# Лекция 2. ОБЗОР СТЕКА TCP\IP

## Основные положения

1. **Общая характеристика стека**

   Стек TCP\IP это 4-х уровневый сетевой стек, ставший стандартом де-факто области сетевой коммуникации. На этом стеке сейчас работает Интернет и подавляющее большинство локальных сетей.

   Исторически стек TCP\IP, который являлся результатом развития проекта ARPANET (1969), появился в рамках инициативы Internet Network Working Group (1974) и получил широкое распространения после включение его в поставку UNIX 4.2 BSD (1984). Развитие Интернет и появление WWW (1992) закрепило успех стека.

   К отличительным особенностям стека относятся:

   a. открытость.
   b. кроссплатформенность
   c. высокая степень абстракции канального уровня.

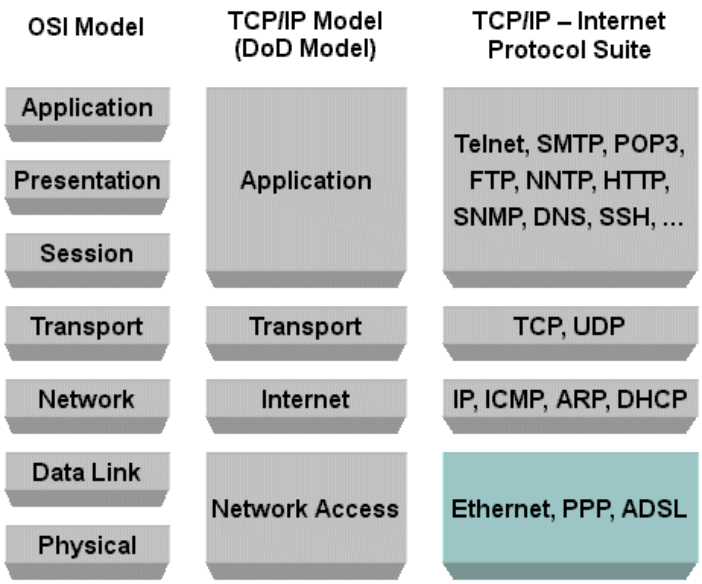
   Работу TCP\IP регламентируются RFC (Request for Comments) — пронумерованными документами, содержащими технические спецификации и стандарты. Управление RFC осуществляет IETF (Internet Engineering Task Force). Формально этой организации полномочия на такую деятельность переданы открытой организацией Internet Society (ISOC). Правами на RFC обладает именно Internet Society.

   Реализации сетка существуют для всех популярных ОС.

   Архитектуру стека отличает то, что им не описывается работа канальных протоколов, а лишь механизмы взаимодействия сетевого и канального уровней. Кроме этого, адресация сетевого уровня не связана с адресацией канального непосредственно. Все это позволяет адаптировать TCP\IP для работы с новыми канальными протоколами.

2. **Сравнение OSI и TCP\IP**

   Подобно OSI стек TCP\IP можно разбить на уровни. Однако количество уровней не 7, а 4. Для стека TCP\IP наиболее полное соответчике функций уровней функциям уровней модели OSI характерно для Транспортного и Сетевого уровней (Транспортного и Межсетевого в терминологии TCP\IP). Прикладному уровню соответствуют уровни Сеансный, Представления и Приложений модели OSI.



Еще раз отметим, что сущностно уровень Доступа к Сети стека TCP\IP не покрывает всех задач Канального и Физического уровней OSI.

## 3. Описание основных протоколов

Рассмотрим кратко назначение некоторых протоколов стека TCP\IP.

FTP (англ. File Transfer Protocol — протокол передачи файлов) – работает по протоколу TCP, порты 20 и 21. Предназначен для передачи файлов межу сервером и клиентом. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.

SMTP (англ. Simple Mail Transfer Protocol — простой протокол передачи почты) – работает по 25 порту TCP, предназначен для передачи сообщений электронной почты между клиентским программным обеспечением и сервером, а также между серверами. Не содержит стандартных средств авторизации отправителя (кроме расширений ESMTP для авторизации клиента).

POP3 (англ. Post Office Protocol Version 3 - протокол почтового отделения, версия 3) – работает по 110 порту TCP. Предназначен для получения клиентом почтовых сообщений с сервера. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.

IMAP4 (англ. Internet Message Access Protocol) — протокол прикладного уровня для доступа к электронной почте. Работает по 143 порту TCP. Предназначен для получения клиентом почтовых сообщений с сервера. Отличается возможностью хранения почтовых сообщений на сервере, их структурирование по каталогам и т.п.

HTTP (сокр. от англ. HyperText Transfer Protocol — протокол передачи гипертекста). Работает по портам 80, 8080 TCP. Предназначен для передачи текстовых и мультимедийных данных от сервера к клиенту по запросу последнего. В настоящее время используется как транспорт для других протоколов прикладного уровня.

RDP (англ. Remote Desktop Protocol — протокол удалённого рабочего стола). Работает по порту 3389 TCP. Протокол терминального доступа Microsoft. Существуют клиенты для различных операционных систем. Поддерживается отображение устройств клиентской стороны в терминальную сессию (принтеров, com-портов, аудиоустройств, смарткарт и дисковых устройств).

SSH (англ. Secure SHell — «безопасная оболочка») — сетевой протокол сеансового уровня

Telnet (англ. TErminaL NETwork — протокол терминального сетевого доступа). Работает по 21 порту TCP. Предназначен для организации полнодуплексного сетевого терминала между клиентом и сервером. Команды выполняются на стороне сервера. Поддерживает авторизацию по имени пользователя и паролю. Не защищен.

DNS (англ. Domain Name System — система доменных имён). Работает по портам 53 UDP для взаимодействия клиента и сервера и 53 TCP для AFXR запросов, поддерживающих обмен между серверами. DNS – протокол, поддерживающий работу одноименной распределённой системы, осуществляющей отображение множества доменных имен и множества IP адресов хостов.

LDAP (англ. Lightweight Directory Access Protocol — облегчённый протокол доступа к каталогам). Работает по портам 389 TCP и UDP. Предназначен для чтения, добавления и изменения данных, хранящимся в службе каталогов. Используется в Active Directory от Microsoft, Open LDAP и др.

TCP (анг. Transmission Control Protocol - протокол управления передачей). Протокол транспортного уровня, обеспечивающий установку двунаправленного соединения

между процессами, идентифицирующийся по сокету (комбинации IP адреса и порта), передачу потока сегментов внутри соединения с подтверждением приема, управление и завершение соединения. Сообщение TCP содержит в заголовке адреса сегментов в направленном потоке и контрольную сумму при расчете которой используется поле данных и заголовок. Для оптимизации передачи и предотвращения перегрузок сети используется механизм переменного окна, позволяющий вести передачу без получения подтверждения приема каждого сообщения. В качестве адресной информации использует порт.

UDP (англ. User Datagram Protocol — протокол пользовательских дейтаграмм). Протокол транспортного уровня, обеспечивающий передачу сообщений между процессами, идентифицирующимися по сокету (комбинации IP адреса и порта). Сеанс не устанавливается, подтверждения приема не осуществляется. В качестве адресной информации использует порт.

ICMP (англ. Internet Control Message Protocol — протокол межсетевых управляющих сообщений). Является диагностическим протоколом стека TCP\IP. Предназначен для запроса и оповещении о состояниях связи по протоколу IP и TCP, UDP. При передаче инкапсулируется в IP. Оповещение реализовано конечным количеством кодов запроса и кодов ответа. Пример ответов: код 3 — Порт недостижим, код 5 — Неверный маршрут от источника. Пример запросов: 8 — Эхо-запрос, 30 — Трассировка маршрута (RFC-1393).

ARP (англ. Address Resolution Protocol — протокол определения адреса). Используется для определения MAC адреса по известному IP адресу. Соотнесение реализуется путем широковещательных рассылок. Область действия ограничена локальной сетью.

RARP (англ. Reverse Address Resolution Protocol — Обратный протокол преобразования адресов). Решает задачу обратную ARP – определение MAC по известному IP.

IP (анг. Internet Protocol — межсетевой протокол). Предназначен для доставки сообщений по составной сети. Реализует доставку данных в пределах локальной сети как подмножество основной задачи. Не гарантирует доставку. Существует в двух версиях IPv4 и IPv6. В качестве адресной информации используется IP адреса, имеющие разный формат в разных версиях протокола.

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла). Предназначен для автоматического конфигурирования сетевого узла. В качестве конфигурационных параметров могут быть переданы: IP, mask, gate, адреса DNS, адрес сервера загрузки, сервера времени и т.п. Идентифицирует клиентов по MAC адресу к которому привязывается назначенный IP.

ESP (анг. Encapsulating Security Payload - инкапсуляция защищенных данных). Подпротокол IPSec. Предназначен для шифрования поля данных IP пакета. Реализуется за счет добавление служебного заголовка в поле данных IP пакета.

AH (анг. Authentication Header - идентификационный заголовок). Подпротокол IPSec. Предназначен для шифрования инкапсулированного IP пакета в IP пакете внешней сети. Реализуется за счет добавление служебного заголовка в поле данных IP пакета. Применяется дополнительно с ESP.

RIP (англ. Routing Information Protocol – протокол маршрутизации IP). Предназначен для автоматического составления таблиц маршрутизации. Является протоколом дистанционно-векторного типа. Алгоритм заключается в рассылке таблиц маршрутизации по соседям. Использует метрику маршрута, равную количеству промежуточных маршрутизаторов до сети назначения. Максимальное значение

метрики – 15. Существует в двух вариантах RIP1 и RIP2. Последний является актуальным. Является внутренним протоколом маршрутизации, т.е. ориентирован на работу внутри автономных систем.

OSPF (англ. Open Shortest Path First – открытие кратчайшего пути первым). Предназначен для автоматического составления таблиц маршрутизации. Основан на технологии отслеживания состояния канала. Использует для нахождения кратчайшего пути Алгоритм Дейкстры. Использует метрики, учитывающие пропускную способность канала. Является внутренним протоколом маршрутизации, т.е. ориентирован на работу внутри автономных систем.

BGP (англ. Border Gateway Protocol - протокол граничного шлюза). Работает через 179 порт TCP. Предназначен для автоматического составления таблиц маршрутизации. Является внешним протоколом маршрутизации. BGP поддерживает бесклассовую адресацию, при которой маршрутизаторы обмениваются уменьшенными таблицами маршрутизации полученными суммированием маршрутов.

PPTP (англ. Point-to-Point Tunneling Protocol - туннельный протокол типа точка-точка). Предназначен для туннелирования трафика по логической топологии точка-точка. Позволяет устанавливать защищённое соединение между двумя узлами путем инкапсуляции кадры PPP в IP. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

L2TP (англ. Layer 2 Tunneling Protocol - протокол туннелирования второго уровня). Предназначен для организации туннеля в том числе и на втором уровне модели OSI. То есть он позволяет создавать туннель не только в сетях IP, но и в таких, как ATM, X.25 и Frame Relay. Реализуется за счет добавление служебного заголовка в поле данных внешнего кадра или IP реализуется за счет добавление служебного заголовка в поле данных кадра или IP пакета в которые производится инкапсуляция Рассмотрим, пусть и очень поверхностно, физические аспекты передачи сигнала. Важнейшим моментом здесь является положение о принципиальной разложимости периодической функции в рад Фурье (ряд, где члены это sin или cos с различными амплитудами, частотами и фазами).

**4. Поток данных по стеку**

Рассмотрим поток данных по стеку TCP\IP.


В общем случае прикладной протокол формирует символьный поток, где данные перемежаются с командами протокола.

На транспортном уровне данные передаются по протоколу UDP (если не нужна надежная доставка) или по протоколу TCP, если нужна проверка целостности

передаваемых данных. Использование того или иного протокола определяется реализацией приложения.

Сегменты TCP или дейтаграммы UDP инкапсулируются в пакеты IP (по сути, пакеты тоже являются дейтаграммами), а затем пакеты инкапсулируются в кадры канального уровня.

Отметим, что в настоящее время на смену TCP приходят другие протоколы, и, в частности, QUIC.

## 5. Адресация в TCP\IP и установка соединений

Рассмотрим адресную информацию на разных уровнях стека TCP\IP.

К адресам уровня приложений относятся адреса DNS – www.itmo.ru. По сути, это прикладной сервис, предоставляющий пользователю удобный сервис строковых имен.

На транспортном уровне адрес это номер порта (TCP или UDP). Порт это двухбайтный номер очереди, которую захватывает приложение, когда передает данные через сетевой стек. Приложение читает и пишет данные в стек через один номер порта. Но через один порт может передаваться множество потоков данных, идентифицирующимися сокетами взаимодействующих приложений (см. далее).

На сетевом уровне используется IP адрес, например - 51.8.12.64. Это адрес хоста в IP сети.

На канальном уровне работают – MAC адреса. В стеке TCP\IP есть протоколы, обеспечивающие отображение пространства IP адресов на пространство MAC адресов и обратно (ARP\RARP).

Существуют синтетические адреса: сокет, комбинация IP адреса и порта ( 87.250.250.242:443) и URL - Унифицированный указатель ресурса, включающий название протокола, адрес хоста, порт, путь до ресурса, имя ресурса и указатель данных внутри ресурса. https://www.ya.ru/...

## 6. Адреса IPv4

Все пространство IP адресов делится на логические группы – IP-сети предназначенные для организации иерархической адресации в составной IP-сети, например Интернете. Каждой локальной сети присваивается одна или несколько IP-сетей. Маршрут до IP-узлов, находящихся в этой локальной сети, строится на маршрутизаторах как маршрут до их IP-сети. Только после того, как пакет попал в конкретную IP-сеть, решается задача его доставки на отдельный узел.

**IP-адрес** – это уникальный числовой адрес, который однозначно идентифицирует узел, группу узлов или сеть.

IPv4-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел «**октетов**», разделенных точками – W.X.Y.Z Каждый октет может принимать значения в диапазоне от 0 до 255.

В IP-адресе выделяются две части – адрес сети и адрес узла.

Существует два способа делить адрес на эти части:

a. деление с помощью классов,
b. деление с помощью масок.

Деление с помощью классов устарело. Но его необходимо знать, так как оно все еще используется для того, чтобы разделять пространство адресов IPv4 по назначению. Разделяются адреса на классы по первым битам первого байта (см. таблицу 1). При

этом для адресации хостов используются только классы A, B, C. Класс D – для многоадресных рассылок. Класс E – не используется вовсе.

| класс | первые биты | распределение байт (C — сеть, X — хост) | число возможных сетей | число возможных хостов | маска подсети | начальный адрес | конечный адрес |
|---|---|---|---|---|---|---|---|
| A | 0 | C.X.X.X | 126 | 16 777 214 | 255.0.0.0 | 1.0.0.0 | 126.255.255.255 |
| B | 10 | C.C.X.X | 16 384 | 65 534 | 255.255.0.0 | 128.0.0.0 | 191.255.255.255 |
| C | 110 | C.C.C.X | 2 097 152 | 254 | 255.255.255.0 | 192.0.0.0 | 223.255.255.255 |
| D | 1110 | групповой адрес | | | | 224.0.0.0 | 239.255.255.255 |
| E | 1111 | зарезервировано | | | | 240.0.0.0 | 255.255.255.255 |

Таблица 1. Классы IPv4 адресов.

Деление с помощью масок происходит с помощью 4-х байтного числа, которое поставлено в соответствие IP-адресу. Макса содержит двоичные 1 в тех разрядах IP-адреса, которые определяют адрес сети и двоичные 0 в тех разрядах IP адреса, которые определяют адрес узла.

Адресом IP-сети считается IP-адрес из этой сети, в котором в поле адреса узла содержатся двоичные 0. Этот адрес обозначает сеть целиком в таблицах маршрутизации. Есть еще служебный IP-адрес – адрес ограниченного широковещания – в поле адреса узла он содержит двоичные 1. Оба эти адреса не используются для адресации реальных узлов сети, однако входят в диапазон адресов IP-сети.

Рассмотрим пример: есть адрес 192.168.170.15 с маской 255.255.252.0. Определим адрес сети, адрес широковещания и допустимый для данной IP-сети диапазон адресов.

| | | | | |
|---|---|---|---|---|
| DEC IP | 192 | 168 | 170 | 15 |
| DEC MASK | 255 | 255 | 252 | 0 |
| BIN IP | 11000000 | 10101000 | 10101010 | 00001111 |
| BIN MASK | 11111111 | 11111111 | 11111100 | 00000000 |
| | С фоном – адрес сети, без фона – адрес узла | | | |
| BIN IP сети | 11000000 | 10101000 | 10101000 | 00000000 |
| | скопируем сетевую часть IP и заполним узловую часть 0 | | | |
| DEC IP сети | 192 | 168 | 168 | 0 |
| BIN IP | 11000000 | 10101000 | 10101011 | 11111111 |

| | Адрес широковещания (скопируем сетевую часть IP и заполним узловую часть 1) | | | |
|---|---|---|---|---|
| DEC IP широковещания | 192 | 168 | 171 | 255 |
| Начало диапазона IP-адресов для узлов | 192 | 168 | 168 | 1 |
| | (значение поля узла +1 к IP адресу сети) | | | |
| Окончание диапазона IP-адресов для узлов | 192 | 168 | 171 | 254 |
| | (значение поля узла -1 от IP-адреса широковещания) | | | |

Таблица 2. Пример вычисления адреса

Если имеется сеть, составленная из нескольких локальных сетей, соединенных между собой маршрутизаторами, то нужно каждой из этих локальных сетей назначить отдельную IP-сеть. В случае, если для такой сети выдается большая IP-сеть в управление (например, такую сеть может назначить провайдер Интернет), то эту сеть необходимо разделить с помощью масок на части. В таблице 3 приведены значения некоторых масок.

| Маска | Количество двоичных 0 | Количество всех адресов в IP сети с такой маской |
|---|---|---|
| 255.255.255.252 | 00 | 4 |
| 255.255.255.248 | 000 | 8 |
| 255.255.255.240 | 0000 | 16 |
| 255.255.255.224 | 00000 | 32 |
| 255.255.255.192 | 000000 | 64 |
| 255.255.255.128 | 0000000 | 128 |
| 255.255.255.0 | 00000000 | 256 |
| 255.255.254.0 | 0.00000000 | 512 |

Таблица 3. Примеры масок IP сетей

Маски могут записываться в виде указания после IP-адреса через слеш количества двоичных единиц в маске. Например, для 255.255.255.0 - /24.

Выделяют особую IP сеть - 127.0.0.0 / 24 – это подсеть, все адреса которой означают сам хост отправитель для самого отправителя. Любой адрес из этой сети используется для того, чтобы хост мог обратиться к самому себе.

Так же в каждом классе адресов выделяют специальные диапазоны для использования в сетях, не являющихся частью Интернета:

10.0.0.0 — 10.255.255.255 (маска -255.0.0.0 или /8)

172.16.0.0 — 172.31.255.255 (маска 255.240.0.0 или /12)

192.168.0.0 — 192.168.255.255 (маска255.255.0.0 или /16)

Эти адреса гарантировано не будут встречаться в Интернет.

**7. Адреса IPv6**

В протоколе IPv6 размер адреса составляет 128 бит. Предпочтительным является следующее представление адреса IPv6: x:x:x:x:x:x:x:x, где каждая буква x — это шестнадцатеричные значения шести 16-битных элементов адреса.
Диапазон адресов IPv6 составляет от
0000:0000:0000:0000:0000:0000:0000:0000
до
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Используется соглашение по сокращению адреса IPv6. Можно не указывать **ведущие** нули в группах и сокращать **последнюю** группу из двоичных нулей.
Так, адрес:
2001:0DB8:00AF:ABCD:0000:0000:0000:0034
Будет сокращен при записи до:
2001:DB8:AF:ABCD::34

Адреса IPv6 тоже делятся на сетевую и узловую часть с помощью префикса (подобия маски, для IPv6). Префикс, это количество бит с начала адреса, отводящихся под адрес сети.

Выделяют несколько типов адресов:
Global unicast адрес - аналог адреса IPv4 из диапазона Интернет. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически. Начинается с 2 или с 3. От 2000 до 3FFF.
Link-local - Local IPv6-адрес канала позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 по одному и тому же каналу (локальной сети). Не является аналогом «серого» IPv4. Локальные IPv6-адреса канала находятся в диапазоне FE80::/10. /10
Loopback-адрес используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 - ::1/128 или просто ::1.
Unspecified адрес - неопределённый адрес состоит из нулей и в сжатом формате представлен как ::/128 или просто :: Он не может быть назначен интерфейсу и используется только в качестве адреса источника в IPv6-пакете. Неопределённый адрес используется в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес.
Unique local — IPv6-адреса имеют некоторые общие особенности с «серыми» адресами IPv4, но имеют и значительные отличия. Находятся в диапазоне от FC00::/7 до FDFF::/7. Хотя протокол IPv6 обеспечивает особую адресацию для сайтов, он не предназначен для того, чтобы скрывать внутренние устройства под управлением IPv6 от Интернета IPv6.
IPv4 embedded – адреса для обеспечения перехода с протокола IPv4 на IPv6..
Выглядят как ::73.3.68.45

**8. Типы рассылок в TCP\IP**

Сетевой уровень стека TCP\IP предполагает три вида рассылок для IPv4:

a. Одноадресные. Используются для передачи данных конкретному адресату. Адреса отправителя и получателя, как на сетевом уровне, так и на канальном принадлежат конкретным хостам.
b. Широковещательные. Используются для доставки сообщений всем узлам в локальной сети, например для поиска сервисов или узлов. Адрес канального уровня всегда FF:FF:FF:FF:FF:FF, адрес сетевого уровня или 255.255.255.255 или IP-широковещания.
c. Многоадресные рассылки используются для отправки одного пакета сразу группе узлов. Сетевой адрес – адрес из сети класса D, а канальный адрес – адрес ассоциированного узла, например маршрутизатора, который будет рассылать пакет. Для IPv6 предусмотрены:
a. Одноадресные рассылки,
b. Anycast рассылки, когда адреса назначаются группе интерфейсов, обычно принадлежащих различным узлам. Пакет, отправленный на такой адрес, доставляется на один из интерфейсов данной группы, как правило наиболее близкий к отправителю с точки зрения протокола маршрутизации.
c. Multicast рассылки, когда адрес также используется группой узлов, но пакет, отправленный на такой адрес, будет доставлен каждому узлу в группе.
d. Бродкаста нет

## Основные термины

1. Дейтаграмма – сообщение не требующее подтверждение приема.
2. Сегмент – сообщение, представляющее собой часть потока и требующее подтверждения приема данных.
3. RCF - Request for Comments — пронумерованными документами, содержащими технические спецификации и стандарты TCP\IP, управляемые IETF (Internet Engineering Task Force).
4. Адрес сети – IP адрес, содержащий двоичные 0 в поле адреса узла.
5. Адрес широковещания - IP адрес, содержащий двоичные 1 в поле адреса узла.
6. Unicat (юникаст) – одноадресаня рассылка от узла к узлу.
7. Broadcast – широковещательная рассылка в пределах локальной сети от узла ко всем остальным узлам в LAN.
8. Multicats – многоадресная рассылка, от узла к группе узлов.
9. Маска – для IPv4 4-х байтное число, которое поставлено в соответствие IP-адресу и содержит двоичные 1 в тех разрядах IP-адреса, которые определяют адрес сети и двоичные 0 в тех разрядах IP адреса, которые определяют адрес узла.
10. Префикс - для IPv6 число разрядов адреса, отводимых под адрес сети.

## Персоналии

Винтон Серф (Vinton Cerf) – американский учёный в области теории вычислительных систем, один из разработчиков стека протоколов TCP/IP, нередко называемый «отцом интернета».

## Дополнительная литература


1. https://www.rfc-editor.org
2. http://rfc.com.ru
3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020 г.
4. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб.: Питер, 2019 г.