### Общие теоретические сведения

### Назначение протокола STP. Его функционирование

Протоколы остовного дерева — Spanning Tree Protocol (STP, стандарт 802.1d)  — сетевой протокол, работающий на втором уровне модели OSI.

Основное предназначение STP — автоматическое управление топологией сети с дублирующими каналами. Логично, что если сетевое оборудование связано для надежности избыточным числом соединений, 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, «победившее» 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 [6].

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 c 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 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" [7].

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 .

## 2. Построение логической топологии администратором сети

Не всегда протокол STP осуществляет автоматическое построение оптимальной логической топологии (рисунок 1). В этом случае настройка активной топологии должна быть выполнена вручную с использованием команд операционной системы, функционирующей на коммутаторах.

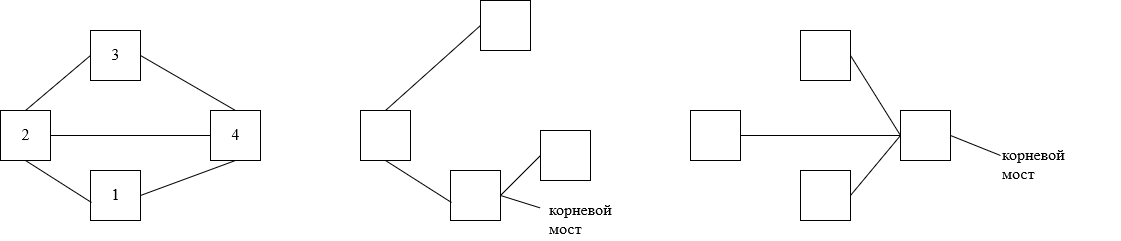


Рисунок 1 – Построение логической топологии протоколом STP

а) физическая топология, б) неоптимальная логическая топология, построенная протоколом STP, в) оптимальная топология, формируемая вручную

В тоже время задание корневого моста административно позволяет также указывать несколько маршрутов для распространения трафика по сети. Для балансирования нагрузки должны быть выполнены условия наличия в сети:

1. нескольких маршрутов, которые формируются физическими целевыми связями;
2. нескольких сетей VLAN.

В этом случае для трафика каждой из сетей VLAN администратором задается свой маршрут следования. При этом для конкретной сети VLAN формируется свой экземпляр связующего дерева. Таким образом, в пределах одной VLAN сеть является беспетлевой. Трафик в этой VLAN использует только один маршрут к пункту назначения. Балансирование (выравнивание) нагрузки основывается на выборе местоположения корневого моста для каждой VLAN. Правильное размещение корневого моста в каждой из сетей VLAN дает возможность потокам данных следовать к получателям по разным маршрутам. Размещение корневого моста должно осуществляться по следующим правилам:

1. корневые мосты необходимо размещать на маршрутах трафика большого объема (вблизи серверных групп, т.к. трафик “пользователь-сервер” занимает более 90% пропускной способности каналов);
2. корневой мост целесообразно назначить в центре VLAN.

При задании администратором VLAN местоположения корневого моста для каждой VLAN протоколом STP автоматически будут сформированы новые связующие деревья. Примеры балансирования нагрузки путем задания местоположения корневого моста приведены на рисунках 2,3.

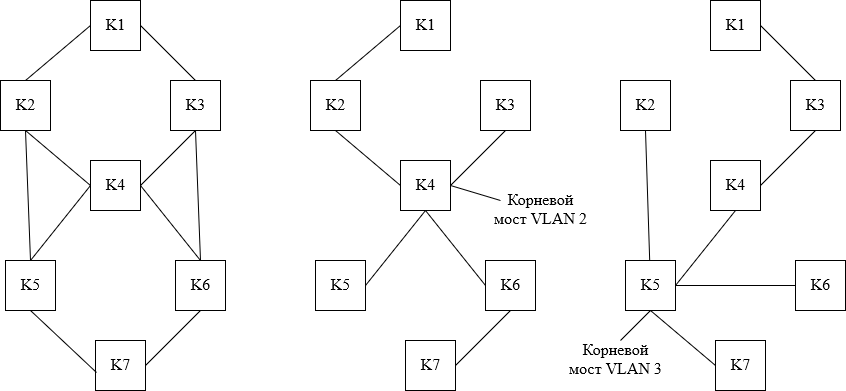


Рисунок 2 – Задание местоположения корневого моста в центре виртуальных локальных сетей

а) физическая топология сети; б) логическая топология для VLAN 2; в) логическая топология для VLAN 3.

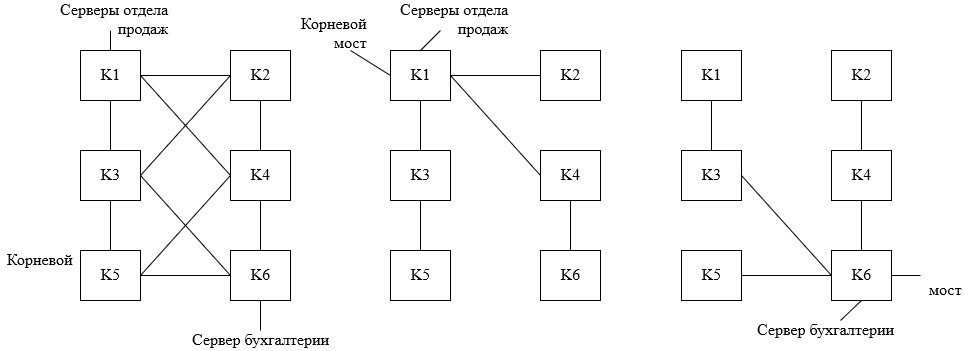


Рисунок 3 – Задание местоположения корневого моста вблизи серверных групп

а) физическая топология; б) логическая топология для VLAN 2; в) логическая топология для VLAN 3.

Для осуществления балансирования нагрузки с помощью выбора корневого моста для каждой сети VLAN реализуется изменение значения приоритета моста. Уменьшая значение приоритета, реализуют уменьшение BID, и, как следствие, изменяют топологию остовного дерева для соответствующей VLAN.

Для изменения приоритета моста используется следующий синтаксис команды:

**S1(config)#spanning-tree vlan *vlan-ID* priority *priority***

где приоритет можно назначать в диапазоне от 0 до 32768 с шагом 4096. Коммутатор с более низким приоритетом и будет корневым для соответствующей VLAN. Пример реализации команды:

**S1(config)#spanning-tree vlan 2 priority 0**

где 0 – приоритет коммутатора, vlan 1 - id VLAN

В тоже время в IOS существует команда, которая позволяет непосредственно указывать, что некоторый коммутатор будет являться корневым мостом в остовном дереве соответствующей VLAN. Синтаксис этой команды следующий:

**S1(config)#spanning-tree vlan *vlan-ID* root primary**

Пример реализации команды, выполняемой на коммутаторе, который должен быть назначен корневым мостом:

**S1(config)#spanning-tree vlan 2 root primary**

Однако только назначение корневого коммутатора каждой из VLAN еще не обеспечивает полного распределения нагрузки VLAN между различными путями следования трафика. На рисунке 4 показана локальная сеть, содержащая две VLAN, в которой, несмотря на назначение корневых мостов вручную, балансирование нагрузки не осуществляется.

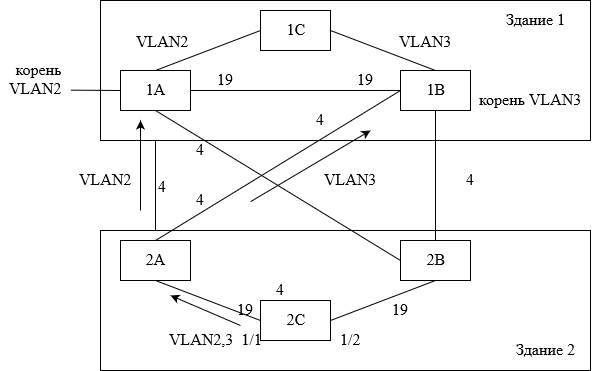


Рисунок 4 – Топология сети без балансирования нагрузки между VLAN 2 и VLAN 3

Балансирование нагрузки не осуществляется между коммутаторами 2A-2C и 2B-2C в здании 2 при пересылке данных с коммутатора 2C на корневые мосты соответствующих VLAN. Причина этому следующая.

При передаче данных с коммутатора 2C на коммутатор 1A (корневой мост VLAN 2) имеется два пути с одинаковой стоимостью (23): 1A-2 B-2C, 1A-2A-2C. В случае, если у 2A MAC-адрес имеет меньшее значение, чем у коммутатора 2B, путь следования данных для VLAN 2 протоколом STP определен следующим: 2C-2A-1A.

При передаче данных с коммутатора 2C на коммутатор 1В (корневой мост VLAN 3) имеется два пути с одинаковой стоимостью (23): 1B-2B-2C, 1B-2A-2C. По той же самой причине маршрут от коммутатора 2C к корневому мосту VLAN 3 следующий: 2C-2A-1B. Таким образом, канал между коммутаторами 2C-2A используя для передачи данных двух VLAN, а канал 2C-2B не загружен вообще.

Для того, чтобы информационный поток VLAN 2 двигался по маршруту 2C-2A-1A необходимо настройки коммутаторов оставить без изменений (протокол STP функционирует по умолчанию). Однако для перемещения трафика VLAN 3 по маршруту 2C-2B-1B необходимо для этой цели изменить приоритет коммутатора 2B, уменьшив его. Тогда при сравнении идентификаторов отправителей (2A и 2B) при равных стоимостях маршрутов порт 1/2 коммутатора 2C будет выбран как корневой. Поэтому трафик пойдет по маршруту 1C-2B-1B. Распределение нагрузки при изменении приоритетов мостов показано на рисунке 5.

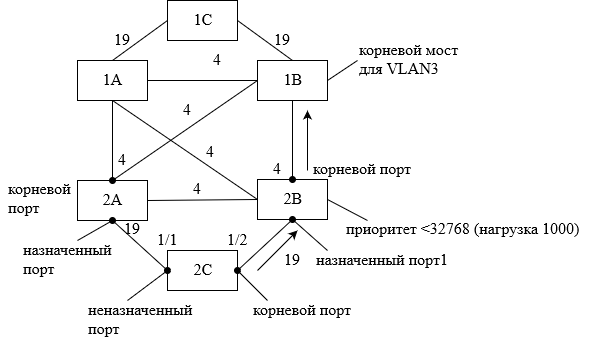


Рисунок 5 – Распределение нагрузки при изменении приоритетов мостов

Для балансирования нагрузки необходимо изменить приоритеты коммутаторов 2A и 2B таким образом, чтобы для VLAN 3 протокол STP выбирал коммутатор 2B, а для VLAN 2 – 2A. Значение приоритета должно находиться между значением приоритета корневого моста и приоритета по умолчанию.

Еще одним методом балансирования нагрузки при задании местоположения корневых мостов VLAN в сети является метод изменения стоимости портов.. Данный метод используется в случае, когда коммутатор уровня доступа соединен с двумя (для распределения нагрузки) коммутаторами распределения каналами связи с одинаковой стоимостью. В этом случае административное увеличение стоимости одного из каналов дает возможность направлять трафик по маршруту с изначально наименьшей стоимостью. Изменение стоимости маршрута осуществляется посредством команды, выполняемой для соответствующего интерфейса (т.е. перед выполнением команды необходимо указать интерфейс, стоимость которого будет изменяться):

**S1(config)#spanning-tree vlan 2 port-priority 160**

где 160 - приоритет, vlan 2 – id VLAN;

Пример балансирования нагрузки за счет изменения стоимости порта показан на рисунке 6. За основу взята физическая топология, изображенная на рисунке 4. Команды настройки стоимости портов на коммутаторе 2C имеет вид:

**S1(config)# interface fa1/2**

**S1(config)#spanning-tree vlan 2 port-priority 1000**

**S1(config)# interface fa1/1**

**S1(config)#spanning-tree vlan 3 port-priority 1000**

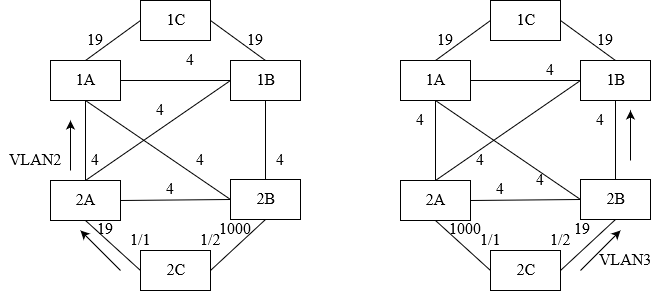
****

Рисунок 11 – Распределение нагрузки за счет изменения стоимости портов

а) VLAN 2; б) VLAN 3

Следует отметить, что упомянутые методы управления приоритетов коммутаторов и стоимостей портов должны применяться совместно с методом размещения корневого моста для VLAN и они позволяют административно управлять процедурой построения логической топологии (связующего дерева) и протоколе STP.