

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего профессионального образования
«Севастопольский государственный университет»

**ИССЛЕДОВАНИЕ СИСТЕМЫ КОМАНД
IOS И СПОСОБОВ КОНФИГУРАЦИИ
СЕТЕВОГО ОБОРУДОВАНИЯ.
СТРУКТУРА IP-АДРЕСА**

**Методические указания
к выполнению лабораторной работы №1
по дисциплине «Архитектура (структуры и
протоколы) инфокоммуникационных систем
и сетей»**

Для студентов, обучающихся по направлению 09.03.02
«Информационные системы и технологии»
по учебному плану подготовки бакалавров
дневной и заочной форм обучения

**Севастополь
2018**

УДК 004.732

Исследование системы команд IOS и способов конфигурации сетевого оборудования. Структура IP-адреса. Методические указания к лабораторным занятиям по дисциплине «Архитектура (структуры и протоколы) инфокоммуникационных систем и сетей» / Сост., В.С. Чернега, А.В. Волкова – Севастополь: Изд-во СевГУ, 2018 – 32 с.

Методические указания предназначены для проведения лабораторных работ по дисциплине «Архитектура (структуры и протоколы) инфокоммуникационных систем и сетей». Целью методических указаний является помочь студентам в построении простейших локальных сетей. Излагаются теоретические и практические сведения необходимые для выполнения лабораторной работы, требования к содержанию отчета.

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры информационных систем (протокол № 10 от 21 апреля 2017 г.)

Рецензент: Моисеев Д.В., канд. техн. наук, доцент кафедры ИТиКС

1 ЦЕЛЬ РАБОТЫ

Исследование структуры IP-адреса сетевых устройств, углубление теоретических знаний в области архитектуры компьютерных сетей и сетевых операционных систем, исследование команд конфигурации коммуникационного оборудования и приобретение навыков в построении и исследовании простейших локальных сетей средствами симулятора Cisco Packet Tracer.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

2.1 Структура IP адреса

Передача сообщений в компьютерной сети основана на том, что каждый компьютер сети имеет индивидуальный адрес – IP-адрес. Этот адрес выражается одним 32-разрядным числом, имеющим две смысловые части. Одна часть IP-адреса определяет номер сети, вторая – номер узла(компьютера) в сети. Так как оперировать длинными двоичными числами достаточно сложно, число, определяющее IP-адрес, разбивают на 4 октета – восьмиразрядных двоичных числа, а каждое из этих чисел представляют в десятичном виде. Октеты отделяют друг от друга точками. Таким образом, 32-разрядный IP-адрес представляется в виде: 255.255.255.255 (десятичное число может меняться от 0 до 255 – максимального значения восьмиразрядного двоичного числа). Например: 128.10.2.30 – десятичная форма представления IP-адреса, 10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса. Запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла.

Например, в адресе **192.168.1.1** можно выделить сетевую часть – три старшие цифры **192.168.1** адреса и хостовую часть – одну младшую цифру **1** адреса, этот адрес принадлежит IP-сети с диапазоном адресов **192.168.1.0 – 192.168.1.255**. В качестве адреса всей сети используется первый из адресов этой сети, то есть **192.168.1.0** для приведенного примера, и он не может назначаться сетевым интерфейсам в качестве их адреса. В результате такого подхода становится возможной адресация групп компьютеров – *сетей* и *подсетей*, что позволяет с помощью *маршрутизаторов (Router)* – устройств, соединяющих сети/подсети в единую *составную сеть (internet working)*, реализовать технологию маршрутизации дейтаграмм между сетями/подсетями.

Для разделения этих частей обычно используется 2 подхода:

- с помощью маски (стандарты RFC 950, RFC 1518), представляющей собой число в паре с IP-адресом. С помощью операции «логическое И» над этими двумя числами выделяется номер сети;

- с помощью классов адресов (стандарт RFC 791).

Вводится пять классов адресов: A, B, C, D, E.

A, B, C – используются для адресации сетей, D и E – имеют специальное назначение. Признаком, на основании которого IP-адрес относят к тому или иному классу, являются значения нескольких первых битов адреса.

Для разных пользователей существует потребность в сетях различного масштаба. Идентификация класса сети, к которому принадлежит IP-адрес, выполняется по старшему байту адреса (рисунок 1.1).

Класс	1 байт (октет)	2 байт (октет)	3 байт (октет)	4 байт (октет)	Наименьший номер сети	Наибольший номер сети	Маска подсети	Примечание	
A	0	№ сети	№ хоста			0.0.0.0 (0 - не используется)	127.0.0.0 (127- зарезервирован)	255.0.0.0 или /8	128 сетей (2 зарезервированы) по $2^{24} = 16\ 777\ 216$ адресов
B	1	0	№ сети	№ хоста		128.0.0.0	191.255.0.0	255.255.0.0 или /16	16,384 сетей по $2^{16} = 65,536$ адресов
C	1	1	0	№ сети	№ хоста	192.0.0.0	223.255.255.0	255.255.255.0 или /24	2,097,152 сетей по $2^8 = 256$ адресов
D	1	1	1	0			224.0.0.0	239.255.255.255	multicast (групповые адреса)
E	1	1	1	1	0		240.0.0.0	255.255.255.255	резерв

Рисунок 1.1 – Классы IP-адресов

В адресном пространстве IPv4 также *зарезервированы* следующие адреса *под специальные нужды*:

- 0.0.0.0 – адрес хоста, сгенерировавшего пакет (используется только в некоторых сообщениях протокола управляющих сообщений Интернета – ICMP);
- 255.255.255.255 – пакет с таким IP-адресом получателя рассыпается всем хостам, находящимся в той же сети, что и отправитель этого пакета – *ограниченное широковещательное сообщение (Limited Broadcast)*;
- в поле номера сети IP-адреса получателя все биты равны нулю – хост-получатель принадлежит той же сети, что и хост-отправитель (например, 0.0.0.X, X=1-224);
- в поле номера хоста IP-адреса получателя все биты равны нулю – такой адрес является адресом сети с заданным в поле номера сети адресом (например, X.X.X.0, X=1-224);
- в поле номера хоста IP-адреса получателя все биты равны единице – пакет рассыпается всем хостам сети с заданным в поле номера сети адресом – *широковещательное сообщение (Broadcast Message)* (например, X.X.X.255, X=1-224);
- старший байт IP-адреса = 127 – *кольцевой адрес (Loopback Address)* – петля (обычно используется адрес 127.0.0.1) – используется для тестирования программ и взаимодействия процессов в пределах одного хоста;
- блоки адресов, зарезервированные для локальных сетей (без выхода в Интернет или использующих сетевую трансляцию адресов) – одна сеть класса A 10.0.0.0-10.255.255.255, 16 сетей класса B 172.16.0.0-172.31.255.255, 256 сетей класса C 192.168.0.0 – 192.168.255.255.

В рамках IP протокола существуют *ограничения* при назначении IP-адресов:

- номера сетей и номера узлов не могут состоять из двоичных нулей или единиц;

- если IP-адрес состоит только из двоичных нулей, то он называется неопределенным адресом и обозначает адрес того узла, который сгенерировал этот пакет;
- если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет; такой адрес может быть использован только в качестве адреса отправителя;
- если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассыпаться всем узлам, находящимся в той же сети, что и источник этого пакета; такой адрес называется *ограниченным широковещательным*, поскольку пакет не сможет выйти за границы сети;
- если в поле адреса назначения в разрядах, соответствующих номеру узла, стоят только единицы, то пакет рассыпается всем узлам сети, номер которой указан в адресе назначения; такой тип адреса называется *широковещательным*;
- если первый октет адреса равен 127, то такой адрес называется внутренним адресом стека протоколов; он используется для тестирования программ, организации клиентской и серверной частей приложений, установленных на одном компьютере;
- групповые адреса, относящиеся к классу D, предназначены для экономичного распространения в Интернете, большой корпоративной сети аудио- или видеопрограмм.

Маской подсети называется 32-разрядное двоичное число, которое определяет, какая часть IP-адреса компьютера относится к адресу сети, а какая часть IP-адреса определяет адрес хоста в подсети. В маске подсети старшие биты, отведенные в IP-адресе компьютера для адреса сети, имеют значение 1, а младшие биты, отведенные в IP-адресе компьютера для адреса компьютера в подсети – 0.

Стандартным классам сетей можно поставить в соответствие следующие значения маски:

- класс A – 255.0.0.0;
- класс B – 255.255.0.0;
- класс C – 255.255.255.0.

2.1.1 Примеры решения задач

Пример №1. Известна маска подсети 255.255.255.0 и IP-адрес компьютера в сети 62.76.167.21. Необходимо найти номер сети и порядковый номер компьютера в сети.

Исходные данные	IP адрес	62.76.167.21
	Маска сети	255.255.255.0
	IP адрес	00111110.01001100.10100111.00010101
	Маска сети	11111111.11111111.11111111.00000000
Логическая операция	&	
Результат	Адрес сети	00111110.01001100.10100111.00000000
		62.76.167.0
	Номер компьютера	00000000.00000000.00000000. 00010101
		21

Пример №2. Если маска подсети 255.255.255.224 и IP-адрес компьютера в сети 162.198.0.157, чему равен номер сети и порядковый номер компьютера в сети. Определить адрес широковещательной рассылки.

Исходные данные	IP адрес	162.198.0.157
	Маска сети	255.255.255.224
	IP адрес	10100010.11000110.00000000.10011101
	Маска сети	11111111.11111111.11111111.11100000
Логическая операция	&	
Результат	Адрес сети	10100010.11000110.00000000.10000000
		162.198.0.128
<i>Номер компьютера</i>		00000000.00000000.00000000.000 11101
		29

Чтобы получить адрес широковещательной рассылки, необходимо выполнить операцию логического ИЛИ между IP-адресом и инверсной маской сети.

Исходные данные	IP адрес	10100010.11000110.00000000.10011101
	Инверсная маска (Wildcard)	00000000.00000000.00000000.00011111
Логическая операция	ИЛИ	
Результат	Адрес широковещательной рассылки (Broadcast)	10100010.11000110.00000000.10011111
		162.198.0.159

Определение количества различных адресов компьютеров, которые теоретически допускает маска, если два адреса (адрес сети и широковещательный) не используются.

Исходные данные	Маска сети	255.255.255.224 11111111.11111111.11111111.11100000
-----------------	------------	--

Так как три двухбайтных октета равны 255, то в двоичном виде они записываются как 24 единицы, а значит, первые три октета определяют адрес сети.

Запишем число 224 в двоичном виде: $224_{10} = 11100000_2$. В конце этого числа стоит 5 нулей, итого у нас есть 5 двоичных разрядов для того, чтобы записать адрес компьютера: $2^5 = 32$, но, так как два адреса не используются, получаем: $32 - 2 = 30$.

Пример №3. Определение диапазона адресов подсети, в которую входит хост 192.168.200.47/20 (192.168.200.47 255.255.240.0).

Решение:

1. Те разряды, которые относятся к адресу подсети, у всех хостов подсети должны быть одинаковы.

2. Адреса хостов в подсети могут быть любыми.

То есть, если наш адрес 192.168.200.47 и маска равна /20, то диапазон будет:

11000000.10101000.11001000.00101111 – адрес

11111111.11111111.11110000.00000000 – маска

11000000.10101000.1100XXXX.XXXXXXXX – диапазон адресов

где 0, 1 – определенные значения разрядов;

Х – любое значение.

Что приводит к диапазону адресов:

от 11000000.10101000.11000000.00000000 (192.168.192.0)

до 11000000.10101000.11001111.11111111 (192.168.207.255)

Пример №4. Определить максимальную длину маски сети, чтобы указанные IP-адреса находились в одной сети: 24.177.20.45 – 24.177.23.169.

Решение: чтобы определить максимальную длину маски сети необходимо перевести в двоичное представление оба адреса и посчитать число совпадающих бит, начиная со старшего бита, до первого различия.

В нашем задании первые два байта IP-адресов совпадают, и поэтому их не нужно переводить в двоичное представление. Так как каждый байт – это 8 бит, то мы уже имеем $8 \cdot 2 = 16$ совпадающих бит.

Рассмотрим третий байт IP-адресов. В двоичном виде (не забываем про незначащие разряды, которые равны 0!):

$$\begin{array}{l} 20 = 00010100_2 \\ 23 = 00010111_2 \end{array}$$

В третьем байте совпадают 6 бит. Таким образом, всего совпадает $16 + 6 = 22$ бит. Поэтому максимальная длина маски сети, при которой оба указанных IP-адреса будут лежать в одной подсети – это 22 бит.

2.2 Построение простейшей компьютерной локальной сети

Локальная компьютерная сеть (Local Area Network – LAN) представляет собой набор компьютеров (часто называемых рабочими станциями (Workstation)), серверов, сетевых принтеров, коммутаторов (Switch), маршрутизаторов (Router), точек доступа (Access Point), другого оборудования, а также соединяющих их кабелей, обычно расположенных на относительно небольшой территории или в небольшой группе зданий (учебный класс, квартира, офис, университет, дом, фирма, предприятие) (рисунок 1.2).



Рисунок 1.2 – Структура простейшей локальной компьютерной сети

В локальной сети можно выделить:

- оконечное оборудование пользователей, поставляющее данные в сеть и принимающее данные для обработки (рабочие станции, серверы, ноутбуки, сете-

вые принтеры и др.);

- активное сетевое оборудование, организующее каналы для передачи информации между оконечным оборудованием пользователей в структурах данных, называемых пакетами, кадрами, сообщениями (коммутаторы, маршрутизаторы, концентраторы, точки доступа, модемы и др.);

- пассивное сетевое оборудование, представляющее собой кабели, кабельные каналы (короба), разъемы, розетки и другое соединительное оборудование, а также стойки и подставки для размещения активного сетевого оборудования.

Для организации работы локальной компьютерной сети необходимо:

а) выполнить физическое построение компьютерной сети:

- установить в оконечное оборудование пользователей сетевые интерфейсные адAPTERы (Network Interface Card – NIC) (данный этап обычно пропускается, так как современные материнские платы оснащаются встроенными NIC);

- подобрать и разместить активное сетевое оборудование;

- выполнить соединение сетевых интерфейсных адAPTERов в оконечном оборудовании пользователей и разъёмов активного сетевого оборудования с помощью кабелей и разъемов (кабели и разъемы не используются при организации беспроводного соединения);

б) настроить параметры набора (стека) сетевых протоколов на оконечном оборудовании пользователей: задать сетевые имена устройств и адреса, установить требуемые параметры сетевых протоколов;

в) выполнить работы по организации совместно используемых сетевых ресурсов и по предоставлению доступа к этим ресурсам пользователей сети;

г) установить необходимое сетевое программное обеспечение (дополнительное к входящему в состав операционных систем).

Под конфигурированием адAPTERа подразумевается настройка используемых системных ресурсов и выбор скорости, режима передачи иногда и других параметров. Конфигурирование осуществляется путем настройки драйвера, параметры конфигурирования хранятся в энергонезависимой памяти EEPROM, установленной на адAPTERе. Для современных адAPTERов характерно конфигурирование с использованием технологии Plug And Play – автоматическое распределение BIOS или операционной системой системных ресурсов между подключенными устройствами с целью предотвращения конфликтов, происходящих при выделении одних и тех же ресурсов различным устройствам.

Наиболее массовым активным сетевым оборудованием современных локальных компьютерных сетей является сетевой коммутатор (*Switch*), к портам которого с помощью кабелей подключается оконечное оборудование пользователей и/или другое активное сетевое оборудование. Коммутаторы осуществляют передачу кадров (*Frame*), из порта, к которому подключено устройство-источник кадров (*Source*), в порт, к которому подключено устройство приемник кадров (*Destination*). Поиск выходного порта осуществляется коммутаторами по таблице коммутации на основании анализа адресной информации в заголовке кадра.

Иногда для организации локальной сети в качестве активного сетевого оборудования используют концентратор (*Hub*), внешним видом очень похожий на коммутатор. Однако принцип работы концентратора отличается: если коммутатор

анализирует адресную информацию в заголовках поступающих в его порты кадров и избирательно передает кадры с входного порта на выходной порт, к которому подсоединен получатель кадров, то концентратор просто копирует сигналы, соответствующие битам информации, со своего входного порта на все остальные порты. С практической точки зрения концентраторы имеют преимущество в скорости работы (точнее, в минимальной длительности задержки передаваемых кадров), поскольку они не выполняют буферизацию заголовков кадров и анализ адресной информации. Однако дублирование потоков кадров даже к тем устройствам, которые не являются адресатами (проверкой и отбрасыванием «не своих» кадров занимается сетевой интерфейсный адаптер устройства), приводит к снижению эффективности использования сети. Кроме того, существует возможность использования программ анализаторов протоколов, которые могут принимать и анализировать весь трафик, поступающий в адаптер. Очевидно, что в таком случае любой из компьютеров локальной сети сможет «видеть» трафик, передаваемый всеми остальными компьютерами, что является серьезным недостатком с точки зрения безопасности передачи информации.

В настоящее время достаточно популярным способом организации локальной сети является построение *беспроводных локальных сетей (Wireless Local Area Network – WLAN)*. Для их организации часто используют *точку доступа (Access Point)*, организующую радиоканалы между участниками сети, которые должны быть оснащены интерфейсными картами беспроводного доступа. При необходимости подключения беспроводного сегмента локальной сети к ее проводному сегменту на коммутаторе/концентраторе точка доступа подключается кабелем к одному из портов коммутатора/концентратора.

2.2.1 Конфигурирование сетевых средств операционных систем компьютеров локальной сети

Чтобы сетевые устройства могли узнать о присутствии других устройств, а также вести обмен данными между собой, на каждом из устройств должен быть установлен одинаковый набор (стек) сетевых протоколов. В настоящее время наиболее распространенным стеком сетевых протоколов является *TCP/IP – Transmission Control Protocol/Internet Protocol – протокол управления передачей/протокол Интернета*, его популярность связана с тем, что данный стек является необходимым условием для подключения компьютера к сети Интернет. Основной настройкой этого протокола является задание *IP-адреса*, который (для наиболее распространенной в настоящее время 4-й версии протокола IP) выглядит как четыре группы цифр, разделенных точками: X.X.X.X, где X – десятичное число в диапазоне от 0 до 255. Старшие одна две или три цифры определяют номер сети, к которой принадлежат компьютеры, для возможности обмена информацией в локальной сети на коммутаторе/концентраторе они должны принадлежать одной IP-сети. В простейшем случае можно использовать сеть с сетевой частью адреса 192.168.0, при этом для компьютеров сети можно задавать адреса от 192.168.0.1 до 192.168.255.254 (адреса 192.168.0.0 и 192.168.0.255 являются служебными). Другой важный параметр стека TCP/IP – *маска подсети (Subnet Mask)*, представляющая собой 32-битное число, старшая часть которого

содержит непрерывный ряд единиц, а младшая – непрерывный ряд нулей. Данный параметр позволяет «разрезать» IP-сети на подсети меньшего достаточно гибко задаваемого размера. В нашем случае будем использовать маску 255.255.255.0, задающую подсеть с адресом, определяемым первыми тремя числами IP-адреса – 192.168.0, в которую можно включить 254 компьютера с адресами от 192.168.0.1 до 192.168.0.254.

Настройку стека TCP/IP в операционной системе Microsoft Windows 7 можно выполнить, открыв свойства Протокола Интернета версии 4 (TCP/IPv4) в свойствах Сетевого подключения, которое находится: *Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера* (для этого понадобятся права Администратора) (см. рисунок 1.3).

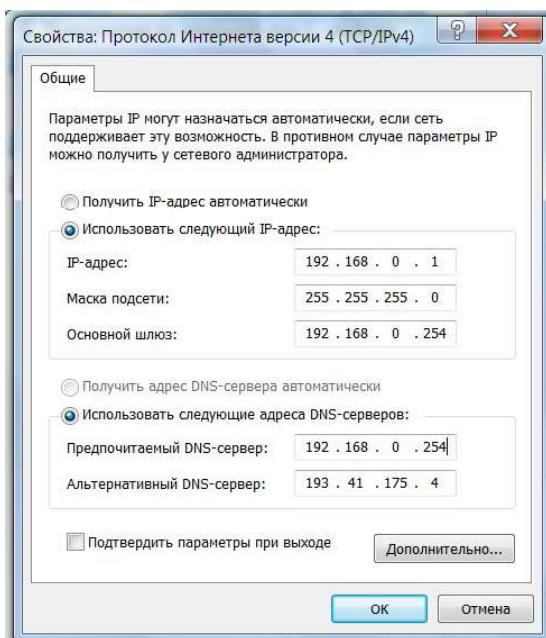


Рисунок 1.3 – Окно свойств сетевого подключения протокола Интернета версии 4 (TCP/IPv4) с адресной информацией

В простейшей локальной сети основной шлюз и DNS-сервер можно не задавать. Кроме адресной информации, каждому компьютеру должно быть задано сетьевое имя компьютера и имя рабочей группы, в которую он входит. В операционной системе Microsoft Windows 7 имена можно задать (также обладая правами Администратора): *Панель управления → Система → Дополнительные параметры → Имя компьютера*.

После задания уникальных IP-адресов и сетевых имен устройствам локальной сети можно проверить наличие связи между ними. Проверку лучше начать с физического уровня модели взаимодействия открытых систем, на котором компьютеры обмениваются сигналами, кодирующими биты информации. Для этого достаточно убедиться, что на коммутаторе/концентраторе светится светодиод, соответствующий порту, к которому подключено проверяемое устройство компьютер (в случае, если коммутатор/концентратор находится в труднодоступном месте, можно проверить, светится ли светодиод сетевого адаптера устройства). Если

светодиоды светятся, это свидетельствует о наличии соединения между приемниками и передатчиками сетевого адаптера и коммутатора/концентратора, если нет, то возможен либо обрыв провода, либо плохой контакт при монтаже разъема, либо неправильная разводка пар в разъемах, точнее это можно выяснить с помощью специальных тестеров кабельных сетей.

При наличии связи на физическом уровне, можно попробовать проверить связь на сетевом уровне. Для этого необходимо открыть окно командной строки (*Пуск → Выполнить → cmd*) и запустить утилиту *ping*, в качестве аргумента которой указать IP-адрес удаленного компьютера, соединение к которому необходимо проверить.

Независимо от того, как обращаются к сетевому устройству: через консоль терминальной программы, подсоединённой через ноль-модем к СОМ-порту сетевого устройства, либо в рамках сеанса протокола Telnet, устройство можно перевести в один из режимов:

Пользовательский режим – это режим просмотра, в котором пользователь может только просматривать определённую информацию о сетевом устройстве, но не может ничего менять. В этом режиме приглашение имеет вид типа *Switch>*.

Привилегированный режим – поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. В этом режиме приглашение имеет вид типа *Switch#*.

Режим глобального конфигурирования – реализует мощные односторонние команды, которые решают задачи конфигурирования. В этом режиме приглашение имеет вид типа *Switch(config)#*.

При первом входе в сетевое устройство пользователь видит командную строку пользовательского режима вида:

```
Switch>
```

Команды, доступные на пользовательском уровне являются подмножеством команд, доступных в привилегированном режиме. Эти команды позволяют выводить на экран информацию без смены установок сетевого устройства.

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим.

```
Press ENTER to start.
Switch>
Switch> enable
Switch#
Switch# disable
Switch>
```

Здесь и далее вывод сетевого устройства будем обозначать обычным шрифтом, а ввод пользователя **жирным** шрифтом.

О переходе в этот режим будет свидетельствовать появление в командной строке приглашения в виде знака **#**. Из привилегированного уровня можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая

режимы конфигурирования интерфейса, подинтерфейса, линии, сетевого устройства, карты маршрутов и т.п. Для выхода из системы IOS необходимо набрать на клавиатуре команду ***exit*** (выход).

```
Switch> exit
```

Команды в любом режиме IOS распознаёт по первым уникальным символам. При нажатии табуляции IOS сам дополнит команду до полного имени.

При вводе в командной строке любого режима имени команды и знака вопроса (?) на экран выводятся комментарии к команде. При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много экранов строк, поэтому иногда внизу экрана будет появляться подсказка - *More*. Для продолжения следует нажать *enter* или пробел.

Команды режима глобального конфигурирования определяют поведение системы в целом. Кроме этого, команды режима глобального конфигурирования включают команды переходов в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования используется команда привилегированного режима ***configure***. При вводе этой команды следует указать источник команд конфигурирования: *terminal* (терминал), *memory* (энергонезависимая память или файл), *network* (сервер tftp (Trivial ftp – упрощённый ftp) в сети). По умолчанию команды вводятся с терминала консоли. Например:

```
Switch# configure terminal
Switch(config)# (commands)
Switch(config)# exit
Switch#
```

Примечание: для вызова команд пользовательского режима из привилегированного или команд привилегированного режима из режима глобальной конфигурации достаточно перед используемой командой добавить команду ***do***.

Команды для активизации частного вида конфигурации должны предваряться командами глобального конфигурирования. Так для конфигурации интерфейса, на возможность которой указывает приглашение *Switch(config-if) #*, сначала вводится глобальная команда для определения типа интерфейса и номера его порта:

```
Switch# conf t
Switch(config)# interface type port
Switch(config-if)# (commands)
Switch(config-if)# exit
Switch(config)# exit
```

3 ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

3.1 Общая характеристика симулятора компьютерных сетей

В качестве лабораторной установки используется персональный компьютер с инсталлированной программой Packet Tracer, позволяющей осуществлять моделирования компьютерных сетей, построенных на оборудовании корпорации Cisco. Симулятор Cisco Packet Tracer поддерживает интерфейс командной строки

Cisco IOS для конфигурирования устройств. С помощью этой программы можно создавать, настраивать, изучать сети и устранять неполадки, используя виртуальное оборудование и модели соединений [1].

Packet Tracer позволяет моделировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров и т.д. Интерактивное взаимодействие пользователей с симулятором дает весьма правдоподобное ощущение настройки реальной сети.

Среда Packet Tracer позволяет настраивать оборудование, используемое в сети, удобным для пользователя образом. Предусмотрено управление сетевыми устройствами с помощью команд операционной системы Cisco IOS, за счет графического интерфейса, так же используется интерфейс командной строки. Несмотря на то, что на данном сетевом симуляторе реализованы не все функции операционной системы Cisco IOS, функциональность, которую обеспечивает программа симуляции, хватает для построения большинства типов сетевых систем и понимания технологических принципов их конфигурации и функционирования.

Cisco Packet Tracer поддерживает режим визуализации, с помощью которого пользователь может отследить перемещение данных по сети, появление и изменение параметров пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения пакетов. Таким образом, анализ событий, происходящих в сети, позволяет понять и исследовать механизм ее работы и обнаружить неисправности.

Packet Tracer может быть использован не только как симулятор для виртуальных сетей, но и как сетевое приложение для симулирования виртуальной сети через реальную сеть, в том числе Интернет. Пользователи на разных компьютерах, независимо от их местоположения, могут работать над одним проектом, производя его настройку или устраняя проблемы.

На основе Cisco Packet Tracer пользователь может строить не только логическую, но и физическую модель сети и, следовательно, получать навыки проектирования. Созданную в учебной среде схему сети можно наложить на чертеж реально существующего здания. С учетом физических ограничений в тех или иных помещениях можно спроектировать размещение устройств, длину и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

Тем не менее, ни один симулятор не может полностью заменить опыт работы в реальной сети. Однако существующее программное обеспечение в этой сфере способствует эффективному обучению сетевым технологиям, доступному в любое время и в любом месте.

3.2 Рабочее окно симулятора Cisco Packet Tracer

При запуске программы Cisco Packet Tracer на экране компьютера появляется главное окно симулятора (рисунок 1.4). Основными составляющими симулятора являются следующие.

1. Главное меню программы:

- Файл – содержит операции открытия / сохранения документов;
- Правка – стандартные операции «копировать / вырезать, отменить / повторить»;

- Настройки/Параметры – параметры анимации, профиль пользователя и др.;
- Вид – масштаб рабочей области и панели инструментов;
- Инструменты – цветовая палитра и окно пользовательских устройств;
- Расширения – мастер проектов, многопользовательский режим;
- Помощь/Справка – справочная информация.

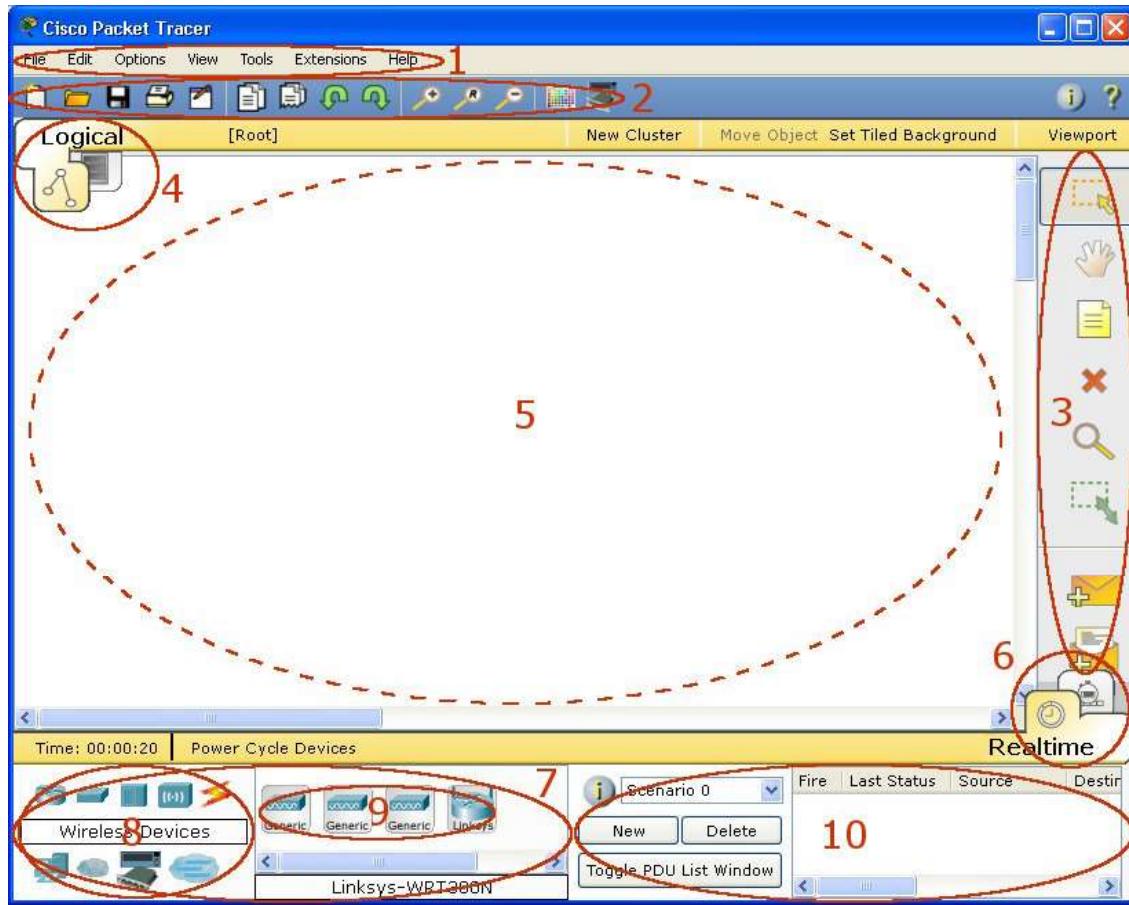


Рисунок 1.4 – Главное окно программы Cisco Packet Tracer

2. Панель инструментов, часть которых дублирует пункты меню (содержит кнопки быстрого вызова команд из меню *File* и *Edit* а так же команд *Zoom*, *Drawing Palette* и *Custom Devices Dialog*).

3. Панель инструментов рабочей области содержит наиболее часто используемые операции, применяемые при построении модели сети: инструменты выделения, удаления, перемещения, масштабирования объектов, а также формирование произвольных пакетов.

4. Навигационная панель позволяет переключать рабочую область между логической и физической топологией сети. Физическая топология подразумевает расположение устройств в городе, районе, офисе. Здесь можно посмотреть, как топологию сети всего города, так и расположение устройств в офисе, и даже на отдельной Rack-стойке.

5. Рабочая область занимает большую часть окна программы. Здесь происходит конструирование виртуальной сети, где размещаются устройства и строятся связи между ними. Двойной клик по любому устройству открывает окно его конфигурации. Окно конфигурации устройств состоит из 3-х вкладок:

– *Physical* – показывает внешний вид устройства и позволяет добавлять либо убирать модули. Модули нельзя добавлять/извлекать при включенном устройстве.

– *Config* – эта вкладка не открывается, пока устройство не загрузилось. Здесь осуществляется графическое конфигурирование оборудования Cisco без применения командной строки, но для информативности внизу отображаются команды, которые выполняются при конфигурации.

– *CLI/Desktop* – в зависимости от устройства позволяет получить доступ к командной строке IOS либо к рабочему столу Linux.

6. Панель симуляции/реального времени. После запуска программа находится в логическом режиме реального времени, можно строить сеть и смотреть, как она работает. Данная панель позволяет переключаться в режим симуляции и обратно. В этом режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет наглядно видеть, по какому интерфейсу в данный момент перемещается пакет, какой протокол используется и т.д. В режиме симуляции можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован.

7. Блок выбора сетевых компонентов. Окно выбора устройств либо способов связи, размещаемых в рабочей области. Состоит из двух составных частей: области выбора типа устройства и области выбора конкретной модели устройства.

8. Окно типа устройств. Позволяет выбрать и моделировать большое количество устройств различного назначения: маршрутизаторы, коммутаторы (в том числе и мосты), хабы и повторители, конечные устройства – ПК, серверы, принтеры, IP-телефоны; беспроводные устройства: точки доступа и беспроводные маршрутизаторы; другие устройства – Internet-облако, DSL-модем и кабельный modem, а также разнообразные линии связи от консольного кабеля до оптической линии.

9. Окно моделей устройств. Область выбора конкретной модели устройства указанного типа. В частности, Packet Tracer может моделировать следующие телекоммуникационные устройства: маршрутизаторы типов 1841, 2620XM, 2621XM, 2811; коммутаторы типов 2959-24, 2950T, 2960, 3560; беспроводные устройства типа Linksys-WRT300N и др.

10. Окно пользовательских пакетов. Окно управляет пакетами, которые были созданы в сети во время сценария симуляции.

3.3 Оборудование и линии связи в Cisco Packet Tracer

3.3.1 Маршрутизаторы

Маршрутизаторы (рисунок 1.5) используется для поиска оптимального маршрута передачи данных на основании специальных алгоритмов маршрутизации, например, выбор маршрута (пути) с наименьшим числом транзитных узлов. Работают на сетевом уровне модели OSI.



Рисунок 1.5 – Панель выбора маршрутизаторов

3.3.2 Коммутаторы

Коммутаторы (рисунок 1.6) – это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в преде-

лах одного или нескольких сегментов сети. Коммутатор передаёт пакеты на основании внутренней таблицы – таблицы коммутации, следовательно, трафик идёт только на тот MAC-адрес, которому он предназначается, а не повторяется на всех портах (как на концентраторе).



Рисунок 1.6 – Панель выбора коммутаторов

3.3.3 Беспроводные устройства

Основными узлами беспроводных Wi-Fi-сетей, осуществляющими ретрансляцию кадров, являются точки доступа (рисунок 1.7).



Рисунок 1.7 – Панель выбора беспроводных устройств

3.3.4 Линии связи

В качестве линий связи, соединяющих телекоммуникационные устройства между собой, могут быть использованы консольный кабель, коаксиальный кабель или витая пара и оптоволокно (рисунок 1.8). Дополнительно можно указать тип кабельного соединения: прямое или кроссоверное. В таблице 1.1 приведено описание предлагаемых кабельных линий связи.



Рисунок 1.8 – Панель выбора линий связи

Таблица 1.1 – Типы линий связи

Тип кабеля	Описание
	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Скорость соединения обеих сторон должна быть одинаковая, передаваться может любой поток данных.
	Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, которые функционируют на разных уровнях OSI. Сигнал передается напрямую из одного конца в другой, а именно с 1-го контакта на 1-й, с 2-го на 2-й и т. д. Используется между ПК и хабом, ПК и DSL-модемом, хабом и коммутатором.
	Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Используется для соединения двух ПК напрямую, т. е. без хаба или коммутатора. Таким образом, можно подключить только 2 компьютера одновременно.

Тип кабеля	Описание
	Optovolokonnyy kabel' ispolzuetsya dlya soedineniya mezhdu opticheskimi portami.
	Soedinenie cherez telefonnuyu liniju moyet byt' osuchestvleno tylko mezhdu ustroystvami, imeyushchimi modemnye porty.
	Koaksialnyy kabel' ispolzuetsya dlya soedineniya mezhdu koaksialnymi portami.
	Soedineniya cherez posledovatel'nye porty, chasto ispolzuutsya dlya svyazi WAN. Dlya nastrойki takix soedinenii neobходimo ustavotit' sinchronizatsiu na storone DCE-ustroystva. Synchronizatsia DTE vykonyaetsya po výboru. Storony DCE mozhno opredelit' po malen'koj ikonke «chakov» ryadom s portom. Pri výbore tipa soedineniya Serial DCE, pervoe ustroystvo, k kotoromu primenyaetsya soedinenie, stavit'sya DCE-ustroystvom, a vtoroe - avtomaticheski stanaet storonoy DTE. Vozmozhno i obratnoe raspolozhenie storon, esli vybran tip soedineniya Serial DTE.

3.3.5 Конечные устройства

Здесь располагаются непосредственно конечные узлы, хосты, сервера, принтеры, телефоны и другое оборудование (рисунок 1.9).



Рисунок 1.9 – Панель выбора конечных устройств

3.3.6 Эмуляция Интернета

В этом блоке (рисунок 1.10) располагаются устройства, используемые при эмуляции глобальных сетей, в частности модемы различных типов (DSL или кабельные), «облако» и проч.

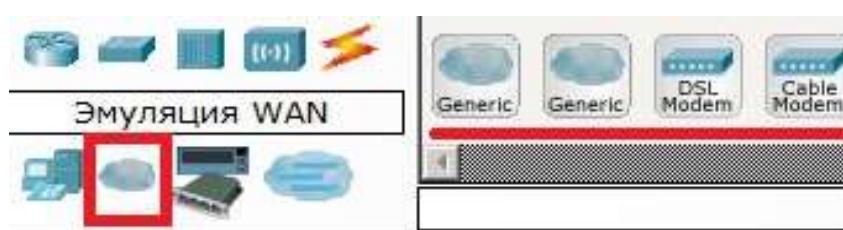


Рисунок 1.10 – Панель выбора топологии сети

3.3.7 Пользовательские устройства



Рисунок 1.11 – Панель выбора пользовательских устройств

3.3.8 Облако для многопользовательской работы

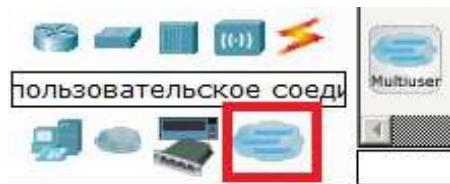


Рисунок 1.12 – Выбор облака для многопользовательской работы

3.4 Примеры подключения к устройствам фирмы Cisco

В Packet Tracer'е управлять оборудованием можно следующими способами:

- GUI (Graphical user interface);
- CLI (Command-line interface) в окне управления;
- терминальное подключение с рабочей станции через консольный кабель;
- удаленное подключение Telnet.

Интерфейс последних трёх идентичный – отличается лишь способ подключения. В реальных устройствах доступны Telnet/SSH, терминальное подключение с рабочей станции через консольный кабель и web-интерфейс (Cisco SDM).

3.4.1 Управление через консольный порт

Данный тип подключения используется в следующих случаях:

- при первоначальной настройке оборудования;
- если что-то сломалось и нельзя получить удаленный доступ к оборудованию;
- если администратор находится рядом с оборудованием.

В качестве консольного порта в большинстве случаев используется СОМ-порт либо Ethernet-порт. Однако современные ПК имеют только USB-порты. В таких случаях используются конвертеры USB-to-COM либо конвертеры RS232-to-Ethernet.

Управление через консоль доступно сразу, а для соединения по telnet нужно установить пароль. Для того чтобы подключиться к устройствам фирмы Cisco, для их последующего конфигурирования через консольный порт в рабочей области Packet Tracer необходимо разместить коммутатор **Catalyst 2960** и один компьютер. Далее с помощью консольного кабеля следует соединить интерфейс **RS-232** компьютера с консольным портом коммутатора. Затем для того, чтобы подключиться с компьютера к коммутатору через консоль, нужно щелкнуть два раза левой кнопкой мыши по изображению компьютера, перейти на вкладку **Desktop** и выбирать приложение **Terminal**.

Обычно все параметры соединения по умолчанию менять смысла нет. Поэтому достаточно нажать на кнопку «OK» и будет осуществлено подключение к коммутатору через консольный порт.

Если в энергонезависимой памяти устройства отсутствует конфигурационный файл (startup-config), а так оно и будет при первом включении нового оборудования, появится информационное окно Initial Configuration Dialog prompt. В окне изложено краткое руководство, позволяющее шаг за шагом настроить основные параметры устройства (hostname, пароли, интерфейсы). Если есть необходимость – читаем, в противном случае отвечаем **no**. Появляется следующее приглашение:

Switch>

Все проделанные действия в симуляторе равносильны реальному соединению компьютера коммутатором через консольный порт. При подключении к коммутатору через консольный порт, по умолчанию он не запрашивает ни логина, ни пароля, что является небезопасным. В таком случае к коммутатору консольным кабелем может подключиться злоумышленник и изменить конфигурацию.

Можно сделать, чтобы при подключении через консольный порт запрашивался только пароль, тогда надо сконфигурировать линию консоли следующим образом:

```
Switch(config)#line console 0
Switch(config-line)#password 123
Switch(config-line)#login
```

При такой конфигурации пользователю при входе не придется вводить имя пользователя, а для получения доступа достаточно будет ввести пароль, который задавался командой `password`.

Так же для линии консоли можно настроить еще несколько параметров, которые смогут немножко повысить безопасность системы. Узнать что это за параметры можно перейдя к конфигурированию линии консоли с помощью `line console 0` и выполнив команду «?».

3.4.2 Удаленное управление с помощью web-интерфейса

Предположим, что удаленный компьютер подключен к порту коммутатора, который находится VLAN 1. Компьютер имеет IP-адрес 192.168.1.2 с маской 255.255.255.0 и шлюзом по умолчанию 192.168.1.1. Для того чтобы настроить связь с компьютера с коммутатором, необходимо выполнить команду:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown
```

После чего на компьютере необходимо открыть браузер и попробовать получить доступ к `http://192.168.1.1`.

Обычно оборудование фирмы Cisco не конфигурируется с помощью web-интерфейса. Все изменения конфигурации выполняются с помощью консоли, так как она позволяет выполнять более гибкое (и порой недоступное в web-интерфейсе) и безопасное конфигурирование. Поэтому можно отключить доступ к вашему оборудованию при помощи web-интерфейса, для этого потребуется отключить действующий на оборудовании web-сервер, это можно выполнить с помощью следующих команд:

```
Router(config)#no ip http server
Router(config)#no ip http secure-server
```

3.4.3 Настройка доступа по Telnet

Telnet – стандартная утилита, как и SSH. Для доступа к Cisco по этим протоколам нужно настроить пароли доступа. Возможность использования SSH зависит от лицензии IOS. Используя службу telnet можно удаленно конфигурировать свое оборудование.

Соберем в Packet Tracer схему, представленную на рисунке 1.13.

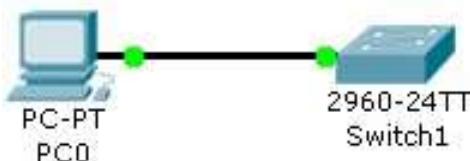


Рисунок 1.13 – Компьютер подключен к коммутатору прямым Ethernet-кабелем.

Компьютеру задан IP-адрес 192.168.1.2 с маской 255.255.255.0 и шлюзом по умолчанию 192.168.1.1. Коммутатор сконфигурирован следующим образом:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#line vty 0 4
Switch(config-line)#password 123
```

Первыми четырьмя строчками задается IP-адрес коммутатору, точнее его виртуальному интерфейсу VLAN 1.

Команда line vty 0 4 позволяет сконфигурировать линии виртуальных терминалов. Командой password 123 задается пароль 123 для доступа (если эту команду не выполнять, то при попытке подключения к устройству появится сообщение – Connection to 192.168.1.1 closed by foreign host). Подключение по telnet или ssh называется виртуальным терминалом (vt). 0 4 – это 5 пользовательских виртуальных терминалов = telnet сессий.

Выполнив данные команды можно попробовать удаленно подключиться к коммутатору, для этого необходимо перейти к консоли компьютера и ввести команду telnet 192.168.1.1, если все сделано верно, то откроется доступ к консоли оборудования и появится сообщение

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>
```

Если необходимо, чтобы при доступе через telnet запрашивался не только пароль, но и еще и логин пользователя, то необходимо сконфигурировать линии виртуальных терминалов следующим образом:

```
Switch(config)#line vty 0 4
Switch(config-line)# login local
```

Только перед этим на оборудовании необходимо создать учетную запись пользователя командой **Switch(config)#username user password 123**.

Итак, указанных выше команд достаточно, чтобы попасть в пользовательский режим, но недостаточно для привилегированного.

Настройки пароля для enable-режима представлены на рисунке 1.13:

```
Router(config)#enable secret 123456
```

```

PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>

[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>enable
% No password set.
Switch>enable
Password:
Switch#

```

Рисунок 1.13 – Настройка пароля для enable-режима

При настройке `secret` пароль хранится в зашифрованном виде в конфигурационном файле, а `password` – в открытом. Поэтому рекомендуется использование `secret`. Если всё-таки задаётся пароль командой `password`, то следует применить также `service password-encryption`, тогда пароль в конфигурационном файле будет зашифрован:

```

line vty 0 4
password 7 08255F4A0F0A0111

```

3.4.4 Настройка баннера

Баннер – это своеобразная вывеска, которая предназначена для сообщения определенной информации, любому, кто пытается получить доступ к сетевому устройству. Логин-баннер отображается пользователю при любом его подключении к устройству с использованием `telnet`, `ssh`-клиента или при подключении с помощью консоли (`RS232`). Существует 3 вида баннеров: `motd`, `exec`, `incoming`.

Синтаксис команды `banner` имеет следующую структуру:

```
banner motd {char} {banner text} {char}
```

где – `{char}` специальный символ разделителя, который не отображается в тексте баннера (символ `#` означает начало и конец строки). Какое-либо содержание между первым и вторым специальным разделителем интерпретируется как баннер-сообщение.

Пример: создание баннера message-of-the-day (MOTD) :

```
dyn1(config)# banner motd #Hello! I'm $(hostname). You are connected on line $(line) on domain $(domain)#

```

```

dyn3# telnet 192.168.1.1
Trying 192.168.1.1 ... Open
Hello! I'm dyn1. You are connected on line 2 on domain xgu.ru

```

3.5 Построение и настройка локальной компьютерной сети

3.5.1 Моделирование и исследование работы локальной сети в Cisco Packet Tracer

Для создания сети необходимо на рабочую область перетащить требуемые оконечные устройства пользователей – компьютеры, ноутбуки, серверы, принтеры и другие устройства.

После размещения необходимого оборудования пользователей можно аналогичным образом разместить на рабочей области сетевое оборудование, сгруппированное в следующих типах устройств: *маршрутизаторы (Routers)*, *коммутаторы (Switches)*, *концентраторы (Hubs)*, *беспроводные устройства (Wireless Devices)* и др.

Для соединения устройств необходимо выбрать тип соединения (прямой медный кабель – *Copper Straight-Through* для соединения компьютера и коммутатора). Подобным образом необходимо соединить все устройства. Обратите внимание, что при создании нового соединения занятые порты устройства не отображаются во всплывающем окне.

Если создавать соединение с автоматическим выбором типа (*Automatically Choose Connection Type*), то всплывающие окна появляться не будут, а Packet Tracer сам определит тип соединения и используемые порты (но эту возможность использовать не рекомендуется, поскольку нужно представлять, какие порты и как соединяются).

После завершения соединения устройств сети Packet Tracer сигнализирует о наличии соединений на физическом и канальном уровнях двумя зелеными периодически мигающими квадратиками на концах каждого соединения (мигание означает активность линии). При отсутствии соединения квадратики становятся красными. Это можно проверить, выключив питание одного из компьютеров. Для этого выполните щелчок левой кнопкой мыши на одном из компьютеров и перейдите в открывшемся окне на вкладку *Физическая конфигурация (Physical)*. Выполните щелчок мышью по кнопке питания на изображении компьютера, обратите внимание, что находящийся над ней индикатор погас. После включения устройства квадратик на линии связи возле устройства не сразу изменяет цвет на зеленый. Это обусловлено необходимостью некоторого времени на распознавание устройства коммутатором.

Следующим шагом может быть создание беспроводного сегмента сети и подключение его к проводной сети. Для этого необходимо добавить на рабочую область *Точку доступа (Access Point-PT)*, предварительно выбрав в Панели типов устройств *Беспроводные устройства (Wireless Devices)*, добавьте также из группы *Оконечные устройства (End Devices) Ноутбук (Laptop-PT)*.

Поскольку ноутбук, по умолчанию, оснащен проводным интерфейсом, необходимо заменить его на беспроводный. Для этого необходимо выполнить щелчок левой кнопкой мыши на ноутбуке и перейти на вкладку *Физическая конфигурация (Physical)*. Чтобы увидеть изображение ноутбука, необходимо прокрутить линейку прокрутки вниз.

Затем нужно отключить питание ноутбука, выполнив щелчок левой кнопкой мыши на кнопке питания, при этом погаснет индикатор питания. Далее необходимо перетащить мышью модуль с проводным интерфейсом в *Список модулей (MODULES)* слева от изображения ноутбука. А после этого, перетащить верхний модуль с беспроводным интерфейсом *Linksys-WPC300N* из *Списка модулей*

(MODULES) в разъем ноутбука, в котором был установлен модуль с проводным интерфейсом. Включив питание ноутбука на физическое схеме будет видно, что ноутбук связался с точкой доступа по радиоканалу (см. рисунок 1.15).

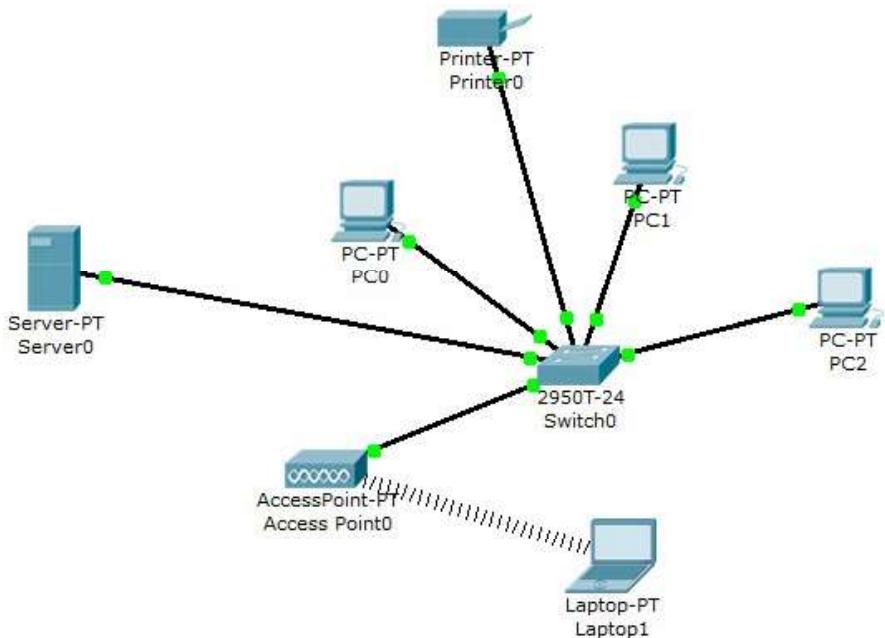


Рисунок 1.15 – Завершенная топология локальной компьютерной сети

Добавьте к сети из группы *Оконечные устройства (End Devices)* на Панели типов устройств *Сервер (Server-PT)* и *Принтер (Printer-PT)*. Оба устройства по умолчанию оснащены проводными интерфейсами *Fast Ethernet*, работающими со скоростью 100 Мбит/с. Подсоедините принтер к порту коммутатора аналогично соединению с ПК. Замените сетевой интерфейс сервера на интерфейс *Gigabit Ethernet*, работающий со скоростью 1000 Мбит/с. Для этого выполните щелчок на изображении сервера и на вкладке *Физическая конфигурация (Physical)* после выключения питания сервера замените так, как для ноутбука, сетевой интерфейс сервера на модуль *PC-HOST-NM-1CGE*.

Обратите внимание, что при подсоединении сервера к коммутатору необходимо выбрать на коммутаторе гигабитный порт, например, *Gigabit Ethernet 1/1*. В этом случае пакеты между коммутатором и сервером будут проходить на скорости в 10 раз большей скорости между коммутатором и остальными устройствами сети, что является оправданным, так как сервер обычно используется несколькими устройствами.

После создания сети следующим шагом является конфигурирование устройств. Сетевые имена устройств задаются автоматически при создании, их можно изменять прямо в рабочей области или в окне конфигурирования устройств. Устройства Packet Tracer поддерживают стек сетевых протоколов TCP/IP, причем поддерживается и IPv4 (в настоящее время наиболее распространенной), и IPv6 (переход к которой уже начался). В данной работе мы будем задавать устройствам адреса протокола IPv4.

Назначение имен и IP-адресов ПК, принтера и сервера происходит одинаковым образом, поэтому приведем последовательность действий по конфигурированию этих параметров на примере ПК. Выполните щелчок по изображению

устройства левой кнопкой мыши, при этом откроется окно конфигурирования устройств, выберите его вкладку *Конфигурация (Config)*.

Из списка слева выберите команду *Настройки (Settings)* для перехода к окну, в котором можно ввести/изменить сетевое имя устройства.

Здесь также можно указать IP-адреса *шлюза (Gateway)* сети, в которую входит данное устройство, и *DNS-сервера*, на котором находятся соответствия имен пользовательских устройств сети и их IP-адресов, и указать будет ли назначаться им адрес автоматически (с использованием сервера, работающего по протоколу *Dynamic Host Configuration Protocol – DHCP-сервера*) или вручную (*Static*).

Сетевой шлюз (Gateway) представляет собой сетевой интерфейс, через который сетевые пакеты от устройств данной сети уходят в другие сети и пакеты от устройств других сетей входят в данную сеть. Поскольку в данной работе моделируется только одна сеть, адрес шлюза задавать не нужно. Рассмотрение работы *Доменной системы имен (Domain Name System – DNS)* и конфигурирование DNS-сервера будет рассмотрено на последующих практических занятиях. Без конфигурирования такого сервера мы сможем посыпать пакеты с помощью утилиты *ping*, используя в качестве ее аргумента только IP-адрес удаленного компьютера. После конфигурирования DNS-сервера появляется дополнительная возможность связи с ним по его сетевому имени.

Из списка слева выберите тип сетевого интерфейса устройства (например, *Fast Ethernet*) для открытия окна задания адресной информации. В поле *IP-адрес (IP Address)* для компьютера с сетевым именем *PC1* введите адрес *192.168.0.1*, далее выполните щелчок в поле *Маска подсети (Subnet Mask)*, программа автоматически введет маску *255.255.255.0*, оставьте ее без изменений. Обратите внимание, что на этой вкладке автоматически задается MAC-адрес, а также скорость и режим передачи данных (100 Мбит/с и полный дуплекс).

Выполните аналогичным способом конфигурирование остальных пользовательских устройств созданной локальной сети, задав им IP-адреса и маски, приведенные в таблице 1.2. Обратите внимание, что сетевой интерфейс сервера имеет тип *Gigabit Ethernet* и работает на скорости 1000 Мбит/с.

Таблица 1.2 – Адресная информация для конфигурирования пользовательских устройств локальной компьютерной сети на рисунке 1.15

Устройство	Сетевое имя	IP-адрес	Маска подсети
ПК-1	PC1	192.168.0.1	255.255.255.0
ПК-2	PC2	192.168.0.2	255.255.255.0
ПК-3	PC3	192.168.0.3	255.255.255.0
Ноутбук	Laptop1	192.168.0.4	255.255.255.0
Сетевой принтер	Printer0	192.168.0.5	255.255.255.0
Сервер	Server0	192.168.0.6	255.255.255.0

Конфигурирование адресов для ноутбука имеет особенности, поскольку мы оснастили его беспроводным интерфейсом. По умолчанию окно конфигурирования интерфейса открывается с установленной настройкой автоматического задания IP-адреса и маски подсети устройствам (*DHCP*). Но поскольку в данной сети отсутствует DHCP-сервер, следует переключить установку в режим ручного задания адресов (*Static*) и задать IP-адрес и маску подсети описанным выше способом.

Обратите внимание на наличие настроек *аутентификации* (*Authentication*) устройств при беспроводном подключении к точке доступа – передачу точке доступа пароля, по которому она будет подключать устройство, и настроек *шифрования*, передаваемых по беспроводной сети данных (*Encryption*). Учитывая простоту несанкционированного подключения к беспроводной сети, на практике эти возможности являются часто используемыми. Пока оставьте их отключенными (*Disabled*).

Конфигурирование сетевого оборудования моделируемой локальной сети выполняется автоматически, однако просмотр возможных параметров конфигурации представляет интерес. В списке интерфейсов беспроводной точки доступа присутствуют два интерфейса – *Port 0* – проводной интерфейс Fast Ethernet, связывающий точку доступа с коммутатором, и беспроводный интерфейс *Port 1*. Здесь так же, как и для беспроводного адаптера есть поля для настройки аутентификации и шифрования, включая указание ключевой/парольной фразы, которую должен передать беспроводный адаптер для подключения к точке доступа.

Конфигурационные параметры коммутатора в окне глобальных настроек (*Global Settings*), включающие имя коммутатора, отображаемое на схеме сети (*Display Name*) и хост-имя (*Hostname*), по которому коммутатор идентифицируется командами межсетевой операционной системы Cisco (*Internetwork Operating System – IOS*) – программного обеспечения, зашитого в постоянную память большинства сетевых устройств производства Cisco Systems. Все выполняемые настройки сопровождаются соответствующими им командами IOS в окне *Equivalent IOS Command*. При выборе команды База данных *VLAN* (*VLAN Database*) из списка команд слева отображается окно со списком виртуальных локальных сетей (*Virtual LAN – VLAN*) – технологии, позволяющей приписывать порты сетевых устройств к различным VLAN, тем самым разделяя эти порты на отдельные сети на канальном уровне. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. В нашей сети все порты приписаны к VLAN с именем *default* (по-умолчанию) и идентификатором 1.

Для проверки связи между устройствами смоделированной локальной сети можно использовать утилиту *ping*. Для этого выполните щелчок левой кнопкой мыши, например, на ПК и перейдите на вкладку *Рабочий стол* (*Desktop*). На нем будут доступны дополнительные инструменты для настройки данного устройства (их доступность зависит от физического конфигурирования устройства – наличия тех либо иных модулей или устройств). Нам понадобится инструмент *Окно командной строки* (*Command Prompt*), в котором можно запустить утилиту *ping* с IP-адресом устройства сети, связь с которым проверяется в качестве ее аргумента.

Также существует возможность проверить связь с сервером, открыв на нем Web-страницу с помощью Web-браузера, которым оснащен ПК. Это возможно, поскольку на сервере, по умолчанию, устанавливается целый ряд серверных приложений, в том числе и HTTP-сервер с несколькими простыми HTML-страницами (рисунок 1.16).

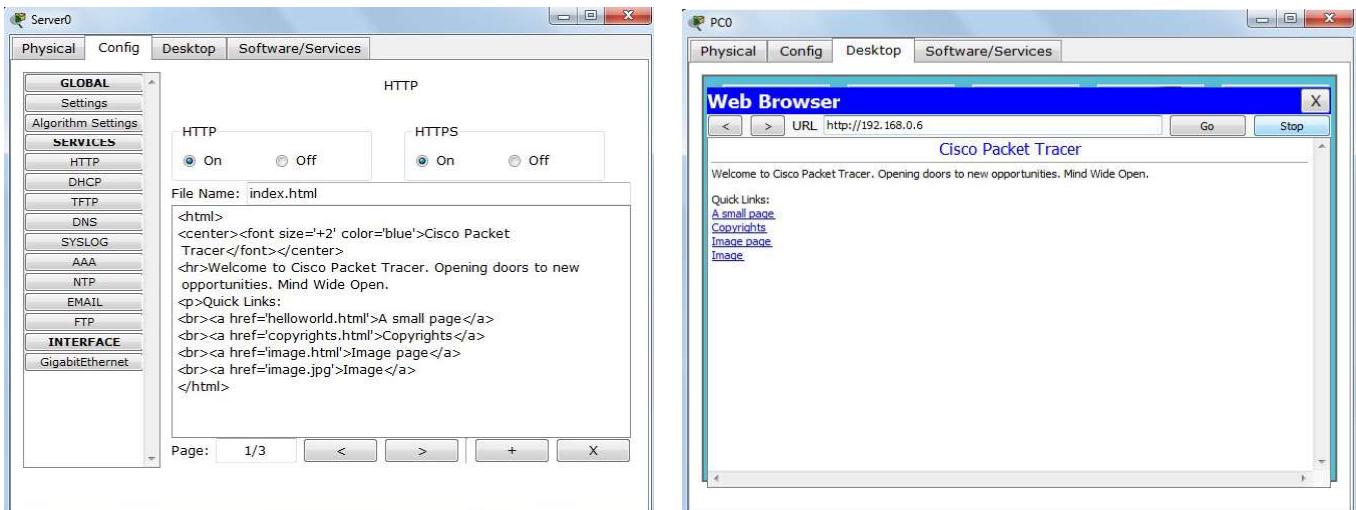


Рисунок 1.16 – Открытие Web-страницы HTTP-сервера в браузере ПК

4 ПРОГРАММА ЛАБОРАТОРНОЙ РАБОТЫ

1. По IP-адресам определить (см. вариант в таблице А.1 Приложения А):

- к сети какого класса они принадлежат;
- маску подсети;
- IP-адрес в формате IPv6 (сайт ip-lookup.net раздел Conversions IPv4 / IPv6);
- географическую локализацию хоста (сайт <http://2ip.ru/whois/>).

2. Просмотр сетевых настроек компьютера:

- определите IP-адрес и маску подсети для своего компьютера (с помощью утилиты ipconfig и сайта 2ip.ru). Узнайте свой IP-адрес в формате IPv6;
- определите класс подсети, в которой находится Ваш компьютер без использования маски подсети и по маске подсети;
- определите адрес подсети, в которой находится Ваш компьютер, с использованием функции «Логическое И» над IP-адресом и маской подсети. Следует иметь в виду, что операция «Логическое И» должна производиться с двоичным представлением operandов.

3. Зная маску и IP-адрес компьютера (номер варианта из таблицы А.2 Приложения А), определить порядковый данного этого компьютера в сети, чему равен номер сети, диапазон возможных IP-адресов хостов этой сети и широковещательный адрес сети. Запишите маску в короткой форме.

4. Для некоторой подсети используется маска, заданная Вами индивидуальным вариантом (см. таблицу А.3 Приложения А). Переведите маску из короткой формы в длинную. Сколько различных адресов компьютеров теоретически допускает эта маска, если два адреса (адрес сети и широковещательный) не используют?

5. По определению маска сети является непрерывной последовательностью битов 1 от старшего разряда после которых идут только биты 0. Поэтому необходимо перевести в двоичное представление указанные маски и проверить этот факт (см. таблицу А.4 Приложения А).

6. Чтобы узнать принадлежат ли адреса к одной подсети, необходимо получить адрес сети для каждого из адресов и сравнить адреса сетей (см. таблицу А.5 Приложения А).

7. Определить максимальную длину маски сети, чтобы указанные IP-адреса находились в одной сети (см. таблицу А.6 Приложения А). Чтобы определить максимальную длину маски сети необходимо перевести в двоичное представление оба адреса и посчитать число совпадающих бит, начиная со старшего бита до первого различия.

8. Построить в программе Cisco Packet Tracer модель локальной компьютерной сети на одном коммутаторе и одной беспроводной точке доступа с очевидными устройствами пользователей, количество которых перечислены в Приложении А, где вариант – номер студента по списку в журнале группы. Компьютеры должны быть оснащены интерфейсами FastEthernet, ноутбуки – беспроводными интерфейсами, а сервера – интерфейсами GigabitEthernet. Сетевой интерфейс сервера необходимо заменить на модуль *PC-HOST-NM-1CGE*, модуль с проводным интерфейсом на ноутбуке – на модуль с беспроводным интерфейсом *Linksys-WPC300N*.

9. Установить на коммутаторе пароль на вход в консоль и в привилегированный режим (для нечетных вариантов пароль хранится в открытом виде, для четных вариантов – в зашифрованном).

10. Задать сетевые имена для компьютеров с PC1 по PCM (M – количество ПК из приложения А), для серверов – с Server1 по Server2, для сетевых принтеров с Printer1 по Printer2, для ноутбуков с Laptop1 по Laptop L (L – количество ноутбуков из приложения А).

11. Задать IP-адреса пользовательским устройством, выбрав их из диапазона адресов IP-сети 192.168.v.0-192.168.v.255 (v – номер варианта студента по списку в журнале), имеющей маску подсети 255.255.255.0. Вначале диапазона IP-адресов разместите сервера, затем принтеры, ПК и ноутбуки. Приведите в отчет таблицу с сетевыми именами и IP-адресами, заданными устройствам, а также названиями сетевых интерфейсов коммутатора, к которым эти устройства подключены.

*Реализовать возможность динамического назначения IP-адресов для ПК и ноутбуков.

12. Выполнить проверку связи между одним из ноутбуков и любым ПК, любым сервером, любым принтером. Приведите в отчет скриншоты с результатами проверки.

13. Изменить IP-адреса первой половины Ваших ПК на адреса из диапазона адресов IP-сети 192.168.(v+1).0-192.168.(v+1).255, имеющей маску подсети 255.255.255.0. Проверьте связь на сетевом уровне между PC1 и PCM (M – максимальный ПК). Проверить связь между PC1 и PC2. Приведите результаты исследования в отчет.

14. Проверить связь с сервером, открыв на нем Web-страницу с помощью Web-браузера, которым оснащен ПК. Но прежде на сервере в HTML-странице HTTP-сервера введите следующую информацию: Ваше Ф.И.О., номер группы и вариант.

15. Реализовать возможность удаленного подключения к коммутатору по протоколу telnet. При доступе к коммутатору через telnet должен запрашиваться логин (Ваше имя) и пароль (Ваша фамилия).

5 СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Цель и программа лабораторной работы.
3. Исходные данные в соответствии с индивидуальным вариантом.
4. Скриншот с топологией локальной сети.
5. Команды и скриншоты этапов настройки локальной сети.
6. Скриншоты результатов тестирования сети.
7. Выводы.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Опишите отличия работы сетевого коммутатора и сетевого маршрутизатора.
2. Какие типы линий связи используются при организации локальной вычислительной сети? Дайте их характеристику.
3. Какие типы устройств входят в состав локальной вычислительной сети?
4. Перечислите действия, необходимые для организации локальной вычислительной сети.
5. Поясните в каких случаях и почему применяются прямой и перекрестный кабели UTP.
6. Что называется шлюзом сети?
7. Какие дополнительные возможности при связи компьютеров дает организация в сети DHCP-сервера.
8. Чем сетевой принтер отличается от обычного принтера, подключенного к компьютеру, входящему в локальную сеть?
9. Какие существуют режимы работы в консоли Cisco Packet Tracer? Охарактеризуйте их.
10. Какие способы подключения к устройствам фирмы Cisco?
11. Что такое баннер? Для чего он нужен?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бони Дж. Руководство по Cisco IOS / Дж.Бони. – М.: Изд-во «Русская редакция», 2008. – 784 с.
2. Таненбаум Э. Компьютерные сети / Э.Таненбаум. 5-е изд. – СПб.: Питер, 2012. – 960 с.
3. Хабракен Д. Как работать с маршрутизаторами Cisco/ Д. Хабракен; Пер. с англ. – М.: ДМК Пресс, 2005. – 320 с.
4. Хьюкаби Д. Руководство Cisco по конфигурированию коммутаторов Catalyst / Дэвид Хьюкаби, Стив Мак-Квери. – М.: Изд-во «Вильямс», 2004. – 560 с.
5. Чернега В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. – Севастополь: Изд-во СевНТУ, 2006. – 500 с.

ПРИЛОЖЕНИЕ А**Варианты индивидуальных заданий для выполнения заданий 1-7****Таблица А.1 – Варианты к заданию №1**

Вариант	Узлы	Вариант	Узлы	Вариант	Узлы
1	www.informika.ru www.rfbr.ru www.ras.ru	9	web.ru www.kamaz.ru www.rulex.ru	17	www.uiggm.nsc.ru hist.dcn-asu.ru www.cemi.rssi.ru
2	www.gpntb.ru www.rusmedserv.com www.nsc.ru	10	www.jinr.ru uic.nnov.ru www.ruthenia.ru	18	www.cam.ac.uk www.u-tokyo.ac.jp www.ucla.edu
3	www.chemnet.ru www.rsl.ru www.philosophy.ru	11	www.tractor.ru www.rsci.ru www.astronet.ru	19	www.gpi.ru iki.cosmos.ru www.spssl.nsc.ru
4	www.rbc.ru www.membrana.ru www.osi.ru	12	www.microsoft.com www.hp.com www.yandex.ru	20	www.inp.nsk.su www.scientific.ru www.med2000.ru
5	www.viniti.ru www.sostav.ru www.ioffe.ru	13	uic.nnov.ru www.ruthenia.ru www.rsl.ru	21	www.gramota.ru www.csa.ru www.bionet.nsc.ru
6	www.fegi.ru www.elibrary.ru www.extech.ru	14	www.sscc.ru www.nlr.ru www.fom.ru	22	www.keldysh.ru www.fom.ru www.inauka.ru
7	www.ripn.net www.shpl.ru sai.msu.su	15	www.viniti.ru www.sostav.ru www.gramota.ru	23	www.viniti.ru www.sostav.ru www.ioffe.ru
8	www.sesml.rssi.ru www.sscc.ru www.nlr.ru	16	psychology.net.ru www.irex.ru www.medlinks.ru	24	www.cisco.com www.hp.com www.yandex.ru

Таблица А.2 – Варианты к заданию №3

Вариант	Исходные данные		Вариант	Исходные данные	
	IP-адрес	Маска		IP-адрес	Маска
1.	130.18.134.220	255.255.255.128	2.	112.154.133.208	255.255.248.0
3.	206.158.124.67	255.255.224.0	4.	56.99.61.195	255.224.0.0
5.	42.160.157.215	255.240.0.0	6.	156.86.29.157	255.255.254.0
7.	194.3.50.241	255.255.255.192	8.	179.65.145.142	255.255.255.240
9.	232.126.150.18	255.255.240.0	10.	137.225.232.195	255.255.192.0
11.	35.42.64.114	255.192.0.0	12.	5.50.42.176	255.255.255.192
13.	226.185.90.162	255.255.252.0	14.	37.73.200.123	255.252.0.0
15.	110.157.233.184	255.255.128.0	16.	246.53.171.203	255.255.255.252
17.	153.124.23.139	255.255.255.224	18.	218.161.0.172	255.254.0.0
19.	17.119.20.175	255.255.255.240	20.	20.55.186.108	255.128.0.0
21.	167.212.40.42	255.248.0.0	22.	113.130.115.57	255.240.0.0
23.	75.59.233.215	254.0.0.0	24.	5.61.215.175	255.255.255.248

Таблица А.3 – Варианты к заданию №4

Вариант	Маска								
1.	/16	2.	/30	3.	/25	4.	/27	5.	/29
6.	/20	7.	/13	8.	/11	9.	/17	10.	/4
11.	/26	12.	/9	13.	/15	14.	/22	15.	/8
16.	/28	17.	/21	18.	/12	19.	/10	20.	/18
21.	/23	22.	/14	23.	/19	24.	/6		

Таблица А.4 – Варианты к заданию №5

Вариант	Маска			
	а	б	в	г
1.	255.254.0.0	255.255.255.214	255.255.255.248	255.255.248.0
2.	255.255.255.0	255.255.255.240	255.253.0.0	255.255.252.0
3.	255.255.252.0	255.255.255.192	255.7.0.0	248.0.0.0
4.	255.254.0.0	255.255.248.0	240.0.3.0	255.255.255.248
5.	248.0.0.0	255.249.0.0	255.255.255.240	224.0.0.0
6.	255.255.0.0	255.253.0.0	255.255.0.0	255.255.0.0
7.	255.248.0.0	255.255.240.0	255.255.254.0	255.255.255.254
8.	255.224.0.0	252.2.0.0	255.240.0.0	255.255.255.240
9.	255.255.255.248	255.255.255.252	255.255.248.0	192.0.0.0
10.	255.248.9.0	255.255.255.0	255.248.0.0	254.0.0.0
11.	255.255.225.255	255.255.193.0	255.255.0.0	255.255.255.128
12.	255.255.255.252	255.255.255.128	255.255.255.248	255.192.0.0
13.	255.224.0.0	250.0.0.0	255.255.254.0	192.0.0.0
14.	255.240.0.0	255.255.192.0	255.255.255.252	255.240.0.0
15.	255.255.255.128	255.240.0.0	224.0.0.0	255.224.224.0
16.	224.0.0.255	255.192.0.0	255.255.255.240	255.252.0.0
17.	255.129.0.0	255.255.248.0	255.255.192.0	254.0.0.0
18.	248.0.0.0	255.128.8.0	192.0.0.0	255.128.0.0
19.	255.255.255.128	255.255.250.254	255.255.255.192	248.0.0.0
20.	255.192.254.0	255.255.255.192	255.128.0.0	255.255.252.0
21.	255.0.0.0	255.224.10.0	252.0.0.0	255.255.224.0
22.	255.252.11.0	248.0.0.0	255.255.248.0	255.255.255.240
23.	255.155.255.255	240.0.0.0	254.0.0.0	255.252.0.0
24.	255.255.248.0	255.255.254.0	255.255.224.0	255.125.128.0

Таблица А.5 – Варианты к заданию №6

Вариант	IP-адреса		Вариант	IP-адреса	
1.	134.50.17.190/30 134.52.17.191/30	169.128.186.152/9 169.144.183.64/9	2.	108.11.214.167/19 108.11.223.5/19	246.235.45.207/29 246.235.45.215/29
3.	223.62.19.244/14 223.67.176.98/14	67.50.242.243/18 67.50.200.172/18	4.	74.28.237.200/25 74.28.237.203/25	181.84.249.67/9 181.65.130.204/9
5.	127.73.18.240/9 137.114.177.17/9	195.94.59.188/30 195.94.59.191/30	6.	199.123.3.50/23 199.123.3.101/23	100.101.216.145/5 100.182.234.25/5
7.	185.63.56.182/16 85.63.239.16/16	199.57.36.63/15 199.57.5.169/15	8.	24.52.254.96/21 24.52.252.93/21	206.240.138.123/26 206.242.138.65/26
9.	136.61.83.119/5 111.181.218.52/5	125.60.255.103/9 125.34.169.199/9	10.	125.160.27.126/29 125.160.27.104/29	90.11.41.223/20 90.11.36.71/20
11.	133.206.62.249/11 133.105.92.88/11	192.243.42.162/25 192.243.42.246/25	12.	245.147.217.10/20 245.137.208.239/20	8.215.223.7/22 8.215.221.121/22
13.	94.176.91.111/20 94.176.92.80/20	4.244.159.102/12 4.246.125.165/12	14.	203.229.237.163/24 203.229.236.44/24	50.140.6.93/12 50.137.106.16/12
15.	47.88.172.145/21 47.88.178.192/21	203.40.171.158/18 203.40.141.180/18	16.	138.38.89.122/27 138.38.89.102/27	33.57.125.225/10 33.105.28.206/10
17.	244.23.38.153/29 244.23.78.154/29	28.3.34.25/4 19.109.158.253/4	18.	1.155.84.168/25 1.155.87.159/25	218.21.244.169/21 218.21.247.183/21
19.	123.65.168.74/27 123.65.164.72/27	135.143.91.179/20 135.143.87.229/20	20.	107.105.106.169/12 107.121.225.62/12	150.135.197.141/6 150.175.141.163/6
21.	116.75.124.87/20 116.75.124.85/20	110.71.140.119/9 110.67.85.239/9	22.	219.115.4.199/14 219.113.224.101/14	194.104.201.41/14 194.112.152.83/14
23.	253.130.198.145/22 253.130.198.145/22	37.125.13.168/21 37.125.15.13/21	24.	134.50.17.190/30 134.52.17.191/30	169.128.186.152/9 169.144.183.64/9

Таблица А.6 – Варианты к заданию №7

Вариант	Диапазоны IP-адресов	
1.	117.220.88.73 - 118.222.74.206	32.102.0.46 - 32.102.0.47
2.	102.244.10.49 - 102.244.10.26	235.41.199.239 - 235.41.41.139
3.	251.252.230.152 - 251.250.29.97	54.134.17.147 - 54.10.33.193
4.	162.235.231.229 - 160.93.14.253	18.10.124.128 - 18.10.124.169
5.	99.149.26.16 - 99.149.26.16	199.225.66.216 - 199.225.66.247
6.	250.54.84.49 - 214.7.75.249	149.182.180.56 - 151.66.167.26
7.	231.81.216.237 - 231.81.212.30	177.77.34.213 - 191.35.196.43
8.	115.115.32.253 - 114.14.56.227	62.225.77.124 - 62.225.76.103
9.	184.155.179.54 - 184.155.66.71	251.106.185.206 - 251.126.234.156
10.	246.168.67.154 - 246.169.9.220	48.107.202.223 - 48.107.203.56
11.	23.115.247.150 - 23.48.37.248	95.129.111.1 - 95.129.111.3
12.	207.234.120.181 - 207.234.120.181	38.23.81.102 - 38.127.45.239
13.	150.27.130.246 - 150.18.140.87	166.220.34.180 - 166.220.34.183
14.	51.79.155.111 - 51.75.182.175	112.56.206.224 - 112.56.202.104
15.	236.74.83.193 - 236.75.195.217	12.95.127.35 - 12.131.135.175
16.	123.157.136.13 - 123.165.203.131	196.200.12.115 - 196.200.12.116
17.	91.1.129.158 - 91.1.172.242	220.225.247.23 - 220.225.71.91
18.	5.35.95.106 - 9.58.248.150	226.4.22.186 - 226.163.205.38
19.	159.218.202.36 - 159.218.156.20	141.85.107.17 - 141.85.107.97
20.	247.242.52.247 - 247.66.88.19	2.57.42.80 - 2.56.92.124
21.	120.149.163.181 - 120.186.35.7	41.0.254.221 - 47.86.238.81
22.	179.76.216.76 - 179.76.216.76	10.42.239.218 - 19.83.23.66
23.	182.133.171.215 - 182.133.221.50	122.186.87.171 - 122.186.87.170
24.	179.204.240.150 - 183.204.240.222	131.185.154.217 - 140.185.154.208

ПРИЛОЖЕНИЕ Б**Варианты индивидуальных заданий для выполнения заданий 8-15**

Вариант	ПК	Сервера	Принтеры	Ноутбуки
1	5	1	2	2
2	7	2	1	3
3	9	1	2	4
4	11	2	1	2
5	13	1	2	3
6	15	2	1	4
7	17	1	2	2
8	19	2	1	3
9	21	1	2	4
10	22	2	1	2
11	20	1	2	3
12	18	2	1	4
13	16	1	2	2
14	14	2	1	3
15	12	1	2	4
16	10	2	1	2
17	8	1	2	3
18	6	2	1	4
19	23	1	2	2
20	16	2	1	3
21	4	1	1	4
22	11	2	2	1
23	13	2	2	1
24	17	2	2	1
25	8	1	1	2
26	10	2	2	3
27	15	2	1	3
28	19	2	1	3