# Программно-аппаратный комплекс управления и мониторинга промышленного коммутатора «ПрофиПлюс» серии PT536300

# Руководство пользователя

Версия документа: 01

Дата выпуска: 24/01/2025

# Содержание

# ПРЕДИСЛОВИЕ

Программно-аппаратный комплекс «ПрофиПлюс» серии PT536300 представляет собой 20-ти портовый промышленный управляемый коммутатор. ПАК «ПрофиПлюс» предназначен для коммутации и передачи данных в локальных вычислительных сетях (ЛВС) на 2-м уровне OSI (канальный уровень). Основное назначение коммутатора 2-го уровня — это коммутация пакетов на основе определения MAC-адреса кадра данных, осуществление передачи в соответствии с MAC-адресом, а также запись этих MAC-адресов и соответствующих портов в таблицу внутренних адресов.

Аппаратная часть оснащена 16 медными Ethernet портами 10/100/1000Base-T(X), двумя слотами для SFP модулей 100/1000Base-X и двумя слотами для SFP модулей 100/1000/2.5GBase-X. Корпус коммутатора адаптирован для установки на стандартную DIN-рейку и для монтажа на вертикальную или горизонтальную поверхность.

Промышленный гигабитный коммутатор 2 уровня «ПрофиПлюс» серии PT536300 поставляется со встроенным ПО «Программное обеспечение управления и мониторинга ПАК «ПрофиПлюс» и не требует загрузки дополнительного ПО (драйверов и т.п.) для начала работы.

Встроенное ПО «Программное обеспечение управления и мониторинга ПАК «ПрофиПлюс» является собственной разработкой компании «2Test» и позволяет осуществлять управление функционалом коммутатора с использованием интерфейса командной строки (CLI).

ПАК «ПрофиПлюс» поддерживает различные сетевые протоколы и отраслевые стандарты, такие как STP/RSTP, 802.1Q VLAN, HTTPS и т.д. Он также обладает набором функций управления, поддерживает настройку портов, статистику портов, контроль доступа, аутентификацию по стандарту 802.1X, быструю настройку, CLI, Telnet, SSH, SNMP. ПАК «ПрофиПлюс» имеет резервированное электропитание от двух независимых источников, которые обеспечивают бесперебойную работу при выходе из строя одного из них. ПАК «ПрофиПлюс» серии PT536300 не имеет внутренней вентиляции, выполнен в корпусе с радиатором для теплоотведения и эффективного рассеивания тепла, что обеспечивает работу в широком диапазоном температур от – 40 ºС до +75 ºС.

В данном руководстве пользователя промышленного коммутатора PT536300 представлены все необходимые для эксплуатации сведения:

- Управление функционалом коммутатора
- Конфигурация сетевого управления
- Обзор принципов сетевого управления
- Введение в CLI связанное с функциями сетевого управления
- Правила и методы конфигурации в CLI

Номер порта, указанный в данном руководстве, является лишь примером и не соответствует фактическому порту с этим номером на коммутаторе. При фактическом использовании предпочтение отдается номеру порта, который вы желаете использовать.

# I. НАЧАЛО РАБОТЫ

В этой главе описаны основные принципы использования интерфейса командной строки (далее – CLI). CLI — это комплексный интерфейс управления коммутатором.

В этом разделе описано, как выполнить следующие действия:

- Вход в систему и возврат к заводским настройкам
- Назначение имени хоста и пароля администратора
- Назначение IP-адреса в VLAN
- Проверка подключения с помощью ‘ping’
- Отображение текущей конфигурации и её сохранение на флэш-накопителе

Перед подключением к коммутатору необходимо подготовить персональный компьютер с операционной системой Windows 10 или выше и установленной на нём программой **PuTTY** (https://putty.org.ru/download.html) или аналогичной или Minicom в Linux.

## 1.1 Подключение к коммутатору через порт «Консоль»

Для управления коммутатором через интерфейс командной строки (CLI), на верхней панели коммутатора установлен последовательный порт «Консоль» RS-232 с разъёмом RJ45 для соединения с ПК. Схема соединения ПК и коммутатора показана на рисунке 1.

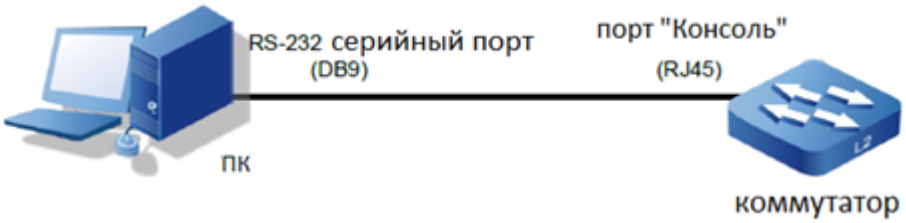



Рис. 1

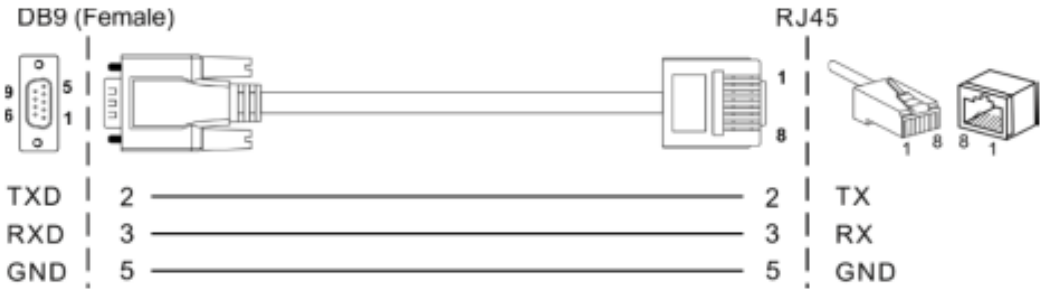



Рис. 2

Включите и настройте программу **PuTTY** для доступа к интерфейсу командной строки коммутатора.

Сочетание клавиш Win+x откроет на ПК меню «Диспетчер устройств». В диспетчере устройств определите работающий COM порт и укажите его номер в окне «Serial line» программы PuTTY. Настройки интерфейса **PuTTY** показаны на рисунках 3, 4 и в таблице 1.

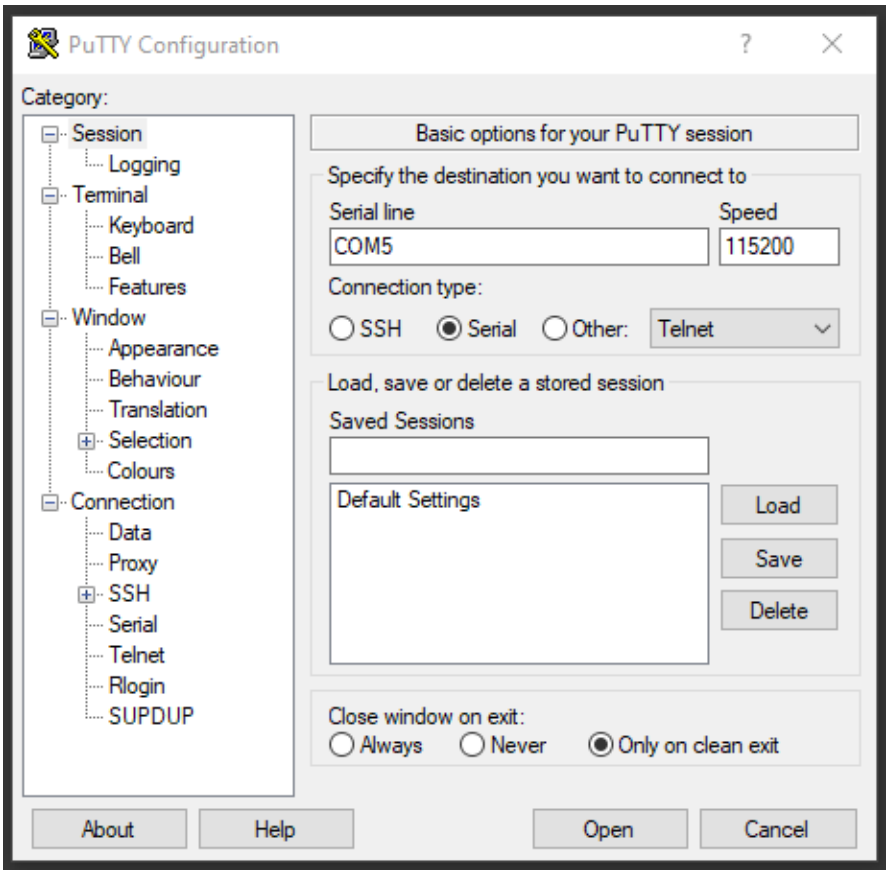

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Serial line
Speed
COM5
115200
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

Рис. 3

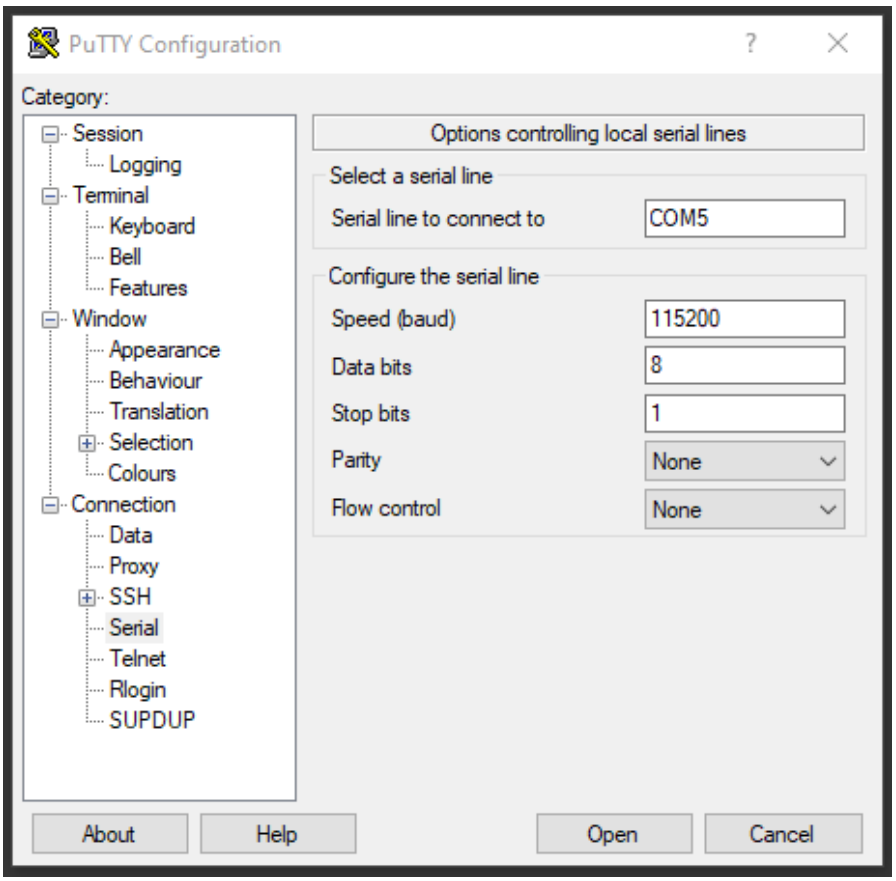

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Options controlling local serial lines
Select a serial line
Serial line to connect to
COM5
Configure the serial line
Speed (baud)
115200
Data bits
8
Stop bits
1
Parity
None
Flow control
None
About
Help
Open
Cancel

Рис. 4

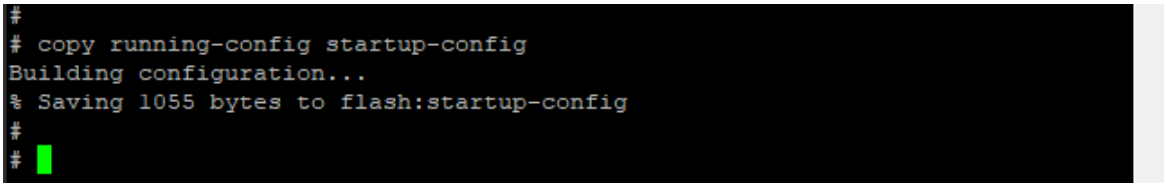
| Параметры порта Debug console | | |
|---|---|---|
| **Параметр** | **Значение** | **Описание** |
| Baud rate | 115200 | Скорость, бит/с |
| Data bits | 8 | Количество битов данных |
| Parity | None | Бит чётности |
| Stop bits | 1 | Количество стоповых битов |
| Hardware flow control | None | Аппаратный контроль потока |
| Software flow control | None | Программный контроль потока |

Таблица 1

После запуска программы PuTTY с указанными настройками появится диалоговое окно интерфейса командной строки. Нажмите ENTER для начала сессии. Введите имя пользователя «admin» и пароль «admin» для входа в интерфейс командной строки.

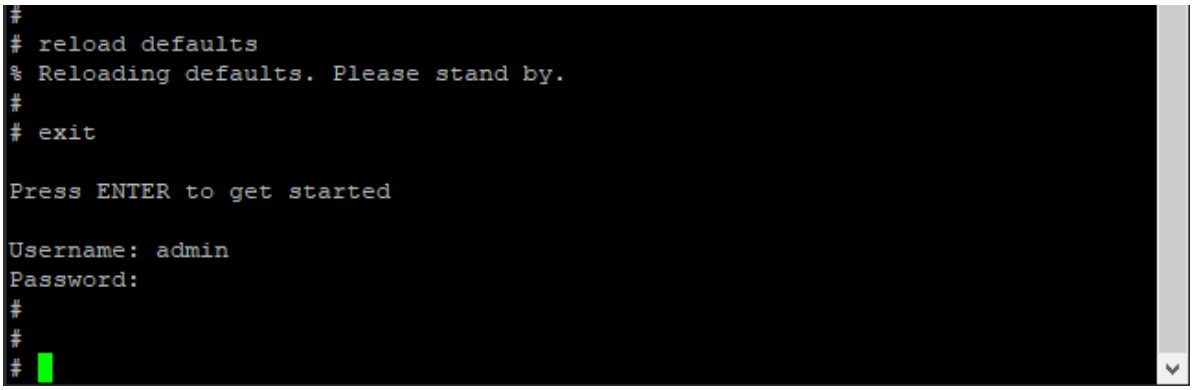

## 1.2 Вход в систему и возврат к заводским настройкам

После первого входа в систему, вам будет предложено изменить пароль. Из соображений безопасности пароль должен состоять не менее чем из 8 букв цифр и символов. После ввода нового пароля необходимо сохранить настройки. Для этого введите команду: `<copy running-config startup-config>`.




Если по каким-то причинам доступ к интерфейсу командной строки отсутствует, возврат к заводским настройкам можно выполнить с помощью DIP-переключателя (см. Руководство по эксплуатации).

Возврат к заводским настройкам с помощью командной строки выполняется командой `<reload defaults>`. После сброса настроек завершите работу с терминалом командой `<exit>` и снова авторизуйтесь.




### 1.3 SSH

Протокол SSH включен по умолчанию. Вы можете отключить SSH. Для этого войдите в режим конфигурации: <configure terminal>, затем введите команду <no ip ssh>.


После отключения SSH вы не сможете войти в CLI через сетевой порт (1-16). Чтобы включить SSH введите команду <ip ssh>.


### 1.4 Назначение имени хоста и пароля администратора

В CLI есть несколько различных режимов. Сразу после авторизации пользователь попадает в режим «выполнения команд» [EXEC]. Этот режим имеет значок **#**. В этом режиме вы можете выполнять операции, связанные с файлами конфигурации, перезагрузкой настроек по умолчанию, отображением системной информации и т.д., но не можете изменять подробные параметры конфигурации. Такие операции выполняются в режиме конфигурации.

Для назначения имени хосту/коммутатору войдите в режим конфигурации:

`# configure terminal`

`(config)#` (вы в режиме конфигурации)

Введите команду <hostname + имя хоста> (в нашем примере это 2test)

```
(config)# hostname 2test
```

2test(config)# (имя хоста назначено)

Выйдите из режима конфигурации:

```
2test(config)# exit
```

Завершите работу с терминалом и снова авторизуйтесь.

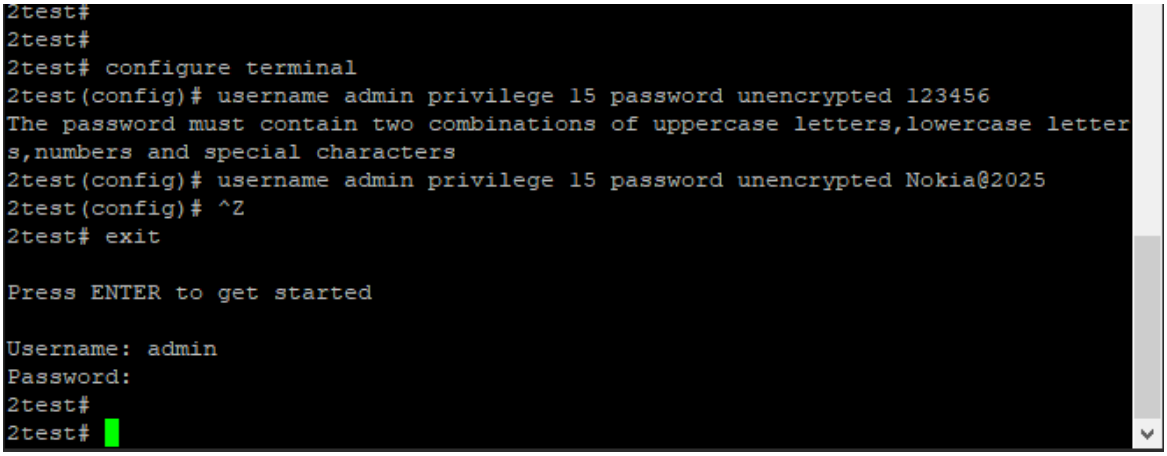
```
2test# exit
```


Для назначения нового пароля Администратора войдите в режим конфигурации:

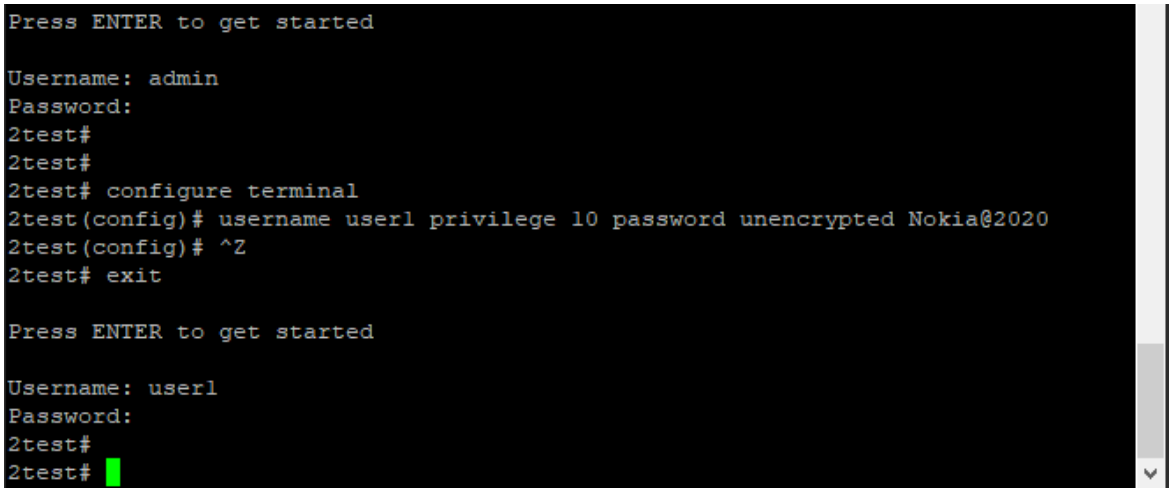
```
# configure terminal
```

Введите команду <username admin privilege 15 password unencrypted [ваш пароль]>

Обратите внимание, что правила безопасности не разрешают назначать простые пароли и требуют соблюдать правила.



Администратор может добавить новых пользователей аналогично приведенному примеру. Ниже показан пример добавления нового пользователя «user1» с уровнем привилегий «10» и паролем «Nokia@2020». Для возврата в режим [EXEC] используйте горячие клавиши Ctrl+z. Для возврата на предыдущий уровень используйте команду <exit>. В режиме [EXEC] для завершения сеанса и выхода из CLI используйте <exit>.




## 1.5 Использование DHCP и назначение IP-адреса в VLAN 1

VLAN 1 используется по умолчанию. Помните, что IP-адрес привязан к VLAN. IPv4 (IP-адрес) коммутатора по умолчанию 192.168.1.254, маска подсети 255.255.255.0 Назначая новый IP-адрес в VLAN 1 и не создавая новых VLAN, этот IP-адрес будет актуален для всех портов коммутатора. Этого часто бывает достаточно для небольших локальных сетей, использующих протокол динамической настройки хоста (DHCP) или статическое распределение IP-адресов.

В системе реализован DHCP-клиент, который после включения будет отправлять запросы на получение IP-адреса. Эти запросы принимаются DHCP-сервером в сети (если он существует и был соответствующим образом настроен). Затем сервер выполнит поиск в своем пуле доступных IP-адресов, выделит один из них и вернет его DHCP -клиенту. Возвращаемая информация обычно включает IP-адрес, маску подсети и шлюз по умолчанию, но также может содержать другую информацию, такую как служба доменных имен (DNS) и адреса серверов.

Эта настройка аналогична настройке имени хоста: войдите в режим конфигурации, <configure terminal> как это было в предыдущих примерах, затем введите команду: <interface vlan 1>. В CLI это будет выглядеть так:

```
2test(config)#
2test(config)# interface vlan 1
```

2test(config-if-vlan)#

теперь вы находитесь в режиме конфигурирования VLAN 1. В данном примере рассматривается вариант использования DHCP для получения IP-адреса или, в случае сбоя DHCP, использовать статический резервный адрес. Включение резервного IP-адреса является необязательным и может быть опущено. Для этого используйте команду: < ip address dhcp fallback 192.168.1.10 255.255.255.0>

2test(config-if-vlan)#

2test(config-if-vlan)# ip address dhcp fallback 192.168.1.10 255.255.255.0

Рассмотрим пример назначения IP-адреса в VLAN 1. Вы можете изменить как текущий IP-адрес в VLAN1, так и добавить ещё одну или несколько VLAN. Администратор может задать до 255 идентификаторов VLAN, включая VLAN 1, которая используется по умолчанию. Также обратите внимание, что IP-адреса могут быть назначены только интерфейсам VLAN. По аналогии с примером применения DHCP для изменения IP-адреса в текущей VLAN1 перейдите в режим конфигурации с помощью команды <configure terminal>. Далее введите имя VLAN IP-адрес которой требуется изменить <interface vlan1>. Затем введите нужный IP-адрес и маску подсети командой <ip address 192.168.1.10 255.255.255.0> – новый IP-адрес VLAN1 создан. Вернитесь в режим «EXEC» через команду <end>.

```
2test#
2test#
2test# configure terminal
2test(config)# interface vlan 1
2test(config-if-vlan)# ip address 192.168.1.10 255.255.255.0
2test(config-if-vlan)# end
2test#
2test#
```

Пользователь может проверить установленный им IP-адрес. Для этого введите команду <show ip interface brief>

```
#
# show ip interface brief
Interface        Address              Method   Status
---------------- -------------------- -------- ------
VLAN 1           192.168.1.10/24      Manual   UP
#
#
```

Для проверки соединения коммутатора с ПК по SSH и Telnet подключите Ethernet кабель к одному из медных портов коммутатора и проверьте соединение пингованием. Вы так же можете проверить соединение коммутатора с внешним узлом (обратным пингованием). Для этого в CLI коммутатора введите команду <ping ip 192.168.1.200> где

192.168.1.200 это адрес внешнего узла, с которым вы проверяете соединение, в данном примере это ваш ПК.

```
2test#
2test#
2test# ping ip 192.168.1.200
PING server 192.168.1.200, 56 bytes of data.
64 bytes from 192.168.1.200: icmp_seq=0, time=0ms
64 bytes from 192.168.1.200: icmp_seq=1, time=0ms
64 bytes from 192.168.1.200: icmp_seq=2, time=0ms
64 bytes from 192.168.1.200: icmp_seq=3, time=0ms
64 bytes from 192.168.1.200: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
2test#
2test#
```

## 1.6 Установка статического ARP

Для установки статического ARP введите команду:

`<ip arp [v_ipv4_abc] [v_mac_addr]>`

На примере показана установка статического ARP.

```
2test#
2test# configure terminal
2test(config)#
2test(config)# ip arp 192.168.1.253 00:10:00:00:01:01
2test(config)#
2test(config)#
```

Пример удаления статического ARP

```
2test#
2test# configure terminal
2test(config)# no ip arp 192.168.1.253
2test(config)#
2test(config)#
```

## 1.7 Просмотр и сохранение конфигурации во флэш-памяти

Текущая конфигурация устройства может быть отображена в виде виртуального файла, содержащего полный набор команд, необходимых для создания идентичной конфигурации. Существует несколько исключений, связанных с тем, что некоторые элементы, такие как закрытые SSH -ключи, не отображаются.

Этот файл называется **running-config** и является изменчивым по своей природе; он не сохраняется при перезагрузках. Поэтому необходимо сохранить файл на флэш-накопителе под именем **startup-config**, поскольку этот файл считывается и выполняется при каждой загрузке и, следовательно, отвечает за восстановление запущенной конфигурации системы до состояния, в котором она находилась на момент сохранения.

Команда <show running-config> отобразит параметры конфигурации, как показано ниже. Для краткости некоторые детали были отредактированы. Кроме того, набор интерфейсов зависит от возможностей оборудования.

```
2test#
2test# show running-config
Building configuration...
hostname 2test
username admin privilege 15 password unencrypted admin
username user1 privilege 10 password unencrypted Nokia@2020
!
vlan 1
!
!
!
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
```

```
!
interface GigabitEthernet 1/20
!
interface 2.5GigabitEthernet 1/17
!
interface 2.5GigabitEthernet 1/18
!
interface vlan 1
 ip address 192.168.1.10 255.255.255.0
!
!
spanning-tree aggregation
!
!
line console 0
!
line vty 0
!
line vty 1
```

Строчки в кавычках “ ” являются комментариями. Файл начинается с имени хоста – hostname и пароля для Администратора admin, за которыми следует имя и пароль Пользователя (user1). Далее описана VLAN 1 и другие элементы, такие как Протокол связующего дерева (STP). Далее следует список всех интерфейсов портов на устройстве, упорядоченный по идентификатору коммутатора, типу и номеру порта.

Все интерфейсы портов имеют настройки по умолчанию, поэтому для них ничего не отображается. Как правило, отображается только конфигурация, отличная от конфигурации по умолчанию, в противном случае выходные данные были бы огромными и

ухудшалась бы читаемость. Есть несколько исключений, которые будут рассмотрены позже.

За физическими интерфейсами следует интерфейс виртуальной сети VLAN 1 с указанием IP-адреса и маски подсети. Сейчас только первому из них присвоен IP-адрес. В конце отображается раздел «line». В нем указываются характеристики для последовательной консоли (строка console 0) или сетевых подключений для управления ICLI (строка vty x).

Команда <dir> выводит список файлов в файловой системе flash, в то время как команда <more> выводит содержимое указанного файла.

```
2test#
2test#
2test# dir
Directory of flash:
    r- 2025-01-29 07:48:08      292 default-config
    rw 2025-01-28 14:49:32     1055 startup-config
2 files, 1347 bytes total.
2test#
2test# more ?
    <url_file>    File in FLASH or on TFTP server. Syntax: <flash:filenam
e |
                  tftp://server/path-and-filename>. A valid file name is
a text
                  string drawn from alphabet (A-Za-z), digits (0-9), dot
(.),
                  hyphen (-), underscore (_). The maximum length is 63 an
d
                  hyphen must not be first character. The file name conte
nt
                  that only contains '.' is not allowed.
2test# more
% Incomplete command.

2test#
2test#
```

Конфигурация, показанная выше, сейчас содержится в файле **running-config**. Для сохранения текущей конфигурации в файл **startup-config** введите команду:

```
<copy running-config startup-config>
```

```
2test#
2test# copy running-config startup-config
Building configuration...
% Saving 1331 bytes to flash:startup-config
2test#
2test#
```

Настройки сохранены в файле startup-config.

Навыки, описанные в этом разделе, формируют основу для повседневной работы с CLI: вход в систему, отображение информации с помощью команды <show>, работа с файлами конфигурации <show running-config>, <copy>, <dir> и т.д., работы с фактической конфигурацией <configure terminal>, <exit>, и подрежимы <interface...>.

# II. ОСНОВЫ CLI

Ключевые характеристики CLI:

- CLI является модальным (определенные операции возможны или невозможны в определенных режимах);
- CLI имеет строчную структуру
- CLI выполняет действие мгновенно после ввода команды
- В основе действий лежат привилегии (для успешного выполнения определенных операций требуется, чтобы пользователь обладал определенным уровнем привилегий).

## 2.1

## 2.2 Структура и синтаксис команд

### 2.2.1 Структура

Команда — это одна строка текста, состоящая из ключевых слов и параметров, например: <show vlan id 10> Ключевыми словами являются show, vlan и id; в то время как 10 — это параметр, который может содержать другое значение при вызове другой команды. Ключевые слова не чувствительны к регистру, поэтому show и SHOW для машины идентичны. И наоборот, параметры могут быть чувствительны к регистру или нет, в зависимости от используемой команды и параметра.

Ключевые слова и некоторые параметры могут быть сокращены, если они являются однозначными. Например, эти команды идентичны:

```
2Test# configure terminal = con terminal
2Test# show interface GigabitEthernet 1/5 capabilities = sh in g 1/5 c
```

```
2Test#
2Test# sh in g 1/5 c

GigabitEthernet 1/5 Capabilities:
  Model:                    CEServices
  Type:                     10/100/1000BaseT
  Speed:                    10,100,1000,auto
  Duplex:                   half,full,auto
  Trunk encap. type:        802.1Q
  Trunk mode:               access,hybrid,trunk
  Channel:                  no
  Broadcast suppression:    no
  Flowcontrol:              yes
  Fast Start:               no
  QoS scheduling:           no
  CoS rewrite:              no
  ToS rewrite:              no
  UDLD:                     no
  Inline power:             no
  RMirror:                  no
  PortSecure:               no
  Dot1x:                    no
2Test#
```

Почему это так работает:

- Есть много ключевых слов, которые начинаются на "s", но только одно начинается на "sh"
- Есть несколько команд, которые начинаются с "показать i", но только одна начинается с "показать in"
- Команда `<show interface>` использует тип порта в качестве параметра. В зависимости от аппаратной функции, возможны следующие варианты: Fast Ethernet, GigabitEthernet, 2,5 гигабитного интернета, 5 гигабитного интернета и 10 гигабитного интернета. Таким образом, "g" — это уникальная аббревиатура для обозначения GigabitEthernet
- При указании интерфейса (например) 1/5 интерфейс идентифицируется как принадлежащий коммутатору 1, порт 5. Этот параметр не может быть сокращен и должен быть указан полностью.
- Команда `<show interface GigabitEthernet 1/5>` может выводить различную информацию: функции, статистику, статус и другую информацию. В данном случае ‘c’ — это уникальное сокращение для обозначения возможностей – capabilities.

При небольшой практике это позволяет выполнять ввод с клавиатуры с высокой эффективностью, особенно в сочетании с функциями контекстно-зависимой справки CLI (см. Контекстно-зависимая Справка).

### 2.2.2 Синтаксис

Команда описывается ее синтаксисом, например: **<show interface list>** {*status* | *statistics* | *capabilities* | *switchport* | *veriphy*}

и

**<show vlan>** [ *id* <*vlan_list*> | *name* <*name*> | *brief*]

Семантика:

- ключевые слова выделены жирным шрифтом.
- параметры выделены курсивом.
- [ ... ] указывает на необязательную конструкцию: она может присутствовать, а может и не присутствовать.
- { ... } указывает на группировку; конструкции внутри нее принадлежат друг другу
- ‘|’ указывает на выбор между двумя или более альтернативами (например, a | b | c, что читается как “a или b или c”).

Таким образом, синтаксис первой команды прост: сначала **show**, затем **interface**, затем список интерфейсов, затем ровно один `из status, statistics, capabilities, switchport` и `veriphy`.

Вторая команда немного сложнее: **show** и **vlan** обязательны, но остальные параметры и ключевые слова необязательны: пользователи могут ввести id, имя или краткое описание.

Например:

- Отобразить информацию о состоянии VLAN:
  `mydevice# show vlan`
- Отображать информацию о состоянии указанного идентификатора VLAN:
  `mydevice# show vlan id 1`
- Отображать информацию о состоянии указанного имени VLAN:
  `mydevice# show vlan name VLAN0002`

Где (mydevice#) – имя хоста.

Есть несколько немного более сложных особенностей синтаксиса, которые сосредоточены вокруг последовательностей необязательных элементов, таких как [a] [b] [c].

- Каждое из значений a, b, c может присутствовать, а может и не присутствовать (“a c” допустимо, как и отсутствие ввода)
- Порядок не важен (“a c” и “c a” эквивалентны)
- Каждый дополнительный элемент может присутствовать ровно ни разу или только один раз (не повторяться).

Есть разные варианты:

- Группа опций, из которых должна присутствовать хотя бы одна: _BOS_ [a] [b] [c] }*1
- Группа опций, в которых одна или несколько опций имеют фиксированное положение: [a] {[b]} [c]
- Это говорит о том, что "b" необязательно, но если оно присутствует, то оно должно следовать после "a" (если присутствует "a") и перед "c" (если присутствует "c").

Например, предположим, что команда имеет такой синтаксис:

a [b] [c] {d | e} {[f] [g]} *1

тогда допустимыми примерами ввода являются:

- ‘a d f", поскольку "b" и "c" являются необязательными, "d" выбирается вместо "e", а "f" выбирается в качестве обязательного необязательного
- "a d f g", поскольку "b" и "c" являются необязательными, "d" выбирается вместо "e", и оба "f" и "g" выбираются в последней группе необязательных
- "a c b e g", поскольку необязательный параметр "b" опущен, вместо "d" выбирается "e", а для обязательного необязательного параметра выбирается "g".

## 2.2 Имя и нумерация Ethernet порта

Интерфейс Ethernet, или порт, идентифицируется тремя элементами информации:

- Тип (FastEthernet, GigabitEthernet, 2,5GigabitEthernet, 5GigabitEthernet, 10 Gigabit Ethernet);
- К какому коммутатору относится порт (для систем без стекирования это значение всегда равно 1;
- Номер порта в пределах типа и коммутатора (нумерация начинается с 1 для каждого типа, поэтому коммутатор может иметь как GigabitEthernet 1/1, так и 2,5GigabitEthernet 1/1).

Многие команды CLI поддерживают список интерфейсов. В своей простейшей форме такой список представляет собой последовательность информации (тип, идентификатор коммутатора, номер порта), разделенную пробелом. Например: GigabitEthernet 1/3 10GigabitEthernet 1/2. Это позволяет смешивать различные типы в одном списке.

Идентификатор коммутатора и номера портов могут быть указаны либо в виде отдельных чисел, либо в виде списка, либо в виде последовательности. Список представляет собой набор отдельных номеров портов или последовательностей, разделенных запятыми, в то время как последовательность имеет вид: от—до.

Вот несколько примеров:

- GigabitEthernet 1/5 для единственного гигабитного порта с номером 5 на коммутаторе 1
- GigabitEthernet 1/2,4,10-12 для гигабитных портов 2, 4, 10, 11, 12 на коммутаторе 1
- GigabitEthernet 1-3/2 для гигабитного порта 2 на коммутаторах 1, 2 и 3

Для обозначения типа и/или идентификатора коммутатора и/или портов можно использовать подстановочный знак, означающий “все типы”, “все идентификаторы коммутатора” и “все порты” соответственно. Подстановочный знак пишется со звездочкой вместо типа, идентификатора коммутатора или порта, возможны и другие сокращения:

- “*” означает “порты всех типов всех коммутаторов”
- Тип “*” означает “все порты указанных типов всех коммутаторов”

Для наглядности приведем несколько примеров. Предположим, что в стеке есть два коммутатора с идентификаторами коммутаторов 1 и 3. Каждый коммутатор имеет 9 гигабитных портов и два порта по 2,5 гигабита. Затем:

- интерфейс * (или: interface * * *) Все порты всех типов на всех коммутаторах: GigabitEthernet 1,3/1-9 2,5GigabitEthernet 1,3/1-2
- интерфейс * 1/2 Коммутатор 1, номер порта 2 всех типов: GigabitEthernet 1/2 2.5GigabitEthernet 1/2

- интерфейс * */2 Все коммутаторы всех типов, номер порта 2: GigabitEthernet 1,3/2 2.5GigabitEthernet 1,3/2
- интерфейс * */4 Все коммутаторы, всех типов, номер порта 4: GigabitEthernet 1,3/4

В результате отсутствуют 2,5-гигабитные порты.

- интерфейс GigabitEthernet 3/* Коммутатор 3, все гигабитные порты: GigabitEthernet 3/1-9
- интерфейс 2.5GigabitEthernet * (или: интерфейс 2.5GigabitEthernet */*) Все 2,5-гигабитные порты на всех коммутаторах: 2,5-гигабитный Интернет 1,3/1-2

Wildcards будут включать максимально возможный набор портов, но могут выдавать сообщение об ошибке, если определенный идентификатор коммутатора или номер порта не существует.

Например, эти записи являются недопустимыми:

- интерфейс * 2/* Все порты всех типов на коммутаторе 2, который не является членом стека
- интерфейс * */100 Ни на одном коммутаторе нет порта 100 любого типа
- интерфейс GigabitEthernet */* 2,5GigabitEthernet 2/* Опять же, стек коммутаторов 2 не существует, поэтому весь набор считается недействительным

Допустимость определяется для каждого набора данных (тип, идентификатор коммутатора, порт), содержащих подстановочные знаки: результат для этого набора считается допустимым, если хотя бы один порт соответствует заданному набору. Список наборов действителен, если все наборы соответствуют хотя бы одному порту в каждом.

## 2.3 Использование «горячих клавиш» в CLI

Интерфейс командной строки предоставляет богатый набор клавиш, помогающих пользователю при работе с командной строкой. Функциональность разделена на:

- Простое редактирование строк
- История команд
- Контекстно-зависимая справка
- Длинные команды и разбивка на страницы

### 2.2.3 Основные команды для редактирования строк

| КОМАНДА | ДЕЙСТВИЕ |
|---|---|
| Left/Right | Переместить курсор влево/вправо |
| Home/Ctrl-A | Переместить курсор в начало строки |
| End/Ctrl-E | Переместить курсор в конец строки |
| Del/Ctrl-D | Удалить символ при наведении курсора |
| Backspace/Ctrl-H | Удалить символ справа от курсора |
| Ctrl-N Delete | Удалить всю текущую строку целиком |
| Ctrl-U/Ctrl-X | Удалить все символы слева от курсора |
| Ctrl-K | Удалить все символы под курсором и справа |
| Ctrl-W | Удалить от курсора до начала слова слева |
| TAB | Дополнить слово автоматически |

### 2.2.4 История команд

В сеансе сохраняется непостоянная история ранее введенных командных строк. История может содержать до 32 строк. После заполнения в новой строке будет удалена самая старая запись.

| КОМАНДА | ДЕЙСТВИЕ |
|---|---|
| Up/Ctrl-P | Предыдущая строка в истории команд |
| End/Ctrl-E | Следующая строка в истории команд |

Количество строк, сохраняемых в истории для текущего сеанса, настраивается в диапазоне от 0 до 32, где 0 полностью отключает историю.

Просмотреть историю команд: `# <show history> [ENTER]`

### 2.2.5 Контекстно-зависимая справка

В ICLI реализовано несколько сотен команд, от самых простых до очень сложных. Поэтому крайне важно, чтобы пользователю была предоставлена помощь в вводе синтаксически правильных команд, а также в поиске соответствующих команд. Эти задачи поддерживаются функциями контекстно-зависимой справки.

Горячие клавиши контекстно-зависимой справки:

| КОМАНДА | ДЕЙСТВИЕ |
|---|---|
| ? | Показать следующий возможный ввод и описание |
| ??/Ctrl-Q | Показать синтаксис возможных команд |
| TAB | Показать следующий возможный ввод без описания или развернуть текущее слово, если оно однозначное |

В контекстно-зависимой справке отображаются только те команды, которые доступны на текущем уровне привилегий сеанса.

```
2Test#
2Test# show a?
    aaa             Authentication, Authorization and Accounting methods
    access-list     Access list
    alarmlog        System logging message
2Test#
```

Использование контекстно-зависимой справки очень простое. Правило: команда «знак вопроса» показывает все возможные команды интерфейса в данном меню, команда «Tab» завершает ввод команды после первой/второй буквы.

### 2.2.6 Длинные строки и разбивка на страницы

Конфигурация сеанса определяет ширину терминала в символах и длину в строках. Эти параметры используются для управления обработкой длинных строк ввода и разбивкой многострочного вывода на страницы. Более подробную информацию об изменении этих параметров см. в разделе «Общие сведения о параметрах терминала».

Длинные строки вступают в силу, когда длина строки превышает ширину терминала за вычетом подсказки. В этом случае часть строки будет скрыта от отображения, что обозначается символом "$" в начале и/или конце видимой части строки.

Разбивка на страницы появляется каждый раз, когда выполнение команды приводит к выводу большего количества строк, чем было настроено в качестве длины терминала. Типичным примером является вывод <show running-config>. После вывода первых нескольких строк отображается запрос на разбивку на страницы:

```
-- more --, next page: Space, continue: g, quit: ^C
```


Эти «горячие клавиши» управляют разбивкой на страницы:

| КОМАНДА | ДЕЙСТВИЕ |
|---|---|
| Enter | Отобразить следующую строку вывода |
| Space | Отобразить следующую страницу вывода |
| G | Отображать оставшуюся часть выходных данных без дополнительной разбивки на страницы |
| Q/Ctrl+C | Завершить вывод информации |
| Any other key | Отобразить следующую страницу вывода. Некоторые клавиши терминала (стрелки, Home, End и т.д.) могут отображаться в CLI в виде нескольких символов, что приводит к быстрому выводу нескольких страниц подряд. |

Длину терминала (также иногда называемую высотой) можно настроить для текущего сеанса с помощью команды `<terminal length lines>`. Если введено значение `lines = 0`, разбивка на страницы отключена.

**Ctrl+z** – из режима общей конфигурации быстро вернуться в режим # [EXEC].

**Ctrl+C** – прекратить вывод запрошенной информации

## 2.4 Фильтрация выходных данных команд

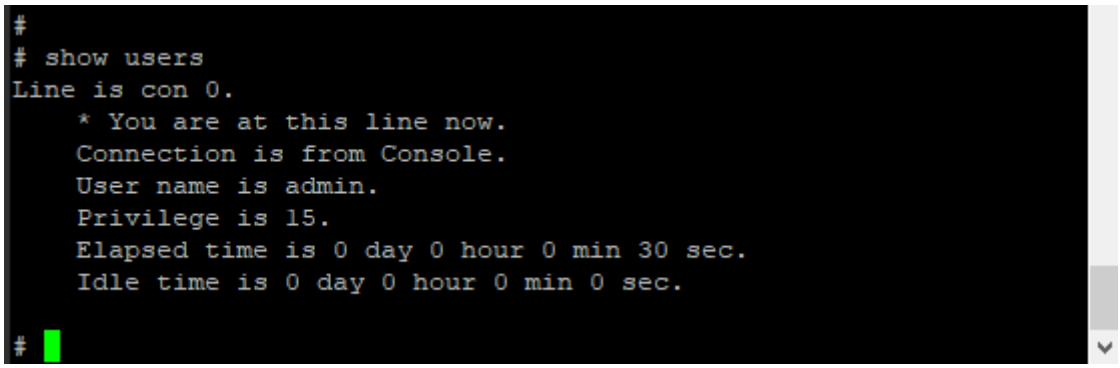
В большинстве случаев выходные данные команд могут быть отфильтрованы. Можно ограничить вывод только теми строками, которые соответствуют определенной подстроке или инициируют ее. Доступна следующая фильтрация:

- Начать – отобразить первую строку, которая соответствует, и все последующие строки;
- Включить – отобразить именно те строки, которые соответствуют;
- Исключить – отобразить именно те строки, которые не соответствуют. В строке учитывается регистр символов.

Синтаксис:

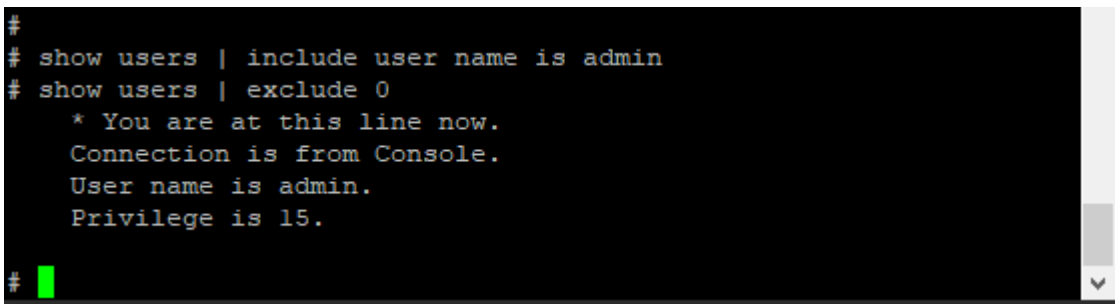
`command '|' { begin | include | exclude } string`

Введите команду, которая генерирует некоторый вывод информации, изначально фильтрация не выполняется, например <show users>

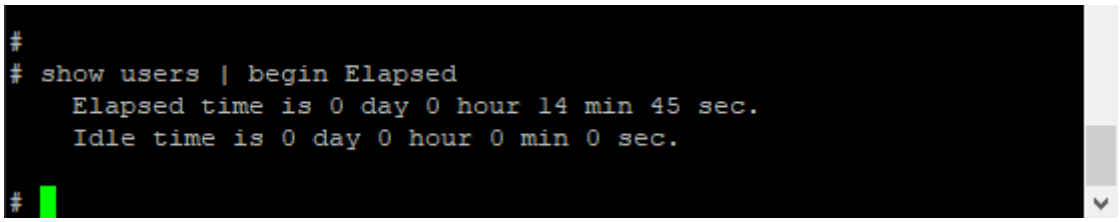



Отфильтруйте, чтобы включить конкретное слово в команду <show users>:

- включить имя пользователя admin.
- исключить все строки, содержащие "0' (ноль)



Начните вывод данных, когда будет найдено определенное слово:




## 2.5 Понятия режима и подрежима

В CLI реализован ряд режимов, которые управляют доступным набором команд. Режимы также зависят от уровня привилегий пользователя; некоторые режимы или команды доступны только администраторам, в то время как для других не требуется никаких привилегий, кроме входа в систему.

В CLI коммутатора «ПрофиПлюс» серии PT536300 существует три основных режима: [EXEC], привилегированный [EXEC] и [Config]. В разделе **Config** существует несколько подрежимов. Подрежимы позволяют настраивать определенные VLAN, интерфейсы Ethernet и т.д.

| Режим/ подрежим | Родительский режим | Назначение |
|---|---|---|
| EXEC | | Режим с самыми низкими привилегиями; используется для базового мониторинга системы. Как правило, не позволяет вносить изменения в систему.<br>Команда: **нет**<br>Изображение: **hostname>** |
| Привилегиров. EXEC | EXEC | Привилегированный режим; позволяет настраивать и вносить другие изменения в систему.<br>Команда: **да**<br>Изображение: **hostname#** |
| Config | Привилегиров. EXEC | Режим конфигурации<br>Команда: **configure terminal**<br>Изображение: **hostname(config)#** |
| VLAN Config | Config | Подрежим конфигурации и активации VLAN<br>Команда: **vlan vlan_id_list**<br>Изображение: **hostname(config-vlan)#** |
| VLAN Interface Config | Config | Подрежим конфигурации интерфейса VLAN<br>Команда: `interface vlan vlan_id_list`<br>Изображение: **hostname(config-if-vlan)#** |
| Interface Config | Config | Подрежим конфигурации Ethernet портов<br>Команда: **interface type**<br>Изображение: **hostname(config-if-vlan)#** |

| Режим/ подрежим | Родительский режим | Назначение |
|---|---|---|
| Line | Config | Подрежим конфигурации терминальных линий<br>Команда: **line { con \| vty } line_num**<br>Изображение: **hostname(config-line)#** |
| IPMC Profile Config | Config | Подрежим настройки профилей многоадресной рассылки<br>Команда: **interface type**<br>Изображение: **hostname(config-if-vlan)#** |
| SNMP Server Host Config | Config | Подрежим конфигурации хоста SNMP-сервера<br>Команда: **snmp-server host host_name**<br>Изображение: **hostname(config-snmps-host)#** |
| DHCP Pool Config | Config | Подрежим конфигурации пулов DHCP-клиентов<br>Команда: **ip dhcp pool pool_name**<br>Изображение: **hostname(config-dhcp-pool)#** |
| STP Aggregation Config | Config | Подрежим конфигурации агрегации STP<br>Команда: **spanning-tree aggregation**<br>Изображение: **hostname(config-stp-aggr)#** |

Пользователь может переключаться между этими режимами, используя определенные команды, в зависимости от уровня привилегий пользователя и текущего уровня привилегий сеанса.

Начальный режим определяется уровнем привилегий пользователя, вошедшего в систему. Если уровень привилегий равен 0 или 1, пользователь является непривилегированным и переходит в режим выполнения (Непривилегированный). Если уровень привилегий выше, сеанс начинается в привилегированном режиме выполнения.

Пользователь может повысить уровень привилегий в режиме [EXEC] до более высокого значения, если для этого уровня был настроен пароль включения. Это повышение осуществляется с помощью команды <enable level>, где уровень — это значение от 1 до 15. Обратная операция (понижение уровня привилегий) выполняется с помощью команды disable (отключить).

После перехода в привилегированный режим [EXEC] можно перейти в режим общей конфигурации, выполнив команду <configure terminal>. Для выхода из режима общей конфигурации введите <end> или <exit>, а затем нажмите [Enter] или сочетание клавиш Ctrl-Z.

Доступ к подрежиму конфигурации (например, к интерфейсам Ethernet) осуществляется через режим общей конфигурации или другой подрежим. Таким образом, можно перейти непосредственно из подрежима VLAN, например, в подрежим интерфейса Ethernet.

Таким образом, каждый режим и подрежим реализуют область действия команд. Внутри каждого режима доступно определенное подмножество команд. Чтобы перейти к

другим командам, обычно необходимо изменить режим/подрежим. Это необходимо, поскольку в разных режимах есть команды с одинаковыми префиксами. Например, существуют команды, которые начинаются с "ip" в режимах Привилегированный EXEC, общей конфигурации [terminal config] и VLAN Конфигурация интерфейса.

Из этого правила есть два исключения:

Находясь в подрежиме конфигурации, доступ к командам режима общей конфигурации возможен при условии отсутствия двусмысленности. Выполнение команды общей конфигурации приводит к выходу из подрежима.

Команды режима [EXEC] (как привилегированные, так и непривилегированные) доступны из режима общей конфигурации или одного из подрежимов с помощью команды <do>.

### 2.5.1 Использование команды <do> в подрежиме

Команда <do> берет произвольную командную строку из [EXEC] и выполняет ее. В следующем примере пользователь хочет изменить IP-адрес в интерфейсе VLAN 1 и использует префикс <do> для проверки текущего адреса, находясь в подрежиме.

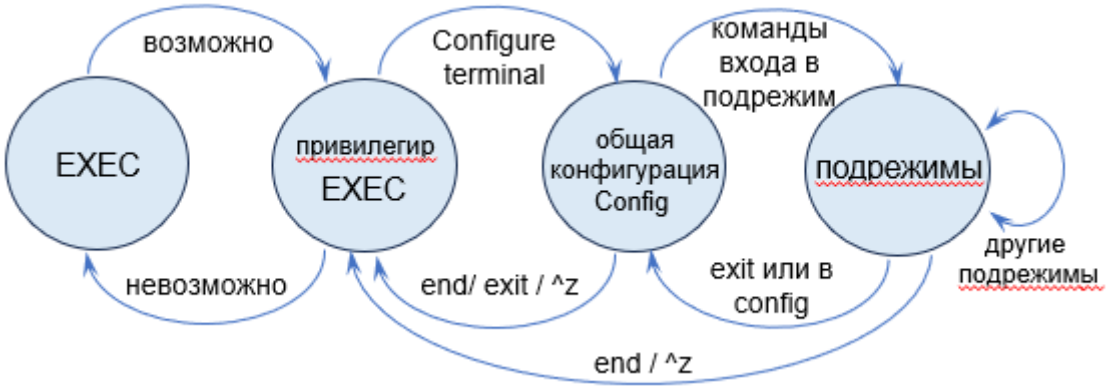
```
#
# configure terminal
(config)#
(config)# interface vlan 1
(config-if-vlan)# do show ip interface brief
Interface        Address              Method   Status
---------------- -------------------- -------- ------
VLAN 1           192.168.1.254/24     Manual   UP
(config-if-vlan)# end
#
#
```

Находясь в режиме [EXEC] нет необходимости использовать префикс <do>.

```
#
# show ip interface brief
Interface        Address              Method   Status
---------------- -------------------- -------- ------
VLAN 1           192.168.1.254/24     Manual   UP
#
#
```

### 2.5.2 Транзит режимов в CLI

На рисунке показаны возможные переходы между основными режимами и подрежимами, а также некоторые из команд.




## 2.6 Понятие уровня привилегий

Уровень привилегий — это число в диапазоне от 0 до 15 включительно, где 0 (ноль) является самой низкой привилегией. Ноль присваивается сеансу пользователя и используется для определения доступа к командам CLI. Доступны только команды с таким же или более низким уровнем привилегий.

У каждого пользователя на устройстве есть уровень привилегий по умолчанию, который копируется на уровень привилегий сеанса при входе в систему. Однако пользователь может изменить уровень привилегий сеанса, выполнив команды включения или отключения. Это можно использовать, например, следующим образом:

- Учетная запись пользователя настроена с уровнем привилегий 0;
- Всякий раз, когда пользователю требуется выполнить команды с более высокими привилегиями, пользователь меняет уровень приоритета сеанса, выполняет необходимые команды, а затем возвращается к уровню приоритета по умолчанию.

Доступ к уровням с более высоким приоритетом должен быть защищен паролем с помощью команд `<enable password>` или `<enable secret>` в режиме общей конфигурации. Основное различие между ними заключается в том, отображаются ли пароли в виде открытого текста или в зашифрованном виде в файлах *running-config* и, следовательно, в *startup-config*.

Ввод пароля также может осуществляться в зашифрованном виде или в виде открытого текста. Последний используется, когда оператор вводит новый пароль, поскольку оператор, как правило, не знает зашифрованную форму пароля.

Вводимый пароль отображается в зашифрованном виде. По умолчанию пользователь **admin** имеет 15-й уровень привилегий, что является максимально возможным.

### 2.6.1 Настройка уровня привилегий

В следующем примере настраивается пароль 15-го уровня с помощью *enable secret*, проверяется полученная конфигурация, а затем снова удаляется. Секрет может быть введен как открытым текстом, так и в зашифрованном виде. Цифра указывает, какой тип следует за ним в командной строке:

```
#
# configure terminal
(config)# enable secret ?
    0    Specifies an UNENCRYPTED password will follow
    5    Specifies an ENCRYPTED secret will follow
(config)# enable secret
```

В данном случае: Unencrypted (незашифрованный). Далее следует либо уровень, для которого настраивается пароль, либо, если уровень не указан, пароль для 15-го уровня:

```
    5    Specifies an ENCRYPTED secret will follow
(config)# enable secret 0 ?
    <word32>    Password
    level       Set exec level password
(config)# enable secret 0
```

Таким образом, следующие две команды семантически идентичны:

```
(config)# enable secret 0 my-secret
(config)# enable secret 0 level 15 my-secret
```

После ввода любой из этих команд можно проверить текущую конфигурацию, чтобы увидеть зашифрованную форму:

```
(config)#
(config)# do show running-config | include enable
enable secret 5 level 15 D29441BF847EA2DD5442EA9B1E40D4ED
(config)#
(config)#
```

Чтобы удалить пароль, используйте форму "no" (эти два параметра семантически эквивалентны для уровня 15):

```
(config)# no enable secret
(config)# no enable secret level 15
```

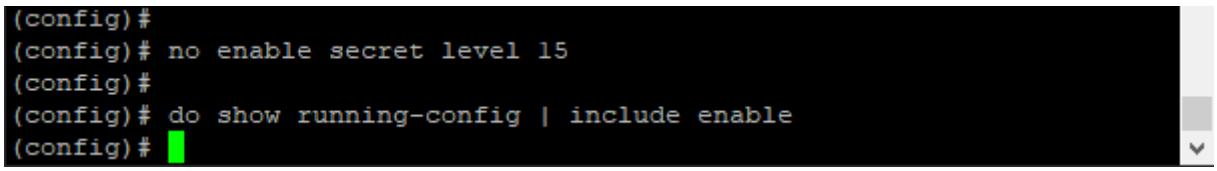
После ввода команды проверить текущую конфигурацию как при установке пароля:

```
(config)# do show running-config | include enable
```

Результат:

```
mydevice(config)#
```

Пароль удалён.




## 2.7 Параметры терминала

Каждый вход в систему создает сеанс, будь то через последовательный порт «консоль», telnet или ssh. Сеанс инициализируется параметрами, которые настраиваются в подрежиме линейной конфигурации, но большинство из них также можно изменить в режиме [EXEC], пока сеанс активен. Однако такие изменения не являются постоянными и теряются при завершении сеанса. В таблице перечислены доступные параметры и режимы, в которых можно настроить каждый из них.

| Параметр | Режим | Описание |
|---|---|---|
| Editing | Exec, Line | Включение/отключение прокрутки командной строки |
| exec-banner | Exec | Включение/выключение отображения баннера Exec (настраивается с помощью ‘banner exec ...’) |
| exec-timeout | Exec, Line | Таймер бездействия; автоматический выход из системы после определенного периода бездействия. Нулевое значение отключает автоматический выход из системы |
| history | Exec, Line | Длина буфера истории команд |
| Length | Exec, Line | Конечная длина в строках, используемая для разбивки на страницы. Ноль отключает разбивку на страницы. |
| Location | Line | Строка текста, описывающая местоположение терминала (например, “Server room”) |
| motd-banner | Line | Включение/выключение отображения баннера с сообщением дня (настраивается с помощью ‘banner motd ...’) |
| privilege | Line | Распределить приоритет по умолчанию |
| width | Exec, Line | Ширина терминала в символах, используемая для разбивки на страницы. |

В таблице перечислены доступные параметры и режимы, каждый из которых может быть настроен.

Система поддерживает один сеанс последовательной консоли и до 16 сетевых сеансов. Сеанс консоли называется “console 0”, тогда как каждый сетевой сеанс называется “vty X” , где vti - это сокращение от Virtual TTY, а X - значение от 0 до 15. Конфигурация отображается в нижней части running-config и выглядит следующим образом:

```
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
```

Для каждого vty можно указать разные настройки, но, как правило, это не рекомендуется, поскольку невозможно связать входящее ssh-соединение или telnet-соединение с конкретным vty.

В этом примере показано, как изменить некоторые значения для текущего сеанса и для всех будущих сеансов консоли. Сначала проверьте текущие настройки для этого сеанса `<show terminal>`:

```
#
# show terminal
Line is con 0.
    * You are at this line now.
    Alive from Console.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 24.
             history size is 32.
             exec-timeout is 10 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 7 min 36 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

#
#
```

Затем установите значение *terminal length* равным нулю, чтобы отключить разбиение на страницы, и значение *exec-timeout* равным нулю, чтобы отключить автоматический выход из системы:

```
#
# terminal length 0
# terminal exec-timeout 0
# show terminal
Line is con 0.
    * You are at this line now.
    Alive from Console.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 0.
             history size is 32.
             exec-timeout is 0 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 13 min 40 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

#
```

Далее мы делаем то же самое, но для всех будущих консольных сессий. Обратите внимание, что команды не имеют префикса "terminal" ("длина терминала" или "length").:

```
#
# configure terminal
(config)# line console 0
(config-line)# exec-timeout 0
(config-line)# length 0
(config-line)# end
#
#
```

Наконец, сохраните конфигурацию в файл **startup-config**, чтобы сделать ее постоянной:

```
#
# copy running-config startup-config
Building configuration...
% Saving 1204 bytes to flash:startup-config
#
#
```

# III. НАСТРОЙКА СИСТЕМЫ

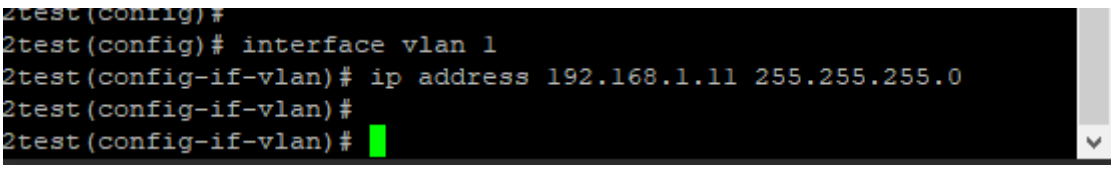
Изменения в конфигурацию системы могут быть внесены только в режиме общей конфигурации и её подрежимах, за исключением случаев работы с файлами конфигурации или перезагрузки настроек по умолчанию. Это делается в привилегированном режиме [EXEC]. Последовательность действий описана ниже.

- Повысьте уровень привилегий до 15.
- Войдите в режим общей настройки <configure terminal>.
- Введите соответствующие команды настройки. При необходимости перейдите в подрежимы и введите соответствующие команды там.
- Выйдите из режима общей настройки.
- Проверьте конфигурацию.
- Сохраните конфигурацию во Flash: <copy running-config startup-config>.

## 3.1 Шаблон конфигурации

В этом примере имя хоста и IP-адрес VLAN 1 настроены, проверены и сохранены. Войдите в режим общей конфигурации <configure terminal>. Низначте хосту имя: <hostname 2test>.


Имя хоста назначено: «2test». IP-адрес коммутатора задается с помощью интерфейса подрежима VLAN команда на вход в подрежим настройки VLAN: <interface vlan 1>.



Выйдите из режима общей конфигурации <end> – вернитесь в режим [EXEC]. Проверьте и верифицируйте текущую конфигурацию <show running-config>.

```
2test(config)#
2test(config)# end
2test#
2test# show running-config
Building configuration...
hostname 2test
username admin privilege 15 password unencrypted admin
username user1 privilege 0 password unencrypted Nokia@2020
!
vlan 1
!
!
!
!
spanning-tree mst name Default revision 0
!
!
interface GigabitEthernet 1/1
 no spanning-tree
!
interface GigabitEthernet 1/2
 no spanning-tree
```

Дополнительная проверка: Отображение IP-интерфейсов и назначенного IP-адреса и статуса: <show ip interface brief>.

```
2test#
2test# show ip interface brief
Interface        Address              Method   Status
---------------- -------------------- -------- ------
VLAN 1           192.168.1.11/24      Manual   UP
2test#
2test#
```

Попробуйте проверить имя хоста <show hostname>:

```
2test#
2test# show hostname
            ^
% Invalid word detected at '^' marker.

2test#
```

Отказ, появилась строка: % Invalid word detected at '^' marker.

Символ '^' говорит о том, что такой команды не существует, но можно извлечь строку с именем хоста из файла running-config с помощью фильтра: <show running-config | include hostname>

```
2test#
2test# show running-config | include hostname
hostname 2test
2test#
```

После ввода команды под ней появилось имя хоста «hostname 2test». Сохраните конфигурацию на Flash.

```
2test#
2test# show running-config | include hostname
hostname 2test
2test# copy running-config startup-config
Building configuration...
% Saving 1636 bytes to flash:startup-config
2test#
```

## 3.2 Сброс или удаление конфигурации с помощью формы «no».

Можно удалить определенные элементы конфигурации или вернуть их к значениям по умолчанию. Почти каждая команда настройки имеет соответствующую форму «no». Форма "no" синтаксически аналогична (но не обязательно идентична) команде настройки , но либо сбрасывает параметры до значений по умолчанию для настраиваемого элемента, к которому обращается пользователь, либо полностью удаляет элемент. Во многих случаях "no" может быть прочитано как no(t), отличное от настроек по умолчанию.

Попробуйте применить "no" для удаления IP-адреса и затем проверьте конфигурацию см пример ниже.

Операции "no" можно рассматривать как сброс к значению по умолчанию, при этом IP -адрес по умолчанию не используется.

```
2test#
2test# configure terminal
2test(config)# interface vlan 1
2test(config-if-vlan)# no ip address
2test(config-if-vlan)# end
2test# show ip interface brief
Interface        Address              Method   Status
---------------- -------------------- -------- ------
2test#
2test#
```

Обычно пользоваться формой "no" очень удобно, но в некоторых случаях может привести к неожиданным результатам. Например, OAM MEP может настроить проверку непрерывности с помощью "mep <номер> cc <приоритет> ..." и сбросить ее с помощью ‘no mep <номер> cc’. Однако, поскольку MEP удаляются с помощью команды "no mep <num>", можно непреднамеренно удалить существующий MEP, введя "no mep 10 ccc" – дополнительная буква "c" означает, что последнее слово не распознается как "cc", что приводит к совпадению MEP команда удаления вместо желаемой команды reset-CC.

# IV. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

В этой главе описано управление локальными пользователями на устройстве. Управление пользователями RADIUS и TACACS+ выходит за рамки данного документа. В системе можно создать несколько учетных записей пользователей. Каждая учетная запись пользователя имеет набор настраиваемых атрибутов:

- Имя пользователя
- Пароль
- Уровень привилегий

Все атрибуты настраиваются с помощью одной и той же команды - `username`.

Имя пользователя `<username>` привилегия `<priv>` зашифрованный пароль `<encry_password_1>`
[ `<encry_password_2>` ]

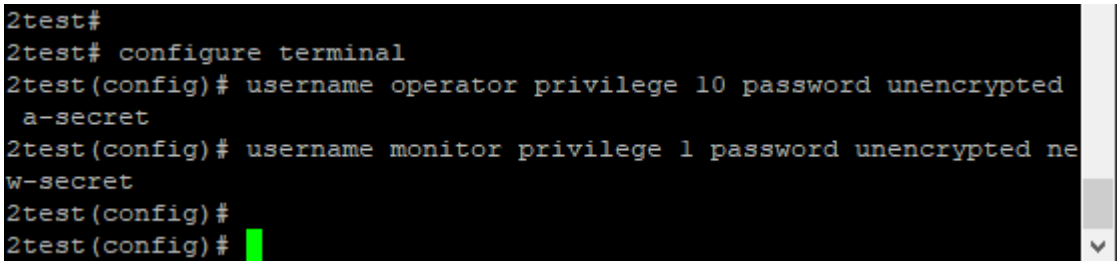
no username `<username>`
`no username` удаляет данную учетную запись пользователя.

## 4.1 Добавление, изменение и удаление пользователя

В следующем примере добавляются две учетные записи пользователей с разными уровнями привилегий, проверяется конфигурация и снова удаляется одна учетная запись, используя `<no username>`.

Отобразите текущий набор учетных записей локальных пользователей:
`<show running-config | include username>`

Добавьте две учетные записи, "operator" и "monitor". Пароли предоставляются в незашифрованном виде. Команда: `username [имя уч записи] privilege 10 password unencrypted [пароль]`



Проверьте правильность введенных данных. Обратите внимание, что пароли отображаются в незашифрованном виде:

```
2test(config)#
2test(config)# do show running-config | include username
username admin privilege 15 password unencrypted admin
username monitor privilege 1 password unencrypted new-secret
username operator privilege 10 password unencrypted a-secret
2test(config)#
2test(config)#
```

Удалите пользователя "оператор" и убедитесь, что он удален из конфигурации:

```
2test(config)#
2test(config)# no username operator
now_user:admin
2test(config)# do show running-config | include username
username admin privilege 15 password unencrypted admin
username monitor privilege 1 password unencrypted new-secret
2test(config)#
2test(config)#
```

## 4.2 Настройка уровня привилегий

Уровень привилегий пользователя. Допустимый диапазон - от 0 до 15. Если значение уровня привилегий равно 15, он может получить доступ ко всем группам, то есть ему предоставляется полный контроль над устройством. Но другие значения должны относиться к уровню привилегий каждой группы. Привилегии пользователя должны быть такими же или превышать уровень привилегий группы, чтобы иметь доступ к этой группе. По умолчанию для большинства групп уровень привилегий 5 имеет доступ только для чтения, а уровень привилегий 10 - для чтения и записи. А для обслуживания системы (загрузка программного обеспечения, заводские настройки по умолчанию и т.д.) требуется уровень привилегий пользователя 15. Как правило, уровень привилегий 15 может использоваться для учетной записи администратора, уровень привилегий 10 - для учетной записи обычного пользователя и уровень привилегий 5 - для учетной записи гостя. Пример: просмотрите уровень привилегий для агрегации.

```
2test#
2test# show web privilege group Aggregation level
Group Name                      Privilege Level
                                CRO CRW SRO SRW
------------------------------- --- --- --- ---
Aggregation                       5  10   5  10
2test#
2test#
```

Пример интерфейса командной строки: установите для конфигурации агрегации привилегию "только для чтения" на 3, а для записи - на 5; Установите для статуса агрегации привилегию "только для чтения" на 3, а для записи - на 5.

```
2test#
2test# configure terminal
2test(config)# web privilege group Aggregation level configRoPriv 3
2test(config)# web privilege group Aggregation level configRwPriv 5
2test(config)# web privilege group Aggregation level statusRoPriv 3
2test(config)# web privilege group Aggregation level statusRwPriv 5
2test(config)#
2test(config)#
```

## 4.3 Просмотр пользователей

Команда для просмотра всей информации о пользователях:
<show users>

```
2test#
2test# show users
Line is con 0.
    * You are at this line now.
    Connection is from Console.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 0 hour 3 min 5 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

Line is vty 0.
    Connection is from 192.168.1.200:51617 by Telnet.
    User name is monitor.
    Privilege is 1.
    Elapsed time is 0 day 0 hour 0 min 36 sec.
    Idle time is 0 day 0 hour 0 min 24 sec.

2test#
```

Команда для просмотра собственной информации пользователей.
<show users myself>

```
2test#
2test# show users myself
Line is con 0.
    * You are at this line now.
    Connection is from Console.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 0 hour 10 min 2 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

2test#
2test#
```

```
2test>
2test> show users myself
Line is vty 0.
    * You are at this line now.
    Connection is from 192.168.1.200:52649 by Telnet.
    User name is monitor.
    Privilege is 1.
    Elapsed time is 0 day 0 hour 0 min 10 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

2test>
2test>
```

# V. ИСПОЛЬЗОВАНИЕ КОМАНД «SHOW»

Семейство команд <show> является краеугольным камнем системного мониторинга на основе CLI. Большинство функций реализуют одну или несколько команд <show>, которые отображают соответствующее сочетание состояния и конфигурации.

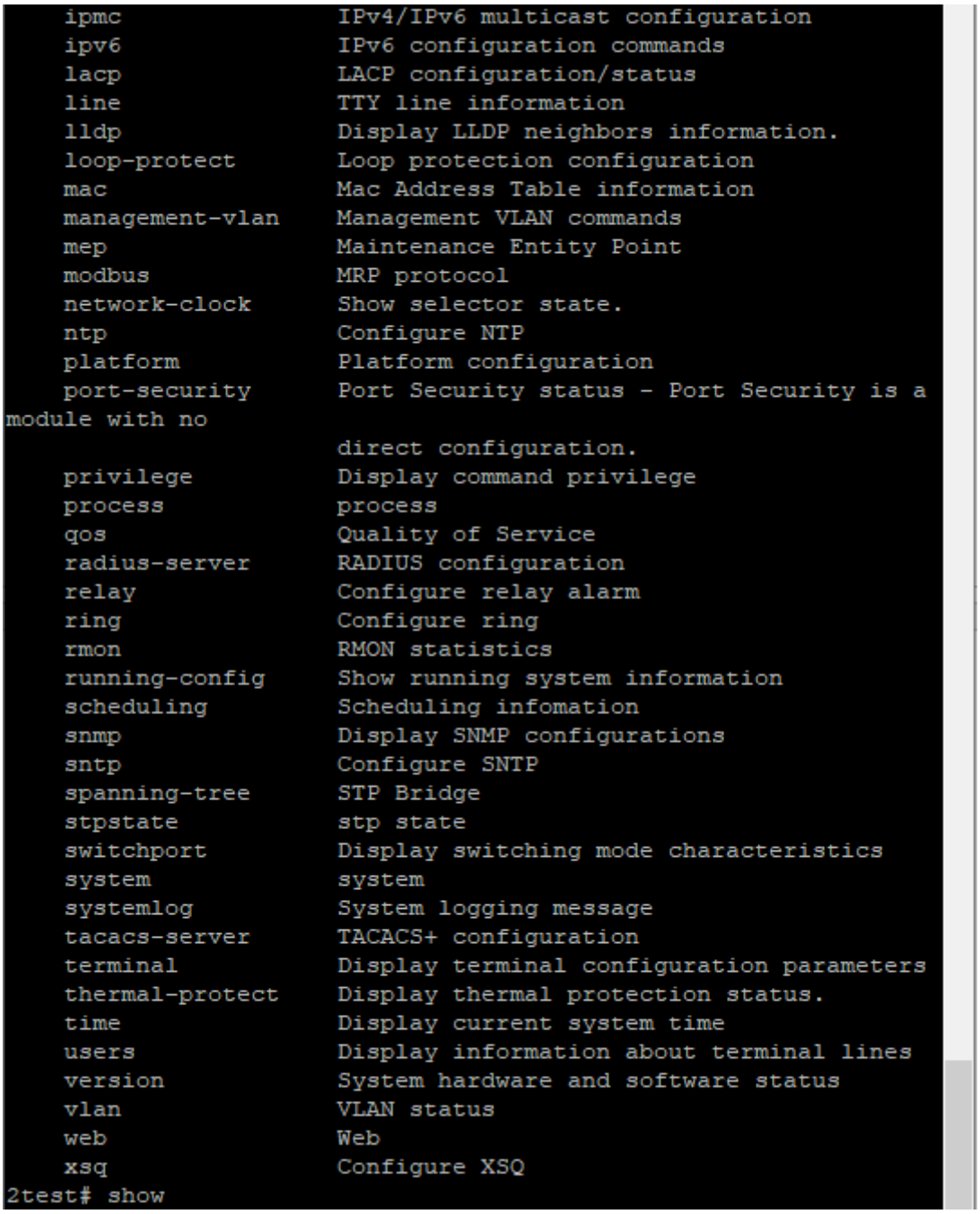
**ВНИМАНИЕ!** Точный набор доступных команд, параметров и формата вывода зависит от конфигурации системы и версии программного обеспечения, если некоторые из приведенных ниже команд и примеров не работают на вашем устройстве, проверьте конфигурацию системы и версию ПО.

Команды <show> доступны только в двух режимах [EXEC] и зависят от уровня привилегий сеанса. Таким образом, для отображения максимально возможного набора команд <show> требуется, чтобы сеанс был 15-го уровня.

## 5.1 Список всех команд <show>

В следующем примере уровень привилегий сеанса повышается до 15. В этом примере был указан секретный режим включения, поэтому для продолжения работы требуется ввести пароль. Затем пользователь вводит команду <show> и использует функцию контекстно-зависимой справки, чтобы перечислить возможные команды <show>, в данном случае для системы Carrier Ethernet.

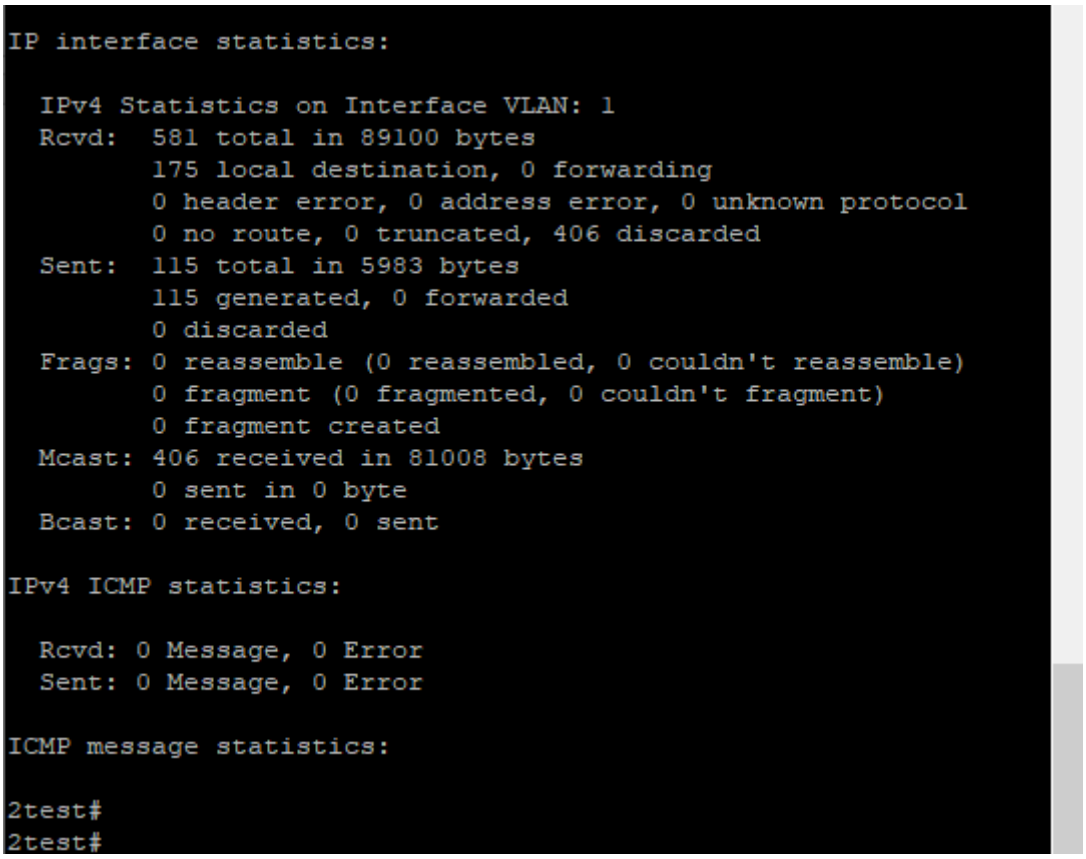
```
Username: admin
Password:
2test# show ?
    aaa                 Authentication, Authorization and Accounti
ng methods
    access              Access management
    access-list         Access list
    aggregation         Aggregation port configuration
    alarmlog            System logging message
    clock               Configure time-of-day clock
    ddmi                DDMI configuration
    dot1x               IEEE Standard for port-based Network Acces
s Control
    erps                Ethernet Ring Protection Switching
    evc                 Ethernet Virtual Connections
    history             Display the session command history
    interface           Interface status and configuration
    ip                  Interface Internet Protocol configuration
commands
    ipmc                IPv4/IPv6 multicast configuration
```


ipmc IPv4/IPv6 multicast configuration
ipv6 IPv6 configuration commands
lacp LACP configuration/status
line TTY line information
lldp Display LLDP neighbors information.
loop-protect Loop protection configuration
mac Mac Address Table information
management-vlan Management VLAN commands
mep Maintenance Entity Point
modbus MRP protocol
network-clock Show selector state.
ntp Configure NTP
platform Platform configuration
port-security Port Security status - Port Security is a module with no
direct configuration.
privilege Display command privilege
process process
qos Quality of Service
radius-server RADIUS configuration
relay Configure relay alarm
ring Configure ring
rmon RMON statistics
running-config Show running system information
scheduling Scheduling infomation
snmp Display SNMP configurations
sntp Configure SNTP
spanning-tree STP Bridge
stpstate stp state
switchport Display switching mode characteristics
system system
systemlog System logging message
tacacs-server TACACS+ configuration
terminal Display terminal configuration parameters
thermal-protect Display thermal protection status.
time Display current system time
users Display information about terminal lines
version System hardware and software status
vlan VLAN status
web Web
xsq Configure XSQ
2test# show

## 5.2 Использование контекстно-зависимой справки для поиска

Функция контекстно-зависимой справки для отображения синтаксиса также полезна для определения точной команды для выполнения. В следующем примере пользователь находит нужную команду <show ip statistics system> с помощью поиска:

```
2test#
2test# show ip ?
    arp
    dhcp            Dynamic Host Configuration Protocol
    domain          Default domain name
    http            Hypertext Transfer Protocol
    igmp            Internet Group Management Protocol
    interface       IP interface status and configuration
    name-server     Domain Name System
    route           Display the current IP routing table
    ssh             Secure Shell
    statistics      Traffic statistics
2test# show ip
% Incomplete command.

2test# show ip statistics ?
    |             Output modifiers
    icmp          IPv4 ICMP traffic
    icmp-msg      IPv4 ICMP traffic for designated message type
    interface     Select an interface to configure
    system        IPv4 system traffic
    <cr>
2test# show ip statistics

IPv4 statistics:

  Rcvd:  845 total in 248336 bytes
         307 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 406 discarded
  Sent:  379 total in 165219 bytes
         247 generated, 0 forwarded
         0 no route, 0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 406 received in 81008 bytes
         0 sent in 0 byte
  Bcast: 0 received, 0 sent

IP interface statistics:

  IPv4 Statistics on Interface VLAN: 1
```


IP interface statistics:
IPv4 Statistics on Interface VLAN: 1
Rcvd: 581 total in 89100 bytes
175 local destination, 0 forwarding
0 header error, 0 address error, 0 unknown protocol
0 no route, 0 truncated, 406 discarded
Sent: 115 total in 5983 bytes
115 generated, 0 forwarded
0 discarded
Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
0 fragment (0 fragmented, 0 couldn't fragment)
0 fragment created
Mcast: 406 received in 81008 bytes
0 sent in 0 byte
Bcast: 0 received, 0 sent
IPv4 ICMP statistics:
Rcvd: 0 Message, 0 Error
Sent: 0 Message, 0 Error
ICMP message statistics:
2test#
2test#

Повторное нажатие клавиши "?" отображает синтаксис:

```
2test#
2test# show ip statistics ?
    |            Output modifiers
    icmp         IPv4 ICMP traffic
    icmp-msg     IPv4 ICMP traffic for designated message type
    interface    Select an interface to configure
    system       IPv4 system traffic
    <cr>
2test# show ip statistics

IPv4 statistics:

  Rcvd:  870 total in 262881 bytes
         319 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 407 discarded
  Sent:  403 total in 179695 bytes
         259 generated, 0 forwarded
         0 no route, 0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 407 received in 81077 bytes
         0 sent in 0 byte
  Bcast: 0 received, 0 sent

IP interface statistics:

  IPv4 Statistics on Interface VLAN: 1
  Rcvd:  582 total in 89169 bytes
         175 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 407 discarded
  Sent:  115 total in 5983 bytes
         115 generated, 0 forwarded
         0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 407 received in 81077 bytes
         0 sent in 0 byte
  Bcast: 0 received, 0 sent

IPv4 ICMP statistics:

  Rcvd: 0 Message, 0 Error
  Sent: 0 Message, 0 Error

ICMP message statistics:

2test#
2test#
```

## 5.3 Отображение текущей конфигурации

Виртуальный файл running-config состоит из списка команд, которые все вместе, приводят к текущей конфигурации системы.

Этот список команд обычно не на 100% идентичен списку команд, которые пользователь вводит для настройки коммутатора. Это связано с тем, что running-config - это текстовое представление конфигурации системы, которое хранится в двоичном виде в оперативной памяти коммутатора.

Поскольку эффективная конфигурация устройства огромна, в running-config в большинстве случаев отображается только разница между настройками по умолчанию и текущими настройками. Это значительно сокращает объем выходных данных и значительно улучшает читаемость конфигурации, но требует, чтобы пользователь знал, каковы настройки по умолчанию.

С помощью команды <show running-config all-defaults> можно просмотреть значения, которые используются по умолчанию.

В следующем примере, если настройки скорости и двусторонней связи интерфейса Ethernet установлены на значения по умолчанию (автоматическое согласование), то выводиться ничего не будет. Если пользователь затем изменит скорость на фиксированную 1 Гбит/с, то это значение теперь не является значением по умолчанию и будет выводиться. Дуплексный режим также выводится, поскольку он принудительно становится «полным», когда скорость зафиксирована на уровне 1 Гбит/с.

Нам нужно отобразить текущую конфигурацию интерфейса. Все настройки указаны по умолчанию:

```
2test# show running-config interface GigabitEthernet 1/4
Building configuration...
interface GigabitEthernet 1/4
 no spanning-tree
!
end
2test#
```

Теперь установите скорость на 1 Гбит/с и снова отобразите конфигурацию:

```
2test# con terminal
2test(config)# interface GigabitEthernet 1/4
2test(config-if)# speed 1000
2test(config-if)# end
2test#
2test# show running-config interface GigabitEthernet 1/4
Building configuration...
interface GigabitEthernet 1/4
 no spanning-tree
 speed 1000
 duplex full
!
end
2test#
```

Запросите через CLI все настройки по умолчанию для этого интерфейса:
<show running-config interface GigabitEthernet 1/4 all-defaults>

```
2test#
2test# show running-config interface GigabitEthernet 1/4 all-defa
ults
Building configuration...
interface GigabitEthernet 1/4
 loop-protect
 no loop-protect action
 loop-protect tx-mode
 switchport mode access
 switchport access vlan 1
 switchport forbidden vlan remove 1-4095
 no ip igmp snooping filter
 no ip igmp snooping max-groups
 no ip igmp snooping mrouter
 no ip igmp snooping immediate-leave
 no ipv6 mld snooping filter
 no ipv6 mld snooping max-groups
 no ipv6 mld snooping mrouter
 no ipv6 mld snooping immediate-leave
 ip dhcp snooping trust
 lldp receive
 lldp transmit
 lldp tlv-select management-address
 lldp tlv-select port-description
 lldp tlv-select system-capabilities
 lldp tlv-select system-name
 lldp tlv-select system-description
 no lldp cdp-aware
 lldp med transmit-tlv capabilities network-policy location
 no lldp med media-vlan policy-list
 lldp med type connectivity
 qos cos 0
 qos pcp 0
 qos dpl 0
 qos dei 0
 no qos trust tag
 qos map tag-cos pcp 0 dei 0 cos 1 dpl 0
 qos map tag-cos pcp 0 dei 1 cos 1 dpl 1
 qos map tag-cos pcp 1 dei 0 cos 0 dpl 0
 qos map tag-cos pcp 1 dei 1 cos 0 dpl 1
 qos map tag-cos pcp 2 dei 0 cos 2 dpl 0
-- more --, next page: Space, continue: g, quit: ^C
```

Вывод информации <show running-config> может быть ограничен определенным интерфейсом. Существует несколько таких фильтров, описанных ниже.

<show running-config>
Здесь отображается вся текущая конфигурация системы.

show running-config feature [feature_name]
Выводите только команды, относящиеся к конкретной функции. Список функций зависит от конфигурации системы и версии программного обеспечения. Например:

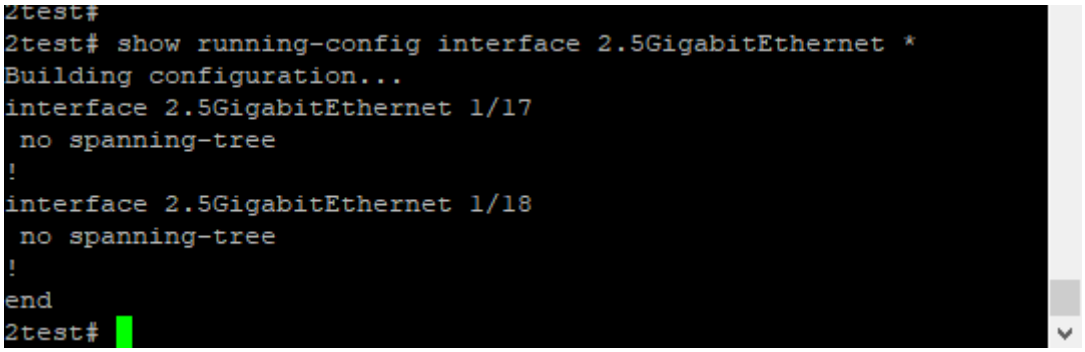
```
2test#
2test#
2test# show running-config feature ?
    <cword>    Valid words are 'access' 'access-list' 'aggregatio
n' 'auth'
               'clock' 'ddmi' 'dhcp' 'dhcp-snooping' 'dhcp6_clien
t_interface'
               'dhcp_server' 'dns' 'dot1x' 'erps' 'evc' 'http' 'i
cli'
               'ip-igmp-snooping' 'ip-igmp-snooping-port'
               'ip-igmp-snooping-vlan' 'ipmc-profile' 'ipmc-profi
le-range'
               'ipv4' 'ipv6' 'ipv6-mld-snooping' 'ipv6-mld-snoopi
ng-port'
               'ipv6-mld-snooping-vlan' 'lacp' 'lldp' 'logging' '
loop-protect'
               'mac' 'mep' 'modbus' 'monitor' 'mstp' 'netmanager'
               'network-clock' 'ntp' 'port' 'port-security' 'qos'
 'relay'
               'rmon' 'snmp' 'sntp' 'ssh' 'swring' 'sysutil' 'the
rmal-protect'
               'time_range' 'user' 'vlan' 'web-privilege-group-le
vel'
2test#
2test# show running-config feature vlan
Building configuration...
!
vlan 1
!
!
!
!
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
!
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
-- more --, next page: Space, continue: g, quit: ^C
```

Здесь большая часть выходных данных опущена для краткости….

В выходных данных сохраняется структура **running-config.** Перечислены подрежимы, такие как интерфейсы VLAN и Ethernet, но они могут быть пустыми, если запрашиваемая функция не имеет отношения к конкретному подрежиму.

`show running-config interface` ( <port_type> [ <list> ] ) [ all-defaults ]

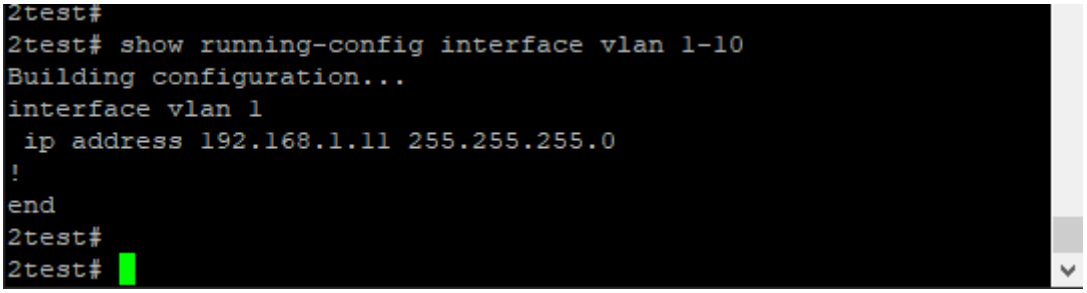
Используя этот фильтр, пользователь может просмотреть определенный список интерфейсов Ethernet. Он может содержать подстановочные знаки, например:




В нашем примере конфигурации имеется только одна VLAN.

Также можно отфильтровать список интерфейсов VLAN, например:

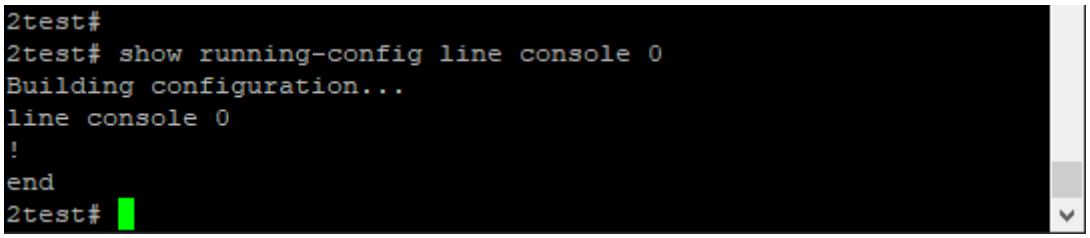
`show running-config interface vlan` <list> [ all-defaults ]




В этом примере в системе имеется только один интерфейс VLAN.

`show running-config line` { console | vty } <list> [ all-defaults ]

Эту команду можно использовать для консоли или списка виртуальных терминальных устройств (vty). В текущем примере используется одно консольное устройство, 0. Например:



# VI. РАБОТА С ФАЙЛАМИ КОНФИГУРАЦИИ

Существует четыре конфигурационных файла:

- **running-config** – виртуальный файл, содержащий текущую конфигурацию коммутатора;
- **startup-config** – содержит конфигурацию для запуска коммутатора. При изменении конфигурации ее необходимо скопировать в startup-config, чтобы эта конфигурация загрузилась при запуске ОС;
- **default-config** – файл доступный только для чтения, используемый при восстановлении настроек по умолчанию, этот файл также используется, если отсутствует startup-config, он содержит настройки коммутатора по умолчанию;
- **пользовательские** файлы конфигурации, созданные пользователем (до 31); они обычно используются для резервного копирования или вариантов конфигурации при запуске.

Все они, за исключением **running-config**, хранятся в файловой системе **flash**. С ними доступны следующие операции:
**copy** `source destination,` где источником и пунктом назначения может быть один из:
running-config
startup-config (or flash:startup-config)
flash: filename
dir

`#more flash: filename`
Выводит содержимое файла на терминал.

`#delete flash: filename`
Удаляет конкретный файл.

## 6.1 Возврат к конфигурации по умолчанию

Восстановить конфигурацию системы по умолчанию можно двумя способами:

- Удаление startup-config и перезагрузка;
- Указание программному обеспечению отменить текущую конфигурацию и вернуться к настройкам по умолчанию без перезагрузки.

Удаление startup-config не приводит к изменению **running-config** до тех пор, пока система не будет перезагружена, после чего будут загружены настройки по умолчанию.

И наоборот, отмена текущей конфигурации действительно влияет на **running-config**, но не затрагивает **startup-config**. Если вы хотите сохранить конфигурацию, вам следует сохранить **startup-config** в **running-config**.

Перезагрузка и сброс настроек по умолчанию выполняются с помощью команды:

```
#reload cold
#reload defaults [ keep-ip ]
```

Версия "холодной перезагрузки" перезагружает систему. Если система работает в режиме стекирования, можно также перезагрузить определенный коммутатор, указав его идентификатор.

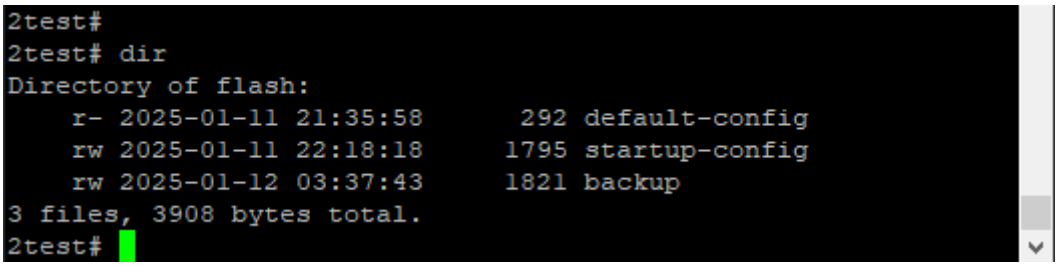
Второй метод загружает настройки по умолчанию. Если задано ключевое слово **keep-ip**, система пытается сохранить наиболее важные части настройки IP-адреса VLAN 1, чтобы поддерживать подключение к управлению (настройка IP-адреса и активный маршрут по умолчанию).

Однако нет никакой гарантии, что вышеуказанных действий будет достаточно для возврата к конфигурации по умолчанию: это зависит от фактических свойств сети и общей конфигурации IP системы. В некоторых случаях может оказаться предпочтительным явно сконфигурировать систему, используя команды "no", или подготовить подходящую конфигурацию и загрузить ее в **startup-config** системы и перезагрузиться.

## 6.2 Использование файлов конфигурации

В следующем примере предполагается, что файловая система содержит дополнительный файл под названием backup, ранее созданный с помощью команды copy.

Запросите список файлов во flash:



Отобразить содержимое файла "backup" (выходные данные сокращены): `2test# more flash:backup`

```
2test#
2test# more flash:backup
hostname 2test
username admin privilege 15 password unencrypted admin
username user1 privilege 0 password unencrypted Nokia@2020
username monitor privilege 1 password unencrypted Nokia@2020
!
vlan 1
!
!
!
!
spanning-tree mst name Default revision 0
!
web privilege group Aggregation level configRoPriv 3 configRwPr
iv 5 statusRoPriv 3 statusRwPriv 5
!
interface GigabitEthernet 1/1
 no spanning-tree
!
interface GigabitEthernet 1/2
 no spanning-tree
!
interface GigabitEthernet 1/3
```

Используйте файл “backup” для следующей загрузки, перезаписав startup-config: `2test# copy flash:backup startup-config`
Затем убедитесь, что размеры файлов совпадают: `dir`

```
2test#
2test# copy flash:backup startup-config
% Saving 1821 bytes to flash:startup-config
2test#
2test# dir
Directory of flash:
    r- 2025-01-11 21:35:58      292 default-config
    rw 2025-01-12 03:48:42     1821 startup-config
    rw 2025-01-12 03:37:43     1821 backup
3 files, 3934 bytes total.
2test#
```

Теперь удалите startup-config: `2test# delete flash:startup-config`

```
2test#
2test# delete flash:startup-config
2test#
2test# dir
Directory of flash:
    r- 2025-01-11 21:35:58      292 default-config
    rw 2025-01-12 03:37:43     1821 backup
2 files, 2113 bytes total.
2test#
```

Используйте текущую конфигурацию для её записи во флэш-память:
`2test# copy running-config startup-config`
И убедитесь что появился файл **startup-config**: `dir`

```
2test#
2test# copy running-config startup-config
Building configuration...
% Saving 1821 bytes to flash:startup-config
2test#
2test# dir
Directory of flash:
    r- 2025-01-11 21:35:58      292 default-config
    rw 2025-01-12 04:04:50     1821 startup-config
    rw 2025-01-12 03:37:43     1821 backup
3 files, 3934 bytes total.
2test#
```

## 6.3 Использование команд перезагрузки

Перезагрузите настройки по умолчанию, но постарайтесь сохранить конфигурацию VLAN 1. Сначала просмотрите текущий IP-адрес, затем верните настройки по умолчанию, сохранив текущий IP <`reload defaults keep-ip`>.

```
2test#
2test# show ip interface brief
Interface        Address              Method   Status
---------------- -------------------- -------- ------
VLAN 1           192.168.1.11/24      Manual   UP
2test#
2test# reload defaults keep-ip
% Reloading defaults, attempting to keep VLAN 1 IP address. Please s
tand by.
#
# show ip interface brief
Interface        Address              Method   Status
---------------- -------------------- -------- ------
VLAN 1           192.168.1.11/24      Manual   UP
#
# dir
Directory of flash:
    r- 2025-01-14 20:33:47      292 default-config
    rw 2025-01-12 04:04:50     1821 startup-config
    rw 2025-01-12 03:37:43     1821 backup
3 files, 3934 bytes total.
#
```

Обратите внимание, что содержание флэш-памяти не изменилось.

Перезагрузите настройки по умолчанию еще раз, но не пытайтесь сохранить настройки VLAN 1, затем убедитесь, что настройки IP-адреса по умолчанию восстановлены:

```
#
# reload defaults
% Reloading defaults. Please stand by.
#
# show ip interface brief
Interface        Address              Method   Status
---------------- -------------------- -------- ------
VLAN 1           192.168.1.254/24     Manual   UP
#
```

Если вы хотите сохранить настройки по умолчанию, то запишите их в файл **“startup-config”** через команду <copy running-config startup-config>.

## 6.4 Работа с образами программного обеспечения

Операционная система может сохранять до двух образов программного обеспечения во флэш-памяти. Образ, выбранный для загрузки, называется активным образом, а другой - альтернативным образом.

Можно поменять местами активный и альтернативный образы, а также перейти на новый образ.

Для обновления встроенного ПО выполните следующие действия:

- Загрузите новую прошивку по протоколу HTTPS и проверьте ее пригодность для работы в системе;
- Перезапишите текущий альтернативный образ загрузив новое ПО;
- Поменяйте местами активный и альтернативный образы и перезагрузите коммутатор.

```
2Test#
2Test# firmware swap
... Erase from 0x41ff0000-0x41ffffff: .
... Program from 0x87feeffc-0x87ffeffc to 0x41ff0000: .
... Program from 0x87fef006-0x87fef008 to 0x41ff000a: .
Alternate image activated, now rebooting.
```

В результате старая активная сборка становится альтернативной, а вновь загруженный образ - активным.

Для работы с образами ПО применяются команды: <firmware swap> и <show version>

# VII. ФУНКЦИОНАЛ СИСТЕМЫ

## 7.1 Информация о системе

Команда *show version* выводит список различных сведений о системе, включая образы во флэш-памяти:

```
2Test#
2Test# show version

MEMORY           : Total=104046 KBytes, Free=99158 KBytes, Max=988
83 KBytes
FLASH            : 0x40000000-0x41ffffff, 512 x 0x10000 blocks
MAC Address      : dc-31-30-04-a3-20
Device Number    : YBD0802000538
Hardware Version : V1.0.1
Previous Restart : Cool

System Contact   :
System Hostname  : 2Test
System Location  :
Timezone Offset  : 0
System Time      : 2025-03-10T09:41:58+00:00
System Uptime    : 00:06:36

Active Image
------------
Image            :  (primary)
Version          : PT536300_V1.6
Date             : Feb  5 2025 20:09:10 by alexmak

Alternate Image
---------------
Image            :  (backup)
Version          : PT536300_V1.5
Date             : Feb  5 2025 13:44:08 by alexmak

Bootloader
----------
Image            : RedBoot (bootloader)
Version          : version 1.1
Date             : 20:13:12, Feb  9 2023

------------------
SID : 1
------------------
Port Count       : 20
Product          : Managed Switch
Software Version : PT536300_V1.6
Build Date       : Feb  5 2025 20:09:10 by alexmak

SoftProductID:298
Port count:20

2Test#
```

Активный образ – primary.
Альтернативный образ – backup.

## 7.2 IP

- Команда <`show interface vlan` [<vlan_list>]> вызывает информацию об IP-интерфейсе.
- Команда <`show ip route`> вызывает информацию об IP-маршруте.
- Команда <`show ip arp`> отображает записи IP-адресов в кэше

## 7.3 Синхронизация часов NTP

Протокол сетевого времени (NTP) синхронизирует время суток между набором распределенных серверов времени и клиентов. Это помогает пользователю сопоставлять события из системных журналов и другие события, зависящие от времени, с нескольких сетевых устройств. NTP использует пользовательский Протокол дейтаграмм (UDP) в качестве транспортного протокола. Все коммуникации NTP используют Всемирное координированное время (UTC).

В ПО коммутатора реализован протокол NTP версии 4. NTP по умолчанию отключен. Можно настроить адрес NTP IPv4 или IPv6, поддерживается максимум пять серверов.

Команды на включение/выключение NTP клиента или сервера:
`ntp mode` { client | server }
`no ntp mode` { client | server }

Настройка IP-адреса NTP-сервера.
`ntp server` <index_var> `ip-address` <ipv4_var>

где:

- <index_var>: значение индекса от 1 до 5.
- <IPv4 _ var>: адрес IPv4 в формате xxx.xxx.xxx.xxx

Для настройки NTP и адреса сервера, используются команды:

```
# configure terminal
```

Включите NTP и укажите IP-адрес сервера

```
(config)# ntp mode client
(config)# ntp server 1 ip-address 217.198.219.102
```

```
2test#
2test# con terminal
2test(config)# ntp mode client
2test(config)# ntp server 1 ip-address 217.198.219.102
2test(config)#
```

CLI позволяет пользователю настраивать местный часовой пояс. Коммутатор должен быть настроен для получения времени с сервера NTP. Часовой пояс по умолчанию настроен как None. При желании выбранному часовому поясу может быть присвоена аббревиатура.

Просмотр статуса NTP.
`show ntp mode` { client | server } `status`
`show ntp status`

```
2test# show ntp status
NTP Mode Client : enabled
Idx   Server IP host address (a.b.c.d) or a host name string
---   ------------------------------------------------------
1     217.198.219.102
2
3
4
5
NTP Mode Server : disabled
NTP Mode ClientTest STRATUM : enabled
NTP Mode ClientTest DISPERSION : enabled
2test#
2test#
```

## 7.4 Часовой пояс

Для установки часового пояса используйте команду:
`clock timezone` <word_var> <hour_var> [ <minute_var> [ <subtype_var> ] ]

где:

- <word_var>: Длина аббревиатуры может составлять до 16 буквенно-цифровых символов, включая специальные символы, такие как "-" (дефис), '.' (точка) и '_' (подчеркивание). В аббревиатуре учитывается регистр символов.
- <часовой пояс>: Часовой пояс UTC-12 – 12.

Пример: установите системный часовой пояс на (GMT+03: 00) Москва, Санкт-Петербург, а сокращение – Moscow (или MOV)

```
(config)# clock timezone Moscow 3
```

Чтобы просмотреть настройки часового пояса используйте команду:

```
< show clock detail >
```

```
2test#
2test# con terminal
2test(config)# clock timezone Moscow 3
2test(config)# ^Z
2test# show clock detail
System Time     : 2025-02-03T09:05:09+03:00

Timezone : Timezone Offset : 1800 ( 180 minutes)
Timezone Acronym : Moscow

Daylight Saving Time Mode : Disabled.
Daylight Saving Time Start Time Settings :
        Week: 1
        Day: 1
        Month: 1
        Date: 1
        Year: 2014
        Hour: 0
        Minute: 0
Daylight Saving Time End Time Settings :
        Week: 1
        Day: 1
        Month: 1
        Date: 1
        Year: 2097
        Hour: 0
        Minute: 0
Daylight Saving Time Offset : 1 (minutes)
2test#
```

## 7.5 Log-файл

Рассмотрим настройку Log-файла и связанные с ним команды. Для этого можно воспользоваться контекстно-зависимой справкой:

```
2test#
2test# con terminal
2test(config)#
2test(config)# logging ?
    host      host
    level     Severity level
    on        Enable Switch logging host mode
2test(config)#
2test(config)# logging level ?
    error             Severity 3: Error conditions
    informational     Severity 6: Informational messages
    notice            Severity 5: Normal but significant condition
    warning           Severity 4: Warning conditions
2test(config)#
2test(config)#
```

где: host = имя хоста (коммутатора), level = приоритет или уровень сложности, on = включить запись лога в режиме host.

Например, в CLI включите серверный режим и задайте адрес сервера для получения логов на адрес 192.168.1.2.

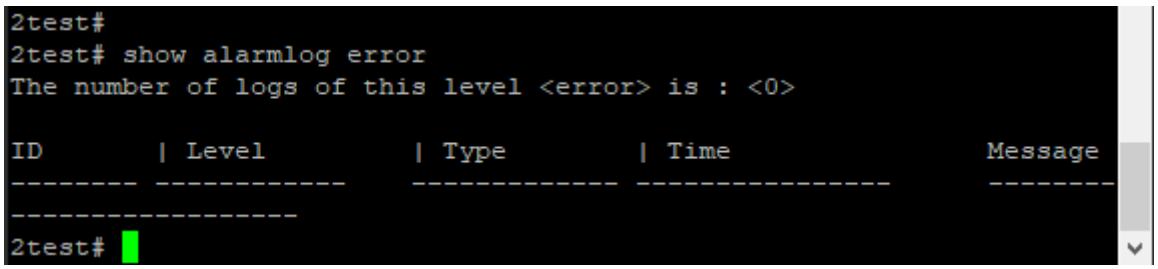
```
2test#
2test#
2test# con ter
2test(config)#
2test(config)# logging on
2test(config)# logging host 192.168.1.2
2test(config)#
2test(config)#
```

Проверка аварийных сообщений в Log-файле
Воспользуемся контекстно-зависимой справкой:

```
2test#
2test# show alarmlog ?
    |                 Output modifiers
    error             Severity 3: Error conditions
    informational     Severity 6: Informational messages
    notice            Severity 5: Normal but significant condition
    warning           Severity 4: Warning conditions
    <cr>
2test#
2test#
```

Пример: Просмотр журнала аварийных сигналов на наличие ошибок

```
# show alarmlog error
```



# VIII. УПРАВЛЕНИЕ ПОРТАМИ

## 8.1 Конфигурация порта

Вы можете просмотреть конфигурацию порта через команду <show interface ?> Здесь и далее воспользуемся контекстно-зависимой справкой для просмотра и выбора команд связанных с конфигурацией портов коммутатора. CLI предлагает выбрать тип порта либо VLAN.

```
2test#
2test# show interface ?
    *                   All switches or All ports
    GigabitEthernet     1 Gigabit Ethernet Port
    2.5GigabitEthernet  2.5 Gigabit Ethernet Port
    vlan                VLAN status
2test#
```

Для просмотра конфигурации медного гигабитного порта (1-16) поддерживаются следующие команды:

```
2test#
2test# show interface GigabitEthernet 1/1 ?
    *                   All switches or All ports
    GigabitEthernet     1 Gigabit Ethernet Port
    2.5GigabitEthernet  2.5 Gigabit Ethernet Port
    capabilities        Display capabilities.
    description         Description of interface
    statistics          Display statistics counters.
    status              Display status.
    switchport          Show interface switchport information
    transceiver         Show interface transceiver
    veriphy             Display the latest cable diagnostic results.
2test#
2test#
```

Для просмотра состояния порта №1 воспользуйтесь командой:
<show interface GigabitEthernet 1/1 status>

```
2test#
2test# show interface GigabitEthernet 1/1 status
Interface              Mode     Speed & Duplex  Flow Control  Max Frame  Excessive  Link

---------------------  -------  --------------  ------------  ---------  ---------  ------

GigabitEthernet 1/1    enabled  Auto            enabled       9600       Discard    1Gfdx

2test#
```

В качестве примера рассмотрим параметры производительности порта №1. Введите команду: <show interface GigabitEthernet 1/1 capabilities>
а затем <show interface GigabitEthernet 1/1 statistic>

```
2test# show interface GigabitEthernet 1/1 capabilities

GigabitEthernet 1/1 Capabilities:
  Model:                  CEServices
  Type:                   10/100/1000BaseT
  Speed:                  10,100,1000,auto
  Duplex:                 half,full,auto
  Trunk encap. type:      802.1Q
  Trunk mode:             access,hybrid,trunk
  Channel:                yes
  Broadcast suppression: no
  Flowcontrol:            yes
  Fast Start:             no
  QoS scheduling:         tx-(8q)
  CoS rewrite:            yes
  ToS rewrite:            yes
  UDLD:                   no
  Inline power:           yes
  RMirror:                no
  PortSecure:             yes
  Dot1x:                  yes
2test#
2test#
2test#
2test#
2test# show interface GigabitEthernet 1/1 statistic

GigabitEthernet 1/1 Statistics:
Rx Packets:                          171   Tx Packets:                           82
Rx Octets:                         22546   Tx Octets:                         16342
Rx Unicast:                            0   Tx Unicast:                            0
Rx Multicast:                        108   Tx Multicast:                         81
Rx Broadcast:                         63   Tx Broadcast:                          1
Rx Pause:                              0   Tx Pause:                              0

Rx 64:                                31   Tx 64:                                 1
Rx 65-127:                            90   Tx 65-127:                             5
Rx 128-255:                           39   Tx 128-255:                           76
Rx 256-511:                           11   Tx 256-511:                            0
Rx 512-1023:                           0   Tx 512-1023:                           0
Rx 1024-1526:                          0   Tx 1024-1526:                          0
Rx 1527-    :                          0   Tx 1527-    :                          0

Rx Priority 0:                       171   Tx Priority 0:                         0
Rx Priority 1:                         0   Tx Priority 1:                         0
Rx Priority 2:                         0   Tx Priority 2:                         0
Rx Priority 3:                         0   Tx Priority 3:                         0
Rx Priority 4:                         0   Tx Priority 4:                         0
Rx Priority 5:                         0   Tx Priority 5:                         0
Rx Priority 6:                         0   Tx Priority 6:                         0
Rx Priority 7:                         0   Tx Priority 7:                        82

Rx Drops:                              0   Tx Drops:                              0
Rx CRC/Alignment:                      0   Tx Late/Exc. Coll.:                    0
Rx Undersize:                          0
Rx Oversize:                           0
Rx Fragments:                          0
```

Для изменения конфигурации порта используются команды, которые можно увидеть в контекстно-зависимой справке. Для этого сначала войдите в общий режим конфигурации `(config)#`, а затем в режим конфигурации порта `(config-if)#.` Обратите внимание на команду `<con ter>` это сокращение от `<configure terminal>`.

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# ?
    access-list           Access list
    aggregation           Create an aggregation
    description           Description of the interface
    do                    To run exec commands in the configuration mode
    dot1x                 IEEE Standard for port-based Network Access Control
    duplex                Interface duplex
    end                   Go back to EXEC mode
    evc                   Ethernet Virtual Connections
    excessive-restart     Restart backoff algorithm after 16 collisions (No
                          excessive-restart means discard frame after 16
                          collisions)
    exit                  Exit from current mode
    flowcontrol           Traffic flow control.
    frame-length-check    Drop frames with mismatch between EtherType/Length
                          field and actually payload size.
    help                  Description of the interactive help system
    ip                    Interface Internet Protocol configuration commands
    ipv6                  IPv6 configuration commands
    lacp                  Enable LACP on this interface
    lldp                  LLDP configurations.
    loop-protect          Loop protection configuration on port
    mac                   MAC keyword
    media-type            Media type.
    mtu                   Maximum transmission unit
    network-clock         network-clock
    no                    Negate a command or set its defaults
    port-security         Enable/disable port security per interface.
    qos                   Quality of Service
    relay                 Port alarm
    rmon                  Configure Remote Monitoring on an interface
    shutdown              Shutdown of the interface.
    snmp-server           Set SNMP server's configurations
    spanning-tree         Spanning Tree protocol
    speed                 Configures interface speed. If you use 10, 100, or
                          1000 keywords with the auto keyword the port will
                          only advertise the specified speeds.
    switchport            Set VLAN switching mode characteristics
    thermal-protect       Thermal group for the interface.
2test(config-if)#
2test(config-if)#
```

Пример: установите скорость порта №1 равной 1Gps

```
(config-if)# interface GigabitEthernet 1/1
(config-if)# speed 1000
```

Затем переведите порт №1 в режим «полный дуплекс» и включите «управление потоком»

```
2test#
2test# con terminal
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# speed 1000
2test(config-if)# duplex ?
    auto    Auto negotiation of duplex mode.
    full    Forced full duplex.
    half    Forced half duplex.
2test(config-if)# duplex full
2test(config-if)# flowcontrol on
2test(config-if)#
```

В следующем примере разберем выключение порта. Закрываем порт №3, порт будет недоступен.

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/3
2test(config-if)# shutdown
2test(config-if)#
```

Открываем порт №3.

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/3
2test(config-if)# no shutdown
2test(config-if)# end
2test#
```

## 8.2 DDMI – цифровой мониторинг интерфейса

Режим DDMI включается командой <ddmi> в режиме общей конфигурации. Проверить статус DDMI можно в режиме [EXEC] с помощью команды <show>

```
2test#
2test# con ter
2test(config)# ddmi
2test(config)# end
2test# show ddmi
Current mode: Enabled
2test#
```

Просмотр данных мониторинга DDMI

```
2test#
2test# show interface GigabitEthernet 1/19 transceiver

GigabitEthernet 1/19
------------------------------
Tranceiver Information
================================================================================
Vendor              :
Part Number         :
Serial Number       :
Revision            :
Data Code           :
Transceiver         : NONE

DDMI Information
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
================================================================================
% SFP module doesn't support DDMI

2test#
```

В данном случае SFP-трансивер не установлен в коммутаторе, поэтому данные не отображаются.

### 8.3 Релейная сигнализация отказов

Просмотреть статус сигнализации отказов можно с помощью команды <show relay>

```
2test#
2test# show relay
Switch relay alarm is disabled
Switch relay power1 alarm is disabled
Switch relay power2 alarm is disabled
relay is configured on following
GigabitEthernet 1/1 disable
GigabitEthernet 1/2 disable
GigabitEthernet 1/3 disable
GigabitEthernet 1/4 disable
GigabitEthernet 1/5 disable
GigabitEthernet 1/6 disable
GigabitEthernet 1/7 disable
GigabitEthernet 1/8 disable
GigabitEthernet 1/9 disable
GigabitEthernet 1/10 disable
GigabitEthernet 1/11 disable
GigabitEthernet 1/12 disable
GigabitEthernet 1/13 disable
GigabitEthernet 1/14 disable
GigabitEthernet 1/15 disable
GigabitEthernet 1/16 disable
GigabitEthernet 1/19 disable
GigabitEthernet 1/20 disable
2.5GigabitEthernet 1/17 disable
2.5GigabitEthernet 1/18 disable
2test#
```

Пример просмотра статуса релейной сигнализации отказов порта №1

```
2test#
2test# show relay interface GigabitEthernet 1/1
GigabitEthernet 1/1 disable
2test#
```

Для включения релейной сигнализации нужно войти в режим общей конфигурации. Ниже пример включения релейной сигнализации источника питания №1.

```
2test#
2test# con ter
2test(config)# relay power 1
2test(config)#
```

Пример включения релейной сигнализации отказов порта №1.

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# relay
2test(config-if)# end
2test#
```

Отключение релейной сигнализации отказов на примере источника питания №1 и порта №1. Обратите внимание, что все действия выполняются в режиме общей конфигурации. Команда <end> завершает работу в режиме общей конфигурации и переводит пользователя в режим # [EXEC].

```
2test#
2test# con ter
2test(config)# no relay power 1
2test(config)#
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# no relay
2test(config-if)# end
2test#
```

# IX. SNMP

## 9.1 Команды для просмотра параметров SNMP

```
2test#
2test# show snmp ?
    |                   Output modifiers
    access              access configuration
    community           Community
    host                Set SNMP host's configurations
    mib                 MIB (Management Information Base)
    security-to-group   security-to-group configuration
    user                User
    view                MIB view configuration
    <cr>
2test#
2test#
```

Ниже приведен пример просмотра конфигурации комьюнити SNMP V3.

```
2test#
2test# show snmp community V3
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

2test#
2test#
```

## 9.2 Настройки SNMP

Ниже приведены соответствующие команды настройки SNMP.

```
2test#
2test# con ter
2test(config)# snmp ?
    access                access configuration
    community             Set the SNMP community
    contact               Set the SNMP server's contact string
    engine-id             Set SNMP engine ID
    host                  Set SNMP host's configurations
    location              Set the SNMP server's location string
    security-to-group     security-to-group configuration
    trap                  Set trap's configurations
    user                  Set the SNMPv3 user's configurations
    version               Set the SNMP server's version
    view                  MIB view configuration
    <cr>
2test(config)#
2test(config)#
```

Ниже приведён пример включения и отключения SNMP, обратите внимание на результаты настройки.

```
2test(config)#
2test(config)# snmp
2test(config)# end
2test#
2test# show snmp

SNMP Configuration
SNMP Mode                     : enabled
SNMP Version                  : 2c
Read Community                : public
Write Community               : private
Trap Mode                     : disabled

SNMPv3 Communities Table:
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0


SNMPv3 Users Table:
User Name               : default_user
Engine ID               : 800007e5017f000001
Security Level          : NoAuth, NoPriv
Authentication Protocol : None
Privacy Protocol        : None


SNMPv3 Groups Table;
Security Model : v1
Security Name  : public
Group Name     : default_ro_group
```

```
Security Model : v2c
Security Name  : private
Group Name     : default_rw_group

Security Model : v3
Security Name  : default_user
Group Name     : default_rw_group


SNMPv3 Accesses Table:
Group Name        : default_ro_group
Security Model    : any
Security Level    : NoAuth, NoPriv
Read View Name    : default_view
Write View Name   : <no writeview specified>

Group Name        : default_rw_group
Security Model    : any
Security Level    : NoAuth, NoPriv
Read View Name    : default_view
Write View Name   : default_view


SNMPv3 Views Table:
View Name    : default_view
OID Subtree : .1
View Type    : included

2test#
```

Теперь мы выключаем SNMP

```
2test#
2test# con ter
2test(config)# no snmp
2test(config)# end
2test# show snmp

SNMP Configuration
SNMP Mode                     : disabled
SNMP Version                  : 2c
Read Community                : public
Write Community               : private
Trap Mode                     : disabled

SNMPv3 Communities Table:
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0


SNMPv3 Users Table:
User Name               : default_user
Engine ID               : 800007e5017f000001
Security Level          : NoAuth, NoPriv
Authentication Protocol : None
Privacy Protocol        : None


SNMPv3 Groups Table;
Security Model : v1
Security Name  : public
Group Name     : default_ro_group

Security Model : v1
Security Name  : private
Group Name     : default_rw_group

Security Model : v2c
Security Name  : public
Group Name     : default_ro_group

Security Model : v2c
Security Name  : private
Group Name     : default_rw_group

Security Model : v3
Security Name  : default_user
Group Name     : default_rw_group
```

…большая часть выходных данных пропущена для краткости…

Команды на включение и выключение SNMP ловушек:

```
(config)# snmp-server trap
(config)# no snmp-server trap
```

Команда для создания нового раздела комьюнити. Создайте новый раздел №1 и установите исходный адрес SNMP -доступа равным 192.168.1.200, а маску источника - 255.255.255.0.

```
(config)# snmp community v3 pub1 192.168.1.200 255.255.255.0
```

Обновление системного идентификатора ядра SNMP. Обратите внимание на то, что обновление идентификатора ядра приводит к удалению всех исходных локальных пользователей.

```
(config)# snmp engine-id local 800007e5017f000002
```

Команды на создание новых записей-ловушек и отключение всех записей-ловушек:

```
(config)# snmp-server host host1
(config-snmps-host)# shutdown
```

Добавление имени комьюнити public 3, назначение IP-адреса источника – 192.168.1.254, с маской подсети 255.255.255.0.

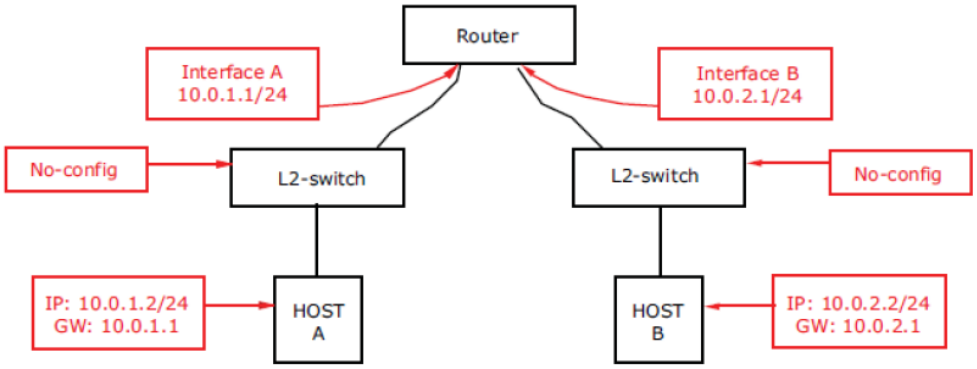
```
(config)# snmp community V3 public3 192.168.1.100 255.255.255.0
```

# X. НАСТРОЙКА СТАТИЧЕСКОЙ МАРШРУТИЗАЦИИ

IP-адрес идентифицирует устройство в IP-сети. Длина адреса IP версии 4 (IPv4) составляет 32 бита. IPv4-адрес может быть назначен только через интерфейс VLAN. IP-адрес может быть задан как вручную (так называемый статический IP) так и автоматически с помощью протокола DHCP.

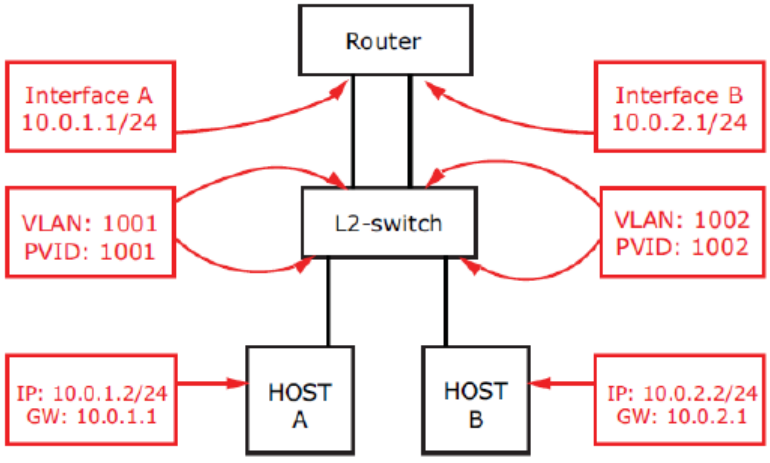
## 10.1 Традиционные сети

Для маршрутизации используются как узел TCP/IP, так и IP-маршрутизатор. На рисунке ниже показана конфигурация традиционной сети с двумя IP-сетями и маршрутизатором. Каждой IP -сети должен быть назначен IP-адрес и шлюз, на который могут пересылаться пакеты.




## 10.2 Использование коммутатора с VLAN

На следующем рисунке показана та же сеть, но настроенная на использование коммутатора с VLAN. Использование VLAN - это метод разделения потоков внутри одного коммутатора.



### 10.3 Настройка маршрутизации

**Шаг 1.** Создайте VLAN 1001 и 1002, чтобы разделить две IP-сети

```
2test# configure terminal
2test(config)# vlan 1001
2test(config-vlan)# vlan 1002
2test(config-vlan)# exit
```

**Шаг 2.** Определите порт VLAN для каждого порта, используя команду <switchport access vlan>, чтобы указать VLAN для каждого интерфейса. Не помеченные тегами кадры будут ассоциироваться с этой VLAN.

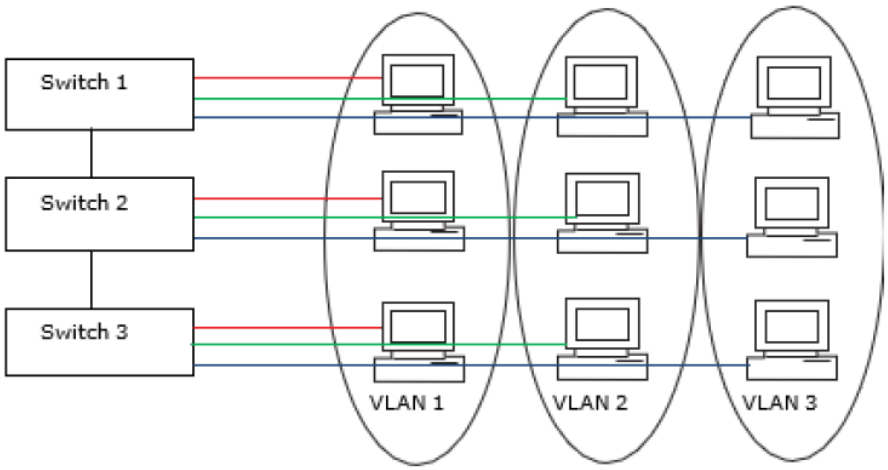
```
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# switchport access vlan 1001
2test(config-if)# exit
2test(config)# interface GigabitEthernet 1/2
2test(config-if)# switchport access vlan 1002
2test(config-if)# exit
```

**Шаг 3.** Настройте сегменты A и B маршрутизатора, используя команду <ip address>, чтобы задать основной IP -адрес для интерфейсов.

```
2test(config)# interface vlan 1001
2test(config-if-vlan)# ip address 10.0.1.1 255.255.255.0
2test(config-if-vlan)# exit
2test(config)# interface vlan 1002
2test(config-if-vlan)# ip address 10.0.2.1 255.255.255.0
2test(config-if-vlan)# end
```

# XI. VLAN

На рисунке показан пример конфигурации виртуальной локальной сети.




Поскольку VLAN 1 создана по умолчанию, нужно только добавить VLAN 2 и 3 следующим образом:

```
#configure terminal
(config)# vlan 2
(config)# vlan 3
```

Назначте порт доступа. Предположим, что порты с 1 по 3 подключены к ПК. PVID каждого порта отличается.

```
#con ter
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 1
(config)# exit
(config)# interface GigabitEthernet 1/2
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config)# exit
(config)# interface GigabitEthernet 1/3
(config-if)# switchport mode access
(config-if)# switchport access vlan 3
(config)# exit
```

Назначте транковый (магистральный) порт. Предположим, что порт 4 подключен к другому коммутатору. Установите для принимаемой VLAN значение 1-3.

```
configure terminal
(config)# interface GigabitEthernet 1/4
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 1-3
```

Настройте порт таким образом, чтобы тегированные кадры всегда передавались на порт №4.

```
(config-if)# switchport trunk vlan tag native
```

## 11.1 Создание и удаление VLAN

Рассмотрим пример создания новой VLAN

```
# con ter
(config)# vlan 2
```

Удаление VLAN

```
# con ter
(config)# no vlan 2
```

```
2test#
2test# con ter
2test(config)# vlan 2
2test(config-vlan)# end
2test# show vlan all
VLAN  Name                             Interfaces
----  -------------------------------  ----------
1     default                          Gi 1/1-6,9-16,19-20 2.5G 1/17-
18
2     VLAN0002
99    99                               Gi 1/7-8

2test# con ter
2test(config)# no vlan 2
2test(config)# end
2test# show vlan all
VLAN  Name                             Interfaces
----  -------------------------------  ----------
1     default                          Gi 1/1-6,9-16,19-20 2.5G 1/17-
18
99    99                               Gi 1/7-8

2test#
```

Поле VLAN с разрешенным доступом влияет только на порты, настроенные как порты доступа. Порты в других режимах являются членами всех VLAN, указанных в поле разрешенные VLAN . По умолчанию включена только VLAN 1. Можно создать больше VLAN, используя следующий синтаксис списка.

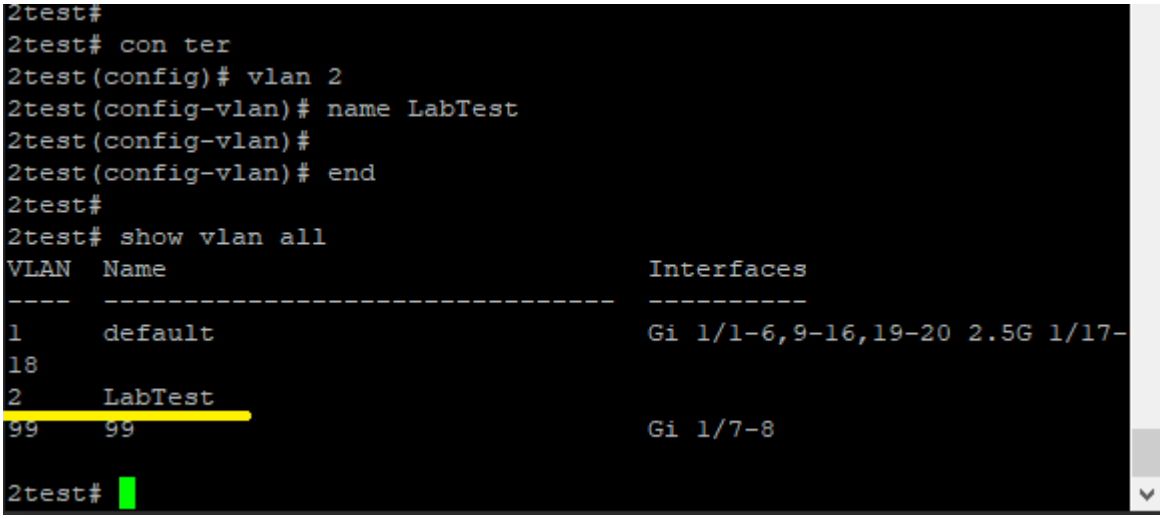
```
# configure terminal
(config)# vlan1,10-13,200,300
```

Отдельные элементы разделяются запятыми, а диапазоны указываются с помощью тире , разделяющего нижнюю и верхнюю границы. Между разделителями допускаются пробелы. В примере приведенном выше создаются сети VLAN 1, 10, 11, 12, 13, 200, и 300.

## 11.2 Присвоение имени VLAN

Задайте имя VLAN #2.

```
# con terminal
(config)# vlan 2
(config-vlan)# name [имя vlan]
```




## 11.3 Настройка портов в VLAN

Режим порта определяет основные параметры работы данного порта. Порт может находиться в одном из трех режимов, при этом по умолчанию используется режим доступа. Сейчас мы рассмотрим три режима работы порта.

### Access – режим доступа

Порты доступа обычно используются для подключения к конечным станциям. Порты доступа имеют следующие характеристики:

- Состоит только в одной VLAN, локальной сети порта или VLAN доступа, которая по умолчанию является 1;
- Принимает кадры без меток и с метками C;
- Отбрасывает все кадры , которые не относятся к VLAN доступа;
- При выходе все кадры передаются без меток.

Пример: настройка порта №1 в качестве порта доступа

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# switchport mode access
2test(config-if)# end
2test#
```

### Trunk – транковый порт (магистральный)

Транковые порты могут передавать трафик по нескольким сетям VLAN одновременно и обычно используются для подключения к другим коммутаторам. Транковые порты имеют следующие характеристики:

- По умолчанию является членом всех существующих сетей VLAN (ограничено использованием разрешенных сетей VLAN);
- Все кадры, кроме тех, которые классифицируются как порт VLAN или собственная сеть VLAN, помечаются на выходе по умолчанию (кадры, классифицированные как порт VLAN, не помечаются C-тегом на выходе);
- Пометку на выходе можно изменить, чтобы пометить все кадры, в этом случае при входе принимаются только помеченные кадры.

Пример: настройка порта №1 в качестве транкового порта

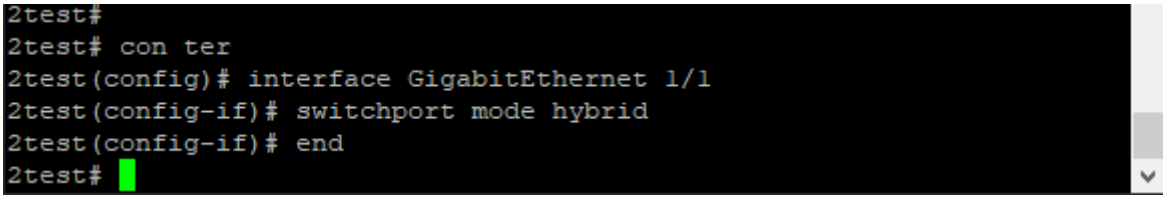
```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# switchport mode trunk
2test(config-if)# end
2test#
```

### Hybrid – гибридный порт

Гибридные порты во многом напоминают магистральные порты, хотя и включают дополнительные функции настройки портов. В дополнение к характеристикам, описанным для магистральных портов, гибридные порты обладают следующими возможностями:

- Можно управлять фильтрацией входных данных;
- Можно независимо настраивать прием входных данных и конфигурацию тегирования выходных данных.

Пример: настройка порта №1 в качестве гибридного порта:




## 11.4 Порт VLAN и PVID

Порт VLAN определяет идентификатор VLAN порта, или **PVID**. Допустимые значения VLAN находятся в диапазоне от 1 до 4095, значение по умолчанию равно 1.

При входе фреймы классифицируются по порту VLAN, если порт настроен как не поддерживающий VLAN, фрейм не помечен тегом или для порта включена поддержка VLAN, но фрейм помечен как приоритетный (идентификатор VLAN = 0).

На выходе кадры, отнесенные к порту VLAN, не помечаются, если для параметра "Пометка на выходе " установлено значение "Не помечать порт VLAN".

Сеть VLAN порта называется "Сетью доступа VLAN" для портов в режиме доступа и собственной VLAN для портов в транковом или гибридном режиме.

Пример: установите значение порта VLAN равным 2 для гигабитного порта 1/1 настроенного в режиме доступа.

```
#con ter
(config)# interface GigabitEthernet 1/1
(config-if)# switchport access vlan ?
<vlan_id> VLAN ID of the native VLAN when this port is in trunk
mode
(config-if)# switchport access vlan 2
```

Пример: установите значение порта VLAN равным 2 для гигабитного порта 1/1 настроенного в режиме транк.

```
#con ter
(config)# interface GigabitEthernet 1/1
(config-if)# switchport trunk native vlan 2
```

Пример: установите значение порта VLAN равным 2 для гигабитного порта 1/1 настроенного в режиме гибридный порт.

```
#con ter
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid native vlan 2
```

## 11.5 Входная фильтрация

Гибридные порты позволяют изменять входную фильтрацию. На портах доступа и транковых портах всегда включена входная фильтрация.

Если включена входная фильтрация, кадры, отнесенные к сети VLAN, членом которой порт не является , отбрасываются.

Если входная фильтрация отключена, кадры, отнесенные к сети VLAN, членом которой порт не является, принимаются и пересылаются в механизм коммутации. Однако порт никогда не будет передавать кадры, отнесенные к сетям VLAN, членом которых он не является.

Установка входной фильтрации на порту 1/1

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# switchport hybrid ?
    acceptable-frame-type    Set acceptable frame type on a port
    allowed                  Set allowed VLAN characteristics when int
erface is
                             in hybrid mode
    egress-tag               Egress VLAN tagging configuration
    ingress-filtering        VLAN Ingress filter configuration
    native                   Set native VLAN
2test(config-if)#
2test(config-if)#
```

## 11.6 Разрешенные VLAN

Порты в транковом и гибридном режимах могут управлять тем, в какие VLAN им разрешено входить. Порты доступа могут быть только членами VLAN Access.

Синтаксис в этом разделе CLI идентичен синтаксису, используемому в разделе Существующие сети VLAN. По умолчанию порт может быть включен во все возможные сети VLAN, поэтому установите для него значение 1-4095.

Пример: установите значение порта VLAN равным 2 для гигабитного порта1/1 (настроенного как транковый порт).

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# switchport trunk allowed vlan ?
    <vlan_list>    VLAN IDs of the allowed VLANs when this port is in
trunk
                   mode
    add            Add VLANs to the current list
    all            All VLANs
    except         All VLANs except the following
    none           No VLANs
    remove         Remove VLANs from the current list
2test(config-if)#
2test(config-if)#
```

Пример: установите значение порта VLAN равным 2 для гигабитного порта1/1 (настроенного как гибридный порт).

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# switchport hybrid allowed vlan ?
    <vlan_list>    VLAN IDs of the allowed VLANs when this port is in
hybrid
                   mode
    add            Add VLANs to the current list
    all            All VLANs
    except         All VLANs except the following
    none           No VLANs
    remove         Remove VLANs from the current list
2test(config-if)#
2test(config-if)#
```

## 11.7 Запрещенные VLAN

Порт может быть настроен таким образом, чтобы он никогда не входил в одну или несколько сетей VLAN. Это особенно полезно, когда необходимо запретить динамическое добавление портов в сети VLAN динамическими протоколами, такими как MVRP и GVRP.

Смысл состоит в том, чтобы пометить такие VLAN как запрещенные на соответствующем порту. Синтаксис идентичен синтаксису, используемому в разделе Существующие VLAN (Existing VLANs).

По умолчанию в разделе VLAN нет запрета на порт, что означает, что порт может стать участником всех возможных сетей VLAN.

В приведенном примере показана настройка запрещенной VLAN на первом гигабитном порту (1/1).

```
2test#
2test# con ter
2test(config)# interface GigabitEthernet 1/1
2test(config-if)# switchport forbidden vlan ?
    add       Add to existing list.
    remove    Remove from existing list.
2test(config-if)#
```

## 11.8 Просмотр статуса VLAN

Воспользуйтесь констектно-зависимой справкой

```
2test#
2test#
2test# show vlan ?
    all       Show all VLANs (if left out only access VLANs are shown)
    brief     VLAN summary information
    id        VLAN status by VLAN id
    name      VLAN status by VLAN name
    status    Show the VLANs configured for each interface.
    <cr>
2test# show vlan
VLAN  Name                            Interfaces
----  ------------------------------  ----------
1     default                         Gi 1/1-6,9-16,19-20 2.5G 1/17-1
8
99    99                              Gi 1/7-8

2test#
```

Введите команду <show vlan status>, CLI покажет конфигурацию VLAN на каждом интерфейсе.

```
2test#
2test# show vlan status
GigabitEthernet 1/1 :
--------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag
       UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------
------  ----  ---------
Combined    C-Port         1     All            Enabled     None
       1     No
Admin       C-Port         1     All            Enabled     None
       1
NAS
             No
MSTP
             No
ERPS
             No
MEP
             No
EVC
             No

GigabitEthernet 1/2 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UV
ID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  --
--  ---------
Combined    C-Port         1     All            Enabled     None               1
    No
Admin       C-Port         1     All            Enabled     None               1

NAS
    No
MSTP
    No
ERPS
    No
MEP
    No
EVC
    No

GigabitEthernet 1/3 :
---------------------
2test#
```

```
GigabitEthernet 1/7 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  ----  ---------
Combined    C-Port         99    All            Enabled     None               99    No
Admin       C-Port         99    All            Enabled     None               99
NAS                                                                                  No
MSTP                                                                                 No
ERPS                                                                                 No
MEP                                                                                  No
EVC                                                                                  No

GigabitEthernet 1/8 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  ----  ---------
Combined    C-Port         99    All            Enabled     None               99    No
Admin       C-Port         99    All            Enabled     None               99
NAS                                                                                  No
MSTP                                                                                 No
ERPS                                                                                 No
```

```
GigabitEthernet 1/19 :
----------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag            UVID  Conflicts
----------  -------------  ----  -------------  ----------  ----------------  ----  ---------
Combined    C-Port         1     All            Enabled     None              1     No
Admin       C-Port         1     All            Enabled     None              1
NAS                                                                                 No
MSTP                                                                                No
ERPS                                                                                No
MEP                                                                                 No
EVC                                                                                 No

GigabitEthernet 1/20 :
----------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag            UVID  Conflicts
----------  -------------  ----  -------------  ----------  ----------------  ----  ---------
Combined    C-Port         1     All            Enabled     None              1     No
Admin       C-Port         1     All            Enabled     None              1
NAS                                                                                 No
MSTP                                                                                No
ERPS                                                                                No
MEP                                                                                 No
EVC                                                                                 No

2test#
```

# XII. DHCP

## 12.1 DHCP сервер

DHCP-сервер назначает DHCP-клиентам IP-адреса из указанных пулов адресов. Он также может управлять этими клиентами и предоставлять сетевые параметры, такие как адрес шлюза по умолчанию, адрес сервера системы доменных имен (DNS) и адрес сервера Windows Службы интернет-имен (WINS). DHCP-сервер может принимать широковещательные рассылки от локально подключенных сегментов локальной сети или DHCP-запросы, пересылаемые агентами ретрансляции DHCP внутри сети.

Включение DHCP сервера:

```
#configure terminal
(config)# ip dhcp server
```

Активация DHCP сервера на интерфейсе VLAN:

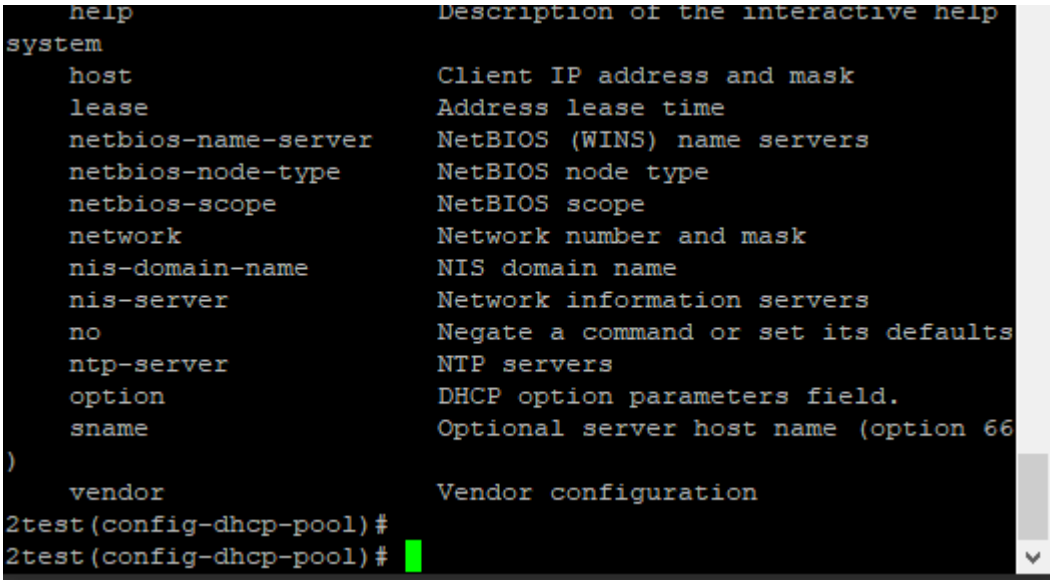
```
#configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip dhcp server
```

Настройка резервного IP-адреса

```
# configure terminal
(config)# ip dhcp excluded-address <ipv4_addr>
```

Пул адресов. В соответствии с пулом DHCP DHCP-сервер выделит IP-адрес и передаст параметры конфигурации DHCP-клиенту. Воспользуйтесь конткстно-зависимой справкой `(config-dhcp-pool)# ?`

```
2test#
2test# con ter
2test(config)# ip dhcp pool 1
2test(config-dhcp-pool)# ?
    broadcast              Broadcast address in use on the clie
nt's subnet
    client-identifier      Client identifier
    client-name            Client host name
    default-router         Default routers
    dns-server             DNS servers
    do                     To run exec commands in the configur
ation mode
    domain-name            Domain name
    end                    Go back to EXEC mode
    exit                   Exit from current mode
    file                   Boot file name (option 67)
    hardware-address       Client hardware address
    help                   Description of the interactive help
system
    host                   Client IP address and mask
    lease                  Address lease time
```




## 12.2 DHCP снупинг

DHCP снупинг – это технология безопасности протокола DHCP канального уровня, которая гарантирует, что DHCP-клиенты получают IP-адреса от действительных DHCP-серверов, и записывает соответствующую взаимосвязь между IP-адресом DHCP-клиента и MAC -адресом, чтобы предотвратить DHCP-атаку в сети.

Режим снупинга.

Если включен режим DHCP снупинга, сообщения с запросами DHCP будут перенаправляться на доверенные порты и разрешать отправку ответных пакетов только с доверенных портов. Включение режима:

```
#configure terminal
(config)# ip dhcp snooping
```

Настройка режима на гигабитном порту.

Trusted = надежный: настраивает порт как надежный источник DHCP-сообщений.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# ip dhcp snooping trust
```

## 12.3 Ретрансляция DHCP

Агент ретрансляции DHCP пересылает DHCP-сообщения между DHCP-сервером и DHCP-клиентами и помогает DHCP-серверу динамически распределять сетевые параметры между DHCP-клиентами.

Когда DHCP-клиент передает сообщения с запросами с IP-адресом назначения 255.255.255.255, только DHCP-сервер, расположенный в том же сегменте сети, что и DHCP -сервер, может получать сообщения с запросами.

Если DHCP-сервер находится в сегменте сети отличном от DHCP-клиента, DHCP-сервер не может получать сообщения с запросами от DHCP-клиента, необходимо развернуть агент ретрансляции DHCP для пересылки DHCP -сообщений на DHCP-сервер.

В отличие от традиционной переадресации IP-сообщений, агент ретрансляции DHCP изменяет формат сообщения для создания нового DHCP-сообщения и затем пересылает его после получения DHCP-запроса или ответного сообщения.

### Режим ретрансляции.

Когда включен режим ретрансляции DHCP, агент переадресовывает и передает DHCP-сообщения между клиентами и сервером, когда они находятся в разных доменах подсети. Широковещательное сообщение DHCP не будет передано по соображениям безопасности.

```
# configure terminal
(config)# ip dhcp relay
```

### Режим ретрансляции инфорации.

Когда включен режим ретрансляции информации DHCP, агент вставляет определенную информацию (опция 82) в DHCP-сообщение при пересылке на DHCP-сервер и удаляет ее из DHCP-сообщения при передаче DHCP-клиенту.

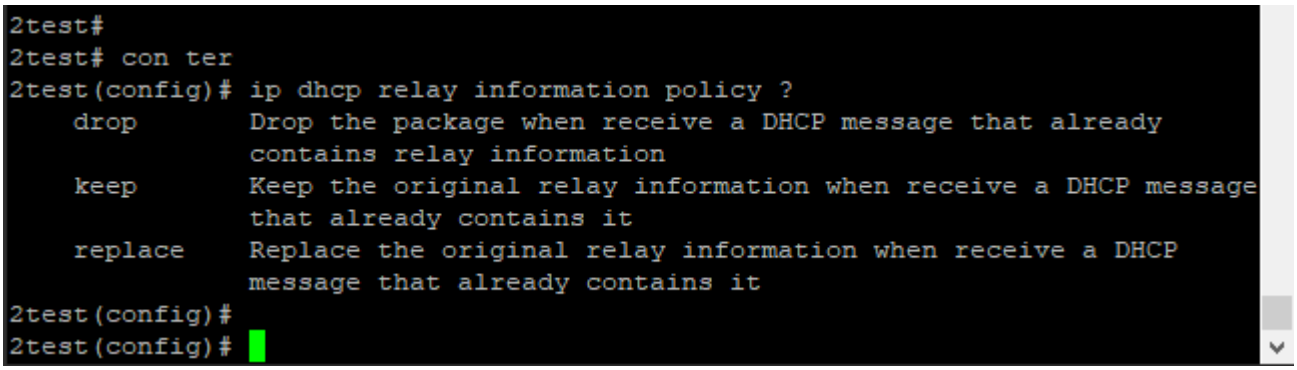
```
# configure terminal
(config)# ip dhcp relay information option
```

### Политика ретрансляции информации.

Режим ретрансляции информации DHCP включается, если агент получает DHCP-сообщение, которое уже содержит информацию об агенте ретрансляции.

- Заменить: Замените исходную информацию о ретрансляции при получении DHCP-сообщения, которое уже содержит ее.
- Сохранить: Сохраните исходную информацию о ретрансляции при получении DHCP-сообщения, которое уже содержит ее.
- Удалить: удаление пакета при получении DHCP-сообщения, которое уже содержит информацию о ретрансляции.

На рисунке показана контекстно-зависимая справка по командам политики ретрансляции.

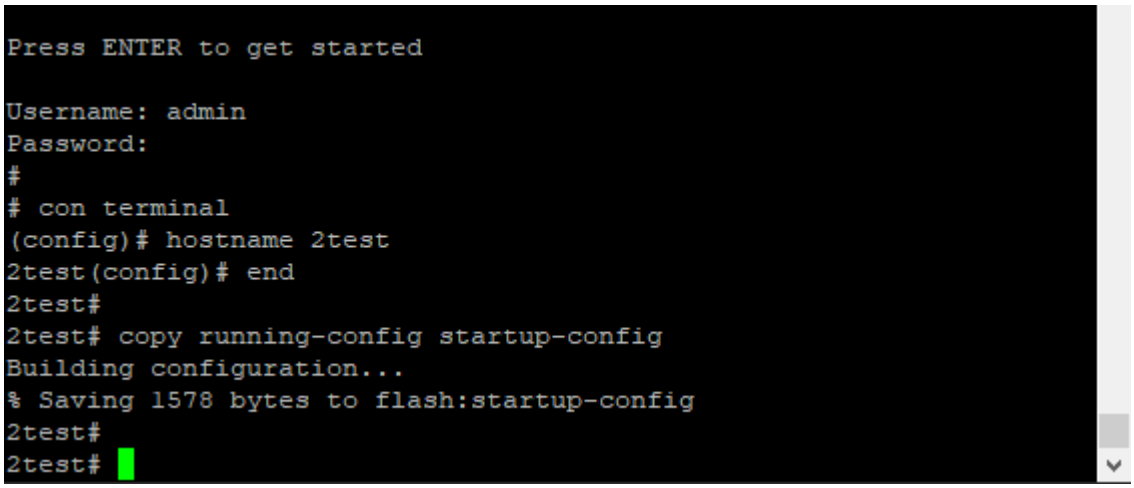

2test#
2test# con ter
2test(config)# ip dhcp relay information policy ?
drop Drop the package when receive a DHCP message that already contains relay information
keep Keep the original relay information when receive a DHCP message that already contains it
replace Replace the original relay information when receive a DHCP message that already contains it
2test(config)#
2test(config)#

# XIII. НАСТРОЙКА DHCP КЛИЕНТА

Эта глава описывает базовое использование CLI для настройки DHCP клиента. Даже при отсутствии сетевого подключения коммутатором можно управлять с помощью подключения к порту «консоль». Настройки утилиты PuTTY или аналога при подключении к последовательному порту должна быть следующие:

- 115200 baud rate
- No parity
- data bits
- 1 stop bit
- No flow control

После подключения к последовательному порту введите имя пользователя и пароль. Войдите в режим конфигурации: `<con terminal>`
Установите имя хоста (коммутатора): `<hostname [имя]>`
Вернитесь в режим #: `<end>`
Сохраниете настройки:`<copy running-config startup-config>`




## 13.1 DHCP клиент

DHCP-клиент коммутатора отправляет запросы на настройку IP-адресов. Когда запросы поступают на DHCP-сервер в сети, сервер выполняет поиск в своем пуле доступных IP-адресов, выделяет один из них и возвращает его DHCP-клиенту. Возвращаемая информация обычно включает IP-адрес, маску подсети и шлюз по

умолчанию, но может также содержать другую информацию, такую как адреса серверов службы доменных имен (DNS).

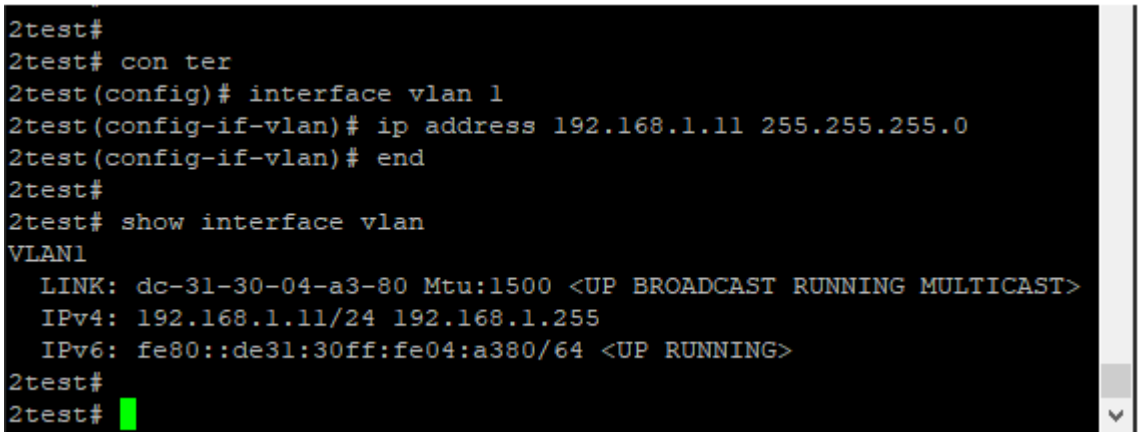
Помните! IP-адреса могут быть назначены только интерфейсам VLAN.

Режим настройки интерфейса используется для настройки параметров интерфейса или ряда интерфейсов. Интерфейсом может быть физический порт, VLAN или другой виртуальный интерфейс. Режим настройки интерфейса также различается в зависимости от типа интерфейса. Команды в CLI для каждого типа интерфейса немного отличаются.

Режим настройки интерфейса VLAN используется для настройки параметров интерфейса VLAN. В следующих разделах описаны команды для доступа к режиму настройки интерфейса VLAN.

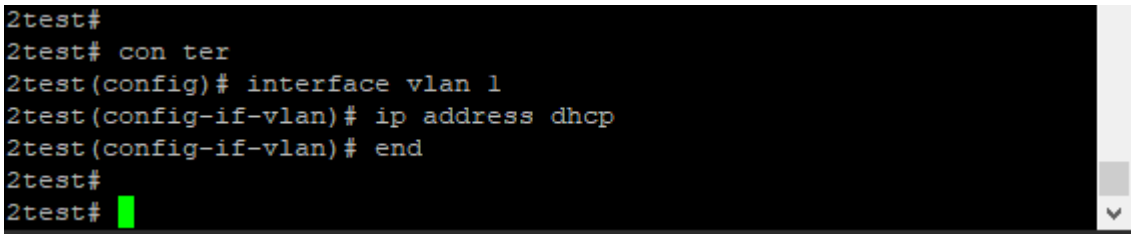
## 13.2 Статический IP-адрес

Как правило VLAN 1 обычно используется в качестве управляющей VLAN. Цель состоит в том, чтобы назначить IP-адрес устройству в VLAN 1 (напрмер 192.168.1.11). Команды CLI показаны на рисунке ниже.



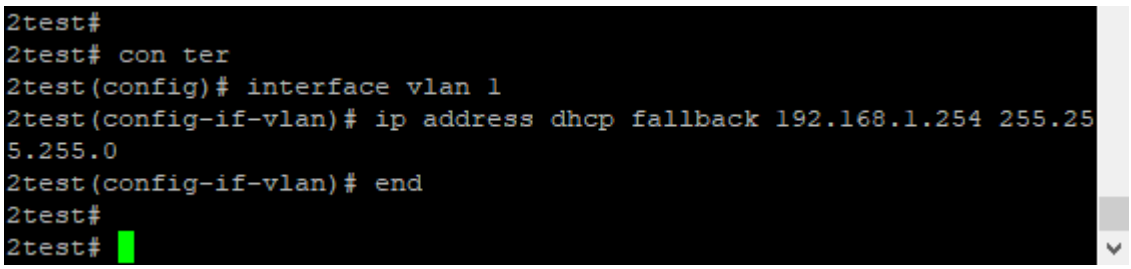
## 13.3 DHCP адрес

DHCP-клиент должен быть включен для автоматического получения IP-адреса от DHCP-сервера, расположенного в сети. Команды на всключение DHCP-клиента на рисунке ниже.



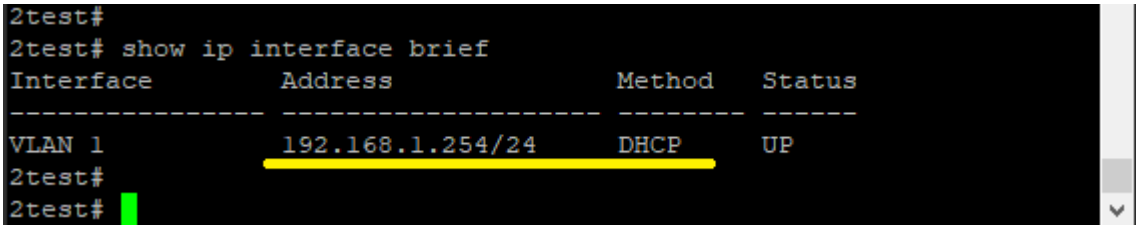

## 13.4 DHCP адрес с резервированием

Если время ожидания получения IP-адреса истекло и в данный момент времени DHCP сервер не обнаружен, рекомендуется назначать резервным IP-адресом IP-адрес присвоенный по умолчанию (в данном случае 192.168.1.254)




## 13.5 Отображение IP-адреса

При включенном режиме DHCP и отстутствии DHCP-сервера в сети после запроса на отображение статического IP-адреса, будет отображен резервный адрес, который вы назначили (cv/ выше):



После успешного согласования клиента с DHCP-сервером, при запросе IP-адреса будет отображаться адрес полученный от DHCP-сервера соответственно.

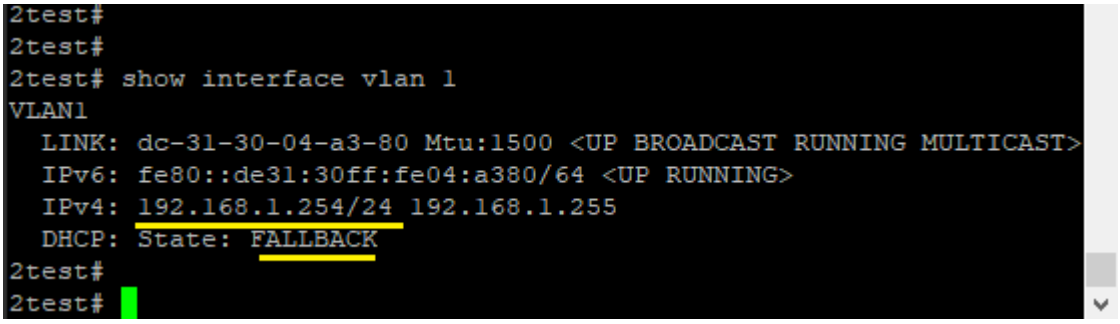
Команда <show ip interface> кратко отображает настроенные и активные IP-интерфейсы. На активных интерфейсах должен отображаться статус **UP** см. скриншот выше).

Если этот статус не отображается, возможно , ни на одном из портов нет соединения. В случае сбоя согласования DHCP назначается резервный IP-адрес? То есть 192.168.1.254.

Команда <show ip dhcp detailed statistics client> отображает статистику сеанса DHCP на каждом порту.

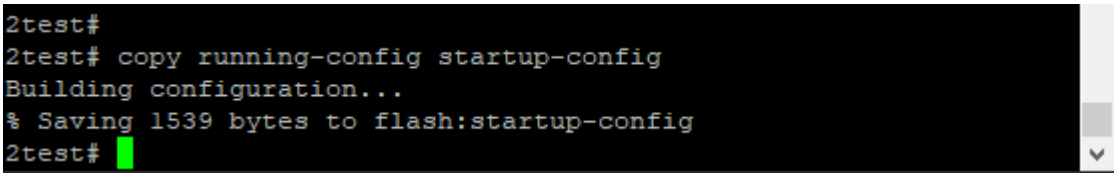
```
2test#
2test#
2test# show ip dhcp detailed statistics client
GigabitEthernet 1/1 Statistics:
--------------------------------
Rx Discover:                    0   Tx Discover:                   42
Rx Offer:                       0   Tx Offer:                       0
Rx Request:                     0   Tx Request:                     0
Rx Decline:                     0   Tx Decline:                     0
Rx ACK:                         0   Tx ACK:                         0
Rx NAK:                         0   Tx NAK:                         0
Rx Release:                     0   Tx Release:                     0
Rx Inform:                      0   Tx Inform:                      0
Rx Lease Query:                 0   Tx Lease Query:                 0
Rx Lease Unassigned:            0   Tx Lease Unassigned:            0
Rx Lease Unknown:               0   Tx Lease Unknown:               0
Rx Lease Active:                0   Tx Lease Active:                0
Rx Discarded checksum error:    0

GigabitEthernet 1/2 Statistics:
--------------------------------
Rx Discover:                    0   Tx Discover:                    0
Rx Offer:                       0   Tx Offer:                       0
Rx Request:                     0   Tx Request:                     0
Rx Decline:                     0   Tx Decline:                     0
Rx ACK:                         0   Tx ACK:                         0
Rx NAK:                         0   Tx NAK:                         0
Rx Release:                     0   Tx Release:                     0
Rx Inform:                      0   Tx Inform:                      0
Rx Lease Query:                 0   Tx Lease Query:                 0
Rx Lease Unassigned:            0   Tx Lease Unassigned:            0
Rx Lease Unknown:               0   Tx Lease Unknown:               0
Rx Lease Active:                0   Tx Lease Active:                0
Rx Discarded checksum error:    0

GigabitEthernet 1/3 Statistics:
--------------------------------
Rx Discover:                    0   Tx Discover:                    0
Rx Offer:                       0   Tx Offer:                       0
Rx Request:                     0   Tx Request:                     0
Rx Decline:                     0   Tx Decline:                     0
Rx ACK:                         0   Tx ACK:                         0
Rx NAK:                         0   Tx NAK:                         0
Rx Release:                     0   Tx Release:                     0
```

Другой способ показать IP-адрес - это отобразить фактическую VLAN, обратите внимание на статус DHCP:




## 13.6 Сохранение текущей конфигурации во флэш-память

Помните! Текущая конфигурация коммутатора автоматически не сохраняется. И при перезагрузке будет утеряна. Используйте команду <copy running-config startup-config>, чтобы сохранить running-config во флэш-памяти под именем startup-config (см. Глава VI стр. 52).




Файл **startup-config** считывается и запускается при каждой загрузке. Он также используется для восстановления текущей конфигурации системы до последнего сохраненного состояния.

# XIV. НАСТРОЙКА HTTPS

В этой главе говорится о том, как настроить HTTPS для безопасного обмена данными между http-клиентом (обычно веб-браузером) и http-сервером с помощью команд CLI.

Функциональность HTTPS предназначена для безопасного обмена данными между браузером (консоль управления) и веб-сервером (коммутатор). Включенный самозаверяющий сертификат может вызвать предупреждение браузера о том, что сертификат выдан ненадежным источником. Механизм загрузки сертификата в программном обеспечении коммутатора позволяет использовать доверенный сторонний сертификат.

## 14.1 Понятие HTTPS

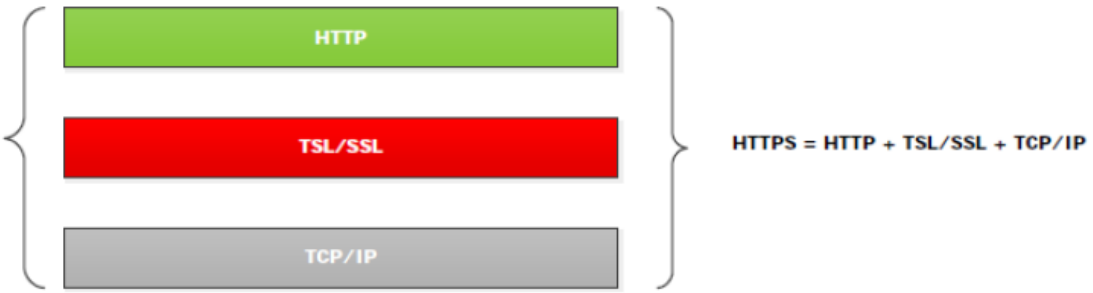
HTTPS (Hypertext Transfer Protocol Secure) - это метод обеспечения безопасности передачи данных HTTP по сети TCP/IP. Он добавляет возможности безопасности SSL/TLS к стандартным HTTP-коммуникациям между HTTP-клиентом (обычно веб-браузером) и HTTP-сервером (обычно веб-сервером). Основной целью использования HTTPS является предотвращение атак типа «человек посередине» или подслушивания.

### Ограничения

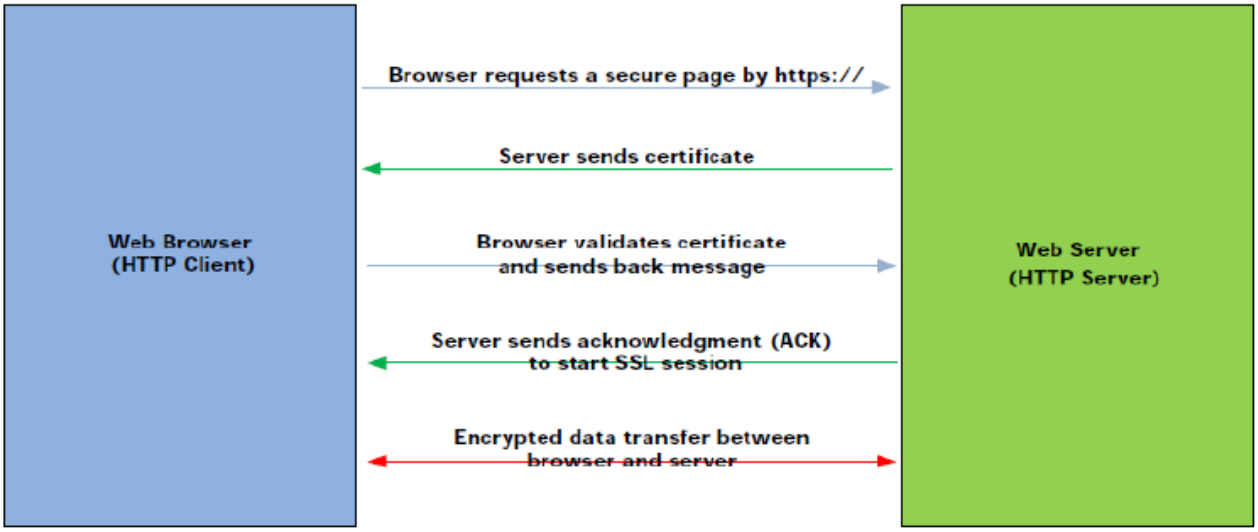
В соответствии с моделями HTTP-связи адреса хостов (веб-серверов) и номера портов обязательно являются частью базовых протоколов TCP/IP. Протокол HTTPS не может защитить их раскрытие, но шифрует содержимое HTTP-данных (полезную нагрузку) - это означает , что перехватчик может определить IP-адрес, доменное имя и номер порта веб -сервера, но не содержимое приложений.

### Рабочая модель HTTPS

- Многоуровневый протокол (рис. ниже): HTTPS - это механизм наложения HTTP поверх SSL/TLS и добавления возможностей защиты данных в HTTP-приложение.



- Проверка подлинности: веб-браузеру требуется сертификат сервера от веб-сервера , прежде чем будет установлено соединение SSL/TLS. Для начала передачи данных по протоколу HTTPS требуется соединение SSL/TLS.
- Шифрование (рис. ниже): как только устанавливается SSL-соединение, передача данных шифруется с помощью открытого ключа, предоставляемого сертификатом безопасности.




## 14.2 Требования к конфигурации

В этом параграфе перечислены необходимые условия для настройки и/или мониторинга операций на коммутаторах, использующих платформу управления.

- Компьютер с разъемом (USB) RS-232 и сетевой картой
- Программное обеспечение эмулятора терминала, поддерживающее последовательный порт (PuTTY, MobaXterm и т.п.)
- Параметры последовательного порта, указанные ниже:
  - Скорость передачи данных 115200 бод
  - Бит данных: 8 бит
  - Стоп бит: 1 бит
  - Управление потоком: запрещено
  - Бит четности: нет.

## 14.3 Настройка HTTPS

Протокол HTTPS включен по умолчанию. Веб-браузер может получить доступ к коммутатору по адресу https://192.168.1.254 (это IP-адрес коммутатора при заводских настройках). В этом параграфе приведены рекомендации по изменению конфигурации для загруженного коммутатора с использованием настроек по умолчанию.

### Настройки HTTPS по умолчанию и настраиваемый диапазон значений.

В таблице приведены подробные сведения о настройках HTTPS по умолчанию и настраиваемом диапазоне значений. Сведения даются на английском языке, как это представлено в CLI.

| Configuration | Default Value | Configurable Value |
|---|---|---|
| Mode | Enable | Enable, Disabled |
| Automatic Redirect | Disabled | Enable, Disabled |
| Certificate Maintain | None | None, Delete, Upload, Generate |
| Certificate Algorithm | RSA | RSA |
| PassPhrase | None | A string pattern |
| Certificate Upload | Browser | Web Browser, URL |
| Certificate Status | N/A | Non-configurable |

Defaul Value – настройки по умолчанию.
Соташgurable Value – настраиваемый диапазон значений.

Настройка HTTPS - это многоступенчатый процесс, как описано выше.

### Включение HTTPS

Войдите в режим общей конфигурации.

```
# con ter
(config)#
```

Включите HTTPS

```
(config)# ip http secure-server
```

Теперь режим HTTPS включен и браузер может запрашивать защищенные данные по протоколу https://

### Автоматическое перенаправление веб-браузера в режим HTTPS

Войдите в режим общей конфигурации.

```
# con ter
(config)#
```

Включите автоматическое перенаправление.

```
(config)# ip http secure-redirect
```

Автоматическое перенаправление браузера включено.

### Создание нового сертификата для замены текущего

Если хотите удалить сертификат:
Выключите HTTPS

```
(config)# no ip http secure-server
```

Удалите сертификат HTTPS

```
(config)# ip http secure-certificate delete
```

Сертификат удалён.

Если хотите заменить сертификат:
Выключите HTTPS

```
(config)# no ip http secure-server
```

Сгенерируйте HTTPS-сертификат с помощью RSA или DSA
Сгенерировать сертификат с помощью алгоритма RSA можно следующим образом:

```
(config)# ip http secure-certificate generate RSA
```

или

Сгенерировать сертификат с помощью алгоритма DSA.

```
(config)# ip http secure-certificate generate DSA
```

Сертификат HTTPS сгенерирован.

### Загрузка стороннего сертификата для замены текущего

Выключите HTTPS

```
(config)# no ip http secure-server
```

Загрузите сертификат с серверов tftp или http, ниже приведен пример загрузки именованного стороннего сертификата:

```
(config)# ip http secre-certificate upload\
tftp://10.0.0.123/https_server_certificate.pem
```

Новый сертификат загружен.

### Обратите внимание!

Необходимо выключить HTTPS перед загрузкой, созданием или удалением сертификата. Включите HTTPS после завершения процесса.

# ПРИЛОЖЕНИЕ 1. УСИЛЕНИЕ БЕЗОПАСНОСТИ КОНФИГУРАЦИИ

## Подавление шторма

**Риски.** Коммутатор получает все фреймы данных в сегменте сети, запоминает исходные MAC-адреса во фреймах данных, создает таблицу MAC-адресов и сохраняет соответствующую взаимосвязь между MAC-адресами и портами. Для полученных фреймов данных, если коммутатор может найти MAC-адрес назначения в таблице MAC-адресов , он переадресует кадры на уровень 2 на основе MAC-адреса назначения, таким образом изолируя коллизию. Если адреса назначения нет в таблице MAC-адресов, коммутатор отправит широковещательную рассылку на все порты, кроме принимающего, что может привести к широковещательному шторму в сети.

**Решение.** В большинстве сценариев использования сетей уровня 2 одноадресный трафик должен быть намного больше широковещательного, что также является необходимым условием для использования коммутаторов в сети. Однако, если широковещательный трафик не ограничен, то при наличии большого количества широковещательного трафика он будет занимать большую полосу пропускания сети, что приведет к снижению производительности сети и даже прерыванию связи. Если генерируемый широковещательный трафик ограничен в коммутаторе, это все равно может гарантировать, что устройство сможет оставить часть полосы пропускания для обычной одноадресной переадресации при резком увеличении широковещательного трафика.

**Пример конфигурации.** Установите значение подавления широковещательной, многоадресной и неизвестной одноадресной рассылки равным 16 kfps.

```
(config)# qos storm broadcast fps 16
(config)# qos storm multicast fps 16
(config)# qos storm unicast fps 16
```

Сохраните конфигурацию:

```
(config)# exit
# copy running-config startup-config
```

## Ограничение сообщений на центральный процессор

**Риски.** В некоторых случаях в сети появляются петли, что в свою очередь вызывает большое количество сообщений протоколов, которые необходимо отправить в центральный процессор для обработки, некоторые из которых являются сообщениями о вредоносных атаках на центральный процессор. Это приводит к высокой загрузке центрального процессора, снижению производительности и влияет на работу обычных служб. Лавинообразный рост сообщений о вредоносных атаках на центральный процессор приводит к перегрузке центрального процессора, что может привести к прерыванию работы системы.

**Решение.** Установите фильтр на поступающие сообщения и ограничивайте их скорость, чтобы избежать перегрузки процессора. Отбрасывайте сообщения, которые не соответствуют правилам, и ограничивайте скорость сообщений протокола, которые соответствуют правилам интерфейса процессора (таким как ограничение скорости порта и ограничение скорости уровня очереди). В то же время ACL может использоваться для точного управления некоторыми потоками специальных протоколов, обеспечивая тем самым обработку процессором обычных сервисов.

**Пример конфигурации.** Соответствующее управление скоростью и потоком данных по умолчанию настроено на интерфейсе ЦП и его 8 очередях с помощью сообщений, передаваемых ЦП, и ручная настройка не требуется; Для сообщений по протоколам шифрования и дешифрования (HTTPS, SSH и т.д.), которые требуют от ЦП выполнения дополнительных вычислений с высокой нагрузкой, управление трафиком может быть выполняется через ACL.

Настройте скорость срабатывания ограничителя скорости от 1 до 500 pps.

```
(config)# access-list rate-limiter 1 pps 500
```

То есть сейчас мы установили ограничение скорости передачи пакетов до 500 в сек.

```
(config)# access-list ace 1 frame-type ipv4-tcp dip 192.168.1.254/32
dport 443 rate-limiter 1
```

Сохраните конфигурацию:

```
(config)# exit
# copy running-config startup-config
```

## Ограничение уровня управления пользователей

**Риски.** Для повышения совместимости и удобства управления пользовательская область и область управления коммутатором по умолчанию не изолированы друг от друга. Пользователи могут входить в систему и управлять устройствами через пользовательсткий интерфейс CLI, что объективно увеличивает вероятность атаки, и злоумышленники могут легко попытаться атаковать уровень управления через сервисный интерфейс.

**Решение.** Администратор может изолировать уровень пользователя и уровень управления, настроив ACL для защиты уровня управления от внешних атак.

**Пример конфигурации.** Изоляция между внутриполосным управлением и пользовательской плоскостью может быть реализована с помощью конфигурации ACL:

- Для VLAN внутриполосного управления: доступ разрешен только к данным управления (HTTPS, SSH, SNMP) путем настройки записей ACL, в то время как к другим данным доступ запрещен.
- Для пользовательской локальной сети VLAN: настройте записи ACL таким образом, чтобы запретить пользователю VLAN доступ к управляющим данным устройства (HTTPS, SSH, SNMP).

например: уровень управления - VLAN 1, IP-адрес для управления устройствами - 192.168.1.254, а уровень пользователя - VLAN 2.

- Выполните следующие настройки по порядку: настройте VLAN 1 для доступа к устройствам по протоколу HTTPS
- Настройте VLAN 1 для доступа к устройствам по протоколу SSH λ Настройте VLAN 1 для доступа к устройствам по протоколу SNMP.
- Настройте другие данные VLAN 1 для доступа к устройствам без доступа.
- Настройте VLAN 2 так, чтобы доступ к устройствам не осуществлялся по протоколу HTTPS.
- Настройте VLAN 2 так, чтобы доступ к устройствам не осуществлялся по протоколу SSH.
- Настройте VLAN 2 так, чтобы доступ к устройствам не осуществлялся по протоколу SNMP.

Сохраните конфигурацию

```
(config)# access-list rate-limiter 1 100kbps 5
(config)# access-list ace 1 next 2 vid 1 frame-type ipv4-tcp dport
443
(config)# access-list ace 2 next 3 vid 1 frame-type ipv4-tcp dport
22
(config)# access-list ace 3 next 4 vid 1 frame-type ipv4-udp dport
161
(config)# access-list ace 4 next 5 vid 1 action deny
```

```
(config)# access-list ace 5 next 6 vid 2 frame-type ipv4-tcp dip
192.168.1.254/32 dport 443 action deny
(config)# access-list ace 6 next 7 vid 2 frame-type ipv4-tcp dip
192.168.1.254/32 dport 22 action deny
(config)# access-list ace 7 vid 2 frame-type ipv4-udp dip
192.168.1.254/32 dport 161 action deny
(config)# exit
# copy running-config startup-config
```

**Обратите внимание!** В соответствии с приоритетом ACL, местоположение записи, запрещающей доступ по VLAN 1, должно располагаться после всех протоколов HTTPS, SSH и SNMP, разрешающих доступ по VLAN1.

## SNMP

**Риски.** Используемые протоколы управления передачей открытого текста, такие как SNMPv1 и SNMPv2, сопряжены с риском утечки информации.

**Решение.** Используйте безопасный протокол управления с шифрованием SNMPv3.

**Безопасная конфигурация.** SNMP - это протокол, используемый для управления сетевыми элементами. В коммутаторе «ПрофиПлюс» в настоящее время поддерживается только версия SNMP v3. SNMPv3 поддерживает механизм безопасности USM (User-based Sequrity Model). Благодаря аутентификации и шифрованию коммуникационных данных SNMP v3 может предотвратить маскировку, подделку и утечку сообщений. По соображениям безопасности рекомендуется настроить аутентифицированных и зашифрованных пользователей версии 3 и использовать шифрование аутентификации версии 3 для управления коммутаторами. Права доступа пользователей ограничены путем привязки к ACL и MIB к пользователям.

**Обратите внимание!** Длина пароля аутентификации должна состоять из 8 символов и более, куда должны входить две или более заглавные буквы, строчные буквы, цифры и специальные символы (# & @ и т.п.).

**Пример конфигурации.**

**Шаг 1** Создайте пользователя V3 user1; Установите режим аутентификации **MD5** и пароль аутентификации `admin123`; Установите режим шифрования **AES** и пароль конфиденциальности `admin345`

```
mydevice(config)# snmp user user2 engine-id 800007e5017f000003 md5
priv aes
```

**Шаг 2** Создайте группу пользователей V3:

```
(config)# snmp security-to-group model v3 name user1 group group1
```

**Шаг 3** Создайте вид узла view 1.

```
(config)# snmp view view1 .1.3.6.1 include
```

**Шаг 4** Настройте представление доступа группы пользователей V3:

```
(config)# snmp access group1 model v3 level priv read view1 write
view1
```

**Шаг 5** Сохраните конфигурацию

```
(config)# end
# copy running-config startup-config
Building configuration...
% Saving 5615 bytes to flash:startup-config
```

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ACL – список правил, запрещающих или разрешающих использование ресурсов сети: доступа к интернету, телефонии, видеосвязи и т.д. (Access Control List).

CLI – интерфейс командной строки (Command Line Interface)

DHCP – протокол прикладного уровня модели TCP/IP, служит для назначения IP-адреса клиенту (dinamic Host Configuration Protocol)

DDMI – цифровой мониторинг интерфейса (Digital Diagnostic Monitoring Interface)

MOTD – баннер входа в систему т.н. «сообщение дня» message of the day

NTP – протокол сетевого времени (Network Time Protocol)

UDP – протокол пользовательских датаграмм (User Datagram Protocol)

UTC – Всемирное координированное время (по Гринвичскому меридиану)

ПАК – программно-аппаратный комплекс

ПК – персональный компьютер

ПО – программное обеспечение

ЦП – центральный процессор

## ДЛЯ ЗАМЕТОК

## ДЛЯ ЗАМЕТОК

## ДЛЯ ЗАМЕТОК

## ДЛЯ ЗАМЕТОК