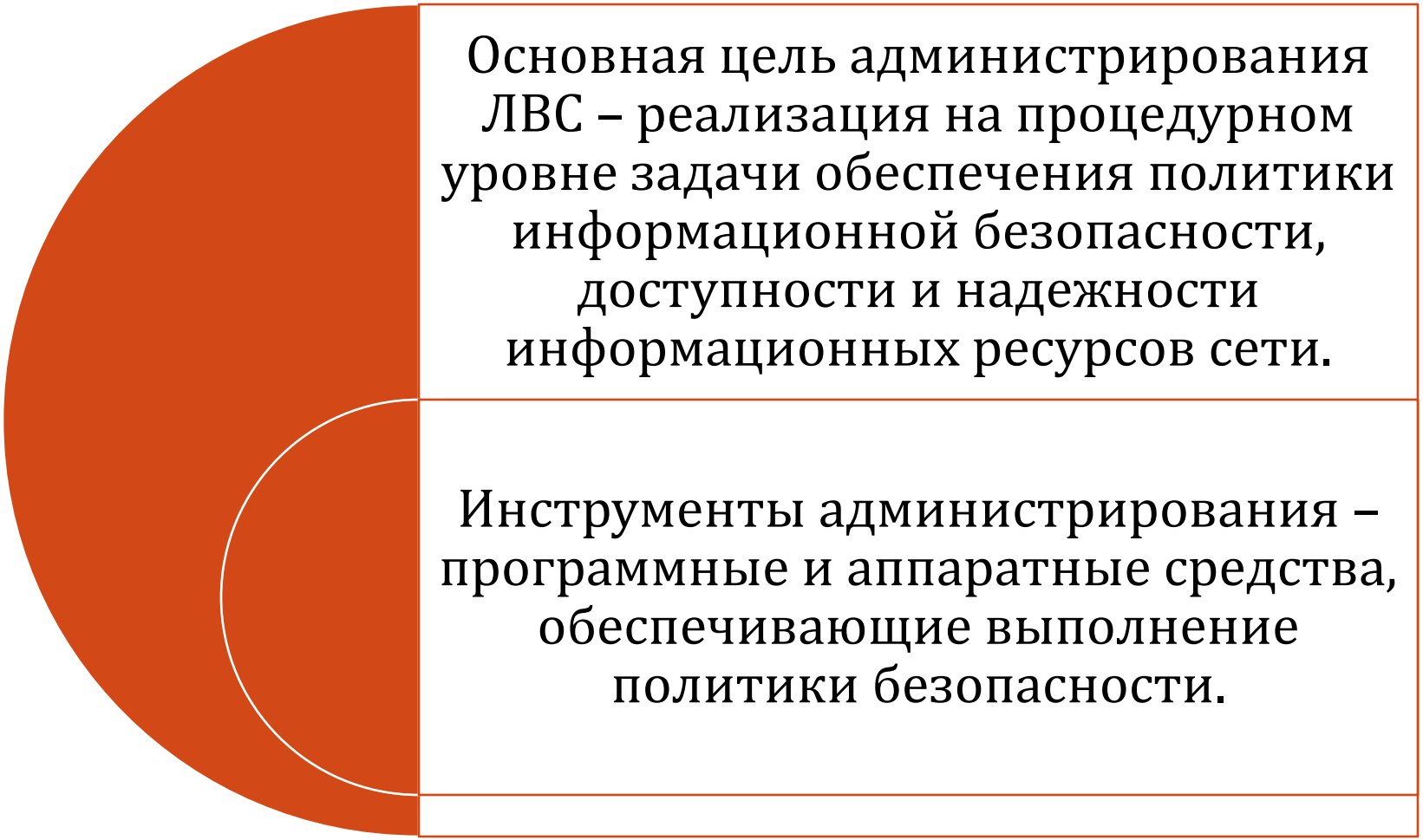
Администрирование локальных сетей

Лекция 7.

Организация доступа к сети

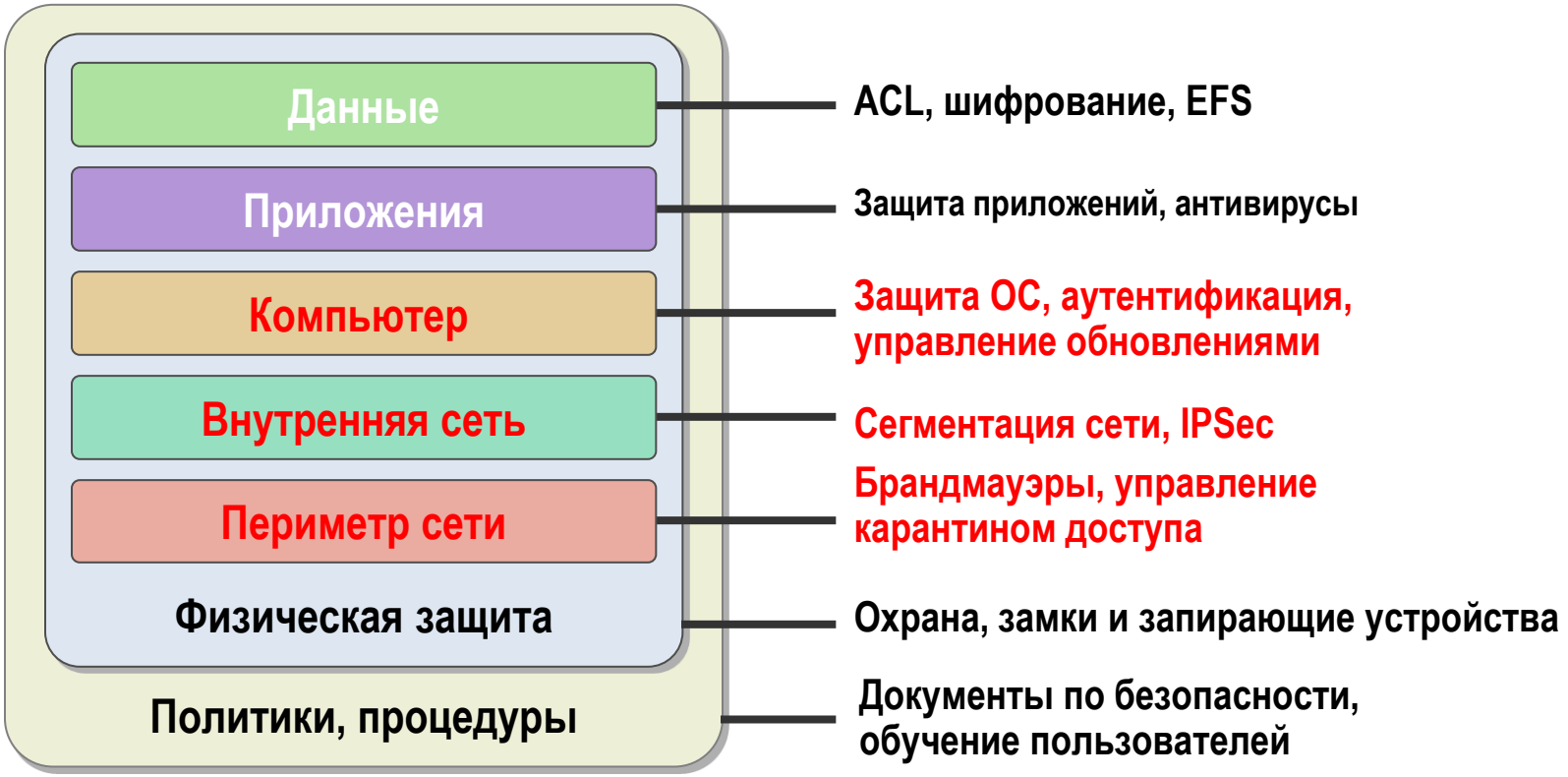
Задачи администрирования локальных сетей



Защита информационных ресурсов – Модель многослойной защиты

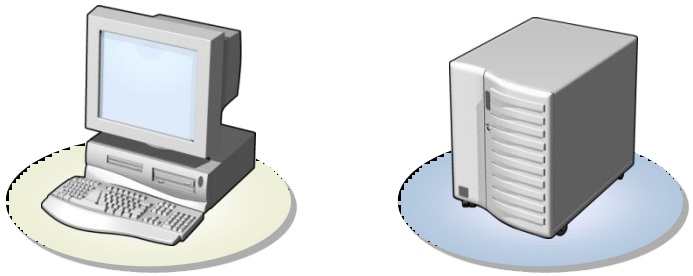
Использование многослойной модели защиты позволяет:

- **Уменьшить шанс успеха атаки**
- **Увеличить вероятность обнаружения атаки**



Описание уровня хоста

- Включает отдельные серверы и ПК пользователей сети
- Выполняют специальные серверные и клиентские роли в ИС
- Обеспечение ИБ хоста требует баланса между защищенностью и удобством работы пользователя



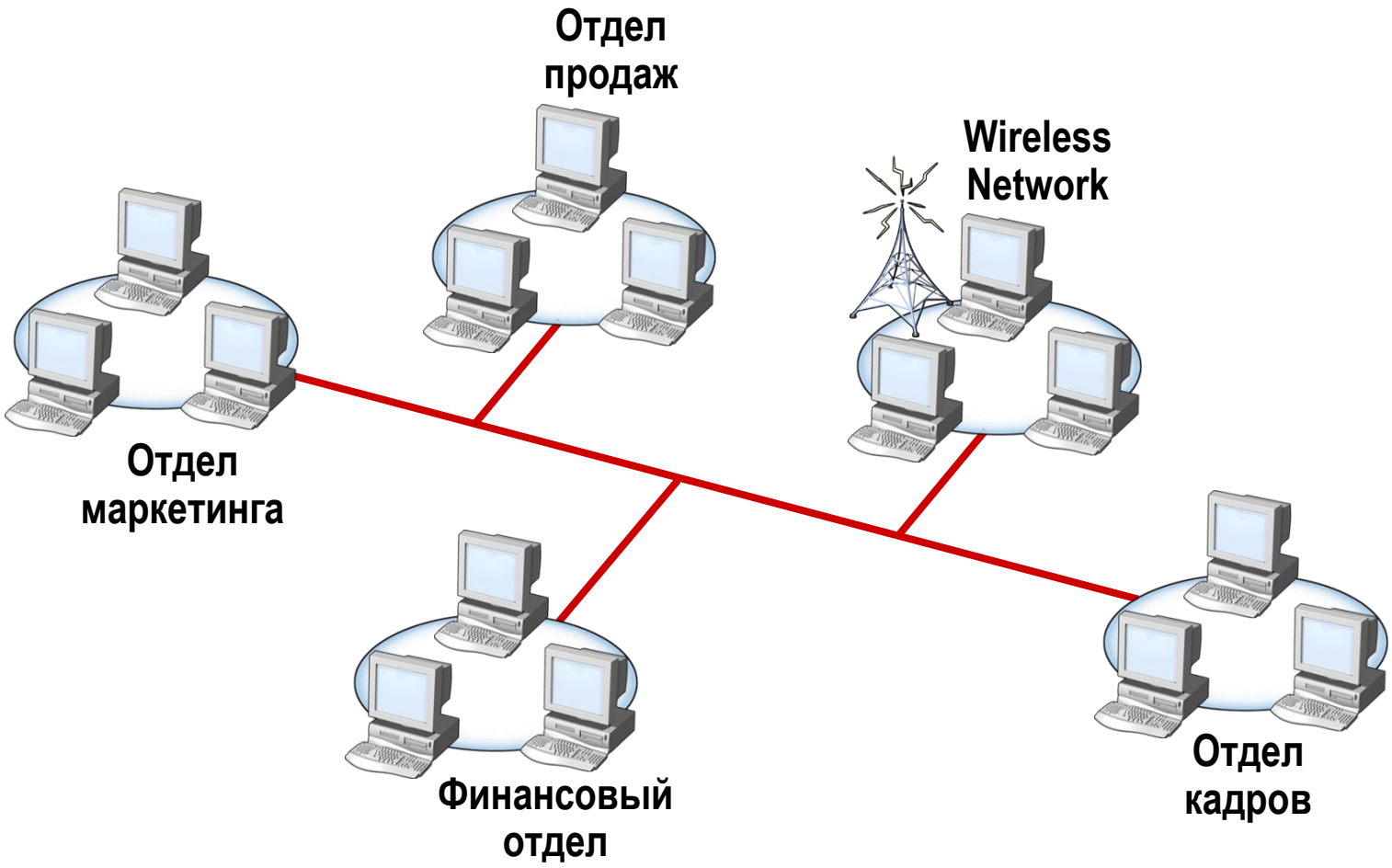
Уязвимости уровня хоста

Задачи администрирования – уровень хоста

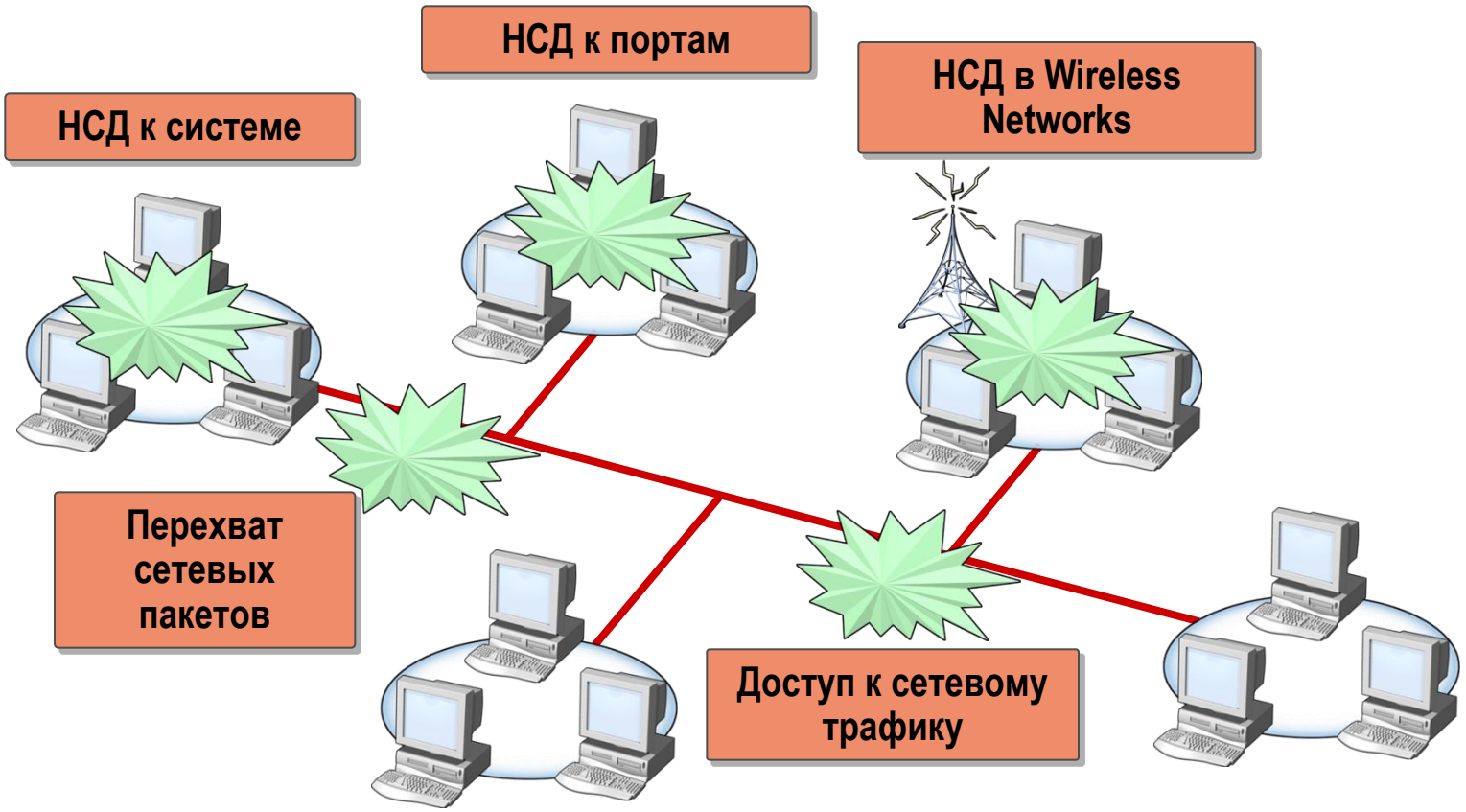
На уровне хоста основные задачи администрирования – определение прав пользователей на работу с компьютером (разграничение входа).

Определение ограничений на выполнение программ и приложений в вычислительной системе.

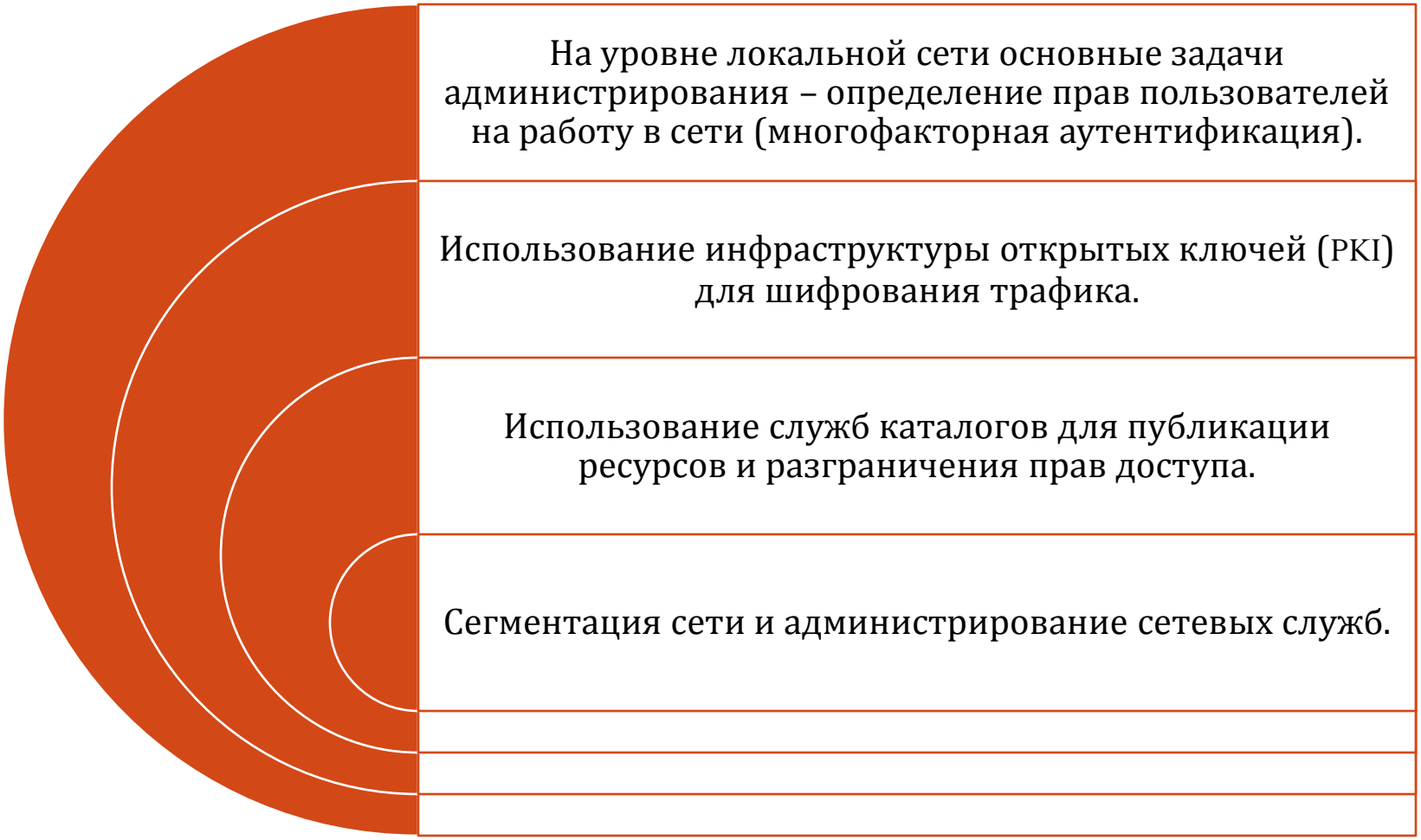
Описание уровня ЛВС



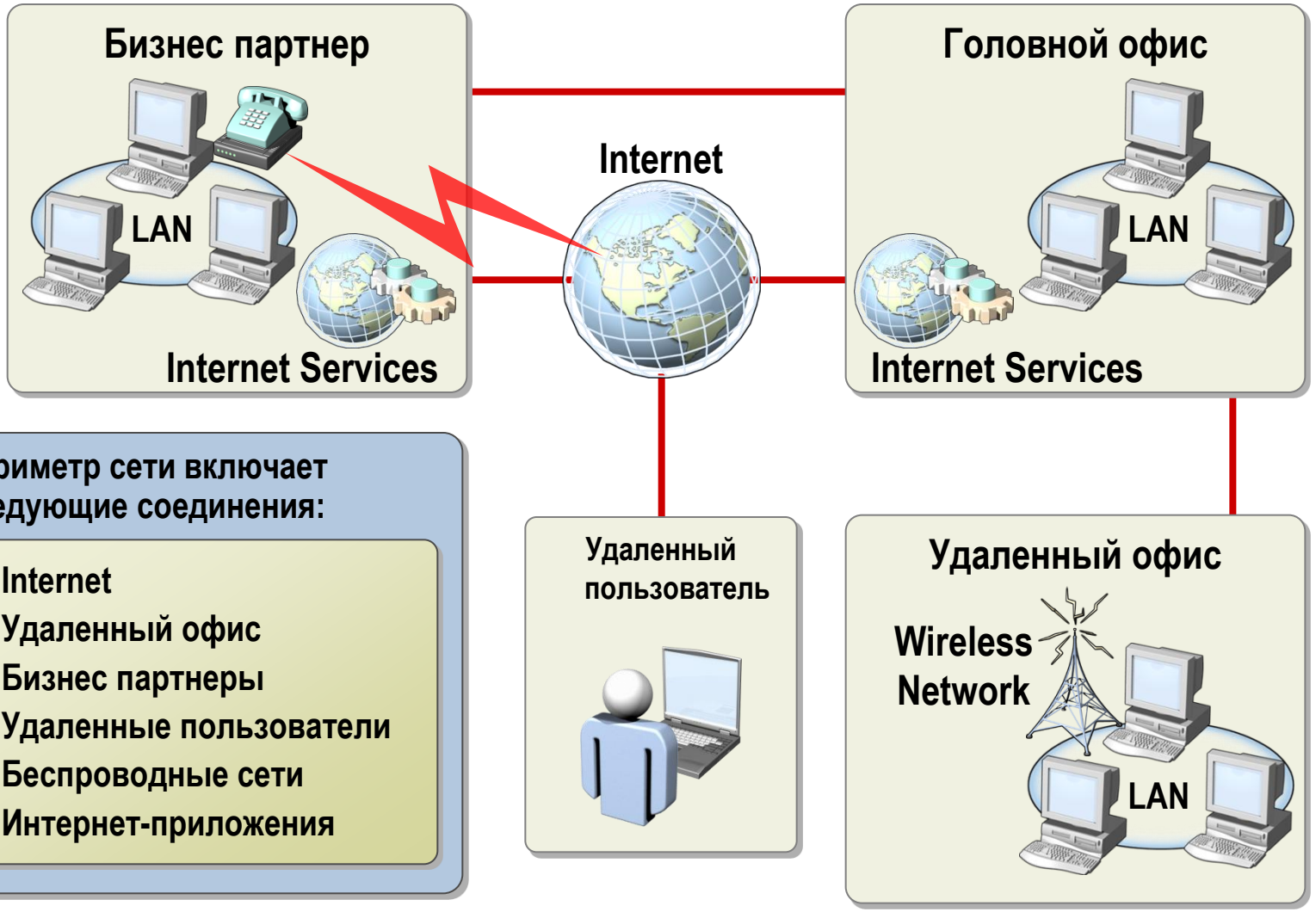
Нарушения уровня ЛВС



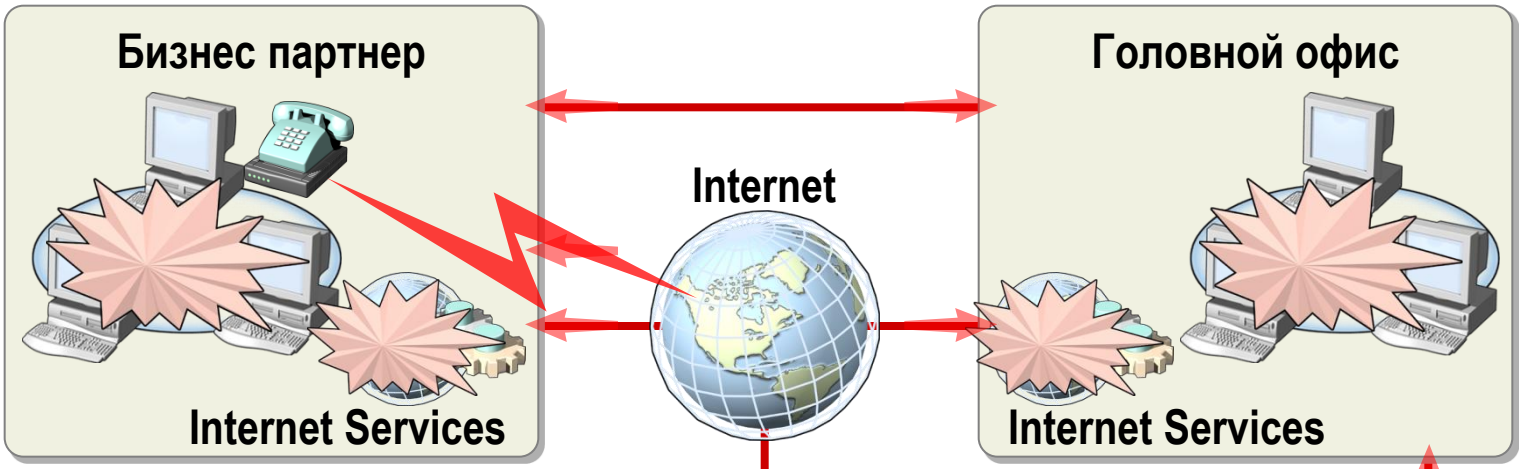
Задачи администрирования – уровень локальной сети



Описание уровня периметра сети



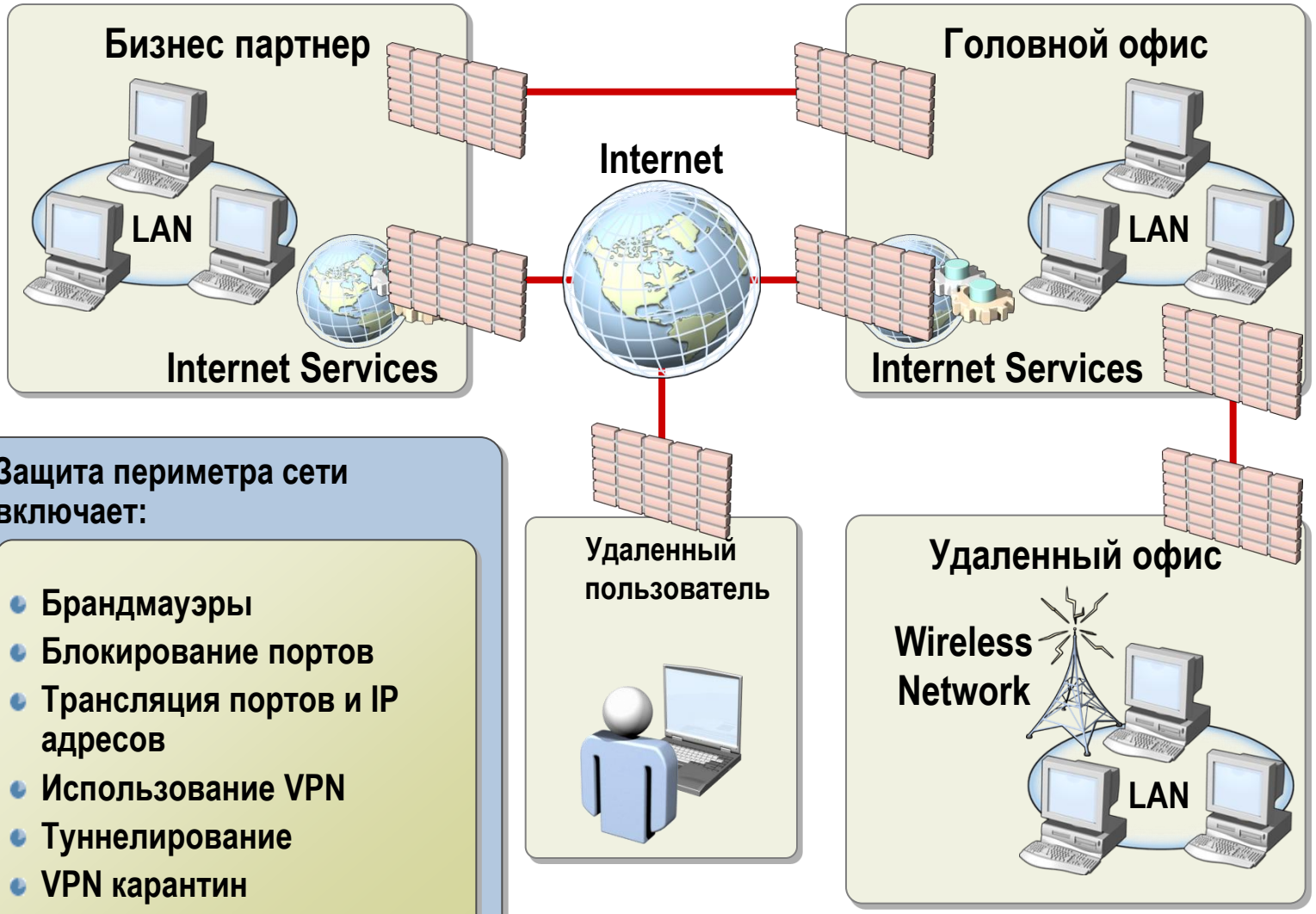
Угрозы на уровне периметра сети



Угрозы на уровне периметра сети включают:

- Атаки на ЛВС
- Атаки на комп. уд. пользователей
- Атаки со стороны сетей бизнес-партенров
- Атаки со стороны сетей уд. офиса
- Атаки на службы Интернет
- Атаки из Интернет

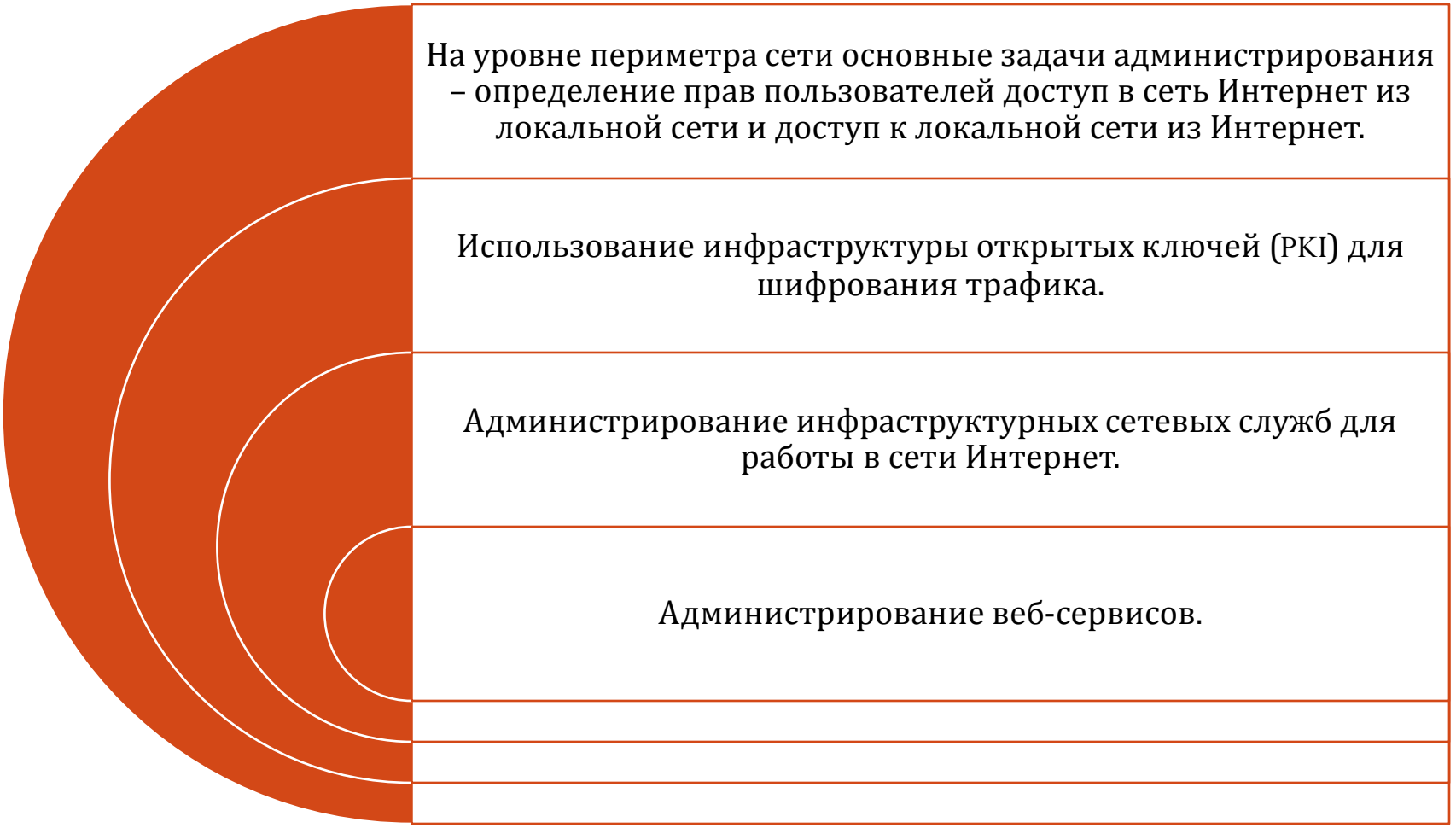
Защита на уровне периметра сети



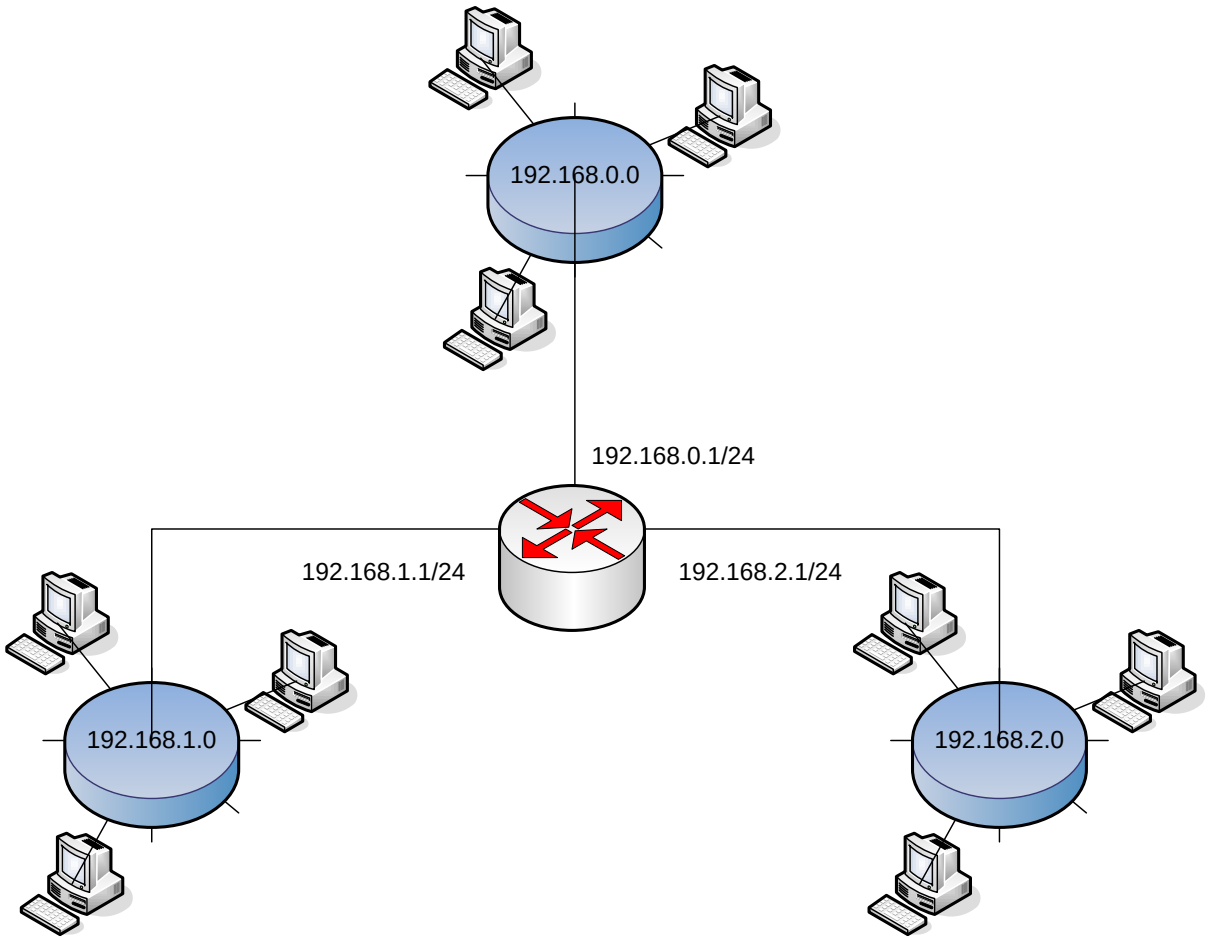
Защита периметра сети включает:

- Брандмауэры
- Блокирование портов
- Трансляция портов и IP адресов
- Использование VPN
- Туннелирование
- VPN карантин

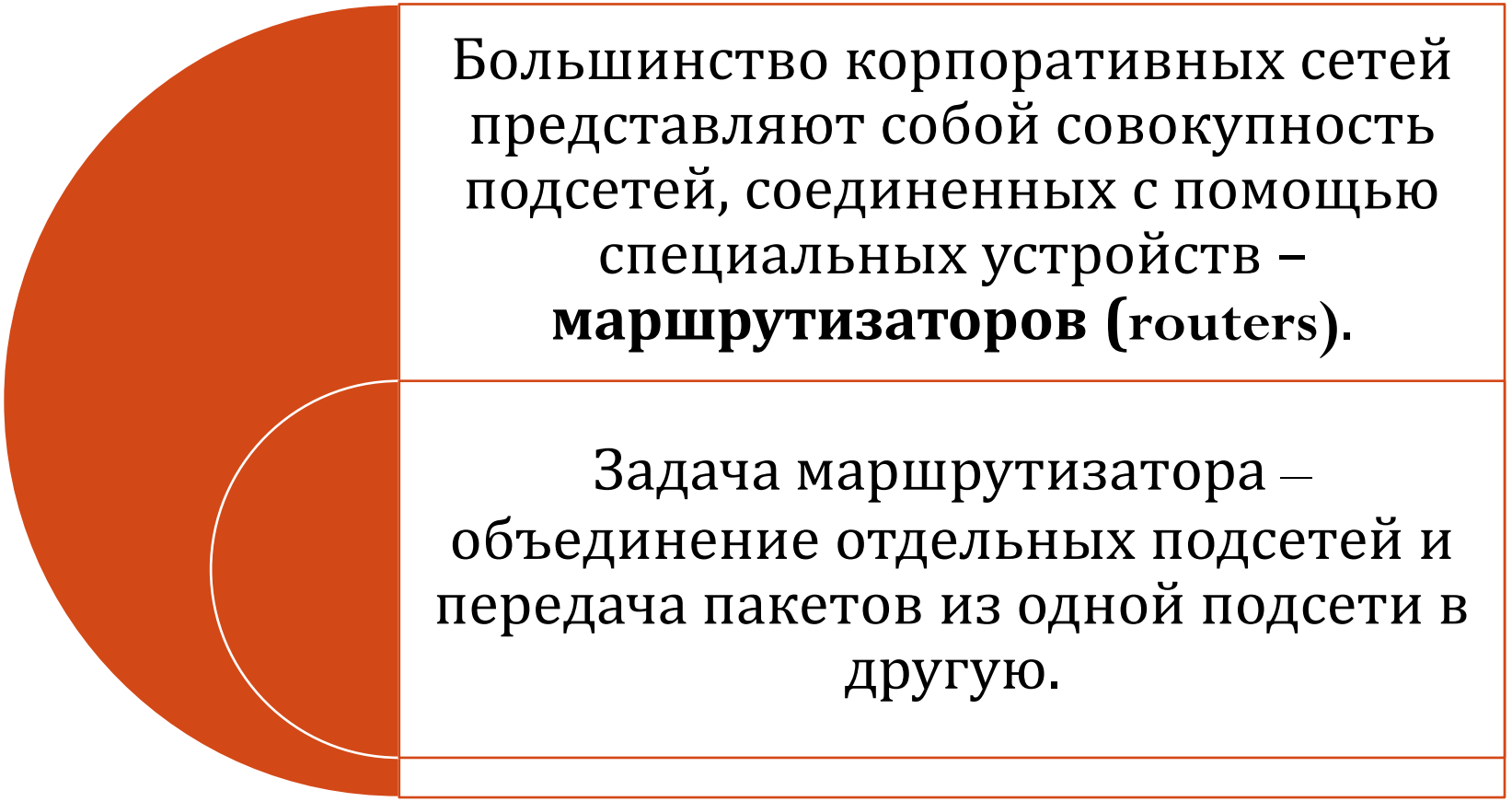
Задачи администрирования – уровень периметра сети



Локальные сети, объединенные маршрутизатором

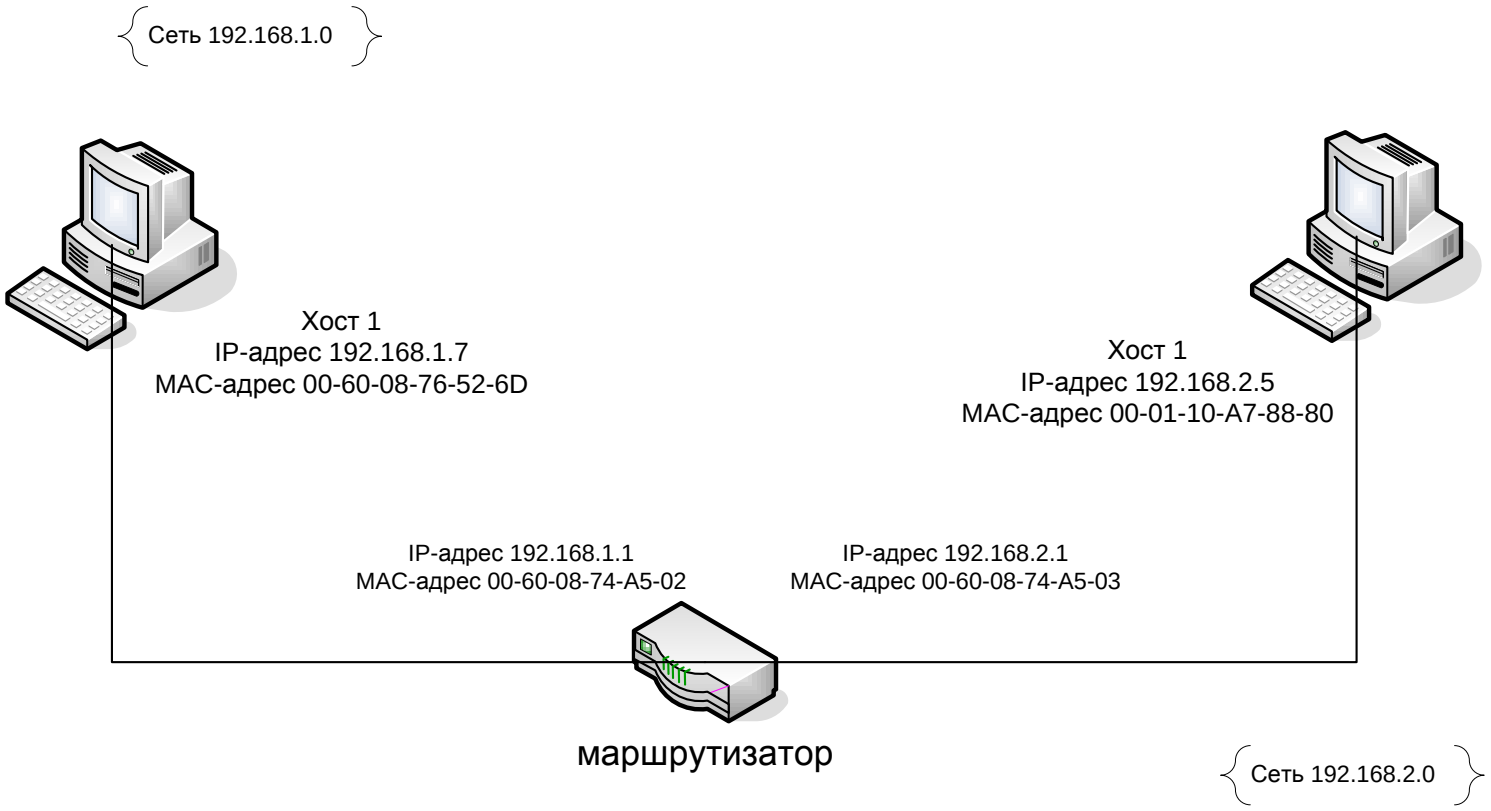


Маршрутизация сетей



Принцип маршрутизации в сетях TCP/IP

- Процесс взаимодействия хостов в двух смежных сетях имеет следующий вид:



Пример маршрутизации в сетях TCP/IP

При отправке пакета от хоста A (192.168.1.7) хосту B (192.168.2.5) компоненты протокола TCP/IP определяют, что хост B расположен в другой сети. Пакет отправляется маршрутизатору по умолчанию (default gateway).

В заголовок пакета включается IP-адрес получателя и MAC-адрес маршрутизатора

- IP-адрес отправителя: 192.168.1.7
- MAC-адрес отправителя: 00-60-80-76-52-6B
- IP-адрес получателя: 192.168.2.5
- MAC-адрес получателя: 00-60-08-74-A5-02

Маршрутизатор анализирует пакет и на основе IP-адреса понимает, что пакет должен быть передан. Маршрутизатор имеет **таблицу маршрутизации** – таблицу ссылок, включающую сетевую информацию и следующий маршрутизатор в линии для конкретного пути.

Заголовок сообщения имеет вид:

- IP-адрес отправителя: 192.168.1.7
- MAC-адрес отправителя: 00-60-08-74-A5-03
- IP-адрес получателя: 192.168.2.5
- MAC-адрес получателя: 00-01-10-A7-88-80

Адресат получив пакет по IP-адресу в заголовке понимает, кто был отправителем сообщения. MAC-адрес указывает, что пакет пришел от маршрутизатора.

Процесс передачи сообщения через маршрутизатор в терминологии TCP/IP называет прыжком (hop).

Построение таблиц маршрутизации

Для выполнения маршрутизации должны быть настроены таблицы маршрутизации – совокупность записей, определяющих интерфейс используемый для доставки пакета.

Существует типа записей:

- **записи, определяющие маршрут к одиночному хосту;**
- **записи, определяющие маршрут к подсети;**
- **записи, определяющие маршрут, используемый по умолчанию.**

Структура таблицы маршрутизации

Записи в таблице маршрутизации имеют пять полей:

- **Адрес назначения;**
- **Маска подсети;**
- **Адрес маршрутизатора;**
- **Адрес интерфейса;**
- **Метрика.**

Пример таблицы маршрутизации

Для вывода таблиц маршрутизации используются команды:

netstat –r

route print

IPv4 таблица маршрута

```
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 0e 0c 4d 4a 57 ...... Intel(R) PRO/100 M Network Connection
0x10004 ...00 0e 0c 4d 4a 56 ...... Intel(R) PRO/1000 CT Network Connection
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес         Маска сети      Адрес шлюза       Интерфейс       Метрика
          0.0.0.0          0.0.0.0    192.168.163.1  192.168.163.115         20
          0.0.0.0          0.0.0.0    212.30.160.1   212.30.160.10   20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1         1
  192.168.163.0    255.255.255.0  192.168.163.115  192.168.163.115         20
 192.168.163.115  255.255.255.255  127.0.0.1       127.0.0.1         20
 192.168.163.255  255.255.255.255  192.168.163.115  192.168.163.115         20
   212.30.160.0    255.255.255.0    212.30.160.10   212.30.160.10   20
  212.30.160.10  255.255.255.255    127.0.0.1       127.0.0.1         20
 212.30.160.255  255.255.255.255    212.30.160.10   212.30.160.10   20
      224.0.0.0        240.0.0.0        192.168.163.115       192.168.163.115         20
      224.0.0.0        240.0.0.0        212.30.160.10   212.30.160.10   20
 255.255.255.255  255.255.255.255  192.168.163.115  192.168.163.115         1
 255.255.255.255  255.255.255.255    212.30.160.10   212.30.160.10   1
Основной шлюз:       212.30.160.1
```

Среда со статической маршрутизацией

- Среда со статической IP-маршрутизацией подходит для небольших статических объединенных IP-сетей с единственными путями.
  - Под термином «небольшая объединенная сеть» понимается сеть, содержащая от 2 до 10 сетей.
  - Термин «сеть с единственными путями» означает, что передача пакетов между любыми двумя конечными точками объединенной сети возможна только по одному маршруту.
  - Термином «статическая сеть» называются сети, топология которых со временем не меняется.
- Среды со статической маршрутизацией могут использоваться в следующих случаях.
  - Малый бизнес.
  - Небольшая офисная объединенная IP-сеть.
  - Единственная сеть офиса подразделения.

Недостатки статической маршрутизации

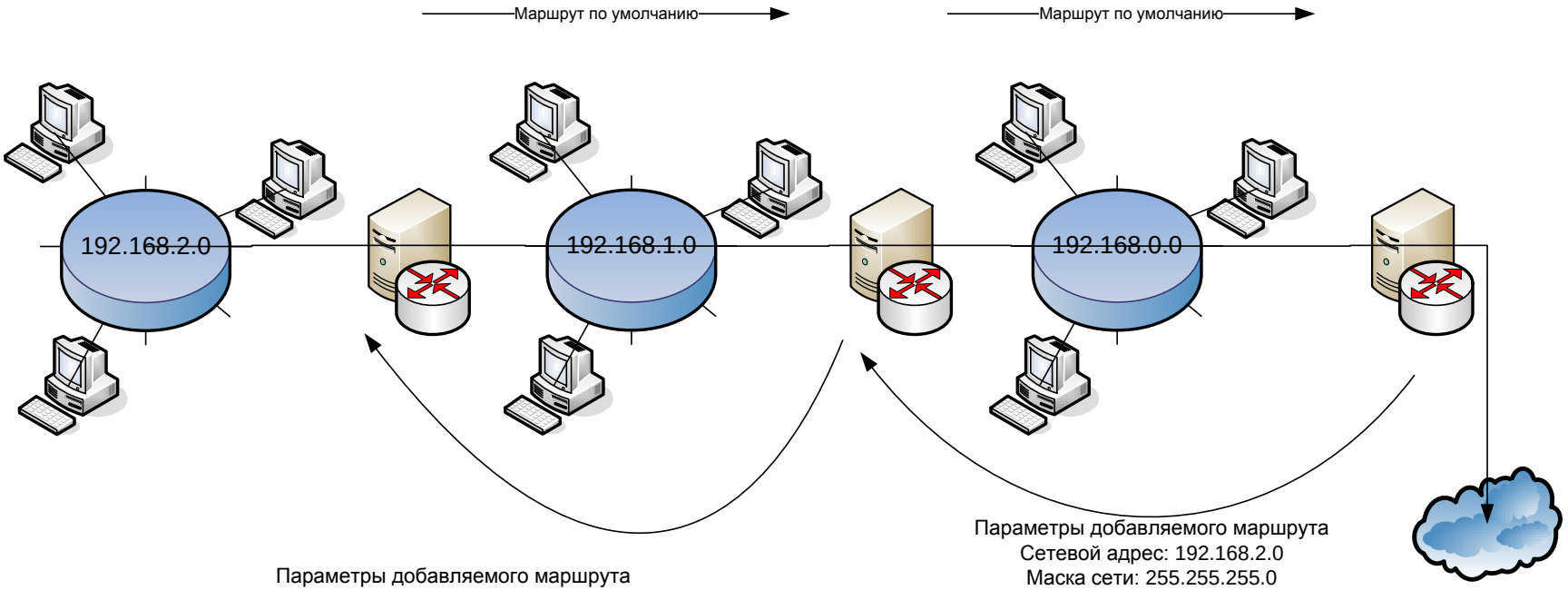
Отсутствие отказоустойчивости

- Если маршрутизатор или канал связи перестают функционировать, статические маршрутизаторы не обнаруживают сбой и не информируют о нем другие маршрутизаторы.
- Эта проблема существенна для больших объединенных сетей организаций;
- Офисные сети (с двумя маршрутизаторами и тремя локальными сетями) испытывают такие трудности.

Затраты на администрирование

- Если в объединенной сети добавляется или удаляется одна из сетей, маршруты к этой сети должны быть добавлены или удалены вручную.
- При добавлении нового маршрутизатора на нем нужно правильно настроить все необходимые маршруты.

Пример статической маршрутизации



Динамическое построение таблицы маршрутизации

- Для обеспечения оперативности изменения таблицы маршрутизации используют методы автоматизации построения таблиц маршрутизации и их обновления.
- Протоколы маршрутизации задают способ обмена специальными сообщениями между маршрутизаторами.
- Существует две категории протоколов:
  - Протоколы маршрутизации, основанные на обмене таблицами маршрутизации;
  - Протоколы, основанные на обмене изменениями в таблицах маршрутизации.
- В Windows Server включена поддержка протоколов маршрутизации:
  - Routing Internet Protocol (RIP);
  - Open Shortest Path First (OSPF).

Трансляция сетевых адресов

- Особенность интеграции корпоративной сети в Интернет является тот факт, что для установки соединения необходимо, чтобы каждый компьютер имел собственный сетевой адрес.
- Пул IP-адресов, выделенных провайдером, как правило, ограничен.
- Имеется механизм **трансляции сетевых адресов (Network Address Translator, NAT),** предполагающий использование непубличных (частных адресов).
- Для их использования выделены следующие диапазоны:
  - 10.0.0.0 с маской подсети 255.0.0.0;
  - 172.16.0.0 с маской подсети 255.240.0.0
  - 192.168.0.0 с маской подсети 255.255.0.0

Основные сведения о NAT

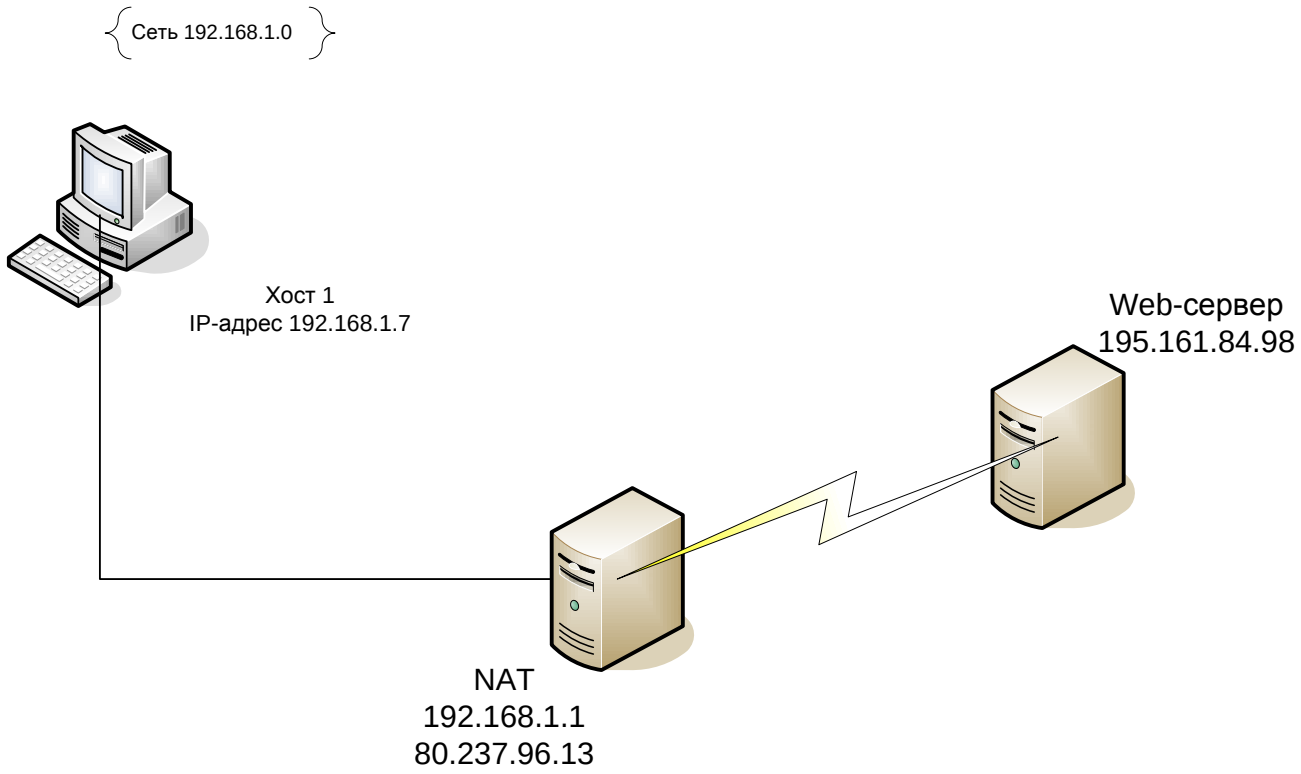
NAT – служба маршрутизации, которая изменяет информацию заголовка ip – датаграмм перед пересылкой адресату.

Данная служба позволяет подключаться к Интернету, совместно используя один или несколько общих зарегистрированных адресов на компьютере со службой NAT.

Маршрутизатор с функцией NAT действует как преобразователь адресов.

Работа механизма трансляции адресов

- При попытке соединения с веб-узлом маршрутизатор, выполняющий роль транслятора сетевых адресов, отображает его частный IP-адрес на действительный Интернет адрес.

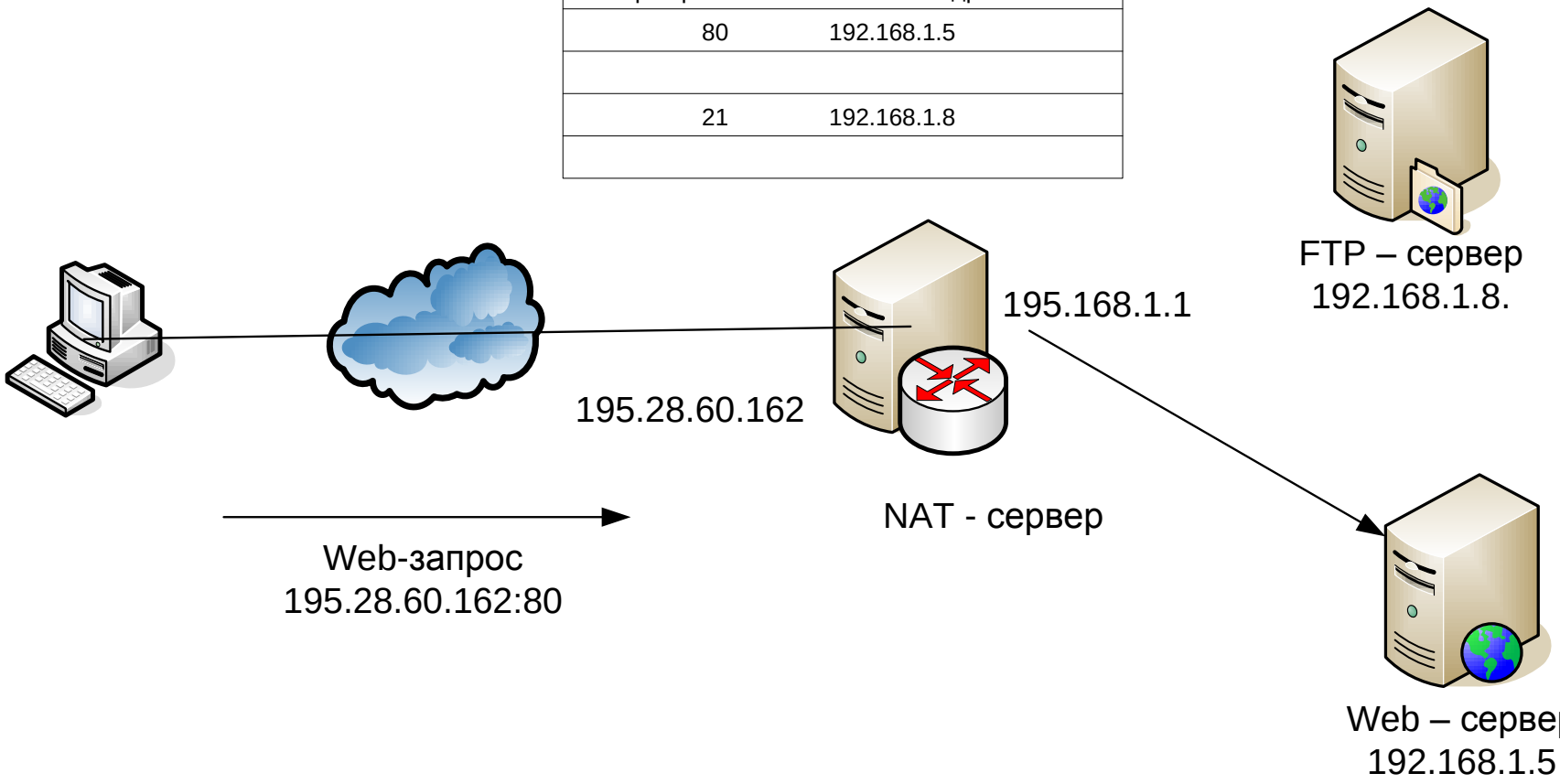


Специальные порты NAT

- Специальные порты службы NAT используются для того, чтобы сопоставить внутреннюю службу (например web-, telnet-, ftp- сервер) внешнему интерфейсу компьютера с NAT.
- Решение позволяет внешние запросы служб внутренней сети направлять на соответствующий компьютер.

Использование специальных портов NAT

Номер порта	Сопоставление адреса
80	192.168.1.5
21	192.168.1.8



Реализация службы маршрутизации в Windows Server

Служба Маршрутизация и удаленный доступ (Routing and Remote Access, RRAS) в Windows Server 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.

Особенности Службы маршрутизации и удаленного доступа Windows

Служба RRAS может быть сконфигурирована для особого вида маршрутизации:

- Многоадресные ip-рассылки;
- Маршрутизация вызовов по требованию;
- Ретрансляция DHCP;
- Фильтрация пакетов

В службу включена поддержка протоколов динамической маршрутизации:

- RIP (routing information protocol)
- OSPF (open shortest path first).

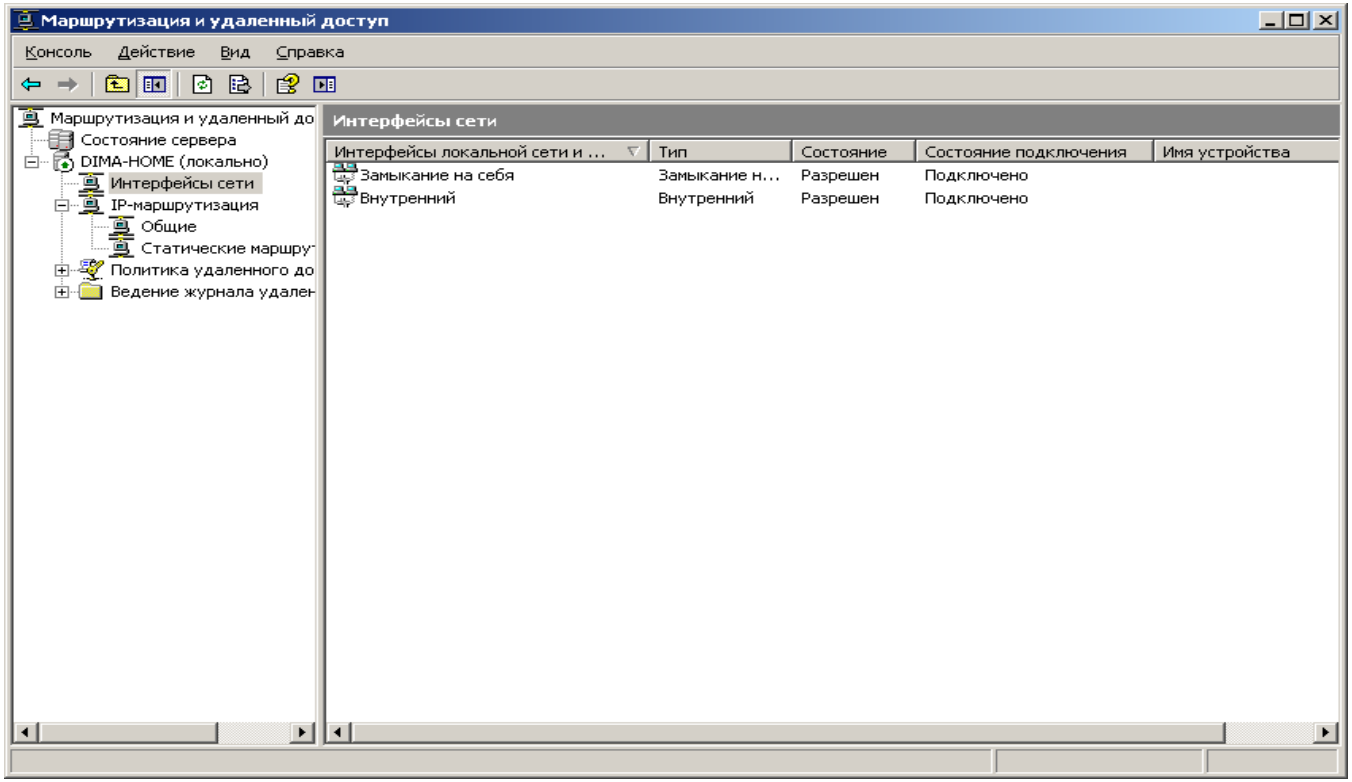
Запуск службы Маршрутизация и удаленный доступ

Активация службы выполняется с помощью установки роли **Сервер политик сети** (службу роли Маршрутизация и удаленный.

Если сервер маршрутизации является рядовым членом домена Active Directory, то он должен быть включен в группу **Серверы RAS.**

Консоль управления Маршрутизация и удаленный доступ

- Консоль управления Маршрутизация и удаленный доступ представляет собой стандартную оснастку Консоли управления Майкрософт (MMC) в Windows.
- В конфигурации по умолчанию поддерживается маршрутизация в ЛВС.



Создание интерфейсов

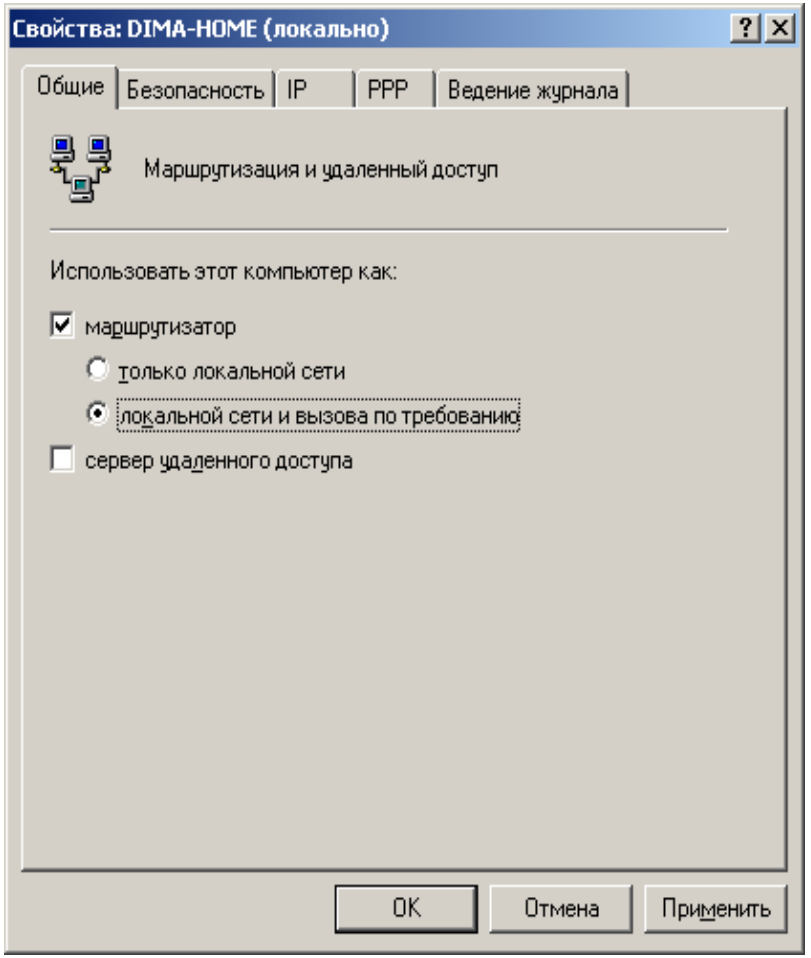
Сетевой интерфейс в консоли управления – программный компонент, подключаемый к физическому устройству (модему или сетевой плате).

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

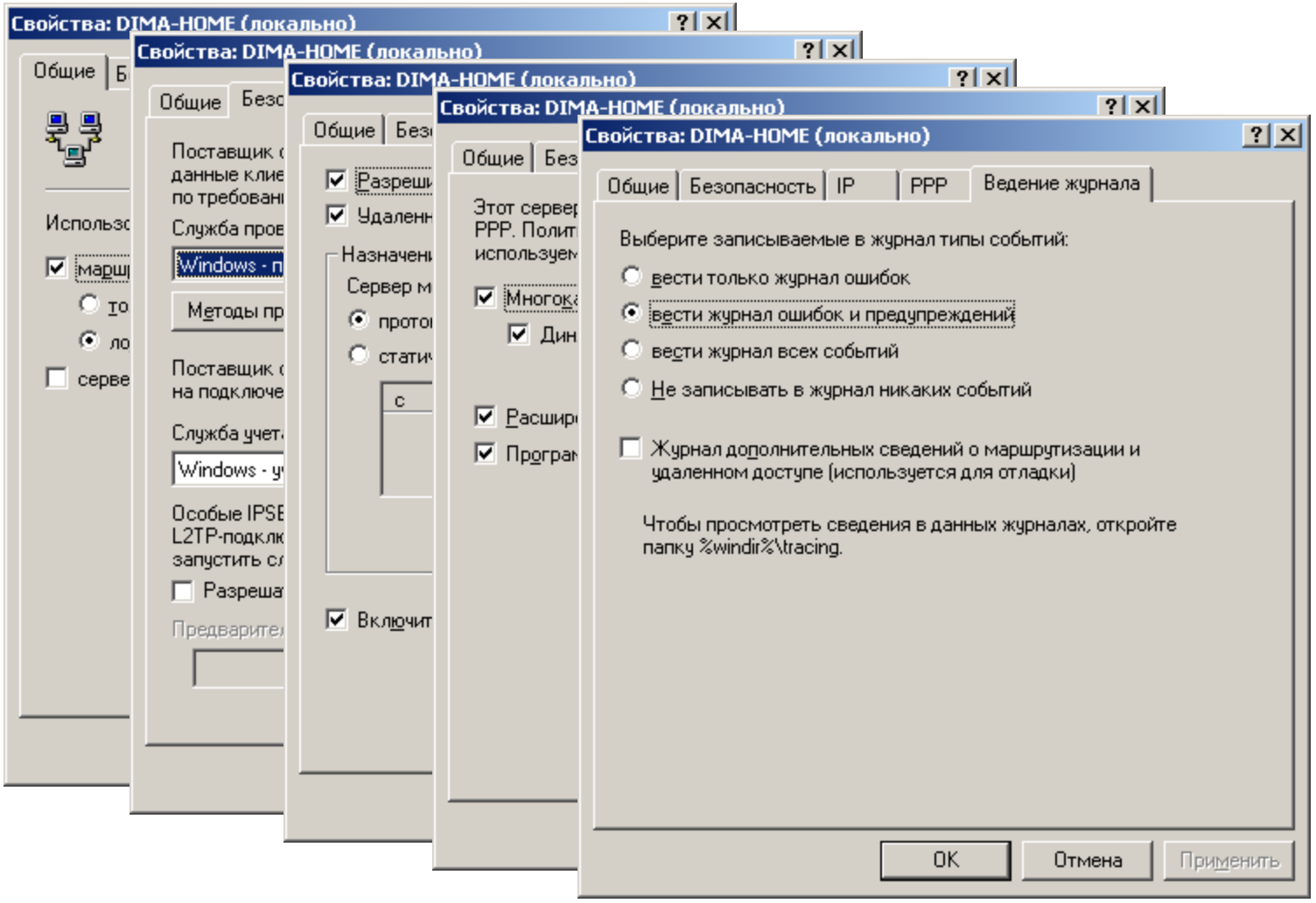
- Для создания интерфейса по вызову, необходимо включить такую возможность в **Свойствах** сервера маршрутизации.
- Для создания подключения используется Мастер интерфейса по требованию



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



Фильтрация пакетов

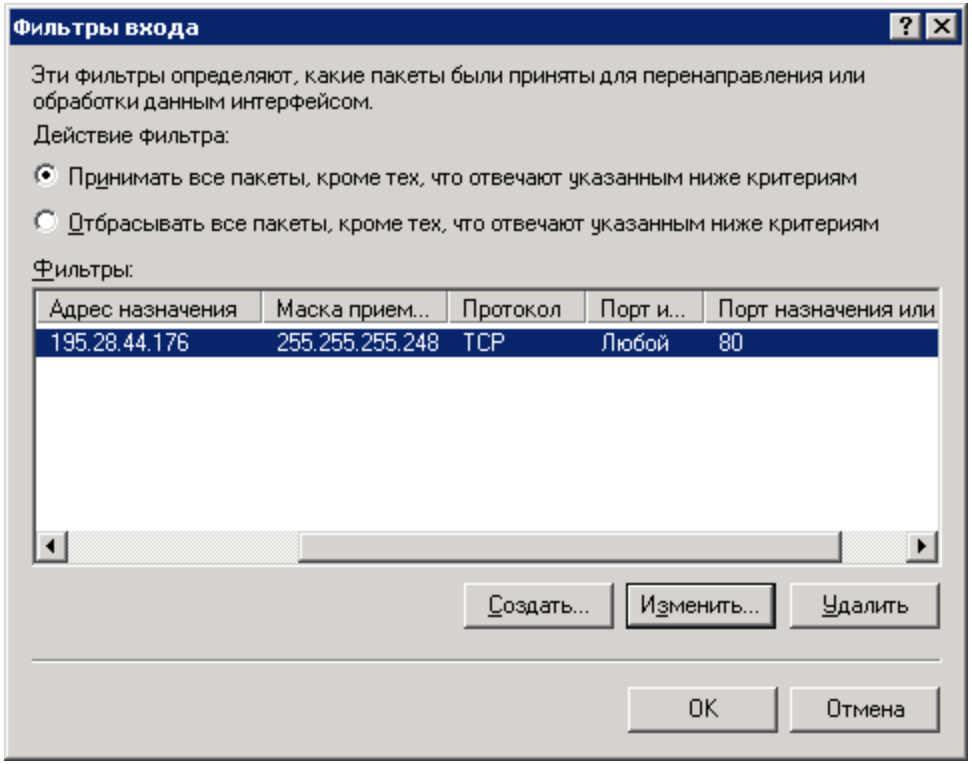
- **Фильтры пакетов** - это правила, определяемые на интерфейсе, которые разрешают или запрещают трафик по определенным признакам: по исходящему адресу, адресу назначения, направлению или потоку.
- Функционирование фильтров в службе Маршрутизация и удаленный доступ основано на исключениях.
- Фильтры назначаются и настраиваются в одном их двух режимах:
  - Пропуск всего трафика за исключением пакетов, запрещенных фильтрами;
  - Запрещение всего трафика за исключением пакетов, разрешенных фильтрами.

Фильтры пакетов

- Фильтры пакетов делятся на два типа:
  - Входные фильтры – ограничивают трафик, поступающий на интерфейс непосредственно подключенной к нему сети;
  - Выходные фильтры – ограничивают трафик, поступающий с интерфейса в сеть.

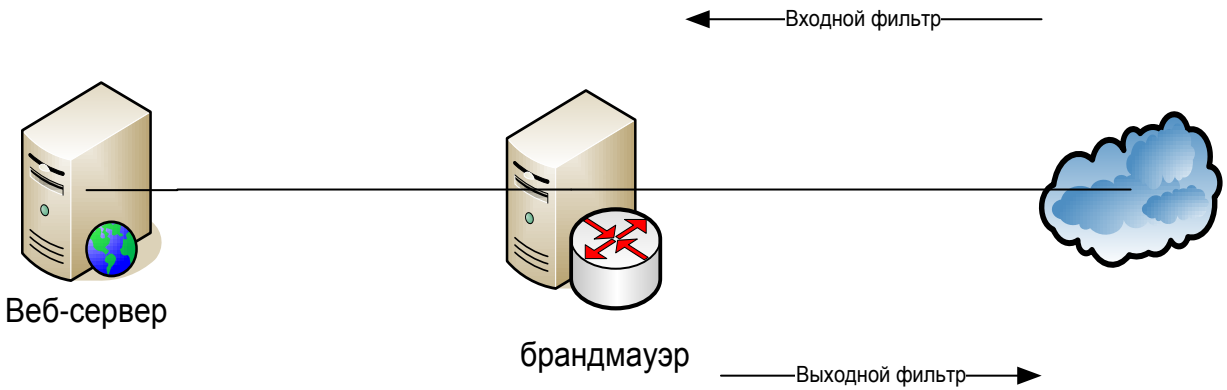
Задание фильтров

- Указанный на рисунке входной фильтр, принимает все пакеты, кроме пакетов, направленных на TCP-порт 80 и IP – сеть 195.28.44.176 с маской 255.255.255.248



Сценарии фильтрации (базовая фильтрация)

- Фильтр входной определяется как фильтр адресата веб-узла с маской 255.255.255.255
- Фильтр выходной определяется аналогично, настроен на протокол TCP и порт 80.

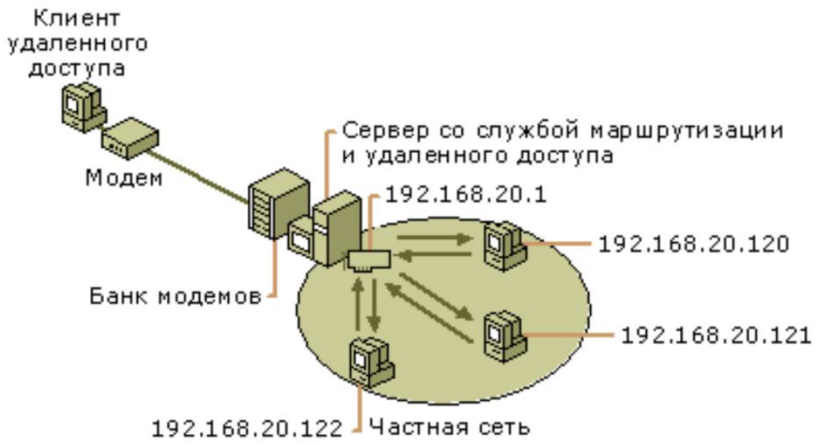


Стандартные конфигурации для серверов удаленного доступа

- При запуске мастера настройки сервера маршрутизации и удаленного доступа выводится запрос для выбора пути настройки, более всего соответствующего решению маршрутизации и удаленного доступа, который планируется развернуть.
- При выборе особого пути настройки необходимо вручную настроить все элементы маршрутизации и удаленного доступа.
- Общие решения удаленного доступа включают:
  - подключения удаленного доступа,
  - подключения виртуальной частной сети (VPN),
  - безопасное соединение между двумя частными сетями.

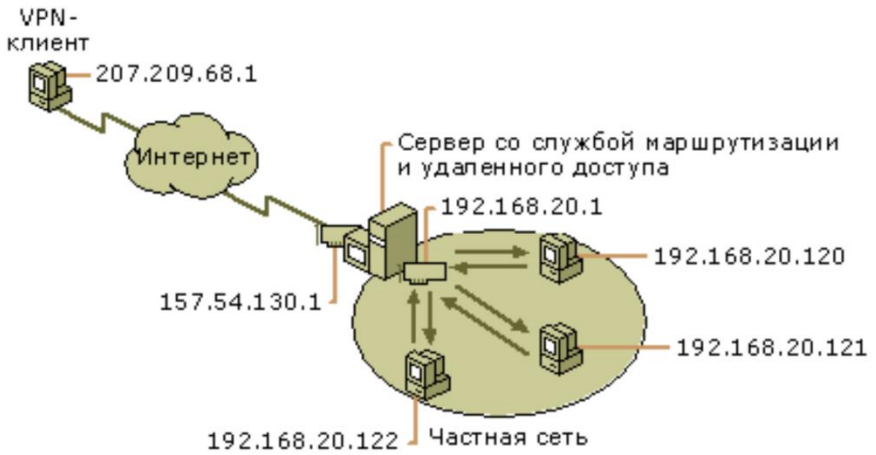
Удаленный доступ (модем)

- При выборе данного пути сервер со службой маршрутизации и удаленного доступа настроен для разрешения подключения клиентов удаленного доступа к частной сети с помощью вызова банка модема или другого оборудования удаленного доступа.
- Дополнительные настройки:
  - установка ответа сервера на вызов;
  - установка разрешений для клиентов удаленного доступа для подключения к частной сети и перенаправления сетевого трафика между клиентами удаленного доступа и частной сетью.



Удаленный доступ (VPN)

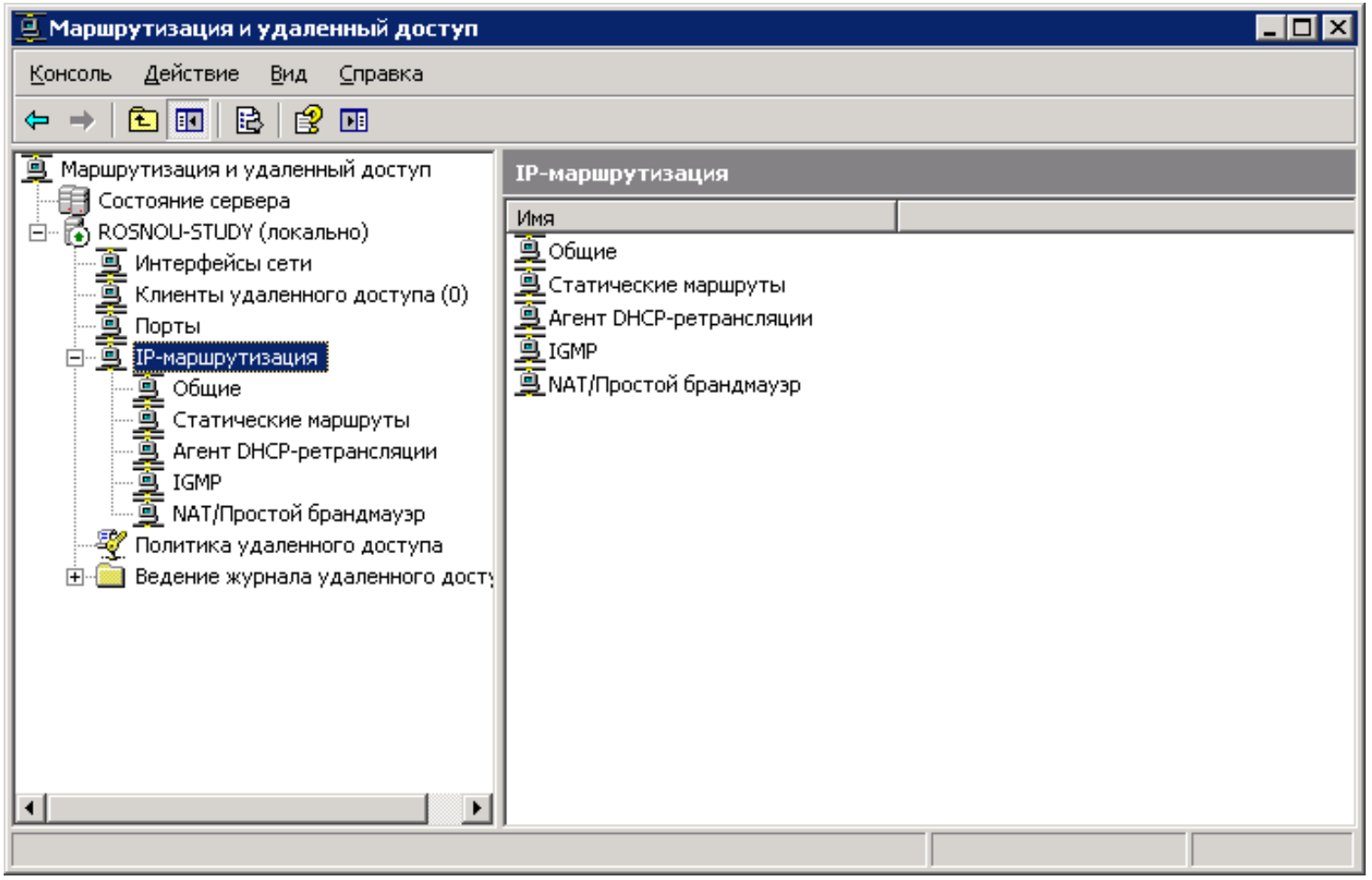
- При выборе данного пути сервер со службой маршрутизации и удаленного доступа настроен для разрешения подключения клиентов удаленного доступа к частной сети через Интернет.
- После окончания работы мастера можно настроить дополнительные параметры. Например:
  - как сервер проверяет разрешения клиентов VPN для подключения к частной сети
  - разрешен ли сетевой трафик между клиентами VPN и частной сетью.



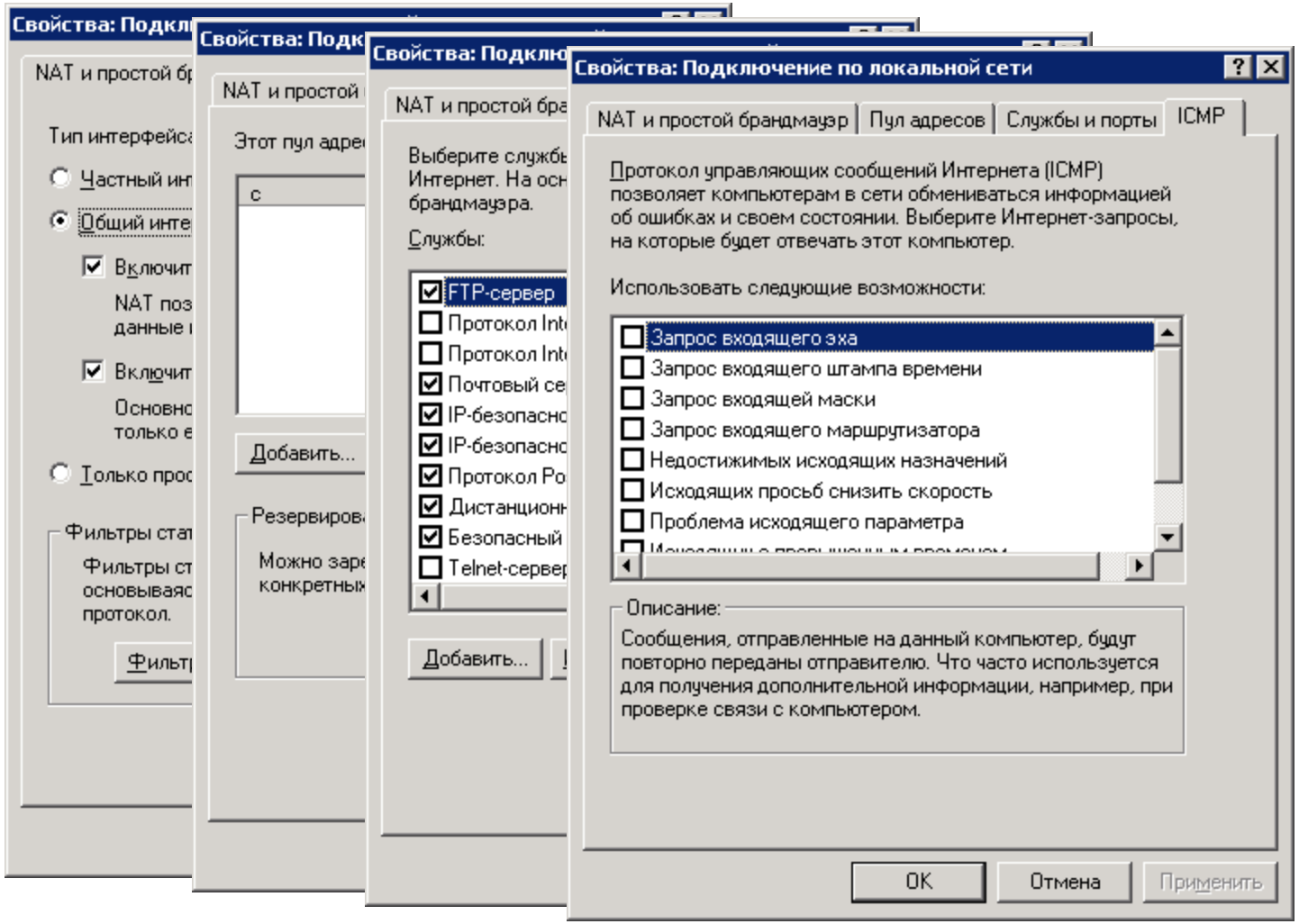
Преобразование сетевых адресов (NAT)

- При выборе данного пути сервер со службой маршрутизации и удаленного доступа настроен для совместного использования с компьютерами частной сети подключения к Интернету и для передачи трафика между общим адресом и частной сетью.
- После окончания работы мастера можно настроить дополнительные параметры. Например:
  - настроить фильтры пакетов
  - выбрать службы для общего интерфейса.

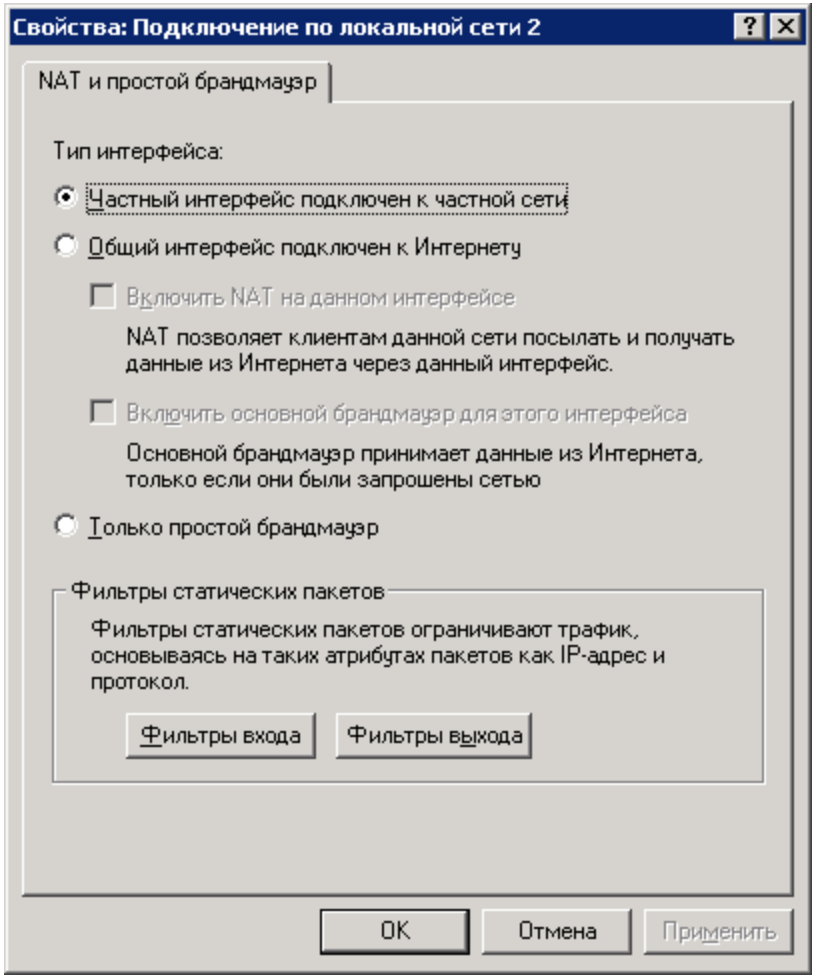
Настройка NAT



Настройка NAT (общие интерфейсы)

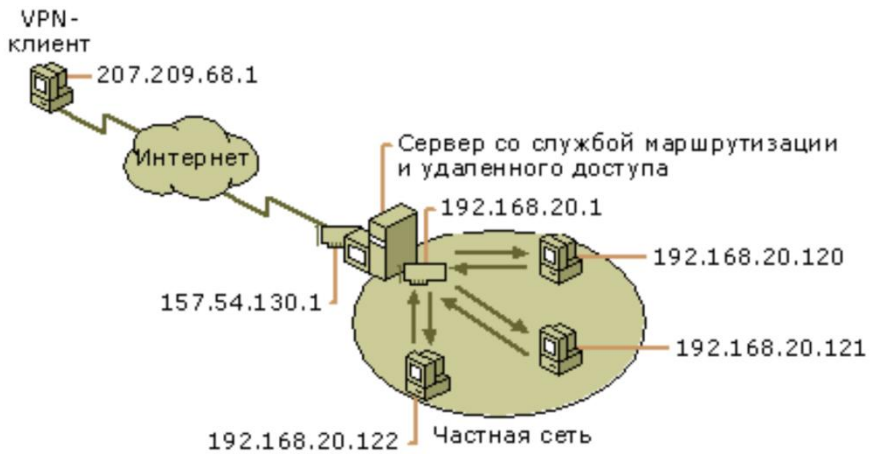


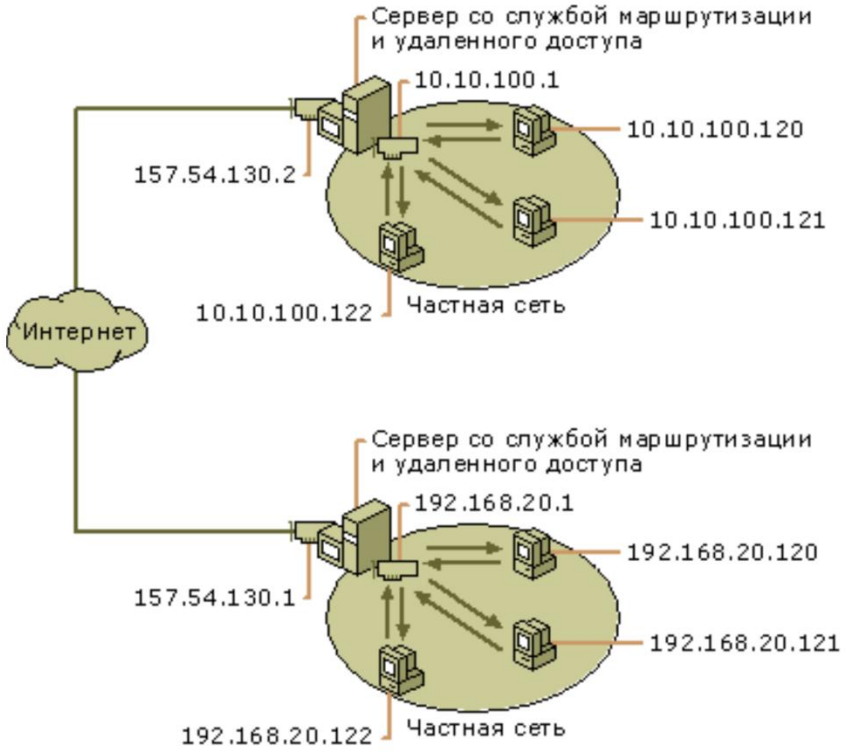
Настройка NAT (внутренние интерфейсы)



Виртуальная частная сеть (VPN) и преобразование сетевых адресов (NAT)

- При выборе данного пути сервер со службой маршрутизации и удаленного доступа настроен для предоставления частной сети преобразования сетевых адресов (NAT) и для принятия соединений по VPN.
- Клиенты VPN в состоянии подключаться к компьютерам частной сети, как если бы они были физически присоединены к этой сети.



Безопасное соединение между двумя частными сетями

- При выборе данного пути два сервера со службой маршрутизации и удаленного доступа настроены для безопасной передачи частных данных через Интернет.
- Подключение между двумя серверами может быть постоянным (включено постоянно), либо по требованию (вызов по требованию).
- На каждом сервере можно настроить дополнительные параметры. Например:
  - какие каждый сервер принимает протоколы маршрутизации
  - как каждый сервер направляет трафик между сетями.