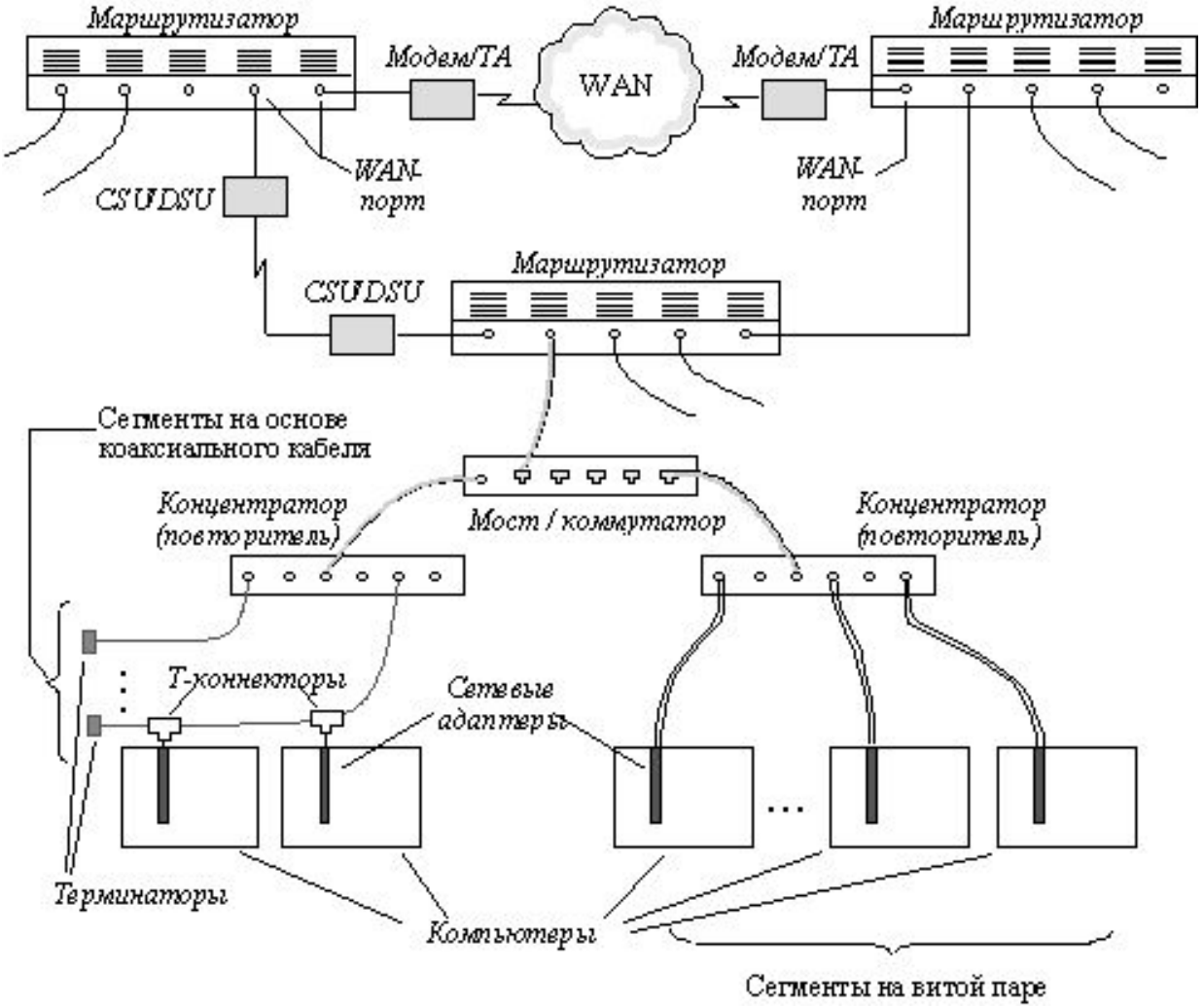
# Операционные системы

Лекция 4

**Компьютерные сети**

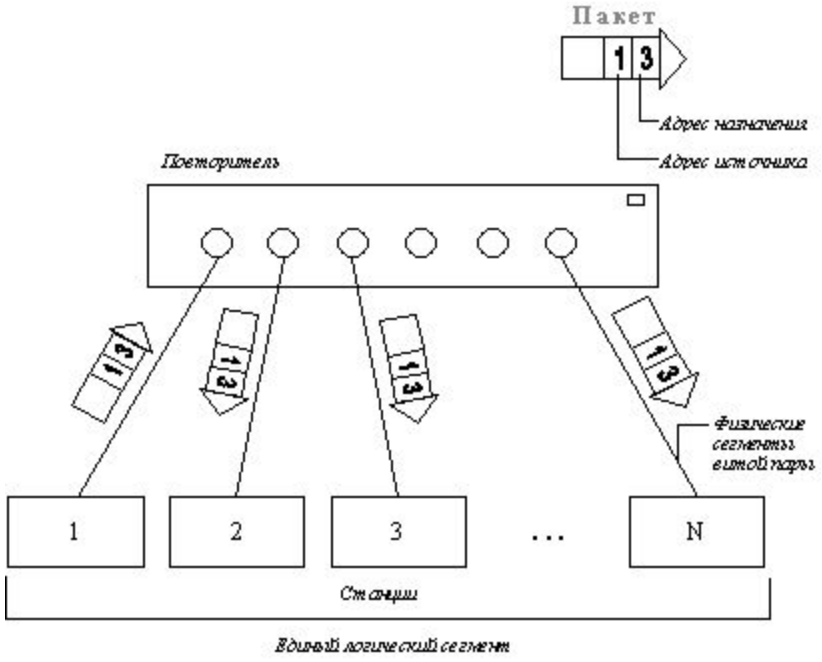
# Сетевое оборудование



# Сетевое оборудование

- Кабельная система
  - Коаксиальная шина (10 Мбит/с)
  - Витая пара + хаб (100/1000 Мбит/с)
  - Оптическая пара (2 Гбит/с)
- Оборудование: кабели и сетевые адаптеры
  - Оформление передаваемой информации в виде кадра определенного формата.
  - Получение доступа к среде передачи данных.
  - Кодирование последовательности бит кадра последовательностью электрических сигналов при передаче данных и декодирование при их приеме.
  - Преобразование информации из параллельной формы в последовательную и обратно.
  - Синхронизация битов, байтов и кадров.
- Телефонные линии
  - V34+ – 33.6 Кбит/с
  - V.90 – 56 Кбит/с | 33.6 Кбит/с
  - ADSL (Asymmetric Digital Subscriber Line) – 6.1 Мбит/с | 640 Кбит/с
  - Выделенные линии (2 Мбит/с)
- Оборудование: модемы и оборудование провайдеров на АТС
  - Линии ISDN (Integrated Services Digital Network) (1984 AT&T) 2 Мбит/с
  - Сети X.25 (с коммутацией пакетов)
  - Frame Relay
  - ATM (Asynchronous Transfer Mode

# Повторитель Ethernet

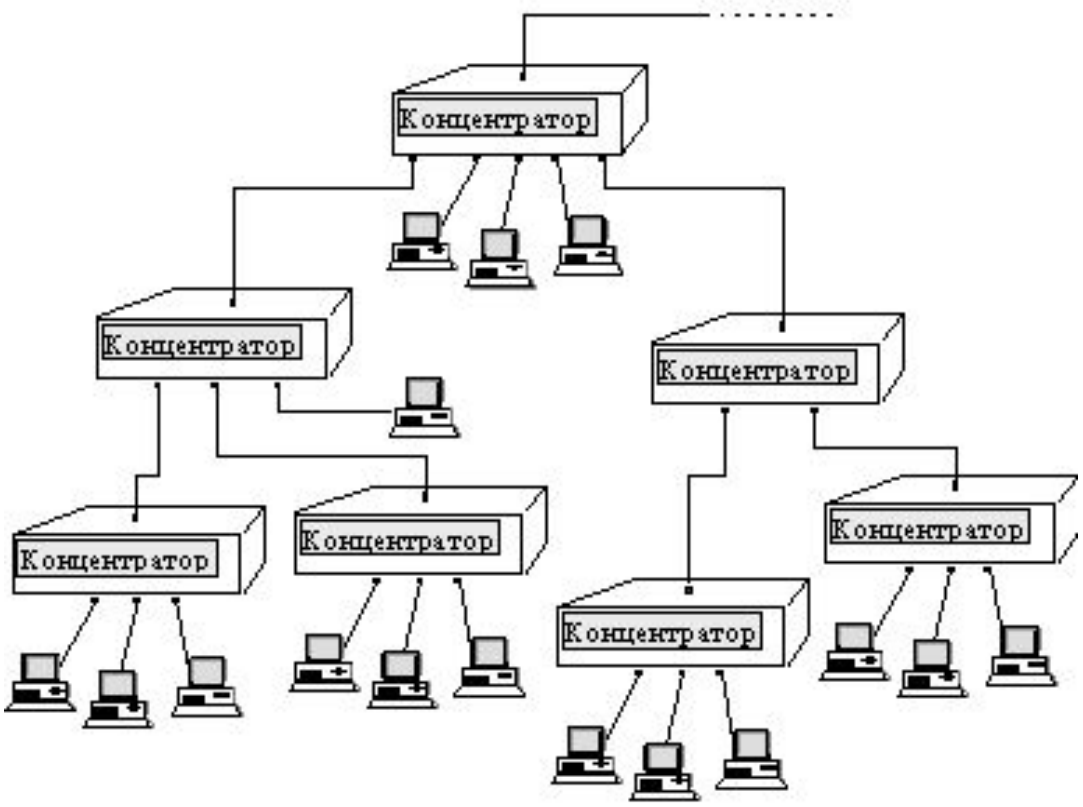



*Повторитель Ethernet синхронно повторяет биты кадра на всех своих портах*

Основная функция *повторителя* (repeater), как это следует из его названия – повторение сигналов, поступающих на один из его портов, на всех остальных портах (Ethernet) или на следующем в логическом кольце порте (Token Ring, FDDI) синхронно с сигналами-оригиналами. Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети станциями.

Многопортовый повторитель часто называют *концентратором* (hub, concentrator), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть. Практически во всех современных сетевых стандартах концентратор является необходимым элементом сети, соединяющим отдельные компьютеры в сеть.

# Логический сегмент, построенный с использованием концентраторов

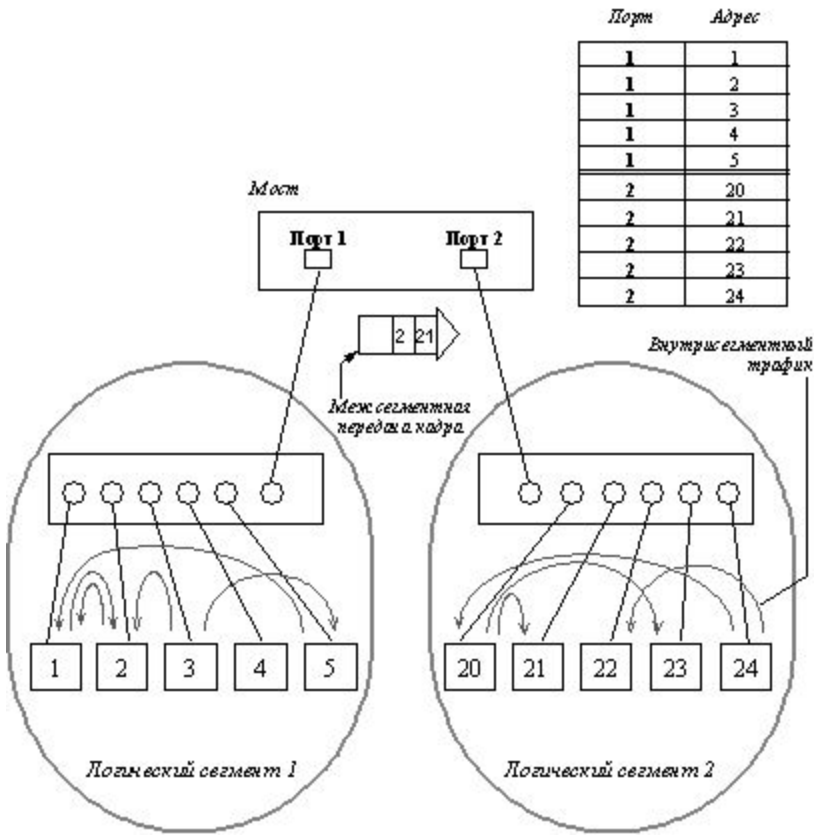



Мост (bridge), а также его быстродействующий функциональный аналог – коммутатор (switching hub), делит общую среду передачи данных на логические сегменты. Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких

# Физические и логические сегменты

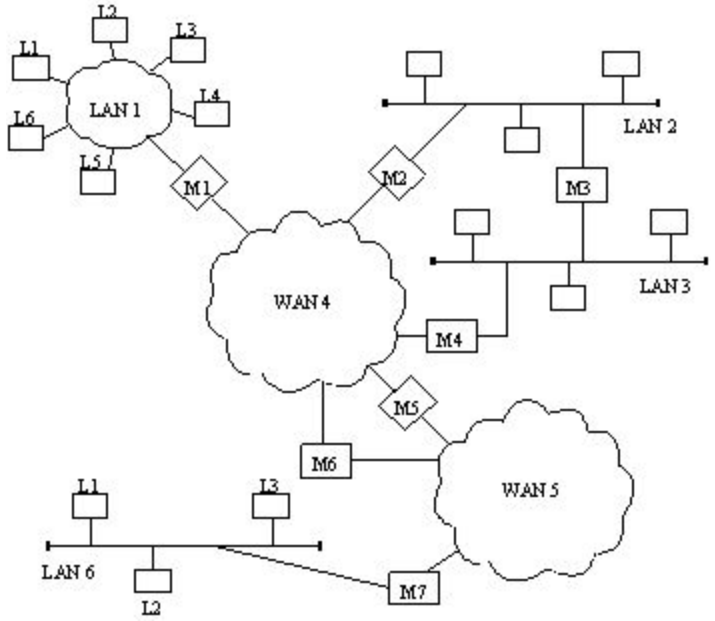
Отрезки кабеля, соединяющие два компьютера или какие либо два других сетевых устройства называются *физическими сегментам*. Таким образом, концентраторы и повторители, которые используются для добавления новых физических сегментов, являются средством физической структуризации сети.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – *логический сегмент* (рис. 1.8). Логический сегмент также называют доменом коллизий, поскольку при попытке одновременной передачи данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. Следует особо подчеркнуть, что какую бы сложную структуру не образовывали концентраторы, например, путем иерархического соединения, все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.



# Маршрутизаторы

*Маршрутизатор* (router) позволяет организовывать в сети избыточные связи, образующие петли. Он справляется с этой задачей за счет того, что принимает решение о передаче пакетов на основании более полной информации о графе связей в сети, чем мост или коммутатор. Маршрутизатор имеет в своем распоряжении базу топологической информации, которая говорит ему, например, о том, между какими подсетями общей сети имеются связи и в каком состоянии (работоспособном или нет) они находятся. Имея такую карту сети, маршрутизатор может выбрать один из нескольких возможных маршрутов доставки пакета адресату. В данном случае под маршрутом понимают последовательность прохождения пакетом маршрутизаторов. Например, для связи станций L2 сети LAN1 и L1 сети LAN6 имеется два маршрута: M1-M5-M7 и M1-M6-M7.

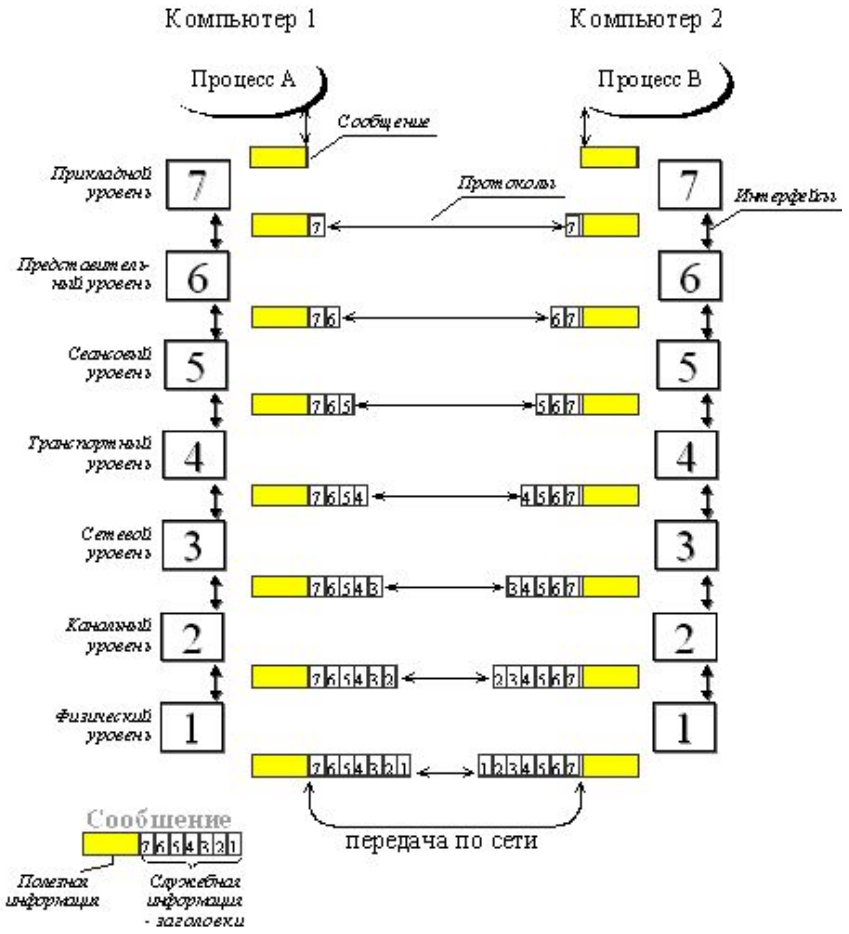


# Модель OSI

Международная Организация по Стандартам (International Standards Organization, ISO) разработала модель, которая четко определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какую работу должен делать каждый уровень. Эта модель называется моделью взаимодействия открытых систем (Open System Interconnection, OSI) или моделью ISO/OSI.

В модели OSI взаимодействие делится на семь уровней или слоев (рис. 1.1). Каждый уровень имеет дело с одним определенным аспектом взаимодействия. Таким образом, проблема взаимодействия декомпозирована на 7 частных проблем, каждая из которых может быть решена независимо от других. Каждый уровень поддерживает интерфейсы с выше- и нижележащими уровнями.

Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам. Следует иметь в виду, что приложение может взять на себя функции некоторых верхних уровней модели OSI, в таком случае, при необходимости межсетевого обмена оно обращается напрямую к системным средствам, выполняющим функции оставшихся нижних уровней модели OSI.

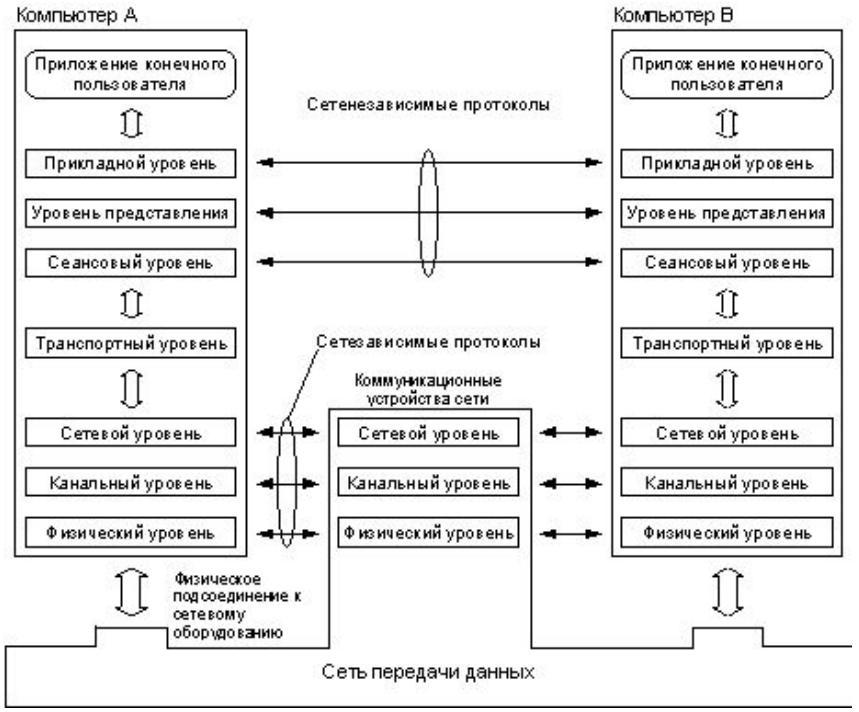


# Модель OSI

Три нижних уровня – физический, канальный и сетевой – являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети, с используемым коммуникационным оборудованием. Например, переход на оборудование FDDI означает полную смену протоколов физического и канального уровня во всех узлах сети.

Три верхних уровня – сеансовый, уровень представления и прикладной – ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют никакие изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Так, переход от Ethernet на высокоскоростную технологию ATM не потребует никаких изменений в программных средствах, реализующих функции прикладного, представительного и сеансового уровней.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних уровней. Это позволяет разрабатывать приложения, независящие от технических средств, непосредственно занимающихся транспортировкой сообщений.



# Стек TCP/IP

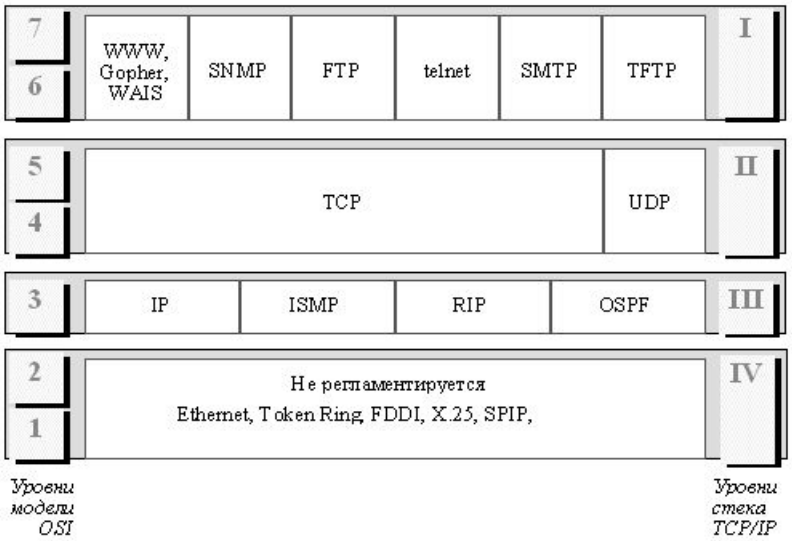
Стек TCP/IP, называемый также стеком DoD и стеком Internet, является одним из наиболее популярных и перспективных стеков коммуникационных протоколов. Если в настоящее время он распространен в основном в сетях с ОС UNIX, то реализация его в последних версиях сетевых операционных систем для персональных компьютеров (Windows NT, NetWare ) является хорошей предпосылкой для быстрого роста числа установок стека TCP/IP.

Стек был разработан по инициативе Министерства обороны США (Department of Defence, DoD) более 20 лет назад для связи экспериментальной сети ARPAnet с другими сателлитными сетями как набор общих протоколов для разнородной вычислительной среды. Сеть ARPA поддерживала разработчиков и исследователей в военных областях. В сети ARPA 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.

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.

# Стек TCP/IP




```
C:\WINNT>arp -a
Интерфейс: 192.168.0.1 on Interface 0x2
  Адрес IP         Физический адрес      Тип
  192.168.0.2      00-e0-4c-39-1a-1e     динамический
  192.168.0.3      00-e0-4c-39-33-a2     динамический
  192.168.0.4      00-e0-4c-39-1a-2d     динамический
```

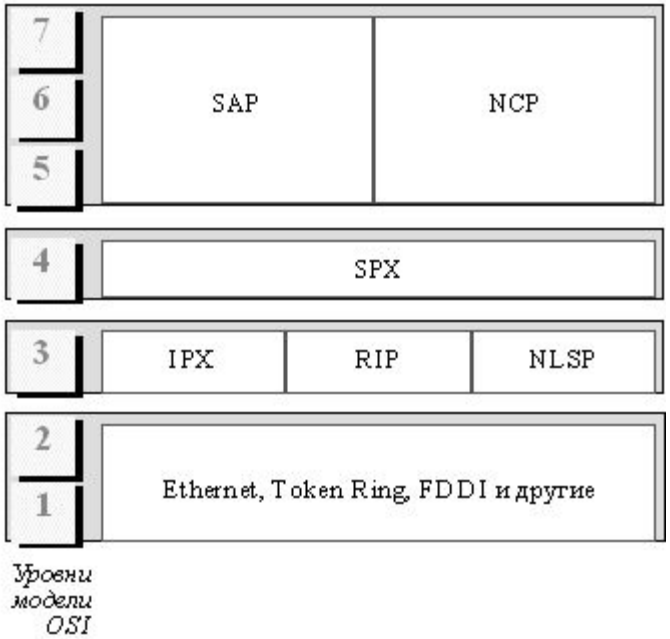
Самый нижний (***уровень IV***) - уровень межсетевых интерфейсов - соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных каналов это Ethernet, Token Ring, FDDI, для глобальных каналов - собственные протоколы работы на аналоговых коммутируемых и выделенных линиях SLIP/PPP, которые устанавливают соединения типа "точка - точка" через последовательные каналы глобальных сетей.

Следующий уровень (***уровень III***) - это уровень межсетевого взаимодействия, который занимается передачей дейтаграмм с использованием различных локальных сетей, территориальных сетей X.25, 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.

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 устойчивое виртуальное соединение между удаленными прикладными процессами. Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным методом, то есть без установления виртуального соединения, и поэтому требует меньших накладных расходов, чем TCP.

Верхний уровень (**уровень I**) называется прикладным. К нему 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.

# Стек IPX/SPX




Этот стек является оригинальным стеком протоколов фирмы Novell, который она разработала для своей сетевой операционной системы NetWare еще в начале 80-х годов. Протоколы Internetwork Packet Exchange (IPX) и Sequenced Packet Exchange (SPX), которые дали имя стеку, являются прямой адаптацией протоколов XNS фирмы Xerox, распространенных в гораздо меньше степени, чем IPX/SPX.

На ***физическом и канальном уровнях*** в сетях Novell используются все популярные протоколы этих уровней (Ethernet, Token Ring, FDDI и другие).

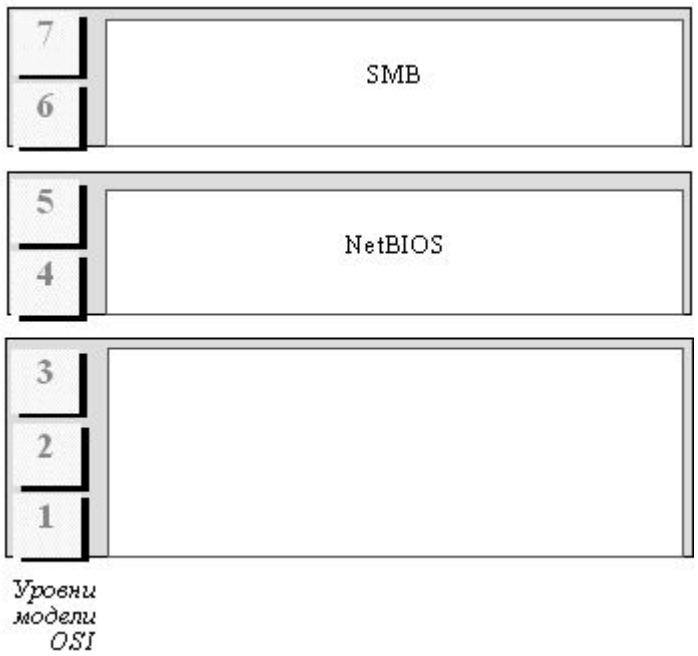
На ***сетевом уровне*** в стеке Novell работает протокол **IPX**, а также протоколы обмена маршрутной информацией **RIP** и **NLSP** (аналог протокола OSPF стека TCP/IP). IPX является протоколом, который занимается вопросами адресации и маршрутизации пакетов в сетях Novell. Протокол IPX поддерживает только дейтаграммный способ обмена сообщениями, за счет чего экономно потребляет вычислительные ресурсы. Итак, протокол IPX обеспечивает выполнение трех функций: задание адреса, установление маршрута и рассылку дейтаграмм.

**Транспортному уровню** модели OSI в стеке Novell соответствует протокол SPX, который осуществляет передачу сообщений с установлением соединений.

На верхних **прикладном, представительном и сеансовом уровнях** работают протоколы NCP и SAP. Протокол **NCP** (NetWare Core Protocol) является протоколом взаимодействия сервера NetWare и оболочки рабочей станции. Этот протокол прикладного уровня реализует архитектуру клиент-сервер на верхних уровнях модели OSI. С помощью функций этого протокола рабочая станция производит подключение к серверу, отображает каталоги сервера на локальные буквы дисководов, просматривает файловую систему сервера, копирует удаленные файлы, изменяет их атрибуты и т.п., а также осуществляет разделение сетевого принтера между рабочими станциями.

**SAP** (Service Advertising Protocol) - протокол объявления о сервисе - концептуально подобен протоколу RIP. Подобно тому, как протокол RIP позволяет маршрутизаторам обмениваться маршрутной информацией, протокол SAP дает возможность сетевым устройствам обмениваться информацией об имеющихся сетевых сервисах.

# Стек NetBIOS/SMB




Фирмы Microsoft и IBM совместно работали над сетевыми средствами для персональных компьютеров, поэтому стек протоколов NetBIOS/SMB является их совместным детищем. Средства NetBIOS появились в 1984 году как сетевое расширение стандартных функций базовой системы ввода/вывода (BIOS) IBM PC для сетевой программы PC Network фирмы IBM, которая на прикладном уровне использовала для реализации сетевых сервисов протокол SMB (Server Message Block).

Протокол **NetBIOS** работает на трех уровнях модели взаимодействия открытых систем: **сетевом, транспортном и сеансовом**. NetBIOS может обеспечить сервис более высокого уровня, чем протоколы IPX и SPX, однако не обладает способностью к маршрутизации. Таким образом, NetBIOS не является сетевым протоколом в строгом смысле этого слова. NetBIOS содержит много полезных сетевых функций, которые можно отнести к сетевому, транспортному и сеансовому уровням, однако с его помощью невозможна маршрутизация пакетов, так как в протоколе обмена кадрами NetBIOS не вводится такое понятие как сеть. Это ограничивает применение протокола NetBIOS локальными сетями, не разделенными на подсети. NetBIOS поддерживает как дейтаграммный обмен, так и обмен с установлением соединений.

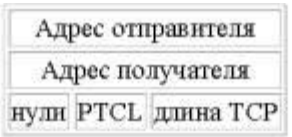
Протокол **SMB**, соответствующий прикладному и представительному уровням модели OSI, регламентирует взаимодействие рабочей станции с сервером.

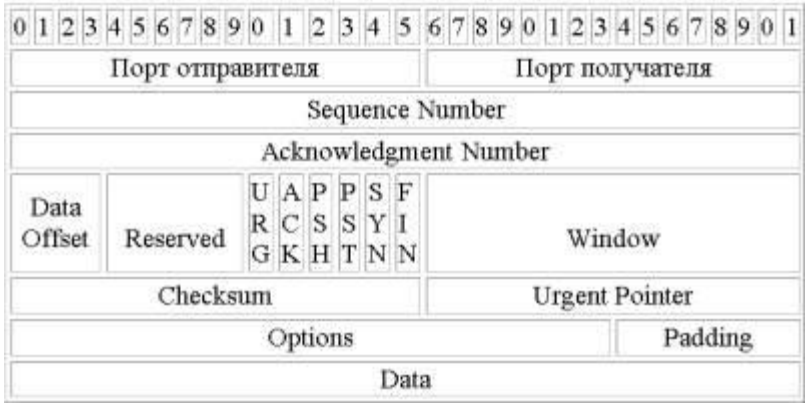
# Классы подсетей TCP/IP

| Класс | Маска | Диапазон первого октета | Доступных подсетей | Доступных адресов в подсети |
|---|---|---|---|---|
| A | 0* | 1-126 | 126 | 16 777 214 |
| B | 10*.* | 128-191 | 16 384 | 65 534 |
| C | 110*.*.* | 192-223 | 2 097 152 | 254 |

127.*.*.* – шлейфовый адрес
192.168.*.* – локальные адреса
*.*.*.255 – широковещательные адреса

# Маршрутизируемый протокол IP

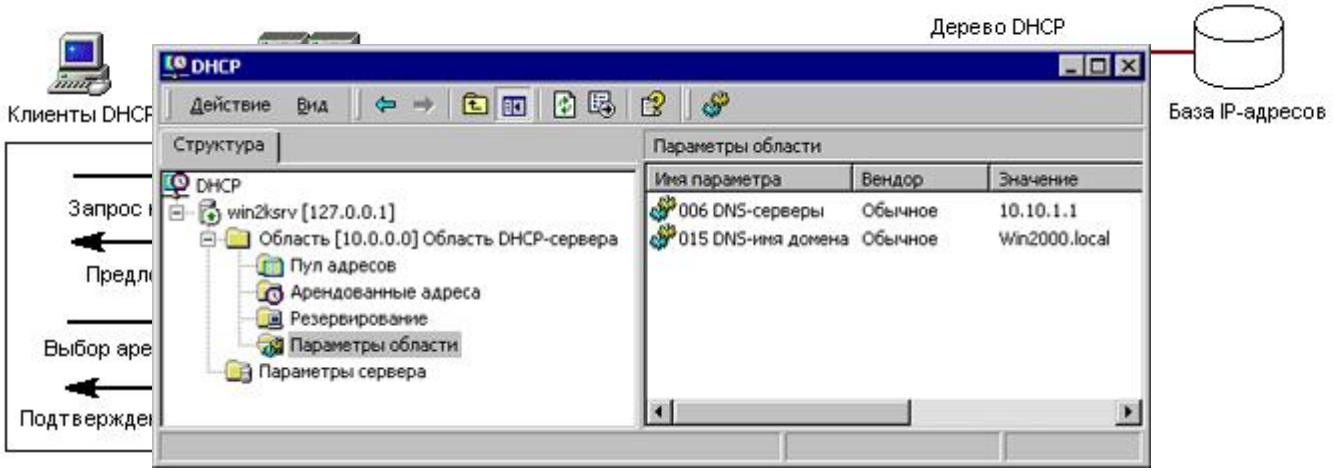
# Структура TCP-пакета

| Поле | Описание |
|---|---|
| Source port(порт отправителя) | Порт TCP узла отправителя |
| Destination port(порт получателя) | Порт TCP узла получателя |
| Sequence Number(порядковый номер) | Номер последовательности пакетов |
| Acknowledgement Number(Номер подтверждения) | Порядковый номер байта, который локальный узел рассчитывает получить следующим |
| Data Length(длинна данных) | Длинна TCP-пакета |
| Reserved(зарезервировано) | Зарезервировано для будущего использования |
| Flags(Флаги) | Описание содержимого сегмента |
| Window(окно) | Показывает доступное место в окне протокола TCP |
| Checksum(контрольная сумма) | Значение для проверки целостности пакета |
| Urgent Point(Указатель срочности) | При отправке срочных данных в этом поле задается гранича области срочных данных |

# Назначение портов

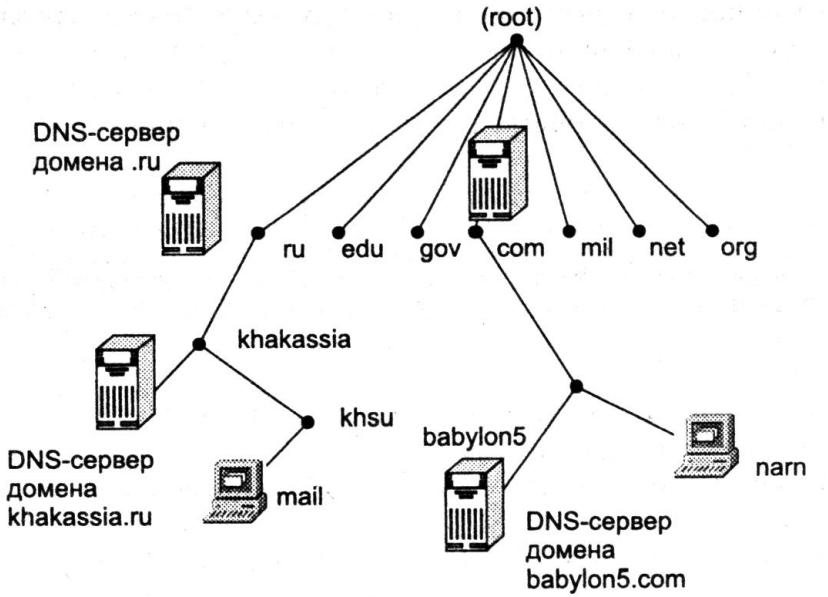
| Keyword | Decimal | Description |
|---|---|---|
| | 0/tcp | Reserved |
| | 0/udp | Reserved |
| tcpmux | 1/tcp | TCP Port Service Multiplexer |
| tcpmux | 1/udp | TCP Port Service Multiplexer |
| daytime | 13/tcp | Daytime (RFC 867) |
| daytime | 13/udp | Daytime (RFC 867) |
| ftp-data | 20/tcp | File Transfer [Default Data] |
| ftp-data | 20/udp | File Transfer [Default Data] |
| ftp | 21/tcp | File Transfer [Control] |
| ftp | 21/udp | File Transfer [Control] |
| ssh | 22/tcp | SSH Remote Login Protocol |
| ssh | 22/udp | SSH Remote Login Protocol |
| telnet | 23/tcp | Telnet |
| telnet | 23/udp | Telnet |
| smtp | 25/tcp | Simple Mail Transfer |
| time | 37/tcp | Time |
| name | 42/tcp | Host Name Server |
| nameserver | 42/tcp | Host Name Server |
| nicname | 43/tcp | Who Is |
| domain | 53/tcp | Domain Name Server |
| whois++ | 63/tcp | whois++ |
| bootps | 67/tcp | Bootstrap Protocol Server |
| bootps | 67/udp | Bootstrap Protocol Server |
| http | 80/tcp | World Wide Web HTTP |
| http | 80/udp | World Wide Web HTTP |
| pop3 | 110/tcp | Post Office Protocol - Version 3 |
| pop3 | 110/udp | Post Office Protocol - Version 3 |

# DHCP




Протокол упрощает работу сетевого администратора, который должен вручную конфигурировать только один сервер DHCP. Когда новый компьютер подключается к сети, обслуживаемой сервером DHCP, он запрашивает уникальный IP-адрес, а сервер DHCP назначает его из пула доступных адресов. Этот процесс состоит из четырех шагов: клиент DHCP запрашивает IP-адрес (DHCP Discover, обнаружение), DHCP-сервер предлагает адрес (DHCP Offer, предложение), клиент принимает предложение и запрашивает адрес (DHCP Request, запрос) и адрес официально назначается сервером (DHCP Acknowledgement, подтверждение). Чтобы адрес не "простаивал", сервер DHCP предоставляет его на определенный администратором срок, это называется *арендным договором* (lease). По истечении половины срока арендного договора клиент DHCP запрашивает его возобновление, и сервер DHCP продлевает арендный договор. Это означает, что когда машина прекращает использовать назначенный IP-адрес (например, в результате перемещения в другой сетевой сегмент), арендный договор истекает, и адрес возвращается в пул для повторного использования.

# DNS

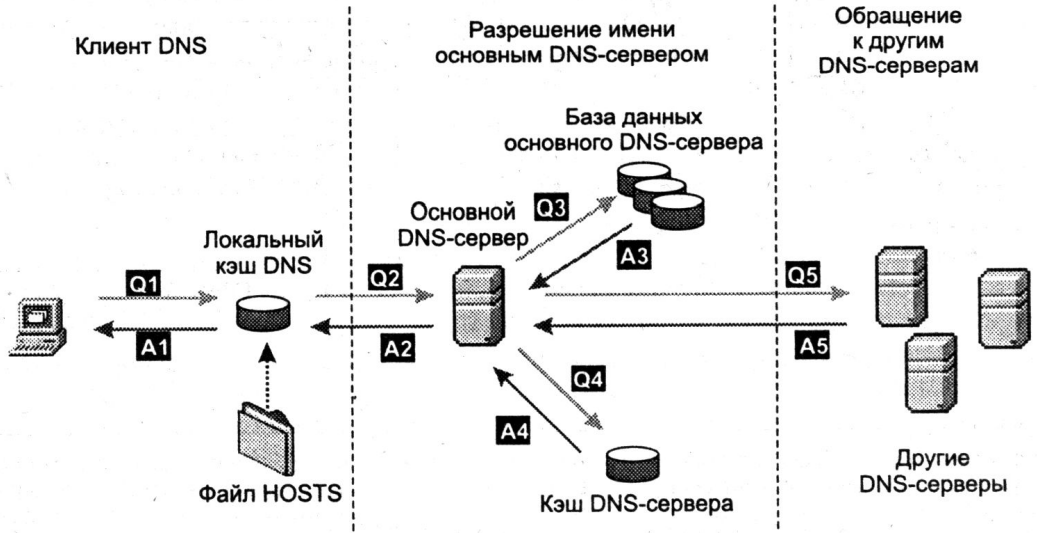


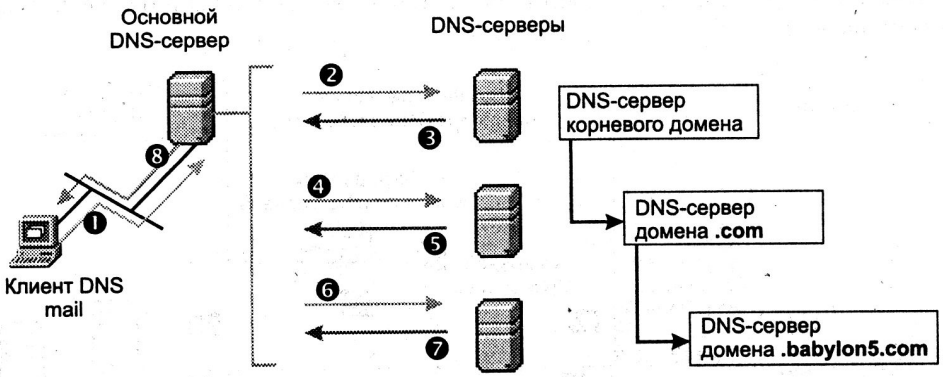

Домен DNS основан на концепции дерева именованных доменов. Каждый уровень дерева может представлять или ветвь, или лист дерева. Ветвь — это уровень, содержащий более одного имени и идентифицирующий набор именованных ресурсов. Лист — имя, указывающее заданный ресурс.

# Типы доменных имен

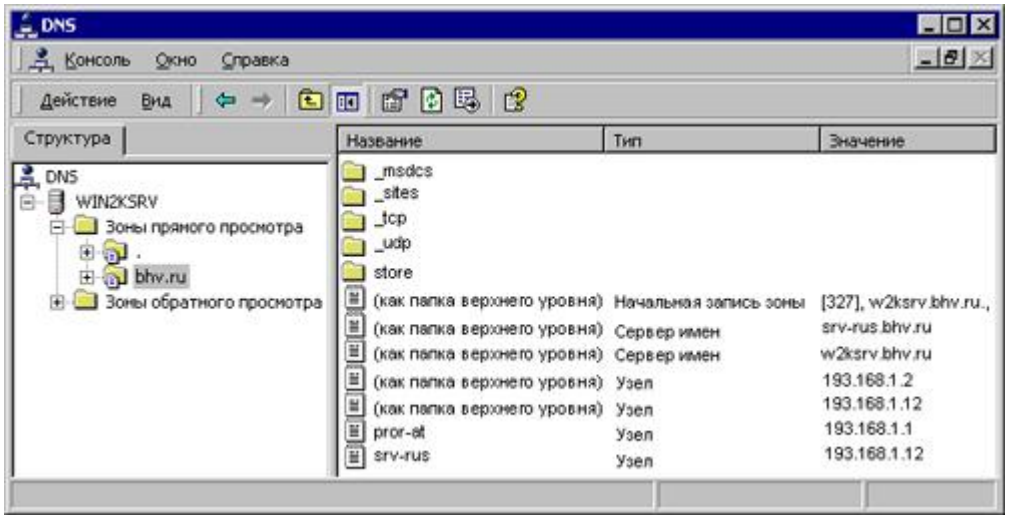
| Тип имени | Описание | Пример |
|---|---|---|
| Корневой домен | Корень дерева именованных доменов, задает неименованный уровень; часто указывается в виде двойных пустых кавычек (" "). При использовании в доменном имени указывается точкой в конце имени. Определяет, что имя расположено в корневом, самом высоком, уровне доменной иерархии | Точка (.) или точка, стоящая в конце имени, например, "sample.mydomain.org." |
| Домен верхнего уровня | Имя, состоящее из двух или трех символов, обычно указывающее страну (Россия — ш, Нидерланды — nl, Украина — ua и т. п.) или тип организации, использующей имя (com — коммерческая, mil — военная, США и т. д.) | ".com" означает, что имя зарегистрировано фирмой или другой организацией для коммерческого использования в Интернете |
| Домен второго уровня | Имя переменной длины, зарегистрированное частным лицом или организацией для использования в Интернете. Такие имена всегда основаны на домене верхнего уровня, в зависимости от типа организации или географического местоположения | "mydomain.org" — имя домена второго уровня (вымышленное) |
| Субдомен | Дополнительные имена, которые организация может создавать в пределах домена второго уровня. Применяются для указания различных организационных единиц или территориальных подразделений больших организаций | "sample.mydomain.org." — субдомен домена второго уровня "mydomain.org." |
| Имя хоста или ресурса | Листья дерева имен DNS, задают определенный ресурс или хост | "host.sampte.mydbmain.org.", где host— имя хоста или какого-либо ресурса в сети |

# Разрешение доменных имен



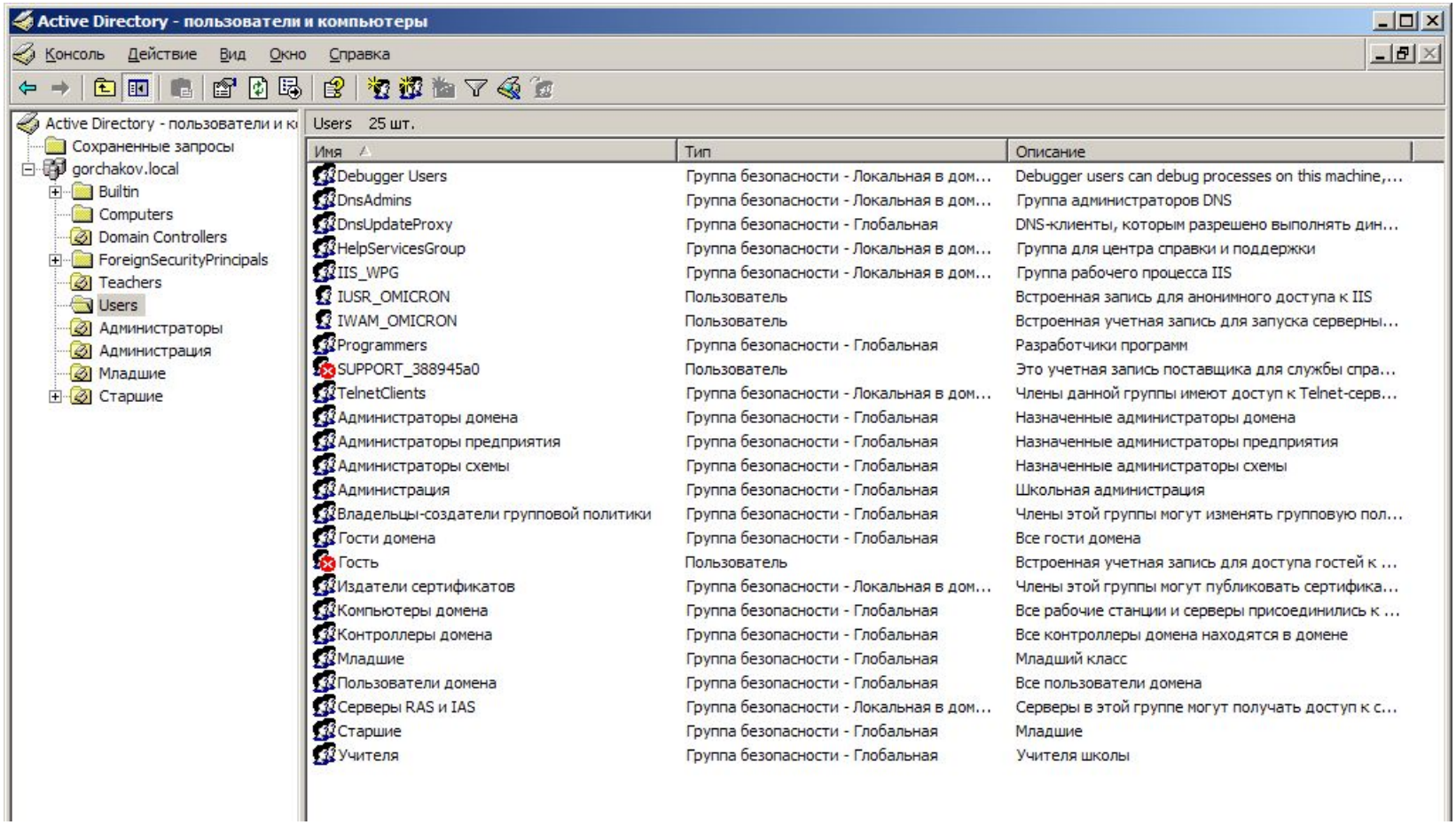



# DNS-сервер в Windows




- DNS-сервер, соответствующий стандартам RFC. Служба DNS поддерживает открытый протокол и соответствует промышленным стандартам (RFC).
- Способность взаимодействовать с другими реализациями серверов DNS. Поскольку служба DNS соответствует стандартам DNS и "понимает" форматы стандартных файлов данных DNS и форматы ресурсных записей, она успешно работает совместно с большинством других реализаций DNS, например, использующих программное обеспечение Berkeley Internet Name Domain (BIND).
- Поддержка Active Directory. Служба DNS обязательна для работы Active Directory. При установке Active Directory на компьютере под управлением Windows 2000 Server операционная система автоматически (но с согласия пользователя) устанавливает и конфигурирует службу DNS для поддержки Active Directory.
- Интеграция с другими сетевыми службами Microsoft. Служба DNS обеспечивает интеграцию с другими службами Windows 2000 и содержит функции, не описанные в RFC. Это касается интеграции со службами WINS и DHCP.
- Улучшенные административные инструменты. Windows 2000 предоставляет оснастку с улучшенным графическим интерфейсом пользователя для управления службой DNS. Windows 2000 Server содержит несколько новых мастеров конфигурации для выполнения повседневных задач по администрированию сервера. Также имеется ряд дополнительных средств, помогающих управлять и поддерживать серверы DNS и клиентов в сети.
- Поддержка протокола динамического обновления в соответствии с RFC. Служба DNS позволяет клиентам динамически обновлять ресурсные записи при помощи динамического протокола обновления DNS (стандарт RFC 2136). Это облегчает администрирование DNS, избавляя от необходимости вносить эти записи вручную. Компьютеры под управлением Windows 2000 могут динамически регистрировать свои имена DNS и IP-адреса.
- а Поддержка инкрементных зональных передач между серверами. Зональные передачи используются между серверами DNS для частичного копирования информации. Инкрементная зональная передача используется, чтобы копировать только измененные части зоны. Зона — набор записей, относящихся к одному домену.
- Поддержка новых типов ресурсных записей. Служба DNS включает поддержку нескольких новых типов ресурсных записей (RR): записи SRV (расположение службы) и ATMA (адрес ATM), что значительно расширяет возможности использования DNS в глобальных сетях.

# Службы каталогов Active Directory




По своей сути, служба каталогов — это средство для именования, хранения и выборки информации в некоторой распределенной среде, доступное для приложений, пользователей и различных клиентов этой среды. Можно вспомнить знакомый многим системный реестр Windows и базу данных Диспетчера безопасности учетных записей (SAM) Windows NT. Служба сетевых каталогов хранит информацию об общедоступных приложениях, файлах, принтерах и сведения о пользователях.

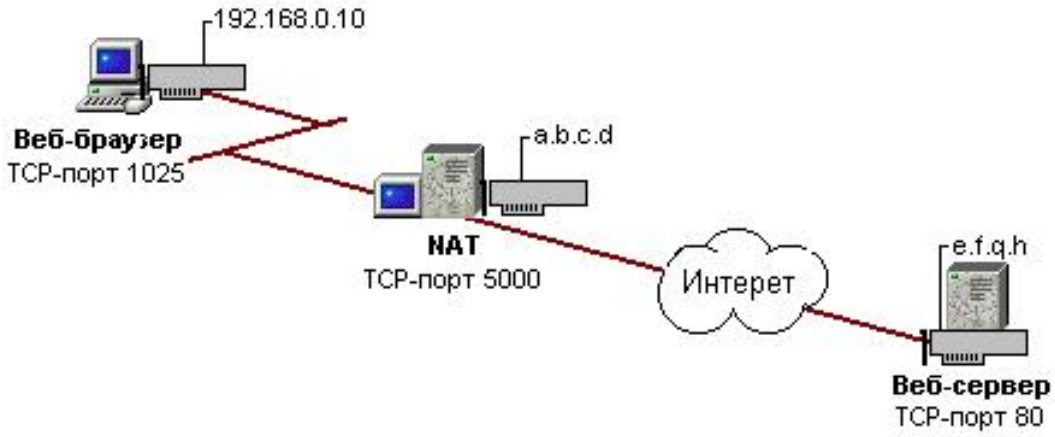
# Служба каталогов Active Directory обеспечивает эффективную работу сложной корпоративной среды, предоставляя следующие возможности:

- **Единая регистрация в сети**; Пользователи могут регистрироваться в сети с одним именем и паролем и получать при этом доступ ко всем сетевым ресурсам (серверам, принтерам, приложениям, файлам и т. д.) независимо от их расположения в сети.
- **Безопасность информации**. Средства аутентификации и управления доступом к ресурсам, встроенные в службу Active Directory, обеспечивают централизованную защиту сети. Права доступа можно определять не только для каждого объекта каталога, но и каждого свойства (атрибута) объекта.
- **Централизованное управление.** Администраторы могут централизованно управлять всеми корпоративными ресурсами. Рутинные задачи администрирования не нужно повторять для многочисленных объектов сети.
- **Администрирование с использованием групповых политик.** При загрузке компьютера или регистрации пользователя в системе выполняются требования групповых политик; их настройки хранятся в объектах групповых политик (GPO) и "привязываются" к сайтам, доменам или организационным единицам. Групповые политики определяют, например, права доступа к различным объектам каталога или ресурсам, а также множество других "правил" работы в системе.
- **Гибкость изменений.** Служба каталогов гибко следует за изменениями структуры компании или организации. При этом реорганизация каталога не усложняется, а может и упроститься. Кроме того, службу каталога можно связать с Интернетом для взаимодействия с деловыми партнерами и поддержки электронной коммерции.
- **Интеграция с DNS.** Служба Active Directory тесно связана с DNS. Этим достигается единство в именовании ресурсов локальной сети и сети Интернет, в результате чего упрощается подключение пользовательской сети к Интернету.
- **Расширяемость каталога.** Администраторы могут добавлять в схему каталога новые классы объектов или добавлять новые атрибуты к существующим классам.
- **Масштабируемость.** Служба Active Directory может охватывать как один домен, так и множество доменов, один контроллер домена или множество контроллеров домена — т. е. она отвечает требованиям сетей любого масштаба. Несколько доменов можно объединить в дерево доменов, а несколько деревьев доменов можно связать в лес.
- **Репликация информации.** В службе Active Directory используется репликация служебной информации в схеме со многими ведущими (multi-master), что позволяет модифицировать каталог на любом контроллере домена. Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость и возможность распределения сетевой нагрузки.
- **Гибкость запросов к каталогу.** Пользователи и администраторы сети могут быстро находить объекты в сети, используя свойства объекта (например, имя пользователя или адрес его электронной почты, тип принтера или его местоположение и т. п.). Это, в частности, можно сделать при помощи команды Пуск | Поиск (Start | Search), папку Мое сетевое окружение (My Network Places) или оснастку Active Directory - пользователи и компьютеры (Active Directory Users and Computers). Оптимальность процедуры поиска достигается благодаря использованию глобального каталога.
- **Стандартные интерфейсы**. Для разработчиков приложений служба каталогов предоставляют доступ ко всем возможностям (средствам) каталога и поддерживают принятые стандарты и интерфейсы программирования (API). Служба каталогов тесно связана с операционной системой что позволяет избежать дублирования в прикладных программах функциональных возможностей системы, например, средств безопасности.

# Частные и публичные адреса

- Чтобы устанавливать соединение с ресурсами Интернета, необходимо использовать адреса, распределенные центром Network Information Center (Информационный центр сети Интернет, InterNIC). Такие адреса могут получать трафик от служб межсетевой сети и называются *public-адресами* (public address). Типичное малое предприятие или офис подразделения получает public-адрес (или адреса) от Интернет-провайдера, который, в свою очередь, получил диапазон public-адресов от InterNIC.
- Для того чтобы разрешить нескольким компьютерам в сети малого офиса или в домашней сети устанавливать соединение с ресурсами Интернета, *каждый* компьютер должен иметь собственный public-адрес. Это требование может привести к нехватке доступных public-адресов.
- Чтобы сократить потребность в public-адресах, InterNIC предусмотрел схему многократного использования адресов, зарезервировав идентификаторы сетей для частных нужд. Частные сети входят в следующие диапазоны (задаются идентификатором и маской):
  - 10.0.0.0 с маской 255.0.0.0
  - 172.16.0.0 с маской 255.240.0.0
  - 192.168.0.0 с маской 255.255.0.0

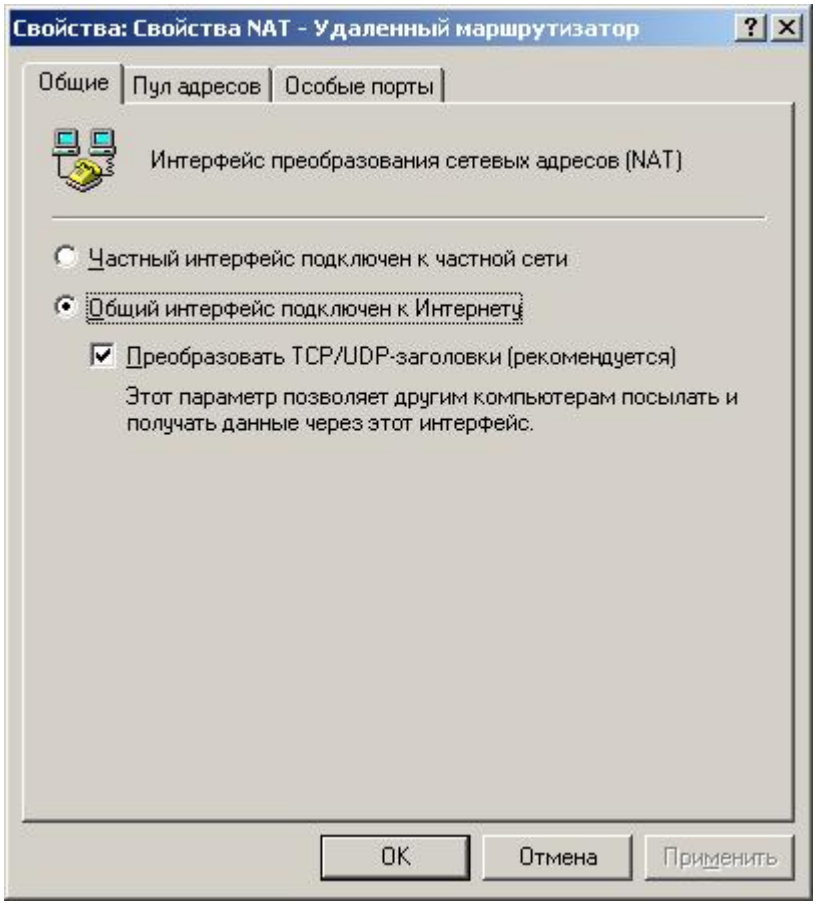
# NAT-служба




Частные адреса не могут получать трафик от компьютеров в межсетевой среде. Следовательно, если интрасеть использует частные адреса и устанавливает связь со службами Интернета, частный адрес должен транслироваться в public-адрес. NAT помещается между интрасетью, которая использует частные адреса, и Интернетом, который использует public-адреса. Пакеты, исходящие из интрасети, имеют частные адреса, которые NAT транслирует в public-адреса. Поступающие из Интернета пакеты имеют public-адреса, и NAT транслирует их в частные адреса.

Если сеть малого предприятия использует идентификатор сети 192.168.0.0 для интрасети и имеется public-адрес a.b.c.d, полученный от Интернет-провайдера, то NAT отображает все частные адреса в сети 192.168.0.0 в IP-адрес a.b.c.d. Если несколько частных адресов отображаются в один public-адрес с использованием NAT, TCP- и UDP-порты выбираются динамически, чтобы отличить один компьютер внутри интрасети от другого.

# NAT-служба




Если частный пользователь на компьютере с адресом 192.168.0.10 соединяется с веб-сервером по адресу e.f.g.h при помощи веб-браузера, то стек IP пользователя создает IP-пакет со следующей информацией:

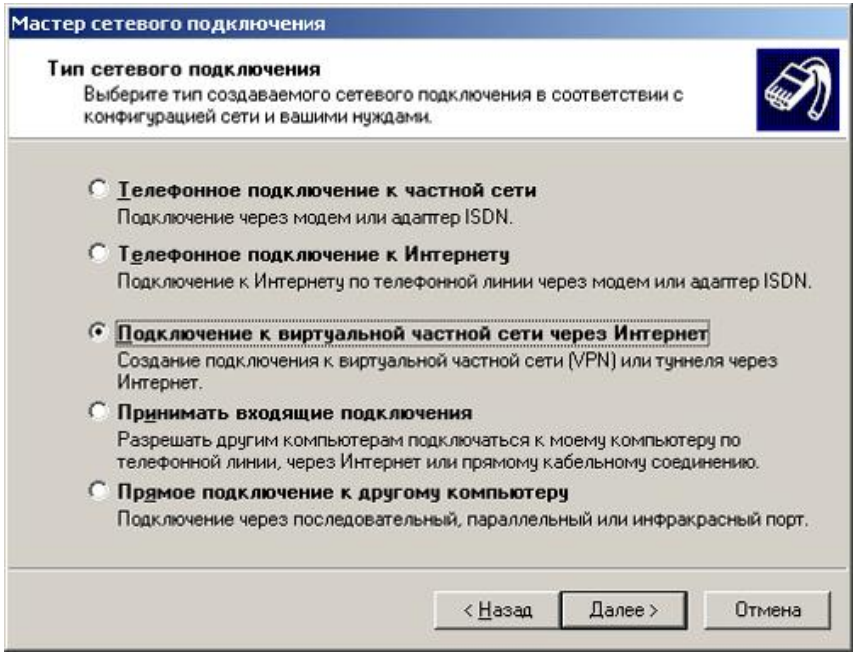
- IP-адрес получателя: e.f.g.h
- IP-адрес отправителя: 192.168.0.10
- Порт получателя: TCP-порт 80
- Порт отправителя: TCP-порт 1025

Этот IP-пакет затем пересылается NAT для преобразования адресов исходящего пакета к следующим:

- IP-адрес получателя: e.f.g.h
- IP-адрес отправителя: a.b.c.d
- Порт получателя: TCP-порт 80
- Порт отправителя: TCP-порт 5000

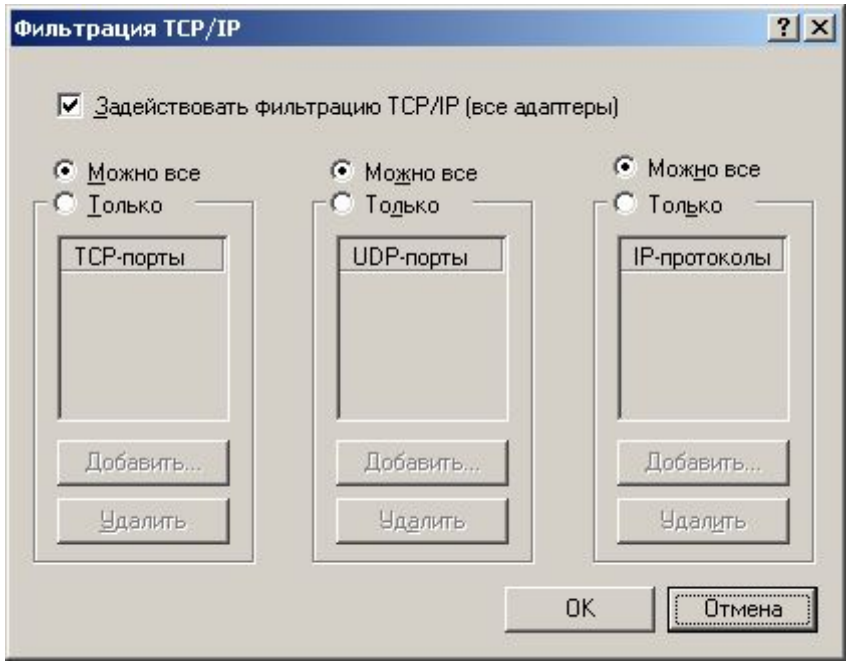
NAT хранит отображение {192.168.0.10, TCP 1025} в {a.b.c:d, TCP 5000} в своей внутренней таблице.

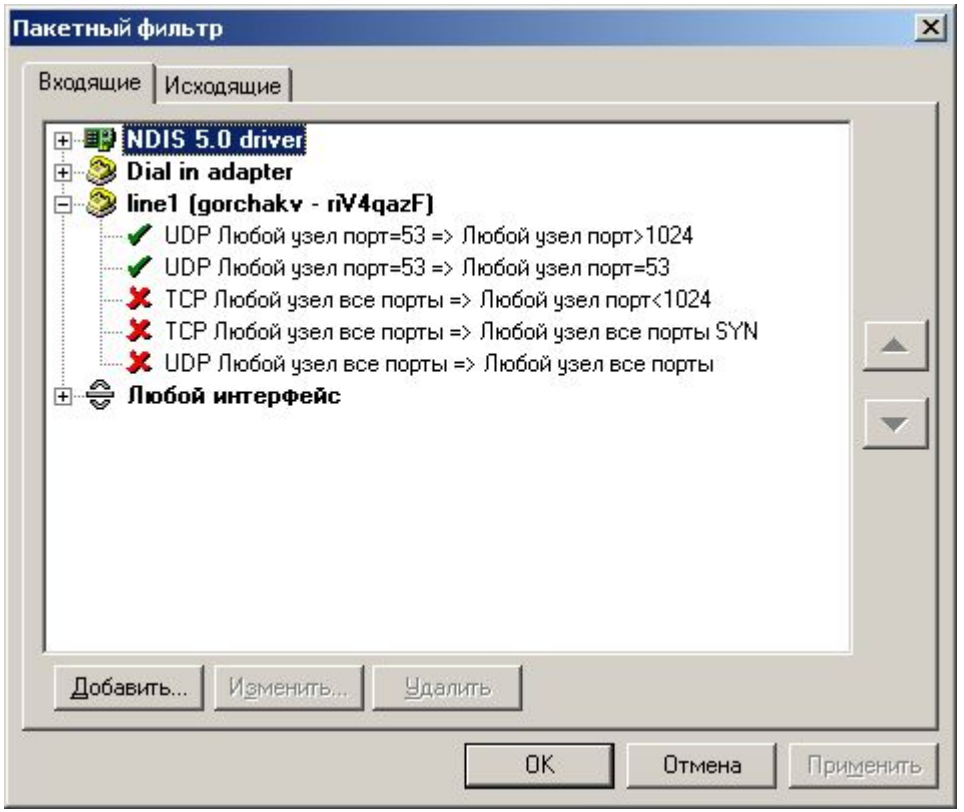
# Виртуальные частные сети (VPN)

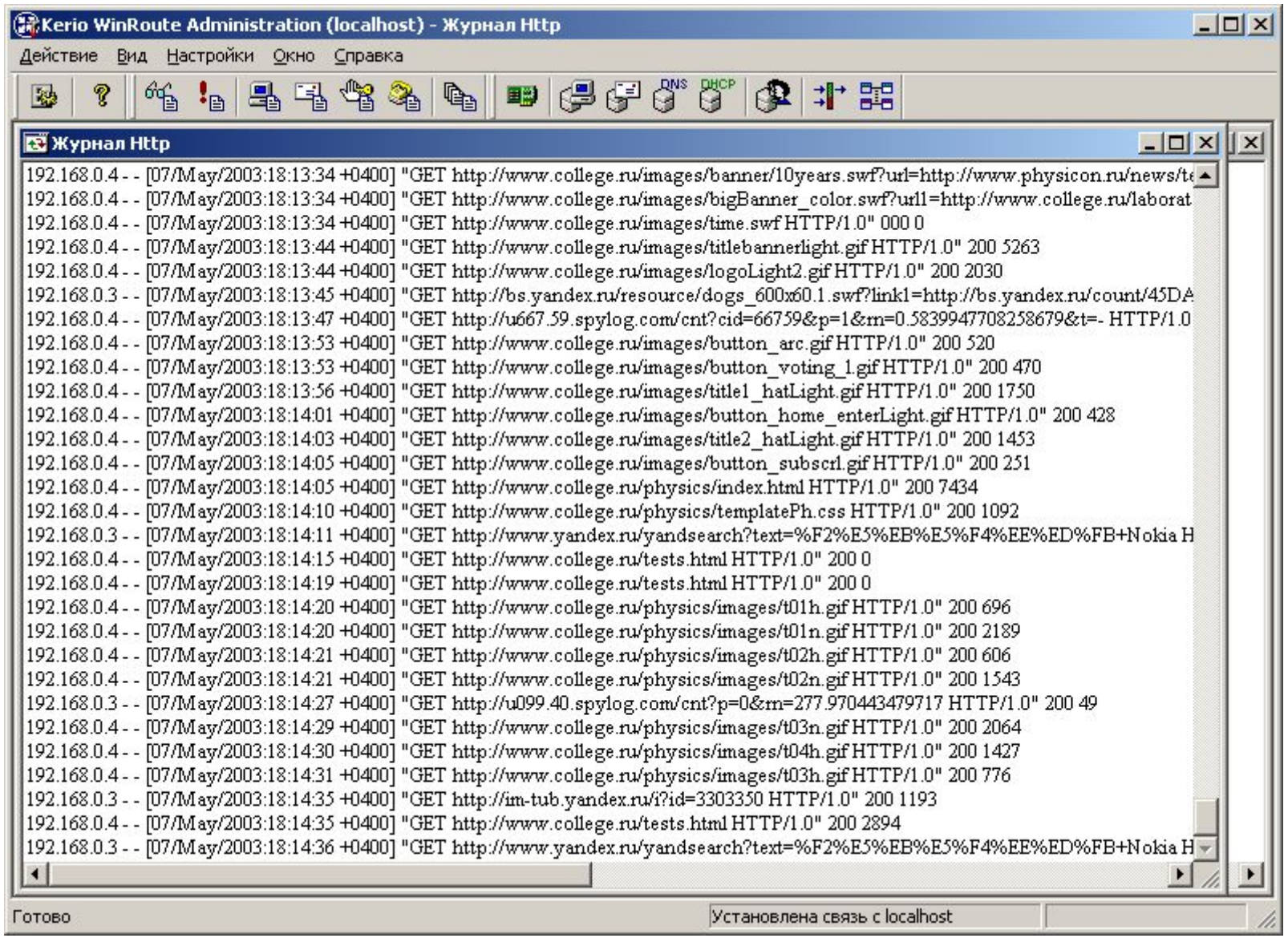

Протоколы PPTP или L2TP, по умолчанию установленные на компьютере, обеспечивают надежный доступ к ресурсам в сети, соединяясь с сервером удаленного доступа Windows 2000 через Интернет или другую сеть. Если для создания сетевого подключение к частной (private) сети используется общедоступная (public) сеть, то совокупность таких подключений называется *виртуальной частной сетью* (Virtual Private Network, VPN).

# Фильтрация TCP/IP

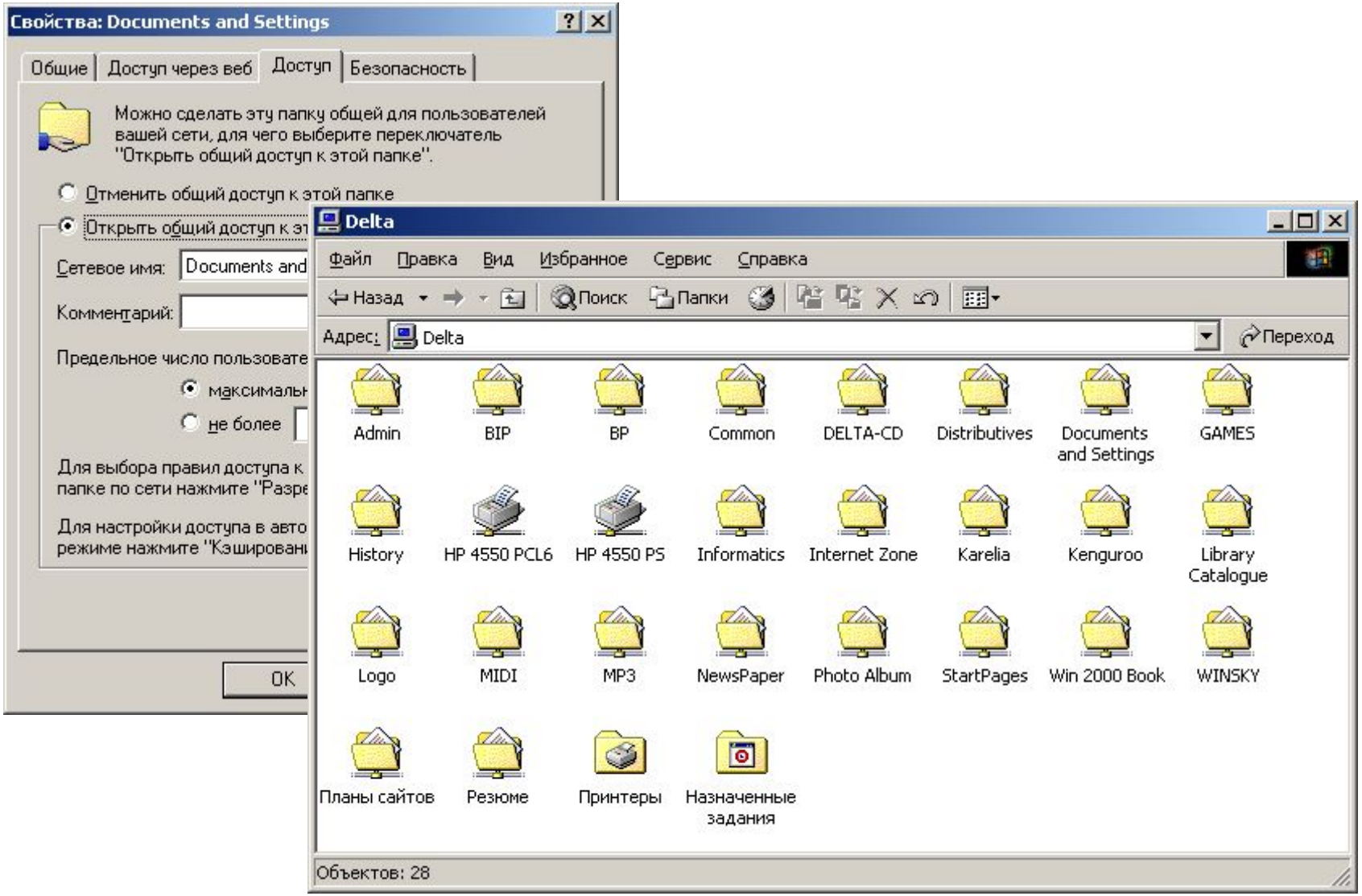


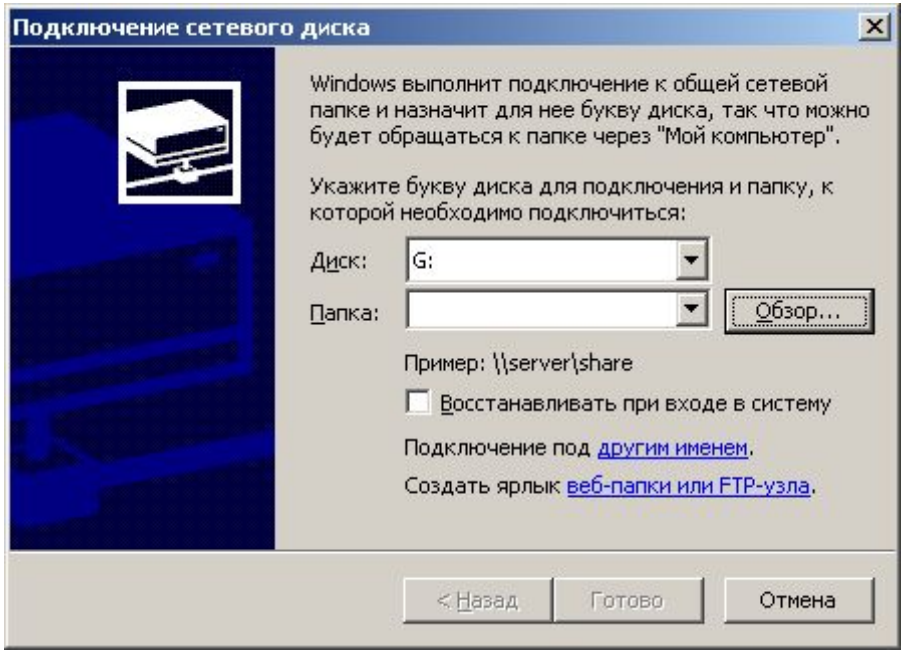
# Proxy-сервер

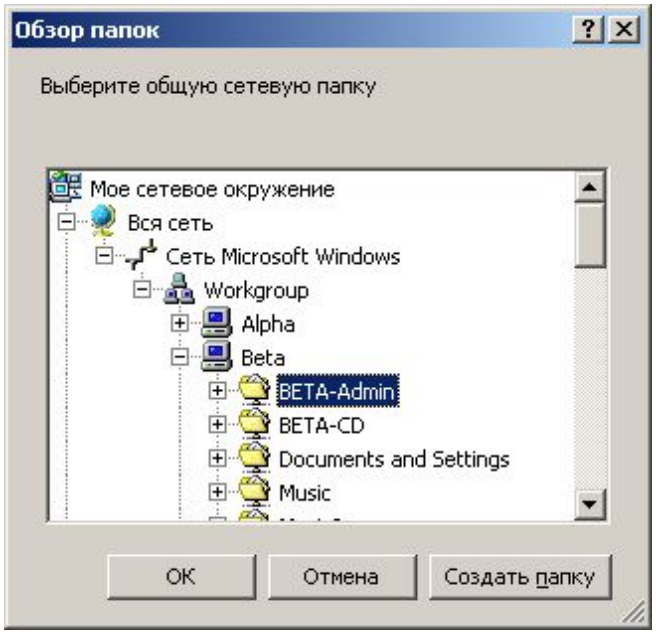


# Сетевая файловая система

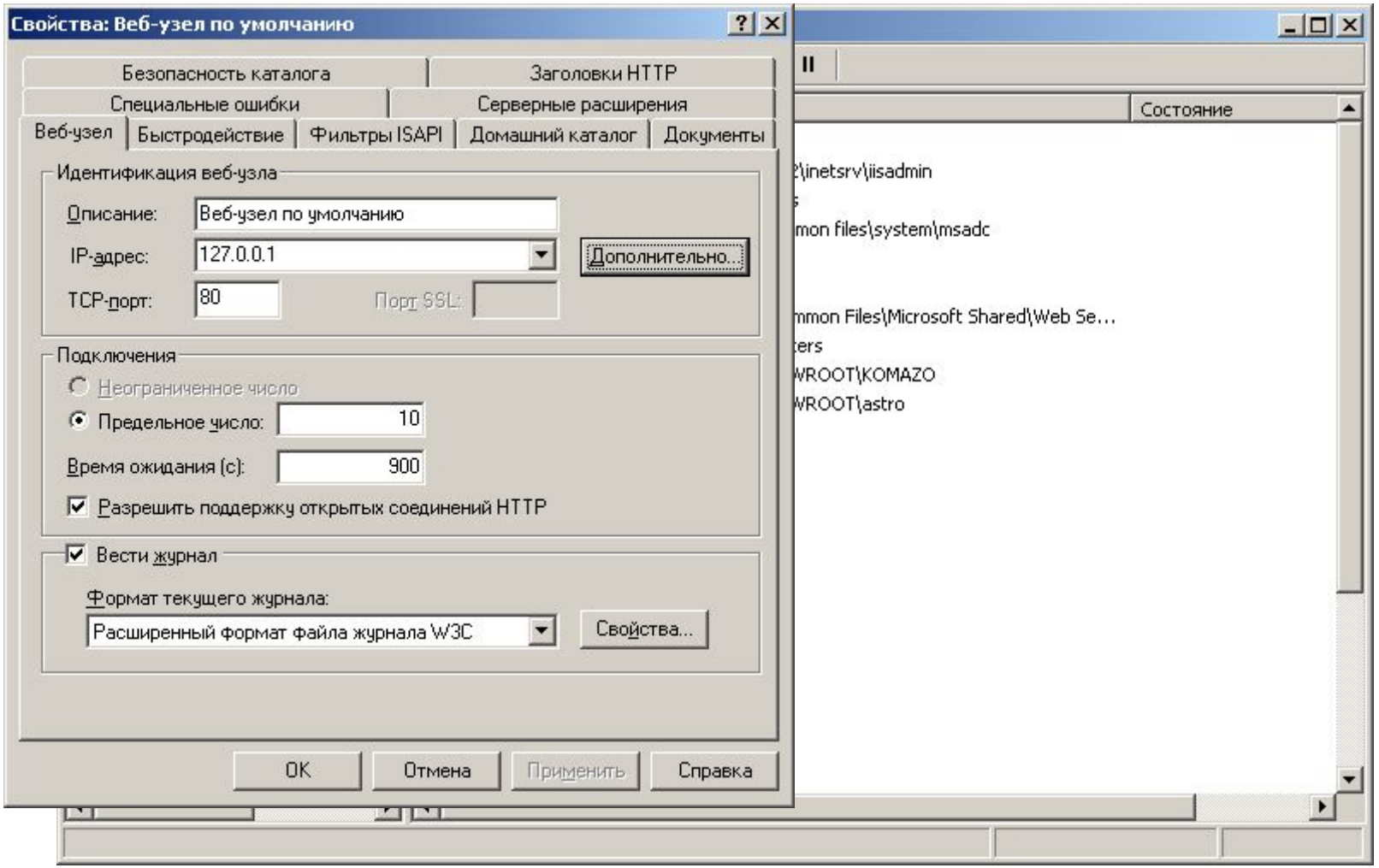


# Сетевые диски

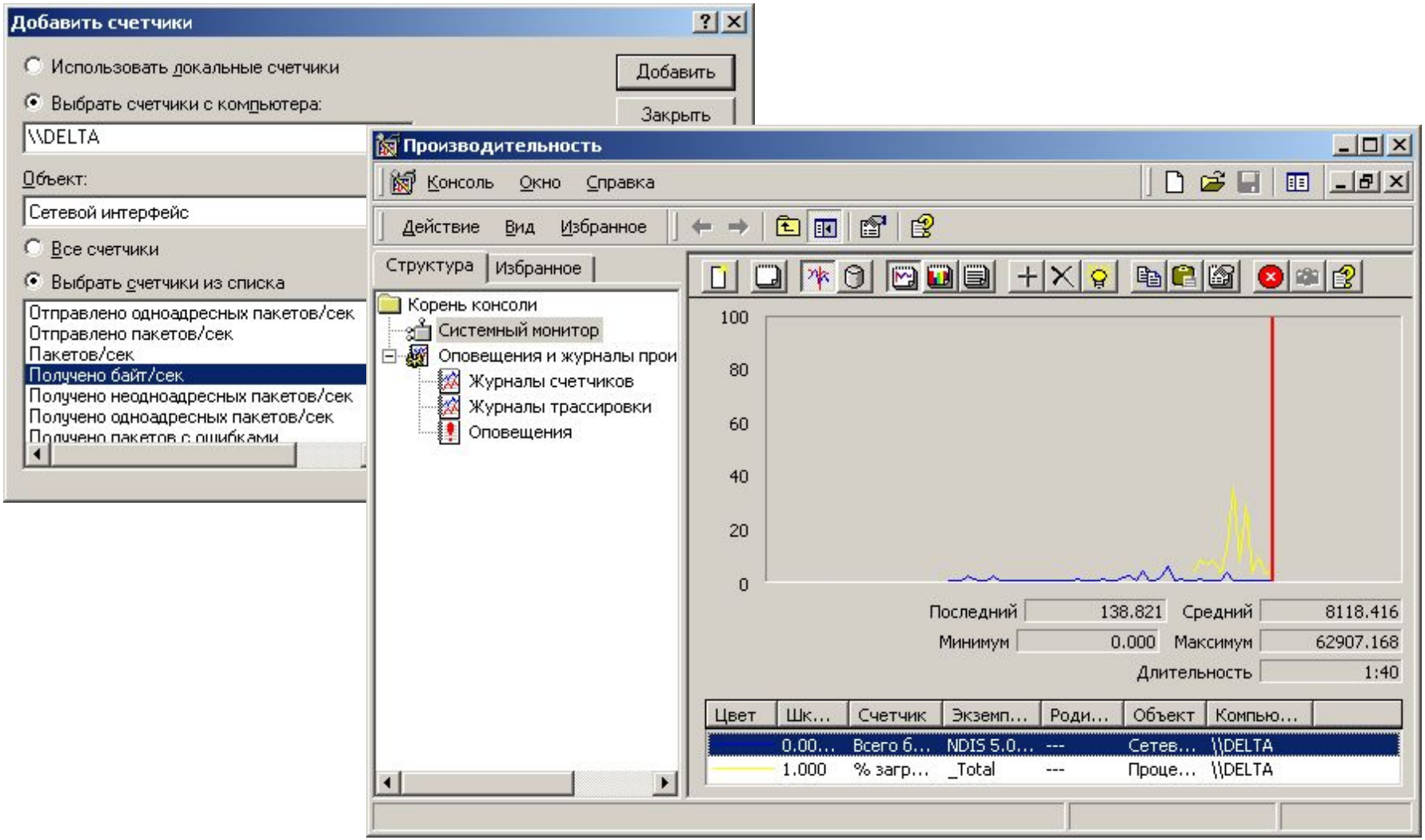


# Web-службы


Свойства: Веб-узел по умолчанию
Безопасность каталога
Заголовки HTTP
Специальные ошибки
Серверные расширения
Веб-узел
Быстродействие
Фильтры ISAPI
Домашний каталог
Документы
Идентификация веб-узла
Описание:
Веб-узел по умолчанию
IP-адрес:
127.0.0.1
Дополнительно...
TCP-порт:
80
Порт SSL:
Подключения
Неограниченное число
Предельное число:
10
Время ожидания (с):
900
Разрешить поддержку открытых соединений HTTP
Вести журнал
Формат текущего журнала:
Расширенный формат файла журнала W3C
Свойства...
OK
Отмена
Применить
Справка
Состояние
?\inetsrv\iisadmin
mon files\system\msadc
mmon Files\Microsoft Shared\Web Se...
ters
WROOT\KOMAZO
WROOT\astro

# Мониторинг сети

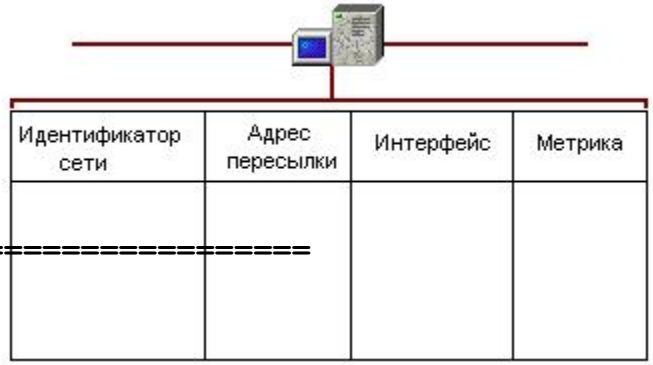


# Поиск неисправностей в сети

```
C:\Documents and Settings\Sasha>ping -t tower
```

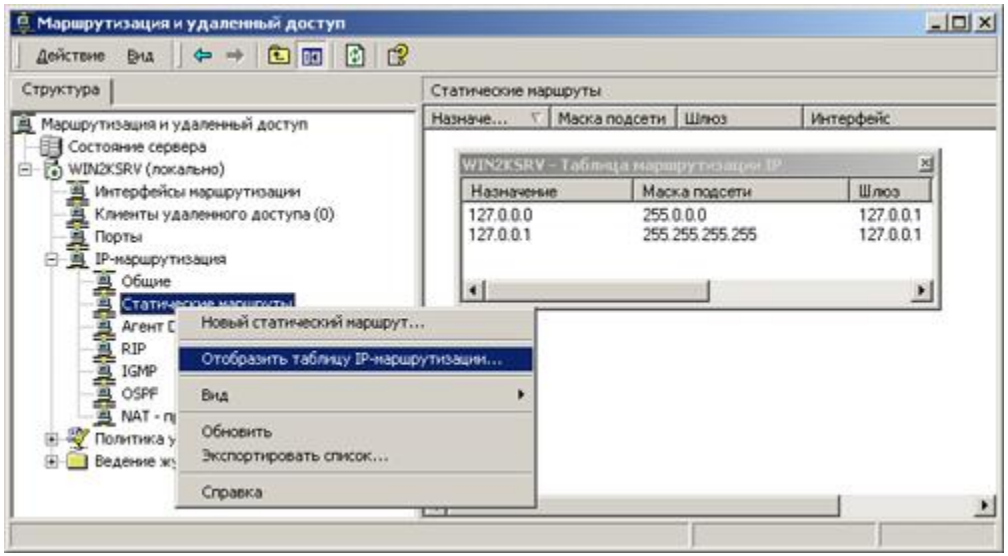
```
C:\WINNT>tracert www.astro.spbu.ru

Трассировка маршрута к urania.astro.spbu.ru [195.19.251.2]
с максимальным числом прыжков 30:

  1   130 ms   150 ms   141 ms  csf.comset.net [213.172.0.206]
  2   160 ms   341 ms   210 ms  Fa0.60.comset-1-gw.comset.net [213.172.0.254]
  3   712 ms   180 ms   160 ms  6.80.ATM0-61.spb-gw.RUNNet.ru [194.85.36.165]
  4   161 ms   200 ms   401 ms  spb-ix.runnet.ru [194.85.36.42]
  5   160 ms   150 ms   190 ms  ptc.spbu.ru [194.190.255.158]
  6   190 ms   221 ms   460 ms  PTCgate.spbu.ru [195.19.224.25]
  7   211 ms   200 ms   150 ms  astro.spbu.ru [195.19.226.170]
  8   170 ms   150 ms   140 ms  urania.astro.spbu.ru [195.19.251.2]

Трассировка завершена.
```

# Маршрутизация

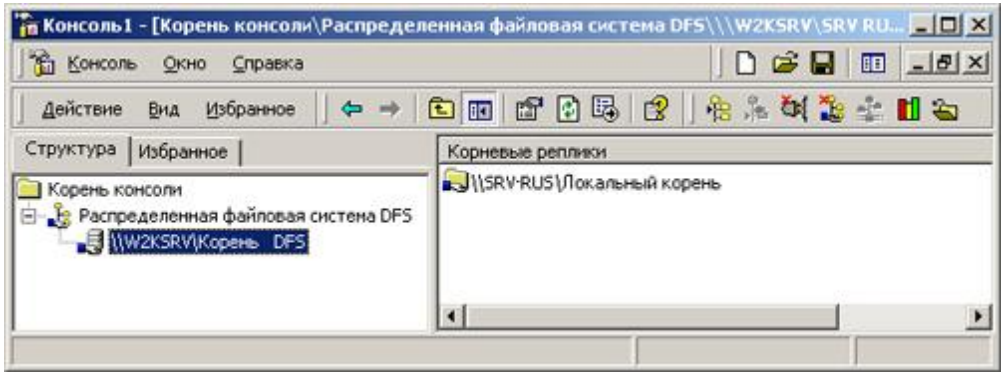


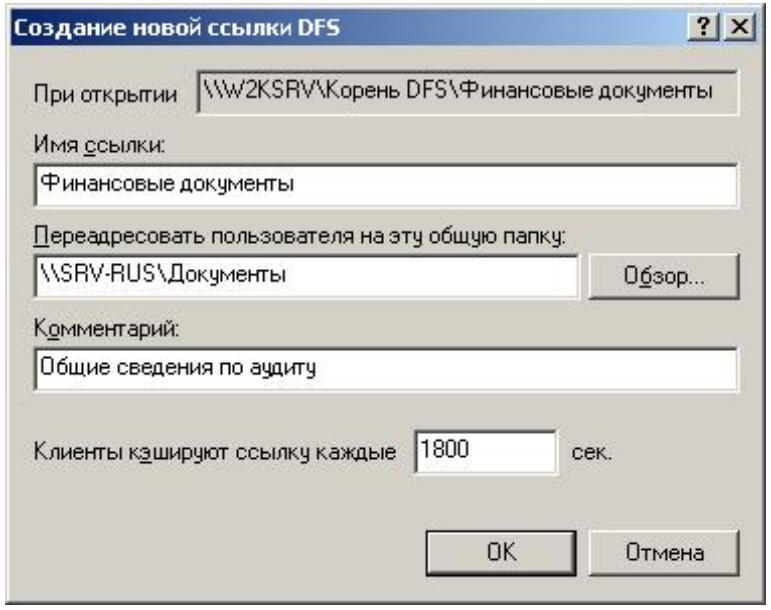

```
C:\>route print
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x2 ...00 e0 4c 39 37 ea ...... NDIS 5.0 driver
0x6000004 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0      213.172.8.1     213.172.8.1       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.0.0    255.255.255.0      192.168.0.1     192.168.0.1       1
      192.168.0.1  255.255.255.255        127.0.0.1       127.0.0.1       1
    192.168.0.255  255.255.255.255      192.168.0.1     192.168.0.1       1
    213.172.0.207  255.255.255.255      213.172.8.1     213.172.8.1       1
      213.172.8.1  255.255.255.255        127.0.0.1       127.0.0.1       1
    213.172.8.255  255.255.255.255      213.172.8.1     213.172.8.1       1
        224.0.0.0        224.0.0.0      192.168.0.1     192.168.0.1       1
        224.0.0.0        224.0.0.0      213.172.8.1     213.172.8.1       1
  255.255.255.255  255.255.255.255      192.168.0.1     192.168.0.1       1
Основной шлюз:         213.172.8.1
===========================================================================
Постоянные маршруты:
  Отсутствует
```

# Маршрутизация в Windows Server




# Распределенная файловая система DFS




Распределенная файловая система (Distributed File System, DFS) для Windows 2000 является средством, облегчающим управление данными в сети и их поиск. DFS позволяет объединить файловые ресурсы, находящиеся на различных компьютерах, в одно пространство имен. Вместо того чтобы работать с физической сетью, состоящей из большого количества машин с собственными именами и общими ресурсами, пользователи смогут увидеть структуру логических имен, связанных с общими ресурсами.

# Автономные файлы