
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Правила вебинара

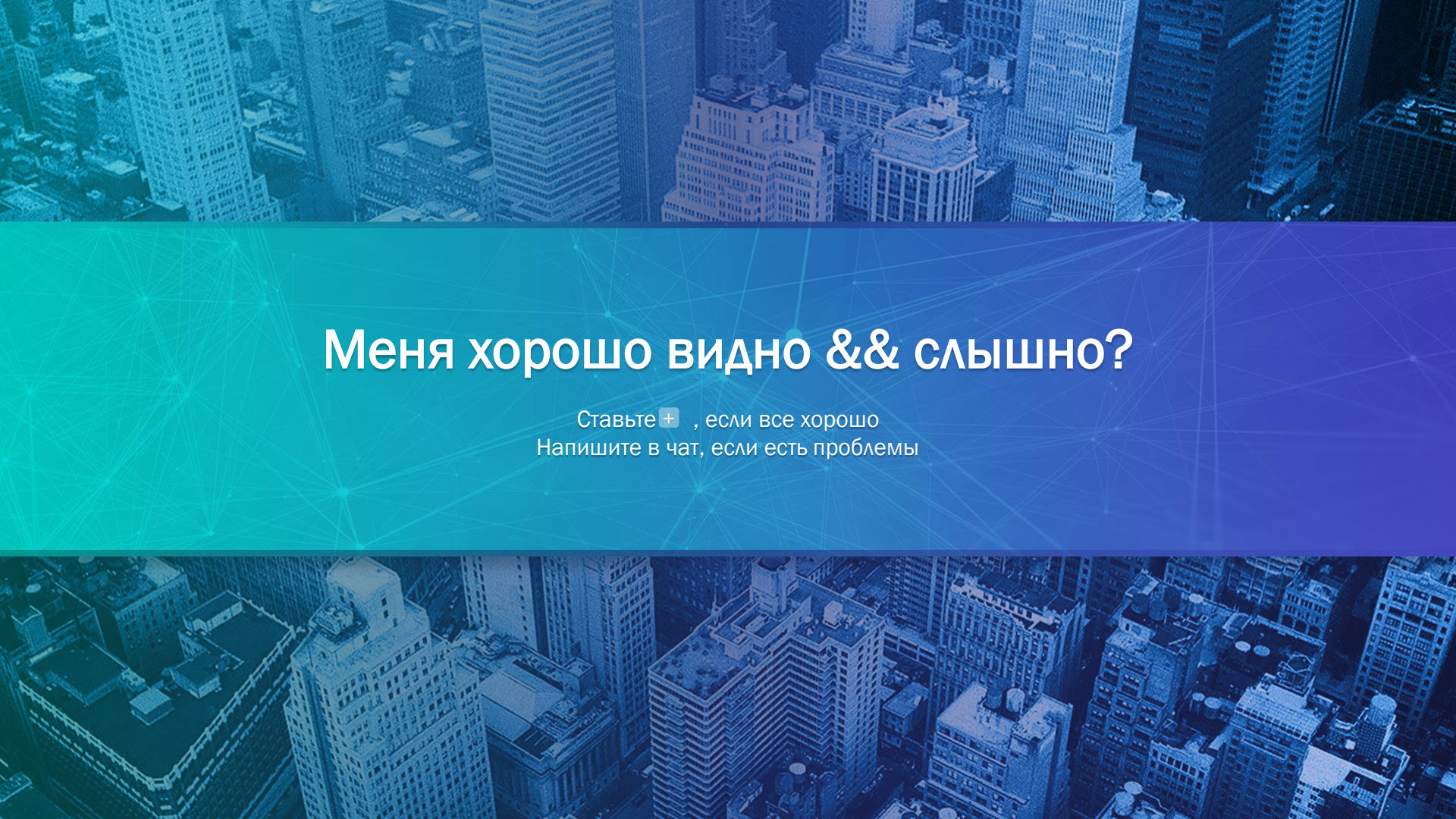
Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Не забыть включить запись!



Меня хорошо видно && слышно?

Ставьте + , если все хорошо
Напишите в чат, если есть проблемы

L2 Security

Рукин Андрей
преподаватель
cisco@sk12.ru

Карта курса


5 Проектная работа
1 Масштабирование сетей
3 Протокол BGP
2 Протоколы маршрутизации IGP
4 Управление и защита сетевой инфраструктуры

УГРОЗЫ БЕЗОПАСНОСТИ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

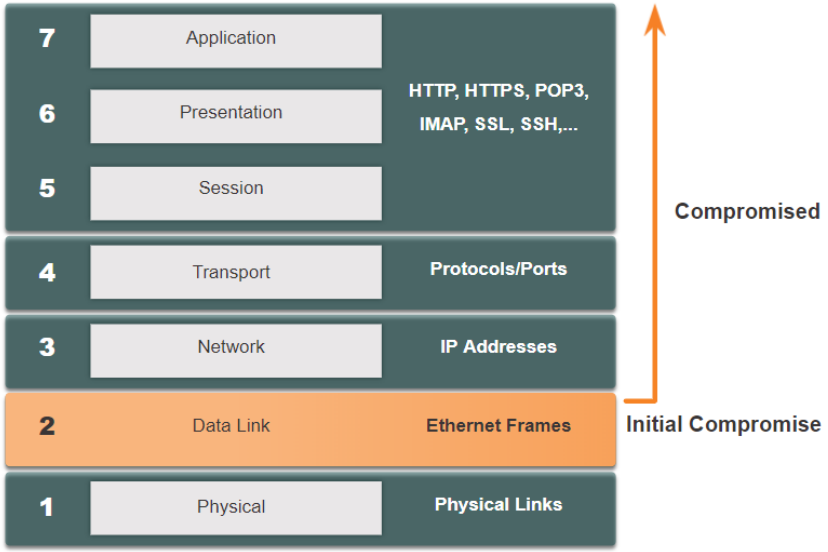
Угрозы безопасности на L2

Уязвимости на уровне 2

Сетевые администраторы регулярно внедряют решения безопасности для защиты элементов от уровня 3 до уровня 7.

Они используют VPN, межсетевые экраны и устройства IPS для защиты этих элементов. Однако, нарушение системы безопасности на уровне 2 также повлияет и на все уровни выше.

Например, если исполнитель угрозы с доступом к внутренней сети захватил кадры уровня 2, то вся защита, реализованная на уровнях выше, будет бесполезной. Атакующий может нанести большой ущерб сетевой инфраструктуре LAN 2-го уровня.



Категории атак на коммутацию

Уровень безопасности определяется наиболее уязвимым звеном системы, которым в данном случае является 2-й уровень.

Это связано с тем, что локальные сети традиционно находились под административным контролем единственной организации. Мы внутренне доверяли всем лицам и устройствам, подключенным к локальной сети.

Категория	Примеры
Атака на таблицу MAC	Включает в себя атаки с переполнением таблицы CAM
Атаки на сети VLAN	Включат в себя атаки с переходам по VLAN и с двойным тегированием VLAN Так же это включает себя атаки между устройствами в общей VLAN
Атаки, связанные с DHCP	Включает спуфинг и атаку истощения ресурсов DHCP
ARP атаки	Включает атаки подмены ARP и и «отравление» ARP-кэша.
Атаки с подменой адреса	Включает атаки подмены MAC и IP адресов
Атака STP	Включает в себя атаки путем манипуляции протокола STP

Технологии нейтрализации атак на коммутацию

Решение	Описание
Безопасность портов	Предотвращает многие типы атак, включая атаки с переполнением CAM таблицы MAC-адресами
Отслеживание DHCP-сообщений	Предотвращает истощение ресурсов DHCP и DHCP-спуфинг.
Динамический анализ ARP-трафика	Предотвращает ARP-спуфинг и «отравление» ARP-кэша.
Функция защиты от подмены IP-адреса отправителя (IP Source Guard)	Предотвращает атаки спуфингом MAC-адресов и IP-адресов.

Эти решения уровня 2 не будут эффективными, если протоколы управления не защищены. Рекомендуются следующие стратегии:

- Всегда используйте безопасные варианты этих протоколов, такие как SSH, протокол защищенного копирования (SCP), защищенный FTP (SFTP) и (SSL / TLS).
- Рассмотрите возможность использования сети внешнего управления для управления устройствами.
- Используйте выделенную сеть управления VLAN, по которой передается только трафик управления.
- Используйте списки контроля доступа для фильтрации несанкционированного доступа.

Атака на таблицу MAC-адресов

Обзор работы коммутатора

Для принятия решений о переадресации коммутатор LAN уровня 2 создает таблицу на основе MAC-адресов источника в принятых кадрах. Это называется таблица MAC-адресов. Таблицы MAC-адресов хранятся в памяти и используются для более эффективной пересылки кадров.

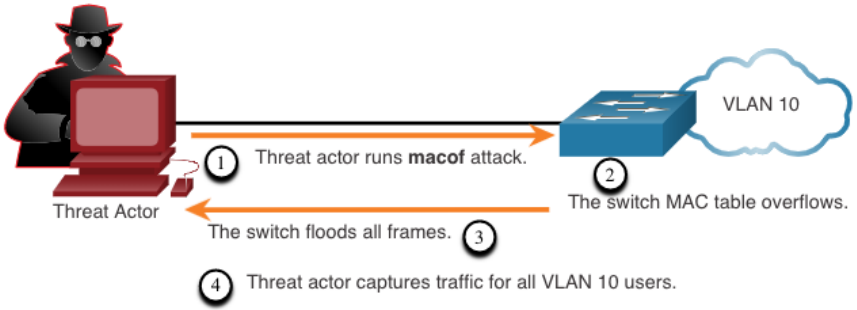
```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

Атака переполнением на таблицу MAC-адресов

Все таблицы MAC имеют фиксированный размер, и, следовательно, коммутатор может исчерпать ресурсы для хранения MAC-адресов. Атаки с переполнением таблицы MAC-адресов используют это ограничение, отправляя фиктивные MAC-адреса источника, до тех пор, пока таблица MAC-адресов коммутатора не заполнится и коммутатор не сможет правильно работать дальше.

Когда это происходит, коммутатор обрабатывает кадр как неизвестную одноадресную рассылку и начинает пересылать весь входящий трафик из всех портов в той же VLAN без учета таблицы MAC. Это условие теперь позволяет атакующему захватить все кадры, отправленные с одного хоста на другой в локальной сети или локальной сети VLAN.

Примечание: трафик лавинообразно пересылается только внутри локальной сети или VLAN Злоумышленник может захватывать трафик только в локальной сети или VLAN, к которой подключен исполнитель угрозы.



Нетрализация атаки переполнением на таблицу MAC-адресов

Что делает такие инструменты, как **macof**, настолько опасными, так это то, что злоумышленник может очень быстро создать атаку переполнения таблицы MAC. Например, коммутатор Catalyst 6500 может хранить 132 000 MAC-адресов в своей таблице MAC-адресов Такой инструмент, как **macof** , может переключать скорость до 8000 поддельных кадров в секунду; создать атаку переполнения таблицы MAC-адресов за несколько секунд.

Другая причина, по которой эти инструменты атаки опасны, заключается в том, что они не только влияют на локальный коммутатор, но и на другие подключенные коммутаторы уровня 2. Когда таблица MAC-адресов коммутатора заполнена, она начинает заполнять все порты, включая те, которые подключены к другим коммутаторам уровня 2.

Чтобы нейтрализовать атаки переполнения таблицы MAC-адресов, сетевые администраторы должны реализовать защиту портов (Port security). Защита порта позволит узнать только определенное количество исходных MAC-адресов порта. Безопасность порта дополнительно обсуждается в другом модуле.

Атаки на локальную сеть

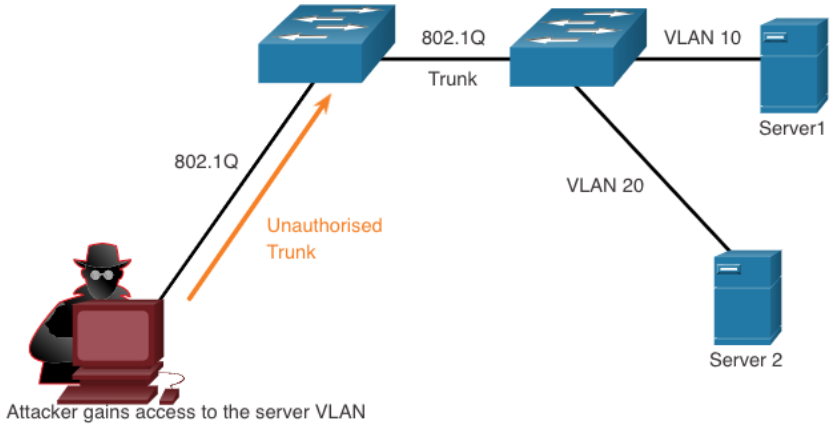
VLAN и DHCP-атаки

- Атака VLAN Hopping
- Атака с двойным тегированием (Double-Tagging) VLAN
- Атака истощением DHCP-пула
- DHCP-спуфинг.

Атака VLAN Hopping

VLAN hopping позволяет видеть трафик из одной VLAN в другой VLAN без помощи маршрутизатора.

В базовой атаке VLAN hopping, атакующий настраивает узел так, чтобы он действовал как коммутатор, чтобы использовать функцию автоматического согласования магистрального порта включенную по умолчанию на большинстве портов коммутатора.

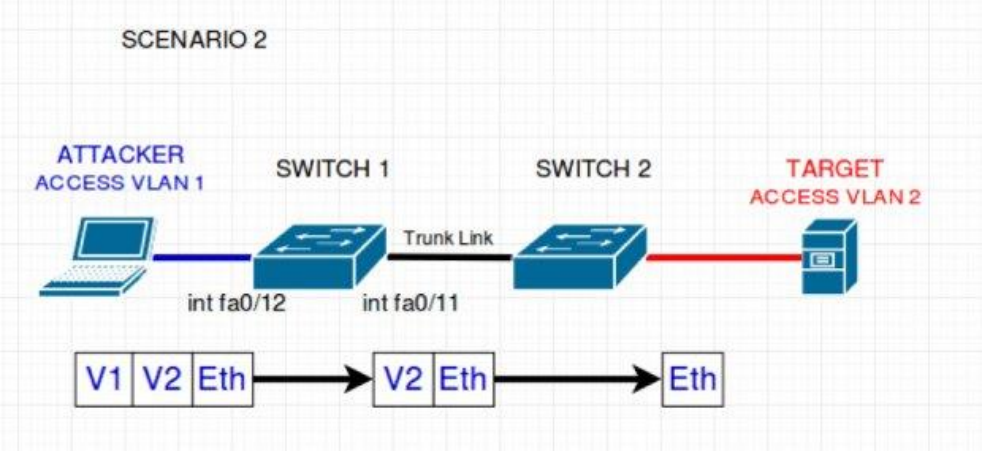


Атака VLAN Hopping

Благодаря этому в некоторых случаях злоумышленник может встроить внутрь кадра скрытый тег 802.1Q в кадр который уже имеет 802.1Q тег. Этот тег позволяет кадру попасть во VLAN, которую не определяет исходный тег 802.1Q

- **Шаг 1:** Злоумышленник передает коммутатору кадр 802.1Q с двойным тегированием. Внешний заголовок имеет тег принадлежащей злоумышленнику сети VLAN, которая совпадает с нативной VLAN магистрального порта.
- **Шаг 2:** Кадр поступает в первый коммутатор, который видит первый 4-байтовый тег 802.1Q. Коммутатор видит, что кадр предназначен для native VLAN. Коммутатор рассылает пакет через все порты native VLAN , отбросив тег native VLAN . В магистральном порте тег VLAN 10 отброшен, но новый тег не присваивается, поскольку это часть сети native VLAN. На этом этапе внутренний тег VLAN все еще не поврежден и не был проверен первым коммутатором.
- **Шаг 3**: Кадр поступает во второй коммутатор, но он не имеет информации о том, что он предназначен для native VLAN. Трафик native VLAN не тегируется передающим коммутатором в соответствии со спецификацией протокола 802.1Q. Второй коммутатор видит только внутренний тег 802.1Q, который передал злоумышленник, и понимает, что кадр адресован целевой VLAN. Второй коммутатор пересылает кадр в порт-жертву или рассылает его по всем портам в зависимости от того, существует ли запись в таблице MAC-адресов для хоста-жертвы.

Атака VLAN Hopping

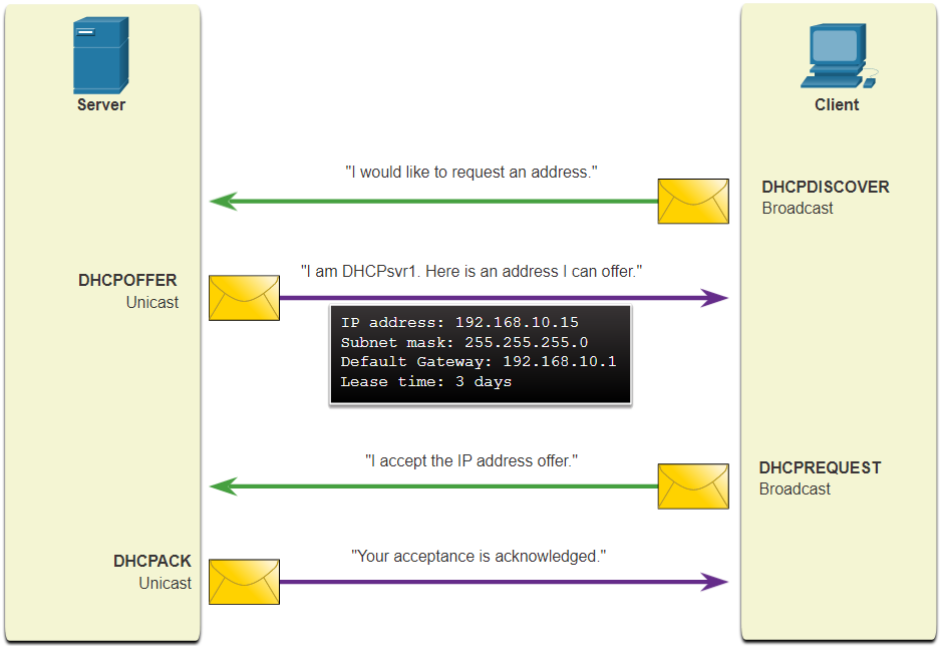


Атаки VLAN hopping и двойной маркировкой VLAN могут быть предотвращены путем реализации следующих рекомендаций по безопасности магистральных каналов, как обсуждалось в предыдущем модуле:

- Отключить транкинг на всех портах доступа.
- Отключить автосогласование транкинга (DTP). Только ручная настройка.
- Убедитесь, что native VLAN используется только для магистральных каналов.

DHCP Сообщения

Серверы DHCP динамически предоставляют клиентам сведения о конфигурации IP, включая IP-адрес, маску подсети, шлюз по умолчанию, DNS-серверы и так далее. Обзор последовательности DHCP сообщений между клиентом и сервером показан на рисунке.



Атаки на системы информационной безопасности локальной сети Атаки с использованием DHCP

Два типа атак DHCP - это истощение DHCP и DHCP spoofing. Обе атаки нейтрализуются за счет реализации DHCP snooping.

- **Цель атаки с истощение DHCP -** создать отказ в обслуживании (DoS) для подключения клиентов. Для атаки путем истощения ресурсов DHCP необходим специальный инструмент, например Gobbler. Gobbler способен искать все доступные для аренды IP-адреса и пытается все их арендовать. В частности, он создает сообщения DHCP Discovery с поддельными MAC-адресами.
- **Атака типа «DHCP-спуфинг»** состоит в том, что к сети подключается мошеннический DHCP-сервер и предоставляет ложные параметры настройки IP легитимным клиентам. Подставной сервер может предоставлять различные неправильные сведения.
  - **Неправильный шлюз по умолчанию** - Злоумышленник предоставляет неправильный шлюз или IP-адрес своего хоста для создания атаки через посредника. Это может пройти полностью незамеченным, поскольку злоумышленник перехватывает поток данных в сети.
  - **Неправильный DNS-сервер.** Хакер предоставляет неправильный адрес DNS-сервера, направляя пользователя на вредоносный веб-сайт.
  - **Неправильный IP-адрес -** Злоумышленник сообщает неправильный IP-адрес шлюза по умолчанию и создает DoS-атаку на DHCP-клиента.

ARP-атаки, STP-атаки и CDP-зондирование

- Атаки ARP спуфинга
- ARP Отравление
- Атака STP
- Разведывательная атака CDP

Атаки с использованием ARP

- Хосты передают ARP-запрос в широковещательном режиме другим хостам в сегменте, чтобы определить MAC-адрес хоста с конкретным IP-адресом. Все хосты в подсети получают и обрабатывают этот ARP-запрос. Хост с IP-адресом, соответствующим ARP-запросу, отправляет ARP-ответ.
- Любой клиент может отправить незапрашиваемый ARP-ответ, который называется gratuitous ARP (самообращенный ARP). Когда хост отправляет самообращенный ARP, другие хосты в подсети сохраняют в своих ARP-таблицах MAC-адрес и IP-адрес, содержащиеся в этом ответе.
- Проблема заключается в том, что злоумышленник может отправить коммутатору сообщение gratuitous ARP, содержащее поддельный MAC-адрес, и коммутатор соответствующим образом обновит свою таблицу MAC-адресов. В типичной атаке субъект угрозы может отправлять незапрошенные ответы ARP другим узлам в подсети с MAC-адресом субъекта угрозы и IP-адресом шлюза по умолчанию.
- В Интернете доступно множество инструментов для организации атак через посредника с использованием ARP.
- IPv6 использует протокол обнаружения соседей ICMPv6 для разрешения адресов уровня 2. IPv6 включает в себя стратегии по нейтрализации подмены объявления соседей (Neighbor Advertissement), подобным образом IPv6 предотвращает поддельный ARP-ответ.
- Атаки ARP спуфинга и «отравление» ARP-кэша нейтрализуются путем внедрения DAI.

Атаки с подменой адреса

- Подмена IP-адреса - это действие, когда злоумышленник перехватывает действительный IP-адрес другого устройства в подсети или использует случайный IP-адрес. Подмену IP-адреса трудно нейтрализовать, особенно когда он используется внутри подсети, которой принадлежит IP-адрес.
- Злоумышленники изменяют MAC-адрес своего хоста в соответствии с другим известным MAC-адресом целевого хоста. Коммутатор перезаписывает текущую запись в таблице CAM и назначает MAC-адрес новому порту. Затем он пересылает кадры, предназначенные для целевого хоста, на атакующий хост.
- Когда целевой хост отправляет трафик, коммутатор исправит ошибку, переназначив MAC-адрес на исходный порт. Чтобы не дать коммутатору вернуть назначение порта в правильное состояние, злоумышленник может создать программу или сценарий, который будет постоянно отправлять кадры коммутатору, чтобы коммутатор сохранял неверную или поддельную информацию.
- На уровне 2 нет механизма безопасности, который позволял бы коммутатору проверять источник MAC-адресов, что делает его таким уязвимым для атак спуфинга.
- Атаки подмены IP и MAC-адресов может быть уменьшена путем внедрения IPSG.

Атаки с использованием STP

- Сетевые злоумышленники могут манипулировать протоколом связующего дерева (STP) для проведения атаки путем подмены корневого моста и изменения топологии сети. Затем злоумышленники могут захватить весь трафик для домена с немедленной коммутацией.
- Для проведения атак путем манипуляций STP хост злоумышленника передает широковещательные пакеты BPDU с информацией об изменении конфигурации и топологии STP, чтобы вызвать перерасчет связующего дерева. Передаваемые хостом злоумышленника пакеты BPDU объявляют о более низком значении приоритета моста для попытки избрания хоста корневым мостом.
- Эта STP-атака нейтрализуется за счет реализации BPDU Guard на всех портах доступа.

Разведывательные атаки на CDP

Протокол Cisco Discovery Protocol (CDP) — это проприетарный протокол обнаружения канала уровня 2. Он включен на всех устройствах Cisco по умолчанию. Сетевые администраторы также используют протокол CDP для настройки сетевых устройств и для поиска и устранения их неполадок. Информация протокола CDP отправляется через порты с поддержкой CDP в периодических незашифрованных широковещательных рассылках. Данные протокола CDP включают IP-адрес устройства, версию ОС IOS, а также сведения о платформе, возможностях и VLAN с нетегированным трафиком. Устройство, получившее сообщение CDP, обновляет свою базу данных CDP.

Чтобы минимизировать вероятность использования CDP злоумышленниками, ограничьте использование протокола CDP на устройствах или портах. Например, отключите CDP на пограничных портах, которые подключаются к недоверенным устройствам.

- Чтобы полностью отключить протокол CDP на устройстве, используйте команду **no cdp run** режима глобальной конфигурации. Чтобы полностью включить протокол CDP, используйте команду **cdp run** режима глобальной настройки.
- Чтобы отключить CDP для порта, используйте команду конфигурации интерфейса **no cdp enable.** Чтобы включить CDP для порта, используйте команду конфигурации интерфейса **cdp enable.**

Примечание: Протокол LLDP тоже уязвим к разведывательным атакам. Чтобы полностью отключить протокол LLDP, настройте режим **no lldp run**. Чтобы отключить протокол LLDP на интерфейсе, настройте режимы **no lldp transmit** а и **no lldp receive**.

Обеспечение безопасности портов

Безопасность портов коммутатора Защита неиспользуемых портов

Атаки 2-го уровня являются одними из самых простых для развертывания хакерами, но эти угрозы также можно смягчить 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

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

- Чтобы настроить для целого диапазона портов, используйте команду **interface range.**

Нейтрализация атак таблицы MAC-адресов

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

- Данная функция ограничивает количество допустимых MAC-адресов на один порт, а также Функции безопасности портов позволяют администратору статически указывать MAC-адреса для порта или разрешать коммутатору динамически определять ограниченное число 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 изучен на порту.
- Ограничив число разрешенных MAC-адресов на порту одним адресом, можно использовать средства безопасности портов для контроля несанкционированного расширения сети.

Включение безопасности порта

Безопасность порта включается с помощью команды настройки интерфейса **switchport port-security.**

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#
```

Включение безопасности порта (продолжение)

Используйте команду **show port-security interface** для отображения текущих настроек безопасности порта для FastEthernet 0/1, как показано в примере.

- Обратите внимание на то, как включена защита порта, режим нарушения (violation mode) отключен, и максимальное количество MAC-адресов равно 1.
- Если устройство подключено к порту, коммутатор автоматически добавит MAC-адрес устройства в качестве защищенного MAC-адреса. In this example, no device is connected to the port.

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#
```

Включение безопасности порта (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 порта 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

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

1. Ручная конфигруация: 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. Динамическое изучение: 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. Динамическое изучение – Sticky: Администратор может включить коммутатор для динамического изучения MAC-адреса и «привязать» его 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.

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#
```

Безопасность порта - устаревание данных

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 -**безопасные 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 безопасных 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.

Безопасность порта - устаревание данных (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
```

Безопасность портов коммутатора Безопасность портов: режимы реагирования на нарушения

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 следующих таблицах 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 счётчика 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).

Безопасность портов: режимы реагирования на нарушения (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 (придолжение)

- 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.** 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 **switch-port 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#
```

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 со 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 mode access.

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

```
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#
```

Нейтрализация атак DHCP

Обзор атак на сети VLAN

Цель атаки с истощение DHCP - создать отказ в обслуживании (DoS) для подключения клиентов.

Напомним, что атаки истощение 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

Чтобы включить отслеживание DHCP, выполните следующие действия:

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

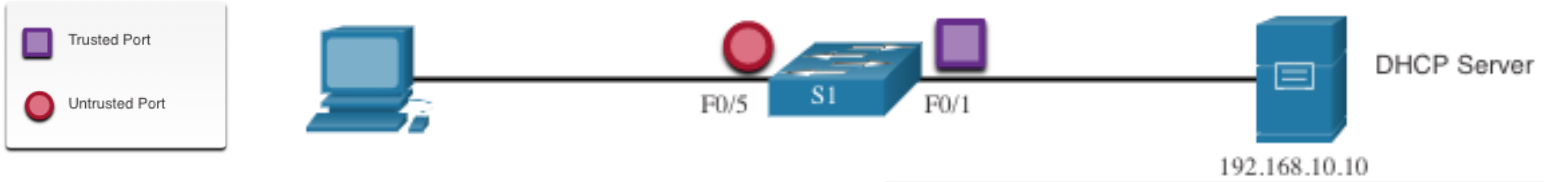
Шаг 2. На доверенных портах используйте команду настройки интерфейса **ip dhcp snooping trust.**

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.**

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

DHCP Snooping пример конфигруации

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 конфигруации

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
```

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:

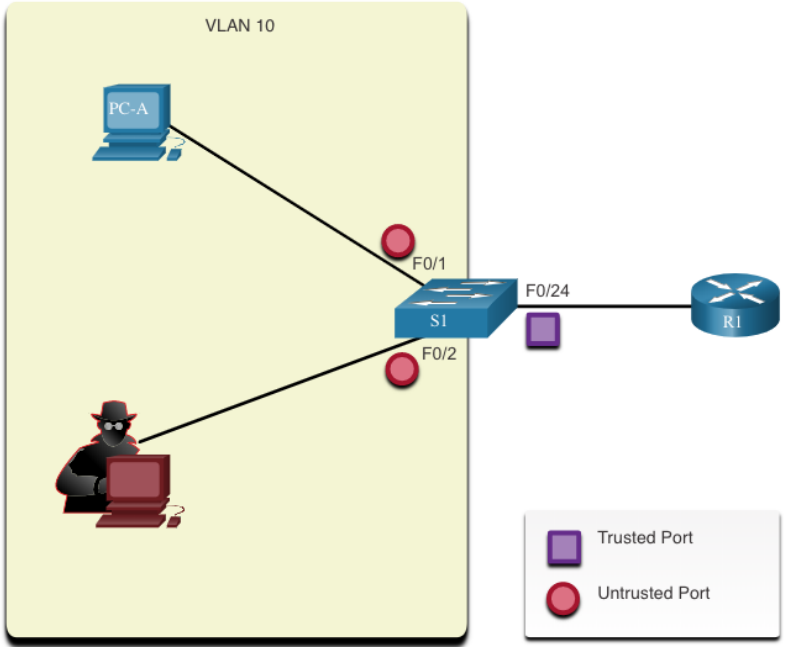
- Не ретранслирует недопустимые или незапрошенные ответы ARP на другие порты в той же VLAN.
- Перехват всех ARP-запросов и ответов на ненадежных портах.
- Проверка каждого перехваченного пакета на предмет правильной привязки IP-к-MAC.
- Удаление и регистрация ARP Ответы, поступающие из недействительных, 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:

- Включить отслеживание DHCP на глобальном уровне.
- Включите отслеживание DHCP на выбранных VLAN.
- Включить DAI на выбранных VLAN.
- 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.



DHCP Snooping пример конфигруации

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 конфигруации (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 конфигруации (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** заменяет 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)#
```

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):

PortFast

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

BPDU guard

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

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** spanning-tree portfast bpduguard default**,** чтобы глобально включить защиту BPDU на всех портах с включенной 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 spanning-tree**
- **show spanning-tree summary** command

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 **showspanning-tree interface** *type/number* **detail** также может использоваться для проверки.

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 ошибкой.
- 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** .
- **Либо используйте команду глобальной конфигурации** spanning-tree portfast bpduguard default**,** чтобы глобально включить защиту BPDU на всех портах с включенной 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#
```


CISCO

Заполните, пожалуйста,
опрос о занятии по ссылке в чате

До новых встреч!
Приходите на следующие занятия

Рукин Андрей
преподаватель
cisco@sk12.ru