ЛАБОРАТОРНАЯ РАБОТА №4

«ИССЛЕДОВАНИЕ СПОСОБОВ КОНФИГУРАЦИИ СЕТЕВЫХ СЕРВЕРНЫХ СЛУЖБ СТЕКА И ПРОТОКОЛОВ ТСР/IP»

1. Цель работы

Исследование особенностей использования основных сетевых серверных служб стека протоколов TCP/IP и конфигурации серверов, реализующих эти службы, приобрести практические навыки по конфигурации серверного сетевого оборудования.

2. Постановка задачи

2.1 Повторить теоретический материал по иерархии протоколов стека TCP/IP, по протоколам прикладного уровня и составу полей кадров и пакетов этих протоколов (выполняется в процессе домашней подготовки).

2.2 Составить в рабочем окне эмулятора схему исследуемой сети, изображенной на рисунке 1.

2.3 Установить для всех серверов сети статический режим адресации и задать их адреса в следующем виде: XY.0.0.10 – DHCP-сервер; XY.0.0.100 –DNS-сервер; XY.0.0.100 – HTTP-сервер www.sevgu.ru; XY.0.0.200 – HTTP-сервер www.kaf.is. Здесь Х-предпоследняя цифра зачетной книжки, а Y-предпоследняя.

2.4 Задать режим динамической адресации для оконечных устройств сети, и провести установку и настройку DHCP-сервера на компьютере XY.0.0.10.

2.5 Установить на серверный компьютер XY.0.0.100 DNS-сервер и осуществить его настройку.

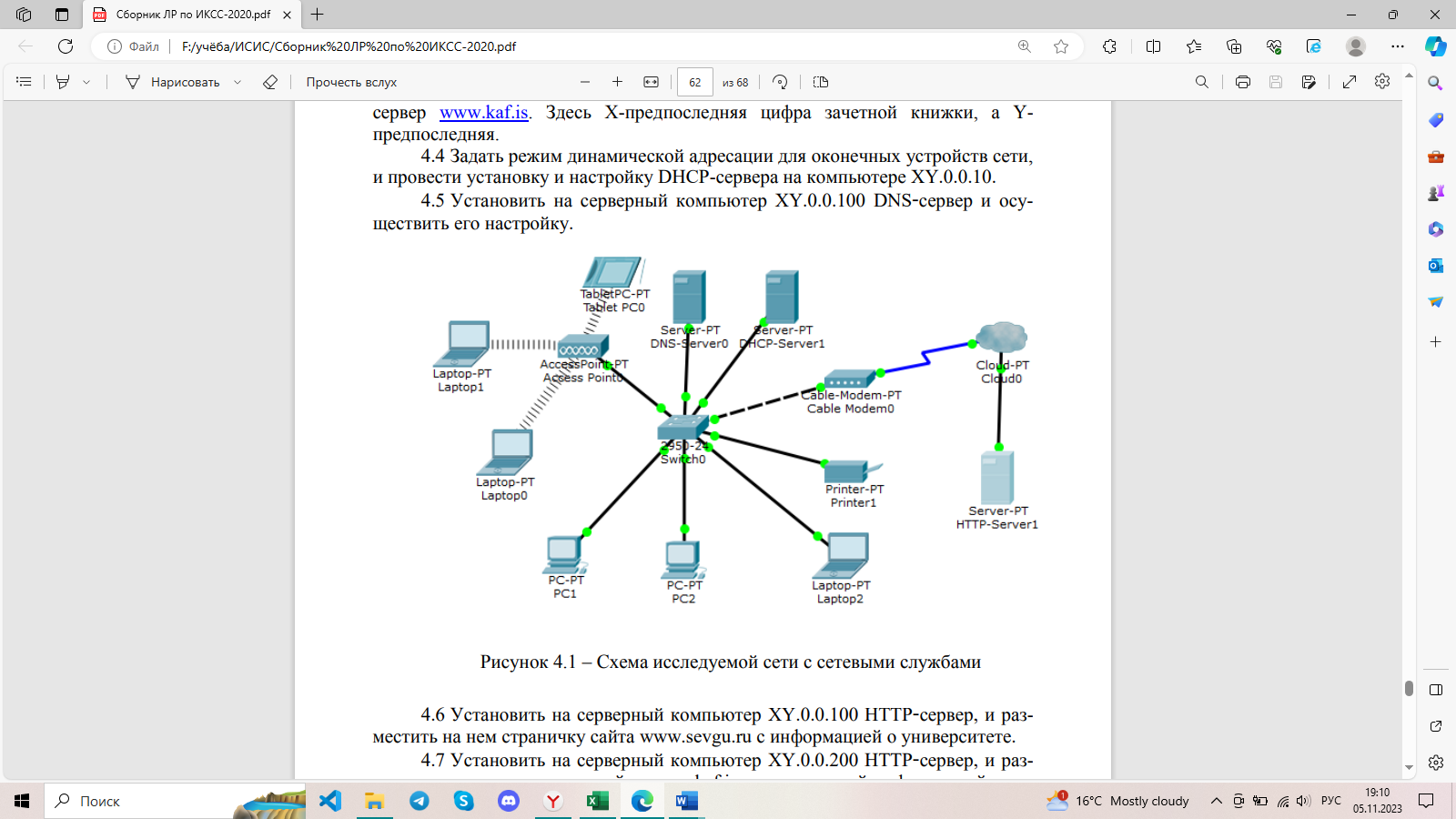


Рисунок 1 – Схема исследуемой сети с сетевыми службами

2.6 Установить на серверный компьютер XY.0.0.100 HTTP-сервер, и разместить на нем страничку сайта www.sevgu.ru с информацией о университете.

2.7 Установить на серверный компьютер XY.0.0.200 HTTP-сервер, и разместить на нем страничку сайта www.kaf.is.ru с рекламной информацией о кафедре ИС.

2.8 Провести проверку связи оконечных устройств друг с другом и доступа к страницам сайтов по их IP-адресам и по доменным символическим именам в реальном режиме и режиме симуляции.

2.9 Исследовать структуру пакетов при обращении к странице одного из сайтов.

3. Ход работы

Была построена схема сети, изображенная на рисунке 2. В таблицу 1 были занесены сетевые адреса используемых устройств (серверов).

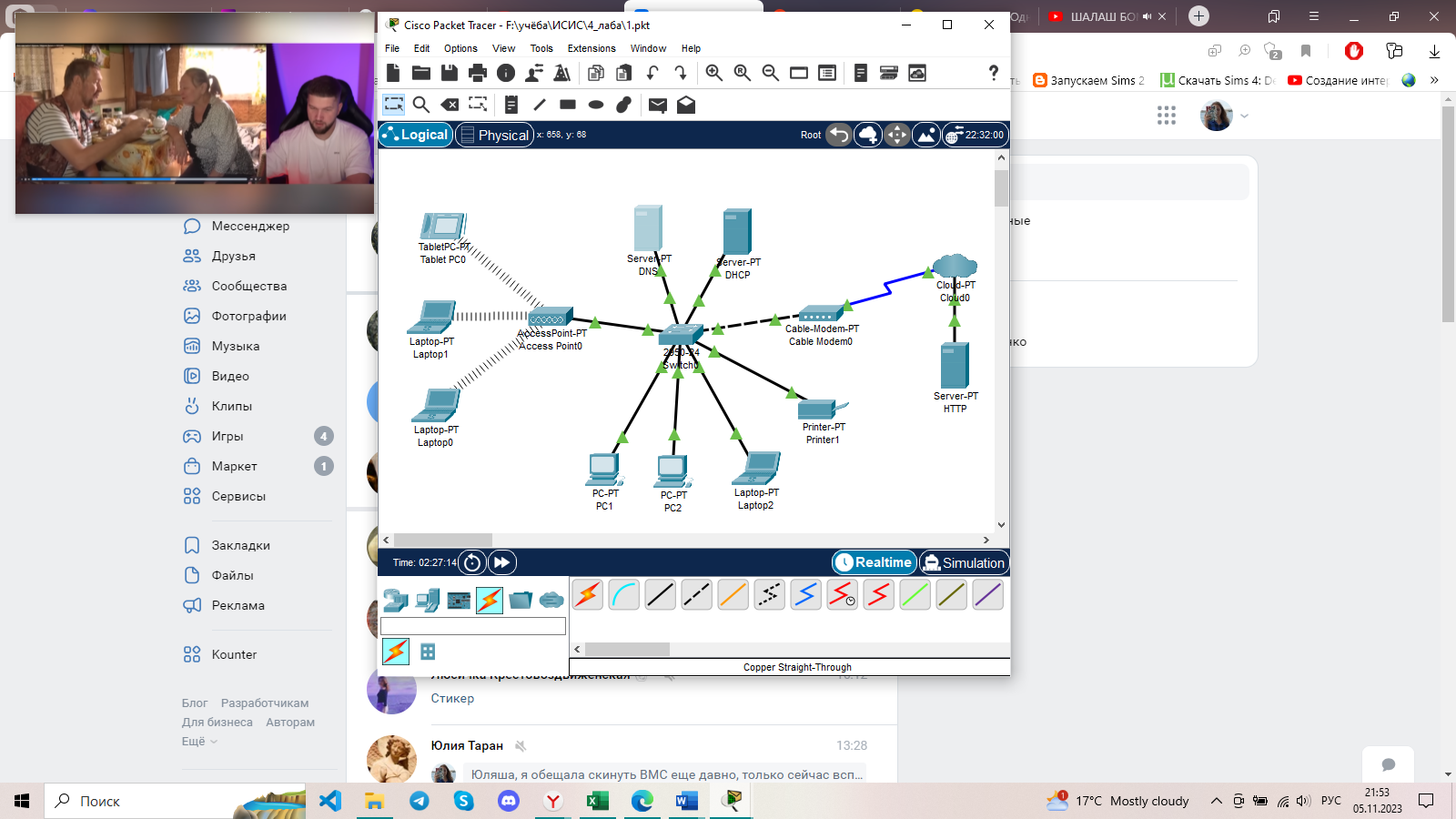


Рисунок 2 – Схема сети

Таблица 1 – Таблица статических IP-адресов

|  |  |
| --- | --- |
| Сервер | IP-адрес |
| DHCP-сервер | 19.0.0.10 |
| DNS-сервер | 19.0.0.100 |
| HTTP-сервер [www.sevsu](http://www.sevgu).ru | 19.0.0.100 |
| HTTP-сервер [www.kaf](http://www.kaf).is | 19.0.0.200 |

Далее была настроена точка доступа так, как показано на рисунке 3.

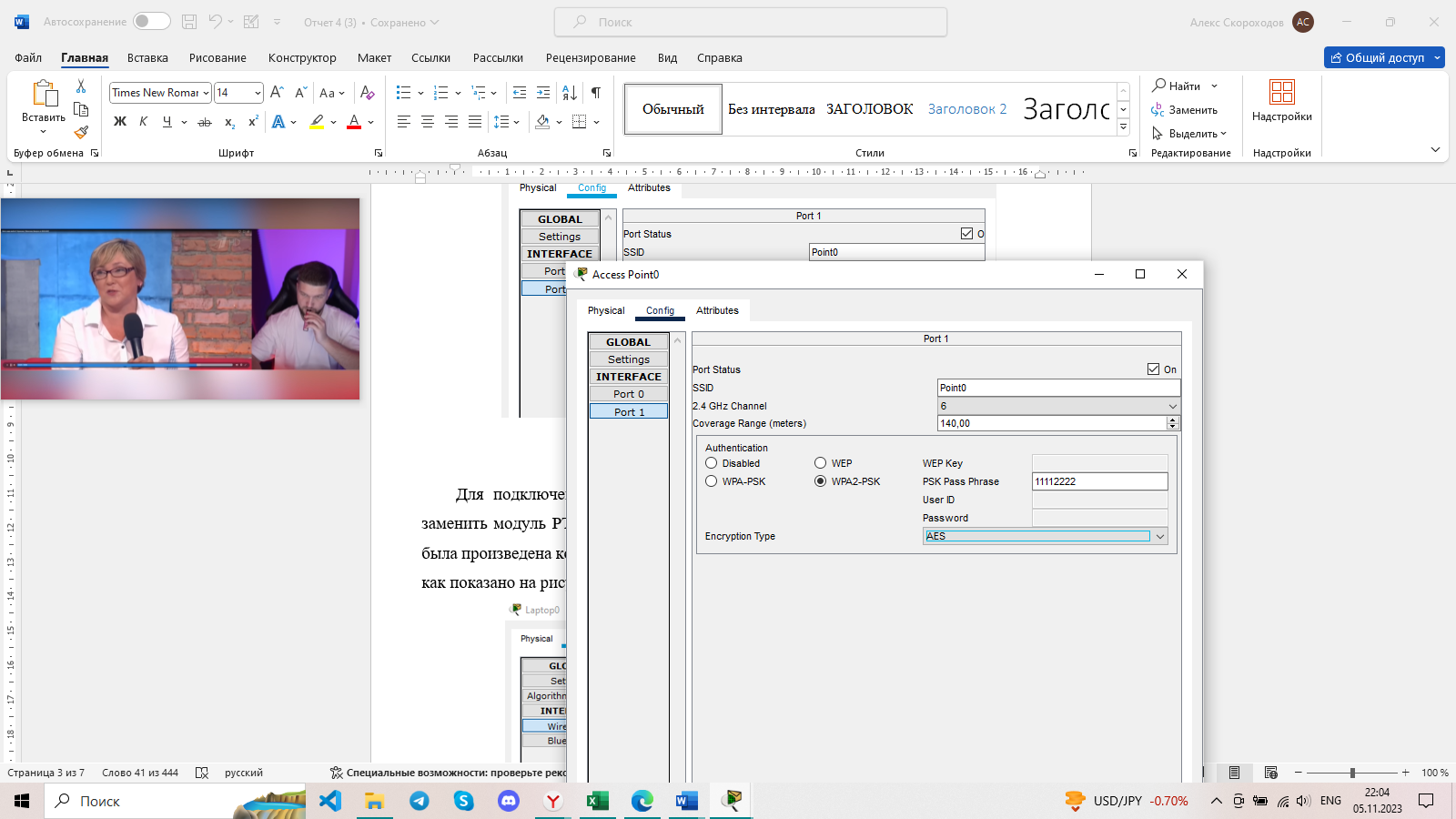


Рисунок 3 – Настройка точки доступа

Для подключения к беспроводной сети Laptop0, Laptop1 необходимо было заменить модуль PT-LAPTOP-NM-1CFE на модуль Linksys-WPC300N. После этого была произведена конфигурация на всех устройствах с беспроводным подключением, как показано на рисунке 4.

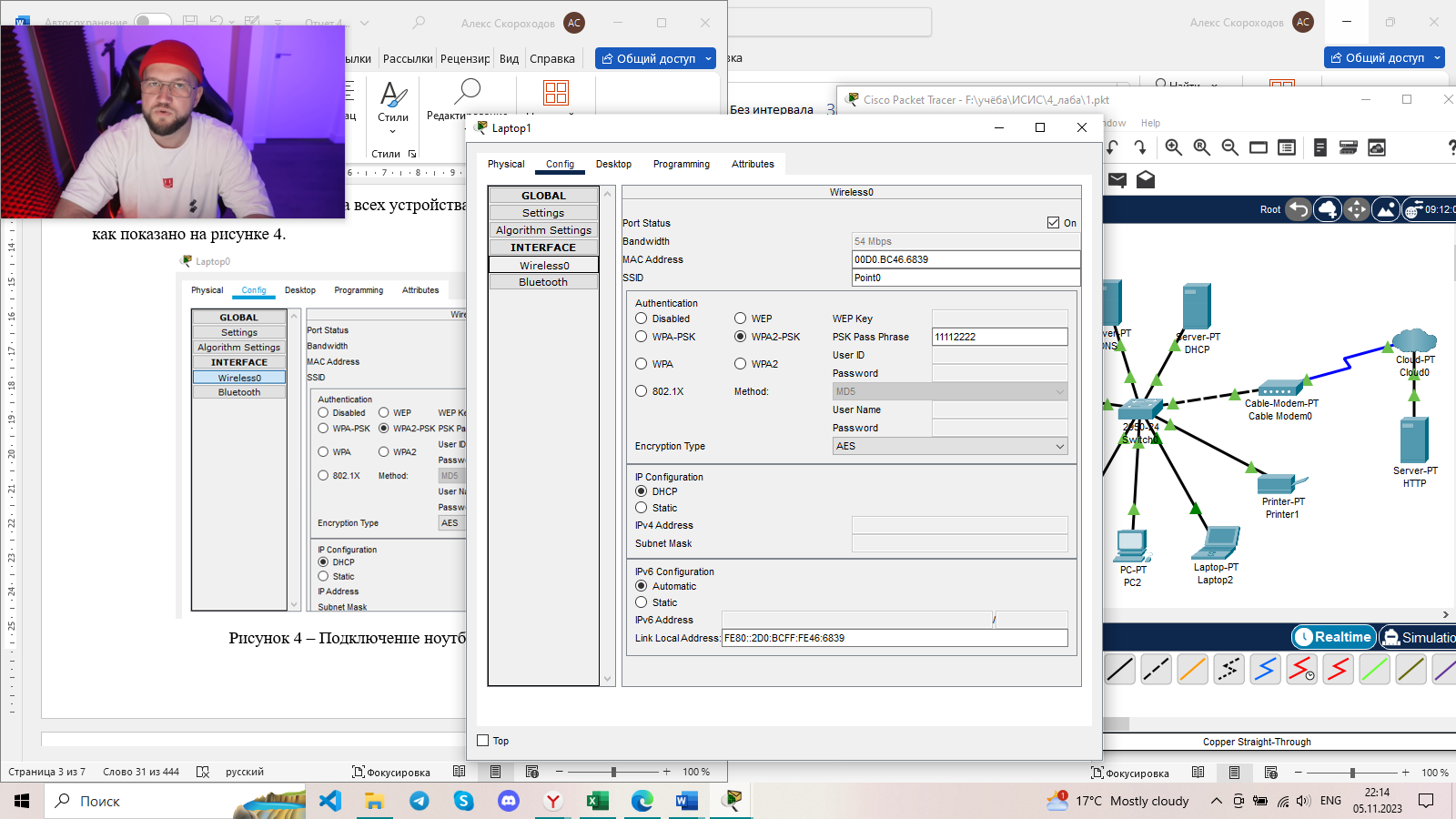


Рисунок 4 – Подключение ноутбука к точке доступа

Далее была произведена настройка серверов. На рисунке 5 показаны параметры настройки сервера DHCP. На рисунке 6 изображена настройка сервера DNS.

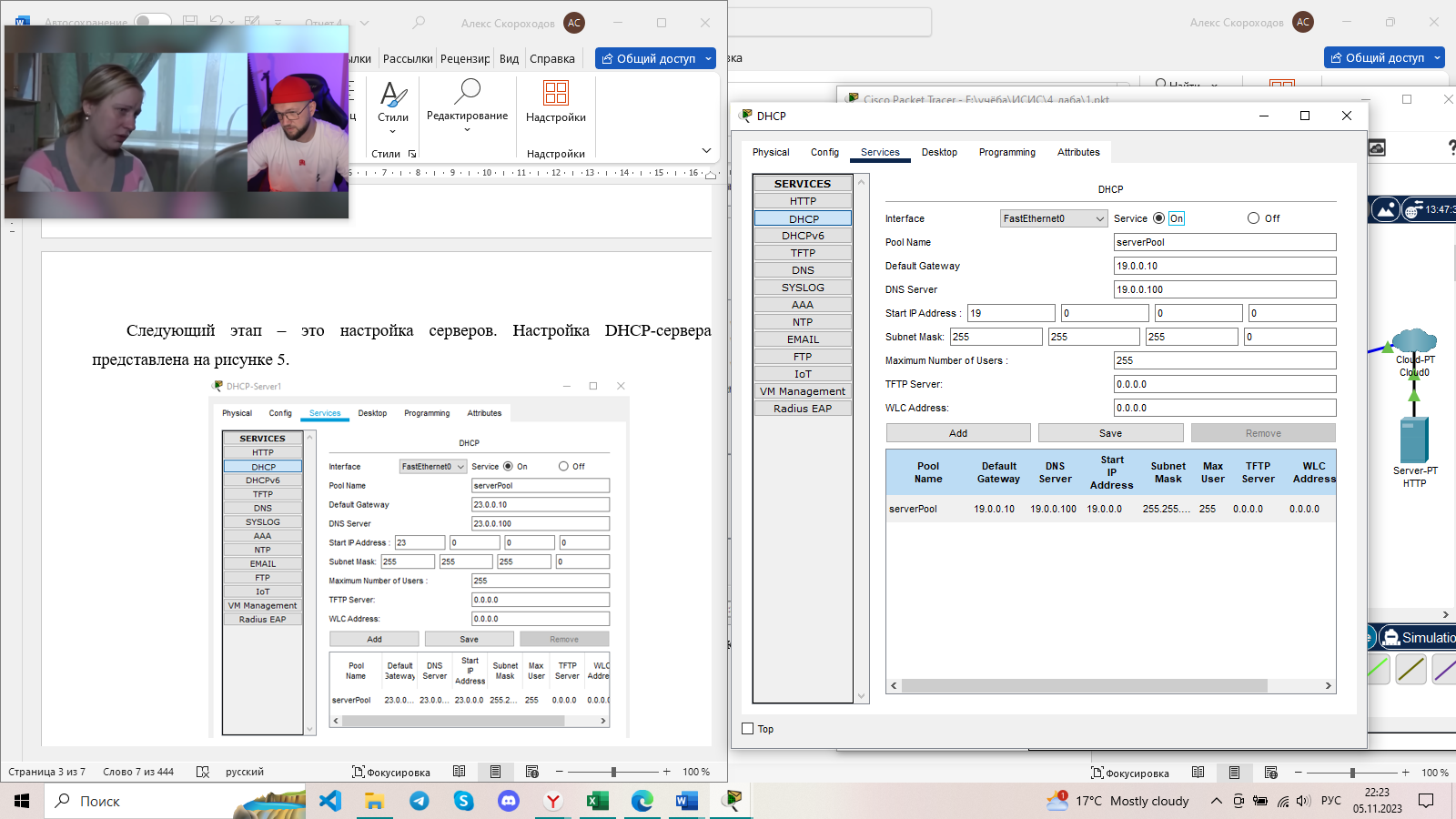


Рисунок 5 – Конфигурация DHCP-сервера

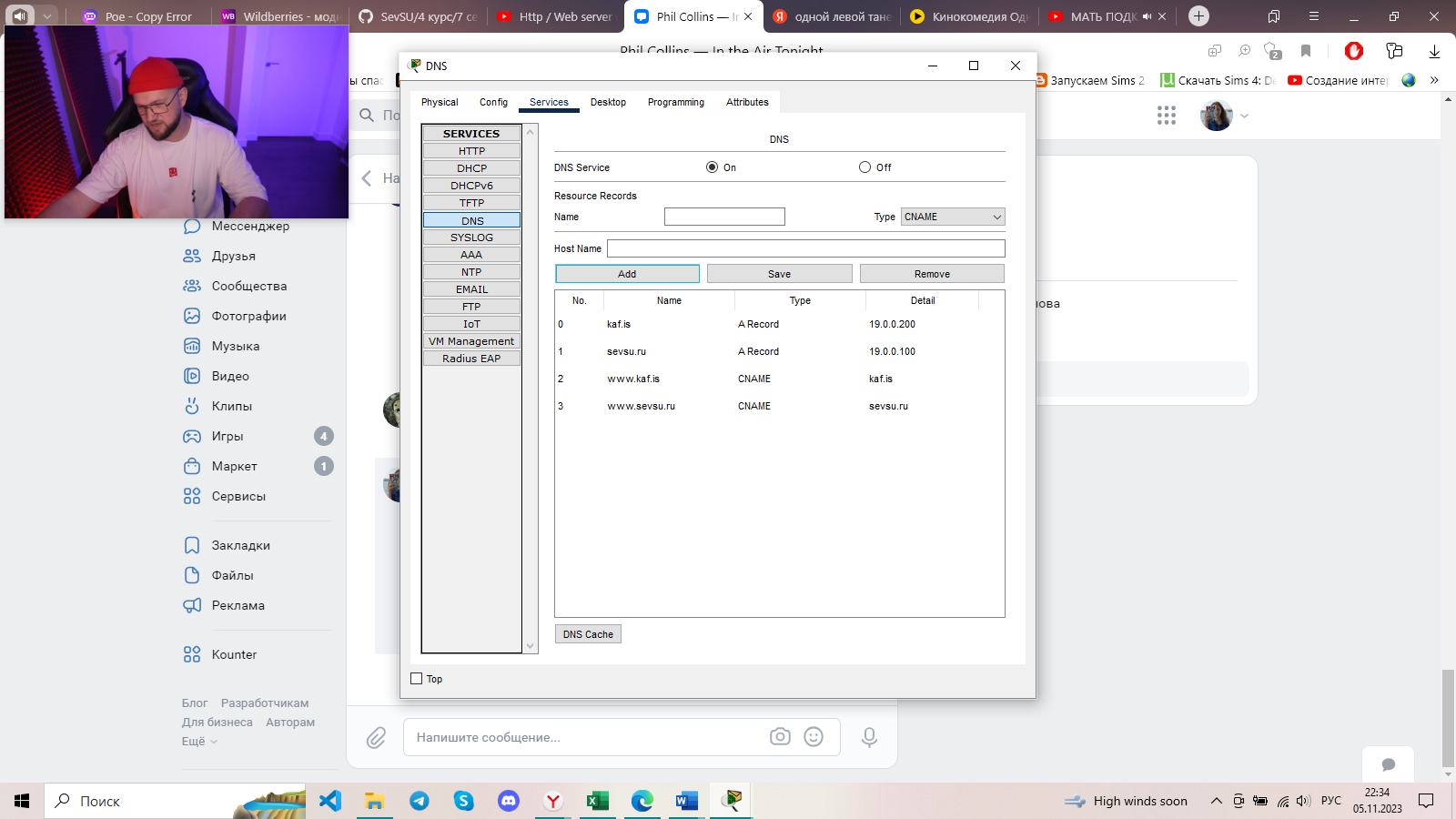


Рисунок 6 – Конфигурация DNS-сервера

Далее требовалось установить на серверный компьютер XY.0.0.100 HTTP-сервер и разместить на нем странички сайтов www.sevsu.ru с информацией о университете и www.kaf.is.ru с рекламной информацией о кафедре ИС.

На рисунке 7 представлен HTML-код странички сайта sevsu.ru, а на рисунке 8 представлен код странички сайта kaf.is.

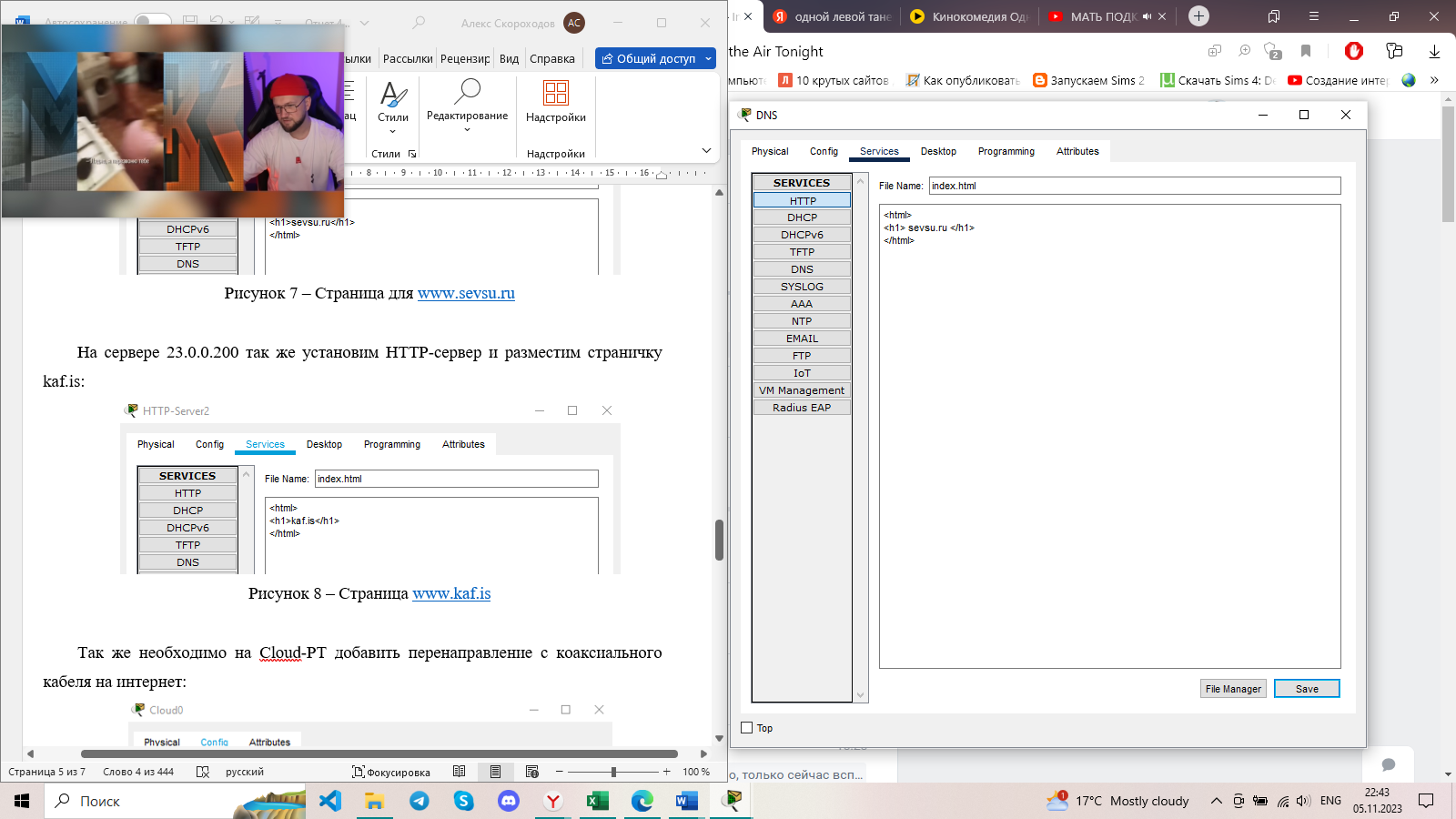


Рисунок 7 – Код сайта sevsu.ru

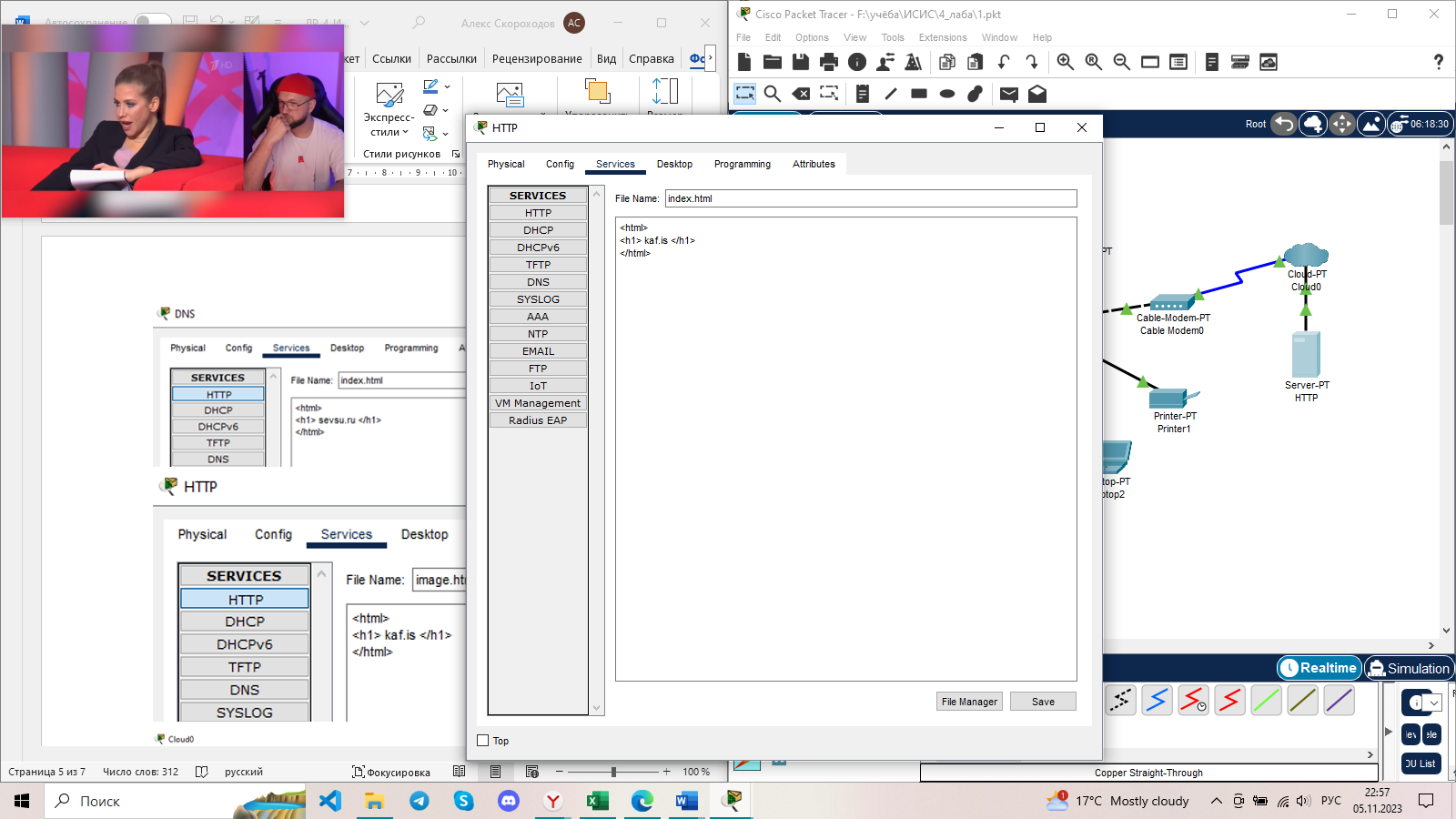


Рисунок 8 – Код сайта kaf.is

Так же необходимо было на Cloud-PT добавить перенаправление с коаксиального кабеля на интернет.

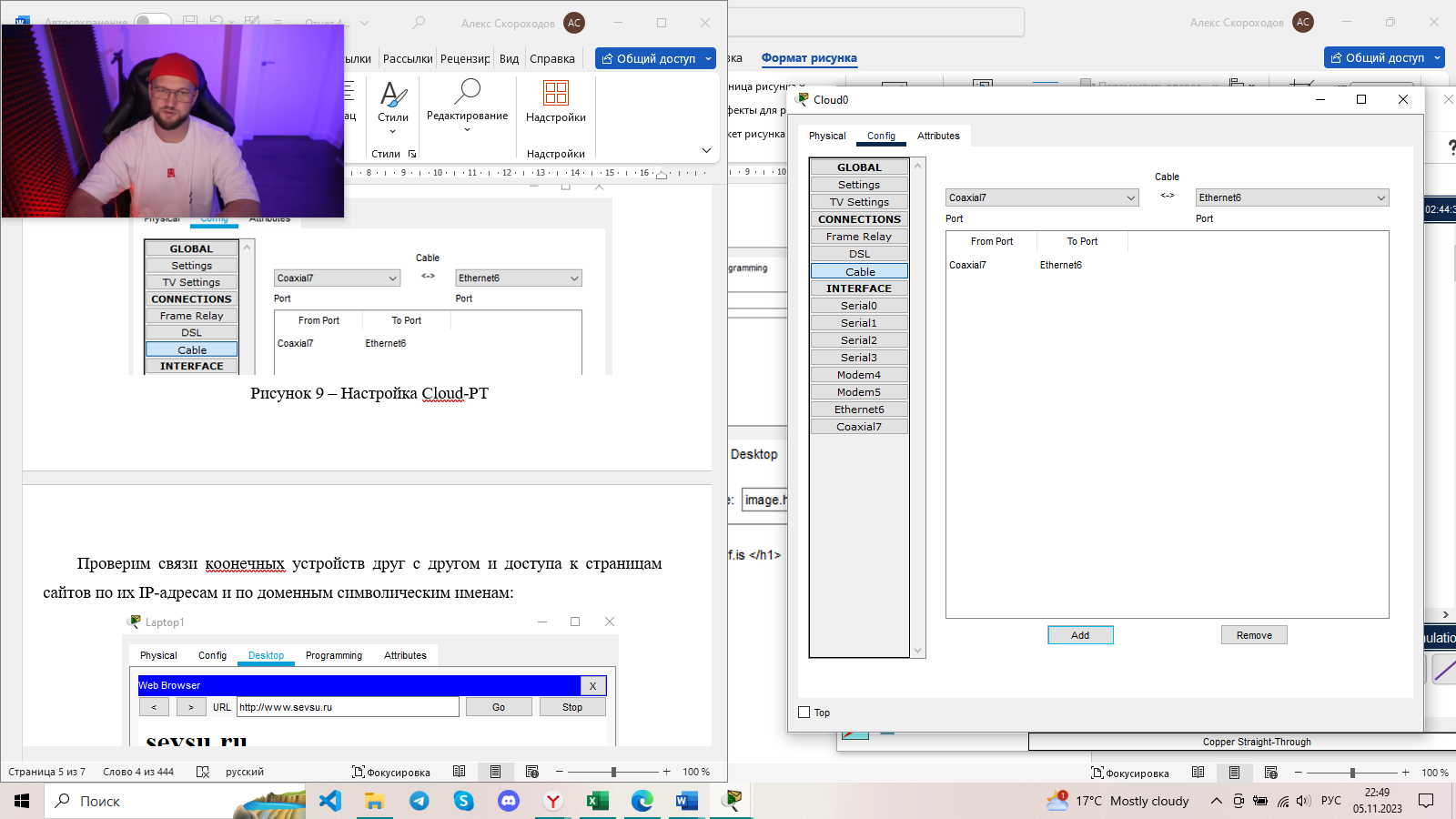


Рисунок 9 – Перенаправление с коаксиального кабеля на интернет

На рисунках 10-13 представлен результат проверки связи оконечных устройств друг с другом и доступа к страницам сайтов по их IP-адресам и по доменным символическим именам в реальном режиме и режиме симуляции.

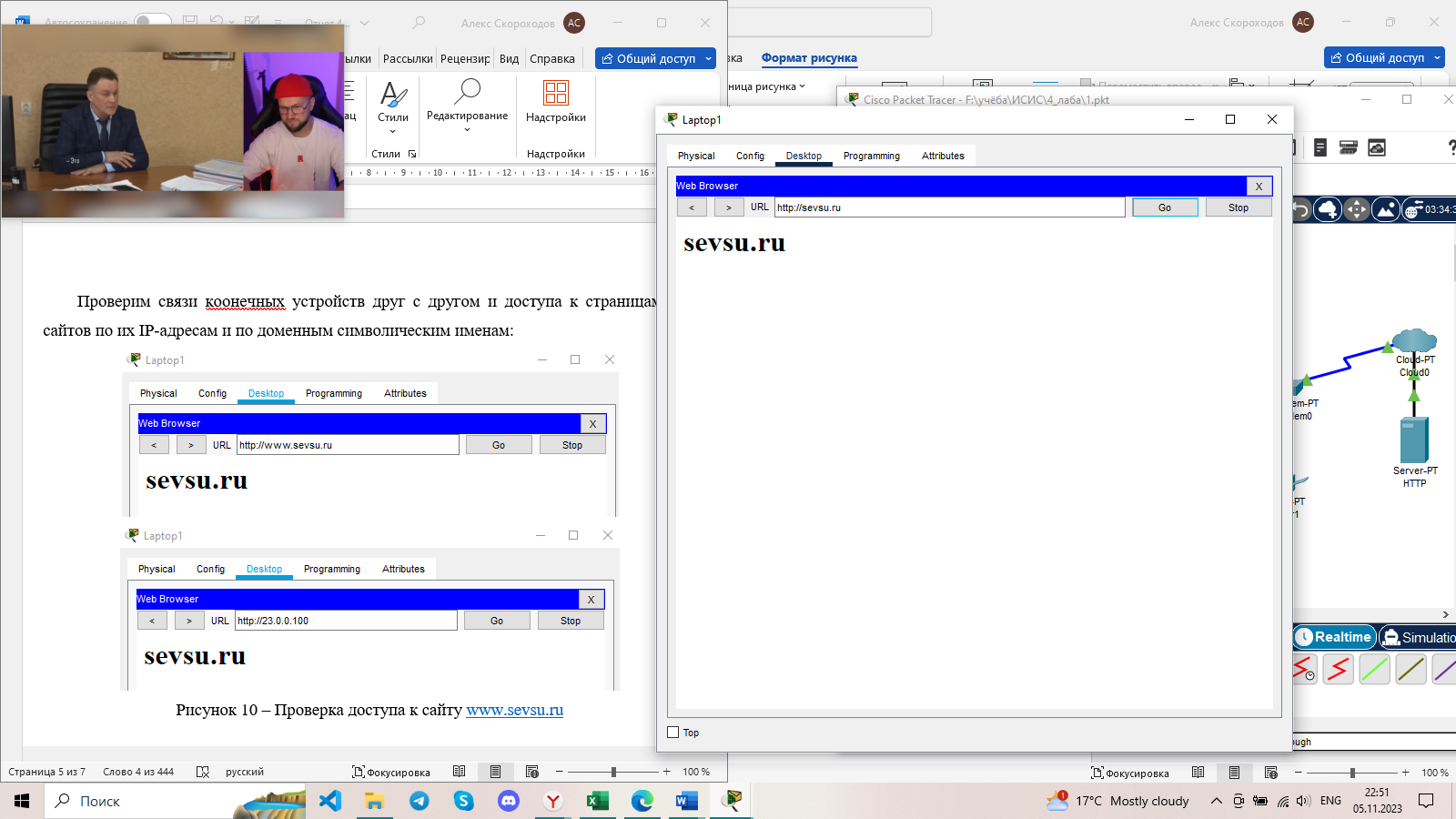


Рисунок 10 – Доступ к странице sevsu.ru по доменному символическому имени

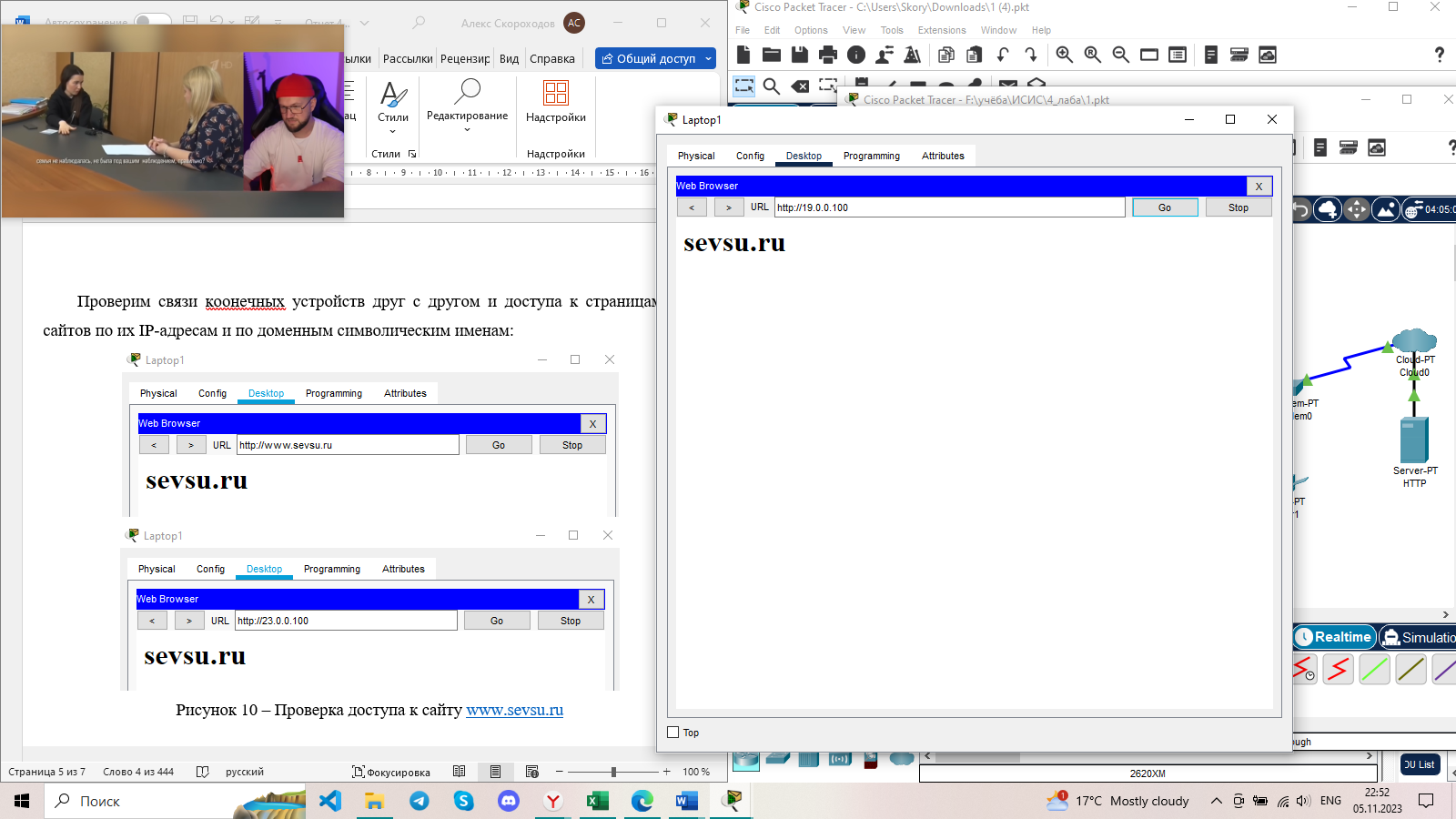


Рисунок 11 – Доступ к странице sevsu.ru по IP-адресу

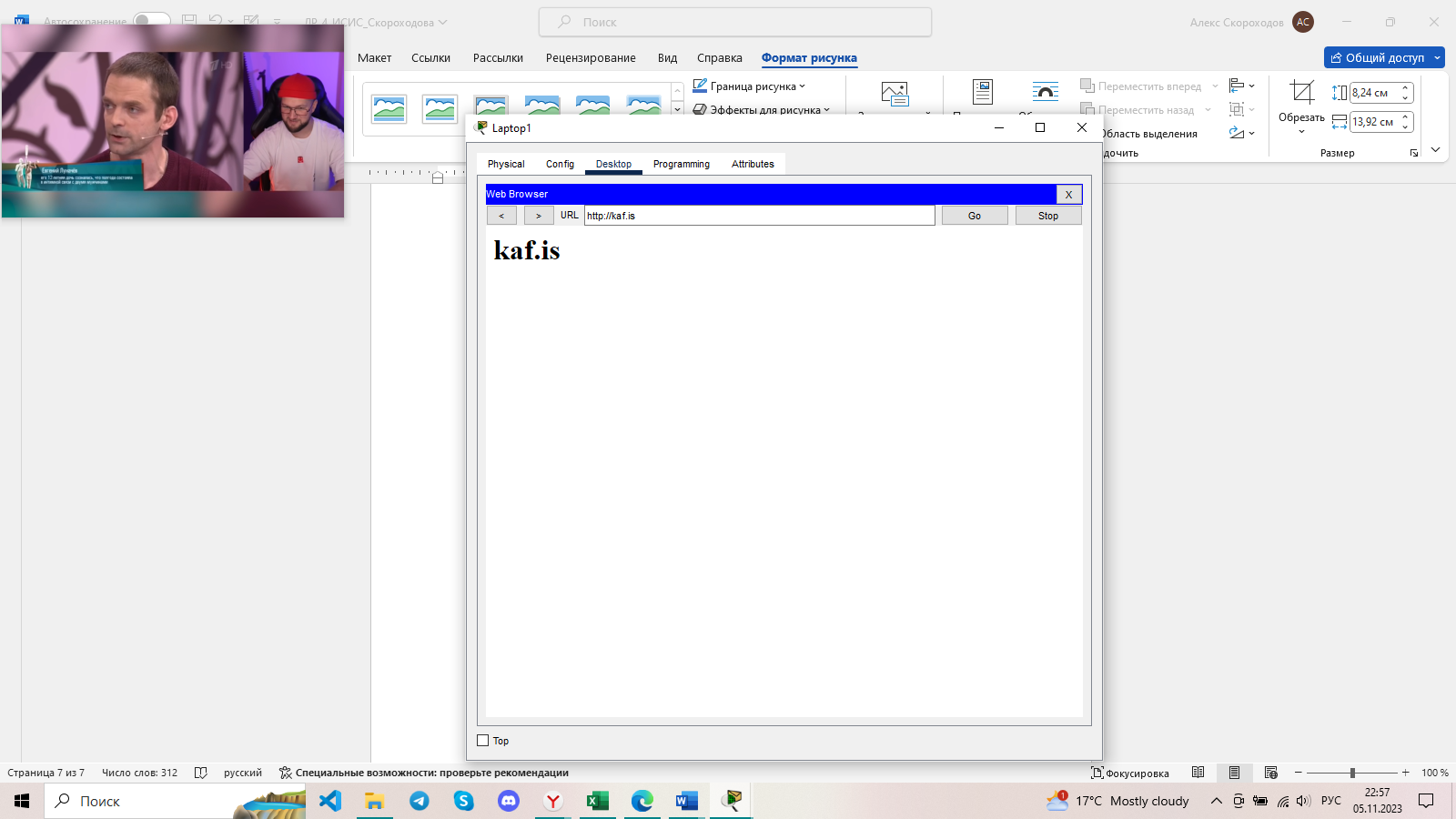


Рисунок 12 – Доступ к странице kaf.is по доменному символическому имени

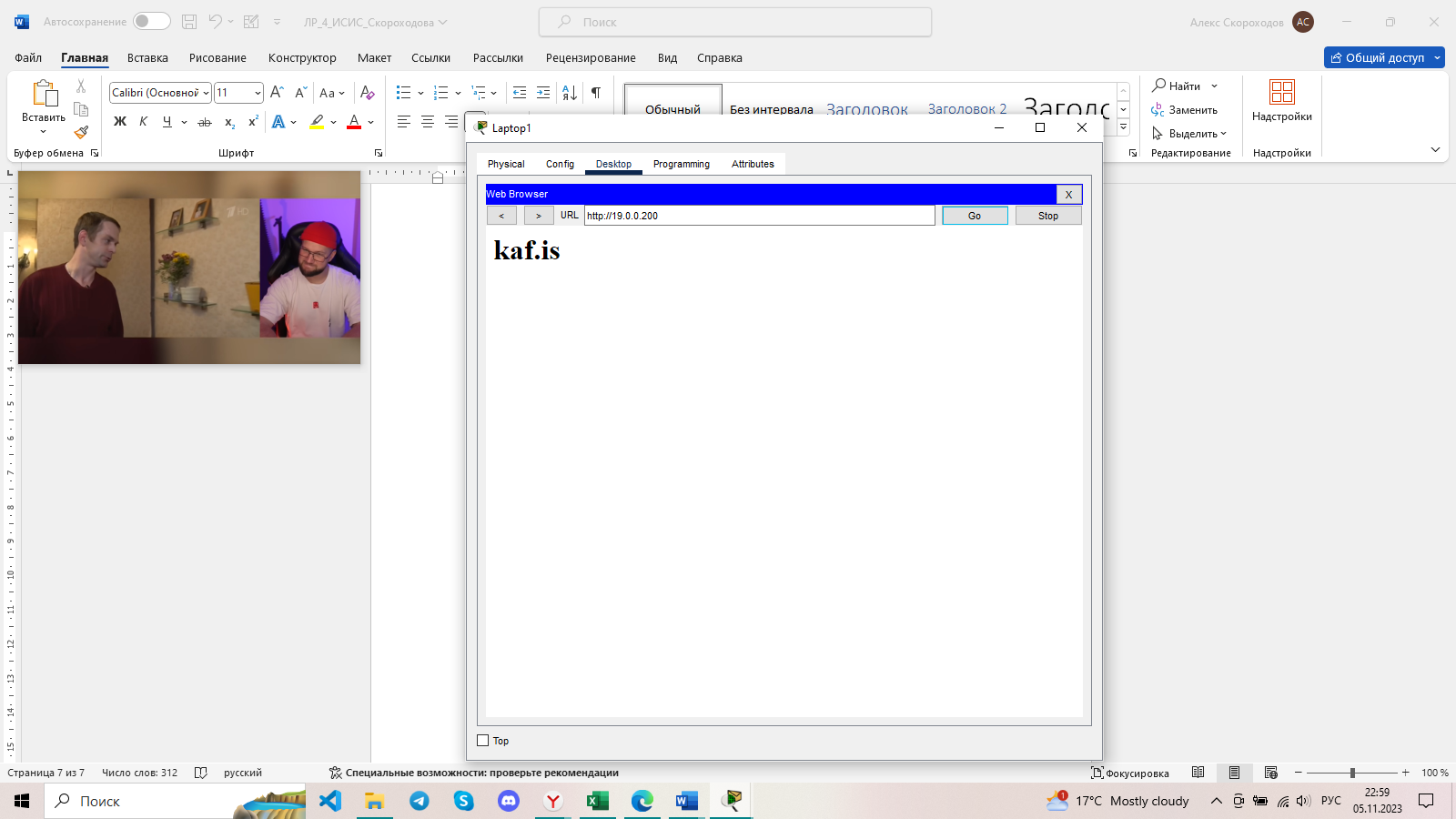


Рисунок 13 – Доступ к странице kaf.is по IP-адресу

ВЫВОДЫ

В ходе выполнения лабораторной работы были исследованы особенности использования основных сетевых серверных служб стека протоколов TCP/IP и конфигурации серверов, реализующих эти службы, приобретены практические навыки по конфигурации серверного сетевого оборудования.

Произведена настройка динамического распределения ip-адресов при помощи DHSP-сервера, настроены доменные имена при помощи DNS-сервера и настроена локальная сеть.

**Контрольные вопросы**:

**7.1 Что представляют собой сетевые службы и зачем они предназначены?**

В простейшем понимании служба — это пара программ, взаимодействующих между собой согласно определенным протоколами по схеме клиент-сервер. Одна из программ этой пары называется сервером, а другая — клиентом. Соответственно, когда говорят о работе сетевых служб, речь идет о взаимодействии оборудования и программного обеспечения сервера с оборудованием и программным обеспечением клиента, обеспечивающих функционирование компьютерной сети.

Зачем нужны некоторые:

**Служба имен (DNS - Domain Name System):** DNS предоставляет механизм преобразования доменных имен (например, www.example.com) в соответствующие сетевые адреса (IP-адреса). Она помогает упростить процесс идентификации и обмена данными между компьютерами в сети.

**Служба файловой передачи (FTP - File Transfer Protocol):** FTP обеспечивает возможность передачи файлов между компьютерами в сети. Она позволяет пользователям загружать и скачивать файлы с удаленных серверов, а также управлять файлами и папками на удаленных компьютерах.

**Служба электронной почты (SMTP - Simple Mail Transfer Protocol):** SMTP используется для отправки электронной почты по сети. Она обеспечивает маршрутизацию и доставку сообщений электронной почты между почтовыми серверами.

**Служба веб-сервера (HTTP - Hypertext Transfer Protocol):** HTTP используется для передачи веб-страниц и других ресурсов через интернет. Веб-серверы обрабатывают запросы от клиентов (браузеров) и предоставляют им запрошенные веб-страницы.

**7.2 Назовите протоколы прикладного уровня стека TCP/IP и поясните для чего используется тот или иной протокол.**

1. HTTP (Hypertext Transfer Protocol): HTTP используется для передачи гипертекстовых документов, таких как веб-страницы, между веб-серверами и клиентами (обычно веб-браузерами). Он определяет формат запросов и ответов, используемых для доступа к веб-ресурсам. HTTP также может использоваться для передачи других данных, таких как изображения, видео и файлы.
2. HTTPS (Hypertext Transfer Protocol Secure): HTTPS является защищенной версией протокола HTTP. Он добавляет шифрование и аутентификацию с использованием протокола SSL/TLS (Secure Sockets Layer/Transport Layer Security), обеспечивая безопасную передачу данных между клиентом и сервером. HTTPS широко применяется для безопасного доступа к веб-сайтам, особенно там, где требуется передача конфиденциальной информации, такой как пароли или финансовые данные.
3. FTP (File Transfer Protocol): FTP используется для передачи файлов между клиентом и сервером. Он обеспечивает команды для управления файлами и директориями, а также для загрузки (upload) и скачивания (download) файлов. FTP может работать в активном или пассивном режиме, в зависимости от конфигурации сети.
4. SMTP (Simple Mail Transfer Protocol): SMTP используется для отправки и доставки электронной почты между почтовыми серверами. Он определяет формат и протоколы, используемые для передачи сообщений электронной почты, и может работать вместе с другими протоколами, такими как POP3 (Post Office Protocol version 3) или IMAP (Internet Message Access Protocol), которые используются для получения почты с сервера.
5. DNS (Domain Name System): DNS преобразует доменные имена (например, www.example.com) в соответствующие IP-адреса. Он обеспечивает распределенную систему именования, позволяя пользователям использовать удобные доменные имена вместо запоминания числовых IP-адресов. DNS также может выполнять другие функции, такие как обнаружение и регистрация служб.
6. DHCP (Dynamic Host Configuration Protocol): DHCP предоставляет автоматическую настройку IP-адресов и других сетевых параметров для устройств в сети. Он позволяет компьютерам и другим устройствам получать IP-адреса, маски подсети, адреса шлюза и другую конфигурационную информацию автоматически при подключении к сети.

**7.3 Приведите формат IP-адреса протокола IPv4, назовите его принципиальное отличие от МАС-адреса**.

Отличие IP-адреса от MAC-адреса заключается в следующем:

**Функциональное назначение:** IP-адрес (Internet Protocol address) используется для идентификации и маршрутизации сетевых узлов (компьютеров, маршрутизаторов, серверов) в сети Интернет или локальной сети. Он определяет уникальный адрес, который используется для доставки пакетов данных от отправителя к получателю. MAC-адрес (Media Access Control address) же применяется на канальном уровне OSI-модели и идентифицирует сетевой интерфейс конкретного устройства. Он является физическим адресом, присвоенным сетевому адаптеру (например, Ethernet-адрес).

**Уникальность:** IP-адреса в IPv4 должны быть уникальными в рамках одной сети. Они могут повторяться в разных сетях, но для обеспечения уникальности в Интернете используется дополнительная структура адресации, такая как система доменных имен (DNS). MAC-адреса, с другой стороны, являются уникальными для каждого сетевого интерфейса и не должны повторяться в пределах сети.

**Иерархия и маршрутизация**: IP-адреса образуют иерархическую структуру, которая позволяет маршрутизаторам определить путь доставки пакетов данных через сеть. Это облегчает глобальную маршрутизацию в Интернете. MAC-адреса не имеют иерархической структуры и используются только для локального обмена данными в пределах одной локальной сети.

**Изменяемость:** IP-адреса могут быть динамически назначены и изменены с помощью протокола DHCP (Dynamic Host Configuration Protocol). MAC-адреса, напротив, являются статическими и остаются неизменными для конкретного сетевого интерфейса.

**7.4 С какой целью разработан протокол ARP и каков основной состав полей заголовка ARP-пакета?**

Протокол ARP (Address Resolution Protocol) разработан с целью связывания (резолюции) IP-адресов с соответствующими MAC-адресами в локальной сети. Он позволяет узлам в сети определить MAC-адрес других узлов по их IP-адресам.

Основной состав полей заголовка ARP-пакета включает следующие поля:

1. Hardware Type (Тип оборудования): Это поле указывает тип физического сетевого устройства, такого как Ethernet. Каждому типу оборудования присвоен уникальный числовой идентификатор.
2. Protocol Type (Тип протокола): Это поле определяет тип протокола сетевого уровня, для которого выполняется резолюция адреса. В случае протокола IPv4 значение этого поля будет равно 0x0800.
3. Hardware Address Length (Длина физического адреса): Это поле указывает размер MAC-адреса в байтах. Например, для Ethernet-адресов длина составляет 6 байт.
4. Protocol Address Length (Длина адреса протокола): Это поле определяет размер IP-адреса в байтах. Для IPv4 адресов длина составляет 4 байта.
5. Operation (Операция): Это поле указывает тип операции, которую выполняет отправитель ARP-запроса или ARP-ответа. Например, значениями могут быть "ARP Request" (запрос ARP) или "ARP Reply" (ответ ARP).
6. Sender Hardware Address (Физический адрес отправителя): Это поле содержит MAC-адрес отправителя ARP-запроса или ARP-ответа.
7. Sender Protocol Address (Адрес протокола отправителя): Это поле содержит IP-адрес отправителя ARP-запроса или ARP-ответа.
8. Target Hardware Address (Физический адрес получателя): Это поле содержит MAC-адрес узла, для которого выполняется резолюция адреса. В ARP-запросе оно обычно устанавливается в нулевое значение.
9. Target Protocol Address (Адрес протокола получателя): Это поле содержит IP-адрес узла, для которого выполняется резолюция адреса.



**7.5 Для чего предназначен протокол DNS и как решается проблема, если в данном DNS-сервере отсутствует запись соответствия символического и сетевого адресов?**

Протокол DNS (Domain Name System) предназначен для преобразования символических имен доменов, таких как "example.com", в их соответствующие IP-адреса и наоборот. Он выполняет роль поисковой системы Интернета, позволяя пользователям использовать удобные символические имена для доступа к ресурсам в сети вместо запоминания числовых IP-адресов.

Когда в DNS-сервере отсутствует запись соответствия символического и сетевого адресов (называемая записью DNS-зоны), возникает проблема неразрешенного имени (unresolved name). В этом случае запрос на разрешение имени, отправленный клиентским устройством, не может быть успешно обработан.

Проблема неразрешенного имени может быть решена следующими способами:

1. Кэширование: Если DNS-сервер не может найти требуемую запись в своей базе данных, он может осуществить запрос другому DNS-серверу, который имеет больше информации. Полученная запись может быть закэширована на DNS-сервере на определенное время, что позволяет удовлетворить будущие запросы без необходимости повторного обращения к удаленному DNS-серверу.
2. Рекурсивный запрос: Если DNS-сервер не может найти запись в своей базе данных или кэше, он может выполнить рекурсивный запрос другому DNS-серверу, начиная с корневого сервера доменных имен. Рекурсивный запрос означает, что сервер продолжает обращаться к другим серверам до тех пор, пока не будет найдена требуемая запись или будет достигнута конечная точка, где будет сказано, что запись не существует.
3. Поиск по умолчанию: Если все попытки разрешения имени завершаются неудачей, DNS-сервер может использовать запись по умолчанию (default record), которая определена для неизвестных или несуществующих записей. Например, DNS-сервер может вернуть специальный IP-адрес, указывающий на то, что запись не найдена или доменное имя не существует.

**7.6 Расскажите об особых (выделенных под специальные нужды) IP-адресах и их назначениях.**

1. IP-адресы петли обратной связи (Loopback addresses): IP-адреса из диапазона 127.0.0.0/8 (127.0.0.1 до 127.255.255.254) назначаются для тестирования и обратной связи в локальном устройстве. Адрес 127.0.0.1 (или localhost) обычно используется для обращения к собственному устройству, когда необходимо выполнить запрос к самому себе.
2. IP-адреса частных сетей (Private network addresses): IP-адреса из следующих диапазонов являются зарезервированными для использования в частных сетях, которые не являются прямо подключенными к Интернету:

* 10.0.0.0 до 10.255.255.255 (диапазон 10.0.0.0/8)
* 172.16.0.0 до 172.31.255.255 (диапазон 172.16.0.0/12)
* 192.168.0.0 до 192.168.255.255 (диапазон 192.168.0.0/16)

Эти адреса могут быть использованы в локальных сетях для назначения IP-адресов устройствам, не подключенным напрямую к Интернету.

1. IP-адреса многоадресной рассылки (Multicast addresses): IP-адреса из диапазона 224.0.0.0 до 239.255.255.255 назначаются для многоадресной рассылки данных. Они используются для отправки пакетов одновременно нескольким узлам в сети, которые являются частью определенной многоадресной группы.
2. IP-адреса зарезервированных для тестирования (Reserved for testing): IP-адреса из диапазона 240.0.0.0 до 255.255.255.254 зарезервированы для целей тестирования и локальных экспериментов. Они не предназначены для использования в реальных сетях.
3. IP-адреса петли маршрутизатора (Router loopback addresses): Некоторые специальные IP-адреса, такие как 0.0.0.0 и 255.255.255.255, могут использоваться для определенных целей в маршрутизации и сетевых протоколах, например, для указания маршрута по умолчанию или для широковещательных сообщений.

**7.7 Что представляют собой локальные IP-адреса, назовите диапазоны сетей таких адресов. Для чего служит протокол сетевой трансляции адресов?**

Локальные IP-адреса представляют собой адреса, которые используются в локальных сетях для идентификации устройств внутри сети. Они не маршрутизируются в Интернете и являются уникальными только в пределах локальной сети. Когда устройство отправляет пакеты в Интернет, локальный IP-адрес транслируется в публичный IP-адрес с использованием сетевой трансляции адресов (NAT).

Диапазоны локальных IP-адресов определены в стандарте RFC 1918 и включают следующие диапазоны:

* 10.0.0.0 до 10.255.255.255 (диапазон 10.0.0.0/8)
* 172.16.0.0 до 172.31.255.255 (диапазон 172.16.0.0/12)
* 192.168.0.0 до 192.168.255.255 (диапазон 192.168.0.0/16)

Протокол сетевой трансляции адресов (Network Address Translation, NAT) является механизмом, который позволяет локальным устройствам в локальной сети использовать локальные IP-адреса, а затем транслирует эти адреса в публичные IP-адреса при общении с устройствами в Интернете. NAT выполняет преобразование IP-адресов и портов в пакетах, проходящих через маршрутизатор или сетевой шлюз, чтобы обеспечить соответствующую коммуникацию между локальными и публичными сетями.

Преимущества использования NAT включают экономию публичных IP-адресов, обеспечение безопасности, скрытие локальной сети от внешнего мира и возможность использования локальных IP-адресов в сетях с большим количеством устройств, не требуя уникальных публичных IP-адресов для каждого устройства.

**7.8 Опишите формат и использование маски подсети. Как по значению маски определить количество адресов, которое она выделяет? Перечислите известные Вам маски и их характеристики для сети класса С.**

Маска подсети — это 32-битное число, которое используется для определения того, какая часть IP-адреса относится к сети, а какая — к устройству внутри сети.

В случае сети класса С, маска подсети состоит из 24 единиц (1) и 8 нулей (0), соответствующих третьему октету IP-адреса. Ниже перечислены известные маски и их характеристики для сети класса С:

Маска подсети /24 (или 255.255.255.0): В этом случае, третий октет маски равен 255, а четвертый октет равен 0. Это означает, что в сети доступно 2^8 (256) адресов, но 2 адреса (0 и 255) зарезервированы и не могут быть назначены устройствам. Таким образом, в этой сети доступно 254 адреса для устройств.

Маска подсети /25 (или 255.255.255.128): В этом случае, третий октет маски равен 255, а четвертый октет равен 128. Это означает, что в сети доступно 2^7 (128) адресов, но 2 адреса (0 и 127) зарезервированы и не могут быть назначены устройствам. Таким образом, в этой сети доступно 126 адресов для устройств.

Маска подсети /26 (или 255.255.255.192): В этом случае, третий октет маски равен 255, а четвертый октет равен 192. Это означает, что в сети доступно 2^6 (64) адресов, но 2 адреса (0 и 63) зарезервированы и не могут быть назначены устройствам. Таким образом, в этой сети доступно 62 адреса для устройств.

Маска подсети /27 (или 255.255.255.224): В этом случае, третий октет маски равен 255, а четвертый октет равен 224. Это означает, что в сети доступно 2^5 (32) адреса, но 2 адреса (0 и 31) зарезервированы и не могут быть назначены устройствам. Таким образом, в этой сети доступно 30 адресов для устройств.

**7.9 Что представляет собой технология бесклассовой междоменной маршрутизации? Запишите адрес и маску суперсети для 2000 хостов.**

Технология бесклассовой междоменной маршрутизации (CIDR - Classless Inter-Domain Routing) представляет собой метод разбиения IP-адресов на более мелкие подсети, не придерживаясь ограничений классовой адресации (классов A, B и C). Вместо использования фиксированных префиксов, CIDR позволяет гибко использовать адресное пространство, определяя длину префикса с помощью маски подсети.

**7.10 Для чего предназначен протокол DHCP и может ли компьютерная сеть функционировать без этого протокола?**

Протокол DHCP (Dynamic Host Configuration Protocol) предназначен для автоматической конфигурации IP-адресов и других сетевых параметров на компьютерах в сети. Он позволяет компьютерам получать IP-адрес, маску подсети, адрес шлюза (маршрутизатора), серверы DNS и другие настройки сети от DHCP-сервера.

Протокол DHCP имеет несколько важных функций:

1. Автоматическая настройка: DHCP позволяет компьютерам автоматически получать конфигурацию сети без необходимости вручную вводить IP-адреса и другие параметры. Когда компьютер подключается к сети, он отправляет запрос DHCP, и DHCP-сервер предоставляет необходимую конфигурацию.
2. Динамическое выделение IP-адресов: DHCP-сервер может динамически выделять IP-адреса из пула доступных адресов. Когда компьютер выключается или отключается от сети, его IP-адрес возвращается в пул и может быть назначен другому компьютеру. Это позволяет эффективно использовать ограниченное адресное пространство.
3. Централизованная управляемость: DHCP позволяет администраторам сети централизованно управлять настройками сети. Изменения в сетевой конфигурации могут быть внесены на DHCP-сервере, и компьютеры автоматически получат обновленные настройки при следующем подключении.

Ответ на вторую часть вопроса: Да, компьютерная сеть может функционировать без протокола DHCP, но это будет требовать ручной настройки каждого компьютера в сети сетевыми параметрами, такими как IP-адрес, маска подсети, адрес шлюза и DNS-серверы.

**7.11 Что представляет собой маршрут по умолчанию, для чего он используется? Каким образом маршрут по умолчанию указывается в таблице маршрутизации?**

Маршрут по умолчанию (default route) представляет собой предопределенный маршрут, который используется в сетях, когда маршрутизатор не может найти более специфичный маршрут для пакета. Он указывает на следующий прыжок (следующий маршрутизатор или шлюз) для пакетов, адрес назначения которых не соответствует ни одному из записанных в таблице маршрутизации.

Маршрут по умолчанию используется в следующих случаях:

* Передача пакетов за пределы локальной сети: Если маршрутизатор получает пакет, адрес назначения которого не соответствует ни одной записи в его таблице маршрутизации, то он отправляет пакет по маршруту по умолчанию. Это позволяет пакетам достичь удаленных сетей или Интернета.
* Отсутствие специфичных маршрутов: Когда в таблице маршрутизации отсутствуют записи для конкретных сетей или подсетей, маршрут по умолчанию используется для обработки пакетов, адресованных этим сетям.

Маршрут по умолчанию указывается в таблице маршрутизации следующим образом:

В IPv4 таблице маршрутизации маршрут по умолчанию обычно записывается с префиксом 0.0.0.0/0 и указывает на адрес следующего прыжка (шлюза), через который пакеты должны быть отправлены. Этот адрес следующего прыжка обычно представляет собой IP-адрес маршрутизатора, который имеет доступ к удаленным сетям или Интернету.

В IPv6 таблицах маршрутизации маршрут по умолчанию записывается с префиксом ::/0 и также указывает на адрес следующего прыжка (шлюза).

Маршрут по умолчанию в таблице маршрутизации имеет наименьший приоритет (метрику), что означает, что он будет использоваться только в случае отсутствия более специфичных маршрутов для пакетов.

**7.12** **Чем отличается статическая маршрутизация от динамической? Приведите названия используемых протоколов динамической маршрутизации.**

Статическая маршрутизация:

* В статической маршрутизации администратор вручную настраивает маршруты в таблице маршрутизации на каждом маршрутизаторе в сети.
* Маршруты не обновляются автоматически и остаются постоянными, пока администратор не внесет изменения вручную.
* Статическая маршрутизация проста в настройке и не требует дополнительных ресурсов для обмена информацией о маршрутах между маршрутизаторами.
* Она подходит для небольших сетей с небольшим количеством маршрутов и ограниченными изменениями в сетевой топологии.

Динамическая маршрутизация:

* В динамической маршрутизации маршруты автоматически обновляются и обмениваются между маршрутизаторами с использованием протоколов маршрутизации.
* Маршруты определяются на основе информации, полученной от других маршрутизаторов, и таблица маршрутизации автоматически обновляется при изменениях в сетевой топологии.
* Динамическая маршрутизация более гибкая и масштабируемая, поскольку позволяет автоматически адаптироваться к изменениям в сети.
* Протоколы динамической маршрутизации, такие как OSPF (Open Shortest Path First), RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol) и BGP (Border Gateway Protocol), используются для обмена информацией о маршрутах и определения наилучших путей для передачи пакетов.

7.13 Какие действия происходят в сети при смене статической адресации на динамическую?

7.14 Как рационально спланировать установку DHCP-серверов в локальных и глобальных сетях?

7.15 Как на практике в эмуляторе Packet Tracer проверить содержимое заголовков пакетов?