*25.09.23 Лекция*

**Типы сетей**

В зависимости от географического охвата сети подразделяются на локальные вычислительные сети, городские вычислительные сети и глобальные вычислительные сети.

* LAN (Local Area Network) – это сеть, состоящая из компьютеров, серверов и сетевых устройств в географической зоне. Зона покрытия LAN обычно составляет несколько тысяч квадратных метров.
* MAN (Metropolitan Area Network) – это сеть, созданная внутри города. Ещё бывают CAN (кампусная).
* WAN (Wide Area Network) – Глобальная вычислительная сеть.
* MWN (Metropolitan Wireless Network) – муниципальная беспроводная городская сеть.
* LPWAN (Low Power Wide Area Network) – WAN малого энергопотребления, энергоэффективная сеть.
* IAN (Internet Area Network) – сеть без привязки к физическому местоположению, интернетофицированная сеть или облачная.
* NAN (Near Area Network) – близко транслируемая сеть или сеть близкого размещения.
* PAN (Personal Area Network) – персональная сеть, состоящая из телефона, смарт-браслета, умных часов, портативной колонки и т.п.
* HAN (Home Area Network) – домашняя сеть.
* BAN (Body Area Network) – нательная сеть, состоит из девайсов, которые есть на теле человека.
* NFC (Near Field Communication) – сеть близкого поля действия, в телефонах, ключах и т.п. У NFC ограниченна скорость до 424 кбит/с. И расстояние до действующего соединения до 4 см.
* WLAN (Wireless Area Network) – беспроводная сеть.
* VLAN (Virtual Local Area Network) – виртуальная локальная сеть. Для изоляции нескольких компьютеров от других.
* Nano Network – нано сеть, которая применяется в нано медицине, в военных или промышленных разработках.

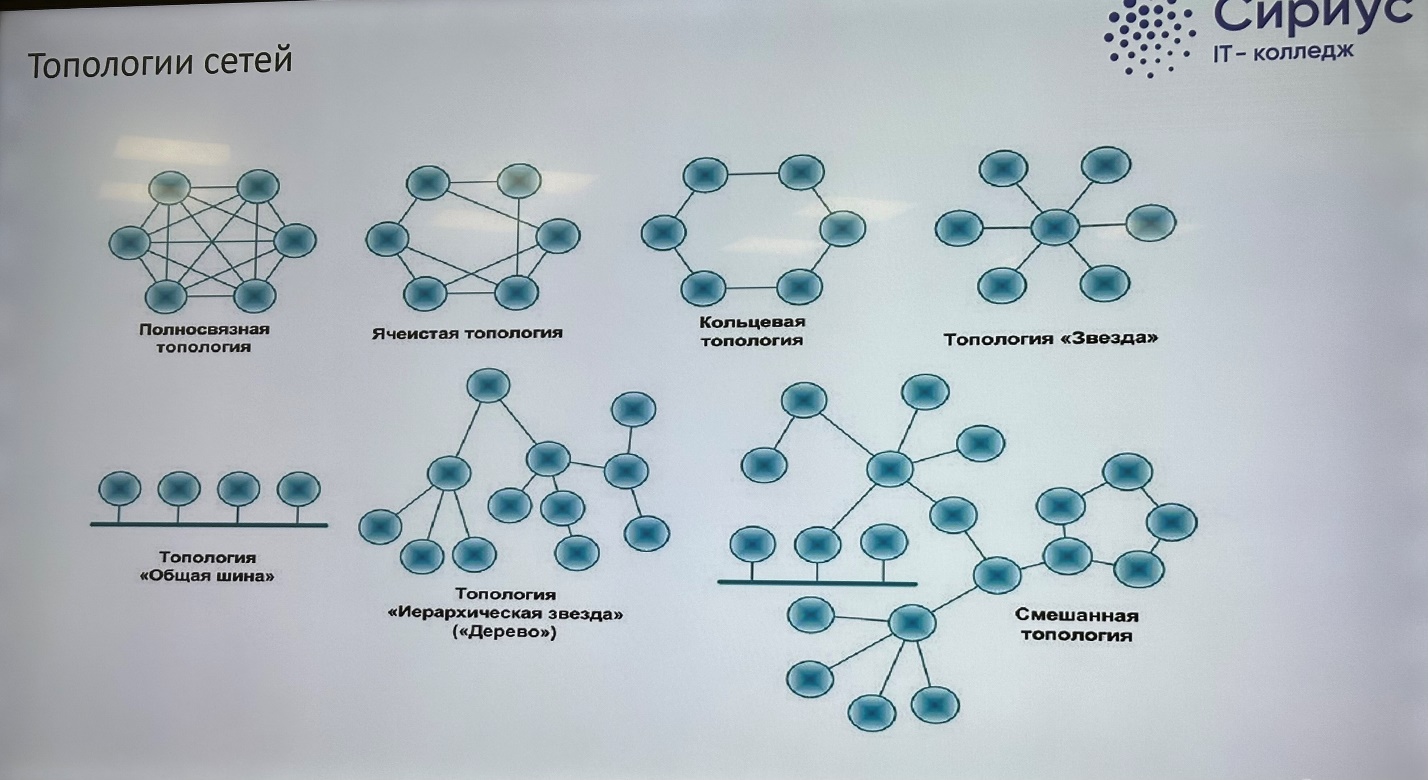
**Топологии сетей**

У сетей есть три уровня: 1) уровень доступа (телефон, с которого мы выходим в сеть), 2) уровень агрегации (когда провайдер устанавливает своё коммуникационное оборудование), 3) уровень ядра (составляет только коммуникационное оборудование, который связывает сети).

Топология сети – структурированная схема, представленную с использованием среды передачи (витая пара или оптические волокна) для соединения различных устройств (таких как компьютеры, маршрутизаторы и коммутаторы).

Используется для описания физической или логической структуры сети в области проектирования сетей и является очень важной концепцией сети.

**Физическая топология** связей определяется электрическими соединениями компьютеров между собой и может отличаться от логической конфигурации. **Логическая конфигурация** представляет собой маршруты передачи данных и образуются с помощью настройки коммуникационного оборудования.

***Виды топологий сети:***

* **Полно связанная топология** – каждый хост связан с каждым отдельным каналом передачи данных. Плюсы – высокая отказоустойчивость за счёт избыточности связей. Минусы – неэкономичность, плохая масштабируемость. Применяется очень редко в маленьких организациях.
* **Ячеистая топология** – получается из полно связной путём удаления некоторых возможных связей. Остаются только те связи, которые способствуют интенсивному обмену данными между хостами. Меньше отказоустойчивость, но выше масштабируемость. Допускает соединение большого количества компьютеров и может использоваться в глобальных сетях.
* **«Общая шина»** - реализована с помощью подсоединения новых хостов к общему коаксиальному кабелю по схеме «монтажное или». До недавнего времени была самая распространённая топология. Передаваемая информация может распространяться в обе стороны, но не одномоментно. Плюсы – снижается стоимость проводки, унифицируется подключение различных модулей, обеспечивается возможность почти мгновенного широковещательного обращения ко всем хостам. Самый серьёзный минус – низкая надёжность. Любой дефект кабеля полностью парализует сеть. Низкая производительность, пропускная способность сети делится между всеми хостами сети.
* **«Кольцо» или кольцевая топология** – данные в сетях с кольцевой топологией передаются от компьютера к компьютеру как правило в одном направлении. Если компьютер распознаёт данные как свои, то он копирует их в свой внутренний буфер. Надёжность в топологии «Кольцо» выше, чем в топологии «Общая шина». Кольцо представляет собой удобную конфигурацию для организации обратной связи. Данные, сделав полный оборот, возвращаются к отправителю, таким образом он может контролировать доставку пакетов. Это свойство также может использоваться для тестирования связности сети и поиска узла, который работает некорректно. В сети с кольцевой топологией нет ограничений на кол-во абонентов – более тысячи. Так как сетевые адаптеры в этой сети усиливают сигнал, то общая длина кольца может достигать несколько десятков километров. При этой длина кольца формально будет ограничена только временем прохождения сигналов по нему и минимальной пропускной способностью.
* **Топология «Звезда»** - в этом случае каждый компьютер подключается отдельным кабелем к общему устройству, как правило к коммутатору, который находится в центре сети. В функции центрального устройства входит: направление передаваемой информации одному или нескольким хостам.  
  Плюсы: 1) существенно большая надёжность по сравнению с топологией «Общая шина», 2) центральное устройство может играть интеллектуального фильтра информации и при необходимости блокировать запрещённые передачи данных. Высокая стоимость и сложность центрального адаптера при простоте и дешевизне абонентских.   
  Минусы: ограничение на кол-во абонентов по кол-ву портов у центрального устройства. Преодоление данного ограничения возможно с использованием нескольких коммутаторов, таким образом из стандартной «Звезды» можно получить иерархическую, которая также называется «Деревом». Для больших сетей, которая будет состоять из нескольких звёзд, возникает проблема их соединения программного и аппаратного. Центральный адаптер может быть обычным компьютером с функциями коммутатора, однако его основные функции с него никто не снимает, поэтому может возникать большая загруженность центрального адаптера.  
  *Топология «Звезда»* может быть двух видов: *обычная (активная)* и *пассивная звезда*. В центре пассивной звезды происходит просто соединение проводов, что фактически даёт «общую шину». А значит управление обменом данными не ведётся.

Сети могут делиться не только по топологии, но и по тому, какие роли есть внутри сети.

1. Одноранговые сети. В такой сети каждый абонент является как потребителем, так и владельцем предоставляемых ресурсов. При этом одна и та же машина является клиентом для одних и сервером для других.
2. Сети с выделенным сервером. Для таких сетей характерно выделение специального компьютера или нескольких, к которым обращаются все остальные с целью использования определённого ресурса.

*07.11.2023 Лекция*

**Многоуровневый подход к решению задачи обмена сообщениями между компьютерами**

Протокол – формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах.

Сеть коммуникационных протоколов – иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети.

Интерфейс – чётко определённые и стандарт

**Модель взаимодействия открытых систем ISO/OSI**

*Модель OSI* описывает только системные средства взаимодействия, реализуемые операционной системой, системными утилитами, системными аппаратными средствами. Модель не включает средства взаимодействия приложений конечных пользователей.

1. **Физический уровень**. Передача битов по физическим каналам связи, например, коаксиальный кабель, витая пара, оптоволокно. К этому уровню имеет отношение характеристики физических сред передачи данных: скорость, пропускная способность, волновое сопротивление, помехоустойчивость и т.п. Для электрических сигналов будут важны уровни напряжения или тока, тип кодирования, скорость передачи сигналов. Также здесь стандартизуется типы разъёмов и назначение каждого контакта. Функции физического уровня реализуются на всех устройствах, подключённых к сети. Со стороны компьютера они выполняются сетевым адаптером или последовательным портом.  
   Задействованные сетевые технологии и протоколы: 802.11 (Wi-Fi); 802.3 (Ethernet); 802.5 (Bluetooth); 100-BASE-T технологии Ethernet, которая определяет в качестве используемого кабеля неэкранированную витую пару 5 категории с волновым сопротивлением 100 Ом, разъём RJ-45 (a.k.a. 8P8C), максимальная длина физического сегмента 100 метров, манчестерский код для представления данных в кабеле.
2. **Канальный уровень (уровень передачи данных)**. На канальном уровне в основном используются коммутаторы, единицей передачи данных будут являться кадры. А также используется MAC-адресация. На физическом уровне просто пересылаются биты, при этом не учитывается, что в некоторых сетях линии связи могут быть разделены попеременно между несколькими парами хостов. Таким образом физическая среда передачи данных может быть занята. Задачей канального уровня является проверка доступности среды передачи, кроме того, есть и другие задачи — это коррекция ошибок, реализация механизмов обнаружения. Обнаружение происходит за счёт введения контрольных сумм. А коррекция будет происходить за счёт повторной передачи повреждённых кадров. Однако, данная функция присутствует не во всех протоколах канального уровня. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, делает он это только в сети с совершенно определённой топологией. Именно той, для которой он был разработан.   
   На канальном уровне будут работать такие устройства как компьютеры, коммутаторы (а также концентраторы), маршрутизаторы и мосты. Со стороны компьютера функции канального уровня реализуются сетевым адаптером и его драйвером. В глобальных сетях канальный уровень может обеспечивать обмен сообщениями только между двумя соседними компьютерами, соединёнными индивидуальными линиями связи. Протокол ARP это протокол канального уровня.
3. **Сетевой уровень**. Служит для образования единой транспортной системы, объединяющей несколько сетей, при чём эти сети могут использовать совершенно различные принципы передачи сообщений и обладать произвольной структурой связи. На сетевом уровне используются в основном маршрутизаторы, IP-адресация, а единицей передачи данных является сетевой пакет. Самой главной задачей сетевого уровня является решение проблемы выбора наилучшего пути следования сетевого пакета. Кроме сетевой задачи есть и другие: 1) чтобы с одной стороны сохранить простоту процедур передачи данных для типовых топологий, а с другой стороны допустить использование произвольных топологий вводится сетевой уровень, 2) согласование разных технологий, 3) упрощение адресации в крупных сетях, 4) создание надёжных и гибких барьеров на пути нежелательного трафика между сетями. На сетевом уровне определяются два типа протоколов: адресные протоколы (сетевые), реализуют продвижение пакетов через сеть, это протокол IP, IPX и т.п; протоколы маршрутизации, которые помогают маршрутизаторам собирать информацию о топологии межсетевых соединений: BGP, RIP, IS-IS, OSPF. Все протоколы этого уровня реализуются программными модулями ОС, а также программными и аппаратными средствами маршрутизаторов.

**TCP и UDP – форматы заголовков**

Порт – это 16-ти разрядное беззнаковое целое число. Первые 1024 порта зарезервированы под наиболее популярные сетевые службы и приложения. Порты с более высокими номерами доступны для общего использования и известны как динамические или эфемерные порты.

Для процесса передачи данных используется сокет – совокупность IP-адреса с маской подсети, порта и транспортного протокола.   
Порядковый номер – 32 бита, каждый байт данных имеет отправленных через TCP соединение имеет свой порядковый номер. В данном поле указывается порядковый номер первого байта, отправляемого в сегменте.  
Новые подтверждения 32 бита – порядковый номер первого байта, но следующего сегмента, который ожидается для получения.   
Длина заголовка 4 бита, указывает на длину заголовка TCP и измеряется в блоках по 32 бита.  
Резерв 6 бит, всегда зарезервирован и имеет значение ноль.  
Биты управления (aka флаги) 6 бит, контролируют обработку сегментов. Существует 6 флагов: 1) **URG** – показатель срочности, 2) **ACK** – флаг подтверждения, 3) **PSH** – выталкивает в поставленную очередь данные из буфера, 4) **RST** – сброс соединение сети по завершению или после разрыва, 5) **FIN** – финиш, завершает передачу, 6) **SYN** – синхронизирует соединение.  
Окно 16 бит, управляет потоком TCP. Значение данного поля представляет собой максимальное кол-во байтов, которое получатель разрешил передавать. Длина измеряется в битах, а значение в байтах.  
Контрольная сумма 16 бит, проверка данных на правильность.  
Указатель срочности, действует только при установке флага **URG**. Это полое указывает на то, что отправитель передаёт данные в аварийном режиме. Значение этого поля указывает на количество байт срочных данных в сегменте. Срочные данные располагаются в начале сегмента.  
Опции, необязательное поле, может содержать дополнительные контрольные суммы, метки времени и т.д. Эта строка дополняется до 32 бит нулями. Длина поля опции может быть от нуля до 40 байт.

!! Нужно, чтобы итоговый размер заголовка был кратен 4

Установление TCP-соединения – трёхстороннее рукопожатие (в презентации)

Выключение TCP-соединения – четырёхстороннее квитирование (в презентации)

TCP поддерживает передачу данных в duplex-ном режиме, что означает возможность передачи данных в обоих направлениях. Значит, после завершения передачи данных соединение должно быть разорвано в обоих направлениях

*22.12.2023 Семинар*

**Планирование IP-адресов**

При планировании необходимо следовать следующим правилам:

1. Уникальность. У каждого хоста в сети должен быть уникальный IP-адрес. Серые адреса – одинаковые IP-адреса в разных локальных сетях
2. Непрерывность. Смежные адреса можно легко суммировать в иерархических сетях. Суммирование маршрутов уменьшает размер таблицы маршрутизации и ускоряет вычисление маршрутов.
3. Масштабируемость. Адреса должны быть надлежащий образом зарезервированы на каждом уровне, чтобы обеспечить смежное адресное пространство для суммирования маршрутов при расширении сети.
4. Сочетание топологии и сервисов. Это нужно для облегчения планирования маршрутов и развёртывания технологии QoS. Правильное планирование IP-адресов помогает легко определить положение устройств и типы сервисов по значению IP-адреса.

**Протокол IPv6**

Организация IANA продавала белые IP-адреса 4 версии с помощью 5 своих региональных интернет регистраторов.

Первый интернет регистратор – APNIC: азиатско-тихоокеанский регион.

Второй регистратор RIPE: Европа, центральная Азия, ближний восток.

Третий регистратор LACNIC: страны южной Америки и карибского бассейна.

Четвёртый регистратор ARIN: северная Америка и некоторые регионы карибского бассейна.

Последний регистратор AFRINIC: Африка.

IPv6 адреса делятся на следующие виды:

1. Индивидуальные адреса. Идентифицирует один интерфейс устройства. Пакеты, отправленные на этот адрес, доставляются только на этот интерфейс. В IPv6 интерфейс может иметь несколько адресов. Имеются специальные адреса – индивидуальные: неуказанный или любой IP-адрес 0:0:0:0:0:0:0:0/128 (::/128), loopback 0:0:0:0:0:0:0:1 (::1).
2. Многоадресный или групповой. Идентифицирует группу интерфейсов. Пакеты, присылаемые на этот адрес, присылаются всем интерфейсам участникам групповой рассылки.
3. Произвольный адрес. Позволяет адресовать группу интерфейсов, однако, в отличие от многоадресных адресов пакеты, передаваемые на произвольный адрес, должны быть доставлены на один из интерфейсов группы рассылки.

Широковещательных адресов в IPv6 нет.