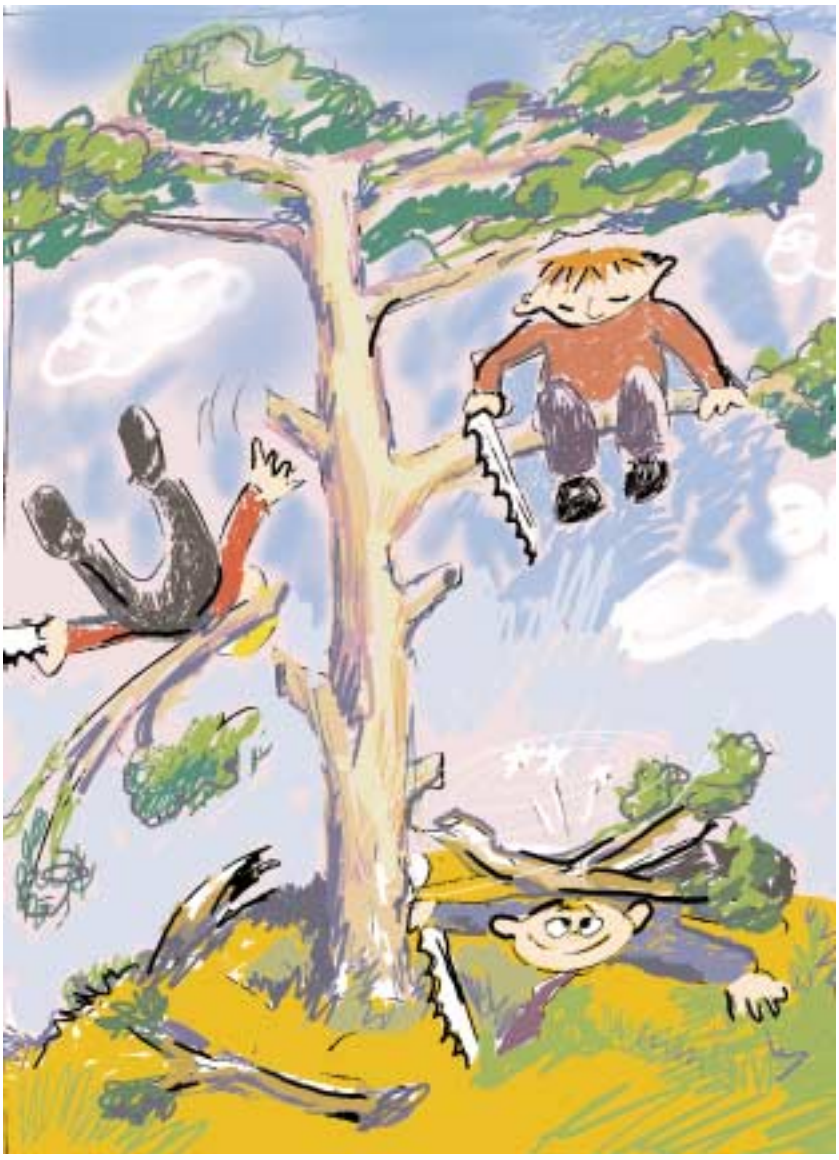
Отсутствие в протоколе Spanning Tree механизмов аутентификации позволяет без труда организовать атаку против сети на базе коммутаторов. Олег Артемьев, Владислав Мяснянкин

Опасные деревья в сетевых лесах



История человечества богата примерами, когда полезные и нужные изобретения, призванные облегчить жизнь, вдруг выходили из-под контроля своего создателя и проявляли совсем не запланированные свойства, зачастую очень неприятные. В этом отношении информационные технологии, в частности телекоммуникации, не составляют исключение.

Разработанная в первой половине 80-х гг. Международной организацией по стандартизации (International Standards Organization, ISO) семиуровневая модель взаимодействия открытых систем (Open System Interconnection, OSI) являет собой стройную иерархическую структуру, в которой каждый уровень строго выполняет возложенные на него обязанности, предоставляя сервисы верхнему и запрашивая их у нижележащего уровня. Однако стремление разработчиков к совершенству подталкивает их к реализации все новых и новых функций. Так, традиционно второй (канальный) уровень модели OSI отвечает за прием/передачу кадров и определение аппаратных адресов, современное же сетевое оборудование реализует на этом уровне механизмы обеспечения отказоустойчивости, мультиплексирования и разделения потоков информации. К сожалению, при этом не всегда до конца продумываются вопросы безопасности.

В данной статье речь пойдет о недочетах в реализации одного из протоколов, работающих на втором уровне OSI, а именно — Spanning Tree Protocol (STP). Учитывая щекотливость ситуации с описанием уязвимых мест и неоднозначное отношение сетевого сообщества к этой теме, изложение будет построено таким образом, чтобы не дать возможности хакерам-любителям использовать его в качестве пошагового руководства к действию. Объем накопленного в процессе исследования протокола STP материала слишком велик для публикации в журнальной статье. В связи с этим полная информация будет доступна в Internet спустя некоторое время после выхода журнала, но с изложенными в публикуемой лицензии ограничениями, под действие которой попадает и данная статья.

ЧТО ТАКОЕ STP?

Основное предназначение STP — автоматическое управление топологией сети с дублирующими каналами. Действительно, если сетевое оборудование связано для надежности избыточным числом соединений (см. Рисунок 1), то без принятия дополнительных мер кадры будут доставляться получателю в нескольких экземплярах, что приведет к сбоям. Следовательно, в каждый момент времени должен быть задействован только один из параллельных каналов, но при этом необходимо иметь возможность переключения при отказах или физическом изменении топологии. С этой задачей может вручную справиться администратор, однако более элегантным и экономичным решением, освобождающим от необходимости круглосуточного мониторинга состояния системы человеком, является использование STP.

Для своей работы STP строит граф, называемый также «деревом», создание которого начинается с корня (root). Корнем становится одно из STP-совместимых устройств, выигравшее выборы. Каждое STP-совместимое устройство (это может быть коммутатор, маршрутизатор или другое оборудование, но для простоты далее мы будем называть такое устройство мостом) при включении считает, что оно является корнем. При этом оно периодически посылает на все свои порты специальные блоки данных — Bridge Protocol Data Units (BPDU). Адрес получателя в пакетах, несущих BPDU, является групповым, что обеспечивает его пропуск неинтеллектуальным оборудованием.

В данном случае под адресом понимается MAC-адрес, так как протокол STP функционирует на уровне управления доступом к среде передачи (Media Access Control, MAC). Из этого также следует, что все дальнейшие рассуждения о STP и его уязвимостях не привязаны к какому-то одному методу передачи, т. е. в равной мере относятся к Ethernet, Token Ring и т. д.

Получив очередной BPDU от другого устройства, мост сравнивает полученные параметры со своими и, в зависимости от результата, перестает или продолжает оспаривать статус корня. В результате корнем становится устройство с наименьшим значением идентификатора моста (Bridge ID). Последний представляет собой комбинацию MAC-адреса и заданного для моста приоритета. Очевидно, что в сети с единственным STP-совместимым устройством оно и будет корнем.

Выбранный корень, или назначенный корневой мост (Designated Root Bridge, в соответствии с терминологией стандарта), не несет никакой дополнительной нагрузки — он всего лишь

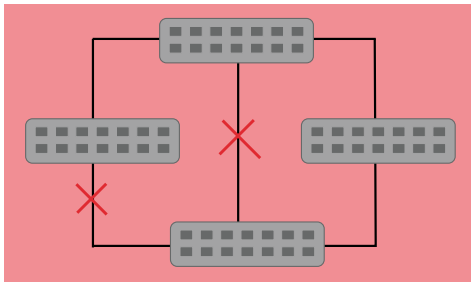


Рисунок 1. Сеть с заблокированными избыточными соединениями.

служит отправной точкой для построения топологии.

Для всех остальных мостов в сети определяется корневой порт (Root Port), т. е. ближайший к корневому мосту порт. От других портов, соединенных с корневым мостом непосредственно или через другие мосты, он отличается своим идентификатором — комбинации из его номера и задаваемым администратором «веса».

На процесс выборов влияет и стоимость пути до корня (Root Path Cost) — она складывается из стоимости пути до корневого порта данного моста и стоимости путей до корневых портов мостов по всему маршруту до корневого моста.

Помимо выделенного корневого моста в STP вводится логическое понятие назначенного моста (Designated

Bridge) — владелец этого статуса считается главным в обслуживании данного сегмента локальной сети. Статус назначенного моста также выборный и может переходить от одного устройства к другому.

Аналогичным образом вводится логическое понятие выборного назначенного порта (Designated Port, он обслуживает данный сегмент сети), а для него — понятие соответствующей стоимости пути (Designated Cost).

После окончания всех выборов наступает фаза стабильности, характеризуемая следующими условиями.

1. В сети только одно устройство считает себя корнем, а остальные периодически анонсируют его как корень.
2. Корневой мост регулярно посылает на все свои порты пакеты с BPDU. Интервал времени, через который происходит рассылка, называется интервалом приветствия (Hello Time).
3. В каждом сегменте сети имеется единственный назначенный порт, через который происходит обмен трафиком с корневым мостом. Он имеет наименьшее значение стоимости пути до корня по сравнению с другими портами в сегменте. При равенстве этой величины в качестве назначенного выбирается порт с наименьшим идентификатором порта (MAC-адрес порта и его приоритет).
4. BPDU принимаются и отправляются STP-совместимым устройством на всех его портах, даже на тех, которые были «отключены» в результате работы STP. Однако BPDU не принимаются на портах, которые были «отключены» администратором.
5. Каждый мост осуществляет пересылку (Forwarding) пакетов только между корневым портом и назначенными портами соответствующих сегментов. Все остальные находятся в блокированном состоянии (Blocking).

Как следует из последнего пункта, STP управляет топологией путем изменения состояния портов, которое может принимать следующие значения:

- блокирован (Blocking). Порт заблокирован, однако, в отличие от пользовательских кадров, кадры с пакетами STP (BPDU) принимаются и обрабатываются;
- ожидает (Listening). Первый этап подготовки к состоянию пересылки. В отличие от пользовательских кадров, кадры с пакетами STP (BPDU) принимаются и обрабатываются. Обучения не происходит, так как в этот период в таблицу коммутации может попасть недостоверная информация;
- обучается (Learning). Второй этап подготовки к состоянию пересылки. Кадры с пакетами STP (BPDU) принимаются и обрабатываются, а пользовательские кадры мост принимает для построения таблицы коммутации, но не пересылает данные;
- передает (Forwarding). Рабочее состояние портов, когда передаются как кадры с пакетами STP, так и кадры пользовательских протоколов.

Во время реконфигурации сети порты мостов находятся в одном из трех состояний — Blocking, Listening или Learning, т. е. пользовательские кадры не передаются, и сеть работает лишь сама на себя.

В стабильном состоянии сети все мосты ожидают периодической посылки корневым мостом специальных пакетов приветствия — Hello BPDU. Если в течение промежутка времени, определяемого значением Max Age Time, таких пакетов от корневого моста не поступает, мост считает, что либо между ним и корневым мостом пропала связь, либо последний отключен. В этом случае он инициирует реконфигурацию топологии сети. Путем задания соответствующих параметров можно регулировать, насколько быстро мосты будут обнаруживать изменения в топологии и задействовать запасные маршруты.

Несколько слов необходимо сказать об особенностях функционирования STP в сетях с поддержкой виртуальных локальных сетей (VLAN). Включение данного механизма на коммутаторе логически эквивалентно установке вместо него нескольких (по числу VLAN) коммутаторов, хотя, конечно, о физическом разделении VLAN речи не идет. Естественно было бы предположить, что в такой ситуации каждой VLAN будет соответствовать собственное дерево STP, однако поддержка раздельного функционирования STP в VLAN реализована не во всех моделях сетевого оборудования (например, Intel 460T поддерживает одно дерево STP на все VLAN; STP для каждой VLAN в серии коммутаторов Cajun компании Avaya поддерживается только в старших моделях). Это обстоятельство разрушает надежду на локализацию возможных атак на STP в пределах одной VLAN. Впрочем, угроза атаки сохраняется и в случае раздельного функционирования деревьев в VLAN.

Кроме рассмотренных выше стандартных свойств STP производители реализуют в своих устройствах дополнительные функции, расширяющие его возможности, такие, как Spanning Tree Portfast в оборудовании Cisco и STP Fast Start в некоторых коммутаторах 3Com. Суть этих расширений и их отношение к рассматриваемой проблеме будут описаны ниже. Кроме того, некоторые компании поддерживают собственные реализации STP, например Dual Layer STP от Avaya. Наконец, нестандартные модификации STP имеются для различных типов сетей (например, DecNet). Здесь стоит отметить, что все они построены на тех же принципах, различаясь в деталях и дополнительных возможностях (так, в случае Dual Layer STP от Avaya деревья 802.1D STP могут заканчиваться на портах 802.1Q-совместимого устройства). Все эти реализации подвержены тем же недостаткам, что и их прототипы. Нестандартные протоколы добавляют еще одну существенную проблему — исправить ошибки в них могут только разработчики.

СХЕМЫ ВОЗМОЖНЫХ АТАК

Идея первой группы атак лежит практически на поверхности. Суть заключается в том, что сам принцип функционирования STP позволяет легко организовать отказ в обслуживании. Действительно, в соответствии со спецификацией протокола, во время реконфигурации Spanning Tree порты задействованных устройств не передают пользовательские кадры. Таким образом, для приведения сети (или, по крайней мере, одного из ее сегмен-

тов) в неработоспособное состояние достаточно заставить STP-совместимое оборудование постоянно находиться в режиме реконфигурации. Это может быть инициализация выборов, например, главного корня, назначенного моста или корневого порта, т. е. любого из выборных объектов. При этом отсутствие в STP каких-либо механизмов аутентификации позволяет злоумышленнику относительно легко добиться своей цели путем посылки пакетов BPDU.

Программу, генерирующую BPDU, можно реализовать на любом из языков высокого уровня, если он позволяет работать с сокетами (raw-socket). Другой вариант — использование стандартных утилит для управления Spanning Tree, например из проекта Linux Bridge Project. Однако в последнем случае невозможна манипуляция параметрами STP со значениями, выходящими за пределы спецификации.

Ниже мы рассмотрим основные разновидности потенциальных атак.

Вечные выборы. Атакующий производит мониторинг сети при помощи сетевого анализатора и дожидается прохождения очередного конфигурационного BPDU от корневого моста, из которого он узнает его идентификатор. После этого он посылает в сеть пакет с идентификатором моста на единицу меньшим, чем у текущего корневого моста, тем самым заявляя о желании стать корневым мостом и инициируя выборы. Затем он вновь уменьшает на единицу значение идентификатора моста и посылает новый пакет, заставляя сеть перейти к новой волне выборов. По достижении минимального значения идентификатора, злоумышленник вновь переходит к значению, с которого он начал. Таким образом, сеть постоянно будет находиться в состоянии выборов корневого моста, и порты STP-совместимых устройств никогда не перейдут в состояние пересылки пакетов в течение этой атаки.

Исчезновение корня. В этой атаке злоумышленнику нет необходимости выяснять идентификатор текущего корневого моста. Он сразу устанавливает в отсылаемых пакетах минимально возможное значение, что, как мы помним, означает наивысший приоритет. По окончании выборов злоумышленник перестает передавать конфигурационные BPDU, что через промежуток времени Max Age Time приводит к повторным выборам, в которых он также участвует (и побеждает). Задав минимально возможное значение Max Age Time, он может добиться ситуации, когда сеть большую часть времени будет находиться в состоянии реконфигурации (данный тезис в равной степени относится и к предыдущей схеме атаки, а именно к той ее стадии, когда злоумышленник возвращается от минимального возможного значения идентификатора моста к начальному). Такая атака может показаться менее эффективной, однако она проще в реализации. Кроме того, в зависимости от масштабов сети и еще ряда условий (в частности, значения задержки пересылки Forward Delay, определяющего скорость перехода портов в состояние пересылки), порты STP-совместимых устройств при этой атаке могут никогда не приступать к пересылке обычных пакетов, что делает угрозу ее применения не менее опасной.

Слияние-расхождение деревьев. В сети с поддержкой VLAN возможно проведение модификации только что описанной атаки. Если злоумышленник подключит свою рабочую станцию, оснащенную двумя сетевыми интерфейсами, к портам коммутаторов, относящимся к разным VLAN, и начнет осуществлять пересылку BPDU из одной VLAN в другую, то в результате деревья STP обеих VLAN «увидят» друг друга, что приведет к перевыборам корня. По окончании выборов злоумышленник разрывает связь между VLAN, что по истечении Max Age Time снова вызывет реконфигурацию. Такие действия можно реализовать практически вручную, замыкая порты с помощью кроссировочного кабеля. Естественно, эта атака эффективна только в сетях с поддержкой отдельного дерева STP на каждую VLAN и организации VLAN на базе портов. К счастью, в крупных организациях доступ к портам оборудования ограничен.

Локализованный отказ в обслуживании. Злоумышленник может вызвать отказ в обслуживании не во всей сети, а лишь на одном из ее участков. Поводов для этого у него может быть много: например, для проведения атаки «ложный сервер» он может захотеть изолировать клиента-жертву от настоящего сервера. Реализацию данного вида атаки лучше рассмотреть на примере. В изображенной на Рисунке 2 сети серверы подключены непосредственно или через концентраторы к одному коммутатору, а клиенты — к другому. Злоумышленнику (на рисунке — атакующий), находящемуся в одном сегменте с клиентом, для «выключения» из работы одного из участников соединения (в данном случае — сервера) необходимо убедить ближайший к себе коммутатор, что он имеет лучший путь до второго коммутатора, к которому подключен сервер. В терминах STP, злоумышленник должен инициировать и выиграть выборы назначенного моста для «серверного» сегмента. В результате коммутаторы «отключат» использующийся в настоящий момент канал, переведя соответствующие порты в блокированное состояние, и связь между сегментами нарушится. После этого злоумышленник может выдавать себя за сервер или просто злорадствовать, если отказ в обслуживании был основной целью атаки.

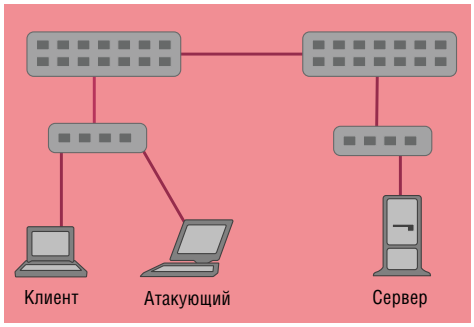


Рисунок 2. Сервер и клиенты подключены к разным компьютерам.

Фильтр BPDU. Основное назначение STP состоит в предотвращении образования колец. Очевидный метод атаки заключается в образовании кольца, наличие которого будет невозможно отследить средствами STP. Этого можно добиться, организовав физическое кольцо с фильтрацией на нем всех BPDU. Такая атака приведет

к частичному отказу в обслуживании или, когда у образующих кольцо каналов разные скорости, к существенной деградации пропускной способности. Действительно, если замкнуть в кольцо два концентратора и пустить запрос ping между двумя рабочими станциями, через некоторое время хождение пакетов прекратится — образовавшееся кольцо приведет к постоянной регенерации кадров.

Незаконный посредник (man in the middle). Эта и следующая атаки имеют принципиальное отличие от рассмотренных выше, так как они направлены не на достижение отказа в обслуживании, а ставят своей целью обеспечение перехвата информации, который при обычном функционировании сети невозможен.

Суть данной атаки с использованием STP заключается в изменении логической структуры сети таким образом, чтобы интересующий трафик шел через станцию атакующего. Снова обратимся к Рисунку 2. В отличие от рассмотренного выше частичного отказа в обслуживании, представим, что станция злоумышленника оснащена двумя сетевыми интерфейсами, один из которых подключен к клиентскому сегменту, а другой — к серверному. Посылая соответствующие BPDU, атакующий инициирует выборы назначенного моста для обоих сегментов и выигрывает их. Существующий канал между коммутаторами выключается, и весь межсегментный трафик направляется через станцию атакующего. В случае отсутствия намерения попутно устроить отказ в обслуживании для других станций и серверов, он должен обеспечить пересылку трафика. Причем если целью является простое прослушивание и модификация проходящего трафика не требуется, то реализация этой функции в виде программного модуля тривиальна; более того, любая ОС с поддержкой функций моста и STP, например Linux Bridge Project (см. ссылку в «Ресурсах Internet»), представляет уже готовое решение. Конечно, следует учитывать тот факт, что связь между коммутаторами может осуществляться со скоростью 100 Мбит/с, а «пользовательские» порты способны работать со скоростью 10 Мбит/с — тогда межсегментное соединение превратится в узкое место с неизбежной потерей пакетов. Ситуация может усугубиться, если часть трафика необходимо каким-либо образом изменить — злоумышленнику понадобится более мощная рабочая станция.

К счастью, эта атака невозможна в сети с единственным коммутатором (тогда это будет уже частичный DoS), и ее реализация тривиальна только в том случае, когда злоумышленник подключен одновременно к двум соседним коммутаторам. Если же он связан с коммутаторами, между которыми нет прямого соединения, ему придется подбирать, как минимум, один идентификатор моста, так как STP-совместимые устройства не передают дальше полученные BPDU, а лишь генерируют на их основе собственные.

Спровоцированный сниффинг. Сниффингом (sniffing) принято называть прослушивание сетевого трафика путем перевода сетевого интерфейса в режим приема всех пакетов (promiscuous mode), а не только адресованных ему или широковещательных. Очевидно, что в сети, построенной на базе коммутаторов, злоумышленник не имеет возможности перехватить пакеты, если они адресованы не ему, так как пакет направляется не во все порты (как на концентраторе), а лишь в тот, к которому присоединен получатель. Традиционно злоумышленники обходили данную проблему путем генерации шторма пакетов с различными MAC-адресами источника. Это приводило к переполнению таблицы коммутации (где хранятся соответствия между MAC-адресами и портами) вследствие ее конечного размера и, фактически, к переводу коммутатора в режим концентратора.

Аналогичных результатов злоумышленник может добиться и с использованием STP. Дело в том, что, в соответствии со спецификацией, после изменения дерева STP (например, после перевыборов назначенного моста) STP-совместимое устройство должно удалить из своей таблицы коммутации записи (за исключением статически заданных администратором значений), «возраст» которых больше, чем время, проведенное в состояниях прослушивания и обучения. Вследствие этого коммутатор кратковременно перейдет в режим концентратора, пока он не «обучится» и не заполнит таблицу вновь.

Внимательный читатель, конечно, уже заметил слабое место в этой теории: коммутатор обучается слишком быстро, после получения первого же пакета от «жертвы» он заносит данные об адресе в таблицу коммутации и перестает посылать следующие пакеты на все порты. Однако данную атаку не стоит игнорировать; это связано с внесением производителями сетевого оборудования расширений STP в свои изделия. Сразу после выборов STP сеть недоступна. Чтобы сократить время, на портах, к которым подключены серверы и рабочие станции, в коммутаторах многих производителей (Cisco, Avaya, 3Com, HP и др.) введена возможность пропуска состояний прослушивания и обучения, т. е. перехода из «блокирован» в «передает» и наоборот. У различных производителей такая возможность называется поразному: например, у Cisco — Spanning Tree Portfast, а у 3Com — STP Fast Start. Если данный режим включен, то постоянная инициализация выборов приведет не к отказу в обслуживании, а к постоянной очистке таблицы коммутации, т. е. переводу коммутатора в режим концентратора. Надо заметить, что эта функция не должна включаться на транковых портах, поскольку сходимость STP (переход в устойчивое состояние или прекращение перевыборов) не гарантирована. К счастью, для успешной реализации описанной атаки, злоумышленнику надо добиваться очистки таблицы коммутации, по крайней мере, вдвое чаще, чем приходят интересующие его пакеты, а на практике это зачастую невозможно.

Перехват трафика (а именно эту цель ставят перед собой две последние атаки) в сети на базе коммутаторов возможно осуществить и при помощи широко известной технологии arp-poisoning, суть которой заключается в дистанционной модификации («отравлении») таблиц arp жертв путем посылки ложных пакетов arp-reply. В результате оба участника соединения считают, что IP-адресу корреспондента соответствует MAC-ад-

рес злоумышленника, и последний может просматривать весь трафик между ними. Впрочем, данная атака эффективна лишь для перехвата IP-трафика и только между двумя IP-адресами. Атака же с использованием STP позволяет перехватывать весь трафик, так как осуществляется на канальном уровне OSI и изменяет маршрут движения всех кадров, несущих различные протоколы (IPX, NETBEUI), а не только IP.

ДРУГИЕ ВОЗМОЖНЫЕ АТАКИ

В числе непроверенных, но потенциально возможных атак, с точки зрения авторов, стоит отметить следующие.

Атака STP на соседнюю VLAN из собственной VLAN. Согласно 802.1Q, мост с поддержкой VLAN может по данному каналу принимать либо все кадры, либо только кадры с выставленными соответствующими тегами. Поскольку в сетях с VLAN на транковых портах STP будет передаваться в кадрах с выставленными тегами, то атаковать VLAN возможно путем отправки пакетов STP в кадрах с выставленными тегами порту, на котором не предусмотрена поддержка тегов. В 802.1Q предусмотрена возможность фильтрации таких кадров в зависимости от настроек моста. Например, оборудование Cisco отбрасывает кадры с выставленными тегами на не поддерживающих теги портах, по крайней мере, пользовательские, что ставит возможность данной атаки под сомнение.

Стоит отметить, что используемые для соединения сетей каналы глобальной сети уязвимы к атакам STP. Это явно указывается в спецификации BCP, где декларируется поддержка STP поверх каналов PPP глобальной сети. Неожиданным следствием этого может стать атака на сеть провайдера Internet через обычное коммутируемое подключение. Согласно RFC 2878, где описывается BCP, для поддержки STP на канале PPP она должна быть запрошена обеими сторонами, чего обычно не происходит. Тем не менее поддержка STP включена, например, на большинстве маршрутизаторов Cisco, как минимум, на тех из них, которые умеют организовывать виртуальные интерфейсы в группы мостов (bridge group).

В описании Generic Attribute Registration Protocol (GARP) отмечается, что STP — частный случай GARP. Часть рассмотренных в данной статье атак осуществима и против GARP вообще, и Generic Vlan Registration Protocol (GVRP) в частности. Данный факт позволяет утверждать, что VLAN нельзя использовать в качестве единственного средства защиты в сетях. Собственно, стандарт 802.1Q — логическое продолжение 802.1D, но при этом не свободен от тех же недостатков.

Авторы планируют продолжить исследование и тестирование нетрадиционного применения STP. Подробный разбор и подтверждение той или иной атаки можно будет найти на сайте авторов (см. «Ресурсы Internet»).

Какие же сети являются уязвимыми к атакам с использованием STP? Ответ неутешителен: все, поддерживающие стандарт 802.1D и, с некоторыми ограничениями, 802.1Q. Причем если для некоторых продуктов использование STP надо явно разрешить при конфигурировании, то другие, и таких большинство, поставляются с включенным STP «из коробки».

СПОСОБЫ ОБНАРУЖЕНИЯ И ЗАЩИТЫ

Основная сложность обнаружения атак против STP состоит в том, что для атаки используются стандартные пакеты протокола — C-BPDU, т. е. сам по себе факт наличия в сети пакетов STP не может безоговорочно означать атаку.

Другая сложность заключается в том, что система обнаружения атак (Intrusion Detection System, IDS) должна обладать некими эмпирическими данными об архитектуре сети и входящих в нее устройствах (в частности, перечнем всех идентификаторов мостов), в противном случае она не сможет отличить пакеты злоумышленника от обычного трафика STP.

Кроме того, поскольку атаке подвергается топология и работоспособность сети, IDS должна иметь собственный независимый канал для передачи сообщений ответственному за безопасность. Они могут передаваться через модем или подключенный к IDS мобильный телефон на пейджер или другой мобильный телефон, либо непосредственно через соединение IDS с рабочим местом администратора безопасности. При этом вполне возможно, что атака не будет обнаружена (false negative), если соответствующие BPDU окажут свое воздействие на оборудование раньше, чем будут зафиксированы датчиком IDS и переданы на центральную станцию, либо не появятся в контролируемых IDS сегментах.

В каждой конкретной сети можно попытаться описать ее нормальное состояние с точки зрения STP. Например, в сети, где STP на всех устройствах отключен, появление соответствующих пакетов с высокой долей вероятности может означать попытку атаки. Проведение серии выборов корневого моста с постоянным снижением значения идентификатора моста либо отсутствие других видов трафика, кроме STP, может означать атаку «вечные выборы». В сети, перечень идентификаторов мостов которой фиксирован и известен, появление BPDU с новым идентификатором также, скорее всего, означает атаку.

Возможно, эффективным решением станет внедрение адаптивных, самообучающихся IDS с применением технологии нейронных сетей, поскольку они могут сравнить текущее состояние сети с «нормальной» ситуацией. Одним из оценочных параметров может быть доля трафика STP в общем сетевом трафике.

Что сетевые администраторы могут сделать самостоятельно до кардинального решения проблемы?

1. Если использование STP в сети не является жизненно необходимым, данный протокол нужно отключить на всех поддерживающих его устройствах. Как уже говорилось выше, в большинстве устройств он включен по умолчанию.
2. В некоторых случаях управление дублирующими каналами можно осуществлять при помощи других механизмов, например Link Aggregation (поддерживается многими устройствами, в том числе Intel, Avaya и др.).
3. Если оборудование обладает функцией индивидуального включе-

Ресурсы Internet

Со средствами и методологией хакеров-любителей можно познакомиться на **http://cybervlad.port5.com/lspitz/enemy/index.html**.

Текст лицензии на данную статью и другие материалы авторов будут публиковаться на **http://olli.digger.org.ru/STP/**.

Стандарты ANSI/IEEE 802.1D на Media Access Control (MAC) Bridges и ANSI/IEEE 802.1Q на Virtual Bridged Local Area Networks можно получить на **http://standards.ieee.org/getieee 802/**.

Текст RFC 2878 с описанием PPP Bridging Control Protocol (BCP) можно найти на **http://www.ietf.org/rfc/rfc2878.txt**.

Описание BPDU можно прочитать на **http://www.protocols.com/pbook/bridge.htm#BPDU.**

Текст RFC 1700 с Assigned Numbers, авторы Дж. Рейнольдс и Дж. Постел, приводится на **http://www.iana.org/numbers.html.**

Описание STP Portfast компании Cisco дается на **http://www.Cisco.com/warp/public/473/65.html**.

Описание поддержки STP в коммутаторах SuperStack II Switch 1000 компании 3Com имеется на **http://support.3com.com/infodeli/tools/switches/s_stack2/3c16902/manual.a02/chap51.htm.**

Книги Медведовского И.Д., Семьянова П.В., Платонова В.В., «Атака через Internet». — СПб.: «Мир и семья», 1997, и Лукацкого А.В., «Обнаружение атак». — СПб.: «БХВ-Петербург», 2001, можно приобрести на **http://www.bolero.ru**.

С проектом Linux Bridge можно познакомиться на **http://www.math.leidenuniv.nl/~buytenh/bridge**.

ния/отключения STP на каждом порту, STP необходимо отключить на всех портах, кроме поддерживающих теги, если они связаны с другим сетевым оборудованием, но не с пользовательскими сегментами. Особенно это касается провайдеров Internet, так как недобросовестные пользователи могут осуществить атаку DoS как против сети провайдера, так и против других клиентов.

4. По возможности, необходимо сегментировать STP, т. е. создать несколько деревьев STP. В частности, если два сегмента сети (офисы) связаны одним каналом глобальной сети, использование STP на этом канале следует отключить.
5. При настройке сетевого оборудования входящее в идентификатор моста поле приоритета следует задать минимальным (что поднимает приоритет). Это снизит шансы злоумышленника выиграть выборы корневого моста при осуществлении атаки.
6. Если доступность сервисов имеет приоритетное значение, а конфиденциальность передаваемой информации обеспечивается протоколами верхних уровней, то при наличии в оборудовании функций, аналогичных Spanning Tree Portfast компании Cisco или STP Fast Start компании 3Com, их необходимо задействовать — это предотвратит атаки, направленные на отказ в обслуживании. Однако, как подчеркивают специалисты компаний-производителей, этого нельзя делать на портах, к которым подключены STP-совместимые устройства.

В свою очередь, разработчикам стандарта и производителям оборудования необходимо предусмотреть внесение ряда изменений в STP. Прежде всего это касается дополнения его механизмом аутентификации объектов, отсутствующим, к слову сказать, и во многих других сетевых протоколах. Реализация этого механизма возможна с использованием какого-либо распространенного криптографического протокола, например, следующим образом.

1. В пределах группы оборудования, которое должно образовать дерево STP, выбирается так называемый общий секрет (пароль, ключ), после чего он заносится в каждое включаемое в группу устройство (аппаратно, при помощи переключателей dip либо на смарт-карте или i-button).
2. Передаваемые BPDU защищаются при помощи Message Authentication Code (MAC), кода идентификации сообщения. Для этого к подготовленному к передаче пакету BPDU присоединяется общий секрет и для всего этого массива рассчитывается значение хэш-функции (например, SHA-1). Полученный хэш добавляется к отправляемому пакету BPDU (сам секрет при этом не передается).
3. На принимающей стороне к пакету добавляется общий секрет, рассчитывается хэш и сравнивается с полученным. В случае совпадения получатель удостоверяется, что пакет поступил от одного из членов группы, «знающих» общий секрет.

ЗАКЛЮЧЕНИЕ

Ошибки в такой сложной области, как информационные технологии и, в частности, телекоммуникации, практически неизбежны. Однако это не означает, что их развитие должно из-за этого тормозиться — не ошибается лишь тот, кто ничего не делает, как гласит народная мудрость. Между тем с усложнением технологий необходимо переходить к качественно другим методам проектирования и разработки, учитывающим все нюансы функционирования будущей системы, в том числе и вопросы обеспечения безопасности. На наш взгляд, перспективным является применение методов математического моделирования, с помощью которых не только проверяется поведение проектируемой системы в условиях стандартных управляющих и возмущающих воздействий, но и прогнозируется ее поведение при выходе ряда параметров за заданные граничные условия.

Закономерно, что разработчик прежде всего думает об основной цели разработки, побочные вопросы решаются во вторую очередь либо оставляются на потом. Однако, как показывает практика, если вопросы безопасности не учитываются с самого начала, в дальнейшем построение подсистемы безопасности в сколько-нибудь сложной информационной системе неэффективно и дорого, так как просчеты проектирования, в отличие от просчетов реализации и конфигурации, труднее всего обнаруживаются и устраняются. LAN

Олег Артемьев — независимый эксперт. С ним можно связаться по адресу: olli@digger.org.ru. Владислав Мяснянкин — независимый эксперт. С ним можно связаться по адресу: hugevlad@yahoo.com.