



Мультипротокольные маршрутизаторы и коммутаторы пакетов NPS–7e, NSG–500, NX–300, NSG–800 (Базовое программное обеспечение)

Руководство пользователя

Часть 5 Приложения и службы IP

Версия программного обеспечения 8.2.4

Обновлено 14.01.2011

АННОТАЦИЯ

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

Данное руководство состоит из следующих разделов:

- Часть 1. Введение в архитектуру маршрутизаторов NSG
- Часть 2. Общесистемная конфигурация
- Часть 3. Настройка физических соединений
- Часть 4. IP-маршрутизация
- Часть 5. Приложения и службы IP
- Часть 6. Службы Frame Relay и прозрачная передача трафика
- Часть 7. Коммутация и службы X.25
- Часть 8. Аутентификация, авторизация и статистика
- Часть 9. Список команд
- Приложение А. Примеры конфигурации
- Приложение Б. Настройка асинхронного доступа по протоколу PPP

Пятая часть руководства посвящена настройке приложений и служб, использующих сеть IP в качестве транспортной среды. К ним относятся службы Telnet и X.25-over-TCP/IP (ХОТ), предназначенные для передачи пользовательских данных, а также SNMP- и Web-управление. Для работы этих служб необходима предварительная конфигурация IP-транспорта, описанная в частях 3 и 4.

Использование мультипротокольных служб, обеспечивающих передачу трафика X.25 по сети IP (шлюз Telnet/PAD, ХОТ), предполагает также знакомство с конфигурацией подсистемы X.25, описанной в части 7.

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" 2003–2011

Логотип NSG является зарегистрированной торговой маркой ООО "Эн-Эс-Джи"

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

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

§ СОДЕРЖАНИЕ §

Часть 5. Приложения и службы IP

§5.1. Сервер Telnet	4
§5.1.1. Структура сервера Telnet	4
§5.1.2. Удаленное управление по Telnet	4
§5.1.3. Асинхронные Telnet-станции и Reverse Telnet	5
§5.1.4. Telnet-станции PAD	5
§5.1.5. Статистика Telnet-станций	5
§5.2. Клиент Telnet	6
§5.2.1. Вызов клиента Telnet	6
§5.2.2. Команды клиента Telnet	7
§5.2.3. Вызов клиента Telnet с низкоинтеллектуальных терминалов	7
§5.2.4. Ручной вызов клиента Telnet	8
§5.3. Инкапсуляция X.25-over-TCP/IP (ХОТ)	9
§5.4. SNMP-управление	11
§5.4.1. Настройка агента SNMP	11
§5.4.2. База MIB	12
§5.4.3. Системные ловушки (Traps)	13
§5.4.4. Перезагрузка устройства и рестарт его компонент	14
§5.4.5. Управление сеансами работы пользователей	16
§5.4.6. Управление модулями IM-DIO	17
§5.5. Web-управление	19
§5.5.1. Сервер HTTP	19
§5.5.2. Запуск и остановка сервера HTTP	20
§5.5.3. Вход в систему	20
§5.5.4. Структура Web-интерфейса	20
§5.5.5. Управление объектами конфигурации	21
§5.5.6. Ручной ввод команд	23
§5.5.7. Побочные эффекты Web-управления	23
§5.6. Клиент SNMP	24
§5.7. Клиент TFTP	25

§5.1. Сервер Telnet

§5.1.1. Структура сервера Telnet

Сервер Telnet представляет собой совокупность станций, каждая из которых может обслуживать одного клиента. Станции могут быть двух типов: ASYNC и PAD, и эквивалентны, соответственно, физическим портам этих типов. Число станций фиксировано и зависит от модели устройства и версии программного обеспечения. Telnet-станции нумеруются от 0 до максимального значения (специфического для данной модели устройства и версии программного обеспечения). Для неиспользуемых станций следует установить тип NOCONF.

Команда Set Parameters для установки параметров станции Telnet имеет следующий вид:

```
S P TN:<номер> TY:<тип> TCPPOORT:<номер_порта> IAC:<режим>
```

По умолчанию, все станции Telnet принимают входящие соединения по стандартному порту TCP 23. Номер порта для каждой станции или группы станций может быть установлен параметром TCPPOORT. Таким образом, при соответствующей конфигурации сервера удаленный пользователь Telnet имеет возможность обратиться к конкретной станции, к станции конкретного типа, или к станции из некоторой группы. Если один порт слушают одновременно несколько станций, то соединение устанавливается с первой свободной из них.

Параметр IAC (Interprete As Command) устанавливает профиль станции:

```
IAC:YES      Станция распознает и обрабатывает команды Telnet (по умолчанию).
IAC:NO      Станция передает все данные прозрачным образом.
```

Помимо указанных параметров, для станции Telnet устанавливаются все те же параметры, что и для физического порта того же типа (см. [Часть 6](#), [Часть 7](#)).

Для просмотра параметров заданной станции Telnet или всех станций используется команда Display Parameters:

```
D P TN:<номер>
D P TN:A
```

Для просмотра статистики работы станции Telnet и сброса этой статистики используются команды Display Status/Statistics и Clear Status/Statistics:

```
D S TN:<номер>
C S TN:<номер>
```

§5.1.2. Удаленное управление по Telnet

Для удалённого досупа к устройству по Telnet необходимо сконфигурировать одну Telnet-станцию как PAD на порту TCP 23. Традиционно для этого использовалась станция TN:0, но в данной версии такая заводская настройка исключена по соображениям безопасности:

```
S P TN:0 TY:PAD TCPPOORT:23 IAC:YES
```

После старта IP-маршрутизатора при обращении по Telnet пользователь соединяется с этой станцией и далее может выполнять все операции, допускаемые физическим портом типа PAD — в первую очередь, осуществлять удаленное управление устройством. Для соединения с модулем Manager необходимо в ответ на приглашение PAD (звездочку) набрать MN. Пароль для входа по Telnet — тот же, что и для консольного порта. Дальнейшая работа полностью эквивалентна локальному управлению через консольный порт.

ВНИМАНИЕ Выполнение команды Factory Settings приводит к удалению всех пользовательских настроек, в том числе IP-адресов, других параметров конфигурации IP-интерфейсов и портов. В результате после следующей перезагрузки системы, рестарта IP-маршрутизатора, используемого IP-интерфейса или порта устройство становится недоступным для удаленного управления и доступ к нему может быть получен только локально через консольный порт.

§5.1.3. Асинхронные Telnet-станции и Reverse Telnet

Чтобы через сеть IP получить доступ к некоторому асинхронному порту устройства NSG (т.н. Reverse Telnet), необходимо сконфигурировать одну из Telnet-станций по типу ASYNC и скоммутировать ее с нужным портом при помощи PVC. Как правило, станции назначается индивидуальный номер порта TCP, чтобы можно было обратиться именно к этой станции и получить доступ именно к этому порту. Пример конфигурации:

```
S P TN:2 TY:ASYNC TCPPORT:2003
A P PO:TN.2 PO:3
W S TN:2
W S PO:3
```

Telnet-станция типа ASYNC также может быть скоммутирована со станцией Frame Relay того же типа. В этом случае асинхронный трафик, поступающий через сеть IP, передается далее по виртуальному каналу сети Frame Relay. Подробно об использовании PVC см. [Часть 6](#).

Помимо указанных, для станции Telnet типа ASYNC действительны все те же параметры, что и для физического порта типа ASYNC (кроме типа и скорости интерфейса, а также формата асинхронных данных). В частности, станция может иметь параметр AU, указывающий на один из способов аутентификации. Однако в результате аутентификации и авторизации пользователя Telnet-станция может динамически принимать единственный тип PAD. Если служба авторизации предписывает дальнейшую работу станции в режиме PPP, пользователю будет выдано сообщение об ошибке.

Telnet-станции типа ASYNC поддерживают также трансляцию сигналов DCD/DTR асинхронного интерфейса (параметр ST). Аналогом сигнала DCD в данном случае является наличие Telnet-соединения со стороны сети IP, а аналогом сигнала DTR — готовность станции к установлению соединения. Подробно о трансляции сигналов интерфейса см. [Часть 6](#).

§5.1.4. Telnet-станции PAD

Telnet-станция типа PAD извлекает пользовательские данные из пакетов Telnet и преобразует их в пакеты X.25. Такая станция принимает входящие соединения из сети IP и обеспечивает удаленным клиентам Telnet доступ в сеть X.25. С точки зрения сети X.25 станция представляет собой обычный PAD.

Помимо общих параметров Telnet-станции (см. §5.1.1), для станции типа PAD должны быть настроены все параметры канального уровня, присущие портам типа PAD (см. [Часть 7](#)), за исключением формата асинхронных данных (параметр AF) и сценария инициализации модема (MS). При этом аналогом сигнала DCD физического порта является факт наличия Telnet-соединения с данной станцией со стороны IP-сети, а аналогом сигнала DTR — готовность станции к работе в IP-сети. Например, при CD:YES станция будет разрывать соединение X.25, если удаленный клиент Telnet отключился от нее. При CO:T, если разорвано соединение X.25, станция разорвет Telnet-соединение и будет готова устанавливать новое соединение через 2 сек. (Настройка CO:YES в данном случае не имеет смысла, поскольку в этом случае станция будет постоянно недоступна со стороны IP-сети.)

Telnet-станция типа PAD может быть скоммутирована с другими объектами сети X.25 одним из двух способов:

- Статически при помощи PVC. Клиент Telnet, подключившийся к такой станции, немедленно оказывается в состоянии соединения (ENGAGED) с удаленным объектом X.25 и может обмениваться данными с ним.
- Динамически при помощи SVC. После соединения со станцией удаленный пользователь Telnet получает приглашение PAD (звездочку) и находится в командном режиме PAD. Чтобы установить соединение X.25, он должен набрать X.121-адрес требуемого объекта. Чтобы разорвать соединение, необходимо перейти в командный режим PAD при помощи команды "Внимание" (по умолчанию CTRL-P) и ввести команду CLR.

Подробно об использовании PAD в сети X.25 см. [Часть 7](#).

§5.1.5. Статистика Telnet-станций

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

```
D S TN:<номер>
```

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

Для сброса статистики Ethernet-станции используется команда Clear Statistics:

```
C S TN:<номер>
```

§5.2. Клиент Telnet

§5.2.1. Вызов клиента Telnet

Клиент Telnet представляет собой многоканальный объект, который обеспечивает установление соединений из сети X.25 в сеть IP. Обращение к нему возможно при помощи коммутируемых логических соединений X.25, для чего в таблице маршрутизации X.25 должна быть сделана запись, устанавливающая маршрут к этому модулю.

Если пользователь сети X.25 посылает вызов с заданным адресом X.121 (или другим критерием маршрутизации), то этот вызов маршрутизируется на клиент Telnet. Последний может, в зависимости от конфигурации маршрута, автоматически установить соединение с заданным IP-адресом и номером порта удаленного сервера, либо предоставить пользователю обычное меню команд Telnet, с помощью которого пользователь может устанавливать соединения вручную. При автоматическом установлении соединения клиент, как и станция, может работать в обычном режиме или в прозрачном режиме (без обработки команд Telnet и символа IAC.)

Пусть, например, в таблице маршрутизации X.25 имеется запись следующего вида:

```
S R PR:14 ID:D RT:1234567890 TO:TC.<параметры>
```

Если пользователь сети X.25 посылает вызов по X.121-адресу 1234567890, то этот вызов маршрутизируется на клиента Telnet. (Подробно о маршрутизации вызовов X.25 см. [Часть 7.](#)) Дальнейшие действия определяются набором дополнительных параметров клиента Telnet:

TO:TC	После соединения с клиентом Telnet пользователь X.25 должен установить соединение с удаленным сервером Telnet при помощи команд Telnet.
TO:TC.<ip-адрес>	При подключении пользователя X.25 автоматически устанавливается соединение с сервером Telnet по указанному IP-адресу и порту TCP 23. Если установить соединение невозможно, или если оно разорвано, то соединение X.25 также разрывается. Аналогичные действия выполняются и в нижеперечисленных частных случаях.

Остальные параметры позволяют установить специфические режимы работы с удаленным сервером. Все они являются необязательными, но обязательно требуют указания IP-адреса и вводятся строго в нижеприведенной последовательности. Все параметры разделяются прямым слэшем (/).

<порт>	Устанавливается Telnet-соединение с заданным IP-адресом и номером порта TCP сервера.
RAW или DAT	<p>Параметр RAW означает, что после установления Telnet-соединения клиент начинает работать в прозрачном режиме, т.е. игнорирует команды Telnet и символ IAC (255). Данный режим аналогичен конфигурации IAC:NO для станции Telnet.</p> <p>Если установлен параметр DAT (поддерживается в версиях программного обеспечения 8.2.0 и старше), то клиент обрабатывает IAC-последовательности, но отключает реакцию на escape-символ (выход в командный режим). Такой режим предназначен для подключения к демону telnetd на UNIX-машинах (включая Linux).</p> <p>Если ни один из параметров RAW или DAT не указан, то соединение производится в обычном режиме, т.е. с возможностью выхода в командный режим и обработкой IAC-последовательностей.</p>
<ip-адрес_источника>	В исходящих пакетах Telnet в качестве IP-адреса источника указывается не адрес интерфейса, с которого посылается пакет, а некоторый заданный IP-адрес.

Если Telnet-соединение устанавливается пользователем вручную, ни один из перечисленных параметров не может быть использован, но номер TCP порта и спецсимволы, интерпретируемые клиентом, можно установить вручную же с помощью команд Telnet (см. следующий параграф).

Пример наиболее подробной конфигурации:

```
TO:TC.123.145.167.189/2023/RAW/132.154.176.198
```

В данном случае после обращения к клиенту Telnet устанавливается соединение с сервером, имеющим адрес 123.145.167.189, по порту TCP 2023, в прозрачном режиме, а в исходящих пакетах указывается IP-адрес источника 132.154.176.198.

ПРИМЕЧАНИЕ В версиях программного обеспечения 8.1.2 и младше обратный адрес допускалось указывать только для прозрачного режима, т.е. после параметра RAW. Начиная с версии 8.2.0 включительно, обратный адрес можно указывать для любого режима.

ВНИМАНИЕ Если задан IP-адрес источника, то либо это должен быть адрес одного из IP-интерфейсов устройства, находящегося в состоянии UP, либо к нему должен быть сконфигурирован маршрут, ведущий через локальный интерфейс:

```
S I NET:<адрес_сети> MASK:<маска> IP:0
```

причем указанный IP-адрес источника должен находиться в диапазоне, определяемом адресом и маской сети.

§5.2.2. Команды клиента Telnet

При работе с удаленным сервером Telnet в обычном режиме (т.е. если не установлен параметр RAW или DAT) пользователь может перейти в командный режим Telnet-клиента, введя специальный escape-символ. По умолчанию, таким символом является комбинация Ctrl-] (0x1D) В командном режиме пользователю доступны следующие стандартные команды Telnet:

open	Установить соединение с заданным узлом
close	Разорвать текущее соединение
send	Передать специальный символ (для получения более подробной информации введите send ?)
set	Установить параметры работы клиента (для получения более подробной информации введите set ?)
status	Вывести информацию о параметрах клиента
help или ?	Вывести справочную информацию
quit	Завершить работу с клиентом Telnet

Для возвращения в режим передачи данных следует ввести пустую строку (нажать клавишу Enter).

Начиная с версии программного обеспечения 8.2.0, поддерживаются две дополнительные команды, которые являются специфическими для устройств NSG,:

set esc <клавиша>	Установить escape-символ для выхода в командный режим. В качестве параметра команды следует нажать желаемую клавишу или сочетание клавиш.
set noesc	Отключить реакцию на escape-символ для выхода в командный режим. При установленном TCP-соединении эта команда обеспечивает прозрачность передачи данных в рамках telnet-протокола. После ввода данной команды соединение функционирует так же, как при использовании параметра DAT клиента Telnet.

После выполнения этих команд клиент Telnet автоматически возвращается в режим передачи данных. Во втором случае выход из этого режима более невозможен до конца сеанса Telnet.

§5.2.3. Вызов клиента Telnet с низкоинтеллектуальных терминалов

Если инициатором соединения Telnet должно быть низкоинтеллектуальное периферийное устройство, имеющее единственный механизм управления связью — сигналы DTR/DCD, то для вызова клиента Telnet следует назначить порту тип PAD с прозрачным профилем и использовать механизм автовызова, например:

```
S P PO:1 TY:PAD IF:V24 SP:9600 AC:0 CD:YES CO:T PROF:3
S A AD0:333
S R PR:1 ID:D RT:333 TO:TC.123.145.167.189/8023
```

При поднятии сигнала DTR терминала (для порта он является сигналом DCD) порт посылает вызов по адресу 333. Вызов маршрутизируется на клиента Telnet, который, в свою очередь, устанавливает соединение с сервером, в данном случае — по адресу 123.145.167.189 и порту TCP 8023. При падении сигнала DCD на порту оба соединения — X.25 внутри устройства и Telnet с удаленным сервером — разрываются; параметр CO:T указывает, что в этом случае устройство NSG должно опустить свой сигнал DTR (который приходит на терминал как DCD) на 2 секунды, чтобы заставить терминал повторно инициализировать соединение. Эта схема работоспособна и в том случае, если терминал подключен к устройству NSG не непосредственно, а через модемную пару.

Аналогичный способ используется для автоматического установления с удаленным портом PAD или сервером Telnet в других случаях, например, для проключения клиентов асинхронного доступа на сервер UUCP.

§5.2.4. Ручной вызов клиента Telnet

Клиент Telnet в устройствах NSG представляет собой, в первую очередь, средство интеграции сетевых решений на основе технологий X.25 и IP, а не отладочный инструмент сетевого администратора. По этой причине он вынесен за пределы управляющего приложения Manager.

Чтобы с устройства NSG установить соединение Telnet с другим устройством, следует создать маршрут X.25 на клиента Telnet, например:

```
S R PR:1 ID:D RT:333 TO:TC
```

Если требуется неоднократно работать с одним и тем же сервером, можно сразу включить в команду маршрутизации его адрес, порт и вспомогательные параметры, например:

```
S R PR:1 ID:D RT:333 TO:TC.123.145.167.189/2323
```

и выйти из менеджера (но не из сеанса Telnet или PAD!)

```
Q M
```

После этого в ответ на приглашение PAD (звездочку) нужно ввести адрес 333, чтобы вместо менеджера установить соединение с клиентом Telnet. После завершения сеанса Telnet снова выводится приглашение PAD; можно ввести MN и вернуться в менеджер.

Удобнее, чтобы не выходить из менеджера, сконфигурировать на устройстве NSG еще одну станцию Telnet типа PAD, например:

```
S P TN:1 TY:PAD PROF:3
W S TN:1
```

и установить к ней отдельный сеанс Telnet с рабочего места администратора. В одном окне производится управление устройством, в другом можно ввести адрес 333 и соединиться с клиентом Telnet. Аналогичным образом можно использовать дополнительный физический порт типа PAD.

Далее, чтобы не вводить каждый раз адрес 333, можно определить для вспомогательной станции индивидуальный номер порта и автовызов по этому адресу:

```
S P TN:1 TY:PAD TCP:8023 AC:0 CO:T PROF:3
S A AD0:333
```

В этом случае пользователь, обратившийся по порту TCP 8023, будет автоматически прокнучаться на клиента Telnet. При разрыве соединения с удаленным сервером станция Telnet также разорвет установленное к ней соединение и через 2 сек. будет готова к повторному соединению.

ВНИМАНИЕ Во всех вышеприведенных конфигурациях клиент Telnet оказывается доступен для неограниченного круга удаленных пользователей. Это не создает непосредственной угрозы безопасности самого устройства NSG, однако позволяет использовать его для противоправных действий в отношении третьих хостов. Чтобы избежать компрометации устройства, необходимо строго ограничить доступ к нему по Telnet с помощью фильтров, либо использовать аутентификацию на станции Telnet (см. ниже).

Источник проблемы в данном случае состоит в том, что клиент Telnet находится вне менеджера и, соответственно, не защищен его паролем. Если для обращения к клиенту Telnet необходимо вводить некоторый специальный адрес X.121, известный только администратору, то его можно, в некоторой степени, рассматривать как пароль — хотя и весьма простой и поддающийся подбору. Однако в последнем варианте (с автовызовом) удаленному пользователю не требуется знать даже этот адрес. Таким образом, злоумышленник может, просканировав сеть, обнаружить открытый порт 8023, подключиться к клиенту Telnet и действовать дальше уже с устройства NSG.

Для защиты Telnet-станции и связанного с ней клиента Telnet в этом случае необходимо настроить либо фильтры, например:

```
S I FILTER PR:0 TY:A PT:TCP DP:8023 SA:<ip-адрес административной станции>
S I FILTER PR:0 TY:D PT:TCP DP:8023 SA:ALL
```

либо аутентификацию, например:

```
S P TN:1 TY:PAD TCP:8023 AC:0 CO:T PROF:3
S A AD0:333
S P AU:1 TY:LOCAL NAME:telnet-to-telnet
A X PAP:1 admin telnet-to-telnet qwerty
S P TN:1 TY:ASYNC AU:1
```


После настройки параметров PAD Telnet-станции присваивается тип ASYNC, обеспечивающий аутентификацию пользователя в терминальном режиме. В данном примере доступ разрешен для пользователя admin с паролем qwerty. В случае успешной аутентификации станция динамически принимает тип PAD с установленными ранее параметрами и посылает вызов по адресу 333. Таким образом, для клиента Telnet обеспечивается столь же надежная парольная защита, как и для других способов доступа к устройству.

Подробнее о фильтрах см. [Часть 4](#), об аутентификации [Часть 8](#).

ВНИМАНИЕ Не следует использовать для обращения к клиенту Telnet тривиальные адреса, такие как 123, 111 и т.п. Рекомендуется производить маршрутизацию не по вызываемому адресу, а по номеру физического порта типа PAD (но не Telnet-станции), вызываемому адресу или полю пользовательских данных.

Если клиент Telnet используется для отладки (например, для последовательного прохождения по цепочке от одного устройства к другому), то по окончании отладки следует удалить маршрут X.25 к нему, по соображениям безопасности.

§5.3. Инкапсуляция X.25-over-TCP/IP (ХОТ)

Технология X.25-over-TCP/IP (ХОТ, RFC-1613) позволяет использовать соединения TCP в качестве транспорта для передачи трафика логических каналов сети X.25. Для ее применения требуется совместная настройка как стека протоколов TCP/IP, так и стека X.25.

В части, относящейся к TCP/IP, необходимо настроить необходимые параметры для соединения с удаленным хостом сети IP, поддерживающим службу ХОТ. Настройка параметров IP сетевого, канального и физического уровня описана в [Частях 3 и 4](#) данного руководства.

ПРИМЕЧАНИЕ В устройствах NSG служба ХОТ включена постоянно и принимает входящие соединения на порту TCP 1998 IP-маршрутизатора. Чтобы запретить доступ по этому порту, следует использовать соответствующие IP-фильтры.

Со стороны сети X.25 необходимо создать в таблице маршрутизации X.25 запись, направляющую пакеты CALL на службу ХОТ, вместо какого-либо физического порта или станции. Пример:

```
S R PR:4 ID:D RT:1234567890 TO:192.168.57.3
```

В данном случае, если получен пакет CALL с X.121-адресом назначения 1234567890, то будет установлено ХОТ-соединение с удаленным IP-хостом, расположенным по адресу 192.168.57.3. Пакет CALL будет передан по этому соединению и отправлен в сеть X.25 на удаленной стороне. Подробнее о маршрутизации вызовов X.25 см. [Часть 7](#).

Если для соединения требуется установить какие-либо специфические параметры, относящиеся к работе сети X.25, то в версиях программного обеспечения 8.2.0 и старше это можно сделать при помощи профиля ХОТ. Номер профиля указывается после IP-адреса через запятую:

```
S R PR:4 ID:D RT:1234567890 TO:192.168.57.31,3
```

Параметры профилей ХОТ и команды для их настройки также описаны в [Части 7](#) данного руководства. Если номер профиля не указан, то параметры ХОТ-соединения устанавливаются по умолчанию.

ПРИМЕЧАНИЕ В версиях 7.6.4–8.1.2 такой же формат команды Set Route использовался, чтобы указать время ожидания установки соединения (в секундах). Остальные параметры ХОТ-соединения не настраивались.

Если к устройству NSG установлено ХОТ-соединение со стороны IP-сети, полученные по нему пакеты передаются подсистеме X.25 и обрабатываются в ней обычным образом. Пакеты CALL используются для установления коммутируемых логических соединений (SVC) в сети X.25, а пакеты других типов передаются по этим соединениям.

Максимальное количество одновременно установленных соединений ХОТ есть постоянная величина, которая определяется моделью устройства и версией программного обеспечения.

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

D S ХОТ:0 Вывести статус всех установленных соединений ХОТ.

D S ХОТ:<номер> Вывести подробную информацию о заданном соединении. Номер требуемого соединения можно узнать с помощью предыдущей команды.

Пример (информация обо всех соединениях):

```
Manager: D S XOT:0
XOT:1 tcb = 2
    Connect to Port 5 Channel 1, src=<NONE>, dst=6666, tm=0:00:04.13
XOT:2 tcb = 4
    Connect to XOT(10.0.10.17), src=<NONE>, dst=5555, tm=0:00:04.14
XOT:63 tcb = 5
    Connect to Manager, src=<NONE>, dst=5555, tm=0:00:04.14
```

Информация о каждом соединении представлена двумя строками. В первой строке указываются параметры TCP:

XOT:n	Номер соединения XOT.
tcb = n	Номер TCB, который описывает установленное TCP-соединение.

Вторая строка описывает логическое соединение X.25. Формат вывода идентичен команде D C.

Пример (информация о заданном соединении):

```
Manager: D S XOT:1
XOT:1 tcb = 2
    Connect to Port 5 Channel 1, src=<NONE>, dst=6666, tm=0:01:53.09
TCB 2: type is CONNECTION, state is ESTABLISHED
Local host: 10.0.10.17, Local port: 65474
Remote host: 10.0.10.17, Remote port: 1998
iss: 3071795200 snduna: 3071795715 sndnxt: 3071795715 sndwnd: 4096
irs: 3071795200 rcvnxt: 3071796212 rcvwnd: 4089
Datagrams(rmss: 1460 smss: 1420):
Rcvd: 135, with data: 66, total data bytes: 1011
Sent: 135(retransmit: 0), with data: 67, total data bytes: 514
```

Здесь добавлена информация о TCP соединении в том же формате, что и в команде D S TCB:n (см. [Часть 4](#)).

§5.4. SNMP-управление

§5.4.1. Настройка агента SNMP

В устройствах NSG содержится встроенный агент SNMP v1, обеспечивающий управление устройством из любой системы сетевого администрирования на основе протокола SNMP. Реализация агента соответствует RFC-1157.

Административная станция или группа станций, с которых осуществляется управление, в терминах протокола SNMP именуется "сообществом" (*community*). Чтобы объявить *community* для агента SNMP, необходимо использовать команду Set Parameters в формате:

```
S P CO:<номер> NAME:<имя> WR:<права> TP:<тип_ловушек> IADR:<ip-адрес> MASK:<маска>
```

Параметры CO и NAME определяют номер и административное имя *community*, соответственно. Имя задается в виде текстовой строки длиной до 16 символов. Пустое имя запрещает агенту использовать параметры данного *community*.

ВНИМАНИЕ По умолчанию, в устройстве определено одно *community* с именем public и правами доступа только на чтение. Для обеспечения максимальной безопасности устройства NSG и подключенных к нему сетей рекомендуется удалить данное *community*:

```
S P CO:0 NAME:""
```

Параметры IADR и MASK содержат IP-адрес и маску в десятичной дотовой нотации и определяют диапазон адресов, в котором должны находиться станции данного *community*.

Права доступа для станций данного *community* устанавливаются параметром WR (Write Enabled):

WR:YES	Разрешены операции чтения (GetRequest, GetNextRequest) и записи (SetRequest).
WR:NO	Разрешены только операции чтения (GetRequest, GetNextRequest).

При возникновении важных событий в системе SNMP-агент рассылает управляющим станциям сообщения специального вида — системные ловушки (*traps*). Базовый перечень таких событий (General Traps) определен рекомендацией RFC-1215. В дополнение к этому перечню поддерживаются сообщения, сигнализирующие о попытках доступа к конфигурации системы и ее изменения, и сообщения, о событиях, специфичных для аппаратуры NSG. Категория отсылаемых ловушек выбирается параметром TP:

TP:NO	Генерация системных ловушек отключена.
TP:GE	Генерируются только общесистемные ловушки согласно RFC-1215.
TP:AU	Генерируются только ловушки, связанные с аутентификацией или специфические для NSG.
TP:ALL	Генерируются ловушки обоих типов: GE и AU.

Для обмена данными между управляющей станцией и агентом SNMP используются датаграммы UDP (порты 161 и 162). При получении запроса от управляющей станции агент SNMP проверяет:

- Наличие имени *community*, указанного в запросе, в списке *communities* данного устройства.
- Принадлежность адреса управляющей станции диапазону адресов найденного *community*.
- Права доступа (при операции SetRequest).

Если проверки выполнены успешно, агент SNMP выполняет запрос и отправляет ответ (GetResponse) управляющей станции. Если соответствия не найдено, то фиксируется ситуация нарушение прав доступа, запрос игнорируется и, при TP:AU или TP:ALL, отправляется системная ловушка типа "Authentication Failure".

Для просмотра параметров SNMP *community* используется команда Display Parameters в одном из следующих форматов:

```
D P CO:<номер>
D P CO:A
```

ПРИМЕЧАНИЕ Справочные сведения об устройстве устанавливаются командой S W (см. Часть 2) со следующими параметрами:

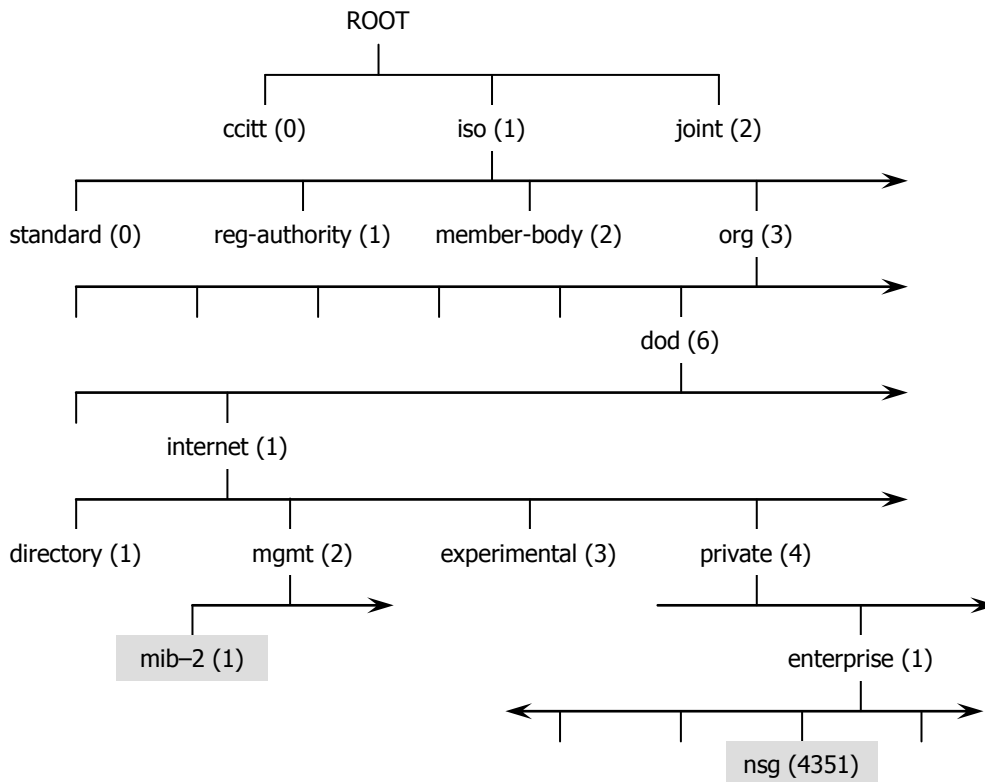
HNAM (Host Name)	Административное имя данного узла.
CONT (Contact)	Информация о специалисте, обслуживающем данное устройство.
LOC (Location)	Информация о местонахождении данного узла.

Значениями этих параметров являются текстовые строки длиной до 255 символов.

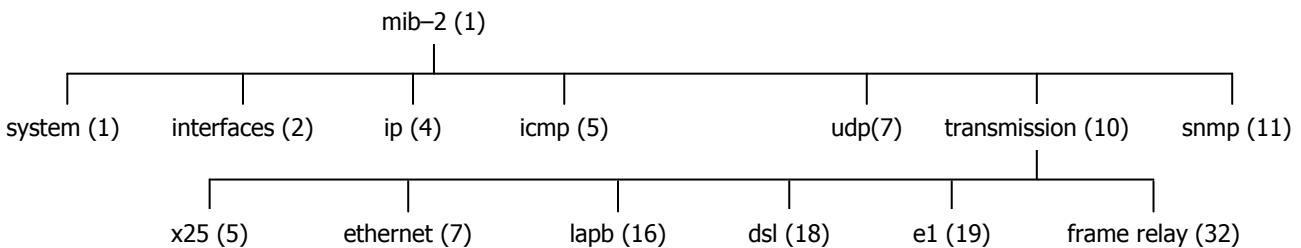
§5.4.2. База MIB

База управляемых переменных реализована соответствии с рекомендацией RFC–1213 (MIB II). Общий путь к управляемым переменным устройства имеет стандартный префикс:

mib-2 = 1.3.6.1.2.1



В рамках MIB II поддерживаются следующие группы управляемых переменных:

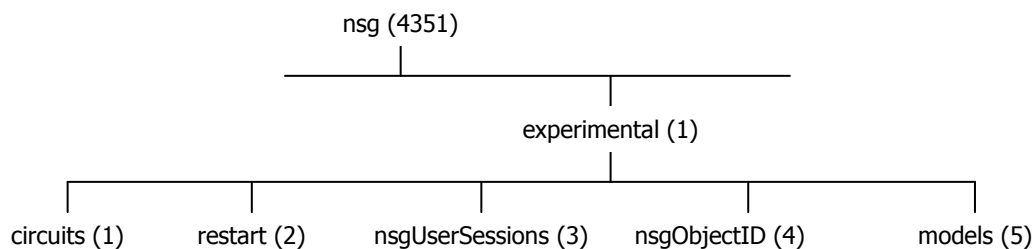


Имена и идентификаторы (OID) переменных, их описания и области допустимых значений приведены в спецификации MIB II (RFC–1213).

Приватная база управляемых переменных (Private MIB) устройств NSG имеет локальный префикс

nsg = 1.3.6.1.4.1.4351

и содержит следующие группы управляемых переменных:



Компоненты Private MIB содержатся в файлах *.mib, которые могут быть загружены с Web-серверов компании <http://www.nsg.ru>, <http://www.nsg2u.ru> или получены у местных дилеров NSG.

Группа `circuits` определена в mib-файлах `nsg-ss.mib` и `nsg-gs.mib`. Группа содержит набор управляемых переменных для контроля за сигнальными линиями интерфейсных модулей IM-DIO.

Группа `restart` определена в mib-файле `nsg-rt.mib`. Группа содержит набор управляемых переменных для перезагрузки устройства в целом, рестарта отдельных его компонент (аналог команды `W S`), либо сброса (обнуления) статистики по отдельным компонентам (аналог команды `C S`).

Группа `nsgUserSessions` определена в mib-файле `nsg-us.mib`. Группа содержит набор управляемых переменных для контроля за сеансами работы пользователей.

Группа `NSG_ObjectID` определена в mib-файле `nsg-ob.mib` и содержит текстовые описания и идентификаторы (OID) основных элементов системы: портов, интерфейсов и станций.

Группа `models` определена в mib-файле `nsg-mo.mib` и содержит текстовые описания и идентификаторы (OID) различных моделей устройств NSG.

§5.4.3. Системные ловушки (Traps)

Расылка сообщений Trap осуществляется только тем управляющим станциям, для которых *community* определено следующим образом:

- IP-адрес является точным адресом станции (`MASK:255.255.255.255`).
- Параметр TP имеет значение GE, AU или ALL.

а) Общесистемные сообщения

При значении параметра TP:GE для управляющей станции будут посылаться следующие сообщения Trap:

ColdStart	В системе произошла переинициализация одного из физических портов, перед которой была произведена запись конфигурации в энергонезависимую память. Это означает, что могло быть произведено изменение конфигурации системы. Данное сообщение посылается также при запуске/сбросе устройства или переинициализации всей подсистемы IP (<code>W S IP:0</code>).
WarmStart	В системе произошла переинициализация одного из физических портов без изменения конфигурации системы, записанной в энергонезависимую память.
LinkUp/LinkDown	Переход одного из физических интерфейсов в состояние UP или DOWN, соответственно. Номер интерфейса, у которого произошло изменение сигнала DCD, передается в сообщении Trap параметром <code>IfIndex</code> . Состояние протокола отображается специфическими сообщениями NSG с номерами 7–10 (см. ниже).

ПРИМЕЧАНИЕ Номер физического интерфейса в сообщении Trap на единицу больше номера порта, к которому он относится. Например, Trap типа LinkUp с `IfIndex=3` означает, что порт номер 2 устройства перешел в состояние UP.

б) Сообщения аутентификации и специфические для NSG

При значении параметра TP:AU для управляющей станции будут посылаться следующие сообщения Trap:

AuthenticationFailure	Обнаружение SNMP-агентом несанкционированного обращения к системе. Несанкционированным считается обращение, при котором в запросе SNMP (<code>GetRequest</code> , <code>GetNextRequest</code> или <code>SetRequest</code>) обнаружено хотя бы одно из следующих нарушений: <ul style="list-style-type: none"> — поле "Community name" не совпадает ни с одним <i>community</i>, объявленным в устройстве (см. параметр Name). — IP-адрес источника (Source Address) не находится в диапазоне адресов, назначенных <i>community</i> с данным именем (параметры IADR, MASK).
EnterpriseSpecific	Обнаружение SNMP-агентом следующих системных событий: <ul style="list-style-type: none"> — Trap=0 (PRIVILEGE VIOLATION FOR SET REQUEST) — получен запрос на изменение параметра системы от управляющей станции, для которой установлены привилегии Read Only (WR:NO). — Trap=1 (CONNECT TO MANAGER) — произошло подключение пользователя к управляющему модулю Manager. — Trap=2 (DISCONNECT FROM MANAGER) — произошло отключение пользователя от управляющего модуля Manager. — Trap=3 (REWRITE CONFIGURATION) — пользователь выполнил команду записи конфигурации (W F).

- Trap=4 (CONNECT TO TELNET STATION) — подключение пользователя к некоторой Telnet-станции. Номер станции передается в сообщении Trap.
- Trap=5 (DISCONNECT FROM TELNET STATION) — отключение пользователя от некоторой Telnet-станции. Номер станции передается в сообщении Trap.
- Trap=6 (SOME CHANNEL HAS CHANGED STATUS) — произошло переключение одного или более входных контактов некоторого модуля IM-DIO. Номер порта, в который установлен модуль IM-DIO, передается в сообщении Trap.
- Trap=7 (FRAME RELAY STATION DOWN) — некоторая станция Frame Relay перешла в состояние DOWN. Номер станции передается в сообщении Trap.
- Trap=8 (FRAME RELAY STATION UP) — некоторая станция Frame Relay перешла в состояние UP. Номер станции передается в сообщении Trap.
- Trap=9 (PAD LOGICAL LINK DOWN) — некоторый порт PAD перешел в состояние DOWN. Номер порта передается в сообщении Trap.
- Trap=10 (PAD LOGICAL LINK UP) — некоторый порт PAD перешел в состояние UP. Номер порта передается в сообщении Trap.

§5.4.4. Перегрузка устройства и рестарт его компонент

Для управления перезагрузкой устройства и рестартом отдельных его компонент необходимо установить в административном приложении на основе SNMP базу управляемых переменных nsg-rt.mib. База содержит следующие группы переменных:

а) рестарт физических портов

rtPortNumber	Число физических портов устройства (Read Only).
rtPortTable	Таблица физических портов. Каждая запись (строка) таблицы содержит две переменные:
rtPortIndex	Индекс физического порта (Read Only). Находится в диапазоне от 0 до rtPortNumber-1.
rtPortOperation	Тип операции с портом (Read-Write): 0 — нет операции (порт продолжает работать) 1 — рестарт порта (аналогично команде W S PO:<rtPortIndex>) 2 — обнуление статистики порта (аналогично команде C S PO:<rtPortIndex>)

б) рестарт настраиваемых физических интерфейсов E1

rtInterfaceNumber	Число настраиваемых физических интерфейсов устройства (Read Only).
rtInterfaceTable	Таблица настраиваемых физических интерфейсов. Каждая запись (строка) таблицы содержит две переменные:
rtInterfaceIndex	Индекс настраиваемого физического интерфейса (Read Only). Находится в диапазоне от 0 до rtInterfaceNumber-1.
rtInterfaceOperation	Тип операции с интерфейсом (Read-Write): 0 — нет операции (интерфейс продолжает работать) 1 — рестарт интерфейса (аналогично команде W S IF:< rtInterfaceIndex>) 2 — обнуление статистики интерфейса (аналогично команде C S IF:< rtInterfaceIndex>)

в) рестарт Telnet-станций

rtTelnetNumber	Число Telnet-станций устройства (Read Only).
rtTelnetTable	Таблица Telnet-станций. Каждая запись (строка) таблицы содержит две переменные:
rtTelnetIndex	Индекс Telnet-станции (Read Only). Находится в диапазоне от 0 до rtTelnetNumber-1.
rtTelnetOperation	Тип операции с Telnet-станцией (Read-Write): 0 — нет операции (станция продолжает работать) 1 — рестарт станции (аналогично команде W S TN:< rtTelnetIndex>) 2 — обнуление статистики станции (аналогично команде C S TN:< rtTelnetIndex>)

г) рестарт IP-интерфейсов

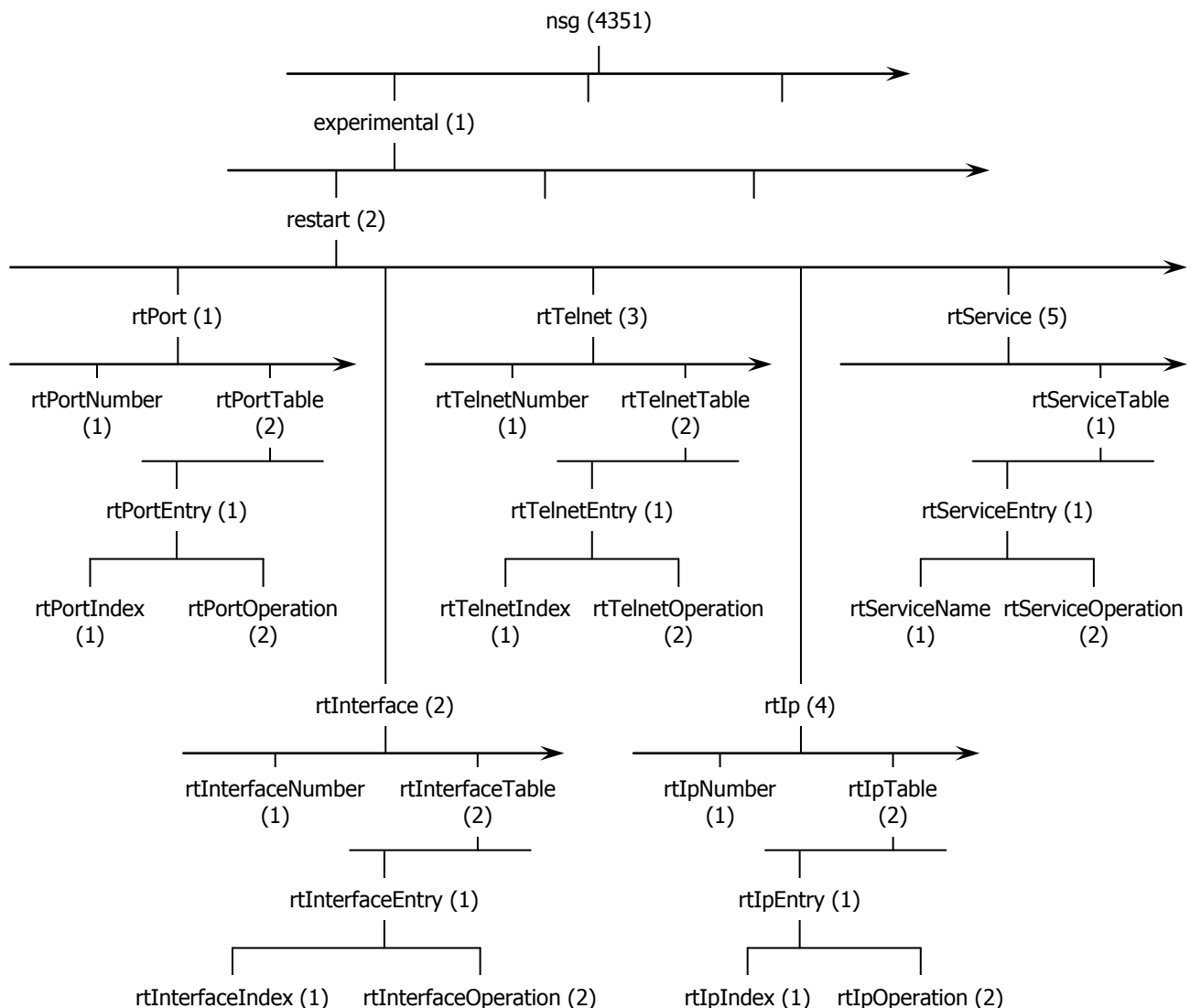
rtIpNumber	Число IP-интерфейсов устройства (Read Only).				
rtIpTable	Таблица IP-интерфейсов. Каждая запись (строка) таблицы содержит две переменные: <table border="0" style="margin-left: 20px;"> <tr> <td>rtIpIndex</td> <td>Индекс IP-интерфейса (Read Only). Находится в диапазоне от 0 до rtIpNumber-1.</td> </tr> <tr> <td>rtIpOperation</td> <td>Тип операции с интерфейсом (Read-Write): 0 — нет операции (интерфейс продолжает работать) 1 — рестарт интерфейса (аналогично команде W S IP: < rtIpIndex >) 2 — обнуление статистики интерфейса (аналогично команде C S IP: < rtIpIndex >)</td> </tr> </table>	rtIpIndex	Индекс IP-интерфейса (Read Only). Находится в диапазоне от 0 до rtIpNumber-1.	rtIpOperation	Тип операции с интерфейсом (Read-Write): 0 — нет операции (интерфейс продолжает работать) 1 — рестарт интерфейса (аналогично команде W S IP: < rtIpIndex >) 2 — обнуление статистики интерфейса (аналогично команде C S IP: < rtIpIndex >)
rtIpIndex	Индекс IP-интерфейса (Read Only). Находится в диапазоне от 0 до rtIpNumber-1.				
rtIpOperation	Тип операции с интерфейсом (Read-Write): 0 — нет операции (интерфейс продолжает работать) 1 — рестарт интерфейса (аналогично команде W S IP: < rtIpIndex >) 2 — обнуление статистики интерфейса (аналогично команде C S IP: < rtIpIndex >)				

д) рестарт отдельных служб и перезагрузка всей системы

rtServiceTable	Таблица служб. Каждая запись (строка) таблицы содержит две переменные: <table border="0" style="margin-left: 20px;"> <tr> <td>rtServiceName</td> <td>Имя (индекс) службы (Read Only): 0 — устройство в целом 1 — IP-маршрутизатор 2 — служба DNS 3 — сервер HTTP 4 — служба ХоХ (HX)</td> </tr> <tr> <td>rtServiceOperation</td> <td>Тип операции (Read-Write): 0 — нет операции (служба продолжает работать) 1 — рестарт службы или узла в целом (аналогично командам W S PO:A, W S IP:0, W S DNS, W S HTTP и W S HX:0)</td> </tr> </table>	rtServiceName	Имя (индекс) службы (Read Only): 0 — устройство в целом 1 — IP-маршрутизатор 2 — служба DNS 3 — сервер HTTP 4 — служба ХоХ (HX)	rtServiceOperation	Тип операции (Read-Write): 0 — нет операции (служба продолжает работать) 1 — рестарт службы или узла в целом (аналогично командам W S PO:A, W S IP:0, W S DNS, W S HTTP и W S HX:0)
rtServiceName	Имя (индекс) службы (Read Only): 0 — устройство в целом 1 — IP-маршрутизатор 2 — служба DNS 3 — сервер HTTP 4 — служба ХоХ (HX)				
rtServiceOperation	Тип операции (Read-Write): 0 — нет операции (служба продолжает работать) 1 — рестарт службы или узла в целом (аналогично командам W S PO:A, W S IP:0, W S DNS, W S HTTP и W S HX:0)				

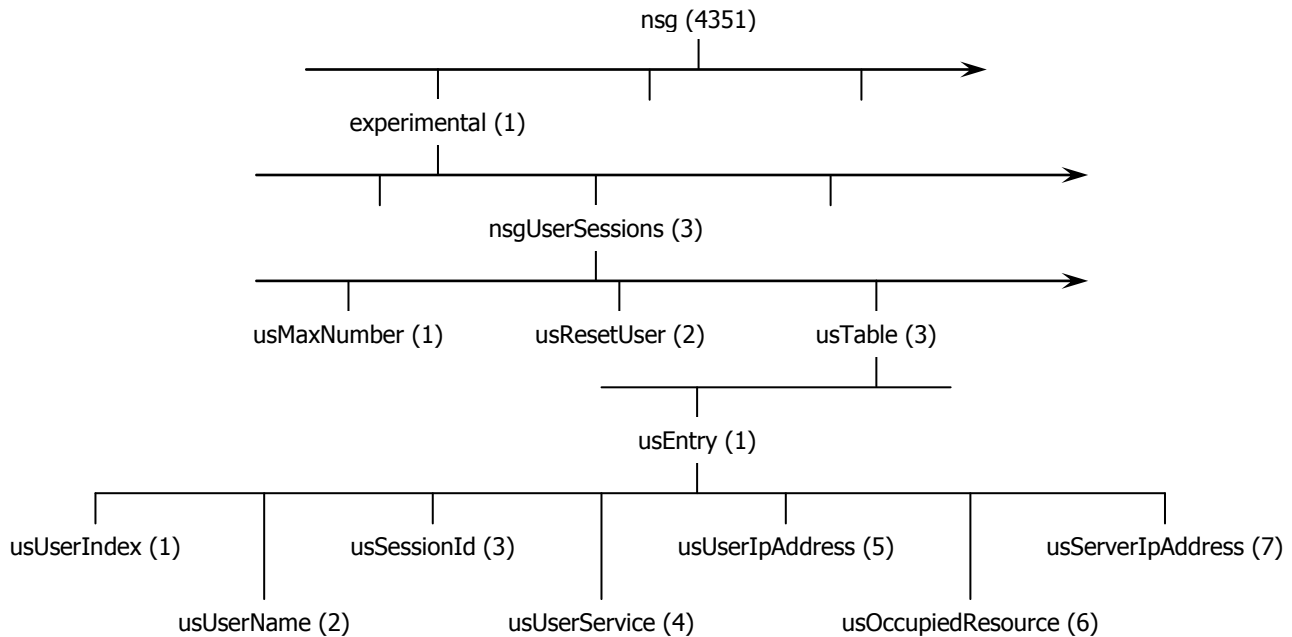
ПРИМЕЧАНИЕ При операции чтения элементов таблиц, которые определяют тип операции (rtPortOperation, rtInterfaceOperation и т.п.) всегда возвращается значение 0 (operate).

Структура ветви restart дерева MIB представлена на рисунке.



§5.4.5. Управление сеансами работы пользователей

Для мониторинга работы пользователей и управления пользовательскими сеансами необходимо установить в административном приложении на основе SNMP базу управляемых переменных `nsg-us.mib`. Структура ветви `nsgUserSessions` дерева MIB представлена на рисунке.



База содержит следующие переменные:

<code>usMaxNumber</code>	Максимальное число пользователей, которые могут быть одновременно подключены к системе. (Read Only)
<code>usResetUser</code>	Запись в эту переменную уникального идентификатора пользователя принудительно завершает сеанс работы пользователя будет и освобождает все занимаемые им ресурсы. Для выполнения такого сброса необходимо знать идентификатор пользователя и иметь привилегии Write. (WR:YES). Операция Read для данной переменной всегда возвращает значение 0.
<code>usTable</code>	Таблица текущих сеансов работы пользователей. Все элементы таблицы имеют атрибут Read Only. Значения полей данной таблицы аналогичны полям таблицы, которая выводится командой <code>D S SY:1</code> (см. Часть 8):
<code>usUserIndex</code>	Номер сеанса. Целое число в диапазоне от 1 до максимального значения (<code>MaxSessionNumber</code>), определенного для данного типа устройства.
<code>usUserName</code>	Имя пользователя, представленное в процессе аутентификации. Если пользователь подключился без аутентификации, то в поле имени выводится строка <code><UNKNOWN></code> .
<code>usSessionId</code>	Уникальный идентификатор сеанса. При удаленной аутентификации (через RADIUS/TACACS+) используется в качестве Account-Session-Id.
<code>usUserService</code>	Тип сервиса, предоставленного пользователю. Возможные значения: PPP, PAD, SLIP.
<code>usUserIpAddress</code>	IP-адрес, назначенный пользователю. Если IP-адрес неприменим для данного типа сервиса (PAD) или неизвестен системе аутентификации (SLIP), то значение этого поля равно 255.255.255.255.
<code>usOccupiedResource</code>	Название ресурса, занимаемого пользователем: PO.<номер> физический порт TN.<номер> Telnet-станция IP.<номер> IP-интерфейс Если пользователь занимает более одного ресурса (например, IP-интерфейс типа PPP и Ethernet-станцию типа PPP), то в таблице будет указан только IP-интерфейс.
<code>usServerIpAddress</code>	Адрес сервера RADIUS/TACACS+, выполнившего аутентификацию данного пользователя. Если пользователь аутентифицирован локально или подключен без аутентификации, то данное поле будет иметь значение 0.0.0.0.

§5.4.6. Управление модулями IM-DIO

Для управления модулями дискретного ввода-вывода IM-DIO используются базы управляемых переменных `nsg-gs.mib` и `nsg-ss.mib`. Первая обеспечивает управление всем модулем как совокупностью входных/выходных пар контактов, вторая — индивидуальное управление каждой парой. Приведенные ниже переменные относятся к модулю IM-DIO/8i4o (восемь входных пар контактов и четыре выходные).

Для отправки сообщений `Ttrap` об изменении состояния входных каналов модуля IM-DIO необходимо установить ненулевую маску сообщений для данного модуля (параметр `TR`):

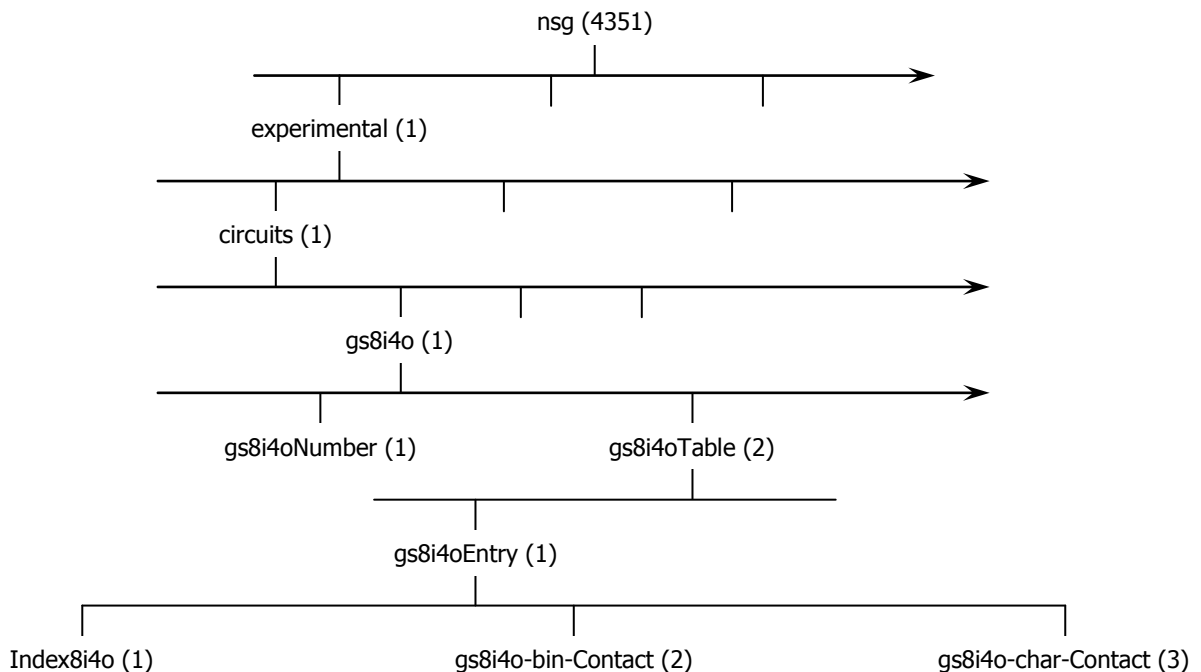
```
S P PO:n TY:SERVICE IF:DIO TR:bbbbbbbb
```

Маска задается в виде строки из 8 символов 0 или 1. Единица в i -ой позиции разрешает генерировать сообщения `Ttrap` для канала `INPUT i`, ноль — запрещает.

База `nsg-gs.mib` содержит следующие переменные:

- `gs8i4oNumber` (1) Число портов, сконфигурированных для работы модулей IM-DIO (Read Only).
- `gs8i4oTable` (2) Таблица, состоящая из записей `gs8i4oEntry` (1). Каждая запись характеризует состояние одного модуля. Число записей указано в `gs8i4oNumber` (1).
- `Index8i4o` (1) Порядковый номер интерфейсного модуля IM-DIO (Read Only).
- `gs8i4o-bin-Contact` (2) Целое число — двоичное интегральное значение всей совокупности контактов. Значащими в данном числе являются 12 младших бит. Нулевое значение каждого бита соответствует разомкнутой цепи, единица — замкнутой. Значение самого младшего бита относится к контактной паре `INPUT 1`, самого старшего — к `OUTPUT 4`. Переменная имеет тип `Read/Write`, но по существу запись имеет смысл только в биты с 8 по 11, отвечающие за контакты `OUTPUT`.
- `gs8i4o-char-Contact` (3) Интегральное значение всей совокупности контактов в символьном виде (`Read/Write`). Строка из 12 символов 0 или 1, где первый символ строки соответствует контактной паре `INPUT 1`, последний — `OUTPUT 4`.

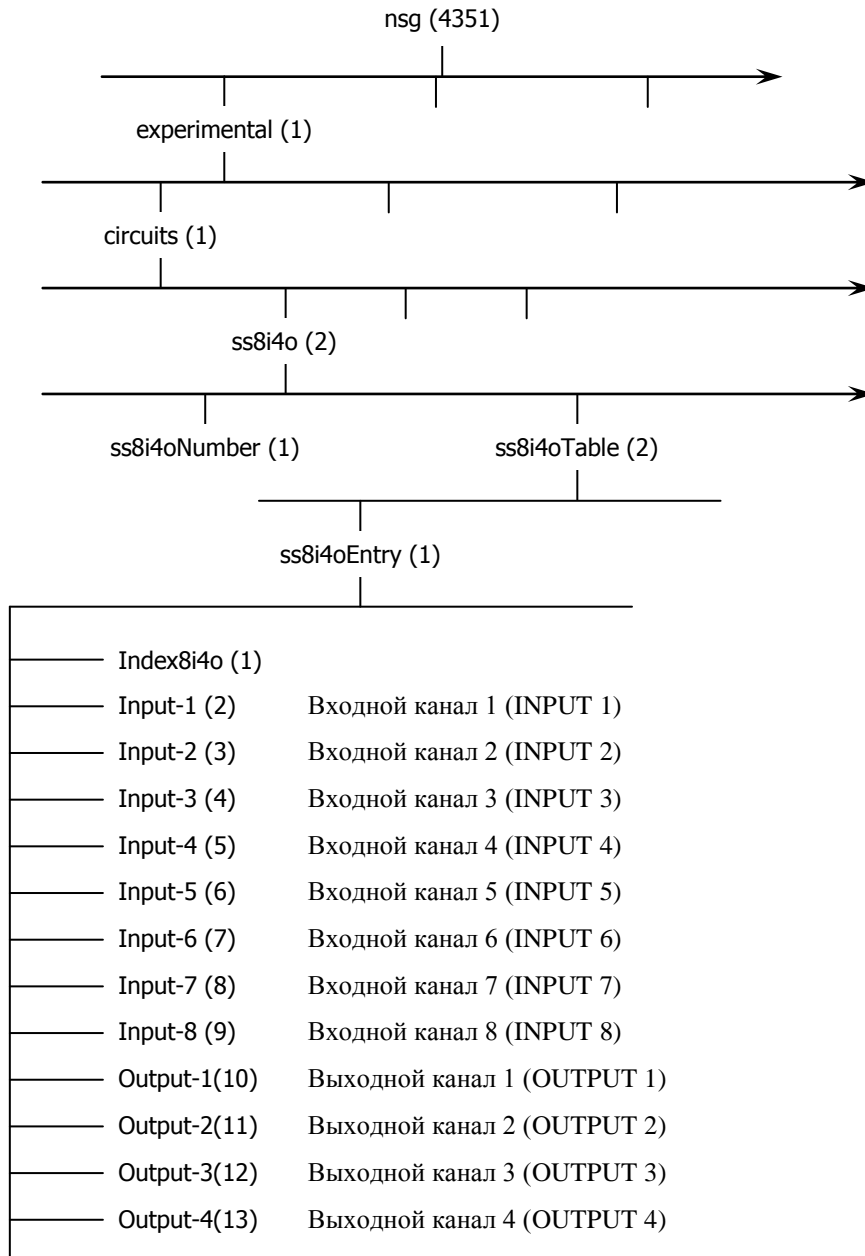
Структура ветви `circuits(1).gs8i4o(1)` дерева MIB представлена на рисунке.



База nsg-ss.mib содержит следующие переменные:

ss8i4oNumber (1)	Число портов, сконфигурированных для работы модулей IM-DIO (Read Only).
ss8i4oTable (2)	Таблица, состоящая из записей ss8i4oEntry (1). Каждая запись характеризует состояние одного модуля. Число записей указано в ss8i4oNumber (1).
Index8i4o (1)	Порядковый номер интерфейсного модуля IM-DIO (Read Only).
Input-1 ... Output-4	12 целых переменных, описывающих состояние соответствующих контактных пар. Значение 0 каждой переменной соответствует разомкнутой цепи, 1 — замкнутой.

Структура ветви circuits(1).ss8i4o(2) дерева MIB представлена на рисунке.



§5.5. Web-управление

§5.5.1 Сервер HTTP

Встроенный сервер HTTP в данной версии программного обеспечения предназначен для удаленного управления устройствами NSG при помощи Web-браузера. Web-интерфейс предлагает большинство функций управления устройством, доступных через интерфейс командной строки. К ним относятся изменение и контроль конфигурации устройства, получение информации о текущем статусе компонентов устройства и статистике их работы, рестарт отдельных подсистем и служб и другие функции.

ВНИМАНИЕ Использование Web-интерфейса ни в коей мере не освобождает пользователя от необходимости понимать сущность и назначение компонент управляемого объекта, взаимосвязь между ними и смысл всех параметров конфигурации. Web-интерфейс избавляет пользователя исключительно от необходимости запоминать точный синтаксис команд и допустимые значения параметров.

ПРИМЕЧАНИЕ Вышеуказанная особенность не является специфической для продуктов NSG, а представляет собой общее свойство Web-интерфейсов для управления *любыми* устройствами и системами — от магистральных маршрутизаторов до интеллектуальных утюгов.

Управляемое устройство должно иметь, как минимум, один действующий IP интерфейс, через который будет осуществляться связь с ним, и активированный стек TCP/IP.

Из за отсутствия полной совместимости Web-браузеров различных производителей круг поддерживаемых браузеров жестко ограничен. Поддерживаются следующие браузеры:

- MS Internet Explorer версии 4.0 и выше;
- Netscape Navigator версии 4.0 и выше.

Осуществление Web-управления из других браузеров не гарантируется. Минимальное разрешение экрана для работы Web-интерфейса NSG — 800×600 точек, рекомендуемое — 1024×768 точек.

Для загрузки и работы сервера HTTP требуются значительные аппаратные ресурсы устройства, в первую очередь, оперативная память. При запуске сервер занимает:

- область Heap — около 160 КБ;
- область Stack — около 4 КБ.

Если в момент запуска сервера HTTP свободной памяти недостаточно, то будет выведено сообщение:

```
HTTP: Unsufficient Memory (xxxx)
```

где xxxx укажет, какой именно памяти недостаточно.

При выполнении запроса управления сервер HTTP дополнительно занимает:

- область Heap — около 5 КБ;
- область Stack — около 20 КБ.

Если в момент выполнения запроса свободной памяти недостаточно, то запрос не будет выполнен, а пользователю будет выведено в окно браузера сообщение:

```
500 Server Error
```

По мере освобождения ресурсов сервер HTTP снова будет отвечать на запросы пользователя.

§5.5.2. Запуск и остановка сервера HTTP

Для запуска сервера HTTP требуется установить параметр HTTP интерфейса IP:0 в значение YES и рестартовать сервер (или все устройство):

```
S P IP:0 HTTP:YES
W S HTTP
```

Для его остановки требуется установить параметр HTTP интерфейса IP:0 в значение NO и рестартовать сервер:

```
S P IP:0 HTTP:NO
W S HTTP
```

При остановке сервера HTTP оперативная память, занимаемая им, освобождается для работы других программных процессов.

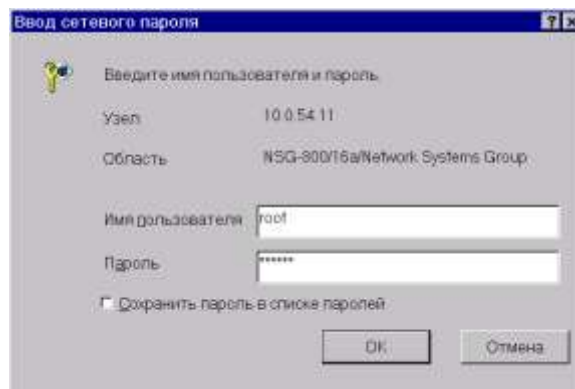
ПРИМЕЧАНИЕ При включении или перезагрузке устройства запуск сервера HTTP определяется тем значением параметра HTTP интерфейса IP:0, которое было сохранено в энергонезависимой памяти.

§5.5.3. Вход в систему

На компьютере, с которого можно установить связь с устройством NSG через сеть TCP/IP, следует запустить Web-браузер и в адресной строке ввести IP-адрес одного из интерфейсов устройства:

```
http://<ip-адрес>
```

При первом обращении к устройству пользователь должен аутентифицировать себя, введя свое имя и пароль в предлагаемом диалоговом окне. Имя пользователя может быть любым, а пароль для входа в Web-интерфейс (при вводе отображается звездочками) совпадает с паролем для входа в модуль Manager.



Если в процессе работы пароль модуля Manager будет изменен (например, администратором, подключенным к модулю Manager через консольный порт, Telnet или сеть X.25), то при очередном обращении из Web-интерфейса пользователю вновь придется пройти процедуру аутентификации.

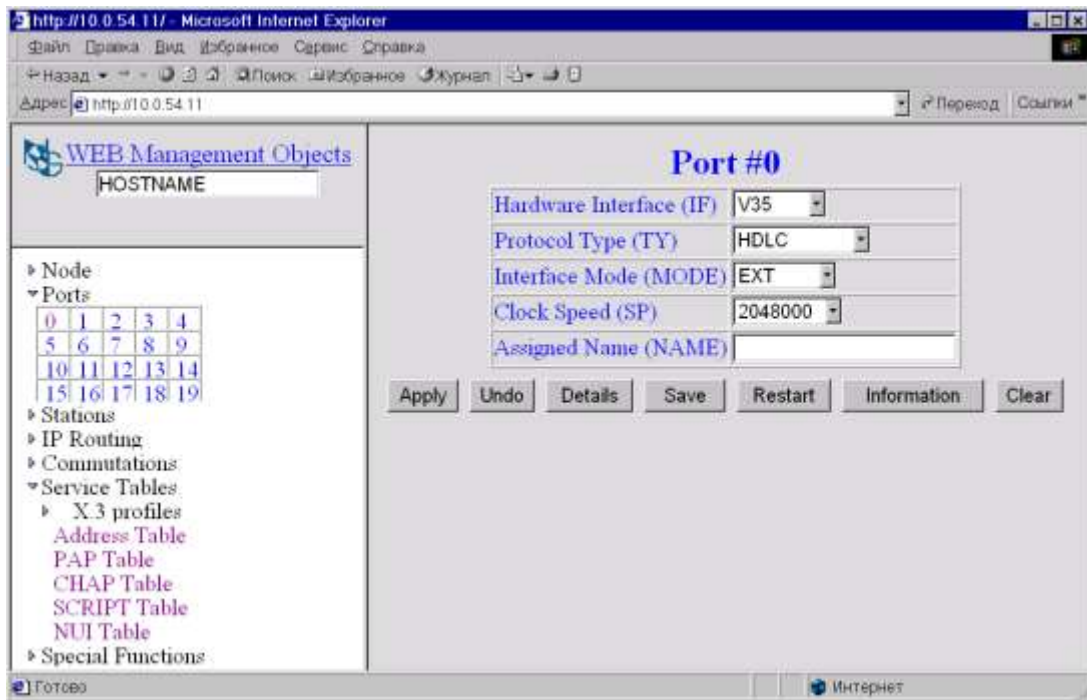
§5.5.4. Структура Web-интерфейса

Окно Web-интерфейса разделено на три поля.

Верхнее левое поле практически не меняется в процессе работы пользователя. Поле содержит гиперссылку Web-Management Objects, при нажатии на которую будет обновлен список управляемых объектов, и административное имя устройства (параметр HNAME). Имя облегчает одновременное управление несколькими устройствами: оно показывает администратору, с каким именно устройством он работает в данном окне.

Нижнее левое поле отображает управляемые объекты устройства, представленные в виде иерархического дерева.

В правом поле страницы (основном информационном поле) вводятся значения параметров управляемых объектов, а также выводится информация о работе устройства и его подсистем.



Под управляемым объектом следует понимать либо какую-то программную компоненту системы (порт, станцию, запись таблицы маршрутизации и т.п.), либо какое-то действие над объектом системы (рестарт порта, рестарт службы, сохранение конфигурации и т.п.). В качестве управляемого объекта может выступать некоторый скалярный элемент (например, параметры модуля Manager), либо набор однотипных элементов (например, физических портов, станций и т.п.).

Все управляемые объекты объединены и представлены в виде иерархической структуры. Для удобства доступа к управляемым объектам ветви дерева могут быть свернуты или развернуты, чтобы отображать на экране только часть управляемых объектов, интересующую пользователя в данный момент.

Управляемый объект, который содержит в себе вложенные объекты или список однотипных объектов, также находится на экране в свернутом либо в развернутом виде. В первом случае он представлен только одной строкой, в которой указывается его название и значок ►, указывающий, что данная ветвь свернута. Во втором случае после названия ветви выводится все ее дочерние ветви, а перед названием стоит значок ▼. Щелчок левой кнопкой мыши на значке ► или ▼ разворачивает и сворачивает ветвь.

§5.5.5. Управление объектами конфигурации

Работа с управляемым объектом предполагает выполнение одной или нескольких из перечисленных ниже операций:

- Установка и контроль значений параметров.
- Определение текущего статуса и статистики.
- Рестарт управляемого объекта.
- Очистка статистики.
- Служебные операции (запись в энергонезависимую память и т.п.).

Для доступа к управляемому объекту необходимо выбрать его в левом окне. После этого в правом окне будут показаны параметры указанного объекта.

Правое окно представляет собой Web-форму, в которой каждый параметр представлен в виде его названия и текущего значения. Вместе с полным названием параметра указывается также его сокращенное обозначение, которое используется в модуле Manager. Для изменения значения параметра необходимо поместить курсор в поле значения и, пользуясь клавиатурой и/или мышью, ввести или выбрать новое значение.

В нижней части окна располагаются кнопки, непосредственно выполняющие функции управления.

Кнопка Apply производит передачу значений, установленных в данном окне, в систему. Нажатие этой кнопки эквивалентно выполнению команды Set Parameters с теми значениями, который в данный момент находятся на экране.

ВНИМАНИЕ До нажатия кнопки Apply никакие действия по изменению параметров системы не производятся.

Перед отправкой заполненной формы в устройство производится анализ значений, введенных пользователем. Если при этом разборе обнаружена ошибка, то форма не отправляется, а пользователь получает сообщение о неправильном значении параметра.

ПРИМЕЧАНИЕ Если пользователь поменял значение параметров, но не нажал кнопку Apply, то при переходе к другому управляемому объекту будет выдано предупреждение.

Кнопка Undo возвращает значение параметров к тем, которые имелись в момент загрузки текущей страницы. Отменить сделанные изменения кнопкой Undo можно только до тех пор, пока они не переданы в устройство кнопкой Apply.

Кнопка Details выводит в текущее окно дополнительные параметры управляемого объекта.

Кнопка Restart перезагружает управляемый объект и эквивалентна команде W S (Warm Start) в интерфейсе командной строки.

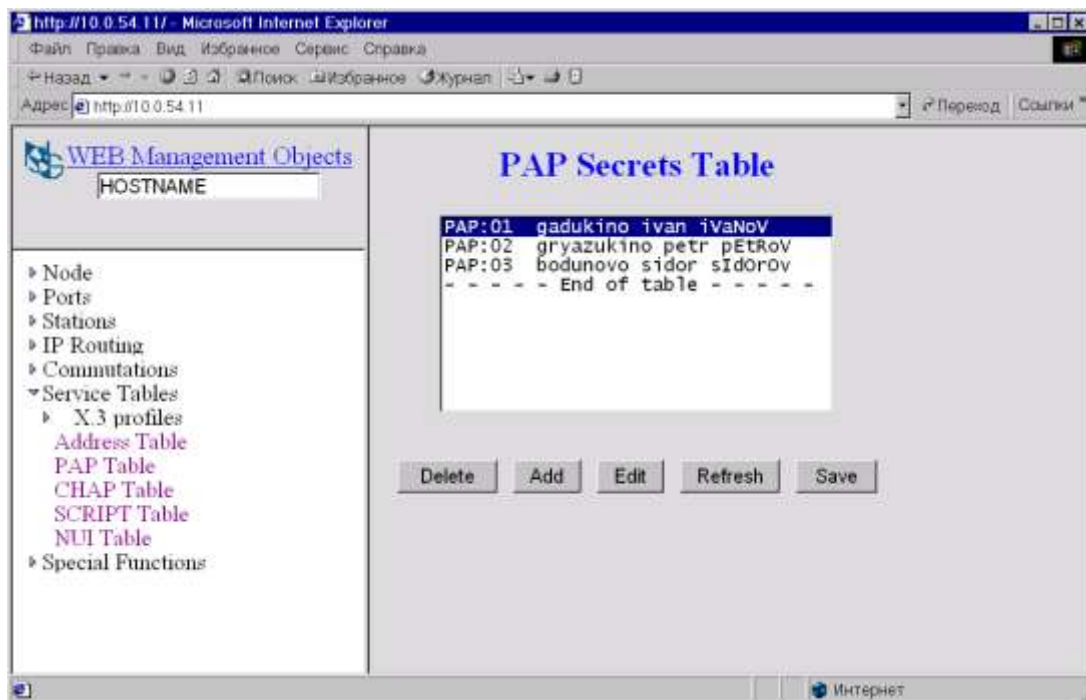
ПРИМЕЧАНИЕ При перезагрузке всего устройства выводится диалоговое окно для подтверждения. Для выполнения перезагрузки необходимо нажать кнопку ОК в этом окне. Перезагрузка занимает несколько секунд, в течение которых устройство будет недоступно.

Кнопка Information выводит информацию о статусе и статистике управляемого объекта. Данная кнопка эквивалентна команде D S (Display Status/Statistics). Информация об объекте выводится однократно на момент выполнения запроса и автоматически не обновляется.

Кнопка Save используется для сохранения текущей конфигурации в энергонезависимой памяти системы. Эквивалентна команде W F (Write Flash). Выполнение этой команды сохраняет текущие значения всех параметров.

Кнопка Clear очищает статистику данного объекта.

В некоторых случаях информация хранится в виде таблиц, состоящих из отдельных записей. К ним относятся, например, таблица статических IP-маршрутов, таблица паролей PAP/CHAP и др. Такая информация выводится в окно также в виде таблицы, каждая строка которой представляет отдельную запись. Над каждым элементом (записью) могут быть произведены следующие действия:



Кнопка Delete — уничтожает выделенную запись.

Кнопка Edit — изменить содержание выделенной записи.

Кнопка Add — добавить новую запись перед выделенной (или в конец таблицы).

Кнопка Refresh — обновить содержимое таблицы на экране.

Кнопка Save — сохранить текущую конфигурацию.

§5.5.6. Ручной ввод команд

Роль Web-интерфейса состоит в том, чтобы генерировать команды с параметрами, установленными в основном окне интерфейса, и передавать эти команды на исполнение модулю Manager. При необходимости пользователь может самостоятельно вводить команды непосредственно в окне Web-браузера — например, если данная команда или параметр не поддерживается в текущей версии Web-интерфейса.

Для ручного ввода команд необходимо выбрать в дереве меню пункт Special Functions —> Manager Command. После этого в правом окне Web-интерфейса открывается форма для ввода командной строки. Для выполнения набранной команды необходимо нажать кнопку Apply.



§5.5.7. Побочные эффекты Web-управления

Web- и SNMP-управление допускают возможность одновременно доступа нескольких администраторов к одному устройству. При этом не исключены ситуации, когда совместное изменение конфигурации устройства может привести к нежелательным последствиям. Чтобы избежать возникновения конфликтных конфигураций, рекомендуется при использовании одного из интерфейсов управления (Web или командную строку) запретить доступ через другие. Web-интерфейс позволяет запретить вход в модуль Manager, а интерфейс командной строки — остановить Web-сервер.

Если во время работы с модулем Manager к данному устройству обращается другой администратор через Web-интерфейс, и если в это время выполняются команды, требующие длительного времени — например, Trace Route (P R), Ping (P P), Display Statistics (D S ... UP:n) — то подключение Web-клиента прервет работу этих команд.

§5.6. Клиент SNTP

Клиент SNTP (Simple Network Time Protocol) реализован в программном обеспечении NSG, начиная с версии 8.1.2. Данная служба обеспечивает автоматическую установку системного времени при включении устройства и его регулярную автоматическую корректировку по заданным серверам SNTP. Её использование особенно актуально в младших сериях NPS–7e и NSG–500, в которых не предусмотрен таймер реального времени (Real Time Clock) и системное время обнуляется при каждом выключении питания устройства.

Для настройки клиента SNTP используется команда:

```
S P SNTP ...
```

со следующими параметрами:

ADM	Административный статус SNTP-клиента: UP или DOWN.
IADR	Собственный IP-адрес SNTP-клиента (в десятичной дотовой нотации). Этот адрес подставляется в качестве исходного (<i>source address</i>) в пакеты запросы к серверу. Если IADR:0.0.0.0, то подставляется адрес IP-интерфейса, через который уходит запрос.
SN:<число>	Число серверов SNTP (от 1 до 4), к которым данный клиент может посылать запросы.
SADR:<ip-адрес>	IP-адрес основного сервера SNTP. Адрес задается в десятичной дотовой нотации.
SADR1, SADR2 ...	IP-адреса резервных серверов SNTP. Число параметров SADRn определяется параметром SN. Если основной сервер, заданный параметром SADR, не отвечает, то запрос сетевого времени посылается серверу SADR1, затем SADR2 и т.д. до конца списка. Критерии для перехода к следующему серверу устанавливаются параметрами TO и RT (см. ниже).
TO:<секунды>	Время ожидания ответа от сервера SNTP (от 1 до 65535). Если за указанное время ответ не получен, посылается повторный запрос.
RT:<число>	Максимальное количество запросов к одному серверу (от 1 до 65535). Если после данного числа запросов ответ от сервера так и не получен, считается, что сервер не доступен, и клиент пытается синхронизировать системное время со следующим сервером.
TA:<минуты>	Периодичность обновления системных часов, в минутах (от 1 до 65535).
TZ:<часы>	Часовой пояс — время в часах, которое добавляется к полученному от сервера времени суток. Стандартные серверы сетевого времени сообщают время по Гринвичу. Допустимые значения от –11 до 12. (Положительная коррекция указывается без знака.)

Все изменения параметров вступают в действие после рестарта клиента командой `W S SNTP`. При выполнении этой команды клиент производит установку системных часов и начинает отсчет интервала TA до следующего обращения к серверам. То же самое происходит при перезагрузке устройства (любым из способов), т.е. время TA всегда отсчитывается от момента последней перезагрузки устройства или рестарта клиента SNTP.

Для проверки конфигурации клиента SNTP используется следующая команда без параметров:

```
D P SNTP
```

Для одноразовой установки системного времени можно использовать команду:

```
S T SNTP
```

По этой команде SNTP-клиент установит системное время, обратившись к серверу(ам) согласно параметрам, заданным командой `S P SNTP`. Параметры TA и ADM будут проигнорированы. Команда `S T SNTP` не влияет на работу SNTP-клиента, то есть время следующего планового запроса к серверу не изменится.

Пример использования SNTP-клиента:

```
S P SNTP ADM:UP IADR:0.0.0.0 TZ:3 TO:10 RT:3 TA:1440 SN:2 SADR:192.5.41.40 SADR1:192.168.0.1
```

По этой команде SNTP-клиент пошлет запрос к серверу 192.5.41.40 и будет ждать ответа 10 секунд. Если за это время сервер не ответит, то будет послан второй запрос. Если сервер не ответит 3 раза, то запрос будет послан серверу 192.168.0.1. (Тоже 3 раза с интервалом 10 секунд). В случае любого положительного ответа, дальнейшие запросы прекращаются, и локальное время вычисляется как время, полученное от сервера, плюс 3 часа. Это значение устанавливается в системные часы, и SNTP-клиент "засыпает" на сутки (1440 минут). Процедура будет повторяться каждые сутки до тех пор, пока не будет введена команда `S P SNTP DOWN`.

Если в ходе выполнения процедуры не получен ответ ни от одного сервера, то системное время не изменяется, а следующий запрос будет послан через время, установленное параметром TA.

По умолчанию, в конфигурации клиента установлены следующие серверы сетевого времени:

SADR:194.149.67.130	ntp.psn.ru	Радиоастрономическая обсерватория ФИАН им. Лебедева, Пушкино, Московская обл.
SADR1:192.43.244.18	time.nist.gov	National Center for Atmospheric Research, Boulder, Colorado
SADR2:192.5.41.40	tick.usno.navy.mil	U.S. Naval Observatory, Washington, DC

и следующие значения остальных параметров:

```
ADM:DOWN IADR:0.0.0.0 TZ:3 TO:10 RT:3 TA:1440 SN:3
```

§5.7. Клиент TFTP

Клиент TFTP (Trivial File Transfer Protocol) реализован в программном обеспечении NSG, начиная с версии 8.1.1, и предназначен для централизованного обновления программного обеспечения с сохранением текущей конфигурации. Для загрузки файла, содержащего новую версию программного обеспечения, с сервера TFTP используется команда Load File:

```
L F IADR:<ip-адрес> FILE:<имя> SIZE:<байт> SADR:<ip-адрес> PORT:<udp> REXMT:<сек> WAIT:<сек>
```

Обязательный параметр IADR (IP Address) задает IP-адрес TFTP-сервера, на котором находится загружаемый файл. Если на устройстве включена и сконфигурирована служба DNS, вместо IP-адреса может быть указано символическое имя сервера.

Параметр FILE указывает имя загружаемого файла. Если этот параметр не указан, по умолчанию берется имя файла, специфическое для данной модели устройства.

ПРИМЕЧАНИЕ Названия файлов с программным обеспечением, поставляемых NSG, соответствуют моделям устройств, например, NSG800_wl.bin. Для устройств серий NX-300, NSG-800 выпускаются несколько модификаций программного обеспечения, предназначенных для использования с интерфейсными модулями IM-E1-x, IM-2E1-x, IM-CE1-x. При установке программного обеспечения по TFTP полученная модификация сравнивается с имеющейся, и разрешается установка только того файла, который соответствует текущей аппаратной конфигурации.

В случае установки/удаления модулей xE1 установка программного обеспечения, соответствующего новой аппаратной конфигурации, производится только локально через консольный порт.

Параметр SIZE содержит размер образа в байтах. По умолчанию берется максимально возможный размер для данной модели.

Параметр SADR (Source Address) задает IP-адрес, который указывается в исходящих пакетах TFTP в качестве адреса источника. Этот параметр требуется в случае, когда загрузка идет через интерфейс, IP-адрес которого неизвестен TFTP-серверу (например, нумерованный интерфейс). Если на устройстве включена и сконфигурирована служба DNS, вместо IP-адреса может быть указано символическое имя данного устройства NSG.

Параметр PORT позволяет выбрать нестандартный порт UDP для подключения к серверу TFTP. По умолчанию используется порт 69.

Параметр REXMT (Retransmit) задает время ожидания перед повтором неподтвержденного пакета, в секундах (по умолчанию — 5 сек).

Параметр WAIT ограничивает общее время ожидания подтверждения пакета, в секундах. По истечении этого времени операция будет прервана (по умолчанию 25 сек).

ПРИМЕЧАНИЕ Прием файла с новой версией программного обеспечения возможен только при наличии достаточного объема свободной оперативной памяти.

Процедура модернизации программного обеспечения и способы решения проблем, связанных с нехваткой оперативной памяти, подробно описаны в [Части 2](#).

ПРИМЕЧАНИЕ При откате с версии программного обеспечения 8.2.0 (или старше) на версию 8.1.2 (или младше) текущая конфигурация устройства становится неработоспособной. В этом случае после загрузки более ранней версии необходимо выполнить процедуру "холодный старт" и сконфигурировать устройство заново с помощью скрипт-файла или вручную.

