OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Настройка протокола RADIUS с помощью интерфейса командной строки (CLI)

Прежде чем приступать к эксплуатации изделия,
внимательно прочтите настоящее руководство

www.osnovo.ru

Оглавление

1. CLI Command line interface (Введение)

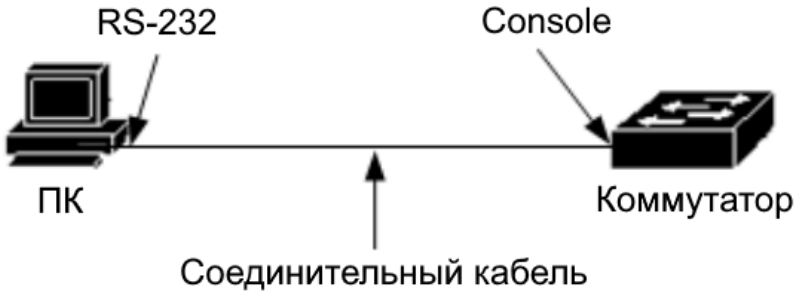
Управление коммутатором через COM-порт (RS-232) с помощью командной строки (CLI) предоставляет пользователю широкие возможности по настройке и управлению режимами работы коммутатора, или в случае, если по каким-либо причинам управление через WEB-интерфейс недоступно.

1.1 Accessing CLI (Доступ к CLI)

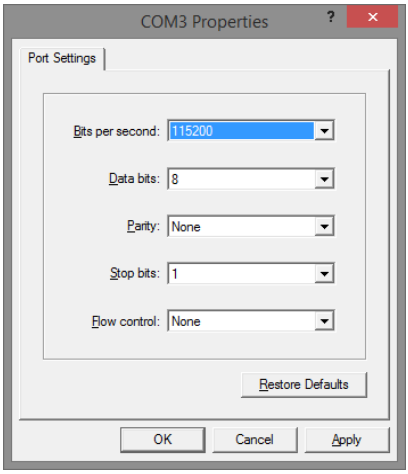
Процедура подготовки к управлению с помощью командной строки описана в руководстве по эксплуатации коммутатором (п.8).

1.1.1 Users access CLI via Console port (Подключение через порт Console)

- Соедините порт Console коммутатора с COM-портом компьютера с помощью кабеля (см. рис. ниже);



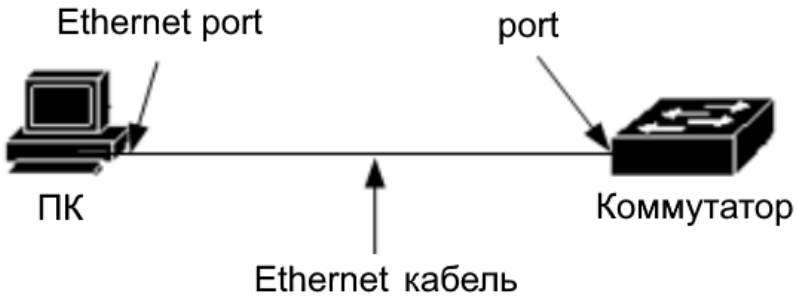
- Запустите HyperTerminal на ПК;
- Задайте имя для нового консольного подключения;
- Выберите COM-порт, к которому подключен коммутатор;
- Настройте COM-порт следующим образом:
  - ✓ Скорость передачи данных (Baud Rate) – 115200;
  - ✓ Биты данных (Data bits) – 8;
  - ✓ Четность (Parity) – нет (no);
  - ✓ Стоп биты (Stop bits) – 1;
  - ✓ Управление потоком (flow control) – нет (no).



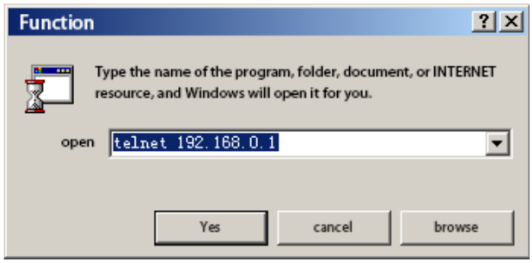
- Включите коммутатор, система предложит войти в интерфейс CLI (управление через командную строку).

1.1.2 Users access CLI via TELNET (Подключение через TELNET)

- Соедините порт коммутатора с Ethernet портом компьютера с помощью кабеля (см. рис. ниже);



- Чтобы получить доступ к CLI коммутатора через Telnet, ПК и коммутатор должны находиться в одной сети. Установите IP адрес сетевого адаптера ПК (например 192.168.0.3) IP адрес коммутатора ***192.168.0.1*** (по умолчанию);
- Если ПК соединен с коммутатором откроется Telnet интерфейс (встроен в командную строку CMD семейства операционных систем Microsoft Windows см. рис. ниже);



- Если пароль не установлен, то Telnet интерфейс предоставит доступ к к CLI коммутатора. В противном случае потребуется аутентификация (по умолчанию: Login: **admin** Password: **admin**).

Внимание !

- IP адрес порта коммутатора зависит от VLAN layer 3 интерфейса. Перед тем как подключиться к коммутатору, должен быть установлен IP адрес VLAN интерфейса. По умолчанию IP адрес vlan1 192.168.0.1. Иной IP адрес VLAN интерфейса может быть установлен через порт console.

- Подключить ПК к коммутатору можно через один из портов непосредственно кабелем Ethernet, или через локальную сеть (если имеется возможность соединения ПК и VLAN коммутатора).

1.2 CLI Mode introduction (CLI режимы)

1.2.1 CLI Role of mode (CLI роли режимов)

Основные функции режимов CLI:

- Упрощение классификации пользователей и предотвращение неавторизованного использования командной строки.
Пользователи разделяются на два уровня: обычный и привилегированный. Обычные пользователи могут только просматривать статусы некоторых операций коммутатора с использованием команд просмотра.
Привилегированные пользователи (в дополнение к перечисленным выше) имеют возможность конфигурировать настройки коммутатора.

- Упрощение управлением коммутатора.

Т.к. коммутатор имеет множество конфигураций, то для пользователей удобно объединять их в различные режимы для использования. Сходные по функциональному назначению команды объединены в режимы. Например связанные с управлением VLAN команды и команды управления интерфейсом объединены в соответствующие режимы.

1.2.2 Identification of CLI mode (Идентификация CLI режимов)

При использовании командной строки пользователь может узнать текущий режим CLI, который указан в CLI prompt. CLI prompt состоит из двух частей, одна идентифицирует хост, а другая идентифицирует режим.

CLI prompt хост использует имя хоста системы. Имя хоста системы (по умолчанию *switch*) может быть изменено. Таким образом, CLI prompt начинает работу с именем хоста «switch».

Изменения части CLI prompt, касающейся режима CLI не предусмотрены. Каждый режим привязан к соответствующей данному режиму строке. Существуют фиксированные строки и изменяемые строки. Например строка режима VLAN конфигурации фиксированная, а строка режима интерфейса конфигурации изменяемая.

Пример:

- CLI prompt switch # определяет привилегированный режим (switch определяет хост, # определяет режим).
- CLI prompt switch (config-ge1 / 1) # определяет режим интерфейса конфигурации и конфигурирует GE1 / 1 порт (switch определяет хост, (config-ge1 / 1), # определяет режим).
- CLI prompt switch (config-vlan2) # определяет режим интерфейса конфигурации vlan2 (switch определяет хост, (config-vlan2), # определяет режим).

1.2.3 Classification of CLI modes (Классификация CLI режимов)

Режимы CLI разделены на четыре группы: обычный (normal mode), привилегированный (privileged mode), глобальной конфигурации (global configuration mode) и конфигурационный (configuration sub mode, включает несколько cli подрежимов).

Простым пользователям доступен только обычный режим, привилегированным пользователям доступны все cli режимы.

При подключении через console и telnet сначала доступен только нормальный режим. После ввода соответствующей команды возможен переход в привилегированный режим при условии успешной аутентификации, *(простой пользователь не имеет возможности перехода в другие режимы*). После входа в привилегированный режим возможно перейти в режим глобальной конфигурации. Для перехода из режима глобальной конфигурации в другие подрежимы (sub mode) следует ввести соответствующие команды.

Таблица основных cli режимов коммутатора.

Режим	**Описание**	**Prompt**	**Команда входа**	**Команда выхода**
Normal mode	Просмотр текущей информации о коммутаторе.	Switch>	Режим доступен автоматически при первичном входе.	exit или quit для выхода из telnet terminal.
Privileged mode	Просмотр текущей информации о коммутаторе. Команды debugging, version upgrade, configuration maintenance.	Switch#	**enable** в режиме normal mode.	**disable** возврат в normal mode. exit или quit для выхода из telnet terminal.
whole situation mode of configuration	Основные команды недоступные в режимах configuration sub mode, такие как configuration static routing.	Switch(config)#	Перейти в режим команд из privileged mode.	**exit**, **quit**, или **end** возврат в privileged mode.
Interface configuration mode	Команды для конфигурации интерфейса портов и VLAN.	Port: Switch(config-ge1/1)# VLAN port: Switch(config-vlan1)#	< **if name** > в режиме global configuration mode.	**exit** или **quit** для выхода из global configuration mode. **end** для выхода из privileged mode.
VLAN mode of	Команды для конфигурации VLAN, такие как	Switch(config-vlan)#	vlan database order	**exit** или **quit** для выхода из global configuration mode.

configuration	создать и удалить VLAN.		в режиме global configuration mode.	**end** для выхода из privileged mode.
MSTP configuration mode	Команды для конфигурации MSTP, такие как создать и удалить MSTP интерфейсы.	Switch(config-mst)#	Войти в spaning tree MST в режиме global configuration mode.	**exit** или **quit** для выхода из global configuration mode. **end** для выхода из privileged mode.
Terminal configuration mode	Команды для конфигурации console и telnet, такие как timeout интерфейса.	Switch(config-line)#	Войти в строку команд vty в режиме global configuration mode.	**exit** или **quit** для выхода из global configuration mode. **end** для выхода из privileged mode.

1.3 Introduction to command syntax (Синтаксис команд)

1.3.1 Command composition (Композиция команд)

CLI команды состоят из ключевых слов объединенных с параметрами. Сначала располагается ключевое слово, далее следующее ключевое слово или параметр. Ключевые слова и параметры могут чередоваться. Команда может содержать только ключевое слово (без параметра).

Пример:

- Команда < write > состоит только из ключевого слова;
- Команда < show version > состоит из двух ключевых слов;
- Команда VLAN < VLAN ID > состоит из ключевого слова и параметра;
- Команда instance < instance ID > VLAN < VLAN ID > состоит из двух ключевых слов и двух параметров, которые чередуются.

1.3.2 Parameter type (Типы параметров)

Параметры CLI команд разделяются на два типа: обязательные и опциональные. При вводе команды обязательные параметры должны быть тоже введены, ввод опциональных параметров не является необходимым.

Пример:

- Для команды VLAN < VLAN ID > параметр является обязательным;
- Для команды < show interface [if name] > параметр является опциональным.

1.3.3 Command syntax rules (Правила синтаксиса)

При описании команд в тексте данной инструкции используются следующие правила:

1) Ключевые слова описываются словами, совпадающими по смыслу.
2) Параметры заключаются в символы < >
   Пример: VLAN < VLAN ID >
3) Опциональный параметр заключается в прямоугольные скобки [ ]
   Пример: VLAN [< VLAN ID >] в этом же случае символы < > могут быть опущены: VLAN [VLAN ID] соответственно параметр VLAN ID может не вводиться. Если параметр обязательный, то в скобки он не заключается.
4) Если необходимо выбрать одно из нескольких ключевых слов или параметров, то для выделения используются фигурные скобки { }. Для разделения ключевых слов и параметров используется символ | с обязательными пробелами до и после |
   Пример: spanning-tree mst link-type {point-to-point | shared}
   Выбор одного из параметров no arp {<ip-address> | <ip-prefix>}
   Ключевые слова и параметры Show spanning-tree mst {none | instance <0-15>}ng
5) Если необходимо выбрать одно ключевое слово или параметр, то для выделения используются прямоугольные скобки [ ]. Для разделения ключевых слов и параметров используется символ | с обязательными пробелами до и после |

Пример: debug ip tcp [recv | send]
Ключевые слова recv и send могут быть выбраны или не выбраны
show ip route [<ip-address> | <ip-prefix>] show interface [<if-name> | switchport]

6) Если необходимо выбрать группу из нескольких ключевых слов или параметров, следует добавить символ «*» после группы (Group) ключевых слов или параметров.
Пример: ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*
-j <count> <ip-address>* --- Несколько IP адресов могут быть добавлены последовательно
-k <count> <ip-address>* --- Несколько IP адресов могут быть добавлены последовательно
7) Если параметр представлен одним и более словами, следует разделить слова символом «-» и использовать строчные буквы
Пример (правильно): <vlan-id>, <if-name>, <router-id>, <count>
Пример (не правильно): <1-255>, <A.B.C.D>, <WORD>, <IFNAME>

1.3.4 Command abbreviation (Сокращения)

При вводе команд в CLI интерфейс, допустимо использование сокращенной записи ключевых слов. CLI поддерживает использование префиксов, соответствующих ключевым словам. В зависимости от уникальности префикса, CLI определяет соответствующую ключевому слову команду. Эта функция создает дополнительное удобство для пользователей CLI, т.к. сокращает число вводимых символов необходимых для завершения команды.

Пример: команда show version ---- sh ver

1.3.5 Grammar help (Помощь)

Интерфейс CLI поддерживает функцию помощи (по синтаксису) для команд и параметров на каждом уровне.

1) При вводе в cli символа ? будет показано первое ключевое слово и описание всех связанных с ним команд.
   Пример: switch (config) #?
2) Введите первую часть команды, далее пробел и ?. Будут выведены все ключевые слова или параметры с описаниями.
   Пример: switch #show?
3) Введите часть ключевого слова и символ ? Будут выведены все ключевые слова с описаниями относящиеся к введенному префиксу.
   Пример: switch #show ver?
4) Введите первую часть команды, далее пробел и tab. Будут выведены все ключевые слова для следующего уровня (кроме параметров, в этом случае информация не выводится).
5) Введите часть ключевого слова, далее tab. Если только одно ключевое слово соответствует префиксу, то он будет дополнен. Если префиксу соответствует несколько ключевых слов, то они все будут выведены.

1.3.6 Command line error message (Сообщения об ошибках)

Сообщение об ошибке появляется при вводе команд с неверным синтаксисом. Типовые сообщения об ошибках приведены в таблице ниже:

Таблица типовых сообщений об ошибках.

Сообщение	Причина ошибки
Invalid input or Unrecognized command	Не найдено ключевое слово. Введен некорректный параметр. Введено слишком много ключевых слов или параметров.
Incomplete command	Неполная команда, не введено ключевое слово или параметр.
Ambiguous command	Неполная команда, несколько ключевых слов соответствует префиксу.

2. System management (Конфигурация управление системой)

Перед переходом к изучению дальнейших возможностей по конфигурированию коммутатора следует провести настройку некоторых основных параметров управления системой. В этом разделе описываются основные настройки системы управления коммутатором:

- System security configuration (Конфигурация системы безопасности)
- System maintenance and commissioning (Обслуживание и эксплуатация)
- Monitoring system (Мониторинг системы)
- Profile management (Управление профилем)

2.1 System security (Конфигурация системы безопасности)

Для предотвращения допуска неавторизованных лиц к управлению коммутатором предусмотрен ряд настроек которые включают следующие:

- Multi user management control (Управление многопользовательским режимом)
- Enable Password control (Защита паролем)
- TELNET service control (Управление TELNET)
- SNMP service control (Управление SNMP)
- HTTP service control (Управление HTTP)

2.1.1 Multi user management control (Многопользовательский режим)

Многопользовательский режим повышает безопасность системы и обеспечивает возможность управления и обслуживания коммутатора несколькими пользователями одновременно. Многопользовательский режим обеспечивает безопасность путем индивидуальной аутентификации пользователей (присвоение каждому пользователю своего имени и пароля для входа в систему). При настройке

многопользовательского режима устанавливаются определенные права для каждого пользователя.

Многопользовательский режим предусматривает два уровня прав для пользователей: обычный и привилегированный. Обычные пользователи могут использовать только обычный режим командной строки CLI, команды display для просмотра информации о коммутаторе. Привилегированные пользователи могут использовать все режимы командной строки CLI, все команды управления коммутатором.

Многопользовательский режим применяется только для управления через telnet и недоступен для управления через console. При управлении через console для входа в систему не требуется аутентификация, пользователь может непосредственно войти в командную строку CLI. При входе в систему через telnet требуется ввести имя пользователя и пароль. Доступ к командной строке CLI возможен только после успешной аутентификации.

По умолчанию *имя пользователя и пароль* **admin**. Пользователь admin является администратором (привилегированным пользователем), его настройки не могут быть изменены на обычного пользователя, и он не может быть удален.

Таблица команд многопользовательского режима.

Команда	**Описание**	**CLI ржим**
username <user-name> password <key> {normal | privilege}	Добавление пользователя, изменение пароля, прав пользователя (если пользователь уже существует). 1й параметр - user name, 2й параметр - пароль, опционально - права пользователя (normal – обычный, privilege – привилегированный).	Global configuration mode
no username [user-name]	Удалить пользователя.	Global configuration mode

show running-config	Просмотр текущей конфигурации системы, конфигурации многопользовательского режима.	Privileged mode

2.1.2 Enable password control (Управление аутентификацией)

Управление аутентификацией применяется для перевода управления коммутатора из обычного режима в привилегированный режим. Перед включением аутентификации пользователю доступна для просмотра только информация о коммутаторе. После включения и прохождения аутентификации пользователь получает доступ к настройкам коммутатора.

Возможность включения аутентификации не имеет привязки к конкретному пользователю. Любой пользователь, который входит через console или telnet в привилегированный режим управления должен ввести корректный пароль. После успешной аутентификации пользователь также может оставаться в обычном режиме управления.

При вводе команды в обычном режиме пользователю необходимо ввести пароль. После успешной аутентификации система перейдет в привилегированный режим управления. В противном случае система останется в обычном режиме управления.

При включенной аутентификации система по умолчанию не будет требовать ввод пароля для входа в обычный режим.

Таблица команд управления режимом аутентификаци.

Команда	**Описание**	**CLI режим**
enable password <key>	Установка пароля для входа в систему.	Global configuration mode
no enable password	Удаление пароля, «пустой» пароль.	Global configuration mode
show running-config	Просмотр текущей конфигурации, в т.ч. пароля.	Global configuration mode
enable	Включение режима аутентификации. Переход	Global configuration

	в привилегированный режим.	mode

Для обеспечения безопасности системы администратору следует включить режим аутентификации и установить пароль.

2.1.3 TELNET service control (Управление TELNET сервисом)

В случаях когда отсутствует необходимость дистанционного управления коммутатором и управление осуществляется локально через console, для обеспечения безопасности системы и предотвращения неавторизованного дистанционного управления, администратор может отключить управление по telnet (включено по умолчанию). Команды приведены в таблице ниже:

Таблица команд управления telnet сервисом

Команда	Описание	CLI ржим
security-manage telnet enable	Включить telnet	Global configuration mode
security-manage telnet disable	Отключить telnet	Global configuration mode
security-manage telnet number <1-100>	Диапазон параметра от1 до 100, по умолчанию 5.	Global configuration mode
security-manage telnet access-group <1-99> (Note: subject to the actual product)	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage telnet access-group	Отключить управление IP адресом.	Global configuration mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

2.1.4 SNMP Service control (Управление SNMP сервисом)

Управление сервисом SNMP и IP адресом доступа к коммутатору через ACL может быть включено или отключено (on / off).
Команды приведены в таблице ниже:
Таблица команд управления SNMP сервисом

Команда	Описание	CLI ржим
security-manage snmp enable	Включить SNMP	Global configuration mode
security-manage snmp disable	Отключить SNMP	Global configuration mode
security-manage snmp access-group <1-99> (Note: subject to the actual product)	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage snmp access-group	Отключить управление IP адресом.	Global configuration mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

2.1.5 HTTP Service control (Управление HTTP сервисом)

Управление сервисом HTTP и IP адресом доступа к коммутатору через ACL может быть включено или отключено (on / off).
Команды приведены в таблице ниже:

Таблица команд управления HTTP сервисом:

Команда	Описание	CLI ржим
security-manage http enable	Включить HTTP	Global configuration mode

security-manage http disable	Отключить HTTP	Global configuration mode
security-manage http access-group <1-99> (Note: subject to the actual product)	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage http access-group	Отключить управление IP адресом.	Global configuration mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

2.1.6 HTTPS Service control (Управление HTTPS сервисом)

Управление сервисом HTTPS и IP адресом доступа к коммутатору через ACL может быть включено или отключено (on / off). Команды приведены в таблице ниже:

Таблица команд управления HTTPS сервисом

Команда	Описание	CLI ржим
security-manage https enable	Включить HTTPS	Global configuration mode
security-manage https disable	Отключить HTTP	Global configuration mode
security-manage https access-group <1-99> (Note: subject to the actual product)	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage https access-group	Отключить управление IP адресом.	Global configuration mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

2.1.7 SSH Service control (Управление SSH сервисом)

Многие программы сетевого сервиса такие как FTP, pop и Telnet не являются безопасными т.к. передают данные и пароли открытым текстом, что делает возможным их перехват злоумышленниками. Методы обеспечения безопасности этих сервисов имеют ряд уязвимостей для атак типа «middleman» (ретрансляция данных через промежуточный сервер). При использовании сервиса SSH производится шифрование передаваемых данных, что делает атаки типа «middleman» не эффективными, кроме того предотвращается DNS spoofing и IP spoofing. Еще одним преимуществом сервиса SSH является сжатие передаваемых данных и повышение скорости передачи.

Сервис SSH не заменяет Telnet, но обеспечивает безопасный канал передачи данных для FTP, pop и PPP. Команды приведены в таблице ниже:

Таблица команд управления SSH сервисом

Команда	Описание	CLI ржим
security-manage ssh enable	Включить ssh	Global configuration mode
security-manage ssh disable	Отключить ssh	Global configuration mode
security-manage ssh access-group <1-99>	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage ssh access-group	Отключить управление IP адресом.	Global configuration mode
ip sshd auth-retries <times>	Установить количество попыток аутентификации.	Global configuration mode
ip sshd silence-period <seconds>	Установить время ожидания после исчерпания всех попыток аутентификации.	Global configuration mode
show ip sshd	Просмотр конфигурации настроек sshd	Privileged mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

2.2 System maintenance and commissioning (Обслуживание системы)

Подготовка к эксплуатации и дальнейшее обслуживание коммутатора включает в себя следующие пункты:

- Configure the system clock (Настройка системных часов)
- Configure terminal timeout attribute (Настройка времени бездействия)
- System reset (Сброс системы)
- View system information (Просмотр системной информации)
- Network connectivity debugging (Устранение сетевых неполадок)
- Traceroute debugging (Устранение неполадок маршрутизации)

2.2.1 Configure the system clock (Настройка системных часов)

В коммутаторе предусмотрены системные часы, которые синхронизированы с реальным временем. С помощью команд можно устанавливать и просматривать текущее время. Для удобства эксплуатации коммутатора системные часы обеспечены встроенным питанием, которое делает не нужной установку времени после длительного отключения коммутатора от энергоснабжения. После первого включения коммутатора следует проверить точность установки системных часов и при необходимости откорректировать.

Таблица команд управления системными часами

Команда	Описание	CLI ржим
set date-time <year> <month> <day> <hour> <minute> <second>	Установка текущего времени и даты в последовательности: год, месяц, день, час, минуты, секунды (вводятся значения параметров).	Privileged mode
show date-time	Просмотр текущей даты и времени системных часов.	Normal mode. privileged mode

2.2.2 Configure terminal timeout attribute (Настройка времени бездействия)

Для обеспечения безопасности в коммутаторе предусмотрена функция автоматического выхода из режима управления при бездействии, по истечении определенного интервала времени, который может быть изменен пользователем.

Процессы выхода из режима управления через console и telnet различаются. При управлении через console по истечении временного интервала, командная строка CLI переходит в обычный режим. При управлении через telnet по истечении временного интервала, соединение telnet прерывается, коммутатор выходит из режима управления. По умолчанию временной интервал бездействия составляет 10 мин, пользователь может изменить его или отключить эту функцию.

Таблица команд настройки времени бездействия

Команда	Описание	CLI ржим
exec-timeout <minutes> [seconds]	Установка времени бездействия. При выборе значения параметра 0, функция будет отключена.	Global configuration mode
no exec-timeout	Установка времени бездействия 10 мин (заводская установка, по умолчаню).	Global configuration mode
show running-config	Просмотр текущей конфигурации системы, в т.ч. установленного времени бездействия.	Privileged mode

2.2.3 System reset (Сброс системы)

Таблица команды сброса системы

Команда	Описание	CLI ржим
reset	Сброс системы	Privileged mode

2.3 Profile management (Управление профилем)

Существует два типа конфигурации: текущая (current configuration) и стартовая (initial configuration). Текущая конфигурация создается с учетом требований эксплуатации коммутатора и хранится в памяти системы. Стартовая конфигурация используется при первичном включении коммутатора и хранится на внутренней flash памяти коммутатора (configuration file). При использовании соответствующих команд стартовая конфигурация может быть изменена. Команда Save (сохранить) позволяет сохранить внесенные изменения и при последующем запуске будет загружена уже измененная (текущая) конфигурация.

Файлы конфигурации имеют тот же формат что и текст командной строки (прост и интуитивно понятен). Формат файла конфигурации имеет следующий вид:

- Файл состоит из текстовых команд.
- Может быть сохранена только измененная конфигурация, неизмененная конфигурация не сохраняется
- Формат команд аналогичен применяемому в командной строке. Команды объединены в сегменты, сегменты разделяются знаком "!". В режиме global configuration команды со сходными значениями объединены в секции, разделяются знаком "!".
- В режиме configuration sub mode, перед командой должен стоять пробел, в режиме global configuration mode пробел перед командой должен отсутствовать.
- Файл конфигурации заканчивается командой "end".

Команды управления файлом конфигурации включают следующие:

- View configuration information (Просмотр конфигурации)
- Save configuration (Сохранение конфигурации)
- Delete configuration profile (Удаление конфигурации)
- Download from configuration file (Загрузка конфигурации)

2.3.1 View configuration information (Просмотр конфигурации)

Пользователь имеет возможность просмотра текущей (current configuration) и стартовой (initial configuration) конфигурации системы. Файл конфигурации хранится на внутренней flash памяти коммутатора, если файл конфигурации отсутствует, то при включении коммутатора загружаются заводские настройки (по умолчанию). В этом случае при вводе команды для просмотра стартовой конфигурации, система выдаст сообщение об отсутствии файла.

Таблица команд просмотра конфигурации

Команда	Описание	CLI ржим
show running-config	Просмотр текущей конфигурации системы.	Privileged mode
show startup-config	Просмотр стартовой конфигурации системы.	Privileged mode

2.3.2 Save configuration (Сохранение конфигурации)

После внесения изменений в текущую конфигурацию системы пользователь имеет возможность сохранить эти изменения для того чтобы при последующем включении коммутатора загрузилась последняя сохраненная версия конфигурации. В противном случае при включении коммутатора будет загружена конфигурация без учета внесенных изменений.

Таблица команд сохранения конфигурации

Команда	Описание	CLI ржим
write	Сохранить текущую конфигурацию	Privileged mode

Внимание *!* Если пользователь не сохранит последние внесенные в текущую конфигурацию изменения, то при выключении коммутатора изменения настроек будут потеряны. При последующем включении коммутатора будет загружена последняя сохраненная конфигурация.

2.3.3 Delete configuration file (Удаление файла конфигурации)

Если пользователю необходимо чтобы при включении были загружены заводские настройки системы (настройки по умолчанию), то следует удалить файл конфигурации. Удаление файла конфигурации не приводит к изменениям в текущей конфигурации до выключения коммутатора. Для возвращения к заводским настройкам после удаления файла следует перезагрузить коммутатор.

Таблица команд удаления файла конфигурации

Команда	Описание	CLI ржим
delete startup-config	Удаление файла конфигурации	Privileged mode

Внимание *!*
Будьте внимательны, удаление файла конфигурации приведет к потере текущей конфигурации после перезагрузки коммутатора.

2.3.4 Download configuration file (Загрузка файла конфигурации)

В случае повреждения или удаления файла конфигурации или необходимости вернуться к заводской конфигурации коммутатора предусмотрена возможность загрузки заводского файла с ПК в память коммутатора.

Загрузка заводского файла конфигурации не приводит к изменениям в текущей конфигурации до выключения коммутатора. Для возвращения к заводским настройкам после загрузки файла следует перезагрузить коммутатор.

Загрузка и скачивание файла конфигурации также доступна через web, подробно процедура описана в полной инструкции по эксплуатации коммутатора.

Таблица команд загрузки файла конфигурации

Команда	Описание	CLI ржим
upload configure <ip-address> <file-name>	Скачивание файла конфигурации на ПК.	Privileged mode

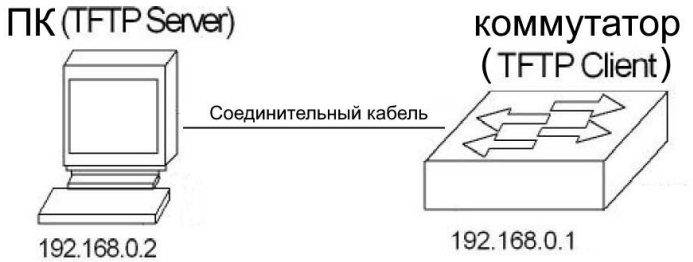
	1й параметр IP адрес ПК 2й параметр имя файла.	
download configure <ip-address> <file-name>	Загрузка файла конфигурации в коммутатор. 1й параметр IP адрес ПК 2й параметр имя файла.	Privileged mode

Загрузите файл конфигурации в коммутатор, используйте протокол TFTP. Запустите TFTP client на коммутаторе и TFTP на ПК. Далее действуйте по пунктам ниже:

Шаг 1: Сформируйте сетевое окружение.
Шаг 2: Сохраните файл конфигурации TFTP software на ПК.
Шаг 3: Сохраните файл конфигурации на коммутаторе.
Шаг 4: Запустите команду configuration file upload на коммутаторе для скачивания файла конфигурации на ПК.
Шаг 5: При необходимости запустите команду configuration file download command на коммутаторе для загрузки файла конфигурации в коммутатор.
Шаг 6: Перезагрузите коммутатор для обновления конфигурации.

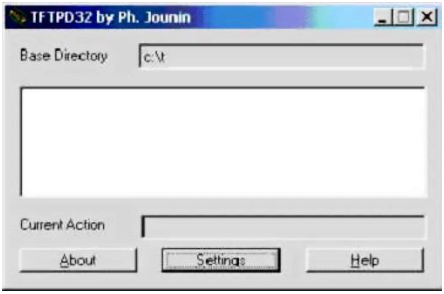
Пример: Загрузка и скачивание файла конфигурации на коммутатор с VLAN и IP адресом.

Шаг 1: Сетевое окружение.

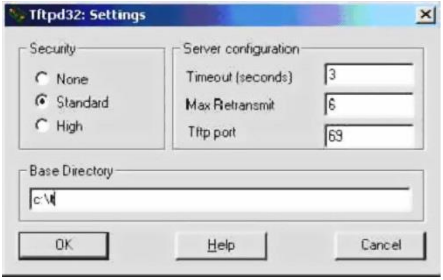


Соединить ПК с конфигурационным портом коммутатора сетевым кабелем. Установить TFTP server на ПК и установить IP адрес сетевого адаптера (например 192 168.0.2) в одной подсети с IP адресом коммутатора (по умолчанию 192.168.0.1), проверить наличие соединения.

Шаг 2: Запустите TFTP сервер на ПК и сконфигурируйте его параметры.



Откройте директорию с файлом конфигурации, далее нажмите [settings].



Введите путь в base directory и нажмите [OK] для завершения.

Шаг 3: Введите команду write на коммутаторе для Сохранения файла текущей конфигурации.

Шаг 4: Запустите команду configuration file upload на коммутаторе для скачивания файла конфигурации на ПК (192 168.0.2).

Шаг 5: Для загрузки файла конфигурации с ПК (192 168.0.2) в коммутатор запустите команду configuration file download command на коммутаторе.

Шаг 6: Для обновления конфигурации вводом команды switch#reset перезагрузите коммутатор.

3. AAA Configure (Конфигурация AAA)

В данной главе описывается конфигурация протоколов 802.1x и RADIUS коммутатора для предотвращения неавторизованного подключения к сети. Глава содержит следующие разделы:

- 802.1x Introduction (введение)
- RADIUS Introduction (введение)
- Configure 802.1x (конфигурация)
- Configure RADIUS (конфигурация)

AAA обозначает аутентификацию (authentication), авторизацию (authorization) и учет (accounting). Протокол обеспечивает три функции безопасности: authentication, authorization и billing. Конфигурация AAA является видом управления сетевой безопасности. В данном случае сетевая безопасность сводится к контролю доступа (пользователи имеющие доступ к сети, сервисы доступные пользователям, учет пользователей сети).

- Authentication: получение доступа пользователем.
- Authorization: сервисы доступные пользователям.
- Accounting: учет использования сетевых ресурсов пользователем.

Обычно используются все возможности протокола AAA, включая 802.1x клиентов, оборудование поддерживающее authentication и hyperboss. Клиенты 802.1x устанавливаются на ПК для выхода в интернет. Для подключения к сети пользователи должны использовать клиента 802.1x для аутентификации. Пользователь получает запрос от клиента и передает имя пользователя (user name) и пароль (password) системе system hyperboss для аутентификации. Коммутатор не проводит аутентификацию. Hyperboss получает запрос от коммутатора, предоставляет актуальные данные и пропускает пользователей прошедших аутентификацию.

Протокол 802.1x используется для коммуникации между 802.1x клиентом и коммутатором, протокол radius используется для коммуникации между коммутатором и hyperboss.

3.1 802.1x introduction (Введение)

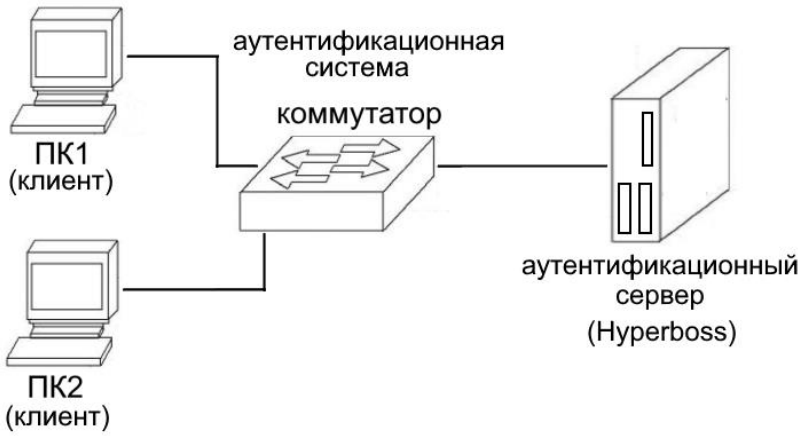
Протокол аутентификации 802.1x основан на управлении доступом порта. Порт может быть логическим, физическим с использованием MAC адреса или VLAN ID. Сетевые коммутаторы реализуют протокол 802.1x основанный на MAC адресе.

Протокол 802.1x является протоколом второго уровня layer-2. Коммутатор и ПК пользователя должны находиться в одной подсети,

пакет протокола не может выходить за пределы сегмента сети. Аутентификация 802.1x воспринимает сервер клиента и должна быть сервером для всех пользователей. До аутентификации пользователя, только аутентификационные данные могут пройти через порт коммутатора. После успешной аутентификации поток данных сможет пройти через порт коммутатора, т.е. для доступа к сети пользователь должен пройти аутентификацию.

3.1.1 802.1x Equipment composition (Подключение оборудования)

802.1x оборудование делится на три группы: клиент (supplicant system), аутентификационная система (authenticator system) и аутентификационный сервер (authentication server). Схема подключения приведена ниже.



Клиент обращается к оборудованию с запросом на доступ к сети (обычно это ПК пользователя). 802.1x клиентское ПО (client software), которое отвечает за клиентскую часть протокола 802.1x должно быть установлено на ПК пользователя. Клиент инициирует запрос на 802.1x аутентификацию к серверу (authentication server) для подтверждения имени и пароля (user name, password). После успешной аутентификации пользователь получает доступ к сети.

Аутентификационная система относится к аутентификационному

оборудованию (коммутатору). Аутентификационная система управляет доступом пользователя к сети путем изменения статуса логического порта пользователя (на основе MAC адреса). Если логический порт пользователя не авторизован, пользователь не может подключиться к сети, если логический порт пользователя авторизован, то пользователь получает доступ к сети.

Аутентификационная система соединяет клиента и аутентификационный сервер (authentication server). Аутентификационная система запрашивает идентификационную информацию пользователя, передает её на аутентификационный сервер и далее результат аутентификации от сервера к клиенту. Аутентификационная система требует реализации протокола 802.1x со стороны сервера и пользователя, а протокола radius со стороны клиента и аутентификационного сервера. Протокол radius клиента аутентификационной системы инкапсулирует информацию EAP отправленную клиентом 802.1x и отправляет её аутентификационному серверу. Информация EAP распаковывается из пакета протокола radius отправленного аутентификационным сервером и переданного клиенту 802.1x через 802.1x сервер.

Аутентификационный сервер это оборудование, которое проводит аутентификацию пользователя. Аутентификационный сервер получает идентификационную информацию пользователя от аутификационной системы и верифицирует её. При успешной аутентификации, аутентификационный сервер авторизует аутификационную систему и позволяет пользователю подключиться к сети. Если аутентификация не состоялась, аутификационный сервер сообщает это аутификационной системе и пользователь не получает доступа к сети. Аутентификационный сервер и аутификационная система взаимодействуют по расширенному EAP RADIUS протоколу.

3.1.2 Protocol package (Пакеты протокола)

Поток аутентификационных данных передаваемый протоколом 802.1x по сети имеет кадровый формат eapol (EAP over LAN). Вся идентификационная информация пользователя (включая user name и password) инкапсулируется в EAP (extended authentication protocol), и EAP инкапсулируется в eapol кадр. Имя пользователя представлено в EAP в виде текста, тогда как пароль представлен в зашифрованном

формате MD5.

Формат кадра Eapol представлен таблице ниже. Тип PAE Ethernet является типом Ethernet протокола с числом eapol и значением 0x888e. Версия протокола это версия eapol со значением 1. Тип пакета относится к формату кадра eapol. Длина пакета это длина содержания кадра eapol, содержание пакета относится к содержанию кадра eapol.

Формат кадра EAPOL:

	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

Коммутатор использует три кадра eapol протокола:

- Eapol start: значение типа пакета 1. Аутентификация инициализирует кадр. Когда пользователь запрашивает аутентификацию, формируется кадр и отправляется от клиента коммутатору.
- Eapol logoff: значение типа пакета 2. Кадр запроса на выход отправляется для уведомления коммутатора о том, что клиент не нуждается в подключении к сети.
- EAP packet: значение типа пакета 0. Информационный кадр аутентификации используется для передачи аутентификационной информации.

Формат пакета EAP представлен таблице ниже. Код относится к типу EAP пакета, включая запрос, ответ, успех и неудача. Идентификатор определяет соответствие ответа и запроса. Длина соответствует длине пакета EAP, включая заголовок. Дата соответствует данным EAP пакета.

EAP пакеты бывают четырех типов:

- EAP request: Значение кода 1, EAP пакет запроса отправляется коммутатором клиенту для запроса user name и password.
- EAP response: Значение кода 2, EAP пакет ответа отправляется

клиентом коммутатору, содержит user name и password.

- EAP success: Значение кода 3, EAP пакет success отправляется коммутатором клиенту, информирует об успешной аутентификации пользователя.

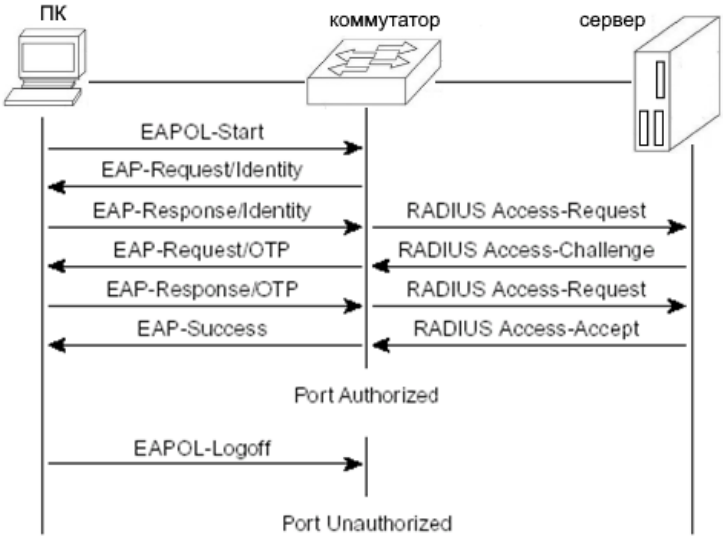
- EAP failure: Значение кода 4. EAP пакет failure отправляется коммутатором клиенту, информирует о неудачной аутентификации пользователя.

Формат пакета EAP:

	Octet Number
Code	1
Identifier	2
Length	3-4
Data	5-N

3.1.3 Protocol flow interaction (Взаимодействие протоколов)

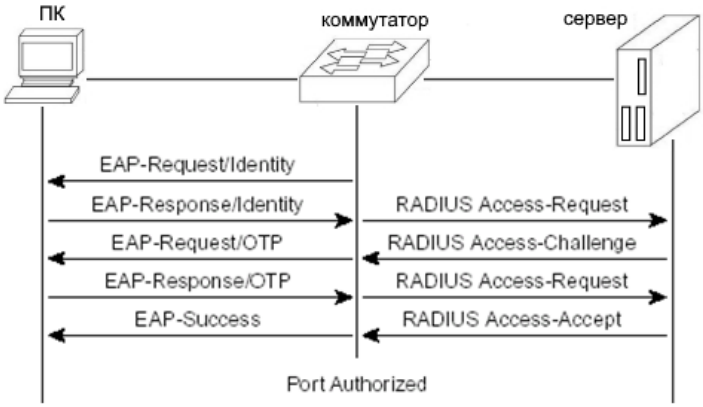
Когда на коммутаторе включен протокол 802.1x а порт находится в статусе auto, все пользователи, подключенные к порту должны пройти процедуру аутентификации перед получением доступа в сеть. Взаимодействие протоколов показано на рисунке ниже.



Когда пользователю необходимо подключиться к сети, клиент отправляет коммутатору eapol start для запроса аутентификации. После получения ответа, коммутатор отправляет EAP запрос пользователю о user name, клиент возвращает EAP ответ. Коммутатор извлекает информацию EAP и инкапсулирует её в пакет radius и отправляет его аутентификационному серверу, который запрашивает пароль пользователя. Коммутатор отправляет запрос пароля пользователя EAP клиенту, клиент возвращает EAP ответ. Коммутатор инкапсулирует информацию EAP в пакет radius и отправляет аутентификационному серверу, который аутентифицирует пользователя согласно имени и паролю. Если коммутатор получает успешный статус EAP аутентификации, то клиент будет уведомлен об этом. Получение клиентом EAP success, означает успешную аутентификацию и возможность доступа к сети.

По окончании сеанса подключения к сети, клиент отправляет уведомление eapol logoff коммутатору, коммутатор переводит логический порт в неавторизованный статус. Одновременно с этим пользователь отключается от сети.

Для предотвращения ненормального отключения клиента, коммутатор задействует процедуру повторной аутентификации. На коммутаторе может быть установлен временной интервал повторной аутентификации. По истечении этого времени, коммутатор инициализирует повторную аутентификацию. При успешной аутентификации, пользователь может продолжить использоваться сетью. Взаимодействие протоколов показано на рисунке ниже.



3.1.4 802.1x port status (Статусы 802.1x порта)

Физический порт коммутатора может иметь четыре статуса: n/a state (неопределенный), auto state (авто), force authorized state (принудительно авторизованный) и force unauthorized (принудительно неавторизованный). Если на коммутаторе отключен протокол 802.1x, все порты находятся в неопределенном статусе (n/a). Перед тем как установить порт коммутатора в статус авто (auto state), авторизованный (force authorized) или неавторизованный (force unauthorized), следует включить 802.1x протокол.

Когда порт коммутатора находится в статусе n/a, все пользователи подключенные к порту могут получить доступ в сеть без аутентификации. Полученные от порта пакеты протокола 802.1x коммутатор отбрасывает.

Когда порт коммутатора находится в статусе force authorized, все пользователи подключенные к порту могут получить доступ в сеть без аутентификации. Когда коммутатор получает от порта пакеты eapol start, коммутатор возвращает обратно EAP success пакеты. Полученные от порта пакеты протокола 802.1x коммутатор отбрасывает.

Когда порт коммутатора находится в статусе force unauthorized, все пользователи подключенные к порту не могут получить доступ в сеть, аутентификационные запросы не проходят. Полученные от порта пакеты протокола 802.1x коммутатор отбрасывает.

Когда порт коммутатора находится в статусе auto, все пользователи подключенные к порту должны пройти аутентификацию для получения доступа в сеть. Работа протокола 802.1x показана на рисунках выше. Для прохождения аутентификации пользователем порт коммутатора должен быть переведен в статус auto.

Когда порт коммутатора находится в статусе auto, одновременно включается функция anti ARP Spoofing. Функция anti ARP Spoofing может контролировать пакеты данных источника MAC, источника IP из группы IP пакетов с информацией предоставленной клиентом в процессе аутентификации, и пакетами данных отправителя IP и MAC из ARP пакетов с информацией предоставленной клиентом в процессе аутентификации и пересланных портом, в случае несовпадения пакеты будут сброшены. Для настройки этой функции, клиент должен иметь статический IP адрес. Если IP адрес назначается динамически

протоколом DHCP, то для использования этой функции следует активировать DHCP snooping protocol. Для получения более подробной информации, следует обратиться к разделу IP MAC binding configuration.

3.2 RADIUS introduction (Введение)

Протокол Radius поддерживает EAP расширение для обеспечения взаимодействия между коммутатором и аутентификационным сервером. Протокол Radius соответствует модели клиент/сервер (client / server). Коммутатору необходимо реализовать radius клиет, а аутентификационный сервер должен реализовать radius сервер.

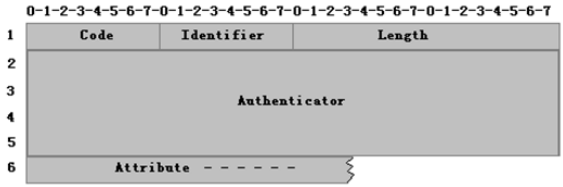
Для обеспечения безопасности взаимодействия коммутатора и аутентификационного сервера и предотвращения взаимодействия с неавторизованными коммутаторами и серверами, коммутатор и аутентификационный сервер должны аутентифицировать друг друга. Коммутатор и аутентификационный сервер должны иметь один и тот же ключ. При отправлении пакетов протокола RADIUS, должны генерироваться краткие сообщения (message summaries) с использованием HMAC алгоритма согласно ключу. Когда коммутатор и аутентификационный сервер получают пакеты протокола RADIUS, краткое сообщение (message summaries) должно быть верифицировано ключом. При удачной верификации, пакет протокола RADIUS считается легальным, в противном случае (нелегальный) пакет протокола RADIUS сбрасывается.

3.2.1 Protocol package (Пакеты протокола)

Протокол Radius основан на UDP. Протокол Radius может инкапсулировать аутентификационную и биллинговую (billing) информацию. Ранний аутентификационный порт radius - 1645, текущий порт - 1812. Ранний radius billing порт - 1646, текущий порт - 1813.

Так как протокол radius хостируется на UDP, существует механизм задержки передачи (timeout retransmission). Для увеличения надежности коммуникации между аутентификационной системой и сервером radius, предусмотрено две схемы сервера radius, в т.ч. механизм ожидания сервера (standby server mechanism).

Формат сообщения (radius message) показан на рисунке ниже. Код относится к типу сообщения протокола radius. Индикатор идентификации используется для определения соответствия запроса и ответа. Длина - это длина всего сообщения (включает заголовок сообщения). Аутентификатор – строка длиной 16 байт, случайный номер пакетов запроса и дайджест сообщений сгенерированный MD5 для ответных пакетов. Атрибут относится к атрибуту пакета протокола radius.



В сети используются следующие пакеты протокола RADIUS:

- Access request (запрос доступа): значение кода - 1, пакет запроса аутентификации отправлен от системы аутентификации к аутентификационнму серверу. Пакет инкапсулирует имя пользователя и пароль.

- Access accept (разрешение доступа): значение кода - 2. Пакет ответа отправленный от аутентификационного сервера к системе аутентификации указывает, что аутентификация прошла успешно.

- Access reject (отказ доступа): значение кода - 3. Пакет ответа отправленный от аутентификационного сервера к системе аутентификации указывает, что аутентификация не пройдена.

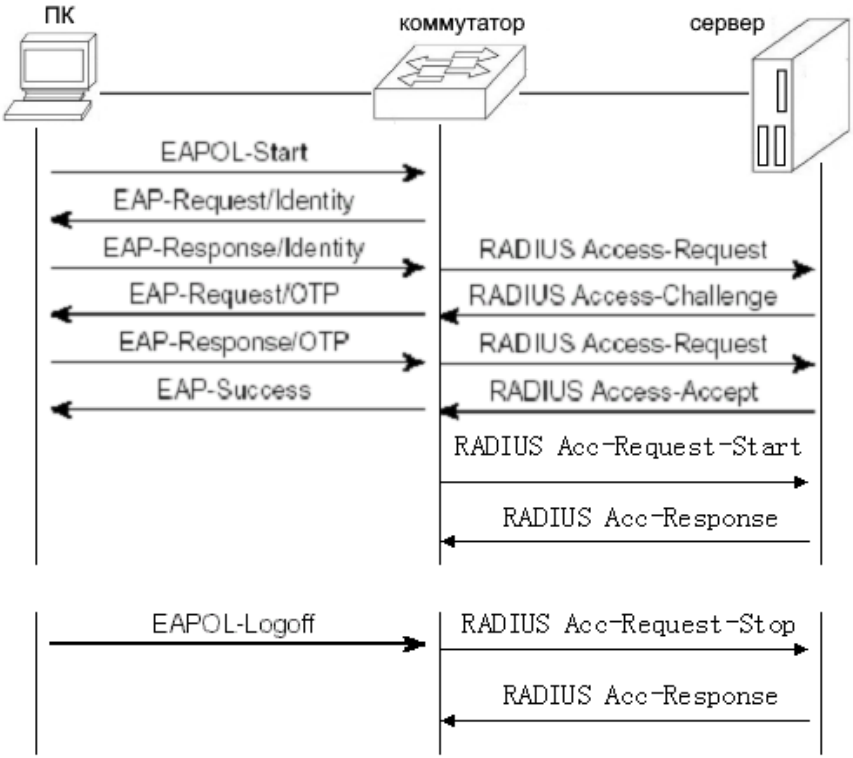
- Access challenge (вызов доступа): значение кода - 11, Пакет ответа отправленный от аутентификационного сервера к системе аутентификации указывает, что аутентификационному серверу требуется больше информации (имя пользователя, пароль и т.п.).

- Accounting request (счет запроса): значение кода - 4. Пакет запроса биллинга (billing) отправленный от системы аутентификации к аутентификационному серверу включает в себя стартовый и конечный пакеты биллинга (start billing package). Пакет инкапсулирует биллинговую информацию.

- Accounting response (счет ответа): значение кода - 5. Пакет ответа биллинга отправленный от аутентификационного сервера к системе аутентификации указывает, что информация о биллинге получена.

3.2.2 Protocol flow interaction (Взаимодействие протокола)

Когда пользователь инициирует процедуру аутентификации, система аутентификации и аутентификационный сервер взаимодействуют по протоколу radius. После успешной аутентификации или перехода пользователя в offline, системе аутентификации необходимо отправить пакет radius charging к аутентификационному серверу. Взаимодействие потоков протокола, когда система аутентификации не отправляет пакеты биллинга, показана на рисунке ниже.



При аутентификации пользователя, коммутатор инкапсулирует в сообщении запроса имя пользователя и отправляет его

аутентификационному серверу. Сервер отвечает на запрос access challenge запросом пароля. Коммутатор запрашивает пароль пользователя (клиента). Клиент инкапсулирует пароль в EAP. После получения EAP, коммутатор инкапсулирует его в access request и отправляет аутентификационному серверу. Аутентификационный сервер аутентифицирует пользователя, и в случае успеха отправляет коммутатору принятие (access accept). После получения этого сообщения коммутатор уведомляет клиента об успешной аутентификации. Одновременно он отправляет запрос accounting request для уведомления аутентификационного сервера о начале обмена, а сервер отправляет обратно ответ accounting response.

Если пользователь не планирует подключаться к сети, коммутатор получает уведомление о переходе в offline, то коммутатор отправляет запрос accounting request для уведомления аутентификационнго сервера об окончании биллинга. Пакет инкапсулирует биллинговую информацию, и аутентификационный сервер отправляет обратно сообщение accounting response.

3.2.3 User authentication method (Методы аутентификации)

Протокол Radius предлагает три метода аутентификации:

- PAP (Password Authentication Protocol) Текстовый ввод имени пользователя и пароля. Коммутатор передает имя пользователя и пароль серверу radius с помощью пакетов протокола radius. Сервер radius проверяет базу данных на соответствие имени и пароля. При совпадении, аутентификация считается пройденной успешно, в противном случае аутентификация считается не пройденной.

- CHAP (Challenge Handshake Authentication Protocol) Генерация 16и байтного случайного кода пользователя (используется для подключения к Internet). Пользователь шифрует случайный код, пароль и домены для генерации ответа и передают имя пользователя и ответ коммутатору. Коммутатор передает имя пользователя, ответ и оригинальный 16и байтный случайный код серверу radius. Radius проверяет базу данных коммутатора на наличие имени пользователя, получает тот же зашифрованный пароль пользователя. Далее шифрует его в соответствии с переданным 16и байтным случайным кодом, и

проверяет результат на соответствие с переданным ответом. При совпадении, аутентификация считается пройденной успешно, в противном случае аутентификация считается не пройденной.

- EAP (Extensible Authentication Protocol) Без участия коммутатора в процессе аутентификации, коммутатор используется только для передачи между пользователем и сервером radius. Когда пользователь запрашивает доступ в Internet, коммутатор запрашивает имя пользователя и передает его серверу radius. Сервер radius генерирует 16и байтный случайный код для пользователя и сохраняет его. Пользователь шифрует случайный код, пароль и домены для генерации ответа и передает имя пользователя и ответ коммутатору, который передает их серверу radius. Radius проверяет базу данных коммутатора на наличие имени пользователя, получает тот же зашифрованный пароль пользователя. Далее шифрует его в соответствии с переданным 16и байтным случайным кодом, и проверяет результат на соответствие с переданным ответом. При совпадении, аутентификация считается пройденной успешно, в противном случае аутентификация считается не пройденной.

3.3 Configure 802.1x (Конфигурация 802.1x)

Данный раздел содержит подробное описание конфигурации протокола 802.1x in и включает в себя следующие продразделы:

- 802.1x Default configuration (конфигурация по умолчанию)
- Turn 802.1x on and off (включение / отключение)
- Configure 802.1x port status (статусы портов)
- Configure re authentication mechanism (повторная аутентификация)
- Configure the maximum number of port access hosts (управление доступом хостов)
- Configure interval and number of retransmissions (интервалы передачи)
- Configure port as transport port (транспортные порты)
- Configure 802.1x client version number (номер версии клиента)
- Configure whether to check the client version number (проверка номера версии клиента)
- Configure authentication method (метод аутентификации)

- Configure whether to check the timing package of the client (проверка тайминга пакетов клиента)
- 802.1x display information (просмотр информации)

3.3.1 802.1xDefault configuration (Конфигурация по умолчанию)

Конфигурация протокола 802.1x по умолчанию представлена ниже:

- 802.1x is closed (протокол отключен)
- Status of all ports is N/A (статус всех портов не определен)
- Recertification mechanism is turned off, and the interval between recertification is 3600 seconds (ресертификация отключена, временной интервал 3600 сек)
- Maximum number of access hosts for all ports is 100 (максимальное число доступа к хостам – 100 для всех портов)
- Timeout interval for resending EAP request is 30 seconds (временной интервал отправки запросов EAP 30 сек)
- Number of times to resend EAP request after timeout is 3 (количество отправок запросов EAP – 3)
- Waiting time for user authentication failure is 60 seconds (Время ожидания повторной попытки аутентификации после неудачной попытки 60 сек)
- Time interval of timeout retransmission at the server is 10 seconds (временной интервал повторной отправки серверу – 10 сек)

Команда возврата коммутатора к настройкам по умолчанию в режиме global config mode:

```
Switch(config)#dot1x default
```

3.3.2 Turn 802.1x on and off (Включение и отключение 802.1x)

Команда включения протокола 802.1x в режиме global config mode:

```
Switch(config)#dot1x
```

Команда отключения протокола 802.1x в режиме global config mode:

```
Switch(config)#no dot1x
```

При отключении 802.1x, все порты возвращаются в статус N/A (не определен).

3.3.3 Configure 802.1x port status (Выбор статуса портов)

Перед установкой статуса порта убедитесь что протокол 802.1x включен. Если все пользователи должны пройти аутентификацию для получения доступа к сети, то порт должен быть установлен в автоматический статус (auto state).

Команда установки автоматического статуса порта GE1/1 (auto state) в режиме interface configuration mode и включение функции anti ARP Spoofing:

Switch(config-ge1/1)dot1x control auto

Возможные причины по которым функция anti ARP Spoofing не активируется:

- Ресурсы системы CFP исчерпаны.
- Функция ACL фильтрации включена на текущем интерфейсе.
- Функция DHCP snooping включена на текущем интерфейсе.
- Текущий интерфейс 3го уровня (three-layer) или находится в режиме trunk.

Команда установки статуса порта GE1/1 в force authorized status в режиме interface configuration mode:

Switch(config-ge1/1)dot1x control force-authorized

Команда установки статуса порта GE1/1 в force unauthorized state в режиме interface configuration mode:

Switch(config-ge1/1)dot1x control force-unauthorized

Команда установки статуса порта GE1/1 в N/A status в режиме interface configuration mode:

Switch(config-ge1/1)no dot1x control

Внимание: если порт имеет привязку к MAC адресу, то он не может быть переведен в статус auto, force authorized или force unauthorized status.

3.3.4 Configure re authentication (Конфигурация реаутентификации)

Для предотвращения аномального перехода клиента в offline относительно коммутатора и аутентификационного сервера, в коммутаторе предусмотрена процедура реаутентификации (повторной аутентификации), которая инициируется коммутатором через определенный промежуток времени (re authentication interval).

Команда запуска реаутентификации в режиме global config mode:

Switch(config)#dot1x reauthenticate

Команда отключения реаутентификации в режиме global config mode:

Switch(config)#no dot1x reauthenticate

Команда установки интервала реаутентификации в режиме global config mode:

Switch(config)#dot1x timeout re-authperiod <interval>

Внимание: интервал реаутентификации не должен быть слишком коротким, в противном случае снижается пропускная способность сети и производительность CPU (процессора) коммутатора.

3.3.5 Configure number of port access hosts (Управление хостами)

Каждый порт коммутатора может управлять доступом к определенному числу хостов. Эта функция ограничивает доступ к сети пользователям, которые могут использовать для неавторизованного доступа к сети несколько хостов. Порт может контролировать до 100 хостов (по умолчанию), их количество может быть уменьшено. Если будет установлено значение 0, то порт будет запрещать доступ к сети всем пользователям.

Команда установки максимального количества хостов доступа порта GE1/1 в режиме interface configuration mode:

Switch(config-ge1/1)dot1x support-host <number>

3.3.6 Configure interval and number of retransmissions (Интервалы передачи)

Стандарты протокола 802.1x определяют временные интервалы и количество передач (ретрансляций) необходимых для организации взаимодействия. Коммутатор использует стандартные значения этих параметров. Пользователям не рекомендуется изменять временные интервалы и количество ретрансляций при использовании периода TX относящегося к передаче пакетов запросов EAP протокола. Параметр Max req указывает количество ретрансляций запросов EAP request. Временной интервал используется для указания времени ожидания реаутентификации пользователем. Интервал Server timeout определяет временной промежуток ретрансляции коммутатором пакетов radius аутентификационному серверу. Интервал Sup timeout определяет временной промежуток отправки коммутатором пакетов EAP запросов клиенту.

Команда установки интервалов и числа ретрансляций в режиме global config mode:

Switch(config)#dot1x timeout tx-period <interval>
Switch(config)#dot1x max-req <number>
Switch(config)#dot1x timeout quiet-period <interval>
Switch(config)#dot1x timeout server-timeout <interval>
Switch(config)#dot1x timeout supp-timeout <interval>

3.3.7 Configure port as transport port (Транспортный порт)

Когда коммутатор не переключается в режим 802.1x аутентификации, а другие коммутаторы в подсети находятся в режиме 802.1x аутентификации, порт связанный с клиентом и аутентификационным коммутатором может быть сконфигурирован как транспортный порт, аутентификационный eapol пакет может быть отправлен от клиента к аутентификационному коммутатору. Аналогичным образом может быть реализована 802.1x аутентификация для других коммутаторов и клиентов.

Команда перевода в транспортный режим передачи порта GE1/1 в interface configuration mode:

Switch(config-ge1/1)dot1x transmit-port

Команда перевода в обычный режим передачи порта GE1/1 в interface configuration mode:

Switch(config-ge1/1)no dot1x transmit-port

3.3.8 Configure 802.1x client version number (Номер верси клиента)

Только клиент с версией не ниже установленной может пройти аутентификацию. На коммутаторе установлена версия клиента 2.0 (по умолчанию).

Команда установки версии клиента в режиме global config mode:

Switch(config)# dot1x client-version <string>

3.3.9 Configure check the client version number (Проверка номера версии клиента)

Функция проверки номера версии клиента включена по умолчанию. Если данная функции включена, то во время проведения аутентификации, коммутатор сначала должен проверить номер версии клиента.

Команда включения функции проверки номера версии клиента в режиме global config mode:

Switch(config)# dot1x check-version open

3.3.10 Configure authentication method (Выбор метода аутентификации)

Режим аутентификации выбирается клиентом и разделяется на основную и расширенную аутентификацию. Коммутатор может быть настроен на применение одного из методов в первую очередь. Если клиент выбирает метод аутентификации несоответствующий установленному на коммутаторе, то после нескольких неудачных попыток аутентификации, клиенту будет предложено начать аутентификацию по другому методу.

Команда выбора расширенного метода аутентификации (extended mode) в режиме global config mode:

Switch(config)# dot1x extended

3.3.11 Configure to check the timing package of the client (Проверка тайминга пакета клиента)

Включение данной функции после настройки тайминга протокола 802.1x, активирует проверку всех пакетов на прохождение аутентификации.

Команда настройки проверки тайминга пакетов клиента в режиме global config mode:

Switch(config)# dot1x check-client

3.3.12 Display 802.1x information (Информация 802.1x)

Команда просмотра информации о настройках 802.1x в режимах normal mode / privileged mode. Команда dot1x выводит для просмотра информацию о всех настройках 802.1x, включая конфигурацию портов. Команда dot1x interface выводит для просмотра информацию о всех клиентах имеющих доступ к порту:

Switch#show dot1x

Switch#show dot1x interface

3.4 Configure RADIUS (Конфигурация RADIUS)

Данный раздел содержит подробное описание конфигурации протокола RADIUS in и включает в себя следующие подразделы:

- Radius default configuration (конфигурация по умолчанию)
- Configure the IP address of the authentication server (IP адрес сервера аутентификации)
- Configure shared key (конфигурация общего ключа)
- Start and close billing (включение/отключение биллинга)
- Configure radius port and attribute information (конфигурация порта и информация атрибута)

- Configure radius roaming function (настройка роуминга)
- Display radius information (информация radius)

3.4.1 RADIUS Default configuration (Конфигурация по умолчанию)

Конфигурация протокола RADIUS по умолчанию представлена ниже:

- IP адрес основного и резервного аутентификационного сервера не установлены (IP адрес 0.0.0.0)
- Ключ shared не сконфигурирован, (string shared ключа не задан)
- Биллинг включен (по умолчанию)
- UDP аутентификационный порт – 1812, UDP биллинговый порт - 1813
- Значение атрибута nasport - 0xc353, значение nasporttype - 0x0f, значение nasportserver - 0x02

3.4.2 IP address of the authentication server (IP адрес сервера аутентификации)

Для обеспечения взаимодействия протокола radius между коммутатором и сервером аутентификации, необходимо прописать в коммутаторе IP адрес сервера аутентификации. На практике может использоваться один или два сервера аутентификации (основной и резервный). Если в коммутаторе прописано два IP адреса аутентификационных серверов, то коммутатор может взаимодействовать с резервным сервером, если соединение с основным сервером по какой-либо причине прервано.

Команда ввода IP адреса основного сервера аутентификации в режиме global config mode:

Switch(config)#radius-server host <ip-address>

Команда ввода IP адреса резервного сервера аутентификации в режиме global config mode:

Switch(config)#radius-server option-host <ip-address>

3.4.3 Configure shared key (Конфигурация общего ключа)

Между коммутатором и аутентификационным сервером требуется взаимная аутентификация, для чего необходим общий ключ (shared key), который должен быть установлен на коммутаторе и сервере аутентификации.

Команда ввода конфигурации общего ключа (shared key) в режиме global config mode:

Switch(config)#radius-server key <string>

3.4.4 Start and close billing (включение/отключение биллинга)

Коммутатор прекращает отправку пакетов протокола radius серверу аутентификации по окончании успешной аутентификации или когда пользователь переходит в режим offline. Обычно в практических случаях функция биллинга (billing) включена.

Команда запуска биллинга в режиме global config mode:

Switch(config)#radius-server accounting

Команда остановки биллинга в режиме global config mode:

Switch(config)#no radius-server accounting

3.4.5 Configure radius port and attribute information (порт radius и информация атрибута)

Внимание: не рекомендуется вносить изменения в конфигурацию порта radius и информацию атрибута.

Команда изменения конфигурации radius UDP порта в режиме global config mode:

Switch(config)#radius-server udp-port <port-number>

Команды изменения информации атрибута (radius attribute) в режиме global config mode:

Switch(config)#radius-server attribute nas-portnum <number>
Switch(config)#radius-server attribute nas-porttype <number>
Switch(config)#radius-server attribute service-type <number>

3.4.6 Configure radius roaming function (Функция роуминга)

В случае когда клиент привязан к Mac, IP адресу или VLAN изменяет свою локацию, перестают выполняться условия аутентификации по протоколу 802.1x. Функция роуминга (radius roaming function) позволяет обойти требования привязки клиента к Mac, IP адресу или VLAN и делает возможной процедуру аутентификации согласно 802.1x протоколу.

Команда включения функции роуминга в режиме global config mode:

```
Switch(config)#radius-server roam
```

Команда отключения функци роуминга в режиме global config mode:

```
Switch(config)#no radius-server roam
```

3.4.7 Display Radius information (Информация Radius)

Команда просмотра информации о настройках radius в режимах normal mode / privileged mode:

```
Switch#show radius-server
```

3.4.8 Configuration example (Пример конфигурации)

Запустить протокол 802.1x, установить порт GE1/1 в режим auto, сконфигурировать основной сервер аутентификации (IP 198.168.80.111) и общий ключ (shared key) коммутатора как ABCDEF.

```
Switch#
Switch# dot1x
Switch#config t
Switch(config)#radius-server host 198.168.80.111
Switch(config)#radius-server key abcdef
Switch(config)# interface ge1/1
Switch(config-ge1/1)# dot1x control auto
```

3.4 TACACS+ Introduction (Протокол TACACS+)

TACACS+ протокол аутентификации и авторизации предоставляет возможности управления авторизацией пользователей, верификации легитимности пользователей и авторизацией команд. При активированной аутентификации TACACS +, пользователю необходимо верифицировать имя пользователя и пароль через сервер TACACS+ для доступа к коммутатору. Пройти аутентификацию для доступа к коммутатору возможно только с корректными данными имени пользователя и паролем.

TACACS+ разделяет права пользователей на два уровня: обычные пользователи и привилегированные пользователи. Обычные пользователи имеют право использовать обычный режим (normal mode) интерфейса ввода CLI команд, привилегированные пользователи имеют доступ ко всем режимам интерфейса ввода CLI команд. Выполнение команд основано на правах различного уровня. Когда пользователь вводит команду (кроме enable end и exit), на сервере TACACS+ проводится верификация пользователя. Если верификация не пройдена, то выполнения команды не происходит.

Аутентификация и авторизация TACACS+ применима только для терминалов telnet и SSH, но не применима для управления через консоль (console terminals). При доступе к коммутатору через терминалы telnet и SSH, имя пользователя и пароль должны быть верифицированы. Доступ к командной строке CLI может быть получен только после верификации имени пользователя и пароля. Доступ к SSH возможен только для привилегированных пользователей. Аутентификация TACACS+ также применяется для доступа к web-интерфейс, но только для верификации пароля привилегий и разрешений без авторизации команд.

Функция TACACS+ на коммутаторе по умолчанию отключена. Telnet, SSH или web используют многопользовательский режим управления. После включения функци TACACS+ доступна настройка многопользовательского режима, но сам многопользовательский режим на практике не используется.

Таблица команд аутентификации TACACS + протокола.

Команда	Описание	CLI режим
tacacsplus enable	Включение TACACS+	Global configuration mode
tacacsplus disable	Отключение TACACS + function	Global configuration mode
tacacsplus host <server-ip>	IP адрес основного сервера с поддержкой IPv4 и IPv6. Рекомендуется использовать ACS (Cisco)	Global configuration mode
tacacsplus option-host <server-ip>	IP адрес standby сервера с поддержкой IPv4 and IPv6. Рекомендуется использовать ACS (Cisco)	Global configuration mode
tacacsplus key WORD	Конфигурация общего ключа для шифрования передаваемых данных (должен соответствовать конфигурации сервера).	Global configuration mode
tacacsplus auth-type (PAP|CHAP)	Выбор метода аутентификаци (включая PAP и chap). PAP (по умолчанию), поле инкапсулирует secret. Chap инкапсулирует проверку кода MD5 secret.	Global configuration mode
show tacacsplus	Просмотр конфигурации TACACS+	Global configuration mode
no tacacsplus host	Сброс IP адреса основного сервера	Global configuration mode
no tacacsplus key	Сброс общего ключа (shared key)	Global configuration mode