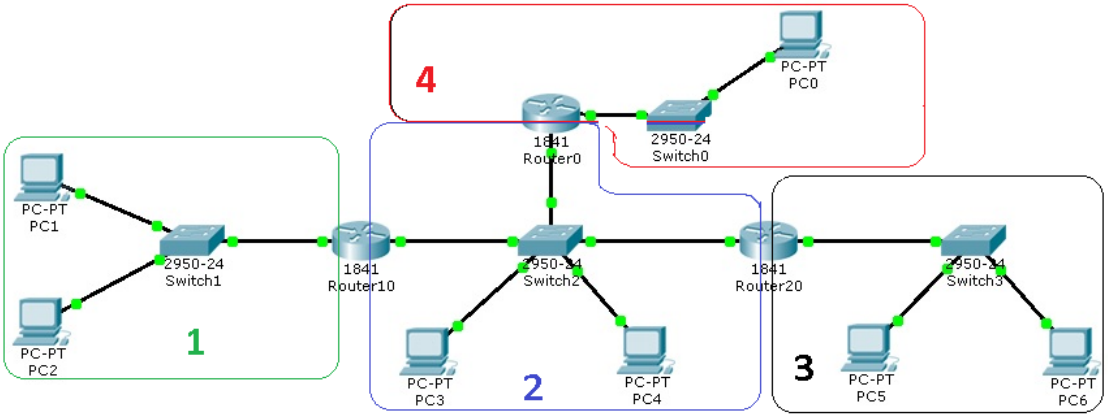


Рисунок 12 – Сеть с тремя подсетями и внешней сетью.

Для маршрутизации пакетов «наверх» шлюз по умолчанию может отправлять пакеты во внешнюю сеть, имитируя связь с интернет-провайдером. Для того, чтобы тестовые пакеты проходили во внешнюю сеть и возвращались обратно, во внешней сети тоже должны быть указаны маршруты (шлюзы) на внутренние подсети 1 и 2. Для роутеров 10 и 20 обязательно также указание дополнительных статических маршрутов для направления пакетов между подсетями 1 и 3 через подсеть 2.

Порядок выполнения работы

1. Выполнить задание 1.
2. Выполнить задание 2.
3. Выполнить задание 3.
4. Построить сеть между двумя ПК (Пример 1). Использовать UTP, задать имена узлов, IPv4-адреса, маски, IPv6-адреса.
5. Исследовать работу сети (*ipconfig*, *ping*, *arp*).
6. Исследовать продвижение пакетов в режиме эмуляции.
7. Построить сеть с четырьмя ПК с использованием коммутатора (Пример 2).
8. Выполнить п.2, п.3.
9. Построить сеть с четырьмя ПК с использованием концентратора (Пример 2).
10. Выполнить п.2, п.3.
11. Построить сеть с двумя подсетями (Пример 3) с применением IP адресов, ***рассчитанных в соответствии с вариантом:***
    Адреса подсетей:
    x.x.20 + № варианта.0
    x.x.100 + № варианта.0
    x.x.180 + № варианта.0
    x.x – произвольные, но из частного диапазона адресов (Private IP Networks), например, 192.168
    Маска подсети везде класса «C», т.е. 255.255.255.0
    4-я подсеть (сеть) класса «A», т.е.
    10.0.0.0, маска 255.0.0.0
12. Выполнить п.2, п.3.

13. Добавить 3-ю подсеть (с адресами ***из своего варианта***) и прописать статические маршруты (Пример 4).
14. Выполнить п.2, при необходимости п.3.
15. Добавить внешнюю сеть (Пример 5) с указанными адресами (например, из диапазона 10.0.0.0 – 10.255.255.255) и прописать статические маршруты, маршруты по умолчанию.
16. Выполнить п.2, при необходимости п.3.

Задания на лабораторную работу

Задание 1

Какие из данных адресов не могут быть использованы в качестве IP-адреса конечного узла сети, подключенной к Internet? Обоснуйте ответ.

Вариант 1 (7).

1) 0.0.0.0
2) 127.0.0.1
3) 169.254.240.13/16
4) 226.4.37.105
5) 103.24.254.0/8
6) 154.12.255.255/16
7) 255.255.255.255
8) 172.16.12.1
9) 193.256.1.16
10) 194.87.45.0/24

Вариант 2 (8).

1) 228.15.36.103
2) 195.34.116.255/24
3) 161.23.45.305/16
4) 204.0.3.1/24
5) 0.0.0.0
6) 127.0.0.1
7) 169.254.0.10/16
8) 255.255.255.255
9) 123.0.0.0/8
10) 192.168.32.250/24

Вариант 3 (9).

1) 169.254.0.17/16
2) 255.255.255.255
3) 194.12.263.2/24
4) 196.15.241.0/24
5) 116.12.123.5/8
6) 172.16.248.0/16
7) 100.255.255.255/8
8) 127.0.0.2

Вариант 4 (10).

1) 167.10.255.255/16
2) 129.44.172.3/16
3) 262.194.0.17
4) 127.0.0.3
5) 10.252.14.0/8
6) 225.12.100.4
7) 0.0.0.0
8) 169.254.10.2
9) 255.255.255.255
10) 167.10.0.0/16

Вариант 5 (11).

1) 227.140.10.0
2) 192.168.0.10/24
3) 255.255.255.255
4) 0.0.0.0
5) 132.100.10.110/16
6) 144.12.0.0/16
7) 260.11.0.0
8) 200.192.8.255/24
9) 169.254.101.3/16
10) 127.0.0.5

Вариант 6 (12).

1) 255.255.255.255
2) 0.0.0.0
3) 120.72.0.1/8
4) 125.0.0.0/8
5) 203.10.13.255/24
6) 10.0.0.15/8
7) 229.0.0.14
8) 127.0.0.0

9) 230.8.38.163
10) 0.0.0.0

9) 12.302.0.6
10) 169.254.220.30

Задание 2 Использование масок. Определение максимального количества узлов подсети

По IP-адресу узла и маске определите номер подсети, номер узла, максимальное число узлов в подсети. Запишите значения в двоичном и десятичном виде.

№ вар	IP-адрес узла и маска подсети	Номер подсети	Номер узла	Максимальное число узлов
1	131.107.17.15/22			
	198.65.12.67, маска 255.255.255.240			
2	10.0.0.5/30			
	129.64.134.5, маска 255.255.128.0			
3	206.73.118.135/26			
	10.10.129.3, маска 255.255.254.0			
4	206.73.118.24/29			
	192.168.23.66 маска 255.255.255.224			
5	10.4.34.3/21			
	131.107.0.10 маска 255.255.255.0			
6	172.16.19.5/22			
	192.168.1.32 маска 255.255.255.128			
7	131.107.100.53/28			
	206.73.118.13 маска 255.255.255.252			
8	10.12.200.169/25			
	192.168.10.9 маска 255.255.248.0			
9	172.20.43.128/24			
	131.107.32.52 маска 255.255.255.240			
10	192.168.244.12/23			
	10.200.53.2 маска 255.255.240.0			
11	131.107.10.13/28			
	172.31.3.24 маска 255.255.255.248			
12	206.73.118.32/27			

	131.107.8.10 маска 255.255.252.0			

Задание 3

По заданному IP-адресу, маске и необходимому количеству подсетей N определить:

- маску для разбиения на подсети;
- список возможных IP-адресов подсетей;
- максимальное количество узлов в каждой подсети;
- минимальный и максимальный IP-адреса для каждой подсети.

№ вар	IP-адрес и маска	Количество подсетей N
1	192.150.148.0/24	6
2	134.234.0.0/16	12
3	134.240.0.0/16	20
4	196.132.14.0/24	3
5	164.20.0.0/16	18
6	220.16.136.0/24	9
7	123.0.0.0/8	100
8	172.16.0.0/16	15
9	120.0.0.0/8	35
10	158.14.50.0/24	7
11	10.0.0.0/8	60
12	126.0.0.0/8	72

Результаты привести в двоичном и десятичном виде и свести в таблицу:

Маска	IP-адреса подсетей	Максимальное количество IP-адресов в подсети	Минимальный IP-адрес в подсети	Максимальный IP-адрес в подсети

Содержание отчета

1. Результаты выполнения заданий 1, 2, 3.
2. Работающая сеть из 3-х подсетей и внешней сети (Пример 5). Файл ***.pkt**. На схеме подписать все настройки компьютеров и роутеров.
3. Результаты тестирования и исследования сети с помощью утилит TCP/IP (скриншоты).
4. Выводы.

Приложения к лабораторной работе №2

Приложение 1. О настройке протокола TCP/IP в ОС Windows

Простая сеть, не имеющая подсетей и шлюзов, не требует настройки, т.к. по умолчанию используется протокол APIPA (*Automatic Private IP Addressing*). Узлам сети назначаются адреса из диапазона 169.254.x.y, где x.y – произвольные значения байтов, генерируемые на каждом узле как случайные числа. Не исключается совпадение IP адресов на узлах. Следует обновить адрес на одном из этих узлов (например, перезагрузив его).

При наличии в сети подсетей и, соответственно, шлюзов, протокол TCP/IP требует настройки, если в сети нет DHCP-сервера. Настройка сетевых компонентов производится в окне Свойства выбранного Сетевого подключения. Выбрав свойства «TCP/IPv4», необходимо переключить выбор на «Использовать следующий IP адрес» и задать значения адреса и маски подсети в соответствующих полях. Если подсеть связана с другими подсетями в сети через шлюзы, то необходимо ввести IP-адрес шлюза (шлюзов). Обычно необходимым условием успешного Web-серфинга по сети Internet является задание адреса сервера DNS. Однако в данной лабораторной работе DNS не используется, как не используется и служба WINS. Остальные параметры стека TCP/IP либо не определены, либо принимаются с установками по умолчанию.

Приложение 2. Пример проектирования сети предприятия.

Пусть количество узлов сети предприятия на сегодня составляет 500. На предприятии существует 12 организационных единиц (отделов). Максимальное количество компьютеров в отделе равно 40. Программа развития предполагает довести количество компьютеров в ближайшем будущем до 600, возможно создание еще 2 отделов. Требуется спроектировать сеть с учетом этих данных.

Проектирование сети выполним поэтапно, но в другой последовательности.

На ***первом этапе*** определим количество бит в той части сетевого адреса, которая предназначена для нумерации подсетей. Для 14-ти подсетей эта часть адреса должна содержать не менее 4 бит.

На ***втором этапе*** определим количество бит в узловой части маски подсети. Так как максимальное количество узлов в подсети определено равным 40, то количество бит должно быть не менее 6 (это позволит адресовать до 62 хостов в каждой подсети).

На ***третьем этапе*** определяем маску сети и маску подсети. Маска сети содержит в узловой части нули, количество которых равно сумме разрядов, необходимых для нумерации всех подсетей и всех хостов в каждой подсети (здесь 4+6=10). Таким образом, маска сети в двоичном представлении равна 11111111 11111111 11111100 00000000, а в десятичном, соответственно, **255.255.252.0**. Маска подсети содержит 6 нулей в узловой части: **255.255.255.192**.

Четвертый этап – определение адреса сети и адресов подсетей. Адрес сети выбираем из диапазона частных подсетей. Адреса из диапазона 172.16.0.0 – 172.31.255.255 рекомендованы для сетей с количеством узлов, большим, чем

254. Возьмем адрес сети равный **172.20.0.0**. В двоичном представлении это **10101100 00010100 000000**00 00000000 (выделена сетевая часть адреса). Тогда адреса подсетей будут равны:

- подсеть № 0 – 172.20.0.0 (двоичное 10101100 000101000 00000**00 00**000000)
- подсеть № 1 – 172.20.0.64 (двоичное 10101100 000101000 00000**00 01**000000)
- подсеть № 2 – 172.20.0.128 (двоичное 10101100 000101000 00000**00 10**000000)
- подсеть № 3 – 172.20.0.192 (двоичное 10101100 000101000 00000**00 11**000000)
- подсеть № 4 – 172.20.1.0 (двоичное 10101100 000101000 00000**01 00**000000)
- подсеть № 5 – 172.20.1.64 (двоичное 10101100 000101000 00000**01 01**000000)
- подсеть № 6 – 172.20.1.128 (двоичное 10101100 000101000 00000**01 10**000000)
- подсеть № 7 – 172.20.1.192 (двоичное 10101100 000101000 00000**01 11**000000)
- подсеть № 8 – 172.20.2.0 (двоичное 10101100 000101000 00000**10 00**000000)
- подсеть № 9 – 172.20.2.64 (двоичное 10101100 000101000 00000**10 01**000000)
- подсеть №10 – 172.20.2.128 (двоичное 10101100 000101000 00000**10 10**000000)
- подсеть №11 – 172.20.2.192 (двоичное 10101100 000101000 00000**10 11**000000)
- подсеть №12 – 172.20.3.0 (двоичное 10101100 000101000 00000**11 00**000000)
- подсеть №13 – 172.20.3.64 (двоичное 10101100 000101000 00000**11 01**000000)
- подсеть №14 – 172.20.3.128 (двоичное 10101100 000101000 00000**11 10**000000)
- подсеть №15 – 172.20.3.192 (двоичное 10101100 000101000 00000**11 11**000000).

В двоичном представлении выделены биты, определяющие номер подсети.

Пятый этап – определение адресов узлов в каждой полсети. Определим адреса узлов для подсети №13:

- хост №1 – 172.20.3.65
- хост №2 – 172.20.3.66
- хост №3 – 172.20.3.67

…

- хост №61 – 172.20.3.125
- хост №62 – 172.20.3.126

Адрес 172.20.3.127 является адресом ограниченной широковещательной рассылки для этой подсети.