МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА МЕТАЛУРГІЙНА АКАДЕМІЯ УКРАЇНИ

О.І. Михальов, Ю.О. Каліберда

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни

«Комп'ютерні мережі»

для студентів напряму – “Комп’ютерні науки”

Дніпропетровськ НМетАУ - 2019

ЛАБОРАТОРНАЯ РАБОТА 1
Создание локальной сети в Packet Tracer

Компьютерная сеть – это совокупность компьютеров, телекоммуникационного оборудования и других устройств, соединенных линиями связи и обменивающихся информацией между собой в соответствии с определенными правилами – протоколом.

Основное назначение компьютерных сетей - это обеспечение доступа к распределенным ресурсам. Ресурсами сети называют информацию, программы и аппаратные средства. Компьютерная сеть (вычислительная сеть, сеть передачи данных) система связи компьютеров и/или компьютерного оборудования (серверы, маршрутизаторы и другое оборудование). Для передачи информации могут быть использованы различные физические явления, как правило различные виды электрических сигналов, световых сигналов или электромагнитного излучения.

Для организации локальной сети с небольшим количеством компьютером (10…30) чаще всего используется одна из типовых топологий (общая шина, кольцо, звезда или полносвязная сеть). Данные топологии обладают свойством однородности – все компьютеры обладают одинаковыми правами в отношении доступа к другим компьютерам (за исключениям центрального компьютера при соединении звезда). Однородность структуры позволяет легко увеличивать число компьютеров, облегчает обслуживание и эксплуатацию сети. Однако данные топологии накладывают ограничения на:

- длину связи между двумя узлами;
- количество узлов в сети;
- интенсивность трафика.

Для снятия этих ограничений используется специальные методы структуризации сети и специальное сетевое оборудование – повторители, концентраторы, мосты, коммутаторы, маршрутизаторы. Данное оборудование называется *коммуникационным*, с его помощью отдельные сегменты сети взаимодействуют друг с другом.

Повторитель – простейшее коммуникационное устройство, используется для физического соединения различных сегментов кабеля локальной сети с целью увеличения общей длины сети. Повторитель улучшает качество передаваемого сигнала (восстановление мощности, амплитуды сигналов и пр.). Повторитель, который имеет несколько портов и соединяет несколько физических сегментов, часто называют *концентратором* или *хабом*.

Мост **(*bridge*)** – делит разделяемую среду передачи сети на части (часто называемые логическими сегментами), передавая информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима, то есть если адрес компьютера назначения принадлежит другой подсети. Тем самым мост изолирует трафик одной подсети от трафика другой, повышая общую производительность передачи данных в сети.

Коммутатор **(*switch*)** по принципу обработки кадров от моста практически ничем не отличается. Единственное его отличие состоит в том, что он является своего рода коммуникационным мультипроцессором, так как каждый его порт оснащен специализированной микросхемой, которая обрабатывает кадры по алгоритму моста независимо от микросхем других портов. За счет этого общая производительность коммутатора обычно намного выше производительности традиционного моста, имеющего один процессорный блок.

Маршрутизатор или ***роутер*** **(*router*)** – специализированный сетевой компьютер, имеющий два или более сетевых интерфейсов и пересылающий пакеты данных между различными сегментами сети. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определенные правила, заданные администратором.

Шлюз – используется для объединения сетей с разными типами программного и аппаратного обеспечения.

Практическая часть

1. Добавим на рабочее поле программы 5 коммутаторов Switch 2960-24TT. По умолчанию они имеют имена – Switch0, Switch1, Switch2, Switch3 и Switch4.
2. Добавим на рабочее поле восемь компьютеров с именами по умолчанию PC0 – PC7.
3. Соединим устройства в сеть Ethernet , как показано на рис.1.1. Компьютер с коммутатором соединяются витой парой, а коммутаторы между собой – кросс-кабелем. На всех устройствах для подключения используются порты FastEthernet.

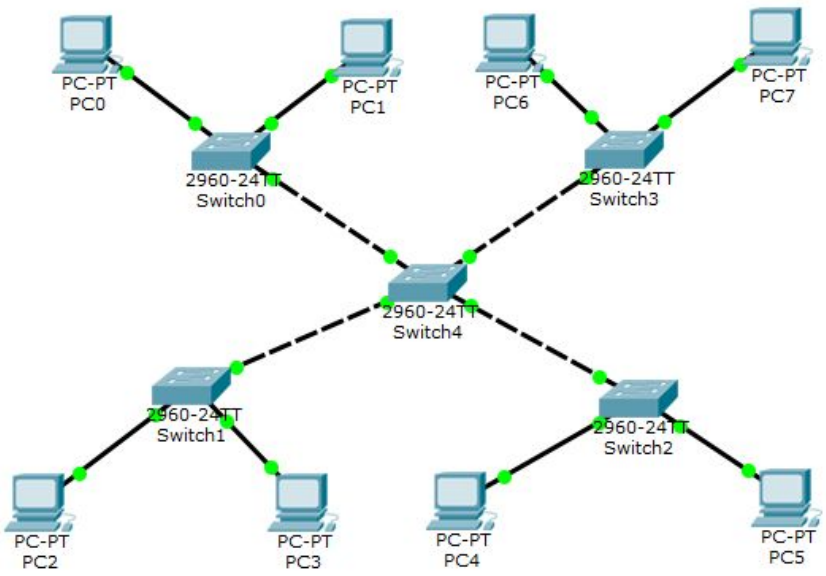


Рис. 1.1. Модель сети Ethernet

4. Сохраним созданную топологию, используя команду Save в меню File.
5. Откроем окно свойств устройства PC0, щелкнув левой кнопкой мыши на его изображении. Перейдем на вкладку *Desktop* и откроем командную строку, нажав на *Command Prompt* (кнопка «*run*»).
6. Для вывода списка доступных команд необходимо в командной строке ввести ? и нажать Enter.
7. Конфигурирование компьютера осуществляется с помощью команды *ipconfig*. Например, чтобы устройству PC0 установить сетевой адрес

192.168.1.2 и задать маску 255.255.255.0 в командной строке необходимо ввести:

ipconfig 192.168.1.2 255.255.255.0

8. Для проверки назначенных сетевого адреса и маски в командной строке нужно еще раз ввести *ipconfig*. Появится сообщение о заданных сетевых параметрах устройства:

   FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80:230:A3FF:FEAA:BD12

   IP Address.....: 192.168.1.2

   Subnet Mask.....: 255.255.255.0

   Default Gateway.....: 0.0.0.0

9. IP адрес и маску сети можно также задать, используя графический интерфейс устройства. Для этого в окне свойств на вкладке Desktop необходимо выбрать IP Configuration. Откроется окно, показанное на рис. 1.2. Сетевой адрес вводится в поле IP Adress, а маска – в поле Subnet Mask. Переключатель способа назначения IP адреса должен находится в положении Static.

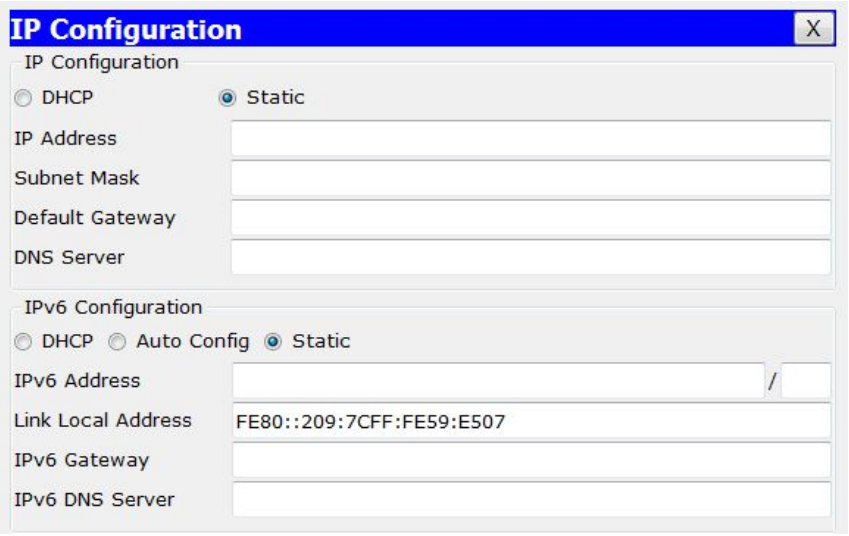


Рис. 1.2. Окно настроек «IP Configuration»

10. Аналогично для всех остальных компьютеров назначим адреса, используя один из выше приведенных способов. Сетевые адреса

устройств и маска подсети приведены в табл. 1.1.

Таблица 1.1. Сетевые параметры компьютеров

Имя компьютера	IP адрес	Маска подсети
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0
PC4	192.168.1.6	255.255.255.0
PC5	192.168.1.7	255.255.255.0
PC6	192.168.1.8	255.255.255.0
PC7	192.168.1.9	255.255.255.0

11. Проверить правильность сетевых настроек устройств и работоспособность сети можно с помощью команды *ping*. Для этого необходимо открыть командную строку устройства, ввести *ping* и IP адрес другого сетевого устройства. Например, зайдем на компьютер PC0 и пропингуем компьютер PC1. Ниже представлены результаты выполнения команды *ping*:

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:

Packets: Sent = 4, Received = 4, Lost =0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

Таким образом, если устройства сети сконфигурированы правильно, можно пропинговать с каждого компьютера любой другой.

12. В среде Packet Tracer существует возможность проследить движение пакетов различных сетевых протоколов с помощью режима симуляции. Для перехода в режим симуляции нужно нажать на кнопку Simulation Mode в правом нижнем углу рабочего пространства либо комбинацию клавиш Shift+S.

Справа от рабочей области откроется окно Simulation Panel (рис. 1.3), в верхней части которого находится область событий Event List (область 3) и кнопка очистки списка событий Reset Simulation. Управление воспроизведением осуществляется с помощью кнопок Play Controls. Так для перехода к следующему событию нужно нажать кнопку «Capture / Forward» (2). В нижней части окна находится фильтр протоколов (1).

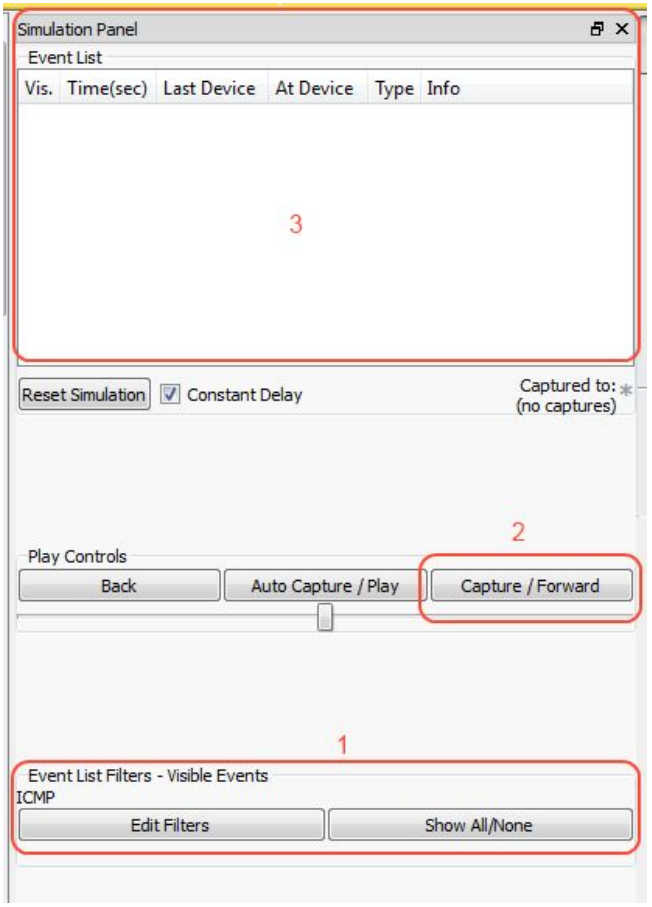


Рис. 1.3. Интерфейс симулятора

13. С узла PC1 пропингуем узел PC3. Из предложенного для исследования списка протоколов выберем только протокол ICMP, чтобы исключить случайный трафик между узлами. Откроем командную строку устройства PC1, введем *ping* и IP адрес сетевого устройства PC3. После чего на узле PC1 образуется пакет («конвертик») (рис. 1.4).

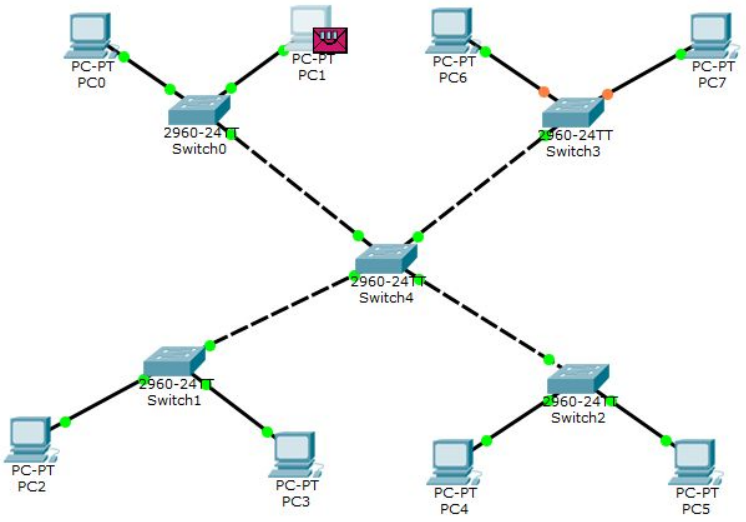


Рис. 1.4. Создание запроса в режиме симуляции

Так же в поле Event List появится данный пакет, с указанием его типа (ICMP) и источника формирования (рис. 1.5).

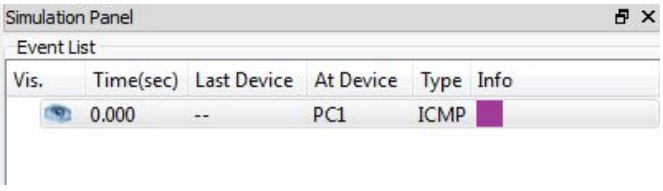


Рис. 1.5. Мониторинг работы протоколов

Для получения подробной информации о пакете нужно щелкнуть на нем левой кнопкой мыши. На вкладке OSI Model можно увидеть на каком уровне сетевой модели OSI был сформирован пакет и какие

уровни он пройдет для передачи на следующий узел (рис. 1.6). На вкладке Outbound PDU Details отображается структура пакета (рис. 1.7).

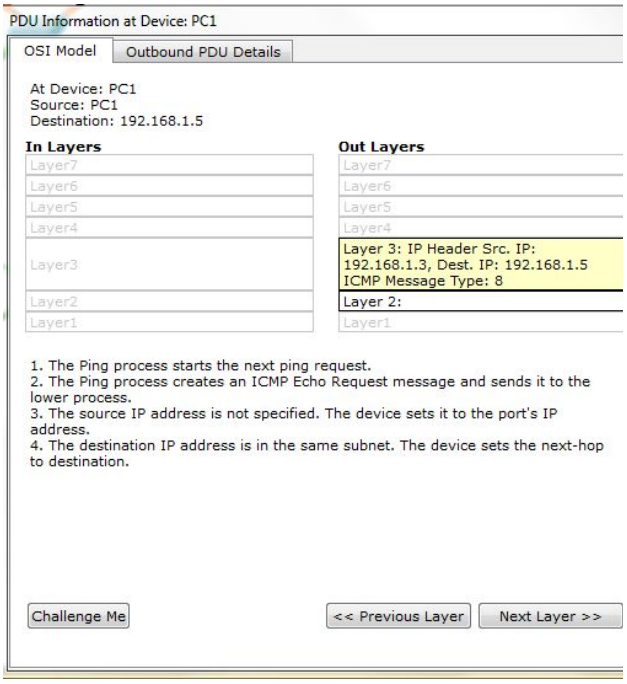


Рис. 1.6. Пакет на уровнях модели OSI

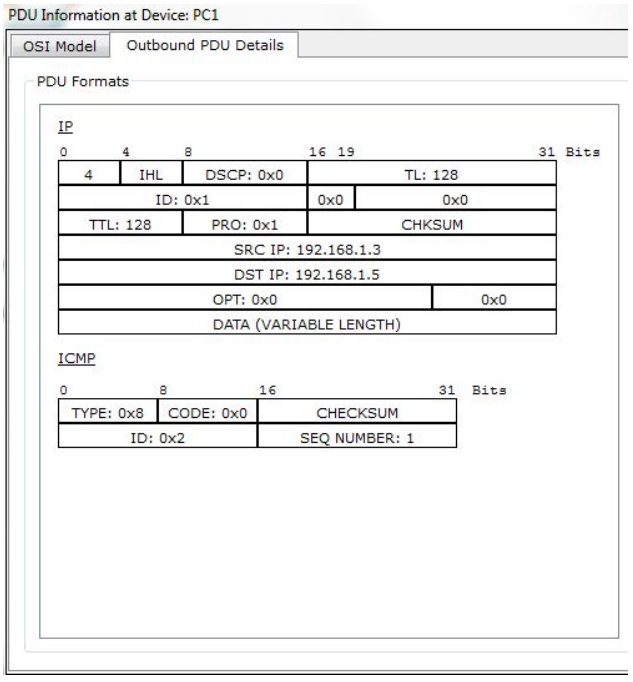


Рис. 1.7. Структура пакета

14. Для запуска пакета в сеть нужно нажать кнопку «Capture / Forward» в окне Simulation Panel. Пакет перейдет на коммутатор Switch0, поскольку это единственное сетевое подключение узла PC1. Коммутатор Switch0 пересылает пакет на коммутатор Switch4. В свою очередь, коммутатор Switch4 пересылает пакет на коммутатор Switch1, после чего Switch1 посылает передаваемый пакет на узел PC3. Получив пакет, PC3 определяет, что он предназначен ему и, сформировав ответ, посылает пакет на PC1.

После того как PC1 получил ответный пакет от PC3, в окне командной строки появляется следующая запись, сообщающая об успешном прохождении эхо-запроса:

PC>ping 192.168.1.5

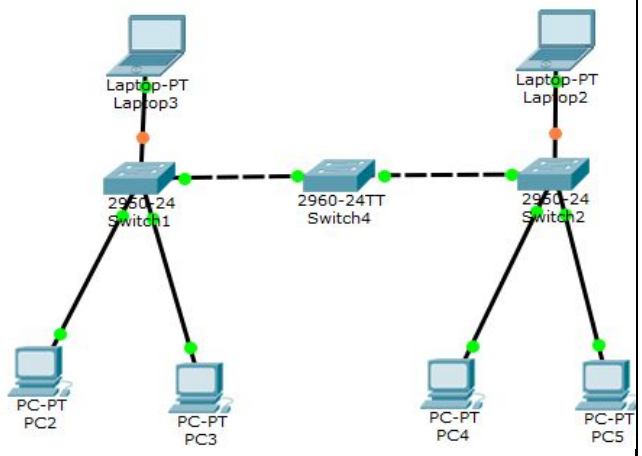
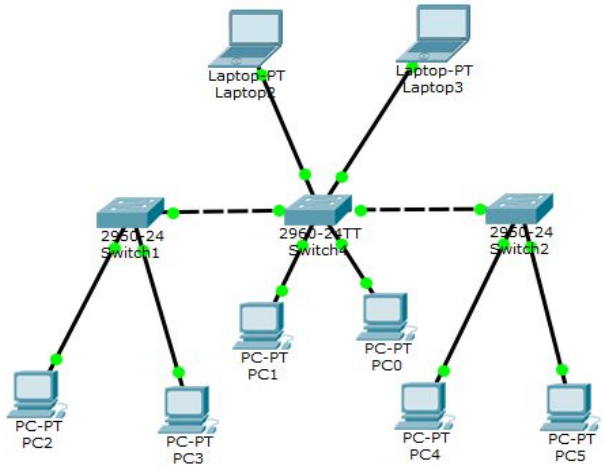
Pinging 192.168.1.5 with 32 bytes of data:

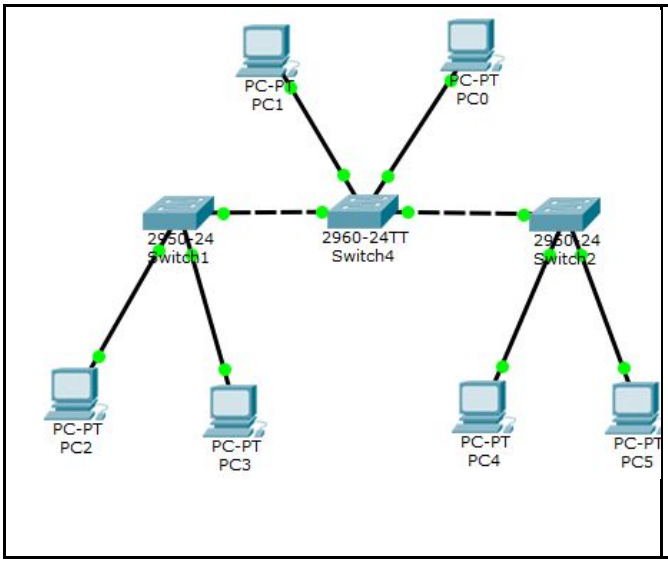
Reply from 192.168.1.5: bytes=32 time=7ms TTL=128

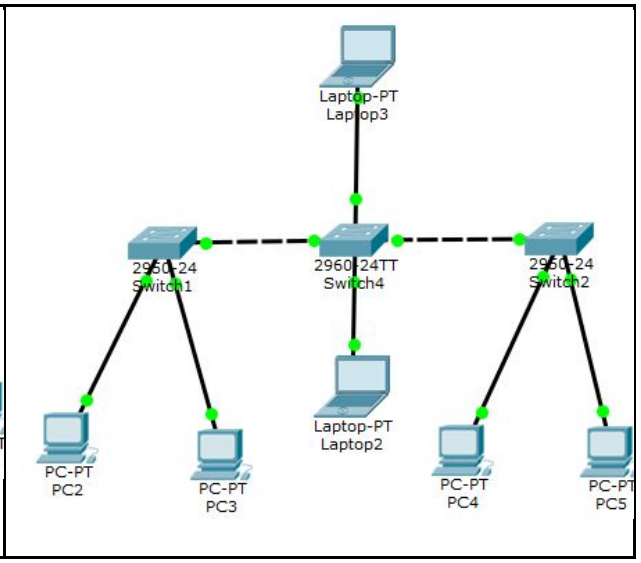
Задание

1. Создать топологию сети согласно заданному варианту (табл. 1.2). Во всех вариантах в качестве коммутаторов использовать Switch 2960.
2. Назначить компьютерам IP адреса согласно заданному диапазону адресов (табл. 1.3). Сетевая маска для всех устройств 255.255.255.0.
3. Присвоить всем оконечным узлам разные имена.
4. Проверить настройки каждого оконечного узла (команда ipconfig).
5. Проверить все соединения между компьютерами (команда ping).
6. В режиме симуляции отправить эхо-запрос (команда ping) с PC3 на PC5. Проследить движение пакета ICMP.

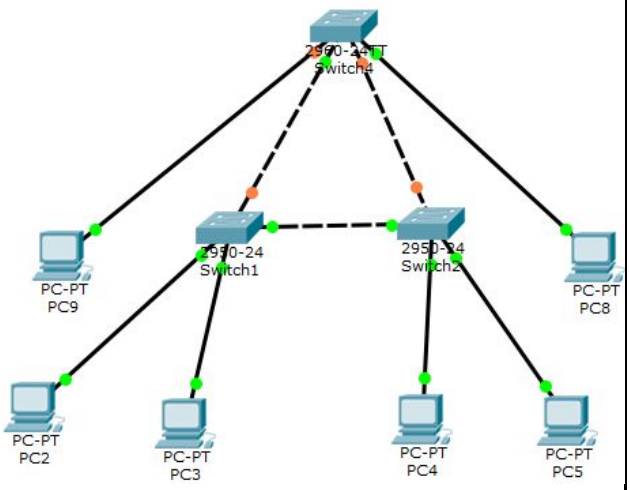
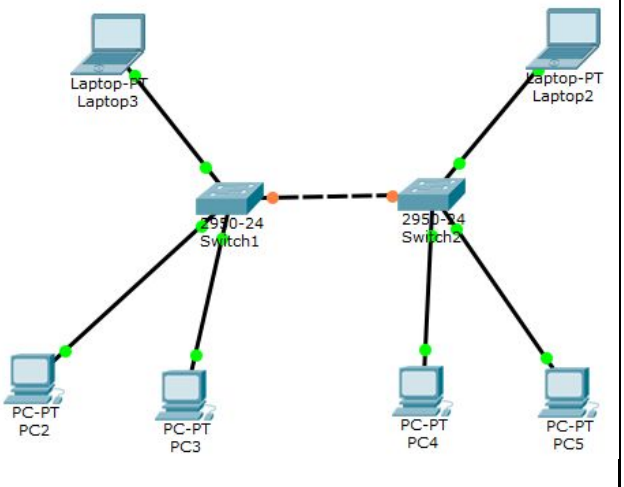
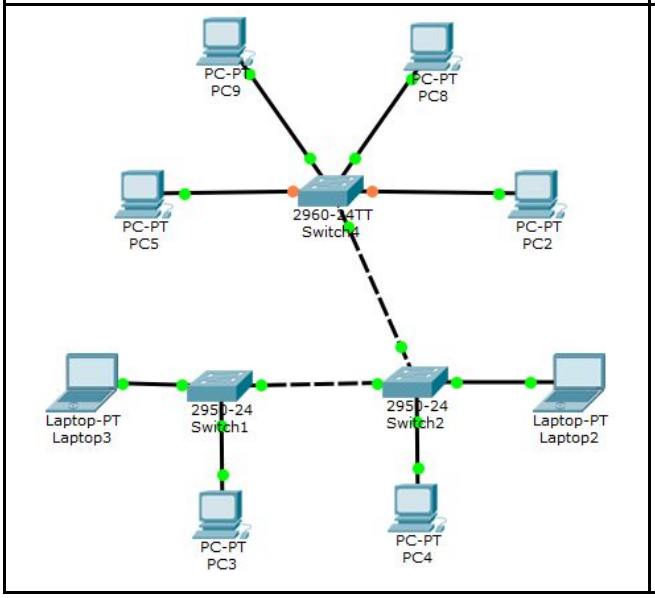
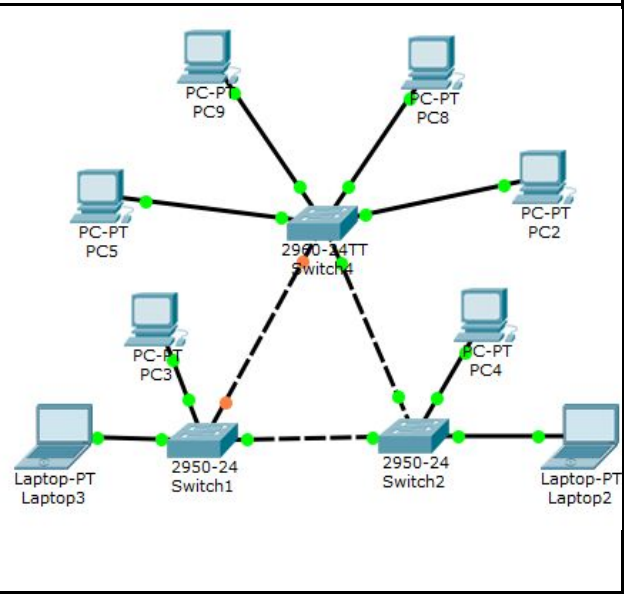
Таблица 1.2. Варианты заданий топологии сети

Вариант 1	Вариант 2
	
Вариант 3	Вариант 4





Продолжение табл. 1.2

Вариант 5	Вариант 6
	
Вариант 7	Вариант 8
	

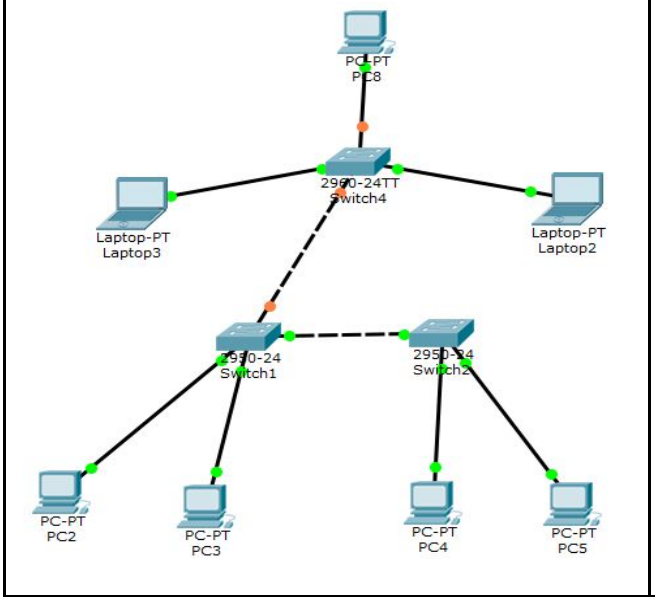
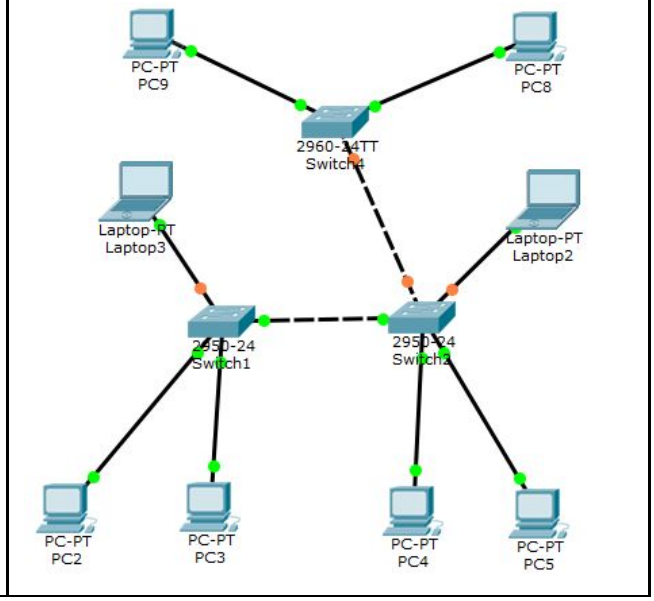
Вариант 9	Вариант 10
	

Таблица 1.3. Варианты диапазонов адресов

№ варианта	**1**	**2**	**3**	**4**	**5**
Диапазон адресов	112.168.5.15 112.168.5.25	13.18.0.45 13.18.0.55	152.164.8.75 152.164.8.85	12.208.6.15 12.208.6.25	122.8.85.45 122.8.85.55
№ варианта	**6**	**7**	**8**	**9**	**10**
Диапазон адресов	144.18.9.15 144.18.9.25	133.73.9.60 133.73.9.69	155.38.0.0 155.38.0.9	12.208.6.15 12.208.6.25	212.28.68.15 212.28.68.25

ЛАБОРАТОРНАЯ РАБОТА 2
Расчет подсетей IPv4

IP адрес – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. IPv4 адрес состоит из 32 битов, которые поделены на 4 части по 8 бит соответственно (эти части называются октетами).

Примеры IP адресов:

217.20.147.94 = 11011001.00010100.10010011.01011110

172.16.2.15 = 10101100.00010000.00000010.00001111

178.68.128.168 = 10110010.01000100.10000000.10101000

Из этих 32 битов часть относится к адресу хоста, которому принадлежит этот IP адрес, а другая часть относится к адресу сети, в которой находится этот хост. Первая часть (слева направо) IP адреса обозначает адрес сети, а вторая часть (оставшиеся биты) – адрес хоста. Чтобы узнать, сколько битов относится к адресу сети, надо воспользоваться маской сети.

Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet – InterNIC (Internet Network Information Center). Номер узла в протоколе IP назначается независимо от локального адреса узла.

Маска подсети – битовая маска, определяющая, какая часть IP адреса узла сети относится к адресу сети, а какая – к адресу самого узла в этой сети (при этом, в отличие от IP адреса, маска подсети не является частью IP пакета). Маска сети состоит из 32 битов, но в отличие от IP адреса, в ней единицы и нули не могут перемешиваться. В маске сети биты равные 1 определяют адрес сети, а равные 0 отведены под адреса хостов.
Примеры масок сети:

255.255.255.0 = 11111111.11111111.11111111.00000000
255.0.0.0 = 11111111.00000000.00000000.00000000
255.255.240.0 = 11111111.11111111.11110000.00000000
255.255.255.128 = 11111111.11111111.11111111.10000000

Иногда, маска сети записывается кратко в виде «префикса маски». Число в префиксе обозначает количество бит относящихся к адресу сети.
Пример:

/16 = 11111111.11111111.00000000.00000000 = 255.255.0.0
/24 = 11111111.11111111.11111111.00000000 = 255.255.255.0
/26 = 11111111.11111111.11111111.11000000 = 255.255.255.192

Чтобы узнать, какая часть IP адреса относится к порции сети, необходимо выполнить бинарную логическую операцию AND (И) IP адреса и маски сети. Операция заключается в сравнении двух битов, причем только в одном случае бинарная операция дает единицу на выходе – в случае сравнения двух единиц. В остальных случаях логическая операция «И» дает на выходе 0. Результаты сравнения логической операцией «И» двух битов:

1 AND 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

В каждой IPv4 сети есть широковещательный адрес (адрес для пересылки данных всем узлам в сети, его значение всегда равно последнему адресу в сети) и адрес сети (его значение всегда равно первому адресу в сети).

Рассчитать количество узлов для каждой сети можно путем анализа ее маски. Если отнять количество битов, используемых сетевой частью, то получится количество битов, используемых для узлов. Тогда количество узлов в подсети = $2^n - 2$, где n – это количество свободных бит (нулей) в порции хоста, а «-2» – это вычет адреса сети и широковещательного адреса.

Количество подсетей сети = 2^n, где n – это количество занятых бит от порции хоста.

Практическая часть

Пример 1. Определить адрес сети, если IP адрес узла 192.168.10.10, а маска подсети 255.255.255.0.

Переводим IP адрес из десятичной системы счисления в двоичную систему: 192.168.10.10 = 110000000.10101000.00001010.00001010

Переводим маску сети из десятичной системы счисления в двоичную систему: 255.255.255.0 = 11111111.11111111.11111111.00000000

Складываем IP адрес с маской с помощью логической операции «И».

110000000.10101000.00001010.00001010 (IP адрес)

И

11111111.11111111.11111111.00000000 (Маска)

=

110000000.10101000.00001010.00000000 (Адрес сети)

Переводим адрес сети из двоичной системы счисления в десятичную систему, и получаем 192.168.10.0 адрес сети в десятичном виде с маской 255.255.255.0. Единицы в маске указывают на часть сетевого адреса (110000000.10101000.00001010), а нули – на часть адреса хоста (00001010).

Пример 2. Определить адрес сети, если IP адрес узла 172.30.239.145, а маска подсети 255.255.192.0.

Переводим IP адрес из десятичной системы счисления в двоичную систему: 172.30.239.145 = 10110100.00100010.11101111.11101111

Переводим маску сети из десятичной системы счисления в двоичную систему: 255.255.192.0 = 11111111.11111111.11000000.00000000

Складываем IP адрес с маской с помощью логической операции «И».

10110100.00100010.11101111.11101111 (IP адрес)

И

11111111.11111111.11000000.00000000 (Маска)

=

10110100.00100010.11000000.00000000 (Адрес сети)

Переводим адрес сети из двоичной системы счисления в десятичную систему, и получаем 172.30.192.0 адрес сети в десятичном виде с маской 255.255.192.0.

Проанализировав эти два примера, можно увидеть, что если маска подсети имеет в октете десятичное значение 255, результатом всегда будет исходное значение этого октета. Если маска подсети имеет в октете десятичное значение 0, результатом для этого октета всегда будет 0.

Пример 3. Определить максимальное количество узлов в сети с маской 255.255.192.0.

Поскольку маска подсети равна 255.255.192.0, то префикс будет /18 (т.е. 18 бит для сетевого адреса). IPv4 адрес содержит 32 бита. Значит для узловой части остается 32 – 18 = 14 бит . Исходя из этого максимальное количество узлов в данной сети равно

$2^{14} – 2 = 16384 – 2 = 16382$ узла

Пример 4. Определить какое количество подсетей с маской 255.255.240.0 можно создать в сети маской 255.255.0.0.

Маска сети 255.255.0.0 или /16

Маска подсети 255.255.240.0 или /20

Количество бит у маски сети 16, а у маски подсети 20. Разница составляет 4 бита. Следовательно, можно создать $2^4 = 16$ подсетей.

Задание

1. В соответствии с вариантом по заданным IPv4 адресу и маске подсети определить следующие параметры:
    a. Адреса сетей А и Б.

b. Широковещательные адреса сетей А и Б.
c. Максимальное количество узлов в сетях А и Б.
d. Диапазон доступных адресов узлов в сетях А и Б.
e. Количество возможных подсетей Б в сети А.

Номер варианта	**IP адрес**	**Маска сети А**	**Маска сети Б**
1	128.107.0.55	255.255.0.0	255.255.255.0
2	192.135.250.180	255.255.255.0	255.255.255.248
3	10.101.99.228	255.0.0.0	255.255.128.0
4	156.56.3.64	255.192.0.0	255.255.0.0
5	81.16.190.64	255.255.128.0	255.255.255.0
6	91.19.35.13	255.255.224.0	255.255.255.224
7	190.15.157.6	255.0.0.0	255.255.192.0
8	65.16.16.182	255.255.0.0	255.255.224.0
9	125.18.19.16	255.255.240.0	255.255.255.0
10	14.196.168.26	255.255.248.0	255.255.255.248

2. Заполнить таблицу

Параметр	**Сеть А**	**Сеть Б**
Маска сети		
Сетевой адрес		
Широковещательный адрес сети		
Адрес IPv4 первого узла в сети		

Адрес IPv4 последнего узла в сети		
Количество узлов в сети		
Количество возможных подсетей Б в сети А		

3. Создать в среде Packet Tracer сеть А, в которой необходимо расположить три стационарный ПК, ноутбук и один коммутатор Switch 2960 25TT
4. Всем оконечным узлам задать IP адреса сети А:
    a. ПК1 – третий адрес сети А.
    b. ПК2 – четвертый адрес сети А.
    c. ПК3 – пятый адрес сети А.
    d. Ноутбук – последний адрес сети А.
5. Всем оконечным узлам задать соответствующие маски подсети.
6. Проверить настройки каждого оконечного узла командой *ipconfig*.
7. Проверить работоспособность сети (команда *ping*).

ЛАБОРАТОРНАЯ РАБОТА 3

Разбиение сети на одинаковые подсети

Бесклассовая адресация CIDR (Classless Inter-Domain Routing) – метод IP адресации, позволяющий гибко управлять пространством IP адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

Подсети позволяют создавать несколько логических сетей в пределах одной сети класса A, B или C. На первых порах метод CIDR рассматривался как способ распределения провайдером Internet между клиентами IP адресов в виде диапазонов IP-адресов (называемых блоками), а не выделения адреса некоторого класса. Обычно Internet-провайдер выделяет своим клиентам адреса определенных классов, что приводит к некоторой избыточности в одном месте и к дефициту в другом. Обратившись к технологии CIDR, провайдеры получили возможность «нарезать» блоки из выделенного им адресного

пространства, которые оптимально подходят под требования каждого клиента, оставляя в то же время возможность его будущего беспроблемного роста.

Каждый канал передачи данных в сети должен иметь уникальный идентификатор сети, при этом каждый узел в канале должен быть членом одной и той же сети. Если разбить основную сеть на небольшие подсети, это позволит создать сеть взаимосвязанных подсетей. Каждый канал передачи данных в этой сети будет иметь уникальный идентификатор сети или подсети. Любое устройство или шлюз, соединяющее n сетей или подсетей должно иметь n уникальных IP адресов по одному для каждой из взаимосвязанных сетей или подсетей.

Разделение сети на подсети выполняется путем расширения маски сети за счет битов, определяющих идентификатор узла в адресе. Это позволяет создавать идентификатор подсети.

Практическая часть

Пусть задана сеть 74.126.205.0 с сетевой маской 255.255.255.0. Необходимо создать 4 подсети.

Вычисляем количество бит в основной маске необходимых для создания подсетей. Т.к. сетей нужно 4, т.е. 2^2, значит будет заимствовано 2 бита у основной маски сети

74.126.205.0 - 01001010.01111110.11001101.00000000

255.255.255.192 - 11111111.11111111.11111111.11000000

Расширение маски до значения 255.255.255.192 произошло за счет двух бит исходной части узла в адресе, которые были использованы для создания подсетей. Идентификатор узла теперь содержит шесть оставшихся бит, поэтому каждая подсеть может содержать 64 (2^6) адреса узлов, 62 из которых фактически могут быть присвоены устройствам, поскольку идентификаторы узлов не могут состоять только из единиц или только из нулей. С учетом всех изложенных факторов созданы подсети, представленные в таблице:

Подсеть	**Подсеть**
74.126.205.0	01001010.01111110.11001101.00000000

74.126.205.64	01001010.01111110.11001101.01000000
74.126.205.128	01001010.01111110.11001101.10000000
74.126.205.192	01001010.01111110.11001101.11000000

Технология разделения на подсети в данном примере позволила создать четыре подсети. Каждая подсеть может поддерживать до 62 адресов узлов. Из этого можно сделать следующий вывод: чем больше битов используется для маски подсети, тем больше доступно подсетей. Однако чем больше доступно подсетей, тем меньше адресов узлов доступно в каждой подсети.

Проверим работоспособность данной сети.

1. Создадим в среде Packet Tracer топологию, содержащую один роутер Generic Router-PT-Empty (Router1), четыре коммутатора Switch 2960-24TT (Switch0 – Switch3) и 8 ПК (PC0 – PC7).
2. Добавим четыре Gigabit Ethernet-модуля PT-ROUTER-NM-1CGE в роутер. Для этого откроем свойства Router1, на вкладке Physical на модели роутера нажмем кнопку питания для выключения, выберем указанный модуль подключения, установим четыре таких модуля в свободные слоты и включим роутер.
3. Компьютеры с коммутаторами соединим витой парой. Порты подключения – FastEthernet. Коммутаторы с роутером также соединим витой парой. Порты подключения – GigabitEthernet.
4. Выполним настройку элементов сети. В каждой подсети зарезервируем для роутера первый доступный IP-адрес, а компьютерам будем задавать второй и последний доступные адреса. Сетевая маска для всех устройств – 255.255.255.192.
5. Для настройки компьютера PC0, который относится к первой подсети, откроем его свойства. На вкладке Desktop выберем опцию IP Config и для режима получения IP-адреса Static в поле IP Address введем второй доступный адрес подсети – 74.126.205.2, в поле Subnet Mask – сетевую маску 255.255.255.192, а в поле Default Gateway (Шлюз по умолчанию) укажем первый доступный IP-адрес подсети, зарезервированный для роутера, т.е. 74.126.205.1.

Компьютер PC1 настраивается аналогично, но в поле IP Address введем последний доступный адрес подсети – 74.126.205.62.

6. Зададим IP адреса для второй подсети: компьютер PC2 – 74.126.205.66, компьютер PC3 – 74.126.205.126, шлюз – 74.126.205.65; для третьей подсети: компьютер PC4 – 74.126.205.130, компьютер PC5 – 74.126.205.190, шлюз – 74.126.205.129; компьютер PC6 – 74.126.205.194, компьютер PC7 – 74.126.205.254, шлюз – 74.126.205.193.
7. Выполним настройку роутера, которая в данном случае будет заключаться в отдельной сетевой настройке каждого Gigabit Ethernet-модуля к которым подключены коммутаторы подсетей. Откроем свойства роутера, перейдем на вкладку Config и в подменю INTERFACE выберем модуль GigabitEthernet0/0, к которому подключен коммутатор первой подсети 74.126.205.0. В поле IP Address первый зарезервированный IP адрес подсети – 74.126.205.1, а в поле Subnet Mask – сетевую маску 255.255.255.192. После чего включим данный модуль – Port Status установим в On. Остальные три модуля настраиваются аналогично – в поле IP Address указывается первый зарезервированный IP адрес подсети, коммутатор которой подключен к модулю.
8. Проверим работоспособность сети. Зайдем на компьютер PC0 и пропингуем компьютер PC7. Для этого откроем свойства компьютера PC0, на вкладке Desktop выберем опцию Command Promt и в открывшемся окне в командной строке введем команду ping и IP адрес компьютера PC7.

Задание

1. В соответствии с вариантом по заданным IP адресу и маске разделить заданную сеть на четыре равные подсети.

Номер варианта	Адрес сети	Маска сети
1	129.138.60.0	255.255.252.0
2	13.140.208.0	255.255.240.0

3	109.88.38.0	255.255.254.0
4	48.185.104.0	255.255.248.0
5	144.29.236.0	255.255.252.0
6	78.97.205.0	255.255.255.0
7	192.199.140.0	255.255.252.0
8	87.247.176.0	255.255.240.0
9	191.197.206.0	255.255.254.0
10	17.53.208.0	255.255.248.0

2. Выполнить расчет и заполнить таблицу.

	А	**Б**	**В**	**Г**
Сетевой адрес подсети				
Маска подсети				
Префикс маски подсети				
Широковещательный адрес подсети				
Диапазон доступных адресов узлов в подсети				
Количество узлов в подсети				

3. Создать сеть в среде Packet Tracer. Всем интерфейсам маршрутизатора задать первые допустимые IP адреса подсети, первым узлам в подсети задать вторые допустимые IP адреса. Вторым узлам в подсети задать последние допустимые IP адреса.

ЛАБОРАТОРНАЯ РАБОТА 4

Разбиение сети на подсети переменной длины

Цель работы

- Научиться работать с подсетями.
- Научиться разделять сеть на подсети переменной длины.
- Научиться эффективно использовать адресное пространство сети.

Краткие сведения из теории

Для эффективного использования адресного пространства существует метод *маски подсети переменной длины* (англ. Variable Length Subnet Masking – VLSM). Маски подсети переменной длины обеспечивают возможность создания более одной маски подсети в переделах одной сети, возможность разбивать на подсети уже разбитые на подсети группы IP адресов. Методы CIDR и VLSM позволяют рекурсивно делить порции адресного пространства на небольшие части. Основное различие между ними в том, что при использовании маски подсети переменной длины рекурсия выполняется на адресном пространстве, выделенном организации ранее. При этом схема деления пространства остается спрятана внутри организации.

В технологии CIDR разделения на подсети во всех подсетях используется одна и та же маска подсети. Это означает, что каждая подсеть содержит одинаковое количество доступных адресов узлов. Иногда это может понадобиться, однако в большинстве случаев использование одинаковой маски подсети для всех подсетей приводит к неэкономному распределению адресного пространства.

VLSM позволяет использовать различные маски для каждой подсети, что дает возможность более рационально распределять адресное пространство.

Допустим для примера, что имеется сеть класса C с адресом 192.214.11.0, и ее необходимо разделить на три подсети. В одной подсети должно быть около 100 узлов, а в двух других – по 50. Исключая два адреса, 0 (номер сети) и 255 (широковещательный адрес для сети) теоретически доступно 256 адресов узлов для сети класса C, т.е. с 192.214.11.0 до 192.214.11.255. Очевидно, что разбить такую сеть на

подсети с требуемым количеством узлов без использования VLSM невозможно.

Чтобы определить параметры подсети в сети 192.214.11.0, сначала необходимо определить маску сети, которая для обычной сети класса С будет представлена в виде 255.255.255.0. Для разделения сети класса С с адресом 192.214.11.0 на подсети можно использовать несколько масок вида 255.255.255.X. Маска, начиная со старшего (самого левого) бита, должна иметь непрерывный ряд единиц и оканчиваться нулями.

До появления VLSM сети обычно делились лишь простыми масками. В этом случае был бы выбор применить маску 255.255.255.128 и разбить адресное пространство на две подсети по 128 узлов в каждой или разбить его маской 255.255.255.192 на четыре подсети по 64 хоста в каждой. Однако ни одна из этих процедур не соответствует предъявленным требованиям получить сегмент сети размером 100 узлов и еще два сегмента по 50 узлов в каждом.

Прибегнув к использованию масок переменной длины, можно выполнить поставленную задачу. Во-первых, разделим сеть 192.214.11.0 на две подсети маской 255.255.255.128. Получим две подсети по 128 узлов в каждой. Эти две подсети будут представлены адресами 192.214.11.0 (от .0 до .127) и 192.214.11.128 (от .128 до .255). Затем вторую подсеть с адресом 192.214.11.128 разобьем еще на две подсети с помощью маски 255.255.255.192 – получим две подсети по 64 адреса в каждой: подсети 192.214.11.128 (адреса от .128 до 191) и 192.214.11.192 (адреса от .192 до 255).

Не смотря на то, что при использовании VLSM длину маски можно изменять произвольно, существует одно ограничение. Максимальная длина маски – 30 единиц. Данное ограничение связано с тем, что при длине маски 31 разряд под номер узла остается один разряд. С помощью одного разряда можно пронумеровать два узла. Но стандарт предусматривает, что два номера всегда заняты – это номер сети (подсети) и широковещательный адрес.

Практическая часть

Пусть задана сеть *74.126.205.0* с сетевой маской 255.255.255.0. Разработаем схему разделения на 4 подсети с применением VLSM с учетом того, что подсеть А должна содержать 14 узлов, подсеть Б – 28 узлов, подсеть В – 15 узлов, подсеть Г – 5 узлов.

Определяем, какую маску подсети следует использовать, чтобы получить требуемое количество узлов.

Сеть А: необходимо вместить 14 узлов. Ближайшее подходящее значение $2^n = 16$, значит количество бит узловой части $n = 4$, количество бит для идентификатора подсети будет 8 – 4 = 4 бита. Следовательно, маска этой подсети будет 255.255.255.240 или /28.

Сеть Б: необходимо вместить 28 узлов. Ближайшее подходящее значение $2^n = 32$, значит количество бит узловой части $n = 5$, а количество бит для идентификатора подсети будет 8 – 5 = 3 бита. Следовательно, маска этой подсети будет 255.255.255.224 или /27.

Сеть В: необходимо вместить 15 узлов. Ближайшее подходящее значение $2^n = 16$, но т.к в каждой сети должны быть широковещательный адрес и адрес подсети, то 16 для этой подсети будет недостаточно. Следовательно, подбираем $2^n = 32$. Количество бит узловой части $n = 5$, а количество бит для идентификатора подсети будет 8 – 5 = 3 бита. Следовательно, маска этой подсети будет 255.255.255.224 или /27.

Сеть Г: необходимо вместить 5 узлов. Ближайшее подходящее значение $2^n = 8$, значит количество бит узловой части $n = 3$, а количество бит для идентификатора подсети будет 8 – 3 = 5 бит. Следовательно, маска этой подсети будет 255.255.255.248 или /29.

VLSM-разбиение на подсети похоже на традиционное тем, что в нем для создания подсетей заимствуются биты. Формулы расчета количества возможных подсетей и количества узлов в каждой подсети также применимы. Различие состоит в том, что разбиение на подсети выполняется в несколько этапов. При использовании VLSM сеть сначала разбивается на подсети, а затем подсети снова делятся на подсети. Этот процесс может повторяться много раз для создания подсетей различного

размера. Для начала отсортируем искомые подсети по количеству доступных узлов:

- *Сеть Б: 32 узлов*;
- *Сеть В: 32 узлов*;
- *Сеть А: 16 узлов*;
- *Сеть Г: 8 узлов*.

Графическое представления разбиения на подсети методом VLSM показано на рис. 4.1.

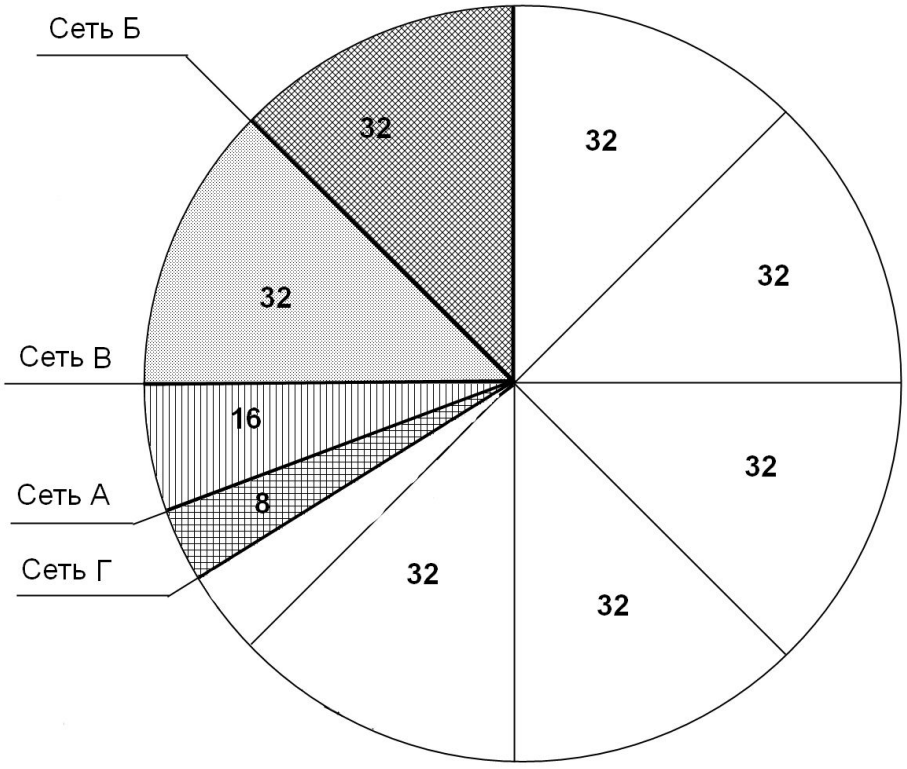


Рис. 4.1. Графическое представление разбиения на подсети методом VLSM

Далее разобьем нашу заданную сеть (в которой возможных 256 узлов) по 32 узла (наибольшая искомая подсеть). В образовавшихся подсетях количество бит идентификатора подсети равно 3, значит новые подсети будут выглядеть следующим образом:

*01001010.01111110.11001101.**000**00000*

*01001010.01111110.11001101.**001**00000*

*01001010.01111110.11001101.**010**00000*

*01001010.01111110.11001101.**011**00000*

*01001010.01111110.11001101.**100**00000*

*01001010.01111110.11001101.**101**00000*

*01001010.01111110.11001101.**110**00000*

*01001010.01111110.11001101.**111**00000*

Нам нужны только две первые подсети (для Б и В). Маска у этих подсетей будет 255.255.255.224 или /27

Для определения следующей подсети делим сеть *01001010.01111110.11001101.**010**00000* пополам (т.е заимствуем еще один бит у идентификатора подсети). Получаем две сети:

*01001010.01111110.11001101.**0100**0000*

*01001010.01111110.11001101.**0101**0000*

Первую из этих подсетей отводим для сети А с маской /28. Вторую делим еще раз пополам, т.е. заимствуем еще один бит у идентификатора подсети. Получаем еще две сети:

*01001010.01111110.11001101.**01010**000*

*01001010.01111110.11001101.**01011**000*

Первая из которых соответствует сети Г с маской /29.

Результат перевода значений найденных подсетей в десятичную форму представлен в табл. 4.1.

Таблица 4.1. Параметры подсетей

Имя	**Подсеть (2)**	**Подсеть (10)**	**Маска (10)**
Б	01001010.01111110.11001101.**000**00000	74.126.205.0	255.255.255.224
В	01001010.01111110.11001101.**001**00000	74.126.205.32	255.255.255.224
А	01001010.01111110.11001101.**0100**0000	74.126.205.64	255.255.255.240
Г	01001010.01111110.11001101.**01010**000	74.126.205.80	255.255.255.248

Для определения диапазона доступных узлов в посети необходимо сначала к номеру подсети прибавить единицу (это будет адрес первого

узла), а затем к номеру подсети прибавить количество доступных адресов (это будет адрес последнего узла). Результаты представлены в табл. 4.2.

Таблица 4.2. Диапазон доступных узлов

Имя	Подсеть	Маска	Диапазон доступных адресов
Б	74.126.205.0	255.255.255.224	74.126.205.1 - 74.126.205.30
В	74.126.205.32	255.255.255.224	74.126.205.33 - 74.126.205.62
А	74.126.205.64	255.255.255.240	74.126.205.65 - 74.126.205.78
Г	74.126.205.80	255.255.255.248	74.126.205.81 - 74.126.205.86

Метод VLSM разделения на подсети в данном примере позволил создать четыре подсети с заданным количеством узлов в каждой, а сеть тогда будет выглядеть, как показано на рис. 4.1.

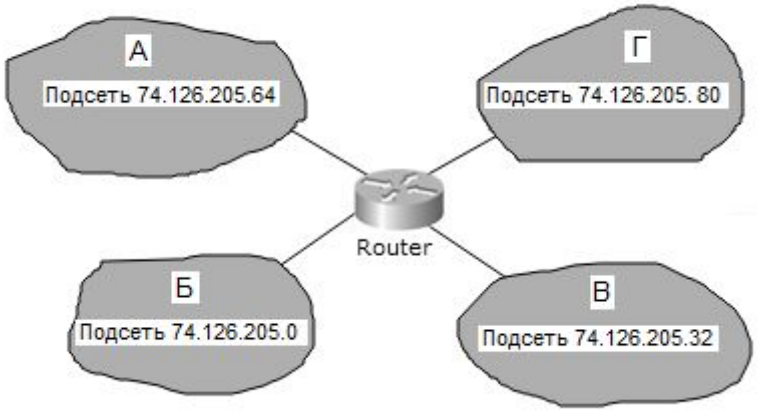


Рис. 4.2. Логическое представление разбиения сети методом VLSM

Создание сети, состоящей из четырех подсетей, и настройка сетевых компонентов в Packet Tracer аналогично описанному в предыдущей работе.

Задание

1. В соответствии с вариантом (таб. 4.3) по заданным IP адресу и маске подсети разделить заданную сеть на четыре подсети с учетом требуемого количества узлов с помощью метода VLSM.

Таблица 4.3. Варианты заданий

Номер варианта	**Адрес сети**	**Маска сети**	**Количество узлов в подсети**			
			А	**Б**	**В**	**Г**
1	126.198.0.0	255.254.0.0	155	255	86	161
2	192.200.0.0	255.248.0.0	72	104	130	109
3	10.192.0.0	255.252.0.0	73	55	133	106
4	156.168.0.0	255.248.0.0	92	180	105	102
5	81.176.0.0	255.248.0.0	89	158	171	60
6	91.184.0.0	255.252.0.0	80	100	64	159
7	190.128.0.0	255.254.0.0	99	63	155	61
8	65.48.0.0	255.248.0.0	120	130	92	145
9	125.192.0.0	255.240.0.0	65	94	59	189
10	14.160.0.0	255.224.0.0	50	258	140	107

2. Выполнить расчет и заполнить таблицу 4.4.

Таблица 3.3. Результаты вычислений

Имя подсети	**А**	**Б**	**В**	**Г**
Сетевой адрес подсети				
Маска подсети				
Префикс маски подсети				
Широковещательный адрес подсети				
Диапазон доступных адресов узлов в подсети				
Количество узлов в подсети				

3. Создать в среде Packet Tracer топологию сети.

4. Всем оконечным узлам задать IP адреса и маски из определенных ранее подсетей (А, Б, В, Г):
   - всем интерфейсам маршрутизатора задать первые допустимые IP адреса подсети;
   - первым узлам в подсети задать вторые допустимые IP адреса;
   - вторым узлам в подсети задать последние допустимые IP адреса.
5. Проверить настройки каждого оконечного узла командой *ipconfig*.
6. Проверить работоспособность сети (команда *ping*).

Содержание отчета

1. Расчет по нахождению параметров всех подсетей.
2. Изображение топологии сети.
3. Изображения *ipconfig* каждого оконечного узла.
4. Изображения команды *ping* между первым и остальными оконечными узлами.
5. Общие выводы по работе.

Контрольные вопросы

1. Какие формы записи маски вы знаете?
2. В чем суть метода VLSM?
3. Можно ли в локальной компьютерной сети применить VLSM?
4. Какова максимальная длина маски при использовании VLSM?
5. Как VLSM способствует экономному использованию адресного пространства?

ЛАБОРАТОРНАЯ РАБОТА 5
Настройка беспроводной сети в среде Packet Tracer

Цель работы

- Научиться организовывать беспроводную сеть.
- Научиться настраивать Wi-Fi точку доступа через Web-интерфейс.

- Научиться настраивать оконечные узлы сети.

Краткие сведения из теории

Беспроводная вычислительная сеть – вычислительная сеть без использования кабельной проводки, полностью соответствующая стандартам для обычных проводных сетей (например, Ethernet). В качестве носителя информации в таких сетях выступают радиоволны СВЧ-диапазона. В настоящее время для организации беспроводных сетей широко применяется стандарт IEEE 802.11 более известный как Wi-Fi.

Wi-Fi – торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от англ. Wireless Fidelity, которое можно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка, когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передает свой идентификатор сети с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с – наименьшая скорость передачи данных для Wi-Fi. Точка доступа организуется с помощью Wi-Fi-роутера.

Wi-Fi роутер – это устройство, которое подключается к сети интернет с помощью кабеля и передает соединение другим устройствам, например, ноутбуку или смартфону.

Методы ограниченного доступа в Wi-Fi сетях.

1. *Фильтрация MAC-адресов*. Данный метод не входит в стандарт IEEE 802.11. Фильтрацию можно осуществлять тремя способами:
   - точка доступа позволяет получить доступ станциям с любым MAC-адресом;
   - точка доступа позволяет получить доступ только станциям, чьи MAC-адреса находятся в доверительном списке;

- точка доступа запрещает доступ станциям, чьи MAC-адреса находятся в «черном списке»;

Наиболее надежным с точки зрения безопасности является второй вариант, хотя он не рассчитан на подмену MAC-адреса.

2. *Режим скрытого идентификатора SSID* (англ. Service Set IDentifier). Для своего обнаружения точка доступа периодически рассылает кадры-маячки (англ. beacon frames). Каждый такой кадр содержит служебную информацию для подключения и, в частности, присутствует SSID (идентификатор беспроводной сети). В случае скрытого SSID это поле пустое, т.е. невозможно обнаружение вашей беспроводной сети и нельзя к ней подключиться, не зная значение SSID.

Методы шифрования в Wi-Fi сетях.

1. *WEP-шифрование* (Wired Equivalent Privacy). Используется симметричный потоковый шифр RC4 (англ. Rivest Cipher 4), который достаточно быстро функционирует. На сегодняшний день WEP и RC4 не считаются криптостойкими. Основные недостатки:
   - использование для шифрования непосредственно пароля, введенного пользователем;
   - недостаточная длина ключа шифрования;
   - использование функции CRC32 для контроля целостности пакетов;
   - повторное использование векторов инициализации и др.
2. *TKIP-шифрование* (англ. Temporal Key Integrity Protocol). Используется тот же симметричный потоковый шифр RC4, но является более криптостойким.
3. *CKIP-шифрование* (англ. Cisco Key Integrity Protocol). Имеет сходства с протоколом TKIP. Создан компанией Cisco. Используется протокол CMIC (англ. Cisco Message Integrity Check) для проверки целостности сообщений.
4. *WPA-шифрование*. Вместо уязвимого RC4, используется криптостойкий алгоритм шифрования AES. Есть два режима:
   - Pre-Shared Key (WPA-PSK) – каждый узел вводит пароль для доступа к сети;

- Enterprise – проверка осуществляется серверами RADIUS.

5. *WPA2-шифрование* (IEEE 802.11i). Принят в 2004 году, а с 2006 года WPA2 должно поддерживать все выпускаемое Wi-Fi оборудование. В данном протоколе применяется RSN (что это: алгоритм, протокол?, нужно общее название) (англ. Robust Security Network, сеть с повышенной безопасностью). Основой является алгоритм AES. Для совместимости со старым оборудованием имеется поддержка TKIP и EAP (англ. Extensible Authentication Protocol) с некоторыми его дополнениями. Как и в WPA есть два режима работы: Pre-Shared Key и Enterprise.

   WPA и WPA2 имеют следующие преимущества:

   - ключи шифрования генерируются во время соединения, а не распределяются статически.
   - для контроля целостности передаваемых сообщений используется алгоритм Michael.
   - используется вектор инициализации существенно большей длины.

Стандарты Wi-Fi. Термин Wi-Fi не является техническим и активно применяется пользователями беспроводных сетей группы стандартов IEEE 802.11. Однако, более профессиональным является термин IEEE 802.11 и «английская буква», характеризующая определенную физическую спецификацию. На данный момент, наибольшее распространение получили следующие стандарты Wi-Fi, приведенные в табл. 1.1.

Таблица 1.1. Стандарты Wi-Fi

Стандарт	Год представления	Частота	Скорость (средняя/ максимальная)	Радиус действия (в помещении/ на открытом пространстве)
802.11-1997	1997	2,4 ГГц	0,9/2,0 Мбит/с	20/100 метров
802.11a	1999	5,0 ГГц	23/54 Мбит/с	35/120 метров
802.11b	1999	2,4 ГГц	4,3/11 Мбит/с	38/140 метров
802.11g	2003	2,4 ГГц	19/54 Мбит/с	38/140 метров

802.11n	2009	2,4 ГГц 5,0 ГГц	74/248 Мбит/с	70/250 метров
802.11y	2008	3,7 ГГц	23/54 Мбит/с	50/5000 метров

Практическая часть

1. Добавим на рабочее поле программы Packet Tracer стационарный компьютер и Wi-Fi роутер WRT300N. Компьютер с роутером соединим витой парой. Порт подключения компьютера FastEthernet, роутера – Ethernet.
2. Стандартный IP адрес современных беспроводных роутеров – 192.168.0.1 с маской – 255.255.255.0. Назначенные адрес и маску роутера можно проверить в окне свойств устройства на вкладке *Config* в подменю *LAN*.
3. Чтобы подключить компьютер к роутеру в окне свойств компьютера на вкладке *Desktop* выберем опцию *IP Configuration*. Для автоматического получения IP адреса переключатель способа назначения адреса установим в положение DHCP. Через некоторое время в соответствующих полях появятся IP адрес компьютера, маска сети и IP адрес шлюза.
4. Для отображения сетевых настроек откроем на компьютере командную строку (Desktop/Command Promt) и введем команду *ipconfig /all*. Результат выполнения команды приведен ниже:

   PC>ipconfig /all

   FastEthernet0 Connection:(default port)

   Physical Address.....: 00D0.9739.B139
   Link-local IPv6 Address.....: FE80::2D0:97FF:FE39:B139
   IP Address.....: 192.168.0.100
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.0.1
   DNS Servers.....: 0.0.0.0
   DHCP Servers.....: 192.168.0.1
   DHCPv6 Client DUID.....: 00-01-00-01-29-8D-D2-19-00-D0-97-39-B1-39
5. Чтобы проверить связь компьютера с роутером отправим эхо-запрос с компьютера, используя команду *ping*:

PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=2ms TTL=255
Reply from 192.168.0.1: bytes=32 time=0ms TTL=255
Reply from 192.168.0.1: bytes=32 time=0ms TTL=255
Reply from 192.168.0.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms

6. Откроем на вкладке Desktop в свойствах компьютера Web Browser. Введем в строку ввода URL IP адрес нашего роутера. Откроется окно запроса имени и пароля. По умолчанию на всех Wi-Fi роутерах установлено имя «admin» и пароль «admin». После их ввода переходим на страницу настройки роутера. Эту страницу также можно открыть через свойства роутера на вкладке GUI. Но в реальных условиях доступ к настройкам Wi-Fi роутера можно получить только через браузер подключенного к нему компьютера.

   На странице настройки роутера имеется несколько вкладок:

   а) На вкладке *Setup* настраивается входящее Интернет-соединение (Internet Setup), которое можно установить на получение динамических настроек (DHCP), статических и настроек PPPoe. Все эти настройки сообщает интернет провайдер. Так же на вкладке Setup можно настроить IP адрес роутера внутри локальной сети (Network Setup) и установки DHCP сервера (сервер автоматической раздачи IP адресов в сети), в роли которого также может выступать Wi-Fi роутер.

   б) На вкладке *Wireless* в подменю *Basic Wireless Setting* можно сконфигурировать установки беспроводной сети:

- Режим работы (Network Mode) – управление режимами скорости передачи данных;
- Идентификатор сети (Network Name (SSID)) – название беспроводной сети, трансляцию которого можно скрыть (SSID Broadcast – Disable);
- Standard Channel – устанавливает канал передачи данных;
- В подменю *Wireless Security* настраивается режим безопасности (Security Mode) беспроводной сети – выбирается способ шифрования (WEP, WPA, WPA2) и устанавливается пароль на подключение к сети;
- В подменю *Wireless MAC Filter* настраивается фильтрация по MAC-адресу – разрешение на подключение к беспроводной сети только определенных заранее известных устройств.

в) На вкладке *Access Restrictions* можно запретить доступ тому или иному приложению или протоколу.

г) На вкладке *Application and Gaming* пункт Port Forwarding служит для настройки так называемого проброса портов (технология трансляции сетевого адреса в зависимости от TCP/UDP-порта получателя).

д) На вкладке Administration можно настроить доступ к роутеру (имя, пароль, доступ по сети, доступ по Web интерфейсу)

На вкладке *Wireless* в подменю *Basic Wireless Setting* в поле идентификатора сети (SSID) введем имя сети LabRab. Режим безопасности в подменю *Wireless Security* установим WPA2 Personal. Алгоритм шифрования – AES. Пароль (Passphrase) должен содержать не менее 8 символов, в это поле введем, например, 11111111.

7. Подключим к нашей беспроводной сети ноутбук. В рабочую область программы поместим устройство Laptop. По умолчанию ноутбук не содержит модуль Wi-Fi. Для его установки необходимо открыть свойства Laptop, выбрать вкладку *Physical*, на модели ноутбука нажать кнопку питания для выключения, извлечь модуль подключения по локальной сети, на его место установить модуль Wi-Fi WPC300N и включить ноутбук. Затем перейти на вкладку *Config* в подменю

Wireless0. Переключатель IP Configuration должен быть в положении DHCP для автоматического получения IP адреса. В поле SSID введем имя нашей сети – LabRab. Переключатель аутентификации установим в положение WPA2-PSK и в поле PSK Pass Phrase введем установленный пароль 11111111. Ноутбук подключится к заданной беспроводной сети. Проверить подключение можно с помощью меню *PC Wireless* на вкладке *Desktop* свойств ноутбука. На вкладке *Connect* отображается список беспроводных сетей и основная информация о них (рис. 5.1). С помощью данного интерфейса также можно подключиться к беспроводной сети. Для этого нужно выбрать сеть, нажать кнопку *Connect* и в открывшемся окне указать тип шифрования и пароль.

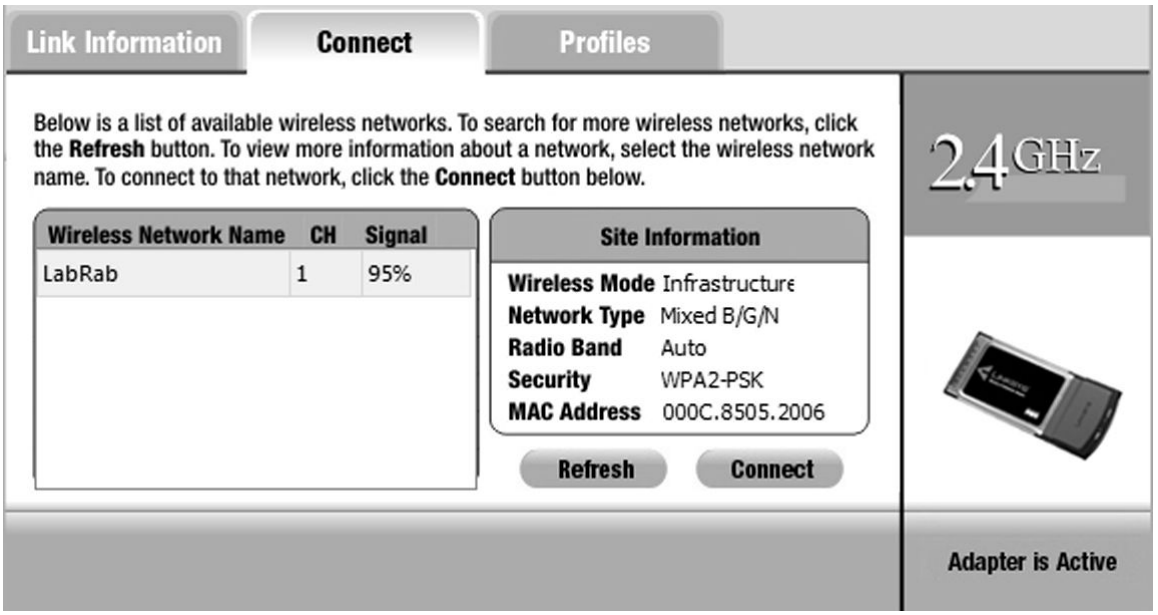


Рис. 5.1. Окно подключения к беспроводной сети

На вкладке *Link information* индикаторами отображается мощность сигнала и качество связи. Получить более детальную информации о сети можно нажав кнопку *More information*.

8. Другие оконечные устройства к Wi-Fi сети без широковещания SSID подключаются аналогично: в свойствах устройства на вкладке *Config* в подменю *Wireless0* нужно, как было описано выше, заполнить поля SSID, Authentication, IP Configuration.

Задание

1. Добавить в рабочую область Packet Tracer стационарный компьютер (PC-PT PC1) и Wi-Fi роутер (WRT300N) и соединить их прямым кабелем витая пара.
2. Через на Web интерфейс компьютера PC1 выполнить настройку Wi-Fi роутера в соответствии с заданным вариантом (табл. 5.1).
3. Изменить внутренний IP адрес роутера сети в соответствии с табл. 5.2. (При смене локального IP адреса роутера прерывается соединение с ПК, т.к. IP адреса этих устройств будут в разных сетях. Для восстановления подключения необходимо на PC зайти в утилиту *IP Configuration* выбрать *Static*, а потом *DHCP*. После этих действий ПК получит новый IP адрес с новым номером сети.)

Таблица 5.1. Варианты заданий коммутации WAN

Номер варианта	**Тип коммутации провайдера**	**Настройки провайдера для роутера**
1	Автоматические настройки	–
2	Статические настройки	Internet IP Address – 45.45.42.42 Subnet Mask – 255.255.0.0 Default-Gateway – 45.45.0.1 DNS Server – 58.255.0.1
3	Настройки PPPoe	Username – a87svfk Password – dsfjhDFS921
4	Автоматические настройки	–
5	Статические настройки	Internet IP Address – 19.52.132.22 Subnet Mask – 255.255.255.0 Default-Gateway – 19.52.132.1 DNS Server – 158.55.30.41
6	Настройки PPPoe	Username – ADSo23473 Password – sdgkj56hg

7	Автоматические настройки	–
8	Настройки PPPoe	Username – BVB44556 Password – htrbYJJYfg676
9	Статические настройки	Internet IP Address – 88.45.42.42 Subnet Mask – 255.255.0.0 Default-Gateway – 88.45.0.1 DNS Server – 88.45.0.1
10	Автоматические настройки	–

4. Сохранить текущую конфигурацию.
5. Включить сервер «получения автоматических настроек» (DHCP) для клиентов. Диапазон выдачи IP адресов задать в соответствии с табл. 5.2.

Таблица 5.2. Варианты заданий диапазона адресов для DHCP сервера

Номер варианта	**IP адрес роутера**	**Первый адрес диапазона**	**Последний адрес диапазона**	**Маска сети**
1	192.168.2.254	192.168.2.20	192.168.2.200	255.255.255.0
2	192.168.7.254	192.168.7.50	192.168.7.100	255.255.255.0
3	192.168.50.254	192.168.50.100	192.168.50.130	255.255.255.0
4	192.168.8.254	192.168.8.140	192.168.8.200	255.255.255.0
5	192.168.5.254	192.168.5.200	192.168.5.220	255.255.255.0
6	192.168.22.254	192.168.22.60	192.168.22.90	255.255.255.0
7	192.168.70.254	192.168.70.90	192.168.70.120	255.255.255.0
8	192.168.150.254	192.168.150.120	192.168.150.160	255.255.255.0
9	192.168.12.254	192.168.12.180	192.168.12.210	255.255.255.0
10	192.168.90.254	192.168.90.70	192.168.90.90	255.255.255.0

Таблица 5.3. Варианты заданий настройки беспроводной связи

Номер варианта	Скорость передачи сигнала (Мбит/с)	Канал передачи данных	Ширина канала (МГц)	Режим защиты	Шифрование
1	11	2	20	WEP	40/64-бит
2	300	4	40	WPA Pers.	TKIP
3	54	6	20	WPA2 Pers.	AES
4	11	8	20	WEP	40/64-бит
5	300	10	40	WPA Pers.	TKIP
6	54	9	20	WPA2 Pers.	AES
7	11	7	20	WEP	40/64-бит
8	300	5	40	WPA Pers.	TKIP
9	54	3	20	WPA2 Pers.	AES
10	11	1	20	WEP	40/64-бит

6. Настроить беспроводную сеть согласно табл. 5.3.
7. В качестве идентификатора (SSID) беспроводной сети использовать «Собственное имя + номер варианта».
8. Разрешить трансляцию SSID.
9. Сменить пароль входа на роутер.
10. Сохранить текущую конфигурацию.
11. Подключить роутер к интернету (элемент Cloud-PT).
12. Добавить в сеть второй компьютер PC2 и соединитьс роутером кабелем витая пара. Назначить интерфейсу PC2 второй доступный адрес в вашей сети с маской 255.255.255.0. В качестве шлюза по умолчанию использовать IP адрес роутера.
13. Добавить в сеть ноутбук, планшет и смартфон. Эти устройства должны быть подключены по беспроводному соединению с динамическими настройками сети (рис. 5.2).
14. Прооверить настройки всех оконечных узлов в сети с помощью команды *ipconfig /all*.

15. Проверить работоспособность сети с помощью команды *ping*.

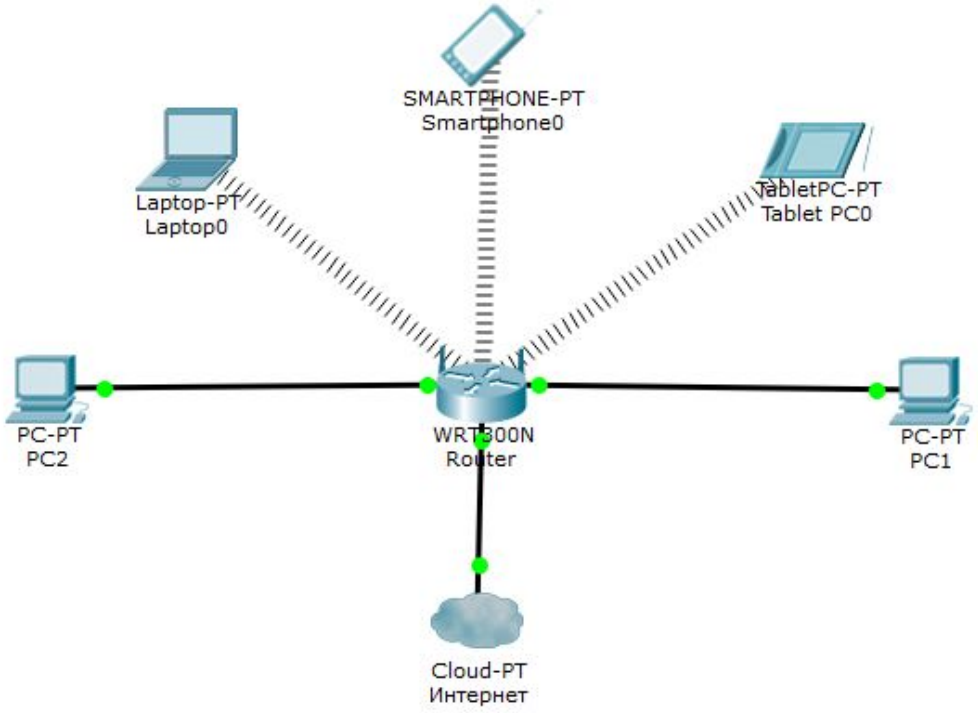


Рис. 5.2. Топология сети

Содержание отчета

1. Изображение топологии сети.
2. Изображения каждой вкладки роутера.
3. Вывод команды *ipconfig* каждого оконечного узла.
4. Вывод команды *ping* с каждого оконечного узла к роутеру.
5. Общие выводы по работе.

Контрольные вопросы

1. Как расшифровывается Wi-Fi?
2. Что такое SSID?
3. Что дает стойкую защиту беспроводного канала?
4. Как сбросить настройки Wi-Fi роутера?
5. Назначение беспроводных маршрутизаторов.
6. Зачем нужно широковещание SSID?

ЛАБОРАТОРНАЯ РАБОТА 6
Объединение сетей

Цель работы

- Ознакомиться с понятием «объединенные сети»;
- Понять принцип взаимодействия между сетями;

Краткие сведения из теории

Существуют сети любого размера, от простых сетей, состоящих из двух компьютеров, до систем, соединяющих миллионы устройств.

В небольших сетях, сетях домашнего офиса возможно организовать общий доступ к ресурсам, таким как принтеры, документы, изображения, музыка между локальными компьютерами.

Сети малых и домашних офисов часто настраиваются людьми, которые работают из дома или удалённого офиса и которым необходимо подключение к корпоративной сети или другим централизованным ресурсам. Кроме того, индивидуальные предприниматели используют сети малого и домашнего офиса в рекламных целях и для продажи продукции, заказа расходных материалов и взаимодействия с клиентами. Как правило, сетевая связь эффективнее и дешевле традиционных методов связи, например, почты или междугородных телефонных звонков.

На предприятиях и в крупных организациях сети могут использоваться в еще более обширном масштабе, чтобы позволить сотрудникам собирать, хранить и получать информацию на сетевых серверах. Кроме того, сети позволяют наладить быструю связь в виде электронной почты, обмена мгновенными сообщениями, а также функций совместной работы между сотрудниками. В дополнение к внутренним организационным преимуществам большинство компаний применяет сети для предоставления продуктов и услуг заказчикам через подключение к Интернету.

Маршрут, по которому сообщение идет от источника к месту назначения, может быть простым, например один кабель, соединяющий

один компьютер с другим, или сложным, как сеть, буквально охватывающая весь мир. Инфраструктура сети – это платформа, поддерживающая конкретную сеть. Она выполняет роль стабильного и надежного канала для передачи данных.

Инфраструктура сети включает в себя три категории компонентов сети: Устройства, Среда, Сервисы.

Устройства и среда – это физические элементы или оборудование сети. Оборудование часто является видимой частью сетевой платформы — ноутбук, ПК, коммутатор, маршрутизатор, точка беспроводного доступа или кабели, используемые для соединения устройств. Некоторые компоненты являются невидимыми. В случае беспроводных сетей сообщения передаются с помощью незримого радиочастотного или инфракрасного излучения.

Компоненты сети используются для предоставления сервисов и процессов. Это коммуникационные программы, называемые программным обеспечением, которые работают на сетевых устройствах. Сетевой сервис предоставляет данные в ответ на запрос. Сервисы включают в себя множество сетевых приложений, которые люди используют ежедневно, например, сервисы электронной почты и сервисы веб-хостинга для веб-сайтов. Процессы обеспечивают функциональность, которая направляет и перемещает сообщения в сети. Процессы менее очевидны для нас, но критически важны для работы сетей.

Для осуществления коммуникации в сети используется среда передачи данных. Среда предоставляет канал, по которому сообщение передаётся от источника к адресату.

Практическая часть

Пусть заданы сети «А» *192.168.1.0* с сетевой маской *255.255.255.0* и сеть «Б» *172.16.0.0* с сетевой маской *255.255.0.0.* Необходимо их объединить.

1. Создадим в среде Packet Tracer топологию, содержащую один роутер Generic Router-PT-Empty (Router0), один коммутатор Generic

Switch-PT-Empty (Switch0), одну беспроводную точку доступа точку Generic Access-Point-PT (Access Point0), 2 ПК (PC0 – PC1) и 2 планшета (Tablet PC0 и Tablet PC1).

2. Добавим один оптический Gigabit Ethernet-модуль PT-ROUTER-NM-1FGE в роутер для подключения сети А и один Gigabit Ethernet-модуль PT-ROUTER-NM-1CGE в роутер для подключения сети Б. Для этого откроем свойства Router0, на вкладке *Physical* на модели роутера нажмем кнопку питания для выключения, выберем указанные модули подключения, установим их в свободные слоты и включим роутер.
3. Добавим один оптический Gigabit Ethernet-модуль PT-SWITCH-NM-1FGE в коммутатор. Откроем свойства Switch0, на вкладке *Physical* на модели коммутатора нажмем кнопку питания для выключения, выберем указанный модуль подключения, установим его в свободный слот. Для подключения компьютеров выберем у установим в свободные слоты два модуля PT-SWITCH-NM-1CFE и включим коммутатор.
4. Компьютеры с коммутатором соединим витой парой. Порты подключения – FastEthernet. Роутер с коммутатором соединим оптическим кабелем – порты подключения GigabitEthernet. Планшеты соединим с точкой доступа по открытому беспроводному соединению. Точку доступа с роутером соединим витой парой – порты, соответственно, Port0 и GigabitEthernet. Топология модели сетей представлена на рис. 6.1.

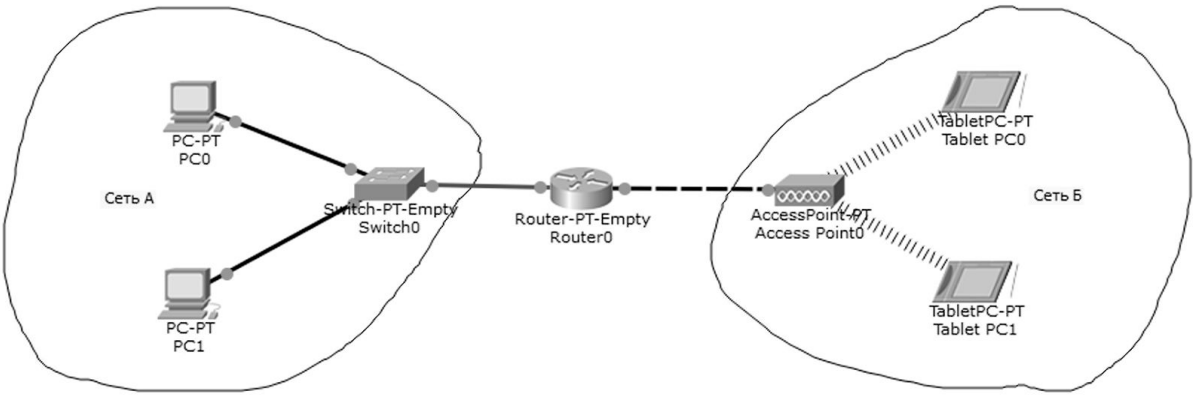


Рис. 6.1 – Пример объединения сетей

5. Выполним настройку элементов сетей. В каждой сети зарезервируем для роутера первый доступный IP-адрес, а оконечным узлам будем задавать второй и последний доступные адреса.
6. Для настройки компьютера PC0, который относится к сети А, откроем его свойства. На вкладке *Desktop* выберем опцию *IP Config* и для режима получения IP-адреса *Static* в поле *IP Address* введем второй доступный адрес подсети – 192.168.1.2, в поле *Subnet Mask* – сетевую маску 255.255.255.0, а в поле *Default Gateway* укажем первый доступный IP-адрес подсети, зарезервированный для роутера, т.е. 192.168.1.1. Компьютер PC1 настраивается аналогично, но в поле *IP Address* введем последний доступный адрес подсети – 192.168.1.254.
7. Зададим IP адреса для устройств сети Б:
   - Планшет Tablet PC0 – 172.16.0.2 маска 255.255.0.0, шлюз – 172.16.0.1;
   - Планшет Tablet PC1 – 172.16.255.254 маска 255.255.0.0, шлюз – 172.16.0.1.
8. Выполним настройку роутера, которая в данном случае будет заключаться в отдельной сетевой настройке каждого модуля к которым подключены коммутатор и точка доступа. Откроем свойства роутера, перейдем на вкладку *Config* и в подменю *INTERFACE* выберем модуль *GigabitEthernet0/0*, к которому подключен коммутатор первой сети А 192.168.1.0. В поле IP Address введем первый зарезервированный IP адрес подсети – 192.168.1.1, а в поле *Subnet Mask* – сетевую маску 255.255.255.0. После чего включим данный модуль – *Port Status* установим в *On*. Второй модуль настраивается аналогично – в поле *IP Address* указывается первый зарезервированный IP адрес сети Б, т.е. 172.16.0.1, а в поле *Subnet Mask* – 255.255.0.0.
9. Проверим работоспособность сети. Например, зайдем на компьютер PC0 и пропингуем планшет Tablet PC1. Для этого откроем свойства компьютера PC0, на вкладке *Desktop* выберем опцию *Command Promt* и

в открывшемся окне в командной строке введем команду *ping* и IP адрес компьютера Tablet PC1. Ниже представлены результаты выполнения команды *ping*:

PC>ping 172.16.0.254
Pinging 172.16.0.254 with 32 bytes of data:

Reply from 172.16.0.254: bytes=32 time=1ms TTL=127
Reply from 172.16.0.254: bytes=32 time=18ms TTL=127
Reply from 172.16.0.254: bytes=32 time=20ms TTL=127
Reply from 172.16.0.254: bytes=32 time=11ms TTL=127

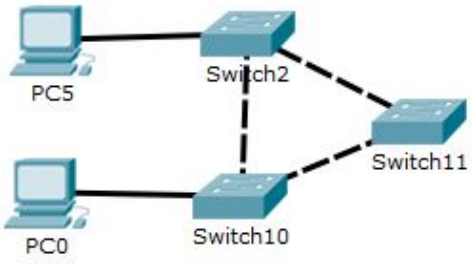
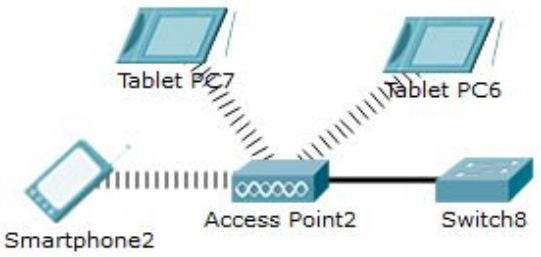
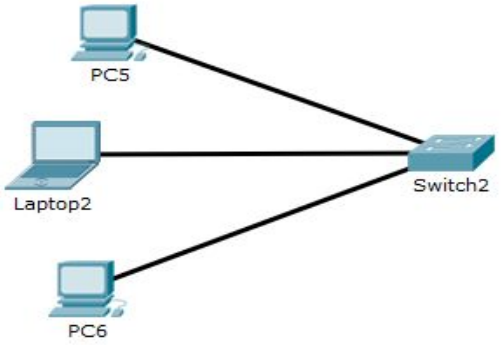
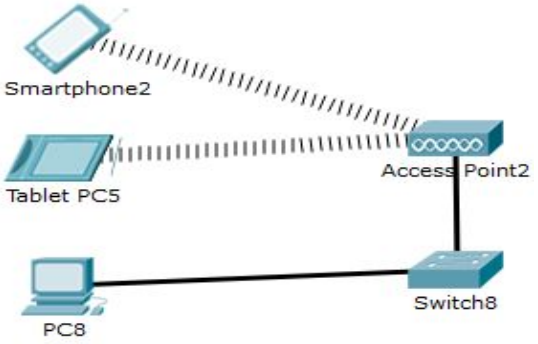
Ping statistics for 172.16.0.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 20ms, Average = 12ms

Что подтверждает правильность сетевых настроек устройств и общую работоспособность сети.

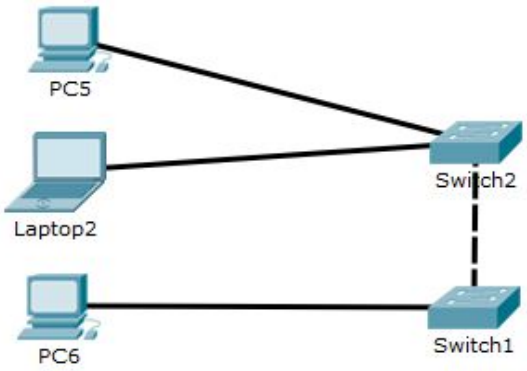
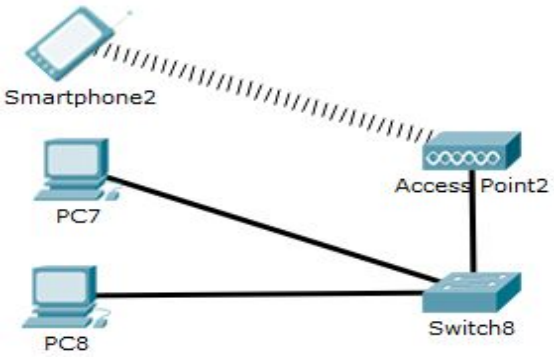
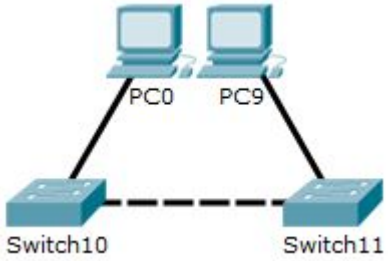
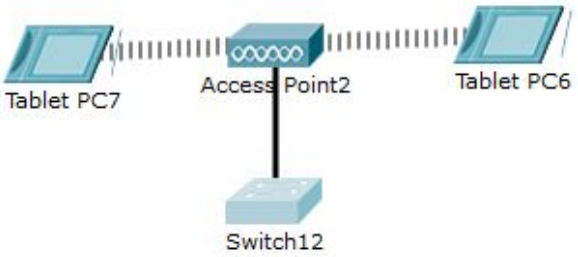
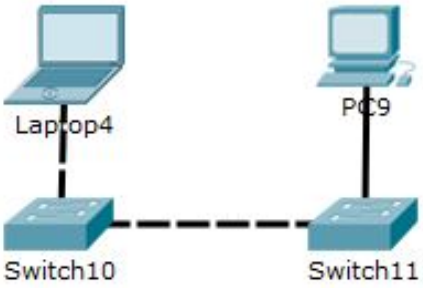
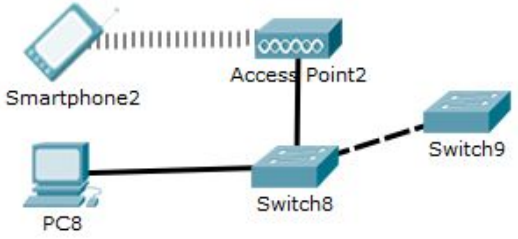
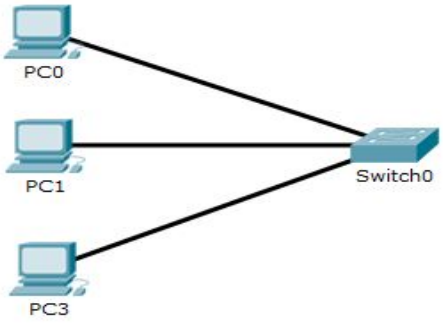
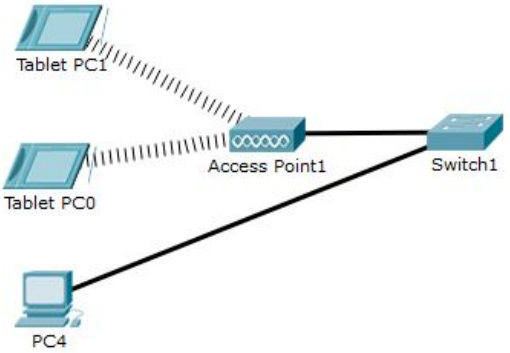
Задание

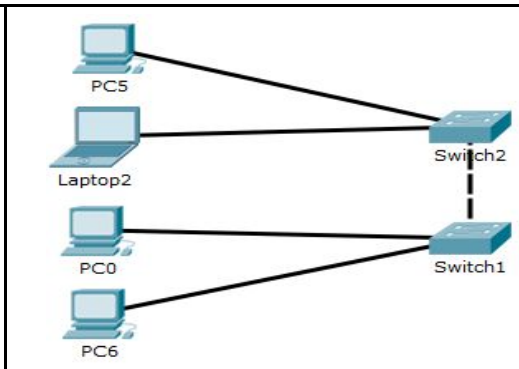
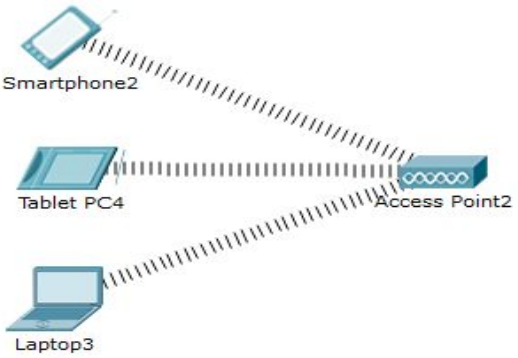
1. В соответствии с заданным вариантом (таб. 6.1) объединить сети «А» и «Б». В качестве устройства объединения использовать роутер Generic Router-PT-Empty. В качестве коммутатора использовать Generic Switch-PT-Empty, а в качестве точки доступа Generic Access-Point-PT.
2. Способ соединения сетей с роутером указан в таб. 6.2. Добавить в роутер и коммутаторы необходимые модули для объединения сетей.
3. Всем узлам задать IP адреса и маски согласно варианту (таб. 6.3):
   - всем интерфейсам маршрутизатора задать последние допустимые IP адреса сети;
   - всем оконечным узлам в сетях задать допустимые IP адреса начиная с первого.
4. Проверить настройки каждого оконечного узла командой *ipconfig*.
5. Проверить работоспособность сети командой *ping*.

Таблица 6.1. Варианты заданий топологии сети

№ вар.	Сеть А	Сеть Б
1	2	3
1		
2		

Продолжение табл. 6.1

1	2	3
3		
4		
5		
6		

7		

Продолжение табл. 6.1

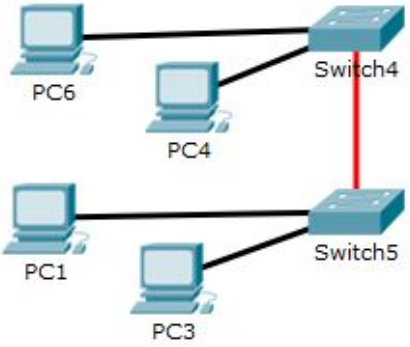
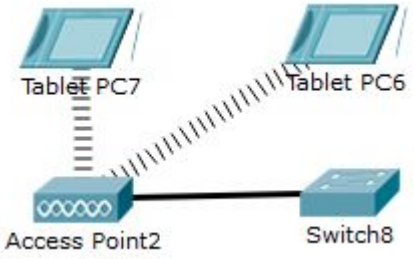
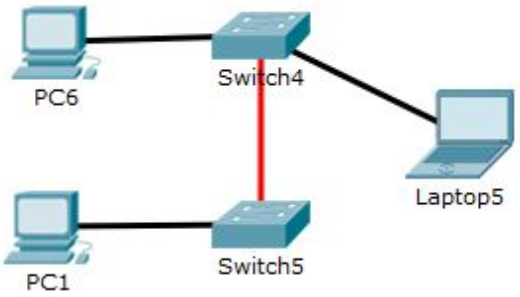
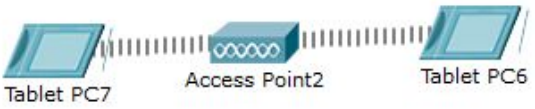
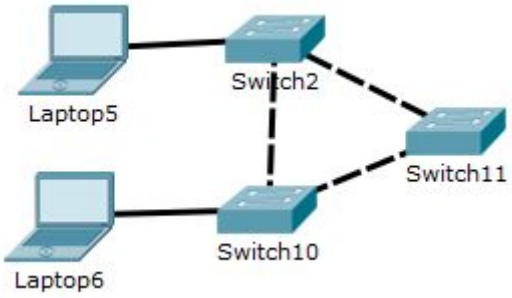
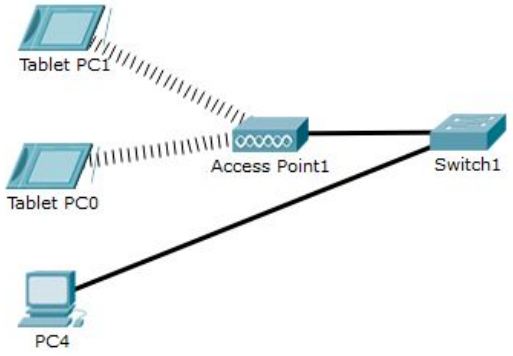
1	2	3
8		
9		
10		

Таблица 6.3. Варианты коммутация сетей

№ вар.	Сеть А	Сеть Б

1	Switch10 витой парой	Switch8 оптическим кабелем
2	Switch2 оптическим кабелем	Switch8 витой парой
3	Switch2 витой парой	Switch8 оптическим кабелем
4	Switch10 оптическим кабелем	Switch12 витой парой
5	Switch11 витой парой	Switch9 оптическим кабелем
6	Switch0 оптическим кабелем	Switch1 витой парой
7	Switch1 витой парой	AccessPoint2 витой парой
8	Switch5 оптическим кабелем	Switch8 витой парой
9	Switch5 витой парой	AccessPoint2 витой парой
10	Switch11 оптическим кабелем	Switch1 витой парой

Таблица 6.3. Варианты заданий

№ вар.	Адрес сети А	Маска сети А	Адрес сети Б	Маска сети Б
1	155.54.14.128	255.255.255.128	16.58.25.32	255.255.255.224
2	182.167.19.64	255.255.255.192	11.16.16.192	255.255.255.224
3	194.151.156.192	255.255.255.192	47.58.69.64	255.255.255.224
4	189.178.15.32	255.255.255.224	13.161.19.64	255.255.255.192
5	65.5.54.128	255.255.255.128	49.46.43.192	255.255.255.192
6	18.15.54.64	255.255.255.192	52.14.16.0	255.255.255.128
7	165.55.18.192	255.255.255.192	13.19.49.32	255.255.255.224
8	168.98.46.32	255.255.255.224	82.84.86.192	255.255.255.192
9	65.49.18.128	255.255.255.128	15.8.66.0	255.255.255.192
10	54.12.18.64	255.255.255.192	19.19.46.192	255.255.255.224

Содержание отчета

1. Изображение топологии сети.
2. Вывод команды *ipconfig* каждого оконечного узла.
3. Вывод команды *ping* между всеми оконечными узлами.
4. Вывод изображения инструмента «*Inspect/Port Status Summary Table*» для роутера.
5. Общие выводы по работе.

Контрольные вопросы

1. Что такое объединение сетей?
2. Зачем используют маршрутизаторы?
3. В чем разница между беспроводным маршрутизатором и точкой доступа?
4. На каком уровне работает роутер?
5. На каком уровне работает коммутатор?

ЛАБОРАТОРНАЯ РАБОТА 7

Настройка и использование сетевого сервиса электронной почты

Цель работы

- Ознакомиться с принципом работы электронной почты;
- Ознакомиться с протоколом SMTP и POP3;
- Научиться настраивать ящик электронной почты.

Краткие сведения из теории

Электронная почта (англ. electronic mail) – технология и служба по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети (в том числе – Интернета).

Электронная почта по составу элементов и принципу работы практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, конверт, вложение, ящик, доставка и другие), так и характерные особенности – простоту использования, задержки передачи сообщений, достаточную надежность и в то же время отсутствие гарантии доставки.

Достоинствами электронной почты являются: легко воспринимаемые и запоминаемые человеком адреса вида имя_пользователя@имя_домена; возможность передачи как простого текста, так и форматированного, а также произвольных файлов (текстовые

документы, медиа-файлы, программы, архивы, и т.д.); независимость серверов (в общем случае они обращаются друг к другу непосредственно); достаточно высокая надежность доставки сообщения; простота использования человеком и программами.

Недостатки электронной почты: наличие такого явления, как спам (массовые рекламные и вирусные рассылки); возможные задержки доставки сообщения (до нескольких суток); ограничения на размер одного сообщения и на общий размер сообщений в почтовом ящике (персональные для пользователей).

Развитие технологии Internet привело к появлению современных протоколов для обмена сообщениями, которые предоставляют большие возможности для обработки писем, разнообразные сервисы и удобство в работе. Так, например, протокол SMTP, работающий по принципу клиент-сервер, предназначен для отправки сообщений с компьютера к адресату. Обычно доступ к серверу SMTP не защищается паролем, так что можно использовать для отправки писем любой известный сервер в сети. В отличие от серверов для отправки писем, доступ к серверам для хранения сообщений защищается паролем. Поэтому необходимо использовать сервер или службу, в которой существует учетная запись. Эти серверы работают по протоколам POP и IMAP, которые различаются способом хранения писем.

SMTP (англ. Simple Mail Transfer Protocol – простой протокол передачи почты) – это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

В то время, как электронные почтовые серверы и другие агенты пересылки сообщений используют SMTP для отправки и получения почтовых сообщений, работающие на пользовательском уровне клиентские почтовые приложения обычно используют SMTP только для отправки сообщений на почтовый сервер для ретрансляции. Для получения сообщений клиентские приложения обычно используют либо *POP* (англ. Post Office Protocol – протокол почтового отделения), либо *IMAP* (англ. Internet Message Access Protocol), либо патентованные

системы (такие как Microsoft Exchange и Lotus Notes/Domino) для доступа к учетной записи своего почтового ящика на сервере.

POP3 (англ. Post Office Protocol Version 3 – протокол почтового отделения, версия 3) – стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP/IP-соединению.

POP и IMAP – наиболее распространенные интернет-протоколы для извлечения почты. Практически все современные клиенты и серверы электронной почты поддерживают оба стандарта. Большинство поставщиков услуг электронной почты также поддерживают IMAP и POP3.

Практическая часть

Пусть задана сеть *192.168.1.0* с сетевой маской *255.255.255.0.* состоящая из двух стационарных компьютеров, коммутатора, и сервера. Необходимо сконфигурировать почтовый сервер и настроить оба ПК для приема и отправки электронных писем.

1. Добавим на рабочее поле программы Packet Tracer два стационарных компьютера (PC0 – PC1), коммутатор 2960-24TT (Switch0) и сервер Generic Server-PT (Server0).
2. Соединим все устройства с коммутатором витой парой. Порты подключения всех устройств и коммутатора – FastEthernet. Топология модели сети представлена на рис. 8.1.
3. Сохраним созданную топологию.

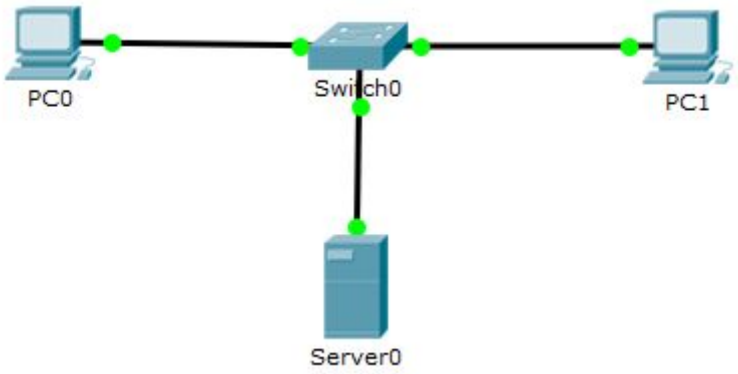


Рис. 8.1 - Топология сети

4. Выполним настройку элементов сети. Зарезервируем для сервера – второй доступный IP адрес, а стационарным компьютерам будем задавать адреса последовательно с третьего доступного. Сетевая маска для всех устройств – 255.255.255.0.
5. Для настройки компьютера PC0 откроем его свойства. На вкладке *Desktop* выберем опцию *IP Config* и для режима получения IP адреса *Static* в поле *IP Address* введем третий доступный адрес сети – 192.168.1.3, в поле *Subnet Mask* – сетевую маску 255.255.255.0, а в поле *Default Gateway* можем отставить пустым (т. к. у нас нет выхода за пределы нашей сети.. Остальные стационарные компьютеры настраиваются аналогично).
6. Для настройки сервера откроем его свойства, перейдем на вкладку *Config* и в подменю *INTERFACE* выберем модуль *FastEthernet0*. В поле *IP Address* введем второй зарезервированный IP адрес сети – 192.168.1.2, а в поле *Subnet Mask* – сетевую маску 255.255.255.0. После чего включим данный модуль – *Port Status* установим в *On*. Далее настроим сервис EMAIL. Перейдем на вкладку *Services* и выберем подменю EMAIL. Для включения переключатель *SMTP Service* установим в положение *On*. Назначим доменное имя почтового сервера – в поле *Domain Name* введем, например, metall.com. Нажмем кнопку SET для сохранения имени домена. Далее создадим две учетные записи пользователей. Для этого необходимо в поле *user* ввести имя учетной записи, а в поле *password* – пароль. Для добавления записи в базу

данных нажмем кнопку «+». Таким способом создадим для записи: user1 с паролем user1 и user2 с паролем user2.

7. Настроим почтовые ящики на PC1 и PC2. На вкладке *Desktop* выберем опцию *Email.* Появится окно для конфигурирования почтового ящика. В поле your name укажем произвольное имя вашего ящика, которое будет хранится на только на локальном ПК (например, для PC1 – U1, а для PC2 – U2). В поле email address необходимо указать полное название почтового ящика, т.е.:

   email = имя учетной записи на сервере + «@» + доменное имя сервера

   Для PC1 – user1@metall.com, а для PC2 – user2@metall.com. В разделе *Server information* укажем ip адрес для серверов входящее и исходящей почты, в нашем случае *incoming mail server* и *outgoing mail server* будут одинаковы – 192.168.1.2 для обоих ПК. В разделе *Logon information* укажем имя и пароль учетной записи предварительно записанной на сервере (для PC1 - user1 с паролем user1, а для PC2 - user2 с паролем user2). Для сохранения конфигурации нажимаем кнопку *Save*.
8. Проверим работоспособность почтовых ящиков. Например, зайдем на компьютере PC0 в раздел *Desktop / Email.* Откроется окно *Mail browser.* Для отправки письма нажмем кнопку *compose*. В поле *To* укажем e-mail адрес получателя (user2@metall.com), в поле *subject* укажем тему письма (например, «test»), в нижнем текстовом поле текст самого письма (например, «Мое первое тестовое сообщение!!!»). Для отправки сообщения нажимаем кнопку *send.* И если все настроено правильно, то мы получим сообщение о том, что сообщение отправлено (см. рис. 8.2).

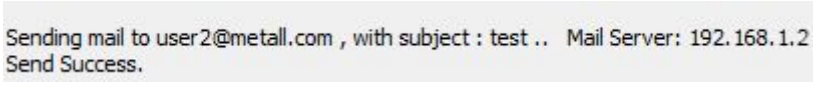


Рис. 8.2 – Сообщение об успешной отправки письма

Для проверки доставки письма зайдем на компьютере PC1 в раздел *Desktop / Email.* Для получения письма нажмем кнопку *Receive*.

Высветится список всех полученных писем (см. рис. 8.3). Открытие письма происходи двойным щелчком мыши.

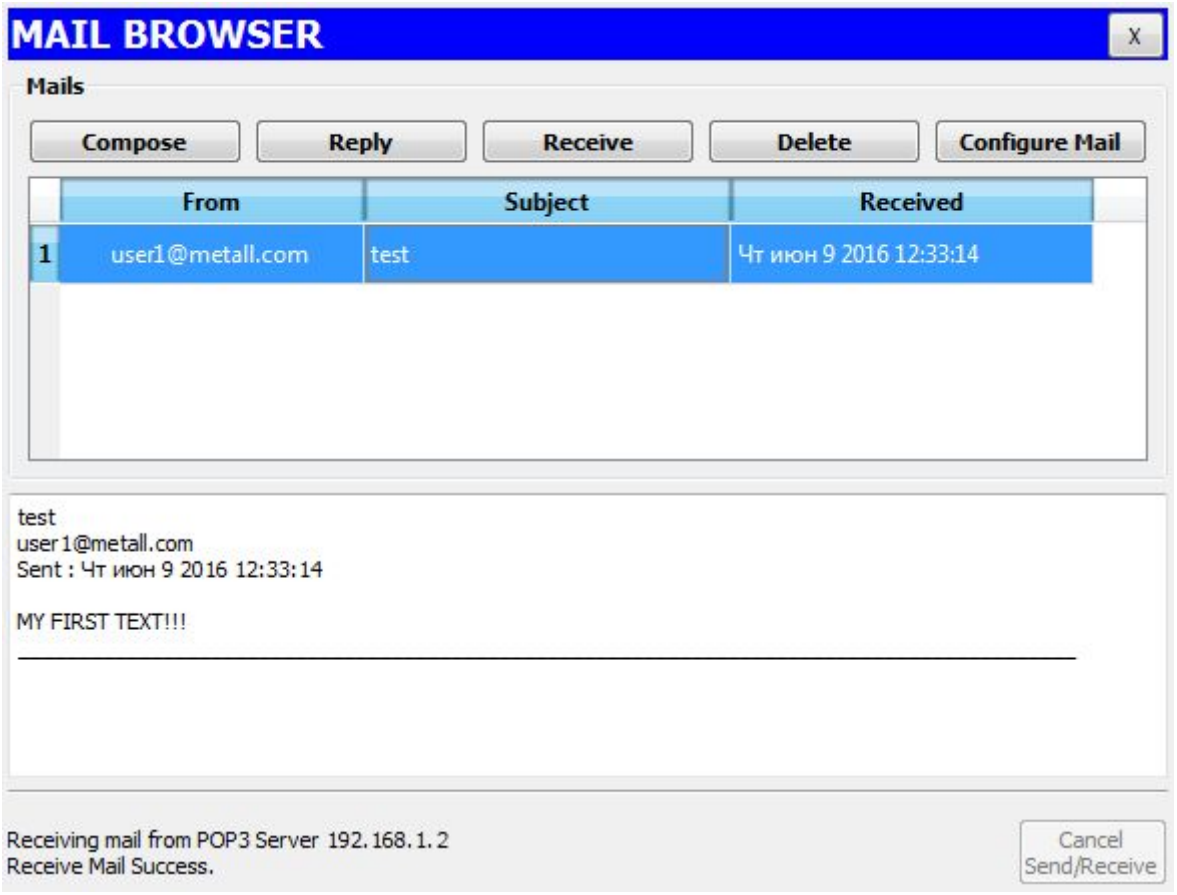


Рис. 8.3 – Список полученных сообщений

Задание

1. Добавить на рабочее поле программы Packet Tracer два стационарных компьютера (PC0, PC1), два ноутбука (Laptop0, Laptop1), два коммутатора 2960-24TT (Switch0, Switch1), роутер Generic Router-PT-Empty (Router0) и два сервера Generic Server-PT (email_A, email_Б).
2. Добавить два Gigabit Ethernet-модуль PT-ROUTER-NM-1CGE в роутер для подключения сети.
3. Соединим все устройства витой парой. Порты подключения роутера и коммутатора GigabitEthernet, остальных устройств и коммутатора – FastEthernet. Топология модели сети представлена на рис. 8.4.

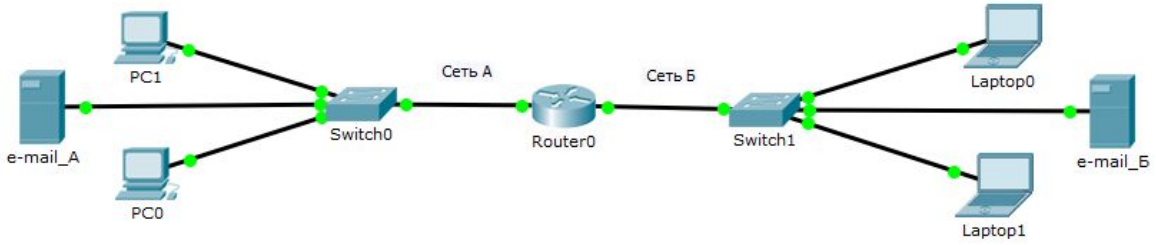


Рис. 8.4 – Заданная топология сети

4. Назначить оконечным узлам в сетях А и Б статические IP адреса в соответствии с заданным вариантом (таб. 8.1):
   - Интерфейсу роутера в сети А и Б назначить первый доступный.
   - Интерфейсу в сети А и Б сервера назначить последний доступный адрес.
   - Компьютеру PC0 назначить второй доступный адрес в сети А.
   - Компьютеру PC1 назначить третий доступный адрес в сети А.
   - Компьютеру Laptop0 назначить второй доступный адрес в сети Б.
   - Компьютеру Laptop1 назначить третий доступный адрес в сети Б.

Таблица 8.1 - Варианты заданий адресов сети

Номер варианта	Адрес сети А	Маска сети А	Адрес сети Б	Маска сети Б
1	14.67.11.128	255.255.255.192	51.18.41.160	255.255.255.224
2	14.67.12.128	255.255.255.224	51.18.42.160	255.255.255.240
3	14.67.13.128	255.255.255.128	51.18.43.160	255.255.255.248
4	14.67.14.128	255.255.255.192	51.18.44.160	255.255.255.224
5	14.67.15.128	255.255.255.224	51.18.45.160	255.255.255.240
6	14.67.16.128	255.255.255.128	51.18.46.160	255.255.255.248
7	14.67.17.128	255.255.255.192	51.18.47.160	255.255.255.224
8	14.67.18.128	255.255.255.224	51.18.48.160	255.255.255.240
9	14.67.19.128	255.255.255.128	51.18.49.160	255.255.255.248
10	14.67.20.128	255.255.255.192	51.18.50.160	255.255.255.224

5. Проверить работоспособность сети – пропинговать с PC1 все остальные узлы.
6. Согласно таблице 8.2 создать на серверах email_A и email_Б почтовые сервера с доменными именами и добавить в них по две учетные записи. Придумать соответствующие пароли.

Таблица 8.2 - Варианты заданий

№ Вар.	Домен сервера email_A	Учетная запись PC0	Учетная запись PC1	Домен сервера email_Б	Учетная запись Laptop0	Учетная запись Laptop1
1	Albania.com	Tirana	Durres	Nigeria.net	Abuja	Lagos
2	Algeria.com	Algiers	Oran	Pakistan.net	Islamabad	Karachi
3	Niger.com	Niamey	Zinder	Peru.net	Lima	Arequipa
4	Angola.com	Luanda	Huambo	Cyprus.net	Nicosia	paphos
5	Ecuador.com	Quito	Loja	Sudan.net	Khartoum	Omdurma
6	Iran.com	ahar	kilan	Taiwan.net	Kaohsiung	Taipei
7	India.com	Mumbai	Delhi	Fiji.net	Suva	lami
8	Cameroon.com	Douala	Yaounde	Vietnam.net	Hanoi	Haiphong
9	Chile.com	Santiago	Arica	Yemen.net	Aden	Sana
10	Cuba.com	Havana	Holguin	Zimbabwe	Harare	Bulawayo

7. Настроить почтовые ящики на всех оконечных узлах в соответствии с таблицей 8.2.
8. Проверить отправку почты:

- отправить тестовые письма с PC0 на все остальные почтовые ящики.
- отправить тестовые письма с Laptop0 на все остальные почтовые ящики.

9. Проверить прием писем на всех устройствах.
10. В режиме симуляции отправить тестовое письмо с PC1 на Laptop1. Проследить движение пакетов по протоколу smtp.

Содержание отчета

1. Изображение топологии сети.
2. Изображения *ipconfig* каждого оконечного узла.
3. Изображения команды *ping* между первым и остальными оконечными узлами.
4. Изображение окна конфигурации каждого почтового ящика по п.7 задания.
5. Изображение окна *Simulation Panel* по п.10 задания.
6. Общие выводы по работе.

Контрольные вопросы

1. Что такое электронная почта?
2. Для чего используется почтовые ящики?
3. Из каких этапов состоит процесс настройки клиентского ПО для работы с электронной почтой?
4. Чем отличаются почтовые протоколы?

ЛАБОРАТОРНАЯ РАБОТА 8
Настройка и использование сетевого сервиса DHCP

Цель работы

- Ознакомиться с протоколом DHCP;

- Ознакомиться с принципом функционирования протокола DHCP;
- Научиться применять технологию DHCP.

Краткие сведения из теории

DHCP (англ. Dynamic Host Configuration Protocol – протокол динамической настройки узла) – сетевой протокол, позволяющий компьютерам автоматически получать IP адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

Протокол DHCP предоставляет три способа распределения IP адресов:

Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определенный IP адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP адрес из определенного администратором диапазона.

Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес

выдается компьютеру не на постоянное пользование, а на определенный срок. Это называется арендой адреса. По истечении срока аренды IP адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов.

Процесс получения IP адреса клиентом от сервера DHCP состоит из четырех этапов.

1. Обнаружение DHCP. Вначале клиент выполняет широковещательный запрос по всей физической сети с целью обнаружить доступные DHCP-серверы.
2. Предложение DHCP. Получив сообщение от клиента, сервер определяет требуемую конфигурацию клиента в соответствии с указанными сетевым администратором настройками. Клиент может получить несколько различных предложений DHCP от разных серверов; из них он должен выбрать то, которое его «устраивает».
3. Запрос DHCP. Выбрав одну из конфигураций, предложенных DHCP-серверами, клиент отправляет запрос DHCP. Он рассылается широковещательно; при этом к опциям, указанным клиентом в сообщении, добавляется специальная опция — идентификатор сервера — указывающая адрес DHCP-сервера, выбранного клиентом.
4. Подтверждение DHCP. Сервер подтверждает запрос и направляет это подтверждение клиенту. После этого клиент должен настроить свой сетевой интерфейс, используя предоставленные опции.

Помимо сообщений, необходимых для первоначального получения IP адреса клиентом, DHCP предусматривает несколько дополнительных сообщений для выполнения иных задач.

Отказ DHCP. Если после получения подтверждения от сервера клиент обнаруживает, что указанный сервером адрес уже используется в сети, он рассылает широковещательное сообщение отказа DHCP, после

чего процедура получения IP адреса повторяется. Использование IP адреса другим клиентом можно обнаружить, выполнив запрос ARP.

Сообщение отмены DHCP. При получении такого сообщения соответствующий клиент должен повторить процедуру получения адреса.

Освобождение DHCP. Клиент может явным образом прекратить аренду IP адреса. Для этого он отправляет сообщение освобождения DHCP тому серверу, который предоставил ему адрес в аренду. В отличие от других сообщений DHCP, это сообщение не рассылается широковещательно.

Информация DHCP. Сообщение информации DHCP предназначено для определения дополнительных параметров TCP/IP (например, адреса маршрутизатора по умолчанию, DNS-серверов и т.п.) теми клиентами, которым не нужен динамический IP адрес (т.е. адрес которых настроен вручную). Серверы отвечают на такой запрос сообщением подтверждения без выделения IP адреса.

Практическая часть

Пусть задана сеть *192.168.1.0* с сетевой маской *255.255.255.0.* состоящая из трех стационарных компьютеров, трех ноутбуков, коммутатора, роутера и сервера. Необходимо сконфигурировать DHCP-сервер и установить автоматическое назначение IP адресов ноутбукам.

1. Добавим на рабочее поле программы Packet Tracer три стационарных компьютера (PC0 – PC2), три ноутбука (Laptop0 – Laptop2), коммутатор 2960-24TT (Switch0), роутер Generic Router-PT-Empty (Router0) и сервер Generic Server-PT (Server0).
2. Добавим один Gigabit Ethernet-модуль PT-ROUTER-NM-1CGE в роутер для подключения сети. Для этого откроем свойства Router0, на вкладке *Physical* на модели роутера нажмем кнопку питания для выключения, выберем указанный модуль подключения, установим его в свободный слот и включим роутер.
3. Соединим все устройства с коммутатором витой парой. Порты

подключения роутера и коммутатора GigabitEthernet, остальных устройств и коммутатора – FastEthernet. Топология модели сети представлена на рис. 9.1.

4. Сохраним созданную топологию.

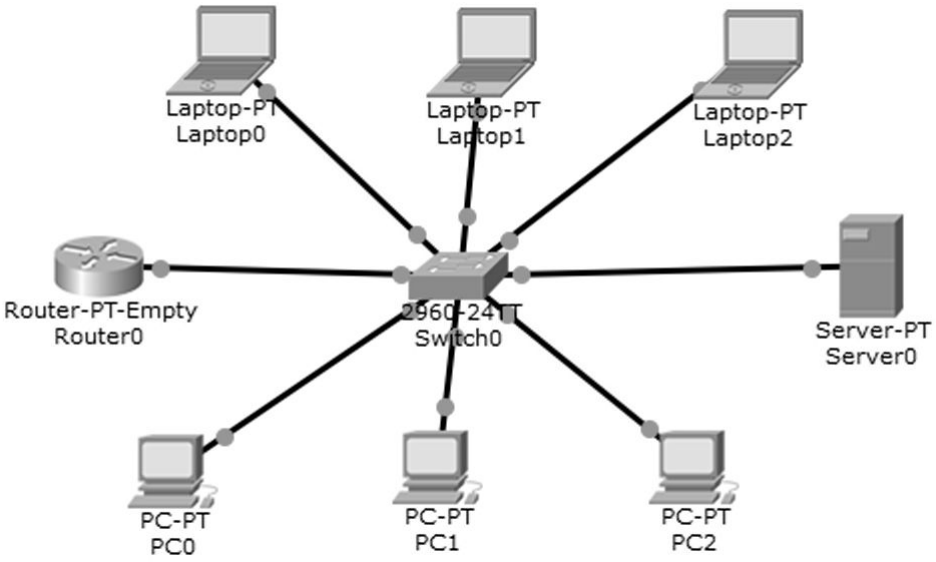


Рис. 9.1. Топология сети

5. Выполним настройку элементов сети. Зарезервируем для роутера первый доступный IP адрес, для сервера – второй, а стационарным компьютерам будем задавать адреса последовательно с третьего доступного. Сетевая маска для всех устройств – 255.255.255.0.
6. Для настройки компьютера PC0 откроем его свойства. На вкладке *Desktop* выберем опцию *IP Config* и для режима получения IP адреса *Static* в поле *IP Address* введем третий доступный адрес сети – 192.168.1.3, в поле *Subnet Mask* – сетевую маску 255.255.255.192, а в поле *Default Gateway* укажем первый доступный IP адрес сети, зарезервированный для роутера, т.е. 192.168.1.1. Остальные стационарные компьютеры настраиваются аналогично.
7. Выполним настройку роутера. Откроем свойства роутера, перейдем на вкладку *Config* и в подменю *INTERFACE* выберем модуль *GigabitEthernet0/0*, к которому подключен коммутатор. В поле IP

Address введем первый зарезервированный IP адрес подсети – 192.168.1.1, а в поле *Subnet Mask* – сетевую маску 255.255.255.0. После чего включим данный модуль – *Port Status* установим в *On*.

8. Для настройки сервера откроем его свойства, перейдем на вкладку *Config* и в подменю *INTERFACE* выберем модуль *FastEthernet0*. В поле *IP Address* введем второй зарезервированный IP адрес сети – 192.168.1.2, а в поле *Subnet Mask* – сетевую маску 255.255.255.0. После чего включим данный модуль – *Port Status* установим в *On*. Далее настроим сервис DHCP. Перейдем на вкладку *Services* и выберем подменю *DHCP*. Для включения переключатель *Service* установим в положение *On*. Назначим имя пула для раздачи адресов – в поле *Pool Name* введем APP_Pool. В поле *Default Gateway* укажем IP адрес роутера 192.168.1.1. Автоматическое назначение IP адресов установим с шестого доступного адрес сети – в поле *Start IP Address* введем 192.168.1.6. В поле *Subnet Mask* укажем сетевую маску 255.255.255.0. После нажатия на кнопку Add в DHCP-таблице появится соответствующая запись.
9. Настроим ноутбуки на автоматическое получение IP адреса. Для настройки ноутбука Laptop0 откроем его свойства. На вкладке *Desktop* выберем опцию *IP Config* и активируем режим получения IP адреса *DHCP*. Через короткое время в полях *IP Address* и *Subnet Mask* появятся сетевые параметры. В данном случае это первый IP адрес из доступных для автоматического назначения – 192.168.1.6 и сетевая маска 255.255.255.0. Остальные ноутбуки настраиваются аналогично. Проверить назначенные адреса можно с помощью инструмента Inspect/Port Status Summary Table.
10. Проверим работоспособность сети. Например, зайдем на компьютер PC0 и пропингуем ноутбук Laptop0. Для этого откроем свойства компьютера PC0, на вкладке *Desktop* выберем опцию *Command Promt* и в открывшемся окне в командной строке введем команду *ping* и IP адрес ноутбука Laptop0. Ниже представлены результаты выполнения команды *ping*:

PC>ping 192.168.1.6
Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Что подтверждает правильность сетевых настроек устройств и общую работоспособность сети.

Задание

1. Создать сеть в соответствии с топологией, представленной на рис. 9.1.
2. Назначить оконечным узлам статические IP адреса в соответствии с заданным вариантом (таб. 9.1):
   - Интерфейсу роутера назначить первый доступный адрес в сети.
   - Интерфейсу сервера назначить второй доступный адрес в сети.
   - Компьютеру PC0 назначить третий доступный адрес в сети.
   - Компьютеру PC1 назначить четвертый доступный адрес в сети.
   - Компьютеру PC2 назначить пятый доступный адрес в сети.

Таблица 9.1. Варианты заданий

Номер варианта	**Адрес сети**	**Маска сети**
1	44.16.105.0	255.255.255.128
2	45.16.115.0	255.255.255.192
3	46.16.125.0	255.255.255.224

4	47.16.135.0	255.255.255.128
5	48.16.145.0	255.255.255.192
6	49.16.155.0	255.255.255.224
7	50.16.165.0	255.255.255.128
8	51.16.175.0	255.255.255.192
9	52.16.185.0	255.255.255.224
10	53.16.195.0	255.255.255.128

3. Настроить на сервере Server0 сервис DHCP.
4. В режиме симуляции настроить ноутбук Laptop0 на динамическое получение IP адреса. Проследить движение пакетов по протоколу DHCP.
5. Настроить остальные ноутбуки в сети на динамическое получение IP адреса.
6. Проверить настройки компьютеров с помощью команды *ipconfig /all*.
7. Проверить работоспособность сети – пропинговать с первого стационарного компьютера все узлы.

Содержание отчета

1. Изображение топологии сети.
2. Изображения *ipconfig* каждого оконечного узла.
3. Изображения команды *ping* между первым и остальными оконечными узлами.
4. Изображение окна *Simulation Panel* по п.4 задания.
5. Общие выводы по работе.

Контрольные вопросы

1. Что такое DHCP?
2. Для чего используется DHCP?
3. Из каких этапов состоит процесс получения IP адреса клиентом от сервера DHCP?

4. Какие сообщения предусматривает DHCP для выполнения задач, не связанных с получением IP адреса?

ЛАБОРАТОРНАЯ РАБОТА 9
Настройка и использование сетевого сервиса DNS

Цель работы

- Ознакомиться с принципом функционирования системы доменных имен (DNS);
- Научиться конфигурировать DNS-сервер.

Краткие сведения из теории

DNS (англ. Domain Name System – система доменных имен) – компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

Распределенная база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определенному протоколу.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу, что позволяет возложить ответственность за актуальность информации на серверы различных организаций, отвечающих только за «свою» часть доменного имени.

Доме́н (англ. domain – область) – узел в дереве имен, вместе со всеми подчиненными ему узлами (если таковые имеются), то есть именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо от младших доменов к доменам высшего уровня (в порядке повышения значимости): вверху находится корневой домен (не имеющий

идентификатора), ниже идут домены первого уровня (доменные зоны), затем – домены второго уровня, третьего и т.д. (например, для адреса uk.wikipedia.org. домен первого уровня – org, второго wikipedia, третьего uk).

Поддомен (англ. subdomain) – подчиненный домен (например, wikipedia.org – поддомен домена org, а uk.wikipedia.org – домена wikipedia.org). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имен используют более строгие ограничения. Например, если есть домен вида mydomain.ua, то можно создать для него различные поддомены вида mysite1.mydomain.ua, mysite2.mydomain.ua и т.д.

DNS-сервер – специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.

DNS-клиент – специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

DNS-запрос (англ. DNS query) – запрос от клиента (или сервера) серверу. Запрос может быть рекурсивным или нерекурсивным.

Термином *рекурсия* в DNS обозначают алгоритм поведения DNS-сервера, при котором сервер выполняет от имени клиента полный поиск нужной информации во всей системе DNS, при необходимости обращаясь к другим DNS-серверам.

При ответе на нерекурсивный запрос, а также при неумении или запрете выполнять рекурсивные запросы, DNS-сервер либо возвращает данные о зоне, за которую он ответственен, либо возвращает ошибку. Настройки нерекурсивного сервера, когда при ответе выдаются адреса серверов, которые обладают большим объемом информации о запрошенной зоне, чем отвечающий сервер (чаще всего – адреса корневых

серверов), являются некорректными, и такой сервер может быть использован для организации DoS-атак.

В случае рекурсивного запроса DNS-сервер опрашивает серверы (в порядке убывания уровня зон в имени), пока не найдет ответ или не обнаружит, что домен не существует (на практике поиск начинается с наиболее близких к искомому DNS-серверов, если информация о них есть в кэше и не устарела, сервер может не запрашивать другие DNS-серверы).

Иногда допускается, чтобы запрошенный сервер передавал рекурсивный запрос «вышестоящему» DNS-серверу и дожидался готового ответа.

При рекурсивной обработке запросов все ответы проходят через DNS-сервер, и он получает возможность кэшировать их. Повторный запрос на те же имена обычно не идет дальше кэша сервера, обращения к другим серверам не происходит вообще. Допустимое время хранения ответов в кэше приходит вместе с ответами (поле TTL ресурсной записи).

Рекурсивные запросы требуют больше ресурсов от сервера (и создают больше трафика), так что обычно принимаются от «известных» владельцу сервера узлов (например, провайдер предоставляет возможность делать рекурсивные запросы только своим клиентам, в корпоративной сети рекурсивные запросы принимаются только из локального сегмента). Нерекурсивные запросы обычно принимаются ото всех узлов сети (и содержательный ответ дается только на запросы о зоне, которая размещена на узле, на DNS-запрос о других зонах обычно возвращаются адреса других серверов).

DNS используется в первую очередь для преобразования символьных имен в IP-адреса, но он также может выполнять обратный процесс. Для этого используются уже имеющиеся средства DNS.

Имя и IP-адрес не тождественны – один IP-адрес может иметь множество имен, что позволяет поддерживать на одном компьютере множество веб-сайтов (это называется виртуальный хостинг). Обратное тоже справедливо – одному имени может быть сопоставлено множество IP-адресов: это позволяет создавать балансировку нагрузки.

Практическая часть

Пусть задана сеть *192.168.1.0* с сетевой маской *255.255.255.0.* состоящая из двух стационарных компьютеров, двух ноутбуков, коммутатора и сервера. Необходимо сконфигурировать DNS-сервер.

1. Добавим на рабочее поле программы Packet Tracer два стационарных компьютера (PC0 и PC1), два ноутбука (Laptop0 и Laptop1), коммутатор 2960-24TT (Switch0) и сервер Generic Server-PT (Server0).
2. Соединим все устройства с коммутатором витой парой. Порты подключения FastEthernet. Топология модели сети представлена на рис. 10.1.
3. Сохраним созданную топологию.
4. Выполним настройку элементов сети. Зарезервируем для сервера первый доступный IP-адрес, а компьютерам будем задавать адреса последовательно со второго доступного. Сетевая маска для всех устройств – 255.255.255.0. Также присвоим компьютерам имена, которые будем использовать в запросах вместо IP адресов: PC0 – APP1, PC1 – APP2, Laptop0 – APP3, Laptop1 – APP4.

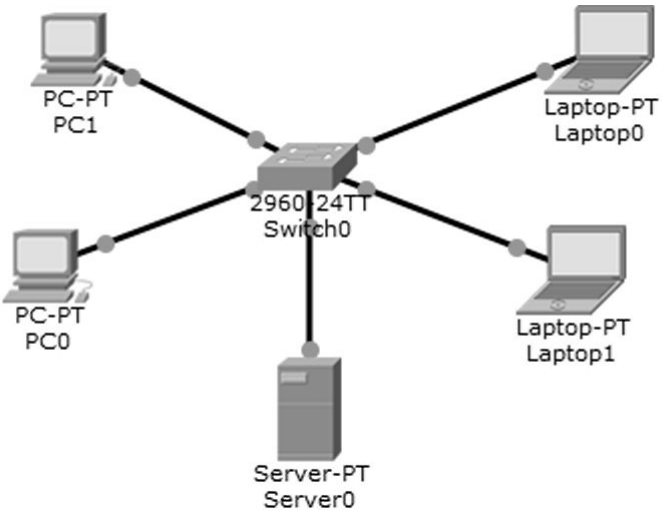


Рис. 10.1. Топология сети

5. Для настройки компьютера PC0 откроем его свойства. На вкладке

Desktop выберем опцию *IP Config* и для режима получения IP-адреса *Static* в поле *IP Address* введем второй доступный адрес сети – 192.168.1.2, в поле *Subnet Mask* – сетевую маску 255.255.255.192, а в поле *DNS Server* укажем первый доступный IP-адрес сети, зарезервированный для сервера, т.е. 192.168.1.1. Имя компьютера можно изменить на вкладке *Config* в подменю *Global Setting* – в поле *Display Name* введем APP1. Остальные компьютеры настраиваются аналогично.

6. Выполним настройку сервера. Откроем его свойства, перейдем на вкладку *Config* и в подменю *INTERFACE* выберем модуль *FastEthernet0*. В поле *IP Address* введем первый зарезервированный IP адрес сети – 192.168.1.1, а в поле *Subnet Mask* – сетевую маску 255.255.255.0. После чего включим данный модуль – *Port Status* установим в *On*. Далее настроим сервис DNS. Перейдем на вкладку *Services* и выберем подменю *DNS*. Для включения сервиса переключатель *DNS Service* установим в положение *On*. Чтобы добавить первый компьютер в DNS-таблицу в поле *Name* введем APP1, а в поле *Address* укажем его IP адрес – 192.168.1.2 и нажмем на кнопку Add. В DNS-таблице соответствующая запись появится. Остальные устройства добавляются аналогично.
7. Проверим работоспособность сети. Например, зайдем на компьютер APP1 и пропингуем ноутбук APP4. Для этого откроем свойства компьютера APP1, на вкладке *Desktop* выберем опцию *Command Promt* и в открывшемся окне в командной строке введем команду *ping* и символьное имя ноутбука APP4. Ниже представлены результаты выполнения команды *ping*:

   PC>ping APP4

   Pinging 192.168.1.5 with 32 bytes of data:

   Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
   Reply from 192.168.1.5: bytes=32 time=1ms TTL=128

Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

Что подтверждает правильность сетевых настроек устройств и общую работоспособность сети.

Задание

1. Создать сеть в соответствии с топологией, представленной на рис. 10.1.
2. Задать всем ПК и ноутбукам произвольные имена по типу: «имя-PC», например, «Alex-PC».
3. Назначить оконечным узлам адреса в соответствии с заданным вариантом (таб. 10.1):
   - Интерфейсу сервера DNS назначить первый доступный адрес в сети.
   - Компьютеру PC0 назначить второй доступный адрес в сети.
   - Компьютеру PC1 назначить третий доступный адрес в сети.
   - Ноутбуку Laptop0 назначить последний доступный адрес в сети.
   - Ноутбуку Laptop1 назначить предпоследний доступный адрес в сети.

Таблица 10.1. Варианты заданий

Номер варианта	**Адрес сети**	**Маска сети**
1	100.10.15.0	255.255.255.240
2	100.11.15.0	255.255.255.128
3	100.12.15.0	255.255.255.0
4	100.13.15.0	255.255.255.240
5	100.14.15.0	255.255.255.128
6	100.15.15.0	255.255.255.0

7	100.16.15.0	255.255.255.240
8	100.17.15.0	255.255.255.128
9	100.18.15.0	255.255.255.0
10	100.19.15.0	255.255.255.240

4. Настроить на сервере Server0 сервис DNS.
5. Проверить работоспособность сети и DNS-сервера – пропинговать с первого компьютера остальные. В качестве аргумента команды *ping* использовать символьные имена.
6. В режиме симуляции отправить эхо запрос с символьным именем с компьютера PC0 на ноутбук Laptop0. Проследить движение пакетов по протоколу DNS и ICMP.

Содержание отчета

1. Изображение топологии сети.
2. Изображения *ipconfig* каждого оконечного узла.
3. Изображения команды *ping* между первым и остальными оконечными узлами.
4. Изображение окна *Simulation Panel* по п.6 задания.
5. Общие выводы по работе.

Контрольные вопросы

1. Что такое DNS?
2. Для чего используется DNS?
3. Как осуществляется связь в сети, в которой отсутствует сервер DNS?
4. Что содержит таблица DNS?
5. Что предпринимает локальный DNS-сервер, если не может найти соответствия в своей таблице?