Режим принудительного переопределения Out-of-Band

Введение

Назначение VLAN может быть осуществлено с помощью нескольких различных методик. Эти методики совместимы друг с другом, но не могут быть применены на одном порту коммутатора. Это означает, что для новейших коммутаторов можно использовать более безопасную и современную методику, а для старых коммутаторов, не поддерживающих новейшие методики — другую.
Как следует из названия, в данном режиме AxelNAC является сервером, который назначает устройству VLAN. Эта VLAN может быть одной из VLAN компании или специальной VLAN, в которой AxelNAC перенаправляет пользователей на Captive-портал для аутентификации или обновления регистрации.

Назначение VLAN позволяет изолировать хосты на уровне OSI Layer 2. Это означает, что такой метод является самым сложным для обхода и лучше всего адаптируется к среде, поскольку он вписывается в используемую методологию назначения VLAN.

Методы назначения VLAN

Существует множество различных методов назначения VLAN. Рассмотрим основные из них.

Проводное подключение: 802.1X + MAC-аутентификация

Стандарт 802.1X обеспечивает аутентификацию на основе портов, которая предполагает обмен данными между супликантом, аутентификатором (NAS) и сервером аутентификации (AAA). Супликантом часто является программное обеспечение клиентского устройства, например ноутбука, аутентификатором — проводной Ethernet-коммутатор или беспроводная точка доступа, а сервером аутентификации, как правило, является сервер RADIUS.

Супликанту (т.е. клиентскому устройству) не разрешается доступ к сети через аутентификатор до тех пор, пока его личность не будет подтверждена. При аутентификации по стандарту 802.1X клиент предоставляет аутентификатору учетные данные, такие как имя пользователя/пароль или цифровой сертификат (ключ), а аутентификатор направляет их на сервер аутентификации для проверки. Если учетные данные действительны (находятся в базе данных сервера аутентификации), то супликанту (клиентскому устройству) разрешается доступ к сети.

Протокол аутентификации EAP (Extensible Authentication Protocol) имеет множество видов. И супликант, и сервер аутентификации должны использовать один и тот же вид протокола EAP. Наиболее популярным вариантом EAP является PEAP-MSCHAPv2 (поддерживается Windows/Mac OSX/Linux для аутентификации с использованием Active Directory).

В нашем примере AxelNAC является сервером аутентификации и возвращает коммутатору соответствующую VLAN, в который должен быть помещено конечное устройство.

MAC-аутентификация — это еще один механизм, использующийся в коммутаторах для работы в случаях, когда клиентское устройство не поддерживает стандарт 802.1x. Разные производители называют его по-разному. Cisco называет его MAC Authentication Bypass (MAB), Juniper — MAC RADIUS, Extreme Networks — Netlogin и т.п.

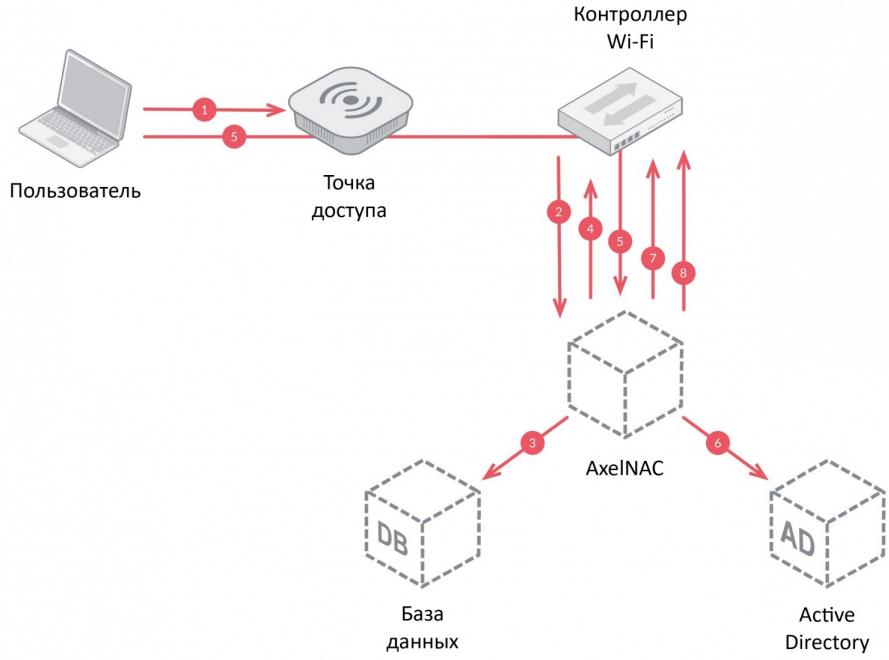
По истечении таймаута коммутатор прекращает попытки выполнить 802.1X и переходит к MAC-аутентификации. Ее преимущество заключается в том, что она использует тот же подход, что и стандарт 802.1X, за исключением того, что вместо имени пользователя отправляется MAC-адрес и не происходит сквозного EAP-обмена (нет строгой аутентификации). При использовании MAC-аутентификации такие устройства, как сетевой принтер или IP-телефон, не поддерживающие стандарт 802.1X, могут получить доступ к сети и нужной VLAN.

Беспроводное подключение: 802.1X + MAC-аутентификация

Аутентификация по стандарту 802.1X и MAC аутентификация с беспроводным подключением работают практически так же, как и при проводном подключении. Отличие заключается в том, что в стандарте 802.1X при настройке ключей безопасности используется шифрование WPA2-Enterprise, а MAC-аутентификация применяется только для авторизации (разрешения или запрета) MAC-адреса в беспроводной сети.

В беспроводных сетях обычная настройка AxelNAC предполагает конфигурирование двух SSID: открытого и защищенного. Открытый используется для того, чтобы помочь пользователям правильно настроить защищенный и требует аутентификации через Captive-портал (который работает в HTTPS).

На схеме ниже показан процесс взаимодействия мобильного клиентского устройства, точки доступа Wi-Fi, контроллера Wi-Fi и AxelNAC:



Алгоритм взаимодействия следующий:

1. Пользователь инициирует подключение к точке доступа Wi-Fi и передает MAC-адрес. Если пользователь получает доступ к сети через зарегистрированное в AxelNAC устройство, перейдите к шагу 8.
2. Контроллер Wi-Fi передает MAC-адрес по протоколу RADIUS на сервер AxelNAC для аутентификации/авторизации этого MAC-адреса на точке доступа.
3. Сервер AxelNAC проводит аудит адресов в своей базе данных. Если он не распознает MAC-адрес, перейдите к шагу 4. Если распознает, перейдите к шагу 8.
4. Сервер AxelNAC направляет контроллеру Wi-Fi через RADIUS (атрибуты RFC2868) запрос на перевод устройства в «неаутентифицированную роль» (набор ACL, который ограничивает/перенаправляет пользователя на портал захвата AxelNAC для регистрации. Или же можно также использовать регистрационную VLAN, в которой AxelNAC выполняет перенаправление трафика (blackholing) DNS и является DHCP сервером).
5. Устройство пользователя отправляет DHCP/DNS-запрос на AxelNAC (на DHCP/DNS-сервер в этой VLAN или для этой роли), которая пересылает IP- и DNS-информацию. В этот момент ACL ограничивают/перенаправляют пользователя на портал захвата AxelNAC для аутентификации. AxelNAC фиксирует устройство (атрибуты пользовательского агента, информацию DHCP и шаблоны MAC-адресов), по отношению к которому может предпринять различные действия, включая: сохранение устройства на Captive-портале, перенаправление на альтернативный портал, авторегистрацию устройства, автоблокировку устройства и др. Если устройство остается на портале регистрации, пользователь регистрируется и указывает имя пользователя/пароль, номер мобильного телефона и др. В это время AxelNAC также может потребовать от устройства пройти оценку состояния (с помощью WinRM, Nessus, OpenVAS и др.).
6. Если требуется аутентификация (имя пользователя/пароль) через форму входа, то эти данные проверяются через сервер Active Directory (или любые другие источники аутентификации — LDAP, SQL, RADIUS, SMS и др.), который предоставляет атрибуты пользователя в AxelNAC, создающую в своей базе данных профиль политики «пользователь + устройство».
7. AxelNAC изменяет авторизацию (RFC3576) на контроллере, а пользователь должен быть повторно аутентифицирован/авторизован, поэтому происходит возврат к шагу 1.
8. Сервер AxelNAC направляет контроллеру Wi-Fi через RADIUS указание поместить устройство в «аутентифицированную роль» или в «обычную» VLAN.

Режим веб-аутентификации

Веб-аутентификация — это метод аутентификации на сетевых устройствах, который перенаправляет HTTP-трафик устройства на Captive-портал. В этом режиме устройство никогда не изменит идентификатор VLAN, а изменится только ACL, связанный с устройством. Примеры конфигурации веб-аутентификации приведены в приложениях к лабораторным работам.

Port-Security и SNMP

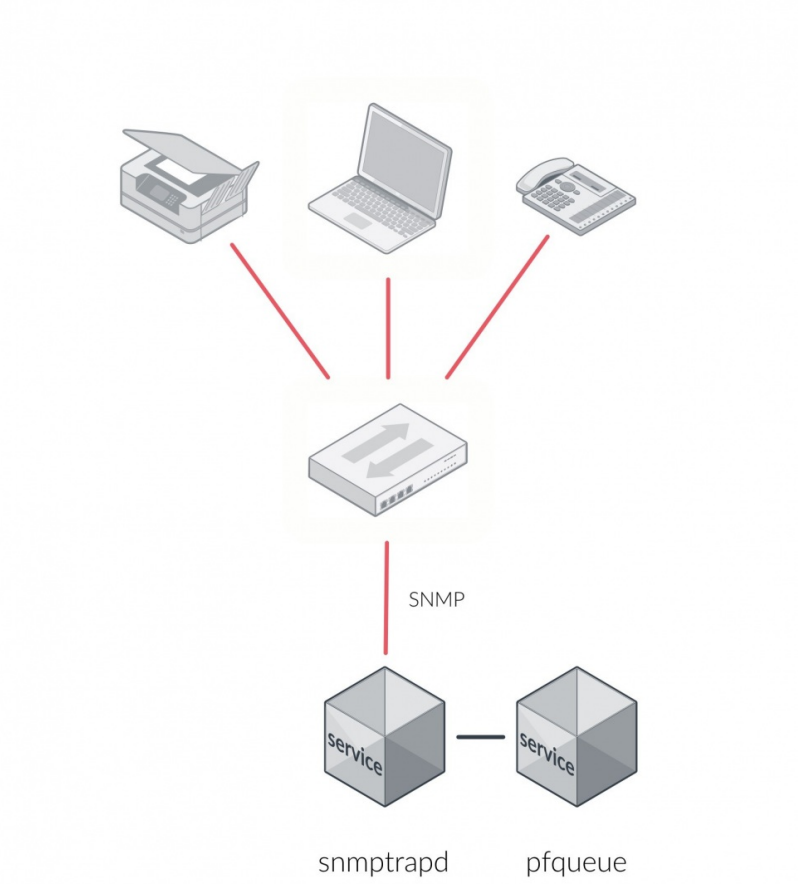
В этом методе используются Port-Security SNMP-trap. Всем портам назначается поддельный статический MAC-адрес, таким образом, любой MAC-адрес будет генерировать нарушение безопасности и trap будет отправлен в AxelNAC. Система авторизует MAC-адрес и помещает порт в нужную VLAN. Поддержка VoIP возможна, но сложна. Она сильно зависит от производителя коммутатора. Например, коммутаторы Cisco поддерживаются успешно, но изоляция ПК за IP-телефоном приводит к необходимости выбора: либо приходится закрыть порт (и телефон одновременно), либо изменить VLAN передачи данных, но ПК не выполняет протокол DHCP (так как не смог обнаружить, что связь прервана), поэтому не может попасть на Captive-портал. За исключением проблемы с изоляцией VoIP именно эта технология доказала свою надежность и имеет наибольшую поддержку со стороны производителей коммутаторов.

Дополнительная информация об SNMP-trap для изоляции VLAN

Когда изоляция VLAN работает через SNMP-trap, все порты коммутатора (на которых должна быть выполнена изоляция VLAN) должны быть настроены на отправку SNMP-trap на хост AxelNAC. На AxelNAC в качестве приемника SNMP-trap используется служба **snmptrapd**. Получая trap, она переформатирует их и отправляет в очередь redis, которая управляется службой **pfqueue**.

Служба **pfqueue** считывает эти trap из очереди redis и принимает решение в зависимости от типа trap. Например, она может ответить на них, настроив порт коммутатора на нужный VLAN. В настоящее время поддерживаются коммутаторы Cisco, Edge-Core, HP, Intel, Linksys и Nortel.

В зависимости от возможностей имеющихся коммутаторов **pfqueue** будет реагировать на различные типы SNMP-trap. Необходимо создать регистрационную VLAN (с DHCP-сервером, но без маршрутизации в другие VLAN), в которую AxelNAC будет помещать незарегистрированные устройства. Если нужно выделить компьютеры с открытым событием безопасности в отдельную VLAN, необходимо также создать изолирующую VLAN.



Изменение ссылок (устаревший метод)

Когда к порту коммутатора подключается хост, коммутатор посылает в AxelNAC trap **linkUp**. Поскольку коммутатору требуется некоторое время, чтобы узнать MAC-адрес вновь подключенного устройства, AxelNAC немедленно помещает порт в регистрационную VLAN, в которую устройство будет посылать DHCP-запросы, чтобы коммутатор узнал его MAC-адрес.

Затем **pfqueue** будет периодически посылать коммутатору SNMP-запросы до тех пор, пока коммутатор не узнает MAC-адрес устройства. Когда MAC-адрес устройства известен, **pfqueue** проверяет его статус (существующее/зарегистрированное/любое событие безопасности) в базе данных и помещает порт в соответствующую VLAN. Когда устройство отключается от сети, коммутатор посылает trap **linkDown** в AxelNAC, который помещает порт в регистрационную VLAN.

При загрузке компьютера инициализация сетевой карты генерирует несколько изменений состояния канала связи. И каждый раз коммутатор посылает в AxelNAC trap **linkUp** и **linkDown**. Поскольку AxelNAC должен реагировать на каждый такой trap, это создает ненужную нагрузку на службу **pfqueue**. Чтобы оптимизировать обработку trap, AxelNAC останавливает каждый поток для trap **linkUp**, когда получает trap **linkDown** на том же порту.

Однако использование только этих trap — не самый масштабируемый вариант. Например, при отключении питания, если сотни компьютеров загружаются одновременно, AxelNAC будет получать большое количество trap практически мгновенно, что может привести к задержкам сетевого соединения.

Trap уведомлений о MAC-адресах (устаревший метод)

Если коммутаторы поддерживают trap уведомлений о MAC-адресах (MAC learned, MAC removed), рекомендуется активировать их в дополнение к trap **linkUp**/**linkDown**.

В этом случае после получения trap **linkUp** службе **pfqueue** не нужно будет постоянно запрашивать коммутатор, пока MAC окончательно не будет изучен. При получении trap **linkUp** для порта, на котором также включены trap уведомлений о MAC-адресах, ему достаточно поместить порт в регистрационную VLAN, после чего процесс может быть завершен.

Когда коммутатор изучит MAC-адрес устройства, он отправляет trap MAC learned (содержащий MAC-адрес) в AxelNAC.

SNMP-Trap для работы Port-Security

В самом базовом виде функция Port-Security запоминает MAC-адрес, подключенный к порту коммутатора, и разрешает взаимодействие на этом порту только этому MAC-адресу. Если через порт попытается установить связь любой другой MAC-адрес, функция Port-Security не разрешит этого и пошлет trap **portsecurity**.

Если коммутаторы поддерживают эту функцию, настоятельно рекомендуется использовать ее вместо **linkUp**/**linkDown** и/или trap уведомлений о MAC-адресах. Это связано с тем, что до тех пор, пока MAC-адрес авторизован на порту и является единственным подключенным, коммутатор не будет посылать trap независимо от того, перезагружается ли устройство, подключается или отключается. Это значительно сокращает количество SNMP-взаимодействий между коммутаторами и AxelNAC.

При включении trap **Port-Security** не следует включать trap **linkUp**/**linkDown** и trap уведомлений о MAC-адресах.

ID статьи: 562
Последнее обновление: 10 июл., 2024
Обновлено от: Егоров В.
Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Поддерживаемые режимы принудительного переопределения -> Режим принудительного переопределения Out-of-Band
https://docs.axel.pro/entry/562/