Защита информации

«*Атака против Spanning Tree*
или
Опасные деревья в сетевых лесах»

Эссе студента 011 группы

Климанова Максима

ФРТК МФТИ
2004г.

Отсутствие в протоколе Spanning Tree механизмов аутентификации позволяет без труда организовать атаку против сети на базе коммутаторов.

Предыстория

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 данном эссе речь пойдет о недочетах в реализации одного из протоколов, работающих на втором уровне OSI, а именно — Spanning Tree Protocol (STP).

Что такое STP?

Основное предназначение STP — автоматическое управление топологией сети с дублирующими каналами. Действительно, если сетевое оборудование связано для надежности избыточным числом соединений (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.

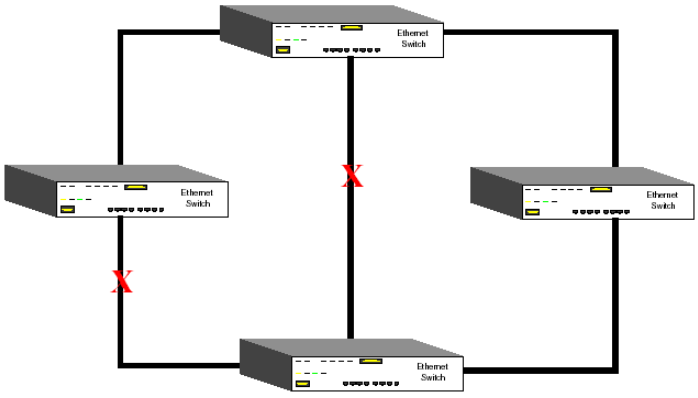

Рисунок 1.

Сеть с заблокированными избыточными соединениями.

Следует сразу оговориться, что речь идёт о топологии локальной сети на коммутаторах, потому что при увеличении числа машин (перерастанием сети размеров локальной) оптимальным решением будет использование ядра сети на устройствах уровня 3 модели OSI (роутерах[1]). Уровень доступа такой сети может использовать устройства первого и второго уровней. В ядре сети, содержащем избыточные связи (Рисунок 2), проблемы роутинга решаются при помощи протоколов маршрутизации (динамической или статической), некоторые из которых поддерживают балансирование нагрузки. На канальном же уровне говорить о маршрутизации не приходится, поэтому в сетях, вероятность появления дублирующих связей в которых велика, используется протокол связующего дерева (Spanning Tree).

[1] Маршрутизаторах.

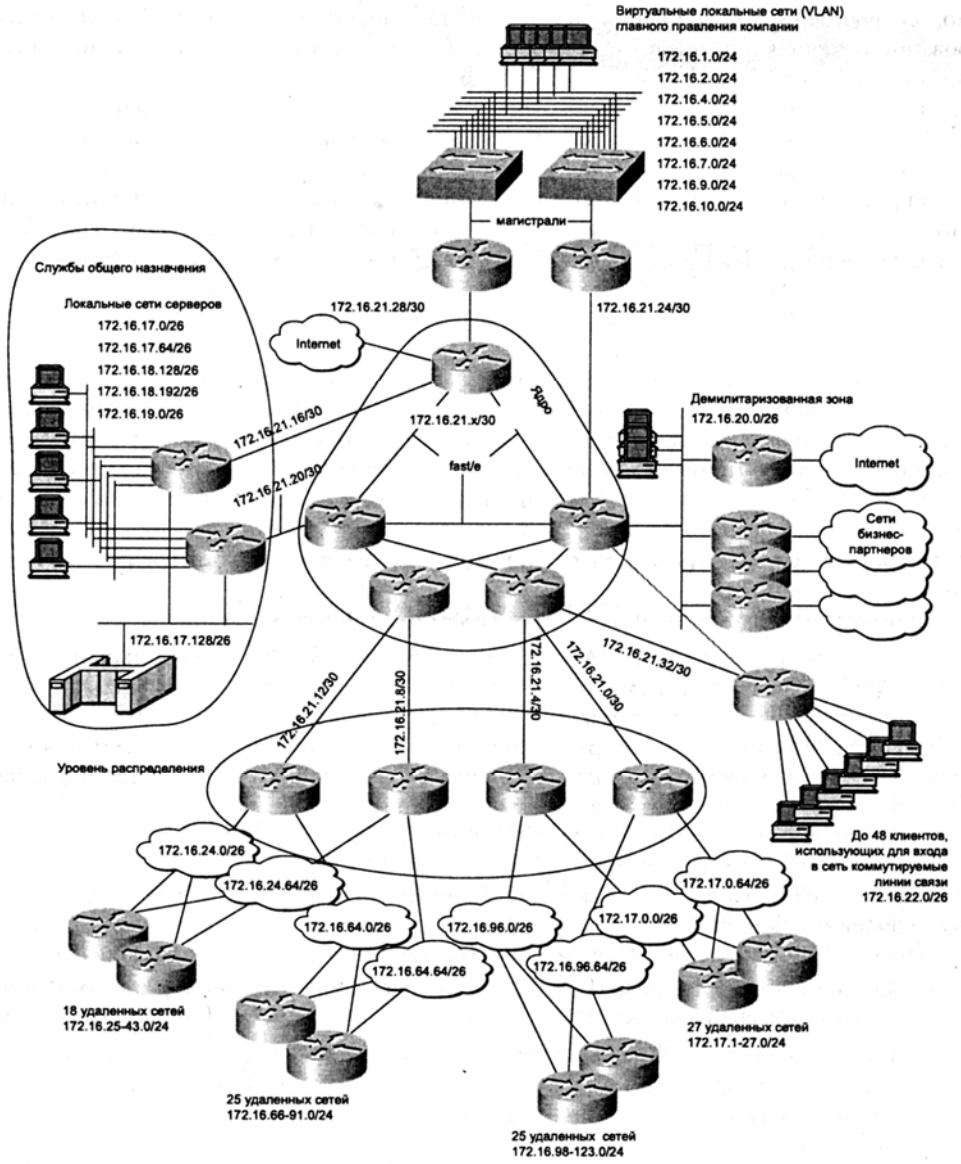

Рисунок 2

Крупномасштабная сеть

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[1]) 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.

Выборы

После получения мостом очередного BPDU происходит сравнение значений параметров, переданных во фрейме с собственными значениями параметров. Мост (основываясь на результате такого сравнения) прекращает, либо продолжает считать себя корнем, то есть оспаривать статус root'а. В конце концов, устройство, обладающее наименьшим (в рамках данной сети) наименьшим идентификатором моста (Bridge ID), становится корнем. Идентификатором моста является комбинация MAC-адреса и приоритета, заданного для этого моста. Если в нашей сети имеется лишь

[1] В данном эссе считаем switch и bridge синонимами.

одно STP-совместимое устройство, то именно оно и будет является корневым, так как никто не будет оспаривать его статус.

Следует отметить, что корень дерева STP или назначенный корневой мост (Designated Root Bridge) не несёт никакой специальной нагрузки, так как служит лишь центральной точкой для построения STP-графа (дерева). Оставшиеся мосты в сети определяют корневой порт (Root Port), которым является ближайший к root'у порт. Выбор корневого порта происходит путём сравнения идентификаторов портов, соединённых с корнем напрямую, либо же через другие мосты. Под идентификатором порта понимается комбинация номера порта и «веса», который задаёт администратор. Важным понятием (влияет на процесс выбора корневого порта) является стоимость пути до корня (Root Path Cost), которая складывается из стоимости пути до корневого порта данного моста и стоимости путей до корневых портов мостов по всему маршруту до корневого моста.

Кроме выбора корневого моста также производится выбор назначенного моста (Designated Bridge). Мост, обладающий таким статусом, является главным в обслуживании данного сегмента сети.

Также можно ввести понятие выборного назначенного порта Designated Port, занимающегося обслуживанием данного сегмента локальной сети. Для назначенного порта определяется стоимость пути (Designated Cost).

Фаза стабильности

Кроме фазы выборов существует фаза стабильности, которую можно выделить по следующим критериям:

1. В локальной сети STP существует единственное устройство-корень, остальные же анонсирует этот корневой девайс.
2. Корневой мост занимается регулярной рассылкой пакетов BPDU на все свои порты. Под интервалом приветствия (Hello Time) понимается отрезок времени, через который происходит рассылка.
3. Для каждого сегмента сети существует единственный назначенный порт, через который осуществляется обмен трафиком с root'ом. Для него характерно наименьшее значение стоимости пути до корня STP-графа по сравнению с другими портами этого сегмента. Если для двух портов стоимость пути совпадает, то назначенным выбирается тот из них, у которого идентификатор порта (MAC-адрес порта и его приоритет) наименьший.
4. Все STP-устройства принимают и отправляют фреймы с BPDU на всех портах без исключения (даже там, где порт был заблокирован механизмом STP). Однако следует заметить, что BPDU не принимаются на административно выключенных портах.
5. Каждое STP-совместимое устройство производит пересылку (Forwarding) данных пользователей только между корневым портом и назначенными портами соответствующих сегментов. Остальные порты находятся в STP-заблокированном состоянии.

Состояния портов

STP управляет топологией путем изменения состояния портов, которое может принимать следующие значения:

1. блокирован (Blocking). Порт заблокирован, однако, в отличие от пользовательских кадров, кадры с пакетами STP (BPDU) принимаются и обрабатываются;
2. 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;
3. 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;
4. 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.

Схемы возможных атак

Первое, что приходит в голову, это проанализировать сам алгоритм работы протокола STP, который позволяет без особых проблем организовывать атаку и отказ в обслуживании. И на самом деле это так, ибо во время построения STP-графа все интеллектуальные устройства сети, которые участвуют в переконфигурации, не могут заниматься пересылкой пользовательских данных. То есть для проведения атаки достаточно заставить сеть заниматься переконфигурацией. Процесс занимает 50 секунд, что является весьма значительным отрезком времени. Если проводить по-

стоянные переконфигурации, то сеть будет полностью неработоспособной. Поскольку в протоколе не существует схемы аутентификации, то это позволяет безнаказанно посылать BPDU, которые и вызывают переконфигурацию. Осуществить этот процесс можно путём постоянной смены корня. Программа, проводящая атаку, может быть написана на любом языке высокого уровня, который позволяет работать с raw-сокетами.

Вечные выборы.

Атакующий прослушивает сеть при помощи программного снифера или аппаратного анализатора, ожидает приход очередного конфигурационного BPDU от root'а. Из этого фрейма атакующий узнает идентификатор корневого моста. Далее атакующий может послать фрейм, содержащий идентификатор, который меньше на единицу, чем тот, который имеет настоящий корень. Это приведёт полную переконфигурацию сети. После установления стабильного состояния идентификатор корня вновь уменьшается на единицу. Мосты никогда не перейдут в состояние пересылки пользовательских пакетов в течении 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.

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 4 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.

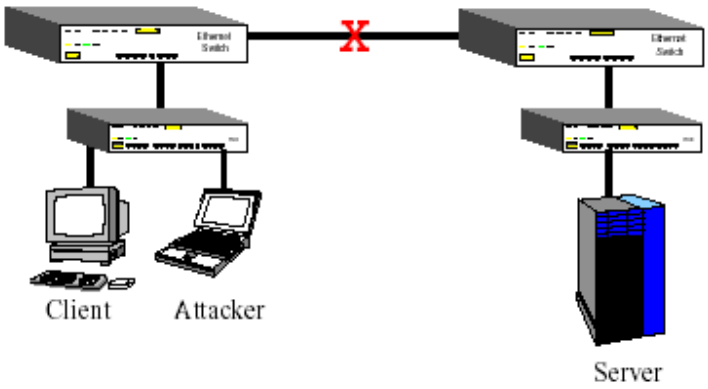

Рисунок 3
Частичный DoS

Фильтр BPDU.

Протокол связующего дерева разрабатывался специально для того, чтобы логически разорвать физические кольца, что происходит путём рассылки BPDU. А что будет происходить, если не давать возможность обмениваться

BPDU мостам, находящимся в кольце? Мосты, на которых взведён STP, будут считать, что кольца нет, значит, разрыва линка не произойдёт. Это приведёт к частичному отказу в обслуживании, ибо любой широковещательный пакет приведёт к бесконечному размножению последнего. Итак организовываем замыкание портов одного или двух разных мостов и ставим фильтр BPDU в этом кольце. Запускаем ping, наслаждаемся локальным отказом, основанном на 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 4. 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 по-разному: 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-адрес 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.

Способы обнаружения и защиты

Проблематичность детектирования атак против протокола связующего дерева состоит в том, чтобы при атаке злоумышленник использует стандартные кадры протокола – C-BPDU, то есть по самому факту присутствия этих фреймов нельзя безоговорочно судить о начале атаки. Другая сложность состоит в том, что сама система детектирования взлома (Intrusion Detection System, IDS) должна обладать некоторыми эмпирическими данными о топологии сети и всех активных устройствах в ней, например, должна содержать список всех идентификаторов мостов сети. Только при этом условии у неё появляется возможность отличить фреймы злоумышленника от легального трафика протокола STP. Так как атака нацелена на топологию и работоспособность сети, то система обнаружения должна обладать собственным независимым каналом передачи сообщения администратору безопасности. Для передачи может использоваться обычный модем, либо мобильный телефон, непосредственно подключённый к интеллектуальному устройству сети, либо же непосредственно через прямое соединение IDS с рабочим место администратора безопасности. При такой организации IDS нет гарантии, что атака вообще будет обнаружена, либо соответствующие BPDU уже окажут своё воздействие на сеть до того, как будут зафиксированы и переданы на центральную станцию. Для каждой STP-сети можно создать описание её нормального (с точки зрения STP) состояния. Например, очень странно будет принять C-BPDU из сегмента, где он административно выключен. Проведение серии выборов корневого моста с постоянным снижением значения идентификатора моста либо отсутствие других видов трафика, кроме STP, может означать атаку «вечные выборы». Если все идентификаторы мостов в сети известны, то появление BPDU с идентификатором не из этого списка, означает атаку. Для анализа безопасности сети можно использовать долю трафика STP по отношению к общему трафику. Что же могут сетевые администраторы сделать для решения подобной 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 включения/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.

Разработчики протокола и устройств, которые его поддерживают, могут также внести лепту в обеспечение безопасности сетей, использующих STP. Следует дополнить протокол связующего дерева механизмами аутентификации. 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.

Литература

1. http://www.bugtraq.ru/library/books/stp/index.html - введение в недокументированное применение протокола Spanning Tree.
2. http://www.protocols.com/pbook/bridge.htm#BPDU – описание BPDU.
3. http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a008007f7c5.html#wp1019820#wp1019820 – описание STP от Cisco.
4. http://www.Cisco.com/warp/public/473/65.html - описание Portfast от Cisco.
5. http://support.3com.com/infodeli/tools/switches/s_stack2/3c16902/manual.a02/chap51.htm - описание поддержки STP в коммутаторах SuperStack II Switch 1000 компании 3Com.
6. http://www.tekoc.ru/text/vlan/vlans.html - краткое описание VLAN технологии.