Начальная настройка коммутаторов Extreme Networks

Содержание


extreme
networks

1. Документация

Данный текст не является официальным документом по настройке оборудования компании Extreme Networks. Цель данного документа – быстрое базовое знакомство с настройкой коммутаторов Extreme.

На официальном сайте Компании Extreme Networks www.extremenetworks.com, по ссылке http://www.extremenetworks.com/Resources/library.aspx можно найти следующие документы:

- Hardware Installation Guides
- Command Reference
- Concepts Guide
- Data sheets

Основными документами по настройке оборудования являются Concept Guide и Command Reference.

Кроме того, есть неофициальный блог: http://extremeblogger.ru/ на котором можно найти дополнительную информацию.
Все остальные ресурсы в зоне .ru никакого отношения к Компании Extreme Networks не имеют и могут содержать ошибочную или устаревшую информацию.

Программное обеспечение и Release Notes к ПО необходимо получать у поставщиков оборудования Extreme Networks.

2. Подключение к коммутатору

2.1. Введение

ExtremeXOS представляет из себя многоуровневую модульную ОС и, в сравнении с монолитной ОС, позволяет снять многие ограничения ей присущие. За счет такой архитектуры ОС удалось достичь высокой доступности за счет устойчивости к программным и аппаратным сбоям, способности динамически останавливаться/перезапускаться, а также загружать/выгружать программные модули, не влияя на сетевые операции,

Все фиксированные коммутаторы Summit используют единый файл операционной системы. Все модульные коммутаторы BlackDiamond так же используют единый файл операционной системы, что позволяет избежать проблем совместимости ОС.

Каждый коммутатор Extreme имеет выделенный Ethernet порт для out of band управления, а так же консольный RS232 порт.

У коммутаторов Extreme существует понятие Virtual Router (VR), представляющее собой логическую сущность, которой принадлежат порты и VLAN коммутатора. В каждом VR своя таблица коммутации и маршрутизации.
По умолчанию, в коммутаторе созданы VR-Mgmt, которому принадлежит Management порт и VR-Default, которому принадлежат все остальные порты коммутатора.
Так же можно создавать свои VR.

Каждый коммутатор имеет два раздела для хранения образов операционной системы коммутатора. Эти разделы называются primary и secondary. Соответственно на эти два раздела можно установить два разных образа ПО.
Для просмотра, какая версия ПО загружена и какая версия будет выбрана при следующей загрузке необходимо выполнить команду:
show switch

SysName: VDB
SysLocation:
SysContact: support@extremenetworks.com, +1 888 257 3000
System MAC: 00:04:96:26:6D:76
System Type: X450e-48p

SysHealth check: Enabled (Normal)
Recovery Mode: All
System Watchdog: Enabled

Current Time: Tue Sep 20 22:13:16 2011
Timezone: [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time: Tue Sep 20 22:11:28 2011
Boot Count: 283
Next Reboot: None scheduled
System UpTime: 1 minute 48 seconds

Current State: OPERATIONAL
Image Selected: primary
Image Booted: secondary
Primary ver: 12.5.2.6
Secondary ver: 12.4.2.17

Config Selected: primary.cfg
Config Booted: primary.cfg

primary.cfg Created by ExtremeXOS version 12.5.2.6
278372 bytes saved on Tue Aug 30 14:27:29 201

В примере выше загружено ПО версии 12.4.2.17 из раздела Secondary. При следующей перезагрузке коммутатора будет выбрано ПО версии 12.5.2.6 из раздела Primary.

Для изменения версии ПО, которая будет выбрана при следующей загрузке коммутатора, необходимо выполнить команду:
use image < primary / secondary >

Основной, используемый по умолчанию конфигурационный файл называется primary.cfg.

Так же стоит отметить поддержку различных скриптов. Их можно писать непосредственно во встроенном редакторе VI или загружать как файлы *.pol.

2.2. Доступ к консоли CLI коммутатора

Каждый коммутатор Extreme Networks имеет выделенный консольный порт для управления. В комплекте с коммутатором поставляется консольный шнур фиолетового цвета.

Ниже приведены настройки по умолчанию для консольного порта:

Table 1 – Настройки по умолчанию для консольного порта

Параметр	**Атрибут**
Physical Connectors	DB-9 / Male
Serial Equipment Type	Data Terminal Equipment (DTE)
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	XON/XOFF

Доступ к CLI возможен через консольный порт, протоколы telnet и SSH а так же через web интерфейс ExtremeXOS ScreenPlay.

По умолчанию коммутатор не имеет настроенных IP адресов. Соответственно к коммутатору «из коробки» доступ возможен только через консольный порт.
Возможность подключения по протоколу SSH появляется после установки дополнительного модуля, представляющего собой отдельный файл. Модуль совершенно бесплатен и может быть предоставлен партнером.

2.3. Доступ к web интерфейсу коммутатора

Web интерфейс коммутатора называется ExtremeXOS ScreenPlay.
Для включения доступа к ScreenPlay необходимо выполнить команду:
enable web http

2.4. Логины и failsafe account

Коммутатор поддерживает два уровня привилегий:

- User (доступ только на чтение)
- Administrator (полный доступ)

По умолчанию созданы две учетные записи: admin и user. Пароли у данных аккаунтов по умолчанию **пустые**.

Создание нового аккаунта:

create account [admin | user] <account-name> {encrypted <password>}

Для защиты от потери паролей пользователей, имеющих административный доступ, имеется возможность создать специальный failsafe аккаунт, который можно использовать для восстановления. Этот аккаунт не отображается при выполнении команды show accounts.

Настройка failsafe аккаунта производится следующим образом:
Настройка логина и пароля:
configure failsafe-account
enter failsafe user name: blue5green
enter failsafe password:
enter password again:

Настройка привилегий:
configure failsafe-account {[deny | permit] [all | control | serial | ssh {vr <vrname>} | telnet {vr <vr-name>}]}

2.5. Нумерация портов

В фиксированных моделях коммутаторов, не объединенных в стек, порты имеют сквозную нумерацию типа: 1, 2, 3.
В модульных коммутаторах, а так же в коммутаторах, объединенных в стек, порты имеют сквозную нумерацию типа <module>:<port>. Например, 3:1, 2:17, 5:23 итд.

При настройке коммутатора порты можно прописывать следующим образом:

- Через запятую: 1,12,23 или 1:1,2:27,3:23
- Через тире: 1-17 или 4:4-14
- Смешанно: 1-4,23 или 4:4-14,5:7

2.6. SSH

Возможность подключения по протоколу SSH появляется после установки дополнительного модуля, представляющего собой отдельный файл. Модуль совершенно бесплатен и может быть получен у сервисных партнеров компании Extreme Networks.

Ниже описана последовательность действий для активации модуля SSH2:

Для загрузки SSH модуля на коммутатор, необходимо выполнить команду:
download image 10.10.10.2 summitX-12.7.1.3-ssh.xmod

Активация нового программного модуля:
run update

Запуск модуля SSH:
start process exsshd

Генерация нового ключа:
configure ssh2 key

Включение SSH2:
enable ssh2

2.7. Серийный номер коммутатора

Что бы посмотреть серийный номер коммутатора, необходимо выполнить команду:
show version
Switch : 800190-00-02 ***0634G-00406*** *Rev 2.0 BootROM: 1.0.5.5 IMG: 12.5.2.6*
XGM2-1 : N/A N/A Rev 0.0

Image : ExtremeXOS version 12.5.2.6 v1252b6 by release-manager
on Tue Mar 1 17:38:45 PST 2011
BootROM : 1.0.5.5

2.8. Лицензирование коммутатора

Коммутаторы Extreme Networks имеют следующие уровни лицензирования:

- L2-Edge

- Edge
- Advanced Edge
- Core

А так же два Feature Pack:

- Direct Attach
- MPLS

В приложении A Concept Guide можно найти таблицы с описанием каждого уровня лицензирования и Feature Pack.

Для того чтобы посмотреть текущий уровень лицензирования коммутатора, необходимо выполнить команду:
show license

Slot-1 Stack.1 # show licenses
Enabled License Level:
Advanced Edge
Enabled Feature Packs:
None
Effective License Level:
Advanced Edge
Slot-1 Stack.2 #

Новый лицензионный ключ имеет формат: xxxx-xxxx-xxxx-xxxx-xxxx и скачивается с сайта extremenetworks.com.

Для добавления новой лицензии необходимо выполнить команду:
enable license {software} <key>
Например:
enable license 2d5e-0e84-e87d-c3fe-bfff

3. ПО и конфигурационные файлы

3.1. Обновление ПО

Каждый коммутатор имеет два partition для хранения образов операционной системы коммутатора.
Загружать новое ПО необходимо на не активную partition.
Посмотреть ПО на коммутаторе можно выполнив команду show switch.

Для загрузки нового ПО на коммутатор необходимо иметь TFTP-сервер и доступ по IP между одним из VR коммутатора (VR-Mgmt или VR-Default) и TFTP сервером.

Для загрузки ПО нужно выполнить команду:

download image [[<hostname> | <ipaddress>] <filename> {{vr} <vrname>} | {<partition>}

Где:
Hostname – адрес TFTP сервера
Filename – имя файла
VRname – имя VR (VR-Mgmt или VR-Default) указывается обязательно
Partition – имя partition (primary или secondary) указывается обязательно

После загрузки и инсталляции ПО нужно выполнить команду show switch.

Для выбора загрузочного раздела (например, для загрузки нового ПО на secondary partition), необходимо выполнить команду:
use image secondary

3.2. Работа с конфигурациями

Для просмотра конфигурации необходимо выполнить команду
show configuration

Так же можно выводить конфигурацию по определенному блоку настроек:
show configuration rip
show configuration acl

Или вывести только необходимую информацию:

show configuration | include <>
show configuration | exclude <>
show configuration | begin <>

Для сохранения конфигурации в памяти коммутатора необходимо выполнить команду:
save configuration primary
или
save configuration

или просто
save

Существует две команды для выгрузки конфигурации на TFTP сервер:

tftp put <target-ip-addres> -vr <vr_name> <config-file-name>

upload configuration [<hostname> | <ipaddress>] <filename> {vr <vr-name>}

Если используется первая команда, tftp put, файл конфигурации выгружается в XML формате.
Если используется вторая команда, upload configuration, файл конфигурации выгружается в ASCII формате.

Выполнив команду show switch, можно узнать, какой файл используется для хранения конфигурации.
Для выбора используемого файла конфигурации, нужно выполнить команду:
use configuration [primary | secondary | filename]

4. Настройка портов

4.1. Настройка скорости и дуплекса на портах

configure port 1 auto off speed 100 duplex half
configure port 1:1-1:5 auto off speed 1000 duplex full
configure port 22 auto on

4.2. Включение и выключение портов

enable port 1
disable port 1:1-1:5

4.3. Просмотр настройки портов

show port config
Данные по портам будут постоянно обновляться, что удобно, так как не требуется постоянно выполнять одну и ту же команду для обновления статуса портов.

show port 1:1-1:3 config no-refresh
Ключ *no-refresh* позволяет вывести статистику по портам, без ежесекундного обновления.

show port 3,4,9-12 config no-refresh
Port Configuration

```
Port    Virtual    Port  Link  Auto   Speed      Duplex   Flow  Load   Media
        router     State State Neg  Cfg Actual Cfg Actual Cntrl Master Pri Red
================================================================================
3       VR-Default  E     R    ON  AUTO     AUTO             UTP
4       VR-Default  E     R    ON  AUTO     AUTO             UTP
9       VR-Default  E     R    ON  AUTO     AUTO             UTP
10      VR-Default  E     R    ON  AUTO     AUTO             UTP
11      VR-Default  E     R    ON  AUTO     AUTO             UTP
12      VR-Default  E     R    ON  AUTO     AUTO             UTP
================================================================================
        > indicates Port Display Name truncated past 8 characters
        Link State: A-Active R-Ready NP- Port not present L-Loopback
        Port State: D-Disabled, E-Enabled
        Media: !-Unsupported Optic Module
        Media Red: * - use "show port info detail" for redundant media type
```

4.4. просмотр VLAN на порту коммутатора

show vlan port <port>
show port 1 info detail

4.5. Port Utilization

show port utilization
show port 1-3 utilization bandwidth
show port 3:4,3:7 utilization packets
show port 17 utilization bytes

4.6. Просмотр статистики QoS

show port 1 qosmonitor no-refresh

4.7. Link Aggregation

Link Aggregation это технология, позволяющая объединять несколько физических каналов в один логический. В терминологии Cisco это называется EtherChannel.

Для создания LAG:
enable sharing <master port> grouping <port list>

Например:
enable sharing 1 grouping 1-2
enable sharing 5:3 grouping 5:3-5:4, 6:3-6:4

Для удаления LAG:
disable sharing <master port>

LACP
Для использования LACP в LAG, необходимо добавить слово LACP в конце команды:
Examples:
enable sharing 1 grouping 1-2 lacp
enable sharing 5:3 grouping 5:3-5:4, 6:3-6:4 lacp

Выбор алгоритма балансировки
Для выбора алгоритма балансировки, необходимо добавить ключ *algorithm address-based* перед ключем *lacp*:
enable sharing 1 grouping 1-3 algorithm address-based L3_L4 lacp

4.8. Jumbo Frames

Jumbo фреймы это Ethernet фреймы более 1522 байт. Максимальный размер фрейма 9216 байт.
По умолчанию jumbo фреймы **выключены**.

Для включения jumbo фреймов нужно выполнить команду:
enable jumbo-frame ports [all | <port_list>]

5. Настройка VLAN

В отличие от Операционных Систем некоторых других вендоров, конфигурация EXOS основывается на настройке VLAN.
Сначала создаются VLAN, потом на VLAN настраивается IP адрес, добавляется 802.1Q тег и порты.

После создания VLAN, ключевое слово “vlan” в командах настройки опционально.

5.1. Создание VLAN

create vlan Data
create vlan Voice

5.2. Создание loopback VLAN

create vlan "lpbk"
enable loopback-mode vlan lpbk

5.3. Настройка тэга 802.1Q в VLAN

configure Data tag 10
configure Voice tag 20

5.4. Настройка IP адреса в VLAN

Для настройки IP адреса на VLAN, необходимо выполнить команду:
configure vlan Data ipaddress 10.1.10.1 255.255.255.0
или
configure Voice ipaddress 10.1.20.1/24

Включение маршрутизации в VLAN
enable ipforwarding vlan Data

Или, для всех настроенных VLAN:
enable ipforwarding
По умолчанию маршрутизация в VLAN выключена.

5.5. Добавление и удаление портов в VLAN

В EXOS VLAN на портах могут быть тегированными (tagged) и не тегированными (untagged). На порту может быть только один untagged VLAN и любое количество tagged VLAN.

Добавление untagged VLAN на порт коммутатора:

configure Data add port 1-12

Добавление tagged VLAN на порт коммутатора:
configure Data add port 2:45-48 tagged

По умолчанию, если не указывать untagged или tagged, VLAN на порту будет не тегированным.

5.6. Просмотр VLAN

show vlan

```
--------------------------------------------------------------------------------
Name         VID  Protocol Addr       Flags              Proto  Ports    Virtual
                                                          Active   router
                                                         /Total
--------------------------------------------------------------------------------
data         11   192.168.11.100 /24  -f-------o--------P------ ANY    0 /18  VR-Default
Default       1   ------------------------------------------- ANY    0 /0   VR-Default
ecv          3999 ------------------------------------C------ ANY    0 /2   VR-Default
Mgmt          4095 ------------------------------------------ ANY    0 /1   VR-Mgmt
ridge        31   192.168.31.100 /24  -f-------o--------P------ ANY    0 /2   VR-Default
voice        21   192.168.21.100 /24  -f-------o--------P------ ANY    0 /2   VR-Default
wireless      41   ------------------------------------P------ ANY    0 /8   VR-Default
--------------------------------------------------------------------------------
Flags : (B) BFD Enabled, (c) 802.1ad customer VLAN, (C) EAPS Control VLAN,
        (d) NetLogin Dynamically created VLAN, (D) VLAN Admin Disabled,
        (E) ESRP Enabled, (f) IP Forwarding Enabled,
        (F) Learning Disabled, (i) ISIS Enabled, (I) Inter-Switch Connection VLAN for
MLAG,
        (L) Loopback Enabled, (l) MPLS Enabled, (m) IPmc Forwarding Enabled,
        (M) Translation Member VLAN or Subscriber VLAN,
        (n) IP Multinetting Enabled, (N) Network Login VLAN, (o) OSPF Enabled,
        (O) Flooding Disabled, (p) PIM Enabled, (P) EAPS protected VLAN,
        (r) RIP Enabled, (R) Sub-VLAN IP Range Configured,
        (s) Sub-VLAN, (S) Super-VLAN, (t) Translation VLAN or Network VLAN,
        (T) Member of STP Domain, (V) VPLS Enabled, (v) VRRP Enabled, (W) VPWS
Enabled

Total number of VLAN(s) : 7
```

5.7. Просмотр таблицы коммутации

Таблица коммутации в Extreme называется Forwarding DataBase (FDB).
Для просмотра FDB используются команды:

show fdb
show fdb [vlan] <vlan name>
show fdb ports <port list>
show fdb <mac_address>

Для очистки FDB, необходимо выполнить команду:
clear fdb

6. Rapid-PVSTP

Spanning Tree Protocol — сетевой протокол, работающий на втором уровне модели OSI и предотвращающий появления петель в кольцевых топологиях. Протокол STP описан в стандарте IEEE 802.1D.
Значительно позже появился протокол Rapid Spanning Tree Protocol (RSTP), характеризующийся гораздо меньшим временем сходимости и более высокой устойчивостью. Протокол STP описан в стандарте IEEE 802.1W.
Rapid Per-VLAN STP (Rapid-PVST) расширяет функциональность STP, в каждом VLAN работает отдельный экземпляр STP. Данный протокол является проприетарным расширением Cisco.

У Cisco Rapid-PVST реализован так, что в untagged vlan (по умолчанию vlan 1) пакеты BPDU отправляются на MAC-адрес 01:80:C2:00:00:00 (это стандартный MAC для протокола STP, 802.1D) и на MAC-адрес 01:00:0c:cc:cc:cd, во всех остальных vlan, пакеты BPDU отправляются на MAC-адрес 01:00:0c:cc:cc:cd.

Для настройки протокола STP на коммутаторе Extreme необходимо выполнить следующие действия:

Создать два домена STP:
create stpd stpd100
create stpd stpd200

Настройка доменов STP как Rapid STP:
configure stpd stpd100 mode dot1w
configure stpd stpd200 mode dot1w

Добавляем vlan vl100 на порт 1 как теггированный, и vl200 на порт 1 как не теггированный:
configure vlan vl100 add ports 1 tagged
configure vlan vl200 add ports 1 untagged

Как уже писалось выше, для теггированных vlan (vl100) прописываем инкапсуляцию pvst-plus:
configure stpd stpd100 add vlan vl100 ports 1 pvst-plus

Для не теггированных vlan (vl200), прописываем инкапсуляцию dot1d:
configure stpd stpd200 add vlan vl200 ports 1 dot1d

Если vlan хоть где-то теггируется, для домена STP нужно прописать тэг. С этим тегом будут передаваться пакеты BPDU этого домена:
configure stpd stpd100 tag 100

В этом примере vlan vl200 прописан только на порту 1 и не теггированный, соответственно тэг для домена stpd200 писать не требуется.

Включение доменов STP:
enable stpd stpd100 ports 1
enable stpd stpd100 ports 1

enable stpd stpd100
enable stpd stpd200

Можно так же прописать инкапсуляцию по умолчанию:
configure stpd "stpd100" default-encapsulation pvst-plus

Проверить работу протокола можно, выполнив команду: show stpd stpd100

```
* sc-vlab-x480-24x-02@R6.28 # sh stpd "stpd100"
Stpd: stpd100           Stp: ENABLED            Number of Ports: 1
Rapid Root Failover: Disabled
Operational Mode: 802.1W                        Default Binding Mode: PVST+
802.1Q Tag: 100
Ports: 1
Participating Vlans: vl100
Auto-bind Vlans: (none)
Bridge Priority: 32768
BridgeID:               80:00:00:04:96:51:94:94
Designated root:        80:00:00:04:96:51:94:94
RootPathCost: 0         Root Port: ----
MaxAge: 0s              HelloTime: 2s           ForwardDelay: 0s
CfgBrMaxAge: 20s        CfgBrHelloTime: 2s      CfgBrForwardDelay: 15s
Topology Change Time: 35s                       Hold time: 1s
Topology Change Detected: FALSE                 Topology Change: FALSE
Number of Topology Changes: 0
Time Since Last Topology Change: 0s
```

Функция, альтернативная BPDU Guard у Cisco называется BPDU restrict. Функция позволяющая при появлении BPDU на порту коммутатора блокировать этот порт.
Например, для порта 21, настройка производится следующим образом:

configure stpd TEST_STP ports link-type edge 21
configure stpd TEST_STP ports edge-safeguard enable 21
configure stpd TEST_STP ports bpdu-restrict enable 21

7. Зеркалирование сетевого трафика

Настройка зеркалирования сетевого трафика состоит из двух действий:
Настройка порта, куда будет зеркалироваться трафик
enable mirroring to port 3:4
Настройка портов, откуда будет собираться трафик:
configure mirroring add port 6:5

Зеркалировать так же можно из списка контроля доступа.

Если происходит зеркалирование в несколько портов, необходим выделенный loopback порт:
enable mirroring to port-list 2:5-2:7 loopback-port 3:1
configure mirroring add port 6:5 ingress

Зеркалирование трафика из VLAN « red»:
enable mirroring to port 4
configure mirroring add vlan red

Зеркалирование трафика из VLAN « red» и из порта 5:
enable mirroring to port 4
configure mirroring add vlan red port 5

Отключение зеркалирования:
disable mirroring

8. IP Routing

7.1. Просмотр таблицы маршрутизации

show iproute

7.2. Просмотр IP интерфейсов на коммутаторе

show ipconfig

7.3. ARP

Просмотр ARP записей:
show iparp
show iparp <vlan name>
show iparp <ipaddress>
show iparp <macaddress>

Очистка ARP записей:
clear iparp
clear iparp <vlan name>
clear iparp <ipaddress>

7.4. Включение маршрутизации

Включение маршрутизации на VLAN:
enable ipforwarding [vlan] <vlan name>

Включение на всех VLAN:
enable ipforwarding

7.5. Создание статических маршрутов

config iproute add default <next hop gateway>
config iproute add default 10.1.1.1

config iproute add <subnet>/<mask> <next hop gateway>
config iproute add 10.1.8.x/24 10.1.10.1

7.6. OSPF

Настройка OSPF routerid:
config ospf routerid <router id>

config ospf routerid 1.1.1.1
enable ospf

Создание OSPF area*:*

create ospf area <area id>

Настройка OSPF router priority
config ospf [vlan] <vlan name> priority <0-255>

config ospf data priority 200

Можно настроить от 0 до 255. Чем выше, тем приоритетнее. По умолчанию приоритет равен 1. При приоритете 0 маршрутизатор не участвует в выборе DR.

Добавление VLAN в OSPF:
config ospf add Data area 0.0.0.0
enable ospf

Выключение VLAN из OSPF:
config ospf delete Data

Просмотр состояния протокола:
show ospf

Просмотр состояния OSPF соседей:
show ospf neighbor

7.7. VRRP

Настройка VRRP:
create vrrp Data vrid 1
config vrrp Data vrid 1 add 10.1.10.1

create vrrp vlan Voice vrid 2
config vrrp Voice vrid 2 add 2 10.1.20.1
enable vrrp

Просмотр настроек и состояния VRRP:
show config vrrp
show vrrp

9. Switch management

8.1. Включение доступа через Web

enable web http

8.2. SNMP

configure snmp add community readonly new_ro
configure snmp add community readwrite new_rw

Настройка SNMP System Name (меняет и имя коммутатора)
config snmp sysname "new name"

8.3. Настройка DHCP сервера

configure vlan test ipaddress 10.1.10.1/24
configure vlan test dhcp-address-range 10.1.10.100 – 10.1.10.150
configure vlan test dhcp-options default-gateway 10.1.10.1
enable dhcp port 1:1-1:12 vlan test

8.4. Настройка DHCP/BOOTP Relay

Технология DHCP-Relay позволяет перенаправлять DHCP запросы между разными подсетями. В коммутаторах Cisco подобная технология настранвается, используя команду ip helper-address.

Для настройки DHCP-Relay в VLAN vl40 DHCP сервера 192.168.1.100, необходимо выполнить команды:

configure trusted-servers vlan vl40 add server 192.168.1.100 trust-for dhcp-server
configure bootprelay add 192.168.1.100 vr VR-Default
configure bootprelay dhcp-agent information option vr VR-Default
enable bootprelay vr VR-Default vlan vl40

8.5. NTP клиент и сервер

Протокол NTP используется для синхронизации точного времени между сетевыми устройствами.

Часовой пояс настраивается следующим образом:

configure timezone {name <tz_name>} <GMT_offset>
{autodst {name <dst_timezone_ID>} {<dst_offset>}
{begins [every <floatingday> | on <absoluteday>] {at <time_of_day_hour>
<time_of_day_minutes>}
{ends [every <floatingday> | on <absoluteday>] {at <time_of_day_hour>
<time_of_day_minutes>}}}

Если автоматический переход на летнее и зимнее время не требуется (как, например, в России), автоматический переход можно отключить, используя команду:

configure timezone {name <tz_name>} <GMT_offset> noautodst

Например:
configure timezone name MST 180 noautodst

Для настройки NTP клиента используется команда:
configure sntp-client [primary | secondary] <host-name-or-ip> {vr <vr_name>}

Например:
configure sntp-client primary ntp.ntp.ru vr "VR-Default"

Для включений NTP клиента используется команда:
enable sntp-client

В случае когда ntp-сервер задан по имени хоста, требуется задать адрес dns-сервера:
configure dns-client add name-server X.X.X.X vr "VR-Default"

Настройка NTP сервера.

Для настройки NTP сервера используются следующие команды:
configure ntp [server | peer] add [<ip_address> | <host_name>] {key <keyid>} {option [burst | initial-burst]}
configure ntp restrict-list [add | delete] <network> {<mask>} [permit | deny]

Для включений NTP сервера используется команда:
enable ntp

Пример настройки NTP сервера:
enable ntp
create ntp key index 100 md5 EXTREME
configure ntp key index 100 trusted
enable ntp vlan internet
enable ntp vlan toSW2
enable ntp vlan toSW3
enable ntp vlan toSW3 broadcast-server key 100
config ntp server add 0.us.pool.ntp.org
config ntp server add 1.us.pool.ntp.org
config ntp local-clock stratum 10