

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

**ИССЛЕДОВАНИЕ ТОПОЛОГИИ И
СПОСОБОВ ПОСТРОЕНИЯ
ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ**

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторной работы №5
по дисциплине
«Инфокоммуникационные системы и сети»
для студентов дневного и заочного отделения по направлению
09.03.02 «Информационные системы и технологии»,
09.03.03 «Прикладная информатика»

**Севастополь
2020**

УДК 681.326

Методические указания к выполнению лабораторной работы **«Исследование топологии и способов построения локальных компьютерных сетей»** по дисциплине «Инфокоммуникационные системы и сети» / Сост. доц. Чернега В.С., ст.преп. Волкова А.В. – Севастополь: Изд-во СевГУ, 2020. – 33 с.

Цель указаний: помочь студентам в изучении топологии локальных компьютерных сетей, способов построения сетей с шинной, радиальной и кольцевой топологией, способов доступа к сети и конфигурации инфокоммуникационного оборудования.

Методические указания предназначены для выполнения лабораторных работ по дисциплине «Инфокоммуникационные системы и сети» для студентов дневной и заочной форм обучения.

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры «Информационные системы»

Рецензент доцент кафедры «Информационные системы»

к.т.н., доцент

Кротов К.В.

СОДЕРЖАНИЕ

1	Цель работы	4
2	Основные теоретические положения	4
2.1	Топология локальных компьютерных сетей.....	4
2.2	Способы доступа к ресурсам сети	6
2.3	Общая структура и оборудование локальной компьютерной сети	8
2.4	Способы адресации узлов в сети.....	11
3	Описание лабораторной установки	16
3.1	Рабочее окно симулятора Cisco Packet Tracer	17
3.2	Оборудование и линии связи в Cisco Packet Tracer	19
3.3	Примеры подключения к устройствам фирмы Cisco.....	21
3.4	Построение и настройка локальной компьютерной сети.....	25
4	Программа и методика выполнения работы.....	29
5	Содержание отчета.....	31
6	Контрольные вопросы	31
	Библиографический список.....	32
	ПРИЛОЖЕНИЕ А Варианты индивидуальных заданий	33

1 ЦЕЛЬ РАБОТЫ

Целью работы является углубление теоретических знаний по архитектуре локальных компьютерных сетей (ЛКС), исследование способов построения локальных сетей и конфигурации коммуникационного оборудования. А также приобретение практических навыков конфигурации и исследования функционирования ЛКС.

2 ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

2.1 Топология локальных компьютерных сетей

Локальные компьютерные сети (ЛКС, Local Area Network – LAN) представляет собой такую разновидность сетей, в которой все ее компоненты, включая ЭВМ различных классов, расположены на ограниченной территории одного помещения, предприятия или учреждения и соединены через единую физическую среду. Расстояния между компьютерами локальной сети составляют от сотен метров до десятков (10-20) км. В локальных сетях сетевые компьютеры называют рабочими станциями. Ограниченность территории, использование собственных линий связи, создает предпосылки для использования специфических способов передачи данных, отличных от традиционных, применяемых в глобальных сетях. Благодаря этому в ЛКС удастся реализовать значительно более высокую скорость передачи (сотни Мбит/с) и на несколько порядков более низкую вероятность ошибок при существенно меньших затратах. Расположение локальной сети на ограниченной территории влияет также на способы административного сетевого управления, а технические характеристики ЛКС приводят к необходимости введения новых протоколов.

В качестве физической среды ЛКС наибольшее распространение получили электрические кабели типа «витая пара», коаксиальные и волоконно-оптические кабели. В последнее время все большую популярность получают беспроводные линии связи. В дальнейшем для упрощения, при описании ЛКС понятия «среда», «линия» и «канал» используются как синонимы.

Основные отличия архитектуры ЛКС от архитектуры глобальных сетей связаны с нижними тремя уровнями. Использование единой физической среды позволяет существенно упростить функции уровня маршрутизации. Нижние два уровня ЛКС имеют свою специфику, связанную с топологией сети и методами доступа к физической среде.

Различают линейную (а), звездообразную (б), кольцевую (в), шинную (г) и древовидную (д) топологию ЛКС (рисунок 2.1).

Все структуры сети, кроме шинной, представляют собой двухточечные звенья. В линейной структуре сети сообщения должны пройти через несколько узлов, прежде чем они достигнут цели. Поэтому в случае повреждения одного из звеньев сообщение не может быть доставлено адресату, что является существенным недостатком такой сети.

Радиальная (звездная, лучевая) топология характеризуется наличием центрального узла коммутации (УК), к которому подключаются все остальные рабочие станции (РС). Через этот узел циркулирует весь сетевой трафик, поэтому нагрузка на узел

очень высокая. Сетевое оборудование центрального узла оказывается намного сложнее, чем оборудование абонентов сети. К достоинствам «звезды» относится достаточно высокая надежность сети в целом. Так обрыв одного сетевого кабеля или короткое замыкание в нем нарушает работу только одного компьютера, а все остальные могут продолжать работу. Положительным свойством является также наличие на каждой линии связи только одного передатчика и приемника, что заметно упрощает сетевое оборудование по сравнению с «шиной». Недосток звездообразной структуры состоит в низкой скорости обработки информации и большой суммарной протяженности линий связи. При этом, при выходе центрального узла из строя отказывает вся сеть.

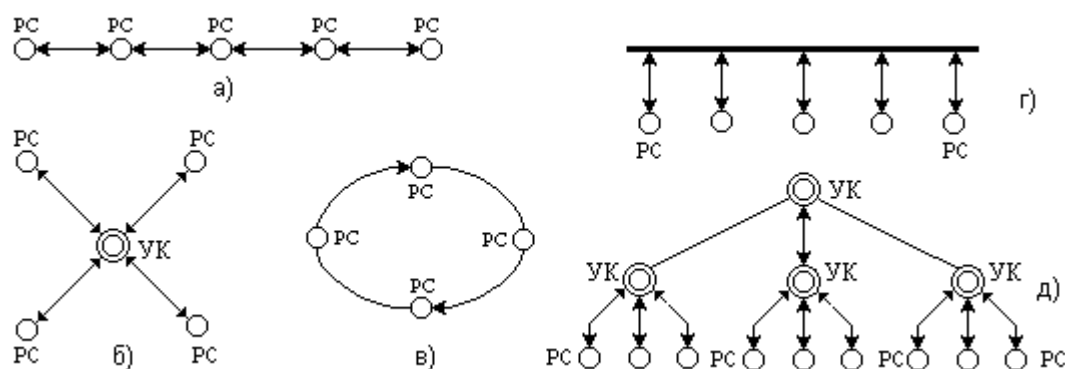


Рисунок 2.1 – Виды топологий локальных компьютерных сетей

Преимуществом «кольца» является возможность использования однонаправленной линии связи, что заметно упрощает и удешевляет сеть. На каждом участке к линии связи подключены только один передатчик и один приемник. По этой причине нет необходимости использовать согласующие сопротивления (терминаторы). Недостатком кольцевой топологии является загрузка узлов всей той информацией, которая передается по сети.

Шинная топология является одной из простейших по способу подключения рабочих станций. В такой структуре отсутствует центральный узел, через который передается вся информация. Это увеличивает надежность сети. Однако она предполагает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов. При таком соединении компьютеры могут передавать данные только по очереди, так как линия связи одна на всех (моноканал). На концах линии связи должны устанавливаться согласующие сопротивления (терминаторы) для исключения появления отраженных волн, вызывающих искажение сигналов. Обрыв или замыкание в линии выводит из строя всю сеть. К существенным недостаткам шинной структуры также относится возможность возникновения *сетевых коллизий*. Коллизия возникает всякий раз, когда одновременно ведут передачу две или несколько рабочих станций сети, что приводит к разрушению информации. Разработаны специальные протоколы связи, позволяющие исключить потери информации при возникновении коллизий, либо исключаяющие их возникновение.

Древовидная топология представляет собой иерархическую звезду. Она имеет достоинства, присущие звездной топологии. Используется для увеличения количества рабочих станций сети при ограниченном числе портов узловой станции.

2.2 Способы доступа к ресурсам сети

Характерной чертой многих локальных сетей является коллективное использование ресурсов среды передачи данных – линии связи, которая является *моноканалом*. Через такую среду в заданный промежуток времени может передавать информацию только одна рабочая станция. Поэтому возникает проблема разделения ресурсов среды передачи данных, которая решается различными способами. Широко используется способ множественного доступа с контролем передачи и обнаружения конфликтов (CSMA/CD), а также способ управления доступом с передачей маркера. Под доступом к сети подразумевается возможность передавать данные в сеть.

Способ доступа CSMA/CD (*Control Send Multi Access/Collision Detecting*). При использовании этого способа рабочие станции могут передавать сообщения только если канал связи свободен. В случае одновременной передачи информации несколькими станциями возникает конфликтная ситуация (*коллизия*), в результате чего происходит разрушение передаваемых данных. Поэтому станции должны прекратить передачу, выждать некоторое время и продолжить ее по одной только при наличии свободного канала. Для определения занятости канала используется контроль уровня несущей в среде. Чтобы избежать повторения коллизий, время ожидания включения станций выбирается различным. Если одна из станций начала передачу, то канал оказывается занятым и все другие станции должны ждать его освобождения.

Большую часть времени устройство приема-передачи рабочей станции (сетевая карта) находится в режиме прослушивания канала связи. В этом состоянии анализируются все кадры, передаваемые в канале. Если заголовок кадра содержит адрес назначения, совпадающий с адресом узла, то сетевая карта переходит в состояние приема, во время которого осуществляется прием кадра. После завершения приема кадра сетевая карта переключается в режим прослушивания. Возможно, что коллизия произойдет во время приема кадра. В этом случае прием кадра прерывается и устройство переключается в состояние прослушивания.

Передача кадра в линию связи может быть произведена только по запросу сетевого программного обеспечения рабочей станции. Если сетевая карта во время этого запроса не находится в состоянии приема, то она переходит в состояние ожидания, при котором она ждет освобождения канала и начинает передачу кадра. В случае успешного завершения передачи (без коллизий), состояние приемо-передатчика вновь изменяется на состояние прослушивания. Если же во время передачи кадра появляется конфликтная ситуация, то передача прерывается и затем, после прослушивания, возобновляется снова через случайный интервал времени, который генерируется датчиком случайных чисел.

Наличие коллизий характерно не только для шинной топологии, но и для беспроводных компьютерных сетей, а также для сетей с радиальной топологией при использовании в качестве узла коммутации концентратора (хаба) в связи с тем, что концентратор, приняв кадр с адресом получателя, ретранслирует его на все свои порты, за исключением того, откуда поступил кадр.

ЛКС с шиной и маркерным доступом. Этот способ характеризуется тем, что в нем право использования среды с топологией шины передается от станции (узла) к станции *организационным* способом, а не *состязательным* путем. Право передачи

данных в канал реализуется посредством посылки специального кадра разрешения – **маркера**. Станция, получившая маркер (*Token*), может начинать передачу данных, и после ее завершения пересылает маркер следующей, например, в порядке увеличения адресов, станции. Маркер передается по логическому кольцу и, достигнув станцию с максимальным адресом, вновь поступает на станцию с наименьшим адресом. Такая процедура управления носит название **передача по логическому кольцу**.

Большую часть времени аппаратура канального уровня находится в состоянии прослушивания. Если заголовок приходящего кадра в адресной части содержит адрес узла, то канальный уровень переходит в состояние приема кадра. При условии, что принятый кадр является кадром пакета данных, сетевой уровень информируется о приеме, а канальный уровень возвращается в состояние прослушивания.

Однако если принятый кадр является маркером, то это означает, что узел получает право передачи в среду. В случае наличия на узле информации, подлежащей передаче, состояние станции переходит в активный режим, при котором производится передача кадра. По окончании передачи в канал выдается новый маркер. Передача маркера происходит также в случае отсутствия на станции пакета данных, подлежащих передаче. После передачи маркера узел снова переключается в режим прослушивания.

Помимо передачи маркера схема с логической шиной должна решать *проблему потери маркера и реконфигурации* кольца. Потеря маркера может произойти из-за повреждения одной из станций логического кольца. В некоторый момент времени маркер приходит в поврежденный узел, но узел не пропускает его дальше, и другие станции по этой причине не получают маркер. *Реконфигурация* кольца выполняется, когда в логическое кольцо добавляется или из него удаляется один из узлов. При потере маркера или сбое в сети все рабочие станции переходят в состояние ожидания (бездействия). Время ожидания каждой из рабочих станций различное и выбирается пропорционально ее номеру (адресу). То есть, после отключения компьютеров первой возбуждится станция с наименьшим адресом. Она формирует маркер и посылает его следующему компьютеру в сети, начиная с узла, адрес которого на 1 больше его собственного.

ЛКС с кольцевой структурой и маркерным доступом. Основное различие этого способа от двух предыдущих заключается в физической кольцевой топологии. В кольцевой среде сигналы, переданные одним из компьютеров сети, распространяются через однонаправленные двухточечные линии между станциями, которые соединяются последовательно, образуя физическое кольцо (рисунок 2.2).

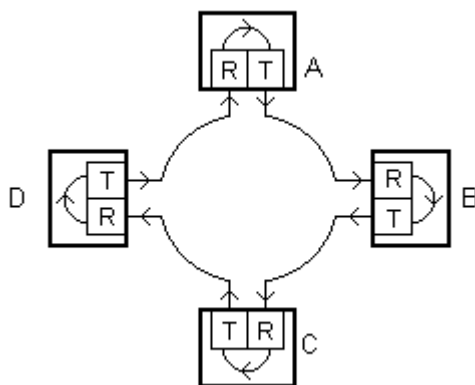


Рисунок 2.2 – Топология физического кольца

Во время передачи по кольцевой среде сигналы проходят через станции от приемного (R) к передающему (T) порту. При этом станции могут анализировать и модифицировать приходящие сигналы. Преимуществом такого решения является возможность увеличения длины соединительных линий за счет усиления и ретрансляции сигналов на узлах. Однако повреждение одной из станций или кабельного сегмента физического кольца приводит к выводу из строя всей сети. При ретрансляции сигналов, выполняемой блоком многократного стробирования, узел вносит задержку, которая равна длительности единичного элемента сигнала.

Как и в случае шинной структуры с передачей маркера, в схеме доступа к кольцевой среде в качестве маркера используется специальный укороченный кадр, у которого имеется **бит-индикатор T (Token)** признака маркера. Первые два байта маркерного и информационных кадров полностью совпадают по формату. Если бит T установлен в единицу, то кадр является маркером, в противном случае дальнейшая последовательность воспринимается как информационный кадр. Если ни у одного из узлов сети нет пакета данных для передачи, маркер непрерывно циркулирует по кольцу. Такой кадр носит название **свободного маркера**. Узел, в котором имеется пакет данных для передачи, должен ждать, пока он не получит свободный маркер. В момент прихода свободного маркера станция переходит в режим передачи, изменяет состояние маркера на занятое ($T=0$) и передает маркер дальше по кольцу, добавляя к нему информационную и служебную часть кадра.

Кадр данных, вместе с занятым маркером, передается по всему кольцу. Модифицировать значение маркера снова на свободное может только тот узел, который изменил его на занятое. В каждом кадре данных содержится адрес узла назначения. Все узлы кольца, за исключением узла источника, обнаружив занятый маркер ($T=0$), ретранслируют кадр, а принимает его только узел назначения. Таким образом, на узле назначения принимаемый кадр фиксируется (копируется) и вместе с маркером передается далее по кольцу.

Когда занятый маркер, вместе с остальной частью кадра, возвращается в узел источника, состояние маркера меняется на свободное, а пакет удаляется из кольца (не передается дальше). Как только маркер становится свободным, любой узел может изменить его на занятый и начать передачу данных.

Звёздная топология с сетевым коммутатором. Особенностью такой топологии является то, что сетевой коммутатор (свитч), приняв кадр с адресом получателя, отправляет его только на порт, к которому подключена адресуемая рабочая станция. Благодаря этому доступ к сети могут получить и все остальные рабочие станции. За счет этого существенно повышается суммарная пропускная способность локальной сети.

2.3 Общая структура и оборудование локальной компьютерной сети

Локальная компьютерная сеть 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).

В локальной сети можно выделить:

- *оконечное оборудование пользователей (хосты)*, поставляющее данные в сеть и принимающее данные для обработки (рабочие станции, серверы, ноутбуки, сетевые 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 адаптеры (современные материнские платы оснащаются встроенными сетевыми адаптерами);
 - подобрать и разместить активное сетевое оборудование;
 - выполнить соединение сетевых интерфейсных адаптеров в оконечном оборудовании пользователей и разъемов 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.

Сетевые интерфейсные адаптеры предназначены для выполнения функций физического и канального уровня семиуровневой модели взаимодействия открытых систем (Open System Interconnection – OSI) в устройствах локальной сети. Адаптеры имеют передающую и принимающую части, которые выполнены независимыми друг от друга с целью поддержки режима полного дуплекса (Full Duplex), при котором передача и прием данных происходят одновременно. Обычно настройки драйверов сетевого адаптера позволяют выбирать и менее производительный режим полудуплекса (Half Duplex), при котором передача и прием данных происходят по очереди.

В первых локальных компьютерных сетях с радиальной топологией в качестве активного сетевого оборудования (узла коммутации) использовался *концентратор (Hub)*. Схема простейшей ЛКС на основе хаба изображена на рисунке 2.3,а. Сетевые интерфейсы рабочих станций (FastEthernet0) с помощью медного прямого кабеля (в Packet Tracer он обозначен Copper Straight-Through) соединяются с аналогичными интерфейсами хаба. При этом номер подключаемого интерфейса хаба не имеет значения.

В дальнейшем, с развитием и удешевлением микропроцессорных устройств, для повышения пропускной способности сети и повышения ее безопасности, функции узла коммутации стал выполнять сетевой коммутатор (*Switch*). Схема локальной компьютерной сети внешне не изменилась (рисунок 2.3,б).

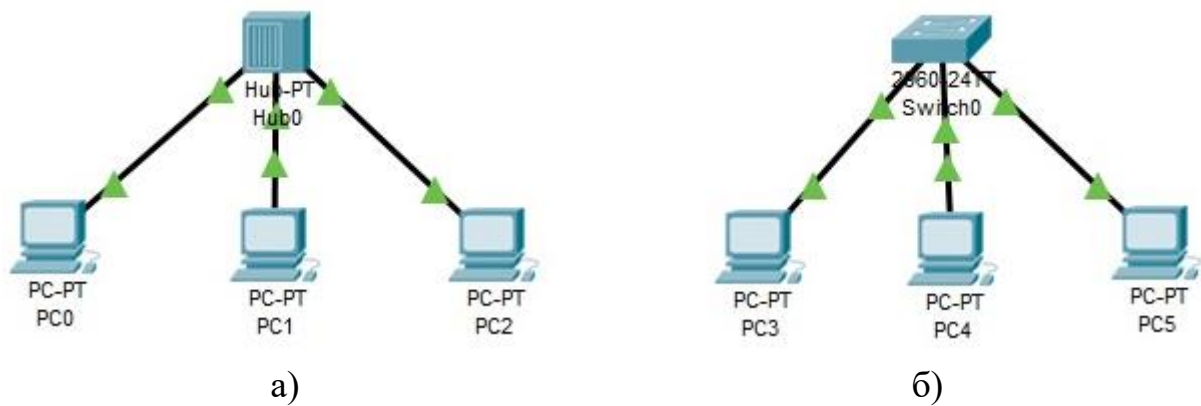


Рисунок 2.3 – Схемы простейших локальных компьютерных сетей на основе концентратора (а) и на основе коммутатора (б)

Хотя конструктивно концентратор по внешнему виду очень похож на коммутатор, однако принцип работы его существенно отличается. Концентратор, получив кадр от рабочей станции, не анализирует его заголовок, а пересылает его на все свои интерфейсы, за исключением того, откуда этот кадр поступил. Коммутатор же анализирует адресную информацию в заголовках кадров, поступающих в его порты и, на основании созданной им таблицы коммутации, избирательно передает кадры со входного порта только на выходной порт, к которому подсоединена рабочая станция — получатель кадров.

С практической точки зрения концентраторы имеют преимущество в скорости работы (в частности, 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 рабочей станции), приводит к снижению пропускной способности 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 (следует отметить, что подавляющее большинство мобильных компьютеров и устройств оснащено встроенными контроллерами беспроводного доступа).

При необходимости подключения беспроводного сегмента локальной сети к ее проводному сегменту на коммутаторе/концентраторе точка доступа подключается телекоммуникационным кабелем к одному из портов коммутатора/концентратора.

Сетевые принтеры представляют собой принтеры, оснащенные сетевыми адаптерами, что позволяет подключать их к сети непосредственно. Использование сетевого принтера является удобным, так как его работа не связана с необходимостью работы

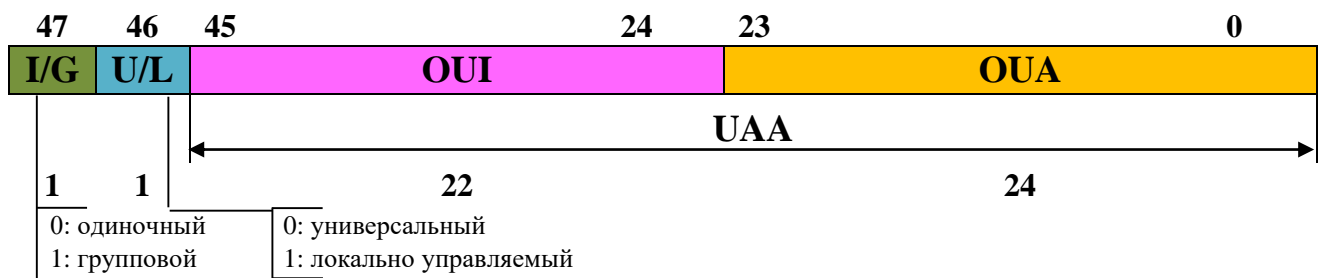
компьютера, к которому подключается обычный принтер. Кроме того, сетевые принтеры обычно имеют повышенные производительность и ресурс картриджа. При отсутствии сетевого принтера совместный доступ к обычному принтеру, подключенному к компьютеру, может быть организован средствами операционной системы.

2.4 Способы адресации узлов в сети

2.4.1 Аппаратный адрес (MAC-адрес)

Один из подходов к адресации узлов в сети был разработан международной организацией IEEE, занимающейся стандартизацией сетей. Идея этого подхода состоит в том, чтобы присваивать уникальный сетевой адрес каждому адаптеру сети еще на этапе его изготовления. Если количество возможных адресов будет достаточно большим, то можно быть уверенным, что в любой сети по всему миру никогда не будет абонентов с одинаковыми адресами. Поэтому был выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов.

MAC-адрес (Media Access Control – MAC) – это уникальный 6-байтовый идентификатор, присваиваемый каждой единице активного оборудования компьютерных сетей. Этот адрес считается жестко привязанным к конкретному интерфейсу, хотя и существует возможность его переопределить в дополнительных настройках драйвера сетевого адаптера. На рисунке 2.4 приведен формат 48-битового MAC-адреса.



I/G – Индивидуальный / групповой (FF FF FF FF FF FF – широковещательный)

U/L – Уникальный (в глобальном смысле) / локальный (назначен администратором)

OUI – Organizationally Unique Identifier – Код изготовителя сетевого оборудования

OUA – Organizationally Unique Address – MAC-адрес устройства, присвоенный изготовителем

UAA – Universally Administered Address – универсально управляемый адрес

Рисунок 2.4 – Формат MAC-адреса

Существуют три типа MAC-адресов: *индивидуальные* или *однопунктовые* (*unicast*), *групповые* (*multicast*) и *широковещательные* (*broadcast*).

Индивидуальный (однопунктовый) адрес определяет одну конкретную рабочую станцию сети, это наиболее часто встречаемый адрес в кадрах Ethernet.

Иногда необходимо разослать информацию всем компьютерам локальной сети. Например, при включении рабочей станции она высылает всем участникам сети свое сетевое имя и адресную информацию (после чего ее имя отображается, например, в окне *сеть*). MAC-адрес, указывающийся в этом случае в поле адреса получателя, является *широковещательным*. Широковещательный адрес представляет собой 48 единичных битов, которые в шестнадцатеричной системе выглядят как FF-FF-FF-FF-FF-FF_H. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

В случае, когда получателей кадра должно быть более одного, но менее, чем все компьютеры локальной сети, используют *групповые* MAC-адреса. Такие адреса используются, например, при потоковой передаче аудио и видео тем компьютерам, пользователи которых подписались на эти передачи. Групповой адрес связан только с интерфейсами, сконфигурированными как члены группы, номер которой указан в групповом адресе. Если сетевой интерфейс включен в группу, то наряду с уникальным MAC-адресом с ним ассоциируется еще один адрес – групповой.

Два старших разряда адреса управляющие, они определяют тип адреса, способ интерпретации остальных 46 разрядов.

Старший (47-й) бит I/G (*Individual/Group*) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получают все имеющие этот групповой адрес сетевые адаптеры. Адрес отправителя может быть только индивидуальным (однопунктовым). Причем групповой адрес определяется 46 младшими разрядами. Второй управляющий бит U/L (*Universal/Local*) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому оборудованию. Указывает, является ли этот адрес уникальным в глобальном смысле (бит равен 0) или в пределах локальной сети в случае, если он переопределен администратором (бит равен 1). Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого оборудования, а организацией, использующей данную сеть. Это случается довольно редко.

Так, значения старшего байта группового адреса могут равняться либо 01_н (для уникального в глобальном смысле адреса), либо 03_н (для уникального в пределах локальной сети адреса).

Старшие 3 байта MAC-адреса представляют собой так называемый *организационно уникальный идентификатор* (*Organizationally Unique Identifier – OUI*) – IEEE выделяет такие уникальные идентификаторы для производителей сетевого оборудования. IEEE присваивает один или несколько OUI каждому производителю сетевого оборудования. Это позволяет исключить совпадения адресов сетевого оборудования от разных производителей. Всего возможно свыше 4 миллионов разных OUI, т.е. теоретически может быть зарегистрировано 4 миллиона производителей.

Младшие 3 байта представляют собой *организационно уникальный адрес* (*Organizationally Unique Address – OUA*), который назначается производителем каждому выпущенному им контроллеру сетевого интерфейса. Всего возможно свыше 16 миллионов комбинаций, то есть каждый производителей может выпустить 16 миллионов сетевых адаптеров. Таким образом, уникальность MAC-адреса обеспечивается, с одной стороны, IEEE – не существует двух одинаковых значений OUI, выделенных разным производителям. С другой стороны производитель задает уникальные значения OUA производимым им контроллерам сетевых интерфейсов. В результате можно гарантировать уникальность значения любого MAC-адреса, записанного в конфигурационную информацию контроллера сетевого интерфейса. Вместе OUA и OUI называются UAA (*Universally Administered Address*) – универсально управляемый адрес или IEEE-адрес.

2.4.2 Сетевой адрес (IP-адрес)

Каждой точке подключения любого устройства к сети (интерфейсу), присваивается уникальный номер, который называют – *IP-адресом*.

Необходимо понимать, что IP-адрес, как и MAC-адрес, присваивается не устройству (компьютеру или маршрутизатору), а именно интерфейсу, поскольку многие устройства могут иметь несколько точек подключения к сети, а следовательно, и несколько различных IP-адресов.

Протокол IPv4 разработан в сентябре 1981 года. IP-адрес имеет длину 4 байта (или 32 бита). Т.е. число в диапазоне от 0 до 4294967295. Для удобства чтения (и по организационным причинам) IP-адреса записываются в «точечно-разделительной нотации» – 32-битные числа разбивают на октеты по 8 бит, каждый октет переводят в десятичную систему счисления и при записи разделяют точками. Например, IP-адрес 11000000101010000000000000000001 записывается как 192.168.0.1. Так как каждое из четырех чисел – это десятичное представление 8-битного байта, то каждое число может принимать значения от 0 до 255 (что дает 256 уникальных значений), т.е. значения в диапазоне от 0.0.0.0 до 255.255.255.255.

IP-адрес состоит из двух частей – идентификатор сети (префикс сети, Network ID) и **идентификатор** узла (номер устройства, Host ID). Такая схема приводит к двух-уровневой адресной иерархии (см. рисунок 2.5).

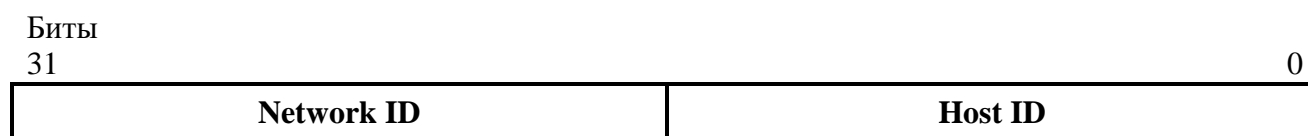


Рисунок 2.5 – Структура IP-адреса

Идентификатор сети идентифицирует все узлы, расположенные на одном физическом или **логическом** сегменте сети, ограниченном IP-маршрутизаторами. Все узлы, находящиеся в одном сегменте должны иметь одинаковый идентификатор сети.

Идентификатор узла идентифицирует конкретный сетевой узел (сетевой адаптер рабочей станции или сервера, порт маршрутизатора). Идентификатор узла должен быть уникален для каждого узла внутри IP-сети, имеющей один идентификатор сети. Таким образом, в целом IP-адрес будет уникален для каждого сетевого интерфейса всей сети TCP/IP.

Адреса IPv4 первоначально выделялись на основе классов, реализуя классовую IP адресацию. В исходной спецификации IPv4 (RFC 791), выпущенной в 1981, авторы установили классы, чтобы обеспечить три различных размера сетей для крупных, средних и небольших организаций. В результате адреса классов А, В и С были определены с помощью определенного формата для битов старшего разряда. Биты старшего разряда являются крайними левыми битами в 32-разрядном адресе (см. рисунок 2.6).

Существует возможность выяснить, кто является владельцем сети, в которую входит произвольный IP-адрес, а также координаты администратора этой сети, выполнив запрос к базе данных регионального или локального регистратора. Для европейских адресов это можно сделать на сайте RIPE NCC <http://www.db.ripe.net/whois>.

Класс	1 байт (октет)		2 байт (октет)	3 байт (октет)	4 байт (октет)	Наимень- ший номер сети	Наибольший номер сети	Маска подсети	Примечание		
A	0	№ сети	№ хоста			0.0.0.0 (0 - не используется)	127.0.0.0 (127-зарезерви- рован)	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 2.6 – Классы IP-адресов

2.4.3 Протокол ARP

В настоящее время все сетевые адаптеры, их драйверы, мосты, коммутаторы и маршрутизаторы могут работать со всеми используемыми на практике форматами кадров, а распознавание их типов происходит автоматически.

Любое устройство, подключенное к локальной сети (Ethernet, FDDI и т.д.), имеет уникальный физический (аппаратный, MAC-) сетевой адрес. Если у компьютера меняется сетевой адаптер, то меняется и его MAC-адрес. 4-байтовый IP-адрес задается администратором сети с учетом положения компьютера в сети Интернет. Если компьютер перемещается в другую часть сети Интернет, то его IP-адрес должен быть изменен.

Для определения физического (MAC) адреса A_{ϕ} сетевого компьютера по известному его IP-адресу A_{ca} протоколом определения адреса **ARP** (*Address Resolution Protocol*) предусмотрено формирование специального блока канального уровня – **кадра ARP**. В этот кадр наряду со служебной информацией помещается сетевой IP-адрес искомой станции. Для того чтобы этот кадр мог достичь всех абонентов адресуемой сети, в качестве MAC-адреса назначения ARP-кадра используется широковещательный адрес. Сформированный таким образом кадр называется **ARP-запрос** (*ARP-request*). Этот кадр передается в сеть и принимается всеми станциями, подключенными к ней. Станции анализируют содержимое принятого запроса и станция, обнаружившая в кадре принятого запроса свой сетевой адрес, формирует ответ на этот запрос (*ARP-reply*). В кадр *ARP-reply* станция помещает свой MAC-адрес и отправляет его в направлении источника запроса, используя при этом физический адрес станции отправителя.

Преобразование IP-адресов в аппаратные выполняется с помощью ARP-таблицы. Каждый сетевой компьютер имеет отдельную ARP-таблицу для каждого своего сетевого адаптера. ARP-таблица хранится в памяти компьютера и содержит строки для каждого сетевого узла. В столбцах таблицы содержатся IP- и MAC-адреса. Если требуется преобразовать IP-адрес в MAC-адрес, то ищется запись с соответствующим IP-адресом. ARP-таблица необходима потому, что IP-адреса и MAC-адреса выбираются независимо друг от друга, и нет никакого математического выражения для преобразования одного в другой.

Для того чтобы не запускать процедуру преобразования адресов всякий раз, когда потребуется организовать обмен с какой либо станцией, применяется аппарат кэширования результатов запросов – **ARP-cache** (буфер ARP). Эффективность функционирования ARP во многом зависит от ARP-кэша, который присутствует на каждом хосте. В кэше содержатся Internet адреса и соответствующие им аппаратные MAC-адреса. Стандартное время жизни каждой записи в кэше составляет 20 минут с момента создания записи.

Порядок преобразования адресов происходит следующим образом:

- 1) по сети передается широковещательный ARP-запрос;
- 2) исходящий IP-пакет ставится в очередь;
- 3) возвращается ARP-ответ, содержащий информацию о соответствии IP- и MAC-адресов, которая заносится в ARP-таблицу;
- 4) для преобразования IP-адреса в MAC-адрес у IP-пакета, поставленного в очередь, используется ARP-таблица;
- 5) MAC-кадр передается по сети Ethernet.

В современных сетевых ОС (Windows, Linux, BSD) таблицу преобразования адресов можно просмотреть в консоли с помощью команды **arp -a**. Чтобы очистить ARP кэш в Windows нужно в командной строке набрать **arp -d**.

Формат кадра протокола ARP показан на рисунке 2.7.

0	8	16	31
Тип оборудования		Тип протокола	
Длина АдрА	Длина АдрП	Код операции	
Аппаратный адрес отправителя (октеты 0...3)			
Адрес отправителя (октеты 4,5)		IP-адрес отправителя (октеты 0,1)	
IP-адрес отправителя (октеты 2,3)		Аппаратный адрес получателя (0,1)	
Аппаратный адрес получателя (октеты 2,5)			
IP-адрес получателя (октеты 0,3)			

Рисунок 2.7 – Формат кадра протокола ARP

Он содержит следующие поля.

Тип оборудования (*Hardware Type*). В этом поле располагается признак типа применяемого протокола канального уровня. Например, протоколу *Ethernet* значение данного поля соответствует 1, сети X.25 – 2, АТМ – 16.

Тип протокола (*Protocol Type*). В него помещается признак типа используемого протокола сетевого уровня. Например, для протокола IP в это поле помещается число 2048, для X.25 – 2053.

Длина АдрА и АдрП (HLEN и PLEN). Содержимое этих полей определяет размер адреса канального (аппаратного) и сетевого (протокольного) уровней соответственно. Наличие данных полей обеспечивает возможность использования протокола ARP для определения физического адреса в различных сетях второго и третьего уровней.

Код операции (*Operation*). В этом поле размещается признак типа информационного кадра: *ARP Request*; *ARP Response*; *RARP Request* или *RARP Response*.

Аппаратный адрес отправителя/получателя (*Sender/Target Hardware*

Address) служат для размещения физических адресов передающей станции и станции назначения соответственно.

IP-Адрес сети отправителя/получателя (*IP Sender/Target Network Address*). В них располагаются сетевые адреса передающей станции и станции назначения соответственно.

Для выполнения функции, обратной действиям ARP разработан **протокол RARP** (*Reverse ARP*). Он предназначен для нахождения логического сетевого адреса узла сети по известному его MAC-адресу.

3 ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

В качестве лабораторной установки используется персональный компьютер с установленной свободно распространяемой системой моделирования компьютерных сетей 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.

Packet Tracer позволяет моделировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, концентраторов, 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 или использования интерфейса командной строки CLI (Command Line Interface). 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.

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.

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.

3.1 Рабочее окно симулятора Cisco Packet Tracer

При запуске программы Cisco Packet Tracer на экране компьютера появляется главное окно симулятора (рисунок 3.1).

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

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*).

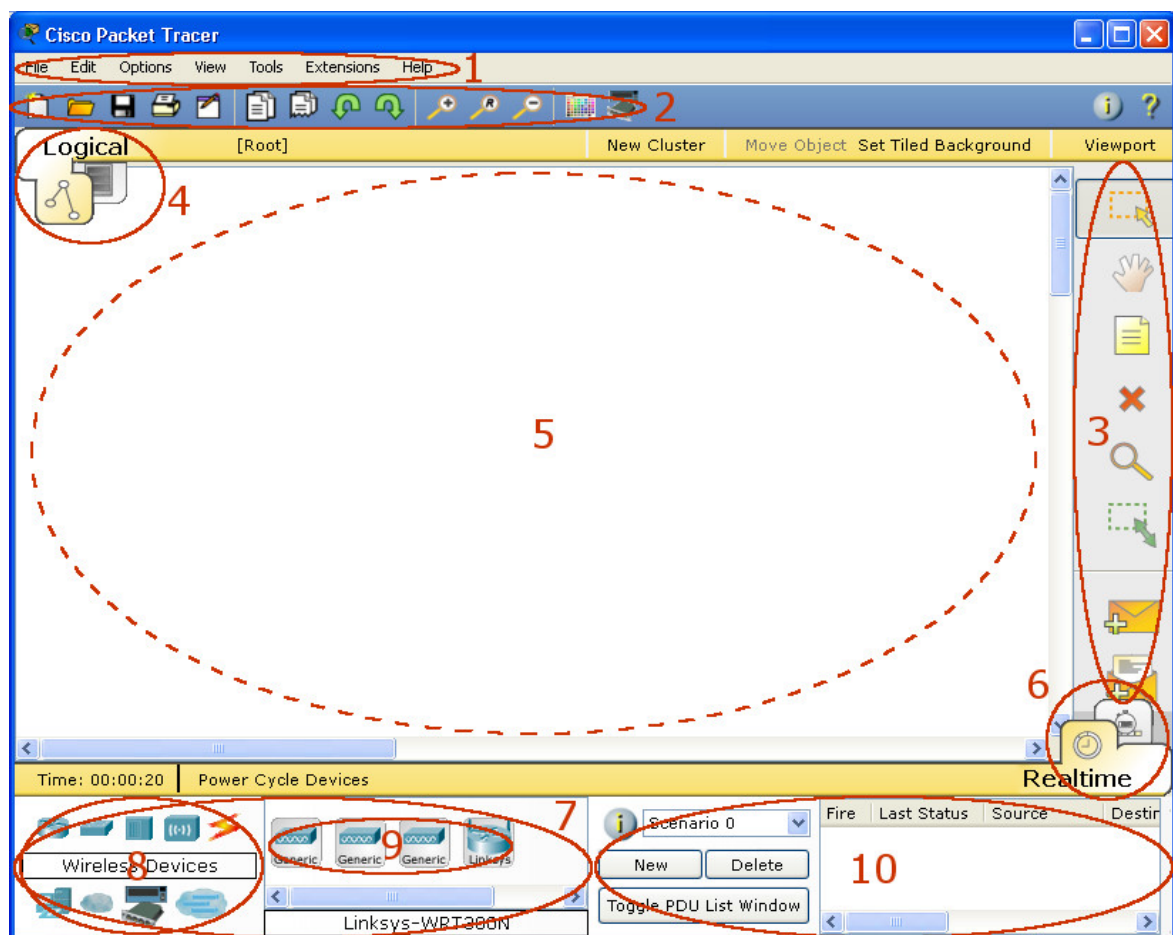


Рисунок 3.1 – Главное окно программы Cisco Packet Tracer

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.

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* – внешний вид устройства и позволяет добавлять/убирать модули. Модули нельзя добавлять/извлекать при включенном устройстве. Перед их смены следует отключить питание устройства, а после замены или добавления интерфейса снова включить.;
- *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 *Simulation* (правая клавиша внизу) можно не только отслеживать движение кадров (в виде конвертов) и 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 модем, 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.

3.2 Оборудование и линии связи в Cisco Packet Tracer

3.2.1 Маршрутизаторы

Маршрутизаторы (рисунок 3.2) используются 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.



Рисунке 3.2 – Панель выбора маршрутизаторов

3.2.2 Коммутаторы

Коммутаторы (рисунок 3.3) – это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Коммутатор передаёт пакеты на основании внутренней таблицы – таблицы коммутации, следовательно, трафик идёт только на тот MAC-адрес, которому он предназначен, а не повторяется на всех портах (как на концентраторе).



Рисунок 3.3 – Панель выбора коммутаторов

3.2.3 Беспроводные устройства

Основными узлами беспроводных Wi-Fi-сетей, осуществляющими ретрансляцию кадров, являются точки доступа (рисунок 3.4).



Рисунок 3.4 – Панель выбора беспроводных устройств

3.2.4 Конечные устройства

Здесь располагаются непосредственно конечные узлы, хосты, сервера, принтеры, телефоны и другое оборудование (рисунок 3.5).

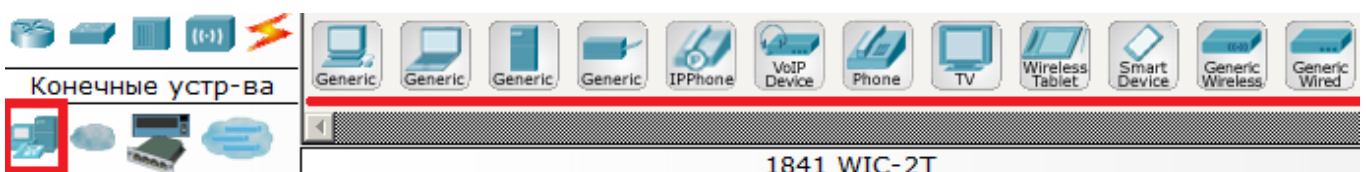


Рисунок 3.5 – Панель выбора конечных устройств








3.2.5 Линии связи

В качестве линий связи, соединяющих телекоммуникационные устройства между собой, могут быть использованы консольный кабель, коаксиальный кабель или витая пара и оптоволоконно (рисунок 3.6). Дополнительно можно указать тип кабельного соединения: прямое или кроссоверное. В таблице 1 приведено описание предлагаемых кабельных линий связи.



Рисунок 3.6 – Панель выбора линий связи

Таблица 3.1 – Типы линий связи

Тип кабеля	Описание
 Console	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Скорость соединения обеих сторон должна быть одинаковая, передаваться может любой поток данных.
 Copper straight-through	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.
 Copper cross-over	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.
 Fiber	Оптоволоконный кабель используется для соединения между оптическими портами.
 Phone	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты.
 Coaxial	Коаксиальный кабель используется для соединения между коаксиальными портами.
 Serial Data Circuit Equipment/Data Terminal Equipment (DCE/DTE)	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке «часов» рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становится DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

3.2.6 Эмуляция Интернета

В этом блоке (рисунок 3.7) располагаются устройства, используемые при эмуляции глобальных сетей, в частности модемы различных типов (DSL или кабельные), «облако» и проч.

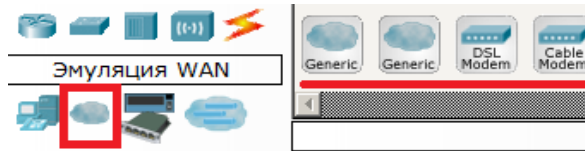


Рисунок 3.7 – Панель выбора топологии сети

3.2.7 Пользовательские устройства

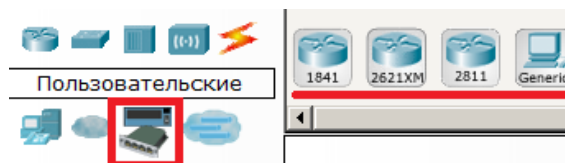


Рисунок 3.8 – Панель выбора пользовательских устройств

3.2.8 Облако для многопользовательской работы

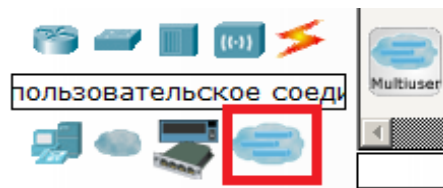


Рисунок 3.9 – Выбор облака для многопользовательской работы

3.3 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).

3.3.1 Управление через консольный порт

Данный тип подключения используется в следующих случаях:

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

В качестве консольного порта в большинстве случаев используется COM-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 выбрать приложение **Terminal**.

Обычно все параметры соединения по умолчанию менять смысла нет. Поэтому достаточно нажать на кнопку «ОК» 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 сделанные 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 немного повысить безопасность системы. Узнать, что это за параметры можно перейдя к конфигурированию линии консоли с помощью line console 0 и выполнив команду «?».

3.3.2 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
```

3.3.3 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 3.10.

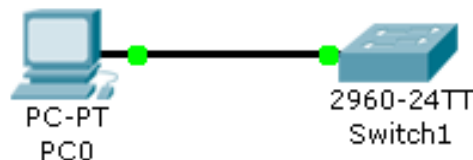


Рисунок 3.10 – Компьютер подключен к коммутатору прямым Ethernet-кабелем

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 3.11:

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

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
```

```
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 3.11 – Настройка пароля для enable-режима

3.3.4 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
```

3.4 Построение и настройка локальной компьютерной сети

Для создания сети необходимо на рабочую область перенести требуемые оконечные устройства (*End Devices*) пользователей – компьютеры, ноутбуки, серверы, принтеры и другие устройства.

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

Для подключения оконечных устройств следует 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 квадратами (или треугольничками) на концах каждого соединения (мигание означает активность линии). При отсутствии соединения квадратики/треугольники 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 конфигура-*

ция (*Physical*). Выполните щелчок мышью по кнопке питания на изображении компьютера, обратите внимание, что находящийся над ней индикатор погас. После включения устройства квадратик/треугольник 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)*, а также добавить из группы *Оконечные устройства (End Devices)* *Ноутбук (Laptop-PT)*.

Поскольку ноутбук, по умолчанию, оснащен только проводным интерфейсом, нужно 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, следует 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. После включения питания ноутбука на физическое схеме будет видно, что ноутбук связался с точкой доступа по радиоканалу (см. рисунок 3.12).

На следующем этапе нужно добавить 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 же, как и 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 одновременно.

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 задавать устройствам адреса следует по протоколу IPv4.

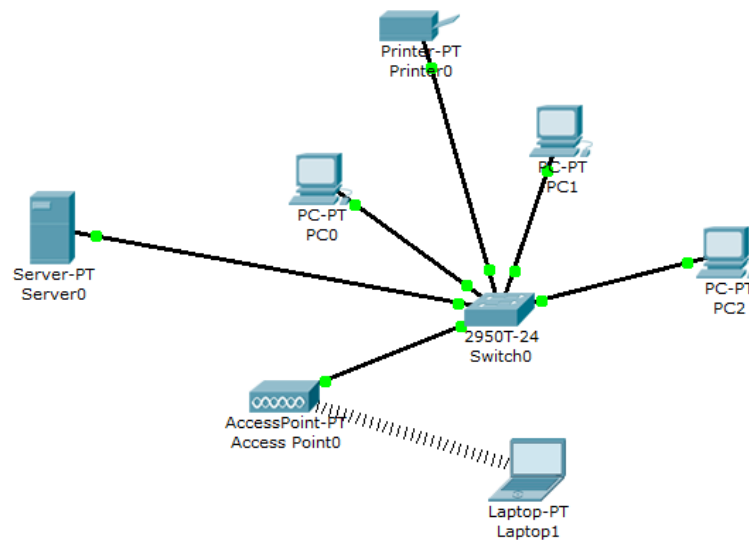


Рисунок 3.12 – Завершенная топология локальной компьютерной сети

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*).

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 3.2. Обратите внимание, что сетевой интерфейс сервера имеет тип *Gigabit Ethernet* и работает на скорости 1000 Мбит/с.

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 вни-

мание 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*).

Таблица 3.2 – Адресная информация для конфигурирования пользовательских устройств локальной компьютерной сети на рисунке 3.12

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 3.13).

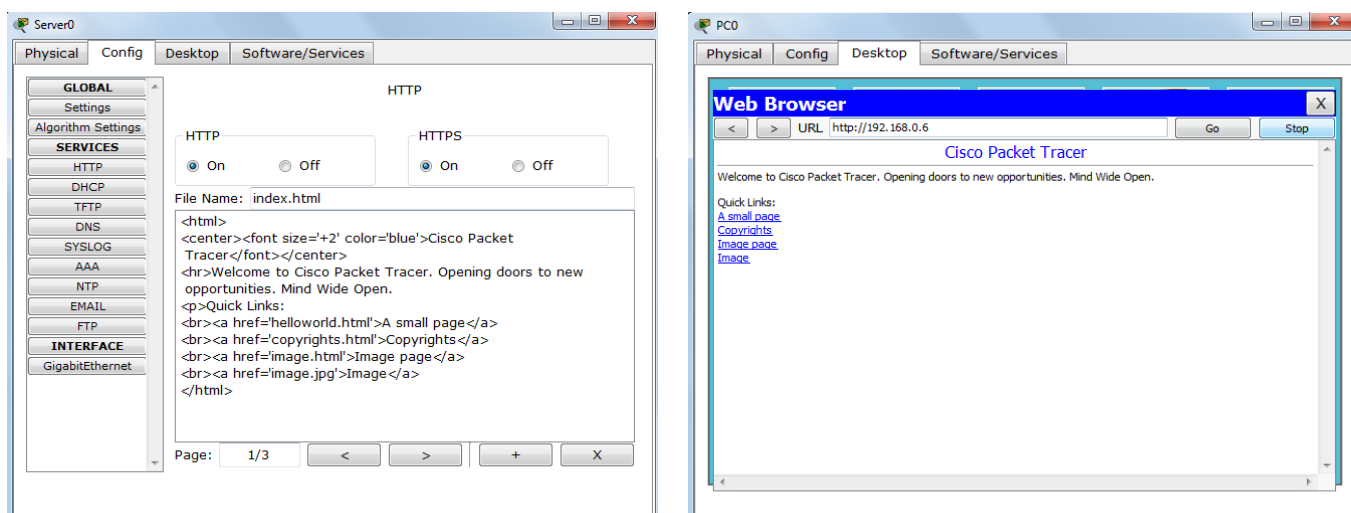


Рисунок 3.13 – Открытие Web-страницы HTTP-сервера в браузере ПК

4 ПРОГРАММА И МЕТОДИКА ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить теоретический материал, касающийся принципам построения локальных компьютерных сетей (выполняется в процессе домашней подготовки).
2. Ознакомиться с особенностями построения системы Packet Tracer и способами построения локальных компьютерных сетей на основе концентратора и коммутатора.
3. Изучить способы конфигурации активного оборудования локальных компьютерных сетей.
4. Построить простейшую локальную сеть на основе концентратора (рисунок 2.3,а) и исследовать ее функционирование в режиме симуляции и в реальном режиме.

IP-адреса рабочих станций при конфигурации выбираются произвольно. **Важно:** адрес сети всех рабочих станций должен быть одинаков!

5. Построить простейшую локальную сеть на основе коммутатора (рисунок 2.3,б) и исследовать ее функционирование в режиме симуляции и в реальном режиме. IP-адреса рабочих станций при конфигурации выбираются произвольно.

При создании сети на основе концентратора (Hub) следует учитывать, что концентратор ретранслирует поступивший на один из портов кадр на все оставшиеся порты. Коммутатор (Switch) пересылает поступивший кадр на основе таблицы коммутации только на порт, к которому подключена адресуемая рабочая станция. Номер каждого из портов связан с MAC адресом компьютера, подключенного к этому порту.

Настройка параметров простейшей сети состоит в назначении сетевых адресов и масок каждой рабочей станции. При этом следует использовать частные сетевые адреса класса А, В или С. Наиболее целесообразно использовать адреса класса С: 192.168.X.X, где X могут принимать значения от 1 до 224. Методика конфигурации рабочих станций и проверки функционирования компьютерной сети детально описана на стр. 25 настоящих методических указаний.

6. Построить в программе Cisco Packet Tracer модель локальной компьютерной сети (рисунок 3.12) на одном коммутаторе и одной беспроводной точке доступа с оконечными 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*.

7. 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).

8. Задать сетевые имена для компьютеров с PC1 по PCМ (М – 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).

9. 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. В начале 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.

10*. Реализовать возможность динамического назначения IP-адресов для хостов.

11. Выполнить проверку связи между одним из ноутбуков и любым ПК, любым сервером, любым принтером. Привести в отчете скриншоты с результатами проверки.

12. 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 РСМ (М – максимальный ПК). Проверить связь между PC1 и PC2. Приведите результаты исследования в отчет.

13. 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.

14*. 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 концентратора, коммутатора и сетевого маршрутизатора.
2. Какие типы линий связи используются при организации локальной вычислительной сети? Дайте их характеристику.
3. Проанализируйте различные топологии компьютерных сетей, их достоинства и недостатки.
4. Какие типы телекоммуникационных устройств входят в состав локальной компьютерной сети и в чем они отличаются друг от друга?
5. Перечислите действия, необходимые для организации локальной вычислительной сети.
6. Поясните в каких случаях и почему применяются прямой и перекрестный кабели UTP.
7. Что называется шлюзом сети и для чего он используется?
8. Какие дополнительные возможности при связи компьютеров дает организация в сети DHCP-сервера.
9. Чем сетевой принтер отличается от обычного принтера, подключенного к компьютеру, входящему в локальную сеть?
10. Перечислите режимы работы в консоли Cisco Packet Tracer и охарактеризуйте их возможности.
11. Что такое баннер и для каких целей он используется?
12. Каким образом коммутатор пересылает пакеты при пинговании, если он работает только на канальном уровне?
13. В каких случаях запускается протокол ARP и какие функции он регламентирует?
14. Зачем нужна маска сети и как она используется?

15. Какие существуют классы сетевых адресов и в каких случаях применяют адреса того или иного класса?

16. Для какой цели введены частные адреса? Можно ли в сети Интернет адресовать устройство с частным адресом?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бони Дж. Руководство по Cisco IOS / Дж.Бони. – М.: Изд-во «Русская редакция», 2008. – 784 с.

2. Дибров М.В. Сети и телекоммуникации. Маршрутизация в IP–сетях. В 2 ч. Часть 2: учебник и практикум для академического бакалавриата / М.В. Дибров. – М.: Изд-во Юрайт, 2019. – 351 с. <https://biblio-online.ru/book/seti-i-telekommunikacii-marshrutizaciya-v-ip-setyah-v-2-ch-chast-2-437865>

3. Сети и телекоммуникации: учебник и практикум для академического бакалавриата / Под ред. К.Е. Самуйлова, И.А. Шалимова, Д.С. Кулябова. – М.: Изд-во Юрайт, 2016. – 363 с.

<https://biblio-online.ru/book/seti-i-telekommunikacii-432824>

4. Таненбаум Э. Компьютерные сети / Э.Таненбаум. 5-е изд. – СПб.: Питер, 2012. – 960 с.

5. Хьюкаби Д. Руководство Cisco по конфигурированию коммутаторов Catalyst / Дэвид Хьюкаби, Стив Мак-Квери. – М.: Изд-во «Вильямс», 2004. – 560 с.

6. Чернега В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. – Севастополь: Изд-во СевНТУ, 2006. – 500 с.

ПРИЛОЖЕНИЕ А
Варианты индивидуальных заданий

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