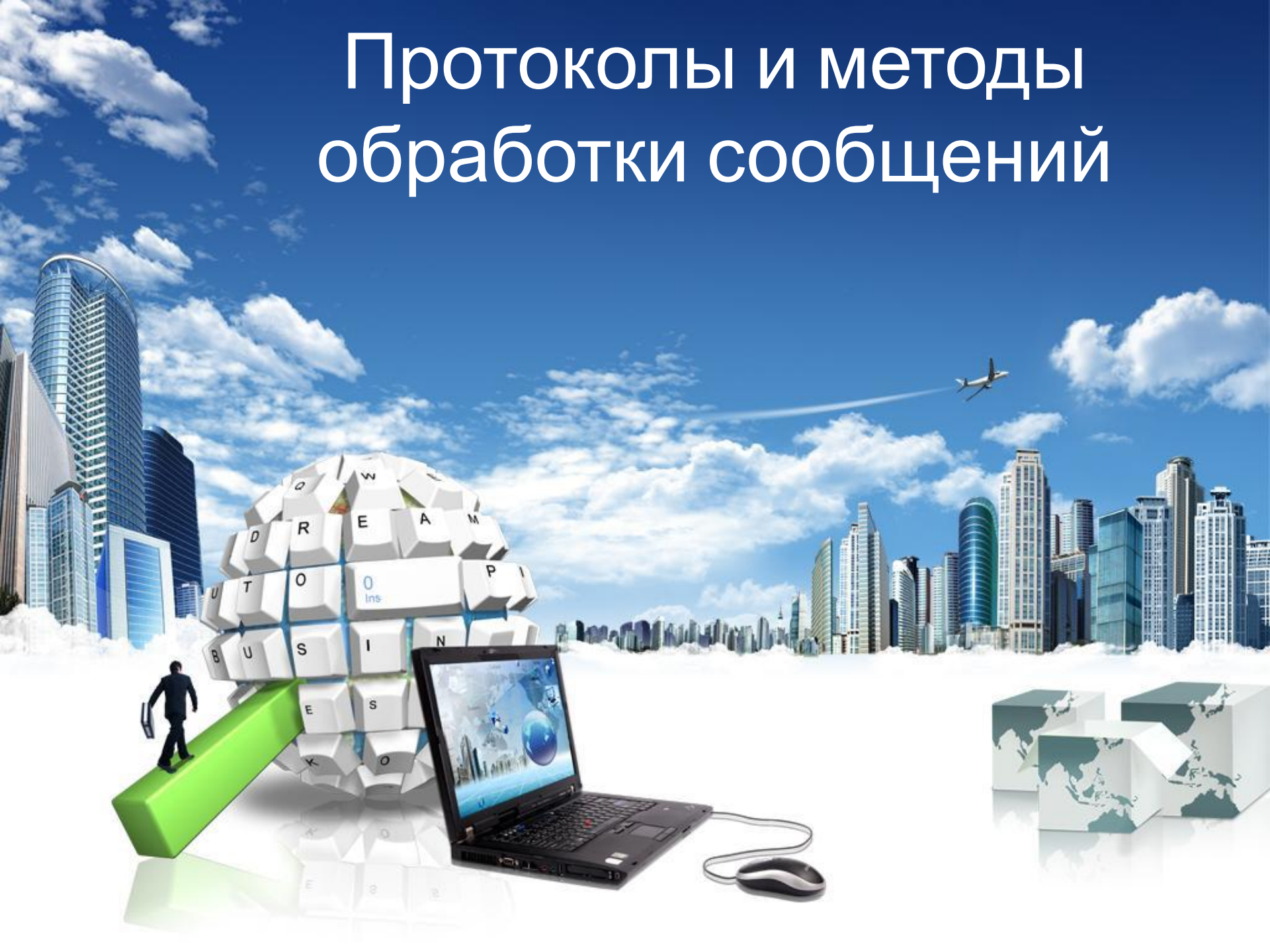
Протоколы и методы обработки сообщений



Сообщением называется логически завершенная порция данных - запрос на передачу файла, ответ на этот запрос, содержащий весь файл и т. п. Сообщения могут иметь произвольную длину, от нескольких байт до многих мегабайт. По такой схеме обычно передаются сообщения, не требующие немедленного ответа, чаще всего сообщения электронной почты.

При коммутации пакетов все передаваемые пользователем сети сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами. Пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт. Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения. Пакеты транспортируются в сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге - узлу назначения.

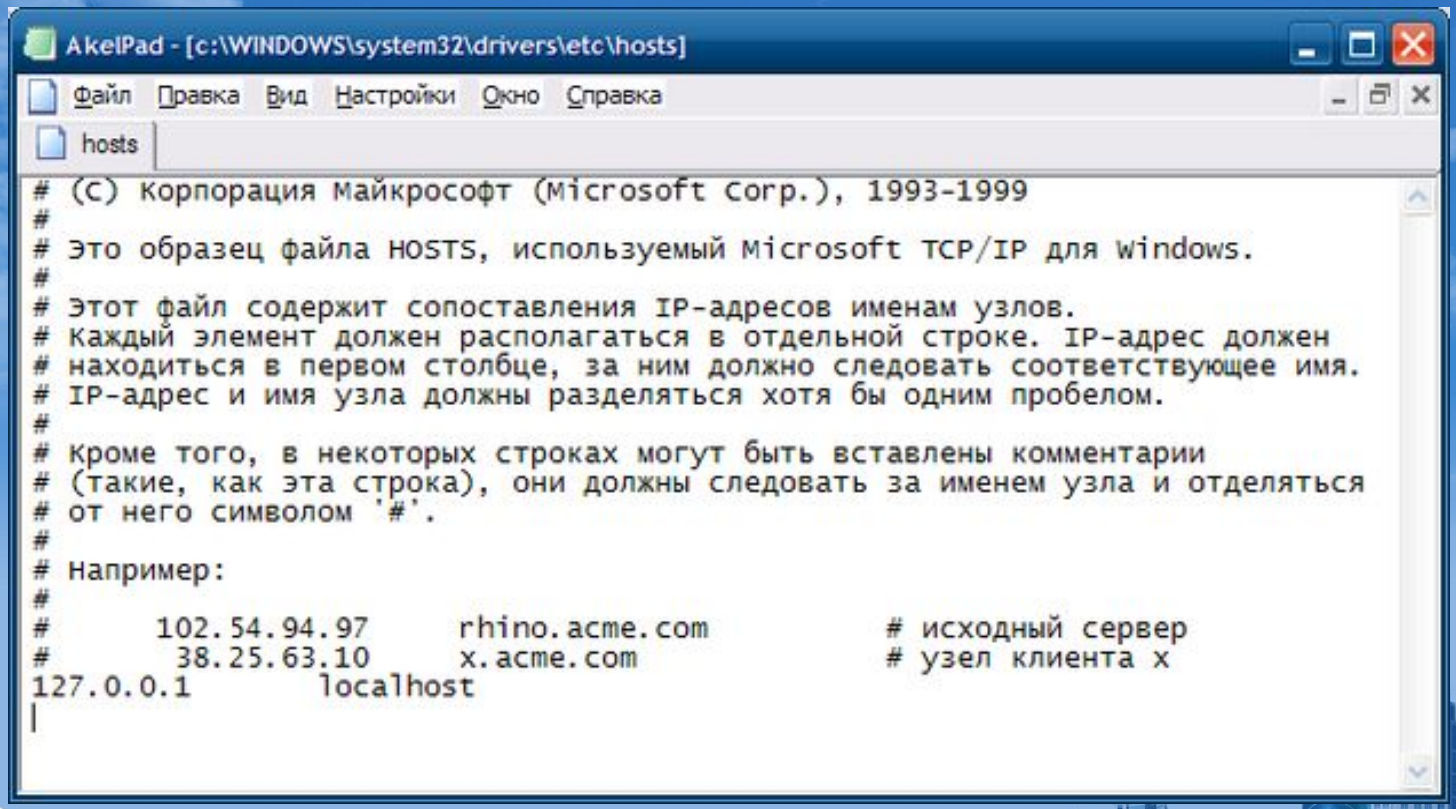
Протокол DNS

DNS (Domain Name System — система доменных имён) — компьютерная распределённая система преобразование символьного имени (just-networks.ru) в IP-адрес (91.106.203.89) и наоборот.

DNS была разработана Полом Мокапетрисом в 1983 году.

В сети интернет DNS выполняет важную задачу, для доступа к веб-серверу необходимо знать его IP-адрес. Необходимость использования DNS обусловлена тем, что людям легче запоминать буквенные (обычно осмысленные) адреса, чем последовательность четырех цифр IP – адреса, компьютерам, в свою очередь, удобнее обрабатывать численное представление адреса (IP-адрес). Также наличие символьного имени сервера позволяет использовать так называемые виртуальные серверы , например, HTTP-серверы, отличающиеся друг от друга именем запроса (доменным именем), но использующие один и тот же IP-адрес.

В начале для преобразования IP-адресов в символьные имена использовался текстовый файл hosts , расположенный:
В Windows: %SystemRoot%\system32\drivers\etc\hosts;
В Unix: /etc/hosts;



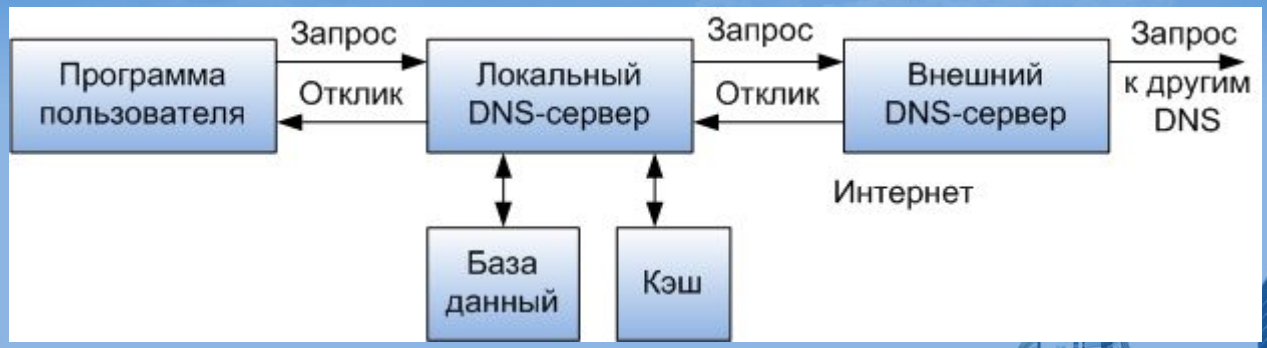
Файл hosts заполнялся автоматически и централизовано на каждой ЭВМ в своей локальной вычислительной сети. Но даны подход со временем показал свою не-состоятельность, поскольку с ростом сети, количество записей в текстовом файле увеличивалось, как следствие увеличивался размер файла, ко всему прочему частая пересылка файла hosts загружала вычислительную сеть.
В итоге стала необходимость в разработке автоматизированного механизма, которым и стала распределенная система DNS.
Следует учесть, что файл hosts используется до сих пор, в частности, при настройке локального сервера на ЭВМ, в hosts записываются созданные локальные символьные имена.
Например:
127.0.0.1 mysite.local

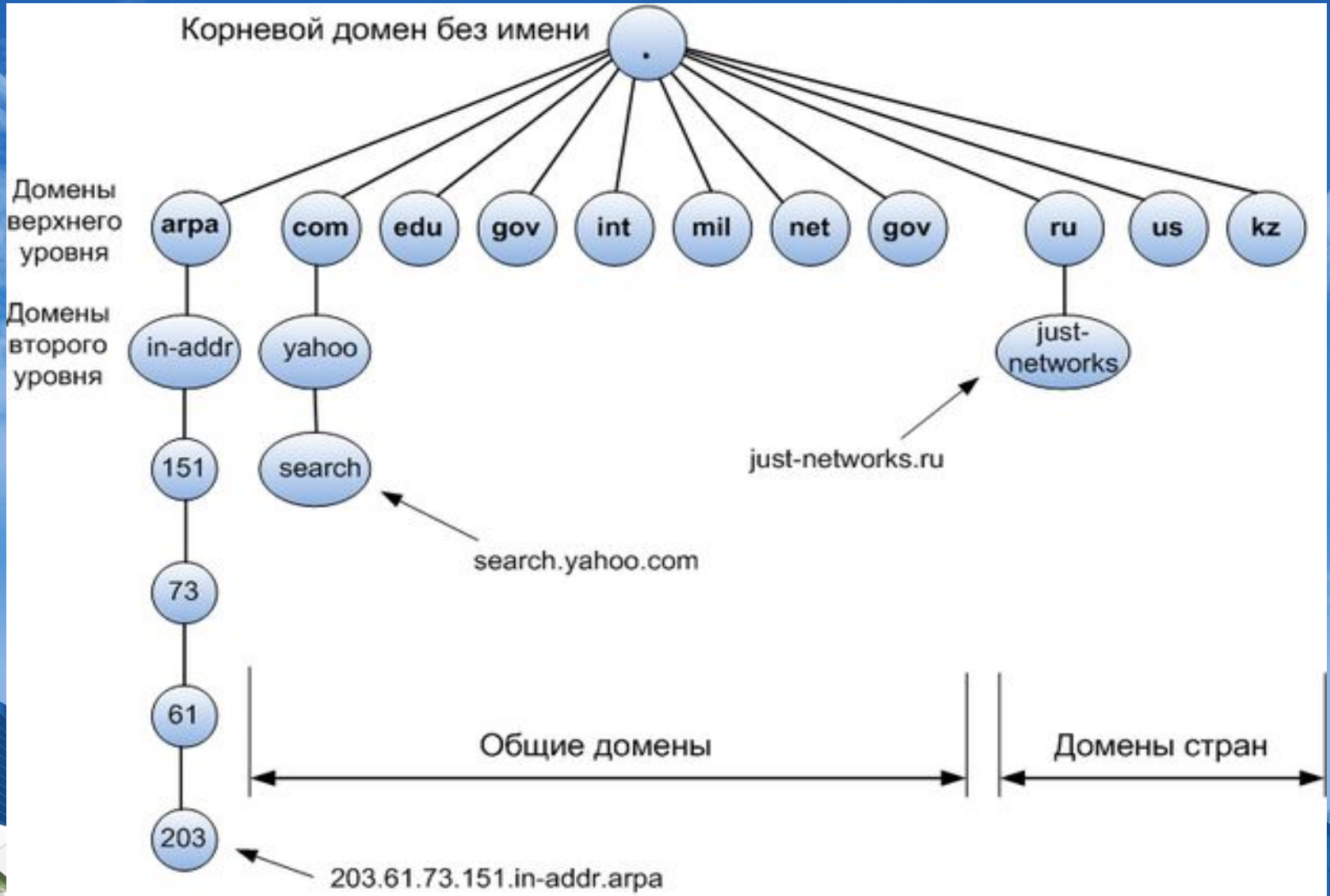
Иерархия имен в DNS

В связи с тем, что число узлов интернета растет с каждым днем, для эффективной работы **DNS** разработана распределенная база данных, поддерживаемая с использование иерархии DNS-серверов

Данная схема позволяет разгрузить сервер DNS по нескольким серверам DNS, что и выполняет распределенная база данных.

В основе иерархической структуры DNS лежит представление о доменном имени и зонах. Каждый DNS сервер, отвечающий за имя, может передать ответственность за дальнейшую часть домена другому серверу, что позволяет делегировать ответственность за вновь добавленную информацию на серверы различных организаций (людей), ответственных непосредственно только за «свою» часть доменного имени.




Корневой домен без имени
.
Домены верхнего уровня
arpa
com
edu
gov
int
mil
net
gov
ru
us
kz
Домены второго уровня
in-addr
yahoo
just-networks
just-networks.ru
151
search
search.yahoo.com
73
61
Общие домены
Домены стран
203
203.61.73.151.in-addr.arpa

Иерархия доменных имен начинается с корневого домена без имени (или еще как его называют «домен точка»), далее идут домены верхнего уровня или домены первого уровня. Домены верхнего уровня поделены на три зоны:
arpa это специальный домен, используемый для сопоставления адрес - имя
Семь трехсимвольных доменов называются общими (generic) доменами или организационными (organizational) доменами.
Двухсимвольные домены, так называемые домены стран или географические домены (ru – Российская федерация, kz - Казахстан), основанные на кодах стран, в соответствии с ISO 3166.
Поскольку DNS поддерживает иерархию доменных имен, но никак не IP-адресов, то для решения “обратной” задачи есть специальный домен, структура которого совпадает со структурой IP-адресов. Называется этот домен **IN-ADDR.ARPA** .
in-addr.arpa — специальная доменная зона, предназначенная для определения имени хоста по его IPv4-адресу, используя PTR-запись. Имена в домене IN-ADDR.ARPA образуют иерархию цифр, которые соответствуют IP-адресам. Правда, записываются эти имена в обратном порядке относительно написания IP-адреса.
Например, доменное имя just-networks.ru, которое имеет адрес **91.106.203.89** должна быть описана в домене in-addr.arpa как **89.203.106.91.in-addr.arpa**, то есть адрес записывается в обратном порядке.

Типы записей DNS

A запись (address record **IPv4**) или запись адреса - основная запись, выполняет связующую роль между именем хоста (just-networks.ru) и IP адресом (5.101.153.37). Если меняется только A запись, то это значит, что наш сайт физически будет размещен на другом хостинге, а все остальные записи останутся работать на старом хостинге.

Название	Тип записи	Адрес
just-networks.ru	A	5.101.153.37

AAA запись (address record **IPv6**) или запись адреса - аналогична записи A, только для IPv6

Название	Тип записи	Адрес
just-networks.ru	AAA	FFEA::CA28:1210:4362

CNAME запись (canonical name record) или каноническая запись имени (псевдоним) - используется для перенаправления на другое имя (по аналогии с ссылками), частным примером использования CNAME записи, является создание доменных имен для ftp, mail, ssh, например

Название	Тип записи	Адрес
ftp.just-networks.ru	CNAME	www.just-networks.ru
mail.just-networks.ru	CNAME	www.just-networks.ru
ssh.just-networks.ru	CNAME	www.just-networks.ru

MX запись (mail exchange) или почтовый обменник, указывает те сервера, с которыми будет осуществлен обмен для данного домена. То есть определяет сервер, который будет обрабатывать почту для вашего домена. В случае отсутствия MX-записи, запрашивается A-запись

Название	Тип записи	Адрес
www.just-networks.ru	MX	mx1.beget.ru
www.just-networks.ru	MX	mx2.beget.ru

NS запись (name server) указывает на DNS сервер текущего домена, так называемые authoritative DNS-серверы. Смена NS-записи, при переходе на другой хостинг, влечёт за собой смену всех записей, соответственно нужно или указывать новые записи или копировать со старого сайта (например, для сохранения почты, нужно скопировать MX-запись со старого хостинга). При неправильном изменении NS записи домена, может привести к остановке работы сайта.

Название	Тип записи	Адрес
www.just-networks.ru	**NS**	**ns1.beget. ru**
www.just-networks.ru	**NS**	**ns2.beget.ru**

TXT запись текстовая запись содержащая 254 байта любой текстовой информации, в основном используется для подтверждения принадлежности домена для сервисов yandex, google.

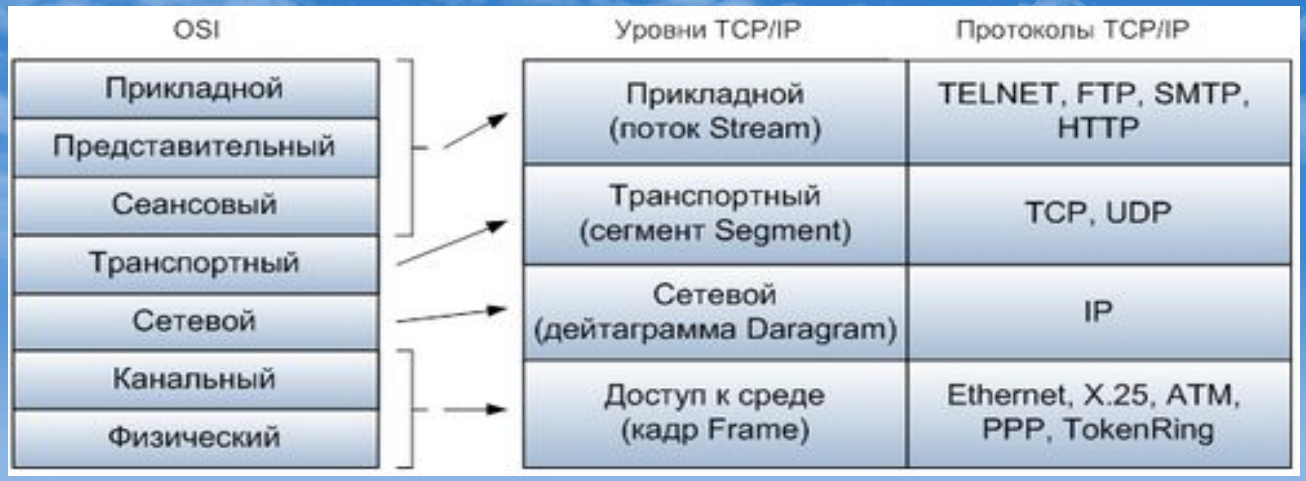
yandex	**validate value for yandex**

Протокол TCP/IP
(Transmission Control Protocol/Internet Protocol)

Это стек сетевых протоколов, повсеместно используемый для Интернета и других подобных сетей (например, данный протокол используется и в ЛВС). Название TCP/IP произошло от двух наиболее важных протоколов:

- **IP (интернет протокол)** - отвечает за передачу пакета данных от узла к узлу. IP пересылает каждый пакет на основе четырехбайтного адреса назначения (IP-адрес).
- **TCP (протокол управления передачей)** - отвечает за проверку корректной доставки данных от клиента к серверу. Данные могут быть потеряны в промежуточной сети. TCP добавлена возможность обнаружения ошибок или потерянных данных и, как следствие, возможность запросить повторную передачу, до тех пор, пока данные корректно и полностью не будут получены.

- Стандартизованные протоколы высокого уровня, используемые для хорошо известных пользовательских сервисов.
- Используются открытые стандарты протоколов, что дает возможность разрабатывать и дорабатывать стандарты независимо от программного и аппаратного обеспечения;
- Система уникальной адресации;
- Независимость от используемого физического канала связи;

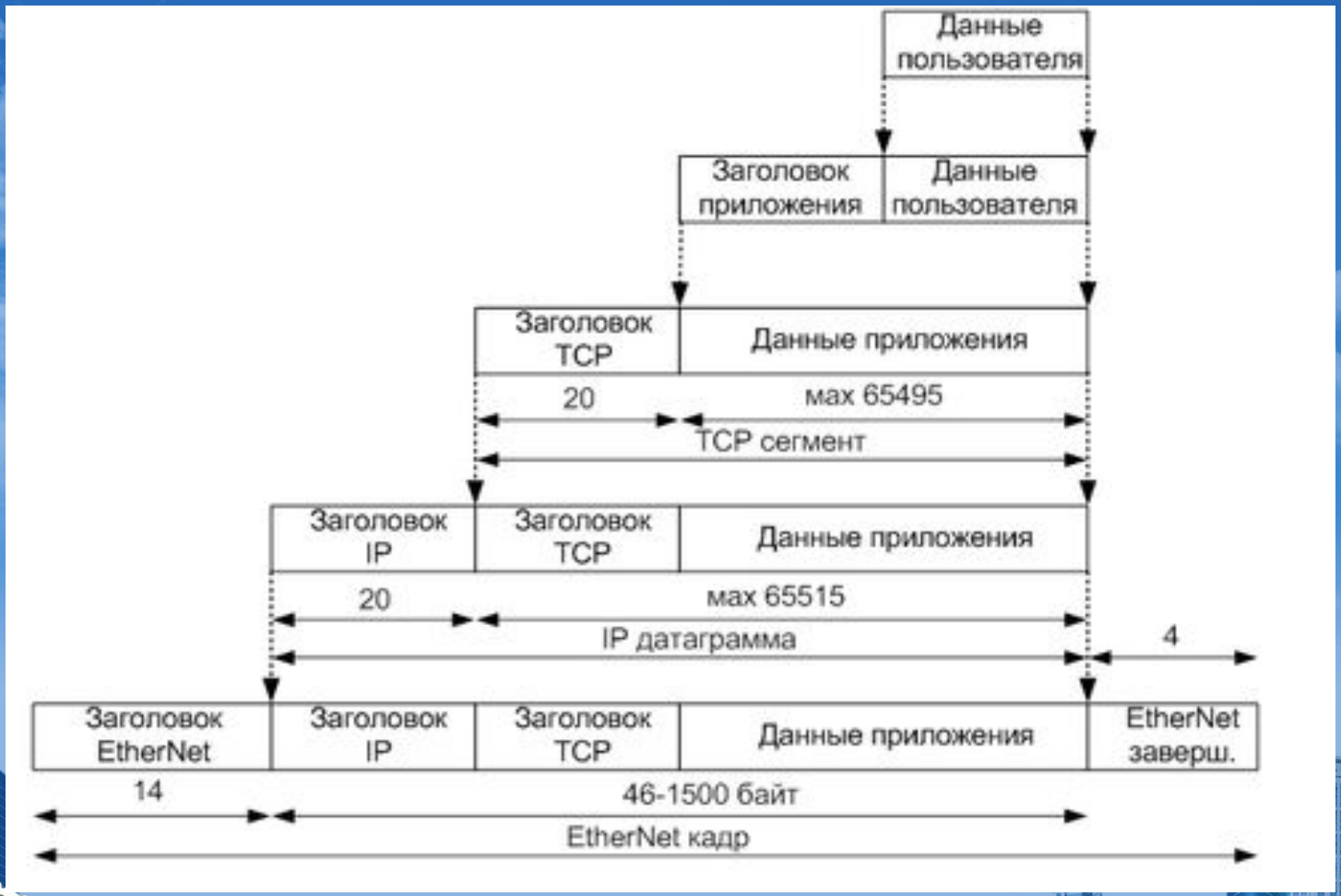


TCP - Transmission Control Protocol - базовый транспортный протокол, давший название всему семейству протоколов TCP/IP.
UDP - User Datagram Protocol - второй транспортный протокол семейства TCP/IP. Различия между TCP и UDP будут обсуждены позже.
ARP - Address Resolution Protocol - протокол используется для определения соответствия IP-адресов и Ethernet-адресов.
SLIP - Serial Line Internet Protocol (Протокол передачи данных по телефонным линиям).
PPP - Point to Point Protocol (Протокол обмена данными "точка-точка").
FTP - File Transfer Protocol (Протокол обмена файлами).
TELNET - протокол эмуляции виртуального терминала.
RPC - Remote Process Control (Протокол управления удаленными процессами).
TFTP - Trivial File Transfer Protocol (Тривиальный протокол передачи файлов).
DNS - Domain Name System (Система доменных имен).
RIP - Routing Information Protocol (Протокол маршрутизации).
NFS - Network File System (Распределенная файловая система и система сетевой печати).

Принцип работы стека протоколов TCP/IP такой же как и в модели OSI, данные верхних уровней инкапсулируются в пакеты нижних уровней.
Если пакет продвигается по уровню сверху вниз - на каждом уровне добавляется к пакету служебная информация в виде заголовка и возможно трейлера (информации помещенной в конец сообщения). Этот процесс называется **инкапсуляция**. Служебная информация предназначается для объекта того же уровня на удаленном компьютере. Ее формат и интерпретация определяются протоколами данного уровня.
Если пакет продвигается по уровню снизу вверх - он разделяется на заголовок и данные. Анализируется заголовок пакета, выделяется служебная информация и в соответствии с ней данные перенаправляются к одному из объектов вышестоящего уровня. Вышестоящий уровень, в свою очередь, анализирует эти данные и также их разделяет их на заголовок и данные, далее анализируется заголовок и выделяется служебная информация и данные для вышестоящего уровня. Процедура повторяется заново пока пользовательские данные, освобожденные от всей служебной информации, не дойдут до прикладного уровня.

Инкапсуляция - способ упаковки данных в формате одного протокола в формат другого протокола. Например, упаковка IP-пакета в кадр Ethernet или TCP-сегмента в IP-пакет. В рамках межсетевого обмена понятие инкапсуляции имеет несколько более расширенный смысл. Если в случае инкапсуляции IP в Ethernet речь идет действительно о помещении пакета IP в качестве данных Ethernet-фрейма, или, в случае инкапсуляции TCP в IP, помещение TCP-сегмента в качестве данных в IP-пакет, то при передаче данных по коммутируемым каналам происходит дальнейшая "нарезка" пакетов теперь уже на пакеты SLIP или фреймы PPP.

Пример инкапсуляции можно представить следующим образом:



Прикладной уровень

Приложения, работающие со стеком TCP/IP, могут также выполнять функции представительного уровня и частично сеансового уровня модели OSI. Распространенными примерами приложений являются программы:

- **Telnet**
- **FTP**
- **HTTP**
- **WWW**
- **Протоколы электронной почты (SMTP, POP3)**

Для пересылки данных другому приложению, приложение обращается к тому или иному модулю транспортного модуля.

Транспортный уровень

Протоколы транспортного уровня обеспечивают прозрачную доставку данных меду двумя прикладными процессами. Процесс, получающий или отправляющий данные, с помощью транспортного уровня идентифицируется на этом уровне номером, который называется номером порта.

Средства транспортного уровня представляют собой функциональную надстройку над сетевым уровнем и решают две основных задачи: обеспечение доставки данных между конкретными программами, функционирующими, в общем случае, на разных узлах сети; обеспечение гарантированной доставки массивов данных произвольного размера.

В настоящее время в Интернет используются два транспортных протокола – **UDP,** обеспечивающий негарантированную доставку данных между программами, и **TCP,** обеспечивающий гарантированную доставку с установлением виртуального соединения.

Сетевой (межсетевой) уровень

Основным протоколом этого уровня является протокол IP, который доставляет блоки данных (дейтаграммы) от одного IP-адреса к другому. IP-адрес является уникальным 32-х битным идентификатором компьютера, точнее его сетевого интерфейса. Данные для дейтаграммы передаются IP модулю транспортным уровнем. IP модуль добавляет к этим данным заголовок, содержащий IP-адрес отправителя и получателя, и другую служебную информацию.
Таким образом, сформированная дейтаграмма передается на уровень доступа к среде передачи, для отправки по каналу передачи данных. Не все компьютеры могут непосредственно связаться друг с другом, часто чтобы передать дейтаграмму по назначению требуется направить ее через один или несколько промежуточных компьютеров по тому или ному маршруту. Задача определения маршрута для каждой дейтаграммы решается протоколом IP.

Когда модуль IP получает дейтаграмму с нижнего уровня, он проверяет IP адрес назначения, если дейтаграмма адресована данному компьютеру, то данные из нее передаются на обработку модулю вышестоящего уровня, если же адрес назначения дейтаграммы чужой, то модуль IP может принять два решения:

Уничтожит дейтаграмму;

Отправить ее дальше к месту назначения, определив маршрут следования, так поступают промежуточные станции – маршрутизаторы. Также может потребоваться на границе сетей, с различными характеристиками, разбить дейтаграмму на фрагменты, а потом собрать их в единое целое на компьютере получателя. Это также задача протокола IP.

Также протокол IP может отправлять сообщения – уведомления с помощью протокола **ICMP,** например, в случае уничтожения дейтаграммы. Более никаких средств контроля корректности данных, подтверждения или доставки, предварительного соединения в протоколе нет, эти задачи возложены на транспортный уровень.

Когда модуль IP получает дейтаграмму с нижнего уровня, он проверяет IP адрес назначения, если дейтаграмма адресована данному компьютеру, то данные из нее передаются на обработку модулю вышестоящего уровня, если же адрес назначения дейтаграммы чужой, то модуль IP может принять два решения:

- Уничтожит дейтаграмму;
- Отправить ее дальше к месту назначения, определив маршрут следования, так поступают промежуточные станции – маршрутизаторы.

Также может потребоваться на границе сетей, с различными характеристиками, разбить дейтаграмму на фрагменты, а потом собрать их в единое целое на компьютере получателя. Это также задача протокола IP.

Также протокол IP может отправлять сообщения – уведомления с помощью протокола **ICMP,** например, в случае уничтожения дейтаграммы.

Более никаких средств контроля корректности данных, подтверждения или доставки, предварительного соединения в протоколе нет, эти задачи возложены на транспортный уровень.

Уровень доступа к среде

- Отображение IP-адресов в физические адреса сети. Эту функцию выполняет протокол **ARP;**
- Инкапсуляция IP-дейтаграмм в кадры для передачи по физическому каналу и извлечение дейтаграмм из кадров, при этом не требуется какого-либо контроля безошибочной передачи, поскольку в стеке TCP/IP такой контроль возложен на транспортный уровень или на само приложение. В заголовке кадров указывается точка доступа к сервису SAP, это поле содержащее код протокола;
- Определение метода доступа к среде передачи, т.е. способа, с помощью которого компьютеры устанавливает свое право на передачу данных;
- Определение представления данных в физической среде;
- Пересылка и прием кадра.

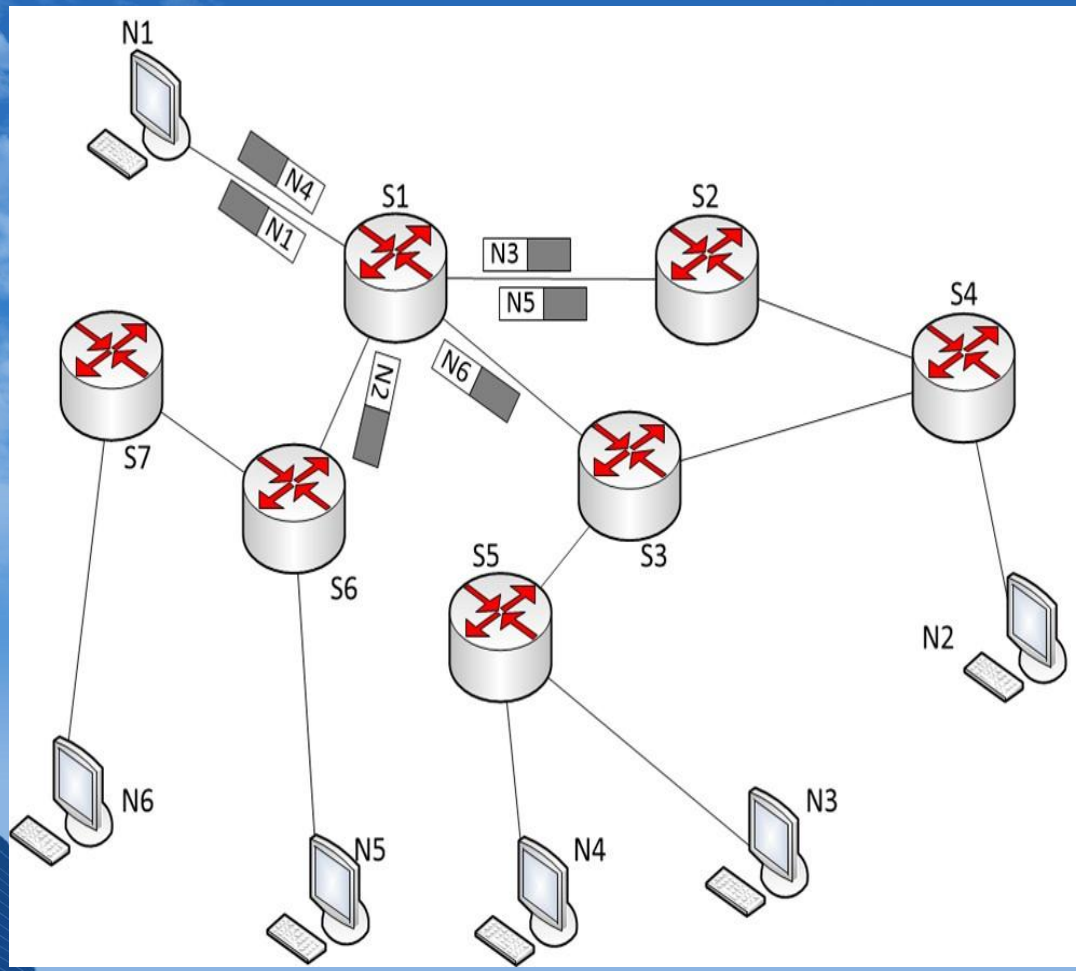


Таблица коммутации коммутатора S1

Адрес Назначения	Адрес следующего коммутатора
N1	Пакет не требуется передавать
N2	S2
N3	S3
N4	S3
N5	S6
N6	S6

Номер версии (4 бита)	Длина загол-ка (4 бита)	Тип сервиса (8 бит)	Общая длина (16 бит)	
Идентификатор (16 бит)			Флаги (3 бита)	Смещение фрагмента (13 бит)
Время жизни (8 бит)		Протокол (8 бит)	Контрольная сумма заголовка (16 бит)	
Адрес отправителя (32 бита)				
Адрес получателя (32 бита)				
Опции (поле переменной длины)			Выравнивание (до 32-битной границы)	

Так как обработка дейтаграммы происходит с помощью программного обеспечения, оборудование не накладывает никаких ограничений на ее содержимое и формат

.

Поле «Номер версии».

Задаёт порядковый номер используемой версии IP-протокола. В настоящее время используется 4-ая версия и планируется переход к 6-ой.

Поле «Длина заголовка».

Задаёт значение длины заголовка в 32-битных словах. Минимальный размер заголовка - 5 слов.

Поле «Тип сервиса».

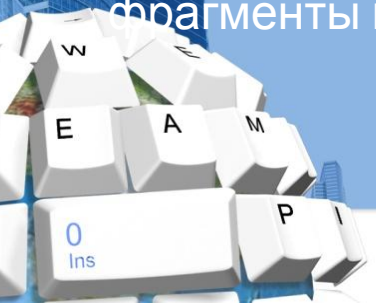
Задаёт тип требуемого обслуживания. Программное обеспечение большинства рабочих станций и маршрутизаторов игнорирует этот тип сетевого сервиса.

Поле «Общая длина».

Задаёт общую длину дейтаграммы с учетом заголовка и поля данных. Максимальный размер дейтаграммы может составлять 65 535 байтов. В соответствии со стандартом все сетевые устройства должны принимать и обрабатывать дейтаграммы длиной до 576 байтов.

Поле «Идентификатор».

Используется для распознавания фрагментированных дейтаграмм. Все фрагменты исходной дейтаграммы имеют одинаковое значение этого поля.



Поле «Флаги».
0-ой бит: не используется;
1-ый бит (DF): задаёт возможность фрагментации (0 - разрешить; 1-запретить);
2-ой бит (MF): задаёт возможность продолжения следования фрагментов (0 - фрагментов более не следует; 1 - за данным фрагментом следует как минимум ещё один).

Поле «Смещение фрагмента».
Задаёт место данного фрагмента в исходной дейтаграмме. Смещение фрагмента изменяется 8-байтовыми словами. Первый фрагмент имеет нулевое смещение. Максимальное количество фрагментов - 8191.

Поле «Протокол».
Задаёт номер протокола верхнего уровня, в распоряжение которого поступает содержимое поля данных дейтаграммы.

Поле «Время жизни».
Задаёт время, в пределах которого дейтаграмма путешествует в сети. Стартовое значение задаётся при отправке и уменьшается по мере прохождения маршрутизаторов. Максимальное значение - 255 секунд. Каждый маршрутизатор уменьшает значение параметра на время, необходимое для его обработки. По достижении нуля дейтаграмма уничтожается.

Поле «Контрольная сумма».
Рассчитывается по всем полям заголовка. При прохождении дейтаграмм через маршрутизаторы, контрольная сумма каждый раз пересчитывается и сравнивается со значением контрольной суммы в заголовке. При обнаружении ошибки дейтаграмма бракуется.

Поле «Адрес отправителя».
Содержит 32-битный IP-адрес отправителя дейтаграммы.

Поле «Адрес получателя».
Содержат 32-битный IP-адрес получателя дейтаграммы.

Поле «Опции».
Не является обязательным. Используется при отладке сетей.

Поле «Выравнивание».
Используется для выравнивания заголовка дейтаграммы по 32-битной границе. Выравнивание выполняется нулями.

Фрагментация — процедура разделения дейтаграммы на несколько частей. Необходимость фрагментации обусловлена различиями в пропускной способности сегментов сетевых структур.

Путешествие дейтаграммы начинается с её передачи на канальный уровень. Каждый канал характеризуется максимальным размером передаваемого кадра MTU (MaximumTransmission Unit).

В сетях Ethernet размер MTU составляет1500 байтов, в сетях FDDI MTU = 4096 байтов.

Ограниченная пропускная способность канала влечёт за собою необходимость разделения дейтаграммы на фрагменты, размеры которых удовлетворяют ограничению, налагаемому значением MTU.


W
E
A
M
P
I
0
Ins