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

## (Базовое программное обеспечение)

## Руководство пользователя

## Часть 8
## Аутентификация, авторизация и статистика

Версия программного обеспечения 8.2.4

Обновлено 05.12.2014

Москва 2014

# 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:



Восьмая часть руководства посвящена службам аутентификации, авторизации и учета работы пользователей. Эти службы относятся как к сетям IP, так и к сетям X.25, а их реализация в устройствах NSG тесно связана для обоих случаев и имеет ряд общих элементов для обоих типов сетей. По этой причине данный круг вопросов вынесен в отдельную часть, дополняющую части 4 и 7, соответственно.

Вопросы учета потребления услуг, специфические для сетей X.25, рассмотрены в части 7 руководства.

**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 8. Аутентификация, авторизация и статистика

# §8.1. Способы аутентификации и авторизации

## §8.1.1. Область применения подсистем AAA устройств NSG

Система аутентификации, авторизации и учета работы пользователей (Authentication, Autorization & Accounting, AAA) предназначена для решения триединой задачи управления пользовательскими сеансами, а именно:

— Аутентификации пользователя, пытающегося получить доступ к сетевым ресурсам (*authentication*).
— Определения набора сетевых ресурсов и сервисов, доступных данному пользователю (*authorization*).
— Учета потребляемых пользователем ресурсов и сервисов (*accounting*).

Аутентификация и авторизация пользователей могут проводиться в следующих ситуациях:

— При обращении удаленного клиента PPP к асинхронному порту устройства.
— При обращении удаленного клиента PAD к асинхронному порту устройства.
— При обращении удаленного клиента PPP к IP-интерфейсу типа PPP, независимо от используемого транспорта (синхронный порт, асинхронный порт, X.25, PPPoE).
— При подключении самого устройства NSG в качестве клиента PPP к удаленному серверу PPP, требующему аутентификации с использованием PAP/CHAP.
— При подключении самого устройства NSG в качестве клиента PPP к удаленному серверу PPP, требующему аутентификации с передачей имени и пароля в текстовом режиме.

Данные задачи могут решаться устройствами NSG как автономно, так и во взаимодействии с внешними серверами RADIUS и TACACS+. В первых двух случаях имя и пароль пользователя передаются открытым текстом, в третьем и четвертом — с помощью протоколов PAP или CHAP. В последнем случае задача решается с помощью механизма сценариев (*scripts*) для интерфейса PPP, подробно рассмотренного в Части 4.

Биллинговая подсистема устройств NSG предназначена только для учета потребления услуг в сети X.25. В сетях IP учет работы пользователей, как правило, не входит в число задач, возлагаемых на маршрутизаторы. Для этой цели используются выделенные сервера RADIUS/TACACS+, что связано как с большим объемом биллинговой информации, так и с необходимостью централизованного доступа к ней.

## §8.1.2. Таблица способов аутентификации

Для аутентификации и авторизации пользователей любым из вышеперечисленных методов требуется, как правило, целый набор параметров — например, IP-адрес сервера RADIUS, ключ для входа на сервер, адреса и ключи для запасных серверов, максимальное время ожидания ответа от сервера и т.п. Совокупность всех таких параметров определяет *способ аутентификации* как некоторый цельный объект, к которому может быть привязан асинхронный порт или интерфейс PPP. Для настройки этого объекта используется команда Set Parameters в следующем формате:

```
S P AU:<номер> ...
```

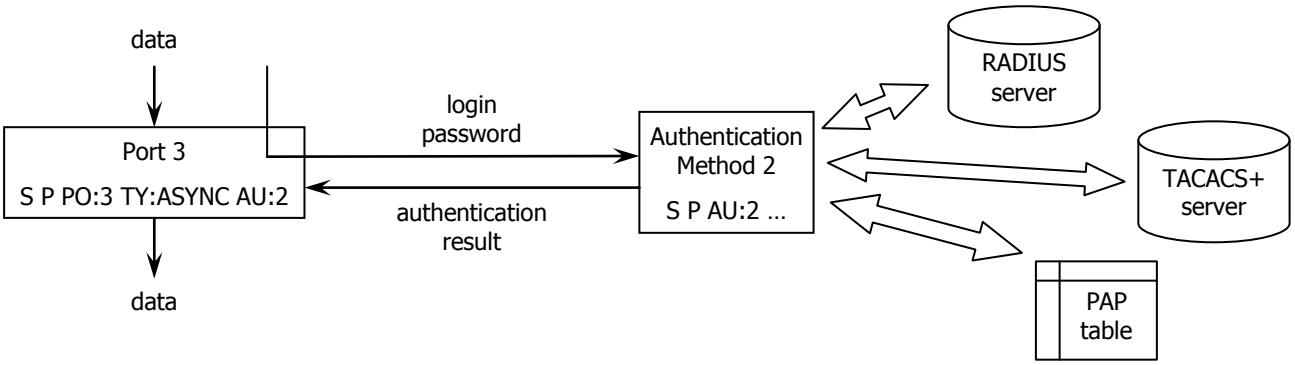
Всего в устройстве определены 4 способа аутентификации, пронумерованные от 1 до 4. Параметры каждого способа аутентификации зависят от его типа и рассмотрены в следующих четырех параграфах. Если некоторый способ не используется, для него следует установить тип NO_AUTH (аналогично NOCONF для портов и станций). Для просмотра параметров некоторого способа аутентификации или всех способов используется команда Display Parameters:

```
D P AU:<номер>
D P AU:A
```

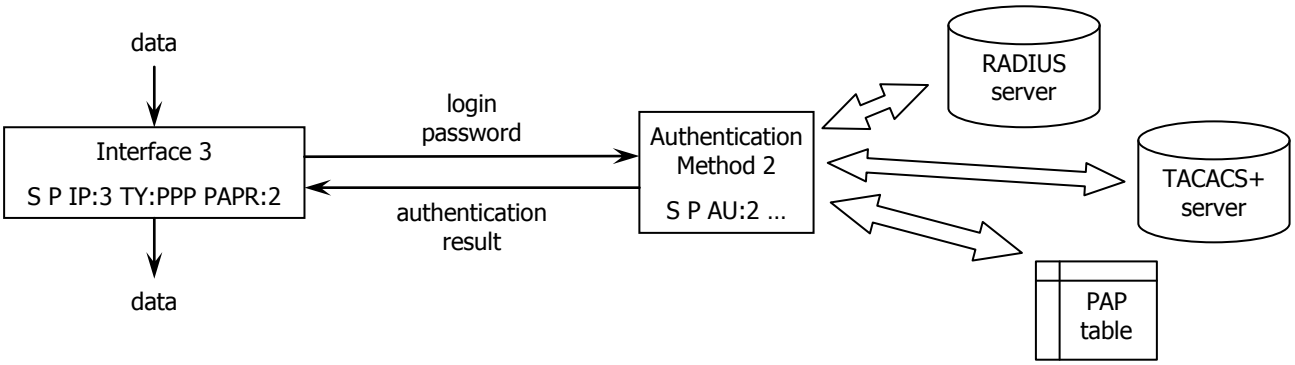
Когда для некоторого объекта (порта, интерфейса) требуется аутентификация, в его параметрах указывается номер используемого способа. Специальный номер 0 означает отсутствие аутентификации.

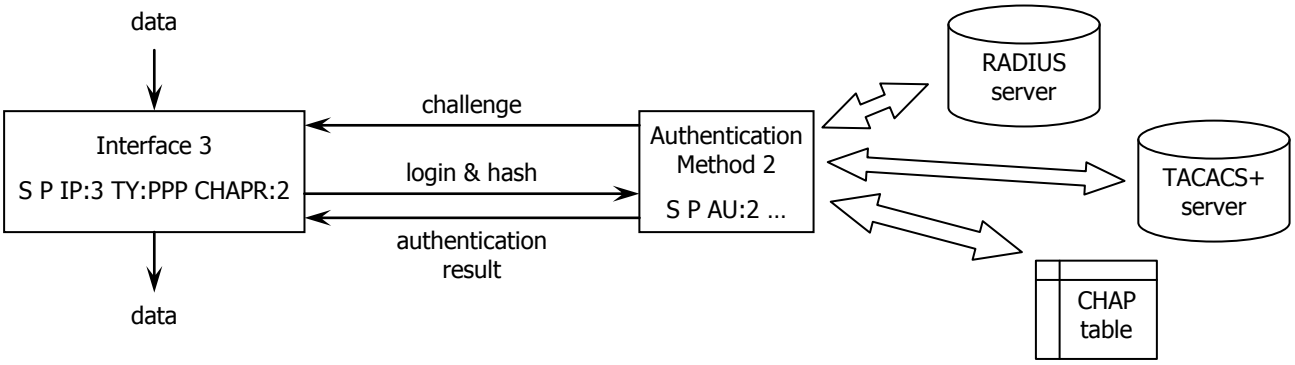
В устройстве могут быть определены однотипные, но различные способы аутентификации. Кроме того, способы аутентификации назначаются портам и интерфейсам индивидуально, в том числе допускается использовать различные способы для однородных объектов. Например, для разных интерфейсов PPP одни и те же серверы RADIUS/TACACS+ могут быть указаны в разной последовательности, чтобы сбалансировать нагрузку на них. Примеры конфигурации приведены в следующих главах данной части.

**ВНИМАНИЕ** Изменения в настройке способа аутентификации вступают с силу со следующего сеанса, для которого предписана аутентификация по данному способу. Текущие сеансы работы пользователей, для начала которых была использована аутентификация по этому способу, не разрываются.




Взаимодействие средств аутентификации для асинхронного порта




Аутентификация для интерфейса PPP с использованием PAP и CHAP

## §8.1.3. Способ аутентификации LOCAL

При локальной аутентификации поиск имени и пароля пользователя производятся в таблице PAP. (Таким образом, область применения этой таблицы шире, чем подразумевает ее устоявшееся название.) Каждая запись таблицы содержит имя клиента, имя сервера и пароль. Формат таблицы и алгоритм работы с ней подробно описаны в §8.2.

Чтобы определить способ аутентификации с использованием локальной таблицы пользователей, используется команда Set Parameters со следующими параметрами:

```
S P AU:<номер> TY:LOCAL NAME:<имя>
```

Параметр NAME определяет фиктивное имя сервера для аутентификации (текстовая строка длиной до 79 символов). Это имя используется в качестве имени сервера при поиске в таблице PAP. С его помощью можно устанавливать разные правила аутентификации для различных портов, например, определить для каждого порта свой список пользователей. (Пример см. в §8.3.3.)

При открытии сеанса PPP анализируется параметр AT (Activity Timer) используемого IP-интерфейса. С его помощью можно принудительно ограничить максимальную продолжительность сеанса (в секундах). AT:0 означает, что продолжительность сеанса не ограничена.

### §8.1.4. Способ аутентификации RADIUS

Данный способ предполагает использование протокола RADIUS (Remote Authentication Dial-In User Service, RFC–2138). В маршрутизаторе реализован клиент RADIUS, который направляет запросы в удаленный сервер RADIUS. Сервер выполняет аутентификацию пользователя и возвращает ответ с результатом, списком сервисов, доступных данному пользователю, и другими параметрами, определяющими сеанс его работы. Во время работы пользователя и при завершении сеанса клиент RADIUS передает серверу учетную информацию о сеансе (RFC–2139). Описание данного способа аутентификации выглядит следующим образом:

```
S P AU:<номер> TY:RADIUS ...
```

Для идентификации самого устройства NSG на сервере RADIUS используются три параметра:

IADR:<ip-адрес> IP-адрес данного устройства NSG, выступающего в роли сервера доступа (в терминах протокола RADIUS — NAS-IP-Address).

NAME:<имя> Символическое имя данного устройства (в терминах протокола RADIUS — имя Network Access Server, NAS). Максимальная длина — 79 символов. Если имя не задано, то по умолчанию будет использоваться административное имя устройства, установленное параметром HNAM (см. Часть 2).

ID:<префикс> Префикс идентификатора сеанса. Сервер RADIUS генерирует идентификатор для каждого сеанса, добавляя к этому префиксу порядковый номер. Наличие префикса упрощает дальнейшую обработку статистики, накопленной на сервере. Максимальная длина префикса — 15 символов.

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

```
S P AU:3 TY:RADIUS NAME:"NSG–800/16A #9 @Gadukino access node" ID:nas_g9
```

Следующая группа параметров предназначена для описания основного и резервных серверов RADIUS.

SN:<число> Число серверов RADIUS (от 1 до 4), к которым данный клиент может посылать запросы.

SADR:<ip-адрес> IP-адрес основного сервера RADIUS. Адрес задается в десятичной дотовой нотации.

KEY:<ключ> Ключ, используемый для защиты паролей пользователей при передаче их серверу RADIUS. Ключ должен совпадать с соответствующим ключом, хранящимся в базе данных сервера. Значение параметра задается в виде символьной строки. Если ключ содержит разделители (пробел : ; = ,) или вопросительный знак, его необходимо заключить в кавычки. Подробно о формате текстовых параметров см. Часть 9.

SADR1, SADR2 ...
KEY1, KEY2 ... IP-адреса и ключи резервных серверов RADIUS. Число пар параметров SADRn и KEYn определяется параметром SN. Если основной сервер, заданный параметром SADR, не отвечает, то запрос на аутентификацию посылается серверу SADR1, затем SADR2 и т.д. до конца списка. Критерии для перехода к следующему серверу устанавливаются параметрами TO и RT (см. ниже).

**ПРИМЕЧАНИЕ** Если сервер присылает ответ с флагом Authentication-Failure, то также производится попытка аутентификации на резервных серверах. Такая процедура обеспечивает работу системы в случае, если список пользователей рассредоточен по разным серверам и ни на одном из них не является полным.

PA:<порт> Номер порта UDP сервера, на который посылаются запросы аутентификации.

PB:<порт> Номер порта UDP сервера, на который посылается учетная информация.

Другая группа параметров данного метода регламентирует взаимодействие с сервером RADIUS.

TO:<секунды> Время ожидания ответа от сервера RADIUS. Если за указанное время ответ не получен, посылается повторный запрос.

RT:<число> Максимальное количество запросов к одному серверу. Если после данного числа запросов ответ от сервера так и не получен, считается, что сервер не доступен, и клиент RADIUS пытается аутентифицироваться на следующем сервере.

TA:<минуты> Периодичность посылки учетной информации на сервер. При TA:0 учетная информация посылается только в начале и в конце сеанса.

A44 Управление атрибутом 44 (Acct-Session-Id) в пакете Access-Request:

A44:YES Acct-Session-Id будет содержаться в пакете Access-Request.
A44:NO Acct-Session-Id не будет содержаться в пакете Access-Request.

В любом случае этот атрибут всегда присутствует в пакете Accounting-Request.

**ПРИМЕЧАНИЕ** Сбор учетной информации может производиться не только для интерфейса типа PPP, но и для IP-интерфейсов любого другого типа. Для этого в их конфигурации необходимо определить параметр ACCT, указывающий на способ аутентификации типа RADIUS.
Чтобы разрешить отсылку статистики для физического порта, необходимо указать в его конфигурации ACCT:YES. Статистика будет отсылаться в соответствии с выбранным способом аутентификации.
Для IP-интерфейса типа PPP рекомендуется устанавливать ACCT:0. При аутентификации пользователя на данном интерфейсе статистика всегда отсылается самим интерфейсом в соответствии с выбранным способом аутентификации (PAPR:n и/или CHAPR:n), при аутентификации на физическом порту — может отсылаться этим портом (AU:n ACCT:YES). Таким образом, параметр ACCT является в определенной степени излишним, поскольку дублирует отсылку статистики. Использовать его для интерфейсов PPP рекомендуется только на выделенных линиях, не использующих никакой аутентификации.

Последний параметр FTM (Filter Template Mode) устанавливает режим обработки атрибута Filter-Id:

FTM:NO — Атрибут Filter-Id используется "как есть", т.е. если он содержит точное имя фильтра (без звездочек), то включается только один фильтр с данным именем.

FTM:YES — К полученному имени фильтра добавляется звездочка, превращающая его в маску имен. Например, если в ответе сервера содержится Filter-ID=guest, то будут включены все динамические фильтры, подпадающие под маску guest*.

В пакете Access-Request серверу передаются следующие атрибуты:

| | |
|---|---|
| User-Name | Имя пользователя |
| User-Password либо CHAP-Password<br>CHAP-Challenge | Пароль пользователя |
| NAS-IP-Address | Значение параметра IADR в описании данного способа. Если этот параметр не задан, то используется IP-адрес интерфейса, через который отправляется запрос RADIUS. |
| NAS-Port | Номер порта устройства NSG |
| Service-Type=Framed-User<br>Framed-Protocol=PPP | Посылается по умолчанию, в ответ сервер может прислать эти же или другие значения. |
| NAS-Identifier | Значение параметра NAME в описании данного способа. |
| Calling-Station-Id | Дополнительная информация, переданная модемом после ключевого слова NMBR. Как правило, это номер телефона абонента, определенный АОН. |
| Connect-Info | Дополнительная информация, переданная модемом после ключевого слова CONNECT. |
| Acct-Session-Id | В зависимости от значения параметра A44 |

**ПРИМЕЧАНИЕ** Атрибуты Calling-Station-Id и Connect-Info отправляются только при аутентификации на PPP-интерфейсе. Чтобы данная информация была воспринята клиентом RADIUS, работа сценария должна быть завершена до получения сообщений CONNECT xxx и NMBR xxx, например:

```
S P IP:<номер> TY:PPP SCRIPT:1 SL:YES
A X SCRIPT:1 "" AT OK ATZ OK "ATS1=0" OK
```

В противном случае эта информация будет утеряна в ходе исполнения сценария, до старта клиента RADIUS. Пример неправильного (для данной задачи) сценария:

```
A X SCRIPT:1 "" AT OK ATZ OK "ATS1=0" CONNECT
```

Во всех пакетах Accounting-Request серверу передаются следующие атрибуты:

| | | |
|---|---|---|
| User-Name | | |
| NAS-IP-Address | | |
| NAS-Port | | |
| Service-Type=Framed-User | либо | Service-Type=Login-User |
| Framed-Protocol=PPP | | Login-Service=Rlogin |
| Framed-IP-Address | | |
| NAS-Identifier | | |
| Acct-Status-Type | | |
| Acct-Session-Id | | |
| Acct-Authentic | | |

В пакетах Accounting-Request, кроме стартового, передаются также следующие атрибуты:

Acct-Delay-Time
Acct-Input-Octets
Acct-Output-Octets
Acct-Session-Time
Acct-Input-Packets
Acct-Output-Packets

### §8.1.5. Способ аутентификации TACACS+

Данный способ предполагает использование протокола TACACS+. В маршрутизаторе реализован клиент TACACS+, который направляет запросы в удаленный сервер TACACS+. Сервер выполняет аутентификацию пользователя и возвращает ответ с результатом, списком сервисов, доступных данному пользователю, и другими параметрами, определяющими сеанс его работы. Во время работы пользователя и при завершении сеанса клиент TACACS+ передает серверу учетную информацию о сеансе. Описание данного способа аутентификации выглядит следующим образом:

```
S P AU:<номер> TY:TACACS+ ...
```

Для идентификации самого устройства NSG на сервере TACACS+ используются два параметра:

IADR:<ip-адрес> — IP-адрес клиента TACACS+ (в десятичной дотовой нотации). Этот адрес используется как адрес источника (source address) в IP-пакетах, посылаемых клиентом TACACS+, и должен быть известен и доступен серверу TACACS+. Если параметр не задан (по умолчанию IADR:0.0.0.0), то в качестве адреса источника используется IP-адрес интерфейса, через который устанавливается соединение с сервером.

ID:<префикс> — Префикс идентификатора сеанса. Сервер TACACS+ генерирует идентификатор для каждого сеанса, добавляя к этому префиксу порядковый номер. Наличие префикса упрощает дальнейшую обработку статистики, накопленной на сервере. Максимальная длина префикса — 15 символов. Подробно о формате текстовых параметров см. Часть 9.

Следующая группа параметров предназначена для описания основного и резервных серверов TACACS+.

SN:<число> — Число серверов TACACS+ (от 1 до 4), к которым данный клиент может посылать запросы.

SADR:<ip-адрес> — IP-адрес основного сервера TACACS+. Адрес задается в десятичной дотовой нотации.

KEY:<ключ> — Ключ, используемый для защиты тела пакетов TACACS+ при передаче их серверу. Ключ должен совпадать с соответствующим ключом, хранящимся в базе данных сервера. Значение параметра задается в виде символьной строки. Если ключ содержит разделители (пробел : ; = ,) или вопросительный знак, его необходимо заключить в кавычки. Подробно о формате текстовых параметров см. Часть 9.

SADR1, SADR2 ... KEY1, KEY2 ... — IP-адреса и ключи резервных серверов TACACS+. Число пар параметров SADRn и KEYn определяется параметром SN. Если основной сервер, заданный параметром SADR, не отвечает, то запрос на аутентификацию посылается серверу SADR1, затем SADR2 и т.д. до конца списка. Критерии для перехода к следующему серверу устанавливаются параметрами TO и RT (см. ниже).

**ПРИМЕЧАНИЕ** Если сервер присылает ответ с флагом Authentication-Failure, то также производится попытка аутентификации на резервных серверах. Такая процедура обеспечивает работу системы в случае, если список пользователей рассредоточен по разным серверам и ни на одном из них не является полным.

Другая группа параметров данного метода определяет взаимодействие с сервером TACACS+.

TO:<секунды> — Время ожидания ответа от сервера TACACS+. Если за указанное время ответ не получен, посылается повторный запрос.

RT:<число> — Максимальное количество запросов к одному серверу. Если после данного числа запросов ответ от сервера так и не получен, считается, что сервер не доступен, и клиент TACACS+ пытается аутентифицироваться на следующем сервере.

TA:<минуты> — Периодичность посылки учетной информации на сервер. При TA:0 учетная информация посылается только в начале и в конце сеанса.

Последний параметр FTM (Filter Template Mode) устанавливает режим обработки параметров inacl и outacl:

FTM:NO — Атрибут используется "как есть", т.е. если он содержит точное имя фильтра (без звездочек), то включается только один фильтр с данным именем.

FTM:YES — К полученному имени фильтра добавляется звездочка, превращающая его в маску имен. Например, если в ответе сервера содержится inacl=103, то будут включены все динамические фильтры, подпадающие под маску 103*.

### §8.1.6. Способ аутентификации NO_AUTH

Тип аутентификации NO_AUTH запрещает подключение пользователей. Через порт или интерфейс, для которого назначен такой способ аутентификации, ни один пользователь не сможет войти в систему. Дополнительных параметров нет. Пример:

```
S P AU:4 TY:NO_AUTH
```

## §8.2. Таблицы аутентификации PAP и CHAP

Если для интерфейса типа PPP используется локальная аутентификация на основе протоколов PAP или CHAP, то имена и пароли для нее хранятся в таблицах PAP и CHAP, соответственно. Эти таблицы используются для аутентификации как удаленных клиентов PPP в данной системе, так и самого устройства NSG на удаленной системе (сервере). Кроме того, в таблице PAP хранятся имена и пароли пользователей для локальной аутентификации при входе через асинхронный порт.

Записи в обеих таблицах имеют одинаковый формат:

<клиент> <сервер> <пароль> <ip-адреса>

Имена и пароли могут вводиться в кавычках или без них. Вместо имени клиента и/или имени сервера может стоять звездочка (*), означающая любое имя; в этом случае для аутентификации выбирается строка с наименьшим количеством звездочек. Сами понятия "клиент" и "сервер" интерпретируются различным образом, в зависимости от того, для какой цели используется аутентификация:

| Ситуация | Поле "клиент" | Поле "сервер" |
|---|---|---|
| Вход удаленного клиента через асинхронный порт | Имя пользователя, полученное в ответ на login: | Имя способа аутентификации (S P AU:n TY:LOCAL NAME:<имя>) |
| Подключение удаленного клиента к интерфейсу PPP | Имя пользователя, полученное в PAP/CHAP Response | Имя интерфейса (S P IP:n TY:PPP NAME:<имя>) |
| Подключение интерфейса PPP к удаленному серверу с аутентификацией PAP | Имя интерфейса (S P IP:n TY:PPP NAME:<имя>) | Имя удаленной системы для данного интерфейса (S P IP:n TY:PPP RNAME:<имя>) |
| Подключение интерфейса PPP к удаленному серверу с аутентификацией CHAP | Имя интерфейса (S P IP:n TY:PPP NAME:<имя>) | Имя сервера, полученное в сообщении CHAP Challenge |

**ВНИМАНИЕ** Пароли хранятся в таблицах в открытом виде и могут быть просмотрены командами D X.

**ВНИМАНИЕ** Большие и маленькие буквы в записях обеих таблиц различаются.

Список IP-адресов содержит адреса, с которых разрешается работать данному удаленному клиенту PPP. Адреса вводятся в десятичной дотовой нотации и разделяются пробелами. Если для клиента указан один или несколько адресов, то он не может работать ни с каких других адресов. Если список адресов пуст, то клиент может работать с любого IP-адреса. Чтобы запретить подключение клиента с любых адресов, следует указать на месте этого списка знак "–". (Это может иметь смысл, например, для временной блокировки клиента, для записи, предназначенной исключительно для аутентификации самого устройства NSG на удаленном сервере, или для порта, предназначенного исключительно для работы в качестве PAD — но с аутентификацией.)

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

```
A X PAP:<номер> <запись>
R X PAP:<номер>
D X PAP
```

```
A X CHAP:<номер> <запись>
R X CHAP:<номер>
D X CHAP
```

где <запись> имеет формат, приведенный выше. Если команда A X содержит номер существующей записи, то эта запись изменяется на новую. Если номер превосходит номер последней существующей строки более чем на единицу, то создаваемая запись получит следующий порядковый номер. При удалении записи в середине таблицы все последующие записи сохраняют свои номера, т.е. в таблице допускаются пропущенные номера.

Используются также следующие общие команды:

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

# §8.3. Подключение пользователей через асинхронный порт или Telnet

## §8.3.1. Режимы работы асинхронного порта и Telnet-станции

Физический порт типа ASYNC может использоваться двумя различными способами:

— В прозрачном режиме — для передачи асинхронного потока данных без инкапсуляции. Такой порт может быть скоммутирован (посредством PVC) с другим объектом типа ASYNC — портом, станцией Frame Relay или станцией Telnet. Примеры использования прозрачного режима приведены в Части 6.

— В протокольном режиме — PAD либо PPP. После подключения пользователя к порту (поднятия сигнала DCD) будет запрашиваться имя и пароль пользователя. В случае успешной аутентификации данный порт будет сконфигурирован, в зависимости от ее результатов, либо по типу PPP (и связан с IP-интерфейсом маршрутизатора), либо по типу PAD. После этого по данной асинхронной линии начнется сеанс PPP либо PAD, соответственно.

Этими же возможностями обладает Telnet-станция типа ASYNC, за одним исключением. После аутентификации и авторизации пользователя станция может динамически принимать только тип PAD. Если в результате авторизации делается попытка назначить данной станции тип PPP, пользователю будет выведено сообщение об ошибке.

Выбор режима осуществляется при помощи параметра AU (Authentication):

| | |
|---|---|
| AU:0 | Аутентификация не используется, порт/станция работает в прозрачном режиме. Поскольку в этом режиме отсутствуют сами понятия пользователя и сеанса, то никакая аутентификация невозможна. |
| AU:<номер> | Используется аутентификация по методу с указанным номером. Всего в устройстве может быть определено до четырех методов аутентификации с номерами от 1 до 4. После успешной аутентификации порт начинает работать в соответствующем протокольном режиме. |

## §8.3.2. Использование асинхронного порта в протокольном режиме

Протокольный режим работы асинхронного порта (или Telnet-станции типа ASYNC) означает, что после аутентификации каждого подключившегося пользователя и в результате его авторизации порт динамически переходит из прозрачного текстового режима в режим PAD либо PPP. Чтобы осуществить эту процедуру, параметр AU должен указывать на один из способов аутентификации 1...4, настроенный соответствующим образом. После разрыва соединения порт снова принимает тип ASYNC.

Аутентификация и авторизация пользователя может производиться локально с помощью таблицы паролей PAP, хранящейся в самом устройстве NSG, либо удаленно с помощью централизованного сервера RADIUS или TACACS+. Во всех случаях процедура аутентификации, с точки зрения пользователя, выглядит одинаково:

— Порт выводит строку login: , предлагая пользователю ввести имя.
— Пользователь вводит свое имя (идентификатор) и завершает ввод нажатием клавиши Enter.
— Порт выводит строку Password: , предлагая пользователю ввести свой пароль.
— Пользователь вводит пароль (на экране не отображается) и завершает ввод нажатием клавиши Enter.

Имя и пароль могут вводиться как вручную, так и с помощью некоторого сценария (скрипта), выполняемого на компьютере пользователя. При написании сценария следует учитывать, что приглашения login: и Password: заканчиваются пробелом после двоеточия — это может быть существенно для отдельных клиентских систем.

Получив имя и пароль пользователя, система выполняет аутентификацию и авторизацию в соответствии с тем способом, на который указывает параметр AU данного порта. Пример согласованной настройки порта и способа аутентификации:

```
S P PO:18 AU:1
S P AU:1 TY:RADIUS …
```

Процедура аутентификации и авторизации для каждого из трех способов (LOCAL, RADIUS и TACACS+) и примеры ее применения подробно рассмотрены в следующих трех параграфах.

Аутентификация в прозрачном текстовом режиме возможна только для порта (или Telnet-станции), сконфигурированного как ASYNC. Если порту заранее назначен тип PAD, то в дальнейшем система может только проверять сетевой идентификатор пользователя (NUI) в команде установления соединения. Если порту заранее назначен тип ASYNC_PPP, то аутентификация может быть выполнена позже средствами IP-интерфейса типа PPP, т.е. при помощи протоколов PAP или CHAP.

**ПРИМЕЧАНИЕ** Аутентификация в прозрачном текстовом режиме при подключении к асинхронному порту ни в коей мере не связана с последующей аутентификацией PAP/CHAP при подключении к IP-интерфейсу типа PPP. Оба метода могут применяться совместно.

**ПРИМЕЧАНИЕ** Аутентификация самого устройства NSG на удаленном сервере PPP в прозрачном текстовом режиме осуществляется с помощью сценариев установки соединения, описанных в Части 4.

Текст приглашения для ввода имени может быть модифицирован администратором при помощи параметра PT (Prompt). Значением параметра является текстовая строка длиной не более 15 символов. Если строка содержит разделители (пробел : ; = ,) или вопросительный знак, ее необходимо заключить в кавычки. (Подробно о формате текстовых параметров см. Часть 9.) Пустая строка ("") или звездочка ("*") означает обычное приглашение "login: "

После успешной аутентификации и авторизации пользователя порт динамически конфигурируется для работы в режиме PPP или PAD, соответственно:

**а) Режим PPP**

Если в результате авторизации порт принимает тип ASYNC_PPP, то для дальнейшей работы необходим свободный IP-интерфейс типа PPP со значением PO:AUTO, либо со значением PO:, указывающим на данный порт. Список интерфейсов, к которым может подключаться данный порт, устанавливается параметром IP и может содержать отдельные номера или диапазоны номеров IP-интерфейсов (через запятую), например:

```
IP:1,3,6–10,12
```

Порт привязывается к первому свободному интерфейсу из указанных в списке. Если указано IP:ALL (по умолчанию), то порт может привязываться к любому свободному интерфейсу типа PPP. При отсутствии такого интерфейса пользователю выводится сообщение об ошибке.

Если предполагается одновременная работа нескольких пользователей, то в системе должно быть сконфигурировано столько же свободных IP-интерфейсов. Пример (для сервера удаленного доступа NSG–16A в сети поставщика услуг Интернет):

```
S P PO:3 TY:ASYNC IF:V24 SP:115200 AU:1 IP:1–16 PT:"Your Username: " ACCT:YES
.....
S P PO:18 TY:ASYNC IF:V24 SP:115200 AU:1 IP:1–16 PT:"Your Username: " ACCT:YES
S P IP:1 TY:PPP PO:AUTO …
.....
S P IP:16 TY:PPP PO:AUTO …
S P AU:1 TY:RADIUS …
```

Если указанный способ аутентификации предусматривает использование внешнего сервера RADIUS/TACACS+, то далее в ходе сеанса и после его завершения порт может отсылать или не отсылать серверу учетную информацию. Отправка статистики определяется параметром ACCT:

| | |
|---|---|
| ACCT:YES | Отсылать статистику |
| ACCT:NO | Не отсылать статистику (по умолчанию) |

**б) Режим PAD**

Если в результате авторизации порту назначается тип PAD, то для дальнейшей работы ему требуются все остальные параметры, присущие портам этого типа. (Подробно о конфигурации портов типа PAD см. Часть 7.) Чтобы получить доступ к этим параметрам, необходимо временно назначить данному порту тип PAD. После этого можно сконфигурировать их должным образом и вернуть порту тип ASYNC. Значения параметров, относящиеся к режиму PAD, не выводятся, но сохраняются в неизменном виде. Пример:

```
Manager: D P PO:3
PO:03 TY:ASYNC SP:9600 AU:1 ACCT:YES
Manager: S P PO:3 TY:PAD
PO:03 TY:PAD IF:V24 SP:9600 AF:8N1 CO:NO RP:NO AC:NO CM:NO
LG:128 MB:NO CD:YES BI:0 AD:NO PT:"*" MS:""
1:1 2:1 3:2 4:0 5:0 6:1 7:2 8:0 9:0 10:0 11:14 12:1 13:4 14:0 15:1 16:8 17:24 18:2 19:2
Manager: S P PO:3 PROF:2 AD:1234567890
PO:03 TY:PAD IF:V24 SP:9600 AF:8N1 CO:NO RP:NO AC:NO CM:NO
LG:128 MB:NO CD:YES BI:0 AD:1234567890 PT:"*" MS:""
1:0 2:0 3:0 4:1 5:0 6:1 7:8 8:0 9:0 10:0 11:14 12:0 13:0 14:0 15:0 16:0 17:0 18:0 19:0
Manager: S P PO:3 TY:ASYNC
PO:03 TY:ASYNC SP:9600 AU:1 ACCT:YES
Manager: W F
Manager: W S PO:3
```

В результате такой конфигурации порт снова выглядит как ASYNC, но готов к работе в режиме PAD с прозрачным профилем №2 и собственным адресом 1234567890. После подключения пользователя PAD будет работать с этими настройками.

**ПРИМЕЧАНИЕ** Начиная с версии 8.0.1b, параметры PAD для порта типа ASYNC включаются в сценарий конфигурации, генерируемый командой M S.

### §8.3.3. Локальная аутентификация

Для локальной аутентификации имена и пароли пользователей должны быть внесены администратором в таблицу PAP, хранящуюся в энергонезависимой памяти данного устройства NSG. Подробно о формате таблиц PAP/CHAP см. §8.2. Пример:

```
S P PO:1 TY:ASYNC AU:2
S P PO:2 TY:ASYNC AU:3
S P AU:2 TY:LOCAL NAME:PORT_1
S P AU:3 TY:LOCAL NAME:PORT_2
A X PAP:1 ivanov PORT_1 IvAn
A X PAP:2 petrov PORT_2 pETr
A X PAP:3 sidorov * sIdOr
W F
W S PO:1
```

В данном случае пользователь ivanov при подключении через порт №1 должен вводить пароль IvAn, пользователь petrov при входе через порт №2 вводит пароль pETr, а пользователь sidorov может входить через любой порт с паролем sIdOr.

Выбор сервиса PPP или PAD происходит на основе суффикса .ppp или .pad, вводимого после имени пользователя (аналогично формату имени при аутентификации на сервере TACACS+). Таким образом, авторизация при локальной аутентификации не производится — каждый пользователь, зарегистрированный в таблице PAP, может самостоятельно выбирать себе тот или иной сервис. Если, например, вышеупомянутый пользователь ivanov введет

```
login: ivanov.ppp
Password: ivan
```

то начнется сеанс PPP, а если он введет

```
login: ivanov.pad
Password: ivan
```

то начнется сеанс PAD. Если пользователь не ввел ни того, ни другого суффикса:

```
login: ivanov
Password: ivan
```

то по умолчанию также начнется сеанс PAD.

При открытии сеанса PPP анализируется параметр AT (Activity Timer) используемого IP-интерфейса. С его помощью можно принудительно ограничить максимальную продолжительность сеанса (в секундах). AT:0 означает, что продолжительность сеанса не ограничена.

### §8.3.4. Удаленная аутентификация и авторизация на сервере RADIUS

Если для порта (или Telnet-станции) выбран метод аутентификации RADIUS, то устройство запрашивает у пользователя имя и пароль и затем посылает их удаленному серверу RADIUS. Имя пользователя должно вводиться точно в том же виде, в котором оно храниться на сервере. В ответе сервера содержится разрешение/запрет на работу данного пользователя, а также ряд атрибутов данного сеанса (протокол, IP-адрес, максимальная продолжительность и т.п.). Если основной сервер не отвечает, запрос будет поочередно посылаться резервным серверам, перечисленным в параметрах данного способа аутентификации.

Для того, чтобы открыть сеанс PPP, сервер RADIUS должен прислать ответ с атрибутами:

```
Service-Type=Framed-User
Framed-Protocol=PPP
```

Для того, чтобы открыть сеанс PAD, ответ должен содержать атрибуты:

```
Service-Type=Login-User
Login-Service=Rlogin
```

При других значениях этих атрибутов никакой сеанс не начнется.

Если в ответе сервера содержится атрибут Reply-Message, то он выводится в терминальное окно клиента (в любом случае). При открытии сеанса PPP будут восприниматься также следующие атрибуты:

Framed-IP-Address
Framed-Compression
Idle-Timeout
Session-Timeout
Filter-Id

Атрибут Filter-Id позволяет включать фильтр или группу фильтров индивидуально для каждого пользователя. В качестве Filter-Id на сервере RADIUS должно быть указано имя фильтра, установленное параметром NAME в командах S I FILTER, X I FILTER. Вместо имени можно использовать шаблон, содержащий одну или несколько звездочек. Подробнее о динамическом создании фильтров см. §8.3.6.

При открытии сеанса PAD воспринимается только атрибут Session-Timeout. Остальные атрибуты игнорируются.

Пример:

```
S P AU:1 TY:RADIUS IADR:10.0.0.17 TO:10 RT:3 ID:"NX300_" SN:2
S P AU:1 SADR:10.0.0.10 KEY:"abcdef" SADR1:10.0.0.12 KEY1:"klmnop"
S P PO:4 TY:ASYNC SP:115200 AU:1
S P IP:3 PO:AUTO
```

## §8.3.5. Удаленная аутентификация и авторизация на сервере TACACS+

При аутентификации TACACS+ каждому пользователю может быть разрешен доступ к нескольким протокольным сервисам, поэтому имя пользователя должно вводиться с суффиксом .ppp или .pad в соответствии с требуемым сервисом:

| | |
|---|---|
| login: vpupkin.ppp | для входа в сеанс PPP |
| login: vpupkin.pad | для входа в сеанс PAD |

Если пользователь ввел только имя без суффикса, то по умолчанию предполагается PPP.

Устройство NSG посылает имя, пароль и запрашиваемый тип сеанса удаленному серверу TACACS+. Если этот протокол установлен для данного пользователя, от сервера приходит ответ с разрешением подключить пользователя и дополнительными параметрами (IP-адресом и т.п.). Если основной сервер не отвечает, запрос будет поочередно посылаться резервным серверам, перечисленным в параметрах данного способа аутентификации.

При открытии сеанса PPP будут вопрниматься следующие параметры TACACS+:

| | |
|---|---|
| addr | IP-адрес, принудительно назначаемый клиенту сервером TACACS+ |
| timeout | Максимальная продолжительность сеанса, в минутах |
| idletime | Максимальное время неактивности пользователя, в минутах |
| inacl, outacl | Включение динамических фильтров для данного сеанса (подробнее см. п.§8.3.6). Оба параметра обрабатываются одинаково. |

**Пример.** Пусть для пользователей nif-nif, nuf-nuf и naf-naf разрешены следующие сервисы:

| Пользователь | Пароль | Протоколы | Дополнительные параметры |
|---|---|---|---|
| nif-nif | straw | pad, ppp | 40.30.20.10 (IP-адрес для сеанса PPP) |
| nuf-nuf | wood | pad | — |
| naf-naf | brick | ppp | 40.30.20.11 (IP-адрес для сеанса PPP) |

Соответствующие фрагменты файла конфигурации для сервера TACACS+ выглядят следующим образом:

```
user = nif-nif {
    login = cleartext straw
    service = pad {}
    service = ppp protocol = ip {
        addr = 40.30.20.10
    }
}

user = nuf-nuf {
    login = cleartext wood
    service = pad {}
}

user = naf-naf {
    login = cleartext brick
    service = ppp protocol = ip {
        addr = 40.30.20.11
    }
}
```

### §8.3.6. Динамические фильтры. Гостевой вход.

Механизм динамически создаваемых фильтров позволяет индивидуально ограничить возможности конкретного пользователя. Наиболее частое применение таких фильтров — организация гостевого входа, при котором пользователю с традиционным именем guest разрешается доступ только к серверу регистрации, на котором он должен активировать карту предоплаты; доступ к другим ресурсам Интернет для него запрещен.

Для создания динамического фильтра в устройстве должен быть предварительно создан шаблон, отличающийся от реально действующего фильтра (см. Часть 4) тем, что параметр EN имеет одно из следующих значений:

| | |
|---|---|
| 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 RADIUS получен атрибут Filter-ID=guest, и в устройстве определен шаблон фильтра

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

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

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

После завершения сеанса данный фильтр удаляется автоматически.

Сервер RADIUS использует для включения фильтра атрибут Filter-Id. Сервер TACACS+ может использовать параметр inacl или outacl; в устройствах NSG оба эти параметра обрабатываются одинаково, для фильтрации по входному интерфейсу, по выходному интерфейсу или по обоим следует использовать значения EN:DI, DO и DIO, соответственно.

**ВНИМАНИЕ** Если получен один из вышеперечисленных атрибутов, но фильтр не может быть создан (нет такого шаблона, параметр EN не начинается с D, не хватает места в таблице фильтров), то пользователь не будет авторизован и соединение разорвется.

Во всех трех случаях указанные атрибуты могут содержать как точное имя фильтра, так и маску имен (с одним или несколькими подстановочными символами *). Если от сервера получено точное имя, то включается ровно один фильтр с указанным именем. Если получена маска, то включаются все фильтры, подпадающие под данную маску.

**ВНИМАНИЕ** Если в ответе сервера содержится несколько атрибутов Filter-Id или inacl, outacl, то обрабатывается только последний из них. Для включение нескольких фильтров одновременно следует назначить им однотипные имена и воспользоваться масками.

Кроме того, если сервер аутентификации настроен так, что присылает однозначное имя фильтра, то оно может быть преобразовано в маску при помощи параметра FTM (Filter Template Mode) в описании способа аутентификации:

| | |
|---|---|
| S P AU:n FTM:NO | Полученное от сервера значение используется "как есть", то будет включен только один фильтр |
| S P AU:n FTM:YES | К полученному имени прибавляется звездочка; например, если от сервера получен атрибут Filter-ID=guest, то будут включены все динамические фильтры с именами вида guest*. Это позволяет легко интегрировать устройства NSG в существующие системы, например, построенные на базе серверов доступа с Cisco-подобным командным языком. |

Пример конфигурации динамических фильтров:

```
S I FILTER PR:0 NAME:"guest-tcpdns" TY:A PT:TCP DP:53 EN:D
S I FILTER PR:1 NAME:"guest-udpdns" TY:A PT:UDP DP:53 EN:D
S I FILTER PR:2 NAME:"guest-regsrv" TY:A DA:123.134.156.99 EN:DI
S I FILTER PR:3 NAME:"guest-world" TY:R EN:DI
```

Если от сервера получено имя фильтра guest*, то на основе данного набора шаблонов будут созданы фильтры, разрешающие доступ к серверу регистрации и серверам DNS и запрещающие доступ ко всем остальным хостам. Первые два фильтра будут действовать на все IP-интерфейсы, третий и четвертый (запрещающий) — только на интерфейс, к которому подключен данный пользователь.

# §8.4. Подключение удаленного клиента PPP

## §8.4.1. Процедура аутентификации для интерфейса PPP (сервера)

IP-интерфейс типа PPP, работающий в качестве сервера, может аутентифицировать удаленных клиентов при помощи внешнего сервера RADIUS, TACACS+, либо локально — во многом аналогично асинхронному порту. Отличие состоит в том, что для передачи пароля между клиентом и сервером доступа PPP используется не прозрачный текстовый режим, а протоколы PAP (Password Authentication Protocol) и/или CHAP (Cryptographic Handshake Authentication Protocol). Оба эти протокола предусматривают аутентификацию пользователя по совокупности трех (вместо двух) параметров: имени пользователя, имени сервера и паролю.

Выбор протокола аутентификации для интерфейса PPP осуществляется параметрами PAPR (PAP Request) и CHAPR (CHAP Request). Использование этих параметров аналогично параметру AU для асинхронного порта: значения 1...4 устанавливают один из заданных способов аутентификации, 0 означает вход без аутентификации по данному протоколу.

Оба параметра PAPR и CHAPR могут иметь ненулевые значения одновременно. В этом случае сначала клиенту предлагается аутентификация по CHAP, а если он не соглашается — тогда по PAP. Если же обе стороны договорились использовать CHAP и попытка аутентификации оказалась неудачной, то на этом процедура завершается с отрицательным результатом.

Пример конфигурации:

```
S P IP:3 TY:PPP NAME:NX–300_pp3 PAPR:2 CHAPR:1
S P AU:1 TY:RADIUS SADR:123.234.156.231
S P AU:2 TY:LOCAL
```

В данном случае реквизиты пользователя проверяются либо по удаленному серверу RADIUS с использованием CHAP, либо по локальной таблице пользователей с использованием PAP, причем приоритетным является первый вариант.

Аутентификация удаленного клиента PPP при подключении к IP-интерфейсу типа PPP выполняется одинаково для всех вариантов используемого транспорта (синхронный порт, асинхронный порт, X.25, PPPoE).

**ПРИМЕЧАНИЕ** Аутентификация PAP/CHAP при подключении к IP-интерфейсу типа PPP ни в коей мере не связана с предварительной аутентификацией в прозрачном текстовом режиме при подключении к асинхронному порту. Оба метода могут применяться совместно.

Одновременно с аутентификацией может производиться проверка или назначение IP-адреса пользователя. При локальной аутентификации список адресов, с которых разрешено работать данному пользователю, хранится в таблицах PAP и CHAP. (Подробно о формате таблиц PAP/CHAP см. §8.2.) При аутентификации с помощью централизованного сервера адрес может содержаться в ответе сервера.

В этом случае, если пользователь имеет статический IP-адрес (который передается в сообщении PAP/CHAP Response), то этот адрес должен содержаться в списке; иначе результат аутентификации будет отрицательным. Если в качестве адреса пользователя указано 0.0.0.0, т.е. пользователь просит назначить ему динамический IP-адрес, то ему будет назначен первый адрес из списка (либо адрес, присланный сервером).

**ПРИМЕЧАНИЕ** Если результат аутентификации не содержит IP-адреса, а пользователю необходимо назначить динамический IP-адрес, то используется значение параметра RADR, установленное для данного IP-интерфейса. (Это значение является более общим, так как оно используется для всех таких пользователей.)

## §8.4.2. Локальная аутентификация PAP/CHAP

Для локальной аутентификации клиентов PPP с использованием PAP или CHAP IP-интерфейс устройства NSG должен быть настроен следующим образом, соответственно:

```
S P IP:<номер> TY:PPP NAME:<имя_интерфейса> PAPR:<номер_способа> ...
S P IP:<номер> TY:PPP NAME:<имя_интерфейса> CHAPR:<номер_способа > ...
```

где указанный способ предписывает локальную аутентификацию. Для успешной аутентификации пользователя необходимо найти в таблице PAP или CHAP, соответственно, запись, содержащую:

— В поле "клиент" — имя, введенное пользователем.
— В поле "сервер" — имя данного интерфейса или звездочку (означающую любое имя).
— В поле "пароль" — пароль, введенный пользователем.

Как можно видеть, существенную роль в данном случае играет имя интерфейса (параметр NAME). С его помощью можно разрешить определенным пользователям подключаться только через определенные интерфейсы PPP. Если имя интерфейса не назначено, вместо него используется административное имя устройства (S W HNAM:<имя>).

Пример:

```
S P IP:1  TY:PPP  NAME:"pp1"  CHAPR:1 …
S P IP:2  TY:PPP  NAME:"pp2"  CHAPR:1 …
S P AU:1  TY:LOCAL
A X CHAPR:123  ivan  pp1  PeTroV  192.168.3.1  192.168.3.2  192.168.3.3
A X CHAPR:124  petr  pp2  iVANov
A X CHAPR:125  vasya  *  pUpk1n
```

В данном случае пользователь ivan может подключаться только через интерфейс IP:1 и только с определенных адресов, пользователь petr — только через интерфейс IP:2, но с любого адреса, а пользователь vasya — через любой интерфейс.

### §8.4.3. Аутентификация с использованием серверов RADIUS/TACACS+

Если аутентификация осуществляется на централизованном сервере RADIUS или TACACS+, то интерфейс PPP устройства NSG получает от пользователя имя и пароль с использованием протокола PAP и/или CHAP и передает их серверу безопасным образом. Кроме того, передаются также атрибуты Calling-Station-Id и Connect-Info. Значениями этих атрибутов является текст, содержащийся в сообщениях модема NMBR и CONNECT, соответственно.

Если используется сервер RADIUS, то в случае успешной аутентификации его ответ должен содержать следующие атрибуты:

```
Service-Type=Framed-User
Framed-Protocol=PPP
```

В противном случае сеанс PPP не начнется. Помимо них воспринимаются также следующие атрибуты:

```
Framed-IP-Address
Framed-Compression
Idle-Timeout
Session-Timeout
Filter-Id
```

Атрибут Filter-Id позволяет включать фильтр или группу фильтров индивидуально для каждого пользователя. В качестве Filter-Id на сервере RADIUS должно быть указано имя фильтра, установленное параметром NAME в командах S I FILTER, X I FILTER. Вместо имени можно использовать шаблон, содержащий одну или несколько звездочек; правила работы с шаблоном такие же, как и в командах, относящихся к созданию/удалению/изменению фильтров.

Если в ответе, полученном от сервера RADIUS, содержится атрибут Filter-Id, то всем фильтрам с именами, соответствующими значению Filter-Id, устанавливается параметр EN:YES, и фильтры начинают действовать. При завершении сессии всем этим фильтрам устанавливается параметр EN:NO, и фильтры перестают действовать.

При использовании сервера TACACS+ ему передается, в дополнение к имени и паролю пользователя, тип запрашиваемого сервиса — PPP. Этот протокол должен быть указан в конфигурации данного пользователя на сервере. В противном случае ответ сервера будет отрицательным.

При успешной аутентификации в ответе сервера TACACS+ воспринимаются также следующие параметры:

```
addr
timeout
idletime
inacl, outacl  (оба параметра обрабатываются одинаково)
```

Атрибуты Filter-Id (RADIUS) и inacl, outacl (TACACS+) позволяют динамически создавать фильтры, относящиеся только к данному пользователю. После завершения сеанса эти фильтры удаляются. Подробно о динамических фильтрах см. п.§8.3.6.

Атрибуты Session-Timeout (RADIUS) и timeout (TACACS+) позволяют ограничить максимальную продолжительность сеанса PPP. Если эти параметы содержатся в ответе сервера, то они имеют приоритет над параметром AT (Activity Timer) IP-интерфейса.

Пример:

```
S P IP:2  TY:PPP  CHAPR:1
S P AU:1  TY:TACACS+  SADR:123.134.156.178 …
```

## §8.5. Подключение к удаленному серверу PPP

Если интерфейс PPP устройства NSG сам является клиентом и должен аутентифицироваться на удаленном сервере, для этого интерфейса необходимо указать PAPA:YES и/или CHAPA:YES, в зависимости от используемого протокола аутентификации. Имена серверов и соответствующие им пароли хранятся в тех же таблицах PAP и CHAP. Имя клиента задается параметром NAME данного интерфейса; при его отсутствии этого параметра используется административное имя устройства (S W HNAM:<имя>).

**а) Аутентификация устройства NSG на удаленном сервере PAP:**

IP-интерфейс устройства NSG настраивается следующим образом:

```
S P IP:<номер> TY:PPP NAME:<имя_интерфейса> RNAME:<имя_сервера> PAPA:YES ...
```

В таблице PAP ищется строка, у которой первое поле (имя клиента) совпадает со значением параметра NAME, а второе (имя сервера) — со значением RNAME. Пароль из этой строки посылается удаленной стороне.

**ПРИМЕЧАНИЕ** Имя RNAME в данном случае является фиктивным и используется только для поиска нужной строки в таблице PAP. Удаленная система использует для аутентификации клиента NSG свое собственное имя, которое может не совпадать с RNAME.

Пример:

```
S P IP:1 TY:PPP NAME:"Malye_Gryazischi" RNAME:"Bolshie_Gryazischi" PAPA:YES
A X PAP:98 Malye_Gryazischi Bolshie_Gryazischi qwerty
```

**б) Аутентификация устройства NSG на удаленном сервере CHAP:**

IP-интерфейс устройства NSG настраивается следующим образом::

```
S P IP:<номер> ADM:UP TY:PPP NAME:<имя_интерфейса> CHAPA:YES ...
```

Интерфейс получает от сервера сообщение CHAP (CHAP Challenge Message), содержащее имя сервера. В таблице CHAP ищется строка, у которой первое поле (имя клиента) совпадает со значением параметра NAME, а второе — с полученным именем сервера. Имя пользователя и хэш пароля из этой строки посылаются удаленной стороне в сообщении CHAP Response Message.

Пример:

```
S P IP:1 TY:PPP NAME:"d.Korovye_Vyazlo" CHAPA:YES
A X PAP:99 "d.Korovye_Vyazlo" GadukinoTelecom_LTD qwerty
```

## §8.6. Мониторинг и управление пользователями

Для просмотра списка пользователей, подключенных к устройству в данный момент, используется команда Display Statistics следующего вида:

```
D S SY:1
```

Таблица пользователей, выводимая по этой команде, содержит следующие поля:

| | |
|---|---|
| # | Номер сеанса. Целое число в диапазоне от 1 до максимального значения (MaxSessionNumber), определенного для данного типа устройства. |
| username | Имя пользователя, представленное в процессе аутентификации. Если пользователь подключился без аутентификации, то в поле имени выводится строка <UNKNOWN>. |
| session_id | Уникальный идентификатор сеанса. При удаленной аутентификации (через RADIUS/TACACS+) используется в качестве Acct-Session-Id. |
| service | Тип сервиса, предоставленного пользователю. Возможные значения: PPP, PAD, SLIP. |
| user_addr | IP-адрес, назначенный пользователю. Если IP-адрес неприменим для данного типа сервиса (PAD) или неизвестен системе AAA (SLIP), то значение этого поля равно 255.255.255.255. |
| resource | Название ресурса, занимаемого пользователем:<br>PO.<номер> физический порт<br>TN.<номер> Telnet-станция<br>IP.<номер> IP-интерфейс<br>Если пользователь занимает более одного ресурса (например, подключился к порту TY:ASYNC, после аутентификации получил сервис PPP и, таким образом, занял еще и IP-интерфейс), то в таблице будет указан только IP-интерфейс. |
| auth_server_addr | Адрес сервера RADIUS/TACACS+, выполнившего аутентификацию данного пользователя. Если пользователь аутентифицирован локально или подключен без аутентификации, то данное поле будет иметь значение 0.0.0.0. |

Пример:

```
Manager: D S SY:1
```

| # | username | sesion_id | service | user_addr | resource | auth_server_addr |
|---|---|---|---|---|---|---|
| 3 | igor | 1728053255 | PPP | 15.0.0.2 | IP.3 | 0.0.0.0 |
| 4 | mike | 1728053252 | PPP | 172.16.3.33 | IP.4 | 10.0.0.10 |
| 24 | <UNKNOWN> | 1728053248 | SLIP | 255.255.255.255 | PO.3 | 0.0.0.0 |
| 25 | <UNKNOWN> | 1728053249 | PAD | 255.255.255.255 | PO.4 | 0.0.0.0 |
| 26 | <UNKNOWN> | 1728053250 | PAD | 255.255.255.255 | TN.0 | 0.0.0.0 |
| 29 | tnmike | 1728053253 | PAD | 255.255.255.255 | TN.3 | 0.0.0.0 |

Для периодического обновления списка можно использовать параметр UP:<интервал> — период обновления, в секундах. Текущий список пользователей можно просмотреть также через Web-интерфейс или административное приложение на основе SNMP. (См. Часть 5.)

Для принудительного отключения пользователя следует выполнить рестарт порта, интерфейса или станции, к которым он подключен, командой Warm Start (W S ...) или иными средствами управления. Например, при исчерпании средств на лицевом счету пользователя (при повременной оплате услуг Интернет) система SNMP-управления может рестартовать интерфейс PPP по команде биллингового сервера.