

The power behind competitiveness

Модуль InsightPower SNMP IPv6 Delta для шкафов распределения питания (ШРП)

Руководство по эксплуатации

www.deltapowersolutions.com



Сохраняйте данное руководство

В этом руководстве содержатся важные инструкции и предупреждения, которые следует соблюдать при установке, эксплуатации, хранении и обслуживании данного продукта. Несоблюдение этих инструкций и предупреждений приведет к аннулированию гарантии.

Авторское право 2013 компании Delta Electronics Inc. Все права защищены. Все права на данное руководство по эксплуатации (далее руководство), включая, но не ограничиваясь содержанием, информацией и числовыми значениями, являются исключительной собственностью компании Delta Electronics Inc. (далее Delta). Руководство может применяться только к эксплуатации или использованию данного продукта. Любая форма передачи, копирования, распространения, воспроизведения, изменения, перевода, изъятия или использования данного руководства, полностью или частично, запрещена без предварительного письменного разрешения компании Delta. Поскольку компания Delta непрерывно совершенствует и развивает свою продукцию, она оставляет за собой право в любое время вносить изменения в информацию, содержащуюся в настоящем руководстве, без обязательного уведомления каких-либо лиц о таких доработках или изменениях. Компания Delta приложит все возможные усилия для обеспечения точности и целостности этого руководства. Компания Delta отказывается от каких-либо видов или форм поручительства, гарантий или обязательств, выраженных прямо или косвенно, включая, но не ограничиваясь перечисленным, в отношении полноты, безукоризненности, точности, отсутствия нарушений, коммерческой пригодности или пригодности для конкретных целей данного руководства.

Содержание

Глава 1: Важная информация о безопасности	1
1-1 Предупреждения	1
1-2 Соответствие стандартам	1
Глава 2 : Введение	2
2-1 Описание продукта	2
2-2 Особенности	2
2-3 Комплект поставки.....	3
2-4 Устройства связи и управления.....	4
Глава 3 : Установка	7
Глава 4 : Настройки системы	8
4-1 Настройка через веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП	8
4-2 Настройка с помощью EzSetting.....	10
4-3 Настройка через Telnet.....	11
4-4 Настройка через COM-порт	12
4-5 Настройка в консольном режиме.....	14
Глава 5 : Веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП	21
5-1 Device (устройство)	22
5-1-1 Status (Состояние)	22
Information (Информация).....	24
System (Система).....	25
Primary (Первичные данные).....	26
Secondary (Вторичные данные)	27
Panel (Панель управления)	28
5-1-2 Data Log (Журнал данных)	28
5-1-3 Environment (Условия окружающей среды)	29
5-1-4 Configuration (Конфигурация)	30
Connection (Связь)	30
Data Log (Журнал данных)	30
Environment (Условия окружающей среды)	30
5-2 System (Система)	31
5-2-1 Administration (Администрирование)	31
Меню User Manager	31
TCP/ IP	32

Web (Сеть).....	33
Console (Консоль).....	34
FTP	35
Time Server (Сервер времени).....	35
Syslog (Системный журнал)	36
Batch Configuration (Пакетное конфигурирование).....	36
Upgrade (Обновление).....	38
5-2-2 Notification (Уведомление).....	38
SNMP Access (Доступ к SNMP).....	38
SNMPv3 USM (Диспетчер пользователей SNMPv3 USM)	39
SNMP Trap (SNMP ловушка)	40
Mail Server (Почтовый сервер).....	41
Event Level (Уровень события).....	42
5-2-3 History (записи действий пользователя или системы)	43
Глава 6 : Обновление встроенного ПО SNMP-устройств	44
Глава 7 : Устранение неисправностей	47
Приложение А: Характеристики	54
Приложение В: Гарантия	55

Глава 1: Важная информация о безопасности

1-1 Предупреждения

- Модуль InsightPower SNMP IPv6 для ШРП, именуемый далее SNMP IPv6, предназначен для работы с ШРП (шкафы распределения питания). Он должен быть установлен в слот SNMP ШРП.
- Запрещается устанавливать и эксплуатировать данное устройство в присутствии легковоспламеняющихся веществ.
- Не пытайтесь разобрать данное устройство.
- Не пытайтесь выполнять внутренние изменения в данном модуле.
- Не пытайтесь ремонтировать или заменять его внутренние компоненты. Когда потребуется ремонт, обратитесь по всем услугам к своему локальному дилеру или сервисному персоналу.
- Не допускайте попадания в модуль каких-либо посторонних предметов или жидкостей.
- При установке и эксплуатации модуля соблюдайте указания данного руководства.
- Не воспроизводите включенный в комплект компакт-диск на обычном лазерном проигрывателе. Это может вызвать громкий шум и привести к необратимой потере слуха.

1-2 Соответствие стандартам

- **EN 55022: 2006 + A1: 2007, класс A**
EN 61000-3-3: 1995+A1: 2001+A2: 2005
- **EN 55024: 1998 + A1: 2001 + A2: 2003**
IEC 61000-4-2: 1995+A1: 1998+A2: 2000
IEC 61000-4-3: 2006
IEC 61000-4-4: 2004
IEC 61000-4-5: 2005
IEC 61000-4-6: 2007
IEC 61000-4-8: 1993+A1: 2000
IEC 61000-4-11: 2004

Глава 2 : Введение

2-1 Описание продукта

Модуль InsightPower SNMP IPv6 для ШРП — это интеллектуальное устройство, служащее интерфейсом между ШРП и сетью. Он обменивается данными с ШРП для получения данных, параметров и информации о состоянии системы, панели управления и распределительных сетей. Благодаря удобному для пользователя веб-интерфейсу постоянного мониторинга и управления можно легко управлять ШРП и SNMP IPv6. Модуль поддерживает широкий диапазон стандартных протоколов, включая SNMPv3, HTTP, SFTP и Telnet.

2-2 Особенности

- **Дистанционное управление и мониторинг**
Управление ШРП с рабочих станций, подключенных к сети.
- **Полная поддержка протоколов**
Включая HTTP, HTTPS, SNMPv3, FTP, SFTP и Telnet.
- **Совместим с датчиком EnviroProbe**
Отлично работает с датчиком Delta EnviroProbe (продается отдельно) для определения температуры окружающей среды и состояния сухого контакта.
- **Поддержка шифрованных подключений**
Включая HTTPS, SSH, SFTP и SNMPv3 для повышения безопасности передачи данных.
- **Полный журнал событий и данных**
Демонстрация и отслеживание состояния системы ШРП, сетевых данных и событий.
- **Поддержка протокола IPv6**
IPv6 Ready Logo Phase 2 (Логотип совместимости с IPv6 фаза 2, идентификатор логотипа 02-C-000624)

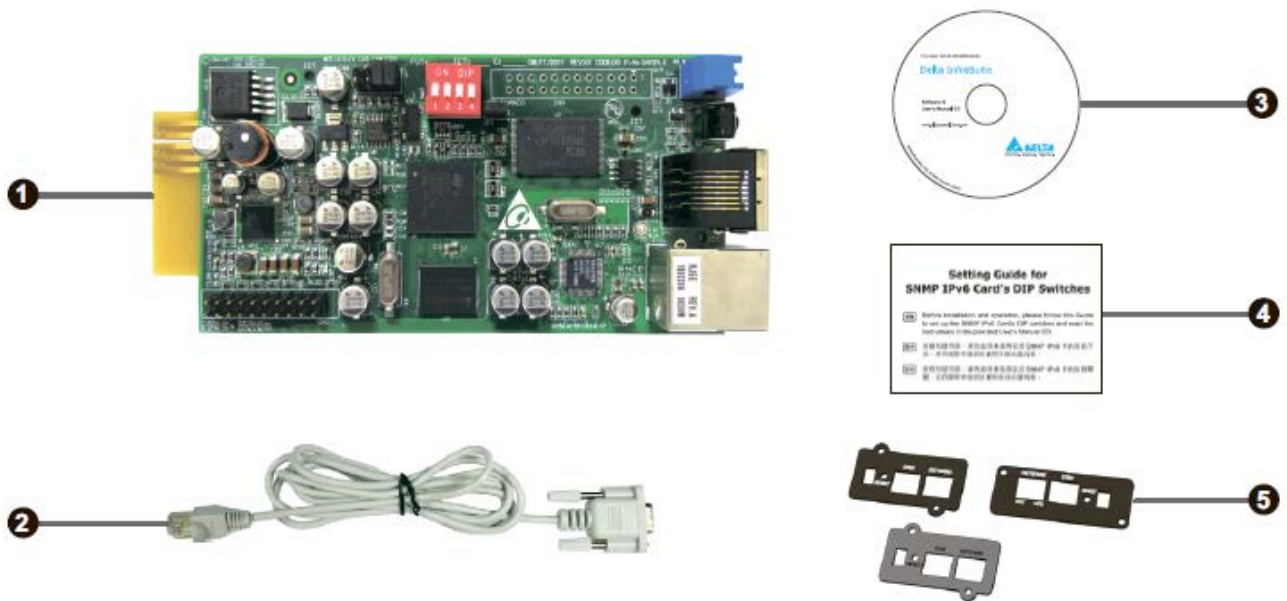
Другие функции и поддерживаемые протоколы:

- Извещение пользователя посредством SNMP ловушек и по электронной почте
- Сетевой протокол времени
- BOOTP/ DHCP

- Регистрационное имя и локальная аутентификация в RADIUS (Службе идентификации удаленных пользователей)
- Удаленное управление журналом событий системы

2-3 Комплект поставки

Внимательно проверьте модуль SNMP IPv6 и аксессуары в комплекте. Свяжитесь с местным дилером, если какой-либо компонент отсутствует или поврежден. В случае возврата любого компонента по любой причине, убедитесь, что они тщательно запакованы с использованием оригинальных упаковочных материалов.



№	Позиция	Кол-во
1	Модуль InsightPower SNMP IPv6 для ШРП	1 шт.
2	Кабель RJ45 - DB9	1 шт.
3	Компакт-диск с ПО и руководством по эксплуатации	1 шт.
4	Руководство по установке DIP-переключателей SNMP IPv6	1 шт.
5	Крышка	3 шт.

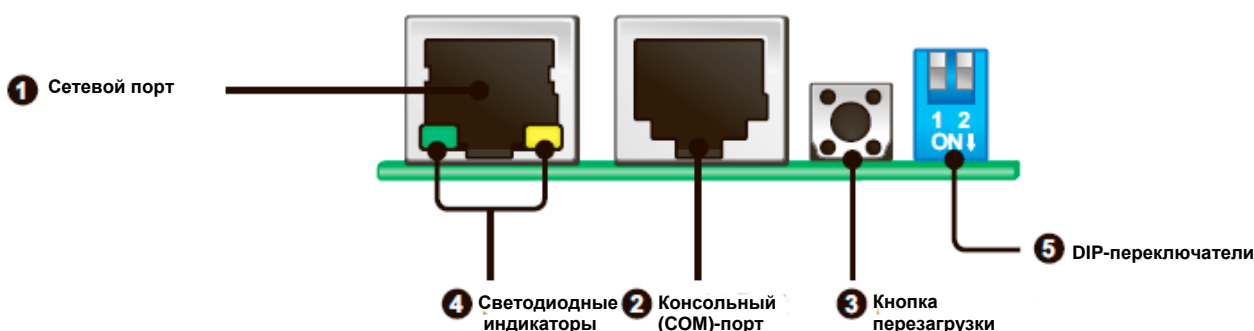
2-4 Устройства связи и управления

Модуль SNMP IPv6 оборудован сетевым портом, COM-портом, светодиодными индикаторами, кнопкой перезагрузки и DIP-переключателями. См. таблицу ниже.

Вид сверху:



Вид спереди:



№	Элемент	Описание
1	Сетевой порт	Для подключения к сети.
2	Консольный (COM)-порт	1. Подключение к рабочей станции через прилагающийся кабель RJ45 - DB9. 2. Подключение к датчику EnviroProbe (опция).
3	Кнопка перезагрузки	Перезагрузка SNMP IPv6. Перезагрузка не влияет на работу ШРП.

№	Элемент	Описание
---	---------	----------

4

Светодиодные индикаторы

Когда модуль SNMP IPv6 выполняет инициализацию или обновляет встроенное ПО, два светодиодных индикатора мигают одновременно, показывая состояние модуля. См. далее:

- **Быстрое одновременное мигание** (каждые 50 мс): выполняется инициализация или обновление встроенного ПО.
- **Медленное одновременное мигание** (каждые 500 мс): сбой инициализации.



ПРЕДУПРЕЖДЕНИЕ: ЗАПРЕЩАЕТСЯ снимать модуль SNMP IPv6 или отключать входное питание ШРП во время инициализации или обновления встроенного ПО! Это может привести к потере данных или повреждению модуля SNMP IPv6.

Зеленый светодиодный индикатор показывает состояние подключения к сети:





- **Горит:** сетевое подключение установлено, и адрес IPv4 можно использовать.
- **Не горит:** модуль не подключен к сети.
- **Медленно мигает** (каждые 500 мс): неверный IP адрес.

Желтый светодиодный индикатор показывает состояние соединения между SNMP IPv6 и ШРП:

- **Быстро мигает** (каждые 50 мс): есть соединение с ШРП.
- **Медленно мигает** (каждые 500 мс): соединения с ШРП нет.

№	Элемент	Описание
---	---------	----------

5 DIP-переключатели Настройка рабочих режимов

DIP-переключатели	Режим работы	Описание
	Нормальный режим	Модуль SNMP IPv6 соединяется с ШРП.
	Режим ретрансляции	Модуль SNMP IPv6 не контролирует ШРП, но использует его COM-порт для подключения ШРП к рабочей станции по протоколу Modbus (скорость передачи: 9600 бит/с).
	Режим поддержки датчика Enviro-Probe	Модуль SNMP IPv6 соединяется с ШРП и датчиком EnviroProbe.
	Режим настройки	Настройка модуля SNMP IPv6 через COM-порт. См. раздел 4-4 Настройка через COM-порт.

ПРИМЕЧАНИЕ

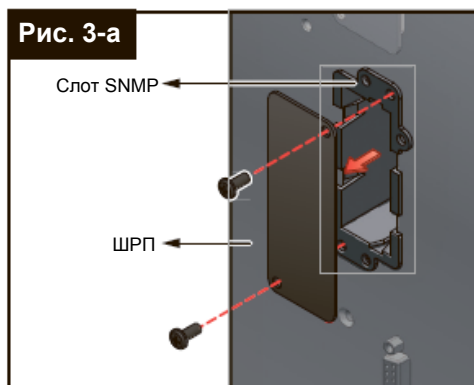


Чтобы узнать больше о датчике EnviroProbe, обратитесь к руководству пользователя этого устройства.

Глава 3 : Установка

- Для установки модуля SNMP IPv6, следуйте приведенным ниже инструкциям.

Шаг 1 Открутите два винта и снимите крышку слота SNMP.



ПРИМЕЧАНИЕ

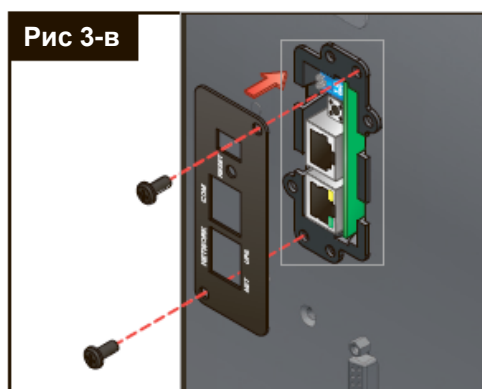


Расположение винтов может различаться в зависимости от моделей ШРП.

Шаг 2 Найдите направляющие в SNMP-слоте. Вставьте модуль SNMP IPv6 в слот SNMP.



Шаг 3 Из комплекта аксессуаров, выберите крышку с нужным расположением отверстий для винтов слота SNMP ШРП и прикрутите ее ранее снятыми винтами.



Глава 4 : Настройки системы

Существует несколько способов настройки SNMP IPv6. Если у вас есть доступ к сети, возможны следующие способы:

- **Настройка через веб-интерфейс:** Веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП (InsightPower SNMP IPv6 for PDC Web) предлагает комплексную систему управления и контроля. См. *Главу 5: Веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП*
- Настройка с помощью программы **EzSetting**: Используйте прилагаемую программу EzSetting для быстрой настройки модуля SNMP IPv6. См. раздел **4-2 Настройка с помощью программы EzSetting**.
- **Режим Telnet:** Настройте SNMP IPv6 в консольном режиме. См. раздел **4-3 Настройка через Telnet**.

Вышеуказанные способы требуют сетевого подключения. Если оно недоступно, используйте прямое соединение COM-порта для настройки модуля SNMP IPv6. См. раздел **4-4 Настройка через COM-порт**.

ПРИМЕЧАНИЕ

1. После первого входа в систему, настоятельно рекомендуется изменить учетную запись и пароль, чтобы обеспечить безопасность системы.
2. Если к вашей сети подключено несколько модулей SNMP IPv6, настоятельно рекомендуется изменить имя узла, присваиваемое модулю по умолчанию, чтобы избежать конфликта имен. Кроме того, рекомендуется отключить BOOTP/ DHCP и вручную назначить модулю SNMP IPv6 допустимый статический IP адрес.

4-1 Настройка через веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП

Для настройки SNMP IPv6 через веб-браузер, следуйте приведенным ниже инструкциям:

- Шаг 1** Подключите сетевой порт SNMP IPv6 к сети кабелем CAT5. Запустите веб-браузер. Введите в поле ввода адресов установленное по умолчанию имя узла **InsightPower** или IP адрес **192.168.1.100**. Если соединение не устанавливается, см. *Главу 7: Устранение неисправностей, Q6*.

ПРИМЕЧАНИЕ 

Если вы ранее изменили имя узла или IP адрес этого модуля, введите соответствующее имя или адрес.

- Шаг 2** Войдите в систему как администратор (учетная запись и пароль по умолчанию: admin/ password, с учетом регистра).
- Шаг 3** Выберите предпочтительный язык отображения (по умолчанию: английский) из выпадающего меню в верхней правой части страницы. SNMP IPv6 запомнит ваше языковое предпочтение. В дальнейших инструкциях считается, что выбран английский.
- Шаг 4** Щелкните пункты **System** → **Administration** → **User Manager**. Администрирование учетных записей и паролей выполняется через меню "Local Authentication". Предусмотрены следующие уровни доступа для разных типов учетных записей:
- 1) **Administrator** (Администратор): возможность изменения всех настроек.
 - 2) **Device Manager** (Менеджер устройства): возможность изменения настроек, относящихся к устройству.
 - 3) **Read Only User** (Пользователь с правом чтения): возможность просмотра установленных настроек без права вносить изменения.

Разрешение на доступ пользователей из других локальных сетей устанавливается вручную. Если необходимо заблокировать попытки входа через внешние соединения, установите настройку **Only in This LAN (Только в этой ЛВС)**. В противном случае установите настройку **Allow Any (Регистрация через внешние соединения разрешена)**.

- Шаг 5** Щелкните пункты **System** → **Administration** → **TCP/IP**, чтобы задать имя узла (Host Name), IP адрес (IP address), маску подсети (Subnet Mask) и IP адрес шлюза (Gateway IP) для модуля SNMP IPv6.
- Шаг 6** Щелкните **Time Server**, чтобы вручную задать системное время и дату или разрешить автоматическую синхронизацию SNMP IPv6 с сервером времени.

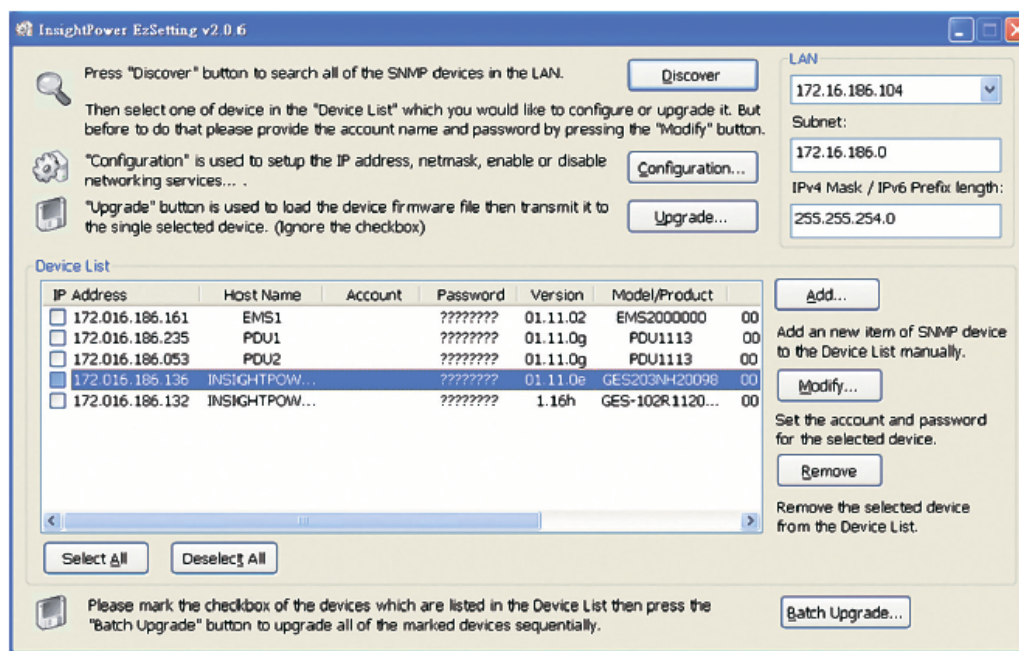
ПРИМЕЧАНИЕ 

Для завершения настройки модуля см. **Главу 5: Веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП**

4-2 Настройка с помощью EzSetting

Использование программы EzSetting (совместима с Windows 2000/ 2003/ 2008/ XP/ Vista/ 7), записанной на прилагающемся компакт-диске – это один из простых способов настроить модуль SNMP IPv6 и обновить встроенное ПО на устройствах SNMP. Следуйте указаниям, приведенным ниже:

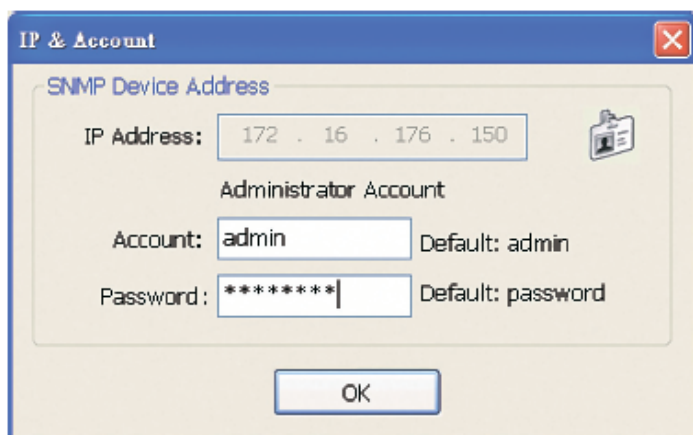
- Шаг 1** Подключите сетевой порт SNMP IPv6 к сети кабелем CAT5.
- Шаг 2** Убедитесь, что оба DIP-переключателя SNMP IPv6 установлены в положение OFF (нормальный режим), чтобы разрешить связь с сетью. Убедитесь, что рабочая станция и модуль SNMP IPv6 подключены к одной и той же локальной сети.
- Шаг 3** Вставьте прилагающийся компакт-диск в дисковод. Запустите программу EzSetting из корневого каталога.
- Шаг 4** Щелкните команду Discover (найти), чтобы найти все доступные SNMP-устройства в данной локальной сети. На экране появится список устройств.



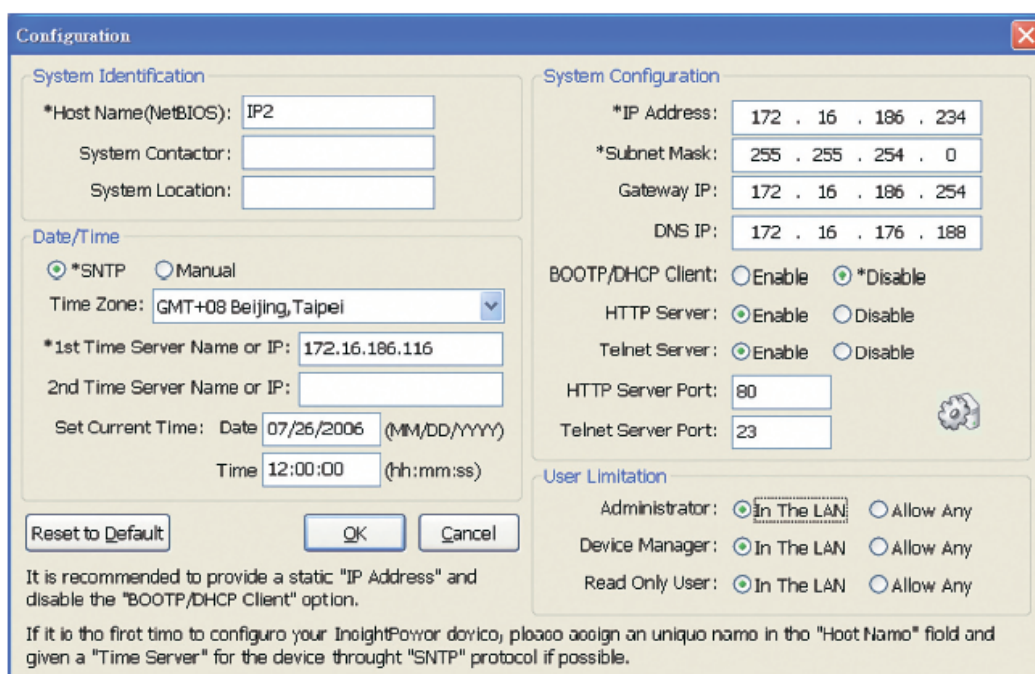
ПРИМЕЧАНИЕ

1. Если вы хотите найти SNMP-устройства в других доменах, измените **Subnet** (название подсети) и **IPv4/ IPv6 Prefix Length (длину префикса)** и затем щелкните **Discover(найти)**.
2. Если найти нужный модуль SNMP IPv6 не удастся, проверьте сетевой порт UDP 3456 на вашей рабочей станции. Убедитесь, что он открыт.

- Шаг 5** Выберите в Device List (списке устройств) модуль SNMP IPv6, настройки которого вы хотите изменить. Щелкните **Modify** (изменить), чтобы ввести свою учетную запись администратора и пароль (по умолчанию: admin/password, с учетом регистра).



Шаг 6 Щелкните **Configuration** (Настройка) и задайте необходимые сетевые параметры.



ПРИМЕЧАНИЕ

См. *Главу 5: Веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП* для всех настроек.

4-3 Настройка через Telnet

- Шаг 1** Подключите сетевой порт SNMP IPv6 к сети кабелем CAT5.
- Шаг 2** Подключите рабочую станцию (Windows или Linux) к той же локальной сети, к которой подключен SNMP IPv6.
- Шаг 3** Для Windows, запустите режим командной строки DOS (**Start** → **Run** → набрать **cmd** и нажать **Enter**). В случае ОС Linux запустите консоль.

- Шаг 4** Введите команду: **telnet InsightPower** или **telnet IP address**, чтобы инициировать telnet-соединение с модулем SNMP IPv6.
- Шаг 5** Когда соединение установлено, введите учетную запись администратора и пароль (по умолчанию: admin/ password, с учетом регистра). На экране откроется главное меню. Подробнее см. раздел **4-5 Настройка в консольном режиме**.

ПРИМЕЧАНИЕ

1. SNMP IPv6 автоматически разрывает неиспользуемое соединение через 60 секунд.
2. См. **Главу 5. Веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП** для всех настроек.

4-4 Настройка через COM-порт

Если сетевое соединение вам недоступно, настройки модуля SNMP IPv6 можно ввести через COM-порт. Следуйте приведенным ниже инструкциям:

ПРИМЕЧАНИЕ

Если ваша станция использует не Windows, а иную операционную систему, найдите в руководстве пользователя вашей ОС инструкции для клиента Telnet.

- Шаг 1** Подключите COM-порт SNMP IPv6 к COM-порту рабочей станции прилагающимся кабелем RJ45 - DB9.
- Шаг 2** Убедитесь, что оба DIP-переключателя SNMP IPv6 установлены в положение **OFF** (нормальный режим).
- Шаг 3** Для Windows 2000, 2003, 2008 и XP перейдите в меню **Start** → **Programs** → **Accessories** → **Communications** и выберите **HyperTerminal**.

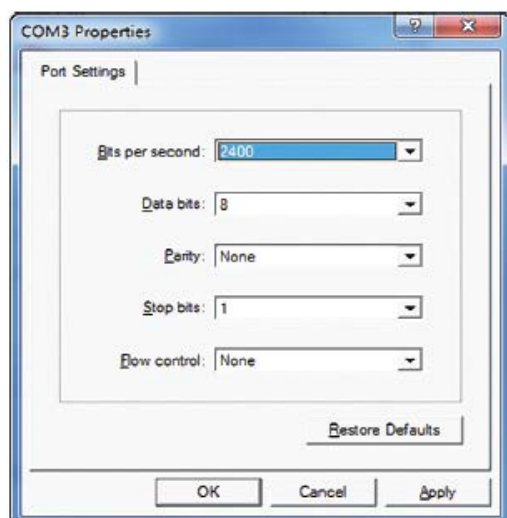
ПРИМЕЧАНИЕ

В Windows Vista и более поздних версиях программа HyperTerminal была удалена корпорацией Microsoft.
Если ваша операционная система не включает данную программу, то есть бесплатный вариант
Telnet/SSH client PuTTY можно загрузить с <http://www.putty.org>.

Шаг 4 Введите имя, выберите иконку для соединения и нажмите **ОК**. В выпадающем меню **Connect using** выберите COM-порт, к которому подключен модуль SNMP IPv6.



Шаг 5 Щелкните **Configure** и задайте параметры COM-порта, как показано ниже:



Шаг 6 Нажмите **ОК** для продолжения. Установите оба DIP-переключателя модуля SNMP IPv6 в положение **ON** (режим настройки). HyperTerminal автоматически выполнит соединение с SNMP IPv6. Если соединение не устанавливается, щелкните иконку с изображением телефона на панели инструментов. Когда соединение установлено, введите учетную запись администратора и пароль (по умолчанию: admin/password, с учетом регистра). После регистрации, на экране появится главное меню. Подробнее см. раздел **4-5 Настройка в консольном режиме**.

4-5 Настройка в консольном режиме

SNMP IPv6 можно настраивать в консольном режиме с помощью Telnet/ SSH клиентов, таких как HyperTerminal и PuTTY. В настоящем разделе приводится описание и значение по умолчанию для каждой из настроек.

Главное меню (Main Menu)

```
+-----+
|      Main Menu      |
+-----+
Web Card Version 01.00.00
MAC Address 00-30-ab-25-e9-1e
[1].User Manager
[2].TCP/IP Setting
[3].Network Parameter
[4].Time Server
[5].Soft Restart
[6].Reset All To Default
[z].Exit Without Save
[0].Save And Exit

Please Enter Your Choice =>
```

Меню User Manager

```
+-----+
|      User Manager   |
+-----+
RADIUS
[1].RADIUS Auth: Disable
[2].Server:
[3].Secret:
[4].Port:          1812
-----
Local Auth
  Administrator
[5].Account:      admin
[6].Password:     *****
[7].Limitation:  Only in This LAN
  Device Manager
[8].Account:      device
[9].Password:     *****
[a].Limitation:  Only in This LAN
  Read Only User
[b].Account:      user
[c].Password:     *****
[d].Limitation:  Allow Any
[0].Back To Previous Menu

Please Enter Your Choice =>
```

№	Элемент	Описание	По умолчанию
[1]	RADIUS Auth	Разрешение аутентификации по протоколу RADIUS	Disable (запрещен)
[2]	Server	Имя RADIUS-сервера	

№	Элемент	Описание	По умолчанию
[3]	Secret	Секретный ключ для RADIUS	
[4]	Port	Номер порта RADIUS	1812
[5]	Administrator Account	Принимаемые по умолчанию учетная запись и пароль администратора (с учетом регистра)	admin
[6]	Administrator Password		password
[7]	Administrator Limitation	Ограничение зоны действия учетной записи администратора.	Only in This LAN (только в данной ЛВС)
[8]	Device Manager Account	Принимаемые по умолчанию учетная запись и пароль (с учетом регистра) менеджера устройства (Device Manager). Данная учетная запись позволяет менять только настройки, относящиеся к данному устройству.	device
[9]	Device Manager Password		password
[a]	Device Manager Limitation	Ограничение зоны действия учетной записи менеджера устройства.	Only in This LAN (только в данной ЛВС)
[b]	Read Only User Account	Принимаемые по умолчанию учетная запись и пароль (с учетом регистра) пользователя с правом чтения. Данная учетная запись дает возможность просмотра установленных настроек без права вносить изменения.	user
[c]	Read Only User Password		password
[d]	Read Only User Limitation	Ограничение зоны действия учетной записи пользователя с правом чтения.	Allow Any (регистрация через внешние соединения разрешена)



TCP/IP Setting (Настройки TCP/IP)

```
+-----+
| TCP/IP Setting |
+-----+

[1].IPv4 Address:      192.168.001.100
[2].IPv4 Subnet Mask: 255.255.255.000
[3].IPv4 Gateway IP:  192.168.001.254
[4].IPv4 DNS or WINS IP:192.168.001.001
[5].DHCPv4 Client:    Enable
[6].IPv6 Address:     fe80::230:abff:fe25:900
[7].IPv6 Prefix Length: 64
[8].IPv6 Gateway IP:  ::
[9].IPv6 DNS IP:      ::
[a].DHCPv6:           Enable
[b].Host Name (NetBIOS): INSIGHTPOWER
[c].System Contact:
[d].System Location:
[e].Auto-Negotiation: Enable
[f].Speed:            100M
[g].Duplex:           Full
[i].Telnet Idle Time: 60 Seconds
[0].Back To Previous Menu

Please Enter Your Choice =>
```

№	Элемент	Описание	По умолчанию
[1]	IPv4 Address	Адрес IPv4.	192.168.001.100
[2]	IPv4 Subnet Mask	Настройка маски подсети IPv4	255.255.255.000
[3]	IPv4 Gateway IP	IP сетевого шлюза IPv4	192.168.001.254
[4]	IPv4 DNS или WINS IP	IP сервера доменных имен IPv4 или WINS.	192.168.001.001
[5]	DHCPv4 Client	Разрешение/запрет протокола DHCPv4.	Enable (разрешен)
[6]	IPv6 Address	Адрес IPv6.	
[7]	IPv6 Prefix Length	Длина префикса IPv6.	
[8]	IPv6 Gateway IP	IP адрес сетевого шлюза IPv6.	
[9]	IPv6 DNS IP	IP адрес сервера доменных имен IPv6.	
[a]	DHCPv6	Разрешение/запрет протокола DHCPv6.	Enable (разрешен)

№	Элемент	Описание	По умолчанию
[b]	Host Name (NetBIOS)	Имя узла для SNMP IPv6.	INSIGHTPOWER
[c]	System Contact	Информация о контактном лице системы.	
[d]	System Location	Информация о местоположении системы.	
[e]	Auto-Negotiation	Автоматическое согласование скорости передачи (10 / 100 Мб/с) разрешено/запрещено	Enable (разрешен)
[f]		Если автоматическое согласование (Auto-Negotiation) запрещено, можно задать скорость передачи.	100M
[g]		Если автоматическое согласование запрещено, можно задать дуплексный режим.	Full (полный дуплекс)
[i]		Установка времени таймаута Telnet.	60 секунд



Network Parameter (Параметры сети)

```

+-----+
| Network Parameter |
+-----+
[1].HTTP Server:      Enable
[2].HTTPS Server:     Enable
[3].Telnet Server:    Enable
[4].SSH/SFTP Server:  Enable
[5].FTP Server:       Disable
[6].Syslog:           Disable
[7].HTTP Server Port: 80
[8].HTTPS Server Port: 443
[9].Telnet Server Port: 23
[a].SSH Server Port:  22
[b].FTP Server Port:  21
[c].Syslog Server1:
[d].Syslog Server2:
[e].Syslog Server3:
[f].Syslog Server4:
[g].SNMP Get,Set Port: 161
[0].Back To Previous Menu

Please Enter Your Choice =>

```

№	Элемент	Описание	По умолчанию
[1]	HTTP Server	Разрешение/запрет протокола HTTP.	Enable (разрешен)
[2]	HTTPS Server	Разрешение/запрет протокола HTTPS.	Enable (разрешен)
[3]	Telnet Server	Разрешение/запрет протокола Telnet.	Enable (разрешен)
[4]	SSH/ SFTP Server	Разрешение/запрет протоколов SSH/ SFTP.	Enable (разрешен)
[5]	FTP Server	Разрешение/запрет протокола FTP.	Disable (запрещен)
[6]	Syslog	Разрешение/запрет дистанционного управления системным журналом.	Disable (запрещен)
[7]	HTTP Server Port	Сетевой порт HTTP.	80
[8]	HTTPS Server Port	Сетевой порт HTTPS.	443
[9]	Telnet Server Port	Сетевой порт Telnet.	23
[a]	SSH Server Port	Сетевой порт SSH.	22
[b]	FTP Server Port	Сетевой порт FTP.	21
[c]	Syslog Server 1	Имя хоста удаленного системного журнала сервера 1.	
[d]	Syslog Server 2	Имя хоста удаленного системного журнала сервера 2.	

№	Элемент	Описание	По умолчанию
[e]	Syslog Server 3	Имя хоста удаленного системного журнала сервера 3.	
[f]	Syslog Server 4	Имя хоста удаленного системного журнала сервера 4.	
[g]	SNMP Get, Set Port	Сетевой порт SNMP.	161

Time Server (Сервер времени)

Вы можете вручную задать для SNMP IPv6 системное время и дату или разрешить автоматическую синхронизацию с сервером времени. SNMP IPv6, Windows XP и более поздние версии поддерживают протокол SNTP (простой протокол сетевого времени). Если на вашей рабочей станции нужно запустить службу сервера времени, обратитесь к **Главе 7: Устранение неисправностей, Q1**.

```

+-----+
|   Time Server   |
+-----+
[1].Time Selection:   SNTP
[2].Time Zone:       +0 hr
[3].1st Time Server: POOL.NTP.ORG
[4].2nd Time Server:
[5].Manual Date:     01/01/2000 (MM/DD/YYYY)
[6].Manual Time:     00:00:00 (hh:mm:ss)
[0].Back To Previous Menu

Please Enter Your Choice =>

```

№	Элемент	Описание	По умолчанию
[1]	Time Selection	Настройка времени – SNTP или ручная	SNTP
[2]	Time Zone	Выбор часового пояса	+0 hr (ч)
[3]	1 st Time Server	Первый сервер времени для SNTP	POOL.NTP.ORG
[4]	2 nd Time Server	Второй сервер времени для SNTP	
[5]	Manual Date	Ручная установка даты	01/01/2000
[6]	Manual Time	Ручная установка времени.	00:00:00

Soft Restart (Мягкая перезагрузка)

Перезагрузка SNMP IPv6. Это не повлияет на работу ШРП.

Default Reset

Загрузка заводских настроек.



Exit Without Saving

Выход без сохранения изменений.



Save and Exit

Выход с сохранением изменений.

Глава 5 : Веб-интерфейс модуля InsightPower SNMP IPv6 для ШРП

Для настройки модуля SNMP IPv6 через веб-интерфейс InsightPower SNMP IPv6 for PDC Web, следуйте приведенным ниже шагам:


- Шаг 1** Убедитесь, что SNMP IPv6 подключен к локальной сети. Подключите сетевой порт SNMP IPv6 к сети кабелем CAT5.
- Шаг 2** Запустите веб-браузер. Введите в поле ввода адресов имя узла SNMP IPv6 **http://InsightPower/** или **IP адрес**. Для шифрованного соединения введите **https://InsightPower/** или **https://192.168.1.100/**.
- Шаг 3** После установления соединения, открывается страница входа в систему. Введите вашу учетную запись и пароль (по умолчанию: admin/ password).



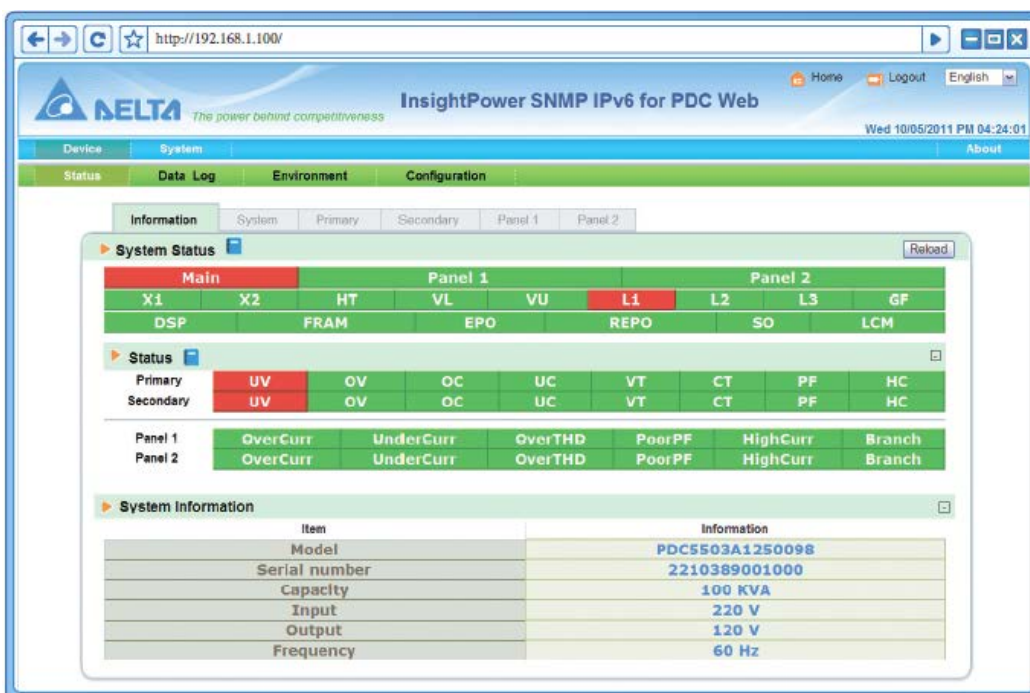
ПРИМЕЧАНИЕ

1. Если вы ранее изменили имя узла или IP адрес этого модуля, введите соответствующее имя или адрес.
2. Если страница входа в систему открывается, но войти не удастся, несмотря на ввод верной учетной записи и пароля, необходимо изменить дополнительные настройки сети. Причина может быть в том, что ваш компьютер и модуль SNMP IPv6 зарегистрированы в разных подсетях. Для решения проблемы см. **Главу 7: Устранение неисправностей, Q3**.
3. SNMP IPv6 автоматически разрывает неиспользуемое соединение через 30 минут.

5-1 Device (устройство)

На этой странице проверьте состояние и параметры системы ШРП. Эта страница автоматически обновляется каждые 10 секунд. Нажмите **Reload** для обновления вручную. При щелчке на иконку  отображается боковое выдвижное окно, которое предоставляет дополнительные сведения. Нажмите **Close** - боковое выдвижное окно исчезнет.

Для изменения параметра, выберите из выпадающего меню или просто щелкните элемент. Введите новое значение в текстовом поле и нажмите **Submit** для активации.



The screenshot shows a web browser window with the URL <http://192.168.1.100/>. The page title is "InsightPower SNMP IPv6 for PDC Web". The interface includes a navigation menu with "Device", "System", "Status", "Data Log", "Environment", and "Configuration". The "System Status" section is expanded, showing a table with columns for Main, Panel 1, and Panel 2. The "Status" section shows a table with columns for Primary and Secondary, and a "System Information" table with columns for Item and Information.

Main		Panel 1				Panel 2			
X1	X2	HT	VL	VU	L1	L2	L3	GF	
DSP	FRAM	EPO	REPO	SO	LCM				

Primary	UV	OV	OC	UC	VT	CT	PF	HC
Secondary	UV	OV	OC	UC	VT	CT	PF	HC

Panel 1	OverCurr	UnderCurr	OverTHD	PoorPF	HighCurr	Branch
Panel 2	OverCurr	UnderCurr	OverTHD	PoorPF	HighCurr	Branch

Item	Information
Model	PDC5503A1250098
Serial number	2210389001000
Capacity	100 KVA
Input	220 V
Output	120 V
Frequency	60 Hz

5-1-1 Status (Состояние)

Main		Panel 1				Panel 2			
X1	X2	HT	VL	VU	L1	L2	L3	GF	
DSP	FRAM	EPO	REPO	SO	LCM				

Красный и зеленый флажки показывают состояние ШРП. Зеленый флажок указывает на нормальную работу. Красный флажок означает, что произошло предупреждающее событие. В следующей таблице приведены флажки и предупреждающие события, которые они обозначают:

Флажок	Описание	Флажок	Описание
Main	Произошло предупреждающее событие главного автоматического выключателя.	Panel #	Произошло предупреждающее событие автоматического выключателя панели №...
X1/ X2	X1: Температура трансформатора превышает 125°C. X2: Температура трансформатора превышает 150°C.	HT	Слишком высокая температура окружающей среды.
VL	Фаза напряжения отсутствует.	VU	Дисбаланс напряжения.
L1 / L2 / L3	Частота вне диапазона.	GF	Неисправность заземления.
DSP	Ошибка связи CAN DSP.	FRAM	Ошибка чтения/записи FRAM.
EPO	Инициировано аварийное отключение питания.	REPO	Инициировано дистанционное аварийное отключение питания.
SO	Перегрузка системы.	LCM	Ошибка связи CAN LCM.
UV	Пониженное напряжение.	OV	Повышенное напряжение.
OC	Сверхток.	UC	Недостаточная сила тока.
VT	Перенапряжение THD (коэффициента искажения синусоидальности кривой напряжения).	CT	Сверхток THD (коэффициента искажения синусоидальности кривой тока).
PF	Плохой коэффициент мощности.	HC	Высокий ток.

Information (Информация)

На этой странице отображается краткий обзор состояния ШРП и системная информация, включая модель, серийный номер, мощность, входное/выходное напряжение и частоту.

The screenshot displays the web interface for the InsightPower SNMP IPv6 for PDC Web. The browser address bar shows <http://192.168.1.100/>. The page title is "InsightPower SNMP IPv6 for PDC Web". The navigation menu includes "Device", "System", "Status", "Data Log", "Environment", and "Configuration". The "System" tab is active, and the "Information" sub-tab is selected. The "System Status" section shows a table with columns for Main, Panel 1, and Panel 2, and rows for X1, X2, HT, VL, VU, L1, L2, L3, GF, DSP, FRAM, EPO, REPO, SO, and LCM. The "Status" section shows a table with columns for UV, OV, OC, UC, VT, CT, PF, and HC, and rows for Primary and Secondary. The "System Information" section shows a table with columns for Item and Information, and rows for Model, Serial number, Capacity, Input, Output, and Frequency.

Item	Information
Model	PDC5503A1250098
Serial number	2210389001000
Capacity	100 KVA
Input	220 V
Output	120 V
Frequency	60 Hz

System (Система)

На этой странице можно проверить состояние ШРП, статистику и параметры. 4-часовая статистика показывает сетевые данные, записанные в течение последних 4-х часов.

Для изменения параметра, просто щелкните на него или выберите из выпадающего меню внизу страницы. Не забудьте нажать **Submit**, чтобы изменения вступили в силу.

The screenshot shows the web interface for the InsightPower SNMP IPv6 for PDC Web. The browser address bar shows the URL http://192.168.1.100/. The page title is "InsightPower SNMP IPv6 for PDC Web". The navigation menu includes "Device", "System", "Status", "Data Log", "Environment", and "Configuration". The "System" tab is selected, and the "Status" sub-tab is active. The main content area displays the following information:

Status

Main	Panel 1			Panel 2				
X1	X2	HT	VL	VU	L1	L2	L3	GF
DSP		FRAM	EPO	REPO		SO		LCM

Parameter

Name	Value
Ambient Temperature	27.3
Total Ground Current	0.0

4 Hour Statistics

Name	Value	L1	L2	L3	Neutral
Max Voltage		222.1	222.4	223.0	
Min Voltage		219.3	219.3	220.0	
Max Current		134.7	260.9	269.8	0.0
Min Current		2.1	3.0	2.4	0.0
Max Frequency	60.0				
Min Frequency	0.3				
Max KW	8.0				
Min KW	0.4				

System Setting

Name	Value
LCD Contrast	1
Upper Ambient Temperature	40.0
Upper Ground Current	5.0

At the bottom of the settings section, there is a dropdown menu with the text "- select one -", a text input field labeled "New Value", and a "Submit" button.

Primary (Первичные данные)

На этой странице отображаются входные данные и параметры ШРП. Можно изменить пороговые параметры в нижней части страницы.

The screenshot shows a web browser window displaying the 'InsightPower SNMP IPv6 for PDC Web' interface. The browser address bar shows 'http://192.168.1.100/'. The page header includes the DELTA logo and the slogan 'The power behind competitiveness'. The navigation menu includes 'Device', 'System', 'Status', 'Data Log', 'Environment', and 'Configuration'. The 'Status' section is active, and the 'Primary' tab is selected. The 'Status' section has a 'Reload' button and a 'UV' tab selected. Below the tabs, there are two tables: 'Parameter' and 'Threshold'.

Name	Value	L1	L2	L3	Neutral
L-L Voltage		0.0	0.0	0.0	
L-N Voltage		0.0	0.0	0.0	
Current		0.0	0.0	0.0	0.0
KWH	0.2				
KVA	0.0				
KW	0.0				
Voltage THD		0.0	0.0	0.0	
Current THD		0.0	0.0	0.0	
Load %		0.0	0.0	0.0	

Name	Value	Neutral
Under Voltage	191.4	
Over Voltage	242.0	
Over Current	113.2	151.0
Under Current	0.0	
Current THD	0.0	

At the bottom of the threshold table, there are input fields for 'Value' and 'Neutral', a dropdown menu, and a 'Submit' button. A note below reads: '* Please keep the field empty if you don't want to assign a new value'.

Secondary (Вторичные данные)

На этой странице отображаются выходные данные и параметры ШРП. Можно изменить пороговые параметры в нижней части страницы.

The screenshot shows the web interface for the Delta InsightPower SNMP IPv6 for PDC Web. The page is titled "Secondary" and displays the following data:

Status

UV	OV	OC	UC	VT	CT	PF	HC

Parameter

Name	Value	L1	L2	L3	Neutral
L-L Voltage		0.0	0.0	0.0	
L-N Voltage		0.0	0.0	0.0	
Current		0.0	0.0	0.0	0.0
KWH		0.0	0.0	0.0	
KVA		0.0	0.0	0.0	
KW		0.0	0.0	0.0	
Power Factor		0.00	0.00	0.00	
Voltage THD		0.0	0.0	0.0	
Current THD		0.0	0.0	0.0	
Load %		0.0	0.0	0.0	
Freq	0.0				

Threshold

Name	Value	Neutral
Under Voltage	104.4	
Over Voltage	132.0	
Over Current	221.6	277.0
Under Current	0.0	
Power Factor	0.00	
Voltage THD	0.0	
Current THD	0.0	

At the bottom of the threshold table, there are input fields for "Value" and "Neutral" with a "Submit" button. A note below reads: "* Please keep the field empty if you don't want to assign a new value".



Panel (Панель управления)

Количество панелей и распределительных сетей может различаться в зависимости от конфигураций ШРП. На этой странице можно проверить данные и состояние панели управления. Для изменения параметра, просто щелкните на него или выберите из выпадающего меню внизу страницы. Не забудьте нажать **Submit**, чтобы изменения вступили в силу.

The screenshot shows the 'Panel 1' configuration page. It features a navigation bar with 'Status', 'Data Log', 'Environment', and 'Configuration'. The main content area is divided into several sections:

- Status Overview:** A table with columns for OverCurr, UnderCurr, OverTHD, PoorPF, HighCurr, and Branch.
- Parameter Table:** A table with columns for Name, L1, L2, L3, and Neutral. Parameters include Current, KWH, KVA, KW, Power Factor, Current THD, and Load %.
- Threshold Table:** A table with columns for Name, Value, and Neutral. Thresholds include Over Current, Under Current, Power Factor, and Current THD.
- Branch Demand Table:** A table with columns for Branch, RMS, Min, Max, Load, KW, KWH, Under, and Over. It lists data for 7 branches.

At the bottom, there are input fields for 'Value' and 'Neutral', a 'Submit' button, and a note: '* Please keep the field empty if you don't want to assign a new value'.

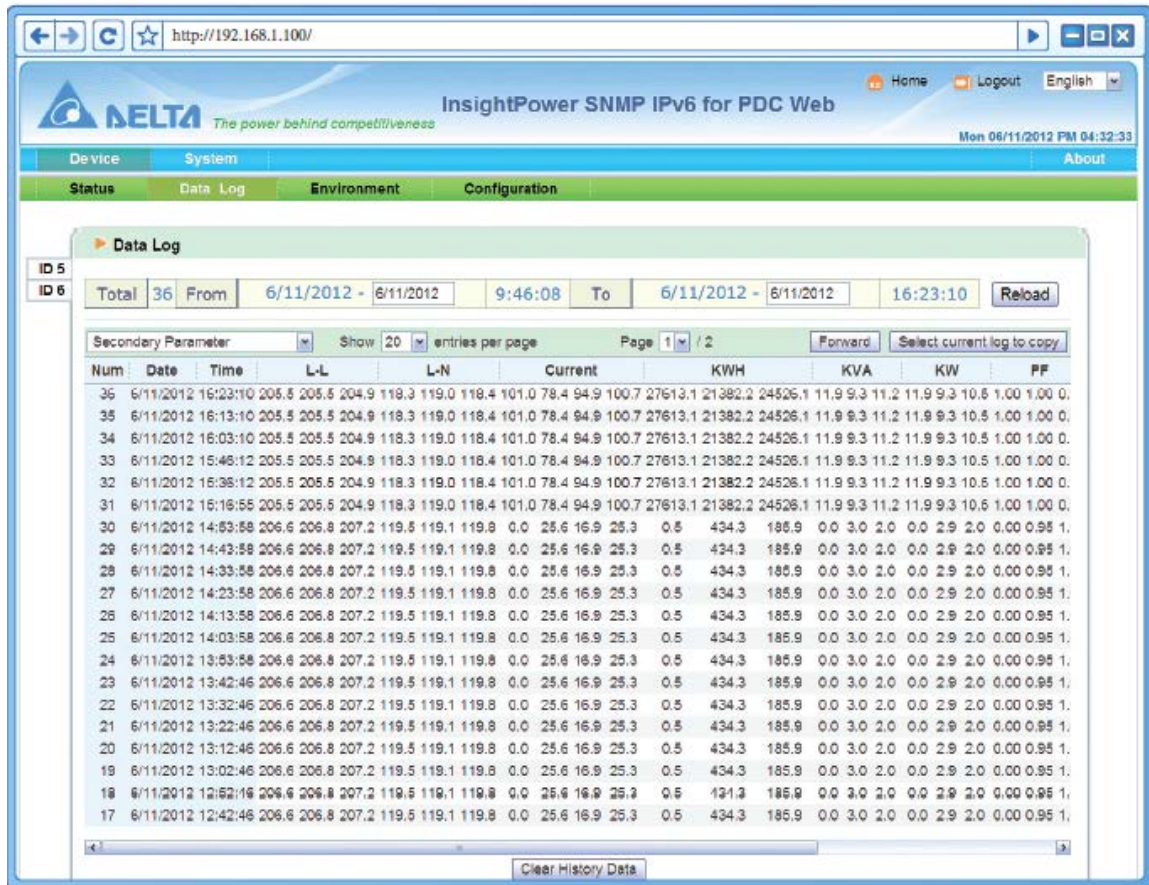
5-1-2 Data Log (Журнал данных)

Наведите курсор на данные для получения подробной информации. Общее число записей журнала отображается в верхней левой части страницы.

Можно определить период времени для отображения записей, записанных в течение указанного времени. Щелкните на дату, чтобы вывести всплывающее окно и указать дату. Щелкните **Click Clear History Data**, чтобы очистить все сохраненные записи (для всех идентификационных меток).

Чтобы проверить конкретный тип ввода данных, выберите тип из выпадающего меню, укажите количество записей для отображения на каждой странице и нажмите **Reload**.

Нажмите **Forward/ Backward**, чтобы выбрать порядок отображения перечисленных журналов данных. Чтобы скопировать все записи данных в таблицу Excel, нажмите **Select current log** для копирования. Нажмите клавиши **CTRL + C** для копирования. Нажмите клавиши **CTRL + V** для вставки в Excel.

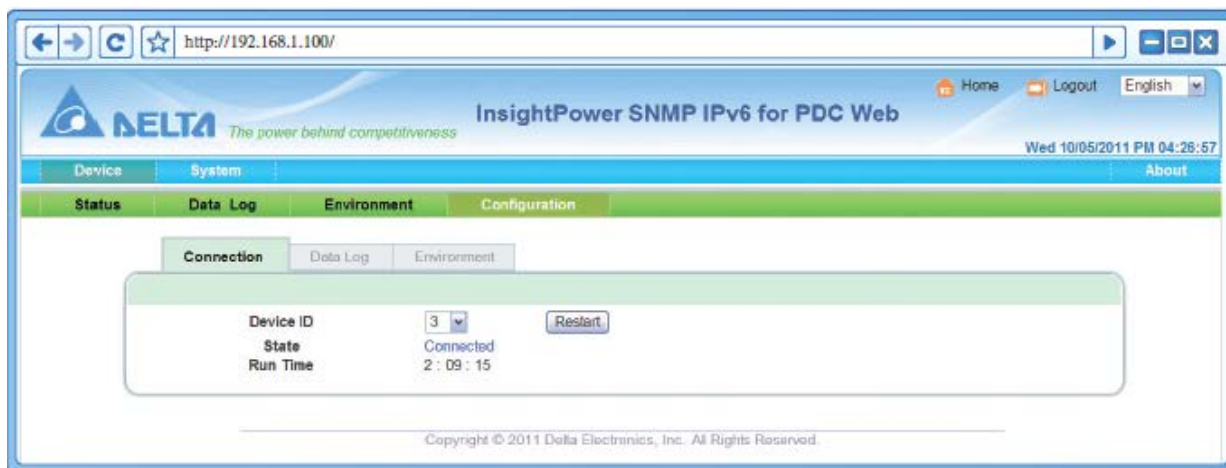


5-1-3 Environment (Условия окружающей среды)

Эта страница появляется только при подключении датчика EnviroProbe. Можно проверить значения температуры/влажности и статус входных контактов.



5-1-4 Configuration (Конфигурация)



Connection (Связь)

По умолчанию, ШРП имеет идентификатор устройства 1, который также является идентификатором, назначенным в протоколе Modbus. Для соединения ШРП с модулем SNMP IPv6, параметр идентификатора данного устройства должен совпадать. Выберите идентификатор устройства ШРП и нажмите **Restart**.

Data Log (Журнал данных)

Укажите частоту сохранения данных для журнала данных. Система автоматически сохраняет данные по истечении указанного времени. Нажмите **Apply** для вступления в силу.

Environment (Условия окружающей среды)

Эта страница появляется только при подключении датчика EnviroProbe. Установите пороговые значения предупреждений и оповещений. Присвойте названия входным контактам и выберите их типы соответственно. Нажмите **Submit** для вступления в силу.

5-2 System (Система)

Проверьте или измените настройки системы на следующих страницах.

5-2-1 Administration (Администрирование)

● Меню User Manager

SNMP IPv6 поддерживает протокол RADIUS. Укажите сервер, секретный ключ и порт (по умолчанию: 1812). Проверьте **User RADIUS** и нажмите **Submit** для активации. Проверьте определенные типы служб для администратора (Administrator), диспетчера устройств (Device Manager) и пользователя только для чтения (Read Only User). Если RADIUS отключен, будет использоваться локальная проверка подлинности. Укажите имя учетной записи, пароль и ограничение входа для отдельных учетных записей.

The screenshot displays the 'User Manager' configuration page in the InsightPower SNMP IPv6 for PDC Web interface. The page is titled 'System » Administration » User Manager' and includes a navigation menu on the left with options like TCP/IP, Web, Console, FTP, IIRIS SERVER, Syslog, and Device Configuration. The main content area is divided into several sections:

- Use RADIUS:** A checkbox labeled 'Use RADIUS' is currently unchecked. Below it are input fields for 'Server (51 chars max.)', 'Secret (32 chars max.)', and 'Port' (set to 1812).
- RFC2865 Service Type:** This section is divided into three columns: Administrator, Device Manager, and Read Only User. Each column contains a list of service types with checkboxes, such as 'Login User', 'Framed User', 'Callback Login', 'Callback Framed', 'Outbound', 'Administrative', 'NAS Prompt', 'Authenticate Only', 'Callback NAS Prompt', 'Call Check', and 'Callback Administrative'.
- Local Authentication:** This section contains a table for configuring local users. The table has four columns: 'Privilege', 'Account Name (16 chars max.)', 'Password (16 chars max.)', and 'Login Limitation'.

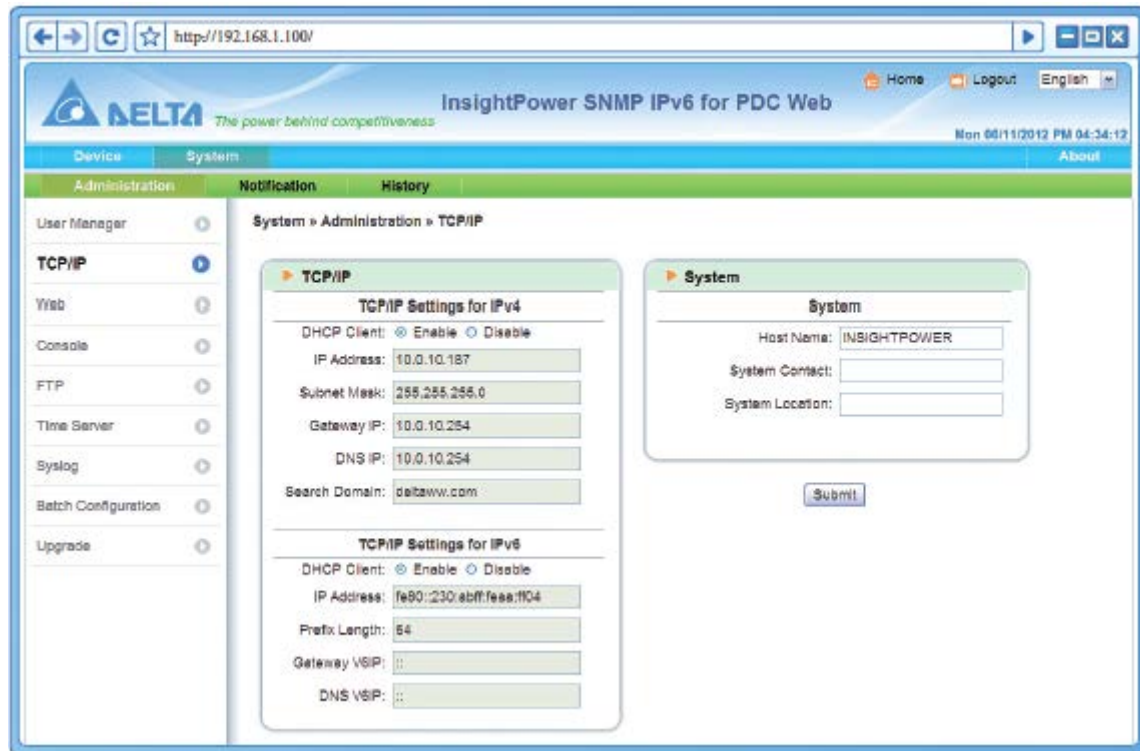
Privilege	Account Name (16 chars max.)	Password (16 chars max.)	Login Limitation
Administrator	admin	*****	<input type="radio"/> Only in This LAN <input checked="" type="radio"/> Allow Any
Device Manager	device	*****	<input type="radio"/> Only in This LAN <input checked="" type="radio"/> Allow Any
Read Only User	user	*****	<input type="radio"/> Only in This LAN <input checked="" type="radio"/> Allow Any

A 'Submit' button is located at the bottom of the Local Authentication section.



TCP/IP

Настройка параметров протокола TCP/IP осуществляется на этой странице.



- **Параметры TCP/IP IPv4 для IPv4**

Укажите IP-адрес IPv4, маску подсети, IP-шлюз, DNS-IP и домен поиска. Если протокол DHCP IPv4 включен, DHCP-сервер автоматически назначает IP-адрес SNMP IPv6. В том случае, если введенное имя узла не найдено, система добавляет домен поиска к имени узла.

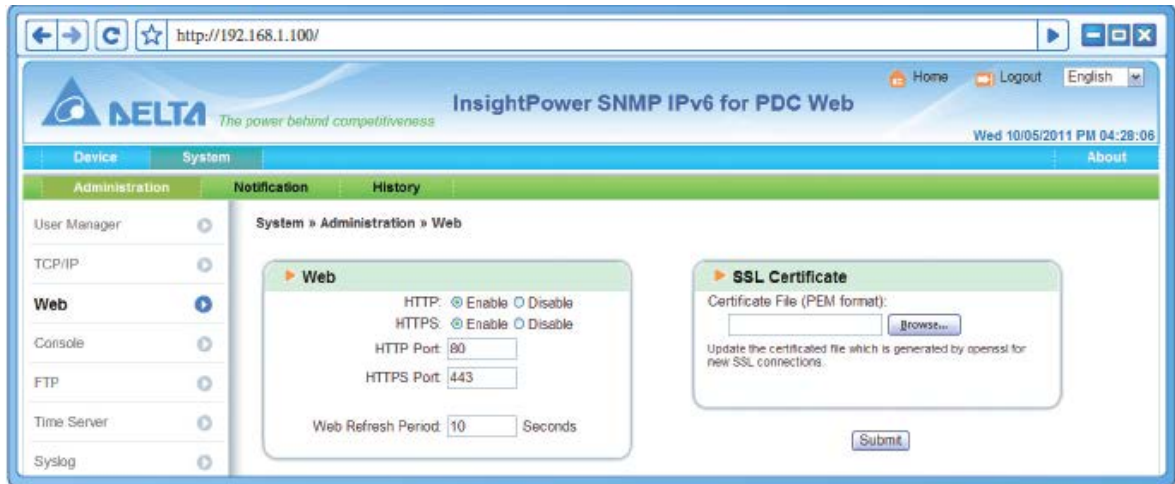
- **Параметры TCP/IP IPv4 для IPv6**

Укажите IP-адрес IPv6, маску подсети, IP-шлюз, DNS-IP и домен поиска. Если протокол DHCP IPv6 включен, DHCP-сервер автоматически назначает IP-адрес SNMP IPv6. В том случае, если введенное имя узла не найдено, система добавляет домен поиска к имени узла.

- **System (Система)**

Укажите имя узла SNMP IPv6 в сети. Предоставьте дополнительные сведения о контактном лице и местоположении системы, которые по умолчанию остаются пустыми.

Web (Сеть)



- **Web (Сеть)**

Разрешение/запрет протоколов HTTP/HTTPS. Изменение портов по умолчанию (HTTP: 80, HTTPS: 443). Укажите период обновления сети (по умолчанию: 10 секунд). Страницы Device → Status и Environment автоматически обновляются и обновляют предоставленные сведения по истечении настроенного времени.

- **SSL Certificate (сертификат SSL)**

Сертификат SSL можно использовать для шифрования данных для повышения безопасности подключения. Модуль SNMP IPv6 поддерживает формат PEM, генерируемый OpenSSL. Для загрузки файла сертификата нажмите Browse.

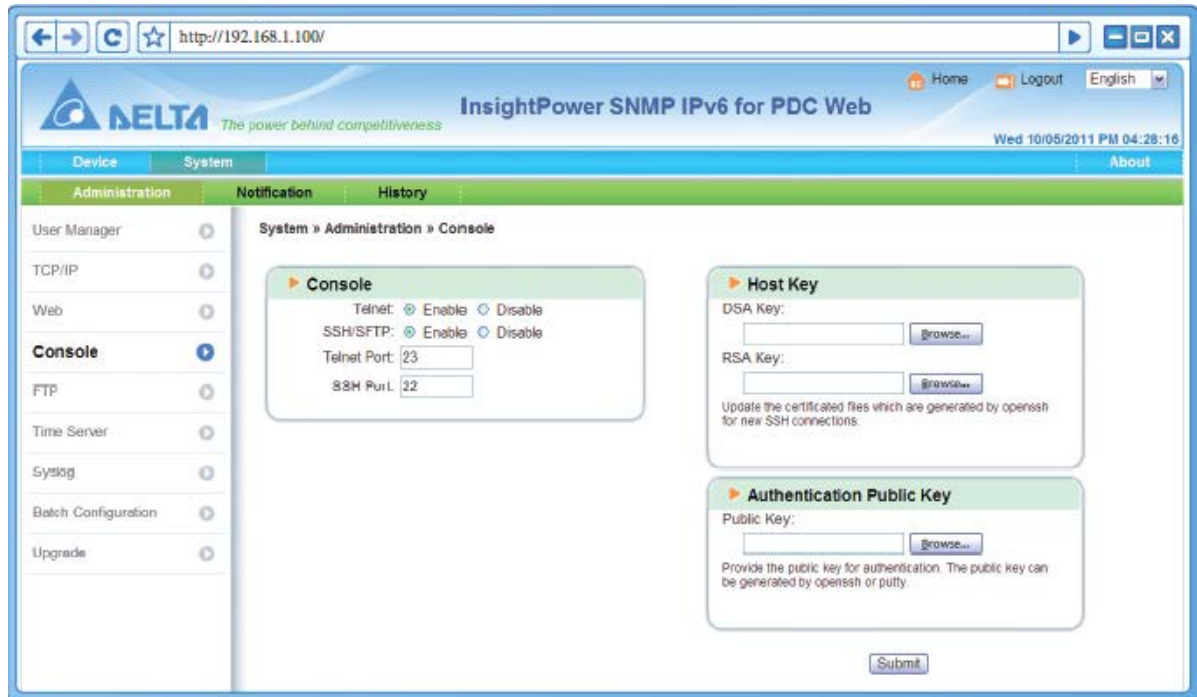
ПРИМЕЧАНИЕ

Подробнее о генерации частного файла сертификата SSL см. **Главу 7: Устранение неисправностей, Q12** или зайдите на <http://www.openssl.org/>.



Console (Консоль)

Эта страница позволяет включать или отключать протоколы связи Telnet/SSH и менять ключи DSA/RSA.



- **Console (Консоль)**

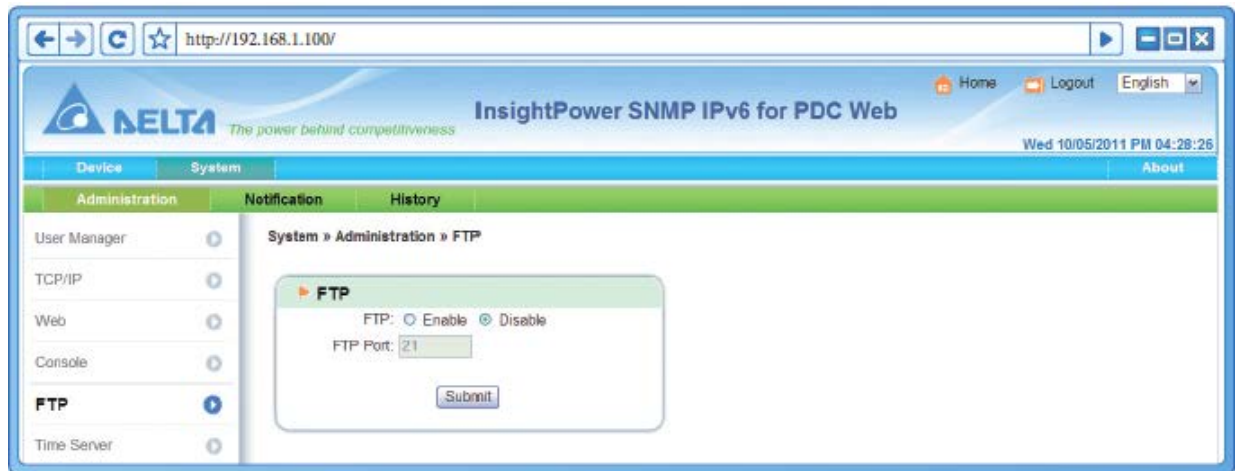
Разрешение/запрет протоколов Telnet и SSH/FTP. Назначение портов при использовании.

- **Host Key (Ключ узла)**

Модуль SNMP IPv6 поддерживает SSH-шифрование для защиты обмена данными. **Обратитесь к Главе 7: Устранение неисправностей, Q13** для генерирования DSA, RSA и открытых ключей. Перечисленные ключи могут загружаться через эту страницу или через протокол SFTP. Чтобы загрузить ключи, обратитесь к **Главе 7: Устранение неисправностей, Q14**.

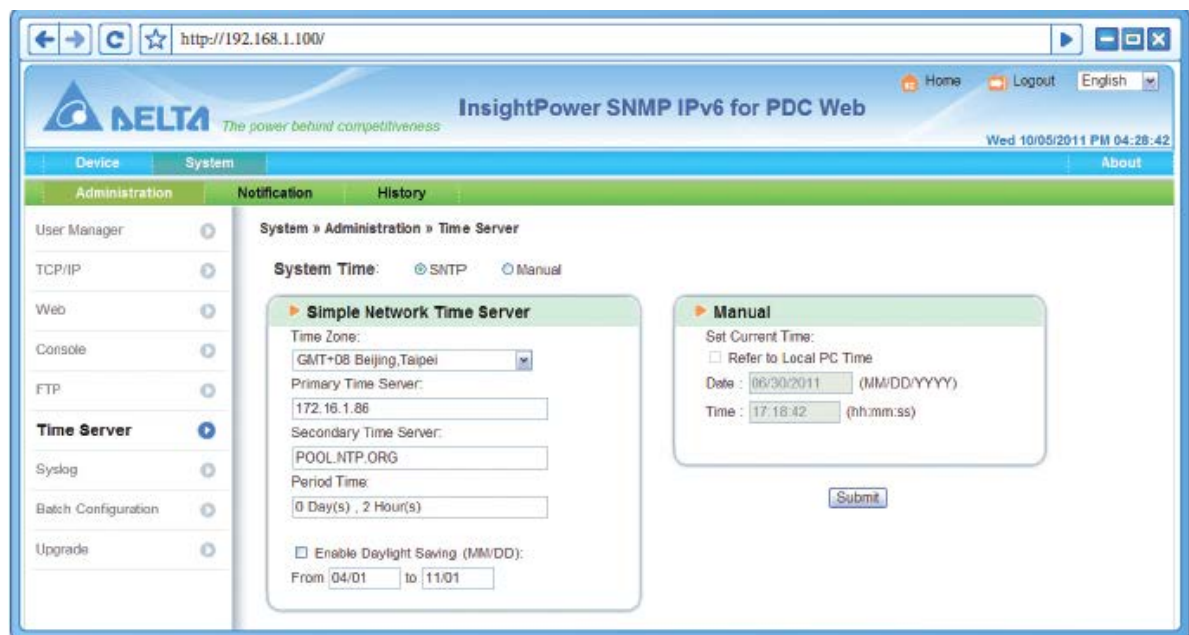
FTP

Разрешение/запрет протокола FTP. Назначение порта при использовании.



Time Server (Сервер времени)

Можно вручную задать системное время и дату или разрешить автоматическую синхронизацию времени с серверами SNTP. Обратите внимание, что если назначенный сервер SNTP не отвечает, журнал событий и данных записываться не будет даже при активации SNTP.



- **Simple Network Time Server (Сервер простого сетевого протокола времени)**

Из выпадающего меню выберите часовой пояс местоположения, в котором находится модуль SNMP IPv6. Укажите IP-адреса или доменные имена для основного и вторичного серверов времени. Модуль SNMP IPv6 синхронизируется с первым отвечающим сервером на основе указанной частоты.

При включенном переходе на летнее время, в течение установленного периода, SNMP IPv6 корректирует время вперед на один час.

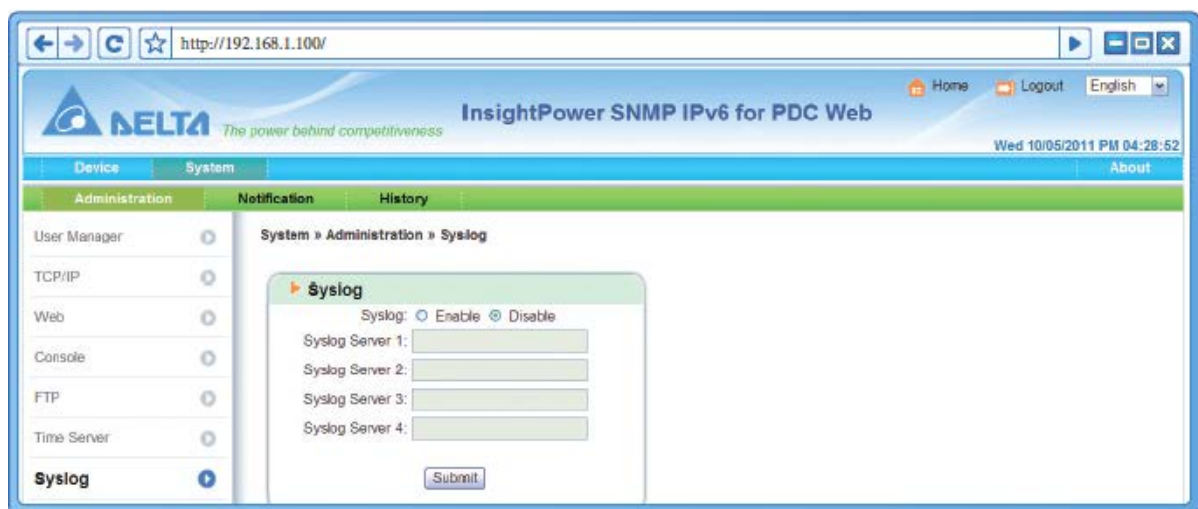
- **Manual (Ручная настройка)**

Если сервер времени недоступен, время и дату можно задать вручную.

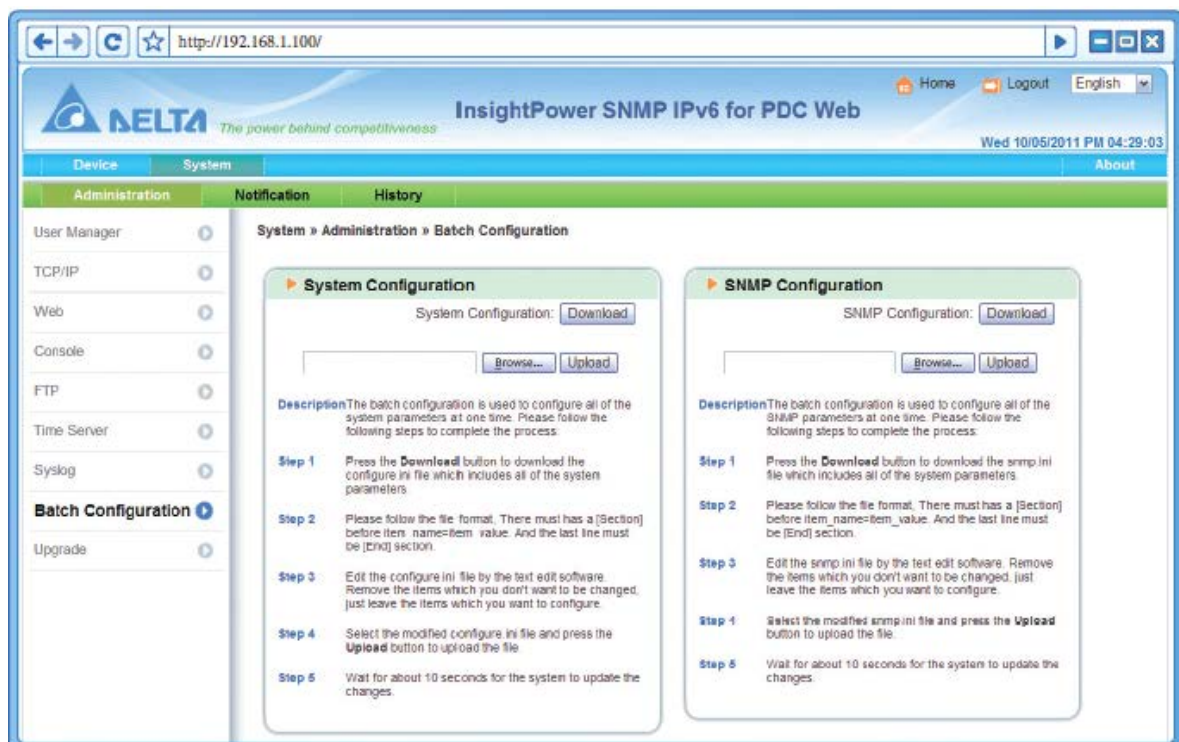
Обратите внимание, что при каждом перезапуске SNMP IPv6, время и дата восстанавливаются до предыдущих назначенных параметров.

- **Syslog (Системный журнал)**

Системный журнал используется для хранения журналов событий на удаленных серверах системных журналов. Эта настройка не влияет на локальные журналы событий. Может быть назначено до четырех серверов системных журналов.



- **Batch Configuration (Пакетное конфигурирование)**



Пакетная конфигурация обеспечивает быструю и легкую установку параметров на нескольких устройствах SNMP IPv6. После завершения настройки системы, выполните экспорт файла конфигурации и его импорт на другие устройства для дублирования настроек и параметров.

- **System Configuration (Конфигурация системы)**

К ней относятся параметры, сохраненные на вкладке **System** → **administration**. Чтобы скачать файл конфигурации, просто нажмите **Download** (configure.ini). Для загрузки файла конфигурации, нажмите **Browse**, выберите файл конфигурации, который хотите загрузить и нажмите **Upload**.

ПРИМЕЧАНИЕ 

Если для модуля SNMP IPv6 назначен статический IP-адрес, откройте файл конфигурации с помощью текстового редактора (например, Notepad или Word Pad) и в разделе [System] удалите следующую строку **IP = XXX. xxx. xxx**. О том, как изменить или назначить IP адрес модуля SNMP IPv6, см. *Главу 4: Настройка системы*.

- **SNMP Configuration (Конфигурация SNMP)**

К ней относятся настройки на вкладке **System** → **Notification**. Для выгрузки файла настроек просто щелкните **Download**. Для загрузки файла настроек щелкните **Browse**, выберите файл для загрузки и щелкните **Upload**.

ПРИМЕЧАНИЕ 

Следуйте инструкциям, приведенным на этой странице, чтобы изменить файлы настроек.

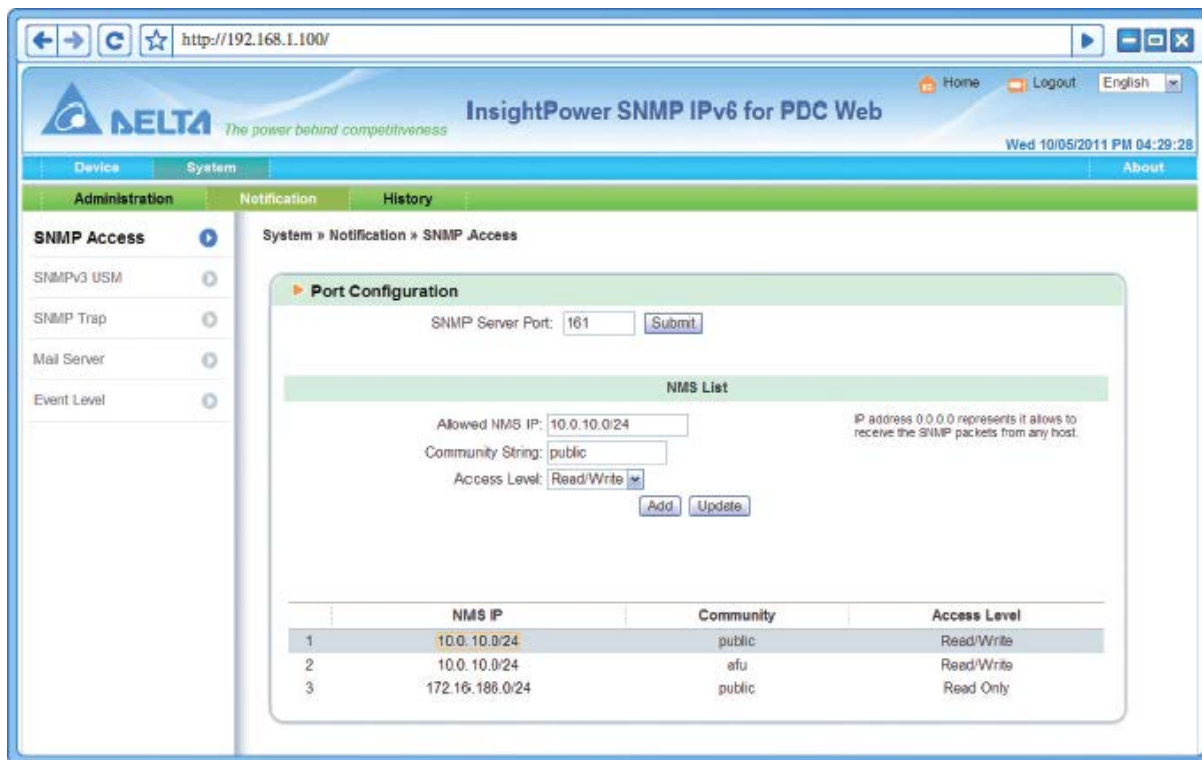
Upgrade (Обновление)

На этой странице, обновите встроенное ПО SNMP IPv6 и проверьте текущую версию встроенного ПО. Нажмите **Browse**, выберите патч-файл и нажмите **Upload**. Процесс обновления должен занять примерно одну минуту.



5-2-2 Notification (Уведомление)

SNMP Access (Доступ к SNMP)



Модуль SNMP IPv6 поддерживает протокол SNMP и систему управления сетью SNMP NMS, которая обычно используется для контроля условий работы сетевых

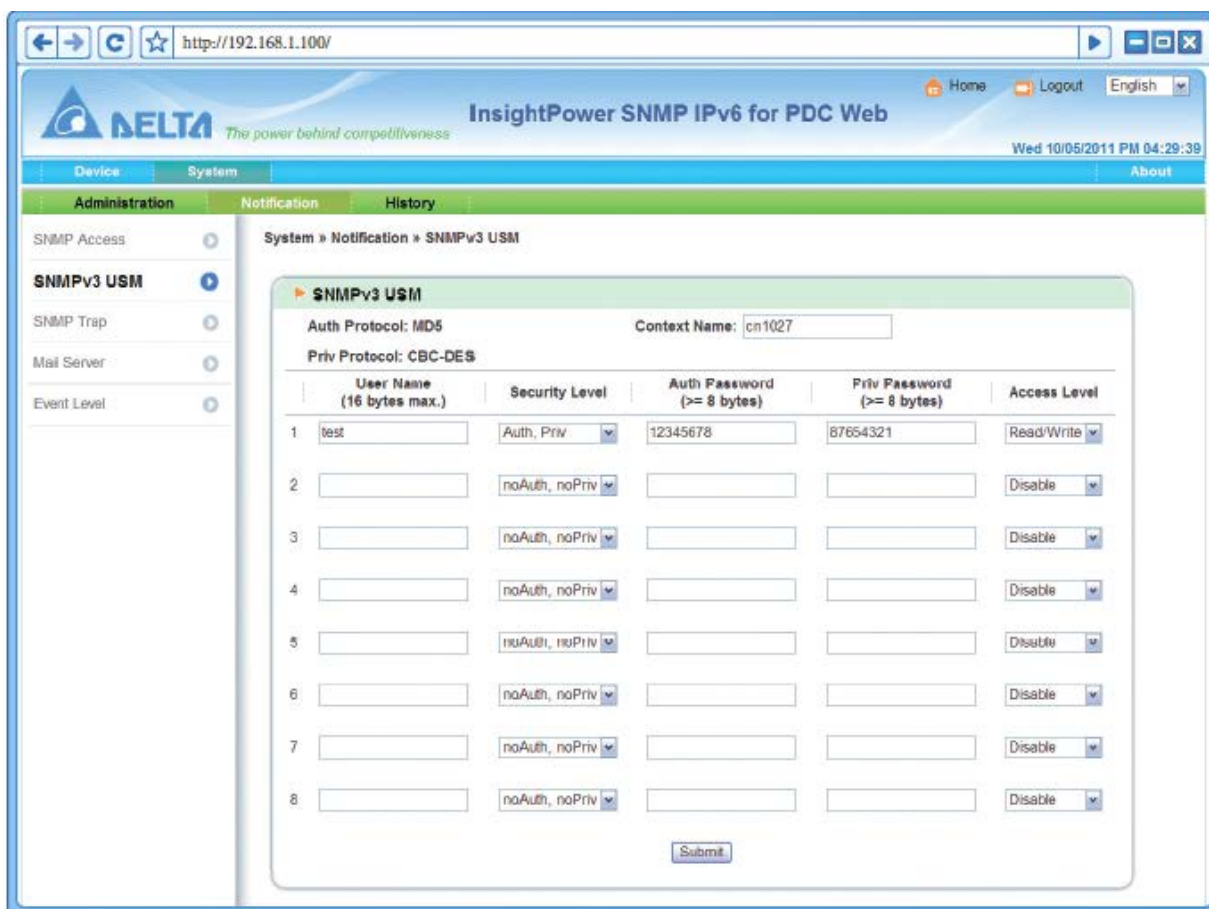
устройств, требующих внимания администратора. Для предотвращения несанкционированного доступа, укажите разрешенные IP-адреса NMS, соответствующие строки сообщества и уровни доступа. Можно назначить до 256 IP-адресов.

ПРИМЕЧАНИЕ 

Если в список добавляется IP-адрес 0.0.0.0, то ограничение доступа к IP NMS игнорируется. Модуль SNMP IPv6 проверит строку сообщества, чтобы определить уровень доступа и разрешение в соответствии с параметрами.

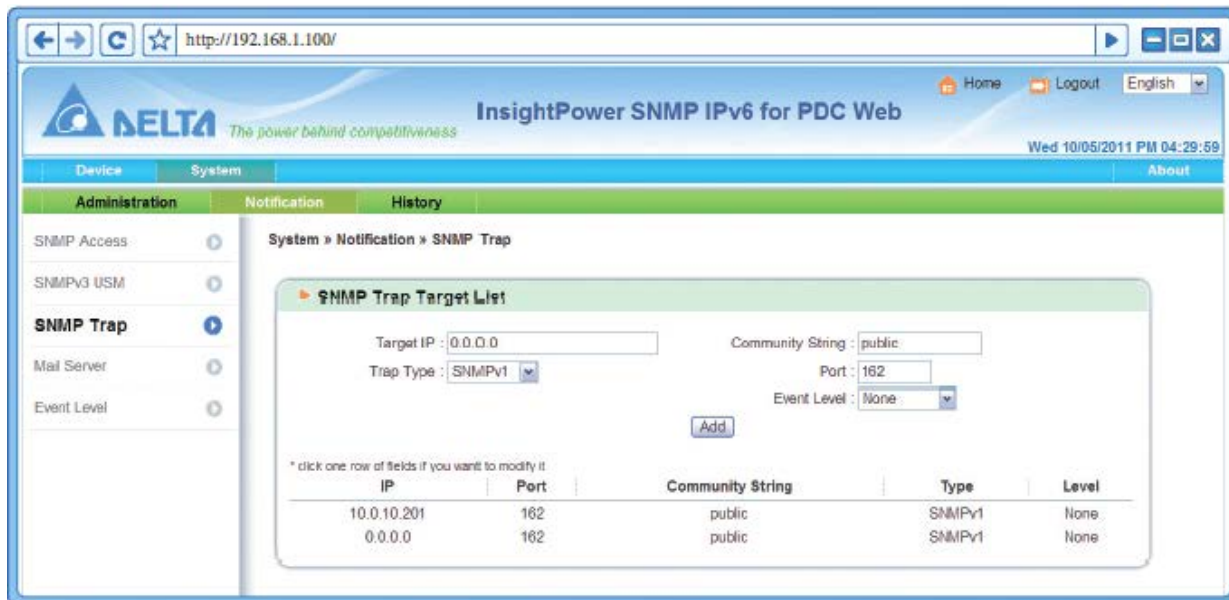
SNMPv3 USM (Диспетчер пользователей SNMPv3 USM)

Протокол SNMPv3 осуществляет шифрование пакетов и аутентификацию пользователя для повышения безопасности подключения. SNMPv3 USM (User Session Management - управление сеансом пользователя) позволяет назначать восемь имен пользователей, права доступа которым предоставляются через протокол SNMPv3. Укажите имя пользователя, уровень безопасности, пароли аутентификации/прав и уровень доступа для каждой учетной записи соответственно.



SNMP Trap (SNMP ловушка)

SNMP ловушка предупреждает пользователей о событиях. Для включения SNMP ловушки, добавьте в список целевые IP-адреса. Укажите строку сообщества, порт, тип ловушки и уровень события, а затем нажмите кнопку **Add**. Щелкните на запись для обновления параметров или удаления их из списка.



ПРИМЕЧАНИЕ

Поддерживаются ловушки SNMPv1, SNMPv2c и SNMPv3. Если ловушка SNMPv3 включена, имена пользователей должны быть указаны в SNMPv3 USM.

Целевые IP-адреса получают уведомления о событиях на основе указанных уровней событий. Три уровня событий показаны следующим образом:

- **Information** (Информация): Все уведомления о событиях отправляются на целевой адрес.
- **Warning** (Предупреждение): Уведомления о предупреждениях и аварийных событиях отправляются на целевой адрес.
- **Alarm** (Аварийное событие): Только уведомления об аварийных событиях отправляются на целевой адрес.

Щелкните на **Event Level (уровень событий)** на левой панели, чтобы изменить уровни отдельных событий.

Mail Server (Почтовый сервер)

Настройка SMTP-сервера для отправки уведомлений о событиях получателям, указанным в списке рассылки почты. Можно добавить до 256 получателей.

The screenshot shows the web interface for configuring the Mail Server. The breadcrumb path is System » Notification » Mail Server. The configuration section includes:

- SMTP Server Name or IP: [text input] (51 bytes max.)
- Account: [text input] (32 bytes max.)
- Password: [text input] (16 bytes max.)
- Submit button

Below the configuration fields is the Mail List section:

- Receiver: [text input] name@company.com
- Event Level: [dropdown menu] None
- Add and Test e-mail buttons

At the bottom, there is a table with the following data:

Receiver	Event Level
1 name@company.com	None

ПРИМЕЧАНИЕ

Если в данной сети DNS сервер недоступен, необходимо вручную ввести адрес SMTP сервера, чтобы активировать систему уведомлений по электронной почте.

- Если имя узла или IP вводится в имя SMTP-сервера, на странице TCP/IP следует добавить IP-адрес DNS.

Укажите адрес электронной почты и уровень событий. При возникновении события, на целевой адрес будет отправлено уведомление. См. далее:

- 1) **Information** (Информация): все уведомления о событиях отправляются на целевой адрес.
- 2) **Warning** (Предупреждение): уведомления о предупреждениях и аварийных событиях отправляются на целевой адрес.
- 3) **Alarm (Аварийное событие)**: только уведомления об аварийных событиях отправляются на целевой адрес.



Event Level (Уровень события)

The screenshot shows the 'Event Level' configuration page for the 'Device' tab. The table lists 24 event messages with their corresponding levels. The levels are dropdown menus with options like 'None', 'Alarm', and 'Warning'. A 'Submit' button is located at the bottom of the table.

ID	Event Message	Level
1	PDC device disconnected %s	None
2	PDC device connected %s	Alarm
3	Main status alarm %s	Warning
4	Recover from main status alarm %s	Warning
5	Primary status alarm %s	Alarm
6	Recover from primary status alarm %s	Alarm
7	Secondary status alarm %s	Alarm
8	Recover from secondary status alarm %s	Alarm
9	Panel status alarm %s	Alarm
10	Recover from panel status alarm %s	Alarm
11	Subfeed status alarm %s	Alarm
12	Recover from subfeed status alarm %s	Alarm
13	Branch over-current alarm %s	Warning
14	Recover from branch over-curren alarm %s	Warning
15	Branch under-curren alarm %s	Alarm
16	Recover from branch under-curren alarm %s	Alarm
17	Branch over-current-demand alarm %s	Warning
18	Recover from branch over-curren-demand alarm %s	Warning
19	Branch under-curren-demand alarm %s	Alarm
20	Recover from branch under-curren-demand alarm %s	Alarm
21	Branch over-KW-demand alarm %s	Alarm
22	Recover from branch over-KW-demand alarm %s	Alarm
23	Branch under-KW-demand alarm %s	Alarm
24	Recover from branch under-KW-demand alarm %s	Alarm

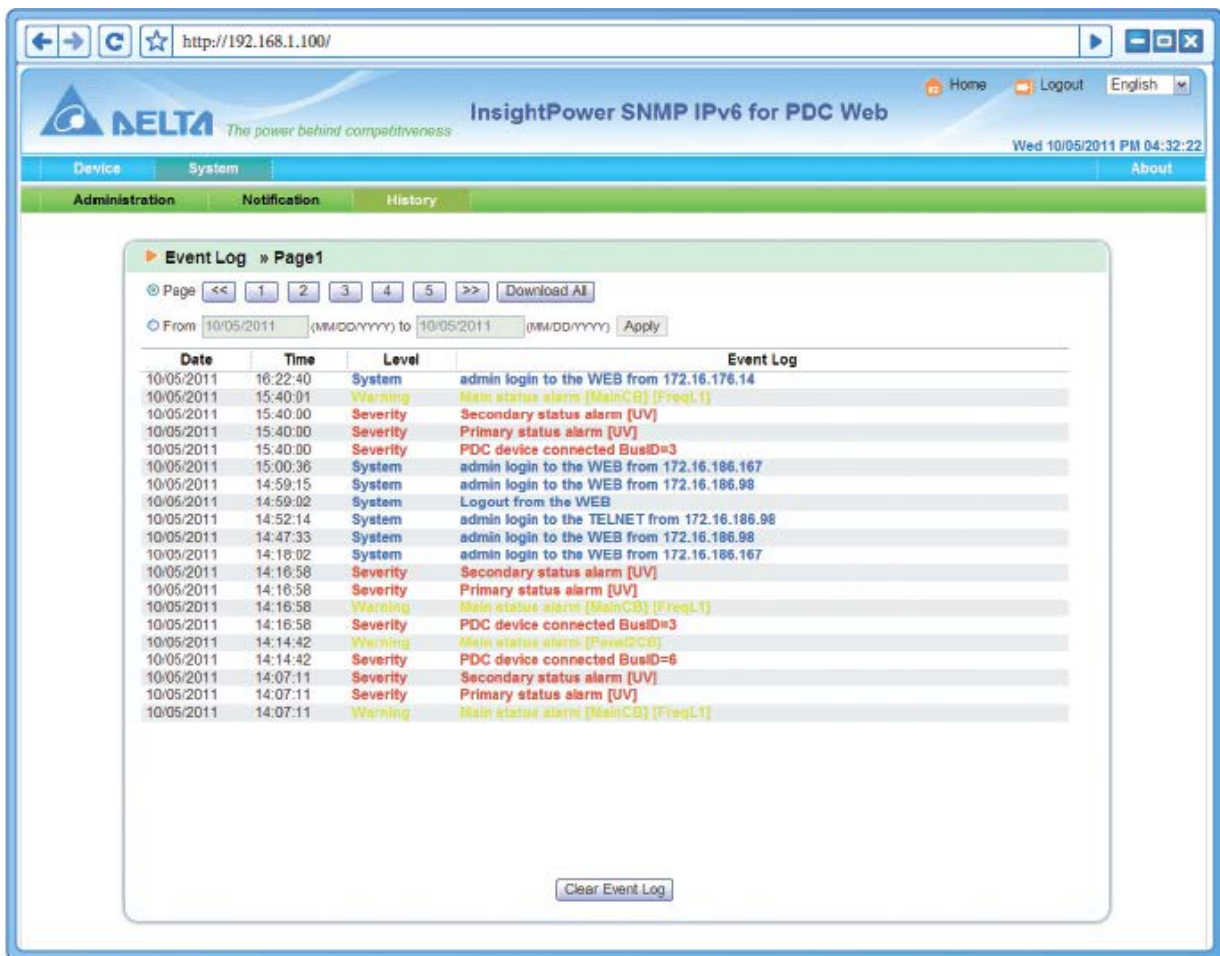
- **Device** (Устройство): Событиям ШРП могут быть назначены три уровня событий, включая информацию (синий), предупреждение (желтый) и аварийное событие (красный). Нажмите **Submit** для вступления в силу.
- **Env.Probe** (Датчик EnviroProbe): Назначение уровней для событий датчика EnviroProbe . Нажмите **Submit** для вступления в силу.

5-2-3 History (записи действий пользователя или системы)

На этой странице проверьте записи событий. Нажмите  и  для перелистывания страниц. Щелкните на номер страницы, чтобы перейти на неё.

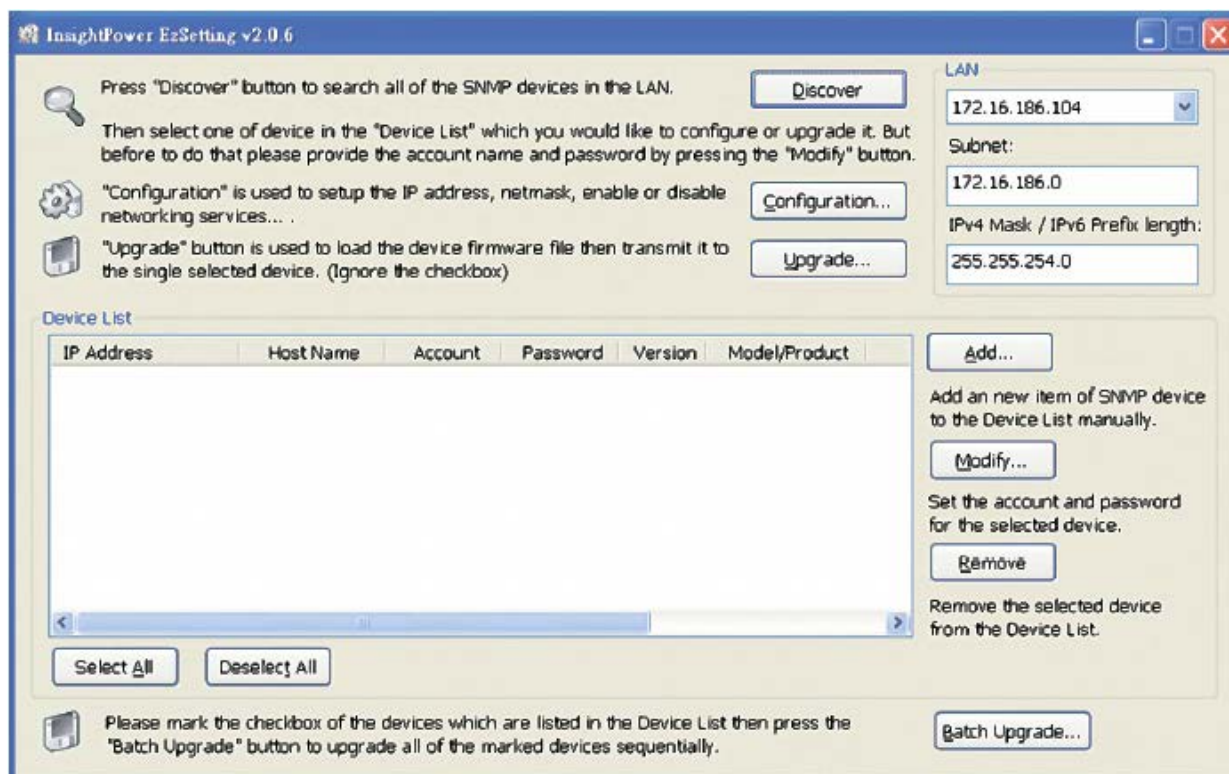
Чтобы проверить записи событий, записанные в течение периода времени, выберите даты и нажмите **Apply**. Чтобы загрузить весь журнал событий, нажмите **Download All** всплывающее окно предложит вам сохранить файл (. csv). Файл можно открыть или отредактировать в Microsoft Excel.

Чтобы стереть все записи событий, нажмите **Clear Event Log**. Рекомендуется сначала загрузить и создать резервную копию журнала событий.



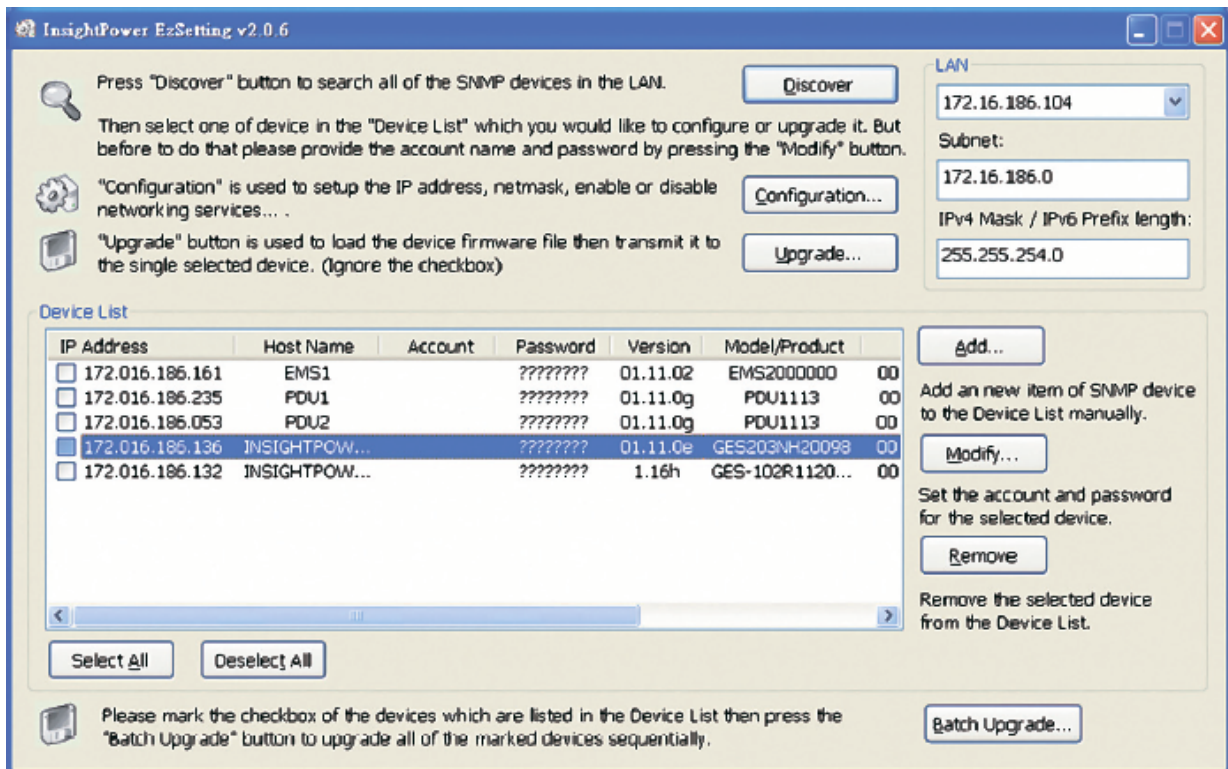
Глава 6 : Обновление встроенного ПО SNMP-устройств

Прилагаемая программа EzSetting позволяет легко обновлять встроенное ПО на устройствах SNMP через ЛВС. Для обновления ПО выполните следующие действия



Шаг 1 Маска подсети позволяет уточнить область поиска устройств в указанных подсетях. Убедитесь, что SNMP устройство, ПО которого требуется обновить, находится в указанной подсети. В противном случае измените подсеть и маску подсети.

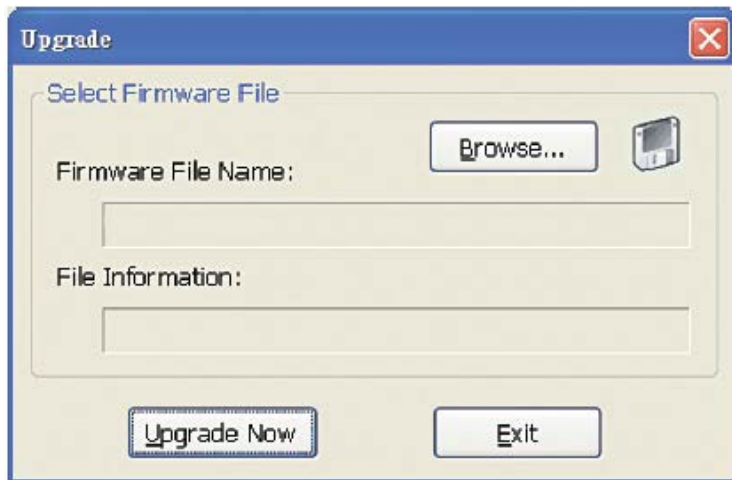
Шаг 2 Щелкните кнопку **Discover** (найти). На экране появится список SNMP устройств, найденных в указанной подсети.



Шаг 3 Выберите нужное устройство из списка устройств Device List, щелкните **Modify** и введите учетную запись и пароль администратора.



Шаг 4 Щелкните **Upgrade** (обновить). Открывается окно диалога обновления. Щелкните **Browse**, чтобы выбрать нужный бинарный файл встроенного ПО. Убедитесь, что в поле File Information указана версия встроенного ПО, а затем щелкните **Upgrade Now**, чтобы выполнить обновление.



Шаг 5 Процесс обновления должен занять около 20 секунд.



Шаг 6 По завершении обновления, открывается следующее окно диалога. Для перезагрузки устройства требуется около 1 минуты.



Глава 7 : Устранение неисправностей

- Q1** Как настроить SNMP сервер на моей рабочей станции, чтобы синхронизировать модуль SNMP IPv6?

Чтобы включить SNMP сервисы в ОС Windows XP, щелкните **Start (Пуск)** → **Control Panel (Панель управления)** → **Add/ Remove Programs (Установка и удаление программ)** → **Add/ Remove Windows Components (Установка/Удаление компонентов Windows)** → **Networking Services (Сетевые службы)** → установите флажок **Simple TCP/ IP Services (Простые службы TCP/IP)** → **ОК**. Чтобы включить синхронизацию времени, нужно задать адреса серверов времени SNMP в меню **Time Server**. См. *Главу 4: Настройки системы*.

- Q2** Как убедиться, что между модулем SNMP IPv6 и ШРП установлено соединение?

Если соединение между SNMP IPv6 и ШРП установлено правильно, то будет часто мигать желтый светодиодный индикатор. Если нет, убедитесь, что параметр идентификатора устройства в модуле SNMP IPv6 и ШРП является согласованным.

```
C:\>ping 172.16.186.230

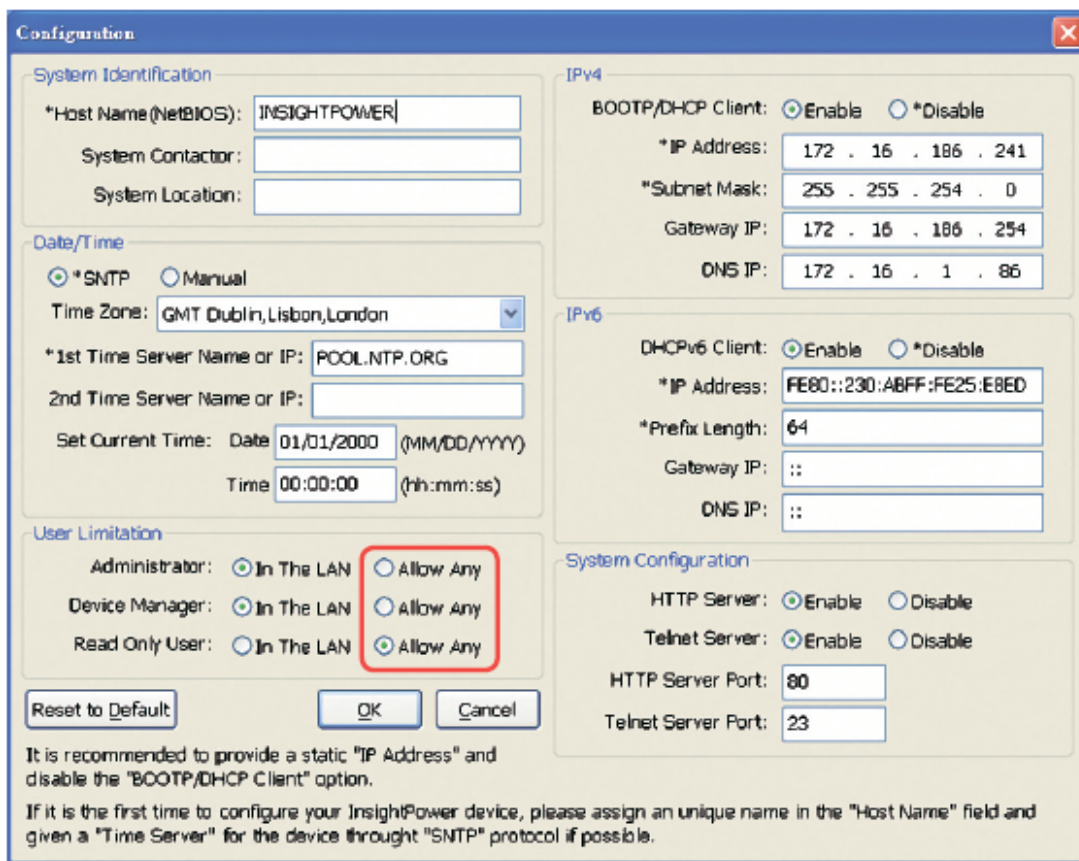
Pinging 172.16.186.230 with 32 bytes of data:
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=4ms TTL=64

Ping statistics for 172.16.186.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\>
```

- Q3** Что делать, если страница InsightPower SNMP IPv6 for PDC Web открывается, но войти в веб-интерфейс не удается?

Проверьте IP-адреса модуля SNMP IPv6 и рабочей станции, с которой вы пытаетесь войти. По умолчанию они должны быть в одной локальной сети, чтобы можно было связаться по веб-интерфейсу. Если это не так, то можно разрешить внешние соединения. Для этого, запустите EzSetting и измените ограничение пользователя (User limitation), чтобы разрешить любые (Allow Any), как показано ниже.



Q4 Что делать, если не удастся связаться с SNMP IPv6 через имя его узла?

Если вы только что назначили SNMP IPv6 новый статический IP адрес, вам нужно обновить таблицу NetBIOS, чтобы привести ее в соответствие с новой настройкой. Хотя Windows периодически обновляет таблицу NetBIOS, вы можете вручную принудительно обновить ее командой **nbtstat -R** в командной строке DOS. После этого можно будет связаться с SNMP IPv6 через имя его узла. Необходимо убедиться, что имя узла, назначенное для SNMP IPv6, не превышает 16 байт.

Q5 Как можно проверить IP адрес моей рабочей станции?

В ОС Windows введите в командной строке команду **ipconfig /all**. В ОС UNIX введите в консоли команду **ifconfig**. Теперь можно проверить IP и физический адрес (MAC-адрес).

```
Physical Address. . . . . : 00-23-4D-A2-3A-2C
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ad55:5b9b:74c6:e5fc%12 (Preferred)
IPv4 Address. . . . . : 172.16.186.97 (Preferred)
Subnet Mask . . . . . : 255.255.254.0

C:\>
```

Q6 Что делать, если не удается связаться с модулем SNMP IPv6?

Если модуль SNMP IPv6 не отвечает, проверьте следующее:

- 1) Если не горит зеленый светодиодный индикатор, проверьте, правильно ли установлен и подключен к маршрутизатору или концентратору сетевой кабель.
- 2) Если зеленый светодиод горит, то возможно, недоступен IP адрес. Назначьте вручную допустимый IP адрес для модуля.
- 3) Если зеленый светодиод мигает и (1) конфигурация сети включает сервер DHCP, то убедитесь, что служба DHCP работает правильно; (2) В противном случае убедитесь, что назначенный вручную IP адрес не занят другим устройством. Учтите, что если текущая конфигурация не может быть использована, то модуль SNMP IPv6 восстановит настройки IP по умолчанию (адрес IPv4: 192.168.1.100/ маска сети: 255.255.255.0/ шлюз: 192.168.1.254).
- 4) Если проблема не устраняется перечисленными выше средствами, то соедините сетевым кабелем модуль и рабочую станцию. Проверьте связь с SNMP IPv6 по умолчанию или статическому IP-адресу в соответствии с вашими настройками. Если ответ на запрос успешно получен, что говорит об исправной работе модуля, то нужно проверить ваше сетевое оборудование. Если нет, то свяжитесь с местным дилером или сервисным центром для оказания помощи.

Q7 Что делать, если не выполняется команда SNMP Get?

См. раздел **5-2-2 Notification (Уведомление)**, чтобы проверить настройки SNMP. Убедитесь, что IP адрес рабочей станции добавлен в список NMS IP с доступом Read или Read/ Write. Рабочая станция и модуль SNMP IPv6 должны относиться к одному сообществу.

Q8 Что делать, если не выполняется команда SNMP Set?

См. раздел **5-2-2 Notification (Уведомление)**, чтобы проверить настройки SNMP. Убедитесь, что IP адрес рабочей станции добавлен к списку NMS IP с доступом Read/ Write. ПК и модуль SNMP IPv6 должны относиться к одному сообществу.

Q9 Не удается получить ловушку SNMP?

См. раздел **5-2-2 Notification (Уведомление)**, чтобы проверить настройки SNMP ловушки. Убедитесь, что IP-адрес рабочей станции добавлен к списку целевых IP-адресов.

Q10 Что делать, если забыли учетную запись и пароль администратора?

Можно восстановить учетную запись и пароль администратора в консольном режиме. См. раздел **4-4 Настройка через COM-порт**, чтобы установить

соединение через COM-порт с SNMP IPv6. Когда система запросит регистрационное имя, введите **rstadmin** в течение 30 секунд и нажмите клавишу **Enter**. По этой команде восстанавливается исходная учетная запись и пароль администратора (admin/ password).

Q11 Как активировать IPv6 в Windows XP?

Если вы работаете в ОС Windows XP, прежде всего, установите IPv6 (щелкните **START (Пуск)**→ **RUN (Выполнить)** и введите строку **ipv6 install**). Модуль SNMP IPv6 поддерживает протокол IPv6, так что дополнительные настройки не требуются. Однако следует заметить, что IPv6 автоматически отключается, если в локальной сети уже имеется идентичный LLA (Local-link Address). Кроме того, если введены настройки для обоих протоколов, IPv4 и IPv6, то в качестве первичного IP адреса модуля SNMP IPv6 используется адрес IPv4. Подробнее о совместимости IPv6 см. на сайте IETF ([http:// tools.ietf.org/html](http://tools.ietf.org/html)) или IPv6 Ready Logo Program (<http://www.ipv6ready.org>).

Q12 Как сгенерировать файл частного SSL сертификата (в формате PEM) для HTTPS-соединения?

Для обеспечения безопасности соединения SNMP IPv6 и рабочей станции необходимо создать свой файл SSL сертификата. Загрузите и установите программу OpenSSL Toolkit с сайта <http://www.openssl.org>. Запустите консоль или интерпретатор командной строки и введите следующую команду для создания файла своего сертификата:

```
openssl req -x509 -nodes -days 3650 -newkey  
rsa:1024 -keyout cert.pem -out cert.pem
```

- 1) Ответьте на вопросы системы. Действуйте в соответствии с указаниями программы. После завершения работы, в текущем рабочем каталоге создается файл с именем cert.pem.
- 2) Загрузите cert.pem в веб-интерфейс модуля InsightPower SNMP IPv6 for PDC Web. См. раздел **5-2-1 Administration (Администрирование) – Web**.

Q13 Как генерировать ключи DSA, RSA и Public keys (открытые ключи) для SSH?

Для Linux:

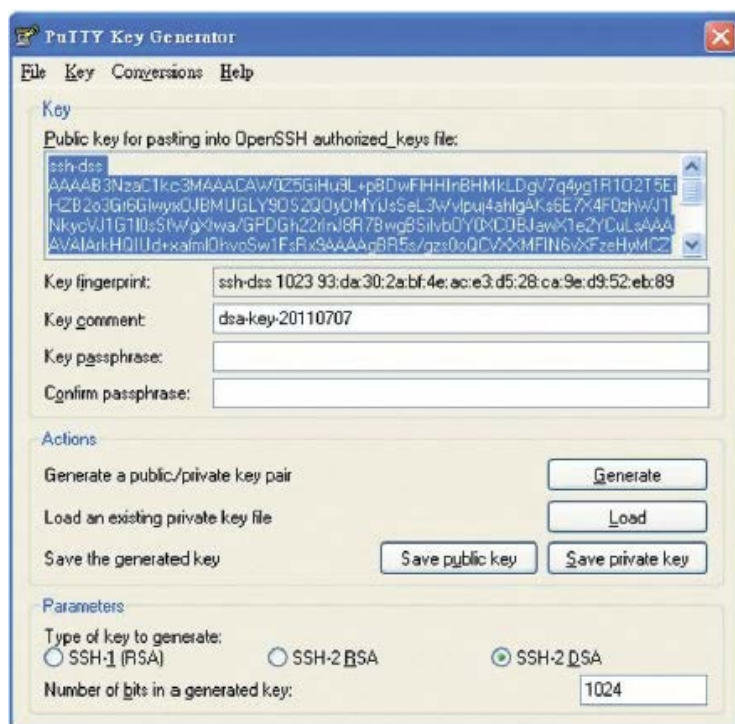
- 1) Загрузите и установите программу OpenSSH с сайта <http://www.openssh.org>.
- 2) Запустите консоль и введите следующую команду, чтобы создать собственные ключи (игнорируйте запрос идентификационной фразы):

```
DSA Key:ssh-keygen -t dsa  
RSA Key:ssh-keygen -t rsa
```

- 3) Загрузите ключи DSA и RSA на веб-интерфейс модуля InsightPower SNMP IPv6 для ШПП. Подробнее см. раздел **5-2-1 Administration (Администрирование)** - Console (Консоль).

Для Windows:

- 1) Загрузите и установите PuTTY с сайта <http://www.puttygen.org>.
- 2) Запустите puttygen.exe из установленного каталога.
- 3) В области Parameters выберите **SSH-2 RSA** и щелкните **Key** → **Generate key pair**, чтобы сгенерировать ключ RSA.
- 4) Выберите **Conversions** → **Export OpenSSH Key** и задайте имя файла для RSA ключа. Игнорируйте запрос идентификационной фразы.
- 5) В Parameters выберите SSH-2 DSA и щелкните Key → Generate key pair, чтобы генерировать ключ DSA.
- 6) Выберите Conversions → Export OpenSSH Key и задайте имя файла для DSA ключа. Игнорируйте запрос идентификационной фразы.
- 7) Скопируйте сгенерированные ключи из текстовой строки, вставьте в текстовый редактор и сохраните в виде текстового файла.



- 8) Загрузите файлы ключей DSA/ RSA/ Public keys на веб-интерфейс модуля InsightPower SNMP IPv6 для ШПП. Для получения дополнительных сведений обратитесь к разделу **5-2-1 Administrator (администратор)** - Console (консоль).

Q14 Как загрузить конфигурацию/ встроенное ПО/ файлы ключей через SSH/SFTP?

Для быстрой настройки модуля SNMP IPv6 можно загрузить файлы через SSH/SFTP. Модуль SNMP IPv6 автоматически импортирует ваши настройки после загрузки файлов в назначенные каталоги. См. следующую таблицу:

Каталог	Файлы
\config_snmp	snmp.ini
\config_system	configure.ini
\ssh_dsa	Ключ DSA
\ssh_rsa	Ключ RSA
\ssh_pubkey	Открытый ключ
\upgrade_snmp	Бинарный пакет обновления встроенного ПО SNMP IPv6
\upgrade_device*	Бинарный пакет обновления встроенного ПО устройства

*Только для конкретных устройств.

Загрузите файлы в соответствующие каталоги. Убедитесь, что названия файлов содержат только английские символы. Подтвердите перезапись существующих файлов, если так запросит программа SFTP client.

Q15 Как проверить SNMPv3 в системе Linux?

Прежде чем обратиться к идентификатору объекта SNMP OID через протокол SNMPv3, необходимо организовать таблицу SNMPv3 USM. Подробнее см. раздел **5-2-2 Notification (Уведомление) - SNMPv3 USM (Диспетчер пользователей SNMPv3)**.

Чтобы проверить SNMPv3 в системе Linux, запустите консоль и введите следующую команду:

```
snmpwalk -v 3 -u <user> -l authPriv -A <password> -X <password> -n <context name> -t 3 <ip> 1.3.6.1.2.1.1.1.0
```

-v: 1 для SNMPv1, 3 для SNMPv3.

-l: далее указывается уровень безопасности. Эти уровни: noAuthNoPriv, authNoPriv и authPriv.

-u: имя пользователя, назначенное в таблице SNMPv3 USM.

-A: пароль Auth, назначенный в таблице SNMPv3 USM.

-X: пароль Priv, назначенный в таблице SNMPv3 USM.

-n: контекстное имя, назначенное в таблице SNMPv3 USM.

-t: таймаут в секундах.

<ip>: IP адрес модуля SNMP IPv6.

<oid>: следующий доступный идентификатор объекта SNMP (например: 1.3.6.1.2.1.1.1.0). См. RFC1213 MIB.

Приложение А: Характеристики

Параметр	Значение
Напряжение питания	12В пост. тока
Потребляемая мощность	2Вт (макс.)
Сетевое подключение	Разъем RJ-45 (10/ 100М)
Физические характеристики	
Размер (Ш x Г)	130 мм x 60 мм
Масса	75г
Условия окружающей среды	
Рабочая температура	0 ~ 60°C
Температура хранения	-40 ~ 125°C
Рабочая влажность	0 ~ 90% (без конденсации)

ПРИМЕЧАНИЕ

- * Обратитесь к табличке номинальной мощности для безопасного уровня мощности.
- * Все технические характеристики могут быть изменены без предварительного уведомления.

Приложение В: Гарантия

Продавец гарантирует отсутствие дефектов материала и производственных дефектов данного продукта в течение гарантийного периода при его использовании в соответствии с действующими инструкциями. При обнаружении каких-либо дефектов продукта в течение гарантийного периода Продавец осуществляет ремонт или замену продукта по собственному усмотрению в зависимости от неисправности.

Эта гарантия не применяется к естественному износу или к повреждению в результате ненадлежащей установки, эксплуатации, использования, технического обслуживания или форс-мажорного обстоятельства (т. е. войны, пожара, стихийных бедствий и т.д.), а также категорически исключает любые побочные и косвенные убытки.

В случае любого повреждения, возникшего по истечении гарантийного периода, сервисное обслуживание предоставляется на платной основе. Если возникает необходимость в техническом обслуживании, нужно связаться с поставщиком или продавцом.



ПРЕДУПРЕЖДЕНИЕ: пользователь должен заранее определить, являются ли окружающая среда и характеристики нагрузки приемлемыми, подходящими и безопасными для установки и эксплуатации данного продукта. Необходимо внимательно соблюдать данное руководство по эксплуатации. Продавец не дает никаких заверений и гарантий относительно пригодности данного продукта для каких-либо конкретных целей применения.



NO.UMEN3915100975-S35PDC130227