



Лекция 2



IT Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™



Открытые стандарты





Протоколы

- **Протокол представляет собой набор правил. Протоколы Интернета — это наборы правил, регулирующие обмен данными между компьютерами в сети. Спецификации протокола определяют формат сообщений, участвующих в обмене.**
- **Основные функции:**
 - **Идентификация и обработка ошибок**
 - **Сжатие данных**
 - **Определение порядка разделения данных и формирования пакетов**
 - **Назначение адресов пакетам данных**
 - **Определение порядка объявления отправки и получения пакетов данных**



Модель OSI

Модель OSI	Уровень	Описание
Уровень приложений	7	Отвечает за предоставление сетевых служб приложениям
Уровень представления	6	Преобразует форматы данных, чтобы обеспечить уровню приложений стандартный интерфейс
Сеансовый уровень	5	Устанавливает и завершает подключения между локальными и удаленными приложениями, а также управляет ими
Транспортный уровень	4	Предоставляет надежный транспорт и управление потоком при передаче данных по сети
Сетевой уровень	3	Отвечает за логическую адресацию и маршрутизацию
Канальный уровень	2	Обеспечивает физическую адресацию и управляет доступом к среде передачи данных
Физический уровень	1	Определяет все электрические и физические требования к устройствам



Модель TCP/IP

Уровень TCP/IP	Описание
Уровень приложений	На нём работают высокоуровневые протоколы, такие как SMTP и FTP
Транспортный уровень	Указывает, какое приложение запросило или получает данные через указанные порты
Уровень Интернет (межсетевой уровень)	На нём происходит IP-адресация и маршрутизация
Уровень доступа к сети	На нём существуют MAC-адресация и физические компоненты сети

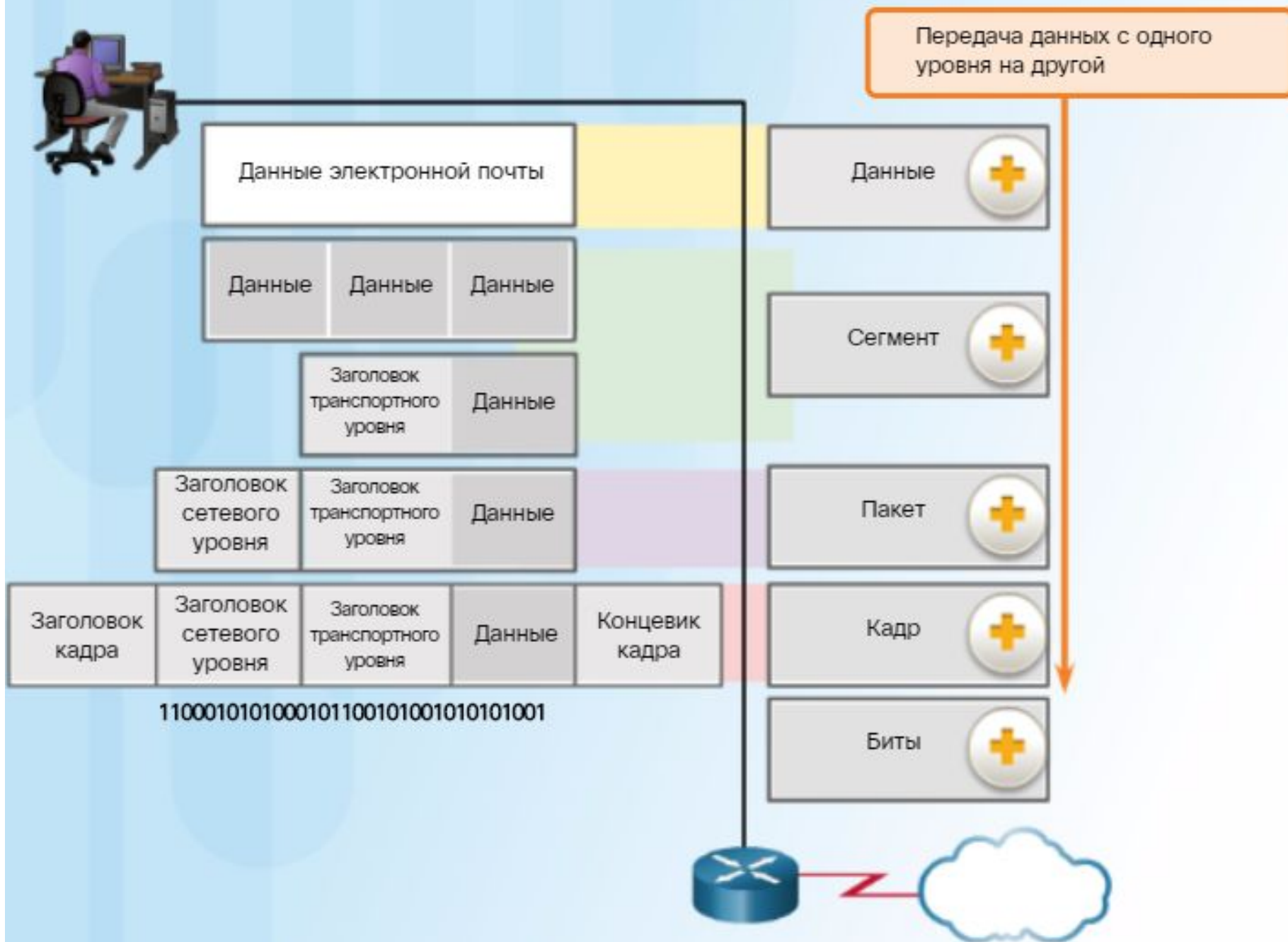
Модель TCP/IP была создана исследователями Министерства обороны США. Она состоит из уровней, выполняющих необходимые функции по подготовке данных для передачи по сети.





Протокольный блок данных (PDU)

- Сообщение начинается с верхнего прикладного уровня и переходит по уровням TCP/IP к нижнему уровню сетевого доступа. **По мере того как данные приложений передаются вниз с одного уровня на другой, на каждом из уровней к ним добавляется информация в соответствии с протоколами. Это называется процессом инкапсуляции.**
- **Форма, которую принимает массив данных на каждом из уровней, называется протокольным блоком данных (PDU).**





- Обратный процесс на принимающем узле называется декапсуляцией. **Декапсуляция — это процесс удаления одного или нескольких заголовков принимающим устройством. По мере продвижения данных вверх с одного уровня на другой к приложениям для конечных пользователей они декапсулируются.**



CSMA/CD

- **Протокол Ethernet описывает правила управления передачей данных в сети Ethernet.**
- Архитектура Ethernet основана на стандарте IEEE 802.3. Стандарт IEEE 802.3 определяет, что в сети реализуется способ контроля доступа «множественный доступ с контролем несущей и обнаружением конфликтов (CSMA/CD)».
- **Несущая** — проводник, используемый для передачи данных.
- **Контроль** — каждое устройство прослушивает проводник, чтобы определить, свободен ли он для передачи данных, как показано на рисунке.
- **Множественный доступ** — в сети могут одновременно присутствовать несколько устройств.
- **Обнаружение конфликтов** — конфликт вызывает удвоение напряжения на проводе, распознаваемое сетевыми платами устройств.



Стандарты кабелей Ethernet

- 1000BASE-T — в настоящее время наиболее часто реализуемая архитектура Ethernet. Ее название включает в себя характеристики стандарта:
- 1000 означает скорость работы порта: 1000 Мбит/с или 1 Гбит/с.
- BASE означает передачу в основной полосе частот. При передаче в основной полосе частот вся пропускная способность кабеля используется для одного типа сигнала.
- T означает медный кабель (Twisted pair)



CSMA/CA

- IEEE 802.11 — это стандарт, определяющий связь для беспроводных сетей. В беспроводных сетях применяется множественный доступ с контролем использования несущей и предотвращением конфликтов (CSMA/CA). CSMA/CA не обнаруживает конфликты, а старается избежать их, ожидая своей очереди для передачи. Каждое передающее устройство включает в кадр сведения о времени, необходимом ему для передачи. Все остальные беспроводные устройства принимают эту информацию и знают, как долго среда передачи данных будет занята. Это означает, что беспроводные устройства работают в полудуплексном режиме. У точки доступа или беспроводного маршрутизатора эффективность передачи уменьшается по мере подключения все большего количества устройств.



Стандарты беспроводной передачи данных

- IEEE 802.11, или Wi-Fi, представляет собой группу стандартов, которые определяют характеристики радиочастотного излучения, скорость передачи и другие параметры беспроводных локальных сетей. За последние годы разработан ряд реализаций стандарта IEEE 802.11, показанных на рисунке.
- Стандарты 802.11a, 802.11b и 802.11g следует считать устаревшими. Новые сети WLAN должны включать в себя устройства, удовлетворяющие стандарту 802.11ac. В существующих реализациях сетей WLAN рекомендуется при приобретении новых устройств выполнить обновление до 802.11ac.



Стандарты беспроводной передачи данных

Стандарт IEEE	Максимальная скорость	Максимальный радиус действия внутри помещений	Частота	Обратная совместимость
802.11a	54 Мбит/с	35 м	5 ГГц	—
802.11b	11 Мбит/с	35 м	2,4 ГГц	—
802.11g	54 Мбит/с	38 м	2,4 ГГц	802.11b
802.11n	600 Мбит/с	70 м	2,4 ГГц и 5 ГГц	802.11a/b/g
802.11ac	1,3 Гбит/с (1300 Мбит/с)	35 м	5 ГГц	802.11a/n



Безопасность беспроводной сети

- Лучший способ защиты беспроводных сетей — использование аутентификации и шифрования. В первоначальном стандарте 802.11 были определены два типа аутентификации.
- **Аутентификация открытой системы** — любое беспроводное устройство может подключиться к беспроводной сети. Этот тип аутентификации следует использовать только в тех случаях, когда безопасность не имеет значения.
- **Аутентификация с помощью общего ключа** — предоставляет механизмы аутентификации и шифрования данных, передаваемых между беспроводным клиентом и точкой доступа.
- В сетях WLAN доступны три варианта аутентификации с помощью общего ключа.



Безопасность беспроводной сети

- **Эквивалент секретности проводной сети (Wired Equivalent Privacy, WEP)** — спецификация обеспечения безопасности WLAN, определенная в первоначальном стандарте 802.11. Однако при передаче пакетов ключ не меняется, поэтому его достаточно легко взломать.
- **Защищенный доступ к Wi-Fi (Wi-Fi Protected Access, WPA)** — этот стандарт использует WEP, но обеспечивает защиту данных при помощи гораздо более надежного протокола шифрования с использованием временных ключей (TKIP). Алгоритм TKIP меняет ключ для каждого пакета, поэтому его гораздо сложнее взломать.



Безопасность беспроводной сети

- **IEEE 802.11i/WPA2** — стандарт IEEE 802.11i является в настоящее время отраслевым стандартом безопасности беспроводных сетей. Версия Wi-Fi Alliance называется WPA2. 802.11i и WPA2 используют для шифрования усовершенствованный стандарт шифрования (Advanced Encryption Standard, AES). В настоящее время AES считается самым надежным протоколом шифрования.
- С 2006 года все устройства, на которые нанесен логотип Wi-Fi Certified, сертифицированы для использования WPA2. Поэтому современные беспроводные сети всегда должны использовать стандарт 802.11i/WPA2.



Сетевое устройство

■ Модемы

- Существуют три основных типа модемов. Модемы преобразуют цифровые компьютерные данные в формат, который можно передавать в сеть интернет-провайдера. Аналоговый модем преобразует цифровые данные в аналоговые сигналы и передает их по телефонной линии. Модем цифровой абонентской линии (DSL) соединяет сеть пользователя непосредственно с инфраструктурой цифровой сети телефонной компании. Кабельный модем соединяет сеть пользователя с поставщиком услуг кабельного ТВ, который обычно имеет гибридную сеть (HFC) с волоконно-оптическими и коаксиальными кабелями.



Сетевое устройство

■ Модемы

- Существуют три основных типа модемов. Модемы преобразуют цифровые компьютерные данные в формат, который можно передавать в сеть интернет-провайдера. **Аналоговый модем** преобразует цифровые данные в аналоговые сигналы и передает их по телефонной линии. **Модем цифровой абонентской линии (DSL)** соединяет сеть пользователя непосредственно с инфраструктурой цифровой сети телефонной компании. **Кабельный модем** соединяет сеть пользователя с поставщиком услуг кабельного ТВ, который обычно имеет гибридную сеть (HFC) с волоконно-оптическими и коаксиальными кабелями.



Сетевое устройство

■ Концентраторы

- Концентраторы (hub), принимают данные на одном порте, затем отправляют их на все другие порты. Концентратор расширяет дальность действия сети, поскольку регенерирует (восстанавливает) электрические сигналы. Кроме того, можно подключать концентраторы к другому сетевому устройству, например к коммутатору или маршрутизатору, который, в свою очередь, подключен к другим сегментам сети.



Сетевое устройство

■ Мосты

- Мосты (bridge) были изобретены для разделения локальных сетей на сегменты. Мосты запоминают, какие устройства находятся в каждом сегменте. Поэтому мост может выполнять фильтрацию сетевого трафика между сегментами локальной сети. Это позволяет уменьшить объем трафика между устройствами.



Сетевое устройство

- Коммутаторы
- Коммутатор выполняет микросегментацию локальной сети. **Микросегментация означает, что коммутаторы осуществляют фильтрацию и сегментацию сетевого трафика, отправляя данные только на устройство, которому этот трафик адресован.**



Сетевое устройство

■ Принцип работы коммутатора

- Коммутаторы ведут таблицу коммутации. Таблица коммутации содержит список всех MAC-адресов сети, а также список портов коммутатора, через которые доступны устройства с определенными MAC-адресами. Таблица коммутации запоминает MAC-адреса, записывая для каждого входящего кадра MAC-адреса источника и порт, на который этот кадр пришел. После этого коммутатор создает таблицу коммутации, в которой MAC-адреса сопоставляются с исходящими портами



Сетевое устройство

- **Принцип работы коммутатора**
- При получении трафика, предназначенного для определенного MAC-адреса, коммутатор с помощью таблицы коммутации определяет, какой порт следует использовать для отправки сообщения на этот MAC-адрес. Трафик пересылается получателю через этот порт. Отправка трафика только через один конкретный порт непосредственно получателю позволяет не оказывать влияние на другие порты.



Сетевое устройство

- **Точки беспроводного доступа**
- Точки беспроводного доступа предоставляют доступ к сети для беспроводных устройств, таких как ноутбуки и планшетные ПК.
- Точка беспроводного доступа имеет ограниченную зону покрытия. Для обеспечения адекватной зоны покрытия крупномасштабных беспроводных сетей требуется несколько точек доступа.



Сетевое устройство

■ Маршрутизаторы

- Коммутаторы используют MAC-адреса для пересылки трафика в рамках одной сети. Маршрутизаторы используют IP-адреса для пересылки трафика в другие сети.
- В крупных сетях маршрутизаторы подключаются к коммутаторам, которые подключаются к локальным сетям.



Сетевое устройство

- В межсетевых экранах применяются различные методы определения разрешенного и запрещенного доступа к сегментам сети, например список контроля доступа (ACL). Этот список представляет собой файл, используемый маршрутизатором и содержащий правила относительно трафика между сетями.



Сетевое устройство

- При выборе аппаратного межсетевого экрана следует учитывать следующие аспекты.
- **Занимаемое место** — устройство устанавливается отдельно и использует специализированное оборудование.
- **Стоимость** — начальная стоимость обновления оборудования и ПО может быть довольно высокой.
- **Число компьютеров** — устройство обеспечивает защиту нескольких компьютеров.
- **Требования к производительности** — незначительное влияние на производительность компьютеров.



Другие устройства

■ Коммутационные панели

- Коммутационная панель (или патч-панель), обычно используется, чтобы собрать в одном месте входящие кабели от различных сетевых устройств. Она обеспечивает точку соединения компьютеров с коммутаторами или маршрутизаторами. Коммутационная панель может иметь или не иметь питание. Коммутационная панель с питанием может регенерировать слабые сигналы перед отправкой их на следующее устройство.



Другие устройства

■ Повторители

- Регенерация слабых сигналов, является основной функцией повторителей (repeater). Повторители также называются расширителями, поскольку они увеличивают расстояние, на которое можно передавать сигнал. В современных сетях повторители наиболее часто используются для регенерации сигналов в оптоволоконных кабелях.



Другие устройства

- **Питание через Ethernet (PoE)**
- Коммутатор с PoE (Power over Ethernet) передает по кабелю Ethernet вместе с данными постоянный ток небольшой мощности для питания устройств, поддерживающих PoE. На низковольтные устройства, поддерживающие технологию PoE, такие как точки доступа Wi-Fi, устройства видеонаблюдения и IP-телефоны, питание можно подавать из удаленных местоположений. Устройства с поддержкой технологии PoE могут получать питание по подключениям Ethernet на расстояния до 100 м.