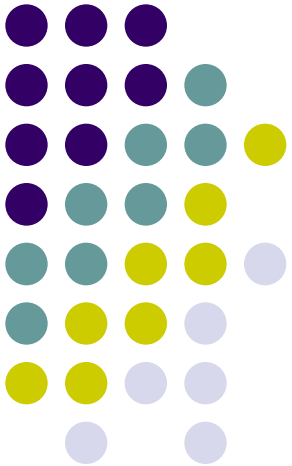
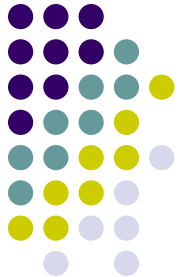
Администрирование информационных систем

Сети, их администрирование

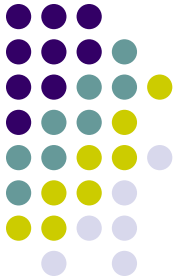


Протоколы TCP/IP



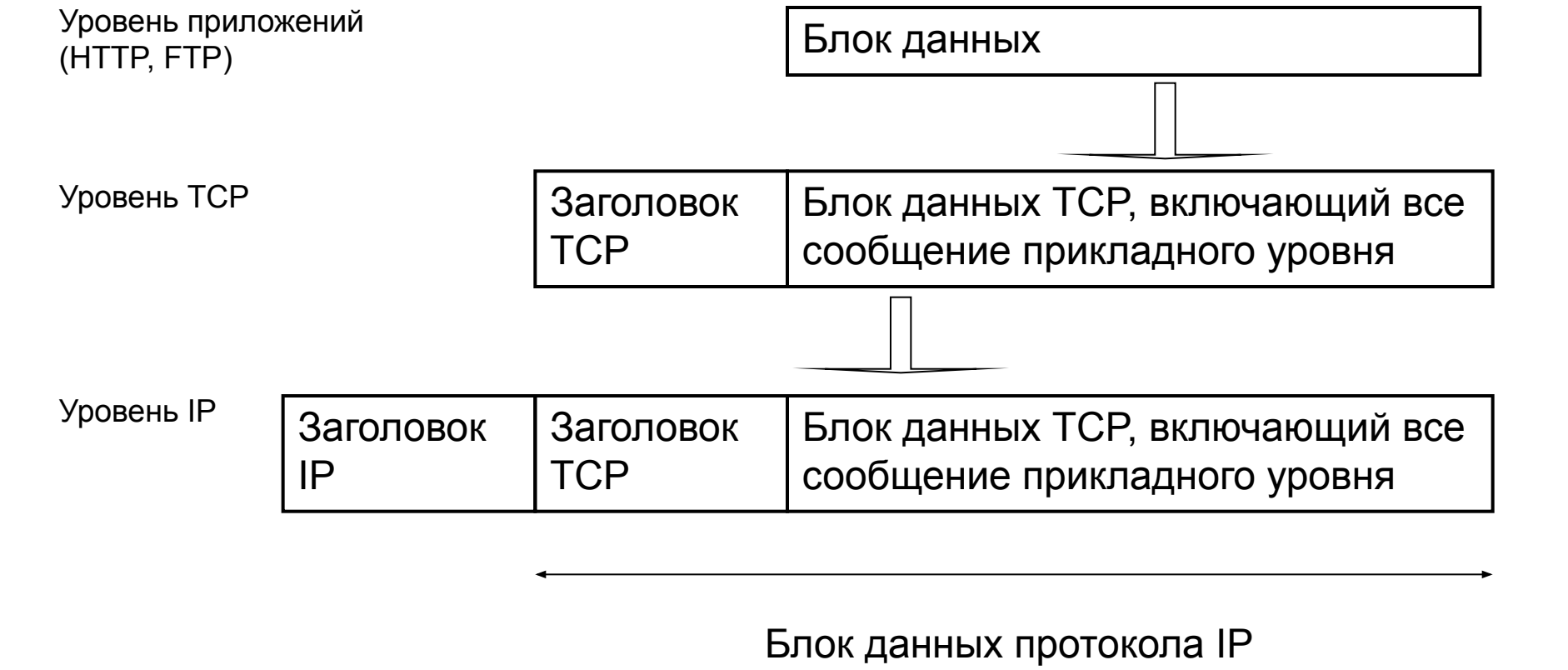
- Под термином "TCP/IP" обычно рассматривается все, что связано с протоколами TCP и IP. Это не только собственно сами проколы с указанными именами, но и протоколы построенные на использовании TCP и IP, и прикладные программы.
- Главной задачей стека TCP/IP – объединение в сеть пакетных подсетей через шлюзы. Каждая сеть работает обеспечивает обмен данными внутри собственной сети, однако предполагается, что шлюз может принять пакет из другой сети и доставить его по указанному адресу. Пакет из одной сети передается в другую подсеть через последовательность шлюзов, которые обеспечивают сквозную маршрутизацию пакетов по всей сети.
- Под **шлюзом** понимается точка соединения сетей. При этом соединяться могут как локальные сети, так и глобальные сети. В качестве шлюза могут выступать как специальные устройства, маршрутизаторы, например, так и компьютеры, которые имеют программное обеспечение, выполняющее функции маршрутизации пакетов.
- **Маршрутизация** – это процедура определения пути следования пакета из одной сети в другую.

Основные понятия передачи данных в сетях TCP/IP

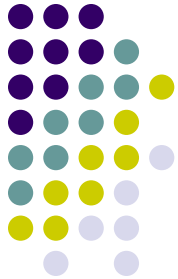


- ***Кадр*** - это блок данных, который принимает/отправляет сетевой интерфейс.
- ***IP-пакет*** - это блок данных, которым обменивается модуль IP с сетевым интерфейсом.
- ***UDP-датаграмма*** - блок данных, которым обменивается модуль IP с модулем UDP.
- ***TCP-сегмент*** - блок данных, которым обменивается модуль IP с модулем TCP.
- ***Прикладное сообщение*** - блок данных, которым обмениваются программы сетевых приложений с протоколами транспортного 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 случае инкапсуляции IP в Ethernet речь идет 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.

Инкапсуляция протоколов верхнего уровня в протоколы TCP/IP



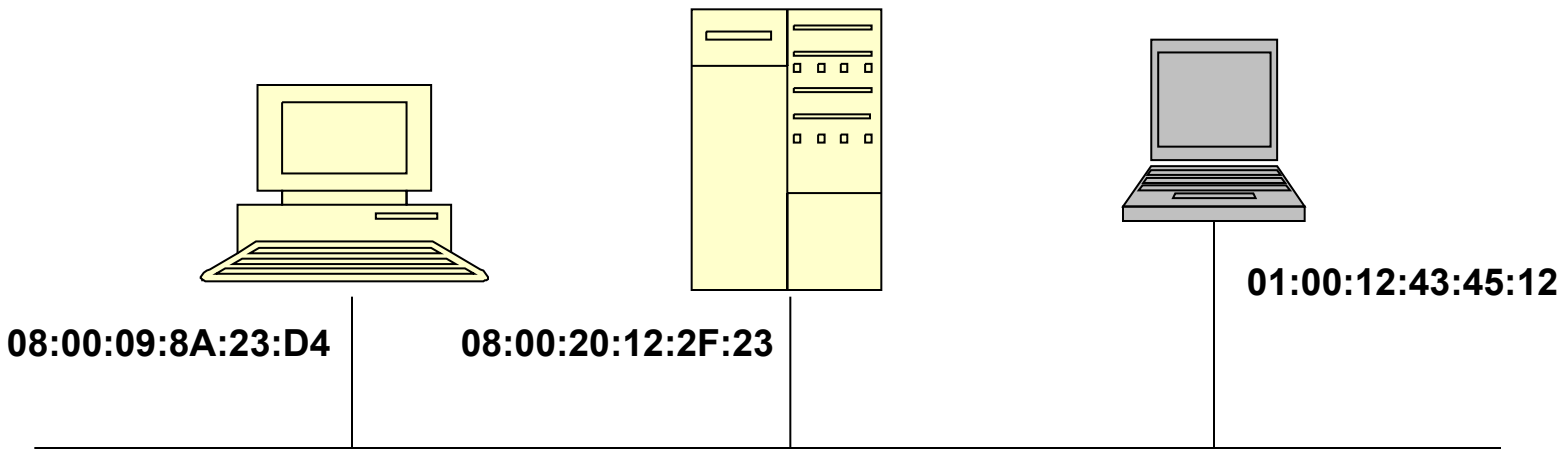
Локальные вычислительные сети и физический уровень



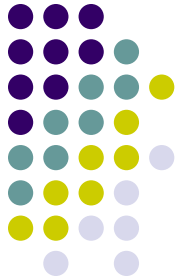
- ***Локальные вычислительные сети*** – высокоскоростные сети с малым количеством ошибок, охватывающие небольшие географические пространства.
- Наиболее распространенными технологиями ЛВС являются
  - Ethernet
  - Fiber Distributed Data Interface (FDDI)
  - Token Ring
- Стандарт Ethernet наиболее распространенным стандартом организации ЛВС. Существует несколько вариантов (IEEE 802.3)

ЛВС и канальный уровень

- Канальный уровень протоколов Ethernet обеспечивает транспортировку данных по физическому, непосредственно соединяющих два устройства.
- Для адресации к сетевым устройствам используются *адреса управления доступом к среде передачи данных* (MAC-адреса).
- Кадр Ethernet содержит адрес назначения, адрес источника, поле типа и данные. Размер MAC-адреса – 6 байтов. Каждый сетевой адаптер имеет свой сетевой адрес. Адаптер "слушает" сеть, принимает адресованные ему кадры и широковещательные кадры с адресом FF:FF:FF:FF:FF:FF, отправляет кадры в сеть.

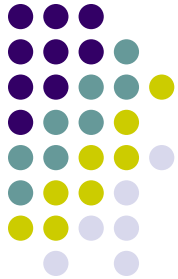


Протокол IP



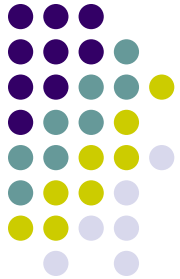
- Протокол IP является самым главным во всей иерархии протоколов семейства TCP/IP. Используется для управления рассылкой TCP/IP пакетов по сети Internet. Среди различных функций, возложенных на IP обычно выделяют следующие:
  - определение пакета, который является базовым понятием и единицей передачи данных в сети Internet. Такой IP-пакет называют датаграммой;
  - определение адресной схемы, которая используется в сети Internet;
  - передача данных между канальным уровнем (уровнем доступа к сети) и транспортным уровнем (другими словами мультиплексирование транспортных датаграмм во фреймы канального уровня);
  - маршрутизация пакетов по сети, т.е. передача пакетов от одного шлюза к другому с целью передачи пакета машине-получателю;
  - "нарезка" и сборка из фрагментов пакетов транспортного уровня.

IP-адресация



- IP-адресация – основа протокола IP (Internet Protocol). Каждая ЛВС должна иметь уникальный IP-адрес. Внутри сети каждый узел имеет IP-адрес, который представляет собой уникальный 32-разрядный логический адрес.
- IP-адресация реализуется на сетевом уровне. В отличие от MAC-адресов, где адреса образуют плоское адресное пространство, IP-адреса имеют иерархическую структуру.
- Каждая организация рассматривается как отдельная уникальная сеть, с которой устанавливается соединение и после этого осуществляется связь с отдельным хостом.

Классы IP-адресов



- Каждый 32-разрядный IP-адрес разделяется на 4 октета:
  - xxx.xxx.xxx.xxx, где xxx – некоторое число из диапазона 0-255.
- Каждый IP-адрес состоит из двух частей: номера сети и номера хоста.
- Класс A составляют адреса, зарезервированные для правительственных учреждений;
- Класс B – адреса для организаций среднего размера
- Класс C – адреса для остальных организаций

Класс A

0	Номер сети (7 битов)	Номер хоста (24 бита)

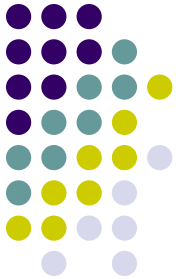
Класс B

1	0	Номер сети (14 битов)	Номер хоста (16 битов)

Класс C

1	1	0	Номер сети (21 бит)	Номер хоста (8 битов)

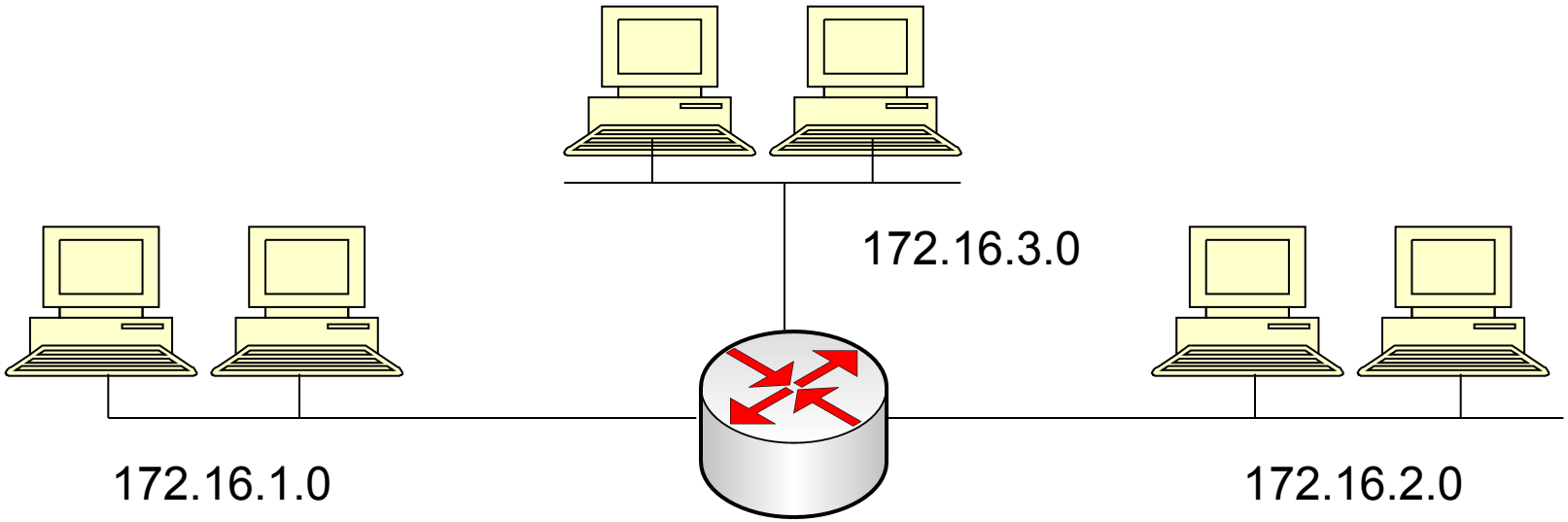
Классы IP-адресов



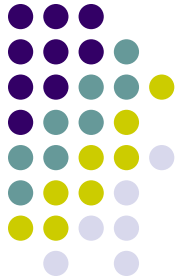
Класс	Диапазон значений первого октета	Возможное количество сетей	Возможное количество узлов
A	1 - 126	126	16777214
B	128 - 191	16382	65534
C	192 - 223	2097150	254
D	224 - 239	-	228
E	240 - 247	-	227

Подсети

- Для нужд организации выделенная сеть может быть разбита на отдельные части – подсети. Также как и адрес сети, адрес подсети является уникальным. Использование подсети не влияет на внешних пользователей, но в пределах организации подсеть рассматривается как структурная единица.

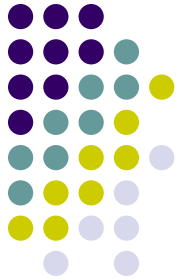


Маскирование подсетей



- Подсети скрыты от внешнего мира с помощью масок, называемых **масками подсети**. С их помощью устройствам сообщается какая часть является адресом подсети, а какая – адресом хоста.
- Маска подсети представляет собой 32 разрядное двоичное число разделена на 4 октета, подобно IP-адресу. Маска подсети имеет все единицы в части, отвечающей сети и подсети, и нули, в части отвечающей адресу хоста.
- Например, для сетей 172.16.1.0 – 172.16.254.0 маска будет иметь вид 255.255.255.0.

Протоколы ARP и RARP

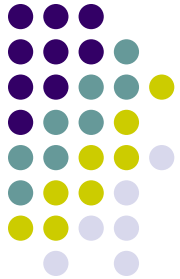


- **Протокол ARP (RFC 826)**. *Address Resolution Protocol* используется для определения соответствия IP-адреса адресу Ethernet. Протокол используется в локальных сетях. Отображение осуществляется только в момент отправления IP-пакетов, так как только в этот момент создаются заголовки IP и Ethernet. Отображение адресов осуществляется путем поиска в ARP-таблице.
- Упрощенно, ARP-таблица состоит из двух столбцов:

IP-адрес	Ethernet-адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54

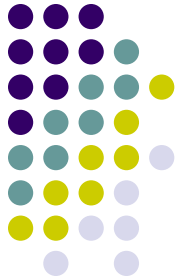
- В первом столбце содержится IP-адрес, а во втором Ethernet-адрес. Таблица соответствия необходима, так как адреса выбираются произвольно и нет какого-либо алгоритма для их вычисления. Если машина перемещается в другой сегмент сети, то ее ARP-таблица должна быть изменена.

Протокол ICMP



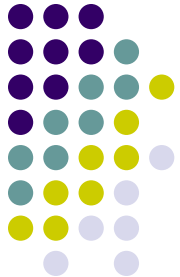
- Протокол ICMP (Internet Control Message Protocol) относят к межсетевому уровню. Протокол используется для рассылки информационных и управляющих сообщений. При этом используются следующие виды сообщений:
  - **Flow control** – если принимающая машина (шлюз или реальный получатель информации) не успевает перерабатывать информацию, то данное сообщение приостанавливает отправку пакетов по сети.
  - **Detecting unreachable destination** – если пакет не может достичь места назначения, то шлюз, который не может доставить пакет, сообщает об этом отправителю пакета. Информировать о невозможности доставки сообщения может и машина, чей IP-адрес указан в пакете. Только в этом случае речь будет идти о портах TCP и UDP, о чем будет сказано чуть позже.
  - **Redirect routing** – это сообщение посылается в том случае, если шлюз не может доставить пакет, но у него есть на этот счет некоторые соображения, а именно адрес другого шлюза.
  - **Checking remote host** – в этом случае используется так называемое ICMP Echo Message. Если необходимо проверить наличие стека TCP/IP на удаленной машине, то на нее посылается сообщение этого типа. Как только система получит это сообщение, она немедленно подтвердит его получение.

Протокол UDP



- Протокол **UDP** (**User Datagram Protocol)** – один из двух протоколов транспортного уровня, которые используются в стеке протоколов TCP/IP. UDP позволяет прикладной программе передавать свои сообщения по сети с минимальными издержками, связанными с преобразованием протоколов уровня приложения в протокол IP. Однако при этом, прикладная программа сама должна заботиться о подтверждении того, что сообщение доставлено по месту назначения.
- Порты в заголовке определяют протокол UDP как мультиплексор, который позволяет собирать сообщения от приложений и отправлять их на уровень протоколов. При этом приложение использует определенный порт. Взаимодействующие через сеть приложения могут использовать разные порты, что и отражает заголовок пакета. Всего можно определить 216 разных портов. Первые 256 портов закреплены за, так называемыми "well known services", к которым относятся, например, 53 порт UDP, который закреплен за сервисом DNS.
- Наиболее известными сервисами, основанными на UDP, является служба доменных имен BIND и распределенная файловая система NFS.

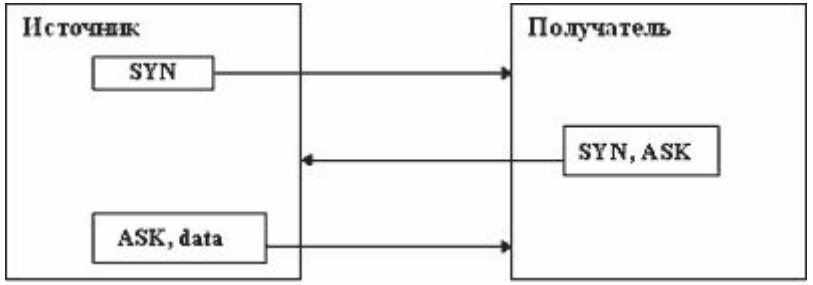
Протокол TCP



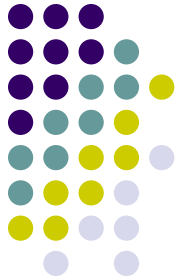
- Протокол TCP (**Transfer Control Protocol**) – “ориентированный на соединение сквозной надежный протокол” (согласно RFC).
  - **Надежность** TCP заключается в том, что источник данных повторяет их посылку, если только не получит в определенный промежуток времени от адресата подтверждение об их успешном получении. Этот механизм называется *Positive Asknowledgement with Retransmission (PAR)*. Как мы ранее определили, единица пересылки (пакет данных, сообщение и т.п.) в терминах TCP носит название сегмента. В заголовке TCP существует поле контррольной суммы. Если при пересылке данные повреждены, то по контрольной сумме модуль, вычленяющий TCP-сегменты из пакетов IP, может определить это. Поврежденный пакет уничтожается, а источнику ничего не посылается. Если данные не были повреждены, то они пропускаются на сборку сообщения приложения, а источнику отправляется подтверждение.

Протокол TCP

- Ориентация на соединение определяется тем, что прежде чем отправить сегмент с данными, модули TCP источника и получателя обмениваются управляющей информацией. Такой обмен называется **handshake** (буквально "рукопожатие"). В TCP используется трехфазный hand-shake:
  - Источник устанавливает соединение с получателем, посылая ему пакет с флагом "синхронизации последовательности номеров" (Synchronize Sequence Numbers - SYN). Номер в последовательности определяет номер пакета в сообщении приложения. Это не обязательно должен быть 0 или единица. Но все остальные номера будут использовать его в качестве базы, что позволит собрать пакеты в правильном порядке;
  - Получатель отвечает номером в поле подтверждения получения SYN, который соответствует установленному источником номеру. Кроме этого, в поле "номер в последовательности" может также сообщаться номер, который запрашивался источником;
  - Источник подтверждает, что принял сегмент получателя и отправляет первую порцию данных.

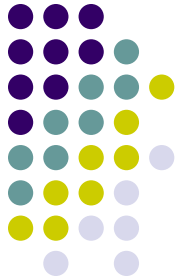


Windows Sockets



- Windows Sockets (Winsock) – стандарт позволяет разрабатывать прикладные программы, способные работать со стеком TCP/IP без необходимости учета каких-либо вариаций в реализациях стека TCP/IP.
- В операционной системе Windows 2000 поддерживается версия Winsock 2.0.
- Стандарт Winsock разработан для организации единообразного набора вызовов интерфейса прикладного программирования (API), которые не изменяются, несмотря на отличия реализаций TCP/IP.

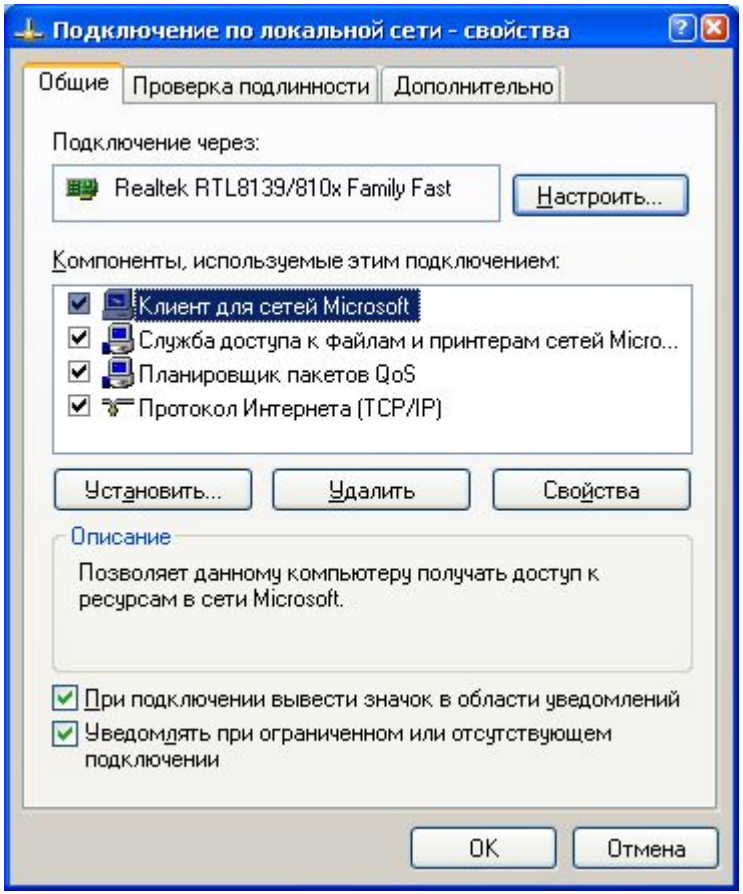
Разрешения имен



- **Система доменных имен** (DNS – Domain Name System) является стандартным методом отображения IP-адресов на имена.
- Пространство доменных имен представляет собой древовидную структуру всех доменов от корневого домена («.») и вплоть до отдельного хоста.
- До того как в сети Интернет была введена система DNS, все имена должны быть были прописана в управляющем файле hosts.txt.
- Корневые домены – первый уровень доменных имен. Они описывают тип организации (*.com, *.edu) или географическое расположение (*.ru, *.fr).
- Для преобразования доменных имен в IP-адреса организованы серверы доменных имен (серверы DNS).
- Для обмена информацией о соответствии имен доменов и IP-адресов используются специальные службы.

Настройка подключения по протоколу TCP/IP

- Настройка подключения компьютера под управлением Windows 2000 включает в себя:
  - Конфигурирование сетевых компонентов



Настройка подключения по протоколу TCP/IP

- Настройку параметров протокола TCP/IP
- Назначение IP-адресов серверам DNS и WINS (для их задания используется окно, вызываемое с помощью кнопки **Дополнительно**.