

Администрирование информационных систем

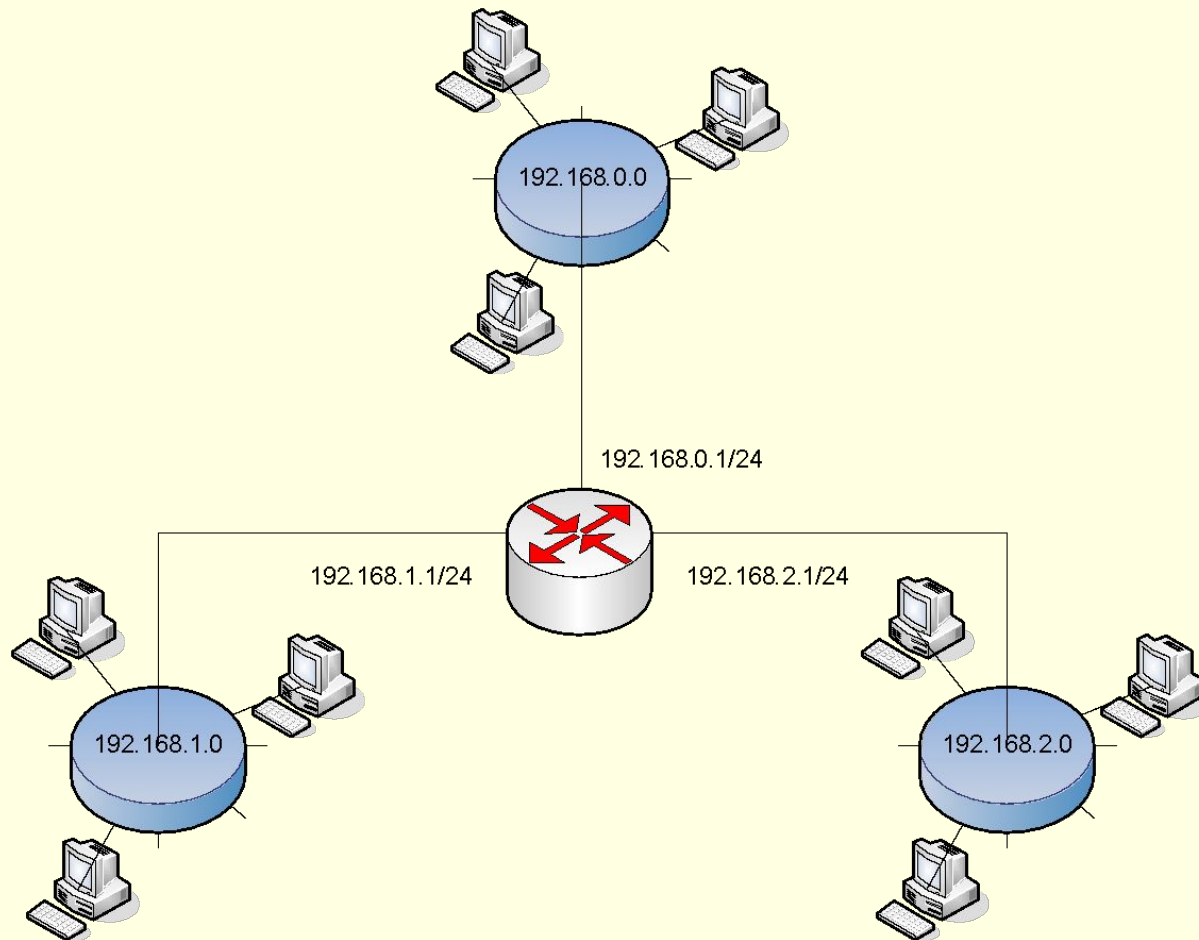
Лекция 10.

Маршрутизация и удаленный доступ

Маршрутизация в Windows Server 2003

- **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.

Локальные сети, объединенные маршрутизатором



Служба Маршрутизация и удаленный доступ

- Служба **Маршрутизация и удаленный доступ** (Routing and Remote Access, RRAS) в Windows 2003 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

- Кроме того, служба 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) и OSPF (open shortest path first).

Организация маршрутизации на сервере под управлением Windows Server 2003

- На аппаратных маршрутизаторах может существовать множество различных портов, обеспечивающих подключение различных сегментов сети. Аппаратный маршрутизатор может пересылать трафик между любыми двумя портами.
- Количество сетевых сегментов, поддерживаемых Службой маршрутизации и удаленного доступа ограничено количеством сетевых интерфейсов компьютера.

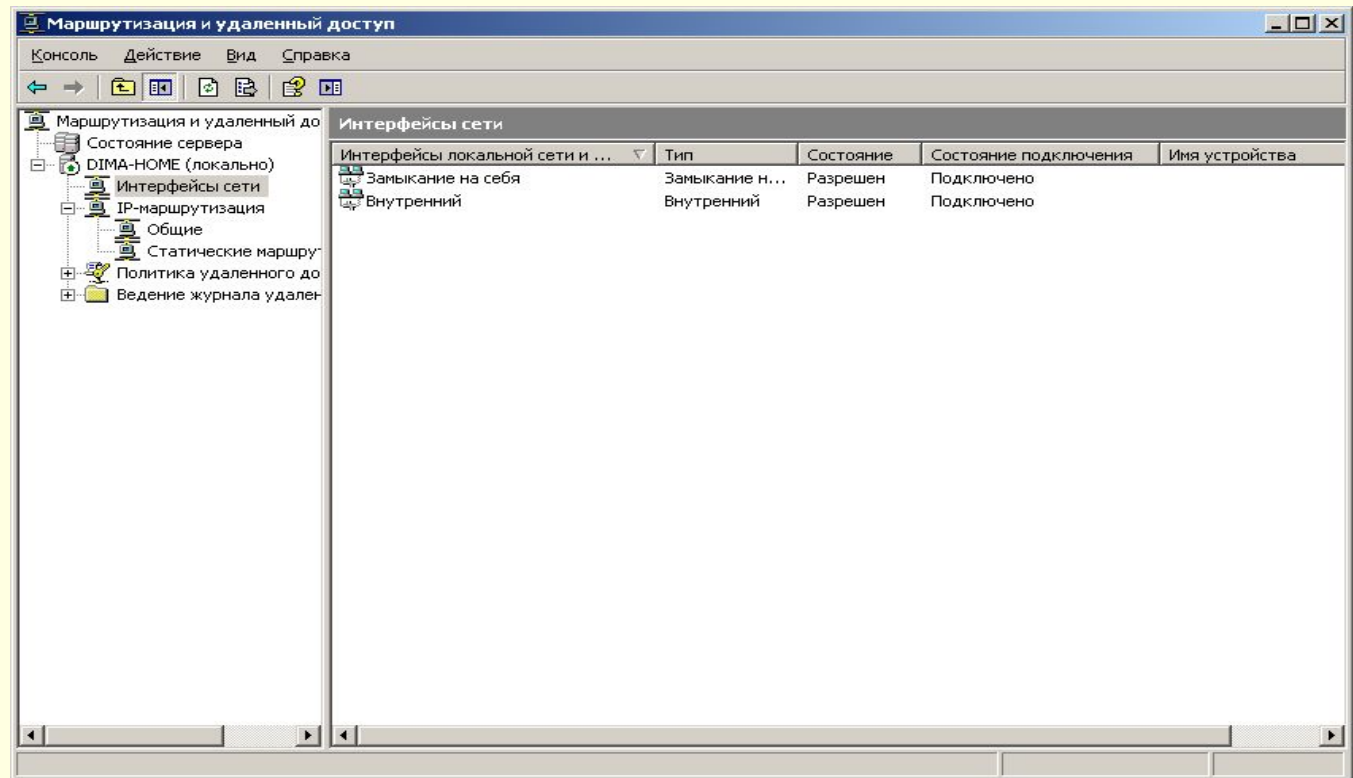
Запуск службы Маршрутизация и удаленный доступ

- При установке Windows server 2003 служба Маршрутизация и удаленный доступ отключена.
- Ее активация выполняется с помощью Мастера настройки сервера маршрутизации и удаленного доступа.
- Если сервер маршрутизации является рядовым членом домена Active Directory, то он должен быть включен в группу Серверы RAS и IAS.
- Контроллеры домена в дополнительной настройке не нуждаются.

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.

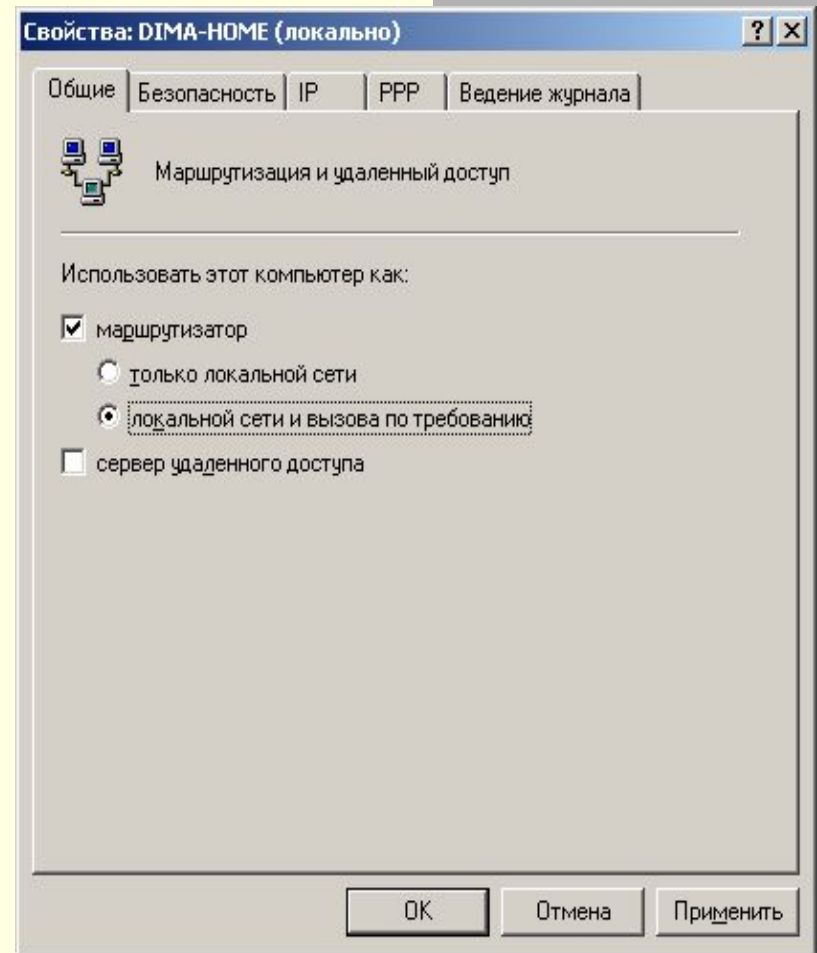


Создание интерфейсов

- 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

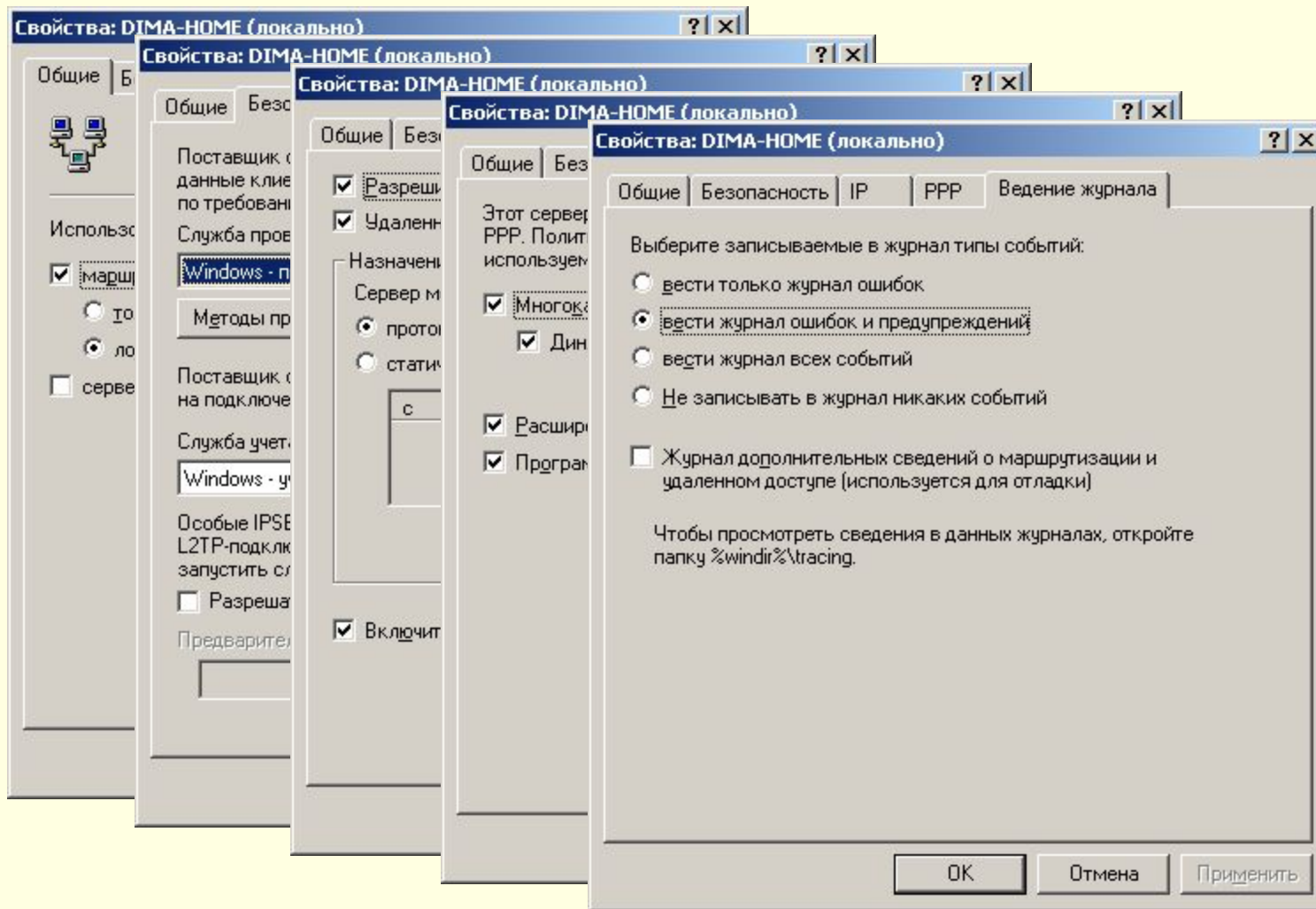
- Для создания интерфейса по вызову, необходимо включить такую возможность в Свойствах сервера маршрутизации.
- Для создания подключения используется Мастер интерфейса по требованию



IP - маршрутизация

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

Настройка параметров службы маршрутизации и удаленного доступа



Управление таблицей маршрутизации

- Маршрутизаторы считывают адреса назначения пакетов и переправляют пакеты в соответствии с информацией, хранящейся в таблицах маршрутизации.
- Отдельные записи таблицы маршрутизации называются маршрутами.
- Существуют три типа маршрута:
 - Маршрут узла – определяет ссылку на определенный узел или широковещательный адрес. Маска маршрута – 255.255.255.255;
 - Маршрут сети – определяет маршрут к определенной сети, а соответствующее поле в таблицах маршрутизации может содержать произвольную маску;
 - Маршрут по умолчанию – один маршрут, по которому отправляются все пакеты, чей адрес не совпадает ни с одним адресом таблицы маршрутизации.
- Просмотр таблицы маршрутизации может быть выполнен с помощью команды
 - **route print**

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.
- Среда со статической маршрутизацией могут использоваться в следующих случаях.
 - Малый бизнес.
 - Небольшая офисная объединенная IP-сеть.
 - Единственная сеть офиса подразделения.

Недостатки статической маршрутизации

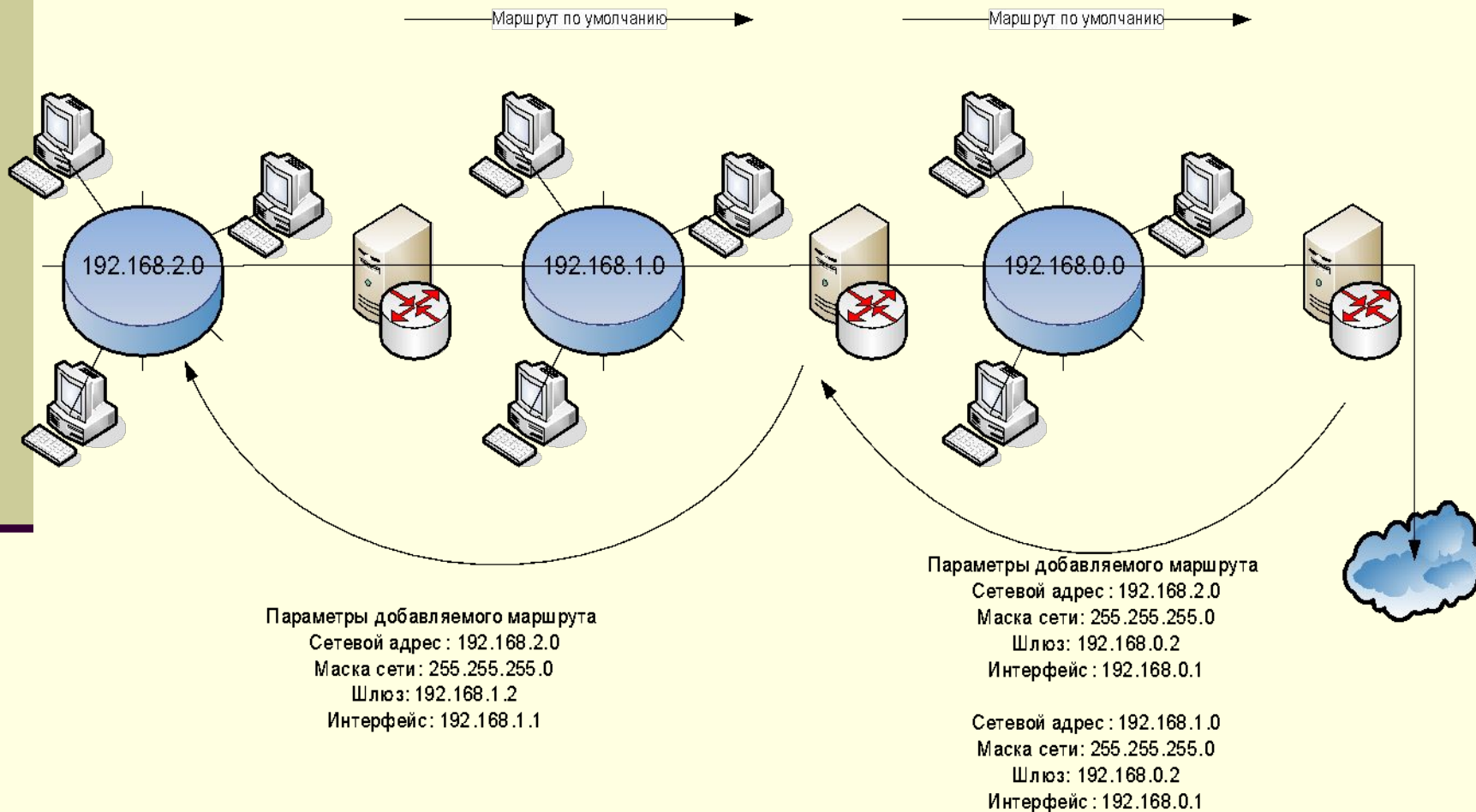
■ Отсутствие отказоустойчивости

- Если маршрутизатор или канал связи перестают функционировать, статические маршрутизаторы не обнаруживают сбой и не информируют о нем другие маршрутизаторы. Эта проблема существенна главным образом для больших объединенных сетей организаций; небольшие офисные сети (с двумя маршрутизаторами и тремя локальными сетями) испытывают такие трудности недостаточно часто для того, чтобы рассматривать вопрос о развертывании топологии с множественными путями и протоколом маршрутизации.

■ 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



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.

Настройка NAT

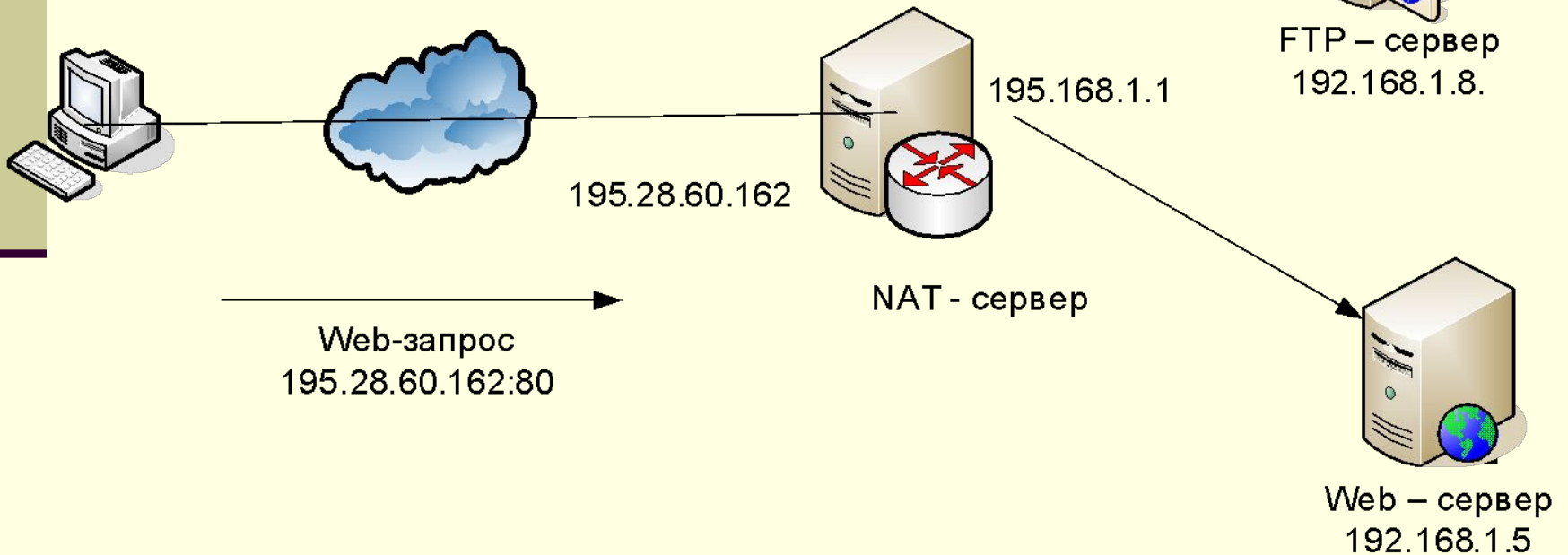
- NAT позволяет выбрать любой частный адрес в качестве внутреннего адреса NAT – сервера, есть возможность отключить DHCP – сервер и DNS – прокси.
- При настройке NAT для предоставления услуг DHCP внутренним клиентам можно задавать любые диапазоны адресов.
- NAT позволяет сконфигурировать внешний совместно 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



Web-запрос
195.28.60.162:80

195.168.1.1

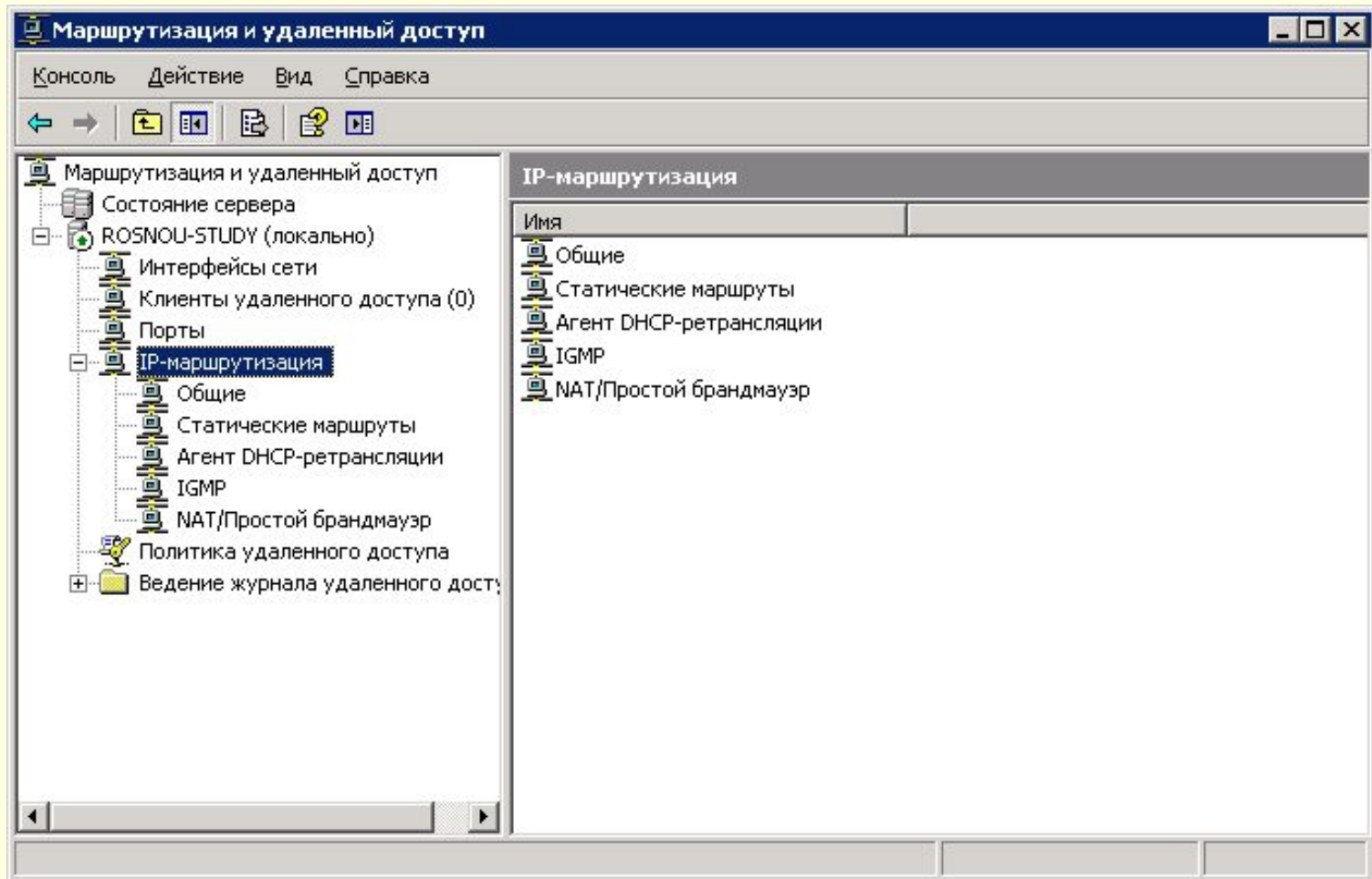
FTP – сервер
192.168.1.8.

NAT - сервер

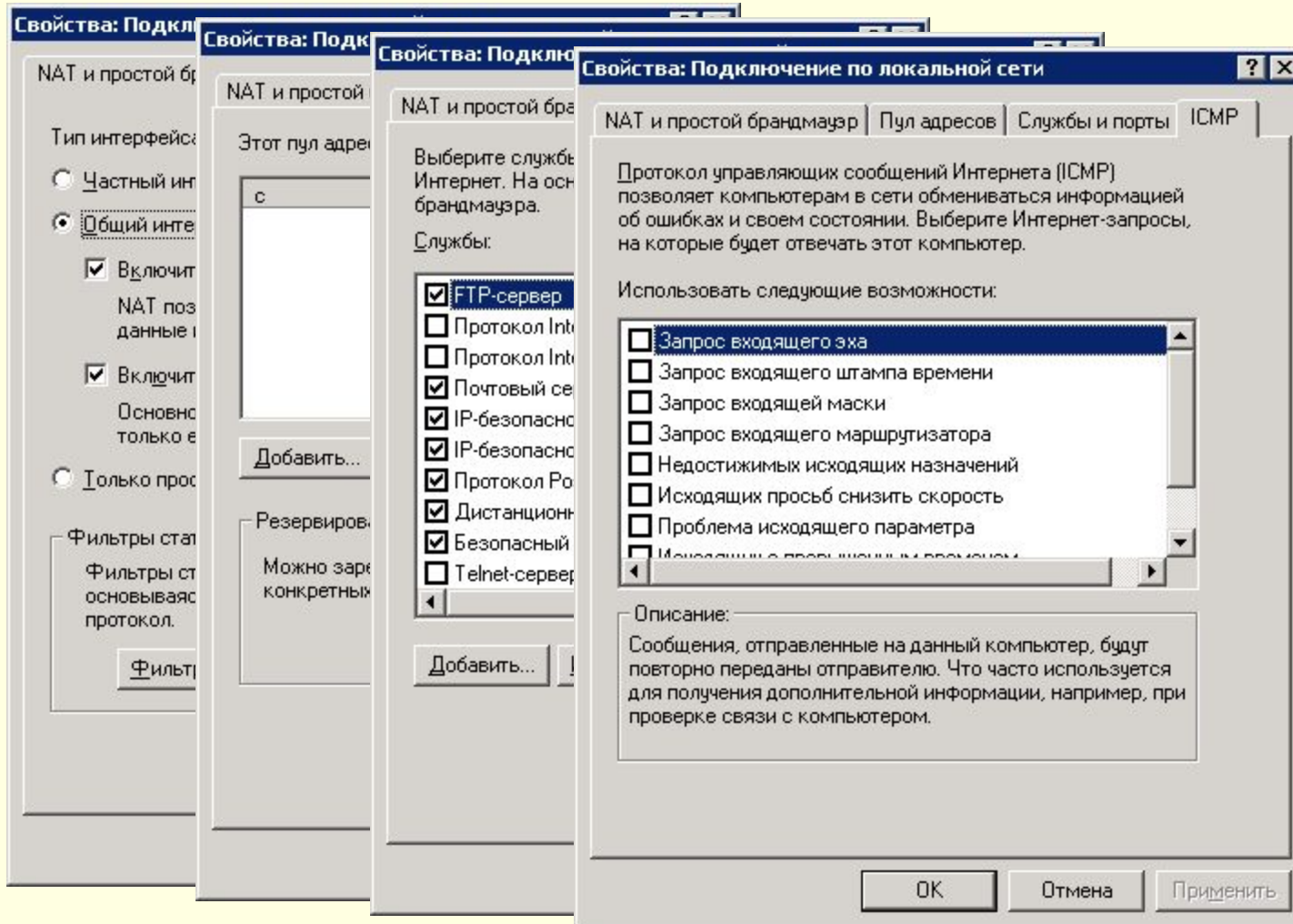
Web – сервер
192.168.1.5

195.28.60.162

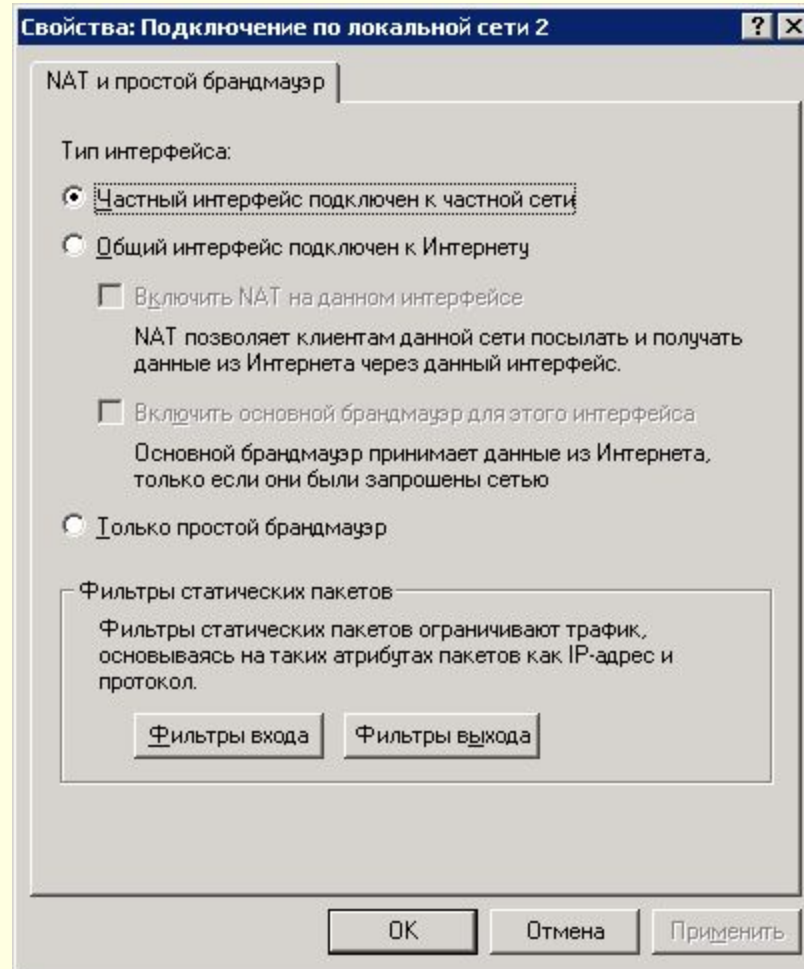
Настройка NAT



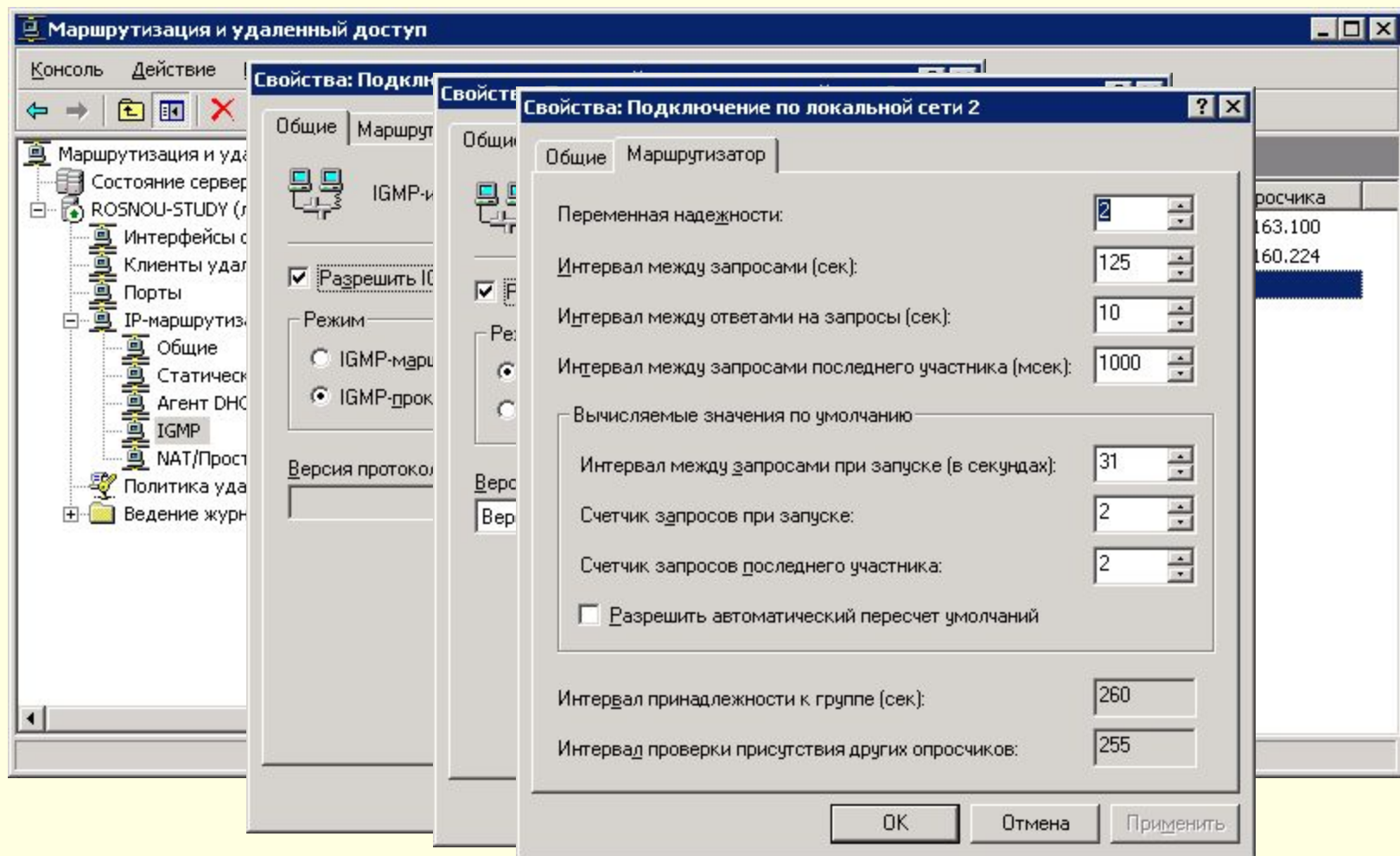
Настройка NAT (общие интерфейсы)



Настройка NAT (внутренние интерфейсы)



Многоадресная маршрутизация



Фильтрация пакетов

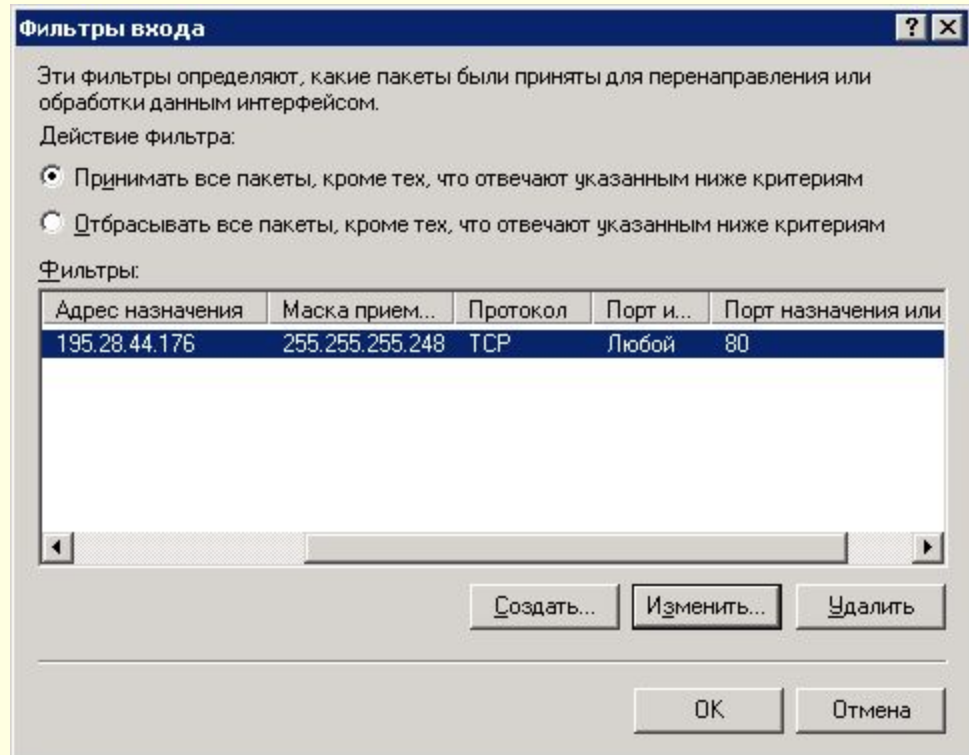
- **Фильтры пакетов** - это правила, определяемые на конкретном интерфейсе, которые разрешают или запрещают трафик по определенным признакам: по исходящему адресу, адресу назначения, направлению или потоку.
- Функционирование фильтров в службе Маршрутизация и удаленный доступ основано на исключениях.
- Фильтры назначаются и настраиваются в одном из 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.

Фильтры пакетов

- 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.

