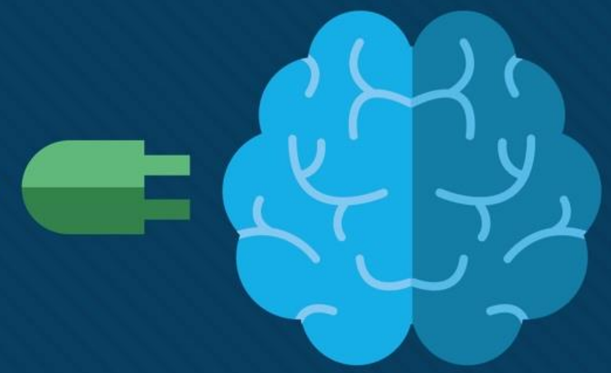


Модуль 11: Настройка параметров безопасности коммутатора

Switching, Routing and Wireless Essentials v7.0 (SRWE)

Module Objectives

Module Title: Switch Security Configuration

Module Objective: Configure switch security to mitigate LAN attacks

Topic Title	Topic Objective
Implement Port Security	Implement port security to mitigate MAC address table attacks.
Mitigate VLAN Attacks	Explain how to configure DTP and native VLAN to mitigate VLAN attacks.
Mitigate DHCP Attacks	Explain how to configure DHCP snooping to mitigate DHCP attacks.
Mitigate ARP Attacks	Explain how to configure ARP inspection to mitigate ARP attacks.
Mitigate STP Attacks	Explain how to configure PortFast and BPDU Guard to mitigate STP Attacks.

11.1 Обеспечение безопасности портов

Обеспечение безопасности портов
Защита неиспользуемых портов

Атаки 2-го уровня являются одними из самых простых для развертывания хакерами, но эти угрозы также можно нейтрализовать с помощью некоторых распространенных решений 2-го уровня.

- Перед введением коммутатора в эксплуатацию необходимо обеспечить безопасность всех портов (интерфейсов) коммутатора. Как порт будет защищен, зависит от его функции.
- Отключение неиспользуемых портов – это простой способ защиты сети от несанкционированного доступа, используемый многими администраторами. Перейдите к каждому неиспользуемому порту и выполните команду выключения Cisco IOS **shutdown**. Если порт необходимо активировать позднее, его можно включить с помощью команды **no shutdown**.
- Чтобы настроить для целого диапазона портов, используйте команду **interface range** command.

```
Switch(config)# interface range type module/first-number - last-number
```

Нейтрализация атак таблицы MAC-адресов

Самый простой и эффективный метод предотвращения атак переполнения таблицы MAC-адресов – это обеспечение безопасности порта.

- Данная функция ограничивает количество доступных MAC-адресов на один порт, а также это позволяет администратору вручную настраивать MAC-адреса для порта или разрешать коммутатору динамически изучать ограниченное количество MAC-адресов. Когда порт, сконфигурированный с защитой порта, получает кадр, MAC-адрес источника кадра сравнивается со списком MAC-адресов защищенного источника, которые были настроены или динамически изучены на порту.
- Ограничив число разрешенных MAC-адресов на порту одним адресом, можно использовать средства безопасности портов для контроля несанкционированного доступа к сети.

Включите защиту портов

Port security is enabled with the **switchport port-security** interface configuration command.

Обратите внимание, что в примере команда **switchport port-security** была отклонена. Это связано с тем, что безопасность портов можно настроить только на настроенных вручную портах доступа или настроенных вручную магистральных портах. По умолчанию, порты коммутатора уровня 2 настроены на динамический автоматический режим (транкинг включен). Поэтому, в примере порт настраивается с помощью команды настройки интерфейса **switchport mode access**.

Примечание: Безопасность магистрального порта выходит за рамки данного курса.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Включите защиту портов (Продолжение)

Используйте команду **show port-security interface** для отображения текущих настроек безопасности порта для FastEthernet 0/1.

- Обратите внимание на то, как включена защита порта, режим нарушения (the violation) отключен, и максимальное количество MAC-адресов равно 1.
- Если устройство подключено к порту, коммутатор автоматически добавит MAC-адрес устройства в качестве защищенного MAC-адреса. В этом примере ни одно устройство не подключено к порту.

Примечание: Если активный порт настроен с помощью команды **switchport port-security** и к этому порту подключено более одного устройства, порт перейдет в состояние error-disabled.

```
S1# show port-security interface f0/1
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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Включите защиту портов (Продолжение)

После включения защиты порта можно настроить другие особенности безопасности порта, как показано в примере.

```
S1(config-if)# switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
  <cr>
S1(config-if)# switchport port-security
```

Ограничение и изучение MAC-адресов

Для определения максимального числа MAC-адресов, разрешенных для конкретного порта, используем следующую команду:

```
Switch(config-if)# switchport port-security maximum value
```

- Значение безопасности по умолчанию равно 1.
- Максимальное количество защищенных MAC-адресов, которые можно настроить, зависит от коммутатора и IOS.
- В этом примере максимум составляет 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

Ограничение и изучение MAC-адресов (Продолжение)

Коммутатор может быть настроен на изучение MAC-адресов на защищенном порту одним из трех способов:

1. Вручную: Администратор вручную настраивает статический MAC-адрес(а) с помощью следующей команды для каждого безопасного MAC-адреса в порту:

```
Switch(config-if)# switchport port-security mac-address mac-address
```

2. Динамически изученный: Когда вводится команда **switchport port-security**, текущий MAC-адрес источника для устройства, подключенного к порту, автоматически защищается, но не добавляется в конфигурацию запуска. Если коммутатор перезагружен, порт должен будет повторно узнать MAC-адрес устройства.

3. Динамически изученный sticky MAC-адрес: Администратор может включить коммутатор для динамического изучения MAC-адреса и “привязать” их к работающей конфигурации с помощью следующей команды:

```
Switch(config-if)# switchport port-security mac-address sticky
```

Сохранение текущей конфигурации передаст динамически изученный MAC-адрес в NVRAM.

Обеспечение безопасности портов

Ограничение и изучение MAC-адресов (Продолжение)

В следующем примере демонстрируется полная конфигурация безопасности порта для FastEthernet 0/1.

- Администратор указывает максимум 4 MAC-адреса, вручную настраивает один безопасный MAC-адрес, а затем настраивает порт для динамического изучения дополнительных защищенных MAC-адресов до 4 максимум защищенных MAC-адресов.
- Используйте команды **show port-security interface** и **show port-security address** для проверки конфигурации.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                      (mins)
----    -----------       ----                          -----   -------------
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1         -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1#
```

Устаревание безопасности портов

Устаревание безопасности порта может использоваться для установки времени устаревания статических и динамических защищенных адресов на порту:

- **Абсолютный** - Защищенные адреса порта удаляются по истечении указанного времени устаревания.
- **По таймеру неактивности** - Защищенные адреса на порту удаляются, только если они неактивны в течение указанного времени.

Используйте устаревание для удаления защищенных MAC-адресов на защищенном порту без удаления существующих безопасных MAC-адресов вручную.

- Устаревание статически настроенных защищенных адресов может быть включено или отключено для каждого порта отдельно.

```
Switch(config-if)# switchport port-security aging {static | time time | type {absolute | inactivity}}
```

Используйте команду **switchport port-security aging**, чтобы включить или отключить статическое устаревание для защищенного порта или установить время или тип устаревания.

Устаревание безопасности портов (Продолжение)

В этом примере показано, как администратор настраивает тип устаревания на 10 минут бездействия.

Команда **show port-security** подтверждает изменения.

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
```

Режимы нарушения безопасности портов

Если MAC-адрес устройства, подключенного к порту, отличается от списка защищенных адресов, происходит нарушение (violation) порта.

- Чтобы установить режим нарушения безопасности порта, используйте следующую команду:

```
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}
```

В следующей таблице показано, как коммутатор реагирует в зависимости от настроенного режима нарушения.

Режим	Описание
shutdown (default)	Порт немедленно переходит в состояние отключения по ошибке, выключает светодиод порта и отправляет сообщение системного журнала. Для этого режима предусмотрено увеличение значения счетчика нарушений. Когда безопасный порт находится в состоянии отключения по ошибке, администратор должен повторно включить его, введя команды **shutdown** и **no shutdown**.
restrict (ограничение)	Порт отбрасывает пакеты с неизвестными адресами источника, пока вы не удалите достаточное количество безопасных MAC-адресов, чтобы опуститься ниже максимального значения или увеличить максимальное значение. Этот режим вызывает увеличение счетчика нарушений безопасности и генерирует сообщение системного журнала (syslog).
protect (защита)	Это наименее безопасный из режимов нарушения безопасности. Порт отбрасывает пакеты с неизвестными адресами источника, пока вы не удалите достаточное количество безопасных MAC-адресов, чтобы опуститься ниже максимального значения или увеличить максимальное значение. Нет сообщений системного журнала (syslog).

Режимы нарушения безопасности портов (Продолжение)

В следующем примере показано, как администратор изменил нарушение безопасности на “restrict”.

Выходные данные команды **show port-security interface** подтверждают, что изменение было внесено.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
S1#
```

Порт в состоянии отключения по ошибке

Когда порт отключен и переведен в состояние error-disabled, трафик на этот порт не отправляется и не принимается.

На консоли отображается ряд сообщений, связанных с безопасностью портов, как показано в следующем примере.

Примечание: Протокол порта и состояние соединения изменяются на “down”, а индикатор порта гаснет.

```
*Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting Fa0/18 in
err-disable state
*Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address 000c.292b.4c75 on port FastEthernet0/18.
*Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/18, changed state
to down
*Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Порт в состоянии отключения по ошибке (Продолжение)

- В этом примере команда **show interface** определяет состояние порта как **err-disabled**. Выходные данные команды **show port-security interface** теперь показывают состояние порта как **secure-shutdown**. Счетчик нарушений безопасности увеличивается на 1.
- Администратор должен определить причину нарушения безопасности. Если к безопасному порту подключено неавторизованное устройство, угроза безопасности устраняется до повторного включения порта.
- Чтобы повторно включить порт, сначала используйте команду **shutdown**, затем, используйте команду **no shutdown**, чтобы сделать порт работоспособным, как показано в примере.

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/18
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   : c025.5cd7.ef01:1
Security Violation Count   : 1
S1#
```

Проверка безопасности порта

После настройки функции безопасности портов на коммутаторе проверьте каждый интерфейс, чтобы убедиться в правильности настройки этой функции и статических MAC-адресов.

Используйте команду **show port-security** без ключевых слов, чтобы вывести параметры защиты порта для коммутатора.

- В примере показано, что все 24 интерфейса настроены с помощью команды **switchport port-security**, поскольку максимально допустимое значение равно 1, а режим нарушения shutdown.
- Следовательно, CurrentAddr (Count) равен 0 для каждого интерфейса.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1              1            0                  0         Shutdown
      Fa0/2              1            0                  0         Shutdown
      Fa0/3              1            0                  0         Shutdown
(output omitted)
     Fa0/24              1            0                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Проверка безопасности порта (Продолжение)

Используйте команду **show port-security interface** для просмотра сведений об определенном интерфейсе, как показано ранее и в этом примере.

```
S1# show port-security interface fastethernet 0/18
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   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
S1#
```

Проверка безопасности порта (Продолжение)

Чтобы убедиться, что MAC-адреса “прилипают” к конфигурации, используйте команду **show run**, как показано в примере для FastEthernet 0/19.

```
S1# show run | begin interface FastEthernet0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
(output omitted)
S1#
```

Проверка безопасности порта (Продолжение)

Чтобы отобразить все защищенные MAC-адреса, которые настроены вручную или динамически запоминаются на всех интерфейсах коммутатора, используйте команду **show port-security address**, как показано в примере.

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------
Vlan    Mac Address       Type             Ports     Remaining Age
                                                          (mins)
----    -----------       ----             -----     -------------
1       0025.83e6.4b01    SecureDynamic    Fa0/18          -
1       0025.83e6.4b02    SecureSticky     Fa0/19          -
------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Packet Tracer – Implement Port Security

In this Packet Tracer, you will complete the following objectives:

- Part 1: Configure Port Security
- Part 2: Verify Port Security

11.2 Нейтрализация атак на сети VLAN

Обзор атак на сети VLAN

В качестве краткого обзора, атака с переходом VLAN может быть запущена одним из трех способов:

- Подмена сообщений DTP от атакующего хоста, чтобы заставить коммутатор войти в режим транкинга. Отсюда злоумышленник может отправлять трафик, помеченный целевой VLAN, а затем коммутатор доставляет пакеты в пункт назначения.
- Представляем вредоносный коммутатор и включаем транкинг. Затем злоумышленник может получить доступ ко всем сетям VLAN на коммутаторе-жертве с вредоносного коммутатора.
- Другим типом атаки с переходом VLAN является атака с двойным тегированием (или двойной инкапсуляцией). Эта атака использует преимущества аппаратного обеспечения большинства коммутаторов.

Шаги, чтобы нейтрализовать атаки VLAN Hopping

Используйте следующие шаги, чтобы нейтрализовать атаки с переходом VLAN:

Шаг 1: Отключите согласование DTP (автоматические магистральные каналы) на немагистральных портах с помощью команды интерфейсной настройки **switchport mode access**.

Шаг 2: Отключите неиспользуемые порты и назначьте их неиспользуемой VLAN.

Шаг 3: Вручную включите магистральный канал на магистральном порту с помощью команды интерфейсной настройки **switchport mode trunk**.

Шаг 4: Отключите согласование DTP (автоматические магистральные каналы) на немагистральных портах с помощью команды интерфейсной настройки **switchport nonegotiate**.

Шаг 5: Установите для native VLAN, VLAN, отличную от VLAN 1, с помощью команды **switchport trunk native vlan** *vlan_number* command.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

11.3 Нейтрализация атак DHCP

Обзор атак DHCP

Цель атаки с истощением DHCP – создать отказ в обслуживании (DoS) для подключения клиентов.

Напомним, что атаки истощением DHCP могут быть эффективно нейтрализованы с помощью защиты портов, поскольку Gobbler использует уникальный MAC-адрес источника для каждого отправляемого запроса DHCP. Однако для нейтрализации атак подмены DHCP требуется больше защиты.

Gobbler может быть настроен на использование фактического MAC-адреса интерфейса в качестве адреса Ethernet источника, но при этом указать другой адрес Ethernet в полезной нагрузке DHCP пакета. Это сделало бы безопасность порта неэффективной, потому что MAC-адрес источника был бы легитимным.

Атаки DHCP-спуфинга можно предотвратить, используя анализ DHCP-трафика на доверенных портах.

DHCP Snooping

DHCP snooping фильтрует сообщения DHCP и объем DHCP трафика из ненадежных источников.

- Устройства, находящиеся под вашим административным контролем, такие как коммутаторы, маршрутизаторы и серверы, являются надежными источниками.
- Эти интерфейсы должны быть явно настроены как доверенные.
- Кроме того, все порты доступа, как правило, рассматривают как ненадежные источники.

Создается таблица DHCP, которая включает MAC-адреса источника устройства на ненадежном порту и IP-адрес, назначенный сервером DHCP этому устройству.

- MAC-адрес и IP-адрес связаны друг с другом.
- Поэтому эта таблица называется таблицей привязки отслеживания DHCP.

Шаги по реализации DHCP Snooping

Чтобы включить отслеживание DHCP, выполните следующие действия:

Шаг 1. Включите отслеживание DHCP с помощью команды глобальной конфигурации **ip dhcp snooping**.

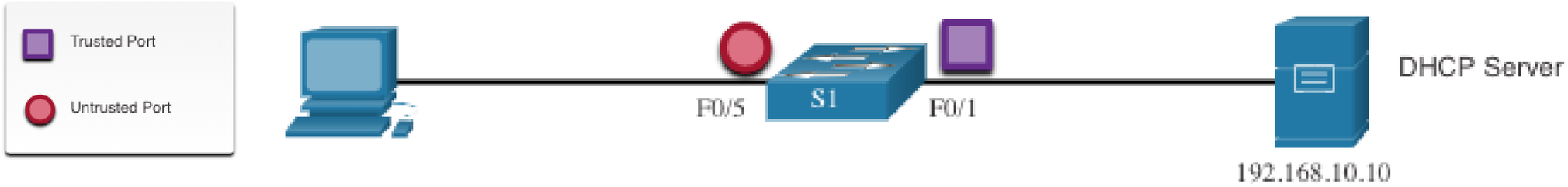
Шаг 2. На доверенных портах используйте команду настройки интерфейса **ip dhcp snooping trust**.

Шаг 3: Ограничьте число сообщений обнаружения DHCP, которые могут приниматься в секунду на ненадежных портах, с помощью команды настройки интерфейса **ip dhcp snooping limit rate** *packets-per-second*.

Шаг 4. Включите отслеживание DHCP по VLAN или по диапазону VLAN с помощью команды глобальной конфигурации **ip dhcp snooping** *vlan*.

DHCP Snooping пример конфигурации

Обратитесь к примеру топологии отслеживания DHCP с доверенными и ненадежными портами.



- DHCP snooping в начале включается на коммутаторе S1.
- Тогда вышестоящий интерфейс к серверу DHCP явно является доверенным.
- С F0/5 по F0/24 не надежные порты и, следовательно, скорость ограничена шестью пакетами в секунду.
- Наконец, отслеживание DHCP включено в VLAN 5, 10, 50, 51, и 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

DHCP Snooping пример конфигурации (Продолжение)

Используйте команду **show ip dhcp snooping** в привилегированном режиме для проверки настроек DHCP snooping.

Используйте команду **show ip dhcp snooping binding** для просмотра клиентов, которые получили информацию DHCP.

Примечание: Отслеживание DHCP также требуется для проверки динамического ARP (DAI), которая является следующей темой.

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5            no         no              6
  Custom circuit-ids:
FastEthernet0/6            no         no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec) Type           VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:03:47:B5:9F:AD  192.168.10.10   193185     dhcp-snooping 5    FastEthernet0/5
```

11.4 Нейтрализация ARP атак

Нейтрализация ARP атак

Dynamic ARP Inspection

В типичной атаке ARP субъект угрозы может отправлять незапрошенные ответы ARP другим узлам в подсети с MAC-адресом субъекта угрозы и IP-адресом шлюза по умолчанию. Чтобы предотвратить подделку ARP и вызванное ею отравление ARP, коммутатор должен обеспечить передачу только действительных запросов и ответов ARP.

Динамическая проверка ARP (DAI) требует отслеживания DHCP и помогает предотвратить атаки ARP путем:

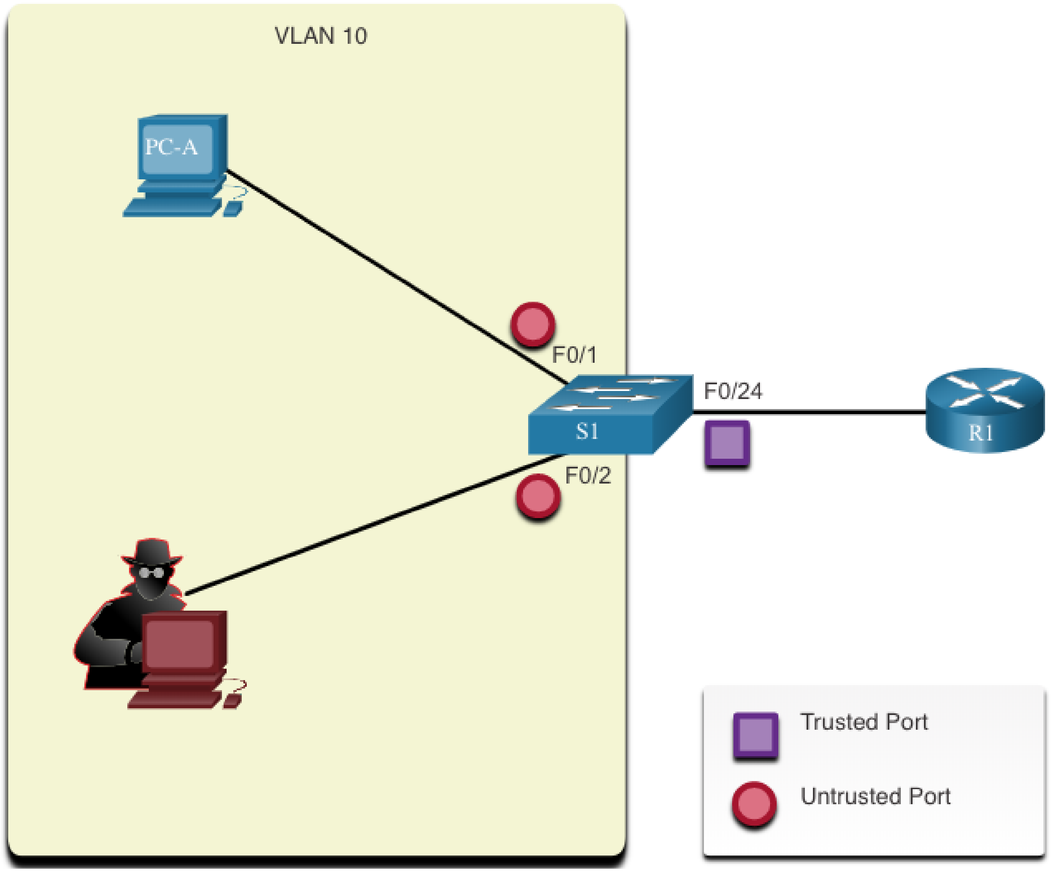
- Не ретранслирует недопустимые или незапрошенные ответы ARP на другие порты в той же VLAN.
- Перехват всех ARP-запросов и ответов на ненадежных портах.
- Проверка каждого перехваченного пакета на предмет правильной привязки IP-к-MAC.
- Удаление и регистрация ARP-ответов, поступающие из недействительных, чтобы предотвратить отравление ARP.
- Ошибка отключения интерфейса, если настроенное число DAI пакетов ARP превышено.

Руководство по внедрению DAI

Чтобы снизить вероятность подделки ARP и отравления ARP, выполните следующие рекомендации по внедрению DAI:

- Включите отслеживание DHCP на глобальном уровне.
- Включите отслеживание DHCP на выбранных VLANs.
- Включите DAI на выбранных VLANs.
- Настройте доверенные интерфейсы для отслеживания DHCP и проверки ARP.

Как правило, рекомендуется настроить все порты коммутатора доступа как ненадежные и настроить все порты связывающие с вышестоящими устройствами, как доверенные.



DAI пример конфигурации

В предыдущей топологии, S1 соединяет двух пользователей в VLAN 10.

- DAI будет настроен для защиты от спуфинга ARP и атак отравления ARP.

- Как показано в примере, отслеживание DHCP включено, поскольку DAI требует для работы таблицы привязки отслеживания DHCP.
- Далее, отслеживание DHCP и проверка ARP включены для ПК в VLAN10.
- Порт аплинк связи с маршрутизатором является доверенным, и поэтому он настроен как доверенный для отслеживания DHCP и проверки ARP.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

DAI пример конфигурации (Продолжение)

DAI также можно настроить для проверки MAC-адресов и IP-адресов назначения или источника:

- **Destination MAC** - Проверяет MAC-адрес назначения в заголовке Ethernet по отношению к целевому MAC-адресу в теле ARP.
- **Source MAC** - Проверяет MAC-адрес источника в заголовке Ethernet на соответствие MAC-адреса отправителя в теле ARP.
- **IP address** - Проверяет тело ARP на наличие недопустимых и неожиданных IP-адресов, включая адреса 0.0.0.0, 255.255.255.255, и все IP-адреса многоадресной рассылки.

DAI пример конфигурации (Продолжение)

Команда глобальной конфигурации **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} используется для настройки DAI для отбрасывания пакетов ARP, когда IP-адреса недопустимы.

- Он может использоваться, когда MAC-адреса в теле пакетов ARP не совпадают с адресами, указанными в заголовке Ethernet.
- Обратите внимание, что в следующем примере можно настроить только одну команду.
  - Поэтому при вводе нескольких команд проверки **ip arp inspection validate** проверяет предыдущую команду.
  - Чтобы включить более одного метода проверки, введите их в той же командной строке, как показано и проверено в следующих выходных данных.

```
S1(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

11.5 Нейтрализация STP атак

Нейтрализация STP атак

PortFast и BPDU Guard

Напомним, что сетевые злоумышленники могут манипулировать протоколом Spanning Tree Protocol (STP) для проведения атаки путем подмены корневого моста и изменения топологии сети.

Чтобы нейтрализовать атаки манипуляций с протоколом STP, используйте средства защиты PortFast и Bridge Protocol Data Unit (BPDU) Guard:

PortFast

- PortFast немедленно переводит интерфейс, настроенный как порт доступа или магистральный порт, в состояние пересылки из состояния блокировки, минуя состояния прослушивания и обучения.
- Применять ко всем портам конечного пользователя.

BPDU Guard

- BPDU guard – защита BPDU немедленно при ошибке отключает порт, который получает BPDU.
- Как и PortFast, защита BPDU guard должна быть настроена только на интерфейсах, подключенных к конечным устройствам.

Нейтрализация STP атак

Конфигурация PortFast

PortFast обходит состояния прослушивания и обучения STP, чтобы минимизировать время, в течение которого порты доступа должны ожидать конвергенции STP.

- Технология PortFast включается только на портах доступа.
- PortFast на межкоммутаторных каналах может создать петлю STP.

PortFast может быть включен:

- **На интерфейсе** – с помощью команды настройки интерфейса **spanning-tree portfast**.
- **Глобально** – с использованием команды интерфейса **spanning-tree portfast default**, чтобы глобально включить защиту BPDU на всех портах с включенным PortFast.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
```

Конфигурация PortFast (Продолжение)

Чтобы проверить, включен ли PortFast глобально, вы можете использовать:

- Команда **show running-config | begin span**
- Команда **show spanning-tree summary**

Чтобы проверить, включен ли PortFast для интерфейса, используйте команду **show running-config interface** *type/number,* как показано в следующем примере.

Команда проверки типа/номера интерфейса **show spanning-tree interface** *type/number* **detail** также может использоваться для проверки.

Нейтрализация STP атак

Конфигурация BPDU Guard

Порт доступа может получить неожиданные BPDU случайно или из-за того, что пользователь подключил неавторизованный коммутатор к порту доступа.

- Если какие-либо BPDU получены на порте с поддержкой BPDU Guard, этот порт переводится в состояние с ошибками.
- Это означает, что порт отключен и должен быть повторно включен вручную или автоматически восстановлен с помощью глобальной команды **errdisable recovery cause psecure_violation**.

BPDU Guard можно включить:

- **На интерфейсе** – Используя команду в режиме конфигурации интерфейса **spanning-tree bpduguard enable**.
- **Глобально** – Используя команду глобальной конфигурации **spanning-tree portfast bpduguard default,** чтобы глобально включить защиту BPDU на всех портах с включенным PortFast.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

11.6 Module Practice and Quiz

Packet Tracer – Switch Security Configuration

In this Packet Tracer activity, you will:

- Secure unused ports
- Implement port security
- Mitigate VLAN hopping attacks
- Mitigate DHCP attacks
- Mitigate ARP attacks
- Mitigate STP attacks
- Verify the switch security configuration

Lab – Switch Security Configuration

In this lab, you will:

- Secure unused ports
- Implement port security
- Mitigate VLAN hopping attacks
- Mitigate DHCP attacks
- Mitigate ARP attacks
- Mitigate STP attacks
- Verify the switch security configuration

What Did I Learn In This Module?

- All switch ports (interfaces) should be secured before the switch is deployed for production use.
- By default, Layer 2 switch ports are set to dynamic auto (trunking on).
- The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security.
- The switch can be configured to learn about MAC addresses on a secure port in one of three ways: manually configured, dynamically learned, and dynamically learned – sticky.
- If the MAC address of a device attached to the port differs from the list of secure addresses, then a port violation occurs. By default, the port enters the error-disabled state. When a port is placed in the error-disabled state, no traffic is sent or received on that port.
- Mitigate VLAN Hopping attacks by disabling DTP negotiations, disabling unused ports, manually setting trunking where required, and using a native VLAN other than VLAN 1.

What Did I Learn In This Module? (Cont.)

- The goal of a DHCP starvation attack is to create a Denial of Service (DoS) for connecting clients. DHCP spoofing attacks can be mitigated by using DHCP snooping on trusted ports.
- DHCP snooping determines whether DHCP messages are from an administratively-configured trusted or untrusted source. It then filters DHCP messages and rate-limits DHCP traffic from untrusted sources.
- Dynamic ARP inspection (DAI) requires DHCP snooping and helps prevent ARP attacks by verifying ARP traffic.
- Implement Dynamic ARP Inspection to mitigate ARP spoofing and ARP poisoning.
- To mitigate Spanning Tree Protocol (STP) manipulation attacks, use PortFast and Bridge Protocol Data Unit (BPDU) Guard.


CISCO