

Лекции №17-18
Локальные вычислительные сети. Технология WWW. Структура Internet.
Адресация в ip-сетях

I. ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Локальные вычислительные сети (ЛВС) позволяют объединять компьютеры, расположенные в ограниченном пространстве. Локальные сети – LAN (Local Area Network) – являются элементами более крупномасштабных образований – CAN (Campus Area Network- кампусная сеть, объединяющая локальные сети близко расположенных зданий), MAN (Metropolitain Area Network – сеть городского масштаба), WAN (Wide Area Network – широкомасштабная сеть), GAN (Global Area Network – глобальная сеть).

Под локальной вычислительной сетью понимают совместное подключение нескольких отдельных компьютерных рабочих мест (рабочих станций) к единому каналу передачи данных.

Понятие локальная вычислительная сеть – ЛВС - относится к географически ограниченным (территориально или производственно) аппаратно-программным реализациям, в которых несколько компьютерных систем связаны друг с другом с помощью соответствующих средств коммуникации.

ЛВС в производственной практике играют очень большую роль. Посредством ЛВС в систему объединяются персональные компьютеры, расположенные на многих удаленных рабочих местах, которые используют совместно оборудование, программные средства и информацию. Рабочие места сотрудников перестают быть изолированными и объединяются в единую систему.

Преимущества, получаемые при сетевом объединении ПК:

- **Разделение ресурсов** позволяет экономно их использовать, например, управлять периферийными устройствами, такими как принтеры. При разделении ресурсов процессора возможно использование вычислительных мощностей для обработки данных другими системами, входящими в сеть.
- **Разделение данных** предоставляет возможность доступа и управления базами данных с периферийных рабочих мест.
- **Разделение программных средств** предоставляет возможность одновременного использования централизованных, ранее установленных программных средств. Многопользовательский режим системы содействует одновременному использованию централизованных прикладных программных средств, ранее установленных и управляемых.

Доступом к сети называют взаимодействие станции (узла сети) со средой передачи данных для обмена информацией с другими станциями. Управление доступом к среде - это установление последовательности, в которой станции получают доступ к среде передачи данных.

Различают **случайные и детерминированные** методы доступа. Среди случайных методов наиболее известен метод **множественного доступа с контролем несущей и обнаружением конфликтов (МДКН/ОК)**. Англоязычное название метода - Carrier Sense Multiple Access /Collision Detection (CSMA/CD). Этот метод основан на контроле несущей в линии передачи данных и устранении конфликтов, возникающих из-за попыток одновременного начала передачи двумя или более станциями, путем повторения попыток захвата линии через случайный отрезок времени.

МДКН/ОК является широкоэмитальным (broadcasting) методом. **Все станции при применении МДКН/ОК равноправны по доступу к сети.** Если линия передачи данных свободна, то в ней отсутствуют электрические колебания, что легко распознается любой станцией, желающей начать передачу. Такая станция захватывает линию. Любая другая

станция, желающая начать передачу в некоторый момент времени t , если обнаруживает электрические колебания в линии, то откладывает передачу до момента $t + t_d$, где t_d - задержка.

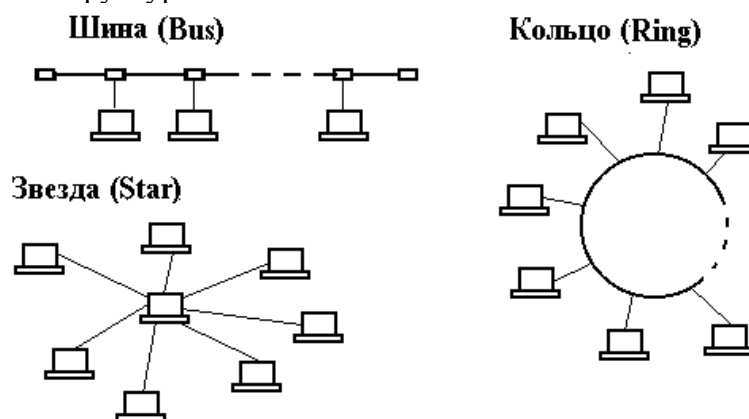
Среди **детерминированных методов преобладают маркерные методы доступа**. Маркерный метод - метод доступа к среде передачи данных в ЛВС, **основанный на передаче полномочий передающей станции с помощью специального информационного объекта, называемого маркером**. Под полномочием понимается право инициировать определенные действия, динамически предоставляемые объекту, например станции данных в информационной сети.

Применяется ряд разновидностей маркерных методов доступа. Например, в **эстафетном методе** передача маркера выполняется в порядке очереди; в способе **селекторного опроса** (квантированной передачи) сервер опрашивает станции и передает полномочие одной из тех станций, которые готовы к передаче. В кольцевых одноранговых сетях широко применяется тактируемый маркерный доступ, при котором маркер циркулирует по кольцу и используется станциями для передачи своих данных.

Топология вычислительной сети

Под **топологией** вычислительной сети понимают конфигурацию физических соединений компонентов вычислительной сети (сервер, станции). Тип топологии определяет производительность и надежность в эксплуатации сети рабочих станции, для которых имеет значение также время обращения к файловому серверу.

Подсети в интернетях объединяются в соответствии с выбранной топологией с помощью блоков взаимодействия. В зависимости от топологий соединений узлов различают сети шинной (магистральной), кольцевой, звездной, иерархической, произвольной структуры



Среди ЛВС наиболее распространены:

шинная (bus) - локальная сеть, в которой связь между любыми двумя станциями устанавливается через один общий путь и данные, передаваемые любой станцией, одновременно становятся доступными для всех других станций, подключенных к этой же среде передачи данных (последнее свойство называют *широковещательностью*); протокол Ethernet.

кольцевая (ring) - узлы связаны кольцевой линией передачи данных (к каждому узлу подходят только две линии); данные, проходя по кольцу, поочередно становятся доступными всем узлам сети; протокол Token Ring,

звездная (star) - имеется центральный узел, от которого расходятся линии передачи данных к каждому из остальных узлов; протоколы Ethernet (с концентратором), Token Ring.

Протоколы ЛВС

В ЛВС не требуется обеспечивать большинство функций, относящихся к сетевому и транспортному уровням ЭМВОС, поэтому выполняемые функции разделены между физическим и канальным уровнями, причем канальный уровень расщеплен на два подуровня: управление доступом к среде (MAC) и управление логическим каналом (LLC).

1. Сети Ethernet. Одной из первых среди ЛВС шинной структуры была создана сеть Ethernet, разработанная фирмой Xerox. В этой сети был применен метод доступа МДКН/ОК. Позднее Ethernet стала основой стандарта IEEE 802/3. Другой вариант шинных ЛВС соответствует стандарту IEEE 802/4, описывающему сеть с эстафетной передачей маркера.

Технология Ethernet наиболее распространена в ЛВС.

1. **Вариант Thick Ethernet** (шина "с толстым" кабелем); принятое обозначение варианта 10Base-5, где первый элемент "10" характеризует скорость передачи данных по линии 10 Мбит/с, последний элемент "5" - максимальную длину сегмента (в сотнях метров), т.е. 500 м; другие параметры: максимальное число сегментов 5; максимальное число узлов на одном сегменте 100; минимальное расстояние между узлами 2,5 м. Здесь под сегментом кабеля понимается часть кабеля, используемая в качестве линии передачи данных и имеющая на концах согласующие элементы (терминаторы) для предотвращения отражения сигналов.

2. **Вариант Thin Ethernet** (шина "с тонким" кабелем, cheapernet); принятое обозначение 10Base-2; максимальное число сегментов 5; максимальная длина сегмента 185 м; максимальное число узлов на одном сегменте 30; минимальное расстояние между узлами 0,5 м; скорость передачи данных по линии 10 Мбит/с.

3. **Вариант Twisted Pair Ethernet** (топология "звезда"); принятое обозначение 10Base-T; это кабельная сеть с использованием витых пар проводов и концентраторов, называемых также распределителями, или хабами (Hubs). В состав сетевого оборудования входят активные (АН) и пассивные (РН) распределители (Active and Passive Hubs), различие между которыми заключается в наличии или отсутствии усиления сигналов и в количестве портов. В одной из разновидностей сети 10Base-T допускаются расстояния между активными распределителями до 600 м и между пассивными до 30 м, предельное число узлов 100, скорость передачи данных по линии 100 Мбит/с.

4. **Вариант Fiber Optic Ethernet** (шина на основе оптоволоконного кабеля), обозначение 10Base-F; применяется для соединений "точка-точка", например, для соединения двух конкретных распределителей в кабельной сети. Максимальные длины - в пределах 2...4 км.

5. **Вариант RadioEthernet** (стандарт IEEE 802.11). Среда передачи данных - радиоволны, распространяющиеся в эфире. Применяется модифицированный метод МДКН/ОК, в котором вместо обнаружения конфликтов используется предотвращение конфликтов. Выполняется это тем, что узел, запрашивающий связь, посылает в эфир специальный кадр запроса, а передачу информации он может начать только после истечения межкадрового промежутка времени Т, если за время Т после запроса в эфире не было других запросов. Иначе попытка передачи откладывается на случайное время. Любой узел может посылать кадр запроса, только если за время Т перед этим в эфире не было других кадров запроса.

6. **Высокоскоростные разновидности Ethernet.**

Сеть **Fast Ethernet**, иначе называемая 100BaseX или 100Base-T (стандарт IEEE 802/30). Информационная скорость 100 Мбит/с. В Fast Ethernet применен метод доступа МДКН/ОК. Используется для построения скоростных ЛВС (последовательно включается не более двух хабов), для объединения низкоскоростных подсетей 10Base-T в единую скоростную сеть и для подключения серверов на расстояниях до 200 м. В последнем случае серверы соединяются с клиентскими узлами через шину 100 Мбит/с и коммутатор,

называемый также конвертором или переключателем скорости 100/10. К конвертору с другой стороны подключено несколько шин 10 Мбит/с, на которые нагружены остальные узлы. Практически можно использовать до 250 узлов, теоретически - до 1024.

Гигабитные скорости достигнуты в **1000Base-X** - варианте **Gigabit Ethernet** сети Ethernet. В соответствии со стандартом IEEE 802.3z имеются разновидности на ВОЛС с длиной волны 830 или 1270 нм (1000Base-SX и 1000Base-LX), расстояния до 550 м, и на витой паре категории 5 (1000BaseCX) на расстояниях до 25 м. Скорость до **1 Гбит/с**. Гигабитная скорость достигается благодаря следующим решениям. Сеть имеет иерархическую структуру. Участки (отдельные компьютеры или подсети) по 10 Мб/с подключаются к портам переключателей (switches) скорости 10/100, их выходы по 100 Мб/с, в свою очередь, подключаются к портам переключателей 100/1000. В сегментах сети, имеющих 1000 Мб/с, используются, во-первых, передача данных по ВОЛС или параллельно по 4 витым парам, во-вторых, 5-уровневое представление данных (например, +2, +1, 0, -1, -2 В), в-третьих, кодирование 8b/10b. В результате в каждой витой паре имеем 250 Мб/с при частоте сигналов 125 МГц.

Компоненты локальной сети

1. Аппаратные средства.
2. Каналы передачи данных.
3. Программное обеспечение (операционные системы).

Аппаратные средства ЛВС

В список сетевого оборудования ЛВС входят **моноканалы** (другие названия - сегменты, стволы), представляющие собой физические линии передачи данных; **сетевые контроллеры** (адаптеры, сетевые карты), управляющие доступом к каналу связи; **приемопередатчики**, служащие для связи сетевого контроллера с моноканалом; блоки взаимодействия данной сети (или подсети) с другими сетями (подсетями); **терминаторы** - устройства согласования сопротивлений на концах моноканалов для исключения искажающих отражений сигналов; **концентраторы** (Hubs) - коммутирующие устройства в сетях звездной архитектуры; концентраторы оконечных систем - для подключения нескольких ООД; **коннекторы** - для механического и непосредственного электрического подключения узлов к кабелю.

В качестве **линий передачи данных** в ЛВС используют коаксиальный кабель, витую (скрученную) пару проводов, волоконно-оптический кабель. Длины используемых отрезков коаксиального кабеля не должны превышать нескольких сотен метров, а у витой пары проводов - десятков метров. При больших расстояниях в среду передачи данных включают формирователи сигналов - повторители для сопряжения отрезков. Волоконно-оптический кабель позволяет существенно увеличить расстояния и скорость передачи данных.

Сетевой контроллер (адаптер) - устройство для связи ООД со средой передачи данных. Блок доступа к каналу называется также средством уровня MAC и реализует принятый метод доступа.

Концентраторы предназначены для объединения в сеть многих узлов. Концентраторами являются **хабы** в Token Ring. Хабы могут быть пассивными и активными, в последнем случае в хабе имеются усилители-формирователи подводимых сигналов. Такие концентраторы создают общую среду передачи данных без разделения трафика.

Коммутаторы в отличие от концентраторов предназначены для объединения в сеть многих узлов или подсетей с возможностью создания одновременно нескольких

соединений. Они называются также переключателями (свитчами – switch). Коммутаторы используются также для связи нескольких ЛВС с территориальной сетью. Коммутатор может объединять несколько как однотипных, так и разнотипных ЛВС.

Использование коммутаторов вместо маршрутизаторов (там, где это возможно) позволяет существенно повысить пропускную способность сети. Коммутатор работает с локальными MAC-адресами, в нем имеется таблица соответствия MAC-адресов и портов. Кроме того, между разными портами коммутатора образуется несколько соединений, по которым пакеты могут передаваться одновременно. В тоже время маршрутизатор оперирует IP-адресами и таблицами маршрутизации и выполняет сложные алгоритмы маршрутизации.

Приемопередатчик ПП (transiver) - устройство для электрического соединения АКД с линией передачи данных.

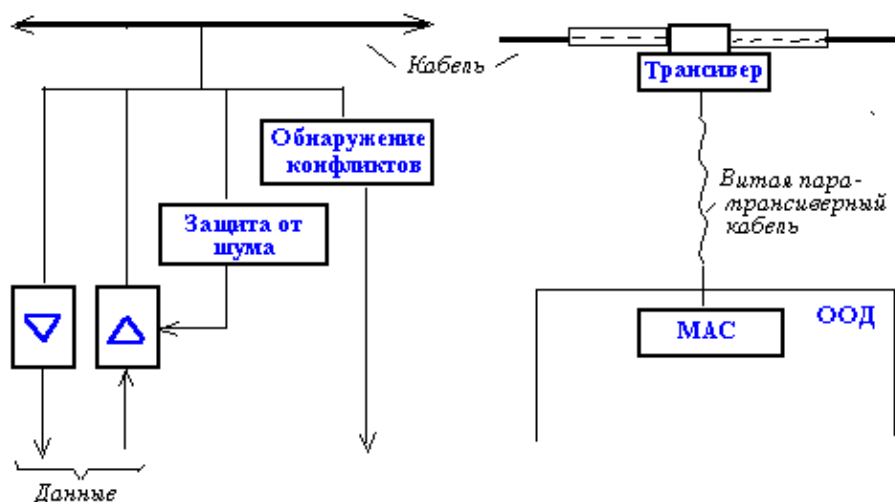


Рисунок 1 – Приемопередатчик в шинной сети

В состав приемопередатчика (рис. 1) в магистральных ЛВС с методом МДКН/ОК входят:

- **приемник сигналов** от линии передачи данных; его назначение - усиление информационных сигналов и обнаружение конфликтов путем выделения постоянной составляющей искаженных сигналов и ее сопоставления в компараторе с эталонным напряжением;
- **передатчик** от станции в линию; обычно реализуется в виде токового переключателя или балансной схемы на насыщенных транзисторах с трансформаторным выходом;
- **ответвитель** для подсоединения входов приемника и выходов передатчика к кабелю; применяется механическое контактирующее устройство, накладываемое на кабель и имеющее винт-иглу, которой прокалывается оплетка кабеля и осуществляется контакт с центральным проводником; игольчатый контакт имеет трансформаторную связь с приемником и передатчиком сигналов;
- **защита от шума** для отключения ООД от кабеля, если ООД ошибочно генерирует сигналы дольше, чем это предусмотрено.

II. СТЕК ПРОТОКОЛОВ TCP/IP

2.1. История и перспективы стека TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) - это промышленный стандарт стека протоколов, разработанный для глобальных сетей.

Стандарты TCP/IP опубликованы в серии документов, названных Request for Comment (RFC). Документы RFC описывают внутреннюю работу сети Internet. Некоторые RFC описывают сетевые сервисы или протоколы и их реализацию, в то время как другие обобщают условия применения. Стандарты TCP/IP всегда публикуются в виде документов RFC, но не все RFC определяют стандарты.

Стек был разработан по инициативе Министерства обороны США (Department of Defence, DoD) более 20 лет назад для связи экспериментальной сети ARPAnet с другими спутниковыми сетями как набор общих протоколов для разнородной вычислительной среды. Сеть ARPAnet поддерживала разработчиков и исследователей в военных областях. В сети ARPAnet связь между двумя компьютерами осуществлялась с использованием протокола Internet Protocol (IP), который и по сей день является одним из основных в стеке TCP/IP и фигурирует в названии стека.

Большой вклад в развитие стека TCP/IP внес университет Беркли, реализовав протоколы стека в своей версии ОС UNIX. Широкое распространение ОС UNIX привело и к широкому распространению протокола IP и других протоколов стека. На этом же стеке работает всемирная информационная сеть Internet, чье подразделение Internet Engineering Task Force (IETF) вносит основной вклад в совершенствование стандартов стека, публикуемых в форме спецификаций RFC.

Если в настоящее время стек TCP/IP распространен в основном в сетях с ОС UNIX, то реализация его в последних версиях сетевых операционных систем для персональных компьютеров (Windows NT 3.5, NetWare 4.1, Windows 95) является хорошей предпосылкой для быстрого роста числа установок стека TCP/IP.

Итак, лидирующая роль стека TCP/IP объясняется следующими его свойствами:

- Это наиболее законченный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю.
- Почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP.
- Это метод получения доступа к сети Internet.
- Этот стек служит основой для создания intranet- корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW, разработанную в Internet.
- Все современные операционные системы поддерживают стек TCP/IP.

- Это гибкая технология для соединения разнородных систем как на уровне транспортных подсистем, так и на уровне прикладных сервисов.
- Это устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер.

2.2. Структура стека TCP/IP. Краткая характеристика протоколов

Так как стек TCP/IP был разработан до появления модели взаимодействия открытых систем ISO/OSI, то, хотя он также имеет многоуровневую структуру, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Структура протоколов TCP/IP приведена на рисунке 2. Протоколы TCP/IP делятся на 4 уровня.

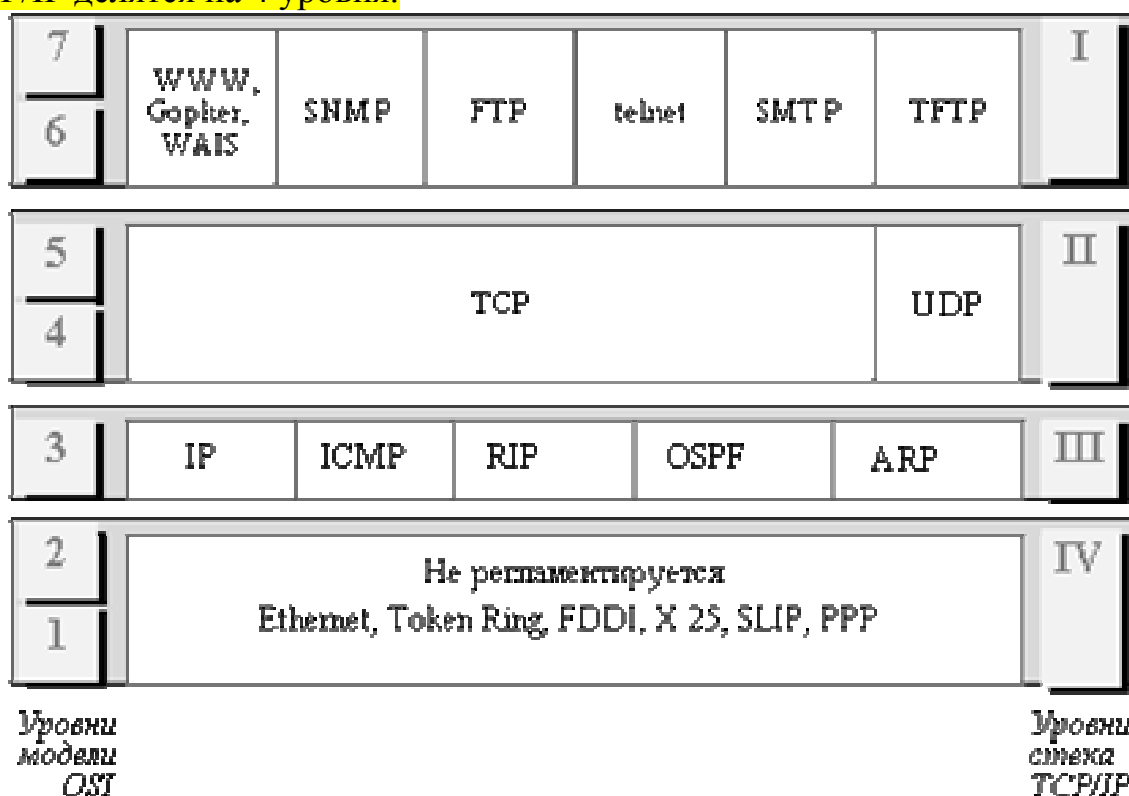


Рисунок 2 – Стек TCP/IP

Самый нижний (**уровень IV**) соответствует физическому и каналному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и каналного уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальных сетей - протоколы соединений "точка-точка" SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана также специальная спецификация, определяющая использование технологии ATM в качестве транспорта каналного уровня. Обычно при появлении новой технологии локальных или глобальных сетей она быстро включается в стек TCP/IP за счет разработки

соответствующего RFC, определяющего метод инкапсуляции пакетов IP в ее кадры.

Следующий уровень (**уровень III**) - это уровень межсетевого взаимодействия, который занимается передачей пакетов с использованием различных транспортных технологий локальных сетей, территориальных сетей, линий специальной связи и т. п.

В качестве основного протокола сетевого уровня (в терминах модели OSI) в стеке используется протокол IP, который изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Протокол IP является дейтаграммным протоколом, то есть он не гарантирует доставку пакетов до узла назначения, но старается это сделать.

К уровню межсетевого взаимодействия относятся и все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом - источником пакета. С помощью специальных пакетов ICMP сообщается о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т.п.

Следующий уровень (**уровень II**) называется основным. На этом уровне функционируют протокол управления передачей TCP (Transmission Control Protocol) и протокол дейтаграмм пользователя UDP (User Datagram Protocol). Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами.

Верхний уровень (**уровень I**) называется прикладным. За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и сервисов прикладного уровня. К ним относятся такие широко используемые протоколы, как протокол копирования файлов FTP, протокол эмуляции терминала telnet, почтовый протокол SMTP, используемый в электронной почте сети Internet, гипертекстовые сервисы доступа к удаленной информации, такие как WWW и многие другие. Остановимся несколько подробнее на некоторых из них.

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Для того, чтобы обеспечить надежную передачу,

FTP использует в качестве транспорта протокол с установлением соединений - TCP. Кроме пересылки файлов протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде, чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов Internet парольная аутентификация не требуется, и ее обходят за счет использования для такого доступа предопределенного имени пользователя Anonymous.

В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Приложения, которым не требуются все возможности FTP, могут использовать другой, более экономичный протокол - простейший протокол пересылки файлов TFTP (Trivial File Transfer Protocol). Этот протокол реализует только передачу файлов, причем в качестве транспорта используется более простой, чем TCP, протокол без установления соединения - UDP.

Протокол telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленного компьютера. При использовании сервиса telnet пользователь фактически управляет удаленным компьютером так же, как и локальный пользователь, поэтому такой вид доступа требует хорошей защиты. Поэтому серверы telnet всегда используют как минимум аутентификацию по паролю, а иногда и более мощные средства защиты, например, систему Kerberos.

Протокол SNMP (Simple Network Management Protocol) используется для организации сетевого управления. Изначально протокол SNMP был разработан для удаленного контроля и управления маршрутизаторами Internet, которые традиционно часто называют также шлюзами. С ростом популярности протокол SNMP стали применять и для управления любым коммуникационным оборудованием - концентраторами, мостами, сетевыми адаптерами и т.д. и т.п. Проблема управления в протоколе SNMP разделяется на две задачи.

Первая задача связана с передачей информации. Протоколы передачи управляющей информации определяют процедуру взаимодействия SNMP-агента, работающего в управляемом оборудовании, и SNMP-монитора, работающего на компьютере администратора, который часто называют также консолью управления. Протоколы передачи определяют форматы сообщений, которыми обмениваются агенты и монитор.

Вторая задача связана с контролируруемыми переменными, характеризующими состояние управляемого устройства. Стандарты регламентируют, какие данные должны сохраняться и накапливаться в устройствах, имена этих данных и синтаксис этих имен. В стандарте SNMP определена спецификация информационной базы данных управления сетью.

Эта спецификация, известная как база данных MIB (Management Information Base), определяет те элементы данных, которые управляемое устройство должно сохранять, и допустимые операции над ними.

III. ТЕХНОЛОГИЯ WWW

В течение последних лет предпринималось немало попыток разработать концепцию универсальной информационной базы данных, в которой можно было бы не только получать информацию из любой точки земного шара, но и иметь удобный способ связи информационных сегментов друг с другом, так чтобы наиболее важные данные быстро могли быть найдены. В 60-е годы исследования в этой области породили понятие "информационной Вселенной" (docuverse = documentation + universe), которая преобразила бы всю информационную деятельность, в частности в области образования. Но только в настоящее время появилась технология, воплотившая эту идею и предоставляющая возможности ее реализации в масштабах планеты.

WWW -- это аббревиатура от "World Wide Web" ("*Всемирная паутина*"). Официальное определение World Wide Web звучит как мировая виртуальная файловая система -- "широкомасштабная гипермедиа-среда, ориентированная на предоставление универсального доступа к документам".

Проект WWW возник в начале 1989 года в Европейской Лаборатории физики элементарных частиц ([European Laboratory for Particle Physics \(CERN\) in Geneva, Switzerland](#)). Основное назначение проекта -- предоставить пользователям не профессионалам "on-line" доступ к информационным ресурсам. Результатом проекта World Wide Web (WWW, W3) является предоставление пользователям сетевых компьютеров достаточно простого доступа к самой разнообразной информации.

WWW технология является самым популярным и наиболее бурно развивающимся сервисом Internet. В течении двух-трех лет WWW технология прочно встала на ноги и, начиная 1993 года, семимильными шагами пошла завоевывать МИР.

Первый такой сервер был организован в CERN'e, там же с целью развития и поддержки стандартов WWW технологий создан [The World Wide Web Consortium](#) (или W3C). WWW сервер [The W3C's Web site](#) является интегрирующим сервером по поддержке WEB технологий Internet. Последнюю информацию о состоянии WWW проекта можно получить по адресу [W3C Project](#).

Позднее к проекту подключились и многие другие организации. Большой вклад в развитие WWW технологий внес Национальный центр суперкомпьютерных приложений ([National Centre for Supercomputing Applications -- NCSA](#)).

Технология World Wide Web базируется на трех важных стандартах. Первый из них -- **URL** (*Universal*, или *Uniform Resource Locator*, универсальный адрес ресурса) -- предоставляет стандартный способ задания местоположения данных, доступных в глобальной компьютерной сети Интернет.

Второй -- протокол **HTTP** (*Hyper Text Transfer Protocol*, *протокол передачи гипертекста*) -- предоставляет доступ к информации и позволяет передавать гипертекстовые документы по сети.

Наконец, **HTML** (*Hyper-Text Markup Language*, *язык разметки гипертекста*) позволяет создавать текстовые документы, включающие ссылки на URL других данных. Зачастую эти ссылки указывают на другие документы HTML, которые, в свою очередь, доступны с помощью HTTP. В результате перед пользователем расстилается огромная паутина взаимосвязанной информации.

3.1. Гипертекст

Информационный WWW сервер использует гипертекстовую технологию. когда каждый человек, знающий, что такое телефон, будет знать, что такое WWW.

WWW работает по принципу клиент-сервер, точнее, клиент-серверы: существует множество серверов, которые по запросу клиента возвращают ему гипермедийный документ - документ, состоящий из частей с разнообразным представлением информации, в котором каждый элемент может являться ссылкой на другой документ или его часть. Ссылки эти в документах WWW организованы таким образом, что каждый информационный ресурс в глобальной сети Интернет однозначно адресуется, и документ, который Вы читаете в данный момент, способен ссылаться как на другие документы на этом же сервере, так и на документы (и вообще на ресурсы Интернет) на других компьютерах Интернет. Причем пользователь не замечает этого, и работает со всем информационным пространством Интернет как с единым целым. Ссылки WWW указывают не только на документы, специфичные для самой WWW, но и на прочие сервисы и информационные ресурсы Интернет. Более того, большинство программ-клиентов WWW (browsers, навигаторы) не просто понимают такие ссылки, но и являются программами-клиентами соответствующих сервисов: ftp, gopher, сетевых новостей Usenet, электронной почты и т.д. Таким образом, программные средства WWW являются универсальными для различных сервисов Интернет, а сама информационная система WWW играет интегрирующую роль.

3.2. HTML

В основе WWW технологии лежит язык HTML (HyperText Markup Language).

Для записи документов в гипертексте используется специальный, но

очень простой язык **HTML** (Hypertext Markup Language), который позволяет управлять шрифтами, отступами, вставлять цветные иллюстрации, поддерживает вывод звука и анимации. В стандарт языка также входит поддержка математических формул.

Для удобства ввода информации предусмотрены специальные **формы, меню**. Программы просмотра позволяют получать доступ не только к WWW серверам, но и к другим службам Internet. С их помощью можно путешествовать по **Gopher** серверам, искать информацию в **WAIS** базах, получать файлы с файловых серверов по протоколу **FTP**. Поддерживается протокол обмена сетевыми новостями Usenet **NNTP**.

Основное достоинство WWW состоит в создании гипертекстовых документов, и если Вас заинтересовал какой либо пункт в таком документе, то достаточно "ткнуть" в него курсором для получения нужной информации. Также в одном документе возможно делать ссылки на другие, написанные другими авторами или даже расположенные на другом сервере. Одно из главных преимуществ WWW над другими средствами поиска и передачи информации - "многосредность". В WWW можно увидеть на одной странице одновременно текст и изображение, звук и анимацию.

3.3. Средства просмотра WWW страниц

Для доступа к WWW вам необходимо запустить специальную программу **WWW-клиент -- просмотрщик** (browser -- браузер) для просмотра гипертекстовых страниц (например, Mosaic, MS Internet Explorer (MSIE) или Netscape Navigator (NN) - *последние два обладают наиболее развитыми средствами просмотра и имеют наибольшее распространение в мире "PC"*), которая может связываться с различными серверами и принимать от них информацию.

Графические просмотрщики (такие как Mosaic, Netscape, HotJava) позволяют не только читать текст, но и осмотреть содержащиеся в нем рисунки и звуковые файлы. Текстовые (Lynx) - представляют вам только текст.

Следует напомнить, что на сегодняшний день количество разработанных различных просмотрщиков (WWW-клиентов) составляет несколько десятков и не ограничивается фаворитами мира PC - NN и MSIE.

В настоящее время пока не существует общепринятого русского термина для программы, предназначенной для доступа к WWW серверам и просмотра WWW страниц, многие просто используют для этого английский термин "browser -- браузер", хотя встречается такие названия как "листатель" и "просмотрщик". Кстати фирмы, лидирующие в производстве таких программ (**Microsoft** и **Netscape Communication**) предлагают такие названия как "исследователь" и "навигатор". В данном пособии будет использоваться преимущественно термин **просмотрщик**.

Кроме доступа к WWW серверу, развитые программы-просмотрщики поддерживают протокол передачи файлов **FTP**, протокол обмена новостями

[NNTP](#), [GOPHER](#) имеют оболочку для организации работы с электронной почтой ([E-mail](#)). Список [методов доступа](#) постоянно растет. Также на многих WWW серверах имеется возможность доступа к различным базам данных.

Просмотрщики MS Internet Explorer и Netscape Navigator (версий 3.1 и старше) наиболее полно поддерживают стандарт языка HTML 3.2, хотя и не на 100 процентов, и имеет ряд расширений. Конкурентная борьба между фирмами [Microsoft](#) и [Netscape Communication](#) привела к тому, что разделила мир WWW на две части. Первая -- это страницы, рассчитанные на просмотр в первую очередь с помощью просмотрщика [MS Internet Explorer](#), и вторая -- это страницы, рассчитанные на [Netscape Navigator](#). Различие между этими двумя типами страниц не очень значительные, но отсутствие взаимозаменяемости часто вызывает раздражение.

Для создания активных WWW страниц используются наряду с языком HTML, язык программирования [Java](#) и технология ActiveX (фирмы Микрософт), а также скриптовые языки [JavaScript](#), [Perl](#) и Visual Basic Script.

URL -- специальная форма адреса информации в сети Интернет, содержащая данные об имени сервера, на котором хранится документ, путь к каталогу файла и собственно имя файла. URL-адрес состоит из двух частей. Сначала указывается *способ связи*, при помощи которого будет осуществляться доступ к данным. От этого зависит, какая дополнительная информация потребуется. Затем помещается информация о том, где эти данные *расположены*. Разделяются эти части двоеточием, например:

http://имя_сервера/путь/файл

Для работы с браузером необходимо указать адрес документа, который вы хотите просмотреть. Адрес документа называется **URL - Uniform Resource Locator** – универсальный локатор ресурса - имеет следующий вид (например):

<http://www.vvsu.ru/cts/index.htm>

здесь:

http:// - идентификатор ресурса - указание браузеру какой протокол или язык использовался при создании ресурса. В данном случае это *http*, предназначенный для работы с WWW (как правило, браузер поддерживает еще несколько протоколов, например *ftp* - для доступа к файловым архивам, но *http* является наиболее часто применяемым, и во многих браузерах указание “*http://*” можно опускать);

www.vvsu.ru - адрес (доменное имя) компьютера в Интернет (сервера WWW), на котором находится искомый документ; - **местоположение ресурса**

/cts/index.htm - путь к искомому файлу в формате Unix на сервере с указанием каталогов (директорий) и имени файла (*index.html*). Как правило, файлы для WWW имеют расширение *.htm* или *.html*. Часто путь к файлу и имя файла опускаются, в этом случае браузер запрашивает файл с именем *index.html* с самого верхнего (корневого) каталога сервера.

IV. СТРУКТУРА ИНТЕРНЕТ (INTERNET)

Internet представляет собой глобальную компьютерную сеть. Само ее название означает "между сетей". Это сеть, соединяющая отдельные сети.

Логическая структура Internet представляет собой некое виртуальное объединение, имеющее свое собственное информационное пространство.

Internet обеспечивает обмен информацией между всеми компьютерами, которые входят в сети, подключенные к ней. Тип компьютера и используемая им операционная система значения не имеют. Соединение сетей обладает громадными возможностями. С собственного компьютера любой абонент Internet может передавать сообщения в другой город, просматривать каталог библиотеки Конгресса в Вашингтоне, знакомиться с картинами на последней выставке в музее Метрополитен в Нью-Йорке, участвовать в конференции IEEE и даже в играх с абонентами сети из разных стран.

Internet предоставляет в распоряжение своих пользователей множество всевозможных ресурсов.

Основные ячейки Internet - локальные вычислительные сети. Это значит, что Internet не просто устанавливает связь между отдельными компьютерами, а создает пути соединения для более крупных единиц - групп компьютеров. Если некоторая локальная сеть непосредственно подключена к Internet, то каждая рабочая станция этой сети также может подключаться к Internet. Существуют также компьютеры, самостоятельно подключенные к Internet. Они называются хост-компьютерами (host - хозяин). Каждый подключенный к сети компьютер имеет свой адрес, по которому его может найти абонент из любой точки света.

Для подключения локальных сетей к Internet используются средства, рассмотренные ранее. Схема подключения локальной сети к Internet приведена на **рис. 3**. Важной особенностью Internet является то, что она, объединяя различные сети, не создает при этом никакой иерархии - все компьютеры, подключенные к сети, равноправны. Для иллюстрации возможной структуры некоторого участка сети Internet приведена схема соединения различных сетей **рис. 4**.

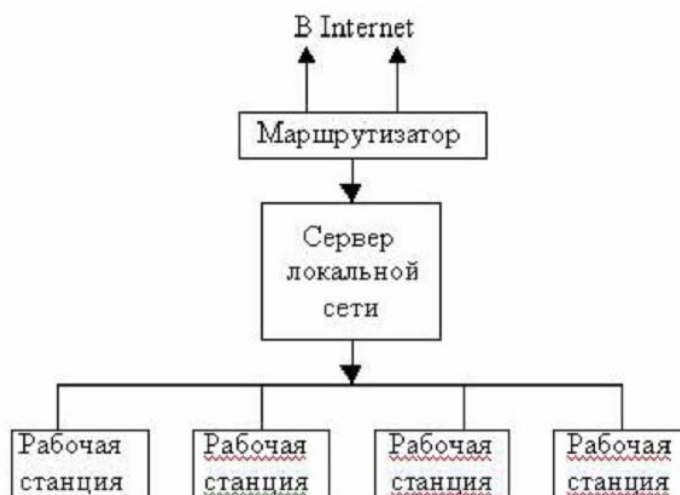


Рисунок 3 – Подключение локальной сети к Internet



Рисунок 4 – Подключение различных сетей к Internet

Internet – любое собрание отдельных физических сетей, объединенных общим протоколом для образования единой логической сети.

Интернет – структура, объединяющая различные сети – «сеть сетей». Интернет включает все сети, использующие протокол IP (Internet Protocol), которые кооперируются для создания единой сети своих пользователей. Не IP-сети подключаются к Интернету посредством шлюзов.

История Интернета.

1969 г. – экспериментальная сеть ARPAnet по заказу Минобороны США. Основные принципы, положенные в основу Интернета:

- сеть априори полагается ненадежной, т.е. любая ее часть может отказать в любой момент, при этом остальные должны оставаться работоспособными;

- любой компьютер связывается как равный с любым другим компьютером в сети.
- 1975 г. – ARPAnet – операционная сеть.
 1979 г. – локальные вычислительные сети.
 1983 г. – протокол TCP/IP.
 1985 г. – сеть NSFNet (национального научного фонда США), объединила 5 компьютерных центров университетов США.
 1995 г. – становление Internet как глобальной сети.
 Дальнейшее развитие Internet.

INTERNET – всемирное собрание взаимосвязанных сетей, которое выросло из ARPAnet и использует IP-протокол для связи различных физических сетей в единую логическую сеть.

V. АДРЕСАЦИЯ В IP-СЕТЯХ

Типы адресов: физический (MAC-адрес), сетевой (IP-адрес) и символичный (DNS-имя)

Каждый компьютер в сети TCP/IP имеет адреса **трех уровней**:

- **Локальный адрес узла**, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это **MAC-адрес** сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются **уникальными** адресами, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются **уникальным образом самим производителем**. Для узлов, входящих в глобальные сети, такие как X.25 или frame relay, локальный адрес назначается администратором глобальной сети.
- **IP-адрес, состоящий из 4 байт (логический 32-разрядный адрес – всего 2^{32} адресов)**, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время **конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла**. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла – гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

- Символьный идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или telnet.

ТРИ ОСНОВНЫХ КЛАССА IP-АДРЕСОВ

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:

128.10.2.30 – традиционная десятичная форма представления адреса,

10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса.

На рисунке 3.1 показана структура IP-адреса.

Класс А

0	N сети	N узла
<i>1ый бит</i>	<i>1 байт</i>	<i>3 байта</i>

Класс В

1	0	N сети	N узла
<i>1ый бит</i>	<i>2ой бит</i>	<i>2 байта</i>	<i>2 байта</i>

Класс С

1	1	0	N сети	N узла
<i>1ый бит</i>	<i>2ой бит</i>	<i>3ий бит</i>	<i>3 байта</i>	<i>1 байт</i>

Класс D

1	1	1	0	адрес группы multicast
---	---	---	---	------------------------

Класс E

1	1	1	1	0	зарезервирован
---	---	---	---	---	----------------

Рисунок 5 – Структура IP-адреса

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу А, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) В сетях класса А количество узлов должно быть больше 216, но не превышать 224.
- Если первые два бита адреса равны 10, то сеть относится к классу В и является сетью средних размеров с числом узлов 28 - 216. В сетях класса В под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса С с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Класс	Наименьший адрес	Наибольший адрес	Число адресов
A	01.0.0 – фиксированный 1ый байт	126.0.0.0	16 777116 – крупные поставщики
B	128.0.0.0 – фиксированные 1ые 2а байта	191.255.0.0	65536 - средние
C	192.0.1.0. - фиксированные 1ые 3и байта	223.255.255.0	256 - мелкие
D	224.0.0.0	239.255.255.255	
E	240.0.0.0	247.255.255.255	

Соглашения о специальных адресах: broadcast, multicast, loopback

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов:

- если IP-адрес состоит только из двоичных нулей,

0 0 0 0 0 0 0 0



то он обозначает адрес того узла, который сгенерировал этот пакет;

- если в поле номера сети стоят 0,

0 0 0 00

Номер узла

то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет;

- если все двоичные разряды IP-адреса равны 1,

1 1 1 1 1 1

то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);

- если в поле адреса назначения стоят сплошные 1,

Номер сети	1111.....11
------------	-------------

то пакет, имеющий такой адрес рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательным сообщением (broadcast);

- адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback.

Уже упоминавшаяся форма группового IP-адреса - multicast - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Такие сообщения в отличие от широковещательных называются мультивещательными. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

VI. ОТОБРАЖЕНИЕ СИМВОЛЬНЫХ АДРЕСОВ НА IP-АДРЕСА: СЛУЖБА DNS

DNS (Domain Name System) - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен - в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Единый каталог Интернета находится у SRI International (Калифорния, США). Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

- **com** - коммерческие организации (например, microsoft.com);
- **edu** - образовательные (например, mit.edu);
- **gov** - правительственные организации (например, nsf.gov);
- **org** - некоммерческие организации (например, fidonet.org);
- **net** - организации, поддерживающие сети (например, nsf.net);
- **biz** – бизнес цели.

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост (ПК, подключенный к Интернету и имеющий IP-адрес) в сети Internet однозначно определяется своим *полным доменным именем (fully qualified domain name, FQDN)*, которое включает имена всех доменов по направлению от хоста к корню.

Пример полного DNS-имени:

`inep.sfedu.ru`