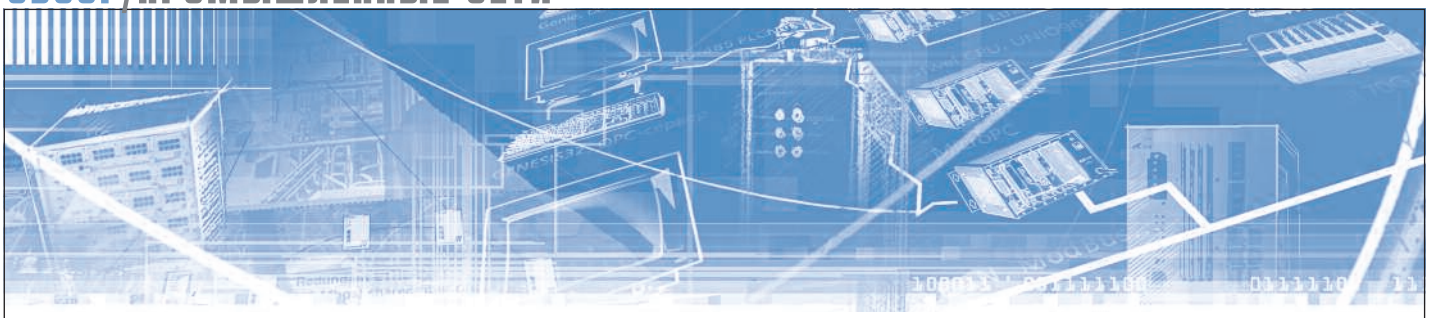


Сергей Воробьёв

“Defense in Depth” в действии. Уровень 2: защита канального уровня

Статья продолжает цикл публикаций, посвящённых многоуровневой защите промышленных Ethernet-сетей на базе принципа “Defense in Depth”. В статье рассмотрены киберугрозы канального уровня, а также возможные методы организации защиты.

Введение

Принцип построения “Defense in Depth” является многоуровневым механизмом обеспечения защиты промышленной Ethernet-сети [1]. Каждый этап подразумевает различные типы анализа и защиты. Например, защита периметра промышленной сети – это в первую очередь защита от внешних угроз. Она реализуется при помощи промышленного IP-брандмауэра, работающего на уровне L3 модели OSI [1, 2]. Однако угрозы, связанные с безопасностью промышленной сети, могут как возникать из внешней сети, так и исходить из внутренней, в которой находятся устройства, функционирующие исключительно на уровне L2 модели OSI. А ведь на уровне L2 свои правила, устройства здесь оперируют исключительно фреймами. И если не знать и не контролировать того, что происходит на уровне L2, то даже некорректная работа собственного внутреннего оборудования или программного обеспечения может привести к проблемам и сбоям. Например, неконтролируемая широковещательная рассылка (broadcast) может заполонить и перегрузить сегмент сети, атаки типа VLAN hopping могут привести к несанкционированному доступу к различным узлам, а MAC flooding может превратить управляемый коммутатор в обычный узел (hub). При этом IP-брандмауэр, который функционирует на уровне L3 и работает исключительно с IP-адресами, будет функционировать в штатном режиме и никак не просигнализирует о наличии угрозы.

Для решения данной проблемы и нейтрализации угроз канального уровня необходимо использовать устройство, которое функционирует на уровне L2 модели OSI и позволяет анализировать трафик. Таким устройством может стать брандмауэр уровня L2 [1] либо коммутатор с расширенными политиками безопасности. Правильная настройка коммутаторов может защитить сеть от множества угроз. Далее рассмотрим возможные угрозы канального уровня и механизмы защиты на базе промышленного коммутатора серии RSP35 от Hirschmann с установленной операционной системой HiOS (рис. 1).

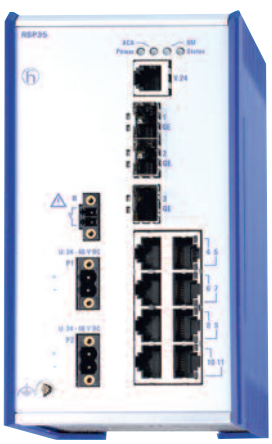


Рис. 1. Промышленный коммутатор Hirschmann RSP35

Угрозы канального уровня: что защищаем?

Канальный уровень (Data Link Layer) является вторым по счёту, как в модели OSI, так и в модели TCP/IP. Передача данных осуществляется при помощи фреймов размером от 64 до 1518 байт. Существуют также вариации меньше 64 (Runts) и больше 1518 (Jumbo). Адресация осуществляется на основе MAC-адресов, а в качестве основного инструмента, позволяющего собрать информацию о подключённых устройствах, выступает протокол ARP (Address Resolution Protocol – протокол определения адреса). С первого взгляда, всё просто: установили коммутаторы, произвели их первоначальную настройку, сеть в итоге работает, а безопасность перекладывается на более высокие уровни, где уже задействованы мощные L3-брандмауэры. При этом многие администраторы просто не уделяют должного внимания тем процессам, которые происходят именно на втором, канальном уровне. В рамках промышленной сети это может негативно отразиться на работе технологических процессов, ведь основное количество устройств функционирует именно на втором уровне. А там всё не так просто, в первую очередь это связано с тем, что многие протоколы второго уровня, например ARP и STP, разрабатывались без какой-либо привязки к безопасности. Например, при базовой конфигурации коммутатора не требуется никакой

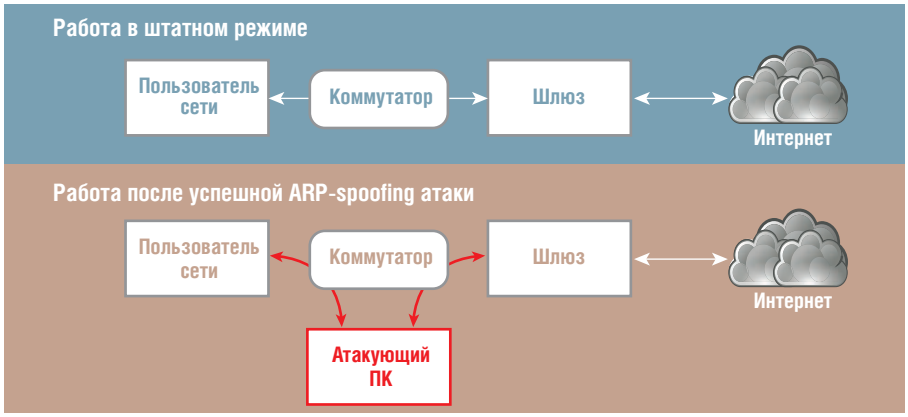


Рис. 2. Пример ARP-spoofing атаки

дополнительной информации, чтобы при помощи ARP-запроса узнать MAC-адрес хоста по известному IP-адресу. В итоге ответ на вопрос в заголовке сводится к тому, что в первую очередь необходимо защитить используемые L2-протоколы путём правильной настройки коммутаторов. Современные промышленные коммутаторы имеют в своём арсенале достаточно инструментария для защиты именно второго, канального уровня.

Но для правильной конфигурации необходимо также понимать логику работы атакующих ПК и технологию потенциальных угроз, разберём самые популярные из них.

ARP- и MAC-spoofing, или Угроза мирному протоколу

Как было упомянуто, ARP-протокол используется для того, чтобы понять, на какой физический MAC-адрес слать фрейм, при условии известного IP-адреса получателя. Работу протокола можно описать следующими действиями.

Сетевое устройство посылает запросы ARP, в которых содержится вопрос: «IP-адрес x.x.x.x – это вы? Да? Прекрасно! Присылайте тогда мне ваш MAC-адрес» [3]. Пакеты рассылаются на все узлы в сегменте сети, и каждый исследует ARP-запрос и отсылает ответ в случае совпадения. Данный принцип работы является уязвимым, а атаки, которые это используют, имеют общее название *spoofing*, которое можно дословно перевести как подмена. Они сводятся к подмене настоящего MAC-адреса устройства адресом злоумышленника. При правильно реализованной атаке это приводит к захвату фреймов и перехвату информации.

Виды атак

- *MAC-spoofing*. Это атака канального уровня, заключается она в том, что на сетевой карте изменяется MAC-адрес, и это заставляет коммутатор отправлять на порт, к которому подключён злоумышленник, пакеты, которые до этого он видеть не мог.
- *ARP-spoofing*. Цель данной атаки состоит в том, чтобы послать хосту специально подготовленный ответ, в котором IP-адрес будет сопоставлен ложному MAC-адресу. Результатом данной атаки будет то, что пакеты придут не к узлу A (изначальному конечному устройству), а к узлу B. При этом жертва даже не будет знать, что посылает пакеты не по тому адресу. Такой процесс называют часто отравлением ARP-кэша [3], рис. 2.

Как защититься?

Подобные атаки достаточно широко известны, построить против них грамотную защиту можно при помощи настройки политик безопасности (Port Security) каждого конкретного порта коммутатора, то есть закрыть доступ к порту всем чужим устройствам. Реализация может быть различной, начиная от банального отключения неиспользуемых портов, что является важным и обязательным действием, и заканчивая настройкой управления доступом в соответствии с IEEE 802.1x.

При правильной настройке Port Security устройство позволяет передавать данные только от желаемых отправителей. Когда эта функция включена, коммутатор проверяет идентификатор VLAN и MAC-адрес отправителя до принятия решения по передаче пакета данных. В итоге коммутатор отбрасывает пакеты данных от других отправителей и регистрирует это событие. На рис. 3 представлен графический интерфейс конфигурирования политик Port Security коммутатора Hirschmann RSP35. Операционная система HiOS позволяет настроить такие параметры, как количество статических и динамических MAC-адресов на каждый порт, возможность настройки параметров отправки SNMP-трапа при регистрации несанкционированного подключения, а также активация функции Auto Disable, которая позволяет полностью выключить порт при подключении чужого устройства. Правильная настройка Port Security коммутатора делает реализацию атак типа MAC- и ARP-spoofing значительно сложнее. При этом наличие возможности ограничения количества динамических MAC-адресов сводит к минимуму воздействие атаки типа MAC-flooding, цель которой – переполнение CAM-таблицы (Content Addressable Memo) коммутатора (CAM-table overflow).

Другим возможным инструментом настройки Port Security является управление доступом в соответствии с IEEE 802.1x. Это стандарт, который исполь-

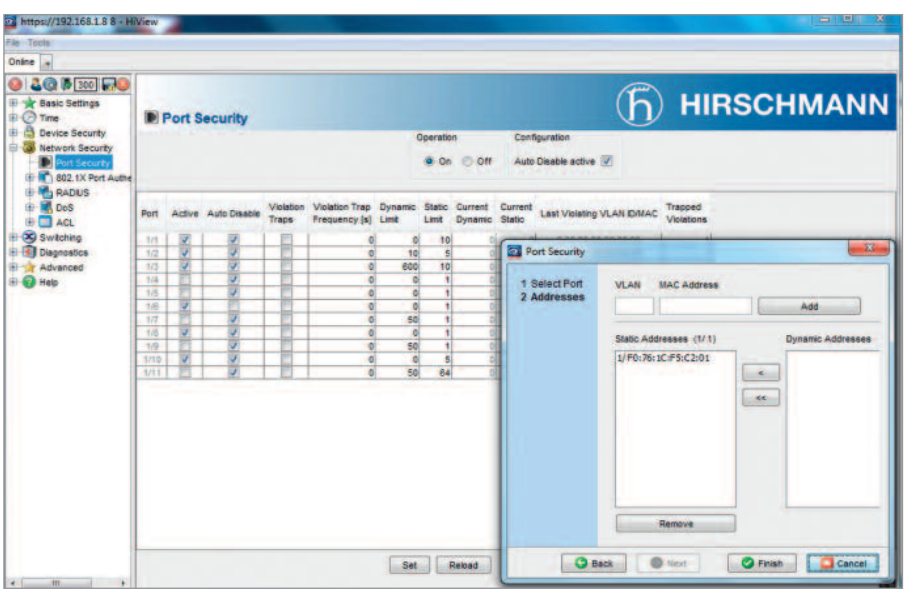


Рис. 3. Пример настройки политик Port Security

Рис. 4. Пример атаки типа VLAN hopping/Double tagging attack

зуется для аутентификации и авторизации пользователей и рабочих станций в сети передачи данных [4]. При помощи данного инструмента можно предоставить права доступа к различным блокам и сервисам сети, в нашем случае это определённые порты коммутатора.

Данный способ является более сложным, требующим наличия сервера аутентификации (RADIUS-сервер), аутентификатора (в нашем случае это коммутатор), а также клиентского ПО 802.1x на рабочей станции конечного пользователя. Аутентификатор и конечные устройства взаимодействуют через протокол аутентификации EAPoL (Extensible Authentication Protocol over LANs). При подобной настройке управления доступом к портам контролируется доступ к сети с подключённых конечных устройств.

VLAN – это про безопасность?

Создание сети при помощи VLAN (Virtual Local Area Network), логических (виртуальных) локальных компьютерных сетей, является одним из самых популярных способов разделения сети на сегменты. Существует механизм уровня L2 – IEEE 802.1Q и L3 – IEEE 802.1v. Самый популярный – это механизм второго уровня, на базе портов коммутатора. Он встречается практически в каждой сети. Всё очень просто: порты коммутатора помещаются в разные VLAN, далее при прохождении фрейма через порт в него дописывается специальный тег, который как раз и позволяет определить номер VLAN. Фактически создаются несколько виртуальных коммутаторов внутри одного. В итоге разделили сеть на несколько VLAN, разнесли оконечные устройства по портам, и всё, создаётся иллюзия, что никакая атака не пройдёт. Но, к сожалению, это только иллюзия. Атаки, связанные с VLAN, – это самый популярный тип атак, носят они название VLAN hopping [5], дословно можно перевести как перепрыгивание. Атаки данного типа предполагают получение доступа в VLAN, который изначально был нереализуем для атакующего ПК. Разберём некоторые из них.

Виды атак

- *VLAN-spoofing, или атака на DTP-протокол*. Данная атака работает преимущественно на коммутаторах Cisco [5] и возможна из-за того, что коммутаторы с поддержкой протокола Cisco DTP (Dynamic Trunking Protocol) могут автоматически согласовывать тип порта (access или trunk). Не вдаваясь в подробности данной атаки, можно сказать, что, используя протокол DTP и «недонастроенный» коммутатор, атакующий ПК может получить доступ ко всем VLAN, присутствующим на коммутаторе.
- *Атака при помощи Native VLAN*. Эта атака связана с тем, что коммутатор «из коробки» сконфигурирован так, чтобы обеспечить работу сети. Native VLAN – это достаточно архаичное понятие в стандарте 802.1Q, обозначающее VLAN, к которой коммутатор относит все фреймы, идущие без тега, то есть трафик внутри Native VLAN передаётся нетегированным. Фактически коммутатор, видя, что к нему пришёл нетегированный фрейм, помещает его автоматически в Native VLAN и далее передаёт его в место назначения. Попадая на другой коммутатор, фрейм без тега помещается в его Native VLAN и так далее. Таким образом возможно получить доступ к ряду хостов. По умолчанию Native VLAN – это VLAN 1.
- *Double tagging attack*. Данная атака также связана с уязвимостью многих коммутаторов, которые поддерживают стандарт 802.1Q. Для дальнейшего пояснения воспользуемся популярной терминологией Cisco и назовём порт, к которому подключены оконечные устройства или хосты, – access, а порты коммутатора, которые подключены к другим коммутаторам, – trunk. Механизм данной атаки заключается в том, что на access-порт коммутатора приходит фрейм с двумя тегами, один из которых соответствует Native VLAN данного коммутатора, а другой тег соответствует VLAN, в которую хочет попасть атакующий. И если в trunk-соединение между коммутаторами включена Native VLAN (по умолчанию она, как правило, включена), то коммутатор передаст данный пакет со вторым тегом, отбросив первый [6], рис. 4.

Как защититься?

На самом деле разделение сети при помощи VLAN может быть безопасным, правильно настроенная конфигурация коммутатора в части VLAN, отличная от начальной «из коробки», позволит увеличить безопасность сети и грамотно разделить потоки данных. Сформулируем ряд рекомендаций, которые позволят сделать сеть, в которой присутствуют VLAN, безопаснее.

1. При создании сети с VLAN необходимо поместить все используемые порты коммутатора в различные VLAN, отличные от ID 1.
2. Не использовать Native VLAN вообще.
3. Использовать принудительное тегирование всех фреймов.
4. Помещать порты между коммутаторами в отдельную VLAN.
5. Настроить порты, задействованные для передачи между коммутаторами, на приём только тегированных фреймов.
6. Для управления коммутаторами рекомендуется создать отдельную VLAN.
7. Создать DUMMY VLAN для неиспользуемых портов, либо отключить их, используя механизм Port Security.
8. Отключить протокол DTP для устройств Cisco.

Далее на примере коммутатора Hirschmann RSP35 рассмотрим сам механизм настройки.

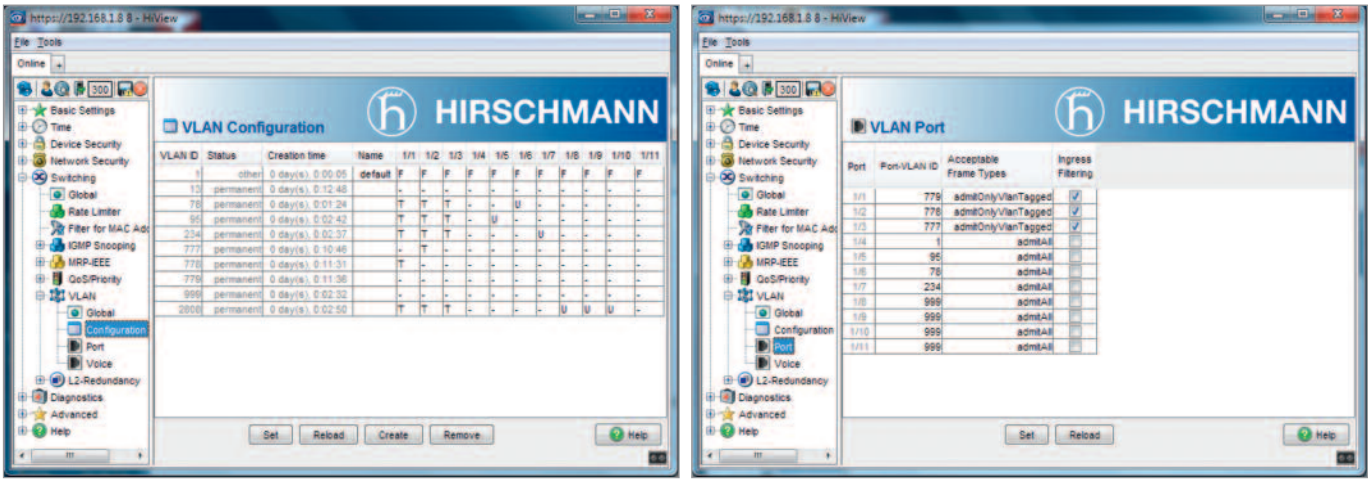
Если абстрагироваться от популярной терминологии Cisco с access- и trunk-портами, то нам необходимо сделать три простых шага:

1. Создать необходимые VLAN.
2. Определить правила для исходящего из порта трафика.
3. Определить правила для входящего в порт трафика.

Визуально это выглядит как заполнение двух табличек (рис. 5). При определении правил для исходящего трафика (рис. 5*а*) необходимо указать по каждому порту действия коммутатора перед отправкой фрейма:

- T – порт находится в данном сегменте VLAN, фреймы посылаются с тегом;
- U – порт находится в данном сегменте VLAN, фреймы посылаются без тега;
- F – порт не находится в данном сегменте VLAN.

Соответственно в зависимости от подключённого к порту устройства нужно



а *б*

Рис. 5. Пример настройки VLAN: *а* – правила для исходящего трафика, *б* – правила для входящего трафика

установить необходимые настройки. Если порт подключён к соседнему коммутатору и нам необходимо передать тегированный трафик, то устанавливаем значение T, если к порту подключён хост, который не умеет работать с VLAN, но пакет должен быть передан, то устанавливаем значение U, и соответственно значение F, если нам передавать трафик данного VLAN в этот порт не нужно.

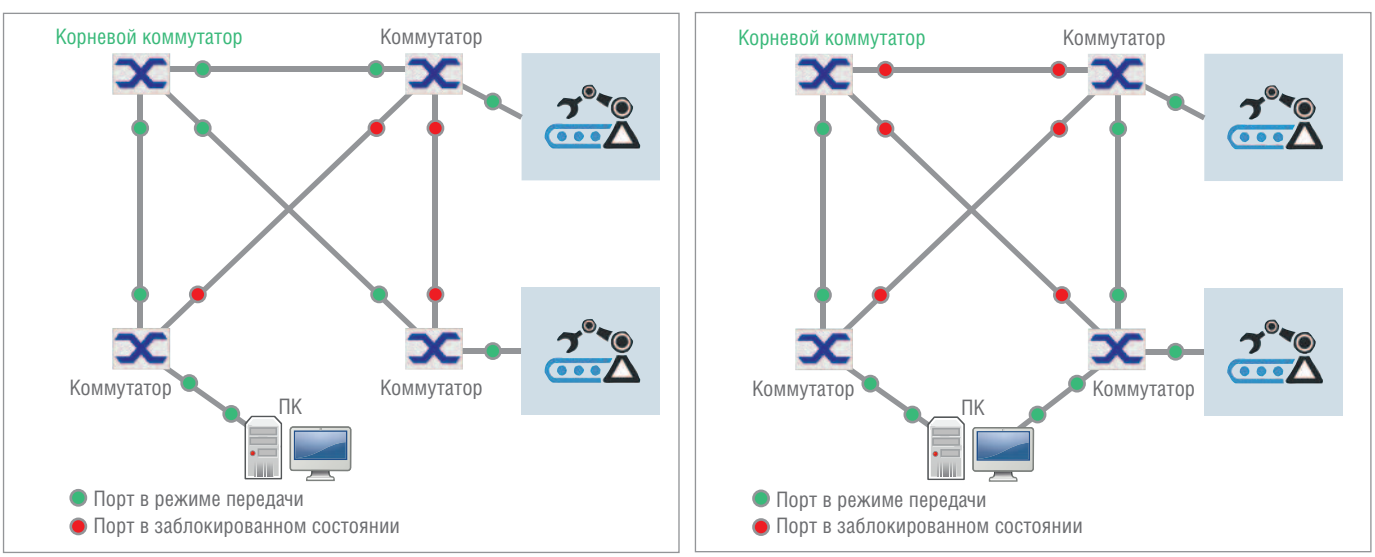
При определении правил для входящего трафика нам необходимо также заполнить простую таблицу, выполнив два действия (рис. 5*б*). Для начала надо поместить порты коммутатора в различные VLAN и далее указать, с каким трафиком будет работать данный порт, с тегом или без тега. Как было описано ранее, если порты соединяют два коммутатора, их необходимо поместить в отдельные VLAN, указав при этом работу исключительно с тегированным трафиком.

При этом такие настройки, как принудительное тегирование всех фреймов, обязательное помещение каждого порта в VLAN, уже присутствуют в коммутаторах Hirschmann изначально, что существенно упрощает процесс настройки. В итоге, правильно настроив VLAN на коммутаторах, можно сделать сеть намного безопаснее.

Резервирование в промышленной сети – необходимость, а как с безопасностью?

Резервированные соединения являются обязательной частью промышленной Ethernet-сети. Сеть должна быть доступна и работоспособна в любой момент времени, иначе может произойти какая-либо нештатная ситуация. Для промышленных сетей, как правило, используются механизмы резервирования, функционирующие на втором, канальном уровне модели OSI. Одни из самых популярных протоколов – это группа xSTP (Spanning Tree Protocol), в которую входят STP, RSTP (Rapid STP) и MSTP (Multiple STP). Основной задачей xSTP является устранение петель в топологии из-за наличия избыточных соединений. Решается эта задача путём выбора корневого пути и блокировки избыточных соединений. В результате работы протокола строится минимальное остовное дерево, которое и будет являться рабочей топологией. Для обмена информацией между собой и формирования структуры дерева коммутаторы используют специальные пакеты, так называемые BPDU (Bridge Protocol Data Units). Конфигурационные пакеты регулярно рассылаются корневым коммутатором на широковещательный адрес, который прослушивают все коммутаторы с включённым xSTP.

В итоге, лишь зная, что в сети используются протоколы xSTP, можно довольно успешно провести на неё атаку и, мало того, перехватить весь трафик сегмента [7].



а *б*

Рис. 6. Пример атаки на xSTP-протокол: *а* – конфигурация сети при штатной работе xSTP-протокола, *б* – конфигурация сети после успешной атаки

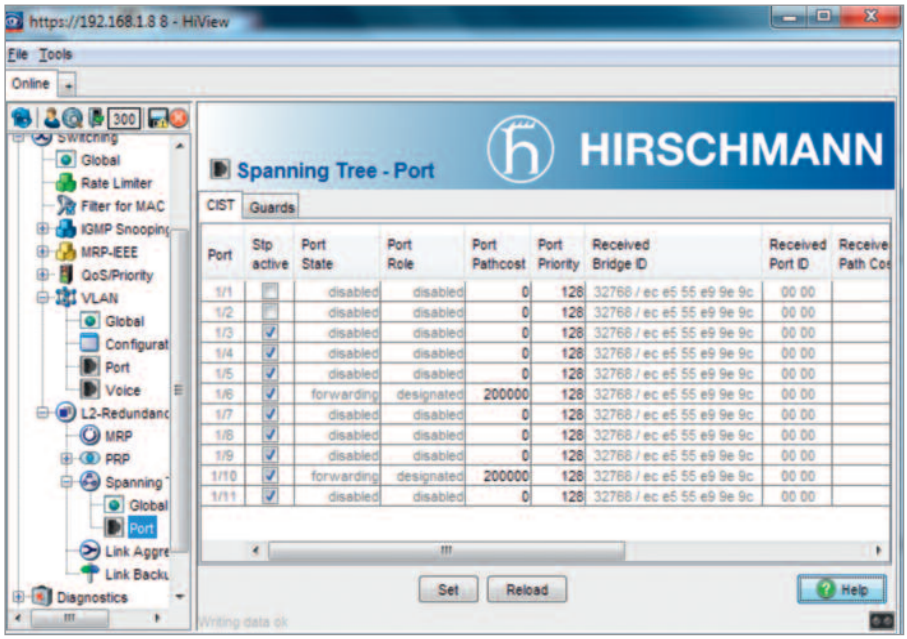


Рис. 7. Пример настройки RSTP, на портах 1 и 2 отключён RSTP-протокол

Атака STP

STP attack. Атака данного типа возможна по той же причине, что и атака на сеть, использующую протокол ARP. Протоколы xSTP никак не защищены. Цель подобной атаки – это разорвать связующие звенья дерева, дестабилизировать CAM-таблицы, а также удерживать сеть в непрерывном состоянии повторного выбора корневого коммутатора. Это можно сделать путём создания ложных BPDU-фреймов несуществующего коммутатора. В итоге можно удерживать сеть в состоянии непрерывного выбора корневого моста, и любой широковещательный трафик станет причиной широковещательного шторма, насыщая сеть фреймами и приводя её в неработоспособное состояние. Другой возможный сценарий – это стать корневым коммутатором, что приведёт к захвату всего трафика сегмента (рис. 6).

Как защититься?

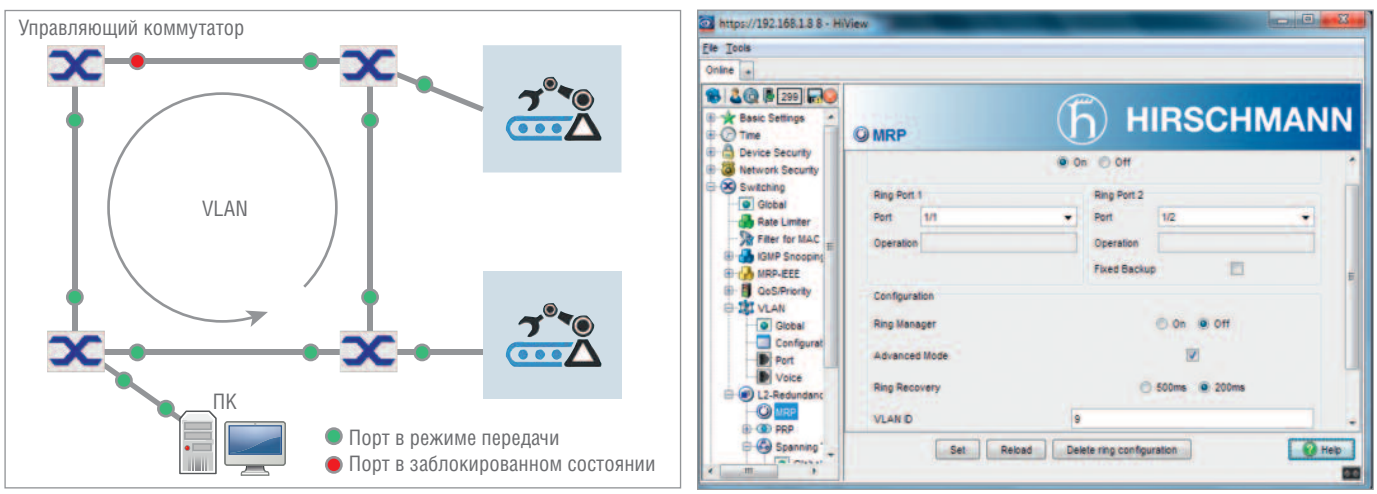
Существует несколько достаточно несложных методов для защиты сети с xSTP-протоколами от атаки. Во-первых, необходимо уйти от первоначальных настроек коммутатора. Коммутатор выходит с фабрики в конфигурации, которая способствует лёгкому внедрению в уже существующую сеть. В нём, как правило, один из xSTP-протоколов по умолчанию включён на всех портах, обычно это RSTP. Так сделано для удобства, но в целях обеспечения безопасности данную конфигурацию необходимо изменить.

Ведь чтобы осуществить STP-атаку, у атакующего ПК должен быть доступ к порту, на котором включён xSTP-протокол для дальнейшей передачи фреймов с ложными BPDU. Следовательно, реализация подобных атак становится намного труднее, если установить запрет на доступ со стороны оконечных устройств и хостов к портам коммутатора, на которых включён xSTP-протокол. Реализуется это путём выключения xSTP на портах, которые не участвуют в построении общей топологии, а также путём настройки Port Security. Пример подобной настройки на базе коммутатора RSP35 изображен на рис. 7. Данные действия значительно усложнят возможность описанной ранее атаки.

Ещё один подход заключается в переходе от xSTP-протоколов к более современным протоколам резервирования. Такими на сегодняшний день являются протоколы кольцевого резервирования, которые обеспечивают быстрое время восстановления (< 200 мс), например, стандартизованный MRP (Media Redundancy Protocol). При использовании данного протокола сама организация связи имеет более высокую защиту. Если рассматривать тот же MRP, то администратором вручную задаётся управляющий коммутатор (Ring Manager) с чётким указанием портов, а при создании служебного канала обмена информацией между коммутаторами автоматически создаётся отдельная VLAN с уже настроенными политиками доступа (рис. 8). Никто, кстати, не запрещает одновременно использовать MRP и протоколы резервирования группы xSTP. В итоге, настроив правильно протоколы резервирования и политики Port Security, можно увеличить степень защиты сети, сохранив при этом её отказоустойчивость.

Легко обнаружить, легко атаковать

Следующий тип атак связан с наличием очень удобной функциональности ряда коммутаторов, которая позволяет обнаружить устройство и задать перво-



а *б*

Рис. 8. Резервирование сети при помощи кольцевой топологии: *а* – пример топологии сети, *б* – пример настройки протокола MRP

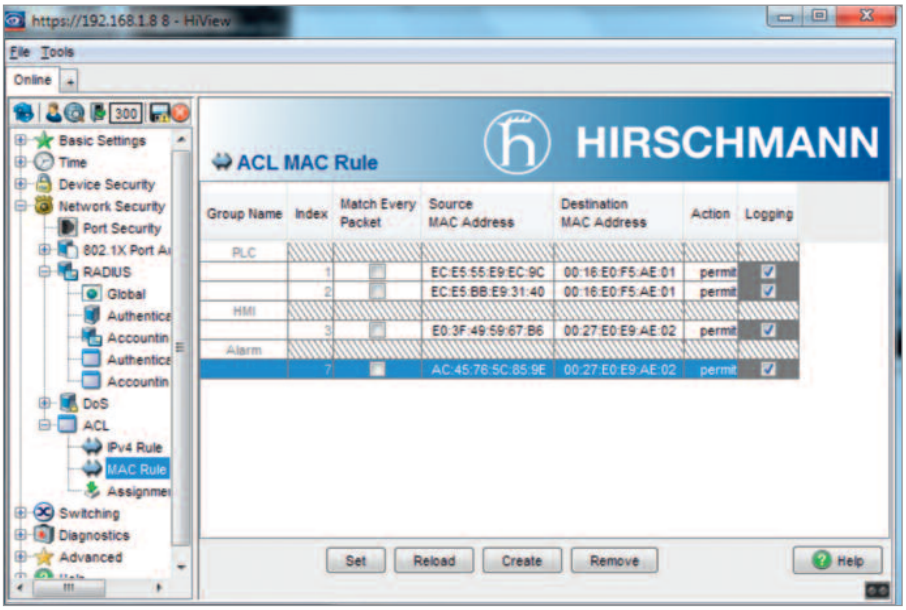


Рис. 9. Пример настройки списков доступа ACL

начальную конфигурацию. Такие протоколы, как CDP от Cisco и HiDiscovery от Hirschmann, фактически позволяют заменить консольный порт, с их помощью можно обнаружить устройство, определить его тип и задать первоначальные настройки.

Атака же сводится к отправке широковещательного запроса и перехвата ответного трафика, который и содержит в себе множество полезной информации, начиная от типа устройства, заканчивая настройками параметров в сети.

Как защититься?

Защититься можно банальным отключением данных протоколов. Да, конечно, обнаружить устройство теперь станет сложнее. Но и потери важных служебных данных не произойдёт.

Защитить DHCP-сервер

DHCP-сервер (Dynamic Host Configuration Protocol) – это сетевое устройство, которое позволяет автоматически получать параметры, необходимые для работы в сети со стеком протоколов TCP/IP. Работа строится по модели «клиент-сервер». Клиент на этапе конфигурации сетевого устройства обращается по DHCP-протоколу к серверу и получает от него нужные параметры. С одной стороны, это позволяет избежать ручной настройки сетевых устройств, а с другой стороны, это делает сеть уязвимой к специфическим атакам.

DHCP-атака

DHCP starvation. Данный тип атаки сводится к тому, что атакующий отсылает DHCP-серверу большое количество DHCP-запросов с разными MAC-адресами. В итоге рано или поздно весь набор свободных параметров закончится, и сервер не сможет обслуживать новых клиентов. В результате нарушается работоспособность сети.

Как защититься?

Данный вид атак не является классической атакой L2-уровня, но всё-таки может нарушить работу многих устройств, в том числе и работающих на канальном уровне. Метод борьбы с подобными атаками имеет название DHCP snooping и зачастую поддерживается коммутаторами [8]. Логика работы сводится к тому, что когда коммутатор получает фрейм, в котором находится DHCP-запрос, он сравнивает MAC-адрес в запросе и адрес, который присутствует на данном порту коммутатора. Если адреса совпадают, то коммутатор отправляет пакет дальше, так как данный клиент известен. Если адреса не совпадают, то коммутатор отбрасывает пакет.

Свой–чужой, списки доступа

Списки доступа – ACL (Access Control List) являются пограничной защитой, которые жёстко что-то разрешают либо что-то запрещают. Обычно список доступа разрешает или запрещает IP-пакеты, и реализуется это на базе брандмауэра. Но также существуют списки доступа на базе MAC-адресов. При этом появляется возможность создания списков доступа, как на базе конкретных портов, так и на базе созданных VLAN. На рис. 9 представлен графический интерфейс коммутатора RSP35. При создании ACL-правил устройство разрешает трафик для созданных правил, а весь остальной блокирует.

Заключение

При построении многоуровневой защиты промышленной Ethernet-сети зачастую не уделяется должного внимания угрозам второго, канального уровня модели OSI. Но угроз здесь достаточно много. Множество угроз не поддаётся обнаружению с помощью мощных L3-брандмауэров. Но они могут быть нейтрализованы при помощи современных промышленных коммутаторов, которые обладают очень удобными и эффективными механизмами защиты. Атаки типа MAC- и ARP-spoofing, VLAN hopping, STP attack, DHCP starvation могут быть предотвращены путём правильной настройки коммутатора. В дополнение создание списков доступа ACL позволит не только создать добавочную защиту, но и уменьшить нежелательный трафик. ●

Литература

1. Воробьёв С. Глубокая защита промышленного сетевого периметра // Современные технологии автоматизации. – 2017. – № 4.
2. Воробьёв С. “Defense in Depth” в действии. Уровень 1: защита границы сети // Современные технологии автоматизации. – 2017. – № 4.
3. ARP Spoofing #1 [Электронный ресурс] // Хакер. – Режим доступа : https://xakep.ru/2001/06/05/12756/.
4. Использование стандарта IEEE 802.1x в сети передачи данных [Электронный ресурс] // Сайт Хабрахабр. – Режим доступа : https://habrahabr.ru/post/138889/.
5. Защищаем сеть L2 коммутаторами [Электронный ресурс] // Сайт Хабрахабр. – Режим доступа : https://habrahabr.ru/post/231491/.
6. Одом У. Cisco CCNA, ICND2 200-101. – М. : Вильямс, 2015.
7. Томицки Л. Атака на протокол Spanning Tree [Электронный ресурс] // Сайт Securitylab. – Режим доступа : http://www.securitylab.ru/analytics/451090.php.
8. Бражук А. Защита внутри периметра [Электронный ресурс] // Хакер. – Режим доступа : https://xakep.ru/2013/08/23/safe-among-perimetr/.

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru