Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук

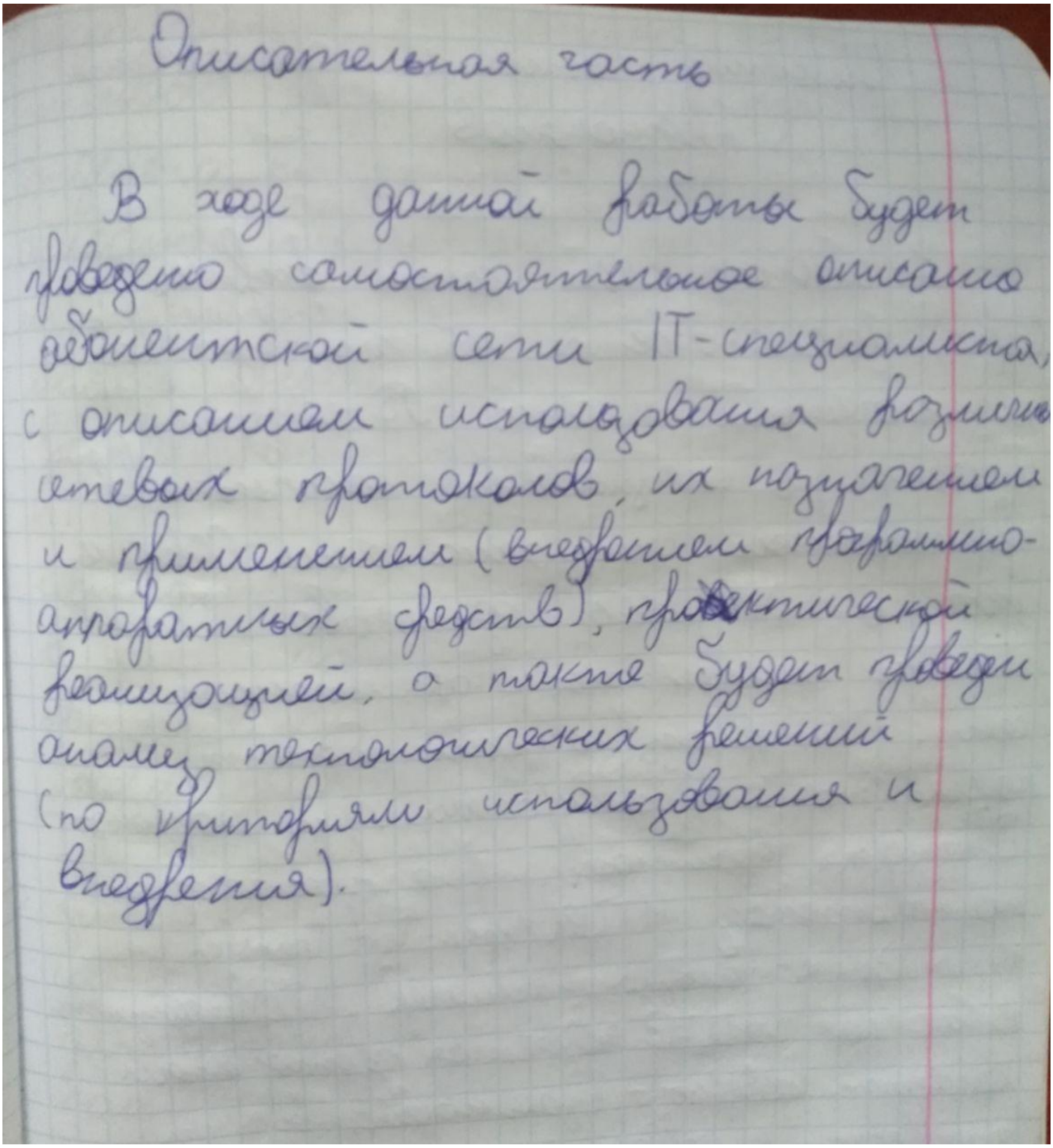
Індивідуальна робота
з дисципліни
„Комп'ютерні мережі"

Виконав: студент
2 курсу групи КС-21
спеціальності
122 – Комп'ютерні науки
Безрук Юрій Русланович
Перевірив:
Богучарський С.І.

Харків 2020

Я студент группы КС-21, Безрук Юрий Русланович, самостоятельно и собственноручно выполнял индивидуальную работу. Содержание выполнено рукописно мной. Номер студенческого билета 12284003

02.04.2020



Описательная часть

В ходе данной работы будет проведено самостоятельное описание абонентской сети IT-специалиста, с описанием использования различных сетевых протоколов, их назначением и применением (внедрением программно-аппаратных средств), практической реализацией, а также будет проведен анализ технологических решений (по критериям использования и внедрения).

Описание сети и применение протоколов

В абонентской сети фирмы (офис) располагается 15 компьютеров, подключенных к сети. В сети имеется 8 специальных компьютеров, применяемых специалистами, Остальные 7 настроены одинаково.

Все компьютеры подключены к сети Интернет, каждый абонент пользуется веб-ресурсами при помощи браузера, взаимодействие происходит по протоколу HTTP(Hypex-Text Transfer Protocol), используя, например, HTML-докумен. Так как HTTP является протоколом клиент-серверного взаимодействия, запросы к серверу инициируются пользователем. Полученный итоговый документ будет состоять из различ поддокументов, являющихся частью итогового документа: например, из отдельно полученного текста, описания структуры документа, изображений, видео-файлов, скриптов и многого другого. Также в сети распространено расширение протокола HTTP — HTTPS (HyperText Tranfer Protocol Secure), используемое с поддержкой шифрования, в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов TSL или SSL. Для этого сайты должны использовать сертификаты соответствующих протоколов, необходимые для безопасного соединения, при помощи которых шифруется вся информация.

Кроме этого, один из компьютеров в сети работает как HTTPS-сервер для сайта компании, используемого для взаимодействия с покупателями. Протокол HTTP работает по TCP-порту 80, HTTPS – 443.

Для хранения данных организации в локальной сети установлен FTP-сервер. FTP (File Transfer Protocol) – протокол передачи файлов по сети, предусматривающий обмен сообщениями с определенным заголовком между сервером и клиентом. FTP-сервер используется в сети для хранения файлов организации в одном месте в локальной сети (т.к. протокол FTP не имеет совершенно никакой защиты). FTP-сервер для большинства абонентов в сети настроен на анонимный режим работы (доступ по логину anonymus и паролю в виде любой электронной почты). Это необходимо ~~для~~ потому, что в FTP аутентификация является обязательной и без неё сервер не пропускает запросы. Кроме того, для вышепоставленных членов организации организуется аутентификация с настоящими логином и паролем, и доступ к большей части ~~фай~~ информации, хранящейся на сервере. В отличие от HTTP FTP позволяет осуществлять различные операции с файловой системой, ~~а~~ использует отдельный канал для каждого соединения и поддерживает два режима ~~работы~~ передачи данных: текстовый и бинарный. Для взаимодействия с интерфейсом используется ~~F~~ FileZilla

Так-как FTP является небезопасным протоколом, для передачи через сеть файлов используются его защищённые аналоги – SFTP и FTPS.

Для передачи файлов в удалённы
офис компании, используется протокол SFTP (SSH File Transfer Protocol), предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения. SFTP на самом деле является расширением SSH-протокола прикладного уровня, дающего возможность шифрования данных и паролей. SFTP поддерживает два способа аутентификации соединений. Как и в FTP, можно просто использовать идентификатор пользователя и пароль. Тем не менее, с SFTP эти учётные данные шифруются, что даёт ей большое преимущество безопасности перед FTP. Другой метод аутентификации,

который можно использовать с SFTP это ключи SSH, которые работают следующим образом: генерируется секретный и открытый ключи SSH, после чего, открытый ключ передаетс другой стороне соединения, так же загружается на сервер и связывается ~~то~~ с исходным аккаунтом. Далее, при подключении, если открытый ключ соответствует закрытому, наряду с новым пользователем или переданным паролем, то верификация будет пройдена. SFTP построен на порт 22.

Кроме этого, некоторые файлы компании выгружаются на удалённый хостинг с возможностью их скачивания другими пользователями. Для этого применяется другой защищённый FTP - FTPS. ~~В отличии~~ ~~от~~ (File Transfer Protocol + SSL).

В отличии от SFTP, который являлся расширением SSH для работ с файлами, FTPS – это прямое расширение FTP, которое добавляет поддержку для криптографических протоколов уровней транспортной безопасности и защищенных сокетов. FTPS, так же как и HTTPS, использует сертификаты SSL. FTPS проверяет подлинность подключения, используя идентификатор пользователя и пароль, сертификат SSL, либо и то, и другое.

Задачей одного из работников омпании является управление почтой и письмами компании, их сортировка и пересылка. Для сохранения упорядоченных цепочек заголовков писем на данном компьютере используется протокол IMAP. IMAP(Internet

Message Access Protocol) - это почтовый протокол, созданный для доступа к почте с локального почтового клиента. В отличии от POP3, IMAP загружает с сервера только заголовки писем, сам текст письма остаётся на сервере. Данный протокол связи работает в две стороны, если происходят изменения на локальном клиенте, они передаются и на сервер. Также, в отличие от POP3, IMAP позволяет получать доступ к почте из множества клиентов. IMAP построен на порт 993 (с безопасным соединением)

Если же фирме по каким-либо причинам необходимо получить либо выгрузить полностью электронные сообщения, соответствующее ПО для работы с протоколами POP3 и SMTP установлено на соседнем компьютере

POP3 (Post Office Protocol, version 3) – стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению. POP3 позволяет абоненту сохранить почтовое сообщение на ваш компьютер и даже прочесть его, без подключения к сети. Письма, скачиваемые при помощи POP3 удаляются с сервера. POP3 не имеет никакого функционала для выгрузки на сервер, и работает только для скачивания. В данной сети настроен на порт 995 (с безопасным соединением).

На том же устройстве в основном проходит и использование протокола SMTP. SMTP (Simple

Mail Transfer Protocol) - сетевой протокол, для отправки почтовых сообщений по сети интернет, при помощи связи с удалённым сервером, и пересылке письма через него непосредственно на сервер получателя сообщений. На сервера отправителя процесс контролируется специальной службой MTA. ~~[illegible]~~ ~~в~~ Фактически, использование данного протокола происходит ~~как~~ схожим образом с электронной почтой с разницей в том, что невозможно никаким образом хранить и получать сообщения. В данной сети используется через порт 465 (с защищённым соединением).

Для управления и настройки сети в оффисе выделен компьютер систем-ного администратора, из которого можно проводить конфигурирование, том же и используется SNMP. SNMP (Simple Network Management Protocol) – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур. К поддерживаемым SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. В данной сети протокол применяется для контроля подключенных к сети устройств на предмет условий, которые требуют внимания дминистратора.

Для того, чтобы сетевые устройства автоматически получали IP-адрес и другие параметры, необходимые для работы сети, в ней установлен DHCP-сервер. DHCP (Dynamic Host Configuration Protocol) - протокол динамической настройки узла прикладного уровня модели OSI. На DHCP-сервере системным администратором задаётся определённый диапазон IP-адресов, которые можно выдавать устройствам-клиентам при обращении. При этом дополнительно может настраиваться срок аренды адреса, в течение которого он закреплён за MAC-адресом компьютера и не может быть занят иным устройством.

Для организации транспортного соединения между устройствами данной сети и ~~отдале~~ устройствами в отдалённом офисе компании для взаимодействия с операционной системой удалённо, [illegible] [illegible] и управления файлами на одном из устройств запускают клиент Telnet. Telnet - сетевой протокол для реализации текстового терминального интерфейса. Основная задача Telnet заключается в том, чтобы позволить терминальным устройств и терминальным процессам взаимодействовать друг с другом, т.е. для связи „терминал- терминал" или „процесс-процесс". Telnet симметричен. Основным применением в сети данного протокола является возможность удалённого доступа к компьютеру через интерфейс консоли.

Для организации обмена данн между устройствами в среде операционных систем Microsoft используется SMB. SMB (Server Message Block) - сетевой протокол прикладного уровня для удаленного доступа к файлам и сетевым ресурсам а также для межпроцессорного взаимодействия. В контексте данной сети SMB применяется для реализации общего доступа к файлам и удалённого доступа к принтеру, за что отвечает одна из выделенных в сети станций. Протокол SMB, в отличие от Telnet, является защищённым.

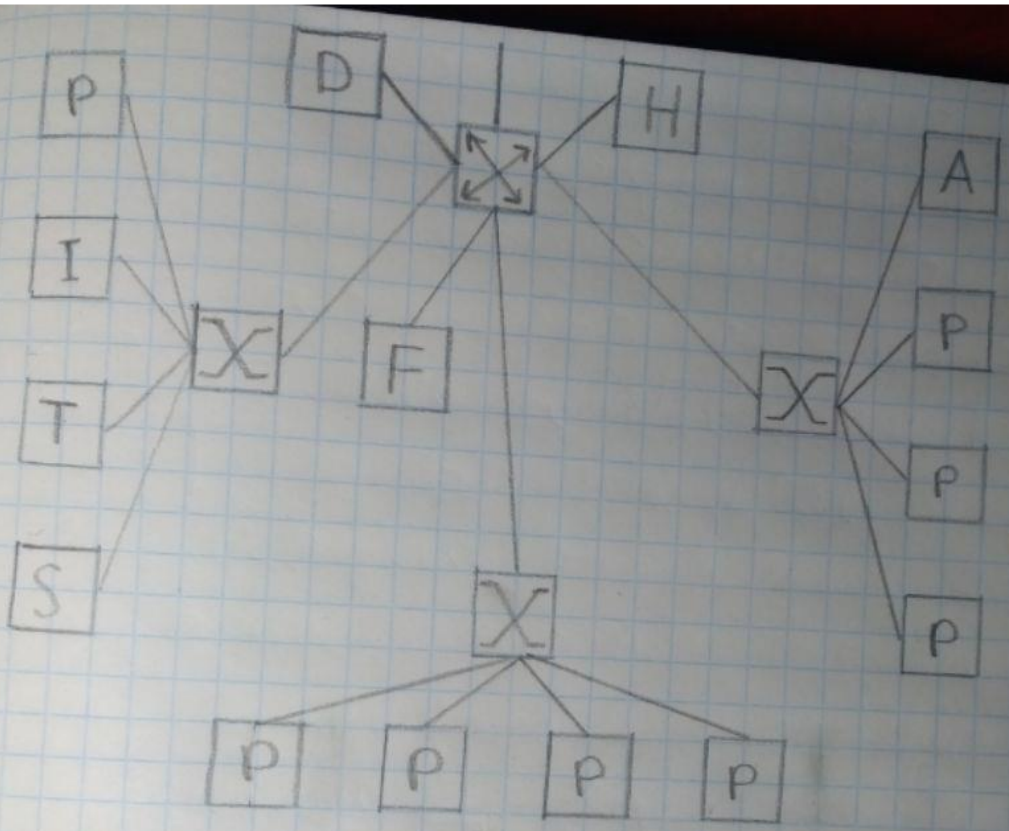
Все компьютеры сети при выходе в интернет обязаны использовать доменные имена, поэтому применение DNS является необходимым. DNS (Domaine Name System) - компьютерная распределённая система для получения информации о доменах. Используется для получения IP-адреса по имени хоста, получения информации о конфигурации почты и/или обслуживающих узлов для протоколов в домене (SRV-запись). Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу. DNS-серверы сгруппированы в зоны и осуществляют определённую иерархию вызовов. Таким образом, если к корневому DNS-серверу поступает запрос в виде доменного имени, адрес которого он не знает, но зато знает о DNS-сервере который отвечает за зону, в которой находится доменное имя, он перенаправляет запрос ему. Так осуществляется иерархия вызовов, пока она не дойдёт до DNS-сервера, ~~который~~ у которого хранит ся IP-адрес соответствующего домена.

Для синхронизации времени на устройствах и рабочих станциях компании используются установленные NTP-клиенты. NTP (Network Time Protocol) - сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью. NTP использует для своей работы протокол UDP и учитывает время передачи. Система NTP чрезвычайно устойчива к изменениям латентности среды передачи. В версии 4 NTP достигает точности 10 мс при работе через Интернет, и до 0,2 мс и лучше внутри локальных сетей

При использовании SMTP и для шифрования и защиты передаваемых по сети данных применяются кодировки SSH. SSH (Secure SHell) – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. Схож по функционалу с Telnet, но, в отличие от него, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования, и позволяет передавать в незащищённой среде практически любой другой сетевой протокол.

Провайдер сети предоставляет абонентам организации доступ к их домашнему каталогу по SSH.

На рисунке 1 представлено схематическое распределение клиентов по районам и приблизительная топология сети.



Усл. обозначения:

⤢	маршрутизатор
X	коммутатор
P	рабочая станция
A	компьютер администратора
P	станция передачи почты (POP3, SMTP)
I	станция проверки (IMAP)
T	станция для терминалов TELNET
S	станция управления SMB
D	DHCP-сервер
F	FTP-сервер
H	HTTPS-сервер сайта компании

Рисунок 1 – схематическое распределение ролей клиентов в организации