

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

# **ИССЛЕДОВАНИЕ АРХИТЕКТУРЫ ПРОТОКОЛОВ ARP и ICMP**

## **МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

по выполнению лабораторной работы по дисциплине  
«Инфокоммуникационные системы и сети»  
для студентов дневного и заочного отделения по направлению  
09.03.02 «Информационные системы и технологии»,  
09.03.03 «Прикладная информатика»

**Севастополь  
2021**

УДК 681.326

Методические указания к выполнению лабораторной работы «**Исследование архитектуры протоколов ARP и ICMP**» по дисциплине «Инфокоммуникационные системы и сети» / Сост. доц. Чернега В.С. – Севастополь: Изд-во СевГУ, 2021. – 28 с.

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

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

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

Рецензент            доцент кафедры «Информационные системы»

к.т.н., доцент

Кротов К.В.

## СОДЕРЖАНИЕ

	Лабораторная работа «Исследование архитектуры протоколов ARP и ICMP .....	4
1	Цель работы .....	4
2	Основные теоретические положения .....	4
2.1	Архитектура протокола ARP .....	4
2.2	Архитектура протокола ICMP .....	6
3	Описание лабораторной установки .....	8
4	Программа выполнения работы .....	9
5	Методические рекомендации по выполнению работы .....	9
6	Содержание отчета .....	10
7	Контрольные вопросы .....	10
	Библиографический список .....	11

## Лабораторная работа

**ИССЛЕДОВАНИЕ АРХИТЕКТУРЫ ПРОТОКОЛОВ ARP и ICMP****1 ЦЕЛЬ РАБОТЫ**

Целью работы является углубление теоретических знаний по архитектуре протоколов стека TCP/IP, исследование способов разрешения адресов, контроля и управления сетью, а также приобретение практических навыков конфигурации и исследования функционирования компьютерных сетей.

**2 ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ****2.1 Архитектура протокола ARP**

Обмен сообщениями между передатчиком и приемником конечных устройств компьютерной сети осуществляется по линии связи в виде кадров (фреймов). Кадры могут поступать на входы многих получателей. Поэтому для приема кадра конкретной станцией назначения в нем должен содержаться аппаратный (физический) адрес нужного приемного устройства, а для возможности отправить ответ передатчику, в кадре должен присутствовать и аппаратный адрес отправителя. Любое устройство, подключенное к локальной сети (Ethernet, FDDI и т.д.), имеет уникальный физический (аппаратный, MAC-) сетевой адрес. Если у компьютера меняется сетевой адаптер, то меняется и его MAC-адрес. Драйвер Ethernet должен знать MAC-адрес интерфейса назначения, чтобы послать туда данные. Однако при передаче сообщений по компьютерной сети используется адресация на логическом уровне, т.е. передаются IP-адреса. При этом аппаратные адреса приемных устройств в большинстве случаев отправителю сообщения не известны.

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

Преобразование IP-адресов в аппаратные выполняется с помощью ARP-таблицы. Каждый сетевой компьютер, а также маршрутизатор, имеет отдель-

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

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

Порядок преобразования адресов происходит следующим образом:

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

В современных сетевых ОС (Windows, Linux, BSD) таблицу преобразования адресов можно просмотреть в консоли с помощью команды **arp -a**. Чтобы очистить ARP кэш в Windows нужно в командной строке набрать команду **arp -d**. Обратите внимание, что между **arp** и дефисом должен быть пробел!

Формат кадра протокола ARP показан на рисунке 2.1.

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

Рисунок 2.1 – Формат кадра протокола ARP

Он содержит следующие поля.

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

**Тип протокола** (*Protocol Type*). В него помещается признак типа исполь-

зуемого протокола сетевого уровня. Например, для протокола IP в это поле помещается число 2048, для X.25 – 2053.

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

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

**Аппаратный адрес отправителя/получателя (Sender/Target Hardware Address)** служат для размещения физических адресов передающей станции и станции назначения соответственно.

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

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

## 2.2 Архитектура протокола ICMP

В процессе обмена информацией в компьютерной сети возможно появление ошибок передачи, отказов аппаратного и программного обеспечения, возникновение условий и аномальных ситуаций, требующих принятия определенных мер. Для реализации механизма реагирования на такие ситуации разработан **протокол передачи управляющих сообщений ICMP (Internet Control Message Protocol)**. Протокол относится к сетевому уровню модели TCP/IP. На данный протокол возлагаются только функции информирования об особых случаях в сети, а не локализация и устранение причин, которые привели к возникновению аномальных ситуаций. При обнаружении тех или иных проблем промежуточные маршрутизаторы или конечные станции генерируют сообщения ICMP того или иного типа, указывая в них код ошибки, и передают отправителю исходного пакета. ICMP выполняет следующие функции:

- передает отклик на пакет или эхо на отклик;
- контролирует время жизни дейтаграмм в системе;
- реализует переадресацию пакета;
- выдает сообщения о недостижимости адресата или о некорректности параметров;
- формирует и пересылает временные метки;
- выдает запросы и отклики для адресных масок и другой информации.

Для передачи сообщений протокола ICMP по сети Интернет используются IP-дейтаграммы обычного формата. Сообщение ICMP в данном случае помещается (инкапсулируется) в поле данных IP-дейтаграммы (рисунок 2.2).

Сообщение ICMP состоит из заголовка и собственно информационно-управляющего сообщения. Заголовок ICMP включает 8 байт, но только первые 4 байта одинаковы для всех сообщений, остальные поля заголовка и тела сообщения определяются типом сообщения. Первые 4 байта содержат три поля: тип сообщения (8 битов); код сообщения (8 битов) и контрольная сумма (16 битов). Поле контрольной суммы охватывает ICMP-сообщение целиком.

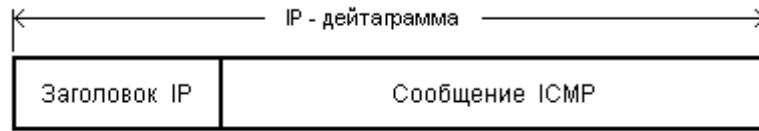


Рисунок 2.2 - Инкапсуляция ICMP-сообщения в IP-дейтаграмму

Сообщения ICMP можно условно разделить на *парные* и *непарные*. Парные сообщения состоят из двух компонентов – **запрос** (*Request*) и **ответ** (*Reply*). Сообщение типа "Ответ" высылается станцией назначения только в ответ на полученное от источника сообщение типа "Запрос". К сообщениям такого типа относятся "Эхо запрос/ответ". Непарные сообщения формируются асинхронно при возникновении какой-либо проблемы при передаче дейтаграммы, и передаются в адрес источника данной дейтаграммы. К сообщениям подобного типа относятся сообщения "Место назначения недоступно" и "Подавление источника" и др. Код сообщения детализирует параметры конкретных управляющих сообщений. В таблице 2.1 приведены некоторые из управляющих сообщений.

Таблица 2.1 – Сообщения протокола ICMP

Тип сообщения	Сообщение
0	Эхо-отклик ( <i>Echo Reply</i> )
3	Место назначения не достижимо ( <i>Destination Unreachable</i> )
4	Подавление источника ( <i>Source Quench</i> )
5	Перенаправление ( <i>Redirect</i> )
8	Эхо-запрос ( <i>Echo Request</i> )
9	Объявление маршрутизатора ( <i>Router Advertisement</i> )
10	Запрос к маршрутизатору ( <i>Router Solicitation</i> )
11	Время истекло ( <i>Time Exceeded</i> )
12	Проблемы с параметрами ( <i>Parameter Problem</i> )
13	Запрос временной метки ( <i>Timestamp Request</i> )
14	Отклик с временной меткой ( <i>Timestamp Reply</i> )
15	Информационный запрос ( <i>Information Request</i> )
16	Информационный отклик ( <i>Information Reply</i> )
17	Запрос маски адреса ( <i>Address Mask Request</i> )
18	Ответ с маской адреса ( <i>Address Mask Reply</i> )

Первым диагностическим средством, с помощью которого начинается идентификация какой-либо проблемы в сетях, является утилита *ping*. Она строится на основе ICMP сообщений "Эхо", которые посылают одно сообщение *Echo Request* в адрес назначения и ожидает получение ответного сообщения *Echo Reply*. Утилиты *ping* с дополнительными ключами формируют несколько последовательных сообщений *Echo Request* и измеряют значение интервала времени, разделяющий момент передачи этих сообщений от момента приема соответствующих ответных сообщений. Помимо доступности, с помощью *ping* можно оценить время возврата пакета от узла, что дает представление о том, "насколько далеко" находится узел.

В поле идентификатора *ping*-сообщения устанавливается идентификатор процесса, отправляющего запрос. Это позволяет программе *ping* идентифицировать вернувшийся ответ, если на одном и том же хосте в одно и то же время запущено несколько программ *ping*.

### 3 Описание лабораторной установки

В качестве лабораторного стенда используется персональный компьютер с установленной программой моделирования компьютерных сетей Cisco Packet Tracer. Работа с этим пакетом моделирования детально описана в предыдущей лабораторной работе. Схема исследуемой сети изображена на рисунке 3.1. Индивидуальные особенности сети определяются вариантом.

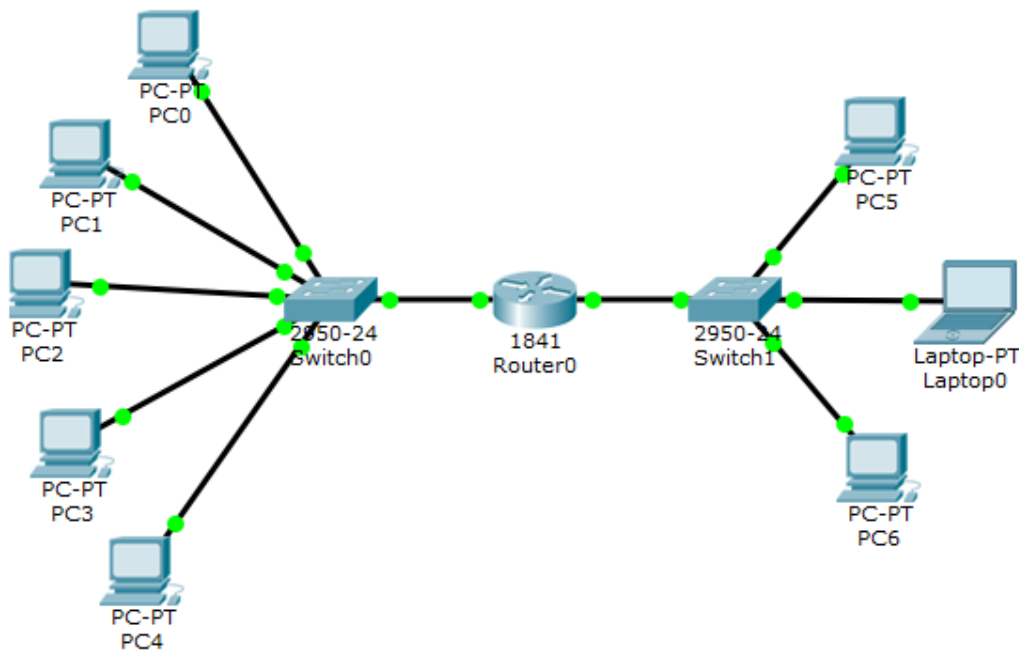


Рисунок 3.1 – Схема исследуемой локальной компьютерной сети



Сеть состоит из двух подсетей, объединенных маршрутизатором Router0. В состав подсетей входят персональные компьютеры PC и ноутбук Laptop0 (рабочие станции) и коммутаторы второго уровня Switch0 и Switch1.

#### **4 Программа выполнения работы**

4.1 Составить схему локальной компьютерной сети, изображенной на рисунке 3.1.

4.2 Выполнить конфигурацию оборудования сети в соответствии с таблицей вариантов. Адрес левой подсети сформировать в виде 172.16.X.0, а адрес правой подсети в виде 192.168.Y.0, где X- последняя цифра зачетной книжки, а Y-предпоследняя.

4.3 Пропинговать поочередно все рабочие станции левой и правой подсетей, проверить и записать содержимое ARP-таблиц персональных компьютеров обеих подсетей.

4.4 Выполнить в режиме симулирования (Simulation) пингование между персональными компьютерами левой подсети.

4.5 Исследовать в режиме симуляции типы используемых пакетов, последовательность обмена пакетами между всеми устройствами сети, а также форматы заголовков передаваемых кадров и пакетов для протоколов ARP и ICMP.

4.6 Выполнить в режиме симулирования пингование между персональными компьютерами левой подсети и персональными компьютерами правой подсети и записать типы используемых пакетов и последовательность обмена пакетами между всеми устройствами сети.

4.7 Исследовать после завершения пингования состав ARP таблиц персональных компьютеров обеих подсетей и маршрутизатора. Проверить ARP-таблицы компьютеров и маршрутизатора с использованием команд консольного интерфейса (CLI). Выполнить сброс ARP-кэша и повторить пингование снова, наблюдая процесс заполнения ARP-таблицы.

4.8 Исследовать в режиме симуляции состав заголовков используемых пакетов.

4.9 Составить отчет по выполненной работе.

#### **5 Методические рекомендации по выполнению работы**

5.1. При задании IP адресов следует помнить, что все интерфейсы, входящие в сеть /подсеть должны иметь одинаковый адрес сети/подсети и различные адреса хостов. При конфигурации хостов им следует также задать адрес шлюза по умолчанию (Gateway), функцию которого выполняет интерфейс маршрутизатора, подключенный к данной подсети.

5.2. Интерфейсы маршрутизаторов должны иметь сетевые адреса такие, как и адреса подсетей, в состав которых они входят.

5.3. Для проверки содержимого ARP таблицы, таблицы коммутации или MAC-адресов следует использовать инструмент Inspect (Лупу), расположенный справа от рабочего окна системы Packet Tracer. Лупу нужно подвести к исследуемому устройству и щелкнуть левой кнопкой мыши.

5.4. Переключения системы моделирования в режим симуляции осуществляется путем нажатия клавиши Simulation, расположенной справа внизу либо нажатием на клавиатуре компьютера (Shift+S).

5.5. Перед запуском симуляции надо в фильтре Edit Filters оставить только использование пакетов ARP и ICMP, а остальные отключить. Это нужно сделать как на вкладке IPv4, так и на вкладке Misc.

5.6. Запуск передачи кадра от одного устройства к соседнему осуществляется однократным нажатием клавиши Capture/Forward. Для наблюдения непрерывной передачи кадров в сети нужно нажать клавишу Auto capture/Play.

5.7. Чтобы исследовать процесс обмена кадрами требуется нажать клавишу Event List.

5.8. Для просмотра состава заголовков определенных кадров, нужно в окне Event List щелкнуть по исследуемому кадру. Для детального анализа состава заголовка для исходящего или входящего трафика нужно нажать соответствующую клавишу PDU Details. Причем, Inbound PDU означает входящий пакет, а Outbound PDU - исходящий.

5.9. ARP-таблица рабочей станции осуществляется командой arp -a, а очистка таблицы командой arp -d в окне Command Prompt. Пробел после arp обязателен! Для сброса ARP-таблицы в маршрутизаторе следует выключить и затем выключить питание маршрутизатора.

## **6 Содержание отчета**

- 6.1 Титульный лист.
- 6.2 Схема моделируемой сети.
- 6.3 Форматы заголовков пакетов ARP и ICMP.
- 6.4 Скриншоты топологии, реализованных настроек и результатов исследования функционирования сети с пояснениями полученных результатов.
- 6.5 Выводы.

## **7 Контрольные вопросы**

- 7.1 Что представляют кадр (фрейм) данных и из каких полей он состоит?
- 7.2 К какому устройству в компьютере относится физический адрес, а к какому логический и какова длина этих адресов?
- 7.3 С какой целью разработан протокол ARP и каков алгоритм получения физического адреса по логическому?
- 7.4 Что такое ARP-кэш и каково его назначение?

- 7.5 Как можно посмотреть ARP-таблицу в персональном компьютере, как можно очистить эту таблицу?
- 7.6 Расскажите о формате кадра протокола ARP и назначении его полей.
- 7.7 Какую функцию регламентирует протокол RARP?
- 7.8 С какой целью разработан протокол ICMP и какие функции он реализует?
- 7.9 Расскажите о формате протокола ICMP и назначении полей пакета.
- 7.10 Чем парные ICMP-сообщения отличаются от непарных?
- 7.11 Какие типы ICMP-сообщения используются в программе ping?
- 7.12 Приведите примеры нескольких типов ICMP-сообщений.
- 7.13 Чем в Packet Tracer отличается режим симуляции от режима реального времени?
- 7.14 Какие исследования и как их можно выполнить в режиме симуляции?
- 7.15 За счет чего сеть можно разделить на подсети и чем они отличаются между собой?
- 7.16 Чем маршрутизатор отличается от сетевого коммутатора?

### Библиографический список

1. Создание простой сети с помощью Packet Tracer. [https://itmarathon.educom.ru/pdf/admin/Сети\(тренировка2\).pdf](https://itmarathon.educom.ru/pdf/admin/Сети(тренировка2).pdf) (дата обращения: 26.04.2021).  
Дибров М.В. Сети и телекоммуникации. Маршрутизация в IP-сетях. В 2 ч. Часть 2: учебник и практикум для академического бакалавриата / М.В. Дибров. – М.: Изд-во Юрайт, 2019. – 351 с. <https://biblio-online.ru/book/seti-i-telekommunikacii-marshrutizaciya-v-ip-setyah-v-2-ch-chast-2-437865> (дата обращения: 26.04.2021).
2. Сети и телекоммуникации: учебник и практикум для академического бакалавриата / Под ред. К.Е. Самуйлова, И.А. Шалимова, Д.С. Кулябова. – М.: Изд-во Юрайт, 2016. – 363 с. <https://biblio-online.ru/book/seti-i-telekommunikacii-432824> (дата обращения: 26.04.2021).
3. Чернега В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. — Севастополь: Изд-во СевНТУ, 2006. — 500 с.