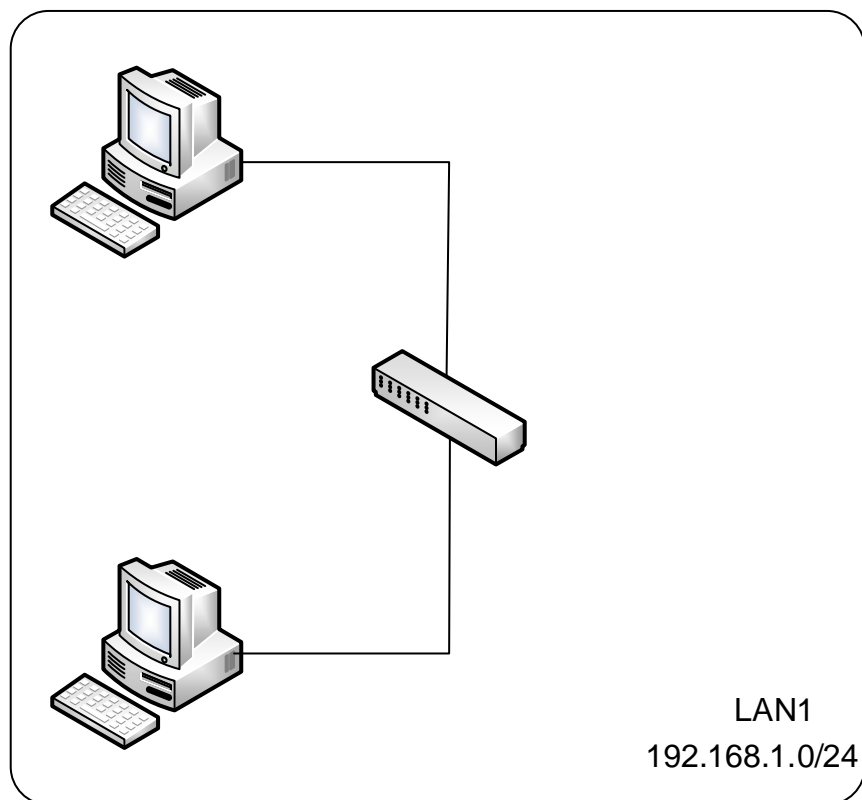


## 1 ЭТАП

Выбрать адресацию для ПК в указанном сегменте сети, настроить адресацию каждого ПК. Проверить доступность ПК в обоих направлениях. Сверить ARP таблицы на каждом ПК с параметрами и настройками каждого ПК.

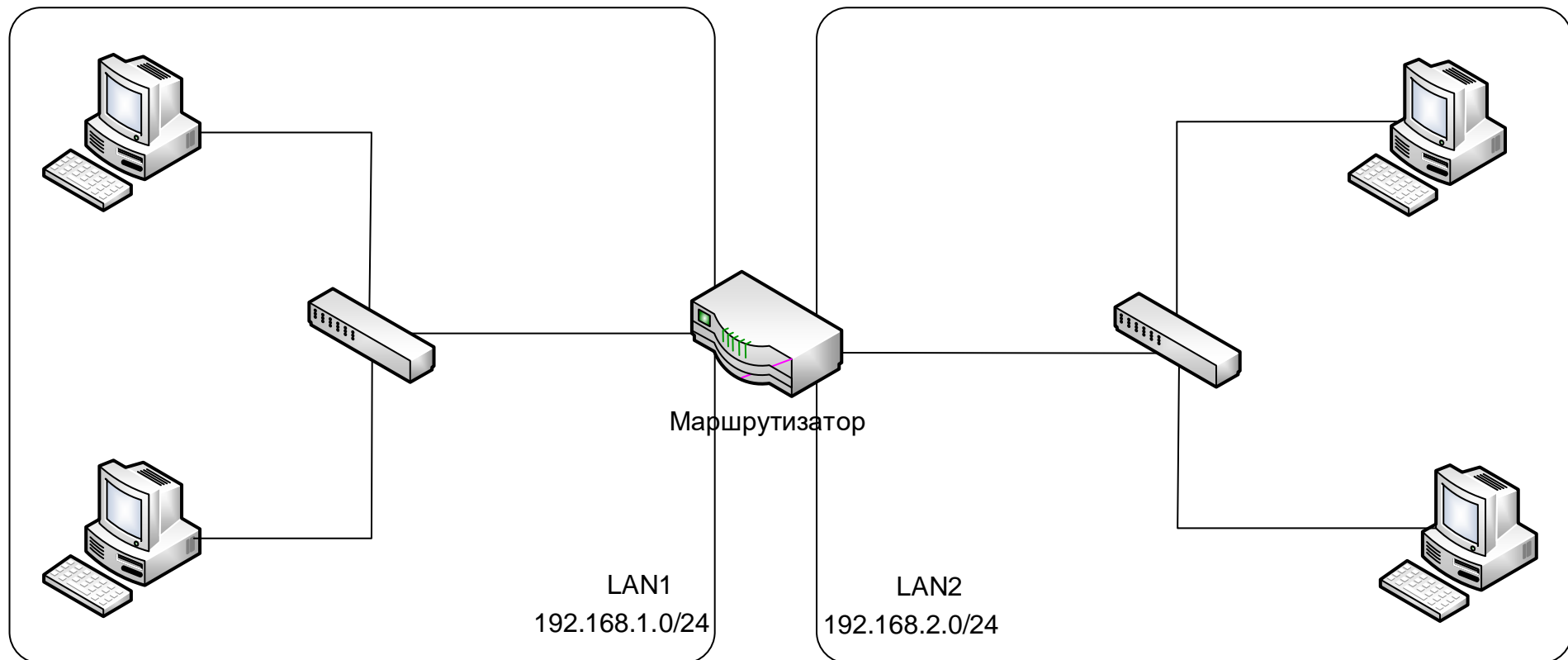


## 2 ЭТАП

Использовать ранее настроенную адресацию LAN1, выбрать и настроить адресацию ПК обоих сегментов, а также настроить адреса на сетевых интерфейсах маршрутизатора

Настроить на маршрутизаторе параметры для передачи пакетов между сетевыми интерфейсами. Для ОС Windows В редакторе реестра найти параметр IpEnableRouter и присвоить ему значение 1 (3 раза в реестре). Для ОС Linux найти файл Ip\_forward (/proc/sys/net/ipv4/ip\_forward) и заменить в нем 0 на 1, сохранить файл, перезапустить сетевую службу или маршрутизатор. В разных Linux форвардинг может настраиваться по разному, могут потребоваться команды вместо редактирования файла Ip\_forward.

Настроить маршруты на каждом ПК для доступа к ПК соседней сети с использованием параметра «Шлюз по умолчанию» в настройках параметров сети в графической оболочке или с помощью команды в командной строке



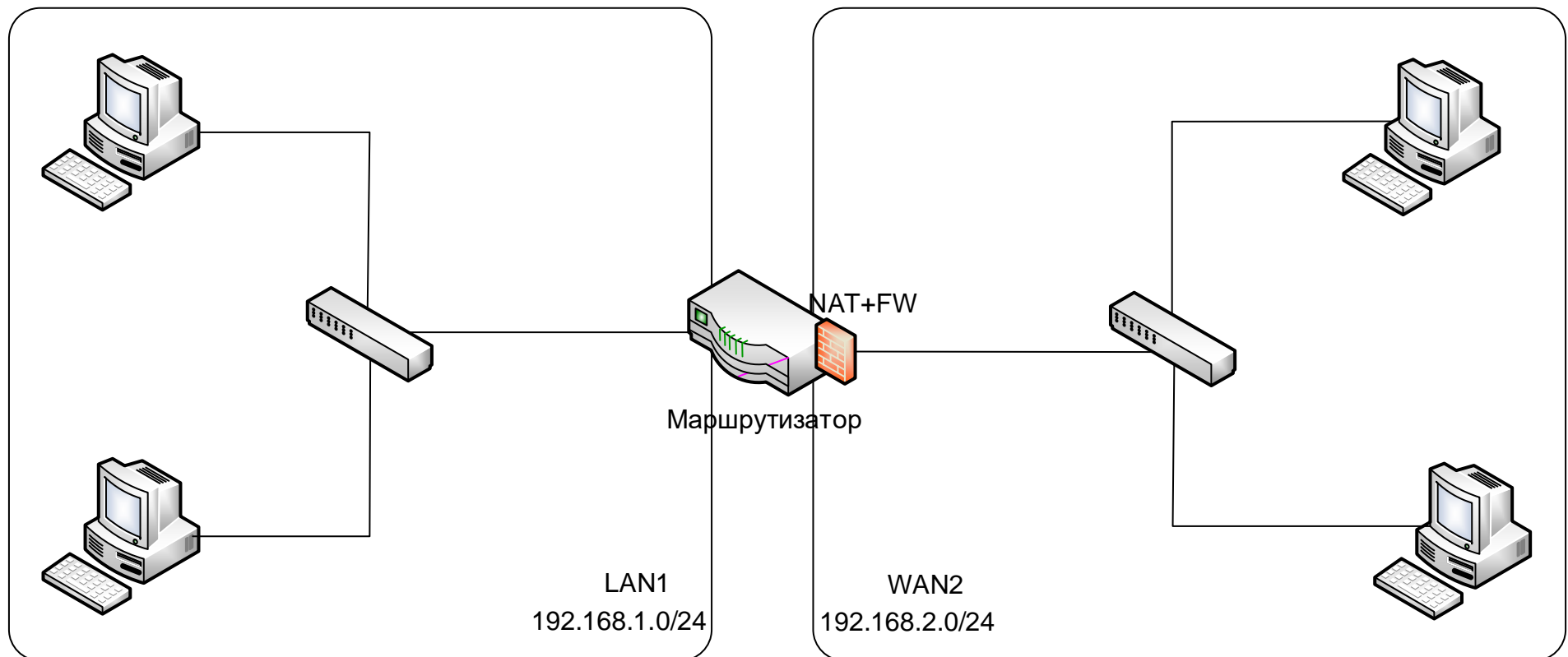
Проверить соединения ПК с маршрутизатором. Проверить соединения ПК в разных сегментах сети. Проверить чтобы трассировка маршрута выдала 2 шага следования пакетов между сетями.

### 3 ЭТАП

Для упрощения понимания механизмов NAT на маршрутизаторе рекомендуется использовать ОС Windows 2003 Server, Linux, VyOS

Настроить NAT на внешнем сетевом интерфейсе маршрутизатора (подключен к WAN2) используя оснастку «Маршрутизация и удаленный доступ» в ОС Windows 2003 Server, iptables в Linux, соответствующие разделы конфигурации в VyOS. При этом адрес отправителя должен подменяться на адрес сетевого интерфейса маршрутизатора (шлюза), подключенного к сети WAN2. Проверить правильность работы трансляции адресов используя анализатор трафика на целевом ПК во внешней сети.

При использовании VyOS на шлюзе обязательна настройка firewall вместе с nat



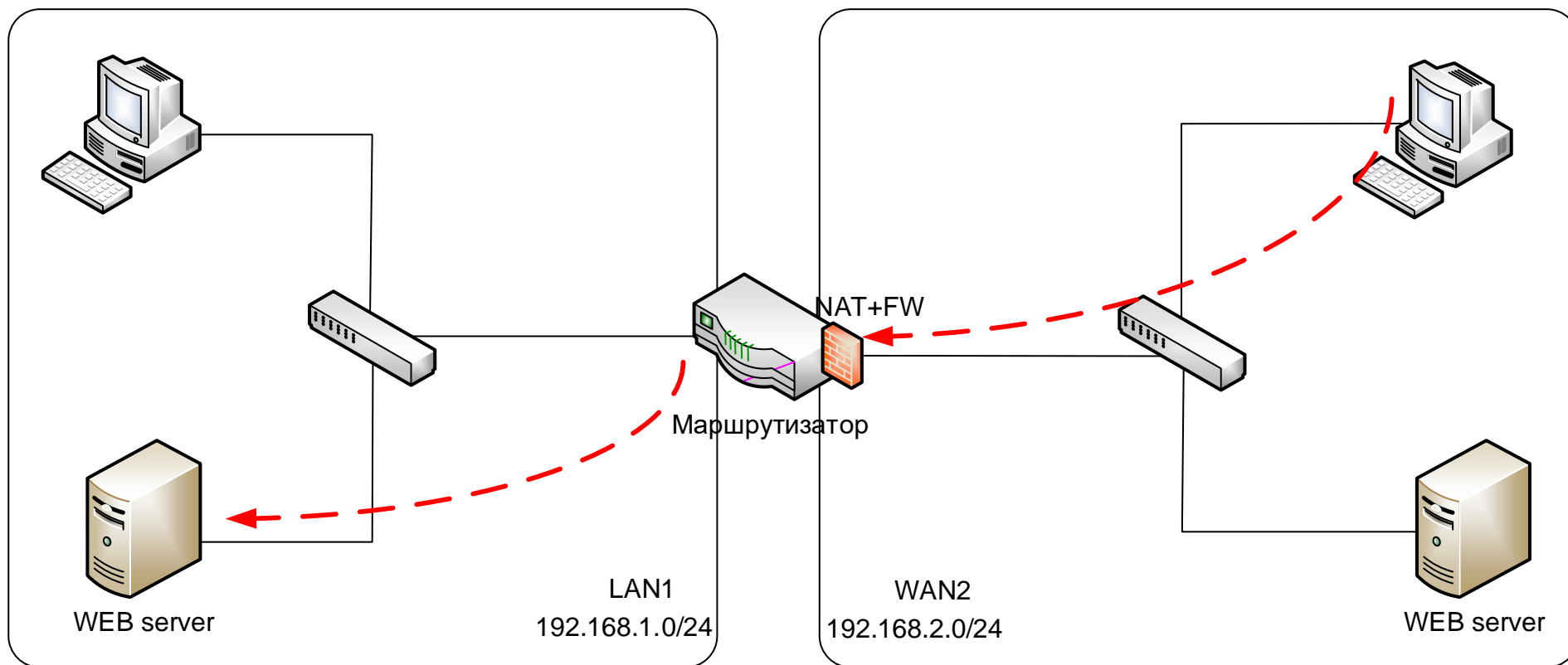
Проверить соединения ПК с маршрутизатором. Проверить соединения ПК в разных сегментах сети. Проверить чтобы трассировка маршрута выдала 2 шага следования пакетов между сетями. Проверить чтобы пакеты из внешней сети не проходили во внутреннюю. Проверить подмену адреса отправителя на ПК получателя используя Wireshark, tcpdump.

## 4 ЭТАП

Для реализации WEB server рекомендуется использовать инструменты настройки IIS в разделе Администрирование в ОС Windows 2003 Server

Настроить destination nat на шлюзе по протоколу http (порт 80) для доступа к web серверу во внутренней сети. При этом На ПК во внешней сети Http://«внешний адрес шлюза» должен переадресовываться на Web Server во внутренней сети.

Настройку шлюза выполнять используя «Маршрутизация и удаленный доступ», iptables, nat+fw в соответствующих ОС на шлюзе



Проверить чтобы пакеты из внешней сети не проходили во внутреннюю.