

ИВАН ТРЕЩЕВ

Сети и телекоммуникации

ДЛЯ СТУДЕНТОВ

Иван Трещев

**Сети и телекоммуникации.
Для студентов**

«Издательские решения»

Трещев И.

Сети и телекоммуникации. Для студентов / И. Трещев —
«Издательские решения»,

ISBN 978-5-44-939742-3

В данной книге сделана попытка обобщить материал по дисциплинам «Сети и телекоммуникации», «Безопасность сетей ЭВМ», «Информационная безопасность распределенных информационных систем», проводимых на базе кафедры в течении 5 лет. Наши выпускники положительно отзываются о наличии в учебном плане группы дисциплин, связанных с сетями и телекоммуникациями и в качестве предложений высказывают пожелание увеличить их долю в учебном плане.

ISBN 978-5-44-939742-3

© Трещев И.
© Издательские решения

Содержание

Введение	6
1 ВВЕДЕНИЕ В СЕТЕВЫЕ ТЕХНОЛОГИИ	7
1.1 Основные определения	7
1.2 Виды сетей	9
1.3 Надежность сетей	10
1.4 Коммуникация и протоколы	11
1.5 Введение в эталонную модель сети	13
1.6 Модель стека TCP/IP	14
1.7 Сегментация и инкапсуляция данных	16
1.8 Передача данных в сети	17
2 Модель стека TCP/IP	20
2.1 Физический (первый) уровень	20
2.1.1 Описание и характеристика	21
2.1.2 Среды передачи данных	22
2.2 Канальный (второй) уровень	25
2.2.1 Описание и характеристика	26
2.2.2 Виды топологий	27
Конец ознакомительного фрагмента.	28

Сети и телекоммуникации Для студентов

Иван Трещев

Специалист по сетям и телекоммуникациям Семен Васильевич Евсеев

Разработка сетевых инфраструктур, сбор материалов Андрей Игоревич Рыжков

© Иван Трещев, 2018

ISBN 978-5-4493-9742-3

Создано в интеллектуальной издательской системе Ridero

Введение

Ни одно современное предприятие не обходится без использования технологий сетевого обмена включая телефонию, передачу данных, видеоконференцсвязь и других. Каждое предприятие сегодня обязательно подключено к сети интернет- аптеки для передачи данных о кассовых чеках, учебные заведения для передачи данных об обучающихся, магазины для связи с налоговой, министерства и ведомства подключены к системе межведомственного электронного взаимодействия и так далее.

Практически у каждого читателя дома установлено и настроено оборудование для беспроводного доступа к сети общего информационного обмена, либо к локальной вычислительной сети.

Знания в области обеспечения сетевого взаимодействия необходимы для любого специалиста по информационным технологиям и являются обязательным условием выполнения должностных обязанностей практически по любой профессии связанной с ЭВМ сегодня.

Отдельно оговоримся, что программирование для сетевых технологий (для сетей глобального и локального информационного обмена, а так же для пассивного и активного сетевого оборудования, описание имеющегося на рынке оборудования) выходит за рамки данной книги и может быть рассмотрено отдельно.

Мы заострим внимание именно на сетевом взаимодействии и обеспечении функционирования сетей. Основные теоретические сведения об оборудовании и терминологии используемых в работе приведены вначале.

1 ВВЕДЕНИЕ В СЕТЕВЫЕ ТЕХНОЛОГИИ

1.1 Основные определения

Сеть передачи данных – совокупность трёх и более оконечных устройств связи, объединённых каналами передачи данных и коммутирующими устройствами (узлами сети), обеспечивающими обмен сообщениями между всеми оконечными устройствами.

Передача данных – физический перенос данных в виде сигналов от точки к точке или от точки к нескольким точкам средствами связи по каналу передачи данных. Примерами подобных каналов могут служить медные провода, волокно-оптические линии связи, беспроводные каналы передачи.

Сетевая инфраструктура включает в себя три категории компонентов сети:

1. Устройства;
2. Среда передачи;
3. Сервисы.

Устройства и среды передачи – это физические элементы или аппаратное обеспечение сети. Аппаратное обеспечение зачастую является видимой частью сетевой платформы: ноутбук, ПК, коммутатор, маршрутизатор, беспроводная точка доступа или кабели, используемые для соединения устройств.

Оконечное устройство является либо отправителем (источником), либо получателем (адресатом) сообщения. Каждому оконечному устройству в сети назначается адрес, чтобы устройства можно было отличить от других. Если оконечное устройство инициирует обмен данными, то в качестве получателя сообщения оно использует адрес оконечного устройства назначения.

Примерами оконечных устройств могут служить:

1. Настольные персональные компьютеры;
2. Ноутбук;
3. Принтер;
4. IP-телефон;
5. Беспроводной планшетный компьютер;
6. Смартфон.

Промежуточные устройства соединяют отдельные оконечные устройства с сетью и могут соединять несколько отдельных сетей для создания глобальных сетей. Такие устройства обеспечивают подключение и прохождение потоков данных по сети. Для определения пути передачи сообщения промежуточные устройства используют адрес оконечного устройства назначения в сочетании с информацией о связях в сети.

Примерами промежуточных устройств могут служить:

1. Коммутатор;
2. Маршрутизатор;
3. Межсетевой экран;
4. Репитер.

Среда передачи данных – физический канал, по которому сообщение передается от источника к адресату.

Типы физических сред передачи данных:

1. Медный кабель;
2. Оптоволоконный кабель;
3. Беспроводная связь.

Сетевая топология – граф, вершинами которого являются оконечные и промежуточные устройства, а ребрами – физические и информационные связи между вершинами. Схема обеспечивает наглядный способ понимания, каким образом устройства в большой сети связаны между собой. Подразделяется на несколько типов:

1. **Физическая топология** – отображает физическое расположение промежуточных устройств и кабельных линий;
 2. **Логическая топология** – отображает устройства, порты и схемы адресации.
- Изображения топологий приведены на рисунках 1 и 2.

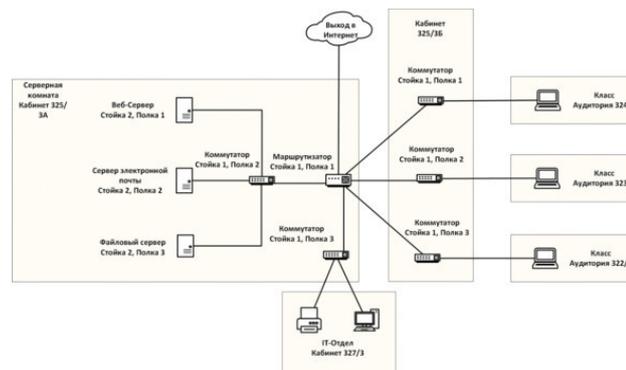


Рисунок 1 – Пример физической топологии

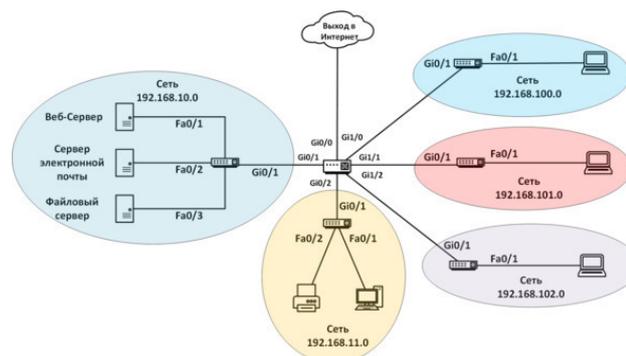


Рисунок 2 – Пример логической топологии

Сетевая карта – устройство, позволяющее взаимодействовать с другими устройствами в сети.

Физический порт – разъем на сетевом устройстве, через который кабели подключены к компьютеру или другому сетевому устройству.

Интерфейс – специализированные порты в сетевом устройстве, которые подключаются к отдельным сетям. Поскольку маршрутизаторы соединяют между собой сети, порты маршрутизатора называются сетевыми интерфейсами.

Часто на практике слова «Порт» и «Интерфейс» являются взаимозаменяемыми.

1.2 Виды сетей

Сети сильно отличаются по площади покрытия, количеству пользователей, типа и объема предоставляемых услуг пользователям. Наиболее распространенными типами сетевых инфраструктур являются локальные сети LAN и глобальные сети WAN.

Локальная сеть (LAN) – сетевая инфраструктура, предоставляющая высокоскоростной доступ пользователям и оконечным устройствам на небольшой территории. Обычно является домашней сетью, сетью малого или крупного предприятия. Управляется одним квалифицированным лицом или отдельным IT-отделом на предприятии.

Глобальная сеть (WAN) – сетевая инфраструктура, предоставляющая доступ к другим сетям на большой территории. Принадлежит провайдеру телекоммуникационных услуг и находится под их управлением.

Интернет – всемирное объединение взаимосвязанных сетей для хранения и передачи информации.

Экстранет – защищённая от несанкционированного доступа корпоративная сеть, использующая Интернет-технологии для внутрикорпоративных целей, а также для предоставления части корпоративной информации и корпоративных приложений деловым партнерам компании.

Интранет – частные сети LAN и WAN, которые принадлежат организации и доступны только ее членам, сотрудникам и прочим авторизованным лицам.

Для сети Экстранет особенно важны аутентификация пользователя (который может и не являться сотрудником компании) и, особенно, защита от несанкционированного доступа, тогда как для приложений Интранет они играют гораздо менее существенную роль, поскольку доступ к этой сети ограничен физическими рамками компании.

Для доступа к Интернет существует множество способов подключения. Домашние пользователи, удаленные сотрудники компаний и малые офисы, как правило, для доступа в Интернет нуждаются в подключении к поставщикам услуг Интернета. Варианты подключения существенно меняются в зависимости от провайдера, географического местоположения и развития инфраструктуры. Популярные варианты включают в себя широкополосную кабельную сеть, широкополосную цифровую абонентскую линию (DSL), беспроводные глобальные сети и мобильные сервисы.

1.3 Надежность сетей

Для поддержания работоспособности и надежности сети требуется, чтобы она соответствовала четырем основным требованиям:

1. Отказоустойчивости;
2. Масштабируемость;
3. Качество обслуживания;
4. Безопасность.

Отказоустойчивость – свойство сети сохранять свою работоспособность после отказа одного или нескольких составных компонентов. Для этого сети используют несколько путей передачи данных от источника к месту назначения. Если один путь недоступен, сообщения можно немедленно отправить по другой линии связи. Наличие нескольких путей к месту назначения называется резервированием.

Масштабируемость – свойство сети, позволяющая быстро расширить, обеспечив поддержку новых пользователей и приложений без снижения эффективности обслуживания существующих.

Качество обслуживания (QoS – Quality of Service) – технология предоставления различным классам трафика различных приоритетов в обслуживании во избежание перегрузки сети.

Обеспечение **безопасности** инфраструктуры сети включает в себя физическую защиту всех устройств, которые необходимы для сетевых подключений, и предотвращение несанкционированного доступа к установленному на них ПО управления.

Безопасность информации означает защиту пакетов данных, передаваемых по сети, а также информации, хранящейся на подключенных к сети устройствах.

Критерии безопасности:

1. Конфиденциальность – только указанные и авторизованные получатели могут иметь доступ к данным;
2. Целостность – гарантия того, что информация не была изменена в процессе передачи от исходного пункта к месту назначения;
3. Доступность – своевременный и надежный доступ к данным для авторизованных пользователей.

1.4 Коммуникация и протоколы

Коммуникация – тип взаимодействия между объектами, который подразумевает обмен информацией между этими объектами. Все способы коммуникаций имеют три общих элемента. Первый – это источник сообщения, или отправитель. Второй элемент – это адресат, или получатель сообщения. Адресат получает и интерпретирует сообщение. Третий элемент, называемый каналом, представляет собой среду передачи данных, по которой сообщение передается от источника к получателю.

В сетях существует несколько способов передачи данных:

1. Индивидуальная (Unicast);
2. Групповая (Multicast);
3. Широковещательная (Broadcast).

Unicast подразумевает собой передачу данных одному единственному адресату в сети. При передаче данных способом **Multicast** данные получают одновременно несколько адресатов в сети. **Broadcast** означает, что данные получают все узлы в сети за исключением того, кто информацию и передает.

Сетевые протоколы определяют общий формат и набор правил для обмена сообщениями между устройствами.

Набор протоколов представляет собой множество протоколов, которые используются вместе для предоставления комплексных сетевых сервисов. Набор протоколов может быть определен организацией по стандартизации или разработан производителем сетевого оборудования.

К примеру, набор протоколов TCP/IP является открытым стандартом. Данные протоколы находятся в свободном доступе, и любой разработчик может использовать эти протоколы в аппаратном или программном обеспечении. Каждый стандартный протокол принят отраслевыми компаниями и утвержден организацией по стандартизации. Использование стандартов в разработке и реализации протоколов гарантирует, что продукты от разных производителей будут успешно взаимодействовать между собой.

Открытые стандарты способствуют совместимости, конкуренции и инновациям. Кроме того, они гарантируют, что продукт отдельной компании не сможет монополизировать рынок или получить несправедливое преимущество по сравнению с конкурентами. Пример – покупка беспроводного маршрутизатора для дома. Существует множество вариантов маршрутизаторов различных производителей, каждый из которых включает стандартные протоколы, такие как IPv4, DHCP, 802.3 (Ethernet) и 802.11 (беспроводная сеть LAN). Открытые стандарты также позволяют клиенту с операционной системой OS X от компании Apple загрузить веб-страницу с веб-сервера под управлением GNU/Linux. Это связано с тем, что обе операционные системы используют протоколы открытых стандартов, например из набора протоколов TCP/IP.

Организации по стандартизации обычно являются независимыми от поставщиков некоммерческими организациями, созданными для разработки и продвижения концепции открытых стандартов.

Некоторые протоколы являются **проприетарными**. Это означает, что описание протокола и принципы его работы определяются одной конкретной компанией или поставщиком. Примерами частных протоколов являются устаревшие наборы протоколов AppleTalk и Novell Netware. Нередко поставщик (или группа поставщиков) разрабатывает частный протокол для удовлетворения потребностей своих заказчиков, а затем способствует принятию этого частного протокола в качестве открытого стандарта.

Примеры различных протоколов различных компаний продемонстрированы на рисунке 3.

Название уровня	TCP/IP	ISO
Уровень приложений	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE
Транспортный уровень	TCP UDP	TP0 TP1 TP2 TP3 TP4
Межсетевой уровень	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS
Уровень доступа к сети	Ethernet PPP Frame Relay ATM WLAN	

Рисунок 3 – Примеры сетевых протоколов и их расположение на различных уровнях стека TCP/IP

1.5 Введение в эталонную модель сети

Чтобы представить взаимодействие между различными протоколами, принято использовать многоуровневые модели. Многоуровневая модель изображает работу протоколов, происходящую внутри каждого уровня, а также взаимодействие с уровнями выше и ниже.

Есть ряд преимуществ в использовании многоуровневой модели для описания сетевых протоколов и операций. Преимущества в использовании многоуровневой модели:

1. Упрощение разработки протоколов, поскольку протоколы, работающие на определенном уровне, определяют формат обрабатываемых данных и интерфейс верхних и нижних уровней;
2. Стимулирование конкуренции, так как продукты разных поставщиков могут взаимодействовать друг с другом;
3. Предотвращение влияния изменений технологий или функций одного уровня на другие уровни (верхние и нижние);
4. Общий язык для описания функций сетевого взаимодействия.

Эталонная модель OSI определяет широкий список функций и сервисов, реализуемых на каждом уровне. Кроме того, она описывает взаимодействие каждого уровня с вышестоящими и нижестоящими уровнями. Всего модель насчитывает семь уровней. На рисунке 4 представлен стек модели OSI с указанием единицы данных, с которым работает каждый из уровней.

Уровень сети модели OSI	Единица данных
7. Прикладной	Данные
6. Представления	
5. Сеансовый	
4. Транспортный	Сегменты
3. Сетевой	Пакеты
2. Канальный	Кадры
1. Физический	Биты

Рисунок 4 – Эталонная модель стека OSI

Описание каждого уровня:

7. *Прикладной уровень* содержит протоколы для обмена данными между приложениями;
6. *Уровень представления* обеспечивает общее представление данных, передаваемых между службами прикладного уровня;
5. *Сеансовый уровень* передает сервисы на уровень представления для организации его диалога и управления обмена данными;
4. *Транспортный уровень* определяет сервисы для сегментации, передачи и сборки данных для отдельных коммуникаций между оконечными устройствами;
3. *Сетевой уровень* представляет функции для обмена отдельными частями данных по сети между указанными оконечными устройствами;
2. Протоколы *канального уровня* описывают способы обмена кадрами данных при обмене данными между устройствами по общей среде передачи данных;
1. Протоколы *физического уровня* описывают электрические, механические, функциональные и процедурные средства для активации, поддержки, деактивации физического соединения, обеспечивающего передачу битов из одного сетевого устройства в другое.

1.6 Модель стека TCP/IP

Протокольная модель сетевого взаимодействия TCP/IP была создана в начале 70-х годов и иногда называется моделью сети Интернет. Как показано на рисунке 5, такая модель определяет четыре категории функций, необходимых для успешного взаимодействия. Архитектура набора протоколов TCP/IP построена на основе этой модели. TCP/IP представляет собой открытый стандарт, ни одна компания не вправе контролировать ее определение.

Уровень сети модели TCP/IP	Единица данных
Приложений (прикладной)	Данные
Транспортный	Сегменты
Сетевой	Пакеты
Уровень сетевого доступа	Кадры
	Биты

Рисунок 5 – Модель стека TCP/IP

Описание каждого уровня:

1. *Уровень приложений* отображает данные для пользователя, а также обеспечивает кодирование и управление сеансами связи;
2. *Транспортный уровень* поддерживает связь между различными устройствами в разных сетях;
3. *Межсетевой уровень* определяет наилучший пути через сеть;
4. *Уровень сетевого доступа* управляет устройствами и средами передачи данных, из которых состоит сеть.

Следует отметить, что различные авторы интерпретировали модель TCP/IP по-разному и не согласны с тем, что уровень связи или вся модель TCP/IP охватывает проблемы уровня OSI уровня 1 (физический уровень) или предполагается, что аппаратный уровень ниже уровня канала. Несколько авторов попытались включить слои 1 и 2 модели OSI в модель TCP/IP, поскольку они обычно упоминаются в современных стандартах.

Набор протоколов TCP/IP может быть описан с точки зрения эталонной модели OSI. В модели OSI уровень доступа к сети и уровень приложений модели TCP/IP дополнительно подразделяются для описания отдельных функций, которые реализуются на этих уровнях. На рисунке 6 показано сопоставление моделей OSI и TCP/IP.

Модель OSI	Модель TCP/IP
7. Прикладной	Приложений (прикладной)
6. Представления	
5. Сеансовый	
4. Транспортный	Транспортный
3. Сетевой	Сетевой
2. Канальный	Уровень сетевого доступа
1. Физический	

Рисунок 6 – Сопоставление моделей OSI и TCP/IP

На уровне доступа к сети набор протоколов TCP/IP не определяет список протоколов, используемых при работе со средой передачи данных, он описывает только передачу информации с сетевого уровня физическим сетевым протоколам. Уровни 1 и 2 модели OSI описывают процедуры доступа к среде передачи и физическим способам отправки данных по сети.

Уровень 3 модели OSI, или сетевой уровень, соответствует сетевому уровню модели TCP/IP. Этот уровень описывает протоколы, определяющие пути передачи данных в сети.

Уровень 4 модели OSI, или транспортный уровень, соответствует транспортному уровню модели TCP/IP. Этот уровень описывает общие сервисы и функции, которые обеспечивают упорядоченную и надежную доставку данных от источника до места назначения.

Уровень приложений TCP/IP включает в себя ряд протоколов, которые поддерживают определенные функции для работы разнообразных приложений конечных пользователей. Уровни 5, 6 и 7 модели OSI используются в качестве образцов разработчиками и поставщиками прикладного программного обеспечения для производства продуктов, предназначенных для работы в сети.

Обе модели (TCP/IP и OSI) широко применяются в отношении протоколов различных уровней. Так как модель OSI разделяет канальный и физический уровни, именно она используется для этих уровней.

1.7 Сегментация и инкапсуляция данных

Для обеспечения надежности и бесперебойности передачи данных, уменьшения задержек используется разделение сообщения на несколько частей – **сегментация**.

Данный процесс имеет несколько преимуществ:

1. Отправка небольших отдельных частей от источника к получателю в сети позволяет поддерживать множество различных чередующихся сеансов обмена сообщениями. Это называется **мультиплексированием**;

2. Сегментация позволяет повысить надежность сетевого взаимодействия. Если какую-либо часть сообщения не удастся доставить к месту назначения из-за отказа сети, необходимо будет повторно передать только недостающие части сообщения.

Инкапсуляция – процесс добавления различной информации протоколами на каждом из уровней стека модели OSI во время прохождения через среду передачи информации. Форма, которую принимает массив данных на каждом из уровней, называется единицей данных протокола (PDU). В ходе инкапсуляции каждый последующий уровень инкапсулирует PDU, полученную от вышестоящего уровня в соответствии с используемым протоколом. На каждом этапе процесса PDU получает другое имя, отражающее новые функции.

Ранее на рисунке 5 уже были продемонстрированы наименования PDU.

Деинкапсуляция – это процесс удаления одного или нескольких заголовков принимающим устройством. По мере продвижения данных по стеку к приложениям для конечных пользователей они деинкапсулируются.

1.8 Передача данных в сети

Сетевой (третий) и канальный (второй) уровни отвечают за доставку данных с устройства-источника на устройство назначения. Как показано на рисунке 7, протоколы на обоих уровнях содержат адреса источника и назначения, но эти адреса служат разным целям

Физический уровень	Канальный уровень	Сетевой уровень	Транспортный уровень	Верхние уровни
Биты временных параметров и синхронизации	Физические адреса назначения и источника	Логические сетевые адреса назначения и источника	Номера процессов (портов) назначения и источника	Кодирование данных приложений

Рисунок 7 – Виды адресов источника и назначения на разных уровнях TCP/IP

1. Адреса источника и назначения сетевого уровня необходимы для доставки IP-пакета от источника к месту назначения в той же или в удаленной сети;
2. Адреса источника и назначения канального уровня необходимы для доставки кадра канала данных от одной сетевой карты к другой в той же сети.

IP-адрес – это логический адрес сетевого уровня (третьего уровня), необходимый для доставки IP-пакета от источника к месту назначения.

IP-пакет содержит два IP-адреса (рисунок 8):

1. **IP-адрес источника** – IP-адрес устройства-отправителя, изначального источника пакета;
2. **IP-адрес назначения** – IP-адрес устройства-получателя, конечного места назначения пакета.

IP-адрес источника 192.168.1.110	IP-адрес назначения 172.16.1.99
----------------------------------	---------------------------------

Рисунок 8 – Расположение адресов источника и назначения в IP-пакете третьего уровня

IP-адрес состоит из двух частей:

1. **Сетевая часть** – левая часть адреса, которая показывает, к какой сети относится данный IP-адрес. Абсолютно все устройства из одной и той же сети будут иметь одинаковую сетевую часть. Определяется с помощью **маски подсети** – битовой маски для определения по IP-адреса сети и адреса узла этой подсети, которая не является частью IP-пакета;

2. **Узловая часть** – оставшаяся часть адреса, определяющее конкретное устройство в сети и является уникальной для каждого узла в сети.

MAC-адреса (или **Физический адрес**) – это уникальный адрес канального (второго) уровня сетевого интерфейса (обычно сетевой карты) для реализации коммуникации устройств в сети.

Назначение **адреса канального уровня** – доставить кадр с одного сетевого интерфейса на другой, когда они находятся в одной и той же сети.

Заголовок кадра канального уровня (рисунок 9) содержит следующие физические (MAC-адреса):

1. **Адрес источника канального уровня** – физический адрес (MAC-адрес) сетевой карты устройства, которое передает пакет;

2. **Адрес назначения канального уровня** – физический адрес (MAC-адрес) сетевой карты устройства, которое получает пакет. Это адрес ближайшего маршрутизатора или устройства назначения.

Заголовок кадра Ethernet		Заголовок IP-пакета	
MAC-адрес назначения	MAC-адрес отправителя	IP-адрес отправителя	IP-адрес назначения

Рисунок 9 – Расположение адресов в кадре канального уровня

Рассмотрим обмен данными с помощью устройств в одной сети и с помощью устройств в разных сетях.

Посмотрим на рисунок 10. В сети находятся компьютер пользователя и FTP-сервер, с которым будет взаимодействовать компьютер. Компьютер пользователя – это устройство-отправитель, FTP-сервер – устройство-получатель. Получаем:

1. IP-адрес источника: **192.168.1.110**;
2. IP-адрес получателя: **192.168.1.9**.

Обратите внимание на левую выделенную часть каждого IP-адреса – это и есть сетевая часть адреса, которая остается неизменной (в том случае если маска подсети 255.255.255.0).

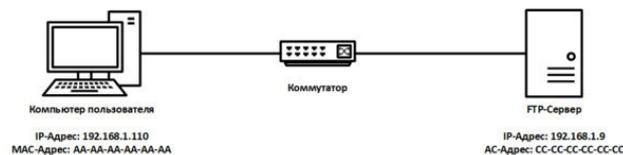


Рисунок 10 – Устройства находятся в одной сети

Так как и отправитель, и получатель находятся в одной сети, кадр отправляется напрямую принимающему устройству.

1. MAC-адрес источника (сетевой карты Компьютера пользователя): AA-AA-AA-AA-AA-AA в шестнадцатеричном представлении.
2. MAC-адресом получателя (FTP-сервера) является MAC-адрес FTP-сервера: CC-CC-CC-CC-CC-CC в шестнадцатеричном представлении.

Таким образом, кадр канального уровня будет выглядеть как на рисунке 11.

Канальный уровень. Заголовок кадра Ethernet		Сетевой уровень. Заголовок IP-адреса		...	Данные
MAC-адрес назначения	MAC-адрес отправителя	IP-адрес отправителя	IP-адрес назначения		
CC-CC-CC-CC-CC-CC	AA-AA-AA-AA-AA-AA	192.168.1.110	192.168.1.9		

Рисунок 11 – Кадр с инкапсулированным IP-пакетом, передающийся напрямую с Компьютера пользователя на FTP-сервер

Теперь рассмотрим ситуацию, когда устройство-отправитель и устройство-получатель находятся в разных сетях. Пример топологии представлен на рисунке 12.

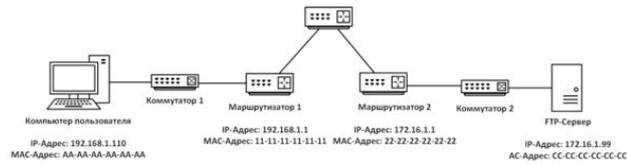


Рисунок 12 – Устройства находятся в разных сетях

Отправитель и получатель пакета находятся в разных сетях, значит IP-адреса источника и назначения будут представлять узлы в разных сетях. На это будет указывать сетевая часть IP-адреса узла назначения.

1. IP-адрес источника: **192.168.1.110**;
2. IP-адрес назначения: **172.16.1.99**.

Если устройства находятся в разных сетях, то и сетевые части адресов устройств будут разными.

Из-за того, что отправитель и получатель IP-пакета находятся в разных сетях, кадр Ethernet не может быть отправлен напрямую к узлу назначения, поскольку он недоступен в сети отправителя. Кадр Ethernet нужно выслать на другое устройство: маршрутизатор или шлюз по умолчанию. В нашем примере шлюз по умолчанию – Маршрутизатор 1.

1. MAC-адрес источника (сетевой карты Компьютера пользователя): AA-AA-AA-AA-AA-AA в шестнадцатеричном представлении.

2. MAC-адрес назначения – устройство-отправитель использует MAC-адрес шлюза по умолчанию или маршрутизатора, если получающее и передающее устройства находятся в разных сетях. В этом примере MAC-адресом назначения является MAC-адрес интерфейса Ethernet Маршрутизатора 1 (11-11-11-11-11-11). Этот интерфейс прикреплен к той же сети, что и Компьютер пользователя.

Таким образом, кадр канального уровня будет выглядеть как на рисунке 13.

Канальный уровень. Заголовок кадра Ethernet		Сетевой уровень. Заголовок IP-адреса		...	Данные
MAC-адрес назначения	MAC-адрес отправителя	IP-адрес отправителя	IP-адрес назначения		
11-11-11-11-11-11	AA-AA-AA-AA-AA-AA	192.168.1.110	172.16.1.99		

Рисунок 13 – Кадр с инкапсулированным IP-пакетом, передающийся на FTP-сервер, находящийся в другой сети

2 Модель стека TCP/IP

2.1 Физический (первый) уровень

2.1.1 Описание и характеристика

Физический уровень – первый уровень сетевой модели OSI. Это нижний уровень модели OSI – физическая и электрическая среда для передачи данных. Физический уровень описывает способы передачи бит (а не пакетов данных) через физические среды линий связи, соединяющие сетевые устройства. На этом уровне описываются параметры сигналов, такие как амплитуда, частота, фаза, используемая модуляция, манипуляция. Решаются вопросы, связанные с синхронизацией, избавлением от помех, скорости передачи данных.

Физический уровень состоит из электронных схем, сред передачи данных и разъемов, разрабатываемых инженерами.

Стандарты физического уровня регламентируют три функциональные области:

1. Физические компоненты;
2. Кодирование;
3. Способы передачи сигналов.

Физические компоненты – это электронные устройства, среды передачи данных, а также другие соединители и разъемы, обеспечивающие передачу сигналов, с помощью которых представлены биты информации. Все аппаратные компоненты, в том числе сетевые карты, интерфейсы и соединители, а также материалы и конструкция кабелей описаны в стандартах, относящихся к физическому уровню.

Кодирование – это способ преобразования потока битов в определенный «код». Коды – это группы битов, используемые для формирования предсказуемых комбинаций, которые могут распознаваться как отправителем, так и получателем. В сети под кодированием понимаются изменения напряжения или тока согласно заданным правилам с целью представления значений битов: нулей и единиц. Пример изображен на рисунке 14.

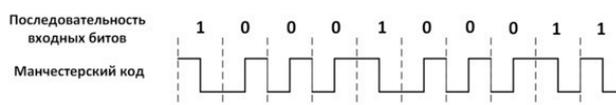


Рисунок 14 – Пример манчестерского кода, при котором происходит кодировка информации

Способы передачи сигналов. Для представления значений битов «1» и «0» в среде подключения физический уровень должен генерировать электрические, оптические или радиосигналы. Метод представления битов с помощью сигналов называется способом передачи сигналов. Стандарты физического уровня должны определять, какой тип сигнала соответствует единице («1»), а какой нулю («0»). Для передачи сигнала можно использовать простое изменение длительности электрического или оптического импульса. Например, длинный импульс может обозначать 1, а короткий – 0.

Основными характеристиками передачи данных являются **пропускная способность** и **производительность**.

Пропускная способность – объем данных, который можно передать из одной точки в другую за определенное время. Обычно пропускная способность измеряется в килобитах в секунду (Кбит/с), мегабитах в секунду (Мбит/с) или гигабитах в секунду (Гбит/с).

Производительность – это количество битов, передаваемых по средам передачи данных за определенный период времени.

2.1.2 Среды передачи данных

Типы физических сред передачи данных:

1. Медный кабель;
2. Оптоволоконный кабель;
3. Беспроводная связь.

Медные кабели используются в сетях из-за их невысокой стоимости, простоты монтажа и низкого электрического сопротивления. Однако при передаче сигналов по медным кабелям имеются ограничения по дальности передачи и помехоустойчивости. Данные по медным кабелям передаются в виде электрических импульсов.

Виды медных кабелей:

1. Неэкранированная витая пара (UTP);
2. Экранированная витая пара (STP);
3. Коаксиальный кабель.

Медные кабели могут быть подвержены воздействиям различных помех: электромагнитным и радиочастотным, источником которых могут быть излучения от электромагнитных устройств, а так перекрестные помехи, создающиеся из-за прохождения тока через круговое магнитное поле по проводу, которое воздействует на соседний провод.

Для обеспечения защиты от электромагнитных и радиочастотных помех кабели могут быть обернуты экранирующей оболочкой, что используется в экранируемой витой паре. Для защиты от перекрестных помех соседние кабели скручиваются между собой, причем все четыре пары скрученных кабелей имеют разное число витков, благодаря чему влияние излучение от других пар уменьшается. Используется в экранируемой и в неэкранированной витой паре.

В данных видах кабелей используется штекер 8P8C стандарта RJ-45 (рисунок 15).



Рисунок 15 – Штекер 8P8C стандарта RJ-45

Существует два варианта обжима разъёма на кабеле:

1. Прямой кабель используется для соединения сетевой карты узла к коммутатору или коммутатора с маршрутизатором;

2. Перекрестный или кроссовый кабель используется для соединения двух однотипных устройств между собой (коммутатор с коммутатором, маршрутизатор с маршрутизатором), а также для соединения двух узлов в сети.

Обжим проводится по двум стандартам: EIA/TIA 568A и EIA/TIA 568B (рисунок 16). Причем для прямого кабеля оба конца должны быть одинаковыми (оба или 568A, или 568B), а для перекрестного разными (один конец – 568A, другой – 568B).

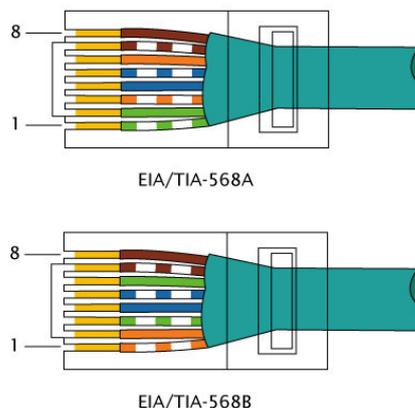


Рисунок 16 – Варианты обжима кабеля¹

Последовательность проводов для EIA/TIA 568A и 568B представлена на рисунке 17.

EIA/TIA-568A	EIA/TIA-568B
1. Бело-зеленый	1. Бело-оранжевый
2. Зеленый	2. Оранжевый
3. Бело-оранжевый	3. Бело-зеленый
4. Синий	4. Синий
5. Бело-синий	5. Бело-синий
6. Оранжевый	6. Зеленый
7. Бело-коричневый	7. Бело-коричневый
8. Коричневый	8. Коричневый

Рисунок 17 – Последовательность проводов

Так же следует отметить медный **консольный кабель**, который соединяет компьютер с маршрутизатором или коммутатором через консольный порт для дальнейшей настройки устройства. Он, как правило, отличается своей плоской формой и синим цветом.

Коаксиальный кабель – электрический кабель, состоящий из центрального проводника и экрана, расположенных соосно и разделённых изоляционным материалом или воздушным промежутком. Коаксиальный кабель использовался в сети Ethernet с самого начала. В настоящее время он не столь широко распространен, хотя и обеспечивает максимальную протяженность сети с топологией типа «шина», которая так же является устаревшей.

Опволоконные кабели позволяют передавать данные на большие расстояния и с более высокой пропускной способностью, чем другие среды передачи. Такой кабель также абсолютно невосприимчив к воздействию электромагнитных и радиочастотных помех. Оптические кабели обычно используются для соединения сетевых устройств друг с другом. Для передачи по опволоконному кабелю биты кодируются с помощью световых импульсов.

Опволоконные кабели подразделяются на два основных типа:

¹ Источник: ru.wikipedia.org/wiki/Витая_пара. Автор: пользователь Lp

1. Одномодовый оптоволоконный кабель. Имеет сердечник очень малого диаметра. Для передачи луча света требуется дорогостоящая лазерная технология. Широко используется для организации линий связи протяженностью несколько сот километров.

2. Многомодовый оптоволоконный кабель. Имеет сердечник большего диаметра. Для передачи световых импульсов используются светодиодные излучатели. Такие кабели популярны в локальных сетях, поскольку позволяют использовать для работы недорогие светодиоды. Обеспечивает пропускную способность до 10 Гбит/с на расстоянии до 550 метров.

В отличие от электрических импульсов, свет по оптоволокну передается только в одном направлении и работы в полнодуплексном режиме требуются два оптоволокна. Поэтому в оптических соединительных кабелях имеется два волокна, на концах каждого из которых смонтированы стандартные одноволоконные разъемы.

Беспроводные среды передачи позволяют передавать двоичные данные, кодируя их в электромагнитные сигналы микроволнового и радиодиапазона.

Беспроводные технологии передачи данных хорошо работают на открытых пространствах, из-за чего подключение к беспроводной сети на относительно дальнем расстоянии будет удобнее, чем проводное соединение. Однако определенные строительные материалы внутри помещений могут ограничивать зону покрытия.

Беспроводная среда гораздо более восприимчива к помехам и может ухудшаться при работе большого количества устройств: сотовые телефоны, микроволновые печи, а также из-за большого количества соседних беспроводных коммуникаций.

Для доступа к среде беспроводного подключения не требуется подключаться к физическим кабелям. Поэтому доступ к этой среде могут получать несанкционированные пользователи и устройства. Для предотвращения несанкционированного доступа требуется обеспечение безопасности администратором сети.

Отметим также, что в каждый момент времени передачу или прием может осуществлять только одно устройство. Среда передачи общая для всех беспроводных пользователей. Чем больше пользователей одновременно подключаются к беспроводной сети, тем меньшая пропускная способность приходится на каждого из них.

2.2 Канальный (второй) уровень

2.2.1 Описание и характеристика

Канальный уровень – второй уровень сетевой модели OSI, предназначенный для передачи данных узлам, находящимся в том же сегменте локальной сети. Может использоваться для обнаружения и исправления ошибок, возникших на физическом уровне при передачи данных. Канальный уровень отправляет пакеты информации протоколу вышестоящего уровня и принимает их от него.

Канальный уровень делится на два подуровня:

1. Верхний подуровень **управления логическим каналом** (LLC – Logical Link Control);

2. Нижний подуровень **управления доступом к среде** (MAC – Media Access Control).

Управление логическим каналом помещает в отправляемый кадр информацию о том, какой протокол сетевого уровня используется для данного кадра. Позволяет протоколом третьего уровня (IPv4 и IPv6) использовать один и тот же сетевой интерфейс и одну и ту же среду передачи данных.

Управление доступом к среде обеспечивает адресацию на канальном уровне, а также обеспечивает доступ к различным сетевым технологиям, в частности взаимодействует с протоколом канального уровня Ethernet, что позволяет передавать и получать информацию через медный или оптоволоконный кабель. Так же MAC взаимодействует с беспроводными технологиями передачи информации.

2.2.2 Виды топологий

Для создания сетей существуют различные способы соединения устройств между собой. Каждый из способов имеет свои достоинства и недостатки. Приведем примеры основных сетевых топологий:

1. Сетевая топология типа **«точка-точка» (Point-to-point)** – простейший вид сетевой топологии, который соединяет между собой устройства с помощью коммуникационного оборудования. Благодаря своей дешевизне является наиболее распространённой топологией, но самой ограниченной: соединить возможно только два устройства между собой (рисунок 18);

2. Топология типа **«шина» (Bus)** – тип топологии, использовавший один коаксиальный кабель в виде среды передачи данных. Данный кабель подключается ко всем оконечным устройствам для создания локальной сети. На концах кабелей находятся терминаторы для предотвращения отражения сигнала. При создании сети не требуется коммутатор или концентратор. К достоинствам можно отнести дешевизну и простоту настройки. Однако, чем больше устройств подключено к шине, тем менее производительной будет сеть. А при повреждении кабеля или одного из терминаторов вся сеть выходит из строя (рисунок 19);

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.