Компьютерные коммуникации и сети.
Настройка сервисов

Учебное пособие

Аннотация

В пособии рассмотрены теория и практические задания раздела дисциплины Настройка сетевых сервисов, именно – способы настройки WEB, DNS, DHCP и почтового серверов, Telnet и SSH в пакете Cisco Packet Tracer. А также основные команды операционной системы CISCO IOS

Телепова Т. П.

TelepovaTP@e1.ru

Российский государственный профессионально-педагогический университет

Учебное пособие составлено для студентов направления подготовки 09.03.02 Информационные системы и технологии бакалаврской программы «Информационные технологии в медиаиндустрии»

Автор: Т.П. Телепова

Содержание

1 НАСТРОЙКА СЕТЕВЫХ СЕРВИСОВ

1.1 Особенности программы Cisco Packet Tracer

Среда моделирования компьютерных сетей Cisco Packet Tracer – это эмулятор сети, созданный компанией Cisco. Программное решение Cisco Packet Tracer позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т.д.

Настройки, в свою очередь, зависят от характера устройств: одни можно настроить с помощью команд операционной системы Cisco IOS, другие – за счет графического веб-интерфейса, третьи – через командную строку операционной системы или графические меню.

Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, пользователь может отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности.

В Cisco Packet Tracer пользователь может симулировать построение не только логической, но и физической модели сети и, следовательно, получать навыки проектирования. Схему сети можно наложить на чертеж реально существующего здания или даже города и спроектировать всю его кабельную проводку, разместить устройства в тех или иных зданиях и помещениях с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

Симуляция, визуализация, многопользовательский режим и возможность проектирования делают Cisco Packet Tracer уникальным инструментом для обучения сетевым технологиям (https://studfile.net/preview/10367119/page:2/#7).

1.2 Интерфейс Cisco Packet Tracer

Главное окно Cisco Packet Tracer

На рис. 1 представлен интерфейс программы:

1. *Главное меню программы со следующими вкладками*: Файл (содержит операции открытия/сохранения документов), Правка (стандартные операции "копировать/вырезать, отменить/повторить"), Настройки, Вид (масштаб рабочей области и панели инструментов), Инструменты (цветовая палитра и кластеризация конечных устройств), Расширения – мастер проектов, многопользовательский ре-

жим и несколько функций, которые из CPT могут сделать целую лабораторию, Помощь.

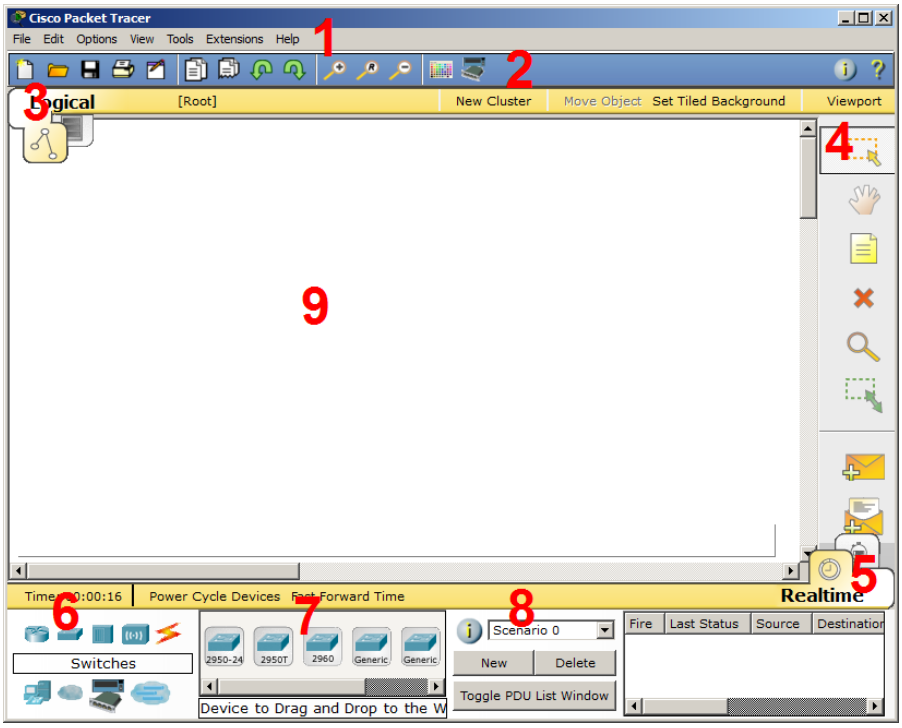


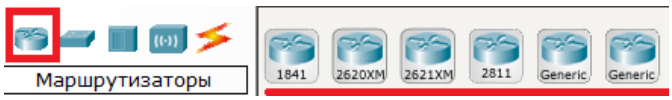
Рисунок 1 – Интерфейс программы Cisco Packet Tracer

2. Панель инструментов, часть которых просто дублирует пункты меню; 3. Переключатель между логической и физической организацией; 4. Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а также формирование произвольных пакетов; 5. Переключатель между реальным режимом (Real-Time) и режимом симуляции; 6. Панель с группами конечных устройств и линий связи; 7. Сами конечные устройства, здесь содержатся всевозможные коммутаторы, узлы, точки доступа, проводники. 8. Панель создания пользовательских сценариев; 9. Рабочее пространство.

Пример размещения цветовых областей, позволяющий, например, отделять визуально одну подсеть от другой можно изучить на сайте (https://studfile.net/preview/10367119/page:2/#7).

Оборудование и линии связи в Cisco Packet Tracer:

Маршрутизаторы. Работают на сетевом уровне модели OSI:



Коммутаторы. Устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети:

Концентраторы. Концентратор повторяет пакет, принятый на одном порту на всех остальных портах:

Беспроводные устройства. Беспроводные технологии Wi–Fi и сети на их основе. Включает в себя точки доступа:

Линии связи. С помощью этих компонентов создаются соединения узлов в единую схему:

С помощью этих компонентов создаются соединения узлов в единую схему. Packet Tracer поддерживает широкий диапазон сетевых соединений. Каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов.

Консоль – консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами.

Медный прямой – этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, который функционирует на разных уровнях OSI. Он должен быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).

Медный кроссовер – этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Он может быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet)

Оптика – оптоволоконная среда используется для соединения между оптическими портами (100 Мбит/с или 1000 Мбит/с).

Телефонный – соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты. Стандартное представление модемного соединения – это конечное устройство (например, ПК), дозванивающееся в сетевое облако.

Коаксиальный – коаксиальная среда используется для соединения между коаксиальными портами, такие как кабельный модем, соединенный с облаком Packet Tracer.

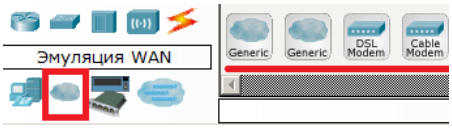
Серийный DCE, Серийный DTE – соединения через последовательные порты, часто используются для связей WAN.

Конечные устройства

Здесь представлены конечные узлы, хосты, сервера, принтеры, телефоны и т.д.:

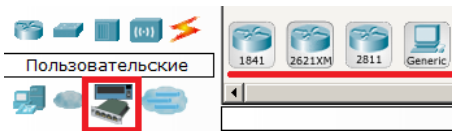
Эмуляция Интернета

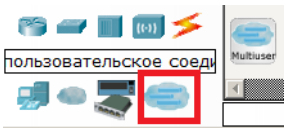
Пример эмуляция глобальной сети. Модем DSL, "облако" и т.д. :



Пользовательские устройства и облако для многопользовательской работы

Устройства можно комплектовать самостоятельно. Можно создавать произвольные подключения:





1.3 Комплектация маршрутизаторов в CPT

Задание 1. Изменение комплектации оборудования

Установите в рабочем поле роутер Cisco 1841. В настройках на роутере открываем его физическую конфигурацию (рис. 2).

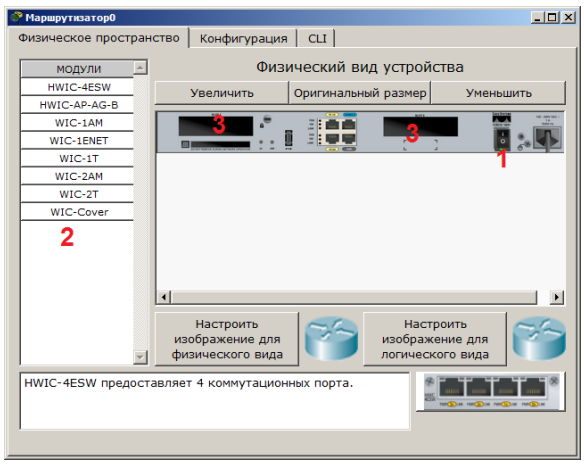


Рисунок 2 – Физическая конфигурация маршрутизатора

Слева, список модулей (цифра 2), которыми можно укомплектовать данный роутер. Сейчас в нем 2 пустоты (цифра 3). В них вкладываются модули. Эту операцию нужно производить при выключенном питании (цифра 1).

По аналогии с ПК – есть платы, подключаемые к PCI-шине (TV-тюнеры, звуковые карты, USB–разветвители, сетевые карты). Модули WIC роутера – платы расширения, увеличивающие функционал устройства.

Таким образом, устройство Cisco – это тот же системный блок со своей ОС и многими сетевыми картами, который может делать что-то только с сетью.

Модули маршрутизатора:

WIC (Wide Area Network) – WAN интерфейсная карта – это разъем на роутере, в который подключается кабель от провайдера. Сетевой кабель, по котором роутер получает доступ в интернет.

HWIC – высокоскоростная интерфейсная карта WAN – эволюция WIC, сейчас используется на маршрутизаторах ISR.

Особенности и характеристики маршрутизаторов Cisco ISR: http://www.technorium.ru/cisco/routers/.

VIC (Voice Interface Card) – карта голосового интерфейса (поддержка только голоса).

VIC2 – evolution of the above (развитие VIC).

VWIC (Voice Wan Interface Card) – голос и интерфейсная карта (карта E1/T1, которая может быть использована для голоса или данных).

VWIC2 – развитие VWIC.

Ниже представлена информация о каждом модуле:

HWIC (High-Speed WAN Interface Card) – 4ESW (ЛВС) – высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45. Позволяет сочетать в маршрутизаторе возможности коммутатора.

Технология Ethernet: https://ru.wikipedia.org/wiki/Ethernet, Что такое RJ45?: http://www.denaie.ru/?p=2998, https://www.avs–el.ru/blogs/blog/konnektor–rj–45–rj–11–i–ego–osobennosti

HWIC-AP-AG-B (точка доступа) – это высокоскоростная WAN-карта, обеспечивающая функционал встроенной точки доступа для роутеров линейки Cisco 1800 (модульных), Cisco 2800 и Cisco 3800.

Что такое точка доступа WiFi: https://www.getwifi.ru/p_router_ap.html

WIC-1AM (телефонка) включает в себя два разъема RJ–11, используемых для подключения к базовой телефонной службе Карта использует один порт для соединения с телефонной линией, другой может быть подключен к аналоговому телефону для звонков во время простоя модема.

RJ 11:

http://www.tktdf.ru/poleznaya_informatsiya/tehnologicheskie_novinki/article_id=36.html.

WIC-2AM содержит два разъема RJ-11, используемых для подключения к базовой телефонной службе. В WIC-2AM два модемных порта, что позволяет использовать оба канала для соединения одновременно.

WIC-1ENET – это однопортовая 10 Мб/с Ethernet карта для 10BASE-T Ethernet LAN. Для передачи данных используется 4 провода кабеля витой пары (две скрученные пары) категории 3 или категории 5. Максимальная длина сегмента – 100 метров. Для маршрутизаторов 1700–й серии.

Модуль Cisco (WIC–1ENET=): https://elmir.ua/switch_modules/module_cisco_wic–1enet.html Подробнее: https://elmir.ua/switch_modules/module_cisco_wic–1enet.html

WIC-1T – предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам, например, SDLC концентраторам, системам сигнализации и устройствам packet over SONET (POS) (SONET – синхронная оптическая сеть, POS – передача пакетов через SONET).

SDLC https: //www.intuit.ru/studies/courses/15855/94/lecture/2829

POS-оборудование: https://ru.wikipedia.org/wiki/POS–%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5.

WIC-2T – 2-портовый синхронный/асинхронный серийный сетевой модуль предоставляет гибкую поддержку многих протоколов с индивидуальной настройкой каждого порта в синхронный или асинхронный режим.

WIC-Cover – стенка для WIC слота, необходима для защиты электронных компонентов и для улучшения циркуляции охлаждающего воздушного потока.

Для изменения комплектации оборудования необходимо:

– отключить питание, кликнув мышью на кнопке питания, – перетащить мышью модуль 4ESW в свободный слот и включить питание, – подождать окон-

чания загрузки роутера. В конфигурации GUI можем увидеть появившиеся 4 новых интерфейса (рис. 3).

Рисунок 3 – Конфигурация интерфейсов устройства (GUI)

Остальные устройства комплектуются аналогично. Добавляются новые модули Ethernet (10/100/1000), оптоволоконные разъемы нескольких типов, адаптеры беспроводной сети. На рабочий компьютер есть возможность добавить, например, микрофон с наушниками, жесткий диск для хранения данных.

Контрольные вопросы

Какая плата расширения маршрутизатора обеспечивает функционал встроенной точки доступа? Какая плата расширения предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам? Как называется высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45? Перечислите сетевые карты, позволяющие подключаться к WAN сетям? Назовите модели коммутаторов второго уровня? Назовите модели коммутаторов третьего уровня? Какой тип кабеля следует использовать при соединении роутеров между собой? Укажите серии маршрутизаторов. Широковещательная рассылка? В каких случаях используется интерфейс SERIAL? Как организовать связь двух магистральных маршрутизаторов? Перечислите все возможные режимы работы программы Cisco Packet Tracer? Перечислите все типы связей, используемых в Cisco Packet Tracer и укажите их назначение.

1.4 Сетевые службы

Теоретические сведения

Сеть – это совокупность устройств и систем, подключенных друг к другу (логически или физически) и общающихся между собой (рис. 4). Сюда можно отнести сервера, компьютеры, телефоны, маршрутизаторы и пр. Размер этой сети

может достигать размера Интернета, а может состоять всего из двух устройств, соединенных между собой кабелем.

Компоненты сети:

1) оконечные узлы: устройства, которые передают и/или принимают какие–либо данные (компьютеры, телефоны, сервера, какие–то терминалы или тонкие клиенты, телевизоры).

2) промежуточные устройства: устройства, которые соединяют оконечные узлы между собой (коммутаторы, концентраторы, модемы, маршрутизаторы, точки доступа Wi-Fi).

3) сетевые среды: среды, в которых происходит непосредственная передача данных (кабели, сетевые карточки, различного рода коннекторы, воздушная среда передачи). Если это медный кабель, то передача данных осуществляется при помощи электрических сигналов. У оптоволоконных кабелей, – при помощи световых импульсов, у беспроводных устройств, – при помощи радиоволн (рис. 4).

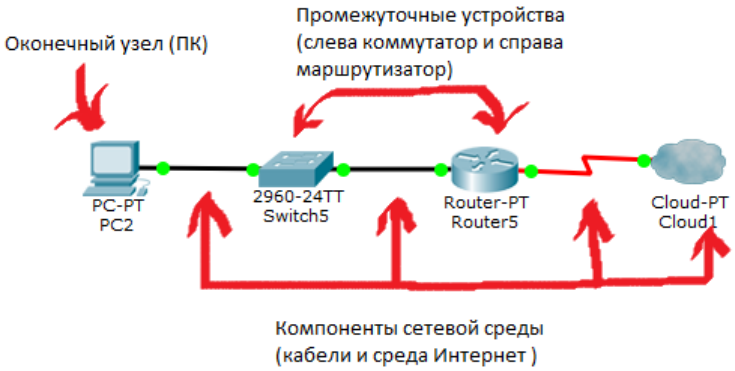


Рисунок 4 – Сетевые среды

Применение сетей: передача данных между устройствами при помощи приложений, организация удалённых сетевых ресурсов, организация хранилищ, резервное копирование, VoIP …

Виды топологии сетей

1) топология с общей шиной (англ. Bus Topology);

Одна из первых физических топологий. К одному длинному кабелю подсоединяли все устройства. На концах кабеля требовались терминаторы ⇨.

2) кольцевая топология (англ. Ring Topology);

Каждое устройство подключается к 2-м соседним, создавая, таким образом, кольцо. С одного конца компьютер только принимает, а с другого только отправляет. Каждый следующий компьютер играет роль ретранслятора сигнала ➢.

3) топология звезда (англ. Star Topology)

Все устройства подключаются к центральному узлу, который уже является ретранслятором. Используется в локальных сетях, когда к одному коммутатору подключаются несколько устройств, и он является посредником в передаче ➢.

4) полносвязная топология (Full-Mesh Topology)

Все устройства связаны напрямую друг с другом. То есть с каждого на каждый. Данная модель является, пожалуй, самой отказоустойчивой, так как не зависит от других. Но строить сети на такой модели сложно и дорого ➢.

5) неполносвязная топология (Partial-Mesh Topology)

Как правило, вариантов ее несколько. Она похожа по строению на полносвязную топологию. Однако соединение построено не с каждого на каждый, а через дополнительные узлы ➢.

6) смешанная топология (Hybrid Topology)

Самая популярная топология, которая объединила все топологии выше в себя. Представляет собой древовидную структуру ➢.

Рассмотрим сетевую модель OSI и стек протоколов TCP/IP

Задачу стандартизации сетевых технологий решала на начальных этапах их развития международная организация по стандартизации (ISO – International Organization for Standartization). Они изучали многие, применяемые на то время, модели и в результате придумали модель OSI, релиз которой состоялся в 1984 году (рис. 5). Однако в это время другие модели модернизировались и набирали обороты. В настоящее время хоть ее и не применяют в том виде, в каком она есть, принципы работы у других моделей схожи с ней.

Рисунок 5 – Сетевая модель OSI

Состоит она из 7 уровней и каждый уровень выполняет определенную ему роль и задачи ➢.

Стек протоколов TCP/IP

Как было написано выше, модель OSI в наше время не используется. Популярность получил стек протоколов TCP/IP. На рисунке 6 приведены сравнения уровней и их ролей.

Рисунок 6 – Сравнение уровней

Три верхних уровня OSI: прикладной, представления и сеансовый объединены у TCP/IP в один, под названием прикладной. Сетевой уровень сменил название и называется – Интернет. Транспортный остался таким же и с тем же названием. А два нижних уровня OSI: канальный и физический объединены у TCP/IP в один с названием — уровень сетевого доступа. Стек TCP/IP в некоторых источниках обозначают еще как модель DoD (Department of Defence).

Протоколы прикладного уровня (по стеку TCP/IP)

Протоколы прикладного уровня обеспечивают взаимодействие между человеком и сетью. Этих протоколов огромное количество, и выполняют они совершенно различные роли. часто используемые протоколы в сети: HTTP, DNS, DHCP, SMTP и POP3, Telnet, SSH, FTP, TFTP (https://habr.com/ru/post/307714/).

Протокол HTTP (HyperText Transport Protocol)

Протокол передачи данных, используемый обычно для получения информации с веб-сайтов. Использует он «клиент-серверную» модель. То есть существуют клиенты, которые формируют и отправляют запрос. И серверы, которые слушают запросы и, соответственно, на них отвечают.

В качестве клиентов выступают известные многим веб-браузеры: Internet Explorer, Mozilla Firefox, Google Chrome и т.д. А в качестве серверного ПО используют: Apache, IIS, nginx и т.д. ➢.

Как правило, сервер отдает в сеть ресурсы, а клиент эти ресурсы использует. Также, на серверах устанавливаются специализированное программное и ап-

паратное обеспечение. На одном компьютере может работать одновременно несколько программ-серверов. Сервисы серверов часто определяют их название:

Cisco EMAIL – почтовый сервер, для проверки почтовых правил. Электронное письмо нельзя послать непосредственно получателю – сначала оно попадает на сервер, на котором зарегистрирована учетная запись отправителя. Тот, в свою очередь, отправляет "посылку" серверу получателя, с которого последний и забирает сообщение.

FTP – файловый сервер. В его задачи входит хранение файлов и обеспечение доступа к ним клиентских ПК, например, по протоколу FTP. Ресурсы файл-сервера могут быть либо открыты для всех компьютеров в сети, либо защищены системой идентификации и правами доступа.

Эмулятор Cisco Packet Tracer позволяет проводить настройку таких сетевых сервисов, как: HTTP, DHCP, TFTP, DNS, NTP, EMAIL, FTP в составе сервера сети. Рассмотрим настойку некоторых из них.

1.5 Лабораторная работа Настройка сетевых сервисов

1.5.1 Настойка WEB сервера (протокол HTTP)

WEB (HTTP) сервер – позволяет создавать простейшие веб–странички и проверять прохождение пакетов на 80-ый порт сервера. Эти серверы предоставляют доступ к веб-страницам и сопутствующим ресурсам, например, картинкам (https://www.intuit.ru/studies/courses/3549/791/lecture/29220). Открываем программу CPT и моделируем сеть как на картинке ниже (рис. 7).

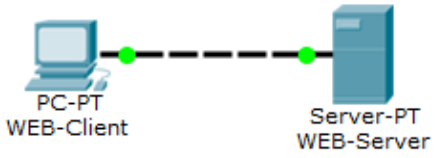


Рисунок 7 – Схема сети

Отрываем вкладки *Desktop* на рабочем компьютере (Web Client) и сервере (Web Server), далее переходим в окно *IP Configuration*.

Указываем IP-адреса (нужны для идентификации узлов в сети) в поля под цифрой 3, вводим маску подсети (нужна для того, чтобы узлу было понятно, в одной подсети он находится с другим узлом или нет) (рис. 8).

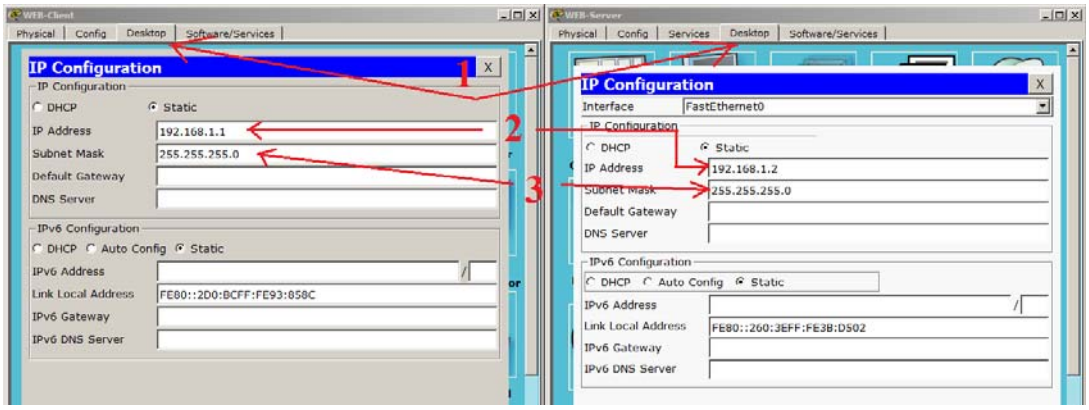


Рисунок 8 – Конфигурирование ПК

Создаем WEB-документ на сервере.

Открываем на сервере вкладку Services, а затем HTTP и редактируем первую (стартовую) страницу сайта с названием index.html. Набираем следующий код:

```
<html>
<body>
<h1>Welcome to WEB–Server CISCO!</h1>
<p>Server working: <font color="red"><b>OK!</b></font></p>
</body>
</html>
```

Добавить новую страницу + , удалить текущую X , переключение между страницами < | > . Текст можно переносить в окно через буфер обмена. Он может быть только на английском языке (рис. 9).

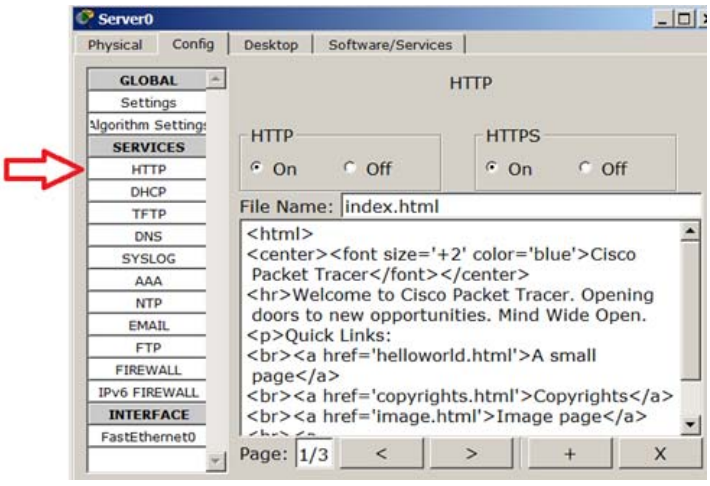


Рисунок 9 – Вкладка Config, служба сервера HTTP

Включаем службу HTTP и HTTPS переключателем On.

HTTPS (HyperText Transfer Protocol Secure), это расширение протокола HTTP, которое поддерживает криптографические протоколы и передает информацию не в открытом виде, а в зашифрованном.

Запоминаем: HTTP использует 80 порт, а HTTPS 443 порт.

Для проверки работоспособности сервера, открываем клиентскую машину и на вкладке *Desktop* (Рабочий стол) запускаем приложение *Web Browser* (рис. 10). После чего набираем адрес WEB–сервера 192.168.1.2 и нажимаем на кнопку *GO*. Убеждаемся, что веб-сервер работает.

Рисунок 10 – Текст web–страницы

Для отчета, сохранить файл с именем HTTP.pkt.

1.5.2 Настойка DNS сервера

https://habr.com/ru/post/307714/

DNS сервер – (Domain Name System), система доменных имен, позволяет организовать службу разрешения доменных имён. Функция DNS сервера заключается в преобразовании доменных имен серверов в IP-адреса.

Эта лабораторная работа основывается на предыдущей. Поэтому адресация будет такой же. Моделируем сеть как на картинке ниже (рис. 11).

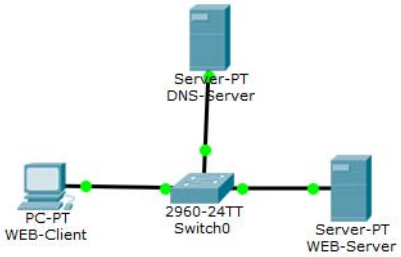


Рисунок 11 – Моделируемая сеть

Добавлен еще один сервер, который будет выполнять роль DNS сервера и коммутатор. Когда в сети появляются 3 и более устройств, то для их соединения используют коммутатор.

В *Desktop-IP Configuration* DNS сервера пропишем IP адрес с маской. Затем зайдем в Services (сервисы) и настроим DNS службу (рис. 12).

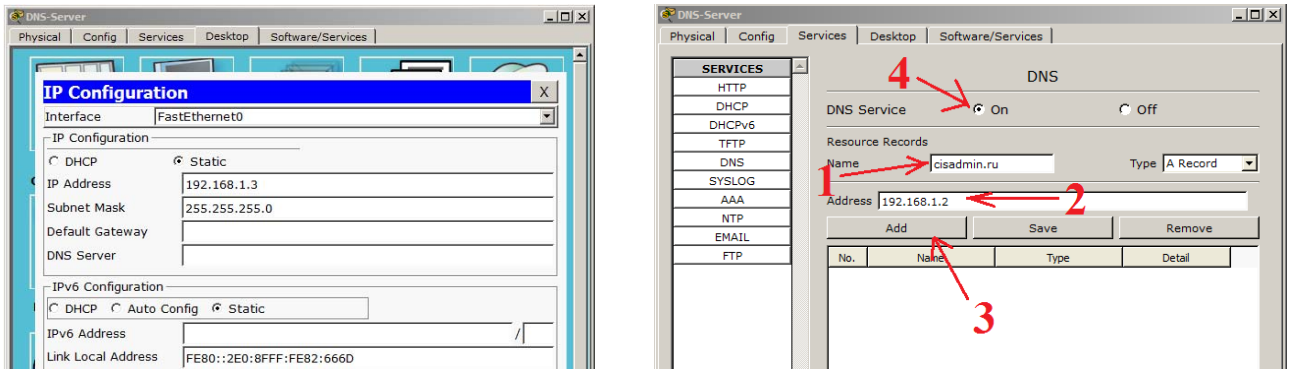


Рисунок 12 – Настройка DNS службы

В окне *Name* запишем имя, которое хотим привязать к IP адресу. (например, *cisadmin.ru*). В окне *Address*, соответственно, IP-адрес, который будет работать в связке с выше написанным именем. (здесь укажем тот же адрес, что и в лабораторной по HTTP – *192.168.1.2*). Нажимаем кнопку *Add*, чтобы добавить эту запись. Не забываем включить саму службу (рис. 13).

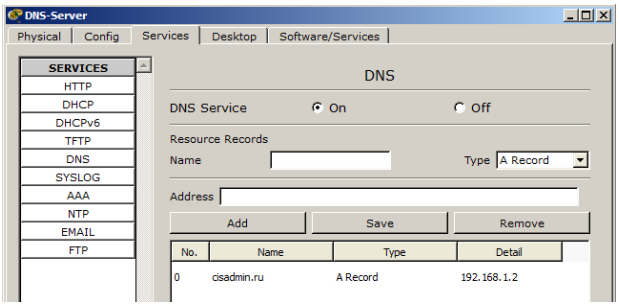


Рисунок 13 – Результат

Теперь надо в настройках Web сервера и компьютера (Web клиента) во вкладке *Desktop-IP Configuration* указать адрес DNS сервера (рис. 14).

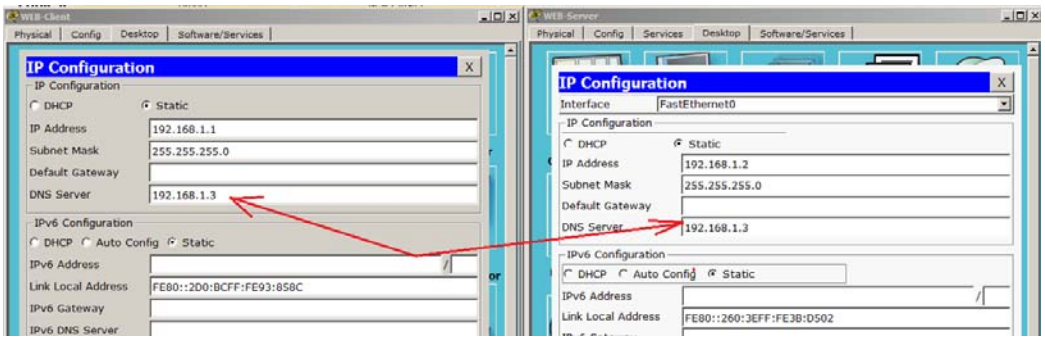


Рисунок 14 – Настройка Web сервера и компьютера

Настройка DNS сервера и узлов закончена. Проверим работоспособность.

Переключаем среду в режим симуляции и попробуем с компьютера зайти на сайт по имени «cisadmin.ru» (*Desktop–web Browser*) (рис. 15).

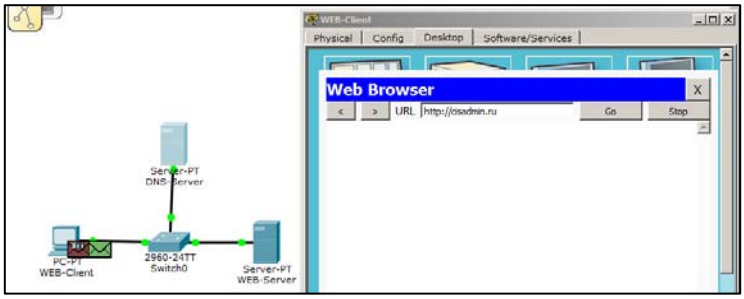


Рисунок 15 – Проверка работоспособности

В результате по имени «cisadmin.ru» откроется страница, находящаяся на сервере с IP адресом 192.168.1.2. Сайт открывается по доменному имени (рис. 16).

Рисунок 16 – Результат

Утилита nslookup

Она позволяет обратиться к DNS серверу и узнать у него информацию о имени или IP–адресе (рис. 17). Кликаем по компьютеру на схеме и на вкладке *Desktop* выбираем *Command Prompt*. Это имитация командной строки.

Введя знак **?**, можно получить список всех доступных команд. Введем *nslookup* и нажмем ENTER.

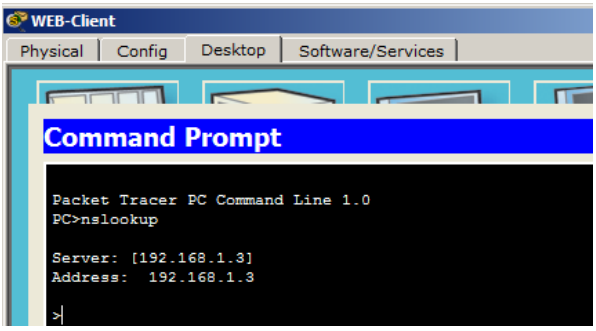


Рисунок 17 – Утилита nslookup

Открывается сама утилита, о чем свидетельствует знак птички слева. Показывается нам адрес DNS сервера и его имя. Так как имени нет, то он дублирует туда строку с IP–адресом. Впишем доменное имя сайта *cisadmin.ru*. Выдастся имя и IP адрес (рис. 18).

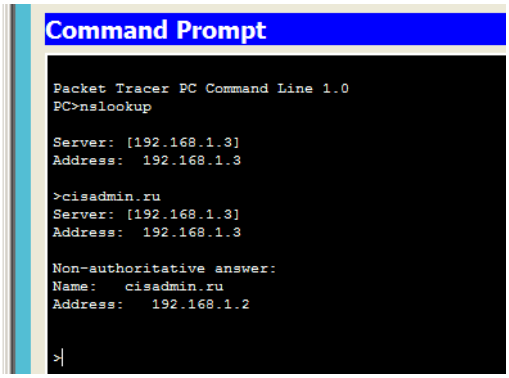


Рисунок 18 – Результат

Есть еще один файл в каждой ОС, который тесно связан с DNS. Название у него «hosts» ➢.

Для отчета, сохранить файл с именем DNS.pkt.

1.5.2 Настройка DHCP сервера

DHCP сервер (Dynamic Host Configuration Protocol) – протокол динамической настройки узла. Он позволяет узлам динамически получать IP адреса и другие параметры для корректной работы в сети (основной шлюз, маску подсети, адреса DNS серверов). При помощи DHCP можно обеспечить полный контроль над IP адресами: создавать отдельные пулы для каждой подсети, выдавать адреса в аренду, резервировать адреса и многое другое. ➢.

Моделируем сеть как на картинке ниже (рис. 19).

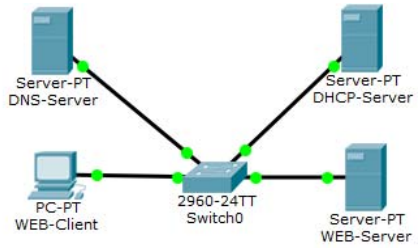


Рисунок 19 – Моделируема сеть

Настроим сервер. Присваиваем свободный адрес и маску (рис. 20).

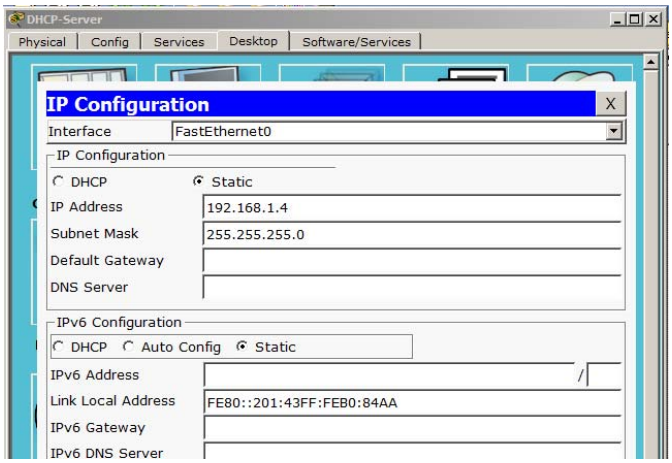


Рисунок 20 – Настройка сервера

Выбираем службу DHCP (рис. 21).

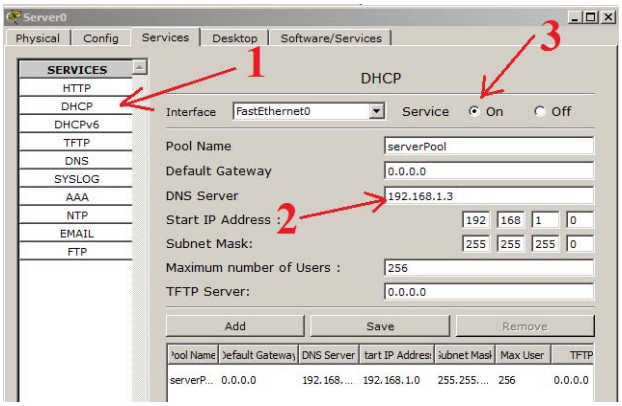


Рисунок 21 – служба DHCP

Здесь уже создан стандартный пул IP адресов. Его удалить нельзя. Только изменить.

Можно добавить адрес шлюза, адрес DNS сервера. Мы пока не касались вопроса шлюза, поэтому пока не будем его трогать. DNS сервер у нас есть, и его можно указать. Старт адресов оставим, как есть.

Включить сервер! Переключаем среду в режим симуляции и посмотрим, как компьютер получит адрес. Соответственно переходим в настройки конфигурации и переключаем на DHCP (рис. 22).

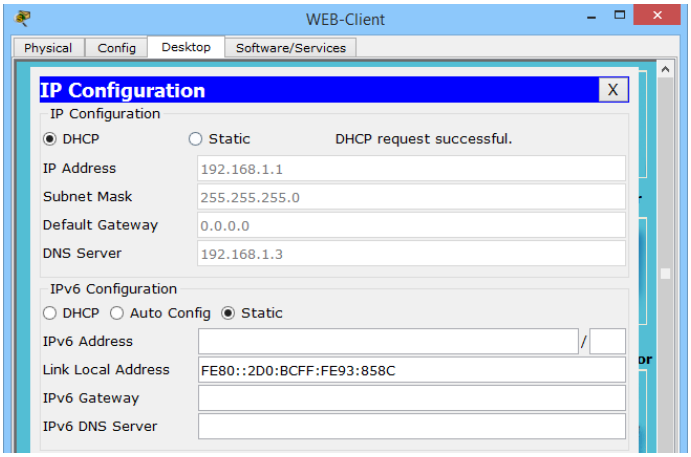


Рисунок 22 – Результат

Для отчета, сохранить файл с именем DHCP.pkt

1.5.3 Настройка почтового сервера

POP3 (Post Office Protocol Version 3, протокол почтового отделения версии 3). Клиент заходит на сервер и смотрит, есть ли для него письмо. И если оно присутствует, он загружает его к себе и ставит отметку об удалении на сервере («загрузи и удали»).

- POP3. Порт, который прослушивается протоколом – 110.

У него есть расширенная версия – POP3S. При помощи криптографического протокола SSL шифруется содержимое и письма передаются в защищенном виде. POP3S использует 995 порт.

Аналог POP3 – протокол IMAP (Internet Message Access Protocol, протокол доступа к электронной почте). Их различие в том, что клиент, заходя на сервер, не удаляет почту, а копирует ее. Таким образом, у клиента отображается копия почтового ящика, который хранится на почтовом сервере. И если клиент у себя удаляет какое–либо письмо, то оно удаляется только у него. На сервере оригинал остается целым.

- IMAP. Слушает он 143 порт.

SMTP (Simple Mail Transfer Protocol). Простой протокол передачи почты. Используется он для передачи почты на почтовый сервер.

- SMTP. Использует он 25 порт.

Важно помнить, что все почтовые протоколы работают по TCP-соединению. Это значит, что перед тем, как начнет работать почтовый протокол, а в данном случае протокол SMTP, должно установиться предварительное соединение между компьютером и сервером.

Открыть предыдущую работу по DHCP и изменить схему (рис. 23).

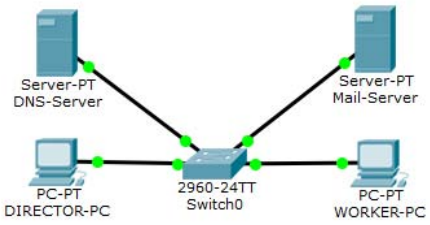


Рисунок 23 – Моделируемая схема

Убрать HTTP сервер и вместо него добавить компьютер рабочего, назвать WORKER-PC. Присвоить ему IP-адрес, который был у HTTP сервера. То есть 192.168.1.2. Старый компьютер переименовать в DIRECTOR-PC. DNS-Server оставить. Сервер DHCP переименовать в Mail-Server. И его настроить (рис. 24).

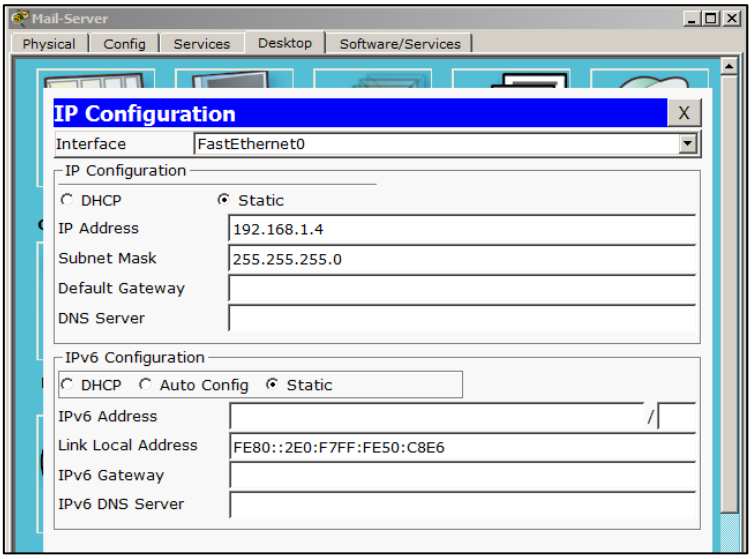


Рисунок 24 – Настройка Mail-Server

Переходим в службы и находим «*EMAIL*».

В поле «*Domain Name*» надо записать имя домена. Это то, что будет писаться после знака "@". Любая почта записывается в таком формате – логин@домен. Нажимаем кнопку «*Set*» (рис. 25).

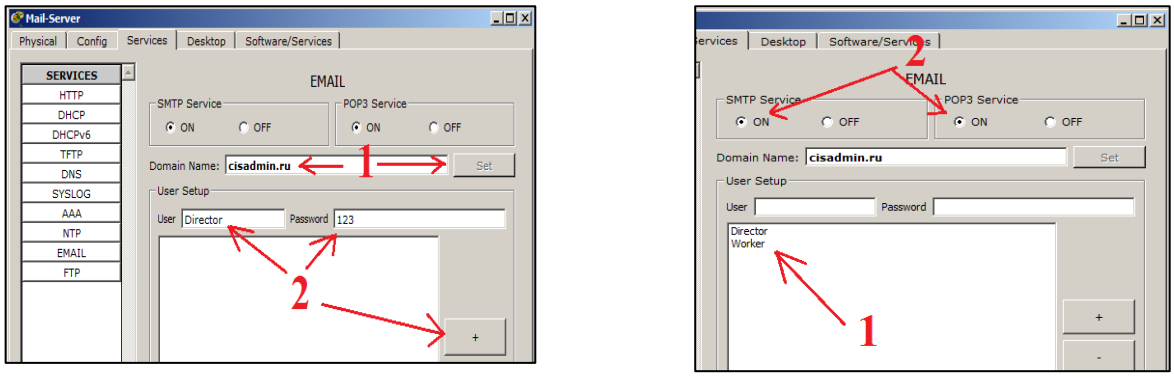


Рисунок 25 – Настройка «EMAIL»

Создадим пользователей. В поле «User» запишем первого пользователя *Director*. Зададим пароль «123». Нажимаем на знак "+", чтобы добавить его в базу. Аналогично создадим второго пользователя. Это будет *Worker* с таким же паролем «123».

Видим в базе список созданных пользователей. Их можно удалять, добавлять и менять пароли при помощи кнопок справа. Не забываем включить службы POP3 и SMTP, если они отключены. Настройка на стороне сервера закончена.

Настройка на стороне клиентов

Настройка компьютера *Director*. Открываем вкладку *Desktop* и выбираем Email. Откроется окно настройки (рис. 26).

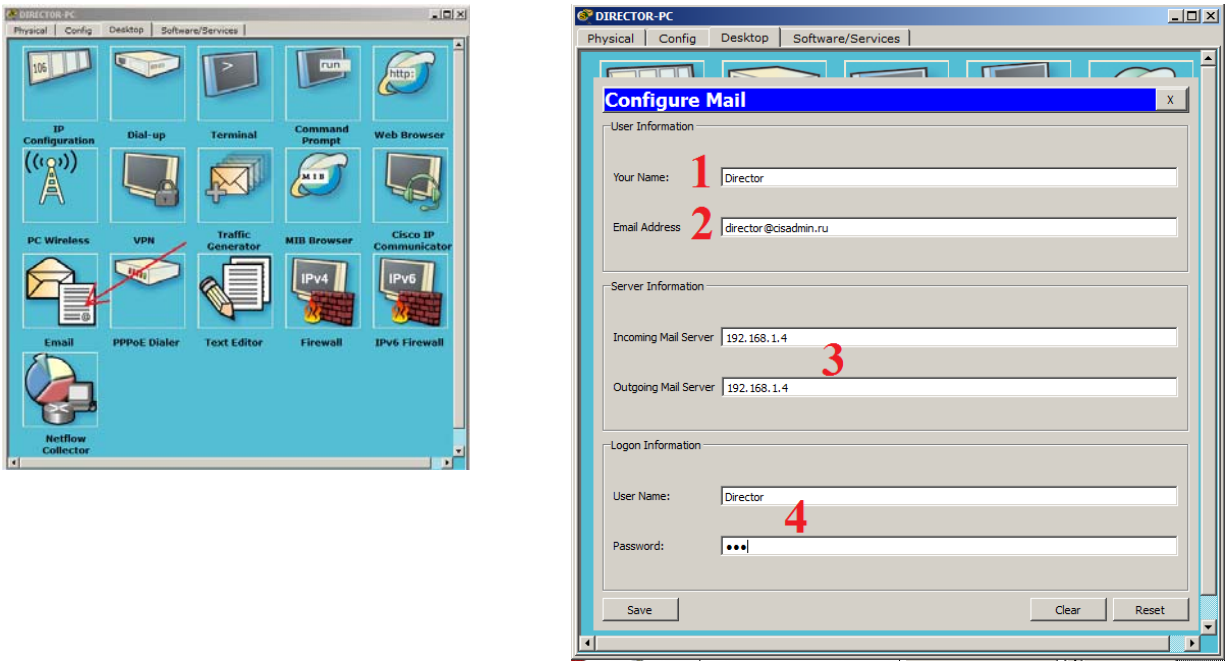


Рисунок 26 – Настройка на стороне клиентов

В поле «*Your Name*» пишем Director. В поле «*Email Address*» пишем почтовый ящик, director@cisadmin.ru.

В поля «*Incoming Mail Server*» (Сервер входящей почты) и «Outgoing Mail Server» записываем адрес почтового сервера (192.168.1.4). В поле «*User Name*»

пишем логин Director и пароль 123. Нажимаем кнопку *Save*. Открывается почтовый клиент (почтовый обозреватель) (рис. 27).

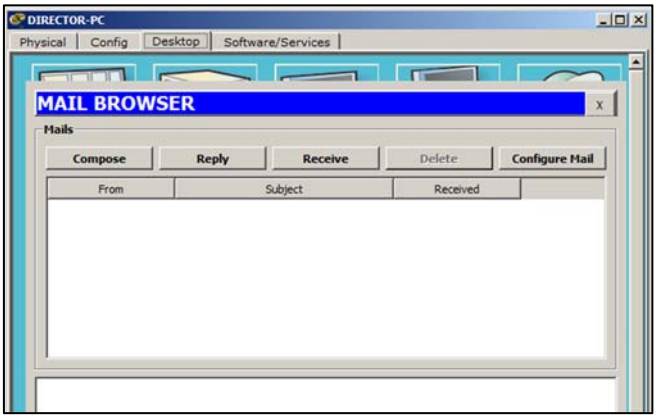


Рисунок 27 – Почтовый обозреватель

Аналогичная настройка будет на компьютере Worker (рис. 28).

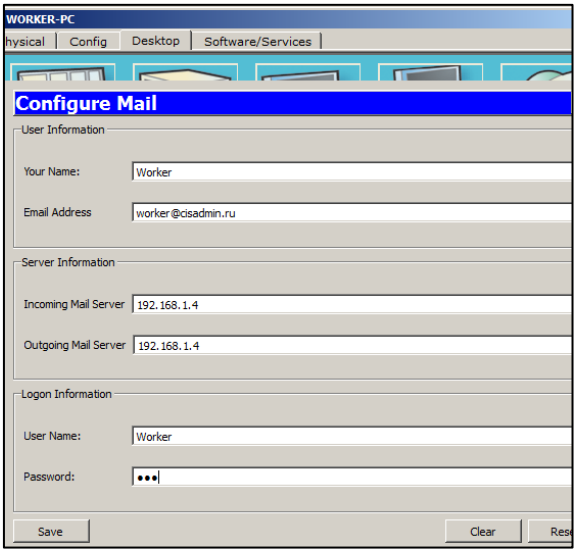
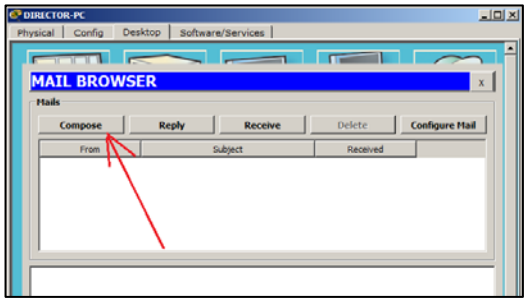


Рисунок 28 – настройка на компьютере Worker

Работа почты в режиме реального времени

Открываем почтовый клиент на компьютере директора и создадим письмо. Жмем на кнопу Compose, открывается привычное окно (рис. 29).



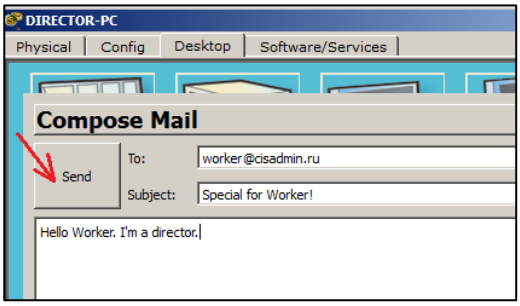


Рисунок 29 – Создаем письмо

Пишем кому отправляем, тему письма, сам текст письма и нажимаем кнопку Send (рис. 30). Видим следующее сообщение о том, что отправка завершена успешно.

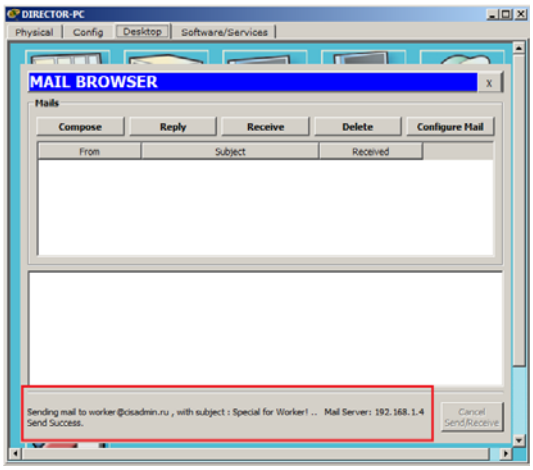


Рисунок 30 – Отправляем письмо

Посмотрим, как письмо будет доставлено рабочему. Открываем почтовый клиент на компьютере рабочего. Нажимаем кнопку Receive, обновление. Видим появившееся письмо и сообщение об успешном получении (рис. 31).

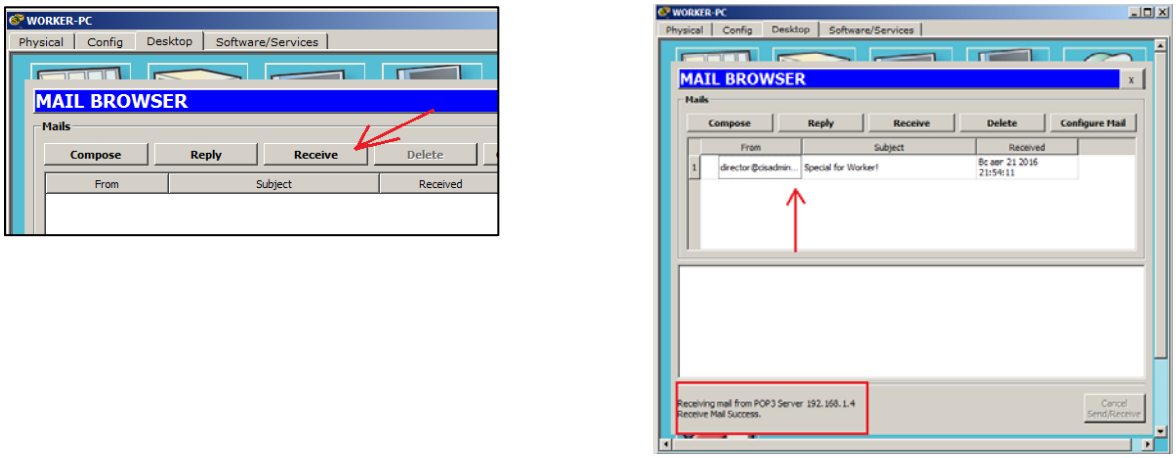


Рисунок 31 – Почтовый клиент на компьютере Worker

Откроем письмо, ответим на него, нажав на кнопку Reply и отправим письмо директору (рис. 32).

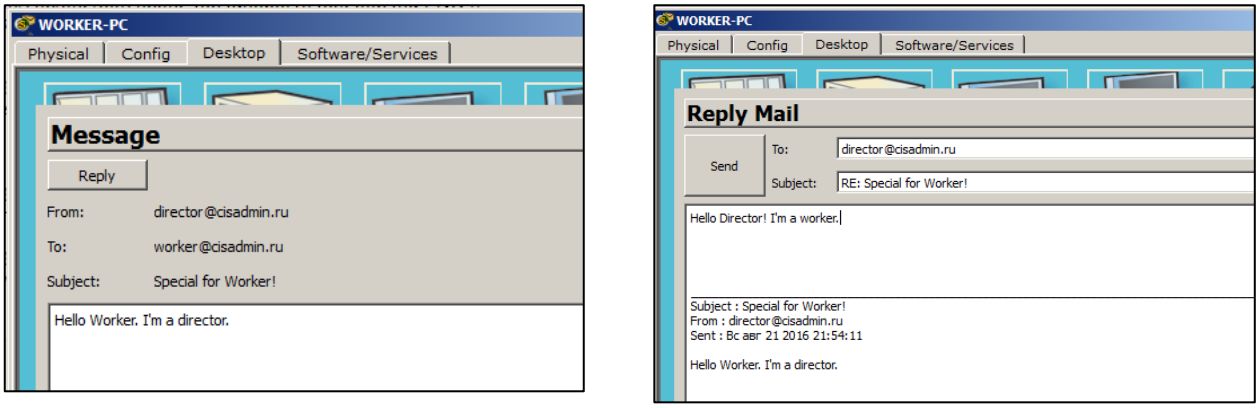


Рисунок 32 – Отправляем письмо директору

Проверим письмо на компьютере директора. Нажимаем кнопку Receive, чтобы обновить почту и видим, что письмо дошло (рис. 33).

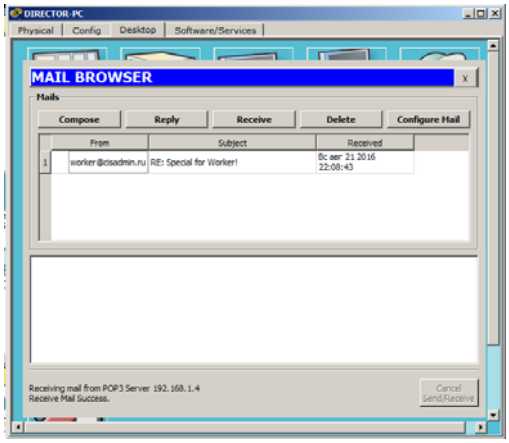


Рисунок 33 – Результат

Открываем письмо, чтобы до конца удостовериться (рис. 34).

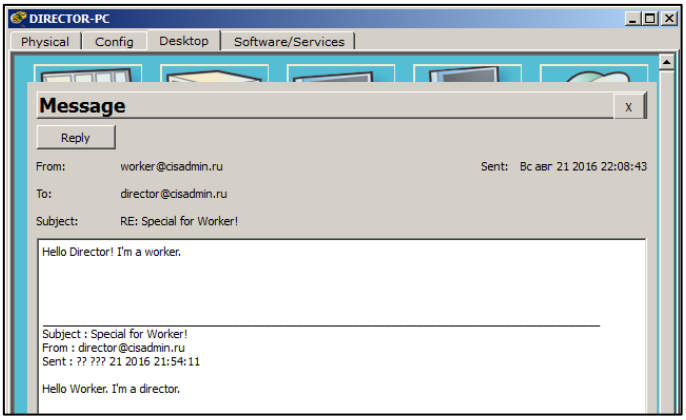


Рисунок 34 – Проверка

Переключитесь в режим симуляции, напишите ответ и проанализируйте подробно процесс (установление TCP-сессии, работа протокола SMTP, установка портов) (рис. 35).

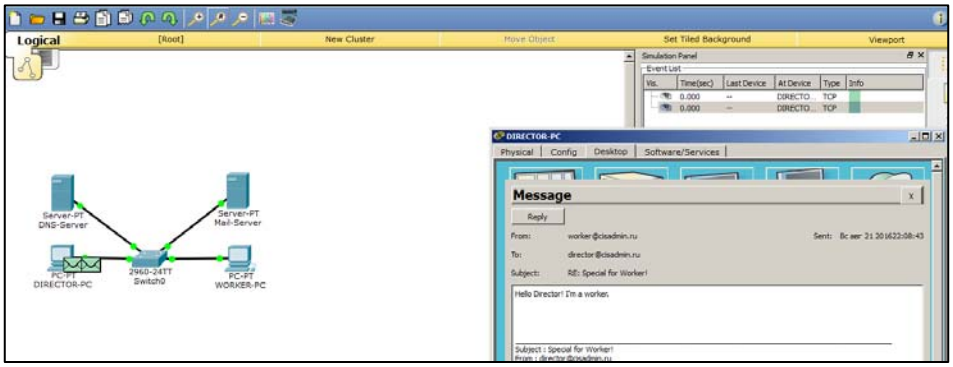


Рисунок 35 – Режим симуляции

Для отчета, сохранить файл с именем POP3.pkt.

1.5.4 Настройка Telnet

Telnet (terminal network, сетевой терминал**).** Основы этого протокола были заложены давно, и до сих пор он не теряет своей актуальности. Применяется он для отображения текстового интерфейса, а также для управления ОС.

Достоинство. Каждое сетевое устройство, интерфейс которого представляет собой командную строку, настраивается либо при помощи специального консольного кабеля, либо через виртуальные терминалы, в который и входит протокол Telnet. Если консольный кабель требует нахождения специалиста рядом с настраиваемым оборудованием, то настройка при помощи виртуальных терминалов, а в данном случае Telnet, не ограничивает специалиста в расстоянии.

- Использует Telnet 23 порт.

А самые популярные дистрибутивы, которые работают с этим протоколом – это Putty, Kitty, XShell и т.д.

Недостаток. Он фактически не защищенный и все передается в открытом виде.

Telnet работает точно так же, как и почтовые протоколы, то есть создается TCP-сессия, и, после установления соединения, начинает работать Telnet. Как только он отрабатывает, он начинает разрывать соединение.

Использовать Telnet будем для доступа к коммутатору Cisco 2960. Он, как и все Cisco устройства, использует разработанную компанией Cisco операционную систему IOS. А интерфейс командной строки называется *CLI* (Command Line Interface).

Настроим коммутатор

Зададим IP-адрес и разрешим доступ по Telnet.

Список вводимых команд:

Switch>enable – переход в привилегированный режим. Отсюда доступно большинство команд.

Switch#**configure terminal** – переход в режим глобальной конфигурации. В этом режиме возможен ввод команд, позволяющих конфигурировать общие характеристики системы. Из режима глобальной конфигурации можно перейти во множество режимов конфигурации, специфических для конкретного протокола или функции.

Switch(config)#**username** admin **secret** cisco – создаем пользователя с именем admin и паролем cisco.

Switch(config)#**interface vlan 1** – переходим в виртуальный интерфейс vlan 1 и зададим IP-адрес. Не важно, на каком именно из 24-х портов коммутатора он будет задан. Главное, чтобы с какого-либо порта был доступ до него.

Switch(config–if)#**ip address 192.168.1.254 255.255.255.0** – присваиваем последний адрес 192.168.1.254 с маской 255.255.255.0

Switch(config–if)#**no shutdown** – по умолчанию интерфейс выключен, поэтому включаем его. В IOS 90% команд отменяются или выключаются путем приписывания перед командой «no».

Switch(config)#**line vty 0 15** – переходим в настройки виртуальных линий, где как раз живет Telnet. От 0 до 15 означает, что применяем это для всех линий. Всего можно установить на нем до 16 одновременных соединений.

Switch(config–line)#**transport input all** – разрешаем соединение для всех протоколов, так как позже будет рассматриваться другой протокол.

Switch(config–line)#**login local** – указываем, что учетная запись локальная, и он будет проверять ее с той, что мы создали.

Switch#**copy running-config startup-config** – обязательно сохраняем конфигурацию. Иначе после перезагрузки коммутатора все сбросится. Коммутатор настроен.

Подключимся к нему с рабочего компьютера. Открываем командную строку и пишем команду *telnet* и адрес, куда подсоединиться (рис. 36):

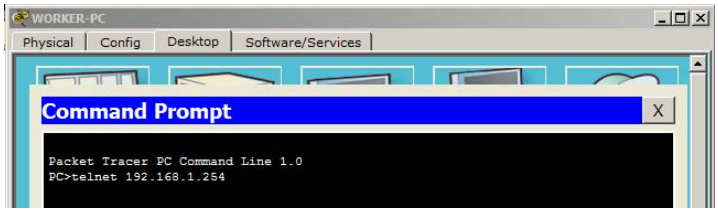


Рисунок 36 – Команда подключения к telnet

Открывается окно с запросом логина и пароля (рис. 37).

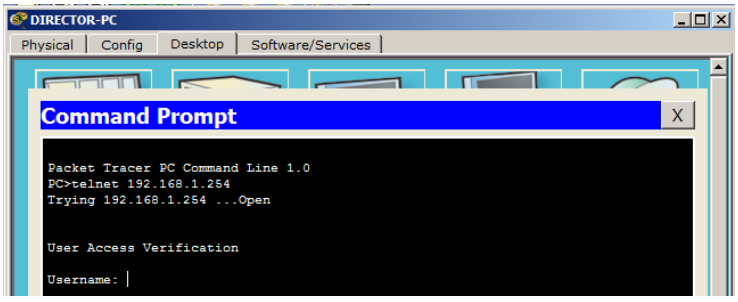


Рисунок 37 – Окно с запросом логина и пароля

Пишем логин: *admin* и пароль: *cisco*. Проверим доступность компьютера директора, при помощи команды *ping* (рис. 38).

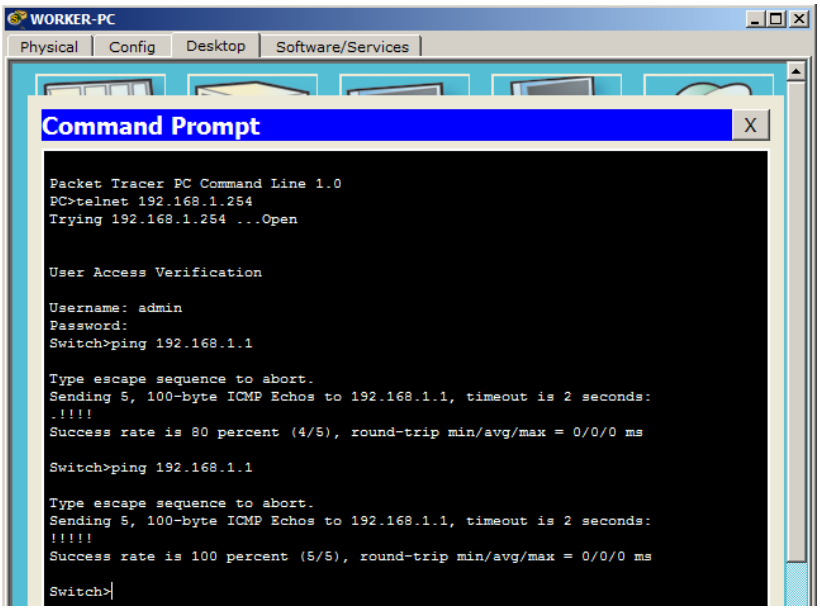


Рисунок 38 – Доступность компьютера директора

Ping успешен.

➢ Проверка доступности осуществляется не с компьютера рабочего, а с коммутатора. Компьютер здесь является управляющим устройством.

Для отчета, сохранить файл с именем Telnet.pkt

1.5.4 Настройка SSH протокола

SSH (Secure Shell, безопасная оболочка**).** Как и Telnet позволяет управлять ОС. Отличие его в том, что он шифрует весь трафик и передаваемые пароли. Шифруется при помощи алгоритма Диффи-Хеллмана. Практически все современные ОС системы умеют работать с этим протоколом.

Если у вас стоит выбор, какой протокол применять, то используйте SSH. Подключаться и управлять будем тем же коммутатором. Давайте попробуем подключиться по SSH с компьютера директора к коммутатору (рис. 39).

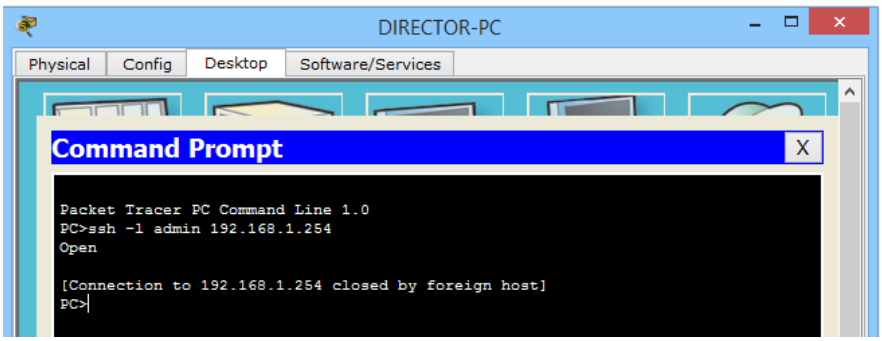


Рисунок 39 – Подключени по SSH

Синтаксис команды немного другой, нежели при подключении по Telnet. Пишем *ssh* с ключом l, после набираем логин (у нас это admin) и адрес, куда подключаемся (192.168.1.254). Завершаем это дело клавишей ENTER.

Выдается сообщение, что соединение было закрыто внешним хостом. То есть коммутатор закрыл соединение. Все потому, что не были созданы ключи, которые работают с шифрованием.

Зайдем на коммутатор и настроим его для корректной работы по SSH.

Switch(config)#hostname SW1 – меняем имя коммутатора. С этим стандартным именем нельзя прописать домен, который нужен для генерации ключей.

SW1(config)#ip domain-name cisadmin.ru – *прописываем домен.*

SW1(config)#crypto key generate rsa – *генерируем RSA ключи.*

The name for the keys will be: SW1.cisadmin.ru (Название ключей будет следующим: SW1.cisadmin.ru).

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: (Выберите размер модуля ключа в диапазоне от 360 до 2048 для ваших ключей общего назначения. Выбор модуля ключа больше 512 может занять несколько минут. Сколько бит в модуле [512]: 1024).

1024 – *Указываем размер ключа. По умолчанию предлагается 512.* % Generating 1024 bit RSA keys, keys will be non–exportable. *(*% Генерация 1024–битных ключей RSA, ключи не будут экспортироваться). [OK] Выходит сообщение об удачной генерации ключей.

Настройка завершена, и попробуем еще раз подключиться к коммутатору (рис. 40).

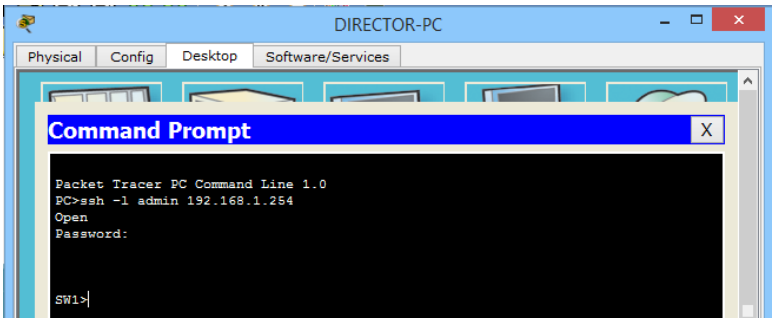


Рисунок 40 – Подключение к коммутатору

Выдается сообщение с запросом на ввод пароля. Вводим пароль «*cisco*» и оказываемся на коммутаторе.

Воспользуемся командой *ping* и проверим доступность рабочего компьютера (рис. 41).

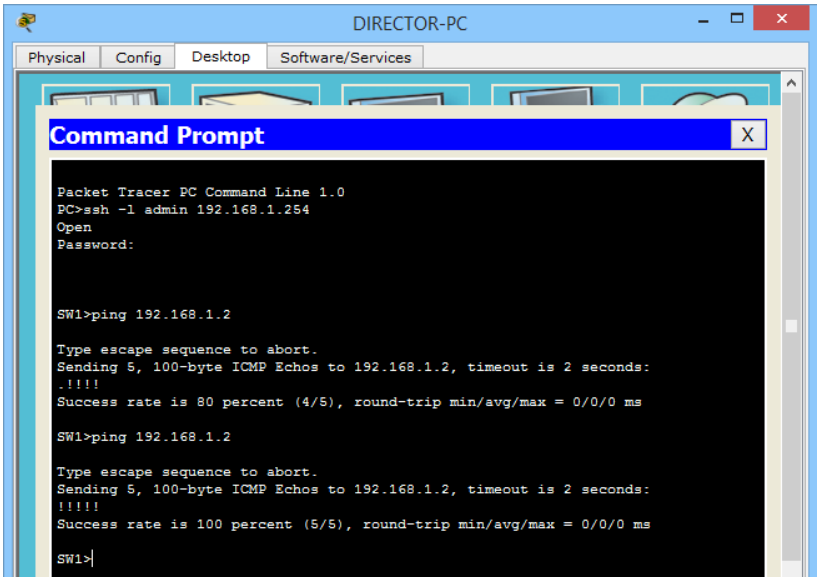


Рисунок 41 – Доступность рабочего компьютера

Для отчета, сохранить файл с именем SSH.pkt.

Самостоятельное задание

Создайте следующую схему сети, представленную на рис. 42:

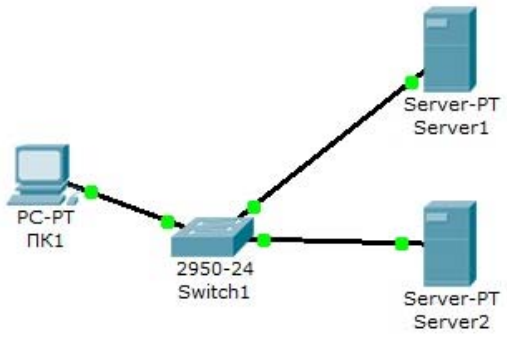


Рисунок 42 – Схема сети

Настроить сеть следующим образом:

1 – Server1 – DNS и Web сервер;

2 – Server2 – DHCP сервер;

3 – Компьютер ПК1 получает параметры протокола TCP/IP с DHCP сервера и открывает сайт www.rambler.ru на Server1.

Варианты

№ n	IP	Фраза на web сервере	Пул адресов

Этапы выполнения

1. Задайте в конфигурации серверов следующие настройки IP:

Server1: IP адрес – 10.0.0.1, маска подсети – 255.0.0.0

Server2: IP адрес – 10.0.0.2, маска подсети – 255.0.0.0

2. Войдите в конфигурацию ПК1 и установите настройку IP через DHCP сервер.

3. Настройте службу DNS на Server1 (задайте две ресурсные записи в прямой зоне DNS, задайте стартовую страницу сайта WWW.RAMBLER.RU, проверьте работу службы DNS командой nslookup).

4. Настройте DHCP службу на Server2.

5. Осуществите проверку работы клиента.

Войдите в конфигурации хоста ПК1 на рабочий стол и в командной строке сконфигурируйте протокол TCP/IP.

Командой PC>ipconfig /release сбросить старые параметры IP адреса, командой: PC>ipconfig /renew получить новые параметры с DHCP сервера.

Откройте сайт WWW.RAMBLER.RU в браузере на клиенте.

Для отчета сохраните файл с именем SServis.pkt. В отчете представить этапы настройки со скринами результатов выполненных этапов.

Контрольные вопросы

Что такое рекурсивный запрос DNS и какова схема его работы? Укажите назначение типов ресурсных записей в прямой и обратной зонах DNS. Как на DNS сервере настраивается пересылка пакетов на другие DNS сервера? Опишите работу службы DHCP. Этапы настройки в Cisco пакете. Как настраивается клиент DHCP? Этапы настройки в Cisco пакете. Укажите местоположения папки с контентом Web узла и FTP сервера. Как определяется состав обратных зон DNS сервера в корпоративной сети. Продемонстрируйте настройку служба DNS в Cisco Packet Tracer? Продемонстрируйте настройку служба DHCP в Cisco Packet Tracer? Продемонстрируйте настройку служба FTP в Cisco Packet Tracer? Продемонстрируйте настройку WEB сервер в Cisco Packet Tracer?

2 ОСНОВНЫЕ КОМАНДЫ ОПЕРАЦИОННОЙ СИСТЕМЫ CISCO IOS

Теоретические сведения

Большинство сетевых устройств компании CISCO допускают конфигурирование. Для этого администратор сети должен подключиться к устройству через прямое кабельное (консольное) подключение ➢.

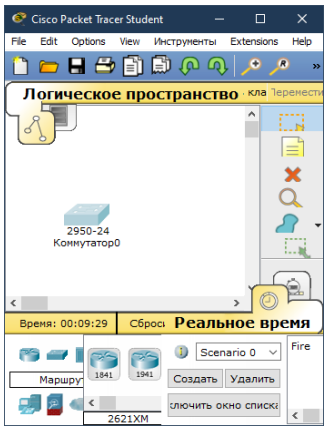
Подключив консоль и получив доступ к устройству через командную строку, администратор сети может определять параметры конфигурации оборудования.

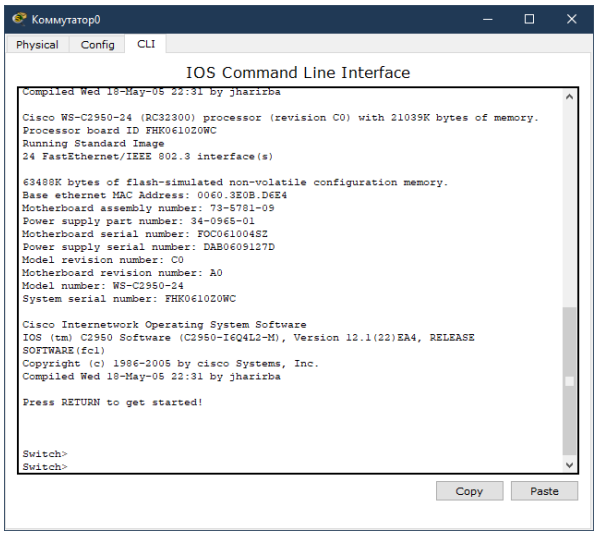
В Cisco Packet Tracer интерфейс командной строки устройств доступен в окне настроек на вкладке *CLI*. Это окно имитирует прямое консольное подключе-

ние к сетевому устройству. Настройка (программирование) сетевого устройства производится с помощью команд операционной системы *Cisco IOS*.

Для настройки сетевого оборудования в вашем распоряжении имеются разнообразные команды операционной системы Cisco IOS. Создайте на рабочем столе CPT коммутатор.

При входе в сетевое устройство (ПКМ по устройству) командная строка имеет вид: Switch>:





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

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

Press ENTER to get start.

Switch>

Switch> enable

Switch#

О переходе в привилегированный режим будет свидетельствовать появление в командной строке приглашения в виде знака #. Из привилегированного уровня можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая режимы конфигурирования интерфейса, подъинтерфейса, линии, сетевого устройства, карты маршрутов и т.п.

Выход из привилегированного режима:

Switch# disable

Switch>

Для выхода из системы IOS необходимо набрать на клавиатуре команду exit (выход):

Switch> **exit**

Возможна работа в следующих режимах:

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

Switch>

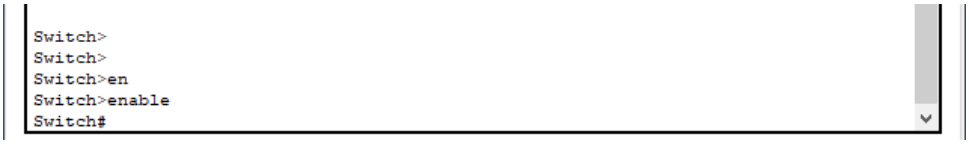
– привилегированный режим – поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. В этом режиме приглашение имеет вид:

Switch#

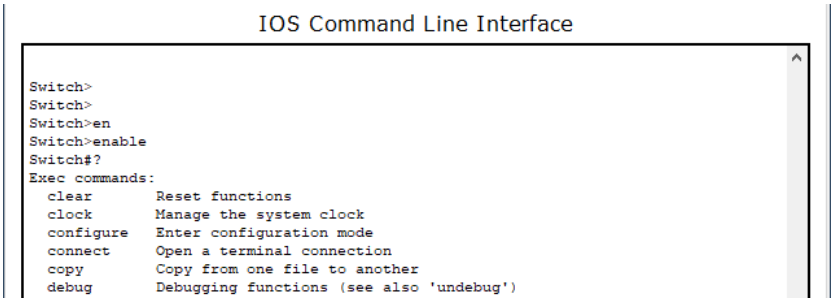
– режим глобального конфигурирования – реализует мощные однострочные команды, которые решают задачи конфигурирования. В том режиме приглашение имеет вид:

Switch(config)#

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



При вводе в командной строке любого режима имени команды и знака вопроса (?) на экран выводятся комментарии к команде:



При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много экранов строк, поэтому иногда внизу экрана будет появляться подсказка – More. Для продолжения следует нажать enter или пробел.

Команды режима глобального конфигурирования определяют поведение системы в целом. Кроме этого, команды режима глобального конфигурирования

включают команды переходf в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд.

Для входа в режим глобального конфигурирования используется команда привилегированного режима configure. При вводе этой команды следует указать источник команд конфигурирования:

– terminal (терминал),

– memory (энергонезависимая память или файл),

– network (сервер tftp (Trivial ftp – упрощённый ftp) в сети).

По умолчанию команды вводятся с терминала консоли, например:

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

Команды для активизации частного вида конфигурации должны предваряться командами глобального конфигурирования. Так для конфигурации интерфейса, на возможность которой указывает приглашение:

```
Switch(config-if)#
```

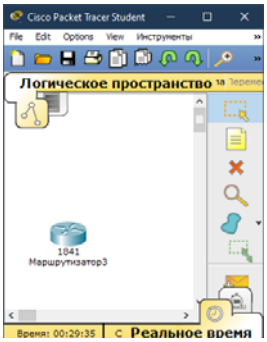
сначала вводится глобальная команда для определения типа интерфейса и номера его порта:

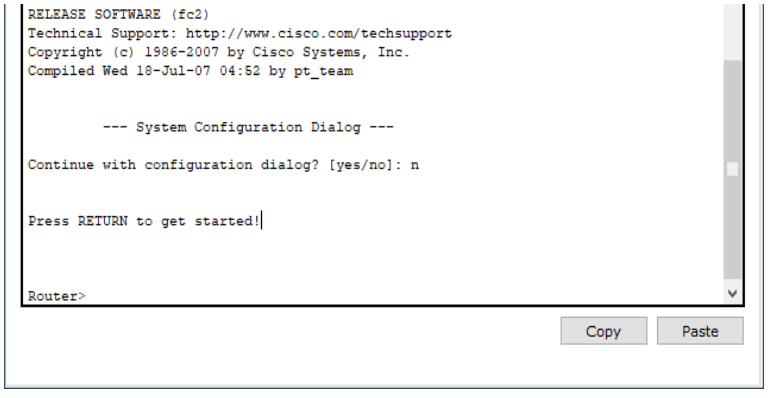
```
Switch#conf t
Switch(config)#interface type port
Switch(config-if)#(commands)
Switch(config-if)#exit
Switch(config)#exit
```

2.1 Лабораторная работа Знакомство с командами IOS

Основные команды сетевого устройства:

1. Войдите в настройки сетевого устройства Router (коммутатор) и нажмите *Enter*:





2. Теперь войдите в привилегированный режим:

Router>enable — Router#

3. Просмотрите список доступных команд в привилегированном режиме:

Router#**?** Клавишу Enter нажимать не надо.

4. Перейдём в режим конфигурации:

Router#config terminal — Router(config)#

5. Когда вы входите в роутер, вы видите его Имя перед символом режима (">" или "#"). Имя устройства используется для его идентификации. Установите "Router1" как имя вашего роутера:

Router(config)#hostname Router1 — Router1(config)#

6. Пароль доступа позволяет контролировать доступ в привилегированный режим. Установите пароль доступа "parol":

Router1(config)#enable password parol

7. Перейдите в пользовательский режим (команды: exit и disable), и попытайтесь зайти в привилегированный режим:

Router1(config)# exit — Router1#disable – Router1>enable — Password:*****

Для сброса пароля можно произвести перезагрузку роутера.

Основные Show команды

Перейдите в пользовательский режим командой disable. Введите команду для просмотра всех доступных show команд.

Router1>show ?

1. Команда show version используется для получения типа платформы сетевого устройства, версии операционной системы, имени файла образа операционной системы, время работы системы, объём памяти, количество интерфейсов и конфигурационный регистр.

2. Просмотр времени:

Router1>show clock

3. Во флеш-памяти сетевого устройства сохраняется файл-образ операционной системы Cisco IOS. В отличие от оперативной памяти, в реальных устройствах флеш память сохраняет файл-образ даже при сбое питания.

Router1>show flash

4. ИКС сетевого устройства по умолчанию сохраняет10 последних введенных команд

Router1>show history

5. Две команды позволят вам вернуться к командам, введённым ранее. Нажмите на стрелку вверх или <ctrl> P.

6. Две команды позволят вам перейти к следующей команде, сохранённой в буфере. Нажмите на стрелку вниз или <ctrl> N

7. Можно увидеть список хостов и IP-Адреса всех их интерфейсов:

```
Router1>show hosts
```

8. Следующая команда выведет детальную информацию о каждом интерфейсе:

```
Router1>show interfaces
```

9. Следующая команда выведет информацию о каждой telnet сессии:

```
Router1>show sessions
```

10. Следующая команда показывает конфигурационные параметры терминала:

```
Router1>show terminal
```

11. Можно увидеть список всех пользователей, подсоединённых к устройству по терминальным линиям:

```
Router1>show users
```

12. Команда:

```
Router1>show controllers
```

показывает состояние контроллеров интерфейсов.

13. Перейдём в привилегированный режим.

```
Router1>en
```

14. Введите команду для просмотра всех доступных show команд:

```
Router1#show ?
```

Привилегированный режим включает в себя все show команды пользовательского режима и ряд новых.

15. Посмотрим активную конфигурацию в памяти сетевого устройства. Необходим привилегированный режим. Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания. Чтобы сохранить настройки роутера используйте следующие команды:

сохранение текущей конфигурации:

```
Router# write memory
```

Или

```
Router# copy run start
```

Просмотр сохраненной конфигурации:

Router# Show configuration

или

Router1#show running-config

В строке more, нажмите на клавишу пробел для просмотра следующей страницы информации.

16. Следующая команда позволит вам увидеть текущее состояние протоколов третьего уровня:

Router#show protocols

Конфигурация интерфейсов

Рассмотрим команды настройки интерфейсов сетевого устройства.

1. На сетевом устройстве Router1 войдём в режим конфигурации:

Router1#conf t – Router1(config)#

2. Теперь настроим Ethernet интерфейс. Для этого мы должны зайти в режим конфигурации интерфейса:

Router1(config)#interface FastEthernet0/0 – Router1(config–if)#

3. Посмотрим все доступные в этом режиме команды:

Router1(config–if)#?

Для выхода в режим глобальной конфигурации наберите exit. Снова войдите в режим конфигурации интерфейса:

Router1(config)#int fa0/0 — использовали сокращенное имя интерфейса.

4. Для каждой команды можно выполнить противоположную команду, поставив перед ней слово no. Следующая команда включает этот интерфейс:

Router1(config–if)#no shutdown

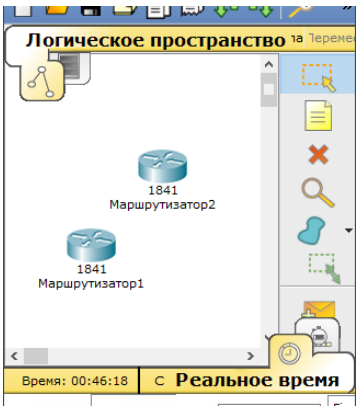
5. Добавим к интерфейсу описание:

Router1(config–if)#description Ethernet interface on Router 1

Чтобы увидеть описание этого интерфейса, перейдите в *привилегированный* режим и выполните команду show interface:

Router1(config–if)#end — Router1#show interface

6. Теперь присоединитесь к сетевому устройству Router 2 и поменяйте имя его хоста на Router2:



Router#conf t — Router(config)#hostname Router2

Войдём на интерфейс FastEthernet 0/0:

Router2(config)#interface fa0/0

Включите интерфейс:

Router2(config–if)#no shutdown

Теперь, когда интерфейсы на двух концах нашего Ethernet соединения включены на экране появится сообщение о смене состояния интерфейса на активное.

7. Перейдём к конфигурации последовательных интерфейсов. Зайдём на Router1.

Проверим, каким устройством выступает наш маршрутизатор для последовательной линии связи: оконечным устройством DTE (data terminal equipment), либо устройством связи DCE (data circuit):

Router1#show controllers fa0/1

Если видим сообщение:

DCE cable

то наш маршрутизатор является устройством связи, и он должен задавать частоту синхронизации тактовых импульсов, используемых при передаче данных. Частота берётся из определённого ряда частот.

Router1#**conf t**

Router1(config)#**int fa0/1**

Router1(config-if)#**clock rate ?**

Выберем частоту 64000:

Router1(config-if)#**clock rate 64000**

и включаем интерфейс:

Router1(config-if)#**no shut**

Для отчета, сохранить файл с именем IOS.pkt. В отчете – схему и IOS команды, реализованные в ходе работы на маршрутизаторах.

Контрольные вопросы.

Какой командой можно посмотреть текущие настройки роутера? Какими командами настраивается сетевой интерфейс роутера. Как просмотреть конфигурационные настройки коммутатора? Как определить распределение вилланов по портам коммутатора? Перечислите основные режимы конфигурации при настройке коммутатора. Перечислите основные режимы конфигурации при настройке роутера. Как посмотреть таблицу маршрутизации на роутере? Какие команды формируют таблицу маршрутизации роутера? Какими командами настраиваются вилланы на коммутаторе? Какими командами настраивается взаимодействие между вилланами?

Приложение Дополнительный материал

Применение сетей

1) Передача данных между устройствами при помощи **приложений**. Это могут быть как консольные приложения, так и приложения с графическим интерфейсом:

Загрузчики. Это файловые менеджеры, работающие по протоколу FTP, TFTP (скачивание фильма, музыки, картинок с файлообменников или иных источников). FTP – это стандартный протокол передачи данных с установлением соединения. Работает по протоколу TCP. **Стандартный номер порта 21.** Чаще всего используется для загрузки сайта на веб–хостинг и выгрузки его. Самым популярным приложением, работающим по этому протоколу — это Filezilla.

Интерактивные приложения. Приложения, позволяющие осуществить интерактивный обмен. Например, модель «человек–человек» (ICQ, электронная почта, форум). Или модель «человек–машина» (удаленная настройка базы, конфигурация сетевого устройства). Здесь, в отличие от загрузчиков, важно постоянное вмешательство человека.

Приложения в реальном времени. Приложения, позволяющие передавать информацию в реальном времени (IP–телефония, системы потокового вещания, видеоконференции). задержка не должна превышать 300 мс. К данной категории можно отнести Skype, Lync, Viber (когда совершаем звонок).

2) Организация удалённых сетевых ресурсов: например, сетевые принтеры или сетевые камеры.

3) Организация хранилищ, доступных для многих **(**google диск, яндекс диск и тому подобные сервисы).

4) Резервное копирование (используют центральный сервер, куда все компьютеры копируют важные файлы для резервной копии. Это нужно для последующего восстановления данных).

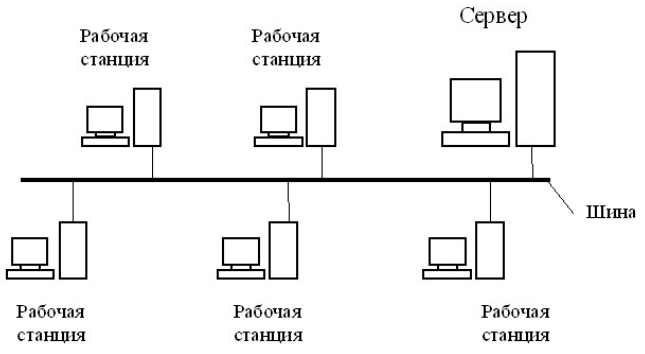
5) **VoIP**: телефония, работающая по протоколу IP.

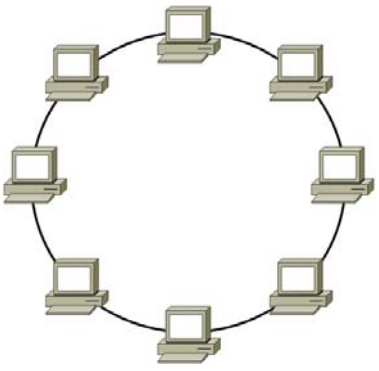
Виды топологии сетей

Топология с общей шиной (англ. Bus Topology)

Одна из первых физических топологий. К одному длинному кабелю подсоединяли все устройства. На концах кабеля требовались терминаторы… Как правило — это было сопротивление на 50 Ом, которое использовалось для того, чтобы сигнал не отражался в кабеле. Преимущество ее было только в простоте установки. С точки зрения работоспособности она была крайне неустойчивой. Если где–то в кабеле происходил разрыв, то вся сеть оставалась парализованной, до замены кабеля.

Кольцевая топология (англ. Ring Topology)





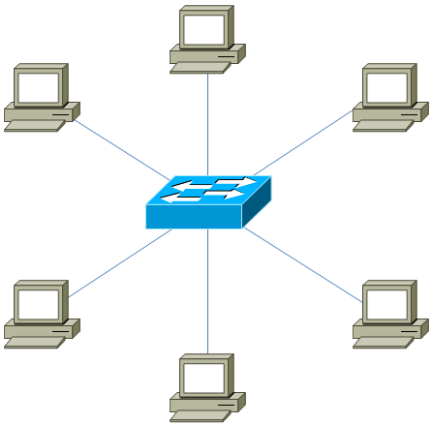
Каждое устройство подключается к 2–ум соседним. Создавая, таким образом, кольцо. С одного конца компьютер только принимает, а с другого только отправляет. Каждый следующий компьютер играет роль ретранслятора сигнала. За счет этого нужда в терминаторах отпала. Соответственно, если где–то кабель повреждался, кольцо размыкалось и сеть становилась не работоспособной. Для повышения отказоустойчивости, применяют двойное кольцо, то есть в каждое устройство приходит два кабеля, а не один.

Топология звезда (англ. Star Topology)

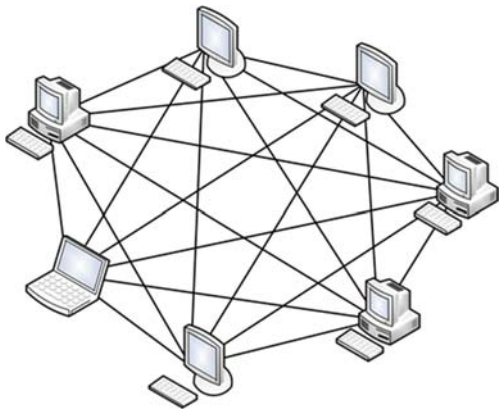
Все устройства подключаются к центральному узлу, который уже является ретранслятором. Используется в локальных сетях, когда к одному коммутатору подключаются несколько устройств, и он является посредником в передаче. Отказоустойчивость значительно выше, чем в предыдущих двух. При обрыве, какого–либо кабеля, выпадает из сети только одно устройство. Все остальные продолжают спокойно работать. Однако если откажет центральное звено, сеть станет неработоспособной.

Полносвязная топология (англ. Full–Mesh Topology)

Все устройства связаны напрямую друг с другом. То есть с каждого на каждый. Данная модель является, пожалуй, самой отказоустойчивой, так как не зависит от других. Но строить сети на такой модели сложно и дорого.



Звезда



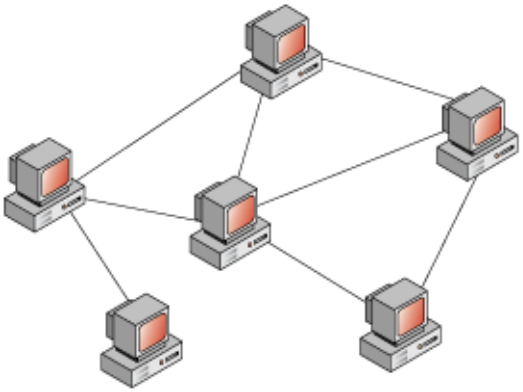
Полносвязная

Неполносвязная топология (англ. Partial–Mesh Topology)

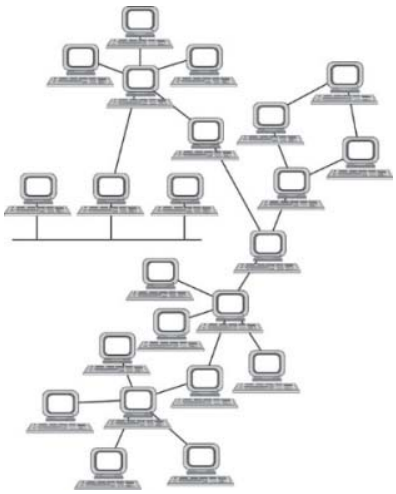
Как правило, вариантов ее несколько. Она похожа по строению на полносвязную топологию. Однако соединение построено не с каждого на каждый, а через дополнительные узлы. То есть узел А, связан напрямую только с узлом В, а узел В связан и с узлом А, и с узлом С. Так вот, чтобы узлу А отправить сообщение узлу С, ему надо отправить сначала узлу В, а узел В в свою очередь отправит это сообщение узлу С. В принципе по этой топологии работают маршрутизаторы. Приведу пример из домашней сети. Когда вы из дома выходите в Интернет, у вас нет прямого кабеля до всех узлов, и вы отправляете данные своему провайдеру, а он уже знает куда эти данные нужно отправить.

Смешанная топология (англ. Hybrid Topology)

Самая популярная топология, которая объединила все топологии выше в себя. Представляет собой древовидную структуру, которая объединяет все топологии. Одна из самых отказоустойчивых топологий, так как если у двух площадок произойдет обрыв, то парализована будет связь только между ними, а все остальные объединенные площадки будут работать безотказно. На сегодняшний день, данная топология используется во всех средних и крупных компаниях.



Неполносвязная



Смешанная

Сетевая модель OSI

Разберем, что делает каждый уровень снизу вверх:

1) Физический уровень (Physical Layer): определяет метод передачи данных, какая среда используется (передача электрических сигналов, световых импульсов или радиоэфир), уровень напряжения, метод кодирования двоичных сигналов.

2) Канальный уровень (Data Link Layer): он берет на себя задачу адресации в пределах локальной сети, обнаруживает ошибки, проверяет целостность данных. Если слышали про MAC–адреса и протокол «Ethernet», то они располагаются на этом уровне.

3) Сетевой уровень (Network Layer): этот уровень берет на себя объединения участков сети и выбор оптимального пути (т.е. маршрутизация). Каждое сетевое устройство должно иметь уникальный сетевой адрес в сети. Думаю, многие слышали про протоколы IPv4 и IPv6. Эти протоколы работают на данном уровне.

4) Транспортный уровень (Transport Layer): Этот уровень берет на себя функцию транспорта. К примеру, когда вы скачиваете файл с Интернета, файл в виде сегментов отправляется на Ваш компьютер. Также здесь вводятся понятия портов, которые нужны для указания назначения к конкретной службе. На этом уровне работают протоколы TCP (с установлением соединения) и UDP (без установления соединения).

5) Сеансовый уровень (Session Layer): Роль этого уровня в установлении, управлении и разрыве соединения между двумя хостами. К примеру, когда открываете страницу на веб–сервере, то Вы не единственный посетитель на нем. И вот для того, чтобы поддерживать сеансы со всеми пользователями, нужен сеансовый уровень.

6) Уровень представления (Presentation Layer): Он структурирует информацию в читабельный вид для прикладного уровня. Например, многие компьютеры используют таблицу кодировки ASCII для вывода текстовой информации или формат jpeg для вывода графического изображения.

7) Прикладной уровень (Application Layer): Наверное, это самый понятный для всех уровень. Как раз на этом уроне работают привычные для нас приложения — e–mail, браузеры по протоколу HTTP, FTP и остальное. Самое главное помнить, что нельзя перескакивать с уровня на уровень (Например, с прикладного на канальный, или с физического на транспортный). Весь путь должен проходить строго с верхнего на нижний и с нижнего на верхний. Такие процессы получили название **инкапсуляция** (с верхнего на нижний) и **деинкапсуляция** (с нижнего на верхний). Также стоит упомянуть, что на каждом уровне передаваемая информация называется по–разному.

Подробности:

Важно помнить, что нельзя перескакивать с уровня на уровень (Например, с прикладного на канальный, или с физического на транспортный). Весь путь должен проходить строго с верхнего на нижний и с нижнего на верхний. Такие процессы получили название инкапсуляция (с верхнего на нижний) и деинкапсуляция (с нижнего на верхний).

Также стоит упомянуть, что на каждом уровне передаваемая информация называется по–разному. На прикладном, представления и сеансовым уровнях, передаваемая информация обозначается как PDU (Protocol Data Units). На русском еще называют блоки данных (данные).

Информацию транспортного уровня называют сегментами. Хотя понятие сегменты, применимо только для протокола TCP. Для протокола UDP используется понятие — датаграмма. Но, как правило, на это различие закрывают глаза.

На сетевом уровне называют IP пакеты или просто пакеты.

И на канальном уровне — кадры.

Пример, который поможет разобраться с процессом инкапсуляции и деинкапусуляции:

1) Представим ситуацию, что вы сидите у себя дома за компьютером, а в соседней комнате у вас свой локальный веб–сервер. И вот вам понадобилось скачать файл с него. Вы набираете адрес страницы вашего сайта. Сейчас вы используете протокол HTTP, которые работает на прикладном уровне. Данные упаковываются и спускаются на уровень ниже.

2) Полученные данные прибегают на уровень представления. Здесь эти данные структурируются и приводятся в формат, который сможет быть прочитан на сервере. Запаковывается и спускается ниже.

3) На этом уровне создается сессия между компьютером и сервером.

4) Так как это веб сервер и требуется надежное установление соединения и контроль за принятыми данными, используется протокол TCP. Здесь мы указываем порт, на который будем стучаться и порт источника, чтобы сервер знал, куда отправлять ответ. Это нужно для того, чтобы сервер понял, что мы хотим попасть на веб–сервер (стандартно — это **80 порт**), а не на почтовый сервер. Упаковываем и спускаем дальше.

5) Здесь мы должны указать, на какой адрес отправлять пакет. Соответственно, указываем адрес назначения (пусть адрес сервера будет 192.168.1.2) и адрес источника (адрес компьютера 192.168.1.1). Заворачиваем и спускаем дальше.

6) IP пакет спускается вниз и тут вступает в работу канальный уровень. Он добавляет физические адреса источника и назначения, о которых подробно будет расписано в последующей статье. Так как у нас компьютер и сервер в локальной среде, то адресом источника будет являться MAC–адрес компьютера, а адресом назначения MAC–адрес сервера (если бы компьютер и сервер находились в разных сетях, то адресация работала по–другому). Если на верхних уровнях каждый раз добавлялся заголовок, то здесь еще добавляется концевик, который указывает на конец кадра и готовность всех собранных данных к отправке.

7) И уже физический уровень конвертирует полученное в биты и при помощи электрических сигналов (если это витая пара), отправляет на сервер.

Процесс **деинкапсуляции** аналогичен, но с обратной последовательностью:

1) На физическом уровне принимаются электрические сигналы и конвертируются в понятную битовую последовательность для канального уровня.

2) На канальном уровне проверяется MAC–адрес назначения (ему ли это адресовано). Если да, то проверяется кадр на целостность и отсутствие ошибок, если все прекрасно и данные целы, он передает их вышестоящему уровню.

3) На сетевом уровне проверяется IP адрес назначения. И если он верен, данные поднимаются выше. Не стоит сейчас вдаваться в подробности, почему у нас адресация на канальном и сетевом уровне. Это тема требует особого внимания, и я подробно объясню их различие позже. Главное сейчас понять, как данные упаковываются и распаковываются.

4) На транспортном уровне проверяется порт назначения (не адрес). И по номеру порта, выясняется какому приложению или сервису адресованы данные. У нас это веб–сервер и номер порта — 80.

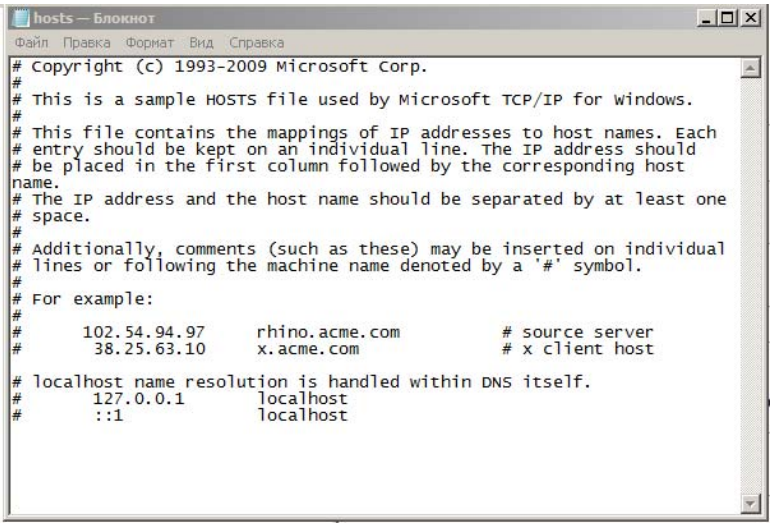
5) На этом уровне происходит установление сеанса между компьютером и сервером.

6) Уровень представления видит, как все должно быть структурировано и приводит информацию в читабельный вид.

7) И на этом уровне приложения или сервисы понимают, что надо выполнить.

«HOSTS»

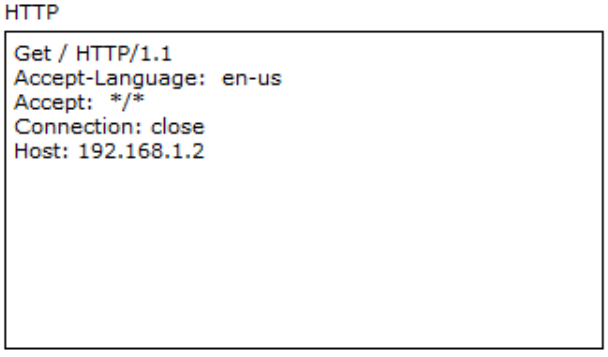
Стандартное расположение его в Windows системах «windows\system32\drivers\etc\hosts». А в *nix подобных системах: "/etc/hosts". Делает он то же самое, что и DNS сервера. И контролируется этот файл администратором компьютера. И самое важное: он имеет приоритет перед DNS сервером. И, если у вас в файле написано, что сайту habrahabr.ru соответствует IP адрес, который на самом деле соответствует google.ru, то, соответственно, открывать он будет google, а не habrahabr. Этим часто пользуются злоумышленники, когда вносят исправления в этот файл. Пример этого файла.



Вот так он выглядит. Можете открыть его у себя и поймете, что он точно такой же.

Протокол HTTP

На рисунке представлен **HTTP запрос** от клиента к серверу.



В первой строчке используется, ключ запроса GET Так как после GET стоит символ "/", то это означает, что запрашивается главная или корневая страница по URL (англ. Uniform Resource Locator) пути.

URL — это некий идентификатор какого–либо ресурса в сети.

Так же в этой строчке присутствует запись HTTP/1.1. Это версия протокола. Выпустили ее в 1999 году. Хоть разработана версия 2.0, версия 1.1 занимает пока лидирующее положение. Теперь о нижней строчке. Здесь указывается адрес сервера или имя, на котором располагается нужный ресурс.

HTTPS (HyperText Transfer Protocol Secure), это расширение протокола HTTP, которое поддерживает криптографические протоколы и передает информацию не в открытом виде, а в зашифрованном.

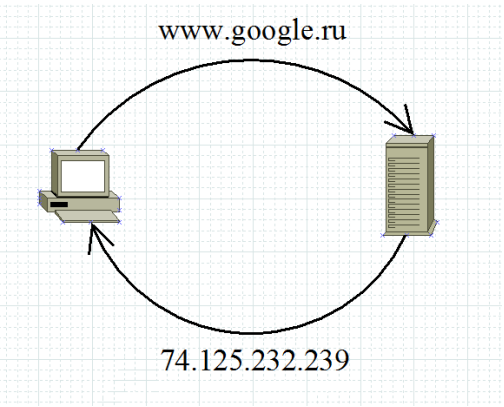
Запоминаем: HTTP использует 80 порт, а HTTPS 443 порт.

DNS сервер

DNS сервер – (Domain Name System), система доменных имен? позволяет организовать службу разрешения доменных имён. Функция DNS сервера заключается в преобразовании доменных имен серверов в IP–адреса.

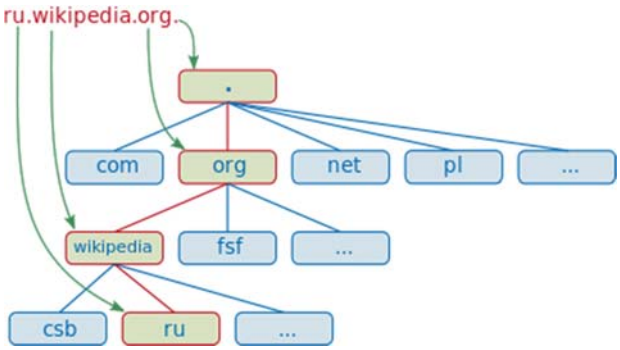
Если говорить в целом, то она хранит информацию о доменах. Например, какому IP адресу соответствует определенное имя. Приведу пример: когда вы открываете свой любимый сайт, то обращаетесь к нему по имени. Но в поля Source Address и Destination Address, которые работают на сетевом уровне нельзя вставить имя. Там обязательно должен присутствовать именно IP адрес.

Вот DNS как раз этим и занимается. Она сообщает, какой IP адрес у запрошенного имени. Вы, к примеру, обращаетесь на google.ru. Ваш компьютер понятия не имеет, кто и что это. Он спрашивает у DNS сервера: Кто такой google.ru? И сервер отвечает, что google.ru — это 74.125.232.239 (это один из его адресов). И уже после этого, компьютер отправляет запрос на 74.125.232.239. Для пользователя все останется по–прежнему, и в адресной строке он также будет видеть google.ru. Как обычно, покажу это на картинке



Думаю, что выше описанное понятно, и двигаемся дальше. Служба эта иерархичная. И часто DNS сервер (на котором запущена эта служба) работает в связке с другими DNS серверами. Что это значит? Иерархичность его заключается в том, что он работает с доменами уровня. Работает он от младшего уровня к старшему, слева направо.

Например, имя: ru.wikipedia.org. Самым старшим будет доменное имя «org», а младшим — «ru». Но часто бывают случаи, когда DNS сервер не может нам рассказать о каком–то доменном имени, и тогда он обращается к старшему DNS серверу, который отвечает за доменные имена более высокого уровня. Приведем картинку из википедии. Там эта работа проиллюстрирована хорошо.



Предположим, мы набрали в браузере адрес ru.wikipedia.org. Браузер спрашивает у сервера DNS: «какой IP–адрес у ru.wikipedia.org»? Однако сервер DNS может ничего не знать не только о запрошенном имени, но даже обо всём домене wikipedia.org. В этом случае сервер обращается к корневому серверу — например, 198.41.0.4. Этот сервер сообщает — «У меня нет информации о данном адресе, но я знаю, что 204.74.112.1 является ответственным за зону org.» Тогда сервер DNS направляет свой запрос к 204.74.112.1, но тот отвечает «У меня нет информации о данном сервере, но я знаю, что 207.142.131.234 является ответственным за зону wikipedia.org.» Наконец, тот же запрос отправляется к третьему DNS серверу и получает ответ — IP–адрес, который и передаётся клиенту — браузеру.

DHCP (Dynamic Host ConfigurationProtocol)

Инициализация сетевых интерфейсов может проводиться автоматически при помощи протокола динамического конфигурирования хостов DHCP (Dynamic Host Configuration Protocol). Протокол DHCP работает по схеме «клиент–сервер». При первом включении компьютер посылает в сеть широковещательный запрос на получение IP–адреса, а также других параметров, требующихся для работы в сетях TCP/IP. DHCP сервер посылает в ответ сообщение, содержащее, IP–адрес и другую инициализирующую информацию. Сервер DHCP обеспечивает различные режимы работы:

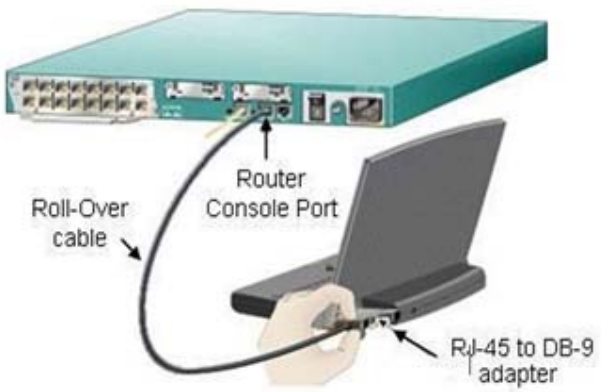
ручное задание статических адресов, когда администратор вводит в сервер исходную информацию о соответствии IP–адресов физическим адресам или другим идентификаторам рабочих станций;

автоматическое назначение статических адресов, когда сервер произвольным образом выбирает клиенту IP–адрес из множества наличных адресов, при этом адрес закрепляется за данным клиентом;

динамическое распределение адресов, когда сервер выдает адрес клиенту на ограниченное время, называемое «сроком аренды»; при удалении компьютера из сети, назначенный IP–адрес автоматически освобождается. Режим динамического распределения адресов допускает построение сетей, у которых количество узлов превышает число имеющихся IP–адресов.

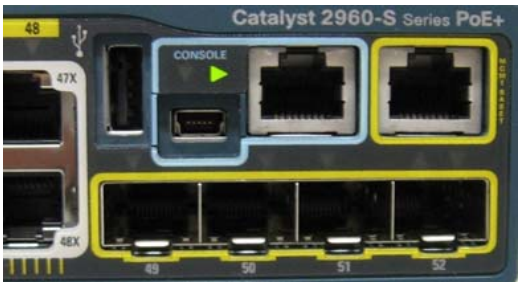
Консоль

Большинство сетевых устройств компании CISCO допускают конфигурирование. Для этого администратор сети должен подключиться к устройству через прямое кабельное (консольное) подключение.



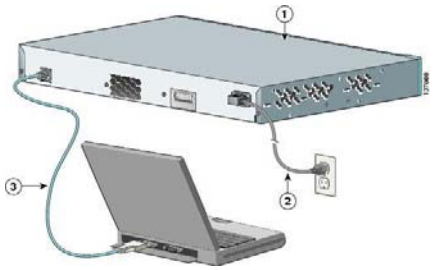
Консольное подключение к сетевому устройству

Программирование устройств CISCO чаще всего производят через консольный порт RJ–45. На рис. приведены фотографии консольных разъёмов на маршрутизаторе и 2 варианта консольного кабеля.



Варианты консольных кабелей

Синим цветом показаны разъёмы под управляющий (консольный) кабель



Подключение к коммутатору при помощи консольного кабеля

Классический консольный кабель имеет разъем DB9 для подключения к COM–порту компьютера и разъем RG–45 для подключения к консольному порту маршрутизатора. Сейчас Cisco активно продвигает новые маршрутизаторы серий 28xx, 38xx и т.д. В них предусмотрена возможность конфигурирования через USB–интерфейс (используются обычные USB–кабели).