

Настройка коммутаторов Cisco

Глава 8

В рамках этой темы...

Технологии маршрутизации IP

Настройка интерфейсов SVI.

Защита сетевых устройств

Настройка и проверка средств защиты сетевых устройств.

- Защита устройства паролем.

- Привилегированный режим или защита.

- SSH.

- VTY.

- Служебный пароль.

- Описание основных методов аутентификации.

Настройка и проверка средств защиты порта коммутатора.

- Автоматическое обнаружение MAC-адресов.

- Ограничение MAC-адресов.

- Статические и динамические.

- Реакция при нарушении защиты.

 - Отключение из-за ошибки.

 - Отключение.

 - Ограничение.

- Отключение неиспользуемых портов.

- Восстановление после ошибки.

- Присвоение неиспользуемых портов неиспользуемым VLAN.

Защита доступа к командной строке

- **Первый этап защиты коммутатора** - это защита доступа к интерфейсу CLI (пользовательскому и привилегированному режиму):
 - ✓ Стандартная конфигурация консоли позволяют консольному пользователю перейти из пользовательского режима в привилегированный, **не вводя пароль**.
 - ✓ стандартные параметры конфигурации коммутатора **не разрешают** сеансы vty (Telnet или SSH) н и в пользовательском, ни в привилегированном режиме.

Защита простым паролем

- Для пользователей Telnet и консоли коммутаторы Cisco способны защитить **пользовательский режим простым паролем** (без имени пользователя):
 - **пользователи консоли** должны ввести пароль консоли (console password), заданный в режиме конфигурации линии консоли (line console 0).
 - **пользователи Telnet** должны вводить пароль Telnet (Telnet password), называемый также паролем vty (vty password), поскольку его конфигурация находится в режиме конфигурации линии vty.

Защита простым паролем

- Коммутаторы Cisco защищают **привилегированный режим** при помощи **привилегированного пароля** (enable password):
 - ✓ пользователь **в пользовательском режиме** вводит команду enable, запрашивающую привилегированный пароль;



Защита простым паролем

- Команда `login` указывает операционной системе IOS использовать простой пароль, а команда `password пароль_значение` задает пароль.
- Операционная система IOS защищает привилегированный режим, используя привилегированный пароль, заданный глобальной командой `enable secret пароль_значение`.

Защита простым паролем



```
Switch> enable
Switch# configure terminal
Switch(config)# enable secret cisco
Switch(config)# hostname Emma
Emma(config)# line console 0
Emma(config-line)# password faith
Emma(config-line)# login
Emma(config-line)# exit
Emma(config)# line vty 0 15
Emma(config-line)# password love
Emma(config-line)# login
Emma(config-line)# exit
Emma(config)# exit
Emma#
```

Ввод команд в CLI

- ✓ **Первая строка** демонстрирует приглашение к вводу команд коммутатора **Switch >** (стандартное приглашение);
- ✓ **Символ >** указывает на пользовательский режим;
- ✓ пользователь ввел команду **enable**, активирующую привилегированный режим (символ #);

```
Switch> enable
```


Ввод команд в CLI

- ✓ Пользователь переходит в глобальный режим конфигурации (команда **configure terminal**).
- ✓ Оказавшись в глобальном режиме конфигурации, пользователь вводит две команды (**enable secret** и **hostname**), распространяющиеся на весь коммутатор.

```
Switch# configure terminal
```

```
Switch(config)# enable secret cisco
```

```
Switch(config)# hostname Emma
```

Ввод команд в CLI

- ✓ используя команду **line console 0**, пользователь должен войти в режим конфигурации канала консоли.
- ✓ команда **password** задает простой текстовый пароль (faith), а команда **login** указывает коммутатору запрашивать его при входе.
- ✓ командой **exit** пользователь выходит из режима настройки консоли;

```
Emma (config)# line console 0
```

```
Emma (config-line)# password faith
```

```
Emma (config-line)# login
```

```
Emma (config-line)# exit
```

Ввод команд в CLI

- следующие строки примера повторяют те же действия, но для всех **16 каналов vty** (линии vty от 0 до 15) .
- 16 каналов vty означает, что коммутатор может принять **16 параллельных подключений** Telnet к коммутатору.
- команда **end (exit)** возвращает пользователя в привилегированный режим.

```
Emma (config) # line vty 0 15  
Emma (config-line) # password love  
Emma (config-line) # login  
Emma (config-line) # exit  
Emma (config) # exit  
Emma #
```

Результат ввода команд

- **у пользователя консоли** будет запрашиваться пароль (без имени пользователя) , и он должен ввести hope.
- **у пользователей Telnet** будет запрашиваться пароль (тоже без имени пользователя), и он должен будет ввести love.
- **для перехода в привилегированный режим** пользователи консоли и Telnet должны использовать команду enable с паролем cisco.
- **пользователи SSH** пока не смогут войти на этот коммутатор, поскольку для поддержки протокола SSH необходимо больше действий.

Новый файл текущей конфигурации running-config на коммутаторе Emma

```
Emma# show running-config
```

```
!
```

```
Building configuration...
```

```
Current configuration : 1333 bytes
```

```
!
```

```
version 12.2
```

```
!
```

```
hostname Emma ★
```

```
!
```

```
enable secret 5 $1$YXRN$11zOe1Lb0Lv/nHyTquobd. ★
```

```
!
```

```
spanning-tree mode pvst
```

```
spanning-tree extend system-id
```

```
!
```

```
interface FastEthernet0/1
```

```
!
```

```
interface FastEthernet0/2
```

```
!
```

```
interface FastEthernet0/24
```

```
!
```

```
interface GigabitEthernet0/1
```

```
!
```

```
interface GigabitEthernet0/2
```

```
!
```

```
interface Vlan1
```

```
no ip address
```

```
no ip route-cache
```

```
!
```

```
!
```

```
line con 0 ★
```

```
password faith
```

```
login
```

```
!
```

```
line vty 0 4 ★
```

```
password love
```

```
login
```

```
!
```

```
line vty 5 15 ★
```

```
password love
```

```
login
```

Защита по локальному имени пользователя и паролю

- Коммутаторы Cisco поддерживают **метод аутентификации**, подразумевающий использование имени пользователя и пароля:
 - для использования этого метода достаточно одной или нескольких глобальных команд конфигурации **username имя password пароль**.
 - затем нужно уведомить каналы консоли и vty об использовании заданных имен пользователя и пароля (**подкоманда линии login local**).

Защита по локальному имени пользователя и паролю

② Глобальный режим:

Создать имя пользователя и пароль

① Режим VTY:

Разрешить использование локальных имен пользователя

Конфигурация

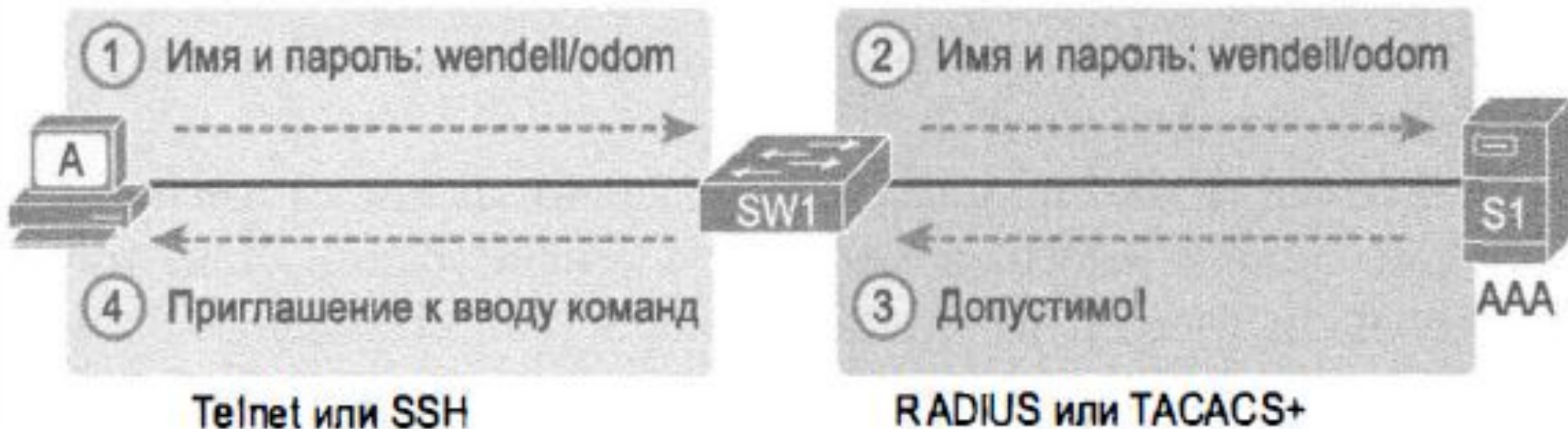
```
username wendell password odom
username chris password youdaman

line vty 0 15
 login local
```

Рис. 8.2. Настройка на коммутаторе аутентификации по локальному имени пользователя и паролю

Защита с помощью AAA

- Коммутаторы и маршрутизаторы Cisco поддерживают еще один способ проверки правильности имен пользователя и паролей - внешний сервер аутентификации, авторизации и учета (**Authentication, Authorization, And Accounting – AAA**):
 - при аутентификации коммутатор (или маршрутизатор) просто посылает на сервер AAA **сообщение с запросом**, допустимы ли данное имя пользователя и пароль, а сервер AAA **отвечает**.



Настройка протокола SSH

ЭТАП	ДЕЙСТВИЕ
1	Настройте линии vty на использование имен пользователя локально (используя команду login local)
2	При использовании локальных имен пользователя добавьте одну или несколько глобальных команд конфигурации username , чтобы задать пары имен пользователей и паролей
3 (новые команды)	Настройте коммутатор на создание соответствующих пар открытых и закрытых ключей, используемых при шифровании. Для этого используются две команды: <ol style="list-style-type: none">1. В качестве предпосылки для следующей команды задайте имя домена DNS при помощи глобальной команды конфигурации ip domain-name ИМЯ.2. Создайте ключи шифрования, используя глобальную команду конфигурации crypto key generate rsa.
4	Для повышения защиты разрешите использование версии 2 протокола SSH, используя глобальную команду ip ssh version 2 (необязательно).

Настройка протокола SSH

③ Глобальный режим:

Создать ключ шифрования

② Глобальный режим:

Создать имя пользователя и пароль

① Режим VTY:

Разрешить использование локальных имен пользователя

Конфигурация

```
ip domain-name example.com  
crypto key generate rsa
```

```
username wendell password odom  
username chris password youdaman
```

```
line vty 0 15  
login local
```

Рис. 8.4. Настройка на коммутаторе поддержки протокола SSH

Настройка протокола SSH

```
Emma# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Emma(config)# line vty 0 15
! Ниже вводится команда этапа 1
Emma(config-line)# login local
Emma(config-line)# exit
↑
! Ниже вводится команда этапа 2
Emma(config)# username wendell password odom

Emma(config)# username chris password youdaman
!
! Ниже вводится команда этапа 3
Emma(config)# ip domain-name example.com
Emma(config)# crypto key generate rsa
The name for the keys will be: Emma.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 4 seconds)

Emma(config)# ip ssh version 2
Emma(config)# ^Z
Emma#
```

Результаты ввода команд

- Команда `show ip ssh` отображает информацию о состоянии самого сервера SSH.
- Команда `show ssh` отображает информацию о каждом клиенте SSH, подключенном к коммутатору в настоящее время

```
Emma# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQgQC+/mp2iaeaGwjqkIgLNH+lN/04LTc2u6qHVHHv3hoq
/DDBd9vABNnJGsq8z0Hm9HcrSudC20N/cCuEb4x5+T9rvNkUeAqwEEoJALpdiWVOpBliomhPy
svJi+m4
wI16AH31KI+GFCZv1AIjZSYHQEbvdCEqsYezAeKnPhvzTrUqaQ==
```

```
Emma# show ssh
Connection Version Mode Encryption Hmac      State      Username
0           2.0      IN   aes128-cbc hmac-shal Session started wendell
0           2.0      OUT  aes128-cbc hmac-shal Session started wendell
%No SSHv1 server connections running.
```

Отключение протоколов

- Коммутатор поддерживает на линиях vty **доступ по протоколам** Telnet и SSH, но для повышения безопасности **можно отключить** один или оба из них.
- Коммутатор контролирует поддержку протоколов Telnet и SSH на линиях vty, используя подкоманду vty transport input {all/none/telnet/ssh) со следующими параметрами:

transport input all или transport input telnet ssh. Поддерживать оба.

transport input none. Не поддерживать ни один.

transport input telnet. Поддерживать только Telnet.

transport input ssh. Поддерживать только SSH.

Шифрование паролей

- По умолчанию для некоторых из команд конфигурации, пароли хранятся в виде открытого текста в файле **running-config**.
- Только команда **enable secret** автоматически скрывает значение пароля.
- Результатом применения методов шифрования пароля будет невозможность просмотреть пароли в выводе команды **show running-config**.

Шифрование паролей

- Некоторые пароли можно зашифровать при помощи глобальной команды конфигурации **service password-encryption**:
 - ✓ Немедленно после ввода данной команды IOS шифрует все существующие команды **password** (в режимах консоли и vty), а также пароли команды **username password**.
 - ✓ Пока данная команда остается в конфигурации, IOS шифрует пароли, даже если их значения изменяются.
 - ✓ Немедленно после ввода команды **no service password-encryption** шифрование паролей отменяется, но существующие пароли остаются зашифрованными.
 - ✓ После удаления данной команды из конфигурации операционная система IOS сохраняет значения всех измененных паролей этих команд в виде обычного текста.

Шифрование паролей

```
Switch3# show running-config | begin line vty
line vty 0 4
  password cisco
  login
line vty 5 15
  password cisco
  login
```



пароли
открытым
текстом

```
Switch3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch3(config)# service password-encryption
Switch3(config)# ^Z
```

пароли
зашифрован
ы

```
Switch3# show running-config | begin line vty
line vty 0 4
  password 7 070C285F4D06
  login
line vty 5 15
  password 7 070C285F4D06
  login
```



```
end
Switch3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch3(config)# service password-encryption
```


Шифрование привилегированного пароля

- Старая команда **enable password** сохраняет пароль на привилегированный режим как открытый текст.
- Новая команда **enable secret** автоматически шифрует пароль, применяет к нему математическую функцию Message Digest 5 (MD5 – тип 5), сохраняя результат вычисления в файле конфигурации.

```
Switch3(config)# enable secret fred
Switch3(config)# ^Z
Switch3# show running-config | include enable secret

enable secret 5 $1$ZGMA$e8cmvkz4UjiJhVp7.maLE1
```

Шифрование локальных паролей

- Для лучшего шифрования локальных паролей добавлена глобальная команда **username пользователь secret пароль** (использует алгоритм шифрования SHA-256 (тип 4)) как альтернатива команде **username пользователь password пароль**.

```
sam(config)#username sam secret lol
```

```
hostname sam
```

```
!
```

```
enable secret 5 $1$mERr$kC67g8eGWIE.qR4xUJC6z0
```

```
!
```

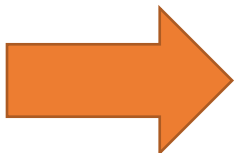
```
!
```

```
!
```

```
!
```

```
username sam secret 5 $1$mERr$OWyfpXTYZksXUEAfH.1kg0
```

```
!
```



Отображаемое сообщение

- **Отображаемое при подключении сообщение (banner)** - это просто текст, который выводится на экран пользователя.
- **Команда banner** режима глобальной конфигурации применяется позволяет настроить 3 типа сообщений:
 1. **Сообщение дня** (Message of the Day - MOTD) - отображается до того, как появится приглашение аутентификации.
 2. **Сообщение перед аутентификацией** (login) - отображается до выполнения аутентификации, но после сообщения дня.
 3. **Сообщение после аутентификации** (exec) - отображается после успешной аутентификации пользователя.

Буфер истории команд

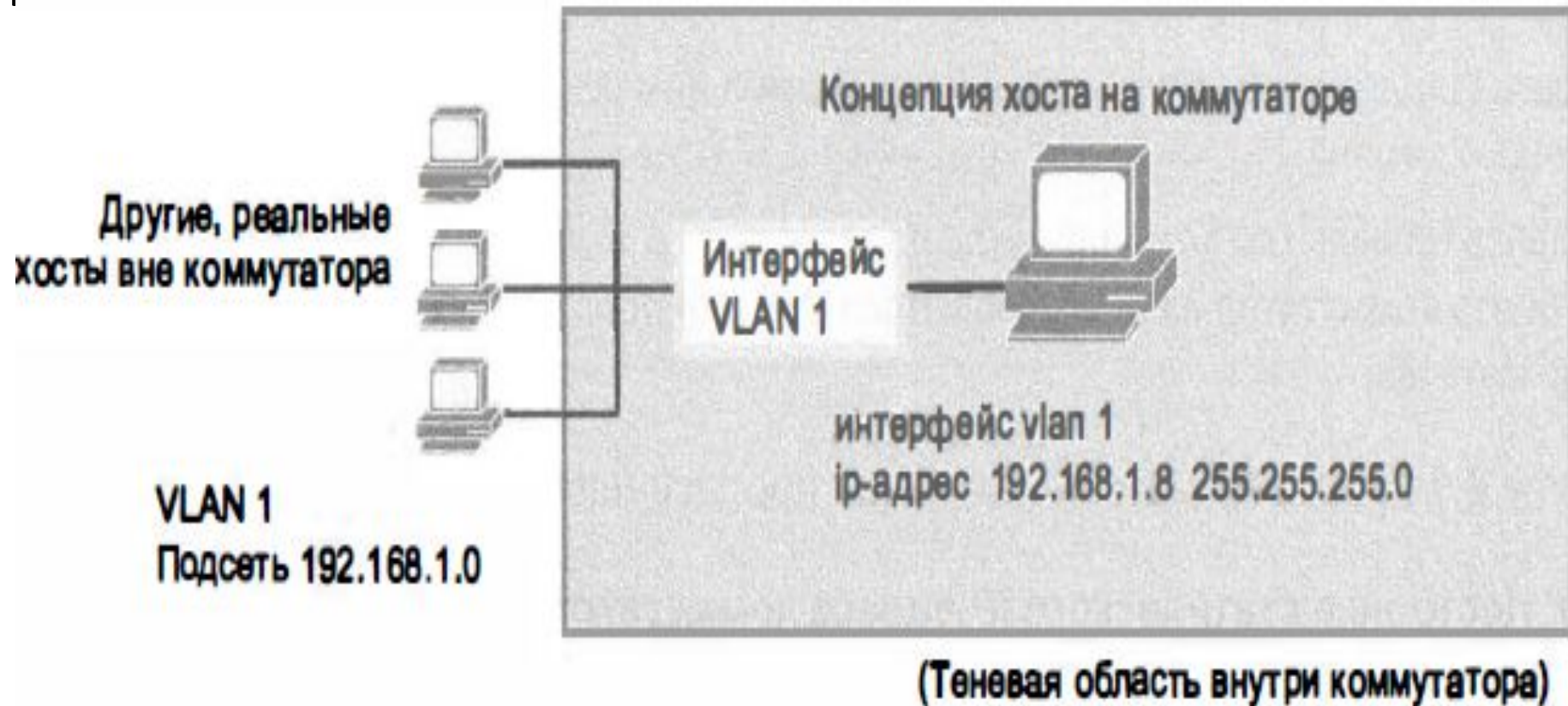
- В **буфер истории** сохраняется несколько последних введенных команд.
- Некоторые из наиболее полезных команд для работы с буфером истории:
 1. **show history** - отображает команды, находящиеся в буфере истории команд;
 2. **history size x** - задает количество команд (x), которое будет сохраняться в буфере истории команд (для консольного или сеанса vty);
 3. **terminal history size x** - позволяет задавать размер буфера истории команд (x) только для текущего сеанса пользователя.

Стандартные настройки коммутатора

- Коммутаторы Cisco поставляются со **стандартными настройками**, позволяющими им работать из коробки (не требуется дополнительной настройки):
 1. работа всех интерфейсов разрешена (стандартное состояние **no shutdown**);
 2. включены автопереговоры для всех портов, которые могут их использовать (стандартное состояние **duplex auto** и **speed auto**);
 3. все интерфейсы стандартно являются частью сети VLAN 1 (**switchport access vlan 1**).

Концепция SVI

- Коммутатор использует **коммутируемый виртуальный интерфейс** (Switched Virtual Interface - SVI) или - **интерфейс VLAN** (VLAN interface), действующий как собственная сетевая плата коммутатора для подключения к локальной сети и передачи пакетов IP.



Выбор VLAN для настройка IP адреса



Настройка IPv4-адреса

- Коммутатор настраивает свой IPv4-адрес и маску на специальном, подобном сетевой плате, интерфейсе VLAN:
 1. перейти в режим конфигурации сети VLAN 1 с помощью команды **interface vlan 1** из глобального режима конфигурации устройства;
 2. присвоить IP-адрес и маску с помощью команды **ip address ip-адрес маска** в подрежиме конфигурации интерфейса;
 3. включить виртуальный интерфейс сети VLAN 1 с помощью **команды no shutdown** в подрежиме конфигурации интерфейса;
 4. Указать стандартный шлюз устройства в глобальном режиме конфигурации с помощью команды **ip default-gateway ip –адрес**;
 5. Добавить глобальную команду **ip name-server ip-адрес1 ip-адрес2 ...**, чтобы настроить коммутатор на использование DNS при поиске имен по их IP-адресам (необязательно).

Настройка IPv4-адреса

```
Emma# configure terminal
Emma(config)# interface vlan 1
Emma(config-if)# ip address 192.168.1.200 255.255.255.0
Emma(config-if)# no shutdown
00:25:07: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
00:25:08: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
Emma(config-if)# exit
Emma(config)# ip default-gateway 192.168.1.1
```

Проверка IPv4-адреса

• **Конфигурацию** IPv4-адреса коммутатора можно проверить несколькими способами:

1. посмотреть текущую конфигурацию, используя команду **show running- config;**
2. посмотреть информацию об IP-адресе и маске, используя команду **show interface vlan x**, где x – номер влана;
3. при использовании сервера DHCP команда **show dhcp lease** позволяет посмотреть зарезервированный (временно) IP-адрес и другие параметры

Проверка IPv4-адреса

```
Emma# show dhcp lease
```

```
Temp IP addr: 192.168.1.101 for peer on Interface: Vlan1
```

```
Temp sub net mask: 255.255.255.0
```

```
  DHCP Lease server: 192.168.1.1, state: 3 Bound
```

```
  DHCP transaction id: 1966
```

```
  Lease: 86400 secs, Renewal: 43200 secs, Rebind: 75600 secs
```

```
Temp default-gateway addr: 192.168.1.1
```

```
  Next timer fires after: 11:59:45
```

```
  Retry count: 0 Client-ID: cisco-0019.e86a.6fc0-V11
```

```
  Hostname: Emma
```

```
Emma# show interface vlan 1
```

```
Vlan1 is up, line protocol is up
```

```
  Hardware is EtherSVI, address is 0019.e86a.6fc0 (bia 0019.e86a.6fc0)
```

```
  Internet address is 192.168.1.101/24
```

```
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
```

```
    reliability 255/255, txload 1/255, rxload 1/255
```

```
! Остальная информация опущена
```

```
Emma# show ip default-gateway
```

```
192.168.1.1
```

Настройка интерфейсов коммутатора

- В операционной системе Cisco IOS для настройки интерфейсов используется специализированный режим конфигурирования интерфейса, называемый обычно

```
Emma# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Emma (config)# interface FastEthernet 0/1  
Emma (config-if)# duplex full  
Emma (config-if)# speed 100  
Emma (config-if)# description Server1 connects here  
Emma (config-if)# exit  
Emma (config)# interface range FastEthernet 0/11 - 20  
Emma (config-if-range)# description end-users connect_here  
Emma (config-if-range)# ^Z
```

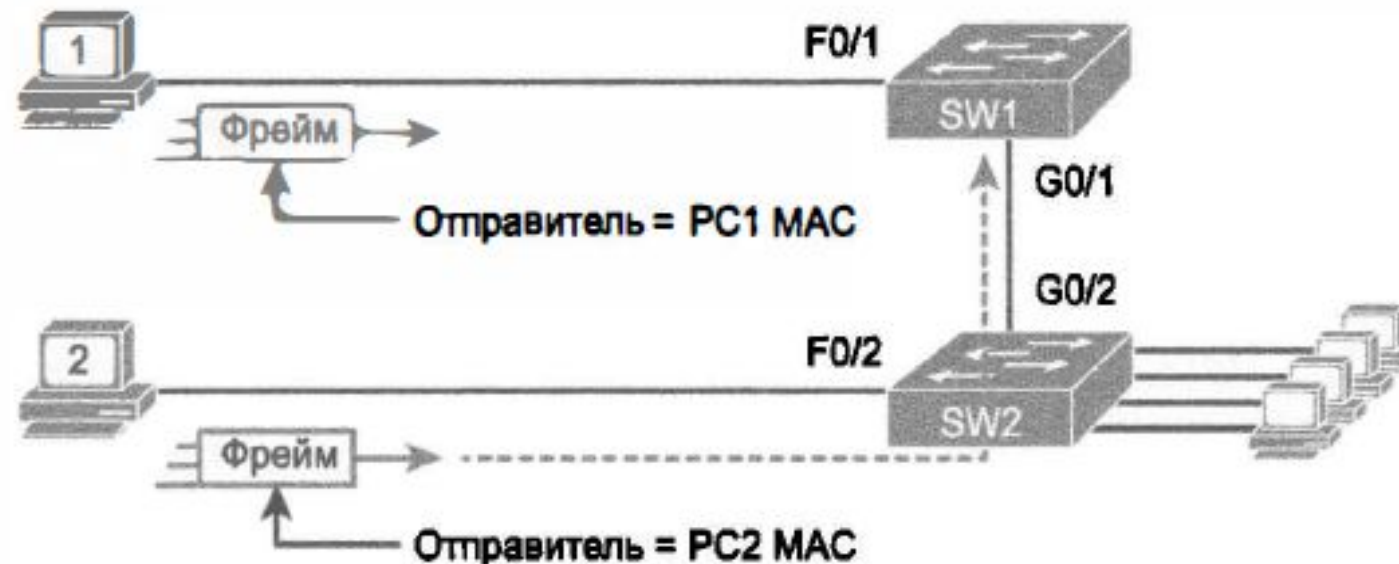
Настройка интерфейсов коммутатора

```
Emma# show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	Server1 connects h	notconnect	1	full	100	10/100BaseTX
Fa0/2		notconnect	1	auto	auto	10/100BaseTX
Fa0/3		notconnect	1	auto	auto	10/100BaseTX
Fa0/4		connected	1	a-full	a-100	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Fa0/6		connected	1	a-full	a-100	10/100BaseTX
Fa0/7		notconnect	1	auto	auto	10/100BaseTX
Fa0/8		notconnect	1	auto	auto	10/100BaseTX
Fa0/9		notconnect	1	auto	auto	10/100BaseTX
Fa0/10		notconnect	1	auto	auto	10/100BaseTX
Fa0/11	end-users connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/12	end-users connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/13	end-users connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/14	end-users connect	notconnect	1	auto	auto	10/100BaseTX
Fa0/15	end-users connect	notconnect	1	auto	auto	10/100BaseTX

Защита портов коммутатора

- Если известно, какие конкретно устройства будут подключены кабелями к каким интерфейсам коммутатора, то можно использовать **защиту порта (port security)**, чтобы его могли использовать только указанные устройства:
 - ✓ *Защита порта идентифицирует устройства по MAC-адресу отправителя во фрейме Ethernet.*



Основные правила защиты порта

1. Определите **максимальное разрешенное количество** MAC-адресов отправителя для всех входящих фреймов на интерфейс.
2. **Отследите все входящие фреймы** и сохраните список всех MAC-адресов отправителей, добавьте счетчик количества отличных MAC-адресов отправителя.
3. Если при добавлении нового MAC-адреса отправителя в список **количество хранимых MAC-адресов** превысит заданный максимум, срабатывает защита порта и коммутатор принимает меры (стандартное действие – отключение интерфейса)

Последовательность защиты порта

1. Используя подкоманды интерфейса **switchport mode access** или **switchport mode trunk**, объявите интерфейс коммутатора статическим портом доступа или магистральным портом соответственно;
2. Включите защиту порта подкомандой интерфейса **switchport port-security**;
3. Переопределите стандартное максимальное количество разрешенных MAC-адресов, интерфейса (1) подкомандой интерфейса **switchport port-security maximum число** (Необязательно.)
4. Задайте все допустимые MAC-адреса отправителей для данного интерфейса, используя команду **switchport port-security mac-address MAC-адрес** (Необязательно).
5. Можно также включить автоматическое обнаружение MAC-адресов, чтобы коммутатор сам изучил MAC-адреса. Используйте подкоманду интерфейса **switchport port-security mac-address sticky** (Необязательно.)

Последовательность защиты порта

```
fred# show running-config
```

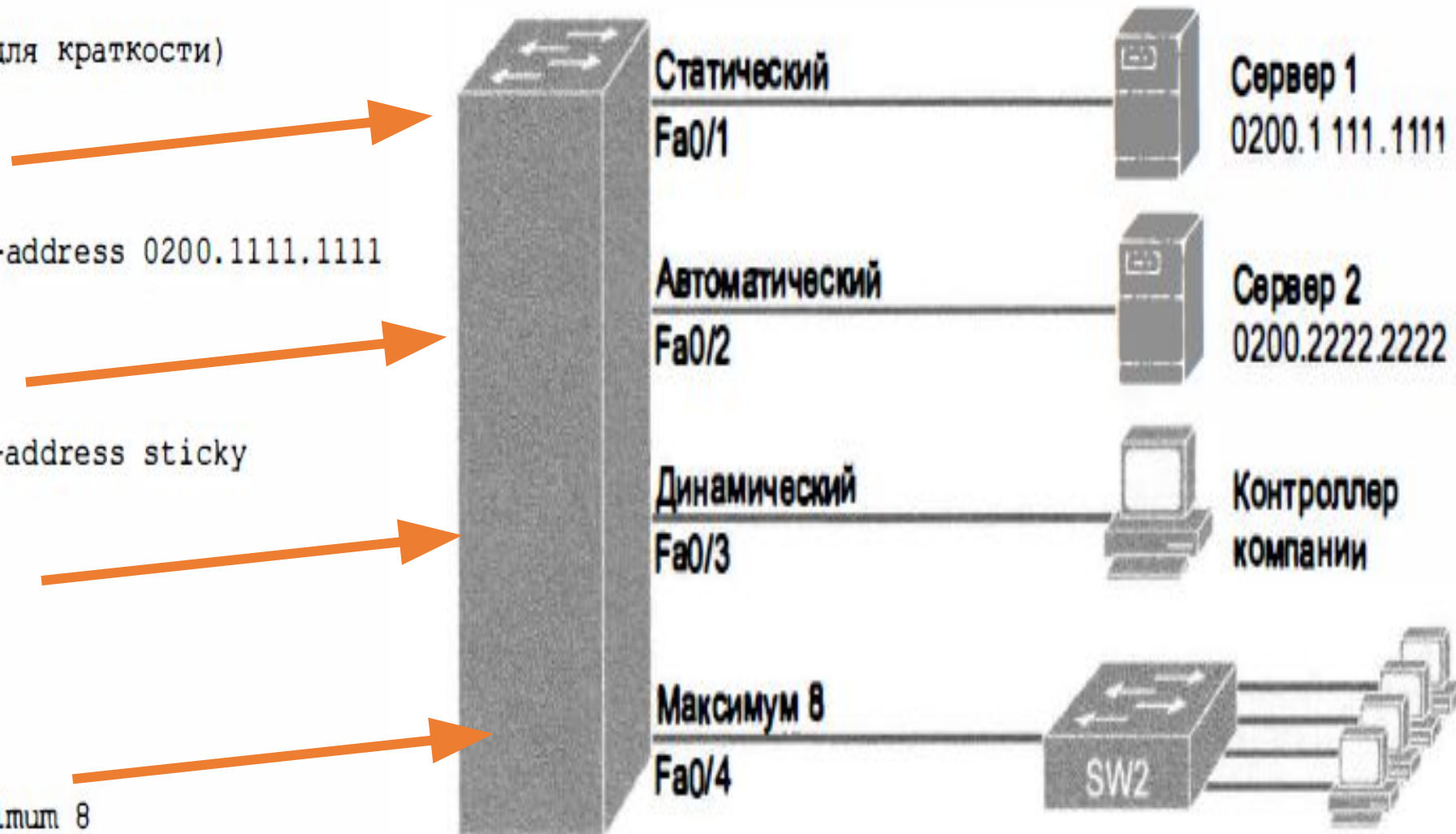
! (Часть конфигурации опущена для краткости)

```
interface FastEthernet0/1
  switchport mode access
  switchport port-security
  switchport port-security mac-address 0200.1111.1111
```

```
interface FastEthernet0/2
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
```

```
interface FastEthernet0/3
  switchport mode access
  switchport port-security
```

```
interface FastEthernet0/4
  switchport mode access
  switchport port-security
  switchport port-security maximum 8
```



Проверка защиты порта

```
SW1# show port-security interface fastEthernet 0/1
```

```
Port Security           : Enabled  
Port Status             : Secure-shutdown  
Violation Mode         : Shutdown  
Aging Time              : 0 mins  
Aging Type              : Absolute  
SecureStatic Address Aging : Disabled  
Maximum MAC Addresses  : 1  
Total MAC Addresses     : 1  
Configured MAC Addresses : 1  
Sticky MAC Addresses    : 0  
Last Source Address:Vlan : 0013.197b.5004:1  
Security Violation Count : 1
```

```
SW1# show port-security interface fastEthernet 0/2
```

```
Port Security           : Enabled  
Port Status             : Secure-up  
Violation Mode         : Shutdown  
Aging Time              : 0 mins  
Aging Type              : Absolute  
SecureStatic Address Aging : Disabled  
Maximum MAC Addresses  : 1  
Total MAC Addresses     : 1
```

```
Configured MAC Addresses : 1  
Sticky MAC Addresses     : 1  
Last Source Address:Vlan : 0200.2222.2222:1  
Security Violation Count : 0
```

```
SW1# show running-config
```

(строки опущены для краткости)

```
interface FastEthernet0/2  
  switchport mode access  
  switchport port-security  
  switchport port-security mac-address sticky  
  switchport port-security mac-address sticky 0200.2222.2222
```

Действия по защите порта

- Коммутатор может быть настроен так, чтобы использовать при нарушении безопасности одно из трех действий:

```
switchport port-security violation {protect | restrict | shutdown}
```

Параметр/Действие при нарушении безопасности	Защита (protect)	Ограничение (restrict)	Выключение (shutdown, стандартное действие)
Отбрасывание подозрительного трафика	Да	Да	Да
Отправка сообщения в системный журнал и через протокол SNMP	Нет	Да	Да
Выключение интерфейса и блокирование всего трафика	Нет	Нет	Да

Полезные команды

- **copy running-configuration startup-configuration (write, write memory, wr mem):**
 - ✓ Эта команда сохранит текущие модификации в настройках (running-configuration, которая хранится в RAM), в энергонезависимую RAM (NVRAM).
- **show interface:**
 - ✓ отображает состояние интерфейсов маршрутизатора.
- **show ip interface и show ip interface brief:**
 - предоставляет информацию о конфигурации и состоянии протокола IP и его службах на всех интерфейсах.
- **show vlan:**
 - ✓ Показать существующие vlan и привязку к ним физических интерфейсов.

Ключевые темы

Описание

Настройка простых паролей и имен хостов

Настройка на коммутаторе аутентификации по локальному имени пользователя и паролю

Этапы настройки протокола SSH на коммутаторе

Ключевые факты о командах `enable secret` и `enable password`

Команды буфера истории команд

Концепция виртуального интерфейса коммутатора (SVI)

Настройка IP-адреса и стандартного шлюза коммутатора

Настройка конфигурации коммутатора на изучение параметров IP в режиме клиента DHCP

Основные варианты защиты порта

Последовательность настройки защиты порта

Действия при нарушении защиты порта

Рекомендованные настройки неиспользуемых портов коммутатора
