# Мультипротокольные маршрутизаторы и коммутаторы пакетов NPS–7e, NSG–500, NX–300, NSG–800

## (Базовое программное обеспечение)

## Руководство пользователя

## Часть 4
## IP-маршрутизация

Версия программного обеспечения 8.2.4

Обновлено 05.02.2013

Москва 2013

# АННОТАЦИЯ

Данный документ содержит руководство по настройке и применению мультипротокольных маршрутизаторов и коммутаторов пакетов компании NSG. Документ относится к продуктам серий NPS–7e, NSG–500, NX–300, NSG–800, основанным на аппаратной платформе Motorola MC68EN302, MC68EN360, MPC 855T/860 и базовом программном обеспечении NSG. Руководства по применению других продуктов NSG, а также альтернативной версии программного обеспечения NSG Linux, содержатся в отдельных документах.

Данное руководство состоит из следующих разделов:



Четвертая часть руководства посвящена настройке стека TCP/IP и связанных с ним (исключительно или преимущественно) протоколов канального уровня. При описании процедур конфигурации предполагается предварительное знакомство с материалом частей 1–3 данного руководства. Для настройки мультипротокольных режимов, например, передачи трафика IP по сети Frame Relay, необходимо также знакомство с соответствующими разделами частей 6 и 7.

Настройка прикладных служб IP для передачи данных и для управления — Telnet, XOT, Web, SNMP — рассмотрена в части 5. В отдельную часть 8 вынесены вопросы, связанные с аутентификацией, авторизацией и статистикой и также универсально применимые к различным протокольным стекам.

**ВНИМАНИЕ** Продукция компании непрерывно совершенствуется, в связи с чем возможны изменения отдельных аппаратных и программных характеристик по сравнению с настоящим описанием. Сведения о последних изменениях приведены в файлах README.TXT, CHANGES, а также в документации на отдельные устройства.

Замечания и комментарии по документации NSG принимаются по адресу: doc@nsg.net.ru.



ООО "Эн-Эс-Джи"
Россия 105187 Москва
ул. Кирпичная, д.39, офис 1302
Тел.: (+7–495) 918–32–11
Факс: (+7–495) 918–27–39

http://www.nsg.ru/
mailto:info@nsg.net.ru
mailto:sales@nsg.net.ru
mailto:support@nsg.net.ru

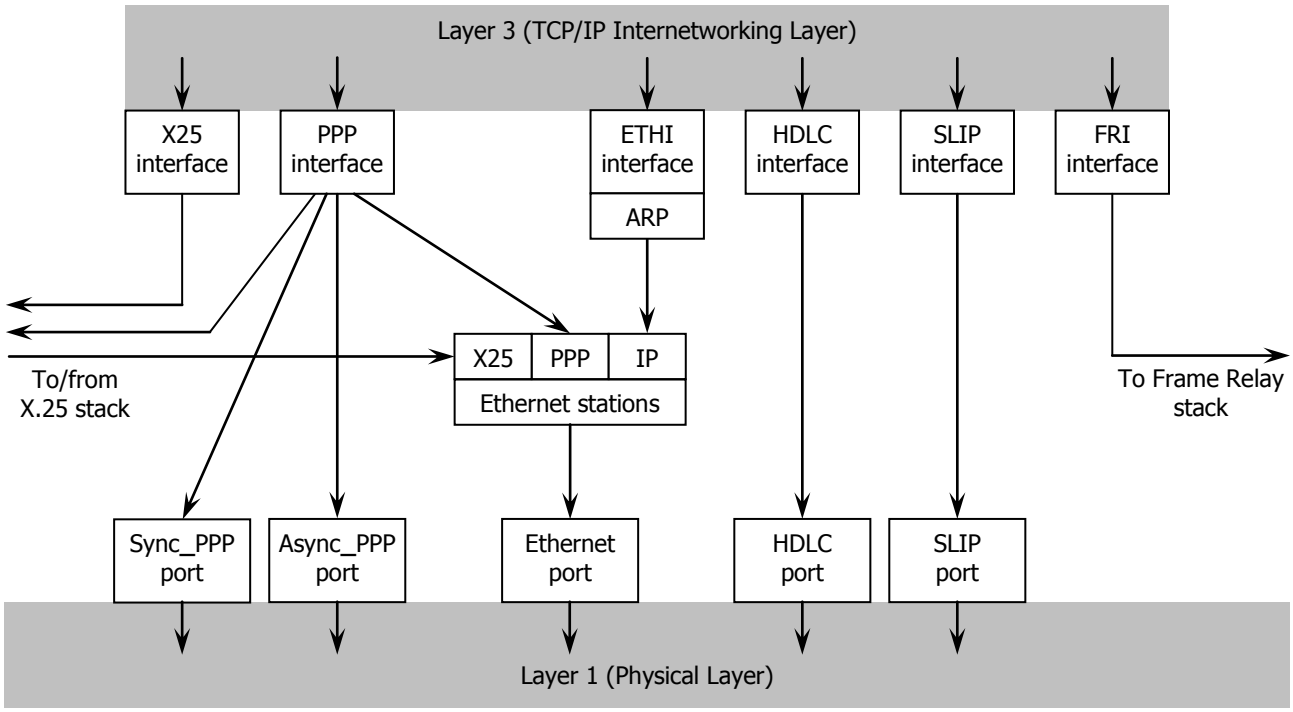
# § СОДЕРЖАНИЕ §

## Часть 4. IP-маршрутизация

# §4.1. Объекты и протоколы канального уровня

## §4.1.1. Структура канального уровня TCP/IP в устройствах NSG

Канальный уровень подсистемы TCP/IP в устройствах NSG включает в себя три типа программных объектов: порты, IP-интерфейсы и станции. Физические порты связывают канальный уровень с физическим, если на физическом уровне используются простые однопортовые интерфейсы. Логические порты выполняют эту же функцию, но применительно к настраиваемым многопортовым физическим интерфейсам. IP-интерфейсы связывают канальный уровень с сетевым. Станции являются промежуточными объектами и служат для перенаправления трафика между различными интерфейсами и портами.




Структура канального уровня стека TCP/IP в устройствах NSG

Хотя стандарты и спецификации TCP/IP не определяют канальный уровень явным образом, на практике существует ряд протоколов, применяемых исключительно или преимущественно для передачи IP-трафика. По этой причине их удобно рассматривать как часть подсистемы TCP/IP устройства. К таким протоколам относятся PPP, SLIP, Cisco-HDLC и Ethernet. Передача IP-трафика по сетям Frame Relay и X.25 требует настройки, помимо стека TCP/IP, также и соответствующих служб для этих сетей.

Настройка физических и логических портов со стороны физического уровня подробно описана в Части 3 настоящего руководства. В дальнейшем предполагается, что физические соединения настроены и работоспособны.

Следующая задача состоит в настройке объектов канального уровня подсистемы TCP/IP. Она включает в себя:

1. Настройку параметров канального уровня для физических и логических портов.
2. Настройку станций типа IP и PPP.
3. Настройку параметров канального уровня для IP-интерфейсов маршрутизатора.
4. Установление связей между этими объектами каким-либо из следующих способов:
   — статически в процессе настройки (параметром PO или ET)
   — статически при помощи PVC в сетях Frame Relay и X.25
   — при помощи правил маршрутизации для динамического установления SVC в сетях X.25.
5. Настройку параметров сетевого уровня для IP-интерфейсов маршрутизатора.

Первые четыре задачи имеют свои особенности для каждого из протоколов канального уровня. Последняя, наоборот, уже освобождена от специфики используемых протоколов (или мультипротокольного транспорта) и определяет характеристики каждого интерфейса и маршрутизатора в целом как элементов IP-сети.

### §4.1.2. Команды для настройки объектов канального уровня

Все настройки IP-интерфейсов, портов и станций Ethernet и Frame Relay производятся командой Set Parameters, соответственно:

```
S P IP:<номер>
S P PO:<номер>
S P ET:<номер>
S P ST:<номер>
```

Изменения конфигурации портов вступают в силу после рестарта данного порта (или всех портов); конфигурации IP-интерфейсов вступают в силу после рестарта данного интерфейса или всего маршрутизатора, соответственно:

```
W S PO:<номер>          W S IP:<номер>
W S PO:A                W S IP:0
```

Для рестарта станции Ethernet и Frame Relay следует рестартовать порт, к которому они привязаны. При этом одновременно рестартуют IP-интерфейсы, привязанные к этим станциям. При рестарте порта типа HDLC также рестартует привязанный к нему IP-интерфейс.

Для просмотра параметров отдельного IP-интерфейса, порта, станции или всех объектов данного типа используется команда Display Parameters:

```
D P IP:<номер>    D P PO:<номер>    D P ET:<номер>    D P ST:<номер>
D P IP:A          D P PO:A          D P ET:A          D P ST:A
```

Перед конфигурацией IP-интерфейсов необходимо определить, как минимум, один параметр маршрутизатора как целого: максимальное число IP-интерфейсов. Оно задается параметром NUM и может принимать значения от 1 до некоторого максимального значения, специфичного для данной модели устройства и версии программного обеспечения. IP-интерфейсы, конфигурация которых рассмотрена в следующих параграфах, могут иметь номера от 1 до NUM.

Для управления всем IP-маршрутизатором в устройствах NSG используется формальный объект, называемый *локальным псевдоинтерфейсом*. Большинство его параметров относятся к сетевому и прикладному уровням, т.е. к последней из задач, перечисленных в предыдущем параграфе. Поэтому подробно его конфигурация будет рассмотрена ниже. На данном этапе конфигурации существенны только две команды, связанные с ним:

```
S P IP:0 NUM:<число>
W S IP:0
```

Как можно видеть, за локальным псевдоинтерфейсом закреплен специальный номер 0. Первая команда устанавливает количество реальных IP-интерфейсов (по умолчанию — один). Изменения конфигурации маршрутизатора вступают в силу после рестарта локального псевдоинтерфейса (вторая команда).

### §4.1.3. Настройка протокола SLIP

SLIP является простейшим из протоколов канального уровня, и его настройка требует наименьших усилий. Для работы протокола SLIP необходимо:

— Настроить физический порт с асинхронным интерфейсом V.24 или UART и назначить ему тип SLIP. Дополнительных настроек канального уровня для данного типа портов не требуется. Формат асинхронных данных для него — всегда 8, none, 1.

— Назначить IP-интерфейсу тип SLIP и привязать его к физическому порту параметром PO:<номер>.

Пример конфигурации (включая настройку физического интерфейса):

```
S P PO:2 TY:SLIP IF:V24 SP:19200
S P IP:1 TY:SLIP PO:2
W S PO:2
```

### §4.1.4. Настройка протокола Cisco-HDLC

Протокол Cisco-HDLC предназначен для передачи трафика IP по синхронным соединениям "точка-точка". Для работы протокола Cisco-HDLC необходимо:

— Настроить физический порт с любым синхронным интерфейсом (IF:V24, V35, RS530, X21, SRM, xDSL, C1_xxx, G703, G703_1, E1) и назначить ему тип HDLC. Для данного типа порта существует один специфический параметр TA — интервал между посылкой пакетов KeepAlive (в формате Cisco-HDLC). Допустимые значения этого параметра — от 0 (сообщения не посылаются) до 65535 секунд.

— Назначить IP-интерфейсу тип HDLC и привязать его к физическому порту параметром PO:<номер>.

Пример конфигурации (включая настройку физического интерфейса):

```
S P PO:2 TY:HDLC IF:V35 MODE:EXT SP:2048000
S P IP:1 TY:HDLC PO:2
W S PO:2
```

Рестарт интерфейса в данном случае не требуется, при рестарте порта типа HDLC связанный с ним IP-интерфейс рестартует автоматически.

### §4.1.5. Настройка протокола Ethernet

Для приема/передачи трафика IP по локальной сети Ethernet необходимо:

— Настроить порт Ethernet (TY:ETH).

— Назначить Ethernet-станцию тип IP и привязать ее к физическому порту. Станции нумеруются последовательно от 0 до максимального номера, допустимого для данной модели устройства и версии программного обеспечения. При необходимости можно указать формат пакетов для данной станции:

| | |
|---|---|
| FRTY:Ethernet | формат Ethernet (по умолчанию) |
| FRTY:EtherSNAP | формат IEEE 802.3 |

— Назначить IP-интерфейсу тип ETHI и привязать его к Ethernet-станции параметром ET:<номер>.

Каждая Ethernet-станция должна быть привязана к некоторому физическому порту типа ETH. Один порт Ethernet может обслуживать одну станцию типа IP, одну станцию типа PPP и несколько станций типа X25 и/или FR одновременно. Все эти станции имеют один MAC-адрес.

Каждый IP-интерфейс типа ETHI должен быть привязан к некоторой Ethernet-станции типа IP. Каждая станция может обслуживать только один интерфейс.

**ПРИМЕЧАНИЕ** В версиях программного обеспечения до 7.6.5 включительно допускалось создание на одном порту Ethernet 10Base–T (но не 10/100Base–T) *нескольких* Ethernet-станций типа IP. Станциям назначались последовательные MAC-адреса, начиная с адреса, присвоенного порту. К каждой из них можно было привязать свой IP-интерфейс и получить, таким образом, несколько подсетей IP в одной физической сети Ethernet. Начиная с версии 8.0.0b, этот механизм заменен более универсальной функцией назначения вторичных IP-адресов (*aliases*) непосредственно IP-интерфейсам.
Ethernet-станции типа X25 в любом случае используют один MAC-адрес.

**ПРИМЕЧАНИЕ** В вышеописанном правиле, однако, сохраняется одна небольшая лазейка. На одном порту Ethernet можно создать две станции типа IP и две независимые подсети, если одна из них использует формат кадров Ethernet, а другая — формат EtherSNAP.

Пример конфигурации (включая настройку физического интерфейса):

```
S P PO:3 TY:ETH IF:TP MODE:HALF SP:10000000 ADDR:00.09.56.02.00.8C
S P ET:0 TY:IP PO:3
S P IP:1 TY:ETHI ET:0
W S PO:3
```

Рестарт интерфейса в данном случае не требуется, при рестарте порта типа ETH рестартуют все связанные с ним станции и IP-интерфейсы.

Число Ethernet-станций фиксировано в каждом устройстве и в каждой версии программного обеспечения. Для неиспользуемых станций следует установить TY:NOCONF.

**ПРИМЕЧАНИЕ** Настройка инкапсуляции PPPoE описана в §4.1.9. Использование инкасуляций Frame Relay-over-Ethernet и X.25-over-Ethernet рассмотрено в Части 6 и Части 7, соответственно.

### §4.1.6. Настройка протокола PPP

PPP — наиболее гибкий и многовариантный протокол для передачи IP-трафика по соединениям "точка-точка", поэтому его конфигурация содержит наибольшее число параметров. Для работы протокола PPP в простейшей конфигурации необходимо:

— Настроить физический порт с любым синхронным или асинхронным интерфейсом и назначить ему тип SYNC_PPP или ASYNC_PPP, соответственно. Дополнительных настроек канального уровня для данных типов портов не требуется. Формат асинхронных данных для порта ASYNC_PPP — 8, none, 1. (При необходимости контроль четности и число стоп-битов могут быть изменены; число бит данных для протокола PPP всегда 8.)

— Назначить IP-интерфейсу тип PPP, настроить для него параметры канального уровня (см. ниже) и привязать его к физическому порту параметром PO:<номер>.

При статической конфигурации интерфейс может выступать в роли как инициатора соединения (клиента), так и отвечающей стороны (сервера).

Помимо этого, для интерфейсов типа PPP возможна динамическая привязка, задаваемая параметром

PO:AUTO

В этом случае интерфейс не связывается немедленно с каким-либо объектом канального уровня, а находится в состоянии ожидания до тех пор, пока не поступит вызов PPP, адресованный либо данному интерфейсу, либо IP-маршрутизатору в целом (тогда используется первый свободный интерфейс с такой конфигурацией). Динамическая привязка возможно только для интерфейса, работающего в режиме сервера. Вызов от клиента может поступить через следующие объекты:

— Асинхронный физический порт, сконфигурированный как порт типа ASYNC с авторизацией. При подключении к порту пользователь должен ввести имя и пароль; по результатам аутентификации ему предоставляется сервис PPP либо PAD. В первом случае порт принимает тип ASYNC_PPP и связывается со свободным интерфейсом маршрутизатора. Подробно о динамической конфигурации асинхронных портов см. Часть 8.

— Ethernet-станцию типа PPP. Подробно об инкапсуляции PPP-over-Ethernet (PPPoE) см. §4.1.9.

— Логический канал порта или станции X.25, вызов с которых направлен коммутатором X.25 на интерфейсы PPP. Подробно об инкапсуляции PPP-over-X.25 см. §4.1.8.

Параметры канального уровня для интерфейса типа PPP можно разделить на несколько функциональных групп, соответствующих фазам установки PPP-соединения.

**а) Установление и разрыв соединения на физическом уровне:**

Функция данного интерфейса в PPP-соединении определяется параметром SL (SiLent):

| | |
|---|---|
| SL:YES | Режим сервера: сеанс PPP начинается по инициативе удаленной стороны. |
| SL:NO | Режим клиента и сервера: интерфейс сам инициирует сеанс PPP-соединения, а также может принимать запросы на начало сеанса PPP от удаленной стороны. |

Если интерфейс работает в режиме клиента (SL:NO), то он может либо поддерживать физическое соединение постоянно, либо устанавливать его по требованию. Этот режим выбирается параметром DOD (Dial On Demand):

| | |
|---|---|
| DOD:YES | Соединение инициализируется, только если IP-маршрутизатор начинает передавать данные через этот интерфейс. Используется, как правило, для соединений с модемными пулами корпоративных сетей или поставщиков услуг Интернет по коммутируемым линиям. Кроме того, если устанавливается физическое соединение, интерфейс может отвечать на входящие запросы на установление PPP-соединений. |
| DOD:NO | Соединение инициализируется при старте IP-интерфейса. Данный режим предназначен для соединений по выделенным линиям, либо с выделенными модемами поставщика услуг или корпоративной сети. |

**ПРИМЕЧАНИЕ** Не рекомендуется использовать режим SL:NO DOD:NO, если предуматривается возможность ответа на входящие запросы. Для отвечающего устройства следует установить режим сервера (SL:YES) либо режим соединений по требованию (SL:NO DOD:YES).
Исключением является случай подключения клиента Windows по нуль-модемному кабелю или выделенной линии. В этом случае необходимо использовать на клиенте файл настроек MDMNSG.INF и установить на сервере именно SL:NO DOD:NO.

Далее, если интерфейс работает в режиме клиента с установлением соединения по требованию (DOD:YES), то для управления модемом (или другой аппаратурой связи) может использоваться параметр DTR (DTR control). Как следует из названия, этот параметр управляет сигналом DTR в зависимости от состояния PPP-соединения:

DTR:0 — DTR установлен только при наличии или инициализации PPP-соединения. Данный режим актуален для некоторых типов аппаратуры передачи данных (например, спутниковых модемов), которые безусловно начинают устанавливать физическое соединение при поднятии сигнала DTR. Установка DTR:0 запрещает такому модему устанавливать связь до тех пор, пока этого не потребует IP-интерфейс.

DTR:1 — При разрыве PPP-соединения DTR падает на 2 сек, затем снова устанавливается. Этот режим подходит для большинства случаев и актуален, если модем должен как инициировать соединения по требованию, так и отвечать на входящие звонки.

В остальных случаях при активном IP-интерфейсе сигнал DTR поднят всегда и сбрасывается на 2 сек. только при разрыве соединения.

**ПРИМЕЧАНИЕ** Реакция модема на изменения сигнала DTR может быть различной, в зависимости от его модели и конфигурации. Общее правило для всех Hayes-совместимых модемов состоит в том, что при падении DTR физическое соединение разрывается. В частных случаях возможны другие варианты, например:

— при падении DTR модем разрывает соединение и инициализируется, как при выключении/включении питания;
— при поднятии DTR модем устанавливает соединение по выделенной линии;
— при поднятии DTR модем автоматически начинает дозваниваться по заданному номеру.

Подробное описание функциональных возможностей для конкретных модемов см. в соответствующих Руководствах пользователя этих модемов.

Процедура установления асинхронного модемного соединения, как правило, включает в себя целую последовательность операций: инициализация модема, дозвон, вход в удаленную систему и т.п. Эти операции программируются в устройствах NSG в виде сценария, состоящего из строк типа: "жду" — "посылаю" — "жду" — "посылаю" —… Сценарии дозвона записываются в специальную таблицу сценариев (см. §4.1.7). Для использования сценария необходимо указать для интерфейса PPP параметр

SCRIPT:<номер>

указывающий на запись в таблице сценариев. Сценарий исполняется:

— В режиме сервера (SL:YES) — всякий раз при поднятии сигнала DTR, что позволяет инициализировать модем после разрыва предыдущего соединения.
— В режиме выделенной линии (SL:NO DOD:NO) — также при поднятии сигнала DTR (после включения устройства, рестарта интерфейса и т.п.), что и приводит к установлению соединения.
— В режиме установления соединений по требованию (SL:NO DOD:YES) — при поступлении данных на интерфейс. В данном случае, чтобы инициализировать модем немедленно после разрыва предыдущего соединения, следует установить для интерфейса DTR:1 и для самого модема — режим инициализации при поднятии DTR.

При SCRIPT:0 никакой сценарий не используется. (Например, при подключении по выделенной линии.) Если запись с указанным номером не существует, то интерфейс также пытается установить соединение безо всякого сценария.

Если попытка установления соединения не увенчалась успехом, то перед началом следующей попытки может быть установлена пауза от 0 до 65535 секунд, которая определяется параметром

HOLD:<секунды>

Для разрыва соединения интерфейс сбрасывает сигнал DTR (постоянно при SL:NO DOD:YES DTR:0, на 2 сек. в остальных конфигурациях). Разрыв соединения производится в следующих случаях:

— При падении сигнала DCD, т.е. разрыве соединения на физическом уровне.
— По истечении времени, заданного атрибутами Session-Timeout в ответе сервера RADIUS, timeout в ответе сервера TACACS+ (см. Часть 8), либо параметром Activity Timer самого интерфейса:
  AT:<секунды>
  AT:0 означает, что продолжительность сеанса не ограничена. Максимальное значение параметра — 65535 сек.
— При длительном отсутствии активности на интерфейсе. Величина тайм-аута задается параметром
  KEEP:<секунды>
  либо атрибутами Idle-Timeout (RADIUS), idletime (TACACS+). Если за указанное время не принято ни одного пакета от удаленной стороны, соединение будет разорвано. Максимальная величина тайм-аута — 65535 секунд. Специальное значение KEEP:0 указывает, что разрыв по тайм-ауту запрещен.
— При непрохождении пакетов LCP Echo Request/Echo Reply. В случае отсутствия данных на приеме интерфейс посылает пакеты LCP Echo Request для проверки целостности линии. Удаленная сторона должна отвечать на них пакетами LCP Echo Reply. Если ответ не получен 10 раз подряд, линия считается неисправной и PPP-соединение разрывается. Интервал между посылкой пакетов Echo Request устанавливается параметром
  ECHO:<секунды>
  Максимальный интервал — 65535 секунд. Если ECHO:0, то пакеты Echo Request не посылаются.

**б) Согласование параметров линии (Line Control Protoclol)**

На данном этапе происходит согласование основных параметров создаваемого соединения. К ним относятся, в частности, использование механизмов сжатия, аутентификации (собственно аутентификация и согласование параметров сжатия производятся позже). Размер MTU устанавливается параметром MTU данного интерфейса (см. §4.2.2).

Особенности передачи управляющих символов устанавливаются параметром AM, который задается в виде 32-битного шестнадцатеричного числа. Значение параметра представляет собой битовую маску, которая определяет, какие управляющие символы не могут быть приняты по асинхронной линии. PPP-интерфейс будет запрашивать удаленную сторону посылать эти символы как двухбайтовые ESC-последовательности. Каждый бит в этой маске, равный единице, представляет один из запрещенных символов. Бит 0 (0x00000001) представляет символ 0x00 (NUL), бит 31 (0x80000000) представляет символ 0x1f. Пример:

```
AM:000A0000
```

| 1F | 1E | 1D | 1C | 1B | 1A | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 0F | 0E | 0D | 0C | 0B | 0A | 09 | 08 | 07 | 06 | 05 | 04 | 03 | 02 | 01 | 00 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | | | | 0 | | | | 0 | | | | A | | | | 0 | | | | 0 | | | | 0 | | | | 0 | | | |

При данном значении AM в принимаемой асинхронной последовательности запрещены символы XOFF (0x11) и XON (0x13). Это вероятное решение для асинхронного соединения с программным управлением потоком.

**в) Аутентификация PAP/CHAP**

Следующая группа параметров определяет процедуру аутентификации с использованием протоколов PAP (Password Authentication Protocol) и CHAP (Cryptographic Handshake Authentication Protocol). Первый метод использует передачу пароля обычным образом, второй — в защищенном виде.

Для сервера PPP могут устанавливаться параметры PAPR (PAP Request) и CHAPR (CHAP Request), требующие от удаленного клиента аутентификации по тому или иному методу:

```
PAPR:<номер>
CHAPR:<номер>
```

Значения этих параметров указывают номер записи в таблицах аутентификации PAP и CHAP, соответственно. Подробно о процедурах аутентификации см. Часть 8. Нулевые значения указывают, что соответствующий метод аутентификации не используется.

Для клиента PPP устанавливаются аналогичные параметры PAPA (PAP Agreement) и CHAPA (CHAP Agreement). Для обоих параметров допустимы значения

| | |
|---|---|
| YES | Разрешить аутентификацию по данному протоколу |
| NO | Запретить аутентификацию по данному протоколу |

Имя и пароль для аутентификации данного устройства на удаленном сервере хранятся в тех же таблицах PAP и CHAP.

Кроме того, для аутентификации устройства как клиента PAP на удаленной системе необходимо указать параметр RNAME (Remote Name), совпадающий с именем сервера в соответствующей таблице аутентификации. Значением параметра является строка длиной не более 20 символов:

```
RNAME:"GadukinoTelecom_Ltd."
```

Если назначаемое имя содержит разделители (пробел : ; = ,) или вопросительный знак, его необходимо заключить в кавычки. Подробно о формате текстовых параметров см. Часть 9.

Наряду с аутентификацией по PAP и CHAP для клиентов PPP устройства NSG позволяют осуществлять аутентификацию, авторизацию и учет потребления услуг для заранее неизвестных клиентов при помощи локальной таблицы пользователей, серверов RADIUS и TACACS+. В этом случае пользователь после установления физического соединения с портом ASYNC должен ввести имя и пароль для входа в сеть. Если авторизация успешна и для данного пользователя назначен сервис PPP, то асинхронный порт принимает тип ASYNC_PPP, и начинается процедура установления PPP-соединения (что не исключает последующую повторную аутентификацию по PAP/CHAP). Подробнее о процедурах AAA (Authentication, Authorization & Accounting) см. Часть 8.

**ПРИМЕЧАНИЕ** В некоторых системах доступа, в частности, в сотовых сетях GSM/GPRS и т.п., аутентификация де-факто производится на основе номера абонентского модема. Тем не менее, в ряде случаев при этом требуется формальная аутентификация по PAP или CHAP — с именем и паролем, совпадающими с именем оператора, либо с пустыми именем и паролем. В частности, последний режим может быть установлен на оборудовании оператора по умолчанию, и сотрудники его техподдержки могут быть не осведомлены об этой тонкости. В этих случаях следует обратить внимание на то, чтобы клиентская аутентификация (параметры PAPA, CHAPA) была включена на интерфейсе устройства NSG.

**г) Согласование и установка параметров IP (IP Control Protocol)**

На данном этапе происходит согласование основных параметров работы протокола IP. К этим параметрам относятся, в первую очередь, IP-адреса локального и удаленного устройств. Каждая из участвующих сторон может работать со своим IP-адресом, установленным заранее, или же получить динамический IP-адрес от удаленной стороны.

Способ назначения локального IP-адреса для PPP-интерфейса относится, как правило, к устройству NSG, работающему в качестве клиента. Он определяется параметром ACCL (Accept Local IP address):

| | |
|---|---|
| ACCL:YES | Принимать динамический IP-адрес, предлагаемый удаленной стороной |
| ACCL:NO | Использовать статический IP-адрес, заданный параметром IADR данного интерфейса (см. §4.2.2). |

Для динамического назначения IP-адреса удаленной стороне предназначен параметр RADR (Remote Address). Как правило, он используется для устройства NSG, работающего в режиме сервера (особенно сервера доступа по коммутируемым линиям). Значением параметра является IP-адрес, который будет предлагаться удаленной стороне. Адрес записывается только в десятичной дотовой нотации. Пример:

```
RADR:198.98.98.2
```

На удаленном устройстве должно быть установлено динамическое назначение IP-адреса. При RADR:0.0.0.0 IP-адрес назначается статически на удаленной стороне.

**ПРИМЕЧАНИЕ** Особый случай представляет использование ненумерованных (*unnumbered*) интерфейсов. Подробнее об этом случае см. §4.2.3.

**ПРИМЕЧАНИЕ** Если средства аутентификации и авторизации предписывают специфический IP-адрес или список адресов для данного пользователя, то эти адреса имеют приоритет над параметром RADR. Подробно об аутентификации и авторизации см. Часть 8.

При работе в режиме сервера устройство NSG также передает удаленному клиенту адреса DNS, если они установлены параметрами DNS1 и DNS2 псевдоинтерфейса IP:0 (см. §4.2.1).

**д) Согласование сжатия**

Использование сжатия для полей адреса и протокола пакета PPP определяется параметрами AC (Address/Control Compression) и PC (Protocol field Compression).

| | |
|---|---|
| AC:YES | Согласовывать сжатие полей адреса и управления с удаленной стороной. |
| AC:NO | Запретить сжатие полей адреса и управления. |
| PC:YES | Согласовывать сжатие поля протокола с удаленной стороной. |
| PC:NO | Запретить сжатие поля протокола. |

Сжатие заголовка производится по методу Van Jacobson; степень сжатия устанавливается параметром VJ (Van Jacobson style IP header compression):

| | |
|---|---|
| VJ:2 … VJ:16 | Согласовывать сжатие при указанном максимальном числе слотов (от 2 до 16) |
| VJ:NO | Запретить сжатие |

Если сжатие заголовков разрешено, то отдельный параметр VJC (VJ Connection-ID compression) определяет сжатие идентификатора соединения:

| | |
|---|---|
| VJC:YES | Согласовывать сжатие с удаленной стороной. |
| VJC:NO | Запретить сжатие. |

Для сжатия поля данных по методу BSD предусмотрен параметр BSDC (BSD Compression). Данный параметр может быть задан в одном из следующих форматов:

| | |
|---|---|
| BSDC:n:m | Сжатие будет согласовываться с максимальными параметрами n и m, где<br>n — параметр сжатия на приеме (запрашиваемый у удаленной стороны)<br>m — параметр сжатия на передаче (предлагаемый данным интерфейсом).<br>Значения m и n могут быть равны 0 или находиться в диапазоне от 9 до 15. Если один из параметров равен нулю, то в данном направлении сжатие не требуется. Например, BSDC:0:15 означает, что интерфейс не будет запрашивать у удаленной стороны сжатия пакетов PPP, но сам готов сжимать с максимальным параметром 15. |
| BSDC:n | Сжатие будет согласовываться с максимальным параметром n в обоих направлениях. |
| BSDC:NO | Сжатие не используется. (Равносильно BSDC:0:0 или BSDC:0.) |

Сжатие пакетов PPP позволяет значительно уменьшить объем передаваемых данных и тем самым повысить фактическое быстродействие соединения. Однако при выборе режимов сжатия необходимо учитывать, что сжатие расходует значительный объем аппаратных ресурсов, в первую очередь, оперативной памяти (область HEAP), на обеих сторонах соединения.

**ПРИМЕЧАНИЕ** По умолчанию все параметры PPP имеют значения 0 или NO, соответственно. Для быстрой установки другого типового набора параметров можно использовать команду:

```
S P IP:n TY:PPP DEF
```

которая формирует следующий профиль:

```
SL:NO PAPR:0 PAPA:YES CHAPR:0 CHAPA:YES SCRIPT:0
AC:YES PC:YES VJ:16 VJC:YES BSDC:NO KEEP:0 HOLD:0 ECHO:3
AM:00000000 ACCL:NO DOD:NO DTR:0 RNAME:"" RADR:0.0.0.0
```

Значения параметров, относящихся к сетевому уровню IP-интерфейса, при этом не изменяются.

Примеры конфигурации протокола PPP:

Сервер удаленного доступа по коммутируемым линиям для поставщика услуг Интернет или корпоративной сети (предполагается, что аутентификация производится средствами аснхронного порта):

```
S P IP:16 TY:PPP PO:16 SL:YES KEEP:600 AC:YES PC:YES VJ:YES VJC:YES BSDC:15:15 RADR:197.135.1.16
```

Клиент удаленного доступа по выделенной линии со статическим IP-адресом:

```
S P IP:1 TY:PPP PO:2 SL:NO DOD:NO SCRIPT:0 HOLD:0 KEEP:0 ACCL:NO
```

Клиент удаленного доступа по коммутируемой линии с аутентификацией PAP и динамическим IP-адресом:

```
S P IP:1 TY:PPP PO:0 SL:NO DOD:YES DTR:1 SCRIPT:2 HOLD:60 KEEP:300 ACCL:YES
S P IP:1 PAPA:YES NAME:"Local_Office" RNAME:"Head_Office"
A X PAP:1 Local_Office Head_Office qWeRTy
```

(Подробно о настройке аутентификации см. Часть 8.)

## §4.1.7. Сценарии соединения для интерфейсов PPP

Сценарии, используемые клиентами PPP для установления соединений, хранятся в таблице сценариев. Сценарий представляет собой последовательность записей "жду" — "посылаю", разделенных пробелами. Нечетные члены последовательности представляют собой сообщения, ожидаемые от модема или удаленной системы, а следующие за ними четные — команды, выдаваемые интерфейсом в линию. Пример сценария:

```
"ogin: " vasya.pupkin "assword: " qwerty
```

Каждая запись сценария может быть записана в кавычках или без них. Кавычки обязательны, если запись содержит пробелы (как в данном примере после двоеточия в приглашениях [L|l]ogin: и [P|p]assword: ), дефисы (–), знаки равенства (=) или точку с запятой (;). Запись без этих спецсимволов может содержать кавычки внутри себя, но не может начинаться с кавычки.

Приведенный выше пример означает, что интерфейс PPP будет ожидать от удаленной системы приглашения, оканчивающегося на ogin: (с пробелом). Когда эта последовательность символов будет получена, в линию будет послана строка vasya.pupkin. Затем клиент будет ждать, пока из линии будет получено приглашение assword: , и в ответ пошлет строку qwerty — и так далее до конца сценария. Каждая посылаемая последовательность символов дополняется символом <CR>.

**ВНИМАНИЕ** Пароль для входа в удаленную систему представляет собой, с точки зрения сценария, обычную запись, не выделяющуюся среди остальных, и хранится в таблице сценариев в открытом виде.

Если по существу требуется ввести запись, содержащую одновременно кавычки и другие спецсимволы, то ее необходимо заключить в кавычки, а внутренние кавычки предварить escape-символом \ (обратная косая черта). Например, фрагмент сценария для подключения с помощью GPRS-модема может выглядеть следующим образом:

```
... OK "AT+CGDCONT=1,\"IP\",\"internet.cellprovider.ru\"" OK ATD*99# CONNECT ...
```

В этом случае в модем будет послана команда:

```
AT+CGDCONT=1,"IP","internet.cellprovider.ru"
```

Если в качестве записи ожидания стоит пустая запись (""), то клиент PPP ничего не ждет и сразу переходит к посылке следующей записи. В частности, чтобы начать выполнение сценария не с ожидания, а с выдачи команды модему, следует указать пустой первый член последовательности:

```
"" ATZ OK ATDP1234567 CONNECT ...
```

Если пустая запись стоит на месте записи, посылаемой в модем, то посылается символ <CR>, т.е. пустая строка.

Концом сценария является конец строки в таблице сценариев. Максимальная длина одной строки программно ограничена только размером всей таблицы — 4096 символов. Если возникает необходимость перенести часть сценария на следующую строку (например, для удобства администрирования), необходимо закончить строку символом \. В этом случае исполнение сценария продолжается, пока очередная строка не завершится каким-либо иным символом.

**ПРИМЕЧАНИЕ** Если сценарий состоит более чем из одной строки и параметр SCRIPT в конфигурации PPP-интерфейса указывает не на первую строку сценария, а на какую-либо из строк продолжения, выполнение сценария начнется с данной строки. Это, с одной стороны, может служить источником ошибок, а с другой стороны — позволяет составлять сценарии "с вариантами". Пример (для самостоятельного анализа):

```
A X SCRIPT:1 "" ATZ OK ATDP1234567 CONNECT "" \
A X SCRIPT:2 "ogin:" "vasya.pupkin" "assword:" qwerty
S P IP:1 PO:1 TY:PPP SCRIPT:1 NAME:"BACKUP (DIALUP CONN.)"
S P IP:2 PO:2 TY:PPP SCRIPT:2 NAME:"MAIN (LEASED LINE)"
```

Если в течение некоторого времени (по умолчанию 45 секунд) ожидаемая последовательность не будет получена, то выполнение сценария заканчивается неудачей и интерфейс PPP переходит в исходное состояние. Продолжительность тайм-аута может быть изменена включением параметра TIMEOUT в сценарий перед строкой ожидания. Например, в сценарии

```
"" ATZ OK ATDT5551212 CONNECT "" TIMEOUT 10 "ogin:" sidorov
```

тайм-аут перед ожиданием строки ogin: будет уменьшен до 10 секунд. Нулевое значение TIMEOUT указывает, что время ожидания не ограничено.

**ВНИМАНИЕ** Ключевое слово TIMEOUT должно вводиться заглавными буквами. Ответы модема должны быть записаны с соблюдением регистра. Для команд, посылаемых в модем, также может иметь значение регистр (в зависимости от типа модема).

В качестве записи ожидания может быть указана последовательность записей "ожидание"–"посылка"–…–"ожидание", разделенных дефисами. Например, сценарий

```
"" ATD1234 CONNECT–ATD1256–CONNECT–ATD1278–CONNECT ""
```

означает, что если после набора номера 1234 в течение 45 секунд не получен ответ CONNECT, то модем должен набрать номер 1256; если по этому номеру тоже не удается соединиться (нет связи, получен BUSY, NO CARRIER, NO DIALTONE и т.п.) — набрать 1278. Как только получен ответ CONNECT, выполнение альтернативной ветви завершается и исполняется следующий шаг основного сценария — в данном случае, посылка пустой строки и нормальное завершение сценария. Если все варианты альтернативных посылок испробованы и ни на одну из них не получен ожидаемый ответ (в общем случае он может быть свой для каждой из посылок), выполнение сценария завершается аварийно.

Аналогичный пример для команд и ответов, содержащих спецсимволы:

```
"" "AT+CPIN?" "+CPIN: READY–AT+CPIN=9876–+CPIN: READY" ATD1234 CONNECT ""
```

В этом случае сначала проверяется регистрация модуля IM–GPRS (или внешнего модема) в сети GSM. Если получен ответ +CPIN: READY, интерфейс приступает к набору номера; если нет — вводит PIN-код (AT+CPIN=9876) и снова ждет ответа +CPIN: READY.

Помимо обычных символов, в сценариях предусмотрены следующие дополнительные спецсимволы:

| | |
|---|---|
| \– | Дефис (–) как текстовый символ в записи ожидания — чтобы отличать его от дефиса, разделяющего альтернативные варианты посылок/ответов. Для команд, посылаемых PPP-интерфейсом, допускается вводить дефис обычным образом. |
| \b | Символ <BS> (0x08) |
| \c | Подавить символ <CR> в конце строки. Данный спецсимвол может использоваться только в конце строки и только для команд, посылаемых PPP-интерфейсом. По умолчанию, в конце каждой посылаемой строки вставляется символ <CR>. |
| \n | Символ <LF> (0x0A) |
| \N | Послать символ NULL (0x00; только для команд, посылаемых PPP-интерфейсом) |
| \r | Символ <CR> (0x0D) |
| \s | Пробел (символ 0x20). Это альтернативный способ ввода пробела, не разрывающий целостность отдельной записи. Его можно использовать вместо апострофов, чтобы ввести пробел в тело посылки/ответа, например: AT+CGREG? +CGREG:\s1,1 |
| \t | Символ горизонтальной табуляции (0x09) |
| ^A … ^Z | Непечатаемые управляющие символы с кодами от 0x01 до 0x1A |
| ^[, ^], ^^,^_ | Непечатаемые управляющие символы с кодами от 0x1B, 0x1D, 0x1E, 0x1F, соответственно |
| \^ | Символ ^ |
| \' | Апостроф |
| \" | Двойная кавычка " |
| \\ | Обратный слэш \ |

Для IP-интерфейса типа PPP, работающего в режиме сервера, сценарий обычно содержит команды инициализации модема и перевода его в режим ожидания входящих звонков:

```
"" ATZ OK "ATS0=1"
```

Строки в таблице сценариев нумеруются, начиная с 1. Для добавления, удаления и просмотра строк используются команды Add, Remove и Display:

```
A X SCRIPT:<номер> <сценарий>
R X SCRIPT:<номер>
D X SCRIPT
```

Первая команда добавляет в таблицу строку с указанным номером; весь остаток команды, после номера, рассматривается как сценарий, который должен быть записан в этой строке. Если в таблице уже имеется строка с таким номером, то она заменяется на новую. Таким образом, номера всех остальных строк сохраняются в любом случае, чтобы избежать ошибок в конфигурации. Если введенный номер больше номера последней существующей строки более чем на единицу, то новой строке будет присвоен номер, следующий за этой строкой.

Вторая команда удаляет из таблицы строку с заданным номером. При этом все следующие строки сохраняют свои номера. (Таким образом, в таблица могут быть пропущенные строки.) Третья команда выводит всю таблицу сценариев. Помимо этого, возможны также следующие общие команды:

```
R X SCRIPT:A     Удалить все записи из таблицы сценариев
D X              Вывести все таблицы PPP (SCRIPT, PAP и CHAP)
```

**ПРИМЕЧАНИЕ** Команды добавления и удаления строк не проверяют взаимосвязь текущей, предшествующей и последующей строк. Если в таблице используются сценарии, состоящие более чем из одной строки (с символом продолжения \ в конце), то контроль за их целостностью возлагается на администратора, составляющего таблицу.

### §4.1.8. Инкапсуляция IP-over-PPP-over-X.25

Передача трафика IP, инкапсулированного в пакеты PPP, по сети X.25 требует настройки как стека протоколов TCP/IP, так и стека X.25. При этом IP-маршрутизатор может работать только в качестве сервера, т.е. принимать входящие запросы на установление соединений PPP через сеть X.25.

В части, относящейся к TCP/IP, необходимо назначить IP-интерфейсу тип PPP и динамическую привязку к портам: PO:AUTO. Со стороны сети X.25 необходимо создать запись в таблице маршрутизации, направляющую все входящие пакеты CALL, удовлетворяющие некоторому критерию маршрутизации, на PPP-интерфейсы маршрутизатора. Конфигурация подсистемы X.25 подробно рассмотрена в Части 7 данного руководства.

Пример конфигурации локального устройства:

```
S P IP:2 TY:PPP PO:AUTO ...
W S IP:2
S R PR:28 ID:D RT:12345 TO:PP.2
```

В данном случае, если из сети X.25 поступает вызов с адресом назначения 12345, то он маршрутизируется на IP-интерфейс номер 2. Если к этому интерфейсу уже установлено другое соединение, удаленному пользователю X.25 будет отправлено сообщение о том, что соединение невозможно.

Вместо фиксированного IP-интерфейса типа PPP входящий вызов может маршрутизироваться на всю совокупность таких интерфейсов. Пример:

```
S R PR:28 ID:D RT:12345 TO:PP
```

В этом случае логическое соединение X.25 устанавливается с первым свободным IP-интерфейсом типа PPP, для которого разрешена динамическая привязка к портам (TY:PPP PO:AUTO). Если таких интерфейсов нет, или все они заняты, соединение установлено не будет.

Подключение к устройству возможно с помощью стандартного клиента удаленного доступа, например, входящего в состав операционной системы Windows (в режиме терминального окна или сценария доступа). Пользователь должен подключиться к PAD (например, по коммутируемой линии) и дождаться приглашения — звездочки. После этого он набирает адрес сервера (в вышеприведенном примере, 12345). Как только соединение X.25 установлено и сервер начинает посылать пакеты LCP, пользователь должен нажать клавишу "продолжить" или завершить выполнение сценария. Аутентификация производится средствами протокола PPP, т.е. с использованием PAP или CHAP.

### §4.1.9. Инкапсуляция PPP-over-Ethernet (сервер)

Инкапсуляция IP-трафика в пакеты PPP при передаче их по локальной сети Ethernet позволяет эмулировать в локальной сети соединения "точка-точка" и обеспечивает индивидуальную аутентификацию каждого подключенного пользователя. Аутентификация осуществляется стандартными средствами интерфейса PPP, т.е. серверами PAP и/или CHAP на основании уникального сочетания имени и пароля пользователя. (Подробно о настройке интерфейсов PPP см. §4.1.6, системы аутентификации — Часть 8.)

Для работы в качестве сервера доступа PPPoE необходимо:

— Настроить порт Ethernet (TY:ETH IF:TP).
— Настроить Ethernet-станцию типа PPP и привязать ее к физическому порту. Станции нумеруются последовательно от 0 до максимального номера, допустимого для данной модели устройства и версии программного обеспечения.
— Назначить некоторому IP-интерфейсу тип PPP и динамическую привязку к портам: PO:AUTO.

Конфигурация Ethernet-станции типа PPP содержит следующие параметры:

```
S P ET:<номер> PO:<номер> TY:PPP NAME:<имя> IP:<список_интерфейсов>
```

Параметр NAME определяет административное имя сервера доступа PPPoE. Это имя может быть указано в настройках клиентов PPPoE. При подключении клиент PPPoE рассылает по сети широковещательный запрос о наличии серверов и принимает ответы от серверов, готовых с ним работать. Если для него указано имя сервера, то он будет работать только с этим сервером, если нет — то с первым ответившим.

**ПРИМЕЧАНИЕ** Некоторые клиенты PPPoE не работают с серверами, имеющими пустое имя. Это относится, в частности, к встроенному клиенту в Windows XP. Для работы с такими клиентами необходимо определить произвольное непустое имя сервера.

Параметр IP содержит список IP-интерфейсов, которые могут использоваться данной станцией. Интерфейсы должны иметь тип PPP (TY:PPP) и быть сконфигурированы для динамической привязки к портам (PO:AUTO). Список может содержать один номер интерфейса, диапазон номеров (через дефис), или несколько номеров и диапазонов, разделенных запятыми. Вместо списка может использоваться значение ALL. Пример:

```
IP:1,3,6–9,12
```

Если указано IP:ALL (по умолчанию), то станция будет привязываться к первому свободному интерфейсу данного типа.

На следующем шаге клиент PPPoE посылает выбранному серверу запрос на установление соединения. Получив этот запрос, сервер PPPoE просматривает IP-интерфейсы, заданные в списке, и привязывается к первому свободному интерфейсу. После этого интерфейс устанавливает соединение с удаленным клиентом PPP обычным образом согласно своим настройкам.

Для одновременной работы нескольких клиентов необходимо сконфигурировать в устройстве соответствующее число IP-интерфейсов типа PPP с PO:AUTO. Теоретически максимальное количество клиентов PPPoE определяется числом поддерживаемых IP-интерфейсов (которое, в свою очередь, зависит от модели устройства и версии программного обеспечения), но практически оно может быть ограничено производительностью процессора и быстродействием портов WAN.

Каждая Ethernet-станция должна быть привязана к некоторому физическому порту типа ETH. Один порт Ethernet может обслуживать не более чем две станции типа IP (с разными форматами кадров), одну станцию типа PPP и несколько станций типа X25 одновременно. Все эти станции имеют один MAC-адрес.

Пример конфигурации (на максимум 8 пользователей одновременно):

```
S P PO:0 TY:ETH IF:TP
S P ET:0 TY:PPP PO:0 IP:1–8 NAME:"NSG"
S P IP:1 TY:PPP PO:AUTO
.....
S P IP:8 TY:PPP PO:AUTO
W S PO:0
W S IP:1
.....
W S IP:8
```

### §4.1.10. Инкапсуляция IP-over-X.25

Для передачи трафика IP по сети X.25 требуется конфигурация как стека протоколов TCP/IP, так и стека X.25. В части, относящейся к TCP/IP, необходимо назначить IP-интерфейсу тип X25. Со стороны сети X.25 к данному интерфейсу должно быть установлено постоянное либо коммутируемое логическое соединение. Конфигурация подсистемы X.25 подробно рассмотрена в Части 7 данного руководства .

При использовании постоянного логического соединения (PVC) необходимо связать IP-интерфейс со смежным объектом сети X.25. Таким объектом может быть канал некоторого физического порта типа X25, станции Ethernet либо Frame Relay типа X25, станции XoX. Далее этот PVC должен быть проложен через сеть X.25 вплоть до удаленного IP-интерфейса. Пример конфигурации локального устройства с использованием PVC:

```
S P PO: TY:X25 ...
S P IP:2 TY:X25 ...
A P PO:PO.1 CH:3 PO:IP CH:2
W S PO:1 (либо W S PVC)
W S IP:2
```

Если в сети X.25 предполагается использовать коммутируемые логические соединения (SVC), то у IP-интерфейсов типа X25 предусмотрены дополнительные параметры для их установления и разрыва :

| | |
|---|---|
| XADR:<адрес> | Адрес X.121 удаленного IP-интерфейса с инкапсуляцией X.25. |
| LADR:<адрес> | Адрес X.121 локального IP-интерфейса типа X25. Максимальная длина обоих адресов — по 15 десятичных цифр. Правила использования этих адресов описаны ниже. |
| KEEP:<секунды> | Максимальное время неактивности соединения. Если за это время не принято и не передано никакой информации, соединение будет разорвано. Значение 0 указывает, что разрыв соединения по тайм-ауту не производится. |
| HOLD:<секунды> | Интервал между попытками установления соединения. Для двух интерфейсов, связанных друг с другом через сеть X.25, значения параметров HOLD должны быть различаться не менее, чем на время, требуемое для установления соединения в данной сети. |

На обоих устройствах и на всех промежуточных коммутаторах сети X.25 необходимо задать соответствующие правила маршрутизации вызовов. Подробно о конфигурации подсистемы X.25 см. Часть 7.

Если на IP-интерфейсе типа X25 устройства NSG появляются пакеты для передачи, а какое-либо логическое соединение с данным интерфейсом в этот момент отсутствует, то интерфейс пытается установить SVC к удаленному узлом, заданному по умолчанию. Для этого он отправляет в сеть пакет CALL, в котором в качестве вызывающего адреса (*calling address*) указывается значение параметра LADR, а в качестве вызываемого адреса (*called address*) — параметра XADR. Если один или оба параметра имеют значение NO, то соответствующий адрес в пакете CALL не указывается.

Если из сети X.25 на устройство NSG поступает вызов от удаленного хоста IP-over-X.25, то он может быть маршрутизирован либо на некоторый определенный IP-интерфейс типа X25, либо на всю совокупность таких интерфейсов. В первом случае правило маршрутизации имеет вид:

```
S R PR:<номер> ... TO:IP.<номер>
```

При этом значение вызываемого адреса, указанное в пакете CALL, сравнивается со значением параметра LADR, а значение вызывающего адреса — с параметром XADR. Если эти параметры совпадают, между интерфейсами устанавливается логическое соединение; в противном случае вызов отвергается.

Во втором случае правило маршрутизации имеет вид:

```
S R PR:<номер> ... TO:IP
```

Это означает, что коммутатор X.25 будет последовательно проверять все IP-интерфейсы типа X25, начиная с первого. Соединение будет установлено с тем интерфейсом, у которого значение LADR совпадает с вызываемым адресом, а XADR — с вызывающим адресом, указанными в пакете CALL. Если таких интерфейсов несколько, соединение будет установлено с первым свободным из них. Если ни одного такого интерфейса не найдено, или ко всем ним уже установлены логические соединения, новое соединение установлено не будет.

**ВНИМАНИЕ** Пустому полю вызываемого адреса должно соответствовать значение LADR:NO, а пустому полю вызывающего адреса — значение XADR:NO. По умолчанию оба параметра LADR и XADR имеют значения NO. Если входящий пакет CALL маршрутизировался по вызываемому адресу (что имеет место в большинстве практических случаев), то он, следовательно, содержит вызываемый адрес, и для IP-интерфейса NSG *необходимо* установить параметр LADR. Если при этом удаленная сторона указывает в пакете CALL и свой адрес в качестве вызывающего, то для IP-интерфейса NSG необходимо установить также параметр XADR. В противном случае соединение установлено не будет.

Пример конфигурации с использованием SVC:

```
S P PO:1 TY:X25 ...
```

```
S  P  IP:2  TY:X25  XADR:12345  LADR:67890  ...
W S PO:1
W S IP:2
S  R  PR:17  ID:D  RT:12345  TO:PO.1
S  R  PR:18  ID:D  RT:67890  TO:IP.2
```

В данном случае интерфейс 2 по умолчанию пытается установить коммутируемое логическое соединение X.25 с хостом по адресу 12345. Если же из сети поступает вызов по адресу 67890 (от удаленного узла IP-over-X.25), то он маршрутизируется на IP-интерфейс номер 2. (Задание обоих правил маршрутизации не обязательно. Интерфейс может работать только как клиент, или только как сервер доступа, или в обоих качествах.)

### §4.1.11. Инкапсуляция IP-over-Frame Relay

Для передачи трафика IP по сети Frame Relay требуется конфигурация как стека протоколов TCP/IP, так и стека Frame Relay. В части, относящейся к TCP/IP, необходимо произвести следующие настройки:

— Назначить станции Frame Relay тип IP
— Назначить IP-интерфейсу тип FRI и привязать его к станции Frame Relay параметром ST:<номер>

Каждый IP-интерфейс типа FRI должен быть привязан к некоторой станции Frame Relay типа IP. Одна станция обслуживает один поток данных, т.е. передает трафик одного IP-интерфейса по одному виртуальному соединению. После завершения настройки необходимо рестартовать физический порт (для рестарта всех связанных с ним станций и IP-интерфейсов).

IP-интерфейс типа FRI в сочетании со станцией Frame Relay типа IP осуществляет инкапсуляцию пакетов IP в кадры Frame Relay. При этом на приеме автоматически распознается как формат кадров IETF, предусмотренный стандартом RFC 1490, так и фирменный формат кадров компании Cisco Systems. Никакой дополнительной конфигурации для этого не требуется. На передаче всегда используется формат RFC 1490. Поскольку маршрутизаторы Cisco также автоматически распознают на приеме оба указанных формата, совместимость обеспечивается в обе стороны.

Настройка Frame Relay включает в себя настройку портов, станций и установление постоянных виртуальных соединений между двумя устройствами сети. Подробно она рассмотрена в части 6 данного руководства.

Пример конфигурации (подробности конфигурации Frame Relay опущены):

```
S  P  PO:1  TY:FR ...
S  P  ST:3  TY:IP PO:1 ...
S  P  IP:2  TY:FRI ST:3
W S  PO:1
```

(Рестарт интерфейса в данном случае не требуется, поскольку при рестарте порта типа FR рестартуют все связанные с ним станции и IP-интерфейсы.)

# §4.2. Общие параметры IP-интерфейсов

## §4.2.1. Локальный псевдоинтерфейс

Для настройки общих параметров IP-маршрутизатора используется формальный объект, называемый *локальным псевдоинтерфейсом*. Для него зарезервирован специальный номер 0, т.е. его настройка и просмотр параметров производятся командами, соответственно:

```
S P IP:0 ...
D P IP:0
```

Нумерация реальных интерфейсов, через которые производится обмен данными, начинается с единицы.

Помимо нулевого номера, для локального псевдоинтерфейса всегда используется формальный тип

```
TY:LOCAL
```

Другие значения данного параметра для него невозможны.

Параметр NUM (Number of interfaces) определяет число IP-интерфейсов, используемых для передачи данных.

Параметр NAME для локального псевдоинтерфейса определяет административное имя маршрутизатора — до 29 символов.

Параметр MTU устанавливает размер MTU. Допустимые значения — от 64 до 1600 байт, по умолчанию 1500.

Параметр TTL устанавливает максимальное время жизни (число шагов маршрутизации) для пакетов, отправляемых прикладными службами устройства (например, PING). Допустимые значения — от 1 до 255 (по умолчанию 255).

Два параметра определяют функционирование соединений TCP:

| | |
|---|---|
| TKO (TCP Keepalive Outgoing) | Интервал между посылкой пакетов TCP *keepalive* (в 1/100 сек). |
| TKI (TCP Keepalive Incoming) | Ожидаемый интервал между приемом пакетов TCP *keepalive* от удаленной стороны (в 1/100 сек). Если не принято 5 пакетов подряд и никаких данных за это время, соединение разрывается. |

Допустимые значения для обоих параметров — от 100 до 4294967295. Значения по умолчанию равны 6000 (1 минута).

Параметр ADM разрешает или запрещает работу всего IP-маршрутизатора:

| | |
|---|---|
| ADM:UP | Маршрутизатор включен. |
| ADM:DOWN | Маршрутизатор выключен. |

Все вышеперечисленные параметры вступают в силу после рестарта локального псевдоинтерфейса, т.е. всего маршрутизатора, командой

```
W S IP:0
```

**ВНИМАНИЕ** Маршрутизатор стартует (при установленном значении ADM:UP) *только* в том случае, если хотя бы один из его интерфейсов:

а) имеет ненулевые значения IP-адреса и маски;

б) находится в состоянии ADM:UP;

в) имеет действующее соединение на канальном уровне.

Настройка указанных параметров IP-интерфейсов описана в следующем параграфе.

Последняя группа параметров относится к различным дополнительным службам маршрутизатора:

| | |
|---|---|
| RIP | Использование протокола маршрутизации RIPv1. Подробнее о RIP см. §4.3.4. |
| DNS, DNS1, DNS2 | Параметры службы DNS. Подробнее о службе DNS см. §4.3.5. |
| ACCT | Размер таблицы учета по IP-адресам. Подробнее о статистике см. §4.6. |
| FACCT | Размер таблицы учета по IP-фильтрам. Подробнее о фильтрации см. §4.5. |
| HTTP | Использование встроенного сервера HTTP. Подробнее о Web-управлении см. Часть 5. |
| XOT | Использование сервера XOT. Подробнее о подсистеме X.25 см. Часть 7. |

**ПРИМЕЧАНИЕ** Службы DNS и HTTP могут быть перезагружены отдельно от остальных компонент IP-маршрутизатора командами

```
W S DNS
W S HTTP
```

Изменения таблиц учета (параметрами ACCT, FACCT) вступают в силу немедленно и не требуют рестарта маршрутизатора.

### §4.2.2. Сетевые параметры интерфейсов маршрутизатора

Данная группа параметров описывает интерфейсы IP-маршрутизатора со стороны сетевого уровня, т.е. с точки зрения сети IP. Эти параметры никак не связаны с лежащими под ними протоколами канального уровня и физическими интерфейсами и имеют одинаковый смысл для всех IP-интерфейсов.

Установка и просмотр параметров IP-интерфейсов производится командами Set Parameter и Display Parameter следующего вида:

```
S P IP:<номер> <параметр>:<значение> ...
D P IP:<номер>
D P IP:A
```

где номер интерфейса может принимать значения от 1 до NUM. Эти параметры дополняют параметры канального уровня, перечисленные в §4.1.

Административный статус данного IP-интерфейса устанавливается параметром ADM:

| | |
|---|---|
| ADM:UP | Интерфейс включен. |
| ADM:DOWN | Интерфейс выключен. |

Ключевыми характеристиками IP-интерфейса являются IP-адрес и маска подсети, которые устанавливаются параметрами IADR (Interface Address) и MASK (Network Mask), соответственно. Пример:

```
S P IP:4 IADR:198.98.4.2 MASK:255.255.255.0
```

Адрес и маска задаются в десятичной дотовой нотации.

**ПРИМЕЧАНИЕ** Адрес IP-интерфейса не может быть равен 0.0.0.0. Если адрес заранее неизвестен, а должен быть назначен удаленной стороной (для интерфейса PPP), то при настройке интерфейса необходимо назначить ему какой-либо фиктивный неиспользуемый адрес, например, 192.168.200.1.

Административное имя интерфейса устанавливается параметром NAME (Name of interface). Значение данного параметра — текстовая строка длиной не более 29 символов. Если назначаемое имя содержит разделители (пробел : ; = ,) или вопросительный знак, его необходимо заключить в кавычки. Подробно о формате текстовых параметров см. Часть 9. По умолчанию имя — пустая строка. Данный параметр необходим для аутентификации удаленных клиентов PPP на данном интерфейсе и самого интерфейса как клиента PPP на удаленных серверах по протоколам PAP и CHAP. В остальных случаях имя интерфейса используется только для удобства администрирования и не является обязательным. Пример:

```
S P IP:8 TY:PPP NAME:"Interface #8"
```

**ПРИМЕЧАНИЕ** Если параметр NAME для интерфейса не указан, то для аутентификации вместо него используется административное имя устройства (команда S W HNAM:<имя>).

Максимальный размер датаграммы, передаваемой данным интерфейсом, устанавливается параметром MTU (Maximum Transmit Unit). Допустимые значения этого параметра — от 64 до 1600 байт, по умолчанию — 1500 байт. Пример:

```
S P IP:8 TY:PPP MTU:1200
```

Служба трансляции сетевых адресов настраивается индивидуально для каждого интерфейса параметром NAT (Network Address Translation):

| | |
|---|---|
| NAT:NO | NAT не используется. |
| NAT:YES | NAT используется. |

Подробнее о службе NAT см. §4.4.

Параметр ACCT (Accounting) определяет способ отсылки статистической информации о работе данного IP-интерфейса на удаленный сервер RADIUS. Подробнее об учете и статистике см. Часть 8.

| | |
|---|---|
| ACCT:0 | Не отсылать статистику. |
| ACCT:<номер> | Отсылать статистику в соответствии с указанным способом аутентификации. |

Все изменения параметров (при работающем IP-маршрутизаторе) вступают в силу после рестарта интерфейса командой

```
W S IP:<номер>
```

Если IP-маршрутизатор в данный момент не работает, необходимо стартовать его командами

```
S P IP:0 ADM:UP
W S IP:0
```

**ВНИМАНИЕ** Начиная с версии программного обеспечения 8.0.0b, IP-интерфейсы, привязанные к протоколам, способным определять состояние соединения на канальном уровне (Frame Relay, Cisco-HDLC, а также Fast Ethernet для серии NSG–800), при ADM:UP автоматически переходят в состояние UP/DOWN в зависимости от состояния соединения. Интерфейсы PPP переходят в состояние DOWN до следующей успешной попытки соединения. Эти изменения сказываются, в частности, на таблице маршрутизации (см. §4.3.1).
При ADM:DOWN эти интерфейсы выключены всегда.

### §4.2.3. Ненумерованные IP-интерфейсы

Особым случаем является ненумерованный (*unnumbered*) интерфейс, используемый для соединения "точка-точка" и не имеющий собственного IP-адреса. Для такого интерфейса всегда используется маска 255.255.255.255, а параметр IADR задает IP-адрес удаленной стороны. Кроме того, для него предусмотрен специальный параметр SADR (Source Address). Этот адрес подставляется в качестве адреса источника во все IP-пакеты, посылаемые локальными службами устройства (Telnet, PING, HTTP, XOT и т.п.) через данный интерфейс. Аналогичный смысл имеет параметр SADR в ряде других команд. Указанный адрес либо должен либо принадлежать одному из IP-интерфейсов устройства, находящегося в состоянии UP, либо к нему должен быть сконфигурирован маршрут, ведущий через локальный интерфейс (подробно об IP-маршрутизации см. следующий раздел.) Пример:

```
S P IP:7 IADR:192.168.4.7 SADR:192.168.4.254 MASK:255.255.255.255
S I NET:192.168.4.254 MASK:255.255.255.255 IP:0
```

Параметр SADR позволяет также разрешить конфликтную ситуацию, которая возникает, если ненумерованный интерфейс является PPP-сервером и должен динамически назначать адрес удаленной стороне (PPP-клиенту). В этом случае значение IADR совпадает со значением RADR (или адресом, который выделяется для данного клиента сервером авторизации — см. Часть 8). Но такая конфигурация заведомо некорректна, поскольку клиент получает одинаковые адреса для себя самого и для сервера — и аварийно завершает процедуру IPCP. Чтобы избежать этого, следует установить для параметра SADR ненулевое значение, отличное от IADR и RADR; именно оно будет передаваться клиенту в качестве IP-адреса сервера. Пример:

```
S P IP:3 IADR:192.168.4.7 MASK:255.255.255.255 RADR:192.168.4.7 SADR:192.168.4.254
```

Избежать данной ситуации можно также другим способом — назначить IP-интерфейсу NSG произвольный фиктивный IP-адрес. Ничем, кроме лишних записей в таблице маршрутизации, такое решение не грозит.

### §4.2.4. Вторичные IP-адреса

Начиная с версии программного обеспечения 8.0.0b, для IP-интерфейсов маршрутизатора поддерживается механизм вторичных IP-адресов (*aliases*). Количество задаваемых вторичных адресов теоретически может быть любым, но на практике ограничено размером системной области памяти HEAP. В случае ее исчерпания попытка задать очередной вторичный адрес будет отвергнута с соответствующим диагностическим сообщением. (Размеры данной области могут быть увеличены командой S W HS:<байт>; подробнее об этой команде см. Часть 2.)

Механизм вторичных IP-адресов позволяет создавать в одной физической сети несколько подсетей IP. Вторичные IP-адреса могут назначаться интерфейсам любого типа, в том числе тем, которые подключены по схеме "точка-точка".

Для задания и удаления вторичного IP-адреса используются команды и Set IP и Clear IP следующего формата:

```
S I SECONDARY:<ip-адрес/маска> IP:<номер_ip-интерфейса>
C I SECONDARY:<ip-адрес/маска> IP:<номер_ip-интерфейса>
```

Адрес и маска задаются в десятичной дотовой нотации. Если маска не задана, то по умолчанию используется маска, соответствующая классу заданного IP-адреса. Примеры:

```
S I SECONDARY:192.168.1.15/255.255.255.248 IP:1
C I SECONDARY:192.168.3.254 IP:2
```

В обоих случаях для вступления изменений в силу необходимо рестартовать IP-интерфейс командой:

```
W S IP:<номер>
```

**ПРИМЕЧАНИЕ** Вторичные IP-адреса различных интерфейсов могут находиться в сетях с вложенными, но не совпадающими пространствами адресов. Например, допустима ситуация, когда для одного IP-интерфейса установлен адрес 10.0.0.1 с маской 255.0.0.0, а для другого — адрес 10.1.2.3 с маской 255.255.255.0.

Просмотреть вторичные IP-адреса, назначенные интерфейсу, можно при помощи команды Display Parameters:

```
D P IP:<номер>
```

Кроме того, для вторичных IP-адресов, как и для первичных, автоматически создаются записи в таблице маршрутизации, которую можно просмотреть командой D I.

# §4.3. IP-маршрутизация

## §4.3.1. Таблицы маршрутизации

Таблица IP-маршрутизации определяет адреса и маски IP-сетей, доступных в данный момент, интерфейсы и шлюзы, через которые передаются пакеты в эти сети, метрики маршрутов, количество пакетов, переданных по каждому маршруту, и другую информацию. Просмотр текущего состояния таблицы производится командой Display IP:

```
D I
```

Записи в таблице IP-маршрутизации формируются динамически на основании трех источников:

— таблицы статических маршрутов (*Static Routes*), назначенных администратором системы в явном виде (см. §4.3.2).
— параметров IADR и MASK тех IP-интерфейсов, которые активны в данный момент (см. ниже).
— информации, полученной маршрутизатором по протоколу RIP.

Каждый интерфейс маршрутизатора определяет некоторую IP-сеть, непосредственно подключенную к данному интерфейсу. Адрес сети формируется из параметров IADR и MASK интерфейса следующим образом: в адресе интерфейса обнуляются те биты, которые имеют нулевое значение в маске. Пример:

```
S P IP:1 ADM:UP IADR:14.0.0.1 MASK:255.0.0.0
```

Данная конфигурация определяет, что интерфейс IP:1 активен и обслуживает сеть с адресами 14.x.x.x. Сам интерфейс имеет в этой сети IP-адрес 14.0.0.1. После запуска устройства (или рестарта маршрутизатора командой W S IP:0) в таблице IP-маршрутизации будут автоматически созданы следующие записи для данного интерфейса:

| net | mask | gateway | metric | intf | ttl | use |
|---|---|---|---|---|---|---|
| 14.255.255.255 | 255.255.255.255 | 14.0.0.1 | 0 | 0 | 999 | 0 |
| 14.000.000.000 | 255.255.255.255 | 14.0.0.1 | 0 | 0 | 999 | 0 |
| 14.000.000.001 | 255.255.255.255 | 14.0.0.1 | 0 | 0 | 999 | 0 |
| 14.000.000.000 | 255.000.000.000 | 14.0.0.1 | 0 | 1 | 999 | 0 |

Для процесса IP-маршрутизации эта информация означает, что пакеты с адресами назначения 14.0.0.1 (адрес интерфейса), 14.0.0.0 (адрес сети) и 14.255.255.255 (широковещательный адрес в данной сети) будут направлены на локальный интерфейс (IP:0). Любой другой пакет с адресом назначения вида 14.x.x.x будет направлен через интерфейс IP:1 в подключенную к нему сеть. Метрика маршрута 0 указывает, что сеть подключена непосредственно к интерфейсу; шлюзом в этом случае является сам интерфейс. Для маршрутов в сети, не подключенные к маршрутизатору непосредственно, в таблице маршрутизации указывается IP-адрес следующего шлюза.

Параметр TTL (Time To Live) указывает оставшееся время действия записи (в секундах). Для динамических записей, созданных протоколом RIPv1, максимальное время жизни составляет 180 сек.; если за это время не получено новое сообщение RIP о существовании данного маршрута, запись удаляется из таблицы. Для статических записей TTL равно 999, что в данном случае означает неограниченный срок действия.

Если для некоторого адреса назначения найдено несколько подходящих записей, то выбирается запись с наименьшим количеством нулевых бит в маске.

Маршрут по умолчанию отличается от остальных маршрутов тем, что для него адрес и маска сети равны 0.0.0.0. Таким образом, под эту запись подпадают любые пакеты, проходящие через маршрутизатор. Но с учетом описанных выше приоритетов это означает, что маршрут по умолчанию применяется только для тех пакетов, чьи адреса назначения не удовлетворяют ни одной из остальных записей маршрутной таблицы.

Начиная с версии программного обеспечения 8.0.0b, IP-интерфейсы, привязанные к протоколам, которые способны определять состояние соединения на канальном уровне (Frame Relay, Cisco-HDLC, PPP, а также Fast Ethernet для серии NSG–800), автоматически переходят в состояние UP/DOWN в зависимости от состояния соединения. При этом в таблице маршрутизации появляются/исчезают записи, связанные с данным интерфейсом. В частности, происходит переинициализация всех статически заданных маршрутов.

### §4.3.2. Настройка статических маршрутов

Таблица статических маршрутов составляется администратором. Она служит одним из источников информации для формирования таблицы маршрутизации, но не совпадает с ней. Если, некоторый статический маршрут не является активным по каким-либо причинам (например, не определен путь к заданному шлюзу или имеется маршрут с меньшей метрикой), такой маршрут хранится в таблице статических маршрутов, но не включается в число действующих.

Для просмотра таблицы статических маршрутов используется команда Display IP следующего вида:

D I STATIC Вывод всех статических маршрутов (активных и неактивных)

Для установления статического маршрута к некоторой сети используются команды SET IP с обязательными параметрами NET, MASK и хотя бы одним из двух параметров GW и IP. Формат команды может быть одним из следующих:

S I NET:<ip-адрес> MASK:<маска> GW:<шлюз> MET:<метрика>

Для завершения записи в таблице производится дальнейший поиск до тех пор, пока не будет найдена запись, указывающая на один из IP-интерфейсов маршрутизатора. Шлюз может находиться как в непосредственно подключенной сети, так и в любой другой сети, маршрут к которой известен.

S I NET:<ip-адрес> MASK:<маска> IP:<номер_интерфейса> MET:<метрика>

Данный формат актуален для интерфейсов, привязанных к соединениям "точка-точка". Все пакеты, адресованные в указанную сеть, отправляются через указанный интерфейс.

S I NET:<ip-адрес> MASK:<маска> GW:<шлюз> IP:<номер_интерфейса> MET:<метрика>

Данный формат применим для интерфейсов любого типа и полностью определяет следующий шаг маршрута. Шлюз должен находиться в сети, непосредственно подключенной к указанному интерфейсу.

Метрика маршрута в исходном толковании этого параметра означает число промежуточных маршрутизаторов, через которые должен пройти пакет, прежде чем он достигнет требуемой сети. Однако поскольку метрика для статических маршрутов задается административно, ее можно использовать в качестве критерия для указания более или менее предпочтительного маршрута (например, через двух операторов или по двум каналам связи с различной стоимостью трафика). Если для некоторого адреса назначения найдено несколько подходящих записей, то выбирается запись с наименьшим количеством нулевых бит в маске, а если таких записей несколько — то с наименьшей метрикой. Пример:

```
S I NET:15.000.000.000 MASK:255.000.000.000 GW:14.0.0.3 IP:1 MET:4
S I NET:15.000.000.000 MASK:255.000.000.000 GW:16.0.0.4 IP:4 MET:2
S I NET:15.192.123.000 MASK:255.255.255.000 GW:14.0.0.7 IP:1 MET:1
```

В данном примере пакеты, адресованные хостам 15.192.123.x, будут передаваться через интерфейс IP:1 и шлюз 14.0.0.7. Пакеты с другими адресами вида 15.x.x.x будут передаваться через этот же интерфейс и шлюз 14.0.0.3. Если же, например, этот интерфейс будет выключен командами

```
S P IP:1 ADM:DOWN
W S IP:1
```

то те и другие пакеты пойдут по более длинному (или дорогому, или менее желательному по иным соображениям) маршруту через интерфейс IP:4 и шлюз 16.0.0.4.

Если несколько статических маршрутов проходят через работающие IP-интерфейсы и имеют одинаковую метрику, то приоритет имеет маршрут, который стоит выше в таблице статических маршрутов.

Для удаления маршрута используется команда CLEAR IP:

C I NET:<ip-адрес> MASK:<маска> ...

Дополнительно можно указать IP-адрес шлюза, номер интерфейса и/или метрику, чтобы удалить какой-либо конкретный маршрут. Если в действующей таблице маршрутизации содержится несколько маршрутов в данную сеть, а дополнительные параметры не указаны (или недостаточны для однозначной идентификации маршрута), удаляется первый из найденных маршрутов.

Если маршрут был задан статически, то он удаляется из обеих таблиц маршрутизации — статической и действующей (если он в это время находится в ней).

Для установления и удаления маршрутов по умолчанию используются команды:

```
S I DEFAULT GW:<шлюз> IP:<номер_интерфейса> MET:<метрика>
C I DEFAULT GW:<шлюз> IP:<номер_интерфейса> MET:<метрика>
```

Все IP-адреса и маски задаются в десятичной дотовой нотации. Обязательным является хотя бы один из двух параметров GW и IP. Значение метрики по умолчанию равно единице.

**ВНИМАНИЕ** Любой шлюз (параметр GW) должен находиться в IP-сети, маршрут к которой известен и действует. В противном случае маршрут будет добавлен в таблицу статических маршрутов, но не будет активирован.

**ПРИМЕЧАНИЕ** Если интерфейс, ведущий к удаленному шлюзу (заданному явно или по умолчанию), является интерфейсом типа ETHI, то метрика этого маршрута не может быть нулевой.

Как и другие параметры конфигурации, таблицу маршрутизации необходимо записать в энергонезависимую память командой

```
W F
```

### §4.3.3. Маршрутизация в NULL

Формальный интерфейс NULL в устройствах NSG не предусмотрен. Для уничтожения пакетов, которые не должны передаваться далее, следует использовать фильтры типа Drop или Reject. Подробно о фильтрации см. §4.5.

### §4.3.4. Служба RIP

Устройства NSG, работающие под управлением базового программного обеспечения, поддерживают протокол динамической маршрутизации RIPv1 (Routing Information Protocol, RFC–1058). С помощью этого протокола осуществляется обмен маршрутной информацией между смежными IP-маршрутизаторами и построение динамических таблиц маршрутизации. Включение и выключение службы RIP производится параметром RIP локального псевдоинтерфейса:

```
S P IP:0 RIP:YES   Использовать RIP.
S P IP:0 RIP:NO    Не использовать RIP.
```

Дополнительная настройка RIP не предусмотрена. Служба RIP всегда работает со следующими параметрами:

— Если служба RIP включена, то она работает на всех IP-интерфейсах маршрутизатора, в активном режиме и с использованием метода "расщепления горизонта" (*split horizon*).
— Для передачи сообщений RIP используется только широковещательная рассылка.
— Значения таймеров RIP соответствуют рекомендованным в RFC: 30, 180 и 120 секунд.
— Рассылка маршрутов в непосредственно подключенные сети производится всегда.
— Маршруты, полученные по RIP, имеют метрику от 1 до 15. Это следует учитывать в том случае, если для статических маршрутов назначаются более высокие значения метрики.
— В исходящие сообщения RIP включаются также статические маршруты и маршруты, используемые по умолчанию.
— Во входящих сообщениях RIP игнорируется информация о маршрутах, используемых по умолчанию.

Чтобы изменения вступили в силу, необходимо рестартовать IP-маршрутизатор командой W S IP:0.

**ПРИМЕЧАНИЕ** Расширенный набор протоколов динамической маршрутизации (RIPv2, OSPF, BGP и др.) поддерживается устройствами NSG–800, работающими под управлением программного обеспечения NSG Linux.

### §4.3.5. Служба DNS

Служба DNS (Domain Name Service) устанавливает соответствия между символьными именами хостов Интернет (например, www.gadukinotelecom.ru) и их цифровыми IP-адресами. Устройства NSG, работающие под управлением базового программного обеспечения, сами по себе не являются серверами DNS, но могут использовать внешние серверы DNS для локальных служб ping и traceroute, а также передавать их адреса удаленным клиентам PPP.

Работа службы DNS определяется параметрами DNS, DNS1, DNS2 локального псевдоинтерфейса:

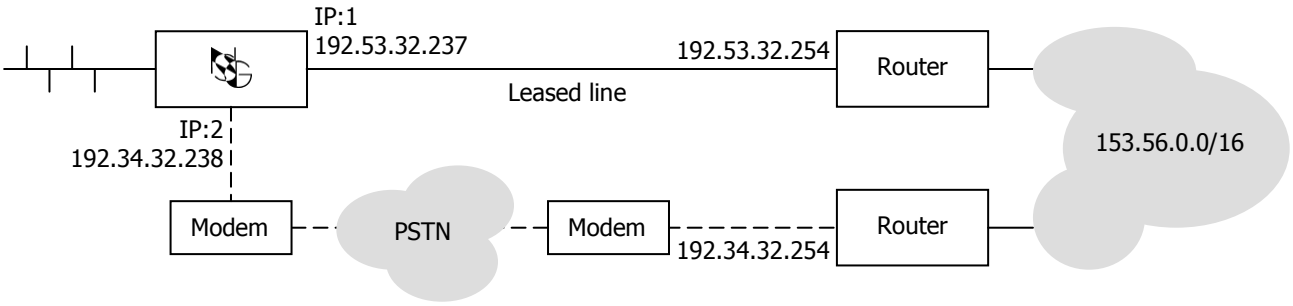
```
DNS:YES                 Использовать DNS (требует указания DNS1 и DNS2).
DNS:NO                  Не использовать DNS.
DNS1:<ip-адрес>         IP-адреса первичного и вторичного серверов DNS в десятичной дотовой нотации
DNS2:<ip-адрес>         (xxx.xxx.xxx.xxx).
```

Чтобы изменения вступили в силу, необходимо рестартовать службу DNS командой W S DNS, либо весь IP-маршрутизатор командой W S IP:0.

**ПРИМЕЧАНИЕ** Более широкая поддержка DNS (встроенный сервер или ретранслятор) может быть реализована на устройствах NSG–800, работающих под управлением программного обеспечения NSG Linux.

## §4.3.6. Установление резервного соединения по коммутируемой линии

Поддержка нескольких альтернативных маршрутов в таблице маршрутизации совместно с установлением исходящих соединений по требованию, обеспечиваемым PPP-интерфейсами устройств NSG, позволяет автоматически устанавливать резервные соединения по коммутируемым телефонным линиям в случае отказа основного соединения. Для этого требуется указать в таблице маршрутизации второй маршрут через PPP-интерфейс, к которому подключен резервный модем, и назначить ему более высокую метрику. Вместо метрики можно использовать порядок следования маршрутов в таблице. PPP-интерфейс следует настроить на установление соединения по требованию. Пример конфигурации:




```
S  P  PO:1  TY:HDLC  IF:SDSL
S  P  IP:1  TY:HDLC  PO:1 IADR:192.53.32.237  MASK:255.255.255.0  KEEP:180  ADM:UP

S  P  PO:2  TY:ASYNC_PPP  IF:V24  SP:115200
S  P  IP:2  TY:PPP  PO:2  SL:NO  DOD:YES  IADR:192.34.32.238  MASK:255.255.255.0  ADM:UP

S  I  NET:153.56.0.0  MASK:255.255.0.0  IP:1  MET:1
S  I  NET:153.56.0.0  MASK:255.255.0.0  IP:2  MET:2

S  P  IP:0  ADM:UP
W F
W S PO:A
```

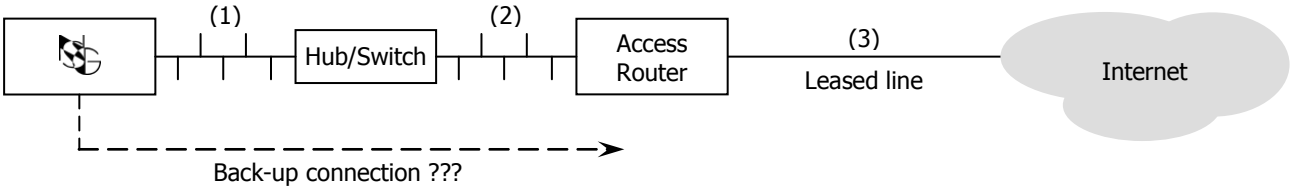
В нормальном режиме работы все пакеты, адресованные в сеть 153.56.0.0 с маской 255.255.0.0, передаются по выделенной линии SDSL с использованием протокола Cisco-HDLC. При отказе этого соединения соответствующий маршрут удаляется из таблицы маршрутизации, и его место занимает резервный маршрут с метрикой 2. Как только по этому маршруту посылается первый пакет, интерфейс PPP начинает устанавливать соединение по коммутируемой линии.

Если соединение по выделенной линии восстановлено, то основной маршрут снова появляется в таблице маршрутизации и становится действующим. Все пакеты отправляются по этому маршруту, а резервный интерфейс PPP через 3 минуты (KEEP:180) разрывает соединение по тайм-ауту.

**ПРИМЕЧАНИЕ** IP-адрес интерфейса номер 2 в данном примере может назначаться динамически удаленной стороной.

**ВНИМАНИЕ** Автоматическое установление резервного соединения возможно только для тех типов портов, которые способны определять состояние соединения на канальном уровне: Frame Relay, Cisco-HDLC, PPP, Fast Ethernet, и только начиная с версии 8.0.0b.

Необходимо подчеркнуть, что критерием для переключения на резервный канал является отказ на физическом или канальном уровне соединения, *непосредственно* входящего в маршрутизатор NSG. Например, если настраиваемый маршрутизатор включен в сеть Fast Ethernet, а на другой стороне этой сети находится маршрутизатор доступа, обеспечивающий связь с поставщиком услуг Интернет (см. рис.), то средствами этих двух уровней принципиально возможно — и это ни в коей мере не является особенностью продуктов NSG — обнаружить только отказ на участке (1) соединения с сетью, например, обрыв кабеля или выключение концентратора/коммутатора LAN. Если отказ произойдет на участке (2) между концентратором/коммутатором и внешним маршрутизатором, или, что наиболее вероятно, на соединении WAN (3) с Интернет-провайдером, то обнаружить его средствами физического или канального уровней в той точке, где расположен маршрутизатор NSG, невозможно. Следовательно, маршрутизатор NSG не будет переключаться на резервное соединение. Резервирование в этом случае необходимо обеспечить на внешнем маршрутизаторе.



### §4.3.7. Тест PING

Утилита PING (Programmable Inter-Networking Gauge) является основным инструментом для проверки доступности узлов IP-сети. Успешное прохождение *ping* на заданный адрес свидетельствует о нормальной работе данного маршрута на всех уровнях, включая физические соединения, протоколы канального уровня и IP-маршрутизацию на всех устройствах, через которые проходит маршрут.

Для выполнения теста PING используется команда Probe Ping:

```
P P IADR:<назначение>
```

где <назначение> — символическое имя требуемого хоста (при условии, что на устройстве включена и настроена служба DNS), либо его IP-адрес. Команда может иметь следующие необязательные параметры:

| | |
|---|---|
| SADR:<ip-адрес> | IP-адрес источника, который будет указываться в пакетах ICMP Echo-Request. По умолчанию, в качестве адреса источника указывается адрес того IP-интерфейса маршрутизатора, через который посылаются данные пакеты; если интерфейсу назначено несколько IP-адресов — то тот из них, который относится к тестируемому маршруту. Параметр SADR позволяет указать некоторый адрес явным образом. (Например, это может быть адрес в сети, находящейся по другую сторону от маршрутизатора NSG.) |
| CNT:<число> | Число посылаемых пакетов (от 0 до 2147483647). При CNT:0 (значение по умолчанию) тест продолжается до тех пор, пока не будет прерван нажатием клавиши Enter. |
| SIZE:<размер> | Длина поля данных в пакете (от 56 до 1586 байт.) Значение по умолчанию — 56 байт. Полная длина пакета больше этой величины на 8 байт. |
| WAIT:<секунды> | Время ожидания ответа удаленной системы (от 1 до 2147483647 сек). Значение по умолчанию — 0 (не ограничено). |
| PAUSE:<секунды> | Пауза между посылкой пакетов (от 0 до 2147483647 сек). Значение по умолчанию — 1 сек. |

### §4.3.8. Тест Traceroute

Утилита Traceroute предназначена для последовательного тестирования маршрута к заданному узлу IP-сети. Тест состоит в том, что на указанный адрес посылаются пакеты ICMP Echo-Request с ограниченным максимальным числом шагов (TTL). Когда время жизни пакета истекает на некотором промежуточном узле, узел возвращает сообщение, в котором содержится искомая информация о маршруте до этого узла. После этого пакеты посылаются со значением TTL, увеличенным на единицу, и доходят до следующего узла — и так далее до тех пор, пока не будет получен ответ от нужного адресата.

Для выполнения теста используется команда Probe Route:

```
P R IADR:<назначение>
```

где <назначение> — символическое имя требуемого хоста (при условии, что на устройстве включена и настроена служба DNS), либо его IP-адрес. Команда может иметь следующие необязательные параметры:

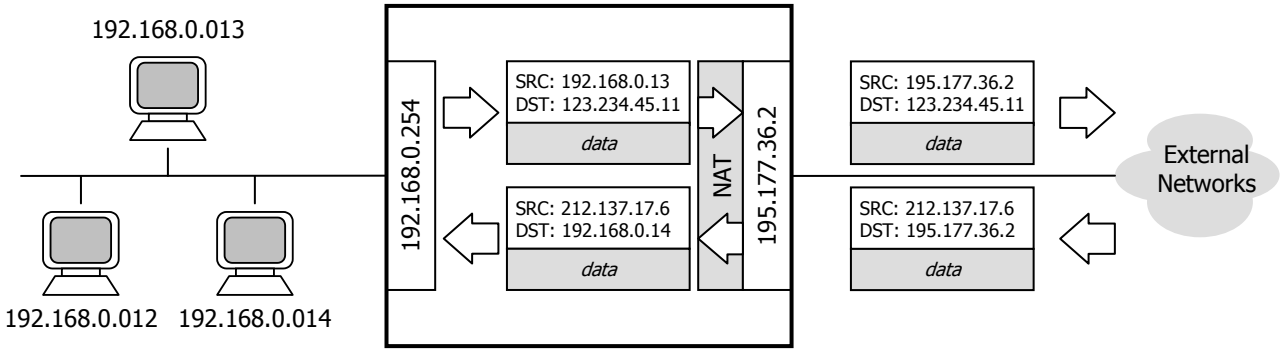
| | |
|---|---|
| SADR:<ip-адрес> | IP-адрес источника, который будет указываться в пакетах ICMP Echo-Request. По умолчанию, в качестве адреса источника указывается адрес того IP-интерфейса маршрутизатора, через который посылаются данные пакеты; если интерфейсу назначено несколько IP-адресов — то тот из них, который относится к тестируемому маршруту. Параметр SADR позволяет указать некоторый адрес явным образом. (Например, это может быть адрес в сети, находящейся по другую сторону от маршрутизатора NSG.) |
| MIN:<ttl> | Минимальное значение TTL, с которого начинается выполнение теста (от 0 до 255). Значение по умолчанию — 0. В ходе выполнения теста значение TTL увеличивается до тех пор, пока не будет получен ответ с IP-адреса назначения. |
| MAX:<ttl> | Максимальное значение TTL, до которого будет выполняться тест (от 0 до 255). Значение по умолчанию — 255. |
| CNT:<число> | Число пакетов, посылаемых с каждым значением TTL (от 0 до 2147483647). Значение по умолчанию — 3. |
| WAIT:<секунды> | Время ожидания ответа удаленной системы (от 0 до 2147483647 сек). Значение по умолчанию — 0 (не ограничено). |

# §4.4. Служба NAT

## §4.4.1. Трансляция сетевых адресов

Механизм трансляции сетевых адресов и портов (Network Address Translation, NAT) предназначен для преобразования IP-адресов и номеров портов TCP/UDP между сетью, подключенной к данному IP-интерфейсу маршрутизатора (далее именуемой *внешней сетью*, *внешними адресами* и т.п.), и всеми остальными IP-сетями, подключенными к маршрутизатору (далее — *внутренними сетями* и т.п.).

При передаче пакетов между собой хосты внутренней сети и соединенный с ней IP-интерфейс маршрутизатора используют свои внутренние IP-адреса. При передаче пакетов во внешний мир IP-интерфейс, связанный с внешней сетью, подставляет вместо внутреннего адреса источника заданный внешний адрес и отправляет пакет дальше. При поступлении пакетов на внешний интерфейс вместо адреса назначения подставляется адрес одного из локальных хостов (если для этого имеется подходящее правило преобразования) и пакет передается во внутреннюю сеть.




Использование трансляции сетевых адресов решает три важные задачи:

— Позволяет использовать одни и те же IP-адреса во многих подсетях, поскольку адресное пространство каждой внутренней подсети является локальным, а не частью глобального адресного пространства всего Интернет. Уникальными должны быть только внешние IP-адреса, назначенные интерфейсу с поддержкой NAT; эти адреса распределяются централизованно поставщиками услуг Интернет. Во внутренней сети могут использоваться любые адреса, назначенные администратором или, например, унаследованные в ходе какой-либо реструктуризации сети.

— Устраняет нехватку глобальных IP-адресов, присущую протоколу IPv4. За одним или несколькими глобальными адресами может стоять намного большее число хостов внутренней сети.

— Скрывает истинную структуру внутренней сети от внешнего мира и тем самым повышает ее безопасность.

**ПРИМЕЧАНИЕ** Следующие диапазоны IP-адресов выделены исключительно для использования в корпоративных сетях, изолированных от глобальной сети Интернет преобразователями адресов:

в классе A — 10.0.0.0 ... 10.255.255.255
в классе B — 172.16.0.0 ... 172.31.255.255
в классе C — 192.168.0.0 ... 192.168.255.255

Эти адреса и сети называются приватными (*private*), локальными или "серыми", в отличие от глобальных или "белых" адресов, распределяемых централизованно.

Именно эти адреса желательно использовать при построении внутренних сетей. Напротив, в глобальной сети Интернет такие адреса использоваться не могут, а любой пакет, приходящий извне с таким адресом источника или назначения, должен уничтожаться — это либо результат ошибки в конфигурации чьего-то маршрутизатора, либо попытка злонамеренного вмешательства в работу данной сети.

Понятие NAT является собирательным и включает в себя целый ряд различных алгоритмов, по которым производится преобразование IP-адресов и портов при обращении из внутренней сети во внешнюю, из внешней во внутреннюю, или в обоих направлениях. В настоящее время устройства NSG поддерживают два наиболее употребительных варианта NAT: IP-маскарадинг и виртуальные сервера.

Механизм NAT работает и настраивается независимо для каждого IP-интерфейса.

**ПРИМЕЧАНИЕ** Для работы NAT необходимо, чтобы интерфейсу был назначен хотя бы один глобальный IP-адрес.

### §4.4.2. IP-маскарадинг

Механизм IP-маскарадинга позволяет нескольким хостам внутренней сети выходить во внешнюю сеть, используя один внешний адрес. Обмен IP-пакетами происходит следующим образом:

— Интерфейс получает пакет от хоста во внутренней сети, адресованный во внешнюю сеть. Внутренний IP-адрес источника заменяется внешним адресом интерфейса; для пакетов TCP и UDP номер порта источника заменяется некоторым новым номером порта, относящимся к данному интерфейсу, а для пакетов ICMP — идентификатор пакета заменяется новым идентификатором. Последние преобразования обязательны, поскольку именно они позволяют различать пакеты, относящиеся к различным хостам внутренней сети.

— В списке текущих сеансов NAT делается запись о выполненном преобразовании, после чего пакет отправляется во внешнюю сеть.

— Когда на интерфейс из внешней сети поступает пакет, в котором адрес назначения равен IP-адресу интерфейса, номер порта назначения или идентификатор исходного пакета, указанные в заголовке, проверяются по таблице текущих сеансов NAT. Если запись с таким номером порта или идентификатором найдена, выполняется обратное преобразование, и пакет отправляется во внутреннюю сеть. Если такая запись не найдена, т.е. ни один из внутренних хостов ранее не обращался к данному внешнему хосту, пакет уничтожается.

Таким образом, при использовании IP-маскарадинга хосты внутренней сети остаются невидимыми для внешнего мира до тех пор, пока они сами не обратятся к некоторому внешнему серверу. После этого они становятся видимыми для данного сервера, и только для него, причем строго определенным образом:

— Пакеты датаграммных протоколов (UDP и ICMP) принимаются интерфейсом с включенной функцией NAT строго определенным образом: на один исходящий во внешнюю сеть пакет может быть принят только один входящий пакет. После этого запись удаляется из таблицы NAT.

— Пакеты TCP-соединений, установленных по инициативе внутреннего хоста (например, при работе web-броузера, электронной почты, Telnet и др. приложений) могут передаваться в произвольном порядке и произвольном количестве до тех пор, пока это соединение не разорвано.

— Пакеты, использующие любые иные протоколы транспортного уровня (в частности, GRE, L2TP, VPN) через NAT не проходят и уничтожаются.

— Внешние хосты не могут инициировать обмен пакетами с хостами внутренней сети ни в каком случае.

**ПРИМЕЧАНИЕ** Исключением из последнего правила являются соединения ftp-data (порт 20), устанавливаемые в направлении от внешнего сервера FTP к клиенту во внутренней сети. (Так называемый "активный режим" протокола FTP.) Для входящих пакетов ftp-data ищется ранее установленное соединение ftp (порт 21) от внутреннего клиента к данному внешнему хосту. Если такое соединение найдено, пакет передается этому клиенту.

**ПРИМЕЧАНИЕ** Как можно видеть, механизм IP-маскарадинга не предусматривает работу приложений, в которых запрос из одного или нескольких пакетов, посланных во внешнюю сеть, генерирует поток пакетов UDP в обратном направлении. К таким приложениям относятся, в частности, сетевые игры, потоковое аудио- и видеовещание. Чтобы использовать эти приложения, их необходимо настроить таким образом, чтобы они использовали в качестве транспорта протокол TCP или какой-либо прикладной протокол на его основе (чаще всего — HTTP). Соответствующие режимы выбираются в разделе "настройка" данного приложения.

Обойти ограничения на передачу UDP-потоков и иных протоколов, помимо UDP/TCP/ICMP можно с помощью избирательного преобразования адресов (см. пункт "в" ниже). Если таблица NAT задана явно, то все пакеты из сетей, не подпадающих под эту таблицу, передаются без преобразования. Таким образом, требуемые хосты можно вывести из-под действия NAT.

Механизм IP-маскарадинга для каждого IP-интерфейса может находиться в одном из следующих режимов:

**а) передача без преобразования**

NAT для данного интерфейса выключен командой:

```
S P IP:<номер> NAT:NO
```

Этот режим устанавливается по умолчанию.

**б) преобразование всех пакетов с использованием первичного IP-адреса интерфейса**

Интерфейс преобразует все проходящие через него пакеты. В пакетах, поступающих из маршрутизатора для передачи во внешнюю сеть, вместо IP-адреса источника подставляется первичный IP-адрес интерфейса. Для пакетов, принимаемых из внешней сети и имеющих этот адрес в качестве адреса назначения, ищется запись в таблице NAT.

Для использования данного режима необходимо установить

```
S P IP:<номер> NAT:YES
```

а таблица NAT для данного интерфейса (см. ниже) не должна содержать ни одной записи.

**в) избирательное преобразование с использованием таблицы NAT**

Интерфейс преобразует проходящие через него пакеты, если для их источника установлено некоторое правило NAT. Пакеты от тех хостов, которые не подпадают ни под одну из записей таблицы NAT, передаются без изменения.

Для использования данного режима необходимо установить

```
S P IP:<номер> NAT:YES
```

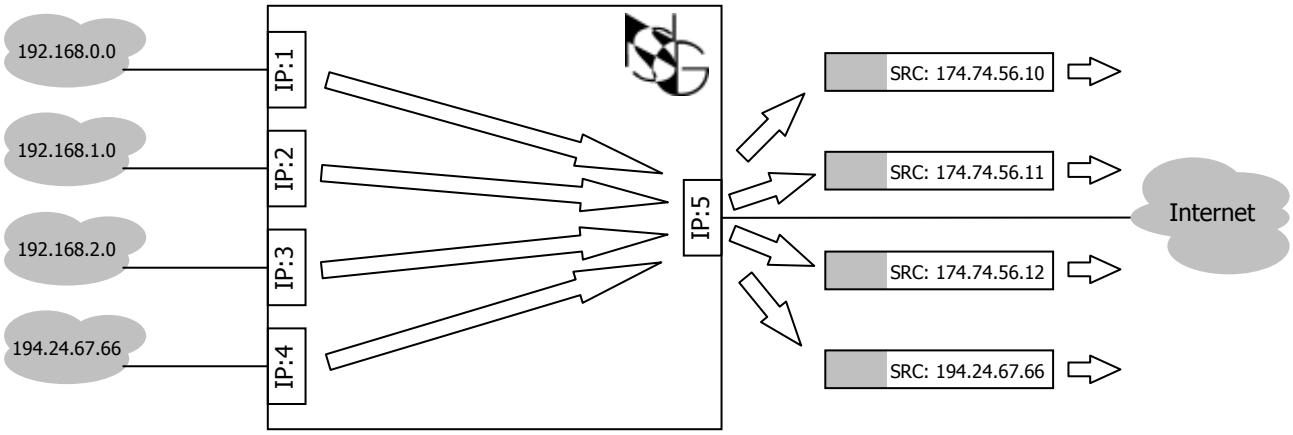
а таблица NAT должна содержать хотя бы одну запись.

Таблица трансляции адресов формируется для каждого интерфейса отдельно. Каждая запись таблицы определяет некоторую внутреннюю сеть (адрес и маска) и внешний (глобальный) адрес, подставляемый при процедуре трансляции. Для добавления и удаления записей используются команды Set NAT и Clear NAT:

```
S N IP:<номер_интерфейса> EADR:<внешний_ip-адрес> IADR:<ip-адрес_сети> MASK:<маска_сети>
C N IP:<номер_интерфейса> EADR:<внешний_ip-адрес> IADR:<ip-адрес_сети> MASK:<маска_сети>
```

Все параметры обязательны и должны вводиться строго в указанной последовательности. После внесения изменений в таблицу необходимо рестартовать данный IP-интерфейс. Пример:

```
S N IP:5 EADR:174.74.56.10 IADR:192.168.0.0 MASK:255.255.255.0
S N IP:5 EADR:174.74.56.11 IADR:192.168.1.0 MASK:255.255.255.0
S N IP:5 EADR:174.74.56.12 IADR:192.168.2.0 MASK:255.255.255.0
W S IP:5
```




В данном случае для трех внутренних сетей установлены три раздельных внешних IP-адреса, соответственно. Пакеты, отправляемые из четвертой сети (194.24.67.66), а также из остальных сетей, подключенных к маршрутизатору, будут проходить через интерфейс номер 5 без преобразования, а компьютеры, расположенные в этой сети, будут доступны из Интернет.

При формировании таблицы NAT возможны следующие частные случаи:

— Один внешний адрес может использоваться для трансляции адресов нескольких внутренних сетей.
— Адресные пространства внутренних сетей, указанных в различных строках таблицы NAT, могут пересекаться, т.е. адреса некоторых внутренних хостов могут подпадать под действие сразу нескольких строк таблицы. В этом случае глобальный адрес выбирается из строки, в которой маска подсети определена наиболее полно (т.е. содержит наибольшее количество единиц).
— Чтобы определить индивидуальное преобразование адреса для некоторого хоста, следует указать его IP-адрес в качестве внутренней сети с маской 255.255.255.255.

Для просмотра таблицы NAT используется команда Display NAT:

```
D N IP:<номер_интерфейса>
```

Все записи таблицы трансляции адресов, наряду с другими параметрами конфигурации, сохраняются в энергонезависимой памяти устройства командой W F. Список текущих сеансов NAT выводится командой Display Status/Statistics следующего формата:

```
D S NAT:<номер_интерфейса>
```

В начале списка также выводится текущая таблица NAT. Пример вывода:

```
Manager: d s nat:2
~~~~~~~~~~~ Current Address Translation Table ~~~~~~~~~~~~~~~~~~~~
External Address        Internal Net          Subnet Mask
194.67.244.230          10.0.0.0              255.0.0.0
~~~~~~~~~~~~~ Current  Virtual  Server  Table  ~~~~~~~~~~~~~~~~~~
   External Address:Port          Internal Address:Port          Protocol
[здесь выводится таблица виртуальных серверов, см. следующий параграф]
#     Prot  Internal IP/Port(ID)      Local IP/Port(ID)          Remote IP/Port
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
2     TCP   10.0.0.21  2043    194.67.244.230  59521   194.67.35.191    80
3     TCP   10.0.0.19  1094    194.67.244.230  59046   208.239.159.17   80
4     TCP   10.0.0.19  1097    194.67.244.230  59047   208.239.159.17   80
1     TCP   10.0.0.21  2044    194.67.244.230  59514   205.188.7.144    5190
5     TCP   10.0.0.15  2164    194.67.244.230  59051   212.5.91.195     110
6     TCP   10.0.0.15  2165    194.67.244.230  59052   194.67.23.76     110
7     TCP   10.0.0.15  2166    194.67.244.230  59053   213.180.193.87   110
8     TCP   10.0.0.21  2310    194.67.244.230  59054   213.180.194.130  80
9     TCP   10.0.0.21  2312    194.67.244.230  59056   194.67.35.195    80
10    TCP   10.0.0.21  2315    194.67.244.230  59059   213.180.194.113  80
11    TCP   10.0.0.21  2317    194.67.244.230  59060   213.180.194.131  80
12    TCP   10.0.0.21  2316    194.67.244.230  59061   213.180.194.130  80
13    TCP   10.0.0.21  2318    194.67.244.230  59062   213.180.194.113  80
14    TCP   10.0.0.21  2319    194.67.244.230  59063   213.180.194.131  80
15    TCP   10.0.0.19  1098    194.67.244.230  59064   208.239.159.17   80
```

### §4.4.3. Виртуальные сервера

Механизм виртуальных серверов позволяет размещать во внутренней сети серверы, доступные из внешнего мира. Когда из внешней сети поступает IP-пакет с глобальным адресом, типом протокола и номером порта назначения, указанными в таблице NAT, интерфейс передает их соответствующему хосту во внутренней сети. В ответах, посылаемых внешнему клиенту, внутренний IP-адрес сервера и номер порта источника заменяются глобальным IP-адресом и номером порта.

Внутри локальной сети сервер доступен по своему внутреннему адресу и номеру порта.

Для добавления и удаления записей в таблице виртуальных серверов используются команды Set NAT и Clear NAT следующего формата:

```
S  N  IP:<номер>  EADR:<ip-адрес>  IADR:< ip-адрес>  PT:<протокол>  DEP:<порт>  DIP:<порт>
C  N  IP:<номер>  EADR:<ip-адрес>  IADR:< ip-адрес>  PT:<протокол>  DEP:<порт>  DIP:<порт>
```

где параметры EADR и DEP определяют IP-адрес и номер порта, по которым сервер виден из внешнего (*external*) мира; IADR и DIP — фактические IP-адрес и номер порта сервера во внутренней (*internal*) сети. Номера внутреннего и внешнего портов могут быть как одинаковыми, так и различными. Параметр PT определяет тип протокола транспортного уровня и может принимать значение TCP или UDP. Все параметры обязательны и должны вводиться строго в указанной последовательности.

Сочетание внешнего адреса (EADR) и номера порта (DEP) для данного типа протокола должно быть уникальным для данного интерфейса. Также уникальным должно быть сочетание внутреннего адреса (IADR) и номера порта (DIP) для данного типа протокола.

Кроме того, запись, определяющая виртуальный сервер, одновременно используется для IP-маскарадинга: если указанный хост (IADR) во внутренней сети начнет посылать пакеты наружу, с указанным типом протокола и номером порта источника (DIP), то во внешнюю сеть они будут отправляться с адресом источника EADR и номером порта источника DEP.

**ПРИМЕЧАНИЕ** Для некоторых серверов таблица должна содержать более одной записи. Например, сервер FTP использует два порта (20 и 21).

После внесения изменений в таблицу NAT необходимо рестартовать IP-интерфейс командой W S IP:<номер>.

Таблица виртуальных серверов является частью таблицы NAT, и для ее просмотра используется та же команда

```
D  N  IP:<номер>
```

При выполнении этой команды сначала выводятся строки из таблицы IP-маскарадинга, а затем строки таблицы виртуальных адресов, например:

```
Manager: D N IP:2

  IP:2 EADR:210.1.2.7 IADR:10.0.0.0 MASK:255.0.0.0
  IP:2 EADR:210.1.2.1 IADR:10.0.0.2 PT:TCP DEP:80 DIP:80
  IP:2 EADR:210.1.2.5 IADR:10.0.0.2 PT:TCP DEP:23 DIP:23
```

Все записи таблицы трансляции адресов, наряду с другими параметрами конфигурации, сохраняются в энергонезависимой памяти устройства командой W F.

Просмотр текущих сеансов NAT (включая IP-маскарадинг и работу виртуальных серверов) осуществляется командой

```
D S NAT:<номер>
```

Виртуальные сервера могут располагаться на одной или нескольких машинах внутренней сети и использовать один внешний IP-адрес или различные адреса. Этот же адрес может использоваться хостами внутренней сети для доступа в Интернет. Примеры:

**а) различные машины, различные внешние адреса**

```
S P IP:2 IADR:210.1.2.81 ... NAT:YES
S N IP:2 EADR:210.1.2.83 IADR:10.0.0.1 PT:TCP DEP:20 DIP:20
S N IP:2 EADR:210.1.2.83 IADR:10.0.0.1 PT:TCP DEP:21 DIP:21
S N IP:2 EADR:210.1.2.89 IADR:10.0.0.2 PT:TCP DEP:80 DIP:80
```

FTP-сервер, представленный внешним адресом 210.1.2.83, находится на машине с адресом 10.0.0.1. HTTP-сервер, представленный внешним адресом 210.1.2.89 — на машине с адресом 10.0.0.2. Все машины локальной сети выходят во внешний мир под адресом 210.1.2.81, но к своим серверам FTP и HTTP обращаются по внутренним адресам 10.0.0.1 и 10.0.0.2, соответственно.

**б) различные машины, один внешний адрес**

```
S P IP:2 IADR:210.1.2.83 ... NAT:YES
S N IP:2 EADR:210.1.2.83 IADR:10.0.0.1 PT:TCP DEP:20 DIP:20
S N IP:2 EADR:210.1.2.83 IADR:10.0.0.1 PT:TCP DEP:21 DIP:21
S N IP:2 EADR:210.1.2.83 IADR:10.0.0.2 PT:TCP DEP:80 DIP:8080
S N IP:2 EADR:210.1.2.83 IADR:10.0.0.3 PT:TCP DEP:25 DIP:25
```

FTP-сервер находится во внутренней сети на машине с адресом 10.0.0.1, HTTP-сервер — на машине с адресом 10.0.0.2, сервер SMTP — на машине с адресом 10.0.0.3. Для сервера HTTP производится еще и отображение портов (*port mapping*). Однако во внешней сети все три сервера представлены одним адресом 210.1.2.83. С точки зрения клиентов, обращающихся к этим серверам откуда-то из Интернет, это одна и та же машина, на которой работают все три сервера, но на самом деле эта машина виртуальная. Кроме того, под этим же адресом (210.1.2.83) машины локальной сети выходят во внешний мир.

**в) одна машина, различные внешние адреса**

```
S P IP:2 IADR:210.1.2.83 ... NAT:YES
S N IP:2 EADR:210.1.2.83 IADR:10.0.0.1 PT:TCP DEP:20 DIP:20
S N IP:2 EADR:210.1.2.83 IADR:10.0.0.1 PT:TCP DEP:21 DIP:21
S N IP:2 EADR:210.1.2.89 IADR:10.0.0.1 PT:TCP DEP:80 DIP:80
S N IP:2 EADR:210.1.2.86 IADR:10.0.0.1 PT:TCP DEP:25 DIP:25
```

Все три сервера (FTP, HTTP и SMTP) физически работают на одной машине с адресом 10.0.0.1 во внутренней сети. Хосты внутренней сети могут обращаться к ним по этому адресу. Однако для клиентов, находящихся во внешней сети, это три различных хоста с адресами 210.1.2.83, 210.1.2.89 и 210.1.2.86, соответственно.

# §4.5. Фильтрация и коммутация IP-пакетов

## §4.5.1. Таблица фильтров

Правила фильтрации и коммутации IP-пакетов хранятся в устройствах NSG в виде таблицы фильтров, где каждая запись представляет собой один фильтр. Фильтры применяются к пакетам в порядке следования в таблице; таким образом, номер фильтра в таблице определяет его приоритет. Наивысший приоритет имеет фильтр с номером 0, стоящий в таблице первым.

Для создания фильтров используется команда Set IP со следующими обязательными параметрами:

```
S I FILTER PR:<приоритет> TY:<тип> NAME:<имя> EN:<статус> <критерии...>
```

Параметр PR определяет номер фильтра в списке, т.е. его приоритет. Если в таблице уже имеется запись с таким номером, то она и все последующие записи сдвигаются на одну позицию вниз. Аналогично, при удалении фильтра с некоторым номером все последующие записи сдвигаются вверх. Таким образом, таблица фильтров всегда имеет сплошную нумерацию от 0 до номера последнего фильтра и сохраняет порядок следования существующих фильтров (но не их абсолютные номера). Если номер создаваемого фильтра не указан, он записывается в таблицу последним.

Параметр TY определяет тип фильтра. Допустимые типы фильтров и совершаемые ими действия описаны в §4.5.3.

Параметр NAME задает имя фильтра в виде текстовой строки длиной до 31 символа. Если имя содержит разделители (пробел : ; = ,) или вопросительный знак, его необходимо заключить в кавычки. Подробно о формате текстовых параметров см. Часть 9. Кроме того, имя фильтра не может содержать звездочку (*). Если имя не задано, оно назначается автоматически в виде NONAME_xxx, где xxx — уникальное трехзначное число. Имена позволяют производить групповые операции с фильтрами, а также включать/выключать их при помощи атрибута Filter-Id, который может содержаться в ответе сервера RADIUS.

Параметр EN (Enable) устанавливает административный статус фильтра:

EN:YES Фильтр включен постоянно.

EN:NO Фильтр выключен постоянно.

Следующие четыре значения данного параметра описывают шаблоны, которые используются для динамического включения фильтров при сеансовом доступе по протоколу PPP. Чтобы включить фильтр, сервер доступа должен прислать его имя в атрибуте Filter-Id (RADIUS) или inacl, outacl (TACACS+). В этом случае на основе указанного шаблона создается индивидуальный фильтр по следующим правилам:

EN:D Фильтр копирует шаблон "как есть" (аналогично динамически включаемым фильтрам в версиях 8.1.0–8.2.1) и отличается от него только именем.

EN:DI В параметр IN создаваемого фильтра подставляется номер интерфейса, к которому подключен данный пользователь.

EN:DO Номер интерфейса подставляется в параметр OUT создаваемого фильтра.

EN:DIO Номер интерфейса подставляется в параметры IN и OUT создаваемого фильтра.

Имя создаваемого фильтра состоит из имени шаблона и номера интерфейса. Например, если пользователь подключен к IP-интерфейсу 3, в ответе сервера получен атрибут Filter-ID=guest, и в устройстве определен шаблон фильтра

```
S I FILTER PR:n NAME:guest EN:DI ...
```

то при открытии сеанса PPP будет создан и включен следующий фильтр:

```
FILTER PR:n NAME:guest3 IN:3 ...
```

Фильтр вставляется в таблицу с тем же приоритетом, что исходный шаблон, т.е. сам шаблон и все последующие строки фильтров сдвигаются вниз на единицу. После завершения сеанса данный фильтр удаляется автоматически. Более подробно об использовании динамических фильтров см. Часть 8.

Остальные параметры задают критерии, по которым производится отбор пакетов. Подробно эти критерии рассмотрены в следующем параграфе.

Для удаления фильтров используется команды Clear IP в одном из следующих форматов:

```
C I FILTER PR:<приоритет>
C I FILTER NAME:<имя>
```

Для просмотра отдельной записи или всей таблицы фильтров используется команда Display IP:

```
D I FILTER PR:<приоритет>
D I FILTER NAME:<имя>
D I FILTER
```

Для изменения параметров существующих фильтров используются команды:

```
X I FILTER PR:<приоритет> ...
X I FILTER NAME:<> ...
```

Параметры этой команды полностью аналогичны команде S I FILTER. Фильтр безусловно идентифицируется своим номером в таблице, т.е. если параметры PR и NAME заданы одновременно, но значение NAME не совпадает с именем существующего фильтра под номером PR, то этот фильтр будет переименован. В остальных случаях для обращения к фильтру достаточно указать его имя.

Просмотр, изменение параметров и удаление могут производиться не только с отдельными фильтами, но с группами фильтров, имеющих единообразные имена. Соответствующие команды допускают в качестве параметра NAME как точное значение имени, так и шаблоны имен, содержащие одну или несколько звездочек. Звездочка означает любое количество символов и может стоять в любом месте шаблона. Например, под шаблон A*B*C подпадают все имена, которые начинаются с A, оканчиваются на C и имеют в середине букву B. Или, если есть набор фильтров с именами Ad1, Ad2, Advertising, AdSite и т.п., запрещающих доступ к генераторам бесполезного трафика, то команда

```
X I FILTER NAME:Ad* EN:YES
```

включает сразу все эти фильтры. Это же относится и к динамически создаваемым фильтрам, причем звездочки могут как содержаться в ответе сервера аутентификации, так и прибавляться к нему уже при обработке ответа в устройстве NSG (параметр FTM:YES в описании способа аутентификации). Подробнее об использовании динамических фильтров см. Часть 8.

## §4.5.2. Критерии фильтрации

Для фильтрации пакетов используется совокупность следующих критериев:

**IN, OUT** Номера IP-интерфейсов, через которые пакеты поступают в маршрутизатор и отправляются из него, соответственно. Значениями обоих параметров являются списки IP-интерфейсов (через запятую). Непрерывные диапазоны номеров интерфейсов могут быть указаны через дефис. Пример:

```
IN:1,3,7–10,18 OUT:0,2
```

Данный фильтр применяется к пакетам, входящим через интерфейсы номер 1, 3, 7, 8, 9, 10 и 18 и уходящим через интерфейсы номер 0 и 2.

**SA, DA** Адреса источника (Source Address) и назначения (Destination Address), соответственно. Значения параметров записываются в формате адрес/маска в десятичной дотовой нотации, например:

```
DA:192.168.0.0/255.255.0.0
```

— фильтр применяется ко всем пакетам, направленным в сети 192.168.x.x.

Если маска не указана, то по умолчанию полагается маска 255.255.255.255, т.е. фильтр применяется только к конкретному IP-адресу.

**PT** Тип протокола транспортного уровня:

| | |
|---|---|
| PT:ICMP | Протокол ICMP. |
| PT:UDP | Протокол UDP. |
| PT:TCP | Протокол TCP. |

**SP, DP** Номера портов источника (Source Port) и назначения (Destination Port), соответственно. Эти параметры допустимы только для протоколов TCP и UDP. Значения параметров указывают конкретный номер или диапазон номеров портов. Примеры:

| | |
|---|---|
| SP:1234 | Порт 1234 |
| DP:2001–8000 | Диапазон портов от 2001 до 8000 включительно |
| SP:1024– | Диапазон портов от 1024 и выше (до 65535 включительно) |
| DP:–1023 | Все порты с номерами до 1023 включительно |

**IT** Тип пакетов ICMP. Параметр допустим только для протокола ICMP. Указывается в виде:

```
IT:<идентификатор_типа>
```

**ВНИМАНИЕ** Если в устройстве используется NAT, то параметры SA, DA, SP, DP всегда должны отражать IP-адреса и номера портов во *внешней* сети.

Для любого из вышеперечисленных параметров допустимо также значение ALL, означающее любые интерфейсы, IP-адреса, номера портов или типы пакетов, соответственно.

Чтобы фильтр сработал, пакет должен удовлетворять всем критериям одновременно. Если какие-либо критерии не указаны явно, то для них по умолчанию полагается значение ALL; таким образом, пакет должен удовлетворять только явно заданным критериям.

**ПРИМЕЧАНИЕ** Значение PT:ALL несовместимо ни с какими значениями параметров SP, DP, IT, кроме ALL.

### §4.5.3. Типы фильтров

Каждый пришедший IP-пакет проверяется на предмет соответствия записям в таблице фильтрации в порядке убывания приоритетов (начиная с записи номер 0). Сначала проверяется номер интерфейса, с которого пришел пакет. Далее проверяются адреса, тип протокола и параметры протокола. Если параметры пакета совпали с параметрами записи таблицы фильтрации, то дальнейшие действия зависят от типа фильтра:

TY:D Сброс пакета (Drop). По таблице маршрутизации определяется номер интерфейса, на который должен пересылаться данный пакет. Если данный интерфейс содержится в списке значений параметра OUT, пакет уничтожается; если нет — пакет продолжает проверяться на предмет соответствия последующим фильтрам.

TY:R Отказ в приеме пакета (Reject). Выполняются те же действия, что и в случае TY:D, но при уничтожении пакета отправителю возвращается ICMP-сообщение "хост недоступен" (для пакетов ICMP) или "порт недоступен" (для пакетов TCP/UDP).

TY:A Прием пакета (Accept). По таблице маршрутизации определяется номер интерфейса, на который должен пересылаться данный пакет. Если данный интерфейс содержится в списке значений параметра OUT, пакет пересылается, и дальнейшие фильтры к нему не применяются; если нет — пакет продолжает проверяться на предмет соответствия последующим фильтрам.

TY:E Прием пакетов TCP только для установленных (Established) TCP-соединений. Если соединение установлено, то все передаваемые по нему пакеты имеют флаг ACK и/или RST. Для таких пакетов выполняются те же действия, что и при TY:A; для пакетов TCP без этих флагов, а также для пакетов UDP и ICMP, продолжается проверка на предмет соответствия последующим фильтрам.

Использование данного фильтра предполагает, что в параметре IN указываются интерфейсы, подключенные к Интернет (или к менее защищенному сегменту сети), а в параметре OUT — к корпоративной сети (или к более защищенному сегменту). Таким образом, хосты корпоративной сети могут посылать в Интернет любые пакеты, в том числе устанавливать TCP-соединения; однако фильтр не разрешает хостам Интернет инициировать соединения с хостами внутри корпоративной сети. После того, как соединение установлено, пакеты передаются в обоих направлениях. Разрыв соединения возможен по инициативе любой из сторон.

**ПРИМЕЧАНИЕ** Применение фильтров типа Accept и Established имеет смысл в том случае, если после них определены (с низшим приоритетом) фильтры типа Drop или Reject с более широкими критериями. Пример:

```
S I FILTER PR:10 TY:E IN:1 OUT:2 DP:1024–
S I FILTER PR:11 TY:D IN:1 OUT:2 DP:1024–
```

Такой набор фильтров пропускает с интерфейса номер 1 на интерфейс номер 2 пакеты TCP с номером порта назначения 1024 и выше только в том случае, если они относятся к уже установленному соединению. В противном случае такие пакеты уничтожаются.

Данная ситуация отчасти схожа с тем, что имеет место при IP-маскарадинге: хосты внутренней сети становятся недоступными из Интернет. Однако использование фильтра типа Established для этой цели имеет два принципиальных отличия: а) правило фильтрации относится только к TCP-соединениям; б) IP-адреса и номера портов не изменяются.

TY:S Статическая коммутация IP-пакетов (Switching). Пакет пересылается на интерфейс, заданный параметром OUT. Этот параметр является обязательным и должен содержать только один номер интерфейса:

```
S I FILTER PR:<приоритет> TY:S OUT:<интерфейс> <критерии...>
```

Вместе с номером интерфейса может быть задан IP-адрес шлюза, которому должен быть передан пакет, в следующем формате:

```
OUT:<интерфейс>/<шлюз>
```

Указание шлюза имеет смысл только для IP-интерфейса, подключенного к сети Ethernet. Если для такого интерфейса номер шлюза не указан, пакет передается в сеть Ethernet с широковещательным адресом назначения.

**ПРИМЕЧАНИЕ** Правила IP-коммутации являются односторонними, т.е. задание коммутации с интерфейса N на интерфейс M никак не определяет прохождение пакетов в обратном направлении. Для двусторонней коммутации необходимо определить два правила, действующие во встречных направлениях.

Если все параметры пакета соответствуют критериям данного фильтра, то выполняются указанные действия, и на этом фильтрация прекращается. Если хотя бы один критерий не выполняется, то данный фильтр игнорируется, и устройство пытается применить к пакету следующий фильтр. Если пакет не подпадает ни под один из фильтров, то он маршрутизируется обычным образом.

Таким образом, по умолчанию фильтрация носит разрешительный характер: все пакеты, которые не запрещены явно одним из фильтров типа Drop или Reject, в конце концов пропускаются и маршрутизируются. Для того, чтобы ввести "параноидальный" или "диктаторский" принцип фильтрации — "запрещено всё, что не разрешено" — последним в таблице должен стоять запрещающий фильтр, под который подпадают все пакеты:

```
S I FILTER TY:D EN:YES
```

В этом случае будут пропущены только пакеты, удовлетворяющие заданным критериям для вышестоящих фильтров типа Accept и Established.

Пример:

```
PR:00 TY:S IN:1,2,4–7,10 SA:ALL DA:ALL PT:ALL OUT:3/10.0.0.10
PR:01 TY:A IN:ALL SA:192.92.92.1/255.255.255.255 DA:ALL PT:ALL OUT:ALL
PR:02 TY:D IN:ALL SA:192.92.92.0/255.255.255.0 DA:ALL PT:ALL OUT:ALL
PR:03 TY:D IN:ALL SA:ALL DA:ALL PT:TCP SP:0–65535 DP:2000–65535 OUT:8
```

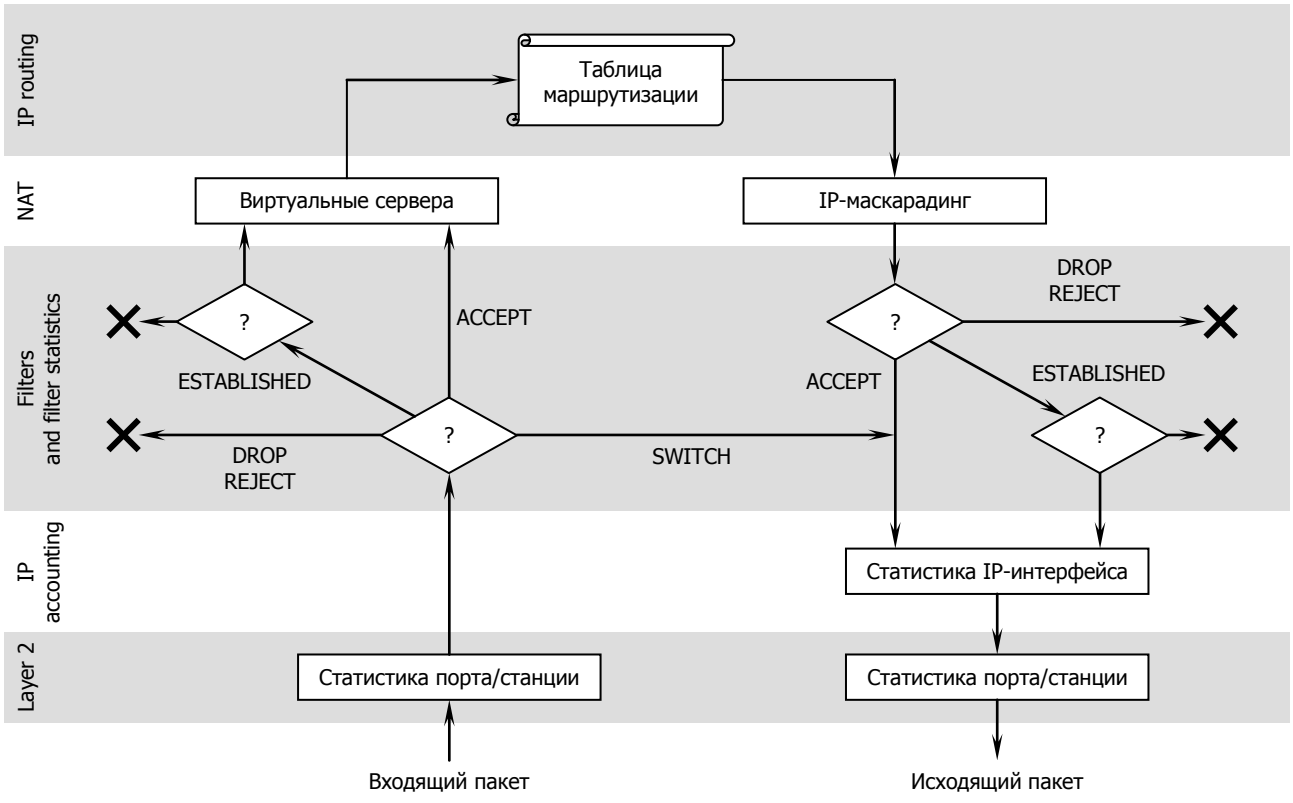
В данном примере все пакеты, приходящие с интерфейсов номер 1, 2, 4, 5, 6, 7 и 10, отправляются через третий интерфейс на адрес 10.0.0.10. Далее все пакеты, приходящие из сети 192.92.92.0, кроме тех, которые идут от узла 192.92.92.1 (PR:1), уничтожаются (PR:2). Последний фильтр запрещает любую передачу TCP-пакетов с портами назначения 2000 и выше на интерфейс номер 8.

## §4.5.4. Взаимосвязь маршрутизации, фильтрации, NAT и статистики

Фильтрация пакетов применяется раньше, чем IP-маршрутизация. Если помимо этого используется NAT, то механизм IP-маскарадинга воздействует на пакеты после IP-маршрутизации, но до выходного фильтра, а механизм вирутальных серверов — после входных фильтров, до IP-маршрутизации. В частности, фильтры типа SWITCH могут быть использованы для того, чтобы обойти как записи маршрутной таблицы, так и правила NAT.

Если при этом на выходном интерфейсе включен сбор IP-статистики, то он работает после маршрутизации, NAT и фильтров. Таким образом, он учитывает только исходящие IP-пакеты. (Подробнее об IP-статистике см. §4.6.) Помимо этого, фильтры (как на входе, так и на выходе) собирают собственную статистику, а на втором уровне собирается статистика портов и станций.

Последовательность прохождения пакета через различные службы IP-маршрутизатора показана на рисунке. (Несколько условно, так как входной и выходной фильтры, в общем случае, представляют собой единое целое.)



### §4.5.5. Маршрутизация в NULL и борьба с зацикливанием пакетов

Частным случаем применения запрещающих фильтров является уничтожение пакетов, которые не могут быть переданы далее из-за неготовности требуемого маршрута. (В оборудовании других производителей эта задача решается с помощью формального интерфейса NULL, однако разработчики NSG в данном случае следовали философскому принципу "не плодить сущностей сверх необходимого", поскольку механизм фильтров предоставляет для этого достаточные средства.)

В качестве примера рассмотрим сервер доступа NSG–800/16A со следующей конфигурацией интерфейсов:

```
S P IP:1 TY:ETHI ET:0 IADR:123.45.67.89 MASK:255.255.255.0
S P IP:3 TY:PPP PO:3 PAPR:1
.....
S P IP:18 TY:PPP PO:18 PAPR:1
S P AU:1 TY:TACACS+
S I DEFAULT IP:1 GW:123.45.67.90
```

IP-адреса пользователей назначаются сервером аутентификации из некоторого пула (например, с 123.45.68.0 по 123.45.68.15) и действительны только в течение сеанса. Когда удаленный пользователь завершает сеанс PPP, маршрут у нему удаляется из таблицы маршрутизации. При этом, если сеанс завершен некорректно (например, по причине обрыва модемного соединения) и в адрес данного пользователя продолжают поступать пакеты, то устройство будет, не найдя нужной записи в таблице маршрутизации, отправлять их на шлюз по умолчанию, т.е. возвращать вышестоящему шлюзу 123.45.67.90. В результате пакеты зацикливаются между двумя устройствами и передаются туда-обратно до обнуления параметра TTL.

Чтобы избежать этого, следует запретить отправку пакетов, адресованных пользователям, обратно в магистральный интерфейс с помощью следующего фильтра:

```
S I FILTER PR:0 TY:R DA:123.45.68.0/255.255.255.240 OUT:1
```

либо, что еще нагляднее:

```
S I FILTER PR:0 TY:R IN:1 OUT:1
```

Фильтр типа Reject в данном случае уместнее, чем Drop, поскольку уведомляет источник пакетов, что данный адресат более недоступен. В этом случае удаленный хост, как правило, должен прекратить посылку последующих пакетов. (В иных ситуациях, наоборот, может быть предпочтительно молчаливое уничтожение пакетов.)

### §4.5.6. Фильтрация пакетов с локальным адресом

Все пакеты, адресованные прикладным службам и подсистемам устройства NSG, принимаются и отправляются через локальный псевдоинтерфейс IP:0. Для этого, в частности, в таблице маршрутизации автоматически создаются записи, маршрутизирующие все пакеты, в которых в качестве адреса назначения указан адрес какого-либо из IP-интерфейсов устройства, на IP:0.

Таким образом, чтобы разрешить или запретить трафик, адресованный непосредственно устройству NSG или генерируемый им, следует создать соответствующий фильтр со значением IN:0 или OUT:0, соответственно. Например, следующий фильтр:

```
S I FILTER PR:0 TY:D PT:TCP DP:23 OUT:0
```

запрещает обращение к устройству по Telnet откуда бы то ни было, по любому из назначенных ему IP-адресов.

### §4.5.7. Статистика фильтрации

Для учета работы фильтров необходимо сначала включить учет параметром FACCT (Filter Accounting) в командах настройки IP-маршрутизатора и установить максимальное количество записей в таблице учета фильтров.

```
S P IP:0 FACCT:<число> Включить учет IP-фильтров и установить размер таблицы
S P IP:0 FACCT:NO      Выключить учет IP-фильтров
```

Изменения вступают в силу немедленно (рестарт маршрутизатора не требуется). После этого можно включать и выключать учет каждого фильтра в отдельности при помощи параметра ACCT (Accounting) для данного фильтра:

```
ACCT:YES   Включить учет для данного фильтра.
ACCT:NO    Выключить учет для данного фильтра.
```

Фильтр идентифицируется по номеру записи (PR) или имени (NAME), установленным командами S I FILTER, X I FILTER. В частности, если вместо имени фильтра использовать шаблон, то можно одной командой включать/выключать учет для группы фильтров. Пример:

```
X I FILTER NAME:Blacklist_* ACCT:YES
```

Если учет включен (ACCT:YES), то дополнительно можно детализировать статистику по учитываемым IP-адресам источника и назначения при помощи параметров SAM (Source Aggregate Mask) и DAM (Destination Aggregate Mask). При срабатывании фильтра маска накладывается на адрес источника или назначения, соответственно, и все срабатывания с одинаковым результатом суммируются в одной записи. Таким образом, пространства адресов, определенные параметрами SA и DA, разбиваются на более мелкие части. Если параметры SAM и DAM не заданы, то по умолчанию все срабатывания фильтра суммируются и выводятся в одной строке; если они равны 255.255.255.255, то учет ведется раздельно по каждому адресу.

Как можно видеть, максимальное число записей в таблице учета, занимаемых одним фильтром, равно 2 в степени

<число двоичных единиц в маске SAM/DAM> — <число двоичных единиц в маске SA/DA>

**Пример.** Если имеется набор фильтров с именами Porno1, Porno2 и т.п., запрещающих доступ к известным сайтам известного содержания, то команда

```
S I FILTER NAME:Porno* ACCT:YES SA:10.10.0.0/255.255.0.0 SAM:255.255.255.0
```

блокирует обращения к любым из этих сайтов со всех хостов корпоративной сети с адресами 10.10.x.x и ведет статистику отдельно по каждой подсети вида 10.10.0.x, 10.10.1.x, 10.10.2.x и т.д.

Для просмотра полученной статистики по всем или по некоторому одному фильтру используется команда Display IP следующего формата:

```
D I FILTER ACCT
D I FILTER ACCT:<номер_фильтра>
```

Дополнительно в этих командах можно указать период обновления статистики параметром UP:<секунды>.

Для других операций с таблицей статистики фильтров используются команды:

| | |
|---|---|
| C I FILTER ACCT | Зафиксировать накопленную статистику во вспомогательной таблице и обнулить текущие значения. |
| C I FILTER ACCT CHECKPOINT | Обнулить зафиксированную ранее таблицу статистики. |
| D I FILTER ACCT CHECKPOINT | Вывести зафиксированную ранее таблицу статистики по всем фильтрам. |
| D I FILTER ACCT:<номер> CHECKPOINT | Вывести зафиксированную ранее статистику по заданному фильтру. |

## §4.5.8. Фильтры как средство сбора расширенной статистики

Помимо своего основного назначения — ограничения распространения пакетов — фильтры могут использоваться для сбора статистики IP-трафика по расширенному набору критериев, включая входной и выходной интерфейсы, адреса и порты источника и назначения и т.п. Таким образом, они дополняют базовые возможности учета трафика, предоставляемые командой S I IPACCT (см.§4.6).

Для учета некоторой специфической категории трафика достаточно определить фильтр типа Accept с соответствующим набором критериев, например:

```
S I FILTER PR:3 TY:A DP:119
```

Все указанные пакеты (в данном случае — обращения к хостам NNTP) будут пропускаться, но при этом учитываться. Дальнейший анализ статистики фильтра позволит определить более точно, кто из локальных пользователей любит читать новости и с каких серверов.

Аналогичным образом можно использовать статистику запрещающих фильтров, например:

```
S I FILTER PR:4 TY:D DA:123.145.167.189 DP:23
```

Данный фильтр не только запрещает попытки обращения к указанному хосту по Telnet, но и фиксирует их в своей статистике, что позволяет определить потенциального злоумышленника.

# §4.6. Мониторинг IP-трафика

## §4.6.1. Процедура подсчета статистики по IP-адресам

Для учета исходящего трафика по IP-адресам необходимо сначала включить учет параметром ACCT (Accounting) в командах настройки IP-маршрутизатора и установить максимальное количество записей в таблице учета.

```
S P IP:0 ACCT:<число>   Включить учет по IP-адресам и установить размер таблицы.
S P IP:0 ACCT:NO        Выключить учет по IP-адресам.
```

Изменения вступают в силу немедленно (рестарт маршрутизатора не требуется). После этого можно включать и выключать учет по отдельным подсетям при помощи команды Set IP:

```
S I IPACCT IADR:<ip-адрес/маска> AM:<агрегат.маска> UM:<агрегат.маска> IP:<список_интерфейсов>
```

Обязательный параметр IADR содержит IP-адрес и маску в десятичной дотовой нотации. Наложение маски на адрес дает адрес учитываемой подсети, т.е. если две команды с разными IP-адресами после наложения маски дают одинаковый результат, то считается, что обе они относятся к одному счетчику. Если маска не задана, то по умолчанию принимается маска, соответствующая классу сети. Чтобы задать учет только по единственному IP-адресу, следует указать маску 255.255.255.255. Если адрес не задан, то по умолчанию полагается IADR:ALL, т.е. учет ведется по всем адресам.

**ПРИМЕЧАНИЕ** Поле IP-адреса в параметре IADR должно содержать именно адрес сети, т.е. все биты, выходящие за пределы маски, должны быть равны нулю. Например, IADR:10.0.0.0/255.0.0.0 — правильная запись, а IADR:10.1.2.3/255.0.0.0 — неправильная.

Параметры AM (Aggregate Mask) и UM (Undefined Addresses Aggregate Mask) позволяют обобщать статистику по группам адресов. При срабатывании счетчика по IP-адресу источника либо назначения, указанному в заголовке пакета, маска AM накладывается на этот адрес. Если для другого адреса также имеется подходящий счетчик, то на него накладывается маска AM, указанная в этом счетчике; если такого счетчика не найдено, то на второй адрес накладывается маска UM. Все срабатывания с одинаковым результатом суммируются в одной записи.

Последний параметр IP задает список IP-интерфейсов, на которых следует учитывать пакеты. Список может содержать один номер интерфейса, диапазон номеров (через дефис), или несколько номеров и диапазонов, разделенных запятыми.

По умолчанию AM:255.255.255.255, UM:0.0.0.0 и IP:ALL, т.е. учет ведется по всем IP-интерфейсам и по каждому адресу из сети, определенной параметром IADR, выводится информация о трафике:

— С данного IP-адреса на каждый из адресов, заданных остальными счетчиками.
— С данного IP-адреса на все остальные адреса.
— На данный IP-адрес с каждого из адресов, заданных остальными счетчиками.
— На данный IP-адрес со всех остальных адресов.

При этом пакеты, адресованные в данную сеть, учитываются только на интерфейсе, через который проходит маршрут в эту сеть, а пакеты, посылаемые из данной сети — на остальных интерфейсах.

Пример:

```
S I IPACCT IADR:192.168.0.0/255.255.0.0 AM:255.255.255.0 UM:255.0.0.0 IP:1,2,4–6,8–10
```

Учитываются пакеты, посылаемые через IP-интерфейсы 1, 2, 4, 5, 6, 8, 9 и 10 в сети с адресами 192.168.x.x и из этих сетей. Данные о трафике между этими сетями выводятся отдельно по каждой паре подсетей вида 192.168.0.x, 192.168.1.x, 192.168.2.x и т.д. Данные о трафике между ними и всем остальным миром выводятся отдельно по каждой паре подсетей вида 192.168.0.x, 192.168.1.x, … и 1.x.x.x, 2.x.x.x, …

**ПРИМЕЧАНИЕ** В статистике по IP-адресам учитываются только реально отправленные исходящие пакеты. Пакеты, блокированные фильтрами, сброшенные из-за переполнения выходной очереди и т.п., не учитываются.
Если на интерфейсе включен NAT (IP-маскарадинг), то в статистике отражаются только внешние адреса, т.е. те, с которыми пакеты были переданы следующему узлу.

Просмотреть список счетчиков и удалить конкретный счетчик трафика можно при помощи команд Display IP и Clear IP следующего формата:

```
D I IPACCT
C I IPACCT IADR:<ip-адрес/маска>
```

## §4.6.2. Статистика по IP-адресам

Для просмотра полученной статистики по всем или по некоторому одному IP-интерфейсу используется команда Display IP следующего формата:

```
D I ACCT
D I ACCT:<номер_интерфейса>
```

Дополнительно в этих командах можно указать период обновления статистики параметром UP:<секунды>.

Для других операций со статистикой IP-трафика используются команды:

| | |
|---|---|
| C I ACCT | Зафиксировать накопленную статистику во вспомогательной таблице и обнулить текущие значения. |
| C I ACCT CHECKPOINT | Обнулить зафиксированную ранее таблицу статистики. |
| D I ACCT CHECKPOINT | Вывести зафиксированную ранее таблицу статистики по всем интерфейсам. |
| D I ACCT:<номер> CHECKPOINT | Вывести зафиксированную ранее статистику по заданному интерфейсу. |

Пример списка фильтров и статистики:

```
Manager: D I IPACCT

IADR:10.0.0.0        /255.0.0.0         AM:255.0.0.0         UM:0.0.0.0  IP:1,2
IADR:194.67.234.64 /255.255.255.224 AM:255.255.255.224 UM:0.0.0.0  IP:1,2
IADR:ALL                                AM:255.255.255.255 UM:0.0.0.0  IP:2
```

```
Manager: D I ACCT:A

     Source          Destination        Packets          Bytes    Interface
10.0.0.0         10.0.0.0              169              5602            1
0.0.0.0          10.0.0.0            97823         104496806            1
194.67.234.64    194.67.161.1           44              1816            2
194.67.234.64    194.67.160.3          181              7394            2
194.67.224.230   192.118.82.140          6               216            2
194.67.224.230   194.67.111.89          18               648            2
194.67.234.64    195.2.72.152          821             32589            2
194.67.224.230   194.67.110.93           5               180            2
194.67.234.64    195.2.72.153         1843             54720            2
194.67.234.64    212.219.56.162        787             18492            2
194.67.234.64    194.67.137.187       1132            148001            2
194.67.234.64    63.246.130.50         785             42907            2
194.67.234.64    66.187.233.205         48              1398            2
194.67.234.64    195.161.119.244       306             16340            2
194.67.234.64    195.161.119.246       271             23817            2
194.67.234.64    195.161.119.249       127             10142            2
```

## §4.6.3. Статистика по IP-интерфейсам

Для просмотра статистики обмена пакетами по IP-интерфейсам используется команда Display Statistics/Status в следующем формате:

```
D S IP:<номер>
```

Формат и содержимое статистики зависят от типа интерфейса. Дополнительно может быть указан необязательный параметр UP:<интервал> — период обновления статистики (в секундах). По умолчанию его значение равно 0 — обновление не производится.

Для сброса статистики IP-интерфейса используется команда Clear Statistics:

```
C S IP:<номер>
```

### §4.6.4. Просмотр состояния TCP-соединений

Для просмотра статуса TCP-соединений используется команда Display Status в следующем формате:

| | |
|---|---|
| D S TCB:A | Вывести статус всех установленных TCP-соединений. |
| D S TCB:<номер> | Вывести подробную информацию о заданном соединении. Номер требуемого соединения можно узнать с помощью предыдущей команды. |

Данная команда выводит информацию управляющих блоков TCP (TCP Control Block, TCB) для всех TCP-соединений, имеющихся в устройстве на данный момент.

Пример (информация обо всех соединениях):

```
Manager: D S XOT:0

TCB 0: type is SERVER, state is LISTEN
Local port: 23

TCB 1: type is SERVER, state is LISTEN
Local port: 1998

TCB 2: type is SERVER, state is LISTEN
Local port: 80

TCB 3: type is CONNECTION, state is ESTABLISHED
Local host: 10.0.6.30, Local port: 23
Remote host: 10.0.0.6, Remote port: 34484
```

Пример (информация о заданном соединени):

```
Manager: D S TCB:3

TCB 3: type is CONNECTION, state is ESTABLISHED
Local host: 10.0.6.30, Local port: 23
Remote host: 10.0.0.6, Remote port: 34484
iss: 769318912 snduna: 769337889 sndnxt: 769337891 sndwnd: 17280
irs: 1989637931 rcvnxt: 1989638803 rcvwnd: 4096
Datagrams(rmss: 1460 smss: 1440):
Rcvd: 740, with data: 394, total data bytes: 871
Sent: 735(retransmit: 0), with data: 342, total data bytes: 18978
```

# §4.7. Дополнительные службы для локальных сетей

## §4.7.1. Статический ARP

Для обмена IP-пакетами в локальной сети (Ethernet или иного типа) используется протокол ARP (Address Resolution Protocol). Протокол динамически формирует таблицу соответствия между IP- и MAC-адресами устройств данной сети. Эта процедура выполняется автоматически и не требует вмешательства администратора.

Наряду с динамическим ARP, устройства NSG поддерживают статическую таблицу ARP, которая формируется администратором. Для создания записи в таблице ARP используется команда Set IP следующего вида:

```
S I ARP:<номер_интерфейса> IADR:<ip-адрес> ADDR:<мас-адрес>
```

где ARP:<номер> Номер IP-интерфейса маршрутизатора, к которому относится данная запись
IADR:<ip-адрес> IP-адрес некоторого устройства в сети, подключенной к этому интерфейсу
ADDR:<мас-адрес> MAC-адрес требуемого устройства.

Для просмотра статической и текущей таблиц ARP для некоторого IP-интерфейса используются команды Display IP следующего вида:

```
D I STATIC ARP:<номер_интерфейса>
D I ARP:<номер_интерфейса>
```

Для удаления записей (как статических, так и динамических) из таблицы ARP используется команда Clear IP:

```
C I ARP:<номер_интерфейса> IADR:<ip-адрес>
```

Статические записи ARP выполняют в устройствах NSG двоякую роль:

— Если на некотором IP-устройстве в сети Ethernet служба ARP не поддерживается или отключена по какой-либо причине, администратор сети может указать его MAC-адрес вручную (*Static ARP*).

— Статические записи в таблице ARP имеют приоритет над динамическими (*Strict ARP*). Если для некоторого IP-адреса задан статический MAC-адрес, устройство NSG будет посылать пакеты только по этому адресу. В тех случаях, когда в сети используются службы аутентификации, биллинга и т.п., основанные на IP-адресах, такая административная привязка IP-адресов к физическим адресам портов Ethernet позволяет повысить их надежность и достоверность.

**ПРИМЕЧАНИЕ** Strict ARP не запрещает удаленному устройству, MAC-адрес которого не соответствует заданному IP-адресу, посылать пакеты в сеть. Ограничение состоит лишь в том, что пакеты, поступающие на данный IP-адрес, будут отправляться исключительно на MAC-адрес, заданный в таблице ARP; таким образом, устройство с неправильным MAC-адресом не сможет получить никаких ответов на свои запросы.
Механизм ARP обеспечивает поиск MAC-адреса по известному IP-адресу, но не в обратную сторону. Если устройство с MAC-адресом, содержащимся в статической таблице ARP, начнет работать под другим IP-адресом, то разрешение адресов быдет выполняться обычным образом, т.е. с помощью динамического ARP.

## §4.7.2. ARP-прокси

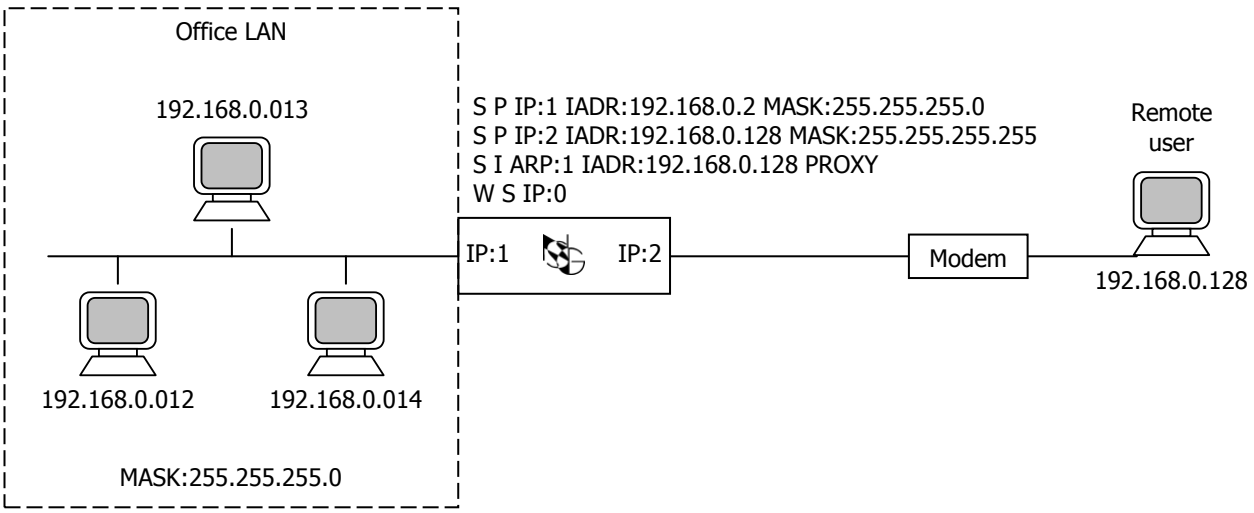
IP-интерфейсы маршрутизатора поддерживают режим ARP-прокси, т.е. могут отвечать на запросы ARP с указанными IP-адресами, посылая в ответ собственный MAC-адрес. Таким образом, они получают возможность принимать пакеты, адресованные некоторым хостам вне локальной сети, и далее пересылать эти пакеты в соответствии с установленной таблицей маршрутизации. Пример подключения удаленного клиента показан на рисунке на следующей странице. Чтобы ПК из локальной сети могли обращаться к этому удаленному хосту (и наоборот), нет необходимости настраивать маршрутизацию и шлюз по умолчанию на каждом из них; вместо этого поиск требуемых узлов выполняется автоматически клиентами ARP.

Для включения и выключения режима прокси с заданным IP-адресом используются команды Set IP и Clear IP, соответственно:

```
S I ARP:<номер_интерфейса> IADR:<ip-адрес> PROXY
C I ARP:<номер_интерфейса> IADR:<ip-адрес>
```

Информация о прокси-сервисах интерфейса, наряду с другими записями таблицы ARP, выводится командами Display IP:

```
D I STATIC ARP:<номер_интерфейса>
D I ARP:<номер_интерфейса>
```




**ПРИМЕЧАНИЕ** Для соединения "точка-точка" с удаленным пользователем в данном примере использован ненумерованный (*unnumbered*) интерфейс IP:2. IP-адрес 192.168.0.128 назначен удаленному пользователю статически.

**ПРИМЕЧАНИЕ** Служба ARP обрабатывает только одноадресные (*unicast*) пакеты. Для работы приложений, использующих широковещательную рассылку (*broadcast*) — например, для сетевого клиента, который таким образом производит обзор локальной сети — следует дополнить вышеприведенный пример фильтрами типа Switch для коммутации широковещательных пакетов между интерфейсами (см. §4.5):

```
S I FILTER TY:S EN:YES IN:1 DA:192.168.0.255 OUT:2
S I FILTER TY:S EN:YES IN:2 DA:192.168.0.255 OUT:1
S I FILTER TY:S EN:YES IN:1 DA:255.255.255.255 OUT:2
S I FILTER TY:S EN:YES IN:2 DA:255.255.255.255 OUT:1
```

Если удаленный клиент должен обращаться к хостам, расположенным за пределами локальной сети, то необходимо определить также шлюз по умолчанию (см. §4.3.2) и DNS (см. §4.3.5, либо статически на самом клиенте). Данные параметры настраиваются так же, как и на компьютерах локальной сети.

### §4.7.3. Ретранслятор BOOTP/DHCP

Механизм BOOTP обеспечивает удаленную загрузку сетевых устройств (в первую очередь, бездисковых рабочих станций) по локальной сети Ethernet с централизованного сервера. Частным случаем применения BOOPT является получение клиентом IP-адреса при помощи протокола DHCP. Ретранслятор запросов и ответов BOOTP/DHCP обеспечивает работу этих протоколов в случае, когда сервер расположен вне локальной сети, в которой находится клиент.

Ретранслятор BOOTP (BOOTP-relay) настраивается индивидуально для каждого IP-интерфейса. Для его работы необходимо указать адрес сервера BOOTP при помощи параметра HADR (Helper Address):

```
S I HADR:<ip-address> IP:<ip-interface>
```

Для выключения службы BOOTP-relay используется команда Clear IP:

```
C I HADR IP:<ip-interface>
```

Механизм BOOTP-relay работает следующим образом:

1. BOOTP-клиент посылает широковещательный запрос в виде UDP-пакета на порт 67 (BOOTP-сервер).
2. BOOTP-relay (маршрутизатор NSG), получив такой пакет, определяет, задан ли на интерфейсе, с которого пришел этот пакет, параметр HADR. Если да, то BOOTP-relay прописывает в поле giaddr запроса IP-адрес данного интерфейса, а качестве IP-адреса назначения подставляет значение параметра HADR. И отправляет пакет дальше в соответствии с таблицей маршрутизации.
3. BOOTP-сервер, находящийся по адресу, заданному параметром HADR, получает пакет и отправляет ответ на порт 67 (BOOTP-сервер) по адресу, записанному в поле giaddr, т.е. ретранслятору BOOTP.

4. BOOTP-relay (маршрутизатор NSG), получив ответ от сервера, выполняет одно из двух действий:

   — Подставляет IP-адрес BOOTP-клиента и отправляет ответ на MAC-адрес BOOTP-клиента. Оба адреса содержатся в самом ответе.

   — Если установлен флаг широковещательной рассылки (*broadcast flag*) или дальнейшая передача не требует MAC-адреса, отправляет ответ по широковещательному адресу.

   Ответ отправляется на порт 68 (BOOTP-клиент).

Аналогичным образом происходит обращение к серверу DHCP. При этом сервер получает информацию о сети, из которой пришел запрос (по адресу, указанному в поле giaddr), и, соответственно, может назначить клиенту адрес из диапазона, выделенного специально для этой сети.

Просмотреть адрес сервера BOOTP, назначенный интерфейсу, можно при помощи команды Display Parameters:

```
D P IP:<номер>
```

### §4.6.4. Статистика Ethernet-станций

Для просмотра статистики работы Ethernet-станций используется команда Display Statistics/Status в следующем формате:

```
D S ET:<номер>
```

Дополнительно может быть указан необязательный параметр UP:<интервал> — период обновления статистики (в секундах). По умолчанию его значение равно 0 — обновление не производится.

Для сброса статистики Ethernet-станции используется команда Clear Statistics:

```
C S ET:<номер>
```