1. **Введение в сети**
   1. Основные понятия

В самом начале нашего курса мы уделим внимание изучению основных понятий, которые являются фундаментом для понимания всей темы в целом. Ознакомление с этими понятиями поможет вам быстрее ориентироваться в дальнейшем материале, упростит восприятие новых знаний и обеспечит прочную основу для усвоения более сложных аспектов курса. Понимание базовых терминов и идей — ключ к успешному освоению курса, поэтому мы рекомендуем уделить этим знаниям особое внимание с самого начала. Такой подход значительно повысит эффективность обучения и сделает процесс более понятным и увлекательным.

Сеть – это совокупность объектов, образуемых устройствами передачи и обработки данных. Сети объединяют различные устройства для обмена информацией. Такие устройства называют узлами сети.

Узел сети — любой активный компонент сети, включающий устройства, такие как компьютеры, маршрутизаторы, коммутаторы, или программные элементы, участвующие в передаче данных. Сетевые устройства, такие как ПК, ноутбуки, смартфоны, принтеры, IP-телефоны и различные серверы, называют оконечными устройствами. Они принимают или отправляют информацию и преобразуют ее в сигналы для передачи по каналам связи и делятся на клиенты и серверы.

Клиент — устройство или программное обеспечение, которое инициирует запросы и получает ресурсы или услуги от сервера. Например, браузер, запрашивающий веб-страницу.

Сервер — устройство или программа, предоставляющая услуги, ресурсы или данные по запросу клиента. Примеры — веб-сервер, файловый сервер, почтовый сервер.

Для соединения оконечных устройств используют промежуточные сетевые устройства. Они могут соединять также и несколько отдельных сетей. Такие устройства делятся на:

* Коммутатор — это сетевое устройство, предназначенное для пересылки кадров в пределах одной сети.
* Маршрутизатор — это сетевое устройство, соединяющее сети и предназначенное для пересылки пакетов из одной сети в другую.
* Точка доступа — это сетевое устройство, которое представляет из себя базовую станцию для создания беспроводной локальной сети, работающей поверх проводной сети или параллельно с ней.
* И другие (сетевой адаптер, модем).

А передача данных происходит в сетевой среде – канале, передающем информацию от отправителя к получателю. Различают три типа сетевой среды:

* Беспроводная среда – данные передаются при помощи электромагнитных волн
* Медный кабель – данные передаются с помощью электрических сигналов
* Оптоволоконный кабель – данные передаются посредством световых импульсов

Протокол – это совокупность правил, устанавливающих формат и процедуры обмена информацией между двумя или несколькими устройствами. На различных этапах обмена информацией могут использоваться специализированные протоколы, которые передают результат работы другим протоколам.

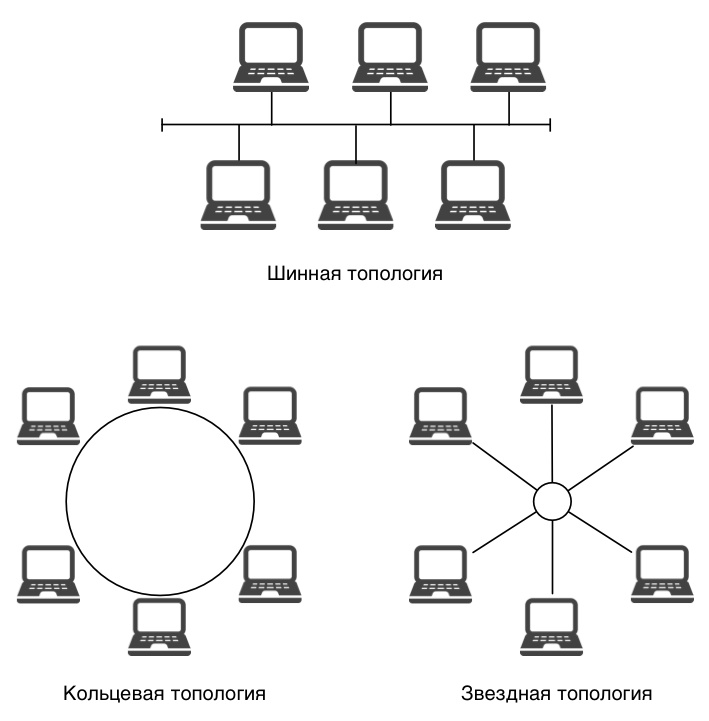
Интерфейс – совокупность средств и методов взаимодействия между элементами или устройствами системы. Интерфейсы могут быть аппаратными или программными. Физический (аппаратный) интерфейс, расположенный на сетевом устройстве, называют портом. Интерфейсы являются основой взаимодействия всех современных информационных систем.

Трафик – это поток сообщений в сети передачи данных. Под ним понимают количественное измерение в выбранных точках сети числа проходящих блоков данных и их длины, выраженное в битах в секунду.

Метод доступа – это способ определения того, как сеть управляет доступом к каналу связи (кабелю), что существенно влияет на ее характеристики. В сети все рабочие станции физически соединены между собою каналами связи по определенной структуре, называемой топологией. Примеры методов доступа:

* CSMA/CD (Carrier Sense Multiple Access with Collision Detection) — используется в беспроводных сетях для обнаружения коллизий (столкновения данных от разных источников в сети).
* CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) — используется проводных сетях для предотвращения коллизий.

Топология – это описание физических соединений в сети, указывающее, какие рабочие станции могут связываться между собой.



Архитектура – это концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети. Она предусматривает логическую, функциональную и физическую организацию технических и программных средств сети. Основные виды сетевой архитектуры:

* Одноранговая — все узлы являются как клиентом, так и сервером.
* Клиент-сервер – узлы делятся на клиентов и сервера.

Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки.

* Конфиденциальность — защита данных от несанкционированного доступа.
* Целостность — обеспечение неизменности данных.
* Доступность — гарантированная возможность доступа к данным пользователям, имеющим на это право.
  1. Эталонные модели

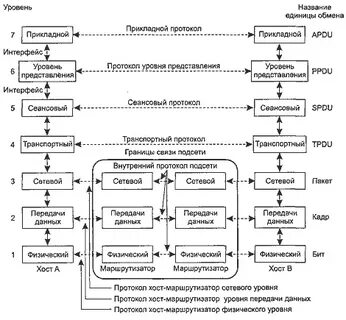
Помимо базовых понятий важно изучить модели, лежащие в основе работы сетей. В рамках курса мы рассмотрим две ключевые модели — OSI и TCP/IP. Они помогают понять структуру и взаимодействие компонентов сети. Освоение этих моделей способствует более глубокому пониманию процессов передачи данных.

1. Эталонная модель OSI:

Модель OSI состоит из 7 уровней, каждый из которых выполняет свою уникальную функцию в процессе передачи данных. Эти уровни представлены на рисунке ниже и разработаны с учётом определённых принципов, что позволяет разделить сложные сетевые процессы на более простые и управляемые части.

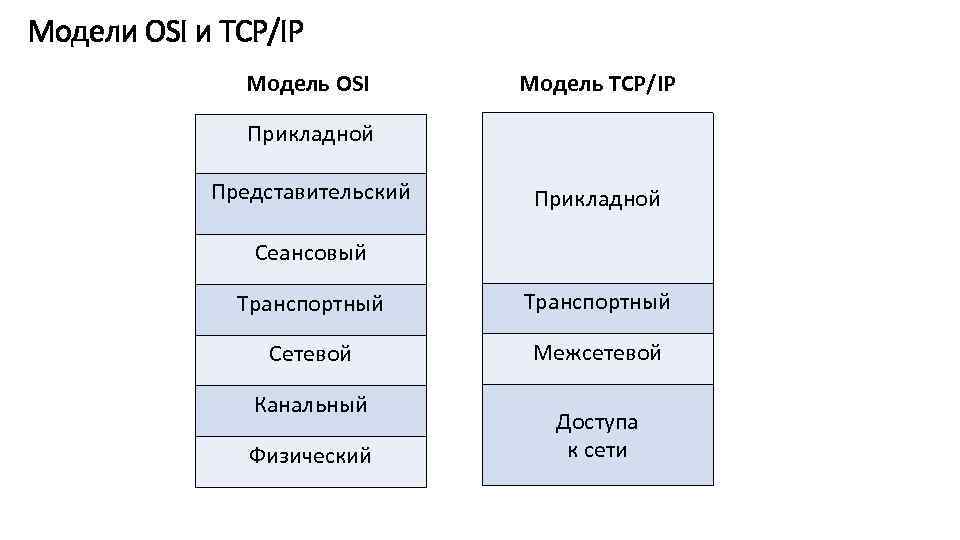
Среди основных принципов выделения уровней:

* Все уровни выполняют четко определенные функции.
* Функция каждого уровня выбирается с учетом создания в дальнейшем международных стандартизированных протоколов.
* Границы уровней должны выбираться так, чтобы минимизировать поток информации через интерфейсы.



1. Эталонная модель TCP/IP:

Модель TCP/IP включает всего четыре уровня, что делает её более упрощённой по сравнению с моделью OSI. При этом некоторые уровни этой модели объединяют функции нескольких уровней из модели OSI, что способствует более гибкому и практическому использованию в реальных сетевых технологиях. Эта модель широко применяется в современных сетевых инфраструктурах и является основой для большинства протоколов интернета



1. Теперь рассмотрим подробнее функции каждого уровня модели OSI.

Физический уровень - определяет метод передачи данных и отвечает за передачу необработанных битов по физической среде (кабели, радиоволны, оптоволокно).

Канальный уровень - отвечает за адресацию в локальной сети (MAC-адреса), а также обнаруживает ошибки и проверяет целостность данных. Обеспечивает передачу кадров данных между соседними узлами сети.

Сетевой уровень - отвечает за маршрутизацию данных между сетями и управление их адресацией. Использует IP-адреса для определения конечного устройства (каждое устройство имеет уникальный сетевой адрес).

Транспортный уровень - обеспечивает надежную передачу данных между приложениями, включая контроль целостности и управление потоком. Делит данные на сегменты и обеспечивает их правильную последовательность при получении. Для указания назначения сегментов используются порты.

Сеансовый уровень - устанавливает, управляет и разрывает соединения между приложениями. Поддерживает сеансы с несколькими пользователями.

Уровень представления (представительский) - отвечает за преобразование данных из одного формата в другой, их шифрование и сжатие. Приводит данные в вид понятный конечному пользователю

Прикладной уровень (уровень приложений) – отвечает за взаимодействие пользователя с приложением.

При передаче данных все уровни проходятся последовательно. Процесс перехода с верхнего на нижний – инкапсуляция. Декапсуляция – с нижнего на верхний. На каждом уровне, как можно было заметить ранее, информация называется по-разному. На прикладном уровне это PDU (Protocol Data Units) или просто данные. На уровне представления к данным добавляется заголовок представления (Например HTTP, DHCP). На транспортном происходит сегментация, соответственно информацию называют сегментом, состоящим из PDU и заголовка транспортного уровня (Например TCP, UDP). Далее на сетевом уровне образуются пакеты – сегмент с заголовком сетевого уровня (Например IPv4, ICMP, IPv6) и на канальном образуется кадр – пакет с заголовком канального уровня (Например WiFi, Ethernet).

Для понимания как это все работает рассмотрим пример процесса инкапсуляции:

Прикладной, представления и сеансовый уровни (PDU)

1. Данные создаются приложением (например, HTTP для веб-страниц).
2. На уровне представления данные приводятся к необходимому формату, который может быть прочитан сетевым устройством, также происходит шифрование данных .
3. На уровне сеанса устанавливается сессия между устройствами.

Транспортный уровень (сегменты)

1. Данные разбиваются на более мелкие блоки — сегменты.
2. Добавляются номера портов отправителя и получателя, чтобы данные могли быть направлены нужному приложению.

Сетевой уровень (пакеты)

1. Добавляются IP-адреса (логические адреса) отправителя и получателя, чтобы данные могли быть доставлены в нужную сеть.

Канальный уровень (кадры)

1. Добавляются физические адреса (MAC-адреса) отправителя и получателя для передачи данных внутри локальной сети.
2. Также добавляется контрольная информация для проверки целостности данных.

Физический уровень (биты)

1. Данные преобразуются в биты и отправляются через физическую среду передачи (кабели, радиоволны и т.п.).

Аналогичным образом происходит процесс декапсуляции, но в обратном порядке.

Также мы упоминали заголовки, добавляемы на каждом уровне. Они служат для обозначения протоколов. Рассмотрим кратко основные из них на каждом уровне:

На уровне прикладном, представления и сеансовом

* DNS - протокол распознавания доменных имен. Сообщает запрашивающему IP- адрес сайта по его имени.
* DHCP - протокол динамической настройки узла. Позволяет оконечному устройству в автоматическом режиме получить IP-адрес.
* HTTP/HTTPS - протоколы передачи гипертекста (нешифрованный и шифрованный соответственно). Передают запросы пользователя Web-серверу и содержимое веб-страниц от сервера в браузер пользователя.

На транспортном уровне:

* ТСР – протокол для надежной доставки данных. Используется для передачи текста, изображений, видео- и музыкальных файлов.
* UDP – протокол для быстрой передачи данных без контроля доставки. Применяется для передачи потокового видео.

На сетевом уровне:

* IPv4, IPV6 - протокол негарантированной доставки IP версии 4 и 6.
* ICMP - протокол контрольных сообщений, используется для проверки связности.

На канальном уровне, физическом:

* ARP - протокол, используемый для определения MAC-адреса устройства по его IP-адресу.
* Ethernet - протокол передачи данных по медному кабелю (коаксиальному или витой паре.
* WiFi - протокол передачи данных по беспроводной среде