

NetXpert NXI-3011, v2

СЕРИЯ ПРОМЫШЛЕННЫХ КОНВЕРТЕРОВ ИНТЕРФЕЙСОВ

Руководство по эксплуатации

Модели устройств:

- NXI-3011, v2-2T-1D;
- NXI-3011, v2-2T-4D;
- NXI-3011, v2-2GX-4D.

Версия 1.5

© НАТЕКС, 2026

Права на данный документ принадлежат НАТЕКС. НАТЕКС, предоставляя в данном документе максимально точную информацию, не несет никакой ответственности за возможные несоответствия и оставляет за собой право вносить изменения в настоящее руководство без предварительного уведомления заказчиков. При несоответствии настоящего документа фактическому состоянию продукта, заказчик может получить обновления, направив запрос по адресу help@nateks.ru.

ОГЛАВЛЕНИЕ

1.	ПРЕДИСЛОВИЕ	6
1.1.	Задача руководства	6
1.2.	Кому следует использовать данное руководство	6
1.3.	Поддерживаемая платформа	6
2.	ВВЕДЕНИЕ	7
2.1.	Общая информация.....	7
2.2.	Функции.....	8
3.	НАЧАЛО РАБОТЫ	9
3.1.	Внешний вид, передняя и задняя панель.....	9
3.2.	Первая установка.....	10
3.3.	Заводские настройки по умолчанию	10
3.3.1.	Настройки сети по умолчанию	10
3.3.2.	Другие настройки по умолчанию	10
4.	КОНФИГУРАЦИЯ И НАСТРОЙКА	12
4.1.	Конфигурация сетевых параметров через утилиту управления устройством	12
4.2.	Конфигурация через Web-интерфейс	15
4.3.	Конфигурация автоматического назначения IP-адресов с помощью DHCP	17
4.4.	Web Overview.....	17
4.5.	Сетевые настройки	18
4.6.	Serial	19
4.6.1.	Обзор меню COM-порта.....	20
4.6.2.	Конфигурация COM-порта	21
4.6.3.	Конфигурирование COM-порта: Расширенные настройки	22
4.7.	Настройки IPsec Settings	24
4.7.1.	Настройки IPsec Settings.....	28
4.7.2.	IPsec Status	33
4.7.3.	Примеры настроек IPsec.....	33
4.8.	STP	39
4.8.1.	Настройки связующего дерева.....	40
4.8.2.	Параметры коммутатора STP.....	41
4.8.3.	Настройки порта связующего дерева	42
4.9.	Настройки SNMP/ALERT	45
4.10.	Настройки E-Mail	47
4.11.	Настройки журнала	48
4.11.1.	Настройки журнала системы	49
4.11.2.	Настройки журнала COM-порта	50
4.11.3.	Журнал событий	51
4.11.4.	Журнал данных COM Datalog	51

4.12.	Настройка системы	52
4.12.1.	Настройки даты/времени	53
4.12.2.	Настройки администратора	54
4.12.3.	Обновление прошивки	55
4.12.4.	Настройки резервного копирования/восстановления	56
4.12.5.	Ping.....	57
4.13.	Перезагрузка	58
5.	КАНАЛЬНЫЕ РЕЖИМЫ И ПРИЛОЖЕНИЯ	59
5.1.	Конфигурация канального режима.....	59
5.1.1.	Канальный режим: Конфигурирование NetXpert NXI-3011, v2 в качестве TCP-сервера.....	59
5.1.2.	Канальный режим: Конфигурирование NetXpert NXI-3011, v2 в качестве TCP-клиента	63
5.1.3.	Канальный режим NetXpert NXI-3011, v2 в UDP	66
5.2.	Приложения канального режима	69
5.2.1.	Приложение TCP-сервера: Включение виртуального COM	69
5.2.2.	Приложение TCP-сервера: Включение RFC 2217 через Virtual COM.....	69
5.2.3.	Приложение TCP-клиента: Включение Virtual COM	70
5.2.4.	Приложение TCP-клиента: Включение RFC 2217 через Virtual COM	70
5.2.5.	Приложение TCP -сервера: Конфигурирование NetXpert NXI-3011, v2 в качестве Pair Connection Master	71
5.2.6.	Приложение TCP-клиент: Конфигурирование NetXpert NXI-3011, v2 в качестве Pair Connection Slave	72
5.3.	Приложение TCP-сервера: Включение Reverse Telnet	73
6.	УСТАНОВКА И УСТРАНЕНИЕ НЕПОЛАДОК VCOM	74
6.1.	Включение VCOM	74
6.1.1.	Установка драйвера VCOM	76
6.1.2.	Ограничения.....	77
6.1.3.	Установка	77
6.1.4.	Удаление	77
6.2.	Включение VCOM на серверах последовательных устройств и выбор VCOM в Windows	77
6.2.1.	Включение VCOM на серверах последовательных устройств.....	77
6.2.2.	Запуск программной утилиты Serial/IP в Windows.....	78
6.2.3.	Конфигурирование VCOM-портов.....	80
6.3.	Исключения	83
6.4.	Использование монитора последовательного/IP-порта.....	88
6.4.1.	Запуск монитора порта.....	88
6.4.2.	Вкладка Activity	89
6.4.3.	Вкладка Trace.....	90
6.5.	Расширенные настройки Serial/IP	91

6.5.1.	Параметры расширенных настроек	92
6.5.2.	Использование Serial/IP с Proxy-сервером	92
7.	ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ	94
7.1.	Аппаратное обеспечение	94
7.2.	Назначение контактов разъема последовательного порта	96
7.3.	Назначение контактов разъема для LAN-интерфейса NetXpert NXI-3011, v2	97
7.4.	Назначение контактов разъёма питания и аварийной сигнализации	98
7.5.	Консольный кабель RJ-45-DB9	100
7.6.	Светодиодные индикаторы	100
7.7.	Программное обеспечение	101

1. ПРЕДИСЛОВИЕ

1.1. Задача руководства

Данное руководство предназначено для поддержки пользователя при установке и настройке промышленных конвертеров NetXpert NXI-3011, v2. В нем описаны технические характеристики, доступные для данного продукта. Руководство содержит расширенную информацию по управлению сетью, инструкции, примеры, рекомендации и общую теорию, предназначенные для помощи пользователям в управлении данным устройством и соответствующим программным обеспечением. При его чтении необходимо владение основами теоретических знаний. Следует обратиться к Глоссарию для поиска технических терминов и сокращений (если таковые имеются).

1.2. Кому следует использовать данное руководство

Данное руководство предназначено для использования квалифицированным персоналом по обслуживанию сетей или специалистами службы поддержки, которые знакомы с сетевой работой. Оно может быть полезно для системных программистов или планировщиков сети. Это руководство также предоставляет полезную и доступную информацию для начинающих пользователей.

1.3. Поддерживаемая платформа

Данное руководство разработано для промышленных конвертеров NetXpert NXI-3011, v2 и только для этой серии.

2. ВВЕДЕНИЕ

2.1. Общая информация

NetXpert NXI-3011, v2 представляет собой промышленный сервер последовательных устройств Ethernet, который выполняет роль шлюза для связи между портом Ethernet (TCP/UDP) и портом RS232/RS422/RS485. Информация, передаваемая моделью NetXpert NXI-3011, v2, прозрачна как для хост-компьютеров (Ethernet), так и для последовательных устройств (RS232/RS422/RS485). Данные, поступающие из порта Ethernet, передаются на назначенный порт RS232/RS422/RS485, а данные, полученные из порта RS232/RS422/RS485, отправляются на порт Ethernet, обеспечивая полнодуплексную и двунаправленную связь. В областях автоматизированного производства или промышленной автоматизации полевые устройства могут напрямую подключаться к сети Ethernet через устройство NetXpert NXI-3011, v2. В обычных ПК или ноутбуках с помощью нашего программного обеспечения может быть создан виртуальный COM-порт, чтобы удаленно получать последовательные данные от NetXpert NXI-3011, v2 через Ethernet.

Модель устройства NetXpert NXI-3011, v2 позволяет обмениваться данными с удаленным последовательным устройством через локальную сеть или через сеть Интернет, что значительно повышает доступность и масштабируемость.

На рисунке 2.1 показан пример нескольких устройств, подключенных к промышленному серверу последовательных устройств. ПК подключается к промышленному серверу последовательных устройств через интерфейс Ethernet, а управляемое устройство передает отчеты на промышленный сервер последовательных устройств через интерфейс RS232/RS422/RS485. Можно подключить несколько компьютеров к одному промышленному серверу последовательных устройств через транспортные протоколы TCP или UDP, а также подключить несколько управляемых устройств через RS232/RS422/RS485 к промышленному серверу последовательных устройств.

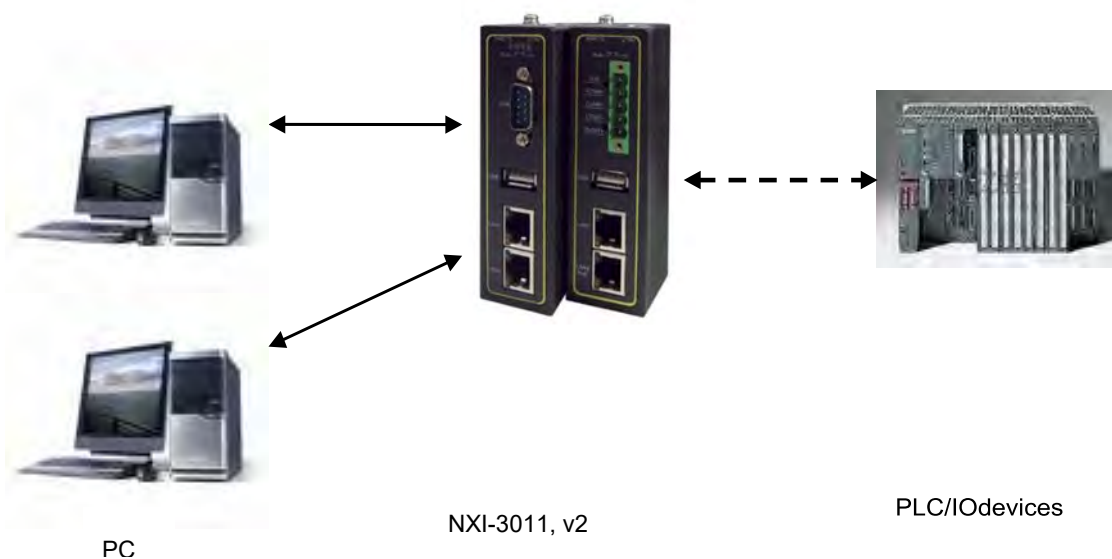


Рис. 2.1. Применение промышленного сервера последовательных устройств NetXpert NXI-3011, v2 для нескольких устройств.

2.2. Функции

Серия промышленных серверов последовательных устройств NetXpert NXI-3011, v2 использует одну и ту же программную платформу на разных доступных аппаратных средствах. Она обеспечивает:

- Гибкую аппаратную платформу, с разными вариантами портов в зависимости от имеющихся потребностей.
- Поддерживаемые режимы TCP Server/Client, UDP, Virtual COM и Tunneling.
- Удаленный мониторинг, управление и контроль промышленных полевых устройств.
- Настройку через WEB-браузер/Последовательную консоль/Консоль Telnet/Утилиту Windows (Утилита управления устройством).
- Прочный металлический корпус с защитой IP30 для настенного монтажа или монтажа на DIN-рейку.
- Широкий диапазон входного питания от 9 ... 56 В постоянного тока.

Внимание!

Начиная с этого момента, следует проявлять крайнюю осторожность.

Нельзя устанавливать или работать с электричеством или кабелями во время грозовой активности. Никогда не следует подключать или отключать питание при наличии опасных газов.

Осторожно: ГОРЯЧЕЕ! Следует отключить электропитание и дать устройству остыть в течение 5 минут, прежде чем прикасаться к нему.

3. НАЧАЛО РАБОТЫ

3.1. Внешний вид, передняя и задняя панель

На следующих рисунках показана передняя и верхняя панели конкретных устройств NetXpert NXI-3011, v2.

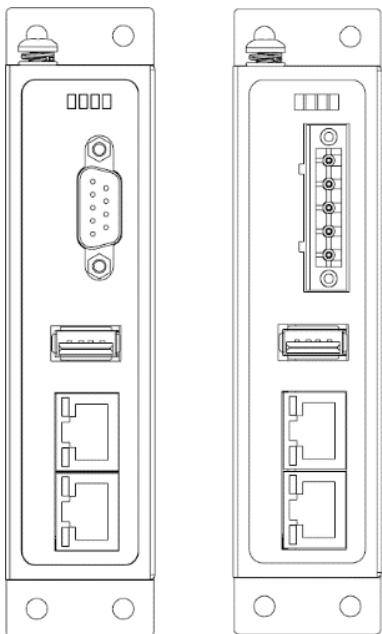


Рис. 3.1. NetXpert NXI-3011, v2-2T-1D.

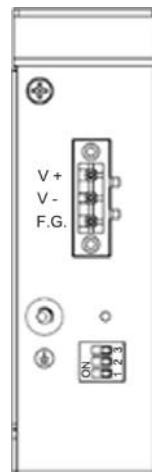


Рис. 3.2. NetXpert NXI-3011, v2-xx-1D.

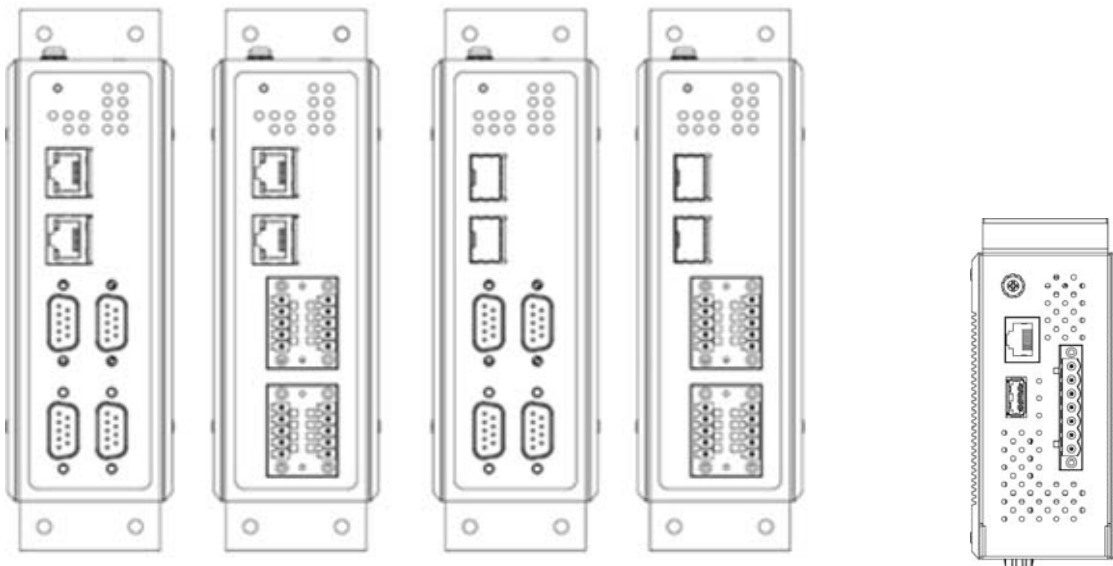


Рис. 3.3. NetXpert NXI-3011, v2-xx-4D.

3.2. Первая установка

Перед установкой устройства строго соблюдайте все процедуры обеспечения безопасности, описанные в руководстве по установке аппаратного обеспечения, которое входит в комплект поставки устройства. Не следует пытаться каким-либо образом использовать устройство, если не уверены в действиях, описанных здесь. В подобных случаях следует немедленно связаться с поставщиком.

В данном руководстве не приводятся конкретные инструкции по установке, поскольку они могут значительно отличаться в зависимости от приобретенного аппаратного обеспечения.

3.3. Заводские настройки по умолчанию

3.3.1. Настройки сети по умолчанию

Промышленный сервер последовательных устройств NetXpert NXI-3011, v2 оснащен двумя LAN-интерфейсами с двумя IP-адресами по умолчанию. Его сетевые параметры по умолчанию перечислены в таблице 3.1.

Таблица 3.1. Настройки сети по умолчанию.

Интерфейс	IP-адрес устройства	Маска подсети	IP-адрес шлюза	DNS
LAN1	10.0.50.100	255.255.0.0	10.0.0.254	255.255.255.255
LAN2	192.168.1.1	255.255.255.0	192.168.1.254	255.255.255.255

3.3.2. Другие настройки по умолчанию

Промышленный сервер последовательных устройств NetXpert NXI-3011, v2 поставляется со следующими настройками по умолчанию.

Таблица 3.2. Настройки безопасности, последовательных портов и SNMP по умолчанию.

Параметр	Значения по умолчанию
<i>Security (безопасность)</i>	
User Name (имя пользователя)	admin
Password (пароль)	default
<i>Serial (последовательные)</i>	
COM1	RS232, 9600 бит/сек, 8 бит данных, бит проверки на четность отсутствует, 1 стоповый бит, контроль потока отсутствует итнтервал между пакетами: автоматически.
COM2	RS232, 9600 бит/сек, 8 бит данных, бит проверки на четность отсутствует, 1 стоповый бит, контроль потока отсутствует итнтервал между пакетами: автоматически.
COM3	RS232, 9600 бит/сек, 8 бит данных, бит проверки на четность отсутствует, 1 стоповый бит, контроль потока отсутствует итнтервал между пакетами: автоматически.
COM4	RS232, 9600 бит/сек, 8 бит данных, бит проверки на четность отсутствует, 1 стоповый бит, контроль потока отсутствует итнтервал между пакетами: автоматически.
<i>SNMP</i>	
SysName	System
SysLocation	Location
SysContact	Contact

SNMP-агент	Отключен
Read Community	public
Write Community	private
Сервер SNMP-трапов	0.0.0.0 (отсутствует)

Примечание: Необходимо нажать кнопку “Reset” на передней панели в течение 5 секунд или выполнить программную процедуру для восстановления заводских настроек по умолчанию промышленного сервера последовательных устройств NetXpert NXI-3011, v2.

4. КОНФИГУРАЦИЯ И НАСТРОЙКА

4.1. Конфигурация сетевых параметров через утилиту управления устройством

Необходимо установить утилиту конфигурирования. После ее запуска, если Промышленный сервер последовательных устройств NetXpert NXI-3011, v2 уже подключен к той же подсети, что и ваш ПК, доступ к устройству можно получить с помощью широковещательных пакетов. Утилита конфигурирования автоматически обнаружит ваше устройство и отобразит его в окне программы. В противном случае, если нужное устройство не отображается в сети, следует нажать значок «Rescan», и список устройств, включая ваше устройство NetXpert NXI-3011, v2, подключенное в данный момент к сети, будет отображен как показано на рисунке 4.1.

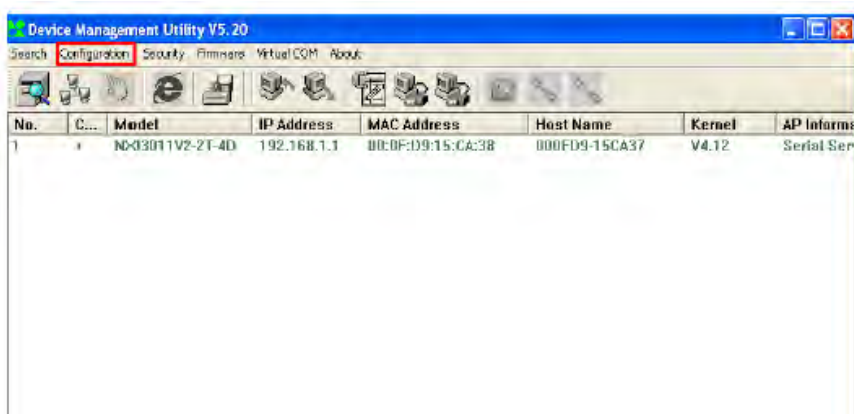


Рис. 4.1. Список устройств в утилите управления устройством.

Примечание: Данное изображение служит только для иллюстрации. Фактические значения/настройки могут отличаться в зависимости от устройства.

Иногда устройство NetXpert NXI-3011, v2 может не находиться в той же подсети, что и ваш ПК; в таком случае необходимо использовать утилиту, чтобы найти его в виртуальной среде. Чтобы настроить каждое устройство, сначала необходимо нажать, чтобы выбрать нужное устройство NetXpert NXI-3011, v2 (IP-адрес по умолчанию: 10.0.50.100) в списке утилиты, а затем выбрать в меню «Configuration → Network...» (или Ctrl + N) как показано на рисунке 4.2 или нажать на второй иконке, которая называется Network, на панели значков меню, и появится всплывающее окно, как показано на рисунке 4.3.

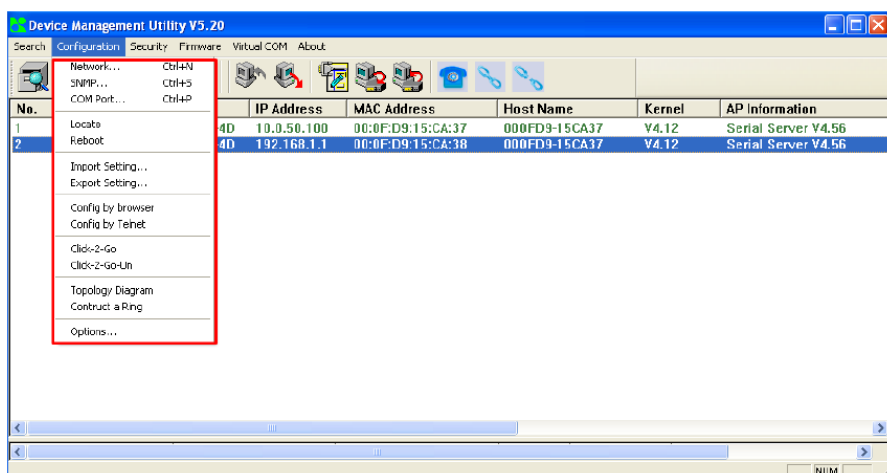


Рис. 4.2. Выпадающее меню конфигурации и сети.

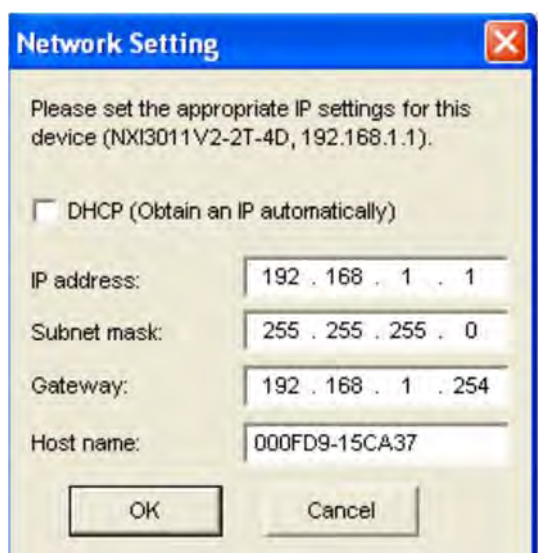
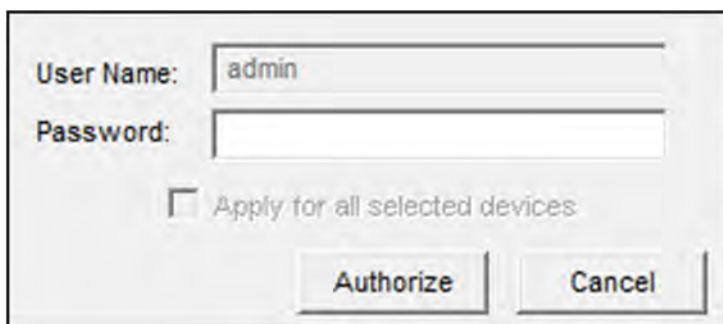


Рис. 4.3. Всплывающее окно сетевых настроек.

Затем можно изменить IP-адрес, чтобы избежать конфликта IP-адресов с другими хостами в локальной сети, или подключить устройство к существующей локальной сети, как показано на рисунке 4.3. Система запросит учетные данные для авторизации изменений. Необходимо ввести имя пользователя и пароль, как показано на рисунке 4.4. Имя пользователя по умолчанию - «admin», а пароль по умолчанию - «default». После нажатия на кнопку «Authorize» появится окно с уведомлением, как показано на рисунке 4.5, и некоторые устройства могут быть перезагружены. После перезагрузки устройства (для некоторых моделей) оно издаст два звуковых сигнала, что означает нормальную работу устройства. Затем устройство NetXpert NXI-3011, v2 можно будет найти по новому IP-адресу. Оно может автоматически отобразиться в списке утилиты управления устройствами Device Management Utility®, или его можно найти, нажав значок «Rescan». Следует обратить внимание, что если вы не изменили IP-адрес, но изменили другой параметр, может появиться другое окно уведомления, как показано на рисунке 4.6.



A dialog box for authorization. It contains two text input fields: 'User Name:' with the value 'admin' and 'Password:' which is empty. Below these fields is a checkbox labeled 'Apply for all selected devices'. At the bottom right are two buttons: 'Authorize' and 'Cancel'.

Рис. 4.4. Авторизация для изменения настроек сети.

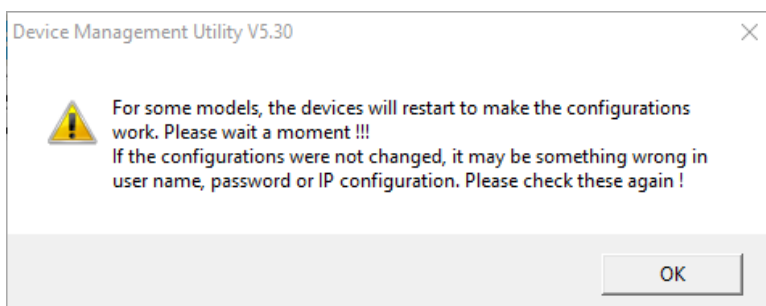


Рис. 4.5. Всплывающее окно уведомления после авторизации.

Необходимо обратиться к системному администратору, если необходимо узнать маску подсети и адрес шлюза.

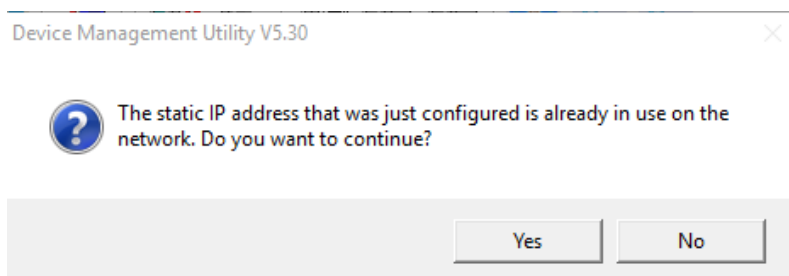


Рис. 4.6. Всплывающее окно уведомления при наличии такого же IP-адреса в сети.

4.2. Конфигурация через Web-интерфейс

Каждый Промышленный сервер последовательных устройств NetXpert NXI-3011, v2 оснащен встроенным WEB-сервером в прошивке. Поэтому к устройству можно получить доступ для настройки с помощью WEB-браузера, введя IP-адрес устройства (IP-адрес по умолчанию 10.0.50.100) в поле адреса WEB-браузера. Требуется аутентификация, и необходимо будет ввести имя пользователя (значение по умолчанию «admin») и пароль (значение по умолчанию «default») для доступа к WEB-интерфейсу, как показано на рисунке 4.7. Необходимо обратить внимание, что может появиться всплывающее окно с предупреждением, в котором предлагается изменить или сбросить пароль, чтобы он отличался от значения по умолчанию, как показано на рисунке 4.8. На рисунке 4.9 показана общая страница WEB-интерфейса. На рисунке 4.10 перечислены все разделы меню и подменю для WEB-конфигурации. Следует обратиться к пп. 3.3 для настроек по умолчанию.

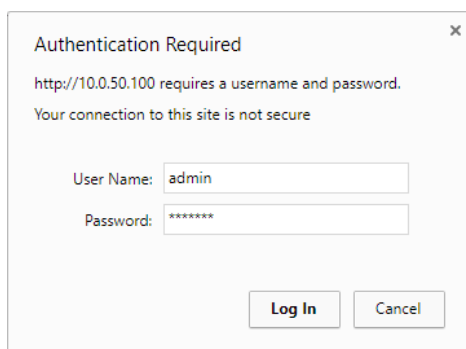


Рис. 4.7. Требуется аутентификация для доступа к WEB-интерфейсу.

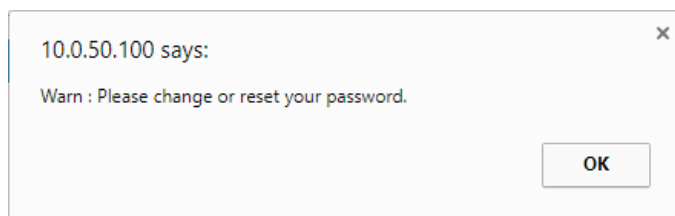


Рис. 4.8. Всплывающее окно с предупреждением об изменении или сбросе пароля для значения по умолчанию.

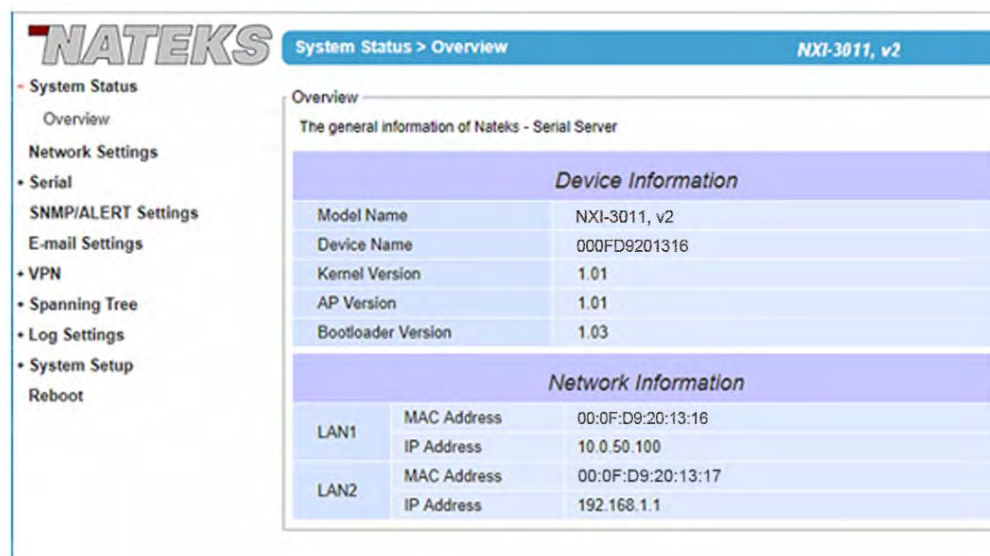


Рис. 4.9. Обзор WEB-страницы Промышленного сервера последовательных устройств NetXpert NXI-3011, v2.

- System Status
 - [Overview](#)
- Network Settings
- Serial
 - COM1
 - COM2
 - COM3
 - COM4
- SNMP/ALERT Settings
- E-mail Settings
- IPsec Settings
- Log Settings
 - System Log Settings
 - COM Log Settings
 - Event Log
 - COM Datalog
- System Setup
 - Date/Time Settings
 - Admin Settings
 - Firmware Upgrade
 - Backup/Restore Settings
 - Ping
- Reboot

Рис. 4.10. Карта страницы конфигурации Промышленного сервера последовательных устройств NetXpert NXI-3011, v2.

Данный способ доступа (WEB-интерфейс) для настройки устройства является наиболее удобным для пользователя. Это рекомендуемый и наиболее распространенный способ, используемый для серии промышленных серверов последовательных устройств NetXpert NXI-3011, v2. Необходимо перейти в соответствующий раздел для подробного объяснения.

4.3. Конфигурация автоматического назначения IP-адресов с помощью DHCP

DHCP-сервер может автоматически назначать IP-адреса, маску подсети и сетевой шлюз для интерфейса LAN. Это можно сделать, поставив флажок в поле “DHCP (Obtain an IP Automatically)” в диалоговом меню сетевых настроек Network Setting, как показано на рисунке 4.3 с помощью утилиты и перезагрузить устройство. После перезагрузки IP-адрес будет сконфигурирован автоматически.

4.4. Web Overview

В этом разделе будет отображаться текущая информация о состоянии и настройках устройства. Пример страницы общей информации о NetXpert NXI-3011, v2 показан на рисунке 4.11.

Device Information		
Model Name	NXI-3011, v2	
Device Name	000FD9201316	
Kernel Version	1.01	
AP Version	1.01	
Bootloader Version	1.03	

Network Information		
LAN1	MAC Address	00:0F:D9:20:13:16
	IP Address	10.0.50.100
LAN2	MAC Address	00:0F:D9:20:13:17
	IP Address	192.168.1.1

Рис. 4.11. WEB-страница Overview.

Следующая информация подробно представлена и разделена на 2 части (Информация об устройстве и Информация о сети):

- Device Information (Информация об устройстве).

Model Name, как следует из названия, показывает модель устройства.

Device Name показывает заданное имя устройства, для которого значением по умолчанию является MAC-адрес LAN-интерфейса.

Kernel Version - это номер версии прошивки ядра устройства.

AP Version - номер версии встроенного программного обеспечения устройства.

Bootloader Version - версия программы, которая загружает операционную систему устройства.

- Network Information (сетевая информация) отображает информацию о проводном сетевом интерфейсе на устройстве.

LAN: здесь отображается текущий MAC-адрес и IP-адрес интерфейса Ethernet.

4.5. Сетевые настройки

В этом разделе можно настроить как сетевые интерфейсы, так и соответствующие сетевые параметры устройства NetXpert NXI-3011, v2.

Существует четыре набора параметров, а именно: LAN1 Settings (настройки LAN1), LAN2 Settings (настройки LAN2), Default Gateway (шлюз по умолчанию) и DNS Server (DNS-сервер), которые можно ввести, как показано на рисунке 4.12. Во-первых, в разделе «LAN1 Settings» можно настроить IP-адрес, маску подсети и шлюз по умолчанию для проводной сети LAN1.

Можно установить флажок для опции DHCP, чтобы автоматически получать IP-адрес. Если установлен этот флажок, остальные параметры для настроек LAN1 будут выделены серым цветом или отключены. Во-вторых, настройки LAN2 Settings такие же, как настройки LAN1, но для второго интерфейса Ethernet. В-третьих, в разделе «Default Gateway» можно выбрать сеть шлюза по умолчанию для сервера последовательных устройств. Можно выбрать LAN1 или LAN2, нажав на соответствующий переключатель. В-четвертых, в разделе DNS Server можно указать IP-адрес предпочитаемого DNS - Preferred DNS (сервера доменных имен) и альтернативного DNS - Alternate DNS.

Если устройство NetXpert NXI-3011, v2 подключено к Интернету и должно подключаться к другим серверам через Интернет для получения каких-либо сервисов, таких как сервер протокола сетевого времени (NTP), потребуется настроить DNS-сервер, чтобы иметь возможность разрешить имя хоста NTP-сервера. Следует обратиться к сетевому администратору или поставщику услуг Интернета для получения IP-адресов локальных DNS.

The screenshot displays the 'Network Settings' web interface. At the top, there is a blue header with a back arrow and the text '> Network Settings'. Below this, the main content area is titled 'Network Settings' and contains four distinct sections, each with a purple header:

- LAN1 Settings:** Includes a 'DHCP' checkbox (unchecked) with the label 'Obtain an IP Address Automatically'. Below it are input fields for 'IP Address' (10.0.50.100), 'Subnet Mask' (255.255.0.0), and 'Gateway' (10.0.0.254).
- LAN2 Settings:** Similar to LAN1, with 'DHCP' (unchecked), 'IP Address' (192.168.1.1), 'Subnet Mask' (255.255.255.0), and 'Gateway' (192.168.1.254).
- Default Gateway:** Features a 'Default Gateway Select' section with two radio buttons: 'LAN1' (selected) and 'LAN2'.
- DNS Server:** Contains two input fields: 'Preferred DNS' (0.0.0.0) and 'Alternate DNS' (0.0.0.0).

Рис. 4.12. WEB-страница сетевых настроек.

После завершения конфигурации сетевых настроек необходимо нажать кнопку Save & Apply, чтобы сохранить все выполненные изменения. После этого WEB-браузер будет перенаправлен на страницу Overview, как показано на рисунке 4.11. Если требуется отменить все настройки, необходимо нажать кнопку Cancel.

4.6. Serial

Поскольку устройство NetXpert NXI-3011, v2 является промышленным сервером последовательных устройств, оно поддерживает последовательную связь через COM-порт(ы). Следует отметить, что линейка устройств NetXpert NXI-3011, v2 может иметь до четырех COM-портов: COM 1, COM 2, COM 3 и COM 4, тогда как типичные однопортовые модели имеют только один COM-порт (COM1). На рисунке 4.13 показано меню Serial в левой части окна WEB-интерфейса устройства NetXpert NXI-3011, v2. В следующих разделах будет описан процесс конфигурации этих COM-портов.

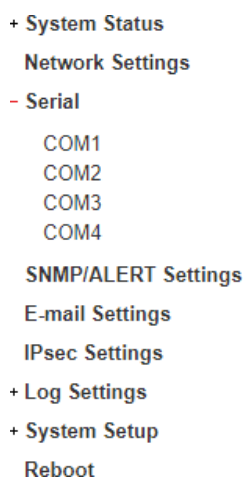


Рис. 4.13 Меню Serial.

4.6.1. Обзор меню COM-порта

Поскольку подробные сведения о разделе Link Mode (режимы подключения) и его настройках приведены в главе 5, этот раздел будет посвящен только настройкам последовательного интерфейса. На рисунке 4.14 показан пример настроек порта COM1, где верхняя часть предназначена для настроек режима подключения (Link Mode), а нижняя часть предназначена для настроек последовательного порта (Serial). Следует отметить, что подобная WEB-страница настроек применима также для настроек портов COM 2/COM 3/COM 4 на устройстве NetXpert NXI-3011, v2.

Serial > COM1

COM 1 Port Settings

Link Mode
To choose specific working mode for COM 1 port.

☒ TCP Server
 ☐ TCP Client
 ☐ UDP

TCP Server

Application	Virtual COM ▼
IP Filter	☐ Enable
Source IP	0.0.0.0
Local Port	4660
Maximum Connection	1 ▼
Response Behavior	☐ Request & Response Mode ☒ Reply to request only ☐ Reply to all ☒ Transparent Mode

To configure COM 1 port parameters.

Serial Settings

Serial Interface	☐ RS232 ☒ RS422 ☐ RS485 ☐ RS485(4-Wire)
Baud Rate	19200 ▼ bps
Parity	☒ None ☐ Odd ☐ Even ☐ Mark ☐ Space
Data bits	☐ 5 bits ☐ 6 bits ☐ 7 bits ☒ 8 bits
Stop bits	☒ 1 bits ☐ 2 bits
Flow Control	☒ None ☐ Xon/Xoff ☐ RTS/CTS

Save & Apply
Cancel
Advanced Settings

Рис. 4.14. WEB-страница настроек порта COM 1.

4.6.2. Конфигурация COM-порта

На рисунке 4.15 представлен раздел настроек Serial Settings для COM-порта NetXpert NXI-3011, v2. Следует отметить, что эти настройки должны соответствовать параметрам последовательного порта подключаемого конечного устройства. Каждая опция описана далее.

To configure COM 1 port parameters.

Serial Settings	
Serial Interface	☐ RS232 ☒ RS422 ☐ RS485 ☐ RS485(4-Wire)
Baud Rate	19200 ▼ bps
Parity	☒ None ☐ Odd ☐ Even ☐ Mark ☐ Space
Data bits	☐ 5 bits ☐ 6 bits ☐ 7 bits ☒ 8 bits
Stop bits	☒ 1 bits ☐ 2 bits
Flow Control	☒ None ☐ Xon/Xoff ☐ RTS/CTS

Рис. 4.15. Раздел настроек Serial Settings для порта COM 1.

- Serial Interface: эта опция позволяет выбрать между стандартами RS232, RS422, RS485 и RS485 (4-Wire).

Примечание: RS485 относится к 2-Wire RS485, а RS422 совместим с 4-Wire RS485.

- Baud Rate: пользователь может выбрать одно из значений пропускной способности (от 1200 до 921600 бит/сек) из выпадающего списка.
- Parity: для контроля по четности доступны опции None (отсутствует), Odd (нечетный), Even (четный), Mark (отметка) или Space (пробел).
- Data Bits: настройка для бит данных может быть 5 бит, 6 бит, 7 бит или 8 бит.
- Stop Bits: число стоповых битов может быть 1 бит или 2 бита.
- Flow Control: пользователь может выбрать из опций None (контроль потока отсутствует), RTS/CTS (аппаратный контроль потока) или Xon/Xoff (программный контроль потока). Если выбрана опция Xon/Xoff, то Xon и Xoff являются изменяемыми. По умолчанию их значения равны 0x11 для Xon и 0x13 для Xoff. Следует отметить, что это шестнадцатеричные числа символов ASCII (то есть, 0x11 = '1' и 0x13 = '3').

После окончания конфигурирования настроек Serial Settings COM-порта, необходимо нажать кнопку Save & Apply для сохранения внесенных изменений. Следует отметить, что после нажатия на кнопку Save & Apply, WEB-браузер обновится и останется на странице Serial Settings. Если необходимо отменить изменения и вернуть первоначальные значения всем параметрам, следует нажать на кнопку Cancel. Кнопка Advanced Settings будет описана в следующем разделе.

4.6.3. Конфигурирование COM-порта: Расширенные настройки

Для доступа к расширенным настройкам COM-порта, можно нажать на кнопку Advanced Settings в конце страницы Serial Settings, после чего откроется другое окно WEB-браузера, как показано на рисунке 4.16 ниже. Описание каждой опции приведено далее.

COM 1 Port Advance Settings

Advanced Settings		
TCP	TCP Timeout	☐ Enable 0 (0~60000) seconds
Delimiters	Serial to Network Packet Delimiter	☐ Interval Timeout 0 (1~30000) ms ☐ Auto(Calculate by baudrate) ☐ Manual Setting ☒ Max. Bytes 518 (within one packet: 1 ~ 1452 bytes) ☐ Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
	Netowrk to Serial Packet Delimiter	☒ Interval Timeout 1 (1~30000) ms ☐ Max. Bytes 0 (within one packet: 1 ~ 1452 bytes) ☐ Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
	Character Send Interval	☒ Enable 768 (0 ~ 1000) ms
	Response Interval Timeout	☒ Enable 232 (0 ~ 60000) ms
	Serial FIFO	☐ Enable (Disabling this option at baud rates higher than 115200bps would result in data loss).
	Serial Buffer	☐ Empty serial buffer when a new TCP connection is established.

Save & Apply Close

Рис. 4.16. WEB-страница расширенных настроек COM 1.

TCP

TCP timeout: Если щелкнуть поле «Enable» параметра TCP Timeout и ввести значение в секундах от 0 до 60000, в NetXpert NXI-3011, v2 будет включена функция поддержания активности сокета TCP. После истечения таймера процедура поддержания активности TCP отправит пакет keepalive своему партнеру, чтобы проверить, не разорвано ли соединение.

Delimiters

- Serial to Network Packet Delimiter: Разделитель пакетов - это способ упаковки данных при последовательной связи. Он разработан, чтобы сохранить пакеты неповрежденными. NetXpert NXI-3011, v2 поддерживает три типа разделителя: Time Delimiter (разделитель времени), Maximum Bytes (максимальное число байтов) и Character Delimiter (разделитель символов). Следует отметить, что при выборе следующих разделителей (интервал, максимальное число байт и символ), они программируются с использованием логического оператора ИЛИ. Это означает, что если будет выполнено любое из трех условий, NetXpert NXI-3011, v2 будет передавать последовательные данные в своем буфере по сети.
- Interval timeout: NetXpert NXI-3011, v2 будет передавать последовательные данные в своем буфере при достижении заданного интервала времени и если больше не поступает последовательных данных. Значение по умолчанию рассчитывается автоматически на основе скорости передачи данных, которая является параметром Auto (calculate by baudrate). Если автоматическое значение приводит к разрыву данных, время ожидания можно увеличить вручную, переключившись на «Manual setting» (поставив флажок в поле, показанном на рисунке 4.19) и указав большее значение в текстовом поле выше. Следует отметить, что максимальный интервал составляет 30 000 миллисекунд.

Внимание! Расчет интервала ожидания вручную. Оптимальный «Интервал ожидания» зависит от приложения, но он должен быть как минимум больше, чем односимвольный интервал в пределах указанной скорости передачи. Например, предположим, что для последовательного порта задано значение 1200 бит/сек, 8 бит данных, 1 стоповый бит и нет проверки четности. В этом случае общее количество битов, необходимых для отправки символа, составляет 10 битов (включая 1 стартовый бит), а время, необходимое для передачи одного символа, составляет $(10 \text{ (бит)} / 1200 \text{ (бит/сек)}) * 1000 \text{ (мс/сек)} = 8,3 \text{ мс}$. Поэтому, необходимо установить «Интервал ожидания» больше 8,3 мс. Округление 8,3 мс до следующего целого числа даст значение 9 мс, которое может быть установлено в качестве значения интервала ожидания.

- **Max Bytes:** NetXpert NXI-3011, v2 будет передавать последовательные данные в свой буфер при достижении указанной длины в байтах. Диапазон максимального числа байтов составляет от 1 до 1452 байтов. Для включения этой опции необходимо установить флажок перед параметром Max. Bytes, если требуется, чтобы NetXpert NXI-3011, v2 помещал в очередь данные, пока они не достигнут определенной длины. Эта опция по умолчанию отключена.
- **Character:** NetXpert NXI-3011, v2 будет передавать последовательные данные в своем буфере при обнаружении входящих данных, включающих указанный символ (в шестнадцатеричном (HEX) формате). В этом поле можно указать один или два символа. Если разделитель символов установлен как 0x0d, устройство NetXpert NXI-3011, v2 очистит свой последовательный буфер, когда он увидит 0x0d (символ возврата каретки) в последовательных данных. Эта опция по умолчанию отключена.
- **Network to Serial Packet Delimiter:** Эта группа параметров аналогична описанным выше разделителям, но они управляют потоком данных в противоположном направлении. NetXpert NXI-3011, v2 будет хранить данные от сетевого интерфейса в своей очереди до тех пор, пока не будет выполнено одно из условий, описанных выше, NetXpert NXI-3011, v2 будет отправлять данные на последовательный интерфейс.
- **Character Send Interval:** Эта опция определяет промежуток времени между каждым символом. При установке значения в одну секунду (1000 мс) NetXpert NXI-3011, v2 будет разбивать данные в очереди и передавать только один символ (байт) каждую 1 секунду. Максимальное значение для этой опции составляет 1000 миллисекунд или 1 секунда. Эта опция по умолчанию отключена.
- **Response Interval Timeout:** эта опция влияет только на режим Request & Response Mode и не влияет на Transparent Mode. (см. описание различий между режимами Request & Respond Mode и Transparent Mode в главе 5, раздел 5.1.1). Когда принимаются данные TCP (запрос от сети) и передаются на сторону последовательного устройства, NetXpert NXI-3011, v2 будет ожидать в течение установленного временного интервала перед передачей других данных TCP, если сторона последовательного устройства не получила никаких данных (нет ответа от последовательного устройства). Максимальное значение для этой опции составляет 60000 миллисекунд или 1 минуту.

Serial

- **Serial FIFO:** По умолчанию в NetXpert NXI-3011, v2 включена функция «первым пришел - первым вышел» (FIFO) для оптимизации производительности последовательного интерфейса. В некоторых приложениях (в частности, когда включен механизм управления потоком), может потребоваться отключить функцию FIFO, чтобы минимизировать объем данных, которые передаются через последовательный интерфейс после появления события отключения потока, чтобы уменьшить возможность перегрузки буфера в последовательном устройстве. Следует обратить внимание, что отключение этой опции на скорости свыше 115200 бит/с заметно снизит целостность данных.
- **Serial Buffer:** По умолчанию NetXpert NXI-3011, v2 очищает свой последовательный буфер, когда устанавливается новое TCP-соединение. Это означает, что приложение TCP не будет получать буферизованные последовательные данные во время обрыва

канала TCP. Чтобы сохранить последовательные данные при отсутствии TCP-соединения и отправить буферные последовательные данные сразу после установления TCP-соединения, эту опцию можно отключить.

После окончания конфигурирования расширенных настроек (Advanced Settings) порта COM необходимо нажать на кнопку Save & Apply для сохранения внесенных изменений. Затем можно закрыть окно браузера Advanced Settings, нажав на кнопку Close, и произойдет возврат на страницу COM 1 Port Setting.

4.7. Настройки IPsec Settings

IPsec (или Internet Protocol Security – безопасность интернет-протокола) является сетевым протоколом, который может устанавливать безопасную и надежную связь для различных сценариев применения. IPsec обеспечивает конфиденциальность данных, целостность данных, аутентификацию источника данных и функцию анти-повтора.

NetXpert NXI-3011, v2 имеет функцию соединения IPsec для установки безопасного канала связи типа хост-хост, хост-подсеть (или хост-сеть) и подсеть-подсеть (или сеть-сеть). Следует отметить, что на другой конечной точке Интернета для успешного установления защищенной связи необходим маршрутизатор или шлюз с полной поддержкой IPsec. NetXpert NXI-3011, v2 поддерживает два типа режимов подключения IPsec: Tunnel mode (туннельный режим) и Transport mode (транспортный режим).

В Туннельном режиме весь IP-пакет подлежит шифрованию и аутентификации. Затем IP-пакет инкапсулируется в новый IP-пакет с новым IP-заголовком. Туннельный режим, который используется для создания виртуальной частной сети (VPN), может применяться к соединениям типа хост-хост, хост-подсеть и подсеть-подсеть. Формат пакета (датаграммы) для туннельного режима выглядит следующим образом:

<i>Новый IP заголовок</i>	<i>Заголовок IPsec</i>	<i>Оригинальный IP пакет</i>	<i>Дополнительный трейлер IPsec</i>
---------------------------	------------------------	------------------------------	-------------------------------------

В транспортном режиме обычно шифруется или аутентифицируется только полезная нагрузка IP-пакета. Маршрутизация не повреждается, поскольку IP-заголовок не изменяется и не шифруется. Однако, когда используется заголовок аутентификации, IP-адреса нельзя изменить с помощью трансляции сетевых адресов (NAT). Транспортный режим может применяться только при обмене данными между хостами. Формат пакета (датаграммы) для транспортного режима выглядит следующим образом:

<i>Оригинальный IP заголовок</i>	<i>Заголовок IPsec</i>	<i>Оригинальный IP пакет</i>	<i>Дополнительный трейлер IPsec</i>
----------------------------------	------------------------	------------------------------	-------------------------------------

Соединение типа хост-хост обычно используется в простой прямой связи между двумя точками. Оно используется для прямой связи с сервером или между устройством (NetXpert NXI-3011, v2) и одноранговым устройством (как, например, другое устройство NetXpert NXI-3011, v2). Следует отметить, что этот тип соединения нельзя использовать для доступа ко всем ресурсам подсети. На рисунке 4.17. показан пример соединения хост-хост. Эта конфигурация может быть установлена как в туннельном режиме, так и в транспортном режиме.



Рис. 4.17. Пример соединения хост-хост.

Соединение хост-подсеть (или хост-сеть) в основном используется, когда одной конечной точке необходим доступ к подсетям другой стороны. Типичное применение - это сотрудники, в бизнес-командировках и хотели бы подключиться к своей корпоративной штаб-квартире через мобильные устройства. Они могут устанавливать соединения IPsec для доступа к ресурсам внутренней корпоративной сети. На рисунке 4.18 показано приложение для удаленного доступа, в котором NetXpert NXI-3011, v2 может получить доступ к удаленному ресурсу подсети через одноранговый шлюз. На рисунке 4.19 показано приложение шлюза, в котором NetXpert NXI-3011, v2 может пассивно принимать запросы на подключение от удаленных сторон и предоставлять доступ к ресурсам подсети NetXpert NXI-3011, v2. Следует отметить, что обе эти конфигурации требуют установки типа соединения только в туннельный режим.

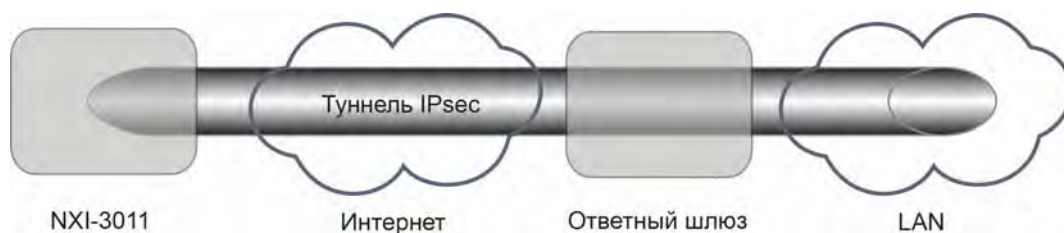


Рис. 4.18. Приложение для удаленного доступа с использованием соединения хост-подсеть.

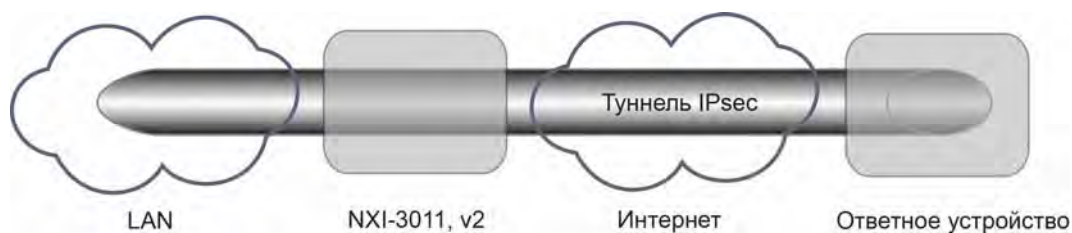


Рис. 4.19. Приложение шлюза с использованием соединения хост-подсеть.

Соединение подсеть-подсеть в основном используется для соединения двух подсетей от разных сторон. Как правило, приложениями являются корпоративные головные офисы и филиалы, которые совместно используют ресурсы внутренней сети. Конкретное приложение также можно настроить в качестве подсети одной стороны для установки VPN-туннелей IPsec для доступа к устройству в подсети другой стороны или в качестве устройства в подсети одной стороны для установки VPN-туннелей IPsec для доступа к другому устройству в подсети другой стороны.

На рисунке 4.20 показан пример подключения подсеть-подсеть с помощью сетевого приложения. Хост в удаленной подсети также может подключаться к локальной подсети (приложение хост-сеть) на основе этого соединения подсеть-подсеть, как показано на рисунке 4.20. С другой стороны, два разных устройства в двух разных подсетях (приложение хост-хост) могут быть подключены через VPN-туннель IPsec на основе этого соединения подсеть-подсеть, как показано на рисунке 4.21. Следует отметить, что все настройки подсеть-подсеть должны устанавливать тип соединения только в туннельный режим.

На рисунке 4.20 приведен пример сетевого приложения с использованием соединения типа подсеть-подсеть через NetXpert NXI-3011, v2 и однорангового устройства.



Рис. 4.20 Пример приложения хост-сеть через соединение подсеть-подсеть.



Рис. 4.21. Пример приложения хост-хост через соединение подсеть-подсеть.

В некоторых сетевых конфигурациях на шлюзе/маршрутизаторах реализована трансляция сетевых адресов (NAT). NAT обычно используется для разрешения частных IP-адресов в частных сетях за шлюзами/маршрутизаторами с одним общедоступным IP-адресом, подключенным к общедоступному Интернету. Внутренние сетевые устройства могут связываться с хостами во внешней сети, изменяя исходный адрес исходящих запросов на адрес устройства NAT (шлюз/маршрутизатор) и передавая ответы обратно на исходное устройство. Клиенты IPsec виртуальной частной сети (VPN) используют обход трансляции сетевых адресов (NAT) для того, чтобы пакеты инкапсулирующей защитной полезной нагрузки (ESP) проходили через NAT. В своей работе IPsec использует несколько протоколов, которые должны быть включены для прохождения межсетевых экранов и трансляторов сетевых адресов (NAT), такие как

- Протокол обмена ключами в Интернете (IKE) использует порт 500 протокола пользовательских датаграмм (UDP).
- Инкапсулирующая защитная полезная нагрузка (ESP) использует IP-протокол номер 50.
- Аутентификационный заголовок (AH) использует IP-протокол номер 51.
- Для преодоления NAT IPsec использует UDP-порт номер 4500, если соответствующая функция запущена.

NetXpert NXI-3011, v2 также имеет функцию, называемую преодолением NAT (NAT-T), которая позволяет туннелю IPsec проходить через NAT в своей сети. NetXpert NXI-3011, v2 активирует эту опцию автоматически и инкапсулирует пакеты IPsec внутри UDP-порта 4500, чтобы иметь возможность проходить через NAT-маршрутизатор.

NetXpert NXI-3011, v2 использует протокол обмена ключами по Интернету (IKE) для настройки

ассоциации безопасности (SA) в наборе протоколов IPsec. Следует отметить, что IKE основывается на протоколах Oakley и ISAKMP (ассоциация безопасности Интернета и протокол управления ключами). IKE использует сертификаты X.509 для аутентификации с помощью общего ключа или открытого ключа с использованием DNS (предпочтительно с помощью DNSSEC). IKE также использует обмен ключами Диффи-Хеллмана (DH) для установки общего секретного сеанса, в ходе которого получены криптографические ключи. Ассоциации безопасности IPsec (SA) делятся на две фазы. На первом этапе IKE создает защищенный канал с проверкой подлинности между NetXpert NXI-3011, v2 и одноранговым устройством, который называется ассоциацией безопасности IKE. На этом этапе всегда осуществляется соглашение о ключе Диффи-Хеллмана (DH) для создания общего секретного ключа или ключа DH. На втором этапе IKE согласовывает ассоциации безопасности IPsec и генерирует необходимый материал ключа для IPsec. Этот ключ IPsec, который является симметричным ключом, будет использоваться для массовой передачи данных внутри туннеля IPsec. На втором этапе может быть заключено новое соглашение Диффи-Хеллмана, или ключи могут быть получены из общего секретного ключа первого этапа.

4.7.1. Настройки IPsec Settings

На рисунке 4.22 показана WEB-страница настроек IPsec Settings в меню IPsec Settings. На этой странице расположено четыре раздела настроек: General Settings, Authentication Settings, IKE Settings и Dead Peer Detection Settings.

IPsec Settings

General Settings		
IPsec	☒ Enable	
Peer Address	☒ Dynamic ☐ Static: 10.0.50.100	
Remote Subnet	☒ None (Host Only) ☐ Network: 192.168.1.0 / 24	
Local Subnet	☒ None (Host Only) ☐ Network: 10.0.50.0 / 24	
Connection Type	Tunnel ▼	
Authentication Settings		
Method	☒ Pre-Shared Key: secrets	
IKE Settings		
Phase 1 SA (ISAKMP)	Mode	Main ▼
	DH Group	Group 2 (1024-bit) ▼
	Encryption Algorithm	AES-128 ▼
	Authentication Algorithm	SHA1 ▼
	SA Life Time	3600 seconds
Phase 2 SA	Protocol	ESP ▼
	Perfect Forward Secrecy	Group 2 (1024-bit) ▼
	Encryption Algorithm	AES-128 ▼
	Authentication Algorithm	SHA1 ▼
SA Life Time	28800 seconds	
Dead Peer Detection Settings		
DPD Action	Hold ▼	
DPD Interval	30 seconds	
DPD Timeout	120 seconds	

Note: When Save Settings the device will not auto-connect.

Рис. 4.22. WEB-страница IPsec Tunnels в меню IPsec Setting.

Для конфигурации IPsec Settings в первую очередь необходимо сконфигурировать раздел General Settings в меню IPsec Settings. В General Settings есть пять параметров, которые необходимо настроить:

- **IPsec:** Установив флажок для этой опции, вы включаете функцию IPsec для NetXpert NXI-3011, v2.
- **Peer Address:** Этот параметр позволяет указать IP-адрес удаленного хоста, однорангового хоста или удаленного шлюза. Существует два варианта для адреса Peer Address: динамический Dynamic и статический Statics.

Dynamic: При выборе опции Dynamic переключателя Dynamic адрес равноправного узла или IP-адрес удаленного устройства не является фиксированным или неизвестным. Следует отметить, что когда для адреса Peer Address задан динамический режим, NetXpert NXI-3011, v2 может принять запрос на удаленное подключение или будет респондентом.

Static: С другой стороны, если IP-адрес удаленного устройства известен, можно выбрать переключатель для опции Static и ввести IP-адрес в текстовое поле за ним. NetXpert NXI-3011, v2 будет инициатором/респондентом.

- **Remote Subnet:** Этот параметр указывает, необходимо ли создать соединение IPsec с удаленной подсетью. Есть также два варианта для доступа Remote Subnet:

None (Host Only): Этот параметр указывает, что удаленная подсеть не поддерживается или отсутствует, и поддерживается только доступ к хосту. То есть удаленный конец туннеля IPsec является только хостом или одноранговым устройством.

Network: Этот параметр обозначает удаленную подсеть путем ввода IP-адреса подсети и количества битов маскирования подсети Subnet Masking Bits или соответствующего префикса маршрутизации. Эта опция поддерживает описание бесклассовой междоменной маршрутизации (CIDR). Например, IP-адрес подсети - 192.168.11.0, а маска подсети - 24 бита (из 255.255.255.0).

- **Local Subnet:** Этот параметр позволяет включить соединение IPsec с локальной подсетью. Существует два варианта доступа к локальной подсети:

None (Host Only): Этот параметр указывает, что локальная подсеть не поддерживается или отсутствует, и поддерживается только локальный доступ к хосту. То есть локальный конец туннеля IPsec является только хостом или одноранговым устройством.

Network: Этот параметр обозначает Локальную подсеть путем ввода IP-адреса подсети и количества битов маскирования подсети Subnet Masking Bits или соответствующего префикса маршрутизации. Эта опция поддерживает описание бесклассовой междоменной маршрутизации (CIDR). Например, IP-адрес подсети - 192.168.11.0, а маска подсети - 24 бита (из 255.255.255.0).

- **Connection Type:** Эта опция указывает тип соединения IPsec, который может быть либо в туннельном, либо в транспортном режиме. Необходимо выбрать соответствующий тип соединения из выпадающего списка. Следует отметить, что туннельный режим может применяться к соединениям хост-хост, хост-подсеть и подсеть-подсеть. Транспортный режим может применяться только при соединении хост-хост.

Вторая часть настроек IPsec Settings - это настройки аутентификации Authentication Settings. Здесь есть метод аутентификации, который уже выбран в качестве предварительного общего ключа Pre-Shared Key. Затем необходимо ввести секретный ключ или пароль в текстовое поле за ним. Оба конца VPN-туннеля должны использовать один и тот же секретный ключ или пароль. Предварительно общий ключ может содержать от 1 до 60 символов ASCII с учетом регистра и специальных символов.

Третья часть настроек IPsec - это настройки IKE (Internet Key Exchange – протокола обмена ключами). Протокол обмена ключами (IKE), который поддерживает NetXpert NXI-3011, v2, - это IKE версии 1 или IKEv1. В рамках Phase 1 SA (ISAKMP) существует пять параметров безопасности, которые необходимо настроить. На этапе 1 два VPN-шлюза обмениваются информацией об алгоритмах шифрования, которые они поддерживают, а затем устанавливают временное безопасное соединение для обмена информацией об аутентификации.

Первая опция - это режим Mode сеанса IKE, который определяет, сколько шагов или пакетов будет использоваться или обмениваться во время взаимодействия IKE SA. Можно выбрать основной режим Main Mode или агрессивный режим Aggressive Mode. Основной режим отправляет предложения SA, открытый ключ Диффи-Хеллмана и аутентификацию сеанса ISAKMP в трех пакетах обмена данными, в то время как в агрессивном режиме все предложения SA, открытый ключ DH и аутентификация сессии ISAKMP будут помещены в один пакет обмена данными. Агрессивный режим делает согласование IKE более быстрым, чем основной режим. Разница между основным режимом и агрессивным режимом заключается в том, что в основном режиме используется «защита персональных данных». Идентификатор передается в зашифрованном виде в основном режиме, но не шифруется в агрессивном режиме. Как правило, рекомендуется использовать основной режим.

Вторая опция – это выбор группы Диффи-Хеллмана (DH Group) стандартизированных глобальных уникальных простых чисел и генераторов, которые будут использоваться для обеспечения безопасного обмена асимметричным ключом. Группа DH используется для шифрования этого взаимодействия IKE. NetXpert NXI-3011, v2 поддерживает две группы DH, а именно DH Group 2, которая является 1024-битной модульной группой потенцирования (MODP), и DH Group 5, которая является 1536-битной группой MODP.

Третья опция – это выбор алгоритма шифрования Encryption Algorithm, который может быть AES-128 или 3DES. Эта опция выбирает размер ключа и алгоритм шифрования, который будет использоваться в IKEv1 Phase 1. Значение по умолчанию равно AES-128.

Четвертая опция – это выбор алгоритма аутентификации Authentication Algorithm, который может быть SHA1 или MD5. Эта опция выбирает, какой алгоритм хеширования будет использоваться для аутентификации пакетных данных в the IKEv1 Phase 1. Значение по умолчанию равно SHA1.

Пятая опция – это время жизни SA Life Time, которое должно быть установлено в секундах. Это значение представляет время жизни ключа IKE, который выделен в Фазе 1 между конечным хостом или сетью. Время жизни SA по умолчанию составляет 10800 секунд. Конфигурируемый диапазон для параметра SA Life Time составляет от 300 до 86400 секунд.

В Phase 2 SA имеется пять параметров безопасности, которые необходимо настроить. Подобно Phase 1 SA, NetXpert NXI-3011, v2 и его одноранговое устройство будут согласовывать или обмениваться предложениями, чтобы определить, какие параметры безопасности будут использоваться в этой Фазе Phase 2 SA. Предложение фазы 2 также включает протокол безопасности Protocol (первая опция), который можно выбрать либо для инкапсуляции полезной нагрузки безопасности (ESP), либо для заголовка аутентификации (AH). Вторая опция – это Perfect Forward Secrecy, которая является свойством протокола согласования ключей, гарантирующим, что ключ сеанса, полученный из набора долгосрочных ключей, не будет скомпрометирован, если один из долгосрочных ключей будет скомпрометирован в будущем. В Phase 2 SA NetXpert NXI-3011, v2 также поддерживает две группы DH: DH Group 2 (1024-битная) и DH Group 5 (1536-битная).

Затем можно перейти к выбору алгоритмов шифрования и аутентификации. Третья опция - выбор алгоритма шифрования Encryption Algorithm, который может быть AES-128 или 3DES. Этот алгоритм шифрования будет использоваться в туннеле IPsec. Значением настройки по умолчанию является AES128. Четвертая опция - выбор алгоритма аутентификации, который может быть SHA1 или MD5. Это алгоритм хеширования, который будет использоваться для аутентификации пакетных данных в туннеле IPsec. Значение по умолчанию SHA1. Наконец, последняя опция - это SA Life Time для фазы 2, который должен быть установлен в секундах. Диапазон этой настройки может быть от 180 до 86400 секунд. Время жизни SA Life Time по умолчанию составляет 3600 секунд.

Последняя часть настроек IPsec - это настройки обнаружения неработающих узлов сети Dead Peer Detection Settings. Обнаружение неработающих узлов (DPD) представляет собой механизм, который NetXpert NXI-3011, v2 использует для проверки существования удаленного шлюза обмена ключами в Интернете (IKE) или однорангового устройства NetXpert NXI-3011, v2. Чтобы обнаружить одноранговое устройство, NetXpert NXI-3011, v2 будет отправлять зашифрованные сообщения полезной нагрузки IKE Phase 1 (или hello-сообщение) одноранговому устройству и ожидать подтверждения DPD от однорангового устройства.

Если NetXpert NXI-3011, v2 не получает подтверждающее сообщение в течение определенного интервала времени (тайм-аут DPD - DPD timeout), он будет считать, что одноранговое устройство не работает. Затем NetXpert NXI-3011, v2 удалит ассоциацию безопасности фазы 1 и все ассоциации безопасности фазы 2 этого неработающего однорангового устройства.

В разделе Dead Peer Detection Settings необходимо выбрать действие DPD Action, которое будет выполнять NetXpert NXI-3011, v2, если обнаружит, что одноранговое устройство не работает. Можно выбрать Hold, чтобы по-прежнему поддерживать ассоциацию безопасности для однорангового устройства и ждать, пока одноранговое устройство не вернется к работе, или Restart, чтобы перезапустить процесс ассоциации безопасности.

Интервал DPD interval - это период времени для отправки hello-сообщения на одноранговое устройство или интервал, в течение которого NetXpert NXI-3011, v2 будет повторно проверять конечную точку с помощью сообщения keep-alive. Интервал DPD может иметь значение от 1 до 65535 секунд. Значение по умолчанию для интервала DPD равно 30 секунд. Тайм-аут DPD Timeout будет временем, когда NetXpert NXI-3011, v2 объявляет одноранговое устройство неработающим, если оно не получило никакого ответа или трафика от этого устройства.

Если проверка активности завершается неудачно до истечения этого периода времени, NetXpert NXI-3011, v2 выполнит действие PDP. Диапазон значений времени ожидания DPD Timeout составляет от 1 до 65535 секунд. Значение по умолчанию для параметра DPD Timeout равно 120 секунд. Описание каждого параметра на WEB-странице туннелей IPsec приведено в таблице 4.1.

Таблица 4.1. Описание параметров WEB-страницы IPsec Tunnels.

Название поля		Описание	Значение по умолчанию
<i>General Settings</i>			
IPsec		Включение туннеля IPsec.	Disable
NAT Traversal		Включение механизма прохождения NAT.	Enable
Peer Address		IP-адрес удаленного устройства, который может быть динамическим (любой адрес) или статическим (фиксированный адрес).	Dynamic
Remote Subnet		Удаленная подсеть может быть None (только для хоста) или Network (IP и маска сети).	None (Host Only)
Local Subnet		Локальная подсеть может быть None (только для хоста) или Network (IP и маска сети).	None (Host Only)
Connection type		Туннельный режим или Транспортный режим.	Tunnel
<i>Authentication Settings</i>			
Method		Общий ключ.	secrets
<i>IKE Settings</i>			
Phase 1 SA	Mode	Выбор способа выполнения IKE-согласования между основным режимом и агрессивным режимом.	Main Mode

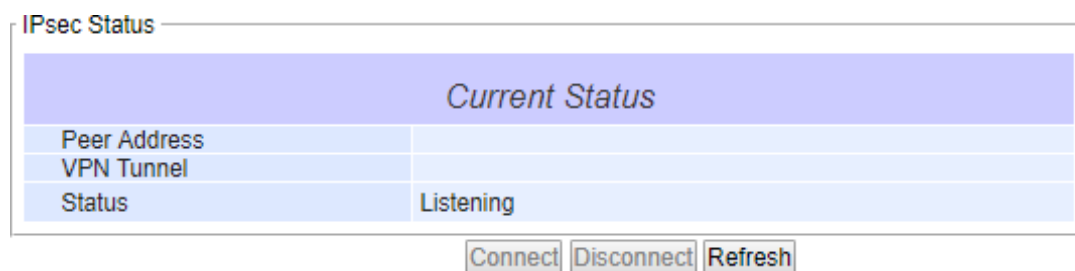
	DH Group	Группы Диффи-Хеллмана определяют силу ключа, используемого в процессе обмена ключами: DH Group 2 (1024-битная) или DH Group 5 (1536-битная).	Group 2 (1024-bit)
	Encryption Algorithm	Алгоритм шифрования, используемый в процессе обмена ключами: 3DES или AES.	AES128
	Authentication Algorithm	Алгоритм хеширования, используемый для аутентификации пакетных данных в процессе обмена ключами IKEv1 фазы 1: MD5 или SHA1.	SHA1
	SA Life Time	Как долго должен длиться конкретный экземпляр соединения (набор ключей шифрования/аутентификации для пользовательских пакетов) от успешного согласования до истечения срока действия. Значение может составлять от 300 до 86 400 секунд.	3600
Phase 2 SA	Protocol	Необходимо выбрать способ шифрования IP-пакета и проверить: Encapsulate Security Payload (ESP) или заголовок IP-аутентификации (AH).	ESP
	Perfect Forward Secrecy	Группы Диффи-Хеллмана для полной безопасности пересылки ключей определяют силу ключа, используемого в процессе обмена ключами: DH Group 2 (1024-битная) или DH Group 5 (1536-битная).	Group 2 (1024-bit)
	Encryption Algorithm	Необходимо выбрать, какой размер ключа и алгоритм шифрования будут использоваться в туннеле IPsec: 3DES или AES128.	AES128
	Authentication Algorithm	Раздел алгоритма хеширования, который будет использоваться для аутентификации пакетных данных в туннеле IPsec: MD5 или SHA1.	SHA1
	SA Life Time	Значение, представляющее время жизни ключа IKE, выделенного в фазе 2 между конечным хостом и сетью. Доступный диапазон значений составляет от 180 до 86 400 секунд.	28800
<i>Dead Peer Detection Settings</i>			
DPD Action		Необходимо выбрать значение Hold или Restart ассоциации безопасности туннеля для однорангового устройства. Следует отметить, что Hold подходит для статистически определенного туннеля.	Hold
DPD Interval		Продолжительность времени отправки hello-сообщения на одноранговое устройство: диапазон значений составляет от 1 до 65535 секунд.	30 seconds

DPD Timeout	Длительность времени, чтобы объявить, что узел не работает: диапазон значений составляет от 1 до 65535 секунд.	120 seconds
-------------	--	-------------

После завершения конфигурирования настроек IPsec settings необходимо нажать кнопку Save, чтобы сохранить все выполненные изменения. Если требуется отменить все настройки, необходимо нажать кнопку Cancel.

4.7.2. IPsec Status

На этой WEB-странице можно проверить состояние соединения IPsec между NetXpert NXI-3011, v2 и его одноранговым устройством в различных типах и режимах соединения. Первая информация - это адрес узла Peer Address, который является IP-адресом другого устройства, подключенного к NetXpert NXI-3011, v2. Вторая информация - это статус VPN-туннеля. Третья информация - это состояние соединения IPsec, которое может быть отключено (Disabled), прослушивается (Listening) или подключено (Connected). Показывает WEB-страницу состояния IPsec Status в меню настроек IPsec. В конце WEB-страницы расположены три кнопки: Connect - «Подключить», Disconnect - «Отключить» и Refresh - «Обновить». Кнопки «Подключить» и «Отключить» позволяют установить или разорвать соединение IPsec. Кнопка «Обновить» позволяет проверить последний статус подключения.



Current Status	
Peer Address	
VPN Tunnel	
Status	Listening

Рис. 4.23. WEB-страница IPsec Status.

4.7.3. Примеры настроек IPsec

В следующих главах приведены примеры настроек IPsec. Однако каждый пример будет сфокусирован только на части общих настроек. Другие разделы настроек IPsec можно настроить в соответствии с предпочтениями пользователя. Следует обратиться к предыдущему разделу для более подробной информации о настройках аутентификации, настройках IKE и настройках обнаружения неработающих узлов. Следует отметить, что соединения типа сеть-сеть (или подсеть-подсеть) теперь поддерживаются в новой прошивке NetXpert NXI-3011, v2.

4.7.3.1. Соединения хост-хост

Для соединений типа хост-хост можно настроить два сценария: со статическим одноранговым узлом и с динамическим одноранговым узлом. Топология хост-хост для обоих сценариев показана на рисунке 4.24. Необходимо следовать инструкциям ниже для настройки Общих параметров каждого сценария.

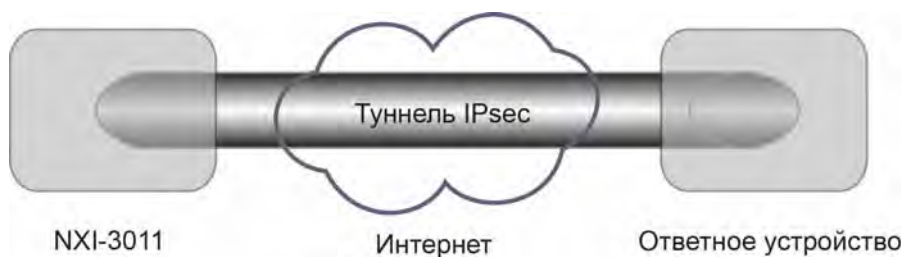


Рис. 4.24. IPsec VPN-туннель с топологией хост-хост.

Сценарий: соединение хост-хост со статическим одноранговым узлом, как показано на рисунке 4.25.

- Необходимо поставить флажок в поле Enable для IPsec.
- В поле Peer Address необходимо выбрать опцию Static и ввести IPv4-адрес однорангового узла.

Примечание: Когда в качестве адреса однорангового узла вводится статического адрес, NetXpert NXI-3011, v2 выступает в качестве инициатора, который берет на себя инициативу и устанавливает соединение. NetXpert NXI-3011, v2 также может выступать как респондент и пассивно принимает соединение, инициированное удаленным шлюзом

- Установить переключатель None (Host Only) в поле Remote Subnet.
- Поскольку данное VPN-соединение основано на двух хостах, опция Connection Type может иметь значение Transport или Tunnel.

IPsec Settings	
General Settings	
IPsec	☒ Enable
Peer Address	☐ Dynamic ☒ Static: 172.16.1.1
Remote Subnet	☒ None (Host Only) ☐ Network: 192.168.1.0 / 24
Local Subnet	☒ None (Host Only) ☐ Network: 10.0.50.0 / 24
Connection Type	Tunnel

Рис. 4.25. Общие настройки для соединения хост-хост со статическим одноранговым узлом.

Сценарий: соединение хост-хост с динамическим одноранговым узлом, как показано на рисунке 4.26.

- Необходимо поставить флажок в поле Enable для IPsec.
- В поле Peer Address необходимо выбрать опцию Dynamic.

Примечание: Когда VPN подключается к одноранговому узлу с динамическим IP-адресом, NetXpert NXI-3011, v2 выступает в качестве респондента и пассивно принимает подключение, инициированное удаленным шлюзом.

- Остальные настройки такие же, как для соединения хост-хоста со сценарием статического однорангового узла, описанного выше.

IPsec Settings

General Settings	
IPsec	☒ Enable
Peer Address	☒ Dynamic ☐ Static:
Remote Subnet	☒ None (Host Only) ☐ Network: /
Local Subnet	☒ None (Host Only) ☐ Network: /
Connection Type	Tunnel ▼

Рис. 4.26. Общие настройки для соединения хост-хост с динамическим одноранговым узлом.

4.7.3.2. Соединения хост-сеть

Для соединений типа хост-сеть (или хост-подсеть или хост-сайт) также можно настроить два сценария: со статическим одноранговым узлом и с динамическим одноранговым узлом. Следует отметить, что NetXpert NXI-3011, v2 является хостом в этих сценариях. Топология хост-сеть для обоих сценариев показана на рисунке 4.27. Необходимо следовать инструкциям ниже для настройки Общих параметров каждого сценария.

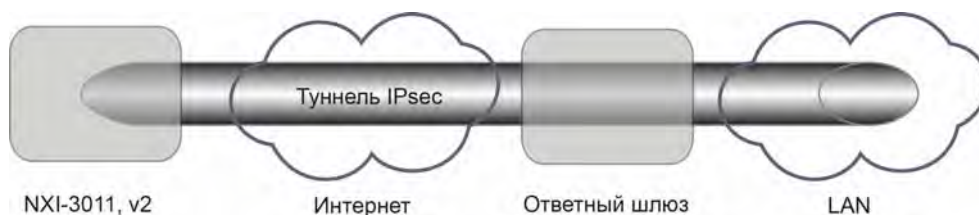


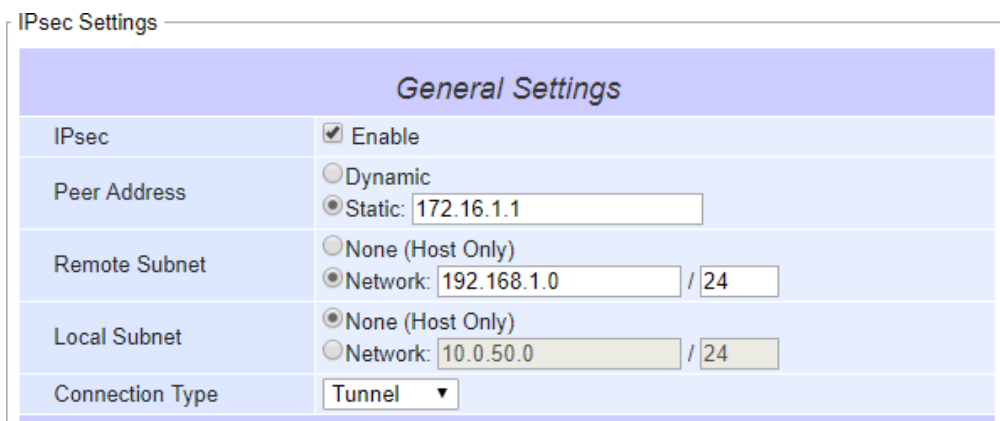
Рис. 4.27. IPsec VPN-туннель с топологией хост-сеть.

Сценарий: хост-сеть со статическим одноранговым узлом, как показано на рисунке 4.28.

- Необходимо поставить флажок в поле Enable для IPsec.
- В поле Peer Address необходимо выбрать опцию Static и ввести IPv4 адрес однорангового узла.

Примечание: Когда адрес однорангового узла вводится как статический адрес, NetXpert NXI-3011, v2 является инициатором, который берет на себя инициативу и устанавливает соединение, или может быть респондентом, ожидающим соединения. NetXpert NXI-3011, v2 также действует как респондент и пассивно принимает соединение, инициированное удаленным шлюзом.

- Необходимо задать адрес IPv4 в Remote Subnet с количеством битов для маски подсети в «длине префикса адреса» или после символа «/».
- Поскольку у этого IPsec VPN-соединения на одном конце расположена подсеть, для параметра Connection Type должно быть установлено значение только Tunnel.



General Settings	
IPsec	☒ Enable
Peer Address	☐ Dynamic ☒ Static: 172.16.1.1
Remote Subnet	☐ None (Host Only) ☒ Network: 192.168.1.0 / 24
Local Subnet	☒ None (Host Only) ☐ Network: 10.0.50.0 / 24
Connection Type	Tunnel

Рис. 4.28. Общие настройки для соединения хост-сеть со статическим одноранговым узлом.

Сценарий: хост-сеть с динамическим одноранговым узлом, как показано на рисунке 4.29.

- Необходимо поставить флажок в поле Enable для IPsec.
- В поле Peer Address необходимо выбрать опцию Dynamic.

Примечание: Когда VPN-соединение установлено с одноранговым узлом с динамическим IP-адресом, NetXpert NXI-3011, v2 будет действовать как респондент и пассивно примет соединение, инициированное удаленным шлюзом.

- Необходимо установить сетевой IPv4-адрес в поле Remote Subnet с количеством битов для маски подсети в «длине префикса адреса» или после символа «/».
- Поскольку это VPN-соединение IPsec на одном конце имеет подсеть, для параметра Connection Type должно быть установлено только значение Tunnel.

IPsec Settings

General Settings	
IPsec	☒ Enable
Peer Address	☒ Dynamic ☐ Static:
Remote Subnet	☐ None (Host Only) ☒ Network: 192.168.1.0 / 24
Local Subnet	☒ None (Host Only) ☐ Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Рис. 4.29. Общие настройки для соединения хост-сеть с динамическим одноранговым узлом.

4.7.3.3. Соединения сеть-сеть (подсеть-подсеть)

Для соединений типа сеть-сеть (или подсеть-подсеть) также можно настроить два сценария: со статическим одноранговым узлом или с динамическим одноранговым узлом. VPN-туннель будет создан между двумя отдельными частными подсетями. Следует отметить, что в этих сценариях NetXpert NXI-3011, v2 является шлюзом для локальной сети. Топология сеть-сеть для обоих сценариев показана на рисунке 4.30. Необходимо следовать инструкциям ниже для настройки Общих параметров каждого сценария.



Рис. 4.30. IPsec VPN туннель с топологией сеть-сеть.

Сценарий: сеть-сеть со статическим одноранговым узлом, как показано на рисунке 4.31.

- Необходимо поставить флажок в поле Enable для IPsec.
- В поле Peer Address необходимо выбрать опцию Static и ввести адрес однорангового узла IPv4.

Примечание: Когда одноранговый адрес вводится как статический адрес, NetXpert NXI-3011, v2 является инициатором, который берет на себя инициативу и устанавливает соединение, или может быть респондентом, ожидающим соединения. NetXpert NXI-3011, v2 также действует как респондент и пассивно принимает соединение, инициированное удаленным шлюзом.

- Необходимо установить сетевой IPv4-адрес в поле Remote Subnet с количеством бит для маски подсети в «длине префикса адреса» или после символа “/”.
- Необходимо установить сетевой адрес IPv4 в поле Local Subnet с количеством бит для маски подсети в «длине префикса адреса» или после символа “/”.
- Поскольку это VPN-соединение IPsec на обоих концах имеет подсети, для параметра Connection Type должно быть установлено только значение Tunnel.

General Settings	
IPsec	☒ Enable
Peer Address	☐ Dynamic ☒ Static: 172.16.1.1
Remote Subnet	☐ None (Host Only) ☒ Network: 192.168.1.0 / 24
Local Subnet	☐ None (Host Only) ☒ Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Рис. 4.31. Общие настройки для соединения сеть-сеть со статическим одноранговым узлом.

Сценарий: сеть-сеть с динамическим одноранговым узлом, как показано на рисунке 4.32.

- Необходимо поставить флажок в поле Enable для IPsec.
- В поле Peer Address необходимо выбрать опцию Dynamic.

Примечание: Когда VPN-соединение установлено с одноранговым узлом с динамическим IP-адресом, NetXpert NXI-3011, v2 будет действовать как респондент и пассивно примет соединение, инициированное удаленным шлюзом

- Необходимо установить сетевой IPv4-адрес в поле Remote Subnet с количеством бит для маски подсети в «длине префикса адреса» или после символа “/”.
- Необходимо установить сетевой адрес IPv4 в поле Local Subnet с количеством бит для маски подсети в «длине префикса адреса» или после символа “/”.
- Поскольку это VPN-соединение IPsec на обоих концах имеет подсети, для параметра Connection Type должно быть установлено только значение Tunnel.

General Settings	
IPsec	☒ Enable
Peer Address	☒ Dynamic ☐ Static:
Remote Subnet	☐ None (Host Only) ☒ Network: 192.168.1.0 / 24
Local Subnet	☐ None (Host Only) ☒ Network: 10.0.50.0 / 24
Connection Type	Tunnel

Рис. 4.32. Общие настройки для соединения сеть-сеть с динамическим одноранговым узлом.

4.8. STP

Серия серверов промышленных устройств NetXpert NXI-3011, v2 поддерживает функционал STP. Протокол связующего дерева (STP) обеспечивает предотвращение возникновения петель коммутации и широковещательного шторма на уровне OSI 2. Петля коммутации образуется в сети, когда имеется несколько соединений или избыточных связей между двумя сетевыми коммутаторами.

Петля коммутации может создавать широковещательный шторм, который представляет собой накопление широковещательного и многоадресного трафика в компьютерной сети. Поскольку широковещательные и многоадресные сообщения пересылаются коммутаторами на каждый порт, коммутаторы будут повторно передавать широковещательные сообщения, вызывая перегрузки в сети. STP создает топологию связующего дерева и отключает те звенья сети, которые не являются частью связующего дерева, оставляя только один активный путь между любыми двумя узлами сети. Эта функция позволяет избежать лавинной пересылки и повысить надежность сети.

RSTP (протокол быстрого связующего дерева), IEEE 802.1W - это единственный режим связующего дерева, поддерживаемый в NetXpert NXI-3011, v2. Это шаг в развитии STP (стандарт IEEE 802.1D), но оно все еще обратно совместимо со стандартом STP. RSTP имеет преимущество перед STP. При изменении топологии, такой как неисправность канала в сети, RSTP значительно быстрее преобразуется в новую топологию связующего дерева. RSTP улучшает конвергенцию в каналах связи точка-точка, сокращая максимальное время ожидания до трехкратного интервала Hello, удаляя состояние прослушивания (Learning) STP и обмениваясь подтверждениями установления связи между двумя коммутаторами, чтобы быстро перевести порт в состояние пересылки.

Меню Spanning Tree и его подменю можно найти в левой части WEB-интерфейса NetXpert NXI-3011, v2. Список меню Spanning Tree показан на рисунке 4.33. Подменю Spanning Tree - это Setting (настройки), Bridge Info (Информация о мосте) и Port Setting (Настройка порта). Каждое из этих подменю будет описано в следующих главах.

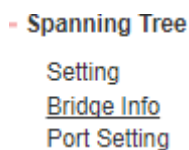


Рис. 4.33. Меню Spanning Tree.

4.8.1. Настройки связующего дерева

На рисунке 4.34 показан пример страницы Setting меню Spanning Tree. Страница Spanning Tree Setting разделена на три части: Mode Setting, Main Setting и Port Setting.

Для NetXpert NXI-3011, v2 пользователь может выбрать только один режим связующего дерева, которым является RSTP (протокол быстрого связующего дерева) в разделе Mode Setting. Пользователь может включить или отключить протокол связующего дерева в разделе Main Setting (Основные настройки), установив флажок в поле опции Enabled.

Следует отметить, что когда опция Enabled включена, остальные поля будут активными. Затем пользователь может настроить параметры Priority, Maximum Age, Hello Time и Forward Delay или может оставить значения по умолчанию для каждого из этих параметров.

В разделе Port Setting пользователь может выбрать два разных порта для параметров Primary Port (Основной порт) и Secondary Port (Вторичный порт) из выпадающего списка. После настройки параметров связующего дерева необходимо нажать кнопку Update в конце страницы, чтобы изменения вступили в силу. Описание каждого параметра приведено в таблице Таблица 4.2. Описание параметров STP.

Рис. 4.34. WEB-страница настроек связующего дерева.

Таблица 4.2. Описание параметров STP.

Параметр	Описание	Заводские настройки
Mode	Режим протокола связующего дерева, который будет включен на устройстве NetXpert NXI-3011, v2.	RSTP
Enabled	Необходимо поставить флажок в этом поле для включения функционала связующего дерева.	Disable
Priority	Необходимо ввести число для настройки приоритета устройства. Диапазон значений от 0 до 61440. Чем меньше число, тем выше приоритет.	32768
Maximum Age	Максимальное ожидаемое время получения hello-сообщения. Оно должно быть, больше, чем интервал Hello Time.	20
Hello Time	Интервал Hello time в секундах. Диапазон значений от 1 до 10.	2
Forward Delay	Необходимо указать время, затрачиваемое на прослушивание и изучение состояний в секундах. Диапазон значений от 4 до 30.	15
Primary Port	Основной порт	LAN1
Secondary Port	Вторичный порт	LAN2

Примечание: для отключения функции связующего дерева на NetXpert NXI-3011, v2 пользователь может убрать флажок в поле Enable и затем нажать кнопку Update.

4.8.2. Параметры коммутатора STP

Bridge Info (информация) отображает текущие настройки параметров протокола связующего дерева, как показано на рисунке 4.35. Следует отметить, что на этой странице не будут отображаться данные по всем полям, если на WEB-странице настройки связующего дерева не был включен RSTP.

Информация далее разделена на две части: Root Information (информация о корневом коммутаторе) и Topology Information (информация о топологии). Чтобы проверить последнюю информацию, необходимо нажать на кнопку Refresh в конце страницы. В таблице 4.3 и таблице 4.4 приведены описания каждой записи в корневой информационной таблице и информационной таблице топологии, соответственно.

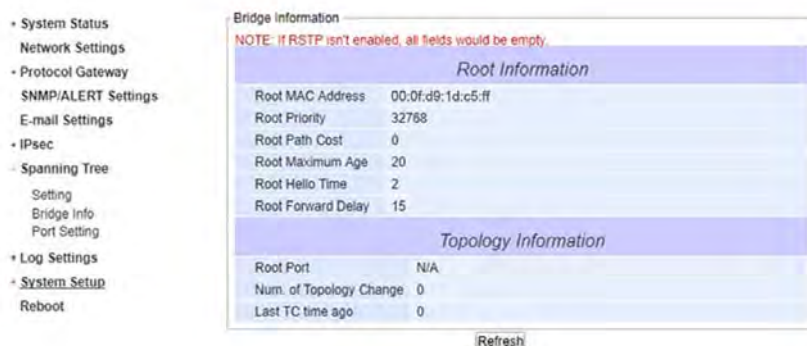


Рис. 4.35. WEB-страница информации коммутатора STP.

Таблица 4.3. Информация о корне моста.

Параметр	Описание
Root MAC Address	MAC-адрес корневого коммутатора.
Root Priority	Значение приоритета корневого коммутатора. Устройство с наивысшим приоритетом имеет наименьшее значение приоритета, и оно будет выбрано в качестве корневого коммутатора.
Root Path Cost	Стоимость корневого пути рассчитывается исходя из скорости передачи данных порта устройства.
Root Maximum Age	Максимальный срок действия корневого коммутатора - это максимальное время, в течение которого устройство будет хранить информацию протокола, полученную по каналу связи.
Root Hello Time	Интервал hello корневого коммутатора, которое представляет собой интервал времени, в течение которого RSTP отправляет сообщение hello соседним узлам для обнаружения любых изменений в топологии.
Root Forward Delay	Задержка на передачу корневого коммутатора - это время, в течение которого коммутатор будет находиться в состоянии обучения и прослушивания, прежде чем канал начнет пересылку.

Таблица 4.4. Информация о топологии моста.

Параметр	Описание
Root Port	Порт кратчайшего пути до корневого коммутатора.
Num. of Topology Change	Общее количество изменений топологии за все время.
Last TC time ago	Продолжительность времени с момента последнего изменения топологии.

4.8.3. Настройки порта связующего дерева

Настройки Port Setting связующего дерева отображают сконфигурированное значение протокола связующего дерева для каждого порта, как показано на рисунке 4.36 и рисунке 4.37.

Сконфигурированная информация для каждого порта - это state (состояние), role (роль), path cost (стоимость тракта), path priority (приоритет тракта), link type (тип канала связи), edge (границы), cost (стоимость) и designated information (назначенная информация).

Чтобы проверить последние обновления статистики, необходимо нажать на кнопку Refresh.

В таблице 4.5 приведены описания настроек портов связующего дерева. Если протокол связующего дерева включен, таблица Spanning Tree Port Setting становится редактируемой, и на этой странице можно настроить четыре параметра Path Cost (Config) (стоимость тракта), приоритет пути (Pri), Type Link (Config) (тип канала связи) и Edge (Config) (границы). Пользователь может использовать кнопку Update, чтобы сохранить настройки.

Spanning Tree Port Setting

Port	State	Role	Path Cost		Pri	Link Type		Edge
			Config	Actual		Config	P2P?	
Port1	Disc	Disabled	200000	200000	128	P2P	Yes	☐
Port2	Fwd	Designated	200000	200000	128	P2P	Yes	☒

Рис. 4.36. Настройки порта связующего дерева (часть 1).

Spanning Tree Port Setting

Link Type		Edge		Designated					
Config	P2P?	Config	Edge?	Cost	P.Pri	Port	B.Pri	Bridge MAC	
P2P	Yes	☐	No	0	0	1	0	00:00:00:00:00:00	
P2P	Yes	☒	Yes	0	128	2	32768	00:0f:d9:1d:c5:ff	

Рис. 4.37. Настройки порта связующего дерева (часть 2).

Таблица 4.5. Описание настроек порта связующего дерева.

Параметр	Описание	Заводские настройки
Port	Имя порта NetXpert NXI-3011, v2	-
State	Состояние порта: 'Disc': отбрасывание - пользовательские данные не передаются через порт. 'Lrn': Изучение - порт еще не пересылает кадры, но заполняет свою таблицу MAC-адресов. 'Fwd': передача – порт полностью в работе.	Недоступно
Role	не-STP или STP роли порта моста RSTP: 'Root' – порт, через который идет кратчайший маршрут до корневого коммутатора. 'Designated' - порт переадресации для определенного сегмента LAN. 'Alternate' - альтернативный путь к корневому коммутатору. 'Backup' - резервный путь к сегменту, к которому уже подключен другой порт коммутатора. 'Disabled' – порт отключен.	Non- STP

Path Cost		Настройка стоимости пути для каждого порта коммутатора.	
	Config	Настройка стоимости пути (по умолчанию: 0, что означает использование системного значения по умолчанию (в зависимости от скорости соединения)).	0
	Actual	Фактическое значение стоимости пути (для RSTP см. Примечание 1 ниже и таблицу).	0
Pri		Установка приоритета порта, используемого в поле Port ID пакета BPDU, значение = $16 \times N$, ($N:0\sim15$).	128
Link Type		Соединение между двумя или более коммутаторами (для RSTP).	
	Config	Настройка типа канала связи. P2P: порт, который работает в полнодуплексном режиме, предполагается, что это канал типа точка-точка. Non-P2P: полудуплексный порт (через хаб). Auto: автоматическое определение типа канала связи.	Auto
	P2P?	Yes: Этот порт является портом точка-точка (P2P). No: Этот порт не является портом точка-точка (Non-P2P).	No
Edge		Пограничный порт - это порт, к которому другие коммутаторы STP/RSTP не подключаются (для RSTP). Пограничный порт может быть установлен в состояние пересылки напрямую.	
	Config	Функционал граничного порта установлен: Yes или No.	No
	Edge?	Yes: этот порт является граничным портом. No: этот порт является граничным портом.	No
Designated		Показывает некоторую информацию о лучшем пакете BPDU через этот порт.	
	Cost	Стоимость корневого пути.	0
	P. Pri. (Port Priority)	Приоритет порта (верхние 4 бита идентификатора порта), значение = $16 \times N$, ($N: 0\sim15$).	128
	Port	Номер интерфейса (нижние 12 бит идентификатора порта).	-
	Bri. Pri. (Bridge Priority)	Приоритет моста, (значение = $4096 \times N$, ($N: 0\sim15$)).	32768
	Bridge MAC	MAC-адрес коммутатора, который отправил этот BPDU.	-

Примечание:

В основном, стоимость пути зависит от скорости соединения. В таблице 4.6 перечислены значения по умолчанию стоимости пути для RSTP.

Таблица 4.6. Значения по умолчанию стоимости пути для RSTP.

<i>Скорость передачи данных</i>	<i>Стоимость RSTP (802.1W-2004)</i>
4 Мбит/сек	5,000,000
10 Мбит/сек	2,000,000
16 Мбит/сек	1,250,000
100 Мбит/сек	200,000
1 Гбит/сек	20,000
2 Гбит/сек	10,000
10 Гбит/сек	2,000

4.9. Настройки SNMP/ALERT

Простой протокол управления сетью (SNMP) используется программным обеспечением управления сетью для мониторинга устройств в сети, получения информации о сетевом статусе устройств и для настройки сетевых параметров устройств.

Страница настроек SNMP/ALERT, показанная на рисунке 4.38, позволяет пользователю настроить устройство NetXpert NXI-3011, v2 так, чтобы его можно было просматривать сторонним программным обеспечением SNMP, и позволяет NetXpert NXI-3011, v2 отправлять события оповещения администратору и SNMP-серверу прерывания.

SNMP/ALERT Settings

The SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

Basic Data Objects	
System Contact	contact
System Name	System
System Location	location
SNMP	☒ Enable
SNMP Version	v2
Read Community	
Write Community	
SNMP Trap Server	
SNMP Trap Server	0.0.0.0

Event alert settings

Alert Type	Email	SNMP Trap
Cold start	☐	☐
Warm start	☐	☐
Authenticate failed	☐	☐
IP Address changed	☐	☐
Password changed	☐	☐

Рис. 4.38. WEB-страница настроек SNMP/Alert.

NetXpert NXI-3011, v2 предоставляет три основных поля SNMP в разделе Basic Data Objects (основные объекты данных): System Contact - обычно используется для указания контактной информации устройства на случай чрезвычайной ситуации (значение по умолчанию «contact»), System Name - обычно используется для идентификации этого устройства (значение по умолчанию «System»), и System Location - обычно используется для указания местоположения устройства (значение по умолчанию - «location»).

Чтобы сделать информацию об устройстве доступной для общего просмотра/редактирования, можно включить функцию SNMP, установив флажок Enable и введя две парольные фразы (или строки сообщества SNMP) под ним. Следует отметить, что когда флажок SNMP не проставлен, появятся три строки параметров настройки, как показано на рисунке 4.38.

Ввод парольной фразы для опции «Read Community» позволяет устройству NetXpert NXI-3011, v2 предоставлять другому программному обеспечению для управления сетью свою информацию для чтения. Ввод парольной фразы для опции «Write Community», позволяет устройству NetXpert NXI-3011, v2 предоставлять другому программному обеспечению для управления сетью свою информацию для чтения/изменения. По умолчанию строки сообщества SNMP в NetXpert NXI-3011, v2 (или парольные фразы) для сообществ Read Community и Write Community, являются, «public» и «private» соответственно, как показано на рисунке 4.38.

Дополнительно можно настроить SNMP Trap Server в сети для получения и сбора всех аварийных сообщений от NetXpert NXI-3011, v2. Чтобы настроить NetXpert NXI-3011, v2 для отправки аварийных сообщений, возникших в результате любых непредвиденных ситуаций, можно заполнить IP-адрес сервера прерываний SNMP Trap Server в поле, показанном на рисунке 4.38. Следует отметить, что любые изменения в этих настройках вступят в силу после перезагрузки устройства NetXpert NXI-3011, v2.

В разделе SNMP Trap Server есть список типов предупреждений Alert Type в окне Event alert settings на рисунке 4.38. Для каждого события оповещения допускается до двух возможных действий: Email и SNMP Trap.

Можно включить соответствующие действия для каждого события оповещения, установив флажок в столбце Email и/или SNMP Trap. Если установлен флажок Email и происходит соответствующее событие, для NetXpert NXI-3011, v2 будет инициировано действие по отправке оповещения по электронной почте на назначенные адреса, заданные в настройках электронной почты (описанных в следующей главе).

Если установлен флажок SNMP Trap и происходит соответствующее событие, для NetXpert NXI-3011, v2 будет инициировано действие по отправке предупреждение о прерывании на назначенный сервер прерывания SNMP (указанный в предыдущем абзаце). Существует пять событий, которые вызовут сообщение предупреждения от NetXpert NXI-3011, v2, как показано на рисунке 4.38. Однако о каком-то событии можно сообщить только по электронной почте. Эти предупреждения полезны для контроля безопасности или мониторинга безопасности устройства NetXpert NXI-3011, v2:

- Cold Start: это событие происходит при запуске устройства после отключения электропитания.
- Warm Start: это событие происходит при программной перезагрузке устройства.
- Authentication Failure: это событие возникает, когда вводится неправильное имя пользователя и/или пароль, что может указывать на несанкционированный доступ к NetXpert NXI-3011, v2.
- IP Address Changed: это событие возникает при изменении IP-адреса устройства NetXpert NXI-3011, v2.
- Password Changed: это событие происходит при изменении пароля администратора.

После окончания конфигурирования the SNMP/Alert Settings необходимо нажать кнопку Save & Apply для сохранения внесенных изменений и применения настроек. После того, как сохранение и применение настроек завершено, WEB-браузер останется на странице SNMP/Alert Settings. Если необходимо отменить изменения и вернуть первоначальные значения всем параметрам, следует нажать на кнопку Cancel.

4.10. Настройки E-Mail

Когда устройство NetXpert NXI-3011, v2 генерирует аварийное и/или предупреждающее сообщение, оно может отправить электронное письмо на почтовый ящик администратора. На этой странице настроек электронной почты E-mail Settings можно настроить NetXpert NXI-3011, v2, чтобы иметь возможность отправлять электронную почту.

На рисунке 4.39 показана страница настроек электронной почты, на которой есть две конфигурируемые части: E-mail Address Settings (настройки адреса электронной почты) и E-mail Server (сервер электронной почты). Сначала в разделе E-mail Address Settings необходимо указать адрес электронной почты отправителя в текстовом поле Sender, который будет использоваться в поле «От» письма.

Следует отметить, что максимальная длина адреса электронной почты отправителя составляет 48 символов. Затем в текстовом поле Receiver можно ввести несколько адресов получателей, которые будут использоваться в поле «Кому» электронной почты. Следует отметить, что для ввода нескольких адресов электронной почты получателя в текстовом поле Получателя, необходимо разделять их точкой с запятой (;).

> E-mail Settings

E-mail Settings

E-mail Address Settings

Sender	
Receiver	 Use a semicolon (;) to delimit the receiver's e-mail address.

E-mail Server

SMTP Server	
Authentication	☐ SMTP server authentication required.
User name	
Password	

Save & Apply

Cancel

Рис. 4.39. WEB-страница настроек E-mail.

Затем в разделе E-mail Server необходимо ввести IP-адрес или Host Name (имя хоста) почтового сервера, находящегося в локальной сети в текстовом поле SMTP Server. Максимальная длина адреса SMTP-сервера равна 31 символа. Если почтовый сервер (или сервер Простого протокола электронной почты (SMTP)) требует аутентификации пользователя, необходимо поставить флажок в поле "SMTP server authentication required" в опции Authentication. После активации этой опции можно ввести имя пользователя (Username) и пароль (Password) ниже. Следует обратиться к сетевому администратору, чтобы узнать IP-адрес почтового сервера Mail Server и требуемые пароль и имя пользователя.

Внимание! Также важно правильно настроить шлюз по умолчанию и DNS-серверы в настройках сети, чтобы NetXpert NXI-3011, v2 мог искать доменные имена и направлять электронную почту на соответствующий шлюз по умолчанию. В дефолтных настройках ДНС "0.0.0.0 (отсутствует)".

После окончания конфигурирования настроек E-mail Settings необходимо нажать кнопку Save & Apply для сохранения внесенных изменений и применения настроек. После того, как сохранение и применение настроек завершено, WEB-браузер останется на странице E-mail Settings. Если необходимо отменить изменения и вернуть первоначальные значения всем параметрам, следует нажать на кнопку Cancel.

4.11. Настройки журнала

В меню настроек журнала Log Settings WEB-интерфейса серии Промышленных серверов последовательных устройств NetXpert NXI-3011, v2 можно настроить ведение журнала различных данных для устройства. На рисунке 4.40 приведен список подменю раздела настроек журнала Log Settings. Оно состоит из пунктов System Log Settings, COM Log Settings, Event Log и COM Datalog. Каждый из этих разделов подменю будет описан в следующих главах.

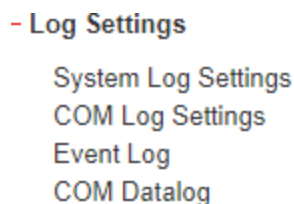


Рис. 4.40. Меню настроек журнала.

4.11.1. Настройки журнала системы

Функция Syslog по умолчанию включена и не может быть отключена для NetXpert NXI-3011, v2. Она используется для сохранения журнала системных событий и отправки отчетов на внешний сервер Syslog при необходимости. На рисунке 4.41 показана страница настроек журнала системы System Log Settings в меню Log Settings. Описание каждой опции представлено ниже.

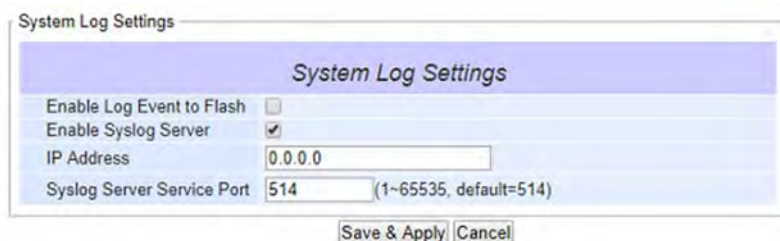


Рис. 4.41. WEB-страница настроек журнала системы в меню Log Settings.

- Enable Log Event to Flash: когда установлен этот флажок, NetXpert NXI-3011, v2 будет записывать события журнала в локальную флэш-память. В противном случае события журнала будут очищены при перезагрузке устройства, поскольку по умолчанию они хранятся в оперативной памяти. Enable Syslog Server: когда установлен этот флажок NetXpert NXI-3011, v2 будет отправлять события системного журнала на удаленный сервер Syslog с указанным IP-адресом (следующая опция). Все данные, отправленные/полученные от последовательного интерфейса, будут записаны в журнал и отправлены на сервер Syslog.
- Syslog Server IP: в этом поле пользователь должен указать IP-адрес удаленного сервера системного журнала.
- Syslog Server Service Port: этот параметр позволяет пользователю указать номер порта удаленного сервера системного журнала в диапазоне от 1 до 65535. Следует отметить, что по умолчанию номер порта равен 514.

После окончания конфигурирования настроек Log Settings необходимо нажать кнопку Save & Apply для сохранения внесенных изменений и применения настроек. После того, как сохранение и применение настроек завершено, WEB-браузер останется на странице Log Settings. Если необходимо отменить изменения и вернуть первоначальные значения всем параметрам, следует нажать на кнопку Cancel.

4.11.2. Настройки журнала COM-порта

Передача данных через COM-порт может быть занесена в журнал для целей записи и отладки. Дополнительно записи журнала могут быть также отправлены на внешний сервер Syslog. На рисунке 4.42 показана страница настроек журнала COM Log Settings в меню Log Settings. Описание каждой опции приведено ниже.

COM Log Settings

COM Log Settings

☒ Log Data Contents Types: ☒ HEX ☐ ASCII

COM Ports: ☐ COM1 ☐ COM2 ☐ COM3 ☐ COM4

Enable Syslog Server: ☐ Enable

IP Address: 0.0.0.0

Syslog Server Service Port: 514 (1~65535, default=514)

Save & Apply Cancel

Рис. 4.42. COM Log Settings WEB-страница under System Setup.

- Log Data Contents: если эта опция включена, функция ведения журнала COM-порта будет регистрировать данные контента, которые передаются и принимаются в необработанных байтах. Если эта опция отключена, функция ведения журнала COM-порта будет регистрировать только длину данных, чтобы снизить нагрузку на систему.

Примечание: NetXpert NXI-3011, v2 может хранить в устройстве до 100 кбайт. Запрос или ответ будут находиться в одной строке, а данные длиной более 512 байт перейдут на другую строку. Можно получить журналы с помощью FTP-клиента. Имя пользователя для FTP такое же, как имя для входа через WebUI. Журналы расположены в /var/log/logcomxx (xx это номер порта). Когда зарезервированное пространство заполнено, новые журналы будут заменять старые. Настоятельно рекомендуется отправлять журналы COM на удаленный сервер Syslog.

- Types Формат данных: Здесь имеется две кнопки-переключателя: шестнадцатеричный (HEX) и ASCII, пользователю необходимо выбрать желаемый формат данных журнала.
- COM Ports: Пользователь может выбрать, данные каких портов будут регистрироваться в журнале, установив соответствующие флажки.
- Enable Syslog Server: когда установлен этот флажок, NetXpert NXI-3011, v2 будет отправлять события журнала COM на удаленный сервер Syslog. Можно отправлять журналы COM на тот же сервер Syslog, который использовался ранее для регистрации событий (см. пп. 4.11.1).
- IP Address: если сервер Syslog включен в предыдущей опции, необходимо указать в этом поле IP-адрес удаленного сервера Syslog.
- Syslog Server Service Port: этот параметр позволяет пользователю указать номер порта удаленного сервера системного журнала в диапазоне от 1 до 65535. Следует отметить, что по умолчанию номер порта равен 514.
- После окончания конфигурирования настроек COM Log Settings необходимо нажать кнопку Save & Apply для сохранения внесенных изменений и применения настроек. После того, как сохранение и применение настроек завершено, WEB-браузер останется на странице COM Log Settings. Если необходимо отменить изменения и вернуть первоначальные значения всем параметрам, следует нажать на кнопку Cancel.

4.11.3. Журнал событий

На этой странице отображается текущий журнал событий или системный журнал, хранящийся на устройстве NetXpert NXI-3011, v2. На рисунке 4.43 показан пример зарегистрированного события. Каждая запись системного журнала (System Log) состоит из описания времени (Time), уровня серьезности (Severity) и сообщения (Message).

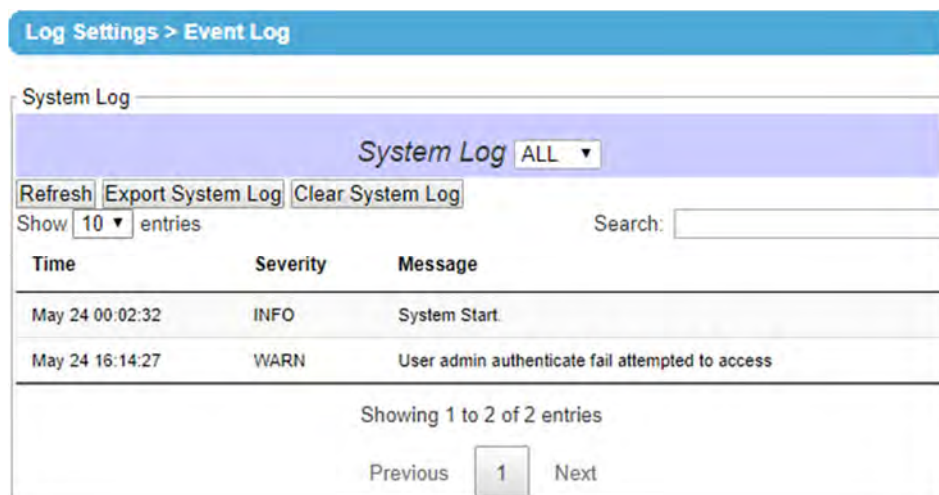


Рис. 4.43. WEB-страница системного журнала в меню настройки системы.

В конце страницы System Log имеется три гиперссылки, которые можно использовать для навигации по записям. Можно нажать на кнопку «Previous», чтобы перейти на предыдущую страницу журнала или нажать на кнопку «Next», чтобы перейти на следующую страницу журнала. Вверху таблицы System Log имеется три кнопки: Refresh, Export System Log и Clear System Log. Для отображения последних событий можно нажать на кнопку «Refresh».

При нажатии на кнопку «Export System Log», файл журнала будет сохранен на ПК. При нажатии на кнопку «Clear System Log» можно очистить все события, сохраненный на устройстве, и журнал системы System Log будет пуст. Будет показано сообщение «No data available in table» (в таблице отсутствуют данные) в середине таблицы.

Кроме того, можно выбрать из выпадающего списка от 10 до 25 записей для отображения в пункте Show entries. Также, можно выполнить поиск по журналу System Log, введя ключевое слово в поле Search.

4.11.4. Журнал данных COM Datalog

На этой странице отображается текущий журнал данных COM, хранящийся на устройстве. Нужный номер 48COM-порта можно выбрать из выпадающего списка COM x Log на рисунке 4.44, который позволяет отображать журналы с разных COM-портов. Пример журнала COM 1 Log показан на рисунке 4.44. Каждая запись в журнале состоит из времени (Time), индекса COM (COM Index), направления (T/R) и данных (Data).

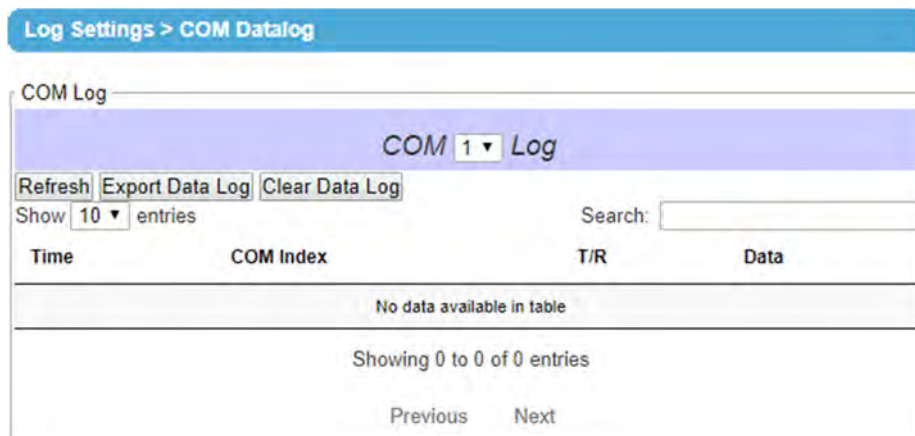


Рис. 4.44. WEB-страница журнала данных COM в меню настройки Log Settings.

Под заголовком COM x Log есть три кнопки: Refresh, Export Data Log и Clear Data Log. Первая кнопка «Refresh» может быть использована для обновления приведенной ниже таблицы COM-журнала и отображения последней информации. Вторая кнопка «Export Data Log» позволяет пользователю сохранить данные журнала на своем ПК. Имя файла по умолчанию для экспортированного журнала данных будет «DataLog.txt». Третья кнопка «Clear Data Log» очистит все события, хранящиеся на устройстве, и журнал данных COM будет очищен с последующим сообщением «No data available in table» (в таблице отсутствуют доступные данные).

В конце страницы COM Datalog есть две гиперссылки, которые можно использовать для навигации по всем записям. Можно нажать на кнопку «Previous», чтобы перейти на предыдущую страницу журнала или нажать на кнопку «Next», чтобы перейти на следующую страницу журнала.

4.12. Настройка системы

В меню настройки системы System Setup WEB-интерфейса серии Промышленных серверов последовательных устройств NetXpert NXI-3011, v2 можно выполнить ряд задач для администрирования устройства. На рисунке 4.45 приведен список подменю раздела System Setup. Он состоит из пунктов Date/Time Settings, Admin Settings, Firmware Upgrade, Backup/Restore Setting и Ping. Каждое из этих подменю будет описано в следующих главах.

- System Setup
 - Date/Time Settings
 - Admin Settings
 - Firmware Upgrade
 - Backup/Restore Settings
 - Ping

Рис. 4.45. Меню настройки системы.

4.12.1. Настройки даты/времени

Дата и время могут быть установлены вручную или с помощью сетевого протокола службы времени (NTP) для автоматической синхронизации даты и времени устройства NetXpert NXI-3011, v2 с сервером синхронизации.

На рисунке 4.46 показана страница Настроек Даты/Времени (Date/Time Settings).

Первая часть страницы представляет собой последнюю Текущую Дату/Время в формате день/месяц/год ЧЧ:ММ:СС.

Вторая часть страницы - Настройки Часового Пояса (Time Zone Settings). Можно выбрать свой локальный часовой пояс из выпадающего списка.

Третья часть страницы - это настройки NTP-сервера NTP Server Settings. В этой части можно включить локальную службу NTP для NetXpert NXI-3011, v2, установив флажок «Local NTP Service» в разделе «NTP Settings», или автоматически синхронизироваться с сервером синхронизации или NTP-сервером.

Чтобы включить автоматическую синхронизацию времени, необходимо установить флажок «Sync with NTP Server». Затем перейти к вводу IP-адреса или имени хоста для NTP-сервера. Следует отметить, что если введено имя хоста, должен быть правильно настроен DNS-сервер.

Четвертая часть страницы - это настройки перехода на летнее время, которые можно включить, если установлен флажок «Enable Daylight Saving Time». Когда он проставлен, пользователь может выбрать подробные настройки периода перехода на летнее время, такие как Дата начала (Start Date) и Дата окончания (End Date) и смещение (Offset).

Пятая часть страницы - это настройки времени вручную (Manual Time Settings), где можно установить дату и время, используя соответствующие выпадающие списки на рисунке 4.46.

Date/Time Settings

The NTP (Network Time Protocol) is used to synchronize the date/time from the NTP server.

Current Date/Time

15 / Jan / 2019 15:43:13

Time Zone Settings

Time Zone (GMT+03:00) Moscow, St. Petersburg, Volgograd

NTP Settings

Local NTP Service ☐

Sync with NTP Server ☐

NTP Server

Daylight Saving Time Settings

☐ Enable Daylight Saving Time

Start Date -- / -- / -- (Month / Week / Date / Hour)

End Date -- / -- / -- (Month / Week / Date / Hour)

Offset 0 hour(s)

Manual Time Settings

Date -- / -- / --

Time -- : -- : --

Save & Apply Cancel

Рис. 4.46. WEB-страница настроек Даты/Времени в меню настройки системы.

Внимание! Также важно правильно настроить шлюз по умолчанию и DNS-серверы в настройках сети, чтобы NetXpert NXI-3011, v2 мог искать DNS-имена и направлять на нужный NTP-сервер.

После окончания конфигурирования настроек Date/Time Settings необходимо нажать на кнопку Save & Apply для сохранения внесенных изменений и применения настроек. После того, как сохранение и применение настроек завершено, WEB-браузер останется на странице Date/Time Settings. Если необходимо отменить изменения и вернуть первоначальные значения всем параметрам, следует нажать на кнопку Cancel.

4.12.2. Настройки администратора

Серия NetXpert NXI-3011, v2 поддерживает управление пользователями и паролями на странице Admin Settings в меню System Setup. По умолчанию имя пользователя “admin” и пароль “default”. Для настройки или изменения их значений можно ввести информацию в полях User name (имя пользователя), Old password (старый пароль), New password (новый пароль) и Repeat new password (повторить новый пароль) в разделе Account Settings, как показано на рисунке 4.47. В конце страницы Admin Settings расположен раздел Web mode, который позволяет пользователю выбрать между обычным HTTP или HTTPS для безопасного соединения с помощью пользовательского WEB-интерфейса (Web UI).

System Setup > Admin Settings

Admin Settings
Set up the login user name and password.

Account Settings

User name	admin
Old password	
New password	
Repeat new password	

Web mode

Web Mode	☒ HTTP ☐ HTTPS
----------	---

Save & Apply Cancel

Рис. 4.47. WEB-страница настроек администратора в меню настройки системы.

После окончания конфигурирования настроек Admin Settings необходимо нажать на кнопку Save & Apply для сохранения внесенных изменений и применения настроек. Появится новое всплывающее окно для повторной аутентификации пользователя для доступа к WEB-интерфейсу NetXpert NXI-3011, v2, как показано на рисунке 4.7. Необходимо повторно ввести имя пользователя и пароль для входа в NetXpert NXI-3011, v2. После завершения сохранения, применения и повторной аутентификации WEB-браузер останется на странице настроек Admin Settings. Если необходимо отменить изменения и вернуть первоначальные значения всем параметрам, следует нажать на кнопку Cancel.

4.12.3. Обновление прошивки

Обновленные прошивки для NetXpert NXI-3011, v2 время от времени предоставляются компанией HATEКС для исправления ошибок и оптимизации производительности. Очень важно, чтобы устройство НЕ было выключено или отключено электропитание во время обновления прошивки (пожалуйста, будьте терпеливы, поскольку этот процесс может занять до 5 минут). Перед обновлением прошивки следует убедиться, что устройство имеет надежный источник электропитания, который не будет отключен или перезапущен во время процесса обновления прошивки.

Чтобы обновить новую прошивку на NetXpert NXI-3011, v2, необходимо загрузить последнюю версию прошивки для вашей модели NetXpert NXI-3011, v2. Затем скопировать новый файл прошивки на локальный компьютер. Следует отметить, что файл прошивки представляет собой файл в двоичном формате с расширением «.dld». Затем необходимо открыть WEB-интерфейс и выбрать страницу «Firmware Upgrade» в меню «System Setup». Затем нажать кнопку «Browse ...», как показано ниже на рисунке 4.48, чтобы найти и выбрать новый файл прошивки. Затем нажать кнопку «Upload», чтобы начать процесс обновления прошивки. Программа покажет статус загрузки. Необходимо дождаться окончания процесса загрузки (длительность процесса зависит от используемого оборудования). Наконец, будет выполнена перезагрузка устройства NetXpert NXI-3011, v2. В некоторых случаях может потребоваться перенастройка устройства NetXpert NXI-3011, v2. Процедура восстановления резервной конфигурации из файла описана в следующей главе.



Рис. 4.48. WEB-страница обновления прошивки в меню настройки системы.

4.12.4. Настройки резервного копирования/восстановления

Как только все настройки выполнены, и устройство работает должным образом, пользователю необходимо выполнить резервное копирование текущей конфигурации NetXpert NXI-3011, v2. Файл конфигурации резервной копии можно использовать, когда при загрузке нового встроенного программного обеспечения для устройства были установлены заводские настройки по умолчанию. Это сделано для предотвращения случайной загрузки несовместимых старых настроек. Файл конфигурации резервной копии также можно использовать для эффективного развертывания нескольких устройств серии NetXpert NXI-3011, v2 с одинаковыми настройками путем загрузки этих настроек на все устройства.

Для резервного копирования конфигурации необходимо нажать на кнопку "Backup" в разделе Backup Configuration, как показано на рисунке 4.49, после чего файл резервной копии (ModelName-MACAddress.dat) будет автоматически сохранен на ПК. Важно НЕ изменять вручную сохраненный файл конфигурации каким-либо редактором. Любая модификация файла может повредить файл и его нельзя будет использовать для последующего восстановления.

Чтобы восстановить конфигурацию из резервной копии, необходимо нажать кнопку «Browse» в разделе «Restore Configuration», как показано на рисунке 4.49, чтобы найти файл конфигурации резервной копии на компьютере пользователя. Затем необходимо нажать кнопку «Upload», чтобы загрузить файл конфигурации из резервной копии на устройство. Как только файл конфигурации резервной копии будет успешно загружен, устройство выполнит перезагрузку. Следует отметить, что время, необходимое для этого процесса, может варьироваться в зависимости от используемого оборудования.

Если необходимо восстановить заводскую конфигурацию по умолчанию на NetXpert NXI-3011, v2, можно нажать на кнопку Restore в разделе Restore Factory Default, как показано на рисунке 4.49.

System Setup > Backup/Restore Settings

Backup & Restore Configuration
To upgrade the firmware, browse to the location of the new firmware binary file (.dld) and click **Upload** button. In some cases, the device reconfiguration is required.

Backup Configuration

Click **Backup** to save the current configuration to your computer.

Backup

Restore Configuration

Browse a backup configuration file and click Upload button to restore the device's configuration.

Browse...

Upload

Restore Factory Default

Click **Restore** to restore factory default configuration.

Restore

Рис. 4.49. WEB-страница настройки резервного копирования/восстановления в настройках системы.

4.12.5. Ping

WEB-интерфейс NetXpert NXI-3011, v2 имеет интерфейс для отправки команды Ping, которая является утилитой сетевой диагностики для проверки доступности. Можно использовать функцию Ping, чтобы определить, может ли NetXpert NXI-3011, v2 получить доступ к шлюзу или другим устройствам в сети. Чтобы использовать функцию Ping, необходимо ввести IP-адрес назначения в текстовом поле после Ping To и нажать кнопку «Start», как показано на рисунке 4.50. Этот процесс обычно занимает около 20 секунд. На рисунке 4.50 представлен успешный пинг без потери пакетов от NetXpert NXI-3011, v2 на адрес 10.0.50.101 и обратно, тогда как на рисунке 4.51 показано, что подключающееся устройство по адресу 10.0.50.202 недоступно, так как ни один из переданных пакетов пинг не возвращен.

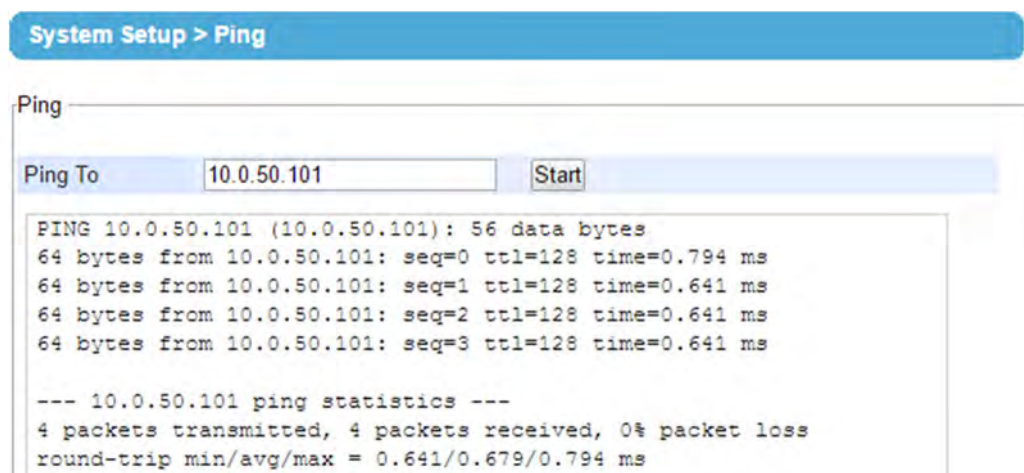


Рис. 4.50. WEB-страница Ping в меню настройки системы.

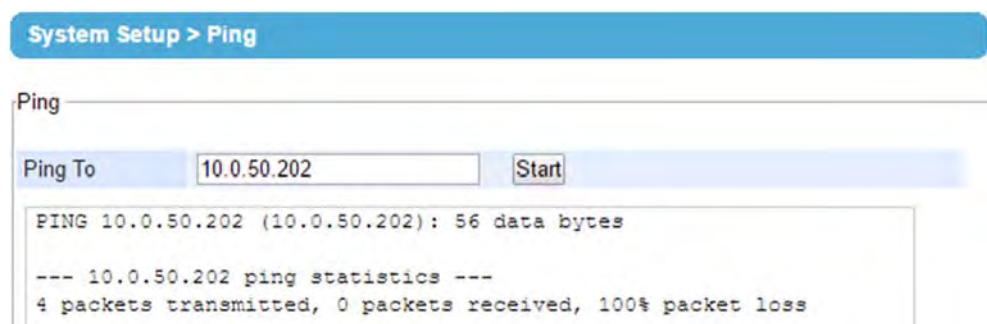


Рис. 4.51. Пример недоставленного ping.

4.13. Перезагрузка

Чтобы вручную перезагрузить устройство NetXpert NXI-3011, v2, следует нажать кнопку «Reboot» в конце страницы «Reboot», как показано на рисунке 4.52. Устройство выполнит перезагрузку. После завершения процесса перезагрузки вы дважды услышите звуковой сигнал с устройства, и может потребоваться обновить WEB-браузер, чтобы снова войти в WEB-интерфейс NetXpert NXI-3011, v2.

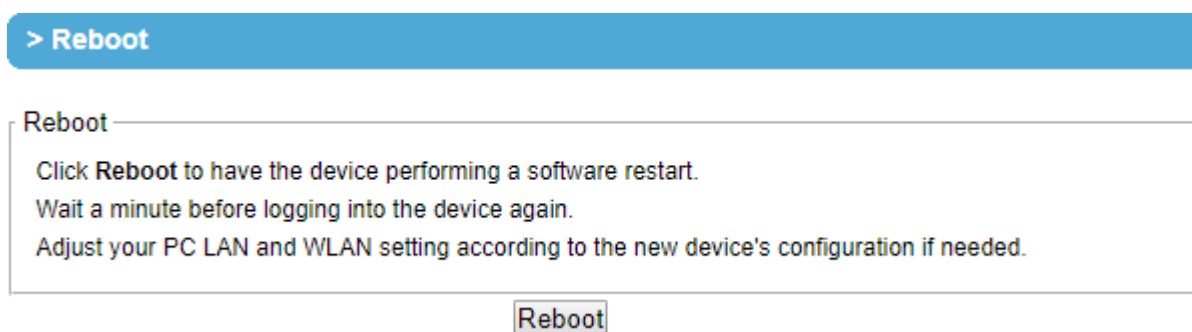


Рис. 4.52. WEB-страница перезагрузки.

5. КАНАЛЬНЫЕ РЕЖИМЫ И ПРИЛОЖЕНИЯ

5.1. Конфигурация канального режима

Серия NetXpert NXI-3011, v2 поддерживает три различных режима соединения: TCP-сервер, TCP-клиент и UDP. Канальный режим описывает роль NetXpert NXI-3011, v2 и соединение между устройством NetXpert NXI-3011, v2 и другими удаленными устройствами в сети, которые хотели бы обмениваться данными с последовательными устройствами через COM-порт(ы) NetXpert NXI-3011, v2.

В трех режимах соединения TCP-сервер может поддерживать приложения RAW, Virtual COM, Reverse Telnet и Pair Connection Master, а в режиме TCP-клиента может поддерживать только приложения RAW, Virtual COM и Pair Connection Slave. Следует отметить, что режим UDP не имеет тех же поддерживаемых приложений, что и предыдущие два режима TCP.

Информация о том, как правильно настроить различные канальные режимы, будет представлена в следующих главах. На рисунке 5.1 показаны параметры режима связи Link Mode для порта COM 1, которые можно найти на странице WEB-интерфейса COM1 в меню «Serial» (подробности о настройках последовательного интерфейса см. в пп. 4.6).

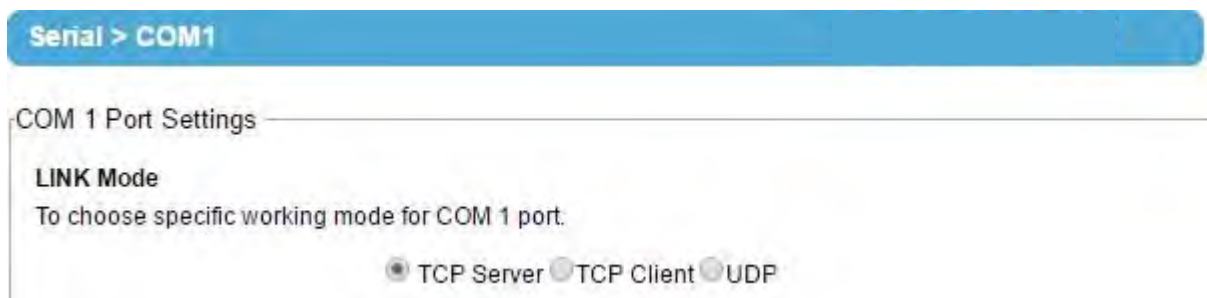


Рис. 5.1. Опции канального режима для порта COM 1.

5.1.1. Канальный режим: Конфигурирование NetXpert NXI-3011, v2 в качестве TCP-сервера

Серия NetXpert NXI-3011, v2 может быть настроена как сервер протокола управления передачей данных (TCP) в сети TCP/IP для прослушивания входящего соединения TCP-клиента с последовательным устройством.

На рисунке 5.2 изображен пример устройства PLC (последовательного), которое подключено к NetXpert NXI-3011, v2 по последовательной шине, где удаленный хост-компьютер отправляет запрос через сеть Ethernet. После установления соединения между сервером последовательных устройств (NetXpert NXI-3011, v2) и удаленным хост-компьютером (удаленный TCP-клиент) как на рисунке 5.2, данные могут передаваться в обоих направлениях. Эта схема также применяется всякий раз, когда приложение Virtual COM (VCOM) работает в режиме сервера. Следует обратить внимание, что это режим связи по умолчанию для устройства NetXpert NXI-3011, v2.

TCP Server Mode



Рис. 5.2. Канальный режим NetXpert NXI-3011, v2 настроен как TCP-сервер.

Режим соединения по умолчанию для NetXpert NXI-3011, v2 - это режим TCP-сервера. На рисунке 5.3 показан пример настройки конфигурации для канального режима TCP-сервера на странице COM 1. Имеются также дополнительные параметры соединения, которые можно настроить, как показано на рисунке 5.3. Необходимо выполнить следующие шаги, чтобы настроить параметры подключения канального режима для каждого COM-порта.

LINK Mode

To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	RAW
IP Filter	☐ Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1
Response Behavior	☐ Request & Response Mode ☐ Reply to requester only ☒ Reply to all ☒ Transparent Mode

Рис. 5.3. Настройки соединения Канального режима TCP-сервера.

- Необходимо нажать на ссылку COM 1 в окне меню в левой части пользовательского WEB-интерфейса для перехода к странице COM 1, как показано на рисунке 5.4. Следует отметить, что если необходимо сконфигурировать COM 2 (или любой другой COM-порт), необходимо выполнить ту же процедуру.

Serial > COM1

COM 1 Port Settings

Link Mode
To choose specific working mode for COM 1 port.

☒ TCP Server
 ☐ TCP Client
 ☐ UDP

TCP Server

Application	RAW ▼
IP Filter	☐ Enable
Source IP	0.0.0.0
Local Port	4660
Maximum Connection	1 ▼
Response Behavior	☐ Request & Response Mode ☒ Reply to request only ☐ Reply to all ☒ Transparent Mode

To configure COM 1 port parameters.

Serial Settings

Serial Interface	☐ RS232 ☒ RS422 ☐ RS485 ☐ RS485(4-Wire)
Baud Rate	19200 ▼ bps
Parity	☒ None ☐ Odd ☐ Even ☐ Mark ☐ Space
Data bits	☐ 5 bits ☐ 6 bits ☐ 7 bits ☒ 8 bits
Stop bits	☒ 1 bits ☐ 2 bits
Flow Control	☒ None ☐ Xon/Xoff ☐ RTS/CTS

Рис. 5.4. Настройки канального режима TCP-сервера на странице COM 1.

- Необходимо установить переключатель TCP Server в опциях Канального режима.
- В разделе TCP Server расположены следующие опции:

Application: здесь можно выбрать одно из четырех приложений связи:

RAW: в этом режиме нет протокола, что означает, что данные передаются прозрачно.

Virtual COM: протокол Virtual COM включен на последовательном устройстве для связи с виртуальным портом с удаленного клиента. В Windows/Linux можно создать виртуальный COM-порт для связи с последовательным устройством в качестве удаленного клиента.

Reverse Telnet: это приложение используется для соединения последовательного устройства с другим последовательным устройством (обычно это терминальный сервер) с программой Telnet. Программы Telnet в Windows/Linux обычно требуют специального

подтверждения связи, чтобы выходные данные и форматирование отображались правильно. Серия NetXpert NXI-3011, v2 будет взаимодействовать с этими специальными командами (командами CR/LF) после включения приложения Reverse Telnet.

Pair Connection Master: это приложение используется, когда пользователь хочет подключить два последовательных устройства через сеть Ethernet.

IP Filter: Данная опция активирует опцию Source IP ниже. Если эта опция включена, NetXpert NXI-3011, v2 будет блокировать или отфильтровывать все другие IP-адреса при доступе к COM-порту, кроме указанного в качестве адреса Source IP.

- Source IP: Эта опция указывает IP-адрес удаленного клиента Source IP, который будет передавать данные на TCP-сервер (в NetXpert NXI-3011, v2). Другими словами, TCP-сервер будет пропускать только данные с этого IP-адреса (следовательно, его собственное имя подразумевает Source IP). Следует отметить, что разрешен только один адрес источника.
- Local Port: В этом параметре указывается номер порта, который должен прослушиваться TCP-сервером (на NetXpert NXI-3011, v2). Он также используется удаленным TCP-клиентом для подключения к TCP-серверу. Локальный порт по умолчанию равен 4660. В этой опции можно ввести другой номер порта.
- Maximum Connection: эта опция указывает максимальное количество удаленных устройств/клиентов (максимум 4 клиента), которые могут быть подключены к последовательному устройству через этот COM-порт.
- Response Behavior: эта опция указывает, как NetXpert NXI-3011, v2 будет работать или вести себя при получении запросов от удаленных подключенных хостов, здесь имеются следующие параметры:

Request & Response Mode: В этом режиме COM-порт на NetXpert NXI-3011, v2 будет удерживать запросы от всех других удаленных подключенных хостов до тех пор, пока последовательное устройство не ответит или до окончания интервала Response Interval Timeout для его отмены. Однако незапрошенные данные (при спорадической передаче), отправленные с последовательного устройства, будут перенаправлены всем подключенным хостам. Кроме того, пользователь может указать, как ответное сообщение от последовательного устройства будет отправляться на удаленные подключенные хосты, для этого можно выбрать один из двух вариантов:

Reply to requester only: COM-порт ответит только удаленному подключенному хосту, который запросил данные.

Reply to all: ответ будет отправлен всем удаленным подключенным хостам.

Transparent mode: COM-порт на NetXpert NXI-3011, v2 будет перенаправлять запросы от всех удаленных подключенных хостов на последовательное устройство незамедлительно и отвечать всем удаленным подключенным хостам, как только получит данные от последовательного устройства.

Другие настройки Serial Settings на той же странице конфигурации описаны в пп. 4.6.2, а расширенные настройки Advanced Settings описаны в пп. 4.6.3.

После окончания конфигурирования Канального режима необходимо перейти вниз страницы и нажать на кнопку Save & Apply для сохранения всех выполненных изменений.

Примечание: LINK1 ассоциирован с COM 1; LINK 2 ассоциирован с COM 2, и т.д.

5.1.2. Канальный режим: Конфигурирование NetXpert NXI-3011, v2 в качестве TCP-клиента

Серия NetXpert NXI-3011, v2 может быть сконфигурирована как TCP-клиент в сети TCP/IP для установления соединения с TCP-сервером на удаленном хост-компьютере. На рисунке 5.5 показан пример двух последовательных устройств ввода, подключенных к двум разным устройствам NetXpert NXI-3011, v2, где оба устройства NetXpert NXI-3011, v2 находятся в одной и той же сети Ethernet, что и удаленный хост-компьютер. Стрелка на рисунке 5.5 указывает на запрос соединения со стороны клиента TCP-соединения. После установления соединения данные могут передаваться между последовательным устройством (подключенным к COM-порту каждого из устройств NetXpert NXI-3011, v2) и удаленным хост-компьютером в обоих направлениях. Это также относится к приложению Virtual COM, работающему в режиме клиента.



Рис. 5.5. Пример NetXpert NXI-3011, v2 сконфигурированного в канальном режиме TCP-клиента.

На рисунке 5.6 показан пример конфигурации для канального режима TCP Client на странице COM 1. Дополнительные настройки соединения могут быть заданы, как показано на рисунке 5.7. При выборе режима TCP Client, программа TCP-сервера на удаленном хост-компьютере должна быть готова принять запрос на соединение от NetXpert NXI-3011, v2. Необходимо выполнить следующие шаги для конфигурации настроек соединения канального режима для каждого COM-порта.

☐ TCP Server ☒ TCP Client ☐ UDP

<i>TCP Client</i>	
Application	RAW
Destination IP 1	10 . 0 . 50 . 1
Destination Port 1	4660
Destination 2	☐ Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	☐ Request & Response Mode ☐ Reply to requester only ☒ Reply to all ☒ Transparent Mode

Рис. 5.6. Настройки соединения для канального режима TCP Client.

- Необходимо нажать на ссылку COM 1 в окне меню в левой части пользовательского WEB-интерфейса для перехода к COM 1 как показано на рисунке 5.7. Следует отметить, что если необходимо сконфигурировать COM 2 (или любой другой COM-порт), необходимо выполнить ту же процедуру.

Serial > COM1

COM 1 Port Settings

Link Mode
To choose specific working mode for COM 1 port.

☐ TCP Server
 ☒ TCP Client
 ☐ UDP

TCP Client

Application	RAW ▼
Destination IP 1	10.0.50.200
Destination Port 1	518
Destination 2	☒ Enable
Destination IP 2	10.0.50.300
Destination Port 2	768
Response Behavior	☐ Request & Response Mode ☐ Reply to request only ☐ Reply to all ☒ Transparent Mode

To configure COM 1 port parameters.

Serial Settings

Serial Interface	☒ RS232 ☐ RS422 ☐ RS485 ☐ RS485(4-Wire)
Baud Rate	19200 ▼ bps
Parity	☒ None ☐ Odd ☐ Even ☐ Mark ☐ Space
Data bits	☐ 5 bits ☐ 6 bits ☐ 7 bits ☒ 8 bits
Stop bits	☒ 1 bits ☐ 2 bits
Flow Control	☒ None ☐ Xon/Xoff ☐ RTS/CTS

Рис. 5.7. Настройка в канальном режиме TCP Client.

- Необходимо выбрать переключатель TCP Client в опциях Link Mode.
- В разделе TCP Client расположены следующие опции:

Application: Здесь доступны только три приложения связи: RAW, Virtual COM and Pair Connection Slave, для которых действуют те же определения, как описано ранее в пп. 5.1.1.

Destination IP 1: Необходимо указать адрес назначения Destination IP-программы TCP-сервера на удаленном хосте в этом поле. Он должен соответствовать настройкам IP-адреса программы TCP-сервера.

Destination Port 1: Необходимо указать предпочтительный номер порта программы TCP-сервера на удаленном хосте в этом поле. И вновь, он должен соответствовать настройкам IP-адреса программы TCP-сервера.

Destination 2: При необходимости можно включить второй удаленный адрес назначения для TCP-соединения, установив флажок Enable в этой опции. Можно задать два разных TCP-сервера для резервирования.

Destination IP 2: Необходимо указать предпочтительный адрес назначения Destination IP второй программы TCP-сервера на удаленном хосте в этом поле.

Он должен соответствовать настройкам IP-адреса второй программы TCP-сервера.

Destination Port 2: Необходимо указать предпочтительный номер порта второй программы TCP-сервера на удаленном хосте в этом поле. И вновь, он должен соответствовать настройкам IP-адреса второй программы TCP-сервера.

Response Behavior: этот параметр указывает, как NetXpert NXI-3011, v2 будет работать или действовать при получении запроса от удаленных подключенных хостов. Описание каждой опции аналогично описанному в пп. 5.1.1).

- Другие настройки Serial Settings на той же странице конфигурации описаны в пп. 4.6.2, а расширенные настройки Advanced Settings описаны в пп. 4.6.3.
- После окончания конфигурирования Канального режима необходимо перейти вниз страницы и нажать на кнопку Save & Apply для сохранения всех выполненных изменений.

5.1.3. Канальный режим NetXpert NXI-3011, v2 в UDP

Поскольку протокол пользовательских датаграмм (UDP) является транспортным протоколом без установления соединения, он не гарантирует доставку сетевых датаграмм до конечного получателя. NetXpert NXI-3011, v2 также поддерживает протокол UDP без установления соединения наравне с протоколом TCP с установлением соединения. Серия NetXpert NXI-3011, v2 может быть настроена для передачи данных с помощью одноадресной или многоадресной рассылки UDP от последовательного устройства на один или несколько хост-компьютеров. Данные могут передаваться между последовательным устройством и удаленным хост-компьютером в обоих направлениях.

В этом протоколе нет концепции сервера или клиента. Все сетевые устройства называются узлами или пирами. Поэтому достаточно только указать локальный порт, который NetXpert NXI-3011, v2 должен прослушивать, и указать IP-адреса назначения удаленных узлов UDP. На рисунке 5.8 показан пример канального режима UDP, в котором последовательное устройство отображения информации подключено к последовательной шине NetXpert NXI-3011, v2. Два удаленных хост-компьютера, которые находятся в той же сети Ethernet, что и NetXpert NXI-3011, v2, могут отправлять датаграммы UDP или сообщения на последовательное устройство отображения информации через NetXpert NXI-3011, v2.

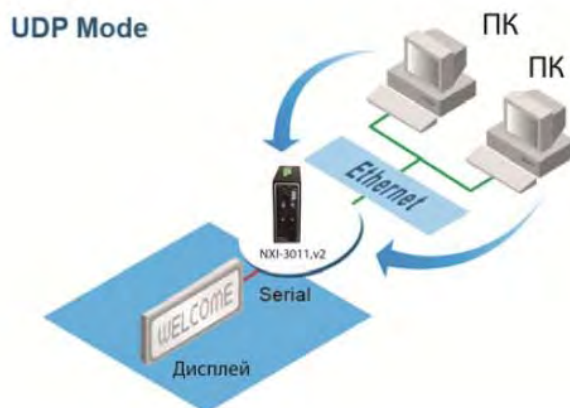


Рис. 5.8. Пример конфигурации NetXpert NXI-3011, v2 в канальном режиме UDP.

На рисунке 5.9 показан пример настроек конфигурации для режима UDP Link Mode на странице COM 1. Дополнительные настройки соединения могут быть заданы, как показано на рисунке 5.10. Следует отметить, что хотя UDP обеспечивает лучшую эффективность с точки зрения времени отклика и использования ресурсов, он не гарантирует доставку данных. Рекомендуется использовать UDP только с циклическими протоколами опроса, где каждый запрос повторяется и является независимым, например протокол Modbus. Необходимо выполнить следующие шаги для конфигурации настроек соединения канального режима для каждого COM-порта.

LINK Mode

To choose specific working mode for COM 1 port.

☐ TCP Server ☐ TCP Client ☒ UDP

UDP					
Local Port: 4660					
☒ Destination IP Address 1	10	0	50	1 ~ 100	Port: 4660
☐ Destination IP Address 2	0	0	0	0 ~ 0	Port: 4660
☐ Destination IP Address 3	0	0	0	0 ~ 0	Port: 4660
☐ Destination IP Address 4	0	0	0	0 ~ 0	Port: 4660

Рис. 5.9. Настройки соединения в канальном режиме UDP.

- Необходимо нажать на ссылку COM 1 в окне меню в левой части пользовательского WEB-интерфейса для перехода к COM 1 page как показано на рисунке 5.10. Следует отметить, что если необходимо сконфигурировать COM 2 (или любой другой COM-порт), необходимо выполнить ту же процедуру.

Serial > COM1
M

COM 1 Port Settings

Link Mode
To choose specific working mode for COM 1 port.

☐ TCP Server
 ☐ TCP Client
 ☒ UDP

UDP

Local Port:

☒ Destination IP Address 0	10 0 50 101 ~ 102	Port: 511
☒ Destination IP Address 1	10 0 100 100 ~ 150	Port: 252
☒ Destination IP Address 2	10 0 201 200 ~ 250	Port: 65535
☒ Destination IP Address 3	10 0 55 100 ~ 100	Port: 65535

To configure COM 1 port parameters.

Serial Settings

Serial Interface	☒ RS232 ☐ RS422 ☐ RS485 ☐ RS485(4-Wire)
Baud Rate	19200 bps
Parity	☒ None ☐ Odd ☐ Even ☐ Mark ☐ Space
Data bits	☐ 5 bits ☐ 6 bits ☐ 7 bits ☒ 8 bits
Stop bits	☒ 1 bits ☐ 2 bits
Flow Control	☒ None ☐ Xon/Xoff ☐ RTS/CTS

Рис. 5.10. Настройка канального режима UDP на странице COM 1.

- Необходимо выбрать переключатель UDP в опции Link Mode.
- В разделе UDP расположены следующие опции:

Local Port: В этом поле указывается номер локального порта для канального режима UDP в NetXpert NXI-3011, v2, который он будет прослушивать, это может быть любое число от 1 до 65535. Следует отметить, что обычно рекомендуется выбирать номер порта больше 1024, чтобы избежать конфликта с хорошо известными номерами портов. Следует сопоставить этот параметр с удаленной программой UDP. Следует отметить, что этот номер обычно называется портом назначения в удаленной программе UDP.

Destination IP Address от 1 до 4 и его Port Numbers: в каждой строке этих опций можно указать диапазон IP-адресов и номер порта, которые будут обмениваться данными с NetXpert NXI-3011, v2. Пользователь здесь может определить начальный (Begin) и конечный (End) IP-адреса. Разрешены четыре группы диапазонов IP-адресов. Необходимо поставить флажок напротив этой строки, чтобы включить его. Это IP-адреса удаленных программ UDP и порт, который они прослушивают. Следует отметить, что максимальное количество узлов UDP, которое может обрабатывать NetXpert NXI-3011, v2, будет в значительной степени зависеть от нагрузки трафика. Было выяснено, что NetXpert NXI-3011, v2 может обрабатывать до 200 узлов UDP (со скоростью передачи 9600 бит/сек, интервалом запроса 100 мс и длиной данных 30 байт).

- Другие настройки Serial Settings на той же странице конфигурации описаны в пп. 4.6.2, а расширенные настройки Advanced Settings описаны в пп. 4.6.3.
- После окончания конфигурирования Link Mode, необходимо перейти вниз страницы и нажать на кнопку "Save & Apply" для сохранения всех выполненных изменений.

5.2. Приложения канального режима

В этом разделе описываются параметры приложения для канальных режимов TCP-сервера, TCP-клиента и UDP. Опции приложения будут определять, как будет осуществляться последовательная передача данных по сетевому каналу связи. Пользователь будет иметь гибкие возможности в выборе подходящего приложения, которое соответствует его потребности в последовательной передаче данных.

5.2.1. Приложение TCP-сервера: Включение виртуального COM

NetXpert NXI-3011, v2 будет инкапсулировать контрольные пакеты поверх реальных данных, когда функция Virtual COM включена. Это позволит виртуальному COM-порту в операционной системе Windows/Linux получить доступ к COM-портам NetXpert NXI-3011, v2. Преимущество использования Virtual COM заключается в том, что не требуется перезапись существующей программы COM для чтения IP-пакетов. Другими словами, можно использовать обычную или устаревшую последовательную (COM) программу. Преобразование/виртуализация IP в COM прозрачно выполняется в системном драйвере. На рисунке 5.11 показан NetXpert NXI-3011, v2 в режиме TCP-сервера с включенным приложением Virtual COM. Необходимо выполнить следующие шаги, чтобы включить приложение Virtual COM в режиме TCP Server Link Mode.

LINK Mode

To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Virtual COM
IP Filter	☐ Enable
Source IP	0 . 0 . 0 . 0
Local Port	4860
Maximum Connection	1
Response Behavior	☐ Request & Response Mode ☐ Reply to requester only ☐ Reply to all ☒ Transparent Mode

Рис. 5.11. Приложение Virtual COM в режиме TCP-сервера.

- Необходимо выполнить шаги из пп. 5.1.1 для правильной конфигурации устройства NetXpert NXI-3011, v2 в режиме TCP Server.
- Необходимо нажать на выпадающий список в опции Application в разделе TCP Server и переключиться на "Virtual COM" для включения приложения Virtual COM в NetXpert NXI-3011, v2.
- Необходимо перейти вниз страницы и нажать на кнопку "Save & Apply" для сохранения всех выполненных изменений.
- Необходимо настроить Virtual COM в операционной системе на удаленном хост-компьютере. Для Windows, следует обратиться к главе 6 для получения необходимых инструкций. Необходимо запомнить IP-адрес и номер локального порта устройства NetXpert NXI-3011, v2, настроенные на этой странице, чтобы позже ввести эту же информацию на панели управления Serial/IP Virtual COM. Следует отметить, что программное обеспечение Serial/IP Virtual COM Redirector предоставляется в качестве служебного программного обеспечения.

5.2.2. Приложение TCP-сервера: Включение RFC 2217 через Virtual COM

Базовый протокол Virtual COM основан на стандарте RFC 2217, который является опцией управления Telnet COM, следовательно, можно использовать RFC 2217 для

NetXpert NXI-3011, v2 в режиме TCP-сервера. Следует отметить, что RFC 2217 позволяет удаленному клиенту, которым может быть любое сетевое устройство, инициировать сеанс Telnet с сервером доступа (т.е. NetXpert NXI-3011, v2) для связи с последовательным устройством через COM-порт сервера доступа. Следует обратиться к пп. 5.2.1 (предыдущий раздел), чтобы включить Virtual COM, чтобы NetXpert NXI-3011, v2 получил информацию об именах команд и кодах, определенных в RFC 2217. Следует обратить внимание, что нет необходимости настраивать Virtual COM в операционной системе удаленного хост-компьютера, поскольку виртуальные COM-порты не будут использоваться.

5.2.3. Приложение TCP-клиента: Включение Virtual COM

Также возможно включить Virtual COM в канальном режиме TCP-клиента. показывает конфигурацию приложения Virtual COM в канальном режиме TCP-клиента. Virtual COM в канальном режиме TCP-клиента обычно проще использовать, если NetXpert NXI-3011, v2 использует динамический IP-адрес (через DHCP), поскольку установка статического IP-адреса на панели управления Virtual COM в операционной системе невозможна. Необходимо выполнить следующие шаги для включения приложения Virtual COM в канальном режиме TCP Client.

LINK Mode
To choose specific working mode for COM 1 port.

☐ TCP Server ☒ TCP Client ☐ UDP

TCP Client	
Application	Virtual COM
Destination IP 1	10 . 0 . 50 . 1
Destination Port 1	4660
Destination 2	☐ Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	☐ Request & Response Mode ☐ Reply to requester only ☐ Reply to all ☒ Transparent Mode

Рис. 5.12. Приложение Virtual COM в режиме TCP Client.

- Необходимо выполнить шаги из пп 5.1.2 для правильной конфигурации NetXpert NXI-3011, v2 в канальном режиме TCP Client.
- Необходимо нажать на выпадающий список в опции Application в разделе TCP Client и переключиться на "Virtual COM" для включения приложения Virtual COM в NetXpert NXI-3011, v2.
- Необходимо перейти вниз страницы и нажать на кнопку "Save & Apply" для сохранения всех выполненных изменений.
- Необходимо настроить Virtual COM в операционной системе на удаленном хост-компьютере. Для Windows следует обратиться к главе 6 для получения необходимых инструкций. Необходимо запомнить номер порта назначения Destination Port, настроенный на этой странице, чтобы позже ввести эту информацию в панель управления Serial/IP Virtual COM.

5.2.4. Приложение TCP-клиента: Включение RFC 2217 через Virtual COM

Базовый протокол Virtual COM основан на стандарте RFC 2217, который является опцией управления Telnet COM, следовательно, можно использовать RFC 2217 для

NetXpert NXI-3011, v2 в режиме TCP-клиента. Следует отметить, что RFC 2217 позволяет клиенту, которым является в данном случае устройство NetXpert NXI-3011, v2, инициировать сеанс Telnet с удаленным хост-компьютером доступа для связи с последовательным устройством или последовательной (COM) программой на удаленном хост-компьютере. Следует обратиться к пп 5.2.3 (предыдущий раздел), чтобы включить Virtual COM, чтобы NetXpert NXI-3011, v2 получил информацию об именах команд и кодах, определенных в RFC 2217. Следует обратить внимание, что нет необходимости настраивать Virtual COM в операционной системе удаленного хост-компьютера, поскольку виртуальные COM-порты не будут использоваться.

5.2.5. Приложение TCP -сервера: Конфигурирование NetXpert NXI-3011, v2 в качестве Pair Connection Master

Приложение Pair Connection используется при подключении двух последовательных устройств через Ethernet или когда невозможно установить Virtual COM на последовательные устройства. Однако приложению Pair Connection для работы в паре требуются два NetXpert NXI-3011, v2. Один из них станет мастером такого соединения, а другой - подчиненным. На рисунке 5.13 показана конфигурация приложения Pair Connection Master в канальном режиме TCP-сервера. Необходимо выполнить следующие шаги для включения приложения Pair Connection и настройки NetXpert NXI-3011, v2 в качестве мастера в канальном режиме TCP-сервера.

Link Mode
To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Pair Connection Master ▼
IP Filter	☐ Enable
Source IP	0.0.0.0
Local Port	4660
Maximum Connection	1 ▼
Response Behavior	☐ Request & Response Mode ☒ Reply to request only ☐ Reply to all ☒ Transparent Mode

Рис. 5.13. Приложение Pair Connection Master Application в режиме TCP-сервера.

- Необходимо выполнить шаги из пп. 5.1.1 для настройки NetXpert NXI-3011, v2 в качестве TCP-сервера для правильной конфигурации в канальном режиме.
- Необходимо нажать на выпадающий список в опции Application в разделе TCP Server и переключиться на "Pair Connection Master" для включения приложения Pair Connection в NetXpert NXI-3011, v2.
- Необходимо перейти вниз страницы и нажать на кнопку "Save & Apply" для сохранения всех выполненных изменений.
- Необходимо запомнить здесь IP-адрес мастера Pair Connection (т.е. IP-адрес NetXpert NXI-3011, v2 на желаемом сетевом интерфейсе (Ethernet или Wi-Fi)) и номер локального порта, чтобы позже ввести данную информацию на другом устройстве NetXpert NXI-3011, v2 с настройками ведомого Pair Connection.
- Необходимо перейти к следующему разделу, чтобы настроить подчиненное устройство для подключения к этому мастер-устройству.

5.2.6. Приложение TCP-клиент: Конфигурирование NetXpert NXI-3011, v2 в качестве Pair Connection Slave

Приложение Pair Connection Slave настраивается для NetXpert NXI-3011, v2 в режиме TCP-клиента, как показано на рисунке 5.14. Необходимо выполнить сопряжение с мастер-устройством Pair Connection, как описано в предыдущем разделе. Прежде чем продолжить, необходимо установить Master Pair Connection на другом устройстве NetXpert NXI-3011, v2. Необходимо выполнить следующие шаги, чтобы включить приложение Pair Connection и установить это устройство NetXpert NXI-3011, v2 в качестве ведомого в канальном режиме TCP-клиенте.

COM 1 Port Settings

Link Mode
To choose specific working mode for COM 1 port.

☐ TCP Server
 ☒ TCP Client
 ☐ UDP

TCP Client	
Application	Pair Connection Slave ▼
Destination IP 1	10.0.100.50
Destination Port 1	518
Destination 2	☒ Enable
Destination IP 2	10.0.100.60
Destination Port 2	768
Response Behavior	☐ Request & Response Mode ☒ Reply to request only ☐ Reply to all ☒ Transparent Mode

Рис. 5.14. Приложение Pair Connection Slave в режиме TCP-клиента.

- Необходимо выполнить шаги из пп. 5.1.2 для правильной конфигурации NetXpert NXI-3011, v2 в канальном режиме в режиме TCP-клиента.
- Необходимо нажать на выпадающий список в опции Application в разделе TCP Client и переключиться на "Pair Connection Slave" для включения приложения Pair Connection на устройстве NetXpert NXI-3011, v2.
- Необходимо ввести адрес назначения Destination IP и номер порта назначения Destination Port (для Destination 1 и (опционально Destination 2)), которые соответствуют настройкам IP-адреса и номера порта мастер-устройства Pair Connection (другого устройства NetXpert NXI-3011, v2), которые были настроены ранее.
- Необходимо перейти вниз страницы и нажать на кнопку "Save & Apply" для сохранения всех выполненных изменений.

5.3. Приложение TCP-сервера: Включение Reverse Telnet

Приложение Reverse Telnet используется, если программа Telnet используется для подключения к NetXpert NXI-3011, v2, а последовательный интерфейс NetXpert NXI-3011, v2 подключен к серверу терминалов.

Программы Telnet в операционных системах Windows/Linux требуют специального подтверждения связи для корректного отображения выходных данных и форматирования символов. NetXpert NXI-3011, v2 будет взаимодействовать с помощью специальных команд (таких как команды CR/LF), если включен Reverse Telnet. На рисунке 5.15 показана конфигурация приложения Reverse Telnet в канальном режиме TCP-сервера. Следует отметить, что приложение Reverse Telnet доступно только в том случае, если NetXpert NXI-3011, v2 настроен в канальном режиме TCP-сервера. Необходимо выполнить следующие шаги для включения приложения Reverse Telnet в канальном режиме TCP-сервера.

LINK Mode

To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Reverse Telnet
IP Filter	☐ Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1
Response Behavior	☐ Request & Response Mode ☐ Reply to requester only ☒ Reply to all ☒ Transparent Mode

Рис. 5.15. Приложение Reverse Telnet в канальном режиме TCP-сервера.

- Необходимо выполнить шаги из пп. 5.1.1 для правильной конфигурации NetXpert NXI-3011, v2 в канальном режиме TCP Server.
- Необходимо нажать на выпадающий список в опции Application в разделе TCP Server и переключиться на "Reverse Telnet" для включения приложения reverse telnet на устройстве NetXpert NXI-3011, v2.
- Необходимо перейти вниз страницы и нажать на кнопку "Save & Apply" для сохранения всех выполненных изменений.

6. УСТАНОВКА И УСТРАНЕНИЕ НЕПОЛАДОК VCOM

6.1. Включение VCOM

NetXpert NXI-3011, v2 будет инкапсулировать контрольные пакеты поверх фактических последовательных данных, когда включено приложение Virtual COM (VCOM). Это позволит виртуальному COM-порту в системе Windows/Linux получать доступ к COM-портам устройства NetXpert NXI-3011, v2. Следует обратить внимание, что приложение Virtual COM Application можно включить только на TCP-сервере, как показано на рисунке 6.1 или на TCP-клиенте как показано на рисунке 6.2.

COM 1 Port Settings

LINK Mode
To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Virtual COM
IP Filter	☐ Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1
Response Behavior	☐ Request & Response Mode ☐ Reply to requester only ☐ Reply to all ☒ Transparent Mode

Рис. 6.1. Включение приложения Virtual COM при настройке канального режима TCP-сервера.

COM 1 Port Settings

LINK Mode
To choose specific working mode for COM 1 port.

☐ TCP Server ☒ TCP Client ☐ UDP

TCP Client	
Application	Virtual COM
Destination IP 1	0 . 0 . 0 . 0
Destination Port 1	4660
Destination 2	☐ Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	☐ Request & Response Mode ☐ Reply to requester only ☐ Reply to all ☒ Transparent Mode

Рис. 6.2. Включение приложения Virtual COM при настройке канального режима TCP-клиента.

Virtual COM на хост-компьютере обеспечивает удаленный доступ к последовательным устройствам по сети TCP/IP через последовательные/IP COM-порты, которые работают как локальные собственные COM-порты. На рисунке 6.3 приведен пример диаграммы приложения Virtual COM.

На схеме изображено несколько последовательных серверов (то есть устройств NetXpert NXI-3011, v2), подключенных через Ethernet концентратор, каждый из которых подключается к последовательному устройству. Доступ к их последовательным устройствам возможен через TCP/IP сеть концентратора. Следует отметить, что на персональном компьютере (ПК) традиционно есть не более двух физических COM-портов (COM 1 и COM 2), в то же время может быть несколько виртуальных COM-портов, таких как COM 3, 4, 5 и т. д.

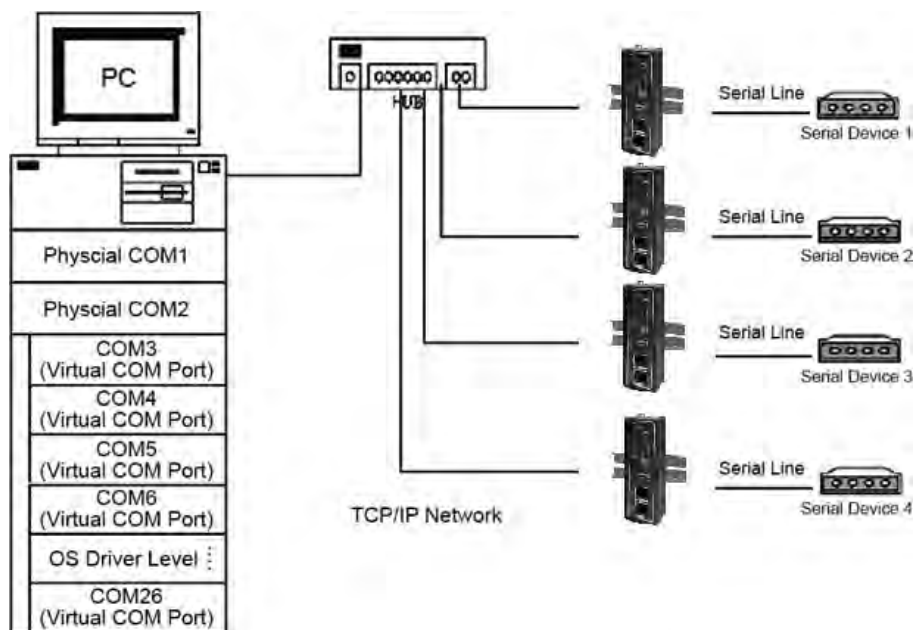


Рис. 6.3. Пример диаграммы приложения Virtual COM по сети TCP/IP.

Для включения Virtual COM на хост-компьютере потребуется программная утилита или программный драйвер VCOM для эмуляции COM-порта. Для операционной системы Windows поддерживается программная утилита под названием Serial/IP, которую можно использовать для этих целей. Описание утилиты драйвера VCOM находится в следующих главах.

6.1.1. Установка драйвера VCOM

К поддерживаемому драйверу VCOM или утилите Serial/IP предъявляются следующие требования. Системные требования:

- Поддержка платформы операционной системы Windows (32/64 бит)
 - Win10
 - Win8
 - Win7
 - Vista
 - XP
 - 2008
 - 2003 (также Microsoft 2003 Terminal Server)
 - 2000 (также Microsoft 2000 Terminal Server)
 - NT (также Microsoft NT Terminal Server)
 - 4.0
 - 9x
 - Citrix MetaFrame Access Suite

6.1.2. Ограничения

Драйвер Virtual COM поддерживает до 256 виртуальных COM-портов на одном ПК. Выбор номера COM-порта доступен в диапазоне от COM1 до COM4096. Следует отметить, что COM-порты, которые уже заняты системой или другими устройствами, будут недоступны.

6.1.3. Установка

Необходимо запустить установочный файл Virtual COM, находящийся на компакт-диске, или загрузить копию с WEB-сайта разработчика, чтобы установить драйвер Virtual COM для вашей операционной системы. Следует отключить антивирусное программное обеспечение и попробовать еще раз, если установка не удалась. В конце установки необходимо выбрать хотя бы один виртуальный COM-порт на панели управления Serial/IP.

6.1.4. Удаление

- В меню Windows «Пуск» необходимо выбрать «Панель управления», и затем «Добавление и удаление программ».
- Необходимо выбрать Serial/IP Version x.x.x в списке установленного программного обеспечения.
- Необходимо нажать на кнопку «Удалить» для удаления программы.

6.2. Включение VCOM на серверах последовательных устройств и выбор VCOM в Windows

В этом разделе описана процедура включения Virtual COM (VCOM) на NetXpert NXI-3011, v2 и на ПК на базе Windows. Необходимо следовать инструкциям, описанным здесь, чтобы настроить приложение Virtual COM.

6.2.1. Включение VCOM на серверах последовательных устройств

Включение Virtual COM на серверах последовательных устройств (т.е. NetXpert NXI-3011, v2) осуществляется путем входа в пользовательский WEB-интерфейс. Он расположен в настройках COM 1 или другого COM в меню Serial, как описано в пп. 5.2.1.

На рисунке 6.4 показано, как включить Virtual COM в режиме TCP Server Link Mode на NetXpert NXI-3011, v2. Подробная информация о настройке Канального режима с Virtual COM находится в предыдущей главе начиная с пп. 5.1.

LINK Mode

To choose specific working mode for COM 2 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Virtual COM
IP Filter	☐ Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1
Response Behavior	☐ Request & Response Mode ☐ Reply to requester only ☒ Reply to all ☒ Transparent Mode

Рис. 6.4. Включение приложения Virtual COM для COM 2 в режиме TCP-сервера.

6.2.2. Запуск программной утилиты Serial/IP в Windows

После установки драйвера Virtual COM в операционной системе Windows, как было описано в пп. 6.1.3, можно открыть панель управления Serial/IP Control Panel одним из следующих способов:

- Нажать на меню Windows Пуск → Выбрать Все программы → Выбрать Serial/IP → Выбрать Панель управления.
- В панели управления Windows открыть утилиту Serial/IP.
- В области уведомлений Windows, как показано на рисунке 6.5, сделать щелчок правой кнопкой мыши на значке Serial/IP и нажать на меню Configur для открытия панели управления Serial/IP.

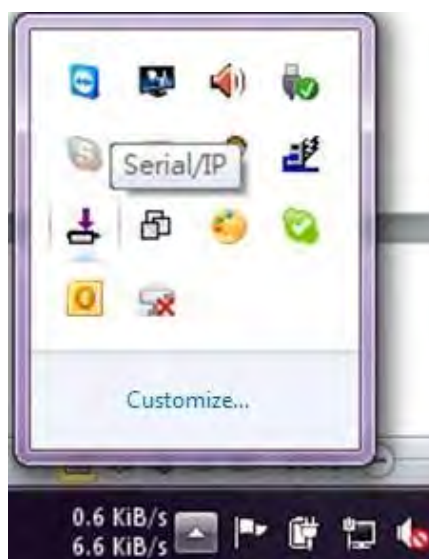


Рис. 6.5. Значок Serial/IP в области уведомлений Windows.

Если виртуальный COM-порт не выбран, появится диалоговое окно «Select Ports» и попросит пользователя выбрать хотя бы один COM-порт в качестве виртуального COM-порта, прежде чем продолжить, как показано во всплывающем окне на рисунке 6.6. Можно выбрать COM-порт, установив флажок в списке виртуальных COM-портов. Следует отметить, что если номер COM-порта отсутствует в списке, он может использоваться другим приложением или операционной системой. Пользователь может выбрать диапазон из нескольких COM-портов, которые будут использоваться в качестве виртуальных COM-портов, введя диапазон COM-порта в текстовое поле под списком. После выбора виртуальных COM-портов необходимо нажать кнопку ОК, чтобы продолжить.

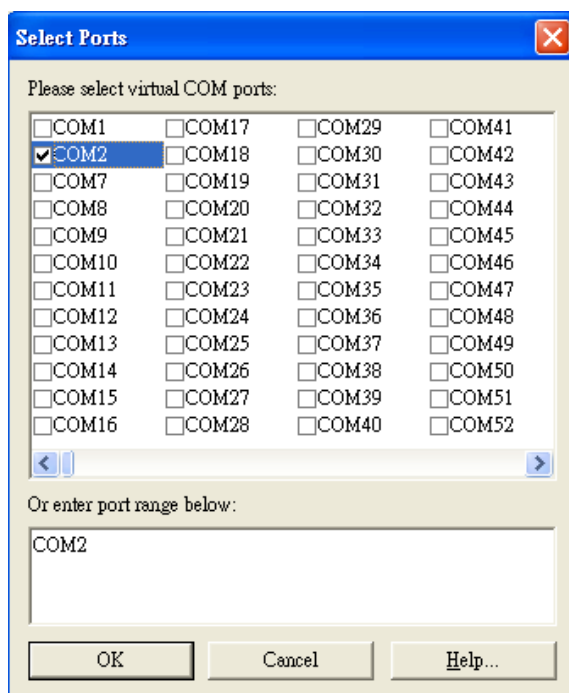


Рис. 6.6. Всплывающее окно для выбора виртуальных COM-портов.

После того, как будет выбран хотя бы один виртуальный COM-порт, появится окно Serial/IP Control Panel, как показано на рисунке 6.7. В левой части окна панели управления отображается список выбранных виртуальных COM-портов. Можно нажать на кнопку «Select Ports...» под списком, чтобы добавить или удалить виртуальные COM-порты из списка. В правой части окна Serial/IP Control Panel отображаются конфигурации выбранного виртуального COM-порта, отмеченного синим в списке. Каждый виртуальный COM-порт может иметь свои собственные настройки. Подробная информация о настройке виртуального COM-порта будет описана в следующей главе.

Примечание: Изменения в виртуальных COM-портах вступают в силу незамедлительно, поэтому нет необходимости сохранять настройки вручную. Однако, если виртуальный COM-порт уже используется, необходимо закрыть и открыть его после полного завершения TCP-соединения, чтобы изменения вступили в силу.

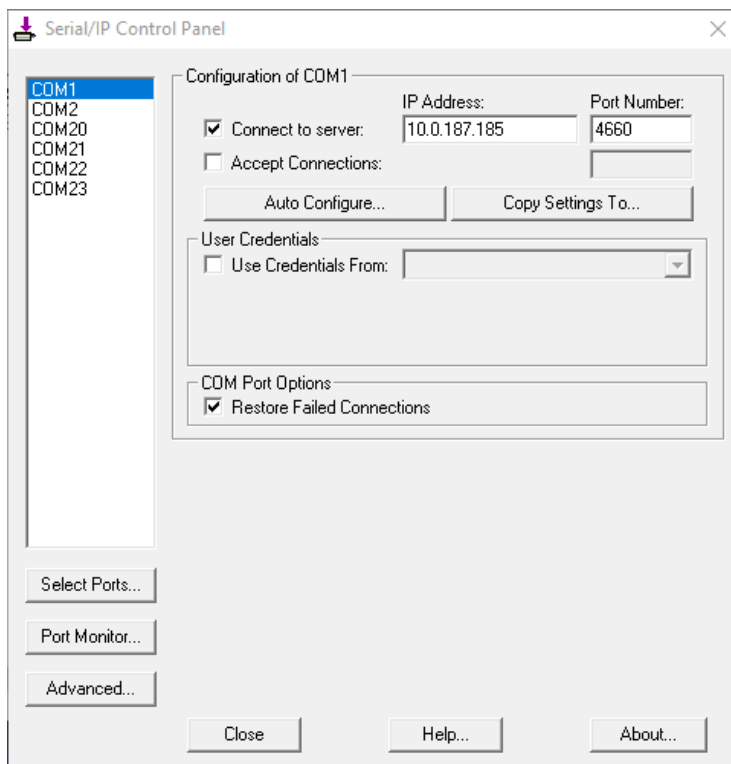


Рис. 6.7. Окно панели управления Serial/IP.

6.2.3. Конфигурирование VCOM-портов

Для каждого VCOM-порта, выбранного в списке в левой части панели управления Serial/IP Control Panel, можно использовать следующие процедуры для конфигурации этого VCOM-порта.

Если сервер последовательных устройств (то есть NetXpert NXI-3011, v2) работает в канальном режиме TCP-сервера (рекомендовано), утилита Serial/IP на хост-компьютере должна быть настроена как TCP-клиент, подключающийся к серверу последовательных устройств. Необходимо включить опцию «Connect to Server» (поставив флажок перед ней, как показано рисунке 6.9) и ввести IP-адрес сервера последовательных устройств с указанным номером порта. Номер порта здесь является Локальным порт прослушивания (Local Listening Port) для сервера последовательных устройств, который указан в поле Local Port на рисунке 5.11.

Если сервер последовательных устройств (то есть NetXpert NXI-3011, v2) работает в канальном режиме TCP-клиента, утилита Serial/IP на хост-компьютере должна быть настроена как TCP-сервер, ожидающий подключения сервера последовательных устройств к хост-компьютеру. Необходимо включить опцию «Accept Connections option» (установив флажок перед ней) и ввести указанный номер порта. Этот номер порта является портом назначения (Destination Port) сервера последовательных устройств. Нельзя одновременно включать опции «Connect to Server» (Подключиться к серверу) и «Accept Connections» (Принимать подключения).

В поле «User Credentials» (учетные данные пользователя) можно включить опцию «Use Credentials From» (Использовать учетные данные из), установив флажок перед ней, а затем выбрать параметры в раскрывающемся списке. Доступные источники учетных данных: Prompt on COM Port Open (запрос при открытии COM-порта), Prompt at Login (запрос при входе в систему) и Use Credentials Below (использование учетных данных ниже), как показано на рисунке 6.8. Если выбрана опция «Use Credentials Below», как показано на рисунке 6.9, требуется указать имя пользователя и пароль в соответствующих текстовых полях.

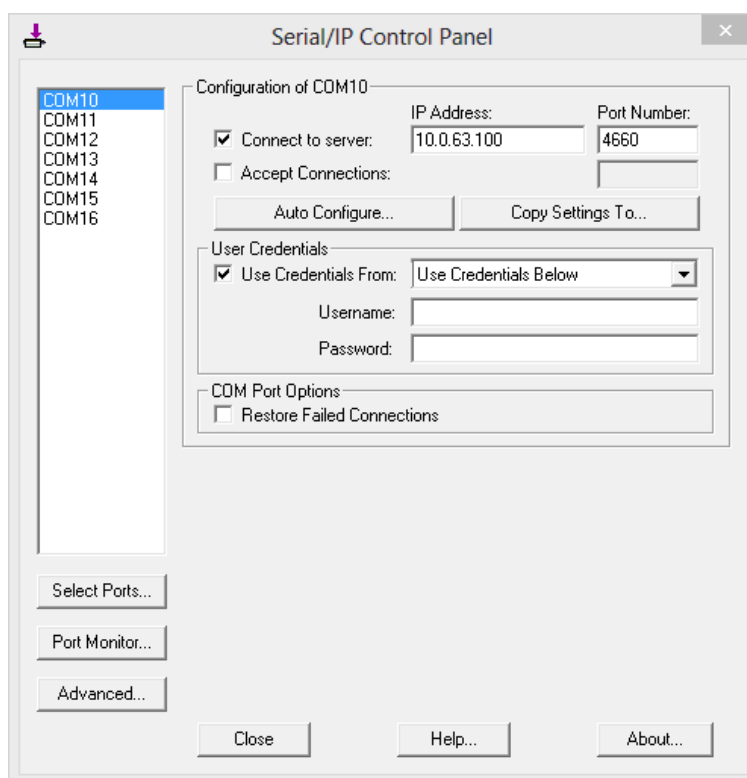


Рис. 6.8. Доступные опции для параметра Use Credential From на панели управления Serial/IP Control Panel версии 4.9.10.

В поле COM Port Options можно включить опцию Restore Failed Connections (восстанавливать неисправные соединения), поставив флажок перед ней, чтобы Virtual COM принудительно автоматически восстанавливал неисправные соединения с сервером последовательных устройств в случае нестабильных сетевых соединений.

Чтобы проверить соединение Virtual COM, можно нажать кнопку «Auto Configure...», а затем нажать кнопку «Start» во всплывающем окне, как показано на рисунке 6.10. Если тест пройден, все галочки в текстовом поле «Status» должны быть зеленого цвета. В этом окне Мастера настройки можно изменить IP-адрес сервера (IP Address), номер порта (Port Number), имя пользователя (Username) (если включена опция «Use Credential») и пароль (Password) (если включена опция «Use Credential»).

Чтобы применить изменения в окне мастера настройки к панели управления Serial/IP, необходимо нажать кнопку «Use Settings» в нижней части окна на рисунке 6.10. Также можно нажать кнопку «Copy», чтобы скопировать результаты в системный буфер обмена ПК.

Для переноса настроек между портами Virtual COM необходимо нажать на кнопку Copy Settings To, как показано на рисунке 6.9.

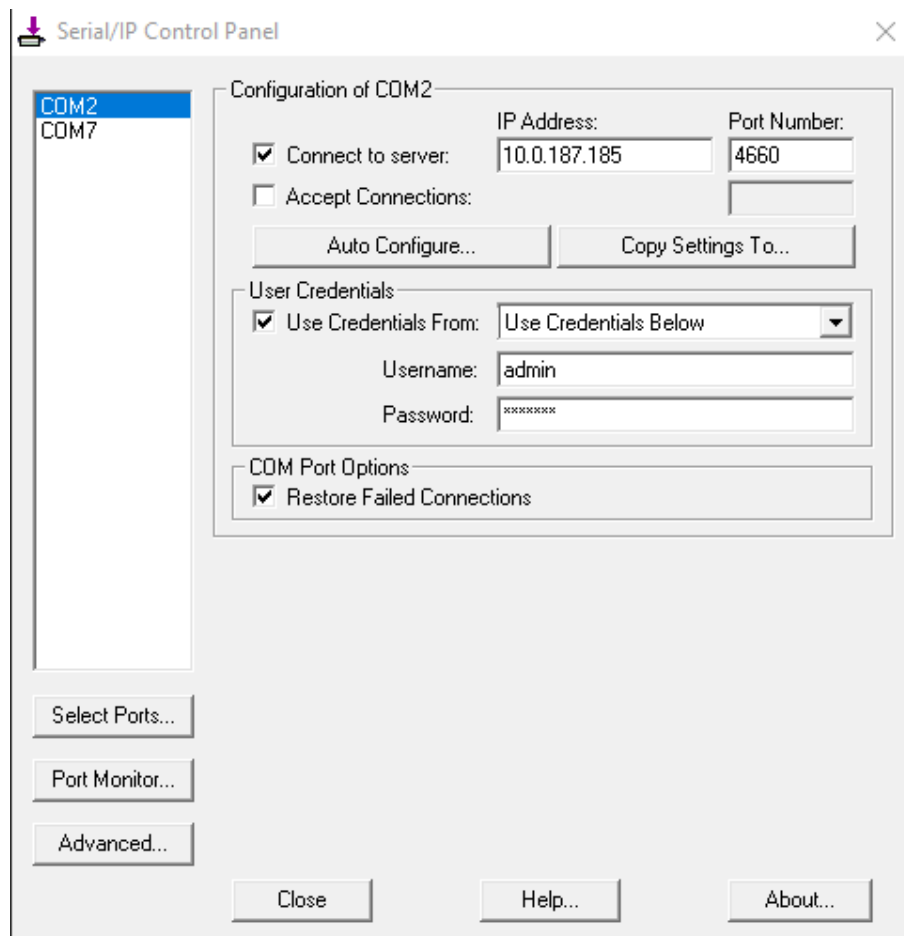


Рис. 6.9. Конфигурация порта Virtual COM 2 в качестве TCP-клиента.

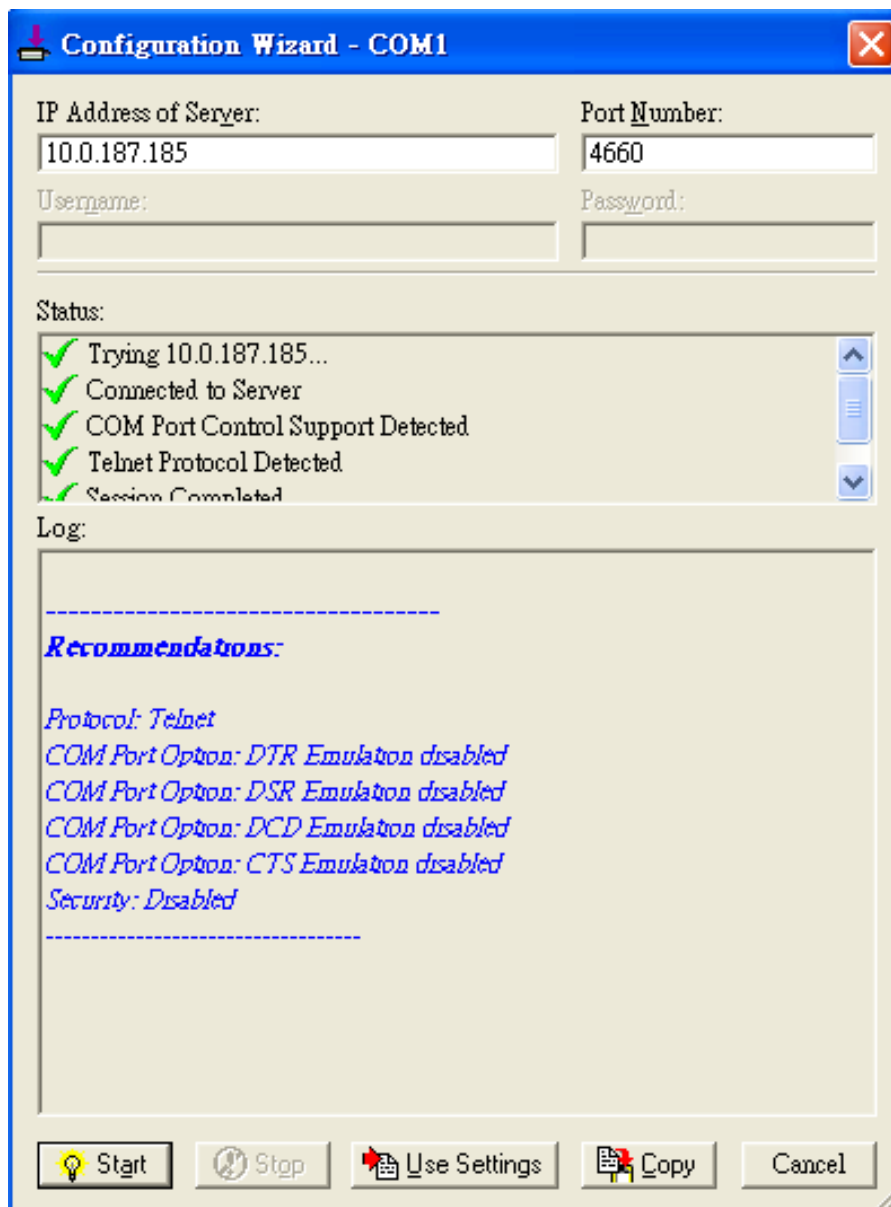


Рис. 6.10. Окно автоматической конфигурации (ранее Мастер настройки) для COM 1.

6.3. Исключения

В этом разделе приведены возможные исключения, которые могут произойти, когда пользователь тестирует соединение VCOM с помощью кнопки Auto Configure (ранее Мастер настройки). Если возникнет проблема с подключением, в текстовых полях «Status» и «Log» будут отображаться сообщения об ошибках или предупреждения. Для каждого случая далее приведены возможные исправления или советы по устранению неполадок.

Если состояние отображается с восклицательным знаком и сопровождается сообщением “Warning: timeout trying x.x.x.x”, как показано на рисунке 6.11, следует перепроверить или исправить IP-адрес VCOM и конфигурацию номера порта или конфигурацию сети ПК.

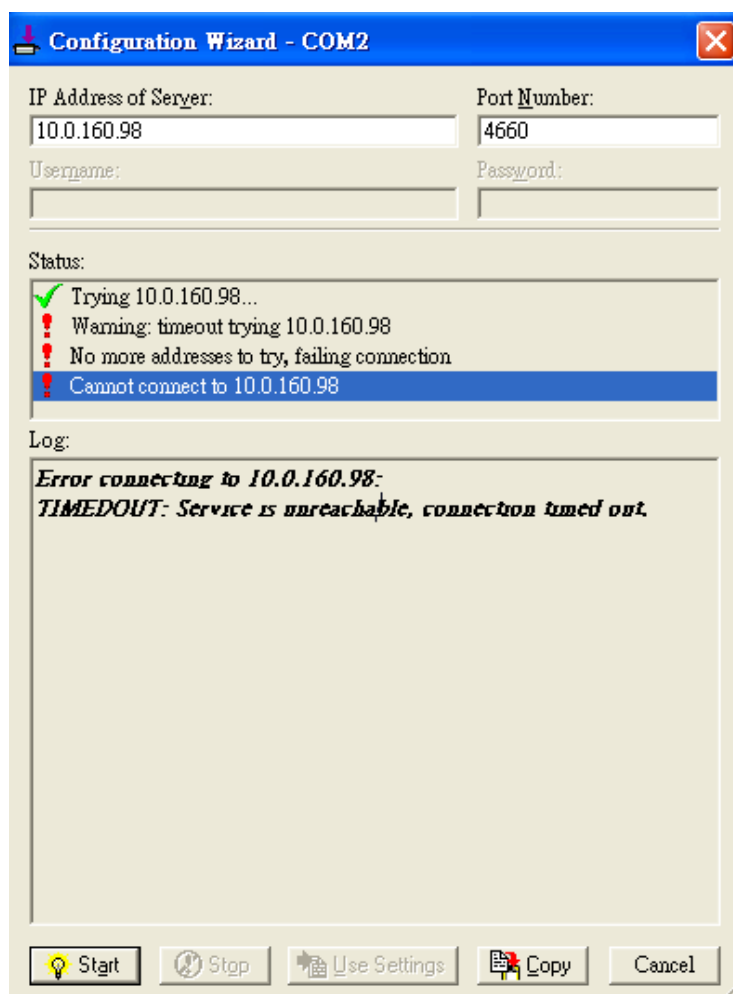


Рис. 6.11. Предупреждение об истечении срока ожидания для соединения VCOM.

Если состояние отображается с символом галочки и сопровождается сообщением "Raw TCP Connection Detected" и восклицательным знаком с сообщением "Client not licensed for this server", как показано на рисунке 6.12. следует включить опцию Virtual COM на сервере последовательных устройств.

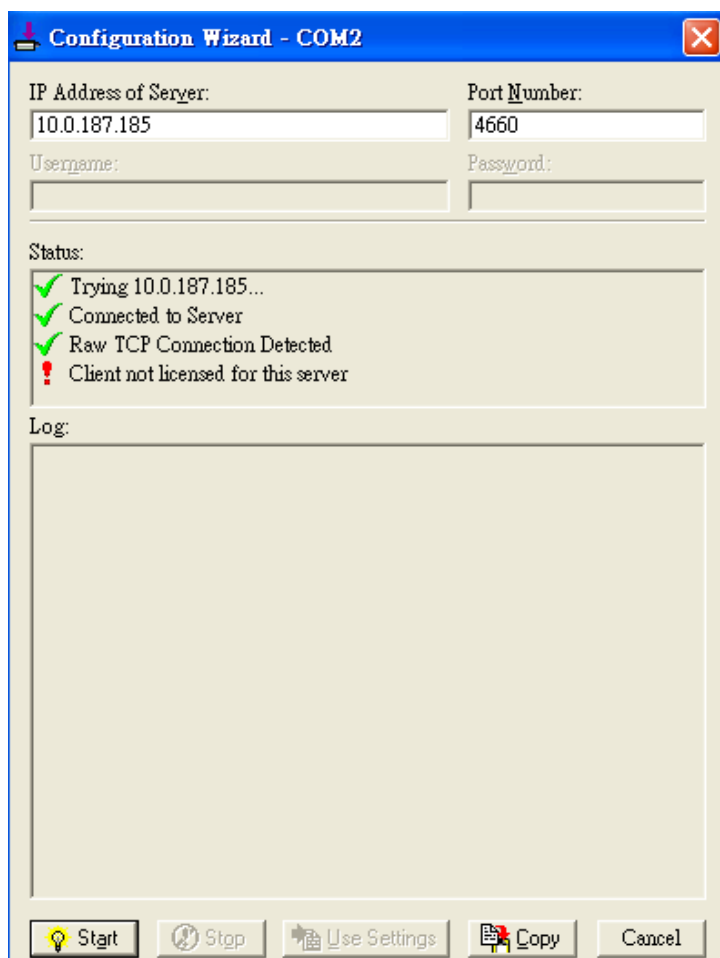


Рис. 6.12. Ошибка отсутствия лицензии у клиента для данного сервера.

Если состояние отображается с восклицательным знаком и сопровождается сообщением “Server requires username/password login”, как показано на рисунке 6.13, это означает, что опция VCOM Authentication на сервере последовательных устройств (т.е. NetXpert NXI-3011, v2) включена, но опция User Credentials в программной утилите Serial/IP не включена. Необходимо выполнить действия из пп. 4.12.2 для включения опции учетных данных и ввести имя пользователя и пароль.

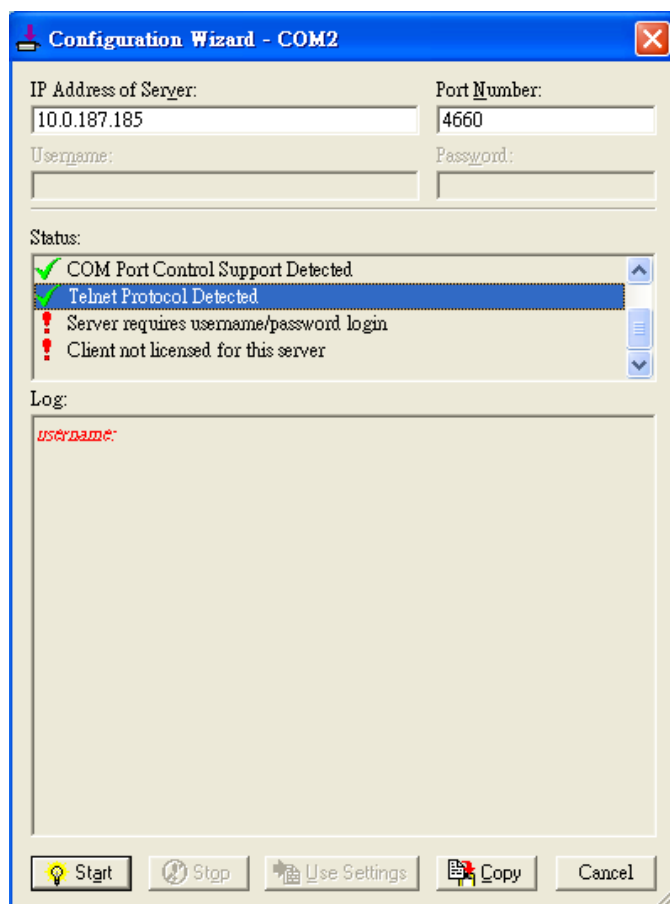


Рис. 6.13. Неудачная попытка аутентификации VCOM из-за отсутствующего имени пользователя/пароля.

Если состояние отображается с восклицательным знаком и сопровождается сообщением "Username and/or password incorrect", как показано на рисунке 6.14, это означает, что было введено неверное имя пользователя и/или пароль и процесс аутентификации прошел неудачно.

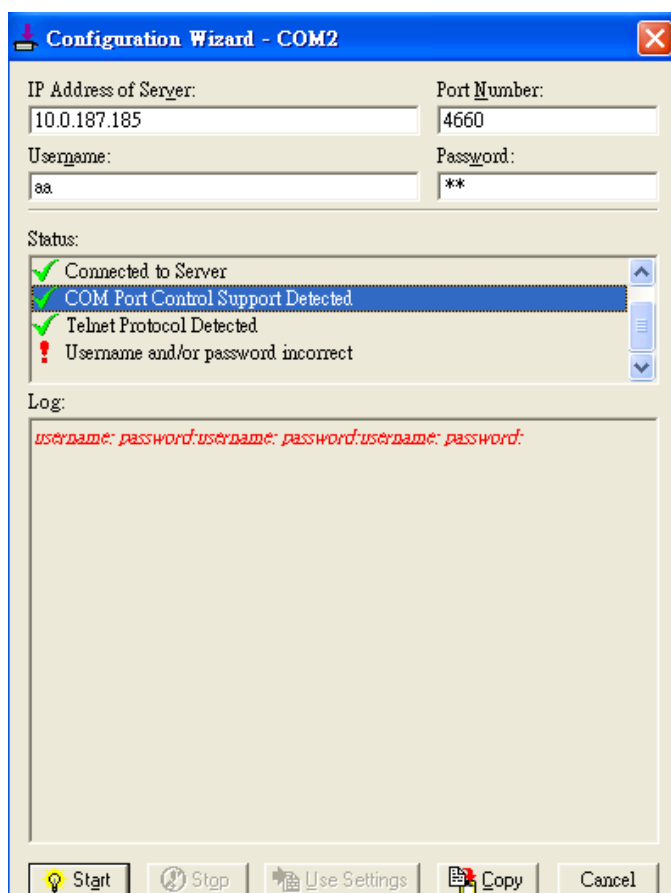


Рис. 6.14. Ошибка аутентификации VCOM из-за неправильного имени пользователя/пароля.

Если состояние отображается с восклицательным знаком и сопровождается сообщением “No login/password prompts received from server”, как показано на рисунке 6.15, это означает, что опция User Credentials в программной утилите Serial/IP включена, но опция аутентификации VCOM на сервере последовательных устройств (то есть NetXpert NXI-3011, v2) не включена.

Необходимо включить опцию VCOM Authentication на устройстве NetXpert NXI-3011, v2, настроив новое не пустое имя пользователя администратора и пароль для NetXpert NXI-3011, v2, как описано в пп. 4.12.2. Следует отметить, что параметры Username и Password для аутентификации VCOM имеют те же значения, что и имя пользователя и пароль для входа в пользовательский WEB-интерфейс NetXpert NXI-3011, v2. Учетная запись по умолчанию, с именем пользователя “admin” и паролем “default”, считается незащищенной или не является опцией аутентификации.

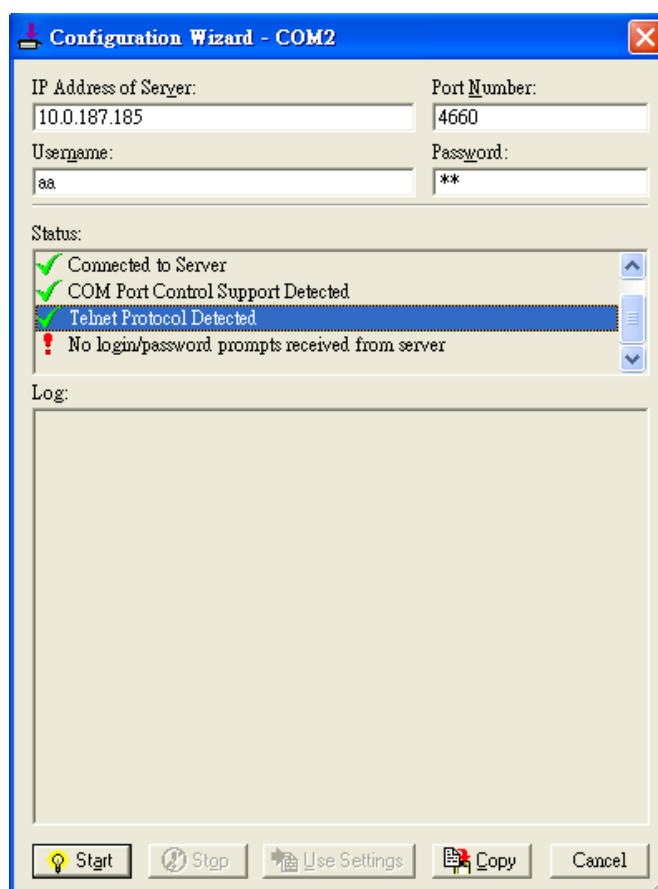


Рис. 6.15. Ошибка аутентификации VCOM из-за отключенной аутентификации VCOM на устройстве NetXpert NXI-3011, v2.

6.4. Использование монитора последовательного/IP-порта

Другой утилитой, предоставленной пользователю, является монитор последовательного/IP-порта. Он позволяет пользователю контролировать активность или состояние виртуального COM-порта и отображать сообщения, которыми обмениваются последовательные порты, которые называются трассировкой порта.

6.4.1. Запуск монитора порта

Утилита монитора последовательного/IP-порта может быть открыта одним из следующих способов:

- Нажать на кнопку Windows Пуск → Выбрать Все программы → Выбрать Serial-IP → Выбрать Port Monitor.
- Выполнить двойной щелчок мышкой на иконке Serial/IP в панели задач Windows.
- В панели задач Windows нажать правой кнопкой мышки на иконке Serial/IP и в открывшемся контекстном меню выбрать пункт Port Monitor.
- Нажать кнопку Port Monitor в окне панели управления Serial/IP.

6.4.2. Вкладка Activity

Вкладка Activity в режиме реального времени отображает состояние всех последовательных/IP COM-портов, как показано на рисунке 6.16. Если виртуальный COM-порт открыт и правильно настроен для подключения к серверу последовательных устройств (например, NetXpert NXI-3011, v2), то его состояние будет отображаться как Connected. Если монитору Serial/IP не удастся обнаружить указанный сервер последовательных устройств, то состояние порта будет отображаться как Offline.

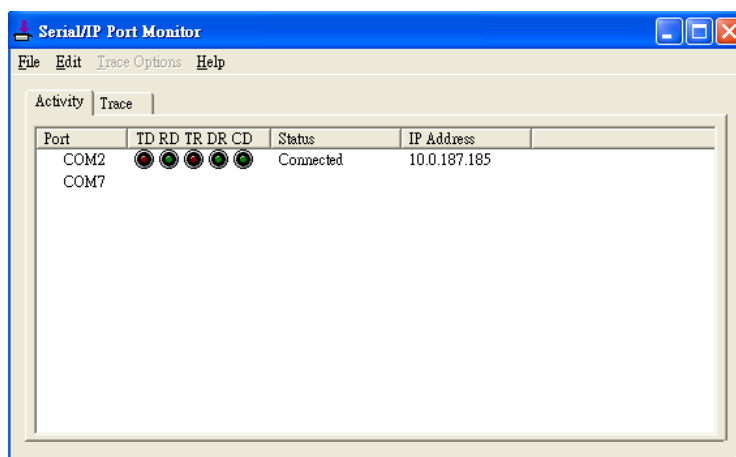


Рис. 6.16. Вкладка Activity монитора последовательного/IP-порта.

Каждый столбец на вкладке Activity Panel описывается следующим образом:

- Port: номер виртуального COM-порта.
- Индикаторы линейного сигнала: Красный цвет означает отсутствие активности, а зеленый - активность.

TD - указывает на то, что данные отправляются на сервер.

RD - указывает на то, что данные принимаются с сервера.

TR (DTR) - сигнал от приложения к серверу о том, что приложение открыло виртуальный COM-порт. Наиболее распространенное использование DTR - программно опустить его, чтобы подать сигнал модему на отключение.

DR (DSR) - сигнал от сервера к приложению о том, что модем или последовательное устройство подключено к серверу и готово к общению.

CD (DCD) - сигнал от сервера к приложению о том, что модем успешно согласовал соединение с другим устройством.

- Status: указывает на состояние соединения программного обеспечения и сервера последовательных устройств, которое может быть connected (подключен) или offline (отключен).
- IP Address: IP-адрес сервера последовательных устройств.

Примечание:

Индикаторы линейного сигнала появляются только в том случае, когда приложение открывает виртуальный COM-порт.

Индикаторы TR, DR и CD появляются только в том случае, когда используется протокол управления COM-портом или включены параметры COM-порта.

6.4.3. Вкладка Trace

Вкладка Trace обеспечивает подробное отображение с временными метками всех операций последовательных/IP COM-портов в режиме реального времени, как показано на рисунке 6.17. Чтобы начать ведение журнала виртуального COM-общения, необходимо поднять флажок Enable Trace. Чтобы остановить ведение журнала, необходимо снять флажок Enable Trace. Пользователь может переключать формат отображения между текстом ASCII (более читабельным) и шестнадцатеричным форматом (более подробно) с помощью флажка Hex Display. При поднятом флажке Auto Scroll дисплей будет постоянно показывать самые последние данные трассировки. Чтобы окно Port Monitor всегда находилось поверх окон других приложений, необходимо установить флажок Always on Top. Чтобы очистить данные трассировки, отображаемые во вкладке Trace, необходимо нажать кнопку Clear.

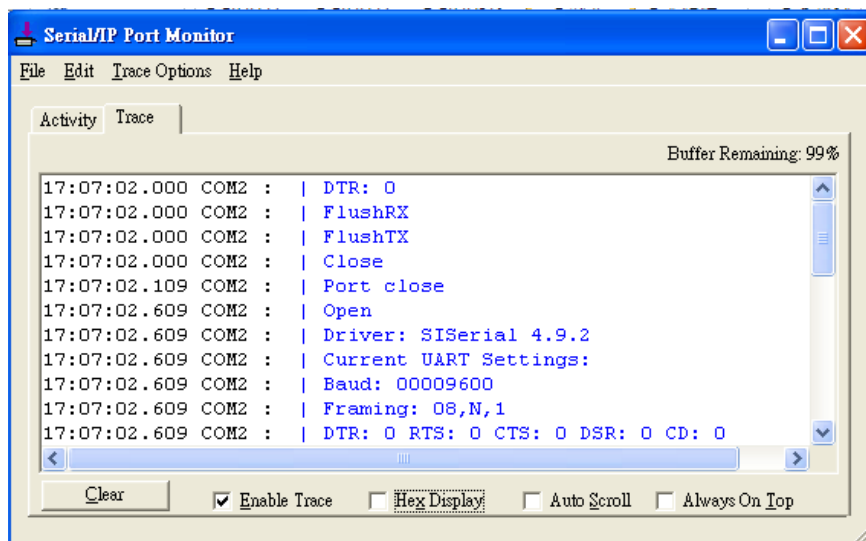


Рис. 6.17. Вкладка Trace монитора последовательного/IP-порта.

Выпадающее меню окна Port Monitor позволяет пользователю сохранять журнал и настраивать сбор данных последовательного соединения.

- **File:** Чтобы сохранить файл журнала, который в случае возникновения проблем с виртуальным COM-соединением можно выслать в Nateks для последующего анализа, необходимо нажать на меню File и затем выбрать Save As.
- **Trace Options:**

Select Ports to Captur. Этот пункт меню позволяет уменьшить количество отслеживаемых портов до подмножества всех сконфигурированных виртуальных COM-портов. Эта функция позволяет уменьшить влияние трассировки на память и производительность системы для больших приложений.

Select Ports to Display. Этот пункт меню позволяет уменьшить количество отображаемых на дисплее портов до подмножества захватываемых портов. Для широкого применения, эта функция позволяет сфокусироваться на интересующих портах среди всех захваченных.

Buffer Size: Этот пункт меню позволяет изменять объем выделенной оперативной памяти, используемой для трассировки, который может быть нормальным или большим.

System Debug Output: Этот пункт меню позволяет пользователю включить отправку данных трассировки в канал отладки системы и при желании поставить на них метку.

На вкладке Trace отображается одно последовательное событие на строку, упорядоченное по времени. Каждое событие начинается с временной отметки. События передачи будут показаны зелёным цветом, и перед ними будет значок "»", в то время как события приёма будут показаны красным цветом, а перед ними будет значок "«". Управляющие события будут показаны синим цветом, а перед ними будет значок "|".

Примечание: дисплей Trace вмещает до 512 килобайт данных о событиях, что достаточно для покрытия достаточно продолжительного сеанса трассировки. Однако, если предел достигнут, трассировка очищается и начинается заново.

6.5. Расширенные настройки Serial/IP

Чтобы открыть окно расширенных настроек Serial/IP Advanced Settings (рисунок 6.18), на панели управления Serial/IP Control Panel необходимо нажать на кнопку Advanced. Окно Serial/IP Advanced Settings содержит две вкладки: Options и Proxy Server. Для загрузки настроек по умолчанию, на вкладке Options необходимо нажать на кнопку Use Default Settings. Подробное описание каждого параметра и руководство по настройке прокси-сервера будет приведено в следующих подразделах.

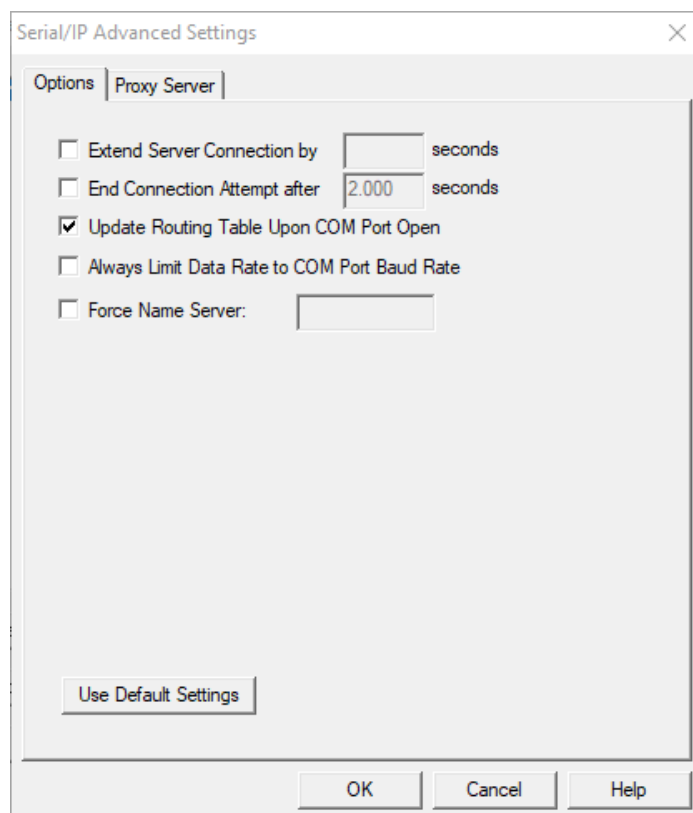


Рис. 6.18. Окно Serial/IP Advanced Settings.

6.5.1. Параметры расширенных настроек

На вкладке Options можно изменять ряд расширенных настроек и ввести необходимые параметры для программного обеспечения Serial/IP. Описание каждого параметра приведено ниже.

- **Extend Server Connection:** Если этот параметр включен, то TCP-соединение поддерживается в течение указанного времени после закрытия COM-порта. Значение времени по умолчанию составляет 8000 миллисекунд.
- **End Connection Attempt after:** Если этот параметр включен, то ожидающие попытки подключения завершаются, если они не увенчались успехом в указанное время. Значение времени по умолчанию составляет 2000 миллисекунд.
- **Update Routing Table Upon COM Port Open:** Если этот параметр включен, то поддерживается IP-маршрутизация к серверу в другой подсети путем изменения таблицы IP-маршрутизации.
- **Always Limit Data Rate to COM Port Baud Rate:** Если этот параметр включен, то скорость передачи данных, действующая для виртуального COM-порта, ограничивается.
- **Force Name Server:** Данная опция позволяет пользователю ввести желаемый IP-адрес DNS-сервера.

6.5.2. Использование Serial/IP с Proxy-сервером

Serial/IP Redirector также поддерживает сетевые соединения TCP, осуществляемые через прокси-сервер, который может контролировать доступ ко внешним сетям (таким как Интернет) из частной сети, в которой отсутствует прозрачная маршрутизация на основе IP, такая как преобразование сетевых адресов (NAT).

Можно включить поддержку Serial/IP виртуального COM-порта через прокси-сервер с помощью настроек Serial/IP Proxy Server settings.

Настройки прокси-сервера можно найти в окне «Advanced Settings» и перейти на вкладку Proxy Server, как показано на рисунке 6.19. Для включения использования прокси-сервера необходимо поставить флажок в поле опции Use a Proxy Server. Затем необходимо выбрать тип протокола из выпадающего списка Protocol Type, который может быть HTTPS или Socks V4, или Socks V5. Затем ввести IP-адрес прокси-сервера в текстовом поле IP Address of Server и указать номер порта в поле Port Number.

По умолчанию номер порта для HTTPS равен 8080, а для Socks V4 и V5 равен 1080. Дополнительно в блоке Login to Server Using можно ввести имя пользователя в поле Username и пароль в поле Password, который может потребовать прокси-сервер. Либо можно нажать на кнопку Auto Detect, чтобы программное обеспечение автоматически определило настройки прокси-сервера. Также можно проверить настройки прокси-сервера, нажав на кнопку Test, и остановить тестирование, нажав на кнопку Stop.

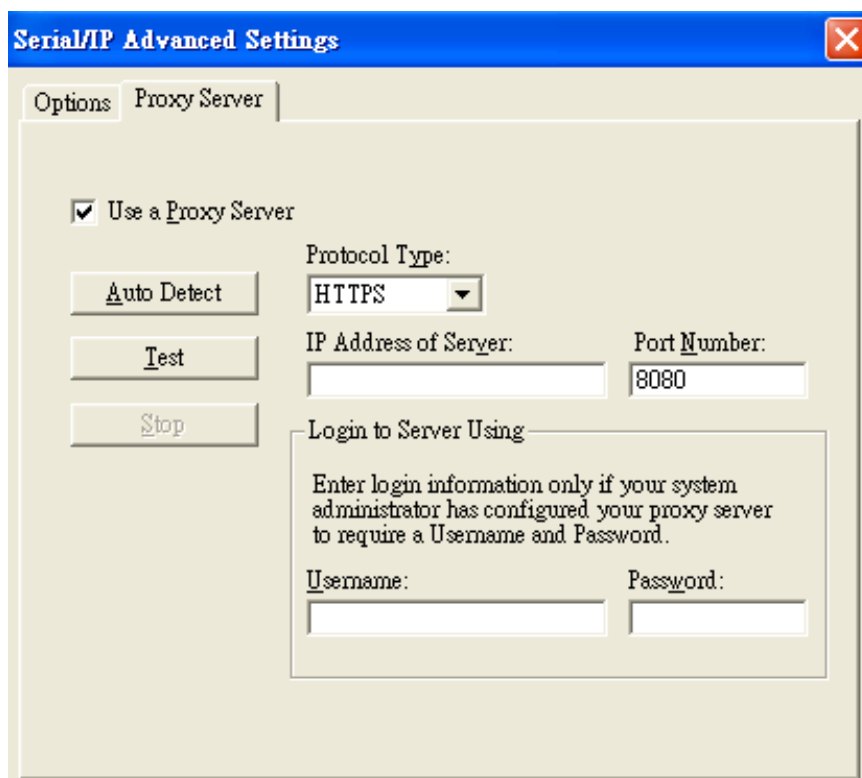


Рис. 6.19. Вкладка Proxy Server в расширенных настройках Serial/IP.

7. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

7.1. Аппаратное обеспечение

Таблица 7.1. Спецификация аппаратного обеспечения.

Система			
ЦП	32-бит ARM на основе TI CPU AM3354 800MHz		
Флэш-память	32 Мб		
ОЗУ	256 Мб		
EEPROM	8 кб		
Перезагрузка	Встроенный ключ (сброс до заводских настроек)		
Схема обеспечения безопасности	Аппаратная встроенная		
Сеть			
Интерфейс Ethernet	IEEE 802.3 10BaseT IEEE 802.3u 100BaseT(X) IEEE 802.3ac 1000BaseT(X) SFP на специальной версии Подключение: SFP или RJ-45		
Протокол	ICMP TCP UDP IPv4 HTTP Syslog	DNS DHCP-клиент SNMPv1, v2c, v3 RADIUS	SMTP NTP ARP Telnet RFC2217
Безопасность	VPN через IPsec-туннелирование (максимально 64 туннелей) по LAN (программно-реализованный)		
Serial			
Последовательный интерфейс	RS232/422/485 программно-выбираемый (по умолчанию: RS232)		
Последовательный разъем	1 или 4 последовательных порта (DB-5 или DB-9)		
Связь через последовательный порт	Скорость передачи данных: 1200 бит/сек ... 921600 бит/сек Проверка четности: None (отсутствует), Even (четный), Odd (нечетный), Mark (метка) или Space Data (пустые данные). Биты: 5, 6, 7, 8 Стоповый бит: 1, 2 программно-выбираемый. Контроль потока: RTS/CTS (только RS232), XON/XOFF, отсутствует		

<i>Светодиодная индикация</i>	
Светодиодная индикация	Power RUN ALARM LAN COM port:
<i>Требования по электропитанию и электромагнитной совместимости</i>	
Вход	9 ... 56 В постоянного тока с резервированием.
Потребление	Максимально 7.8 Вт
<i>Механические</i>	
Размеры (ВхШхГ, мм)	NXI-3011, v2-2T-1D: 110 x 32 x 90 NXI-3011, v2-2T-4D: 145 x 55 x 113 NXI-3011, v2-2GX-4D: 145 x 55 x 113
Корпус	IP30 защита, металлический корпус.
<i>Окружающая среда</i>	
Температура	Работа -40 ... +85°C
	Хранение -40 ... +85°C
Относительная влажность	5 ... 95%, при 25°C без образования конденсата

7.2. Назначение контактов разъема последовательного порта

Разъём DB9 портов RS232/RS485/RS422.

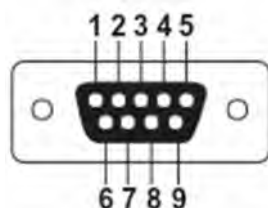


Рис. 7.1. Номера контактов разъема DB9.

Таблица 7.2. Назначение контактов разъема для DB9 к разъемам RS232/RS422/RS485.

№ контакта	RS232 полнодуплексный	RS422 полнодуплексный	RS485 полудуплексный
1	DCD	Недоступно	Недоступно
2	RxD	TxD+	Data+
3	TxD	RxD+	Недоступно
4	DTR	Недоступно	Недоступно
5	SG (сигнальная земля)	SG (сигнальная земля)	SG (сигнальная земля)
6	DSR	Недоступно	Недоступно
7	RTS	RxD-	Недоступно
8	CTS	TxD-	Data-
9	RI	Недоступно	Недоступно

5-контактный терминальный блок к портам RS232/422/485 для моделей NetXpert NXI-3011, v2-xx-4D.

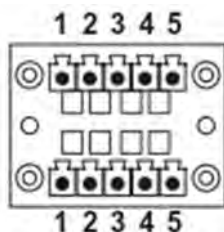


Рис. 7.2. Номера контактов разъема терминального блока (ТВ-5).

Таблица 7.3. Назначение контактов разъема для 5-контактного терминального блока портов RS232/422/485.

№ контакта	RS232	RS422 4-жильный RS485	2-W RS485
1	RxD	TxD+	Data+
2	CTS	TxD-	Data-
3	TxD	RxD+	Недоступно
4	RTS	RxD-	Недоступно
5	SG (сигнальная земля)	SG (сигнальная земля)	SG (сигнальная земля)

5-контактный терминальный блок к портов RS232/422/485 для моделей NetXpert NXI-3011, v2-xx-1D.

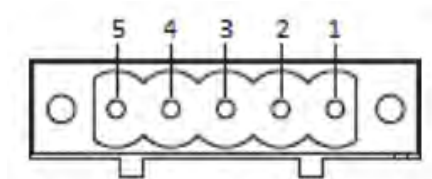


Рис. 7.3. Номера контактов разъема терминального блока (ТВ-5).

Таблица 7.4. Назначение контактов разъема для 5-контактного терминального блока портов RS232/422/485 для моделей NetXpert NXI-3011, v2-xx-1D.

№ контакта	RS232	RS422 4-жильный RS485	2-W RS485
1	RxD	TxD+	Недоступно
2	CTS	TxD-	Недоступно
3	TxD	RxD+	Data+
4	RTS	RxD-	Data-
5	SG (сигнальная земля)	SG (сигнальная земля)	SG (сигнальная земля)

7.3. Назначение контактов разъема для LAN-интерфейса NetXpert NXI-3011, v2

Разъемы RJ-45 для 10/100/1000BaseT(X) Ethernet.

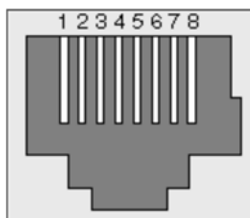


Рис. 7.4. NetXpert NXI-3011, v2. Ethernet-порт на RJ-45 с номерами контактов.

Таблица 7.5. Назначение контактов разъема для RJ-45 NetXpert NXI-3011, v2.

10/100/1000BaseT(x)								
№ контакта	1	2	3	4	5	6	7	8
Сигнал	Tx+	Tx-	Rx+	-	-	Rx-	-	-
1000Base-T								
№ контакта	1	2	3	4	5	6	7	8
Сигнал	BI_DA+	BI_DA-	BI_DB+	BI_DC+	BI_DC-	BI_DB-	BI_DD+	BI_DD-

7.4. Назначение контактов разъёма питания и аварийной сигнализации

7-ми контактный клеммный разъём для моделей NetXpert NXI-3011, v2-xx-4D

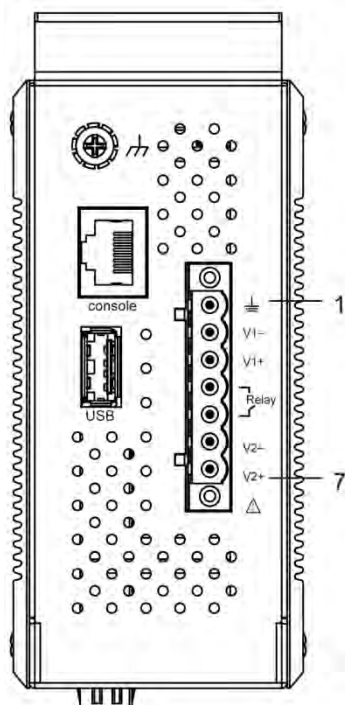


Рис.7.5. Вид верхней панели с разъёмом питания для моделей NetXpert NXI-3011, v2-xx-4D.

Таблица 7.6 назначение контактов разъема

№ контакта	обозначение	описание
1		Защитное заземление
2	V1-	Минус источника питания 1
3	V1+	Плюс источника питания 1
4	 Relay	Реле аварийной сигнализации нормально разомкнутое (1A 30B)
5		
6	V2-	Минус источника питания 2
7	V2+	Плюс источника питания 2

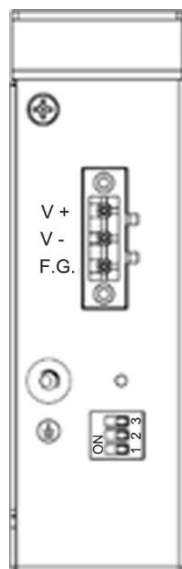
3-х контактный клеммный разъём для моделей NetXpert NXI-3011, v2-xx-1D.

Рис. 7.6. Вид верхней панели с разъёмом питания для моделей NetXpert NXI-3011, v2-xx-4D.

Таблица 7.7 назначение контактов разъема

№ контакта	обозначение	описание
1	V +	Плюс источника питания
2	V -	Минус источника питания
3	F.G.	Защитное заземление

Назначение контактов DIP-переключателя.

Таблица 7.8 назначение контактов разъема

№ переключателя	функция	положение	сопротивление
1	Терминация	on	120 Ом
		off	-
2	Подтяжка к низкому уровню	on	1 кОм
		off	100 кОм
3	Подтяжка к высокому уровню	on	1 кОм
		off	100 кОм

7.5. Консольный кабель RJ-45-DB9

На одном конце кабеля расположен разъем RJ-45 для подключения к консольному порту коммутатора, на другом конце находится разъем DB9 для подключения к компьютеру. На Рисунке 7.7 показан порядок соединения для кабеля DB9-RJ-45.



Рис. 7.7. Порядок соединения для кабеля DB9-RJ-45.

Таблица 7.9. Назначение контактов разъемов для кабеля DB9-RJ-45.

Разъем DB9	Разъем RJ-45	Значение	Описание
2	3	RXD	Прием данных
3	6	TXD	Передача данных
5	4	GND	Заземление

7.6. Светодиодные индикаторы

Таблица 7.10. Значение цветов светодиодной индикации устройства NetXpert NXI-3011, v2.

Название	Цвет	Состояние	Сообщение
PWR (Power)	Зеленый	Постоянно горит/включен	Электропитание подключено и работает
		выключен	Электропитание выключено
TX	Зеленый	мигает	COM-порт передает данные
		выключен	COM-порт не передает данные
RX	Зеленый	мигает	COM-порт получает данные
		выключен	COM-порт не получает данные
RUN	Зеленый	мигает	Прошивка AP работает нормально
		Вкл/Выкл	Система не готова или остановлена
LAN	Оранжевый (скорость)	включен	Ethernet передает на 1 Гбит/сек
		Медленно мигает	Ethernet передает на 100 Мбит/сек
		выключен	Ethernet передает на 10 Мбит/сек
	Зеленый (данные)	мигает	Ethernet данные передаются
		выключен	Ethernet отсутствуют данные для передачи

7.7. Программное обеспечение

Таблица 7.11. Программные средства и утилиты.

<i>Программное обеспечение</i>	
Утилиты	Windows Virtual COM Driver
Инструменты настройки	Утилита Web Console SSH Telnet