Инструкция по настройке режима Port Forwarding в модемах Acorp Sprinter@ADSL LAN120, LAN420 и W400G

I. Введение

Использование xDSL модема в режиме маршрутизатора с активированной службой NAT/Firewall является неоспоримым преимуществом в плане защиты домашней сети от нежелательных вторжений из сети Интернет, но вместе с безопасностью, пользователю, возможно, предстоит столкнуться с необходимостью настройки службы Port Forwarding.
Целью написания данной инструкции является необходимость развеять миф о сложности настройки службы Port Forwarding у начинающего пользователя.
Перед тем как погрузится в мир настройки описываемой службы, следует пояснить для каких целей она применяется. Наверно, все в какой-то мере пробовали играть в он-лайн игры с использованием сети Интернет (Рис. 1).

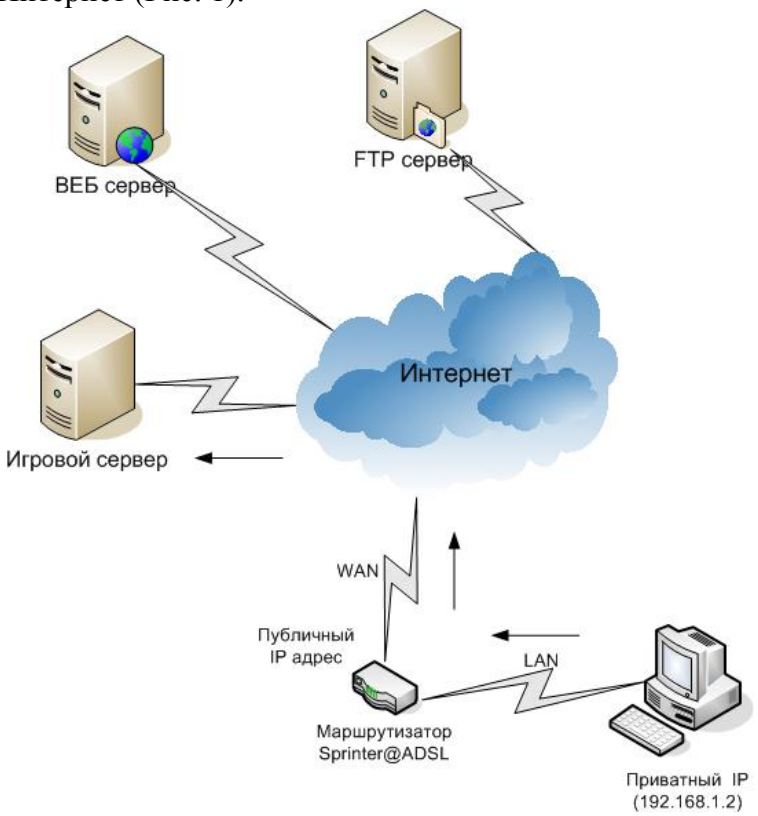

Рис. 1

Вы подключаетесь к определенному серверу, и начинается сеанс игры (направление установления сеанса показано стрелками). Но что будет, если вы хотите организовать подобный сервер у себя дома? Или в связи с постоянным доступом в Интернет, посредством xDSL модема, возникло желание перенести свою домашнюю страничку с бесплатного «хостинга» на свой домашний HTTP сервер. А может, вы часто ездите по миру и вам необходимо сделать доступ на свою директорию при помощи FTP сервера. В этом случае, удаленный компьютер должен обратиться к вашему Игровому, HTTP или FTP серверу, находящемуся за xDSL модемом (направление установления сеанса показано стрелками), но в данном случае непременно возникнет следующая проблема – невидимость вашего персонального компьютера или локальной сети из-за службы NAT/Firewall модема (Рис. 2).

NAT (Network Address Translation) – служба трансляции IP адресов внутренней сети в IP адреса внешней сети. Данная служба применяется, когда адреса внутренней сети выбираться из диапазонов приватных IP адресов зарезервированных для использования в локальных сетях, таких как 10.x.x.x, 172.16.x.x-172.31.x.x и 192.168.x.x. Важной особенностью приватных адресов является невозможность обращения из сети Интернет к хосту имеющему подобный адрес, т.е. они невидимы из сети Интернет. А также невозможность доступа в сеть Интернет с подобного адреса без использования службы NAT.

Следует это из-за того, что невозможно обратиться к вашему персональному компьютеру с IP адресом 192.168.1.2 из сети Интернет (подробности читайте во врезке о службе NAT). Но, в тоже время, вы всегда можете обратиться к публичному IP адресу вашего модема, получаемого из пула IP адресов провайдера. Для чего это можно применить? А очень просто. Совместно со службой NAT можно настроить проброс портов, открытых на WAN интерфейсе модема, во внутреннюю сеть на определенный персональный компьютер и, таким образом, получить доступ к Игровому, HTTP или FTP серверу. Да и не только к ним, а к любому порту, используемому сетевым приложением на вашем персональном компьютере. Именно для реализации всего этого применяется служба Port Forwarding.

Порт – точка входа в сетевое приложение, применяемое для отделения данных одного приложения от данных предназначенных для другого приложения, совместно исполняемых в данный момент на персональном компьютере. Порты могут подразделяться на UDP и TCP, т.е. зависеть от транспортного протокола. Значения портов могут принимать значения 0-65535, множество портов зарезервировано за определенными приложениями. Например, 21/TCP порт для службы FTP, 6881/TCP и 6881/UDP порты для P2P сети BitTorrent. Со списком портов используемых различными приложениями можно ознакомится по данному адресу: www.iana.org/assignments/port-numbers

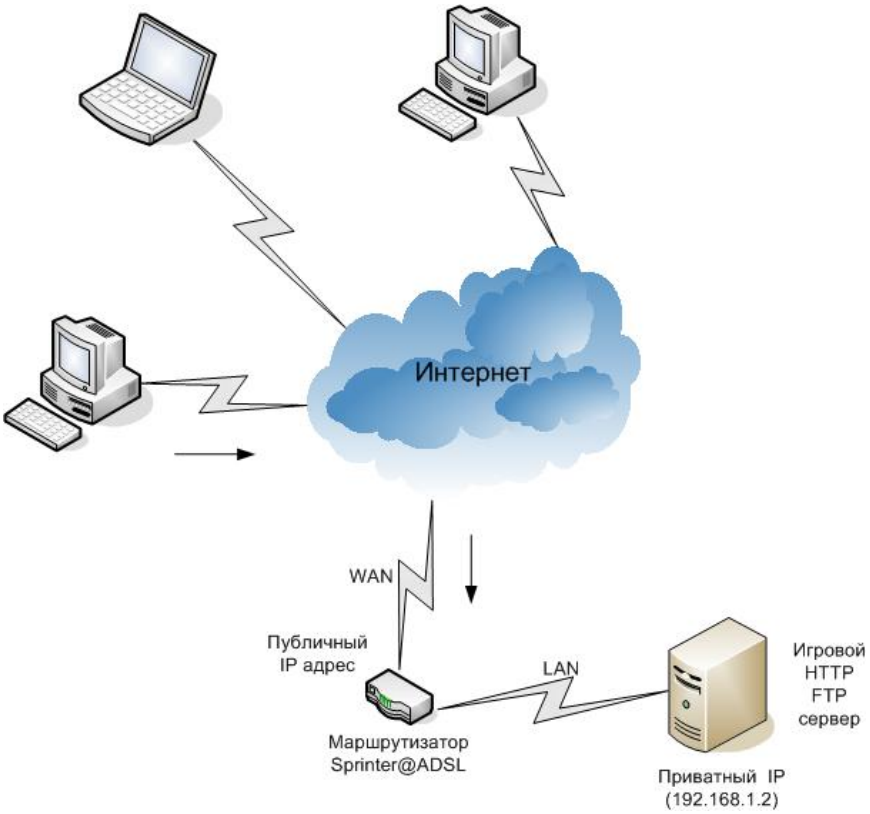

Рис. 2

II. Резервирование IP-адреса

Перед настройкой службы Port Forwarding необходимо произвести резервирование IP-адреса вашего персонального компьютера в маршрутизаторе Acorp Sprinter@ADSL.

1. Нажмите кнопку Пуск / Выполнить и запустите команду *cmd*. Откроется окно командной строки, в котором необходимо выполнить команды (Рис. 3):
   Ipconfig /release
   Ipconfig /renew

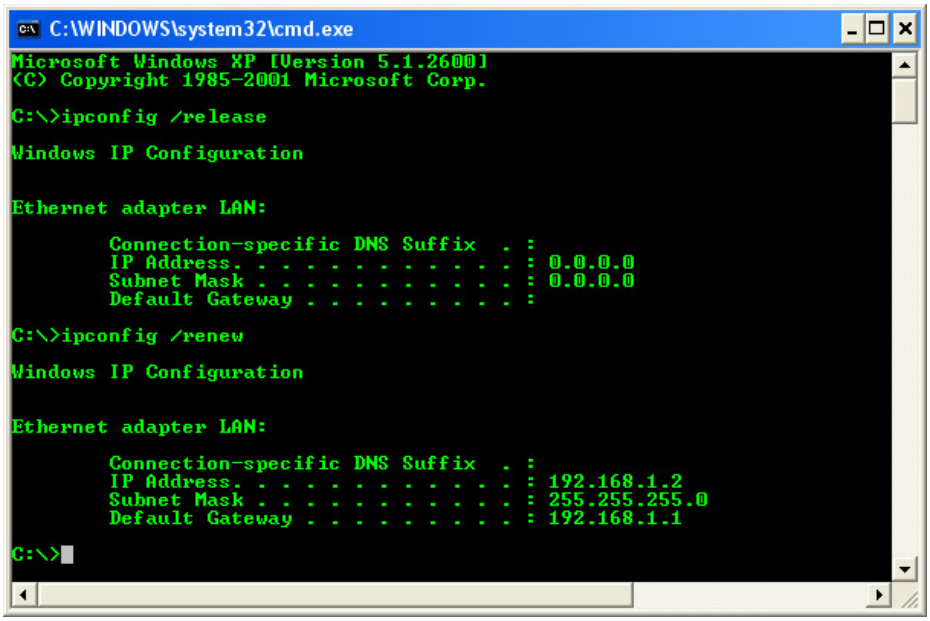

Рис. 3

2. Откройте Интернет браузер и введите в адресной строке адрес *192.168.1.1*, тем самым вы получите доступ к ВЕБ-интерфейсу маршрутизатора. После авторизации перейдите на закладку **ADVANCED** и выберите пункт меню **LAN Clients** (Рис. 4)

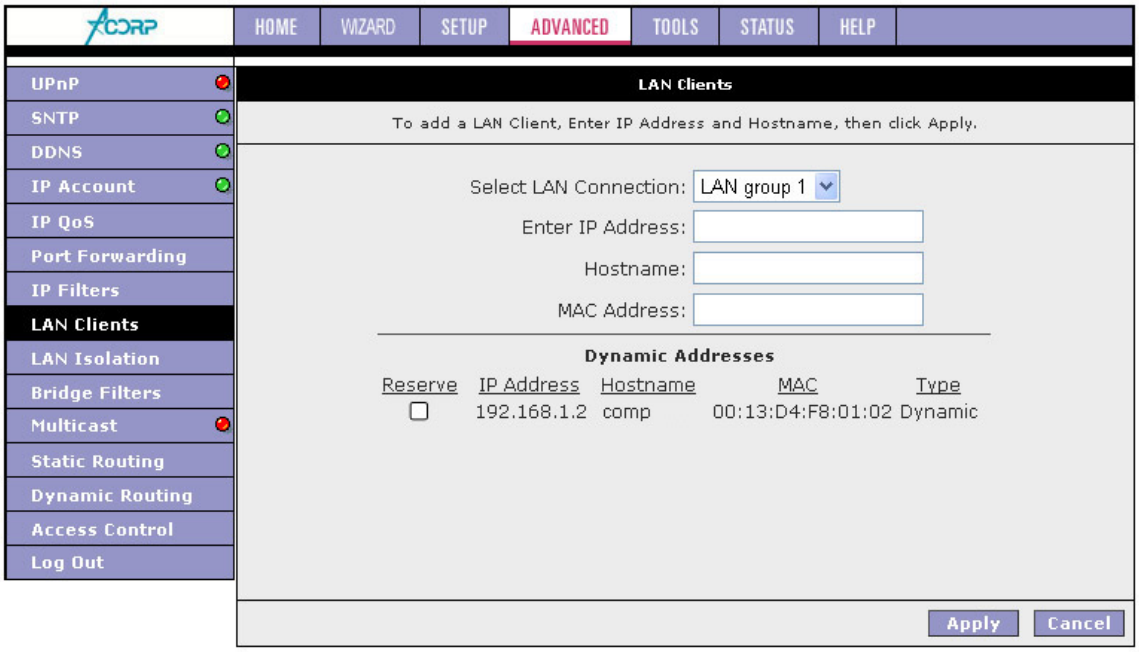

Рис. 4

3. В открывшемся окне установите галочку напротив резервируемого IP-адреса для службы Port Forwarding и нажмите **Apply** (Рис. 5)

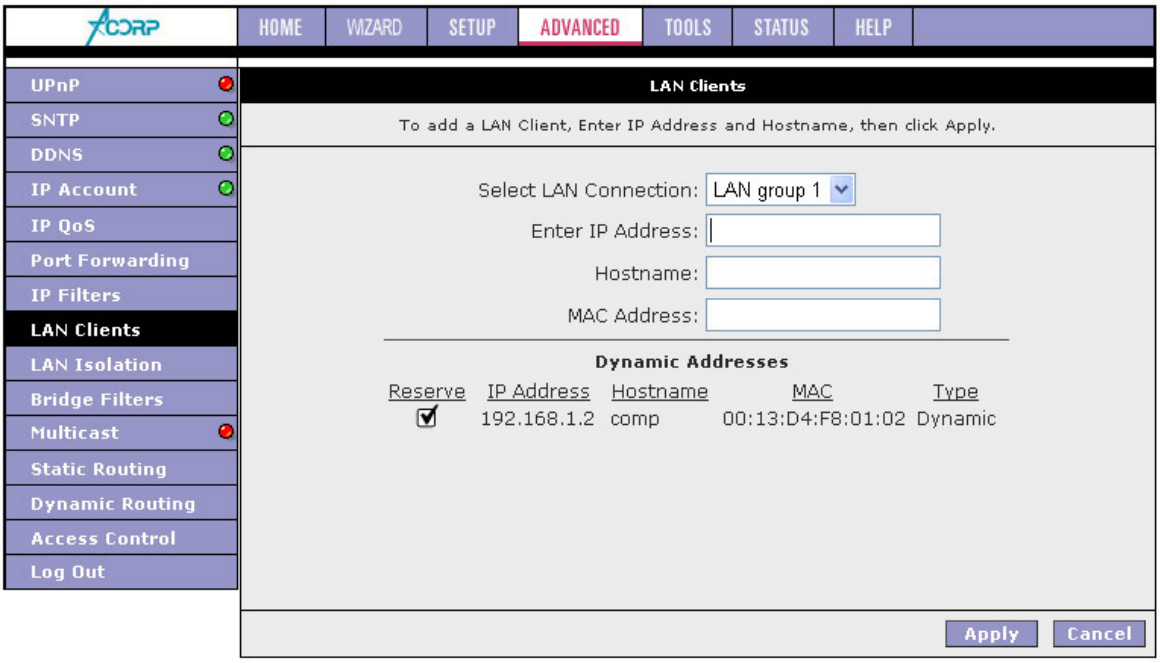

Рис. 5

4. Результатом резервирования IP-адреса будет перевод данного IP-адреса в разряд статических IP-адресов, что позволит маршрутизатору всегда выдавать указанному персональному компьютеру данный IP-адрес. Это действие очень важно для возобновления работы службы Port Forwarding после перезагрузки маршрутизатора (Рис. 6)

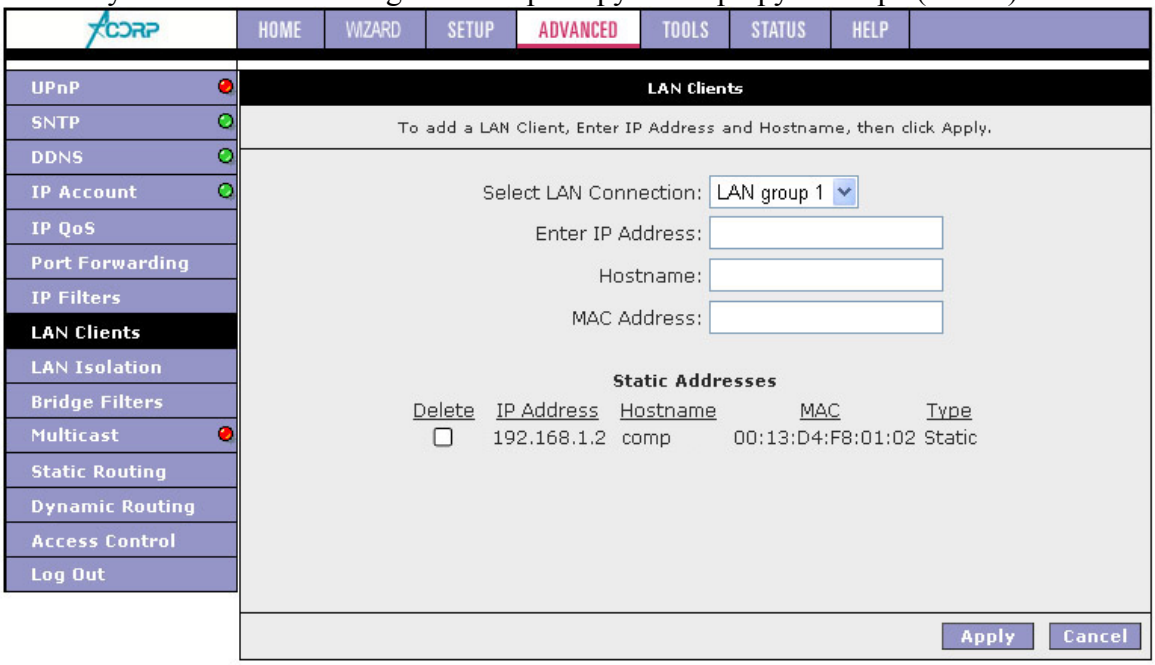

Рис. 6

III. Настройка правил службы Port Forwarding

Перейдем к настройке правил службы Port Forwarding в маршрутизаторе Acorp Sprinter@ADSL.

1. На закладке **ADVANCED** ВЕБ-интерфейса маршрутизатора выберите пункт меню **Port Forwarding** (Рис. 7).

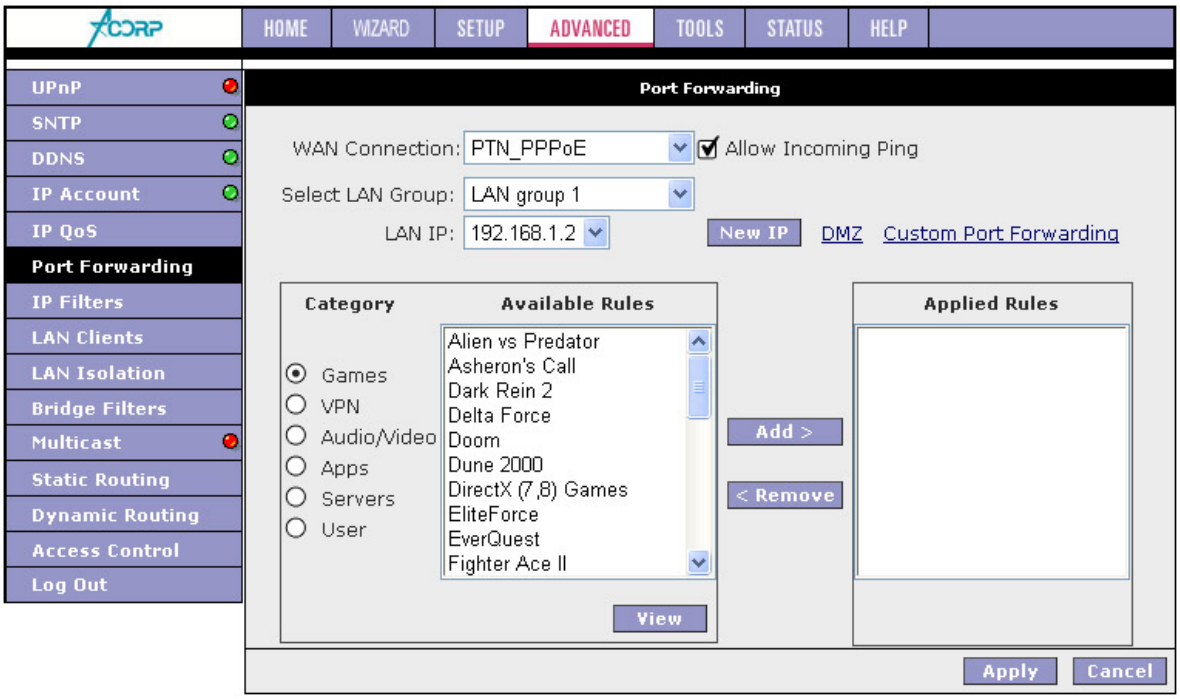

Рис. 7

Данную закладку условно можно разделить на три части:

- WAN подключение, Сетевая группа и IP-адрес, для которого назначаются правила Port Forwarding;
- Предустановленные производителем правила и созданные пользователем;
- Используемые в данный момент правила.

Для назначения правил Port Forwarding необходимо выбрать WAN Connection, т.е. подключение, используемое для доступа в Интернет, а также LAN Group и LAN IP, для которого назначается правило. Далее среди предустановленных правил необходимо выбрать правило, которое подходит для открытия порта сетевого приложения.
Рассмотрим случай, в котором вам требуется открыть доступ для Игрового сервера игры Half-Life или Counter-Strike. В этом случае вам необходимо в предустановленных правилах выбрать правило Half Life (Рис. 8).

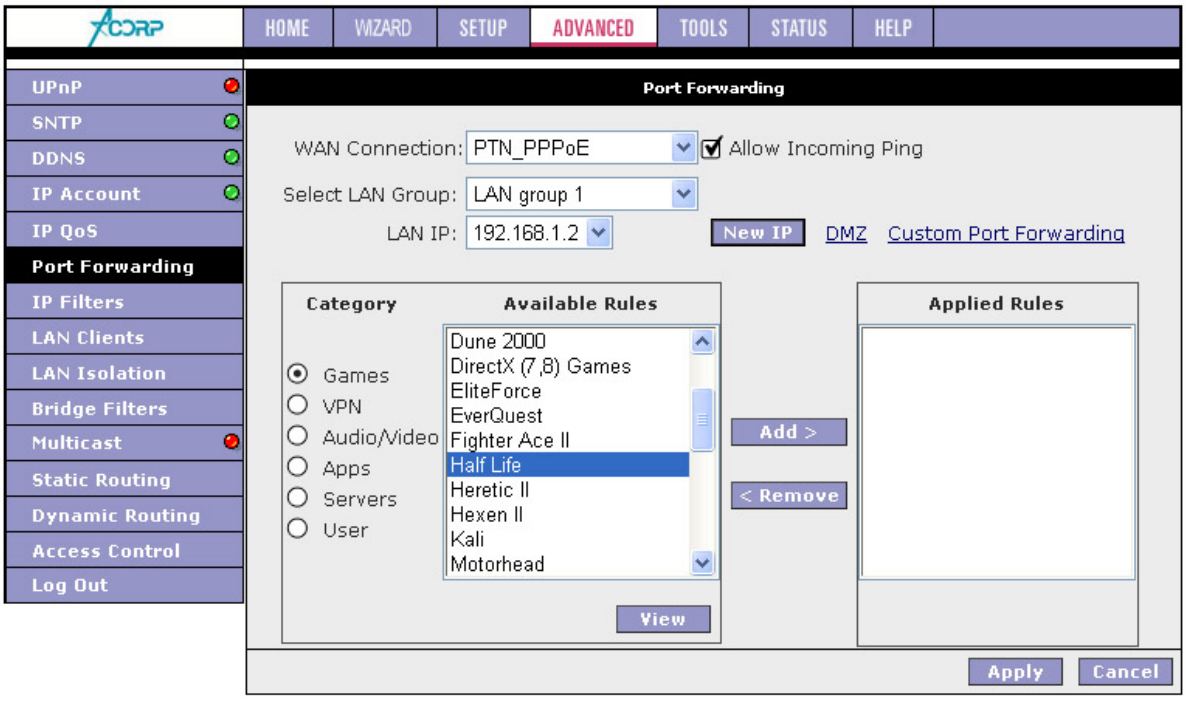

Рис. 8

После того как выбрано правило, необходимо нажать на кнопку **Add>** и в результате правило будет добавлено в список используемых правил (Рис. 9).
В случае необходимости удаления правила из списка используемых, воспользуйтесь кнопкой **<Remove**.

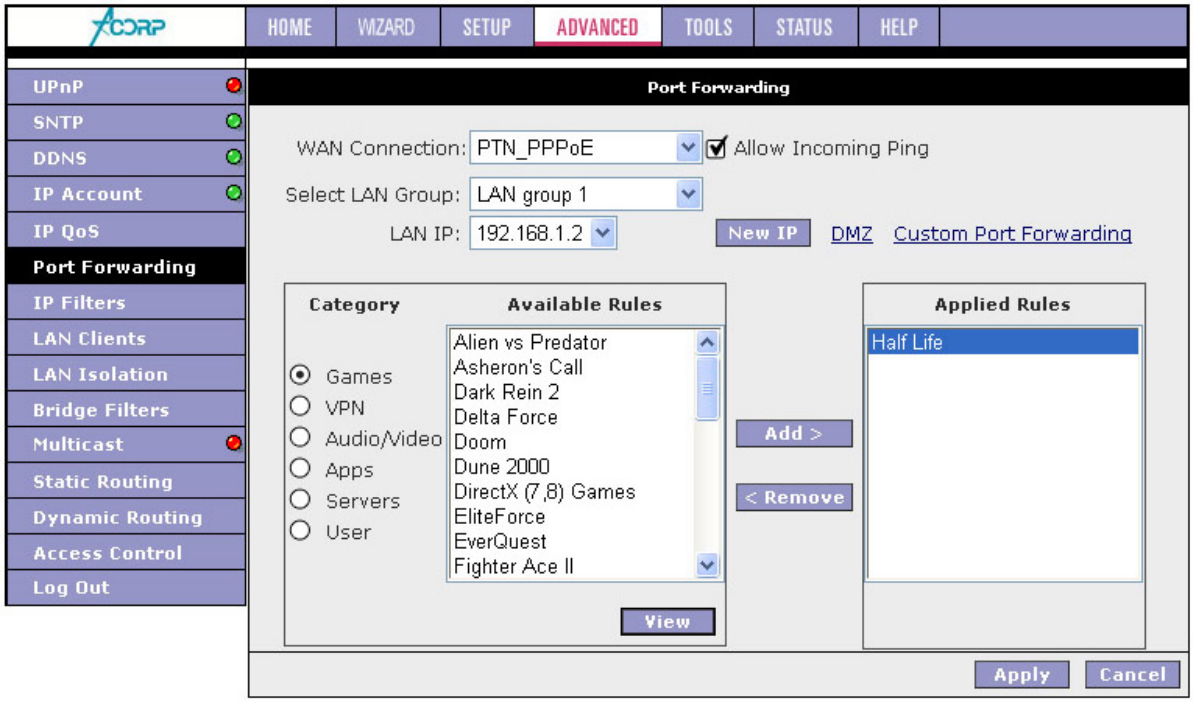

Рис. 9

Для подтверждения назначения используемых правил нажмите клавишу **Apply**.

2. Рассмотрим случай, когда в списке предустановленных правил не обнаружено требуемое правило открытия портов для вашего сетевого приложения, и его необходимо создать вручную. Для примера, рассмотрим случай размещения в локальной сети сервера HTTP, на котором предполагается разместить домашнюю страничку. Для создания своего правила выберите в разделе предустановленных правил подраздел **User** (Рис. 10).

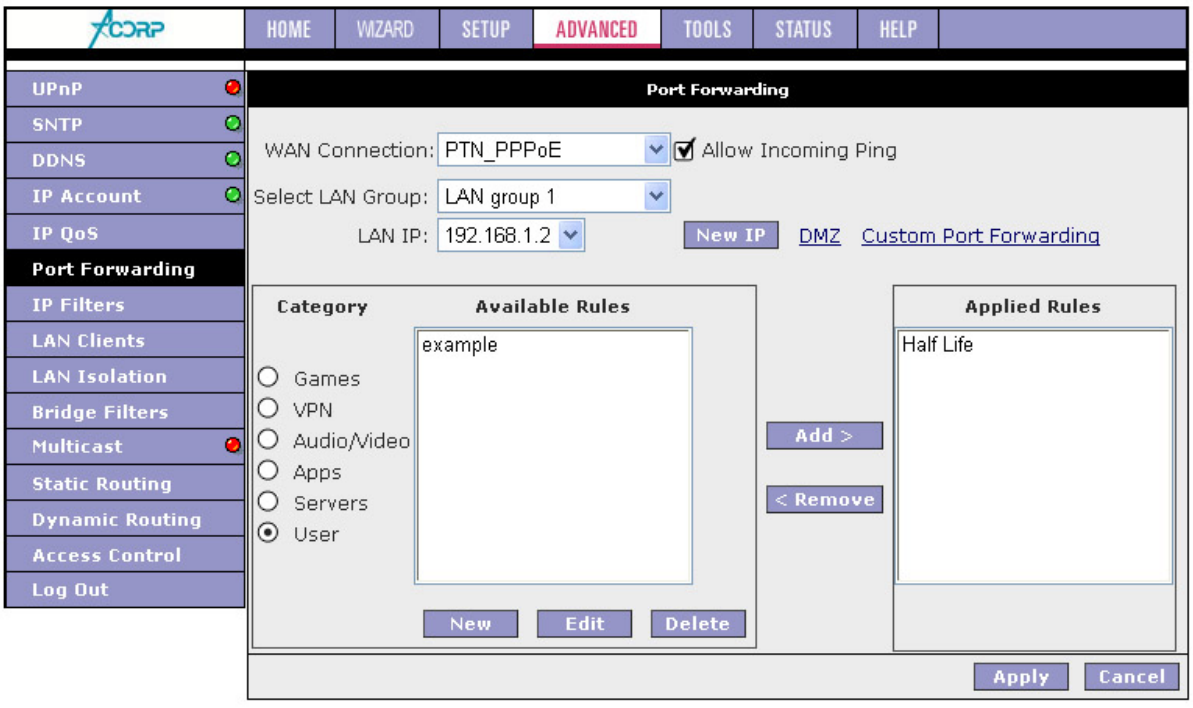

Рис. 10

Далее нажмите кнопку **New** и в открывшемся окне в поле **Rule Name** введите имя создаваемого правила (в нашем примере HTTP). В поле **Protocol** выберете требуемый вашему сетевому приложению сетевой протокол (в нашем примере TCP). В поле **Port Start** укажите начальный внешний порт диапазона открываемых портов (в нашем примере 80). В поле **Port End** укажите последний внешний порт диапазона открываемых портов (в нашем примере 80). В поле **Port Map** укажите порт назначения, на который служба Port Forwarding будет перенаправлять весь трафик, приходящий на диапазон внешних портов указанных в полях **Port Start** и **Port End** (в нашем примере 80) (Рис. 11).

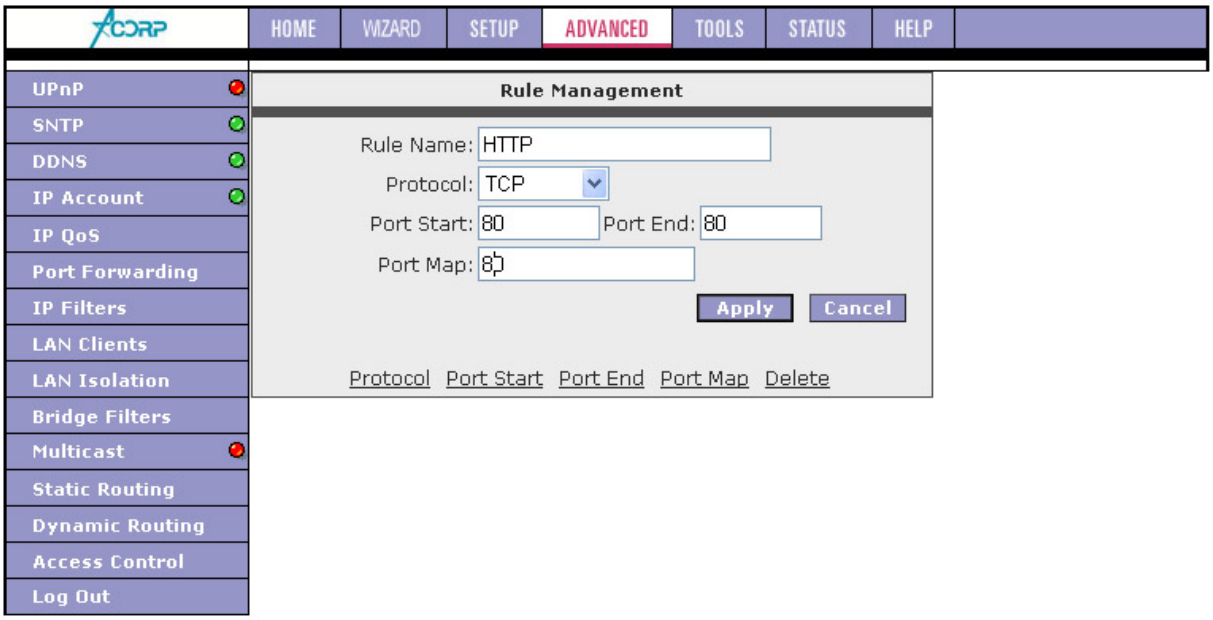

Рис. 11

После заполнения всех полей необходимо нажать кнопку **Apply**.
Результатом создания нашего правила будет следующее. Весь сетевой трафик, приходящий на внешний порт маршрутизатора (в нашем примере 80), будет перенаправлен на порт 80 персонального компьютера (с IP-адресом 192.168.1.2, на который будет далее назначено правило), находящегося в локальной сети за маршрутизатором (Рис. 12). По сути, для просмотра вашей домашней странички вы обращаетесь на внешний IP-адрес маршрутизатора, выданный вашим провайдером. А маршрутизатор все запросы пересылает на сервер HTTP в локальной сети, а уже сервер формирует вашу страничку и дает ответ маршрутизатору, который передает вам, т.е. он работает как посредник. По аналогии формируются правила для любых сетевых приложений.

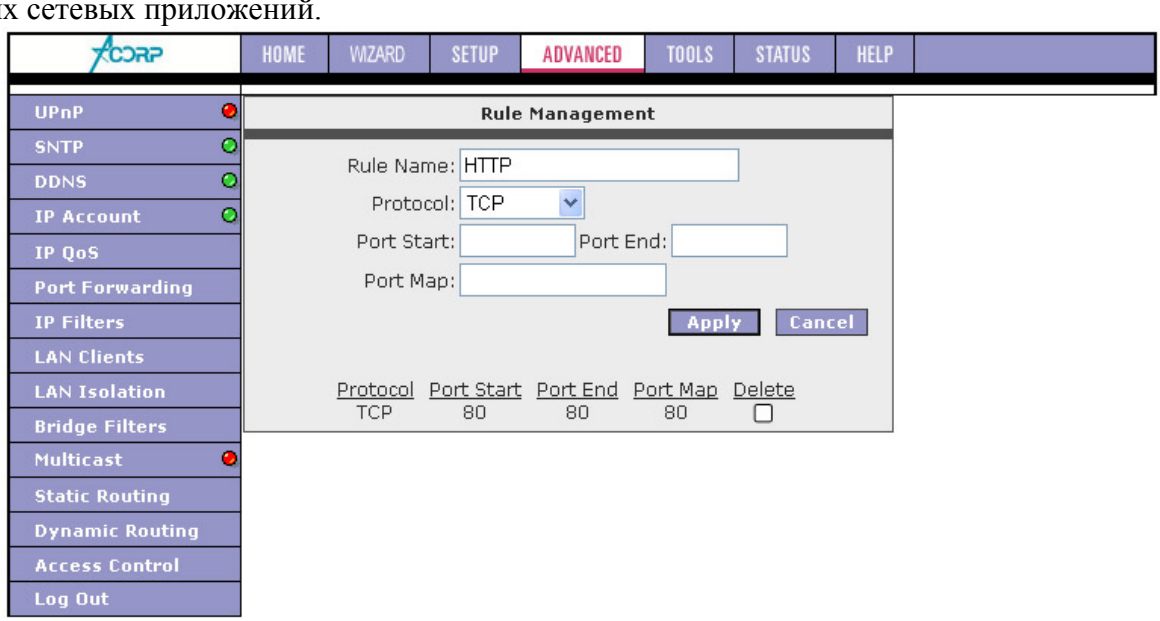

Рис. 12

При необходимости перенаправления дополнительных портов в рамках данного правила повторите описанную процедуру заполнения полей **Protocol, Port Start, End и Map** и нажмите **Apply**.

В случае нашего примера в этом нет необходимости, поэтому вернемся в раздел **Port Forwarding** ВЕБ-Интерфейса маршрутизатора и откроем подзакладку **User**, предустановленных и пользовательских правил, и обнаружим созданное ранее правило HTTP (Рис. 13).

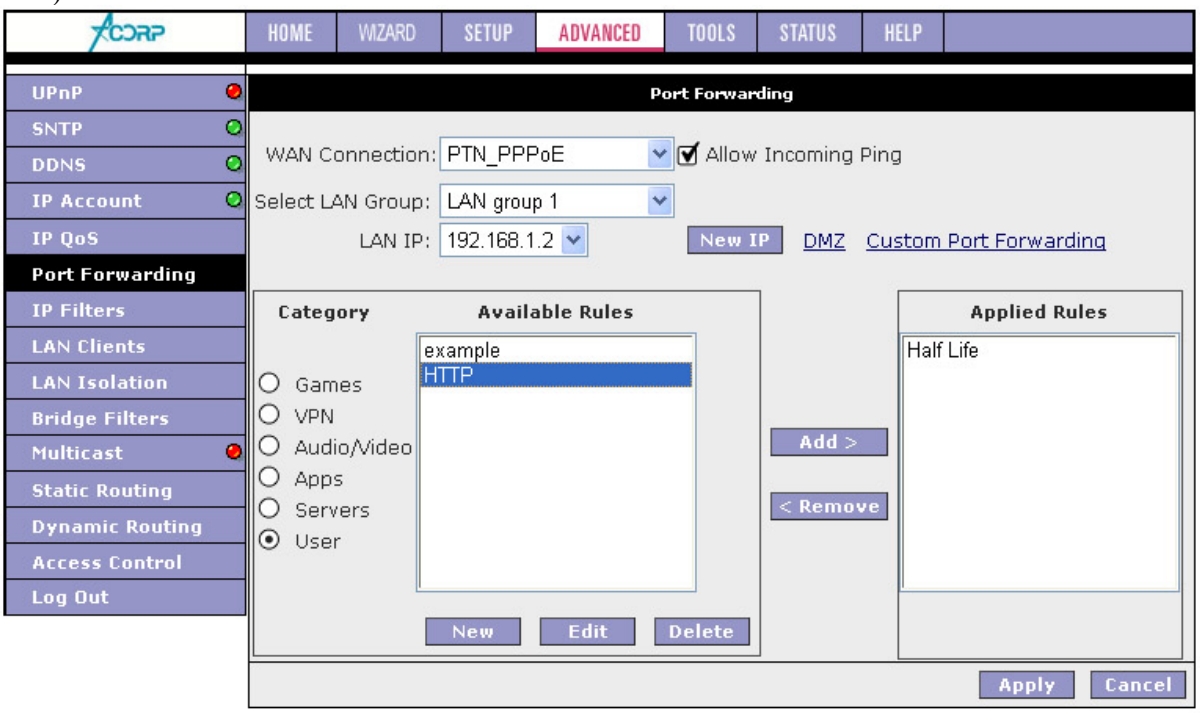

Рис. 13

Выберите требуемые: WAN Connection, LAN Group, LAN IP (IP-адрес, для которого будет использовано данное правило), а также правило HTTP и нажмите кнопку **Add>**(Рис. 14).

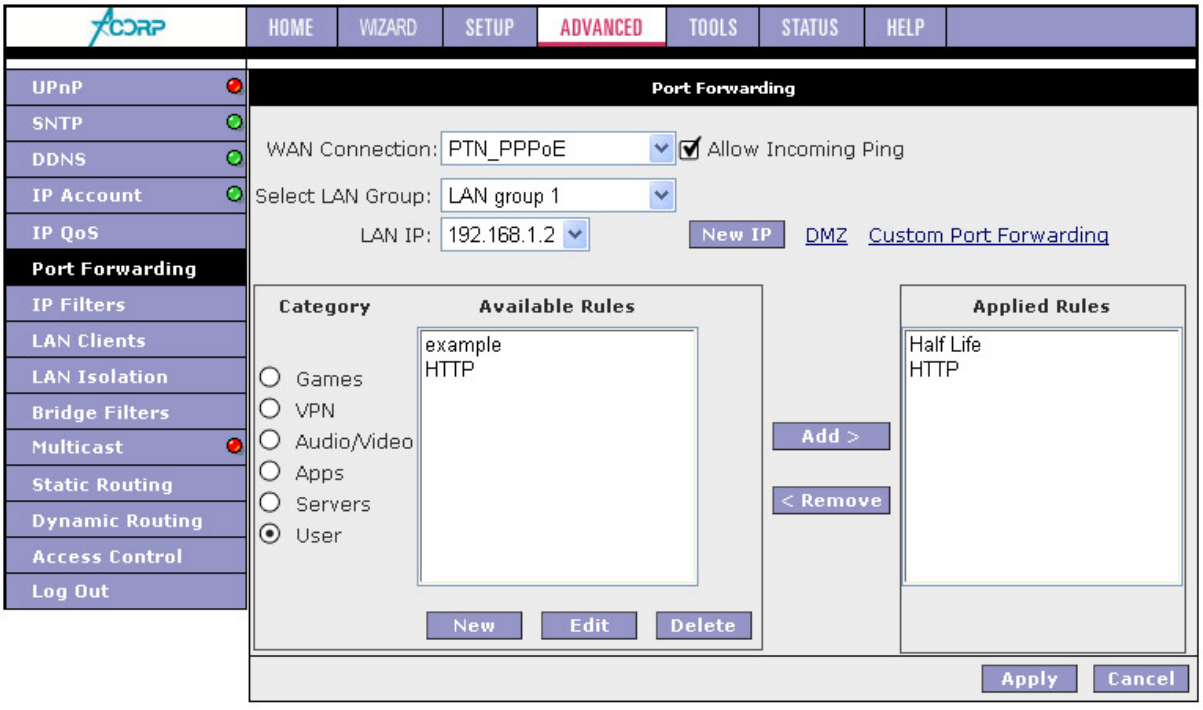

Рис. 14

Для подтверждения назначения используемых правил нажмите клавишу **Apply**.

3. Результат назначения правил службы Port Forwarding можно просмотреть в журнале маршрутизатора. На закладке **STATUS** ВЕБ-интерфейса маршрутизатора выберите пункт меню **System Log** (Рис.15)

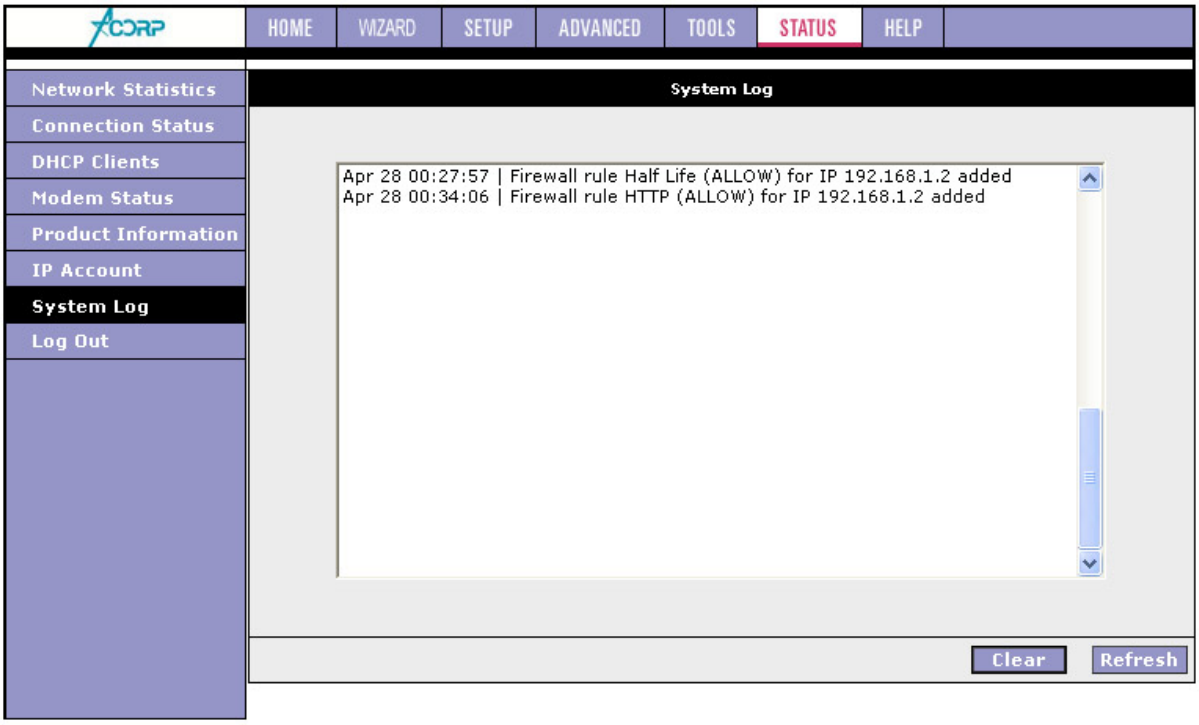

Рис. 15

4. После выполнения всех настроек, связанных с **Port Forwarding** и **LAN Clients,** обязательно необходимо сохранить все настройки путем выполнения команды **Save All** на закладке **TOOLS**, пункт меню **System Commands**. В противном случае, после отключения питания или перезагрузки маршрутизатора все настройки будут утрачены.