

Port серии 6000

Руководство пользователя

Четвертое издание, июнь 2008

The logo for MOXA, featuring the word "MOXA" in a bold, green, sans-serif font. A registered trademark symbol (®) is located to the upper right of the letter "A".

© 2008 Moxa Inc. Все права защищены.

Запрещено воспроизведение данных материалов без соответствующего разрешения.

Официальный дистрибьютор в России

ООО «Ниеншанц-Автоматика»

www.nnz-ipc.ru www.moxa.ru

sales@moxa.ru

support@moxa.ru

Оглавление

1 Введение	8
Обзор	9
Комплект поставки.....	9
NPort 6610/6650.....	9
NPort 6450.....	10
NPort 6150 и NPort 6250	11
Функции устройства	11
Таблица выбора устройства	12
Техническая спецификация.....	13
NPort 6610/6650.....	13
NPort 6450.....	15
NPort 6250, 6250-S-SC и 6250-M-SC.....	16
NPort 6150.....	17
2 Начало работы.....	19
Внешние элементы.....	20
NPort 6610/6650.....	20
NPort 6450.....	21
NPort 6250.....	21
NPort 6150.....	22
Монтаж на стену, на DIN-рейку и в стойку.....	23
Настенный монтаж	23
Монтаж на DIN-рейку	23
Установка в стойку.....	24
Аппаратное подключение.....	24
Требования к электропроводке	24
Подключение питания к NPort 6600-32/16/8-48V	25
Заземление NPort 6600-32/16/8-48V.....	25
Подключение к сети Ethernet.....	25
Подключение последовательных устройств	25
Светодиодные индикаторы.....	26
Регулируемые подтягивающие сопротивления для интерфейса RS-485	27
3 Начальная конфигурация IP адреса	30
Статический и динамический IP-адреса	31
Заводские настройки IP-адреса.....	31
Способы настройки	31
Утилита NPort Search Utility	31

Web-консоль.....	31
Панель оператора (только для NPort 6610, 6650 и 6450).....	31
Протокол ARP.....	32
Telnet-консоль.....	33
Последовательная консоль.....	37
4 Выбор режима работы последовательных портов.....	40
Обзор.....	40
Описание режимов работы NPort 6000.....	41
Режимы Device Control.....	41
Real COM и Secure Real COM.....	41
Reverse Real COM.....	42
RFC2217.....	43
Режимы Socket.....	43
TCP Server и Secure TCP Server.....	43
TCP Client и Secure TCP Client.....	43
UDP.....	44
Режимы Pair Connection и Secure Pair Connection.....	44
Режим Ethernet Modem.....	44
Режимы Terminal.....	45
Terminal ASCII.....	45
Terminal BIN.....	45
SSH.....	45
Режимы Reverse Terminal.....	46
Reverse Telnet.....	47
Reverse SSH.....	47
Режимы Printer.....	47
Режимы Dial In/Out.....	48
Режим Disabled.....	48
5 Настройка через WEB-консоль.....	49
Использование WEB-браузера.....	49
Настройки Browser Cookie.....	49
Установка надежных узлов.....	50
Открытие WEB-консоли.....	52
Навигация в WEB-консоли.....	54
Basic Settings.....	55
Server Settings.....	55
Time Settings.....	55
Network Settings.....	56

Basic Network Settings.....	56
Advanced Network Settings (Расширенные сетевые настройки)	60
Заполнение таблицы маршрутизации	61
6 Настройки модулей.....	65
NM-TX01, NM-TX02, NM-FX01-M-SC, NM-FX01-S-SC, NM-FX02-M-SC, NM-FX02-S-SC	66
Использование резервирования в сегментах Ethernet.....	66
Стандарт STP/RSTP	67
Различия между STP и RSTP	70
Пример STP	70
Настройка режима Turbo Ring	73
Сущность Turbo Ring.....	73
Настройка Turbo Ring 2.....	74
Модуль NM-GPRS/GSM	75
Режим GSM	76
Режим GPRS	78
Режим SMS	79
Модуль NM-Modem	83
7 Настройка режимов работы последовательных портов	85
Port Basic Settings (Основные настройки порта)	86
Device Control Applications (Режимы СОМ-порта)	87
Режим Real COM – «виртуальный СОМ-порт».....	87
Режим Reverse Real COM.....	91
Socket Applications (Режимы сокетов).....	95
TCP Server.....	95
TCP Client	99
UDP	102
Режим Pair Connection (Парного соединения).....	104
Pair Connection Master (мастер парного соединения).....	104
Pair Connection Slave (ведомое устройство парного соединения)	105
Режим Ethernet Modem.....	106
Terminal Applications (Терминал)	109
ASCII-терминал (TERM_ASC).....	109
BIN-терминал (TERM_BIN)	111
SSH.....	113
Reverse Terminal Applications (Инверсный терминал).....	114
Reverse Telnet	114
Reverse SSH	116
Printer Applications (приложения печати)	117

RAW PRN	117
LPD PRN	118
Приложения Dial In/Out	119
Режим PPP	119
Режим PPPD	120
Режим SLIP	122
Режим SLIPD	123
Режим Dynamic	124
Disabled (последовательный порт отключен)	125
8 Дополнительные настройки последовательных портов	126
Port Communication Parameters (Настройки связи порта)	127
Serial parameters (Параметры последовательной передачи данных)	127
Port Data Buffering/Log (буферизация/запись данных последовательного порта)	128
Port Modem Settings (Настройки модемного соединения)	129
Port Cipher Settings (Настройки шифрования)	130
Welcome Message (Приветственное сообщение)	131
9 Системные настройки	132
Misc. Network Settings (Прочие сетевые настройки)	133
Accesible IP List (список разрешенных IP-адресов)	133
SNMP Agent Settings (настройки для SNMP-агента)	134
DDNS	135
Host Table	135
User Table (таблица пользователей)	136
Authentication Server (Сервер авторизации)	137
System Log Settings (настройки системных записей)	137
Configure the Remote Log Server (настройка удаленного сервера записей)	139
Auto Warning Settings (Настройки автооповещения)	140
Event Settings (настройки событий)	140
Serial Event Settings (настройки событий по последовательным портам)	141
E-mail Alert (оповещения по электронной почте)	142
SNMP Trap (прерывания по SNMP)	143
Maintenance (Функции технического обслуживания и диагностики)	144
Console Setting (консольные настройки)	144
Ping (проверка связи с другими хостами)	145
Firmware Upgrade (обновление прошивки)	146
Configuration Import/Export (импорт/экспорт настроек)	147
Load Factory Defaults (Загрузить заводские настройки)	148
Change Password (Изменить пароль)	148

Certificate	149
Ethernet SSL Certificate Import	149
Certificate/Key Delete	149
System Monitoring	150
Serial to Network Connections (Соединения между последовательными и Ethernet-портами)	150
Serial Port Status (Состояние последовательного порта)	151
Serial Port Error Count (счетчик ошибок последовательных портов)	151
Serial Port Settings (Параметры последовательной связи)	152
Serial Cipher Usage Status (статус использования последовательного шифра)	152
Network Connections (Ethernet-соединения)	153
System Monitor/System Status/Network Module	153
Network Statistics	154
Serial Data Log	155
System Log	156
Routing	157
Dout State (для 6450/6650)	158
Save Configuration (Сохранение настроек)	159
Restart (Перезапуск)	160
Restart System (Перезапуск системы)	160
Restart Ports (Перезагрузка портов)	160
10 Установка/настройка программного обеспечения	161
Обзор	162
NPort Windows Driver Manager	163
Установка утилиты	163
Работа с утилитой	166
NPort Search Utility	178
Установка утилиты	178
Настройка	180
Linux Real TTY Drivers	182
Основная последовательность действий	182
Аппаратная установка	182
Установка файлов Linux Real TTY Driver	182
Создание TTY-портов	183
Удаление TTY-портов	184
Удаление файлов Linux Real TTY Driver	184
Unix Fixed TTY Driver	184
Установка Unix Driver	184

Настройка Unix Driver	185
Приложение А Распиновка и разводка кабеля	187
Распиновка порта.....	188
RS-232/422/485 («Папа» DB9)	188
RS-232/422/485 («Папа» RJ45)	188
Распайка кабелей	189
Ethernet-кабели.....	189
Кабели для интерфейса RS-232	189
Кабели для интерфейса RS-422/4-хпровод. RS-485	191
Кабели для двухпровод. RS-485	193
Распиновка разъемов DB9 и DB25	194
Приложение В RFC2217	195
Приложение С DDNS-сервер	196
Обзор	196
Настройка	197
Приложение D Стандартная нумерация портов	198
Приложение E SNMP-агент с поддержкой MIB II и RS-232	201
RFC1213 MIB-II – SNMP-переменные	202
RFC1317 RS-232 Like Groups	204
Моха-NP6000-MIB	204
Приложение F RADIUS-сервер	211
О протоколе RADIUS.....	212
Определение	212
Архитектура «Клиент/Сервер».....	212
Настройка NPort 6000	213
Задание IP-адреса RADIUS-сервера	213
Настройка последовательного порта	213
Настройка UNIX-хостов	213
Настройка в ОС Windows NT	214
Настройка в ОС Windows 2000	216
Настройка в ОС Windows 2003	219

1 Введение

Серия устройств NPort 6000 дополнена некоторыми функциями. В настоящее время модельный ряд NPort 6000 представлен 17-ю типами асинхронных последовательных серверов с функциями безопасности. Различаются они в основном числом портов и возможностями сетевых подключений. Вся представленная информация по настройкам применима ко всем устройствам серии Nport 6000. Особенности конкретных устройств будет уделено отдельное внимание. Для полного представления о различиях устройств серии NPort 6000 см. параграф Таблица выбора изделия.

Данная глава содержит следующие разделы:

- **Обзор**
- **Комплект поставки**
 - NPort 6610/6650
 - NPort 6450
 - NPort 6150 и NPort 6250
- **Функции устройства**
- **Таблица выбора устройства**
- **Техническая спецификация**
 - NPort 6610/6650
 - NPort 6450
 - NPort 6250, 6250-S-SC и 6250-M-SC
 - NPort 6150

Обзор

NPort 6000 используется для подключения любых устройств с последовательным интерфейсом в сети Ethernet и поддерживает различные режимы работы. Также NPort 6000 имеет дополнительные режимы с функциями безопасности: Secure TCP Server, Secure TCP Client, Secure Pair Connection и Secure Real COM – для задач, где необходимо защитить информацию (в банковской сфере, телефонии, контроле доступа и удаленном управлении сайтом).

NPort 6000 имеет функцию Any Baudrate, которую можно использовать для подключения последовательного устройства на любой нестандартной скорости и в любом режиме.

Например, для некоторых специальных задач может потребоваться скорость соединения 500 Кбит/с. Многие серверы могут быть настроены только на скорость 460,8 Кбит/с, в результате получается ошибка рассогласования скорости 7,84%. Для последовательного канала обмена допустимая ошибка – 3%. NPort 6000 позволяет более точно выставлять скорость соединения и может быть настроен на скорость 491,5 Кбит/с. Ошибка в этом случае составляет всего 1,7%, что вполне подходит для последовательной передачи данных.

В некоторых задачах данные не должны теряться даже в случае разрыва соединения. NPort 6000 предоставляет возможности по обеспечению надежного сохранения данных в буферной памяти. Когда возникает проблема с сетевым соединением, данные сохраняются в NPort'e 6000. При возобновлении Ethernet-соединения сохраненные в буфере данные будут отправлены получателю. По умолчанию объем буфера на каждый последовательный порт составляет 64 Кбайт. Для моделей NPort 6610, NPort 6250, NPort 6450 и NPort 6650 пользователи могут воспользоваться дополнительной SD-картой памяти для увеличения объема буфера.

Комплект поставки

Каждый NPort 6000 поставляется в отдельной коробке с рядом стандартных аксессуаров. Кроме того, могут быть заказаны некоторые дополнительные модули. При получении устройства внимательно проверьте его комплектность и сообщите представителю Moxa об отсутствующих или поврежденных элементах.

NPort 6610/6650

Существует 6 моделей NPort 6610 и 6 моделей NPort 6650:

Модель	Количество последовательных портов		Требования по питанию
NPort 6610-8	8	RS-232	100-240 В перем., шнур питания
NPort 6610-16	16		
NPort 6610-32	32		
NPort 6610-8-48V	8	RS-232	±48 В пост. (от 20 до 72 В пост., от -40 до -72 В пост.), клеммный блок
NPort 6610-16-48V	16		
NPort 6610-32-48V	32		
NPort 6650-8	8	RS-232/422/485	100-240 В перем., шнур питания
NPort 6650-16	16		
NPort 6650-32	32		
NPort 6650-8-48V	8	RS-232/422/485	±48 В пост. (от 20 до 72 В пост., от -40 до -72 В пост.), клеммный блок
NPort 6650-16-48V	16		
NPort 6650-32-48V	32		

Стандартная комплектация для NPort 6610 и Nport 6650

- Краткая инструкция по установке
- 2 зажима для установки в стойку
- Шнур питания (только для питания перем.)
- Переходник CBL-RJ45M9-150 с разъема RJ45 на DB9, «папа» – 1 шт.
- Гарантия на изделие

Кабельные переходники для NPort 6610 и NPort 6650 (могут быть заказаны отдельно)

- CBL-RJ45M9-150 (8-конт. RJ45 на DB9, “папа”; 150 см)
- CBL-RJ45F9-150 (8-конт. RJ45 на DB9, “мама”; 150 см)
- CBL-RJ45M25-150 (8-конт. RJ45 на DB25 “папа”; 150 см)
- CBL-RJ45M25-150 (8-конт. RJ45 на DB25 “мама”; 150 см)

Дополнительные модули для NPort 6610 и NPort 6650 (заказываются отдельно)

NM-TX01: Ethernet-модуль с одним портом RJ45 (поддерживает 10/100BaseTX, соединение в цепочку и резервирование RSTP/STP)

NM-TX02: Ethernet-модуль с двумя портами RJ45 (поддерживает 10/100BaseTX, соединение в цепочку и резервирование RSTP/STP)

NM-FX01-S-SC: Ethernet-модуль с одним портом с SC-разъемом для одномодового оптоволокна (поддерживает 10/100BaseFX, соединение в цепочку и резервирование RSTP/STP)

NM-FX01-M-SC: Ethernet-модуль с одним портом с SC-разъемом для многомодового оптоволокна (поддерживает 10/100BaseFX, соединение в цепочку и резервирование RSTP/STP)

NM-FX02-S-SC: Ethernet-модуль с двумя портами с SC-разъемами для одномодового оптоволокна (поддерживает 10/100BaseFX, соединение в цепочку и резервирование RSTP/STP)

NM-FX02-M-SC: Ethernet-модуль с двумя портами с SC-разъемами для многомодового оптоволокна (поддерживает 10/100BaseFX, соединение в цепочку и резервирование RSTP/STP)

NM-GPRS/GSM: модуль GPRS/GSM-модема

NM-Modem: модуль модема V.92 на скорость 56 К.

NPort 6450

Существует единственная модель NPort 6450:

Модель	Количество последовательных портов	Требования по питанию
NPort 6450	4 (RS-232/422/485)	100-240 В перем., адаптер питания

Стандартная комплектация для NPort 6450

- Краткая инструкция по установке
- Адаптер питания
- Гарантия на изделие
- 2 ушка для крепления на стену

Элементы для крепления на DIN-рейку для NPort 6450 (приобретаются отдельно)

- Комплект крепежа DK-35A на DIN-рейку (35 мм)
- Блок питания на DIN-рейку

Дополнительные модули для NPort 6450 (заказываются отдельно)

- NM-TX01: Ethernet-модуль с одним портом RJ45 (поддерживает 10/100BaseTX, соединение в цепочку и резервирование RSTP/STP)
- NM-TX02: Ethernet-модуль с двумя портами RJ45 (поддерживает 10/100BaseTX, соединение в цепочку и резервирование RSTP/STP)

- NM-FX01-S-SC: Ethernet-модуль с одним портом с SC-разъемом для одномодового оптоволоконна (поддерживает 10/100BaseFX, соединение в цепочку и резервирование RSTP/STP)
- NM-FX01-M-SC: Ethernet-модуль с одним портом с SC-разъемом для многомодового оптоволоконна (поддерживает 10/100BaseFX, соединение в цепочку и резервирование RSTP/STP)
- NM-FX02-S-SC: Ethernet-модуль с двумя портами с SC-разъемами для одномодового оптоволоконна (поддерживает 10/100BaseFX, соединение в цепочку и резервирование RSTP/STP)
- NM-FX02-M-SC: Ethernet-модуль с двумя портами с SC-разъемами для многомодового оптоволоконна (поддерживает 10/100BaseFX, соединение в цепочку и резервирование RSTP/STP)
- NM-GPRS/GSM: модуль GPRS/GSM-модема
- NM-Modem: модуль модема V.92 на скорость 56 К.

NPort 6150 и NPort 6250

Есть одна модель NPort 6150 и три разновидности NPort 6250:

Модель	Количество последовательных портов	Требования по питанию
NPort 6150	1	100-240 В перем., адаптер
NPort 6250	2	100-240 В перем., адаптер
NPort 6250-M-SC	2	100-240 В перем., адаптер
NPort 6250-S-SC	2	100-240 В перем., адаптер

Стандартная комплектация для NPort 6610 и Nport 6650

- Краткая инструкция по установке
- Адапте питания
- Гарантия на изделие
- 2 ушка для крепления на стену

Элементы для крепления на DIN-рейку для NPort 6450 (приобретаются отдельно)

- Комплект крепежа DK-35A на DIN-рейку (35 мм)
- Блок питания на DIN-рейку

Функции устройства

Все устройства серии NPort 6000 характеризуются следующими особенностями:

- Режимы работы с функциями защиты данных: Secure Real COM, Secure TCP Server, Secure TCP Client и Secure Pair Connection.
- Различные режимы работы с сокетом, включая TCP Server, TCP Client, UDP и Real COM-драйвер.
- Функция буферизации данных для предотвращения их потери при разрыве соединения.
- Удаленная настройка через HTTPS и SSH.
- Скорости обмена через последовательные порты – до 921,6 Кбит/с
- Возможность резервирования Ethernet (технологии STP, RSTP, Turbo Ring и Turbo Ring v2)
- Возможность резервной передачи через сотовый GSM/GPRS-модем или модем V.92
- Функция Any Vaudrate – для упрощения настройки нестандартной скорости обмена.

Таблица выбора устройства

Таблица ниже показывает отличия между различными моделями NPort 6000:

Модель	Число посл. портов	Послед. интерфейсы	Питание	Корпус	Встр. сетевой интерфейс	Доп. сет. Модули	Индикатор и реле-аларм	Разъем для SD
6150	1	RS-232/422/485	100-240 В перем.	Алюм. (1 мм)	Ethernet	---	---	---
6250	2	RS-232/422/485	100-240 В перем.	Алюм. (1 мм)	Ethernet	---	---	+
6250-M-SC	2	RS-232/422/485	100-240 В перем.	Алюм. (1 мм)	Многомод. оптовол.	---	---	+
6250-S-SC	2	RS-232/422/485	100-240 В перем.	Алюм. (1 мм)	Одномод. оптовол.	---	---	+
6450	4	RS-232/422/485	100-240 В перем.	Алюм. (1 мм)	Ethernet	+	+	+
6610-8	8	RS-232	100-240 В перем.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6610-16	16	RS-232	100-240 В перем.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6610-32	32	RS-232	100-240 В перем.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6610-8-48V	8	RS-232	±48 В пост.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6610-16-48V	16	RS-232	±48 В пост.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6610-32-48V	32	RS-232	±48 В пост.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6650-8	8	RS-232/422/485	100-240 В перем.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6650-16	16	RS-232/422/485	100-240 В перем.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6650-32	32	RS-232/422/485	100-240 В перем.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6650-8-48V	8	RS-232/422/485	±48 В пост.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6650-16-48V	16	RS-232/422/485	±48 В пост.	Тонкол. ст. (1мм)	Ethernet	+	+	+
6650-32-48V	32	RS-232/422/485	±48 В пост.	Тонкол. ст. (1мм)	Ethernet	+	+	+

Техническая спецификация

NPort 6610/6650

LAN

Ethernet	10/100 Мбит/с, RJ45
Защита	Изоляция на 1,5 кВ

Оптоволокно (для моделей с дополнительными сетевыми модулями)

Дальность	Многомод: от 0 до 2 км, 1310 нм (62,5/125 мкм, 500 МГц*км) Одномод: от 0 до 40 км, 1310 нм (9/125 мкм, 3,5PS/(нм*км))
Мин. мощность передатчика	Многомод: -20 дБмВт; Одномод: -5 дБмВт
Макс.мощность передатчика	Многомод: -14 дБмВт; Одномод: 0 дБмВт
Чувствительность приемника	Многомод: от -34 до -30 дБмВт Одномод: от -36 до -32 дБмВт

GPRS/GSM (для дополнительных GPRS/GSM-модулей)

Поддерживаемые стандарты	GSM и GPRS
Частотные диапазоны	850/900/1800/1900 МГц
Мощность передатчика	1 Вт для GSM 1800/1900, 2 Вт EGSM 900/GSM 850
Класс многоканального GPRS	Class 10, Алгоритмы кодирования: CS1 – CS4
Класс терминальных GPRS-устр.	Class B
Скорость передачи данных CSD	до 14400 бит/с
SMS	Точка-точка, текстовый формат или PDU: Mobile Oriented (MO) и Mobile Terminated (MT Cell Broadcast: множ. рассылка в соответствии с GSM 07.05)
SIM Control	3,3 В / 1,8 В

Последовательный интерфейс

Число портов	8 портов (модели NPort 6610-8, NPort 6650-8) 16 портов (модели NPort 6610-16, NPort 6650-16) 32 портов (модели NPort 6610-32, NPort 6650-32)
Интерфейс	NPort 6610: RS-232 (8-конт. RJ45) NPort 6650: RS-232/422/485 (8-конт. RJ45)

Параметры последовательного канала связи

Контроль четности	Нет, Четность, Нечетность, Пробел, Метка
Биты данных	5, 6, 7, 8
Стоповые биты	1, 1.5, 2
Контроль направления потока	RTS/CTS, XON/XOFF, DTR/DSR
Скорость обмена	от 50 бит/с до 921.6 Кбит/с
Консольный порт	1 x RS-232

Дополнительное расширение объема памяти

SD-карта	1 разъем
----------	----------

Программные особенности

Протоколы	ICMP, IP, TCP, UDP, DHCP, BOOTP, Telnet, DNS, SNMP, DDNS, HTTP, SMTP, HTTPS, SSL, SSH, PPPoE, RFC2217, IPv6, IPv4, Turbo Ring, Turbo Ring 2
Утилиты	NPort Search Utility for Windows 98/ME/NT/2000/XP/2003/Vista/XP x64/ Vista x64
Протоколы шифрования	DES/3DES/AES
Драйверы для ОС	Real COM drivers: Windows 95/98/ME/NT/2000/XP/x64/2003/2003 x64/Vista/Vista x64 Real TTY driver: Linux Fixed TTY drivers: SCO Unix, SCO OpenServer 5, OpenServer 6, UnixWare 7, UnixWare 2.1, SVR 4.2, QNX 4.25, QNX 6, Solaris 10, FreeBSD 5, FreeBSD 6
Способы настройки	Через WEB-консоль, через последовательную/телнет-консоль. Примечание: с помощью Windows-утилиты можно обнаруживать устройства в сети, назначать IP, обновлять прошивку

Требования к питанию

Вход питания	100 – 240 В перем., от 47 до 63 Гц ±48 В пост. (от 20 до 72 В пост., от -20 до -72 В пост.)
Потребляемая мощность	NPort 6610-8/16/32: 285 мА @ 100 В перем.; 190 мА @ 240 В перем. NPort 6610-8/16/32-48V: 293 мА @ 48 В пост. NPort 6650-8/16/32: 285 мА @ 100 В перем.; 190 мА @ 240 В перем. NPort 6610-8/16/32-48V: 293 мА @ 48 В пост.

Конструктивные особенности

Материал корпуса	листовой металл SECC (1 мм)
Условия окружающей среды	
Рабочий диапазон температур	от 0 до 55° C (от 32 до 131° F), относит. влаж.: от 5 до 95%
Температура хранения	от -20 до 85° C (от -4 до 158° F), относ. влаж.: от 5 до 95%

Сертификаты

EMC (электромагн. совместимость)	FCC Class A, CE Class A
Безопасность	UL, CUL, TUV

NPort 6450

LAN

Ethernet 10/100 Мбит/с, RJ45

Защита Изоляция на 1,5 кВ

Оптическое волокно (для моделей с дополнительными сетевыми модулями)

Дальность Многомод: от 0 до 2 км, 1310 нм (62,5/125 мкм, 500 МГц*км)

Одномод: от 0 до 40 км, 1310 нм (9/125 мкм, 3,5PS/(нм*км))

Мин. мощность передатчика Многомод: -20 дБмВт; Одномод: -5 дБмВт

Макс.мощность передатчика Многомод: -14 дБмВт; Одномод: 0 дБмВт

Чувствительность приемника Многомод: от -34 до -30 дБмВт
Одномод: от -36 до -32 дБмВт

GPRS/GSM (для дополнительных GPRS/GSM-модулей)

Поддерживаемые стандарты GSM и GPRS

Частотные диапазоны 850/900/1800/1900 МГц

Мощность передатчика 1 Вт для GSM 1800/1900, 2 Вт EGSM 900/GSM 850

Класс многоканального GPRS Class 10, Алгоритмы кодирования: CS1 – CS4

Класс терминальных GPRS-устр. Class B

Скорость передачи данных CSD до 14400 бит/с

SMS Точка-точка, текстовый формат или PDU: Mobile Oriented (MO) и Mobile Terminated (MT Cell Broadcast: множ. рассылка в соответствии с GSM 07.05)

SIM Control 3,3 В / 1,8 В

Последовательный интерфейс

Число портов 4

Интерфейс RS-232/422/485 (DB9, «папа»)

Параметры последовательного канала связи

Контроль четности Нет, Четность, Нечетность, Пробел, Метка

Биты данных 5, 6, 7, 8

Стоповые биты 1, 1.5, 2

Контроль направления потока RTS/CTS, XON/XOFF, DTR/DSR

Скорость обмена от 50 бит/с до 921.6 Кбит/с

Консольный порт 1 x RS-232 (Порт №1)

Дополнительное расширение объема памяти

SD-карта 1 разъем

Программные особенности

Протоколы	ICMP, IP, TCP, UDP, DHCP, BOOTP, Telnet, DNS, SNMP, DDNS, HTTP, SMTP, HTTPS, SSL, SSH, PPPoE, IPv6, IPv4, Turbo Ring, Turbo Ring 2
Утилиты	NPort Search Utility for Windows 98/ME/NT/2000/XP/2003/Vista/XP x64/ Vista x64
Протоколы шифрования	DES/3DES/AES
Драйверы для ОС	Real COM drivers: Windows 95/98/ME/NT/2000/XP/x64/2003/2003 x64/Vista/Vista x64 Real TTY driver: Linux Fixed TTY drivers: SCO Unix, SCO OpenServer 5, OpenServer 6, UnixWare 7, UnixWare 2.1, SVR 4.2, QNX 4.25, QNX 6, Solaris 10, FreeBSD 5, FreeBSD 6
Способы настройки	Через WEB-консоль, через последовательную/телнет-консоль. Примечание: с помощью Windows-утилиты можно обнаруживать устройства в сети, назначать IP, обновлять прошивку

Требования к питанию

Вход питания 12-48 в пост.

Потребляемая мощность 730 мА (при 12 В)

Конструктивные особенности

Материал корпуса листовой металл SECC (1 мм)

Условия окружающей среды

Рабочий диапазон температур от 0 до 55° C (от 32 до 131° F), относит. влаж.: от 5 до 95%

Температура хранения от -20 до 85° C (от -4 до 158° F), относ. влаж.: от 5 до 95%

Сертификаты

EMC (электромагн. совместимость) FCC Class A, CE Class A

Безопасность UL, CUL, TUV

NPort 6250, 6250-S-SC и 6250-M-SC

LAN

Ethernet	NPort 6250	10/100 Мбит/с, RJ45
	NPort 6250-S-SC	одномодовое оптоволокно
	NPort 6250-M-SC	многомодовое оптоволокно
Защита	Изоляция на 1,5 кВ	

Последовательный интерфейс

Число портов	2
Интерфейс	RS-232/422/485 (DB9, «папа»)

Параметры последовательного канала связи

Контроль четности	Нет, Четность, Нечетность, Пробел, Метка
Биты данных	5, 6, 7, 8
Стоповые биты	1, 1.5, 2
Контроль направления потока	RTS/CTS, XON/XOFF, DTR/DSR

Скорость обмена	от 50 бит/с до 921.6 Кбит/с
Консольный порт	1 x RS-232 (Порт №1)
Программные особенности	
Протоколы	ICMP, IP, TCP, UDP, DHCP, BOOTP, Telnet, DNS, SNMP, DDNS, HTTP, SMTP, HTTPS, SSL, SSH, PPPoE, IPv6, IPv4
Утилиты	NPort Search Utility for Windows 98/ME/NT/2000/XP/2003/Vista/XP x64/ Vista x64
Протоколы шифрования	DES/3DES/AES
Драйверы для ОС	Real COM drivers: Windows 95/98/ME/NT/2000/XP/x64/ 2003/2003 x64/Vista/Vista x64 Real TTY driver: Linux Fixed TTY drivers: SCO Unix, SCO OpenServer 5, OpenServer 6, UnixWare 7, UnixWare 2.1, SVR 4.2, QNX 4.25, QNX 6, Solaris 10, FreeBSD 5, FreeBSD 6
Способы настройки	Через WEB-консоль, через последовательную/телнет-консоль. Примечание: с помощью Windows-утилиты можно обнаруживать устройства в сети, назначать IP, обновлять прошивку
Требования к питанию	
Вход питания	12-48 В пост.
Потребляемый ток	285 мА (при 12 В)
Конструктивные особенности	
Материал корпуса	алюминий (1 мм)
Условия окружающей среды	
Рабочий диапазон температур	от 0 до 55° С (от 32 до 131° F), относит. влаж.: от 5 до 95%
Температура хранения	от -20 до 85° С (от -4 до 158° F), относ. влаж.: от 5 до 95%
Сертификаты	
EMC (электромагн. совместимость)	FCC Class A, CE Class A
Безопасность	UL, CUL, TUV

NPort 6150

LAN

Ethernet	10/100 Мбит/с, RJ45
Защита	Изоляция на 1,5 кВ

Последовательный интерфейс

Число портов	1
Интерфейс	RS-232/422/485 (DB9, «папа»)

Параметры последовательного канала связи

Контроль четности	Нет, Четность, Нечетность, Пробел, Метка
Биты данных	5, 6, 7, 8
Стоповые биты	1, 1.5, 2

Контроль направления потока	RTS/CTS, XON/XOFF, DTR/DSR
Скорость обмена	от 50 бит/с до 921.6 Кбит/с
Консольный порт	1 x RS-232 (Порт №1)
Дополнительное расширение объема памяти	
SD-карта	1 разъем
Программные особенности	
Протоколы	ICMP, IP, TCP, UDP, DHCP, BOOTP, Telnet, DNS, SNMP, DDNS, HTTP, SMTP, HTTPS, SSL, SSH, PPPoE, IPv6, IPv4, Turbo Ring, Turbo Ring 2
Утилиты	NPort Search Utility for Windows 98/ME/NT/2000/XP/2003/Vista/XP x64/ Vista x64
Протоколы шифрования	DES/3DES/AES
Драйверы для ОС	Real COM drivers: Windows 95/98/ME/NT/2000/XP/x64/2003/2003 x64/Vista/Vista x64 Real TTY driver: Linux Fixed TTY drivers: SCO Unix, SCO OpenServer 5, OpenServer 6, UnixWare 7, UnixWare 2.1, SVR 4.2, QNX 4.25, QNX 6, Solaris 10, FreeBSD 5, FreeBSD 6
Способы настройки	Через WEB-консоль, через последовательную/телнет-консоль. Примечание: с помощью Windows-утилиты можно обнаруживать устройства в сети, назначать IP, обновлять прошивку
Требования к питанию	
Вход питания	12-48 в пост.
Потребляемая мощность	730 мА (при 12 В)
Конструктивные особенности	
Материал корпуса	листовой металл SECC (1 мм)
Условия окружающей среды	
Рабочий диапазон температур	от 0 до 55° C (от 32 до 131° F), относит. влаж.:от 5 до 95%
Температура хранения	от -20 до 85° C (от -4 до 158° F), относ. влаж.: от 5 до 95%
Сертификаты	
EMC (электромагн. совместимость)	FCC Class A, CE Class A
Безопасность	UL, CUL, TUV

2 Начало работы

В главе даны указания по аппаратной установке NPort 6000. Программная настройка описывается в следующих главах.

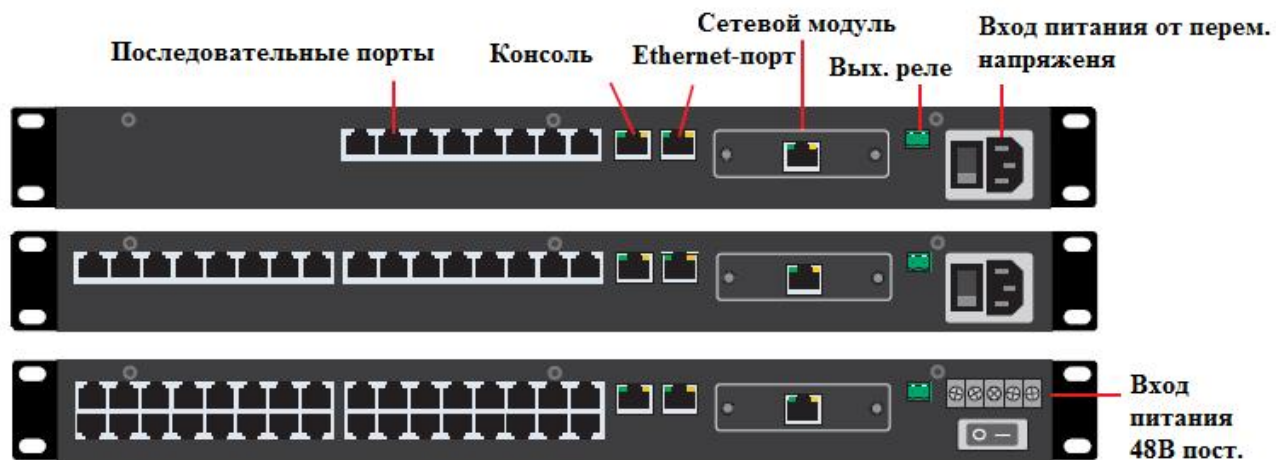
Глава содержит следующие разделы:

- **Внешние элементы**
 - NPort 6610/6650
 - NPort 6450
 - NPort 6250
 - NPort 6150
- **Монтаж на стену, на DIN-рейку и в стойку**
 - Настенный монтаж
 - Монтаж на DIN-рейку
 - Установка в стойку
- **Аппаратное подключение**
 - Требования к электропроводке
 - Подключение питания к NPort 6600-32/16/8-48V
 - Заземление NPort 6600-32/16/8-48V
 - Подключение к сети Ethernet
 - Подключение последовательных устройств
 - Светодиодные индикаторы
 - Регулируемые подтягивающие сопротивления для интерфейса RS-485

Внешние элементы

NPort 6610/6650

Виды сзади



Вид сверху



Виды спереди



Дополнительные сетевые модули

Порты Ethernet (разъем RJ45)



Порты для оптоволоконна



GPRS/GSM

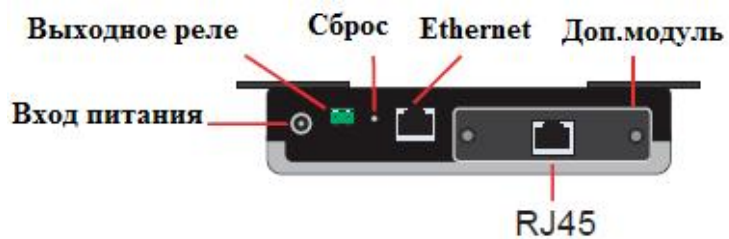


Modem



NPort 6450

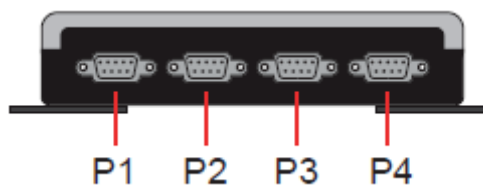
Вид сзади



Вид сверху

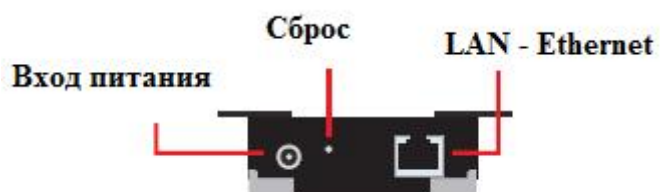


Вид спереди



NPort 6250

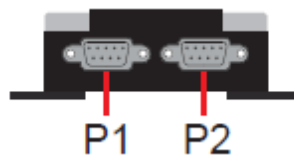
Вид сзади



Вид сверху

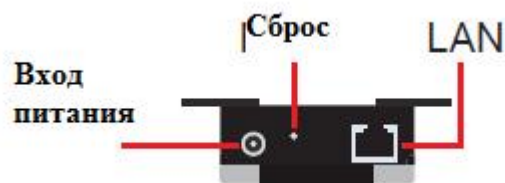


Вид спереди



NPort 6150

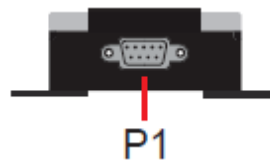
Вид сзади



Вид сверху



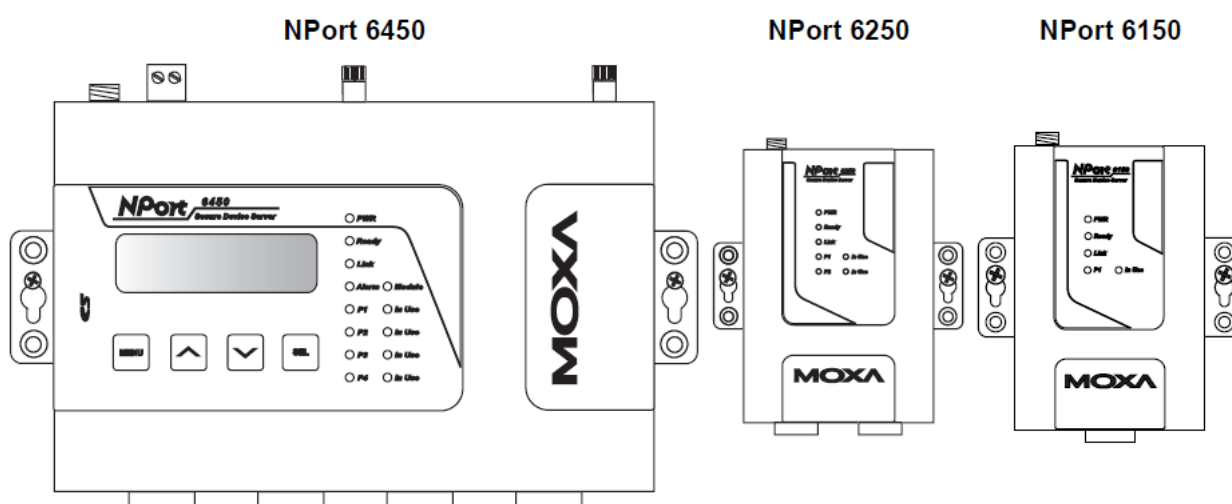
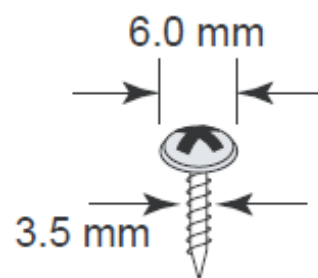
Вид спереди



Монтаж на стену, на DIN-рейку и в стойку

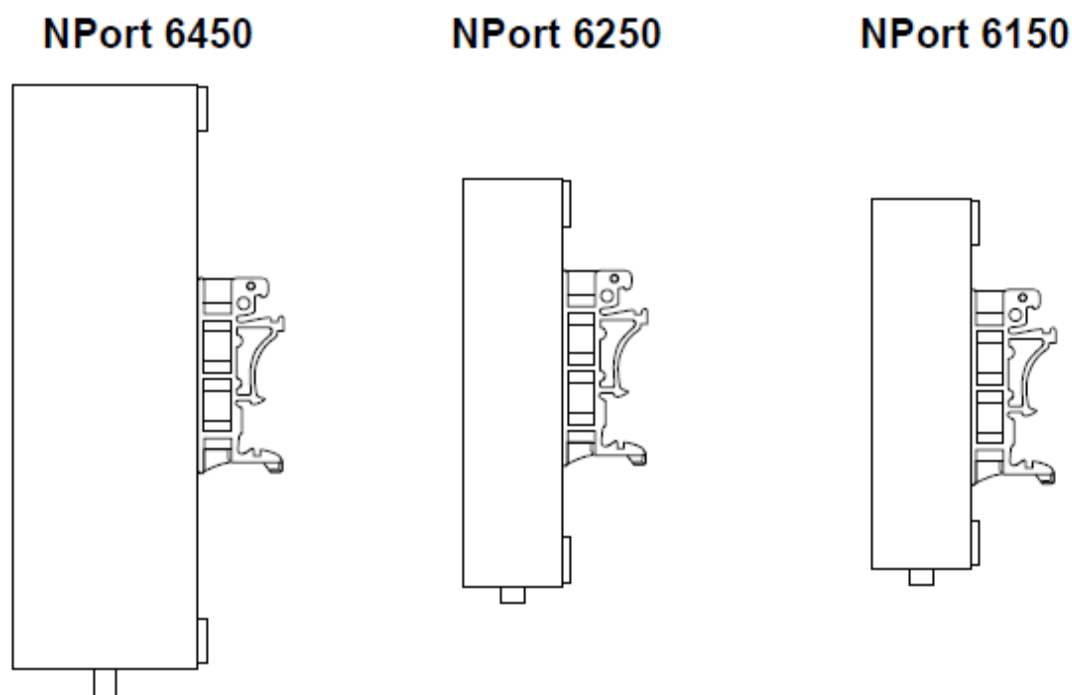
Настенный монтаж

На NPort'ах 6150, 6250 и 6450 есть крепеж для монтажа на стену или плоскую поверхность какого-либо корпуса. Для крепления используются два винта. Диаметр головки винта должен быть менее 6 мм, диаметр стержня – менее 3,5 мм.



Монтаж на DIN-рейку

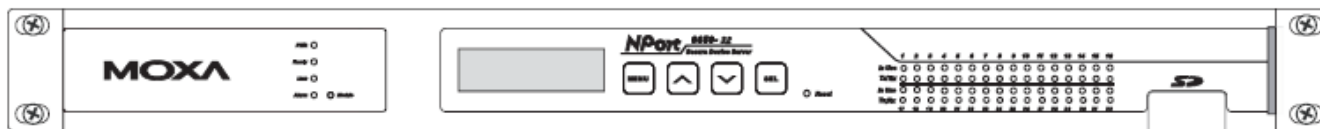
Крепеж на DIN-рейку приобретается для моделей NPort 6150, 6250 и 6450 отдельно. При установке на DIN-рейку убедитесь, чтобы пружина находилась сверху.



Установка в стойку

Для установки NPort 6610/6650 в стойку используйте 4 винта.

NPort 6610/6650



Аппаратное подключение

Требования к электропроводке



ВНИМАНИЕ

Отключайте питание перед любыми переподключениями
Отключайте шнур питания перед установкой и/или действиями с электропроводкой NPort'a 6000.

Ток, идущий через провода, не должен превышать максимально допустимый

Рассчитывайте максимально возможный ток на каждый провод и общий. Придерживайтесь всех электрических правил и норм, указывающих максимально допустимый ток для каждого размера провода.

Превышение максимального тока может вызвать перегрев проводов и привести к повреждениям оборудования.

Работающее устройство может сильно нагреться, используйте меры предосторожности при взятии его в руки.

Будьте осторожны. Внутренние элементы NPort 6000 выделяют тепло и могут вызывать нагревание устройства.

Следует придерживаться следующих общих рекомендаций:

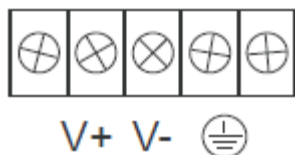
- Использовать отдельные пути для прокладки проводов питания и сигнальных. Если необходимо их пересечение, постарайтесь обеспечить их взаимную перпендикулярность в точке пересечения.

ПРИМЕЧАНИЕ: Не используйте для прокладки сигнальных проводов и питания одни и те же желобки. Во избежание наводок провода с разными характеристиками сигналов следует прокладывать отдельно друг от друга.

- Тип передаваемого сигнала определяет, какие провода должны быть проложены отдельно. Провода со сходными электрическими характеристиками могут быть сгруппированы.
- Провода передачи входных и выходных сигналов следует прокладывать отдельно друг от друга.
- Полезно маркировать кабели от всех устройств в системе.

Подключение питания к NPort 6600-32/16/8-48V

Для подключения питания к NPort 6600-32/16/8-48V через клеммный блок выполните следующие действия:



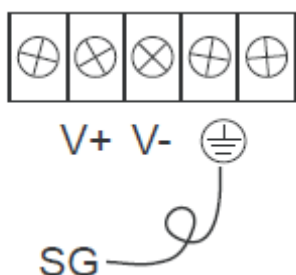
1. Послабьте винты клемм V+ и V- терминального блока.
2. Подключите «+» источника 48 В пост. к V+, а проводок заземления к V-, затем затяните винты. (Примечание: устройства NPort 6600-32/16/8-48V имеют защиту от неправильной полярности).

Если питание подключено правильно, индикатор «Ready» загорится красным цветом, после полной загрузки устройства индикатор «Ready» становится зеленым.

ПРИМЕЧАНИЕ Следует прикладывать крутящий момент затяжки винта не более 8 кг-см и диаметр проводов 22-14 AWG при подключении питания к клеммному блоку NPort 6600-32/16/8-48V.

Заземление NPort 6600-32/16/8-48V

Заземление и правильная прокладка кабелей позволяет снизить влияние помех и электромагнитных наводок. Прокладывайте провода заземления перед подключением устройств.



Контакт экранированное заземление (иногда называемое «защищенная земля») – второй справа на клеммном блоке, расположенном на задней стороне NPort 6600-32/16/8-48V.



ВНИМАНИЕ

Данное устройство предназначено для установки на хорошо заземленную поверхность, например металлический щит.

Подключение к сети Ethernet

Один конец Ethernet-кабеля подключается к Ethernet-порту 10/100М, противоположный конец – к сети.

Если кабельное соединение выполнено правильно, это покажет соответствующая индикация NPort 6000:

- Индикатор рядом с Ethernet-портом горит зеленым цветом при подключении к Ethernet-сегменту 100 Мбит/с.
- Индикатор рядом с Ethernet-портом горит оранжевым цветом при подключении к Ethernet-сегменту 10 Мбит/с.
- Данные индикаторы мигают при передаче данных через порт.

Подключение последовательных устройств

Кабели для подключения последовательных устройств к NPort 6000 приобретаются отдельно.

Светодиодные индикаторы

Значения состояния светодиодных индикаторов на передней панели NPort 6000 приведены в таблице:

Индикатор	Цвет	Значение
PWR	Красный	Подключено питание
Ready	Красный	Постоянно: Питание подключено, NPort 6000 полностью загружен. Мигание: Существует конфликт IP-адресов или нет ответа от DHCP-сервера или BOOTP-сервера.
	Зеленый	Постоянно: Питание есть, NPort 6000 работает нормально. Мигание: NPort найден утилитой NPort Search Utility.
	Выключен	Устройство обесточено или имеются проблемы с питанием.
Link	Оранжевый	NPort 6000 подключен к Ethernet-сегменту 10 Мбит/с.
	Зеленый	NPort 6000 подключен к Ethernet-сегменту 100 Мбит/с.
	Выключено	Кабель Ethernet-соединения не подключен или испорчен.
P1 – P16 in-use	Зеленый	Последовательный порт открыт программой сервера
	Выключено	Последовательный порт не открыт программой сервера
P1, P2, P3, P4 (6150/6250/6450)	Оранжевый	Через порт принимаются данные.
	Зеленый	Через порт идет отправка данных.
	Выключен	Обмен данными через порт отсутствует.
P1 - P16 Tx (6610/6650)	Зеленый	Через порт идет отправка данных.
	Выключен	Отправка данных через порт отсутствует.
P1 - P16 Rx (6610/6650)	Зеленый	Через порт принимаются данные.
	Выключен	Отсутствует прием данных через порт.

NPort'ы 6450 и 6650 имеют дополнительный индикатор аларма и индикаторы на сетевых модулях:

Индикатор	Цвет	Значение
Module (6450/6610/6650)	Зеленый	Модуль оптоволоконных разъемов вставлен и обнаружен
	Выключен	Отсутствует модуль оптоволоконных разъемов
Link (на доп. модулях NM-FX01-M-SC, NM-FX01-S-SC)	Оранжевый	Постоянно: NPort 6000 подключен к оптоволоконному сегменту, но обмен данными отсутствует. Мигание: Идет обмен данными.
Alarm	Красный	Выходное реле (DOUT) сработало
	Выключено	Выходное реле (DOUT) закрыто (нормальное состояние)
GSM (на модуле NM-GPRS/GSM)	Зеленый	Есть GSM-соединение
GPRS	Оранжевый	Установлено GPRS-соединение
GPRS/GSM Signal Strength (на модуле NM-GPRS/GSM)	Зеленый	Чем больше полос, тем сильнее сигнал; 4 – означают максимальное значение мощности.
DCD (на модуле NM-Modem)	Зеленый	Установлено модемное соединение.
TxD (на модуле NM-Modem)	Зеленый	Модем передает данные.
	Выключен	Отсутствует передача данных через модем.
DxD (на модуле NM-Modem)	Зеленый	Модем принимает данные.
	Выключен	Отсутствует прием данных.

Регулируемые подтягивающие сопротивления для интерфейса RS-485

В некоторых случаях для предотвращения отражения сигналов нужно использовать терминальные резисторы. При их установке важно правильно настроить подтягивающие сопротивления, чтобы сигнал не искажался. В NPort'ах 6000 они настраиваются джамперными переключателями или DIP-переключателями для каждого последовательного порта.

Для установки подтягивающих сопротивлений 150 кОм – убедитесь, что обе джамперных переключки (по две на порт) не замкнуты. (Для NPort 6650 оба DIP-переключателя должны быть в позиции OFF). Это настройки по умолчанию.

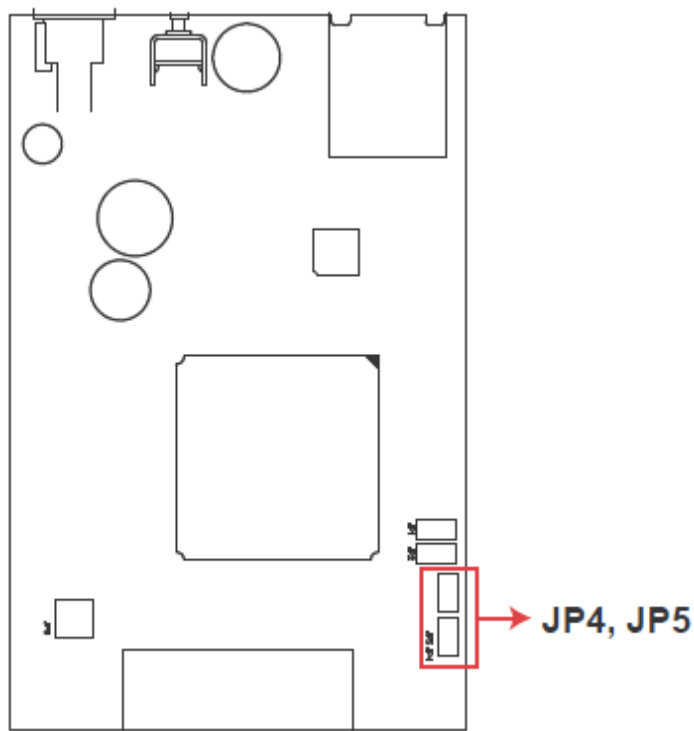
Для установки подтягивающих сопротивлений 1 кОм – замкните обе джамперные переключки (Для NPort 6650 оба DIP-переключателя должны быть в позиции ON).



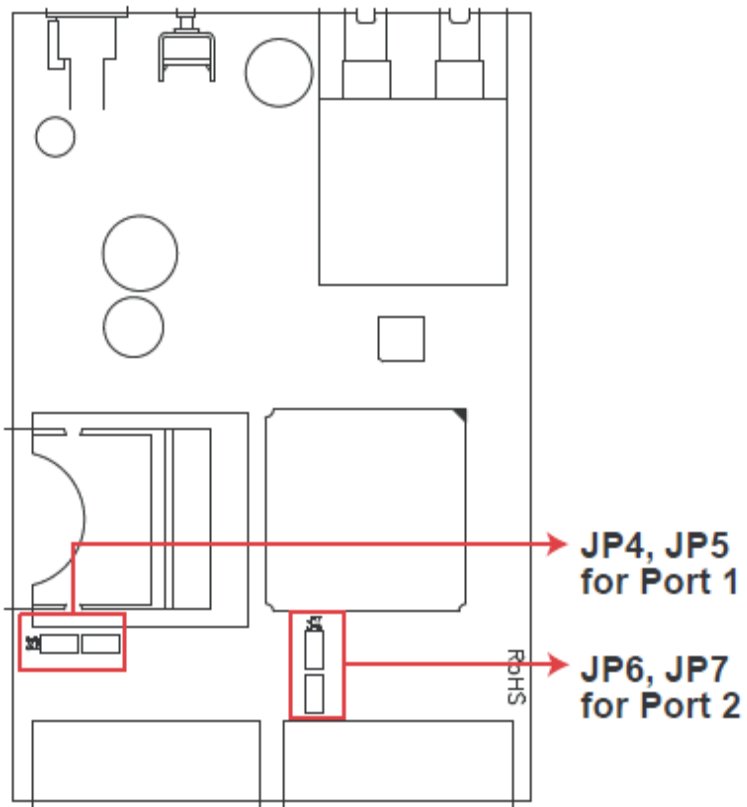
ВНИМАНИЕ

Не используйте сопротивление 1 кОм при использовании интерфейса RS-232, т.к. это ослабит сигналы и приведет к уменьшению дальности передачи.

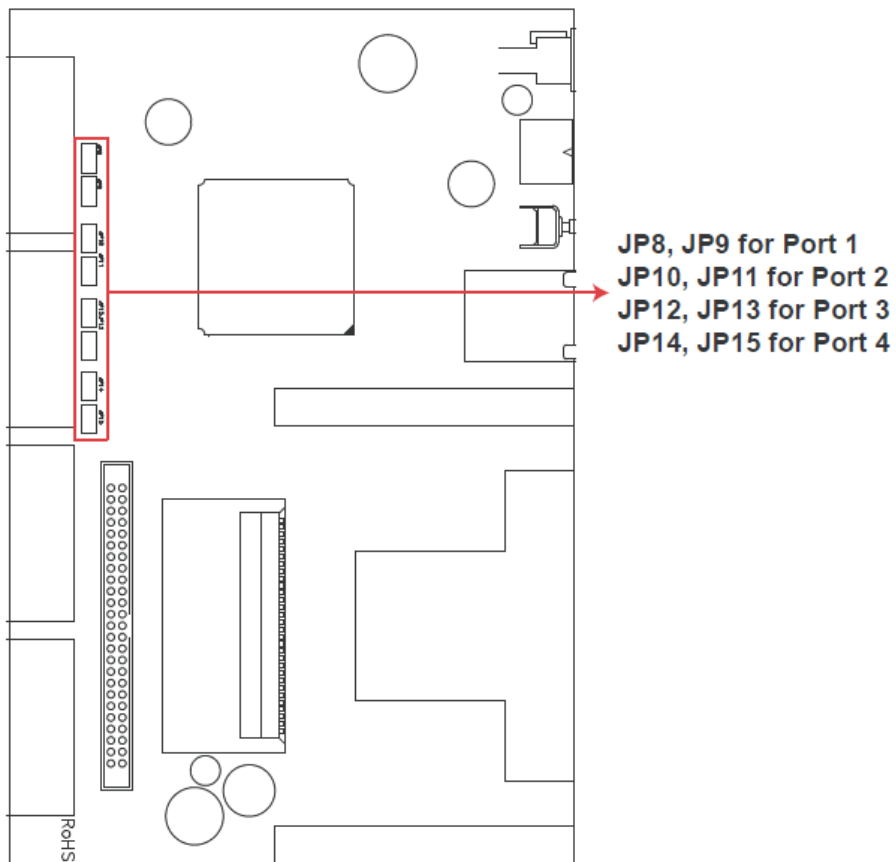
Джамперные переключки на NPort 6150



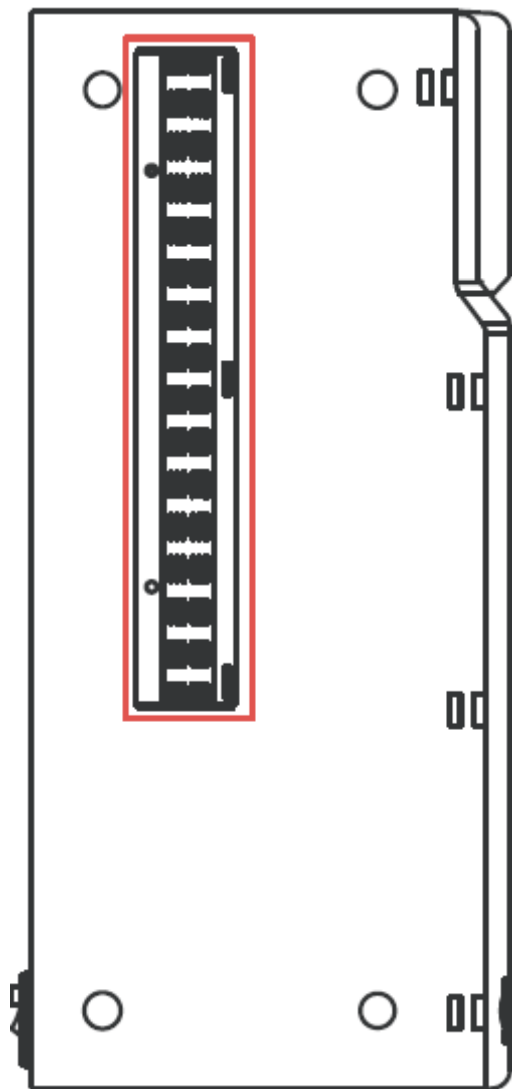
Джамперные перемычки на NPort 6250



Джамперные перемычки на NPort 6450



DIP-переключатели на NPort 6650



Положе ние	1	2	3
	Смещение вверх	Смещение вниз	Терминальн ый резистор
ON	1 кОм	1 кОм	120 кОм
OFF	150 кОм	150 кОм	---

3 Начальная конфигурация IP адреса

В первую очередь при настройке NPort 6000 нужно задать его IP-адрес. В данной главе представлены несколько разных способов изменения IP-настроек. Более подробную информацию о сетевых настройках см в главе 9.

Данная глава содержит следующие разделы:

- **Статический и динамический IP-адреса**
- **Заводские настройки IP-адреса**
- **Способы настройки**
 - Утилита NPort Search Utility
 - Web-консоль
 - Панель оператора (только для NPort 6610, 6650 и 6450)
 - Протокол ARP
 - Telnet-консоль
 - Последовательная консоль

Статический и динамический IP-адреса

Определите, какой адрес будет иметь NPort 6000: постоянный или динамический (назначаемый либо DHCP, либо BOOTP/PPPoE).

- Если NPort 6000 используется в сети с постоянными IP, то необходимо прописать статический IP-адрес NPort'a способами описанными ниже в данной главе.
- Если NPort 6000 используется в сети с динамически назначаемыми IP-адресами, то режим настройки IP нужно установить в DHCP, DHCP/BOOTP, BOOTP или PPPoE.



ВНИМАНИЕ

Уточните у своего сетевого администратора, как зарезервировать фиксированный IP-адрес для NPort'a 6000 в таблице MAC-адресов при использовании DHCP-сервера или BOOTP-сервера. Во многих случаях лучше использовать фиксированный IP-адрес для NPort 6000.

Заводские настройки IP-адреса

По умолчанию IP-адрес NPort 6000:

192.168.127.254

IP-адреса, начинающиеся со «192.168» назначаются в локальных сетях. К устройствам с такими адресами нет прямого доступа из публичных сетей. Например, такое устройство не получится пинговать из удаленной точки по сети Интернет. Если в Вашей задаче нужно передавать данные через глобальную сеть, например, Интернет, то NPort 6000 должен иметь постоянный выделенный IP-адрес, который может быть арендован у интернет-провайдера.

Способы настройки

Утилита NPort Search Utility

Можно настраивать сетевые параметры NPort 6000 с помощью идущей с ним в комплекте утилиты NPort Search Utility for Windows. См. главу 10, где описаны установка и использование данной программы.

Web-консоль

Можно настраивать NPort 6000 через стандартный Web-браузер. Подробнее о настройках через Web-консоль см. главу 10.

Панель оператора (только для NPort 6610, 6650 и 6450)

Данная опция имеется только в моделях NPort 6610, 6650 и 6450. Через LCM-панель можно выполнять некоторые настройки. Она может быть настроена в режим просмотра или просмотра/изменения настроек. Режим просмотра (Read only) позволяет только видеть настройки, без возможности их корректировки. По умолчанию установлен режим просмотра/изменения (writable access), что позволяет менять значения параметров через LCM-консоль.



ВНИМАНИЕ

Если был установлен пароль для доступа в LCM-консоль NPort'a 6000 и LCM-консоль настроена в режиме просмотра/записи, то для доступа к настройкам потребуется ввести пароль. В режиме просмотра/записи ввод пароля не требуется.

Кнопка **MENU** открывает главное меню. Она также используется для выхода из текущего меню и возврата в предыдущее.

Кнопки **UP** и **DOWN** позволяют перемещаться между функциями меню.

SEL подтверждает выбор выделенного меню или подменю.

Режим назначения IP-адреса (Static, DHCP, PPPoE и т.п.) настраиваются через **Main Menu** → **Network setting** → **IP config**. Сам IP-адрес назначается через **Main Menu** → **Network setting** → **IP address**. После изменения IP-адреса потребуется перезагрузка NPort'a через **Main Menu** → **Save/Restart**.

Для настройки IP-адреса NPort 6000 через LCM-дисплей нужно выполнить последовательность действий:

1. Нажмите **MENU** для входа в главное меню.
2. Первая строка на дисплее показывает текущее меню – **Main Menu**. Вторая строка показывает текущий пункт – **Server setting**. Кнопками **UP** и **DOWN** выберите пункт **Network Setting**. Нажмите **SEL** для входа в меню **Network setting**.
3. В меню **Network setting** выберите пункт **IP config**. Для входа в него нажмите **SEL**.
4. В меню **IP config** кнопками **UP** и **DOWN** выберите нужный режим (static, DHCP и т.д.). Нажмите **SEL** для подтверждения выбора. Для отмены выбора и возврата в предыдущее меню можно нажать кнопку **MENU**.
5. Вернитесь в меню **Network setting**. Выберите пункт **IP address**.
6. Кнопками **UP** и **DOWN** задайте значение IP-адреса. Для перехода к следующей части IP-адреса нажимайте **SEL**. Если Вы ошиблись, то для возврата в меню **Network setting** и отмены изменений нажмите **MENU**. Вернуться на ввод предыдущей части адреса нельзя.
7. После ввода IP-адреса изменения сохранены, но еще не вступили в силу. Необходимо перезагрузить NPort. До перезагрузки можно просматривать и изменять значения параметров в меню **Network setting** → **IP address**.
8. Нажмите кнопку **MENU** для выхода из меню **Network setting** и возврата в главное меню. Кнопками **UP-DOWN** выберите **Save/Restart** и нажмите **SEL**. **UP-DOWN** выберите **Yes** и нажмите **SEL** для перезагрузки.

Протокол ARP

Для настройки IP-адреса можно использовать протокол ARP (Address Resolution Protocol). По команде ARP ПК связывает MAC-адрес NPort'a 6000 с IP-адресом. После этого откройте telnet-консоль NPort'a 6000 – IP-адрес изменится.



ВНИМАНИЕ

Для использования ARP-протокола нужно, чтобы ПК и NPort 6000 были в одной подсети LAN. Можно также использовать кроссовый Ethernet-кабель для подключения NPort'a 6000 напрямую к сетевой карте компьютера. Перед выполнением ARP-команды нужно выставить заводские настройки по умолчанию для NPort'a 6000 (192.168.127.254), ПК и NPort 6000 должны быть в одной подсети.

Последовательность действий для настройки IP-адреса через ARP:

1. Получите у сетевого администратора уникальный IP-адрес для NPort 6000.
2. Посмотрите MAC-адрес NPort 6000 на табличке на нижней стороне устройства.
3. На компьютере выполните из командной строки `arp -s`:

arp -s <IP address> <MAC address>

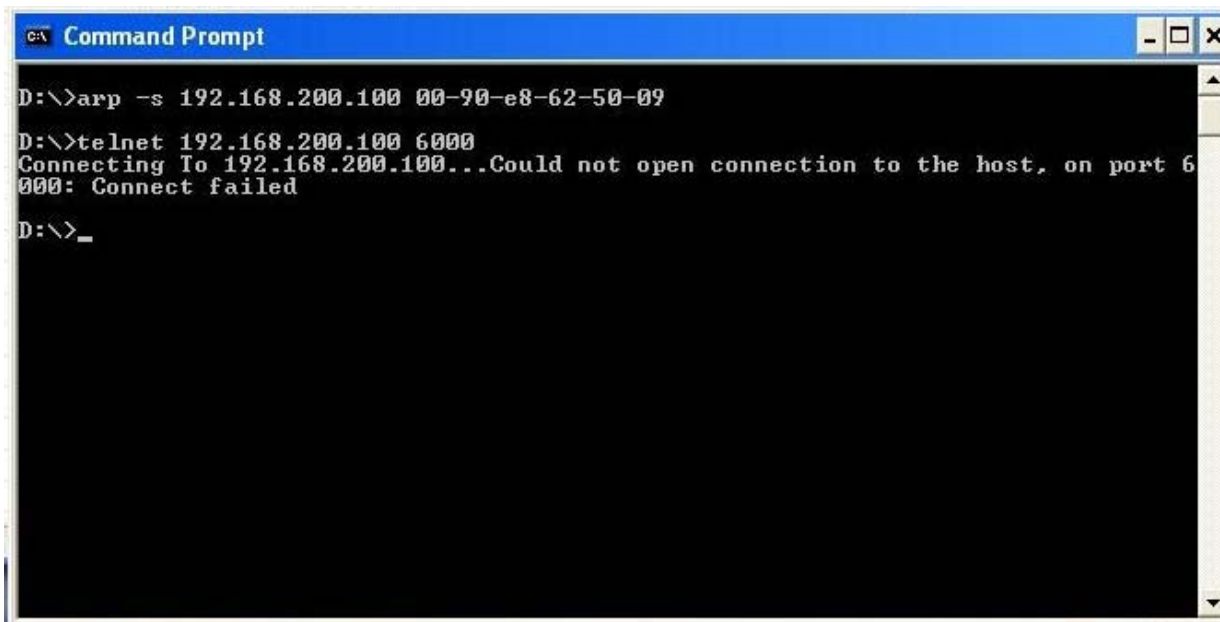
Например,

```
C:\> arp -s 192.168.200.100 00-90-E8-04-00-11
```

4. Выполните команду Telnet:

```
telnet 192.168.200.100 6000
```

После этого будет выдано сообщение **Connect failed**:



```
Command Prompt
D:\>arp -s 192.168.200.100 00-90-e8-62-50-09
D:\>telnet 192.168.200.100 6000
Connecting To 192.168.200.100...Could not open connection to the host, on port 6000: Connect failed
D:\>_
```

5. После перезагрузки NPort 6000 его IP-адрес изменится на новый адрес и можно снова попробовать получить доступ через Telnet.

Telnet-консоль

В зависимости от того, как настроены компьютер и сеть, удобным может оказаться доступ к NPort 6000 для изменения его IP-адреса по сети. Это можно сделать через Telnet-консоль.



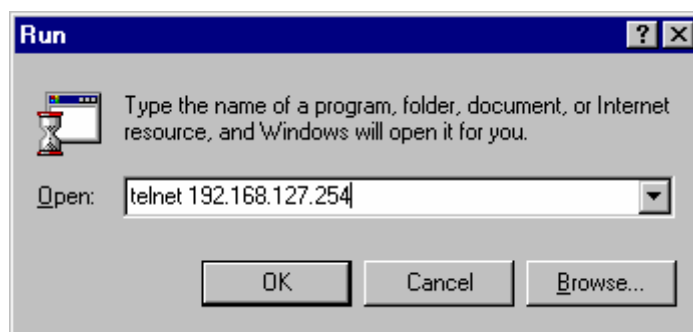
ВНИМАНИЕ

Скриншоты Telnet-консоли приведены для конкретной модели NPort 6650.

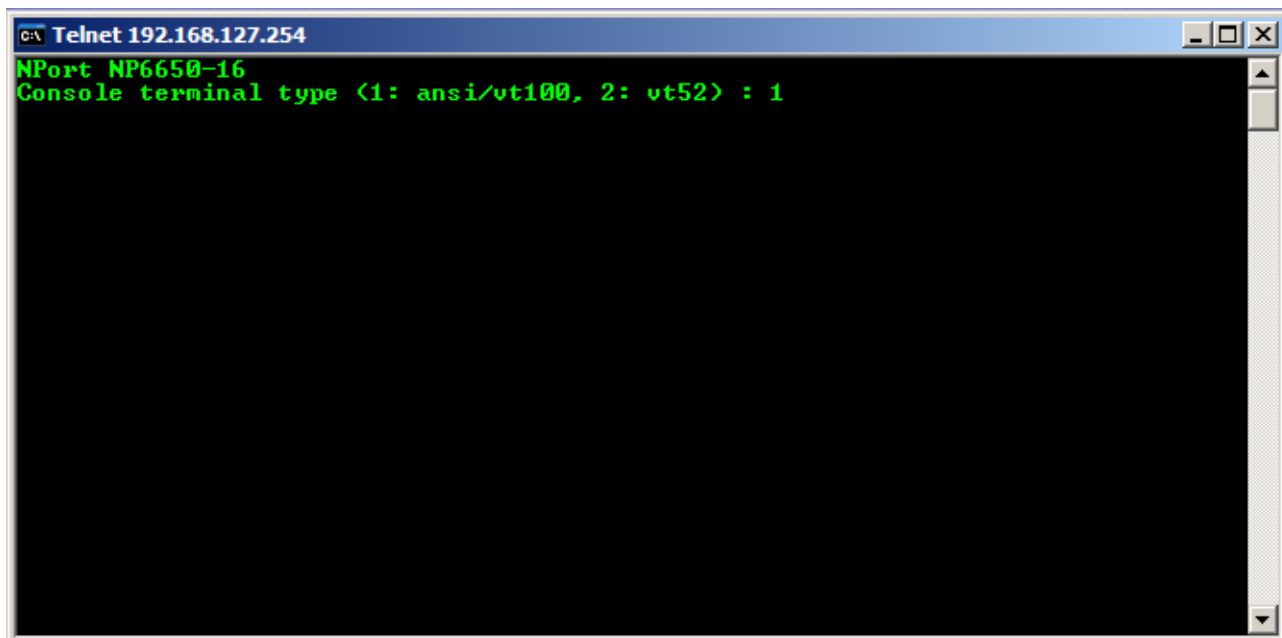
1. Из командной строки Windows (Пуск->Выполнить) наберите команду:

```
telnet 192.168.127.254
```

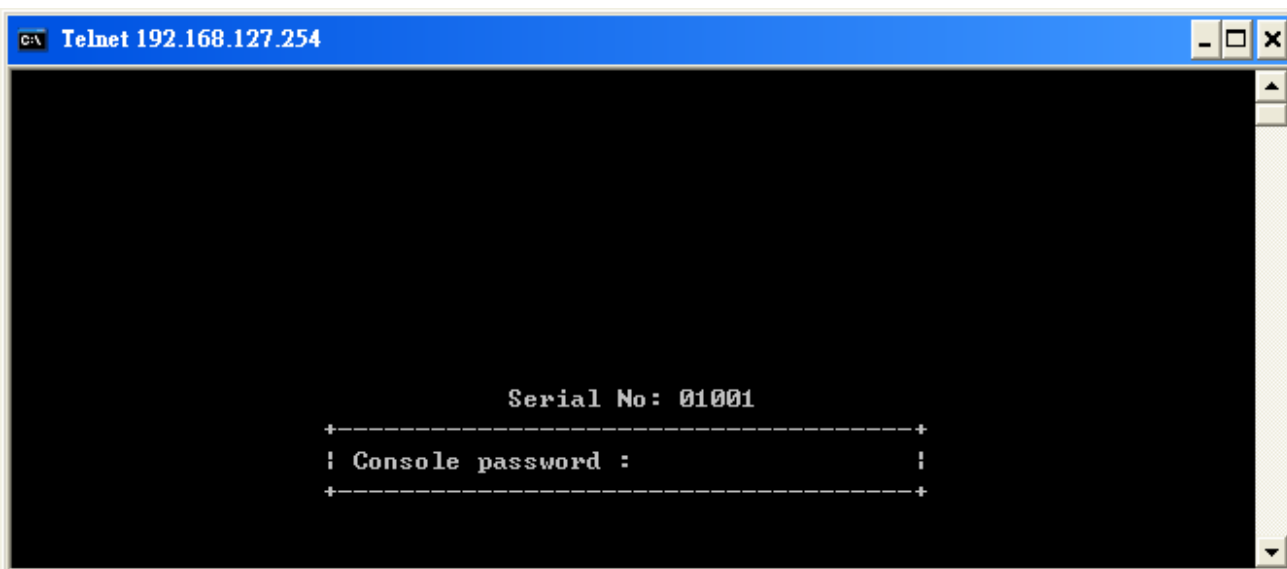
Если NPort'у 6000 задан другой IP-адрес, то введите его вместо адреса по умолчанию. Нажмите **ОК**.



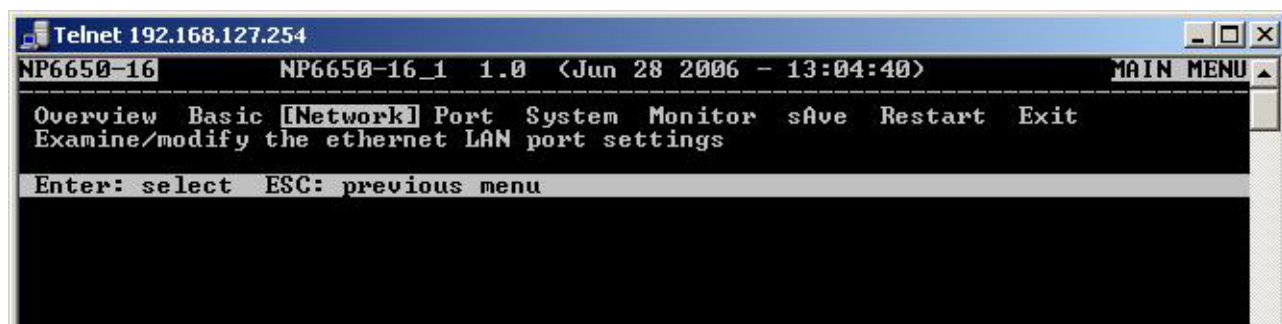
2. **Terminal type** задайте **ansi/vt 100**: введите **1** и нажмите **ENTER** для продолжения.



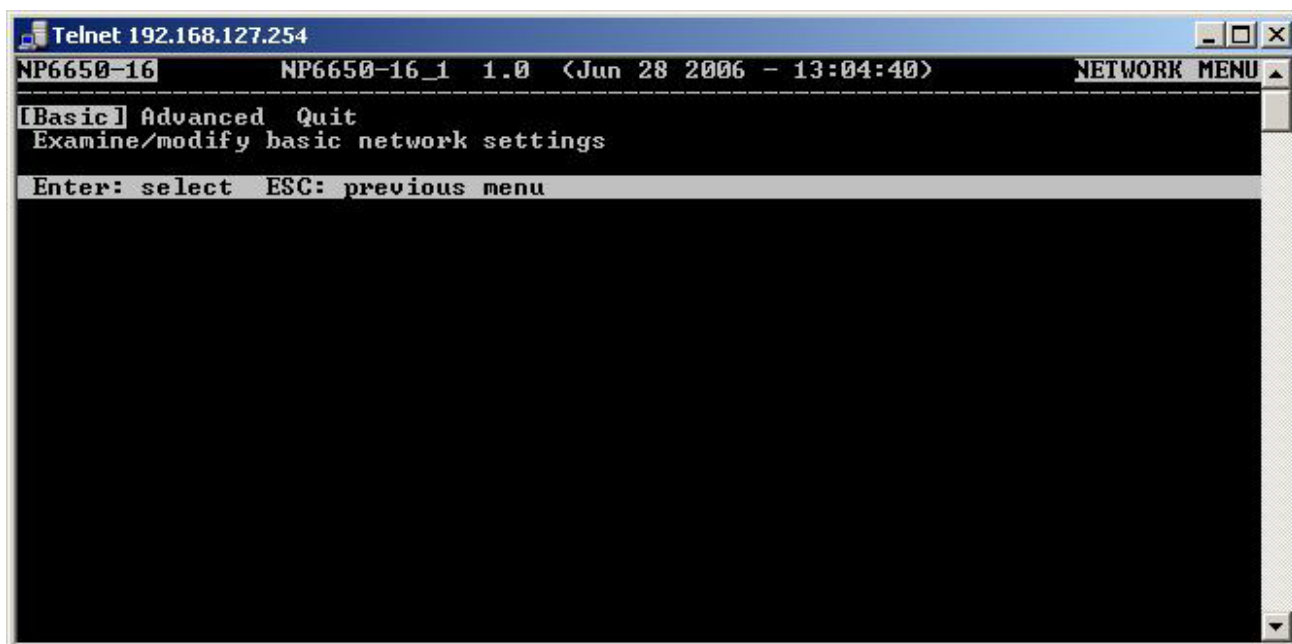
3. Если настроена защита паролем для входа в консоль, то появится показанное ниже окно. Введите пароль и нажмите **ENTER**.



4. Нажмите клавишу **N** или курсорными стрелками выберите пункт меню **Network** и нажмите **ENTER**.

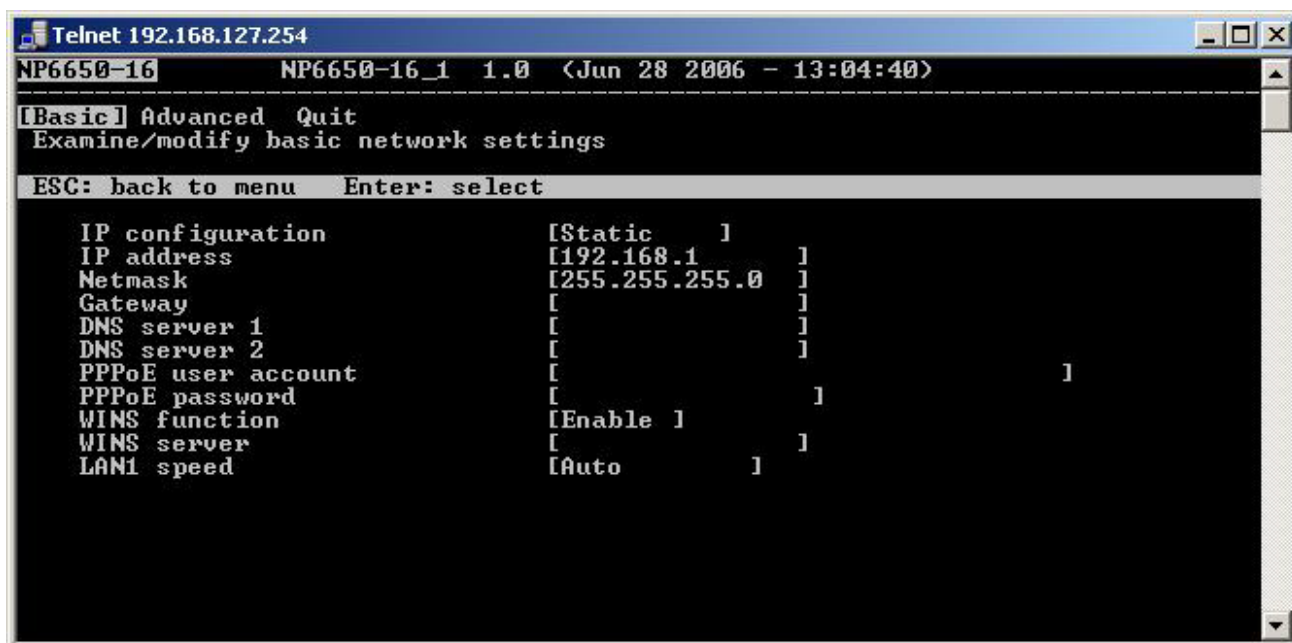


5. Нажмите клавишу **B** или курсорными стрелками выберите пункт меню **Basic** и нажмите **ENTER**.



```
Telnet 192.168.127.254
NP6650-16      NP6650-16_1  1.0  <Jun 28 2006 - 13:04:40>  NETWORK MENU
[Basic] Advanced Quit
Examine/modify basic network settings
Enter: select  ESC: previous menu
```

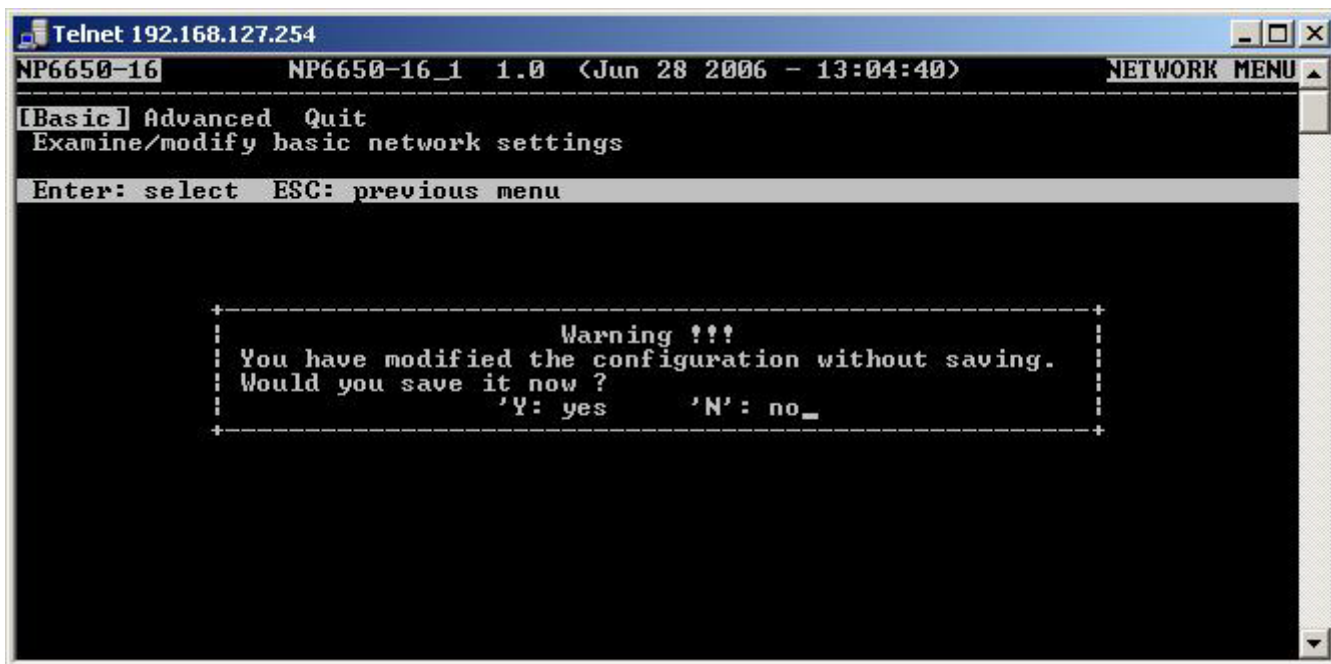
6. Используя курсорные клавиши, выберите пункт **IP address**. Удалите текущий IP-адрес кнопками **DELETE**, **BACKSPACE** или **ПРОБЕЛ**, введите новый IP-адрес и нажмите **ENTER**. Помните, что если используется режим динамического IP (BOOTP, DHCP и т.п.), то нужно будет соответственно изменить параметр **IP configuration field**.



```
Telnet 192.168.127.254
NP6650-16      NP6650-16_1  1.0  <Jun 28 2006 - 13:04:40>
[Basic] Advanced Quit
Examine/modify basic network settings
ESC: back to menu  Enter: select

IP configuration      [Static  ]
IP address            [192.168.1  ]
Netmask              [255.255.255.0 ]
Gateway              [          ]
DNS server 1         [          ]
DNS server 2         [          ]
PPPoE user account   [          ]
PPPoE password       [          ]
WINS function        [Enable ]
WINS server          [          ]
LAN1 speed           [Auto    ]
```

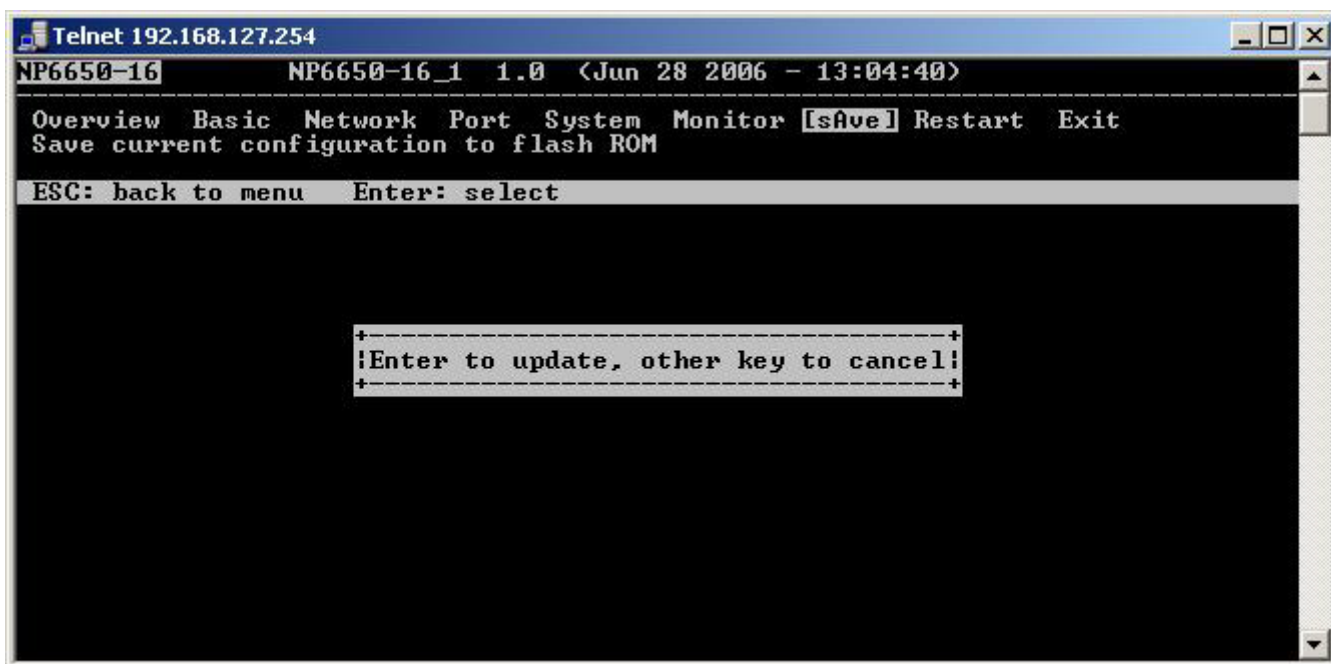
- Для возврата на предыдущую страницу настроек дважды нажмите **ESC**. Выберите **Y** для подтверждения изменений.



```
Telnet 192.168.127.254
NP6650-16      NP6650-16_1  1.0  <Jun 28 2006 - 13:04:40>      NETWORK MENU
[Basic] Advanced Quit
Examine/modify basic network settings
Enter: select  ESC: previous menu

+-----+
|                          Warning !!!                          |
| You have modified the configuration without saving.             |
| Would you save it now ?                                         |
|      'Y': yes           'N': no_                                |
+-----+
```

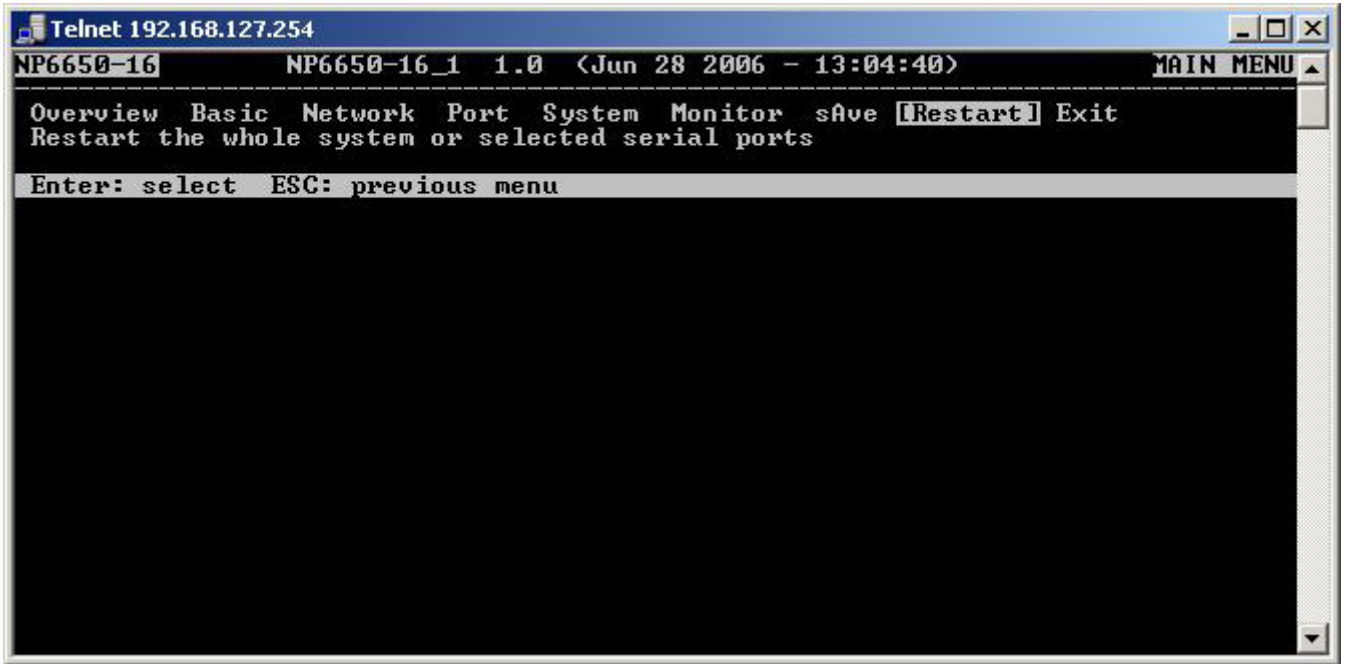
- Нажмите **ESC** для возврата на предыдущую страницу.
- Нажмите **A** или выберите курсорными клавишами пункт **Save** и нажмите **ENTER**. Повторно нажмите **ENTER** для выполнения команды сохранить (save).



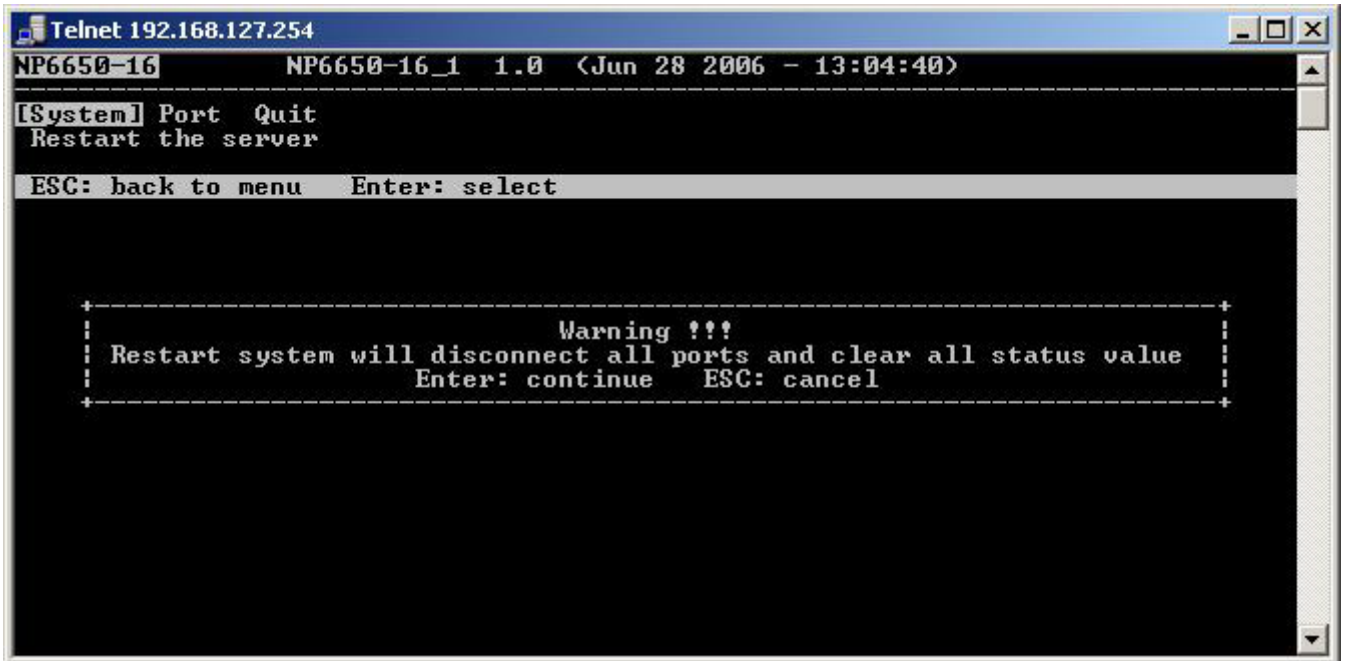
```
Telnet 192.168.127.254
NP6650-16      NP6650-16_1  1.0  <Jun 28 2006 - 13:04:40>
Overview Basic Network Port System Monitor [save] Restart Exit
Save current configuration to flash ROM
ESC: back to menu  Enter: select

+-----+
| !Enter to update, other key to cancel! |
+-----+
```

10. Нажмите **R** или используя курсорные клавиши выберите пункт **Restart** и нажмите **ENTER**.



11. Нажмите **S** или курсорными клавишами выберите **System** и затем нажмите **ENTER** для перезагрузки NPort'a 6000.



Последовательная консоль

Устройства серии NPort 6000 можно настраивать через последовательную консоль, которая является такой же Telnet-консолью, только доступ к ней осуществляется через порт RS-232, а не через Ethernet. Принцип работы с ней такой же, как и с Telnet-консолью.

Ниже показаны действия, которые нужно выполнить для открытия этой консоли с использованием утилиты PCOMM Terminal Editor, который находится в свободном доступе как один из модулей программы PCOMM Lite Suite. Можно использовать и другие терминальные программы, в этом случае процесс открытия консоли будет отличаться от приведенного ниже.

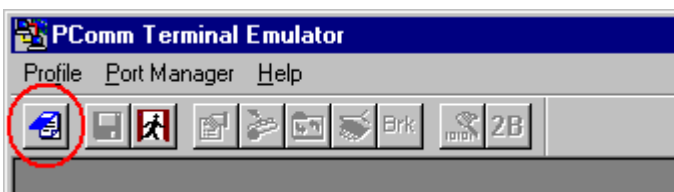
1. Обесточьте NPort 6000. Используя нуль-модемный кабель подключите консольный порт к COM-порту компьютера.



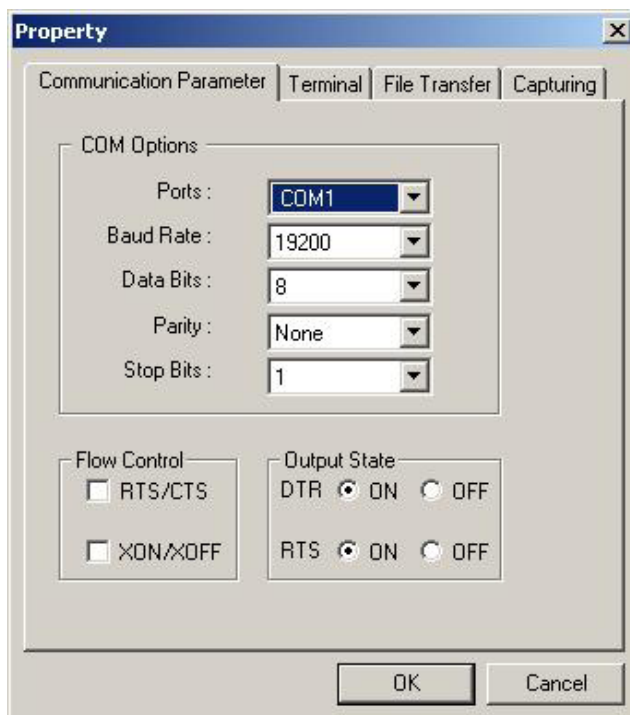
ВНИМАНИЕ

NPort 6610/6650 имеют отдельный консольный порт. У всех остальных устройства серии 6000 консольным является только port 1.

2. Запустите терминальную программу: **Пуск**→**Программы**→**PComm Lite**→**Terminal Emulator**.
3. Появится окно PComm Terminal Emulator. В меню **Port Manager** выберите **Open** или нажмите пиктограмму **Open**:



4. Откроется окно выбора свойств Property. Зайдите на вкладку **Communication Parameters** и выберите COM-порт, к которому подключено устройство (COM1 в примере). Установите параметры: **19200, 8, N, 1**.

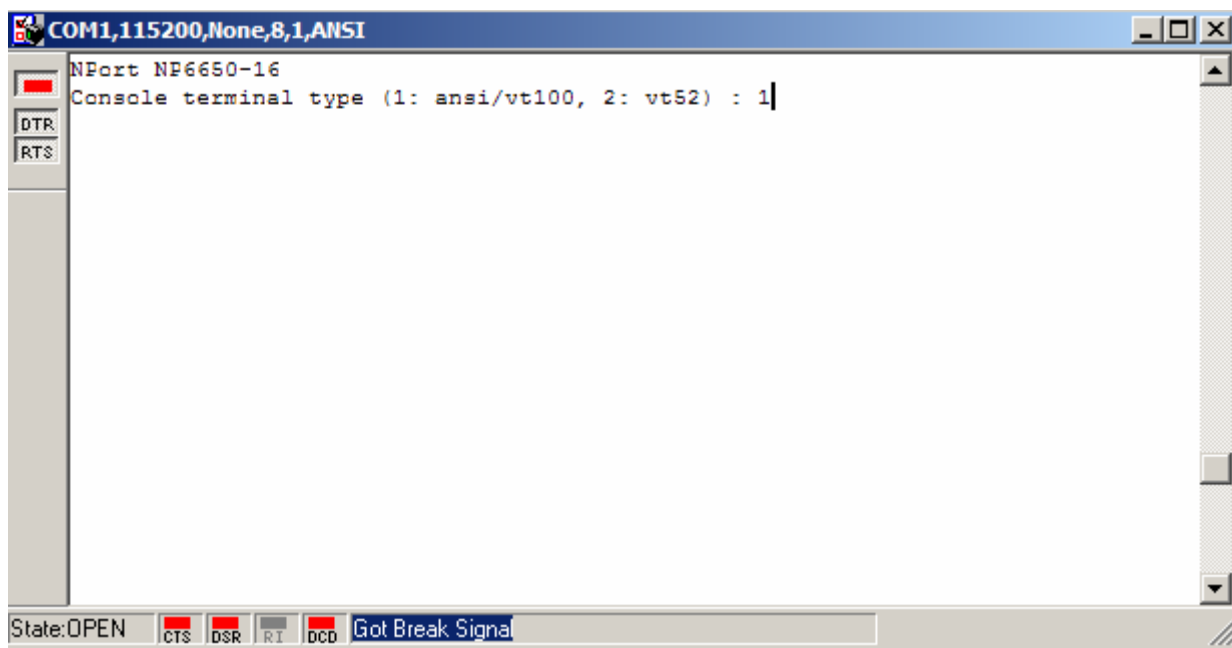


5. На вкладке Terminal выберите **ANSI** или **VT100** в качестве **Terminal Type** и нажмите **OK**.
6. Если используется устройство NPort 6610/6650, то теперь его уже можно включить. Если используются устройства моделей NPort 6150, 6250 или 6450 – то при их включении нажимайте кнопку «гравис», показанную на рисунке.

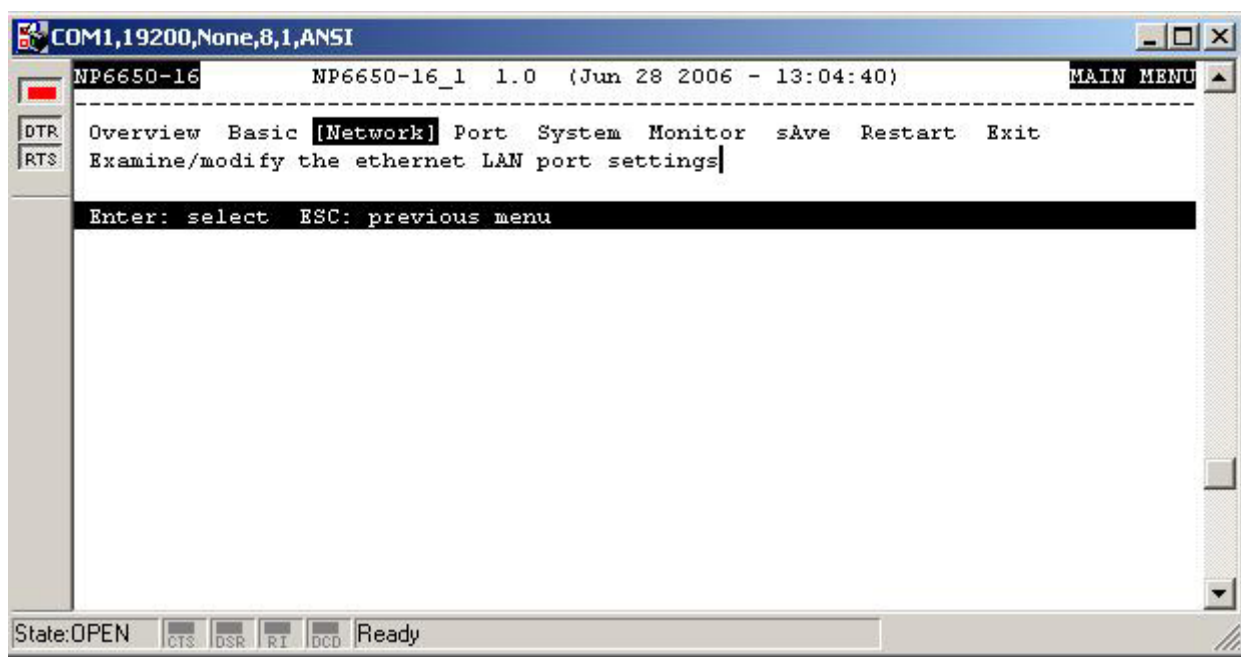


NPort 6000 автоматически перейдет из режима данных в консольный.

7. Если была установлена парольная защита на вход в консоль, то потребуется ввести пароль. После ввода пароля нужно выбрать протокол канального уровня: ansi/vt 100 в поле terminal type. Введите **1** для выбора и нажмите **ENTER**.



8. Появится главное меню. Как только Вы попали в консоль настроек, с ней можно работать так же как с Telnet-консолью. См. шаги 4-11 при работе в параграфе Telnet-консоль – по настройке IP-параметров.



4 Выбор режима работы последовательных портов

В данной главе описаны различные режимы работы Nport 6000. Все режимы объединены в несколько групп по типу применения, например Device Control или Reverse Terminal. Есть режимы для работы на основе драйверов, установленных на хост-компьютере, и режимы на основе протоколов TCP/IP. После выбора подходящего режима работы обращайтесь к главе 5 Настройка через WEB-консоль – за детальной информацией по настройкам.

Данная глава содержит следующие разделы:

- **Обзор**
- **Описание режимов работы NPort 6000**
- **Режимы Device Control**
 - Real COM и Secure Real COM
 - Reverse Real COM
 - RFC2217
- **Режимы Socket**
 - TCP Server и Secure TCP Server
 - TCP Client и Secure TCP Client
 - UDP
- **Режимы Pair Connection и Secure Pair Connection**
- **Режим Ethernet Modem**
- **Режимы Terminal**
 - Terminal ASCII
 - Terminal BIN
 - SSH
- **Режимы Reverse Terminal**
 - Reverse Telnet
 - Reverse SSH
- **Режимы Printer**
- **Режимы Dial In/Out**
- **Режим Disabled**

Обзор

Nport 6000 – устройства для подключения в сеть устройств с последовательным интерфейсом (RS-232/422/485). Nport представляет собой мини-компьютер с процессором, поддерживающий протоколы TCP/IP, и может использоваться для двунаправленного обмена данными через последовательные и Ethernet-порты. Со своего компьютера Вы можете иметь доступ к управлению и настройке удаленного оборудования по сети Интернет из любой точки мира.

В обычных SCADA и системах сбора данных используются последовательные порты для получения информации от различного оборудования. Т.к. NPort 6000 позволяет подключать к сети TCP/IP устройства с интерфейсом RS-232/422/485, SCADA и системы сбора данных могут обращаться к ним независимо от того, являются ли эти устройства локальными или удаленными.

NPort 6000 – устройство для работы с IP-сетями, позволяющее увеличивать число последовательных портов хост-компьютера. Если Ваш компьютер поддерживает протокол TCP/IP, снимаются ограничения шины ISA или PCI и проблемы, связанные с отсутствием нужных драйверов для различных операционных систем.

Помимо доступа к socket NPort 6000 имеет драйвер Real COM/TTY, передающий все последовательные сигналы. Это позволяет использовать имеющееся программное обеспечение, поддерживающее COM/TTY.

Существует три различных режима socket: TCP Server, TCP Client, UDP Server/Client. Основное отличие протоколов TCP и UDP в том, что в первый гарантирует доставку пакетов данных за счет запроса передатчиком от приемника подтверждения о доставке. В UDP такое подтверждение отсутствует, что повышает скорость обмена. UDP также позволяет организовывать однонаправленную и широковещательную отправку данных на один IP-адрес или группу IP-адресов.

NPort 6000 также поддерживает консольное управление включая Reverse Telnet, Reverse SSH. Режимы Reverse terminal позволяют подключаться к консольному порту сервера по IP-сети для удаленного управления и/или мониторинга сервера.

NPort 6000 поддерживает стандарт SSL защиты доступа к данным для режимов Real COM/TTY, TCP Server, TCP Client и Pair Connection. Данные, передаваемые по Ethernet будут надежно защищены.

Описание режимов работы NPort 6000

В NPort 6000 каждый последовательный порт настраивается независимо от других. Например, в Nport 6450 пользователь может настроить два порта в режиме Real COM, один порт – в режиме Ethernet Modem и еще один в Reverse Telnet. Обратитесь к **главе 7 Настройка режимов работы последовательных портов** за детальной информацией и инструкциями по настройке.

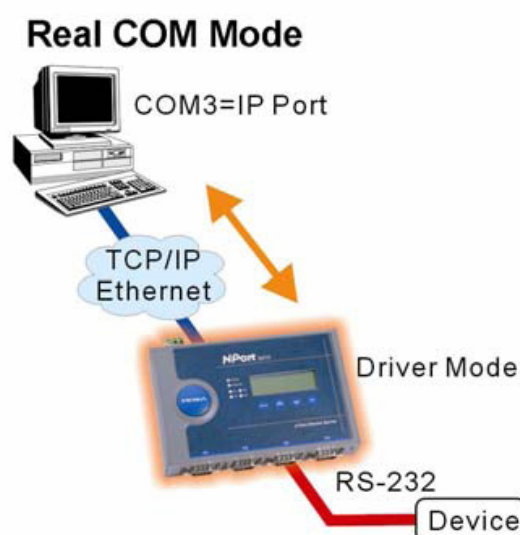
Режимы Device Control

В данной группе режимов доступны следующие: Real COM/Secure Real COM и RFC2217.

Real COM и Secure Real COM

NPort поставляется с набором драйверов виртуальных COM-портов для работы в ОС Windows 95/98/Me/NT/2000/XP/2003, а также с виртуальными TTY-драйверами для Linux. В режиме Real COM можно настроить шифрование данных, используя протокол SSL. (Для платформы Windows данная опция поддерживается для Windows 2000/XP/Vista/XP x64/2003/2003 x64/Vista x64). Драйвер устанавливает прозрачное соединение между хостом и последовательным устройством путем привязки адреса IP:Port соответствующего последовательного канала NPort-сервера к номеру виртуального COM-порта хост-компьютера. При этом последовательный порт на сервере воспринимается хостом как его собственный COM/TTY порт. Этот режим также поддерживает возможность установки до 8 соединений одновременно, т.е. одновременно до 8 хостов могут получать данные с одного последовательного устройства.

Одним из главных преимуществ использования режима Real COM является то, что в нем можно использовать ПО, предназначенное для работы с последовательными портами. Драйвер Real COM принимает данные, отсылаемые в COM-порт хоста, упаковывает их в пакеты TCP/IP и затем отправляет их по сети Ethernet в хост. На противоположном конце



линии NPort 6000 получает пакеты данных по Ethernet, распаковывает их и прозрачно отправляет через последовательный порт на присоединенные устройства.



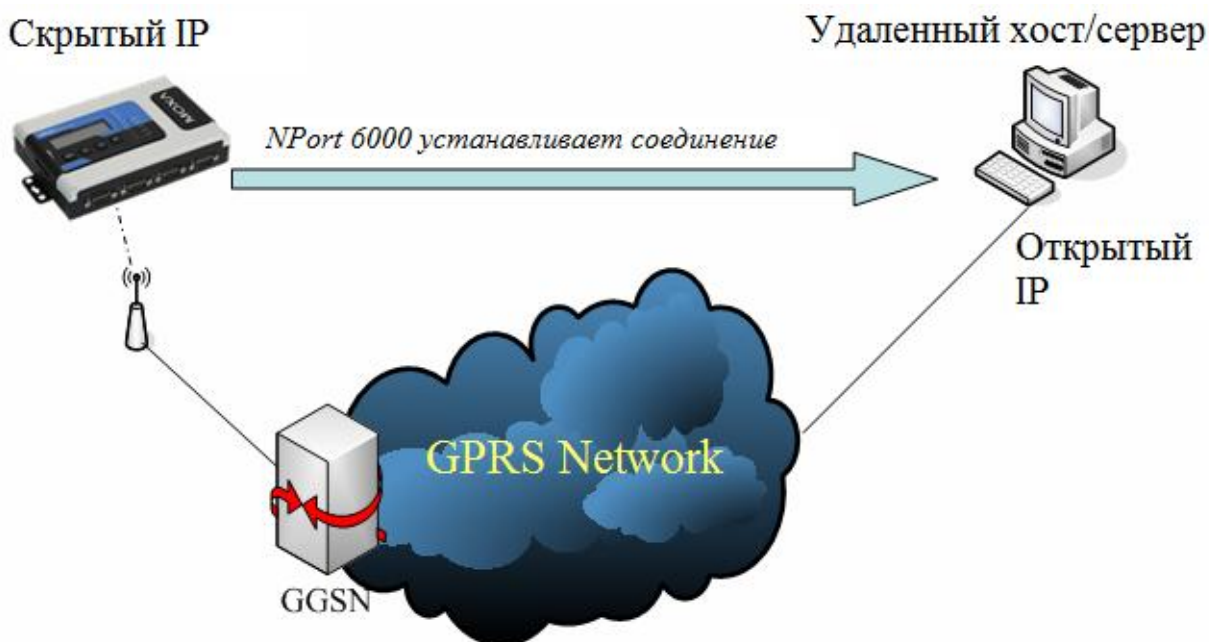
ВНИМАНИЕ

В режиме Real COM несколько хостов могут обращаться к одному NPort 6000. Имеющиеся драйверы NPort 6000 управляют доступом хостов путем проверки их IP-адреса. См. также параграф Accessible IP List (список IP-адресов, имеющих доступ) в главе 9 System Management Settings (Настройки управления системой).

Reverse Real COM

Режим Real COM не работает, когда NPort имеет скрытый IP-адрес, как например, в GPRS-сетях, или когда IP-адрес ему назначается динамически. В обоих случаях, хост не сможет связаться с NPort 6000.

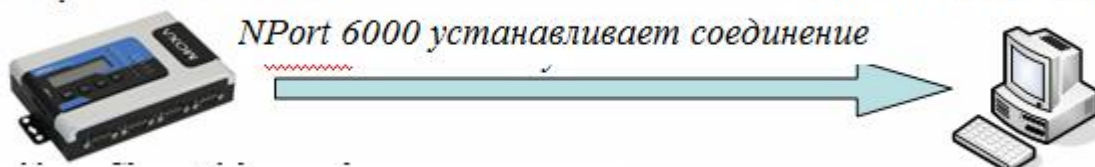
Пример, где NPort 6000 имеет скрытый IP-адрес.



Динамический IP-адрес

Динамический IP-адрес

Удаленный хост/сервер



IP-адрес периодически изменяется

Reverse Real COM – новый режим, разработанный Муха. Он обеспечивает выполнение тех же функций NPort 6000, но без необходимости открытого IP-адреса. Другими словами, Real COM можно использовать даже если NPort имеет скрытый или динамический IP-адрес.

В режиме Reverse Real COM NPort 6000 самостоятельно устанавливает соединение с удаленным хостом/сервером, который имеется в списке “destination IP” после загрузки устройства.

RFC2217

Данный режим похож на Real COM. Заключается в том, что драйвер используется для установки прозрачного соединения между хостом и последовательным устройством через последовательный порт NPort'a и локальный COM-порт хоста. RFC2217 имеет общие опции управления COM-портом по протоколу Telnet. Драйверы сторонних производителей, поддерживающих RFC-2217 доступны в Интернете и могут использоваться для создания виртуального COM-порта.

Режимы Socket

В данной группе доступны следующие режимы: TCP Server/Secure TCP Server, TCP Client/Secure TCP Client и UDP.

TCP Server и Secure TCP Server

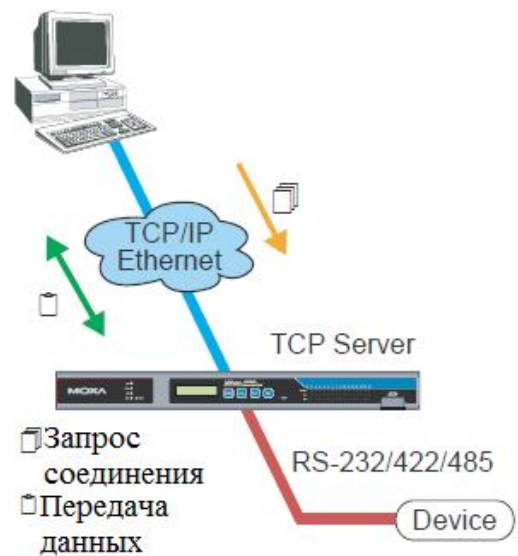
В режиме TCP Server последовательному порту NPort'a 6000 назначается номер, который не должен конфликтовать с номерами других портов устройства. Хост устанавливает соединение с NPort 6000 и получает данные с последовательного устройства. При этом поддерживается до 8 одновременных подключений, что дает возможность доступа к NPort с нескольких хостов для одновременного получения информации с последовательного устройства.

Как показано на рисунке процесс передачи данных следующий:

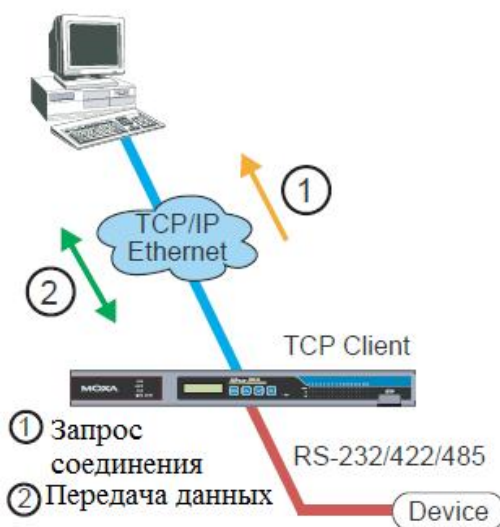
Хост запрашивает соединение с NPort 6000, настроенным в режиме TCP Server.

После того, как соединение установлено данные могут передаваться в обоих направлениях между хостом и NPort'ом.

Режим TCP Server имеет также дополнительную настройку шифрования данных по SSL.



TCP Client и Secure TCP Client



В режиме TCP Client NPort может самостоятельно устанавливать TCP-соединение с назначенным хостом при получении данных с последовательного порта.

На рисунке показано, что процесс передачи данных состоит из этапов:

NPort 6000, настроенный в режиме TCP Client, посылает запрос на соединение с хостом.

После установления соединения данные могут передаваться в обоих направлениях между компьютером и NPort'ом 6000.

Режим TCP Client имеет опцию шифрования данных по протоколу SSL.

UDP

В отличие от TCP протокол UDP обеспечивает более быстрый и эффективный обмен. В режиме UDP можно применять одно- или многоточечную адресацию и получать данные с последовательных устройств одном или нескольких хостах. Данные особенности делают режим UDP подходящим для отображения сообщений.

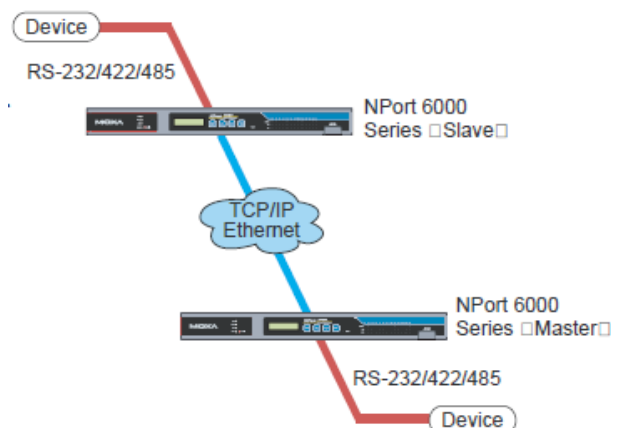


на

Режимы Pair Connection и Secure Pair Connection

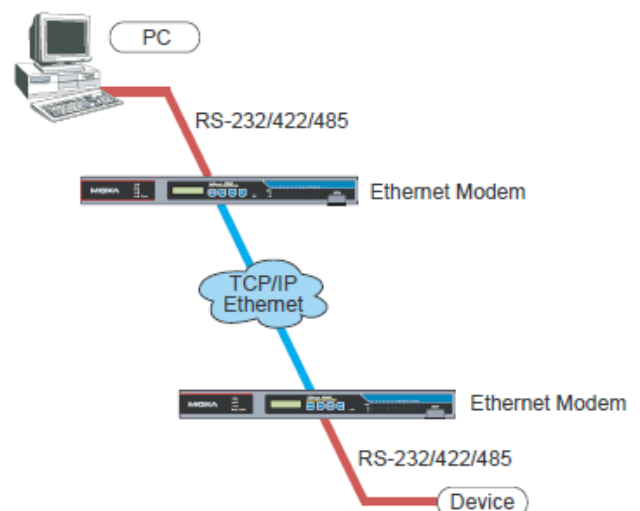
Режим Pair Connection (парного соединения двух NPort'ов 6000) используется для удлинения интерфейса RS-232 с помощью Ethernet. Один из NPort'ов произвольно назначается «мастером» (не имеет значения, какой), другой – «слэйвом». Один сервер через свой последовательный порт подключен к интерфейсу RS-232 COM-порта ПК или др. типам компьютеров, например, портативным, имеющим последовательный порт; другой сервер соединен с последовательным устройством через свой интерфейс RS-232.

Два NPort'а соединены между собой по сети Ethernet.

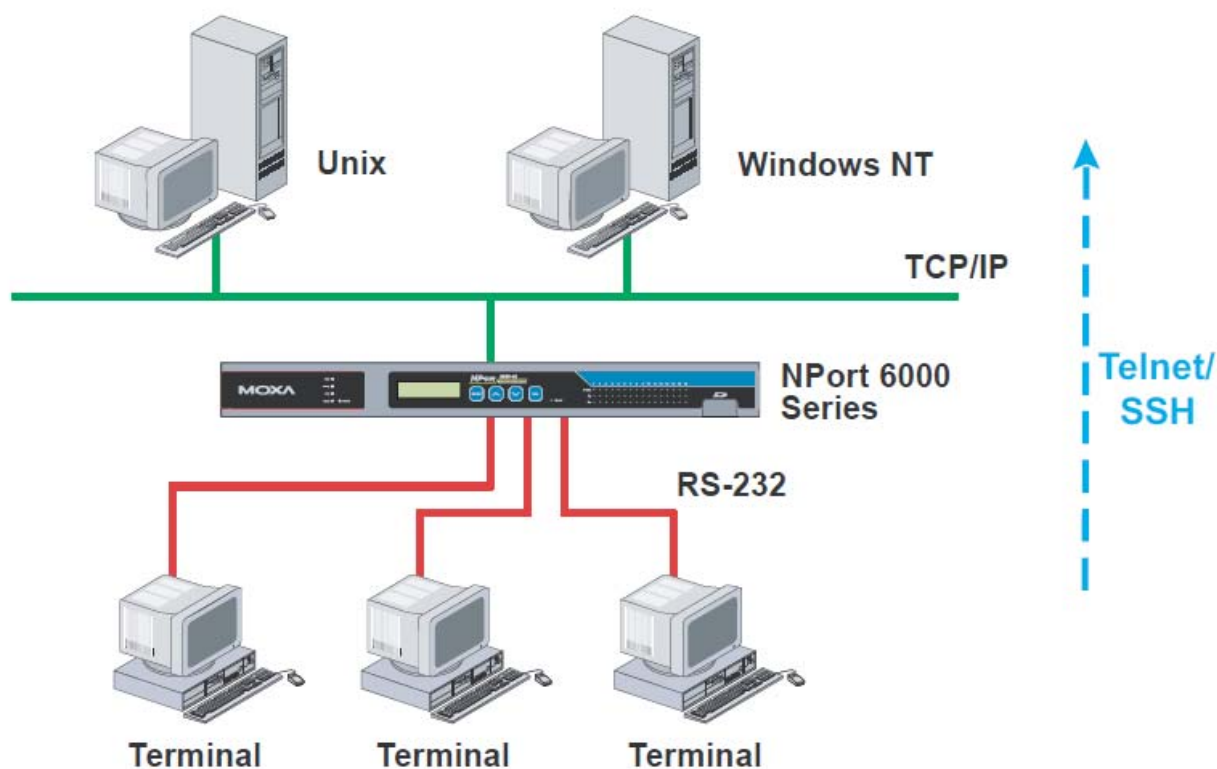


Режим Ethernet Modem

Режим Ethernet Modem предназначен для работы с прежними операционными системами, такими как MS-DOS, не поддерживающими TCP/IP Ethernet. Используя NPort 6000, настроенный в данном режиме работы, можно использовать программное обеспечение, поддерживающее передачу данных только через модем, для обмена по Ethernet.



Режимы Terminal



Режимы Terminal позволяют подключать по сети терминалы к серверам с ОС UNIX или Windows. Терминалы подключаются к настроенным соответствующим образом последовательным портам NPort'a 6000, который передает информацию из/в системы UNIX или Windows по сети через свой Ethernet-порт. Вам необходимо уточнить режим Terminal у сетевого администратора. Все режимы Terminal поддерживают «горячие клавиши», используемые во многих терминальных приложениях.

Обращайтесь к главе 7 за более детальной информацией по настройке.

Terminal ASCII

В данном режиме можно запускать до 8 сессий на одном порте с возможностью переключаться между сессиями на одном и том же терминале. Этот режим используется для текстовых терминалов без передачи файлов и шифрования.

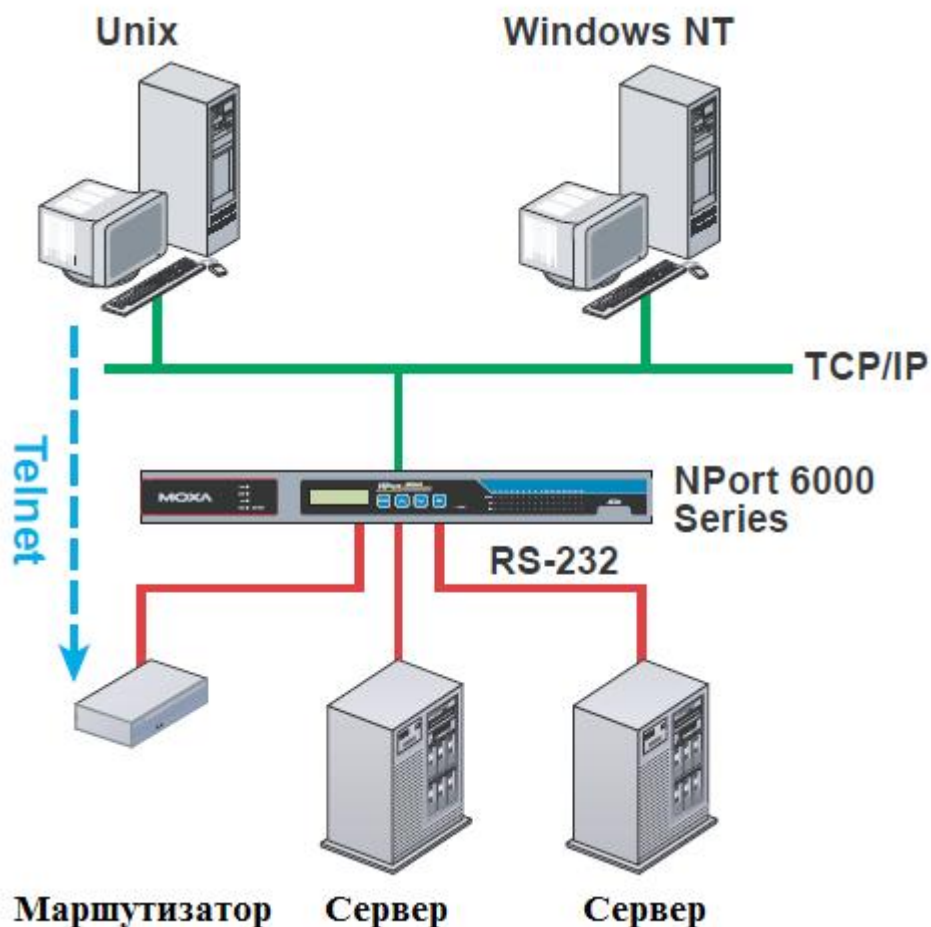
Terminal BIN

Этот режим позволяет запускать одну сессию на каждом порте и используется для терминальных приложений с передачей файлов.

SSH

В режиме SSH можно открывать одну сессию на каждом порте; используется для терминальных приложений, работающих по протоколу SSH.

Режимы Reverse Terminal



Режимы Reverse Terminal аналогичны режимам Terminal, т.к. в обоих случаях NPort 6000 используется для связи терминалов и серверов. Отличие в том, что в режимах reverse terminal терминал подключается через сеть, сервер – через последовательный порт. Обычно на практике сессия Reverse Terminal используется для удаленного соединения с устройством, имеющим последовательный консольный порт, настроенный для настройки устройства.

Например, множество маршрутизаторов, коммутаторов, систем бесперебойного питания и других устройств (включая NPort 6000) имеют Console/AUX или COM-порты к которым может подключаться терминал для консольного управления. С помощью NPort 6000 консольный порт устройства можно подключить к последовательному порту NPort 6000 для того, чтобы сетевой администратор мог удаленно по сети настраивать устройство. Несмотря на то, что современное сетевое оборудование обеспечивает и другие возможности для удаленной сетевой настройки, в некоторых случаях необходимо или желательно настраивать устройство через последовательную консоль (например, из соображений информационной безопасности при использовании оборудования предыдущих поколений или при восстановлении конфигурации, когда сеть неработоспособна).

Режимы Reverse Terminal позволяют применять авторизованный доступ – для этого используют NPort 6000 User Table или RADIUS server. См. описание вкладки Misc. Network Settings в главе 9, где приведены инструкции по настройке NPort 6000 User Table.

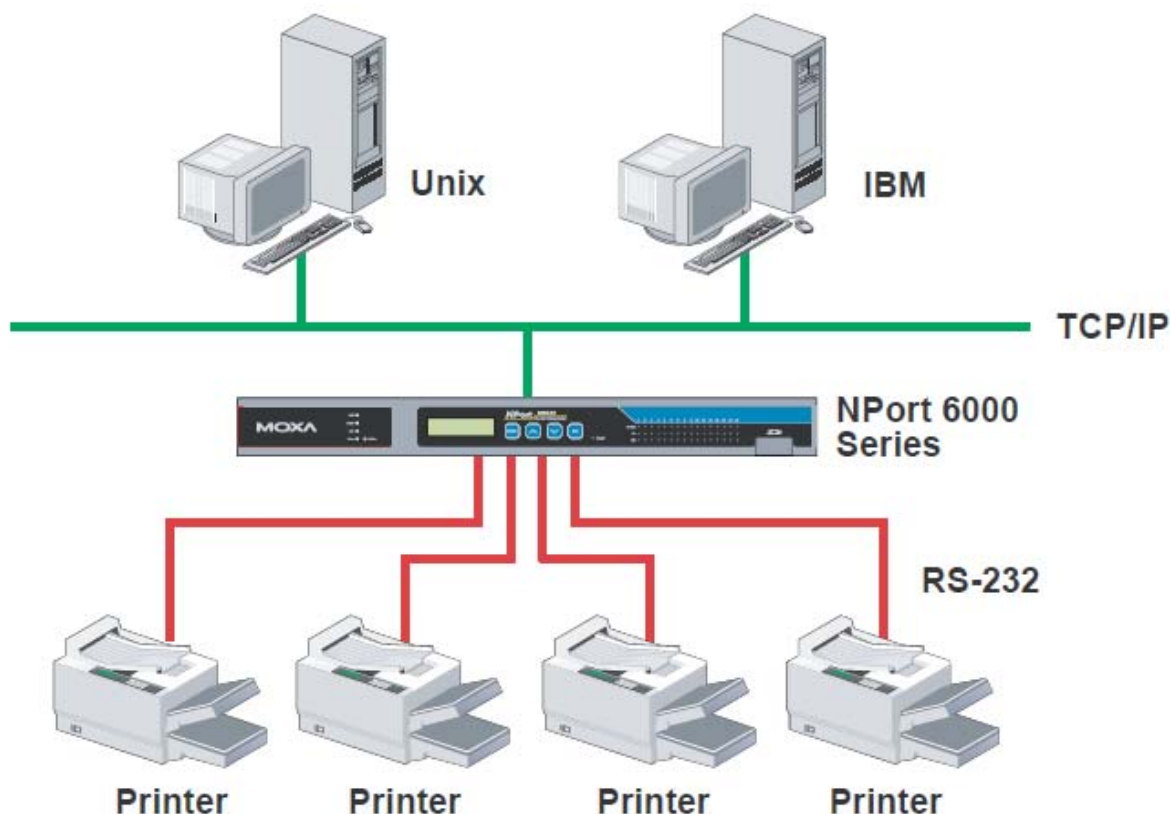
Reverse Telnet

Данный режим широко применяется для управления устройствами из удаленных диспетчерских центров. Система ожидает, пока хост в сети установит соединение. Т.к. режим TCP Server не осуществляет преобразование команд CR/LF, то при необходимости такого преобразования следует использовать режим Reverse Telnet.

Reverse SSH

NPort 6000 также имеет режим Reverse SSH для обеспечения возможности использования утилит на основе SSH, таких как PuTTY, для связи с удаленными серверами.

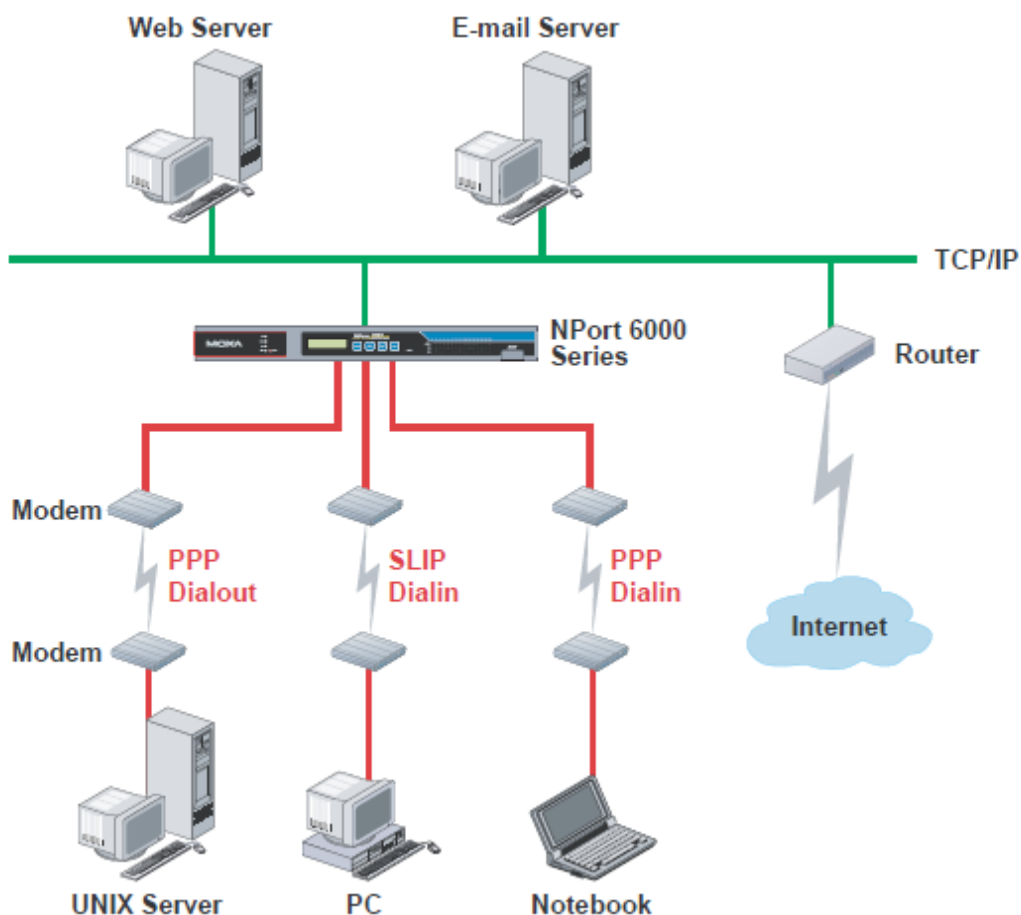
Режимы Printer



Режим Printer является прекрасным решением для банковских и биржевых сервисов с большими потребностями в печати. Данный режим объединяет в сеть принтеры, подключенные к последовательному порту Nport'a 6000, с номером порта, назначенным для определения положения принтера. Windows или UNIX-хосты могут получать доступ к принтерам в режимах RAW или LPD.

См. главу 7 – детальную информацию и указания по настройке.

Режимы Dial In/Out



NPort 6000 обеспечивает возможность доступа в интернет через телефонную линию для предприятий, которым необходим удаленный доступ. Когда удаленный пользователь использует соединение по телефонной линии по протоколу PPP, NPort 6000 играет роль dial-up сервера, и обеспечивает проверку авторизации пользователя в сети посредством NPort 6000 User Table или RADIUS Server. См. главу 9 – где подробно описаны настройки NPort 6000 User Table.

NPort 6000 поддерживает протоколы PPP, SLIP и Terminal для доступа dial-in/dial-out. Независимо от используемой операционной системы Вы всегда можете использовать стандартный PPP dial-up для установления соединения. NPort 6000 также может выполнять роль маршрутизатора для подключения последовательных портов в глобальную сеть. Могут быть назначены протоколы маршрутизации (static, RIP I и RIP II) для маршрутизации в разных глобальных сетях.

См. главу 5 – подробнее о настройках.

Режим Disabled

Можно отключить любой порт NPort'a 6000, установив режим Disabled.

5 Настройка через WEB-консоль

WEB-консоль имеет дружелюбный пользовательский интерфейс, позволяющий настраивать NPort 6000. Используя стандартный браузер, можно легко изменять настройки и режимы. В данной главе описана WEB-консоль и основные настройки. Те же самые настройки доступны по Telnet и последовательной консоли.

Данная глава содержит следующие разделы:

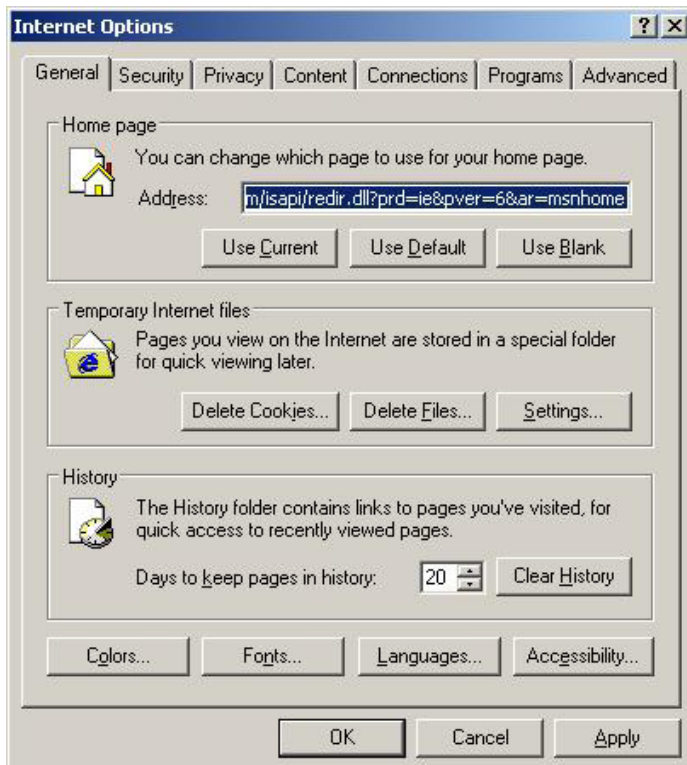
- **Использование WEB-браузера**
 - Настройки Browser Cookie
 - Установка надежных узлов
 - Открытие WEB-консоли
- **Навигация в WEB-консоли**
- **Basic Settings (Основные настройки)**
 - Настройки Server
 - Настройки Time
- **Network Settings (Сетевые настройки)**
 - Basic Network Settings (Основные сетевые настройки)
 - Avanced Network Settings (Расширенные сетевые настройки)
 - Configuring Route Table (Конфигурация таблицы маршрутизации)

Использование WEB-браузера

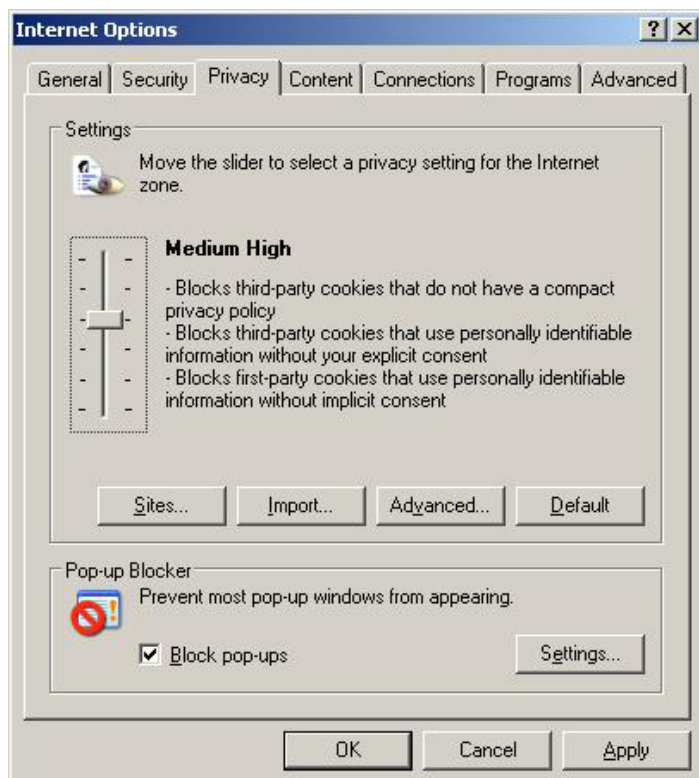
Настройки Browser Cookie

Убедитесь, что для Вашего браузера включены Cookies. Если они отключены, вы не сможете использовать WEB-консоль. (Cookies используются только для передачи пароля).

1. В Internet Explorer активировать Cookies можно через свойства обозревателя: Меню Сервис->Свойства обозревателя:



2. Выберите вкладку «Privacy» (Конфиденциальность). Есть 6 уровней конфиденциальности: Блокировать все файлы «cookies», высокий, умеренно высокий, средний, низкий и принимать все файлы. Нужно выбрать умеренно высокий уровень (Medium High) или ниже, как показано на рисунке для того, чтобы иметь доступ к WEB-консоли NPort 6000.



ВНИМАНИЕ

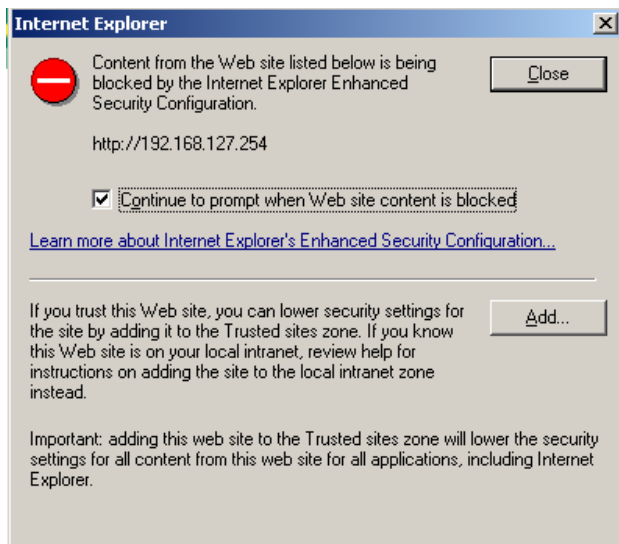


Если не используется Internet Explorer, cookies обычно включены установкой web-браузера «разрешить все cookies, сохраненные для данном компьютере» или «разрешить все cookies в данной сессии».

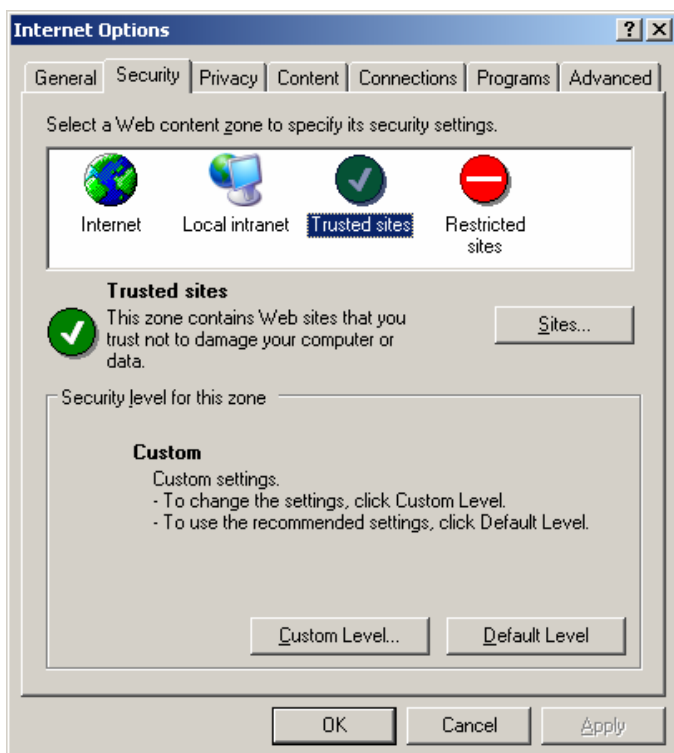
Установка надежных узлов

Пользователям Windows 2003 возможно будет необходимо добавить IP-адрес NPort'a 6000 в список доверенных сайтов браузера.

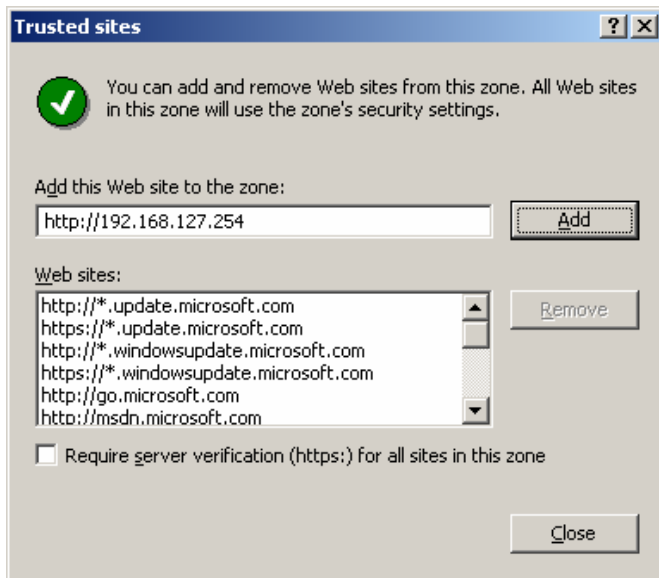
1. Если при попытке открытия WEB-консоли появляется показанное ниже окно, щелкните по кнопке **Add...** (Добавить...) для изменения списка надежных сайтов:



Вы можете также напрямую обратиться к списку надежных узлов через окно Свойства обозревателя -> вкладка Безопасность (Security), затем щелкните на пиктограмме Надежные узлы (Trusted Sites) и нажмите кнопку **Sites...**:



2. В обоих случаях в итоге должно появиться окно, показанное ниже, показывающее список сайтов, которые были в ключены в список надежных узлов Internet Explorer. Добавьте IP-адрес NPort'a 6000 (его заводской IP-адрес: 192.168.127.254).



После добавления IP-адреса NPort'a 6000 в список надежных узлов можно будет открыть WEB-консоль, набрав IP-адреса NPort'a 6000 в строке браузера.

Открытие WEB-консоли

Откройте WEB-браузер и введите IP: 192.168.127.254 в адресной строке. Это адрес, установленный по умолчанию для NPort'a 6000; если был назначен другой адрес, введите его.

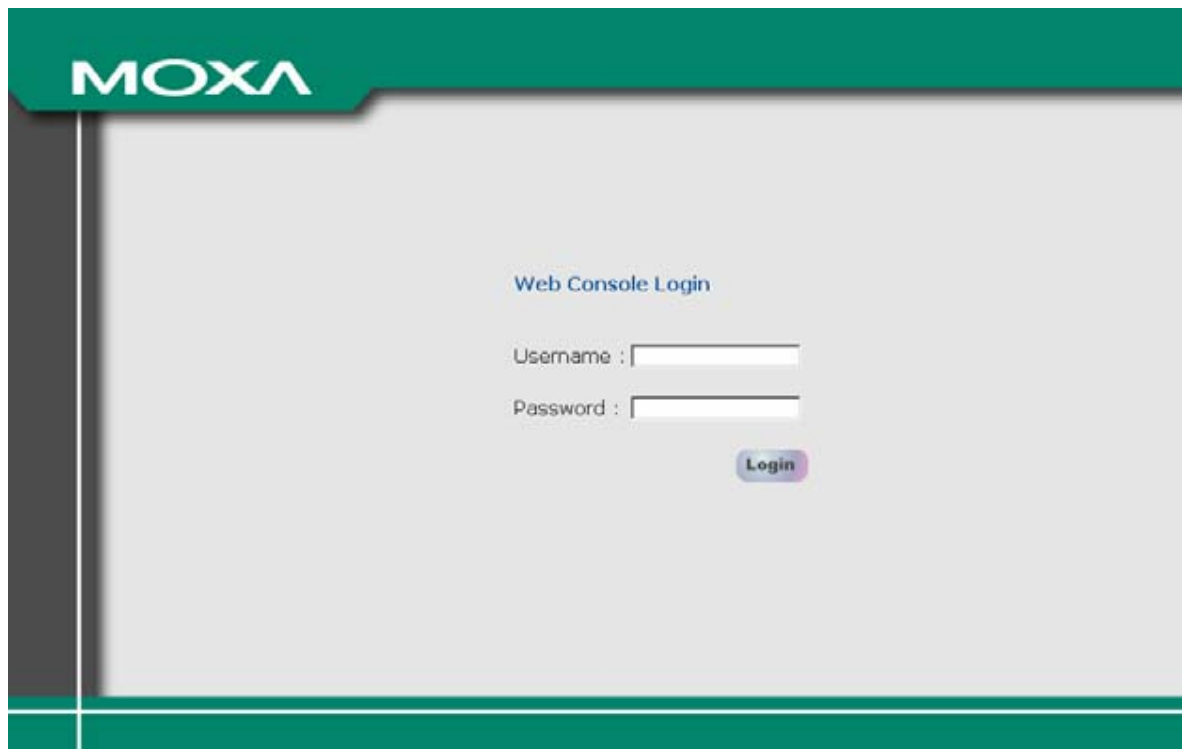
После ввода нажмите Enter.



ВНИМАНИЕ

Если не используется Internet Explorer, cookies обычно включены установкой web-браузера «разрешить все cookies, сохраненные для данном компьютере» или «разрешить все cookies в данной сессии».

Одновременно в WEB-консоли может быть авторизован только один пользователь. При отсутствии активности пользователя в течение 5 минут, производится автоматический выход из системы. По умолчанию установлен логин «**Admin**» без пароля. Только пользователь admin может обновлять прошивку устройства.



ВНИМАНИЕ

Если в WEB-браузере появляются сообщения **“Login Error”** или **“Already Login”**, это означает, что пользователь еще авторизован или при закрытии WEB-браузера не был произведен выход из системы. Если Вы забыли выйти из системы, подождите 5 минут или перезапустите NPort.

Если Вы забыли пароль, единственный способ войти в настройки NPort 6000 – использовать кнопку reset для сброса всех настроек и загрузки всех заводских установок. Если кнопка reset отключена в настройках NPort 6000, то Вы все же можете использовать ее для восстановления заводских установок в течение первых 60 секунд после включения NPort 6000.

Для восстановления конфигурации NPort'a используйте функцию экспорта настроек в файл. Это поможет сэкономить время, если будет забыт пароль и придется загружать заводские настройки.

Внешний вид начальной страницы WEB-консоли NPort 6000.



Навигация в WEB-консоли

В WEB-консоли NPort 6000 левая панель предназначена для навигации и содержит раскрывающееся меню для перемещения по различным настройкам. При выборе конкретного пункта меню в панели навигации в основном окне будет показано соответствующее содержимое данного пункта.

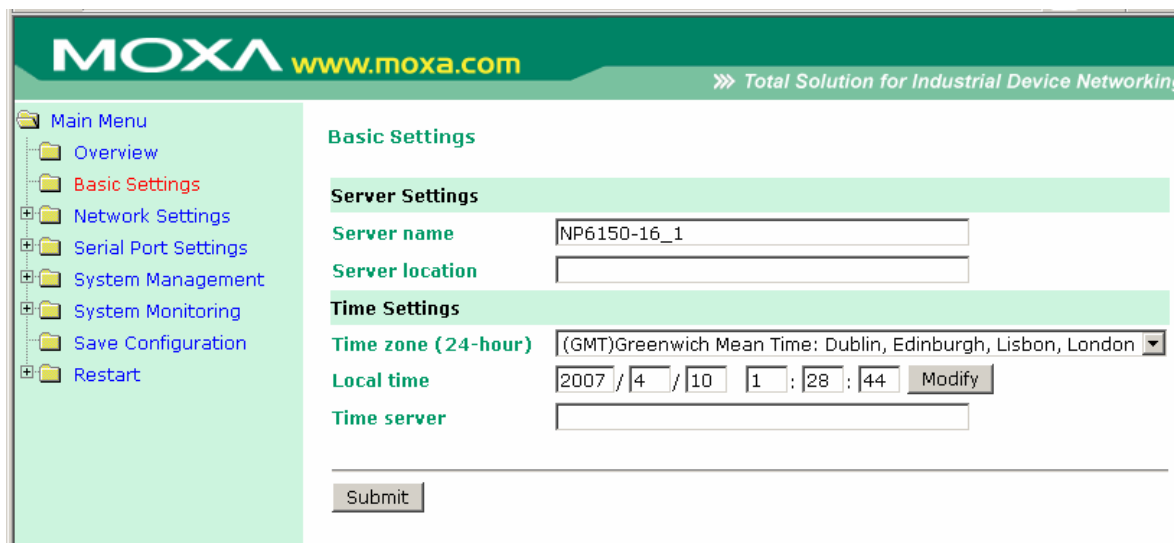
Для того, чтобы изменения в настройках вступили в силу, необходимо нажать кнопку **Submit**, расположенную внизу каждой страницы настроек. При переходе на другую страницу без нажатия данной кнопки изменения настроек не будут сохранены.

Изменения не вступят в силу до тех пор, пока не будут сохранены и Nport не перезагрузится! Можно выполнить эти действия, нажав **Save/Restart** после подтверждения изменений. Если нужно выполнить несколько настроек перед перезагрузкой, можно сохранить промежуточные изменения нажатием **Save Configuration** в панели навигации. Если перезагрузить NPort 6000 без сохранения настроек, все изменения настроек будут проигнорированы.

Basic Settings

Основные настройки доступны из навигационной панели.

Server Settings



Server name: Текстовое поле, в котором можно задавать имя по своему усмотрению; это не влияет на Nport 6000. Может использоваться для того, чтобы проще различать Nport'ы 6000 между собой.

Server location: Текстовое поле, заполняемое по усмотрению пользователя; оно никак не влияет на работу Nport 6000. Полезно для описания местоположения NPort 6000. Эта пометка может быть полезна при обслуживании сети с несколькими серверами.

Time Settings

Nport 6000 имеет встроенные часы реального времени для функций, связанных со временем. В функциях автооповещения по e-mail (Auto Warning Email) или прерывания SNMP (SNMP trap) к сообщениям могут добавляться метки времени.

Перед настройками времени выберите правильный часовой пояс и подтвердите изменения. В консоли будет отображаться текущее время, соответствующее часовому поясу. Для изменения времени щелкните кнопку **Modify**, расположенную рядом с полем **Local field**. После подтверждения новых настроек в прошивке Nport 6000 будет изменено время GMT в соответствии с текущим часовым поясом и местным временем.



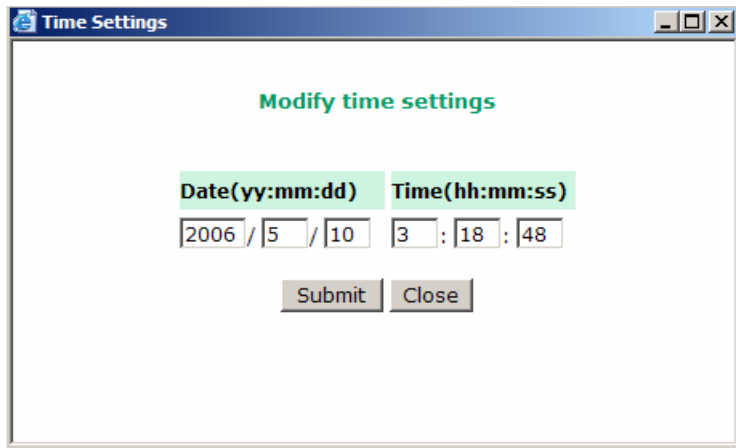
ВНИМАНИЕ

Взрывоопасна установка батареи неправильного типа!

Часы реального времени Nport 6000 питаются от литиевой батареи. Настоятельно рекомендуется не переустанавливать литиевую батарею без квалифицированной поддержки инженеров Мохы. Если Вам необходима замена батареи, свяжитесь с технической поддержкой Мохы.

Time zone (по умолчанию=GMT Greenwich Mean Time): В данном поле отображается текущий часовой пояс.

Local time: В этом поле показано время, в которое был открыта или обновлена страница в браузере. Для установки местного времени нажмите **Modify...**, затем подтвердите внесенные изменения в окне, показанном ниже.



Time server: NPort 6000 использует протокол SNTP (RFC-1769) для автонастройки времени. В этом поле можно задать IP-адрес или имя домена для сервера времени. После этого Nport 6000 будет запрашивать информацию о времени у сервера каждые 10 минут.

Network Settings

Basic Network Settings

Network Settings - Basic

IPv4 Configuration	
IPv4 configuration	Static
IPv4 address	192.168.127.254
Netmask	255.255.255.0
Gateway	
IPv4 DNS server 1	
IPv4 DNS server 2	
PPPoE user account	
PPPoE password	
WINS function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WINS server	
IPv6 Configuration	
IPv6 configuration	Auto
IPv6 address	
Prefix	64
IPv6 Gateway	
IPv6 DNS server 1	
IPv6 DNS server 2	
Connection priority	<input type="radio"/> IPv6 first (RFC 3484) <input checked="" type="radio"/> IPv4 first
Configuration	
LAN1 speed	Auto

Открыть настройки **Basic Network Settings** можно, раскрыв пункт **Network Settings** в панели навигации. В **Basic Network Settings** прописываются IP-адрес Nport'a 6000, маска подсети, шлюз и другие параметры IP-сетей.

ПРИМЕЧАНИЕ: Перед подключением NPort'a 6000 в сеть необходимо назначить ему корректный IP-адрес. Уникальный IP-адрес и соответствующие сетевые настройки выдаются

системным администратором. Новым пользователям NPort 6000 рекомендуется обратиться к главе 3 за дополнительной информацией.

IPv4 Configuration (default=Static): Можно выбрать один из 4-ех режимов.

Режим	Описание
Static	IP-адрес, маска подсети, шлюз задаются пользователем.
DHCP	IP-адрес, маска подсети, шлюз, DNS и сервер времени назначаются DHCP-сервером
DHCP/BOOTP	IP-адрес, маска подсети, шлюз, DNS и сервер времени назначаются DHCP-сервером, либо, если не отвечает DHCP-сервер, то IP-адрес назначается BOOTP-сервером
BOOTP	IP-адрес назначается BOOTP-сервером
PPPoE	Протокол PPP по Ethernet – удаленный провайдер назначает IP-адрес.

IPv4 Address (по умолчанию=192.168.127.254): Назначьте IP-адрес NPort'у 6000. Все последовательные порты NPort'а 6000 будут иметь один и тот же IP. IP-адрес – постоянный числовой адрес, назначаемый сетевым устройствам. Компьютеры используют IP-адрес для идентификации при обмене по сети. IP-адрес устройства должен быть уникальным для данной сети.

Netmask (по умолчанию=255.255.255.0): Задайте маску подсети. Маска подсети объединяет все хосты, расположенные в одной географической точке, в одном здании или в одной и той же локальной сети.

При пересылке пакета по сети NPort 6000 использует маску подсети для определения того, находится ли хост-получатель в том же сегменте локальной сети или нет. Если адрес из той же самой подсети, что и NPort 6000, то соединение с хостом устанавливается напрямую через NPort 6000. В противном случае соединение устанавливается через заданный по умолчанию шлюз.

Gateway: Если необходимо, введите IP-адрес шлюза. Шлюз – это сетевой компьютер, который используется для перехода к другим сетям. Обычно компьютеры, контролирующие трафик внутри сети или локального Интернет-провайдера, являются шлюзами. NPort'у 6000 должен быть известен IP-адрес шлюза, используемого по умолчанию, для обмена с хостами, находящимися за пределами данной локальной сети. Корректный IP-адрес шлюза нужно узнать у сетевого администратора.



ВНИМАНИЕ

В сетях с динамическими IP-адресами встроенное ПО NPort'а 6000 будет производить попытки получения сетевых настроек с DHCP или BOOTP-серверов 3 раза каждые 30 секунд до тех пор, пока они не будут назначены. Первая попытка заканчивается через 1 секунду, вторая - через 3 секунды, третья – через 5 секунд.

Если DHCP/BOOTP-серверы недоступны, встроенное ПО будет использовать IP-адрес (192.168.127.254), маску подсети и шлюз по умолчанию.

IPv4 DNS server 1: Это поле необязательно заполнять. Если Ваша сеть имеет доступ к DNS-серверу, то в этом поле можно указать его IP-адрес. Это позволяет NPort'у 6000 использовать доменные имена хостов вместо IP-адресов.

Система доменных имен (DNS) – способ идентификации и преобразования доменных имен интернета в IP-адреса. Доменное имя – это буквенно-цифровое название, например, www.moxa.com, которое проще запомнить, чем числовой IP-адрес. DNS-сервер – хост, преобразующий это текстовое доменное имя в действующий IP-адрес, используемый для установления TCP/IP-соединения.

Когда пользователь желает посетить конкретный сайт, его компьютер посылает доменное имя (например, www.moxa.com) DNS-серверу для запроса числового IP-адреса веб-сайта. После получения IP-адреса сайта с DNS-сервера, пользовательский ПК использует его для подключения к серверу, на котором размещен веб-сайт.

NPort 6000 играет роль DNS-клиента: он инициирует запрос DNS-сервера об IP-адресе, связанном с конкретным доменным именем. Использование доменных имен вместо IP-адрес поддерживают следующие функции: Time Server, Destination IP Address (в режиме TCP Client), Mail Server, SNMP Trap Server, Destination Address (в режиме Pair Connection), Primary/Secondary Host Address (в режиме Terminal), RADIUS Server, TACACS+Server и SMTP Server.

IPv4 DNS server 2: Это необязательный параметр. IP-адрес второго DNS-сервера можно ввести для того, чтобы он использовался, когда недоступен DNS server 1.

PPPoE user account и PPPoE password: В динамических широкополосных сетях (на основе xDSL или кабельного модема) для установления соединения пользователи должны указать логин и пароль, выдаваемые провайдером. Если последовательный порт в NPort 6000 настроен в режиме PPPoE, введите логин и пароль в данные поля.

WINS function (по умолчанию=enable – включена): включает или отключает WINS-сервер (Windows Internet Naming Server).

WINS server: Если WINS-сервер подключен к сети, введите его IP-адрес в данном поле. Протокол TCP/IP использует IP-адреса для определения хостов, однако пользователи чаще используют символьные имена, такие как имена компьютеров.

Что такое IPv6?

IPv6 – стандарт Internet Protocol версии 6. Это вторая версия интернет-протокола, представленная после предыдущей IPv4. Отличаются данные версии длиной IP-адресов. В IPv4 используются 32-битные IP-адреса, а в IPv6 128-битные. IPv4 в настоящее время остается основным протоколом сети Интернет.

IPv6 Configuration (по умолчанию=Static): Можно выбрать из нескольких вариантов настроек IPv6:

Вариант выбора	Описание
Auto	Назначается маршрутизатором IPv6. Шаг 1: NPort автоматически назначает локальный адрес для связи. Шаг 2: NPort посылает запрос маршрутизатору «Router solicitation» для получения от него IP-адреса. 2.1 Маршрутизатор назначает IP-адрес NPort'у Шаг 4. 2.2 Маршрутизатор выдает адрес DHCPv6-сервера для назначения IP-адреса → Шаг 3. 2.3 Маршрутизатор не отвечает (например, такого маршрутизатора нет в сети) → Шаг 3. Шаг 3. NPort пытается получить IP-адрес от DHCPv6-сервера. Шаг 4. Процесс получения IP завершен.
Static	Определяемый пользователем IP-адрес, маска подсети, шлюз.
Disable	Использовать IPv4.

IPv6 Address (по умолчанию=Auto): В этом поле указывается IPv6-адрес, назначенный NPort'у 6000. Все последовательные порты NPort'a 6000 будут иметь данный IP. IP-адрес должен быть уникальным в данной подсети.

Prefix: Префикс – это часть адреса, которая показывает биты, которые имеют фиксированное значение или биты подсети. Префиксы для подсетей IPv6, маршрутов и диапазонов адресов назначаются по правилам CIDR (Classless Inter-Domain Routing) IPv4. Префикс IPv6 записывается по правилам длины адреса/префикса. Например, 21DA:D3::/48 и 21DA:D3:0:2F3B::/64 – адресные префиксы IPv6.

Замечание: IPv4 используют представление адресов с разделением точками, известное как маска подсети. Маска подсети не используется в IPv6. Поддерживается только нотация длины префикса.

IPv6 Gateway

Gateway: При необходимости в этом поле прописывается IP-адрес маршрутизатора (основного шлюза). Шлюз – сетевое устройство, используемое для перехода в другую сеть. Обычно такими узлами являются компьютеры, управляющие внутрисетевым трафиком, или устройства Интернет-провайдера. Для получения точной информации об IPv6-адресе шлюза обращайтесь к своему сетевому администратору.

IPv6 DNS server 1: Это необязательное для заполнения поле.

IPv6 DNS server 2: Это необязательное для заполнения поле. В нем можно указать IP-адрес DNS-сервера, к которому нужно обращаться, когда недоступен первый DNS-сервер.

Connection Priority: Данную функцию рекомендуется использовать, когда NPort 6000 использует доменное имя для определения IP-адреса удаленного хоста/сервера. В приложениях такого рода NPort 6000 будет запрашивать IP-адрес удаленного хоста/сервера у DNS-сервера; в случае если эти хосты/серверы имеют и IPv4 и IPv6-адреса, DNS-сервер укажет в ответе оба этих адреса. Для таких случаев нужно определить приоритет: «IPv6 first (RFC3484) или IPv4 first».

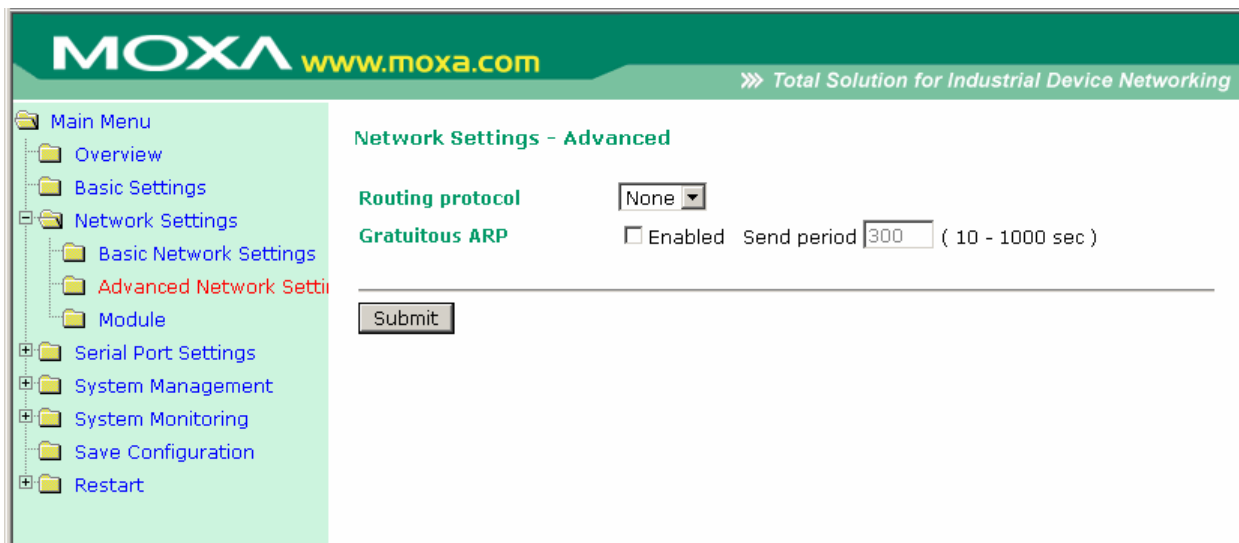
Примеры случаев применения, когда IP-адрес определяется по доменному имени:

Применение	Time Server, DDNS, WINS, RADIUS Server, TACACS+Server, Remote Syslog, E-mail Alert, SNMP Trap Alert.
Режим последовательного порта	TCP Client, Reverse RealCOM, Pair Connection, Terminal

LAN1 speed (по умолчанию=Auto): Можно настроить скорость обмена для встроенного Ethernet-порта NPort'a 6000. Ethernet-стандарт IEEE 802.3 поддерживает автоопределение скорости передачи. Однако для некоторых хабов/концентраторов требуется установить фиксированное значение скорости: 100Мбит/с или 10Мбит/с. Необходимо помнить, что нет возможности настраивать скорость обмена для дополнительных модулей к NPort'ам 6600 и 6450.

Advanced Network Settings (Расширенные сетевые настройки)

Пункт настроек Advanced Network Settings виден при раскрытии вкладки Network Settings панели навигации. В данных настройках выбирают протокол маршрутизации и настраивают протокол ARP (преобразования адресов).



Что такое RIP?

RIP (Routing Information Protocol) – это протокол, используемый для управления маршрутизацией пакетов внутри автономных сетей, например, корпоративных локальных сетей (LAN) или внутри объединенных групп сетей (LAN).

По этому протоколу шлюз с функцией роутера может каждые 30 секунд отсылать ближайшим хостам таблицу маршрутизации, содержащую все известные ему хосты. В свою очередь соседние хосты, получив таблицу, направляют данную информацию своим ближайшим соседям и т.д., до тех пор, пока все хосты внутри сети не будут иметь одинаковую информацию о маршрутах. Данное состояние сети называется конвергенцией. В протоколе RIP используется подсчет числа шагов маршрута пакета для определения длины сети. (В других протоколах могут использоваться более сложные алгоритмы, учитывающие временные задержки.) После отсылки пакета в его заголовке указывается конкретная точка назначения, сетевой маршрутизатор, используя таблицу маршрутизации, определяет адрес следующего хоста, на который следует направлять пакет.

RIP считается эффективным решением для небольших однородных сетей. В больших, сложных сетях, отправка таблицы маршрутизации через каждые 30 секунд, может привести к коллапсу сети из-за огромного количества трафика.

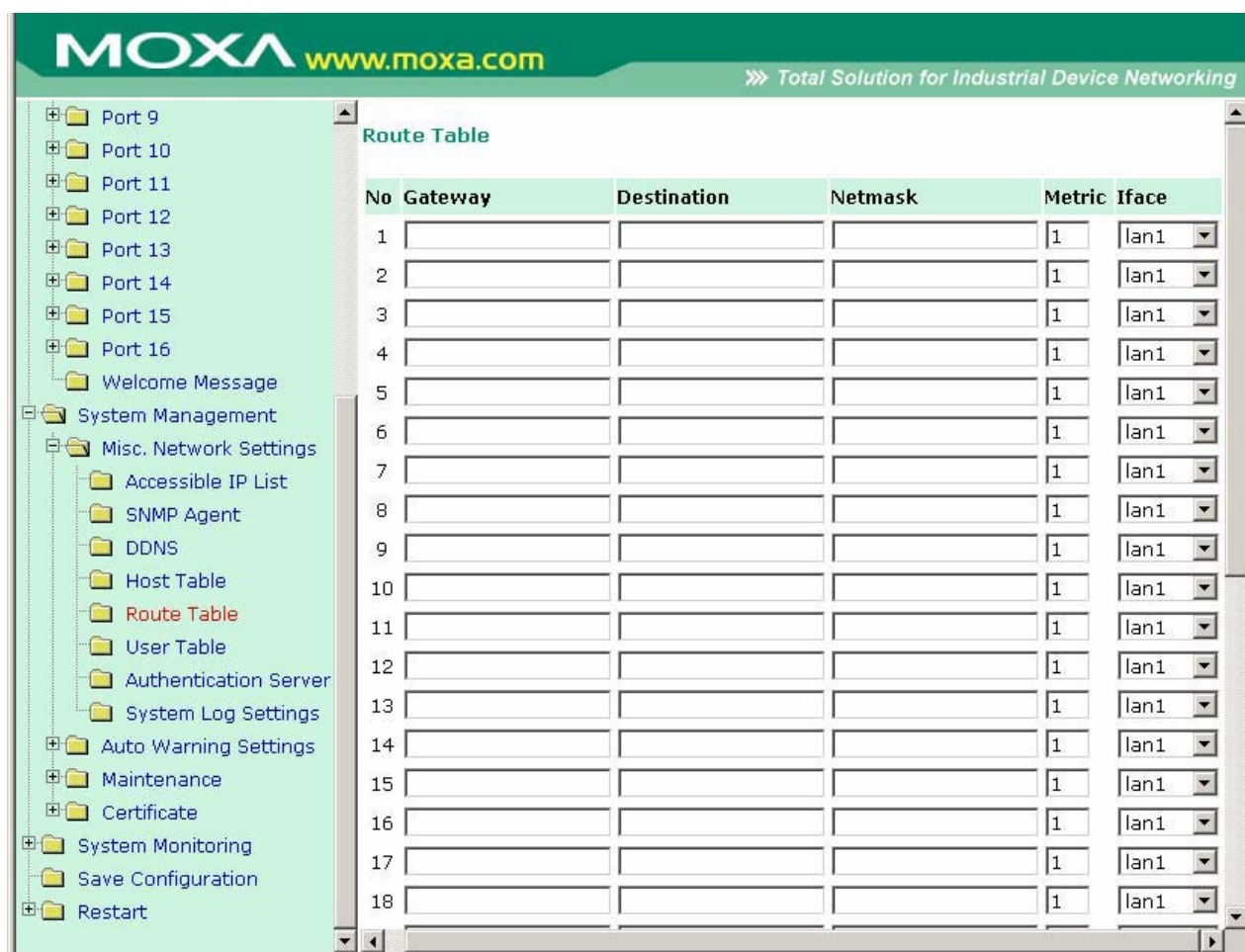
RIP 2 является расширением RIP. Его назначение – увеличить объем полезной информации, содержащейся в RIP-пакетах и добавить элементы безопасности. RIP 2 стал стандартной версией RIP, исходный протокол RIP больше не используется.

Routing Protocol: Можно выбрать один из протоколов маршрутизации, подходящий для Вашей сети.

Gratuitous ARP: В некоторых приложениях может понадобиться рассылка NPort'ом 6000 широковещательных сообщений для обновления ARP-таблицы сервера. Если активирована данная функция и установлена периодичность рассылки [send period], то NPort 6000 будет периодически рассылать широковещательные пакеты в установленные временные интервалы.

Заполнение таблицы маршрутизации

Таблица маршрутизации настраивается на вкладке Route Table (подпункт меню System Management->Misc. Network Settings). В таблице маршрутизации прописывается, каким образом NPort'у 6000 связываться с внешними сетями.



No	Gateway	Destination	Netmask	Metric	Iface
1				1	lan1
2				1	lan1
3				1	lan1
4				1	lan1
5				1	lan1
6				1	lan1
7				1	lan1
8				1	lan1
9				1	lan1
10				1	lan1
11				1	lan1
12				1	lan1
13				1	lan1
14				1	lan1
15				1	lan1
16				1	lan1
17				1	lan1
18				1	lan1

В таблице может быть сделано до 32 записей. В каждой строке нужно прописывать информацию о шлюзе, сети назначения, маске подсети, метрику и используемый порт.

Gateway: IP-адрес следующего роутера (основной шлюз).

Destination: IP-адрес хоста или сети назначения.

Netmask: Маска подсети назначения.

Metric: Можно использовать это дополнительное поле для ввода числа шагов от источника сообщения до получателя. Это позволяет NPort'у 6000 расставлять приоритеты для нескольких возможных маршрутов доставки одного и того же пакета.

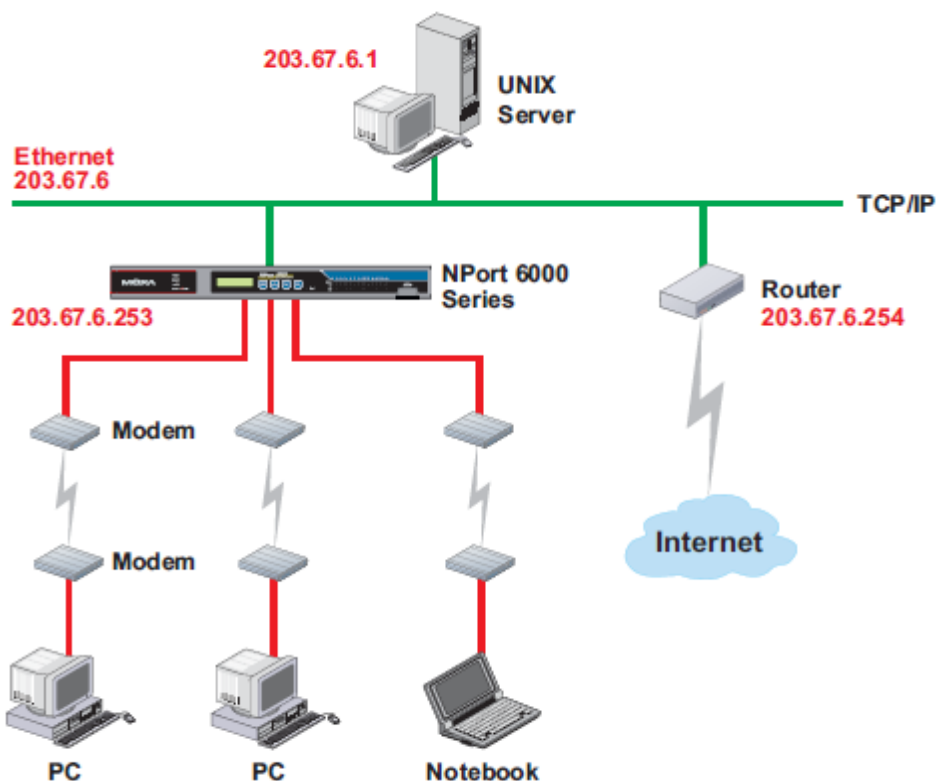
Iface: Сетевой интерфейс (порт NPort'a 6000), используемый для передачи пакета.



ВНИМАНИЕ

При использовании режима PPP/SLIP для последовательных портов в поле Iface должен быть указан соответствующий последовательный порт.

Настройка маршрутизации в Интернет



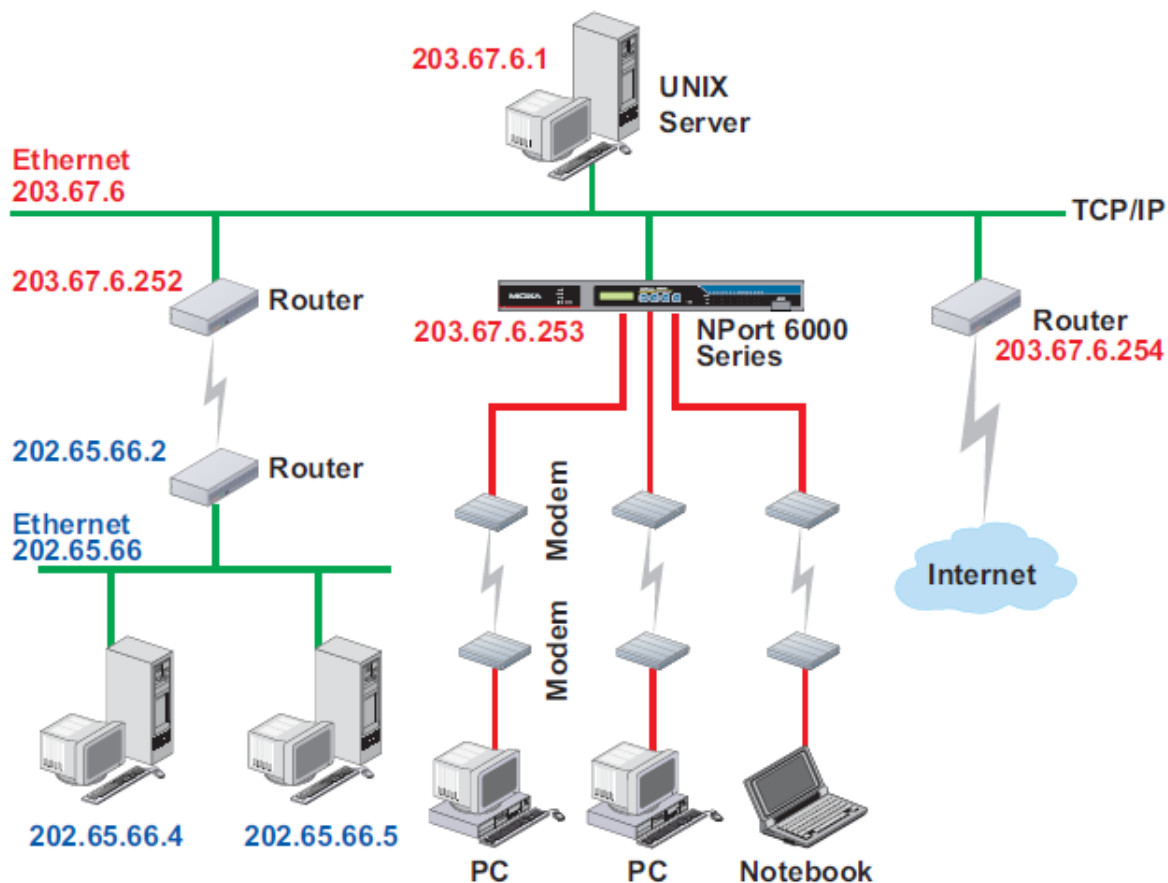
В данном примере ноутбук связывается с NPort'ом 6000 для запроса соединения с Интернет-хостом **240.48.96.9**, который находится за пределами локальной сети **203.67.6.xxx**. В данном случае NPort 6000 выступает в роли маршрутизатора и посылает дейтаграммы к назначенному следующему маршрутизатору – **203.67.6.254**. В данном случае нужно добавить IP-адрес шлюза – **203.67.6.254** – в таблицу маршрутизации для установления перехода к следующему шагу маршрутизации до узла **210.48.96.9**.

The screenshot shows the MOXA web interface with the 'Route Table' configuration page. The table is as follows:

No	Gateway	Destination	Netmask	Metric	Iface
1	203.67.6.254	210.48.96.9	255.255.255.255	1	lan
2				1	lan
3				1	lan
4				1	lan
5				1	lan
6				1	lan
7				1	lan
8				1	lan
9				1	lan
10				1	lan
11				1	lan
12				1	lan
13				1	lan
14				1	lan
15				1	lan
16				1	lan
17				1	lan
18				1	lan

В общем случае выход в Интернет осуществляется назначением основного шлюза в сетевых настройках, а не в таблице маршрутизации.

Настройка маршрутизации в Интранет



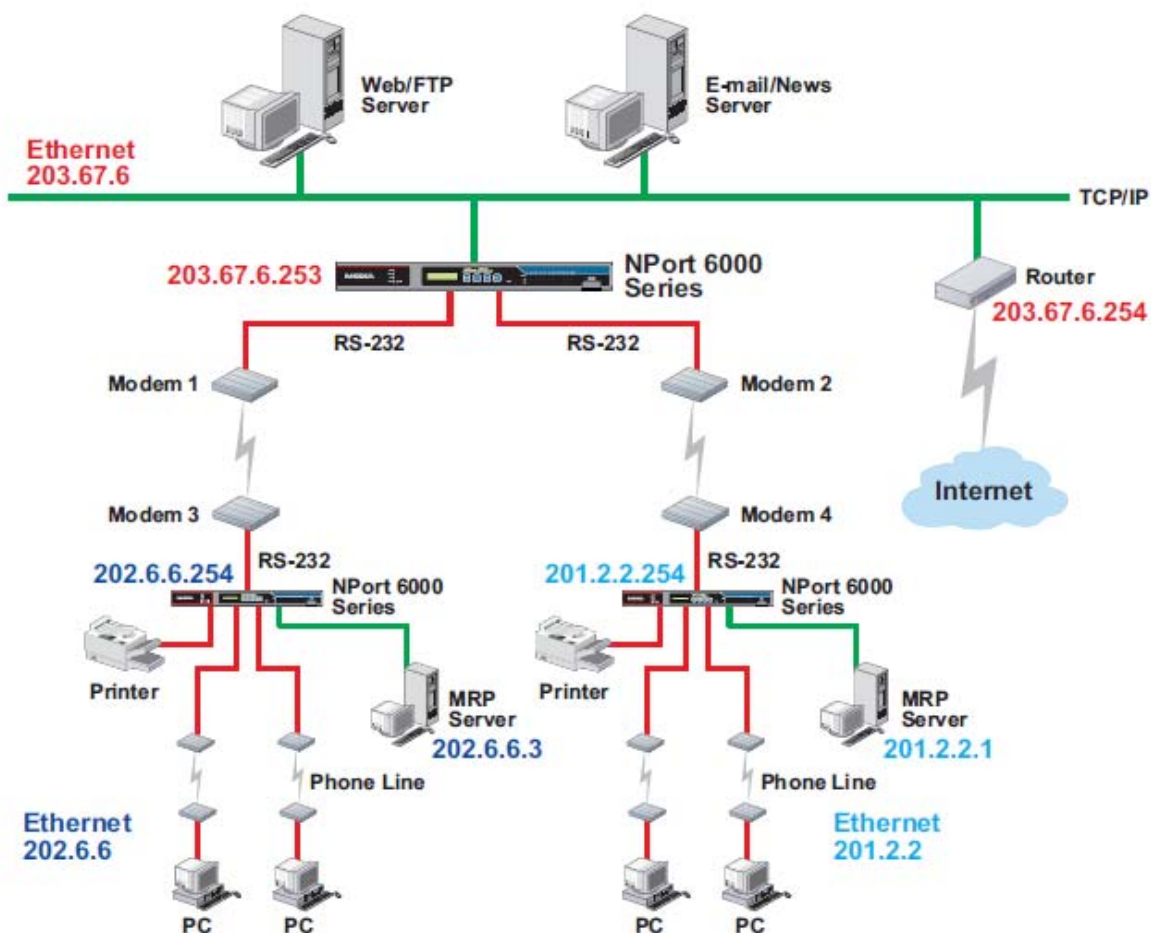
В данном примере пользователи, устанавливающие dial-in-соединение могут посылать запросы к Intranet-хостам **202.65.66.4** или **202.65.66.5**, которые находятся в подсети **202.65.66.xxx** (т.е. находятся не в подсети **203.67.6.xxx**). Метрика в данном случае равна 2-м шагам.

MOXA www.moxa.com »» Total Solution for Industrial Device Networking

- Main Menu
 - Overview
 - Basic Settings
 - Network Settings
 - Serial Port Settings
 - System Management
 - Misc. Network Settings
 - Accessible IP List
 - SNMP Agent
 - DDNS
 - Host Table
 - Route Table
 - User Table
 - Authentication Server
 - System Log Settings
 - Auto Warning Settings
 - Maintenance
 - System Monitoring
 - Save Configuration
 - Restart

No	Gateway	Destination	Netmask	Metric	Iface
1	203.67.6.252	202.65.66.0	255.255.255.0	2	Ian
2				1	Ian
3				1	Ian
4				1	Ian
5				1	Ian
6				1	Ian
7				1	Ian
8				1	Ian
9				1	Ian
10				1	Ian
11				1	Ian
12				1	Ian
13				1	Ian
14				1	Ian
15				1	Ian
16				1	Ian
17				1	Ian

Настройка многоточечной маршрутизации

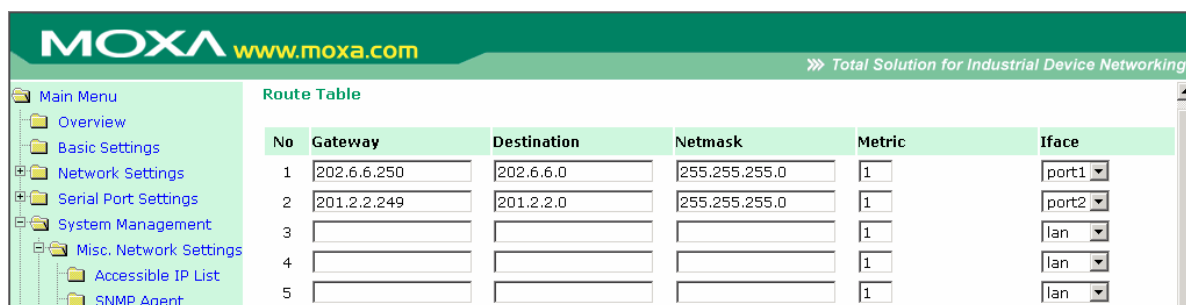


Для распределенных предприятий серверы NPort 6000 можно размещать в различных офисах и использовать одновременно как роутеры и серверы удаленного доступа. Когда hosts (например, Web/FTP и E-mail/News-серверы, показанные на рисунке) посылают запросы к узлам из других подсетей, например, 202.6.6.xxx или 201.2.2.xxx, соответствующий NPort 6000 направляет запросы на ближайший NPort 6000 на удаленном конце сети: 202.6.6.254 или 201.2.2.254 – как на следующий шаг маршрутизации.

В данном примере: Modem 1 подключен к последовательному порту port 1, Modem 2 – к port 2, и IP-адреса модемов-источников и приемников настроены в соответствии с таблицей ниже.

	Источник	Приемник		Источник	Приемник
Modem 1	203.67.6.250	202.6.6.250	Modem 3	202.6.6.250	203.67.6.250
Modem 2	203.67.6.249	201.2.2.249	Modem 4	201.2.2.249	203.67.6.249

В данном случае нужно добавить в таблице маршрутизации две строки, как показано на рисунке ниже:



6 Настройки модулей

В данной главе описываются дополнительные настройки, относящиеся к модулям NM-TX01, NM-FX01-M-SC, NM-FX01-S-SC, NM-FX02-M-SC, NM-FX02-S-SC и NM-GPRS/GSM. Данные настройки доступны и через Telnet и из последовательной консоли.

Глава содержит следующие разделы:

- **NM-TX01, NM-TX02, NM-FX01-M-SC, NM-FX01-S-SC, NM-FX02-M-SC, NM-FX02-S-SC**
 - Использование резервирования в сегментах Ethernet
 - Стандарт STP/RSTP
 - Различия между STP и RSTP
 - Пример STP
- **Настройка режима Turbo Ring**
 - Сущность Turbo Ring
 - Настройка Turbo Ring 2
- **Модуль NM-GPRS/GSM**
 - Режим GSM
 - Режим GPRS
 - Режим SMS
- **Модуль NM-Modem**

NM-TX01, NM-TX02, NM-FX01-M-SC, NM-FX01-S-SC, NM-FX02-M-SC, NM-FX02-S-SC

Использование резервирования в сегментах Ethernet

Использование технологий резервирования Ethernet (избыточных связей) в NPort 6000 помогает повысить надежность важных соединений, избежать сетевых петель и построить топологию «кольцо», сводя вероятность отказа сети к минимуму.

Функция Ethernet Redundancy (избыточные/резервные связи) позволяют объединять несколько NPort'ов 6000 в «кольцо» для обеспечения резервных маршрутов передачи данных в случае обрыва одной из связей. Это очень важно при применении в промышленных условиях, где поиск и устранение обрыва может занимать минуты. Даже несколько минут неработоспособности сети могут привести к большим производственным потерям.

Устройство NPort 6000 поддерживает 3 различных технологии резервирования: **Redundancy Spanning Tree Protocol (IEEE-802.1w)**, **Turbo Ring** и **Turbo Ring 2**.



ВНИМАНИЕ

Функция резервирования соединений доступна в NPort'ах 6450 и во всех серии NPort 6600, которые могут быть оборудованы одним из дополнительных сетевых модулей:

NM-TX01	Ethernet-модуль с одним портом RJ45
NM-TX02	Ethernet-модуль с двумя портами RJ45
NM-FX01-S-SC	Ethernet-модуль с одним портом с SC-разъемом для одномодового оптоволоконна
NM-FX01-M-SC	Ethernet-модуль с одним портом с SC-разъемом для многомодового оптоволоконна
NM-FX02-S-SC	Ethernet-модуль с двумя портами с SC-разъемами для одномодового оптоволоконна
NM-FX02-M-SC	Ethernet-модуль с двумя портами с SC-разъемами для многомодового оптоволоконна

Технологии Turbo Ring, Turbo Ring v2 и STP/RSTP не могут использоваться в одном кольце. Таблица ниже показывает ключевые отличия между данными технологиями. Используя данную информацию, Вы можете оценить преимущества каждой и выбрать подходящую для применения в Вашей сети.

Протокол	STP	RSTP
Топология	Кольцо, петля	Кольцо, петля
Время восстановления	До 30 сек	До 5 сек

Moха разработала запатентованную технологию Turbo Ring для оптимизации резервирования связей и достижения наименьшего времени восстановления сети. Протокол поддерживается как Ethernet-устройствами, так и серверами последовательного интерфейса. В связи с различиями в характере работы коммутаторов и последовательных серверов, время восстановления также различается.

Протокол	Turbo Ring		Turbo Ring 2	
	Кольцо		Кольцо	
Скорость/Время восстановления	921,6 Кбод/с	До 100 мс	921,6 Кбит/с	До 100 мс
	9600 бод/с	До 40 мс	9600 бод/с	До 20 мс

ПРИМЕЧАНИЕ: Время восстановления рассчитано при режиме работы последовательного порта “Real COM, N, 8, 1, Hi-Perfomance, HW flow control” NPort’a 6450; испытания проводились в течение 8 часов.

Стандарт STP/RSTP

Протокол «Разветвленного дерева» (STP) создан для обеспечения резервирования связей в сети и гарантирует отсутствие петель в топологии. Сети со сложной архитектурой подвержены «широковещательному шторму», появляющемуся из-за невыявленных замкнутых петель в топологии. Функция STP в NPort'ах 6000 по умолчанию отключена. Для эффективного использования данной функции она должна быть активна на всех NPort'ах 6000, входящих в сеть.

Технология RSTP включает алгоритм «Разветвленного дерева» (STP) и протокол, определяемый стандартом IEEE 802.1w-2001. RSTP дает следующие преимущества:

- Топология на основе сетевых мостов более быстродействующая по сравнению с STP.
- RSTP обратно совместима с технологией STP, делая переход на нее более простым. Например:
 - По умолчанию идет обмен протокольными блоками данных типа BPDU (Bridge Protocol Data Unit), если получаются пакеты данного формата.
 - STP (802.1D) и RSTP (802.1w) могут быть настроены для различных портов одного и того же NPort’a 6000.

Данные особенности оказываются очень полезны, когда NPort 6000 соединяется с более старым оборудованием, в том числе с ранними моделями NPort'ов 6000.

Обе данные технологии STP и RSTP – имеют одинаковое по сути назначение. Чтобы понять отличия между ними, обращайтесь к параграфу «Различия между STP и RSTP».

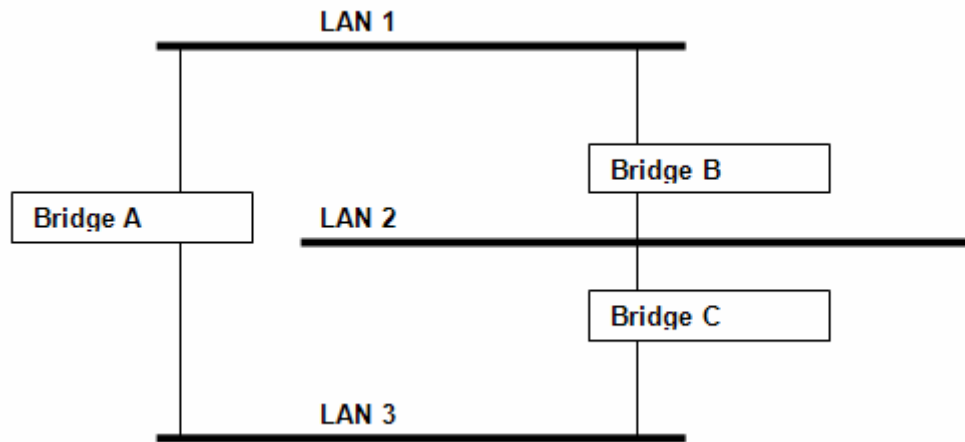
ПРИМЕЧАНИЕ: Протокол STP - часть стандарта IEEE 802.1D, 1998 Edition Bridge Specification. В примерах на схемах ниже вместо NPort'ов показаны сетевые мосты.

Что такое STP?

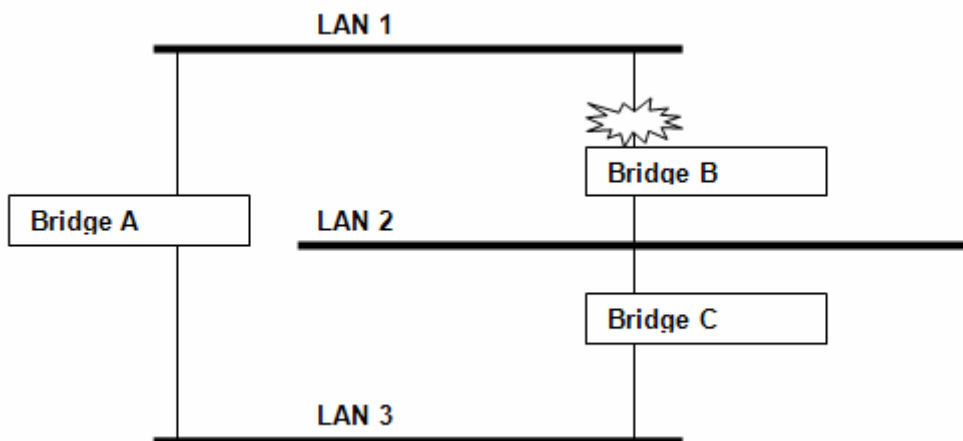
STP (802.1D) – сетевая архитектура на основе мостов, в которой используется несколько маршрутов передачи трафика. В STP реализована процедура выявления петель для:

- Выявления и отключения наименее эффективных маршрутов (например, с низкой полосой пропускания)
- Включения менее производительных участков сети в случае выхода из строя других.

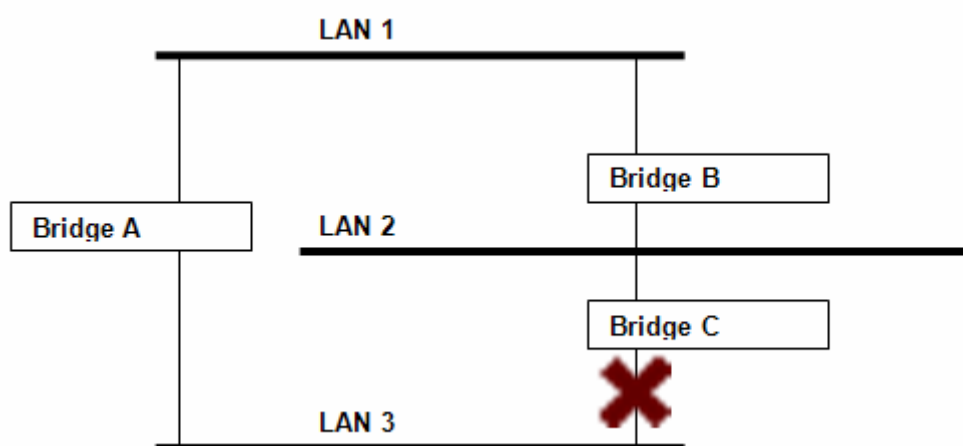
На рисунке ниже показана сеть, состоящая из трех локальных подсетей, соединенных между собой тремя мостами. Каждый сегмент может использовать два маршрута для связи с другими локальными сетями. Если функция STP не активна, то имеющиеся в топологии петли приведут к перегрузке сети.



Если функция STP включена, она определит дублирующие друг друга маршруты трафика и заблокирует передачу трафика по одному из них. В примере ниже STP определила, что данные между сегментами 1 и 2 лучше передавать через мосты С и А, т.к. соответствующие каналы имеют большую пропускную способность.



Что же происходит при обнаружении обрыва какого-либо канала? Как показано на рисунке ниже, STP перенаправит трафик между сегментами 1 и 2 через мост В.



Таким образом, STP определяет маршрут с большей пропускной способностью и блокирует дублирующие. На трех приведенных выше рисунках STP сначала определила, что путь трафика через мост С наиболее производителен, заблокировала передачу данных через мост В. После выхода из строя моста С STP пересчитала новое состояние сети и открыла передачу трафика через мост В.

Как работает технология STP

Когда функция STP активна, она подбирает наиболее производительный маршрут передачи сетевого трафика. Ниже описан способ решения данной задачи.

Требования технологии STP к сети

Для того, чтобы STP могла настроить сеть ее архитектура должна удовлетворять следующим требованиям:

- Обеспечены связи между всеми мостами. Данная связь поддерживается протокольными блоками данных (BPDU), которые передаются в широковещательных пакетах на заданные адреса.
- Каждый мост должен иметь идентификатор моста (Bridge Identifier), который определяет центральный мост, или Root Bridge; в STP мосты с меньшим значением Bridge Identifier рассматриваются как Root Bridge. Bridge Identifier вычисляется по MAC-адресу моста и приоритету, определенного для этого моста. По умолчанию для NPort 6000 установлен приоритет 32768.
- Каждому порту присвоена функция стоимости, определяющая эффективность каждой связи. Оценка эффективности передачи данных обычно определяется пропускной способностью канала; каналам с наименьшим значением пропускной способности присваивается большее значение функции стоимости.

Расчеты STP

Первый этап работы функции STP – выполнение расчетов. В этот момент все мосты сети обмениваются протокольными блоками данных. При этом вычисляются следующие характеристики:

- Какой мост будет выполнять функцию центральной точки, с которой начинается конфигурирование сети (Root Bridge).
- Вычисляется стоимость маршрута от каждого моста до центрального (Root Path Cost).
- Для каждого моста устанавливается его так называемый Root-порт, т.е. порт, связывающий данный мост с центральным наиболее эффективным маршрутом (т.е. маршрутом с меньшим значением функции стоимости). Соответственно сам центральный мост не имеет Root-порта.
- Для каждого сегмента локальных подсетей определяется назначенный мост [designated bridge], который связывает данную сеть с центральным мостом маршрутом с наименьшей функцией стоимости. Если для нескольких мостов стоимость маршрутов до центрального моста одинакова, то [designated] назначается мост с наименьшим значением [Bridge Identifier]. Данные в сторону центрального моста будут передаваться через [designated bridge]. Порт, подключающий данный сегмент, называется [designated bridge port] назначенным портом моста.

Настройка STP

После того, как назначен центральный мост и установлены другие необходимые параметры, каждый мост настраивается для передачи трафика только между своим гоо-портом и назначенными портами [designated bridge port] для соответствующих сегментов локальных сетей. Все остальные порты блокируются, это значит, что через них невозможна передача данных.

Перенастройка STP

После того, как топология сети установилась все мосты ожидают сообщения Hello от центрального моста в определенные временные интервалы. Если мост не получает данный служебный пакет в течение назначенного времени (max age time), он автоматически считает, что либо центральный мост, либо канал связи с ним вышли из строя. Это инициирует

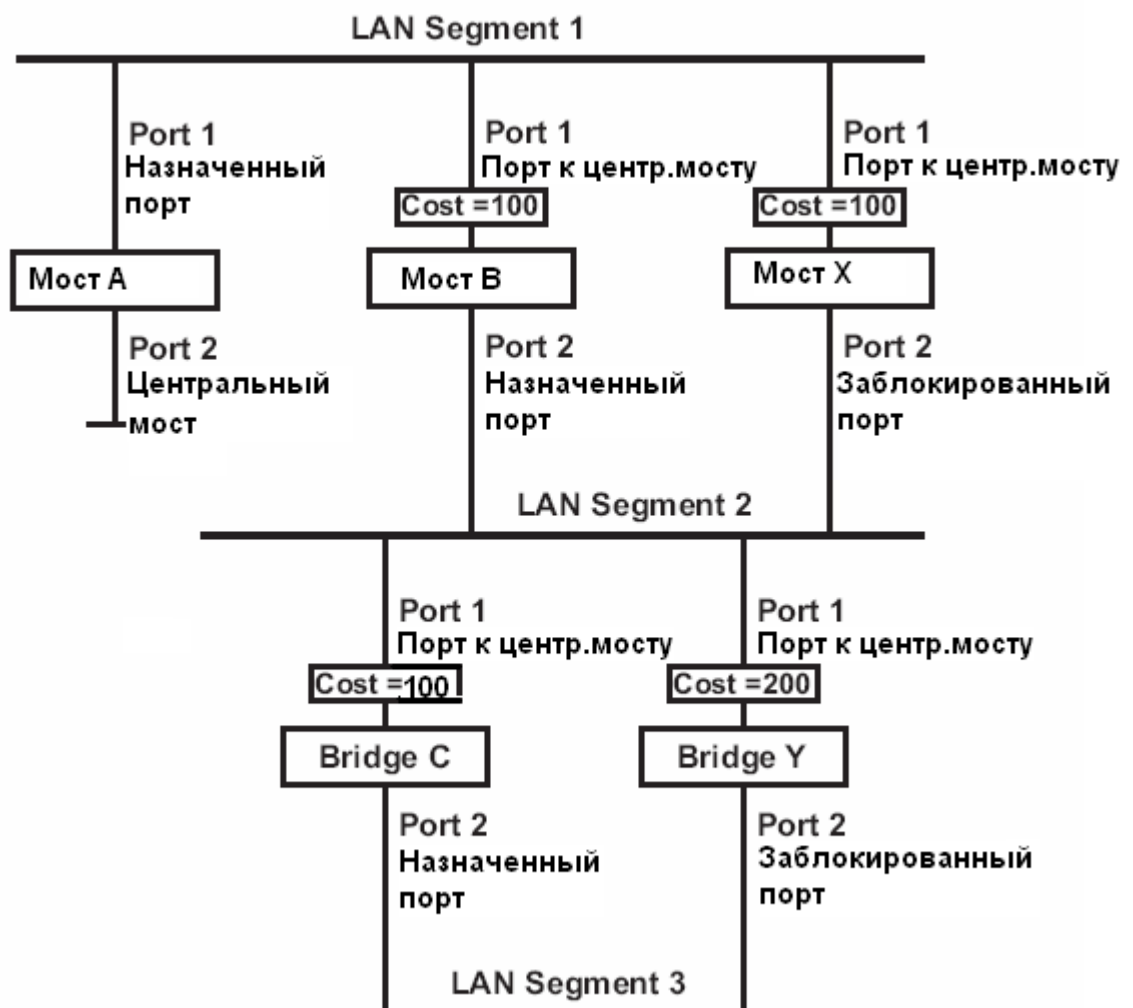
перенастройку сети. Если Вы настроили SNMP-прерывание, то при изменении топологии сети мост, первым обнаруживший изменения, отправляет на указанный адрес SNMP-прерывание.

Различия между STP и RSTP

Технология RSTP похожа на STP, но в пакетах BPDU содержится дополнительная информация, которая позволяет каждому мосту подтверждать, что были предприняты меры по предотвращению появления замкнутых петель в момент активации связи с ближайшим мостом. Мосты, соединенные по схеме «точка-точка» могут устанавливать соединение без ожидания, чтоб все остальные сетевые мосты успели отреагировать на изменения. Главное преимущество RSTP в том, что решения о настройках принимаются локально, что позволяет сети быстрее восстанавливать работу, чем при STP.

Пример STP

Локальная сеть, показанная ниже, состоит из трех сегментов, связанных между собой двумя маршрутами передачи данных. Также на рисунке показаны различные параметры STP, такие как Cost (функция стоимости), Root Port (порт связи с центральным мостом), Designated Bridge Port (назначенный порт сегмента) и Blocked Port (отключенный порт).



- Моста А выбран в качестве центрального, т.к. его параметр Bridge Identifier имеет наименьшее значение.
- Помимо того, что мост А центральный, он является назначенным мостом [designated bridge] для сегмента 1 локальной сети. Назначенным для этого сегмента портом выбран Port 1 моста А.

- Порты port 1 мостов В, С, Х и Y являются root-портами (связывающими с центральным мостом), т.к. от них самый короткий и, таким образом, самый эффективный путь до центрального моста.
- Мосты В и Х дублируют связь с сегментом 2 и имеют одинаковое значение функции стоимости. Однако мост В выбран в качестве назначенного моста для сегмента 2, поскольку имеет меньшее значение Bridge Identifier. Port 2 моста В выбран назначенным портом для сегмента 2.
- Мост С – назначенный мост для третьего сегмента, т.к. он имеет меньшую стоимость маршрута от сегмента 3 до центрального моста:
 - Путь через мосты С и В стоит 200 (от С до В=100, от В до А=100)
 - Путь через мосты Y и В стоит 300 (от Y до В=200, от В до А=100)
- Port 2 – назначенный порт для сегмента 3 локальной сети.

Настройка RSTP

Redundancy Settings

Redundancy protocol

Bridge priority

Hello Time (1 - 10 sec)

Forward Delay (4 - 30 sec)

Max Age [Hint] (6 - 40 sec)

Port	Enable RSTP	Port Priority	Port Cost
1	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="200000"/>
2	<input type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="200000"/>

Bridge priority (приоритет моста)

Диапазон значений	Описание	Значение по умолчанию
Число, выбираемое пользователем	Увеличение приоритета достигается выбором меньшего значения в данном поле. Устройство с большим приоритетом с большей вероятностью может быть назначено центральным мостом в топологии «Расширенное дерево».	32768

Hello time (интервал служебных сообщений), сек.

Диапазон значений	Описание	Значение по умолчанию
Число, выбираемое пользователем	Центральный мост в топологии ST периодически посылает сообщение «hello» остальным устройствам для проверки работоспособности сети. Параметр «hello time» задает временной интервал между последовательной отправкой этих сообщений.	2

Max. Age (максимальное время ответа), сек.

Диапазон значений	Описание	Значение по умолчанию
Число, выбираемое пользователем	Если данное устройство не является центральным мостом и не получает сообщение «hello» в течение времени [max. age], то это оно назначит себя в центральным мостом. После обнаружения в сети двух центральных мостов устройства автоматически перенастроятся на новую топологию ST.	20

Enable RSTP (для каждого порта)

Диапазон значений	Описание	Значение по умолчанию
Enable/Disable (Включить/Выключить)	Выбор режима функционирования порта в качестве узла топологии «дерево»	Disabled

Ограничения настроек RSTP/STP

Настройки для алгоритма топологии Spanning Tree имеют следующие ограничения параметров:

[Eq. 1]: $1 \text{ сек} \leq \text{Hello Time} \leq 10 \text{ сек}$

[Eq. 2]: $6 \text{ сек} \leq \text{Max. Age} \leq 40 \text{ сек}$

[Eq. 3]: $4 \text{ сек} \leq \text{Forwarding Delay} \leq 30 \text{ сек}$

Эти три переменные также связаны между собой тремя неравенствами:

[Eq. 4]: $2 \times (\text{Hello Time} + 1 \text{ сек}) \leq \text{Max. Age} \leq 2 \times (\text{Forwarding Delay} - 1 \text{ сек})$

Прошивка NPort 6000 выдаст предупреждение при нарушении приведенных выше условий. Например, настройки

Hello Time = 5 сек, Max. Age = 20 сек, Forwarding Delay = 4 сек удовлетворяют условиям Eq.1-3, но для них не выполняется условие Eq.4, поскольку:

$2 \times (\text{Hello Time} + 1 \text{ сек}) = 12 \text{ сек}$, and $2 \times (\text{Forwarding Delay} - 1 \text{ сек}) = 6 \text{ сек}$.

Выход из данной ситуации – например, увеличить значение Forwarding Delay по меньшей мере до 11 сек.

HINT: Выполните следующие шаги во избежание выбора значений параметров наугад:

Шаг 1: Выберите значение параметра «Hello Time» и затем вычислите значение левой части выражения Eq.4 для получения нижней границы «Max. Age».

Шаг 2: Выберите значение параметра «Forwarding Delay» и вычислите значение правой части выражения Eq. 4 для получения верхней границы «Max. Age».

Шаг 3: Выберите значение параметра «Forwarding Delay», удовлетворяющего условиям Eq.3 и Eq.4.

Настройка режима Turbo Ring

Сущность Turbo Ring

Компания Moxa разработала протокол Turbo Ring для оптимизации сетевого резервирования, в данной технологии достигнута высокая скорость восстановления работоспособности сети. В протоколах Turbo Ring и Turbo Ring v2 один из NPort'ов 6000 назначается мастером кольца, затем автоматически блокируется трафик через один сегмент кольца, чтобы не было замкнутых петель.

В случае нарушения работы какого-либо сегмента кольца протокол автоматически перенастроит кольцо таким образом, чтобы устройства отключенного сегмента могли переустановить соединение с остальной частью кольца.

Начальная настройка режимов кольца «Turbo Ring» или «Turbo Ring V2»



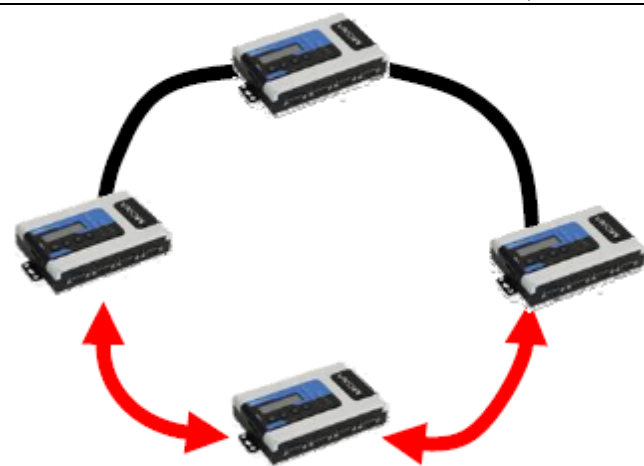
1. Выберите любые два порта для резервирования связей.
2. Организуйте кольцо Turbo Ring на этих портах.

Пользователю необязательно самостоятельно назначать среди NPort'ов мастера кольца. Протоколы Turbo Ring и Turbo Ring V2 автоматически назначают мастера кольца в случае, если ни один не выбран пользователем. Функция мастера заключается в определении резервного сегмента кольца. Ниже объясняется, как выбирается резервная связь для колец Turbo Ring или Turbo Ring V2.

Определение резервного сегмента кольца «Turbo Ring»

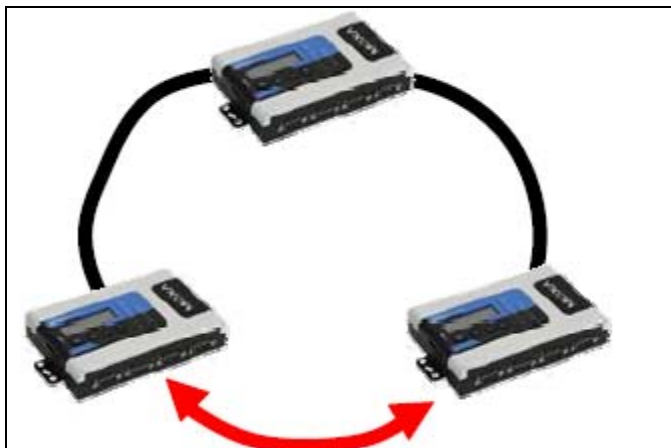
Резервный сегмент (т.е. сегмент, который блокируется в штатном режиме работы кольца) определяется в зависимости от числа устройств, входящих в кольцо, и положения мастера.

Четное число NPort'ов 6000 в кольце



Если в кольце Turbo Ring 2N (четное число) NPort'ов 6000, то резервным будет один из двух сегментов, подключенных к (N+1)-му NPort'у 6000 (т.е. в этом случае он будет прямо напротив мастера).

Нечетное число NPort'ов 6000 в кольце



Если в кольце 2N+1 NPort'ов 6000 (нечетное число) и нумерация сегментов и NPort'ов против часовой стрелки, то сегмент (N+1)-ый работает как резервный.
Например, в примере слева N=1 и таким образом, N+1=2.

Turbo Ring Settings

Redundancy Protocol

Turbo Ring

Master

Enable Disable

1st Redundant Port

1

2nd Redundant Port

2

Submit

Master

Диапазон значений	Описание	Значение по умолчанию
Enable/Disable (Включить/Выключить)	Назначать/Не назначать данный NPort 6000 мастером кольца	Disable

Redundant Ports

Диапазон значений	Описание	Значение по умолчанию
1st Redundant Ports	Нужно выбрать любой свободный Ethernet-порт NPort'a 6000 для организации кольца	Port 1
2nd Redundant Ports	Нужно выбрать любой свободный Ethernet-порт NPort'a 6000 для организации кольца	Port 2

Настройка Turbo Ring 2

Turbo Ring Settings

Redundancy Protocol

Turbo Ring V2

Master

Enable Disable

1st Redundant Port

1

2nd Redundant Port

2

Submit

Master

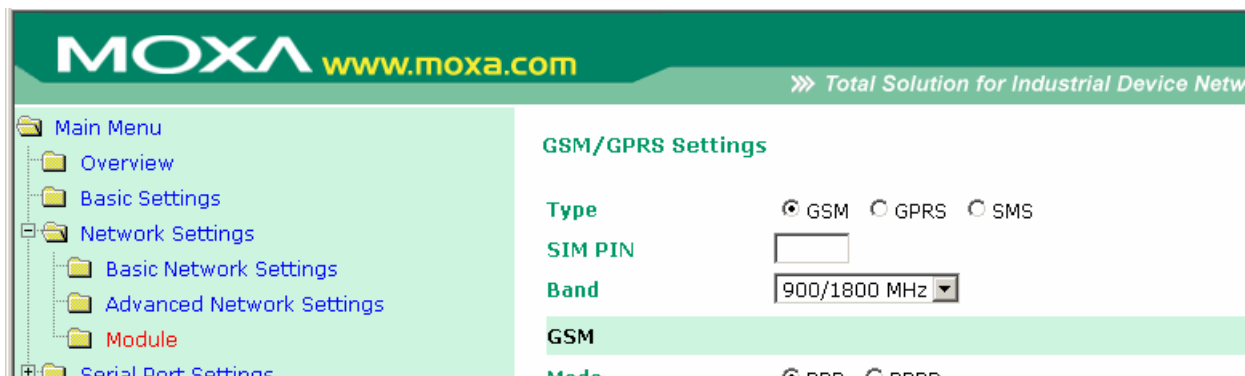
Диапазон значений	Описание	Значение по умолчанию
Enable/Disable (Включить/Выключить)	Назначать/Не назначать данный NPort 6000 мастером кольца	Disable

Redundant Ports

Диапазон значений	Описание	Значение по умолчанию
1st Redundant Ports	Нужно выбрать любой свободный Ethernet-порт NPort'a 6000 для организации кольца	Port 1
2nd Redundant Ports	Нужно выбрать любой свободный Ethernet-порт NPort'a 6000 для организации кольца	Port 2

Модуль NM-GPRS/GSM

Данный параграф относится к NPort'ам 6000 с установленными дополнительными модулями NM-GPRS/GSM. Для настройки GSM/GPRS откройте меню **Network Settings -> Module**. Подробное описание всех настроек этого меню приведено под рисунком.



Type: Модули NM-GPRS/GSM могут работать в одном из трех режимов: GSM, GPRS и SMS.

SIM PIN: Сюда вводится PIN-код SIM-карты (она заблокирована, пока не будет введен корректный код). Это помогает защитить от несанкционированного доступа к настройкам. Код по умолчанию устанавливается оператором связи. Для изменения PIN-кода необходимо использовать сотовый телефон.

Selecting the Radio Band: Несмотря на повсеместное использование частотных диапазонов GSM-900 и GSM-1800, операторы в США, Канаде и некоторых других странах Америки используют диапазоны GSM-850 и GSM-1900. Модуль NM-GPRS/GSM поддерживает настройку 4-ех диапазонов, что позволяет использовать данный промышленный модем сотовой связи в разных странах мира. По умолчанию модули NM-GPRS/GSM настроены на работу в диапазонах частот 900/1800 МГц.

Дополнительные настройки для каждого из трех режимов работы описаны в параграфах ниже.

MOXA www.moxa.com » Total Solution for Industrial Device Networking

Network Settings

- Basic Network Settings
- Advanced Network Set
- Module

GSM/GPRS Settings

Type: GSM GPRS SMS

SIM PIN:

Band: 900/1800 MHz

GSM

Mode: PPP PPPD

Destination IP address:

Source IP address:

IP netmask:

TCP/IP Compression: Enable Disable

Inactivity time: (0 - 65535 ms)

Link quality report: Enable Disable

Username:

Password:

Authentication type: None

Try next type on authentication denied: Enable Disable

Dial-out number:

Initial string:

Connection control: Always On/None

Connection interval: 5 (5 - 65535 min)

Ping remote host:

PPP Mode: поддержка работы по протоколу PPP dial-out.

PPPD Mode: PPPD (PPP Daemon) используется для служб dial-in, поскольку он поддерживает службы PPP только при получении запроса с удаленного ПК.

Destination IP address: Если данные параметры не заданы, их значения будут получены

Source IP address: автоматически по удаленному соединению

IP netmask:

TCP/IP compression (по умолчанию=Disable): Необходимость включения данной функции определяется тем, использует ли удаленное пользовательское приложение сжатие запросов.

Inactivity time (по умолчанию=0 мс): в данном поле устанавливается время отсутствия активности соединения, после которого соединение автоматически разрывается.

Link quality report (по умолчанию=Disable): Активация (Enable) данной функции позволяет NPort'у 6000 разрывать соединение, если уровень помех в канале связи превышает определенный порог.

Username: Это логин пользователя соединения dial-out.

Password: Пароль пользователя dial-out.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Dial-out number: Данное поле используется для задания номера для дозвона.

Dial-in number: Это поле используется для задания номера только для входящего дозвона.

Initial string: В данном поле задается начальное сообщение, используемое модемом для установления соединения.

Тип управления соединением	Условие установления соединения	Условие разрыва соединения	GSM
Always on/None	Всегда активно после включения питания	Нет	Основной канал связи
Periodically connect/inactivity time	Периодическое соединение (через установленные временные интервалы) с сетью GSM после включения питания	Соединение неактивно в течение времени [inactivity time]	Основной канал связи
Remote host fail/remote host recovered	Удаленный Ethernet-хост недоступен. NPort 6000 пингует его по сети Ethernet каждые 3 секунды после включения питания. После 5 неуспешных попыток установить соединение данные с последовательного порта будут отправляться по GSM-сети.	Когда связь с удаленным хостом по Ethernet восстанавливается, данные начинают передаваться по сети Ethernet после 5 последовательных успешных пингований.	Резервный канал связи

Connection interval (по умолчанию = 5 минут): Временной интервал периодического установления соединения.

Ping remote host: задайте IP-адрес или доменное имя удаленного хоста.

Режим GPRS

MOXA www.moxa.com » Total Solution for Industrial Device Networking

GSM/GPRS Settings

Type: GSM GPRS SMS

SIM PIN:

Band: 900/1800 MHz

GPRS

TCP/IP Compression: Enable Disable

Inactivity time: (0 - 65535 ms)

Link quality report: Enable Disable

Initial string:

Username:

Password:

APN:

Connection control: Always On/None

Connection interval: (5 - 65535 min)

Ping remote host:

TCP/IP compression (по умолчанию=Disable): Необходимость включения данной функции определяется тем, использует ли удаленное пользовательское приложение сжатие запросов.

Inactivity time (по умолчанию=0 мс): в данном поле устанавливается время отсутствия активности соединения, после которого соединение автоматически разрывается.

Link quality report (по умолчанию=Disable): Активация (Enable) данной функции позволяет NPort'u 6000 разрывать соединение, если уровень помех в канале связи превышает определенный порог.

Username: Это логин пользователя соединения dial-out.

Password: Пароль пользователя dial-out.

APN: Перед использованием GPRS необходимо добавить команду инициализации с именем точки доступа APN (Access Point Name). Подробные инструкции даны ниже.

Initial string: Данное поле необходимо для настройки начальной команды установки соединения.

Тип управления соединением	Условие установления соединения	Условие разрыва соединения	GPRS
Always on/None	Всегда активно после включения питания	Нет	Основной канал связи
Periodically connect/ inactivity time	Периодическое соединение (через установленные временные интервалы) с сетью GPRS после включения питания	Соединение неактивно в течение времени [inactivity time]	Основной канал связи
Remote host fail/ remote host recovered	Удаленный Ethernet-хост недоступен. NPort 6000 пингует его по сети Ethernet каждые 3 секунды после	Когда связь с удаленным хостом по Ethernet восстанавливается,	Резервный канал связи

	включения питания. После 5 неуспешных попыток установить соединение данные с последовательного порта будут отправляться по GPRS-сети.	данные начинают передаваться по сети Ethernet после 5 последовательных успешных пингований.	
--	---	---	--

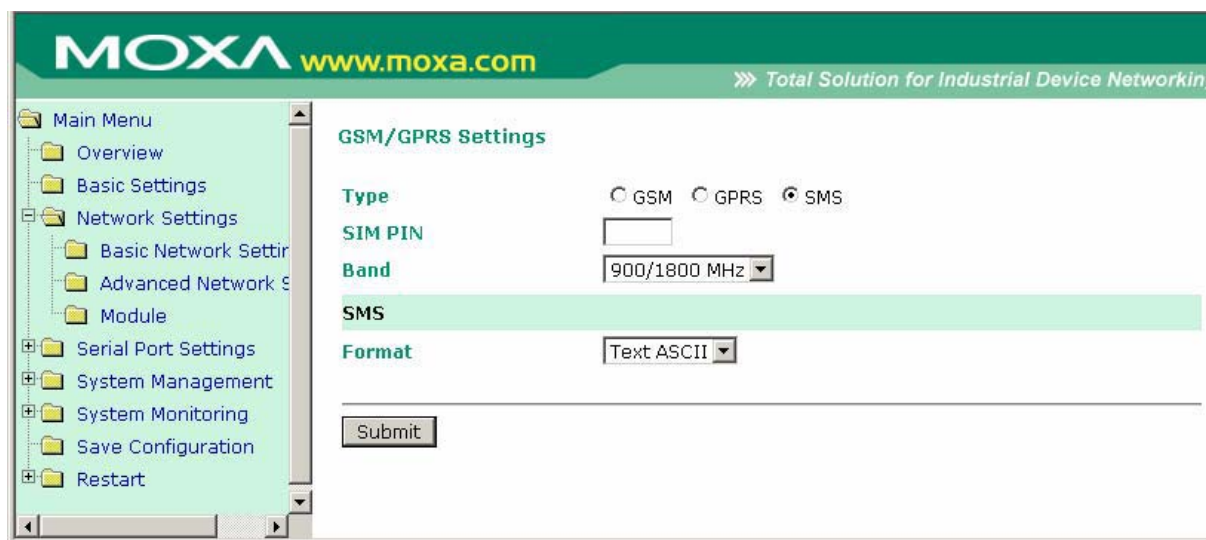
Connection interval (по умолчанию = 5 минут): Временной интервал периодического установления соединения.

Ping remote host: задайте IP-адрес или доменное имя удаленного хоста.

Режим SMS

Служба коротких сообщений (SMS) – протокол связи, позволяющий отправлять короткие (до 160 символов) текстовые сообщения. Данная функция имеется на большинстве мобильных телефонов и некоторых персональных электронных записных книжках со встроенными беспроводными интерфейсами.

Технология GSM дает преимущество в использовании службы SMS как простого способа для связи с другими мобильными сетями. В данной главе объясняется как использовать SMS в модуле NM-GPRS/GSM.



Supports 7-bit ASCII format for alert (поддержка 7-разрядной кодировки ASCII для сообщений предупреждений): NM-GPRS/GSM автоматически отправит на заданный телефонный номер оповещение о системных и сетевых событиях, изменениях в настройках, событиях по последовательным портам, если событие перечислено в настройках оповещения.

ASCII (American Standard Code for Information Interchange): Основу таблицы кодировки символов составляет английский алфавит. ASCII-код представляет текстовую информацию в компьютерах, коммуникационном оборудовании и других устройствах, поддерживающих работу с текстом. Самые современные устройства кодирования, преобразующие гораздо больше символов, так или иначе базируются на ASCII-кодировке.

Настройки автооповещения

При использовании режима SMS также понадобится выполнить настройки на вкладке Auto Warning Settings.

Event Settings (задание событий)

System Event			
Cold start	<input type="checkbox"/> Mail	<input type="checkbox"/> Trap	<input checked="" type="checkbox"/> SMS
Warm start	<input type="checkbox"/> Mail	<input type="checkbox"/> Trap	<input type="checkbox"/> SMS

Network Event			
Ethernet link down	<input type="checkbox"/> Dout	<input type="checkbox"/> SMS	

Config Event			
Console(web/text) login auth fail	<input type="checkbox"/> Mail	<input type="checkbox"/> Trap	<input type="checkbox"/> SMS
IP changed	<input type="checkbox"/> Mail		<input type="checkbox"/> SMS
Password changed	<input type="checkbox"/> Mail		<input type="checkbox"/> SMS

На странице Event Settings можно выполнить настройки оповещения диспетчеров/администраторов о системных, сетевых и событиях настроек. В зависимости от события доступны различные варианты настроек оповещения, как показано выше. **Mail** – оповещения по указанному электронному адресу. **Trap** – отправка SNMP-прерываний. **Dout** – данная функция доступна только в моделях NPort 6450 и 6650 – используется для изменения состояния релейных выходов (разъем дискретного вывода DOUT находится на задней стороне NPort'a 6000) и светодиодного индикатора аларма.

Cold start: Данное событие связано с запуском системы после отключения питания или после обновления прошивки.

Warm start: Данное событие связано с перезагрузкой NPort'a 6000 без отключения питания.

Network Event: Данные настройки доступны только в моделях NPort 6610, 6450 и 6650. Ethernet 1 относится к встроенному Ethernet-порту. Эти настройки позволяют изменять состояние дискретных выходов и светодиодного индикатора NPort'a, если происходит обрыв определенного Ethernet-соединения.

Console (web/text) login auth fail: Данное поле связано с неуспешной попыткой авторизации для входа в защищенную паролем консоль NPort'a 6000.

IP changed: При выборе данной функции NPort 6000 предпримет попытку отправить оповещение по e-mail до перезагрузки после изменения IP-адреса. Однако NPort 6000 перезагрузится с новым значением IP-адреса независимо от того, доставилось или нет сообщение по электронной почте.

Password changed: При выборе данной функции NPort 6000 предпримет попытку отправки оповещения по почте до перезагрузки с новым паролем входа в консоль. Если NPort 6000 не сможет отправить сообщение по e-mail в течение 15 секунд, он перезагрузится без оповещения.

Serial Event Settings (События на последовательных портах связи)

The screenshot shows the MOXA web interface for Serial Event Settings. The left sidebar contains a navigation menu with options like Overview, Basic Settings, Network Settings, Serial Port Settings, System Management, Misc. Network Settings, Auto Warning Settings, Event Settings, Serial Event Settings (highlighted), E-mail Alert, SNMP Trap, SMS Alert, Maintenance, Certificate, System Monitoring, Save Configuration, and Restart. The main content area is titled 'Port Event Settings' and contains a table with 16 rows (Port 1 to Port 16) and an 'All ports' row. Each row has columns for 'Serial Port Event', 'DCD changed', and 'DSR changed'. Under 'DCD changed' and 'DSR changed', there are sub-columns for 'Mail', 'Trap', 'Dout', and 'SMS', each with a checkbox.

Serial Port Event	DCD changed				DSR changed			
	Mail	Trap	Dout	SMS	Mail	Trap	Dout	SMS
Port 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All ports	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

На данной странице настроек можно задать оповещения администраторов об изменениях сигналов DCD и DSR каждого последовательного порта. Mail – отправка оповещения на заданные электронный ящик. Trap – отправка SNMP-прерывания. Dout – только в моделях NPort 6450 и 6650 - изменение состояния дискретного выхода и светодиодного индикатора аларма (разъем Dout находится на задней стороне NPort'a 6000).

DCD changed

Изменения сигнала определения несущей (DCD) показывает, что изменилось состояние соединения с модемом. Например, если уровень сигнала изменился на низкий, это свидетельствует о разрыве соединения. Когда сигнал DCD изменяется на низкий, NPort 6000 автоматически посылает сообщение оповещения администратору, если эта функция настроена на странице Serial Event Settings.

Для NPort'ов 6450 и 6650 после изменения состояния релейных выходов администраторы могут сбросить их, выбрав **Acknowledge Event** (квитирование/подтверждение события) из консоли NPort'a 6000 или восстановив сигнал DCD. См. также параграф System Monitoring (Мониторинг системы) в данной главе.

DSR changed

Изменение сигнала готовности DSR сигнализирует об отключении питания коммуникационного оборудования. Например, если уровень сигнала DSR изменяется на низкий, это показывает, что коммуникационное оборудование обесточено. При этом NPort автоматически посылает оповещение администратору, если данная функция настроена на странице Serial Event Settings.

В NPort'ax 6450 и 6650 после изменения состояния релейных выходов администраторы могут сбросить их, выбрав **Acknowledge Event** (подтверждение/квитирование события) через

консоль NPort'a 6000 или изменив уровень сигнала DSR. См. также параграф System Monitoring (Мониторинг Системы) в данной главе.



ВНИМАНИЕ

По SNMP выдается состояние DCD или DSR-сигналов, но не указывается какого именно. Изменение любого из них с «-» на «+» отображается как «link up» (восстановление соединения), а изменение с «+» на «-» - как «link down».

SMS Alert (Оповещение по SMS)

MOXA www.moxa.com » Total Solution for Industrial Device Networking

Main Menu

- Overview
- Basic Settings
- Network Settings
- Serial Port Settings
- System Management
 - Misc. Network Settings
 - Auto Warning Settings
 - Event Settings
 - Serial Event Settings
 - E-mail Alert
 - SNMP Trap
 - SMS Alert
 - Maintenance
 - Certificate
- System Monitoring
- Save Configuration
- Restart

SMS Alert

SMS Alert

To phone number 1

To phone number 2

To phone number 3

To phone number 4

Submit

To phone number 1/2/3/4: В данные поля вводятся номера телефонов, на которые будут отправляться SMS-сообщения с оповещениями.

Модуль NM-Modem

Данный параграф относится к устройствам NPort 6000, в которых установлен дополнительный модуль NM-Modem. Для открытия настроек модема в левой панели навигации щелкните Network Settings → Module. Различные параметры настроек подробно описаны на рисунке ниже.

The screenshot shows the Moxa V.92 Modem Settings web interface. The interface is divided into a left sidebar and a main content area. The sidebar contains a navigation tree with the following items: Main Menu, Overview, Basic Settings, Network Settings (expanded), Basic Network Settings, Advanced Network Settings, Module (selected), Serial Port Settings, System Management, System Monitoring, Save Configuration, Restart, and Logout System. The main content area is titled 'V.92 Modem Settings' and contains the following configuration fields:

- Mode:** Radio buttons for PPP (selected) and PPPD.
- Destination IP address:** Text input field.
- Source IP address:** Text input field.
- IP netmask:** Text input field.
- TCP/IP Compression:** Radio buttons for Enable and Disable (Disable is selected).
- Inactivity time:** Text input field with a range of 0 to 65535 ms.
- Link quality report:** Radio buttons for Enable and Disable (Disable is selected).
- Username:** Text input field.
- Password:** Text input field.
- Authentication type:** Dropdown menu with 'None' selected.
- Try next type on authentication denied:** Radio buttons for Enable and Disable (Disable is selected).
- Phone number:** Text input field.
- Initial string:** Text input field.
- Connection control:** Dropdown menu with 'Always On/None' selected.
- Connection interval:** Text input field with a range of 5 to 65535 min.
- Ping remote host:** Text input field with a 'Ping Test' button.

A 'Submit' button is located at the bottom left of the main content area.

PPP Mode: поддержка работы по протоколу PPP dial-in/dial-out.

PPPD Mode: PPPD (PPP по запросу) используется для служб dial-in, поскольку он поддерживает службы PPP только при получении запроса с удаленного ПК.

Destination IP address: IP-адрес удаленного сервера dial-in/dial-out.

Source IP address: IP-адрес источника – последовательного порта.

IP netmask: Маска подсети – для PPP-соединения.

TCP/IP compression (по умолчанию=No): Необходимость включения данной функции определяется тем, использует ли удаленное пользовательское приложение сжатие запросов.

Inactivity time (по умолчанию=0 мс): в данном поле устанавливается время отсутствия активности соединения, после которого соединение автоматически разрывается.

Link quality report (по умолчанию=No): Активация (Enable) данной функции позволяет NPort'u 6000 разрывать соединение, если уровень помех в канале связи превышает определенный порог.

Username: Это логин пользователя соединения dial-out.

Password: Пароль пользователя dial-out.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Phone number: Данное поле используется для задания номера для дозвона.

Initial string: В данном поле задается начальное сообщение, используемое модемом для установления соединения.

Тип управления соединением	Условие установления соединения	Условие разрыва соединения	Modem
Always on/None	Всегда активно после включения питания	Нет	Основной канал связи
Periodically connect/ inactivity time	Периодическое соединение (через установленные временные интервалы) с модемом после включения питания	Соединение неактивно в течение времени [inactivity time]	Основной канал связи
Remote host fail/ remote host recovered	Удаленный Ethernet-хост недоступен. NPort 6000 пингует его по сети Ethernet каждые 3 секунды после включения питания. После 5 неуспешных попыток установить соединение данные с последовательного порта будут отправляться через модем.	Когда связь с удаленным хостом по Ethernet восстанавливается, данные начинают передаваться по сети Ethernet после 5 последовательных успешных пингований.	Резервный канал связи

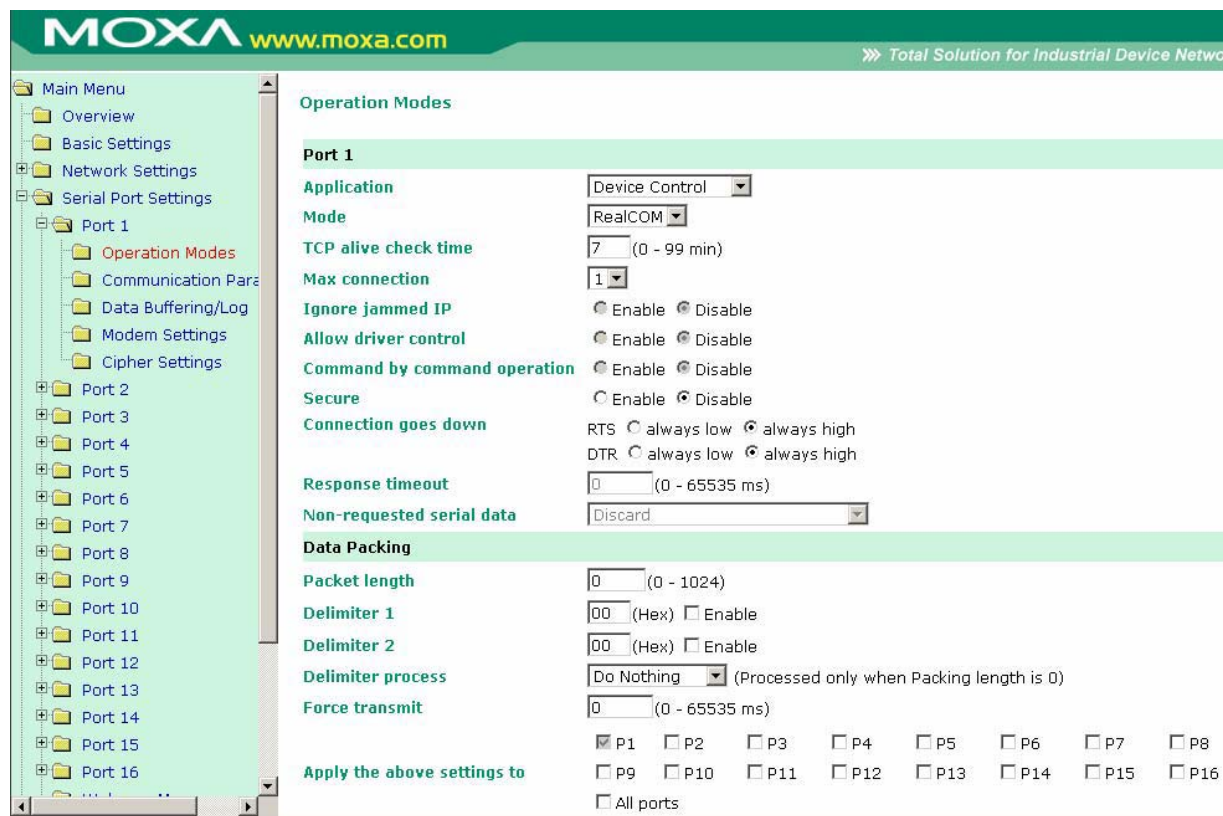
7 Настройка режимов работы последовательных портов

В данной главе объясняется настройка последовательных портов. Глава содержит следующие разделы:

- **Port Basic Settings (Основные настройки порта)**
- **Device Control Applications (Режимы COM-порта)**
 - Режим Real COM «виртуальный COM-порт»
 - Режим Reverse Real COM
 - Режим RFC2217
- **Socket Applications (Режимы сокетов)**
 - TCP Server
 - TCP Client
 - UDP
- **Режим Pair Connection (Парного соединения)**
 - Pair Connection Master (мастер парного соединения)
 - Pair Connection Slave (ведомое устройство парного соединения)
- **Режим Ethernet Modem**
- **Terminal Applications (Терминал)**
 - ASCII-терминал (TERM_ASC)
 - BIN-терминал (TERM_BIN)
 - SSH
- **Reverse Terminal Applications (Инверсный терминал)**
 - Reverse Telnet
 - Reverse SSH
- **Printer Applications (приложения печати)**
 - RAW PRN
 - LPD PRN
- **Приложения Dial In/Out**
 - Режим PPP
 - Режим PPPD
 - Режим SLIP
 - Режим SLIPD
 - Режим Dynamic
- **Disabled (последовательный порт отключен)**

Port Basic Settings (Основные настройки порта)

Каждый последовательный порт NPort'a 6000 настраивается отдельно, независимо от других. Для настройки режима работы и настроек порта раскройте пункт **Serial Port Settings** в меню в навигационной панели, затем выберите порт, который требуется сконфигурировать. Все параметры настроек порта собраны в 4 группы на навигационной панели: Operation Modes, Communication Parameters, Data Buffering/Log и Modem Settings.



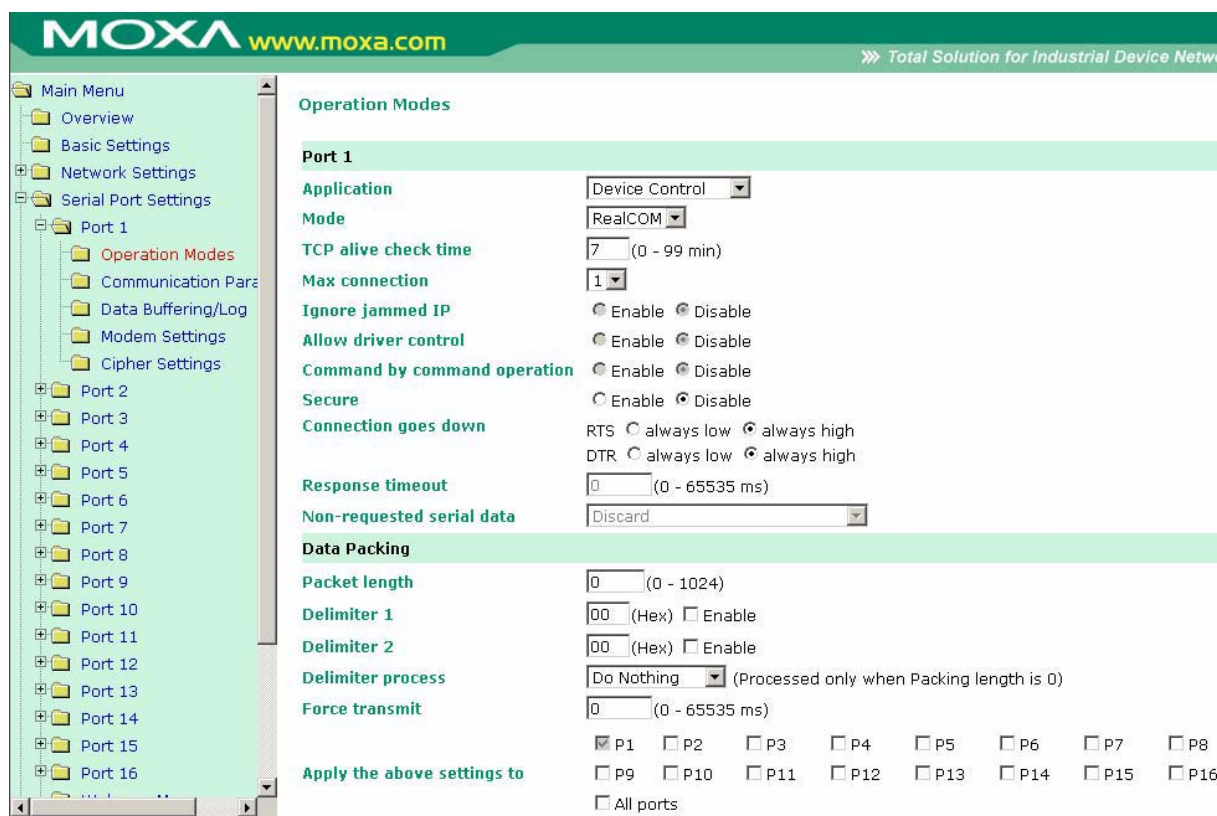
Выберите пункт **Operation Modes** в навигационной панели для задания и настройки режима работы каждого последовательного порта. В многопортовых моделях NPort'a 6000 предусмотрена возможность применить выполненные настройки сразу ко всем последовательным портам: внизу имеется соответствующий флаг [All ports].

Application: Выберите тип применения последовательного порта. Оно определяет доступные режимы.

Mode: После выбора типа применения укажите режим. При этом набор настраиваемых параметров будет изменяться в зависимости от выбранного режима.

Device Control Applications (Режимы COM-порта)

Режим Real COM – «виртуальный COM-порт»



TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Max. Connection (по умолчанию = 1): Данное поле используется, когда необходимо отправлять данные с нескольких хостов одновременно. Когда установлено значение 1, доступ к NPort'у 6000 может иметь только один хост, на котором драйвер Real COM будет полностью управлять последовательным портом. Когда установлено значение 2 и выше, то такое же число хостов могут обращаться к одному последовательному порту одновременно. При одновременном открытии COM-порта на нескольких хостах есть возможность только передачи данных без возможности управления. В качестве настроек последовательного порта используются параметры, определенные в прошивке, а не в прикладном программном обеспечении.

Прикладное программное обеспечение, использующее драйвер COM-порта, будет получать ответ «success», когда программа использует любую из API-функций Win 32. Встроенное ПО будет только отправлять данные обратно на драйвер хоста.

С Ethernet-порта на последовательный порт данные будут пересылаться по правилу FIFO (первым вошел - первым вышел).



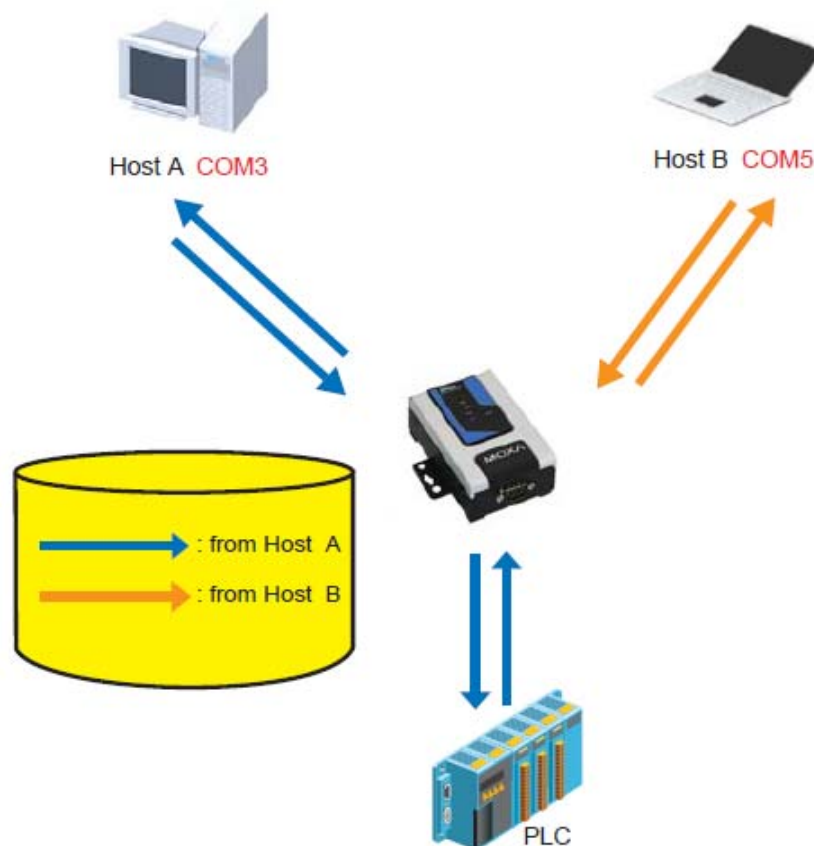
ВНИМАНИЕ

Когда параметр **Max.connection** больше 1, NPort 6000 будет использовать многоточечное соединение (например, от 2 до 8 хостов одновременно могут получать доступ к одному порту). При этом NPort 6000 будет использовать настройки последовательных портов, прописанные в его консоли, соответственно все хосты должны открывать порты с такими же установками. Если какой-либо хост будет использовать другие параметры настроек СОМ-порта, то данные будут передаваться неправильно.

Ignore jammed IP (по умолчанию = No): Данная функция определяет работу порта при подключении нескольких хостов, когда один и несколько из них перестанут отвечать на передачу данных портом. Если выбрано значение **No**, порт будет ожидать успешного завершения передачи данных на все хосты и только после этого будет отправлять следующие пакеты данных. Если выбрано значение **Yes**, то порт проигнорирует хосты, переставшие отвечать и продолжит передачу данных на оставшиеся.

Allow driver control (по умолчанию = No): Данная функция определяет поведение порта при получении управляющих команд одновременно с нескольких хостов, подключенных к порту. Если выбран вариант **No**, эти команды будут проигнорированы. Если выбран вариант **Yes**, управляющие команды будут приняты с приоритетом обработки команд, полученных последними (новейших).

Command by command operation (по умолчанию = Disable): Данный режим последовательных команд поддерживает один запрос и один ответ на каждый хост. Когда NPort 6000 получает команду от любого хоста по Ethernet, он сохраняет ее в буфере. Команды затем пересылаются на последовательный порт по очереди FIFO. См. схему ниже:



Как только ПЛК (PLC) ответил на запрос, NPort 6000 сохраняет его ответ в буфере в предположении, что ответ является корректным, и посылает его затем отправителю запроса.

NPort 6000 может ответить вместо PLC в случае, если в следующий раз будет послана такая же команда.

Secure (по умолчанию=No): Если выбран вариант Yes, данные отправляются по Ethernet с SSL-шифрованием.



ВНИМАНИЕ

Если в режиме Real COM используется SSL, убедитесь, что виртуальный COM-порт на компьютере настроен так же. Это выполняется через утилиту NPort Windows Driver Manager, устанавливаемую вместе с драйверами. См. главу 10.

Connection goes down (по умолчанию = always high): Можно задать характер изменения сигналов RTS и DTR при обрыве Ethernet-соединения. В некоторых задачах последовательные устройства требуют получения информации о состоянии Ethernet-соединения через сигналы RTS и DTR последовательного порта. Используйте значение параметра **goes low**, чтобы сигналы RTS и DTR меняли уровень на низкий при разрыве Ethernet-соединения. Если Вы хотите, чтобы состояние Ethernet-соединения никак не влияло на сигналы RTS и DTR, используйте значение **always high**.

Response time (по умолчанию = 0 мс): В данном поле задается время ожидания NPort'ом 6000 ответа по последовательному каналу перед посылкой следующей команды. NPort 6000 пошлет следующую команду, если ответ на последовательный порт не придет в течение заданного времени. Если установлено значение 0, время ожидания считается бесконечным и NPort 6000 будет ожидать запроса на передачу следующей команды.

Non-requested serial data (по умолчанию = discard): здесь определяются действия NPort'a 6000 с данными, полученными с последовательного устройства, которые NPort не запрашивал. NPort может либо игнорировать эту информацию, либо передавать их хосту по сети хосту, от которого пришел последний запрос, либо пересылать данные на все открытые подключенные хосты.

- **Discard:** сбрасывать такие данные
- **Forward to last requester:** пересылать данные с последовательного порта на хост, от которого пришел последний запрос.
- **Forward to all open connections:** пересылать данные с последовательного порта на все открытые соединения.

Packet length (по умолчанию = 0): настройка длины пакета – это максимальный объем данных, накапливаемых в буфере последовательного порта перед отправкой. По умолчанию установлено значение 0, данные будут отправляться либо в соответствии с настройкам delimiter, либо когда буфер заполнен. Если установлено значение от 1 до 1024 байт, данные из буфера будут пересылаться при достижении установленной длины данных.

Delimiter 1 и Delimiter 2 (по умолчанию = None): Если включена функция Delimiter 1, то при получении заданного символа (в шестнадцатеричной кодировке) данные с последовательного порта пересылаются на Ethernet-порт, буфер очищается. Функция и символ второго разделителя задаются в поле Delimiter 2 – в этом случае оба символа действуют как разделители для управления отправкой данных.



ВНИМАНИЕ

Для того, чтобы была доступна функция Delimiter, необходимо установить параметр packet length в 0. Delimiter 2 может быть включен только совместно с Delimiter 1, иначе возникнет ошибка. Даже при включенных делIMITРАХ NPort 6000 будет упаковывать и отправлять данные, если их объем превысил емкость памяти буфера 1 кБ.

Delimiter process (по умолчанию = Do Nothing): данное поле определяет действие, выполняемое при получении символов разделителей. Для того, чтобы это поле было активно, должен быть назначен по крайней мере Delimiter 1. Если назначены и Delimiter 1, и 2, то действие будет выполняться при получении обоих символов.

- Do Nothing: при получении символа разделителя данные пересылаются из буфера.
- Delimiter + 1: Данные будут пересылаться после получения первого байта, следующего за делиметром (разделителем).
- Delimiter + 2: Данные пересылаются после получения двух байт после разделителя.
- Strip Delimiter: Перед посылкой данных из них сперва удаляется символ-разделитель.

Force transmit (по умолчанию = 0 мс): Этот параметр определяет интервал времени, в течении которого NPort 6000 накапливает последовательные данные во внутреннем буфере. Если буфер оказывается полным или интервал времени Force transmit time превысил интервал времени Force transmit timeout, то NPort 6000 осуществляет посыл данных из буфера через TCP/IP. Если значение параметра 0, то функция отключена и отправка данных происходит при заполнении буфера.

Оптимальное значение Force transmit timeout зависит от используемого приложения, но оно должно быть не менее времени, заданного для передачи символа при данной скорости. Например, предположим, что последовательный порт установлен на 1200 bps, data bits 8, stop bits 1, no parity. В этом случае общее число битов, необходимых для передачи символа, равно 10, и время, затрачиваемое на передачу одного символа, рассчитывается так:

$$(10 \text{ (bps)} / 1200 \text{ (bits/s)}) * 1000 \text{ (ms/s)} = 8.3 \text{ ms (мс)}$$

Из этого следует, что значение Force transmit timeout должно превышать 8.3 мс. В нашем случае лучше всего, если это значение будет больше или равно 10 мс.

Если необходимо в каждом пакете посылать несколько символов, то необходимо чтобы последовательное устройство, подключенное к NPort, передавало их за промежуток времени меньший, чем указан в Force transmit timeout, а также, чтобы общий объем данных был меньше или равен объему буфера NPort'a. Размер буфера последовательных данных у NPort'a равен 1 Кбайт на каждый порт.

Режим Reverse Real COM

Operation Modes

Port 1

Application

Mode

TCP alive check time (0 - 99 min)

Ignore jammed IP Enable Disable

Allow driver control Enable Disable

Secure Enable Disable

Destination address 1 TCP port

Cmd port

Destination address 2 TCP port

Cmd port

Designated local TCP port 1

Designated local cmd port 1

Designated local TCP port 2

Designated local cmd port 2

Connection goes down RTS always low always high

DTR always low always high

Data Packing

Packet length (0 - 1024)

Delimiter 1 (Hex) Enable

Delimiter 2 (Hex) Enable

Delimiter process (Processed only when Packing length is 0)

Force transmit (0 - 65535 ms)

Apply the above settings to P1 P2 P3 P4

All ports

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Ignore jammed IP (по умолчанию = No): Данная функция определяет работу порта при подключении нескольких хостов, когда один и несколько из них перестанут отвечать на передачу данных портом. Если выбрано значение **No**, порт будет ожидать успешного завершения передачи данных на все хосты и только после этого будет отправлять следующие пакеты данных. Если выбрано значение **Yes**, то порт проигнорирует хосты, переставшие отвечать и продолжить передачу данных на оставшиеся.

Allow driver control (по умолчанию = No): Данная функция определяет поведение порта при получении управляющих команд одновременно с нескольких хостов, подключенных к порту. Если выбран вариант **No**, эти команды будут проигнорированы. Если выбран вариант **Yes**, управляющие команды будут приняты с приоритетом обработки команд, полученных последними (новейших).

Secure (по умолчанию=No): Если выбран вариант Yes, данные отправляются по Ethernet с SSL-шифрованием.



ВНИМАНИЕ

Если в режиме Real COM используется SSL, убедитесь, что виртуальный COM-порт на компьютере настроен так же. Это выполняется через утилиту NPort Windows Driver Manager, устанавливаемую вместе с драйверами. См. главу 10.

Destination address 1, 2 (по умолчанию = None): NPort 6000 будет подключаться к удаленному хосту с заданным IP-адресом. Должен быть указан по меньшей мере один адрес.

TCP port (по умолчанию = 60950): номер TCP-порта, назначенный на удаленном сервере/хосте. Это номер порта, используемый последовательным портом NPort'a 6000 для установления соединения с удаленным хостом/сервером. Во избежание совпадения с уже используемыми TCP-портами по умолчанию данный номер установлен равным 60950.



ВНИМАНИЕ

В данном режиме до двух хостов могут установить соединение с одним последовательным портом NPort'a 6000. Перед использованием данного TCP-порта убедитесь, что порт 60950 открыт в антивирусной программе (файрволе).



ВНИМАНИЕ

В качестве параметра Destination address может быть указан IP-адрес удаленного хоста, доменное имя или имя, определенное в таблице хостов NPort'a – host table.

Designated local port 1, 2 (по умолчанию = 7010, 7011): в данном поле назначаются локальные порты.

Connection goes down (по умолчанию = always high): Можно задать характер изменения сигналов RTS и DTR при обрыве Ethernet-соединения. В некоторых задачах последовательные устройства требуют получения информации о состоянии Ethernet-соединения через сигналы RTS и DTR последовательного порта. Используйте значение параметра **goes low**, чтобы сигналы RTS и DTR меняли уровень на низкий при разрыве Ethernet-соединения. Если Вы хотите, чтобы состояние Ethernet-соединения никак не влияло на сигналы RTS и DTR, используйте значение **always high**.

Response time (по умолчанию = 0 мс): В данном поле задается время ожидания NPort'ом 6000 ответа по последовательному каналу перед посылкой следующей команды. NPort 6000 pošлет следующую команду, если ответ на последовательный порт не придет в течение заданного времени. Если установлено значение 0, время ожидания считается бесконечным и NPort 6000 будет ожидать запроса на передачу следующей команды.

Non-requested serial data (по умолчанию = discard): здесь определяются действия NPort'a 6000 с данными, полученными с последовательного устройства, которые NPort не запрашивал. NPort может либо игнорировать эту информацию, либо передавать их хосту по

сети хосту, от которого пришел последний запрос, либо пересылать данные на все открытые подключенные хосты.

- **Discard:** сбрасывать такие данные
- **Forward to last requester:** пересылать данные с последовательного порта на хост, от которого пришел последний запрос.
- **Forward to all open connections:** пересылать данные с последовательного порта на все открытые соединения.

Packet length (по умолчанию = 0): настройка длины пакета – это максимальный объем данных, накапливаемых в буфере последовательного порта перед отправкой. По умолчанию установлено значение 0, данные будут отправляться либо в соответствии с настройкам delimiter, либо когда буфер заполнен. Если установлено значение от 1 до 1024 байт, данные из буфера будут пересылаться при достижении установленной длины данных.

Delimiter 1 и Delimiter 2 (по умолчанию = None): Если включена функция Delimiter 1, то при получении заданного символа (в шестнадцатеричной кодировке) данные с последовательного порта пересылаются на Ethernet-порт, буфер очищается. Функция и символ второго разделителя задаются в поле Delimiter 2 – в этом случае оба символа действуют как разделители для управления отправкой данных.



ВНИМАНИЕ

Для того, чтобы была доступна функция Delimiter, необходимо установить параметр packet length в 0. Delimiter 2 может быть включен только совместно с Delimiter 1, иначе возникнет ошибка. Даже при включенных делиметрах NPort 6000 будет упаковывать и отправлять данные, если их объем превысил емкость памяти буфера 1 кБ.

Delimiter process (по умолчанию = Do Nothing): данное поле определяет действие, выполняемое при получении символов разделителей. Для того, чтобы это поле было активно, должен быть назначен по крайней мере Delimiter 1. Если назначены и Delimiter 1, и 2, то действие будет выполняться при получении обоих символов.

- Do Nothing: при получении символа разделителя данные пересылаются из буфера.
- Delimiter + 1: Данные будут пересылаться после получения первого байта, следующего за делиметром (разделителем).
- Delimiter + 2: Данные пересылаются после получения двух байт после разделителя.
- Strip Delimiter: Перед посылкой данных из них сперва удаляется символ-разделитель.

Force transmit (по умолчанию = 0 мс): Этот параметр определяет интервал времени, в течении которого NPort 6000 накапливает последовательные данные во внутреннем буфере. Если буфер оказывается полным или интервал времени Force transmit time превысил интервал времени Force transmit timeout, то NPort 6000 осуществляет посыл данных из буфера через ТСР/IP. Если значение параметра 0, то функция отключена и отправка данных происходит при заполнении буфера.

Оптимальное значение Force transmit timeout зависит от используемого приложения, но оно должно быть не менее времени, заданного для передачи символа при данной скорости. Например, предположим, что последовательный порт установлен на 1200 bps, data bits 8, stop bits 1, no parity. В этом случае общее число битов, необходимых для передачи символа, равно 10, и время, затрачиваемое на передачу одного символа, рассчитывается так:

$$(10 \text{ (bps)} / 1200 \text{ (bits/s)}) * 1000 \text{ (ms/s)} = 8.3 \text{ ms (мс)}$$

Из этого следует, что значение Force transmit timeout должно превышать 8.3 мс. В нашем случае лучше всего, если это значение будет больше или равно 10 мс.

Если необходимо в каждом пакете посылать несколько символов, то необходимо чтобы последовательное устройство, подключенное к NPort, передавало их за промежуток времени меньший, чем указан в Force transmit timeout, а также, чтобы общий объем данных был меньше или равен объему буфера NPort'a. Размер буфера последовательных данных у NPort'a равен 1 Кбайт на каждый порт.

Выполненные настройки можно применить одновременно к двум и более портам в многопортовых моделях NPort 6000, отметив соответствующие флаги внизу окна.

Socket Applications (Режимы сокетов)

TCP Server

The screenshot shows the MOXA configuration web interface. The left sidebar contains a tree view with 'Main Menu' and 'Serial Port Settings' expanded to 'Port 1'. The main area is titled 'Operation Modes' and shows settings for 'Port 1'. The 'Application' is set to 'Socket' and 'Mode' to 'TCP Server'. 'TCP alive check time' is 7 (0-99 min), 'Inactivity time' is 0 (0-65535 ms), and 'Max connection' is 1. There are radio buttons for 'Ignore jammed IP', 'Allow driver control', 'Command by command operation', and 'Secure', all currently set to 'Disable'. 'TCP port' is 4001 and 'Cmd port' is 966. 'Connection goes down' has radio buttons for 'RTS' and 'DTR', both set to 'always high'. 'Response timeout' is 0 (0-65535 ms) and 'Non-requested serial data' is 'Discard'. The 'Data Packing' section includes 'Packet length' (0-1024), 'Delimiter 1' and 'Delimiter 2' (both 00 Hex, with 'Enable' checkboxes), 'Delimiter process' (Do Nothing), and 'Force transmit' (0-65535 ms).

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Inactivity time (по умолчанию = 0 мс): Время бездействия. В данном поле задается время, в течение которого NPort ожидает входящих или исходящих данных на последовательном порте перед тем как разорвать TCP-соединение. TCP-соединение закрывается, если в течение времени, равного **Inactivity time** через последовательный порт не идут данные ни в каком направлении. Если значение равно 0, то TCP-соединение остается активным, пока не будет получена команда закрытия.



ВНИМАНИЕ

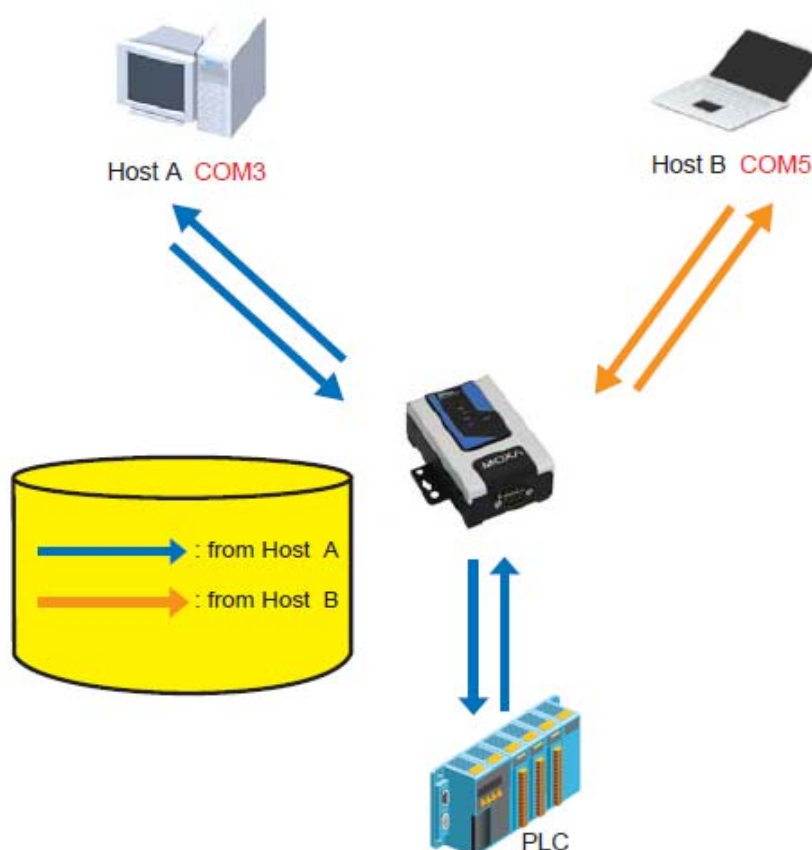
При использовании данного параметра **Inactivity time** необходимо задавать его значение большим, чем **Force transmit time**. Для предотвращения случайной потери данных из-за разрыва соединения рекомендуется, чтобы значение параметра **Inactivity time** было достаточным для завершения передачи данных.

Max. Connection (по умолчанию = 1): Данное поле используется, когда необходимо отправлять данные с нескольких хостов одновременно. Когда установлено значение 1, доступ к NPort'у 6000 может иметь только один хост, на котором драйвер Real COM будет полностью управлять последовательным портом. Когда установлено значение 2 и выше, то такое же число хостов могут обращаться к одному последовательному порту одновременно. С Ethernet-порта на последовательный порт данные будут пересылаться по правилу FIFO (первым вошел - первым вышел).

Ignore jammed IP (по умолчанию = No): Данная функция определяет работу порта при подключении нескольких хостов, когда один и несколько из них перестанут отвечать на передачу данных портом. Если выбрано значение **No**, порт будет ожидать успешного завершения передачи данных на все хосты и только после этого будет отправлять следующие пакеты данных. Если выбрано значение **Yes**, то порт проигнорирует хосты, переставшие отвечать и продолжит передачу данных на оставшиеся.

Allow driver control (по умолчанию = No): Данная функция определяет поведение порта при получении управляющих команд одновременно с нескольких хостов, подключенных к порту. Если выбран вариант **No**, эти команды будут проигнорированы. Если выбран вариант **Yes**, управляющие команды будут приняты с приоритетом обработки команд, полученных последними (новейших).

Command by command operation (по умолчанию = Disable): Данный режим последовательных команд поддерживает один запрос и один ответ на каждый хост. Когда NPort 6000 получает команду от любого хоста по Ethernet, он сохраняет ее в буфере. Команды затем пересылаются на последовательный порт по очереди FIFO. См. схему ниже:



Как только ПЛК (PLC) ответил на запрос, NPort 6000 сохраняет его ответ в буфере в предположении, что ответ является корректным, и посылает его затем отправителю запроса. NPort 6000 может ответить вместо PLC в случае, если в следующий раз будет послана такая же команда.

Secure (по умолчанию=No): Если выбран вариант Yes, данные отправляются по Ethernet с SSL-шифрованием.

TCP port (по умолчанию=4001): Это номер TCP-порта, назначенного последовательному порту NPort'a 6000. Он используется последовательным портом для прослушивания соединения и другие устройства должны использовать его для установления соединения с последовательным портом. Во избежание конфликта с уже используемыми портами его номер установлен по умолчанию 4001.

Command port (по умолчанию = 966): командный порт – это TCP-порт для получения SSDK-команд хоста. Во избежание конфликта с другими приложениями пользователь может назначить другой номер.

Connection goes down (по умолчанию = always high): Можно задать характер изменения сигналов RTS и DTR при обрыве Ethernet-соединения. В некоторых задачах последовательные устройства требуют получение информации о состоянии Ethernet-соединения через сигналы RTS и DTR последовательного порта. Используйте значение параметра **goes low**, чтобы сигналы RTS и DTR меняли уровень на низкий при разрыве Ethernet-соединения. Если Вы хотите, чтобы состояние Ethernet-соединения никак не влияло на сигналы RTS и DTR, используйте значение **always high**.

Response time (по умолчанию = 0 мс): В данном поле задается время ожидания NPort'ом 6000 ответа по последовательному каналу перед посылкой следующей команды. NPort 6000 пошлет следующую команду, если ответ на последовательный порт не придет в течение заданного времени. Если установлено значение 0, время ожидания считается бесконечным и NPort 6000 будет ожидать запроса на передачу следующей команды.

Non-requested serial data (по умолчанию = discard): здесь определяются действия NPort'a 6000 с данными, полученными с последовательного устройства, которые NPort не запрашивал. NPort может либо игнорировать эту информацию, либо передавать их хосту по сети хосту, от которого пришел последний запрос, либо пересылать данные на все открытые подключенные хосты.

- **Discard:** сбрасывать такие данные
- **Forward to last requester:** пересылать данные с последовательного порта на хост, от которого пришел последний запрос.
- **Forward to all open connections:** пересылать данные с последовательного порта на все открытые соединения.

Packet length (по умолчанию = 0): настройка длины пакета – это максимальный объем данных, накапливаемых в буфере последовательного порта перед отправкой. По умолчанию установлено значение 0, данные будут отправляться либо в соответствии с настройкам delimiter, либо когда буфер заполнен. Если установлено значение от 1 до 1024 байт, данные из буфера будут пересылаться при достижении установленной длины данных.

Delimiter 1 и Delimiter 2 (по умолчанию = None): Если включена функция Delimiter 1, то при получении заданного символа (в шестнадцатеричной кодировке) данные с последовательного порта пересылаются на Ethernet-порт, буфер очищается. Функция и символ второго разделителя задаются в поле Delimiter 2 – в этом случае оба символа действуют как разделители для управления отправкой данных.



ВНИМАНИЕ

Для того, чтобы была доступна функция Delimiter, необходимо установить параметр packet length в 0. Delimiter 2 может быть включен только совместно с Delimiter 1, иначе возникнет ошибка. Даже при включенных делIMITерах NPort 6000 будет упаковывать и отправлять данные, если их объем превысил емкость памяти буфера 1 кБ.

Delimiter process (по умолчанию = Do Nothing): данное поле определяет действие, выполняемое при получении символов разделителей. Для того, чтобы это поле было активно, должен быть назначен по крайней мере Delimiter 1. Если назначены и Delimiter 1, и 2, то действие будет выполняться при получении обоих символов.

- Do Nothing: при получении символа разделителя данные пересылаются из буфера.
- Delimiter + 1: Данные будут пересылаться после получения первого байта, следующего за делиметром (разделителем).
- Delimiter + 2: Данные пересылаются после получения двух байт после разделителя.
- Strip Delimiter: Перед посылкой данных из них сперва удаляется символ-разделитель.

Force transmit (по умолчанию = 0 мс): Этот параметр определяет интервал времени, в течении которого NPort 6000 накапливает последовательные данные во внутреннем буфере. Если буфер оказывается полным или интервал времени Force transmit time превысил интервал времени Force transmit timeout, то NPort 6000 осуществляет посыл данных из буфера через TCP/IP. Если значение параметра 0, то функция отключена и отправка данных происходит при заполнении буфера.

Оптимальное значение Force transmit timeout зависит от используемого приложения, но оно должно быть не менее времени, заданного для передачи символа при данной скорости. Например, предположим, что последовательный порт установлен на 1200 bps, data bits 8, stop bits 1, no parity. В этом случае общее число битов, необходимых для передачи символа, равно 10, и время, затрачиваемое на передачу одного символа, рассчитывается так:

$$(10 \text{ (bits)} / 1200 \text{ (bits/s)}) * 1000 \text{ (ms/s)} = 8.3 \text{ ms (мс)}$$

Из этого следует, что значение Force transmit timeout должно превышать 8.3 мс. В нашем случае лучше всего, если это значение будет больше или равно 10 мс.

Если необходимо в каждом пакете посылать несколько символов, то необходимо чтобы последовательное устройство, подключенное к NPort, передавало их за промежуток времени меньший, чем указан в Force transmit timeout, а также, чтобы общий объем данных был меньше или равен объему буфера NPort'a. Размер буфера последовательных данных у NPort'a равен 1 Кбайт на каждый порт.

The screenshot shows the MOXA configuration interface for a TCP Client. The left sidebar contains a tree view with categories like Main Menu, Overview, Basic Settings, Network Settings, and Serial Port Settings. Under Serial Port Settings, Port 1 is expanded to show Operation Modes, Communication Par, Data Buffering/Log, Modem Settings, and Cipher Settings. The main area displays the configuration for Port 1 under the 'Operation Modes' section. The 'Application' is set to 'Socket' and the 'Mode' is 'TCP Client'. The 'TCP alive check time' is set to 7 minutes, and the 'Inactivity time' is 0 ms. There are radio buttons for 'Ignore jammed IP' and 'Secure', both currently set to 'Disable'. Below these are four 'Destination address' fields, each with a 'Port' field set to 4001. There are also four 'Designated local port' fields set to 5010, 5011, 5012, and 5013. The 'Connection control' is set to 'Startup/None'. The 'Data Packing' section includes 'Packet length' (0), 'Delimiter 1' (00 Hex), and 'Delimiter 2' (00 Hex), each with an 'Enable' checkbox.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Inactivity time (по умолчанию = 0 мс): Время бездействия. В данном поле задается время, в течение которого NPort ожидает входящих или исходящих данных на последовательном порте перед тем как разорвать TCP-соединение. TCP-соединение закрывается, если в течение времени, равного **Inactivity time** через последовательный порт не идут данные ни в каком направлении. Если значение равно 0, то TCP-соединение остается активным, пока не будет получена команда закрытия.



ВНИМАНИЕ

При использовании данного параметра **Inactivity time** необходимо задавать его значение большим, чем **Force transmit time**. Для предотвращения случайной потери данных из-за разрыва соединения рекомендуется, чтобы значение параметра **Inactivity time** было достаточным для завершения передачи данных.



ВНИМАНИЕ

Параметр **Inactivity time** активен **только**, когда значение Connection Control установлено в **Any character/Inactivity time**.

Ignore jammed IP (по умолчанию = No): Данная функция определяет работу порта при подключении нескольких хостов, когда один и несколько из них перестанут отвечать на передачу данных портом. Если выбрано значение **No**, порт будет ожидать успешного завершения передачи данных на все хосты и только после этого будет отправлять следующие пакеты данных. Если выбрано значение **Yes**, то порт проигнорирует хосты, переставшие отвечать и продолжит передачу данных на оставшиеся.

Secure (по умолчанию=No): Если выбран вариант **Yes**, данные отправляются по Ethernet с SSL-шифрованием.

Destination address 1-4 (по умолчанию = None): здесь можно задать IP-адреса удаленных хостов, к которым будет подключаться NPort 6000. Должен быть задан по крайней мере один адрес.

TCP port (по умолчанию=4001): Это номер TCP-порта, назначенного последовательному порту NPort'a 6000. Он используется последовательным портом для прослушивания соединения и другие устройства должны использовать его для установления соединения с последовательным портом. Во избежание конфликта с уже используемыми портами его номер установлен по умолчанию 4001.



ВНИМАНИЕ

Может быть установлено соединение максимум с 4-мя хостами. Скорость соединения может быть низкой, если какой-либо из каналов имеет низкую пропускную способность, таким образом, один канал может ухудшить скорости обмена по другим.



ВНИМАНИЕ

В качестве Destination IP может использоваться IP-адрес, доменное имя или имя, определенное в таблице хостов (host table). В некоторых случаях пользователю может понадобиться активная передача данных на удаленный домен.

Designated local port 1-4 (по умолчанию = 5010-5013): Данные поля используются для назначения локальных портов.

Connection control (по умолчанию = Startup/None): Эта настройка определяет параметры, с которыми устанавливается или разрывается TCP-соединение. В таблице ниже приведены различные значения данного параметра. Приведены условия для установления и разрыва соединений.

Значение	Описание
Startup/None	TCP-соединение устанавливается при запуске и остается активным все время.
Any Character/None	TCP-соединение устанавливается при получении любого символа по последовательному порту и остается активным все время.
Any Character/ Inactivity Time	TCP-соединение устанавливается при получении какого-либо символа на последовательный порт и разрывается по истечении времени бездействия Inactivity time .
DSR On/DSR Off	TCP-соединение устанавливается, когда состояние сигнала DSR равно “On”, разрывается, когда состояние сигнала DSR – “Off”.
DSR On/None	
DCD On/DCD Off	TCP-соединение устанавливается, когда состояние сигнала DCD равно “On”, разрывается, когда состояние сигнала DCD – “Off”.
DCD On/None	TCP-соединение устанавливается, когда состояние сигнала DCD равно “On”, и остается активным всё время.

Packet length (по умолчанию = 0): настройка длины пакета – это максимальный объем данных, накапливаемых в буфере последовательного порта перед отправкой. По умолчанию установлено значение 0, данные будут отправляться либо в соответствии с настройкам delimiter, либо когда буфер заполнен. Если установлено значение от 1 до 1024 байт, данные из буфера будут пересылаться при достижении установленной длины данных.

Delimiter 1 и Delimiter 2 (по умолчанию = None): Если включена функция Delimiter 1, то при получении заданного символа (в шестнадцатеричной кодировке) данные с последовательного порта пересылаются на Ethernet-порт, буфер очищается. Функция и символ второго разделителя задаются в поле Delimiter 2 – в этом случае оба символа действуют как разделители для управления отправкой данных.



ВНИМАНИЕ

Для того, чтобы была доступна функция Delimiter, необходимо установить параметр packet length в 0. Delimiter 2 может быть включен только совместно с Delimiter 1, иначе возникнет ошибка. Даже при включенных делиметрах NPort 6000 будет упаковывать и отправлять данные, если их объем превысил емкость памяти буфера 1 кБ.

Delimiter process (по умолчанию = Do Nothing): данное поле определяет действие, выполняемое при получении символов разделителей. Для того, чтобы это поле было активно, должен быть назначен по крайней мере Delimiter 1. Если назначены и Delimiter 1, и 2, то действие будет выполняться при получении обоих символов.

- Do Nothing: при получении символа разделителя данные пересылаются из буфера.
- Delimiter + 1: Данные будут пересылаться после получения первого байта, следующего за делиметром (разделителем).
- Delimiter + 2: Данные пересылаются после получения двух байт после разделителя.
- Strip Delimiter: Перед посылкой данных из них сперва удаляется символ-разделитель.

Force transmit (по умолчанию = 0 мс): Этот параметр определяет интервал времени, в течении которого NPort 6000 накапливает последовательные данные во внутреннем буфере. Если буфер оказывается полным или интервал времени Force transmit time превысил интервал времени Force transmit timeout, то NPort 6000 осуществляет посыл данных из буфера через TCP/IP. Если значение параметра 0, то функция отключена и отправка данных происходит при заполнении буфера.

Оптимальное значение Force transmit timeout зависит от используемого приложения, но оно должно быть не менее времени, заданного для передачи символа при данной скорости. Например, предположим, что последовательный порт установлен на 1200 bps, data bits 8, stop

bits 1, no parity. В этом случае общее число битов, необходимых для передачи символа, равно 10, и время, затрачиваемое на передачу одного символа, рассчитывается так:

$$(10 \text{ (bps)} / 1200 \text{ (bits/s)}) * 1000 \text{ (ms/s)} = 8.3 \text{ ms (мс)}$$

Из этого следует, что значение Force transmit timeout должно превышать 8.3 мс. В нашем случае лучше всего, если это значение будет больше или равно 10 мс.

Если необходимо в каждом пакете посылать несколько символов, то необходимо чтобы последовательное устройство, подключенное к NPort, передавало их за промежуток времени меньший, чем указан в Force transmit timeout, а также, чтобы общий объем данных был меньше или равен объему буфера NPort'a. Размер буфера последовательных данных у NPort'a равен 1 Кбайт на каждый порт.

UDP

The screenshot shows the MOXA web interface for configuring a port. The left sidebar contains a navigation menu with 'Main Menu', 'Overview', 'Basic Settings', 'Network Settings', 'Serial Port Settings', and a list of ports from Port 1 to Port 15. The main content area is titled 'Operation Modes' and is currently set for 'Port 1'. The 'Application' is set to 'Socket' and the 'Mode' is 'UDP'. There are four 'Destination address' sections, each with 'Begin' and 'End' IP address input fields and a 'Port' field set to '4001'. The 'Local listen port' is set to '4001'. The 'Data Packing' section includes 'Packet length' (0), 'Delimiter 1' and 'Delimiter 2' (both '00' with 'Enable' checkboxes), 'Delimiter process' (Do Nothing), and 'Force transmit' (0). Below this is a grid of checkboxes for ports P1 through P32, with P1 checked. An 'Apply the above settings to' section has checkboxes for ports P17 through P32 and an 'All ports' option. A 'Submit' button is at the bottom.

Destination address 1-4 (по умолчанию не заданы): В режиме UDP, можно задать до 4 диапазонов IP-адресов, к которым будет подключаться последовательный порт. Нужно задать хотя бы один диапазон.



ВНИМАНИЕ

Максимальное число IP-адресов равно 64. Однако, при использовании многоадресной передачи данных можно ввести IP-адрес в формате xxx.xxx.xxx.255 в поле **Begin**. Например, если ввести 192.127.168.255, то NPort 6000 сможет отправлять широковещательные UDP-пакеты на все хосты с IP-адресами с 192.127.168.1 по 192.127.168.254.

Local listen port (по умолчанию = 4001): Это UDP-порт, который прослушивает NPort 6000, и который остальные устройства должны использовать для связи с NPort'ом 6000. Во

избежание совпадения его номера с портами, используемыми другими приложениями, он по умолчанию равен 4001.

Packet length (по умолчанию = 0): настройка длины пакета – это максимальный объем данных, накапливаемых в буфере последовательного порта перед отправкой. По умолчанию установлено значение 0, данные будут отправляться либо в соответствии с настройкам delimiter, либо когда буфер заполнен. Если установлено значение от 1 до 1024 байт, данные из буфера будут пересылаться при достижении установленной длины данных.

Delimiter 1 и Delimiter 2 (по умолчанию = None): Если включена функция Delimiter 1, то при получении заданного символа (в шестнадцатеричной кодировке) данные с последовательного порта пересылаются на Ethernet-порт, буфер очищается. Функция и символ второго разделителя задаются в поле Delimiter 2 – в этом случае оба символа действуют как разделители для управления отправкой данных.



ВНИМАНИЕ

Для того, чтобы была доступна функция Delimiter, необходимо установить параметр packet length в 0. Delimiter 2 может быть включен только совместно с Delimiter 1, иначе возникнет ошибка. Даже при включенных делIMITрах NPort 6000 будет упаковывать и отправлять данные, если их объем превысил емкость памяти буфера 1 кБ.

Delimiter process (по умолчанию = Do Nothing): данное поле определяет действие, выполняемое при получении символов разделителей. Для того, чтобы это поле было активно, должен быть назначен по крайней мере Delimiter 1. Если назначены и Delimiter 1, и 2, то действие будет выполняться при получении обоих символов.

- Do Nothing: при получении символа разделителя данные пересылаются из буфера.
- Delimiter + 1: Данные будут пересылаться после получения первого байта, следующего за делИметром (разделителем).
- Delimiter + 2: Данные пересылаются после получения двух байт после разделителя.
- Strip Delimiter: Перед посылкой данных из них сперва удаляется символ-разделитель.

Force transmit (по умолчанию = 0 мс): Этот параметр определяет интервал времени, в течении которого NPort 6000 накапливает последовательные данные во внутреннем буфере. Если буфер оказывается полным или интервал времени Force transmit time превысил интервал времени Force transmit timeout, то NPort 6000 осуществляет посыл данных из буфера через TCP/IP. Если значение параметра 0, то функция отключена и отправка данных происходит при заполнении буфера.

Оптимальное значение Force transmit timeout зависит от используемого приложения, но оно должно быть не менее времени, заданного для передачи символа при данной скорости. Например, предположим, что последовательный порт установлен на 1200 bps, data bits 8, stop bits 1, no parity. В этом случае общее число битов, необходимых для передачи символа, равно 10, и время, затрачиваемое на передачу одного символа, рассчитывается так:

$$(10 \text{ (bps)} / 1200 \text{ (bits/s)}) * 1000 \text{ (ms/s)} = 8.3 \text{ ms (мс)}$$

Из этого следует, что значение Force transmit timeout должно превышать 8.3 мс. В нашем случае лучше всего, если это значение будет больше или равно 10 мс.

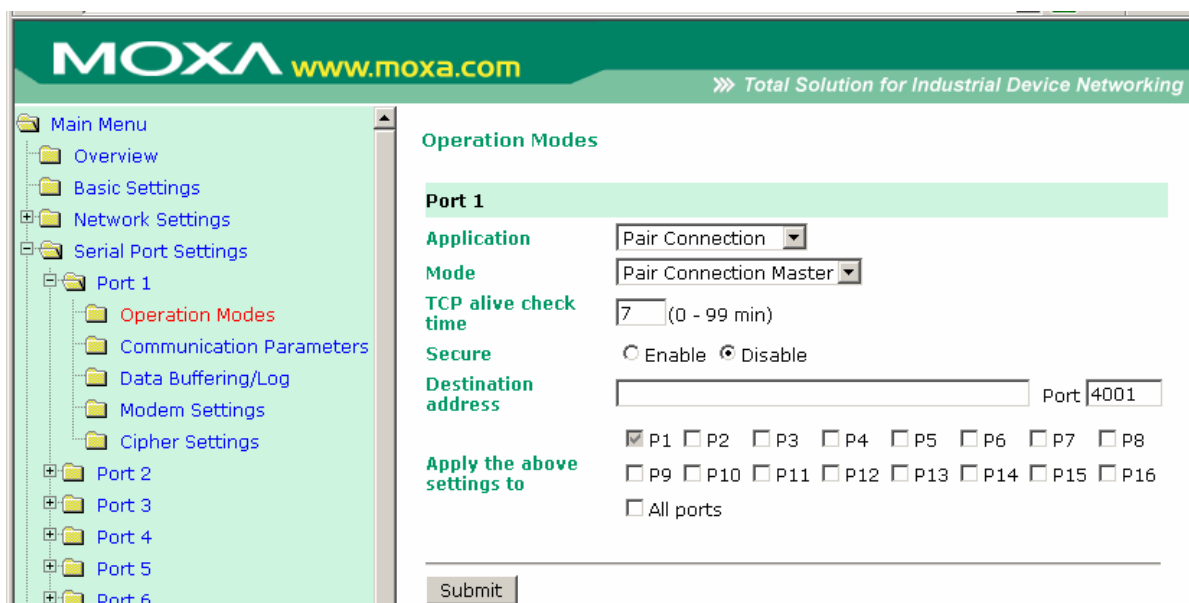
Если необходимо в каждом пакете посылать несколько символов, то необходимо чтобы последовательное устройство, подключенное к NPort, передавало их за промежуток времени меньший, чем указан в Force transmit timeout, а также, чтобы общий объем данных был меньше или равен объему буфера NPort'a. Размер буфера последовательных данных у NPort'a равен 1 Кбайт на каждый порт.

Режим Pair Connection (Парного соединения)

Режим парного соединения может использоваться для преодоления ограничения на длину 15м интерфейса RS-232. В этом режиме устанавливается соединение между последовательными портами двух NPort'ов 6000. Один из последовательных портов подключается к СОМ-порту компьютера. Другой последовательный порт подключается к последовательному порту устройства. Два NPort'a 6000 соединяются между собой перекрестным Ethernet-кабелем и находятся в одной локальной сети (LAN). В более сложных задачах два NPort'a 6000 соединяются по глобальной сети (WAN), т.е. сети, содержащей один и более маршрутизаторов. В режиме Pair Connection, и данные и сигналы управления модемом (кроме DCD-сигналов) могут прозрачно передаваться между двумя NPort'ами 6000.

Pair Connection Master (мастер парного соединения)

При использовании режима Pair Connection, один последовательный порт должен быть назначен мастером (Pair Connection Master), второй – ведомым – слейвом (Pair Connection Slave). Последовательный порт, назначенный мастером, будет играть роль TCP-клиента, а порт, назначенный ведомым – TCP-сервером. На практике не имеет значения, какой порт будет назначен мастером, а какой - слэйвом.



The screenshot shows the MOXA web interface for configuring a serial port. The left sidebar contains a navigation menu with categories like Main Menu, Overview, Basic Settings, Network Settings, and Serial Port Settings. Under Serial Port Settings, Port 1 is selected, and the 'Operation Modes' sub-menu is active. The main content area displays the configuration for Port 1. The 'Application' is set to 'Pair Connection' and the 'Mode' is 'Pair Connection Master'. The 'TCP alive check time' is set to 7 minutes. The 'Secure' option is disabled. The 'Destination address' is set to Port 4001. There are checkboxes for ports P1 through P16, with P1 checked. An 'Apply the above settings to' section includes checkboxes for individual ports and an 'All ports' option. A 'Submit' button is at the bottom.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Secure (по умолчанию=No): Если выбран вариант Yes, данные отправляются по Ethernet с SSL-шифрованием.

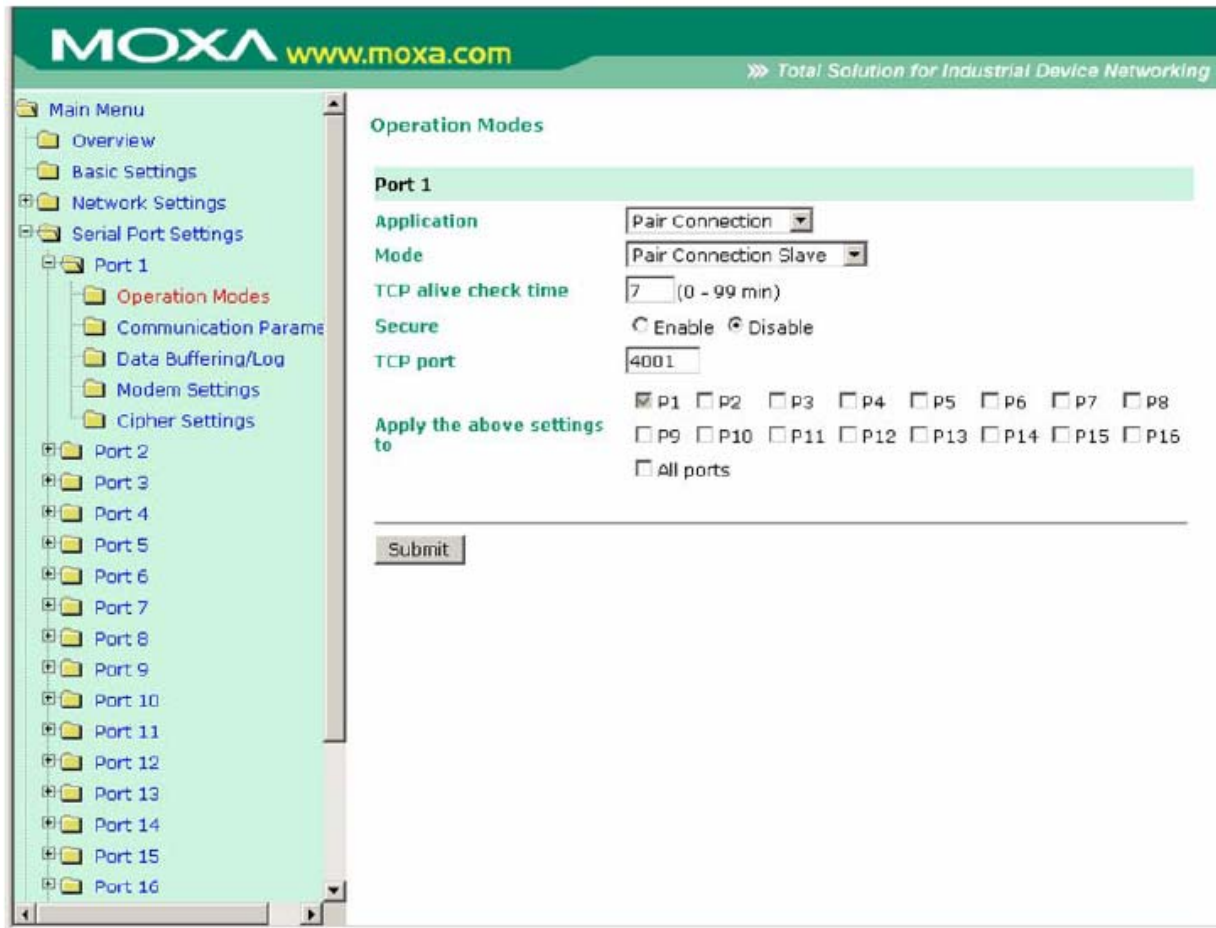


ВНИМАНИЕ

При установлении парного соединения между двумя последовательными портами двух различных NPort'ов 6000 имейте в виду, что если на одном из них установлено шифрование данных, то и на другом данная функция должна быть также включена (т.е. на обоих одновременно параметр Secure равен Yes или No).

Destination IP address: Мастер парного соединения будет соединяться с сетевым устройством, имеющим данный IP-адрес. Номер порта по умолчанию: 4001. Убедитесь, что данный номер совпадает с портом слейва.

Pair Connection Slave (ведомое устройство парного соединения)



The screenshot shows the MOXA web interface for configuring a serial port. The left sidebar contains a navigation tree with 'Serial Port Settings' expanded to 'Port 1', which is further expanded to 'Operation Modes'. The main content area is titled 'Operation Modes' and shows the configuration for 'Port 1'. The 'Application' is set to 'Pair Connection' and the 'Mode' is 'Pair Connection Slave'. The 'TCP alive check time' is set to 7 minutes. The 'Secure' option is set to 'Disable'. The 'TCP port' is set to 4001. There are checkboxes for applying settings to ports P1 through P16, with P1 checked. A 'Submit' button is at the bottom.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Secure (по умолчанию=No): Если выбран вариант Yes, данные отправляются по Ethernet с SSL-шифрованием.

TCP port (по умолчанию=4001): Это номер TCP-порта, назначенного последовательному порту NPort'a 6000. Он используется последовательным портом для прослушивания соединения и другие устройства должны использовать его для установления соединения с последовательным портом. Во избежание конфликта с уже используемыми портами его номер установлен по умолчанию 4001.

Режим Ethernet Modem

The screenshot shows the MOXA web interface for configuring a port. The left sidebar contains a tree view with 'Serial Port Settings' expanded to 'Port 1'. The main area is titled 'Operation Modes' and shows settings for 'Port 1'. The 'Application' is set to 'Ethernet Modem'. The 'TCP alive check time' is set to 7 (0-99 min). The 'TCP port' is set to 4001. There are checkboxes for ports P1 through P16, with P1 checked. A note states: 'Please note that in Ethernet Modem mode, DTR, RTS, and DCD signals are disabled for ports that are using RS-422 or RS-485.' A 'Submit' button is at the bottom.

NPort 6000 получает AT-команду формата <ATD IP address:TCP port> (например, для IPv4: ATD 192.127.168.1: 4001 / для IPv6: ADT [fe80::290:e8ff:fe0d:b0fb]: 65500) по последовательному порту и затем посылает запрос на установление TCP-соединения с удаленным Ethernet-модемом или ПК, в этом случае TCP-порт – это номер порта удаленного Ethernet-модема или ПК. После того, как соединение с удаленным хостом установлено, NPort 6000 посылает сигнал “CONNECT baud” по последовательному порту и затем переходит в режим передачи данных.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

TCP port (по умолчанию=4001): Это номер TCP-порта, назначенного последовательному порту NPort'a 6000. Он используется последовательным портом для прослушивания соединения и другие устройства должны использовать его для установления соединения с последовательным портом. Во избежание конфликта с уже используемыми портами его номер установлен по умолчанию 4001.

Dial-in (Входящий звонок)

NPort 6000 прослушивает TCP/IP-соединение, ожидая запроса от удаленного Ethernet-модема или хоста. Ответ NPort'a 6000 зависит от значения параметра AS0, как показано ниже.

ATS0 = 0:

NPort 6000 временно устанавливает TCP-соединение и затем отправляет сигнал “RING” по последовательному порту. Последовательный контроллер должен дать ответ “ATA” в течение 2,5 секунд для установления соединения, после этого NPort 6000 переходит в режим передачи данных. Если ответа “ATA” не последовало, то после отправки трех сигналов “RING” NPort 6000 разорвет соединение.

ATS0 ≥ 1:

NPort 6000 сразу устанавливает TCP-соединение и затем посылает команду “CONNECT *baud*” на последовательный порт, где *baud* – скорость соединения по последовательному порту NPort'a 6000. После этого NPort 6000 переходит в режим передачи данных.

Dial-out (Исходящий звонок)

Nport 6000 принимает AT-команду формата <ATD IP: TCP port> по последовательному порту и затем посылает запрос на TCP-соединение с удаленным Ethernet-модемом или ПК. В данном случае IP – это адрес удаленного модема или ПК, TCP port – номер порта удаленного модема или ПК. Как только установлено TCP-соединение с удаленным хостом, NPort 6000 отправит сигнал “CONNECT *baud*” на последовательный порт, где *baud* – скорость соединения по последовательному порту NPort'a 6000.

Запрос на разрыв соединения с локального устройства

Когда NPort 6000 работает в режиме передачи данных, пользователь может инициировать разрыв соединения, послав «+++» с локального последовательного порта NPort'a 6000. Некоторые приложения позволяют напрямую устанавливать DTR-сигнал в OFF – это также инициирует разрыв соединения. NPort 6000 переходит в режим передачи данных, по истечении 1 секунды можно ввести “ATH” для закрытия TCP-соединения. NPort 6000 пошлет сигнал “NO CARRIER” через последовательный порт.

ПРИМЕЧАНИЕ Последовательность “+++” должна быть непрерывной. Символ “+” назначается в регистре S2, и в регистре S12 можно изменить защитные временные интервалы, предшествующие и следующие за последовательностью “+++” – для обеспечения защиты собранной информации.

Разрыв соединения с удаленного устройства

После закрытия TCP-соединения удаленным модемом или ПК NPort 6000 отправляет сигнал “NO CARRIER” по последовательному порту и возвращается в командный режим.

AT-команды

Nport 6000 поддерживает приведенные ниже AT-команды, используемые в обычном модеме:

№.	AT-команда	Описание	Примечания
1	ATA	Ответ вручную	
2	ATD <IP>:<Port>	Дозвон до устройства с указанным IP-адресом: номер порта	
3	ATE	ATE0 = выключить эхо ATE1 = включить эхо (по умолчанию)	
4	ATH	ATH0 = с отключенной линией (по умолчанию) ATH1 – с подключенной линией	
5	ATI, ATI0, ATI1, ATI2	Версия модема	Только ответ “ОК”
6	ATL	Громкость динамика	Только ответ “ОК”
7	ATM	Управление динамиком	Только ответ “ОК”
8	ATO	Он-лайн команда	
9	ATP, ATG	Установить Импульсный/Тональный режим	Только ответ “ОК”
10	ATQ0, ATQ1	Команда неактивного состояния (по умолчанию ATQ0)	
11	ATSr = n	Изменить содержимое S-регистра	См. пункт «S-регистры»

12	ATSr?	Прочитать содержимое S-регистра	См. пункт «S-регистры»
13	ATV	Код типа результата: ATV0 – для дискретных данных, ATV1 – для текстовых (по умолчанию) 0 = ОК 1 = connect (соединение) 2 = ring (звонок) 3 = No carrier (отсутствует несущая) 4 = error (ошибка)	
14	ATZ	Сброс (разрыв соединения, переход в режим комад и восстановление настроек из флэш-памяти)	
15	AT&C	Управление DCD-сигналом последовательного порта AT&C0=DCD всегда в состоянии ON AT&C1=терминальное устройство определяет соединение по состоянию сигнала DCD (по умолчанию)	
16	AT&F	Восстановить заводские установки	
17	AT&G	Выбор защитного временного интервала	Только ответ “ОК”
18	AT&R	Команда RTS-сигнала последовательного порта	Только ответ “ОК”
19	AT&S	Управление DSR-сигналом последовательного порта	Только ответ “ОК”
20	AT&V	Просмотр настроек	
21	AT&W	Сохранить текущие настройки во флэш-память для последующей загрузки	

S-регистры

№.	S-регистр	Описание и значение по умолчанию	Примечания
1	S0	Количество звонков перед ответом (по умолчанию=0)	
2	S1	Счетчик поступающих вызовов (всегда = 0)	не настраивается
3	S2	Код символа ESCAPE (по умолчанию=43-ASCII «+»)	
4	S3	Символ возврата каретки (по умолчанию=13 ASCII)	
5	S4	Символ перевода строки (по умолчанию = 10 ASCII)	
6	S5	Символ BACKSPACE (по умолчанию = 8 ASCII)	
7	S6	Время ожидания гудка (всегда=2 с)	не настраивается
8	S7	Время одной попытки при наборе (по умолчанию = 3 с) – время ожидания несущей при наборе	
9	S8	Продолжительность паузы (всегда =2 с)	не настраивается
10	S9	Время определения несущей (всегда = 6, ед.изм. = 1/10 с)	не настраивается
11	S10	Время восстановления несущей (всегда = 14, ед.изм.=1/10 с)	не настраивается
12	S11	Длительность тонального набора на двух	не настраивается

		частотах (всегда=100 мс)	
13	S12	Пауза для передачи ESCAPE последовательности (по умолчанию =50, ед. изм. = 1/50 с) для управления временем для «+++»	

Terminal Applications (Терминал)

ASCII-терминал (TERM_ASC)

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Inactivity time (по умолчанию = 0 мс): Время бездействия. В данном поле задается время, в течение которого NPort ожидает входящих или исходящих данных на последовательном порте перед тем как разорвать TCP-соединение. TCP-соединение закрывается, если в течение времени, равного **Inactivity time** через последовательный порт не идут данные ни в каком направлении. Если значение равно 0, то TCP-соединение остается активным, пока не будет получена команда закрытия.



ВНИМАНИЕ

При использовании данного параметра **Inactivity time** необходимо задавать его значение большим, чем **Force transmit time**. Для предотвращения случайной потери данных из-за разрыва соединения рекомендуется, чтобы значение параметра **Inactivity time** было достаточным для завершения передачи данных.

Auto-Link Protocol: Если в этом поле установлено None, NPort 6000 не будет автоматически подключаться к хосту. Если этот параметр установлен в Telnet или Rlogin, NPort 6000 автоматически подключается к хосту, используя специальный протокол.

Primary и Secondary host address: Указанные в этих полях адреса указывают, к каким хостам будет всегда подключаться терминал.

Telnet TCP port (по умолчанию=23): По умолчанию номер порта телнет-сервиса равен 23.

Terminal type (по умолчанию = ansi): Некоторые приложения ранних версий могут требовать определения протокола канального уровня перед установлением соединения. Для выбора правильного типа протокола обращайтесь к документации сервера. В большинстве случаев эта настройка необязательна и не имеет особого значения.

Max. Sessions (по умолчанию = 4): Данный параметр позволяет задавать максимальное количество подключений к одному последовательному порту.

Change Session (по умолчанию = (^T)0x14): Это поле определяет клавишу быстрой смены подключения.

Quit (по умолчанию = (^E)0x05): Это поле определяет клавишу закрытия подключения.

Break: данный параметр определяет клавишу отправки сигнала паузы.

Interrupt: Это поле определяет клавишу закрытия программы.

Auto-login prompt (по умолчанию = ogin:)

Password prompt (по умолчанию = password:)

Login user name: Введите здесь логин пользователя терминала.

Login password: Пароль для авторизации пользователя терминала.

Двоичный терминал использует два режима передачи файлов: XMODEM или ZMODEM. В данном режиме можно открывать только одно соединение.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Inactivity time (по умолчанию = 0 мс): Время бездействия. В данном поле задается время, в течение которого NPort ожидает входящих или исходящих данных на последовательном порте перед тем как разорвать TCP-соединение. TCP-соединение закрывается, если в течение времени, равного **Inactivity time** через последовательный порт не идут данные ни в каком направлении. Если значение равно 0, то TCP-соединение остается активным, пока не будет получена команда закрытия.



ВНИМАНИЕ

При использовании данного параметра **Inactivity time** необходимо задавать его значение большим, чем **Force transmit time**. Для предотвращения случайной потери данных из-за разрыва соединения рекомендуется, чтобы значение параметра Inactivity time было достаточным для завершения передачи данных.

Auto-Link Protocol: Если в этом поле установлено None, NPort 6000 не будет автоматически подключаться к хосту. Если этот параметр установлен в Telnet или Rlogin, NPort 6000 автоматически подключается к хосту, используя специальный протокол.

Primary и Secondary host address: Указанные в этих полях адреса указывают, к каким хостам будет всегда подключаться терминал.

Telnet TCP port (по умолчанию=23): По умолчанию номер порта телнет-сервиса равен 23.

Terminal type (по умолчанию = ansi): Некоторые приложения ранних версий могут требовать определения протокола канального уровня перед установлением соединения. Для выбора правильного типа протокола обращайтесь к документации сервера. В большинстве случаев эта настройка необязательна и не имеет особого значения.

Quit (по умолчанию = (^E)0x05): Это поле определяет клавишу закрытия подключения.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Auto-login prompt (по умолчанию = ogin:)

Password prompt (по умолчанию = password:)

Login user name: Введите здесь логин пользователя терминала.

Login password: Пароль для авторизации пользователя терминала.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Inactivity time (по умолчанию = 0 мс): Время бездействия. В данном поле задается время, в течение которого NPort ожидает входящих или исходящих данных на последовательном порте перед тем как разорвать TCP-соединение. TCP-соединение закрывается, если в течение времени, равного **Inactivity time** через последовательный порт не идут данные ни в каком направлении. Если значение равно 0, то TCP-соединение остается активным, пока не будет получена команда закрытия.



ВНИМАНИЕ

При использовании данного параметра **Inactivity time** необходимо задавать его значение большим, чем **Force transmit time**. Для предотвращения случайной потери данных из-за разрыва соединения рекомендуется, чтобы значение параметра Inactivity time было достаточным для завершения передачи данных.

Primary и Secondary host address: Указанные в этих полях адреса указывают, к каким хостам будет всегда подключаться терминал.

SSH TCP port (по умолчанию = 22): по умолчанию номер TCP-порта для SSH равен 22.

Quit (по умолчанию = (^E)0x05): Это поле определяет клавишу закрытия подключения.

Break: данный параметр определяет клавишу отправки сигнала паузы.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Login user name: Введите здесь логин пользователя терминала.

Login password: Пароль для авторизации пользователя терминала.

Reverse Terminal Applications (Инверсный терминал)

Reverse Telnet

The screenshot shows the MOXA web interface for configuring a serial port. The left sidebar shows a tree view with 'Serial Port Settings' expanded to 'Port 1'. The main content area is titled 'Operation Modes' and contains the following settings for 'Port 1':

- Application:** Reverse Terminal (dropdown)
- Mode:** Reverse Telnet (dropdown)
- TCP alive check time:** 7 (0 - 99 min)
- Inactivity time:** 0 (0 - 99 min)
- TCP port:** 4001

The 'Terminal' section includes:

- Authentication type:** None (dropdown)
- Try next type on authentication denied:** Enable Disable
- Map keys <CR-LF>:** CR-LF (dropdown)

At the bottom, there are checkboxes to 'Apply the above settings to' ports P1 through P16, with P1 checked. A 'Submit' button is located at the bottom left of the configuration area.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва

соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Inactivity time (по умолчанию = 0 мин.): Время бездействия. В данном поле задается время, в течение которого NPort ожидает входящих или исходящих данных на последовательном порте перед тем как разорвать. Если значение равно 0, то порт остается активным, даже при отсутствии соединения.

TCP port (по умолчанию = 4001): Это номер TCP-порта последовательного интерфейса NPort'a 6000. Данный порт прослушивается NPort'ом 6000 для установления соединений и другие устройства должны использовать его для установления соединений с последовательным портом. Во избежание совпадения с TCP-портами, используемыми другими приложениями, данный номер установлен по умолчанию равным 4001.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Map keys <CR-LF> (по умолчанию=CR-LF): здесь определяется как **ENTER**, полученное с Ethernet-порта отображается на последовательном порте.

Значение	Описание
<CR-LF>	Возврат каретки+перевод строки (т.е. происходит переход курсора на первый символ следующей строки)
<CR>	Возврат каретки (т.е. курсор переходит на первый символ текущей строки)
<LF>	Перевод строки (т.е. курсор переходит на следующую строку, но не перемещается по горизонтали)

Reverse SSH

The screenshot shows the MOXA web interface for configuring a serial port. The left sidebar contains a navigation menu with options like 'Main Menu', 'Overview', 'Basic Settings', 'Network Settings', 'Serial Port Settings', and a list of ports from Port 1 to Port 15. The main area is titled 'Operation Modes' and is currently set for 'Port 1'. It contains the following settings:

- Application:** Reverse Terminal
- Mode:** Reverse SSH
- TCP alive check time:** 7 (0 - 99 min)
- Inactivity time:** 0 (0 - 99 min)
- TCP port:** 4001

The 'Terminal' section includes:

- Authentication type:** None
- Try next type on authentication denied:** Enable (selected), Disable
- Map keys <CR-LF>:** CR-LF

At the bottom, there are checkboxes to 'Apply the above settings to' ports P1 through P16, with P1 checked. A 'Submit' button is located at the bottom left of the configuration area.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Inactivity time (по умолчанию = 0 мин.): Время бездействия. В данном поле задается время, в течение которого NPort ожидает входящих или исходящих данных на последовательном порте перед тем как разорвать. Если значение равно 0, то порт остается активным, даже при отсутствии соединения.

TCP port (по умолчанию = 4001): Это номер TCP-порта последовательного интерфейса NPort'a 6000. Данный порт прослушивается NPort'ом 6000 для установления соединений и другие устройства должны использовать его для установления соединений с последовательным портом. Во избежание совпадения с TCP-портами, используемыми другими приложениями, данный номер установлен по умолчанию равным 4001.

Каждому последовательному порту NPort'a 6000 назначается свой TCP-порт: для порта №1: 4001, для порта №2: 4002 и т.д.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.

Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Map keys <CR-LF> (по умолчанию=CR-LF): здесь определяется как **ENTER**, полученное с Ethernet-порта отображается на последовательном порте.

Значение	Описание
<CR-LF>	Возврат каретки+перевод строки (т.е. происходит переход курсора на первый символ следующей строки)
<CR>	Возврат каретки (т.е. курсор переходит на первый символ текущей строки)
<LF>	Перевод строки (т.е. курсор переходит на следующую строку, но не перемещается по горизонтали)

Printer Applications (приложения печати)

RAW PRN

The screenshot shows the MOXA web interface for configuring serial ports. The left sidebar shows a tree view with 'Serial Port Settings' expanded to 'Port 1'. The main area is titled 'Operation Modes' and shows settings for 'Port 1':

- Application:** Printer
- Mode:** RAW_PRN
- TCP alive check time:** 7 (0 - 99 min)
- Group:** Group01
- TCP port number:** 2048
- Apply the above settings to:**
 - P1
 - P2
 - P3
 - P4
 - P5
 - P6
 - P7
 - P8
 - P9
 - P10
 - P11
 - P12
 - P13
 - P14
 - P15
 - P16
 - All ports

A 'Submit' button is located at the bottom of the configuration area.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Group (по умолчанию=Group 01): Это поле объединяет в группу принтеры, подключенные к различным портам. Когда запрос на печать посылается группе, то все входящие в нее принтеры воспринимают это задание. Например, объединение последовательных портов 1, 3 и 6 NPort'a 6000 в одну группу Group 01 позволит работать с подключенными к ним принтерами как в одном.

TCP port number: Данное поле заполняется автоматически NPort'ом 6000 и не может быть изменено пользователем. Хост использует данное значение для определения группы, к которой относится принтер данного порта. Группам 01 – 06 назначаются номера: 2048-2063 соответственно.

LPD PRN

The screenshot shows the MOXA web interface for configuring a port. The left sidebar shows a tree view under 'Serial Port Settings' with 'Port 1' selected. The main content area is titled 'Operation Modes' and shows the configuration for 'Port 1'. The 'Application' is set to 'Printer' and the 'Mode' is 'LPD_PRN'. The 'TCP alive check time' is set to 7 minutes. There are input fields for 'Queue name (RAW)' and 'Queue name (ASCII)'. The 'Append from feed' option is set to 'Disable'. Below these are checkboxes for applying settings to ports P1 through P16, with P1 checked. A 'Submit' button is at the bottom.

TCP alive check time (по умолчанию = 7 мин.): данный параметр определяет, как долго NPort 6000 ожидает ответа (пакетов «keep alive») перед тем, как разорвать TCP-соединение. NPort 6000 проверяет состояние соединения, периодически посылая пакеты “keep alive”. Если удаленный хост не отвечает в течение заданного в этом поле времени, то NPort 6000 разорвет текущее TCP-соединение. В режимах socket и device control после разрыва соединения NPort 6000 будет прослушивать TCP-канал. Если параметр **TCP alive check time** установлен в 0, то TCP-соединение будет оставаться открытым все время, и не будет посылаться никаких пакетов “keep alive”.

Queue name (RAW): (необязательно) данное поле определяет имя очереди заданий для принтера (в режиме RAW).

Queue name (ASCII): (необязательно) данное поле определяет имя очереди заданий для принтера (в режиме ASCII).

Append from feed (по умолчанию = Disable): данное поле предписывает порту распределять строки между заданиями на печать, а не последнему освободившемуся принтеру. Это может понадобиться в некоторых приложениях.

Приложения Dial In/Out

Режим PPP

The screenshot shows the MOXA web interface for configuring a port. The left sidebar contains a navigation tree with categories like Main Menu, Overview, Basic Settings, Network Settings, and Serial Port Settings. The main area is titled 'Operation Modes' and 'Port 1'. The configuration fields are as follows:

- Application:** Dial in/out (dropdown)
- Mode:** PPP (dropdown)
- Destination IP address:** (text input)
- Source IP address:** (text input)
- IP netmask:** (text input)
- TCP/IP compression:** Enable (radio), Disable (radio, selected)
- Inactivity time:** 0 (text input) (0 - 65535 ms)
- Link quality report:** Enable (radio), Disable (radio, selected)
- Username:** (text input)
- Password:** (text input)
- Authentication type:** None (dropdown)
- Try next type on authentication denied:** Enable (radio), Disable (radio, selected)
- Disconnect by:** None (dropdown)

Below these fields, there are checkboxes to 'Apply the above settings to' ports P1 through P16. P1 is checked, while P2 through P16 are unchecked. There is also an 'All ports' checkbox which is unchecked. A 'Submit' button is located at the bottom of the configuration area.

Режим PPP обеспечивает стандартные службы для соединений dial-in и dial-out.

Destination IP address: Это IP-адрес удаленного dial-in/dial-out -сервера.

Source IP address: IP-адрес устройства, непосредственно подключенного к данному последовательному порту.

IP netmask: маска подсети определяет подсеть для установления PPP-соединения.

TCP/IP compression (по умолчанию = No): данная функция используется, если удаленное приложение требует сжатия данных.

Inactivity time (по умолчанию = 0 мс): Это поле определяет время отсутствия сетевой активности перед разрывом соединения. Если установлено 0 мс, то соединение поддерживается даже при отсутствии обмена.

Link quality report (по умолчанию = No): Если значение Yes, то NPort 6000 будет разрывать соединение при уровне помех выше определенного предела.

Username: логин аккаунта пользователя сервиса dial-out.

Password: пароль аккаунта.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Disconnect by (по умолчанию = None): Если установлено значение **DCD-off**, соединение будет разрываться при переход сигнала DCD в OFF. Если выбрано **DSR-off**, то соединение разрывается, когда сигнала DSR переходит в состояние «выкл.»

Режим PPPD

PPPD (PPP on demand – по требованию) – используется для службы удаленного доступа (dial-in) – PPP-соединение устанавливается только при получении запроса с удаленного ПК.

Destination IP address: IP-адрес удаленного сервера служб dial-in/dial-out.

Source IP address: IP-адрес устройства, соединенного с последовательным портом.

IP netmask: маска подсети для установления PPP-соединения.

TCP/IP compression (по умолчанию = No): данная функция используется, если удаленное приложение требует сжатия данных.

Inactivity time (по умолчанию = 0 мс): Это поле определяет время отсутствия сетевой активности перед разрывом соединения. Если установлено 0 мс, то соединение поддерживается даже при отсутствии обмена.

Link quality report (по умолчанию = No): Если значение **Yes**, то NPort 6000 будет разрывать соединение при уровне помех выше определенного предела.

Username: логин аккаунта пользователя сервиса dial-out.

Password: пароль аккаунта.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Disconnect by (по умолчанию = None): Если установлено значение **DCD-off**, соединение будет разрываться при переход сигнала DCD в OFF. Если выбрано **DSR-off**, то соединение разрывается, когда сигнала DSR переходит в состояние «выкл.»

The screenshot shows the MOXA web interface for configuring serial ports. The left sidebar shows a tree view under 'Serial Port Settings' with 'Port 1' selected. The main area is titled 'Operation Modes' and 'Port 1'. The configuration includes:

- Application:** Dial in/out (dropdown)
- Mode:** SLIP (dropdown)
- Destination IP address:** (text input)
- Source IP address:** (text input)
- IP netmask:** (text input)
- TCP/IP compression:** Radio buttons for 'Enable' and 'Disable' (selected)
- Inactivity time:** 0 (text input) (0 - 65535 ms)
- Disconnect by:** None (dropdown)
- Apply the above settings to:** Checkboxes for P1 through P16, and 'All ports'.

A 'Submit' button is located at the bottom of the configuration area.

SLIP обеспечивает службу SLIP (протокол последовательной межсетевой связи) для dial-in и dial-out-соединений.

Destination IP address: IP-адрес удаленного сервера служб dial-in/dial-out.

Source IP address: IP-адрес устройства, соединенного с последовательным портом.

IP netmask: маска подсети для установления PPP-соединения.

TCP/IP compression (по умолчанию = No): данная функция используется, если удаленное приложение требует сжатия данных.

Inactivity time (по умолчанию = 0 мс): Это поле определяет время отсутствия сетевой активности перед разрывом соединения. Если установлено 0 мс, то соединение поддерживается даже при отсутствии обмена.

Disconnect by (по умолчанию = None): Если установлено значение **DCD-off**, соединение будет разрываться при переход сигнала DCD в OFF. Если выбрано **DSR-off**, то соединение разрывается, когда сигнала DSR переходит в состояние «выкл.»

Режим SLIPD

The screenshot shows the MOXA web interface for configuring serial ports. The left sidebar displays a tree view under 'Serial Port Settings' with folders for 'Port 1' through 'Port 14'. The 'Port 1' folder is expanded, showing sub-folders: 'Operation Modes', 'Communication Parameters', 'Data Buffering/Log', 'Modem Settings', and 'Cipher Settings'. The main content area is titled 'Operation Modes' and shows settings for 'Port 1'. The 'Application' is set to 'Dial in/out' and the 'Mode' is set to 'SLIPD'. There are input fields for 'Destination IP address', 'Source IP address', and 'IP netmask'. The 'TCP/IP compression' is set to 'Disable'. The 'Inactivity time' is set to '0' (0 - 65535 ms). The 'Disconnect by' dropdown is set to 'None'. Below these settings, there are checkboxes for 'Apply the above settings to' ports P1 through P16, with P1 checked. A 'Submit' button is at the bottom.

SLIPD (SLIP on demand – по требованию) – используется для службы SLIP только при получении запроса с удаленного ПК.

Destination IP address: IP-адрес удаленного сервера служб dial-in/dial-out.

Source IP address: IP-адрес устройства, соединенного с последовательным портом.

IP netmask: маска подсети для установления PPP-соединения.

TCP/IP compression (по умолчанию = No): данная функция используется, если удаленное приложение требует сжатия данных.

Inactivity time (по умолчанию = 0 мс): Это поле определяет время отсутствия сетевой активности перед разрывом соединения. Если установлено 0 мс, то соединение поддерживается даже при отсутствии обмена.

Disconnect by (по умолчанию = None): Если установлено значение **DCD-off**, соединение будет разрываться при переход сигнала DCD в OFF. Если выбрано **DSR-off**, то соединение разрывается, когда сигнала DSR переходит в состояние «выкл.»

Режим Dynamic

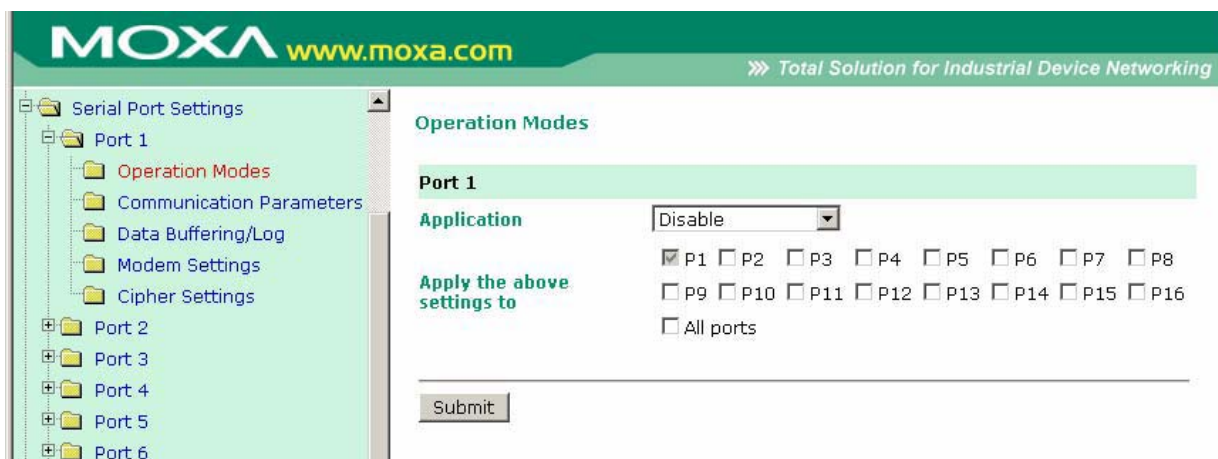
Данный режим объединяет режимы PPPD, SLIPD и Terminal dial-in. В этом режиме автоматически определяется, какой тип соединения используется удаленным хостом, и выбирается соответствующий вариант. Можно включать/отключать PPP/SLIP/Terminal по отдельности выбором Enable/Disable в соответствующем поле.

Authentication Type (по умолчанию=None): В этом поле можно выбрать метод, используемый для проверки имени пользователя и его авторизации.

Вариант выбора	Описание
Local	Сверять имя пользователя по таблице пользователей [User Table] NPort'a 6000.
RADIUS	Проверять имя пользователя на внешнем сервере RADIUS.
RADIUS-Local	В первую очередь выполняется попытка проверки на RADIUS-сервере, в случае неудачи – переключение на режим Local.
Local-RADIUS	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью RADIUS-сервера.
TACACS+	Авторизация с помощью TACACS - Terminal Access Controller Access Control System - Система управления доступом для контроллера доступа к терминалу
TACACS+-Local	В первую очередь выполняется попытка авторизации по TACACS+, затем переключение на режим Local.
Local-TACACS+	Авторизация выполняется сначала с помощью локальной таблицы, в случае неудачи – с помощью TACACS+
None	Отсутствие авторизации.

Try next type on authentication (по умолчанию=Disable): данная настройка включает/отключает переход системы к следующему типу авторизации в случае неудачи с первой.

Disabled (последовательный порт отключен)



Если выбран режим **Disable**, соответствующий порт отключен.

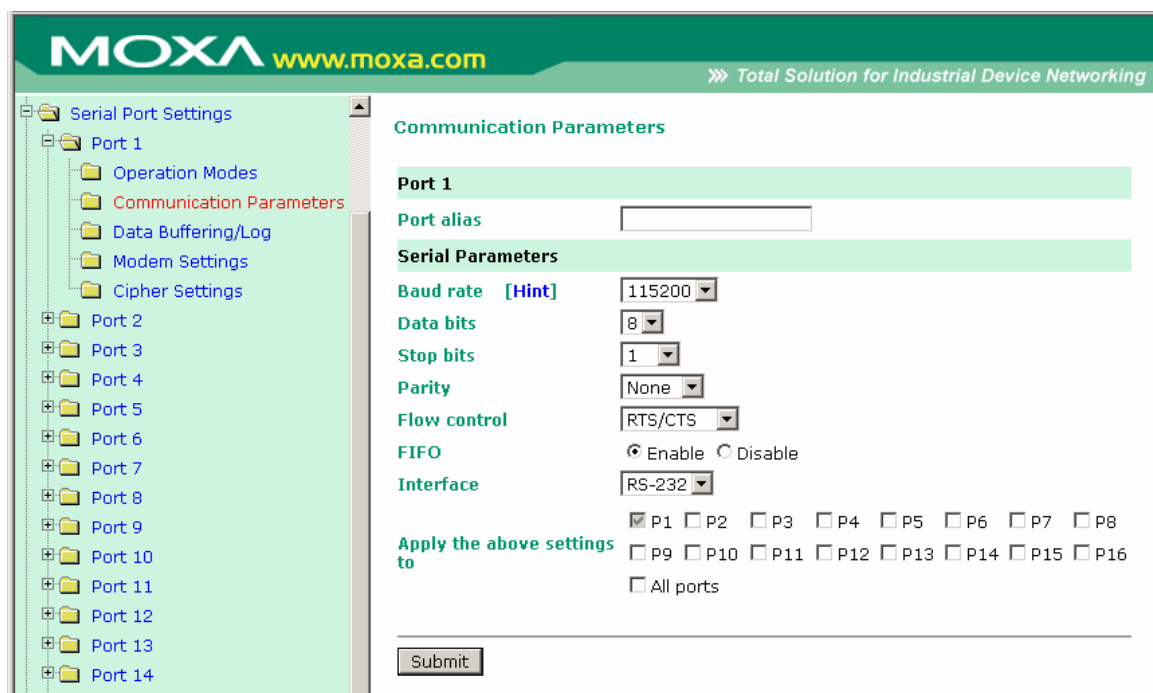
8 Дополнительные настройки последовательных портов

В данной главе описаны дополнительные настройки последовательных портов NPort'a 6000. Те же самые опции доступны также по telnet и по последовательной консоли.

Данная глава содержит следующие разделы:

- **Port Communication Parameters (Настройки связи порта)**
- **Serial parameters (Параметры последовательной передачи данных)**
- **Port Data Buffering/Log (буферизация/запись данных последовательного порта)**
- **Port Modem Settings (Настройки модемного соединения)**
- **Port Cipher Settings ()**
- **Welcome Message (Приветственное сообщение)**

Port Communication Parameters (Настройки связи порта)



The screenshot shows the MOXA web interface for configuring port communication parameters. The left sidebar contains a tree view of settings, with 'Port 1' selected under 'Communication Parameters'. The main area displays the configuration for 'Port 1', including a 'Port alias' field, 'Serial Parameters' (Baud rate: 115200, Data bits: 8, Stop bits: 1, Parity: None, Flow control: RTS/CTS, FIFO: Enable), and checkboxes for applying settings to ports P1 through P16. A 'Submit' button is located at the bottom of the configuration area.

Port alias: Это необязательное поле позволяет Вам назначать метку порта для более понятной идентификации.

Serial parameters (Параметры последовательной передачи данных)



ВНИМАНИЕ

Параметры каждого последовательного порта NPort'a 6000 должны совпадать с настройками, используемыми подключенным последовательным устройством. Для выбора нужных параметров следует руководствоваться рекомендациями, приведенными в документации на последовательное устройство.

Baud rate (по умолчанию=115200 бит/с): Данное поле используется для настройки скорости обмена. Выберите одно из стандартных значений в выпадающем списке или пункт **Other** и затем наберите значение скорости в поле ввода.



ВНИМАНИЕ

Если для работы порта необходима скорость, отсутствующая в списке, к примеру, 500000 бит/с, нужно выбрать вариант **Other** и затем ввести требуемое значение скорости в текстовое поле. NPort 6000 автоматически вычисляет ближайшую поддерживаемую скорость. Погрешность автоопределения составляет менее 1,7% для всех скоростей, меньших 921600 бит/с.

Data bits (число битов данных, по умолчанию=8): В данном поле задается число битов данных. Замечание: Если это число задано равным 5, то число стоп-битов автоматически будет установлено равным 2.

Stop bits (стоп-биты, по умолчанию=1): В данном поле задается число стоповых битов. Замечание: Если число битов данных установлено равным 5, то число стоповых автоматически будет равно 1,5 бит.

Parity (по умолчанию = None): В этом поле настраивается контроль четности.

Flow control (по умолчанию = RTS/CTS): В данном поле задается способ управления потоком данных.

FIFO (по умолчанию = Enable): Данное поле включает или отключает буфер FIFO (очередь типа «первым пришел - первым ушел») на 128 байт. NPort 6000 имеет FIFO-память для каждого последовательного порта, для обоих сигналов Tx/Rx (передача/прием). Однако, если подключаемое последовательное устройство не имеет своего FIFO-буфера, то и на NPort'e 6000 следует отключить данную опцию. Это вызвано тем, что устройство, не имеющее промежуточной памяти, не сможет обработать данные, поступающие из FIFO-буфера NPort'a 6000.

Interface (по умолчанию = RS-232): Можно настроить один из последовательных интерфейсов: RS-232/422/485 (двух- или четырехпроводный).

Port Data Buffering/Log (буферизация/запись данных последовательного порта)

The screenshot shows the MOXA web interface for configuring a serial port. The left sidebar shows a tree view with 'Serial Port Settings' expanded to 'Port 1', and 'Data Buffering/Log' selected. The main content area is titled 'Data Buffering/Log' and shows settings for 'Port 1'. The 'Port buffering' option is set to 'Disable'. The 'Port buffering location' is set to 'Memory(64K)'. The 'Port buffering SD file size' is set to '1' Mbytes. The 'Serial data logging (64K)' option is set to 'Disable'. There are checkboxes for applying settings to individual ports (P1-P16) and an 'All ports' option. A 'Submit' button is at the bottom.

NPort 6000 имеет возможность буферизации данных последовательного порта для предотвращения потери данных при отсутствии Ethernet-соединения. Буферизация может применяться в режимах TCP Server, TCP Client, а также парного соединения Pair Connection. Для других режимов настройки буферизации неприменимы.

Port buffering enable (по умолчанию = No): Можно включить буферизацию, установив в этом поле значение Yes.

Port buffering location (по умолчанию = Memory (64K)): Если включена буферизация, используйте данный параметр для определения используемого буфера – встроенной памяти или дополнительной SD-карты. Если требуется размер памяти больше 64 Кбайт, используйте дополнительную карту памяти. Необходимо помнить, что SD-карта невозможно установить в модели NPort 6150.

Port buffering SD file size (по умолчанию = 1 Мбайт): В данном поле задается размер буфера, на SD-карте. Внимание: дополнительные SD-карты не поддерживаются NPort'ами 6150.

Serial data logging enable (по умолчанию = No): Если в данном поле значение Yes, то NPort 6000 будет сохранять логи данных со всех последовательных портов в системной RAM-

памяти. Необходимо помнить, что данные не сохраняются, когда NPort 6000 обесточен. Для хранения данных с каждого последовательного порта выделяется 64 Кбайт.

Port Modem Settings (Настройки модемного соединения)

The screenshot shows the MOXA web interface for configuring serial port settings. The left sidebar contains a tree view with 'Serial Port Settings' expanded to show 'Port 1', 'Port 2', 'Port 3', 'Port 4', 'Port 5', 'Port 6', 'Port 7', 'Port 8', and 'Port 9'. Under 'Port 1', there are sub-items: 'Operation Modes', 'Communication Parameters', 'Data Buffering/Log', 'Modem Settings' (highlighted in red), and 'Cipher Settings'. The main content area is titled 'Modem Settings' and shows the configuration for 'Port 1'. The 'Enable modem' section has radio buttons for 'Enable' and 'Disable', with 'Disable' selected. The 'Initial string' field contains 'AT'. The 'Dial up' field contains 'ATD'. The 'Phone number' field is empty. Below these fields, there are checkboxes for 'Apply the above settings to' ports P1 through P16, and an 'All ports' checkbox. A 'Submit' button is located at the bottom of the settings area.

Настройки модема используются для режимов Dial In/Out. Данные настройки не будут иметь силы, если последовательные порты работают в других режимах.

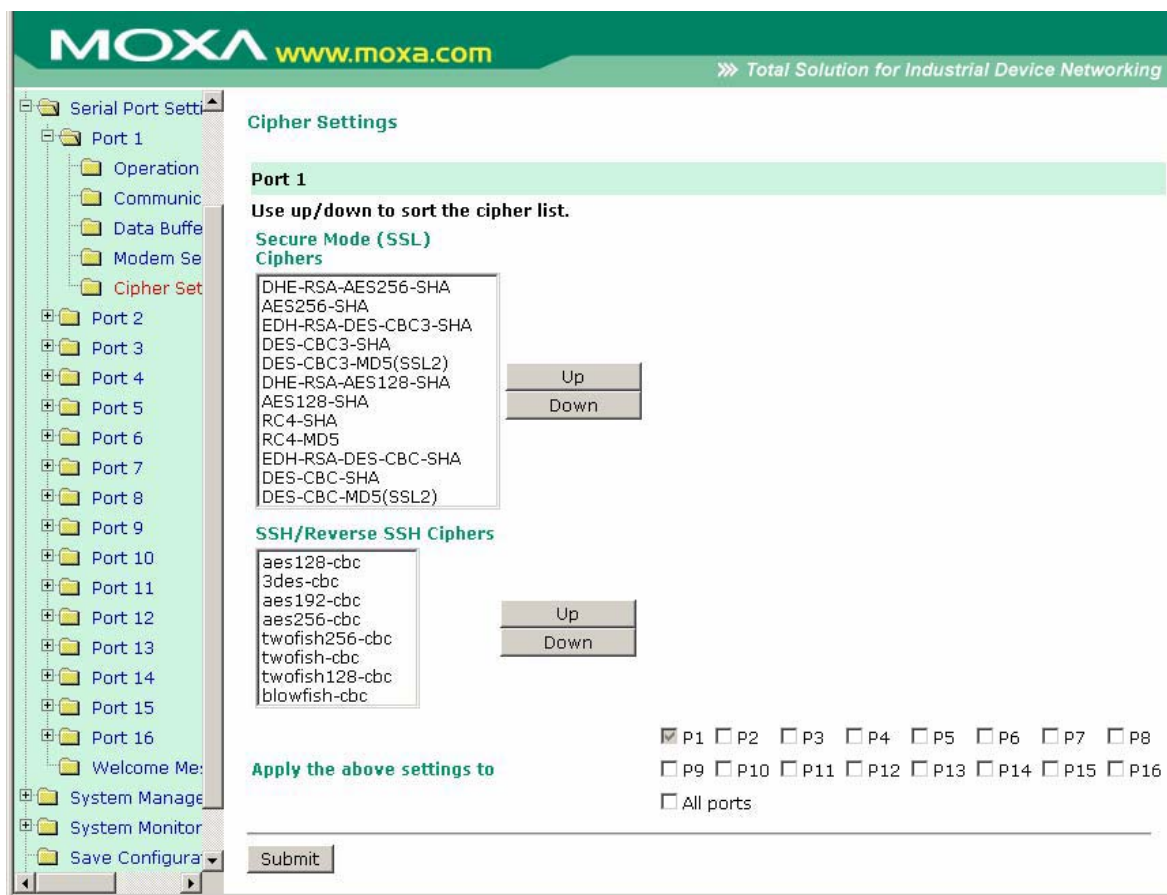
Enable modem (по умолчанию = Disable (отключен)): Включить/отключить модем

Initial string: Данное поле используется для задания начальной строки, используемой модемом для установления соединения. Например, **AT&S0=1** для автоответа.

Dial up: Данное поле используется для настройки строки AT-команды дозвона Dial-up.

Phone number: Данное поле используется для указания номера дозвона.

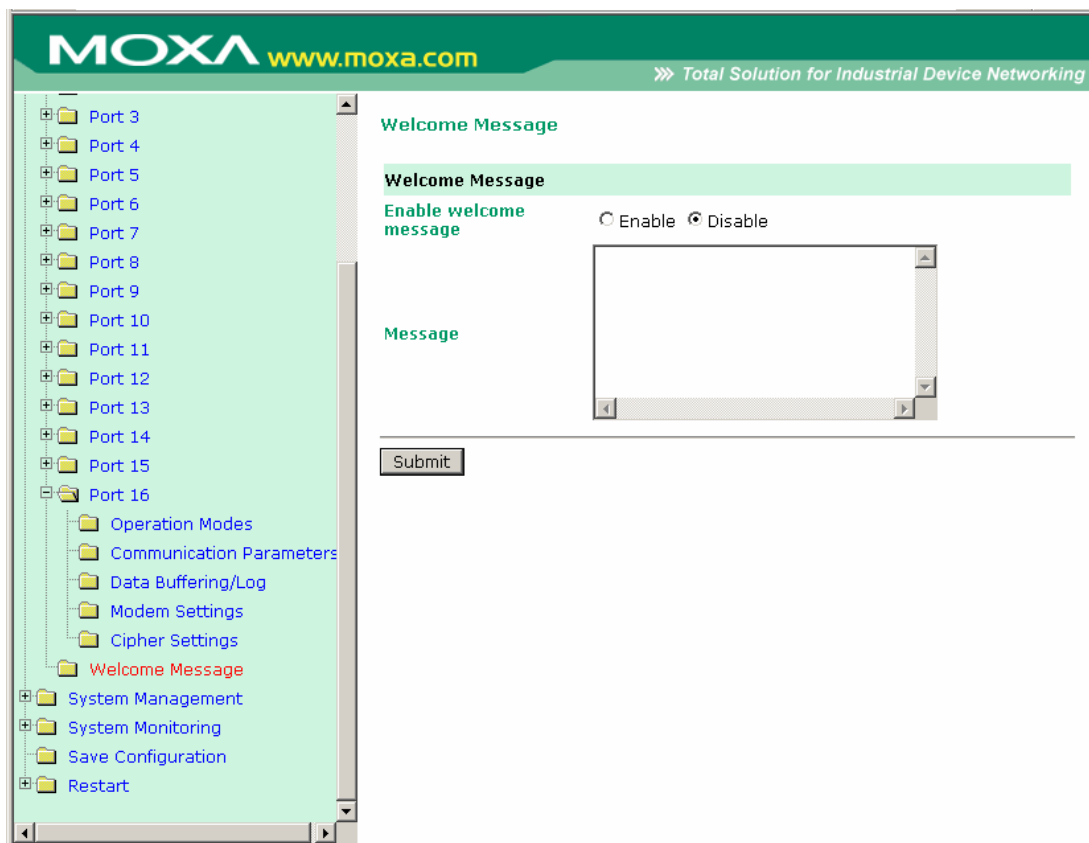
Port Cipher Settings (Настройки шифрования)



Serial Port Settings → Port N → Cipher Settings

Используемые по приоритетам шифры для установления безопасных SSL и SSH-соединений. Список **Secure Mode (SSL) Ciphers** используется, когда выбран режим Secure. Список **SSH/Reverse SSH Ciphers** используется только в режимах SSH terminals и Reverse SSH terminals.

Welcome Message (Приветственное сообщение)



Вы можете включить функцию приветственного сообщения для дозванивающихся по Dial-in пользователей и ввести его текст. Для портов, настроенных в других режимах, данная функция неприменима.

9 Системные настройки

В данной главе описаны дополнительные системные настройки NPort'a 6000. Те же самые опции доступны также по telnet и по последовательной консоли.

Данная глава содержит следующие разделы:

- **Misc. Network Settings (Прочие сетевые настройки)**
 - Accesible IP List (список разрешенных IP-адресов)
 - SNMP Agent Settings (настройки для SNMP-агента)
 - DDNS
 - Host Table (таблица с именами хостов)
 - User Table (таблица пользователей)
 - Authentication Server (Сервер авторизации)
 - System Log Settings (настройки системных записей)
 - Configure the Remote Log Server (настройка удаленного сервера записей)
- **Auto Warning Settings (Настройки автооповещения)**
 - Event Settings (настройки событий)
 - Serial Event Settings (настройки событий по последовательным портам)
 - E-mail Alert (оповещения по электронной почте)
 - SNMP Trap (прерывания по SNMP)
- **Maintenance (Функции технического обслуживания и диагностики)**
 - Console Setting (консольные настройки)
 - Ping (проверка связи с другими хостами)
 - Firmware Upgrade (обновление прошивки)
 - Configuration Import/Export (импорт/экспорт настроек)
 - Load Factory Defaults (Загрузить заводские настройки)
 - Change Password (Изменить пароль)
- **Certificate**
 - Ethernet Certificate Import
 - Certificate/Key Delete
- **System Monitoring**
 - Serial to Network Connections
 - Serial Port Status
 - Serial Port Error Count
 - Serial Port Settings
 - Serial Cipher Usage Status
 - Network Connections
 - System Monitor/System Status/Network Module
 - Network Module
 - Network Statistics
 - Serial Data Log
 - System Log
 - Routing
 - Dout State (для 6450/6650)
- **Save Configuration (Сохранение настроек)**
- **Restart (Перезапуск)**
 - Restart System (Перезапуск системы)
 - Restart Ports (Перезагрузка портов)

Misc. Network Settings (Прочие сетевые настройки)

Accessible IP List (список разрешенных IP-адресов)

MOXA www.moxa.com Total Solution for Industrial Device Networking

Accessible IP List

Enable the accessible IP list ("Disable" will allow all IP's connection request.)

No	Active	IP Address	Netmask
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
11	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
12	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
13	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
14	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
15	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
16	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Submit

NPort 6000 используют метод контроля доступа к последовательным портам на основе IP-адресов.

Список допустимых IP-адресов позволяет ограничивать сетевой доступ к NPort'у 6000. Доступ осуществляется на основе IP-адреса. Когда список включен (флаг enable), для того, чтобы удаленный хост имел доступ к NPort'у 6000, необходимо, чтобы IP-адрес этого хоста присутствовал в списке Accessible IP list. Можно также задавать определенные диапазоны адресов, используя различные комбинации параметров IP-адрес и маска подсети, как показано ниже:

Для разрешения доступа с определенного IP-адреса:

Введите IP-адрес в соответствующем поле; в качестве маски подсети укажите **255.255.255.255**.

Для разрешения доступа с хостов одной определенной подсети:

При указании IP-адреса и маски последнее число равно 0 (например, **192.168.1.0** и **255.255.255.0**).

Для разрешения неограниченного доступа

Снимите флажок [Enable the accessible IP list].

См. примеры настроек в таблице ниже:

Разрешенные хосты	Параметры настроек: IP-адрес/Маска подсети
Любой хост	Disable (снят флаг Enable)
192.168.1.120	192.168.1.120 / 255.255.255.255
С 192.168.1.1 по 192.168.1.254	192.168.1.0 / 255.255.255.0
С 192.168.0.1 по 192.168.255.254	192.168.0.0 / 255.255.0.0
С 192.168.1.1 по 192.168.1.126	192.168.1.0 / 255.255.255.128
С 192.168.1.129 по 192.168.1.254	192.168.1.128 / 255.255.255.128

SNMP Agent Settings (настройки для SNMP-агента)



SNMP: для активации функции SNMP-агента установите переключатель в **Enable** и затем введите имя SNMP-группы (в примере **public**).

Read community string (по умолчанию = public): Это механизм текстового пароля, используемый в запросах на авторизацию агентов управляемых сетевых устройств.

Write community string (по умолчанию = private): Это механизм текстового пароля, используемый при изменениях авторизации для агентов управляемой сети.

Contact name: Дополнительная информация для соединения по SNMP, обычно включает контактное имя и телефон или номер пэйджера.

Location: Данное поле используется для указания местонахождения для SNMP-агентов, таких как NPort 6000. Эта строка обычно указывается улица, где географически расположен NPort 6000.

SNMP agent version: NPort 6000 поддерживает версии SNMP v1, v2 и v3.

Контроль доступа для чтения и чтения/записи

Данные поля позволяют определять имена пользователей, пароли и параметры авторизации для двух уровней доступа: чтения и чтения/записи. Название поля показывает соответствующий уровень доступа. Например, режим **Read Only** допускает только доступ к чтению, в то время как **Read/write** позволяет Вам настраивать доступ на чтение/запись. Для каждого уровня доступа можно настроить:

User name: Данное поле используется для задания имени пользователя с определенным уровнем доступа.

Authentication mode (по умолчанию = Disable - отключен): данное поле используется для выбора метода шифрования пароля: MD5 или SHA – для определенного уровня доступа; можно просто отключить авторизацию.

Privacy mode (по умолчанию = disable): данное поле используется для включения/отключения шифрования данных DES_CBC для определенного уровня доступа.

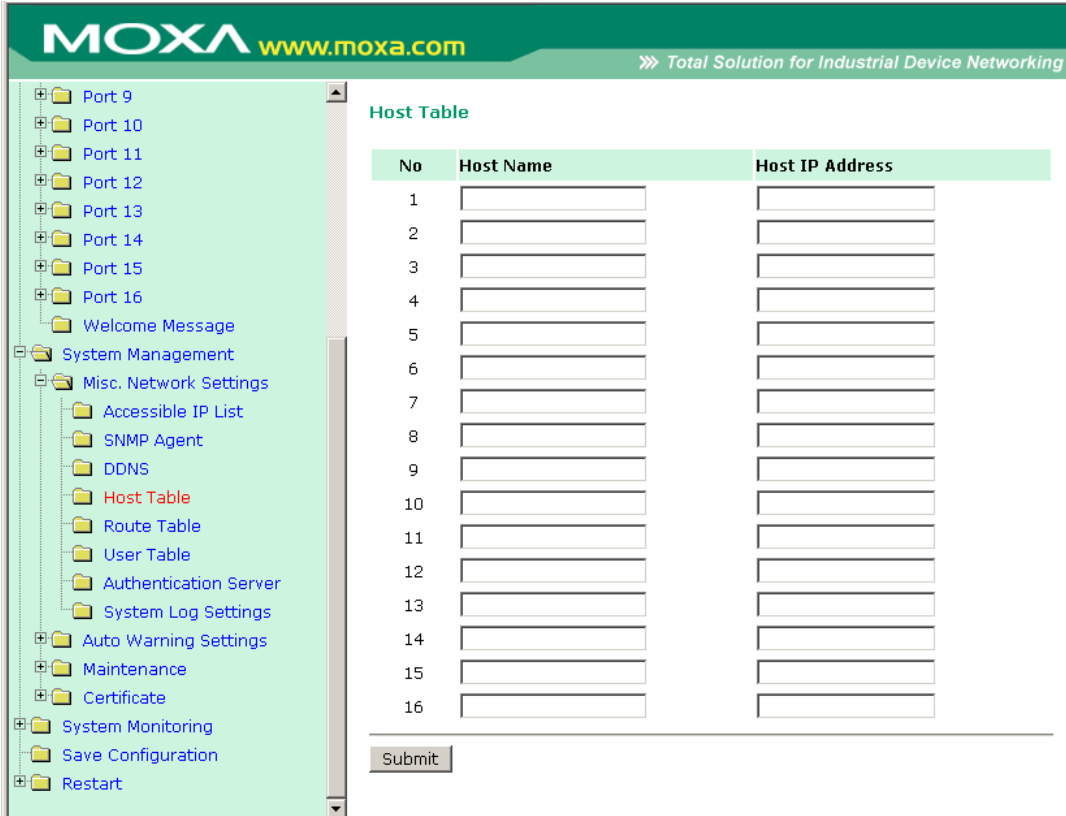
Password: Данное поле используется для задания пароля к определенному уровню доступа.

Privacy: данное поле используется для задания ключа шифрования для определенного уровня доступа.

DDNS

См. приложение Приложение C *DDNS-сервер* – подробнее о настройках DDNS на устройстве NPort 6000.

Host Table



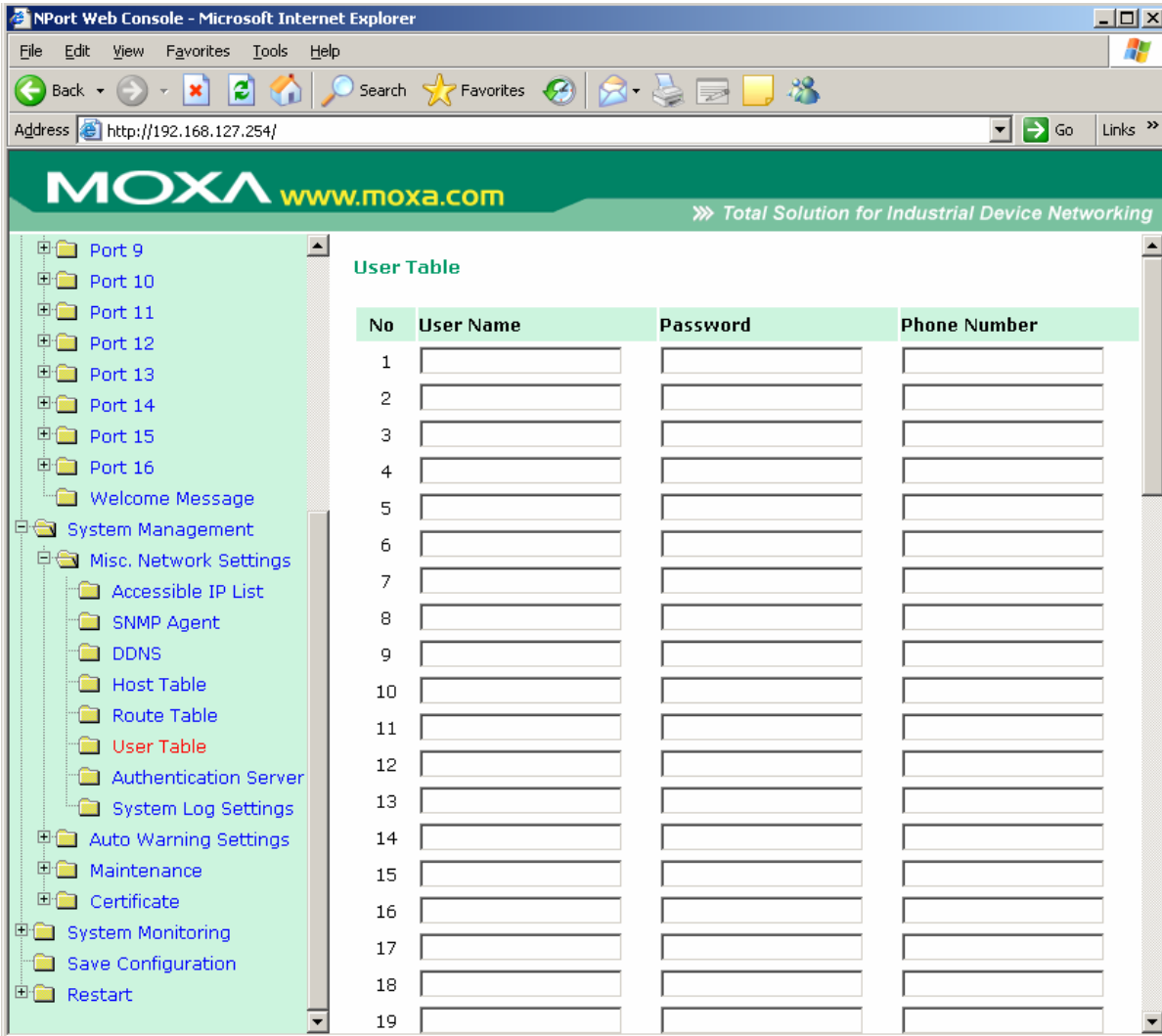
The screenshot shows the MOXA web interface for NPort 6000. The navigation tree on the left includes folders for Port 9 through Port 16, System Management, Misc. Network Settings, Auto Warning Settings, Maintenance, Certificate, System Monitoring, Save Configuration, and Restart. The 'Host Table' folder is selected. The main content area displays a table with the following structure:

No	Host Name	Host IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>
13	<input type="text"/>	<input type="text"/>
14	<input type="text"/>	<input type="text"/>
15	<input type="text"/>	<input type="text"/>
16	<input type="text"/>	<input type="text"/>

At the bottom of the table, there is a 'Submit' button.

Таблица хостов Host Table может быть использована для упрощения использования IP-адресов при настройке NPort'ов 6000 присвоением им текстовых имен доменов. Если хосту назначено имя, то везде, где потребуется вводить его IP-адрес, можно вместо него указывать это имя. В таблице может быть сохранено до 16 имен.

User Table (таблица пользователей)



The screenshot shows the NPort Web Console interface in a Microsoft Internet Explorer browser window. The address bar displays `http://192.168.127.254/`. The page header features the MOXA logo and the slogan "Total Solution for Industrial Device Networking". A left-hand navigation tree lists various system management options, with "User Table" highlighted in red. The main content area displays a table titled "User Table" with four columns: "No", "User Name", "Password", and "Phone Number". The table contains 19 rows, each with a number in the first column and empty input fields in the others.

No	User Name	Password	Phone Number
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>
13	<input type="text"/>	<input type="text"/>	<input type="text"/>
14	<input type="text"/>	<input type="text"/>	<input type="text"/>
15	<input type="text"/>	<input type="text"/>	<input type="text"/>
16	<input type="text"/>	<input type="text"/>	<input type="text"/>
17	<input type="text"/>	<input type="text"/>	<input type="text"/>
18	<input type="text"/>	<input type="text"/>	<input type="text"/>
19	<input type="text"/>	<input type="text"/>	<input type="text"/>

Таблицу пользователей NPort'a 6000 можно использовать для авторизации пользователей для терминального или обратного терминального доступа; функция нужна, например, в случае, если нет внутреннего RADIUS-сервера для авторизации. В таблице User Table NPort 6000 может быть до 64 имен.

Authentication Server (Сервер авторизации)

MOXA www.moxa.com Total Solution for Industrial Device Net

Main Menu

- Overview
- Basic Settings
- Network Settings
- Serial Port Settings
- System Management
 - Misc. Network Settings
 - Accessible IP List
 - SNMP Agent
 - DDNS
 - Host Table
 - Route Table
 - User Table
 - Authentication Server**
 - System Log Settings
 - Auto Warning Settings
 - Maintenance
 - Certificate
 - System Monitoring
 - Save Configuration
 - Restart
 - Logout System

Authentication Server

RADIUS

RADIUS server

RADIUS key

UDP port

RADIUS accounting Enable Disable

TACACS+

TACACS+ server

TACACS+ secret

TACACS+ accounting Enable Disable

RADIUS server IP: Если для авторизации пользователей используется RADIUS-сервер, в данном поле указывается его IP-адрес.

RADIUS key: В данном поле вводится ключ доступа для авторизации пользователей RADIUS-сервера.

UDP port (по умолчанию = 1645): В данном поле назначается UDP-порт, используемый для RADIUS-сервера.

RADIUS accounting: Данный параметр включает/отключает использование RADIUS-сервера.

TACACS+server: IP-адрес или доменное имя сервера для авторизации TACACS+server.

TACACS+secret: Пароль для авторизации пользователей TACACS+secret.

TACACS+accounting: Включение/отключение TACACS+accounting.

System Log Settings (настройки системных записей)

System Log Settings

Event Group	Local Log	Remote Log	Summary
System	<input type="checkbox"/>	<input type="checkbox"/>	System Cold Start, System Warm Start
Network	<input type="checkbox"/>	<input type="checkbox"/>	DHCP/BOOTP/PPPoE Get IP/Renew, NTP, Mail Fail, NTP Connect Fail, IP Conflict, Network Link Down
Config	<input type="checkbox"/>	<input type="checkbox"/>	Login Fail, IP Changed, Password Changed, Config Changed, Firmware Upgrade, SSL Certificate Import, Config Import, Config Export
OpMode	<input type="checkbox"/>	<input type="checkbox"/>	Connect, Disconnect, Authentication Fail, Restart

Настройки системных записей позволяют администратору определять, какие сетевые события будут фиксироваться NPort'ом 6000. События сгруппированы в 4 класса и сетевой администратор отмечает в столбце Local Log, какие группы попадают в записи. Конкретные системные события, которые будут фиксироваться, перечислены в столбце Summary. Например, если включена группа System, то будут выполняться записи о событиях System Cold Start (холодный перезапуск системы) и System Warm Start (теплый перезапуск системы).

Local Log (записи хранятся в NPort'е 6000)	Записи помещаются во внутреннюю флэш-память NPort'а 6000 – возможно до 512 записей.
Remote Log (записи хранятся на удаленном устройстве)	Записи находятся на определенном удаленном сервере записей Log Server. Если выбрана данная функция, то понадобится задание удаленного сервера в настройках: <i>System Management / Misc. Network Settings / Remote Log Settings</i> .

System (системные события)

System Cold Start	Холодный перезапуск NPort'а 6000
System Warm Start	Теплый перезапуск NPort'а 6000

Network (сетевые события)

DHCP/BOOTP/PPPoE Get IP/Renew	Обновился IP-адрес NPort'а 6000
NTP	Успешная синхронизация времени.
NTP Connect Fail	Не удалось подключиться к NTP-серверу.
Mail Fail	Не удалось доставить почту
IP Conflict	В локальной сети имеется конфликт IP-адресов.
Network Link Down	Потеряно соединение по Ethernet-порту LAN 1.

Config (настройки)

Login Fail	Неудачная попытка авторизации
IP Changed	Изменен IP-адрес
Password Changed	Изменен пароль
Config Changed	Изменены настройки
Firmware Upgrade	Обновлена прошивка
SSL Certificate Import	Импорт SSL-сертификата
Config Import	Импорт файла конфигурации
Config Export	Экспорт файла конфигурации

OpMode

Connect	Используется один из режимов работы
Disconnect	Не используется ни один из режимов работы
Authentication Fail	Неудачная авторизация в режимах terminal; reverse terminal; dial in/out.
Restart	Перезагружен последовательный порт

Configure the Remote Log Server (настройка удаленного сервера записей)

Remote Log Server

Configuration

SYSLOG server

SYSLOG facility

SYSLOG severity

SYSLOG server

IP-адрес или доменное имя удаленного сервера авторизации.

SYSLOG facility

Это информационное поле, связанное с сообщением о событии.

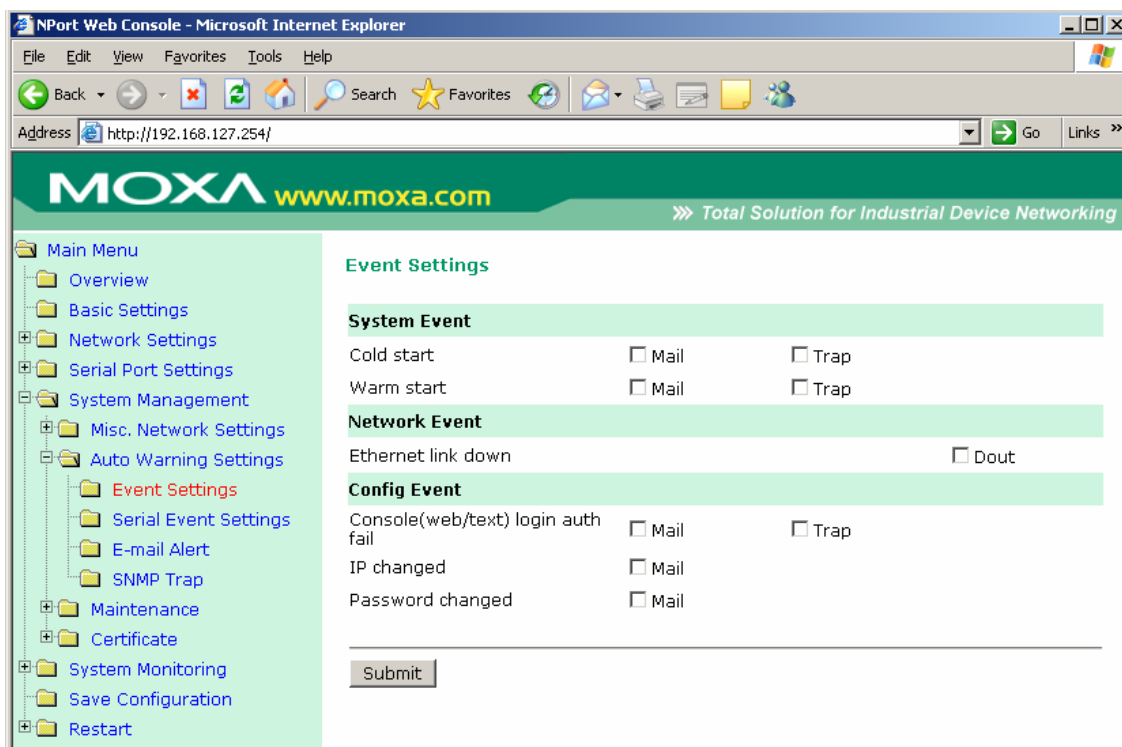
SYSLOG severity

Степень важности сообщения (из списка):

0	Emergency (Крайне важно)
1	Alert (Тревога)
2	Critical (Угроза)
3	Error (ошибка)
4	Warning (Предостережение)
5	Notice (Предупреждение)
6	Informational (Информационное сообщение)
7	Debug (отладка)

Auto Warning Settings (Настройки автооповещения)

Event Settings (настройки событий)



На странице настроек событий можно задать оповещение сетевых администраторов об определенных системных, сетевых событиях и изменениях настроек. Для различных событий доступны различные функции автооповещения, как показано на рисунке выше.

Mail: Электронная почта отправляется на указанный e-mail. **Trap:** это отправка SNMP-прерываний. **Dout** – функция доступна на моделях NPort 6450 и 6650, связана с изменением состояния релейного выхода (разъем DOUT находится на задней стороне NPort'a 6000) и светодиодного индикатора тревоги.

Cold start: Запуск системы из выключенного состояния или после обновления прошивки.

Warm start: Перезапуск NPort'a 6000 без отключения питания.

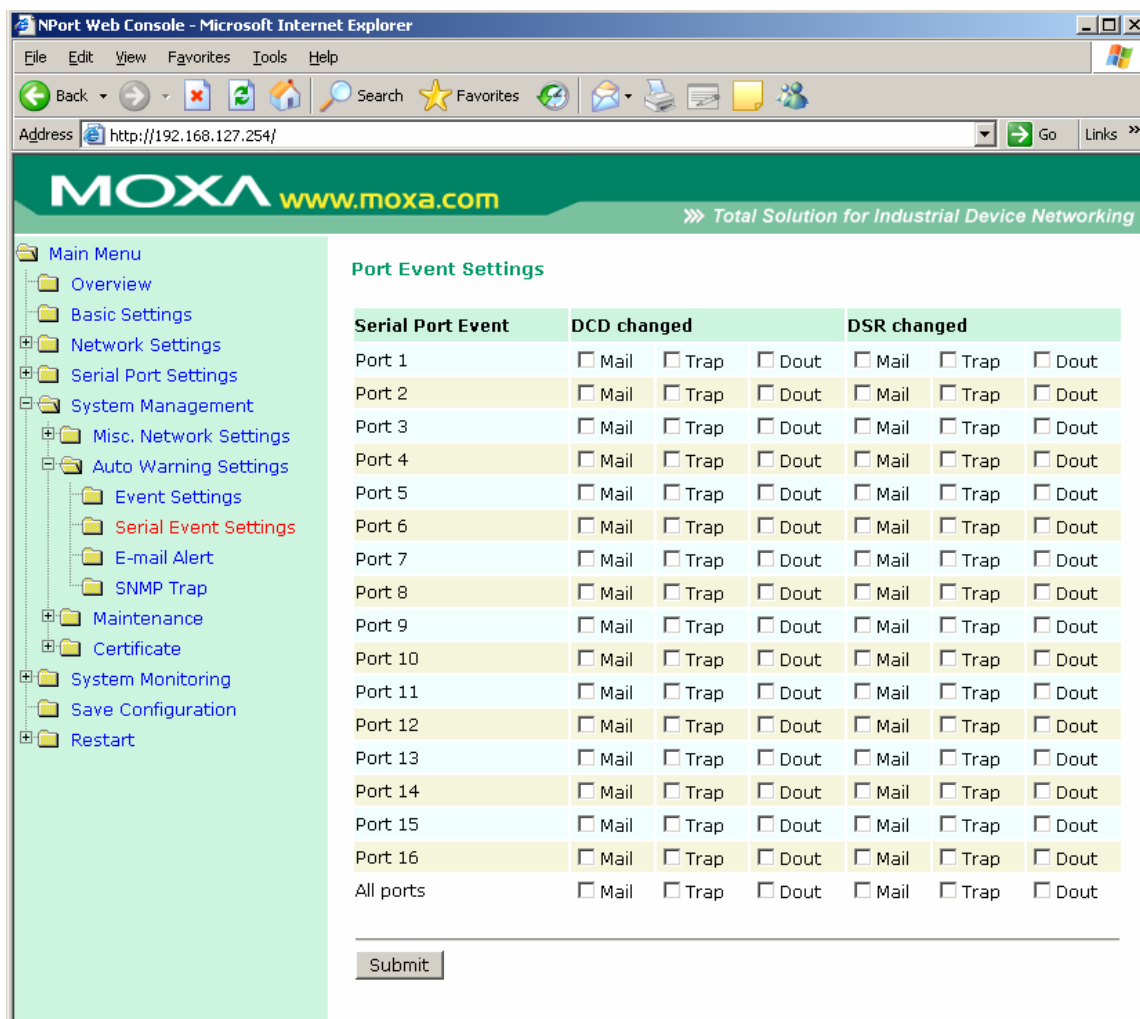
Network Event: Эти настройки доступны на устройствах NPort 6450 и 6650. **Ethernet 1** – это встроенный Ethernet-порт, **Ethernet 2 и 3** – порты дополнительных сетевых модулей. Эти параметры позволяют настроить изменение состояния релейного выхода светодиодного индикатора-аларма NPort'a, когда указанное соединение обрывается.

Console (web/text) login auth fail: Индикация неудачной попытки авторизоваться в консоли NPort'a 6000.

IP changed: Если включена данная функция, то NPort 6000 попытается отправить сообщение по электронной почте перед перезагрузкой с новым IP-адресом. Если NPort'у 6000 не удастся отправить сообщение на почтовый сервер в течение 15 секунд, то в любом случае он перезагрузится с новым IP без отправки оповещения.

Password changed: Если включена данная функция, то NPort 6000 попытается отправить сообщение по электронной почте перед перезагрузкой с новым паролем на вход в консоль. Если NPort'у 6000 не удастся отправить сообщение на почтовый сервер в течение 15 секунд, то он перезагрузится без отправки оповещения.

Serial Event Settings (настройки событий по последовательным портам)



На странице настройки событий по последовательным портам можно настроить оповещения сетевого администратора об изменениях сигналов DCD и DSR последовательных портов. Для различных событий доступны различные функции автооповещения, как показано на рисунке выше. **Mail:** Электронная почта отправляется на указанный e-mail. **Trap:** это отправка SNMP-прерываний. **Dout** – функция доступна на моделях NPort 6450 и 6650, связана с изменением состояния релейного выхода (разъем DOUT находится на задней стороне NPort'a 6000) и светодиодного индикатора тревоги.

DCD changed

Изменение сигнала DCD (обнаружения несущей) сигнализирует об изменении состояния соединения с модемом. Например, если DCD-сигнал перешел в состояние низкого уровня, значит, соединение оборвалось. Когда DCD-сигнал переходит на низкий уровень, NPort 6000 автоматически посылает оповещение сетевому администратору, если эта функция включена на странице настроек событий.

В NPort'ax 6450 и 6650 сброс состояния сработавших реле производит сетевой администратор выбором **Acknowledge Event** (квитировать/подтвердить событие) из консоли NPort'a 6000 или изменением состояния DCD-сигнала.

DSR changed

Изменение уровня DSR (Data Set Ready – сигнал готовности) показывает, что DCE-устройство отключилось. Например, если данный сигнал перешел на низкий уровень, то это означает, что отключено питание модема. В таком случае NPort 6000 автоматически отправит оповещение сетевому администратору, если это настроено на странице событий.

В NPort'ах 6450 и 6650 сброс состояния сработавших реле производит сетевой администратор выбором **Acknowledge Event** (квитировать/подтвердить событие) из консоли NPort'а 6000 или изменением состояния DSR-сигнала. См. также параграф *System Monitoring* (Мониторинг системы) ниже в данной главе.



ВНИМАНИЕ

Состояние сигналов DCD или DSR можно получать по SNMP, но невозможно узнать состояние каждого по отдельности. Изменение любого сигнала с «-» на «+» показывается как «link up» (восстановление соединений), переход с «+» на «-» индицируется как «link down» (потеря связи).

E-mail Alert (оповещения по электронной почте)

The screenshot shows the NPort Web Console interface. The browser window is titled "NPort Web Console - Microsoft Internet Explorer" and the address bar shows "http://192.168.127.254/". The page header features the MOXA logo and the tagline "Total Solution for Industrial Device Networking". The left sidebar contains a navigation menu with "E-mail Alert" selected. The main content area is titled "E-mail Alert" and includes the following fields and options:

- Mail Server Settings**
- Mail server (SMTP)**: [Text input field]
- My server requires authentication
- User name**: [Text input field]
- Password**: [Text input field]
- From e-mail address**: [Text input field]
- To e-mail address 1**: [Text input field]
- To e-mail address 2**: [Text input field]
- To e-mail address 3**: [Text input field]
- To e-mail address 4**: [Text input field]
- Submit**: [Submit button]

Настройки оповещений по электронной почте задают, куда будут приходить соответствующие сообщения. Можно задать до 4-ех адресов-получателей оповещений.



ВНИМАНИЕ

Уточните у Вашего сетевого администратора или провайдера настройки почтовых серверов. Функция автооповещения не будет работать при некорректных настройках почтовых серверов. The NPort 6000's SMTP AUTH поддерживает LOGIN, PLAIN, и CRAM-MD5 (RFC 2554).

Mail server: Доменное имя или IP-адрес почтового сервера.

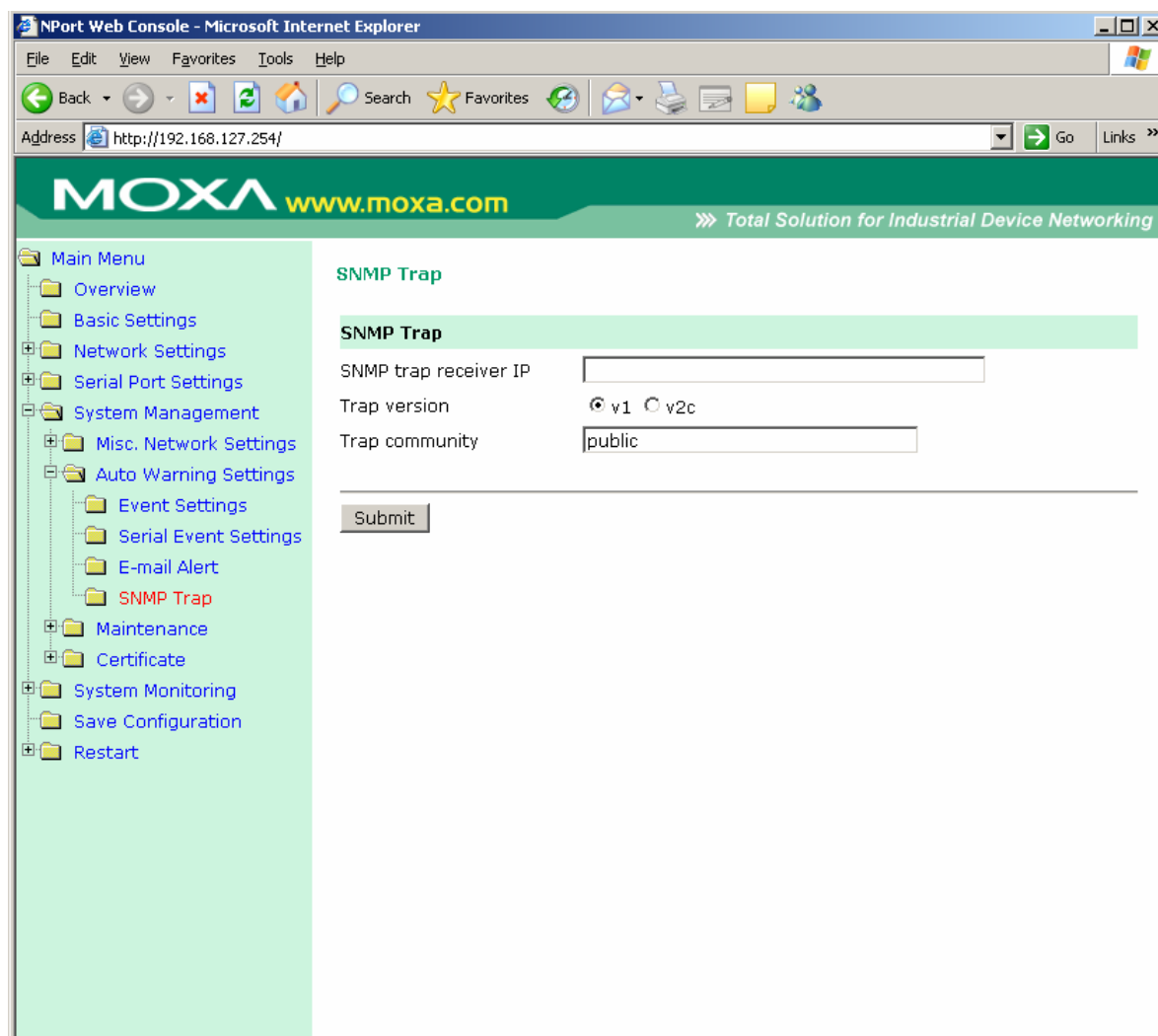
User name: Логин почтового ящика (если требуется).

Password: Пароль почтового ящика (если требуется).

From e-mail address: адрес, с которого будут автоматически отправляться оповещения.

To e-mail address 1 to 4: Один или несколько адресов, на которые будут отправляться автооповещения.

SNMP Trap (прерывания по SNMP)



The screenshot shows a web browser window titled "NPort Web Console - Microsoft Internet Explorer" with the address bar displaying "http://192.168.127.254/". The page header features the Moxa logo and the slogan "Total Solution for Industrial Device Networking". A left-hand navigation menu lists various settings categories, with "SNMP Trap" highlighted in red. The main content area is titled "SNMP Trap" and contains three configuration fields: "SNMP trap receiver IP" (an empty text box), "Trap version" (radio buttons for "v1" and "v2c", with "v1" selected), and "Trap community" (a text box containing the value "public"). A "Submit" button is located below these fields.

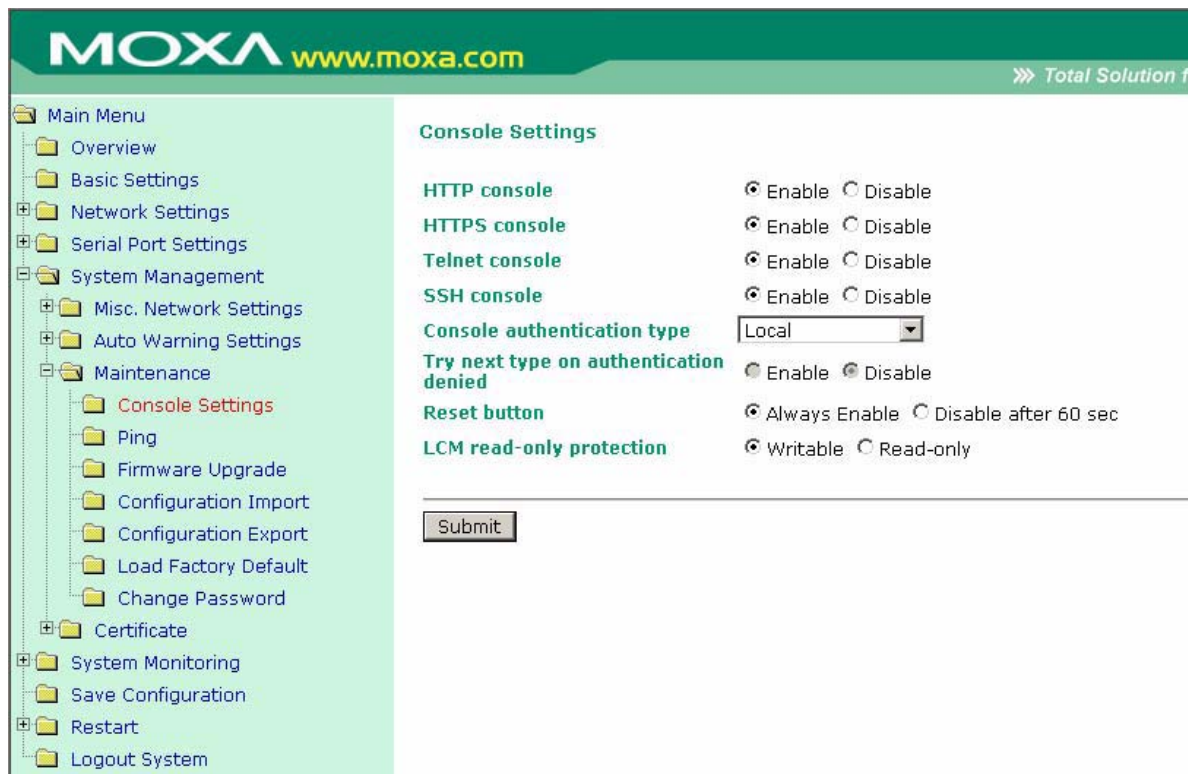
SNMP trap server IP: Данное поле используется для указания IP-адреса получателя SNMP-прерываний.

Trap version (по умолчанию = v2): выбор версии SNMP trap.

Trap community (по умолчанию = public): здесь указывается SNMP-группа.

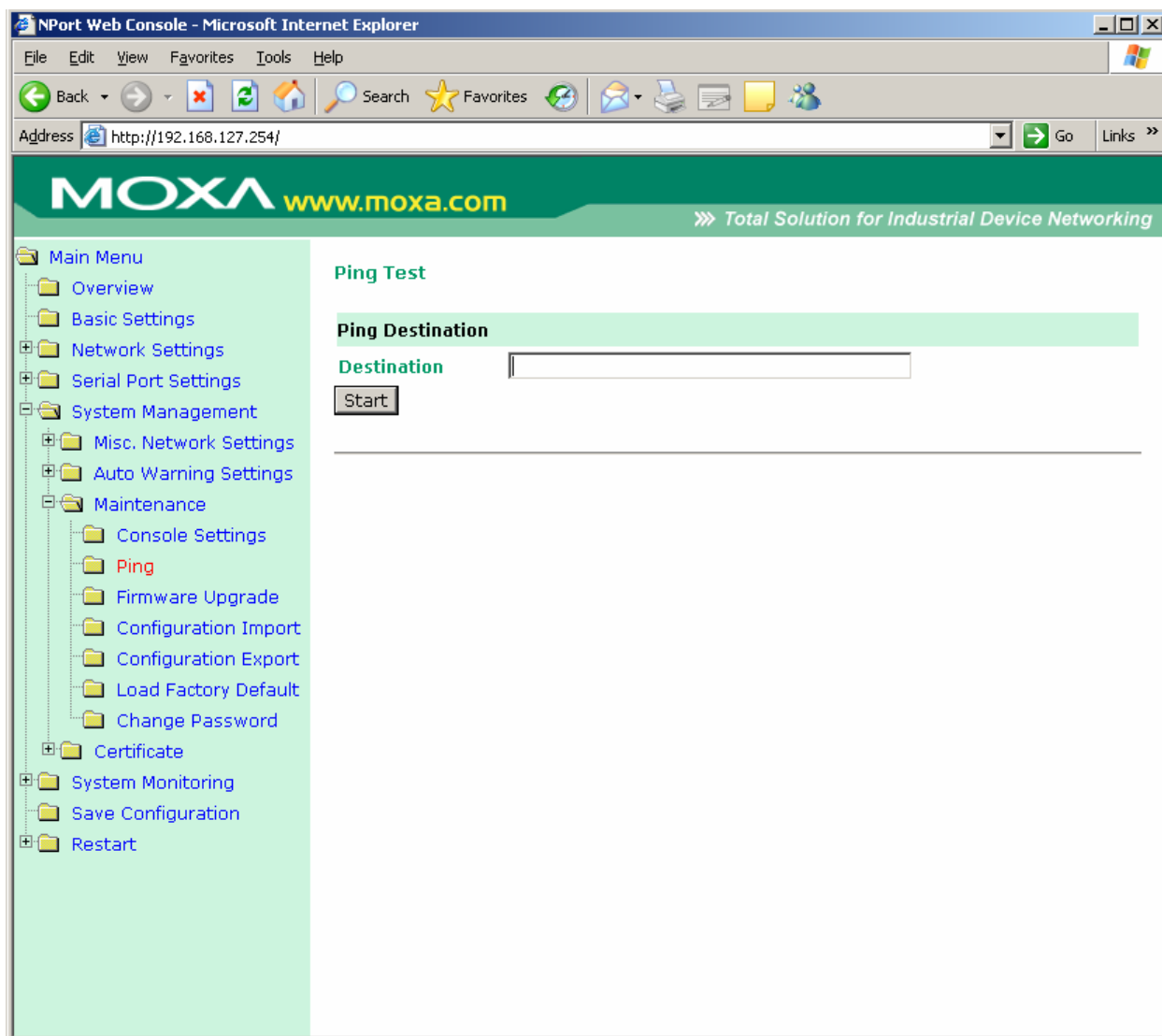
Maintenance (Функции технического обслуживания и диагностики)

Console Setting (консольные настройки)



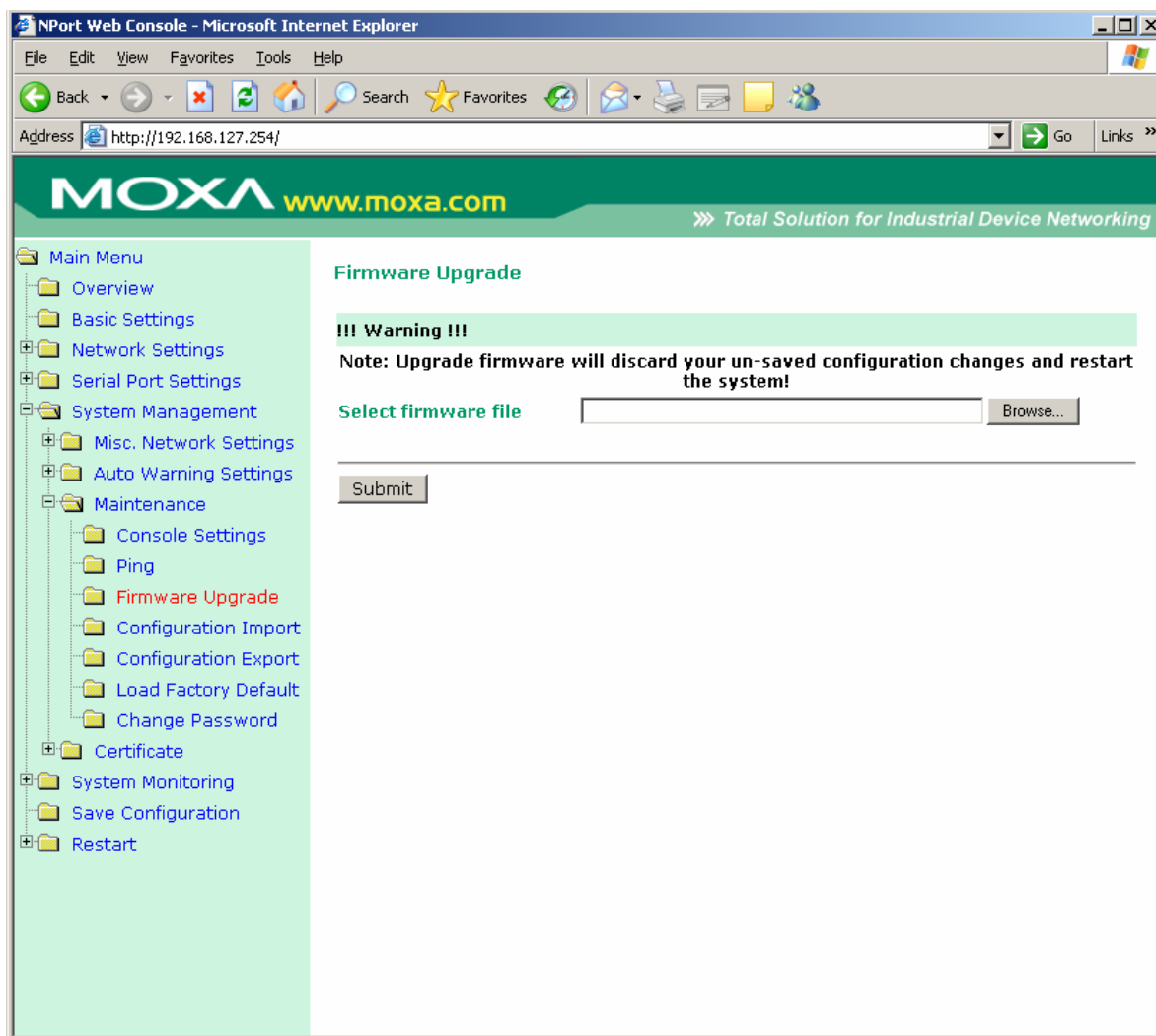
На данной вкладке настроек можно включить или отключить доступ к консоли настроек NPort'a 6000 (HTTP, HTTPS, Telnet, SSH). Также можно настроить возможность доступа из LCM-дисплея для просмотра или изменения настроек. Т.е. дисплей оператора можно будет использовать либо только для проверки настроек (read only), либо для их просмотра и редактирования (writeable). Необходимо помнить, что, если доступ в консоль защищен паролем и для LCM разрешено редактирование (writeable), то необходимо будет ввести пароль при подтверждении любых изменений настроек. См. также параграф Change Password ниже. Можно также активировать/деактивировать кнопку сброса (Reset).

Ping (проверка связи с другими хостами)



Пинговать IP-адреса можно прямо из консоли Nport'a 6000 для проверки Ethernet-соединения. Введите IP-адрес или доменное имя в поле **Destination** для проверки наличия связи с определенным хостом.

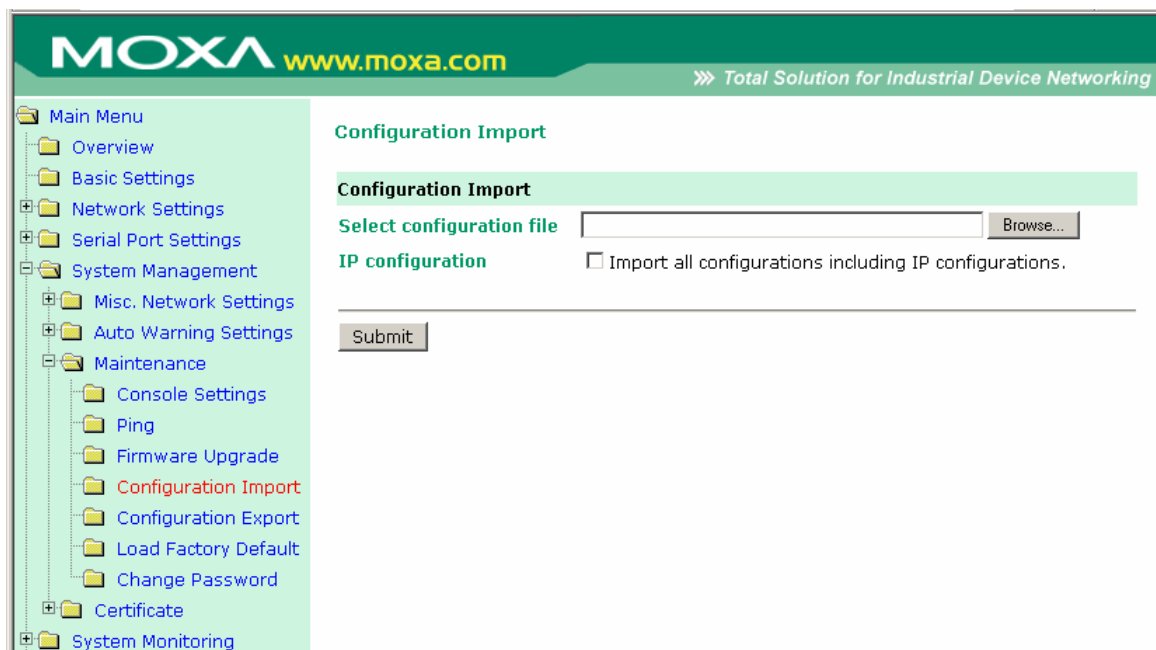
Firmware Upgrade (обновление прошивки)



Прошивку NPort'a 6000 можно обновить через web-консоль, последовательную консоль или через утилиту NPort Search. Если были произведены изменения в настройках, то их нужно сохранить перед обновлением прошивки. См. параграф Save Configuration – о том, как сохранять выполненные настройки. Все несохраненные изменения не вступят в силу после обновления прошивки. Для обновления прошивки укажите имя файла и нажмите **Submit**. Последние версии прошивок всегда можно скачать с сайта www.moxa.com.

Configuration Import/Export (импорт/экспорт настроек)

Для NPort'ов 6000 можно множить одинаковые настройки или восстанавливать конфигурацию с помощью файла, импортируемого с одного устройства на другое.

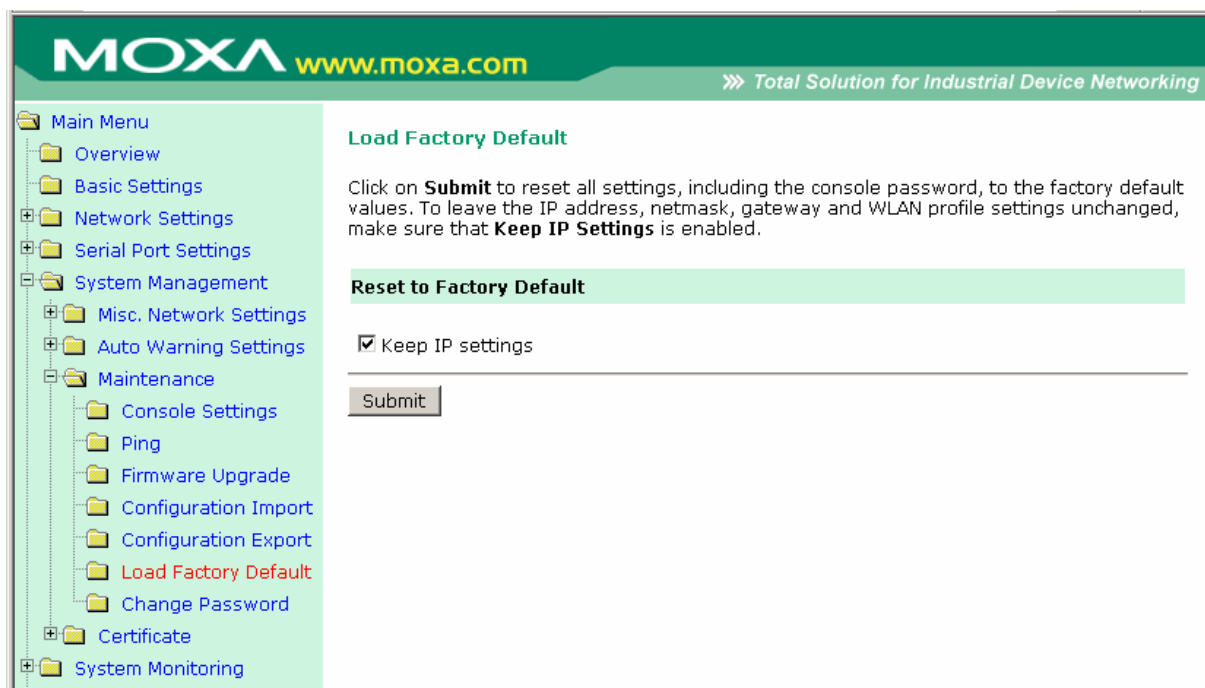


Для импорта конфигурации необходимо зайти на вкладку **System Management** → **Maintenance** → **Configuration Import**. Укажите путь к файлу и нажмите **Submit**. Настройки NPort'a 6000 установятся в соответствии с заданным файлом. Если нужно импортировать и настройки IP-адресов, то отметьте флажок **Import all configurations including IP configurations**.



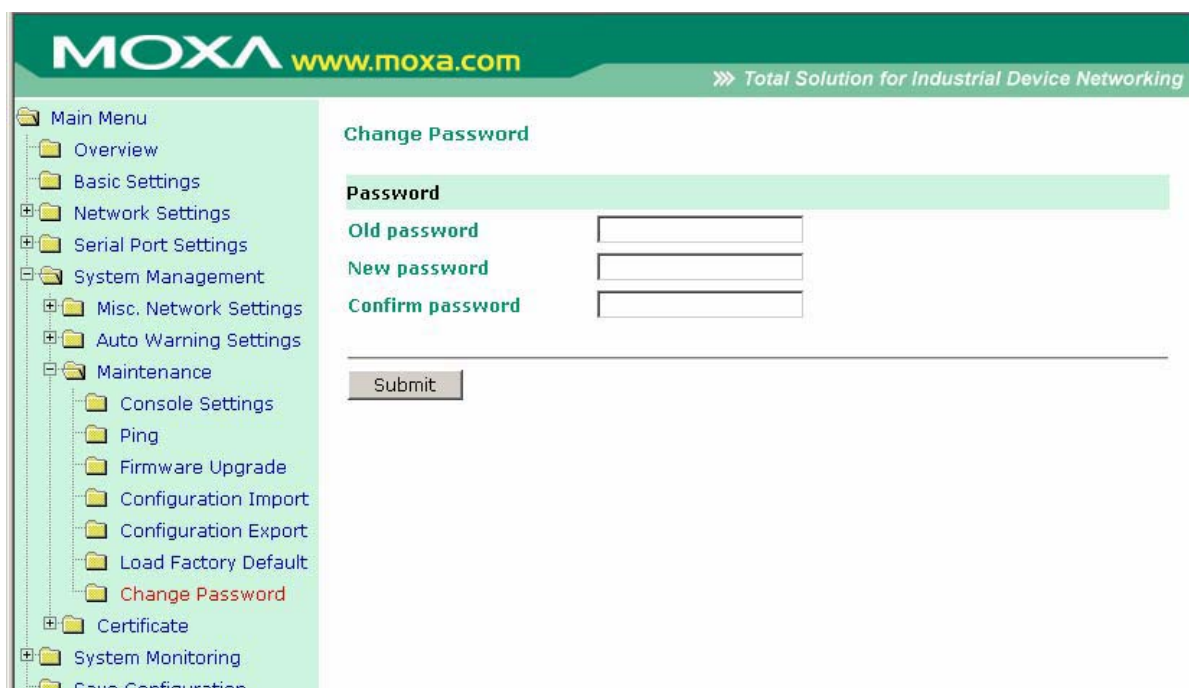
Для экспорта настроек зайдите на вкладку **System Management** → **Maintenance** → **Configuration Export** и нажмите **Download**. Появится стандартное окно загрузки, где нужно выбрать файл и его местонахождение.

Load Factory Defaults (Загрузить заводские настройки)



Данная функция сбрасывает все настройки NPort'a 6000 к заводским значениям по умолчанию. Все предыдущие значения параметров, включая пароль консоли, будут утеряны. Если нужно сохранить сетевые настройки (IP-адресов), то перед загрузкой заводских настроек отметьте флажок **Keep IP settings**.

Change Password (Изменить пароль)



На изменение настроек NPort'a 6000 можно установить пароль. Сначала нужно указать старый пароль (old password) – если установка производится в первый раз, оставьте это поле незаполненным. Для задания нового пароля или изменения существующего введите новое значение в **New Password** и подтвердите его в **Confirm password**. Для снятия парольной защиты оставьте пустыми поля **New Password** и **Confirm password**.



ВНИМАНИЕ

Если старый пароль утерян или забыт, единственный способ получить доступ к NPort'у 6000 – использовать кнопку сброса Reset, загружающую заводские настройки.

Перед установкой пароля в первый раз хороший способ – создать файл экспорта полностью выполненных настроек NPort'a 6000. В этом случае конфигурацию достаточно просто можно восстановить при необходимости сброса к заводским настройкам в случае утери пароля или др. См. также параграф Configuration Import/Export ранее в данной главе.

Certificate

Ethernet SSL Certificate Import

The screenshot shows the Moxa web interface. The top header includes the Moxa logo and website URL (www.moxa.com) along with the tagline 'Total Solution for Industrial Device Networking'. A left sidebar contains a navigation menu with categories like Main Menu, Overview, Basic Settings, Network Settings, Serial Port Settings, System Management, System Monitoring, Save Configuration, and Restart. Under System Management, the 'Certificate' folder is expanded, showing 'Ethernet SSL Certificate' (highlighted in red) and 'Certificate/Key Delete'. The main content area is titled 'Ethernet SSL Certificate Import'. It features an 'Installed Certificate' section with a table showing 'Issued to' and 'Issued by' as 192.168.127.254, and 'Valid' from 2027/4/3 to 2037/4/2. Below this is a 'Select SSL certificate/key file' section with a text input field and a 'Browse...' button. A 'Submit' button is located at the bottom of the form.

Certificate/Key Delete

The screenshot shows the Moxa web interface for the 'Certificate/Key Delete' page. The layout is consistent with the previous screenshot, including the Moxa header and the left navigation sidebar. In the main content area, the title is 'Certificate/Key Delete'. Below the title, there is a section for 'SSL certificate' with two radio button options: 'Delete' and 'Keep', where 'Keep' is selected. A 'Submit' button is positioned below the options.

System Monitoring

Serial to Network Connections (Соединения между последовательными и Ethernet-портами)

В меню **Serial Status** зайдите на вкладку **Serial to Network Connections** для просмотра режима работы и состояния каждого соединения для каждого последовательного порта. Все функции мониторинга обновляются каждые 5 секунд.

The screenshot shows the MOXA web interface. The top header includes the MOXA logo and the website URL www.moxa.com. Below the header is a navigation menu on the left with categories like Main Menu, System Management, System Monitoring, and System Status. The 'Serial Status' menu item is expanded, showing 'Serial to Network Connections' as the selected option. The main content area displays a table titled 'Serial to Network Connections' with columns for 'Port', 'OP Mode', and 'Connections'. The table lists 13 ports, all with 'Device Control/RealCOM' as the operating mode. The 'Connections' column contains empty brackets for each row.

Port	OP Mode	Connections
1	Device Control/RealCOM	[] [] []
2	Device Control/RealCOM	[] [] []
3	Device Control/RealCOM	[] [] []
4	Device Control/RealCOM	[] [] []
5	Device Control/RealCOM	[] [] []
6	Device Control/RealCOM	[] [] []
7	Device Control/RealCOM	[] [] []
8	Device Control/RealCOM	[] [] []
9	Device Control/RealCOM	[] [] []
10	Device Control/RealCOM	[] [] []
11	Device Control/RealCOM	[] [] []
12	Device Control/RealCOM	[] [] []
13	Device Control/RealCOM	[] [] []

Serial Port Status (Состояние последовательного порта)

На вкладке **Serial Port Status** можно посмотреть состояние каждого последовательного порта. В столбце **Buffering** показывается число байт буфера, используемое каждым последовательным портом.

Port	TxCnt	RxCnt	TxTotalCnt	RxTotalCnt	DSR	DTR	RTS	CTS	DCD	Buffering
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0

Serial Port Error Count (счетчик ошибок последовательных портов)

Для просмотра количества ошибок на каждом последовательном порту зайдите на вкладку **Serial Port Error Count**.

Port	ErrCnt			
	Frame	Parity	Overrun	Break
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0

Frame: Ошибка кадра; показывает, что в принятом символе отсутствовал корректный стоповый бит.

Parity: Ошибка контроля четности; показывает, что принятый символ имеет ошибку проверки четности.

Overrun: NPort не успевает сохранять принимаемые данные в аппаратном буфере, поскольку скорость входного потока превосходит скорость обработки данных NPort'ом.

Break: Прерванная передача; показывает, что принимаемый поток данных передавался дольше длительности одного полного слова. Время слова определяется как общее время для передачи стартового бита, бита данных, паритета и стопового.

Serial Port Settings (Параметры последовательной связи)

Для просмотра сводной таблицы настроек последовательных портов зайдите на вкладку **Serial Port Settings**.

The screenshot shows the MOXA web interface with the 'Serial Port Settings' page selected. The table lists 16 serial ports with their respective configurations.

Port	Baud Rate	Data Bits	Stop Bits	Parity	Flow Control			FIFO	Interface
					RTS/CTS	XON/XOFF	DTR/DSR		
1	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
2	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
3	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
4	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
5	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
6	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
7	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
8	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
9	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
10	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
11	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
12	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
13	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
14	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
15	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
16	115200	8	1	None	ON	OFF	OFF	Enable	RS-232

Serial Cipher Usage Status (статус использования последовательного шифра)

Serial Status → Cipher Usage Status

The screenshot shows the MOXA web interface with the 'Cipher Usage Status' page selected. The table lists 16 serial ports and their cipher usage status.

Port	OP Mode	Connections	Cipher
1	Device Control/RealCOM		
2	Device Control/RealCOM		
3	Device Control/RealCOM		
4	Device Control/RealCOM		
5	Device Control/RealCOM		
6	Device Control/RealCOM		
7	Device Control/RealCOM		
8	Device Control/RealCOM		
9	Device Control/RealCOM		
10	Device Control/RealCOM		
11	Device Control/RealCOM		
12	Device Control/RealCOM		
13	Device Control/RealCOM		
14	Device Control/RealCOM		
15	Device Control/RealCOM		
16	Device Control/RealCOM		

Просмотр шифра и состояния соединения каждого порта. Зависит от настроек Cipher Settings

Network Connections (Ethernet-соединения)

Для просмотра сетевых соединений зайдите на вкладку **Network Connections**.

MOXA www.moxa.com Total Solution for Industrial Device Networking

Network Connections

Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	192.168.127.254:8000	*:*	LISTEN
TCP	0	0	192.168.127.254:4900	*:*	LISTEN
TCP	0	0	192.168.127.254:14900	*:*	LISTEN
TCP	0	0	192.168.127.254:80	*:*	LISTEN
TCP	0	0	192.168.127.254:443	*:*	LISTEN
TCP	0	0	192.168.127.254:23	*:*	LISTEN
TCP	0	0	192.168.127.254:22	*:*	LISTEN
TCP	0	0	192.168.127.254:950	*:*	LISTEN
TCP	0	0	192.168.127.254:951	*:*	LISTEN
TCP	0	0	192.168.127.254:952	*:*	LISTEN
TCP	0	0	192.168.127.254:953	*:*	LISTEN
TCP	0	0	192.168.127.254:954	*:*	LISTEN
TCP	0	0	192.168.127.254:955	*:*	LISTEN
TCP	0	0	192.168.127.254:956	*:*	LISTEN
TCP	0	0	192.168.127.254:957	*:*	LISTEN
TCP	0	0	192.168.127.254:958	*:*	LISTEN
TCP	0	0	192.168.127.254:959	*:*	LISTEN
TCP	0	0	192.168.127.254:960	*:*	LISTEN
TCP	0	0	192.168.127.254:961	*:*	LISTEN
TCP	0	0	192.168.127.254:962	*:*	LISTEN
TCP	0	0	192.168.127.254:963	*:*	LISTEN
TCP	0	0	192.168.127.254:964	*:*	LISTEN
TCP	0	0	192.168.127.254:965	*:*	LISTEN
TCP	0	0	192.168.127.254:966	*:*	LISTEN
TCP	0	0	192.168.127.254:967	*:*	LISTEN
TCP	0	0	192.168.127.254:968	*:*	LISTEN
TCP	0	0	192.168.127.254:969	*:*	LISTEN
TCP	0	0	192.168.127.254:970	*:*	LISTEN

System Monitor/System Status/Network Module

MOXA www.moxa.com

Network Redundancy

Auto refresh

Redundancy Protocol Turbo Ring V2

Status Break

Master/Slave Slave

1st Redundant Port Status (Port1) Forwarding

2nd Redundant Port Status (Port2) Link down

Проверьте сведения и состояние дополнительных сетевых модулей, вставленных в NPort 6000.

Auto Refresh:

По умолчанию (включено): обновление состояния каждые 5 секунд.

Redundancy Protocol:

Показывает используемые протоколы резервирования: Turbo Ring, Turbo Ring v2, RSTP или ни один из них.

Status:

Здесь отображается слово **Healthy** при нормальном функционировании кольца и **Break** – в противном случае (когда активен резервный сегмент кольца).

Master/Slave:

Показывает, является ли NPort 6000 мастером кольца. (Это параметр активен в случае использования Turbo Ring или Turbo Ring v2).



ВНИМАНИЕ

Пользователю не обязательно самому назначать мастера Turbo Ring. Если мастер не назначен, то он устанавливается автоматически из числа коммутаторов EDS. Нужен он только для определения блокируемого сегмента, который будет использоваться в качестве резервного пути передачи данных.

1 st Redundant Port Status (Port 1) – состояние соединения по первому порту резервного кольца

2 st Redundant Port Status (Port 2) – состояние соединения по второму порту резервного кольца.

Forwading свидетельствует о нормальной передаче данных, **Blocking** показывает, что данный порт относится к заблокированной резервной линии, **Link down** индицирует отсутствие связи.

Network Statistics

Для мониторинга сетевой статистики зайдите на вкладку **Network Statistics**.

MOXA www.moxa.com »» Total Solution for Industrial Device Networking

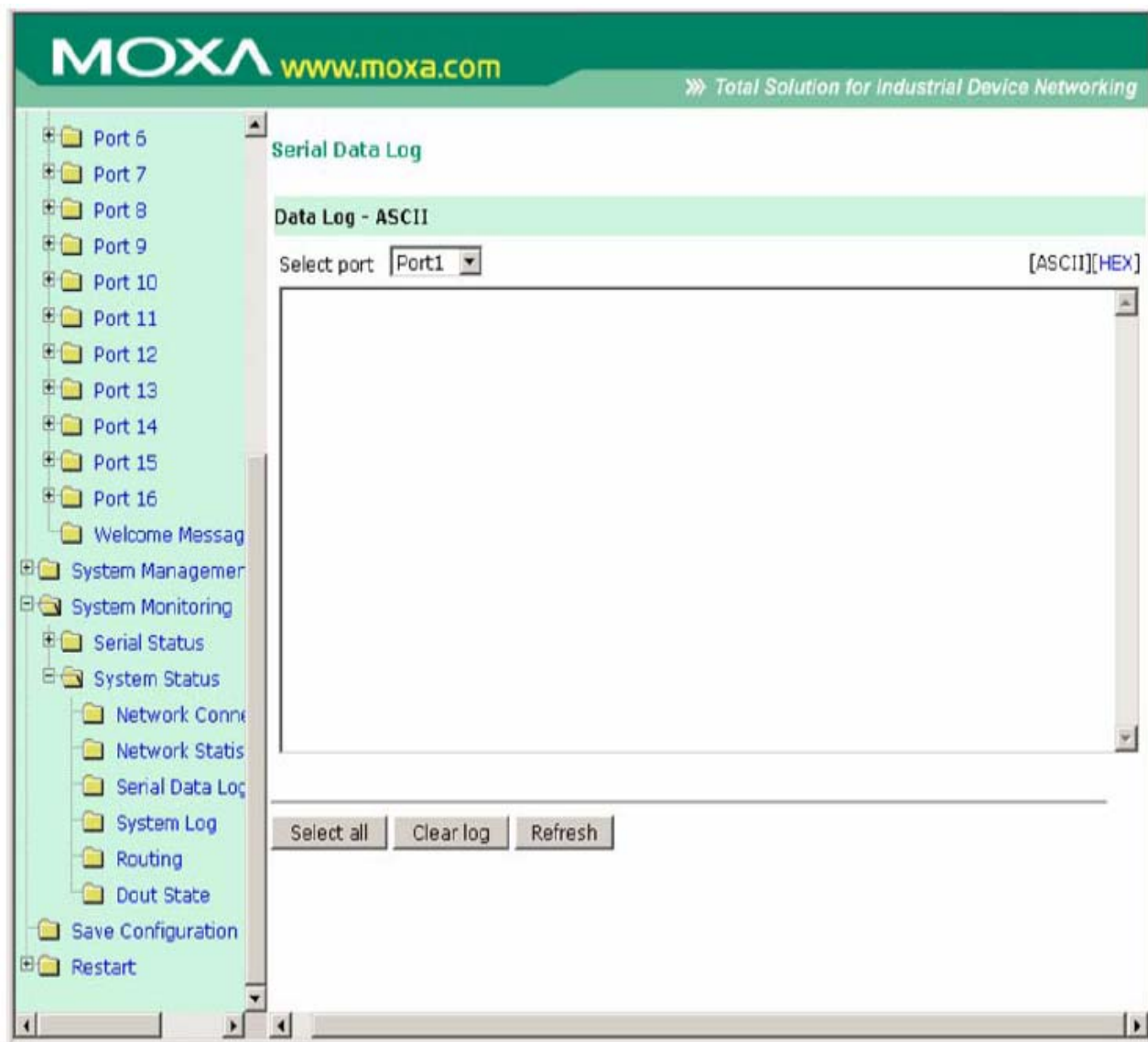
- Port 6
- Port 7
- Port 8
- Port 9
- Port 10
- Port 11
- Port 12
- Port 13
- Port 14
- Port 15
- Port 16
- Welcome Message
- System Management
- System Monitoring
 - Serial Status
 - System Status
 - Network Connecti
 - Network Statistics**
 - Serial Data Log
 - System Log
 - Routing
 - Dout State
- Save Configuration
- Restart

Network Statistics

ETHERNET	Received	235		Sent	321
PPP	Received	0		Sent	0
	RDiscard	0	ErrSum 0	SDiscard	0
IP	Received	226		Sent	310
	RDiscard	0	SNoRoute 0	SDiscard	0
	ErrHeader	0	ErrProto 0	ErrAddr	0
ICMP	Received	0		Sent	0
	REchoReq	0		SEchoReq	0
	REchoRply	0		SEchoRply	0
UDP	Received	52		Sent	9
	ErrHeader	0	ErrPorts 0		
TCP	Received	169		Sent	299
	ErrHeader	0	ErrPorts 0	ReSent	2
	CurrEstab	1	Opens 10		

Serial Data Log

Записи данных для каждого последовательного порта можно просмотреть в формате ASCII или 16-ричном (HEX). После выбора последовательного порта и формата можно нажать кнопку **Select All** для просмотра целиком всей записи, если нужно копировать и вставить ее содержимое в текстовый файл.



System Log

Данная функция отображает записи о системных событиях. Можно нажать кнопку **Select All** для просмотра целиком всей записи, если нужно копировать и вставить ее содержимое в текстовый файл.

System Log

System Log

```
2008/03/26 07:00:21 [System ] System Cold Start
2008/03/26 07:00:47 [Network] Ethernet1 Link Down
2008/03/26 07:01:20 [Config ] Config Changed
2008/03/26 07:01:28 [System ] System Warm Start
2008/03/26 07:02:08 [Config ] Config Changed
2008/03/26 07:02:17 [System ] System Warm Start
2008/03/26 07:02:33 [Network] Get IP Fail (IPv6)
```

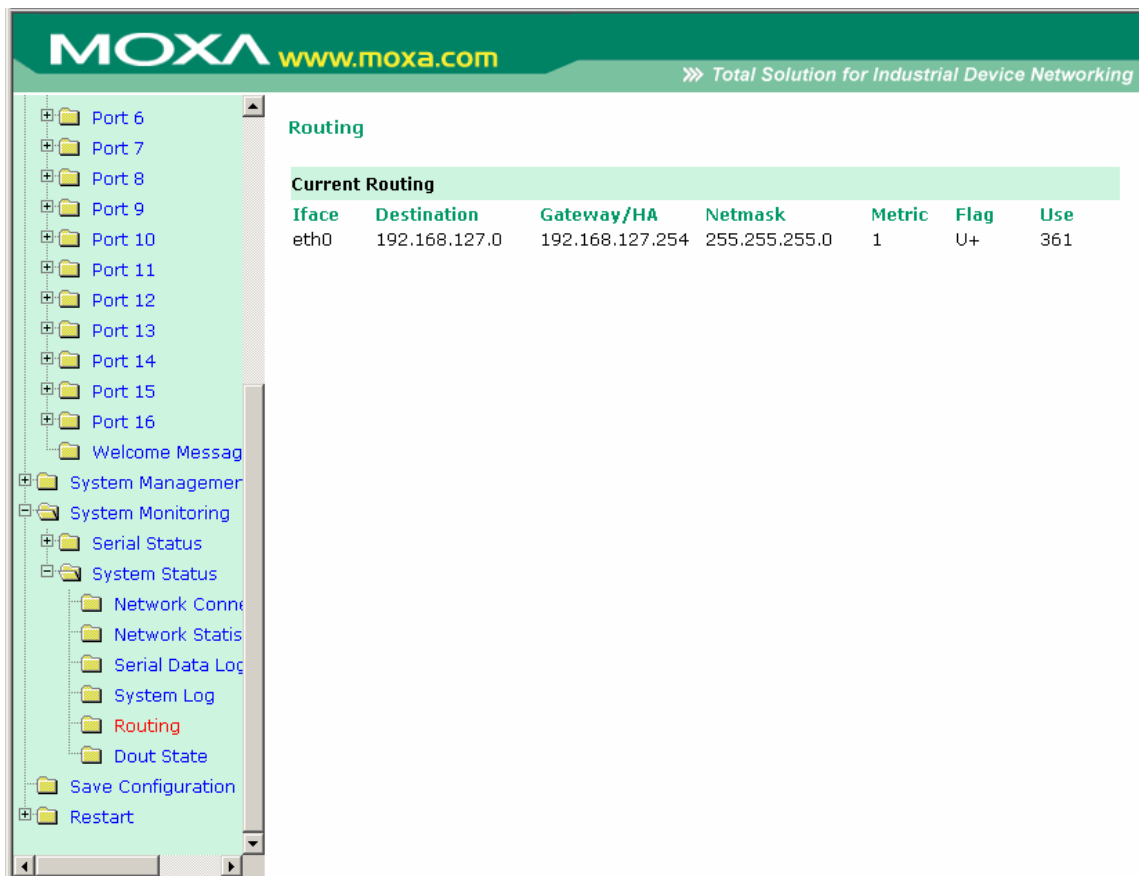
Select all

Clear log

Refresh

Routing

На данной вкладке отображается информация о маршрутизации.



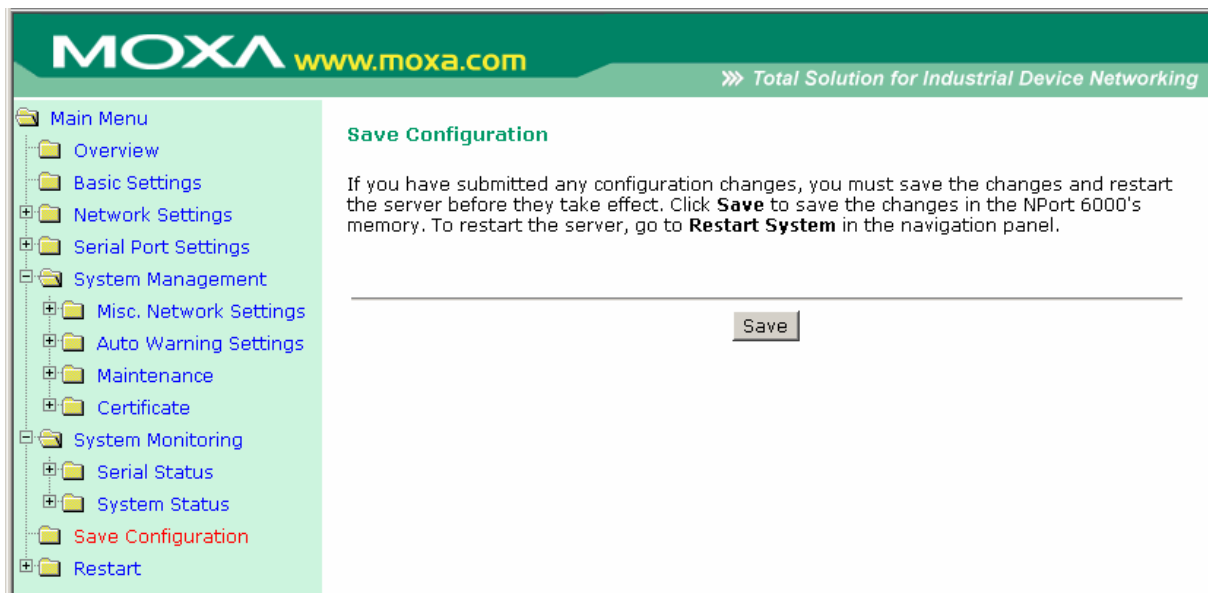
Dout State (для 6450/6650)

Dout State – это состояние выходного реле, состояние которого изменяется в зависимости от возникновения определенных системных событий через настройки **Auto Warning Settings** в меню **System Management**. Можно выбрать пункт меню Dout State для отображения списка событий, которые могут вызывать изменение состояния релейного выхода.



Save Configuration (Сохранение настроек)

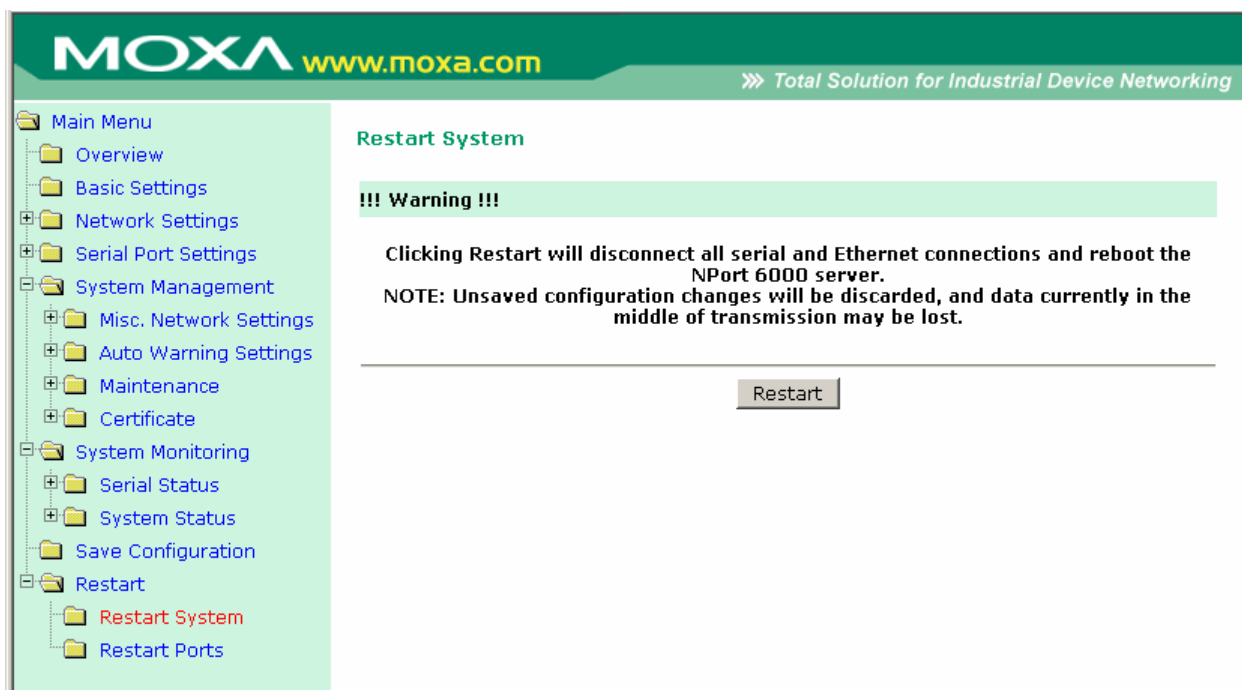
Для сохранения подтвержденных (submit) настроек во флэш-памяти NPort'a 6000 зайдите в пункт **Save Configuration** и нажмите кнопку **Save**. Изменения настроек вступят в силу только после перезагрузки NPort'a 6000. Если изменения не были сохранены до перезагрузки, то они пропадут.



Restart (Перезапуск)

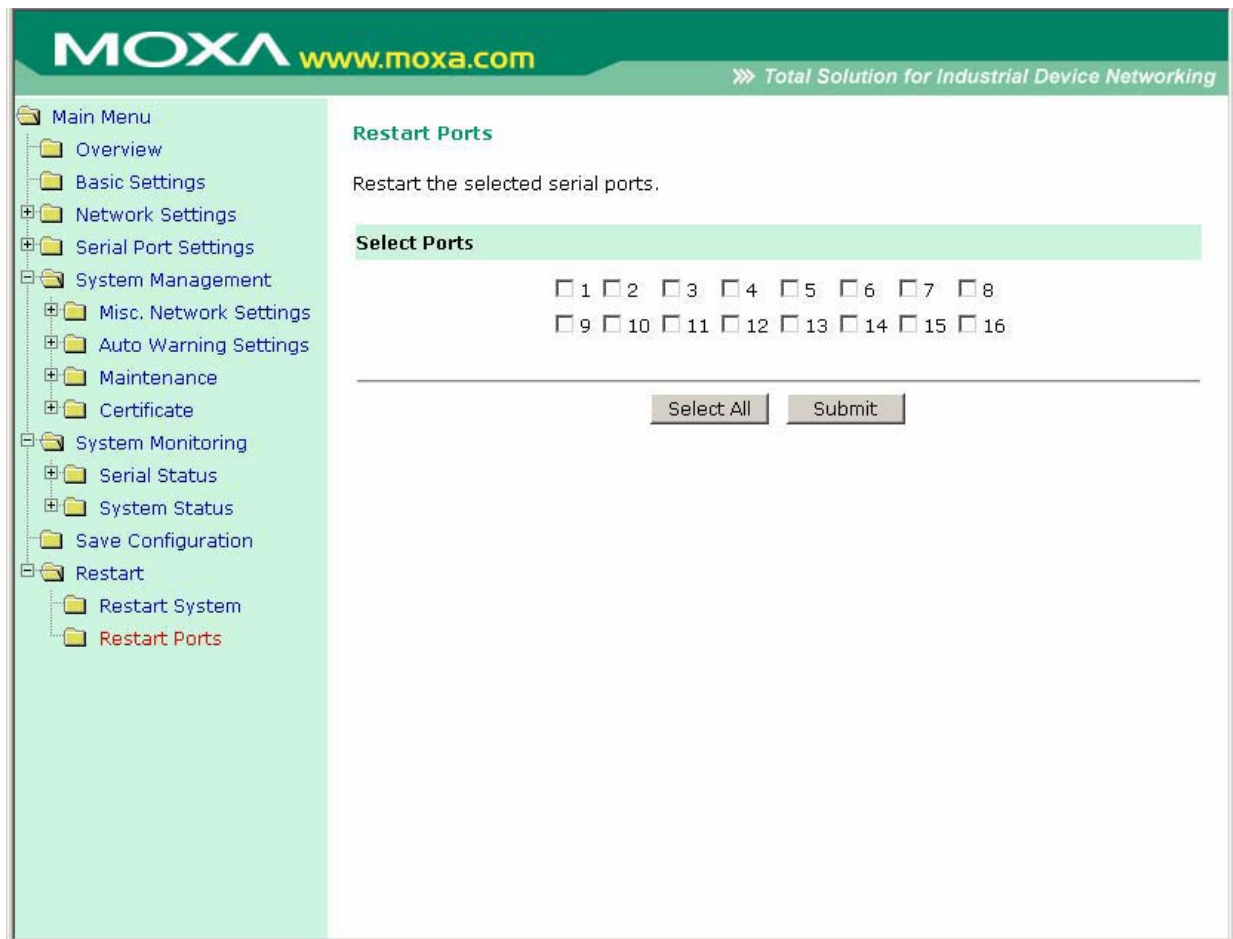
Restart System (Перезапуск системы)

Для перезагрузки Nport'a 6000 войдите на вкладку **Restart System** и нажмите кнопку **Restart**. Перед перезагрузкой убедитесь, что сохранены все необходимые изменения настроек.



Restart Ports (Перезагрузка портов)

Выберите пункт меню **Restart Ports** и затем укажите порты, которые нужно перезагрузить. Щелкните **Select All** для выделения всех портов. После этого нажмите **Submit**.



10 Установка/настройка программного обеспечения

Данная глава содержит следующие разделы:

- Обзор

- **NPort Windows Driver Manager**
 - Установка утилиты
 - Работа с утилитой
- **NPort Search Utility**
 - Установка утилиты
 - Настройка
- **Linux Real TTY Drivers**
 - Основная последовательность действий
 - Аппаратная установка
 - Установка файлов Linux Real TTY Driver
 - Создание TTY-портов
 - Удаление TTY-портов
 - Удаление файлов Linux Real TTY Driver
- **Unix Fixed TTY Driver**
 - Установка Unix Driver
 - Настройка Unix Driver

Обзор

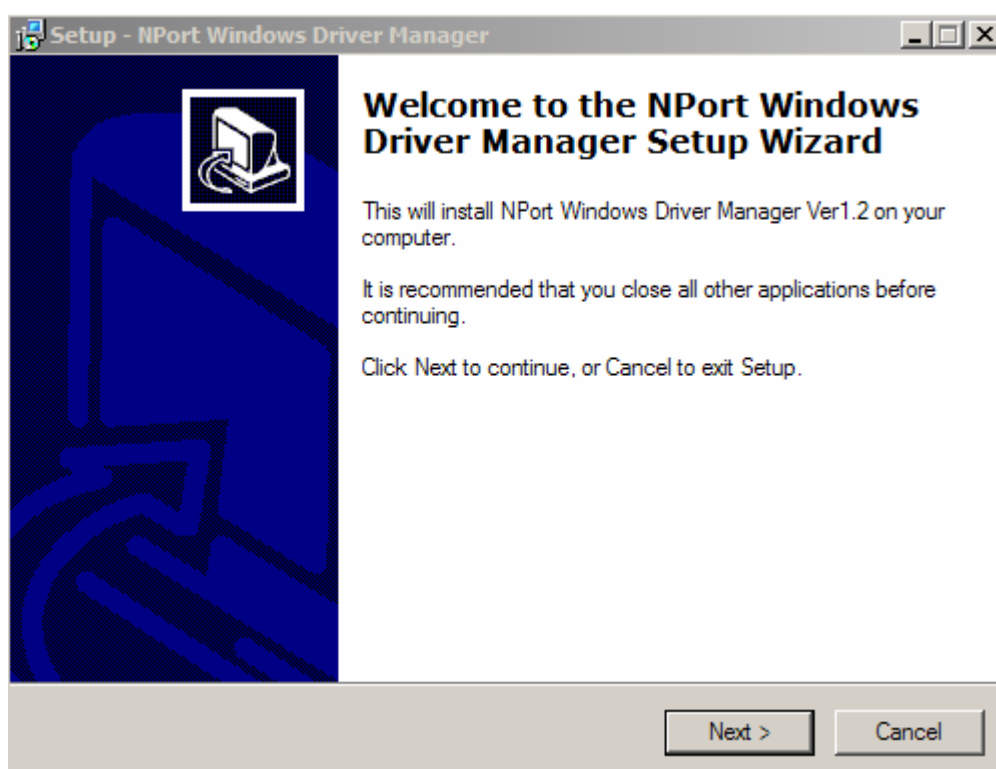
Компакт-диск с документацией и утилитами поставляется в комплекте с NPort'ом 6000. На данном CD имеется утилита NPort Windows Driver Manager (для создания виртуальных СОМ-портов), NPort Search Utility (для ширококвещательного поиска всех NPort'ов 6000 доступных в сети), Руководство пользователя NPort'a 6000 и утилита для обновления прошивки устройства.

NPort Windows Driver Manager

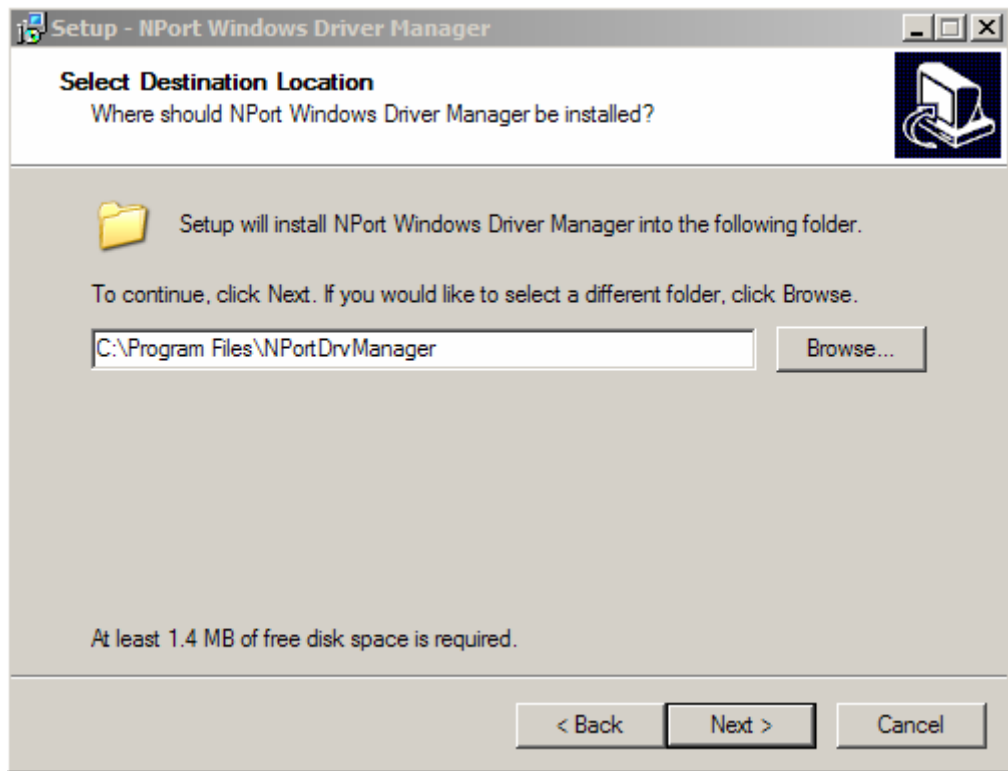
Установка утилиты

Данная утилита предназначена для работы с COM-портами NPort'a 6000, настроенными в режиме работы Real COM. Эта программа устанавливает драйверы, и позволяет назначать свободные номера COM-портов ПК последовательным портам NPort'a 6000. Драйверы можно использовать в ОС Windows 98/ME/2000/XP/2003. После того, как установлены и настроены драйверы, с устройствами, подключенными к последовательным портам NPort'a 6000, можно работать так, как будто они подключены к обычным COM-портам ПК.

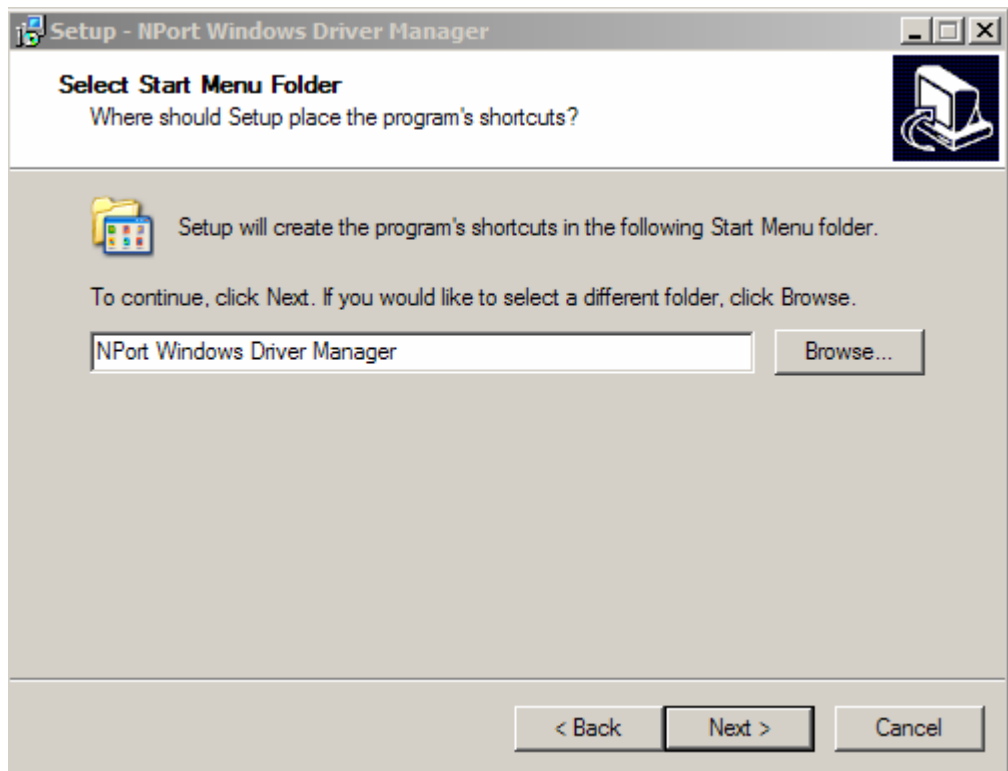
1. Щелкните на кнопке **INSTALL COM Driver** окна автозапуска CD для установки утилиты NPort Windows Driver Manager. Для продолжения установки в появившемся окне нажмите **Yes**.
2. Щелкните **Next** в приветственном окне для продолжения установки.



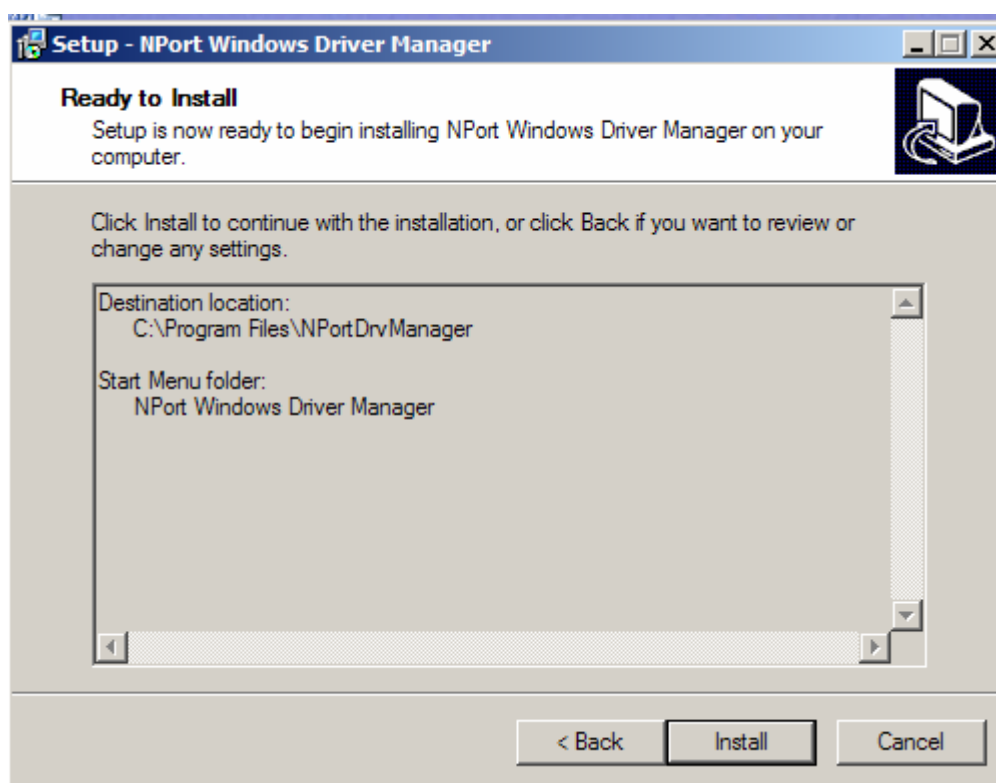
Щелкните **Next** для установки файлов приложения в папку по умолчанию или кнопку **Browse** для выбора другой директории.



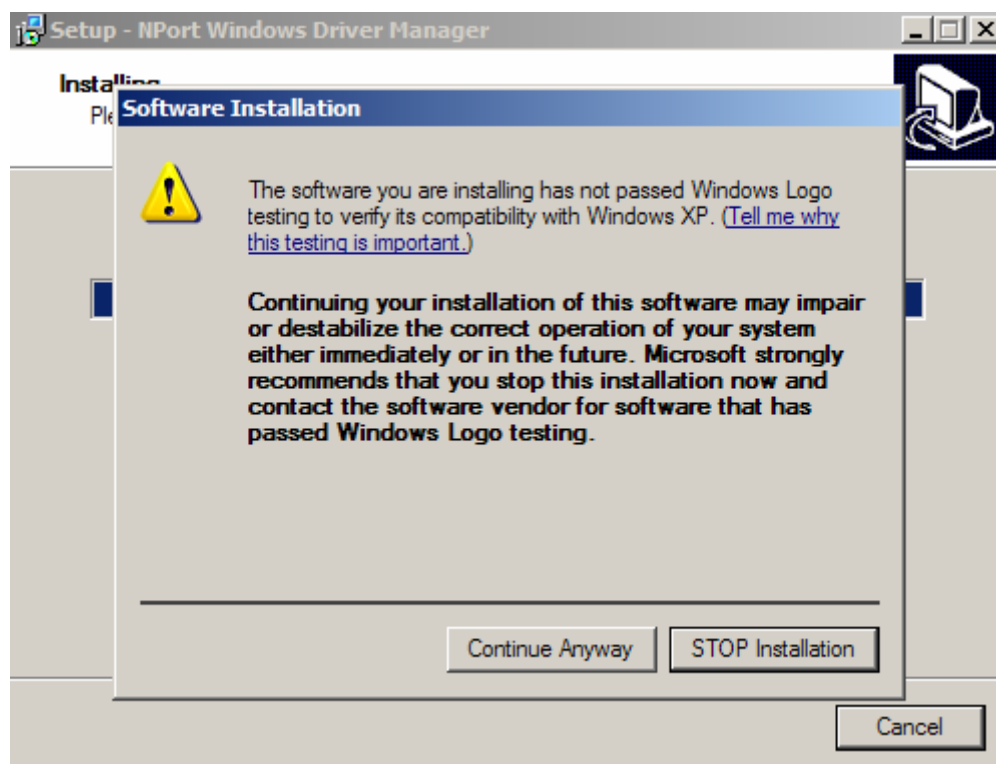
3. Нажмите **Next** для установки в папку с указанным названием.



4. Нажмите **Next** для продолжения установки. Программа установки выведет основные параметры установки.

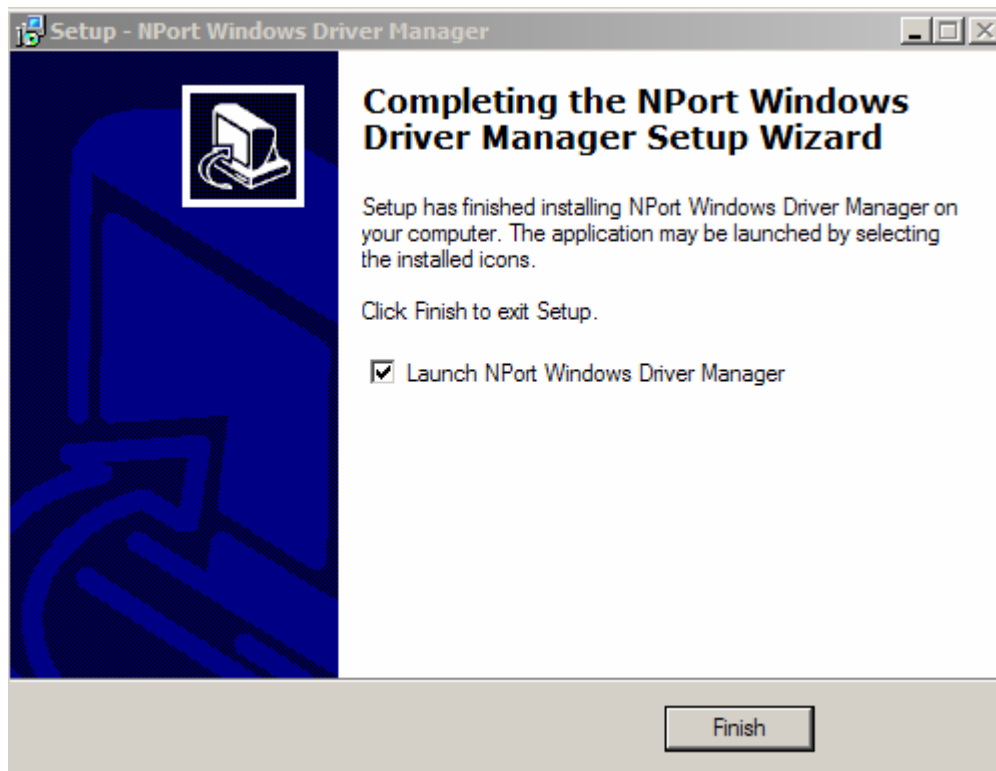


5. Нажмите **Install** для начала установки. Окно установки показывает ход процесса. Для изменения параметров установки кликните **Back** и перейдите в предыдущее окно. В системе Windows XP программа установки покажет сообщение, что ПО не прошло тестирование на совместимость с Windows:



Для завершения установки нажмите кнопку **Continue Anyway**.

6. Нажмите Finish для завершения установки утилиты NPort Windows Driver Manager.

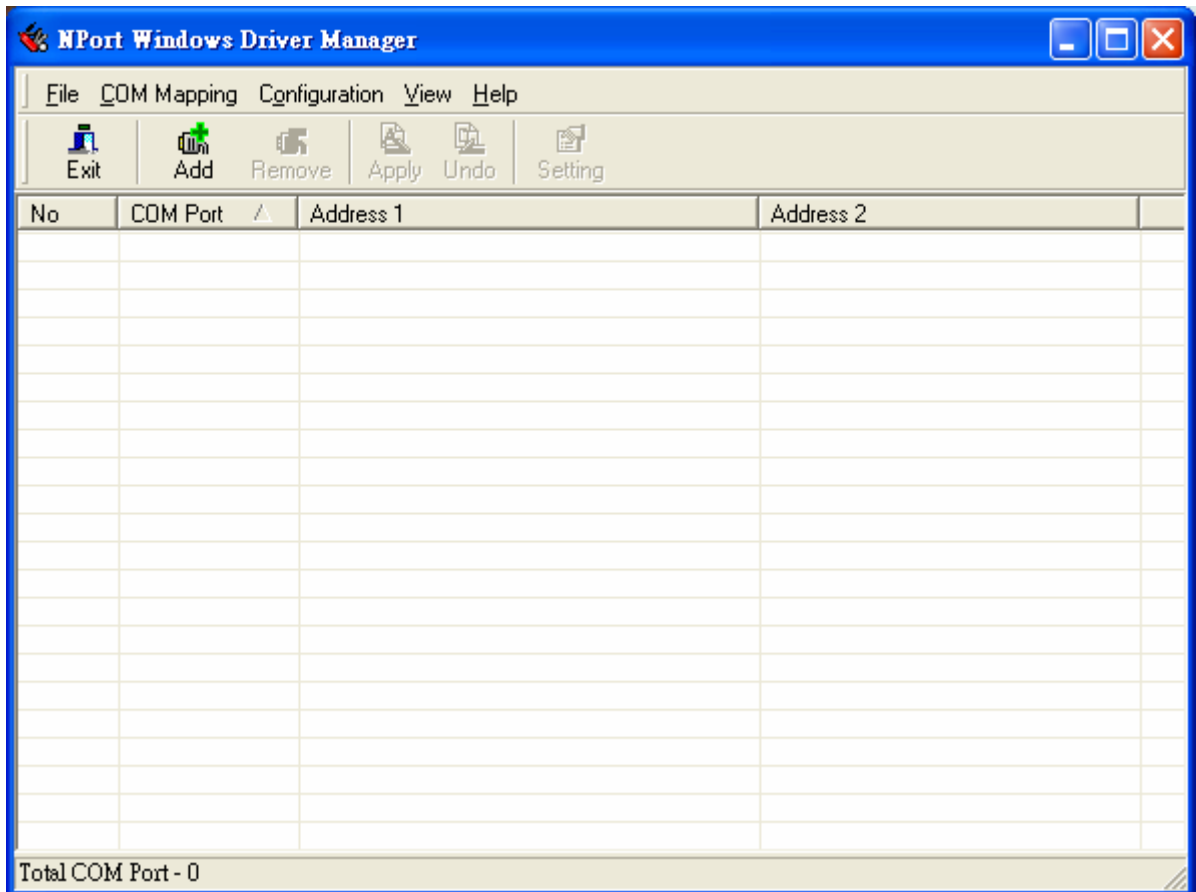


Работа с утилитой

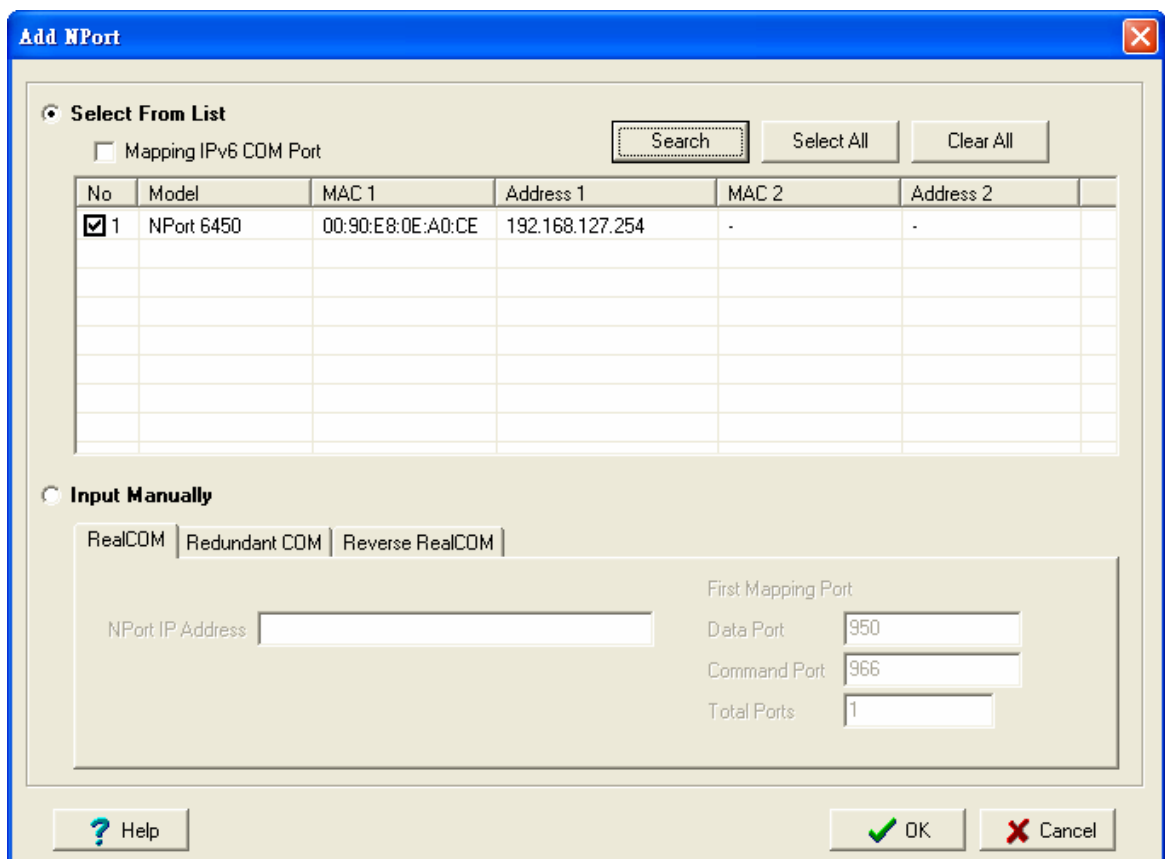
Режим Real COM

После того, как установлена утилита NPort Windows Driver Manager, можно настроить последовательные порты NPort'а 6000 в качестве удаленных COM-портов компьютера. При создании виртуальных COM-портов убедитесь, что соответствующие последовательные порты NPort'а 6000 настроены в режиме Real COM.

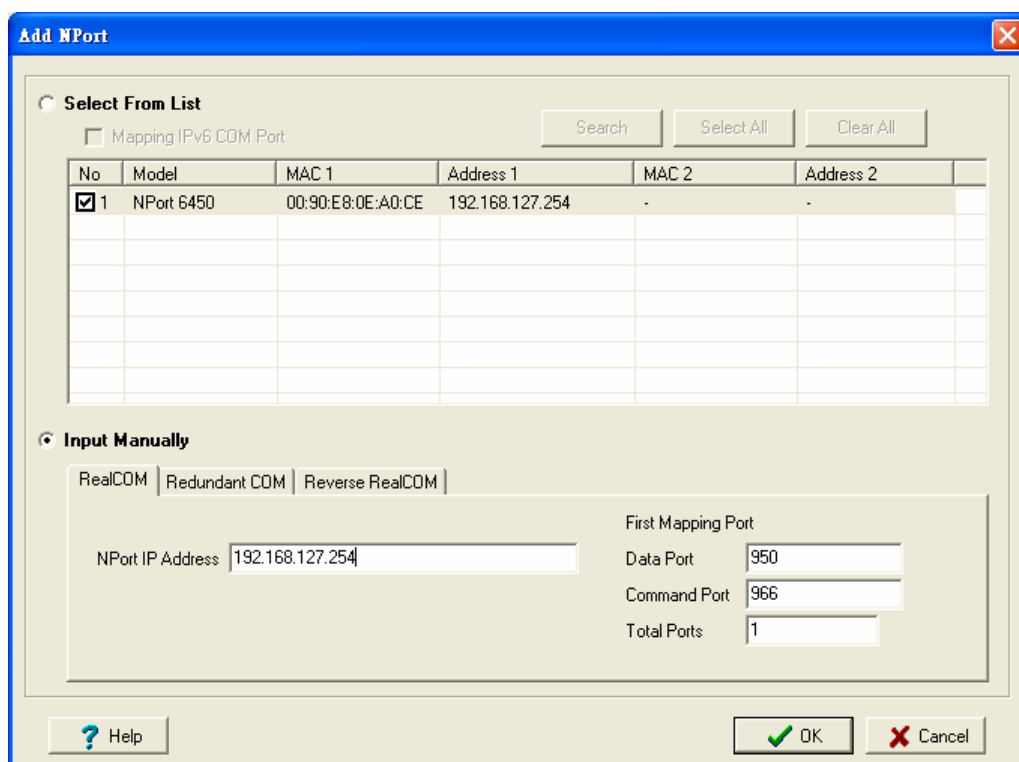
1. Запуск утилиты: **Пуск**→**Программы**→ **NPort Windows Driver Manager**→ **NPort Windows Driver Manager**.
2. Щелкните пиктограмму **Add**.



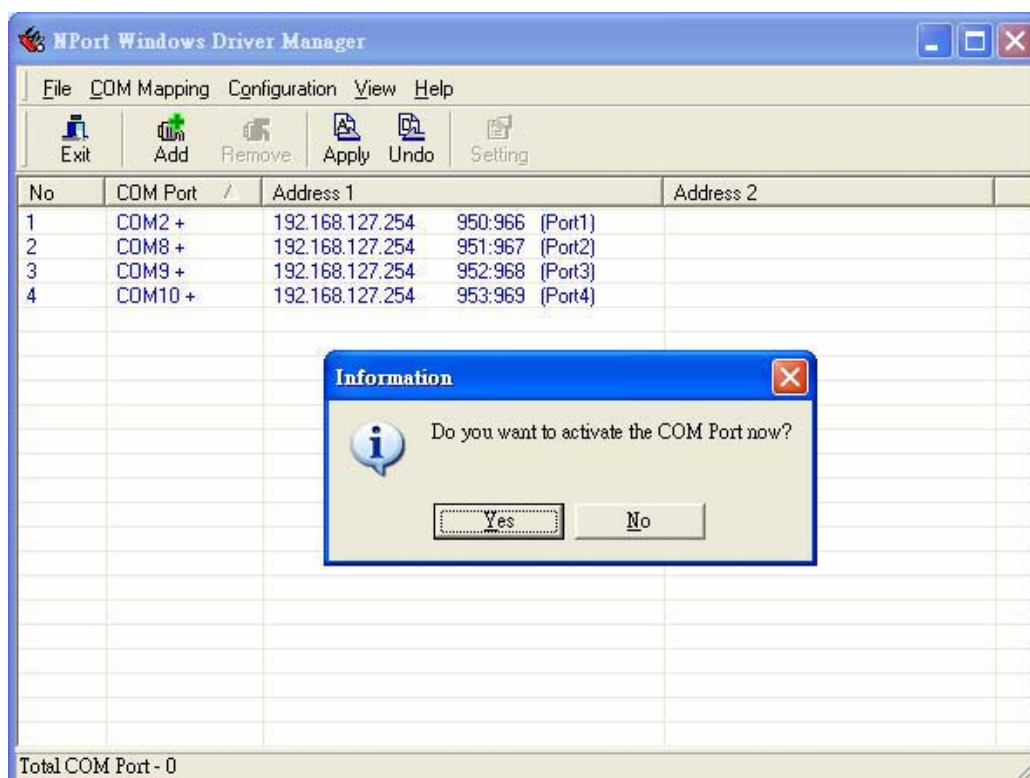
3. Нажмите **Search** для поиска всех устройств NPort. После того, как появится список имеющихся устройств, выберите нужный сервер и кликните ОК. По умолчанию используются IP-адреса стандарта IPv4 – можно изменить на IPv6, отметив флаг “Mapping IPv6 COM Port”.



Также можно выбрать способ Input Manually и вручную ввести IP-адрес нужного NPort'a, номер первого порта данных (1st Data Port), первого командного порта (1st Command Port) и общее число (total ports) создаваемых последовательных портов. Для перехода к следующему шагу создания COM-порта нажмите ОК. Поддерживается также FQDN (Fully Qualified Domain Name), в случае использования доменного имени IP-адрес будет введен автоматически.



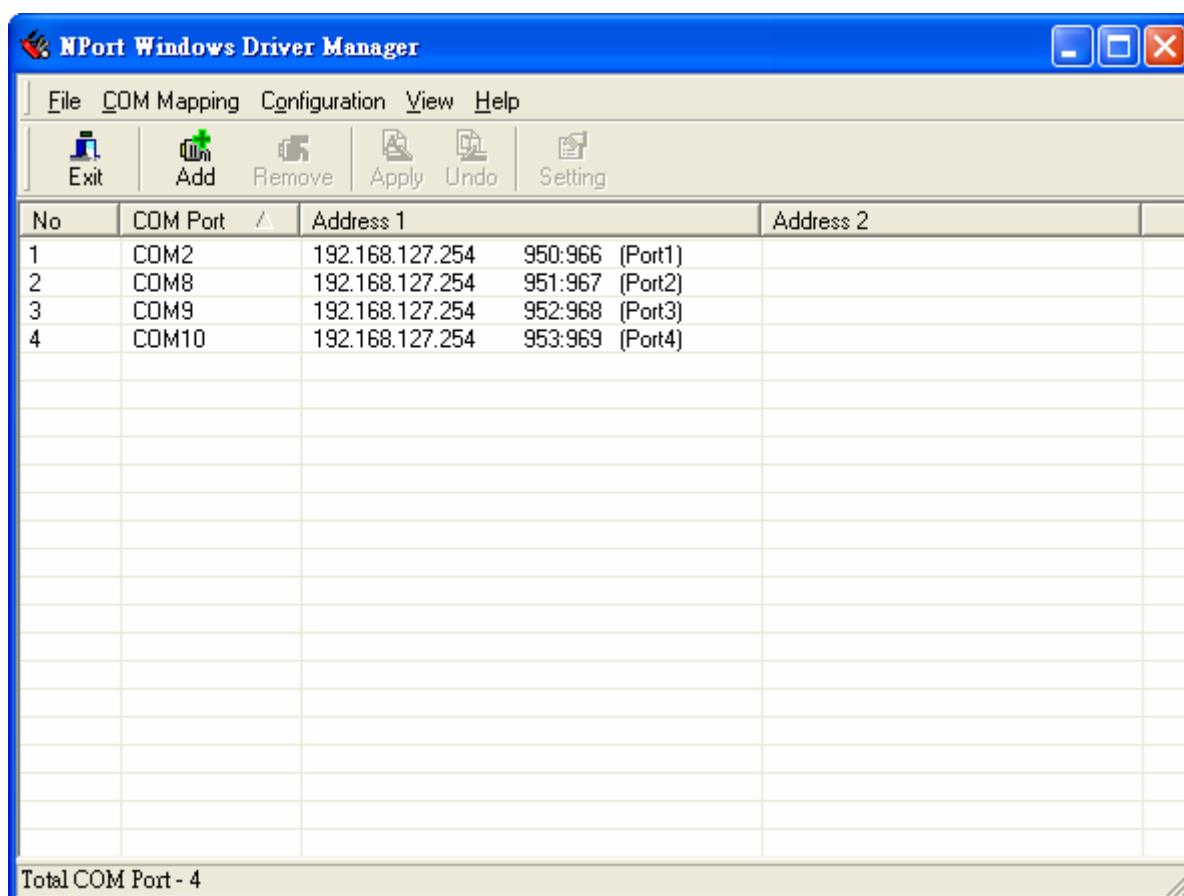
4. Неактивированные COM-порты будут выделены голубым цветом. Их подключение (активация) сохраняет информацию в регистре ОС хоста и позволяет дальнейшее использование COM-портов. Нажмите **Yes** для немедленной активизации COM-портов и **No**, чтобы подключить их позже.



5. В ОС Windows XP при создании каждого COM-порта появляется сообщение, показанное ниже. Для продолжения нажимайте **Continue Anyway**.



6. Активные COM-порты отображаются в списке черным цветом.



Add NPort [X]

Select From List

Mapping IPv6 COM Port

Search Select All Clear All

No	Model	MAC 1	Address 1	MAC 2	Address 2

Input Manually

RealCOM | Redundant COM | Reverse RealCOM |

MAC Address of NPort [.....]

1st Mapping Port Index [1] (1~32)

Total Ports [1]

(The "Port Index" means the NPort serial port index. E.g., for a 32-port NPort, the port index should be 1~32.)
 (If your NPort is a dual-LAN model, please input the MAC address of LAN1.)

? Help [OK] [Cancel]

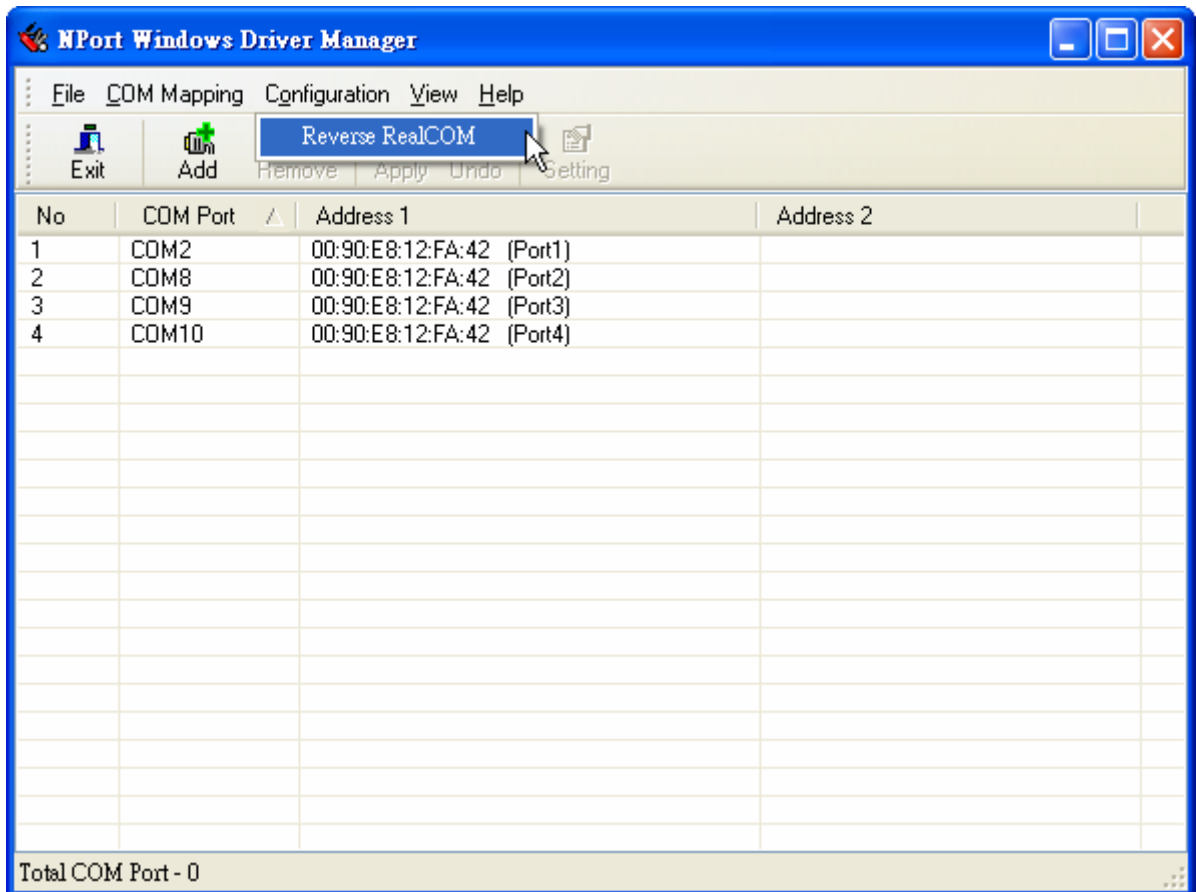
В зависимости от Вашей задачи, в режиме Reverse Real COM понадобится настраивать только часть последовательных портов. Пользователю нужно указать, какие из портов NPort'a будут работать в этом режиме.

Пример 1: Если нужно настроить только порт 15, то значения параметров будут как в таблице:

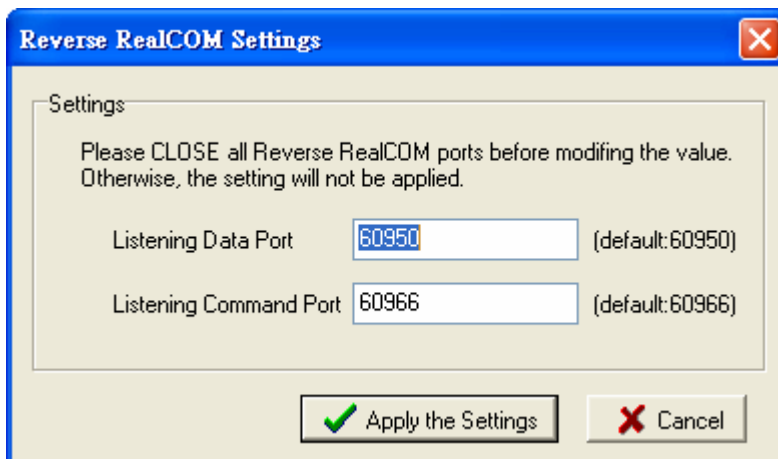
MAC Address of NPort	MAC-адрес NPort'a для идентификации	00:90:18:18:f1:36
1st Mapping Port Index	Номер первого порта	15
Total Number of Ports	Только порт №15 будет использоваться в данном режиме, поэтому общее число равно 1	1

Пример 2: Если нужно настроить только порты с 3 по 15, то значения параметров будут как в таблице:

MAC Address of NPort	MAC-адрес NPort'a для идентификации	00:90:18:18:f1:36
1st Mapping Port Index	Номер первого порта	3
Total Number of Ports	Порты с №3 по №15 будут использоваться в данном режиме, поэтому общее число равно 13	13

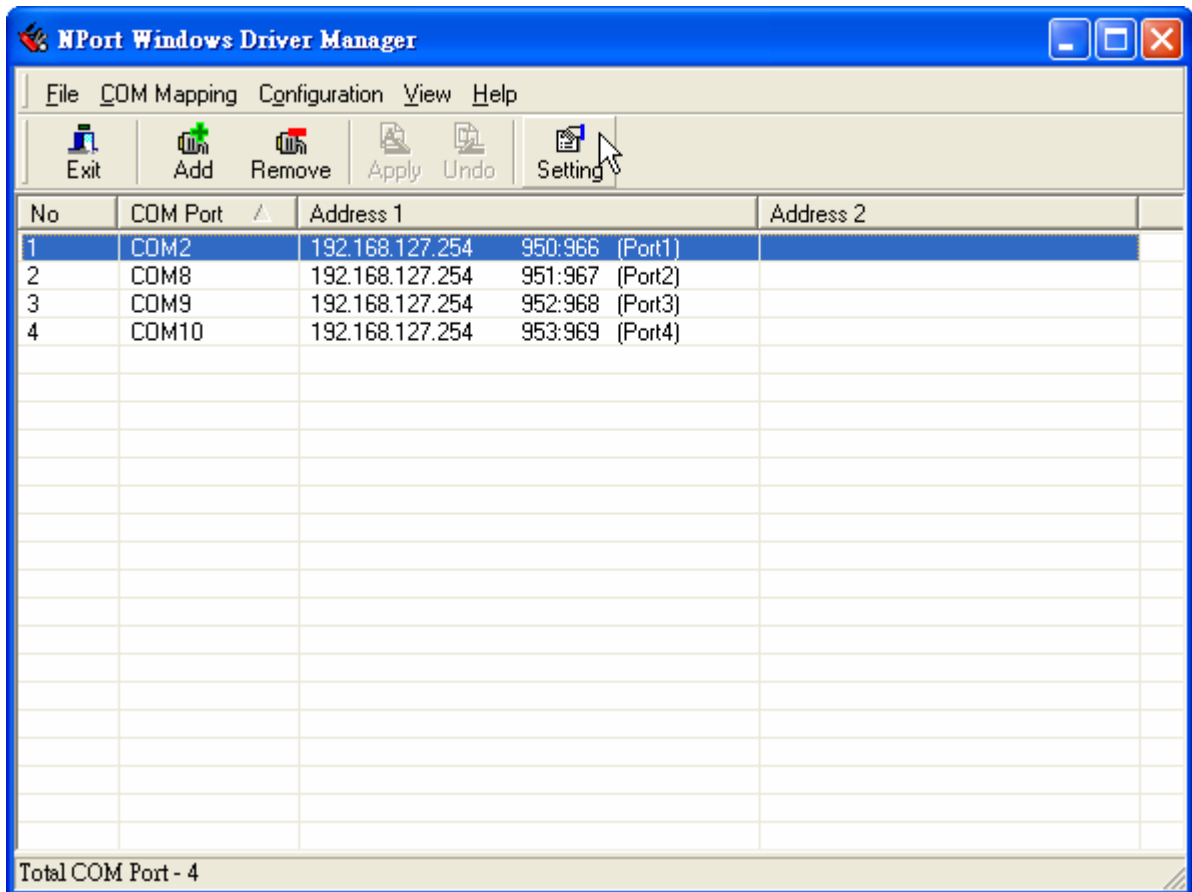


Это номер TCP-порта, используемый для соединения NPort'a 6000 с удаленным хостом/сервером. Во избежание совпадения с уже занятыми номерами по умолчанию этот порт установлен равным 60950.

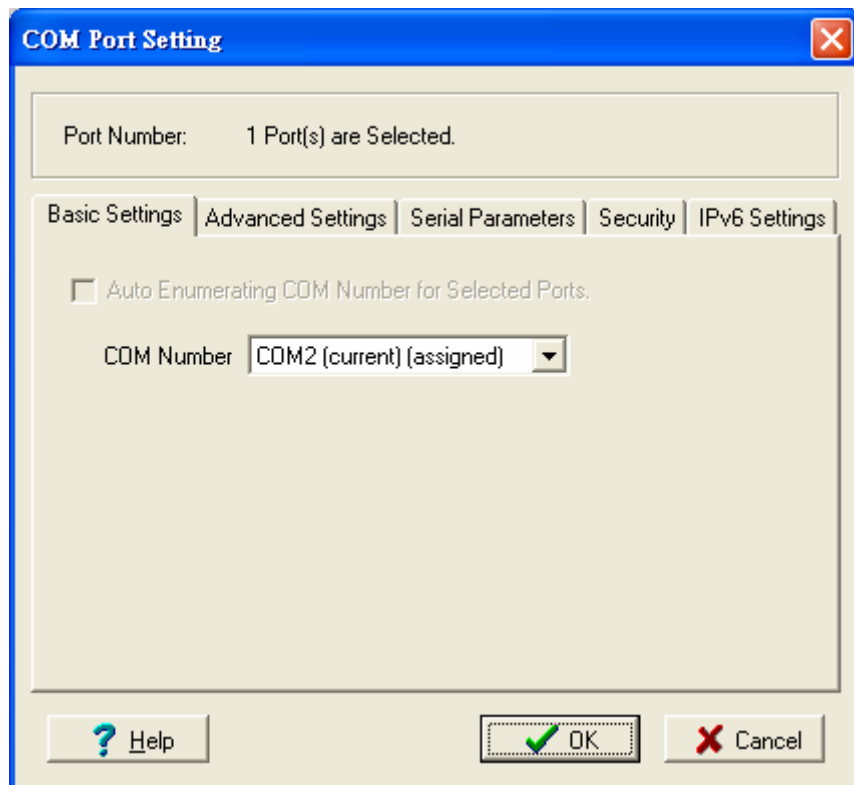


Настройка параметров COM-портов

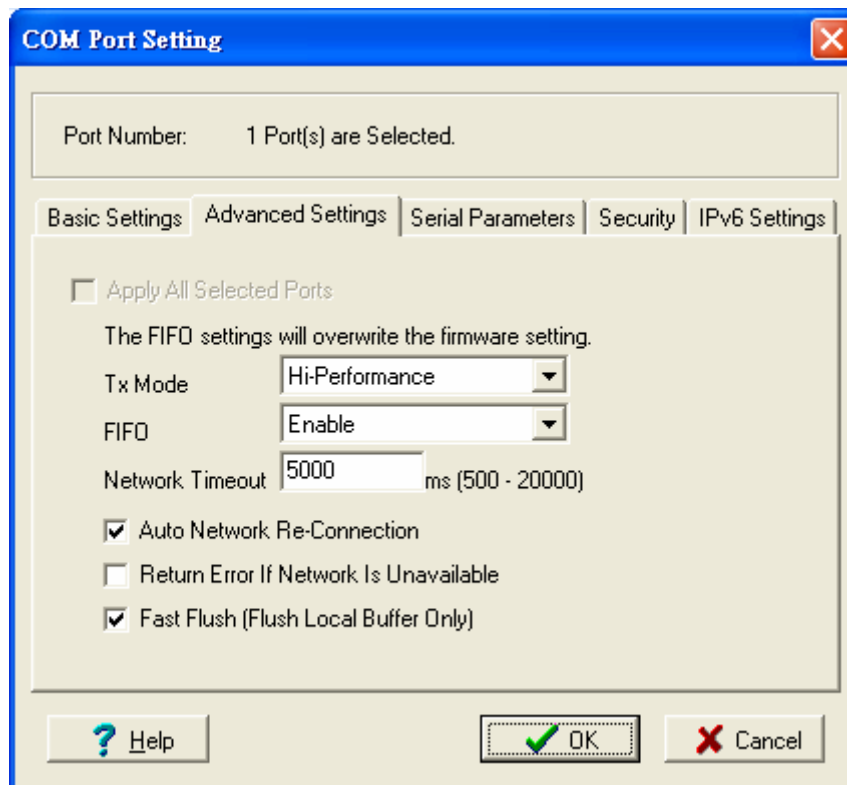
Для настройки параметров конкретных последовательных портов, работающих в режимах Real COM/Reverse Real COM нужно выделить строку с этим COM-портом и нажать кнопку **Setting**.



1. На вкладке Basic Setting в раскрывающемся списке **COM Number** выберите номер COM-порта. Для автоматической нумерации отметьте флажок **Auto Enumerating COM Number for Selected Ports**. Занятые номера отмечены как “in use”.



2. На вкладке **Advanced Setting** можно изменять параметры Tx Mode, FIFO и Flash Flush.



Tx Mode

Hi-Performance – значение по умолчанию. После отправки данных на NPort 6000 драйвер немедленно передает в программу ответ «Tx Empty» (Tx пуст). В режиме **Classical** драйвер отправляет этот ответ “Tx Empty” только после прихода подтверждения о получении данных последовательным портом NPort’a 6000. Это уменьшает пропускную способность. Рекомендуется использовать режим Classical, если нужно обязательное подтверждение доставки данных перед продолжением передачи.

FIFO

Если FIFO отключен (**Disabled**), то NPort 6000 будет передавать по байту до тех пор, пока Tx FIFO не станет пустым, Rx также будет передавать каждый принятый байт. Это дает большую скорость реакции, но меньшую пропускную способность.

Network Timeout

Сетевой таймаут. Эта функция служит для предотвращения блокирования связи, если нужный NPort недоступен.

Auto Network Re-Connection

Автоматическое переустановка соединения. Когда включена эта функция, драйвер будет повторно пытаться установить TCP-соединение при отсутствии ответа от NPort 6000 на пакеты “check alive”.

Return error if network is unavailable

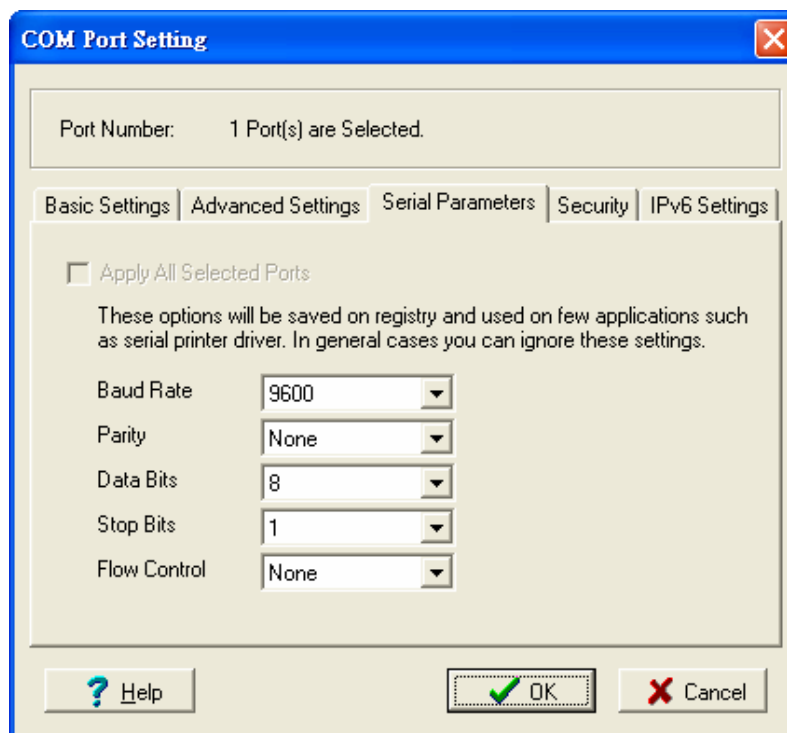
Выдавать ошибку, если недоступна сеть. Если эта функция отключена, драйвер не будет сигнализировать об ошибках, когда невозможно установить соединение с NPort’ом 6000. Если эта функция включена, функция Win32 Comm будет выдавать ошибку “STATUS_NETWORK_UNREACHABLE” при невозможности установления соединения с NPort’ом 6000. Обычно это означает сбой в работе сети хоста, возможно из-за повреждения кабеля. Однако, если другие сетевые устройства доступны, то возможно, что NPort 6000 обесточен или отключен от сети. Для использования этой функции необходимо, чтобы было активно **Auto Network Re-Connection**.

Fast Flush (очищает только локальный буфер)

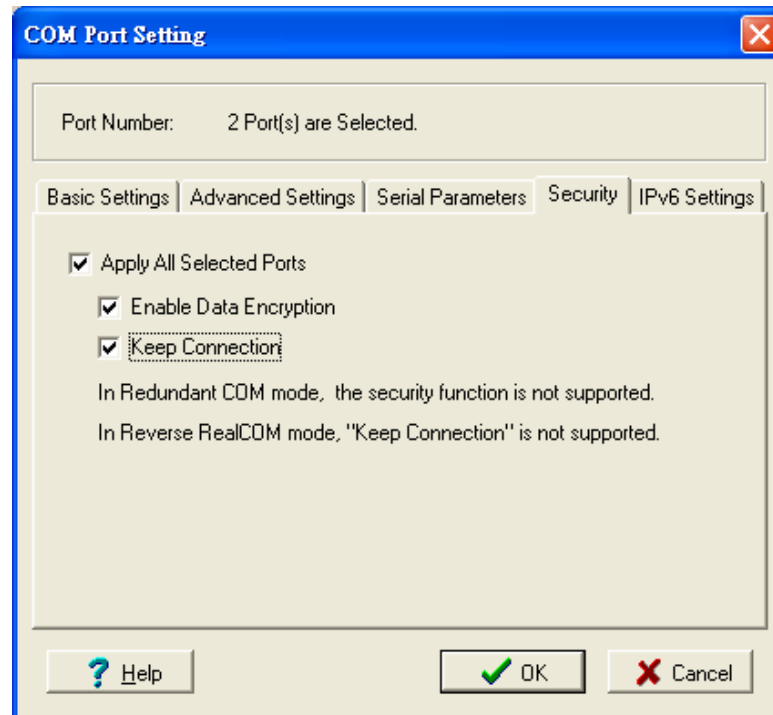
В некоторых задачах прикладная программа будет использовать функцию Win32 “PurgeComm()” перед чтением или записью данных. При применении функции “PurgeComm()” драйвер NPort’a посылает запросы на NPort несколько раз для подтверждения, что данные поставлены в очередь в буфере перед тем, как удалить их из локального буфера. Эта функция используется в некоторых приложениях. Однако требуется больше времени (на несколько сотен миллисекунд), чем при использовании локального СОМ-порта на ПК за счет дополнительных задержек при передаче данных по Ethernet. Поэтому “PurgeComm()” работает значительно быстрее на встроенных СОМ-порты ПК, чем на виртуальных СОМ-портах NPort’a 6000. Для приложений, требующих меньшее время реакции, в новой версии драйвера NPort’a есть функция Fast Flush. По умолчанию эта функция включена.

Если Вы отключили функцию Fast Flush и после этого виртуальные СОМ-порты заметно медленнее, чем обычные СОМ-порты, попытайтесь выяснить, не использует ли Ваше приложение функции “PurgeComm()”. Если да, то включите функцию Fast Flush и посмотрите результат.

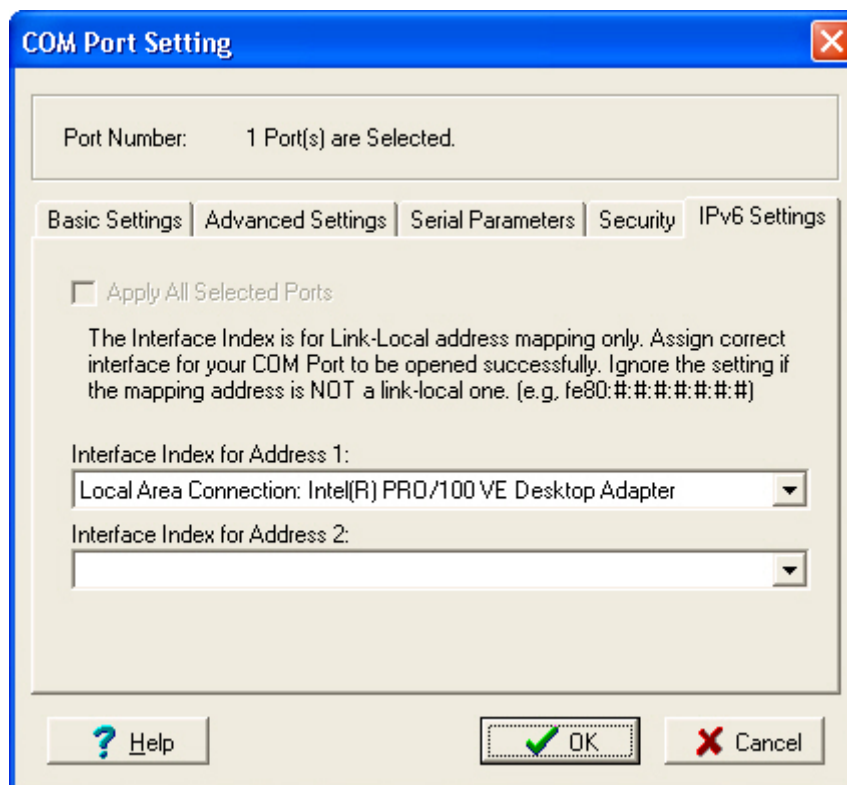
3. На вкладке **Serial Parameters** показываются настройки по умолчанию, которые выставляются при включении NPort’a 6000. Однако программа может открыть СОМ-порт через Win 32 API с другими параметрами последовательной связи.



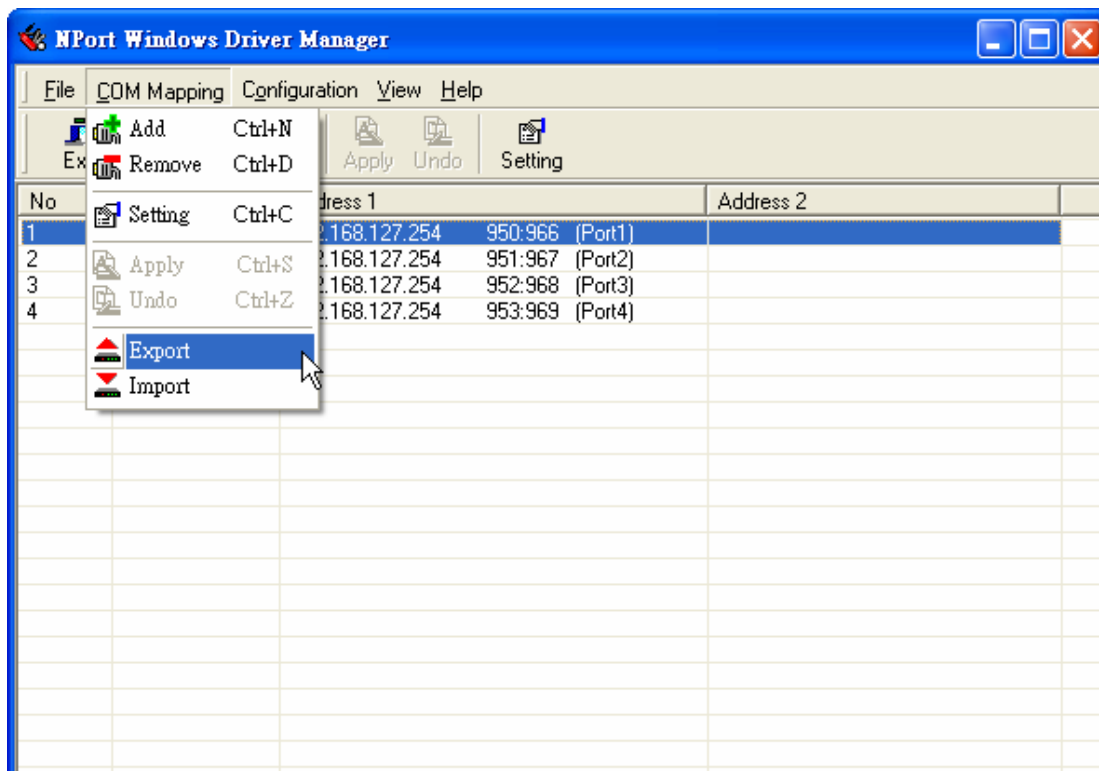
4. Для настроек параметров безопасности перейдите на вкладку **Security**. Для включения шифрования данных при передаче по СОМ-порту отметьте флаг **Enable Data Encryption**. Для подключения функции шифрования без перезагрузки СОМ-портов отметьте флаг **Keep connection**. (Если Ваша программа часто открывает/закрывает СОМ-порты и NPort 6000 используется только одним хостом, то можно включить данную функцию для увеличения быстродействия открытия/закрытия. Однако это приведет к тому, что последовательный порт NPort’a будет все время занят одним хостом, в то время как другие не смогут его использовать). Для применения настроек шифрования ко всем последовательным портам отметьте флаг **Apply All Selected Ports**.



5. На вкладке **IPv6 Settings** настраиваются адреса локальной сети. При использовании глобальных (белых) IPv6-адресов, данная функция не будет применяться. Когда используются локальные IPv6-адреса, пользователь должен указать сетевой интерфейс в списке Interface Index for address 1. Interface Index for address 2 предназначен для технологии Redundant COM (Резервированный COM-порт) и используется только в устройствах серии CN 2600.



6. Для сохранения настроек в текстовом файле, в меню **COM mapping** выберите пункт **Export**. Впоследствии можно импортировать этот файл настроек в другой NPort и использовать такие же самые настройки COM-портов на других хостах.



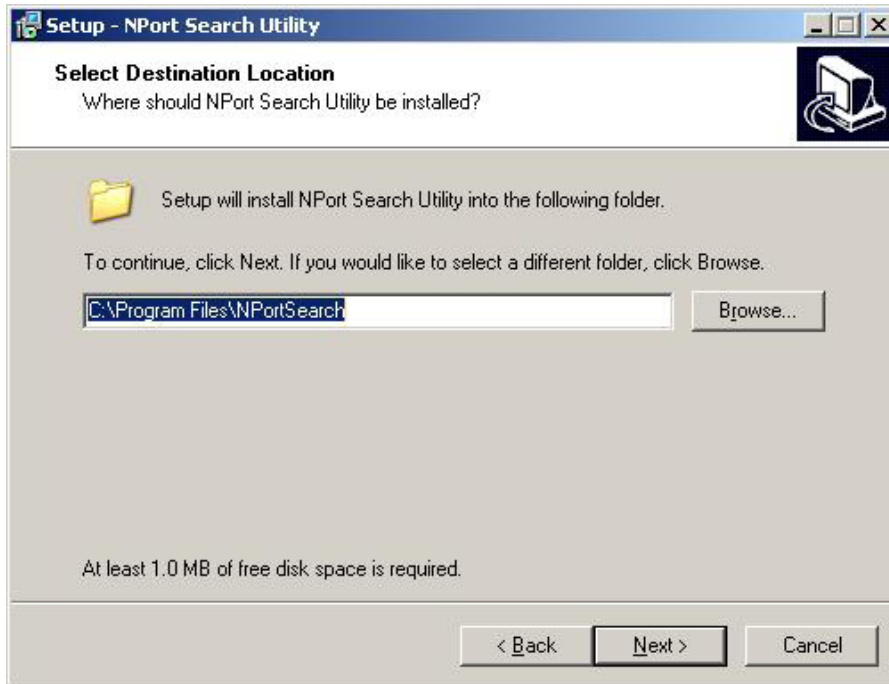
NPort Search Utility

Установка утилиты

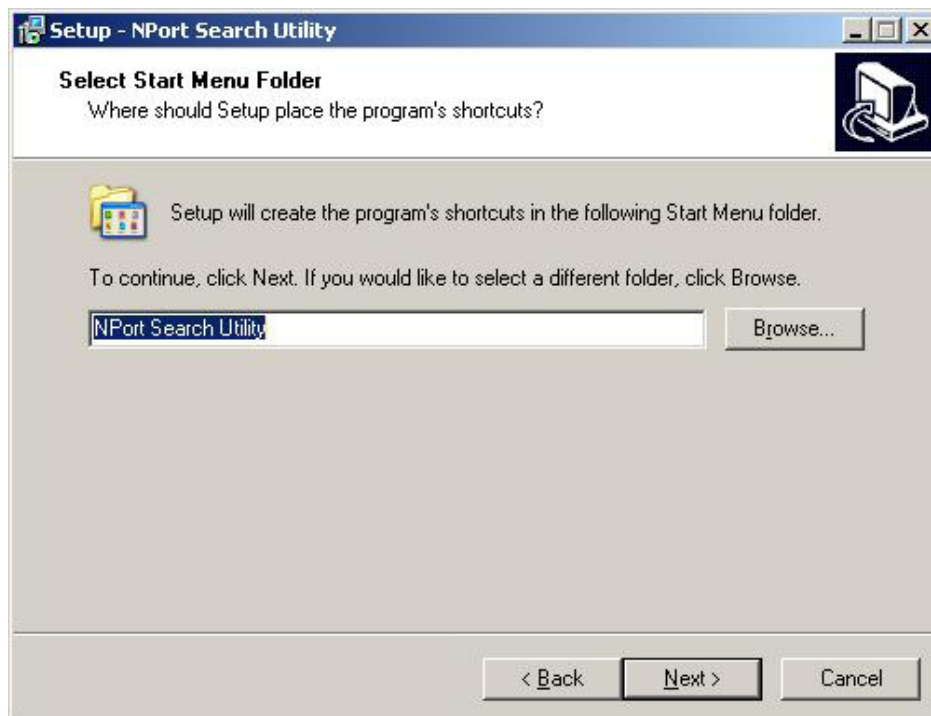
1. В окне автозапуска установочного CD нажмите кнопку **INSTALL UTILITY** для установки утилиты NPort Search Utility. После запуска программы нажмите **Yes** для продолжения процесса.
2. Нажмите **Next**, когда откроется приветственное окно.



3. Нажмите **Next** для установки файлов в папку по умолчанию или **Browse** для выбора другого местоположения.



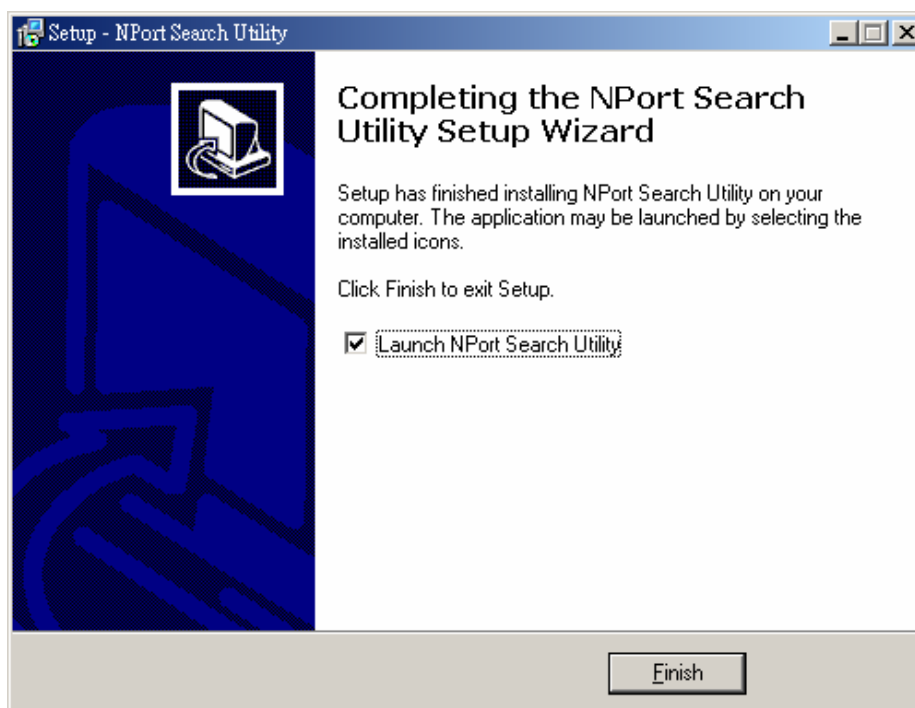
4. Нажмите **Next** для установки в папку с названием по умолчанию.



5. Нажмите **Next** для продолжения установки. Программа установки покажет список параметров установки.



6. Нажмите **Install** для начала установки. Окно установки будет показывать ход процесса установки. Для изменения настроек, нажмите кнопку **Back** и перейдите в предыдущие окна.
7. Нажмите **Finish** для завершения установки NPort Search Utility.

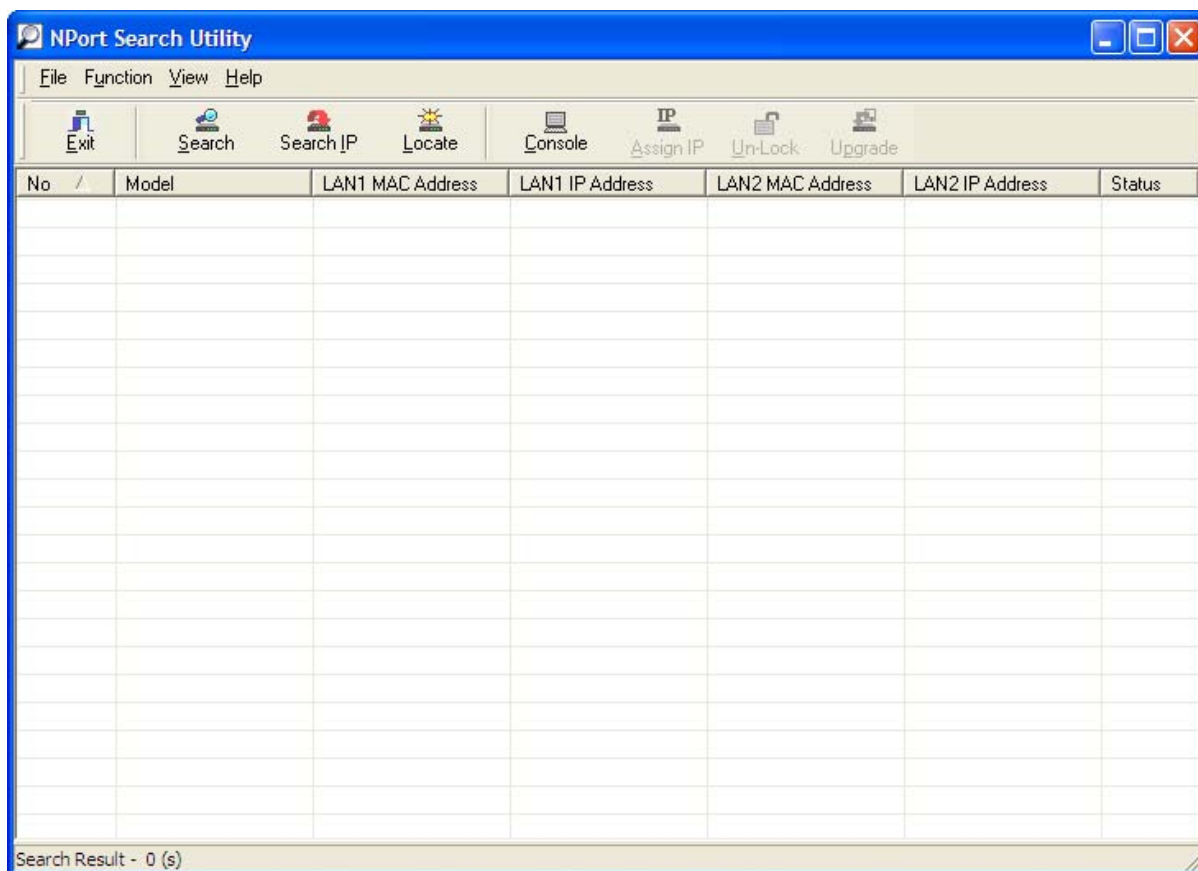


Настройка

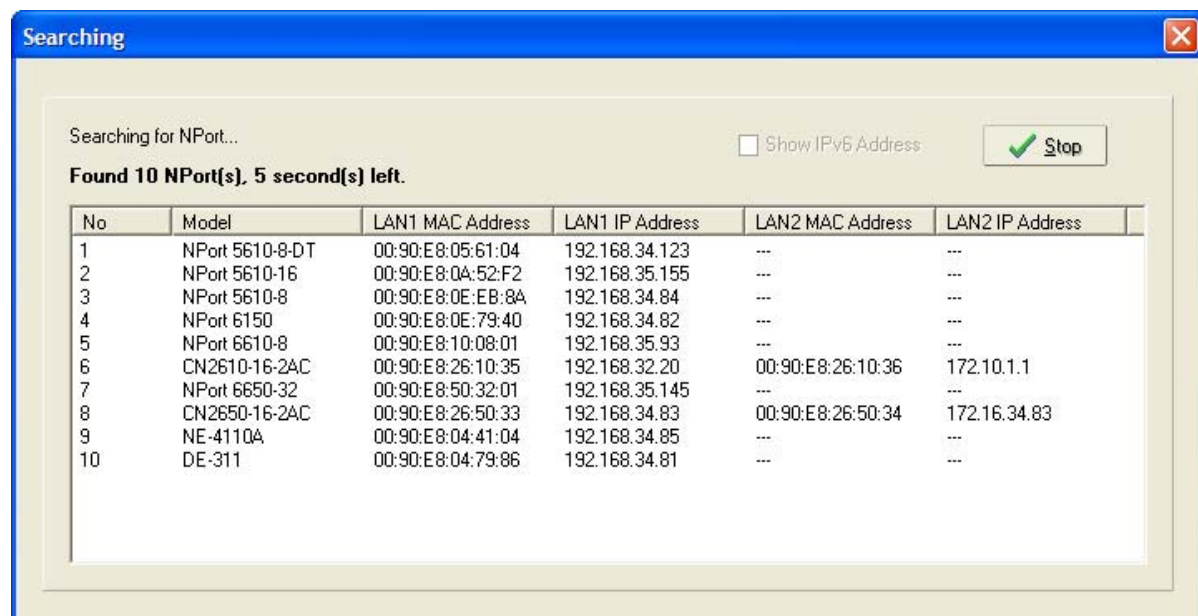
Широковещательный поиск позволяет обнаружить все NPort'ы, находящиеся в одной локальной сети с ПК. После нахождения NPort'ов можно изменить их IP-адреса.

Поскольку функция широковещательного использует поиск не по IP-адресам, а по MAC-адресам, то будут найдены все NPort'ы 6000 локальной сети, независимо от того, находятся ли они в одной подсети с ПК или нет.

1. Запустите утилиту NPort Search Utility и затем щелкните пиктограмму **Search**.



Окно поиска показывает ход процесса – найденные NPort'ы.



2. После завершения поиска будет выведен список устройств NPort в рабочем окне утилиты.

No.	Model	LAN1 MAC Address	LAN1 IP Address	LAN2 MAC Address	LAN2 IP Address	Status
1	NPort 5610-8-DT	00:90:E8:05:61:04	192.168.34.123	---	---	
2	NPort 5610-16	00:90:E8:0A:52:F2	192.168.35.155	---	---	
3	NPort 5610-8	00:90:E8:0E:EB:8A	192.168.34.84	---	---	
4	NPort 6150	00:90:E8:0E:79:40	192.168.34.82	---	---	
5	NPort 6610-8	00:90:E8:10:08:01	192.168.35.93	---	---	
6	CN2610-16-2AC	00:90:E8:26:10:35	192.168.32.20	00:90:E8:26:10:36	172.10.1.1	
7	NPort 6650-32	00:90:E8:50:32:01	192.168.35.145	---	---	
8	CN2650-16-2AC	00:90:E8:26:50:33	192.168.34.83	00:90:E8:26:50:34	172.16.34.83	
9	NE-4110A	00:90:E8:04:41:04	192.168.34.85	---	---	
10	DE-311	00:90:E8:04:79:86	192.168.34.81	---	---	

Для изменения настроек выделенного NPort'a, щелкните на пиктограмме Console для открытия страницы WEB-консоли. Откроется WEB-страница, в которой можно выполнить все необходимые настройки. См. главу 5 о работе с WEB-консолью.

Linux Real TTY Drivers

Основная последовательность действий

Для создания виртуального TTY-порта в ОС Linux, выполните следующие действия:

1. Подключите NPort 6000. После проверки наличия доступа к нему по IP-адресу (с помощью процедур ping, telnet и т.д.) можно задать конкретные настройки каждого последовательного порта в режиме Real COM.
2. Установите на компьютере файлы драйвера Linux Real TTY.
3. Создайте виртуальные TTY-порты.

Аппаратная установка

Перед программной установкой убедитесь, что произведена полная аппаратная установка. IP-адрес по умолчанию равен **192.168.127.254**.

ПРИМЕЧАНИЕ После аппаратной установки нужно настроить режим работы Real COM последовательных портов.

Установка файлов Linux Real TTY Driver

1. Файл с драйвером есть на CD-диске либо его можно скачать с WEB-сайта <http://www.moxa.com>.

2. Авторизуйтесь в консоли в качестве root-пользователя.
3. Выполните команду `cd /` для перехода в корневую папку.
4. Скопируйте файл драйвера **npreal2xx.tgz** в папку `/`.
5. Выполните `tar xvfz npreal2xx.tgz`, чтобы распаковать все файлы.
6. Выполните команду `/tmp/moxa/mxinst`.

При использовании RedHat AS/ES/WS и Fedora Core1 нужно использовать команду с дополнительными аргументами: `# /tmp/moxa/mxinst SP1`

Скрипт-сценарий автоматически установит необходимые драйвера.

7. После установки драйвера можно просмотреть файлы в папке `/usr/lib/npreal2/driver`:
 - > **mxaddsvr** (Добавить Сервер, назначить TTY-порт)
 - > **mxdelsvr** (Удаление Сервера, удаление TTY-порта)
 - > **mxloadsvr** (Перезагрузка сервера)
 - > **mxmknod** (Создание узел устройства/tty-порт)
 - > **mxrmnod** (Удалить device node/tty-порт)
 - > **mxuninst** (Удалить tty-порт и файл драйверов)

На этом последовательные порты Nport'a готовы к использованию в качестве виртуальных TTY-портов.

Создание TTY-портов

Проверьте, чтобы режим работы последовательных портов, назначаемых как виртуальные TTY-порты, был установлен в Real COM. После авторизации войдите в директорию `/usr/lib/npreal2/driver` и выполните команду **mxaddsvr** для назначения последовательных портов Nport'a в качестве TTY-портов. Формат команды **mxaddsvr**:

```
mxaddsvr [IP-адрес NPort'a] [Общее число портов] ([Порт данных] [Командный порт])
```

Команда **mxaddsvr** выполняет следующие действия:

1. Изменяет **npreal2d.cf**.
2. Создает TTY-порты в директории `/dev` со старшим и младшим номером, настроенным в **npreal2d.cf**.
3. Перезагружает драйвер.

Автоматическое создание TTY-портов

Для автоматического создания TTY-портов можно выполнить команду **mxaddsvr** с IP-адресом и номерами портов, как в примере ниже:

```
# cd /usr/lib/npreal2/driver
# ./mxaddsvr 192.168.3.4 16
```

В данном примере будет добавлено 16 TTY-портов, у всех будет общий IP-адрес 192.168.3.4, номера портов данных: с 950 по 965 и командных портов: с 966 по 981.

Создание TTY-портов вручную

Для ручного создания TTY-портов можно выполнить команду **mxaddsvr** с IP-адресом и при этом самостоятельно задать номера портов данных и команд, как в примере ниже:

```
# cd /usr/lib/npreal2/driver
# ./mxaddsvr 192.168.3.4 16
```

В данном примере будет добавлено 16 TTY-портов, у всех будет общий IP-адрес 192.168.3.4, номера портов данных: с 950 по 965 и командных портов: с 966 по 981.

Удаление TTY-портов

После авторизации войдите в директорию **/usr/lib/npreal2/driver** и выполните команду **mxdelsvr** для удаления устройства. Формат команды:

```
mxdelsvr [IP-адрес устройства]
```

Например:

```
# cd /usr/lib/npreal2/driver
# ./mxdelsvr 192.168.3.4
```

Команда **mxdelsvr** выполняет следующие действия:

1. Изменяет файл `npreal2d.cf`.
2. Удаляет соответствующие tty-порты в папке **/dev**.
3. Перезагружает драйвер.

Если команда введена без IP-адреса устройства, то на экран будет выведен список всех установленных серверов и общее число портов. Вам нужно будет выбрать конкретный NPort.

Удаление файлов Linux Real TTY Driver

Предусмотрена возможность удаления всех файлов драйверов, назначенных TTY-портов и деинсталляция драйвера. Для выполнения данного действия, нужно войти в директорию **/usr/lib/npreal2/driver** и выполнить команду **mxuninst**. При этом будут произведены следующие действия:

1. Удален драйвер.
2. Удалены все файлы и папки из директории **/usr/lib/npreal2**
3. Удалена директория **/usr/lib/npreal2**
4. Соответствующим образом изменен файл сценария запуска системы.

Unix Fixed TTY Driver

Установка Unix Driver

1. Авторизуйтесь в ОС UNIX и создайте папку для Моха TTY. Для создания папки с именем **/usr/etc** введите команду:

```
# mkdir -p /usr/etc
```

2. Скопируйте **moxatty.tar** в созданную папку. Если создана папка, указанная выше, то нужно выполнить команду:

```
# cp moxattyd.tar /usr/etc
```

```
# cp /usr/etc
```

3. Распакуйте архив выполнив следующую команду:

```
# tar xvf moxattyd.tar
```

Будут извлечены следующие файлы:

README.TXT

moxattyd.c --- исходная программа
moxattyd.cf --- пустой файл настроек
Makefile --- формирование файла
VERSION.TXT --- версия драйвера tty

FAQ.TXT

4. Компиляция и связывание

Для ОС SCO UNIX:

```
# make sco
```

Для UnixWare 7:

```
# make svr5
```

Для UnixWare 2.1.x, SVR4.2:

```
# make svr42
```

Настройка Unix Driver

Изменение настроек

Конфигурация, используемая программой **moxattyd**, хранится в текстовом файле **moxattyd.cf**, который находится в папке, содержащей саму программу. Можно использовать **vi** или любой текстовый редактор для изменения файла:

```
ttyp1 192.168.1.1 950
```

Более подробную информацию о настройках можно просмотреть в файле **moxattyd.cf**, содержащем детальное описание различных параметров.

ПРИМЕЧАНИЕ “Device name” (Название устройства) зависит от используемой ОС. См. раздел Device Name Rule в файле README.TXT.

Для начала работы с **moxattyd** после загрузки системы, добавьте строку в **/etc/inittab** с именем **tty**, определенном в файле **moxattyd.cf**, как показано в примере ниже:

```
ts:2:respawn:/usr/etc/moxattyd/moxattyd -t 1
```

Device naming rule

Для ОС UnixWare 7, UnixWare 2.1.x и SVR4.2:

```
pts/[n]
```

Для всех остальных UNIX-систем:

```
ttyp/[n]
```

Запуск **moxattyd**

Выполните команду **init q** или перезапустите Вашу ОС UNIX.

Добавление нового сервера

1. Измените текстовый файл **moxattyd.cf** для добавления дополнительного сервера. Для этого можно использовать **vi** или любой текстовый редактор. Более подробную информацию о настройках можно посмотреть в файле **moxattyd.cf**, содержащем детальное описание различных параметров.

2. Отыщите PID программы **moxattyd**.

```
# ps -ef | grep moxattyd
```

3. Обновите конфигурацию программы **moxattyd**.

```
# kill -USR1 [PID]
```

(например, если PID = 404, то **kill -USR1 404**)

На этом процедура добавления нового сервера заканчивается.

Приложение А Распиновка и разводка кабеля

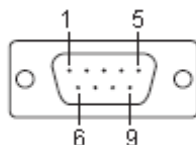
Приложение содержит следующие главы:

- **Схемы распиновки порта**
 - RS-232/422/485 («Папа» DB9)
 - RS-232/422/485 («Папа» RJ45)
- **Распайка кабелей**
 - Ethernet-кабели
 - Кабели для интерфейса RS-232
 - Кабели для интерфейса RS-422/4-хпровод. RS-485
 - Кабели для двухпровод. RS-485
 - Распиновка разъемов DB9 и DB25

Распиновка порта

RS-232/422/485 («Папа» DB9)

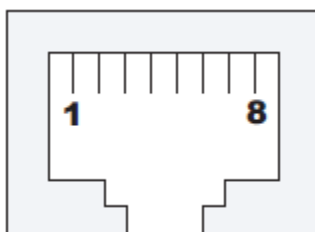
(для моделей NPort 6150, 6250 и 6450)



Номер контакта	RS-232	RS-422/485 (4-проводный)	RS-485 (2-проводный)
1	DCD	TXD-(A)	—
2	RxD	TXD+(B)	—
3	TxD	RXD+(B)	Data+(B)
4	DTR	RXD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	—	—
7	RTS	—	—
8	CTS	—	—
9	—	—	—

RS-232/422/485 («Папа» RJ45)

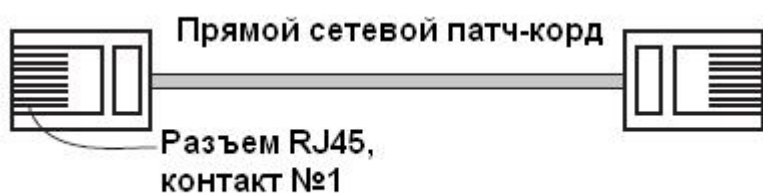
(для модели NPort 6650)



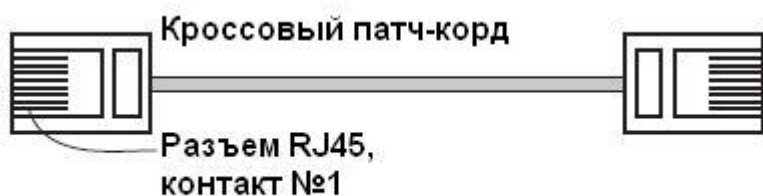
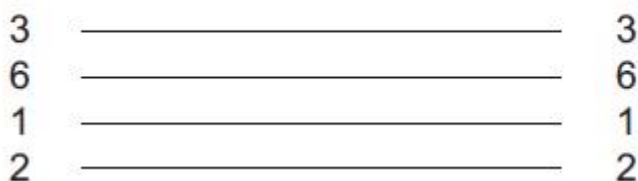
Номер контакта	RS-232	RS-422/485 (4-проводный)	RS-485 (2-проводный)
1	DSR	—	—
2	RTS	TXD+(B)	—
3	GND	GND	GND
4	TxD	TXD-(A)	—
5	RxD	RXD+(B)	Data+(B)
6	DCD	RXD-(A)	Data-(A)
7	CTS	—	—
8	DTR	—	—

Распайка кабелей

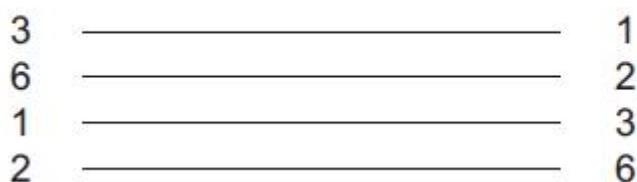
Ethernet-кабели



Распайка кабеля



Распайка кабеля

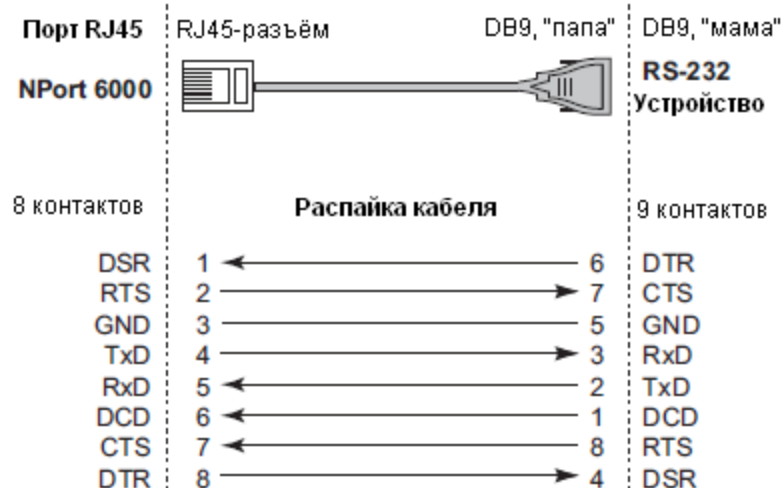


Кабели для интерфейса RS-232

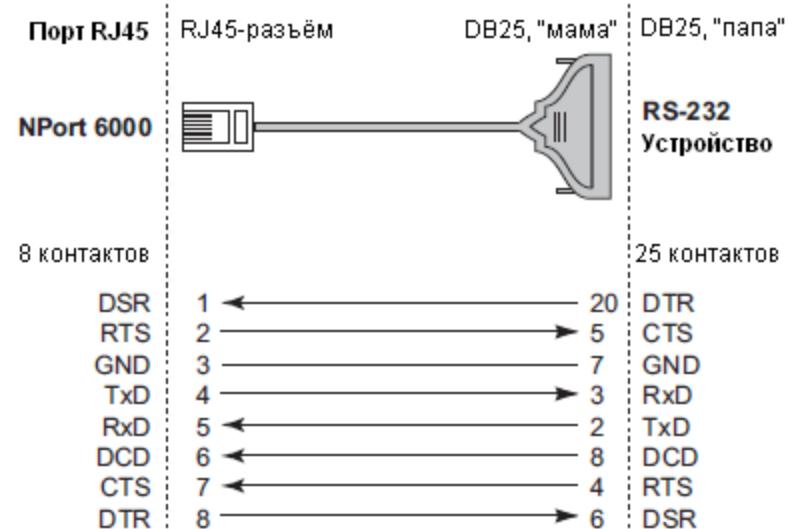
Переходник RJ45 (8-конт.) на DB9 ("мама")



Переходник RJ45 (8-конт.) на DB9 "папа"



Переходник RJ45 (8-конт.) на DB25 ("мама")



Переходник RJ45 (8-конт.) на DB25 ("папа")



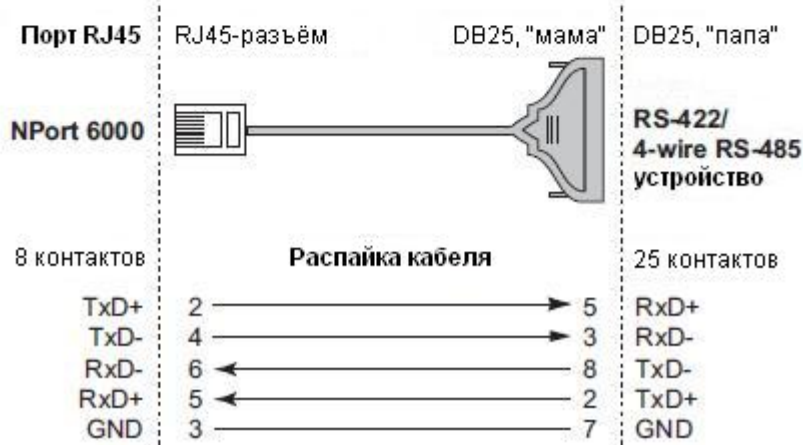
Переходник RJ45 (8-конт.) на DB9 ("мама")



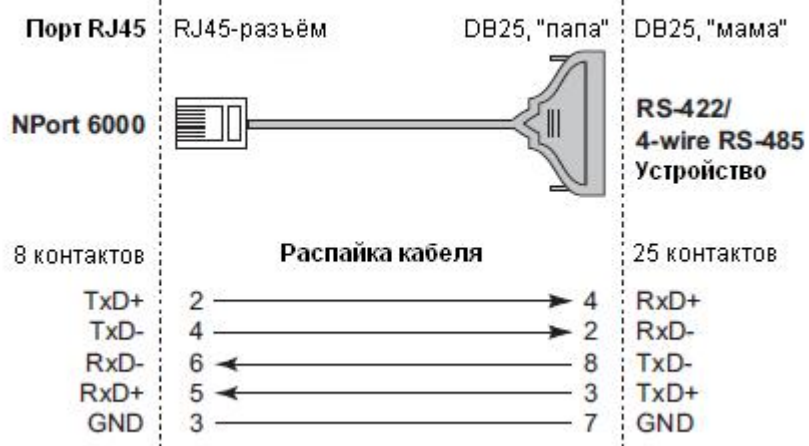
Переходник RJ45 (8-конт.) на DB9 "папа"



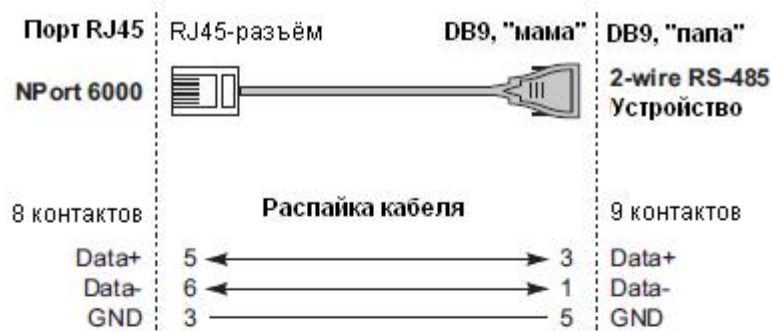
Переходник RJ45 (8-конт.) на DB25 ("мама")



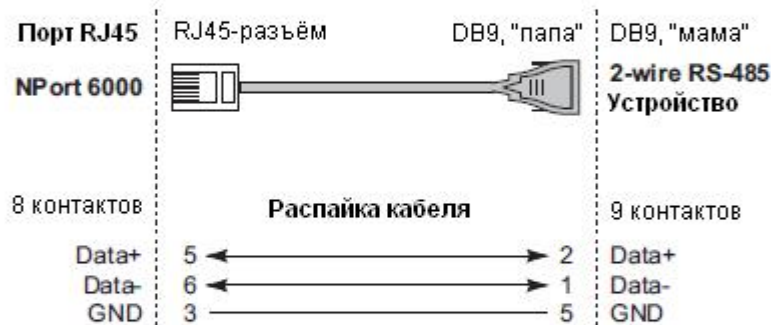
Переходник RJ45 (8-конт.) на DB25 ("папа")



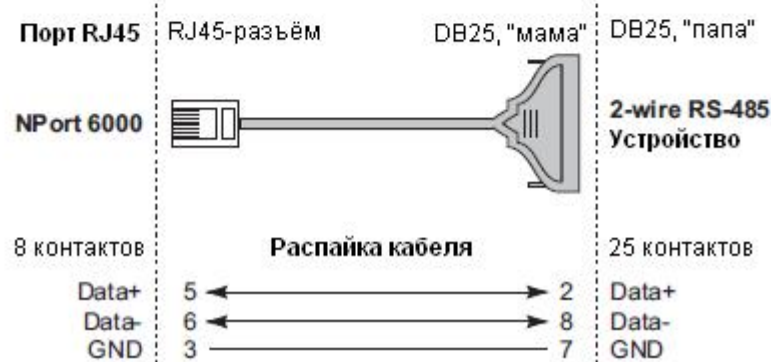
Переходник RJ45 (8-конт.) на DB9 ("мама")



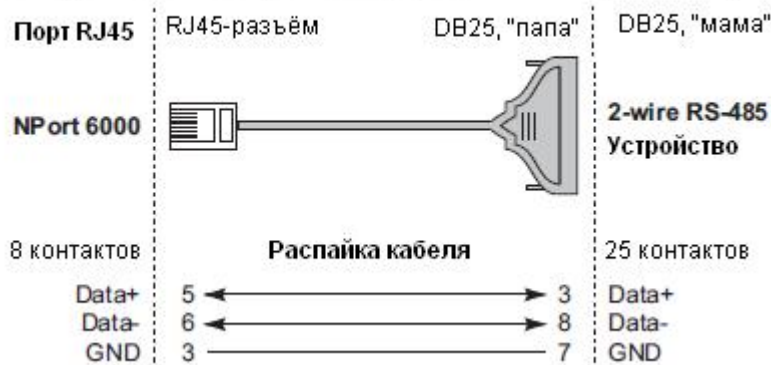
Переходник RJ45 (8-конт.) на DB9 "папа"



Переходник RJ45 (8-конт.) на DB25 ("мама")



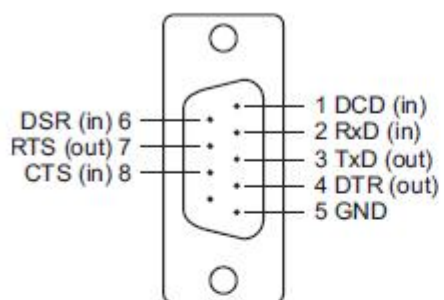
Переходник RJ45 (8-конт.) на DB25 ("папа")



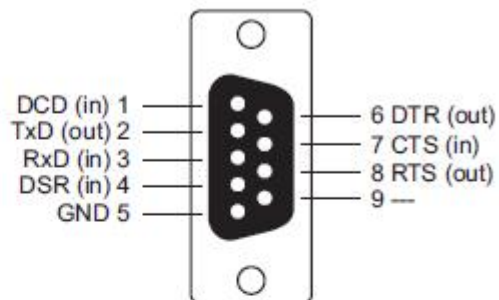
Распиновка разъемов DB9 и DB25

Распиновка разъема DB9, "папа" и ответного DB9, "мама"

Разъем DB9, "папа"

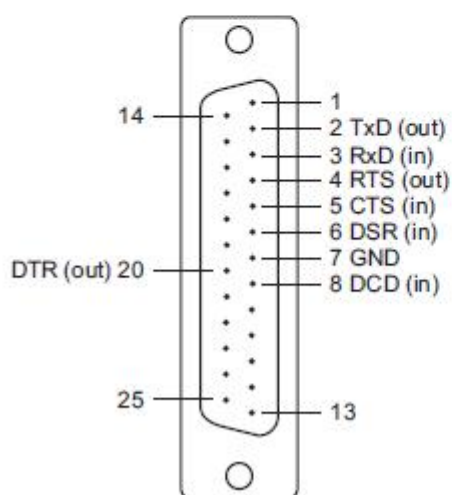


Разъем DB9, "мама"

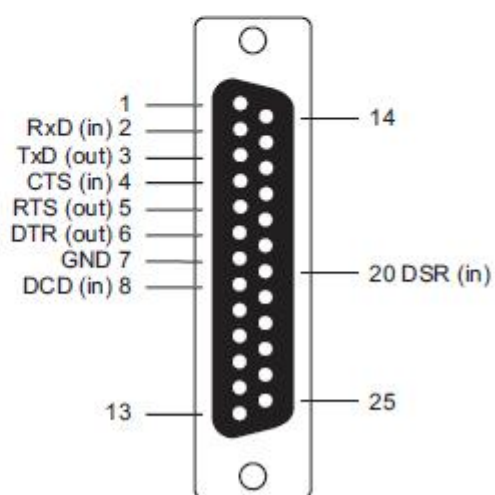


Распиновка разъема DB25, "папа" и ответного DB25, "мама"

Разъем DB25, "папа"



Разъем DB25, "мама"



Приложение В RFC2217

В приложении поясняется, каким образом настраивается режим RFC-2217. RFC-2217 определяет функции управления COM-портом на основе Telnet-протокола и используется для назначения COM-портов сетевым портам. Любое устройство стороннего производителя, поддерживающее стандарт RFC-2217, может использовать виртуальные COM-порты NPort'a 6000. Ниже показаны настройки:

1. В консоли настроек NPort'a 6000 выберите режим RFC2217 для нужного последовательного порта. По умолчанию первому последовательному порту NPort 6000 назначен TCP-порт 4001, второму – 4002 и т.д.

MOXA www.moxa.com Total Solution for Industrial Device Networking

Operation Modes

Port 1

Application: Device Control

Mode: RFC2217

TCP alive check time: 7 (0 - 99 min)

TCP port: 4001

Data Packing

Packet length: 0 (0 - 1024)

Delimiter 1: 00 (Hex) Enable

Delimiter 2: 00 (Hex) Enable

Delimiter process: Do Nothing (Processed only when Packing length is 0)

Force transmit: 0 (0 - 65535 ms)

Apply the above settings to: P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 P11 P12 P13 P14 P15 P16 All ports

Submit

2. Загрузите и установите драйвер устройства стороннего производителя, поддерживающего RFC-2217, например Serial/IP COM Port Redirector (Tactical Software).
3. Используя программу настройки от стороннего производителя, назначьте COM-портам IP-адрес NPort'a 6000 и соответствующие номера TCP-портов.
4. Попробуйте открыть назначенный Вами COM-порт. Если у Вас получилось открыть его, это означает, что драйвер виртуального порта установлен успешно; с устройствами, подключенными к последовательному порту NPort'a 6000, можно работать, как если бы они были соединены напрямую с ПК.

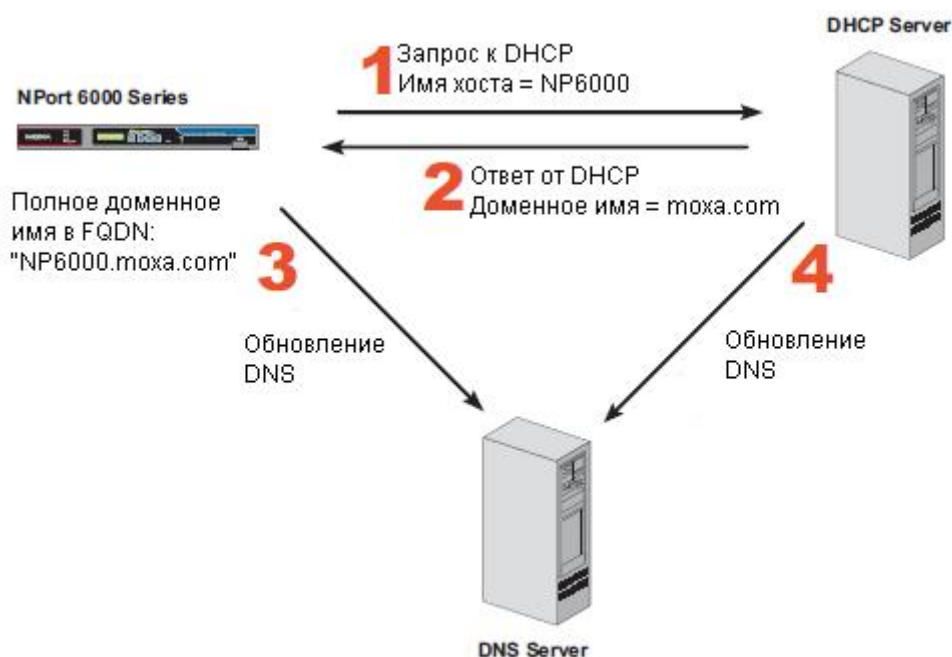
Приложение С DDNS-сервер

В приложении поясняется, каким образом использовать функцию DDNS с NPort'ом 6000. После того, как NPort 6000 получил IP-адрес с DHCP-сервера, удаленные серверы не смогут получить к нему доступ, используя фиксированный IP-адрес. При использовании функции DDNS (Dynamic Domain Name Server) удаленные серверы смогут обращаться к NPort'у 6000 по его доменному имени вместо IP-адреса.

Обзор

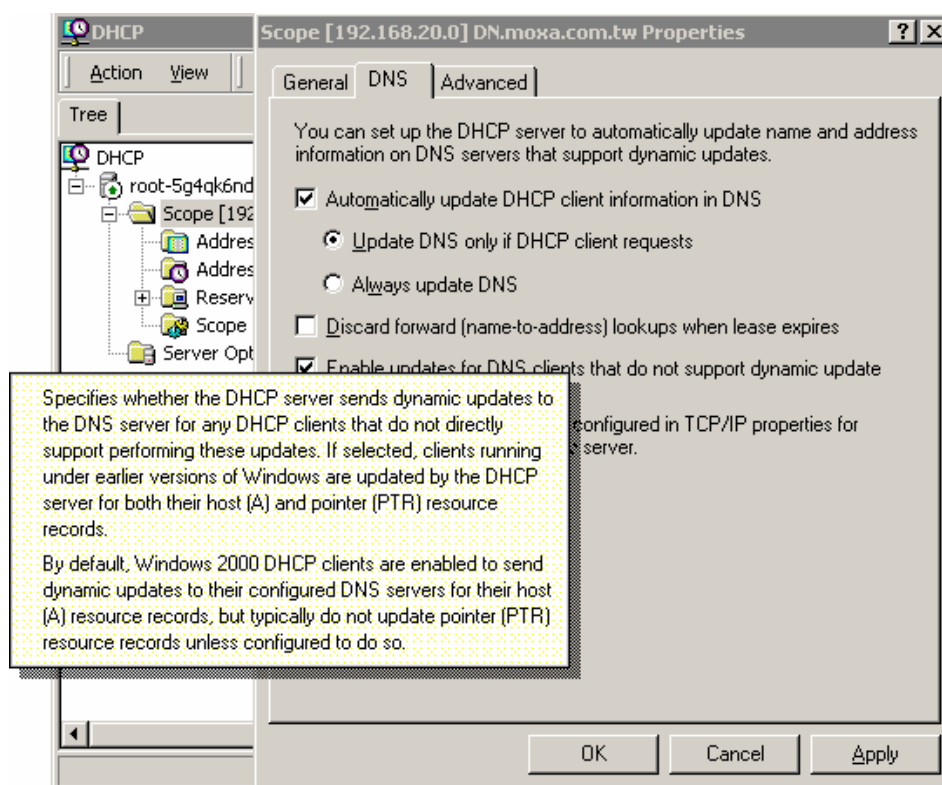
Ниже приведено общее описание функции:

1. NPort 6000 отправляет запрос на получение IP-адреса на DHCP-сервер. Одновременно он отправляет свое доменное имя (в примере – “NP6000”) в соответствии с функцией 12 стандарта.
2. DHCP-сервер в ответ отправляет IP-адрес, назначенный NPort'у 6000, вместе с своим доменным именем (в примере “moxa.com”) и IP-адресами DNS-серверов и шлюза.
3. Если NPort 6000 имеет разрешение на обновление имени на DNS-сервере, он будет зарегистрирован в службе FQDN (Fully Qualified Domain Name) с DNS-сервером. Имя Nport'а 6000 будет иметь формат [имя сервера.имя домена] (в примере “NP6000.moxa.com”).
4. Если NPort 6000 не имеет разрешения на обновление DNS-сервера, то для этого может использоваться DHCP-сервер. DHCP-сервер регистрирует DNS-сервер с PTR RR (запись запроса на доменное имя с IP-адресом).



На скриншоте показано, как в DHCP настроить обновление имени устройства в DNS.

В настоящий момент NPort 6000 поддерживает DNS-службу DynDNS. Более детальную информацию см. на сайте <https://www.dyndns.com>.



Настройка

DDNS (по умолчанию = Disable): Включение/отключение функции DDNS.

Server address (по умолчанию = DynDns.org): В настоящий момент это единственный вариант адреса сервера.

Host name: В данном поле введите имя, созданное на www.dyndns.com. NPort 6000 будет обновлять свое имя на DynDNS-сервере.

Username: Логин для авторизации.

Password: Пароль для авторизации.

Приложение D Стандартная нумерация портов

В данном приложении приводится список стандартных номеров портов, которые не должны совпадать с номерами, назначаемыми портам NPort'ам 6000. См. также RFC 1700 или представленный ниже список от IANA (полномочный орган по цифровым адресам в Интернет):

Номера портов собраны в три группы: Широко известные порты, Зарегистрированные порты, и Порты, используемые по своему усмотрению.

Широко известные (занятые) порты: с 0 по 1023.

Зарегистрированные порты: с 1024 по 49151.

Свободные порты: с 49152 по 65535.

Первая группа назначает IANA и в большинстве систем могут использоваться только служебными процессами или программы, выполняемые от имени пользователей с высоким приоритетом. Таблица ниже показывает распространенные номера портов. Более детально см. на сайте: <http://www.iana.org/assignments/port-numbers>.

ТСР-порт	Служба
0	Зарезервирован
1	Для обслуживания нескольких служб на одном и том же ТСР порту
2	Управляющая утилита
7	Протокол ECHO — предназначен для тестирования связи путём отправки данных на сервер и получения от него их же в неизменном виде
9	Протокол DISCARD — предназначен для тестирования связи путём отправки данных на сервер, который отбрасывает принятое, не отправляя никакого ответа
11	Протокол SYSTAT — выдаёт список активных пользователей в операционной системе
13	Протокол DAYTIME — предназначен для тестирования связи путём получения от сервера текущих даты и времени в текстовом виде
15	Состояние сети (Протокол NETSTAT)
20	Порт данных FTP
21	Порт команд FTP
23	Телнет
25	SMTP (Простой протокол передачи почты) - используется для пересылки почтовых сообщений между серверами. Сообщения отправляются в виде простого незашифрованного текста

37	Time protocol — используется для синхронизации времени (старый)
42	Имя хоста (названия сервера)
43	Ник
49	Протокол входа хоста
53	DNS (протокол сервера имен)
79	Finger - сетевой протокол, предназначенный для предоставления информации о пользователях удалённого компьютера.
80	HTTP
119	<u>Network News Transfer Protocol</u> (NNTP) — используется для отправки сообщений новостных рассылок
123	<u>Network Time Protocol</u> (NTP) —используется для синхронизации времени
213	IPX (<i>Internetwork Packet Exchange</i>) — протокол сетевого уровня модели OSI в стеке протоколов SPX
160-223	Зарезервировано для будущих целей

UDP-порт	Служба
0	Зарезервирован
2	Управляющая утилита
7	Протокол ECHO — предназначен для тестирования связи путём отправки данных на сервер и получения от него их же в неизменном виде
9	Протокол DISCARD — предназначен для тестирования связи путём отправки данных на сервер, который отбрасывает принятое, не отправляя никакого ответа
11	Протокол SYSTAT — выдаёт список активных пользователей в операционной системе
13	Протокол DAYTIME — предназначен для тестирования связи путём получения от сервера текущих даты и времени в текстовом виде
35	Протокол приватного сервера печати <u>printer server</u>
39	Resource Location Protocol — протокол поиска ресурсов (RLP) — служит для нахождения серверов, предоставляющих услуги верхнего уровня
42	Протокол сервера имён - Host Name Server Protocol

43	Протокол WHOIS
49	Протокол входа хоста
53	DNS (протокол сервера имен)
69	<u>Trivial File Transfer Protocol</u> (TFTP) — тривиальный FTP — этот протокол применяется например для развёртывания установки операционной системы на большое количество компьютеров в сетях предприятий.
70	Протокол <u>Gopher</u>
79	Finger - сетевой протокол, предназначенный для предоставления информации о пользователях удалённого компьютера.
80	HTTP
107	Удаленная телнет-служба
111	Sun Remote Procedure Call (Sunrpc)
119	<u>Network News Transfer Protocol</u> (NNTP) — используется для отправки сообщений новостных рассылок
123	<u>Network Time Protocol</u> (NTP) —используется для синхронизации времени
161	SNMP (Simple Network Mail Protocol)
162	SNMP Traps -прерывания
213	IPX (<i>Internetwork Packet Exchange</i>) — протокол сетевого уровня модели OSI в стеке протоколов SPX

Приложение Е SNMP-агент с поддержкой MIB II и RS-232

NPort 6000 имеет встроенную поддержку SNMP-агентов, SNMP-прерываний, RFC1317, групп RS-232 и RFC 1213 MIB-II. В таблицах ниже приведены MIB-II-группы, а также соответствующие переменные для NPort'a 6000.

RFC1213 MIB-II – SNMP-переменные

System MIB	Interfaces MIB	IP MIB	ICMP MIB
sysDescr	ifNumber	ipForwarding	icmpInMsgs
sysObjectID	ifIndex	ipDefaultTTL	icmpInErrors
sysUpTime	ifDescr	ipInReceives	icmpInDestUnreachs
sysContact	ifType	ipInHdrErrors	icmpInTimeExcds
sysName	ifMtu	ipInAddrErrors	icmpInParmProbs
sysLocation	ifSpeed	ipForwDatagrams	icmpInSrcQuenchs
sysServices	ifPhysAddress	ipInUnknownProtos	icmpInRedirects
	ifAdminStatus	ipInDiscards	icmpInEchos
	ifOperStatus	ipInDelivers	icmpInEchoReps
	ifLastChange	ipOutRequests	icmpInTimestamps
	ifInOctets	ipOutDiscards	icmpTimestampReps
	ifInUcastPkts	ipOutNoRoutes	icmpInAddrMasks
	ifInNUcastPkts	ipReasmTimeout	icmpInAddrMaskReps
	ifInDiscards	ipReasmReqds	icmpOutMsgs
	ifInErrors	ipReasmOKs	icmpOutErrors
	ifInUnknownProtos	ipReasmFails	icmpOutDestUnreachs
	ifOutOctets	ipFragOKs	icmpOutTimeExcds
	ifOutUcastPkts	ipFragFails	icmpOutParmProbs
	ifOutNUcastPkts	ipFragCreates	icmpOutSrcQuenchs
	ifOutDiscards	ipAdEntAddr	icmpOutRedirects
	ifOutErrors	ipAdEntIfIndex	icmpOutEchos
	ifOutQLen	ipAdEntNetMask	icmpOutEchoReps
	ifSpecific	ipAdEntBcastAddr	icmpOutTimestamps
		ipAdEntReasmMaxSize	icmpOutTimestampReps
		ipRouteDest	icmpOutAddrMasks
		ipRouteIfIndex	icmpOutAddrMaskReps
		ipRouteMetric1	
		ipRouteMetric2	
		ipRouteMetric3	
		ipRouteMetric4	
		ipRouteNextHop	
		ipRouteType	
		ipRouteProto	

System MIB	Interfaces MIB	IP MIB	ICMP MIB
		ipRouteAge	
		ipRouteMask	
		ipRouteMetric5	
		ipRouteInfo	
		ipNetToMediaIfIndex	
		ipNetToMediaPhysAddress	
		ipNetToMediaNetAddress	
		ipNetToMediaType	
		ipRoutingDiscards	

Address Translation MIB	TCP MIB	UDP MIB	SNMP MIB
atIfIndex	tcpRtoAlgorithm	udpInDatagrams	snmpInPkts
atPhysAddress	tcpRtoMin	udpNoPorts	snmpOutPkts
atNetAddress	tcpRtoMax	udpInErrors	snmpInBadVersions
	tcpMaxConn	udpOutDatagrams	snmpInBadCommunityNames
	tcpActiveOpens	udpLocalAddress	snmpInBadCommunityUses
	tcpPassiveOpens	udpLocalPort	snmpInASNParseErrs
	tcpAttemptFails		snmpInTooBig
	tcpEstabResets		snmpInNoSuchNames
	tcpCurrEstab		snmpInBadValues
	tcpInSegs		snmpInReadOnly
	tcpOutSegs		snmpInGenErrs
	tcpRetransSegs		snmpInTotalReqVars
	tcpConnState		snmpInTotalSetVars
	tcpConnLocalAddress		snmpInGetRequests
	tcpConnLocalPort		snmpInGetNexts
	tcpConnRemAddress		snmpInSetRequests
	tcpConnRemPort		snmpInGetResponses
	tcpInErrs		snmpInTraps
	tcpOutRsts		snmpOutTooBig
			snmpOutNoSuchNames
			snmpOutBadValues
			snmpOutGenErrs

Address Translation MIB	TCP MIB	UDP MIB	SNMP MIB
			snmpOutGetRequests
			snmpOutGetNexts
			snmpOutSetRequests
			snmpOutGetResponses
			snmpOutTraps
			snmpEnableAuthenTraps
			snmpSilentDrops
			snmpProxyDrops

RFC1317 RS-232 Like Groups

RS-232 MIB	Async Port MIB
rs232Number	rs232AsyncPortIndex
rs232PortIndex	rs232AsyncPortBits
rs232PortType	rs232AsyncPortStopBits
rs232PortInSigNumber	rs232AsyncPortParity
rs232PortOutSigNumber	
rs232PortInSpeed	
rs232PortOutSpeed	

Input Signal MIB	Output Signal MIB
rs232InSigPortIndex	rs232OutSigPortIndex
rs232InSigName	rs232OutSigName
rs232InSigState	rs232OutSigState

Moxa-NP6000-MIB

overview	basicSetting	networkSetting	opModeSetting
modelName	serverName	ipConfiguration	portIndex
serialNumber	serverLocation	sysIpAddress	portApplication
firmwareVersion	timeZone	netMask	portMode
macAddress	localTime	defaultGateway	
viewLanSpeed	timeserver	dnsServer1IpAddr	
viewLanModuleSpeed		dnsServer2IpAddr	
upTime		pppoeUserAccount	

overview	basicSetting	networkSetting	opModeSetting
moduleType		pppoePassword	
		winsFunction	
		winsServer	
		lan1Speed	
		routingProtocol	
		gratuitousArp	
		gratuitousArpSendPerios	

deviceControl Mode	socket Mode
deviceControlTcpAliveCheck	socketTcpAliveCheck
deviceControlMaxConnection	socketInactivityTime
deviceControlIgnoreJammedIp	socketMaxConnection
deviceControlAllowDriverControl	socketIgnoreJammedIp
deviceControlSecure	socketAllowDriverControl
deviceControlLocalTcpPort	socketSecure
deviceControlConnectionDownRTS	socketLocalTcpPort
deviceControlConnectionDownDTR	socketCmdPort
	socketTcpServerConnectionDownRTS
	socketTcpServerConnectionDownDTR
	socketTcpClientDestinationAddress1
	socketTcpClientDestinationPort1
	socketTcpClientDestinationAddress2
	socketTcpClientDestinationPort2
	socketTcpClientDestinationAddress3
	socketTcpClientDestinationPort3
	socketTcpClientDestinationAddress4
	socketTcpClientDestinationPort4
	socketTcpClientDesignatedLocalPort1
	socketTcpClientDesignatedLocalPort2
	socketTcpClientDesignatedLocalPort3
	socketTcpClientDesignatedLocalPort4
	socketTcpClientConnectionControl
	socketUdpDestinationAddress1Begin
	socketUdpDestinationAddress1End
	socketUdpDestinationPort1

deviceControl Mode	socket Mode
	socketUdpDestinationAddress2Begin
	socketUdpDestinationAddress2End
	socketUdpDestinationPort2
	socketUdpDestinationAddress3Begin
	socketUdpDestinationAddress3End
	socketUdpDestinationPort3
	socketUdpDestinationAddress4Begin
	socketUdpDestinationAddress4End
	socketUdpDestinationPort4
	socketUdpLocalListenPort

pairConnection Mode	ethernetModem Mode
pairConnectionTcpAliveCheck	ethernetModemTcpAliveCheck
pairConnectionSecure	ethernetModemTcpPort
pairConnectionDestinationAddress	
pairConnectionDestinationPort	
pairConnectionTcpPort	

terminal Mode	reverseTerminal Mode
terminalTcpAliveCheck	reverseTerminalTcpAliveCheck
terminalInactivityTime	reverseTerminalInactivityTime
terminalAutoLinkProtocol	reverseTerminalTcpPort
terminalPrimaryHostAddress	reverseTerminalAuthenticationType
terminalSecondHostAddress	reverseTerminalMapKeys
terminalTelnetTcpPort	
terminalSshTcpPort	
terminalType	
terminalMaxSessions	
terminalChangeSession	
terminalQuit	
terminalBreak	
terminalInterrupt	
terminalAuthenticationType	
terminalAutoLoginPrompt	
terminalPasswordPrompt	

terminal Mode	reverseTerminal Mode
terminalLoginUserName	
terminalLoginPassword	

printer Mode	dial Mode	dataPacking
printerTcpAliveCheck	dialTERMBINMode	portPacketLength
printerTcpPort	dialPPPDMode	portDelimiter1Enable
printerGroup	dialSLIPDMode	portDelimiter1
printerQueueNameRaw	dialAuthType	portDelimiter2Enable
printerQueueNameASCII	dialDisconnectBy	portDelimiter2
printerAppendFromFeed	dialDestinationIpAddress	portDelimiterProcess
	dialSourceIpAddress	portForceTransmit
	dialIpNetmask	
	dialTcpIpCompression	
	dialInactivityTime	
	dialLinkQualityReport	
	dialOutgoingPAPID	
	dialPAPPassword	
	dialIncomingPAPCheck	

comParamSetting	dataBuffering	modemSetting
portAlias	portBufferingEnable	portEnableModem
portInterface	portBufferingLocation	portInitialString
portBaudRate	portBufferingSDFileSize	portDialUp
portBaudRateManual	portSerialDataLoggingEnable	portPhoneNumber
portDataBits		
portStopBits		
portParity		
portFlowControl		
portFIFO		

welcomeMessage	sysManagement
portEnableWelcomeMessage	enableAccessibleIpList
portMessage	accessibleIpListIndex
	activeAccessibleIpList
	accessibleIpListAddress

welcomeMessage	sysManagement
	accessibleIpListNetmask
	snmpEnable
	snmpContactName
	snmpLocation
	dDNSEnable
	dDNSServerAddress
	dDNSHostName
	dDNSUserName
	dDNSPassword
	hostTableIndex
	hostName
	hostIpAddress
	routeTableIndex
	gatewayRouteTable
	destinationRouteTable
	netmaskRouteTable
	metricRouteTable
	interfaceRouteTable
	userTableIndex
	userNameUserTable
	passwordUserTable
	phoneNumberUserTable
	radiusServerIp
	radiusKey
	udpPortAuthenticationServer
	radiusAccounting
	sysLocalLog
	networkLocalLog
	configLocalLog
	opModeLocalLog
	mailWarningColdStart
	mailWarningWarmStart
	mailWarningAuthFailure
	mailWarningIpChanged
	mailWarningPasswordChanged

welcomeMessage	sysManagement
	trapServerColdStart
	trapServerWarmStart
	trapServerAuthFailure
	alarmServerEthernet1LinkDown
	alarmServerEthernet2LinkDown
	alarmServerEthernet3LinkDown
	mailDCDchange
	trapDCDchange
	alarmDCDchange
	mailDSRchange
	trapDSRchange
	alarmDSRchange
	emailWarningMailServer
	emailRequiresAuthentication
	emailWarningUserName
	emailWarningPassword
	emailWarningFromEmail
	emailWarningFirstEmailAddr
	emailWarningSecondEmailAddr
	emailWarningThirdEmailAddr
	emailWarningFourthEmailAddr
	snmpTrapReceiverIp
	trapVersion
	httpConsole
	httpsConsole
	telnetConsole
	sshConsole
	lcmReadOnlyProtect
	resetButtonFunction
	loadFactoryDefaultSetting

sysStatus	saveConfiguration	restart
remoteIpIndex	saveConfig	restartPorts
monitorRemoteIp		restartSystem
monitorTxCount		
monitorRxCount		
monitorTxTotalCount		
monitorRxTotalCount		
monitorDSR		
monitorDTR		
monitorRTS		
monitorCTS		
monitorDCD		
monitorErrorCountFrame		
monitorErrorCountParity		
monitorErrorCountOverrun		
monitorErrorCountBreak		
monitorBaudRate		
monitorDataBits		
monitorParity		
monitorRTSCTSFlowControl		
monitorXONXOFFFlowControl		
monitorFIFO		
monitorInterface		
relayOutputEthernet1LinkDown		
ethernet1LinkDownAcknowledge		
relayOutputEthernet2LinkDown		
ethernet2LinkDownAcknowledge		
relayOutputEthernet3LinkDown		
ethernet3LinkDownAcknowledge		
portDCDChangedStatus		
portDCDChangedAcknowledge		
portDSRChangedStatus		
portDSRChangedAcknowledge		

Приложение F RADIUS-сервер

Управление разнотипными последовательными каналами и группами модемов для большого числа пользователей требует значительной поддержки со стороны сетевых администраторов. Если модемы подключаются к глобальным сетям, должное внимание необходимо уделять вопросам безопасности, ограничения доступа. Все это наилучшим образом достигается за счет создания единой базы, содержащих пользователей, имеющих доступ (проверка их имен и паролей), а также детальную информацию по типу сервисов, предоставляемых каждому пользователю (например, SLIP, PPP, Telnet, rlogin). NPort 6000 поддерживает протокол RADIUS, для которого требуется одна база для управления доступом удаленных пользователей.

Данное приложение содержит следующие разделы:

- **О протоколе RADIUS**
 - Определение
 - Архитектура «Клиент/Сервер»
- **Настройка NPort 6000**
 - Задание IP-адреса RADIUS-сервера
 - Настройка последовательного порта
- **Настройка UNIX-хостов**
- **Настройка в ОС Windows NT**
- **Настройка в ОС Windows 2000**
- **Настройка в ОС Windows 2003**

О протоколе RADIUS

Определение

RADIUS – Remote Authentication Dial-up User Service – стандарт для централизации идентификации, авторизации удаленных пользователей и учета пользовательских ресурсов.

В данном приложении кратко описывается работа RADIUS. Когда пользователь пытается получить доступ к удаленному устройству, то это устройство связывается с центральным RADIUS-сервером для установления прав пользователя на подключение к LAN. RADIUS-сервер выполняет авторизацию и в ответ посылает результат – либо одобрение, либо отказ в авторизации. Если пользователь авторизован, то он получает доступ к сети; если нет, то сервер разрывает соединение пользователя. RADIUS-сервер поддерживает также работу с пользовательскими аккаунтами, однако удаленный сервер также должен их поддерживать.

С технологией RADIUS сетевому администратору или интернет-провайдеру нужна только одна центральная база данных, в которую будут занесены все удаленные пользователи. Это существенно облегчает администрирование большого количества dial-up-пользователей.

Архитектура «Клиент/Сервер»

RADIUS использует архитектуру «клиент-сервер». Коммуникационные устройства, такие как NPort 6000, играют активную роль, в то время как RADIUS-серверы – пассивную.

Когда удаленный хост связывается с Nport'ом 6000, требуется ввод ID пользователя и пароля.

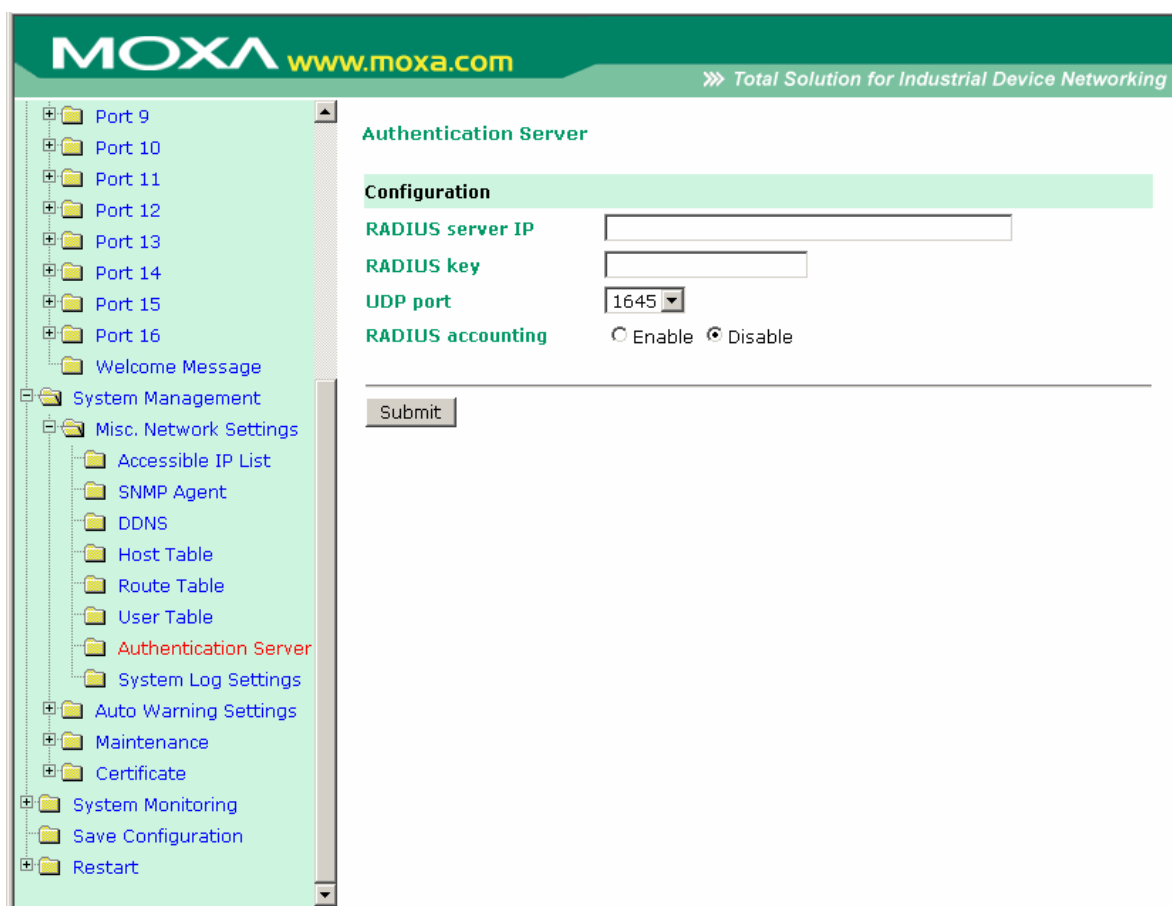
После получения ID пользователя и пароля NPort 6000 отправляет эту информацию на заданный RADIUS-сервер. В данный момент пользователь все еще не имеет доступа к сети.

RADIUS-сервер производит сверку логина и пароля по внутренней базе данных и по сети посылает одобрение/отказ для доступа пользователя.

Если NPort 6000 получает сообщение-одобрение (асепт) от RADIUS-сервера, удаленному пользователю разрешается доступ к сети. В противном случае NPort 6000 либо закрывает соединение с пользователем, либо предлагает повторить попытку входа через некоторый промежуток времени.

Настройка NPort 6000

Задание IP-адреса RADIUS-сервера



RADIUS server IP: IP-адрес RADIUS-сервера.

RADIUS key: Пароль, используемый бддя доступа

UDP port: Назначенный UDP-порт RADIUS-сервера

RADIUS accounting: Включение/отключение аккаунта на RADIUS'e

Настройка последовательного порта

RADIUS – эффективный способ для dial-up-служб. Кроме dial-up-служб (PPP, SLIP и Dynamic) NPort 6000 позволяет использовать технологию RADIUS для терминальных приложений и консольного управления. Это задается параметром Authentication type при выборе режима работы (operation mode) конкретного порта. См. главу 7 – подробнее о настройках.

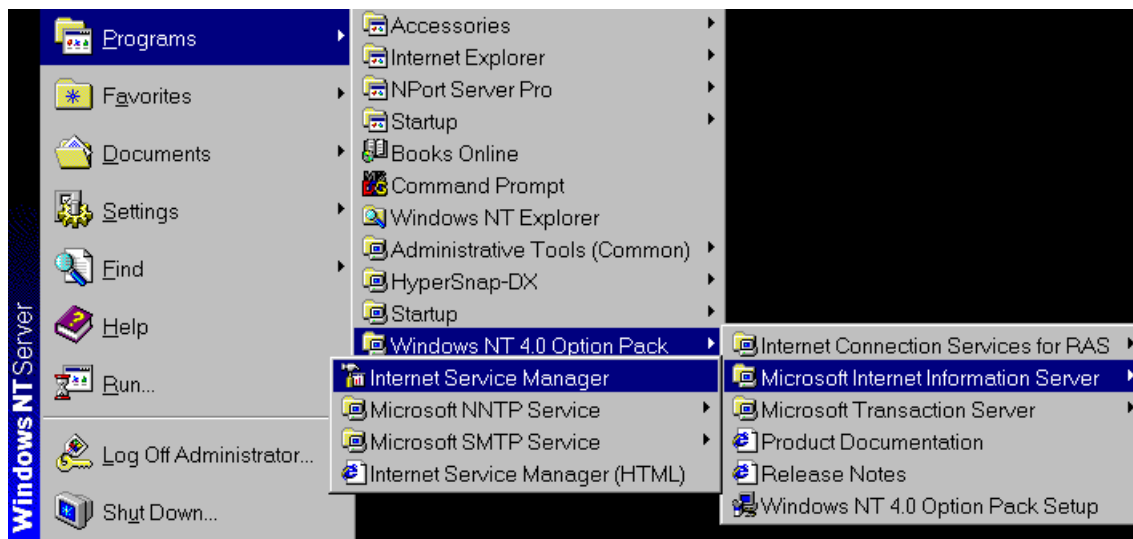
Настройка UNIX-хостов

Производители Мохы рекомендуют использовать FreeRADIUS-сервер для ОС UNIX. FreeRADIUS – один из первых RADIUS-серверов, открытая система и одна из 5 лидирующих в мире. Она эффективна как для небольших систем, требующих незначительного объема памяти, так и для систем с миллионами пользователей. Является достаточно быстрой, гибкой, настраиваемой и поддерживает больше протоколов аутентификации, чем многие платные серверы.

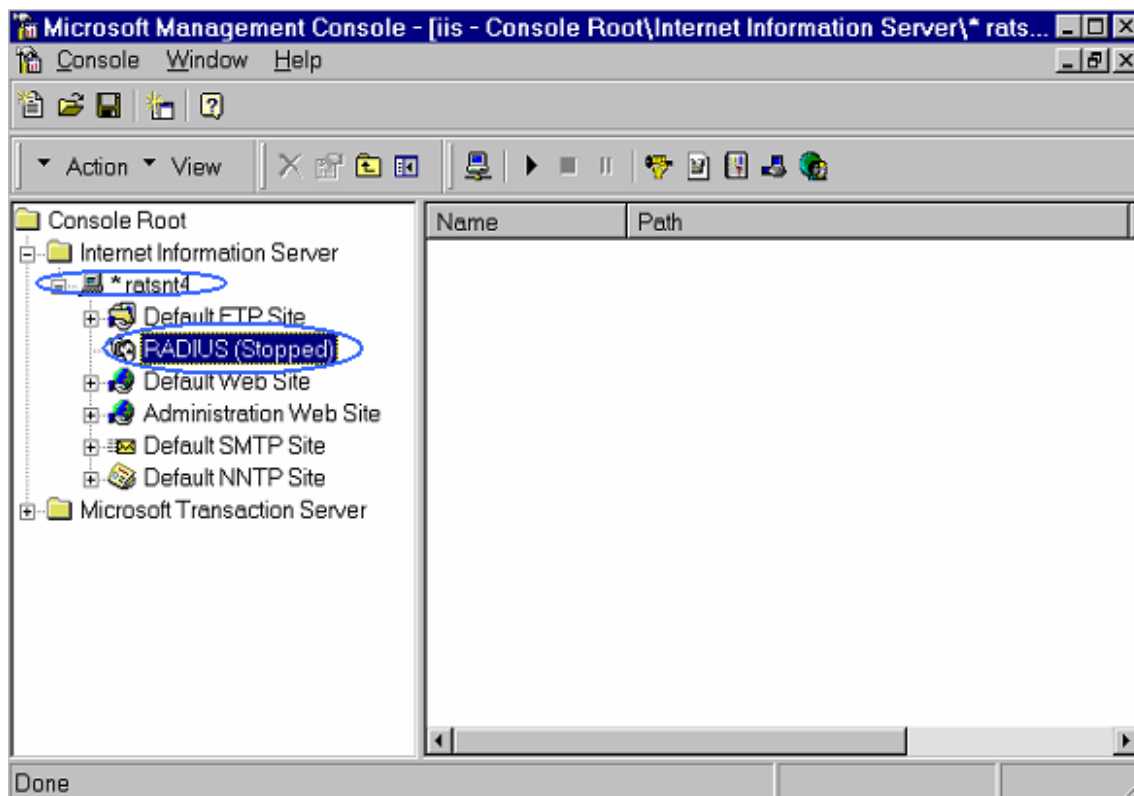
Сервер доступен на основе лицензии GNU General Public License (GPL), это означает, что программу можно свободно скачать и установить. FreeRADIUS можно скачать по ссылке: www.freeradius.com.

Настройка в ОС Windows NT

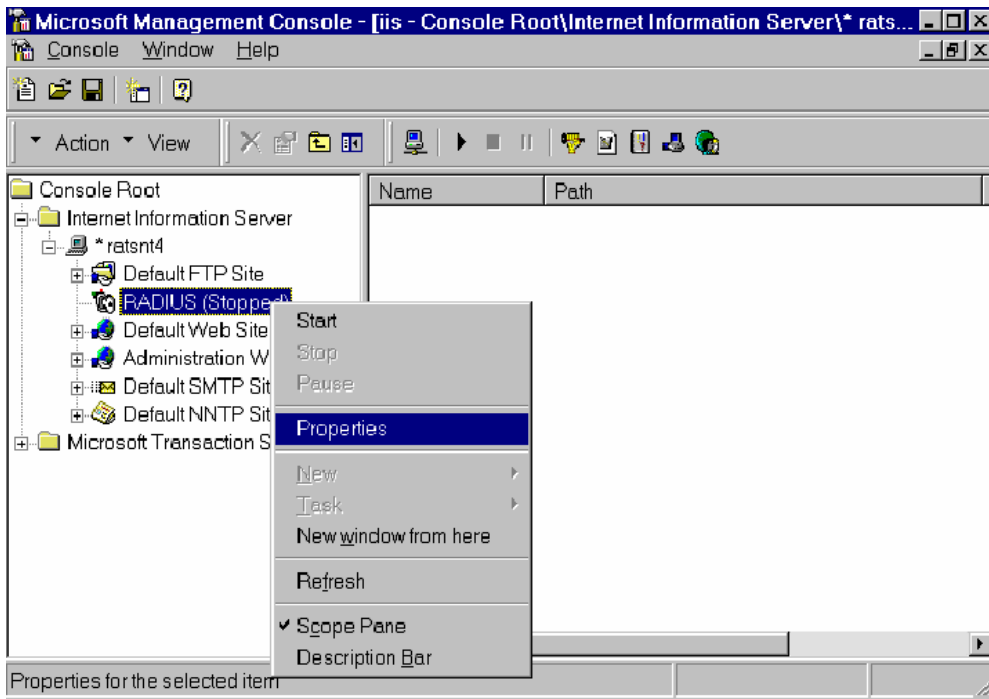
1. Установите Windows NT OPTION PACK 4.0 на сервер с Windows NT server.
2. Откройте меню **Пуск**→**Программы**→**Windows NT 4.0 Option Pack**→**Microsoft Internet Information Server**→**Management Console Manager**.



3. В окне навигации (слева) зайдите на вкладку Console Root→Internet Information Server. Должно быть видно имя Вашего компьютера.
4. Найдите слева имя своего компьютера и щелкните на нем, правее появится информация о RADIUS.



- Щелкните правой кнопкой мыши по RADIUS и выберите пункт Properties.

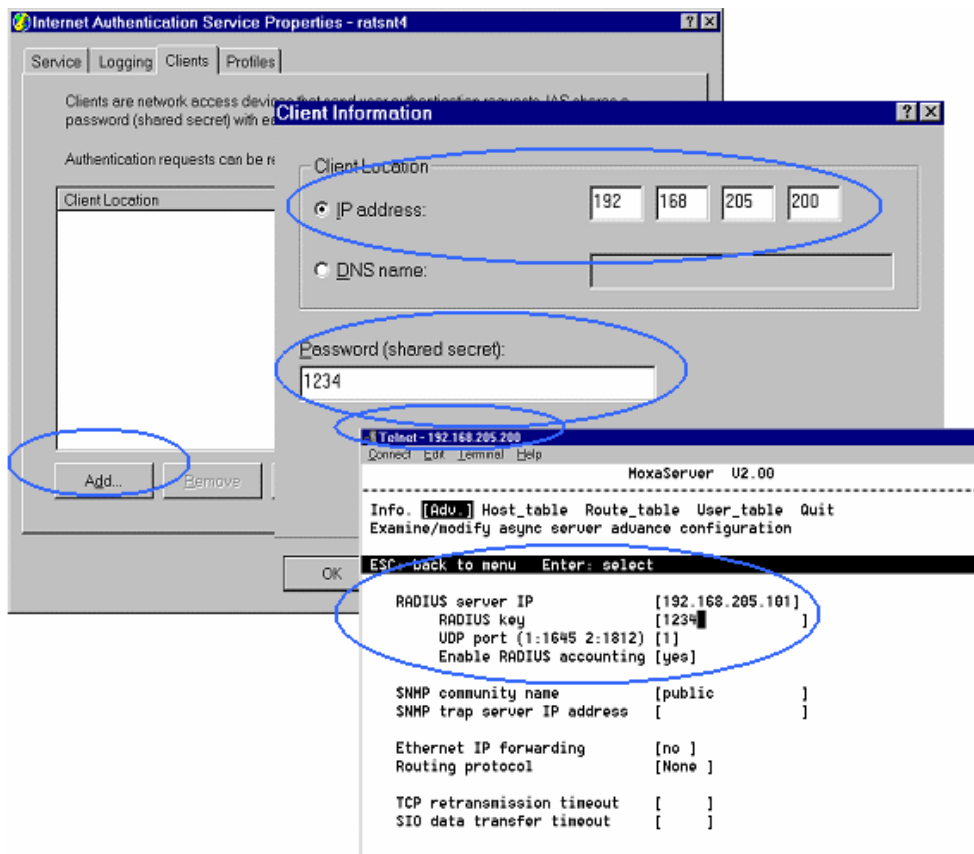


- Выберите вкладку **Service**. Проверьте, чтобы назначенные RADIUS-порты соответствовали Вашей конфигурации:

[Authentication] 1645 или 1812

[Accounting] 1646 или 1813

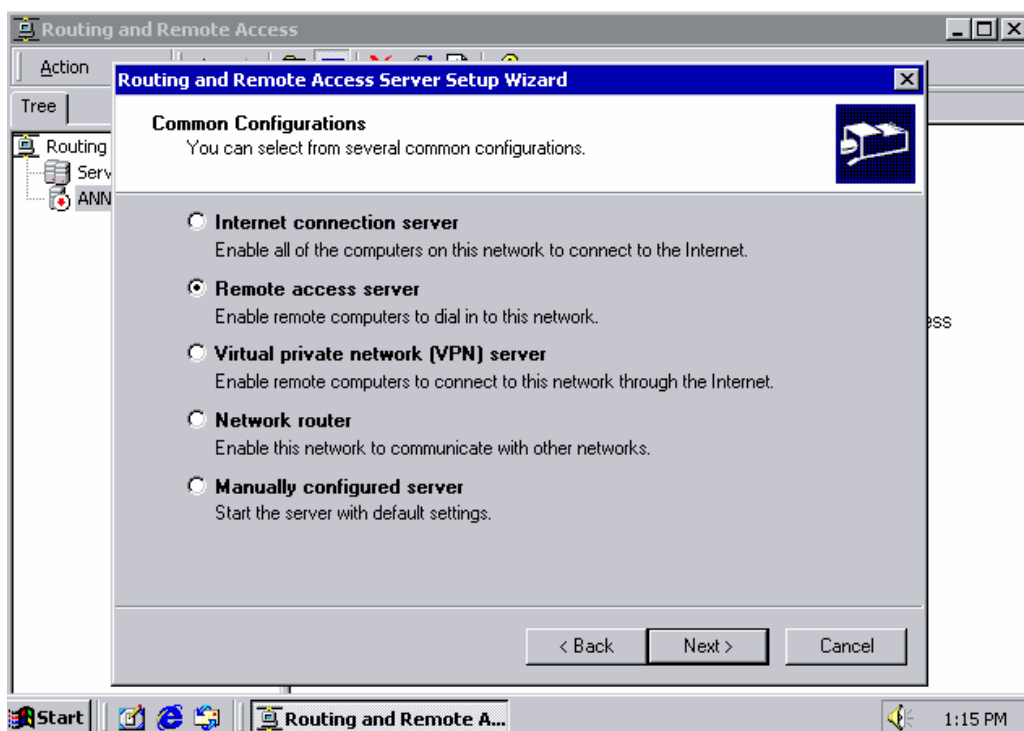
- Перейдите на вкладку **Client** и затем нажмите **Add**. Введите IP-адрес NPort'a 6000 в поле IP address. Введите ключ к RADIUS-серверу в поле Password. Этот параметр должен совпадать с тем, что было указано в настройках NPort'a 6000.



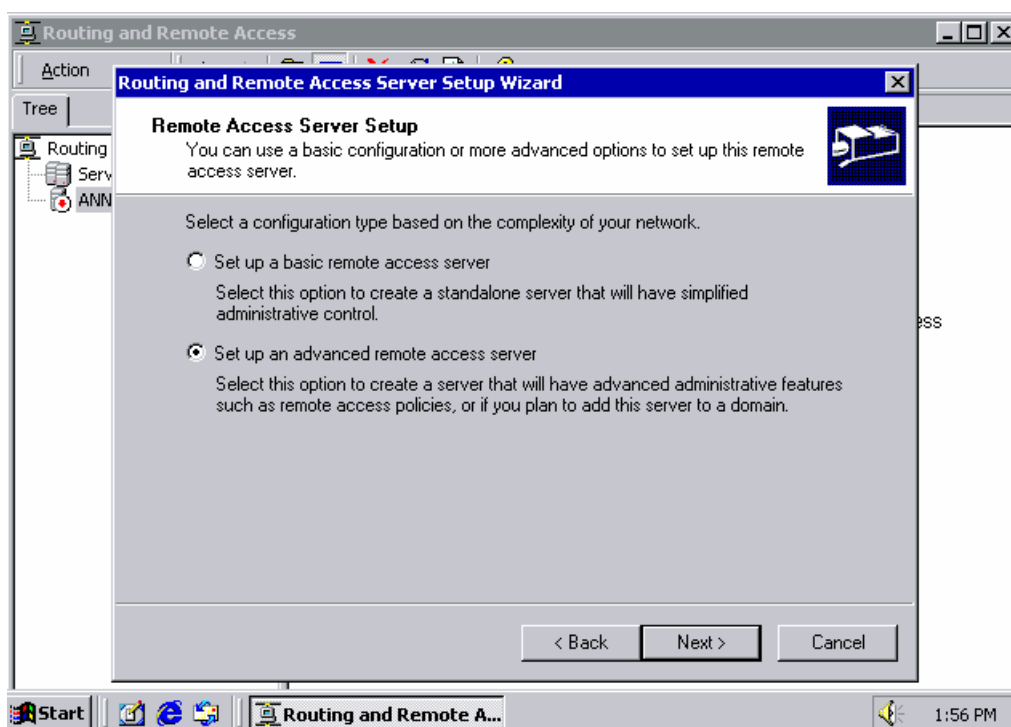
8. Нажмите кнопку **Apply**.
9. Щелкните правой кнопкой мыши на **RADIUS** в левой части окна – выберите пункт **Start**. RADIUS-сервер запустится.

Настройка в ОС Windows 2000

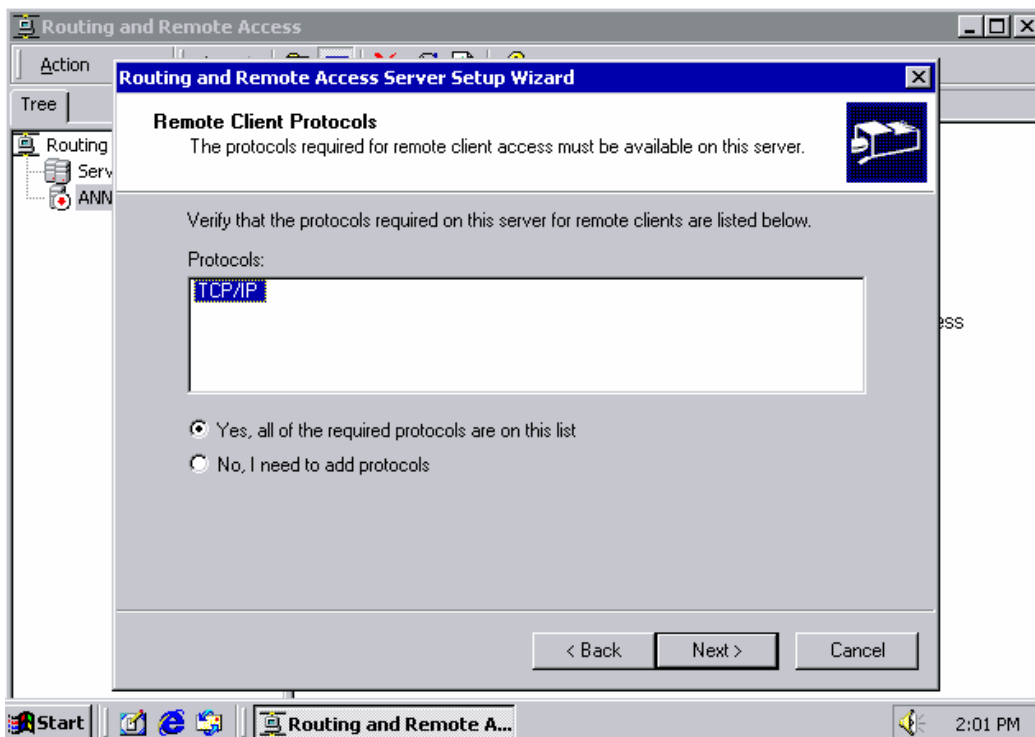
1. Откройте меню **Пуск**→**Программы**→**Administrative Tools**→**Routing and Remote Access**.
2. Щелкните правой кнопкой **Server (Local)** и выберите **Configure and Enable Routing Access**. Нажмите **Next** для продолжения.
3. Выберите **Remote access server** и нажмите **Next** для продолжения.



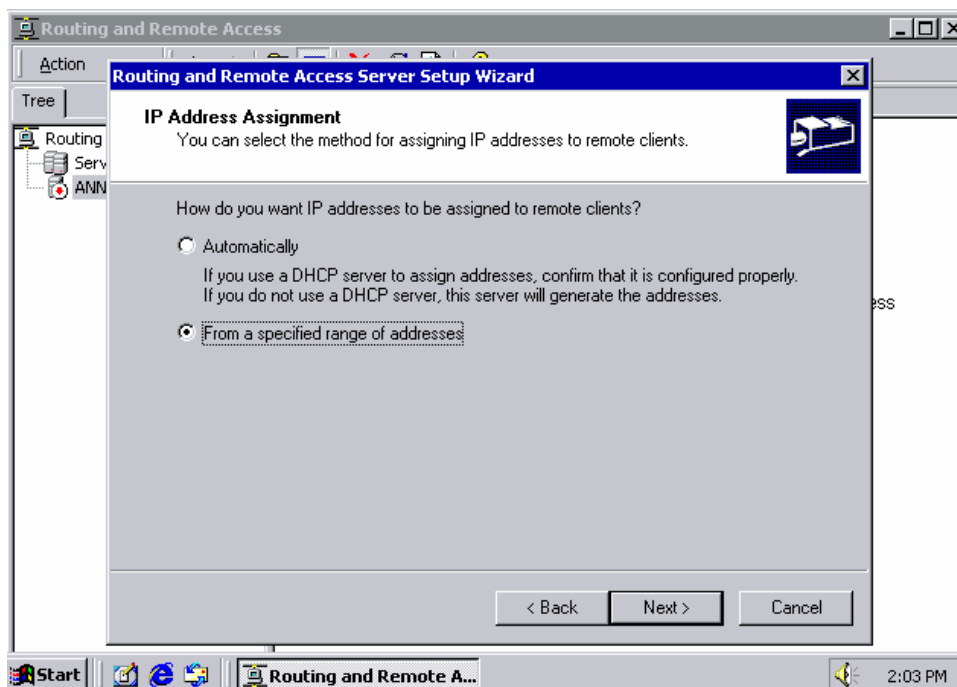
4. Выберите **Set up an advanced remote access server** и нажмите **Next** для продолжения.

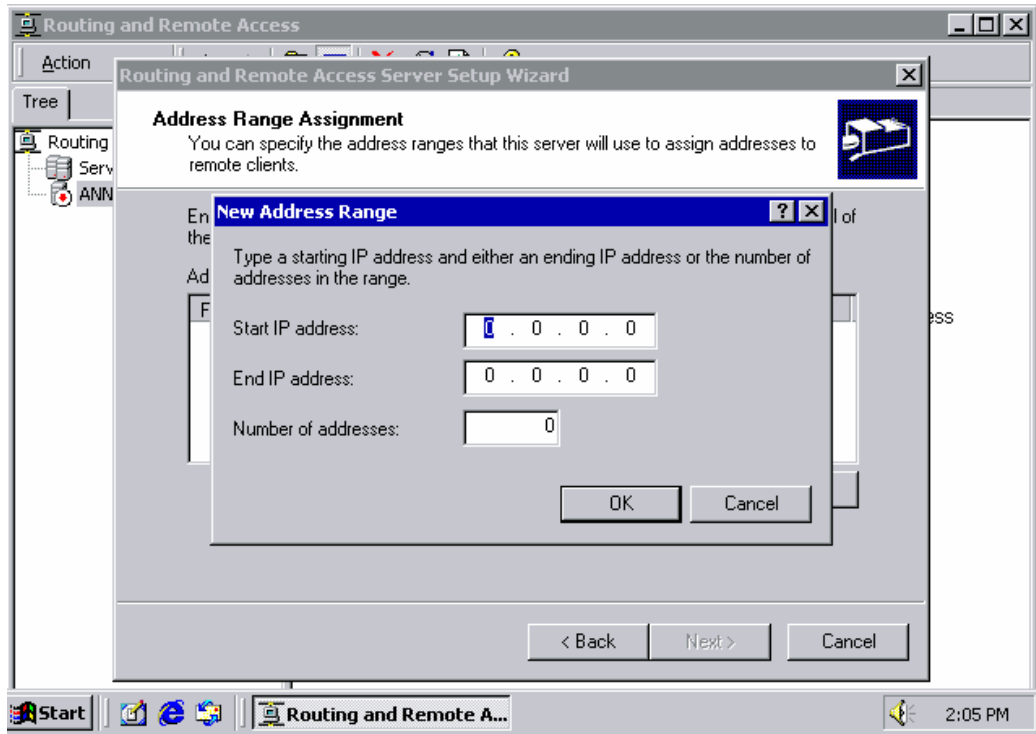


5. Выберите протокол **TCP/IP protocol** и нажмите **Next** для продолжения.

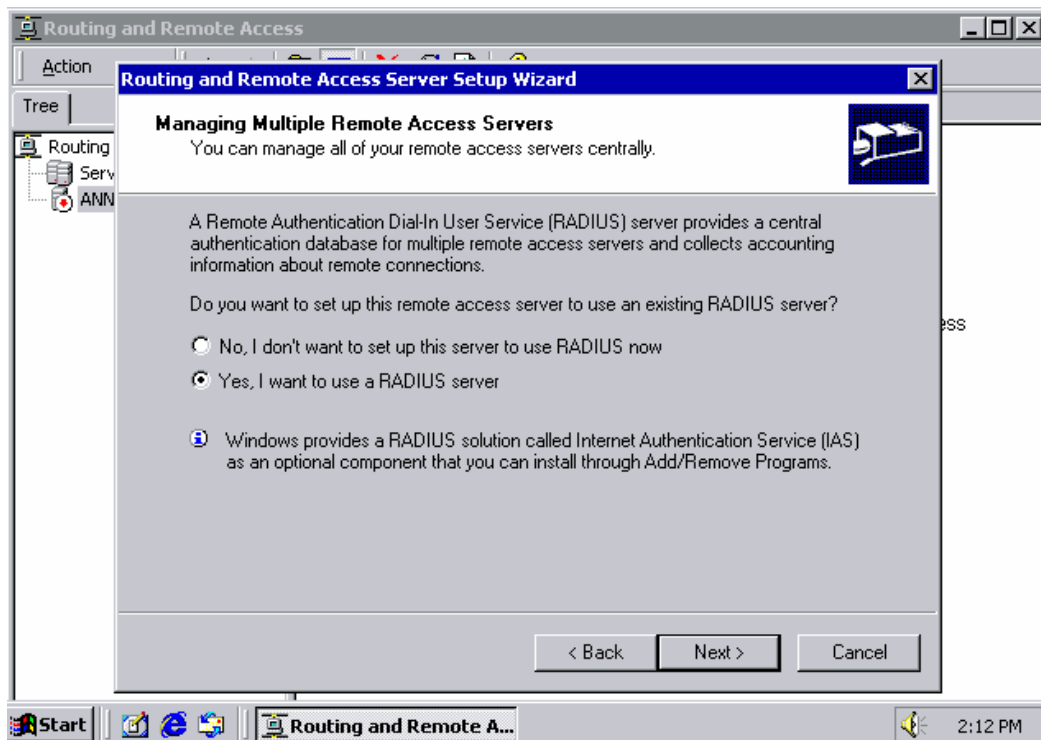


6. Укажите способ определения Вашего IP-адреса, как показано на рисунках ниже:





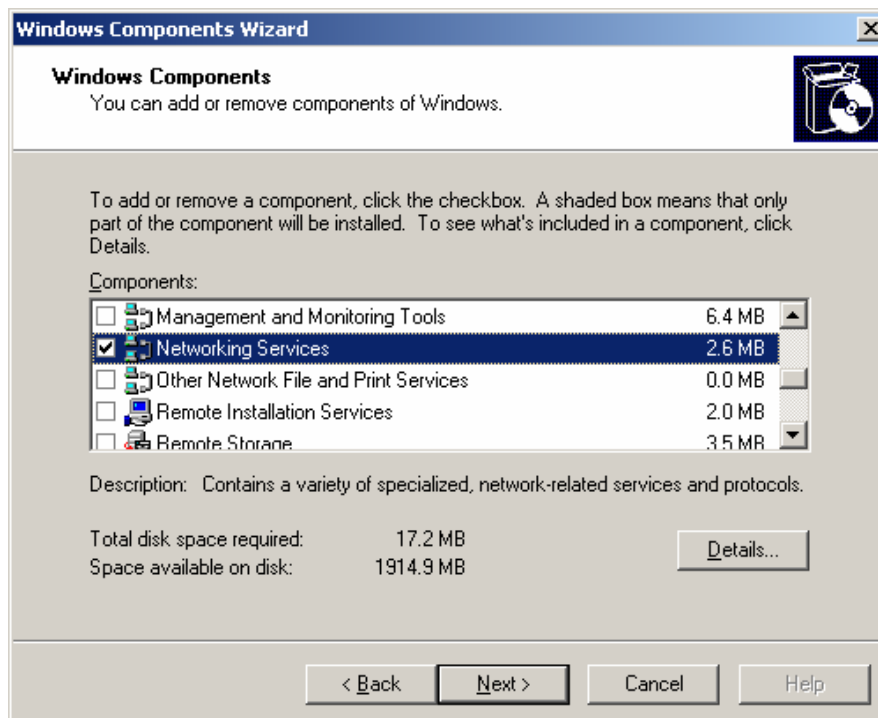
7. Выберите **Yes, I want to use a RADIUS server** и нажмите **Next**.



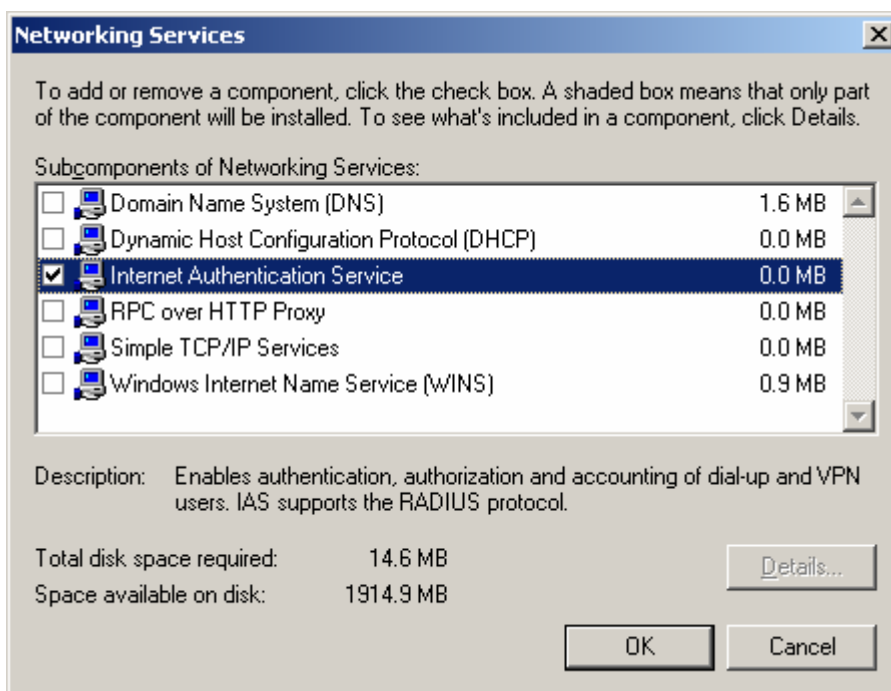
Настройка в ОС Windows 2003

Windows 2003 использует службу IAS вместо RADIUS. Поэтому нужно сначала установить эту службу для использования RADIUS в ОС Windows 2003 (Она по умолчанию не установлена).

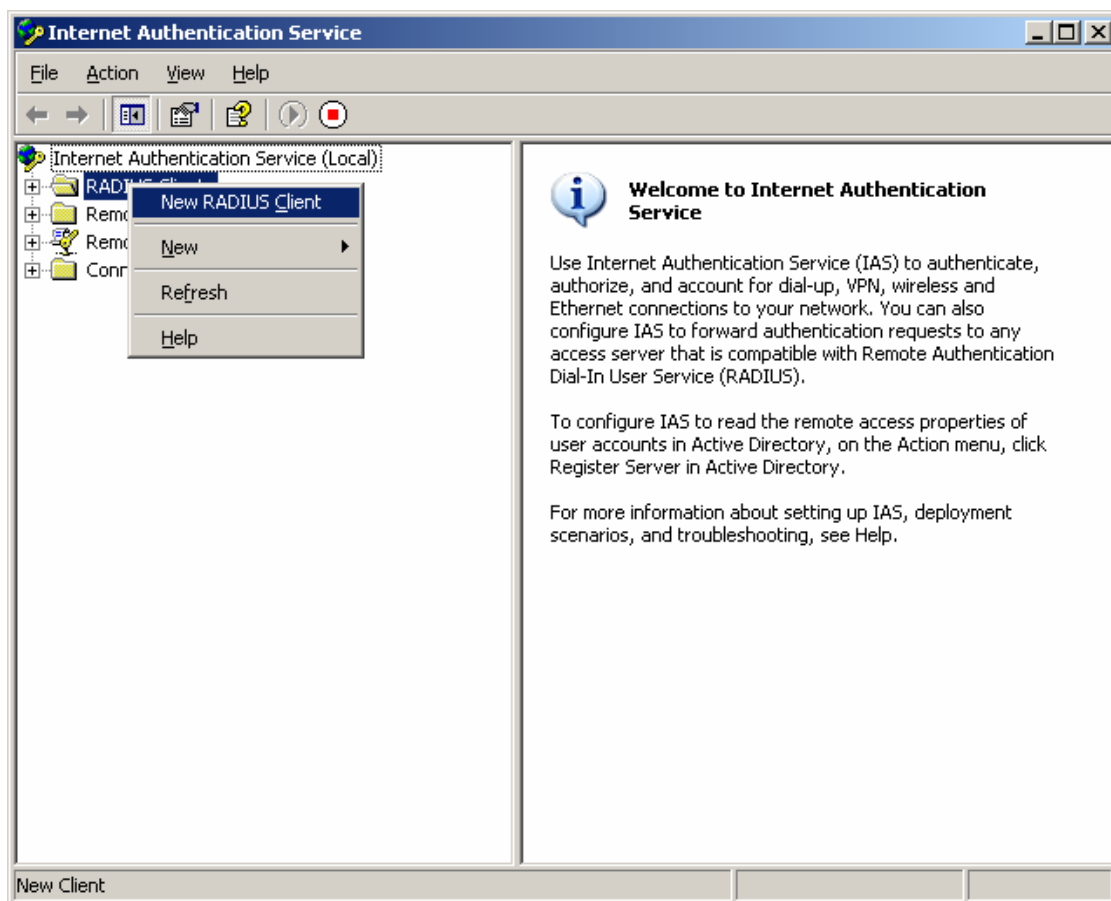
1. Откройте **Start**→**Add or Remove Programs**→**Add/Remove Windows Components**.
2. Выберите в мастере установки пункт **Networking Services**.



3. Выберите **Details** и затем **Internet Authentication Service**. Продолжите установку, нажимая **ОК** до ее завершения.



4. После завершения установки запустите **Administrative Tools** и **Internet Authentication Service**. Откроется окно, показанное ниже:



5. Выберите пункт **New RADIUS Client** для добавления нового RADIUS-клиента. Теперь можно использовать эту функцию.