НСК Коммуникации Сибири

26.30.11.120

УТВЕРЖДАЮ

Директор ООО «НСК Коммуникации Сибири»

_____ С. В. Давыдов

« 17 » _____марта_____ 2017 г.

SPRINTER TX 10G
Руководство по эксплуатации

РЭ26.30.11-007-62880827-2016

Сертификат соответствия

№ ОС-1-СП-1509 от 10.02.2017 г.

Новосибирск, 2017

1 Общее описание, устройство и функционирование

1.1 Описание устройства

Sprinter TX (10G) - управляемый коммутатор Metro Ethernet разработанный для применения на уровне агрегации распределенных сетей операторов связи и Интернет провайдеров. Sprinter TX (10G) имеет 24 SFP+ 10G портов и 3 медных порта 1000BASE-T.

Управление осуществляется через сеть Ethernet, локально через USB порт, а также через GSM модуль для возможности управления в случае аварии в опорной сети.

Два сменных блока питания обеспечивают резервирование и гибкость при выборе питающего напряжения (220VAC, 48VDC). Съемный фильтр для защиты от пыли и автоматический контроль скорости вращения вентиляторов.

Порты, выключатели и контактные группы коммутаторов размещены на передней панели, что обеспечивает быстрый и удобный доступ, установку и обслуживание в ограниченном пространстве монтажных шкафов.

Характеристики Ethernet Switch

1. **Эксплуатационные свойства**

   - пропускная способность 240 Gbps (полный дуплекс);
   - Размер таблицы MAC-адресов: 16K;
   - Max frame size 16K;
   - IGMP Snooping;
   - Зеркалирование портов;
   - DHCP.

2. **Способы управления**

   - локальное управление через последовательный порт мини-USB;
   - удаленное управление через сеть передачи данных по протоколам telnet, snmp, ftp, http, GSM канал;
   - управление с помощью командной строки и системы меню.

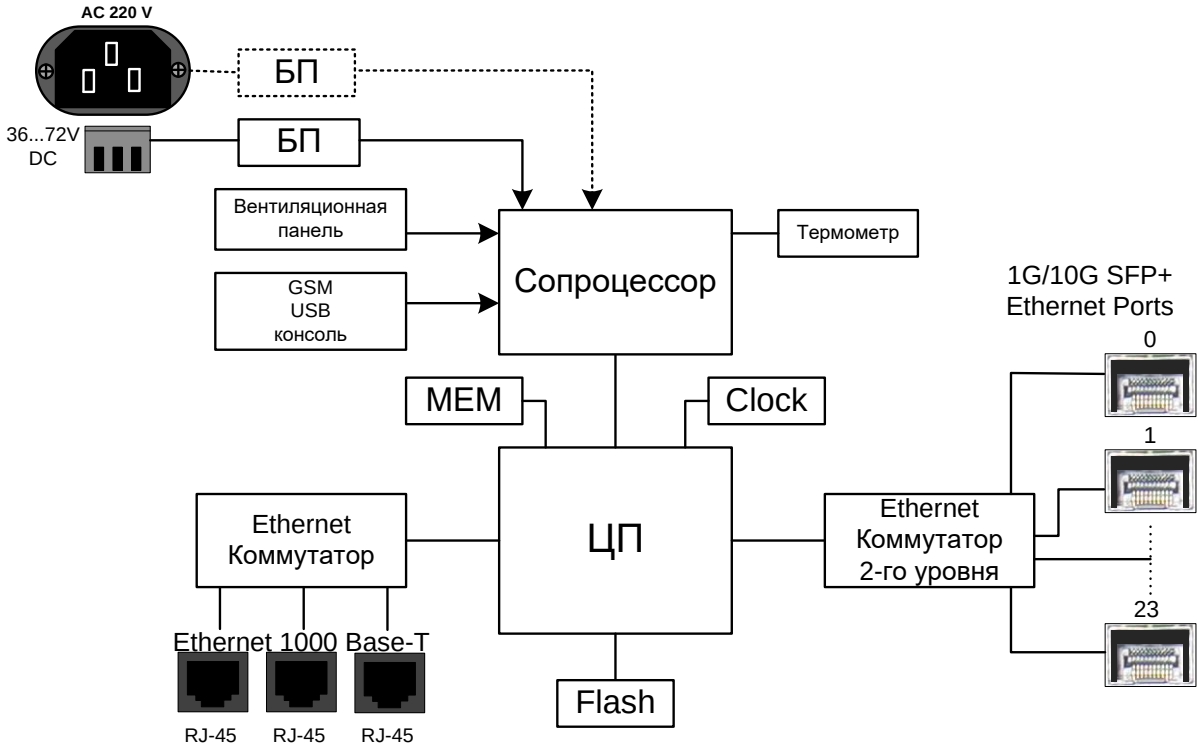
1.2 Функционирование устройства

Мультиплексор представляет собой сложное микропроцессорное устройство, состоящее из следующих основных узлов: Центрального Процессора (ЦП), Ethernet коммутатора 2-го уровня и сопроцессора измерений.

Вышеописанные узлы работают под управлением центрального процессора, программное обеспечение которого выполняет следующие основные функции:

- проверку и конфигурацию всех узлов мультиплексора при включении питания;
- передачу Ethernet со скоростью 10 Гбит/с;
- контроль параметров входных сигналов и состояния агрегатных интерфейсов во время работы мультиплексора;
- запись в энергонезависимую память данных обо всех отклонениях от нормы входных сигналов и нарушениях работоспособности мультиплексора;

- индикацию функционирования мультиплексора и выдачу диагностической информации по протоколам telnet, HTTP, SNMP.



Основные узлы мультиплексора

Входящие Ethernet пакеты принимаются пользовательскими интерфейсами.

Центральный процессор выполняет функции протоколов маршрутизации, обрабатывает информацию о маршрутах, а также выполняет функции управления сетью.

Пакетный коммутатор, в свою очередь, на основе имеющейся у него информации о маршрутах (и на основе алгоритма обучения) с учетом приоритета и меток VLAN направляет пакеты, в линию передачи.

Встречный мультиплексор принимает адресованные ему пакеты, выполняет контроль поступивших данных, при необходимости запрашивая повтор поврежденных пакетов, и направляет пользовательские пакеты в абонентские интерфейсы Ethernet.

Мультиплексор работает под управлением встроенной операционной системы LP OS. Код операционной системы и настройки мультиплексора хранятся в микросхемах флэш-памяти, организованных в файловую систему.

Обновление программного обеспечения мультиплексора может быть выполнено через порт USB, удаленно через сеть TCP/IP по протоколу FTP, а также через GSM канал. Для защиты от несанкционированного доступа предусмотрен запрос пароля и проверка IP адреса управляющей станции.

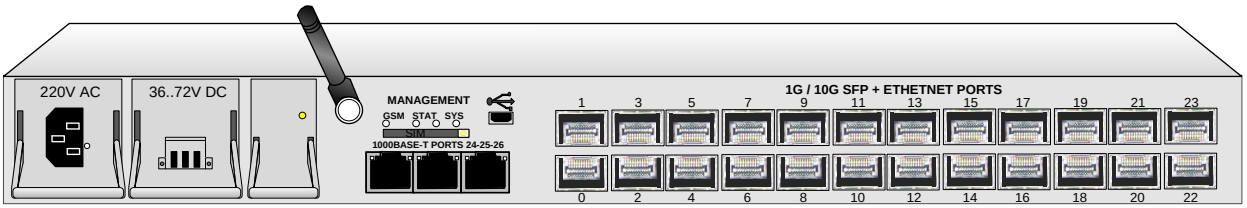
1.3 Конструктивное исполнение

Мультиплексор Sprinter TX выполнен в виде изделия в металлическом корпусе для монтажа в стойку 19” размерами 430x44x220 мм. На передней панели расположены:

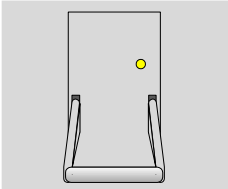
- 24 десяти гигабитных порта SFP +;
- 3 медных порта RJ-45 для управления устройством;
- 1 порт консоли (мини-USB);
- GSM модуль для возможности управления в случае аварии в опорной сети.

Также на передней панели расположены два сменных блока питания обеспечивают резервирование и гибкость при выборе питающего напряжения (220VAC, 48VDC).

Sprinter TX (10G) вид спереди.



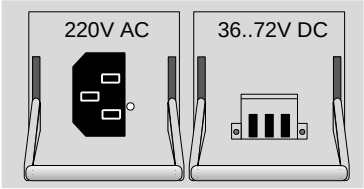
1.3.1 Вентиляционная панель



В мультиплексор устанавливается съемный блок с четырьмя вентиляторами.

При работе мультиплексора температура контролируются. Посмотреть температуру в корпусе мультиплексора можно командой *envir*. Так же в мультиплексоре есть съемный фильтр для защиты от пыли и автоматический контроль скорости вращения вентиляторов.

1.3.2 Сменные блоки питания



Мультиплексор может комплектоваться блоками питания 220VAC и 48VDC. Два сменных блока питания обеспечивают резервирование и гибкость при выборе питающего напряжения.

Электропитание от источника постоянного напряжения осуществляться отрицательным напряжением -48 В (допустимые пределы изменения -36...-72В). Также мультиплексор защищен от подачи напряжения неправильной полярности. В этом случае светодиодные индикаторы не светятся, устройство может находиться в этом состоянии неограниченное время.

1.3.3 Интерфейс Ethernet 1000Base-T

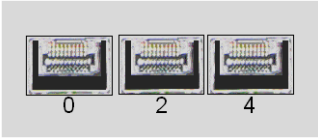
1	2	3	4	5	6	7	8
TD+	TD-	TD+	TD+	TD-	TD-	TD+	TD-
Пара 1	Пара 1	Пара 2	Пара 3	Пара 3	Пара 2	Пара 4	Пара 4

Мультиплексор содержит интерфейсы Ethernet 1000BaseT для передачи данных со скоростью 1000 Мбит/с в соответствии со спецификацией IEEE802.3. Каждый интерфейс Ethernet выведен на разъем RJ-45, расположенный на передней панели устройства. Интерфейс Ethernet соединяется с портом коммутатора локальной сети или с

компьютером кабелем UTP или STP категории 5. Интерфейс автоматически распознает тип кабеля – прямой или скрещенный.

Состояние каждого интерфейса Ethernet индицируется двумя светодиодными индикаторами – зеленым LINK и желтым ACT, расположенными в разъеме RJ-45. Постоянное свечение индикатора LINK указывает на то, что мультиплексор подключен к сети Ethernet. Мигание индикатора ACT показывает прием или передачу пакетов данных.

1.3.4 Интерфейс SFP



На передней панели устройства расположены 24 интерфейса SFP/SFP+.

SFP модули (англ. Small Form-factor Pluggable — компактный сменный приемопередатчик) являются компактными оптическими трансиверами. Стандартные SFP модули используются для дуплексной передачи данных по двум волокнам (одномодовым или многомодовым). SFP модуль выступает в качестве оптического интерфейса для активного телекоммуникационного оборудования (коммутаторов, маршрутизаторов, либо другого оборудования).

SFP+ модули используются при организации высокоскоростных дуплексных каналов со скоростью передачи данных до 10 Гбит/с. WDM SFP+ предназначены для организации дуплексного канала связи в одном волокне.

Состояние каждого интерфейса SFP+ индицируется светодиодным индикатором, постоянное свечение индикатора указывает на то, что соединение установлено.

Модули SFP/SFP + не входят в комплект поставки оборудования. Их можно дополнительно заказать, предварительно ознакомившись с функциями и стоимостью на сайте http://nsc-com.com/?page=12.

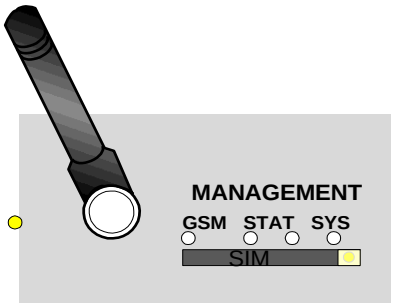
Установка и удаление SFP+ модулей

Подключение SFP-модуля рекомендуется проводить в следующей последовательности:

- Подключить SFP-модуль к оборудованию;
- Подключить оптические кабели к оптическим портам SFP модуля.

Для установки модуля достаточно вставить его в слот устройства до упора. Для снятия трансивера необходимо опустить рычаг () вниз и потянуть трансивер «на себя».

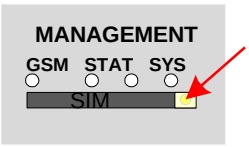
1.3.5 GSM слот



В Sprinter TX реализована возможность подключения к устройству, используя GSM канал.

При подключении с помощью канала связи GSM доступны те же функции, что и при работе по консоли:

1. управление и конфигурирование устройства;
2. мониторинг состояния устройства;
3. обновление ПО.

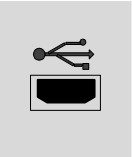


Чтобы была возможность подключиться к устройству по GSM каналу, необходимо установить SIM карту. Для этого извлеките SIM лоток путем нажатия непроводящим предметом (например, зубочисткой) на кнопку. Затем установите SIM карту контактами вверх,

и вставьте лоток в слот устройства.

*Для работы по GSM каналу сотовый оператор должен поддерживать режим **Data Call.***

1.3.6 Последовательный порт (мини-USB)



Для управление мультиплексором в консольном режиме используется последовательный порт, который реализован через мини-USB интерфейс.

USB (англ. Universal Serial Bus) — универсальная последовательная шина, предназначенная для подключения периферийных устройств. Шина USB представляет собой последовательный интерфейс передачи данных для среднескоростных и низкоскоростных периферийных устройств.

Для использования данного интерфейса необходима установка специальных драйверов, которые можно скачать с сайтов в сети Internet.

1.4 Индикация на передней панели

После подачи питающего напряжения желтый индикатор SYS на передней панели отображает состояние мультиплексора.

1.4.1 Состояния индикатора SYS

Свечение индикатора SYS	Состояние мультиплексора
Частое мигание	Процесс начальной загрузки и диагностики мультиплексора
Одна вспышка, пауза	Выполнена начальная загрузка, мультиплексор готов к работе
Четыре вспышки, пауза	Неверный System ID
Медленное мигание	Не загружена программа сопроцессора
Длинная вспышка, пауза	Мультиплексор работоспособен, но необходимо заменить литиевую батарейку
Две длинные вспышки, пауза	Питающее напряжение или температура вне допустимых пределов
Постоянное свечение или его отсутствие	Отказ управляющего микропроцессора

Если после подачи напряжения состояние индикатора SYS не соответствует режиму готовности к работе, выключите электропитание и повторно включите его через несколько секунд. Рекомендуется подключить мультиплексор к управляющему компьютеру с целью диагностики через последовательный порт.

1.4.2 Состояние индикатора GSM

Свечение индикатора GSM	Состояние SIM модуля
Частое мигание	SIM карта не установленна, либо не определяется

Медленное мигание	SIM карты определена, GSM модуль готов к работе
Отсутствие свечения	Неисправен GSM модуль или мультиплексор

1.4.3 Состояние индикаторов STAT

Свечение индикатора STAT	Состояние мультиплексора
Мигание левого индикатора	Выполнена начальная загрузка, мультиплексор готов к работе
Отсутствие свечения левого индикатора	Мультиплексор не работоспособен
Постоянное свечение правого индикатора	Установлено соединение по GSM каналу

1.4.4 Состояние интерфейса Ethernet

Состояние интерфейса **Ethernet** индицируется двумя светодиодными индикаторами, зеленым LINK и желтым ACT, расположенными в разъеме RJ-45 этого интерфейса.

Состояние интерфейса Ethernet	Свечение зеленого индикатора LINK	Свечение желтого индикатора ACT
Соединение не установлено	Выключен	Выключен
Соединение установлено	Постоянное свечение	Выключен
Идет передача данных	Постоянное свечение	Мигание

1.4.5 Состояние интерфейса SFP+

Состояние интерфейса SFP+	Свечение индикатора
Соединение установлено	Постоянное свечение
Соединение не установлено / установлено неверно	Отсутствие свечения

1.5 Соответствие стандартам

Мультиплексор соответствует стандартам

IEEE 802.1 d, IEEE 802.1 w, IEEE 802.1 s, IEEE 802.1 p, IEEE 802.1 q, IEEE 802.3, IEEE 802.3d, IEEE802.3z

1.6 Комплект поставки

В базовый комплект поставки мультиплексора Sprinter TX входят:

- мультиплексор выбранного исполнения;
- выбранные блоки питания;
- клеммная кабельная часть для подключения к источнику постоянного напряжения питания;

- кабель питания для подключения к источнику переменного напряжения 220В;
- документация;
- упаковочная коробка.

2 Протоколы

2.1 Протокол резервирования STP (Spanning Tree Protocol)

STP (англ. *Spanning Tree Protocol* - протокол разворачивающегося дерева) — сетевой протокол, работающий на втором уровне модели OSI. Основан на одноименном алгоритме, разработчиком которого является Радья Перлман (англ. Radia Perlman).

Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов. Происходит это путем автоматического блокирования ненужных в данный момент для полной связности портов. Протокол описан в стандарте IEEE 802.1D.

Принцип действия STP:

- В сети выбирается один *корневой мост*.
- Далее каждый, отличный от корневого, мост просчитывает кратчайший путь к корневому. Соответствующий порт называется *корневым портом*. Он у любого не корневого коммутатора только один!
- После этого для каждого сегмента сети просчитывается кратчайший путь к корневому порту. Мост, через который проходит этот путь, становится назначенным для этой сети. Непосредственно подключенный к сети порт моста — назначенным портом.
- Далее на всех мостах блокируются все порты, не являющиеся корневыми и назначенными. В итоге получается древовидная структура (математический граф) с вершиной в виде корневого коммутатора.

Алгоритм действия STP

- После включения коммутаторов в сеть, по умолчанию ***каждый*** (!) коммутатор считает себя корневым (root).
- Затем коммутатор начинает посылать по всем портам конфигурационные Hello BPDU пакеты раз в 2 секунды.
- Исходя из данных Hello BPDU пакетов, тот или иной коммутатор приобретает статус root, т.е. корня.
- После этого все порты кроме root port и designated port блокируются.
- Происходит посылка Hello-пакетов раз в 20 секунд либо при пропадании/восстановления какого-нибудь линка, с целью препятствия появления петель в сети.

2.2 Rapid Spanning Tree Protocol (RSTP)

RSTP (англ. *Rapid spanning tree protocol* - быстрый протокол разворачивающегося дерева) характеризуется значительными усовершенствованиями STP, среди которых необходимо отметить уменьшение времени сходимости и более высокую устойчивость.

Принцип работы в общих чертах похож на STP: выбирается корневой коммутатор, к которому, каждый из участвующих в построении дерева коммутатор, ищет кратчайший маршрут (с учётом пропускной способности канала) через соседние коммутаторы (или напрямую). Линии, не попавшие в маршрут, переводятся в режим ожидания и не используются для передачи данных, пока работают основные линии. В случае выхода из строя основных линий, ожидающие линии

используются для построения альтернативной топологии, после чего одна из линий становится активной, а остальные продолжают находиться в режиме ожидания.

2.2.1 Настройка RSTP

Режим RSTP включается на каждом порту отдельно, по умолчанию он выключен. Существует возможность блокировать порты, на которых выключен RSTP, если на них начинают приходить BPDU-пакеты. Для включения и отключения RSTP на порту используется команда *ethmode* с ключом *-p*

- ***ethmode*** *<port number> [-p no|rstp]*

-p	режим резервирования – может быть одним из: *no, rstp*;

Для настройки и просмотра параметров RSTP по каждому порту используется команда *rstp* с различными ключами.

rstp *[<port number>] [-i port priority] [-e yes|no] [-c port cost] [-p yes|no|auto] [-g no|yes] [-z]*

-i	чем меньше port priority – тем выше приоритет порта, может принимать значения от 0 до 240, по умолчанию 128;
-e	edge port – крайний порт; если включен, то переводится в режим передачи при подключении внешней сети, без задержки;
-c	стоимость соединения, чем меньше стоимость соединения – тем выше приоритет порта, значение по умолчанию зависит от скорости соединения: 10 Mb/s: Cost=2 000 000 100 Mb/s: Cost=200 000 1000 Mb/s: Cost=20 000
-p	включение/выключение соединения типа точка-точка;
-g	включение/выключение функции Root Guard;
-z	запрещает сохранение изменений в файле конфигурации.

Для настройки и просмотра параметров RSTP для устройства, используйте команду *rstpbridge*.

- ***rstpbridge*** *[-p bridge priority] [-f forward delay] [-h hello time][-a max message age] [-z]*

-p	чем меньше значение bridge priority – тем больше приоритет устройства; может принимать значения от 0 до 61440, по умолчанию 32768;
-f	задержка переключения порта в режим Forwarding (в секундах); может принимать значения от 4 до 30, по умолчанию 15;
-h	интервал посылки пакетов BPDU (в секундах); может принимать значения от 1 до 10, по умолчанию 2;
-a	максимальное время жизни пакета (в секундах); может принимать значения от 6 до 40, по умолчанию 8;
-z	запрещает сохранение изменений в файле конфигурации.

Для настройки и просмотра параметров блокировки портов, используйте команду *stp.*

➢ ***stp*** *[-b no|dis|pdown] [-m minutes] [-z]*

-b	метод отключения портов в случае нарушения режима untrusted: no – отсутствие блокировки, dis – блокировка порта, pdown – включение режима Power down порта;
-m	время блокировки порта при получении BPDU-пакета в минутах (0 для перманентной блокировки до принудительного включения администратором);
-z	запрещает сохранение изменений в файле конфигурации.

Пример конфигурации:

Пусть имеется несколько устройств, которые необходимо объединить в кольцо. Устройства соединены между собой портами 0 и 1.

Для включения RSTP необходимо на каждом устройстве выполнить команды *ethmode 0,1 –p rstp*.

Обратите внимание, что замыкать кольцо необходимо только после включения RSTP на всех устройствах, задействованных в кольце!!!

В случае возникновения каких-либо проблем в работе или настройке RSTP необходимо связаться со службой технической поддержки и предоставить результаты выполнения команд *show cfg.sys, rstp, rstpbridge, stp, ethstat, ethstat -b*

Устройство может прозрачно пропускать BPDU-пакеты, не обрабатывая их. Такая необходимость иногда возникает при замыкании кольца на стороннем оборудовании, для того чтобы Sprinter никак не участвовал в построении дерева RSTP.

Для включения прозрачного BPDU-режима необходимо выполнить следующие команды:

ethmode *–p no* на всех портах устройства
switchcfg *–b no*

2.3 IGMP (Internet Group Management Protocol)

IGMP (англ. *Internet Group Management Protocol* — протокол управления группами Интернета) — протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы, а также для поддержки потокового видео и онлайн игр.

2.3.1 Характеристики IGMP

Важные характеристики многоадресной IP-рассылки:

1. Членство в группах динамическое, что позволяет узлам присоединяться к группе и покидать ее в любое время.
2. Присоединение узлов к группам многоадресной рассылки обеспечивается с помощью IGMP-сообщений.
3. Группы не ограничены по размеру и их члены могут быть разбросаны по различным IP-сетям (если маршрутизаторы, которыми соединены эти сети, поддерживают распространение многоадресного IP-трафика и информации о членстве в группах).
4. Узел может отправлять IP-трафик по IP-адресу группы, не будучи сам членом этой группы.

При согласовании работы нескольких маршрутизаторов, один из них выбирается в качестве "ведущего". Этот маршрутизатор отслеживает принадлежность к группе multicast рассылки. IGMP используется для определения, какие из принимаемых пакетов, маршрутизатор должен передавать в подключенные к нему подсети. Маршрутизатор, приняв пакет групповой рассылки, проверяет, есть ли хотя бы один член группы multicast рассылки, который сделал запрос на прием этих пакетов. Если да, то пакет продвигается, если не существует ни одного члена группы многоадресной рассылки - пакет отбрасывается.

Для каждой группы есть один маршрутизатор, который работает в режиме распределения пакетов, предназначенных для этой группы. Это означает, что если есть три маршрутизатора групповой рассылки, подключенных к сети, их групповые идентификаторы (groupids) — единственные.

Конечные пользователи, которым необходимо получать multicast пакеты, должны иметь возможность сообщить ближайшим маршрутизаторам о своем желании стать членом группы многоадресной рассылки и получать пакеты, предназначенные этой группе.

Существует понятие *членства в группе*. Когда хост имеет членство, это означает, что один из его процессов получает multicast пакеты от некоторой группы. Когда маршрутизатор имеет членство - сеть, подключенная к другому его интерфейсу, получает эти multicast пакеты. В обоих случаях, сохраняется список групповых идентификаторов и транслируется их запрос к «ведущему» маршрутизатору.

2.3.2 Объединение групп

Хост или маршрутизатор могут присоединиться к группе. Хост поддерживает список процессов, которые имеют членство в группе. Когда процесс хочет присоединиться к новой группе, он посылает свой запрос хосту. Хост добавляет имя процесса и имя требуемой группы к списку. Если присоединение от хоста к группе выполняется впервые, то посылается сообщение

членства. Если это не первый запрос, то сообщение не отсылается, так как хост — уже член группы; он уже получает multicast пакеты от этой группы.

Маршрутизатор в данном случае действует подобно хосту, т.е. при необходимости присоединения одного из интерфейсов к группе, маршрутизатор отсылает сообщение членства. Но при этом у маршрутизатора список группы намного более широк, потому что он накапливает членов, которые соединены с его интерфейсами.

Обратите внимание, что сообщение членства рассылают из всех интерфейсов, кроме того, от которого прибывает запрос.

2.3.3 Настройка IGMP

Устройства Sprinter TX поддерживают IGMP версии 2 и 3.

Для включения и выключения обработки IGMP-пакетов на порту используйте команду *ethmode* с ключом *-i*

- ***ethmode*** *<port number> [-i no|yes]*

- i	запрещает/разрешает IGMP snooping;

Для включения и выключения обработки IGMP-пакетов на устройстве используйте команду *igmp*

- ***igmp*** *[-d] [-e] [-f ports] [-r ports] [-s ports] [-v VLAN] [-z][-d][-e][-f][-a]*

-d	выключение IGMP;
-e	включение IGMP;
-f	указание списка портов, для которых нужно использовать fast leave режим;
-q	список портов, на которых отключен режим fast leave;
-r	список пользовательских портов, которые должны отдавать multicast -вещание конечному пользователю;
-s	список портов, принимающих multicast - вещание от сервера (источники);
–v	устанавливает VLAN ID 802.1p для потоков multicast (MVR режим), метка задается как десятичное число от 1 до 4095. 0 – означает отсутствие метки;
-z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Настройка IGMP на одном устройстве – необходимо включить IGMP и разрешить на всех портах IGMP snooping:

- ***igmp*** *–e*
- ***ethmode*** *0,1,2,3 –i yes*

Настройка MVR. Пусть multicast - вещание идет в 200 VLAN, порты 0 и 1 – источники, 2 и 3 – пользовательские, тогда устройство необходимо сконфигурировать следующим образом:

- ***igmp*** *–e*
- ***igmp*** *–v 200*
- ***igmp*** *–s 0,1*
- ***igmp*** *–r 2,3*

- ***ethmode*** *0,1,2,3 –i yes*

Чтобы устройство прозрачно пропускало весь multicast необходимо выполнить следующие команды:

- ***igmp*** *–d*
- ***ethmode*** *0,1,2,3 –i no*

2.4 DHCP (Dynamic Host Configuration Protocol)

DHCP (англ. *Dynamic Host Configuration Protocol* — протокол динамической конфигурации узла) - это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

2.4.1 Назначение DHCP

Для использования протокола TCP/IP в сети администратор должен задать для каждого из компьютеров, по меньшей мере, три параметра - IP-адрес, маску подсети и адрес используемого по умолчанию шлюза. При этом каждый компьютер должен иметь уникальный IP-адрес. Кроме того, присвоенный адрес должен находиться в диапазоне подсети, к которой подключено устройство. В большой сети иногда бывает трудно определить, к какой же из подсетей подключен тот или иной компьютер. Однако DHCP "знает", из какой подсети приходит запрос на получение IP-адреса, и сделает за вас все как надо.

Если в сети используются Windows Internet Naming Service (WINS) и Domain Name Service (DNS), то на каждом из клиентских компьютеров администратору необходимо также указать IP-адреса WINS и DNS-серверов.

2.4.2 Применение DHCP

Протокол динамического конфигурирования DHCP очень удобен, так как настройка стека TCP/IP клиентских машин не требует никакого внимания со стороны администратора. Администратор конфигурирует один или несколько DHCP-серверов так, чтобы они автоматически присваивали IP-адреса каждому компьютеру в сети. Для этого конфигурируется сервер, вводится диапазоны адресов, настраивается несколько дополнительных параметров и периодически осуществлять мониторинг.

С другой стороны, в общем случае адреса назначаются случайным образом, и заранее неизвестно какой хост получит какой адрес. Если нужно сохранить удобство использования DHCP, но при этом сделать так, чтобы адреса были чётко закреплены за каждым компьютером, используется так называемая привязка к MAC-адресу: DHCP-сервер имеет таблицу соответствия MAC-адресов IP-адресам, и назначает IP-адреса в соответствии с этой таблицей. Минус этого решения — необходимость отслеживания MAC-адресов и сопровождения таблицы соответствия.

В некоторых случаях может помочь компромиссное решение — поставить IP-адреса в соответствие не MAC-адресам, а портам коммутатора, к которым подключен клиентский компьютер. Другой вариант — выдавать IP-адреса в зависимости от того, с какого DHCP-ретранслятора пришел запрос. В этом случае выдаются адреса из одной подсети, но с привязкой конкретных диапазонов адресов к различным коммутаторам, работающим как DHCP-ретрансляторы. Это может помочь облегчить администрирование сети в том смысле, что по IP-адресу клиентского компьютера, будет понятно к какому коммутатору он подключен.

По DHCP протоколу могут взаимодействовать две или три стороны:

1. DHCP-клиент — тот, кто хочет получить параметры настройки TCP/IP;
2. DHCP-сервер — тот, кто выдаёт эти параметры;
3. DHCP-ретранслятор (relay agent) — вспомогательный участник, который может играть роль посредника между клиентом и сервером.

DHCP-ретранслятор используется в тех случаях, когда у клиента нет возможности обратиться к серверу напрямую, в частности, в том случае, если они находятся в разных широковещательных доменах. DHCP-ретранслятор обрабатывает стандартный широковещательный DHCP-запрос и перенаправляет его на DHCP-сервер в виде целенаправленного (unicast) пакета, а полученный от DHCP-сервера ответ, в свою очередь, перенаправляет DHCP-клиенту.

Устройства Sprinter TX может выступать в роли DHCP-ретранслятора, при этом выставляя option 82.

Опция 82 DHCP (DHCP option 82) — опция протокола DHCP, использующаяся для того чтобы проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора и через какой его порт был получен запрос.

Получение IP-адреса по DHCP

Устройство Sprinter TX может автоматически получать IP-адрес, используя протокол DHCP. Для этого необходимо выполнить команду *ipconfig -r*

2.4.3 Настройка DHCP Relay

Для отключения и включения режима DHCP relay option 82 на порту используйте команду *ethmode* с ключом *–r*

➢ ***ethmode*** *<port number> [-r no|trunk|user]*

-r	no - запрещает DHCP relay на выбранном порту;
	trunk – включает DHCP relay на порту, который ведет к DHCP-серверу;
	user - включает DHCP relay на порту, к которому подключен конечный пользователь

Для отключения и включения режима DHCP relay option 82 на устройстве используйте команду *dhcprelay*

➢ ***dhcprelay*** *[-d] [-e] [-i IP|-f] [-t ports] [-u ports] [-m minutes] [–b no|dis|pdown] [-v VLAN] [-s] [-z]*

-d	выключение перенаправления DHCP запросов;
-s	показать IP адреса подключенных пользователей;
-e	включение перенаправления DHCP запросов;
-i	IP-адрес DHCP-сервера, на который перенэто я еще не читалаправляются запросы;
-t	указание списка trusted (доверенных) портов;
-u	указание списка untrusted (недоверенных) портов;

-m	время блокировки untrusted порта при получении от него пакета DHCP сервера;
-b	метод отключения портов в случае нарушения режима untrusted: no – отсутствие блокировки, dis – блокировка порта, pdown – включение режима Power down порта;
-f	включение режима широковещательных запросов к DHCP-серверу;
–v	устанавливает VLAN ID 802.1p для перенаправляемых запросов, метка задается как десятичное число от 1 до 4095. 0 – означает отсутствие метки;
-z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Необходимо настроить DHCP relay. Пусть порты 0-20 - пользовательские, порты 21, 22 – транковые. Если на пользовательском порту пытается обнаружиться DHCP-сервер, то необходимо заблокировать этот порт на 10 минут. Для этого необходимо выполнить следующие команды:

- ***ethmode*** *0-20 –r user*
- ***ethmode*** *21,22 –r trunk*
- ***dhcprelay*** *–e*
- ***dhcprelay*** *–u 0-20*
- ***dhcprelay*** *–t 21,22*
- ***dhcprelay*** *–b dis –m 10*

2.5 SNMP (Simple Network Management Protocol)

SNMP (англ. *Simple Network Management Protocol* — протокол простого управления сетями) - это протокол управления сетями связи на основе архитектуры TCP/IP.

Это технология, призванная обеспечить управление и контроль за устройствами и приложениями в сети связи, путём обмена управляющей информацией между агентами, располагающимися на сетевых устройствах, и менеджерами, расположенными на станциях управления. В настоящее время SNMP является базовым протоколом управления сети Internet. SNMP определяет сеть как совокупность сетевых управляющих станций и элементов сети (главные машины, шлюзы и маршрутизаторы, терминальные серверы), которые совместно обеспечивают административные связи между сетевыми управляющими станциями и сетевыми агентами.

Обычно при использовании SNMP присутствуют управляемые и управляющие системы. В состав управляемой системы входит компонент, называемый агентом, который отправляет отчёты управляющей системе. По существу SNMP агенты передают управленческую информацию на управляющие системы как переменные (такие как «свободная память», «имя системы», «количество работающих процессов»).

Управляющая система может получить информацию через операции протокола GET, GETNEXT и GETBULK. Агент может самостоятельно без запроса отправить данные, используя операцию протокола TRAP или INFORM. Управляющие системы могут также отправлять конфигурационные обновления или контролирующие запросы, используя операцию SET для непосредственного управления системой. Операции конфигурирования и управления используются только тогда, когда нужны изменения в сетевой инфраструктуре. Операции мониторинга обычно выполняются на регулярной основе.

Переменные доступные через SNMP организованы в иерархии. Эти иерархии и другие метаданные (такие как тип и описание переменной) описываются Базами Управляющей Информации (англ. Management Information Bases (MIBs)).

2.5.1 Настройка SNMP

Команда *Snmpcom* устанавливает имена snmp community.

- ***snmpcom*** *[-r read community] [-w write community] [-t trap community] [-z]*

read community	используется для аутентификации при чтении (по умолчанию “public”);
write community	используется для аутентификации при записи (по умолчанию “public”);
trap community	используется для аутентификации при передачи trap'ов (по умолчанию “public”);
-z	запрещает сохранение внесенных изменений в файле конфигурации.

Команда *Snmptrapip* устанавливает параметры *snmp trap.*

- ***snmptrapip*** *[ip] [-d|-e] [-v 1|2c] [-z]*

ip	IP адрес управляющей станции принимающей send traps;
-d	запретить посылку traps;
-e	разрешить посылку traps;
-v	версия SNMP (1 или 2c);
-z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Активировать snmp traps.

- ***snmptrapip*** *192.168.0.1 –e*

2.6 VLAN (Virtual Local Area Network)

VLAN (англ. *Virtual Local Area Network* — виртуальная локальная компьютерная сеть) – группа хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети.

VLAN могут являться частью большего LAN, имея определенные правила взаимодействия с другими VLAN, либо быть полностью изолированными от них.

Простейший механизм изоляции различных подсетей, работающих через общие коммутаторы и маршрутизаторы, известен как 802.1Q.

Преимущества VLAN

- Увеличивает число широковещательных доменов, но уменьшает размер каждого широковещательного домена. Тем самым, уменьшается широковещательный и многоадресный сетевой трафик;
- Увеличивают безопасность сети из-за ограничения взаимодействия членов различных сегментов на 1-2 уровнях;

- По сравнению с реализацией на раздельных коммутаторах, уменьшает количество оборудования, хотя требует обязательного использования более дорогих управляемых коммутаторов;
- В случае использования соответствующего оборудования, позволяет разделить данные по различным сегментам сети в зависимости от их типа (например, обеспечить приоритетную передачу голосового трафика);
- Конфигурирование VLAN в сложных сетях требует применения специализированных протоколов (GVRP) или существенного объёма ручной работы;
- При использовании протокола ISL требуется абонентское оборудование, понимающее этот протокол (поддерживается малым количеством пользователей);
- Использование IEEE 802.1Q требует использования коммутаторов, поддерживающих (как минимум) стандарт 802.3ab, стандартное оборудование 802.3u может уничтожать часть фреймов как нарушающие стандарт;
- В случае статической конфигурации, оконечное оборудование теряет функциональность plug-n-play (так как порты коммутатора становятся не взаимозаменяемыми).

2.6.1 Протоколы и принцип работы

Наиболее простой вариант использования VLAN заключается в отнесении каждого порта одного свитча конкретного VLAN, что позволяет разделить физический коммутатор на несколько логических. (Например, порты 1-5,7 — это VLAN № 3, порты 6,9-12 — VLAN № 2). При этом пакеты из одного VLAN не передаются в другой VLAN.

VLAN № 1 (Native VLAN, Default VLAN) используется по умолчанию и не может быть удален. Весь трафик (не тегированный или не направленный явно в конкретный VLAN) переходит, по умолчанию, в VLAN № 1.

Имеется ограничение на число VLAN в одной сети.

Наиболее распространен сейчас VLAN, основанный на протоколе тегирования IEEE 802.1Q. Этому предшествовали другие протоколы, такие как Cisco ISL (Inter-Switch Link, вариант IEEE 802.10) и VLT (Virtual LAN Trunk), предложенный 3Com.

Изначально VLANы применяли с целью уменьшения коллизий в большом цельном сегменте сети Ethernet, и тем самым увеличивали производительность. Появление Ethernet-коммутаторов решало проблему коллизий, и VLAN стали использовать для ограничения широковещательного домена на канальном уровне (по MAC-адресам). Виртуальные сети также могут служить для ограничения доступа к сетевым ресурсам, не влияя на топологию сети.

Виртуальные сети работают на канальном (2-ом) уровне модели OSI. Но VLAN часто настраивают для непосредственной работы с IP-сетями или подсетями, вовлекая сетевой уровень. В частности, на некоторых коммутаторах возможно направление пакетов в различные VLAN'ы в зависимости от адресов получателя/отправителя, портов и общей загруженности канала (англ. Policy based VLAN).

2.6.2 Тегирование трафика

Trank VLAN — это физический канал, по которому передается несколько VLAN каналов, которые различаются тегами (метками, добавляемыми в пакеты). Такой трафик называется *тегированый* и обычно создается между устройствами свитч-свитч или свитч-

маршрутизатор. Маршрутизатор (свитч третьего уровня) выступает в роли магистрального ядра сети (backbone) для сетевого трафика разных VLAN.

Протокол VTP (VLAN Trunking Protocol) предусматривает VLAN-домены для упрощения администрирования. VTP также выполняет «чистку» трафика, направляя VLAN трафик только на те коммутаторы, которые имеют целевые VLAN-порты.

2.6.3 Обозначение членства в VLAN

Для этого существуют следующие решения:

- *по порту (Port-based, 802.1Q)*

Порту коммутатора вручную назначается одна VLAN. В случае, если одному порту должны соответствовать несколько VLAN (например, если соединение VLAN проходит через несколько свитчей), то этот порт должен быть членом транка.

Метки Native VLAN свитч будет добавлять ко всем принятым кадрам не имеющим никаких меток.

VLAN, построенные на базе портов, имеют некоторые ограничения. Они очень просты в установке, но позволяют поддерживать для каждого порта только одну VLAN. Следовательно, такое решение мало приемлемо при использовании концентраторов или в сетях с мощными серверами, к которым обращается много пользователей (сервер не удастся включить в разные VLAN). Кроме того, вносить изменения в VLAN на основе портов достаточно сложно, поскольку при каждом изменении требуется физическое переключение устройств.

- *по MAC-адресу (MAC-based)*

Членство в VLANe основывается на MAC-адресе рабочей станции. В таком случае свитч имеет таблицу MAC-адресов всех устройств вместе с VLANами, к которым они принадлежат.

- *по протоколу (Protocol-based)*

Данные 3-4 уровня в заголовке пакета используются чтобы определить членство в VLANe. Например, IP-машины могут быть переведены в первую VLAN, а AppleTalk-машины во вторую. Основной недостаток этого метода в том, что он нарушает независимость уровней, поэтому, например, переход с IPv4 на IPv6 приведет к нарушению работоспособности сети.

- *методом аутентификации (Authentication based)*

Устройства могут быть автоматически перемещены в VLAN основываясь на данных аутентификации пользователя или устройства при использовании протокола 802.1x.

2.6.4 Настройка VLAN

Для задания режима порта используйте команду *ethmode* с ключом *–m.* Для задания VLAN'а порта используйте команду *ethmode* с ключом *–v.*

➢ ***ethmode*** *<port number> [-m mode] [-v VLAN]*

-m	режим работы – может быть одним из: **down, trunk, multi, access, qinq**;
-v	идентификатор VLAN;

Интерфейс может работать в одном из следующих режимов:

down	интерфейс выключен;
trunk	интерфейс пропускает только тегированные кадры;
milti	интерфейс пропускает все кадры;
access	интерфейс используется для передачи пользовательских данных;
qinq	режим double tagging.

Для задания VLAN'а управления используйте команду *ipconfig* с ключом *–v.*

- ***ipconfig*** *[-v VLAN]*

-v	метка VLAN для управления (0 для отсутствия тегирования);

Для просмотра и ручной конфигурации таблицы VLAN'ов используйте команду *vlan*

vlan *[VLAN ID] [-n name] [-d] [-p ports_list] [-t ports_list] [-u ports_list] [-b db] [-s] [-z]*

-n	символическое описание заданного идентификатора VLAN ID;
-d	удалить заданный идентификатор VLAN;
-p	список портов, принадлежащих к VLAN; на выходе этих портов фреймы не изменяются; если идентификатор VLAN ID не задан, то показывается список всех VLAN, к которым принадлежат эти порты;
–t	список портов, принадлежащих к VLAN; на выходе этих портов фреймы тегируются;
-u	список портов, принадлежащих к VLAN; на выходе этих портов снимаются теги фреймов;
-s	показывает информацию о заданном идентификаторе VLAN ID;
–b	номер базы MAC для определения маршрутизации;
–z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример: Добавить идентификатор VLAN равный 100 для портов 0,2,3

- *vlan 100 -p 0,2,3*

#	*VID*	*name*	*0*	*1*	*2*	*3*	*cpu*	*slv*
0	*1*	*Eth port*	*M*	*M*	*M*	*M*	*M*	*M*
1	*100*	*user*	*M*		*M*	*M*		

Показать список VLAN, к которым принадлежат порты 1,2

- *vlan -p 2,3*
  port 1

member vlans *: 1*
port 2

3 Функционирование мультиплексора

Для правильной работы мультиплексоров в сети их необходимо надлежащим образом сконфигурировать. Все настройки мультиплексора сохраняются в файле *"/mnt/cfg.sys"* в виде последовательности команд конфигурирования, выполняющихся при старте устройства. При вводе консольных команд результат исполнения может быть сохранен в файле конфигурации автоматически. Сформированный файл может быть записан в каталог "mnt" мультиплексора по протоколу Xmodem или через сеть по протоколу FTP. Содержимое этого файла может быть выведено в окне терминала командой

show /mnt/cfg.sys.

При каждом включении мультиплексор настраивается, выполняя построчно команды, указанные в текстовом файле cfg.sys. Файл расположен в каталоге mnt в флэш-памяти устройства.

3.1 Файловая система

Файловая система мультиплексора объединяет в себе собственно файлы, идентификаторы процессов, устройства и т п. Структура файловой системы:

- dev
- mnt
  - kernel.bin
  - kernel.bkb
  - fwXXX.rbf
  - log
  - cfg.sys
  - menu
  - htdocs
- svc
- sys

Исходные файлы управляющей программы и файлы конфигурации и диагностики находятся в директории /mnt. Назначение и содержимое этих файлов следующее:

kernel.bin	Управляющая программа мультиплексора. Эта программа запускается начальным загрузчиком каждый раз при включении устройства. Поставляется изготовителем. Может быть заменена пользователем при обновлении программного обеспечения. При отсутствии этого файла и его резервной копии мультиплексор может быть загружен только через вспомогательный последовательный порт с использованием команд начального загрузчика.
kernel.bkb	Резервная копия управляющей программы. Загружается при включении устройства при отсутствии или нарушении контрольной суммы файла kernel.bin.
fwXXX.rbf	Драйвер аппаратной части устройства. Поставляется изготовителем и может быть заменен пользователем при обновлении программного обеспечения. XXX – соответствует версии аппаратной части мультиплексора.
log	Протокол событий. Создается автоматически при первом включении устройства. Может быть просмотрен соответствующими командами.
menu	Файл системы меню мультиплексора. Поставляется изготовителем, заменяется при обновлении программного обеспечения. Может быть модифицирован для добавления или изменения пунктов меню.

cfg.sys	Файл конфигурации устройства. Поставляется изготовителем, его необходимо изменить для правильной работы устройства в конкретной сети пользователя. Этот текстовый файл содержит набор строк, каждая строка которого представляет собой команду управления устройством. При каждом включении устройства управляющая программа исполняет все команды в том порядке, в котором они встречаются в этом файле. Минимальный набор команд, указанных в этом файле, обязательно должен содержать ipconfig для указания IP адреса локального устройства.
htdocs	Папка, содержащая файлы встроенного веб сервера, обеспечивающего управление по протоколу http через браузер.

3.2 Работа с файловой системой

Для доступа к файловой системе мультиплексора может использоваться FTP клиент в пассивном режиме и Xmodem через консоль.

3.2.1 Работа по протоколу FTP

Мультиплексор содержит встроенный FTP-сервер, обеспечивающий наглядную и удобную работу с его файловой системой. Чтение и запись файлов производится при помощи FTP-клиента. Программа должна использовать пассивный режим обмена (passive mode). Например, в Internet Explorer этот режим устанавливается так: Tools->Internet Options->Advanced->Use passive FTP; в Total Commander надо при создании нового FTP соединения установить галочку на Use passive mode for transfers. Доступ к FTP серверу имеет только привилегированный пользователь admin.

3.2.2 Работа по протоколу Xmodem

Для управления в консольном режиме подключите один конец консольного кабеля с мини-USB разъемом к консольному порту мультиплексора, а другой – к USB порту Вашего компьютера.

Для работы по консоли на Вашем компьютере должна быть установлена коммуникационная программа эмуляции терминала (такая, как HyperTerminal) с установками: эмуляция терминала VT100, без контроля четности, 8 битов данных, 1 стоп-бит, без управления потоками и скорость порта 115200 бит/с.

Данный протокол не передает размер файла, поэтому его необходимо указывать самостоятельно. Для загрузки любого файла (программное обеспечение или загрузочная конфигурация) необходимо выполнить на мультиплексоре команду upload с указанием пути, куда сохранять принимаемый файл и размера этого файла. На терминал начнут выводиться символы “C” – управляющая последовательность протокола, означающая готовность к приему данных. После этого следует указать терминальной программе пересылаемый файл и инициировать передачу. Пересылка файла может занять несколько десятков секунд, в зависимости от его размера.

Пример: Загрузка файла *cfg.sys* размером 177 байт с помощью программы HyperTerminal.

- ***upload /mnt/cfg.sys 177***

Transfer->Send file-> Выбрать *cfg.sys* и протокол *Xmodem*

После окончания передачи файл будет сохранен во флэш-памяти согласно указанным параметрам.

3.3 Пользователи и пароли

Для выполнения команд конфигурации и диагностики, а также для изменения и обновления программного обеспечения возможен как локальный, так и удаленный доступ к мультиплексору. Оба вида доступа содержат единый механизм защиты от несанкционированного доступа, основанный на идентификации по имени пользователя и паролю. Устройство поддерживает идентификацию трех различных пользователей: привилегированного с именем admin и непривилегированных с именами oper1 и oper2. Привилегированный пользователь может изменять настройки устройства и обновлять программное обеспечение, непривилегированные пользователи могут только просматривать диагностические сообщения.

Производитель устанавливает по умолчанию следующие пароли:

Имя пользователя	Пароль
admin	admin
oper1	oper1
oper2	oper2

Перед эксплуатацией устройства в целях безопасности необходимо изменить эти пароли командой passwd. Новые пароли могут представлять последовательность латинских букв и цифр длиной до 18 символов включительно.

Информация о паролях мультиплексора хранится в файле *"/mnt/config.sys"* в зашифрованном виде. В алгоритме шифрования используется серийный номер конкретного устройства, поэтому при переносе этого файла на другой мультиплексор он не будет загружен. При удалении *config.sys* (эта операция доступна только администратору) пароли примут значения по умолчанию.

3.4 Системные параметры

В этой главе описываются основные параметры мультиплексора.

3.4.1 Встроенные календарь и часы

Мультиплексор имеет встроенные часы реального времени и календарь с батарейным питанием. Они используются для указания времени возникновения событий в журнале. При каждом старте мультиплексор проверяет сохраненную в энергонезависимой памяти часов информацию и при ошибке чтения индицирует и необходимости сменить литиевую батарею часов.

Системные время и дату можно изменить с помощью консольных команд *date* и *time*, а также с помощью меню и SNMP агента.

3.4.2 Символическое имя мультиплексора

Каждый мультиплексор может иметь символическое имя, выводимое в подсказке консоли и облегчающее идентификацию мультиплексора. Имя мультиплексора можно изменить с помощью команды *setdevname*, а также с помощью меню и SNMP агента.

3.4.3 Адрес в сети

Изготовитель устанавливает каждому мультиплексору уникальный MAC-адрес, зависящий от аппаратного серийного номера устройства. При изменении MAC-адреса устройства необходимо следить за несовпадением адресов у различных узлов сети.

MAC адрес, IP адрес, маску и шлюз по умолчанию можно изменить с помощью команд *setmac* и *ipconfig* соответственно, а также с помощью меню и SNMP агента.

3.4.4 Доверенные узлы

По соображениям безопасности устройство может быть доступно только с выбранных управляющих компьютеров (компьютеров имеющих определенные адреса в сети). Для определения списка доверенных узлов можно использовать конкретные IP-адреса, все адреса текущей подсети (используется адрес и маска сети мультиплексора), а также все узлы всех сетей. Список доверенных узлов может быть изменен с помощью консольной команды *hosts*, а также с помощью меню и SNMP агента.

3.4.5 Таймаут

Если пользователь не вводит команды в течение определенного времени, соединение telnet или ftp будет разорвано мультиплексором. По умолчанию время таймаута составляет 15 мин и может быть изменено командой *timeout*. Время таймаута сбрасывается при каждом выключении мультиплексора.

3.5 Пакетные Ethernet интерфейсы

Ethernet интерфейс - интерфейс оборудования в соответствии со стандартом IEEE 802.3.

Мультиплексор содержит оптические SFP интерфейсы для передачи данных со скоростью 1000 Мбит/с либо 10 Гбит/с а также интерфейсы Ethernet 1000BaseT для передачи данных со скоростью 1000 Мбит/с в соответствии со спецификацией IEEE802.3.

Ethernet-интерфейс мультиплексора может работать в режиме автосогласования, а так же позволяет вручную установить скорость и режим дуплекса (для медных интерфейсов) на каждом интерфейсе в отдельности.

Несоответствие установок скорости и дуплекса на порту Ethernet мультиплексора и порту подключаемого оборудования может приводить к блокировке встроенного Ethernet коммутатора и невозможности передачи данных как через неправильно сконфигурированный порт, так и через другие порты!

Команда *ethmode* настраивает режим работы выбранного пакетного интерфейса, его идентификатор VLAN, скорость, дуплекс, параметры резервирования. Для целей резервирования команда может описывать топологию соединений между мультиплексорами.

Интерфейс может работать в одном из следующих режимов:

down	интерфейс выключен;
trunk	интерфейс пропускает только тегированные кадры, этот режим используется для связи с другим мультиплексором непосредственно;
multi	интерфейс пропускает все кадры; Режим по умолчанию, используемый, если явно не указан другой режим. Политика использования интерфейсов определяется внешним оборудованием, например, маршрутизаторами 3-го уровня, связывающими мультиплексоры;
access	интерфейс используется для передачи пользовательских данных. Пакеты с другим идентификатором VLAN ID не коммутируются в этот интерфейс. Пакеты, поступающие в этот интерфейс, тегируются с идентификатором, равным указанному параметром VLAN ID;
qinq	режим double tagging. На выходе все пакеты тегируются дополнительным идентификатором, равным указанному параметром VLAN ID, на входе дополнительный тег снимается.

4 Локальный и удаленный доступ к мультиплексору

Для выполнения команд конфигурации и диагностики, а также для изменения и обновления программного обеспечения возможен как локальный, так и удаленный доступ к мультиплексору.

4.1 Локальный доступ

Локальный доступ к устройству осуществляется через последовательный порт. Для этого нужно соединить устройство и последовательный порт управляющего компьютера кабелем, и запустить на управляющем компьютере терминальную программу, поддерживающую эмуляцию ANSI терминала и протокол Xmodem передачи файлов, например, Hyperterminal из состава Windows. Параметры настройки последовательного порта компьютера – 115000 кбит/с, 8 бит, без четности, без контроля передачи. После запуска терминальной программы, в ответ на приглашение системы, нужно набрать имя пользователя, а затем пароль, после чего система выведет подсказку:

LPOS>

Далее можно вводить любые команды управления и конфигурации, описанные ниже.

4.2 Удаленный доступ

4.2.1 Удаленный доступ по telnet

Удаленный доступ к устройству осуществляется через сеть IP по протоколу telnet. Для этого нужно подключить один из медных интерфейсов Ethernet к сети и убедиться, что светодиодные индикаторы показывают наличие соединения. Необходимо запустить на управляющем компьютере любую программу – клиент telnet, например, Hyperterminal из состава Windows. Необходимо указать IP адрес мультиплексора, при этом командой *hosts* мультиплексора, в свою очередь, должен быть разрешен доступ к нему управляющего компьютера с данным IP адресом. Можно разрешить доступ только с определенных компьютеров (до пяти IP адресов), со всех компьютеров локальной сети, или с любого компьютера. Доступность мультиплексора можно проверить командой ping с удаленного компьютера.

Настройки программы telnet должны включать эмуляцию ANSI терминала и перевод строки после возврата каретки.

После запуска клиента telnet в ответ на приглашение системы нужно набрать имя пользователя и пароль, после чего система выведет подсказку:

LPOS>

Далее можно вводить любые команды управления и конфигурации, описанные ниже.

Если пользователь не вводит команды в течение определенного времени, соединение telnet будет разорвано мультиплексором из соображений безопасности. По умолчанию время таймаута составляет 15 мин и может быть изменено командой timeout.

4.2.2 Удаленный доступ по FTP

Чтение и запись файлов программного обеспечения при удаленном доступе производится по протоколу FTP. Для этого запустите на удаленном компьютере программу – клиент FTP, например, Internet Explorer. Программа должна использовать passive mode (в IE соответствующие установки ***Tools > Internet Options > Advanced > Use passive mode***). Логин и

пароль для доступа к директории /mnt тот же, что и для привилегированного доступа к устройству. Поддерживаются чтение, запись и удаление файлов.

4.2.3 Удаленный доступ по GSM каналу

Важным способом удаленного доступа к устройству, является доступ по GSM каналу.

Главное преимущество данного подключения – это возможность работать с устройством при потере доступа по telnet, ftp, http, а также отсутствии возможности локального подключения.

Еще одним плюсом является то, что доступ к устройству по GSM каналу возможен как администратору, так и службе технической поддержки производителя мультиплексора (при обращении клиента).

При подключении с помощью канала связи GSM доступны те же функции, что и при работе по консоли:

1. управление и конфигурирование устройства;
2. мониторинг состояния устройства;
3. обновление ПО.

---

*Для работы по GSM каналу сотовый оператор должен поддерживать режим **Data Call.***

---

*Режим **Data Call** по своим характеристикам идентичен обычному голосовому режиму, только при этом передаётся не кодированный звуковой сигнал, а пользовательские данные. Максимальная скорость передачи (которая остаётся неизменной в течение всего сеанса связи) равна 9600 бит/с.*

Для работы с устройством по GSM каналу необходимо:

1. установить SIM карту оператора сотовой связи;
2. ввести команду *phone reset* (ввод этой команды также необходим при замене SIM карты). Как только устройство определит SIM, индикатор GSM на передней панели устройства начнет медленно мигать;
3. добавить номера телефонов, с которых будут совершаться подключения, в память устройства. Для этого вводится команда *phone –add <номер абонента>.*

Далее с удаленного компьютера при помощи GSM модема, либо второго Sprinter TX можно осуществлять подключение к устройству.

5 Конфигурирование мультиплексора

5.1 Команды терминального управления

В этом разделе описаны команды управления и диагностики, доступные с локального терминала (консоли) устройства и удаленно по протоколу telnet. Для набора этих команд необходимо установить соединение с мультиплексором через последовательный порт или через сеть по протоколу telnet. Ввод команды должен завершаться клавишей **<Enter>**.

Справку по всем доступным в данный момент командам можно получить, нажав <TAB> или ввести ?».

Справку по использованию конкретной команды можно получить, набрав:

- *<имя команды> _ <Tab> либо*
- *<имя команды> _ ?*

Все эти команды также могут быть указаны в текстовом файле */mnt/cfg.sys,* по одной команде в строке. В этом случае указанная последовательность команд будет выполнена при старте устройства.

5.1.1 Синтаксис команд

Синтаксис команд, вводимых в командной строке:

команда *[параметр] [ключ [параметр]]*

где:

Команда	строго заданная последовательность символов, определяющая дальнейшие параметры и смысл выполняемого действия.
Параметр	ключевое слово, IP-адрес, маска сети, MAC-адрес, число, слово, строка.
Ключ	знак «-» за которым следует один символ.

Команда, ключи и параметры отделяются друг от друга символами «пробел».

<u>При описании синтаксиса команд используются следующие обозначения:</u>

- в угловых скобках <> указываются обязательные параметры;
- в квадратных скобках [] указываются необязательные параметры;
- символ “|” обозначает логическое “или” – выбор между различными параметрами;
- ключевые слова выделяются жирным шрифтом.

<u>Типы параметров команд:</u>

Ключевое слово – слово несущее определенную смысловую нагрузку, например, название вводимого параметра.

IP-адрес – A.B.C.D – задается в виде четырех десятичных чисел, разделенных точками.

Маска сети – A.B.C.D – задается в виде четырех десятичных чисел, разделенных точками.

MAC-адрес – HH-HH-HH-HH-HH-HH – задается в виде шести групп чисел, разделенных символами “-“ Каждая группа состоит из двух шестнадцатеричных чисел.

Последние пять веденных команд хранятся в буфере. Чтобы воспользоваться ранее введенной командой, необходимо нажать клавишу “↑” (вверх) или “↓” (вниз).

5.1.2 Сообщения об ошибках

В таблице приведены сообщения об ошибках, которые могут выводиться во время работы с командной строкой.

Сообщение об ошибке	Описание ошибки	Рекомендуемые действия
syntax error: invalid parameter	неверный параметр	ввести правильный параметр
syntax error: omitted parameter	пропущен параметр	ввести пропущенный параметр
syntax error: invalid type	неверный тип параметра	ввести параметр правильно
syntax error: missed value	пропущен параметр ключа	ввести пропущенный параметр
syntax error: invalid delimeter	пропущен обязательный разделитель	ввести пропущенный разделитель
privileged comand: no rights enough	команда недоступна пользователю	с помощью команды su войти под именем admin
is not recognized as a command	команда не была идентифицирована, введена ошибочная команда	с помощью справки “?” следует проверить корректность вводимой команды.
open error	открытие файла не удалось	ввести правильное имя файла

5.1.3 Системные команды

Эти команды позволяют просмотреть или изменить параметры операционной системы, сведения об учетных записях пользователей, параметры терминальной сессии и т.п.

help

Печатает список возможных команд, а при указании команды в качестве параметра печатает подсказку по использованию этой команды.

- ***[команда]*** *нажать TAB*

menu

Запустить интерфейс меню определенный в файле /mnt/menu или в указанном в команде файле. Для того чтобы выйти в предыдущий пункт меню, нажмите клавишу Esc два раза.

- ***menu*** *[menu file]*

file	Использовать указанный файл меню;

defmenu

Установить меню как интерфейс по умолчанию, если ключ –d не указан, и интерфейс командной строки как интерфейс по умолчанию, если ключ –d указан.

- ***defmenu*** *[-d]*

-d	интерфейс командной строки как интерфейс по умолчанию.

cls

Очищает экран терминала.

- ***cls***

date

Позволяет просмотреть и установить (установить - только для администратора) текущую дату, используемую мультиплексором. При вводе без параметров выводится текущая дата. Изменить ее можно, указав нужную дату в формате DD.MM.YY в качестве параметра, где DD – день, MM – месяц, YY – год, все числа двухзначные.

- ***date [DD.MM.YY]***

Пример:

Установка даты 1 мая 2011 года.

- ***date*** *01.05.11*

The current date is: *01.05.11*

time

Мультиплексор имеет встроенные часы. Они используются для указания времени возникновения событий в журнале. При вводе без параметров выводится текущее время. Изменить его можно, указав нужное время в формате HH:MM:SS, где HH – часы, MM – минуты, SS – секунды, все числа двухзначные. Часы указываются в диапазоне от 0 до 24. Указание секунд не обязательно. Мультиплексор поддерживает автоматическую синхронизацию с сервером точного времени по протоколу NTP а также автоматический переход на летнее время и обратно.

- ***time*** *[HH:MM[:SS]] [-z time zone] [-i IP] [-s] [-a no|yes][-p days]*

-z	задает часовой пояс региона, в котором находится устройство;
-i	задает IP адрес сервера синхронизации времени;
-s	выполняет синхронизацию времени;
-a	разрешает/запрещает автоматическую синхронизацию времени, которая проводится раз в месяц.
-p	Устанавливает период синхронизации времени в днях(от 1 до 30). Значение по умолчанию равно 7.
-d	устанавливает настройки по умолчанию

Пример:

Установка времени 15 часов 5 минут и шестого часового пояса.

- ***time*** *15:05 –z 6*

The current time is : *15:05:00 (GMT+06:00)*
Internet time server: *62.149.2.1*
Next synchronization: *01.05.11*

Синхронизация с сервером точного времени.

- ***time*** *-s*

The current time is : *15:05:37 (GMT+06:00)*
Internet time server: *62.149.2.1*
Next synchronization: *01.05.11*

passwd

Позволяет изменить пароль данного пользователя или другого пользователя (при указании его имени). Пароль может состоять из латинских букв и цифр и может иметь длину до 18 символов включительно. Во избежание ошибок при вводе пароль вводится два раза. Пользователь admin может изменить пароль любого пользователя.

- ***passwd*** *[имя пользователя]*

Пример:

Изменение пароля пользователя oper1 пользователем admin.

- ***passwd*** *oper1*

Enter old password
Enter new password
Enter new password again

reset

Вызывает сброс и перезапуск управляющего микропроцессора и начальную загрузку всех узлов мультиплексора. Эту команду может выполнять только администратор.

- ***reset***

activate

Активировать (yes) или деактивировать (no) системные сервисы.

- ***activate*** *[-t (no|yes)] [-r (no|yes)] [-h (no|yes)] [-s (no|yes)] [-f (no|yes)]*

-t	telnet сервис;
-r	терминальный сервис (консоль);
-h	http сервис;
-s	сервис snmp агента;
-f	ftp сервис.

Пример:

Активировать агента snmp.

- ***activate*** *-s yes*

snmpcom

Устанавливает имена snmp community.

В мультиплексоре реализован протокол SNMPv1. Модель безопасности этого протокола основана на сообществах (Community-based Security Model). Она

подразумевает лишь аутентификацию на основе «строки сообщества», фактически, пароля, передаваемого по сети в теле сообщения SNMP в открытом тексте.

- ***snmpcom*** *[-r read community] [-w write community] [-t trap community] [-z]*

read community	используется для аутентификации при чтении (по умолчанию “public”);
write community	используется для аутентификации при записи (по умолчанию “public”);
trap community	используется для аутентификации при передачи trap'ов (по умолчанию “public”);
-z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:
Установить имена snmp community.

- ***snmpcom*** *public specific trap*

snmptrapip

Устанавливает параметры snmp trap.

- ***snmptrapip*** *[ip] [-d|-e] [-z]*

ip	IP адрес управляющей станции принимающей send traps;
-d	Запретить посылку traps;
-e	Разрешить посылку traps;
-z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Активировать snmp traps.

- ***snmptrapip*** *192.168.0.1 -e*

setdevname

Изменяет имя мультиплексора, отображаемое в подсказке командной строки. Помогает идентифицировать мультиплексор.

- ***setdevname*** *<имя мультиплексора> [-z]*

-z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:
Установка имени “Gate_1”.
- ***setdevname*** *Gate_1*

Gate_1 >

setdevloc

Изменяет описание местоположения мультиплексора. Помогает идентифицировать мультиплексор.

- ***setdevloc*** *<местоположение> [-z]*

-z	запрещает сохранение внесенных изменений в файле конфигурации.

su

Позволяет заново войти в систему с другим именем пользователя, не разрывая текущего соединения.

- **su** <имя пользователя>

Пример:

Вход в систему под именем admin.

- **su** admin

Enter password
LPOS >

timeout

Указывает время в минутах (или 0, чтобы отключить разъединение по таймауту), в течение которого сессия telnet может находиться в состоянии простоя. Если пользователь не вводит информацию в течение этого времени, из соображений безопасности производится автоматическое разъединение. При исполнении команды с ключом –*s* указанное время сохраняется в энергонезависимой памяти для всех будущих сессий telnet (может исполняться только администратором).

- ***timeout*** *[-s] [минуты]*

-s	сохраняет установленное значение таймаута для всех последующих сессий

Пример:

Установка таймаута, равного 20 минутам, и сохранение его для последующих сессий.

- ***timeout*** *-s 20*

timeout is 20 min

whoami

Показывает имя текущего пользователя (admin, user1, user2).

- ***whoami***

exit

Завершает текущую сессию управления. Останавливает текущую сессию telnet и разрывает соединение.

- ***exit***

ver

- ***ver***

Отображает текущие версии следующих компонентов:

System ID	ID устройства;
Hardware version	модель устройства;
Bootloader version	версия загрузчика;
Software version	версия операционной системы;
Environment probe version	версия программы сопроцессора.

stats

Отображает информацию о мультиплексоре.

- ***stats***

Пример:

- ***stats***

The current date&time *: 01.05.11 19:26:32*
System ID *: TXA5A5A5A5*
Hardware version *: 1424.1.00*
Software version *: LP ARM OS 1.0.8.2SR1 (Apr 15 2011)*
Firmware version *: 1424.1.00*
Bootloader version *: v 1.0.0.9*
Environment probe version *: 14.1*
Descriptor *: Multiplexer*

Case Temperature *: 2.812C*
Physical Address *: 5A-00-3B-33-05-71*
System uptime *: 9 mins*

E1 channels equipped *:*
Ethernet channels equipped: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 , 16, 17, 18, 19, 20, 21, 22, 23, 24, 25*
Features *: rhsfmt*

В строке ***Feature block*** каждая буква означает, возможен ли определенный доступ к устройству:

R – через консоль;

H – по протоколу HTTP;

S – по протоколу SNMP;

F – по протоколу FTP;

M – через консольное меню (команда menu);

T – используя программу telnet.

exec

Выполняет последовательность команд, указанных в файле filename.

- ***exec*** *<filename> [-s]*

-s	Подавляет вывод на экран результатов исполнения команд;

5.1.4 Команды управления файлами

Эти команды позволяют управлять файлами мультиплексора.

cd

Меняет текущий каталог на подкаталог dirname текущего каталога (допускается использовать “/”, “.” и “..” для указания на корневую, текущую и родительскую директории соответственно).

- ***cd*** *<dirname>*

Пример:

Переход в каталог mnt из корневого каталога.

- ***cd*** *mnt*

ls

Выводит список файлов в текущей директории мультиплексора.

- ***ls***

pwd

Выводит имя текущей директории.

- ***pwd***

show

Выводит на консоль содержимое указанного файла.

- ***show*** *<filename>*

Пример:

Вывод содержимого файла cfg.sys.

- ***show*** */mnt/cfg.sys*

ipconfig *-a 192.168.111.21 -m 255.255.255.0 -g 192.168.111.1*
hosts *-g*

mkdir

Создает директорию dirname

- ***mkdir*** *<dirname>*

Пример:

Создание директории htdocs.

- ***mkdir*** *htdocs*

delete

удаляет файл filename.

- ***delete*** *<filename>*

Пример:

Удаление файла cfg_old.txt.

- ***delete*** */mnt/cfg_old.txt*

upload

Инициирует прием файла указанной длины (необходимость этого параметра связана с тем, что в протоколе XModem нет возможности передать длину файла точно) по протоколу XModem, принятый файл сохраняется под указанным именем. Используется только при работе с консоли.

- ***upload <filename> <len>***

Пример:

Передача файла startup.cmd размером 208 байт и его запись в каталог “mnt”.

- ***upload*** */mnt/startup.cmd 208*

CCCCwrite 208

tftpsend

Инициирует передачу файла по протоколу TFTP на указанный сервер.

- ***tftpsend*** *<filename> <tftp server IP> [-r remote file name]*

filename	Имя файла для отправки на tftp сервер
tftp server IP	IP адрес сервера
-r	Имя, под которым файл будет сохранен на tftp сервере. Если не указано, то совпадает с локальным именем файла

Пример:

Передача файла startup.cmd на TFTP сервер с адресом 192.168.0.23.

- ***tftpsend*** */mnt/startup.cmd 192.168.0.23*

tftpget

Инициирует прием файла по протоколу TFTP, принятый файл сохраняется под указанным именем.

- ***tftpget*** *<filename> <tftp server IP> [-r remote file name]*

filename	Имя файла для получения с tftp сервера (под этим именем файл будет сохранен)
tftp server IP	IP адрес сервера
-r	Имя, под которым файл будет запрошен на tftp сервере. Если не указано, то совпадает с локальным именем файла

Пример:

Прием файла startup.cmd байт и его запись в каталог “mnt”, на TFTP сервере файл называется special.cmd.

- ***tftpget*** */mnt/startup.cmd 192.168.0.23 -r special.cmd*

uploadboot

Инициирует прием файла начального загрузчика по протоколу XModem, принятый файл сохраняется в области загрузчика. Используется только при работе с консоли.

Загрузка неверного файла в область загрузчика приведет к невозможности в дальнейшем эксплуатировать мультиплексор!

- ***uploadboot***

setboot

Переносит указанный файл в область загрузчика.

- ***setboot*** *<filename>*

testfs

Производит проверку на целостность файловой системы и поиск потерянных секторов

- ***testfs*** *[-c]*

-c	дополнительно производить поиск потерянных секторов

5.1.5 Команды конфигурации Ethernet и TCP/IP

Эти команды позволяют производить конфигурацию и мониторинг интерфейсов Ethernet. Все интерфейсы Ethernet обозначаются в управляющей программе номерами, в соответствии с указанными на передней панели.

setmac

Устанавливает MAC адрес мультиплексора в формате HH-HH-HH-HH-HH-HH, где H шестнадцатеричная цифра. Эту команду может выполнять только администратор. При самостоятельном изменении MAC-адреса устройства необходимо следить за несовпадением адресов у различных узлов сети. Изготовитель устанавливает каждому мультиплексору уникальный MAC-адрес. После изменения MAC адреса может понадобиться команда *arp –d ** на управляющем компьютере для очистки таблицы соответствия MAC и IP адресов для доступа к мультиплексору.

Изменение MAC-адреса может привести к неправильной работе мультиплексора

- ***setmac*** *[MAC|-d] [-z] [-s]*

-d	Восстановить MAC адрес по умолчанию;
-s	сохранить введенные данные в файл конфигурации, не применяя их немедленно;
–z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Установка MAC-адреса 5A-00-3b-33-05-73.

➢ ***setmac*** *5A-00-3b-33-05-73*

Physical Address . . . : *5A-00-3B-33-05-73*

Ok

ipconfig

Устанавливает IP-адрес мультиплексора, маску подсети и адрес шлюза. Команда без параметров показывает текущие значения. Указанные в команде параметры вступают в силу немедленно после исполнения. Эту команду может выполнять только администратор.

➢ ***ipconfig*** *–a 192.168.0.21 –m 255.255.255.0 –g 192.168.0.1 –s*

Изменение IP-адреса через telnet-сессию приведёт к её разрыву.

➢ ***ipconfig*** *[–a <IP адрес>] [-b <IP адрес slave-мультиплексора>] [-n номер slave-процессора][-m <маска подсети>] [-g <адрес шлюза по умолчанию>] [-v VLAN] [-p vlan PRI] [-s] [–z] [-r] [-i]*

-a	IP-адрес мультиплексора;
-b	устанавливает IP адрес slave-процессора (данный ключ поддерживается только на многопроцессорных устройствах);
-n	устанавливает номер slave-процессора, для которого устанавливается IP адрес ключом -b (данный ключ поддерживается только на двухпроцессорных устройствах);
-m	маска подсети;
-g	IP-адрес шлюза по умолчанию;
-v	метка VLAN для управления (0 для отсутствия тегирования);
-p	биты приоритета, указываемые в метке VLAN для управления;
-s	сохранить введенные данные в файл конфигурации, не применяя их немедленно;
–z	запрещает сохранение внесенных изменений в файле конфигурации.
-r	автоматически устанавливает IP адрес с помощью DHCP.
-i	получить свободный IP адрес из интервала.

Установка по умолчанию:

IP-адрес мультиплексора – 192.168.0.24;

маска подсети – 255.255.255.0;

IP-адрес шлюза по умолчанию – 192.168.0.1.

Пример:

Установка IP-адреса, маски подсети, шлюза по умолчанию и проверка настроек.

➢ ***ipconfig*** *-a 192.168.0.21 -m 255.255.255.0 -g 192.168.0.1*

➢ ***ipconfig***

Physical Address . . . : *5A-00-3B-33-05-71*
IP Address . . . . . : *192.168.0.21*
Subnet Mask. . . . . : *255.255.255.0*
Default Gateway. . . . : *192.168.0.1*

hosts

Позволяет включить определенный IP адрес внешнего компьютера в список адресов, с которых разрешен доступ к мультиплексору для управления (trusted hosts), или исключить его из этого списка. Позволяет установить текущий режим доступа. Без параметров выводит текущий список доверенных узлов. Эту команду может выполнять только администратор.

Изменение списка адресов доверенных узлов через telnet-сессию может привести к её разрыву без возможности восстановления соединения с этого узла, если он исключен из числа доверенных

➢ ***hosts*** *[-g|-l|-p][–a <IP address>[-m <IP mask>]] [–d <IP address>] [-r yes|no] [-f yes|no][-s][-z]*

-g	режим доступа - с любого адреса;
-l	режим доступа - с адресов локальной подсети, а также указанных в списке;
-p	режим доступа - только с адресов, присутствующих в списке;
–a	добавить указанный адрес в список доверенных;
–d	удалить указанный адрес из списка доверенных;
-r	разрешить (yes) или запретить (no) дополнительным процессорам отвечать на внешним запрос ping;
-f	разрешить (yes) или запретить (no) доступ по протоколу FTP к дополнительным процессорам;
-s	сохранить введенные данные в файл конфигурации, не применяя их немедленно;
–z	запрещает сохранение внесенных изменений в файле конфигурации.
-m	режим доступа для адресов, соответствующих маске в формате xxx.xxx.xxx.xxx (используется с ключом –a).

Пример:

Разрешение доступа к мультиплексору только с IP-адреса 192.168.0.15.

➢ ***hosts*** *-p -a 192.168.0.15*

Trusted host list:
192.168.0.15

ethstat

Эта команда показывает текущее состояние выбранных или всех пакетных интерфейсов устройства.

- ***ethstat*** *[номер интерфейса|cpu] [-m] [-c] [-q] [-r] [-h] [full] [-b]*

-m	дополнительно отображается режим работы интерфейса;
-c	дополнительно отображается статистика работы интерфейса;
-q	дополнительно отображается загрузка интерфейса;
-h	показывает распределение прошедших пакетов по размерам;
-r	используется для сброса текущей и общей статистики (доступен только администратору)
-b	дополнительно отображается полная статистика работы интерфейса;
full	показывает полную информацию о порте;

Результат исполнения:

Состояние Ethernet интерфейсов мультиплексора, содержат следующие обозначения:

power down	интерфейс выключен;
no link	соединение не установлено, нет линии;
negotiation in progress	процесс автоопределения не завершен;
OK half duplex 10Mb/s	соединение установлено, режим обмена полудуплексный, скорость 10 Мб в сек;
OK full duplex 10Mb/s	соединение установлено, режим обмена полнодуплексный, скорость 10 Мб в сек;
OK half duplex 100Mb/s	соединение установлено, режим обмена полудуплексный, скорость 100 Мб в сек;
OK full duplex 100Mb/s	соединение установлено, режим обмена полнодуплексный, скорость 100 Мб в сек;
OK full duplex 1000 Mb/s	соединение установлено, режим обмена полнодуплексный, скорость 1 Гб в сек.
OK full duplex 10 Gb/s	соединение установлено, режим обмена полнодуплексный, скорость 10 Гб в сек.

Описание счетчиков, выводимых ключами *–b* и *–c:*

Счетчики на входе	
goodoctets	количество принятых без ошибок байт;

Badoctets	количество принятых с ошибками байт;
unicast	количество принятых unicast-пакетов;
broadcast	количество принятых broadcast-пакетов;
multicast	количество принятых multicast-пакетов;
Pause	количество принятых pause-пакетов;
allignerr	количество принятых пакетов с длиной в нецелое количество байт;
undersize	количество принятых пакетов с длиной меньше 64 байт и верным FCS;
fragments	количество принятых пакетов с длиной меньше 64 байт и неверным FCS;
oversize	количество принятых пакетов с длиной больше максимальной (1522 байта) и верным FCS;
jabber	количество принятых пакетов с длиной больше максимальной (1522 байта) и неверным FCS;
FCSerr	количество принятых пакетов с допустимой длиной (64-1522 байта) и неверным FCS;
discards	количество принятых пакетов, которые были отброшены и не обработаны из-за нехватки места в очереди;
filtered	количество принятых пакетов, которые были отброшены из-за неверного VLAN ID или ограничения MAC-адресов на порту;
Счетчики на выходе	
goodoctets	количество отправленных без ошибок байт;
unicast	количество отправленных unicast-пакетов;
broadcast	количество отправленных broadcast-пакетов;
multicast	количество отправленных multicast-пакетов;
pause	количество отправленных pause-пакетов;
FCSerr	количество пакетов с неверным FCS;
discards	количество пакетов, которые не были переданы из-за нехватки места в очереди;
single	количество успешно посланных пакетов, во время передачи которых возникла только одна коллизия;
multiple	количество успешно посланных пакетов, во время передачи которых возникло больше одной коллизии;
excessive	количество непереданных пакетов из-за того, что возникло 16 коллизий подряд;

late	количество коллизий, в которые попали больше 512 бит;
collisions	количество остальных коллизий;
deffered	количество посланных пакетов, которые были задержаны из-за занятости передающей среды во время первой попытки.

Счетчики *single, multiple, excessive, late, collisions, deffered* изменяются только в *half-duplex* режиме.

ethmode

Эта команда настраивает режим работы выбранного пакетного интерфейса устройства, его идентификатор VLAN, скорость, дуплекс и параметры резервирования. Для целей резервирования команда может описывать топологию соединений между мультиплексорами. Для каждого фрагмента сети, участвующего в кольце, требуется сконфигурировать каждый интерфейс, участвующий в резервировании или передаче данных между мультиплексорами.

- ***ethmode*** *<port number> [-m mode] [-d 802.3mode] [-v VLAN] [-n monitor] [-s nolearn|mac|no] [-p no|rstp] [-c tag|ip|tagip|iptag|no] [-o pri] [-i no|yes] [-z] [-x port] [-q maxMAC] [-r no|yes] [-e] [-f VLAN ID] [-a]*

-m	режим работы – может быть одним из: **down, trunk, multi, access, qinq**;
-p	режим резервирования – может быть одним из: **no, rstp**;
-v	идентификатор VLAN;
-d	скорость и дуплекс может быть одним из **auto, half10, full10, half100, full100, full1000,auto10, full1000, full 10G**;
–s	режим безопасности – может быть одним из: **nolearn** – отключает автоматическое добавление MAC-адресов, с которых приходят пакеты в указанный порт; **mac** - разрешает доступ к указанному порту только MAC-адресам, хранящимся в таблице MAC-адресов (добавить необходимый адрес можно с помощью команды mapmac); **no** – отключает режим безопасности (значение по умолчанию);
–n	определяет интерфейс, в который будут копироваться все входящие и исходящие фреймы этого интерфейса, -1 если нет интерфейса для мониторинга;
–q	ограничивает количество MAC адресов подключенных к порту указанным значением (0 – отключает ограничения, максимальное значение 255);
–c	способ установления приоритетов - может быть одним из: **tag, ip, tagip, iptag, no**; определяет заголовки протокола и порядок определения приоритета;
–o	определяет приоритет по умолчанию (если нет соответствующих заголовков фрейма, или опция -c установлена в no); может принимать значение от 0 до 7;
-i	запрещает/разрешает IGMP snooping;

-r	запрещает/разрешает DHCP relay;
–e	снимает блокировку порта, установленную при нарушении правил безопасности;
-f	задать VLAN ID принудительно (no|yes)
–z	запрещает сохранение внесенных изменений в файле конфигурации;
–x	копирует конфигурацию из указанного порта.
-a	режим smart vlan (no|yes)

режимы работы

Интерфейс может работать в одном из следующих режимов:

down	интерфейс выключен;
trunk	интерфейс пропускает только тегированные кадры;
milti	интерфейс пропускает все кадры;
access	интерфейс используется для передачи пользовательских данных;
qinq	режим double tagging.

режимы работы резервирования

Интерфейс может работать в одном из следующих режимов резервирования:

no	интерфейс не используется для резервирования;
rstp	интерфейс используется в составе топологии с резервированием с автоматическим конфигурированием по протоколу RSTP

Пример:

Установка режима полудуплекса и скорости передачи 10 Мбит/с для интерфейса номер двадцать четыре.

- ***ethmode*** *24 -d half10*

ok

Установка режима резервирования для кольца, состоящего из 3-х мультиплексоров.

- ***Site1 >*** *ethmode 0 -p rstp*
- ***Site1 >*** *ethmode 1 -p rstp*

- ***Site2 >*** *ethmode 1 -p rstp*
- ***Site2 >*** *ethmode 0 -p rstp*

- ***Site3 >*** *ethmode 0 -p rstp*
- ***Site3 >*** *ethmode 1 -p rstp*

lacp

Эта команда позволяет настроить агрегацию Ethernet-интерфейсов на оборудовании Sprinter TX 10G. При добавлении Ethernet-интерфейса в агрегацию, нужно учитывать, что настройки VLAN-ов на этих интерфейсах должны быть идентичными.

Команда доступна с версии ПО: LPOS 1.0.8.2SR22.

- ***lacp*** *[port_list] [-a add to bonding] [-r remove from bonding] [-b bondid] [-m active | passive]*

port_list	номера Ethernet-интерфейсов;
-a	добавить Ethernet-интерфейс в группу агрегированных каналов;
-r	удалить Ethernet-интерфейс из группы агрегированных каналов;
-b	указание id группы Ethernet-интерфейсов;
–m	задание режима работы агрегации: **active** – включить LACP (инициатор согласования каналов); **passive** - включить LACP только если придет сообщение LACP;

dhcprelay

Эта команда управляет перенаправлением DHCP запросов (по умолчанию перенаправление выключено).

- ***dhcprelay*** *[-d] [-e] [-i IP|-f] [-t ports] [-u ports] [-m minutes] [–b no|dis|pdown] [-v VLAN] [-z] [-s]*

-d	выключение перенаправления DHCP запросов;
-b	метод отключения портов в случае нарушения режима untrusted: no – отсутствие блокировки, dis – блокировка порта, pdown – включение режима Power down порта;
-e	включение перенаправления DHCP запросов;
-f	включение режима широковещательных запросов к DHCP-серверу;
-i	IP-адрес DHCP-сервера, на который перенаправляются запросы;
-m	время блокировки untrusted порта при получении от него пакета DHCP сервера;
-s	показать IP адреса пользователей;
-t	указание списка trusted (доверенных) портов;
-u	указание списка untrusted (недоверенных) портов;
–v	устанавливает VLAN ID 802.1p для перенаправляемых запросов, метка задается как десятичное число от 1 до 4095. 0 – означает отсутствие метки;
-z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

разрешение перенаправления DHCP на сервер 192.168.1.1.

- *dhcprelay –e –i 192.168.1.1*

ok

igmp

Эта команда управляет igmp snooping.

- ***igmp*** *[-d] [-e] [-f ports] [-v VLAN] [-z] [-q ports] [-s ports] [-r ports]*

-d	выключение IGMP snooping;
-e	включение IGMP snooping;
-f	указание списка портов, для которых нужно использовать fast leave режим;
–v	устанавливает VLAN ID 802.1p для потоков multicast (MVR режим), метка задается как десятичное число от 1 до 4095. 0 – означает отсутствие метки;
-q	список портов, на которых отключен режим Fast Leave
-s	список портов - источников мультикаст-вещания;
-r	список портов, принимающих мультикаст-вещание.
-z	запрещает сохранение внесенных изменений в файле конфигурации

Пример:

Указание метки multicast потоков 1232.

- ***igmp*** *–e –v 1232*

switchcfg

Эта команда устанавливает режим пакетного коммутатора.

- ***switchcfg*** *[-t yes|no] [-z] [-b no|yes]*

-t	режим работы QinQ (double tagging). При указании yes при маршрутизации используется верхний (снимаемый) тег, при указании no снимаемый тег отбрасывается, и пакет маршрутизируется как будто дополнительного тега не было;
–z	запрещает сохранение внесенных изменений в файле конфигурации.
-b	обработка BPDU пакетов (no|yes);

Пример:
Установка режима отбрасывания дополнительного тега.

- ***switchcfg*** *–t no*

vlan

Эта команда позволяет настраивать таблицу идентификаторов VLAN.

- ***vlan [VLAN ID]*** *[-n name] [-d] [-p ports_list] [-t ports_list][-u ports_list] [-b db] [-s] [-z]*

-n	символическое описание заданного идентификатора VLAN ID;
-d	удалить заданный идентификатор VLAN;
-p	список портов, принадлежащих к VLAN; на выходе этих портов фреймы не изменяются; если идентификатор VLAN ID не задан, то показывается список всех VLAN, к которым принадлежат эти порты;
–t	список портов, принадлежащих к VLAN; на выходе этих портов фреймы тегируются;
-u	список портов, принадлежащих к VLAN; на выходе этих портов снимаются теги фреймов;
-s	показывает информацию о заданном идентификаторе VLAN ID;
–z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Добавить идентификатор VLAN равный 100 для портов 0,2,3

- ***vlan*** *100 -p 0,2,3*

#	VID	name	0	1	2	3	cpu	slv
0	1	Eth port	M	M	M	M	M	M
2	100	user	M		M	M		

Показать список VLAN, к которым принадлежат порты 1,2

- ***vlan*** *-p 2,3*

port 1
member vlans *: 1,32*

port 2
member vlans *: 1,32,100*

maptac

Эта команда предназначена для ручной маршрутизации пакетов.

- ***maptac*** *[mac] [-n name] [-d] [-p dest_ports] [-f] [-s] [-z] [–b db] [-o pri] [-d all|dynamic] [-c all|dynamic] [-p MAC] [-i]*

Параметры:

-n	символическое описание заданного mac-адреса;
-d	удалить заданный mac-адрес;
-c	очистить таблицу mac-адресов (all – удаляются все адреса, dynamic – удаляются только автоматически добавленные адреса);

-p	список портов, из которых могут посылаться пакеты на указанный mac-адрес; если mac-адрес не задан, то показывается таблица mac-адресов, на которые могут посылаться пакеты из указанных портов;
-f	отображает все mac-адреса, в том числе добавленные автоматически;
-b	номер базы MAC для определения маршрутизации;
-o	приоритет для пакетов с указанным mac-адресом;
-i	показать групповые адреса;
-s	не выводить таблицу маршрутизации;
–z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Добавить mac-адрес 00-10-20-30-40-50 для портов 0 и 2

- ***mapmac*** *00-10-20-30-40-50 -p 0,2*

# MAC address	*name*	*pri*	*ports*	*ttl*
0 00-10-20-30-40-50	*user*	*1*	*0,2*	*F*

Посмотреть всю базу маршрутизации

- *mapmac -f*

# MAC address	*name*	*pri*	*ports*	*ttl*
0 00-10-20-30-40-50	*user 1*	*0,2*		*F*
1 00-13-D4-4A-9B-30	*learned*	*0*	*3*	*D*
2 00-16-EC-2B-36-D4	*learned*	*0*	*3*	*E*
3 00-18-F3-06-D1-94	*learned*	*0*	*3*	*D*
4 00-30-4F-3E-06-61	*learned*	*0*	*3*	*D*
5 01-80-C2-00-00-00	*learned*	*3*	*cpu*	*E*
6 5A-00-3B-19-DD-A8	*learned*	*0*	*2*	*E*
7 5A-00-3B-1C-2F-F5	*learned*	*0*	*cpu*	*E*
8 5A-00-3B-1D-30-F6	*learned*	*0*		*E*

ethrate

Эта команда настраивает ограничение пропускной способности выбранного пакетного интерфейса устройства.

- ***ethrate*** *<port_number> [-r ingress_rate_limit] [-s egress_rate_limit] [-p pri][-m 0|1|2|3] [-z] [-l] [-f uuni|umulti|broad|multi|uni|mgmt|no|arp|tcpdata|tcpctl|udp|nontcpudp]*

-r	ограничивает скорость входящего потока пакетов интерфейса значением в килобитах в секунду. Может принимать значения от 128 до 250*1024, 0 для отмены ограничения;
-s	ограничивает скорость исходящего потока пакетов интерфейса значением в килобитах в секунду. Может принимать значения от 128 до 250*1024, 0 для

	отмены ограничения;
-m	режим ограничения 0 – при ограничении учитываются все пакеты (значение по молчанию) 1 – учитываются broadcast, multicast и flooded unicast пакеты 2 – учитываются broadcast и multicast пакеты 3 – учитываются только broadcast пакеты
-l	Номер правила ограничения
-f	Фильтр ограничения. Может принимать значения: *uuni* - unknown unicast пакеты *umulti* - unknown multicast пакеты *broad* - broadcast пакеты *multi* - multicast пакеты *uni* - unicast пакеты *mgmt* - MGMT пакеты *no* - убрать фильтр (будет ограничиваться весь трафик) *arp* - arp пакеты *tcpdata* - TCP Data пакеты *tcpctl* - TCP Ctrl пакеты *udp* - UDP пакеты *nontcpudp* - не TCP/UDP пакеты (IGMP, ICMP, IGRP и тд).
-z	запрещает сохранение внесенных изменений в файле конфигурации

Пример:

Ограничение скорости входящего потока 16 Мбит/сек для интерфейса номер 24, приоритет третьей очереди равен 32Мбит/сек

- ***ethrate*** *24 -r 16384 –p 211*

Ограничение скорости исходящего потока 512 Кбит/сек для интерфейса номер 25

- ***ethrate*** *25 -s 512*

ethtype

Эта команда позволяет установить признак отсутствия или тип интерфейса Ethernet (например, тип оптики BL или BN). Исполнение этой команды влияет только на отображение наименование порта, и не влияет на его функционирование. Эту команду может выполнять только администратор.

- ***ethtype*** *<номер интерфейса> <no|cu|bl|bn|sfp1000|sfp10000> [-z]*

no	интерфейс отсутствует;
cu	интерфейс 100Base-TX;

bl	оптический интерфейс 100Base-FX передача 1310нм прием 1550нм;
bn	оптический интерфейс 100Base-FX передача 1550нм прием 1310нм;
sfp 1000	SFP интерфейс 1Гб/сек
sfp 10000	SFP интерфейс 10 Гб-сек
–z	запрещает сохранение внесенных изменений в файле конфигурации.

ethdesc

Устанавливает символическое описание интерфейса Ethernet или удаляет его при указании ключа *–d*. Если в описании присутствует символ «пробел» описание следует заключить в кавычки.

- ***ethdesc*** *<список имен интерфейсов> [описание интерфейса|-d] [-z]*

–z	запрещает сохранение внесенных изменений в файле конфигурации;
–d	удаляет символическое описание для выбранных каналов.

Пример:

Определение описания интерфейса.

- ***ethdesc*** *0 'important channel'*

ethreportlevel

Эта команда определяет степень детализации журнала и SNMP оповещений. Уровень 0 соответствует отсутствию сохранения или отправки сообщений, уровень 2 соответствует журнализации и отправке важных сообщений (по умолчанию) и уровень 5 соответствует сохранению и отправке всех сообщений (режим отладки)

- ***ethreportlevel*** *[<port numbers>] [-l log level] [-t trap level] [-d]*

-l	Уровень детализации журнала;
-t	Уровень детализации оповещений snmp;
-d	Отключить установленный уровень детализации.

rstp

Эта команда определяет настройки протокола Rapid Spanning Tree Protocol для портов.

- ***rstp*** *[<port number>] [-i port priority] [-e yes|no] [-c port cost][-p yes|no|auto] [-g no|yes] [-z]*

-i	чем меньше port priority, тем выше приоритет порта, может принимать значения от 0 до 240, по умолчанию 128;

-e	edge port – крайний порт; если включен, то переводится в режим передачи при подключении внешней сети, без задержки;
-c	стоимость соединения 10 Mb/s: Cost=2 000 000 100 Mb/s: Cost=200 000 1000 Mb/s: Cost=20 000
-p	включение/выключение соединения типа точка-точка;
-g	включение/выключение функции Root Guard;
-z	запрещает сохранение изменений в файле конфигурации.

rstpbridge

Эта команда определяет настройки протокола Rapid Spanning Tree Protocol для всего устройства.

- ***rstpbridge*** *[-p bridge priority] [-f forward delay] [-h hello time][-a max message age] [-b no|dis|pdown] [-m minutes] [-z]*

-p	чем меньше значение bridge priority, тем больше приоритет устройства; может принимать значения от 0 до 61440, по умолчанию 32768;
-f	задержка переключения порта в режим Forwarding (в секундах); может принимать значения от 4 до 30, по умолчанию 4;
-h	интервал посылки пакетов BPDU (в секундах); может принимать значения от 1 до 10, по умолчанию 1;
-a	максимальное время жизни пакета (в секундах); может принимать значения от 6 до 40, по умолчанию 6.
-z	запрещает сохранение изменений в файле конфигурации.
-b	метод отключения портов в случае нарушения режима untrusted: no – отсутствие блокировки, dis – блокировка порта, pdown – включение режима Power down порта;
-m	время блокировки порта при получении запрещенного BPDUпакета в минутах (0 для перманентной блокировки до принудительного включения администратором).

ipprimap

Эта команда позволяет настроить таблицу приоритетов IP-фреймов. По байту ToS, содержащемуся в пакете (учитываются 6 старших бит), выставляется соответствующий приоритет для этого пакета. Таблица состоит из восьми регистров, можно задать приоритеты как для всего регистра, так и для отдельного байта ToS.

- ***ipprimap*** *[-t ToS] [-p pri] [-r] [-z]*

-t	байт ToS, для которого задается приоритет (задается как шестнадцатеричное число, должен быть кратен 4);

-p	приоритет для указанного ToS (может принимать значение от 0 до 3);
–r	установка приоритетов по умолчанию (при использовании с ключом -t сбрасывается приоритет только для заданного Tos, с ключом -v сбрасываются приоритеты для заданного регистра);
–z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Посмотреть текущие значения приоритетов

- ***ipprimap***

```
ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri
-----------------------------------------------------------------------
 00  00 | 04  00 | 08  00 | 0C  00 | 10  00 | 14  00 | 18  00 | 1C  00
 20  00 | 24  00 | 28  00 | 2C  00 | 30  00 | 34  00 | 38  00 | 3C  00
 40  01 | 44  01 | 48  01 | 4C  01 | 50  01 | 54  01 | 58  01 | 5C  01
 60  01 | 64  01 | 68  01 | 6C  01 | 70  01 | 74  01 | 78  01 | 7C  01
 80  02 | 84  02 | 88  02 | 8C  02 | 90  02 | 94  02 | 98  02 | 9C  02
 A0  02 | A4  02 | A8  02 | AC  02 | B0  02 | B4  02 | B8  02 | BC  02
 C0  03 | C4  03 | C8  03 | CC  03 | D0  03 | D4  03 | D8  03 | DC  03
 E0  03 | E4  03 | E8  03 | EC  03 | F0  03 | F4  03 | F8  03 | FC  03
```

Задать приоритет для ToS 98 равным 0

- ***ipprimap*** *-t 98 -p 0*

```
ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri
-----------------------------------------------------------------------
 00  00 | 04  00 | 08  00 | 0C  00 | 10  00 | 14  00 | 18  00 | 1C  00
 20  00 | 24  00 | 28  00 | 2C  00 | 30  00 | 34  00 | 38  00 | 3C  00
 40  01 | 44  01 | 48  01 | 4C  01 | 50  01 | 54  01 | 58  01 | 5C  01
 60  01 | 64  01 | 68  01 | 6C  01 | 70  01 | 74  01 | 78  01 | 7C  01
 80  02 | 84  02 | 88  02 | 8C  02 | 90  02 | 94  02 | 98  00 | 9C  02
 A0  02 | A4  02 | A8  02 | AC  02 | B0  02 | B4  02 | B8  02 | BC  02
 C0  03 | C4  03 | C8  03 | CC  03 | D0  03 | D4  03 | D8  03 | DC  03
 E0  03 | E4  03 | E8  03 | EC  03 | F0  03 | F4  03 | F8  03 | FC  03
```

Задать вектор приоритетов для ToS 40-5C (строка 2)

- ***ipprimap*** *-v 2 21300201*

```
ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri  ToS pri
-----------------------------------------------------------------------
 00  00 | 04  00 | 08  00 | 0C  00 | 10  00 | 14  00 | 18  00 | 1C  00
 20  00 | 24  00 | 28  00 | 2C  00 | 30  00 | 34  00 | 38  00 | 3C  00
 40  02 | 44  01 | 48  03 | 4C  00 | 50  00 | 54  02 | 58  00 | 5C  01
 60  01 | 64  01 | 68  01 | 6C  01 | 70  01 | 74  01 | 78  01 | 7C  01
 80  02 | 84  02 | 88  02 | 8C  02 | 90  02 | 94  02 | 98  00 | 9C  02
 A0  02 | A4  02 | A8  02 | AC  02 | B0  02 | B4  02 | B8  02 | BC  02
 C0  03 | C4  03 | C8  03 | CC  03 | D0  03 | D4  03 | D8  03 | DC  03
```

E0 03 | E4 03 | E8 03 | EC 03 | F0 03 | F4 03 | F8 03 | FC 03

tagprimap

Эта команда переопределяет приоритеты тегированных фреймов. Для гигабитных устройств возможно переопределение для каждого порта.

- ***tagprimap*** *[port_number] [-g] [-t tag] [-p pri] [-r] [-z]*

-g	глобальное переопределение приоритетов;
-t	значение IEEE Tag, для которого задается приоритет (может принимать значение от 0 до 7);
-p	приоритет для указанного IEEE Tag (может принимать значение от 0 до 3 для глобального переопределения и до 7 для переопределения порта);
-r	установка приоритетов по умолчанию (при использовании с ключом -t сбрасывается приоритет только для заданного IEEE Tag);
–z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Посмотреть текущие значения приоритетов

- ***tagprimap***

```
   remap  remap  remap  remap  remap  remap  remap  remap
 #  pri 0  pri 1  pri 2  pri 3  pri 4  pri 5  pri 6  pri 7
---- -------------------------------------------------------
 0    00     01     02     03     04     05     06     07
 1    00     01     02     03     04     05     06     07
 2    00     01     02     03     04     05     06     07
 3    00     01     02     03     04     05     06     07
glob   01     00     00     01     02     02     03     03
```

Задать приоритет для IEEE Tag 5 равным 0

- ***tagprimap*** *-t 5 -p 0 -g*

```
   remap  remap  remap  remap  remap  remap  remap  remap
 #  pri 0  pri 1  pri 2  pri 3  pri 4  pri 5  pri 6  pri 7
---- -------------------------------------------------------
 0    00     01     02     03     04     05     06     07
 1    00     01     02     03     04     05     06     07
 2    00     01     02     03     04     05     06     07
 3    00     01     02     03     04     05     06     07
glob   01     00     00     01     02     00     03     03
```

Задать вектор приоритетов для второго порта

- ***tagprimap*** *2 -v 12300011*

```
   remap  remap  remap  remap  remap  remap  remap  remap
 #  pri 0  pri 1  pri 2  pri 3  pri 4  pri 5  pri 6  pri 7
---- -------------------------------------------------------
 0    00     01     02     03     04     05     06     07
 1    00     01     02     03     04     05     06     07
 2    01     02     03     00     00     00     01     01
 3    00     01     02     03     04     05     06     07
```

glob 01 00 00 01 02 00 03 03

ethtest

Эта команда позволяет тестировать состояние кабеля, подключенного к медным портам.

- ***ethtest*** *[port number]*

Результат исполнения:

normal cable	к порту подсоединен исправный кабель;
short in cable	к порту подсоединен неисправный кабель;
open in cable	второй конец кабеля никуда не подсоединен;
test fail	тест не смог запуститься;
test not completed	тест не смог завершиться;

Поле *amplitude* отражает вернувшееся напряжение (значение 0x1F соответствует напряжению +1В, значение 0x10 – напряжению 0В, значение 0x00 – напряжению -1В).

Поле *distance* показывает примерное расстояние (в метрах), на котором произошел обрыв или замыкание кабеля.

Пример:

Тестирование портов 2 и 3

- *ethtest 2,3*

#	status	amplitude	distance
2	open in cable	18	1
3	normal cable	10	

5.1.6 Команды общей диагностики

Эти команды показывают текущие значения питающего напряжения и температуры внутри мультиплексора и обеспечивают доступ к журналу, в который записываются все системные сообщения мультиплексора. Журнал содержит 2730 последних сообщений и находится в системной памяти мультиплексора, и пользователи, как привилегированный, так и непривилегированные, не могут стереть сообщения. Все аномалии в работе мультиплексора, пропадание или появление сигнала на внешних интерфейсах, подключение и отключение управляющего компьютера для конфигурации мультиплексора, записываются в журнал с указанием времени возникновения.

envir

Показывает величину питающего напряжения и температуру в корпусе мультиплексора, если указанные параметры доступны ЦПУ.

- ***envir***

log

Выдает на экран список системных сообщений с момента последнего включения устройства.

- ***log*** *[-a][-e]*

–a	включает выдачу всех системных сообщений, хранящихся в файле журнала.
-e	очистить список.
-c	для выбора уровня журнализации выполненных команд. *eth* – только команды для Ethernet, *No* – отключает сохранение; *all* – устанавливает настройки по умолчанию.

syslog

Настраивает параметры протокола syslog. По умолчанию эта функция выключена, для ее включения необходимо задать IP-адрес syslog-сервера.

- ***syslog*** *[-i IP] [-f] [-d] [-z]*

–i	IP-адрес syslog-сервера;
-f	тип запроса;
-d	выключение функции syslog;
-z	запрещает сохранение внесенных изменений в файле конфигурации.

ping

Посылает ICMP-пакет по указанному сетевому адресу и выводит в окно терминала время его передачи туда и обратно или сообщение об отсутствие ответа.

- ***ping*** *<IP адрес> [-w timeout ms] [-t repeat] [-v VLAN ID]*

-w	Время ожидания ответа (по умолчанию 1000 мс)
-t	Количество запросов (по умолчанию один)
-v	Номер VLAN’а, в котором осуществляется пинг

Пример:

«Пинг» IP-адреса 192.168.0.2.

- ***ping*** *192.168.0.2*

Echo reply 0.384ms

5.1.7 Команды управления портом терминального сервера

Эти команды позволяют настроить параметры последовательного порта для удаленного администрирования устройства.

sersetup

Устанавливает указанные параметры для последовательного порта:

- ***sersetup*** *–s <baud rate> [-p <stop bits>] [-n|-o|-e] [-z]*

-s	Устанавливает скорость в бодах (например, 2400, 4800, 9600,115200)

-p	Устанавливает количество стоповых битов (1 или 2)
-n|-o|-e	Устанавливает четность (чет(-e) или нечет(-o)) или ее отсутствие (–n).
–z	запрещает сохранение внесенных изменений в файле конфигурации.

Пример:

Включение терминального сервера для управления модемом М-1Д.

- ***sersetup*** *-s 38400 -p 1 –n*

arp

Отображает таблицу соответствия MAC и IP адресов.

- ***arp*** *[-r]*

-r	Очищает таблицу

Пример:

- ***arp***

ARP table

#	*IP*	*MAC*	*time*
0	192.168.000.182	00-16-AC-2B-36-D4	118
1	192.168.000.157	00-18-A3-06-D1-94	118
2	192.168.000.137	00-16-A4-5C-9D-61	0

total 3 items

5.1.8 Команды для работы с устройством по GSM каналу

С помощью этих команд можно подключиться к удаленному мультиплексору, чтобы узнать о его состоянии, посмотреть и изменить конфигурацию, а так же обновить программное обеспечение, при потере доступа к устройству по telnet, ftp, http и отсутствии консольного подключения.

phone

Устанавливает настройки мультиплексора для удаленного подключения по GSM:

- ***phone*** *[-list] [-add <номер телефона>][-dell <номер телефона>][-call <номер телефона>]*

-list	показывает список текущих номеров, с которых устройство может принимать вызов, в память SIM карты
-add	добавить номер в память SIM карты
-dell	удалить номер из памяти SIM карты

–call	установить соединение с указанным номером
-reset	перезагрузка GSM модуля

Номер записывается в федеральном формате, т.е. состоит из трех частей:

кода страны (CC — Country Code),

национального кода направления (NDC — National Destination Code)

номера абонента (SN — subscriber number).

Например:

CC = +7, NDC = 913, SN=1234567, итоговый пример: +79131234567.

5.2 Меню конфигурирования

В качестве альтернативы консольным командам имеется интерфейс в виде текстового иерархического меню. Для его запуска необходимо набрать команду **menu** и нажать **<Enter>**. Для перехода в требуемое подменю необходимо нажать клавишу с соответствующей цифрой (1,2…) или выбрать его клавишами со стрелками “↑” (вверх) или “↓” (вниз) и нажать <Enter>. Для возврата в меню верхнего уровня следует нажать **<BackSpace>** или два раза **<Esc>**. Пример основного меню приведен на рисунке

```
Menu
   ----------------------------------------------------------------------
    0. Brief status overview                                            >
    1. Device configuration                                             >
    2. Ethernet ports configuration                                     >
    3. Performance counters                                             >
    4. View log
    5. Exit to command prompt
   ------------------------------------------- some --------------------
```

Верхняя строчка указывает название отображаемого меню и его положение в структуре меню.

5.2.1 Меню «Brief status overview»

Меню «*Brief status overview*» служит для просмотра информации текущих статусах Ethernet портов, о версиях программного обеспечения каждого модуля мультиплексора, а также температуры внутри корпуса (если эта информация доступна).

```
Menu / Brief status overview
----------------------------------------------------------------------
 0. Ethernet port 0 . . . . . no link
 1. Ethernet port 1 . . . . . no link
 2. Ethernet port 2 . . . . . no link
 3. Ethernet port 3 . . . . . no link
 4. Case temperature  . . . . 3.125
 5. Hardware version  . . . . 1424.1.00
 6. Firmware version  . . . . 1424.1.00
 7. Bootloader version  . . . v 1.0.0.9
 8. Operating system version  LP ARM OS 1.0.8.2 SR 3 (Apr 13 2011)
 9. Probe software version  . 14.1
----------------------------------------------------------------------
```

5.2.2 Меню «Device configuration»

Меню «Device configuration» позволяет просматривать и устанавливать информацию об имени и расположении мультиплексора (для удобства последующей идентификации), состояния служб управления.

```
Menu / Device configuration
----------------------------------------------------------------------
 0. Network settings                                                 >
 1. Passwords management                                             >
 2. Restrict access by IP                                            >
 3. SMNP parameters                                                  >
 4. Auxiliary port parameters                                        >
 5. Date&time                                                        >
 6. Device name . . . . . . . LPOS
 7. Device location . . . . .
 8. System date . . . . . . . 10.10.06
 9. System time . . . . . . . 14:47:47
 A. Allow Web access. . . . . YES
 B. Allow FTP access. . . . . YES
 C. Allow telnet access . . . YES
 D. Autostart menu in telnet. NO
 E. Allow to autosave cfg . . YES
 F. Allow RS-232 pipe . . . . YES
```

«Device name» символьное имя мультиплексора

«Device location» расположение мультиплексора

«System date» текущая дата

«System time» текущее время

Состояния служб управления отображаются в следующих строчках

Telnet access

Web access

FTP access

RS Pipe

состояние отображается в виде YES/NO, где YES означает, что данная служба активна и через нее возможно управление и мониторинг состояния мультиплексора, а NO означает, что данная служба остановлена.

5.2.3 Меню «Network settings»

Меню «Network settings» служит для просмотра и установки MAC-адреса, IP-адреса мультиплексора, маски подсети и адреса шлюза по умолчанию.

```
Menu / Device configuration / Network settings
----------------------------------------------------------------------
 0. Device MAC  . . . . . . . 5A-00-3B-12-01-08
 1. Device IP . . . . . . . . 192.168.0.42
 2. Subnet mask . . . . . . . 255.255.255.0
 3. Default gateway IP  . . . 192.168.0.1
 4. Default VLAN  . . . . . . 0
```

«Device MAC»	MAC-адрес мультиплексора.
«Device IP»	IP адрес мультиплексора.
«Subnet mask»	Маска подсети
«Default gateway IP»	IP адрес главного шлюза.
«Default VLAN»	устанавливаемый по умолчанию номер VLAN.

5.2.4 Меню «Passwords management»

Меню «Passwords management» служит для изменения паролей пользователей “admin”, “oper1” и “oper2”. Пароль может содержать до 18 букв латинского алфавита и цифр.

```
Menu / Device configuration / Passwords management
----------------------------------------------------------------------
 0. Set password for user 'admin'
 1. Set password for user 'oper1'
 2. Set password for user 'oper2'
----------------------------------------------------------------------
```

‘admin’ – привилегированный пользователь.

По умолчанию установлены следующие пароли:

Для пользователя *‘admin’* пароль: *admin*

Для пользователя *‘oper1’* пароль: *oper1*

Для пользователя *‘oper2’* пароль: *oper2*

5.2.5 Меню «Restrict access by IP»

Меню «Restricy access by IP» служит для просмотра и установки адресов управляющих станций, с которых возможен доступ к мультиплексору по протоколу IP.

```
Menu / Device configuration / Restrict access by IP
----------------------------------------------------------------------
 1. Pass from any IP  . . . . YES
 2. Pass from the same subnet YES
 3. Pass from IP :  . . . . .
 4. Pass from IP :  . . . . .
 5. Pass from IP :  . . . . .
 6. Pass from IP :  . . . . .
 7. Pass from IP :  . . . . .
----------------------------------------------------------------------
```

Существует 3 уровня доступа к устройству:

1. Доступ разрешен для всех, т.е. с любого IP адреса
2. Доступ только для тех IP адресов, которые принадлежат данной локальной сети
3. Доступ только для тех IP адресов, которые перечислены.

5.2.6 Меню «SNMP parameters»

Меню «SNMP parameters» служит для просмотра и установки параметров службы SNMP.

```
Menu / Device configuration / SNMP parameters
----------------------------------------------------------------------
 0. Enable SNMP agent . . . . YES
 1. Read community. . . . . . public
 2. Write community . . . . . public
 3. Enable alarm traps. . . . YES
 4. Trap community. . . . . . public
 5. Send alarm traps to . . .
 6. SNMP Version 2. . . . . . NO
```

«Enable SNMP agent»	включение/выключение SNMP агента
«Read community»	snmp- пароль на чтение
«Write community»	snmp- пароль на запись
«Enable alarm traps»	включение/выключение трапов
«Trap community»	пароль на посылку трапов
«Send alarm traps to»	IP адрес сервера, который обрабатывает трапы

5.2.7 Меню «Auxiliary port parameters»

Меню «Auxiliary port parameters» служит для установки режимов последовательного порта.

```
Main Menu / System / Auxiliary port parameters
----------------------------------------------------------------------
  1. Baud rate . . . . . . . . 115200
  2. Stop bits . . . . . . . . 1
  3. Parity. . . . . . . . . . NO
----------------------------------------------------------------------
```

Для работы порта терминального сервера следует установить следующие параметры:

«Baud rate»	скорость в бодах: «115200», «57600», «38400», «19200», «9600», «4800», «2400», «1200»;
«Stop bits»	формат передачи символа – количество стоповых битов. Возможны следующие варианты 1,1.5,2
«Parity»	формат передачи символа – чётность (дополнение до чётного, либо до нечётного). Возможны следующие варианты NO,ODD,EVEN

5.2.8 Меню «Date&time»

Меню «Date&time» служит для установки системной даты и времени, а также параметров автоматической синхронизации со временем интернета.

```
Menu / Device configuration / Date&time
-----------------------------------------------------------------------
 1. System date . . . . . . . 12.04.11
 2. System time . . . . . . . 12:02:14
 3. Time zone . . . . . . . . 6
 4. Internet time server. . . 62.149.2.1
 5. Auto synchronization. . . YES
 6. Next synchronization. . . 15.04.11
 7. Synchronize time now
-----------------------------------------------------------------------
```

«System date»	текущая дата.
«System time»	текущее время.
«Time zone»	часовой пояс.
«Internet time server»	IP адрес сервера, с которым должна проходить синхронизация.
«Auto synchronization»	включение/выключение автосинхронизации с сервером.
«Next synchronization»	дата следующей синхронизации.
«Synchronize time now»	включение немедленной синхронизации.

5.2.9 Меню «Eth configuration»

Меню «ETH configuration» служит для установки режимов выбранного интерфейса Ethernet:

```
Menu / Ethernet ports configuration / Ethernet port 0
-----------------------------------------------------------------------
 0. Port description. . . . .
 1. Port status . . . . . . . no link
 2. Port type . . . . . . . .
 3. Port role . . . . . . . . MULTI
 4. Port mode . . . . . . . . AUTO
 5. Ingress rate limiting . . 0
 6. Egress rate limiting. . . 0
 7. Rate limit mode . . . . . ALL
 8. VLAN ID . . . . . . . . . 1
 9. Priority mode . . . . . . TAG
 A. Default priority. . . . . 1
 B. Reservation mode. . . . . NONE
 C. IGMP snooping . . . . . . NO
```

Для настройки пакетной передачи служат следующие параметры:

«Port role»	режим работы – может быть одним из: **down, trunk, multi, access, qinq**
«Port mode»	скорость и дуплекс может быть одним из: **auto, half10, full10, half100, full100, full1000, full 10G**
«Ingress rate limiting»	ограничивает скорость входящего потока пакетов интерфейса значением в килобитах в секунду. Может принимать значения от 128 до 250*1024, 0 для

	отмены ограничения
«Egress rate limiting»	ограничивает скорость исходящего потока пакетов интерфейса значением в килобитах в секунду. Может принимать значения от 128 до 250*1024, 0 для отмены ограничения
«Rate limit mode»	режим ограничения **ALL** – при ограничении учитываются все пакеты (значение по умолчанию) **BMF** – учитываются broadcast, multicast и flooded unicast пакеты **BM** – учитываются broadcast и multicast пакеты **B** – учитываются только broadcast пакеты
«VLAN ID»	идентификатор VLAN
«Priority mode»	способ установления приоритетов - может быть одним из: **tag, ip, tagip, iptag, no**; определяет заголовки протокола и порядок определения приоритета
«Reservation mode»	режим резервирования – может быть одним из: **no, rstp**
«IGMP snooping»	запрещает/разрешает IGMP snooping

5.3 SNMP Агент

Мультиплексор оснащен агентом SNMP. По протоколу SNMP можно просматривать текущие режимы устройства, состояние интерфейсов, статистику локальных и удаленных ошибок, а также изменять эти параметры.

Для доступа к устройству по протоколу SNMP необходимо с консоли установить следующие параметры:

«Enable SNMP agent»	разрешение чтения и установки параметров через SNMP протокол
«Read community»	пароль для доступа на запрос информации
«Write community»	пароль для доступа на установку параметров

Устройство может посылать SNMP сообщения (traps) при возникновении чрезвычайных событий. Для этого следует установить следующие параметры:

«Enable alarm traps»	разрешение посылки сообщений о чрезвычайных событиях
«Trap community»	пароль для посылки сообщений о чрезвычайных событиях
«Send alarm traps to»	IP-адрес для посылки сообщений о чрезвычайных событиях

<u>SNMP-сообщения (traps) посылаются при возникновении следующих событий:</u>

- включение или перезагрузка мультиплексора – сообщение «COLD START»;
- попытка несанкционированного доступа по протоколу SNMP – сообщение «AUTHENTICATION FAILURE»;
- потеря сигнала или циклового синхронизма на оптической линии – сообщение «LINK DOWN»;
- переход оптической линии в нормальный режим – сообщение «LINK UP»;

5.3.1 Наборы информации управления (MIB)

В мультиплексоре реализован набор информации управления (MIB):

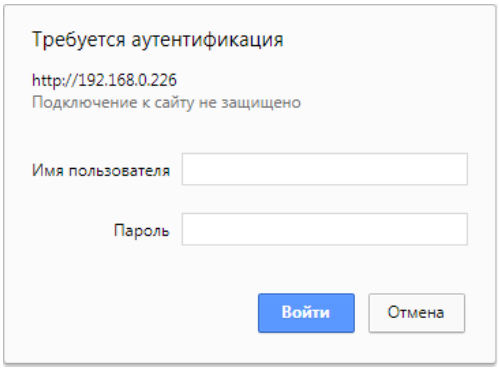
EMUX-3XX-MIB – специализированный набор информации управления, содержащий состояние интерфейсов. Файлы со спецификацией EMUX-3XX-MIB доступны на сайте *http://www.nsc-com.com*.

5.4 HTTP Browser

Мультиплексор оснащен встроенным http сервером. По протоколу http можно просматривать текущие режимы устройства, состояние интерфейсов, статистику локальных и удаленных ошибок.

При подключении к мультиплексору по http протоколу необходимо набрать в строке адрес мультиплексора.

При этом, из соображений безопасности, устройство запросит у Вас имя пользователя и пароль:



По умолчанию установлены следующие пароли:

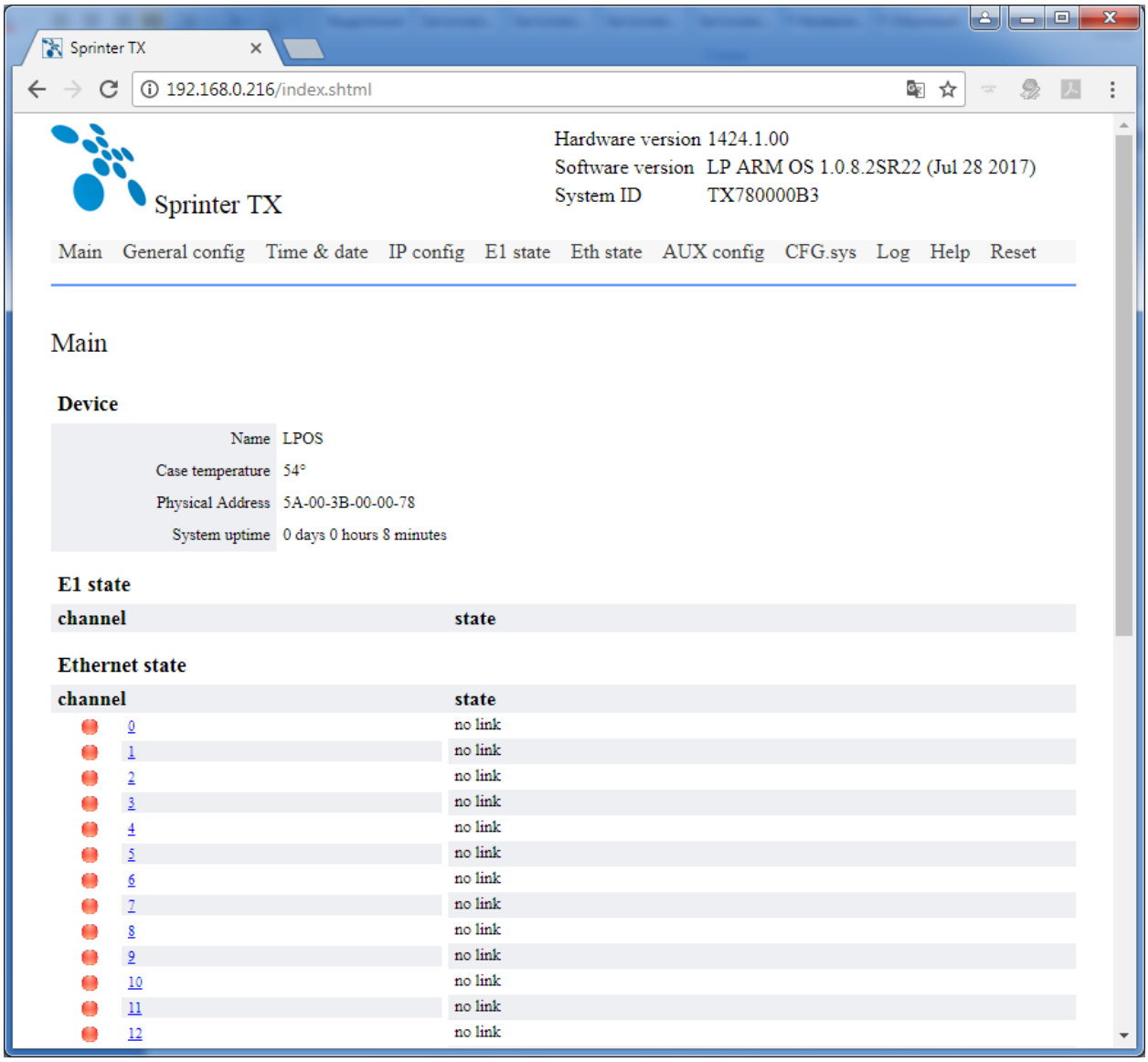
Для пользователя *'admin'* пароль: *admin*

Для пользователя *'oper1'* пароль: *oper1*

Для пользователя *'oper2'* пароль: *oper2*

Изменить пароли возможно либо через командную строку командой password, либо через меню: Menu / Device configuration / Passwords management.

5.4.1 Main



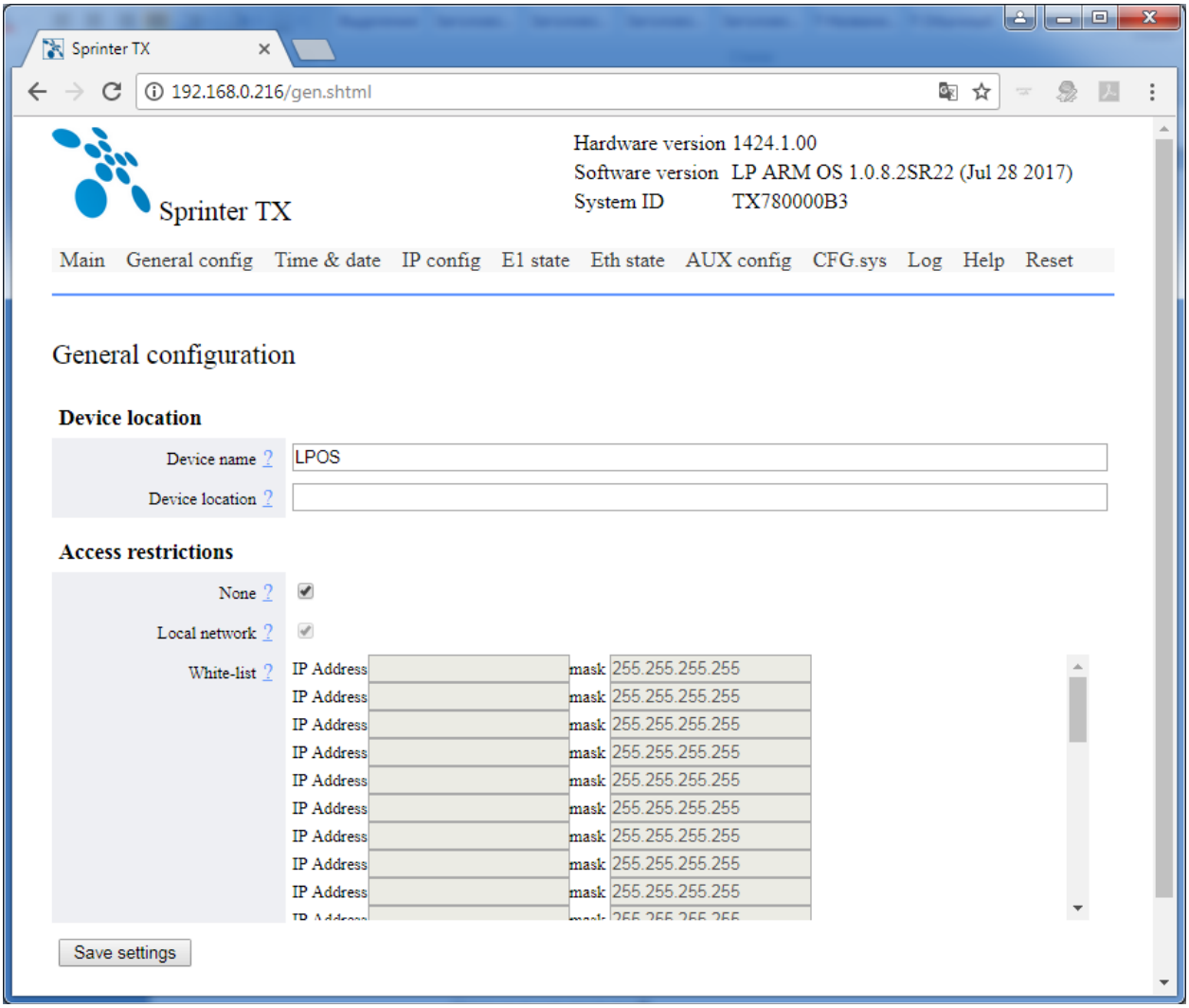
«Name»	символьное имя мультиплексора
«Case temperature»	температура в корпусе
«Physical Address»	физический адрес
«System uptime»	время, которое мультиплексор находится в сети.

Ethernet state – информация о Ethernet портах, их номер, символьное имя и статус. Цвет лампочки соответствует статусу порта:

Зеленая	линк есть
Красная	нет линка
Серая	канал выключен

По нажатию на номер канала осуществляется переход в меню конфигурации данного канала.

5.4.2 General config

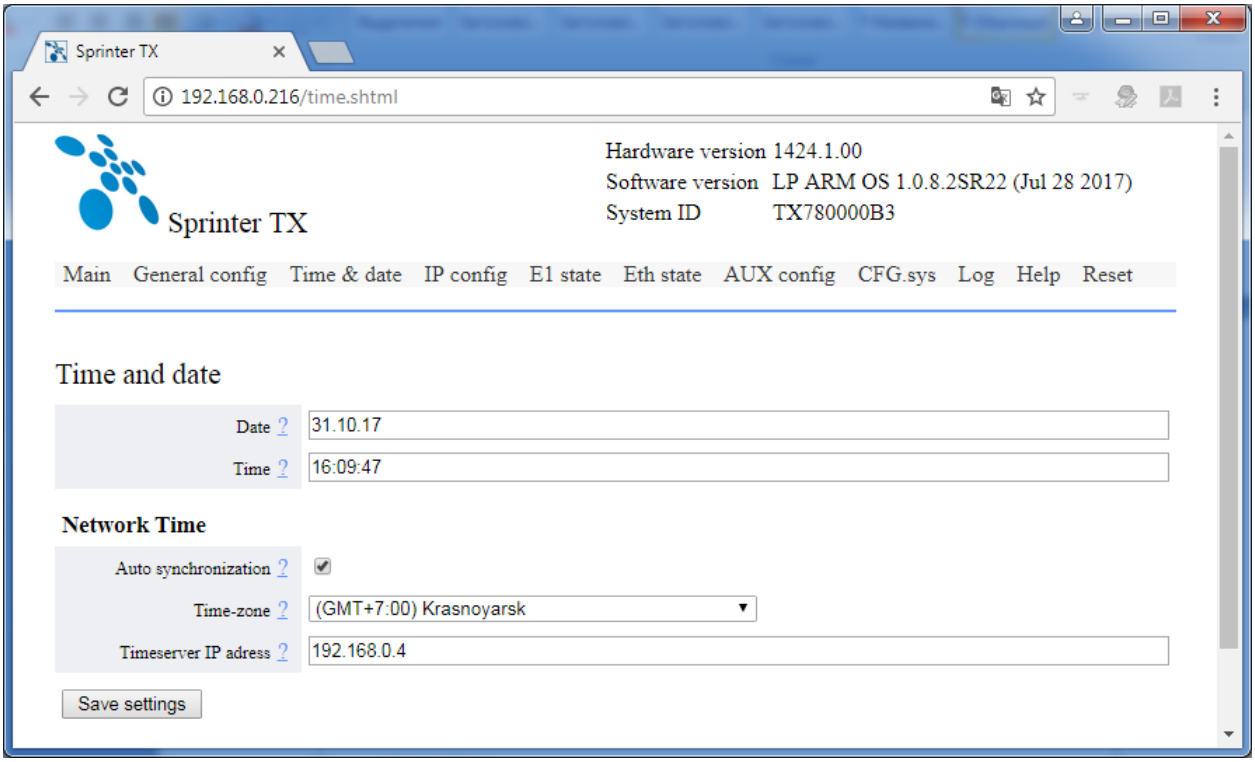


«Device name» символьное имя мультиплексора
«Device location» символьный адрес мультиплексора

<u>Ограничение доступа:</u>

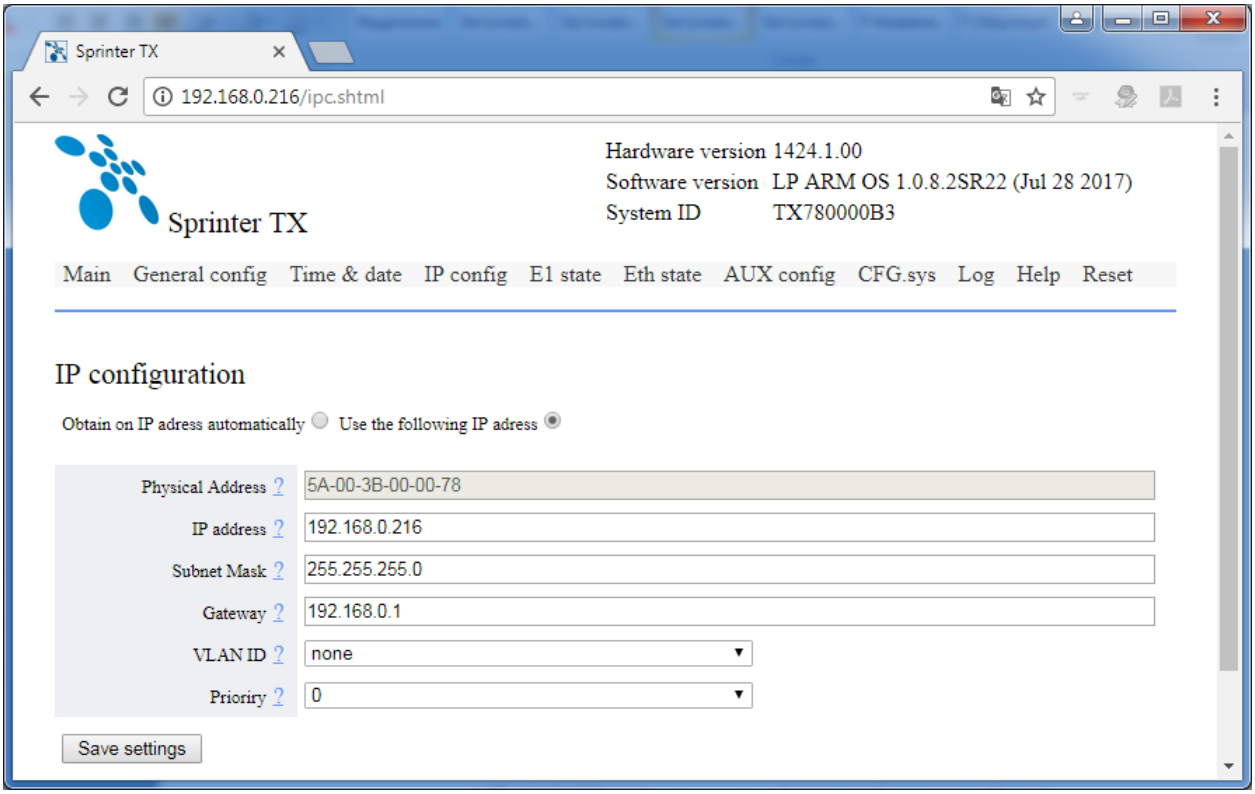
«None» отсутствие ограничений; доступ разрешен со всех IP адресов.
«Local network» доступ разрешен только с IP адресов, расположенных в данной сети
«White-list» доступ разрешен только с IP адресов, Включенных в «wite-list»

5.4.3 Time&date



«Date»	отображается текущая дата.
«Time»	отображается текущее время
«Auto synchronization»	включения/выключение авто синхронизации с сервером.
«Time-zon»	выбор часового пояса
«Timeserver IP adress»	IP адрес сервера, с которым будет происходить авто синхронизация

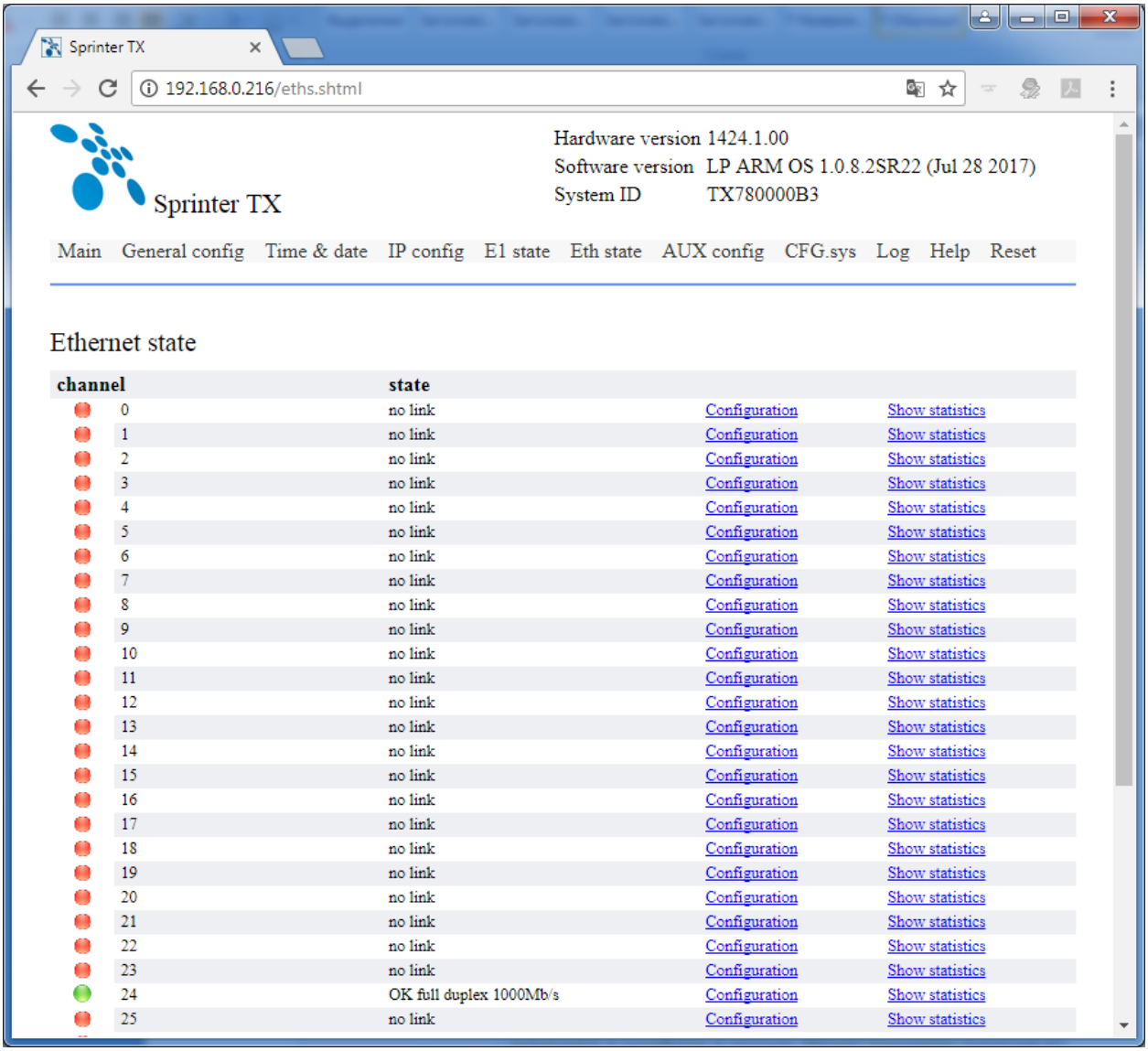
5.4.4 IP configuration



«Physical Address»	физический адрес устройства
«IP address»	IP адрес устройства
«Subnet Mask»	Маска подсети
«Gateway»	IP адрес главного шлюза
«VLAN ID»	Номер VLAN
«Prioriry»	Приоритет (значения от 0 до 7)

5.4.5 Ethernet state

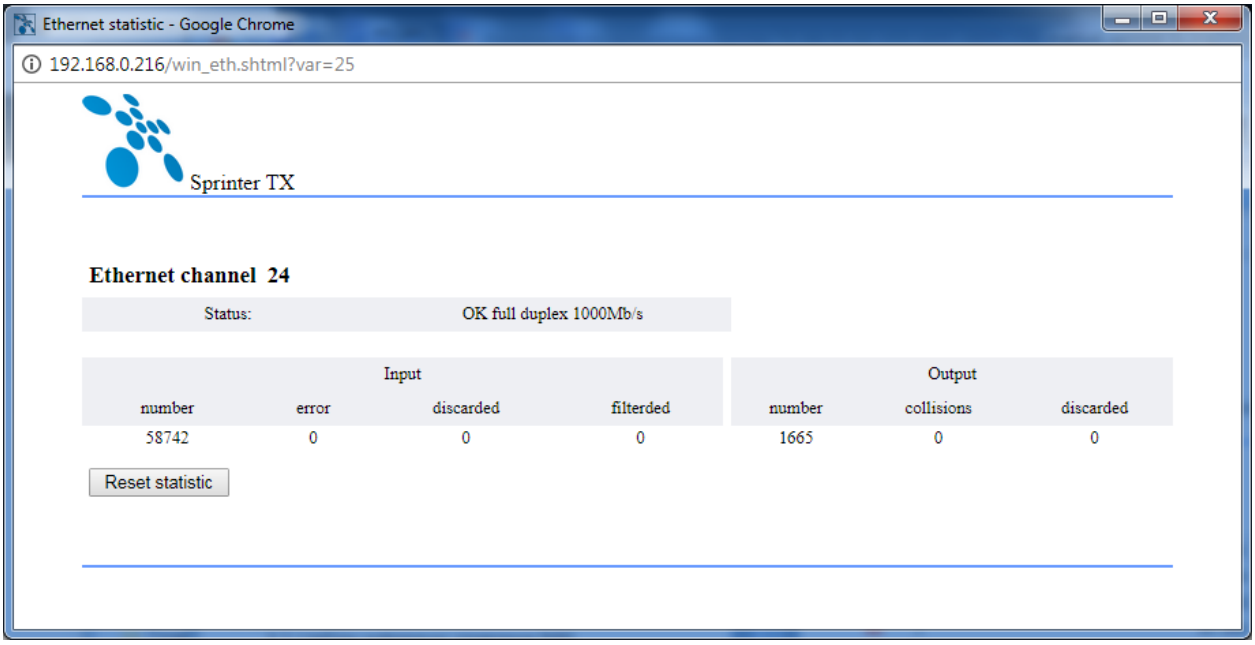
Ethernet state -> Configuration



«Port role»	режим работы – может быть одним из: *down, trunk, multi, access, qinq*
«Port mode»	скорость и дуплекс может быть одним из: *auto, half10, full10, half100, full100, full1000, full 10G*
«Ingress rate limiting»	ограничивает скорость входящего потока пакетов интерфейса значением в килобитах в секунду. Может принимать значения от 128 до 16*1024 (стомегабитный коммутатор) или до 250*1024 (гигабитный коммутатор), 0 для отмены ограничения
«Egress rate limiting»	ограничивает скорость исходящего потока пакетов интерфейса значением в килобитах в секунду. Может принимать значения от 128 до 16*1024 (стомегабитный коммутатор) или до 250*1024 (гигабитный коммутатор), 0 для отмены ограничения

«Rate limit mode»	режим ограничения *ALL* – при ограничении учитываются все пакеты (значение по молчанию) *BMF* – учитываются broadcast, multicast и flooded unicast пакеты *BM* – учитываются broadcast и multicast пакеты *B* – учитываются только broadcast пакеты
«VLAN ID»	идентификатор VLAN
«Priority mode»	способ установления приоритетов - может быть одним из: *tag, ip, tagip, iptag, no*; определяет заголовки протокола и порядок определения приоритета
«Secure mod»	режим безопасности – может быть одним из: no learn – только вручную введенные адреса; no – обычные режим, без ограничений; mac – только с одного заданного mac адреса.
«Reservation mode»	режим резервирования – может быть одним из: *no, rstp*
«IGMP»	запрещает/разрешает IGMP snooping
Force VLAN mode	назначение специального VLAN для всех пакетов.
Smart VLAN mode	режим изоляции. Пакеты одного пользователя запрещено передавать в порты принадлежащие любому пользователю с той же VLAN.

Ethernet state -> Show statistic



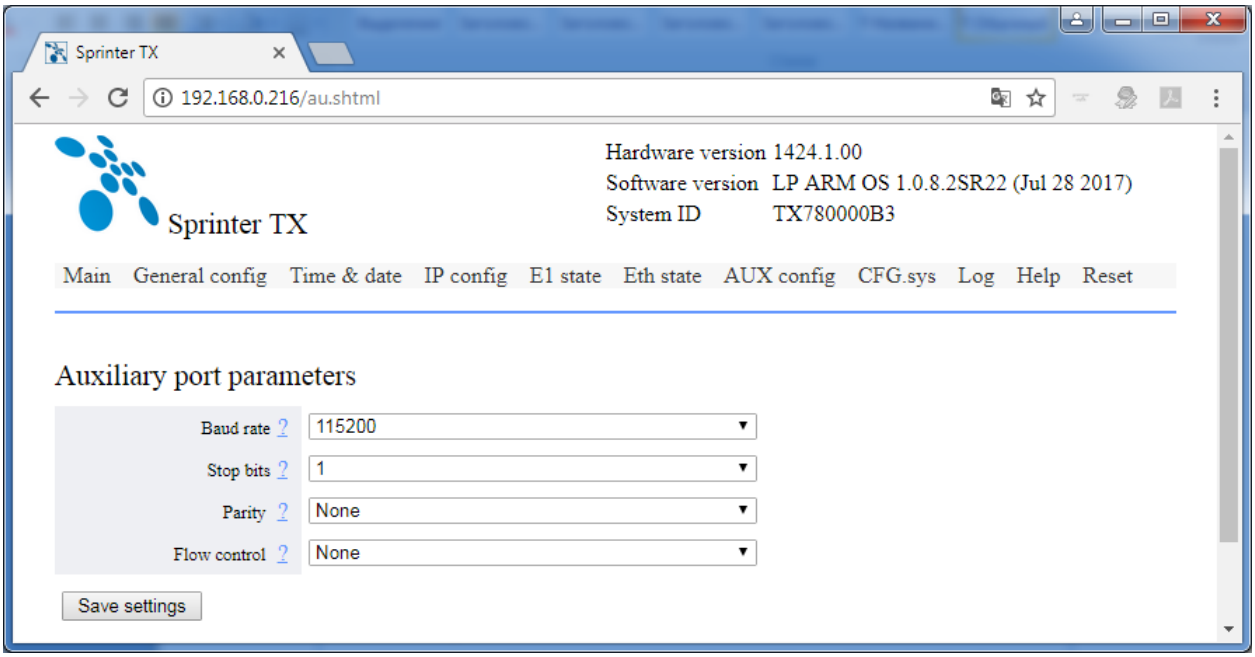
Reset statistic - сброс статистики по Ethernet

Input

«number»	Количество принятых пакетов
«error»	Количество ошибочных пакетов

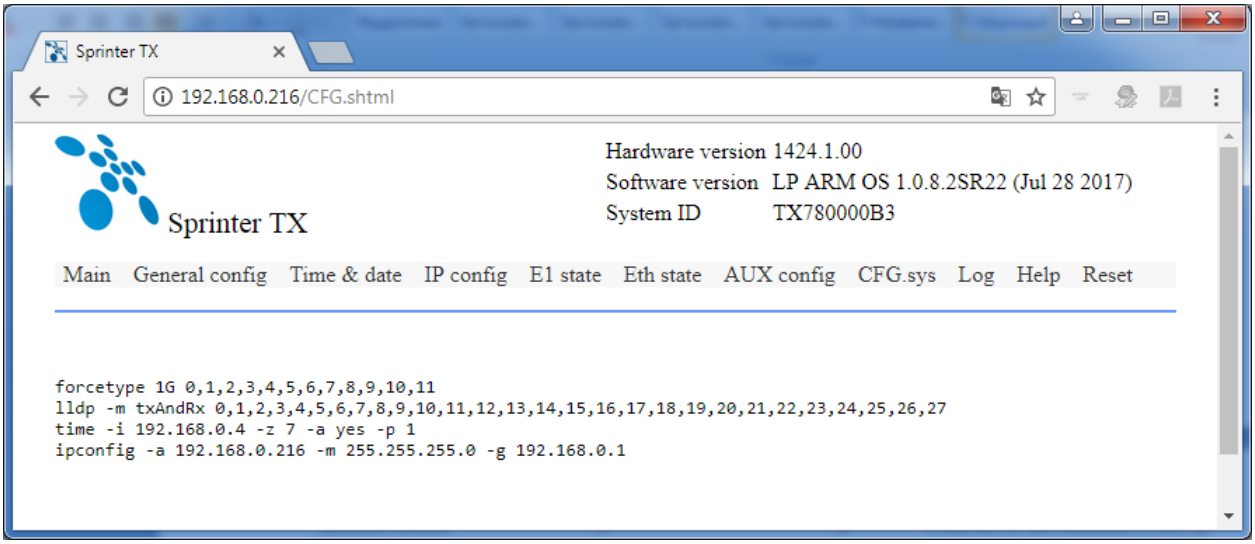
«discarded»	Количество принятых пакетов, которые были отброшены и не обработаны из-за нехватки места в очереди
«filterded»	Количество принятых пакетов, которые были отброшены из-за неверного VLAN ID или ограничения MAC-адресов на порту
	Output
«number»	Количество отправленных пакетов
«collisions»	Количество коллизий
«discarded»	Количество пакетов, которые не были переданы из-за нехватки места в очереди

5.4.6 AUX



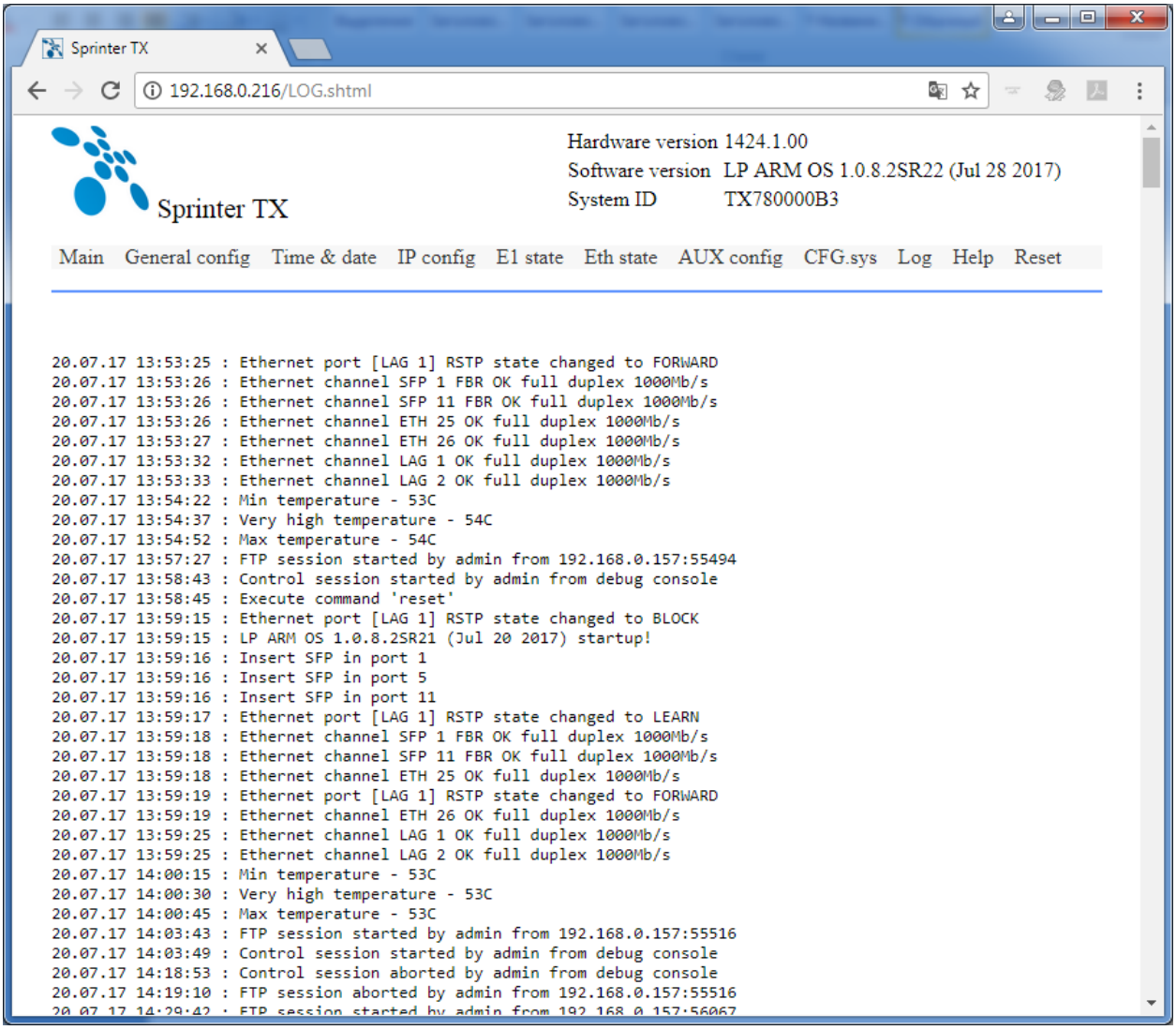
«Baud rate»	скорость в бодах: «115200», «57600», «38400», «19200», «9600», «4800», «2400», «1200»;
«Stop bits»	формат передачи символа – количество стоповых битов. Возможны следующие варианты 1,1.5,2
«Parity»	формат передачи символа – чётность (дополнение до чётного, либо до нечётного). Возможны следующие варианты NO,ODD,EVEN

5.4.7 CFG.sys



В закладке CFG.sys находится файл конфигурации устройства. Этот текстовый файл содержит набор строк, каждая строка которого представляет собой команду управления устройством. При каждом включении устройства управляющая программа исполняет все команды в том порядке, в котором они встречаются в этом файле.

5.4.8 Log



Log - протокол событий. Создается автоматически при первом включении устройства. В него вносятся любые изменения. Благодаря этому пользователь всегда может отследить поведение линков: в какое время происходило падение/поднятие. Так же можно увидеть, кто и когда заходил на устройство.

6 Рекомендации по устранению неисправностей

Мультиплексор представляет собой сложное микропроцессорное устройство, поэтому устранение неисправностей, если они не связаны с очевидными причинами – ошибочной конфигурацией, обрывом кабеля питания, механическим повреждением разъёма и т. п. – возможно только на предприятии-изготовителе или в его представительствах.

При возникновении вопросов, связанных с эксплуатацией мультиплексора, обращайтесь, пожалуйста, в службу технической поддержки компании-производителя.

В этом разделе описаны способы обнаружения и устранения неисправностей возникающих при эксплуатации мультиплексора.

6.1 Диагностика ошибочных состояний

Диагностика ошибочных состояний может быть произведена на основе анализа светодиодных индикаторов на передней панели. В более сложных случаях необходимо подключиться к мультиплексору и выполнить консольные команды диагностики. Кроме этого, мультиплексор оборудован журналом работы, в который заносится информация обо всех событиях, происходящих с мультиплексором. Каждая запись в журнале снабжена меткой времени. Пользователь может просмотреть журнал событий, используя telnet, локальный терминал или браузер, через протокол HTTP

6.1.1 Светодиодная индикация

Светодиодные индикаторы на передней панели мультиплексора отражают текущее состояние интерфейсов Ethernet, а также состояние мультиплексора в целом. Состояние медных Ethernet соединений отображается традиционно: зеленый индикатор сигнализирует о подключении кабеля и установлении соединения, а желтый о передаче данных.

6.1.2 Консольные команды

Для отображения конфигурации пользовательских интерфейсов, их состояния и счетчиков ошибок в мультиплексоре реализованы следующая консольная команда:

Для информации о Ethernet интерфейсах

- ***ethstat***

В этой команде может быть указаны имена интерфейсов, для которых нужно отобразить состояние или конфигурацию, а также дополнительные ключи.

6.1.3 Журнал событий

Все изменения состояния интерфейсов заносятся в системный журнал с указанием временной метки события. Для просмотра журнала можно использовать команду ***log.***

Для правильного отображения временных меток в мультиплексоре необходимо правильно установить текущую дату и время.

6.2 Устранение неисправностей

Основные типы ошибочных состояний и способы их устранения

Состояние	Вероятная причина	Рекомендуемое действие
Нет питания мультиплексора, все светодиодные индикаторы погашены	Кабель питания неисправен	Проверьте кабель, измерив напряжение на разъеме.
Нет питания мультиплексора,	Питающее напряжение за	Выберете источник питания с

все светодиодные индикаторы погашены	пределами допустимого диапазона	напряжением питания в указанном диапазоне (мультиплексор будет в состоянии «отключено», если напряжение холостого хода источника питания выше максимально допустимого значения)
Нет соединения с мультиплексором по протоколу telnet или ftp	Кабель Ethernet неисправен	Проверьте кабель, подключив мультиплексор заведомо исправным (проверенным) кабелем.
Нет соединения с мультиплексором по протоколу telnet или ftp	Неправильно установлен IP адрес или маска в мультиплексоре	Установите правильный адрес, используя последовательный порт
Нет соединения с мультиплексором по протоколу telnet или ftp	Управляющий компьютер находится в другом сегменте сети и шлюз по умолчанию настроен неверно	Выполните подключение из одного сегмента сети с мультиплексором
Нет соединения с мультиплексором по протоколу telnet или ftp	Адрес управляющего компьютера не находится среди адресов доверенных узлов мультиплексора	Добавьте адрес управляющего компьютера в список доверенных узлов, используя последовательный порт
Нет соединения с мультиплексором по последовательному порту	Неправильно установлен baud rate,количество стоповых бит, четность, контроль передачи	Параметры настройки последовательного порта компьютера – 115000 кбит/с, 8 бит, без четности, без контроля передачи.

6.3 Диагностические тесты

Для выявления и устранения неисправностей часто бывает необходимо провести диагностические тесты.

6.3.1 Проверка доступа к мультиплексору

Для проверки связности сети используется команда Windows ping с указанием IP-адреса удаленного устройства.

Пример.

Проверка связности сети с помощью посылки ICMP-пакетов на мультиплексор с IP-адресом 192.168.111.21.

C:\>ping 192.168.111.21
Pinging 192.168.111.21 with 32 bytes of data:
Reply from 192.168.111.21: bytes=32 time<1ms TTL=64
Reply from 192.168.111.21: bytes=32 time<1ms TTL=64
Reply from 192.168.111.21: bytes=32 time<1ms TTL=64
Reply from 192.168.111.21: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.111.21:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Параметр *Loss*, равный *0%*, указывает на полную связность между устройствами. Отличное от нуля значение говорит о возможных неполадках (электромагнитные наводки на кабель, неправильная настройка и т. п.).

Время передачи данных от мультиплексора до любого другого устройства можно определить при помощи команды мультиплексора ping. Сообщение *«Echo request time out»* говорит об отсутствии связности между мультиплексором и удалённым устройством.

Пример. Определение задержки при передаче данных между локальным и удаленными мультиплексорами. IP-адрес удаленного мультиплексора равен 192.168.0.22.

LPOS > *ping 192.168.0.22*
Echo reply 0.231ms

6.3.2 Проверка состояния интерфейса Ethernet

Для проверки состояния интерфейса используется команда ethstat.

Пример. Отображение статистики работы интерфейса Ethernet.

LPOS > *ethstat*
1. *SFP 0 OK full duplex 1000 Mb/s*
2. *ETH 1 no link*
3. *SFP 2 OK full duplex 10Gb/s*
4. *ETH 3 no link*

По каждому интерфейсу выводится информация об установлении соединения, режиме дуплекса и скорости работы.

7 Техническая поддержка

Техническая поддержка может быть получена от дистрибьютора, у которого был куплен мультиплексор. За дополнительной информацией, пожалуйста, обращайтесь к производителю.

8 Обновление программного обеспечения

8.1 Введение

Прошивка в мультиплексорах Sprinter TX 10G - это набор файлов расположенных в каталоге /mnt/ файловой системы мультиплексора, и заменой этих файлов производится обновление ПО мультиплексора. Файлы kernel.* - две копии ядра операционной системы. Файлы help.txt и menu представляют собой текстовые файлы, содержащие справочную информацию и структуру меню соответственно. Файлы в подкаталоге htdocs представляют собой набор файлов для встроенного web сервера и служат для организации web-интерфейса. Кроме файлов в каталоге /mnt/ существует начальный загрузчик устанавливаемый командами uploadboot и setboot, доступный только по специальному запросу в службу поддержки. Не меняйте без абсолютной необходимости начальный загрузчик и не используйте указанные команды без твердой уверенности в правильности своих действий, так как это может привести к неработоспособности мультиплексора, а в ряде случаев к утрате гарантии на него.

8.2 Процедура обновления ПО

1. подключитесь к мультиплексору, используя FTP клиента Total Commander или Windows Explorer в пассивном режиме;
2. Скопируйте файл LPOS_XXXXXXX.zip (где XXXXXXX – версия) в папку /mnt/, в процессе копирования произойдет автоматическое обновление ПО;
3. проконтролируйте, что в файле /mnt/cfg.sys не содержится команд и ключей, не поддерживаемых новой версией ПО, при необходимости скорректируйте файл cfg.sys;
4. перезапустите мультиплексор командой reset.

8.3 Процедура обновления bootloader’a

Не производите обновление программного обеспечения, если не уверены в правильности своих действий. В подавляющем большинстве случаев обновление не требуется.

Для обновления bootloader’a через сеть необходимо с помощью FTP клиента скопировать в каталог /mnt файл lposboot.bin, затем в telnet сессии выполнить команду:

setboot /mnt/lposboot.bin

файл загрузчика будет перемещен в область начального загрузчика.

Для обновления bootloader’a через последовательный порт необходимо в консольной сессии (например, используя hiperterminal) выполнить команду

uploadboot

затем используя протокол X-Modem залить файл lposboot.bin

9 Гарантии изготовителя

Мультиплексор прошёл предпродажный прогон в течение 48 часов. Изготовитель гарантирует соответствие мультиплексора техническим характеристикам при соблюдении пользователем условий эксплуатации, транспортирования и хранения.

Срок гарантии указан в гарантийном талоне изготовителя.

Изготовитель обязуется в течение гарантийного срока безвозмездно устранять выявленные дефекты путём ремонта или замены мультиплексора или его модулей.

Если в течение гарантийного срока:

• пользователем были нарушены условия эксплуатации, приведенные в разделе 1.3, или на мультиплексор были поданы питающие напряжения, не соответствующие указанным в разделе 1.3.2;

• мультиплексору нанесены механические повреждения;

• интерфейсы мультиплексора повреждены внешним опасным воздействием,

то ремонт осуществляется за счет пользователя.

Доставка неисправного мультиплексора в ремонт осуществляется пользователем.

Гарантийное обслуживание прерывается, если пользователь произвел самостоятельный ремонт мультиплексора (в том числе, замену встроенного предохранителя).