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

(Базовое программное обеспечение)

Руководство пользователя

Приложение Б
Настройка сеансового доступа по протоколу PPP

Версия программного обеспечения 8.2.4

Обновлено 14.01.2011

Москва 2011

АННОТАЦИЯ

Данный документ является приложением к руководству 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.

Руководство состоит из следующих разделов:

В данном документе рассмотрены в комплексе все вопросы, относящиеся к организации сеансового доступа по протоколу PPP. Подробное описание команд, технологий и функциональных возможностей, используемых в этих задачах, содержится в частях 1–9 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 §

Приложение Б. Настройка сеансового доступа по протоколу PPP

Б.1. Последовательность настройки PPP-доступа

Протокол PPP — наиболее гибкий и многовариантный протокол канального уровня, используемый для передачи IP-трафика. Однако оборотной стороной этой гибкости является многоступенчатая процедура установления соединений и обилие параметров PPP, нередко вызывающие затруднения у пользователей и сетевых администраторов. Для успешной настройки протокола PPP следует последовательно отладить все этапы установления соединения:

Шаг 0: Постановка задачи. В первую очередь, сетевой администратор должен четко сформулировать параметры создаваемого соединения PPP: тип транспортной среды, используемые средства аутентификации и авторизации пользователей, распределение IP-адресов, методы сжатия IP-пакетов, а также взаимосвязь данного соединения с различными прикладными службами (например, клиентом сети Microsoft Windows).

Шаг 1: Настройка транспортной среды для протокола PPP. Такой средой для устройств NSG может быть физическое соединение по выделенной или коммутируемой линии (в т.ч. беспроводной), а также соединение "точка-точка" поверх сети Ethernet или логическое соединение по сети X.25. В результате выполнения данного этапа конфигурации обеспечивается передача данных между IP-интерфейсом устройства NSG и стеком TCP/IP удаленного устройства.
Кроме того, настройка физического уровня тесно связана с ролью, отведенной данному устройству в сетевом решении: клиент, сервер или то и другое попеременно.

После завершения этого шага IP-интерфейс и удаленное устройство приступают к согласованию параметров PPP-соединения на канальном уровне в рамках протокола LCP (Line Control Protocol). Процедура конфигурации разбивается далее на три четко определенные стадии, в соответствии с этапами выполнения протокола:

Шаг 2: Настройка аутентификации и авторизации. Аутентификация и авторизация пользователей в устройствах NSG может выполняться:
— в двух разных режимах (клиент и сервер доступа)
— с помощью трех протоколов (PAP, CHAP и/или терминальный режим)
— двумя различными объектами протокольной архитектуры NSG (асинхронный порт и IP-интерфейс типа PPP)
— по трем различным источникам (локальная таблица пользователей, внешние серверы RADIUS или TACACS+)
— а также завершаться тремя различными результатами: отказ в доступе, предоставление услуги PPP, либо предоставление услуги PAD (последняя, в свою очередь, может использоваться для автоматического или ручного проключения к серверам других услуг)
Применительно к рассматриваемой задаче, результатом данного этапа является успешная аутентификация пользователя и авторизация его для доступа к услуге PPP.

Шаг 3: Настройка параметров IP — а именно, протокола IPCP (IP Control Protocol). Данный протокол определяет процедуру согласования IP-адресов двух устройств (говоря более строго — двух IP-интерфейсов). Кроме адресов, PPP-сервер может передать клиенту дополнительную информацию, такую как адреса серверов DNS.
Результатом выполнения данного этапа является возможность обмена IP-пакетами между двумя программными процессами третьего уровня (уровня межсетевого взаимодействия): IP-маршрутизатором, работающим в устройстве NSG, и стеком TCP/IP удаленного устройства.

Шаг 4: Настройка параметров сжатия. Сжатие заголовков IP-пакетов и пользовательских данных согласовывается двумя сторонами при помощи протокола CCP (Compression Control Protocol). Использование сжатия не является обязательным, однако несогласованные настройки двух сторон могут существенно задержать установление соединения (до нескольких десятков секунд).

В заключение следует обратить внимание на службы и протоколы, работающие через установленное соединение IP-over-PPP:

Шаг 5: Настройка IP-маршрутизации. Маршрут к непосредственно подключенному интерфейсу PPP удаленной стороны создается автоматически. Однако если за удаленным устройством расположены еще какие-либо сети, маршруты к ним необходимо описать отдельно (явным образом или с помощью шлюза по умолчанию).

Шаг 6: Настройка прикладных служб. Данный этап актуален, в основном, для клиентов, использующих операционные системы Windows, в силу тесной взаимосвязи между их компонентами.

При настройке интерфейса PPP необходимо соблюдать следующие два правила:

— Настройка должна производиться согласованно на обеих сторонах соединения.

— Все вышеперечисленные шаги выполняются строго в указанной последовательности, поскольку каждый из них имеет смысл только при условии успешного выполнения предыдущих шагов. Даже если настройка интерфейса производится за один прием, сетевому администратору следует держать в уме вышеописанную последовательность и контролировать все настройки именно в таком порядке. Если параметры интерфейса заданы неверно и соединение не устанавливается, то для поиска ошибки следует последовательно проконтролировать этапы 1–4. Если соединение установлено, но сетевые службы и приложения не могут использовать его должным образом, ошибку следует искать на этапах 5 или 6.

Непосредственно настройка протокола PPP состоит в исполнении шагов 1–4. Элементы конфигурации, определяемые на каждом шаге, могут варьироваться в зависимости от требований конкретного сетевого решения. Основные примеры конфигурации для каждого шага приведены в разделах Б.2–Б.5 данного Приложения. Чтобы получить полную конфигурацию IP-интерфейса и связанных с ним объектов для большинства типовых задач, необходимо выбрать по одному варианту из разделов Б.2–Б.5 и объединить их.

Вопросы IP-маршрутизации непосредственно не относятся к настройке соединения PPP и поэтому не рассматриваются в данном документе. Отдельные аспекты, которые следует учитывать при настройке маршрутизатора, затронуты в разделе Б.4.

Особенности настройки клиентов на основе операционных систем Windows рассмотрены в разделе Б.8.

Особенности настройки PPP-соединений в сотовых сетях GSM/GPRS рассмотрены в разделе Б.9.

Б.2. Шаг 1 — настройка физического соединения или иного транспорта для PPP

При организации PPP-доступа с использованием модемных соединений возможны две существенно различные ситуации: работа под коммутируемой и по выделенной линии.

В рамках данного документа под работой по *коммутируемой* линии подразумевается режим, при котором модемы устанавливают физическое соединение по команде, полученной от устройств DTE, и сигнализируют об установлении соединения поднятием сигнала DCD и сообщением CONNECT. В этом режиме устройства NSG поддерживают только асинхронную передачу данных, причем возможны две существенно различные конфигурации физического уровня в зависимости от того, по какому протоколу производится аутентификация клиента.

Под работой по *выделенной* линии подразумевается режим, при котором физическое соединение устанавливается модемами автоматически по включению питания или поднятию сигнала DTR на обеих сторонах. С точки зрения устройств DTE, такое соединение эквивалентно прямому нуль-модемному соединению. В режиме выделенной линии возможна как асинхронная, так и синхронная передача данных.

Кроме модемного соединения, транспортом для протокола PPP могут служить соединение "точка-точка" поверх сети Ethernet или логическое соединение по сети X.25. В обоих этих случаях устройство NSG может использоваться только в качестве сервера; работа в режиме клиента не предусмотрена.

Б.2.1. Коммутируемая асинхронная линия, аутентификация в терминальном режиме

Сервер доступа. Для аутентификации пользователей в терминальном режиме порт сервера имеет тип ASYNC (подробно о настройке аутентификации см. раздел Б.3). В IP-маршрутизаторе должны быть созданы интерфейсы типа PPP с динамической привязкой к портам; при успешной аутентификации пользователя и его авторизации на услугу PPP порт принимает тип ASYNC_PPP и привязывается к первому свободному IP-интерфейсу. Максимальное число одновременно подключенных пользователей ограничено числом IP-интерфейсов с TY:PPP PO:AUTO. После установления физического соединения сервер не инициирует процедуру LCP, а только ожидает получения LCP-запросов от удаленной стороны. При длительном отсутствии активности соединение разрывается. Пример конфигурации:

```
S P PO:m TY:ASYNC AU:1 IF:V24 SP:115200
S P AU:1 …
S P IP:n TY:PPP PO:AUTO SL:YES KEEP:300
```

Для управления модемом в данном случае предусмотрен только сброс сигнала DTR на 2 сек. при разрыве соединения. Режим автоответа (S0=1) должен быть установлен в настройках самого модема — а именно, в профиле по умолчанию, устанавливаемом по команде ATZ и по включению питания. Если в программном обеспечении модема предусмотрена настройка, позволяющая повторно инициализировать его при падении сигнала DTR, рекомендуется использовать эту возможность. (Как правило, для этого используется команда AT&Dn со значениями n>2, специфичными для конкретных модемов.)

ПРИМЕЧАНИЕ Список IP-интерфейсов, доступных для подключения через данный порт, может быть дополнительно ограничен параметром IP: в настройках порта. В этом случае порт не сможет использовать остальные IP-интерфейсы с TY:PPP PO:AUTO, даже если они свободны.

Клиент. Порт имеет тип ASYNC_PPP и жестко привязан к IP-интерфейсу типа PPP. Соединение с сервером устанавливается по требованию, т.е. при наличии в IP-маршрутизаторе пакетов, которые должны быть переданы по данному соединению. Клиент использует сценарий соединения (скрипт), чтобы инициализировать модем и выдать ему команду на установление соединения. После этого он, в рамках того же сценария, переходит к процедуре аутентификации. После завершения работы сценария IP-интерфейс переходит к процедуре LCP и начинает посылать запросы серверу. При длительном отсутствии активности соединение разрывается. Пример конфигурации:

```
S P PO:x TY:ASYNC_PPP IF:V24 SP:115200
S P IP:y TY:PPP PO:x SL:NO DOD:YES DTR:{0|1} KEEP:300 SCRIPT:1
A X SCRIPT:1 "" AT OK ATZ OK ATD1234567 "login: " basile "password: " pOuPkiNe
```

Дополнительный параметр DTR позволяет управлять состоянием модема в то время, когда соединение отсутствует. (Запись вида DTR:{0|1} означает, что параметр может иметь любое из указанных значений.)

Двунаправленное соединение при терминальной аутентификации невозможно, поскольку настройки клиента и сервера, как можно видеть из вышеприведенных примеров, в данном случае оказываются несовместимыми.

Б.2.2. Коммутируемая асинхронная линия, аутентификация по PAP или CHAP

Сервер доступа. Для аутентификации пользователей по PAP или CHAP порт сервера имеет тип ASYNC_PPP (подробно о настройке аутентификации см. раздел Б.3) и жестко привязан к IP-интерфейсу типа PPP. После установления физического соединения сервер не инициирует процедуру LCP, а только ожидает получения LCP-запросов от удаленной стороны. При длительном отсутствии активности соединение разрывается. Пример конфигурации:

```
S P PO:m TY:ASYNC_PPP IF:V24 SP:115200
S P IP:n TY:PPP PO:m SL:YES KEEP:300 SCRIPT:1
A X SCRIPT:1 "" AT OK ATZ OK "ATS0=1" OK ""
```

Клиент. Порт имеет тип ASYNC_PPP и жестко привязан к IP-интерфейсу типа PPP. Соединение с сервером устанавливается по требованию, т.е. при наличии в IP-маршрутизаторе пакетов, которые должны быть переданы по данному соединению. Клиент использует сценарий соединения (скрипт), чтобы инициализировать модем и выдать ему команду на установление соединения. После того, как от модема получено сообщение CONNECT, выполнение сценария завершается и IP-интерфейс начинает посылать LCP-запросы серверу. При длительном отсутствии активности соединение разрывается. Пример конфигурации:

```
S P PO:x TY:ASYNC_PPP IF:V24 SP:115200
S P IP:y TY:PPP PO:x SL:NO DOD:YES DTR:{0|1} KEEP:300 SCRIPT:1
A X SCRIPT:1 "" AT OK ATZ OK ATD1234567 CONNECT ""
```

Дополнительный параметр DTR позволяет управлять состоянием модема в то время, когда соединение отсутствует. (Запись вида DTR:{0|1} означает, что параметр может иметь любое из указанных значений.)

Двунаправленное соединение. Такая конфигурация типична, например, для соединения между двумя офисами, которое может устанавливаться по требованию любой из сторон. При этом сценарий соединения реализует функции клиента, т.е. установление исходящего соединения. Для ответа на входящие соединения режим автоответа (S0=1) должен быть установлен в настройках самого модема — а именно, в профиле по умолчанию, устанавливаемом по команде ATZ и по включению питания. Сигнал DTR поднят постоянно и опускается только на 2 сек. после разрыва соединения.

```
S P PO:x TY:ASYNC_PPP IF:V24 SP:115200
S P IP:y TY:PPP PO:x SL:NO DOD:YES DTR:1 KEEP:300 SCRIPT:1
A X SCRIPT:1 "" AT OK ATZ OK ATD1234567 CONNECT ""
```

Если в программном обеспечении модема предусмотрена настройка, позволяющая повторно инициализировать его при падении сигнала DTR, рекомендуется использовать эту возможность. (Как правило, для этого используется команда AT&Dn со значениями n>2, специфичными для конкретных модемов.)

Б.2.3. Выделенная асинхронная линия и нуль-модемное соединение

При работе по выделенной линии, по самой постановке задачи, заранее известно устройство-клиент и требуемый ему тип сервиса — PPP. Поэтому аутентификация, если она вообще требуется, производится средствами IP-интерфейса, и настройки наиболее близки к случаю Б.2.2. Применительно к данной задаче, различие между клиентом и сервером состоит в том, что сервер и его модем постоянно включены и готовы к установлению соединений, а клиент и его модем могут включаться/выключаться пользователем в произвольное время.

Помимо модемного соединения, важным частным случаем выделенной линии являются системы передачи голоса и данных по одной медной паре, работающие в режиме "прозрачного удлинителя" асинхронного интерфейса RS–232 (например, на основе технологии ISDN), а также непосредственное соединение двух устройств нуль-модемным кабелем.

Сервер доступа. Порт сервера имеет тип ASYNC_PPP и жестко привязан к IP-интерфейсу типа PPP. После установления физического соединения (поднятия сигнала DCD) сервер, как правило, не инициирует процедуру LCP, а только ожидает получения LCP-запросов от удаленной стороны. При длительном отсутствии активности посылаются пакеты LCP Echo Request, чтобы проконтролировать целостность линии; если на них не получены ответы (LCP Echo Reply) 10 раз подряд, то соединение разрывается и сигнал DTR опускается на 2 сек, что заставляет модемы заново приступить к установлению физического соединения. Пример конфигурации:

```
S P PO:m TY:ASYNC_PPP IF:V24 SP:115200
S P IP:n TY:PPP PO:m SL:YES ECHO:30
```

ВНИМАНИЕ Важным исключением является подключение клиентского ПК под управлением ОС Windows с помощью нуль-модемного кабеля. В этом случае необходимо установить на устройстве NSG следующие значения параметров: SL:NO DOD:NO. Подробнее об этой задаче см. раздел Б.8.

Клиент. Порт имеет тип ASYNC_PPP и жестко привязан к IP-интерфейсу типа PPP. Сразу после включения или перезагрузки устройства IP-интерфейс начинает посылать LCP-запросы для установления соединения с сервером. Как и сервер, клиент использует механизм LCP Echo, чтобы при отсутствии полезного трафика периодически контролировать целостность линии. Пример конфигурации:

```
S P PO:x TY:ASYNC_PPP IF:V24 SP:115200
S P IP:y TY:PPP PO:x SL:NO DOD:NO ECHO:30
```

Двунаправленное соединение. Если последовательность включения устройств на двух сторонах соединения заранее не определена, т.е. каждое устройство может выступать и в роли клиента, и в роли сервера, то два устройства NSG могут быть настроены как клиенты, т.е. SL:NO DOD:NO. Однако такая настройка не идеальна, поскольку устройство, включенное первым, будет посылать по 10 LCP-запросов и после этого опускать сигнал DTR на 2 сек. для переустановления физического соединения; если в это время другая сторона попытается установить соединение, попытка будет неудачной. Поэтому для двунаправленного соединения с произвольным оборудованием на удаленной стороне рекомендуется использовать режим установления соединений по требованию (см. пример Б.2.2), с небольшой модификацией:

```
S P PO:x TY:ASYNC_PPP IF:V24 SP:115200
S P IP:y TY:PPP PO:x SL:NO DOD:YES DTR:1 KEEP:0 ECHO:30
```

С практической точки зрения, отличие такой конфигурации от постоянного соединения состоит только в том, что соединение устанавливается не сразу после включения устройств, а только тогда, когда на одной из сторон появляются данные, предназначенные для передачи другой стороне. После того, как соединение единожды установлено, оно может сохраняться в течение неопределенно долгого времени, поскольку разрыв по отсутствию активности запрещен (KEEP:0).

Б.2.4. Выделенная синхронная линия

Настройка PPP-доступа по выделенной синхронной линии в целом аналогична асинхронной линии. Отличия состоят в типе физического порта и соответствующем выборе физических интерфейсов. Примеры конфигурации:

Сервер доступа:

```
S P PO:m TY:SYNC_PPP IF:V35 MODE:EXT SP:2048000
S P IP:n TY:PPP PO:m SL:YES ECHO:30
```

Клиент:

```
S P PO:x TY:SYNC_PPP IF:V35 MODE:EXT SP:2048000
S P IP:y TY:PPP PO:x SL:NO DOD:NO ECHO:30
```

Двунаправленное соединение. Либо оба устройства настраиваются в режиме клиента, либо используется следующая конфигурация:

```
S P PO:x TY:SYNC_PPP IF:V35 MODE:EXT SP:2048000
S P IP:y TY:PPP PO:x SL:NO DOD:YES DTR:1 KEEP:0 ECHO:30
```

Возможные реализации выделенной синхронной линии для устройств NSG включают:

— Прямое соединение двух устройств по последовательному интерфейсу (V.24, V.35, RS–530 или X.21) с помощью кросс-кабеля. В этом случае физический интерфейс одного из устройств должен иметь аппаратный тип DTE (MODE:EXT), а другого — DCE (MODE:INT или MODE:TTC).

— Соединение через пару внешних устройств DCE (модемов, мультиплексоров, конвертеров и т.п.), подключенных по последовательным интерфейсам. В этом случае физические интерфейсы обоих устройств имеют, как правило, аппаратный тип DTE.

— Соединение по физической медной паре с помощью интерфейсных модулей IM–*x*DSL, представляющих собой встраиваемые модемы. Модули на двух сторонах линии должны иметь противоположные настройки MODE:MASTER|SLAVE либо MODE:COE|CPE.

— Соединение через сеть оператора связи, с подключением по интерфейсу G.703.1 (E0). Скорость — 64 Кбит/с. Для подключения используются модули IM–703/64 (IF:G703_1).

— Неструктурированный канал G.703.6 (E12) через сеть оператора связи. Скорость — 2048 Кбит/с. Для подключения используются модули IM–703, IM–703–2 (IF:G703), либо модули IM–*x*E1–*x*, настроенные для работы в неструктурированном режиме:

```
S P PO:x TY:SYNC_PPP IF:E1 MODE:EXT
S P IF:y FG:NO
```

— Канал данных в структурированном потоке E1, входящем в сеть оператора связи. Канал данных представляет собой фиксированную группу канальных интервалов (таймслотов), числом от 1 до 31, со скоростью от 64 до 1984 Кбит/с, соответственно. Для подключения используются модули IM–*x*E1–*x*, настроенные для работы в структурированном режиме, например:

```
S P PO:x TY:SYNC_PPP IF:E1 MODE:EXT SP:256000
S P IF:y FG:YES DS.x:1–4
```

— Комбинации вышеперечисленных вариантов, например, на одной стороне — устройство NSG с интерфейсным модулем IM–IDSL, на другой — произвольное устройство DTE и модем IDSL иного производителя.

Б.2.5. Сервер доступа PPPoE

Устройства NSG могут использоваться в качестве сервера доступа PPP-over-Ethernet (PPPoE). Основное назначение такой инкапсуляции состоит в том, чтобы обеспечить аутентификацию, аутентификацию и учет работы пользователей в коммерческой локальной сети. Аутентификация выполняется средствами IP-интерфейса с использованием протокола PAP или CHAP.

Для настройки физического транспорта PPPoE необходимо настроить порт Ethernet (или Fast Ethernet), привязать к нему Ethernet-станцию типа PPP и создать необходимое число IP-интерфейсов с динамической привязкой к портам/станциям. Максимальное число одновременно работающих пользователей ограничено числом этих интерфейсов. При подключении очередного пользователя ему динамически предоставляется первый свободный IP-интерфейс; если свободные интерфейсы в системе исчерпаны, то в подключении будет отказано. Пример конфигурации:

```
S P PO:n TY:ETH
S P ET:m TY:PPP PO:n
S P IP:0 NUM:k+1
S P IP:1 TY:PPP PO:AUTO SL:YES KEEP:300
.....
S P IP:k TY:PPP PO:AUTO SL:YES KEEP:300
```

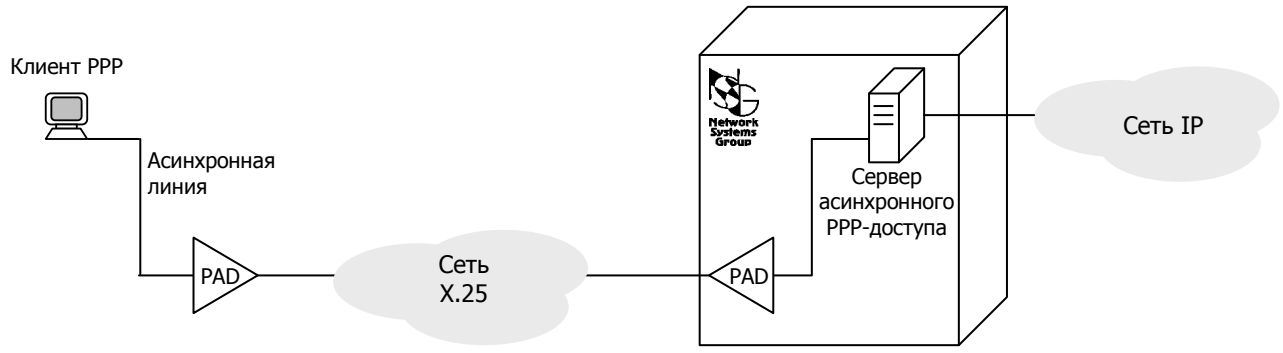
(Здесь k+1-ый интерфейс используется для подключения к магистральной сети).

Дополнительно в настройках станции можно ограничить список IP-интерфейсов, которые разрешается использовать для работы сервера PPPoE (параметр IP:xxx). Остальные интерфейсы со значением PO:AUTO в этом случае будут зарезервированы для доступа исключительно по асинхронным линиям (с терминальной аутентификацией) или по сети X.25. Параметры DOD и DTR для сервера PPPoE не имеют смысла.

ПРИМЕЧАНИЕ Для работы клиента PPPoE, входящего в состав операционной системы Windows XP, необходимо назначить Ethernet-станции произвольное непустое имя (параметр NAME:"yyy").

Б.2.6. PPP-доступ через сеть X.25

Доступ к услуге PPP может осуществляться посредством коммутируемого логического соединения в сети X.25. Схема такого подключения в общем случае показана на рисунке. Логическое соединение X.25 передает пакеты PPP от одного PAD-а до другого прозрачным образом, как асинхронный трафик общего вида; таким образом, оно эквивалентно физической асинхронной линии между клиентом и сервером PPP.



Устройство NSG в данном случае сочетает в себе функции PAD (со стороны сервера) и собственно сервера асинхронного доступа. Для работы в таком качестве необходимо настроить подключение к сети X.25 (в простейшем случае — через синхронный физический порт), создать необходимое число IP-интерфейсов с динамической привязкой к портам, и настроить маршрутизацию вызовов X.25 на все множество этих интерфейсов. Пример конфигурации:

```
S P PO:n TY:X25 ...
S P IP:0 NUM:k+1
S P IP:1 TY:PPP PO:AUTO SL:YES KEEP:300
.....
S P IP:k TY:PPP PO:AUTO SL:YES KEEP:300
S R ID:D RT:777666100 TO:PP
```

(Здесь k+1-ый IP-интерфейс используется для подключения к магистральной сети). Для установления соединения клиент должен подключиться к PAD и послать вызов (вручную или с помощью механизма автовызова) по адресу 777666100. Этот вызов маршрутизируется через сеть X.25 на устройство NSG и внутри него — на первый свободный IP-интерфейс со значением PO:AUTO. После установления соединения X.25 клиентскому PAD-у автоматически назначается прозрачный профиль.

Максимальное число пользователей, подключенных одновременно по сети X.25 (а также по асинхронным линиям с терминальной аутентификацией и по соединениям PPPoE) определяется числом IP-интерфейсов с динамической привязкой к портам. Если при подключении очередного пользователя окажется, что свободные интерфейсы в системе исчерпаны, вызов X.25 будет отвергнут.

Другой вариант конфигурации состоит в том, чтобы выделить каждому клиенту индивидуальный адрес X.121 для доступа к серверу и индивидуальный IP-интерфейс, на который маршрутизируется его вызов:

```
S P PO:n TY:X25 ...
S P IP:0 NUM:k+1
S P IP:1 TY:PPP PO:AUTO SL:YES KEEP:300
S P IP:2 TY:PPP PO:AUTO SL:YES KEEP:300
.....
S P IP:k TY:PPP PO:AUTO SL:YES KEEP:300
S R ID:D RT:777666101 TO:PP.1
S R ID:D RT:777666102 TO:PP.2
.....
S R ID:D RT:77766610k TO:PP.k
```

В этом случае заранее известно, какой клиент к какому IP-интерфейсу подключен, что упрощает управление пользователями. Аналогичным образом, используя альтернативную маршрутизацию X.25, можно ограничить список IP-интерфейсов, доступных для пользователей сети X.25, и зарезервировать остальные интерфейсы с TY:PPP PO:AUTO для других способов PPP-доступа.

Аутентификация пользователей производится средствами IP-интерфейса, т.е. с использованием протокола PAP или CHAP. Параметры DOD и DTR при доступе через сеть X.25 не имеют смысла.

Настройка клиентов зависит от того, каким образом посылается вызов X.25. Если PAD со стороны клиента настроен в режиме автовызова, т.е. при поднятии сигнала DCD он автоматически посылает пакет CALL по адресу 777666100 (для первого примера), то проключение через сеть X.25 происходит совершенно прозрачным для пользователя образом. Клиент подключается к PAD точно так же, как он если бы он подключался непосредственно к серверу асинхронного доступа.

Если PAD не поддерживает механизм автовызова, или используется для предоставления различных услуг различным пользователям, то клиент PPP посылает вызов самостоятельно. Для этого он должен использовать сценарий следующего вида:

```
<инициализация модема, набор номера>
ждать "*"
послать "777666100"<CR>
ждать "COM"
завершить сценарий
```

Конкретный формат, естественно, зависит от языка сценариев для данного клиента.

Б.2.7. Контроль правильности настройки транспорта для PPP

Чтобы убедиться, что транспортная среда для протокола PPP настроена должным образом, можно использовать следующие инструменты.

1. Трассировщик портов — для всех типов физических портов. В трассе порта видно выполнение сценария соединения, аутентификация в терминальном режиме (при наличии таковой), установление коммутируемого соединения X.25. На этом этапе обмен данными происходит в текстовом режиме. После того, как сценарий отработан полностью и получено сообщение CONNECT (либо COM для порта типа PAD, либо пакеты CALL и CALL CONFIRMATION для порта типа X25), начинается процедура согласования параметров PPP-соединения на канальном уровне с помощью протокола LCP. Визуально пакеты LCP выглядят как нечитаемые двоичные последовательности, обрамленные знаками "тильда" (~); в частности, при аутентификации по протоколу PAP в них можно наблюдать имя и пароль пользователя, передаваемые в открытом текстовом виде, и ответы сервера, например, Welcome! или Connection Rejected.
2. Статус физического порта (синхронного или асинхронного). Статус и статистику следует выводить с коротким периодом обновления, например, D S PO:n UP:3. В первую очередь следует обратить внимание на сигнал DCD (если он обеспечивается аппаратурой связи). Значение DCD:DOWN показывает, что физическое соединение отсутствует.

ПРИМЕЧАНИЕ Для портов типа ASYNC_PPP или SYNC_PPP состояние сигнала DCD выводится, начиная с версии ПО 8.2.3.

Далее, если порт имеет тип ASYNC (с терминальной аутентификацией) и при поднятом сигнале DCD этот тип сохраняется, это означает, что физическое соединение установлено, но аутентификация и авторизация клиента еще не произведены — см. следующий раздел. После успешной авторизации тип порта меняется на ASYNC_PPP.

Для портов типа ASYNC_PPP или SYNC_PPP, если в статусе порта появляются, хотя бы иногда, сообщения вида:

```
Connect to IP interface N
PPP phase: xxx          — любое, кроме Establish и Dead
LCP  state: Opened
IPCP state: xxx
CCP  state: xxx
```

это означает, что этап установления физического соединения пройден успешно и начата процедура LCP. Соответственно, ошибки надо искать на последующих стадиях. Если же при поднятом сигнале DCD процедура останавливается в одном из нижеперечисленных состояний, то причиной являются ситуации, описанные в правой колонке:

PPP phase: Dead ..... DCD: UP	Процедура LCP не стартует по одной из причин: — не отрабатывается до конца сценарий — интерфейс NSG настроен в режиме соединения по требованию (DOD:YES) и не имеет пакетов на передачу; удаленная сторона также не инициирует процедуру LCP в силу своих настроек
PPP phase: Establish LCP state: Stopped ..... DCD: UP	Интерфейс NSG настроен в режиме сервера (SL:YES) и не пытается использовать установленное соединение. Удаленная сторона также не инициирует процедуру LCP в силу своих настроек.
PPP phase: Establish LCP state: ReqSent ..... DCD: UP	Процедура LCP стартовала, запрос удаленной стороне послан, но ответ на него не приходит. Ошибку следует искать в настройках удаленной стороны.

ПРИМЕЧАНИЕ В данной реализации PPP процедура LCP стартует после завершения работы сценария, независимо от значения сигнала DCD. Если никакой сценарий не используется, а установление соединения останавливается на этапе

```
PPP phase: Establish
LCP state: ReqSent    (или Stopped)
.....
DCD: DOWN
```

это означает, что физическое соединение не установлено.

Если в статусе порта ASYNC_PPP или SYNC_PPP постоянно выводится

```
Not connected to IP interface
```

это показывает, что порт был рестартован отдельно от связанного с ним IP-интерфейса. В этом случае необходимо рестартовать соответствующий IP-интерфейс (W S IP:n) или весь IP-маршрутизатор (W S IP:0).

3. Сообщение об установлении логического соединения X.25 — для клиента, подключенного через PAD. Если соединение с IP-интерфейсом установлено успешно, клиент получает сообщение COM, после чего следуют пакеты LCP. Если вместо этого получено сообщение об ошибке, это означает либо проблемы в сети X.25 (отсутствуют свободные каналы, не настроена маршрутизация на устройство NSG и в нем — на IP-интерфейс типа PPP), либо отсутствие свободных IP-интерфейсов с TY:PPP PO:AUTO.
4. Список логических соединений (D C PO:n или D C PO:a) — для сервера асинхронного доступа с терминальной аутентификацией или PPP-over-X.25. Если список показывает, что IP-интерфейс с TY:PPP PO:AUTO привязан к некоторому физическому порту, то данное соединение (физическое или X.25) функционирует нормально. Если искомые IP-интерфейс и порт в списке отсутствуют, это означает либо неправильную настройку транспорта (не отрабатывается сценарий, не устанавливается соединение X.25 и т.п.), либо отсутствие свободных IP-интерфейсов с динамической привязкой.

   Для портов типа SYNC_PPP и ASYNC_PPP данный способ малоинформативен, поскольку они постоянно соединены с некоторым IP-интерфейсом. Отсутствие искомого порта и интерфейса в списке может означать только, что порт был рестартован отдельно от связанного с ним IP-интерфейса. В этом случае необходимо рестартовать IP-интерфейс (W S IP:n или W S IP:0).

   Для соединений PPPoE данный способ неприменим, поскольку одна Ethernet-станция типа PPP обслуживает многих клиентов. По этой причине она не включается в список логических соединений, выводимый командой D C.

Если процесс подключения дошел до описанной стадии, это означает, что транспорт для PPP настроен правильно. Все дальнейшие проблемы, если они имеют место, следует искать на уровне настройки IP-интерфейса и связанных с ним объектов: сценария соединения, способа аутентификации, таблиц пользователей или централизованных серверов аутентификации.

Б.3. Шаг 2 — настройка аутентификации

Аутентификация пользователей при подключении к устройству NSG, вероятно, представляет наиболее сложный этап настройки PPP-доступа, ввиду обилия вариантов и методов. На устройстве NSG, работающем как сервер доступа, аутентификация и авторизация пользователя могут производиться:

— Двумя различными объектами протокольной архитектуры NSG: физическом порту типа ASYNC и IP-интерфейсе типа PPP
— С использованием трех различных протоколов: PAP, CHAP и в терминальном режиме
— По трем источникам: удаленному серверу RADIUS, TACACS+, либо локальной таблице пользователей
— Завершаться, при положительном результате, предоставлением доступа к одной из двух услуг: PPP либо PAD. Последняя, в свою очередь, может быть использована для прозрачного проключения пользователя, вручную или автоматически, на серверы других услуг, таких как UUCP, BBS, FIDO, терминальный доступ к унаследованным корпоративным приложениям.

Аутентификация с использованием протоколов PAP/CHAP рекомендуется для большинства практических задач, относящихся к доступу исключительно в IP-сети. Она выполняется средствами *IP-интерфейса* типа PPP единообразно для всех видов подключений: синхронные и асинхронные физические соединения, PPPoE, доступ через сеть X.25.

На сервере могут быть включены одновременно протоколы PAP и CHAP. В этом случае сервер сначала предложит клиенту аутентифицироваться по протоколу CHAP, а затем, если клиент не согласится — по PAP. Для клиента также могут быть одновременно разрешены ответы по PAP и CHAP в зависимости от того, что предложит сервер.

Аутентификация PAP/CHAP может быть взаимной, т.е. две системы могут одновременно аутентифицировать друг друга по своим таблицам пользователей или с помощью централизованных серверов.

Аутентификация в терминальном режиме целесообразна для отдельных специфических задач, в частности, в следующих ситуациях:

— Требуется подключение к сети X.25 в режиме PAD с аутентификацией (что выходит за рамки данного документа)
— Удаленная сторона PPP не поддерживает протоколы PAP/CHAP (что в настоящее время большая редкость)
— Требуется динамический выбор предоставляемой услуги (либо PPP, либо PAD и прозрачное проключение на другие услуги) в зависимости от имени пользователя
— Терминальная аутентификация требуется по существу данного решения (например, имя/пароль пользователя настолько секретны, что не могут храниться на клиентской машине и должны каждый раз вводиться пользователем вручную 8-).

Терминальная аутентификация возможна только при доступе по асинхронным линиям. На устройстве NSG, работающем в качестве сервера, она производится средствами *физического порта*. В исходном состоянии порту должен быть назначен тип ASYNC. После успешной аутентификации пользователя порт динамически принимает тип ASYNC_PPP либо PAD в зависимости от результата авторизации; это можно видеть в текущем статусе порта, выводимом командой D S. После окончания сеанса порт снова инициализируется с типом ASYNC.

На устройстве NSG, работающем в качестве клиента, аутентификация в терминальном режиме производится с помощью *сценария соединения*, назначенного соответствующему IP-интерфейсу. Физический порт клиента всегда имеет тип ASYNC_PPP и статически связан с IP-интерфейсом типа PPP.

Допускается **двойная аутентификация** — сначала в терминальном режиме на асинхронном порту, затем по PAP/CHAP на IP-интерфейсе. На практике такой вариант представляет интерес лишь в отдельных специфических случаях. Выбор одного из протоколов аутентификации по усмотрению клиента — либо терминального режима, либо PAP/CHAP — не предусмотрен.

Аутентификация может быть настроена **избирательно** для различных IP-интерфейсов и физических портов — как на клиенте, так и на сервере. Ключевыми связующими параметрами между различными объектами конфигурации в этом случае являются номер и имя способа аутентификации.

Отрицательный результат аутентификации всегда является окончательным. Если в результате аутентификации выбранным методом получен отказ, то соединение с пользователем разрывается и никакие другие попытки аутентификации (с использованием альтернативных методов, протоколов, резервных серверов RADIUS/TACACS+ и т.п.) не предпринимаются.

Если система доступа используется **без аутентификации**, то для сервера необходимо установить значения

```
S P IP:k PAPR:0 CHAPR:0
```

Отсутствие аутентификации для IP-интерфейса указывается *только* такой совокупностью параметров, а для физического порта — жестко заданным типом ASYNC_PPP или SYNC_PPP. Способ аутентификации с типом TY:NO_AUTH имеет совершенно противоположный смысл: если сделать указание на такой способ, то подключение пользователей через данный порт или интерфейс будет запрещено.

Для клиента без аутентификации рекомендуется следующая установка: S P IP:k PAPA:NO CHAPA:NO

Б.3.1. Сервер с аутентификацией PAP/CHAP по локальной таблице пользователей

Если устройство NSG является сервером и должно аутентифицировать удаленных пользователей по локальному списку, то необходимо настроить IP-интерфейсы, способ(ы) аутентификации и список пользователей. Имена и пароли пользователей для локальной аутентификации хранятся в таблице PAP или CHAP, соответственно. Интерфейс может иметь как статическую привязку к физическому порту типа SYNC_PPP или ASYNC_PPP, так и динамическую привязку к порту типа ASYNC или иному транспорту для PPP. Простейшие конфигурации выглядят следующим образом:

```
S P IP:k TY:PPP PAPR:n                    или    S P IP:k TY:PPP CHAPR:n
S P AU:n TY:LOCAL                                S P AU:n TY:LOCAL
A X PAP:1 username1 * password1                  A X CHAP:1 username1 * password1
A X PAP:2 username2 * password2                  A X CHAP:2 username2 * password2
A X PAP:3 username3 * password3                  A X CHAP:3 username3 * password3
.....                                            .....
```

Звездочки во второй колонке таблицы PAP означают, что имя сервера может быть любым. В данном случае имя сервера — это административное имя способа аутентификации (в т.ч. пустое), т.е. все пользователи имеют равную возможность подключаться ко всем IP-интерфейсам сервера, предназначенным для этой цели.

Максимальная длина таблиц PAP и CHAP — 4096 символов. При этом необходимо учитывать разделители между записями (один символ "конец строки" на каждую запись) и разделители внутри записи (пробелы). Длина отдельной записи не регламентируется.

Б.3.2. Сервер с аутентификацией PAP/CHAP на удаленном сервере RADIUS/TACACS+

Если устройство NSG является сервером и должно аутентифицировать удаленных пользователей централизованным образом в системе на основе RADIUS или TACACS+, то необходимо настроить IP-интерфейсы и способ(ы) аутентификации. В настройках способа аутентификации должно быть указано, как минимум, число серверов аутентификации (основной и до трех резервных), их IP-адреса и ключи для обмена данными с ними. Остальные параметры могут быть установлены по умолчанию или модифицированы согласно требованиям конкретной системы.

Интерфейс может иметь как статическую привязку к физическому порту типа SYNC_PPP или ASYNC_PPP, так и динамическую привязку к порту типа ASYNC или иному транспорту для PPP. Минимальная конфигурация выглядит следующим образом:

```
S P IP:k TY:PPP PAPR:n          или    S P IP:k TY:PPP CHAPR:n
S P AU:n TY:RADIUS              или    S P AU:n TACACS+
S P AU:n SN:m SADR:x.x.x.x KEY:aaaaaa
S P AU:n SADR1:y.y.y.y KEY1:bbbbbb
.....
S P AU:n SADRm:z.z.z.z KEYm:cccccc
```

Дополнительные возможности. При аутентификации с помощью PAP/CHAP IP-интерфейс устройства NSG может передавать удаленному серверу RADIUS, в частности, следующие атрибуты:

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.

Чтобы данная информация была воспринята клиентом RADIUS, работа сценария должна быть завершена до получения сообщений CONNECT xxx и NMBR xxx, например:

```
S P IP:k 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
```

Другие возможности аутентификации с помощью серверов RADIUS/TACACS+ см. в п.Б.3.9. Полный список поддерживаемых атрибутов RADIUS и параметров TACACS+ см. в Части 8.

Б.3.3. Сервер с аутентификацией в терминальном режиме по локальной таблице пользователей

Если устройство NSG является сервером асинхронного доступа и должно аутентифицировать удаленных пользователей в терминальном режиме по локальному списку, то физическим портам устройства должен быть назначен тип ASYNC и некоторый ненулевой способ аутентификации. Помимо этого, необходимо настроить IP-интерфейсы, способ(ы) аутентификации и список пользователей.

Интерфейс в данном случае должен иметь динамическую привязку к порту. Имена и пароли пользователей для локальной аутентификации хранятся в таблице PAP. Простейшая конфигурация:

```
S  P  IP:k  TY:PPP  PO:AUTO
S  P  PO:m  TY:ASYNC  AU:n
S  P  AU:n  TY:LOCAL
A  X  PAP:1  username1  *  password1
A  X  PAP:2  username2  *  password2
A  X  PAP:3  username3  *  password3
.....
```

Особое внимание следует обратить на количество IP-интерфейсов с TY:PPP PO:AUTO. Количество таких интерфейсов есть максимальное число пользователей, которые могут быть одновременно подключены к серверу. В случае успешной аутентификации очередного пользователя порт принимает тип ASYNC_PPP и связывается с первым свободным IP-интерфейсом; если таких интерфейсов нет, в доступе будет отказано, и физическое соединение с пользователем будет разорвано.

ПРИМЕЧАНИЕ Список IP-интерфейсов, доступных для подключения через данный порт, может быть дополнительно ограничен параметром IP: в настройках порта. В этом случае порт не сможет использовать остальные IP-интерфейсы с TY:PPP PO:AUTO, даже если они свободны.

Звездочки во второй колонке таблицы PAP означают, что имя сервера может быть любым. В данном случае имя сервера — это административное имя способа аутентификации (в т.ч. пустое), т.е. все пользователи имеют равную возможность подключаться ко всем IP-интерфейсам сервера, предназначенным для этой цели.

Максимальная длина таблицы PAP — 4096 символов. При этом необходимо учитывать разделители между записями (один символ "конец строки" на каждую запись) и разделители внутри записи (пробелы). Длина отдельной записи не регламентируется.

Имя пользователя. При локальной аутентификации пользователя PPP в терминальном режиме имя должно вводиться в виде username.ppp. Суффикс .ppp является обязательным; если он отсутствует, то по умолчанию предполагается услуга PAD.

Б.3.4. Сервер с аутентификацией в терминальном режиме на удаленном сервере RADIUS/TACACS+

Если устройство NSG является сервером и должно аутентифицировать удаленных пользователей в терминальном режиме в централизованной системе на основе RADIUS или TACACS+, то физическим портам устройства следует назначить тип ASYNC и некоторый ненулевой способ аутентификации. В настройках способа аутентификации должно быть указано, как минимум, число серверов аутентификации (основной и до трех резервных), их IP-адреса и ключи для обмена данными с ними. Остальные параметры могут быть установлены по умолчанию или модифицированы согласно требованиям конкретной системы.

Интерфейс в данном случае должен иметь динамическую привязку к порту. Минимальная конфигурация:

```
S  P  IP:k  TY:PPP  PO:AUTO
S  P  PO:m  TY:ASYNC  AU:n
S  P  AU:n  TY:RADIUS          или          S  P  AU:n  TACACS+
S  P  AU:n  SN:m  SADR:x.x.x.x  KEY:aaaaaa
S  P  AU:n  SADR1:y.y.y.y  KEY1:bbbbbb
.....
S  P  AU:n  SADRm:z.z.z.z  KEYm:cccccc
```

Особое внимание следует обратить на количество IP-интерфейсов с TY:PPP PO:AUTO. Количество таких интерфейсов есть максимальное число пользователей, которые могут быть одновременно подключены к серверу. В случае успешной аутентификации очередного пользователя порт принимает тип ASYNC_PPP и связывается с первым свободным IP-интерфейсом; если таких интерфейсов нет, в доступе будет отказано, и физическое соединение с пользователем будет разорвано.

ПРИМЕЧАНИЕ Список IP-интерфейсов, доступных для подключения через данный порт, может быть дополнительно ограничен параметром IP: в настройках порта. В этом случае порт не сможет использовать остальные IP-интерфейсы с TY:PPP PO:AUTO, даже если они свободны.

Б.3.5. Аутентификация пользователя в терминальном режиме при доступе по сети X.25

Если подключение удаленного клиента PPP к устройству NSG происходит через сеть X.25, то аутентификация его на устройстве NSG возможна только по протоколам PAP/CHAP. Аутентификация в терминальном режиме, если она необходима по существу данного сетевого решения, должна производиться средствами PAD при входе в сеть X.25.

В частности, если PAD-ом является другое устройство NSG, то его конфигурация может выглядеть следующим образом:

```
S P PO:m TY:ASYNC AU:n
S P AU:n TY:LOCAL
A X PAP:1 username1 * password1 –
A X PAP:2 username2 * password2 –
A X PAP:3 username3 * password3 –
.....
```

Пользователь вводит свое имя в виде username либо username.pad (по умолчанию, эти два формата эквивалентны), после чего ему предоставляется услуга PAD. Последний параметр в записях таблицы PAP — дефис — в данном случае явно запрещает подключение любых PPP-клиентов. (Этот же результат можно было бы обеспечить неявно — одним только фактом отсутствия IP-интерфейсов с TY:PPP PO:AUTO.) Аналогичным образом настраивается централизованная аутентификация RADIUS/TACACS+.

Помимо аутентификации, порт типа PAD устройства NSG может обеспечить и другие услуги, в частности, автоматическое соединение с заданным узлом в сети X.25. После настройки параметров PAD порту снова назначается тип ASYNC; установленные таким образом параметры вступают в силу после аутентификации, если порт принимает тип PAD:

```
S P PO:m TY:PAD AC:k
S A ADk:777666123
S P PO:m TY:ASYNC AU:n
.....
```

Такой прием позволяет прозрачно проключать пользователя к различным службам в сети X.25, в т.ч. к удаленному серверу PPP-доступа, асинхронному порту произвольного назначения (через удаленный PAD), или Telnet-клиенту на этом же или другом устройстве NSG.

Б.3.6. Клиент с аутентификацией PAP

Если устройство NSG является клиентом и должно аутентифицировать себя на удаленном сервере доступа с помощью протокола PAP, то имя пользователя должно быть вписано в административное имя интерфейса. Оно же является ключом, по которому ищется подходящая запись в таблице PAP. Простейшая конфигурация:

```
S P IP:n TY:PPP PO:m PAPA:YES NAME:my_username
A X PAP:1 my_username * my_password
```

Физический порт клиента всегда имеет тип ASYNC_PPP или SYNC_PPP и статически связан с IP-интерфейсом.

Дополнительные возможности. Если разные интерфейсы устройства NSG могут подключаться к нескольким удаленным системам под одним и тем же именем, но с разными паролями, то для выбора нужного пароля используется дополнительный параметр RNAME — имя сервера.

```
S P IP:1 TY:PPP PO:1 PAPA:YES NAME:my_username RNAME:my_provider1
S P IP:2 TY:PPP PO:2 PAPA:YES NAME:my_username RNAME:my_provider2
A X PAP:1 my_username my_provider1 my_password1
A X PAP:2 my_username my_provider2 my_password2
```

В этом случае 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.

Имя RNAME в данном случае является внутренним параметром устройства NSG 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.

Б.3.7. Клиент с аутентификацией CHAP

Если устройство NSG является клиентом и должно аутентифицировать себя на удаленном сервере доступа с помощью протокола CHAP, то имя пользователя должно быть вписано в административное имя интерфейса. Оно же является ключом, по которому ищется подходящая запись в таблице CHAP. Простейшая конфигурация:

```
S P IP:n TY:PPP PO:m CHAPA:YES NAME:my_username
A X PAP:1 my_username * my_password
```

Физический порт клиента всегда имеет тип ASYNC_PPP или SYNC_PPP и статически связан с IP-интерфейсом.

Дополнительные возможности. В начале процедуры аутентификации интерфейс получает от сервера пакет CHAP Challenge Message, в котором содержится имя сервера. Таким образом, аутентификация может производиться по совокупности трех параметров — помимо имени клиента и пароля, анализируется имя сервера.

```
S P IP:1 TY:PPP PO:1 CHAPA:YES NAME:my_username
A X CHAP:1 my_username my_provider1 my_password1
A X CHAP:2 my_username my_provider2 my_password2
```

В таблице CHAP ищется строка, у которой первое поле (имя клиента) совпадает со значением параметра NAME, а второе (имя сервера) — со значением, полученным от удаленной стороны. Пароль из этой строки хэшируется и посылается удаленной стороне.

Б.3.8. Клиент с аутентификацией в терминальном режиме

Если устройство NSG является клиентом и должно аутентифицировать себя на удаленном сервере доступа с в терминальном режиме, то имя пользователя и пароль должны быть включены в сценарий соединения. Простейшая конфигурация:

```
S P IP:n TY:PPP PO:m SCRIPT:1
A X SCRIPT:1 "" ATZ OK ATDP1234567 "ogin: " my_username "assword: " my_password ""
```

При составлении сценария следует обратить особое внимание на формат приглашений, выдаваемых удаленной системой: "login" или "username", с маленькой или с большой буквы, наличие двоеточия и пробела в конце подсказки, и т.п.

Физический порт клиента всегда имеет тип ASYNC_PPP и статически связан с IP-интерфейсом.

Б.3.9. Дополнительные возможности аутентификации

Выбор протокола аутентификации PAP/CHAP. Допускается выбор одного из двух протоколов аутентификации:

```
S P IP:k PAPR:n CHAPR:m   (n, m = 1...4)
```

В этом случае сервер сначала предложит клиенту аутентифицироваться по протоколу CHAP (согласно способу аутентификации AU:m), а затем, если клиент не согласится — по PAP (согласно тому же или другому способу AU:n).

Для клиента могут быть одновременно разрешены ответы по PAP и CHAP в зависимости от того, что предложит сервер:

```
S P IP:k PAPA:YES CHAPA:YES
```

При этом имя и пароль пользователя должны быть записаны и в таблицу PAP, и в таблицу CHAP.

Проверка/назначение IP-адресов. При аутентификации (как по PAP/CHAP, так и в терминальном режиме) пользователю может быть назначен динамический IP-адрес, зависящий от его имени, либо проверен его статический IP-адрес. В случае локальной аутентификации IP-адреса хранятся в таблице пользователей:

```
A X PAP:m username * password x.x.x.x y.y.y.y z.z.z.z ...
```

Если список задан и пользователь имеет статический IP-адрес, то этот адрес должен содержаться в списке; при любом другом IP-адресе попытка аутентификации будет отвергнута. Если на месте списка стоит дефис (−), то подключение запрещено с любых IP-адресов.

При централизованной аутентификации IP-адреса пользователей хранятся на сервере RADIUS/TACACS+; дальнейший алгоритм работы определяется настройками сервера. Сервер может разрешить работу с данным статическим IP-адресом, или назначить пользователю другой адрес (если пользователь согласится его принять), или отказать в доступе.

Если клиент просит назначить ему динамический IP-адрес, то в случае успешной аутентификации ему будет назначен, соответственно, первый адрес из локального списка или адрес, присланный сервером RADIUS/TACACS+. Если такого адреса нет, используется параметр RADR, установленный для данного IP-интерфейса.

Дополнительные атрибуты сеанса. При централизованной аутентификации (как по PAP/CHAP, так и в терминальном режиме) в ответе сервера RADIUS/TACACS+ воспринимаются следующие атрибуты и параметры:

RADIUS	TACACS+	Значение
Framed-IP-Address	addr	IP-адрес, назначаемый клиенту
Framed-Compression		Режим сжатия заголовков (Van Jacobson Compression)
Idle-Timeout (сек.)	idletime (мин.)	Максимальное время неактивности пользователя
Session-Timeout (сек.)	timeout (мин.)	Максимальная продолжительность сеанса
Filter-Id	inacl, outacl	Имя или маска имен фильтров, включаемых динамически для данного сеанса

Особое внимание следует обратить на атрибуты Filter-Id, inacl, outacl. Если требуемый фильтр отсутствует или не может быть активирован по какой-либо причине, пользователь будет отвергнут. Подробно о поддерживаемых атрибутах RADIUS и параметрах TACACS+ см. Часть 8.

При локальной или отключенной аутентификации, начиная с версии программного обеспечения 8.2.3, продолжительность сеанса можно ограничить с помощью параметра AT (Active Time) в настройках IP-интерфейса.

Дифференцированный доступ. При необходимости можно дифференцировать возможность доступа различных пользователей через различные интерфейсы, например, зарезервировать определенные интерфейсы только для привилегированных пользователей или для самого системного администратора; для этого следует назначить IP-интерфейсам различные способы аутентификации и указать имена этих способов в соответствующих записях таблицы PAP. Пример:

```
S P IP:1 TY:PPP CHAP:1
S P IP:2 TY:PPP CHAP:2
S P AU:1 TY:LOCAL NAME:vipuser
S P AU:2 TY:LOCAL NAME:anyuser
A X CHAP:m boss * vnature
A X CHAP:n bratok anyuser konkretno
```

В этом случае к интерфейсу 1 может подключаться только пользователь boss, а к интерфейсу 2 — любой из двух пользователей. Более подробно о процедуре аутентификации см. Часть 8.

Б.3.10. Контроль правильности настройки аутентификации

Выполнение процедуры аутентификации можно проконтролировать при помощи следующих инструментов:

1. Трассировщик физических портов — для всех типов портов, включая соединения через порты типа X25. При аутентификации в терминальном режиме все приглашения сервера, имя и пароль пользователя передаются в текстовом виде, и ход процедуры легко анализируется по трассе порта. При аутентификации по PAP имя и пароль пользователя передаются в открытом текстовом виде и видны в теле двоичных пакетов LCP. При аутентификации по протоколу CHAP в открытом виде передаются имя сервера и имя клиента. Во всех случаях ответ сервера, как правило, также дублируется текстовым сообщением, например, Welcome! или Connection Refused.
2. Статус физического порта (синхронного или асинхронного). Статус и статистику следует выводить с коротким периодом обновления, например, D S PO:n UP:3. Если в статусе порта появляются, хотя бы на короткое время, сообщения вида:

   ```
   Connect to IP interface N
   PPP phase: Network
   LCP  state: Opened
   IPCP state: xxx
   CCP  state: xxx
   ```

   это означает, что аутентификация выполнена успешно и выполняются последующие этапы процедуры. Если процедура останавливается на шаге

   ```
   PPP phase: Authenticate
   ```

   и затем возвращается в состояние PPP phase: Dead, это *может означать*, что аутентификация не выполнена. Причиной может быть несовпадение протоколов аутентификации, установленных на клиенте и сервере, несовпадение реквизитов пользователя, предъявленных клиентом и хранящихся на сервере, или отсутствие связи с сервером аутентификации RADIUS/TACACS+. Данный критерий, однако, не является абсолютно надежным, поскольку в случае успешной аутентификации следующий шаг — процедура IPCP — выполняется очень быстро; в результате вывод команды D S выглядит одинаково как при ошибке аутентификации, так и при успешной аутентификации и ошибке на шаге IPCP.
3. Журнал сервера RADIUS/TACACS+, наличие трафика между сервером доступа и сервером аутентификации, журнал и системные сообщения удаленной стороны.

Б.4. Шаг 3 — настройка протокола IP

Согласование параметров протокола IP на обеих сторонах соединения производится после аутентификации. Для этой цели используется протокол IPCP (IP Control Protocol). На этапе IPCP могут быть назначены динамические IP-адреса, а также переданы дополнительные параметры, такие как адреса серверов DNS. В отличие от предыдущего шага (аутентификации) и последующего (согласование сжатия), данный шаг процедуры является обязательным.

После согласования IP-адресов в таблице маршрутизации устройства NSG автоматически создаются маршруты к удаленной системе, а именно, к ее интерфейсу, к которому непосредственно подключено устройство NSG. Если за удаленным устройством находятся еще какие-либо сети, то маршруты к ним необходимо создать дополнительно с помощью команд S I NET, S I DEFAULT или протокола RIP.

Наиболее сложными являются задачи с назначением динамического адреса одной из сторон, а также задачи с использованием ненумерованных IP-интерфейсов. В этих случаях необходимо обратить особое внимание на параметры, относящиеся к согласованию IP-адресов.

Б.4.1. Статические IP-адреса на обеих сторонах

Простейший случай настройки протокола IP в соединении "точка-точка" — это классическая мини-сеть из двух хостов, со статическими IP-адресами и длиной маски 30 бит. **Каждое устройство** знает свой IP-адрес и адрес удаленной стороны. Настройка IP-интерфейса устройства NSG в этом случае выглядит следующим образом (в части, касающейся IP-адресов):

```
S P IP:n TY:PPP IADR:10.0.0.1 MASK:255.255.255.252
```

Удаленная сторона в данном примере имеет адрес 10.0.0.2. Следует также обратить внимание на параметры, относящиеся к динамическому назначению IP-адресов — эти параметры сохраняют значения по умолчанию:

```
S P IP:n TY:PPP ACCL:NO RADR:0.0.0.0
```

После настройки и рестарта интерфейса в таблице маршрутизации появляются соответствующие записи:

```
Manager: D I
```

net	mask	gateway	metric	intf	ttl	use
010.000.000.003	255.255.255.255	010.000.000.001	00	000	999	0000
010.000.000.000	255.255.255.255	010.000.000.001	00	000	999	0000
010.000.000.001	255.255.255.255	010.000.000.001	00	000	999	0000
010.000.000.000	255.255.255.252	010.000.000.001	01	n	999	0000

Б.4.2. Назначение IP-адреса устройству NSG удаленной стороной

Если устройство NSG не имеет заранее заданного IP-адреса и должно получить динамический адрес от удаленной стороны, то при создании IP-интерфейса ему необходимо назначить произвольный фиктивный IP-адрес. Для этого адреса, как и для любого другого, создаются соответствующие записи в таблице маршрутизации, поэтому рекомендуется использовать для этой цели схему с ненумерованным интерфейсом (см. п.Б.4.4): в этом случае создается только одна лишняя запись вместо четырех.

Важнейшим параметром в данной ситуации является ACCL:YES — принимать адрес, назначаемый удаленной стороной. Конфигурация IP-интерфейса в части, касающейся IP-адресов, выглядит следующим образом:

```
S P IP:n TY:PPP IADR:192.168.0.1 MASK:255.255.255.255 ACCL:YES RADR:0.0.0.0
```

На удаленной стороне, соответственно, должны быть заданы ее собственный IP-адрес и адрес, назначаемый партнеру. Если, например, удаленная сторона имеет IP-адрес 123.145.167.1/30 и назначает устройству NSG адрес 123.145.167.2, то после установления соединения соответствующий фрагмент таблицы маршрутизации в устройстве NSG имеет вид:

```
Manager: D I
```

net	mask	gateway	metric	intf	ttl	use
192.168.000.001	255.255.255.255	192.168.000.001	00	n	999	0000
123.145.167.001	255.255.255.255	123.145.167.001	01	n	999	0000
123.145.167.002	255.255.255.255	123.145.167.002	00	000	999	0000

Б.4.3. Назначение IP-адреса удаленной стороне устройством NSG

Если устройство NSG динамически назначает адрес удаленной стороне, то этот адрес может быть задан одним из двух способов:

— Взят из локальной таблицы пользователей или получен от централизованного сервера аутентификации RADIUS/TACACS+, в зависимости от выбранного способа аутентификации
— Установлен в параметре RADR IP-интерфейса

Если в двух этих местах заданы два разных IP-адреса, то приоритет имеет первый, как более специфичный для данного пользователя. Если в ходе аутентификации пользователя IP-адрес не оговаривается, то используется адрес RADR — единый для всех пользователей, подключающихся к данному интерфейсу.

Пример конфигурации IP-интерфейса (с собственным статическим IP-адресом и 30-битной маской):

```
S P IP:n TY:PPP IADR:10.0.0.1 MASK:255.255.255.252 ACCL:NO RADR:10.0.0.2
```

На удаленной стороне должен быть включен режим получения динамического IP-адреса. Если удаленная сторона пытается работать со статическим IP-адресом, соединение установлено не будет.

Б.4.4. Ненумерованный интерфейс устройства NSG, статический IP-адрес удаленной стороны

Интерфейс типа PPP может не иметь собственного IP-адреса. В этом случае для него указывается специальная маска 255.255.255.255, указывающая, что значение параметра IADR есть адрес удаленной стороны, а не адрес самого интерфейса.

Однако при этом протокол IPCP все равно требует, чтобы каждому устройству были известны два несовпадающих IP-адреса: его собственный адрес и адрес удаленной стороны. Поэтому необходимо использовать дополнительный параметр SADR (Source IP Address). Этот адрес передается в пакетах IPCP как адрес самого устройства NSG. Он же указывается в качестве источника в IP-пакетах, отправляемых устройством NSG через данный интерфейс (например, службой Telnet или утилитой *ping*).

Значением SADR может быть IP-адрес любого из нумерованных интерфейсов устройства NSG, например, интерфейса, обращенного в локальную сеть. Пример конфигурации IP-интерфейсов:

```
S P IP:m TY:ETHI IADR:19.17.15.13 MASK:255.255.255.0 …
S P IP:n TY:PPP IADR:12.14.16.18 MASK:255.255.255.255 SADR:19.17.15.13 ACCL:NO RADR:0.0.0.0
```

На удаленной стороне в данном случае задан статический адрес 12.14.16.18 с произвольной маской.

В таблице маршрутизации при этом создается единственная запись:

```
Manager: D I
      net              mask            gateway        metric  intf   ttl   use
012.014.016.018  255.255.255.255  012.014.016.018      00      n     999   0000
```

Б.4.5. Ненумерованный интерфейс устройства NSG, динамический IP-адрес удаленной стороны

Данный случай представляет собой комбинацию двух предыдущих и наиболее актуален для организации услуг доступа в Интернет. При такой постановке задачи необходимо указать IP-адрес, назначаемый удаленной стороне (в настройках службы аутентификации или в параметре RADR) и адрес SADR, под которым для нее будет известно устройство NSG:

```
S P IP:m TY:ETHI IADR:19.17.15.13 MASK:255.255.255.0 …
S P IP:n TY:PPP IADR:12.14.16.18 MASK:255.255.255.255 SADR:19.17.15.13 ACCL:NO RADR:12.14.16.18
```

В данном примере значение RADR совпадает со значением IADR, т.е. удаленной стороне назначается именно тот адрес, под которым оно известно устройству NSG. Это наиболее естественное решение: каждому IP-интерфейсу соответствует жестко заданный IP-адрес пользователя и, при доступе по физическим линиям, жестко заданный физический порт. Экономить IP-адреса за счет их плавающего распределения между интерфейсами в данном случае бессмысленно: если уж предполагается, что все порты устройства могут работать одновременно, то для него нужно выделить ровно такое же количество IP-адресов.

Если RADR≠IADR, или IP-адрес удаленной стороны назначается сервером RADIUS/TACACS и заранее неизвестен, то адрес IADR является фиктивным и нужен только для создания IP-интерфейса NSG. Для него создается одна формальная запись в таблице маршрутизации; после установления соединения к ней добавляется вторая запись, относящаяся к фактическому адресу удаленной стороны:

```
S  P  IP:m  TY:ETHI  IADR:19.17.15.13  MASK:255.255.255.0  …
S  P  IP:n  TY:PPP  IADR:10.0.0.1  MASK:255.255.255.255  SADR:19.17.15.13  ACCL:NO  RADR:12.14.16.18
```

```
Manager: D I
      net              mask            gateway          metric  intf  ttl  use
010.000.000.001  255.255.255.255  010.000.000.001  00      n     999  0000
012.014.016.018  255.255.255.255  012.014.016.018  00      n     999  0000
```

На удаленной стороне должен быть включен режим получения динамического IP-адреса. Если удаленная сторона пытается работать со статическим IP-адресом, соединение установлено не будет.

Б.4.6. Два ненумерованных IP-интерфейса

Возможна конфигурация, когда оба интерфейса в PPP-соединении являются ненумерованными. Это не противоречит протоколу, при условии, что каждая из сторон знает два различных IP-адреса: для себя и для партнера. Такая конфигурация уместна, например, при соединении двух офисов. В качестве IADR и SADR (т.е. в качестве адреса удаленной стороны и локального адреса) в этом случае следует указать адреса интерфейсов Ethernet, обращенных в сети удаленного и локального офисов, соответственно.

Для устройства в сети А:

```
S  P  IP:1  TY:ETHI  IADR:192.168.1.1  MASK:255.255.255.0  …
S  P  IP:2  TY:PPP  IADR:192.168.2.1  MASK:255.255.255.255  SADR:192.168.1.1
```

Для устройства в сети Б:

```
S  P  IP:1  TY:ETHI  IADR:192.168.2.1  MASK:255.255.255.0  …
S  P  IP:2  TY:PPP  IADR:192.168.1.1  MASK:255.255.255.255  SADR:192.168.2.1
```

Б.4.7. Контроль правильности настройки IP-адресов

После выполнения процедуры IPCP соединение готово к передаче IP-трафика, независимо от результата последнего шага — CCP. Если аутентификации завершается успешно, но соединение не приходит в рабочее состояние, то ошибку следует искать в несогласованных настройках IP-адресов на двух сторонах.

Отладка протокола IPCP в большинстве случаев ограничивается пассивной проверкой настроек IP на одной и на другой стороне. При этом следует обратить особое внимание на следующие параметры, в зависимости от постановки задачи:

Задача	Параметры NSG	Настройки удаленной стороны
1. Статические IP-адреса на обеих сторонах	IADR, MASK, ACCL:NO, RADR:0.0.0.0	Статический IP-адрес или ненумерованный интерфейс; назначение IP-адреса партнеру отключено
2. NSG получает IP-адрес от удаленной стороны	IADR, MASK — фиктивные; ACCL:YES, RADR:0.0.0.0	Статический IP-адрес или ненумерованный интерфейс; назначение IP-адреса партнеру включено
3. NSG назначает IP-адрес удаленной стороне	IADR, MASK, ACCL:NO; RADR (или назначение IP-адреса в процессе авторизации)	Получение динамического IP-адреса от партнера; назначение IP-адреса партнеру отключено
1a, 3a. Вариации пп. 1 и 3: интерфейс NSG — ненумерованный	IADR, MASK, ACCL, RADR — аналогично пп. 1 и 3, соотв.; SADR — обязательно	Аналогично пп. 1 и 3, соответственно.

Явным образом проследить за установлением соединения на этапе IPCP возможно только для физических портов. Если статус порта (D S PO:n UP:3) выглядит следующим образом:

```
Connect to IP interface N
PPP phase: Network
LCP  state: Opened
IPCP state: Opened
CCP  state: xxx
```

это означает, что согласование IP-адресов выполнено успешно и выполняется (или уже выполнен) последний этап процедуры — согласование сжатия. Любые другие состояния протокола IPCP, помимо Initial, Opened, Stopping и Stopped, означают, что данная процедура начата и не завершена успешно.

Б.4.8. Передача адресов DNS удаленной стороне

Протокол PPP предусматривает обмен целым рядом дополнительных параметров, наиболее важными из которых являются адреса серверов DNS. Устройство NSG, работающее в качестве сервера, позволяет передать клиенту адреса двух серверов DNS (основного и резервного). Для этого необходимо включить на нем службу DNS и настроить адреса серверов:

```
S P IP:0 DNS:YES DNS1:x.x.x.x DNS2:y.y.y.y
```

Заданные таким образом параметры DNS являются глобальными, т.е. относятся ко всему устройству в целом. При подключении пользователя к любому IP-интерфейсу ему будут переданы эти два адреса. На клиенте должна быть включена опция "Адреса DNS назначаются сервером" (если таковая предусмотрена).

Б.5. Шаг 4 —настройка сжатия

Согласование механизмов сжатия для заголовков и тела IP-пакетов представляет собой последний этап процедуры установления PPP-соединения. При этом сам факт сжатия согласовывается сторонами в начале процедуры, а после завершения этапа IPCP происходит согласование алгоритмов и параметров сжатия. Этот этап регламентируется протоколом Compression Control Protocol (CCP).

Сжатие не является обязательным: если оно запрещено на одной из сторон, или стороны не смогли договориться об используемом алгоритме, PPP-соединение продолжает работать без сжатия.

Б.5.1. Сжатие заголовков IP-пакетов

При сжатии заголовков IP-пакетов различные поля сжимаются независимо, в частности, одни поля могут быть сжаты, другие — нет. По умолчанию, все механизмы сжатия заголовков в устройствах NSG отключены, т.е. для интерфейса типа PPP установлены следующие значения параметров:

```
S P IP:x AC:NO PC:NO VJ:NO VJC:NO
```

Чтобы разрешить сжатие заголовков "по максимуму", следует установить

```
S P IP:x AC:YES PC:YES VJ:16 VJC:YES
```

В частности, данный набор параметров, а также ряд других параметров, устанавливается подкомандой DEF для быстрой настройки IP-интерфейса.

Вообще говоря, стандарт PPP предусматривает, что сжатие заголовков должно согласовываться в любом случае; однако если заранее известно, что соединенные устройства не поддерживают совместимых алгоритмов сжатия, или если сжатие нежелательно по какой-либо иной причине (нехватка аппаратных ресурсов на любой из сторон, ненадежная программная реализация, и т.п.), его можно заранее отключить на обеих сторонах. Это несколько ускорит установление PPP-соединения, исключив из него заведомо безрезультатную процедуру.

Аналогичным образом, если известно, что удаленная сторона не поддерживает какой-либо из механизмов сжатия, или, например, поддерживает сжатие Van Jakobson только с меньшим числом слотов, то можно избирательно отключить/ограничить лишние параметры, что также ускорит процедуру установления соединения.

С другой стороны, конкретные реализации протокола PPP в оборудовании других производителей могут (по крайней мере, теоретически) интерпретировать стандарт максимально строгим образом и не соглашаться на PPP-соединение без согласования сжатия заголовков. В этом случае необходимо включить сжатие заголовков и на устройстве NSG.

Б.5.2. Сжатие данных

Для сжатия тела IP-пакетов при передаче по протоколу PPP могут использоваться различные алгоритмы — как стандартные, так и фирменные различных производителей. Устройства NSG поддерживают только сжатие по методу BSD (BSD Compression, BSDC). По умолчанию, оно выключено:

```
S P IP:x BSDC:NO
```

Включать сжатие данных имеет смысл только в том случае, если достоверно известно, что удаленная сторона также поддерживает BSD Compression и настроена аналогичным образом. При этом можно избирательно устанавливать степень сжатия (с параметром от 9 до 15) в одном и в другом направлении. Бóльшие значения параметра обеспечивают более высокую степень сжатия, однако требуют, соответственно, увеличенного объема оперативной памяти (в разделе Heap). В частности, использовать сжатие на устройствах младшего уровня (серии NPS–7e, NSG–500) не рекомендуется вовсе.

Если на удаленной стороне BSD Compression не поддерживается, или не включено, то включение BSDC на устройстве NSG не имеет смысла и только удлиняет процесс установления PPP-соединения. То же самое относится к случаю, когда на одной стороне параметры сжатия ограничены, а на другой — заведомо завышены.

Б.5.3. Контроль правильности настройки сжатия

Вывод текущих параметров сжатия для установленного PPP-соединения в устройствах NSG не предусмотрен. Возможно только проследить за ходом процедуры CCP для физических портов (строка CCP state:).

В нормальных условиях процедура согласования параметров сжатия выполняется быстро, и увидеть это состояние крайне маловероятно. Если же установление PPP-соединения задерживается на этом шаге, это свидетельствует о неэффективной настройке параметров сжатия: на одной из сторон включены механизмы и алгоритмы, не поддерживаемые другой стороной (обе стороны последовательно перебирают все разрешенные варианты), либо заведомо завышенные степени сжатия (согласование происходит от максимальной степени в сторону уменьшения, пока не будет достигнут приемлемый показатель для обеих сторон), либо на одной из сторон какой-либо из механизмов сжатия работает некорректно. В этом случае рекомендуется выполнить одну из следующих процедур:

— сначала отключить всё сжатие, а затем последовательно включать отдельные его компоненты и увеличивать степени сжатия до тех пор, пока процедура не становится опять аномально длительной

— сначала включить сжатие заголовков, а затем последовательно отключать отдельные его компоненты и уменьшать степень сжатия до тех пор, пока процедура не войдет в нормальные временные рамки.

Б.6. Средства диагностики и отладки PPP-соединений

Б.6.1. Прозрачное проключение на физический порт

Если к асинхронному порту устройства NSG подключен модем и требуется получить непосредственный доступ к этому модему — для его настройки, перепрошивки программного обеспечения, отладки процедуры дозвона и терминальной аутентификации — это можно сделать двумя способами.

Подключение через свободный физический порт. Предположим, что модем подключен к порту m устройства; кроме того, в устройстве имеется свободный порт n с интерфейсом V.24 (RS–232) и соответствующим соединительным кабелем, который может быть подключен к COM-порту ПК. Следует назначить обоим портам тип ASYNC без аутентификации и установить между ними постоянное виртуальное соединение:

```
S P PO:m TY:ASYNC IF:V24 SP:115200
S P PO:n TY:ASYNC IF:V24 SP:115200
A P PO:PO.n PO:PO.m
W S PO:m
W S PO:n
```

На ПК используется любая программа эмуляции терминала, настроенная для работы с соответствующим COM-портом. Все символы, вводимые пользователем, прозрачно передаются на модем, и наоборот.

Подключение через Telnet. Если на устройстве нет свободных портов, или у администратора нет желания возиться с лишними кабелями, вместо этого можно аналогичным образом подключиться к модему через Telnet-станцию. Станции также назначается тип ASYNC и индивидуальный номер порта TCP, например:

```
S P PO:m TY:ASYNC IF:V24 SP:115200
S P TN:1 TY:ASYNC TCPPORT:8023
A P PO:PO.m PO:TN.1
W S PO:m
W S TN:1
```

Устройство должно быть доступно по сети IP. На ПК используется любой клиент Telnet, с помощью которого устанавливается соединение к порту 8023 (вместо стандартного 23). После этого символы, вводимые пользователем в клиенте Telnet, прозрачно передаются на модем, и наоборот.

После того, как доступ к модему получен любым из этих способов, можно вводить любые AT-команды, посылать файлы по Xmodem, и т.п. Применительно к предмету данного документа, задача обычно состоит в том, чтобы отладить последовательность команд и ответов для набора номера и аутентификации в терминальном режиме. Полученная последовательность далее записывается в виде сценария PPP-соединения.

Восстановление штатной конфигурации. После завершения работы порту снова назначается тип ASYNC_PPP (либо требуемый способ аутентификации) и удаляется PVC между ним и вспомогательным портом/станцией. В заключение необходимо рестартовать соответствующий IP-интерфейс (или IP-маршрутизатор в целом), чтобы восстановить его привязку к данному порту:

```
S P PO:m TY:ASYNC_PPP IF:V24 SP:115200
R P PO:PO.m
W S PO:m
W S IP:k (или W S IP:0)
```

Б.6.2. Трассировщик физических портов

Трассировщик представляет собой служебный процесс, с помощью которого можно производить мониторинг данных, получаемых и передаваемых физическим портом. Трассировщик включается и подключается к требуемому порту командами:

```
T R START
T R PO:n ON
```

После этого все данные, проходящие через указанный порт, копируются в трассу. Чтобы увидеть эту трассу, необходимо сконфигурировать в устройстве вспомогательный физический порт или Telnet-станцию типа PAD и определить маршрут к трассировщику, например:

```
S P TN:2 TY:PAD
S R ID:D RT:123 TO:TC
```

После подключения к физическому порту или Telnet-станции на экран будет выведено приглашение PAD (звездочка), в ответ на которое следует ввести вызываемый адрес 123. В ответ будет получено COM (сигнал об установлении физического соединения), после чего начнет выводиться трасса порта в шестнадцатеричном и текстовом виде (по 14 байт в строке), например:

```
root@nsgboard2 root]# telnet 10.0.0.1
Trying 10.0.0.1...
Connected to 10.0.0.1
Escape character is '^]'.

*123
COM
4:25:10.08 PO:01 t–> 41 54 0D                                    | AT.
4:25:10.08 PO:01 <–r 41 54 0D                                    | AT.
4:25:10.09 PO:01 <–r 0D 0A 4F 4B 0D 0A                           | ..OK..
4:25:10.10 PO:01 t–> 0D                                          | .
4:25:10.10 PO:01 t–> 41 54 2B 43 47 44 43 4F 4E 54 3D 31 2C 22   | AT+CGDCONT=1,"
                     49 50 22 2C 22 69 6E 74 65 72 6E 65 74 2E   | IP","internet.
                     62 65 65 6C 69 6E 65 2E 72 75 22 0D         | beeline.ru".
4:25:10.20 PO:01 <–r 0D                                          | .
4:25:10.20 PO:01 <–r 41 54 2B 43 47 44 43 4F 4E 54 3D 31 2C 22   | AT+CGDCONT=1,"
                     49 50 22 2C 22 69 6E 74 65 72 6E 65 74 2E   | IP","internet.
                     62 65 65 6C 69 6E 65 2E 72 75 22 0D         | beeline.ru".
4:25:10.22 PO:01 <–r 0D 0A 4F 4B 0D 0A                           | ..OK..
4:25:10.34 PO:01 t–> 41 54 2B 43 47 52 45 47 3D 31 0D            | AT+CGREG=1.
4:25:10.34 PO:01 t–> 41 54 2B 43 47 52 45 47 3F 0D               | AT+CGREG?.
4:25:10.48 PO:01 <–r 41 54 2B 43 47 52 45 47 3D 31 0D            | AT+CGREG=1.
4:25:10.49 PO:01 <–r 0D 0A 4F 4B 0D 0A 0D 0A 2B 43 47 52 45 47   | ..OK....+CGREG
                     3A 20 31 0D 0A                              | : 1..
4:25:10.50 PO:01 <–r 41 54 2B 43 47 52 45 47 3F 0D               | AT+CGREG?.
4:25:10.50 PO:01 <–r 0D 0A 2B 43 47 52 45 47 3A 20 31 2C 31 0D   | ..+CGREG: 1,1.
                     0A 0D 0A 4F 4B 0D 0A                        | ...OK..
4:25:10.56 PO:01 t–> 41 54 2B 43 47 44 41 54 41 3D 31 0D         | AT+CGDATA=1.
4:25:10.60 PO:01 <–r 41 54 2B 43 47 44 41 54 41 3D 31 0D         | AT+CGDATA=1.
4:25:10.61 PO:01 <–r 0D 0A 43 4F 4E 4E 45 43 54 20 31 31 35 32   | ..CONNECT 1152
                     30 30 0D 0A                                 | 00..
.....................................................................
```

Здесь строки с указателем t–> означают данные, посылаемые устройством NSG в физический порт, строки с указателем <–r — данные, принимаемые из порта. Непечатаемые символы заменяются точками.

В частности, можно использовать для мониторинга трассы станцию TN:0, обычно используемую для управления устройством; для этого следует не входить в модуль Manager (не вводить команду mn), либо выйти из него (команда Q M), но не разрывать Telnet-соединение.

Для выключения трассировщика необходимо ввести в модуле Manager команду

```
T R STOP
```

Чтобы отключить трассировщик от данного порта, не останавливая его (например, для мониторинга какого-либо другого порта), можно использовать команду

```
T R PO:n OFF
```

Б.6.3. Статус и статистика портов, станций и интерфейсов

Команда D S (Display Status/Statistics) позволяет судить об активности требуемого объекта (физического порта, станции PPPoE, IP-интерфейса), а также о ходе процедуры установления PPP-соединения. Удобно использовать данную команду с периодическим обновлением через каждые 3–5 сек:

```
D S PO:n UP:3
```

Формат вывода статистики различается в зависимости от выбранного транспорта для PPP.

Физический порт типа ASYNC_PPP **или** SYNC_PPP. В статусе порта могут присутствовать следующие сообщения:

Not connected to IP interface — Порт не связан с соответствующим IP-интерфейсом. Такая ситуация наблюдается в случае, если порт был рестартован отдельно от IP-интерфейса. Для восстановления связи между ними необходимо рестартовать IP-интерфейс (W S IP:n) или весь IP-маршрутизатор (W S IP:0).

Connect to IP interface N — Порт связан с указанным IP-интерфейсом типа PPP. После этого сообщения выводится информация о статусе PPP-соединения.

Проверить состояние внутренних соединений между физическими портами и IP-интерфейсами можно также при помощи команды Display Connections (см. следующий параграф).

В части относящейся к протоколу PPP, выводится статус PPP-соединения в целом (PPP phase) и протоколов, относящихся к отдельным его фазам. Соединение может находиться в одном из следующих состояний:

Dead — Исходное состояние — интерфейс не пытается установить PPP-соединение. Устройство NSG либо находится на этапе выполнения сценария, либо сконфигурировано в режиме соединений по требованию (DOD:YES) и не инициирует его выполнение.

Establish — Выполнение сценария завершено (или никакой сценарий не используется), начата процедура LCP, но она еще не завершена. Фазы протокола LCP выводятся в следующей строке. Длительная задержка или остановка процедуры на этой стадии может свидетельствовать о неправильной настройке параметров SL, AM и параметров сжатия.

Authenticate — Первоначальные параметры канального уровня согласованы, выполняется аутентификация по протоколам PAP/CHAP. Остановка на этом этапе означает неправильную настройку аутентификации на одной или обеих сторонах, либо отсутствие связи с централизованным сервером RADIUS/TACACS+. Следует обратить внимание на следующие параметры и объекты:
- PAPR, CHAPR и способ аутентификации (AU:n) на стороне, запрашивающей аутентификацию
- PAPA, CHAPA, имя интерфейса (NAME) и имя удаленной стороны (RNAME) на стороне, пытающейся аутентифицировать себя
- таблицы паролей (на обеих сторонах) и настройки централизованных серверов аутентификации

Network — PPP-соединение установлено и готово для работы протокола вышележащего уровня (в данном случае — IP). В этой фазе выполняется согласование параметров IP (IPCP) и сжатия (CCP). После завершения этапа IPCP соединение полностью готово к передаче IP-пакетов.

Terminate — Выполняется процедура разрыва PPP-соединения. Это происходит при ошибке или отказе на этапе аутентификации, IPCP, или по инициативе одной из сторон во время работы соединения (например, по причине длительного отсутствия активности). Данная фаза выполняется быстро, поэтому застать порт в этом состоянии удается редко.

Для протоколов LCP, IPCP и CCP наиболее вероятны следующие состояния:

Initial — Исходное состояние протокола: не завершено исполнение сценария (для LCP), либо не выполнены предшествующие процедуры (для IPCP, CCP).

ReqSent, AckRcvd, AckSent — Выполняется согласование параметров, относящихся к данному протоколу. Если процедура доходит до этой фазы и затем аварийно завершается, значит, на двух сторонах соединения установлены несовместимые параметры. На выполнение данных этапов влияют следующие параметры IP-интерфейса NSG (и аналогичные настройки для удаленной стороны):

- на этапе LCP: AM, AC, PC, VJC, VJ, BSDC (последние два — только в смысле "да/нет")
- на этапе IPCP: IADR, MASK, ACCL, RADR (или назначение IP-адреса клиенту централизованным сервером), SADR
- на этапе CCP: VJ, BSDC

Если установление соединения прерывается на одном из этих этапов, необходимо проверить вышеперечисленные параметры и их согласование с аналогичными настройками удаленной стороны.

Для протокола LCP остановка в состоянии ReqSent может также означать, в данной реализации PPP, что физическое соединение отсутствует. Различить эти две ситуации можно по состоянию сигнала DCD.

Opened — Согласование параметров соединения, относящихся к данной фазе, успешно завершено. Процедура перешла в следующую фазу, или же соединение уже готово к передаче IP-пакетов (если данная фаза — последняя).

Closing, Closed — Данная фаза соединения завершается/завершена неудачно, либо не выполнялась (CCP при выключенных параметрах сжатия). Список параметров, относящихся к каждому из трех протоколов, см. выше. После аварийного завершения одного из протоколов (кроме CCP) происходит завершение работы всех предшествующих протоколов и разрыв физического соединения.

Stopping, Stopped

Данная фаза соединения была выполнена успешно, но теперь работа данного протокола прекращается/прекращена. Причиной может быть ошибка на одном из последующих этапов, либо принудительное разъединение (например, по таймеру неактивности). Для протокола LCP состояние Stopped устанавливается также в случае, если интерфейс сконфигурирован в режиме сервера (SL:YES), а сценарий соединения успешно завершен или отсутствует.

Далее следует состояние сигналов интерфейса и статистика трафика в порту (число принятых/переданных байт и т.п.) Первоочередное внимание следует обратить на состояние сигнала DCD.

ПРИМЕЧАНИЕ Для портов типа ASYNC_PPP и SYNC_PPP состояние сигналов выводится, начиная с версии ПО 8.2.3; в более ранних версиях можно пользоваться соответствующим индикатором модема.

Ethernet-станции типа PPP. Для данного типа объектов столь подробный вывод статистики не предусмотрен. О ходе установления соединения можно судить косвенно по наличию трафика на станции — при условии, что это соединение единственное.

Физические порты типа PAD**.** Для данного типа портов выводятся показатели статуса и статистики, относящиеся к их работе в качестве PAD; передача пакетов PPP является одним из частных случаев трафика PAD и никак особо не отражается. О ходе установления соединения можно судить косвенно по наличию трафика, а также по наличию соединения с IP-интерфейсом (команда Display Connections).

Физические порты типа ASYNC (с аутентификацией в терминальном режиме). Формат вывода статуса/статистики изменяется в зависимости от *текущего* состояния порта. После успешной аутентификации пользователя и его авторизации на услугу PPP порт принимает тип ASYNC_PPP и привязывается к IP-интерфейсу; дальнейшие ошибки следует искать в настройках параметров, относящихся к этапам IPCP и CCP.

Если текущий тип порта показывается как ASYNC, это означает, что процедуры установления физического соединения и аутентификации пользователя еще не завершены.

Если текущий тип порта показывается как PAD, это означает, что пользователю вместо PPP назначена услуга PAD (например, при аутентификации по локальной таблице имя пользователя было введено без суффикса .ppp).

IP-интерфейсы типа PPP**.** Статистика IP-интерфейса представляет интерес в совокупности со статистикой физического порта или Ethernet-станции. Различие между ними состоит в следующем:

— Для IP-интерфейса учитываются только IP-пакеты с полезной нагрузкой, переданные по установленному PPP-соединению

— Для порта/станции учитываются все пакеты PPP, переданные по данному физическому соединению — в том числе служебные пакеты LCP, IPCP, CCP.

В частности, если в соединении должен быть какой-то полезный трафик (например, запущен *ping* с одного устройства на другое), но при этом трафик порта/станции растет, а трафик IP-интерфейса — нет, это означает, что PPP-соединение находится в процессе установления, и еще не готово к работе.

Б.6.4. Список логических соединений

Команда Display Connections позволяет проверить список логических соединений, установленных между различными объектами внутри устройства. Пример вывода команды:

```
Manager: D C PO:A

PO:02           Bind to IP interface 2
PO:03  CH:001   Connect to Manager, src=<NONE>, dst=<NONE>, tm=0:03:06.01
ET:00           Bind to IP interface 1
```

Все физические порты типа ASYNC_PPP или SYNC_PPP должны быть статически соединены с соответствующими IP-интерфейсами. Если такая связь отсутствует, причина может быть одной из следующих:

— Неправильная конфигурация порта — задан другой тип
— Неправильная конфигурация IP-интерфейса — см. параметры TY:PPP PO:n
— Не рестартован порт и/или IP-интерфейс, поэтому требуемая конфигурация еще не введена в действие
— Порт рестартован вручную отдельно от IP-интерфейса

Для физических портов типа ASYNC и PPP-подключений через сеть X.25 (физическую, X.25-over-Frame Relay или X.25-over-Ethernet) связь с IP-интерфейсом устанавливается динамически. Если требуемый объект присутствует в списке, это означает, что транспорт для PPP функционирует нормально и терминальная аутентификация выполнена успешно; дальнейшие ошибки следует искать в настройках IP-интерфейса.

Если искомое соединение отсутствует, это может означать, что:

— Физическое соединение или соединение X.25 не функционирует должным образом
— Аутентификация и авторизация пользователя на физическом порту не включена (параметр AU: для данного порта равен нулю), не сконфигурирована должным образом, или не завершена

Естественно, его также не будет в случае, когда транспортное соединение разорвано по любой из следующих причин:

— Терминальная аутентификация завершена с отрицательным результатом
— Для входящего вызова X.25 не настроена маршрутизация на интерфейс(ы) типа PPP
— IP-интерфейсы с TY:PPP PO:AUTO отсутствуют, или все заняты, или не входят в список разрешенных для данного порта

Наличие PPP-соединений через сети X.25-over-TCP/IP и X.25-over-X.25 можно проверить аналогичным образом с помощью команд:

```
D S XOT
D S HX:0
```

ПРИМЕЧАНИЕ Команда D C не показывает соединения для Ethernet-станций типа PPP, поэтому для них этот способ контроля неприменим.

Б.6.5. Контроль назначенного IP-адреса

Если IP-интерфейс устройства NSG работает в качестве PPP-клиента и динамически принимает IP-адрес, назначаемый удаленной стороной, то проверить, какой адрес назначен ему в данном сеансе, можно из таблицы маршрутизации при помощи команды D I, например:

```
Manager: D I
      net             mask            gateway        metric  intf  ttl   use
123.145.167.001  255.255.255.255  123.145.167.001     01      002   999   0000
123.145.167.002  255.255.255.255  123.145.167.002     00      000   999   0000
```

В данном случае интерфейсу 2 назначен IP-адрес 123.145.167.2, а адрес удаленной стороны, расположенной за этим интерфейсом — 123.145.167.1. Маршруты к обоим этим адресам всегда имеют маску 255.255.255.255.

ПРИМЕЧАНИЕ IP-адреса клиента и сервера, в общем случае, никак не связаны друг с другом. Если запись с адресом удаленной стороны легко идентифицируется по номеру интерфейса, то адрес самого интерфейса следует внимательно искать среди записей, указывающих на локальный псевдоинтерфейс 0. Более того, они могут переназначаться удаленной стороной в ходе сеанса. Это наблюдается, в частности, у некоторых сотовых операторов.

Б.6.6. Утилита ping

Процедура *ping* является общепринятым средством проверки связности IP-сетей и контролирует работоспособность всех трех нижних уровней протокола TCP/IP. Применительно к обсуждаемой задаче это:

— Транспортное соединение для PPP (модемное соединение, нуль-модемный кабель, логическое соединение X.25, сеть Ethernet)
— Протокол PPP (инициализация PPP-соединения и согласование его параметров)
— IP-маршрутизация

PPP-соединение можно считать полностью работоспособным, если проходит *ping* с одного устройства на другое, и обратно. Если *ping* не проходит, это может означать ошибку на любом из трех уровней. Поскольку маршрут на удаленную сторону PPP-соединения создается автоматически, то на третьем уровне ошибки маловероятны. (Если только они не привнесены искусственно, например, пакеты ICMP Echo запрещены фильтрами.) Таким образом, следующий шаг в отладке PPP-соединения состоит, как правило, в том, чтобы локализовать ошибку на первом либо втором уровне, а затем на некотором его подуровне.

Если *ping* между двумя устройствами проходит нормально, но *ping* на третье устройство или с третьего на четвертое, расположенные за ними по разные стороны соединения, не проходит, это означает проблемы с IP-маршрутизацией. Следует помнить, что автоматически создаются только маршруты в непосредственно подключенные сети (для данного случая — к удаленной стороне PPP-соединения). Маршруты в несмежные сети на всех устройствах должны быть заданы явным образом, либо в качестве маршрутов по умолчанию, либо с помощью протоколов динамической маршрутизации.

Б.7. Администрирование системы PPP-доступа

Б.7.1. Рестарт портов, станций и интерфейсов

Логическое соединение между портом типа ASYNC_PPP, SYNC_PPP и соответствующим IP-интерфейсом устанавливается в момент старта интерфейса. При этом предполагается, что порт уже сконфигурирован (и рестартован) с требуемыми параметрами. По этой причине настраивать и рестартовать их необходимо в строго определенной последовательности: сначала порт, затем IP-интерфейс.

При перезагрузке устройства в целом требуемая последовательность соблюдается автоматически, т.е. сначала стартуют порты, а затем — IP-маршрутизатор.

При рестарте IP-интерфейса (ручном, или по завершении PPP-соединения) автоматически рестартует и связанный с ним порт. В частности, для физического порта при этом опускается сигнал DTR и, соответственно, разрывается физическое соединение; после рестарта процедура установления соединения на всех уровнях выполняется с самого начала.

При ручном рестарте порта IP-интерфейс *не рестартует* и его привязка к порту не восстанавливается. Для восстановления работоспособности необходимо вслед за портом рестартовать также и IP-интерфейс. Это следует иметь в виду, в частности, если в процессе отладки порту был временно назначен тип ASYNC для прозрачного проключения на модем (см. п.Б.6.1).

Для всех остальных конфигураций, использующих динамическую привязку IP-интерфейса, рестарт одного из объектов приводит, в первую очередь, к разрыву этой связи. В частности, при рестарте интерфейса с TY:PPP PO:AUTO происходит, в зависимости от подключенного к нему объекта:

— Рестарт физического порта (с терминальной аутентификацией) и его возвращение к исходному типу ASYNC
— Освобождение соответствующего канала станции Ethernet типа PPP
— Разрыв логического соединения X.25 (как правило, влекущий за собой разрыв и физического соединения с клиентом)

При рестарте физического порта, порта Ethernet (и всех связанных с ним станций), а также при разрыве соединения X.25, все связанные с ними IP-интерфейсы освобождаются и рестартуют автоматически.

Рестарт портов, станций и IP-интерфейсов может выполняться с помощью любых средств управления, включая SNMP.

Б.7.2. Управление работой пользователей

Просмотреть список пользователей, подключенных к устройству в данный момент, можно с помощью команды Display System, например:

```
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
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 клиентов PPP в качестве используемого ресурса указывается имя IP-интерфейса, как старшего в протокольной иерархии (к тому же однозначно присутствующего во всех случаях PPP-доступа). Чтобы принудительно отключить клиента, следует рестартовать IP-интерфейс; соответствующий физический порт при этом рестартует автоматически. Рестарт может быть выполнен любыми средствами управления, включая SNMP.

При установлении PPP-соединения может быть задана его максимальная продолжительность, а также некоторые другие атрибуты (фильтры и т.п.) Подробнее об их назначении см. п.Б.3.9.

Б.8. Особенности настройки PPP-доступа для клиентов Windows

Б.8.1. Особенности Службы Удаленного Доступа

Компонента операционной системы, называемая на языке корпорации Майкрософт "Службой Удаленного доступа" или "Подключением к Интернету" (в зависимости от версии Windows), представляет собой комплексный объект для управления модемом, установления PPP-соединения на канальном и сетевом уровнях, и обеспечения работы сети Microsoft поверх установленного соединения. Настройка ее, в соответствии с общей логикой продуктов этой фирмы, предельно автоматизирована с тем, чтобы компьютер жил своей собственной жизнью и не обременял пользователя излишним пониманием происходящего. Поэтому процедура настройки PPP-клиента Windows нуждается в дополнительных пояснениях для сетевого администратора.

Установка модема и параметров телефонной сети. Принципиально важной компонентой является INF-файл модема, содержащий перевод команд и откликов конкретного модема на внутренний язык операционной системы. Он необходим, поскольку PPP-клиент ориентируется не на аппаратные сигналы интерфейса, а на текстовые сообщения модема (CONNECT, NO CARRIER и т.п.). Для большинства модемов можно ограничиться INF-файлом одного из "Стандартных Модемов", входящим в состав системы; однако для непосредственного соединения кросс-кабелем, а также для нестандартных модемов (с языком команд, сильно отличным от типового Hayes-совместимого) следует использовать только "родной" INF-файл.

В ходе установки, или при первой попытке сконфигурировать "Подключение Удаленного Доступа", операционная система требует ввести параметры телефонной сети в месте расположения данного ПК — код региона, режим набора номера (тон/пульс) и т.п., а при настройке соединений — коды страны/города для удаленного модема. Предполагается, что в дальнейшем система будет самостоятельно определять, находятся ли они в одном регионе или в разных, и выбирать префиксы для местного/междугородного/международного вызова. На практике этот механизм чрезмерно запутан и усложнен; гораздо проще отключить опцию "Использовать правила набора номера" (или включить "Force local call", в зависимости от версии) и вводить все номера вручную, например, 8w1234567890 (междугородный звонок), корректируя префиксы по мере надобности. Аналогичным образом, если эта трудноуправляемая система набирает номер в тоновом режиме вместо импульсного, то можно просто ввести номер в формате D1234567 (или наоборот).

Реальная скорость в порту, управление потоком и формат асинхронных данных во всех случаях устанавливаются в "Свойствах" Подключения Удаленного Доступа. Значения скорости, установленные в свойствах других системных объектов, к PPP-подключению не относятся.

Протокол PPP. Многоканальные соединения PPP (Muntilink PPP) и расширения протокола PPP (*callback* и др.) устройствами NSG не поддерживаются, поэтому на клиентской стороне их следует отключить.

Аутентификация. Имя и пароль при этом берутся из двух полей в основном окне PPP-клиента. На языке корпорации Майкрософт варианты аутентификации называются "Использовать Небезопасный Пароль" и "Использовать Безопасный Пароль". Первое означает, что PPP-клиент согласен аутентифицироваться по обширному списку протоколов, включая PAP и CHAP — в зависимости от того, что затребует удаленная сторона. Второй вариант разрешает использовать только протоколы, в которых пароль не передается в открытом виде, в т.ч. CHAP; если удаленная сторона предложит аутентификацию по PAP, Windows разорвет соединение.

Выбор производится с помощью опции или выпадающего меню на вкладке "Безопасность" или "Тип сервера", в зависимости от версии Windows. В современных версиях (XP/2000), помимо двух вышеуказанных вариантов, можно выбрать один или несколько протоколов аутентификации вручную с помощью кнопки "Дополнительные параметры". Применительно к соединению с устройствами NSG, интерес представляют только PAP и CHAP; другие (фирменные) протоколы и механизмы аутентификации не поддерживаются.

В старых версиях (95/98) пароль хранится отдельно от остальных параметров "Соединения Удаленного Доступа" — а именно, в настройках клиента сети (см. Панель Управления —> Сеть). Если никакой клиент сети не установлен, опция "сохранить пароль" в основном окне PPP-клиента недоступна. ("Щёлкни кобылу по носу — она махнет хвостом." © К. Прутков)

Аутентификация в терминальном режиме включается отдельно, местонахождение соответствующих опций зависит от версии. Для ручного ввода имени и пароля необходимо включить опцию "Открывать окно терминала после дозвона". Для использования сценария необходимо указать путь к файлу сценария. Подробнее о сценариях соединения см. п.Б.8.3.

Настройка TCP/IP. Выбор IP-адреса должен строго соответствовать настройкам IP-интерфейса NSG. Если со стороны NSG IP-адрес клиента задан параметром RADR или настройками аутентификации (в локальной таблице или на централизованном сервере), то на клиенте необходимо оставить опцию "IP-адрес назначается сервером". Если на устройстве NSG он не задан, то на клиенте необходимо установить статический IP-адрес (совместимый с адресом/маской интерфейса NSG). В любом другом случае соединение будет отвергнуто на этапе IPCP.

Аналогичным образом настраиваются адреса DNS. Если они установлены на устройстве NSG, то следует оставить опцию "Адреса DNS назначаются сервером", если нет — их необходимо статически определить на клиенте.

Сжатие IP-заголовков рекомендуется включить. Однако если есть подозрения, что этот механизм работает некорректно (особенно в старых версиях Windows), можно выключить его на обеих сторонах.

Сжатие PPP-трафика. Продукты компаний NSG и Майкрософт не поддерживают взаимно совместимых алгоритмов сжатия данных. По этой причине опцию "Сжатие данных" следует всегда выключать. В противном случае время установления PPP-соединения может резко возрасти.

IP-маршрутизация. Опция "Использовать основной шлюз в удаленной сети" в переводе на русский язык означает не что иное, как создать в Windows маршрут по умолчанию, проходящий через данный IP-интерфейс. Как правило, для клиента этот маршрут является единственным, поэтому данную опцию следует оставить включенной. В более сложных случаях маршрутизация настраивается вручную с помощью команды route (выполняется в режиме командной строки). В современных версиях можно также использовать так называемый "Слушатель RIP".

Прикладные службы. В первую очередь, это Клиент Сети Microsoft и сервер этой сети ("Служба доступа к файлам и принтерам"). В старых версиях при создании "Подключения Удаленного Доступа" они устанавливается по умолчанию. Если предполагается использовать данный ПК не в "растянутой" локальной сети, а только для работы IP-приложений (Интернет, электронная почта, корпоративные приложения, в т.ч. подключение банкоматов), эти службы следует удалить или отключить. Также следует отключить все остальные протоколы — NetBIOS, NetBEUI, SPX/IPX и т.п. — и опцию "Войти в сеть", которая в большинстве случаев приводит к 1-минутной задержке перед завершением подключения. О работе удаленного ПК в составе сети Microsoft см. следующий параграф.

Подробные пошаговые инструкции по кликанию мышкой в окошках для различных версий Windows можно найти на сайте компании http://www.nsg.ru, или на диске поддержки пользователей NSG, в разделе "Техническая поддержка" —> "FAQ".

ВНИМАНИЕ Пункты 1 и 2 указанных инструкций относятся исключительно к подключению ПК через нуль-модемный кабель. Для общего случая подключения через модем следует рассматривать только пункты 3–6; драйвер модема при этом устанавливается в соответствии с указаниями его изготовителя.

Б.8.2. Настройки для подключения к локальной сети Microsoft

Если удаленный ПК предназначается для работы в "растянутой" локальной сети Microsoft, то необходимо включить/установить службу "NetBIOS over TCP/IP" и клиента сети. Кроме того, в Windows XP для работы NetBIOS over TCP/IP должен быть включен "Брандмауэр/Общий доступ к Интернету", даже если никакая фильтрация трафика не требуется.

Если данный ПК должен работать в сети не только в качестве клиента, но и в качестве сервера, то необходимо установить также "Службу доступа к файлам и принтерам". В Windows XP необходимо также разрешить "Общий доступ к файлам и принтерам" — по умолчанию для PPP-соединений он запрещен.

На сервере доступа NSG необходимо настроить режим эмуляции моста с помощью ARP Proxy (см. Часть 4). Этого, однако, недостаточно для полноценной работы удаленного ПК в сети Microsoft; требуется, чтобы работал "Обозреватель Сети" — прикладная служба, которая обнаруживает другие компьютеры и показывает их в "Сетевом Окружении", а заодно оповещает их о существовании данного ПК. Он может использовать для этой цели два механизма.

По умолчанию, компьютеры сети Microsoft обнаруживают друг друга путем рассылки широковещательных пакетов. В этом случае для нормальной работы Обозревателя Сети необходимо настроить на устройстве NSG четыре фильтра для широковещательных пакетов — для пакетов с широковещательным адресом данной сети и для пакетов с адресом 255.255.255.255, например:

```
S P IP:1 TY:ETHI ET:0 IADR:192.168.1.1 MASK:255.255.255.0
S P IP:2 TY:PPP PO:1 IADR:192.168.1.254 MASK:255.255.255.255 SADR:192.168.1.1
S I ARP:1 IADR:192.168.2.254 PROXY
S I FILTER TY:S EN:YES IN:1 DA:192.168.1.255 OUT:2
S I FILTER TY:S EN:YES IN:2 DA:192.168.1.255 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
```

Такое решение имеет одно существенное ограничение — на устройстве NSG возможно организовать только одно соединение с эмуляцией локальной сети. Коммутация широковещательных пакетов с одного интерфейса на несколько запрещена. Кроме того, ретранслировать весь широковещательный трафик локальной сети в низкоскоростное модемное соединение — очевидно, не самый рациональный вариант.

Альтернативный вариант состоит в том, чтобы использовать службу WINS (Windows Naming Service) — функциональный аналог DNS. В этом случае "Обозреватель Сети" будет целенаправленно запрашивать информацию о составе сети у заданного сервера WINS, и через него же станет известен остальным ПК. В качестве сервера WINS можно указать любой ПК, расположенный в локальной сети. Именно такой вариант рекомендуется использовать для удаленных ПК, особенно в случае, когда несколько таких клиентов подключено к одному серверу доступа. Для более оперативной и корректной работы рекомендуется указать этот же сервер в настройках остальных компьютеров сети.

Вместо WINS можно использовать также традиционный сервер DNS, если он имеется в данной сети. В этом случае компьютеры сети не будут автоматически обнаруживаться, но к ним и к их разделяемым ресурсам можно обратиться по символьным именам, например, ввести в адресной строке "Проводника" (Explorer) или "Обозревателя" (Internet Explorer):

```
\\computer_name
\\computer_name\shared _directory\filename.ext
\\ИванИванович\Мои Документы\Квартальный отчет.doc
```

В любом случае, даже при отсутствии служб WINS и DNS, удаленный клиент может обратиться к компьютерам сети, зная их точные IP-адреса, например:

```
\\192.168.1.123\Мои Документы\Квартальный отчет.doc
```

Б.8.3. Сценарии доступа для аутентификации в терминальном режиме

Сценарий соединения исполняется "Подключением Удаленного Доступа" после того, как от модема получена заданная строка, означающая установление физического соединения. Сценарии подключаются:

— Для Win XP/2000 — в "Свойствах Подключения" на вкладке "Безопасность". Необходимо отметить опцию и ввести путь\имя для файла сценария (по умолчанию %windir%\system32\ras*.scp).

— Для Win ME/98/95OSR2 — в "Свойствах Подключения" на вкладке "Сценарии". Необходимо ввести путь\имя для файла сценария (по умолчанию %ProgramFiles%\Accessories*.scp). Сам факт наличия записи на данной странице означает, что следует использовать сценарий; если окно "Имя файла сценария" пустое, это означает, что никакой сценарий не используется.

— Для Win 95 1st release используется отдельное приложение Dial-Up Scripting Tool, вызываемое из меню "Пуск" —> "Аксессуары". В окне данного приложения необходимо выбрать название "Подключения Удаленного Доступа", к которому следует применить сценарий, и путь\имя для файла сценария.

Сопутствующая опция "Минимизировать окно терминала после открытия" во всех этих окнах скрывает работу сценария от пользователя. Для отладочных целей целесообразно, наоборот, отключить ее, чтобы наблюдать ход исполнения сценария.

Язык сценариев Windows (за исключением Win 95 1st release) весьма богат и позволяет описывать разветвленные терминальные процедуры. При этом имя и пароль могут быть как записаны в теле сценария в явном виде, так и получены из основного окна PPP-клиента через переменные $USERID, $PASSWORD. Для практических целей, однако, достаточно ограничиться всего несколькими основными командами. Примеры сценариев приведены ниже.

Простой сценарий с явным вводом имени и пароля. Предполагается, что аутентификация производится с помощью централизованного сервера RADIUS/TACACS+, поэтому имя пользователя посылается устройству NSG в неизменном виде.

```
proc main
    waitfor "ogin: "
    transmit "basile"
    transmit "^M"
    waitfor "assword: "
    transmit "poUpkINe"
    transmit "^M"
endproc
```

Сценарий с получением имени и пароля из основного окна PPP-клиента. Предполагается, что аутентификация производится по локальной таблице, поэтому к имени пользователя добавляется суффикс .ppp. (Вместо этого можно было бы также вводить имя в виде username.ppp непосредственно в основном окне.)

```
proc main
    waitfor "ogin: "
    transmit $USERID
    transmit ".ppp"
    transmit "^M"
    waitfor "assword: "
    transmit $PASSWORD
    transmit "^M"
endproc
```

Сценарий с раздельным хранением имени и пароля. Такой сценарий особенно удобен для систем Win ME/98/95, если на них не установлен никакой клиент сети и поэтому возможность сохранения пароля штатными средствами отсутствует. Предлагаемое решение хранит имя пользователя и пароль порознь: имя — в системном реестре, пароль — в текстовом файле. Файл сценария следует поместить в место, отличное от стандартного (см. выше), дать ему какое-нибудь непримечательное имя, которое не будет служить подсказкой для злоумышленника, и изменить стандартное расширение .scp на какое-нибудь другое. Как показывает практика, именно такой вариант оказывается наименее уязвимым.

```
proc main
    waitfor "ogin: "
    transmit $USERID
    transmit "^M"
    waitfor "assword: "
    transmit "poUpkINe"
    transmit "^M"
endproc
```

Удаление ненужных процессов, особенно сетевых, повышает скорость и устойчивость работы системы, а также улучшает ее безопасность. Более того, при штатном варианте хранения пароля он, наряду с именем пользователя, записывается в системный реестр Windows — в место, хорошо известное хакерам; столь же общеизвестны утилиты для его извлечения и расшифровки. Таким образом, злоумышленнику, проникшему на машину, не составляет труда скопировать к себе известные файлы реестра и извлечь из них реквизиты пользователя.

Сценарий для соединения через сеть X.25. Предполагается, что ПК устанавливает модемное соединение с некоторым абстрактным PAD-ом, позволяющим войти в сеть X.25. После этого необходимо в ответ на приглашение PAD (звездочку) ввести X.121 адрес устройства NSG, предоставляющего услуги PPP клиентам этой сети. После соединения с ним начинается обычная процедура LCP и аутентификация по PAP/CHAP.

```
proc main
    transmit "^M"
    waitfor "*"
    transmit 777666100
    transmit "^M"
    waitfor "COM"
endproc
```

Более сложные примеры сценариев можно найти на сайте компании http://www.nsg.ru, или на диске поддержки пользователей NSG, в разделе "Техническая поддержка" —> "FAQ".

Полное описание языка сценариев для PPP-клиента Windows содержится в документе корпорации Майкрософт: "*Язык макросов подключения для редактора макросов подключения*", который можно найти на ее Web-сайте или в Интернет.

Б.8.4. Особенности настройки нуль-модемного соединения

INF-файл. Основная проблема состоит с том, что процедура LCP в Windows (или эмулятор терминала для аутентификации в терминальном режиме) стартует не по поднятию аппаратного сигнала DCD, а по получении заданного текстового сообщения от модема. Поскольку в данном случае модем отсутствует, приходится использовать специальные способы, чтобы запустить эту процедуру.

В силу этой особенности, *необходимо* использовать настроечный файл MDMNSG.INF (либо аналогичный настроечный файл нуль-модема от другого производителя сетевого оборудования). Основная особенность этого файла — в нем записано, на языке Windows, что сигналом об установлении соединения следует считать любой один символ, полученный из порта. Кроме того, в нем установлены соответствующие двоичные ключи, позволяющие показывать его в списке доступных модемов при создании PPP-соединения. Данный файл можно найти на сайте компании http://www.nsg.ru, или на диске поддержки пользователей NSG, в разделе "Техническая поддержка" —> "Драйверы и MIB".

На устройстве NSG необходимо установить следующие параметры IP-интерфейса:

```
SL:NO DOD:NO
```

В этом случае интерфейс будет непрерывно посылать в линию запросы LCP. Как только на ПК будет запущено "Подключение удаленного доступа", первый принятый байт будет означать успешное физическое соединение, и Windows инициирует процедуру LCP на своей стороне.

ПРИМЕЧАНИЕ При данном способе подключения возможна задержка на 1–2 секунды. Такая задержка является нормальной. Она вызвана тем, что IP-интерфейс после 10 попыток рестартует и делает паузу на 2 сек перед следующей попыткой.

"Родной" .INF-файл нуль-модемного соединения, входящий в состав Windows, предназначен для совершенно иной цели — для объединения двух ПК в мини-сеть по последовательному кабелю. Протокол такого соединения является фирменным для продукции Microsoft и начинается с обмена сообщениями CLIENT, SERVER или CLIENTSERVER — которых, естественно, не следует ожидать от сервера PPP-доступа. Именно поэтому, а не по недосмотру разработчиков, оно не показывается в списке модемов.

Сказанное относится также к любой аппаратуре передачи данных, эмулирующей прозрачное нуль-модемное соединение. К сожалению, имеются примеры тому, как иногда производители таких устройств поставляют, по существу, немного модифицированный .INF-файл от Windows, в котором всего лишь разрешено показывать это соединение в списке модемов. Для организации PPP-соединений такой файл непригоден.

Параметры асинхронного порта. При установлении нуль-модемного соединения ПК под управлением Windows с устройством NSG следует использовать следующие параметры порта:

Формат асинхронных данных — 8n1
Управление потоком — аппаратное
Скорость — в соответствии со скоростью, установленной в порту устройства NSG

Значения данных параметров устанавливаются в окне "Свойства модема" или аналогичном (в зависимости от версии Windows), доступном через "Свойства" PPP-клиента. Значения, установленные в других окнах Windows, к работе PPP-клиента не относятся.

Набираемый номер. Поскольку нуль-модемное PPP-соединение в Windows не предусмотрено, система бдительно следит за тем, чтобы пользователь не создал "Подключение Удаленного Доступа" с пустым телефонным номером. Чтобы создать требуемое соединение, следует ввести в поле "номер телефона" произвольный фиктивный номер, например, единицу или запятую.

Подробные пошаговые инструкции по кликанию мышкой в окошках для различных версий Windows можно найти на сайте компании http://www.nsg.ru, или на диске поддержки пользователей NSG, в разделе "Техническая поддержка" —> "FAQ".

Б.8.5. Особенности настройки доступа PPPoE для Windows XP

Встроенный клиент PPPoE версии Windows XP нормально работает с сервером PPPoE NSG, при условии, что Ethernet-станции типа PPP назначено любое непустое имя:

```
S P ET:n PO:m TY:PPP NAME:"XXX"
```

Процедура создания "Подключения Удаленного Доступа" выполняется с помощью "Мастера Новых Подключений". Для создания PPPoE-соединения нужно последовательно выбрать опции:

- "Подключить к Интернету"
  - "Установить подключение вручную"
    - "Через высокоскоростное подключение, запрашивающее имя пользователя и пароль"

Остальные шаги одинаковы для асинхронных и PPPoE-соединений.

ПРИМЕЧАНИЕ "Имя службы", фигурирующее в свойствах PPPoE-соединения, никакого отношения к имени Ethernet-станции NSG не имеет.

Б.8.6. Просмотр состояния и статистики PPP-соединений в Windows.

Для мониторинга PPP-соединений в системе Windows можно использовать следующие инструменты.

Окно состояния соединения. После того, как PPP-соединение установлено, его состояние можно проконтролировать с помощью пункта "Состояние" контекстного меню. (Вызывается щелчком правой кнопкой, либо двойным щелчком левой, по иконке данного соединения в системной панели.) В окне "Состояние соединения" выводится количество переданных и принятых данных, время соединения, а также:

— Для старых версий Windows — кнопка "Дополнительно". При нажатии открывается дополнительное поле, содержащее список всех протоколов, относящихся к данному PPP-соединения. В частности, таким образом можно проверить, какой протокол аутентификации был фактически использован при установлении соединения.

— Для современных версий — вторая вкладка под названием "Сведения". На ней отображаются все технические детали данного соединения, в том числе протокол аутентификации, IP-адреса клиента и удаленного сервера, и т.п.

Утилита *winipcfg*. Присутствует в старых версиях Windows (до ME включительно). Выводит параметры IP любого интерфейса, включая интерфейсы PPP; работает в оконном режиме. Для вызова программы следует набрать winipcfg.exe в окне "Пуск" —> "Выполнить"; после этого в окне программы следует выбрать интересующий интерфейс и, при необходимости, нажать кнопку "Дополнительно".

Утилита *ipconfig*. Присутствует в ветви Windows NT (NT4.0, 2000, XP), а также в ME. Аналогична *ipconfig*, но выполняется в режиме командной строки. Пример вызова данной утилиты для просмотра параметров всех IP-интерфейсов из окна "Пуск" —> "Выполнить":

```
command.com /k ipconfig.exe /all | more.com
```

Примеры использования утилит *winipcfg* и *ipconfig* для различных версий Windows можно найти на сайте компании http://www.nsg.ru, или на диске поддержки пользователей NSG, в разделе "Техническая поддержка" —> "FAQ" (пункт 6 всех примеров по PPP для Windows).

Б.8.7. Характерные проблемы и их устранение

Следующие проблемы являются специфическими для клиентов Windows. (В дополнение к общим ошибкам, вероятным при настройке PPP-соединения.)

Длительная (около 1 минуты) задержка после аутентификации. На ПК выводится сообщение "Регистрация в сети" или "Вход в сеть". В подавляющем большинстве случает причиной является неотключенная опция "Вход в сеть" (в старых версиях Windows) или опция "Сжатие данных". Следует отключить обе эти опции.

При этом соединение де-факто готово к передаче IP-трафика уже с момента появления вышеуказанного сообщения. Попытка запустить сетевого клиента или согласовать сжатие продолжается параллельно с передачей трафика других приложений и служб, и не является помехой для них.

Не устанавливается соединение PPPoE в WinXP. После длительного ожидания на этапе "Набор номера…" подключение завершается с ошибкой 678 "Удаленный компьютер не отвечает." Причина — используемая Ethernet-станция типа PPP имеет пустое имя. Следует назначить ей произвольное непустое имя.

Б.9. Особенности настройки PPP-доступа по сетям GSM/GPRS и CDMA

Б.9.1. Выбор услуг сети GSM: CSD vs. GPRS

Для передачи данных по сети GSM могут использоваться два принципиально разных принципа: канальный (Channel Separated Data, CSD) и пакетный, из реализаций которого наиболее распространен General Packet Radio Service — GPRS. Интерфейсный модуль IM–GPRS поддерживает оба эти режима.

Для режима CSD характерны следующие особенности:

— Соединение постоянно занимает один канал сети GSM, точно так же как голосовое или факсимильное соединение. По этой причине тарификация производится, как правило, на повременной основе.

— Скорость передачи данных является постоянной и гарантированной (если только не ухудшается качество принимаемого радиосигнала). Канал для CSD-соединения предоставляется сетью на равных условиях с голосовыми соединениями.

— Скорость одинакова в обоих направлениях.

— Максимальная скорость составляет, как правило, 9600 бит/с. Это значение является предельным, если на другой стороне GSM-сети звонок проходит через обычную аналоговую телефонную сеть.

— Для звонков, проходящих исключительно по цифровым каналам (внутри сети GSM, между двумя сетями GSM, между сетями GSM и ISDN) рекомендуется использовать протокол V.110. Данный протокол позволяет повысить скорость до 14400 бит/с, при условии, что эта скорость поддерживается сетью; однако даже если она не поддерживается, протокол V.110 имеет определенные преимущества, в частности, по скорости установления соединения. При использовании данного протокола он должен быть включен на обеих сторонах соединения (для IM–GPRS см. команду AT+CBST).

— Канал CSD через сотовую сеть может работать в двух режимах: прозрачном и непрозрачном. Выбор предпочтительного режима (в частности, с точки зрения быстрого установления соединения) зависит от конкретной сети; управление этими режимами в модуле IM–GPRS также осуществляется командой AT+CBST.

— Соединения устанавливаются по схеме "точка-точка" между двумя модемами. В частности, удаленной стороной может быть другой GSM-модем, модем, расположенный в проводной телефонной сети, сервер доступа в Интернет самого GSM-оператора, сервер доступа стороннего поставщика услуг IP или X.25, сервер корпоративной сети.

— Соединение может устанавливаться по инициативе любой стороны. Однако для приема входящих звонков на GSM-модем требуется установить для данного телефонного номера тип звонка "данные". Эта конфигурация относится не к модему, к самой сети GSM и выполняется оператором. Для смены типа звонка следует обратиться в абонентскую службу оператора, или сразу заказать нужный тип при покупке новой SIM-карты. Автоматическое определение типа входящего звонка (голос/факс/данные) отечественными операторами на практике не поддерживается.

— С протокольной точки зрения, CSD-соединение ничем не отличается от обычного соединения между проводными модемами, и поверх него могут работать любые асинхронные протоколы: PPP, SLIP, PAD (X.28) и прозрачная передача произвольного асинхронного трафика. Никакие особые ограничения и настройки для этих протоколов (например, фильтрация трафика или выбор сетевых адресов) не накладываются.

— Ввиду высокой повременной оплаты, для CSD-соединений особенно актуальны развитые механизмы установления и разрыва соединений — сценарии, *keepalive* и т.п.

Соединения GPRS, в свою очередь, отличаются следующими особенностями:

— Данные передаются в свободных слотах на разовой основе. Таким образом, постоянное соединение на физическом уровне, по существу, отсутствует. Технология GPRS лишь эмулирует такое соединение, организуя систематический обмен одиночными пакетами. В силу именно этой особенности, а не маркетинговых решений, тарификация GPRS-услуг возможна только по трафику.

— Фактическая скорость передачи данных является величиной переменной и варьируется между значениями (0…N)×9600 бит/с либо (0…N)×14400 бит/с, в зависимости от настроек сети. Здесь N — максимальное число слотов, поддерживаемое данным терминалом и разрешенное данным оператором.

— Скорость передачи данных в восходящем (от пользователя в сеть) и нисходящем (из сети к пользователю) направлениях устанавливается независимым и, как правило, асимметричным образом. В частности, модуль IM–GPRS поддерживает до 4 нисходящих и до 2 восходящих слотов, при общем числе слотов не более 5.

— Услуга гарантированной минимальной скорости на практике, как правило, не предоставляется. Слоты для трафика GPRS предоставляются сетью по остаточному принципу, после канальных соединений и необходимой нормы резервирования свободных каналов. Если базовая станция сильно нагружена, то свободных слотов для GPRS не остается вообще, и фактическая скорость передачи пакетных данных падает до нуля — при том, что соединение номинально сохраняется.

Предоставление гарантированной минимальной скорости для GPRS теоретически возможно, однако по существу это означает не больше и не меньше, чем постоянное резервирование одного или нескольких каналов за данным пользователем. Именно по этой причине такая услуга, если бы она и поддерживалась, была бы чрезвычайно дорогой и неконкурентоспособной. Также не поддерживаются на практике две другие аналогичные услуги GPRS — запрашиваемая максимальная скорость соединения и гарантированная доставка данных.

— Соединения устанавливаются по схеме "точка-многоточка" между абонентами сотовой сети и так называемым узлом доступа (Access Point Node, APN). Как следствие, по GPRS-соединению могут работать только те протоколы и протокольные стеки, которые поддерживаются данным APN. Фактически механизм GPRS целиком формирует соединение третьего уровня между клиентом сети передачи данных и сетью определенного типа (IP, IPX, X.25). На практике это исключительно IP-over-PPP; все остальные варианты, такие как IPX-over-PPP или PAD, существуют, в основном, на бумаге.

— Сетевые адреса, режимы сжатия заголовков пакетов и данных на практике назначаются оператором.

— Соединения устанавливаются по инициативе пользователя.

— Ввиду отсутствия гарантированного качества услуги, особую важность имеют механизмы контроля соединения — применительно к PPP это LCP Echo. Однако сами по себе эти механизмы также поддерживаются далеко не все сотовыми операторами. Механизмы принудительного разрыва соединения, напротив, для GPRS не актуальны, поскольку соединение может существовать постоянно без повременной оплаты.

— Применительно к единственной услуге IP-over-PPP конкретными сотовыми операторами могут накладываться дополнительные протокольные ограничения, в частности:
  — IP-адреса назначаются оператором, как правило, динамически. Статические адреса поддерживаются не всеми операторами, или оплачиваются по отдельному тарифу.
  — Сеть GPRS может назначать пользователям IP-адреса из приватного диапазона, а на выходе в Интернет выполнять трансляцию адресов. Таким образом, на пользовательский трафик накладываются все ограничения, связанные с сутью механизма NAT и его конкретной реализацией.
  — Передача отдельных видов трафика (например, VPN) может быть запрещена фильтрами или просто не реализована в сети оператора.

Б.9.2. Инициализация модуля IM–GPRS, IM–CDMA и регистрация в сети

С программной точки зрения, модуль IM–GPRS или IM–CDMA конфигурируется как интерфейс V.24 и далее управляется с помощью сценариев, аналогично внешнему модему. Язык AT-команд для модуля IM–GPRS описан в документе компании Компэл:

Руководство по AT-командам. Описание AT команд для работы с модулями и модемами компании Wavecom.

Краткий список основных команд и примеры сценариев приведены в документах NSG:

Управление модулем IM–GPRS с помощью AT-команд
Управление модулем IM–CDMA с помощью AT-команд

Указанные документы доступны на Web-сайте NSG http://www.nsg.ru, или на диске поддержки пользователей NSG, в разделе "Документация" —> "Руководства пользователя".

Специфика сотовых соединений вообще и модулей IM–GPRS, IM–CDMA в частности заключается в следующем:

— Модуль IM–GPRS, как и большинство модемов, автоматически устанавливает в своем асинхронном порту такую же скорость, как и в порту устройства NSG, к которому он подключен. Для модуля IM–CDMA, напротив, скорость в асинхронном порту устанавливается вручную следующей командой:

```
AT+IPR=bbbb <Enter>
```

где bbbb — скорость в бит/с. После этого необходимо перенастроить порт устройства NSG на работу с новой скоростью.
По умолчанию, оба модуля сконфигурированы для работы на скорости 115200 бит/с.

— При включении питания или рестарте модуля требуется определенное время (порядка нескольких секунд) для его загрузки. Если в это время интерфейс будет посылать в модуль какие-либо команды, модуль будет возвращать сообщения об ошибках, сценарий аварийно завершится, и интерфейс рестартует. Как правило, при этом производится также аппаратный рестарт модуля (выключение/включение питания), и процесс повторяется снова. Чтобы избежать зацикливания, рекомендуется установить в начале сценария принудительную задержку, например:

```
A X SCRIPT:1 TIMEOUT 10 "XXX–AT–OK" AT&F …
```

— При некоторых некорректных ситуациях в сети, в частности, при падении фактической скорости до нуля в процессе установления GPRS-соединения, модуль может впадать в нештатное состояние, из которого его можно вывести только аппаратным рестартом. Для этого предусмотрен следующий механизм: если

установление PPP-соединения оканчивается неудачей, IP-интерфейс рестартует обычным образом, при этом рестратует также и физический порт, падает сигнал DTR в порту, и по этому сигналу может производиться аппаратный рестарт модуля. Рекомендуется использовать эту возможность в сетях GPRS, особенно при неустойчивой работе. Выбор дополнительной реакции модуля IM–GPRS на падение сигнала DTR и связанные с этим различия в его аппаратных модификациях описаны во втором из вышеприведенных документов; в модуле IM–CDMA аппаратный рестарт происходит всегда, за исключением отдельных экземпляров из первой опытной партии.

— При передаче данных в режиме GSM CSD, напротив, рекомендуется отключить аппаратный рестарт модуля по падению DTR и не вводить принудительную задержку в начале сценария. Это позволит ускорить установление соединения.

— Если для регистрации в сети GSM требуется PIN-код, он вводится командой AT+CPIN=nnnn. Текущий статус модуля запрашивается командой AT+CPIN?. Для модуля IM–CDMA аналогичная команда имеет синтаксис AT+RLOCK=1,nnnn; единожды введенный правильный PIN запоминается в энергонезависимой памяти модуля, и при последующих включениях не запрашивается.

— По умолчанию, модуль IM–GPRS сконфигурирован как GSM-терминал класса B, т.е. с поддержкой одновременно CSD- и GPRS-соединений. В этом случае он при старте автоматически регистрируется в сети как пользователь канальных услуг (см. команду AT+CREG?). Для подключения к услуге GPRS необходимо использовать дополнительно команду AT+CGATT=1. При необходимости можно также изменить статус терминала на CC (только режим CSD) или CG (только режим GPRS) — см. команду AT+CGCLASS=xx. Возможно также переопределить список услуг, к которым терминал подключается автоматически — см. команду AT+WGPRS.

— Команды AT+CREG=1 и AT+CGREG=1 не подключают те или иные услуги GSM, как можно было бы предположить, а только устанавливают определенный режим и формат вывода сообщений о смене статуса услуг.

— В языке AT-команд и ответов на них широко используются символы, требующие особых правил ввода в теле сценария: пробел, кавычки, двоеточие, вопросительный знак.

— Процедуры подключения к услугам сотовой сети и установления соединения выполняются в строго определенной последовательности; если некоторая команда не выполнена или не завершена, результаты выполнения всех последующих команд оказываются непредсказуемыми.

Часть настроек сохраняется в энергонезависимой памяти модуля. По опыту практических инсталляций, можно рекомендовать максимально использовать эту возможность, а сценарий установления PPP-соединения упростить до минимума. Для этого необходимо предварительно подключиться к модулю в прозрачном режиме (с помощью Reverse Telnet или PVC между двумя асинхронными портами) и ввести необходимые AT-команды вручную. В наиболее важных частных случаях настройки выглядят следующим образом:

Модуль IM–GPRS, подключение в режиме GPRS:

AT+CPIN=nnnn	— ввод PIN-кода
AT+CLCK="SC",0,nnnn	— отключение PIN-кода
AT+CGCLASS="CG"	— выбор класса терминала CG
AT+CGDCONT=1,"IP","internet.operator.ru"	— запись контекста GPRS

Сценарий установления соединения:

```
A X SCRIPT:1 "" "AT" "OK" "ATD*99***1#" "CONNECT" ""
```

Ввод вызываемого номера в полной форме, т.е. с номером используемого контекста (***1) в данном случае необходим, чтобы автоматически активировать данный контекст; в проивном случае для этого пришлось бы использовать дополнительно команду AT+CGACT=1.

Модуль IM–GPRS, подключение в режиме CSD:

AT+CPIN=nnnn	— ввод PIN-кода
AT+CLCK="SC",0,nnnn	— отключение PIN-кода
AT+CGCLASS="CC"	— выбор класса терминала CC

Сценарий установления соединения:

```
A X SCRIPT:1 "" AT OK AT+CBST=71,0,x OK ATD8ccccnnnnnnn TIMEOUT 55 CONNECT ""
```

В данном случае принудительно устанавливается протокол V.110, обеспечивающий, помимо прочих достоинств, быстрое установление соединения. Последний параметр в команде AT+CBST определяет режим передачи данных в сотовой сети и подбирается экспериментально в зависимости от особенностей настройки конкретной сети (в частности, по критерию скорейшего установления соединения).

Модуль IM–CDMA:

AT+RLOCK=1,nnnn — ввод PIN-кода для данной и последующих сессий

Сценарий установления соединения:

```
A X SCRIPT:1 TIMEOUT 20 XXX–AT–OK ATD#777 CONNECT ""
```

Во всех трех случаях запрос PIN-кода для данной SIM- или R-UIM карты можно также отключить с помощью обычного сотового телефона GSM или CDMA 450, соответственно.

Б.9.3. Аутентификация в сети GSM/GPRS

Абонентский терминал сотовой сети (телефон, модем) однозначно идентифицируется номером вставленной в него SIM- или R-UIM карты (или номером, жестко прописанным в самом устройстве), поэтому дополнительная аутентификация при подключении к IP-сети оператора является, в общем случае, излишней. По этой причине аутентификация клиентов PPP в сетях сотовых операторов, как правило, либо отключена, либо является формальной: в качестве имени и пароля указывается имя оператора. Для аутентификации в сетях GSM/GPRS обычно используется протокол PAP, в сети CDMA SkyLink — CHAP. Точная информация об используемых реквизитах предоставляется, естественно, самим сотовым оператором.

На практике также имеют место ситуации, когда аутентификация включена, но не настроена. В этом случае следует включить аутентификацию на устройстве NSG (PAPA:YES или CHAPA:YES) с произвольным, или пустым, именем и паролем.

ПРИМЕЧАНИЕ Вышесказанное относится только к услугам доступа в сети передачи данных, предоставляемые самим сотовым оператором. Для соединений CSD между двумя сотовыми модемами по схеме "точка-точка" аутентификация настраивается обычным образом в соответствии с политикой безопасности, принятой в данной корпоративной сети.