Стек протоколов TCP/IP
Базовые понятия

Педагог: Михаил Романович 2022 г.

- **Стек TCP/IP** – это набор иерархически упорядоченных сетевых протоколов. Название стек получил по двум важнейшим протоколам – TCP (Transmission Control Protocol) и IP (Internet Protocol). Помимо них в стек входят ещё несколько десятков различных протоколов. В настоящее время протоколы TCP/IP являются основными для Интернета, а также для большинства корпоративных и локальных сетей.
- В операционной системе Microsoft Windows Server 2003 стек TCP/IP выбран в качестве основного, хотя поддерживаются и другие протоколы (например, стек IPX/SPX, протокол NetBIOS).
- Стек протоколов TCP/IP обладает двумя важными свойствами:
- • платформонезависимостью, т. е. возможна его реализация на самых разных операционных системах и процессорах;
- • открытостью, т. е. стандарты, по которым строится стек TCP/IP, доступны любому желающему.

История создания TCP/IP

- В 1967 году Агентство по перспективным исследовательским проектам министерства обороны США (ARPA – Advanced Research Projects Agency) инициировало разработку компьютерной сети, которая должна была связать ряд университетов и научно-исследовательских центров, выполнявших заказы Агентства. Проект получил название ARPANET. К 1972 году сеть соединяла 30 узлов.
- В рамках проекта ARPANET были разработаны и в 1980–1981 годах опубликованы основные протоколы стека TCP/IP – IP, TCP и UDP. Важным
- фактором распространения TCP/IP стала реализация этого стека в операционной системе UNIX 4.2 BSD (1983).
- К концу 80-х годов значительно расширившаяся сеть ARPANET стала называться Интернет (Interconnected networks – связанные сети) и объединяла университеты и научные центры США, Канады и Европы.
- В 1992 году появился новый сервис Интернет – WWW (World Wide Web – всемирная паутина), основанный на протоколе HTTP. Во многом благодаря WWW Интернет, а с ним и протоколы TCP/IP, получил в 90-е годы бурное развитие.
- В начале XXI века стек TCP/IP приобретает ведущую роль в средствах коммуникации не только глобальных, но и локальных сетей.

Модель OSI

- Модель взаимодействия открытых систем (OSI – Open Systems Interconnection) была разработана Международной организацией по стандартизации (ISO – International Organization for Standardization) для единообразного подхода к построению и объединению сетей. Разработка модели OSI началась в 1977 году и закончилась в 1984 году утверждением стандарта. С тех пор модель является эталонной для разработки, описания и сравнения различных стеков протоколов.
- Модель OSI включает семь уровней: физический, канальный, сетевой, транспортный, сеансовый, представления и прикладной.

- Рассмотрим кратко функции каждого уровня.
- 1. Физический уровень (physical layer) описывает принципы передачи сигналов, скорость передачи, спецификации каналов связи. Уровень реализуется аппаратными средствами (сетевой адаптер, порт концентратора, сетевой кабель).
- 2. Канальный уровень (data link layer) решает две основные задачи – проверяет доступность среды передачи (среда передачи чаще всего оказывается разделена между несколькими сетевыми узлами), а также обнаруживает и исправляет ошибки, возникающие в процессе передачи. Реализация уровня является программно-аппаратной (например, сетевой адаптер и его драйвер).
- 3. Сетевой уровень (network layer) обеспечивает объединение сетей, работающих по разным протоколам канального и физического уровней, в составную сеть. При этом каждая из сетей, входящих в единую сеть, называется *подсетью* (subnet). На сетевом уровне приходится решать две основные задачи – *маршрутизации* (routing, выбор оптимального пути передачи сообщения) и *адресации* (addressing, каждый узел в составной сети должен иметь уникальное имя). Обычно функции сетевого уровня реализует специальное устройство – *маршрутизатор* (router) и его программное обеспечение.
- 4. Транспортный уровень (transport layer) решает задачу надежной передачи сообщений в составной сети с помощью подтверждения доставки и повторной отправки пакетов. Этот уровень и все следующие реализуются программно.
- 5. Сеансовый уровень (session layer) позволяет запоминать информацию о текущем состоянии сеанса связи и в случае разрыва соединения возобновлять сеанс с этого состояния.
- 6. Уровеньпредставления (presentation layer) обеспечивает преобразование передаваемой информации из одной кодировки в другую (например, из ASCII в EBCDIC).
- 7. Прикладной уровень (application layer) реализует интерфейс между остальными уровнями модели и пользовательскими приложениями.

Структура TCP/IP

- В основе структуры TCP/IP лежит не модель OSI, а собственная модель, называемая DARPA (Defense ARPA – новое название Агентства по перспективным исследовательским проектам) или DoD (Department of Defense – Министерство обороны США). В этой модели всего четыре уровня. Соответствие модели OSI модели DARPA, а также основным протоколам стека TCP/IP

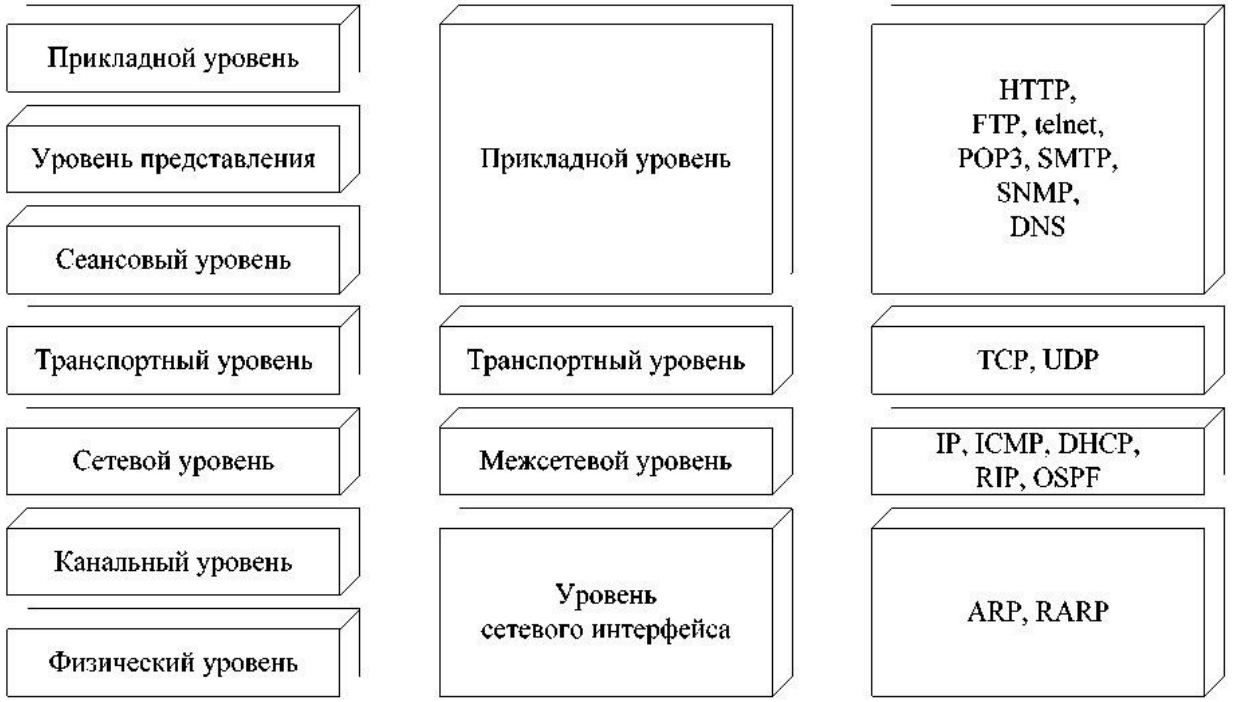


Рис. 2.2. Соответствие протоколов TCP/IP моделям OSI и DARPA

Следует заметить, что нижний уровень модели DARPA – уровень сетевых интерфейсов – строго говоря, не выполняет функции канального и физического уровней, а лишь обеспечивает связь (интерфейс) верхних уровней DARPA с технологиями сетей, входящих в составную сеть (например, Ethernet, FDDI, ATM).

Все протоколы, входящие в стек TCP/IP, стандартизованы в документах RFC.

Основные протоколы

- ***Протокол IP*** *(Internet Protocol)* – это основной протокол сетевого уровня, отвечающий за адресацию в составных сетях и передачу пакета между сетями. Протокол IP является *дейтаграммным* протоколом, т. е. не гарантирует доставку пакетов до узла назначения. Обеспечением гарантий занимается протокол транспортного уровня TCP.
- ***Протоколы RIP*** *(Routing Information Protocol* – протокол маршрутной информации*) и OSPF (Open Shortest Path First* – «первыми открываются кратчайшие маршруты»*)* – протоколы маршрутизации в IP-сетях.
- ***Протокол ICMP*** *(Internet Control Message Protocol* – протокол управляющих сообщений в составных сетях) предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов сообщает о невозможности доставки пакета, о продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.
- ***Протокол ARP*** *(Address Resolution Protocol* – протокол преобразования адресов) преобразует IP-адреса в аппаратные адреса локальных сетей. Обратное преобразование осуществляется с помощью протокола *RAPR* (Reverse ARP).
- ***TCP*** *(Transmission Control Protocol* – протокол управления передачей) обеспечивает надежную передачу сообщений между удаленными узлами сети за счет образования логических соединений. TCP позволяет без ошибок доставить сформированный на одном из компьютеров поток байт на любой другой компьютер, входящий в составную сеть. TCP делит поток байт на части – *сегменты* и передает их сетевому уровню. После того как эти сегменты будут доставлены в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

- ***UDP*** *(User Datagram Protocol* – протокол дейтаграмм пользователя) обеспечивает передачу данных дейтаграммным способом.
- Далее рассматриваются протоколы прикладного уровня.
- ***HTTP*** *(HyperText Transfer Protocol* – протокол передачи гипертекста) – протокол доставки web-документов, основной протокол службы WWW.
- ***FTP*** *(File Transfer Protocol* – протокол передачи файлов) – протокол для пересылки информации, хранящейся в файлах.
- ***POP3*** *(Post Office Protocol version 3* – протокол почтового офиса) и ***SMTP*** *(Simple Mail Transfer Protocol* – простой протокол пересылки почты) – протоколы для доставки входящей электронной почты (POP3) и отправки исходящей (SMTP).
- ***Telnet*** – протокол эмуляции терминала1, позволяющий пользователю подключаться к другим удалённым станциям и работать с ними со своей машины, как если бы она была их удалённым терминалом.
- ***SNMP*** *(Simple Network Management Protocol* – простой протокол управления сетью) предназначен для диагностики работоспособности различных устройств сети.

Терминал – это сочетание устройства ввода и устройства вывода, например клавиатура и дисплей

Утилиты диагностики TCP/IP

- В состав операционной системы входит ряд утилит (небольших программ), предназначенных для диагностики функционирования стека TCP/IP. Каждый системный администратор должен знать эти утилиты и уметь применять их на практике.
- Информацию о любой утилите можно вывести, набрав в командной строке имя утилиты с ключом «/?», например: IPconfig /?

- **IPconfig**
- Утилита предназначена, во-первых, для вывода информации о конфигурации стека TCP/IP, во-вторых, для выполнения некоторых действий по настройке стека.
- При вводе названия утилиты в командной строке без параметров на экране отобразится информация об основных настройках TCP/IP (эти настройки рассматриваются в следующих лекциях):
- – суффикс DNS (Connection-specific DNS Suffix); – IP-адрес (IP Address);
- – маска подсети (Subnet Mask);
- – шлюз по умолчанию (Default Gateway). Приведем основные ключи утилиты:
- • **/all** – отображение полной информации о настройке стека TCP/IP на данном компьютере. Следует отметить, что при наличии нескольких сетевых адаптеров выводятся данные по каждому адаптеру отдельно. Наиболее важные сведения кроме представленных выше – физический адрес (MAC-адрес) сетевого адаптера (Physical Address) и наличие разрешения DHCP (DHCP Enabled).
- • **/release** – освобождение IP-адреса (имеет смысл, если DHCP разрешен).
- • **/renew** – обновление конфигурации TCP/IP (обычно выполняется, если DHCP разрешен).
- • **/displaydns** – вывод на экран кэша имен DNS. • **/flushdns** – очистка кэша имен DNS.
- • **/registerdns** – обновление аренды DHCP и перерегистрация доменного имени в базе данных службы DNS.

- Ping
- Основная цель этой популярной утилиты – выяснение возможности установления соединения с удаленным узлом. Кроме того, утилита может обратиться к удаленному компьютеру по доменному имени, чтобы проверить способность преобразования символьного доменного имени в IP-адрес.
- Принцип работы: утилита отправляет на удаленный узел несколько пакетов (число пакетов определяется ключом **–n**, по умолчанию четыре) по протоколу ICMP. Такие пакеты называются эхо-пакетами, т. е. требуют
- ответа. Если удаленный узел доступен, он отвечает на каждый эхо-пакет своим пакетом, а утилита измеряет интервал между отправкой эхо-пакета и приходом ответа.
- Нужно отметить, что отсутствие ответа может быть связано не с физической недоступностью удаленного компьютера, а с тем, что на нем установлено программное обеспечение, запрещающее отправку ответов на эхо-пакеты (брандмауэр – firewall).
- Основные ключи:
- • **–t** – пакеты отправляются до тех пор, пока пользователь не нажмет комбинацию CTRL+C.
- • **–a** – определение доменного имени по IP-адресу.
- • **–l <размер>** – максимальный размер пакета (по умолчанию 32 байта).
- • **–w <таймаут>** – задание времени ожидания ответа в миллисекундах (по умолчанию 1000 миллисекунд = 1 секунда).

Утилита **Netstat**

- Утилита отображает статистическую информацию по протоколам IP, TCP, UDP и ICMP, а также позволяет отслеживать сетевые соединения. Основные ключи:
- • **/a** – список всех подключений и прослушивающихся портов. • **/e** – статистика для Ethernet.
- • **/n** – список всех подключений и портов в числовом формате. • **/s** – статистика для перечисленных четырех протоколов.
- • **<interval>** – интервал в секундах, через который утилита выводит требуемую информацию (для прекращения вывода – CTRL+C).
-
- **Arp**
- Эта утилита работает с протоколами преобразования IP-адресов в MAC-адреса и обратно ARP и RARP. С её помощью можно выводить на экран таблицу соответствия IP-адресов и MAC-адресов (ARP-кэш), добавлять и удалять записи в ней.
- Основные ключи:
- • **/a** – отображение таблицы ARP или, если указан IP-адрес, запись только для этого адреса.
- • **/s** – добавление записи в таблицу. • **/d** – удаление записи из таблицы.
-
- **Hostname**
- Это самая простая утилита – она выводит на экран имя компьютера.

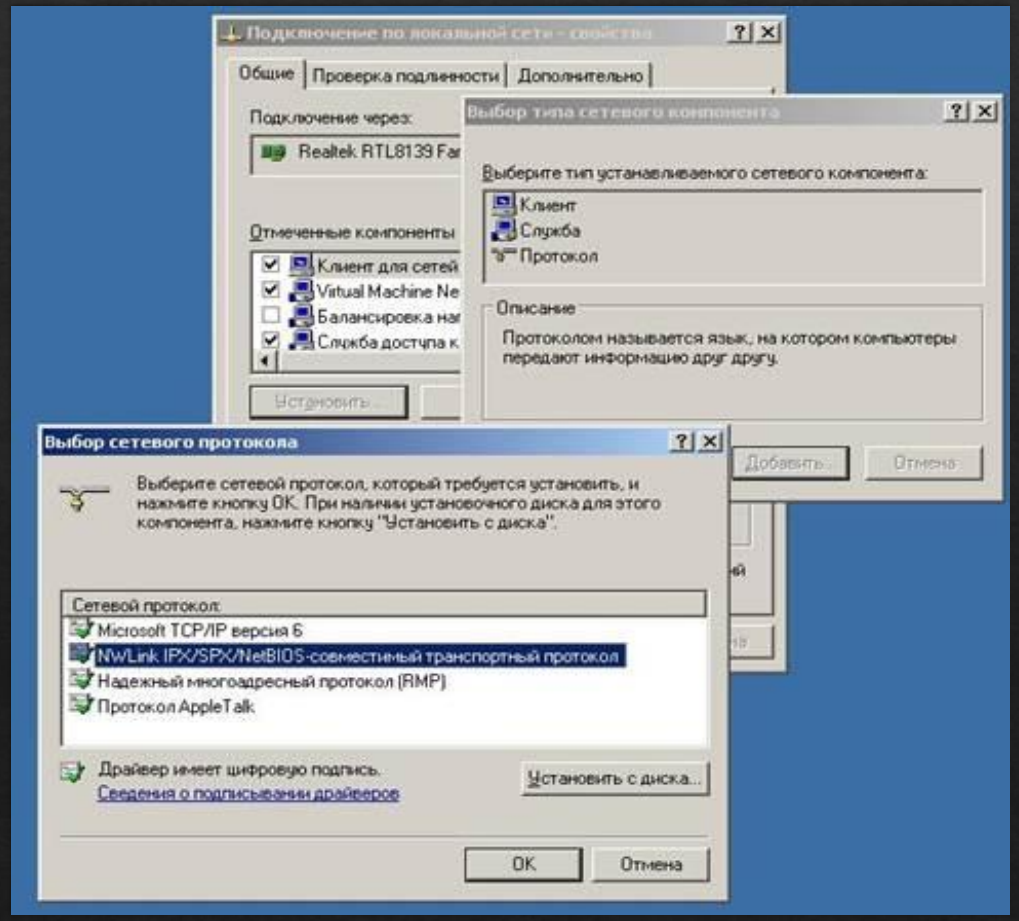
- Стек протоколов TCP/IP – это самый распространенный на сегодняшний день набор иерархически упорядоченных протоколов, применяемый как в локальных, так и в глобальных сетях. Важнейшие протоколы стека – IP, TCP и UDP – появились в начале 80-х годов в рамках проекта ARPANET, который являлся предшественником Интернета. В 90-е годы по мере развития Интернета роль стека TCP/IP сильно возросла.
- Стек TCP/IP был разработан на основе модели сетевого взаимодействия DARPA, хотя между уровнями модели DARPA, международной семиуровневой моделью OSI и стеком TCP/IP может быть установлено соответствие. Стандарты протоколов TCP/IP отражены в свободно доступных документах RFC.
- Основными протоколами стека являются IP, TCP, UDP, ICMP, ARP, протоколы маршрутизации RIP и OSPF, протоколы прикладного уровня HTTP, FTP, POP3, SMTP, telnet, SNMP.
- Для диагностики и управления стеком TCP/IP в операционной системе Microsoft Windows существуют специальные утилиты – IPconfig, ping, tracert, netstat, arp, hostname и др.

Стек протоколов IPX/SPX

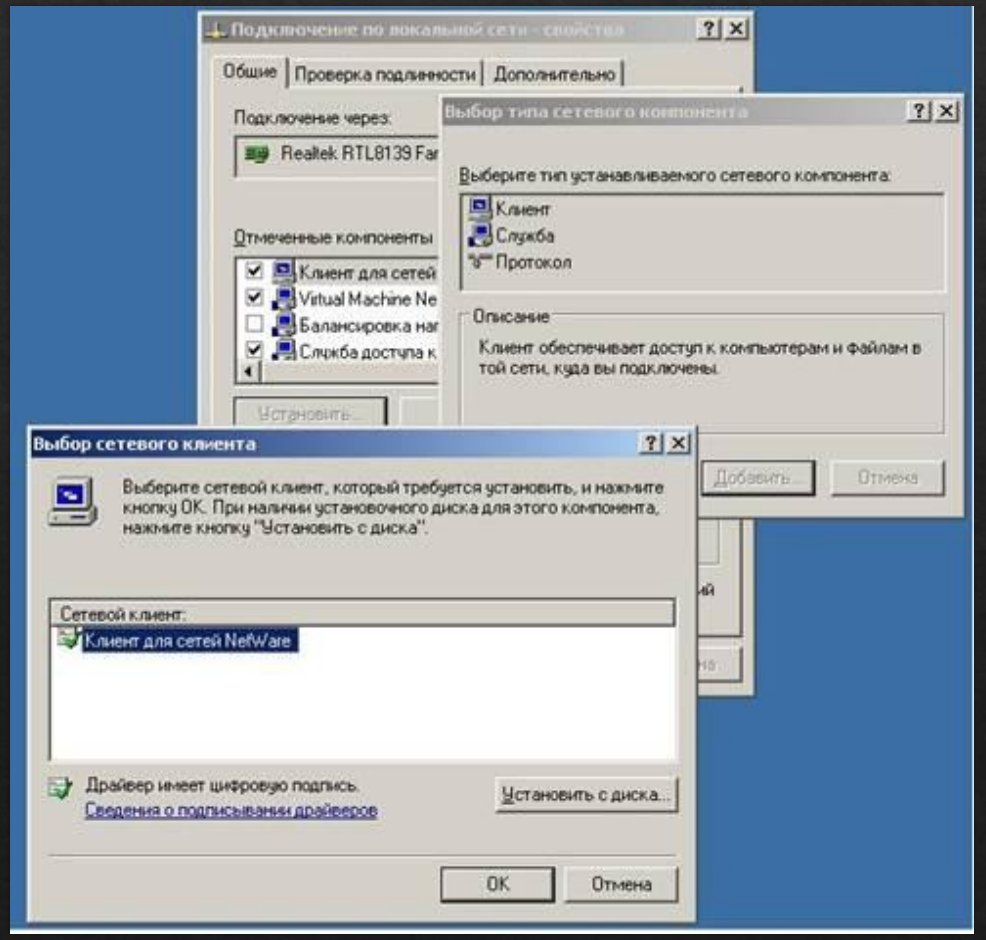
- Этот стек является оригинальным стеком протоколов фирмы Novell, разработанным для сетевой операционной системы NetWare еще в начале 80-х годов. Протоколы сетевого и сеансового уровня Internetwork Packet Exchange (IPX) и Sequenced Packet Exchange (SPX), которые дали название стеку, являются прямой адаптацией протоколов XNS фирмы Xerox, распространенных в гораздо меньшей степени, чем стек IPX/SPX. Популярность стека IPX/SPX непосредственно связана с операционной системой Novell NetWare.

- Многие особенности стека IPX/SPX обусловлены ориентацией ранних версий ОС NetWare (до версии 4.0) на работу в локальных сетях небольших размеров, состоящих из персональных компьютеров со скромными ресурсами. Понятно, что для таких компьютеров Novell нужны были протоколы, на реализацию которых требовалось бы минимальное количество оперативной памяти и которые бы быстро работали на процессорах небольшой вычислительной мощности. В результате протоколы стека IPX/SPX до недавнего времени хорошо работали в локальных сетях и не очень — в больших корпоративных сетях, так как они слишком перегружали медленные глобальные связи широковещательными пакетами, которые интенсивно используются несколькими протоколами этого стека (например, для установления связи между клиентами и серверами). Это обстоятельство, а также тот факт, что стек IPX/SPX является собственностью фирмы Novell, и на его реализацию нужно получать у нее лицензию, долгое время ограничивали распространенность его только сетями NetWare. С момента выпуска версии NetWare 4.0 Novell внесла и продолжает вносить в свои протоколы серьезные изменения, направленные на приспособление их для работы в корпоративных сетях. Сейчас стек IPX/SPX реализован не только в NetWare, но и в нескольких других популярных сетевых ОС, например, Microsoft Windows NT. Начиная с версии 5.0 фирма Novell в качестве основного протокола своей серверной операционной системы стала использовать протокол TCP/IP, и с тех пор практическое применение IPX/SPX стало неуклонно снижаться.

- Как уже говорилось выше, стек протоколов IPX/SPX является фирменным запатентованным стеком компании Novell. Реализация данного протокола в операционных системах Microsoft называется NWLink (или IPX/SPX-совместимый протокол). Добавить данный протокол можно через *Свойства* «*Подключения по локальной сети*» (кнопка «*Установить*», выбрать «*Протокол*», кнопка «*Добавить*», выбрать «*NWLink*», кнопка «*ОК*».



- Для того, чтобы из сети под управлением систем семейства Windows получить доступ в сеть под управлением служб каталогов Novell, кроме NWLink, необходимо установить также клиента сетей Novell (*Свойства* «*Подключения по локальной сети*», кнопка «*Установить*», выбрать «*Клиент*», кнопка «*Добавить*», выбрать «*Клиент для сетей NetWare*», кнопка «*ОК*»; рис. 6.2).



- В серверных системах Windows (до Windows 2000 включительно) имелась также служба под названием «*Шлюз для сетей NetWare*», позволявшая клиентам сетей Microsoft без установки клиента сетей NetWare получать доступ к ресурсам серверов под управлением Novell NetWare (через шлюз, установленный на сервере Windows NT/2000). В системе Windows 2003 служба шлюза отсутствует.