Тема 1 Управление инцидентами информационной безопасности

Лекция 9. Методы и средства обеспечения ИБ компьютерной сети

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

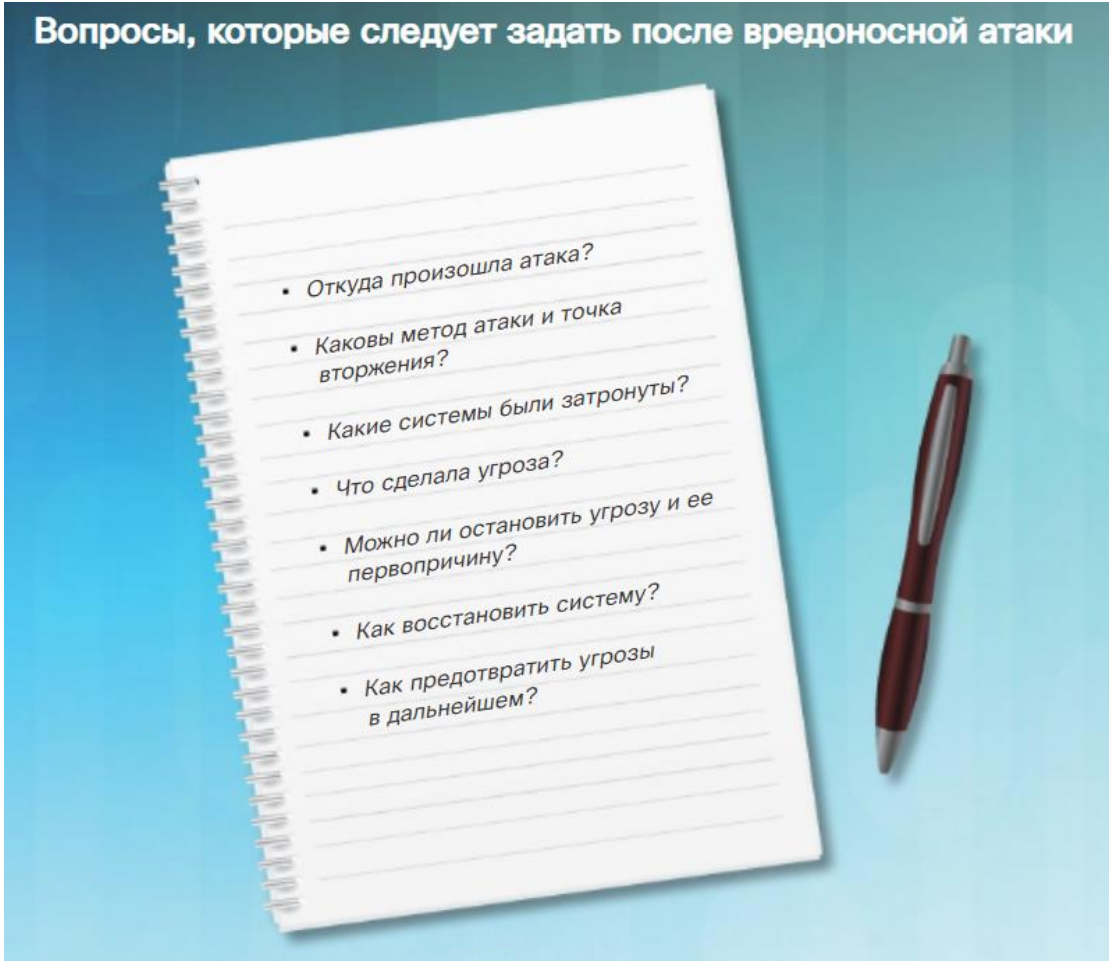
Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы и цели занятия:

1. Угрозы в локальной сети.
2. Защита таблицы CAM.
3. Защита протоколов DHCP, ARP.
4. Защита технологии VLAN, PVLAN.
5. Защита протокола STP.

Первый учебный вопрос

Первый учебный вопрос



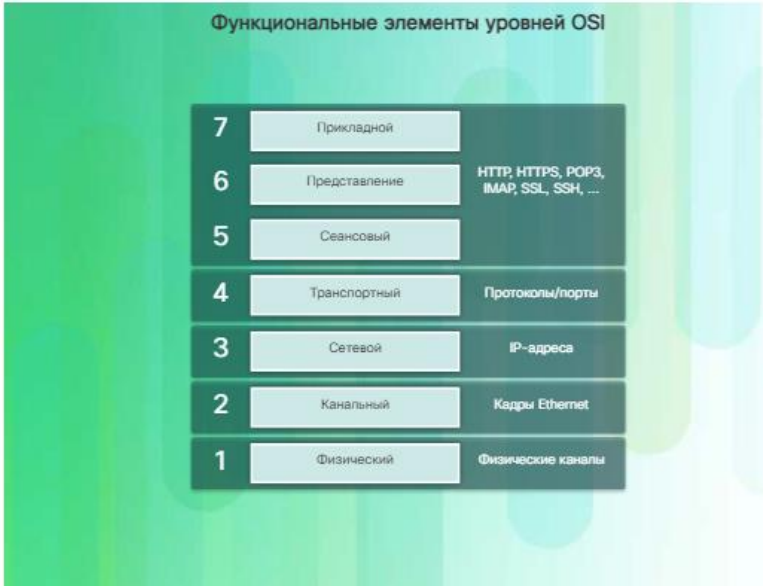
Первый учебный вопрос

Современные решения обеспечения ИБ

AMP (Antimalware Protection) -
Защита о вредоносного ПО

ESA (Email Security Appliance)
WSA (Web Security Appliance) -
Защита электронной почты и веб-трафика

NAC (Network Admission Control)
Система контроля доступа к сети



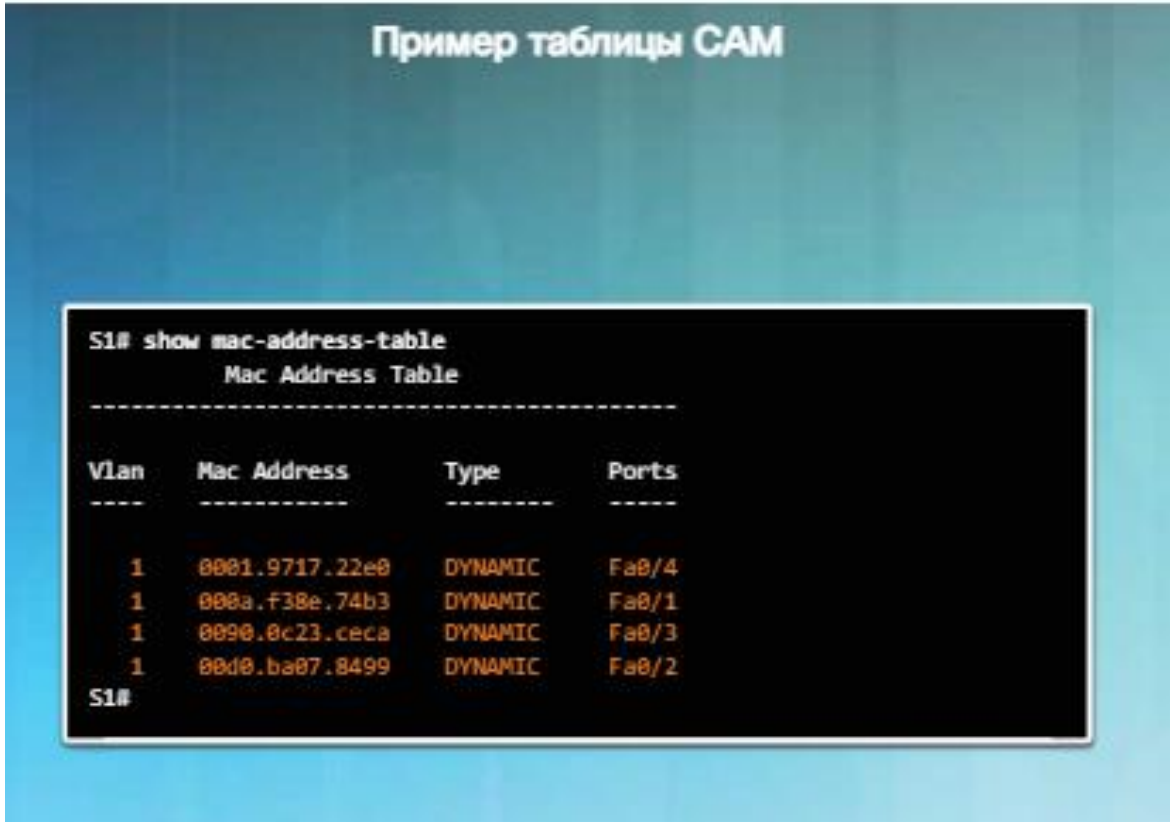
Описание уязвимостей на 2-м уровне

Эталонная модель OSI состоит из 7 уровней, каждый уровень выполняет специфическую функцию и содержит ключевые элементы, которые могут использоваться для воздействия.

Сетевые администраторы регулярно внедряют решения по защите элементов на уровнях с 3-го по 7-й, используя VPN, межсетевые экраны и устройства IPS. Однако, как видно из рис. 2, компрометация на 2-м уровне затрагивает все вышестоящие уровни. Например, если сотрудник или посетитель, имеющий доступ к внутренней сети, сможет получить контроль над кадрами 2-го уровня, все меры безопасности, реализованные на более высоких уровнях, станут бесполезными. Сотрудник сможет также нанести ущерб сетевой инфраструктуре локальной сети 2-го уровня.

Категории атак на коммутаторы

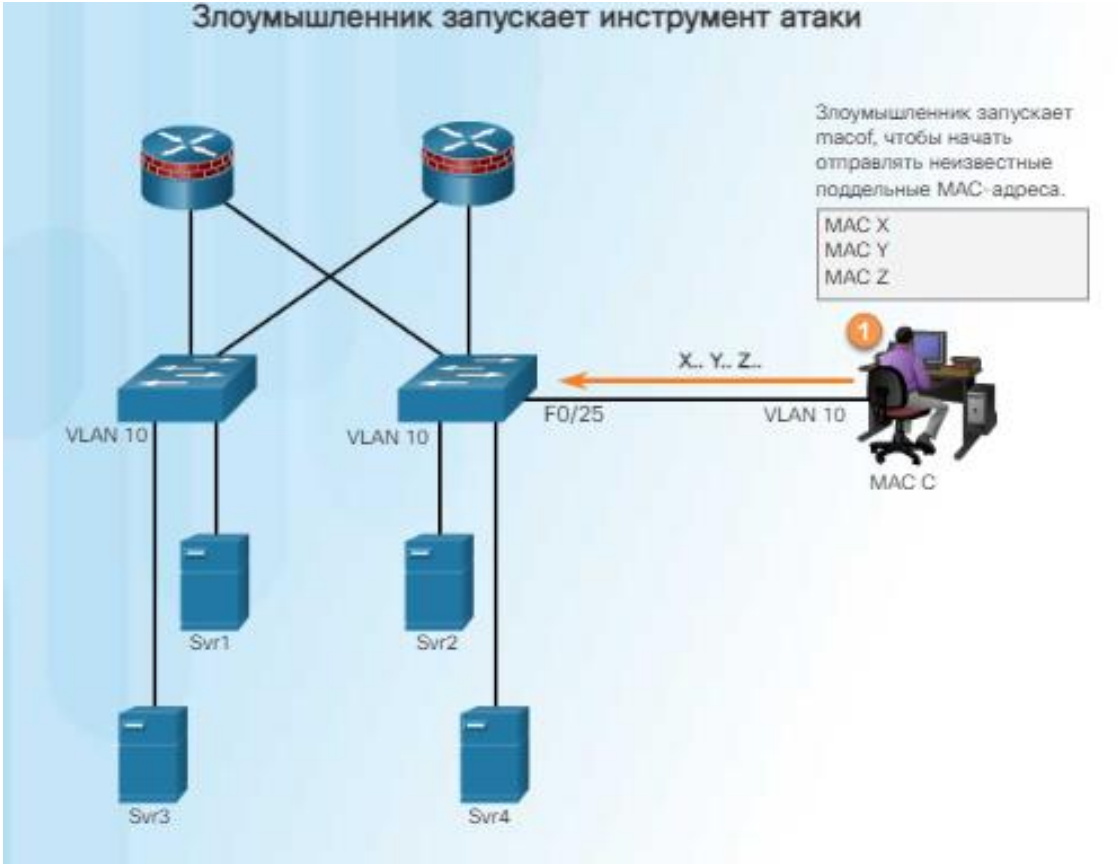
Уровень безопасности определяется наиболее уязвимым звеном системы, которым в данном случае является 2-й уровень. Это связано с тем, что локальные сети традиционно находились под административным контролем единственной организации. Мы внутренне доверяли всем лицам и устройствам, подключенным к локальной сети. В нынешней ситуации, с учетом внедрения концепции BYOD и появления более изощренных способов атак, наши локальные сети становятся более уязвимыми для проникновения извне.



Базовый режим работы коммутатора

Чтобы принять решение о пересылке, коммутатор локальной сети 2-го уровня строит таблицу MAC-адресов, которые сохраняются в таблице ассоциативной памяти (CAM, Content Addressable Memory). Таблица CAM совпадает с таблицей MAC-адресов.

Второй учебный вопрос



Атака на таблицу CAM

Все таблицы CAM имеют фиксированный размер и, следовательно, ресурсы коммутатора для хранения MAC-адресов могут быть исчерпаны. Атаки путем переполнения таблицы CAM (также называемые атаками путем переполнения MAC-адресов) используют преимущества этого ограничения, бомбардируя коммутатор подложными MAC-адресами отправителя до того момента, когда таблица MAC-адресов коммутатора станет заполнена.

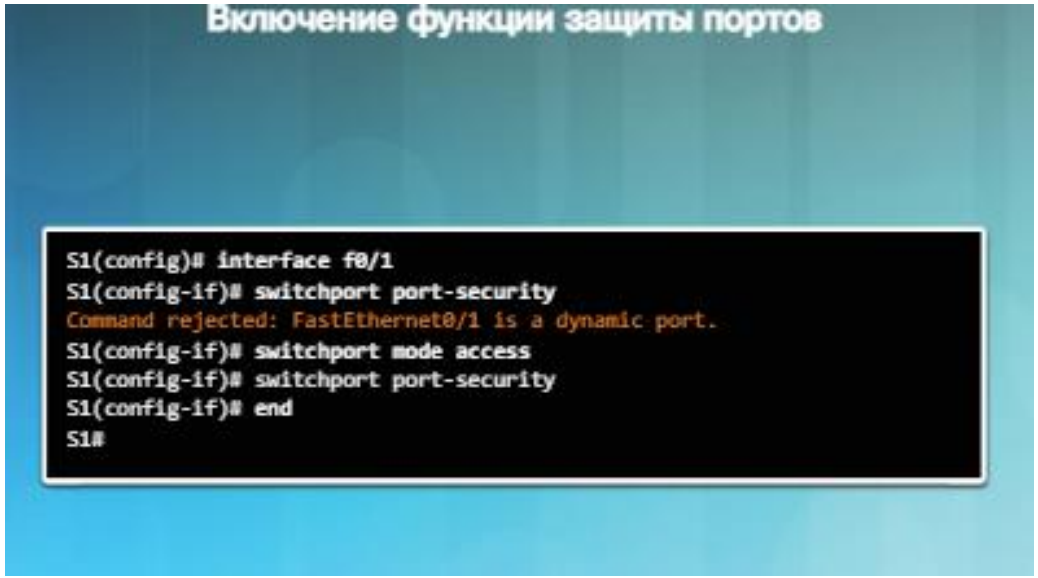
Второй учебный вопрос

Инструменты атаки на таблицу CAM

Лавинное заполнение таблицы CAM

```
# macof âC"i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

Особая опасность этих инструментов заключается в том, что для создания атаки путем переполнения таблицы CAM злоумышленнику требуется лишь несколько секунд. Например, коммутатор Catalyst 6500 может сохранять в своей таблице CAM 132 000 MAC-адресов. Такой инструмент, как macof, может направлять в коммутатор до 8 000 поддельных кадров в секунду;



Защита портов

Чтобы включить защиту порта, используйте для порта доступа команду конфигурирования интерфейса **switchport port-security,** как показано в примере на рис. 1. Обратите внимание, что до включения защиты порт должен быть сконфигурирован как порт доступа. Это связано с тем, что защита портов может конфигурироваться только в портах доступа, а порты коммутаторов 2-го уровня по умолчанию устанавливаются в режим dynamic auto (транкинг включен).

Второй учебный вопрос

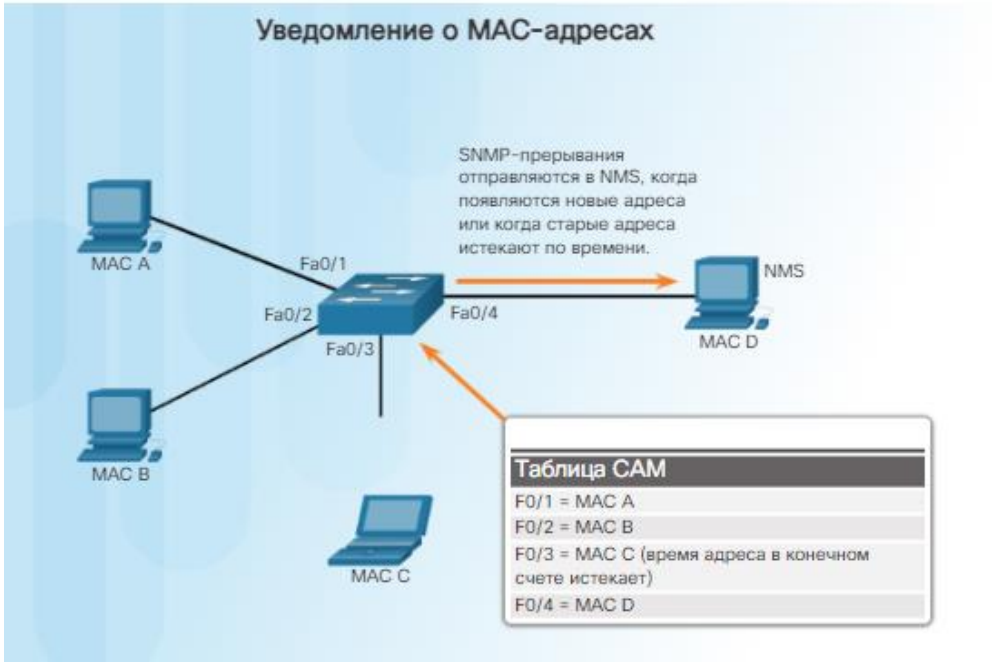
Нарушения защиты портов

Если MAC-адрес устройства, подключенного к порту, не входит в перечень безопасных адресов, возникает нарушение защиты порта, и порт переходит в состояние ***error-disabled*** (отключение из-за ошибки). Нарушение защиты возникает в ситуации, когда станция с MAC-адресом, не входящим в таблицу адресов, пытается осуществить доступ к интерфейсу при заполненной таблице.

Второй учебный вопрос

Работа защиты портов совместно с IP-телефонами

Порту доступа, к которому подключается IP-телефон и компьютер, как показано на рис. 1, обычно требуется два безопасных MAC-адреса. Однако в некоторых коммутаторах количество адресов должно быть увеличено до трех, поскольку если порт подключен к IP-телефону Cisco, то последнему необходимо иметь два MAC-адреса.

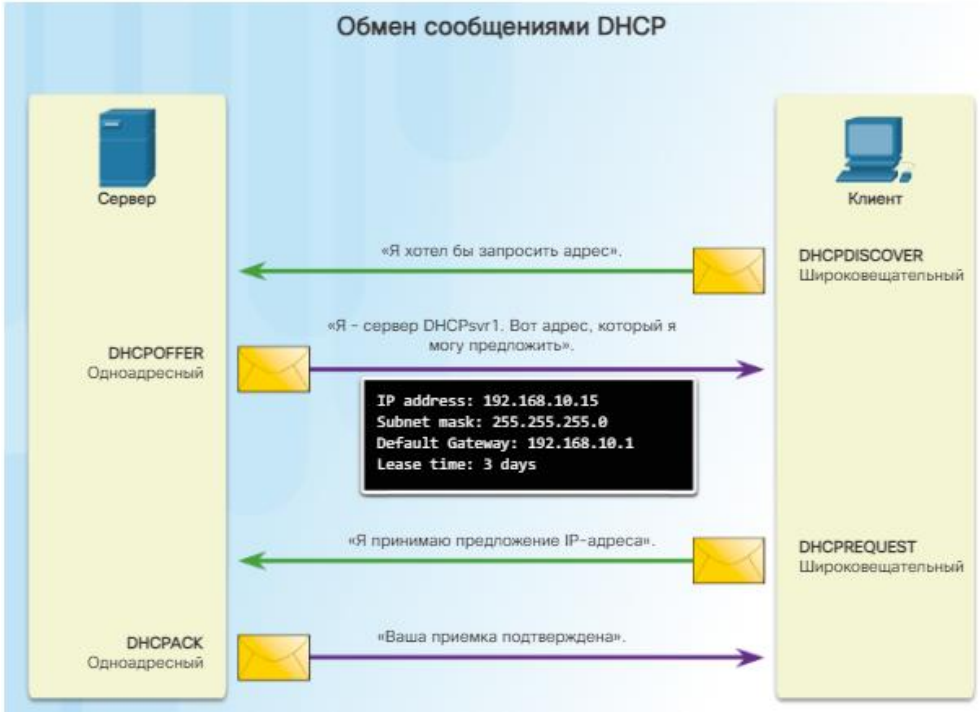


SNMP-уведомление об изменениях MAC-адресов

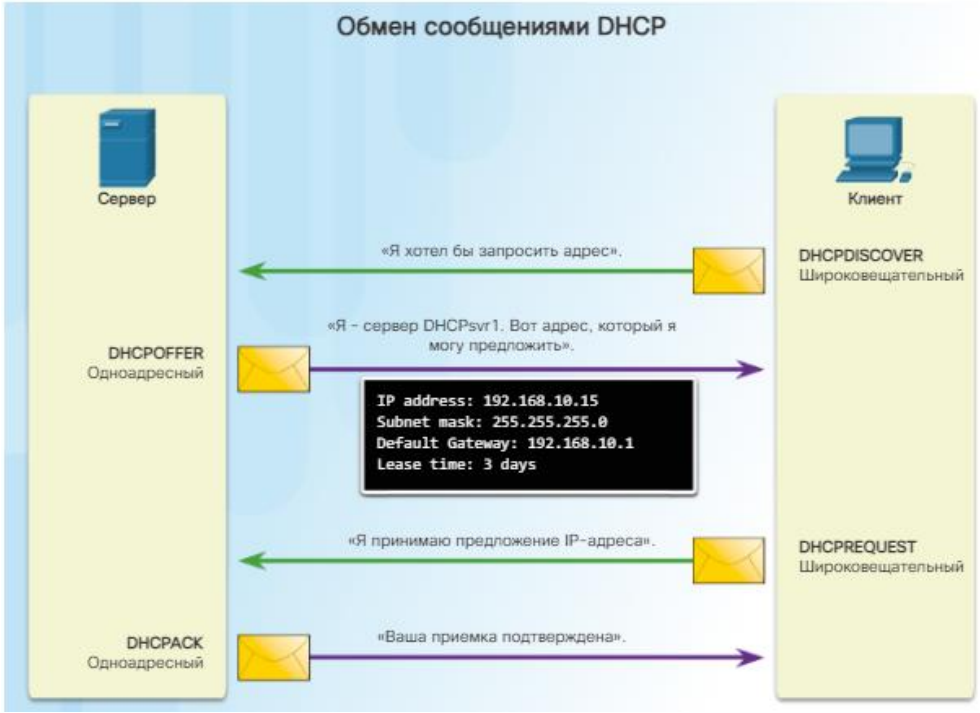
Менеджеры сети должны иметь возможность видеть пользователей сети и их местонахождение. Например, если порт F0/1 коммутатора защищен, при исчезновении записи с MAC-адресом для этого порта из таблицы CAM генерируется прерывание SNMP.

Третий учебный вопрос

Спуфинг DHCP



DHCP-серверы в динамическом режиме предоставляют клиентам информацию о конфигурации IP-сети, включая IP-адрес, маску подсети, шлюз по умолчанию, серверы DNS и другие данные. Последовательность обмена сообщениями DHCP между клиентом и сервером показана на рис



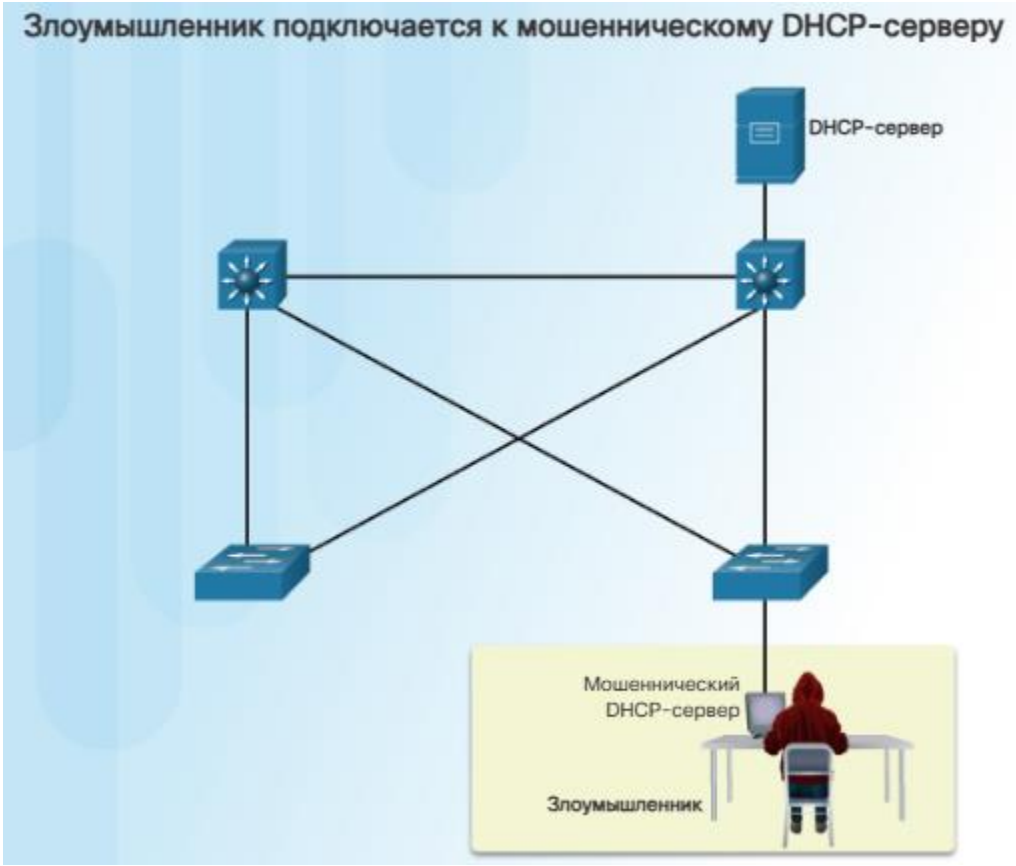
Спуфинг DHCP

Спуфинг DHCP возникает в тот момент, когда подставной DHCP-сервер подключается к сети и предоставляет легитимным клиентам фальшивые параметры конфигурации IP-сети. Подставной сервер может предоставлять разнообразную недостоверную информацию:

Неправильный шлюз по умолчанию – Злоумышленник сообщает недействительный шлюз или IP-адрес своего хоста, чтобы создать атаку типа «человек посередине». Эта ситуация может остаться совершенно незамеченной, поскольку злоумышленник перехватывает поток данных внутри сети.

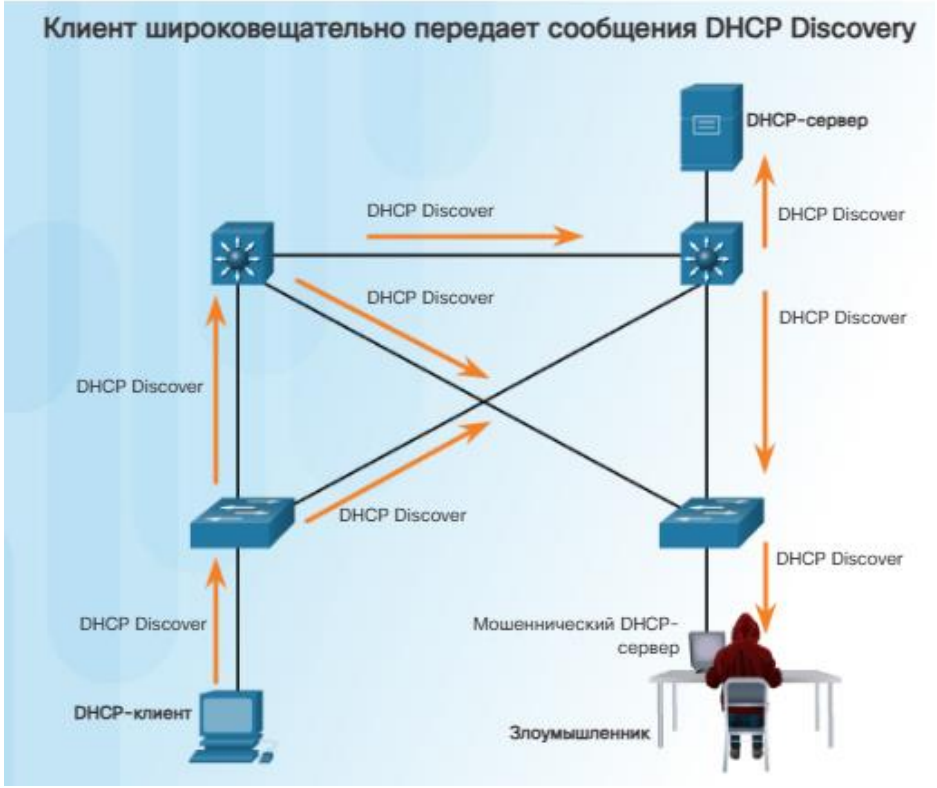
Неправильный сервер DNS – Злоумышленник сообщает неправильный адрес сервера DNS, ведущий пользователя на вредоносный веб-сайт.

Неправильный IP-адрес – Злоумышленник сообщает неправильный IP-адрес шлюза по умолчанию и создает DoS-атаку на DHCP-клиента.



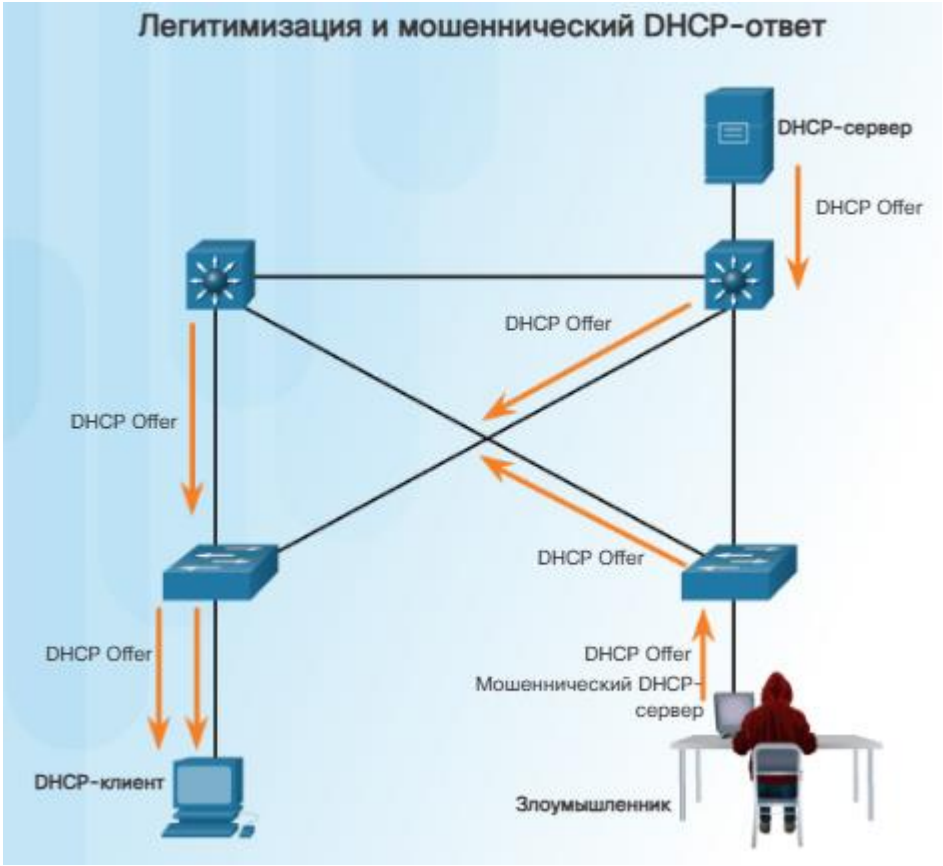
Спуфинг DHCP

Механизм атаки спуфинга DHCP разбирается на следующих рисунках: На рис. 2 злоумышленник успешно подключает подставной DHCP-сервер к порту коммутатора в той же подсети, где находятся клиенты. Задача подставного сервера – предоставить клиентам фальшивую информацию о конфигурации IP-сети.



Спуфинг DHCP

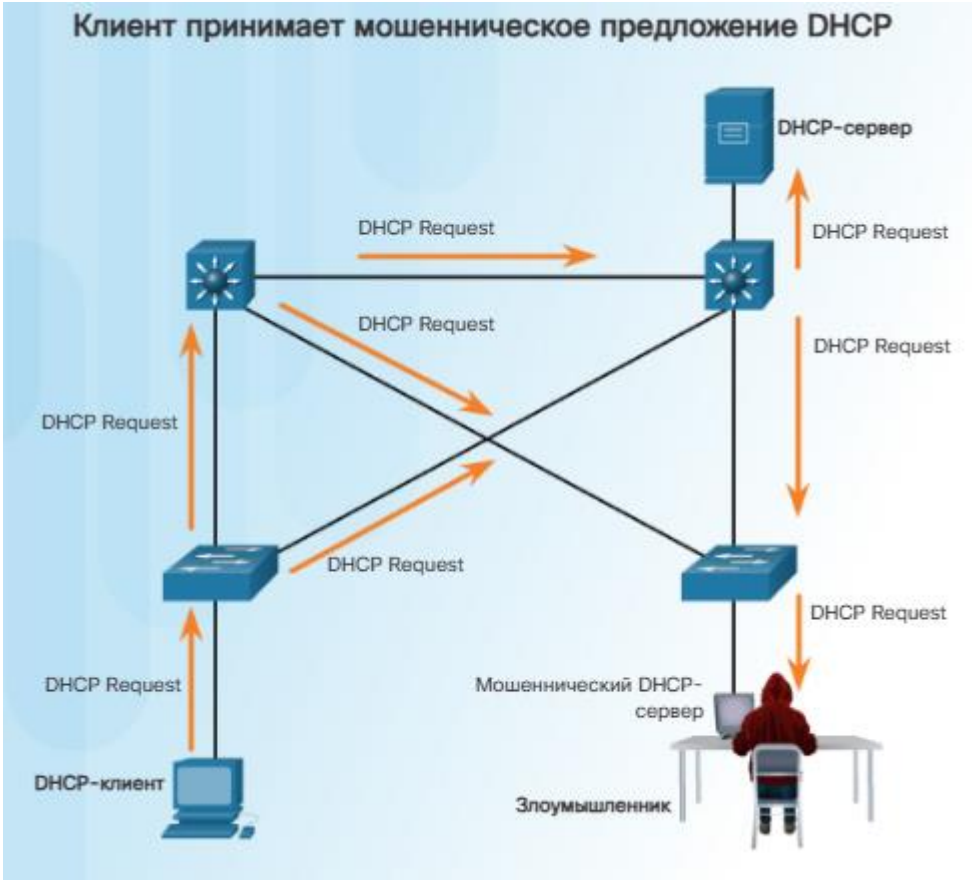
На рис. 3 легитимный клиент подключается к сети и запрашивает параметры конфигурации IP-сети. При этом клиент рассылает широковещательный запрос обнаружения DHCP Discovery, ожидающий ответа от DHCP-сервера. Оба сервера принимают сообщение и посылают ответ.



Спуфинг DHCP

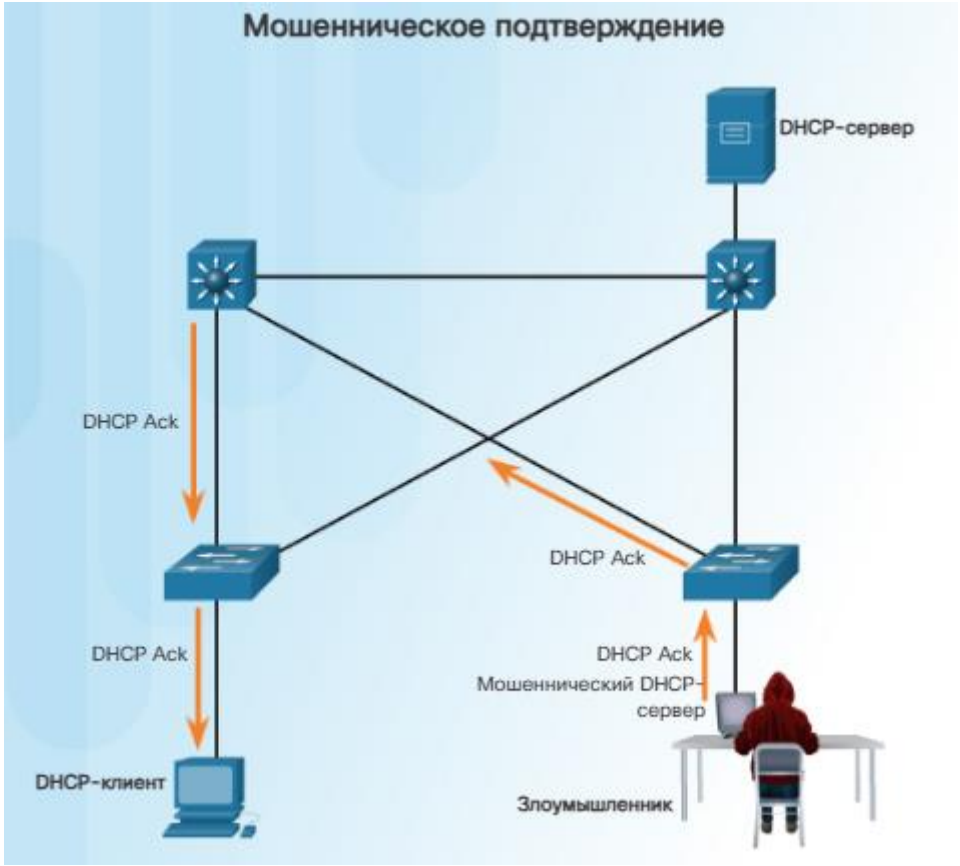
На рис. 4 легитимный DHCP сервер отвечает, сообщая действительные параметры конфигурации IP-сети. Однако подставной сервер также отвечает на запрос, высылая сообщения предложения DHCP Offer с параметрами конфигурации IP-сети, заданными злоумышленником. Клиент ответит на первое принятое предложение.

Третий учебный вопрос



Спуфинг DHCP

На рис. 5 первым поступает предложение от подставного сервера, поэтому клиент рассылает широковещательное сообщение запроса DHCP Request, которым подтверждает прием заданных злоумышленником параметров от подставного сервера. Легитимный и подставной серверы получают запрос клиента.



Спуфинг DHCP

На рис. 6 подставной сервер направляет клиенту индивидуальный ответ с подтверждением запроса. Легитимный сервер больше не взаимодействует с клиентом.

Истощение DHCP

Другим видом атаки DHCP является атака истощения ресурсов. Целью такой атаки является создание DoS-атаки для подключенных клиентов. Атаки истощения DHCP требуют наличия такого инструмента, как Gobbler.

Gobbler способен искать все доступные для аренды IP-адреса и пытается все их арендовать.

В частности, он создает сообщения DHCP Discover с поддельными MAC-адресами.

Нейтрализация атак DHCP

Нейтрализовать атаки истощения DHCP легко с помощью защиты портов. Однако нейтрализация атак спуфинга DHCP требует более серьезных методов защиты.

Например, Gobbler использует уникальный MAC-адрес для каждого запроса DHCP и защиты порта. Для нейтрализации этой угрозы достаточно сконфигурировать защиту порта. Однако Gobbler можно сконфигурировать так, чтобы он для каждого запроса использовал один и тот же MAC-адрес интерфейса с разными аппаратными адресами. В этом случае защита портов становится неэффективной.

Атаки путем спуфинга DHCP могут быть нейтрализованы с помощью механизма DHCP snooping в доверенных портах. DHCP snooping также помогает бороться с атаками истощения DHCP путем ограничения количества сообщений DHCP Discovery, которые может принимать недоверенный порт. Механизм DHCP snooping создает и поддерживает базу данных привязок DHCP snooping, которую коммутатор может использовать для фильтрации сообщений DHCP из недоверенных источников. База данных привязок DHCP snooping содержит MAC-адрес клиента, IP-адрес, время аренды DHCP, тип привязки, номер VLAN, информацию об интерфейсе каждого недоверенного порта или интерфейса коммутатора.

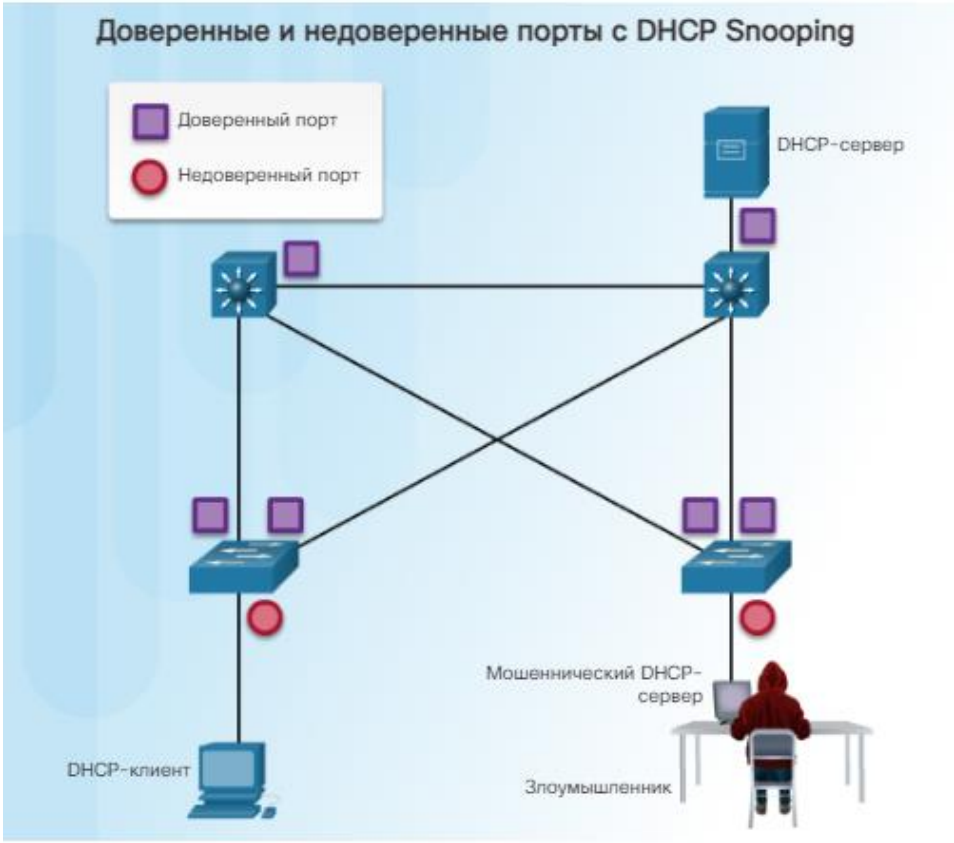
Нейтрализация атак DHCP

В большой сети может потребоваться некоторое время на создание таблицы привязок DHCP после ее включения. Например, если время аренды DHCP составляет четыре дня, создание таблицы DHCP snooping может занять два дня. Если в интерфейсе или в сети VLAN включено DHCP snooping и коммутатор принимает пакет в недоверенный порт, коммутатор сравнивает информацию об источнике с информацией, которая хранится в таблице привязок DHCP snooping. Коммутатор отклоняет пакеты, содержащие определенную информацию, а именно:

- Неавторизованные сообщения DHCP-сервера с недоверенного порта
- Неавторизованные сообщения DHCP-клиента, не соответствующие таблице снупинга или превышающие определенное количество сообщений в секунду
- Пакеты DHCP relay-agent с опцией 82 с недоверенного порта

Для противодействия инструменту Gobbler, использующему один тот же MAC-адрес, механизм DHCP snooping вынуждает коммутатор проверять поле Client Hardware Address (CHADDR) в сообщении DHCP Request. Это обеспечивает сопоставление аппаратного MAC-адреса в таблице привязок DHCP snooping и MAC-адреса в таблице CAM. Если совпадение адресов отсутствует, запрос отклоняется.

Аналогичные технологии нейтрализации существуют для клиентов DHCPv6 и IPv6. Поскольку устройства IPv6 могут также получать свою адресную информацию из объявлений маршрутизатора (RA, Router Advertisement), они также являются решением для предотвращения поддельных сообщений RA.



Конфигурирование DHCP Snooping

Как показано на рисунке, механизм DHCP Snooping распознает два типа портов:

Доверенные порты DHCP – Доверенными портами могут быть только порты, подключенные к вышестоящему DHCP-серверу. В этих портах ожидается получать сообщения DHCP Offer и DHCP Ack. Доверенные порты должны быть явно обозначены в конфигурации.

Недоверенные порты – Эти порты подключаются к хостам, которые не должны быть источником сообщений DHCP-сервера.

По умолчанию все порты коммутатора считаются недоверенными. Общее правило при конфигурировании DHCP Snooping – «доверять порту и включить DHCP Snooping во VLAN». Таким образом, при включении DHCP Snooping должны выполняться следующие действия:

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

Шаг 2. Для доверенных портов используйте команду конфигурирования интерфейса **ip dhcp snooping trust** .

Шаг 3. Включите DHCP Snooping в сети VLAN или в нескольких сетях VLAN.

Для недоверенных портов необходимо установить ограничение скорости принимаемых сообщений DHCP Discovery с помощью команды конфигурирования интерфейса **ip dhcp snooping limit rate** .

Примечание. Ограничение скорости сообщений дополнительно нейтрализует риск атак истощения DHCP.


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

Пример конфигурирования DHCP Snooping

Приведены команды, сконфигурированные в коммутаторе S1 для включения DHCP Snooping.
Обратите внимание, как DHCP Snooping включается в первый раз. Затем объявляется доверенным восходящий интерфейс в направлении DHCP-сервера.
На следующем шаге, поскольку порты FastEthernet с F0/5 по F0/24 являются недоверенными, для них устанавливается ограничение скорости шесть пакетов в секунду.
Наконец, включается DHCP Snooping в сетях VLANS 5, 10, 50, 51 и 52.

Пример конфигурирования DHCP Snooping

```
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:

<output omitted>
```

Чтобы получить больше информации о фактическом клиенте, который создал запрос DHCP, включите опцию 82 DHCP с помощью команды **ip dhcp snooping information option** режима глобальной конфигурации. После этого в запрос DHCP добавляется идентификатор порта коммутатора.

На рисунке приведен результат выполнения привилегированной EXEC-команды **show ip dhcp snooping** . А на рис. 4 приведен результат выполнения команды **show ip dhcp snooping binding** . В качестве альтернативного способа проверки можно использовать команду **show ip dhcp snooping database** .

Примечание. DHCP Snooping также необходим для динамического инспектирования ARP (DAI).

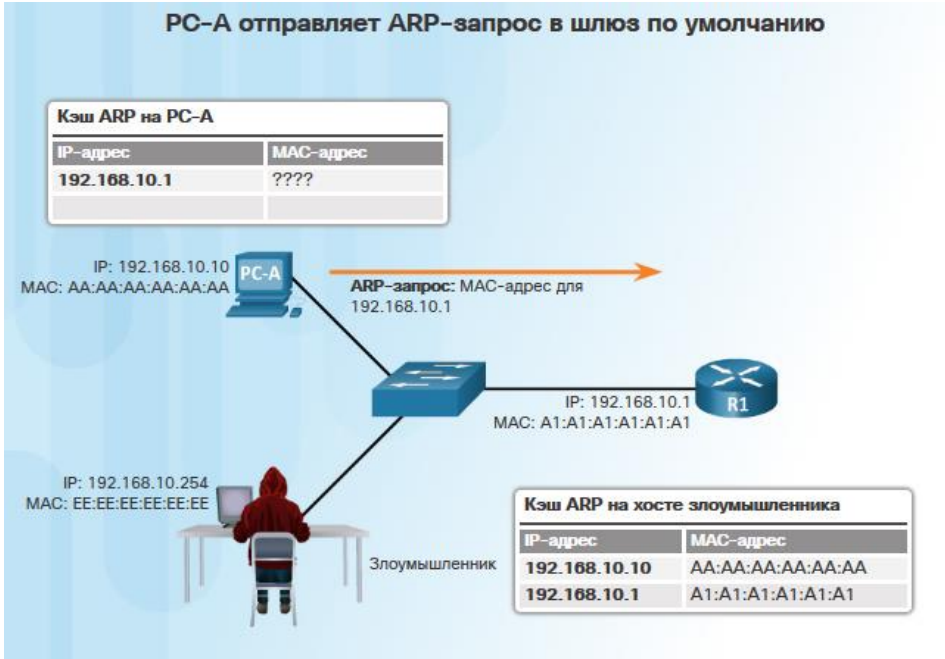
Спуфинг ARP и ARP Poisoning

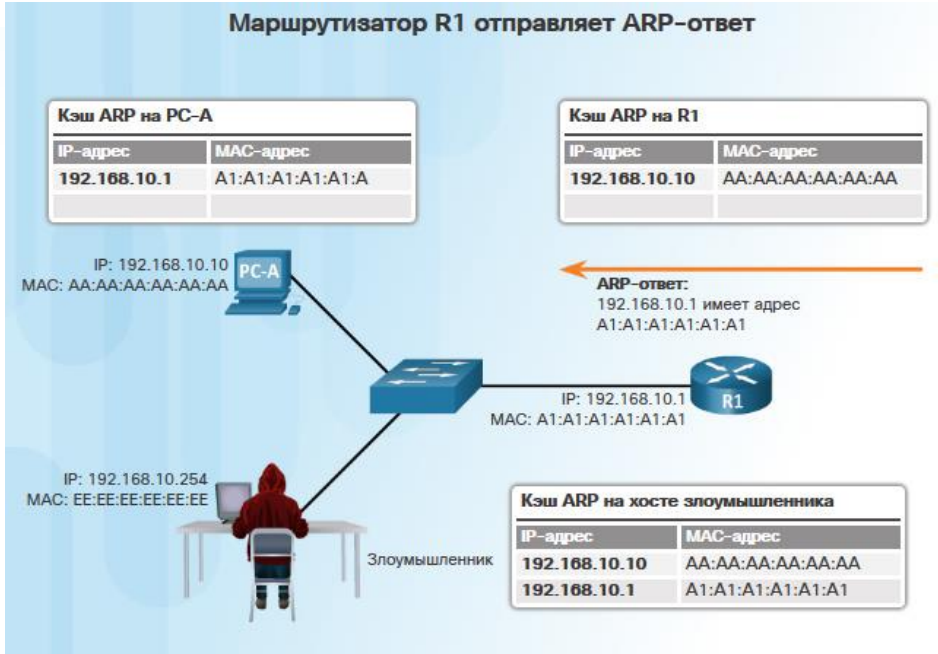
Обычно хост рассылает ARP-запрос другим хостам, чтобы определить MAC-адрес хоста с конкретным IP-адресом. Все хосты подсети получают и обрабатывают ARP-запрос. Хост с IP-адресом, который соответствует ARP-запросу, передает ARP-ответ.

В соответствии с ARP RFC клиенту разрешается передать незатребованный ARP-ответ, который называется произвольным ARP (gratuitous). Когда хост передает произвольный ARP, другие хосты подсети сохраняют в своих ARP-таблицах MAC-адрес и IP-адрес, содержащиеся в произвольном ARP.

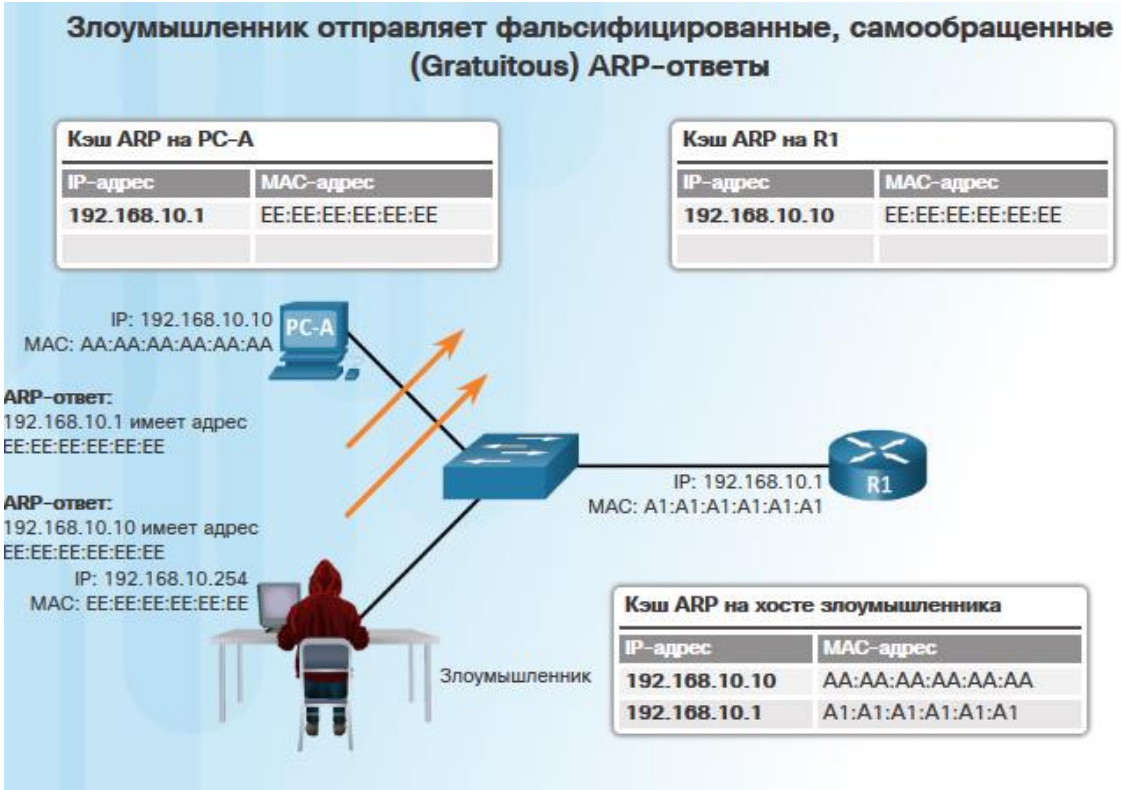
Проблема заключается в том, что злоумышленник может передать коммутатору произвольное сообщение ARP, содержащее фальшивый MAC-адрес, и коммутатор соответственно обновит свою таблицу CAM. Таким образом любой хост может объявить себя владельцем любого IP/MAC-адреса. При типичной атаке злоумышленник может передать незатребованные ARP-ответы другим хостам подсети со своим MAC-адресом и IP-адресом шлюза по умолчанию.

Третий учебный вопрос



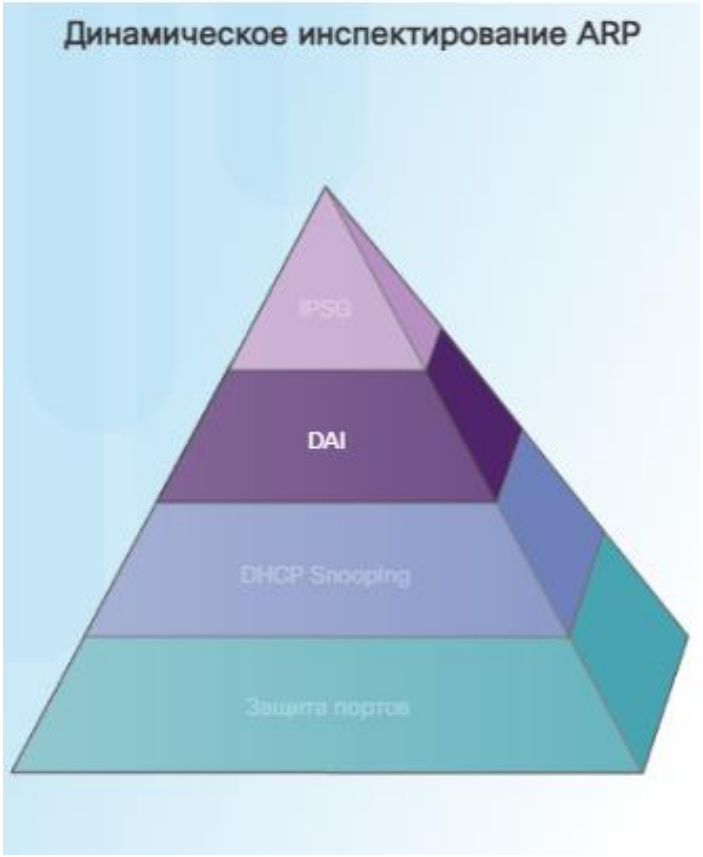


Третий учебный вопрос



Злоумышленник передает два фальшивых произвольных ARP-ответа с использованием собственного MAC-адреса на IP-адреса указанных получателей. Компьютер PC-A обновляет свой кеш ARP, и теперь для шлюза по умолчанию используется MAC-адрес хоста злоумышленника. Маршрутизатор R1 также обновляет свой кеш ARP IP-адресом компьютера PC-A, который указывает на MAC-адрес злоумышленника.

Теперь хост злоумышленника совершает атаку ARP Poisoning. Она заключается в отправке злоумышленником фальсифицированных ARP для перенаправления трафика. ARP poisoning открывает возможность для различных атак типа «человек посередине», создающих серьезную угрозу безопасности сети.

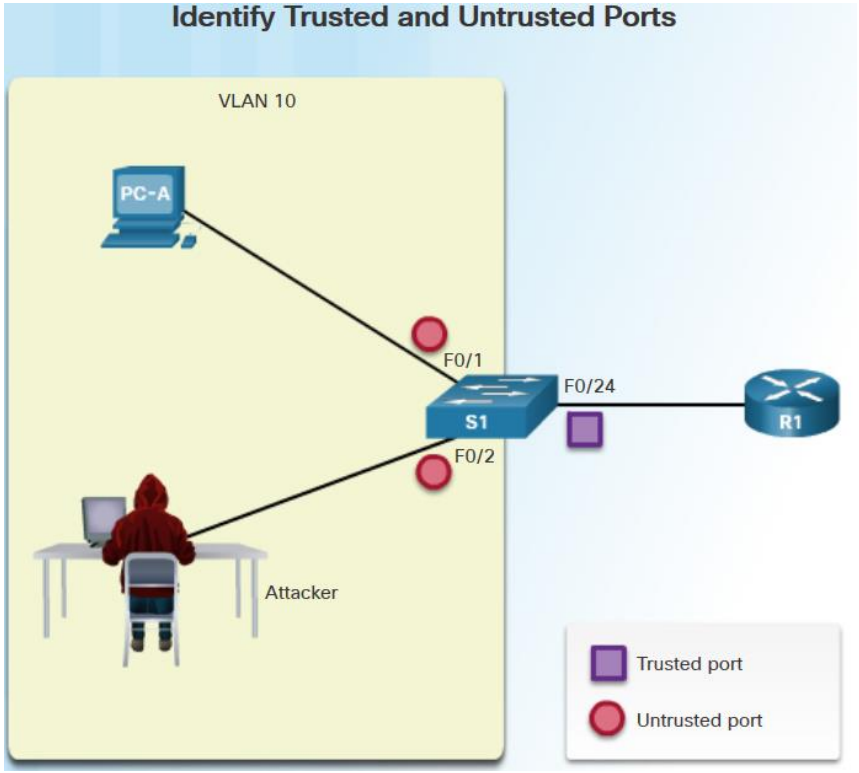


Нейтрализация атак ARP

Для предотвращения спуфинга ARP или ARP poisoning коммутатор должен обеспечить ретрансляцию только действительных запросов и ответов ARP. При типичной атаке злоумышленник может передать незатребованные ARP-ответы другим хостам подсети со своим MAC-адресом и IP-адресом шлюза по умолчанию.

Динамическое инспектирование ARP помогает предотвратить такие атаки, не ретранслируя недействительные или произвольные ARP-ответы в другие порты той же сети VLAN. Динамическое инспектирование ARP перехватывает все ARP-запросы и все ответы в недоверенных портах. Каждый перехваченный пакет проверяется на предмет действительности привязки IP-адреса к MAC-адресу. ARP-ответы, поступающие от недействительных устройств, либо отбрасываются, либо регистрируются в коммутаторе для аудита с целью предотвращения атак ARP poisoning. DAI также может иметь ограничение по скорости, чтобы ограничить количество пакетов ARP, а интерфейс может переводиться в состояние отключения из-за ошибок при превышении установленного порога. Для DAI требуется DHCP Snooping. DAI определяет достоверность ARP-пакета на основании действительных привязок IP-адресов к MAC-адресам, хранящихся в базе данных, которая создается DHCP Snooping. Кроме того, для работы с хостами, которые используют статические IP-адреса, DAI может проверять пакеты по сконфигурированным пользователями спискам ARP ACL.

Третий учебный вопрос




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

В данном примере к коммутатору S1 подключены два пользователя в сети VLAN 10. Для предотвращения спуфинга ARP и ARP Poisoning будет сконфигурировано DAI.
Как показано на рисунке, включен DHCP Snooping, поскольку для DAI необходима таблица DHCP Snooping. Затем включаются DHCP Snooping и инспектирование ARP для компьютеров во VLAN10. Восходящий порт к маршрутизатору является доверенным портом, поэтому он конфигурируется как доверенный для DHCP Snooping и инспектирования ARP.

Третий учебный вопрос


```
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)#
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)#
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)#
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

DAI может также конфигурироваться для проверки MAC- и IP-адресов отправителя и получателя:

MAC-адрес получателя – Проверяет соответствие MAC-адреса получателя в заголовке Ethernet целевому MAC-адресу в сообщении ARP.

MAC-адрес отправителя – Проверяет соответствие MAC-адреса отправителя в заголовке Ethernet MAC-адресу отправителя в сообщении ARP.

IP-адрес – Проверяет сообщение ARP на наличие недействительного и непредвиденного IP-адреса, включая адреса 0.0.0.0, 255.255.255.255 и все групповые IP-адреса.

команда глобальной конфигурации **ip arp inspection validate {[src-mac] [dst-mac] [ip]}** используется для конфигурирования DAI таким образом, чтобы пакеты ARP отбрасывались в случае недействительного IP-адреса. Это может использоваться, когда MAC-адреса в теле пакетов ARP не соответствуют адресам, указанным в заголовке Ethernet. Обратите внимание, что сконфигурировать команду можно только один раз. Поэтому при вводе нескольких команд **ip arp inspection validate** последующие команды отменяют предыдущие. Чтобы включить несколько методов проверки, вводите их в той же строке.

Третий учебный вопрос

Спуфинг адресов

MAC-адреса и IP-адреса могут фальсифицироваться с разными целями. Атаки спуфинга используются, когда один хост выставляет себя в качестве другого хоста для получения недоступных ранее данных или для обхода защищенных конфигураций.

Метод, который используется коммутаторами для обновления таблиц MAC-адресов, создает уязвимость, известную как спуфинг MAC-адресов. Атаки спуфинга MAC-адресов возникают, когда злоумышленники меняют MAC-адрес своего хоста на другой известный MAC-адрес целевого хоста, как показано на рис. 1. Атакующий хост передает в сеть кадр с вновь сформированным MAC-адресом. Когда коммутатор получает кадр, он узнает MAC-адрес отправителя. Коммутатор переписывает текущую запись в таблице CAM и приписывает MAC-адрес к новому порту, как показано на рис. 2. После этого он непреднамеренно направляет кадры, предназначенные для целевого хоста, атакующему хосту.

Когда коммутатор меняет таблицу CAM, целевой хост не получает трафик до тех пор, пока он не начинает передавать трафик. Когда целевой хост передает трафик, коммутатор принимает и изучает кадр, что приводит к новому обновлению таблицы CAM, в результате чего порту вновь назначается правильный MAC-адрес. Чтобы не допустить обратную замену фальсифицированного MAC-адреса на правильный, атакующий хост может создать программу или скрипт, который будет постоянно передавать коммутатору кадры, в результате чего коммутатор будет сохранять неправильные или фальсифицированные данные. На 2-м уровне отсутствует механизм защиты, который позволяет коммутатору проверять MAC-адреса отправителя, и это является основной причиной уязвимости для спуфинга.

Спуфинг IP-адресов возникает, когда подставной ПК похищает действительный IP-адрес соседа или использует случайный IP-адрес. Спуфинг IP-адресов трудно нейтрализовать, особенно когда он используется внутри подсети, которой принадлежит IP-адрес.

Третий учебный вопрос

Нейтрализация атак спуфинга адресов

Для защиты от спуфинга MAC- и IP-адресов сконфигурируйте функцию защиты источника IP (IPSG, IP Source Guard). IPSG работает аналогично DAI, но она контролирует каждый пакет, а не только пакеты ARP. Подобно DAI, функция IPSG также требует, чтобы был включен DHCP Snooping.

IPSG разворачивается в недоверенных портах доступа и магистральных портах 2-го уровня. IPSG динамически поддерживает списки VLAN ACL (PVACL) для каждого порта на базе привязок IP-MAC-коммутатор-порт. Изначально весь IP-трафик в порту заблокирован, за исключением пакетов DHCP, которые перехватываются процессом DHCP Snooping. Список PVACL устанавливается в порту, когда клиент получает действительный IP-адрес от DHCP-сервера или когда пользователь конфигурирует привязку статического IP-адреса отправителя. Этот процесс ограничивает IP-трафик клиента, пропуская только те IP-адреса отправителя, которые сконфигурированы в привязке. Любой IP-трафик с IP-адресом отправителя, отличным от IP-адреса отправителя в привязке, будет отфильтровываться. Эта фильтрация ограничивает возможность хоста атаковать сеть, объявляя IP-адрес соседнего хоста.

Для каждого недоверенного порта существует два возможных уровня защитной фильтрации IP-трафика:

Фильтрация IP-адресов отправителя – IP-трафик фильтруется по IP-адресу отправителя, при этом пропускается только IP-трафик с IP-адресами отправителя, которые соответствуют записям привязки IP-адресов отправителя. Если в порту создается или удаляется запись привязки источника IP, происходит автоматическая коррекция списка PVACL, отражающая изменение в привязках источника IP.

Фильтр IP- и MAC-адреса источника – IP-трафик фильтруется по IP-адресу отправителя и по MAC-адресу. Пропускается только IP-трафик с IP-адресами отправителя и MAC-адресами, которые соответствуют записям привязки источника IP.

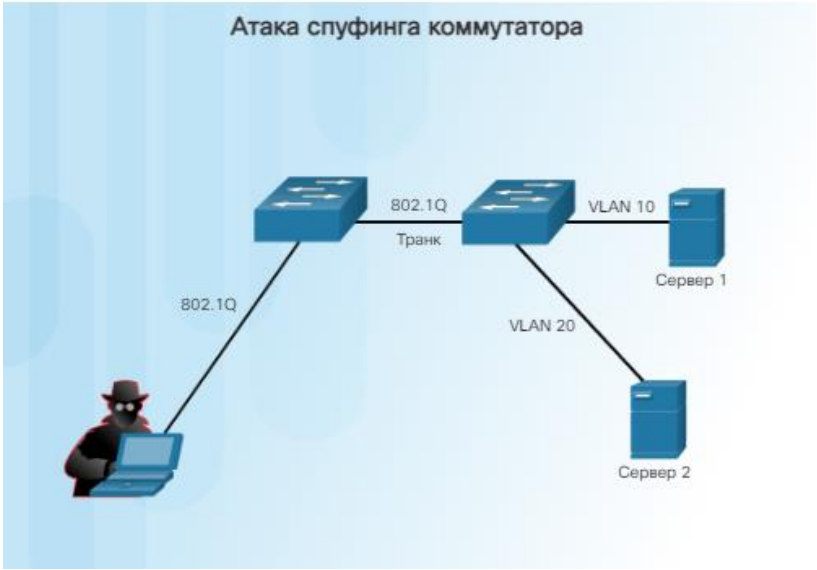
```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

IP Source Guard включена в недоверенных портах с помощью команды **ip verify source** . Следует помнить, что функция может быть сконфигурирована только в порте доступа или магистральном порте 2-го уровня и что необходимо использовать функцию DHCP Snooping для обучения действительным парам IP-адреса и MAC-адреса.

Используйте команду **show ip verify source** для проверки конфигурации IP Source Guard, как показано на рис. 3. В данном примере в портах FastEthernet F0/1 и F0/2 сконфигурирована IP Source Guard. Для каждого интерфейса существует одна действительная привязка DHCP.

Атаки перехода (Hopping) VLAN

Спуфинг сообщений DTP от атакующего узла, чтобы вынудить коммутатор перейти в режим транкинга. С этого момента злоумышленник может передавать тегированный трафик для целевой сети VLAN, и коммутатор доставляет пакеты по адресу назначения.



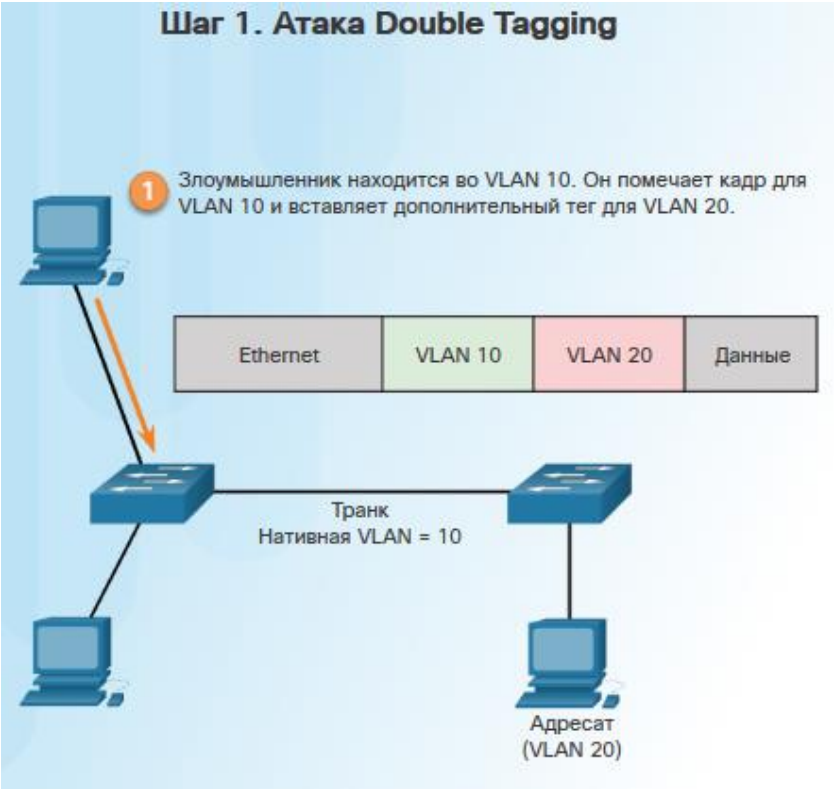
Атака путем переключения VLAN может быть создана одним из следующих способов:

- Спуфинг сообщений DTP от атакующего хоста, чтобы вынудить коммутатор перейти в режим транкинга. С этого момента злоумышленник может передавать тегированный трафик для целевой сети VLAN, и коммутатор доставляет пакеты по адресу назначения.
- Ввод подставного коммутатора и включение транкинга. После этого злоумышленник получает доступ ко всем сетям VLAN коммутатора-жертвы из подставного коммутатора.

Атаки перехода (Hopping) VLAN

Архитектура VLAN упрощает обслуживание сети и повышает ее производительность, однако она открывает возможности для злоупотреблений.
Одной из угроз, связанных с VLAN, является атака путем переключения VLAN. Атака путем переключения VLAN позволяет видеть трафик одной из сетей VLAN в другой VLAN без помощи маршрутизатора. В базовом варианте атаки путем переключения VLAN злоумышленник пользуется возможностями функции автоматического транкинга, включенной по умолчанию в большинстве портов коммутатора. Сетевой злоумышленник конфигурирует хост, чтобы обманом вынудить коммутатор использовать сигнализацию 802.1Q и сигнализацию проприетарного динамического протокола транкинга Cisco (DTP) для организации магистрального канала с подключенным коммутатором. В случае успешного установления магистрального канала между хостом и коммутатором, злоумышленник получает доступ ко всем сетям VLAN коммутатора и может переключать (т. е. передавать и принимать) трафик во всех сетях VLAN.

Четвертый учебный вопрос



Атака с двойным тегированием (Double-Tagging) VLAN

Другим типом атаки с переключением VLAN является атака с двойным тегированием (или двойной инкапсуляцией). Эта атака использует принципы работы аппаратных средств большинства коммутаторов.

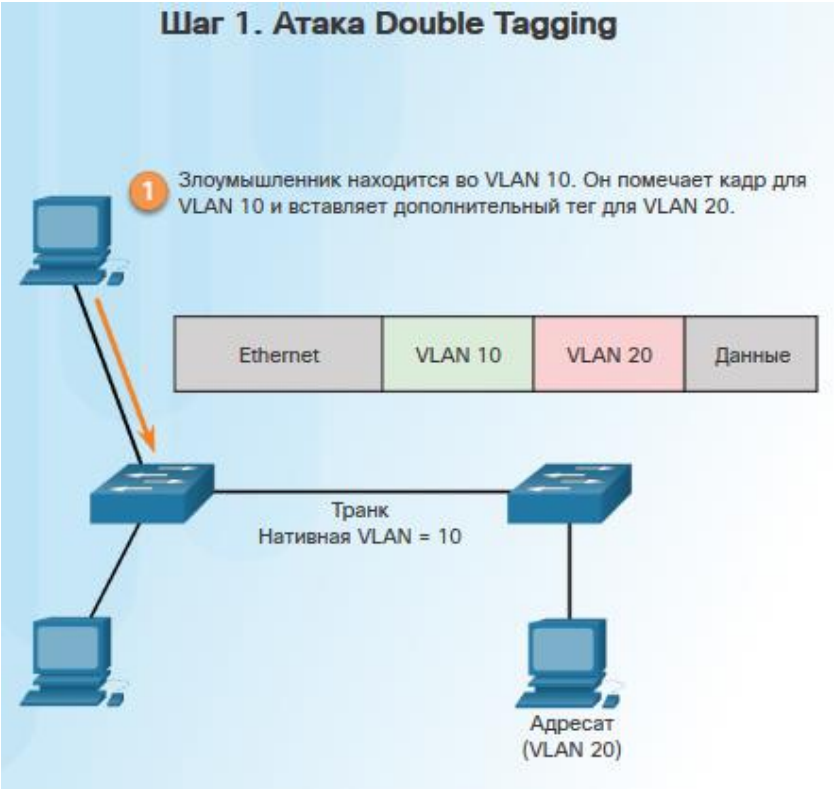
Большинство коммутаторов реализуют только один уровень инкапсуляции/декапсуляции 802.1Q. Благодаря этому в некоторых случаях злоумышленник может встроить внутрь кадра скрытый тег 802.1Q. Этот тег позволяет кадру попасть во VLAN, которую не определяет исходный тег 802.1Q.

Важной характеристикой атаки VLAN с двойной инкапсуляцией является возможность ее работы даже в условиях отключения магистральных портов, поскольку хост обычно передает кадры в сегменте сети, который не является магистральным каналом.

Атака с двойным тегированием состоит из трех этапов:

•На рис. 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. В рамках рассматриваемого примера примем, что это VLAN 10. Внутренний тег указывает на VLAN-жертву, в данном примере VLAN 20.

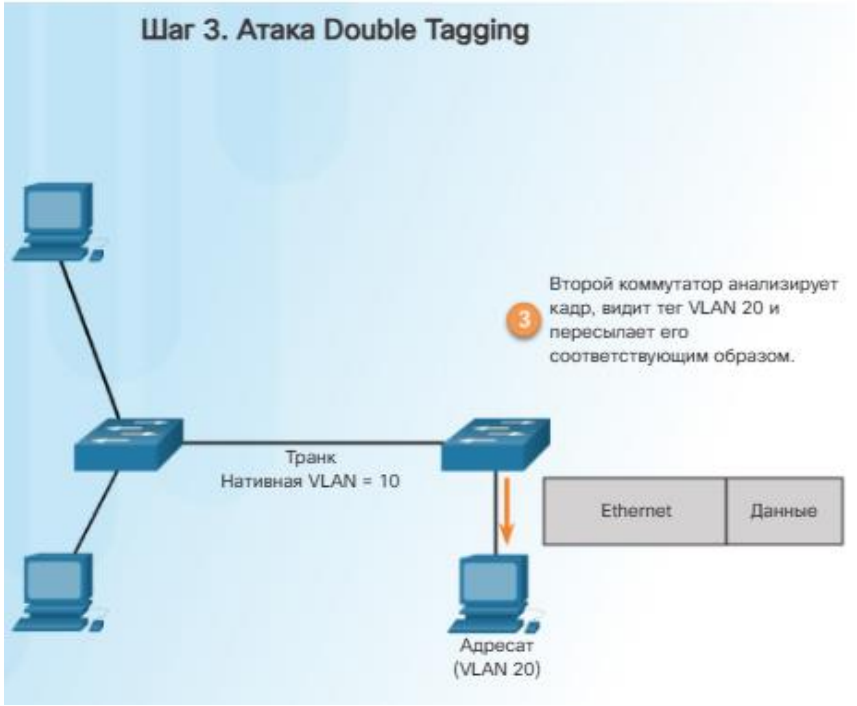
Четвертый учебный вопрос



Атака с двойным тегированием (Double-Tagging) VLAN

•На рис. 2 кадр поступает в первый коммутатор, который видит первый 4-байтовый тег 802.1Q. Коммутатор понимает, что кадр предназначен для VLAN 10, которая является его нативной VLAN. Коммутатор рассылает пакет через все порты VLAN 10, отбросив тег VLAN 10. В магистральном порте тег VLAN 10 отброшен, но новый тег не присваивается, поскольку это часть нативной VLAN. В этот момент тег VLAN 20 по-прежнему остается в сохранности и не проверяется первым коммутатором.

Четвертый учебный вопрос



Атака с двойным тегированием (Double-Tagging) VLAN

•В итоге кадр поступает во второй коммутатор, но он не имеет информации о том, что он предназначен для VLAN 10. Трафик нативной 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 сети VLAN 20, или целевой VLAN. Второй коммутатор пересылает кадр в порт-жертве или рассылает его по всем портам в зависимости от того, существует ли запись в таблице MAC-адресов для хоста-жертвы.
Этот вид атаки является однонаправленным и работает только в том случае, если злоумышленник подключен к порту, принадлежащему нативной VLAN магистрального порта. Идея атаки заключается в том, что двойное тегирование позволяет злоумышленнику передавать данные хостам или серверам в сеть VLAN, которая в противном случае была бы блокирована одним из средств управления доступом. Обратный трафик также может быть предположительно разрешен, при этом злоумышленник получит возможность взаимодействовать с устройствами блокированной VLAN.

Нейтрализация атак перехода VLAN

1. Отключите согласование по протоколу DTP (автоматический транкинг) в немагистральных портах с помощью команды конфигурирования интерфейса switchport mode access.

2. Вручную включите магистральный канал в магистральном порту с помощью команды конфигурирования интерфейса switchport mode trunk.

3. Отключите согласование по протоколу DTP (автоматический транкинг) в магистральных портах с помощью команды конфигурирования интерфейса switchport non-negotiate.

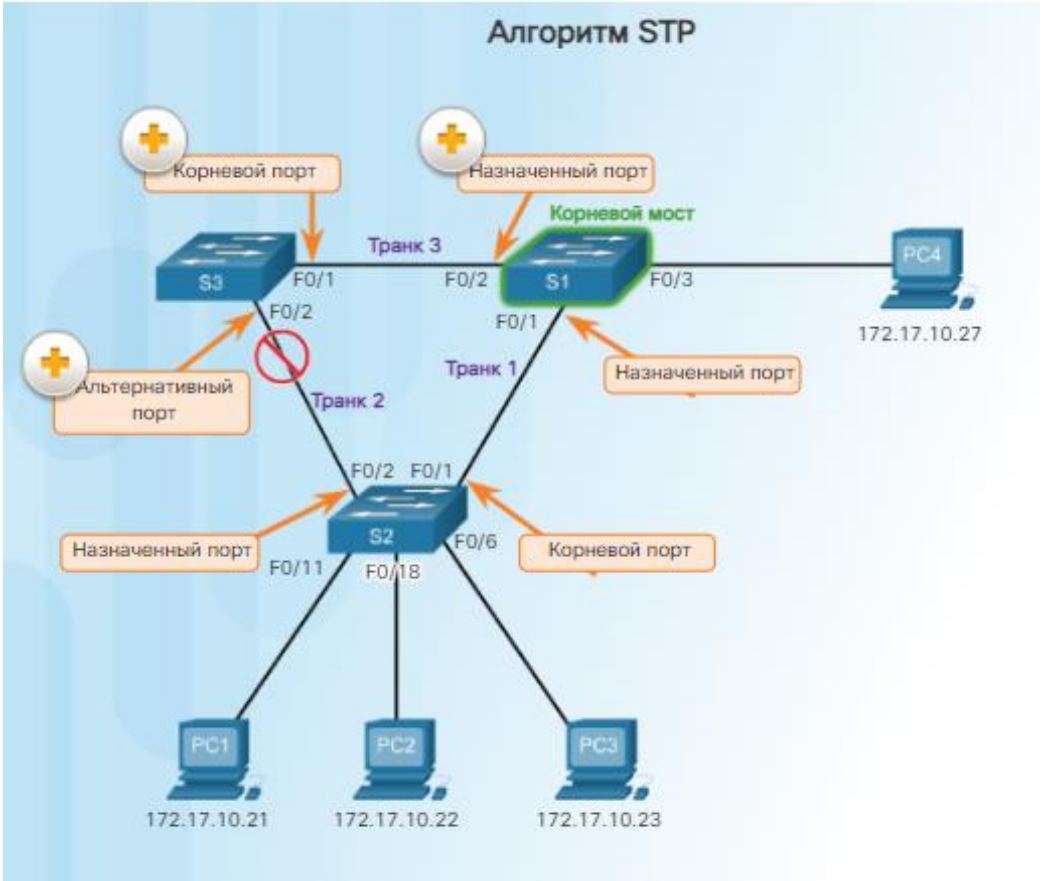
4. Настройте в качестве нативной неиспользуемую VLAN, которая будет не совпадать с VLAN 1, с помощью команды конфигурирования интерфейса switchport trunk native vlan *vlan_number*.

5. Отключите неиспользуемые порты и поместите их в неиспользуемую VLAN.

```
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)# shutdown
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)# exit
S1(config)#
```

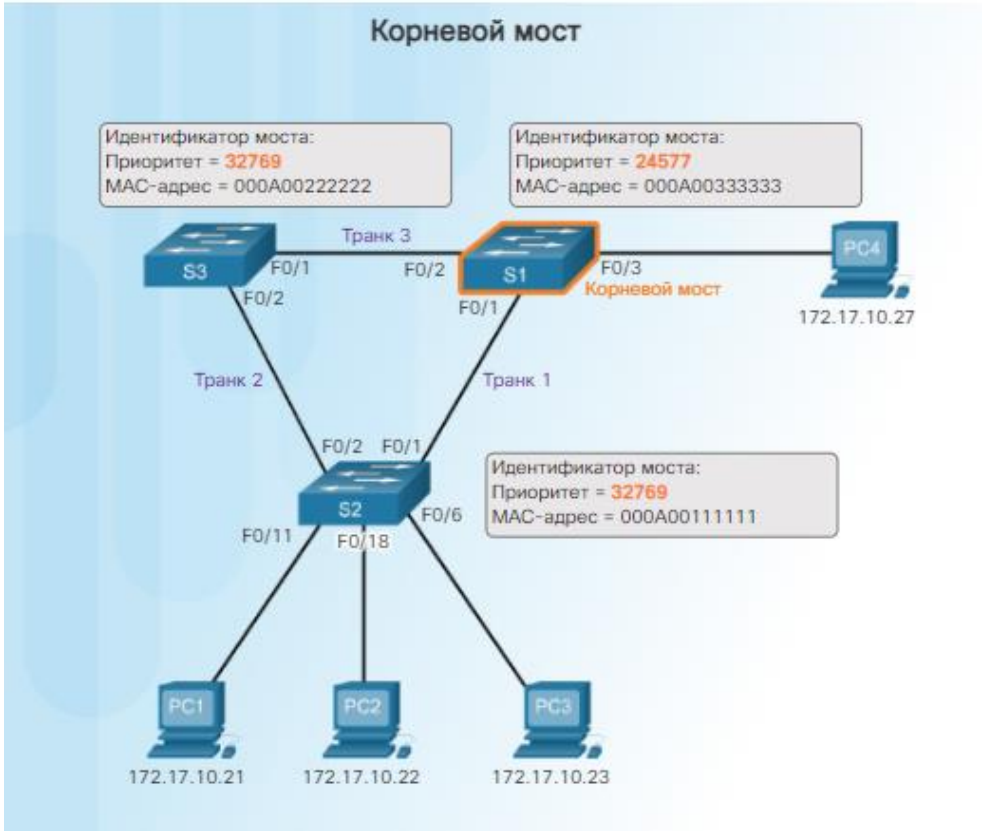
Введение в протокол связующего дерева

Протокол связующего дерева (Spanning Tree Protocol, STP) – это еще одна технология 2-го уровня, которая создает уязвимости в инфраструктуре 2-го уровня. Поэтому важно понимать роль и работу протокола STP.
Резервирование повышает готовность инфраструктуры 2-го уровня благодаря защите сети от критической точки отказа, например неисправного сетевого кабеля или неисправного коммутатора.



Роли портов STP

В алгоритме связующего дерева один коммутатор обозначается как корневой мост, который используется в качестве исходной точки для расчета всех трактов. На рисунке корневой мост (коммутатор S1) определяется в процессе выборов. Все коммутаторы, участвующие в протоколе STP, обмениваются кадрами BPDU, чтобы определить коммутатор с минимальным идентификатором моста (BID) в сети. Коммутатор с минимальным BID автоматически становится корневым мостом для расчетов по алгоритму связующего дерева.



Корневой мост STP

Как показано на рис. , в каждом экземпляре связующего дерева (коммутируемая локальная сеть или широковещательный домен) имеется коммутатор, выполняющий роль корневого моста. Корневой мост служит опорной точкой при всех расчетах связующего дерева для определения резервных трактов, которые должны быть блокированы.

Стоимость пути STP

Стоимость портов по умолчанию STP

Скорость канала и его имя	Стоимость (пересмотренная спецификация IEEE)	Стоимость (предыдущая спецификация IEEE)
10 Гбит/с	2	1
1 Гбит/с	4	1
100 Мбит/с	19	10
10 Мбит/с	100	100

Когда в экземпляре связующего дерева выбран корневой мост, алгоритм связующего дерева начинает процедуру определения оптимальных путей к корневому мосту от всех адресатов в широковещательном домене. Информация о тракте определяется путем суммирования индивидуальных стоимостей портов вдоль тракта от адресата к корневому мосту. Фактически каждый «адресат» это порт коммутатора.

Пятый учебный вопрос

Поля BPDU

Номер поля	Байтов	Поле
1-4	2	Protocol ID
	1	Version
	1	Message type
	1	Flags
5-8	8	Root ID
	4	Cost of path
	8	Bridge ID
	2	Port ID
9-12	2	Message age
	2	Max age
	2	Hello time

Protocol ID

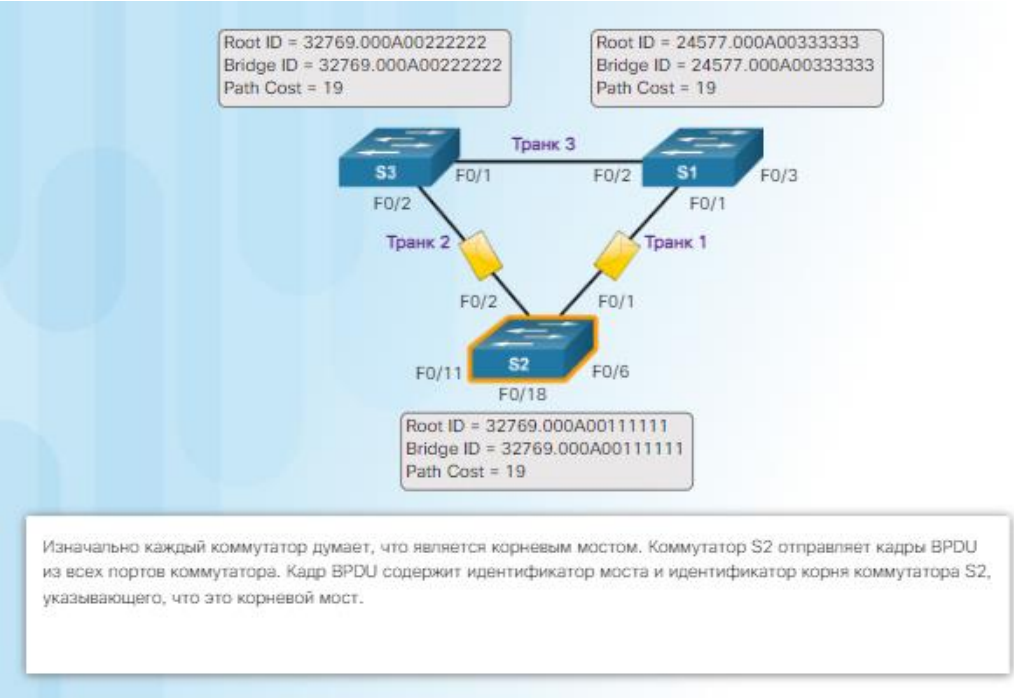
В поле Protocol ID указывается тип используемого протокола. Это поле содержит значение 0.

Формат кадра BPDU 802.1D

Алгоритм связующего дерева зависит от обмена пакетами BPDU для определения корневого моста.

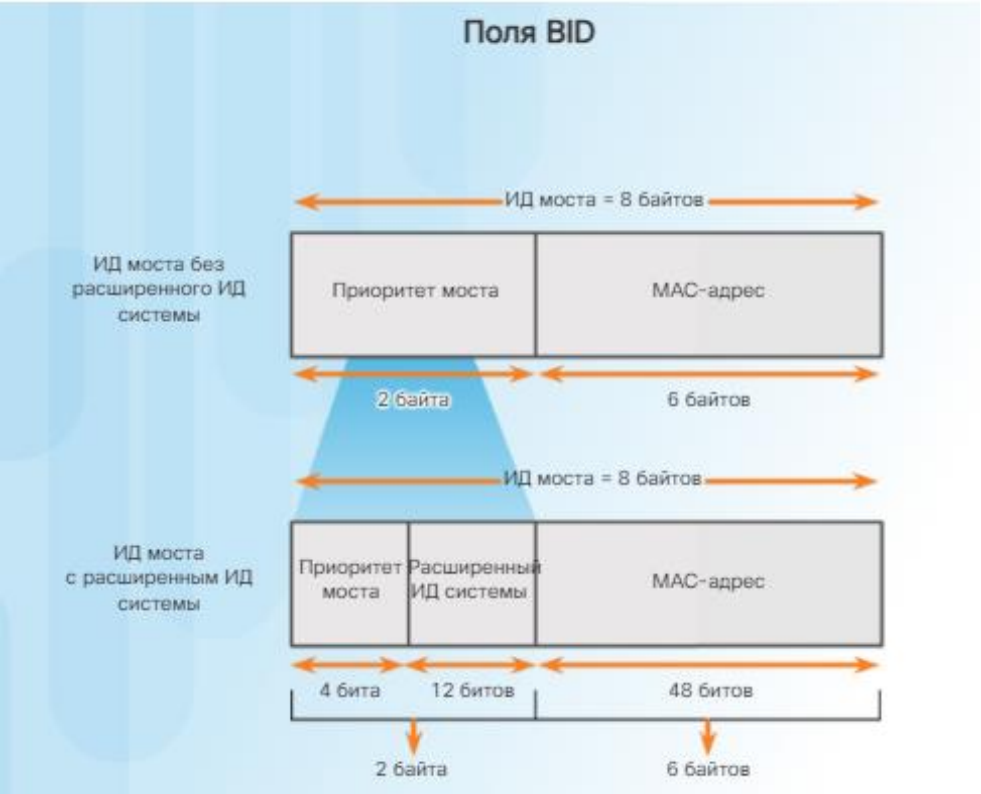
Кадр BPDU состоит из 12 отдельных полей, в которых передается информация о тракте и приоритете, используемая для определения корневого моста и трактов к нему.

Распространение и обработка BPDU-сообщений



Каждый коммутатор в широковещательном домене первоначально полагает, что он является корневым мостом экземпляра связующего дерева, поэтому передаваемые кадры BPDU содержат BID локального коммутатора в качестве идентификатора корня.

По умолчанию после загрузки коммутатора кадры BPDU передаются каждые две секунды.

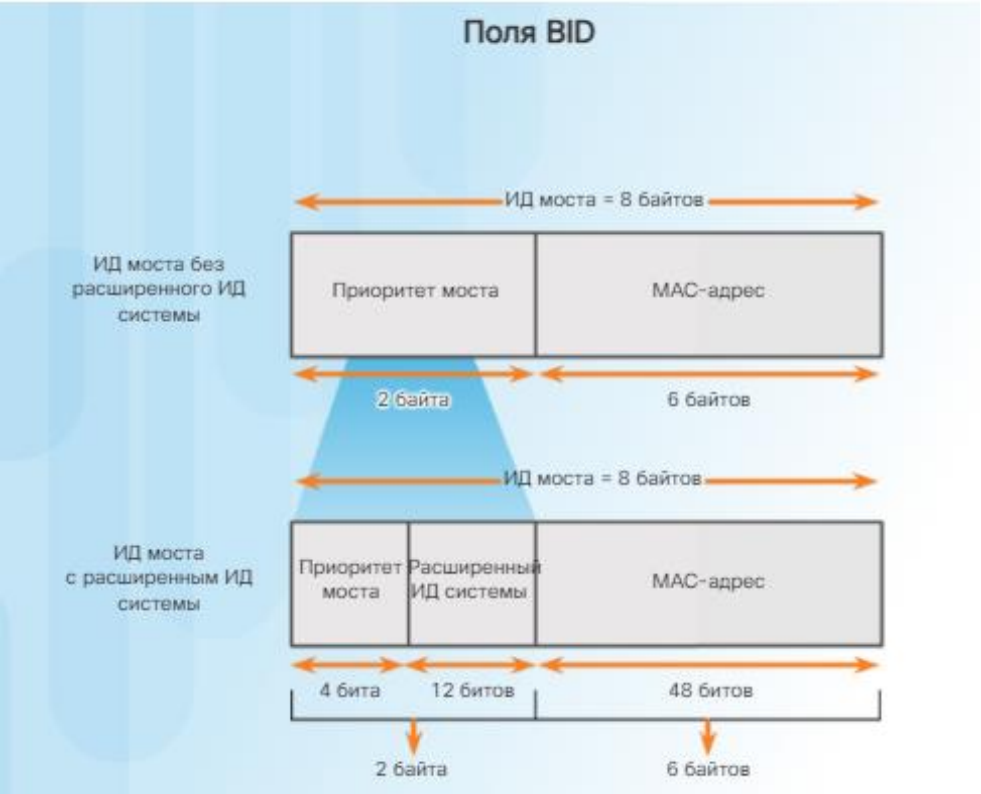


Расширенный ИД системы

Идентификатор моста (BID) используется для определения корневого моста в сети. Поле BID кадра BPDU состоит из трех отдельных полей. Каждое поле используется в процессе выбора корневого моста.

Приоритет моста

Приоритет моста – это настраиваемая величина, которая может использоваться для влияния на выбор коммутатора в качестве корневого моста. Коммутатор с наименьшим значением приоритета, что подразумевает наименьший BID, становится корневым мостом, поскольку наименьшее значение приоритета является предпочтительным. Например, чтобы гарантировать роль корневого моста конкретному коммутатору, установите значение его приоритета меньше, чем у других коммутаторов в сети. Значение приоритета по умолчанию для всех коммутаторов Cisco составляет 32768. Можно выбрать значение в диапазоне от 0 до 61440 с шагом 4096. Действительными значениями приоритета являются 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 и 61440. Все прочие значения отклоняются. Приоритет моста со значением 0 имеет преимущество перед всеми другими приоритетами.



Расширенный ИД системы

Расширенный идентификатор системы

Первые варианты стандарта IEEE 802.1D были созданы для сетей, в которых не использовались сети VLAN. Для всех коммутаторов существовало единое общее связующее дерево. По этой причине в старых коммутаторах Cisco расширенный идентификатор системы в кадрах BPDU мог не использоваться. С распространением использования сетей VLAN при сегментации сетевой инфраструктуры стандарт 802.1D был расширен и включил в себя поддержку сетей VLAN в форме требования включить идентификатор VLAN в кадр BPDU. Информация о VLAN включена в формат кадра BPDU с помощью расширенного идентификатора системы. Во всех новых коммутаторах использование расширенного идентификатора системы включается по умолчанию.

Как показано на рис. 1, поле приоритета моста занимает 2 байта или 16 бит; 4 бита используются для приоритета моста, а 12 бит – для расширенного идентификатора системы, который идентифицирует сеть VLAN, участвующую в данном процессе STP. Использование этих 12 бит для расширенного идентификатора системы сокращает приоритет моста до 4 бит.

Расширенный ИД системы

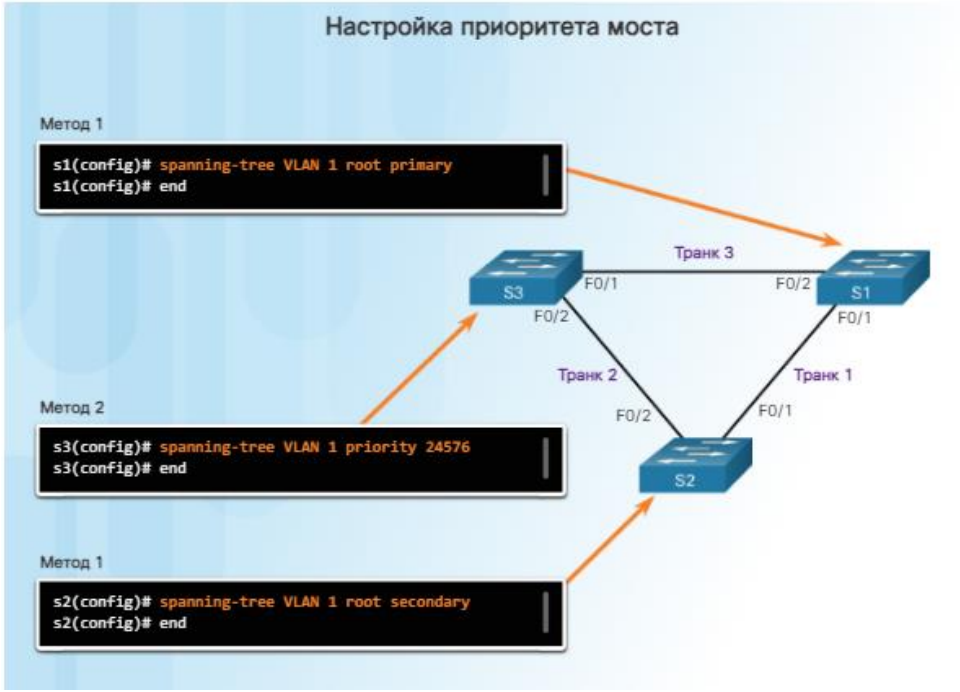
В этом процессе младшие 12 бит зарезервированы для идентификатора VLAN, а старшие 4 бита – для приоритета моста. Это объясняет, почему значение приоритета моста может конфигурироваться только с шагом 4096 или 2^12. Если старшие биты имеют значение 0001, тогда приоритет моста имеет значение 4096; если старшие биты имеют значение 1111, тогда приоритет моста имеет значение 61440 (= 15 x 4096). Коммутаторы Catalyst серий 2960 и 3560 не позволяют конфигурировать для приоритета моста значение 65536 (= 16 x 4096), поскольку оно предполагает использование 5-го бита, что невозможно вследствие использования расширенного идентификатора системы.

Значение расширенного идентификатора системы добавляется к значению приоритета моста в BID, чтобы идентифицировать приоритет и VLAN кадра BPDU.

Если два коммутатора сконфигурированы с одинаковым приоритетом и имеют одинаковые расширенные идентификаторы системы, коммутатор с меньшим шестнадцатеричным значением MAC-адреса будет иметь меньший BID. Изначально все коммутаторы сконфигурированы с одинаковым значением приоритета по умолчанию. Поэтому MAC-адрес становится решающим фактором при определении коммутатора, который станет корневым мостом. Администратору рекомендуется сконфигурировать предполагаемый корневой мост с минимальным значением приоритета, чтобы гарантировать, что решение о выборе корневого моста будет наилучшим образом соответствовать сетевым требованиям. Это также гарантирует, что добавление в сеть новых коммутаторов не запустит новый выбор связующего дерева, что может прервать связь до выбора нового корневого моста.

На рис. 2 коммутатор S1 имеет более низкое значение приоритета, чем другие коммутаторы; поэтому он предпочтителен в качестве корневого моста для данного образца связующего дерева.

Если все коммутаторы сконфигурированы с одинаковым приоритетом, например когда все коммутаторы сохраняют конфигурацию по умолчанию со значением приоритета 32768, MAC-адрес становится решающим фактором для выбора коммутатора в качестве корневого моста.



Выбор корневого моста

Если администратор хочет использовать в качестве корневого моста конкретный коммутатор, следует настроить значение приоритета моста таким образом, чтобы оно было **меньше значений приоритета** моста всех других коммутаторов сети.

Для конфигурирования значения приоритета моста в коммутаторах Cisco Catalyst существует два метода.

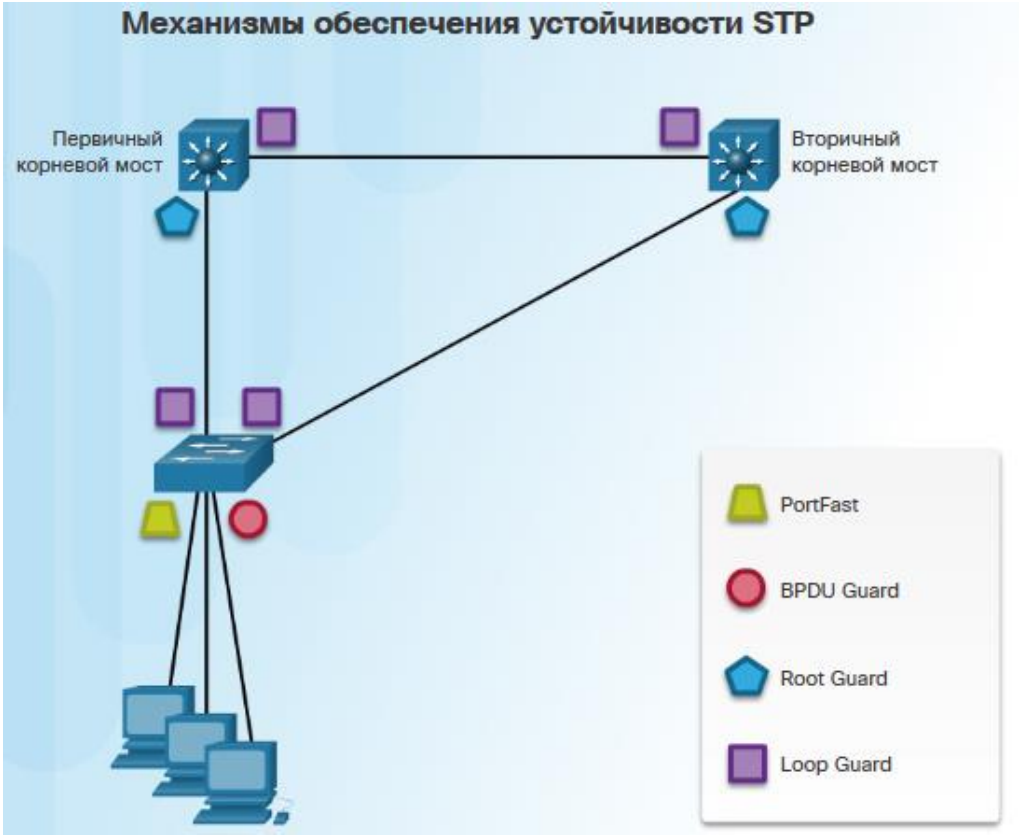
Пятый учебный вопрос

Сетевые злоумышленники могут манипулировать STP, чтобы проводить атаки путем спуфинга корневого моста и изменения топологии сети. Злоумышленники могут сделать так, чтобы их хосты выглядели как корневые мосты, и в результате перехватить весь трафик ближайшего коммутируемого домена.

Как показано на рис. 1, 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. В случае успеха, как показано рис. 2, хост злоумышленника становится корневым мостом и получает доступ к множеству кадров, которые в противном случае были бы ему недоступны.

Атака может использоваться для разрушения всех трех объектов защиты: конфиденциальности, целостности и готовности.

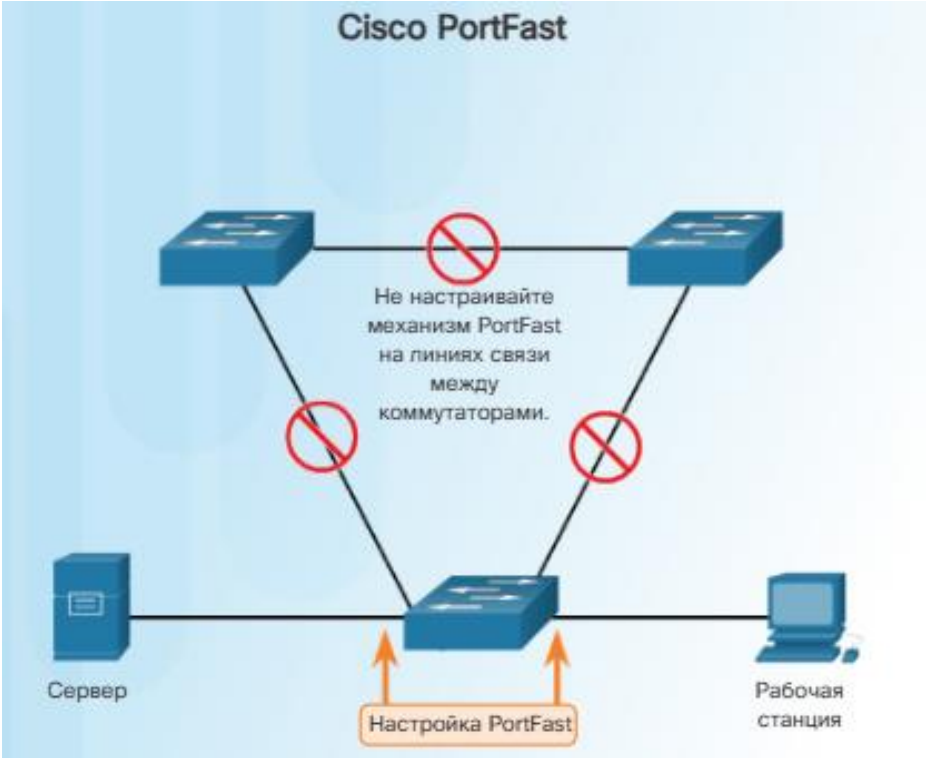
Пятый учебный вопрос



Рекомендуются следующие механизмы обеспечения стабильности STP:

- **PortFast** незамедлительно переводит интерфейс в состояние передачи;
- **BPDU Guard** незамедлительно переводит порт в состояние отключения, когда порт принимает пакет BPDU;
- **Root Guard** предотвращает переход неподходящего коммутатора в состояние корневого моста;
- **Loop Guard** предотвращает превращение альтернативных или корневых портов в назначенные порты.

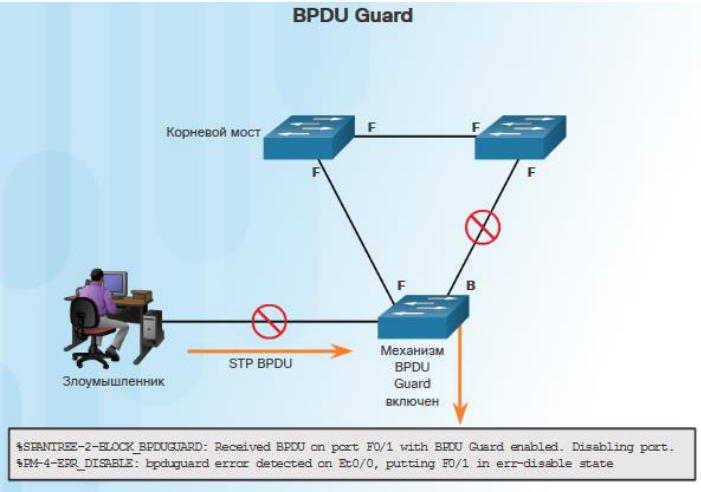
Пятый учебный вопрос



Функция связующего дерева PortFast незамедлительно переводит интерфейс, сконфигурированный как порт доступа 2-го уровня, из состояния блокировки в состояние передачи, минуя состояния прослушивания и обучения. Функция PortFast может использоваться в портах доступа 2-го уровня, подключенных к одиночной рабочей станции или серверу, как показано на рисунке. Этот механизм позволяет устройствам подключаться к сети немедленно, не ожидая конвергенции STP. Поскольку механизм PortFast имеет целью минимизировать время ожидания конвергенции STP портами доступа, он должен использоваться только в портах доступа. Если PortFast включен в порте, подключенном к другому коммутатору, существует риск образования петли связующего дерева.

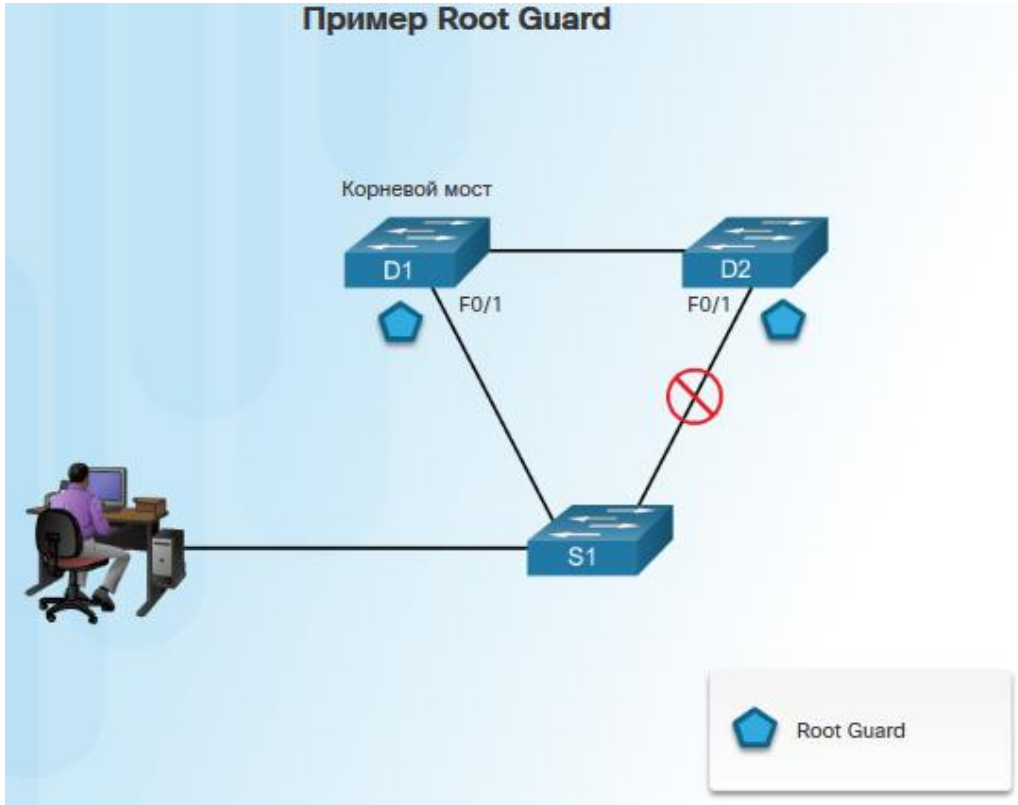
Portfast может быть сконфигурирован глобально во всех немагистральных портах с помощью команды **spanning-tree portfast default** режима глобальной конфигурации. Кроме того, PortFast можно включить в интерфейсе с помощью команды конфигурирования интерфейса **spanning-tree portfast interface** . Чтобы проверить включение механизма PortFast, используйте команду **show running-config interface** *type slot/port* .

Пятый учебный вопрос



Используйте команду **spanning-tree portfast bpduguard default** в режиме глобальной конфигурации, чтобы глобально включить функцию BPDU Guard во всех портах с включенной функцией PortFast.
BPDU guard наилучшим образом работает в портах, обращенных к пользователям, где она предотвращает появление мошеннических коммутаторов и других сетевых устройств на хостах злоумышленников. В данном примере злоумышленник пытается отправить пакет BPDU в коммутатор с глобально включенными функциями PortFast и BPDU guard. Обратите внимание на уведомление в командной строке, в котором сообщается об отключении порта FastEthernet 0/1.
Чтобы отобразить информацию о состоянии связующего дерева, используйте команду **show spanning-tree summary.**

Другой полезной командой для проверки конфигурации BPDU guard является команда **show spanning-tree summary totals**. Команда показывает сводную информацию о состояниях портов или общие данные в разделе состояния связующего дерева.
Внимание на уведомление в командной строке, в котором сообщается об отключении порта FastEthernet 0/1.



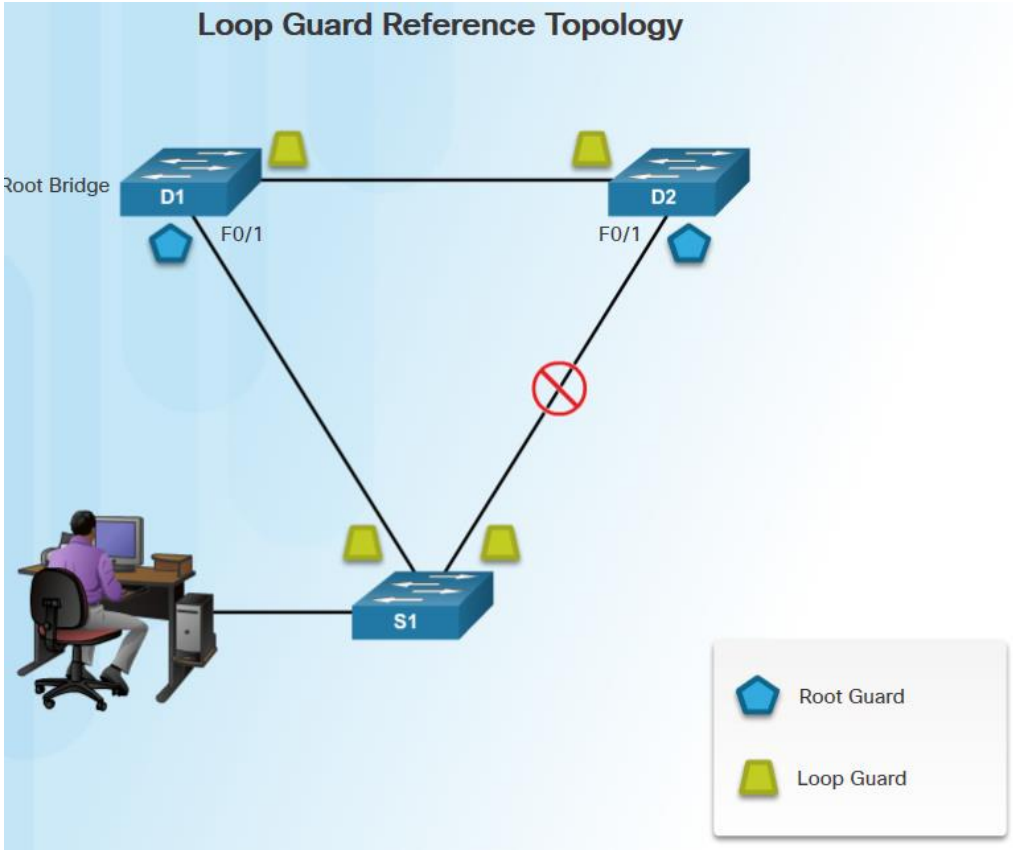
Конфигурирование Root Guard
В сети существуют некоторые коммутаторы, которые никогда, ни при каких обстоятельствах не должны становиться корневым мостом STP. Root Guard обеспечивает способ укрепления положения корневых мостов в сети, вводя ограничения на коммутаторы, которые могут стать корневым мостом.

Используйте команду конфигурирования интерфейса **spanning-tree guard root**, чтобы сконфигурировать Root Guard в интерфейсе.

Пятый учебный вопрос

В сети существуют некоторые коммутаторы, которые никогда, ни при каких обстоятельствах не должны становиться корневым мостом STP. Root Guard обеспечивает способ укрепления положения корневых мостов в сети, вводя ограничения на коммутаторы, которые могут стать корневым мостом.
Root Guard лучше всего устанавливать на портах, к которым подключены коммутаторы, которые не должны быть корневыми мостами. Если порт с включенной Root Guard принимает пакеты BPDU, которые имеют более высокий приоритет по сравнению с теми, что посылает текущий корневой мост, этот порт переводится в состояние несовместимости с корнем. По существу, это состояние эквивалентно состоянию прослушивания STP, когда через порт не передается трафик данных. Восстановление работы порта происходит немедленно после того, как атакующее устройство перестает посылать высокоприоритетные пакеты BPDU.
Используйте команду конфигурирования интерфейса **spanning-tree guard root,** чтобы сконфигурировать Root Guard в интерфейсе.
На рисунке корневым мостом является устройство D1. В случае отказа устройства D1 корневым мостом должно стать только устройство D2. Чтобы коммутатор S1 никогда не мог стать корневым мостом, в интерфейсах F0/1 устройств D1 и D2 должна быть включена Root Guard.
Для просмотра портов Root Guard, которые получили высокоприоритетные пакеты BPDU и переведены в состояние несовместимости с корнем, используйте команду **show spanning-tree inconsistent ports** .
Примечание. Root Guard может показаться необязательной, поскольку администратор может вручную установить приоритет моста коммутатора равным 0. Однако это не служит гарантией того, что такой коммутатор будет выбран корневым мостом. Другой коммутатор также может быть выбран корневым мостом, если он также имеет приоритет со значением ноль и меньшее значение MAC-адреса.

Пятый учебный вопрос



Если по какой-либо причине передача трафика в одном направлении прекращается, образуется однонаправленный канал, что может привести к созданию петли на 2-м уровне.

Loop Guard включена во всех портах, где не включена Root Guard, с помощью команды конфигурирования интерфейса **spanning-tree guard loop** .

Конфигурирование Loop Guard

В двунаправленных каналах трафик передается в обоих направлениях. Если по какой-либо причине передача трафика в одном направлении прекращается, образуется однонаправленный канал, что может привести к созданию петли на 2-м уровне. Работа протокола STP основывается на непрерывных приеме или передаче пакетов BPDU в соответствии с ролями портов. Назначенный порт передает пакеты BPDU, а неназначенный порт принимает пакеты BPDU. На 2-м уровне петля обычно возникает в том случае, когда порт STP в топологии с резервированием прекращает принимать пакеты BPDU и ошибочно переходит в состояние передачи.

Функция Loop Guard STP предоставляет дополнительную защиту от возникновения петель на 2-м уровне. Если пакеты BPDU не поступают в неназначенный порт с включенной функцией Loop Guard, порт переходит в несовместимое с петлями состояние блокировки, вместо состояний прослушивания/обучения/передачи. Без функции Loop Guard порт принял бы роль назначенного порта и создал петлю.

Как показано на рис. 1, Loop Guard включена во всех портах, где не включена Root Guard, с помощью команды конфигурирования интерфейса **spanning-tree guard loop** .

Примечание. Loop Guard может быть также включена глобально с помощью команды **spanning-tree loopguard default** режима глобальной конфигурации. Это позволяет включить Loop guard на всех двухточечных каналах.

С помощью средства проверки синтаксиса, приведенного на рисунке 2, сконфигурируйте PortFast и BPDU Guard.

Учебные вопросы и цели занятия:

1. Угрозы в локальной сети.
2. Защита таблицы CAM.
3. Защита протоколов DHCP, ARP.
4. Защита технологии VLAN, PVLAN.
5. Защита протокола STP.

Заключение

На сегодняшнем занятии рассмотрены методы и средства обеспечения ИБ компьютерной сети, а также раскрыли данную тему, путем приведения основных методов обеспечения ИБ сетевого оборудования и протоколов маршрутизации.

Полученные знания позволяют применять их для эксплуатации, построения и модернизации сетей ТСКП, RSNET, понимании роли и места протоколов защищенного удаленного доступа в ТСКП.

На самостоятельной работе необходимо дополнительно изучить рекомендованную литературу с целью получения дополнительных сведений из области знаний.