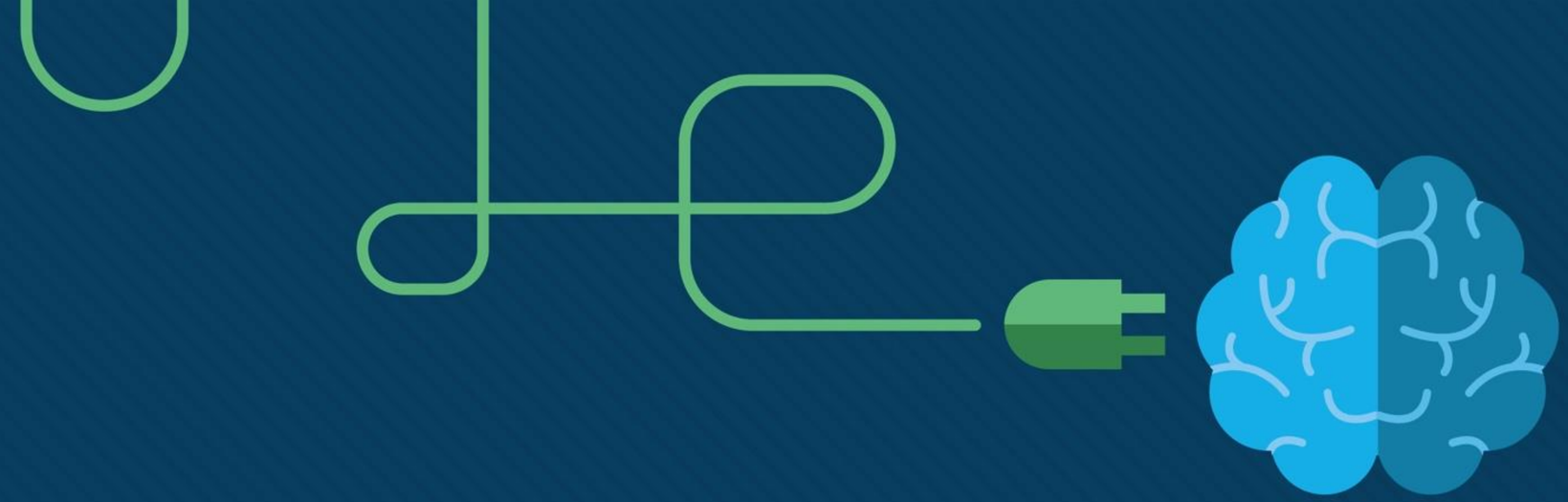


Модуль 10: Принципы обеспечения безопасности сети

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

Module Objectives

Module Title: LAN Security Concepts

Module Objective: Explain how vulnerabilities compromise LAN security

Topic Title	Topic Objective
Endpoint Security	Explain how to use endpoint security to mitigate attacks
Access Control	Explain how AAA and 802.1x are used to authenticate LAN endpoints and devices
Layer 2 Security Threats	Identify Layer 2 vulnerabilities
MAC Address Table Attack	Explain how a MAC address table attack compromised LAN security
LAN Attacks	Explain how LAN attacks compromise LAN security

10.1 Безопасность оконечных устройств

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.

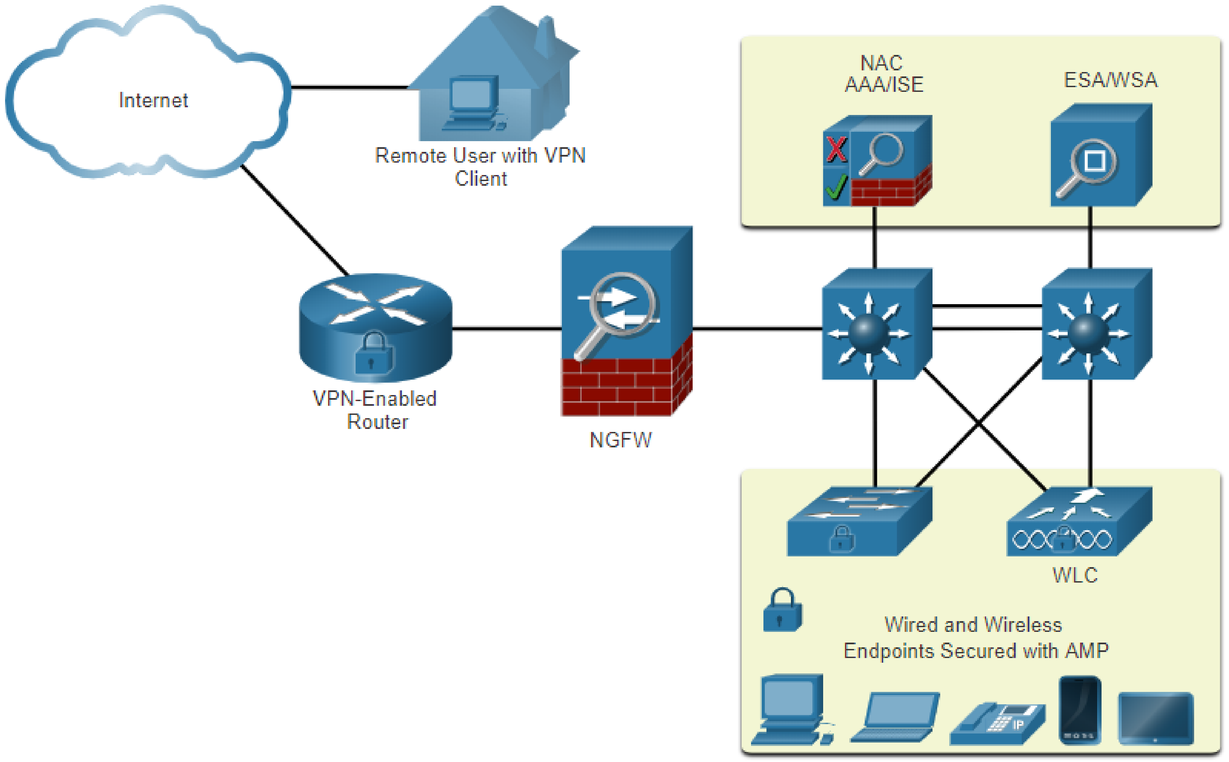
Безопасность сетевых устройств

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

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

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/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).



Cisco Email Security Appliance

The Cisco ESA device is designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos, which detects and correlates threats and solutions by using a worldwide database monitoring system. This threat intelligence data is pulled by the Cisco ESA every three to five minutes.

These are some of the functions of the Cisco ESA:

- Block known threats
- Remediate against stealth malware that evaded initial detection
- Discard emails with bad links
- Block access to newly infected sites.
- Encrypt content in outgoing email to prevent data loss.

Cisco Web Security Appliance

- The Cisco Web Security Appliance (WSA) is a mitigation technology for web-based threats. It helps organizations address the challenges of securing and controlling web traffic.
- The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.
- Cisco WSA provides complete control over how users access the internet. Certain features and applications, such as chat, messaging, video and audio, can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization's requirements.
- The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.

10.2 Управление доступом

Аутентификация с локальным паролем

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

Самый простой способ аутентификации удаленного доступа – это настройка комбинации логина и пароля на консоли, линиях vty и вспомогательных портах, как показано в строках 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.

```
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
```

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.

Управление доступом
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).

Управление доступом
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.

Управление доступом
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.

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 используются в сочетании с аутентификацией AAA.

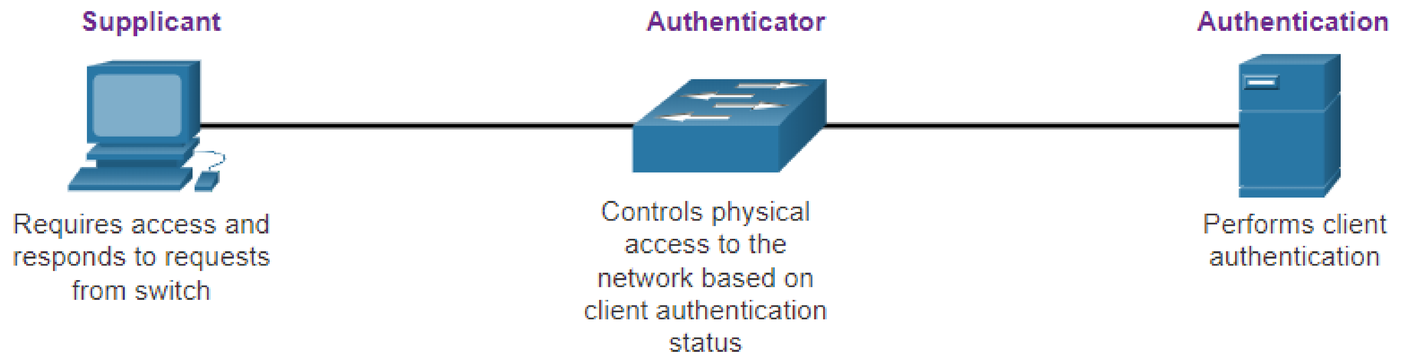
- Серверы AAA ведут журналы с подробной информацией о том, какие действия прошедший аутентификацию пользователь выполнял на данном устройстве, как показано на рисунке. Сюда входят все команды EXEC и команды настройки конфигурации, поданные пользователем.
- Журнал содержит множество полей данных, включая 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.

Управление доступом
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 LAN.

При использовании аутентификации 802.1X на уровне портов устройства в сети могут иметь следующие роли:

- **Запрашиваемое 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.

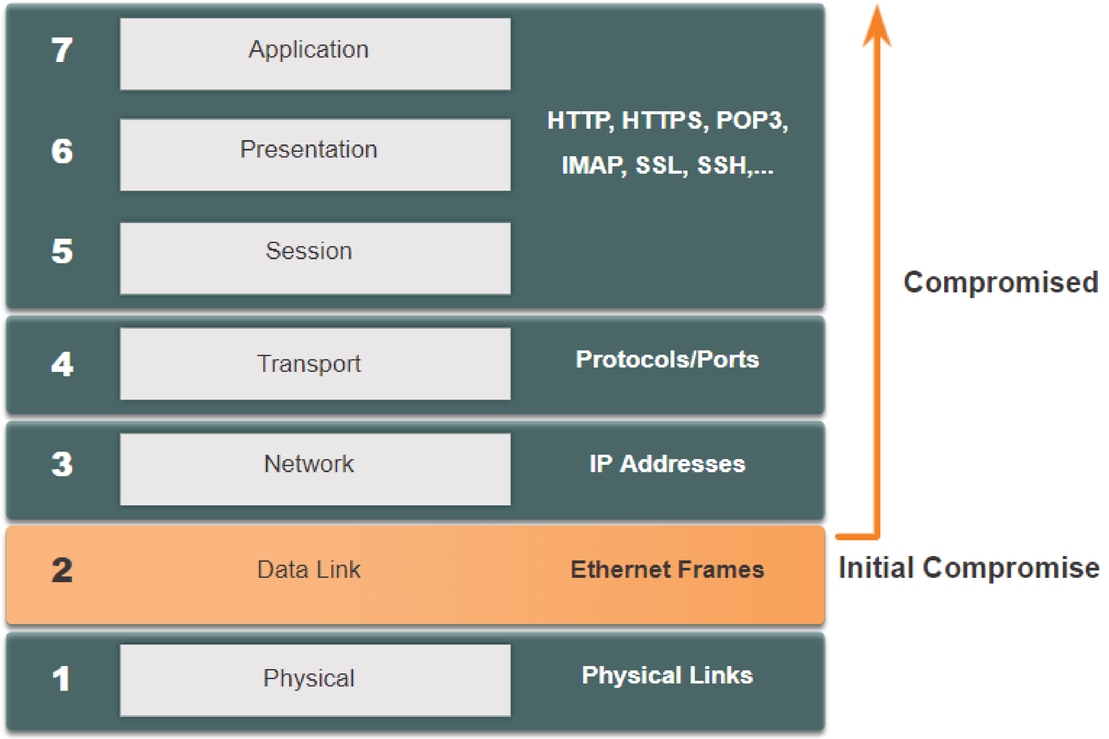


10.3 Угрозы безопасности на уровне 2

Layer 2 Vulnerabilities

Recall that the OSI reference model is divided into seven layers which work independently of each other. The figure shows the function of each layer and the core elements that can be exploited.

Network administrators routinely implement security solutions to protect the elements in Layer 3 up through Layer 7. They use VPNs, firewalls, and IPS devices to protect these elements. However, if Layer 2 is compromised, then all the layers above it are also affected. For example, if a threat actor with access to the internal network captured Layer 2 frames, then all the security implemented on the layers above would be useless. The threat actor could cause a lot of damage on the Layer 2 LAN networking infrastructure.



Угрозы безопасности на уровне 2

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. 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
Атаки на таблицу MAC	Включает в себя атаки с переполнением таблицы MAC.
Атаки на сети VLAN	Включает в себя атаки с переходам по VLAN и с двойным тегированием VLAN. Сюда также входят 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 подменной адреса	Включает атаки подмены MAC и IP адресов.
Атаки STP	Включает в себя атаки путем манипуляции протокола STP.

Угрозы безопасности на уровне 2

Технологии нейтрализации атак на коммутацию

Решение	Описание
Безопасность портов	Предотвращает многие типы атак, включая атаки с переполнением MAC таблицы MAC-адресами и истощением ресурсов DHCP.
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 Secure Socket Layer / Transport Layer Security (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.

10.4 Атаки на таблицу MAC-адресов

MAC Address Table Attack

Switch Operation Review

Recall that to make forwarding decisions, a Layer 2 LAN switch builds a table based on the source MAC addresses in received frames. This is called a MAC address table. MAC address tables are stored in memory and are used to more efficiently switch frames.

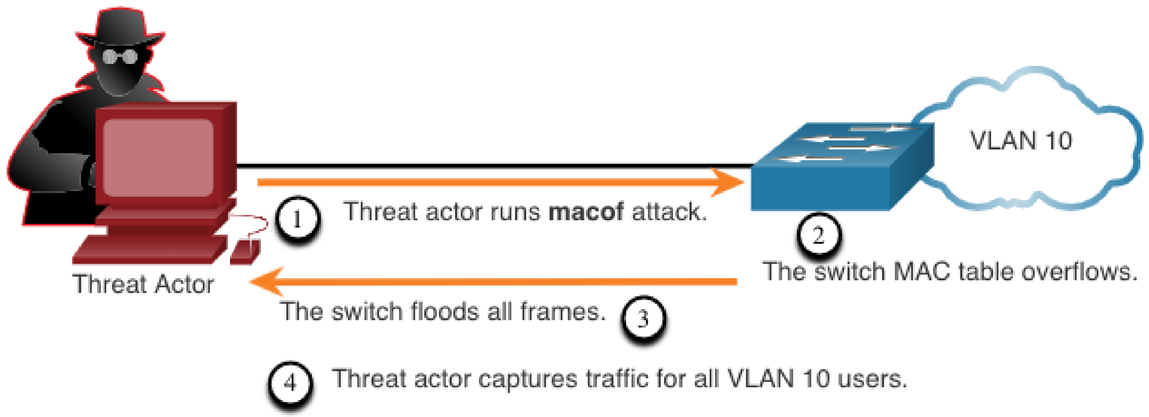
```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    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 эти ограничения, 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 захватить трафик только в локальной сети или VLAN, к которой подключен исполнитель угрозы.



MAC Address Table Attack Mitigation

What makes tools such as **macof** so dangerous is that an attacker can create a MAC table overflow attack very quickly. For instance, a Catalyst 6500 switch can store 132,000 MAC addresses in its MAC address table. A tool such as **macof** can flood a switch with up to 8,000 bogus frames per second; creating a MAC address table overflow attack in a matter of a few seconds.

Another reason why these attack tools are dangerous is because they not only affect the local switch, they can also affect other connected Layer 2 switches. When the MAC address table of a switch is full, it starts flooding out all ports including those connected to other Layer 2 switches.

To mitigate MAC address table overflow attacks, network administrators must implement port security. Port security will only allow a specified number of source MAC addresses to be learned on the port. Port security is further discussed in another module.

10.5 Атаки на локальную сеть

Video – VLAN and DHCP Attacks

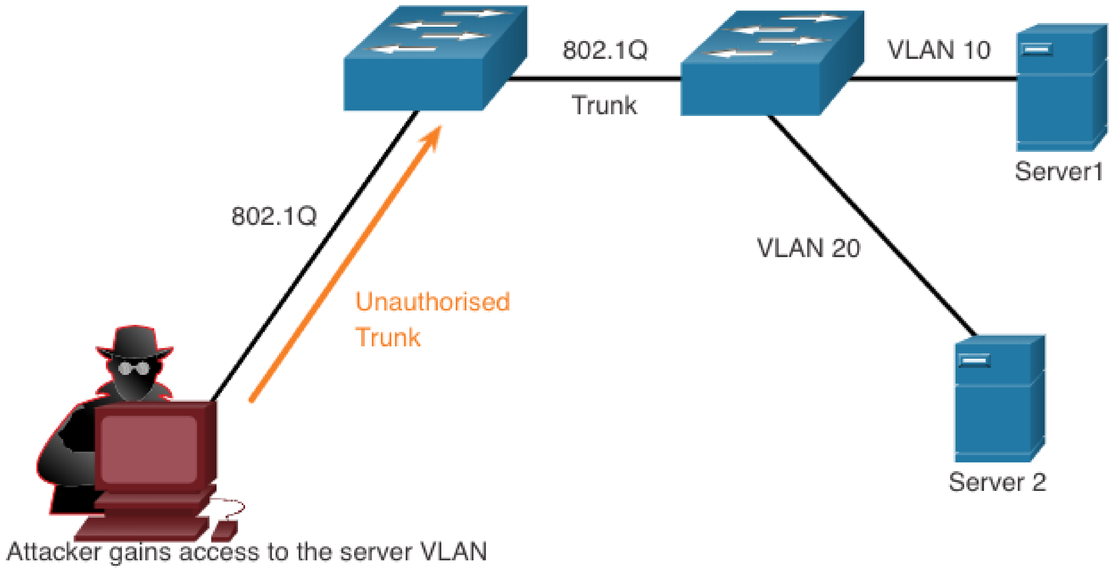
This video will cover the following:

- VLAN Hopping Attack
- VLAN Double-Tagging Attack
- DHCP Starvation Attack
- DHCP Spoofing Attack

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.



Атака VLAN Двойного тегирования

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 Двойного тегирования (Продолжение)

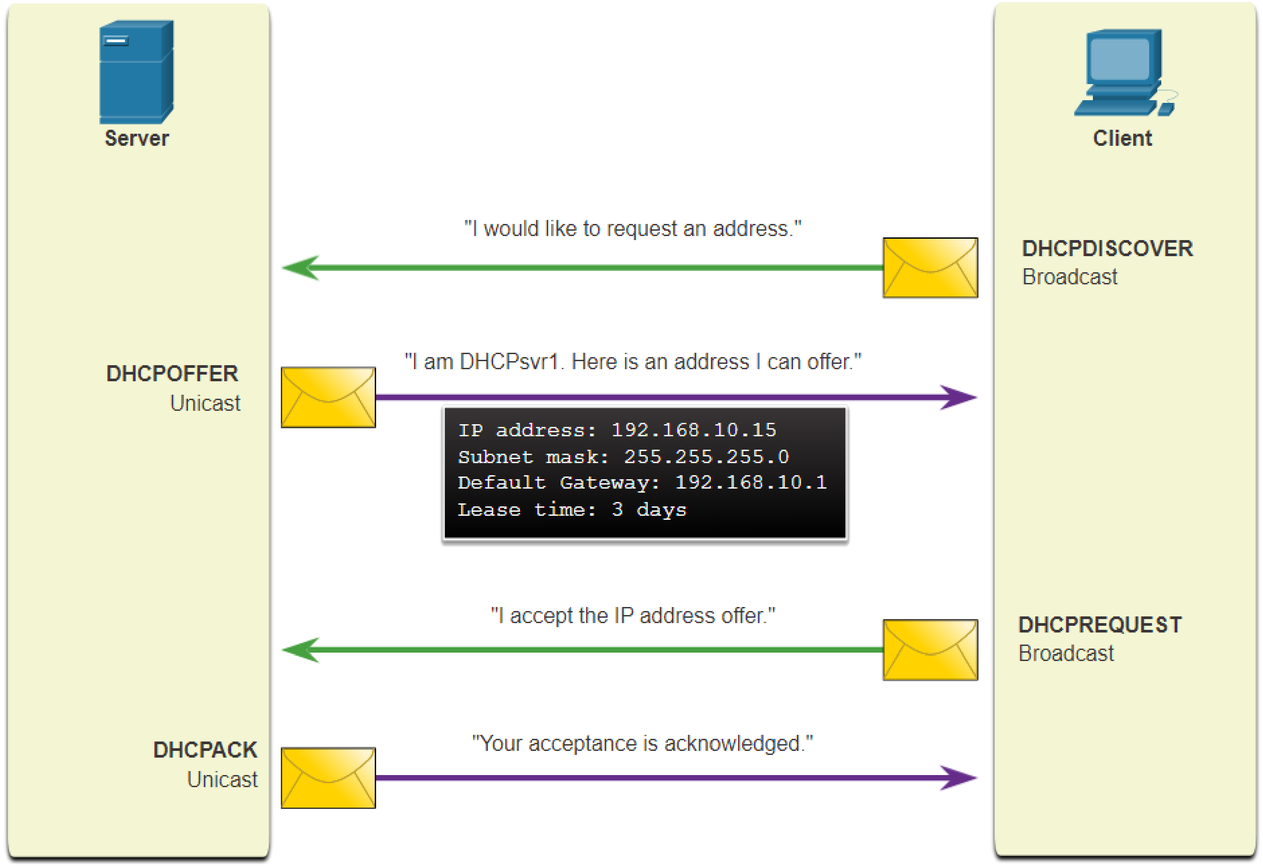
Этот вид атаки является однонаправленным и работает, только если злоумышленник подключен к порту, находящимся в той же VLAN, что и сеть native VLAN транкового порта. Идея состоит в том, что двойное тегирование позволяет злоумышленнику отправлять данные на хосты или серверы VLAN, которые в противном случае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

Защита от атак VLAN двойного тегирования – могут быть предотвращены путем реализации следующих рекомендаций по безопасности магистральных каналов, как обсуждалось в предыдущем модуле:

- Отключить транкинг на всех портах доступа.
- Disable auto trunking on trunk links so that trunks must be manually enabled.
- 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.



DHCP Атаки

Два типа атак DHCP – это истощение DHCP и DHCP спуфинг. Обе атаки нейтрализуются за счет реализации DHCP snooping.

- **Атака истощения DHCP –** Цель этой атаки – привести к отказу в обслуживании (DoS) при подключении 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 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.

Video – ARP Attacks, STP Attacks, and CDP Reconnaissance

This video will cover the following:

- ARP Spoofing Attack
- ARP Poisoning Attack
- STP Attack
- CDP Reconnaissance

ARP Атаки

- Памятуя о том, что хосты передают ARP-запрос в широковещательном режиме другим хостам в сегменте, чтобы определить MAC-адрес хоста с конкретным IP-адресом. Обычно это делается для обнаружения MAC-адреса шлюза по умолчанию. Все хосты в подсети получают и обрабатывают этот ARP-запрос. Хост с IP-адресом, соответствующим ARP-запросу, отправляет ARP-ответ.
- В соответствии с ARP RFC, 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. Таким образом, любой хост может заявить, что он является владельцем любой комбинации IP и MAC-адресов, которую выберет. 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 Advertisement), подобным образом IPv6 предотвращает поддельный ARP-ответ.
- Атаки ARP спуфинга и “отравление” ARP-кэша нейтрализуется путем внедрения Dynamic ARP Inspection (DAI).

Атака с подменной адреса

- IP-адреса и MAC-адреса могут быть подделаны по разным причинам. 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. Затем атакующий хост отправляет по сети кадр с только что заданным MAC-адресом. Когда коммутатор получает кадр, он проверяет MAC-адрес источника. Коммутатор перезаписывает текущую запись в таблице MAC 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 IP Source Guard (IPSG).

STP Атаки

- Сетевые злоумышленники могут манипулировать протоколом связующего дерева (STP) для проведения атак путем подмены 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.
- Для проведения атак путем манипуляции 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.
- STP атака нейтрализуется за счет реализации BPDU Guard на всех портах доступа. BPDU Guard обсуждается более подробно позже в курсе.

Разведывательная атака 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 подключается 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 вклбчить 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** и **no lldp receive**.

10.6 Module Practice and Quiz

What Did I Learn In This Module?

- Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing, such as DDOS, date breaches, and malware. These endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs). Endpoints are best protected by a combination of NAC, host-based AMP software, an email security appliance (ESA), and a web security appliance (WSA).
- AAA controls who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).
- The IEEE 802.1X standard is a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports.
- If Layer 2 is compromised, then all layers above it are also affected. The first step in mitigating attacks on the Layer 2 infrastructure is to understand the underlying operation of Layer 2 and the Layer 2 solutions: Port Security, DHCP Snooping, DAI, and IPSG. These won’t work unless management protocols are secured.

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

- MAC address flooding attacks bombard the switch with fake source MAC addresses until the switch MAC address table is full.
- A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without the aid of a router.
- A VLAN double-tagging attack is unidirectional and works only when the threat actor is connected to a port residing in the same VLAN as the native VLAN of the trunk port.
- VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines:
  - Disable trunking on all access ports.
  - Disable auto trunking on trunk links so that trunks must be manually enabled.
  - Be sure that the native VLAN is only used for trunk links.
- Two types of DHCP attacks are DHCP starvation and DHCP spoofing. Both attacks are mitigated by implementing DHCP snooping.

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

- ARP Attack: A threat actor sends a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch updates its MAC table accordingly. Now the threat actor sends unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway. ARP spoofing and ARP poisoning are mitigated by implementing DAI.
- Address Spoofing Attack: IP address spoofing is when a threat actor hijacks a valid IP address of another device on the subnet or uses a random IP address. MAC address spoofing attacks occur when the threat actors alter the MAC address of their host to match another known MAC address of a target host. IP and MAC address spoofing can be mitigated by implementing IPSG.
- STP Attack: Threat actors manipulate STP to conduct an attack by spoofing the root bridge and changing the topology of a network. Threat actors make their hosts appear as root bridges; therefore, capturing all traffic for the immediate switched domain. This STP attack is mitigated by implementing BPDU Guard on all access ports.
- CDP Reconnaissance: CDP information is sent out CDP-enabled ports in periodic, unencrypted broadcasts. CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN. The device receiving the CDP message updates its CDP database. the information provided by CDP can also be used by a threat actor to discover network infrastructure vulnerabilities. To mitigate the exploitation of CDP, limit the use of CDP on devices or ports.


CISCO