Администрирование локальных сетей

Тема 5.

Протоколы семейства TCP/IP

Основные вопросы лекции

- Сетевой уровень взаимодействия. Маршрутизируемые протоколы, их преимущества.
- Структура стека протоколов TCP/IP.
- IP-адресация. Классы сетей. Принцип маршрутизации в IP-сетях. Публичные и приватные сети.
- Механизм трансляции сетевых адресов (NAT).
- Механизм доступа к сети передачи данных. Протокол разрешения адресов – ARP.
- Использование протокола ICMP для задач мониторинга и настройки сетей. Информационные Команды контроля работы IP-соединений.
- Маршрутизация в сетях TCP/IP.
- Протоколы транспортного уровня: UDP и TCP, их особенности. Порты.

Сетевой уровень взаимодействия

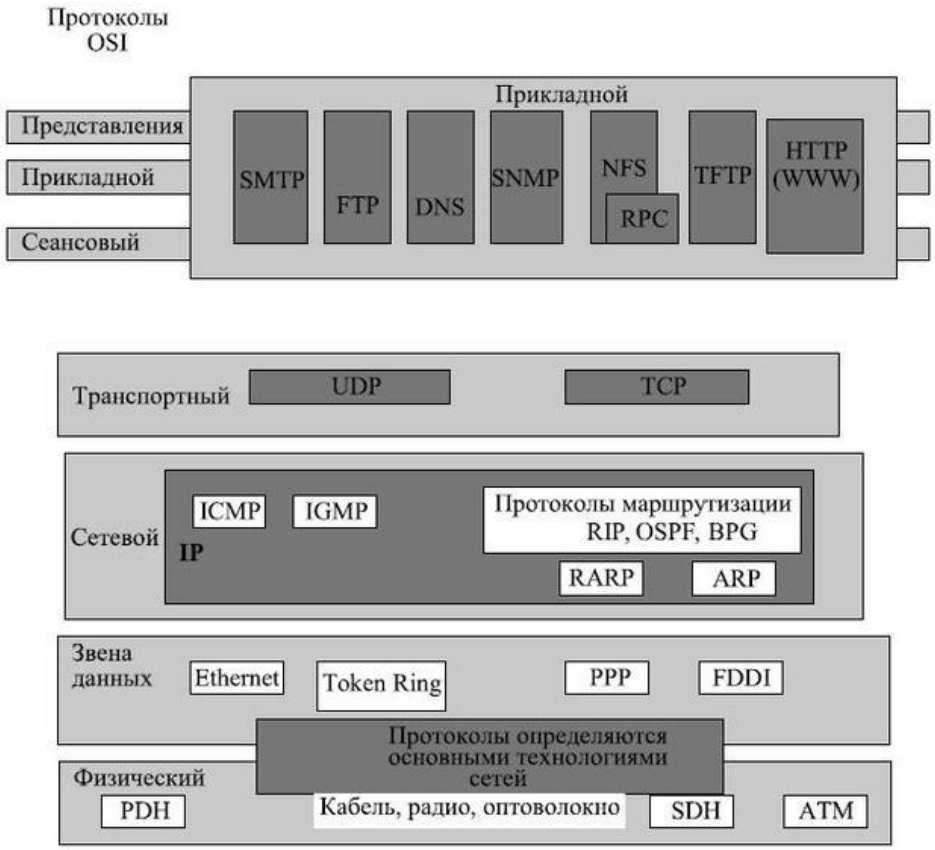
- **Сетевой уровень** (Network layer) – 3 уровень в модели OSI служит для образования единой транспортной системы, объединяющей несколько сетей.
- Сетевой уровень обеспечивает доставку данных между компьютерами сети, представляющей собой объединение различных физических сетей.
- Данный уровень предполагает наличие средств **логической адресации**, позволяющих однозначно идентифицировать компьютер в объединенной сети.
- Одной из главных функций, выполняемых средствами данного уровня, является целенаправленная передача данных конкретному получателю.

Маршрутизируемые протоколы, их преимущества

- Протоколы сетевого уровня могут быть **маршрутизируемыми** и **немаршрутизиремыми**.
  - Немаршрутизируемые протоколы не содержат адресной информации на сетевом уровне; к таким протоколам относятся, например, протокол LAT (Local Area Transport — транспортный протокол для терминального сервера) компании DEC и протокол NetBEUI (Network Basic Input/Output System).
  - Отсутствие информации об адресах сетевого уровня лишает маршрутизаторы возможности определить, в какую сеть или к какому хосту направлять пакеты.
  - Поэтому немаршрутизируемые протоколы требуют наличия мостов или коммутаторов, использующих информацию уровня 2 — физические MAC-адреса.
  - Как правило, немаршрутизируемые протоколы являются широковещательными, что приводит к неэффективному использованию полосы пропускания и увеличивают трафик в сети.
- Маршрутизируемые протоколы, позволяют объединить множество сетей без использования широковещательного трафика.
  - При соединении выбранной сети с другими сетями используется маршрутизатор, хранящий информацию о маршрутах доставки пакетов в нужную сеть.
  - Такой подход позволяет предотвратить распространение широковещательного трафика в другие сети.

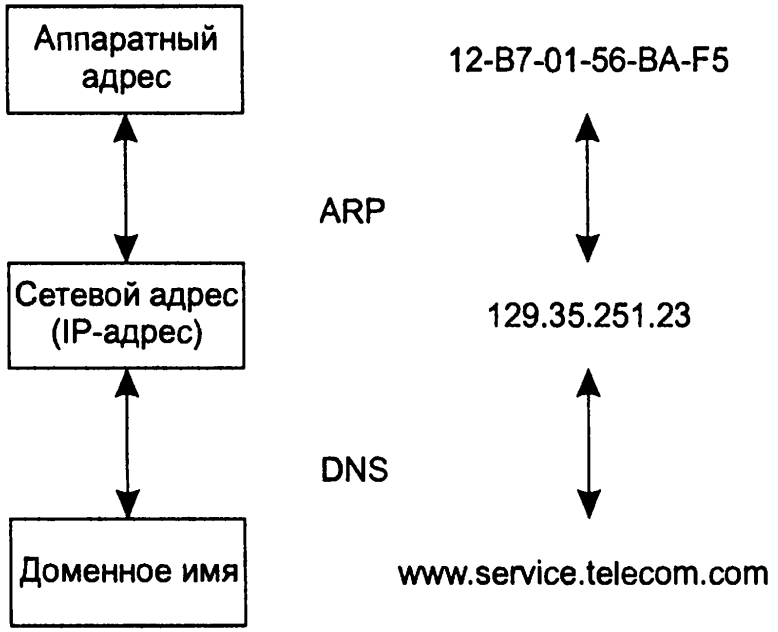
Структура стека протоколов TCP/IP

- Стек TCP/IP описывает набор протоколов в масштабируемых сетях, типа Интернет.
- Стек TCP/IP — иерархический, составленный из диалоговых модулей, каждый из которых обеспечивает заданные функциональные возможности; но эти модули не обязательно взаимозависимые.
- В отличие от модели OSI, где определяется строго, какие функции принадлежат каждому из ее уровней, уровни набора протокола TCP/IP содержат относительно независимые протоколы, которые могут быть смешаны и согласованы в зависимости от потребностей системы.



IP-адресация

- В технологии TCP/IP для решения задачи объединения сетей используется глобальная система адресации, не зависящая от способов адресации узлов в отдельных сетях.
- Эта система адресации позволяет универсальным и однозначным способом идентифицировать любой интерфейс составной сети.
- Используется уникальная нумерация всех сетей составной сети, а затем нумерация всех узлов в пределах каждой из этих сетей.
- Пара, состоящая из номера сети и номера узла, служит в качестве сетевого адреса.



Порядок назначения IP-адресов

- По определению схема IP-адресации должна обеспечивать уникальность нумерации сетей, а также уникальность нумерации узлов в пределах каждой из сетей.
- Процедуры назначения номеров как сетям, так и узлам сетей являются *централизованными.*
  - Рекомендуемый порядок назначения IP-адресов дается в RFC 2050.

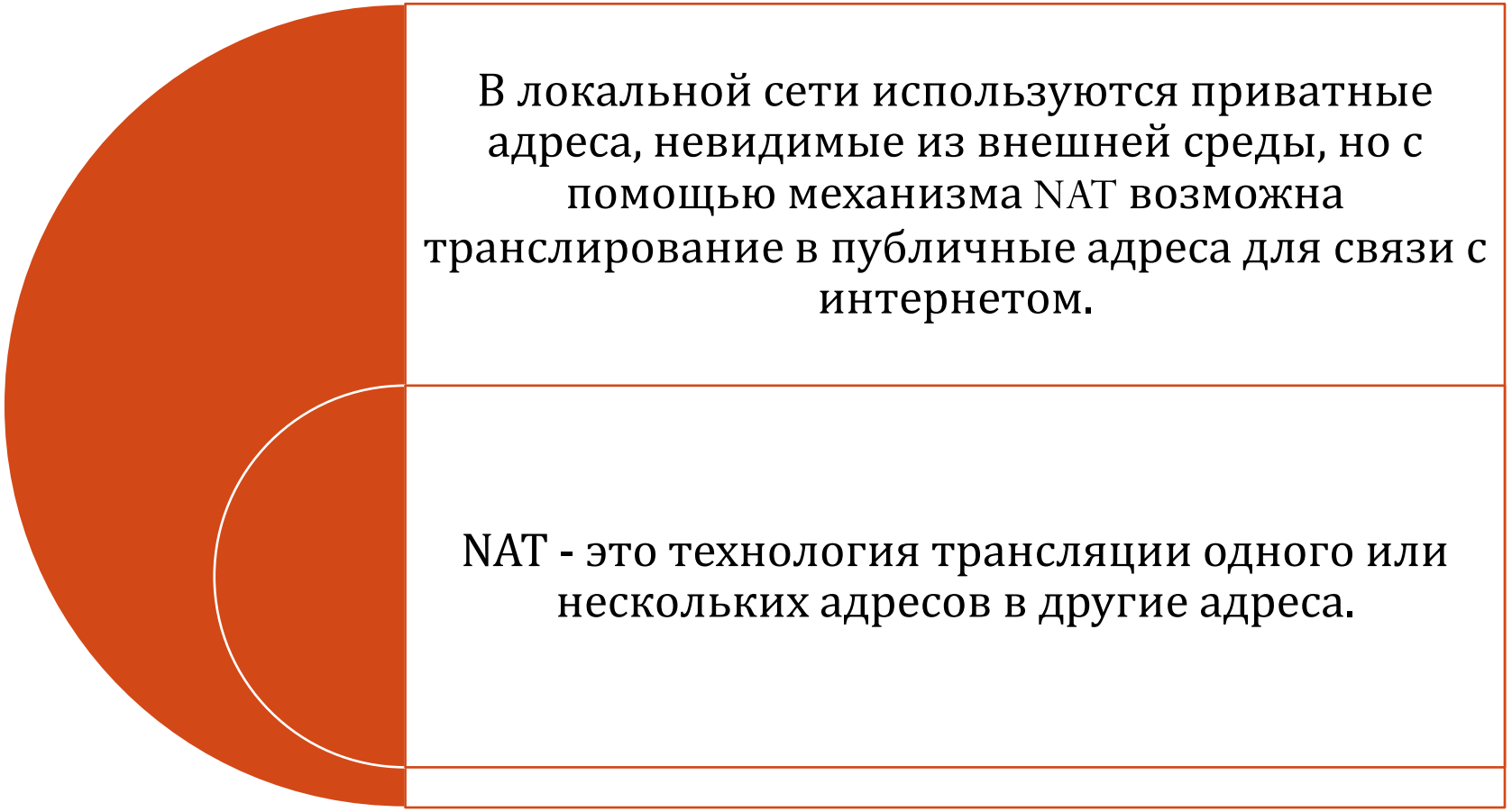
Приватные адреса

При произвольном выборе адресов локальной сети адреса могут совпасть с централизовано назначенными адресами Интернета.

Для того чтобы избежать коллизий, связанных с такого рода совпадениями, в стандартах Интернета определено несколько так называемых **частных (приватных) адресов**, рекомендуемых для автономного использования:

- в классе A — сеть 10.0.0.0;
- в классе B — диапазон из 16 номеров сетей 172.16.0.0-172.31.0.0;
- в классе C - диапазон из 255 сетей - 192.168.0.0-192.168.255.0.

Механизм трансляции сетевых адресов

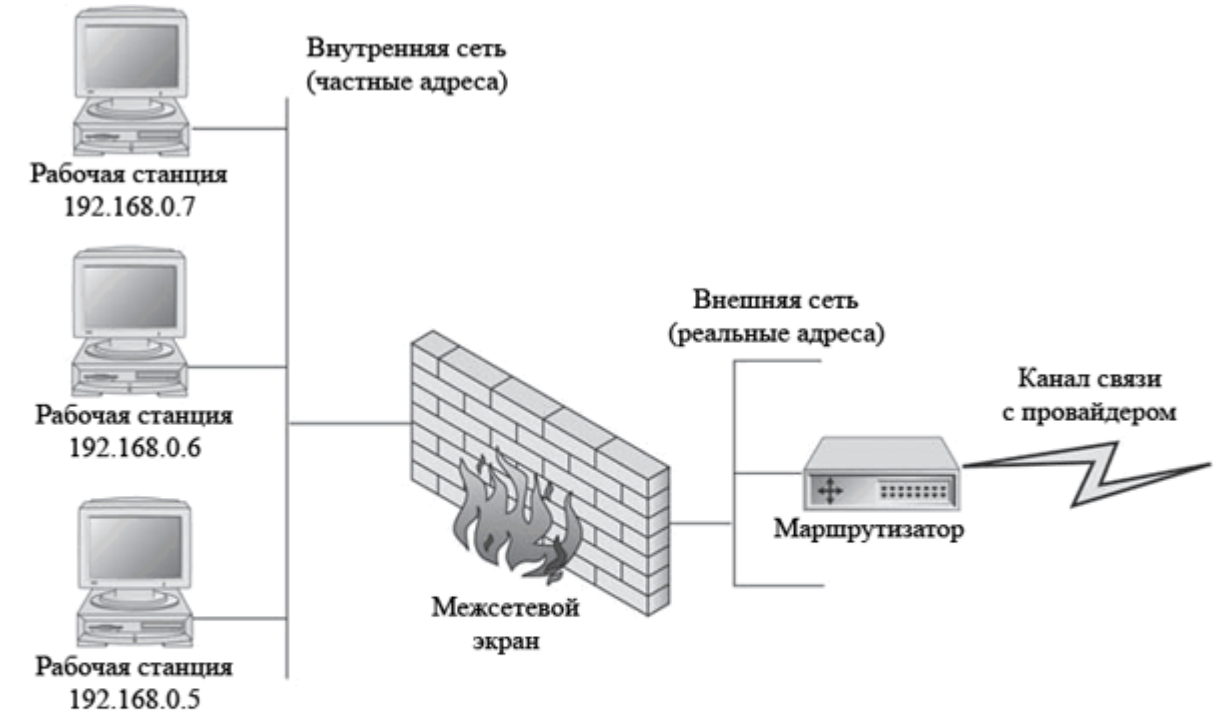


Основные сведения о NAT

- NAT (Network Address Translation) – служба маршрутизации, которая изменяет информацию заголовка ip – датаграмм перед пересылкой адресату.
- Данная служба позволяет подключаться к Интернету, совместно используя один или несколько общих зарегистрированных адресов на компьютере со службой NAT.
- Компьютер с NAT действует как преобразователь адресов.

Статическая трансляция адресов

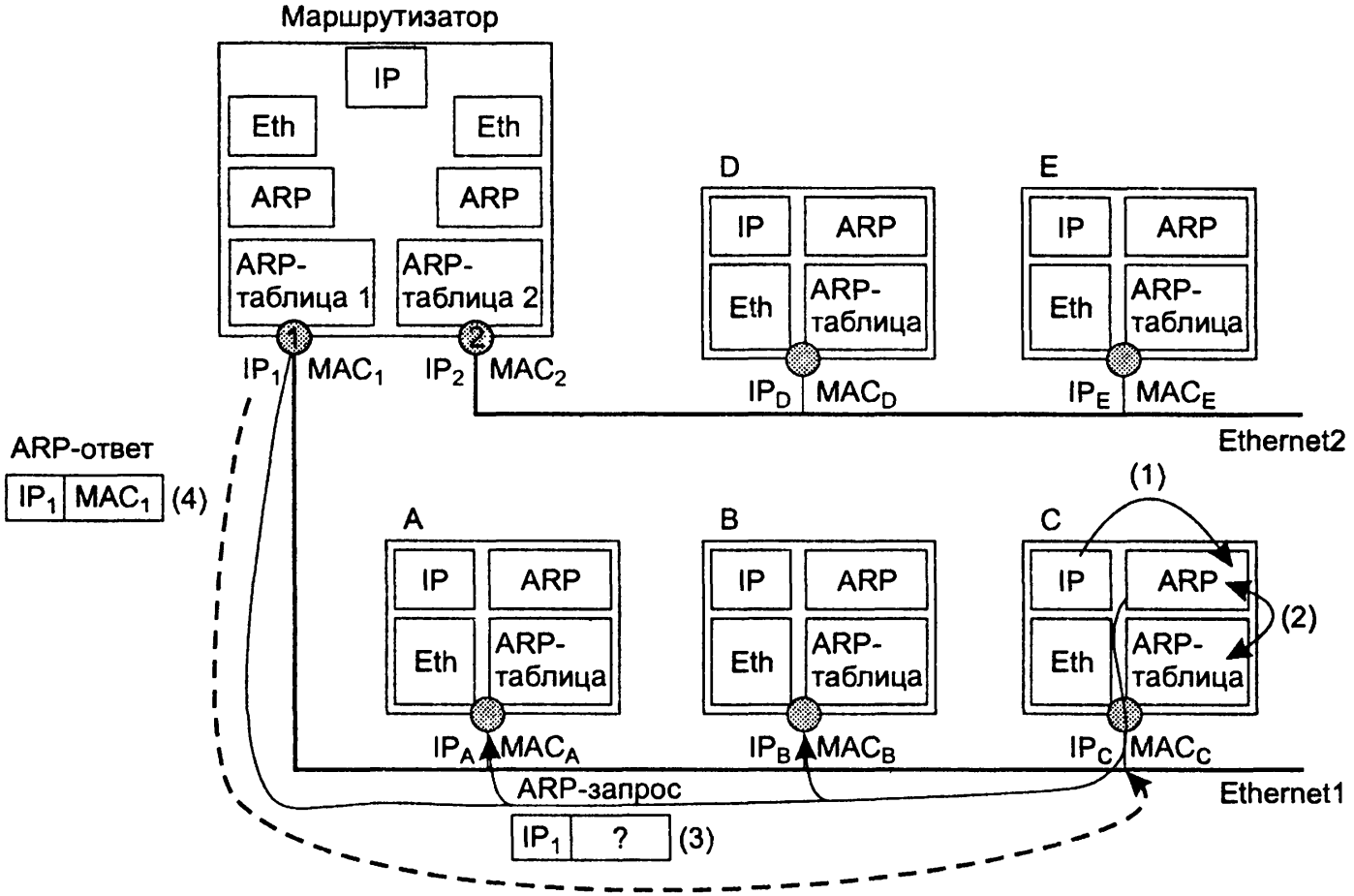
Динамическая трансляция адресов



Протокол разрешения адресов (ARP)

- Для определения локального адреса по IP-адресу используется **протокол разрешения адресов** (Address Resolution Protocol, ARP).
- Протокол разрешения адресов реализуется различным образом в зависимости от протокола локальной сети (Ethernet, Token Ring, FDDI) или глобальной сети.

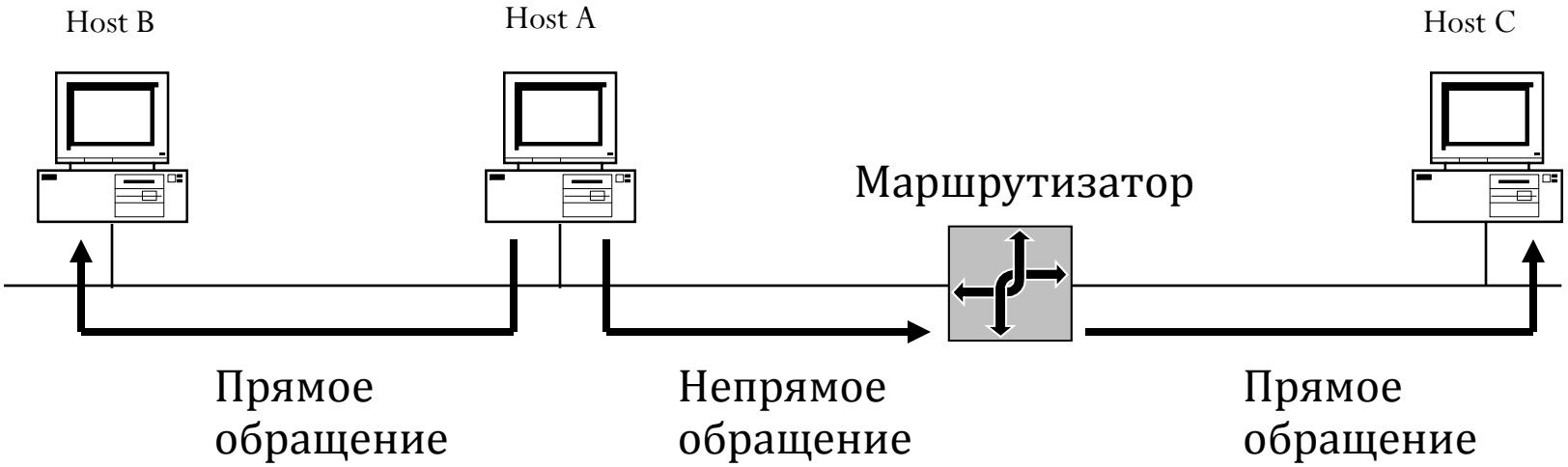
Схема работы протокола ARP



Протокол ICMP

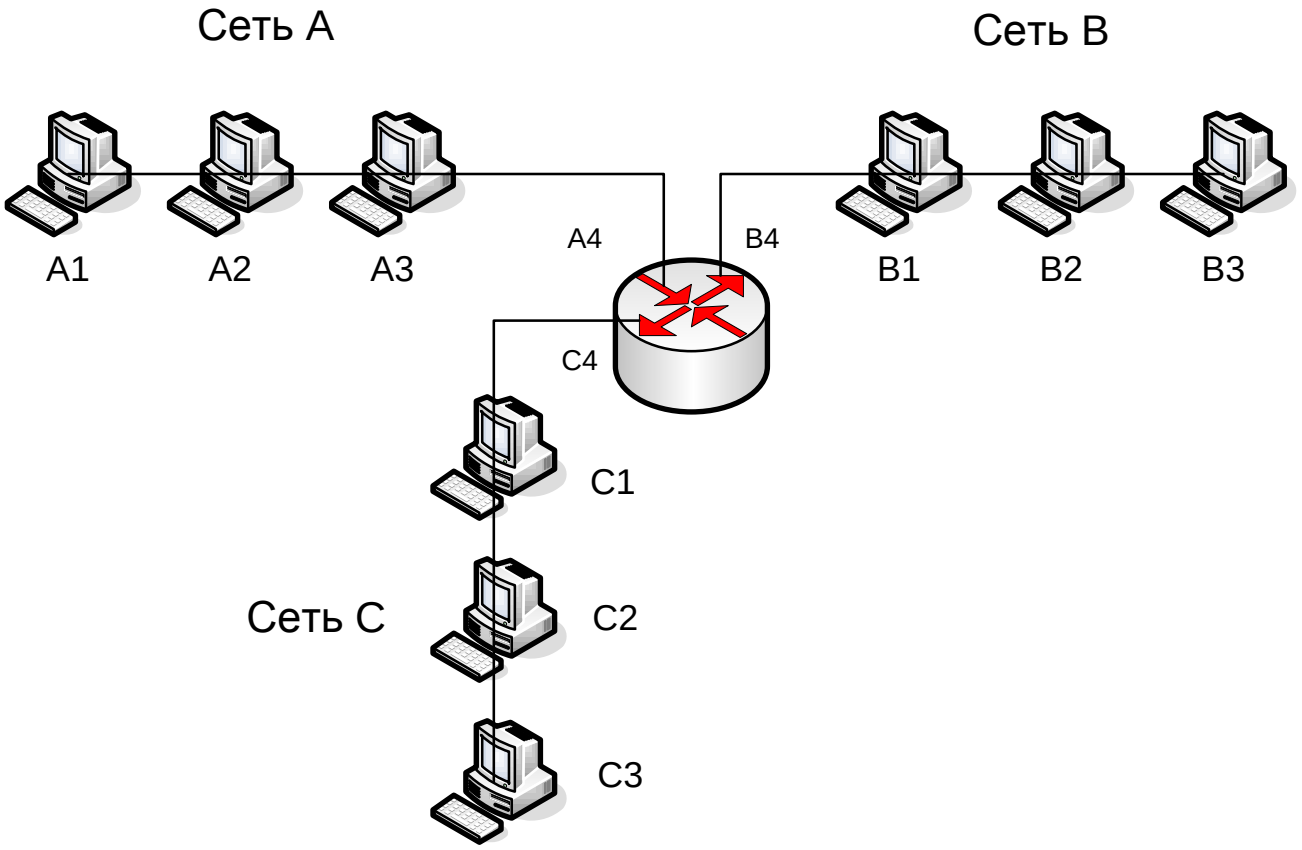
- Протокол передачи команд и сообщений об ошибках (ICMP) выполняет различные функции:
  - осуществляет передачу запросов и откликов;
  - контролирует время жизни дейтаграмм в системе;
  - реализует переадресацию пакета;
  - выдает сообщения о недостижимости адресата или о некорректности параметров;
  - формирует и пересылает временные метки;
  - выдает запросы и отклики для адресных масок и другую информацию.
- ICMP-протокол сообщает об ошибках в IP-дейтаграммах, но не дает информации об ошибках в самих ICMP-сообщениях.

Маршрутизация в IP-сетях



Объединение сетей

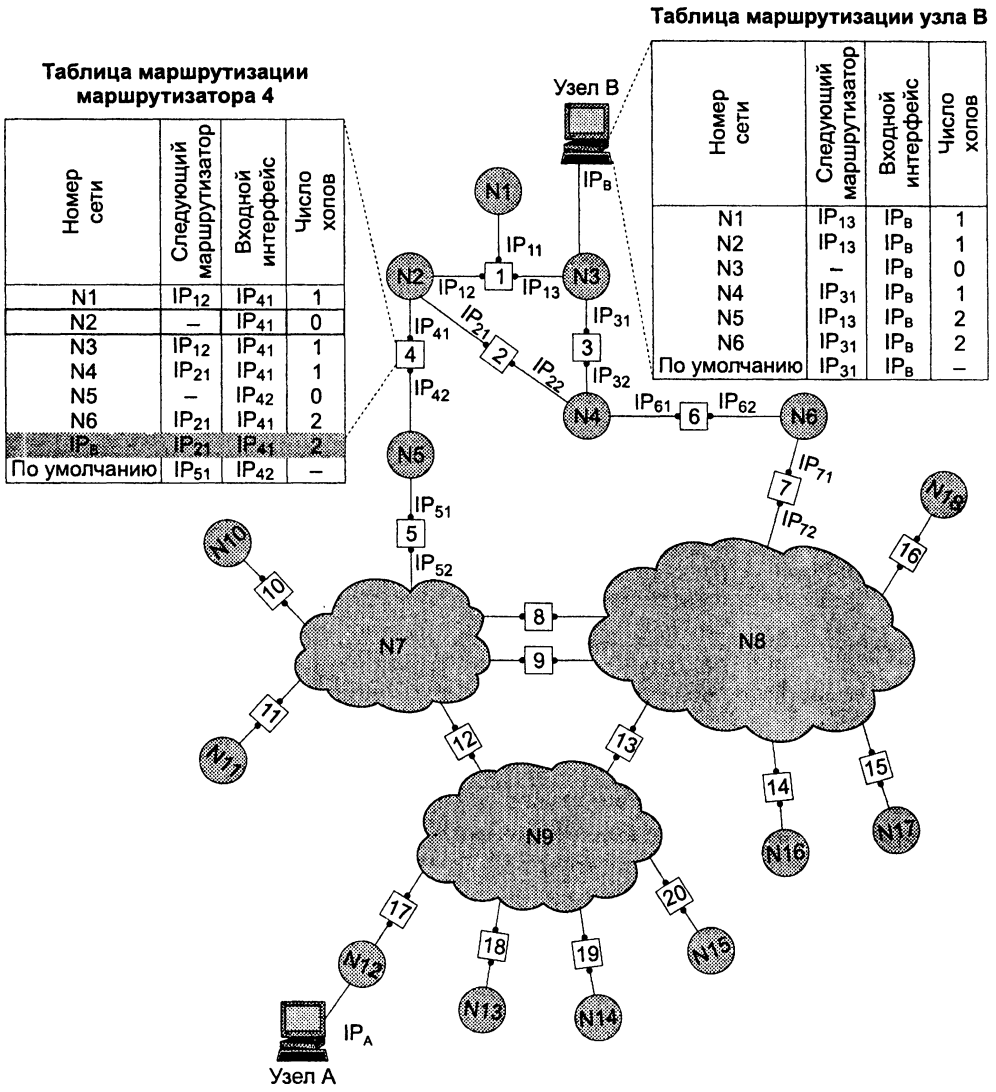
- Для успешной маршрутизации пакетов данных необходимо, чтобы каждая сеть имела уникальный номер. Эти номера записываются в заголовках пакетов сетевого уровня и анализируются маршрутизаторами для передачи пакетов из сети в сеть.



Маршрутизация в локальных сетях

- **Маршрутизация –** процесс пересылки данных между локальными вычислительными сетями (ЛВС). В отличие от мостов и коммутаторов, маршрутизатор принимает и пересылает пакеты данных, ориентируясь на программные адреса.
- В ip-сетях маршрутизация выполняется по таблицам ip-маршрутизации, которые существуют на всех хостах.
- IP - маршрутизаторы отличаются от хостов тем, что используют таблицы маршрутизации для пересылки трафика, полученного от других маршрутизаторов или хостов.

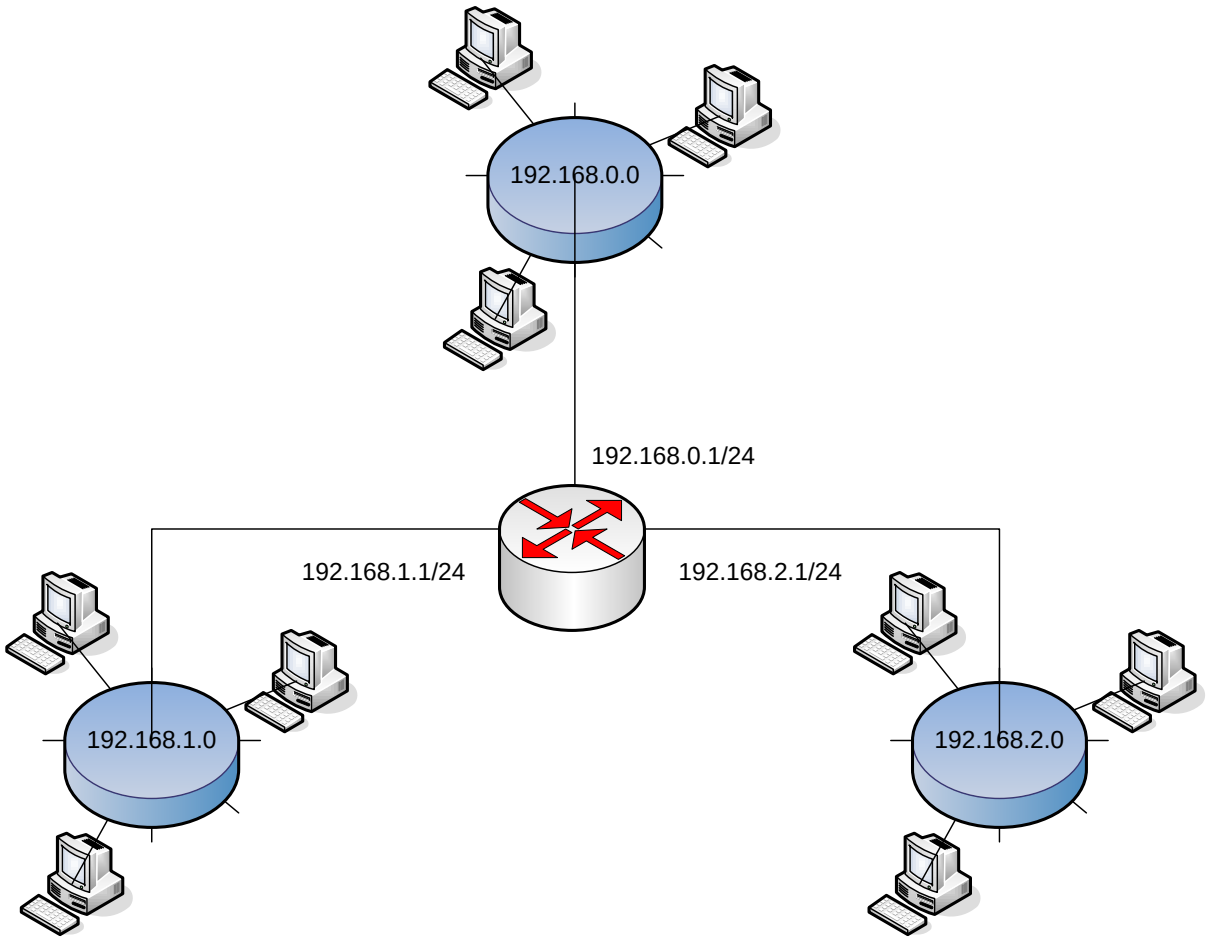
Пример маршрутизации в объединенной сети



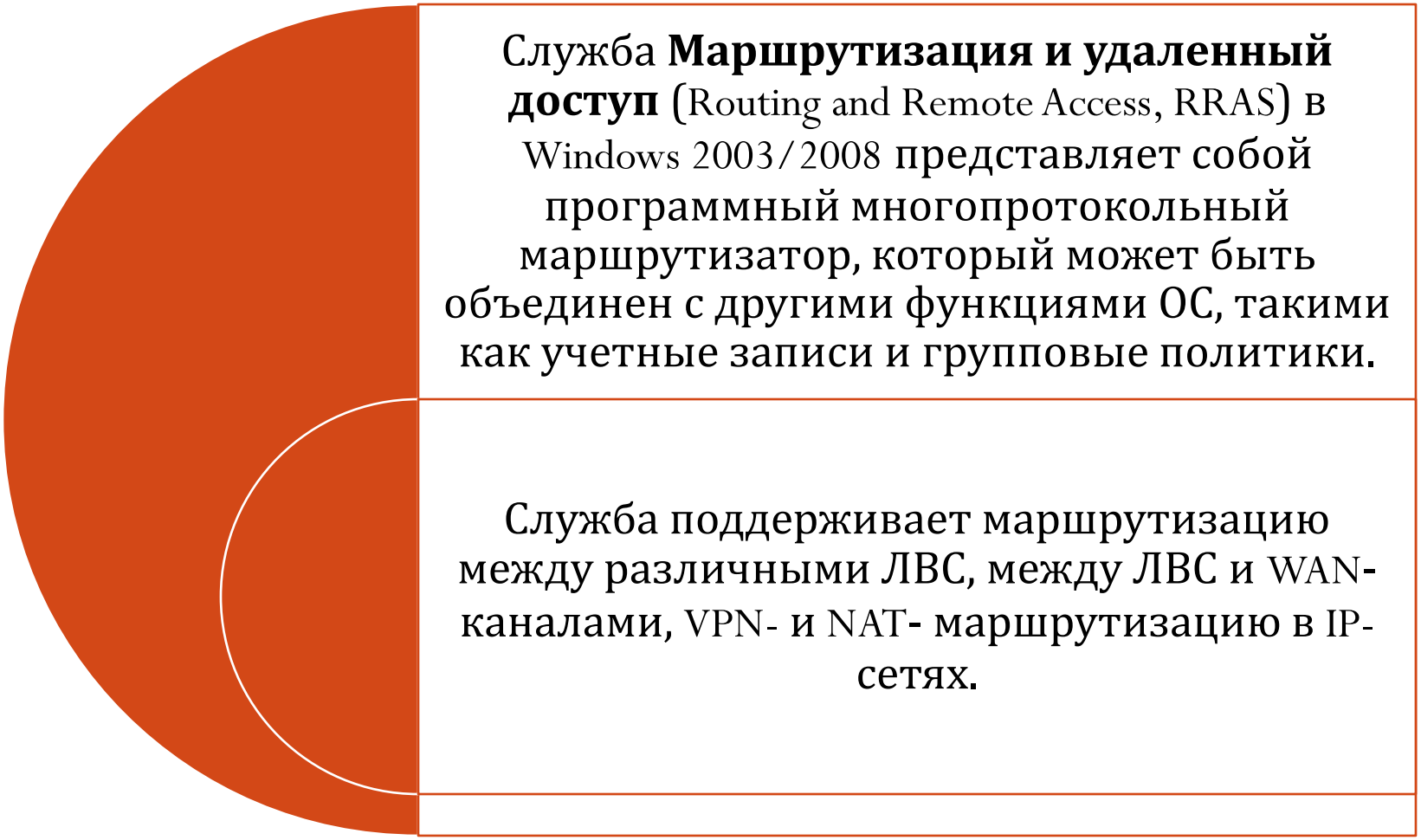
Команды управления таблицей маршрутизации Windows

- Вывод таблицы маршрутизации локального компьютера:
  - route print
- Добавление маршрута в таблицу маршрутизации:
  - route add *адрес_сети* mask *маска адрес_шлюза* metric *метрика*
- Удаление маршрута из таблицы маршрутизации
  - route delete *адрес_сети*

Локальные сети, объединенные маршрутизатором



Служба Маршрутизация и удаленный доступ

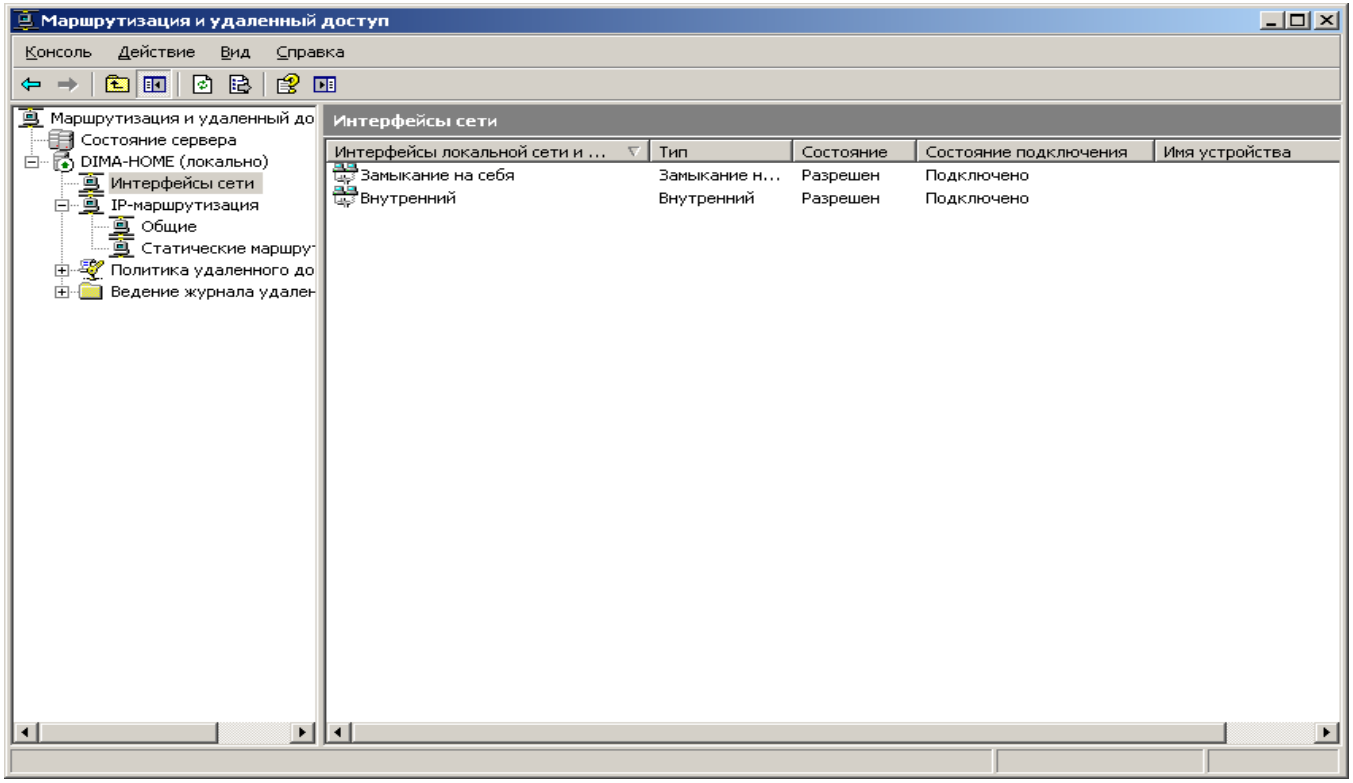


Служба **Маршрутизация и удаленный доступ** (Routing and Remote Access, RRAS) в Windows 2003/2008 представляет собой программный многопротокольный маршрутизатор, который может быть объединен с другими функциями ОС, такими как учетные записи и групповые политики.

Служба поддерживает маршрутизацию между различными ЛВС, между ЛВС и WAN-каналами, VPN- и NAT- маршрутизацию в IP-сетях.

Консоль управления Маршрутизация и удаленный доступ

- Консоль управления Маршрутизация и удаленный доступ представляет собой стандартную оснастку консоли управления в Windows.
- В конфигурации по умолчанию поддерживается маршрутизация в ЛВС.



Создание интерфейсов

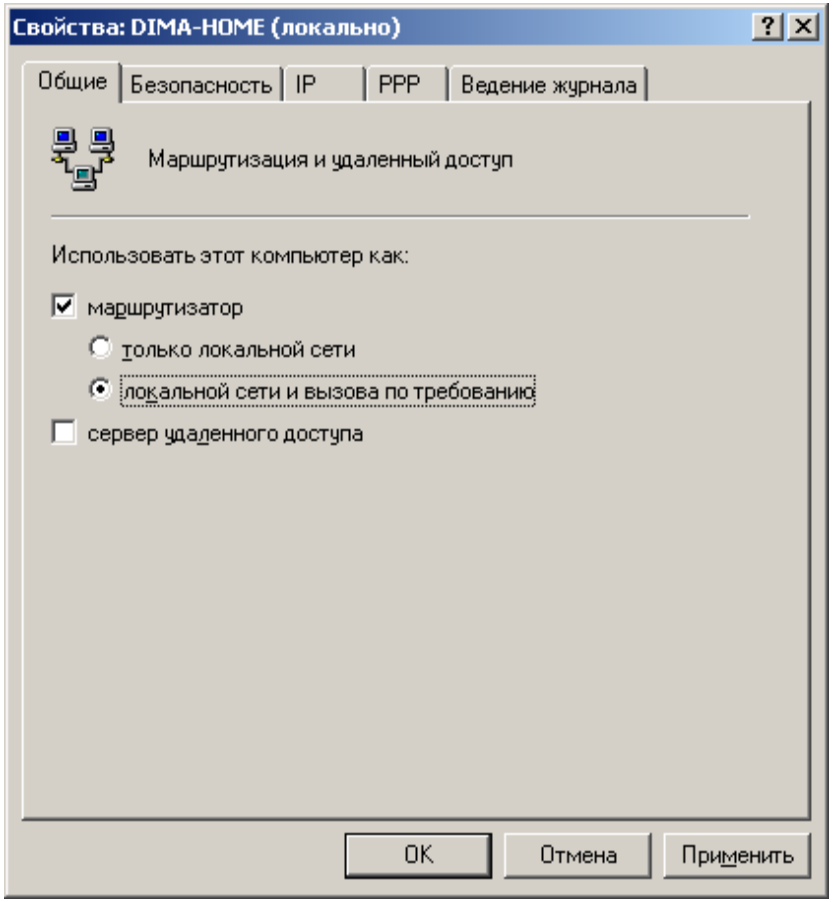
Сетевой интерфейс в консоли управления – программный компонент, подключаемый к физическому устройству (модему или сетевой плате).

В процессе настройки необходимо, чтобы все интерфейсы, через которые необходимо маршрутизировать трафик присутствовали в консоли управления.

Если необходимо сконфигурировать маршрутизацию через подключение по требованию или постоянное подключение по коммутируемой линии, VPN или PPOE-подключение (Point-to-Point Protocol over Ethernet), необходимо выполнить конфигурирование интерфейсов в ручную.

Создание интерфейсов по вызову

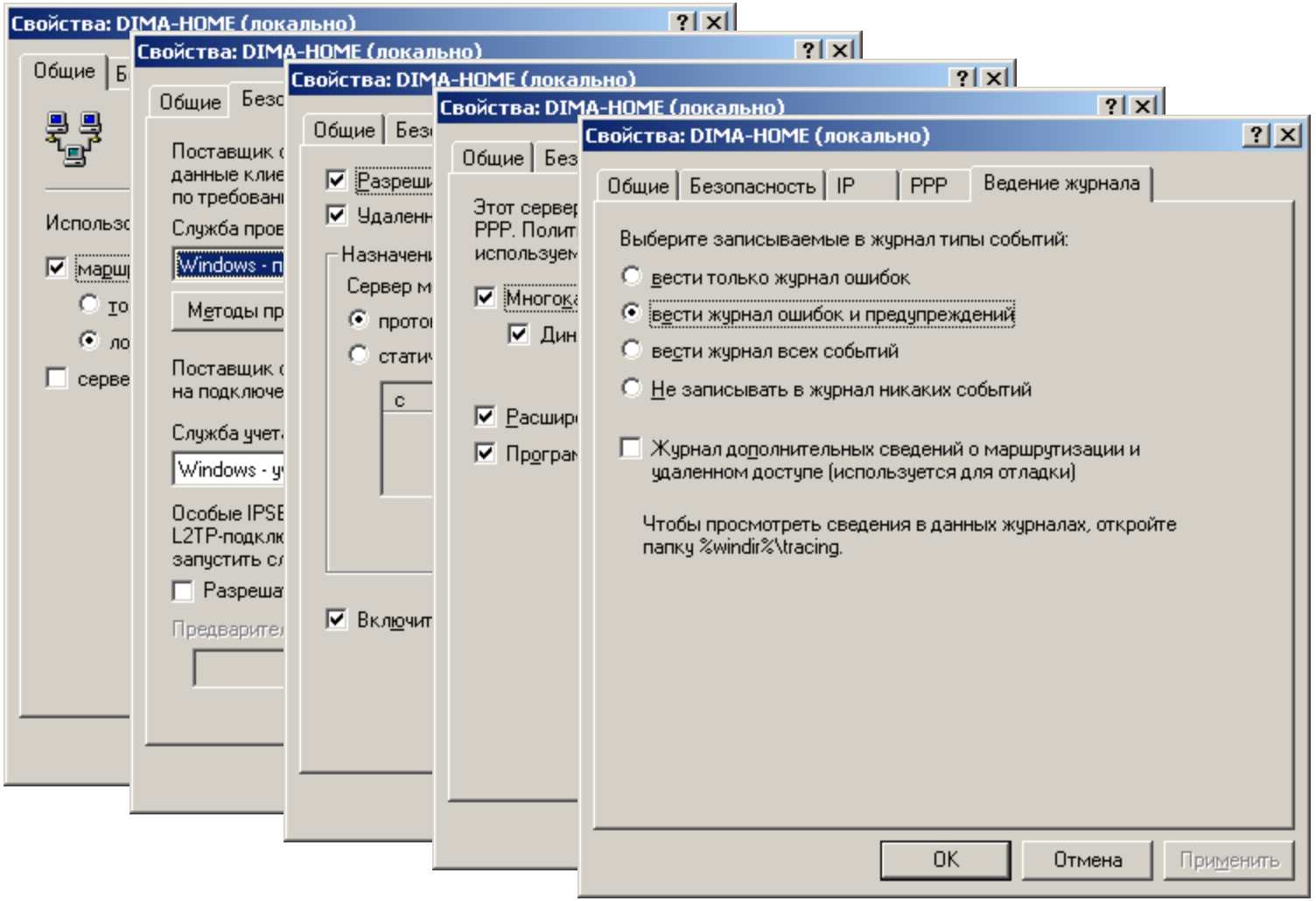
- Для создания интерфейса по вызову, необходимо включить такую возможность в Свойствах сервера маршрутизации.
- Для создания подключения используется Мастер интерфейса по требованию



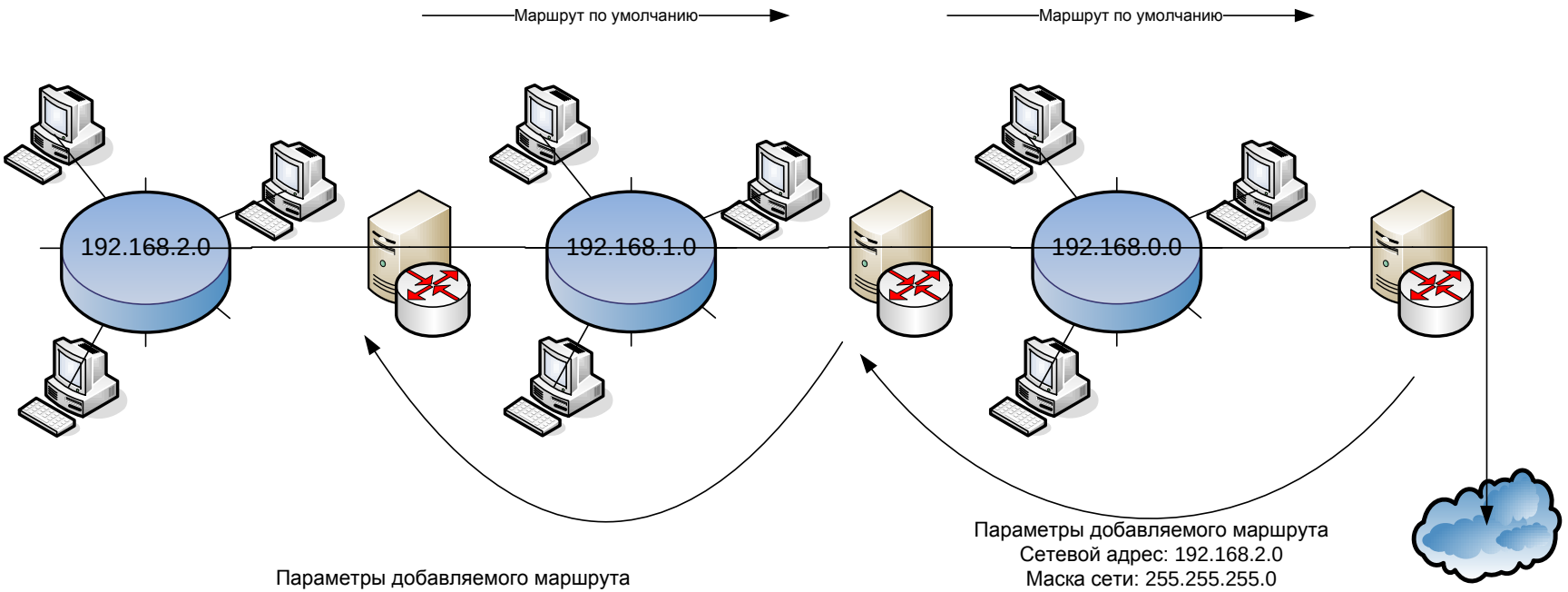
IP - маршрутизация

- Узел ip – маршрутизация используется дла настройки основных параметров по протоколу IP.
- По умолчанию содержится три подузла:
  - Общие
  - Статические маршруты
  - NAT / простой брандмауэр

Настройка параметров службы маршрутизации и удаленного доступа



Статическая маршрутизация



Настройка NAT

NAT позволяет выбрать любой частный адрес в качестве внутреннего адреса NAT – сервера, есть возможность отключить DHCP – сервер и DNS – прокси.

При настройке NAT для предоставления услуг DHCP внутренним клиентам можно задавать любые диапазоны адресов.

NAT позволяет сконфигурировать внешний совместно используемый интерфейс с одним или несколькими общими адресами. Множественные общие адреса могут быть использованы для задания внутренним серверам различные общие ip – адреса.

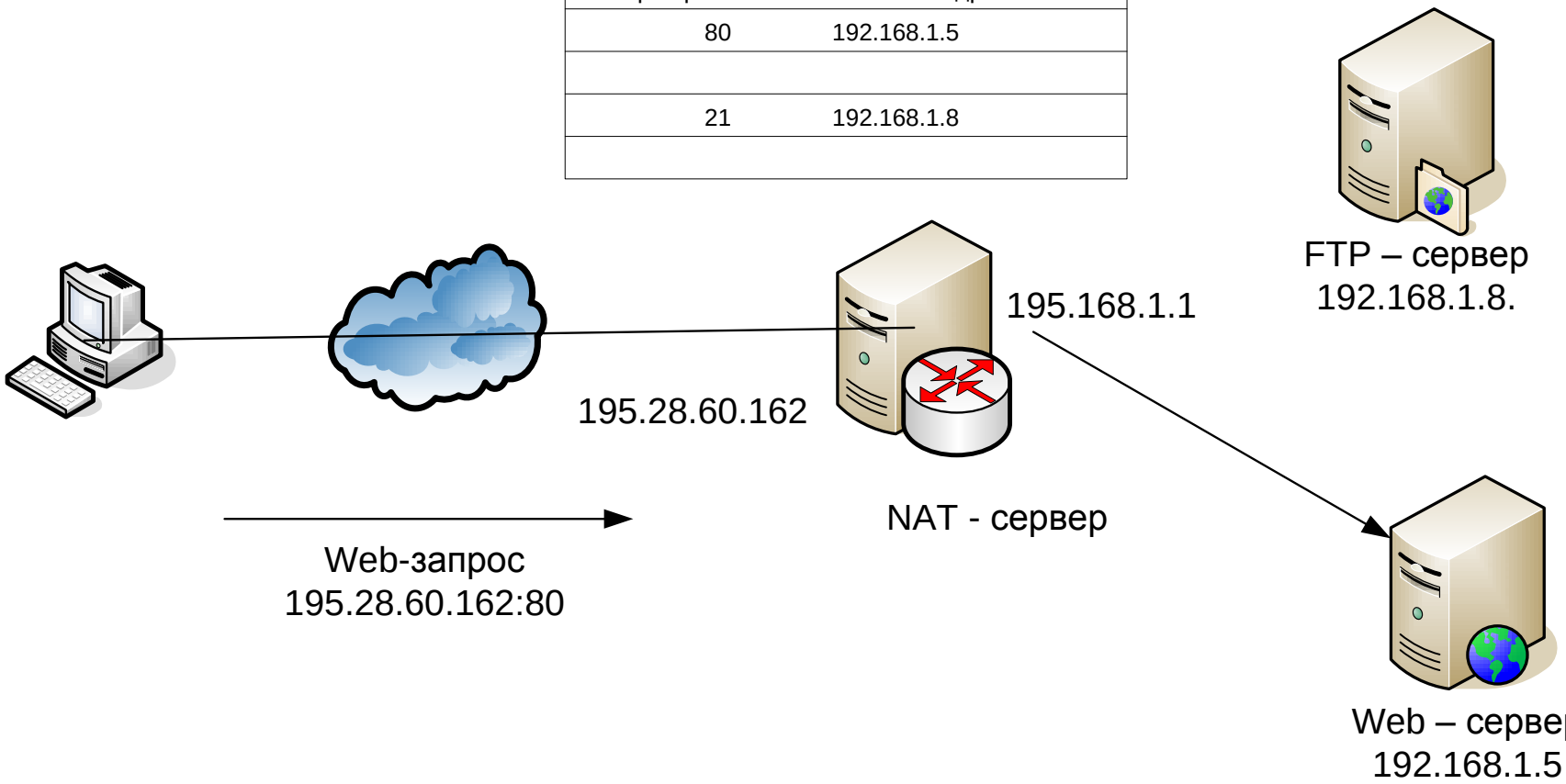
Специальные порты NAT

Специальные порты службы NAT используются для того, чтобы сопоставить внутреннюю службу (например web-, telnet-, ftp- сервер) внешнему интерфейсу компьютера с NAT.

Такое решение позволяет внешние запросы служб внутренней сети направлять на соответствующий компьютер.

Специальные порты NAT

Номер порта	Сопоставление адреса
80	192.168.1.5
21	192.168.1.8



Протоколы TCP/IP транспортного уровня

На транспортном уровне стека протоколов TCP/IP используется два протокола:

- Протокол управления передачей (**TCP**) – надежный протокол установления соединения. Он отвечает за разбиение сообщения на сегменты, их сборку, повторную отсылку всего того, что оказалось не полученным и сборку сообщений из сегментов.
  - Протокол TCP обеспечивает виртуальный канал между приложениями конечных пользователей.
- Протокол датаграмм пользователя (**UDP**) – протокол, не ориентированный на установление соединения.
  - Протокол отвечает за передачу сообщения но не содержит механизмов проверки доставки сообщения.

Некоторые номера портов стека TCP/IP

- Разработчики прикладного программного обеспечения договорились использовать широко известные номера портов, определенные в документе RFC 1700.
- Некоторые из зарезервированных портов приведены в таблице:

Десятичный номер	Ключевое слово	Описание
7	Echo	Эхо
21	ftp	Протокол FTP
23	telnet	Терминальное соединение
25	smtp	Протокол SMTP
53	domain	Сервер имен домена
69	tftp	Протокол TFTP
79	finger	Служба Finger
110	pop3	Протокол POP3
123	ntp	Протокол сетевого времени