Министерство образования и науки Российской Федерации

САНКТ-ПЕТЕРБУРГСКИЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

А. Б. Анисифоров

ЦИФРОВАЯ КУЛЬТУРА
ЧАСТЬ 1
КОМПЬЮТЕРНЫЕ СЕТИ И СИСТЕМЫ

Учебное пособие

Санкт-Петербург

2022

УДК 004.7

Анисифоров А.Б. Цифровая культура. Часть 1: Компьютерные сети и системы : учеб. пособие / А.Б. Анисифоров. – СПб., 2022. – 98 с.

В учебном пособии рассматриваются теоретические основы построения и функционирования компьютерных сетей и систем, а также принципы реализации коммуникационных процессов в сетях. Теоретический материал подкреплен несколькими практическими работами в среде Cisco Packet Tracer.

Пособие охватывает раздел «Компьютерные сети и системы» дисциплины «Цифровая культура» и предназначено для студентов, обучающихся по направлениям: 38.03.01 «Экономика», 38.03.02 «Менеджмент», 38.03.03 «Управление персоналом», 38.03.04 «Государственное и муниципальное управление», 38.03.05 «Бизнес-информатика», 38.03.06 «Торговое дело», 38.03.07 «Товароведение», 43.03.01 «Сервис», 43.03.02 «Туризм», 43.03.03 «Гостиничное дело», 38.05.01 «Экономическая безопасность». Также оно может быть использовано при обучении студентов по другим направлениям и дисциплинам, связанным с построением ИТ-инфраструктуры предприятия или организации.

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ИС – информационная система
ИТ – информационные технологии
ОС – операционная система
СУБД – система управления базами данных
ЭВМ – электронная вычислительная машина
ARP – Address Resolution Protocol
ARPANET – Advanced Research Project Agency Network
BGP – Border Gateway Protocol
BYOD – Bring Your Own Device
CLI – Command-Line Interface
COBIT – Control Objectives for Information and Related Technology
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name System
EIGRP – Enhanced Interior Gateway Routing Protocol
ENIAC – Electronic Numeral Integrator and Computer
FDDI – Fiber Distributed Data Interface
FTP – File Transfer Protocol
HTTP – Hypertext Transfer Protocol
HTTPS – HTTP Secure
ICANN – Internet Corporation for Assigned Names and Numbers
IETF – Internet Engineering Task Force
IP – Internet Protocol
ICMP – Internet Control Message Protocol
ITIL – Information Technology Infrastructure Library
ITU – International Telecommunications Union
LAN – Local Area Network
MAC – Media Access Control
MAN – Metropolitan Area Network
NAT – Network Address Translation
NIC – Network Interface Card
TCP – Transmission Control Protocol
OSI – Open System Interconnection
OSPF – Open Shortest Path First
POP3 – Post Office Protocol Version 3
PPP – Point-to-Point Protocol
RIP – Routing Information Protocol
SMTP – Simple Mail Transfer Protocol
SNMP – Simple Network Management Protocol
SSH – Secure Shell
TFTP – Trivial File Transfer Protocol
UDP – User Datagram Protocol
WAN – Wide Area Network

ГЛОССАРИЙ ТЕРМИНОВ

Вычислительная система – это совокупность одного или нескольких компьютеров или процессоров, программного обеспечения и периферийного оборудования, организованная для совместного выполнения информационно-вычислительных процессов.

Глобальная сеть (Wide Area Network, WAN) – сетевая инфраструктура, предоставляющая доступ к другим сетям на большой территории. Обычно принадлежит провайдерам телекоммуникационных услуг и находится под их управлением.

Интерфейс – формально определенная логическая и/или физическая граница между взаимодействующими независимыми объектами. Интерфейс задает параметры, процедуры и характеристики взаимодействия объектов.

Клиент – это модуль, предназначенный для формирования и передачи запросов к ресурсам удаленного компьютера от разных приложений с последующим приемом результатов из сети и передачей их соответствующим приложениям.

Коммутатор (switch) – это высокоскоростной многопортовый мост. Switch создает таблицу MAC-адресов всех устройств, которые к нему подсоединены, и использует ее для передачи данных только на требуемый порт.

Компьютерная сеть – это совокупность компьютеров, связанных через каналы передачи данных для обеспечения обмена информацией и коллективного доступа пользователей к информационным, аппаратным и программным ресурсам сети.

Логический интерфейс (протокол) – это набор информационных сообщений определенного формата, которыми обмениваются два устройства или две программы, а также набор правил, определяющих логику обмена этими сообщениями.

Локальная сеть (Local Area Network, LAN) – объединяет компьютеры, находящиеся на небольшой территории. Это может быть домашняя сеть, сеть малого или крупного предприятия, которая им принадлежит и управляется одним лицом или ИТ-службой.

Маршрутизатор (router) – это промежуточное устройство, которое связывает сети. Он может фильтровать данные по сетевому адресу или продвигать их по наилучшему маршруту, который определяет по таблице маршрутизации.

Модель OSI (Open System Interconnection) – модель взаимодействия открытых систем. Модель определяет уровни взаимодействия систем в сетях с коммутацией пакетов и функции каждого уровня.

Сервер – это модуль, который постоянно ожидает прихода из сети запросов от клиентов, и, приняв запрос, пытается его обслужить, как правило, с участием локальной ОС. Один сервер может обслуживать запросы сразу нескольких клиентов.

Сетевая технология – это согласованный набор аппаратных и программных средств (сетевых адаптеров, драйверов, кабелей и разъемов), а также механизмов передачи данных по линиям связи, достаточный для построения вычислительной сети.

Топология сети – конфигурация графа, вершинам которого соответствуют узлы сети, а ребрам – физические или информационные связи между вершинами.

Физический интерфейс (порт) – определяется набором электрических связей и характеристиками сигналов. Обычно он представляет собой разъем с набором контактов, каждый из которых имеет определенное назначение.

DHCP (Dynamic Host Configuration Protocol) – служба динамического назначения IP-адресов

DNS (Domain Name System) – распределенная система преобразования имени узла в IP-адрес.

Ethernet – доминирующая технология локальных сетей. Стандарты Ethernet описывают реализацию двух нижних уровней модели OSI – проводные соединения и электрические сигналы (на физическом уровне), а так же форматы данных и протоколы управления доступом к сети (на канальном уровне).

ВВЕДЕНИЕ

Активное внедрение и широкое использование информационных, коммуникационных и цифровых технологий во всех сферах человеческой деятельности – одно из важнейших направлений мирового развития. Мы живем в так называемую информационную эпоху, а современную среду обитания называют «информационным обществом». Все чаще мы слышим от специалистов слова «цифровизация», «цифровая экономика», «цифровая трансформация», что указывает на новый виток информатизации с учетом потрясающего уровня развития ИТ. и большого опыта автоматизации деятельности предприятий и организаций. Достижения в области сетевых технологий стали одними из наиболее значимых. Сети позволили создать мир без границ. Сети изменили характер социального, коммерческого, политического и личного взаимодействия. Интернет дает доступ к самым разным ресурсам и сервисам в любое время независимо от местоположения пользователя. Сети поддерживают мгновенный обмен сообщениями, файлами и электронной почтой, обеспечивают функционирование социальных сетей и форумов, служат основой для реализации инструментов и сервисов совместной работы или учебы. Кроме того, ИТ-инфраструктура любого предприятия, организации и даже небольшого офиса представляет собой компьютерную сеть. Поэтому знакомство с основами построения и принципами функционирования компьютерных сетей и систем является важнейшей частью формирования общей цифровой культуры современного человека.

Пособие включает два раздела. В первом разделе рассматриваются теоретические аспекты построения компьютерных сетей, основные понятия, классификации, компоненты сетевой инфраструктуры, а также принципы реализации коммуникационных процессов, в том числе технологии коммутации и маршрутизации. Кроме того, раздел знакомит читателя со стеком коммуникационных протоколов TCP/IP, правилами адресации и работой наиболее важных сетевых служб.

Вторая часть содержит три практических занятия, направленных на закрепление теоретических знаний. Каждое практическое занятие выполняется в эмуляторе Cisco Packet Tracer и включает несколько задач, среди которых построение простой сети на основе управляемого коммутатора, создание сети небольшого предприятия на основе беспроводного маршрутизатора и настройка популярных сетевых служб.

Полученные знания, умения и навыки формируют фундамент для изучения других дисциплин или разделов, связанных с созданием и управлением ИТ-инфраструктурой предприятий и ИТ-поддержкой бизнеса.

Тема 1. Компьютерная сеть как основа корпоративной ИТ-инфраструктуры

Перечень рассматриваемых вопросов:

1) История развития вычислительной техники и сетевых технологий
2) Основные понятия компьютерных систем и сетей
3) Классификации сетей
4) Топологии сетей
5) Сетевая инфраструктура, компоненты сети
6) Обособленные и конвергентные сети
7) Концепция «Принеси с собой свое устройство»
8) Иерархическая архитектура корпоративной сети

История развития вычислительной техники и сетевых технологий

История вычислительной техники насчитывает много веков, однако первые электронные вычислительные машины появились только в середине прошлого века. Это были громоздкие, очень дорогие устройства с низким быстродействием и огромным потреблением электроэнергии.

Например, знаменитая американская машина ENIAC выполняла 5000 операций сложения в секунду и потребляла 150 кВт электроэнергии.

В первом поколении ЭВМ (сер. 40-х – сер. 50-х годов XX века) в качестве элементной базы использовались электронные вакуумные лампы. Данные вводились с помощью перфокарт и перфолент, а у каждой машины был свой язык. Такие машины использовались военными и в других государственных структурах.

Элементная база второго поколения ЭВМ (сер. 50-х – нач. 60-х годов) – транзисторы, информация хранится на дисковых и ленточных магнитных накопителях, появляются языки высокого уровня (Fortran, Cobol), вычислительные машины стали активно использоваться в государственных и научно-исследовательских учреждениях, а также на крупных промышленных предприятиях. Для максимально эффективного использования вычислительной мощности применялась пакетная обработка данных. Удобство пользователя во внимание не принималось.

Пакетная обработка данных предполагает, что все, подлежащие решению выполнению программы, группируются в «пакеты». Пользователь не имеет непосредственного доступа к ЭВМ, а пакеты формируются оператором вручную или с помощью операционной системы (автоматический планировщик, приоритеты, очередь и т.д.).

Достоинство – высокий коэффициент использования ЭВМ (особенно, если задания достаточно большие).

Главный недостаток – от постановки задания в очередь до получения результатов проходит значительное время (от нескольких часов до нескольких дней).

В 1958 г. появились первые интегральные микросхемы. Они стали элементной базой ЭВМ третьего поколения (нач. 60-х – нач. 70-х годов). В этот

период родилась концепция многотерминального многопользовательского режима на основе мэйнфрейма (большая универсальная ЭВМ). Появляются многотерминальные системы разделения времени. Это был прообраз компьютерной сети (рис. 1).

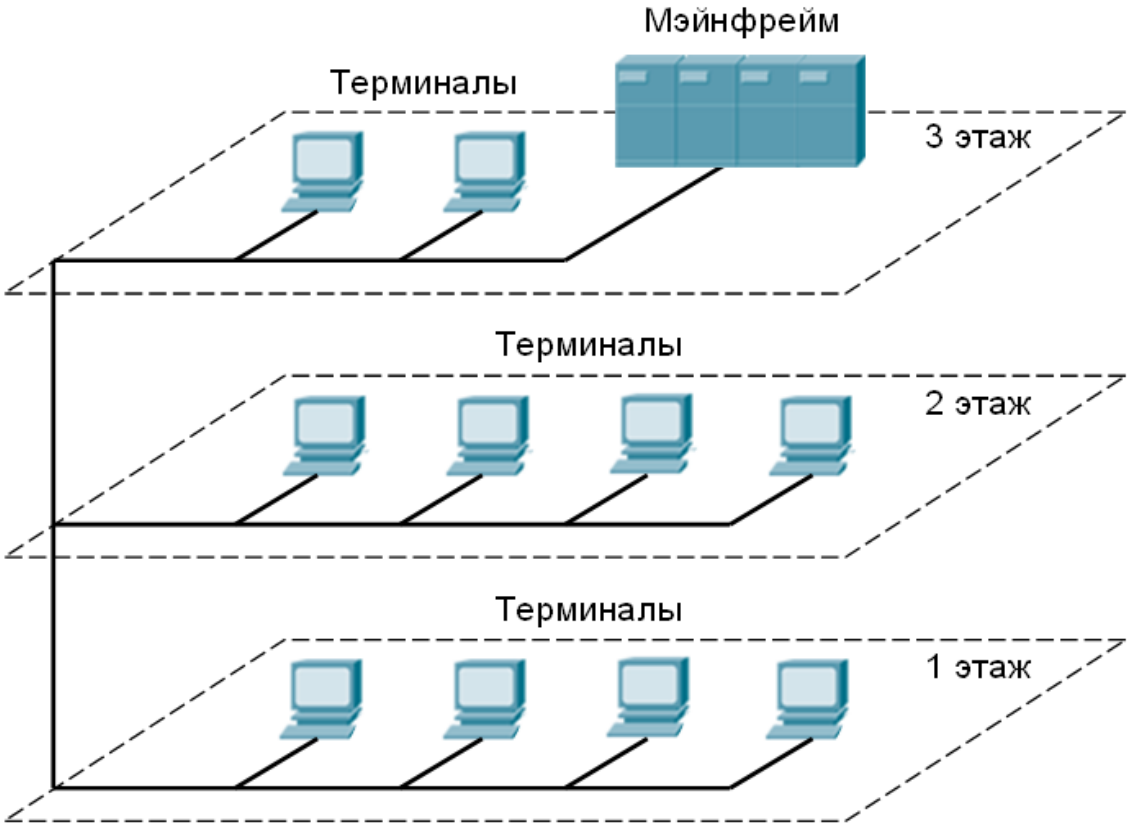


Рисунок 1 – Многотерминальные системы разделения времени

Итак, в 60-е годы появляются новые способы организации вычислительного процесса, которые позволили учесть интересы пользователей. Начали развиваться многотерминальные системы разделения времени – прообраз сети. Вычислительная мощность осталась централизованной, а ввод-вывод стал распределенным.

Однако потребность в создании локальных вычислительных сетей еще не возникла, нечего было объединять. Покупка нескольких компьютеров была непозволительной роскошью (действовал закон Гроша – «производительность компьютера пропорциональна квадрату его стоимости»). Вместе с тем в 1969 г. происходит испытание первой глобальной сети ARPANET, которая объединила компьютеры нескольких университетов США. Таким образом, сначала появились глобальные сети. Они многое унаследовали от телефонных сетей, инфраструктура которых использовалась для передачи данных, но при этом привнесли новое – принцип коммутации пакетов.

В вычислительных машинах четвертого поколения (нач. 70-х годов – настоящее время) используются большие и сверхбольшие интегральные схемы (БИС, СБИС). Появляются микроЭВМ, затем и персональные компьютеры (первая модель ПК была создана Apple в 1976 г., IBM представила IBM PC в 1981 г.). Вычислительная техника используется предприятиями и

организациями для решения широкого круга задач. В 70-е годы возникает потребность в создании локальных сетей, а к началу 80-х – необходимость в стандартизации сетевых технологий.

К середине 80-х годов XX века развитие ИТ привело к существенному перераспределению трудовых ресурсов. В развитых странах количество людей, занятых в информационной сфере, превысило число работников в сфере материального производства. Закончилась индустриальная эпоха, началась эпоха информационная (постиндустриальная).

Возникло новое понятие – информационные ресурсы, а на рубеже веков информация превратилась в важнейший ресурс не только предприятий, но и вообще любой целесообразной деятельности. Развитие информационной сферы стало основой развития общества. В это время начинает формироваться ИТ-рынок, наращиваются темпы информатизации предприятий, растет сложность ИС, усиливается зависимость предприятий от ИТ, появляется дисциплина «Информационный менеджмент», рождается концепция «Архитектуры предприятия», начинается широкомасштабный сбор лучших практик по управлению ИТ-инфраструктурой (проект ITIL) и т.д.

1 января 1983 г. глобальная сеть ARPANET переведена на использование протоколов стека TCP/IP. Так появился Интернет. В настоящее время реализуется новый этап информатизации общества, предприятий и государства – цифровизация, т.е. переход к цифровой экономике.

Возможность доступа и эффективного использования информационных ресурсов предоставляют ИС и ИТ. Совокупность следующих элементов вместе с ИТ-процессами формируют так называемую корпоративную архитектуру ИТ:

1) приложения – прикладные системы и ручные процедуры для обработки информации;
2) информация – данные, введенные в ИС, обработанные и выведенные в любой используемой бизнесом форме;
3) инфраструктура – технологии и устройства, обеспечивающие работу приложений (аппаратное обеспечение, сетевое оборудование, ОС, СУБД, мультимедиа, а также среда, в которой все это находится и поддерживается);
4) персонал – люди, необходимые для планирования, организации, приобретения, внедрения, работы, обслуживания, мониторинга и оценки ИС и услуг.

Очевидно, что именно компьютерная сеть предприятия является платформой для функционирования бизнес-приложений, хранения корпоративных данных, обеспечения доступа к информационным ресурсам любому пользователю из любого места и реализации процессов информационного обмена.

Компания Cisco Systems – крупнейший производитель и поставщик сетевого оборудования для крупных организаций и телекоммуникационных предприятий, знаменитая также своей Сетевой Академией, нацеленной на фундаментальную подготовку IT-специалистов, считает, что достижения в

сетевых технологиях, являются одними из самых значительных изменений в мире. Сети создают мир, в котором границы стран, расстояния и физические границы перестают иметь значение и составляют все меньше препятствий.

Возможность мгновенных коммуникаций через Интернет способствует созданию глобальных сообществ. Глобальные сообщества обеспечивают эффективное взаимодействие людей независимо от местоположения или часового пояса. Cisco называет это «человеческой сетью». В основе этой сети – взаимосвязь Интернета и сетей с людьми и предприятиями.

Основные понятия компьютерных систем и сетей

Под вычислительной (компьютерной) системой – будем понимать совокупность одного или нескольких компьютеров или процессоров, программного обеспечения и периферийного оборудования, организованную для совместного выполнения информационно-вычислительных процессов.

Если компьютерная система состоит из достаточно удаленных компьютеров, такую систему называют распределенной. За такими системами закрепился термин «компьютерная сеть».

Компьютерная сеть – набор связанных между собой автономных компьютеров (Эндрю Таненбаум «Компьютерные сети»). Вероятно, это самое компактное определение, но мы будем использовать более емкое.

Компьютерная сеть – это совокупность компьютеров, связанных через каналы передачи данных для обеспечения обмена информацией и коллективного доступа пользователей к информационным, аппаратным и программным ресурсам сети.

Классификации сетей

Сети можно классифицировать на основе разных признаков. Чаще всего используют технологические признаки, связанные с территорией покрытия. При таком подходе все сети можно разделить на локальные и глобальные.

Локальная сеть (Local Area Network, LAN) – объединяет компьютеры, находящиеся на небольшой территории. Это может быть домашняя сеть, сеть малого или крупного предприятия, которая им принадлежит и управляется одним лицом или ИТ-службой.

Глобальная сеть (Wide Area Network, WAN) – сетевая инфраструктура, предоставляющая доступ к другим сетям на большой территории. Обычно принадлежит провайдерам телекоммуникационных услуг и находится под их управлением.

Иногда упоминают третий тип – городская сеть (Metropolitan Area Network, MAN). Она охватывает территорию больше, чем локальная сеть, но меньше, чем глобальная (например, город), и сочетает в себе признаки и локальных, и глобальных сетей.

Локальные сети используют сервисы глобальных сетей для соединения друг с другом, глобальные сети соединяются между собой. Объединение взаимосвязанных сетей в мировом масштабе образует Интернет. Интернет не

принадлежит какому-либо лицу или группе людей. Обеспечение эффективного функционирования такой сложной и разнообразной инфраструктуры требует применения общепризнанных технологий и стандартов. Поэтому вопросами регулирования структуры и стандартизации протоколов и процессов Интернета занимаются специальные организации, в том числе Инженерная группа по развитию Интернета (IETF), Исследовательская группа интернет-технологий (IRTF), Ассоциация по присвоению имен и адресов (ICANN), Администрация адресного пространства Интернета (IANA), Международный союз электросвязи (ITU) и другие.

В зависимости от используемой среды передачи данных сети бывают проводными и беспроводными.

С точки зрения типа пользователей, которым сеть предоставляет услуги, рассматривают сети операторов связи, которые предоставляют публичные услуги, и корпоративные сети, они предоставляют услуги только сотрудникам предприятия. Характерно, что корпоративная сеть может иметь любой размер. Сеть крупного распределенного предприятия состоит из локальных сетей и глобальной сети, которая их объединяет.

Топологии сетей

Сети можно классифицировать на основе топологии. Под топологией сети понимается конфигурация графа, вершинам которого соответствуют узлы сети, а ребрам – физические или информационные связи между вершинами. Рассмотрим базовые топологии сетей.

Точка-точка

Простейшая топология. Является наиболее распространенной в глобальных сетях (рис. 2).

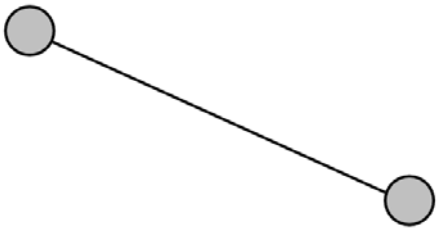


Рисунок 2 – Топология «точка-точка»

Полносвязная

Каждый узел связан с каждым. Очень надежная структура, но административные и физические расходы могут быть весьма значительными. Применяется в глобальных сетях, а также в многомашинных комплексах, объединяющих небольшое количество компьютеров (рис. 3).

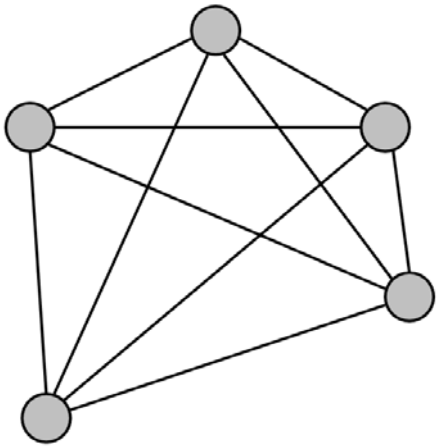


Рисунок 3 – Полносязная топология

Ячеистая

Получается из полносвязной путем удаления некоторых связей. Характерна для крупных сетей (рис. 4).

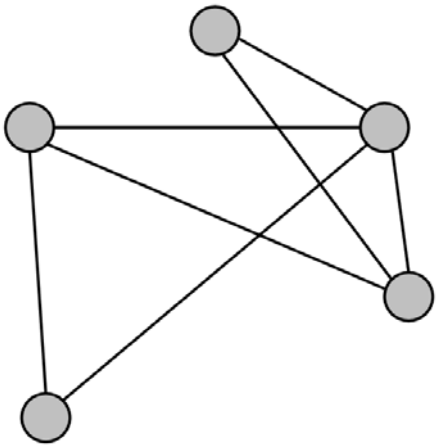


Рисунок 4 – Ячеистая топология

Общая шина

Все узлы подключены к общему кабелю. Дополнительное коммуникационное оборудование (концентраторы, коммутаторы) не требуется (рис. 5). Самая дешевая и наименее надежная топология. Шинные топологии использовались ранее в коаксиальных вариантах технологии Ethernet.

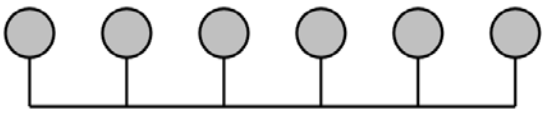


Рисунок 5 – Топология «Общая шина»

Звезда

В топологии такого типа узлы подключаются к центральному промежуточному устройству, например к концентратору или коммутатору (рис. 6). Самая популярная топология. Характерные особенности: простой монтаж, высокая масштабируемость и простое устранение неполадок.

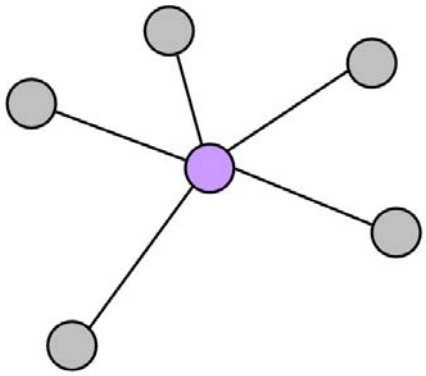


Рисунок 6 – Топология «Звезда»

Иерархическая звезда (дерево)

Пример гибридной топологии. Дополнительные концентраторы или коммутаторы обеспечивают соединение с другими звездообразными топологиями (рис. 7).

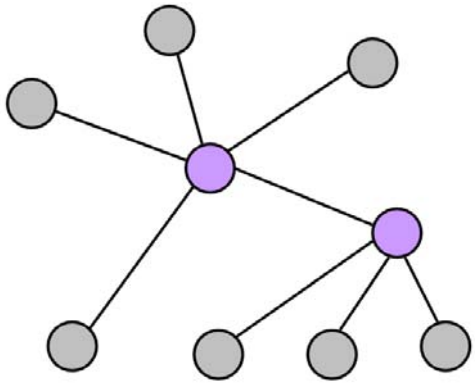


Рисунок 7 – Топология «Иерархическая звезда»

Кольцо

Каждый узел соединяется с соседним, образуя сеть в форме кольца (рис. 8). Топология использовалась в устаревших сетях FDDI и Token Ring.

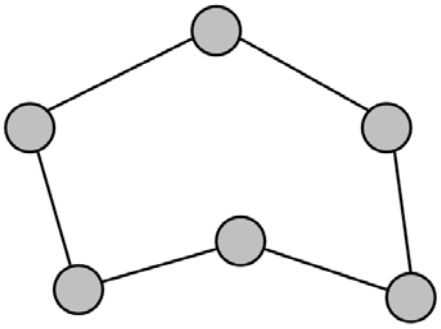


Рисунок 8 – Топология «Кольцо»

Сетевая инфраструктура, компоненты сети

Сетевая инфраструктура включает в себя три категории аппаратных средств (рис. 9):

- оконечные устройства (компьютеры, ноутбуки, IP-телефоны, смартфоны, планшеты, принтеры и др.);
- промежуточные устройства (маршрутизаторы, межсетевые экраны, коммутаторы, точки беспроводного доступа и др.);
- среда передачи данных (проводная или беспроводная).

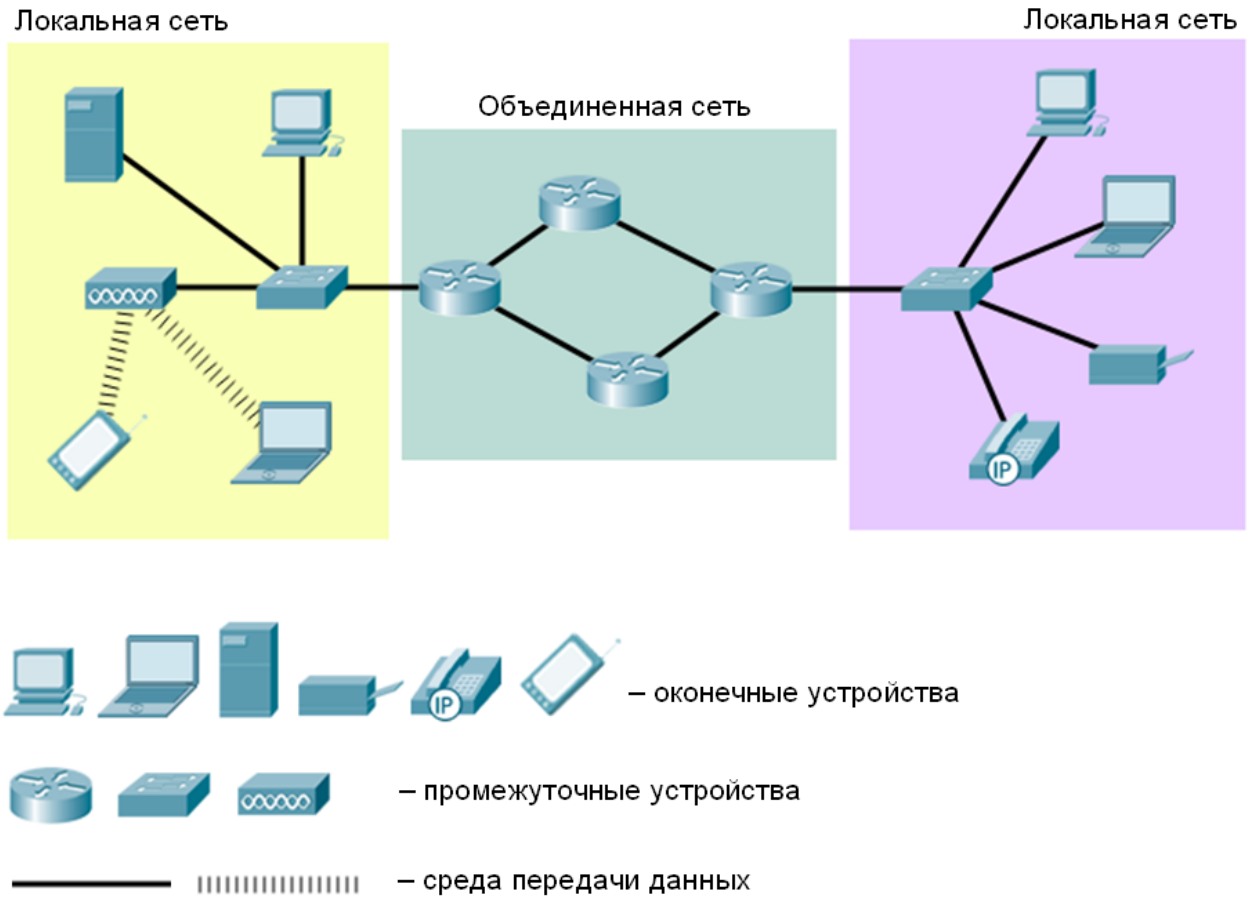


Рисунок 9 – Сетевая инфраструктура и ее компоненты

Кроме того, важнейшими компонентами сети являются сетевые операционные системы и сетевые приложения и сервисы, которые используются нами для решения различных задач, например, электронная почта или web-служба.

Оконечные устройства знакомы пользователям лучше всего. Оконечное устройство может быть либо отправителем, либо получателем сообщения. Чтобы устройство подключить к сети, оно должно быть оборудовано сетевыми средствами. Сетевая интерфейсная карта (NIC) – адаптер сети, который обеспечивает физическое подключение к сети настольного компьютера или другого устройства, реализуя внешний интерфейс (рис. 10, 11).

Интерфейс – важное понятие, которое активно используется сетевыми инженерами и другими специалистами ИТ-отрасли.

Интерфейс (в широком смысле) – формально определенная логическая и/или физическая граница между взаимодействующими независимыми объектами. Интерфейс задает параметры, процедуры и характеристики взаимодействия объектов. Разделяют физический и логический интерфейсы.

Рисунок 10 – Адаптер проводной сети

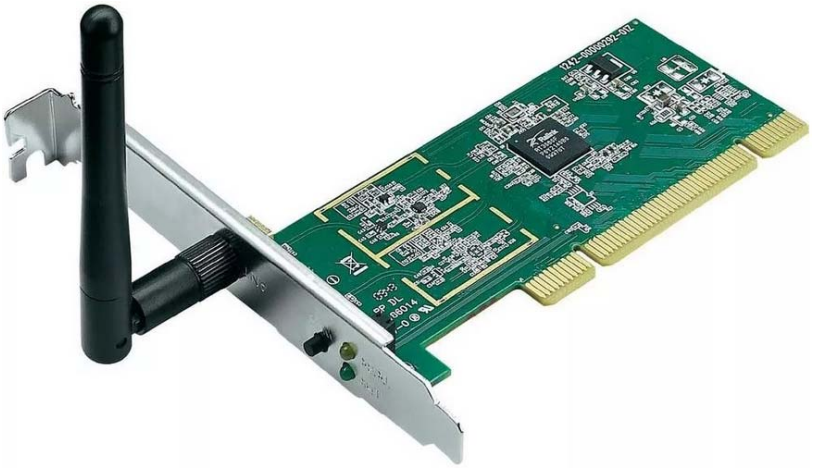


Рисунок 11 – Адаптер беспроводной сети

Физический интерфейс (порт) – определяется набором электрических связей и характеристиками сигналов. Обычно это разъем с набором контактов, каждый из которых имеет определенное назначение.

Логический интерфейс (протокол) – это набор информационных сообщений определенного формата, которыми обмениваются два устройства или две программы, а также набор правил, определяющих логику обмена этими сообщениями.

Каждому оконечному устройству в сети, вернее, его сетевому интерфейсу назначается адрес, чтобы устройства можно было различать. Если оконечное устройство инициирует обмен данными, то в качестве получателя сообщения оно использует адрес оконечного устройства назначения.

Промежуточные устройства соединяют оконечные устройства с сетью и могут связать несколько отдельных сетей для создания объединенной сети. Промежуточные устройства обеспечивают подключение и прохождение потоков данных по сети. Для определения пути передачи сообщения промежуточные устройства используют адрес оконечного устройства назначения в сочетании с информацией о связях в сети. На рисунке 12 представлены наиболее популярные промежуточные устройства компьютерных сетей и их изображения, используемые на схемах.

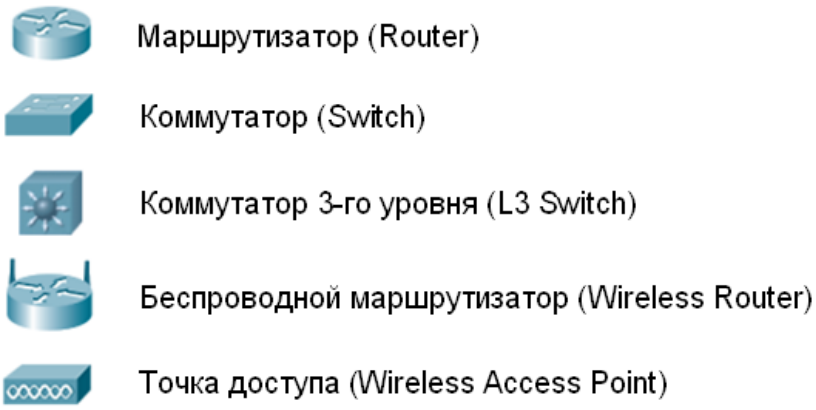


Рисунок 12 – Промежуточные устройства

Основными функциями промежуточных устройств являются: продвижение пакетов, обеспечение доступа беспроводных клиентов к проводной сети, сбор и актуализация информации о существующих маршрутах между сетями, перенаправление информации по альтернативным маршрутам, разрешение или запрет передачи данных в зависимости от настроек безопасности и др.

Более подробно принципы работы коммутатора и маршрутизатора будут рассмотрены во второй лекции.

Среда передачи данных – это канал (линия) связи, по которому сообщение передается от источника к адресату. В современных сетях в основном используются три типа среды передачи.

- кабели на основе скрученных пар медных проводов («витая пара» экранированная или неэкранированная) – данные кодируются электрическими сигналами (рис. 13);
- волоконно-оптические кабели – данные кодируются световыми импульсами (рис. 14).
- беспроводная среда – для передачи данных используются радиосигналы.

Коаксиальные кабели с медной жилой (рис. 15) использовались в ранних спецификациях технологии Ethernet. В настоящее время не используются в локальных сетях, однако некоторые провайдеры еще применяют этот кабель для подключения клиентов к интернету.

Рисунок 13 – Кабель на основе скрученных медных пар

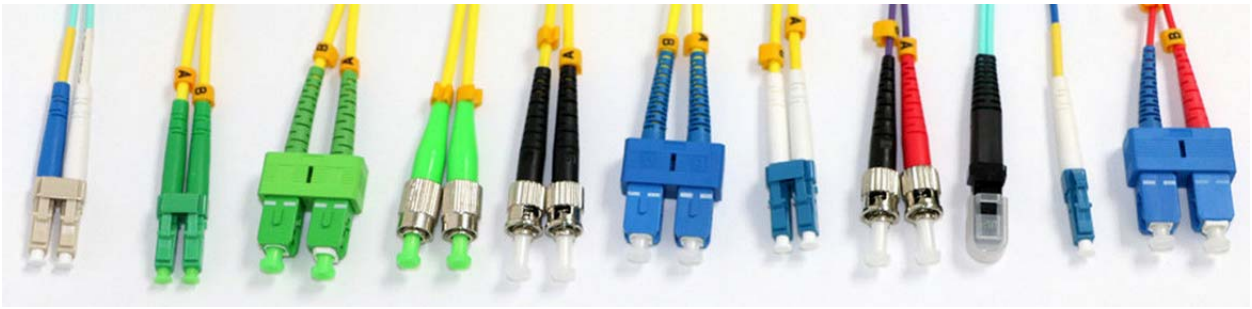


Рисунок 14 – Волоконно-оптические кабели

Рисунок 15 – Коаксиальный кабель

Обособленные и конвергентные сети

Не так давно телефонная связь, телевидение и сети передачи данных существовали обособленно, а значит, не могли взаимодействовать друг с другом. Применялись разные технологии передачи сигналов, в каждой сети для обеспечения связи использовался свой собственный набор правил и стандартов. Сегодня разрозненные сети данных, телефонные и видео сети объединяются. В отличие от выделенных сетей конвергентные сети позволяют передавать и данные, и голос, и видео между различными устройствами при использовании одной и той же сетевой инфраструктуры по одним и тем же правилам, соглашениям и стандартам реализации.

Концепция «Принеси с собой свое устройство»

По мере развития новых технологий и появления на рынке новых оконечных устройств предприятия и пользователи должны приспосабливаться к изменяющимся условиям. Среди основных трендов можно выделить концепцию Bring Your Own Device (BYOD) – «принеси (на работу) свое устройство». Обеспечение доступа с любого устройства к любому контенту любым способом – глобальная тенденция, которая требует пересмотра способов использования устройств. Популярность и потребительские свойства устройств растут, а цена падает, поэтому многие сотрудники и учащиеся могут иметь в личном пользовании самые совершенные вычислительные и сетевые инструменты. Концепция BYOD предполагает, что конечные пользователи могут применять личные устройства (ноутбуки, нетбуки, планшеты, смартфоны) для доступа к информации в корпоративной сети. Мобильный или удаленный доступ к корпоративной сети открывает для бизнеса новые возможности, однако создает дополнительные угрозы информационной безопасности.

Иерархическая архитектура корпоративной сети

Современная корпоративная сеть использует иерархическую модель, чтобы разделить архитектуру на уровни. Каждый уровень выполняет определенные функции, что упрощает проектирование, развертывание и администрирование сети (рис. 16).

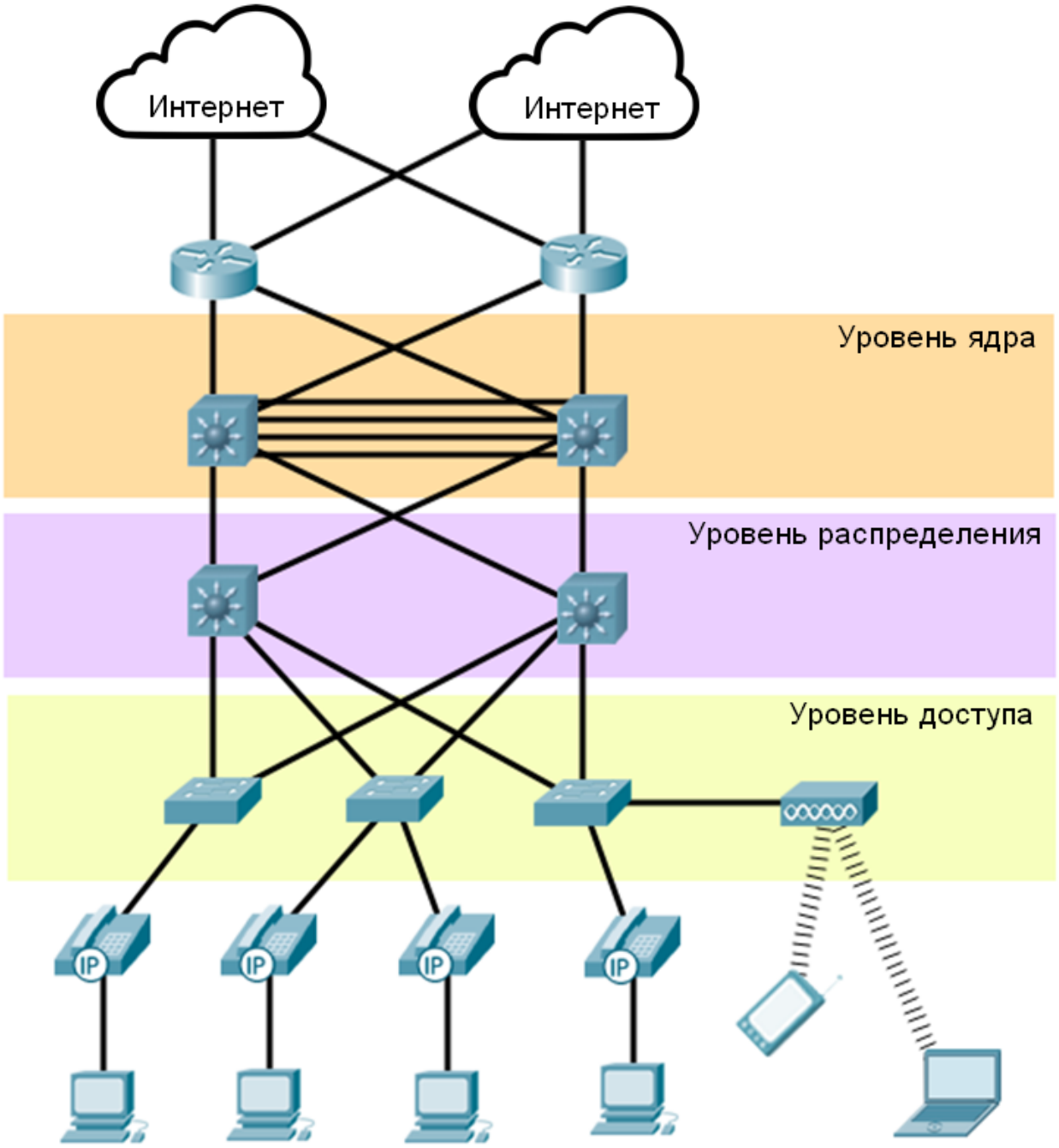


Рисунок 16 – Архитектура корпоративной сети

1) Уровень доступа предоставляет конечным устройствам и пользователям прямой доступ к сети.

2) Уровень распределения объединяет уровни доступа и обеспечивает возможность подключения к сервисам с заданным классом обслуживания.

3) Уровень ядра (сетевая магистраль) обеспечивает связь между уровнями распределения для крупных локальных сетей, т.е. обеспечивает высокоскоростное магистральное подключение и изоляцию сбоев.

Хотя иерархическая модель имеет три уровня, небольшие корпоративные сети часто используют двухуровневую иерархическую модель. Здесь уровни ядра и распределения совмещены (вырожденное ядро) для упрощения, уменьшения количества устройств и снижения затрат (рис. 17).

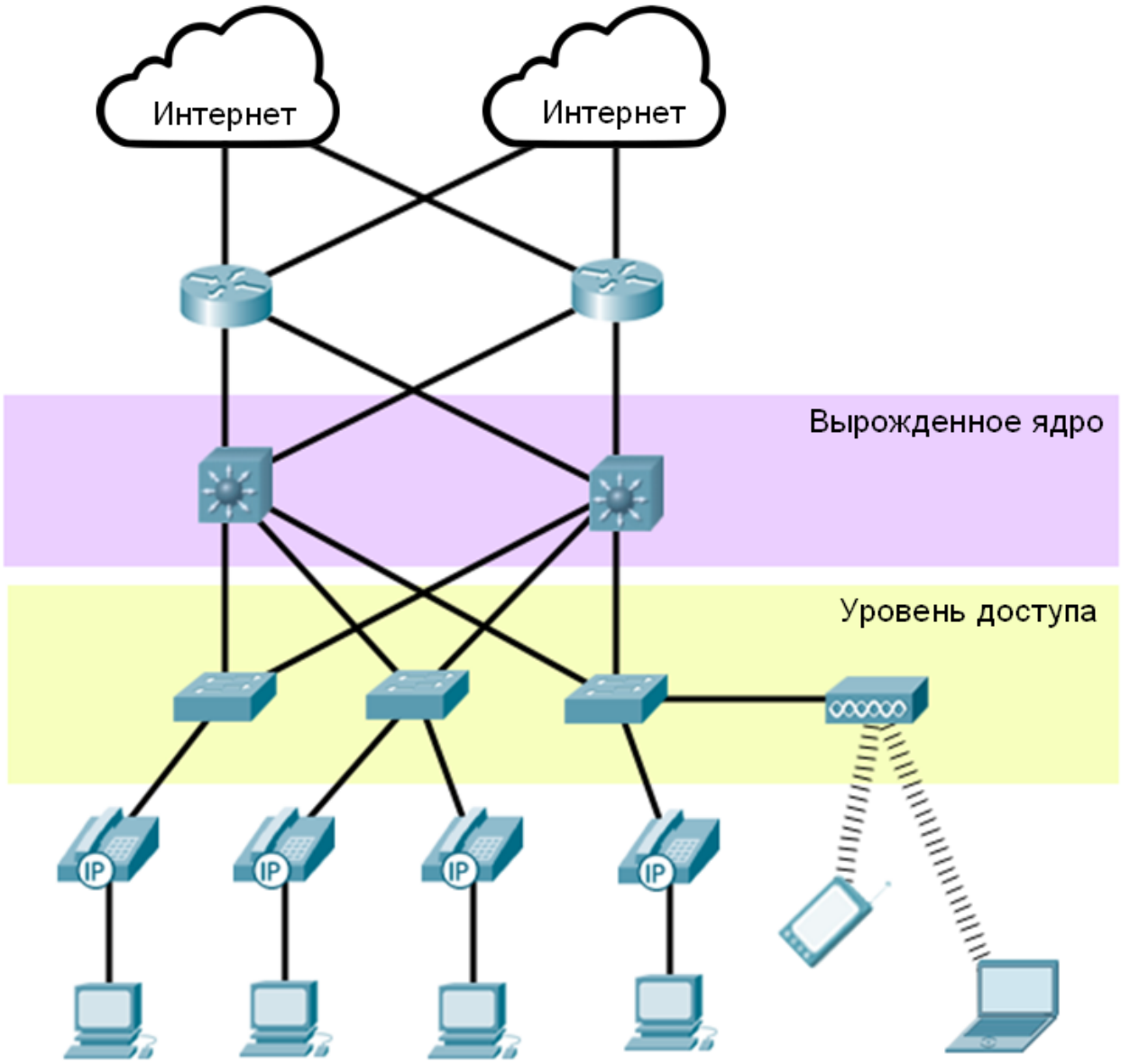


Рисунок 17 – Двухуровневая модель с вырожденным ядром

В плоской сетевой архитектуре изменения часто затрагивают большое количество систем. Иерархическая модульная структура упрощает управление и повышает отказоустойчивость, поскольку изменения затрагивают лишь часть сети, а неисправности эффективнее изолируются благодаря уменьшению доменов отказа. Модульность обеспечивает высокую масштабируемость и внедрение новых сервисов по мере необходимости.

Для повышения эффективности использования иерархической модели корпоративной сети рекомендуется в частности:

- использовать расширяемое модульное оборудование, которые можно легко модернизировать для увеличения их возможностей, т.е. для поддержки новых функций просто добавляются новые аппаратные модули в уже существующее оборудование;
- использовать иерархичность и модульность архитектуры для добавления и обновления функциональных областей сети, не затрагивая при этом другие области (например, реализация изменений на уровне доступа не затрагивает уровни распределения и ядра);
- использовать продуманную иерархическую стратегию адресации устройств, чтобы при появлении новых пользователей и сервисов не потребовалось заново настраивать адреса во всей сети;
- использовать маршрутизаторы и коммутаторы 3-го уровня для ограничения широковещания и сокращения объема трафика к ядру сети;
- реализовать резервные каналы между критически важными устройствами, а также между устройствами уровня доступа и уровня ядра;
- использовать несколько каналов между различными устройствами с использованием функций агрегации каналов или распределение нагрузки в целях увеличения пропускной способности;
- обеспечить беспроводные подключения для поддержки мобильности и расширения.

Реализация и эксплуатация этой модели происходит в условиях постоянных изменений требований, связанных с изменяющимися потребностями бизнеса, появлением новых технологий, необходимостью развертывания новых сервисов и внедрения ИТ-решений, обеспечения заданного уровня информационной безопасности, а также необходимостью обеспечивать поддержку пользователей с согласованным уровнем обслуживания.

Для решения этих задач на предприятиях создается ИТ-служба, которая управляет всей сложной ИТ-инфраструктурой, используя специальные методы и инструменты, осуществляя постоянный мониторинг ее состояния.

В настоящее время существует целый ряд методик управления ИТ-инфраструктурой, опирающихся на международные стандарты и хорошие практики, и реализующих сервисный подход. Этот стандарты ISO/IEC 20000, COBIT, лучшие практики организации ИТ-процессов и ИТ-услуг (библиотека ITIL) и др. Они помогают справиться со всеми сложностями при управлении ИТ-инфраструктурой предприятия, а также персоналом, задействованным в оказании и поддержке услуг.

Перспективным направлением в развитии технологий управления сетями является концепция сетей, управляемых на основе намерений. На ИТ-рынке уже предлагаются соответствующие продукты. Например, лидер отрасли – компания Cisco Systems – предлагает технологическое решение, в рамках которого сеть самостоятельно преобразует бизнес-намерения в соответствующие конфигурации сети для всех устройств. Сетевому администратору нужно только описать в бизнес-терминах задачи и показатели для сети, а также «пропустить» это описание через искусственный интеллект. Остальное сеть сделает сама. Объем ручной работы минимизируется, осуществляет-

ся непрерывное отслеживание с автоматической перенастройкой сети, согласованное с заданными намерениями, что обеспечивает дополнительный уровень мониторинга сети. Это позволяет любые изменения в бизнес-модели достаточно быстро конвертировать в сетевую инфраструктуру, обеспечив поддержку процессов информационного обмена в соответствии с требованиями бизнеса.

Вопросы для самопроверки

1) Для чего нужны компьютерные сети?
2) Какая топология является наиболее распространенной в локальных сетях?
3) Что значит «конвергентная сеть»?
4) Каковы основные функции промежуточных устройств?
5) Какой тип кабеля обеспечивает передачу данных на дальние расстояния?
6) Какие элементы формируют корпоративную ИТ-архитектуру?
7) Какое оборудование относят к оконечным устройствам сети?
8) Какой уровень модели корпоративной сети реализует сетевую магистраль?

Тема 2. Основные принципы реализации коммуникационных процессов в компьютерных сетях

Перечень рассматриваемых вопросов:

1) Модель взаимодействия открытых систем
2) Сетевые технологии, технология Ethernet
3) Стек TCP/IP
4) Промежуточные устройства. Коммутаторы, маршрутизаторы
5) Сетевые службы

Модель взаимодействия открытых систем

Итак, чтобы подключать устройства к компьютерной сети, их нужно оборудовать сетевыми средствами, но для обеспечения сетевого взаимодействия этого недостаточно. Необходимо организовать процесс информационного обмена, определить задачи и разработать правила и порядок их решения. Перечислим наиболее важные:

- формирование сообщений;
- разделение их на сегменты для передачи пакетами;
- преобразование имен и адресов;
- определение маршрута в сложной сети;
- контроль целостности и коррекция ошибок;
- повторная передача при потере данных.

Среда передачи может содержать большое количество посредников (различных промежуточных устройств). Это приводит к возникновению новых дополнительных коммуникационных задач, для решения которых требуются развитые транспортные средства.

Рассмотрим простую бизнес-задачу, которая покажет, сколько самых разных операций необходимо выполнить для передачи сообщения.

Предположим, директор компании «А» (Иван Иванович) отправляет документ своему партнеру, директору компании «Б» (Петру Петровичу). У каждого директора есть секретарь, а для отправки документа используется либо почта, либо курьер. После подготовки документа директор компании «А» поручает отправку своему секретарю и устанавливает требования, например, передать срочно, проконтролировать доставку, получить подтверждение и т.п., либо просто отправить и забыть. Причем в качестве адресата директор указывает Петра Петровича, а поиск почтового адреса выполнит секретарь. Секретарь положит документ в конверт, укажет адрес и вызовет курьера, либо бросит письмо в почтовый ящик. Когда письмо будет доставлено, его сначала получит секретарь директора компании «Б» и подтвердит получение (если это требовалось). После этого конверт будет распечатан, и документ передан Петру Петровичу.

Данный пример показывает, что, несмотря на элементарность процесса, задача оказалась многоуровневой. Каждый уровень выполняет определенные функции. Директора не интересует технология доставки, он выступает в роли заказчика сервиса, устанавливая требования к нему. Он даже не знает почто-

вого адреса своего партнера по бизнесу. Преобразованием имени в почтовый адрес занимается секретарь. Он также занимается формированием пакета и выбором средства доставки, причем его совершенно не интересует содержание документа, его задача – доставка пакета. Для физической передачи задействуется нижележащий уровень – курьер или почта.

Каждый уровень взаимодействует только со смежным, а одинаковые уровни соседних узлов выполняют аналогичные функции. Один секретарь помещает документ в конверт, снабжает его адресом и передает курьеру, а другой секретарь решает обратную задачу – принимает конверт, проверяет адрес, вскрывает конверт и передает документ директору. В результате директор компании «Б» получил документ именно в том виде, в котором его подготовил партнер. Таким образом, одинаковые уровни выполняют сходные задачи, т.е. реализуют протокол этого уровня. Межуровневый интерфейс обеспечивает взаимодействие соседних уровней на одном узле.

Многоуровневый подход лег в основу организации сетевого взаимодействия.

Модель взаимодействия открытых систем (The Open System Interconnection model, модель OSI) разработана в 1984 г. и является популярной эталонной моделью, которая определяет уровни взаимодействия систем в сетях с коммутацией пакетов и функции каждого уровня, тем самым обеспечивая единообразное применение всех сетевых протоколов и сервисов. В модели OSI средства взаимодействия делятся на семь уровней: прикладной, представления, сеансовый, транспортный, сетевой, канальный и физический (рис. 18). Каждый уровень реализует определенный аспект взаимодействия сетевых устройств.

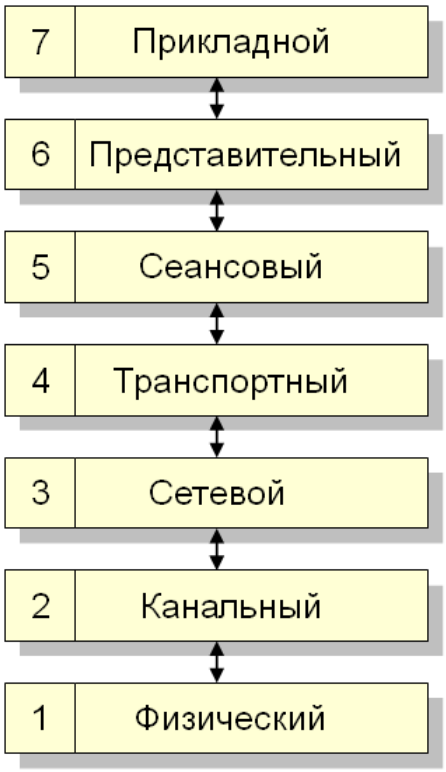


Рисунок 18 – Модель взаимодействия открытых систем (Модель OSI)

Прикладной уровень – это набор протоколов, обеспечивающих взаимодействие пользовательских приложений с сетью.

Уровень представления – обеспечивает преобразование форматов данных. На этом уровне может выполняться шифрование и расшифрование данных.

Сеансовый уровень – обеспечивает управление диалогом, синхронизацию, контрольные точки передачи.

Транспортный уровень – обеспечивает приложениям или верхним уровням стека передачу данных с той степенью надежности, которая им требуется.

Сетевой уровень – уровень взаимодействия сетей. Обеспечивает маршрутизацию данных на основе логической адресации узлов.

Канальный уровень – обеспечивает надежную передачу данных по физическому каналу. Решает задачи управления доступом к среде, обнаружения и коррекции ошибок.

Физический уровень – реализует передачу потоков битов по физическим каналам связи в виде электрических, оптических или радиосигналов.

Верхние уровни модели решают задачи предоставления прикладных сервисов, нижние уровни (с транспортного уровня и ниже) образуют транспортную подсистему, которая решает задачи транспортировки сообщений с заданным уровнем качества в составных сетях.

Если приложение компьютера «А» собирается взаимодействовать с приложением компьютера «Б», оно обращается с запросом к прикладному уровню, где формируется сообщение определенного формата. Затем сообщение передается вниз следующему уровню, где выполняются определенные действия и к сообщению добавляется служебная информация. Наконец, сообщение, которое «обросло» служебной информацией, достигает физического уровня, который передает его по каналам связи в виде электрических, световых или электромагнитных сигналов. Когда сообщение достигает узла назначения, оно принимается его физическим уровнем и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню.

Модель позволяет понять, как реализуется процесс взаимодействия узлов сети. Вместе с тем реальные стеки сетевых протоколов, в том числе доминирующий стек TCP/IP, не в полной мере этой модели соответствуют.

Сетевые технологии, технология Ethernet

Сетевая технология – это согласованный набор стандартных протоколов и реализующих их программно-аппаратных средств (сетевых адаптеров, драйверов, кабелей, разъемов и пр.), достаточный для построения компьютерной сети.

Официально принятой сетевой технологии не существует, но со временем особенно распространилась одна технология, которая называется Ethernet. Ее первая фирменная версия появилась еще в середине 70-х годов

прошлого века. Благодаря своей простоте, гибкости и низкой стоимости Ethernet постепенно вытеснил конкурирующие технологии локальных сетей, де-факто став стандартом локальных проводных сетей. Более того, Ethernet сейчас активно используется как технология операторского класса (Metro Ethernet). За время своего существования технология «разогналась» с 10 Мбит/с до 100 Гбит/с и более.

В 90-е годы начали развиваться технологии беспроводных сетей: Wi-Fi, Bluetooth, ZigBee и др., однако рассмотреть их в рамках небольшого раздела дисциплины не представляется возможным.

В стандартах Ethernet прописаны протоколы, использующиеся на физическом и канальном уровнях модели OSI. В ранних спецификациях Ethernet в качестве среды передачи использовался коаксиальный кабель, но в настоящее время – только медная пара и волоконно-оптические кабели. Именно оптоволокно позволяет передавать информацию с огромной скоростью на дальние расстояния. В локальных сетях на уровне доступа чаще всего используется медная пара категории 5E, позволяющая передавать информацию со скоростью 100 Мбит/с (Fast Ethernet) или 1 Гбит/с (Gigabit Ethernet) при длине кабеля не более 100 м. Для подключения оконечных устройств к сети используются коммутаторы Ethernet (рис. 19). Коммутаторы и все современные сетевые интерфейсные карты могут работать в дуплексном режиме, т.е. передавать и принимать информацию одновременно. Это позволяет устройству инициировать обмен информацией по сети в любой момент, когда это необходимо.

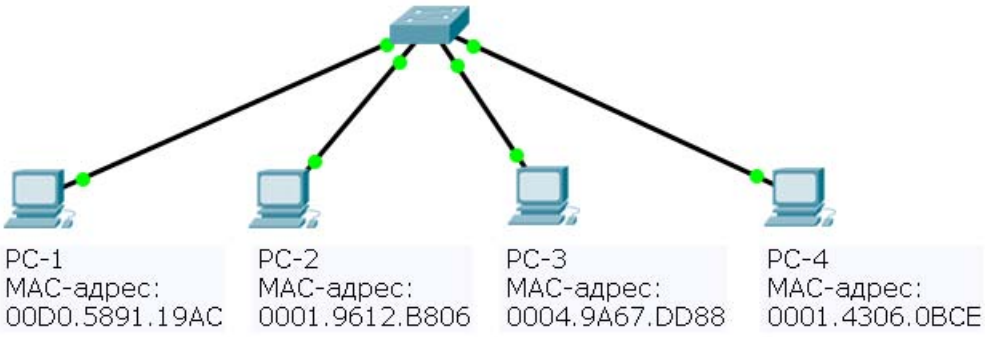


Рисунок 19 – Сеть Ethernet на основе коммутатора

Для идентификации устройств с сети Ethernet используется физический адрес сетевого интерфейса. Он присваивается при изготовлении и называется MAC-адресом (Media Access Control). Адрес 48-битный, обычно он представляется в шестнадцатеричном виде, а за его уникальность отвечает производитель.

При передаче информации на канальном уровне формируется кадр, в который инкапсулируется сообщение (или его фрагмент). Чтобы устройства понимали друг друга, формат кадра строго регламентирован. Кадр может иметь размер от 64 до 1518 байт, из них 18 байт – служебная информация (рис. 20).

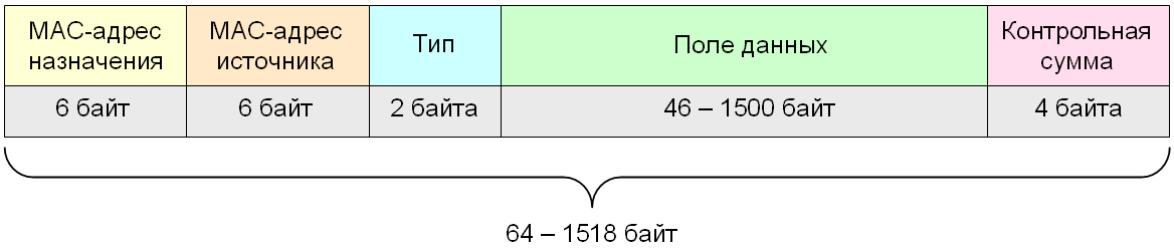


Рисунок 20 – Формат кадра Ethernet

Последние 4 байта кадра занимает контрольная сумма, которая используется для проверки целостности кадра. Если выявлена ошибка, кадр отбрасывается. Никаких запросов повторной передачи не делается, решение этой задачи передано на верхние уровни.

Принимающее устройство сравнивает MAC-адрес назначения со своим. В случае совпадения содержимое поля данных (пакет) передается на сетевой уровень. Если в качестве адреса назначения указан MAC-адрес FFFF.FFFF.FFFF (это широковещательный адрес), то его обязаны обработать все узлы сети.

Стек TCP/IP

В настоящее время стек (набор) протоколов TCP/IP является доминирующим как в глобальных, так и в локальных сетях. Набор протоколов TCP/IP является открытым стандартом, протоколы находятся в свободном доступе, и любой разработчик может их использовать в аппаратном или программном обеспечении.

Сравнение моделей, а также наиболее распространенные протоколы стека показаны на рисунке 21.

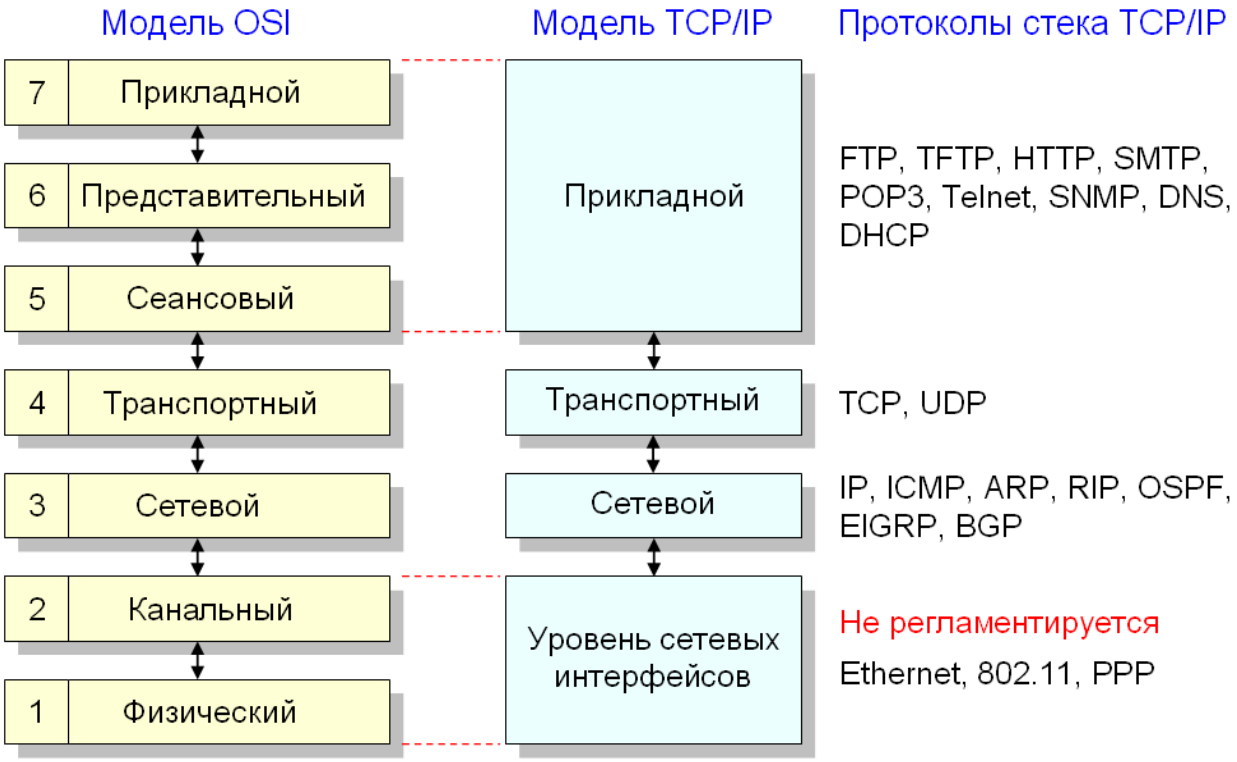


Рисунок 21 – Модели OSI и TCP/IP

Верхние три уровня в модели TCP/IP объединены, транспортный и сетевой уровень соответствует модели OSI. Уровень сетевых интерфейсов, охватывающий канальный и физический уровни, моделью TCP/IP не регламентируются. Таким образом, набор TCP/IP может работать поверх любой сетевой технологии.

Несмотря на справочный характер модели OSI, она является фундаментом, основой для понимания логики сетевого взаимодействия. В частности, для уточнения сетевых функций или при поиске и устранении неполадок в сети специалисты используют тот или иной номер уровня именно модели OSI. Например, кодирование битов данных для передачи по сетевой среде выполняется на 1-м (физическом) уровне. Формирование кадров, обеспечение доступа к среде передачи и обнаружение ошибок описано на 2-м (канальном) уровне и т.д.

Рассмотрим подробнее функции и протоколы сетевого уровня.

Сетевой уровень (как и канальный) отвечает за доставку данных с устройства-источника на устройство назначения. На канальном уровне для этого используются MAC-адреса, однако эти адреса подходят только для доставки кадра в пределах той же сети. Для обеспечения доступа в другие сети потребовалось создать дополнительную логическую систему адресации. Более того, чтобы добраться до устройства назначения может потребоваться преодолеть несколько транзитных сетей. Это значит, необходимо сформировать маршрут в сеть назначения. Таким образом, сетевой уровень отвечает за доставку данных в сложной составной сети, он имеет дело с передачей данных по всему пути от одного конца до другого.

Основным протоколом сетевого уровня является протокол IP (Internet Protocol). Его главная задача – продвижение пакета между сетями – от одного маршрутизатора к другому до тех пор, пока пакет не попадет в сеть назначения. Протокол IP является дейтаграммным, т.е. работающим без установления соединений по принципу доставки с максимальными усилиями. Почему разработчики стека сделали такой важный протокол ненадежным? Дело в том, что надежная передача требует высоких накладных расходов и необходима далеко не всегда. Поэтому задача обеспечения заданного уровня надежности возложена «на плечи» транспортного уровня.

На сетевом уровне формируется пакет, который затем передается на канальный уровень и инкапсулируется в кадр канального уровня. В качестве служебной информации в заголовке пакета указываются в частности:

- IP-адрес источника;
- IP-адрес назначения;
- время жизни пакета;
- приоритет;
- поля, связанные с фрагментацией.

Существуют две версии протокола: IP v.4 и IP v.6. Версия 6 была создана в 1996 г. как способ решения проблемы нехватки адресов IP v.4. Однако благодаря использованию бесклассовой адресации и применению техноло-

гии NAT (трансляция адресов) переход на 6-ю версию сильно затянулся. Поэтому обе версии сосуществуют.

IP v.4 использует 32-битный адрес, который чаще всего представляется в десятичном виде, например:

192.168.0.149

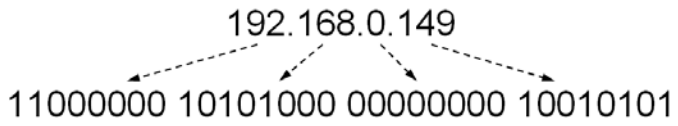
В IP v.6 используется 128-битный адрес, который обычно представляют в шестнадцатеричном формате, например:

2001:0DB8:000A:000B:0123:4567:89AB:CDEF

В рамках курса будут рассматриваться только адреса IP v.4.

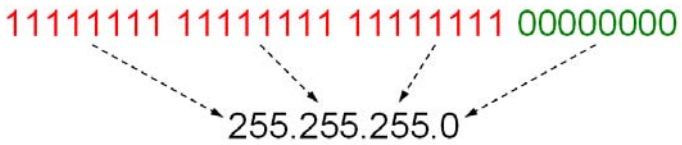
Итак, IP-адрес используется для доставки пакета от одного узла к другому не только в пределах одной сети, но и в сложной составной сети. Именно поэтому IP-адрес имеет иерархическую структуру. Его старшая часть (сетевая) отражает номер сети, а младшая (узловая) – номер узла в этой сети. Чтобы понять, где проходит «граница» между сетевой и узловой частью используется маска подсети (или длина префикса). Она указывается вместе с адресом. На самом деле и маска, и префикс указывают, сколько старших бит IP-адреса относятся к сетевой части адреса (т.е. определяют номер сети).

Вернемся к предыдущему примеру IP-адреса, но представим его в виде, понятном компьютеру, т.е. в двоичном формате:



Верхний вариант – удобный для человека способ представления, причем переход к десятичным числам сделан по октетам, что позволяет лучше запоминать адреса и быстрее решать задачи.

Теперь нужно просто указать, какое количество бит в старшей части адреса образуют его сетевую часть. Если, например, под сетевую часть отдано 24 бита, то в маске нужно указать сначала 24 единицы, а потом 8 нулей:



Маску можно представить компактно в виде длины префикса, т.е. просто указать количество единиц (ведь они всегда справа). В нашем примере в маске 24 единицы, поэтому запись примет вид:

192.168.0.149/24

В маске могут быть все нули и даже все единицы, т.е. 32 варианта, но чаще всего мы используем «простые» маски, соответствующие префиксам «/8», «/16» и «/24». Тогда при решении задач не требуется переходить в двоичную систему. Разумеется, сетевые инженеры должны уметь решать задачи с любыми масками.

Когда известен IP-адрес и маска подсети (или длина префикса), можно дать этой сети полную характеристику:

1. Размер сети – определяется количеством двоичных разрядов, относящихся к узловой части адреса (количество нулей в двоичной маске). В нашем примере в маске 8 нулей, т.е. узловую часть адреса образует один октет. Следовательно:

$$\text{Размер сети} = 2^8 = 256$$

   Таким образом, нашей сети принадлежит 256 адресов.
2. Номер сети – это самый первый IP-адрес в сети, т.е. в узловой части все разряды нулевые. Математически это получается поразрядным умножением двоичного адреса на двоичную маску («наложением» маски). В нашем примере:

$$\text{Номер сети} = 192.168.0.0$$

3. Широковещательный адрес сети – это последний IP-адрес сети (когда в узловой части – все единицы). В нашем примере:

$$\text{Широковещательный адрес} = 192.168.0.255$$

4. Диапазон адресов, доступный для назначения узлам сети, всегда на 2 меньше размера сети, поскольку номер сети и широковещательный адрес присваивать узлам нельзя. Таким образом, узлы нашей сети должны получать IP-адреса из диапазона:

$$192.168.0.1 \ldots 192.168.0.254$$

Сетевые интерфейсы всех оконечных устройств сети должны быть сконфигурированы – им назначается IP-адрес и маска подсети. Это делается либо вручную, либо автоматически (если сеть обслуживает сервер DHCP). Пример ручной настройки представлен на рисунке 22.

Кроме оконечных устройств IP-адреса также должны получить интерфейсы маршрутизаторов, ведь именно маршрутизаторы связывают сети. В настройках сетевого интерфейса на рисунке задан адрес основного шлюза. Если шлюз не указан, то отправить пакет в другую сеть не удастся.

На сетевом уровне стека TCP/IP также функционируют протоколы маршрутизации. В качестве примеров на рисунке 21 были представлены протоколы RIP, EIGRP, OSPF и BGP. Основные принципы функционирования маршрутизаторов рассмотрим в следующем параграфе.

Протокол ARP (Address Resolution Protocol) необходим для преобразования IP-адреса в MAC-адрес, чтобы сформировать кадр Ethernet. Для передачи сообщений об ошибках и выполнения некоторых служебных функция используется протокол ICMP (Internet Control Message Protocol).

На *транспортном уровне* стека TCP/IP используются только два протокола: TCP и UDP.

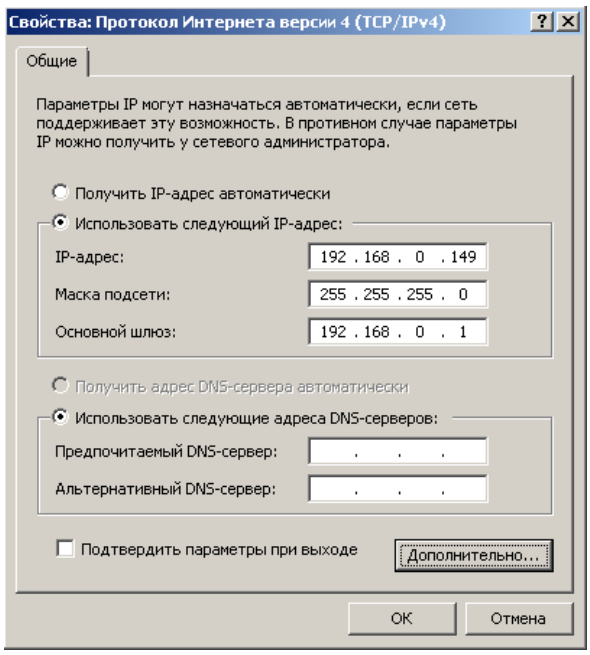


Рисунок 22 – Пример настройки сетевого интерфейса в ОС Windows

UDP (User Datagram Protocol) – дейтаграммный протокол, реализующий ненадежный сервис по возможности, который не гарантирует доставку сообщений адресату. Функции протокола сводятся к простой передаче данных и диагностике (но не исправлении) ошибок. Поврежденные дейтаграммы просто отбрасываются. Каждая дейтаграмма переносит отдельное пользовательское сообщение.

Таким образом, UDP гарантирует только целостность, но не гарантирует доставку и порядок следования дейтаграмм. Есть приложения, для которых потеря некоторых данных во время передачи по сети допускается, но при этом задержки передачи недопустимы. Таким приложениям лучше использовать протокол UDP, поскольку он требует меньших накладных расходов. Протокол UDP более предпочтителен для потокового воспроизведения аудио, видео и передачи голосовой информации в режиме реального времени по протоколу IP (VoIP). Пересылка подтверждений и повторная передача могут замедлить доставку данных.

Протокол TCP (Transmission Control Protocol) предназначен для надежной передачи данных между приложениями. Работа протокола основана на логическом соединении. Это позволяет обеспечивать гарантированную доставку данных, несмотря на то, что для этого используется ненадежный протокол IP. Логическое соединение дает возможность следить за тем, чтобы данные не были потеряны, искажены или продублированы, а также чтобы они пришли к получателю в том порядке, в котором были отправлены. Принятая информация квитируется получателем. Однако подтверждать квитанцией каждый принятый сегмент – неэффективно, поэтому стороны договариваются о «размере окна», т.е. о количестве байт, которые можно передать без подтверждения.

Таким образом, TCP гарантирует доставку, целостность и порядок следования данных, но потребляет больше ресурсов. Таким приложениям, как

базы данных, web-браузеры и почтовые клиенты, необходимо, чтобы данные передавались без ошибок. Повреждение данных не допускается. Поэтому эти приложения разрабатывались исключительно для работы по протоколу TCP.

Рисунок 23 демонстрирует названия протокольных единиц, а также логику работы стека. Прикладные протоколы формируют сообщения либо поток данных и передают их на транспортный уровень. Протокол TCP буферизует поток и делит его на сегменты, которые инкапсулируются в пакеты протокола IP. Протокол UDP помещает сообщение в дейтаграмму и также инкапсулирует ее в IP-пакет. На уровне сетевых интерфейсов (на канальном уровне) IP-пакеты инкапсулируются в кадры Ethernet, а затем передаются по линиям связи.

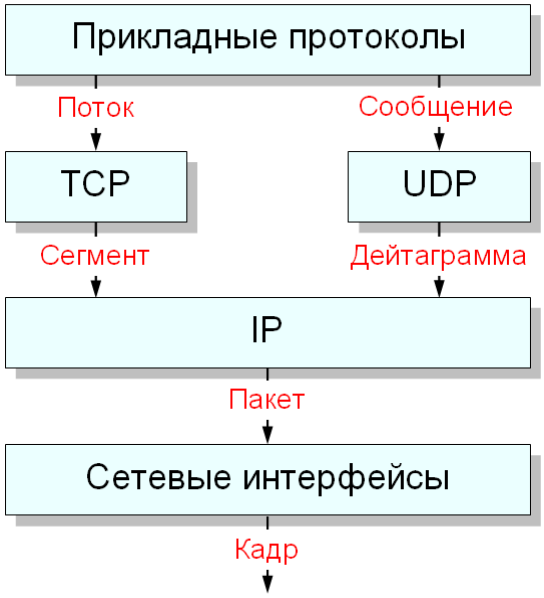


Рисунок 23 – Единицы данных в стеке TCP/IP

Промежуточные устройства. Коммутаторы, маршрутизаторы

Для подключения оконечных устройств к проводной сети обычно используются коммутаторы. На рисунке 24 в качестве примера представлен популярный коммутатор корпоративного класса Cisco Catalyst 2960. Это управляемый коммутатор, поддерживающий большое количество различных протоколов, однако, как и любой другой коммутатор, он готов выполнять свою основную функцию сразу после включения питания.

Рисунок 24 – Коммутатор Ethernet

Чтобы оконечные устройства, например компьютеры, могли начать информационный обмен, их сетевые интерфейсы соединить с портами коммутатора кабелем Ethernet.

Коммутатор самообучающееся устройство. Он самостоятельно формирует таблицу MAC-адресов, в которой указывается, какой MAC-адрес имеет интерфейс, подключенный к соответствующему порту. В результате кадры передаются только в порт назначения.

На рисунке 25 показана сеть на основе коммутатора, который уже сформировал таблицу MAC-адресов. Если узел не будет проявлять активность в течение 5 минут, динамическая запись о его MAC-адресе будет удалена, но после первого переданного кадра она восстановится. Если в таблице нет записи об адресате, кадр будет передан на все активные порты.

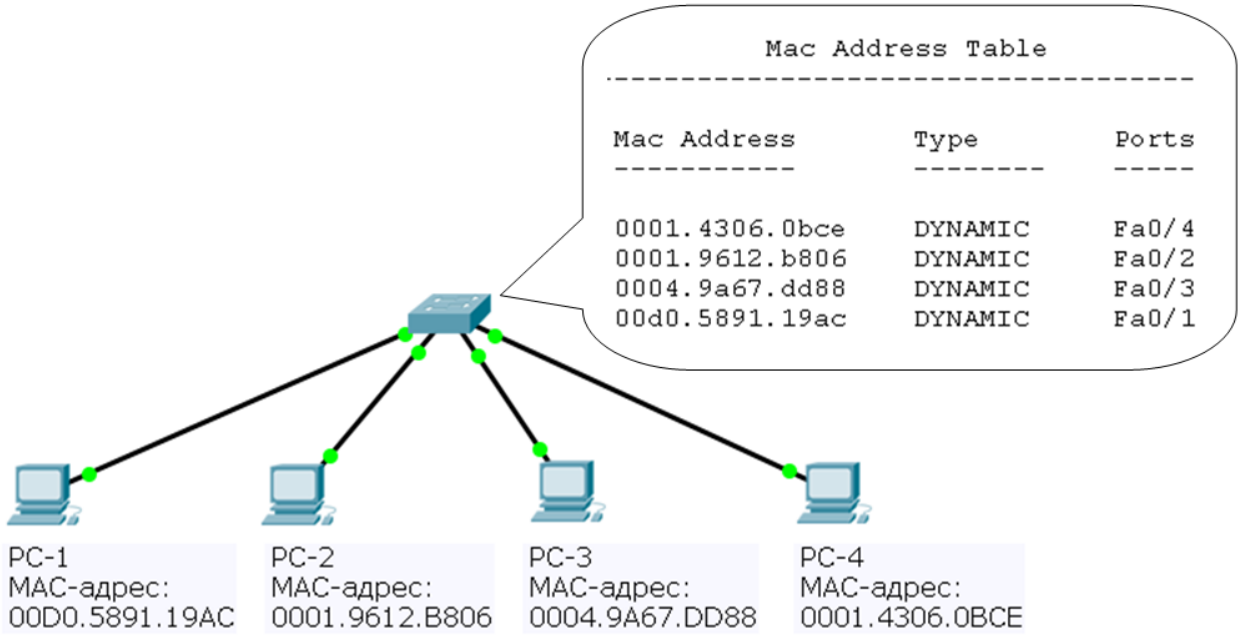


Рисунок 25 – Сеть Ethernet на основе коммутатора

Чтобы обмениваться информацией с узлами другой сети, потребуется устройство 3-го уровня – маршрутизатор. На рисунке 26 представлен популярный модульный маршрутизатор Cisco 1941. С помощью дополнительных модулей можно увеличить количество интерфейсов.

Рисунок 26 – Маршрутизатор

Каждый интерфейс маршрутизатора подключается к соответствующей сети, на этих интерфейсах настраиваются IP-адреса и маски подсети. Затем на каждом узле в настройках сети указывается основной шлюз.

На рисунке 27 показан пример взаимодействия двух локальных сетей. Интерфейсу маршрутизатора можно назначить любой свободный IP-адрес сети, к которой его подключают, но администраторы часто выбирают либо первый (как на схеме), либо последний.

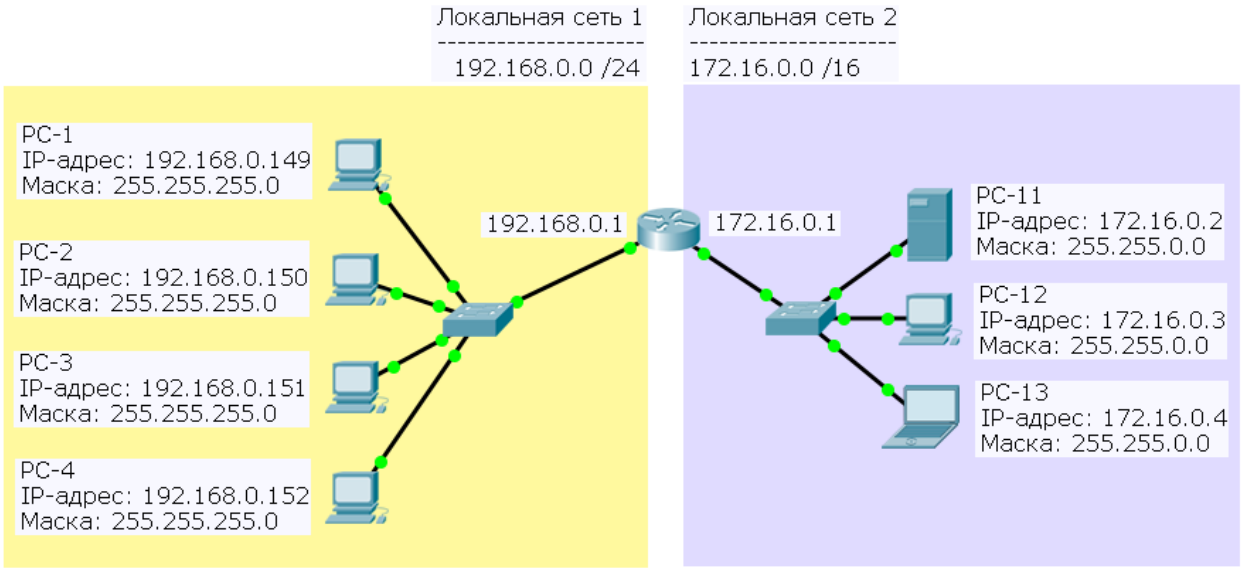


Рисунок 27 – Маршрутизатор связывает две локальные сети

Чтобы передать информацию другому узлу, необходимо знать его IP-адрес. Каждый раз при подготовке пакета к передаче на сетевом уровне определяется необходимость маршрутизации. Возможны два варианта:

1) Если IP-адрес назначения принадлежит сети источника, то маршрутизация не требуется. В этом случае вызывается протокол ARP, который отправляет широковещательный запрос для определения MAC-адреса узла, которому принадлежит IP-адрес назначения. Широковещательный кадр принимают все узлы в пределах локальной сети (маршрутизатор не пропускает широковещание в соседние сети), но ответит на запрос только один узел (если существует) – он отправит свой MAC-адрес. Теперь, когда передающий узел знает MAC-адрес узла назначения, он может инкапсулировать пакет в кадр и отправить его.
2) Если IP-адрес назначения не принадлежит сети источника, то маршрутизация нужна. В этом случае тоже вызывается протокол ARP. Он отправляет широковещательный запрос для определения MAC-адреса интерфейса с IP-адресом основного шлюза (вот зачем его нужно указывать в настройках сети). Широковещательный кадр принимают все узлы в пределах локальной сети, но ответит на запрос интерфейс основного шлюза – он отправит свой MAC-адрес. Передающий узел инкапсулирует пакет в кадр, у которого в качестве MAC-адреса назначения указывается MAC-адрес основного шлюза. Поскольку кадр адресован шлюзу, тот его получает и «извлекает» пакет. В заголовке пакета указан IP-адрес узла назначения. Если

Каким образом маршрутизатор «узнаёт» о других сетях?

В нашем примере только две сети, они непосредственно подключены к маршрутизатору, поэтому он узнает про них в тот момент, когда будут настроены его интерфейсы. Эти сети автоматически добавятся в таблицу маршрутизации.

Как только инфраструктура сети усложнится, даже если просто появится транзитная сеть как на рисунке 28, необходимо настраивать маршрутизацию. Либо статическую, либо динамическую.

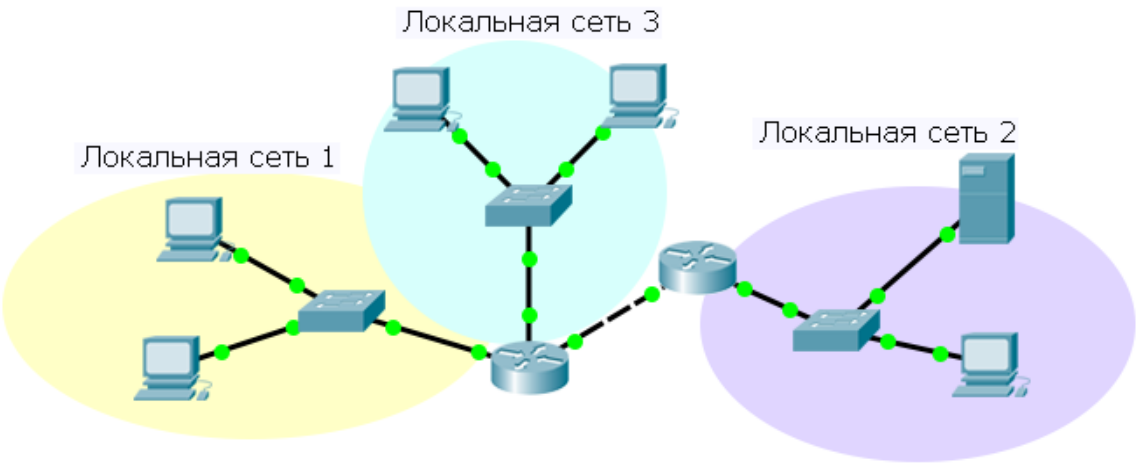


Рисунок 28 – Необходимость настройки маршрутизации

Статические маршруты настраиваются вручную. Подходящий вариант для небольшой сети со стабильной структурой. Для средних и больших сетей динамическая маршрутизация предпочтительнее. Нужно выбрать один из протоколов маршрутизации (например, RIP, EIGRP, OSPF), который поддерживается маршрутизаторами, включить его и выполнить определенные настройки на каждом маршрутизаторе. Изучение протоколов маршрутизации выходит за рамки курса.

Сетевые службы

Для конечного пользователя компьютерная сеть – это, прежде всего, тот набор сетевых служб, с помощью которых он может решать поставленные задачи. Например, получить доступ к информационным ресурсам предприятия, подготовить документ и распечатать его на удаленном принтере, отправить сообщение по электронной почте, найти нужную информацию в интернете, принять участие в видеоконференции и т.д. Совокупность предоставляемых сетевых служб, их возможности, параметры и безопасность определяется характером решаемых задач.

Чтобы обеспечить эффективную и безопасную работу пользователей, а также правильное и надежное функционирование всей сетевой инфраструктуры предприятия, используются административные службы. Это управле-

ние учетными записями пользователей, службы каталогов, системы мониторинга и анализа трафика и др.

Сетевые службы реализуются программными средствами. Базовые службы (такие как файловая служба, служба печати и др.) предоставляются сетевой операционной системой, прикладные – сетевыми приложениями, программами и утилитами, работающими под управлением сетевой ОС.

Для понимания принципов работы сетевой службы необходимо определить понятия «клиент» и «сервер».

Клиент – это модуль, предназначенный для формирования и передачи сообщений-запросов к ресурсам удаленного компьютера от разных приложений с последующим приемом результатов из сети и передачей их соответствующим приложениям.

Сервер – модуль, который ожидает запросов клиентов из сети, а приняв запрос, пытается его обслужить. Один сервер может обслуживать запросы сразу нескольких клиентов.

Пара «клиент-сервер», предоставляющая доступ к конкретному типу ресурса компьютера через сеть, образует сетевую службу.

В данном параграфе рассмотрим работу двух основных инфраструктурных сетевых служб: динамического назначения IP-адресов (DHCP) и разрешения имен (DNS).

Служба DHCP (Dynamic Host Configuration Protocol).

Настройку сетевых параметров оконечных устройств в сети можно выполнять вручную. В небольшой сети обычно так и поступают. Но в крупных сетях процесс автоматизируют путем развертывания одного или нескольких DHCP-серверов.

Чтобы DHCP-сервер начал обслуживать клиентов, т.е. передавать им конфигурационную информацию, необходимо настроить хотя бы одну область. Области нужно назначить:

- имя;
- начальный IP-адрес;
- конечный IP-адрес;
- маску подсети;
- IP-адрес основного шлюза;
- IP-адрес сервера DNS;
- исключаемый диапазон адресов (если необходимо);
- срок аренды.

Также можно настроить резервирование, когда за клиентом с определенным MAC-адресом сетевого интерфейса закрепляется конкретный IP-адрес.

DHCP-сервер можно настроить на компьютере с серверной ОС, например, Microsoft Windows Server. В большинстве домашних беспроводных маршрутизаторов эта возможность тоже реализована.

Рассмотрим порядок взаимодействия клиента и сервера DHCP. Пусть компьютер пользователя настроен на автоматическое получение настроек протокола IP. В сети существует один или несколько серверов DHCP.

1. Клиент отправляет широковещательный запрос DHCPDISCOVER с целью идентификации всех доступных DHCP-серверов в сети.
2. Сервер DHCP отвечает сообщением предложения DHCPOFFER, в котором клиенту предлагается IP-адрес, маска подсети, адреса основного шлюза и сервера DNS, а также указывается срок аренды.
3. Клиент может получить несколько предложений аренды, если в сети более одного сервера DHCP. В таком случае клиент выбирает одно из них и отправляет широковещательное сообщение с запросом DHCPREQUEST, где указывает конкретный сервер и принимаемое предложение аренды.
4. Выбранный сервер возвращает клиенту сообщение с подтверждением DHCPACK, что данный адрес предоставлен клиенту.

Служба DNS (Domain Name System).

Компьютеры и другие сетевые устройства взаимодействуют, используя IP-адреса. Однако пользователям гораздо удобнее обращаться к ресурсам сети используя символьные, а не числовые адреса. Для реализации этого удобства в стеке TCP/IP в дополнение к сетевым адресам была создана символьная система адресов – система доменных имен (DNS). Одновременно с этим должен существовать механизм сопоставления доменного имени и IP-адреса, т.е. служба DNS.

Система иерархическая древовидная с одним корнем. Корень обозначается точкой. Иерархия доменов похожа на иерархию папок в файловой системе. Однако имя файла (полный путь) начинается со старшей части (буква диска), а здесь от младшей к корню. Составные части имени (домены) отделяются друг от друга точками (рис. 29).

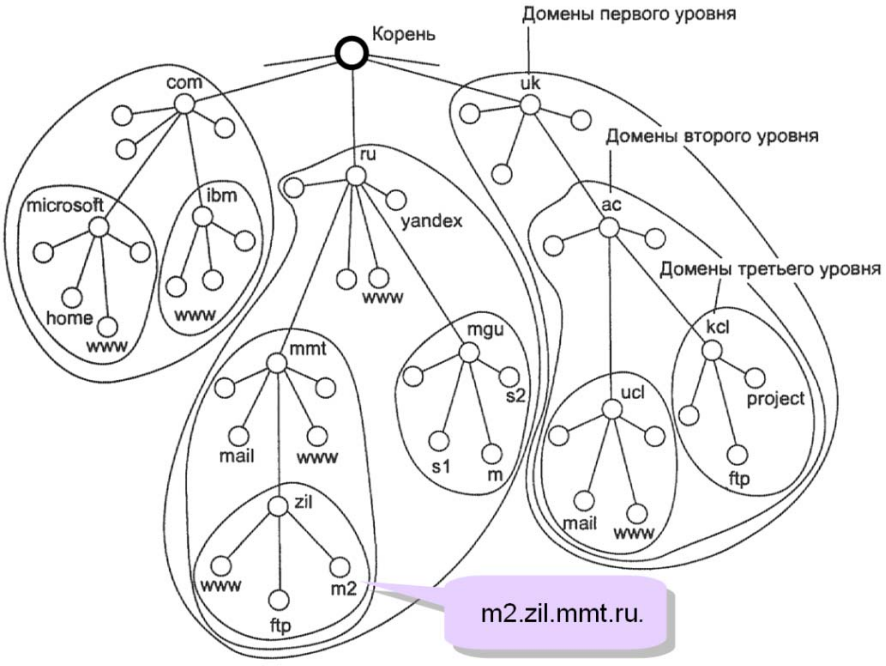


Рисунок 29 – Пространство доменных имен

Например, в полном доменном имени «m2.zil.mmt.ru.» «m2» – имя узла в домене «zil», который является поддоменом домена «mmt». Точка в конце имени означает корень.

Разделение имени на части позволяет разделить административную ответственность за уникальность имен в домене.

Корневой домен управляется центральными органами интернета. Корневые сервера хранят информацию о серверах имен, обслуживающих домены первого (верхнего) уровня. Домены верхнего уровня назначаются для каждой страны, а также для различных типов организаций (рис. 30).

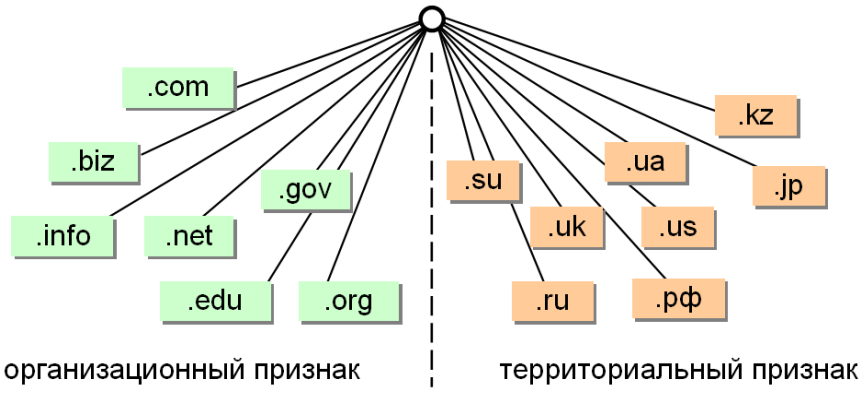


Рисунок 30 – Домены верхнего уровня

Служба DNS состоит из трех компонент:

1. Пространство имен DNS и соответствующие ресурсные записи – это сама распределенная база данных DNS.
2. Серверы имен DNS – компьютеры, хранящие базу данных DNS и отвечающие на запросы DNS-клиентов.
3. DNS-клиенты – компьютеры, посылающие запросы серверам DNS для получения ресурсных записей.

На рисунке 31 представлен фрагмент типичной базы данных домена «example.com» на DNS-сервере.

Название	Тип	Значение
@	SOA	ns1.example.com, admin.example.com [4563] ; serial number 900 ; refresh 600 ; retry 86400 ; expire 3600 ; minimum TTL
@	NS	ns1.example.com.
ns1	A	192.168.1.10
alex	A	192.168.1.25
katia	A	172.16.45.67
petia	A	10.33.55.77
srv	A	10.22.33.44
www	CNAME	srv.example.com.
ftp	CNAME	srv.example.com.
…	…	…

Рисунок 31 – Фрагмент базы данных сервера DNS

Первая запись – начальная запись зоны (SOA, Start of Authority) – в ней указываются различные служебные параметры. Записи типа «NS» описывают сервера имен, обслуживающие данный домен. Основные ресурсные записи – это записи типа «A». Именно они отображают соответствия имен узлов и IP-адресов. Записи типа «CNAME» (canonical name) позволяют указать псевдонимы.

Рассмотрим общий алгоритм разрешения имен (рис. 32). Обычно используется рекурсивная процедура, в которой активную роль играет сервер имен домена, к которому принадлежит имя клиента.

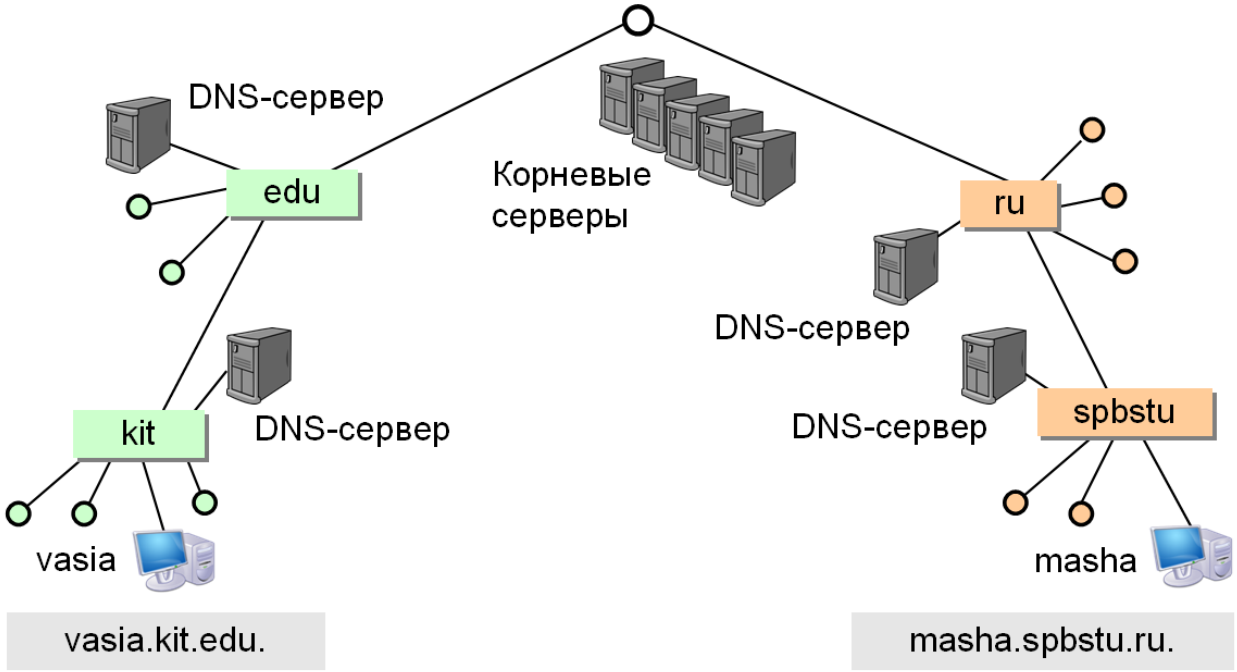


Рисунок 32 – Алгоритм разрешения доменных имен

Предположим, узел «vasia» хочет отправить сообщение узлу «masha», причем пользователь узла «vasia» не знает IP-адреса узла «masha», но знает его полное доменное имя. В настройках протокола IP на узле «vasia» указан DNS-сервер домена «kit». Именно ему будет направлен запрос для разрешения доменного имени «masha.spbstu.ru.» в IP-адрес. Сервер DNS домена «kit» не содержит соответствующих ресурсных записей, поэтому он обращается к корневым серверам. На корневых серверах тоже нет информации об IP-адресе узла «masha.spbstu.ru.», однако корень знает IP-адрес DNS-сервера домена «ru» и возвращает его. Теперь сервер DNS домена «kit» обращается к серверу DNS домена «ru», от которого удается получить только IP-адрес сервера имен домена «spbstu». На DNS-сервере домена «spbstu» есть искомая ресурсная запись. Сервер DNS домена «kit» получает ее и передает узлу «vasia». Теперь «vasia» знает IP-адрес узла «masha» и может отправить пакет. Следует отметить, что полученная информация о соответствии имени и IP-адреса кэшируется и сервером DNS, и клиентом, поэтому при передаче следующего пакета узлу «masha» длинная рекурсивная процедура не потребуется.

Вопросы для самопроверки

1) Какой уровень модели OSI обеспечивает надежную передачу данных по физическому каналу?
2) На какой скорости можно передавать информацию в сети Fast Ethernet?
3) Какие уровни модели OSI совпадают с моделью TCP/IP?
4) Какая служебная информация указывается в заголовке IP-пакета?
5) Какими способами можно назначить IP-адрес узлу?
6) Какие протоколы реализуют транспортный уровень стека TCP/IP?
7) Сколько времени хранится динамическая запись в таблице MAC-адресов коммутатора?
8) Какова разрядность IP-адреса версии 6?

Практическое занятие №1
Создание локальной сети. Первичные настройки коммутатора

Задача 1. Простейшая сеть из двух компьютеров

На панели выбора типа устройства (слева внизу) нужно отметить категорию «End Devices» (оконечные устройства), затем из области выбора конкретного устройства «перетянуть» на рабочее поле два компьютера (PC), или компьютер и сервер (Server), или компьютер и лэптоп (Laptop).

Создать простейшую сеть из двух компьютеров можно без использования коммутатора или концентратора. Для непосредственного соединения узлов потребуется перекрестный медный кабель (Copper Cross-Over), который выбирается из категории «Connections» на панели выбора типа устройства. Кабель изображается черной пунктирной линией. Все современные сетевые адаптеры способны обеспечить взаимодействие непосредственно подключенных хостов даже при использовании стандартного прямого медного кабеля, однако Cisco Packet Tracer этого не позволяет. Перекрестный кабель используется также при соединении коммутаторов, маршрутизаторов и при непосредственном подключении компьютера к порту маршрутизатора.

Подсоединяется кабель к интерфейсам FastEthernet0. Если все сделано правильно, через несколько секунд (примерно через 20) после соединения на обоих концах линии связи появятся зеленые треугольники, которые означают, что порты подняты и на физическом уровне соединение установлено (рис. 33).

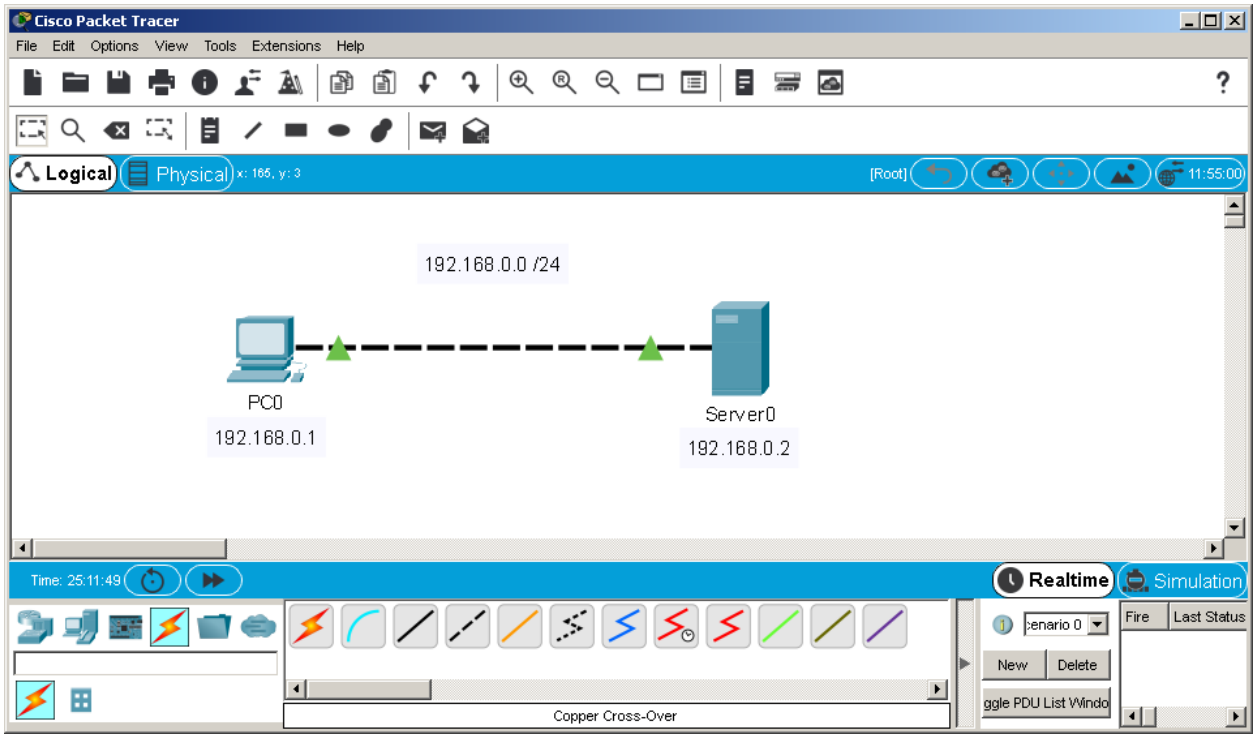


Рисунок 33 – Непосредственное соединение двух узлов

Но этого недостаточно. Чтобы компьютеры смогли передавать друг другу информацию, необходимо назначить IP-адреса сетевым интерфейсам.

Мы будем использовать первые два адреса сети 192.168.0.0 /24. Это показано на рабочем поле в форме заметок (Place Note).

Запись 192.168.0.0 /24 означает, что узлам сети можно назначить IP-адреса из диапазона 192.168.0.1 … 192.168.0.254. Маска подсети: 255.255.255.0. Номер сети: 192.168.0.0, а 192.168.0.255 – широковещательный адрес сети.

Конфигурирование протокола IP на компьютере, лэптопе, сервере и некоторых других оконечных устройствах осуществляется в окне программы «IP Configuration», ярлык которой находится на рабочем столе устройства. Чтобы открыть рабочий стол, нужно один раз щелкнуть левой кнопкой мыши на иконке устройства (например, PC0) и выбрать закладку «Desktop» (рис. 34).

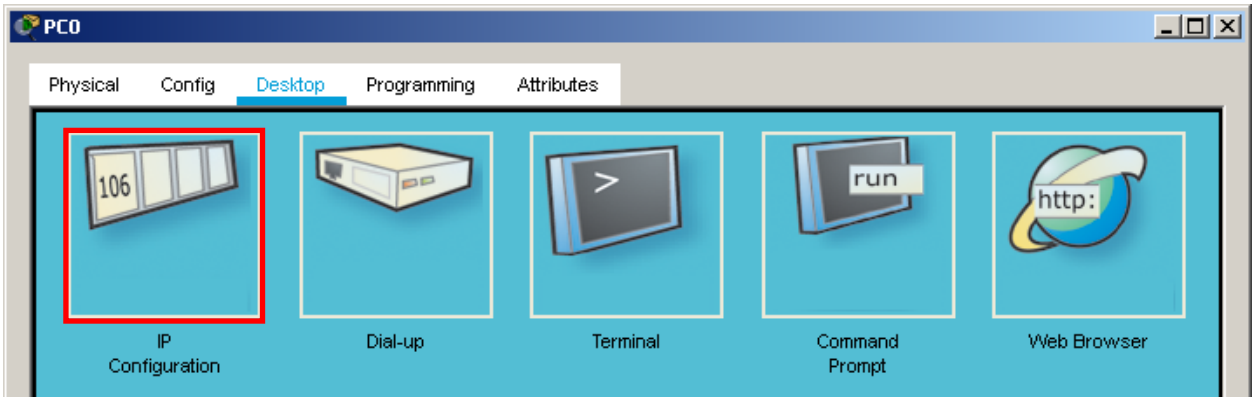


Рисунок 34 – Ярлык программы конфигурирования протокола IP на оконечном устройстве

В окне «IP Configuration» вводится IP-адрес и маска подсети (рис. 35). Другие параметры можно оставить без изменения, поскольку они не используются в этой задаче.

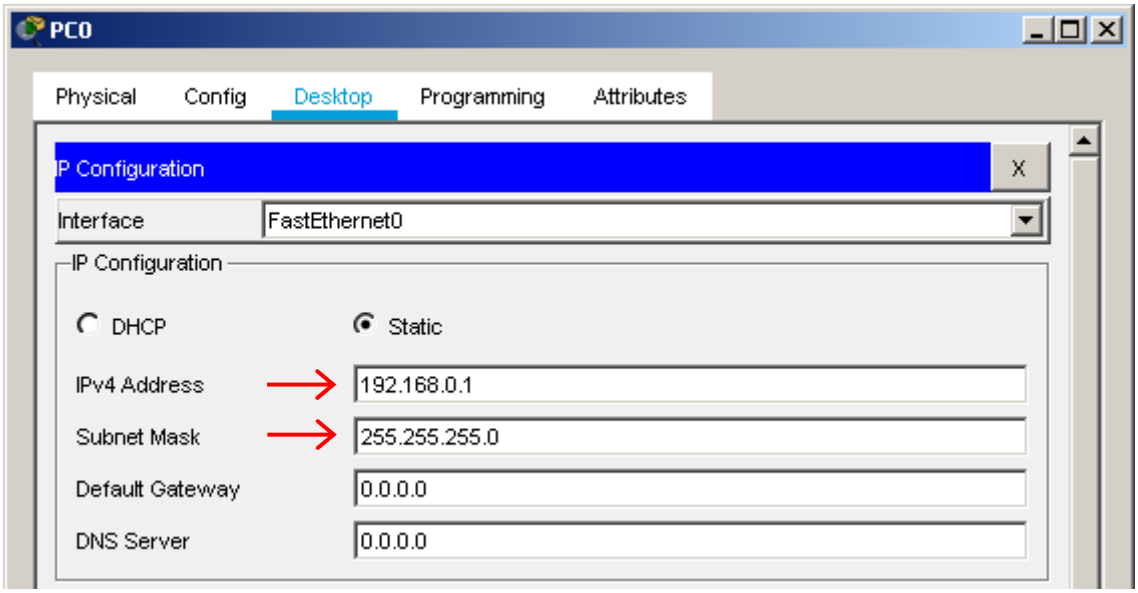


Рисунок 35 – Настройка протокола IP на оконечном устройстве

Когда сетевым интерфейсам обоих устройств назначены IP-адреса, можно проверить доступность. Это делается с помощью программы «ping». Запускается программа из командной строки. Для этого на рабочем столе узла (например, PC0) нужно открыть «Command Prompt» и ввести команду:

ping 192.168.0.2

Получение ответов означает, что проверка прошла успешно, и узлы могут обмениваться информацией по сети (рис. 36).

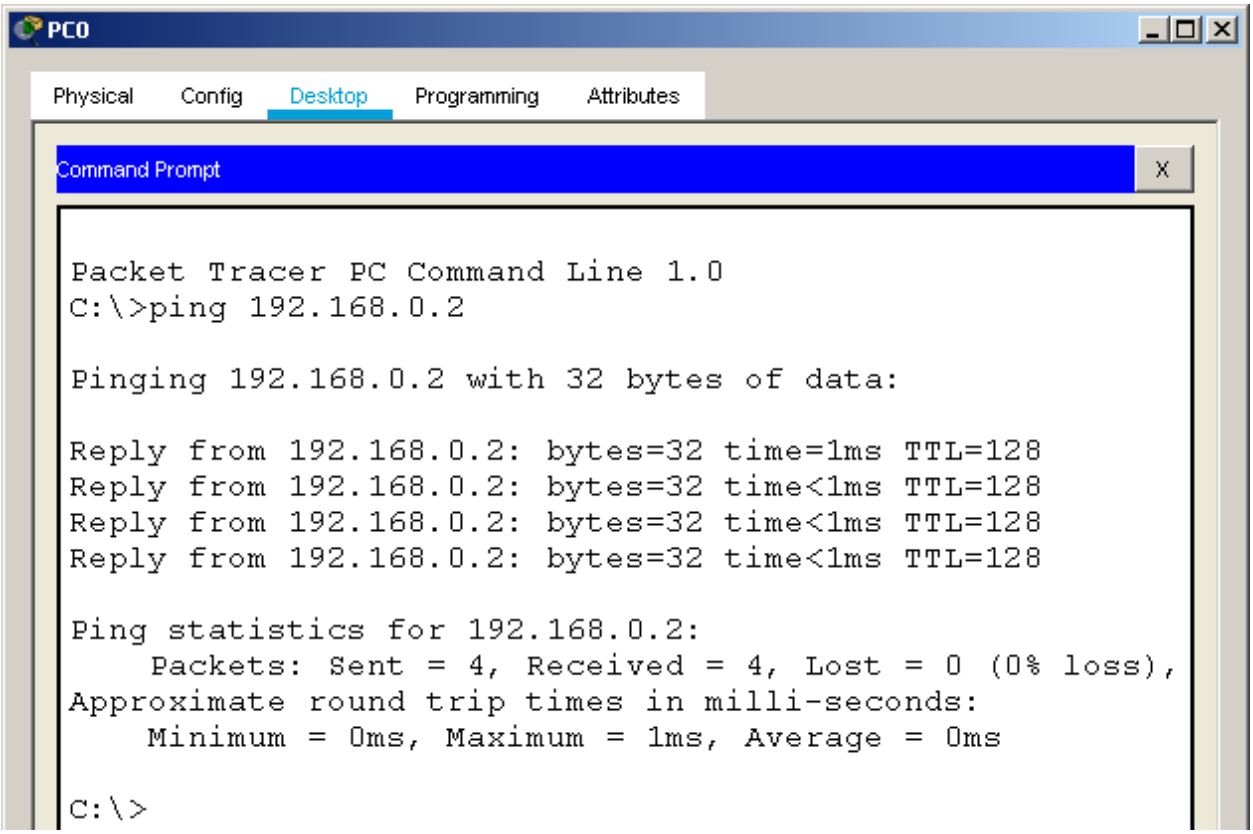


Рисунок 36 – Успешный результат проверки доступности узла сети

Таким образом, построена простейшая сеть из двух компьютеров, непосредственно соединенных перекрестным медным кабелем. Чтобы увеличить количество оконечных устройств в сети, потребуется коммутатор.

Задача 2. Создание простой сети на основе коммутатора Cisco

Для подключения оконечных устройств в компьютерных сетях используются коммутаторы. Одной из самых популярных серий коммутаторов Cisco является Catalyst 2960. Именно этот коммутатор будет использоваться на уровне доступа для решения большинства задач курса. Коммутатор Cisco 2960 имеет фиксированную конфигурацию (24 порта FastEthernet, 2 порта GigabitEthernet) и управляется операционной системой Cisco IOS.

Чтобы задействовать коммутатор для создания локальной сети, на панели выбора типа устройства (слева внизу) нужно отметить категорию «Network Devices» (сетевые устройства), затем чуть ниже – подкатегорию

«Switches» (коммутаторы), а потом из области выбора конкретного устройства «перетянуть» на рабочее поле коммутатор 2960 (рис. 37).

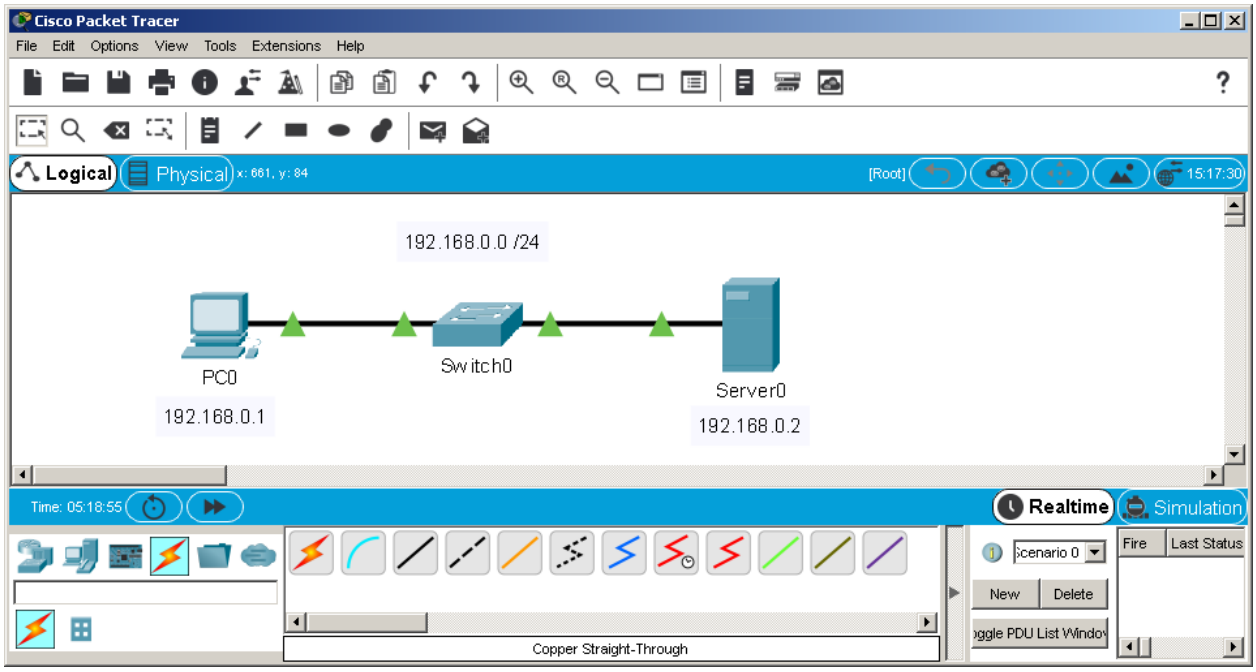


Рисунок 37 – Подключение узлов к коммутатору

Также на рабочем поле разместим два оконечных устройства, например, компьютер и сервер. Узлы подключаются к портам коммутатора прямым медным кабелем (Copper Straight-Through, изображается сплошной черной линией). Со стороны компьютера кабель подключается к интерфейсу FastEternet0, другой конец кабеля подключается к любому порту FastEthernet или GigabitEthernet коммутатора. Через несколько секунд после подключения на концах кабеля загорятся зеленые треугольные маркеры, показывающие, что на физическом уровне соединение установлено.

Если навести указатель мыши на коммутатор, появится всплывающая панель «Port Status Summary Table», на которой будет показано состояние каждого порта коммутатора и некоторые другие параметры (рис. 38).

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	1	--	0009.7C23.B301
FastEthernet0/2	Up	1	--	0009.7C23.B302
FastEthernet0/3	Up	1	--	0009.7C23.B303
FastEthernet0/4	Up	1	--	0009.7C23.B304
FastEthernet0/5	Down	1	--	0009.7C23.B305
FastEthernet0/6	Down	1	--	0009.7C23.B306
FastEthernet0/21	Down	1	--	0009.7C23.B315
FastEthernet0/22	Down	1	--	0009.7C23.B316
FastEthernet0/23	Down	1	--	0009.7C23.B317
FastEthernet0/24	Down	1	--	0009.7C23.B318
GigabitEthernet0/1	Down	1	--	0009.7C23.B319
GigabitEthernet0/2	Down	1	--	0009.7C23.B31A
Vlan1	Down	1	<not set>	00D0.58DD.390C

Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Рисунок 38 – Сводная информация о состоянии портов коммутатора

Компьютеры PC0 и Server0 подключены к портам FastEthernet 0/1 и 0/2. Коммутатор самостоятельно поднял эти порты, устройство готово к работе. Коммутаторы способны выполнять свою основную функцию без каких-либо настроек.

Компьютеры смогут передавать друг другу информацию только после назначения IP-адресов их сетевым интерфейсам. Мы опять будем использовать первые два адреса сети 192.168.0.0 /24, как и в Задаче №1.

Настроенные параметры протокола IP для всех сетевых интерфейсов компьютеров тоже отобразятся на всплывающей подсказке при наведении указателя мыши на оконечное устройство. На рисунке 39 показано, что интерфейсу FastEthernet0 узла PC0 задан IP-адрес и маска подсети.

```
Port            Link   IP Address       IPv6 Address                          MAC Address
FastEthernet0   Up     192.168.0.1/24   <not set>                             00D0.BCB8.0247
Bluetooth       Down   <not set>        <not set>                             00D0.BCC6.D8BC

Gateway:  <not set>
DNS Server:  <not set>
Line Number:  <not set>

Physical Location: Intercity, Home City, Corporate Office
```

Рисунок 39 – Информация о настройках сетевых интерфейсов компьютера

Для проверки связи между оконечными устройствами проводится эхо-тест. Команда «ping» сначала отправит эхо-запрос на заданный IP-адрес и, если узел доступен, получит эхо-ответ (рис. 36).

Добавим в сеть еще несколько оконечных устройств, например, лэптоп и принтер. Для этого также используется прямой медный кабель, который со стороны оконечного устройства подключается к порту FastEthernet0, а другой конец подсоединяется к любому свободному порту коммутатора, кроме «Console» (рис. 40).

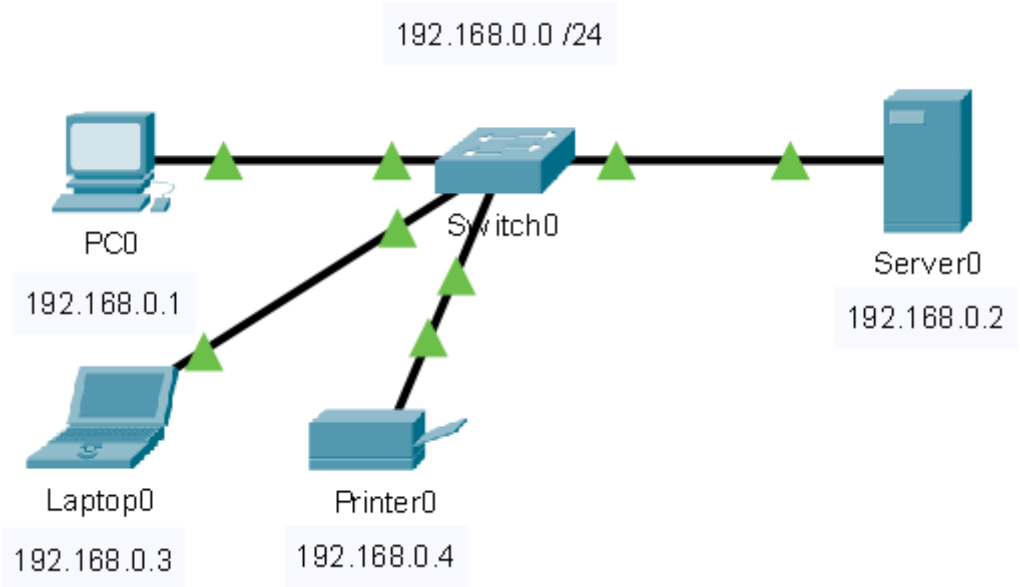


Рисунок 40 – Подключение к коммутатору новых оконечных устройств

IP-адрес и маска подсети назначается сетевому интерфейсу лэптопа в окне «IP Configuration», которое открывается через одноименный ярлык ра-

бочего стола (закладка «Desktop») оконечного устройства (рис. 34, 35). Можно использовать любой свободный IP-адрес нашей сети, например, 192.168.0.3 (маска подсети: 255.255.255.0).

Настройка параметров сетевого интерфейса принтера выполняется на закладке «Config» после выбора интерфейса «FastEthernet0». Все чекбоксы (Port Status и др.) должны быть отмечены (рис. 41).

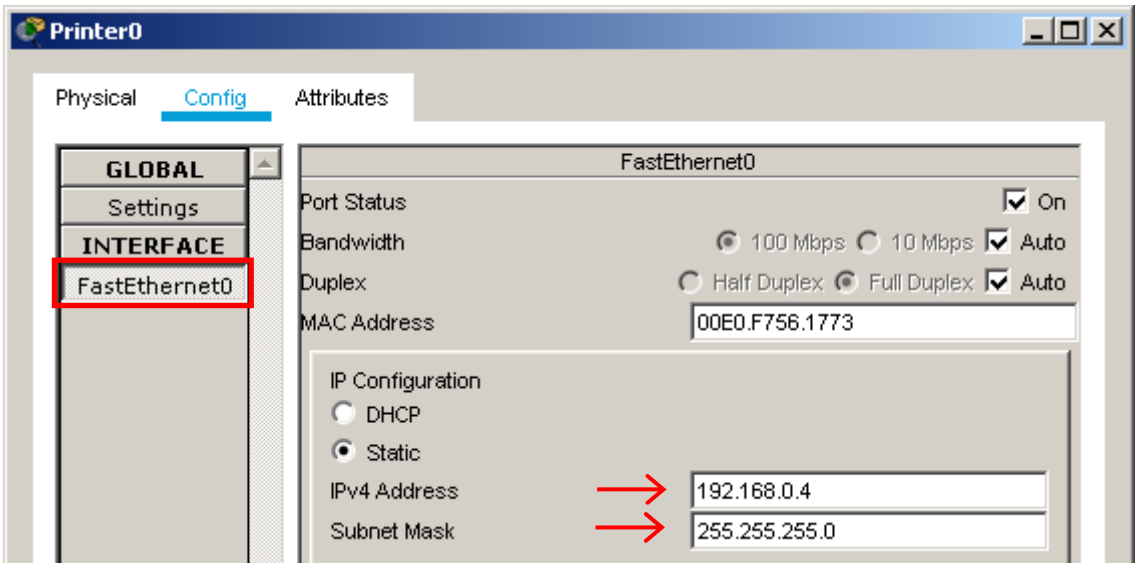


Рисунок 41 – Настройка сетевого интерфейса принтера

Для проверки доступности новых оконечных устройств сети используется эхо-тестирование. Например, чтобы проверить доступность сетевого принтера, в командной строке (Command Prompt) любого компьютера можно выполнить команду:

ping 192.168.0.4

Если эхо-ответы получены, устройства могут взаимодействовать друг с другом в сети.

Количество устройств в локальной сети не ограничено числом портов коммутатора. Размер сети можно увеличить. Для этого потребуется еще один коммутатор или даже несколько. Коммутатор соединяется с другим коммутатором перекрестным медным кабелем (Copper Cross-Over). Используются любые свободные порты (разумеется, кроме «Console»).

Добавим на рабочее поле второй коммутатор 2960 и персональный компьютер PC1. Соединим порты GigabitEthernet обоих коммутаторов перекрестным кабелем, а PC1 подключим к любому порту FastEthernet нового коммутатора Switch1 прямым медным кабелем (рис. 42). Чтобы PC1 мог взаимодействовать с другими оконечными устройствами, его сетевому интерфейсу FastEternet0 должен быть назначен IP-адрес из сети 192.168.0.0 /24. Это может быть любой свободный адрес, например, 192.168.0.5.

Использование двух или более коммутаторов позволяет увеличить размер (диаметр) сети и количество узлов. Однако надо понимать, что это одновременно приводит к увеличению широковещательного домена.

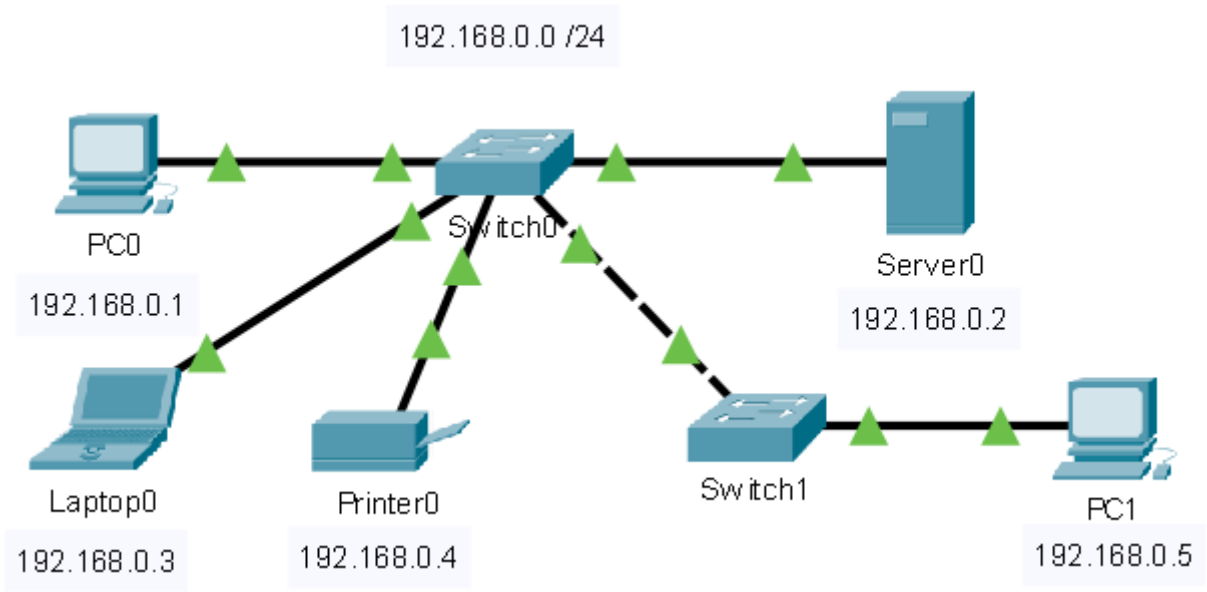


Рисунок 42 – Увеличение размера сети с помощью второго коммутатора

На сервере в Cisco Packet Tracer могут быть настроены различные сервисы. Некоторые из них уже включены по умолчанию, в частности, Web-сервер. Конфигурирование сервисов осуществляется на закладке «Services» (рис. 43).

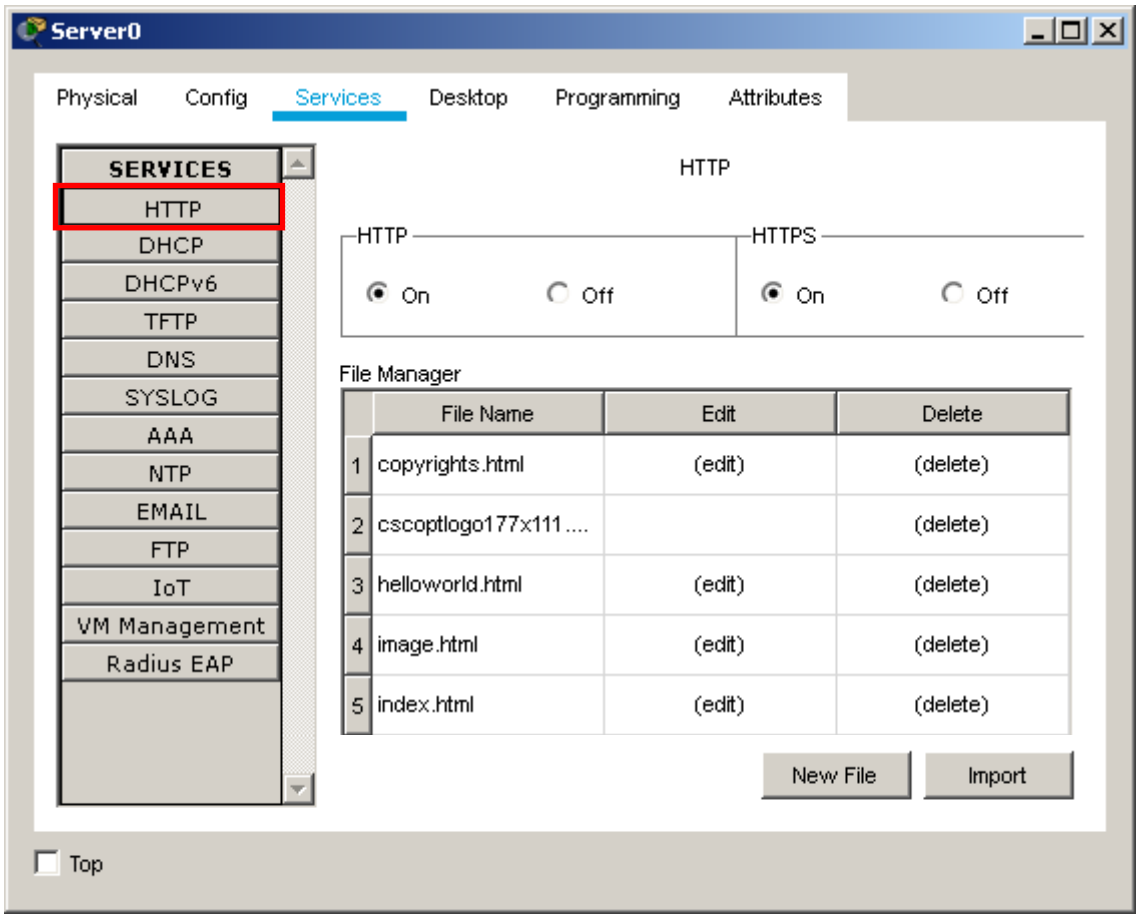


Рисунок 43 – Окно настройки Web-сервера

Сымитируем обращение к Web-серверу с какого-нибудь компьютера сети. Пусть это будет недавно добавленный PC1. Интернет-браузер запускается щелчком по соответствующему ярлыку на рабочем столе компьютера (закладка «Desktop») (рис. 44).

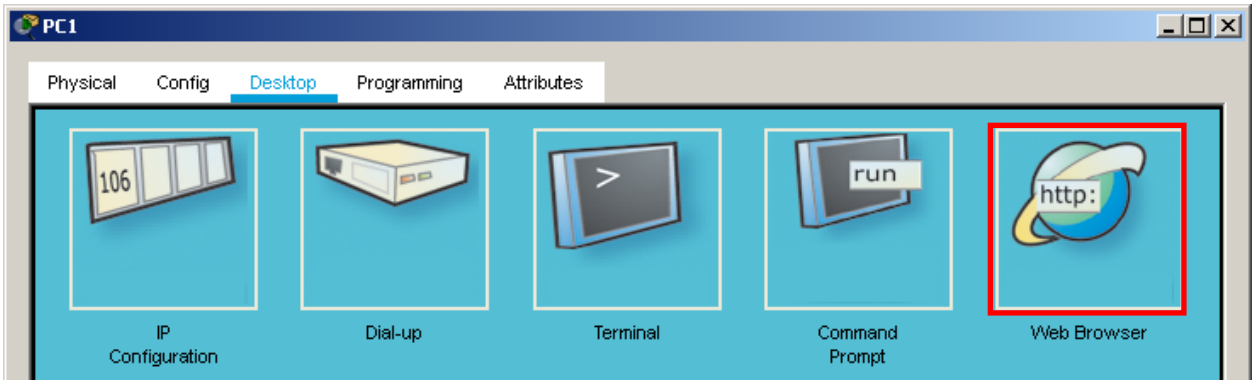


Рисунок 44 – Ярлык интернет-обозревателя

В адресной строке браузера вводим IP-адрес сервера: 192.168.0.2 и нажимаем «Go». Откроется домашняя страница сайта – страница index.html (рис. 45). Гиперссылки работают. В окне настроек Web-сервера (рис. 43) все страницы сайта можно редактировать, удалять, создавать новые или импортировать из локального компьютера.

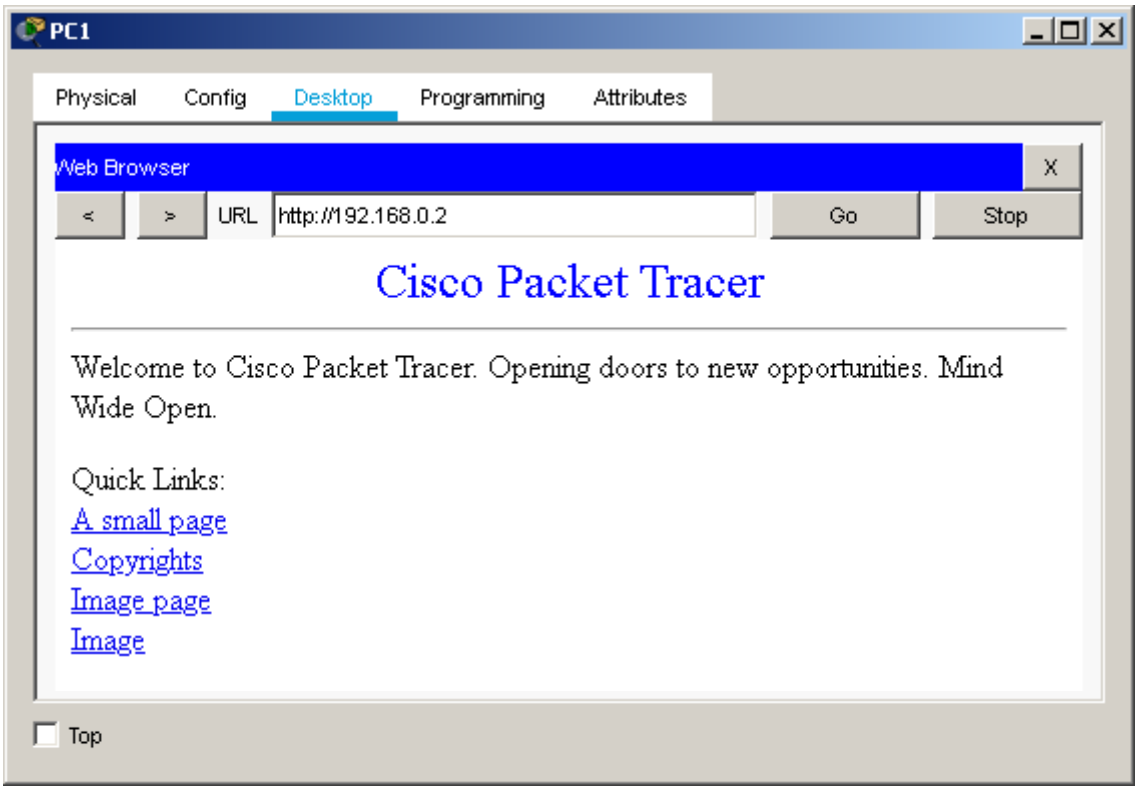


Рисунок 45 – Демонстрация доступности Web-сервера

Таким образом, построена простая изолированная локальная сеть на основе коммутатора.

Задача 3. Первичные настройки коммутатора Cisco

Использование коммутаторов Cisco в небольших домашних сетях или сетях малого офиса вряд ли можно считать экономически обоснованным, поскольку, скорее всего, многие возможности устройства просто останутся невостребованными. И хотя в учебных примерах не будут создаваться сложные сетевые инфраструктуры, реализацию некоторых функций, технологий и протоколов, используемых в корпоративных сетях, мы рассмотрим.

Сначала выполним первичные настройки коммутатора, закроем доступ неавторизованных пользователей и познакомимся с операционной системой Cisco IOS, которая управляет работой промежуточных устройств Cisco.

Существует два варианта доступа к операционной системе коммутатора или маршрутизатора:

- через консольный порт;
- удаленно (по протоколам Telnet, SSH, HTTPS).

Для подключения к консольному порту необходим специальный консольный кабель, который входит в комплектацию устройства Cisco. Один конец кабеля подключается к порту «Console» коммутатора, другой – к последовательному порту «RS 232» компьютера или лэптопа. В Cisco Packet Tracer консольный кабель изображается дугой голубого цвета (рис. 46).

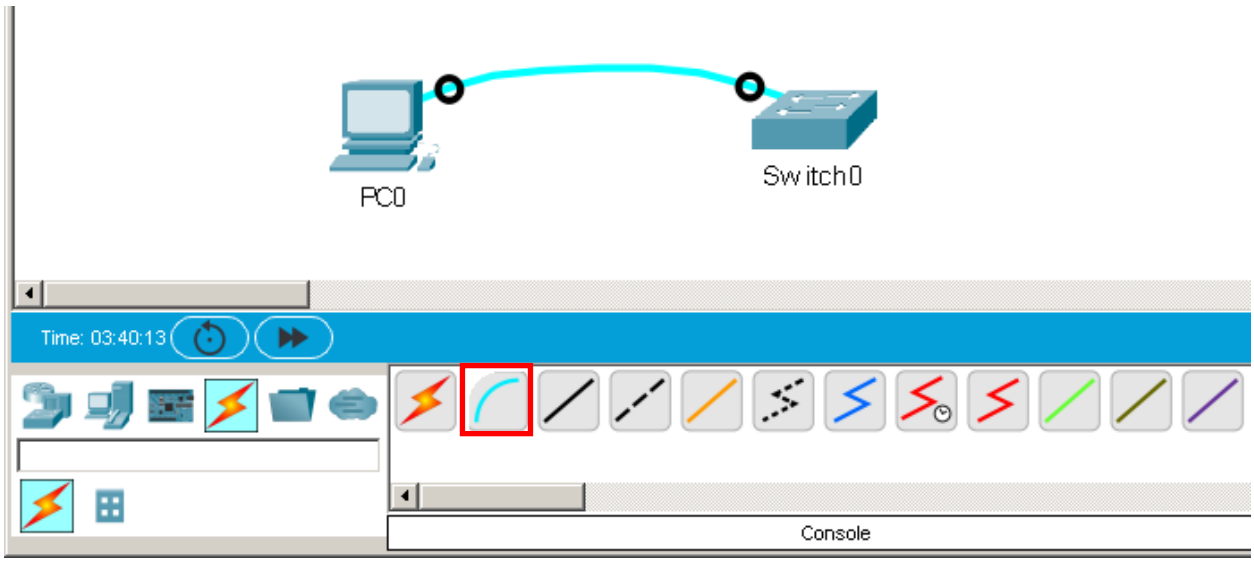


Рисунок 46 – Подключение компьютера к коммутатору консольным кабелем

Теперь на компьютере PC0 нужно запустить эмулятор терминала. Ярлык программы «Terminal» находится на рабочем столе компьютера (закладка «Desktop») (рис. 47). Эмулятор терминала обеспечивает доступ к интерфейсу командной строки (CLI – command-line interface) операционной системы Cisco IOS. Командная строка настолько удобна, что многие сетевые инженеры предпочитают использовать ее также для удаленного управления устройством, несмотря на возможность задействовать Web-интерфейс.

В среде Cisco Packet Tracer настройка коммутатора выполняется только через CLI.

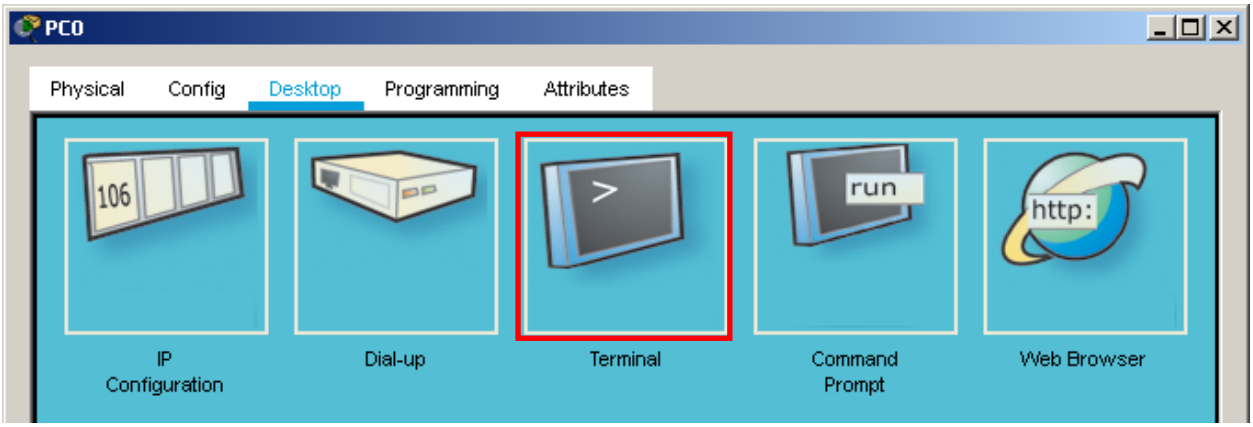


Рисунок 47 – Ярлык эмулятора терминала

Сначала программа предложит настроить параметры порта. Все настройки можно оставить по умолчанию и нажать «OK», чтобы открыть окно терминала (рис. 48).

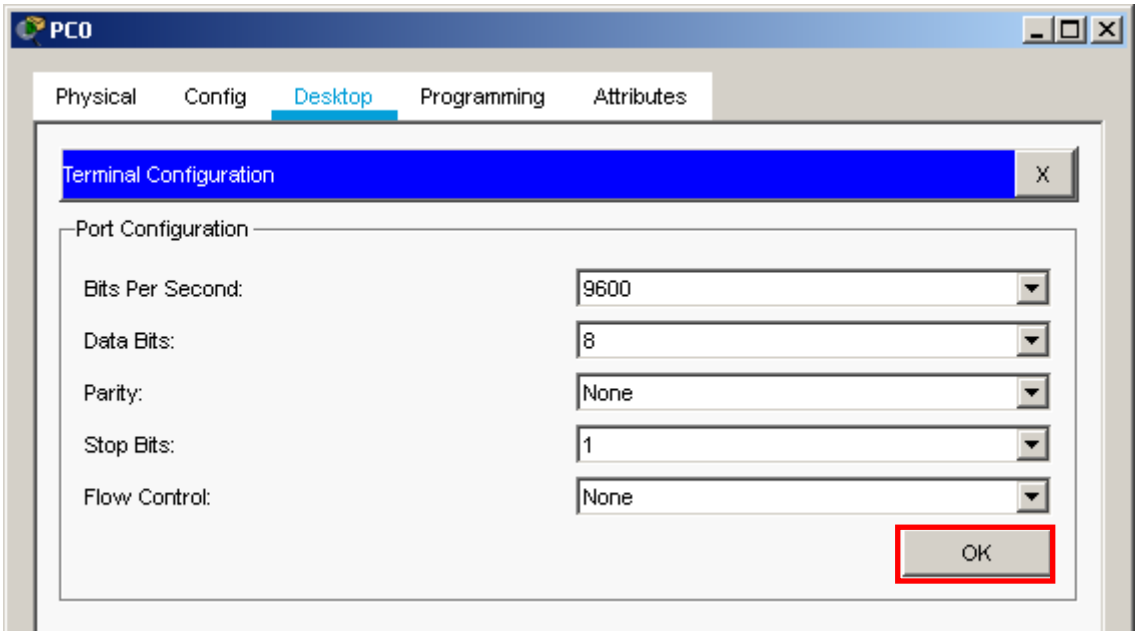


Рисунок 48 – Окно настройки параметров порта

Cisco IOS выводит в окно терминала служебную информацию, связанную с загрузкой устройства, и предлагает нажать кнопку «Enter» (Press RETURN to get started!), чтобы начать работу. После нажатия «Enter» появляется приглашение операционной системы (Switch>), командная строка готова к приему команд (рис. 49).

Перед тем как начать настраивать коммутатор нужно отметить несколько базовых моментов. По соображениям безопасности Cisco IOS предлагает два командных режима доступа к административным функциям:

1. Пользовательский режим EXEC (User EXEC Mode) – режим с ограниченными возможностями. В этом режиме доступно несколько команд, позволяющих, в частности, посмотреть некоторые параметры устройства. Однако невозможно выполнять какие-либо команды для изменения конфигура-

ции устройства. В пользовательском режиме EXEC после имени устройства выводится символ «>».

2. Привилегированный режим EXEC (Privileged EXEC Mode) – в этом режиме сетевой администратор может просмотреть все параметры устройства, а также перейти в режим глобальной конфигурации. В привилегированном режиме EXEC после имени устройства выводится символ «#».

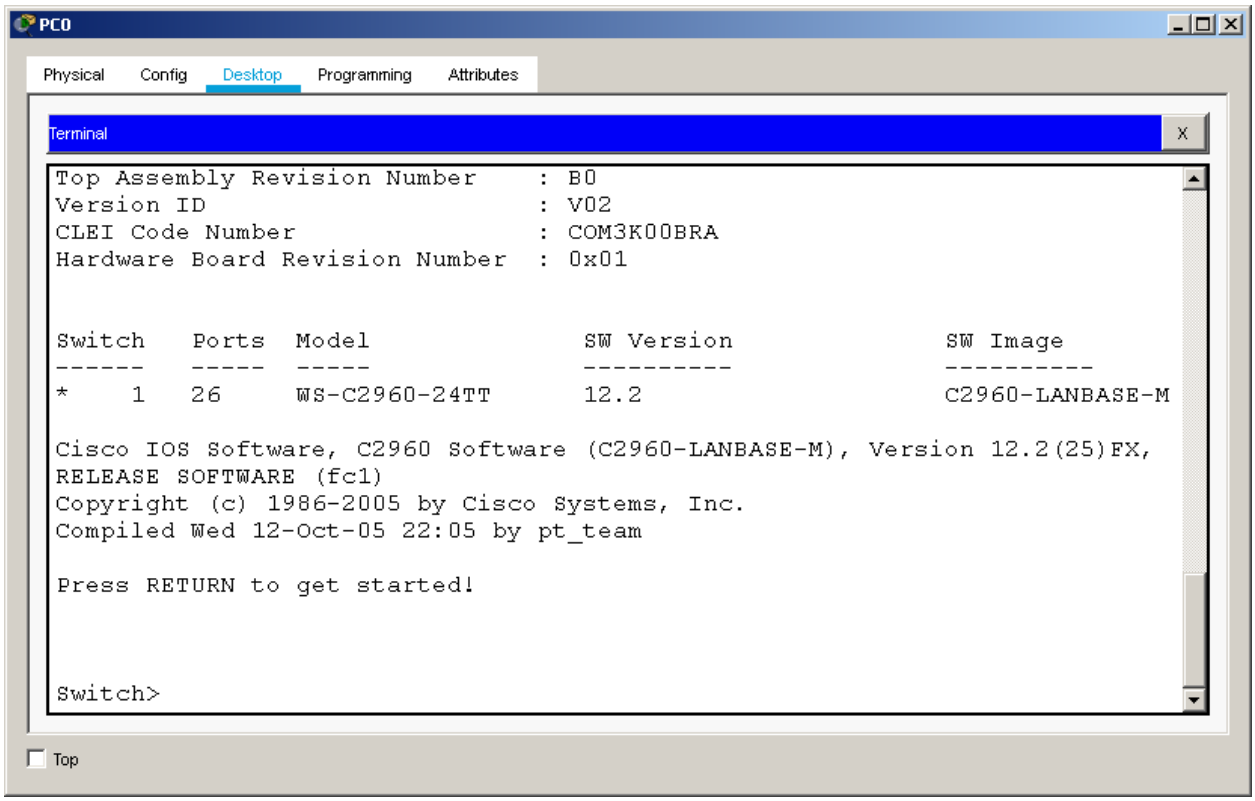


Рисунок 49 – Окно эмулятора терминала

Таким образом, по умолчанию Cisco IOS дает коммутатору имя «Switch» и загружается в пользовательский режим EXEC.

Для перехода в привилегированный режим необходимо ввести команду **enable**. По умолчанию привилегированный режим EXEC не защищен, поэтому переход произойдет беспрепятственно (рис. 50):

Рисунок 50 – Переход в привилегированный режим EXEC

Первым делом необходимо закрыть свободный доступ к привилегированному режиму, т.е. установить пароль. Это делается в режиме глобальной конфигурации.

Для перехода в режим глобальной конфигурации нужно в привилегированном режиме ввести команду **configure terminal** (рис. 51).

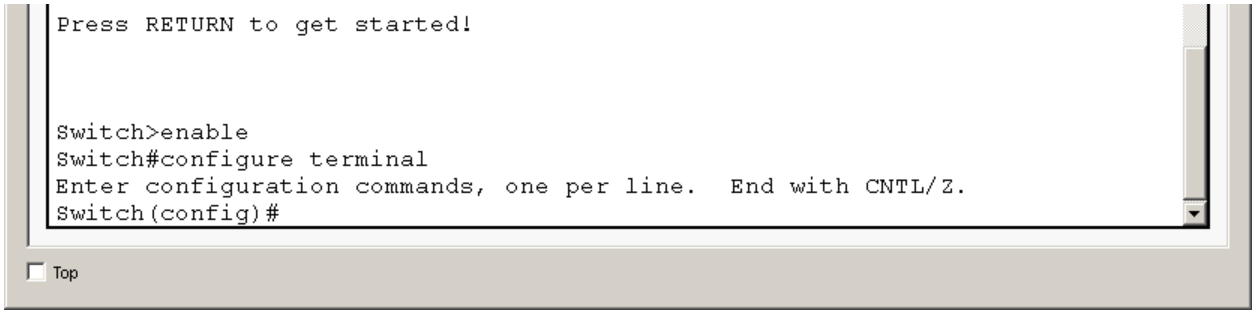


Рисунок 51 – Переход в режим глобальной конфигурации

После имени устройства теперь выводится (config)#. Так CLI показывает, что устройство находится в режиме глобальной конфигурации. Устройство готово к глобальным настройкам или к переходу в подрежимы для конфигурирования интерфейсов, линий, виртуальных локальных сетей и т.д.

Пароль для доступа в привилегированный режим можно задать командой **enable password**, после которой через пробел вводится секретное слово. В учебных примерах мы будем использовать простые пароли, например, **cisco** или **class**. Однако для защиты устройств в реальной сети такие пароли являются слишком примитивными и совершенно не годятся. Зададим пароль **cisco** для защиты привилегированного режима нашего коммутатора (рис. 52).

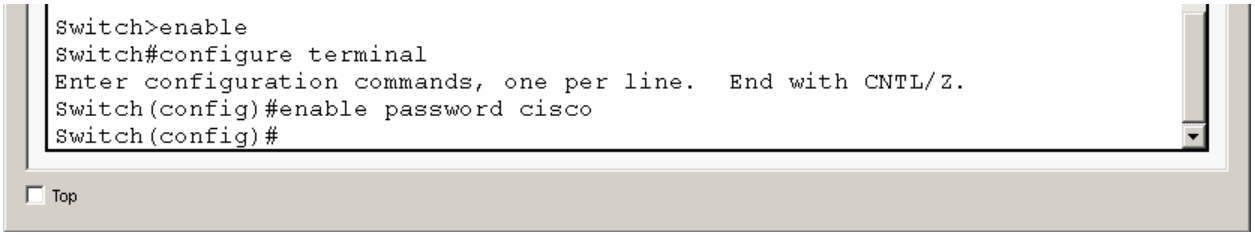


Рисунок 52 – Установка пароля на привилегированный режим

Проверим, будет ли запрашиваться пароль при попытке перейти из пользовательского режима в привилегированный. Для этого нужно сначала покинуть режим глобальной конфигурации, т.е. вернуться в привилегированный режим, введя команду **exit** или нажав Ctrl/Z, а затем перейти в пользовательский, введя команду **disable** (рис. 53).

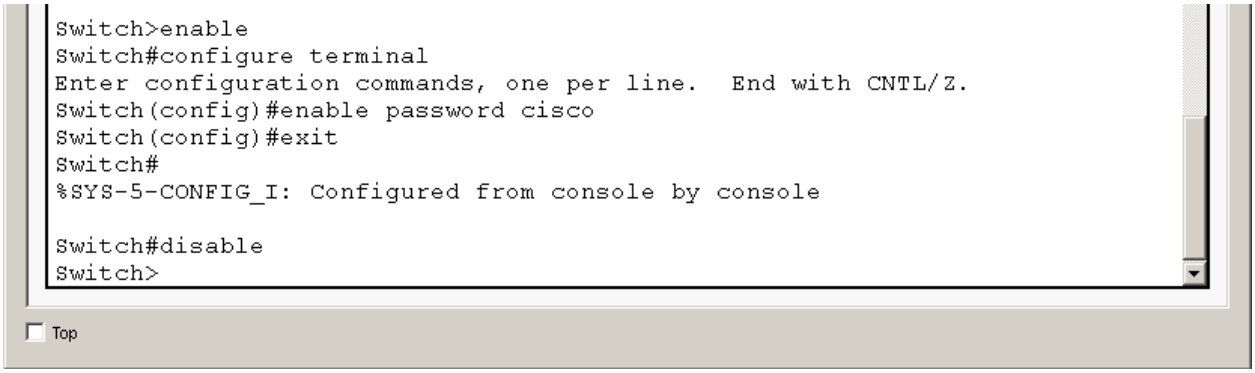


Рисунок 53 – Возвращение в пользовательский режим

Теперь запуск команды **enable** сопровождается запросом пароля. Вводим пароль. Символы при наборе не отображаются и не подменяются кружочками или звездочками. После нажатия «Enter» оказываемся в привилегированном режиме (рис. 54).

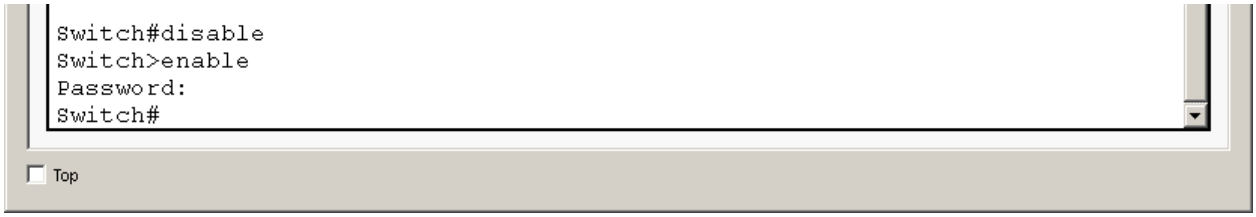


Рисунок 54 – Запрос пароля при переходе в привилегированный режим

Все настройки, которые выполняет администратор, в том числе и для защиты устройства, автоматически сохраняются в файле текущей конфигурации *running-config*. Просмотреть файл конфигурации можно только в привилегированном режиме, выполнив команду **show running-config** (рис. 55).

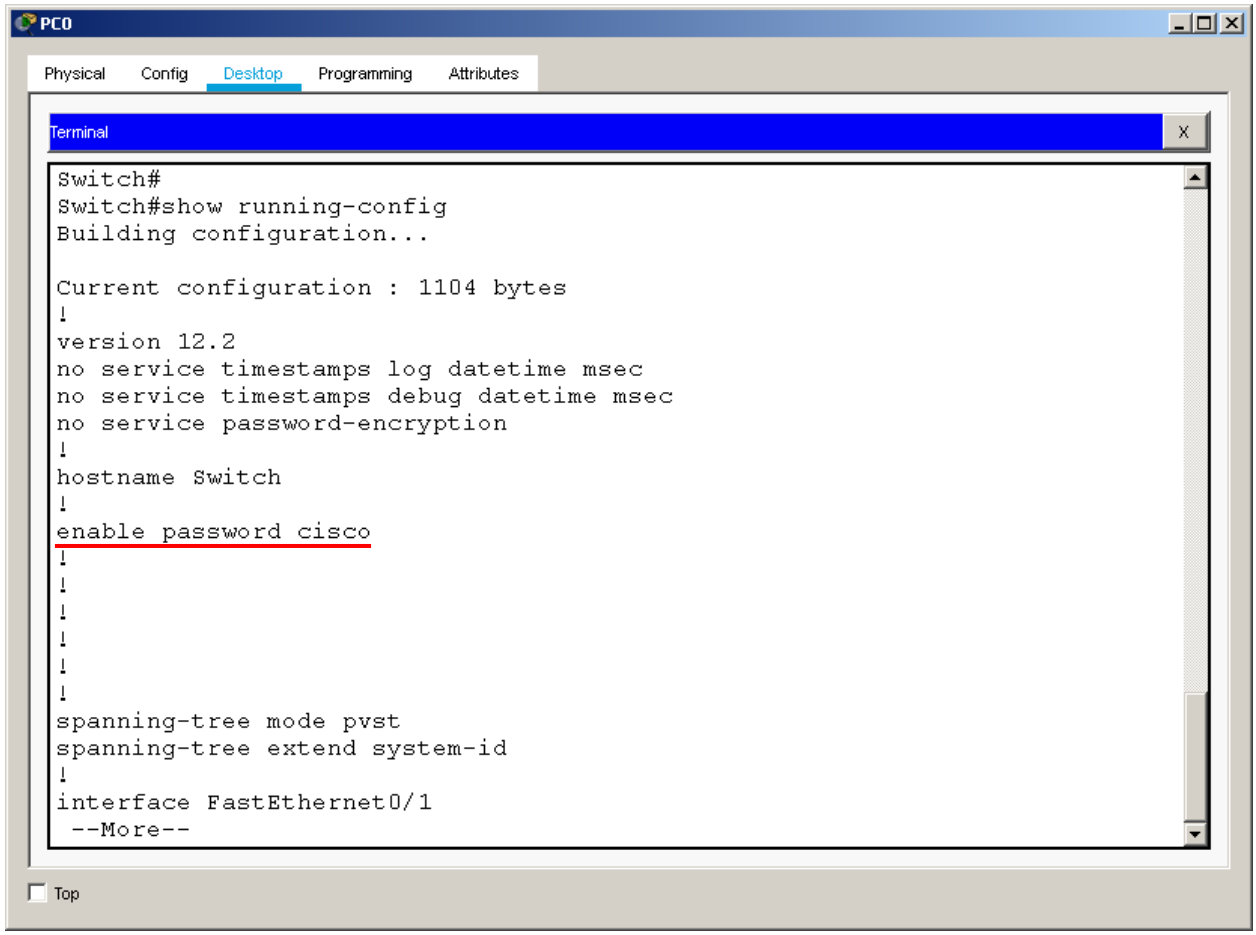


Рисунок 55 – Просмотр файла текущей конфигурации

Файл содержит несколько страниц текстовой информации. Для пролистывания используют клавишу «Пробел», однако глобальные параметры представлены на первой странице. Видно, что пароль привилегированного режима хранится в открытом виде. Это создает угрозу безопасности, по-

скольку при наличии доступа к файлам конфигурации любой пользователь может увидеть пароли.

Чтобы зашифровать все пароли в файле *running-config*, используется команда глобальной конфигурации **service password-encryption** (рис. 56).

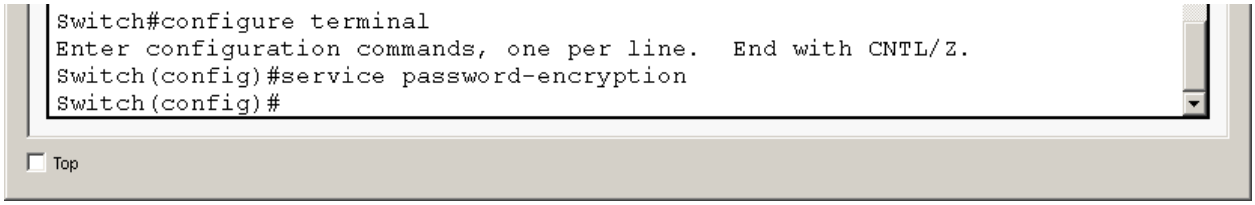


Рисунок 56 – Просмотр файла текущей конфигурации

Команда изменит соответствующий параметр в файле конфигурации, поэтому не только уже заданные, но и новые пароли будут шифроваться автоматически алгоритмом Cisco type 7 (рис 57).

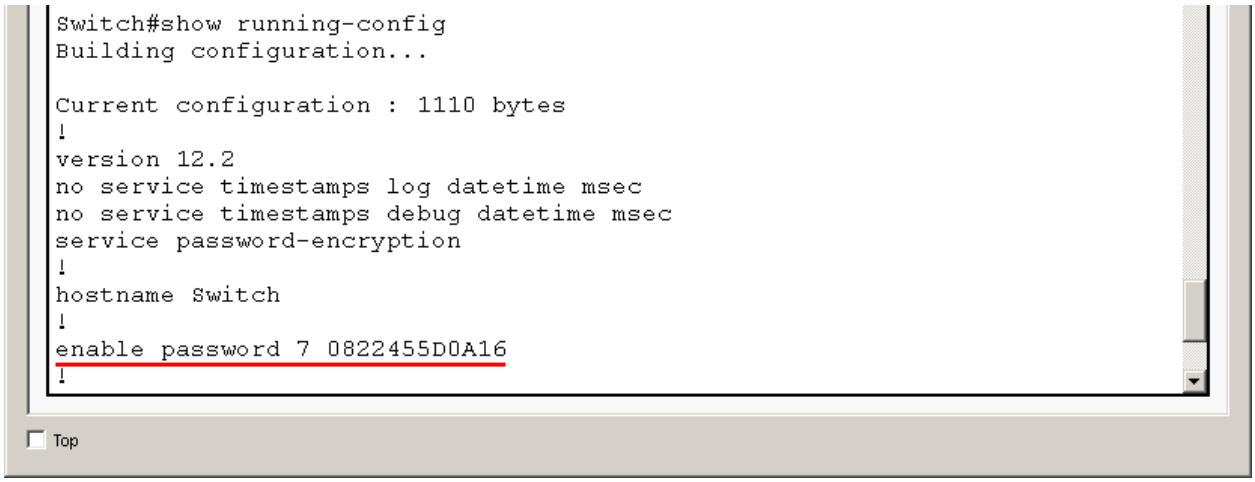


Рисунок 57 – Зашифрованный пароль в файле текущей конфигурации

Для повышения уровня безопасности, необходимо защитить доступ к пользовательскому режиму EXEC. Настроим консольный порт так, чтобы пароль запрашивался уже при подключении. Переход в режим конфигурирования консоли осуществляется из режима глобальной конфигурации командой **line console 0**. Ноль используется для обозначения первого (в данном случае единственного) интерфейса консоли (рис. 58).

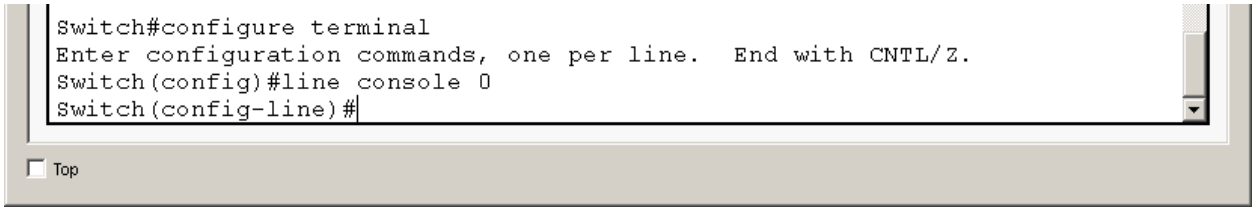


Рисунок 58 – Переход в режим конфигурирования линии консоли

После имени устройства теперь выводится (config-line)#, поскольку режим конфигурирования линии консоли является подрежимом глобальной конфигурации. Зададим пароль, используя команду **password**, после которой введем секретное слово. Пусть это будет слово **class**. Еще раз подчеркнем,

что такой простой пароль не следует использовать в реальной сети. Пароль установлен, но этого недостаточно. Нужно сделать так, чтобы консоль запрашивала этот пароль. Для этого используется команда **login** (рис. 59).

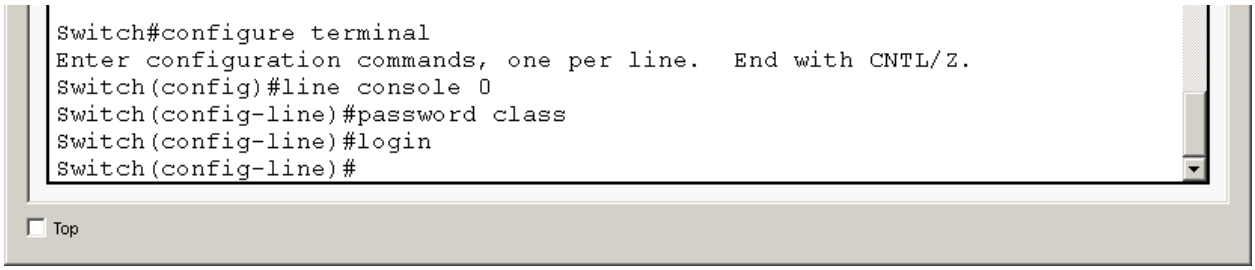


Рисунок 59 – Защита паролем линии консоли

Теперь при подключении к интерфейсу командной строки (CLI) по консоли, будет запрашиваться пароль.

Проверим это, завершив сеанс и выполнив повторное подключение. Команда **end** используется для выхода из режима конфигурирования консоли сразу в привилегированный режим, минуя режим глобальной конфигурации (рис. 60).

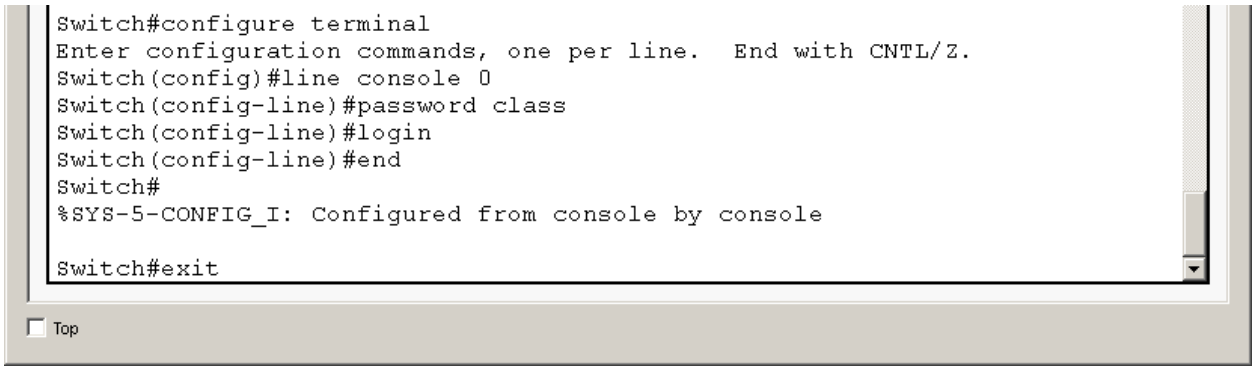


Рисунок 60 – Завершение сеанса управления устройством

После запуска команды **exit** в привилегированном режиме сеанс будет завешен. CLI предложит нажать «Enter» (Press RETURN to get started!), а затем ввести пароль пользовательского режима (рис. 61).

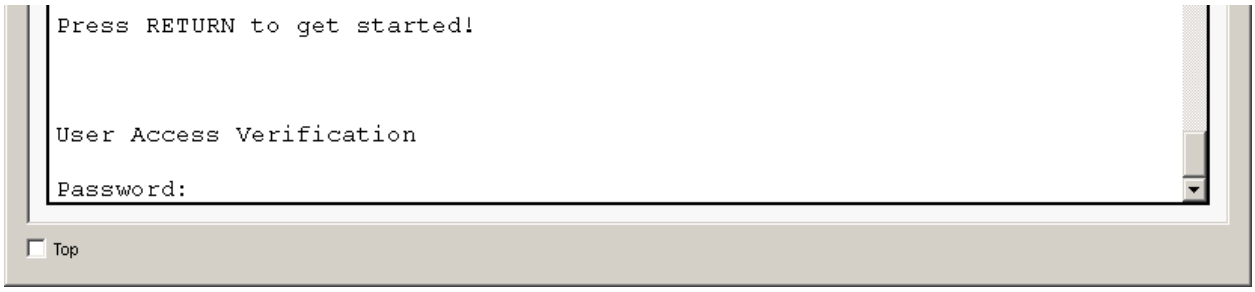


Рисунок 61 – Запрос пароля при подключении к CLI по консоли

Вводим пароль, заданный при конфигурировании линии консоли на коммутаторе (символы при наборе не отображаются). Система позволит войти в пользовательский режим (рис. 62).

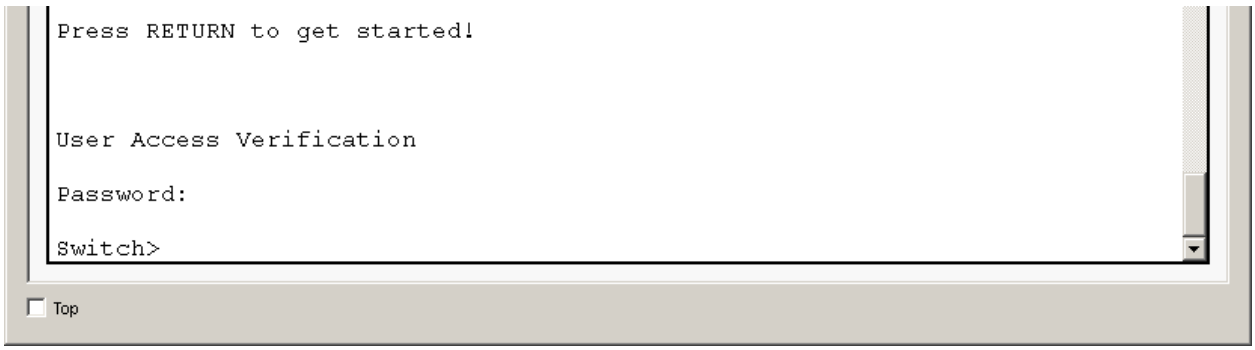


Рисунок 62 – Вход в пользовательский режим по паролю

Таким образом, уровень защищенности устройства повысился. Теперь, чтобы попасть в привилегированный режим EXEC, злоумышленнику потребуется заполучить два пароля, а не один.

Если так случится, что злоумышленник получит доступ к файлу конфигурации или его резервной копии, то он увидит пароли в зашифрованном виде. К сожалению, в Cisco type 7 используется слабый алгоритм шифрования, поэтому рекомендуется задавать пароль привилегированного режима командой глобальной конфигурации **enable secret**. В этом случае в файле конфигурации будет сохранен хэш-код пароля. Это более безопасный вариант.

Пароли, заданные как **secret** имеют больший приоритет, чем **password**, поэтому если использовались оба варианта, то система будет проверять именно **secret**.

Зададим в качестве нового пароля привилегированного режима слово **cisco1** и сделаем соответствующие настройки. Сначала нужно перейти в привилегированный режим, защищенный паролем **cisco**, затем перейти в режим глобальной конфигурации и задать новый пароль **cisco1**, используя команду **enable secret** (рис. 63).

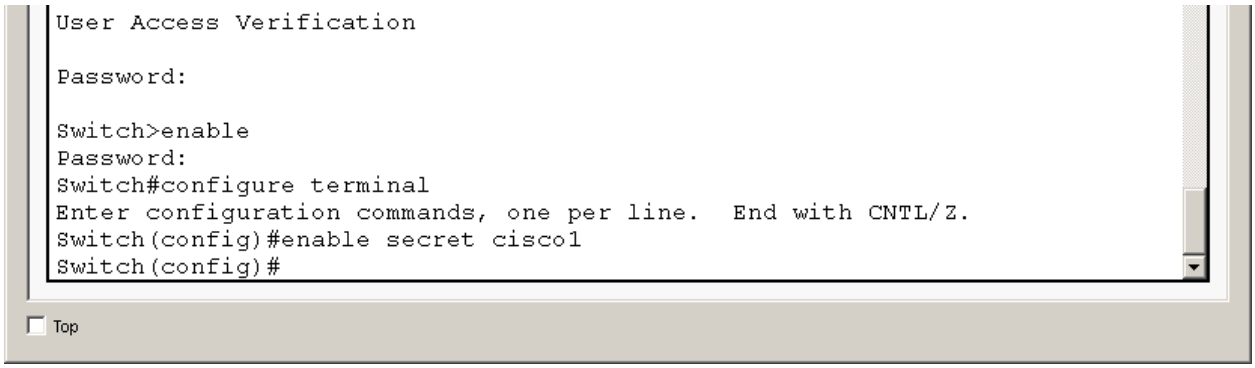


Рисунок 63 – Защита привилегированного режима командой **enable secret**

Вернемся в привилегированный режим и, используя команду **show running-config**, посмотрим, в каком виде сохранился только что заданный пароль привилегированного режима (рис. 64).

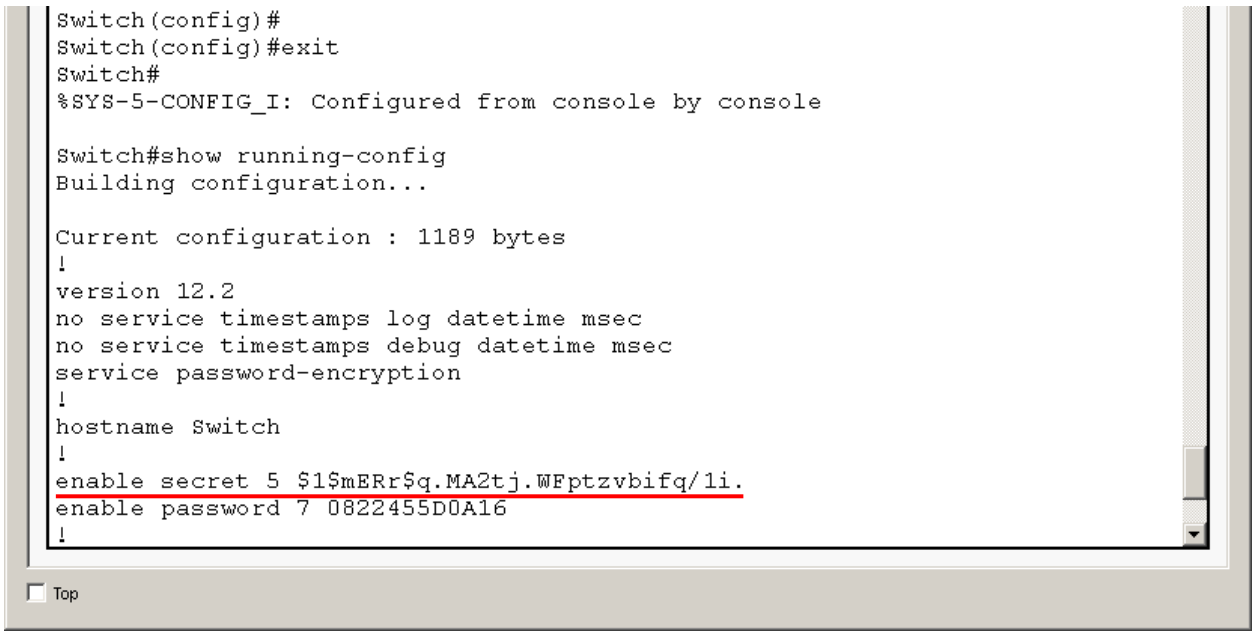


Рисунок 64 – Просмотр файла текущей конфигурации

Цифра «5» после **enable secret** показывает, что используется алгоритм хэширования MD5, т.е. в файле конфигурации хранится хэш-код пароля, причем это не зависит от того, включено ли шифрование паролей (командой **service password-encryption**).

К базовым настройкам коммутатора, которые в первую очередь выполняет администратор, является задание устройству имени. По умолчанию всем коммутаторам назначено имя **Switch**, а маршрутизаторам – имя **Router**. Если в сети несколько промежуточных устройств, назначение каждому из них уникального имени является логичным решением, позволяющим избежать путаницы. Имена могут назначаться в соответствии с определенными правилами, принятыми в организации. В наших учебных примерах обычно будем назначать коммутаторам простые имена **S1**, **S2** и т.д.

Переименование устройства выполняется в режиме глобальной конфигурации с помощью команды **hostname**, после которой указывается новое имя устройства. Итак, чтобы изменить имя коммутатора на **S1**, надо ввести команду **hostname S1** (рис. 65).

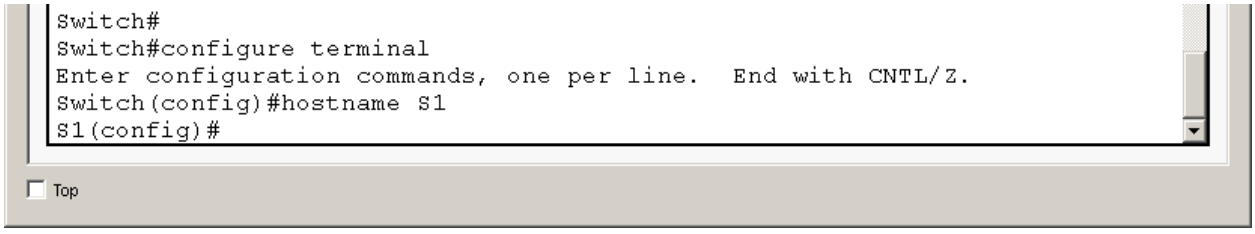


Рисунок 65 – Переименование устройства

Результат переименования виден сразу – изменилось приглашение CLI. Изменился также соответствующий параметр в файле текущей конфигурации *running-config*. Вернемся в привилегированный режим и просмотрим содержимое файла (рис. 66).

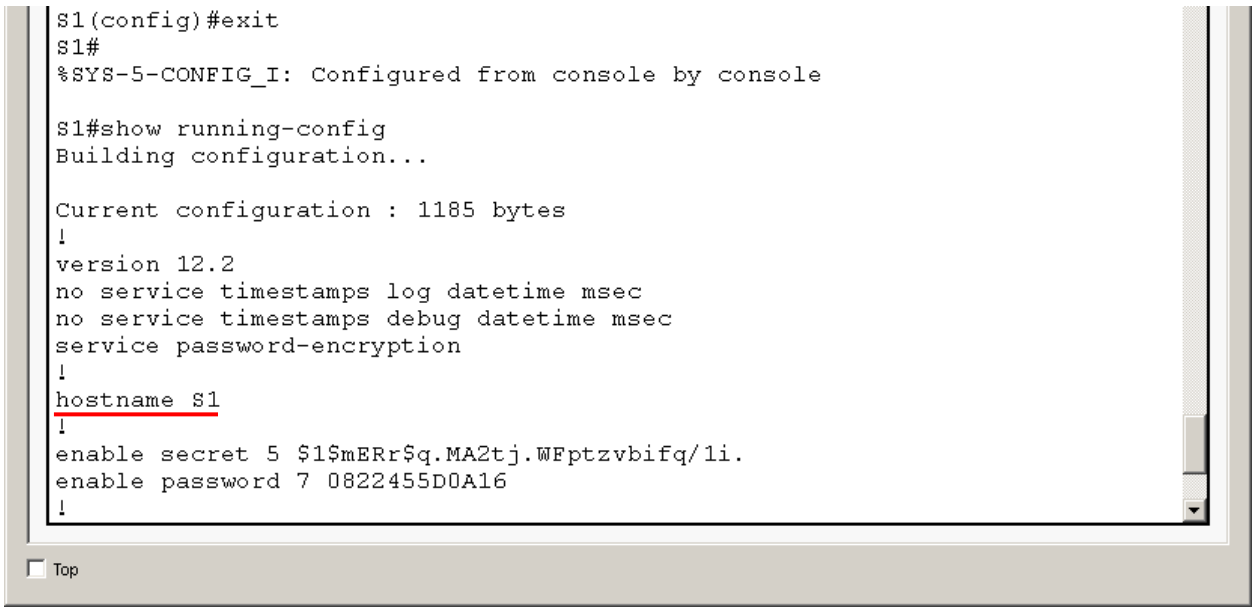


Рисунок 66 – Новое имя устройства в файле текущей конфигурации

Можно считать, что самые основные настройки коммутатора выполнены. Теперь их необходимо сохранить, чтобы после перезагрузки устройство использовало заданные параметры конфигурации. Это делается командой привилегированного режима **write memory** (рис. 67).

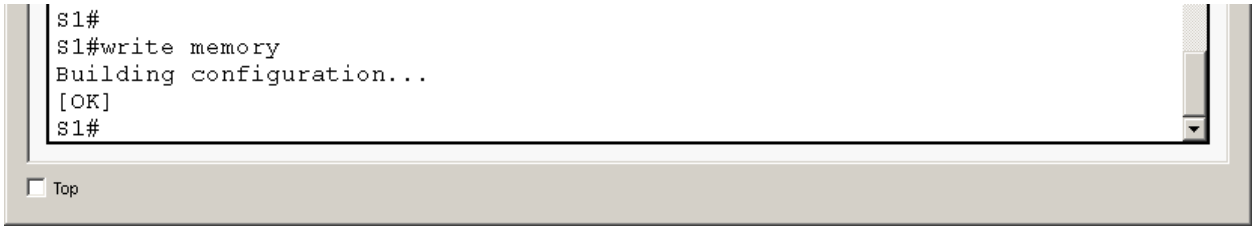


Рисунок 67 – Сохранение конфигурации устройства

В результате выполнения этой команды создается файл *startup-config*, являющийся точной копией файла *running-config*. Именно *startup-config* будет искать операционная система Cisco IOS в постоянной памяти устройства во время загрузки.

Практическое занятие №2
Создание компьютерной сети небольшого предприятия на основе беспроводного маршрутизатора

Задача 1. Создание сети на основе беспроводного маршрутизатора

В качестве центрального устройства сети небольшого предприятия, офиса, а также домашней сети часто используется беспроводной маршрутизатор. Это комплексное устройство, у которого в одном корпусе размещены и соединены соответствующим образом маршрутизатор, коммутатор и точка доступа. Данные компоненты беспроводного маршрутизатора позволяют подключать к сети и проводные, и беспроводные оконечные устройства, а также обеспечивать их доступ к интернету.

В рамках решения первой задачи нужно построить модель компьютерной сети небольшого предприятия. Подберем беспроводной маршрутизатор и оконечные устройства, которые обычно используются сотрудниками небольшого предприятия или офиса, разместим их на рабочем поле программы Cisco Packet Tracer и обеспечим физическое подключение. Имитировать интернет будет маршрутизатор провайдера (ISP) и единственный сервер, который непосредственно подключим к маршрутизатору провайдера.

Сначала разместим на рабочем поле оконечные устройства. Для этого на панели выбора типа устройства (слева внизу) нужно отметить категорию «End Devices» (оконечные устройства), затем из области выбора конкретного устройства «перетянуть» на рабочее поле компьютер (PC), сервер (Server), лэптоп (Laptop) и смартфон (Smart Device).

Центральным устройством сети будет беспроводной маршрутизатор WRT300N. Он находится в категории «Network Devices» (сетевые устройства) и подкатегории «Wireless Devices» (беспроводные устройства) (рис. 68).

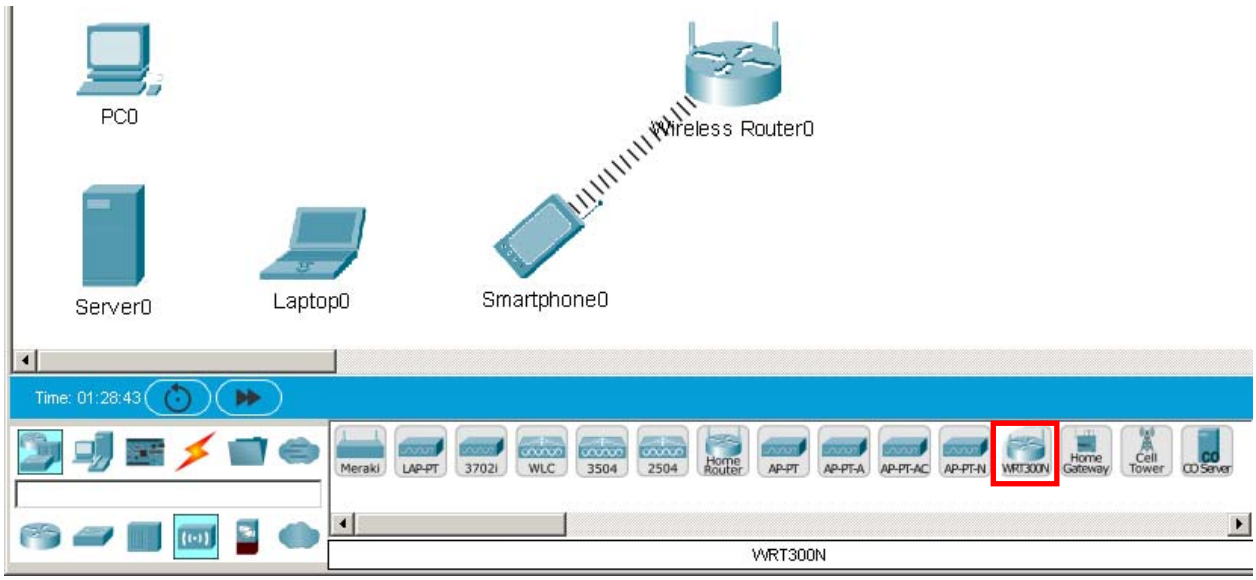


Рисунок 68 – Размещение беспроводного маршрутизатора на рабочем поле

Характерно, что между смартфоном и беспроводным маршрутизатором сразу отобразилась линия связи. Дело в том, что на маршрутизаторе уже настроена и включена незащищенная беспроводная сеть, а смартфон настроен на автоматическое подключение к сети. Однако лэптоп к беспроводной сети не подключился, поскольку по умолчанию у него отсутствует беспроводной сетевой адаптер. Чуть позже снабдим лэптоп беспроводным адаптером, а беспроводную сеть перенастроим и защитим.

Подключим оконечные устройства к беспроводному маршрутизатору. Проверим, сколько проводных интерфейсов доступно. Если навести указатель мыши на устройство на рабочем поле, всплывающая подсказка покажет все интерфейсы и их статус (рис. 69).

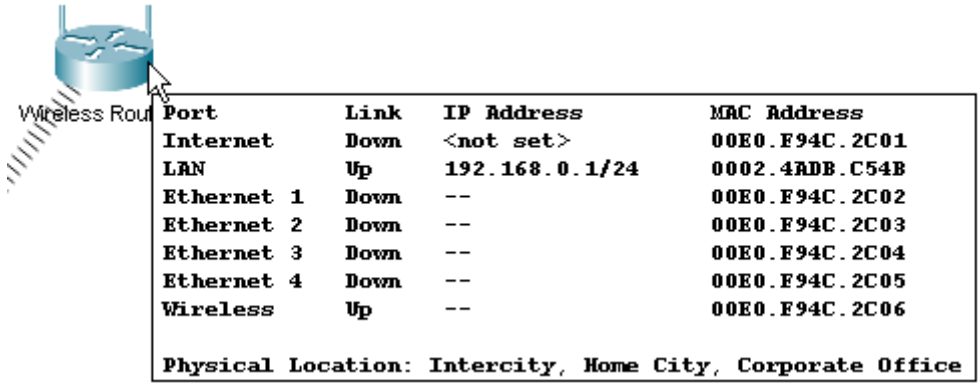


Рисунок 69 – Интерфейсы беспроводного маршрутизатора и их статус

Видно, что доступно четыре проводных интерфейса (Ethernet 1 – Ethernet 4), беспроводная сеть включена, есть проводной интерфейс для подключения к внешней сети (Internet). Кроме того, есть интерфейс LAN, он поднят и ему назначен IP-адрес: 192.168.0.1. Это значит, что устройство готово к удаленному управлению.

Компьютер и сервер подключим к беспроводному маршрутизатору прямым медным кабелем (Copper Straight-Through). Со стороны оконечных устройств PC0 и Server0 кабель подсоединяется к интерфейсам FastEthernet0, со стороны беспроводного маршрутизатора – Ethernet 1 и Ethernet 2. Зеленые треугольники на обоих концах линии связи означают, что на физическом уровне соединение установлено (рис. 70).

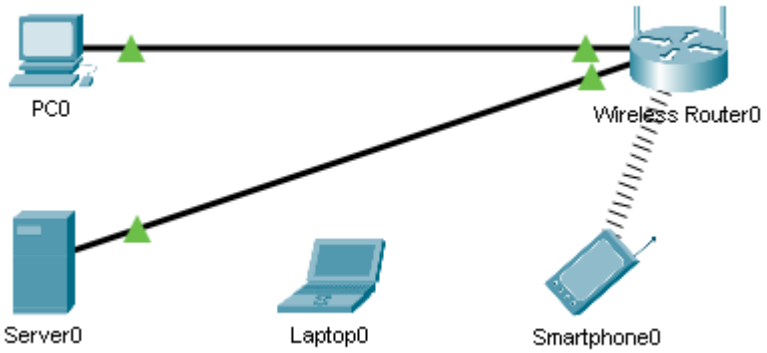


Рисунок 70 – Подключение узлов к беспроводному маршрутизатору

Можно было бы аналогичным образом и лэптоп подключить к проводной сети, но мы решили заменить в лэптопе проводной адаптер на беспроводной и подключить узел к беспроводной сети. Замена производится следующим образом:

- щелчком левой кнопки мыши по значку Laptop0 на рабочем поле открыть окно настройки устройства;
- на закладке «Physical» на изображении лэптопа нажать круглую кнопку (отмечена красной рамкой), чтобы выключить устройство (рис. 71).

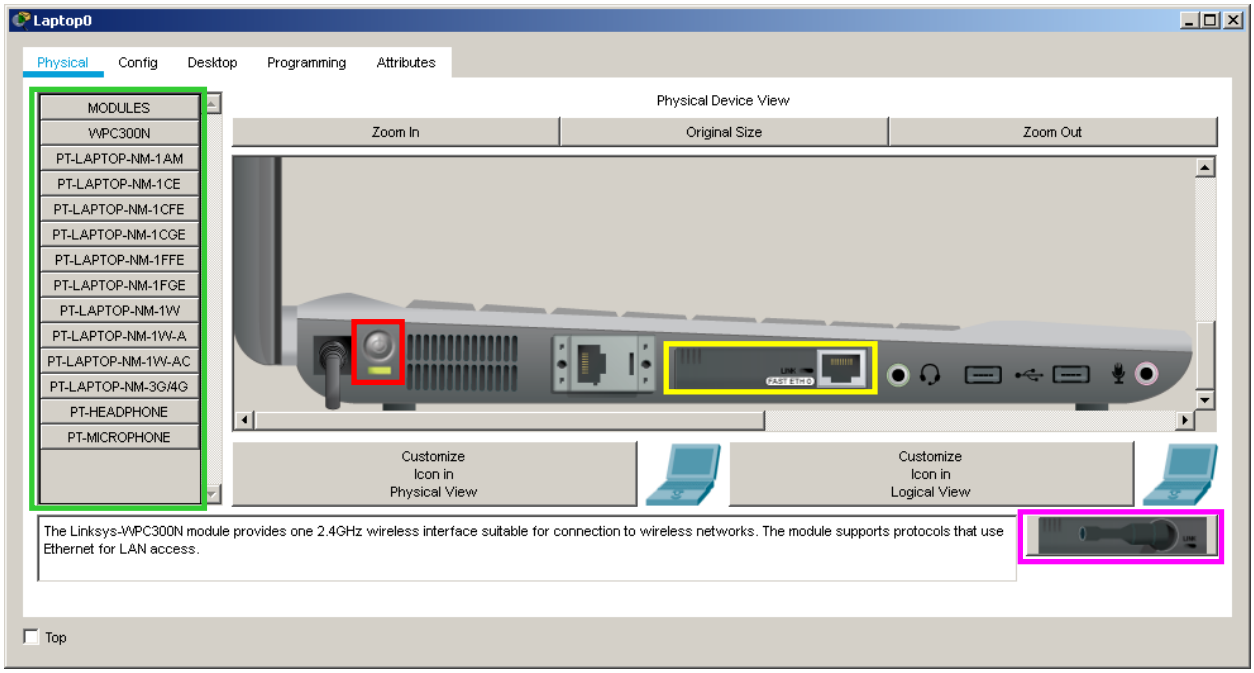


Рисунок 71 – Замена сетевого адаптера в лэптопе

- зацепить мышью проводной сетевой адаптер (рамка желтого цвета), перетянуть и бросить его в область «MODULES» в левой части окна (обозначена зеленой рамкой), тем самым имитируя его излечение;
- справа внизу уже находится подходящий модуль Linksys-WPC300N (рамка розового цвета) – зацепить его левой кнопкой мыши и установить его в освободившееся гнездо;
- включить лэптоп, закрыть окно.

Через несколько секунд лэптоп (как и смартфон) автоматически подключится к открытой беспроводной сети. Таким образом, все оконечные устройства на физическом уровне подключены к сети малого предприятия.

Теперь нужно подключить локальную сеть к интернету. Поскольку Cisco Packet Tracer не позволяет сымитировать интернет, упрощенно представим его маршрутизатором провайдера и единственным сервером. Разместим эти устройства на рабочем поле. В качестве маршрутизатора интернет-провайдера будем использовать Cisco 1941. Маршрутизаторы находятся в категории «Network Devices» (сетевые устройства), в подкатегории «Routers» (маршрутизаторы).

Для соединения двух маршрутизаторов WRT300N и 1941 (как и при непосредственном соединении двух компьютеров) следует использовать перекрестный медный кабель (Copper Cross-Over). У беспроводного маршрутизатора есть соответствующий проводной интерфейс «Internet», а у 1941 два одинаковых интерфейса GigabitEthernet (0/0 и 0/1), поэтому можно выбрать любой. Пусть это будет GigabitEthernet 0/0.

При непосредственном подключении сетевого интерфейса компьютера к маршрутизатору также нужно использовать перекрестный медный кабель (Copper Cross-Over). Характерно, что на концах вновь созданных линий связи со временем так не появятся зеленые треугольники. Вместо них остаются красные вершиной вниз. Это объясняется тем, что интерфейсы маршрутизатора не поднимаются автоматически после подключения к ним сетевых устройств, они поднимаются только вручную и эти настройки предстоит выполнить в рамках решения следующей задачи.

После соединения устройств можно считать, что первая задача решена – построена модель сети небольшого предприятия, подключенная к интернету. Для лучшей визуализации сети подсвечены разными цветами, а маршрутизатор провайдера переименован в ISP (рис. 72).

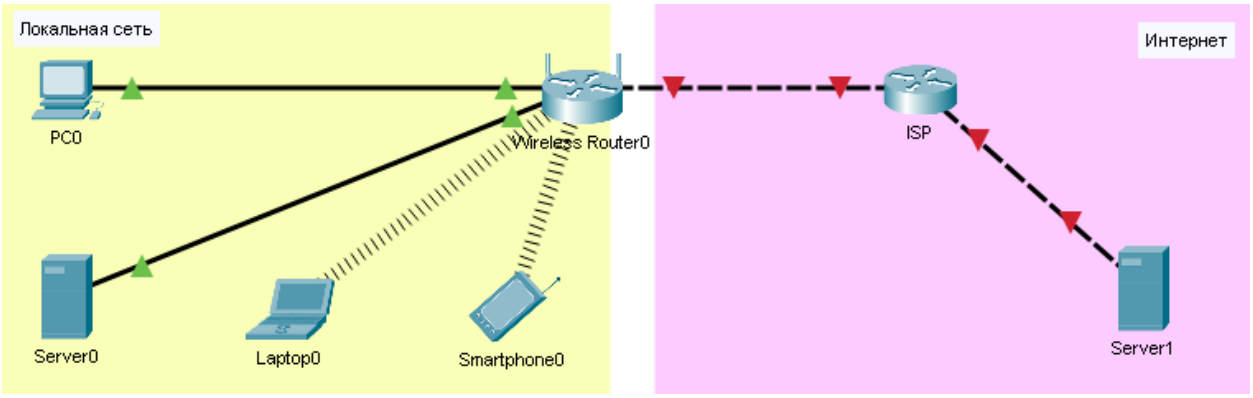


Рисунок 72 – Модель сети небольшого предприятия на основе беспроводного маршрутизатора

Задача 2. Настройка маршрутизатора интернет-провайдера и сервера в интернете

Настройку маршрутизатора ISP выполним известным нам способом – подсоединим компьютер или лэптоп к консольному порту маршрутизатора и подключимся к интерфейсу командной строки (CLI), используя эмулятор терминала.

Подключение к консольному порту маршрутизатора (как и коммутатора) выполняется с помощью специального консольного кабеля. Один конец этого кабеля подключается к порту «Console» маршрутизатора, другой – к последовательному порту «RS 232» компьютера или лэптопа (рис. 73).

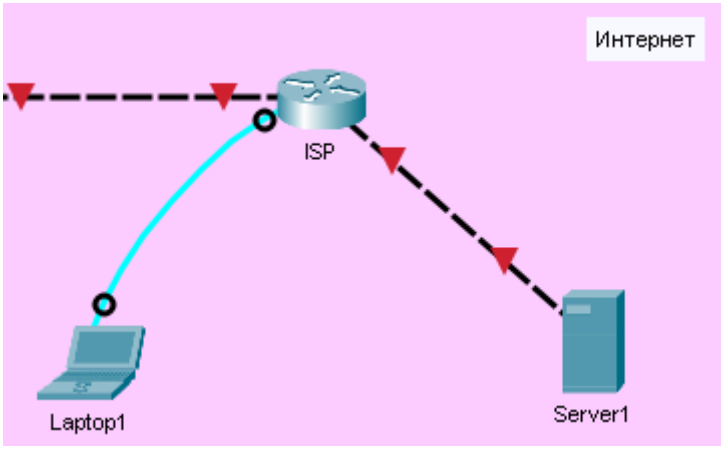


Рисунок 73 – Подключение лэптопа к маршрутизатору консольным кабелем

Для доступа к интерфейсу командной строки нужно на лэптопе открыть эмулятор терминала. Ярлык программы «Terminal» находится на рабочем столе лэптопа (закладка «Desktop») (рис. 67). После запуска программы «Terminal» и согласия с параметрами соединения (рис. 68), открывается CLI с предложением начать конфигурирование устройства в режиме диалога (Would you like to enter the initial configuration dialog? [yes/no]). Вводим **no**, чтобы отказаться. Операционная система предлагает нажать кнопку «Enter» (Press RETURN to get started!), чтобы начать работу. После нажатия «Enter» появляется приглашение операционной системы (Router>), командная строка готова к приему команд пользовательского режима EXEC (рис. 74).

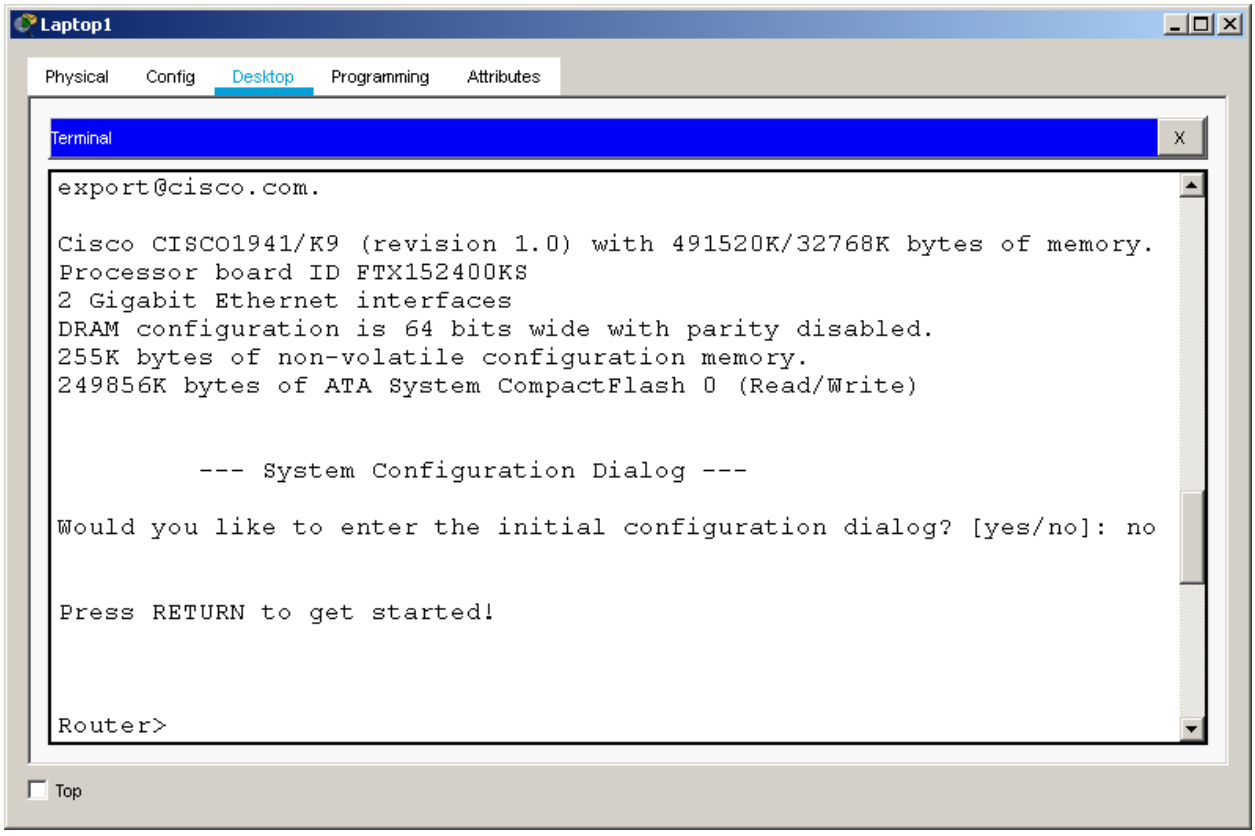


Рисунок 74 – Окно эмулятора терминала

Первичные настройки маршрутизатора (как и коммутатора) включают обеспечение безопасности устройства, в том числе ограничение доступа и защиту привилегированного режима, однако ради решения основной задачи базовые настройки просто пропустим и сразу займемся настройкой интерфейсов.

Сначала нужно продумать адресацию, ведь в нашем примере три сети: локальная сеть небольшого предприятия, интернет и «промежуточная» сеть между беспроводным маршрутизатором и маршрутизатором ISP. В каждой из сетей должен использоваться собственный диапазон адресов. Интерфейсу LAN беспроводного маршрутизатора уже назначен IP-адрес: 192.168.0.1 /24 (рис. 69). Этот адрес относится к сети с номером 192.168.0.0 и маской 255.255.255.0. Другим устройствам в этой локальной сети (вернее, их сетевым интерфейсам) должны быть назначены адреса 192.168.0.2, 192.168.0.3 … 192.168.0.254, тогда они смогут обмениваться информацией. При этом IP-адрес интерфейса LAN беспроводного маршрутизатора (192.168.0.1) должен быть указан в настройках сетевых интерфейсов всех узлов сети в качестве шлюза по умолчанию (default gateway), иначе эти узлы не смогут отправлять пакеты за пределы сети. Итак, в локальной сети используется адресное пространство 192.168.0.0 /24.

В промежуточной сети всего два интерфейса. Это интерфейсы маршрутизаторов. Учебный пример не ограничивает нас в выборе, поэтому доступны все белые адреса (которые в реальной жизни задаются интернет-провайдером). Назначим интерфейсам IP-адреса 11.0.0.1 и 11.0.0.2 из сети 11.0.0.0 /8 (префикс /8 соответствует маске 255.0.0.0). В этой сети более 16 млн. адресов: 11.0.0.1 … 11.255.255.254, но нам потребуется только два.

Интернет включает множество сетей и миллиарды узлов, но для имитации интернета в учебном примере достаточно одного узла, который непосредственно подключен ко второму интерфейсу маршрутизатора провайдера (ISP). Назначим интерфейсам IP-адреса 12.0.0.1 и 12.0.0.2 из сети 12.0.0.0 /8 (префикс /8 соответствует маске 255.0.0.0).

Модель сети с планом адресации представлена на рисунке 75.

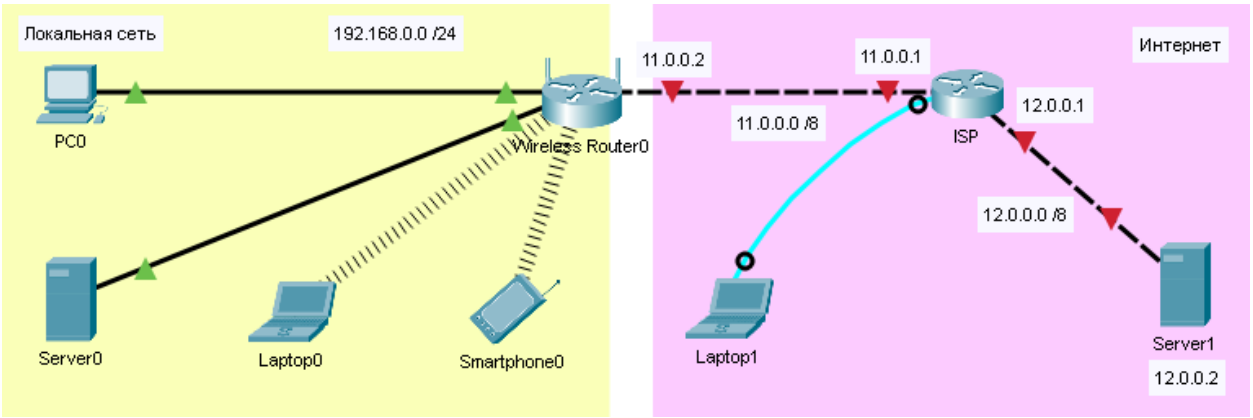


Рисунок 75 – Модель сети с планом адресации

Теперь можно поднять интерфейсы маршрутизатора ISP и назначить им запланированные IP-адреса. Порядок действий следующий:

1. Перейти в привилегированный режим.
2. Перейти в режим глобальной конфигурации.
3. Перейти в режим конфигурирования интерфейса GigabitEthernet 0/0.
4. Назначить интерфейсу IP-адрес и маску подсети.
5. Поднять интерфейс.
6. Перейти к конфигурированию интерфейса GigabitEthernet 0/1.
7. Назначить интерфейсу IP-адрес и маску подсети.
8. Поднять интерфейс.
9. Вернуться в привилегированный режим.
10. Сохранить текущую конфигурацию.

Некоторые команды нам знакомы, но есть и новые. Для перехода в привилегированный режим вводится команда **enable**, для перехода в режим глобальной конфигурации: **configure terminal**.

Переход в режим конфигурирования интерфейса (на 3-м шаге) осуществляется командой: **interface gigabitethernet 0/0** (рис. 76).

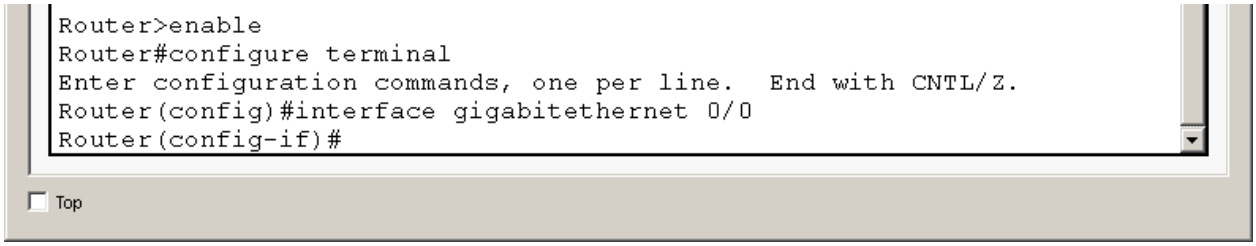


Рисунок 76 – Переход в режим конфигурирования интерфейса

После имени устройства теперь выводится (config-if)#, поскольку режим конфигурирования интерфейса (как и режим конфигурирования линии консоли) является подрежимом глобальной конфигурации.

На 4-м шаге интерфейсу назначается IP-адрес и маска подсети. Именно этот интерфейс маршрутизатора ISP подключен к беспроводному маршрутизатору, поэтому (как указано на рис. 75) этот интерфейс должен получить IP-адрес 11.0.0.1 и маску подсети 255.0.0.0. Это делается командой: **ip address 11.0.0.1 255.0.0.0** (рис. 77).

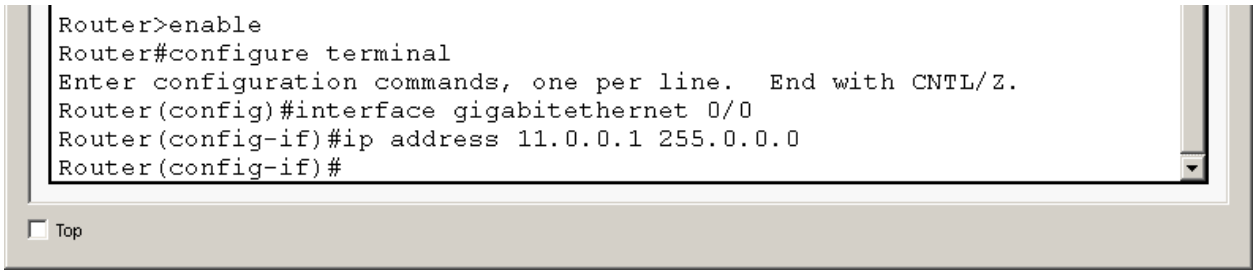


Рисунок 77 – Назначение IP-адреса интерфейсу маршрутизатора

Теперь нужно поднять, т.е. включить интерфейс. Для этого (на 5-м шаге) выполняется команда: **no shutdown**. Операционная система поднимает интерфейс и информирует об этом двумя сообщениями (рис. 78).

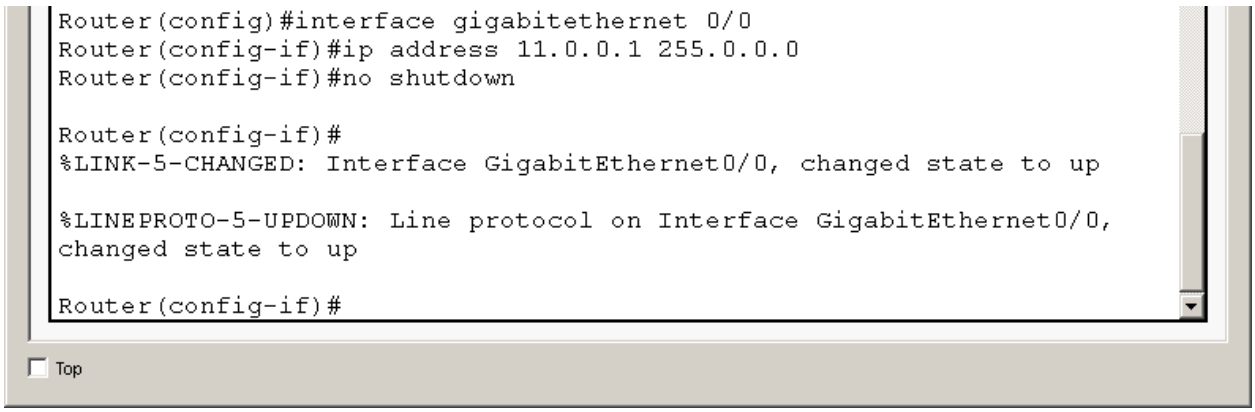


Рисунок 78 – Поднятие интерфейса маршрутизатора

Настройка второго интерфейса маршрутизатора выполняется аналогичным образом.

На 6-м шаге нужно ввести команду: **interface gigabitethernet 0/1**. Причем это можно сделать, находясь в режиме конфигурирования интерфейса gigabitethernet 0/0 (т.е. без возвращения в режим глобальной конфигурации).

На 7-м и 8-м шагах вводится IP-адрес 12.0.0.1 с маской подсети 255.0.0.0, затем поднимаем интерфейс (рис. 79).

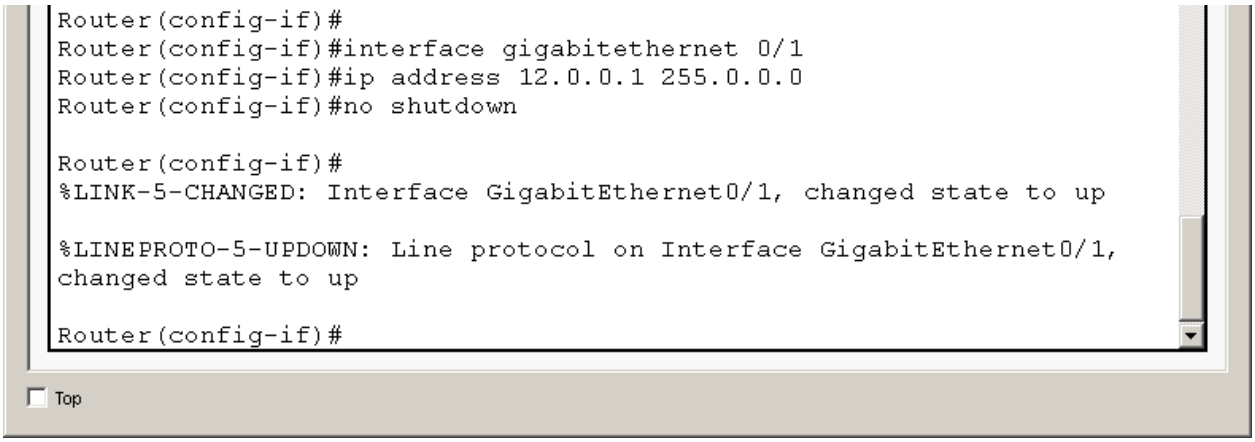


Рисунок 79 – Настройка второго интерфейса маршрутизатора

Для возврата в привилегированный режим (шаг 9) из любого подрежима глобальной конфигурации используется команда **end**. Сохранение текущих настроек (шаг 10) осуществляется командой **write memory** (рис. 80).

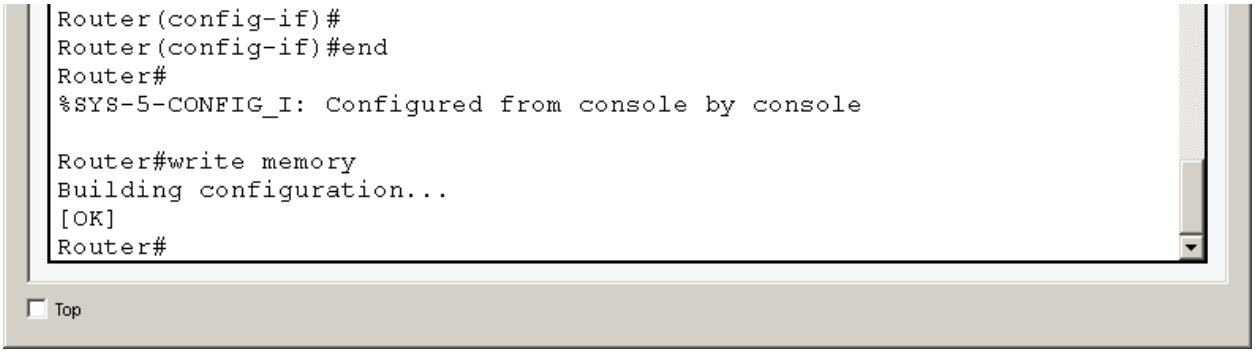


Рисунок 80 – Завершение и сохранение настроек маршрутизатора

Т.к. интерфейсы маршрутизатора ISP подняты, красные треугольники на линиях связи сменились на зеленые. Всплывающая подсказка, появляющаяся при наведении указателя мыши на значок маршрутизатора на рабочем поле, показывает, какие IP-адреса назначены его интерфейсам (рис. 81). Таким образом, маршрутизатор ISP настроен.

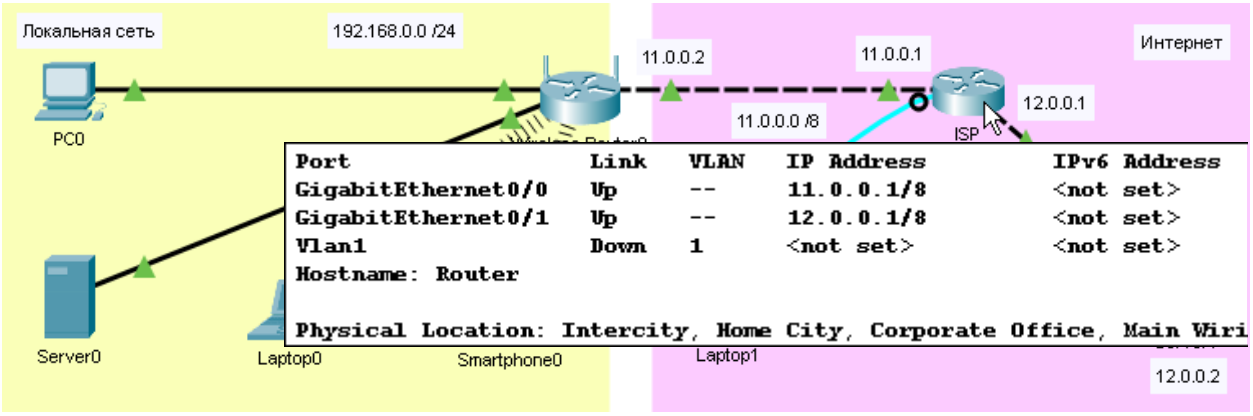


Рисунок 81 – Адреса, назначенные интерфейсам маршрутизатора ISP

Чтобы обеспечить доступ к единственному серверу, который символизирует весь интернет, нужно настроить его сетевой интерфейс. Было решено назначить ему IP-адрес: 12.0.0.2 с маской подсети 255.0.0.0. В качестве шлюза по умолчанию (Default Gateway) укажем адрес соответствующего интерфейса маршрутизатора ISP (IP-адрес: 12.0.0.1), иначе пакеты не смогут попадать в другие сети, из которых приходят запросы. Конфигурирование протокола IP на сервере (как на компьютере или лэптопе) выполняется в окне программы «IP Configuration», ярлык которой находится на рабочем столе устройства (закладка «Desktop») (рис. 82).

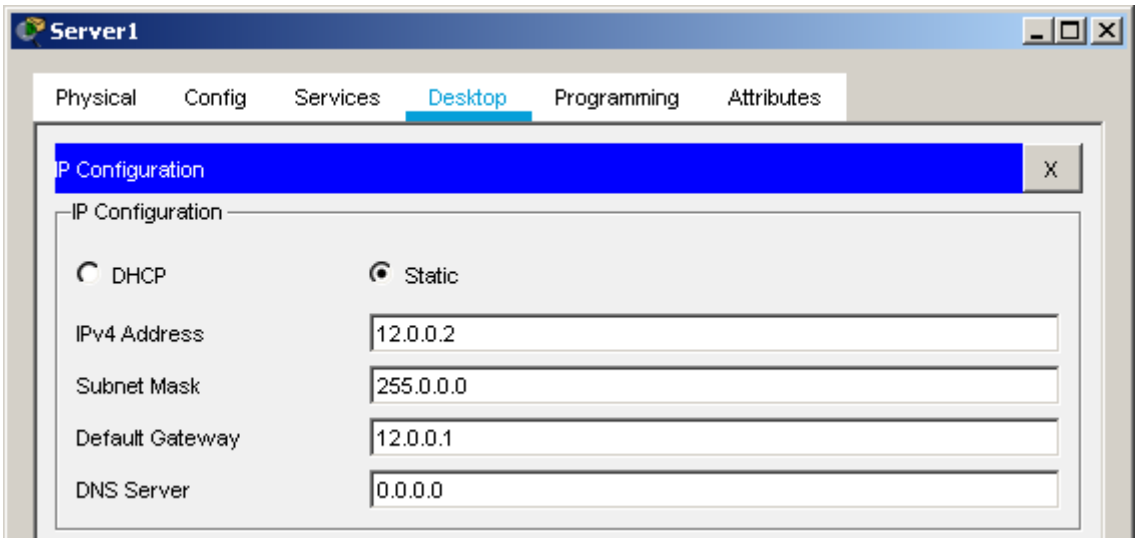


Рисунок 82 – Конфигурирование протокола IP на сервере в интернете

Таким образом, сервер в интернете настроен и готов отвечать на запросы из других сетей.

Задача 3. Настройка беспроводного маршрутизатора. Подключение проводных и беспроводных клиентов

Управление беспроводным маршрутизатором осуществляется через Web-интерфейс с любого оконечного устройства, на котором установлен Web-браузер, например, с компьютера PC0. Но сначала нужно назначить компьютеру PC0 (вернее, его сетевому интерфейсу) IP-адрес из сети 192.168.0.0 /24, причем адрес 192.168.0.1 использовать нельзя, ведь он уже назначен интерфейсу LAN беспроводного маршрутизатора. Более того, этот адрес следует указывать в качестве адреса шлюза по умолчанию.

Назначать IP-адреса узлам сети можно двумя способами: статически (вручную) или динамически. Для реализации второго способа в сети должен быть развернут DHCP-сервер, который будет предоставлять узлам сети IP-адреса в аренду. Настройка DHCP-сервера – это тема отдельного занятия, но т.к. на беспроводном маршрутизаторе есть встроенный DHCP-сервер, он определенным образом сконфигурирован и включен, т.е. готов выдавать клиентам IP-адреса в аренду, просто воспользуемся этой возможностью. Однако есть исключение. В нашей сети развернут сервер (Server0). Ему еще не назначена никакая роль (или роли), но сервер должен получить статический IP-адрес, поэтому его сетевой интерфейс сконфигурируем вручную.

В первую очередь настроим сетевой интерфейс компьютера PC0. Именно с этого компьютера будем управлять беспроводным маршрутизатором. Проводной клиент для этого лучше подходит, ведь предстоит перенастройка беспроводной сети.

Чтобы узел получил IP-адрес от DHCP-сервера, нужно в окне программы «IP Configuration» переставить радиопереключатель в положение «DHCP». Через несколько секунд интерфейс получит от DHCP-сервера параметры конфигурации: IP-адрес, маску подсети и адрес шлюза по умолчанию (рис. 83).

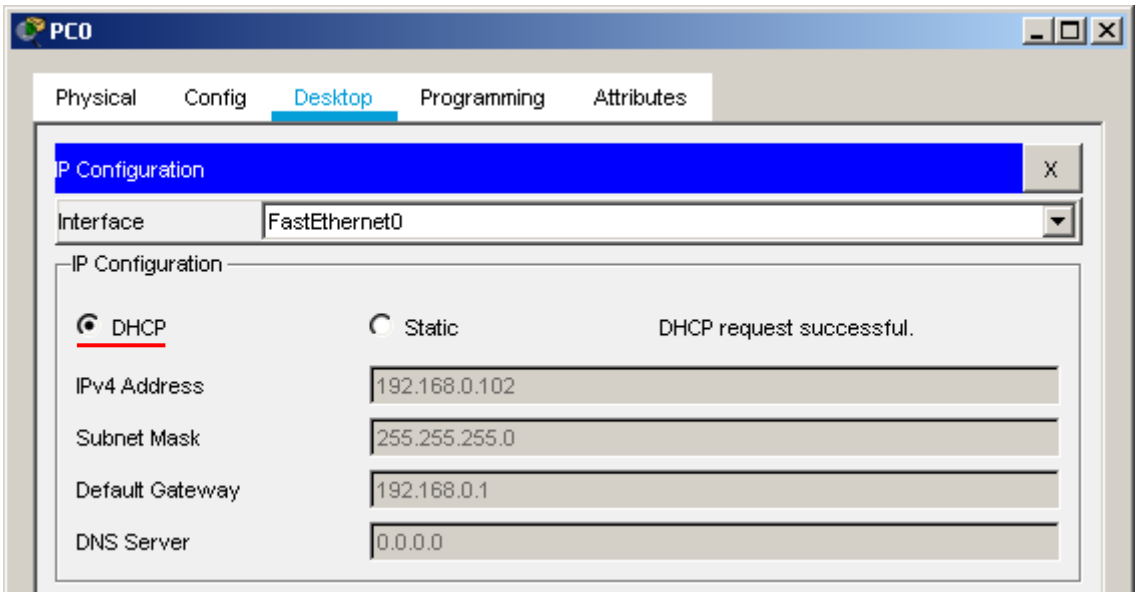


Рисунок 83 – Автоматическое конфигурирование протокола IP на PC0

Теперь можно использовать PC0 для удаленного управления беспроводным маршрутизатором. Управление осуществляется через Web-браузер. Ярлык программы «Web Browser» находится на рабочем столе компьютера (рис. 44). В адресной строке браузера (поле URL) нужно ввести IP-адрес интерфейса LAN беспроводного маршрутизатора (он же адрес шлюза по умолчанию): 192.168.0.1 и нажать кнопку «Go». Маршрутизатор предлагает пройти аутентификацию. Известно, что на устройстве создана стандартная учетная запись с именем «admin» и паролем «admin». Эти параметры нужно ввести в поля формы «Authorization» (рис. 84) и нажать «OK».

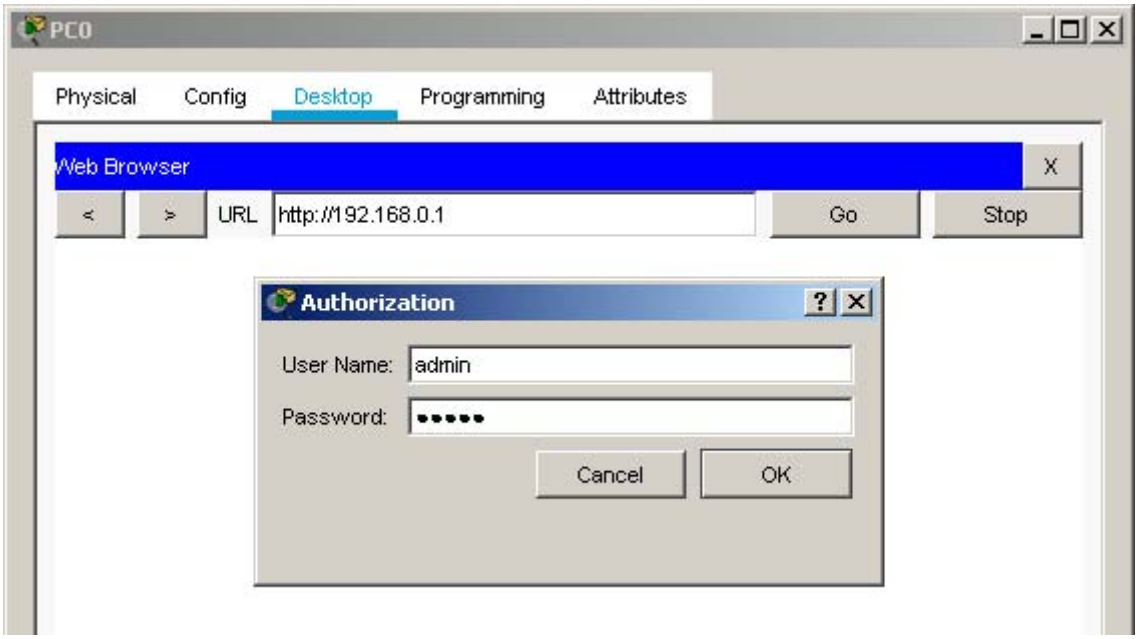


Рисунок 84 – Запрос имени пользователя и пароля при подключении к беспроводному маршрутизатору

После успешной аутентификации администратор получает доступ к Web-интерфейсу маршрутизатора, который позволяет произвести полную настройку оборудования. Поскольку беспроводной маршрутизатор является сложным многофункциональным устройством, параметры сгруппированы по разделам, а переход между разделами осуществляется с помощью кнопок или закладок на навигационной панели. У WRT300N панель навигации находится в верхней части окна, а пользователь сразу попадает на закладку «Setup» (рис. 85), где выполняются базовые настройки маршрутизатора, а именно: настройка внешнего интерфейса (Internet Setup) и встроенного DHCP-сервера (Network Setup).

Нам необходимо настроить внешний интерфейс, назначив ему IP-адрес в соответствии с планом адресации, представленном на рис. 39. По умолчанию параметр «Internet Connection type» имеет значение «Automatic Configuration – DHCP». Для большинства сетей небольших предприятий, офисов или домашних сетей это наиболее популярный вариант, когда внешний интерфейс маршрутизатора сконфигурирован на автоматическое получение IP-адреса от DHCP-сервера интернет-провайдера. Однако в нашем учебном примере предполагается ручная настройка интерфейса.

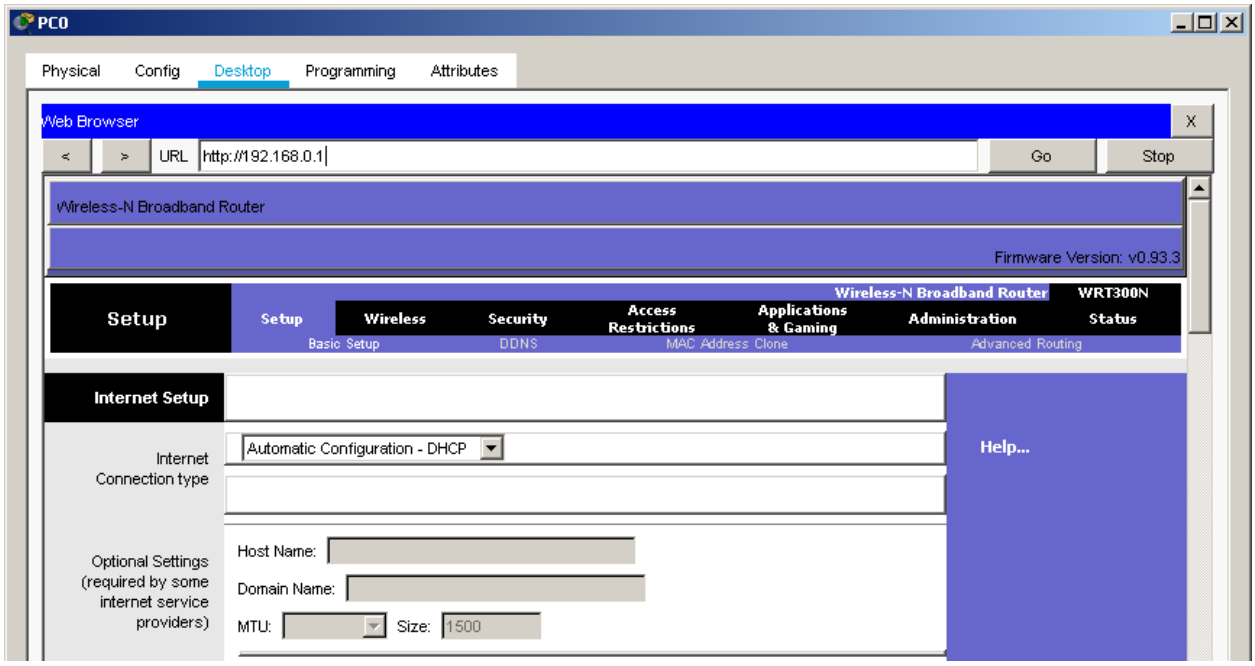


Рисунок 85 – Web-интерфейс беспроводного маршрутизатора. Раздел «Setup»

Чтобы назначить статический IP-адрес внешнему интерфейсу маршрутизатора, нужно в выпадающем списке типов соединений с интернетом (Internet Connection type) выбрать «Static IP» и ввести IP-адреса, предусмотренные планом адресации. В качестве шлюза по умолчанию указывается IP-адрес интерфейса маршрутизатора ISP, к которому подключен наш маршрутизатор (рис. 86).

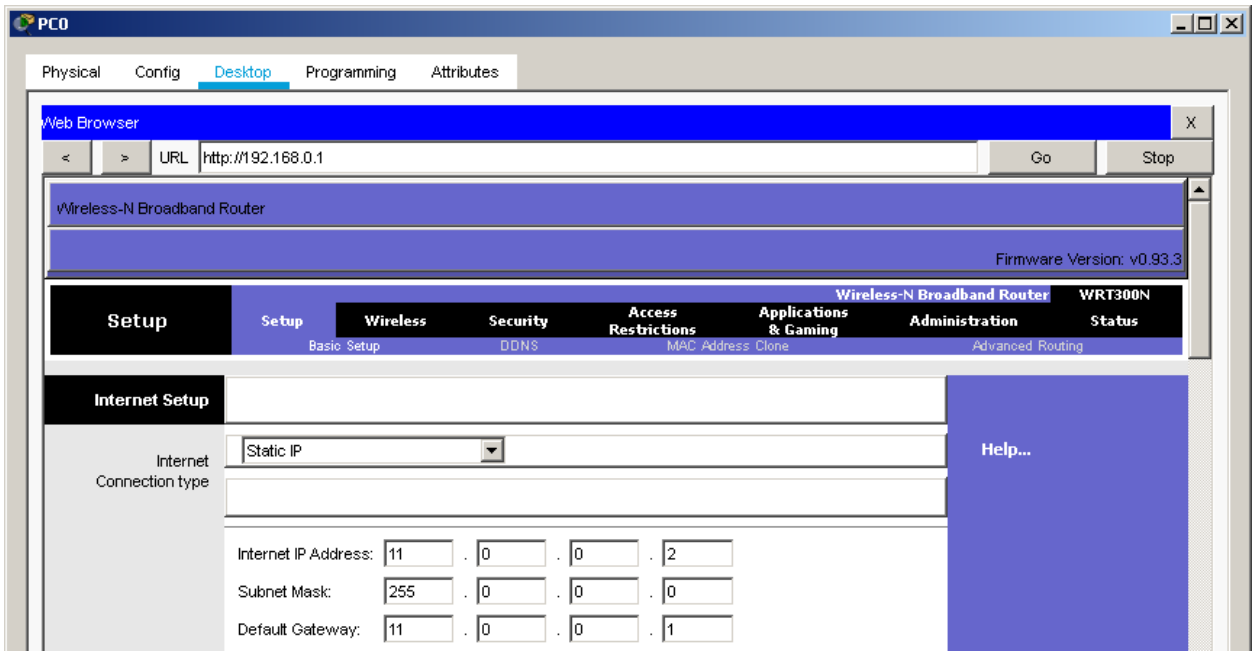


Рисунок 86 – Ручная настройка параметров протокола IP на внешнем интерфейсе беспроводного маршрутизатора

Все изменения нужно сохранять. Кнопка сохранения параметров находится в нижней части окна (рис. 87).

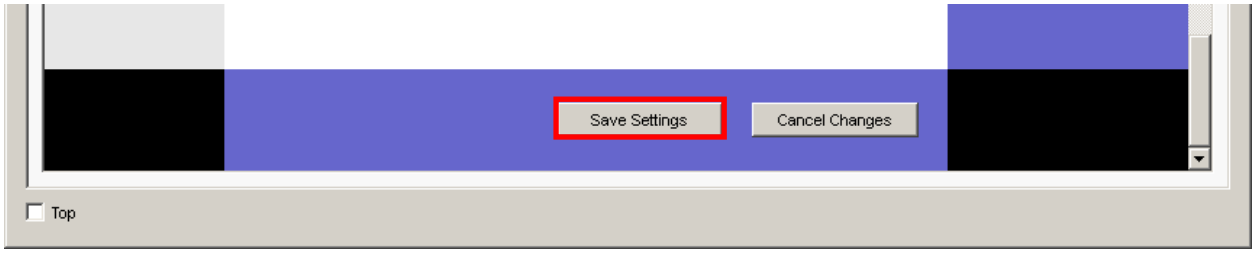


Рисунок 87 – Сохранение конфигурации маршрутизатора

Если изменения не привели к разрыву соединения, будет предложено продолжить настройки (рис. 88).

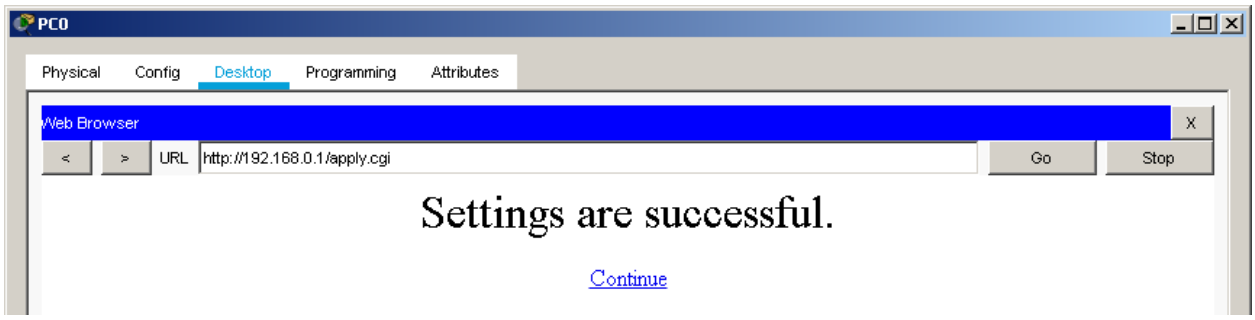


Рисунок 88 – Сообщение об успешном сохранении настроек

Переход по ссылке «Continue» возвращает администратора к Web-интерфейсу маршрутизатора. В нижней половине окна «Setup» находится область «Network Setup». Здесь настраивается локальная сеть, включая внутренний интерфейс маршрутизатора и DHCP-сервер. Настройка DHCP в рамках этого практического занятия не предусмотрена, поэтому просто проанализируем текущие («заводские») настройки (рис. 89).

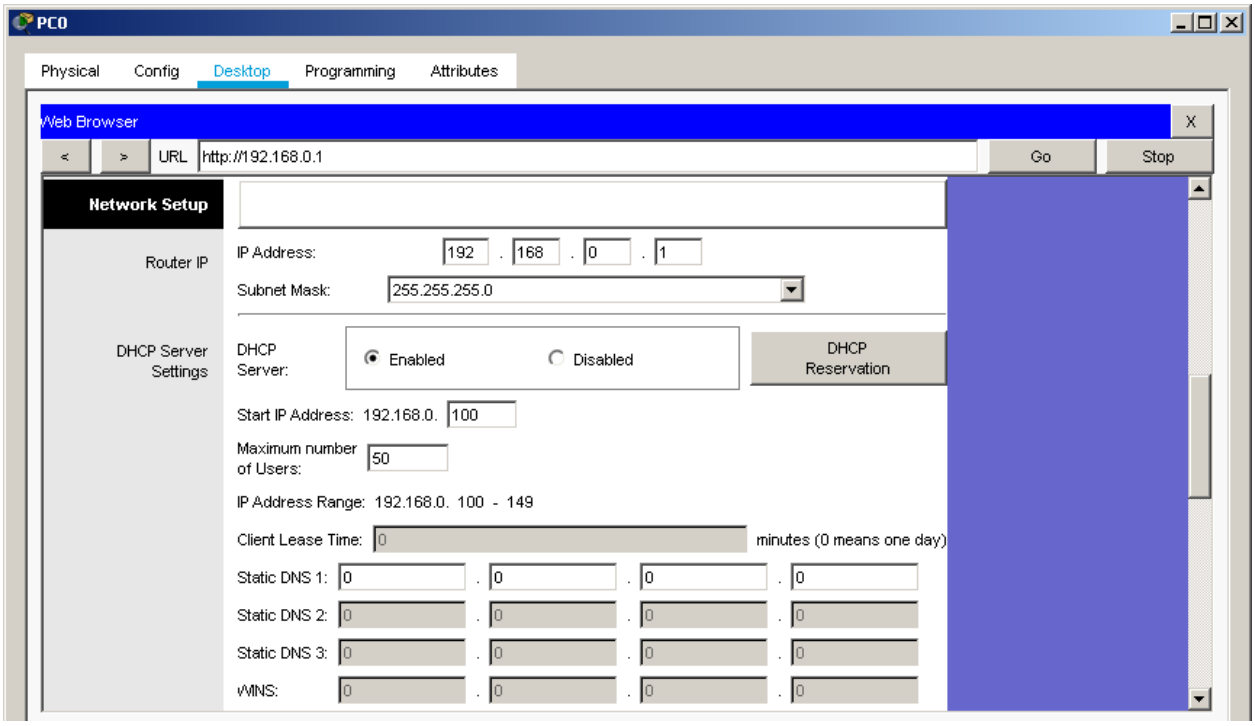


Рисунок 89 – Область настройки локальной сети

Итак, по умолчанию DHCP-сервер включен и предлагает в аренду 50 IP-адресов с 192.168.0.100 по 192.168.0.149. Клиенту передается IP-адрес, маска подсети (255.255.255.0) и адрес шлюза по умолчанию (192.168.0.1). Поскольку IP-адрес сервера DNS не указан, он клиенту не передается. На рисунке 83 показаны настройки протокола IP, которые получил компьютер PC0, как только стал клиентом DHCP.

Поскольку беспроводные узлы по умолчанию настроены на автоматическое получение параметров IP от DHCP-сервера, сетевые интерфейсы лэптопа и смартфона уже сконфигурированы. Это отобразится на всплывающей подсказке, появляющейся при наведении указателя мыши на оконечное устройство, например, на Laptop0 (рис. 90).

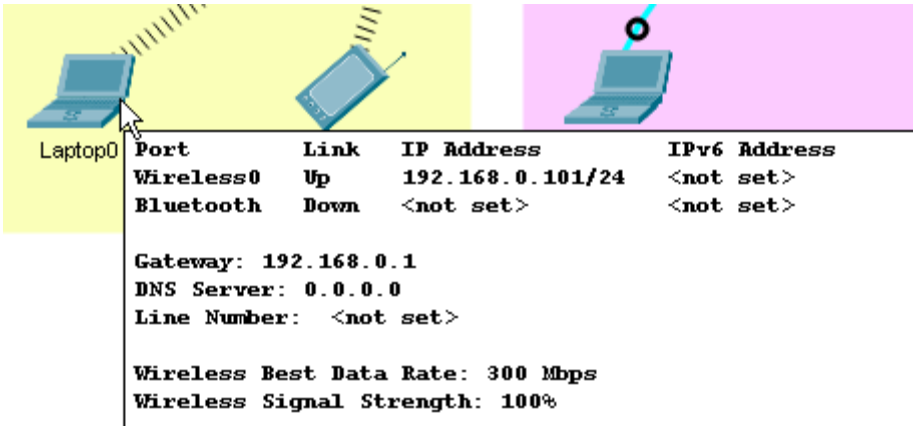


Рисунок 90 – Параметры протокола IP сетевых интерфейсов лэптопа

Таким образом, три узла локальной сети являются клиентами DHCP, т.е. получили IP-адреса от DHCP-сервера, развернутого на беспроводном маршрутизаторе. Сетевой интерфейс сервера (Server0) получит статический IP-адрес. Настроим его позже.

Продолжим конфигурировать беспроводной маршрутизатор. Настроим беспроводную сеть. Для этого перейдем на закладку «Wireless» (рис. 91).

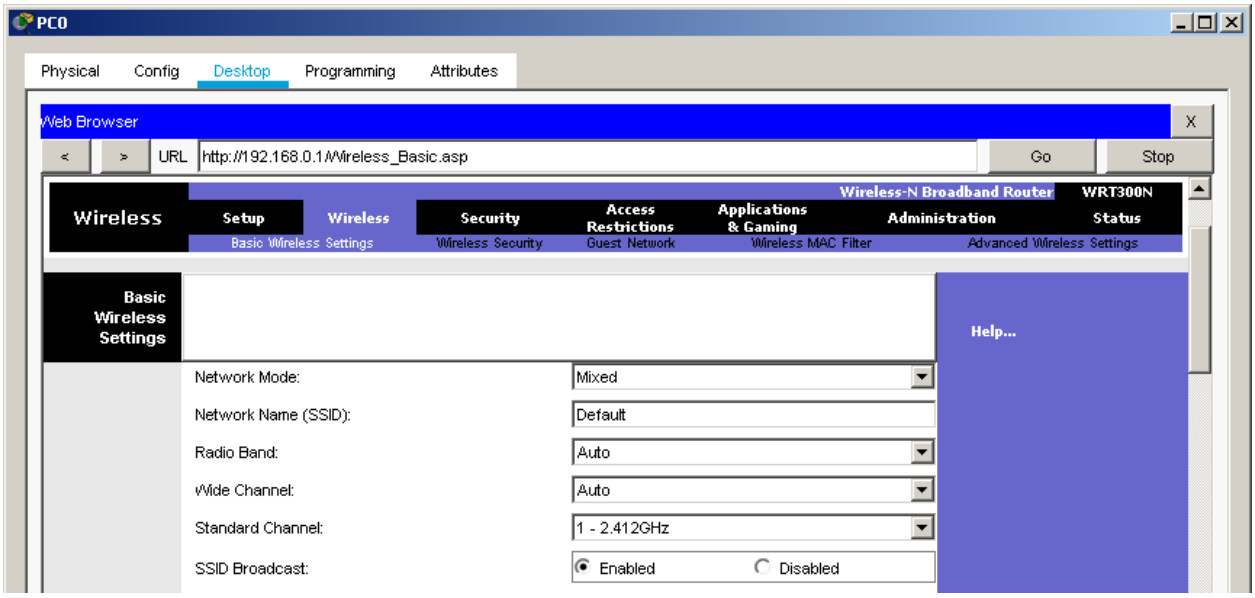


Рисунок 91 – Область настройки беспроводной сети

Назначим имя (SSID) беспроводной сети, например: WRNET. Остальные параметры имеют значение только в реальных условиях, поэтому их можно оставить без изменений (рис. 92).

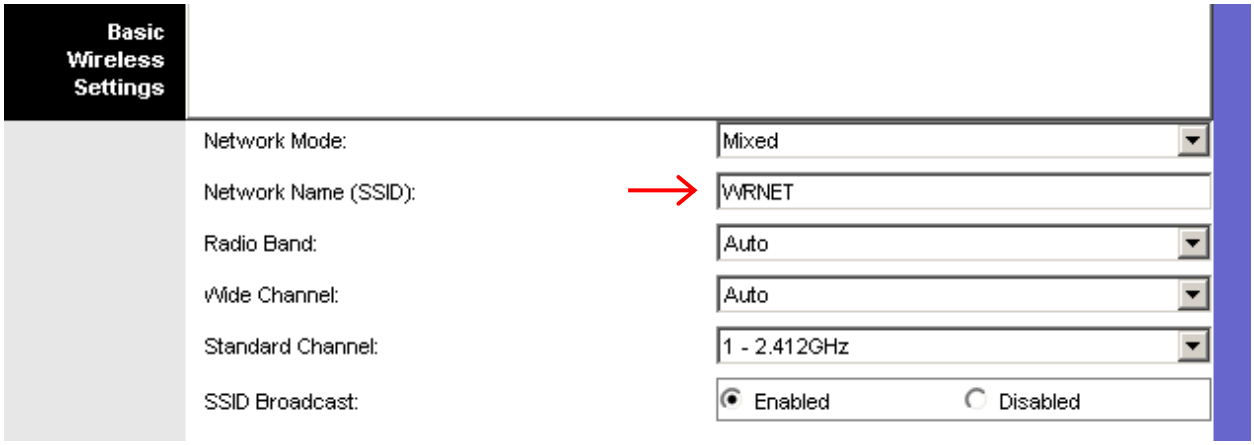


Рисунок 92 – Назначение имени беспроводной сети

Изменения нужно сохранить, нажав кнопку «Save Settings» в нижней части окна, как показано на рисунке 87.

Теперь следует защитить беспроводную сеть. Безопасность сети настраивается в подразделе «Wireless Security». По умолчанию сеть является открытой, т.е. при подключении устройств аутентификация пользователей не проводится, что создает серьезную угрозу безопасности (рис. 93).

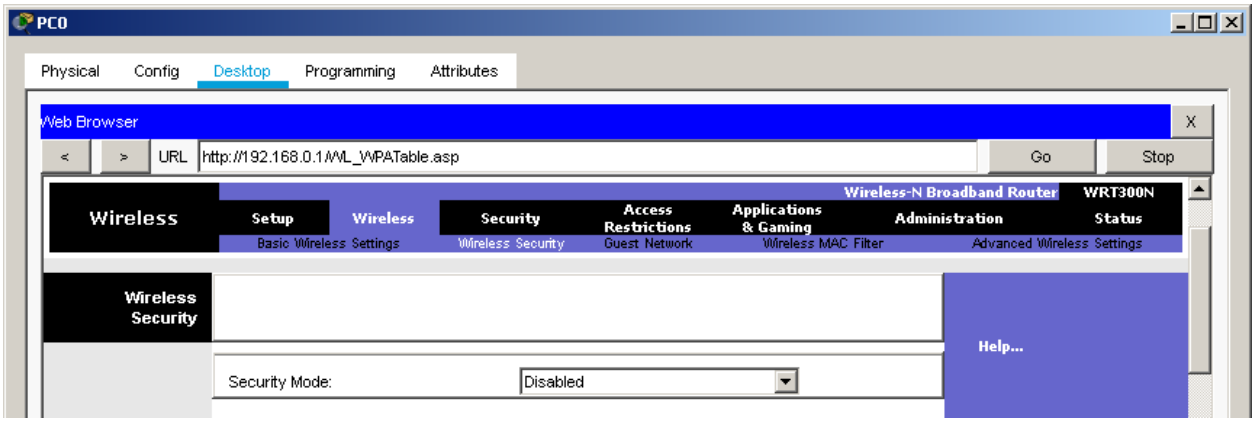


Рисунок 93 – Беспроводная сеть по умолчанию не защищена

Наиболее продвинутым из доступных вариантов защиты является «WPA2 Enterprise», однако он требует развертывания в сети сервера аутентификации, поэтому выберем режим безопасности «WPA2 Personal» (рис. 94), который часто используется в беспроводных сетях небольших предприятий, офисов и в домашних сетях. При использовании персонального метода аутентификации WPA2 пользователи проходят аутентификацию на беспроводном маршрутизаторе с использованием предварительного общего ключа (PSK). Специализированный сервер аутентификации не требуется.

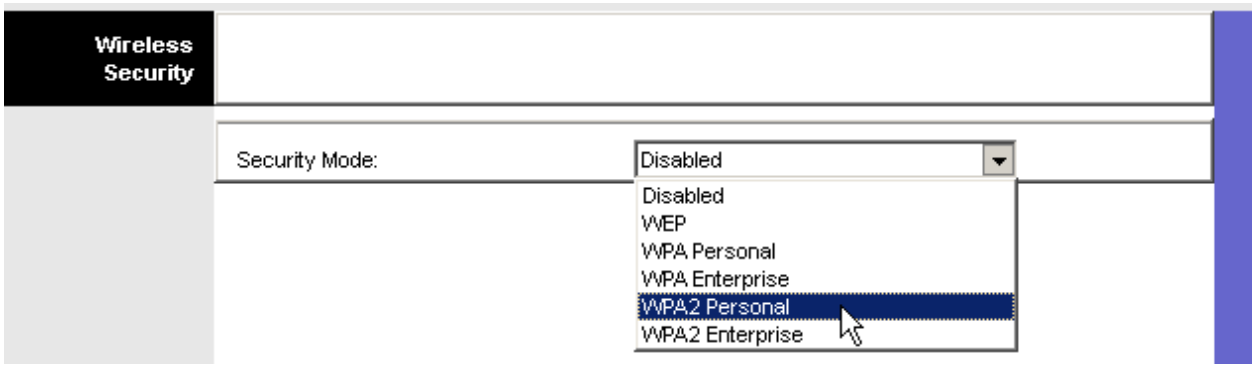


Рисунок 94 – Выбор режима безопасности

После выбора режима безопасности «WPA2 Personal» в подразделе «Wireless Security» появляются возможность выбора алгоритма шифрования (TKIP или AES) и поле для задания пароля (Passphrase). Выбираем алгоритм **AES**, т.к. он является более надежным. Пароль должен быть сложным и включать не менее восьми символов. В учебных целях будем использовать простой пароль, например, **cisco123** (рис. 95). Разумеется, в реальной сети такой пароль использовать категорически не рекомендуется.

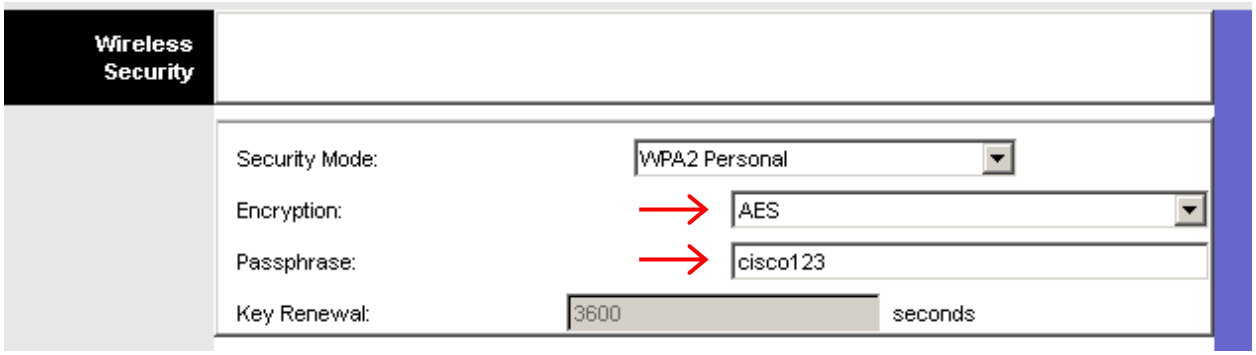


Рисунок 95 – Выбор алгоритма шифрования и задание пароля

Сохраняем изменения нажатием кнопки «Save Settings» в нижней части окна, как показано на рисунке 87.

Таким образом, базовые настройки беспроводного маршрутизатора выполнены.

Поскольку беспроводная сеть перенастроена и защищена, беспроводные оконечные устройства (лэптоп и смартфон) потеряли связь с маршрутизатором. Их нужно переподключить, используя общий ключ.

Начнем с лэптопа. Запускаем программу «PC Wireless». Ярлык программы находится на рабочего столе лэптопа (рис. 96). Окно программы имеет несколько закладок. На закладке «Link Information» выводится информация о состоянии соединения и статусе беспроводного сетевого адаптера. Видно, что связь с точкой доступа отсутствует, а сетевой адаптер неактивен (рис. 97). На закладке «Profiles» можно создать и настроить несколько профилей для подключения к разным сетям, использующих различные методы аутентификации. Кроме того, только создав профиль, можно настроить доступ к беспроводной сети, которая использует режим безопасности «WPA2 Enterprise».

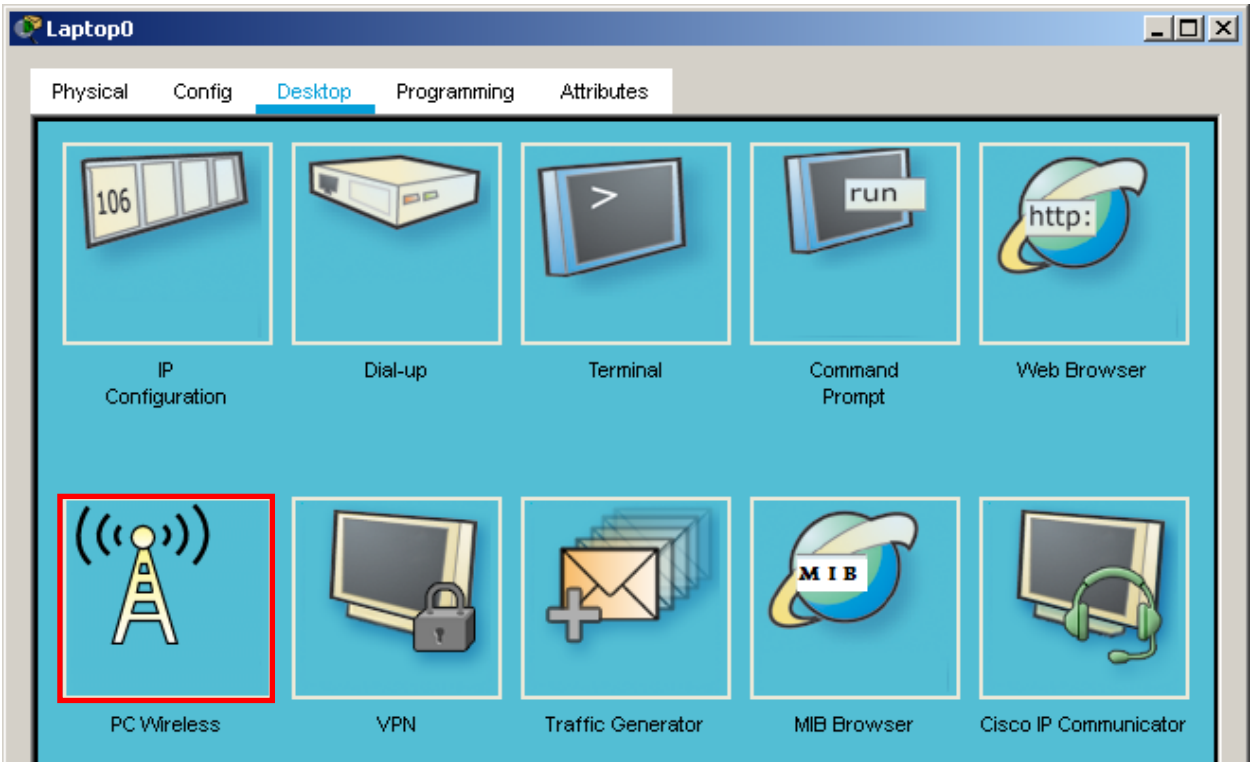


Рисунок 96 – Ярлык программы настройки беспроводной сети на оконечном устройстве

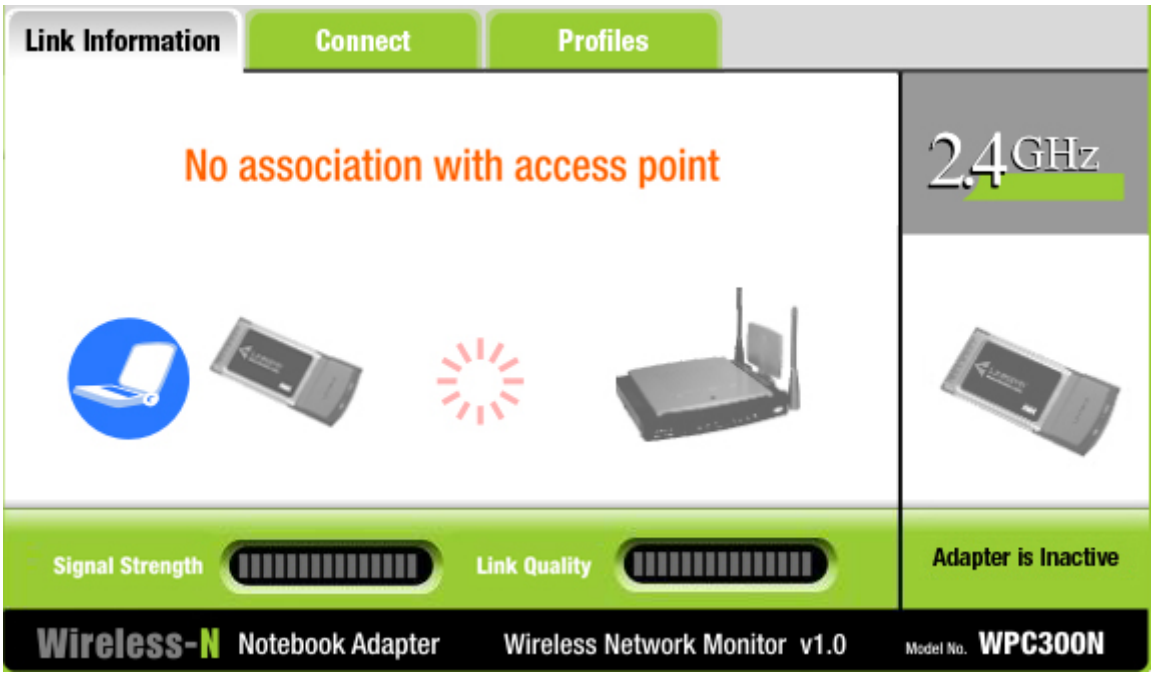


Рисунок 97 – Окно программы беспроводного адаптера «PC Wireless»

Подключение к беспроводной сети при использовании выбранного нами режима безопасности «WPA2 Personal» проще всего настроить на закладке «Connect». В левой части окна выводится список сетей. В списке наблюдается единственная сеть WRNET, которая была настроена на беспроводном маршрутизаторе. В правой части окна в поле «Site Information» выводится информация о настройках, в том числе режим безопасности «WPA2-PSK», т.е. WPA2 Personal (рис. 98).

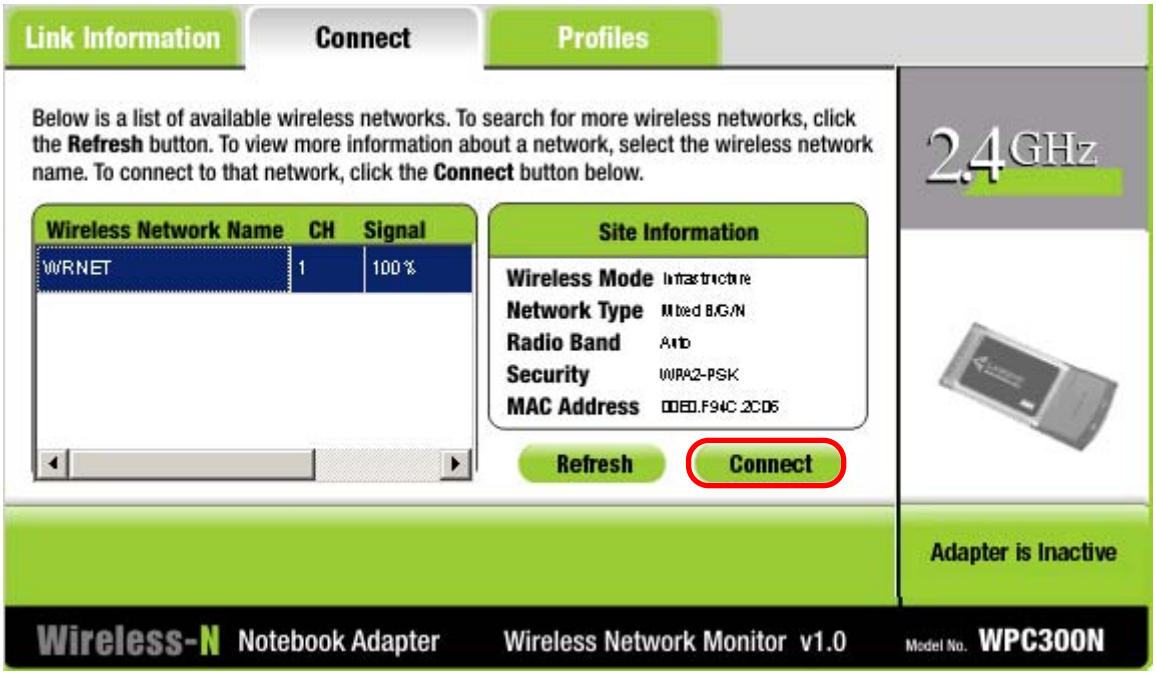


Рисунок 98 – Информация о доступных сетях на закладке «Connect»

Чтобы подключиться к сети WRNET, нужно нажать зеленую кнопку «Connect», а в новом окне ввести в поле «Pre-shared Key» общий ключ **cisco123** и снова нажать «Connect» в правом нижнем углу окна (рис. 99).

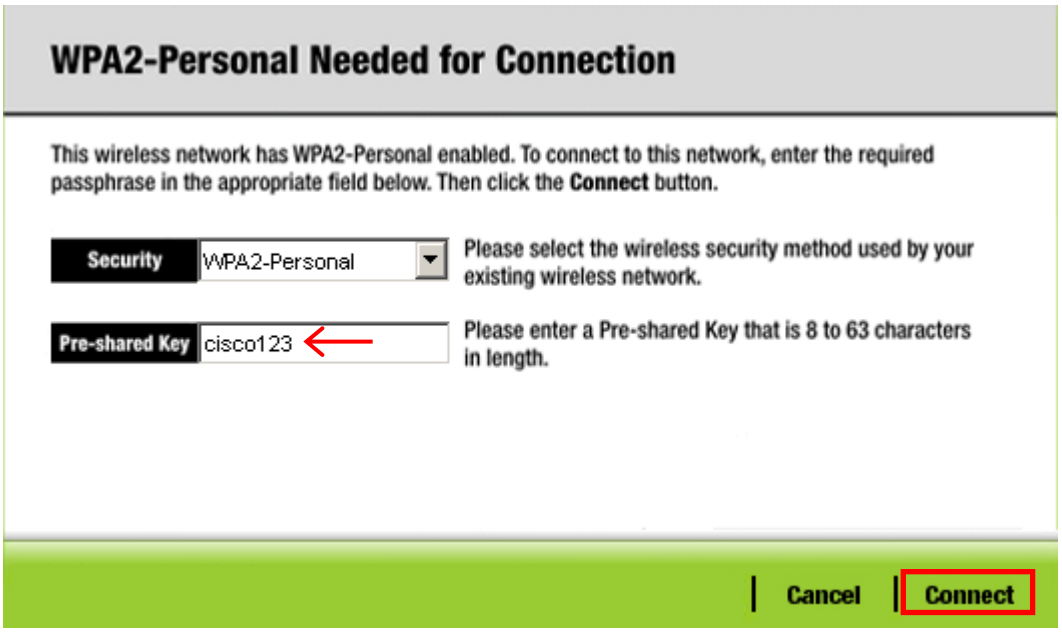


Рисунок 99 – Ввод общего ключа и подключение к сети

В результате статус сетевого адаптера поменялся на «Adapter is Active», а на закладке «Link Information» сообщается об успешном подключении к беспроводной сети (рис. 100). Линия связи между лэптопом и беспроводным маршрутизатором на рабочем поле восстановилась.

Теперь подключим смартфон к беспроводной сети. Технология подключения несколько отличается, поскольку на смартфоне нет программы «PC Wireless» и соответствующего ярлыка на рабочем столе.

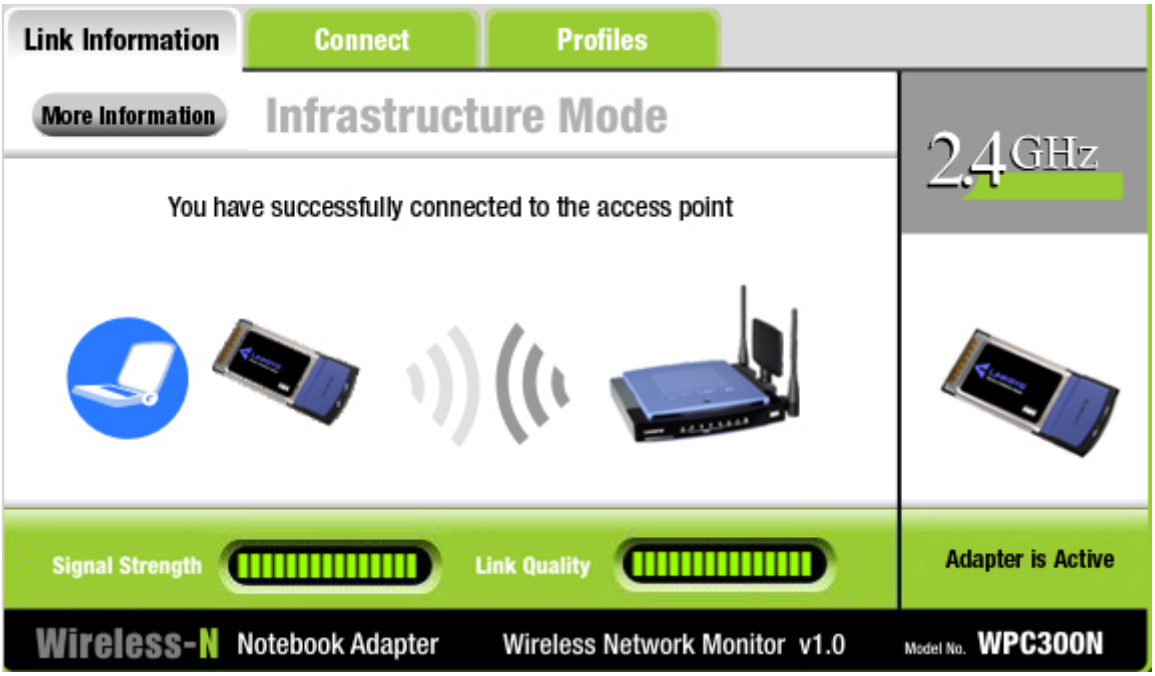


Рисунок 100 – Успешное подключение устройства к беспроводной сети

Настройки сетевого интерфейса осуществляются на закладке «Config» смартфона в окне «Wireless0» (рис. 101).

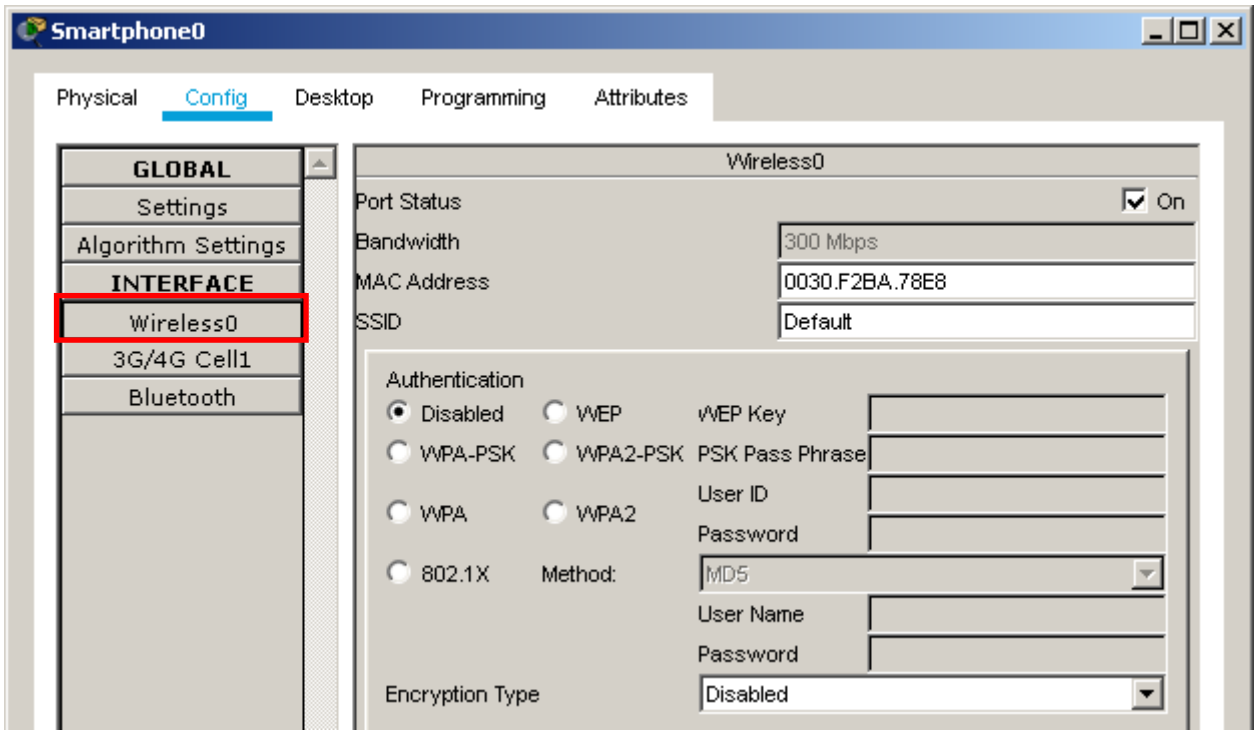


Рисунок 101 – Область настройки беспроводного интерфейса на смартфоне

Имя беспроводной сети (WRNET) придется ввести вручную. Радиопереключатель «Authentication» нужно перевести в положение «WPA2-PSK» и в поле «PSK Pass Phrase» ввести общий ключ **cisco123**. В выпадающем списке «Encryption Type» следует выбрать вариант «AES» (рис. 102).

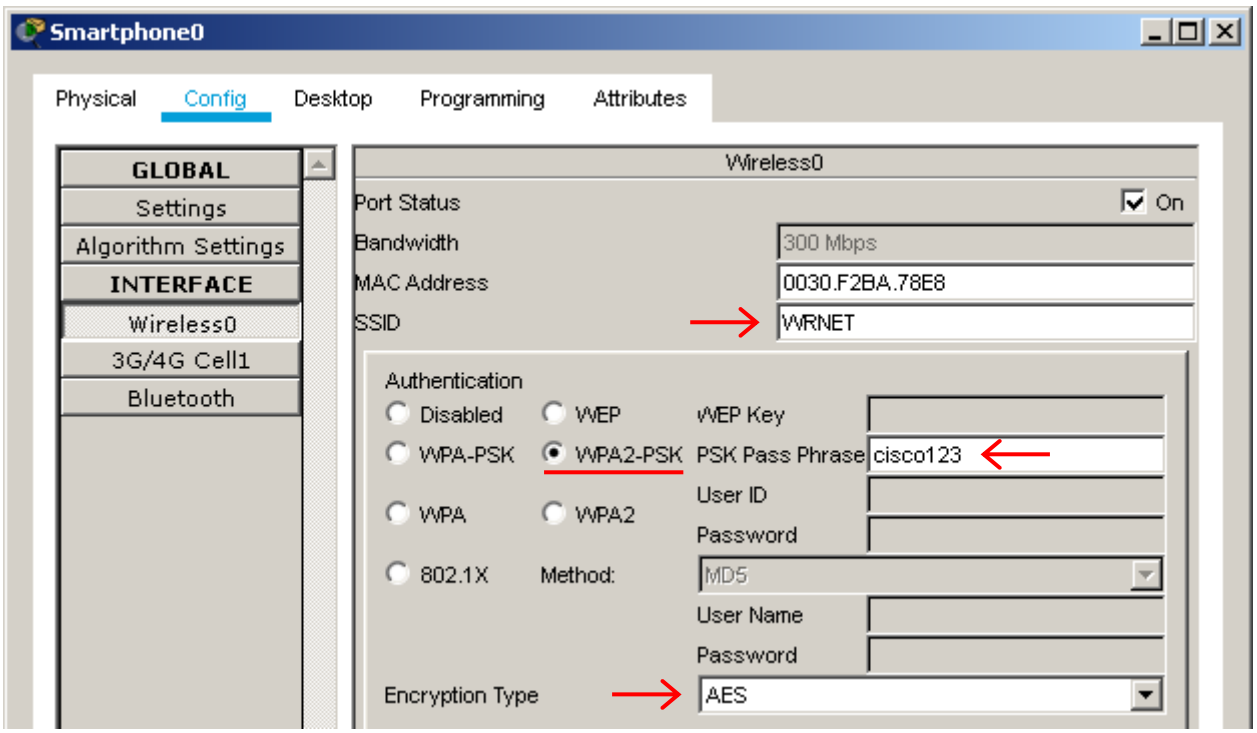


Рисунок 102 – Настройка беспроводного интерфейса на смартфоне

После выполнения настроек и закрытия или сворачивания окна связь между смартфоном и беспроводным маршрутизатором восстановится.

Настройку сетевого интерфейса сервера локальной сети (Server0), как и планировали, выполним вручную. IP-адрес должен принадлежать сети 192.168.0.0 /24, причем адрес 192.168.0.1 назначать нельзя, т.к. он является адресом шлюза по умолчанию. Не стоит использовать адреса из пула DHCP-сервера (50 адресов с 192.168.0.100 по 192.168.0.149). Назначим сетевому интерфейсу сервера IP-адрес: 192.168.0.10 (рис. 103).

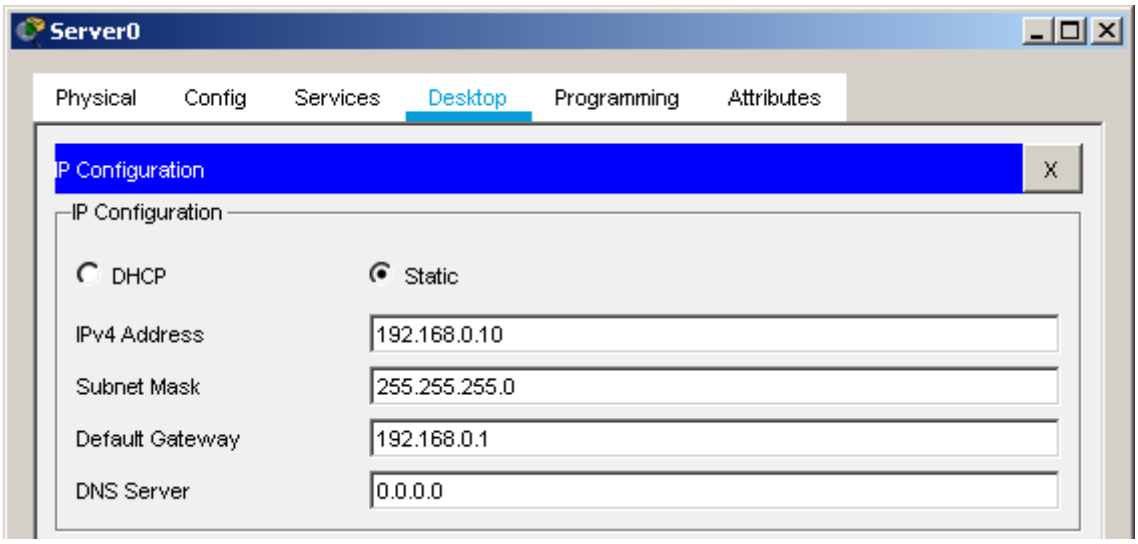


Рисунок 103 – Конфигурирование протокола IP на сервере локальной сети

Таким образом, беспроводные клиенты подключены к сети WRNET, сетевые интерфейсы получили IP-адреса от DHCP-сервера, сервер локальной сети получил статический IP-адрес. Это значит, что узлы сети могут взаимо-

действовать друг с другом и с компьютерами в других сетях, в том числе в интернете. Для проверки доступности узлов используется программа «ping», которая запускается из командной строки. Ярлык «Command Prompt» есть на рабочем столе любого оконечного устройства в нашей сети. Проверим связь смартфона с компьютерами в локальной сети.

IP-адреса для эхо-тестирования:

- PC0: 192.168.0.102 (рис. 83);
- Laptop0: 192.168.0.101 (рис. 90);
- Server0: 192.168.0.10 (рис. 103).

Результаты проверки доступности представлены на рисунках 104 и 105.

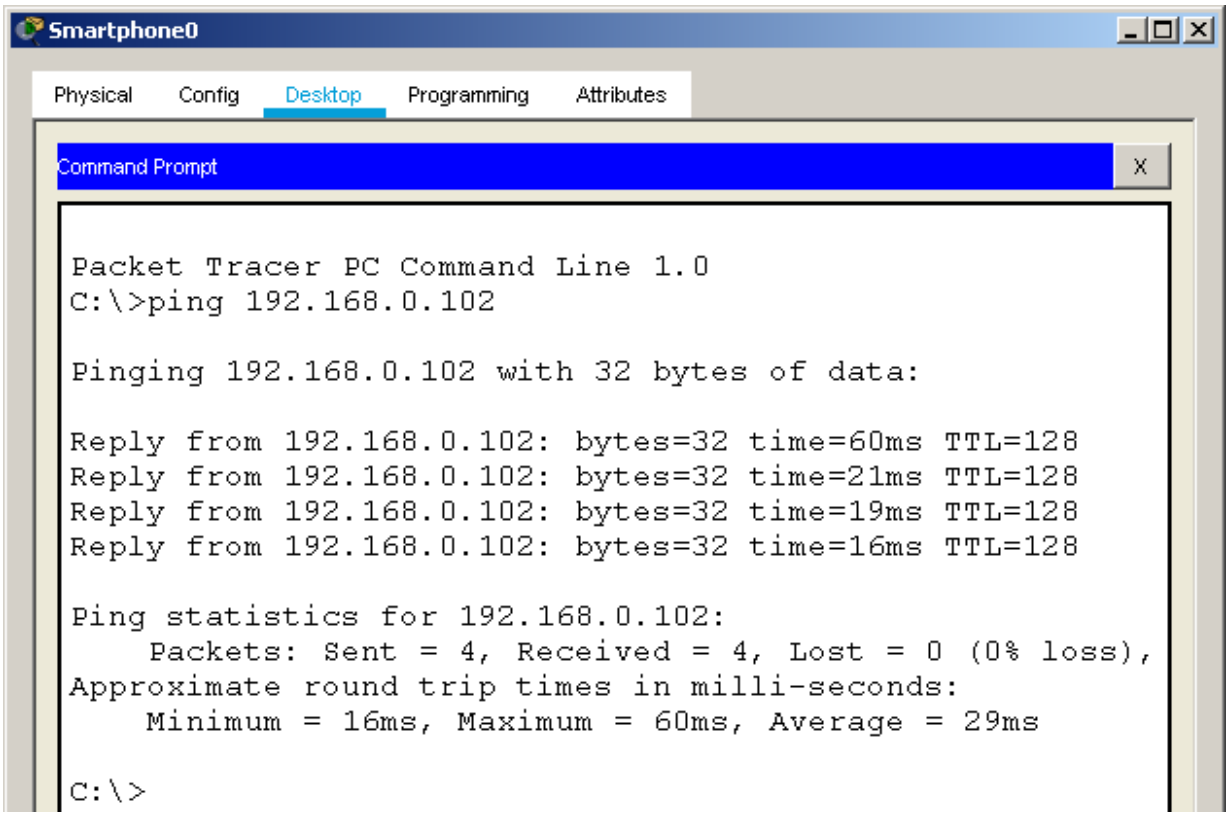


Рисунок 104 – Успешный результат проверки доступности PC0

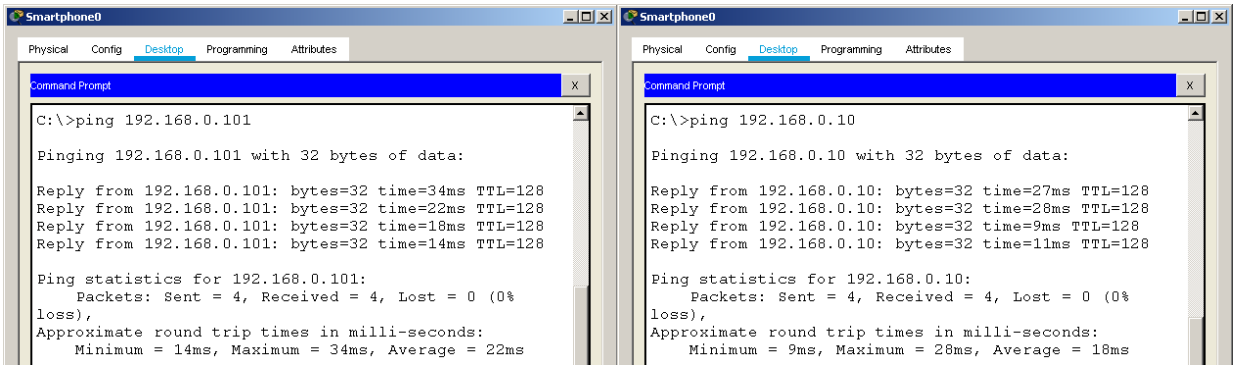


Рисунок 105 – Успешный результат проверки доступности Laptop0 и Server0

Следовательно, узлы в локальной сети могут обмениваться информацией друг с другом.

Теперь проверим доступность узла, имитирующего сервер в интернете. Отправим эхо-запрос на IP-адрес: 12.0.0.2. Результат проверки доступности представлен на рисунке 106.

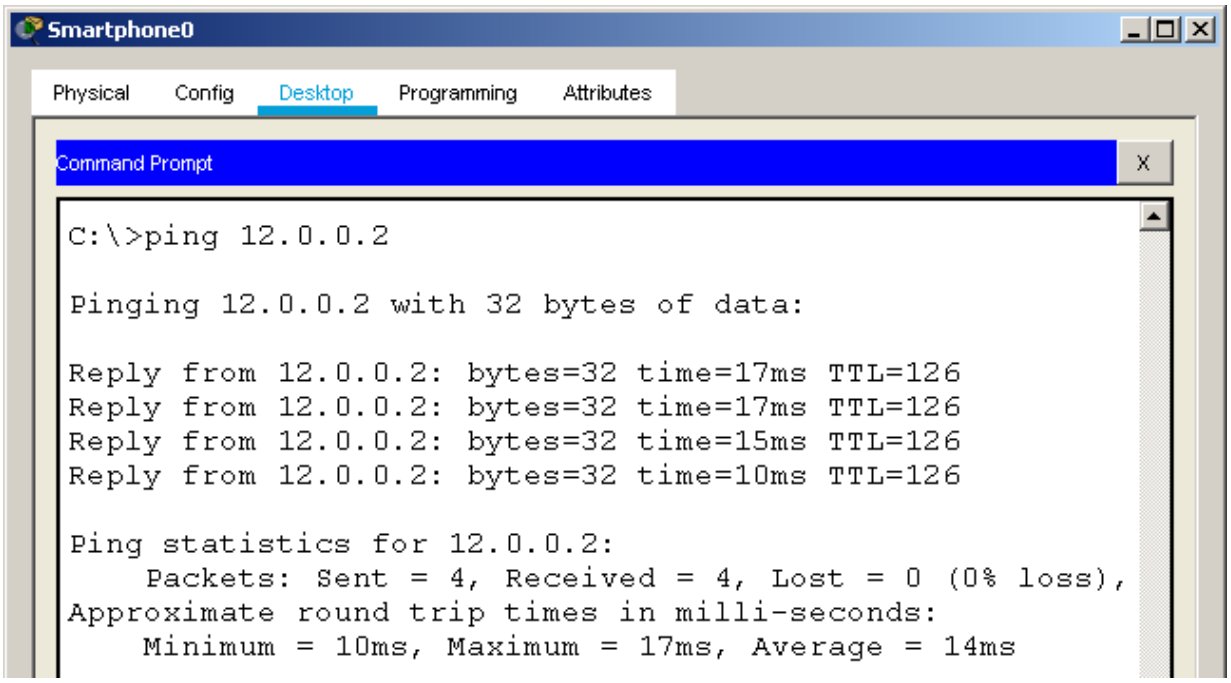


Рисунок 106 – Успешная проверка доступности сервера в интернете

Сымитируем обращение к Web-серверу в интернете. Для этого введем IP-адрес сервера Server1 (12.0.0.2) в поле «URL» интернет-обозревателя какого-либо узла в локальной сети, например, компьютера PC0. Нажмем «Go». Ответ Web-сервера получен (рис. 107).

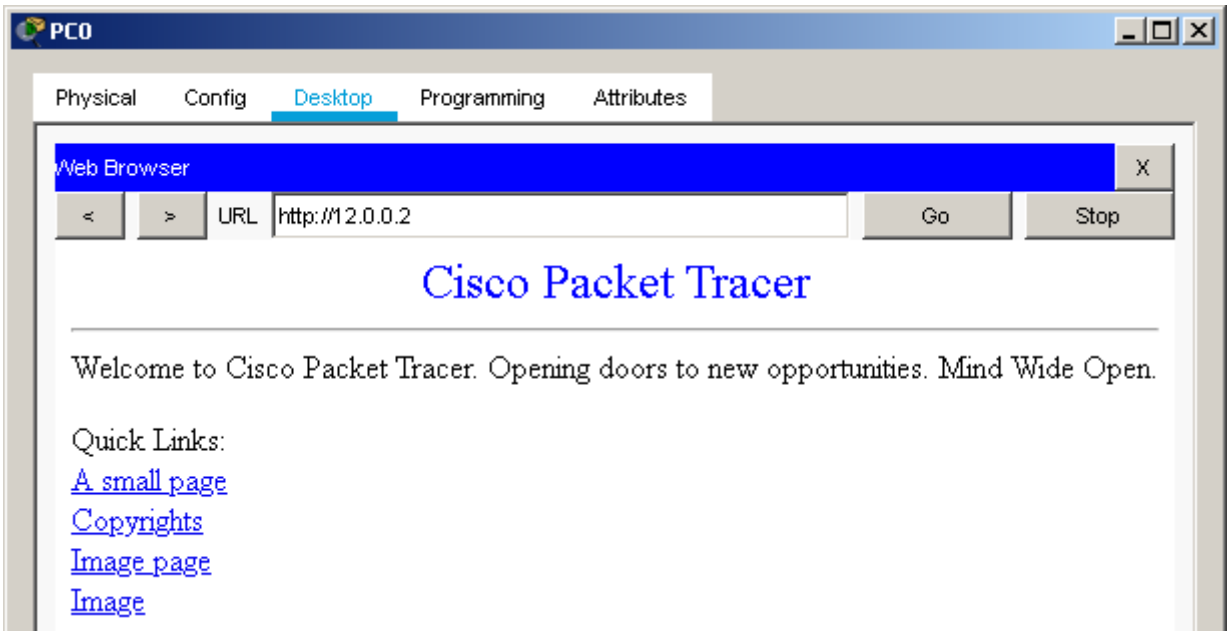


Рисунок 107 – Доступ к Web-серверу в интернете обеспечен

Таким образом, беспроводной маршрутизатор настроен. Проводные и беспроводные клиенты могут взаимодействовать в локальной сети и выходить в интернет.

Практическое занятие №3
Настройка сетевых служб

Задача 1. Настройка DHCP-сервера на беспроводном маршрутизаторе

Конфигурирование беспроводного маршрутизатора, реализованное в рамках 3-й задачи Практического занятия №2, не включало перенастройку DHCP-сервера. Он использовался, сетевые интерфейсы трех узлов в локальной сети получили динамические IP-адреса, однако «заводские» настройки сервера DHCP не менялись.

В ходе решения данной задачи предстоит настроить, вернее, перенастроить DHCP-сервер на беспроводном маршрутизаторе WRT300N, который стал центральным устройством сети, созданной при выполнении Практического занятия №2 (рис. 75).

Настроим DHCP-сервер следующим образом:

- локальная сеть: 192.168.30.0 /24;
- пул адресов, из которого будут выдаваться в аренду IP-адреса: 192.168.30.20 … 192.168.30.29 (10 адресов);
- IP-адрес интерфейса «LAN» маршрутизатора (т.е. адрес шлюза по умолчанию для всех узлов сети): 192.168.30.1;
- IP-адрес DNS-сервера, который будет передаваться клиентам вместе с IP-адресом сетевого интерфейса и адресом шлюза по умолчанию: 8.8.8.8;
- сетевой интерфейс лэптопа (Laptop0) должен всегда получать IP-адрес: 192.168.30.50 (т.е. этот адрес должен быть зарезервирован).

Поскольку меняется номер локальной сети, сетевому интерфейсу сервера (Server0) нужно назначить новый статический IP-адрес: 192.168.30.10

Измененный проект сети небольшого предприятия с учетом изменения адресов в локальной сети представлен на рисунке 108.

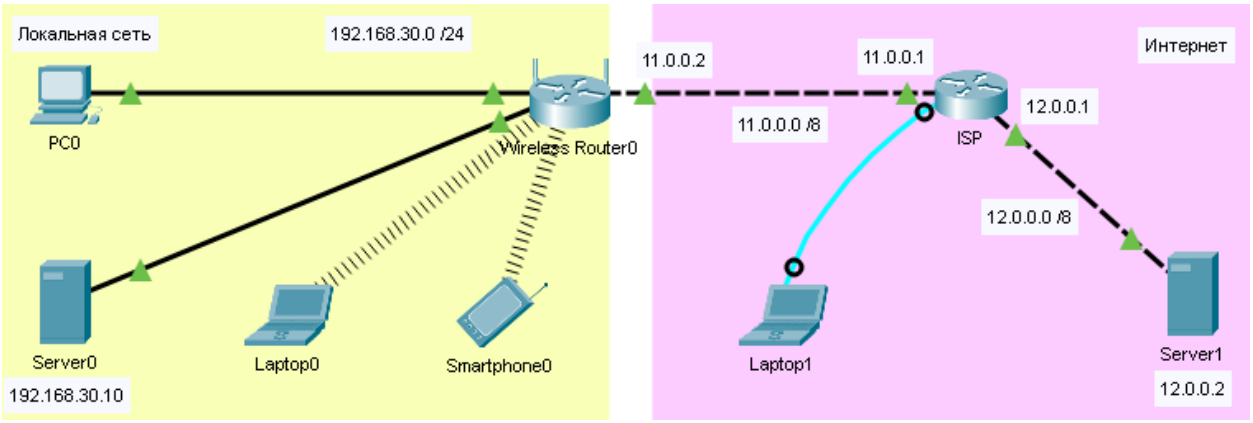


Рисунок 108 – Модель сети предприятия с новым планом адресации

Поскольку управление маршрутизатором осуществляется через Web-интерфейс, настройку DHCP-сервера можно выполнить с любого узла локальной сети, например, с компьютера PC0.

Запуск Web-браузера осуществляется с рабочего стола компьютера (рис. 44). В адресной строке обозревателя нужно ввести IP-адрес внутреннего

интерфейса маршрутизатора: 192.168.0.1 и нажать кнопку «Go», а затем параметры учетной записи администратора (имя: **admin**, пароль: **admin**), как показано на рисунке 84. Web-интерфейс маршрутизатора представит окно «Setup». В нижней части этого окна находится область «Network Setup», предназначенная для настройки локальной сети и сервера DHCP (рис. 109).

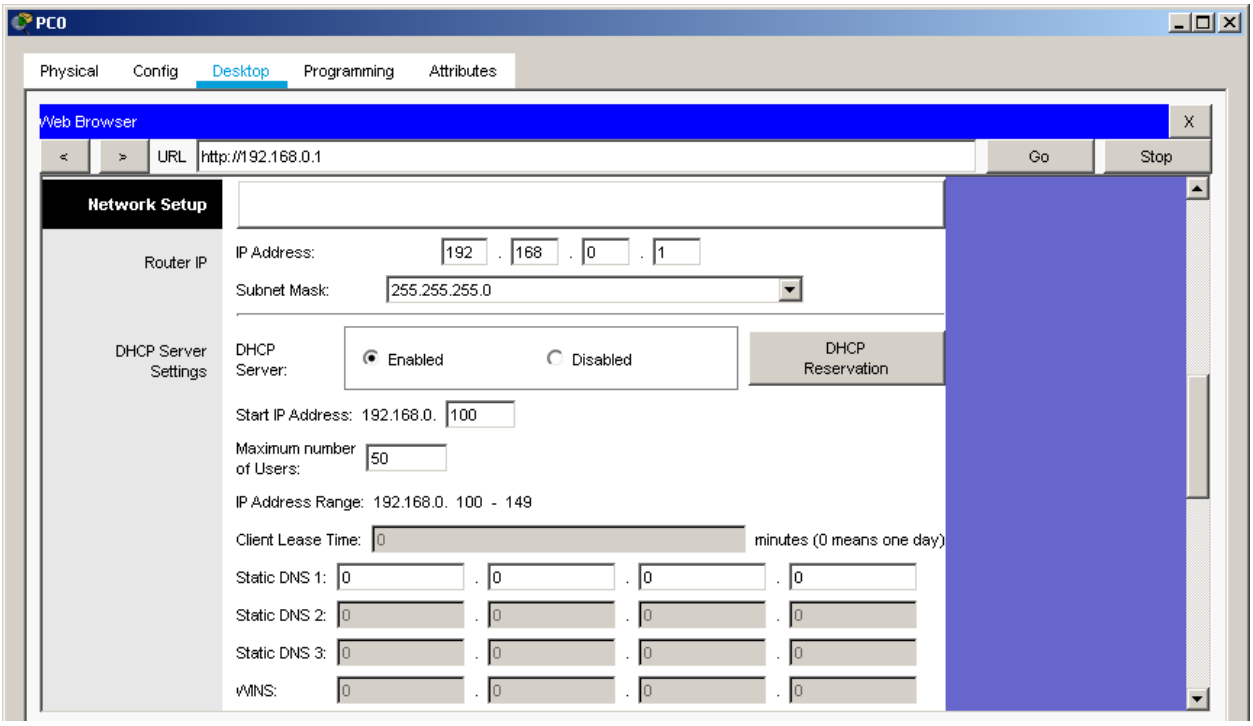


Рисунок 109 – Область настройки локальной сети и DHCP-сервера

Сделаем запланированные настройки (рис. 110).

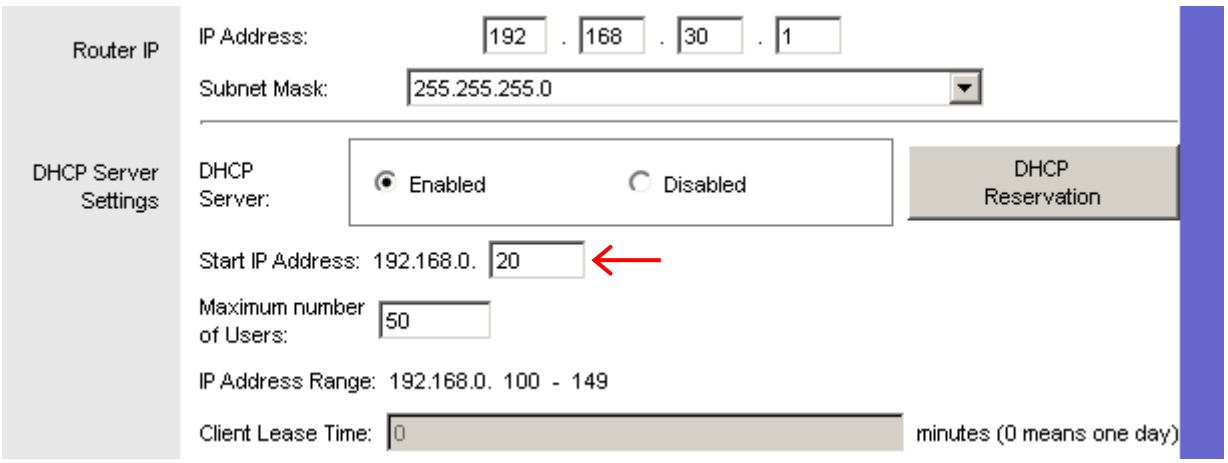


Рисунок 110 – Изменение начального IP-адреса пула адресов

В подразделе «Router IP» изменим «IP Address» на 192.168.30.1 (это адрес внутреннего интерфейса маршрутизатора, он является адресом шлюза по умолчанию). Маску подсети 255.255.255.0 (соответствует префиксу /24) оставим без изменения.

Переходим в подраздел «DHCP Server Settings».

Резервирование («DHCP Reservation») пока пропускаем. Настроим в последнюю очередь.

Начальный IP-адрес пула адресов («Start IP Address»): 192.168.30.20. Вместо «100» в последнем октете вводим «20». Однако изменить третий октет (с «0» на «30») не представляется возможным.

Если сохранить настройки, то значение третьего октета «исправится» автоматически таким образом, чтобы пул адресов и IP-адрес внутреннего интерфейса маршрутизатора были из одной сети 192.168.30.0 /24, т.е. «0» в третьем октете сам поменяется на «30». Убедимся в этом. Нажмем «Save Settings» в нижней части окна (рис. 87). Через несколько секунд Web-интерфейс маршрутизатора сообщит о разрыве связи с компьютером PC0 (рис. 111).

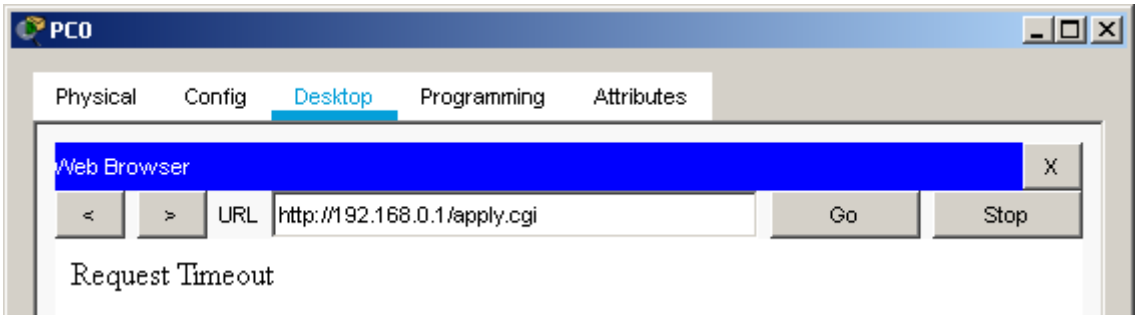


Рисунок 111 – Сообщение маршрутизатора о потере соединения

Причина потери связи понятна – был изменен IP-адрес внутреннего интерфейса маршрутизатора. Чтобы восстановить доступ к Web-интерфейсу маршрутизатора, нужно указать в адресной строке браузера новый адрес (192.168.30.1). Но этого недостаточно, соединение не восстанавливается, браузер снова выводит сообщение «Request Timeout» (рис. 112).

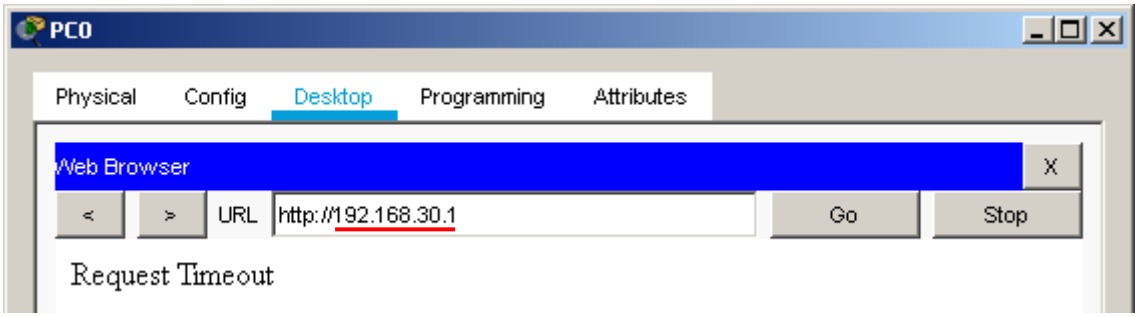


Рисунок 112 – Соединение не восстанавливается

Почему же не удается получить доступ к Web-интерфейсу маршрутизатора по новому IP-адресу? Дело в том, что сетевой интерфейс компьютера PC0 пока использует старые настройки, полученные в аренду от сервера DHCP до его перенастройки. Причем IP-адреса компьютера PC0 (192.168.0.102 /24) и маршрутизатора (192.168.30.1 /24) принадлежат разным сетям, поэтому эти устройства не могут обмениваться информацией, ведь физически они находятся в одной сети. Чтобы исправить ситуацию, сетевой интерфейс компьютера PCO должен получить новый IP-адрес от перенастроенного DHCP-сервера. Поскольку срок аренды («Client Lease Time») составляет один день, сам клиент очень не скоро обратится к DHCP-серверу за новыми настройками, поэтому нужно процесс ускорить. Это можно сделать,

например, в программе «IP Configuration». Для этого нужно радио переключатель перевести в положение «Static», а затем обратно в «DHCP». Тем самым мы заставим сетевой интерфейс PC0 обратиться к DHCP-серверу за новыми настройками. Полученный IP-адрес (192.168.30.20) является первым в пуле, поскольку PC0 стал первым клиентом. Также изменился адрес шлюза по умолчанию (рис. 113).

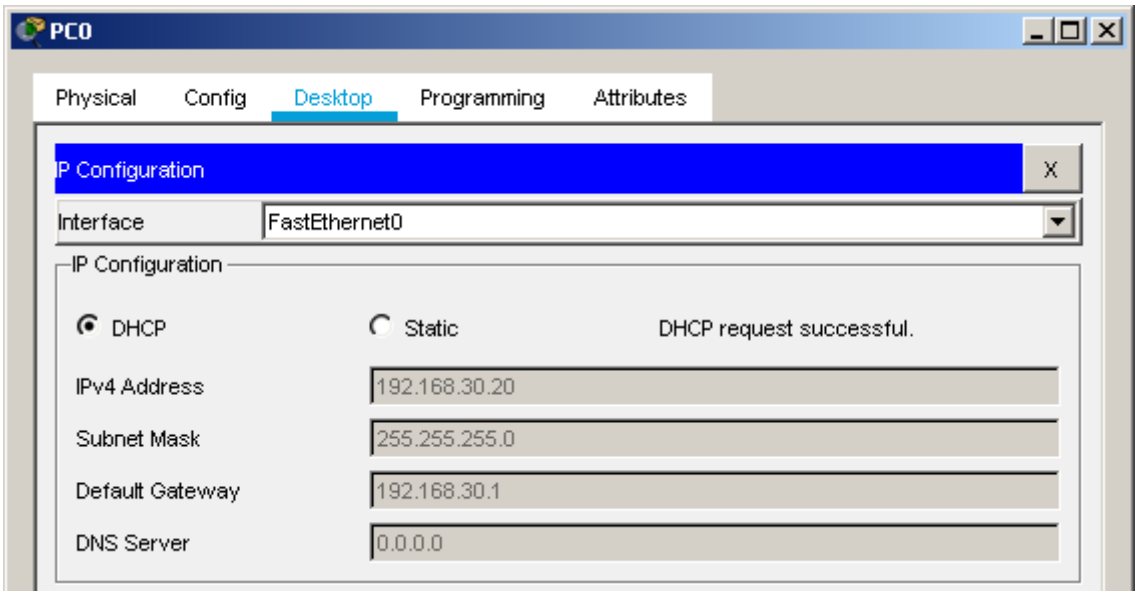


Рисунок 113 – Новые настройки, полученные от DHCP-сервера

Теперь можно подключиться к Web-интерфейсу беспроводного маршрутизатора по IP-адресу 192.168.30.1 и после успешной аутентификации продолжить настройки DHCP-сервера (рис. 114).

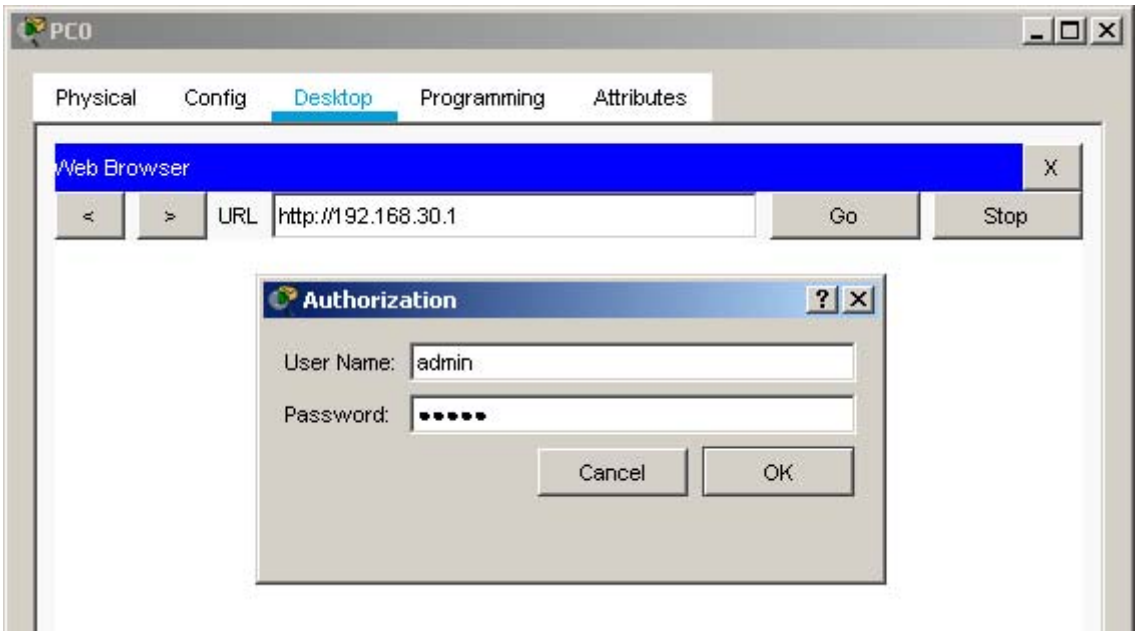


Рисунок 114 – Подключение к Web-интерфейсу маршрутизатора

Осталось выполнить следующие настройки:

- уменьшить размер пула адресов с 50 до 10;
- задать IP-адрес DNS-сервера: 8.8.8.8;

- настроить резервирование таким образом, чтобы сетевой интерфейс лэптопа (Laptop0) всегда получал IP-адрес: 192.168.30.50.

Размер пула адресов указывается в поле «Maximum number of Users». Вводим «10». IP-адрес сервера DNS (8.8.8.8) указываем в секции «Static DNS 1». Значение каждого октета вводится в отдельное поле (рис. 115).

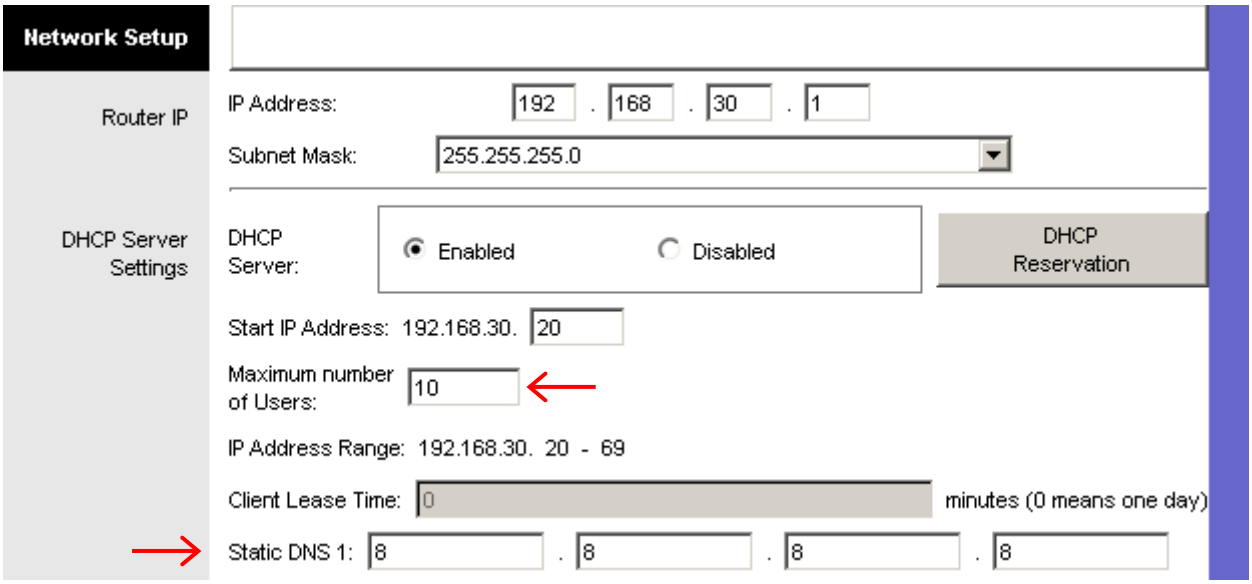


Рисунок 115 – Изменение размера пула и задание IP-адреса сервера DNS

Сохраним настройки нажатием кнопки «Save Settings» в нижней части окна (рис. 87). Внесенные изменения не могли привести к разрыву соединения, поэтому Web-интерфейс маршрутизатора сообщает, что настройки выполнены успешно (рис. 116).

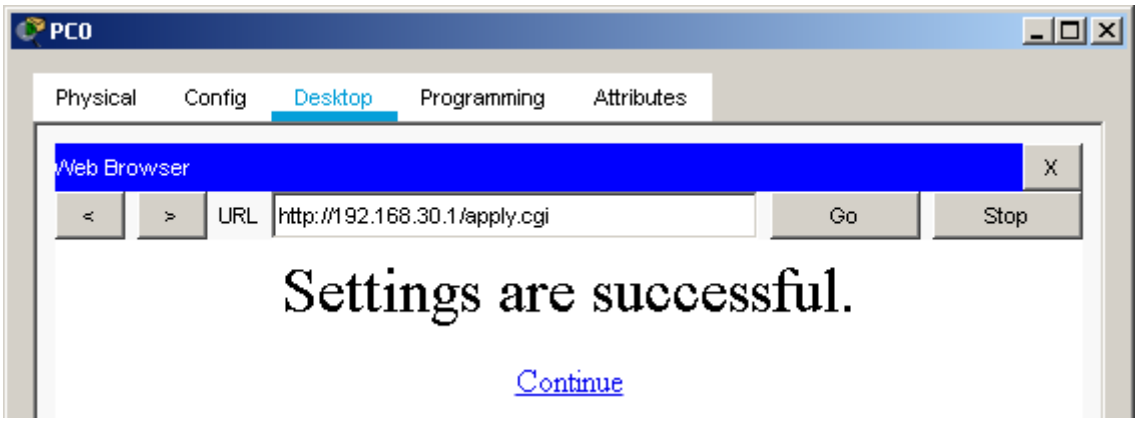


Рисунок 116 – Сообщение об успешном выполнении настроек

Осталось настроить резервирование. Ссылка «Continue» позволяет вернуться к Web-интерфейсу маршрутизатора, чтобы продолжить работу.

В подразделе «DHCP Server Settings» нажимаем большую кнопку «DHCP Reservation» (рис. 115). В результате откроется новое окно «Dialog» (рис. 117). В секции «Select Clients from DHCP Tables» представлен список клиентов DHCP. В каждой строке выводится IP-адрес сетевого интерфейса и его MAC-адрес. На данный момент только PC0 (т.е., его сетевой интерфейс) получил IP-адрес от DHCP-сервера, поэтому в таблице пока одна строка.

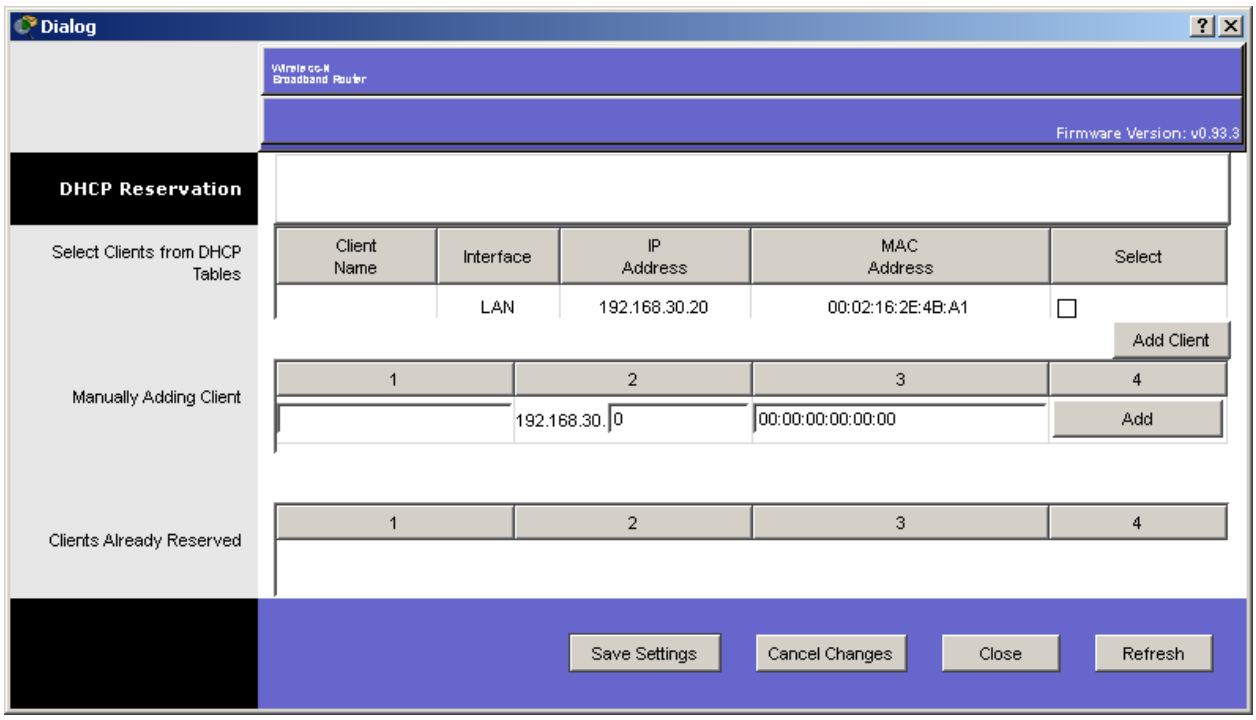


Рисунок 117 – Окно настройки резервирования IP-адресов

Резервирование настраивается в секции «Manually Adding Client». Нужно ввести имя узла (Laptop0), IP-адрес, подлежащий резервированию (192.168.30.50), а также MAC-адрес сетевого интерфейса, для которого резервируется IP-адрес (его необходимо определить). MAC-адрес каждого реального сетевого адаптера уникален и назначается производителем оборудования. Программа Cisco Packet Tracer имитирует уникальность MAC-адресов, поэтому при решении задач они всегда разные. Есть несколько способов узнать MAC-адрес сетевого адаптера, но самый простой – найти его среди характеристик соответствующего интерфейса на закладке «Config» (рис. 118). Придется временно закрыть окно «Dialog», поскольку оно блокирует доступ к рабочему полю.

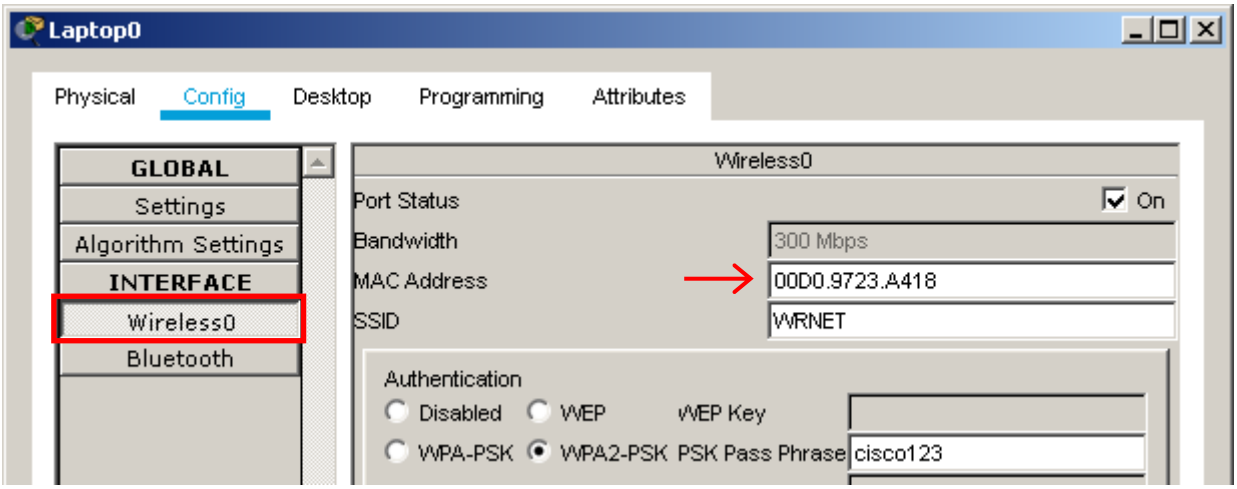


Рисунок 118 – MAC-адрес беспроводного сетевого адаптера лэптопа

MAC-адрес следует скопировать в буфер обмена или записать на лист бумаги.

Теперь можно снова нажать кнопку «DHCP Reservation», чтобы вызвать окно «Dialog» для настройки резервирования. Заполняем соответствующие поля в секции «Manually Adding Client». MAC-адрес вводится (или копируется из буфера обмена) в третье поле, при этом необходимо преобразовать его формат – удалить точки и вставить двоеточия через каждые два знака, например, 00D0.9723.A418 → 00:D0:97:23:A4:18 (рис. 119).

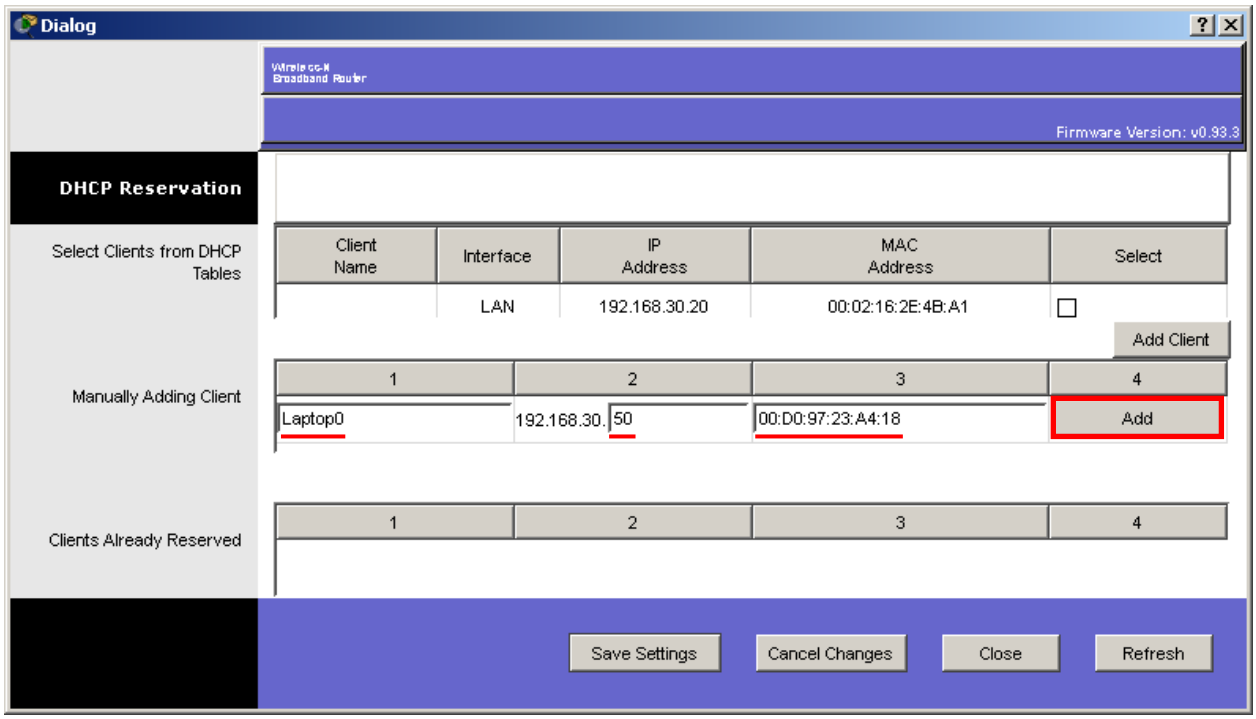


Рисунок 119 – Настройка резервирования IP-адреса

После нажатия кнопки «Add» информация о резервировании попадает в секцию «Clients Already Reserved» (рис. 120).

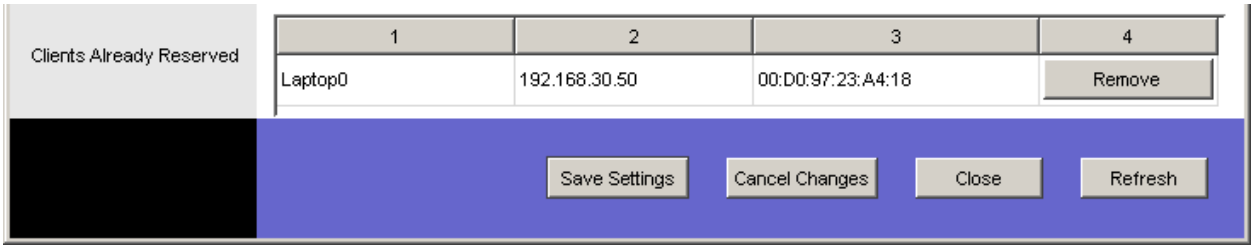


Рисунок 120 – IP-адрес зарезервирован

Резервирование настроено. Нажимаем «Save Settings» и закрываем окно «Dialog». Настройки DHCP-сервера завершены. Web-браузер тоже можно закрыть.

Теперь сетевой интерфейс лэптопа будет всегда получать от DHCP-сервера зарезервированный IP-адрес 192.168.30.50, однако это произойдет, когда выйдет срок аренды уже полученного IP-адреса. Можно инициировать запрос к DHCP-серверу вручную, как было сделано чуть раньше на компьютере PC0. Для этого на рабочем столе лэптопа, используя соответствующий ярлык, запускаем программу «IP Configuration». В открывшемся окне радио переключатель переводим в положение «Static», а затем обратно в «DHCP».

Через несколько секунд сетевой интерфейс лэптопа получит зарезервированный для него IP-адрес 192.168.30.50 (рис. 121).

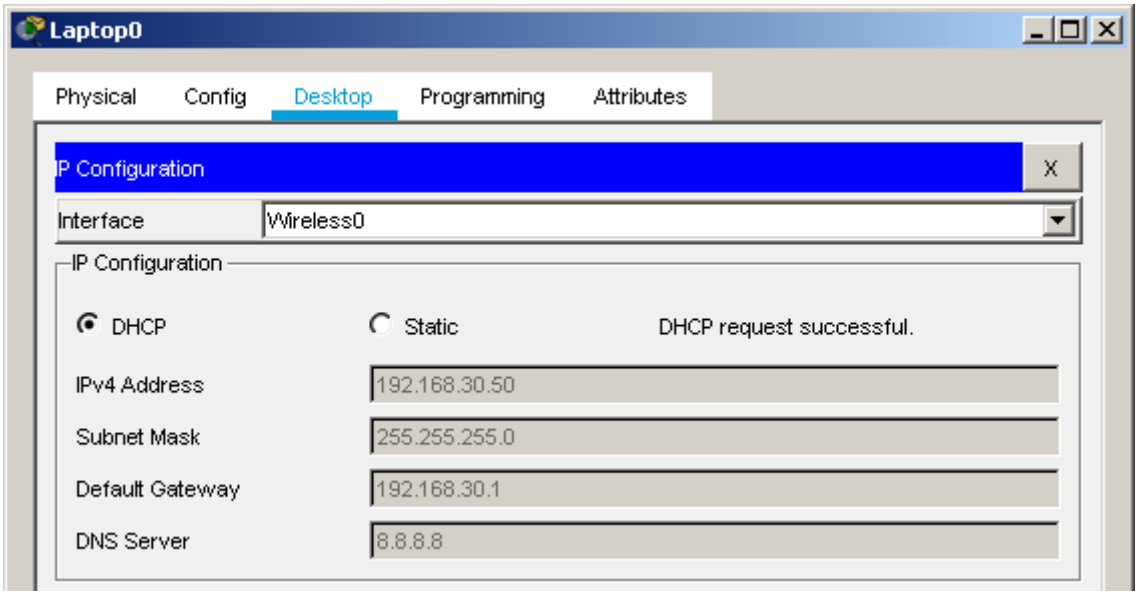


Рисунок 121 – Сетевому интерфейсу лэптопа назначен зарезервированный IP-адрес

Аналогичные действия по инициации обращения к DHCP-серверу нужно выполнить на смартфоне. Сетевой интерфейс Wireless0 смартфона получит свободный IP-адрес из созданного пула адресов. Т.к. первый IP-адрес пула 192.168.30.20 уже назначен PC0, сетевой интерфейс смартфона получит следующий адрес – 192.168.30.21 (рис. 122).

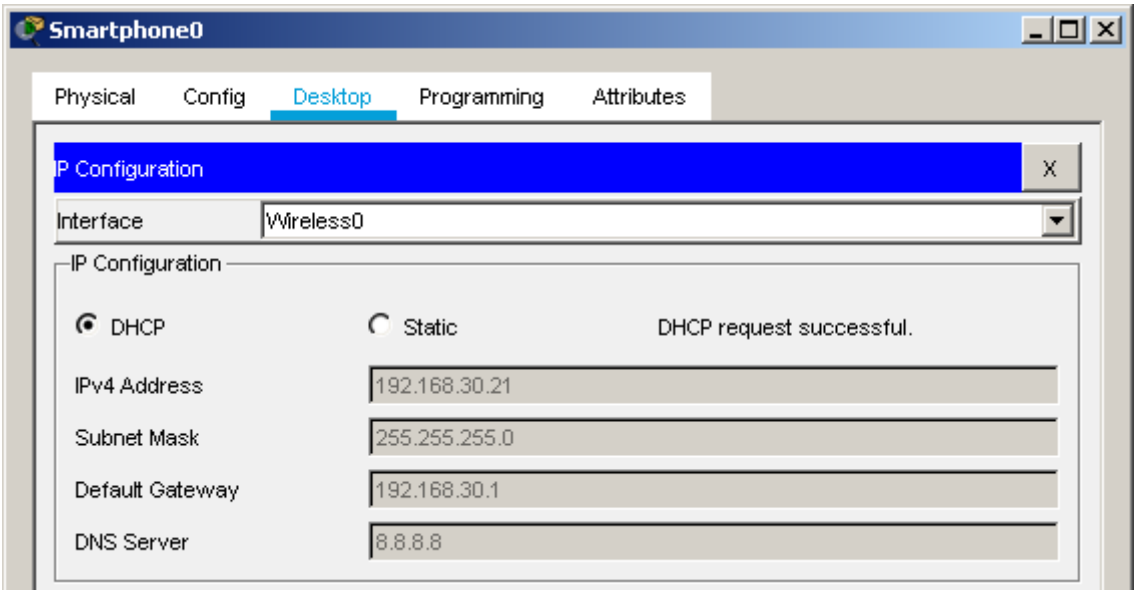


Рисунок 122 – Сетевой интерфейс лэптопа получил новый IP-адрес от DHCP-сервера

Итак, DHCP-сервер настроен, клиенты получили новые IP-адреса. Сервер сети (Server0), который по условию получает статический IP-адрес, нуждается в переконфигурировании (рис. 108). Ранее назначенный сетевому интерфейсу сервера адрес 192.168.0.10 не позволяет ему взаимодействовать с

другими узлами локальной сети. Выход в интернет тоже невозможен, поскольку IP-адрес основного шлюза изменился на 192.168.30.1.

В окне программы «IP Configuration» на сервере введем новые настройки (рис. 123):

- IP-адрес: 192.168.30.10;
- оставляем значение маски подсети: 255.255.255.0;
- адрес шлюза по умолчанию: 192.168.30.1;
- адрес сервера DNS: 8.8.8.8.

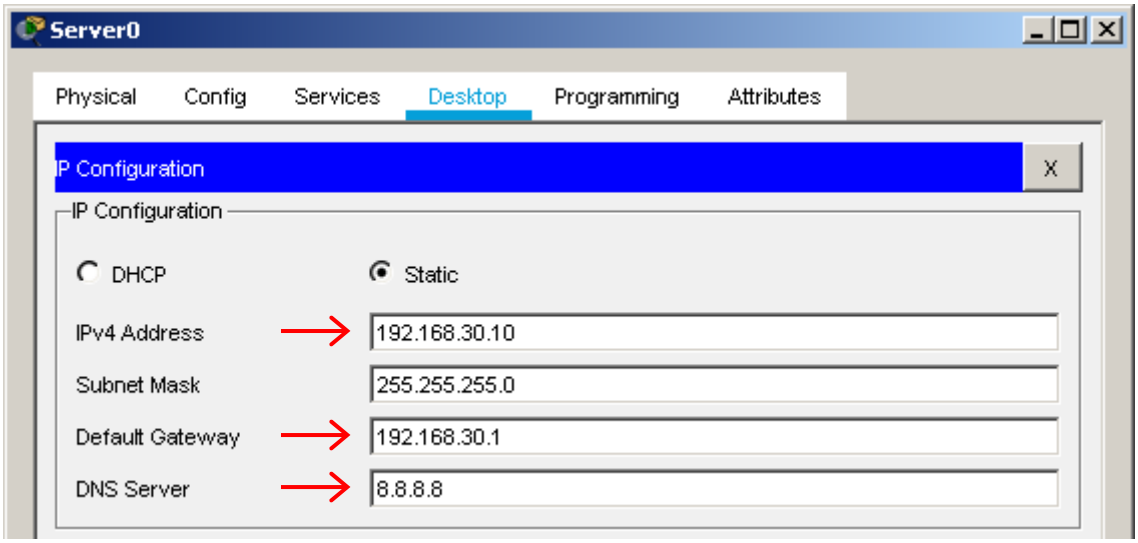


Рисунок 123 – Новые параметры сетевого интерфейса сервера Server0

Все настройки завершены. Теперь следует проверить доступность узлов в локальной сети и компьютера, имитирующего сервер в интернете. Отправим эхо-запрос, например, с лэптопа на сервер локальной сети (на IP-адрес: 192.168.30.10), а затем – узлу в интернете (на IP-адрес: 12.0.0.2). Результаты проверки доступности представлены на рисунке 124.

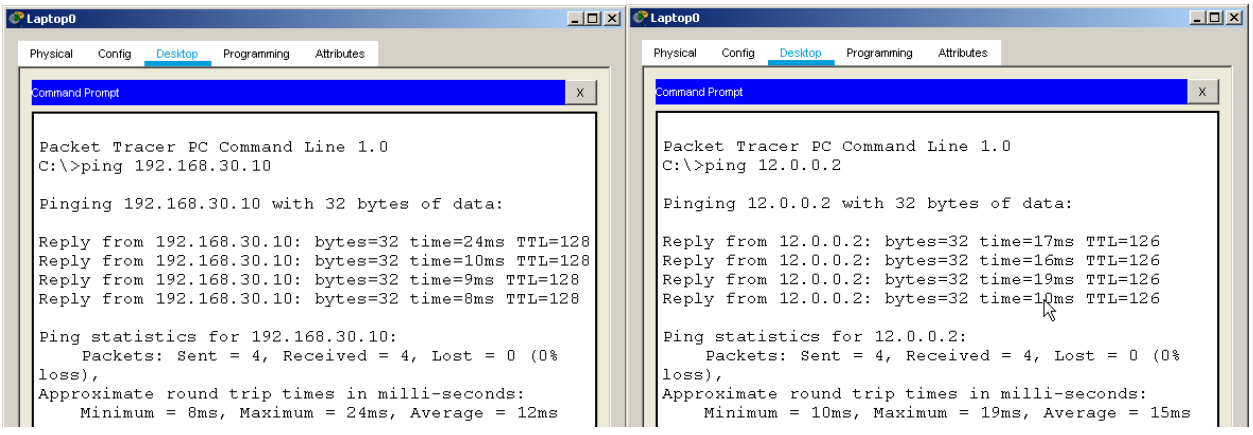


Рисунок 124 – Успешный результат проверки доступности узлов

Аналогичные проверки следует провести на каждом узле. Если эхо-ответы приходят, это значит, что узлы в локальной сети могут обмениваться информацией друг с другом, а также выходить в интернет.

Таким образом, задача решена.

Задача 2. Настройка электронной почты

Для решения данной задачи необходимо развернуть в локальной сети предприятия почтовый сервер, создать учетные записи, а также настроить почтовых клиентов на узлах сети.

Роль почтового сервера получит Server0.

Чтобы перейти к настройкам, нужно на закладке «Services» в левой части окна выбрать «EMAIL» (рис. 125).

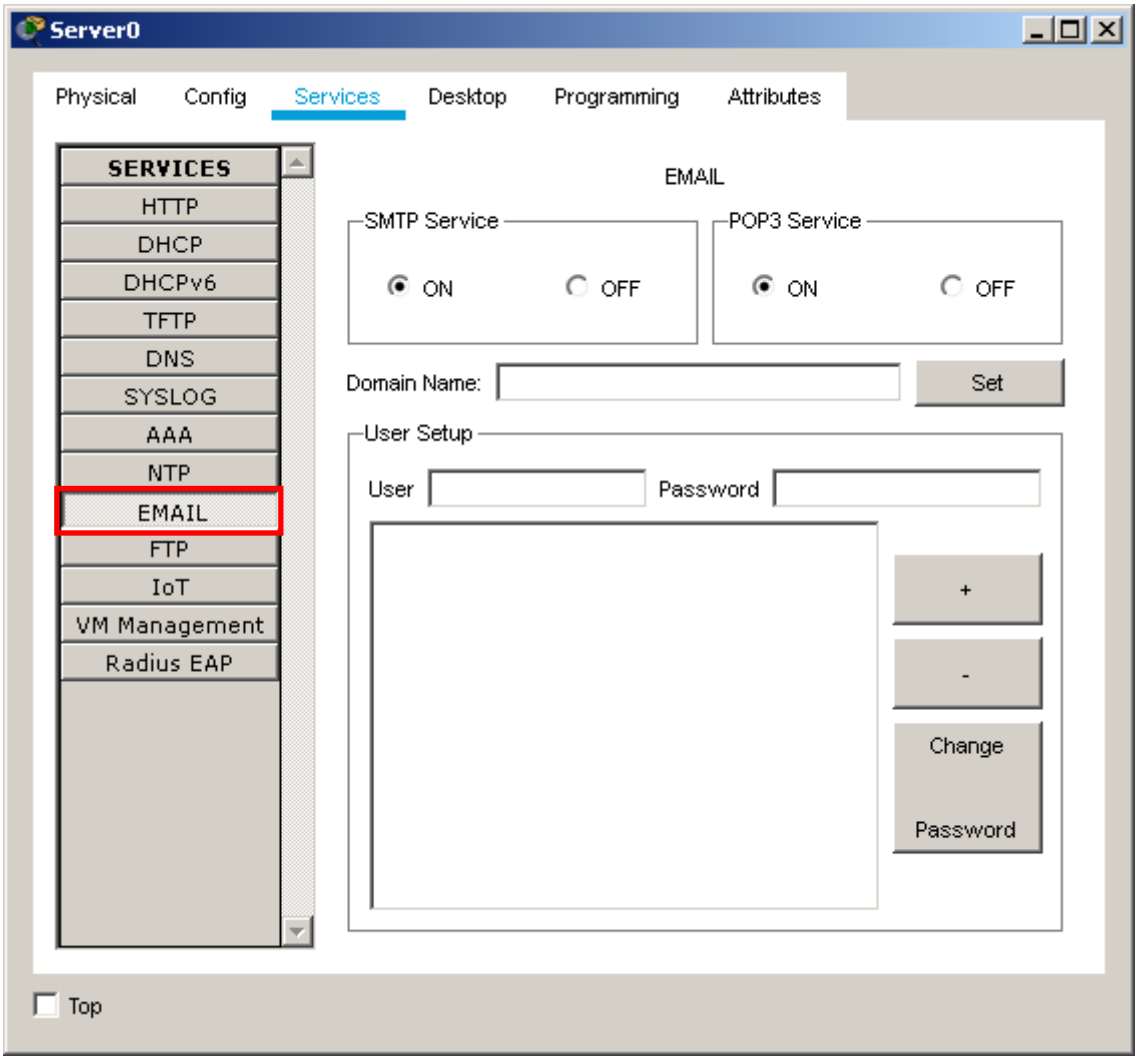


Рисунок 125 – Область настроек почтового сервера

На одном узле можно развернуть и сервер исходящей почты (SMTP), и сервер входящей почты (POP3). По умолчанию включены оба.

В поле «Domain Name» нужно ввести имя домена и нажать «Set». В адресе электронной почты доменное имя располагается после символа «@». Можно выбрать любое имя, но поскольку учебный пример моделирует сеть небольшого предприятия, подходящим именем домена может стать, например: company.com.

В разделе «User Setup» настраиваются учетные записи. В сети три пользователя, поэтому создадим три аккаунта: test, vasia и masha (Таблица 1).

Таблица 1 – Учетные записи пользователей

User	Password
test	cisco123
vasia	cisco456
masha	cisco789

В примере используются простые пароли, однако для защиты реальных учетных записей электронной почты подобные пароли назначать не рекомендуется. После ввода параметров каждой учетной записи нужно нажимать большую кнопку «+». Предусмотрена возможность удаления и изменения учетных записей (рис. 126).

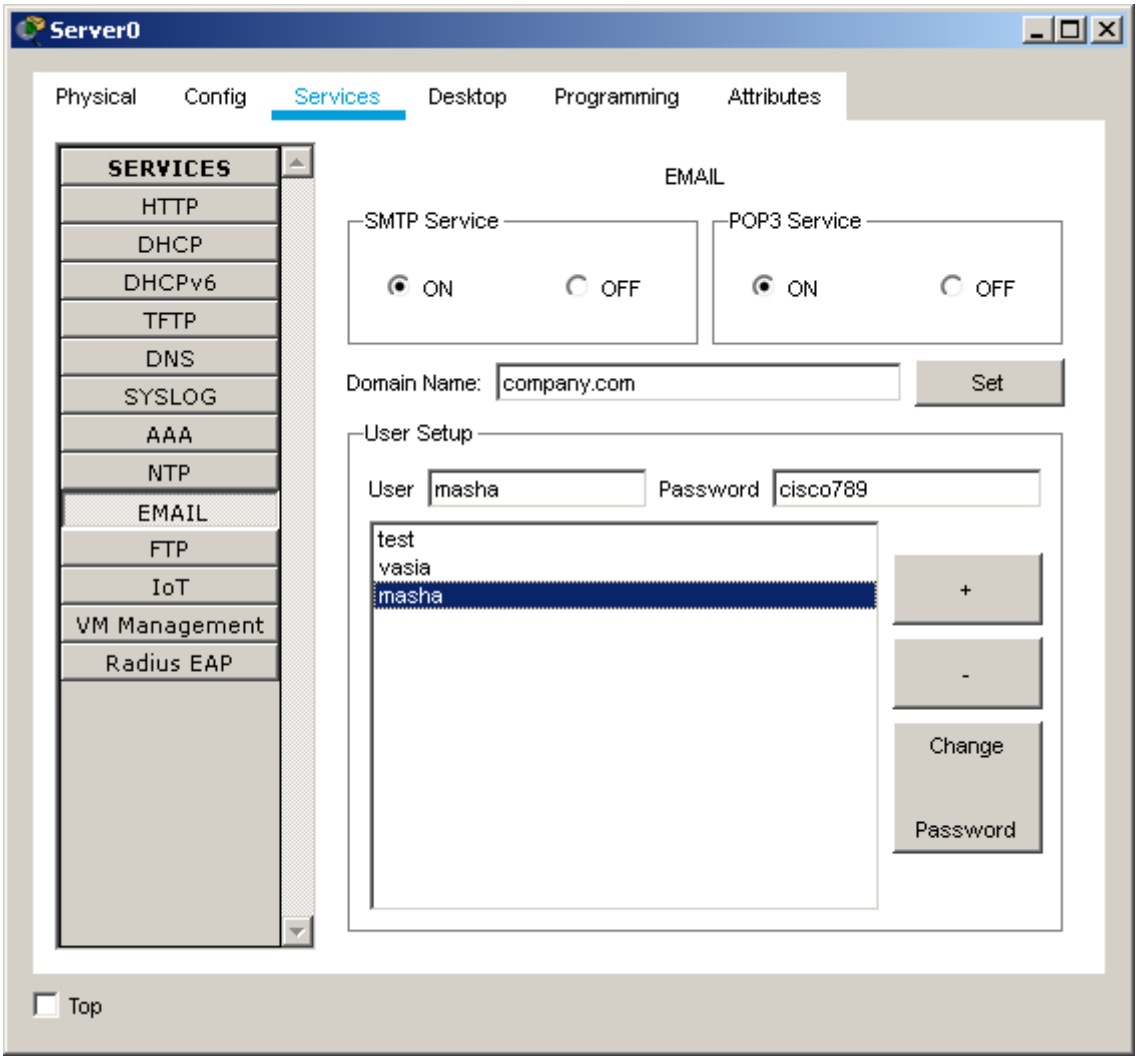


Рисунок 126 – Настройка почтового сервера, создание учетных записей

Сервер электронной почты настроен, учетные записи созданы. Теперь необходимо сконфигурировать почтовые программы на оконечных устройствах пользователей.

Каждый сотрудник нашего небольшого предприятия использует для работы определенное оконечное устройство (таблица 2), поэтому приложе-

ние электронной почты на устройстве нужно настраивать для конкретного пользователя.

Таблица 2 – Рабочие места пользователей сети

End Device	User
PC0	test
Laptop0	vasia
Smartphone0	masha

Настроим клиентские приложения электронной почты. Начнем с PC0.

Для запуска приложения используется ярлык «Email» на рабочем столе компьютера (рис. 127).

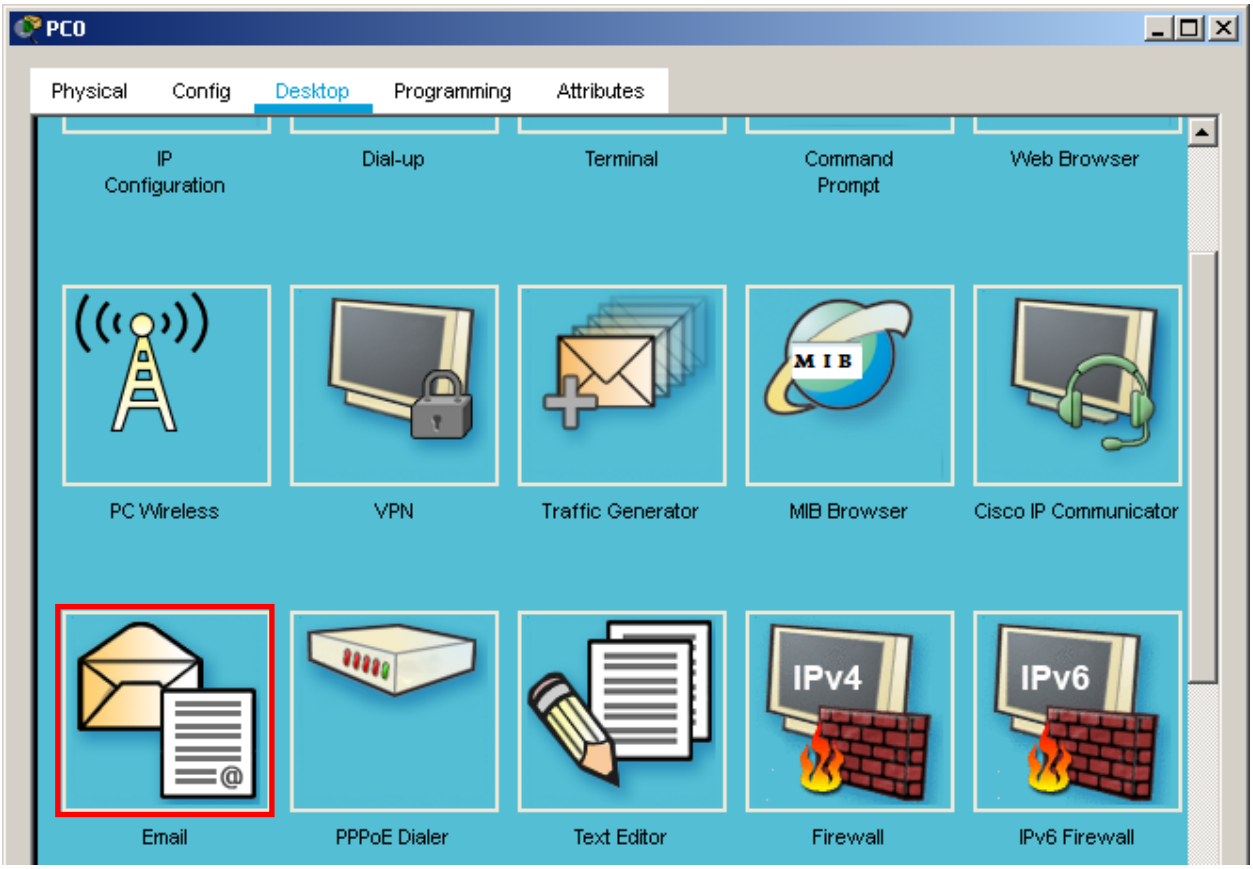


Рисунок 127 – Ярлык клиентского приложения электронной почты

Сначала откроется окно конфигурирования программы («Configure Mail»). Выполним настройки для пользователя с учетной записью **test** (рис. 128). В разделе «User Information» вводится имя пользователя и его почтовый адрес в обычном формате с «@» и доменным именем, которое указали при конфигурировании почтового сервера. В разделе «Server Information» указываются IP-адреса серверов входящей и исходящей почты. В обоих полях вводим 192.168.30.10, поскольку оба сервера развернуты на одном узле Server0. В разделе «Logon Information» вводятся параметры учетной записи **test** в точности как сервере (т.е. как в Таблице 1).

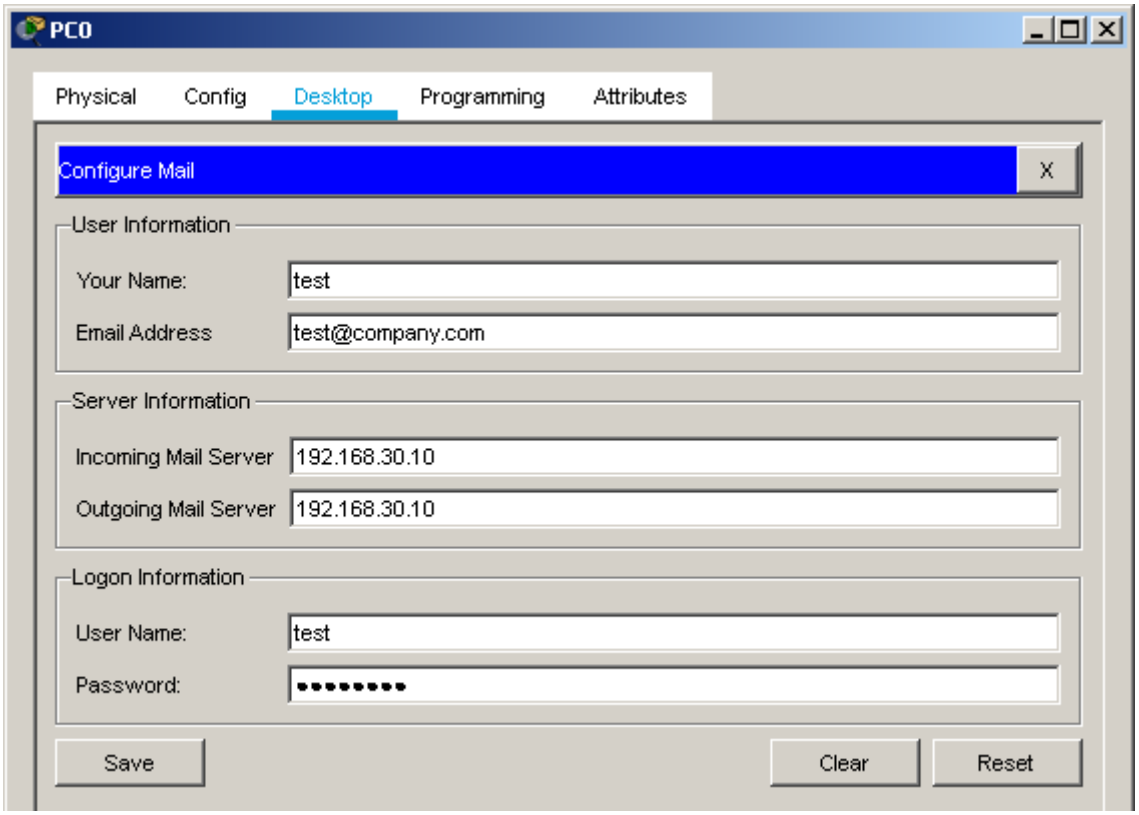


Рисунок 128– Окно конфигурирования приложения электронной почты

После нажатия кнопки «Save» клиентское приложение электронной почты запомнит параметры и перейдет в режим обозревателя «MAIL BROWSER» (рис. 129).

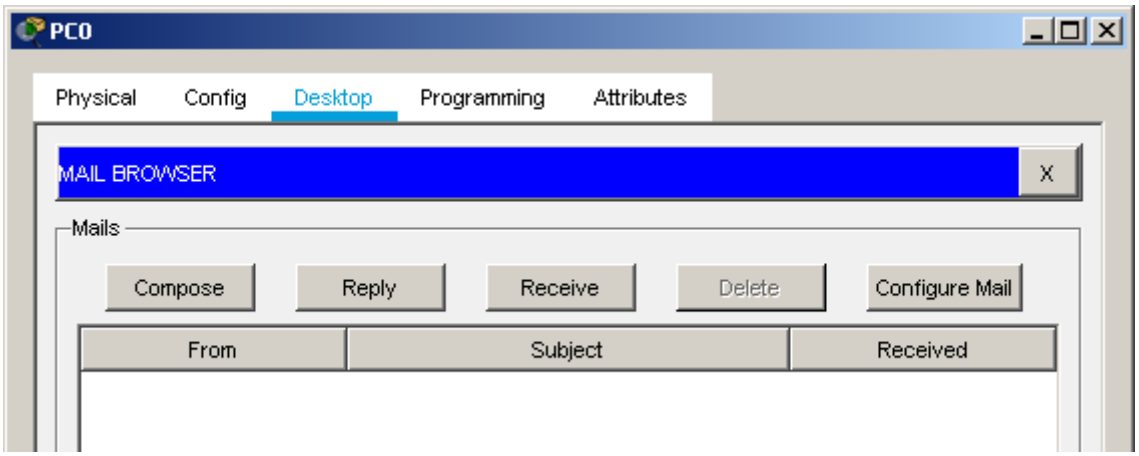


Рисунок 129– Окно обозревателя электронной почты

В этом окне можно написать электронное письмо, отправить, получить, ответить и т.п. или вернуться к конфигурированию приложения. На других оконечных устройствах сети клиентские почтовые приложения пока не настроены, т.е. отправлять почту некому, поэтому свернем окно.

Аналогичным образом настраиваются приложения электронной почты на лэптопе и смартфоне для пользователей с учетными записями **vasia** и **masha** соответственно (рис. 130).

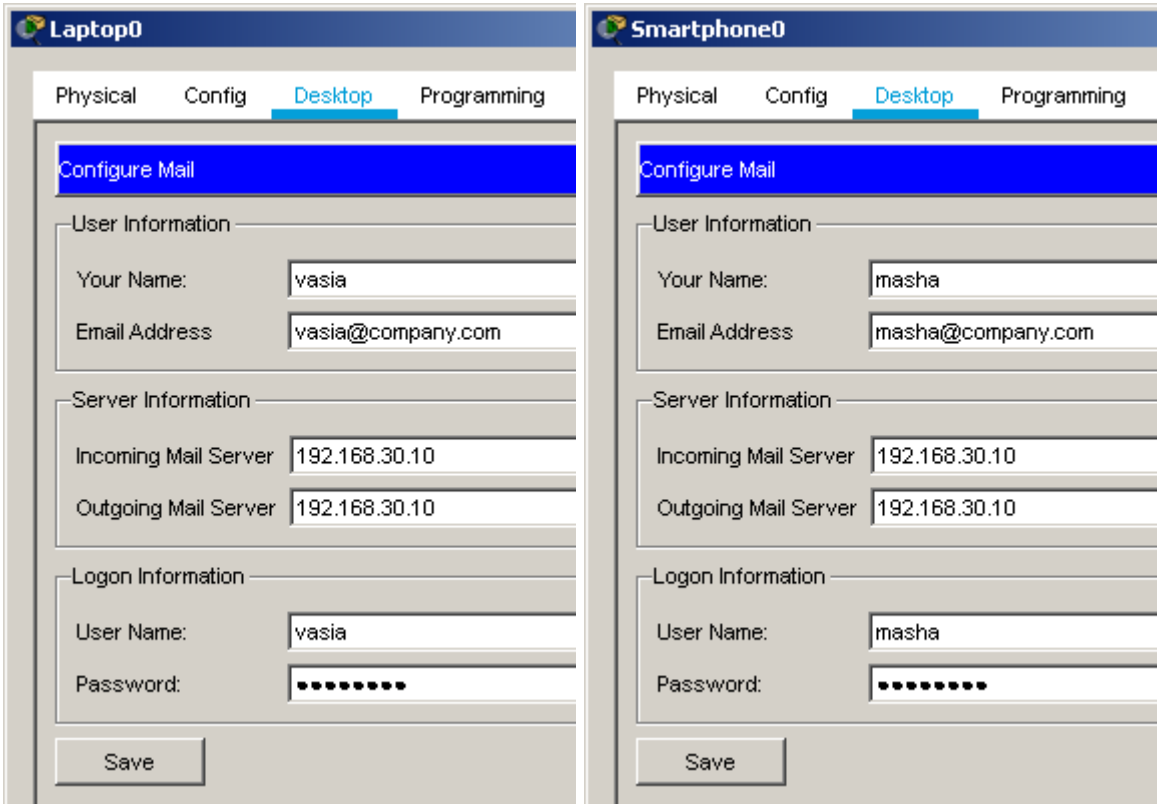


Рисунок 130 – Конфигурирование приложений электронной почты на лэптопе и смартфоне

После нажатия «Save» клиентские почтовые приложения переходят в режим обозревателя.

Теперь, когда все пользователи сети готовы к работе с электронной почтой, можно начать обмен письмами.

Пользователь **test** проверяет связь с сотрудником **vasia** путем отправки короткого письма. Для этого в обозревателе почты нужно нажать кнопку «Compose» и в открывшемся окне заполнить поля, указав адресата («To»), тему («Subject») и набрав текст письма (рис. 131).

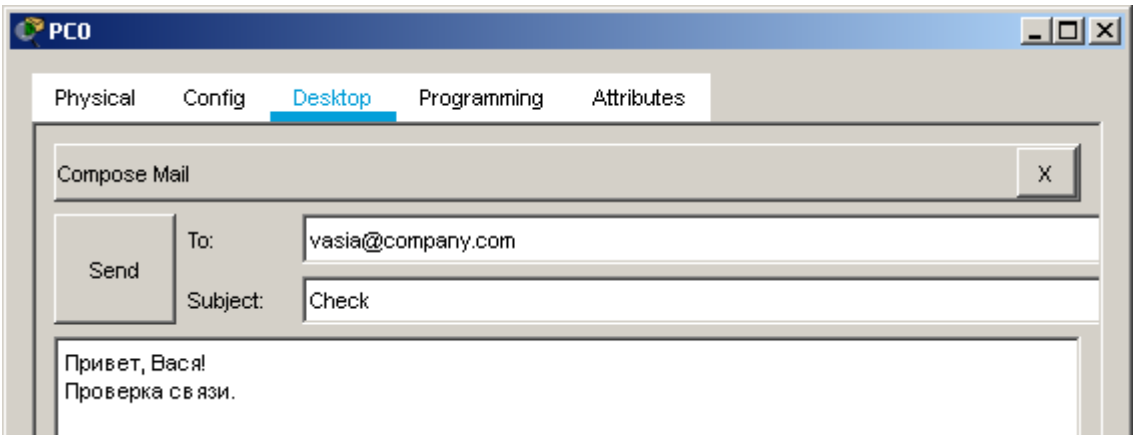


Рисунок 131– Подготовка короткого письма для пользователя **vasia**

Отправка письма инициируется нажатием кнопки «Send». Окно «Compose Mail» закроется, а в нижней части окна браузера почты «MAIL BROWSER» появится сообщение об успешной отправке (рис. 132).

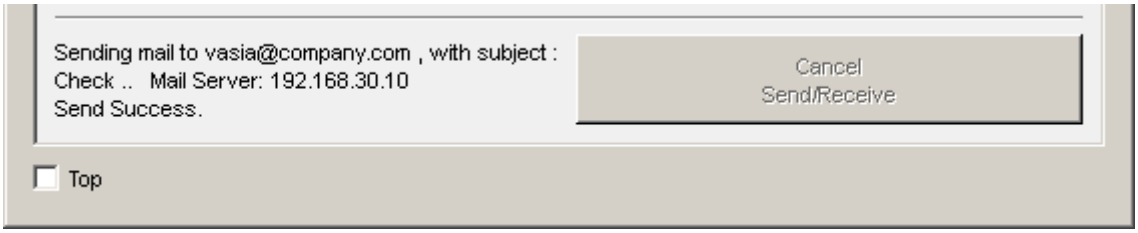


Рисунок 132 – Сообщение об успешной отправке письма

В окне обозревателя почты на лэптопе для получения корреспонденции нужно нажать кнопку «Receive». В результате письмо от пользователя **test** будет получено приложением от почтового сервера – ссылка на него появится в списке (рис. 133).

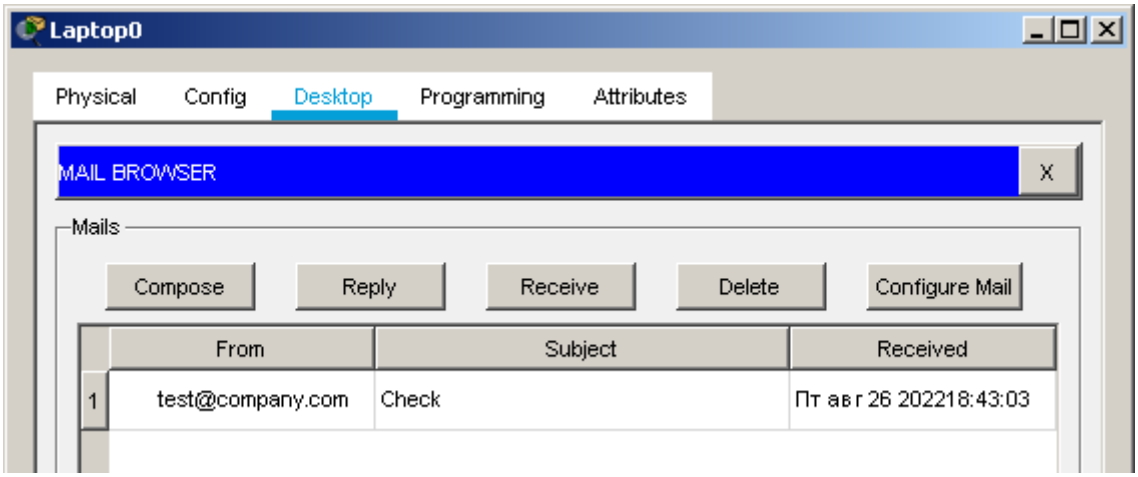


Рисунок 133 – Получение письма почтовым приложением лэптопа

Чтобы прочитать письмо, нужно отметить его в списке щелчком мыши. Текст письма, откроется в нижней части окна обозревателя почты (рис. 134).

Рисунок 134 – Отображение полученного письма в обозревателе почты

Пользователь лэптопа для подтверждения успешного получения письма может отправить ответное письмо. Для этого в окне обозревателя почты нужно нажать кнопку «Reply». В открывшемся окне уже автоматически заполнены поля «To» и «Subject», а под горизонтальной чертой – текст полученного письма со служебной информацией.

Пространство над горизонтальной чертой предназначено для текста ответного письма. Пользователь **vasia** пишет ответ с подтверждением успешного получения письма от пользователя **test** (рис. 135).

Отправка письма происходит после нажатия кнопки «Send». Окно «Reply Mail» также закроется.

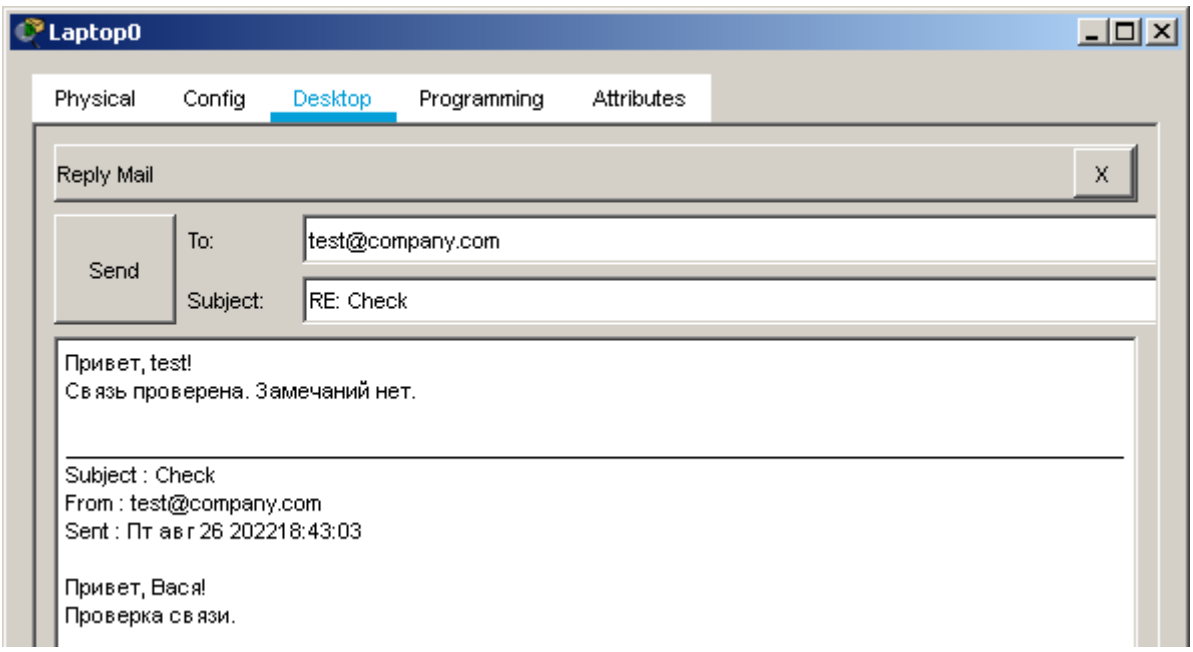


Рисунок 135 – Подготовка пользователем **vasia** ответного письма

Пользователь **test**, использующий для работы компьютер PC0, нажимает кнопку «Receive» в обозревателе почты и получает ответное письмо от пользователя **vasia** (рис. 136).

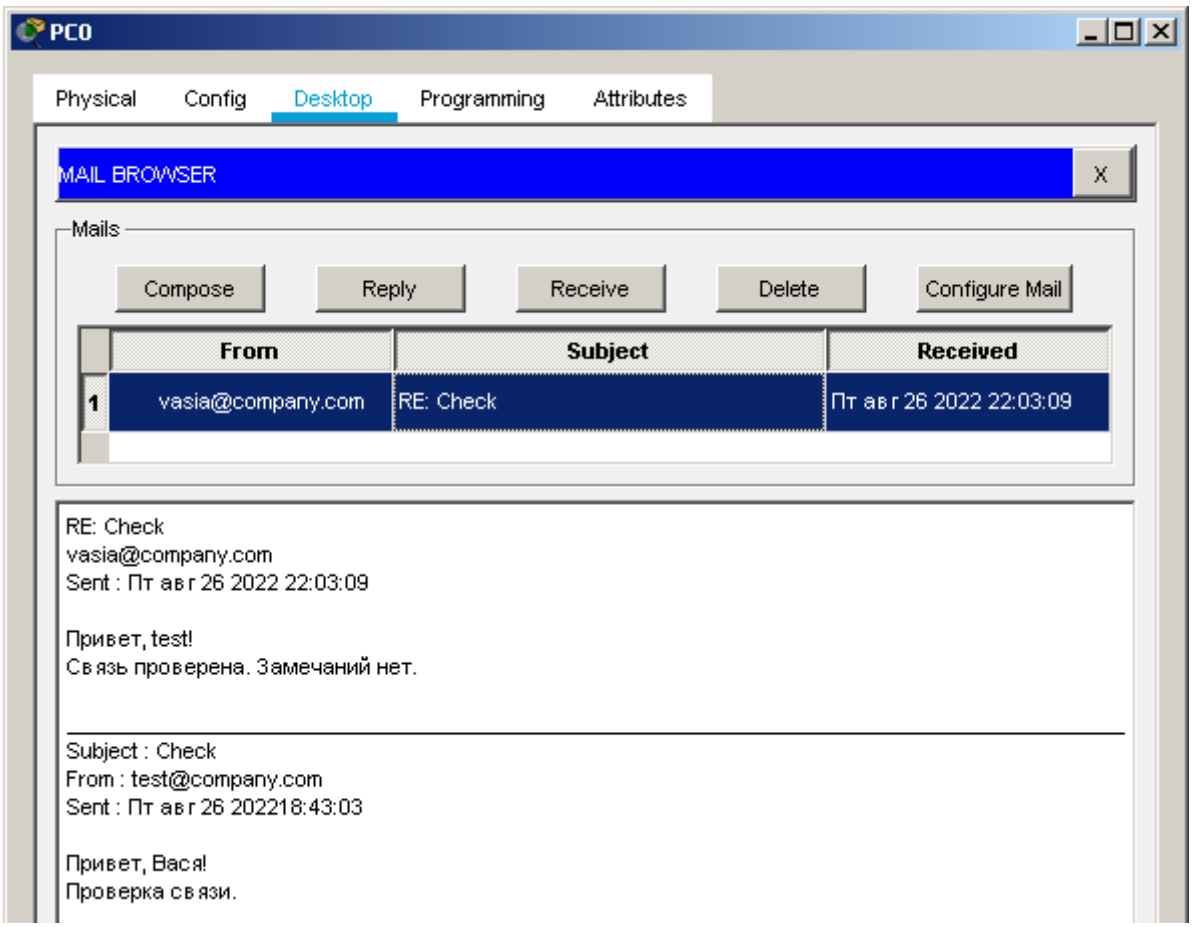


Рисунок 136 – Получение ответного письма почтовым приложением PC0

Аналогичным образом может быть осуществлен обмен электронными письмами с пользователем **masha**.

Таким образом, служба электронной почты в локальной сети предприятия настроена и функционирует. Задачи настройки сетевых служб, предусмотренные планом Практического занятия №3, выполнены полностью.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.
2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. - СПб.: Питер, 2012. – 960 с.
3. Прикладная информатика: справочник : учебное пособие / В. Н. Волкова, В. Н. Юрьев, А. Б. Анисифоров [и др.] ; Под редакцией В.Н. Волковой и В.Н. Юрьева. – Москва : Общество с ограниченной ответственностью "Издательство "Финансы и статистика", 2021. – 767 с. – ISBN 978-5-00184-055-8. – EDN CUITMJ.
4. Полищук С. Intent-Based Networking: сети, ориентированные на бизнес // Издательство «Открытые системы». 19 декабря 2018 г. URL: https://www.osp.ru/lan/2018/06/13054698 (дата обращения 25.10.2022)
5. Romanova C. Что такое BYOD? Модели BYOD // Хабр. 18 октября 2021 г. URL: https://habr.com/ru/company/ipmatika/blog/584014/