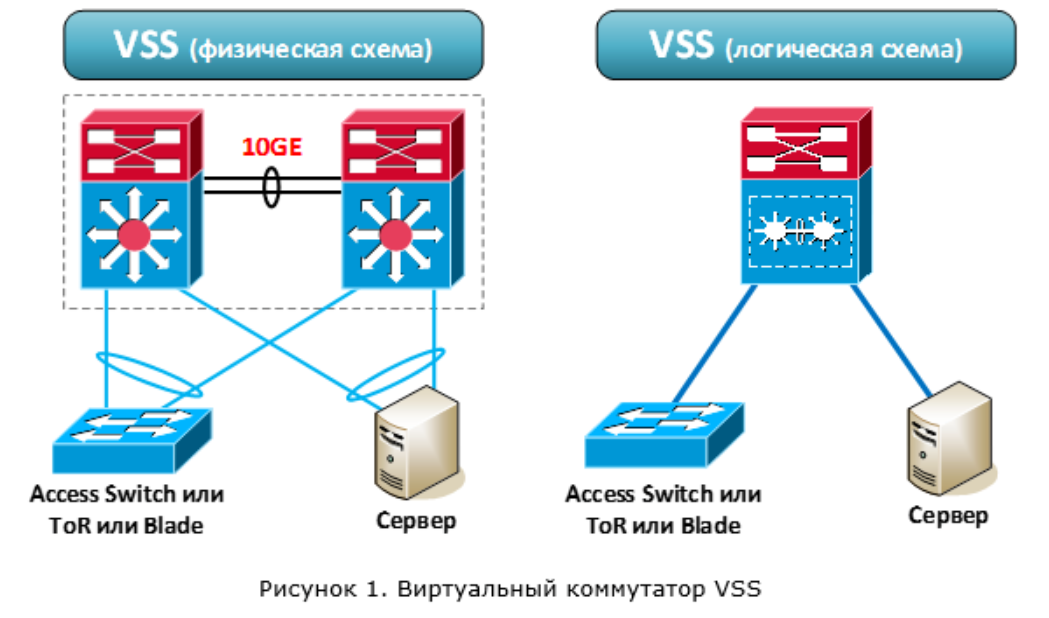
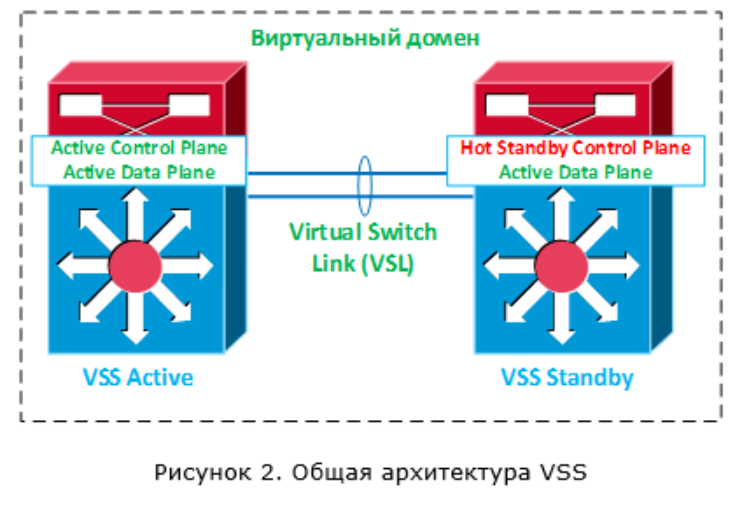
**Cisco VSS**

Технология VSS позволяет объединить два физических коммутатора в один логический. Но в отличии от более классических технологий стекирования (StackWise, FlexStack) для связи коммутаторов между собой используются не какие-то специализированные кабели, а Ethernet-порты. Таким образом, коммутаторы могут находиться на относительно большом удалении друг от друга.

После объединения коммутаторы начинают работать как один логический (рисунок 1). Оба коммутатора являются активными и обеспечивают передачу пакетов. При этом управление обоими коммутаторами осуществляется одним из устройств. Другими словами, уровень обработки данных (data plane) активен на обоих устройствах. А вот уровень управления (control plane) только на одном. Вспомним, что control plane отвечает за логику работы коммутатора: обработку всех сетевых протоколов (L2/L3), формирование таблицы маршрутизации, заполнение таблиц CEF, ACL, QoS и т.д.



Архитектура VSS представлена на рисунке 2. Один из коммутаторов выбирается основным, второй коммутатор — резервным. На основном коммутаторе control plane становится активным (Active), а на резервном переходит в состояние горячего резерва (Hot Standby).



Активный control plane управляет работой обоих коммутаторов. Также в процессе работы происходит постоянная синхронизация состояния между активным control plane на основном коммутаторе и control plane на резервном коммутаторе для обеспечения отказоустойчивости. Управление и синхронизация выполняются через специальный канал – Virtual Switch Link (VSL).

Канал VSL – это прямое соединение между двумя коммутаторами (никаких промежуточных устройств не допускается). Для обеспечения VSL канала коммутаторы подключаются друг к другу через обычные Ethernet-порты. Как можно догадаться, к этим портам также есть определённые требования и эти требования варьируются в зависимости от платформы коммутаторов. Ко всем пакетам, которые передаются через канал VSL, добавляется специализированный заголовок – Virtual Switch Header (его длина 32 байта):

VSL может состоять из нескольких физических каналов (что собственно и рекомендуется делать). Это необходимо для отказоустойчивости нашей системы, а также получения необходимой пропускной способности. Агрегация осуществляется с помощью протоколов PAgP или LACP. Т.е. максимально мы можем иметь 8 активных каналов, объединённых в один логический VSL. Например, если мы используется порты 10 Гбит/с, мы получим до 80 Гбит/с при агрегировании 8 таких каналов.

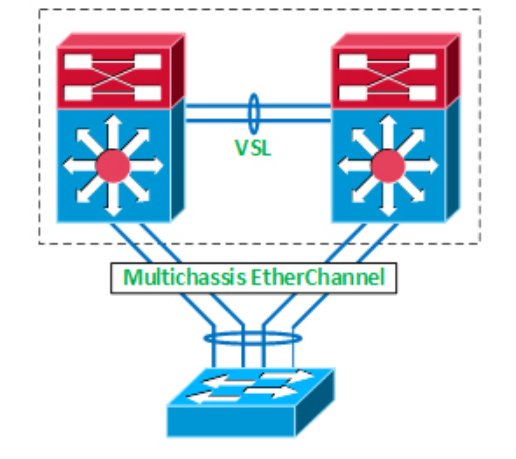
Через VSL передается:

* управляющий трафик системы (трафик протоколов, обеспечивающих работу виртуального коммутатора VSS, в том числе синхронизацию состояния между коммутаторами),
* сетевой управляющий трафик (трафик, адресованный control plane, но полученный резервным коммутатором: CDP, VTP, STP, EIGRP/OSPF и т.д.),
* пользовательский трафик (в том числе, широковещательный и многоадресный),
* сервисный трафик (например, SPAN).

Control plane на основном коммутаторе выполняет две функции. Первая – обеспечивает логику работы коммутатора: программирование коммутатора на основании конфигурации, обработку всех сетевых протоколов (L2/L3), формирование таблицы маршрутизации, таблиц CEF, управление портами и т.д. Вторая функция – заполнение всех аппаратных таблиц (FIB, Adjacency, ACL, QoS и т.д.) на обоих коммутаторах для обеспечения обработки пользовательского трафика (на аппаратном уровне). Control plane на резервном коммутаторе находится в состоянии горячего резерва. При этом состояние активного сontrol plane постоянно синхронизируется с резервным. Это необходимо для того, чтобы обеспечить беспрерывную работу нашего виртуального коммутатора в случае отказа основного физического коммутатора.

За синхронизацию состояния между коммутаторами отвечает механизм переключения с сохранением состояния (Stateful Switchover — SSO). Данный механизм появился достаточно давно. Например, он используется для резервирования супервизоров в рамках одного коммутатора 6500. Он же используется и в технологии VSS (придумывать что-то новое не стали). Но как мы помним, SSO не позволяет синхронизировать состояние протоколов маршрутизации. А значит при переключении на резервный коммутатор протоколы динамической маршрутизации запускаются с нуля. Что автоматически обрывает все L3-соединения с удалёнными устройствами. Т.е. мы получаем временную потерю связи с внешним миром. Для решения данной проблемы технология SSO работает в связке с технологией Non-Stop Forwarding (NSF). Данная технология выполняет следующие задачи: обеспечивает передачу пакетов L3 в момент переключения (по факту замораживает старые записи о всех маршрутах), оповещает удалённые маршрутизаторы о том, что не нужно рвать связь, а также запрашивает у них всю необходимую информацию для построения новой таблицы маршрутизации. Конечно, же удалённые устройства должны в этом случае также поддерживать технологию NSF (так сказать, быть NSF-aware).

Одна из основных причин использовать VSS – возможность агрегации нескольких каналов, приходящих на разные коммутаторы (в терминах Cisco – Multichassis EtherChannel (MEC)). Речь идёт о подключении к виртуальному коммутатору внешних устройств (например, других коммутаторов).



Когда мы агрегируем несколько каналов в один логический в рамках VSS, может использоваться один из протоколов динамической агрегации (PAgP или LACP) или же статический EtherChannel (режим ON). За распределение трафика внутри логического канала отвечает механизм на базе хеш-функции. Хеш-функция применяется к определённым полям заголовков, передаваемого трафика. Например, хеш-функция может применяется к значению IP-адреса отправителя. В этом случае, если у нас агрегируется два канала, то по первому каналу будут передаваться потоки трафика, у которых IP-адреса отправителя чётные, а по второму — нечётные. Это позволяет распределять потоки трафика между разными каналами, объединёнными в один etherchannel. В более сложных вариантах на принятие решения о выборе канала могут влиять сразу несколько параметров (например, Src IP + Dst IP + Src Port + Dst Port).

Оба коммутатора обрабатывают трафик, при этом всё управление сосредоточено на одном из них. В качестве общей соединительной шины используется канал VSL, через который происходит передача как минимум управляющей и синхронизирующей информации. Через этот же канал резервный коммутатор узнаёт, что основной коммутатор «умер». Но что будет если этот канал разорвётся, при этом оба коммутатора будут исправными? Ответ прост, основной коммутатор останется активным, а вот резервный коммутатор посчитает, что его коллега отказал, и соответственно тоже станет активным (везде речь про control plane). А так как конфигурация у этих коммутаторов одна, мы получим в сети два абсолютно одинаковых устройства с идентичной адресацией.

Для того чтобы избежать такой ситуации, как минимум не стоит разрывать VSL канал. Но не всегда это от нас зависит, поэтому есть механизм, который позволяют минимизировать последствия разрыва VSL канала. Данный механизм использует один из трёх методов обнаружения сбойной ситуации:

* Enhanced PAgP
* Fast Hello
* IP BFD

После того как будет определено, что оба коммутатора стали активными в следствии обрыва канала VSL, выполняются следующие действия:

1. Коммутатор, который был активным до того, как разорвался VSL канал, отключает все интерфейсы, кроме VSL и интерфейсов, для которых в ручном режиме указано, что их не нужно отключать. Такое поведение позволяет сети продолжать работать дальше, правда на одном коммутаторе, зато без коллизий.
2. Как только VSL канал будет восстановлен, коммутатор, который был изначально активным, перезагрузится. После перезагрузки он станет резервным.

Таким образом, при наступлении ситуации с двумя активными коммутаторами в конечном итоге активным остаётся тот, который был изначально резервным.

**Fast Hello**. В этом случае между коммутаторами VSS делается дополнительный прямой L2 канал (без промежуточных устройств). В рамках этого канала коммутаторы обмениваются сообщениями VSLP Fast Hello. И если VSL канал упал, но при этом пакеты VSLP Fast Hello продолжают ходить, у нас наступила сбойная ситуация. Время обнаружения сбойной ситуации – доли секунд (VSLP Fast Hello сообщения при падении VSL канала передаются с интервалом в 200 мсек).

**IP BFD (Bidirectional Forwarding Detection).** Данный механизм очень похож на работу Fast Hello, но более медленный (время обнаружения исчисляется секундами). Он может работать через прямой канал L3. Данный механизм не рекомендуется использовать из-за его медленности. Более того в последних релизах IOS он отсутствует.