Занятие 1. Введение в сети. Модели OSI и TCP/IP. Протоколы канального, сетевого и транспортного уровней

В начале развития вычислительных сетей все протоколы и стандарты взаимодействия устройств в основном разрабатывались самими производителями, когда же возникла необходимость объединения сетей или же взаимодействия между ними, взаимодействия сервисов, находящихся в различных сетях, стали разрабатываться модели сетевого взаимодействия, описывающие стандарты и принципы, по которым должны строиться протоколы взаимодействия сетей, сервисов и устройств.

Модель OSI

В начале и середине 1970-х годов вычислительные сети в основном либо спонсировалась государством, либо разрабатывалась производителями с использованием собственных стандартов. Общественные сети передачи данных только начинали появляться. Примерно в 1973-1975 годах назрела необходимость определения протоколов более высокого уровня, это привело к созданию Международной комиссии по стандартам для охвата области конфигурации компьютерных систем.

Начиная с 1977 года Международная организация стандартизации ISO проводила программу по разработке общих стандартов и методов сетевого взаимодействия. Аналогичный процесс развивался в Международном консультационном комитете по телеграфии и телефонии (CCITT). Оба органа разработали документы, определяющие схожие сетевые модели. Модель OSI была впервые определена в начальном виде в феврале 1978 года, а проект стандарта был опубликован ISO в 1980 году. В 1983 году документы CCITT и ISO были объединены, чтобы сформировать базовую эталонную модель для соединения открытых систем, обычно называемой эталонной моделью OSI (Open System Interconnection) или просто моделью OSI. OSI состояла из двух основных компонентов: абстрактной модели сети, называемой базовой эталонной моделью или семислойной моделью, и набора сетевых протоколов. Она продвигает идею последовательной модели уровней протоколов, определяющей взаимодействие между сетевыми устройствами и программным обеспечением.

Концепция семислойной модели была разработана Чарльзом Бахманом в компании Honeywell Information Systems. В этой модели сетевая система была разделена на слои. Внутри каждого слоя один или несколько объектов реализуют его функциональные возможности. Каждая сущность взаимодействовала только со слоем, находящимся непосредственно под ней, и предоставляла средства для использования слоем, находящимся над ней.

OSI была отраслевой инициативой, направленной на то, чтобы заставить участников отрасли согласовать общие сетевые стандарты для обеспечения совместимости с несколькими поставщиками. Модель OSI до сих пор используется в качестве эталона для обучения и документации; однако протоколы OSI, изначально задуманные для этой модели, не получили популярности. Некоторые инженеры утверждают, что эталонная модель OSI все еще актуальна, другие считают, что оригинальная модель OSI не соответствует современным сетевым протоколам.

Суть эталонной модели OSI заключается в том, что протоколы связи позволяют структуре на одном хосте/узле взаимодействовать с соответствующей структурой того же уровня на другом хосте/узле. На каждом уровне N два объекта обмениваются блоками данных с помощью протокола данного уровня на соответствующих устройствах. Каждый блок данных содержит блок служебных данных, связанный с верхним или нижним протоколом.

СХЕМАТИЧЕСКИЙ ВИД УРОВНЕЙ МОДЕЛИ OSI

Уровень	Данные	Примеры протоколов	Среда/оборудование
7 Прикладной	Данные клиентов, сервисов	HTTP, FTP, SMTP и т.д.	Хосты, клиенты, сервисы
6 Представления		TLS/SSL	
5 Сеансовый		RPC, L2TP, PPTP	
4 Транспортный	Сегменты/датаграммы	TCP, UDP	
3 Сетевой	Пакеты	IPv4, IPv6, ICMP	Маршрутизатор
2 Канальный	Кадры	Ethernet	Коммутатор, сетевая карта
1 Физический	Биты	Сигналы и двоичные данные	Витая пара, оптоволокно, радиоканал

Любой протокол модели OSI должен взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и/или ниже своего уровня. Взаимодействия с протоколами своего уровня называются горизонтальными, а с уровнями на единицу выше или ниже — вертикальными. Любой протокол модели OSI может выполнять только функции своего уровня и не может выполнять функций другого уровня.

Начиная с 1990-х годов семиуровневая модель OSI часто критиковалась отдельными авторами. Многие современные протоколы не соответствуют уровням модели OSI или их нельзя отнести к какому-то одному конкретному уровню, например, протоколы семейства TCP/IP стали наиболее востребованными и используемыми, они были разработаны с использованием других протоколов сетевого взаимодействия, и включают в себя транспортный протокол TCP, полностью соответствующий модели OSI, транспортный протокол UDP, лишь частично соотвествующий модели, служебный протокол ICMP и еще около двухсот протоколов, не являющихся транспортными.

Модель TCP/IP

Модель TCP/IP исторически произошла от сети ARPANET из 1970-х годов, разработанной под управлением МО США.

Это сетевая модель передачи данных, представленных в цифровом виде, она описывает способ передачи данных от источника информации к получателю. В модели предполагается прохождение информации через четыре уровня, каждый из которых описывается протоколом. Название TCP/IP происходит из двух важнейших протоколов семейства - TCP (Transport Control Protocol) и IP (Internet Protocol), которые были первыми разработаны и описаны в данном стандарте.

Набор интернет-протоколов обеспечивает сквозную передачу данных, определяющую, как данные должны пакетироваться, обрабатываться, передаваться, маршрутизироваться и приниматься. Эта функциональность организована в четыре слоя абстракции, которые классифицируют все связанные протоколы в соответствии с объемом задействованных сетей. От самого низкого до самого высокого уровня — это уровень связи, содержащий методы связи для данных, которые остаются в пределах одного сегмента сети; интернет-уровень, обеспечивающий межсетевое взаимодействие между независимыми сетями; транспортный уровень, обрабатывающий связь между хостами; и прикладной уровень, который обеспечивает обмен данными между процессами для приложений.

Как таковая модель сети TCP/IP предшествует модели OSI, более всеобъемлющей эталонной структуре для общих сетевых систем.

СХЕМАТИЧЕСКИЙ ВИД УРОВНЕЙ МОДЕЛИ TCP/IP

Уровень	Протоколы
4 Прикладной	HTTP, FTP, SMTP и т.д.
3 Транспортный	TCP, UDP
	Протоколы маршрутизации RIP, OSPF, работают поверх IP
2 Межсетевой	IP
	ARP, работает поверх канального уровня
1 Канальный	Ethernet, физическая среда передачи данных

Протоколы различных уровней моделей OSI и TCP/IP

Обычно принято рассматривать протоколы моделей OSI и TCP/IP, начиная с верхнего уровня.

ПРИКЛАДНОЙ УРОВЕНЬ (OSI, TCP/IP)

Прикладной уровень в обоих моделях обеспечивает взаимодействие пользовательских приложений с сетью, на этом уровне работает большинство сетевых приложений. Они имеют свои собственные протоколы обмена информацией, например, HTTP, FTP, SMTP, SSH и многие другие. В основном эти протоколы работают поверх TCP или UDP и привязаны к определенному порту, например, HTTP - TCP 80, FTP - TCP 20 и TCP 21, SSH - TCP 22, SMTP - TCP 25, DNS - UDP 53 (или TCP 53) и т.д.

УРОВЕНЬ ПРЕДСТАВЛЕНИЯ (OSI)

Уровень представления обеспечивает преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений. На этом уровне может осуществляться сжатие/распаковка или шифрование/дешифрование, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально. Уровень представлений обычно представляет собой промежуточный протокол для преобразования информации из соседних уровней. Частично к уровню представления относят протоколы шифрования SSL/TLS.

СЕАНСОВЫЙ УРОВЕНЬ (OSI)

Сеансовый уровень модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений. К этому уровню относятся протоколы L2TP, PPTP, RPC.

ТРАНСПОРТНЫЙ УРОВЕНЬ (OSI, TCP/IP)

Транспортный уровень модели OSI предназначен для обеспечения надёжной передачи данных от отправителя к получателю. При этом уровень надёжности может варьироваться в широких пределах. Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приёма), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных.

Протоколы транспортного уровня модели TCP/IP могут так же решать проблему негарантированной доставки сообщений, а также гарантировать правильную последовательность прихода данных.

К протоколам транспортного уровня в основном относятся протоколы TCP и UDP, в модели TCP/IP частично к транспортному уровню относятся протоколы маршрутизации, работающие поверх IP.

СЕТЕВОЙ УРОВЕНЬ (OSI), МЕЖСЕТЕВОЙ УРОВЕНЬ (TCP/IP)

Сетевой уровень предназначен для определения пути передачи данных и их передачи из одной сети в другую. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети. Протоколы сетевого уровня маршрутизируют данные от источника к получателю. Работающие на этом уровне устройства (маршрутизаторы) условно называют устройствами третьего уровня (по номеру уровня в модели OSI). К протоколам сетевого уровня относятся IP, работающие поверх IP протоколы маршрутизации RIP, OSPF (частично относятся к транспортному уровню), протокол ICMP (так же работает поверх IP).

КАНАЛЬНЫЙ УРОВЕНЬ (OSI, TCP/IP)

Канальный уровень описывает способ кодирования данных для передачи пакета данных на физическом уровне(то есть специальные последовательности бит, определяющих начало и конец пакета данных, а также обеспечивающие помехоустойчивость). Примером протокола канального уровня в обоих моделях может служить Ethernet.
Кроме того, в модели TCP/IP канальный уровень описывает среду передачи данных, физические характеристики такой среды и принцип передачи данных, что в модели OSI отведено физическому уровню.

ФИЗИЧЕСКИЙ УРОВЕНЬ (OSI)

Физический уровень— нижний уровень модели OSI, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства к другому. Функции физического уровня реализуются на всех устройствах, подключенных к сети. К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами/узлами. Физический уровень определяет такие виды сред передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передач данных и т. п.

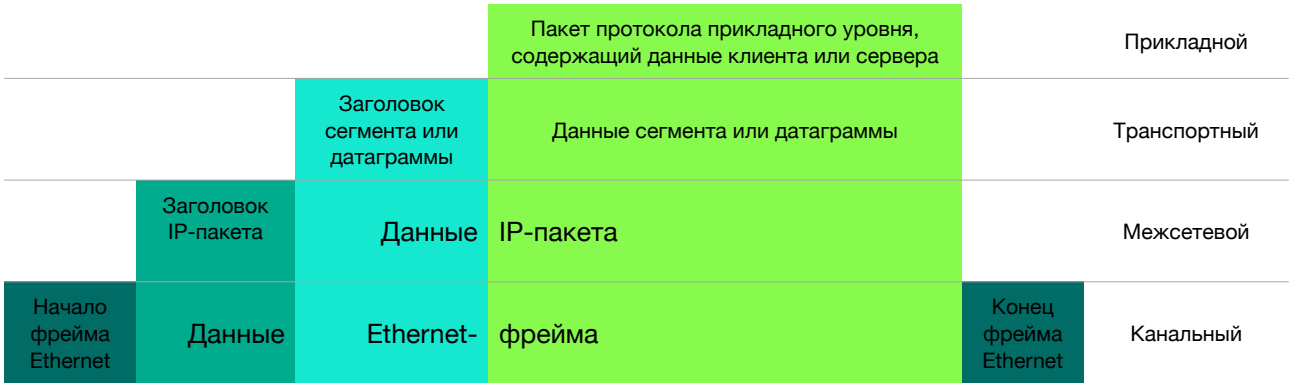
Существует много спорных и конфликтующих вопросов о принадлежности конкретных протоколов различным уровням моделей OSI и TCP/IP или необходимости разделения уровней с 7 по 5 в модели OSI для современных протоколов. А так же спорные протоколы, которые должны принадлежать промежуточному межсетевому уровню модели OSI, который должен находиться между сетевым и канальным.

Инкапсуляция протоколов

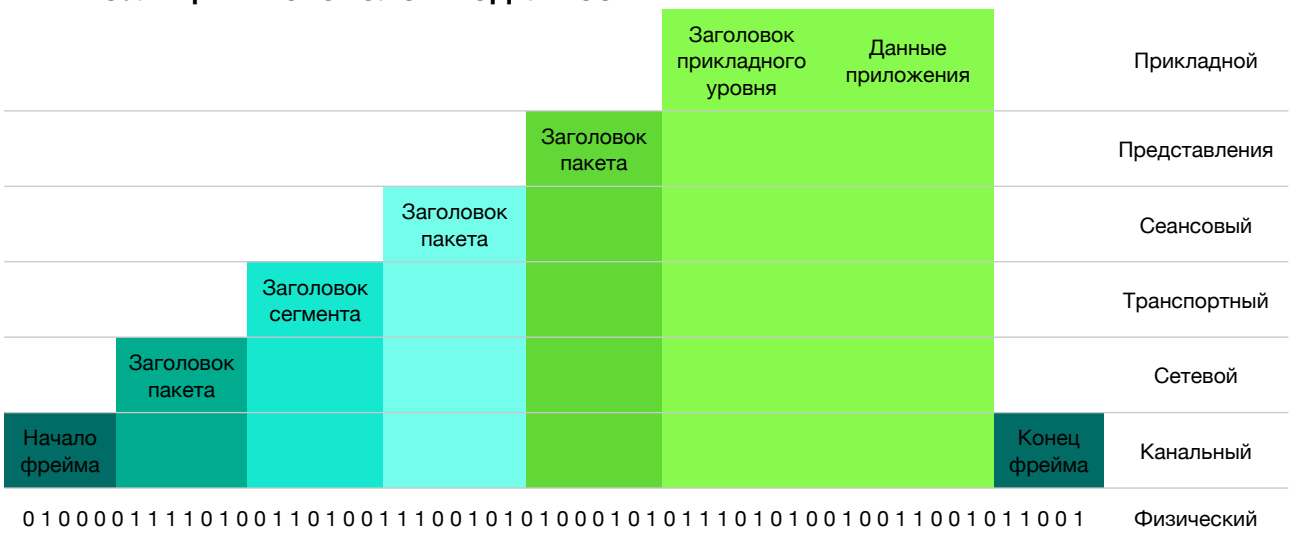
Обе модели были рассмотрены, чтобы нагляднее была понятна инкапсуляция протоколов. Инкапсуляция протоколов - метод проектирования протоколов в которой логически независимые функции сети не зависят от реализации нижележащих механизмов с помощью включения этих механизмов в более высокоуровневые объекты.

Физический уровень ответственен за физическую передачу данных. IP предоставляет глобальный способ адресации устройств и маршрутизации трафика. TCP добавляет возможность выбора порта сервиса. Во время инкапсуляции каждый уровень собирает свой собственный пакет, добавляя некоторый заголовок с контрольной информацией к пакету с более высокого уровня.

ИНКАПСУЛЯЦИЯ ПРОТОКОЛОВ МОДЕЛИ TCP/IP



ИНКАПСУЛЯЦИЯ ПРОТОКОЛОВ МОДЕЛИ OSI



В современных реалиях работа сервисов и программного обеспечения практически невозможна без сетевого взаимодействия, локального или межсерверного, межсетевого. Для разработчика сетевое взаимодействие на уровнях 1-3 модели OSI или 1-2 модели TCP/IP в большинстве случаев осуществляется прозрачно, поскольку в нем участвует сетевое оборудование - сетевые карты, коммутаторы, маршрутизаторы, а межсервисное взаимодействие начинается уже на транспортном уровне. Однако благодаря инкапсуляции протоколы нижних уровней обоих моделей влияют на работу протоколов транспортного и более высоких уровней, учитывая это влияние можно существенно оптимизировать работу сервисов и взаимодействие с клиентами.

Физический уровень модели OSI, протоколы канального, сетевого/межсетевого и транспортного уровней

ФИЗИЧЕСКИЙ УРОВЕНЬ МОДЕЛИ OSI, ФИЗИЧЕСКАЯ СРЕДА ПЕРЕДАЧИ ДАННЫХ КАНАЛЬНОГО УРОВНЯ МОДЕЛИ TCP/IP

Линии связи или линии передачи данных - это среда, по которой передаются информационные сигналы, и специальная аппаратура (повторители, усилители сигнала и т.п.). Каналы передачи данных - это линии связи и аппаратура приема-передачи данных (устройства, преобразующие физический сигнал в цифровой и обратно).

В зависимости от физической среды каналы передачи данных могут быть проводными, кабельными и беспроводными.

К проводным каналам передачи данных относятся каналы передачи телефонных и телеграфных сигналов, они имеют существенные недостатки в виде низкой скорости передачи, слабой помехозащищенности и высокой возможности несанкционированного доступа.

К кабельным каналам передачи данных относятся коаксиальный кабель, витая пара, оптоволокно. Кабельные каналы намного устойчивее к помехам и несанкционированному доступу, обладают высокой пропускной способностью, но в зависимости от типа кабеля могут быть более дорогостоящими и сложными при монтаже и прокладке (ограничения на радиусы изгибов, механическая прочность, чувствительность к некоторым излучениям). Пропускная способность коаксиального кабеля достигает 50-100 Мбит/с, витой пары (в зависимости от количества используемых пар проводов) до 10Гбит/с, оптоволокна (в зависимости от длины сегмента канала и типа волокна - одномодовое или многомодовое) до 100Гбит/с.

К беспроводным каналам передачи данных относятся каналы, где средой передачи сигнала является воздушная среда - радиоканалы, Bluetooth-каналы, WI-FI, GSM-каналы и т.п. Беспроводные каналы передачи данных очень подвержены как естественным, так и искусственным помехам, угрозам несанкционированного доступа, у некоторых существуют значительные ограничения на прямую видимость приемника и передатчика, а так же расстояние между ними и состояние среды передачи. Современные беспроводные каналы и сети реализуют множество средств защиты как от помех, так и от угроз перехвата/подмены данных, которые позволяют не только обеспечить защиту канана, но и значительно увеличить скорость передачи данных по нему. Например, современные стандарты сетей WI-FI позволяют осуществлять передачу данных на скоростях до 30Гбит/с.

Реализации и версии протоколов канального уровня всегда учитывают физическую среду и каналы передачи данных, на которых эти протоколы будут работать.

ПРОТОКОЛ КАНАЛЬНОГО УРОВНЯ ETHERNET

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде. Ethernet стал одной из самых распространённых технологий локальных вычислительных сетей в середине 1990-х годов. Название «Ethernet» (буквально «эфирная сеть» или «среда сети») отражает первоначальный принцип работы этой технологии: всё, передаваемое одним узлом, одновременно принимается всеми остальными (то есть имеется некое сходство с радиовещанием). В настоящее время практически всегда подключение происходит через коммутаторы или свичи, так что кадры, отправляемые одним узлом, доходят лишь до адресата (исключение составляют передачи на широковещательный адрес) — это повышает скорость работы и безопасность сети.

В стандарте первых версий (Ethernet v1.0 и Ethernet v2.0) указано, что в качестве передающей среды используется коаксиальный кабель, в дальнейшем появилась возможность использовать витую пару и оптический кабель.

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес, формат XX:XX:XX:XX:XX:XX), прошитый в ней при изготовлении. Этот номер используется для идентификации отправителя и получателя кадра. Уникальность MAC-адресов достигается тем, что каждый производитель получает в координирующем комитете IEEE Registration Authority диапазон из шестнадцати миллионов (2^{24}) адресов, и по мере исчерпания выделенных адресов может запросить новый диапазон. Поэтому по трём старшим байтам MAC-адреса можно определить производителя.

Наиболее распространенный формат кадра Ethernet содержит в себе MAC-адреса устройств получателя (destination) и отправителя (source), данные (от 46 до 1500 байт) и контрольную сумму. Объем данных, передаваемых в одном кадре, ограничивается размером MTU (maximum transmission unit). Ограничения на максимальный размер кадра могут накладываться по нескольким причинам (в основном они связаны с производительностью сетевого оборудования на узлах, по которым он проходит): для уменьшения времени на повторную передачу в случае потери или искажения пакета, а с увеличением длины пакета вероятность искажения увеличивается, из-за малого размера и быстродействия сетевых буферов сетевых устройств (однако слишком большие буферы так же могут снижать быстродействие). Значение MTU определяется стандартом соответствующего протокола, но может быть переопределено автоматически для определённого канала или вручную для нужного интерфейса. Для высокопроизводительной сети причины, вызвавшие начальные ограничения MTU, устарели, в связи с этим для Ethernet был разработан стандарт Jumbo-кадров с увеличенным MTU.

В зависимости от скорости передачи данных и передающей среды (физического канала передачи данных) существует несколько вариантов технологии и реализации протокола Ethernet. Независимо от способа передачи, стек сетевого протокола и программы работают одинаково практически во всех вариантах.

Краткий список используемых вариантов реализации:

- **Ethernet, 10Mbps:** 10BASE-T - для передачи данных используется 4 провода кабеля витой пары (две скрученные пары) категории 3 или категории-5. Максимальная длина сегмента — 100 метров.
- **Fast Ethernet, 100Mbps:** 100BASE-T - общий термин для обозначения стандартов, использующих в качестве среды передачи данных витую пару. Длина сегмента — до 100 метров. Включает в себя стандарты 100BASE-TX, 100BASE-T4 и 100BASE-T2 в зависимости от типа используемой витой пары и количества проводов.
- **Gigabit Ethernet, 1Gbps:** 1000BASE-T - основной гигабитный стандарт, использует витую пару категории 5e. В передаче данных участвуют 4 пары, каждая пара используется одновременно для передачи по обоим направлениям со скоростью — 250 Мбит/с; 1000BASE-X - общий термин для обозначения стандартов со сменными приёмопередатчиками, в основном использующими оптоволокно в качестве среды передачи, работать на разных длинах волн и длинах сегментов.
- **10G Ethernet, 10Gbps:** 10GBASE-T - стандарт витую пару категории 6 (максимальное расстояние 55 метров)[21] и 6a (максимальное расстояние 100 метров);10GBASE-SR - технология 10-гигабитного Ethernet для коротких расстояний (до 26 или 82 метров, в зависимости от типа кабеля), используется многомодовое волокно. Он также поддерживает расстояния до 300 метров с использованием нового многомодового волокна; 10GBASE-LR - стандарт поддерживает расстояние до 10км при использовании одномодового волокна.
- **40G Ethernet, 100G Ethernet** - стандарты являются следующим этапом развития группы стандартов Ethernet, имевших до 2010 года наибольшую скорость в 10 Гбит/с. В зависимости от используемого стандарта и волокна максимальные расстояния могут быть от 1м до 40км.
- Сейчас уже разрабатываются стандарты и устройства для поддержки 400G Ethernet, 1T Ethernet.

ПРОТОКОЛ СЕТЕВОГО/МЕЖСЕТЕВОГО УРОВНЯ IP

Internet Protocol - маршрутизируемый протокол, именно он стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. Неотъемлемой частью протокола является адресация сети. IP объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов. IP не гарантирует надёжной доставки пакета до адресата — в частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться, оказаться повреждёнными или не прийти вовсе. Гарантию безошибочной доставки пакетов дают некоторые протоколы более высокого уровня, которые используют IP в качестве транспорта.

При доставке IP пакета он проходит через разные каналы доставки. Возможно возникновение ситуации, когда размер пакета превысит возможности узла системы связи. В этом случае протокол предусматривает возможность дробления пакета на уровне IP в процессе доставки. Соответственно, к конечному получателю пакет придет в виде нескольких пакетов, которые необходимо собрать в один перед дальнейшим анализом. Возможность дробления пакета с последующей сборкой называется IP фрагментацией.

Существуют две версии протокола IP - IPv4 и IPv6. В современных сетях широко распространена 4я версия протокола. В начале 1990-х годов стало ясно, что изменений в протоколе IPv4 недостаточно для предотвращения исчерпания адресов. С 1996 года вводится в эксплуатацию 6я версия протокола, которая позволяет адресовать значительно большее количество узлов, чем IPv4.

В протоколе IPv4 каждому узлу сети ставится в соответствие IP-адрес длиной 4 октета (4 байта), при этом компьютеры в подсетях объединяются общими начальными битами адреса, количество этих бит, общее для данной подсети, называется маской сети. Традиционной формой записи IPv4 адреса является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками (xxx.xxx.xxx.xxx/xx). Через дробь указывается длина маски подсети (это количество бит адреса, которые являются общими для всех хостов подсети, то есть номером сети). Адреса IPv6 отображаются как восемь четырёхзначных шестнадцатеричных чисел (то есть групп по четыре символа), разделённых двоеточием (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx). Если две и более групп подряд равны нулю, то они могут быть опущены и заменены на двойное двоеточие. Незначащие старшие нули в группах могут быть опущены.

В адресных пространствах обеих версий протокола IP существуют зарезервированные адреса, не предназначенные для глобальной маршрутизации.

НЕКОТОРЫЕ ЗАРЕЗЕРВИРОВАННЫЕ АДРЕСА IPV4

Подсеть	Назначение
0.0.0.0/32	Обозначает любые IP отправителя или любые сети получателя на текущем хосте.
10.0.0.0/8	Для использования в частных локальных сетях.
127.0.0.0/8	Подсеть для коммуникаций внутри хоста (localhost, интерфейс lo0, loopback). Используется сетевая подсистема, но в действительности такие пакеты не проходят через сетевую карту.
169.254.0.0/16	Подсеть используется для автоматического назначения IP операционной системой в случае, если настроено получение адреса по DHCP, но ни один сервер не отвечает.
172.16.0.0/12	Для использования в частных локальных сетях.
192.168.0.0/16	Для использования в частных локальных сетях.

IP-адрес состоит из двух частей: номера сети и номера узла. В случае изолированной локальной сети ее адрес может быть выбран администратором из специальных зарезервированных диапазонов. Для выхода в глобальную сеть небходимо, чтобы у устройства был IP-адрес из другого диапазона, участвующего в глобальной маршрутизации, так называемый «белый IP-адрес». Такие адреса выдаются либо провайдерами клиентам и специальными регулирующими организациями - RIR (Regional Internet Registry) провайдерам.

По умолчанию устройство, находящееся в определенной сети, видит только хосты, находящиеся в той же сети. Для общения с устройствами, находящимися в других подсетях

(не важно локальных или глобальных) необходим маршрутизатор или шлюз (в виде самостоятельного специального сетевого устройства или же особым образом настроенного компьютера/сервера). Шлюз (gateway) может предоставлять доступ как к конкретной сети или конкретному адресу, так и быть шлюзом по умолчанию для доступа ко всем сетям, отличным от сети, в которой находится устройство (default gateway).

Несмотря на то, что в будущем подавляющее число адресов будет пренадлежать протоколу IPv6, он не будет рассматриваться слишком подробно. Потому что переход с IPv4 на IPv6 - это очень долгий и трудоемкий процесс, который не может быть совершен одномоментно, операторы связи постепенно вводят в свои сети работу с IPv6 и часть глобальных сервисов уже частично переведена на IPv6, однако существует огромное количество оборудования, не поддерживающего технологию IPv6, и после исчерпания адресного пространства IPv4 оба пространства будут существовать параллельно, преобразовываясь на стыковых участках, с постепенным увеличением доли трафика IPv6.

ПРОТОКОЛЫ ТРАНСПОРТНОГО УРОВНЯ МОДЕЛЕЙ OSI И TCP/IP

В отличие от протоколов сетевого или межсетевого уровней протоколы транспортного уровня работают не только между конкретными хостами или узлами сети, а между конкретными клиентом и сервисом. Клиент - это хост или узел, являющийся инициатором установки соединения, устанавливающий соединение с серверов и конкретным сервисом, принимающим соединения на конкретном порту. Сервер/сервис - это хост или узел сети, к которому обращается клиент, сервис принимает соединения на конкретном порту. Порт - это число от 0 до 65535, сервис может слушать на любом порту, но номера портов от 0 до 1024 закреплены за определенными сервисами и протоколами прикладного уровня (например, web-сервис, протокол HTTP - порт 80), и некоторые порты с номерами больше 1024 так же принято использовать для конкретных типов сервисов.

Клиент и сервер могут находиться как в одной сети, так и в разных, поскольку протоколы транспортного уровня работают поверх сетевого и межсетевого, то все механизмы сетевого и межсетевого взаимодейвия (например, маршрутизация) проходят для них «прозрачно». Рассматриваемые ниже протоколы TCP и UDP используют в качестве «транспорта» протокол IP. Соответственно в качестве адресов и клиента и сервера для этих протоколов используется IP-адрес и номер порта.

ПРОТОКОЛ UDP (USER DATAGRAM PROTOCOL)

UPD - это один из ключевых протоколов сети Интернет. При использовании протокола UPD клиенты могут посылать сообщения, отправлять данные другим хостам сети без необходимости предварительной установки соединения, организации специальных каналов передачи или путей данных. Протокол использует простую модель передачи без обеспечения надёжности, упорядочивания или целостности данных. Таким образом, UDP предоставляет ненадёжный сервис, и датаграммы (так в протоколе называются сообщения/данные) могут прийти не по порядку, дублироваться или вовсе исчезнуть без следа. UDP подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении или протоколах более высокого уровня, использующих UDP в качестве транспорта. Чувствительные ко времени приложения часто используют UDP, так как предпочтительнее пропустить данные, чем ждать задержавшиеся пакеты. Природа UDP как протокола без

сохранения состояния также полезна для серверов, отвечающих на небольшие запросы от огромного числа клиентов, например, сервис разрешения доменных имен DNS, очень часто UDP используется в потоковых вещаниях вроде IPTV, Voice over IP, онлайн-трансляций, онлайн-игр. В этих приложениях потеря пакетов обычно не является большой проблемой. Обычно для таких хостов, особенно в локальных сетях, на сетевом и канальном уровнях увеличивается размер MTU, чтобы обеспечить большую пропускную способность сервиса, уменьшив фрагментацию пакетов. Теоретически максимальный размер данных датаграммы составляет 65507, однако поскольку стандартным размером MTU в сетях IPv4 обычно равно 1500, то длина данных составляет 1432 байт (MTU за вычетом размера заголовка IP-пакета). В IPv6 большие UDP-пакеты могут иметь больший размер (их называют jumbogram) - до 4294967287 байт данных, естественно при условии поддержки всеми участниками передачи пакетов такого размера.

ПРОТОКОЛ TCP (TRANSMISSION CONTROL PROTOCOL)

TCP - это один из основных протоколов передачи данных сети Интернет. Механизм протокола предоставляет возможность обмена данными с предварительной установкой соединения между хостами/узлами, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым целостность передаваемых данных и уведомление отправителя о результатах передачи. В протоколе TCP пакеты данных (сообщения) называются сегментами.

В отличие от UDP, который может сразу же начать передачу пакетов, TCP устанавливает соединения, которые должны быть созданы перед передачей данных. TCP-соединение можно разделить на 3 стадии:

1. Установка соединения
2. Передача данных
3. Завершение соединения

Процесс установки TCP-соединения состоит из 3 этапов, так же называемым рукопожатием:

1. Клиент, который намеревается установить соединение, посылает серверу сегмент типа SYN. Сервер получает сегмент, запоминает номер последовательности и пытается создать сокет (предоставить ресурсы для обслуживания соединения на своей стороне), в случае успеха сервер отправляет клиенту сегмент типа SYN,ACK и переходит в состояние SYN-RECEIVED (получил запрос на соединение, отправил ответный запрос и ожидает подтверждения), в случае неудачи клиенту отправляется сегмент RST и установление соединения прекращается.
2. Если клиент получает сегмент типа SYN,ACK, то он переходит в состояние ESTABLISHED (соединение установлено, идет передача данных) и отправляет серверу сегмент типа ACK, если получает сегмент RST, то прекращает попытки установки соединения, если в течение 10 секунд ответ от сервера не получен, то попытка соединения повторяется заново.
3. Если сервер в состоянии SYN-RECEIVED получает от клиента сегмент типа ACK, то он так же переходит в состояние ESTABLISHED, соединение считается установленным, в противном случае после тайм-аута закрывает сокет (высвобождая ресурсы, зарезервированные на обслуживание соединения). Тайм-аут для закрытия сокета определяется параметрами операционной системы.

После успешной установки TCP-соединения может быть осуществлена передача данных от клиента серверу и в обратном направлении. По окончании передачи данных происходит процесс закрытия соединения.

Завершение соединения можно рассмотреть в три этапа:

1. Посылка серверу от клиента сегмента типа FIN на завершение соединения.
2. Сервер посылает клиенту сегменты типа ACK,FIN, что соединение закрыто.
3. После получения этих флагов клиент закрывает соединение и в подтверждение отправляет серверу сегмент типа ACK.

Максимальный размер TCP-сегмента так же как и в случае с протоколом UDP ограничивается значением MTU.

Поскольку процесс установки TCP-соединения достаточно долгий и трудоемкий как для клиента, так и для сервера, то был разработан и используется механизм Keepalive, который позволяет после завершения передачи данных между клиентом и сервером какое-то время держать соединение установленным для последующих передач. Для этого соединение закрывается не сразу, а только после определенного тайм-аута от последней успешной передачи данных или контрольного сообщения проверки соединения или состояния клиента и сервера, определенных обеими сторонами при установке соединения. Поскольку механизм Keepalive в протоколе TCP опциональный, то множество протоколов верхних уровней, использующих TCP в качестве транспорта, имеют свои собственные реализации механизма Keepalive.