



Кафедра «Автоматизированные станочные системы»

Dept. of Automated Manufacturing Systems

ОСНОВНЫЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ИНТЕРНЕТ

Интернет представляет собой глобальную компьютерную сеть.

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

Основные ячейки Интернет - локальные вычислительные сети.

Хост - компьютеры (host - хозяин) – компьютеры, самостоятельно подключенные к Интернет.

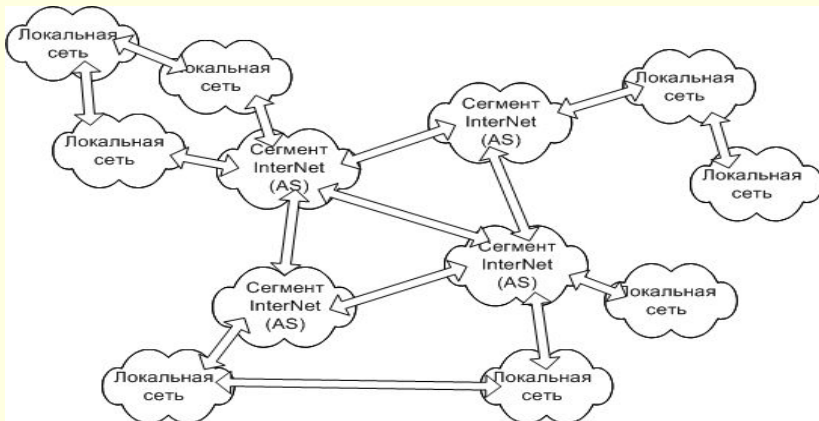
Каждый подключенный к сети компьютер имеет свой адрес (IP-адрес), по которому его может найти абонент из любой точки света.

Схема подключения глобальных сетей к Интернет



Особенностью Интернет является то, что она, объединяя различные сети, не создает при этом никакой иерархии – все компьютеры, подключенные к сети, **равноправны**.

Пример, соединение нескольких локальных сетей.



Административное устройство Интернет

Интернет - организация с полностью добровольным участием.

В Интернет нет единственной авторитарной фигуры. Совет старейшин представляет собой группу приглашенных добровольцев, называемую **IAB (Совет по архитектуре Интернет)**.

IAB регулярно собирается, чтобы принять стандарты и распределить ресурсы, такие, например, как адреса.

Пользователи Интернет высказывают свои жалобы и предложения на встречах **IETF (Оперативного инженерного отряда Интернет)**.

IETF - это другая добровольная организация; также собирается регулярно, чтобы обсудить текущие эксплуатационные и назревающие технические проблемы

Службы Интернет:

E-mail. Служит для отправки электронных документов конкретным абонентам. Посылаемые сообщения могут состоять как из текста, так и включать звуки, графику и прочие ресурсы.

Newsgroups. Группы новостей, которые организованы по принципу доски объявлений. Поступающая от пользователей информация группируется по различным темам.

Chat. Данная служба предоставляет возможность пользователям, подключенных к Интернет, общаться в реальном времени посредством сообщений, набираемых на клавиатуре.

FTP. Обеспечивает доступ к удаленному компьютеру. Использует протокол *FTP* (File Transfer Protocol), который дает возможность пользователю немедленно передать файл через Интернет из одного места в другое.

WWW (*World Wide Web*). Механизм в Интернет, который применяет *гипертекстовые связи* для соединения страниц и ресурсов и позволяет осуществлять переадресацию при просмотре документов.

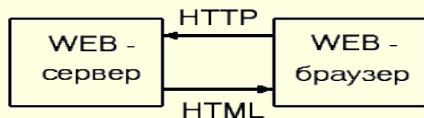
Протокол HTTP и соглашение о URL

Для работы WWW используется протокол *HTTP* (HyperText Transfer Protocol), который обеспечивает обмен гипертекстовой информацией между *Web-сервером* и *Web-браузером*.

Web-сервер — элемент WWW, который выдает информацию (в виде гипертекста) для пользователя.

Программа, с помощью которой пользователь запрашивает информацию у Web-сервера и просматривает ее, называется **Web-браузером**.

Взаимодействие между Web-сервером и Web-браузером



Гипертекстовая информация, посылаемая пользователю и просматриваемая посредством Web-браузера, описывается с помощью специального языка **HTML (HyperText Markup Language)**, который помимо текста допускает использование специальных описателей или **тегов** для разметки страницы, управления шрифтом, цветом и вставки в текст различных объектов (графики, звука и т. п.).

Чтобы идентифицировать полный путь к документу, графическому или другому файлу, в Интернет используется **URL (Uniform Resource Locator)** — унифицированный адрес ресурса.

Uniform Resource Locator имеет следующий формат:

[protocol://server/path](#)

Здесь [protocol](#) – это имя операции, которая будет выполняться при интерпретации данного URL.

[Сервер \(server\)](#) - имя сервера (необязательно). Если имя сервера не указано, то ссылка считается локальной, и полный путь, указанный далее в URL, вычисляется на той машине, с которой взят HTML-документ, содержащий данную ссылку.

[Путь \(path\)](#) - частичный или полный путь к документу, который должен вызваться в результате интерпретации URL.

Примеры использования URL:

<http://www.someones.homepage/default.html>

<ftp://ftp.server.somewhere/ftp.file>

<file://Server/Share/File.doc>

Структура адресов Интернет

Чтобы узнать адрес вашего компьютера, в командной строке наберите команду **ipconfig**.

Команда выдаст сообщение следующего вида:

```
Настройка протокола IP для Windows
Подключение по локальной сети - Ethernet адаптер:
DNS-суффикс этого подключения . . : ass.tula.ru
IP-адрес . . . . . : 192.168.107.10
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 192.168.107.1
```

DNS (англ. *Domain Name System* — система доменных имён) — это система, позволяющая преобразовывать символьные имена доменов (URL) в IP-адреса — система доменных имён) — это система, позволяющая преобразовывать символьные имена доменов (URL) в IP-адреса (и наоборот) в сетях ТСР/ИР

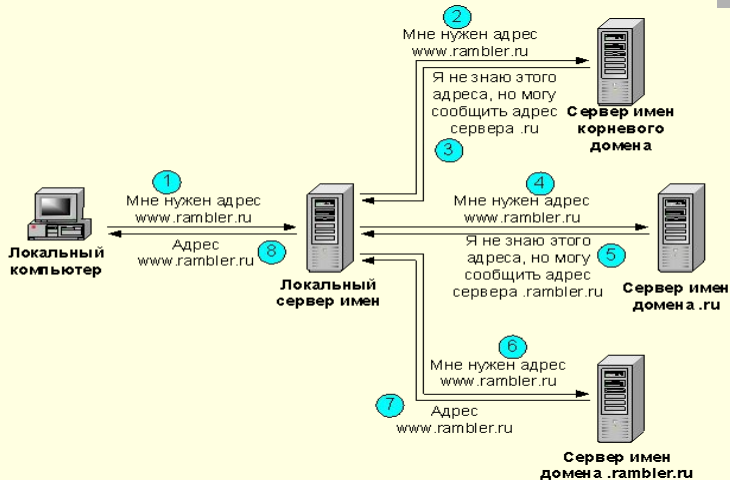
Домен — определённая зона в системе доменных имён (DNS, Domain Name System) Интернета, выделенная какой-либо стране, организации или для иных целей.

Доменное имя содержит, как минимум, две части (обычно называются *метками*), разделённые точкой.

Самая правая метка является **доменом верхнего уровня** (например, для адреса `ru.wikipedia.org` домен верхнего уровня — `org`). Каждая следующая метка справа налево является **поддоменом** (например, `wikipedia.org` — поддомен домена `org`, а `ru.wikipedia.org` — домена `wikipedia.org`).

Система DNS содержит иерархию *серверов DNS*. Каждый домен или поддомен поддерживается как минимум одним *авторитетным сервером DNS* (от англ. *authoritative* — авторитетный, заслуживающий доверия), на котором расположена информация о домене. Иерархия серверов DNS совпадает с иерархией доменов.

Функционирование службы DNS



Маршрутизация в Интернет

Маршрут - это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения.

Маршрутизация в сети Интернет - пакетная.

Маршрутизаторы объединяют отдельные сети в общую составную сеть. К каждому маршрутизатору могут быть присоединены несколько сетей (по крайней мере две).

За связь со шлюзом отвечают задаваемые в настройках соединения параметры "Маска подсети" и "Основной шлюз".

Маршрутизация



Маской подсети или **маской сети** называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети.

Маска назначается по следующей схеме $2^8 - n$, где n - количество компьютеров в подсети + 2, округленное до ближайшей большей степени двойки.

Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции (логическое И).

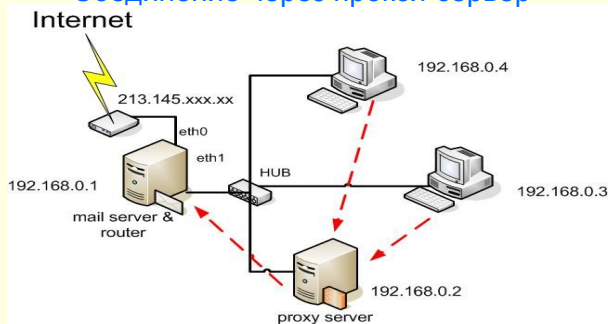
Например:

IP-адрес:	00001100 00100010 00111000 01001110	(12.34.56.78)
Маска подсети:	11111111 11111111 11100000 00000000	(255.255.224.0)
Адрес сети:	00001100 00100010 00100000 00000000	(12.34.32.0)

Прокси-серверы

Прокси-сервер (от англ. proxy — «представитель, уполномоченный») — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам.

Соединение через прокси-сервер



Чаще всего прокси-серверы применяются для следующих целей:

1. Обеспечение доступа с компьютеров локальной сети в Интернет.
2. Кэширование данных: если часто происходят обращения к одним и тем же внешним ресурсам, то можно держать их копию на прокси-сервере и выдавать по запросу, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентом запрошенной информации.
3. Сжатие данных: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде. Такие прокси-серверы используются в основном с целью экономии внешнего трафика.
4. Защита локальной сети от внешнего доступа: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер).

5. Ограничение доступа из локальной сети к внешней: например, можно запретить доступ к определённым веб-сайтам, ограничить использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы.

6. Анонимизация доступа к различным ресурсам. Прокси-сервер может скрывать сведения о источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например, IP-адрес, но не имеет возможности определить истинный источник запроса. Существуют также искажающие прокси-серверы, которые передают целевому серверу ложную информацию об истинном пользователе.