**Лекция 8-9. Стандарты и стеки протоколов**

1. **Стандарты IEEE 802**

Спецификации IEEE 802 (Institute of Electrical and Electronics Engineers) определяют стандарты для физических компонентов сети. Эти компоненты – ***сетевая карта*** (Network Interface Card – NIC) и ***сетевой носитель*** (network media), которые относятся к физическому и канальному уровням модели OSI. Спецификации IEEE802 определяют механизм доступа адаптера к каналу связи и механизм передачи данных. Стандарты IEEE 802 подразделяют канальный уровень на подуровни:

Logical Link Control (LLC) – *подуровень управления логической связью*;

Media Access Control (MAC) – *подуровень управления доступом к устройствам*.

Существует более двадцати спецификаций IEEE 802.

***Стандарт IEEE 802.1*** (Internetworking – *объединение сетей*) задает механизмы управления сетью на MAC-уровне. В разделе 802.1 приводятся основные понятия и определения, общие характеристики и требования к локальным сетям, а также поведение маршрутизации на канальном уровне, где логические адреса должны быть преобразованы в их физические адреса и наоборот.

***Стандарт IEEE 802.2*** (Logical Link Control – *управление логической связью*) определяет функционирование подуровня LLC на канальном уровне модели OSI. LLC обеспечивает интерфейс между методами доступа к среде и сетевым уровнем.

***Стандарт IEEE 802.3*** (Ethernet Carrier Sense Multiple Access with Collision Detection – *CSMA/CD* LANs Ethernet – *множественный доступ к сетям Ethernet с проверкой несущей и обнаружением конфликтов*) описывает физический уровень и подуровень MAC для сетей, использующих шинную топологию и множественный доступ с прослушиванием несущей и обнаружением коллизий (конфликтов). Прототипом этого метода является метод доступа стандарта Ethernet (10BaseT, 10Base2, 10Base5). Метод доступа CSMA/CD. 802.3 также включает технологии Fast Ethernet (100BaseTX, 100BaseFX, 100BaseFX):

100Base-TХ – двухпарная витая пара; использует метод MLT-3 для передачи сигналов 5-битовых порций кода 4В/5B по витой паре, а также имеется функция автопереговоров (Auto-negotiation) для выбора режима работы порта;

100Base-T4 – четырехпарная витая пара; вместо кодирования 4B/5В в этом методе используется кодирование 8B/6T.

100BaseFХ – многомодовое оптоволокно. Эта спецификация определяет работу протокола Fast Ethernet по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах на основе хорошо проверенной схемы кодирования и передачи оптических сигналов, использующейся уже на протяжении ряда лет в стандарте FDDI. Как и в стандарте FDDI, каждый узел соединяется с сетью двумя оптическими волокнами, идущими от приемника и от передатчика.

Этот метод доступа используется в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения – это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме **множественного доступа** (multiply access – MA).

Метод доступа *CSMA/CD* определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети.

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

***Стандарт IEEE 802.4*** (Token Bus LAN – *локальные сети Token Bus*) определяет метод доступа к шине с передачей маркера, прототип – ArcNet.

При подключении устройств в ArcNet применяют топологию «шина» или «звезда». Адаптеры ArcNet поддерживают метод доступа Token Bus (маркерная шина) и обеспечивают производительность 2,5 Мбит/с. Этот метод предусматривает следующие правила:

все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);

в любой момент времени только одна станция в сети обладает таким правом;

кадр, передаваемый одной станцией, одновременно анализируется всеми остальными станциями сети.

В сетях ArcNet используется асинхронный метод передачи данных (в сетях Ethernet и Token Ring применяется синхронный метод), т.е. передача каждого байта в ArcNet выполняется посылкой ISU (Information Symbol Unit – единица передачи информации), состоящей из трех служебных старт/стоповых битов и восьми битов данных.

***Стандарт IEEE 802.5*** (Token Ring LAN – *локальные сети Token Ring*) описывает метод доступа к кольцу с передачей маркера, прототип – Token Ring.

Сети стандарта Token Ring, как и сети Ethernet, используют разделяемую среду передачи данных, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо. Кольцо рассматривается как общий разделяемый ресурс, и для доступа к нему используется алгоритм, основанный на передаче станциями права на использование кольца в определенном порядке. Право на использование кольца передается с помощью маркера, или токена.

***Стандарт IEEE 802.6*** (Metropolitan Area Network – *городские или муниципальные сети*) описывает рекомендации для региональных сетей.

***Стандарт IEEE 802.7*** (Broadband Technical Advisory Group – *техническая консультационная группа по широковещательной передаче*) описывает рекомендации по широкополосным сетевым технологиям, носителям, интерфейсу и оборудованию.

***Стандарт IEEE 802.8*** (Fiber Technical Advisory Group – *техническая консультационная группа по оптоволоконным сетям*) содержит обсуждение использования оптических кабелей в сетях со стандартом 802.3 – 802.6, а также рекомендации по оптоволоконным сетевым технологиям, носителям, интерфейсу и оборудованию, прототип – сеть *FDDI* (Fiber Distributed Data Interface).

Стандарт FDDI использует оптоволоконный кабель и доступ с применением *маркера*. Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Использование двух колец – это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят им воспользоваться, должны быть подключены к обоим кольцам. Скорость сети – до 100 Мбит/с. Данная технология позволяет включать до 500 узлов на расстоянии 100 км.

***Стандарт IEEE 802.9*** (Integrated Voice and Data Network – *интегрированные сети передачи голоса и данных*) задает архитектуру и интерфейсы устройств одновременной передачи данных и голоса по одной линии, а также содержит рекомендации по гибридным сетям, в которых объединяют голосовой трафик и трафик данных в одной и той же сетевой среде.

В ***стандарте IEEE 802.10*** (Network Security – *сетевая безопасность*) рассмотрены вопросы обмена данными, *шифрования* (на основе криптографического преобразования информации), управления сетями и безопасности в сетевых архитектурах, совместимых с моделью OSI.

***Стандарт IEEE 802.11*** (Wireless Network – *беспроводные сети*) описывает рекомендации по использованию беспроводных сетей.

***Стандарт IEEE 802.12*** описывает *рекомендации по использованию сетей 100VG* – AnyLAN со скоростью100 Мб/с и методом доступа по очереди запросов и по приоритету (Demand Priority Queuing – DPQ, Demand Priority Access – DPA).

Технология *100VG* – это комбинация Ethernet и Token-Ring со скоростью передачи 100 Мбит/c, работающая на *неэкранированных витых парах*. В проекте 100Base-VG усовершенствован метод доступа с учетом потребности мультимедийных приложений. В спецификации *100VG* предусматривается поддержка волоконно-оптических кабельных систем. Технология 100VG использует метод доступа – *обработка запросов по приоритету* (*demand priority access*). В этом случае узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу, а затем разрешает этот запрос в соответствии с приоритетом. Имеется два уровня приоритетов – высокий и низкий.

***Стандарт IEEE 802.14*** определяет *функционирование кабельных модемов*.

***Стандарт IEEE 802.15*** (PAN – Personal Area Network, *персональные сети*) рассматривает вопросы организации персональных сетей. В настоящее время уже существует несколько спецификаций данного стандарта.

1. ***Стандарт IEEE 802.15.1*** базируется на спецификациях Bluetooth v1.x. и предназначен для построения так называемых персональных беспроводных сетей (Wireless Personal Area Network, WPAN). Для работы радиоинтерфейса *Bluetooth* используется так называемый нижний (2,45 ГГц) диапазон ISM (industrial, scientific, medical), предназначенный для работы промышленных, научных и медицинских приборов.

2. ***Стандарт IEEE 802.15.3*** предназначен для *беспроводных частных сетей* и является прямым наследником Bluetooth (частота 2,4 ГГц). IEEE 802.15.3 обеспечивает скорость передачи данных до 55 Мбит/с на расстоянии до 100 метров, одновременно работать в такой сети могут до 245 пользователей. Шифрование данных в сетях IEEE 802.15.3 может осуществлятся по стандарту AES 128.

3***. Стандарт IEEE 802.15.4*** (ZigBee) ориентирован, главным образом, на использование в качестве средства связи между автономными приборами и оборудованием.

4. ***Стандарт IEEE 802.15.4a*** (Ultra Wideband, UWB) базируется на технологии сверхширокополосной связи (Ultra Wideband, UWB) основана на передаче множества закодированных импульсов негармонической формы очень малой мощности и малой длительности в широком диапазоне частот.

***Стандарт IEEE 802.16*** предназначен для реализации широкополосных каналов в городских сетях (MAN). В отличии от 802.11 он ориентирован для соединения стационарных, а не мобильных объектов. Его задачей является обеспечения сетевого уровня между локальными сетями (IEEE 802.11) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE802.20. Эти стандарты совместно со стандартом IEEE 802.15 и 802.17 образуют взаимосогласованную иерархию протоколов беспроводной связи.

***Стандарт IEEE 802.17*** называется RPR (Resilient Packet Ring –*адаптивное кольцо для пакетов*), и в отличие от FDDI (а также Token Ring или DQDB) пакеты удаляются из кольца узлом-адресатом, что позволяет осуществлять несколько обменов одновременно.

***Стандарт IEEE* *802.18***  представляет собой требования и рекомендации технической консультативной группы по радиочастотному регулированию – RTAG (*Radio Regulatory Technical Advisory Group*).

***Стандарт* *IEEE* *802.19*** представляет собой  требования и рекомендации технической консультативной группы по сосуществованию – CTAG (*Coexistence Technical Advisory Group*).

***Стандарт* *IEEE* *802.20*** описывает правила беспроводного мобильного широкополосного доступа MBWA (*Mobile Broadband Wireless Access*) для пакетного интерфейса в беспроводных городских сетях WMAN. Этот стандарт должен поддерживать услуги по передаче данных с IP в качестве транспортного протокола и дополнять стандарт IEEE 802.16 в масштабе WiMAX. Стандарт обеспечит скорость передачи данных более 1 Мбит/с и позволит получить мобильный доступ к данным из движущихся транспортных средств (если скорость их не превышает 250 км/ч). Для беспроводного интерфейса HPI (Highspeed Portable Internet) устанавливаются уровни скорости передачи и безопасности. Быстродействие HPI выше, чем универсальной системы мобильной связи UMTS, которая ориентирована на передачу голоса. Стандарт обеспечивает подключение ПК в небольших и домашних офисах (SOHO) как альтернативу сетей «последней мили» по медным или оптическим кабелям, использующим технологии DSL.

***Стандарт* *IEEE* *802.21 –***это стандарт независимой от среды эстафетной передаче соединений – MIHS (*Media Independent Handover Services*).

***Стандарт IEEE* *802.22*** – определяет функционирование беспроводных региональных сетей WRAN (*Wireless Regional Area Network*), использующих для передачи данных телевизионные частотные диапазоны.

***Стандарт IEEE* *802.23*** – этот стандарт определяет независимую от среды структуру в рамках IEEE 802 для обеспечения согласованного доступа к данным. Сюда входит интерфейс уровня канала передачи данных для согласованного просмотра сетей IEEE 802 с помощью возможностей служб экстренной помощи на основе протокола IP.

***Стандарт IEEE* *802.24*** –технологии IEEE 802 применяются для поддержки вертикальных приложений. В данном контексте стандарт IEEE 802.24 определяет, что делают горизонтальные технологии в поддержке приложений. Примерами потенциальных категорий вертикальных приложений могут выступать: умные сети, интеллектуальные транспортные системы (ITS), умные дома, умные города, электронное здравоохранение и т.д.

***Стандарт IEEE* *802.25*** (пока не ратифицирован) – затаргивает вопросы организации Omni-Range Area Network.

1. **Протоколы и стеки протоколов**

Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются **протоколами**.

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется **стеком протоколов**.

Для каждого уровня определяется набор функций-запросов для взаимодействия с вышележащим уровнем, который называется **интерфейсом**.

Существует достаточно много стеков протоколов, широко применяемых в сетях. Это и стеки, являющиеся международными и национальными стандартами, и фирменные стеки, получившие распространение благодаря распространенности оборудования той или иной фирмы. Примерами популярных стеков протоколов могут служить стек IPX/SPX фирмы Novell, стек TCP/IP, используемый в сети Internet и во многих сетях на основе операционной системы UNIX, стек OSI международной организации по стандартизации, стек DECnet корпорации Digital Equipment и некоторые другие.

В общем случае можно выделить три укрупненных уровня протоколов, характерных в той или иной степени для любых стеков:

* сетевые;
* транспортные;
* прикладные.

*Протоколы сетевого уровня*

Сетевые протоколы предоставляют следующие услуги: адресацию и маршрутизацию информации, проверку на наличие ошибок, запрос повторной передачи и установление правил взаимодействия в конкретной сетевой среде. Ниже приведены наиболее популярные сетевые протоколы:

DDP (Datagram Delivery Protocol, протокол доставки дейтаграмм). *Протокол передачи данных Apple*, используемый в Apple Talk;

IP (Internet Protocol, протокол Internet). *Протокол стека TCP/IP*, обеспечивающий адресную информацию и информацию о маршрутизации;

IPX (Internetwork Packet eXchange, межсетевой обмен пакетами) в NWLink. *Протокол Novel NetWare*, используемый для маршрутизации и направления пакетов;

NetBEUI (NetBIOS Extended User Interface, расширенный пользовательский интерфейс базовой сетевой системы ввода/вывода). Разработан совместно IBM и Microsoft, обеспечивает транспортные услуги для NetBIOS.

*Протоколы транспортного уровня*

Транспортные протоколы предоставляют услуги надежной транспортировки данных между компьютерами. Ниже приведены наиболее популярные транспортные протоколы:

ATP (Apple Talk Protocol, транзакционный протокол Apple Talk) и NBP (Name Binding Protocol, *протокол связывания имен*). Сеансовый и транспортный протоколы Apple Talk;

NetBIOS (Network Basis Input/Output System, *базовая сетевая система ввода вывода*). NetBIOS устанавливает соединение между компьютерами, а NetBEUI предоставляет услуги передачи данных для этого соединения;

SPX (Sequenced Packet eXchange, последовательный обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для обеспечения доставки данных;

TCP (Transmission Control Protocol, протокол управления передачей). Протокол стека TCP/IP отвечает за надежную доставку данных.

*Протоколы прикладного уровня*

Прикладные протоколы отвечают за взаимодействие приложений. Ниже приведены наиболее популярные прикладные протоколы:

AFP (Apple Talk File Protocol, файловый протокол Apple Talk). *Протокол удаленного управления файлами Macintosh*;

FTP (File Transfer Protocol, протокол передачи файлов). *Протокол стека TCP/IP*, используемый для обеспечения услуг по передаче файлов;

NCP (NetWare Core Protocol, *базовый протокол NetWare*). Оболочка и редиректоры клиента Novel NetWare;

SNMP (Simple Network Management Protocol, *простой протокол управления сетью*). Протокол стека TCP/IP, используемый для управления и наблюдения за сетевыми устройствами;

HTTP (Hyper Text Transfer Protocol) – протокол *передачи гипертекста* и другие протоколы.

**3. Стек OSI**

Следует различать стек протоколов OSI и модель OSI (рис. 1). **Стек OSI** – это набор вполне конкретных спецификаций протоколов, образующих согласованный стек протоколов. Этот стек протоколов поддерживает правительство США в своей программе GOSIP. Стек OSI, в отличие от других стандартных стеков, полностью соответствует модели взаимодействия OSI и включает спецификации для всех семи уровней модели взаимодействия открытых систем. На физическом и канальном уровнях стек OSI поддерживает спецификации Ethernet, Token Ring, FDDI, а также протоколы LLC, X.25 и ISDN.

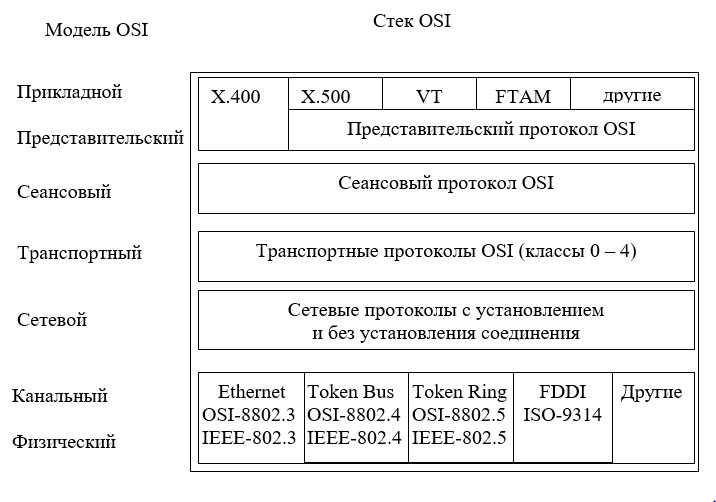


Рис. 1. Стек OSI

На сетевом уровне реализованы протоколы как без установления соединений, так и с установлением соединений. Транспортный протокол стека OSI скрывает различия между сетевыми сервисами с установлением соединения и без установления соединения, так что пользователи получают нужное качество обслуживания независимо от нижележащего сетевого уровня. Для обеспечения этого транспортный уровень требует, чтобы пользователь задал нужное качество обслуживания. Определено 5 классов транспортного сервиса: от низшего класса 0 до высшего класса 4, которые отличаются степенью устойчивости к *ошибкам* и требованиями к восстановлению данных после ошибок.

Сервисы прикладного уровня включают передачу файлов, эмуляцию терминала, службу каталогов и почту. Из них наиболее перспективными являются служба каталогов (стандарт Х.500), электронная почта (Х.400), протокол виртуального терминала (VT), протокол передачи, доступа и управления файлами (FTAM), протокол пересылки и управления работами (JTM). В последнее время ISO сконцентрировала свои усилия именно на сервисах верхнего уровня.

**4. Архитектура стека протоколов TCP/IP**

Набор многоуровневых протоколов, или как называют **стек TCP/IP**, предназначен для использования в различных вариантах сетевого окружения.

Стек TCP/IP позволяет обмениваться данными по сети приложениям и службам, работающим практически на любой платформе, включая Unix, Windows, Macintosh и другие.

Стандартная реализация TCP/IP (например, фирмы Microsoft) соответствует четырехуровневой модели вместо семиуровневой модели, как показано на рис. 2.

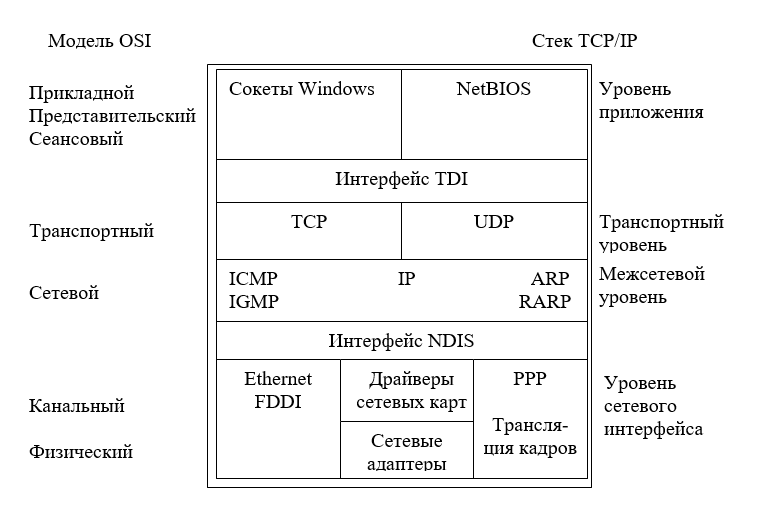


Рис. 2. Соответствие семиуровневой модели OSI и четырехуровневой модели TCP/IP

Отметим, что в целом с позиции логики организации взаимодействия модель TCP/IP соответствует модели OSI, однако некоторые функции перераспределены, либо сгруппированы.

В итоге, модель TCP/IP включает большее число функций на один уровень, что приводит к уменьшению числа уровней. В модели используются следующие уровни:

уровень *Приложения* модели TCP/IP соответствует *Прикладному*, *Представительскому* и *Сеансовому* уровням модели OSI;

*Транспортный уровень* модели TCP/IP соответствует аналогичному уровню модели OSI;

*Межсетевой* уровень модели TCP/IP выполняет те же функции, что и *Сетевой уровень* модели OSI;

уровень С*етевого интерфейса* модели TCP/IP соответствует *Канальному* и *Физическому* уровням модели OSI.

В табл. 1 приведено семейство протоколов TCP/IP.

Таблица 1

**Назначение протоколов TCP/IP**

|  |  |
| --- | --- |
| Название протокола | Описание протокола |
| WinSock | Сетевой программный интерфейс |
| NetBIOS | Связь с приложениями ОС Windows |
| TDI | Интерфейс транспортного драйвера (Transport Driver Interface); позволяет создавать компоненты сеансового уровня |
| TCP | Протокол управления передачей (Transmission Control Protocol) |
| UDP | Протокол пользовательских дейтаграмм (User Datagram Protocol) |
| ARP | Протокол разрешения адресов (Address Resolution Protocol) |
| RARP | Протокол обратного разрешения адресов (Reverse Address Resolution Protocol) |
| IP | Протокол Internet (Internet Protocol) |
| ICMP | Протокол управляющих сообщений Internet (Internet Control Message Protocol) |
| IGMP | Протокол управления группами Интернета (Internet Group Management Protocol) |
| NDIS | Интерфейс взаимодействия между драйверами транспортных протоколов |
| FTP | Протокол пересылки файлов (File Transfer Protocol) |
| TFTP | Простой протокол пересылки файлов (Trivial File Transfer Protocol) |

***Уровень Приложения***

Через уровень *Приложения* модели TCP/IP приложения и службы получают доступ к сети. Доступ к протоколам TCP/IP осуществляется посредством двух программных интерфейсов API: сокеты Windows и NetBIOS.

**Интерфейс сокетов Windows**, или как его называют *WinSock*, является сетевым программным интерфейсом, предназначенным для облегчения взаимодействия между различными TCP/IP – приложениями и семействами протоколов.

**NetBIOS –** это протокол для работы в локальных сетях на персональных компьютеров типа IBM/PC, разработан в виде интерфейса, который не зависит от фирмы-производителя. В стеке TCP/IP используется для связи между процессами (IPC – Interposes Communications) служб и приложений ОС Windows. В целом NetBIOS обеспечивает:

* регистрацию и проверку сетевых имен;
* установление и разрыв соединений;
* связь с подтверждением доставки информации;
* связь без подтверждения доставки информации;
* поддержку управления и мониторинга драйвера и сетевой карты.

***Транспортный уровень***

Транспортный уровень TCP/IP отвечает за установление и поддержание соединения между двумя узлами, а также за обеспечение, при необходимости, надежности передачи.

Основные функции уровня:

* подтверждение получения информации и обеспечение надежности передачи;
* управление потоком данных;
* упорядочение и ретрансляция пакетов.

В зависимости от типа службы могут быть использованы два протокола:

TCP (Transmission Control Protocol – *протокол управления передачей*);

UDP (User Datagram Protocol – *пользовательский протокол дейтаграмм*).

TCP обычно используют в тех случаях, когда приложению требуется передать большой объем информации и убедиться, что данные получены адресатом в неизменном виде. Приложения и службы, отправляющие небольшие объемы данных и не нуждающиеся в получении подтверждения, используют протокол UDP, который является протоколом без установления соединения. На практике протокол UDP логично использовать для передачи служебных сообщений.

**Протокол управления передачейTCP** отвечает за надежную передачу данных от одного узла сети к другому. Он создает сеанс с установлением соединения, иначе говоря, виртуальный канал между машинами. Установление соединения происходит в три шага.

1. Клиент, запрашивающий соединение, отправляет серверу пакет, указывающий номер порта, который клиент желает использовать, а также код (определенное число) ISN (Initial Sequence number).
2. Сервер отвечает пакетом, содержащим ISN сервера, а также ISN клиента, увеличенный на 1.
3. Клиент должен подтвердить установление соединения, вернув ISN сервера, увеличенный на 1.

Трехступенчатое открытие соединения устанавливает номер порта, а также ISN клиента и сервера. Каждый, отправляемый TCP-пакет содержит номера TCP-портов отправителя и получателя, номер фрагмента для сообщений, разбитых на меньшие части, а также контрольную сумму, позволяющую убедиться, что при передаче ошибок не произошло.

В отличие от TCP **пользовательский протокол дейтаграммUDP** не устанавливает соединения. Протокол UDP предназначен для отправки пакетов (например, служебных) без установки соединения и используется приложениями, которые не нуждаются в подтверждении адресатом их получения. UDP также использует номера портов для определения конкретного процесса по указанному IP-адресу. Однако UDP-порты отличаются от TCP-портов и, следовательно, могут использовать те же номера портов, что и TCP, без конфликта между службами.

Таким образом протокол **TCP** отличается от **UDP** по следующим ключевым моментам:

1. TCP устанавливает соединение с получателем, а UDP нет.
2. TCP требует подтверждение передачи, а UDP нет.
3. TCP для обеспечения целостности передаваемых данных использует средства коррекции ошибок, а UDP нет.
4. TCP иUDPпринципиально по-разному работают с очередями пакетов. Так, TCP использует буферы для корректного хранения и обработки все пришедших пакетов, а UDP может хранить в очереди только один пакет и поэтому следующий пришедший пакет приведет к сбросу уже имеющегося в очереди на обработку пакета.

***Межсетевой уровень***

Межсетевой уровень отвечает за маршрутизацию данных внутри сети и между различными сетями, решая при этом функции сетевого и частично канального уровней модели OSI. На этом уровне работают маршрутизаторы, которые зависят от используемого протокола и используются для отправки пакетов из одной сети (или ее сегмента) в другую (или другой сегмент сети).

В стеке TCP/IP на этом уровне используется протоколы IP, ARP, RARP, ICMP, IGMP.

**Протокол Интернета IP** обеспечивает обмен дейтаграммами между узлами сети и является протоколом, не устанавливающим соединения и использующим дейтаграммы для отправки данных из одной сети в другую. Данный протокол не ожидает получение подтверждения (ASK, Acknowledgment) отправленных пакетов от узла адресата. Подтверждения, а также повторные отправки пакетов осуществляются протоколами и процессами, работающими на верхних уровнях модели.

К функциям протокола относится фрагментация дейтаграмм и межсетевая адресация. Протокол IP предоставляет управляющую информацию для сборки фрагментированных дейтаграмм. Главной функцией протокола является межсетевая и глобальная адресация. В зависимости от размера сети применяется одна из трех применяемых на практике схем адресации (физическая, сетевая, символьная).

Протокол IP действует на сетевом уровне модели OSI, поэтому *IP-адреса называются сетевыми*. Они предназначены для передачи сообщений в составных сетях, связывающих подсети, построенные на различных локальных или глобальных сетевых технологиях, например, Ethernet или ATM. Однако для непосредственной передачи сообщения в рамках одной подсети вместо IP-адреса нужно использовать локальный адрес технологии канального уровня – обычно это МАС-адрес. При этом к IP-пакету добавляются заголовок и концевик кадра канального уровня, в заголовке указываются МАС-адреса источника и приемника кадра (рис. 3).

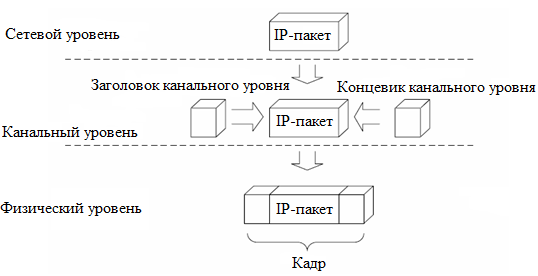


Рис. 3. Формирование кадра на канальном уровне

Принципы организации и практического использования всех трех видов адресов будут рассмотрены в отдельной лекции.

При формировании кадра канального уровня возникает проблема: каким образом по известному IP-адресу определить соответствующий МАС-адрес. Указанная проблема решается при помощи протокола ARP (Address Resolution Protocol, протокол разрешения адресов).

**Протокол сопоставления адреса ARP** определяет МАС-адреса следующим образом. Осуществляется рассылка всем узлам сети специального кадра, который называется **ARP-запрос** (***ARP Request***).

В кадре содержится IP-адрес компьютера, у которого требуется узнать МАС-адрес. Каждый узел сети принимает ARP-запрос и сравнивает IP-адрес из запроса со своим IP-адресом. Если адреса совпадают, узел высылает **ARP-ответ** (**ARP Reply**), содержащий требуемый МАС-адрес.

Результаты своей работы протокол ARP сохраняет в специальной таблице, хранящейся в *оперативной памяти*, которая называется **ARP-кэш**. При необходимости разрешения IP-адреса, протокол ARP сначала ищет IP-адрес в ARP-кэше и только в случае отсутствия нужной записи производит рассылку ARP-запроса.

Записи в ARP-кэше могут быть двух типов: статические и динамические. Статические записи заносятся в кэш администратором при помощи утилиты *arp* с ключом /s. Динамические записи помещаются в кэш после полученного ARP-ответа и по истечении двух минут удаляются.

ARP-кэш имеет структуру, представленную в табл. 2.

Таблица 2

**Внешний вид таблицы ARP-кэш**

|  |  |  |
| --- | --- | --- |
| **IP-адрес** | **MAC-адрес** | **Тип записи** |
| 192.168.1.1 | 03-E8-48-A1-57-7B | статический |
| 192.168.1.2 | 03-E8-48-A1-43-88 | динамический |
| 192.168.1.3 | 03-E8-48-A1-F8-D9 | динамический |

Процесс получения по известному IP-адресу МАС-адреса называется **разрешением IP-адреса**.

Удаление происходит для того, чтобы при перемещении в другую подсеть компьютера с МАС-адресом, занесенным в таблицу, кадры не отправлялись бесполезно в сеть.

Иногда требуется по известному МАС-адресу найти IP-адрес (например, при начале работы компьютеров без жесткого диска, у которых есть МАС-адрес сетевого адаптера и им нужно определить свой IP-адрес). В этом случае используется реверсивный протокол RARP (Reverse ARP).

**Протокол управления сообщениями Интернета** (Internet Control Message Protocol, ICMP) используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации. Этот протокол используется для контроля скорости передачи информации между двумя системами. Если маршрутизатор, соединяющий две системы, перегружен трафиком, он может отправить специальное сообщение ICMP – ошибку для уменьшения скорости отправления сообщений.

Узлы локальной сети используют **протокол управления группами Интернета** (Internet Group Management Protocol, IGMP), чтобы зарегистрировать себя в группе. Информация о группах содержится на маршрутизаторах локальной сети. Маршрутизаторы используют эту информацию для передачи групповых сообщений.

Групповое сообщение, как и широковещательное, используется для отправки данных сразу нескольким узлам.

**Протоколы обмена маршрутной информацией стека TCP/IP** относятся к классу адаптивных протоколов, которые в свою очередь делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:

* дистанционно-векторный алгоритм (Distance Vector Algorithms, DVA),
* алгоритм состояния связей (Link State Algorithms, LSA).

В алгоритмах дистанционно-векторного типа каждый маршрутизатор периодически и широковещательно рассылает по сети вектор расстояний от себя до всех известных ему сетей. Под расстоянием обычно понимается число промежуточных маршрутизаторов, через которые пакет должен пройти прежде, чем попадет в соответствующую сеть. Может использоваться и другая метрика, учитывающая не только число транзитных точек, но и время прохождения пакетов по связи между соседними маршрутизаторами. Получив вектор от соседнего маршрутизатора, каждый маршрутизатор добавляет к нему информацию об известных ему других сетях, о которых он узнал непосредственно (если они подключены к его портам) или из аналогичных объявлений других маршрутизаторов, а затем снова рассылает новое значение вектора по сети. В итоге, каждый маршрутизатор узнает информацию об имеющихся сетях и о расстоянии до них через соседние маршрутизаторы.

Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях. В больших сетях они «засоряют» каналы связи интенсивным широковещательным трафиком, к тому же изменения конфигурации могут отрабатываться по этому алгоритму не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только обобщенной информацией − вектором дистанций, к тому же полученной через посредников.

Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является протокол RIP *(Routing Information Protocol)*. Это один из старейших протоколов обмена маршрутной информацией, однако он до сих пор достаточно распространен в сетях.

*Алгоритмы состояния связей* обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети. Все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. Широковещательная рассылка используется здесь только при изменениях состояния связей, что происходит в надежных сетях не так часто.

Для того, чтобы понять, в каком состоянии находятся линии связи, подключенные к его портам, маршрутизатор периодически обменивается короткими пакетами со своими ближайшими соседями. Этот трафик также широковещательный, но он передается только между соседями и поэтому не так «засоряет» сеть.

Протоколом, основанным на алгоритме состояния связей, в стеке TCP/IP является протокол OSPF (Open Shortest Path Firs). Он принят в 1991 году) и обладает многими особенностями, ориентированными на применение в больших сильно разветвленных (гетерогенных) сетях. Протокол OSPF вычисляет маршруты в IP-сетях, сохраняя при этом другие протоколы обмена маршрутной информацией.

На практике также применяются комбинированные протоколы: более старый − EGP (*Exterior Gateway Protocol*, протокол внешнего шлюза) и его современная версия − BGP (*Border Gateway Protocol*, протокол граничного шлюза). Именно последний, т.е. протокол BGP, является основным протоколом динамической маршрутизации в сети Интернет.

Отметим, что приведенные протоколы обмена маршрутной информацией хоть и относятся к стеку TCP/IP, но также есть их реализации под другие стеки, например, IPX/SPX и т.д. Поэтому их нельзя назвать уникальными в рамках стека TCP/IP, как например, протоколы TCP, UDP или IP. Следовательно данные протоколы – RIP, OSPF, EGP, BGP – не были представлены ни на рисунке 2 (модель TCP/IP), ни в таблице 1.

***NDIS***(Network Device Interface Specification) – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта.

***Уровень сетевого интерфейса***

Этот уровень модели TCP/IP отвечает за распределение IP-дейтаграмм. Он работает с ARP для определения информации, которая должна быть помещена в заголовок каждого кадра. Затем на этом уровне создается кадр, подходящий для используемого типа сети, такого как Ethernet, Token Ring или ATM, затем IP-дейтаграмма помещается в область данных этого кадра. Кадр преобразуется в сигналы требуемого вида и отправляется в сеть.

**Выводы**

Спецификации IEEE802 определяют стандарты для физических компонентов сети: сетевая карта и сетевой носитель, которые относятся к физическому и канальному уровням модели OSI; механизм доступа адаптера к каналу связи и механизм передачи данных. Стандарты IEEE802 подразделяют канальный уровень на подуровни управления логической связью и подуровень управления доступом к устройствам.

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется стеком протоколов. Для каждого уровня определяется набор функций-запросов для взаимодействия с вышележащим уровнем, который называется интерфейсом. Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются протоколами.

Наибольшее распространение для построения составных сетей в последнее время получил стек TCP/IP. Стек TCP/IP имеет 4 уровня: прикладной, основной, уровень межсетевого взаимодействия и уровень сетевых интерфейсов. Соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Прикладной уровень объединяет все службы, предоставляемые системой пользовательским приложениям: традиционные сетевые службы типа Тelnet, FTP, TFTP, DNS, SNMP, а также сравнительно новые, такие, например, как протокол передачи гипертекстовой информации HTTP.

На основном уровне стека TCP/IP, называемом также транспортным, функционируют протоколы TCP и UDP. Протокол управления передачей TCP решает задачу обеспечения надежной информационной связи между двумя конечными узлами. Дейтаграммный протокол UDP используется как экономичное средство связи уровня межсетевого взаимодействия с прикладным уровнем.

Уровень межсетевого взаимодействия реализует концепцию коммутации пакетов в режиме без установления соединений. Основными протоколами этого уровня являются дейтаграммный протокол IP и протоколы маршрутизации (RIP, OSPF, EGP, BGP и др.). Вспомогательную роль выполняет протокол межсетевых управляющих сообщений ICMP, протокол группового управления IGMP и протокол разрешения адресов ARP.

Протоколы уровня сетевых интерфейсов обеспечивают интеграцию в составную сеть других сетей. Этот уровень не регламентируется, но поддерживает все популярные стандарты физического и канального уровней: для локальных сетей – Ethernet, Token Ring, FDDI и т. д., для глобальных сетей – Х.25, Frame relay, PPP, ISDN и т. д.

В стеке TCP/IP для именования единиц передаваемых данных на разных уровнях используют разные названия: поток (сообщение), дейтаграмма, пакет, кадр.

1. **Перспективы TCP/IP**

Протокол QUIC (Quick UDP Internet Connections), который как предполагается, может заменить TCP, позволяет мультиплексировать несколько потоков данных между двумя компьютерами, работая поверх протокола UDP, и содержит возможности шифрования, эквивалентные TLS и SSL. Имеет более низкую задержку соединения и передачи, чем TCP.

Работу над QUIC компания Google начала в 2013 году. Он тестировался в браузерах Chrome и Chromium. Позже технологию начали поддерживать сайты компании, в том числе YouTube. Через пару лет было объявлено, что тестирование протокола прошло успешно, и его представят в IETF (Инженерный совет Интернета).

Совет интернета начал работать над QUIC в марте 2016 года. Как отметили представители IETF, в будущем QUIC должен будет заменить TCP, так как последний исчерпал свои возможности в условиях современных сетей (в основном мобильных).

В протоколе TCP-соединение определяется IP-адресами и портами сервера и клиента. Если по какой-то причине один из этих параметров изменяется, приходится пересоздавать подключение. Отсюда вытекают сложности со стабильностью связи в мобильных сетях. Пользователь может перемещаться между разными сотовыми вышками и, как следствие, будет менять свой IP-адрес.

Задача QUIC — сделать процесс переключения между беспроводными сетями (в том числе Wi-Fi) более «гладким». Помимо этого тесты, проведенные Google, показывают снижение числа ребуферизаций при просмотре видео на YouTube на 30%.

***Особенности работы протокола QUIC***

Работа QUIC строится на протоколе UDP, который позволяет обмениваться данными без проверки готовности получателя к их приему. В QUIC установление соединения будет происходить в один этап с уже знакомым сервером и в два этапа с сервером, с которым клиент раньше не работал. Второй этап нужен, чтобы открыть защищенный канал связи и обменяться криптографическими ключами. В итоге QUIC будет иметь более низкую задержку соединения и передачи, чем TCP. При трансляции данных на большое расстояние (например, с одного континента на другой) посредством мобильного устройства разница в скорости установления подключения между TCP с TLS и пакетом QUIC может достигать 300 мс.

В QUIC больше нет набора параметров, связанных с IP-адресами и портами сервера и клиента. Вместо них протокол работает с идентификатором соединения UUID. Это позволяет переключаться между Wi-Fi и мобильной сетью, каждый раз не пересоздавая соединение (UUID сохраняется).

QUIC дополнительно включает метод контроля целостности данных — прямую коррекцию ошибок, или Forward Error Correction (FEC). Каждый пакет, который передается через QUIC, имеет информацию о соседях. Поэтому если он теряется, содержимое пакета можно восстановить.

Однако пока у технологии есть определенные недостатки.

1. уязвимость перед DDoS-атаками.
2. несовместимость протокола с сетями, в которых используются технологии NAT, Anycast или ECMP. Они работают с TCP-соединениями и не смогут распознавать и регулировать QUIC-трафик. Такая несовместимость сужает возможности для применения.
3. затрудненный поиск неисправностей. Протокол шифрует не только данные, но и заголовок пакета, в котором они передаются. Это мешает системным администраторам оценивать работу сети и быстро устранять неполадки.

Более того, результаты тестирования QUIC показали, что протокол пока что не так хорошо работает на мобильных устройствах, как это предполагалось. Согласно экспериментам, при увеличении пропускной способности сети и объема передаваемых данных время загрузки страницы для TCP и QUIC выравнивается. Это происходит потому, что QUIC работает в пользовательском пространстве, а не в пространстве ядра.

***Перспективы протокола***

Протокол уже поддерживают крупные организации. С QUIC начали работать CDN-сервисы — Cloudflare и Verizon Digital Media Services (VDMS). В Cloudflare функция соединения через QUIC находится в бета-тестировании. Команда VDMS работала над реализацией протокола с 2016 года, и сейчас QUIC могут использовать все клиенты сервиса. Версии протокола QUIC также тестируют Apple, Pandora, Facebook и т.д.

Хотя пока QUIC остается экспериментальной технологией, количество сайтов с поддержкой этого протокола растет.