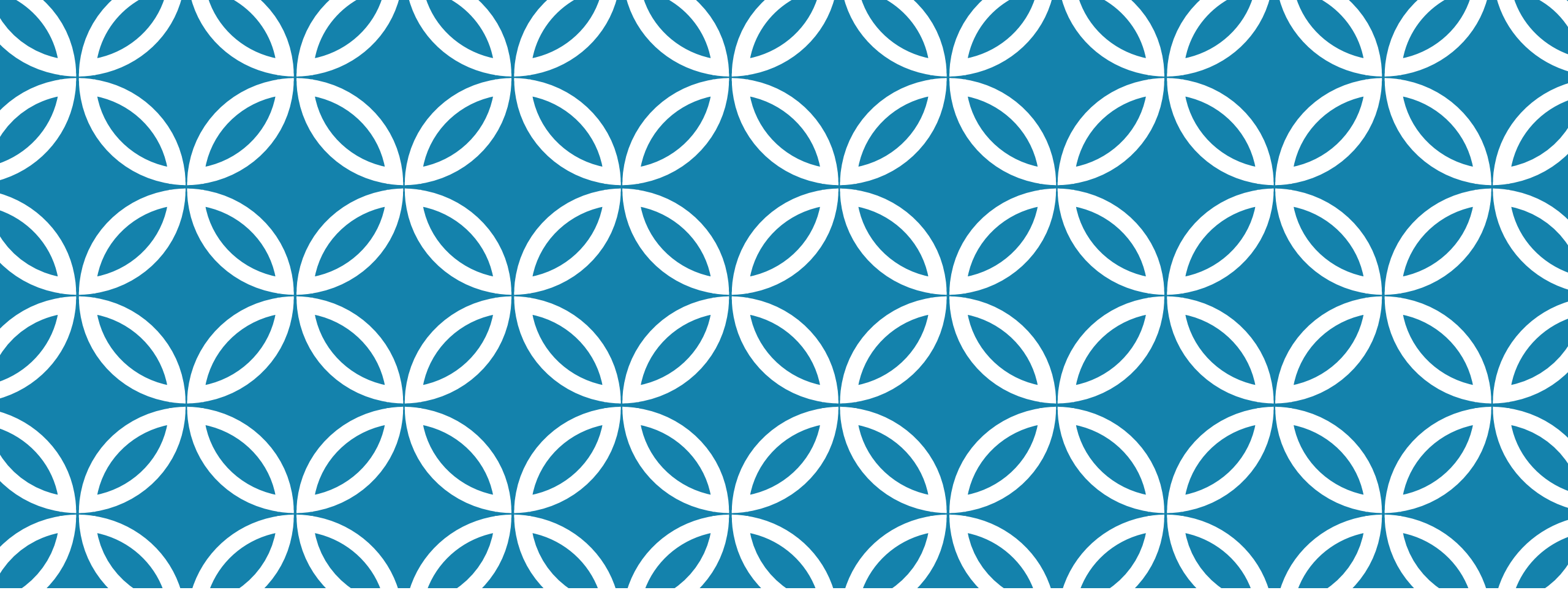


МОДУЛЬ 10. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТИ

КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

10.1 БЕЗОПАСНОСТЬ ОКОНЕЧНЫХ УСТРОЙСТВ

10.1.1 СЕТЕВЫЕ АТАКИ СЕГОДНЯ

В новостях часто рассказывают о внешних сетевых атаках на корпоративные сети. Просто найдите в Интернете «последние сетевые атаки», чтобы найти актуальную информацию о текущих атаках. Скорее всего, эти атаки будут включать одно или несколько из следующих действий:

Распределенный отказ в обслуживании (DDoS) – это скоординированная атака со многих устройств, называемых зомби, с целью ослабления или прекращения публичного доступа к веб-сайту и ресурсам организации.

Кража данных – это атака, при которой серверы или хосты организации подвергаются риску кражи конфиденциальной информации.

Вредоносное ПО – это атака, при которой узлы организации заражаются вредоносным программным обеспечением, вызывающим множество проблем. Например, вымогатель, такой как WannaCry, шифрует данные на хосте и блокирует доступ к нему, пока выкуп не будет выплачен.

10.1.2 БЕЗОПАСНОСТЬ СЕТЕВЫХ УСТРОЙСТВ

Для защиты периметра сети от внешнего доступа необходимы различные устройства обеспечения сетевой безопасности. Эти устройства могут включать в себя следующее:

1. Маршрутизатор с поддержкой VPN обеспечивает безопасное соединение с удаленными пользователями в общедоступной сети и в корпоративной сети. VPN-сервисы могут быть интегрированы в брандмауэр.

2. NGFW предоставляет такие возможности, как отслеживание работы приложений и управление ими, система предотвращения вторжений нового поколения, расширенная защита от вредоносного ПО и фильтрация URL-адресов.

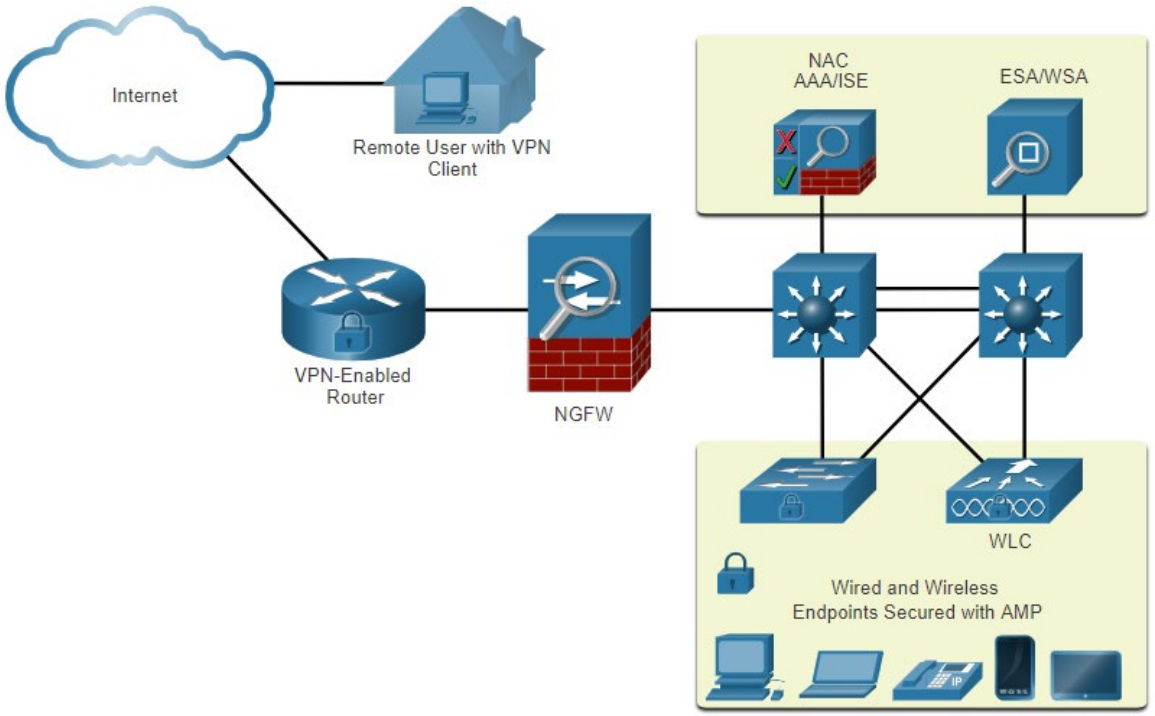
3. Устройство NAC включает в себя такие сервисы (AAA) как аутентификация, авторизация и учет. На крупных предприятиях эти службы могут быть включены в устройство, которое может управлять политиками доступа для широкого круга пользователей и типов устройств. Cisco Identity Services Engine (ISE) является примером устройства NAC.

10.1.3 ЗАЩИТА ОКОНЕЧНЫХ УСТРОЙСТВ

Конечные точки - это хосты, которые обычно состоят из ноутбуков, настольных компьютеров, серверов и IP-телефонов, а также принадлежащих сотрудникам устройств. Конечные точки особенно восприимчивы к атакам, связанным с вредоносными программами, которые исходят из электронной почты или просмотра веб-страниц.

На конечных точках обычно использовались традиционные функции безопасности на уровне хоста, такие как антивирусное ПО, брандмауэры на базе хоста и системы предотвращения вторжений на базе хоста (HIPS).

Однако сегодня конечные точки лучше всего защищены комбинацией NAC, программного обеспечения AMP на основе хоста, устройства защиты электронной почты (ESA) и устройства веб-безопасности (WSA).



10.1.4 УСТРОЙСТВО ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ CISCO ESA

Cisco ESA - это устройство, предназначенное для мониторинга SMTP-протокола. Устройство Cisco ESA постоянно обновляется, используя информационные каналы в режиме реального времени от группы Talos Cisco, которая обнаруживает и сопоставляет угрозы, используя всемирную систему мониторинга баз данных. Эти данные об угрозах извлекаются устройствами Cisco ESA каждые три-пять минут.

Вот некоторые из функций устройства Cisco ESA:
1. Блокировка известных угроз.
2. Защищает от вредоносного ПО, которое уклоняется от первоначального обнаружения.
3. Отбрасывает электронную почту, содержащую плохие ссылки.
4. Блокирует доступ к новым зараженным сайтам.
5. Шифрует содержимого в исходящей электронной почте, чтобы предотвратить потерю данных.

10.1.5 УСТРОЙСТВО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-ТРАФИКА CISCO WSA

Устройство защиты веб-трафика Cisco (WSA) - это технология нейтрализации веб-угроз. Вместе они позволяют решить задачи, связанные с защитой и контролем веб-трафика. WSA предоставляет защиту от вредоносного ПО, мониторинг и контроль функционирования приложений, а также средства управления политиками допустимого использования, создания отчетов.

Cisco WSA обеспечивает полный контроль над доступом пользователей к сети Интернет. Некоторые функции и приложения, такие как чат, обмен сообщениями, видео и аудио, могут быть разрешены, ограничены по времени и полосе пропускания или заблокированы в соответствии с требованиями организации.

WSA может выполнять внесение в черный список URL-адресов, фильтрацию URL-адресов, сканирование на наличие вредоносных программ, категоризацию URL-адресов, фильтрацию веб-приложений, а также шифрование и дешифрование веб-трафика.

10.2 УПРАВЛЕНИЕ ДОСТУПОМ
10.2.1 АУТЕНТИФИКАЦИЯ С ЛОКАЛЬНЫМ ПАРОЛЕМ

Многие типы аутентификации могут быть выполнены на сетевых устройствах, и каждый метод предлагает различные уровни безопасности.

Самый простой метод аутентификации удаленного доступа - это настройка комбинации логина и пароля на консоли, линиях vty и вспомогательных портах, как показано в линиях vty в следующем примере.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

SSH — это наиболее безопасный протокол для удаленного доступа.
Требуется имя пользователя и пароль.
Имя пользователя и пароль могут быть аутентифицированы методом локальной базы данных.
Метод локальной базы данных имеет некоторые ограничения:
Учетные записи пользователей необходимо настраивать локально на каждом устройстве, поэтому такое решение аутентификации не будет масштабируемым.
В системе с локальной базой данных не предусмотрен метод восстановления аутентификации.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

10.2.2 КОМПОНЕНТЫ AAA

Сервисы обеспечения сетевой безопасности AAA (аутентификация, авторизация и учет) предоставляют базовую архитектуру для настройки средств управления доступом на сетевом устройстве.

AAA позволяет контролировать, какие пользователи имеют право доступа к сети (аутентификация), какие действия они могут выполнять, находясь в сети (авторизация), а также позволяет следить за их действиями во время доступа к сети (учет).

10.2.3 АУТЕНТИФИКАЦИЯ

Локальный и серверный являются двумя распространенными методами реализации аутентификации AAA.

Локальная аутентификация (AAA)

- Local AAA хранит имена пользователей и пароли локально в сетевом устройстве, таком как маршрутизатор Cisco.
- Пользователи проходят аутентификацию в локальной базе данных.
- Локальная аутентификация AAA лучше всего подходит для сетей небольшого размера.

Серверная аутентификация (AAA)

- При использовании этого метода маршрутизатор обращается к центральному серверу аутентификации AAA.
- AAA-сервер содержит имена пользователей и пароли для всех пользователей.
- Маршрутизатор аутентификации AAA использует для связи с сервером аутентификации AAA протокол Terminal Access Controller Access Control System (TACACS+) или протокол Remote Authentication Dial-In User Service (RADIUS).
- Когда есть несколько маршрутизаторов и коммутаторов, AAA на основе сервера является более подходящим решением.

10.2.4 АВТОРИЗАЦИЯ

Авторизация выполняется автоматически и не требует от пользователей дополнительных действий после аутентификации.

Средства контроля авторизации определяют, что пользователь может и чего не может делать в сети после успешной аутентификации.

При авторизации используется набор атрибутов, описывающий доступ пользователя к сетевой инфраструктуре. Эти атрибуты используются сервером AAA для определения привилегий и ограничений для этого пользователя.

10.2.5 УЧЕТ

Учет AAA собирает данные об использовании в журналах AAA и формирует отчеты. Организация может использовать такие данные, например, в целях аудита или выставления счетов. Собираться могут такие данные, как время начала и остановки подключения, выполненные команды, количество пакетов и количество байтов.

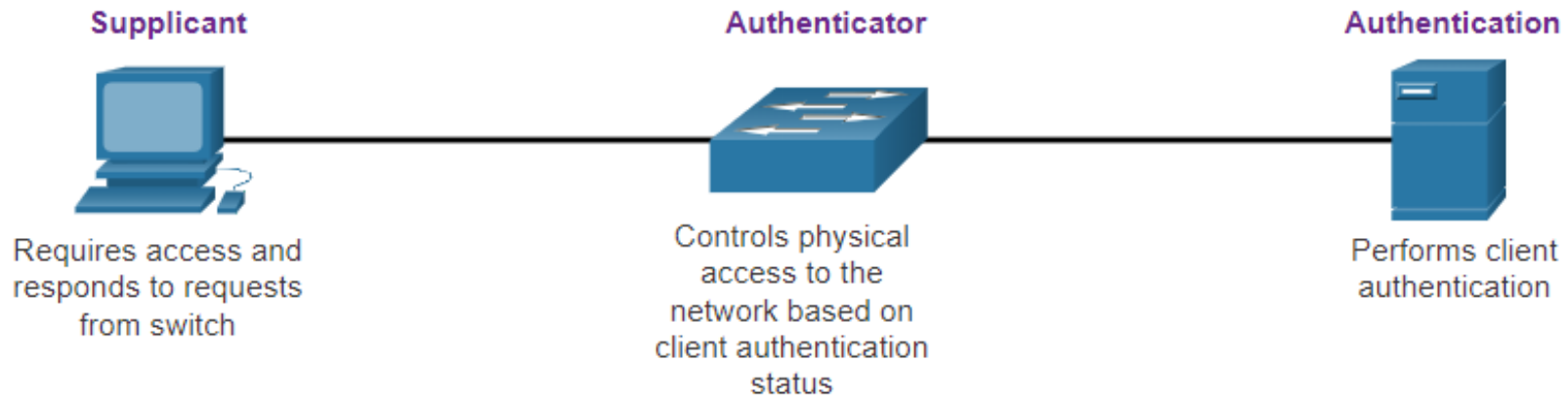
Учет широко используется в сочетании с аутентификацией AAA.
Серверы AAA ведут журналы с подробной информацией о том, какие действия прошедший аутентификацию пользователь выполнял на данном устройстве. Сюда входят все команды EXEC и команды настройки конфигурации, поданные пользователем.
Журнал содержит множество полей данных, включая имя пользователя, дату и время, когда команда была введена пользователем. Эта информация полезна при поиске и устранении неполадок устройств. Она также предоставляет улики в борьбе с лицами, предпринимающими вредоносные действия.

10.2.6 802.1X

Стандарт IEEE 802.1X определяет правила управления доступом на основе портов и протокол аутентификации. Протокол ограничивает подключение неавторизованных рабочих станций к локальной сети через общедоступные порты коммутатора. Сервер аутентификации аутентифицирует все рабочие станции, которые подключаются к порту коммутатора, перед тем, как предоставить им доступ к службам коммутатора или ЛВС.
При использовании аутентификации 802.1X на уровне портов устройства в сети могут иметь следующие роли.
Запрашивающее устройство - это устройство, на котором выполняется совместимое с 802.1X клиентское программное обеспечение, доступное для проводных или беспроводных устройств.
Коммутатор (Аутентификатор) – коммутатор выступает в роли посредника (прокси) между клиентом и сервером аутентификации. Он запрашивает идентификационные данные у клиента, проверяет эту информацию на сервере аутентификации и передает ответ клиенту. Другим устройством, которое может действовать как аутентификатор, является беспроводная точка доступа.
Сервер аутентификации – сервер проверяет подлинность клиента и уведомляет коммутатор или беспроводную точку доступа о том, что клиент имеет или не авторизован для доступа к локальной сети и услугам коммутатора.

10.2.6 802.1X

Стандарт IEEE 802.1X определяет правила управления доступом на основе портов и протокола аутентификации. Протокол ограничивает подключение неавторизованных рабочих станций к локальной сети через общедоступные порты коммутатора. Сервер аутентификации аутентифицирует все рабочие станции, которые подключаются к порту коммутатора, перед тем, как предоставить им доступ к службам коммутатора или ЛВС.



10.2.6 802.1X

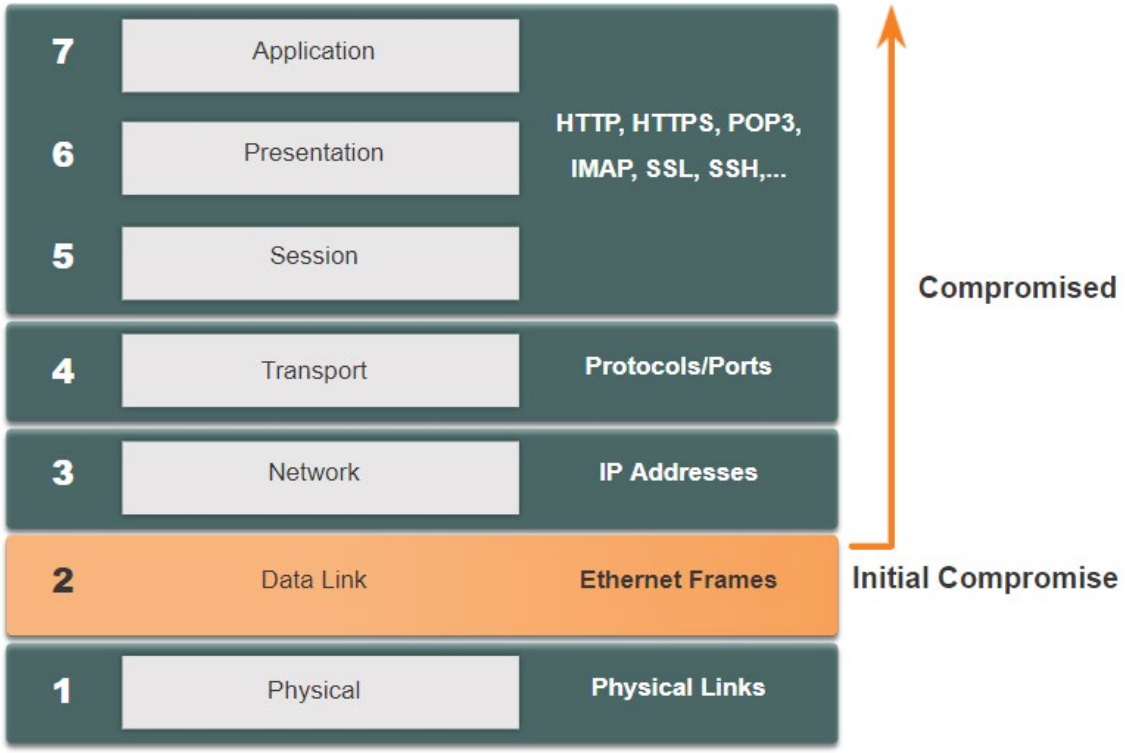
При использовании аутентификации 802.1X на уровне портов устройства в сети могут иметь следующие роли:
Запрашивающее устройство – это устройство, на котором выполняется совместимое с 802.1X клиентское программное обеспечение, доступное для проводных или беспроводных устройств.
Коммутатор (Аутентификатор) – коммутатор выступает в роли посредника (прокси) между клиентом и сервером аутентификации. Он запрашивает идентификационные данные у клиента, проверяет эту информацию на сервере аутентификации и передает ответ клиенту. Другим устройством, которое может действовать как аутентификатор, является беспроводная точка доступа.
Сервер аутентификации – сервер проверяет подлинность клиента и уведомляет коммутатор или беспроводную точку доступа о том, что клиент имеет или не авторизован для доступа к локальной сети и услугам коммутатора.

10.3 УГРОЗЫ БЕЗОПАСНОСТИ НА УРОВНЕ 2

10.3.1 УЯЗВИМОСТИ НА УРОВНЕ 2

Напомним, что эталонная модель OSI разделена на семь уровней, которые работают независимо друг от друга. На рисунке показана функция каждого слоя и основные элементы, которые можно использовать.

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.



10.3.2 УЯЗВИМОСТИ НА УРОВНЕ 2

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.

Категория	Примеры
Атака на таблицу MAC	Включает в себя атаки с переполнением таблицы CAM
Атаки на сети VLAN	Включат в себя атаки с переходом по VLAN и с двойным тегированием VLAN. Также это включает в 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 «отравление» ARP-кэша
Атаки с подменой адреса	Включает атаки подмены MAC и IP адресов
Атака STP	Включает в себя атаки путем манипуляции протоколом STP

10.3.3 ТЕХНОЛОГИИ НЕЙТРАЛИЗАЦИИ 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. В нынешней ситуации, с учетом внедрения концепции BYOD и появления более изощренных способов атак, наши локальные сети становятся более уязвимыми для проникновения извне.

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.

10.4 АТАКА НА ТАБЛИЦУ MAC-АДРЕСОВ

10.4.1 ОБЗОР РАБОТЫ КОММУТАТОРА

Напомним, что 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.

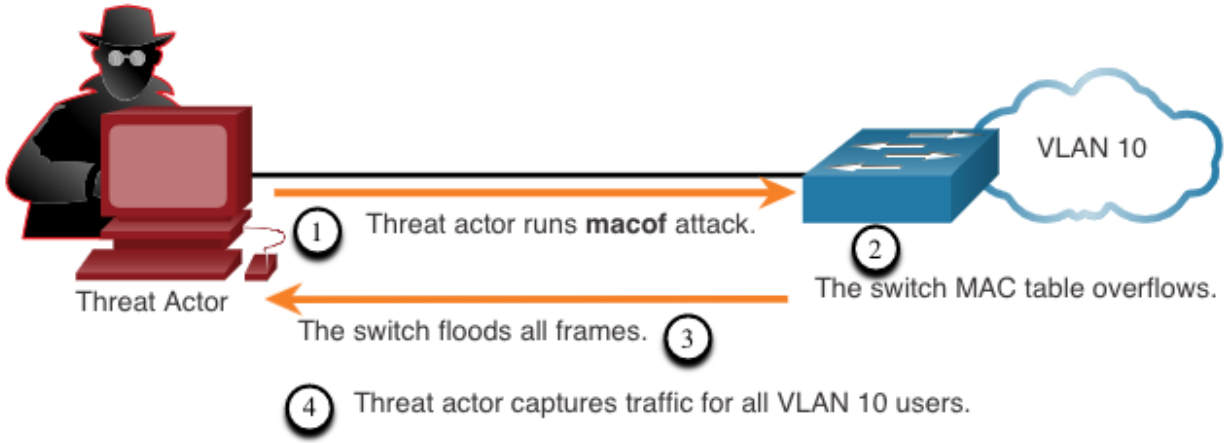
```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca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

10.4.2 ОБЗОР РАБОТЫ КОММУТАТОРА

Все таблицы MAC адресов 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 адресов. 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.



10.4.3 НЕЙТРАЛИЗАЦИЯ 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-адресов. Например, коммутатор Catalyst 6500 может хранить 132 000 MAC-адресов в своей таблице. Такой инструмент как macof может переключать скорость до 8000 поддельных кадров в секунду; создать атаку переполнения таблицы MAC-адресов за несколько секунд.

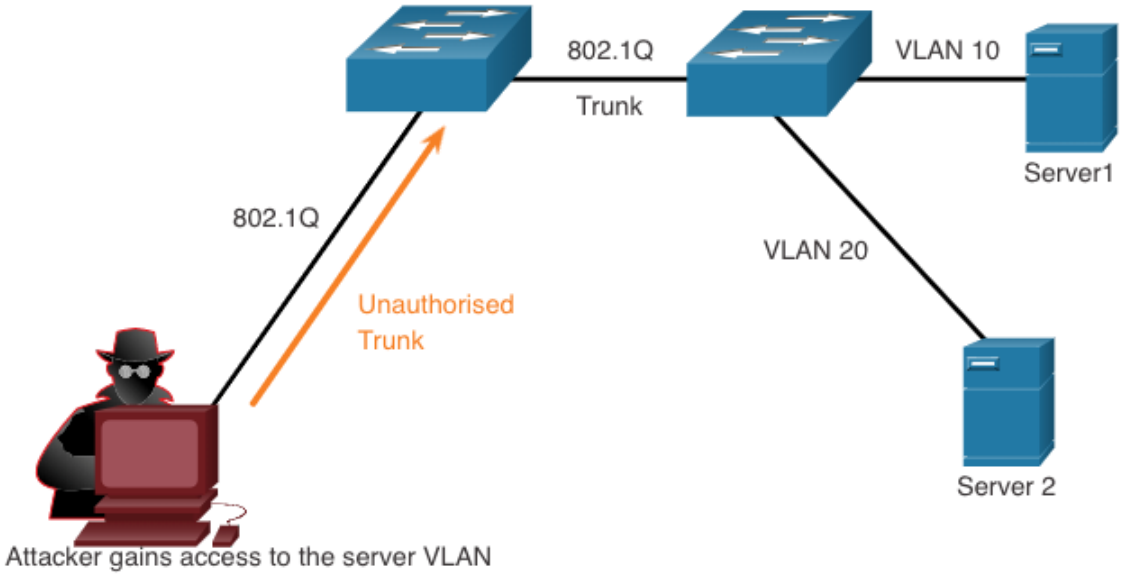
Другая причина, по которой эти инструменты атаки опасны, заключается в том, что они не только влияют на локальный коммутатор, но и на другие подключенные коммутаторы уровня 2. Когда таблица MAC-адресов коммутатора заполнена, она начинает заполнять все порты, включая те, которые подключены к другим коммутаторам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

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

10.5 АТАКИ НА ЛОКАЛЬНУЮ СЕТЬ
10.5.1 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.

Злоумышленник настраивает хост на подделку сигналов 802.1Q и проприетарной сигнализации DTP-протокола Cisco для магистрального канала между коммутаторами. В случае успеха коммутатор устанавливает магистральную связь с хостом, как показано на рисунке. Теперь злоумышленник может получить доступ ко всем VLAN на коммутаторе. Хакер может отправлять и получать трафик в любой VLAN, эффективно переключаясь между VLAN.



10.5.1 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.

10.5.1 АТАКА VLAN HOPPING

Этот вид атаки является однонаправленным и работает, только если злоумышленник подключён к порту, находящимся в той же VLAN, что и сеть native VLAN транкового порта. Идея состоит в том, что двойная маркировка позволяет злоумышленнику отправлять данные на хосты или серверы в VLAN, которые в противном случае были бы заблокированы каким-либо типом конфигурации контроля доступа. Предположительно, обратный трафик также будет разрешен, что дает злоумышленнику возможность общаться с устройствами в заблокированной VLAN.

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

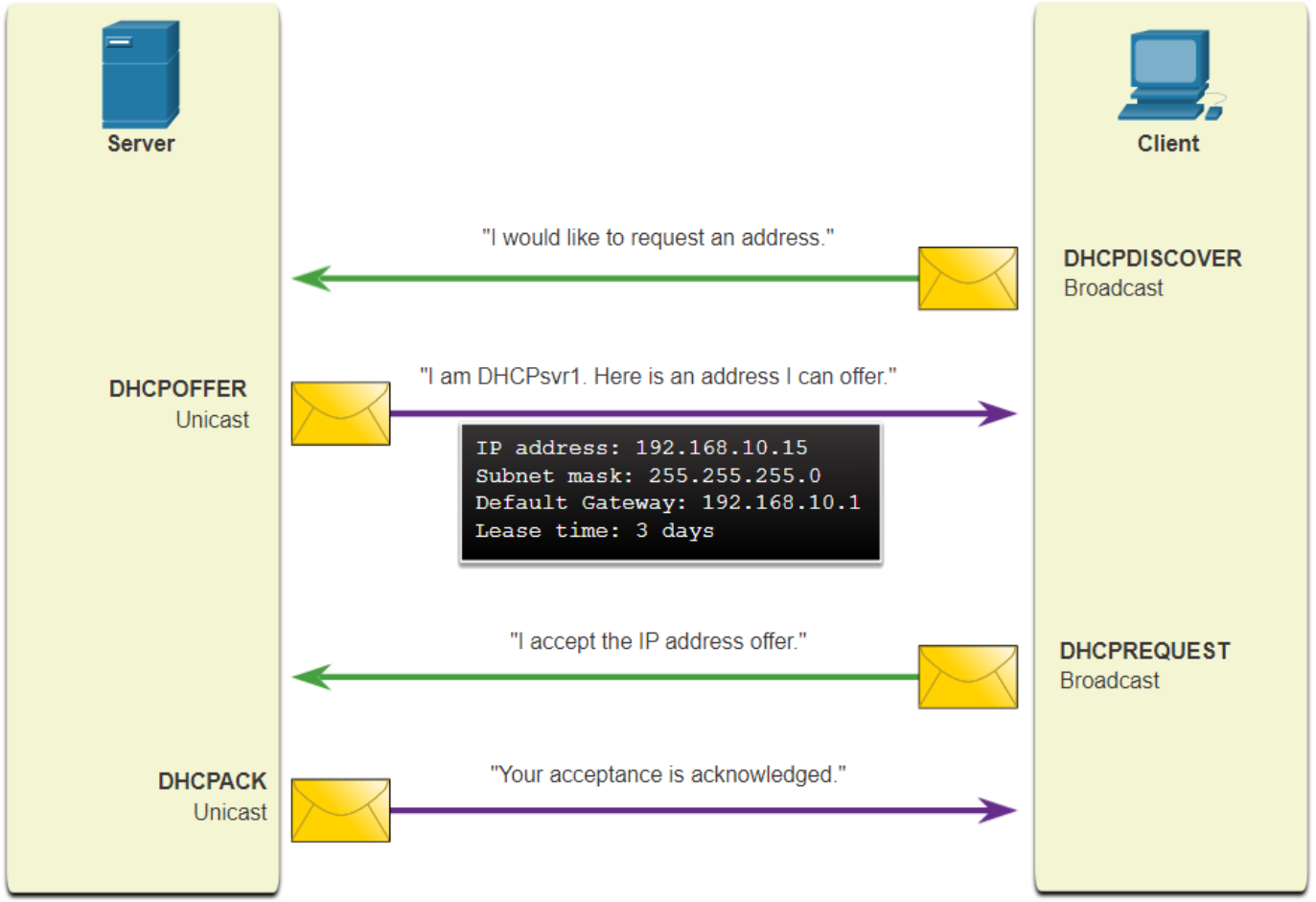
1. Отключить транкинг на всех портах доступа.

2. Принудительно задать режим транка.

3. Убедитесь, что native VLAN используется только для магистральных каналов.

10.5.2 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.



10.5.3 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 истощением 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 Discover 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:

1. 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.

2. Неправильный DNS-сервер. Хакер предоставляет неправильный адрес DNS-сервера, направляя пользователя на вредоносный веб-сайт.

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

10.5.4 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 не запрошенные 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.

10.5.5 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.

10.5.6 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. BPDU Guard обсуждается более подробно позже в курсе.

10.5.7 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, 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 не доверенным устройствам.

10.5.7 РАЗВЕДЫВАТЕЛЬНЫЕ АТАКИ НА CDP

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, введите команду **no lldp run**. Чтобы отключить протокол LLDP на интерфейсе, введите команды **no lldp transmit** и **no lldp receive**.